KRIEG IM INFORMATIONSRAUM

ZUM 21. KONGRESS DER INFORMATIONSSTELLE MILITARISIERUNG

INHALTSVERZEICHNIS

ÜBER DIE AUTOR*INNEN:

SVEN WACHOWIAK ist Literaturwissenschaftler und Übersetzer; MORITZ TREMMEL ist aktiv beim Tech-Kollektiv mtmedia.org und bloggt u.a. bei Netzpolitik.org; HANS-JÖRG KREOWSKI ist Prof. für theoretische Informatik und Mitglied im Vorstand des „Froums Informatiker*innen für Frieden und gesellschaftliche Verantwortung“ (FIFF); FRANZ WANNER ist bildender Künstler und hat zuletzt u.a. im Lenbachhaus München ausgestellt; JOACHIM GUILLIARD ist IT-Berater und u.a. im Heidelberger Friedensbündnis aktiv; CHRISTOPHER SCHWITANSKI studiert Politikwissenschaft in Augsburg; ANNA HUNGER arbeitet seit zwölf Jahren als Journalistin und ist stellvertretende Redaktionsleiterin der „Kontext“-Wochenzeitung; JUDITH LAUTERBACH ist Linguistin, Aktivistin und Mitglied in der Redaktion der Sendung „Resonanz Con(tra)sens“ (http://www.wueste-welle.de/sendung/view/id/204); MICHAEL GODE beschäftigt sich nebenberuflich mit dem Thema Kommunikationsguerilla und bloggt u.a. auf der Plattform maqui.blogsport.eu; JÜRGEN WAGNER, CHRISTOPH MARISCHKA, JACQUELINE ANDRES, CLAUDIA HAYDT und ANDREAS SEIFERT sind aktiv bei der Informationsstelle Militarisierung.

BILDNACHWEISE:

S.4&5: BMVg (Abschlussbericht Aufbaustab, Ausriss); S.7: NATO (Titelbild); S.9: Screenshot JAPCC; S.10: Screenshot; S.11: Heereskommando, Titelblatt; S.13: Europäisches Parlament; S.17: Collage IMI; S.18: NATO StratCom CoE (Titelbild); S.20: commons.wikimedia.org; S.23: cryptome.org; S.25&26: wikileaks.org; S.29: Collage: Kreowski; S.31: FIFF; S.32: Franz Wanner; S. 34 Ausrisse (wie angegeben); S.35-39: Fran Wanner; S.40: Bundesnetzagentur (Titelblatt Frequenzplan); S.41: IMI; S.42: Burkhard Luber: Bedrohungsatlas; S.43: IMI; S.44: Screenshot (dlr.de); S.45&46: IMI; S.48: BMVg (Screenshot); S.49 AFCEA Bonn; S.51: Screenshot (steep.de); S.52: Screenshot (rola.com); S.53: BMVg (Screenshot); S.54: Sceenshots, Collage: IMI; S.55: Screenshot (tagesschau.de); S.56: Screenshot (spiegel.de); S.57: Screenshot (syriaradionetwork.org); S.61: wikipedia.org; S.63&64: Uwe Krüger; S.67: Screenshots, Collage: IMI; S.68: Freies Radio Wüste Welle; S. 70: BMVg via Facebook.

IMPRESSUM:

Herausgegeberin ist die
Informationsstelle Militarisierung e.V.
Hechinger Str. 203, 72072 Tübingen
www.imi-online.de - imi@imi-online.de
Erscheinungszeitpunkt: März 2018
Schutzgebühr: 5,-
Redaktionelle Bearbeitung: IMI

IMI Informationsstelle Militarisierung e.V.

KRIEG IM INFORMATIONSRAUM
BERICHT VOM IMI-KONGRESS 2017

Dass sich der jährliche Kongress der Informationsstelle Militarisierung (IMI e.V.) im November 2017 dem „Krieg im Informationsraum“ widmete, hatte verschiedene Gründe. Der augenfälligste Anlass dürfte die Aufstellung des Kommandos Cyber- und Informationsraum Mitte 2017 gewesen sein. Dem zugehörigen Organisationsbereich mit gut 13.000 Dienststellen steht ein eigener Inspekteur vor, womit er den Teilstreitkräften Heer, Marine und Luftwaffe nahezu gleichgestellt ist. Darüber hinaus zeigte sich auch in der praktischen Arbeit der IMI in den letzten Jahren verstärkt, dass gerade in der internationalen Politik mit vielfältigen, oft manipulierten Nachrichten umzugehen ist. Spekulationen über die Urheber und Motive von Cyberattacken und Leaks sind Teil der Geopolitik und der verschärften Spannungen zwischen den USA und Russland geworden. Immer deutlicher zeigen sie ihr Potential, auch zu handfesten militärischen Konflikten zu eskalieren.

DIE AUSRUFUNG DES INFORMATIONSKRIEGS...

Ein weiterer Anlass für die Themenwahl war ein wenig beachtetes Dokument, welches das Europäische Parlament (EP) im November 2016 verabschiedet hatte und das einleitend vorgestellt wurde. Darin wird die Behauptung aufgestellt, dass sowohl der Islamische Staat wie auch Russland einen „Informationskrieg“ gegen die Europäische Union führen würden und dass dieser Teil einer hybriden Kriegführung wäre. Das EP fordert mit Nachdruck auf, diesen „Informationskrieg“ anzuerkennen und Gegenmaßnahmen zu ergreifen. Sowohl bei der Beobachtung „feindliche[r] Informationsmaßnahmen“ und damit zusammenhängender Finanzströme, als auch bei der Erarbeitung von Fähigkeiten, diese zu unterbinden, sei eine enge und kontinuierliche Zusammenarbeit mit der NATO anzustreben.

Die drei anschließenden Vorträge griffen Beispiele bereits jetzt bestehender Schieflagen in der Berichterstattung durch klassische und „neue“ Medien auf. Christopher Schwitanski zeigte zunächst anhand einer Netzwerkanalyse von Uwe Krüger, dass führende Journalisten und Redakteure sog. Leitmedien, insbesondere der Süddeutschen Zeitung, der Welt, der Frankfurter Allgemeinen Zeitung und der Zeit eng mit NATO-eigenen oder Nato-nahen Thinktanks vernetzt sind und sich hieraus eine wohlwollende Berichterstattung zugunsten des transatlantischen Bündnisses teilweise erkläre. Joachim Guilliard verglich daraufhin die Berichterstattung über die Kämpfe um die Stadt Mossul einerseits und Aleppo andererseits. Obwohl die Stadt Mossul viel umfangreicher zerstört worden und bis heute ein Großteil der Flüchtlinge nicht zurückgekehrt sei, hätten zivile Opfer und sonstige Folgen der Luftangriffe in der Berichterstattung keine große Rolle gespielt. Ganz anders sei hingegen die kurz zuvor begonnene Rückeroberung Aleppos durch die syrische Armee und deren Verbündete dargestellt worden: Im Mittelpunkt standen hier Berichte über zivile Opfer, häufig von Bildern unterfüttert, die von Organisationen wie den White Helmets geliefert wurden, die gemeinsame Sache mit den Islamisten machten. Jacqueline Andres stellte anschließend eine Studie der NATO zu „sozialen Medien als Instrument der hybriden Kriegführung“ vor. Aus dieser gehe u.a. hervor, dass die NATO soziale Medien auch als Quelle für die Zielortung genutzt habe. Anhand der Kampagnen zivilgesellschaftlicher Gruppen, „Kony 2012“ und „#BringBackOurGirls“ wurde beschrieben, wie – vermeintlich für die Betroffenen vor Ort sprechend – Zustimmung für die umfangreiche Stationierung US-amerikanischer Truppen auf dem afrikanischen Kontinent generiert wurde.

...DIE GEHEIMDIENSTE...

Claudia Haydt sprach anschließend über Leaks und Whistelblowing als Instrumente der Geopolitik. Sie nannte dabei v.a. Beispiele aus Südkorea, wo die Einflussnahme der Geheimdienste auf innenpolitische Auseinandersetzungen mittlerweile gut aufgearbeitet sei. Diese hätten im Wahlkampf 2012 mit gefälschten Leaks über Twitter und Facebook den Gegnern der konservativen Präsidentin Park die Zusammenarbeit mit Nordkorea vorgeworfen.Auf der anderen Seite seien Informationen über den Ausbau einer US-Basis in Südkorea über eine US-amerikanische Plattform veröffentlicht worden, was zu massiven Protesten führte, die international jedoch weniger wahrgenommen wurden, als der sog. ‚Sony-Hack‘, bei dem angeblich die Produktionsfirma eines Films in den USA gehackt wurde, der den nordkoreanischen Machthaber lächerlich machte. Haydt stellte anhand dieses Beispiels die Frage, ob man nicht viele Themen und Nachrichten auch als (bewusst oder unbewusst erzeugtes) „Rauschen“ verstehen müsste, in dem relevantere Nachrichten, wie der Konflikt um den Ausbau von US-Militärbasen in Südkorea, untergehen.

Anschließend stellte Moritz Tremmel verschieden Aktivitäten der westlichen Geheimdienste v.a. auf der Grundlage der Snowden-Leaks vor. Einerseits gäbe es bei westlichen Geheimdiensten die Mentalität „alles zu sammeln“, also sämtliche Kommunikation zu verfolgen und möglichst lange zu speichern. Andererseits würden zentrale Knotenpunkte weltweiter Kommunikation, wie etwa in Frankfurt, abgehört. Neben dieser anlass- und verdachtsunabhängigen Massenüberwachung existiere noch das gezielte Hacking, bei dem sich Geheimdienste Sicherheitslücken zunutze machen, um in die Systeme von Gegner*innen

einzudringen und dort u.a. nach belastendem oder diskreditierendem Material zu suchen.

… UND DIE NATO.

Ein weiterer Programmpunkt setzte sich mit der Perspektive der NATO auf den Informationsraum auseinander. Hierzu wurde von Sven Wachowiak einführend ein Strategiedokument aus dem Jahr 2007 vorgestellt, in dem führende Militärs im Bündnis bereits davor gewarnt hatten, dass die Mitgliedsstaaten die Kontrolle der Informationsflüsse und die Hoheit bei der Gestaltung der öffentlichen Meinung zu verlieren drohten. Durch eine eigene Informationsstrategie bzw. Informationsoperationen sei es nötig, „das Ruder wieder zu übernehmen“, um der Weltöffentlichkeit klar zu machen, dass es sich bei der NATO um „eine Macht des Guten“ handele, für die es zentral sei, nach einem Ereignis „auf den Bildschirmen präsent zu sein, bevor es der Gegner ist“.

Hieran knüpfte Jürgen Wagner mit Strategiedokumenten jüngeren Datums an, in denen ganz klar von „Informationen als Waffe“ die Rede ist. Als wichtiger Akteur werde von der NATO eine sog. „Lawfare-Bewegung“ ausgemacht, die den Einsatz bestimmter Waffen verbieten will und angeblich von Russland unterstützt werde, weil dieses die Überlegenheit der NATO-Luftwaffen fürchte. Eine entsprechende Konstellation sei kürzlich auch bei einer gemeinsamen Übung von EU und NATO durchgespielt worden.

(UN-)SAGBARKEIT VON WIDERSPRÜCHEN

Den Samstag beendete der Künstler Franz Wanner mit einem videografischen Vortrag, der Ausschnitte seiner Filme einbezog. Wanner hatte sich mit mehreren Rüstungsunternehmen und militärischen Forschungseinrichtungen auseinandergesetzt. Am Beispiel des Ludwig-Bölkow-Campus in Ottobrunn bei München zeigte er, wie die nationalsozialistische Geschichte und der militärische Charakter des Ortes verschleiert werden. Grundsätzlich gehe er der Frage nach, wie es gelinge, „sich als Gesellschaft selbst als friedfertige Demokratie zu erleben und gleichzeitig einen expansiven Militarismus zu betreiben, der sehr viele Felder betrifft.“ In diesem Zusammenhang verwies er darauf, dass NATO und Bundeswehr bereits seit Jahren versuchten, eine „Battle Management Language“ zu entwickeln, eine Sprache für Mensch-Maschine-Systeme, die keine Mehrdeutigkeiten und keine Widersprüche erlaube bzw. kenne.

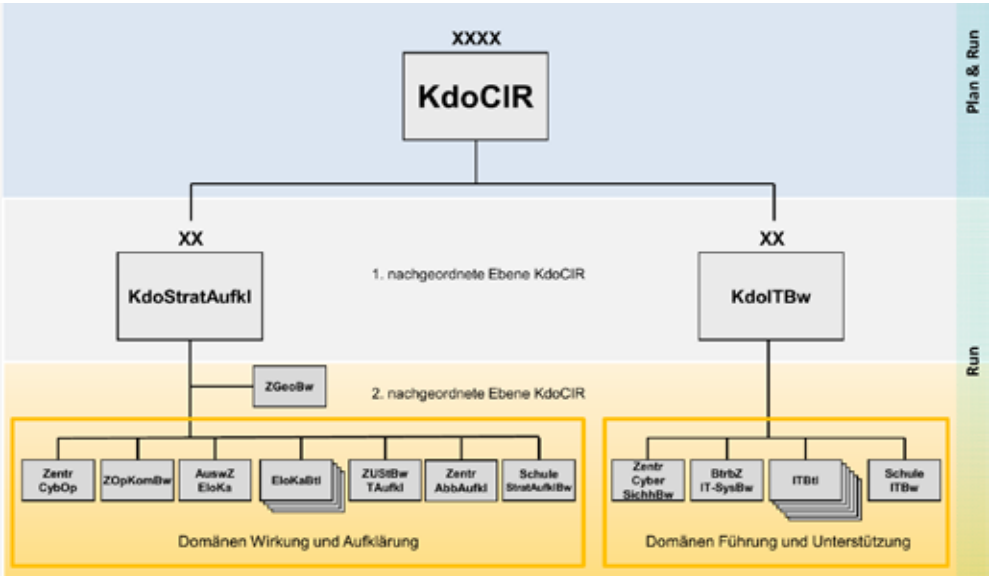
CYBERWAR…

Der Sonntag widmete sich zunächst im engeren Sinne der militärischen Sicht auf Cyberkrieg und Kommunikationstechnik. Hans-Jörg Kreowski, emeritierter Professor für theoretische Informatik, gab zunächst einige Beispiele für erfolgte Cyberattacken. Grundsätzlich ließe sich deren Urheberschaft kaum eindeutig nachweisen. Der Cyberwar bzw. die Vorbereitung hierauf setze voraus und beinhalte, dass mit viel Geld Sicherheitslücken aufrechterhalten und gehandelt werden. Die hierfür notwendigen Fähigkeiten müssten entwickelt werden und prägten bereits teilweise das Fach Informatik. Demgegenüber warb Kreowski für das Konzept des „Cyberpeace“. Voraussetzung hierfür wäre, dass die Fähigkeiten und Ressourcen, die aktuell in die Vorbereitung des Cyberkriegs fließen, für die Beseitigung von Sicherheitslücken aufgebracht würden. Das würde sowohl Gesellschaften und kritische Infrastrukturen wie auch private Anwender*innen vor militärischen, staatlichen und kriminellen Angriffen schützen.

… UND MILITÄRISCHE LANDSCHAFTEN.

Hieran anschließend stellte Christoph Marischka v.a. anhand historischer Beispiele und mit einem räumlichen Ansatz die Kommunikationsinfrastruktur von Bundeswehr und NATO vor. Dabei zeige sich, dass diese bereits in der Vergangenheit einen hybriden Charakter aufgewiesen habe, indem sie öffentliche Infrastruktur, wie Kabel und Richtfunkstrecken der Bundespost genutzt und durch zusätzliche eigene Richtfunkstrecken ergänzt habe.

Andreas Seifert stellte sich daraufhin der Frage: „Wer verdient eigentlich am Cyberkrieg?“ und fokussierte dabei auf eher kleinere und unbekannte Firmen. Hierzu stellte er zunächst den Branchenverband AFCEA vor. Viele der beteiligten Unternehmen befänden sich neben dem Großraum München in Köln und Bonn. AFCEA veranstalte pro Jahr 20 bis 30 Messen, Konferenzen und Fachforen, an denen sich Menschen aus dem Militär, der Politik, der Forschung und der Wirtschaft beteiligen. Bei einer drastischen Erhöhung des Rüstungsetats sei v.a. auch davon auszugehen, dass viel Geld in die Ausbildung und zusätzliches Personal fließen dürfte. Dies bedeute angesichts der Suche nach neuen Formen der Rekrutierung und des an-



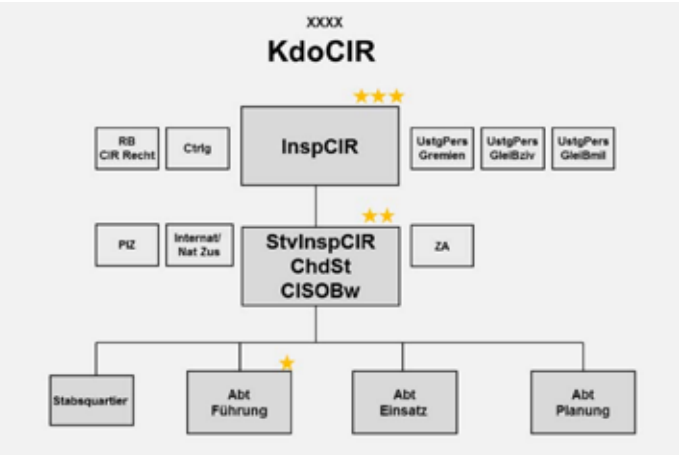
Startaufstellung des Organisationsbereichs Cyber- und Informationsraum entsprechend...

gestrebten „atmenden Personalkörpers“ eben auch die engere Zusammenarbeit mit teilweise kleinen Unternehmen, die besser – und verstärkt auch personell – einbezogen werden sollten.

Spontan wurde das letzte Panel durch einen Beitrag von Emanuel Matondo erweitert, der die Folgen des Exports von Überwachungstechnologie aus Deutschland nach Angola sehr persönlich veranschaulichte. So werde in Angola davon ausgegangen, dass Siemens / Nokia Networks und Rohde & Schwarz aus München führend am Ausbau des dortigen Überwachungsapparates beteiligt seien. Die Menschen in Angola wären spürbar eingeschüchtert, gingen seither bei Telefonaten davon aus, abgehört zu werden, und fühlten sich auch bei ihren Aktivitäten in sozialen Netzen eingeschränkt.

WIDERSTAND UND GEGENÖFFENTLICHKEITEN

Zum Abschlusspodium „Widerstand im Zeitalter von Cyberwar und Strategischer Kommunikation“ waren Personen geladen, die im weiteren Sinne als Medienschaffende zu bezeichnen wären. Anna Hunger, von der Wochenzeitung „Kontext“, beschrieb die eher klassische journalistische Arbeit in einer Redaktion, die allerdings klein ist und somit den engen persönlichen Austausch innerhalb der Redaktion ermögliche. Judith Lauterbach vom freien Radio Wüste Welle sah den Unterschied zu herkömmlichen Medien darin, dass in den Sendungen des freien Radios unmittelbar betroffene und aktive Menschen zu Wort kämen. Dadurch sei die Berichterstattung vielleicht einseitig bzw. parteiisch, aber auch authentisch und glaubwürdig. Tobias Pflüger als IMI-Vorstandsmitglied, Aktivist und Bundestagsabgeordneter bezeichnete gründliche Recherche als Voraussetzung politischer Arbeit, die eben häufig in der Aufbereitung von Informationen bestehe. Am Beispiel der verbotenen Internetportals „Linksunten“ wies er darauf hin, wie staatliche Repressoin auf den öffentlichen Diskurs einwirke. Dass man auch kreativ mit Informationen umgehen kann, zeigte anschließend ein Aktivist auf, der über Adbusting sprach. Dabei werden Werbeplakate manipuliert, um deren ursprüngliche Nachricht umzukehren oder zu pervertieren. Die Bundeswehr sei hierfür ein sehr dankbarer Kooperationspartner, sobald sie an die Öffentlichkeit gehe. Als Quelle seien die Aktivist*innen auf alternative Medien angewiesen und das Adbusting könne diese auch nicht ersetzen, da es auf sehr kurze, plakative Aussagen angewiesen wäre, die nicht als Grundlage für politisches Handeln ausreichten.



...dem Abschlussbericht des Aufbaustabes vom April 2016.

ÜBERRASCHENDE GEMEINSAMKEITEN

Natürlich konnte auch die Abschlussdiskussion keine endgültige Klärung dahingehend bringen, wie Widerstand in Zeiten des Informationskriegs zu gestalten sei, jedoch gelang es, das gegenseitige Verständnis von Medienschaffenden und Aktivist*innen zu erhellen. Auch was das Thema „Krieg im Informationsraum“ anging, wurde während des gesamten Kongresses mehrfach betont, dass die IMI nur erste Ansätze zu dessen Verständnis sammeln wollte und konnte. Trotzdem zeigten sich unabgesprochene und überraschende Parallelen zwischen den einzelnen Zugängen, von denen einige hier abschließend genannt werden sollen:

1. Dass Gegner, denen Propaganda bzw. Informationskrieg vorgeworfen wird, identifiziert werden, setzt die Annahme einer eigenen moralischen Überlegenheit und Wahrheitstreue voraus, die inhaltlich kaum unterfüttert, sondern eben durch den Verweis auf die Manipulation durch den Gegner ersetzt wird.

2. Obwohl sich die aktuell mit dem Begriff des Informationsraums vollzogene Fusionierung von Cyberkrieg und Propaganda bereits länger vollzieht, werden die Aktivitäten des IS und Russlands derzeit als wesentliche Legitimationsfigur verwendet. Westliche und internationale zivilgesellschaftliche Akteure und ihre Argumente werden in frappierender Klarheit als deren Komplizen und Werkzeuge dargestellt und als Feinde im Informationsraum identifiziert.

3. Argumente gegen die eigene Regierung, die EU oder die Nato werden als bezahlte und gesteuerte Propaganda der Gegner disqualifiziert und in keiner Weise inhaltlich adressiert.

4. Die Strategische Kommunikation (Propaganda) von EU und NATO wird eher als „Rauschen“ wahrnehmbar, das Akteure kontinuierlich positiv oder negativ konnotiert und von Ereignissen größerer Relevanz ablenkt.

5. Beim „Cyber- und Informationsraum“ handelt es sich um eine hybride Infrastruktur, die bereits seit ihrem Entstehen von einem Wechselspiel staatlicher, privatwirtschaftlicher und zivilgesellschaftlicher Akteure geprägt ist. Der Krieg im Informationsraum politisiert diese Akteure im Sinne Carl Schmitts: Wer nicht für uns ist, ist gegen uns und wir (egal wer) sind die Guten.

2007: DIE VORWEGNAHME DES POSTFAKTISCHEN UND DER STRATEGISCHEN KOMMUNIKATION DURCH DIE NATO

ODER: DEN STATUS QUO VERTEIDIGEN

AUSZÜGE MIT EINEM KOMMENTAR VON SVEN WACHOWIAK

Oft wird behauptet oder impliziert, das Thema der strategischen Kommunikation habe eigentlich erst im Zuge der Ukrainekrise Eingang in die Überlegungen westlicher Sicherheitspolitiker gefunden. Dass dies nicht zutrifft, zeigt das bereits 2007 vorgestellte NATO-Strategiepapier „Towards a Grand Strategy for an Uncertain World“ (Hin zu einer Gesamt- und Leitstrategie für eine Welt der Ungewissheit), dessen Untertitel „Die Erneuerung der transatlantischen Partnerschaft“ proklamiert.

Die Liste der fünf Urheber des Dokuments liest sich wie ein ‚Who‘s who‘ der transatlantischen Militär-Zusammenarbeit. Sie alle haben in den Neunziger Jahren auf höchster Ebene in ihren jeweiligen nationalen Streitkräften gedient. Deutsche Leser dürften Klaus Naumann kennen, ehemaliger Generalinspekteur der Bundeswehr, der diese unter Verteidigungsminister Volker Rühe zur Interventionsarmee umbaute und anschließend bis zu seiner Pensionierung 1999 als Nato-Oberbefehlshaber diente. Hervorzuheben ist auch John M. Shalikashvili, ehemaliger Generalstabschef der US-Streitkräfte, dessen Strategiepapier „Joint Vision 2010“ die Hinwendung der US-Streitkräfte zur vernetzten Operationsführung einleitete. Des Weiteren zeichnen verantwortlich der ehemalige britische Stabschef Peter Inge, sowie seine Pendants aus Frankreich und den Niederlanden, Jacques Lanxade und Henk van den Breemen.

Das vorgestellte Kapitel aus dem ersten Abschnitt des Papiers trägt den Titel „Verlust des Rationalen“ (Loss of the Rational), der sich auch in anderer Weise als beabsichtigt als programmatisch erweist: So oszilliert die Argumentation der Autoren zwischen luzider Diagnostik und dramatischer Realitätsverkehrung. Gestützt auf die unreflektierte spät-hegelianische Gewissheit, derzufolge der vorgefundene Status Quo notwendigerweise Ausdruck des absolut Rationalen sein müsse, wird alles von dieser Maßgabe abweichende als „irrational“ deklariert und in einen Topf geworfen.

AUS DEM STRATEGIEDOKUMENT „TOWARDS A GRAND STRATEGY FOR AN UNCERTAIN WORLD“: DAS KAPITEL ZUM „VERLUST DES RATIONALEN“

Der Trend zur Regionalisierung, teils aktiv voran getrieben – besonders im Fall der Europäischen Union – hat nicht bloß zu einem Niedergang des Nationalstaats geführt. Er hat mitunter auch dazu geführt, dass sowohl nationale Identität, wie auch die Achtung vor Rechtsstaatlichkeit, Sprache und dem Wert des Staatsbürgertums geschwächt wurden. Mit der Schwächung nationaler Identitäten und dem Bedeutungsverlust des Staatsbürgertums rücken andere Quellen kollektiver Identität – wie die religiöse – in den Vordergrund. Religiosität oder religiöse Orthodoxie sind an und für sich unproblematisch und bilden oftmals einen wichtigen Bestandteil gesunden Staatsbürgertums. Problematisch hingegen ist jener Schwund des Rationalen, der wachsende Verunsicherung nach sich zieht und es dem politischen Fanatismus – gegenwärtig radikalem Islamismus – ermöglicht, sich ungehindert auszubreiten. Daraus erwachsen zweierlei Konsequenzen: Es handelt sich in erster Linie um ein kulturelles und soziales Problem, das sich auf Bewusstsein, Staatsbürgertum und Sicherheit auswirkt. Mündet aber gesellschaftliche Irrationalität in politischer Irrationalität, so bestimmen Kurzsichtigkeit und Strategielosigkeit das politische Handeln, welches dann von feindlich gesinnten Akteuren manipuliert werden kann.

Der Verlust des Rationalen in den westlichen Gesellschaften kann als Teil eines umfassenderen kulturellen Trends gesehen werden, der solche Gesellschaften verwundbarer macht. Er äußert sich in einer Vielzahl von Symptomen, welche vom Harmlosen bis zum Fanatischen reichen. Der auf Popkünstler und Athleten gerichtete Persönlichkeitskult ist ein vergleichsweise unschuldiges Symptom dieses weiter ausgreifenden kulturellen Phänomens. In einigen westlichen Gesellschaften hat das Vertrauen in gänzlich irrationale Glaubenssysteme mittlerweile den Glauben an Religionen mit moralischer und rationaler Substanz und kulturellen Wurzeln überflügelt. Symptome wie das rückläufige Interesse an Wissenschaft sind Ausdruck eines intellektuellen Niedergangs, dessen gesellschaftliche Folgen etwa im Journalismus, im Rechtswesen, selbst im Gesundheitswesen noch unmittelbarer zu spüren sind. Dies steht in Zusammenhang mit einem umfassenderen Verlust des Respekts vor dem Wert von Beweisen und Argumenten. Die Globalisierung der Informationsströme hat zur direkten Auswirkung, dass alle möglichen Formen von irrationalen Vorstellungen oder politischem Fanatismus frei zugänglich im Umlauf sind. Grundzüge der offenen Gesellschaft, wie die Redefreiheit, können infolge dessen gegen sich selbst und andere Freiheiten verwendet werden.

Im Zusammenwirken tragen diese Symptome zur politischen Leichtfertigkeit großer Teile der Bevölkerung in der entwickelten Welt bei und machen die Menschen intellektuell, kulturell und politisch verwundbar. Verlorener Wert des Staatsbürgertums und zunehmende Irrationalität

schaffen den Raum, wo öffentliche Meinung emotional geformt wird, wodurch solide Strategie und Politik schwerer durchführbar sind. Hier entsteht zudem ein fruchtbarer Nährboden für Demagogie. Der Verlust des Rationalen ist, anders ausgedrückt, der Verlust eines besonders wertvollen Teils intellektueller und moralischer Gewissheit und kann Menschen dazu veranlassen, sich die Gewissheit anderswo zu suchen, sei es in den herkömmlichen Kults, sei es in extremen Formen des Fanatismus.

Vertrauen in das eigene rationale Vermögen beinhaltet das Hinterfragen und das Aushalten von Zweifeln. Die Angst vor dem Zweifel ist bisweilen stärker als die Angst vor dem Tod, wenn extremer Zweifel empfänglich macht für die extreme Gewissheit gewaltbereiter Ideologien, von denen die attraktivste (jedoch keineswegs einzige) gegenwärtig der radikale Islamismus ist.

Die Anziehungskraft des radikalen Islamismus lässt sich mit dem psychologischen Appeal anderer, säkularer totalitärer Ideologien des 20. Jahrhunderts insofern vergleichen, als dass jedweder Zweifel beiseite geräumt wird. In den totalitären Regimes des 20. Jahrhunderts nahm Ideologie oftmals den Platz von Religion ein und ersetzte mitunter das Göttliche durch den Tyrannen selbst – eine bizarre Idolatrie, die sich heute noch im Persönlichkeitskult Nordkoreas beobachten lässt. [...]

AUSZUG AUS DEM UNTERKAPITEL „INFORMATIONSOPERATIONEN“:

Da aber die Welt durch nahezu unmittelbare Kommunikation miteinander verbunden ist, erscheint jedes Ereignis unverzüglich zuhause auf den Fernsehbildschirmen, manches Mal schneller als die Befehlswege zu reagieren im Stande sind. Darüber hinaus ist es in vielen Fällen der Feind, der die Information auf den Weg bringt, um den Zusammenhalt der Allianz sowie die Unterstützung für laufende Operationen zu schwächen. Um diese beunruhigende Gemengelage in der Beziehung zur Öffentlichkeit zu bewältigen, gilt es für die NATO, dringend eine Informationsstrategie zu entwickeln, die es ihr selbst und ihren Mitgliedsstaaten ermöglicht, das Steuer wieder in die Hand zu nehmen; andernfalls riskiert sie die Niederlage an der Heimatfront, selbst wenn ihre Streitkräfte auf taktischer oder operationeller Ebene gewinnen.

Daher muss die NATO eine Informationsstrategie entwickeln, die es vermag, drei Zielen gleichzeitig zu dienen:

- **Sie muss die Wahrnehmung der Weltöffentlichkeit dahingehend beeinflussen, dass es sich bei der NATO um eine Macht des Guten handelt.**

- **Zweitens, sie muss auf den Bildschirmen präsent sein, noch bevor es dem Gegner gelingt, die Nachrichten zu verbreiten, d.h. die NATO muss die Informationshoheit im Öffentlichkeitsbereich gewinnen und behalten.**

- **Sie muss drittens helfen, die Herzen und Köpfe sowohl ihrer eigenen Nationen (für das gerechte Vorgehen der NATO), als auch der Menschen in den Einsatzgebieten zu gewinnen.**

Was dem alten Hegel der preußische Staat, das ist den alten Militärs – wenn man ihnen zwar auch ein ‚geistiges Junkertum‘ bescheinigen kann – die bürgerlich-liberale Gesellschaftsform und ihre hegemoniale Stellung in der nach 1990 konsolidierten monopolaren Weltordnung, ein Zustand, der ihnen ganz im Geiste Fukuyamas als ‚Ende der Geschichte‘ und Höhepunkt der Weltvernunft erscheint. Dieses Denksystem, man sieht es, lässt Alternativen nicht zu. Es gibt keine ‚Ratio‘ neben der des Status Quo: Kapitalismus oder Barbarei.

Aber auch die alten Generäle haben mitbekommen, dass die Zeit im Jahr 1990 nicht stehen geblieben ist. Eben darum sollte ihre Gesamt- und Leitstrategie das seinerzeit geltende, für nicht mehr zeitgemäß befundene Strategiekonzept aus dem Jahr 1999 ablösen. Unter einem in den Zeilen mitschwingenden zeitgenössischen Sentiment von Interregnum und Systemdämmerung scheint die Rolle hervor, die man der eigenen Organisation in dieser veränderten Weltlage zudenkt und deuten sich die Konsequenzen an, die man für nötig hält, um ein ‚Abgleiten in die Barbarei‘ zu verhindern. Worin diese – allein im Inneren – letztendlich bestehen könnten, ließ sich zwei Jahre nach Erscheinen des Strategiepapiers bei einem anderen, zivilen ‚Strategen‘ nachlesen, nämlich dem in deutschen Talkshows und Regierungskreisen äußerst wohlgelittenen Berliner Professor und Deutsch-Europa-Ideologen Herfried Münkler: „Die Demokratie wirkt wie eine betuliche alte Tante, die zwar alles weiß, aber vieles nicht mehr hinbekommt. Es gibt jedoch einen jungen und kraftvollen Neffen, der zur Hilfe bereit ist, aber mitunter diktatorische Neigungen hat. Soll man ihn der Tante zur Seite stellen? Ist es besser, ihn fernzuhalten und dieser stattdessen ein umfassendes Revitalisierungsprogramm zu verschreiben, das ihre Entschlusskraft und Handlungsfähigkeit stärkt? Oder ist ihre Zeit abgelaufen, und es will bloß keiner wahr haben, weil sie so nett und freundlich gewesen ist?” Starker Neffe gesucht!, lautete also die Annonce. An Anwärtern auf die Stelle mangelt es nicht. Es folgen, in deutscher Übersetzung, einige aussagekräftige Passagen aus dem Bewerbungsschreiben, das die Herren Naumann, Shalikashvili und Konsorten bereits zwei Jahre zuvor vorsorglich aufgesetzt hatten.

VON DER HEIMATFRONT BIS INS SCHLACHTFELD: DIE NATO IM INFOKRIEG

VON JÜRGEN WAGNER

„Informationen selbst sind zum Angriffsziel und Mittel geworden; der Informationswettbewerb und der Kampf um die Deutungshoheit sind ein entscheidender Faktor in der modernen Kriegsführung geworden.“[1]

Der „Krieg um die Informationshoheit“ nimmt innerhalb der NATO immer weiter an Bedeutung zu. Unter Stichworten wie „Hybride Kriegsführung“ und „Strategische Kommunikation“ (StratKom) wird er aktuell auf unterschiedlichsten Ebenen ausgefochten: An der Heimatfront gilt es, feindlicher – sprich: meist russischer – Propaganda mit Gegeninformationen – sprich: Propaganda – entgegenzuwirken und um Zustimmung für die eigene Militär- und Machtpolitik zu werben. Außerhalb des heimischen Territoriums reichen die Überlegungen bereits so weit, dass im deutschen Heer konkrete Szenarien für einen NATO-Krieg mit Russland durchgespielt werden, in denen dem Kampf um den Informationsraum eine zentrale Rolle eingeräumt wird. Dies wirft automatisch die Frage auf, ob es sich hier um Entwicklungen von grundlegend neuer Qualität handelt – schließlich sind Propaganda, Spionage und Krieg schon immer eng miteinander verwoben gewesen –, die abschließend adressiert werden soll.

1. DIE „ÄRA HYBRIDER EINFLUSSNAHME“

Mit „hybrider Kriegsführung“ wird gemeinhin eine neue Form der offensiven Durchsetzung von Interessen verstanden, bei der ein ganzes Bündel an Instrumenten neben oder sogar unabhängig von der „klassischen“ Kriegsführung zum Einsatz gebracht wird. Eine recht bündige Definition, die zudem auch noch die wesentliche Rolle von Informationen in diesem Zusammenhang herausstreicht, findet sich im „EU Playbook“ zur Abwehr hybrider Bedrohungen: „Hybride Bedrohungen können als ein Mix aus Zwangs- und Subversionsaktivitäten mit konventionellen und unkonventionellen Mitteln (zB diplomatisch, militärisch, wirtschaftlich, technologisch, informationstechnisch) charakterisiert werden. Sie können koordiniert von staatlichen oder nicht-staatlichen Akteuren angewendet werden, um bestimmte Ziele zu erreichen, ohne die Schwelle offener organisierter Gewaltanwendung zu überschreiten […]. Massive Desinformationskampagnen unter Verwendung sozialer Medien zur Kontrolle politischer Narrative oder zur Radikalisierung, Rekrutierung und Steuerung von Stellvertretern können Vehikel hybrider Bedrohungen sein.“[2]

Obwohl er schon länger durch die Gegend geistert, ist der Begriff im NATO-Kontext erst in jüngster Zeit so richtig in Mode gekommen: „Während die hybride Bedrohungslage in der sozialwissenschaftlichen Literatur bereits seit Anfang der 2000er Jahre thematisiert wird, findet der Begriff seitens der NATO erst Ende der 2010er Jahre zunehmend offiziell Verwendung und hält Einzug in die militärischen Strukturen des Bündnisses sowie in die ihm zugehörigen Forschungseinrichtungen und Denkfabriken. […] Die Eskalation im westlich-russischen Verhältnis im Zuge des Konflikts in der Ukraine sowie das Erstarken des so genannten Islamischen Staats (IS) im Irak und Syrien bilden zentrale Ereignisse, in deren Folge das Konzept der Hybridität und die ihm zugesprochene Bedeutung massiv an Gewicht gewinnen: Russlands Agieren im Rahmen des gesamten Konflikts wird als prototypisch für hybride Kriegsführung bewertet und die damit einhergehende Erschütterung des wahrgenommenen geopolitischen Gleichgewichts sorgt für eine zusätzliche Beförderung des Diskurses.“[3]

Um nur ein Beispiel zu nennen, dass der Westen sich tatsächlich in einem regelrechten Informationskrieg mit Russland wähnt, sei ein weiteres Arbeitspapier der „Bundesakademie für Sicherheitspolitik“ zitiert: „Wir sollten uns nicht der Illusion hingeben bzw. den Eindruck aufkommen lassen, dass der derzeitige Konflikt mit Russland von vorübergehender Dauer sei und wir in absehbarer Zeit wieder zur Normalität zurückkehren könnten. […] In seinem Krieg gegen den Westen greift Russland auf verschiedene Instrumente zurück. Eine Reihe staatlich kontrollierter Medien (im In- und Ausland) werden zu Propagandazwecken genutzt – mit dem Ziel, das Vertrauen westlicher Gesellschaften in die eigenen Institutionen und politischen Eliten zu untergraben. […] Moskau greift zunehmend auf Mittel der virtuellen Kriegführung zurück, sowohl direkt (durch seine eigenen Geheimdienste) als auch indirekt (durch Unterstützung von Hacker-Netzwerken). […] In der Konfrontation mit dem Westen bedient sich Russland jener Methoden, die in der Vergangenheit vornehmlich gegen ehemalige Sowjetstaaten (‚Nahes Ausland‘) oder nicht-westliche Staaten verwendet wurden. Dies trifft insbesondere auf mit massiver Propaganda kombinierte, aggressive Cyberangriffe zu, die auf Einmischung in interne Angelegenheiten und eine Beeinflussung politischer Prozesse abzielen (wie der Fall Lisa in Deutschland oder die Anti-Macron-Kampagne in Frankreich).“[4]

Hier wird allerdings so getan, als hätte Russland (und der IS) die Hybride Kriegsführung in die Welt gesetzt, wodurch die NATO gezwungen sei, Gegenmaßnahmen zu ergreifen. Diese Sichtweise hat allerdings den Schönheitsfehler, dass sich gerade NATO-Staaten schon lange „hy-

brider“ Mittel bedienen, um in verschiedensten Ländern missliebige Machthaber zu stürzen. Erst seitdem „feindliche“ Akteure zunehmend ebenfalls in diesem Feld aktiv werden, erblickt die NATO ein Problem. Sichtbarster Ausdruck für die wachsende Bedeutung, die in diesem Zusammenhang auch speziell dem Informationsraum zugesprochen wird, war schließlich 2014 die Gründung eines „NATO-Kompetenzzentrums für Strategische Kommunikation“ in Riga. Bei diesen mittlerweile 24 Kompetenzzentren handelt es sich um die „Speerspitzen“ zur Weiterentwicklung der NATO-Kriegsführung. Noch recht jung ist das neueste Kompetenzzentrum „Abwehr Hybrider Bedrohungen“, das im September 2017 in Finnland seine Arbeit aufnahm. Das Zentrum selbst spricht auf seiner Homepage pathetisch davon, man befinde sich in der „Ära hybrider Einflussnahme“[5], während die Deutsche Welle als Grund für die Aufstellung der Institution folgendes schreibt: „Die EU und die NATO haben sich verbündet, um in Nordeuropa gegen hybride Bedrohungen zu kämpfen. Denn nicht nur Panzer, sondern auch Tweets können heutzutage zum Kriegsgerät werden.“[6]

2. NATO-PROPAGANDAÜBUNGEN

Schon länger ist es ein wesentliches Anliegen der NATO-Staaten, an der Heimatfront um Zustimmung für ihre Militärpolitik zu werben. Allerdings werden die Bemühungen in diesem Bereich in jüngster Zeit erheblich intensiviert. Ein Beispiel hierfür ist die im Mai 2017 veröffentlichte Studie „Mitigating Disinformation Campaigns Against Air Power”. Sie wurde vom in Deutschland beheimateten Luftwaffen-Kompetenzzentrum der NATO (Joint Air Power Competence Centre - JAPCC) angefertigt und beschäftigt sich mit der Frage, wie die öffentliche Meinung über die Luftwaffe „positiv“ beeinflusst werden kann.

Die Studie identifiziert drei „problematische“ Akteursgruppen: Zu Russland heißt es: „Russland ist besorgt über den Machtvorsprung der NATO in der Luft und macht die NATO-Luftstreitkräfte deshalb zum Ziel von Falschinformationen.“ Auch IS-ähnliche Gruppen werden als Problem für das Ansehen der Luftwaffen erachtet, sie würden relativ erfolgreich zwei Kernbotschaften transportieren: „1. NATO-Luftschläge töten wahllos und nehmen besonders Zivilisten ins Visier. […] 2. Die Ausübung von Luftschlägen ist illegal und verwendet illegale Mittel und Methoden.“ Und schließlich gäbe es im Westen kritische Gruppen, die eine geradezu verblendete Abneigung gegenüber der Allianz aufweisen würden: „Viele NGOs [Nichtregierungsorganisationen] haben einen starken, gegen die NATO gerichteten Bias, und tendieren dazu, jeglichen westlichen Einsatz von Gewalt oder militärische Operationen negativ darzustellen.“[7]

Als wesentliches Mittel, um das Aktionsfeld der NATO einzuengen, wird außerdem die „Lawfare-Bewegung“ identifiziert: Nichtregierungsorganisationen wird „unterstellt, dass der Rechtsweg bloß instrumentalisiert und ausgenutzt werde, um der NATO zu schaden: ‚Dieser Ansatz nutzt ein zentrales Element der Demokratie aus, die Achtung des Gesetzes. […] Unter Verweis auf zivile Opfer drängt die Lawfare-Bewegung nicht nur darauf, Munition zu verbieten, die für künftige Konflikte wichtig ist, sondern sie will auch die Regel durchsetzen, dass jeder tote Zivilist und jeder zivile Kollateralschaden ein Kriegsverbrechen darstellt.‘“[8] Und genau diese Lawfare Bewegung würde dann wiederum vom aktuellen Hauptfeind Nummer eins gefördert: „Russland ist ein großer Unterstützer der Lawfare-Bewegung.“[9]

Um dem entgegenzuwirken, spricht die Studie einige Empfehlungen aus. Im Kern geht es aber relativ simpel darum, offensiv die eigene Interpretation in den öffentlichen Raum zu tragen: „Die NATO muss sich aggressiv der Lawfare-Bewegung entgegenstellen“, heißt es in der Studie, wobei sie folgende Kernbotschaft verbreiten müsse: „Die NATO bekämpft wirklich böse Menschen, die die Menschenrechte verletzen.“[10]

Es ist an dieser Stelle überhaupt nicht nötig, sich im Detail mit den teils recht wilden Aussagen dieser Studie auseinanderzusetzen. Vielmehr ist es wichtig, das Muster zu begreifen, das hier – und anderswo – zur Anwendung kommt: „Mit der hier wiedergegebenen Argumentation wird jegliche Kritik an der NATO als illegitim diskreditiert, weil sie entweder aufgrund eines anti-NATO Bias, mangelnder Expertise oder wegen des Einflusses von Falschinformationen und Propaganda erfolge. […] So wird einer Kritik an der NATO von vornherein jede Berechtigung abgesprochen, bzw. Argumentationsmuster geboten, um diese zu diskreditieren.“[11]

In etwa dasselbe Muster weist auch die gemeinsame NATO/EU-Übung PACE 2017 auf, die im Herbst 2017 stattfand. Die Bundesregierung antwortete auf eine Kleine Anfrage der Linksfraktion zum konkreten Inhalt des Szenarios reichlich schwammig: „In dem Szenario der EU PACE 17 unterliegen eine erhebliche Anzahl von EU-Mitgliedstaaten Cyber-Angriffen unterschiedlicher Natur und Intensität. Gleichzeitig kommt es zu erhöhtem und gesteuertem Falschmeldungsaufkommen. […] Welche

konkreten Reaktionen beübt werden, wird sich aus dem dynamisch angelegten Übungsverlauf ergeben."[12]

Auch hier spielen holzschnittartig dieselben drei antiwestlichen Akteure wie bei der zuvor beschriebenen JAPCC-Studie die entscheidende Rolle. Einmal Russland, für das allerdings ein anderer Name gewählt wurde: „Froterre ist ein quasi-demokratischer Staat […], der nach größerem geopolitischem Einfluss strebt, dessen wirtschaftlichen Interessen und Werte aber im Konflikt mit denen der EU und der westlichen Welt stehen." Daneben spiele auch ein – augenscheinlich dem IS ähnelnder – „Newborn Extremist State" (NEXTA) eine Rolle. Dabei handele es sich um eine „global agierende terroristische Gruppe, […] die vor allem auf Propaganda setzt."[13]

Und schließlich sei da noch die Anti-Globalisierungsgruppe (AGG), die Front gegen den Westen mache und – natürlich – von Russland bzw. Froterre unterstützt werde: „Die AGG ist eine internationale Bewegung, die sich gegen die politische Globalisierung wendet. Die AGG verwendet regelmäßig soziale Medien, um Propaganda zu verbreiten und Riots im Gewand von Demonstrationen vorzubereiten. [Die AGG] kritisiert die wachsende militärische Präsenz von EU-Staaten im Mittelmeer. Laut Geheimdienstinformationen erhält die AGG finanzielle Unterstützung von verschiedenen Ländern, die der EU feindlich gesinnt sind, besonders von Froterre." (Ebd.)

Leider sind darüber hinaus wenig Details über dieses Planspiel bekannt. Aber auch hier findet sich dasselbe Muster wieder: Jegliche kritische Position wird als von Russland gesteuert bzw. unterwandert diskreditiert und damit auch eine Legitimationsbasis für Gegenmaßnahmen an der Heimatfront postuliert.

3. 2026: (Informations-)Krieg NATO vs. Russland

Auf besonders beängstigende Weise wird aktuell der „klassische" Landkrieg und der Krieg um den Informationsraum mit Blick auf Russland miteinander verschmolzen. Dass sich die Bundeswehr buchstäblich für einen Landkrieg gegen Russland rüstet, wurde spätestens durch die „Vorläufigen konzeptionellen Vorgaben für das künftige Fähigkeitsprofil der Bundeswehr" bekannt. Dabei handelt es sich um eine Vorarbeit für die künftige „Konzeption der Bundeswehr", die unter Leitung des Chefs der Abteilung Planung im Verteidigungsministerium erstellt wurde und deshalb auch als Bühler-Papier bezeichnet wird.

Das im März 2017 unterzeichnete Dokument ist zwar nicht-öffentlich, wurde allerdings ausführlich in zwei Ausgaben der „Frankfurter Allgemeinen Zeitung" (FAZ) behandelt. Demzufolge solle die Interventionsfähigkeit im Ausland aufrechterhalten werden, aber „die zunehmende Konfrontation mit Russland" erfordere es, künftig zusätzlich drei schwere Divisionen in die NATO einbringen und ins Gefecht führen zu können: „Bis 2026 soll eine erste Division die volle Einsatzfähigkeit erreicht haben. Das würde bedeuten, dass knapp 20 000 Soldaten in drei gepanzerten Brigaden inklusive Divisions- und Brigadetruppen in den Kampf geschickt werden können. Dazu ist die Bundeswehr derzeit nicht in der Lage. […] Ende 2031 sollen auch die beiden anderen Divisionen voll ausgestattet und nach einer Vorlaufzeit von etwa drei Monaten einsatzbereit sein. […] Damit würden die Divisionen wieder die klassische Struktur aus der Zeit vor 1990 einnehmen."[14]

Angesichts des im Bühler-Papier genannten Datums, 2026 die erste schwere Division für einen Krieg gegen

Russland in die NATO einspeisen zu wollen, werden die Inhalte des genau für diesen Zeitpunkt planenden Thesenpapiers „Wie kämpfen die Landstreitkräfte künftig?“ umso gruseliger. Herausgegeben wurde es vom Kommando Heer und verfasst von einem Team unter Leitung von Generalleutnant Frank Leidenberger. Erschienen ist das Thesenpapier, in dem detailliert ein Landkrieg gegen Russland unter den „Rahmenbedingungen des Informationszeitalters“ durchgespielt wird, bereits im Sommer, im Internet zugänglich ist es aber erst seit Ende September 2017.[15]

In dem Dokument geht es darum, ein „Zielbild Landstreitkräfte (LaSK) 2026“ auszuarbeiten, das sich prägend auf die künftige Struktur und Bewaffnung des Heeres auswirken soll: „Die in diesem Papier dargelegten Ideen und Anforderungen werden in einem Operationskonzept vertieft und dann konsequenterweise in neuen Strukturen münden. […] Das zukünftige Operationskonzept soll dabei die quantitativen und qualitativen Forderungen des Fähigkeitsprofils der Bundeswehr – abgeleitet aus den akzeptierten NATO Planungszielen und den nationalen Aufgaben – mit den hier dargestellten Ideen verknüpfen. Es wird so zum gedanklichen Kernelement der zukünftigen Entwicklung der Landstreitkräfte.“.

Der zunehmenden Bedeutung des Informationsraums – sowohl für die Auseinandersetzung auf dem Gefechtsfeld selbst wie auch an der Heimatfront – wird unter anderem folgendermaßen Rechnung getragen: „Jede Präsenz und Aktion von LaSK auf einem zukünftig ‚gläsernen‘ Gefechtsfeld oder Einsatzraum erzeugt reaktiv einen Effekt im Informationsraum, der ‚Kampf‘ um/mit Informationen muss zwingend – und schnell im Sinne einer ‚Golden Hour‘ – geführt werden. […] Das Gefechtsfeld wird transparenter und komplexer, sowohl im Sinne von verbesserten Aufklärungsfähigkeiten aller Seiten, als auch hinsichtlich der Verbreitung von Meldungen/Nachrichten/Gerüchten quasi weltweit, in alle gesellschaftlichen Bereiche und in die eigene Truppe hinein. Das Gefechtsfeld wird durch die Zusammentreffen von verbesserter Aufklärung, schnelleren Entscheidungs- und Bekämpfungszyklen aufgrund taktischer NetOpFü [vernetzter Operationsführung] und zielgenauerer und verbesserter Wirkmittel letaler, selbst für gut geschützte Kräfte. […] Taktische Cyber-Kräfte unterstützen offensiv und defensiv den Einsatz von Landstreitkräften und […] ermöglichen auch […] den Angriff auf gegnerische Systeme und die offensive Beeinflussung von Entwicklungen im Informationsraum.“

Beschrieben wird daraufhin, wie aus Sicht des Heeres ein künftiger (Informations-)Krieg gegen Russland ablaufen könnte. Es beginnt mit dem Aufmarsch der von Deutschland aufgebauten „Ultraschnellen Eingreiftruppe“ (VJTF), was aber nicht die erhoffte abschreckende Wirkung erzeugt: „Der Beschluss zur Aktivierung und Verlegung der VJTF (stand by), bestehend im Kern aus dem DEU Einsatzdispositiv (EDP), wurde aufgrund einer überraschenden Lageentwicklung notwendig. […] Dennoch kommt es nach einer Phase von Desinformation, separatistischen Aktivitäten, lokalen Angriffen von Separatisten und verdeckt operierenden Special Operation Forces zum Angriff der gegnerischen Hauptkräfte.“

Als Reaktion auf diesen russischen Angriff startet die NATO daraufhin ihrerseits eine Offensive – auf dem Gefechtsfeld stellt sich das dann wie folgt dar: „Zur Vorbereitung des Gegenangriffs befiehlt der BrigKdr das Auslösen des langfristig vorbereiteten Lähmens des gegnerischen FüInfoSys [Führungsinformationssystems], um den gegnerischen Entscheidungsprozess zu verlangsamen. Parallel werden in offenen Quellen (soziale Netzwerke, Messenger Services, Nachrichtenkommentare etc.), eine Vielzahl von Meldungen platziert, die auf ein Ausweichen der NATO-Kräfte hindeuten und so die eigene Absicht verschleiern helfen.“

Doch, wie bereits mehrfach erwähnt, soll der (Informations-)Krieg nicht allein auf dem Kriegsschauplatz, sondern auch an der Heimatfront ausgefochten werden: „Nachdem sich der Erfolg des Gegenangriffs abzeichnet, befiehlt der BrigKdr [Brigardekommandierende] eine offensive und mehrsprachige Informationskampagne, die durch Bilder, Text, Videos etc. die Erfolge der NATO-Truppen herausstreicht und zeigt, dass Kollateralschäden vermieden werden, aber auch eigene Verluste nicht verschweigt. Zeitgleich werden ausgesuchte Angehörige des Gegners und deren Angehörige adressiert. Durch diese zeitnahe ehrliche und offene Berichterstattung wird gegnerischer Propaganda entgegengewirkt, die öffentliche Meinung sowohl in den NATO-Staaten als auch beim Gegner beeinflusst und die Informationshoheit umstritten oder gewonnen.“

Deutlicher ist wohl nach dem Ende der Blockkonfrontation noch nie ein Krieg mit Russland öffentlich einsehbar durchgespielt worden. Bemerkenswert daran ist, dass das Heereskommando der Veröffentlichung im Internet explizit zugestimmt hat, es also interessiert daran zu sein scheint, dass seine Kriegsthesen bekannt werden. Lange war dies nicht sonderlich erfolgreich, die Medien ließen das spektakuläre Thesenpapier links liegen. Erst nach einiger Zeit trugen die Bemühungen Früchte – und wohl genau in der vom Heeres-

kommando intendierten Art und Weise. Denn der Spiegel (Nr. 48/2017) nutzte das Thesenpapier schließlich als Aufhänger, um pflichtschuldig auf den angeblich immensen Rüstungsbedarf der Streitkräfte hinzuweisen: „Leidenberger räumt in seinem Papier selbst ein, dass die Truppe ‚erst in Jahren' so weit sein werde."[16]

4. INFOKRIEG: ZÄSUR ODER KONTINUITÄT?

Abschließend drängt sich noch die Frage auf, ob es sich hier nicht um einen alten Hut handelt – Propaganda, Täuschungen und dergleichen gibt es schließlich schon seit Ewigkeiten. In dieser Hinsicht dürfte die „Bundesakademie für Sicherheitspolitik" aber Recht haben, wenn sie mit Blick auf die aktuellen Entwicklungen von einer „Zäsur" spricht. Ein wesentlicher Grund dafür liegt darin, dass die NATO in einen permanenten Informationskrieg mit Russland eingetreten ist, der zeitlich wie räumlich weit vor der Schwelle „klassischer" Kriege ausgetragen wird: „Klassischerweise wird zwischen Friedens- und Kriegszeiten unterschieden – eine Grenze, die im Zeitalter des Informationskriegs zu verschwimmen droht. Doch bereits vor dem Ausbruch eines hochintensiven Konflikts stellt sich die Frage, wie dieser von einem gegnerischen Akteur im Cyber- und Informationsraum vorbereitet wird und welche Vorkehrungen dafür getroffen werden. […] Betrachtet man Kriege durch diese theoretische Brille, so beobachten wir, dass die Bevölkerung, oftmals auch nur Minderheiten oder einzelne Bevölkerungsteile, in die Informationskriege einbezogen und zum Ziel gemacht werden, indem sie einer kontinuierlichen Propaganda ausgesetzt ist. Dies geschieht lange bevor ein bewaffneter Konflikt ausbricht und Streitkräfte überhaupt involviert sind."[17]

Als zweiter prägender Faktor kommt hinzu, dass es die Digitalisierung ermöglicht, auf viel direktere Weise nicht nur im Gefechtsfeld, sondern insbesondere auch im Feindesland mit der Bevölkerung in Kontakt zu treten: „Vom Mittelalter bis heute werden Bevölkerungen und gegnerische Soldaten mittels psychologischer Kriegsführung und somit mittels Informationen beeinflusst. Die Möglichkeiten, die der psychologischen Kriegsführung mit der heutigen Technik gegeben sind, stellt in ihrer Subversion und in ihrer Dimension jedoch eine Zäsur dar. […] Neu ist beispielsweise die technologische Seite, das digitale Informationsumfeld, das Menschen miteinander in einem riesigen globalen Netzwerk verbindet und grenzenlosen Austausch so einfach gemacht hat, wie nie zuvor in der Geschichte der Menschheit. […] Im selben Maße wird auch die Exponierung der Bevölkerung gegenüber digitaler Propaganda, hate speech oder Verschwörungstheorien zunehmen."[18]

Und genau diese „Exponierung der Bevölkerung" will sich die BAKS schließlich drittens zunutze machen, um den Informationskrieg direkt im russischen Feindesland zu führen: „Wichtiger Bestandteil unserer Maßnahmen gegen Russland sollte das verstärkte Einbinden der russischen Zivilgesellschaft sein, sowohl in Russland selbst als auch im Ausland (unter anderem der russischen Diaspora), zum Beispiel durch die Förderung von unabhängigen Initiativen in den Medien, der politischen Debatte, des gesellschaftlichen Handelns etc. Obgleich sie keinen direkten Versuch darstellen, einen Regimewechsel in Russland herbeizuführen, könnten derartige Bestrebungen langfristig zur Entstehung alternativer politischer Eliten in Russland beitragen. Auch wenn dies aufgrund des rigorosen Vorgehens des Kremls gegen die politische Opposition, Zivilgesellschaft, Nichtregierungsorganisationen und unabhängigen Medien Russlands immer schwieriger wird, sollte deren Umsetzung mittels kreativer technologischer und rechtlicher Lösungen angestrebt werden, wie zum Beispiel Fördermittel, Netzwerkarbeit, Satellitenfernsehen, soziale Medien, Internetportale und das Umgehen von VPN-Sperren."[19]

ANMERKUNGEN

1 Carolin Busch und Nadine Düe: Informationskriege: Eine Herausforderung für die Bundeswehr, BAKS-Arbeitspapier Nr. 24/2017.
2 EU operational protocol for countering hybrid threats 'EU Playbook', (Staff Working Document (2016) 227, Brüssel, 7. Juli 2016.
3 Christopher Schwitanski: Hybride Bedrohungen: Analysekategorie oder Steigbügelhalter der Militarisierung?, IMI-Studie 2017/13.
4 Marek Menkiszak: Herausforderung Russland, BAKS-Arbeitspapier Nr. 27/2017.
5 The European Centre of for Countering Hybrid Threats: hybridcoe.fi.
6 Im Kampf gegen hybride Bedrohungen, Deutsche Welle, 3.10.2017.
7 James Sterling Corum u.a.: Mitigating Disinformation Campaigns against Airpower, The Joint Air Power Competence Centre, May 2017.
8 Christopher Schwitanski: Ein Beispiel für Nato-Kriegspropaganda. Die Studie zum Umgang mit Desinformationskampagnen gegenüber der Luftwaffe, (IMI-Analyse 2017/41).
9 Mitigating Disinformation Campaigns, JAPCC 2017.
10 Ebd.
11 Schwitanski: Ein Beispiel für Nato-Kriegspropaganda.
12 Bundestags-Drucksache 18/13503, 05.09.2017.
13 Exercise Instructions (EXINST) for the EU PACE17 Parallel and Coordinated Exercise with NATO CMX17, Brüssel, 14.7.2017. Das Papier findet sich bei statewatch.org.
14 Bis zu den Sternen, FAZ, 19.4.2017.
15 Thesenpapier: Wie kämpfen die Landstreitkräfte künftig? Das Papier erschien auf pivotarea.eu, 22.9.2017. Ale folgenden Zitate in diesem Kapitel entstammen, sofern nicht anders ausgewiesen, diesem Papier.
16 Wie sich Europa in Zukunft wieder selbst verteidigen kann, Der Spiegel 48/2017.
17 Busch und Düe 2017.
18 Ebd.
19 Menkiszak 2017.

EUROPA IM KOMMUNIKATIONSKRIEG

WAS VERSTEHT DAS EUROPÄISCHE PARLAMENT UNTER HYBRIDER KRIEGFÜHRUNG, STRATEGISCHER KOMMUNIKATION UND PROPAGANDA?

VON: CHRISTOPH MARISCHKA

Am 23. November 2016 verabschiedete das Europäische Parlament eine Entschließung mit dem Titel „Strategische Kommunikation der EU, um gegen sie gerichteter Propaganda von Dritten entgegenzuwirken." Im Kopf des Dokuments wird bereits klar, in was für einem ausgreifend und damit auch schwammigen Kontext hier Begriffe wie Informationskrieg, Propaganda und hybride Kriegführung eingeführt und verwendet werden. Die Bezugnahmen reichen von der NATO-Gipfelerklärung aus Wales über die EU-Sicherheitsstrategie und Regionalstrategien gegenüber Russland und dem Nahen Osten bis hin zur sog. „Digitalen Freiheitsstrategie in der Außenpolitik der EU". Da viele der aufgestellten Behauptungen so abwegig wie potentiell folgenreich sind, soll das Dokument im Folgenden mit vielen Zitaten zusammengefasst werden.

Einleitend stellt das Europäische Parlament u.a. fest, dass

„das Vordringen neuer Formen digitaler Medien hochwertigen Journalismus vor ernsthafte Herausforderungen stellt, was eine Abnahme des kritischen Denkens bei den Zielgruppen und somit deren stärkere Anfälligkeit für Desinformation und Manipulation zur Folge hat."

Außerdem stünden

> ***„die EU, ihre Mitgliedstaaten und ihre Bürger unter wachsendem systematischen Druck ..., den Informations-, Desinformations- und Fehlinformationskampagnen sowie der Propaganda von Staaten und nichtstaatlichen Akteuren wie transnationalen terroristischen und kriminellen Vereinigungen in ihrer Nachbarschaft entgegenzuwirken."***

Sodann folgen zwei Kapitel zu den Aktivitäten Russlands und des Islamischen Staates. Jenes zu Russland ist bereits mit der Kernforderung überschrieben:

> ***„Anerkennung und Enthüllung des russischen Desinformations- und Propagandakriegs."***

Darin wird u.a. behauptet,

> ***„dass der Kreml … die Konfrontation mit der EU verschärft und seine Propaganda verstärkt hat ... womit er darauf abzielt, in der europäischen Öffentlichkeit politische Unterstützung für russische Maßnahmen zu erhalten und die Kohärenz der Außenpolitik der EU zu schwächen."***

Das Kapitel zum Islamischen Staat ist überschrieben mit dem Titel:

> ***„Durchdringung und Bekämpfung des Informationskriegs sowie der Desinformations- und Radikalisierungsmethoden des IS/Da'esh"***

Diesem wird v.a. vorgeworfen, dass er

> ***„soziale Medien, insbesondere Twitter und Facebook, im großen Umfang einsetzt, um seine Ziele in den Bereichen Propaganda und Rekrutierung, die insbesondere auf junge Menschen ausgerichtet sind, zu verfolgen."***

Bemerkenswert ist dabei bereits, wie das Europäische Parlament dabei Russland und den Islamischen Staat auf eine Stufe stellt. Spektakulär und folgenreich ist aber, in welcher Offenheit in beiden Fällen von einem Informationskrieg gesprochen und damit ein Kriegszustand nicht nur suggeriert, sondern geradezu deklariert wird. Und dieser beschränkt sich nicht nur auf den Informatiosraum, auf Propaganda. Denn in der Entschließung heißt es an verschiedenen Stellen,

> ***„dass Desinformation und Propaganda zur hybriden Kriegsführung gehören;"***

bzw.

> ***„dass Informationskrieg … ein integraler Bestandteil der hybriden Kriegsführung ist, bei der es sich um eine Kombination aus verdeckten und offenen militärischen und nicht militärischen Maßnahmen handelt und die dazu dient, die politische, wirtschaftliche und soziale Lage von im Fokus stehenden Ländern zu destabilisieren, ohne ihnen formell den Krieg zu erklären;"***

Zwischen Propaganda und hybrider Kriegführung wird dabei gar kein qualitativer Unterschied gemacht. Umso erschreckender, was das Europäische Parlament alles als Formen der Propaganda ausmacht. Hierzu gehören Informationen, die dazu führen (sollen):

**** Wahrheiten zu verzerren***
**** Zweifel zu schüren***
**** Mitgliedstaaten zu entzweien***
**** eine strategische Spaltung zwischen der EU und ihren nordamerikanischen Partnern herbeizuführen***
**** den Entscheidungsprozess lahmzulegen***
**** die EU-Organe und Einrichtungen sowie die transatlantischen Partnerschaften gegenüber den Unionsbürgern und den Bürgern benachbarter Länder zu diskreditieren***
**** der auf demokratischen Werten, Menschenrechten und Rechtsstaatlichkeit beruhenden europäischen Botschaft entgegenzuwirken und sie auszuhöhlen***
**** Angst und Unsicherheit bei den EU-Bürgern zu schüren und***
**** feindselige Staaten und nichtstaatliche Akteure als wesentlich einflussreicher darzustellen, als sie tatsächlich sind;***

Da es sich im Krieg wähnt, schlägt das Europäische Parlament verschiedene Maßnahmen vor, die zu ergreifen wären. So fordert es u.a. die Mitgliedstaaten auf,

„die Spionageabwehr zur Abwehr derartiger Maßnahmen [Informationsmaßnahmen Russlands auf europäischem Boden] zu intensivieren“

und dass

„die Nachrichtendienste der EU-Mitgliedstaaten intensiver zusammenarbeiten mit dem Ziel, den Einfluss von Drittstaaten zu bewerten, die das demokratische Fundament und die demokratischen Werte der EU untergraben wollen.“

Zugleich wird gefordert,

„dass die EU ihre Bemühungen im Bereich der strategischen Kommunikation als Priorität erachten und entsprechende Ressourcen mobilisieren sollte.“

Dabei soll u.a.

„die Task Force für strategische Kommunikation der EU gestärkt [werden], indem aus ihr ein vollwertiges Referat innerhalb des EAD gemacht wird, das für die östliche und die südliche Nachbarschaft zuständig ist.“

Auch in diesem Zusammenhang solle

„die Zusammenarbeit zwischen der EU und der NATO im Bereich der strategischen Kommunikation erheblich intensiviert werden:“

Die Maßnhamen, die insbesondere gegenüber Russland ergriffen werden sollen, erinnern teilweise frappierend an das, was Russland selbst als „Informationskrieg“ vorgeworfen wird. So sei ein

„Vorschlag für eine umfassende und flexible Lösung vorzulegen, mit der unabhängige Medienunternehmen, Denkfabriken und nichtstaatliche Organisationen insbesondere in der Muttersprache der Zielgruppe unmittelbar unterstützt werden können.“

Dabei sollten

„Medien, lokale Medien, der investigative Journalismus und fremdsprachige Medien, insbesondere in den Sprachen Russisch, Arabisch, Farsi, Türkisch, Urdu und weiteren Sprachen, deren Sprecher der Propaganda in besonderem Maße ausgesetzt sind, besonders ernst genommen werden und zu diesem Zweck ausreichend Ressourcen bereitgestellt werden.“

Denn das Parlament ist der Auffassung, dass

„Vielfalt, Objektivität, Unparteilichkeit und Unabhängigkeit der Medien in der EU und deren Nachbarschaft, auch bei nichtstaatlichen Akteuren, gestärkt werden müssen, unter anderem indem Journalisten unterstützt werden und Kapazitätsaufbau-Programme für Medienakteure erarbeitet werden, damit Partnerschaften und Netzwerke zum Informationsaustausch (z. B. gemeinsame Informationsplattformen), medienwissenschaftliche Forschung, Möglichkeiten im Bereich Mobilität und Schulungsangebote für Journalisten und Praktika bei Medien in der EU gefördert werden.“

Zugleich seien

„Finanzflüsse zu unterbinden , mit denen Einzelpersonen und Einrichtungen finanziert werden sollen, die strategische Kommunikation betreiben und zu Gewalt und Hass anstacheln.“

Besonders frappierend ist jedoch, dass der Informationskrieg vom Europäischen Parlament nicht nur gegenüber Drittstaaten ausgerufen wird, sondern im Prinzip auch gegen die eigene Bevölkerung und Zivilgesellschaften – auch EU-kritische Institutionen wie die IMI und viele andere dürften sich dadurch durchaus angesprochen fühlen. So wird explizit festgehalten,

> ***„dass es sich bei strategischer Kommunikation und bei Informationskriegen nicht nur um eine außenpolitische, sondern auch um ein innenpolitische Angelegenheit handelt."***

Explizit zeigt sich das EP

> ***„besorgt über die zahlreichen EU-internen Multiplikatoren der gegen die Union gerichteten Propaganda."***

Es fordert

> ***„die zuständigen EU-Organe und -Behörden auf, streng zu überwachen, aus welchen Quellen die europafeindliche Propaganda finanziert wird;"***

Außerdem werden nicht näher bezeichnete „EU-Akteure" aufgefordert,

> ***„Daten und Fakten zum Konsum von Propaganda zu sammeln."***

Betont wird in diesem Zusammenhang,

> ***„dass die Mitgliedstaaten dafür verantwortlich sind, feindliche Informationsmaßnahmen, die in ihrem Hoheitsgebiet durchgeführt werden oder darauf abzielen, ihre Interessen zu untergraben, aktiv, vorbeugend und gemeinsam zu bekämpfen."***

Während man sich also gegenüber Medien in Russland vermeintlich für „Vielfalt, Objektivität, Unparteilichkeit und Unabhängigkeit der Medien" einsetzen und hierfür gezielt einzelne Journalist*innen und Netzwerke finanziell unterstützen möchte, sollen die Quellen „europafeindlicher Propaganda" innerhalb der EU als feindlich verstanden und sogar vorbeugend „bekämpft" werden. Dies gilt für Informationen, die vermeintlich darauf abzielen „staatliche Interessen zu untergraben". Ein weiteres Kriterium scheint zu sein, ob die entsprechenden Medien Gelder aus Drittstaaten erhalten (was u.a. durch die Geheimdienste überwacht werden soll). So betont das Parlament explizit,

> ***„dass es sich zwar nicht unbedingt bei jeder Kritik an der EU oder ihrer Politik um Propaganda oder Desinformation handelt – insbesondere nicht im Rahmen politischer Äußerungen –, dass aber im Falle einer Manipulation oder Unterstützung aus Drittländern, mit der diese Kritik angefacht oder verschärft werden soll, an der Glaubwürdigkeit der jeweiligen Botschaften gezweifelt werden darf."***

Sowohl für die Unterbrechung entsprechender feindlicher „Propaganda", als auch die Platzierung der eigenen „Strategischen Kommunikation" sollen die nötigen juristischen und technischen Voraussetzungen geschaffen werden. Dies kommt u.a. in der Forderung zum Ausdruck,

> ***„dass für die Widerstandsfähigkeit der Informationssysteme gesorgt werden muss – insbesondere gegen Dienstverweigerung und Unterbrechungen, denen bei hybriden Konflikten und Bemühungen, Propaganda entgegenzuwirken, eine zentrale Rolle zukommen kann."***

Auch „in diesem Zusammenhang" bedürfe es

> ***„einer engen Zusammenarbeit mit der NATO ..., insbesondere mit dem Kompetenzzentrum der NATO für kooperativen Schutz vor Computerangriffen."***

Abschließend sei angemerkt, dass es sich hier um eine Entschließung des Europäischen Parlamentes handelt, das – man muss in diesem Zusammenhang fast schon von Glück reden – wenig zu sagen und damit auch wenig mit der tatsächlichen Umsetzung, den rechtlichen und politischen Hürden etc. zu tun hat. Fakt bleibt jedoch, dass das Europäische Parlament hier einen gewissen Kriegszustand deklariert hat und offenbar auch bereit ist, den Informationskrieg zu führen. Wenn wir aus dieser Zusammenfassung etwas lernen können, dann vielleicht auch das, dass es sich bei Begriffen wie Propaganda, Informationskrieg und hybrider Kriegführung um analytisch nicht tragfähige Begriffe handelt, mit denen primär Politik gemacht wird. Die Unterschiede zwischen „Kritik an der EU", „feindlicher Propaganda" und der eigenen „Strategischen Kommunikation" und Unterstützung von Journalisten und Medien bleiben dabei ebenso unklar, wie die Schwelle zum „Informationskrieg" und der „hybriden Kriegführung". Unabhängig davon wurden die „Anerkennung" eines gegen die EU gerichteten „Informationskrieges" als Teil einer „hybriden Kriegführung" und die Ergreifung entsprechender Maßnahmen eingefordert. Das sollte man zur Kenntnis nehmen – ob es darüber hinaus sinnvoll ist, sich die entsprechenden Begriffe selbst zu eigen zu machen, kann hingegen infrage gestellt werden.

SOCIAL MEDIA ALS KRIEGSINSTRUMENT

VON: JACQUELINE ANDRES

Das Sammeln, Manipulieren und Streuen von Informationen war schon immer Bestandteil von Kriegen, doch mit sozialen Netzwerken und Nachrichtenplattformen, Video- und Bildsharing-Diensten findet dies in ganz neuen Dimensionen statt. Im Gegensatz zu den klassischen Print-, Radio- und TV-Medien erfüllt hier keine Redaktion eine Gatekeeping-Funktion, indem sie über die Inhalte entscheidet und sich mit ihren Veröffentlichungen an viele richtet. Vielmehr ermöglichen die sozialen Medien eine Massenkommunikation, in der Nutzer_innen selbst Inhalte erstellen und verbreiten können und sich somit zumindest theoretisch viele an viele wenden können. Knapp ein Drittel der grob definierten Weltbevölkerung benutzte laut der NATO im Januar 2016 unterschiedliche Seiten sozialer Netzwerke; zusehends nehmen Seiten wie Facebook oder auch Twitter eine wichtige Rolle als Nachrichtenquellen ein.[1] Durch diese Kanäle fließen Unmengen an Daten, die einerseits für die Informationsgewinnung im Rahmen von Militäroperationen interessant sein können, aber auch für die Legitimation solcher. Im Laufe der letzten Jahre richteten Militärallianzen wie die NATO verstärkt ihren Fokus auf die Entwicklung eines effektiveren Nutzens der sozialen Medien.

SOZIALE MEDIEN IN DER KRIEGSOPERATIONALISIERUNG

Neben zahlreichen Workshops und Diskussionen zu sozialen Medien veröffentlichten NATO-Strukturen auch aufschlussreiche Berichte und Studien, die erkennen lassen, welchen Stellenwert soziale Medien mittlerweile in der Militärallianz eingenommen haben. In einer dieser Studien heißt es: „Virtuelle Kommunikationsplattformen sind ein integraler Teil der Kriegsführungsstrategie geworden. Die jüngsten Konflikte in Libyen, Syrien und Ukraine haben gezeigt, dass soziale Medien weithin genutzt werden, um Aktionen zu koordinieren, Informationen zu sammeln, und vor allem, um die Überzeugungen und Einstellungen der Zielgruppe zu beeinflussen und diese sogar für Aktionen zu mobilisieren.“[2] Doch nicht nur die Staaten und bewaffnete Gruppierungen erkennen in den sozialen Medien ein großes Potenzial für die Durchsetzung ihrer Interessen: Soziale Medien gaben auch dem Online-Aktivismus eine neue Bedeutung – innerhalb von wenigen Stunden kann eine Petition von Millionen Menschen unterschrieben werden, ein einfacher Klick erleichtert Spendenaufrufe und Hashtag-Stürme werden als sozialer Protest eingestuft, durch den Personen mit technischem Zugang zu solchen Medien Meinungsbilder beeinflussen können. Dies führt bewusst oder auch unbewusst immer wieder dazu, dass sich auf Twitter, Facebook und YouTube Stimmen und Gruppen für Militärinterventionen von westlichen Armeen stark machen.

Im Jahr 2016 veröffentlichte das NATO Exzellenzzentrum für Strategische Kommunikation in Riga eine Studie mit dem Titel „Die Sozialen Medien als Instrument der Hybriden Kriegsführung“. Die Studie stützt sich zum Teil auf die Ausarbeitungen Thomas Elkjer Nissens für das Dänische Militär über die Nutzung sozialer Medien als Waffe aus dem Jahr 2015. So übernimmt die NATO sechs von Nissen ausdifferenzierte Funktionen sozialer Medien für Militäroperationen, auf einige derer in den folgenden Textabschnitten genauer eingegangen wird: „Informationsgewinnung, Zielerkennung, Informations- und Beeinflussungskampagnen (Psychologische Kriegsführung), Cyberoperationen, Verteidigung und Command and Control.“[3] Anschließend richtet die NATO-Studie mit zwei Falluntersuchungen ihr Augenmerk auf eine Auseinandersetzung mit den Methoden der russischen Regierung und der sich als Islamischen Staat bezeichnenden terroristischen Gruppe. Des Weiteren werden vereinzelt auch aufschlussreiche Beispiele des Einsatzes sozialer Medien für Militäroperationen der NATO selbst angeführt.

INFORMATIONSGEWINNUNG UND ZIELERKENNUNG

Zur Informationsgewinnung, mit der auch eine Zielerkennung einhergehen kann, werden demnach unterschiedliche Methoden angewandt, die entweder in offener Zusammenarbeit mit den Nutzer_innen sozialer Medien oder verdeckt erfolgen können.[4]

Die Auswertung öffentlich zugänglicher Quellen (Open-Source-Intelligence) ist seit jeher eine Komponente auch der militärischen Aufklärung. Eine spezifische Methode der Informationsgewinnung durch die sozialen Medien stellt das ‚Crowdsourcing‘ dar. Dabei werden Informationen von einer oftmals aus freiwilligen und anonymen Einzelpersonen bestehenden Menschenmenge (Crowd) auf Twitter oder einer anderen Plattform hochgeladen. Diese Methode gewährt einerseits Aktivist_innen und Medienschaffenden einen Informationszugang zu schwer zugänglichen Krisengebieten, indem sie auf die online gestellten Inhalte zurückgreifen bzw. mit Nutzer_innen kommunizieren können, die von sich behaupten, vor Ort zu sein. Andererseits ermöglicht das Crowdsourcing auch dem Militär, Informationen zu erhalten oder solche auf ihren Wahrheitsgehalt zu überprüfen. Als Beispiel führt die NATO-Studie ein gemeinsames Projekt der US-amerikanischen, regierungsnahen Denkfabrik Atlantic Council und des Rechercheteams von Bellingcat an, die Bild- und Videomaterial aus Syrien nach Aktivitäten des

russischen Militärs analysierten. Beim Durchforsten von „Profilen russischer Soldat_innen, Google Maps, Bildern in den Medien und der durch Crowd-Sourcing erhaltenen Informationen von Zeug_innen“[5] haben Bellingcat und Atlantic Council die Präsenz des russischen Militärs in der Ukraine nachgewiesen, bevor das russische Verteidigungsministerium die Stationierung eigener Soldat_innen öffentlich bestätigte. Im Oktober 2017 erließ der Kreml dann ein neues Gesetz, welches den aktiven Soldat_innen das Veröffentlichen von Inhalten auf den sozialen Medien verbietet, die Informationen über die Einsätze verraten könnten. Damit versucht die russische Regierung zu verhindern, dass Bild- und Videomaterial[6] ungewollt den Ort der Aufnahme preisgibt oder die oftmals automatisch eingestellte Geolokalisierung von Twitter etc. unbemerkt die geographischen Koordinaten verrät.

Die Auswertung auf sozialen Medien veröffentlichter Kommunikationsinhalte und georeferenzierter Bilder und Tweets bildet immer häufiger auch eine fragwürdige Grundlage für Luftangriffe und andere militärische Aktionen. Unter anderem nutzte die NATO bei ihren Bombardierungen in Libyen im Jahr 2011 crowdgesourcte Informationen über die Truppenbewegungen von Muammar Ghaddafis Militär, die mit Smartphones, Google Maps und Twitter festgehalten und der NATO online zugänglich gemacht wurden.[7] Zwar hätten diese offiziell nicht als Einzelnachweise für die Zielortung eines Luftschlages gereicht, doch sie sollen ein wichtiger Teil der Lagebilderstellung gewesen sein und Anstoß zu einer mit AWACS-Flugzeugen durchgeführten Überprüfung der geposteten Informationen gegeben haben – schlussendlich entschied der zuständige Kommandant, welche Gewichtung er der jeweiligen Twitter-Nachricht beimessen sollte.[8]

Auch im Rahmen der US-Operation Inherent Resolve in Irak und Syrien griff das US-Verteidigungsministerium auf Daten zurück, die Soldat_innen der 361st Intelligence, Surveillance and Reconnaissance Group auf dem Marinestützpunkt Hurlburt Field in Florida durch das Durchkämmen online gestellter Inhalte in verschiedenen sozialen Medien erfassten. So verrieten u.a. das gepostete Selfie eines IS-Anhängers vor dem Hauptquartier und seine lobenden Kommentare zu dessen Funktion für den Islamischen Staat auch seinen Standort – es bleibt zu vermuten, dass die Geolokalisierung aktiviert war oder aber ein Element im Bild Aufschluss über den Ort der Aufnahme gab. In weniger als 24 Stunden bombardierte die US-amerikanische Luftwaffe das Gebäude in Grund und Boden. So ergänzen bzw. ersetzen im Extremfall soziale Medien die Informationsbeschaffung vor Ort und können ausreichen, um einen Luftangriff zu befehligen.[9] Wie einfach solche Informationen manipulierbar und wie tödlich sie für die Bewohner_innen der betroffenen Gegenden sein können, wird in der NATO-Studie jedoch nicht weiter ausgeführt.

Der britische Geheimdienst griff ebenfalls auf soziale Medien zurück, um den Hacker Junaid Hussein zu orten und durch einen von der US-amerikanischen Luftwaffe durchgeführten Drohnenangriff zu töten. Zwei weitere britische Staatsangehörige, die gemeinsam mit Junaid für die Rekrutierung des IS zuständig waren, wurden durch die britische Royal Air Force getötet. Über Surespot, einen Messengerdienst, der als verschlüsselte und damit sichere Alternative zu Whatsapp gilt, schickte der Nachrichtendienst GCHQ (Government Communications Headquarters) dem britischen IS-Anhänger und Strategen für soziale Medien Hussein einen kompromittierten Link, der es ihnen erlaubte ihn in seinem Auto zu orten. Amnesty International verurteilte dieses völkerrechtswidrige Vorgehen Großbritanniens scharf.[10]

PSYCHOLOGISCHE KRIEGSFÜHRUNG

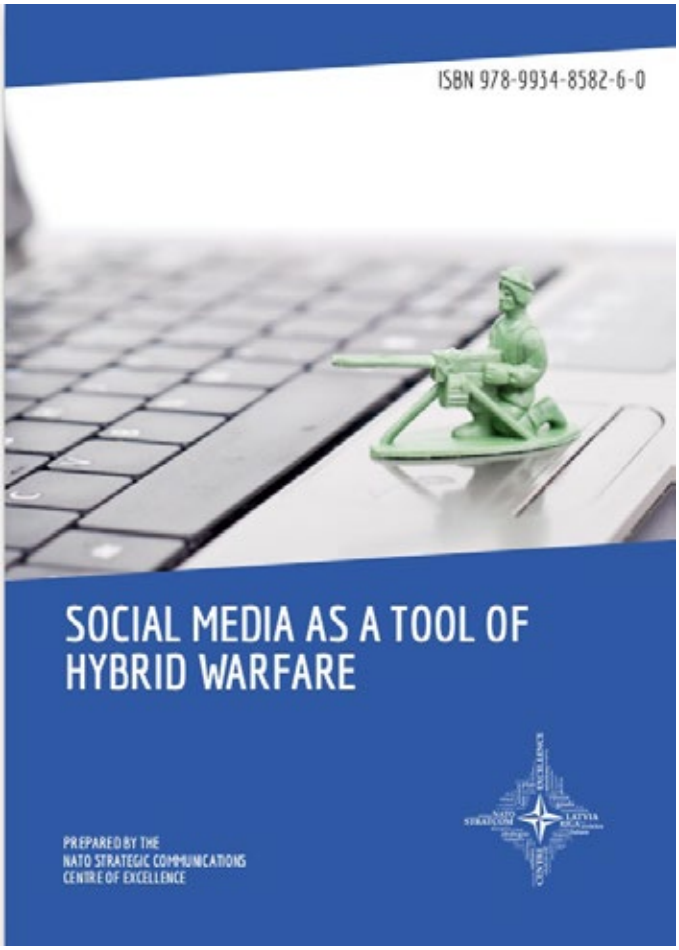
In der gemeinsamen Streitkräftedoktrin für Psychologische Kriegsführung definiert die NATO selbige als „geplante Aktivitäten, die Kommunikationsmethoden und andere Maßnahmen einschließen, die sich an eine genehmigte Zielgruppe richten, um ihre Wahrnehmung, Ein-

stellungen und Verhalten zu beeinflussen, welche sich auf das Erreichen eines politischen und militärischen Ziels auswirken.“[11] Laut der Studie zu „Die Sozialen Medien als Instrument der Hybriden Kriegsführung“ der NATO zählen dazu unterschiedliche Aspekte und Aktivitäten, wie: „Informationen formen, informieren, beeinflussen, manipulieren, aufdecken, kleinreden, fördern, täuschen, zwingen, mobilisieren und überzeugen“. Einerseits kann dies offen durch die Erstellung von offiziellen Websites, Accounts und Kanälen in den sozialen Medien erfolgen. So z.B. verfügt Generalsekretär Jens Stoltenberg über seinen eigenen, offiziellen Twitteraccount mit mittlerweile rund 482.000 Followern und die Bundeswehr ist u.a. mit ihren Rekrutierungsvideos „Die Rekruten“ und „Mali“, auf YouTube und Facebook vertreten. Passend dazu hat die Bundeswehr einen Chat-Bot in dem Facebook-Messenger eingerichtet, um für interessierte User_innen einen „direkten Draht zum Auslandseinsatz“ herzustellen (siehe Beitrag von Alexander Kleiß).[12]

Andererseits wird die psychologische Kriegsführung auch verdeckt geführt: U.a. mit Hilfe von sog. ‚Trolls‘, ‚Bots‘ und ‚Sockenpuppen‘. Unter Trolls versteht man Personen, die absichtlich in Foren, Wikis (Websites, die von Besucher_innen verändert werden können) und Kommentarbereichen stören, um die jeweilige Stimmung innerhalb der Online-Community zu manipulieren. Bots hingegen sind softwarebasierte, automatisierte Programme, die ebenfalls eingesetzt werden, um mit vorgeschriebenen Kommentaren und Tweets gewisse Stimmungen zu erzeugen. Sockenpuppen hingegen setzen sich aus einer Vielzahl an Fake-Accounts zusammen, die von einer Person oder auch einer Personengruppe kontrolliert werden. Sie alle können – oftmals gemeinsam genutzt – die Sichtbarkeit von Nachrichten erhöhen oder senken, Hashtags kapern und das Informationsumfeld der sozialen Medien mit ihren Auffassungen, bzw. der ihrer Auftraggeber_innen beeinflussen.[13]

Um Trolls erkennen zu können, liefert die NATO-Studie im Anhang eine Auflistung erkennbarer Techniken der sozialen Beeinflussung, die in den polnischen, russischen und ukrainische Informationsumgebungen im Kontext des Ukraine-Konflikts angewandt wurden. Gleich im dritten aufgelisteten Muster heißt es: „Die Gegner_innen wollen einen Konflikt generieren: Benutzer_innen geben an, dass der Konflikt zwischen den Staaten essenziell durch die Aktivitäten von Drittparteien generiert wird (NATO, EU und USA), was ihre internationale Position stärkt.“[14] Dadurch zeichnet sich ab, dass eine kritische Haltung den eigenen Regierungen und Bündnissen gegenüber als von einem Troll verbreitete feindliche Propaganda eingeordnet werden und zu einer Delegitimierung dieser Haltung führen kann.

Bekannt sind zwar besonders die sogenannten „Putin-Trolle“, aber auch viele weitere Staaten versuchen gezielt, den Informationsraum sozialer Medien zu beeinflussen. So rief die US-Regierung unter der Obama-Administration im Jahr 2011 die zynisch benannte Operation Earnest Voice (Seriöse Stimme) ins Leben. Das US-Militär zahlte mehr als 2 Millionen US-Dollar an das Unternehmen Ntrepid, damit dieses eine Software entwickelt, mit der US-Soldat_innen jeweils bis zu zehn Sockenpuppen steuern können, die pro-US-amerikanische Kommentare auf Websites außerhalb der USA posten können, um „extremistischer und feindlicher Propaganda entgegenzuwirken“.[15]



Abgesehen von einer angestrebten „Informationshoheit“, geht es auch darum, die Gegner_innen anzugreifen und abzulenken. So werden laut der Studie falsche Informationen und Gerüchte gestreut, die destabilisierende Wirkungen bis hin zu einer Massenpanik erzeugen können. Zu den Angriffen zählt auch das Melden von vermeintlich „unangemessenen Inhalten“ bei Facebook, wenn diese nicht förderlich für die eigenen staatlichen Interessen sind. Es werden Informationen über die Gegner_innen online gesucht, um diese herabzuwürdigen, lächerlich zu machen und zu bedrohen. Falsche Online-Profile würden zudem genutzt, um an Informationen zu gelangen. So z.B. erstellten laut der besagten NATO-Studie die Taliban falsche Profile von Frauen, um Informationen australischer Soldaten zu erfragen. Eine weitere Methode zur Beeinflussung des Informationsraums in sozialen Medien ist das Streuen eines ablenkenden Informationsnebels bzw. -lärms, der ein unbequemes Thema oder Ereignis aus dem internationalen medialen Fokus drängt.

CYBER-OPERATIONEN

Bei Cyber-Operationen handelt es sich um ein offensives Vorgehen im Informationsraum, bei dem es zu Cyberangriffen auf Websites, Profile und E-Mails kommt, um diese zu manipulieren oder kurzzeitig funktionsunfähig zu machen. Dazu zählen absichtlich herbeigeführte Serverüberlastungen (Distributed Denial of Service – DDoS) durch automatisierte Websiteaufrufe.[16] Weitere Angriffsformen umfassen das Hacken von E-Mails, Chaträumen, Smartphones und Online-Profilen, um Daten zu stehlen oder eine Änderung der Inhalte zu ermöglichen. Die Hacker der IS-Gruppe Cyber Caliphat versendeten etwa über mehr als 16.000 französische Websites ihre Nachrichten und attackierten auch strategische Profile bekannter Personen und Organisationen. Einen spektakulären Erfolg hatte Cyber Caliphat im Januar 2015, als es der Gruppe gelang, sich Zugang zu dem Twitter-Account des USCENTCOM zu verschaffen, der für Zentralasien und Teile des Arabischen Ostens – und damit auch für Irak und Syrien – zuständigen Kommandostruktur des US-Militärs. Über diesen Account verschickten sie u.a. folgende Drohungen an US-Soldat_innen: „Amerikanische Soldat_innen wir kommen, seid vorsichtig!“[17] Solche Angriffe können abgesehen von den psychischen auch große wirtschaftliche Schäden verursachen. Die hinter Bashar al-Assad stehende Gruppe Syrian Electronic Army hackte im April 2013 den Twitter-Account einer der größten Nachrichtenagenturen weltweit: der Associated Press (AP). Über diesen schickte die Gruppe eine erfundene Nachricht über zwei Explosionen im Weißen Haus und einen verletzten Präsidenten Obama an die mehr als 1,9 Millionen Twitter-Follower. Auch wenn die Nachricht nach nur drei Minuten von AP revidiert wurde, beförderte sie den Dow Jones an der Börse in einen kurzzeitigen Sinkflug, mit dem Verluste von mehr als 136 Milliarden US-Dollar am Aktienmarkt einher gingen.[18]

COMMAND AND CONTROL

Soziale Medien können Funktionen der klassischen militärischen Führung (Command and Control) übernehmen. Mit Hilfe von Twitter oder auch von geschlossenen Chaträumen koordinieren und kommunizieren Gruppierungen wie der IS ihre Aktivitäten. In nur wenigen Minuten kann eine Nachricht zur Koordination einer Aktion verschickt werden, wodurch sich anschließend unterschiedliche Anhänger_innen kurzfristig zusammenfinden und die Anordnungen ausführen können. Im Gegensatz zu in Gebäuden eingerichteten Hauptquartieren, die – wie das des IS in Raqqa – leicht zum Ziel eines Luftschlages werden können, bildet der digitale Führungsansatz keine physischen Zerschlagungspunkte mehr und ist dementsprechend schlechter zu ermitteln. Die genannte NATO-Studie bemerkt in diesem Zusammenhang, dass es „auf Grund einer Vielzahl an rechtlichen Fragen“[19] schwieriger sei, zivile Strukturen zu zerschlagen, als militärische. Um die Führungsstrukturen, sowie die Anhänger_innen des IS selbst digital zu schützen, verbot der sogenannte Islamische Staat bereits im Jahr 2014 das Nutzen der Geolokalisierungsfunktion bei Twitter und empfahl laut der NATO-Studie zur Kommunikation und Koordination PlayStation, die weniger leicht zu tracken sei.

HASHTAGS FÜR KRIEG?

Mit der zunehmenden Nutzung von sozialen Medien nimmt auch der Online-Aktivismus zu, der oftmals auch mit den Begriffen ‚Clicktivism‘ oder eher kritisch als ‚Slacktivism‘ bezeichnet wird. Zwei Online-Kampagnen, die mit einem Hashtag über Twitter von sich reden machten, waren bzw. sind #Kony2012 und #BringBackOurGirls. Beide Kampagnen haben zur Legitimation von militärischen Interventionen der NATO-Staaten in Afrika beigetragen.

#KONY2012

Die NGO Invisible Children aus der US-amerikanischen Stadt San Diego lud im Jahr 2012 ein Video hoch, welches innerhalb von einer Woche angeblich mehr als 120 Millionen Mal angesehen wurde. Ziel war es, Joseph Kony, den Anführer der ugandischen Lord Resistance Army weltweit bekannt zu machen und die Obama-Administration dazu zu drängen, dafür zu sorgen, dass Kony noch im April 2012 festgenommen wird. Neben den sozialen Netzwerken sollte auch durch Plakate und Graffiti auf den Straßen eine sichtbare Befürwortung der militärischen Zusammenarbeit mit Uganda, Südsudan, der Zentralafrikanischen Republik (CAR) und der Demokratischen Republik Kongo zur Festnahme Konys zum Ausdruck kommen. Bereits seit 2004 drängte Invisible Children die US-amerikanische Regierung zu militärischen Aktivitäten in der Region. So z.B. befürworteten sie ein Gesetz (Lord’s Resistance Army Disarmament and Northern Uganda Recovery Act), welches 2010 vorsah, Kony zu töten oder zu verhaften und die LRA aufzulösen, um, wie der damalige Präsident Obama es formulierte, „eine Zukunft größerer Sicherheit und Hoffnung für die Menschen in Zentralafrika zu erreichen.“ Im Oktober 2011 trafen daraufhin rund 100 US-amerikanische Militärberater_innen in den besagten Ländern ein, um die regionalen Streitkräfte im Kampf gegen Kony zu unterstützen.[20] Der Film von 2012 sollte dafür sorgen, dass diese militärische Präsenz ausgebaut und verlängert wird.

Der ganzen Idee und Aufmachung der Kampagne liegt das koloniale Denken zugrunde, wonach die „unsichtba-

ren“ Kinder aus Norduganda – welche die NGO allein mit ihrem Namen zu vertreten behauptet – militärische Hilfe aus den USA und Europa bräuchten. Ausgeklammert hingegen werden die Verbrechen u.a. des ugandischen Militärs und der SPLA, die ebenfalls durch zahlreiche Berichte für Kinderrekrutierung, Plünderungen, Missbrauch und Vergewaltigungen bekannt sind. Die von der NGO und von der Obama-Administration angewandte Lesart, die in einer Festnahme Konys durch das Militär die Lösung des Problems sah, ist stark simplifizierend und gefährlich, denn sie blendet die sozioökonomischen und politischen Hintergründe komplett aus, darunter die durch Neoliberalismus und den durch die Weltbank mitfinanzierten aggressiven Landraub verursachten Probleme in der Region. Geradezu kaschiert werden dabei auch die geostrategischen Interessen der beteiligten Staaten und die Partikularinteressen der beteiligten militärischen Einheiten. Bei einem öffentlichen Screening des Films in Norduganda, wo zu dem Zeitpunkt nur rund 2% der Bewohner_innen Zugang zu Internet hatten, kam es zu wütenden Reaktionen und Steinwürfen seitens der Zuschauer_innen. Die in dem Film vorgestellten Merchandise-Produkte wurden großenteils als beleidigend wahrgenommen, weil der Kopf und Name Joseph Konys die zahlreichen Poster, T-Shirts, Armbänder, Buttons und Sticker zierten und damit für die Person, die in der Region viel Leid und Elend verursacht hat, visuelle Aufmerksamkeit und Sichtbarkeit geschaffen wurde. Es sei ein Film von weißen Protagonist_innen für ein weißes Publikum, in dem keinerlei Rücksicht auf die Betroffenen genommen werde, so die Kritik. Tatsächlich ging auch nur ein Bruchteil der eingenommenen Spenden an die Menschen in Uganda selbst, während ein Großteil der Gelder zur öffentlichkeitswirksamen Inszenierung Konys in weitere Marketingstrategien, Reisen und Filme investiert wurde.

Das eigens für den afrikanischen Kontinent zuständige Kommando des US-Militärs war erst 2007 gegründet worden und wurde zunächst sehr kontrovers diskutiert. Durch die große Medienpräsenz von Invisible Children erhielt es ein nützliches Aushängeschild zur Verklärung der Gründe seiner jungen Existenz. Sean Poole, einer der Direktoren von Invisible Children, nahm 2014 einen Besuch im AFRICOM in Stuttgart zum Anlass, den „positiven Ansatz“ des AFRICOMs zu loben, das von der Annahme ausgehe, es müssten „afrikanisch-geführte Lösungen für afrikanische Probleme gefunden werden.“[21] Zugleich kooperiert die NGO auch vor Ort mit dem US-Militär und seinen lokalen Verbündeten. Von ihrem Sitz in der kongolesischen Stadt Dungu aus stattet sie Zivilist_innen mit Hochfrequenzradios aus, um die Bewegungen der Rebellen in den weitläufigen Gebieten zwischen Kongo, CAR und Südsudan zu melden. Zugleich bilden dort dem AFRICOM unterstehende US-amerikanische Spezialkräfte kongolesische Soldat_innen aus. Ihre militärische Funktionsfähigkeit hängt von den durch die NGO gewonnenen Bewegungsmustern, der Lagebilderstellung und Aufklärung ab.

#BRINGBACKOURGIRLS

Einen ähnlichen Erfolg wie der Hashtag Kony 2012 hatte #BringBackOurGirls im Jahr 2014. Ibrahim M Abdullahi, ein nigerianischer Anwalt und Obiageli Ezekwesili, die ehemalige Bildungsministerin Nigerias, kreierten #BringBackOurGirls, nachdem die Rebellengruppe Boko Haram mehr als 214 junge Frauen in der Stadt Chibok im Nordosten Nigerias entführt hatte.[22] Es dauerte nicht lange, bis der in Nigeria gestartete Diskurs von den US-Medien in Beschlag genommen und gelenkt wurde. So behaupteten ABC News und CNN kurze Zeit später, die US-Amerikanerin Ramaa Mosley habe den Hashtag gestartet, um Aufmerksamkeit auf das Thema zu lenken. Die Initiator_innen des Hashtags verloren in der Dynamik an Bedeutung und ihre Stimmen wurden auf globaler Ebene marginalisiert und irrelevant. Bilder von bekannten Hollywood-Schauspieler_innen, die auf den roten Teppichen der Welt Schilder mit dem Hashtag hochhielten oder das Selfie einer betroffen wirkenden Michelle Obama im Weißen Haus mit dem Hashtag dominierten die sozialen Medien und fanden ihren Weg in die großen Zeitungen. Der ursprünglich an die nigerianische Regierung gerichtete Hashtag wendete sich zusehends an die westlichen Militärapparate, die intervenieren sollten – und wollten. Die nigerianisch-amerikanische Journalistin Jumoke Balogun kritisierte diese Entwicklung lautstark: „... das US-Militär liebt euren Hashtag, weil er ihm Legitimation verschafft, um seine Militärpräsenz in Afrika auszuweiten. AFRICOM, der Militärapparat, der für die militärischen Aktivitäten der USA in Afrika verantwortlich ist, hat von

#Kony2012 profitiert und wird nun sogar noch mehr von #BringBackOurGirls profitieren. […] Lasst uns nicht vergessen, dass die Mission des AFRICOMs die Durchsetzung von nationalen Sicherheitsinteressen der USA ist".[23]

Tatsächlich schickte das US-Militär im Mai 2014 80 Soldat_innen in den Tschad und seit Oktober 2015 sind mittlerweile rund 300 US-amerikanischen Truppen in Kamerun stationiert, um das dortige Militär für den Kampf gegen Boko Haram auszubilden. In diesem Zuge haben die US-Soldat_innen den kamerunischen Stützpunkt Salak ausgeweitet, der neben den Ausbildungstätigkeiten auch für die Stationierung und Steuerung von Überwachungsdrohnen genutzt wird. Auf dem Gelände sind auch französische Soldat_innen und Söldnergruppen stationiert. Auf dem Stützpunkt finden nach Recherchen von Amnesty International Folter und gesetzwidrige Inhaftierungen statt. Mehr als 60 Opfer berichteten Amnesty International von der erlittenen Folter, von der, wie Forensic Architecture durch eine digitale Nachstellung der Zeugenaussagen herausarbeitete, die US-Militärs zwangsläufig gewusst haben mussten.[24] Mittlerweile ist das US-Militär mit mehr als 6.000 Soldat_innen und 46 Stützpunkten unterschiedlicher Ausmaße absehbar langfristig in Afrika präsent.[25]

Auch bei der #BringBackOurGirls-Kampagne werden die sozioökonomischen Gegebenheiten und geopolitischen Interessen ausgeblendet, während die geforderte Militarisierung die Situation verschlechtert. Zugleich schadet sie dem politischen Ziel der Gruppe in Nigeria, die den Hashtag gestartet hat. Ihr Fokus war es, zunächst den damaligen Präsidenten Goodluck Jonathan zum Handeln zu drängen, jedoch nicht, das Militär zu befähigen, einzugreifen. Das nigerianische Militär – ebenso wie das des Tschad – ist für Gewalt und Missbrauch gegen Terrorverdächtige berüchtigt. Es bombardiert Dörfer und wendet Kollektivstrafen gegen Bevölkerungsgruppen an, die verdächtigt werden, mit Boko Haram zu sympathisieren. Laut Amnesty International seien während des ersten Halbjahres 2013 mehr als 950 Personen im Gewahrsam des nigerianischen Militärs gestorben – die meisten von ihnen wurden der Zugehörigkeit zu Boko Haram verdächtigt. Bis 2016 soll die Zahl der in Haft gestorbenen Verdächtigen auf 8.000 gestiegen sein, weshalb Untersuchungen gegen das nigerianische Militär dringend notwendig seien.[26] Der Einsatz des Militärs gegen die Bewohner_innen Nigerias im so genannten Kampf gegen den Terror sowie die wirtschaftliche und politische Marginalisierung der muslimischen Bevölkerung Nordnigerias sind zwei der ursprünglichen Probleme, die zur Gründung und Radikalisierung Boko Harams geführt haben. Die Forderung #BringBackOurGirls, mit der die nigerianischen Aktivist_innen regelmäßig Demonstrationen und Kundgebungen in der nigerianischen Hauptstadt Abuja organisierten, kritisierte die nigerianische Regierung und ihre Handlungsunfähigkeit und Korruption auf eine viel politischere und tiefgreifende Art, als die plumpe Forderung nach internationalem militärischen Eingreifen.

FAZIT

Soziale Medien nehmen in verschiedenen Funktionen Einfluss auf Militärinterventionen – egal, ob bereits zu Beginn eine entsprechende Absicht dahinter steckte oder nicht. Aus den Bemühungen der NATO ist zu erkennen, dass das Steuern und Nutzen der sozialen Medien wachsen wird, um die eigenen Interessen durch eine Beeinflussung der öffentlichen Meinung und durch Angriffe auf die Nutzung sozialer Medien durch „feindliche" Akteure zu erreichen. Zugleich ist absehbar, dass die Nutzung dieser Medien für den Ausdruck zivilen Dissens' von unterschiedlichen Regierungen zusehends als feindliche Propaganda abgetan und kriminalisiert wird: Wer gegen uns ist, betreibt Propaganda für den Feind!

ANMERKUNGEN

1 NATO Strategic Communications Centre of Excellence: Social Media as a Tool of Hybrid Warfare, stratcomcoe.org, Mai 2016, S. 4.
2 Ebd.
3 Ebd.: 13.
4 Ebd.
5 Ebd.: 14.
6 Russian soldiers face ban on selfies and blog post, bbc.com, 05.10.2017.
7 NATO 2016: 23.
8 Spencer Ackermann: NATO's Newest Bombing Tool: Twitter, wired.com, 06.10.2011.
9 NATO 2016: 25, Michael Hoffman: US Air Force Targets and Destroys ISIS HQ Building Using Social Media, military.com, 03.06.2015.
10 Patrick Wintour und Nicholas Watt: UK forces kill British Isis fighters in targeted drone strike on Syrian city, theguardian.com, 07.09.2015.
11 NATO 2016: 17.
12 Auf Instagramm sind neben ästhetisierenden Bilder aus den Einsatzgebieten auch Videos des Welpen und „Kameraden" Cassey zu sehen und in der Weihnachtszeit 2017 konnten Nutzer_innen täglich bei den #BwAdventskalender von #MajorSanta Preise gewinnen.
13 Markus Reuter: Fake-News, Bots und Sockenpuppen – eine Begriffsklärung, netzpolitik.org, 29.11.2016.
14 Ebd.: 43.
15 Shaun Waterman, "U.S. Central Command 'friending' the enemy in psychological war", washingtontimes.com, 01.03.2011.
16 NATO 2016: 14.
17 Ebd.: 15.
18 Ebd., Max Fisher: Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?, washingtonpost.com, 23.04.2013.
19 NATO 2016: 15.
20 Brian Bennett und Robyn Dixon: U.S. sending military advisors to Uganda, articles.latimes.com, 15.10.2011.
21 Scott Nielsen: Nine Questions for Sean Poole, africom.mil, 20.03.2014.
22 #BBCtrending: The creator of #BringBackOurGirls, bbc.com, 07.05.2014.
23 Jumoke Balogun: 'Dear world, your hashtags won't #BringBackOurGirls', theguardian.com, 09.05.2014.
24 Robert Trafford und Nick Turse: Cameroonian Troops Tortured and Killed Prisoners at Base Used for U.S. Drone Surveillance, theintercept.com, 20.07.2017.
25 Nick Turse: America's War-Fighting Footprint in Africa, tomdispatch.com, 27.04.2017.
26 Another brutal attack by Boko Haram highlights the weakness of Nigeria's military, economist.com, 05.02.2016, Nigeria: Deaths of hundreds of Boko Haram suspects in custody requires investigation, amnesty.org, 15.10.2013.

LEAKS UND DIE KONSTRUKTION VON WIRKLICHKEIT

INFORMATIONSFREIHEIT UND MANIPULATION – DAS BEISPIEL SÜDKOREA

VON: CLAUDIA HAYDT

Geopolitik spielt in der globalen politischen Landschaft eine immer größere Rolle und so genannte Leaks beeinflussen das politische Klima in einzelnen Ländern oder haben sogar weltweit Auswirkungen. Geheime oder zumindest nicht öffentliche Informationen über Regierungshandeln, private Kommunikation oder Pläne von Oppositionskräften sickern immer wieder zufällig oder auch gezielt nach außen. Dies kann man als eine spezielle Form des Whistleblowings bezeichnen und es liegt in der Natur der Sache, dass die Quelle häufig nicht überprüfbar ist. Die Qualität der geleakten Informationen kann nur in begrenztem Umfang beurteilt werden. Klassische Kommunikationsmodelle gehen davon aus, dass wir Sender, Empfänger und Kontext von Kommunikation kennen. Daraus lassen sich Motive erahnen und Konsequenzen abschätzen. Bei Leaks ist dies nicht so einfach. Die Frage „Wer leakt was, an wen, in welchem Kontext, mit welchen Absichten?“ lässt sich nicht ohne Weiteres beantworten. Aus guten Gründen kennen wir die Namen der Whistleblower in der Regel nicht. Dies bedeutet aber auch, dass wir die Glaubwürdigkeit der Personen, die uns die Daten zur Verfügung stellen, nicht einschätzen können. Viele Leaks bestehen zudem aus einer nahezu unübersichtlichen Datenflut – egal ob es um militärische Geheimnisse aus Afghanistan oder um Offshore-Konten geht – wir sind dabei auf die Recherche und Auswahl von Medienhäusern angewiesen. Die Kriterien der Aufarbeitung durch recherchierende Journalist*innen lassen sich zwar in begrenztem Umfang nachvollziehen, sie sind aber ebenfalls nicht frei von Interessen. Dass Geheimdienste in diesem Kontext eine Rolle spielen, liegt nahe, ist aber nur in wenigen Fällen mit überprüfbaren Fakten zu untermauern. Als relativ gut dokumentiertes Beispiel werde ich nach einigen allgemeinen Hinweisen zur Bedeutung von Leaks auf die Instrumentalisierung von Leaks durch den südkoreanischen Geheimdienst eingehen.

KAMPF UM INFORMATIONSFREIHEIT UND MANIPULATIONSGEFAHR

Wir wissen zudem auch nicht zuverlässig, wer die intendierten Empfänger der geleakten Informationen sind. Sind die Informationen für Steuerbehörden gedacht, für die Öffentlichkeit im jeweils „eigenen“ oder einem anderen Land oder geht es um eine – begrenzt vorhandene – globale Öffentlichkeit? Versuchen wir vor dem Hintergrund dieser sparsamen Informationslage die Motivation für die Leaks zu ergründen, dann wird es noch komplexer. Geht es um Informationsfreiheit, um den Versuch Verbrechen von Regierungen oder Unternehmen aufzudecken? Geht es um kriminelle oder politische Absichten und wenn ja: um welche politische Absichten? Es ist nicht zu leugnen, dass im Falle von Leaks Information und Manipulation nicht immer scharf zu trennen sind. Als kritische Konsument*innen von Nachrichten stehen wir hier vor einer großen Herausforderung.

Die Enthüllungsplattform Wikileaks ist wahrscheinlich die bekannteste. Weniger vertraut ist möglicherweise die Vorgänger-Plattform Cryptome (cryptome.org). John Young hat das Prinzip einer Enthüllungsplattform, auf der anonym Informationen von Militärs, Geheimdiensten und Regierungen veröffentlicht werden können, in den 1990er Jahren wesentlich mitentwickelt und etabliert. Dazu gehörte auch die Verbreitung von Techniken, die die eigene Anonymität im Netz sicherstellen (pretty good privacy) und Verschlüsselung nicht nur für Militärs und Geheimdienste zugänglich machen. Wesentliche Akteure dieser Demokratisierung von Wissen und Techniken stammten aus der so genannten Cypherpunk-Bewegung, die seit Ende der 1980er alles daran setzt, einerseits staatliche Geheimniskrämerei durch strikte Offenlegung zu konterkarieren und andererseits private Informationen zu schützen. Young beschrieb die demokratischen Ziele der auch von ihm mitgestützten Cypherpunk-Bewegung 2012 in einem Interview: „Das Anliegen von Cypherpunks war es, mehr Transparenz in die Weltpolitik zu bringen. Wir glauben, dass Geheimniskrämerei einer Demokratie schadet. Sobald Sie akzeptieren, dass Geheimhaltung für dieses und jenes notwendig sei, verbreitet sie sich wie ein Virus.“[1]

Cryptome hat zahlreiche staatliche, vor allem militärische, Informationen offengelegt. Später kamen über Julian Assange und die Plattform Wikileaks Hunderttausende von Dateien, zum Beispiel mit Details des Afghanistan-Krieges, an die Öffentlichkeit. Auch viele der Informationen über die schmutzigen Details des Irak-Krieges, Bilder von Opfern, die das Militär dokumentiert aber nie veröffentlicht hat, haben wir mutigen Whistleblowern zu verdanken. Wir können nur hoffen, dass allein die Möglichkeit, dass Kriegsverbrechen auf diese Weise ans Tageslicht kommen können, einen gewissen Einfluss auf militärisches Handeln haben kann. Für die deutsche Öffentlichkeit von besonderer Bedeutung waren die Veröffentlichungen von Edward Snowden über das, was der US-Geheimdienst NSA in Deutschland und weltweit tut. Das Beispiel Snowdens, der nach wie vor in Russland lebt, zeigt die weitreichenden persönlichen Konsequenzen, die mit einer Veröffentlichung von Staatsgeheimnissen einhergehen können.

Für die demokratische Öffentlichkeit können Leaks eine Informationsquelle von unschätzbarem Wert sein und gleichzeitig ist die Gefahr der Manipulation durch Leaks

nicht von der Hand zu weisen. Gleichzeitig gibt es – beabsichtigt oder unbeabsichtigt – weitere Profiteure von veröffentlichten Leaks. So wurde Chelsea Manning vorgeworfen, sie würde „Terroristen“ oder Angehörigen der Taliban wichtige Informationen über das Vorgehen von US-Militärs zukommen lassen. Das klingt plausibel, doch darf wohl angenommen werden, dass die jeweiligen Gegner des US-Militärs besser über die Praktiken des US-Militärs informiert sind, als die westliche Öffentlichkeit und sie wahrscheinlich wenig Neues aus den Leaks erfahren haben. Dennoch können militärische und politische Leaks auch machtpolitische Konsequenzen haben und werden deswegen auch von staatlichen oder staatsnahen Stellen gezielt eingesetzt.

SÜDKOREA: GEHEIMDIENSTKAMPAGNEN GEGEN LINKE OPPOSITION

Als Beispiel für den strategischen Einsatz von „Leaks“ und Informationskampagnen durch Geheimdienste will ich im Folgenden näher auf politische Entwicklungen der letzten Jahre in Südkorea eingehen.

Beim Präsidentschaftswahlkampf im Jahr 2012 operierte der südkoreanische Geheimdienst massiv mit so genannten Leaks. Mit Millionen von Tweets[2] machten Geheimdienstmitarbeiter Stimmung gegen den Kandidaten der Demokratischen Partei Moon Jae-In mit erfundenen Enthüllungen über seine vermeintliche Kooperation mit Nordkorea und die daraus resultierenden Sicherheitsgefahren für Südkorea. Diese Kampagne trug möglicherweise wesentlich dazu bei, dass seine konservative Konkurrentin Park Geun-Hye damals als Präsidentin gewählt wurde. Mit dem Mittel der „Enthüllung“ wurde gezielt und erfolgreich eine politische Stimmung geschaffen. Wenige Monate später stießen Parlamentarier*innen eine Untersuchung der Vorkommnisse an, woraufhin der Geheimdienst seine illegalen Aktivitäten zugeben musste und Geheimdienstmitarbeiter inklusive des damaligen Direktors gerichtlich verurteilt wurden. Eine wichtige Rolle bei der Aufarbeitung des Geheimdienstskandals spielte neben der Demokratischen Partei auch die kleine Vereinigte Fortschrittspartei (UPP).

Der UPP wurde etwa ein Jahr später von dem gleichen Geheimdienst eine „Verschwörung“ vorgeworfen. Auf Grundlage eines geleakten (und massiv manipulierten) Mitschnitts wurde eine Friedensveranstaltung in einer Kirche zu einer „Verschwörung“ des Nordens. Der Vorwurf: In Absprache mit Nordkorea hätten führende UPP-Partei- und Fraktionsmitglieder angeblich einen gewaltsamen Umsturz in Südkorea geplant. Mehrere UPP-Politiker*innen wurden daraufhin verhaftet und ein Parteiverbotsverfahren gegen die UPP eröffnet. Trotz intensiver Solidaritätsarbeit durch Amnesty International und andere Menschenrechtsorganisationen und obwohl die Staatsanwaltschaft keinen einzigen Beweis für die Vorbereitung eines bewaffneten Aufstandes liefern konnte, wurden Politiker wie der Abgeordnete Lee Seok-ki zu mehrjährigen Haftstrafen[3] verurteilt und das Verbotsverfahren erfolgreich umgesetzt.

Einen Aufschrei der Regierungen westlicher Staaten angesichts dieses und weiterer Angriffe auf die Demokratie in Südkorea gab es nicht - weder aus Berlin noch aus Washington. Dies verwundert kaum, denn schließlich sind Geheimdienst und Militär Südkoreas enge und strategisch wichtige Verbündete der NATO.

VERMEINTLICHER HACK UND TATSÄCHLICHE MILITARISIERUNG

Sechs Jahre bevor der südkoreanische Geheimdienst seine Kampagne für die Kandidatur von Frau Park ins Leben gerufen hatte, wurde bekannt, dass auf der südkoreanischen Insel Jeju ein US-Tiefseehafen errichtet werden soll. Die Bewohner der Insel sprachen sich zu 95% gegen das Projekt aus und nutzten alle demokratischen und legalen Möglichkeiten, das Projekt zu blockieren. 2011 wurde auf der bereits erwähnten Enthüllungsplattform Cryptome veröffentlicht[4], dass Geheimpolizisten ein Fischerdorf auf der Insel überfallen und drei Anführer des friedlichen Widerstands festgenommen hatten. Weitere Repressalien trafen nahezu sämtliche Unterstützer des Protests. Dieser war der Auftakt für eine umfassende Kampagne gegen die Friedensbewegung auf der Insel Jeju und darüber hinaus. Dennoch gelang es den Bewohnern bis zur Fertigstellung

der Militärbasis im Jahr 2015 den Baubetrieb insgesamt sieben Mal zu stoppen.[5]

Trotz Unterstützung durch einzelne Angehörige von internationalen Friedensorganisationen spielte der Kampf der Inselbewohner gegen die Militärbasis, gegen die Zerstörung der Korallenriffe und des fragilen Unterwasser-Ökosystems in der internationalen Presse keine Rolle. Ganz anders war der mediale Widerhall auf den so genannten Sony-Hack. Hier wurde Nordkorea beschuldigt, den Sony-Konzern gehackt zu haben – vorgeblich aus Unzufriedenheit über den Film „Das Interview“, der den Nordkoreanischen Staatschef Kim Jong-Un despektierlich darstellte. Auch wenn vieles darauf hindeutet[6], dass ehemalige Mitarbeiter für den Angriff auf die EDV des Unternehmens verantwortlich waren, wurde diesem Sony-Hack sehr viel mehr Aufmerksamkeit gewidmet, als dem Ausbau der US-Militärinfrastruktur im Pazifik und dem Protest dagegen.

„LEAKS“ ALS MITTEL DER REPRESSION

Bis zu den millionenfachen Kerzenlichtdemonstrationen gegen Präsidentin Park Ende 2016 waren die Bedingungen für linke Opposition und linke Öffentlichkeitsarbeit nach dem Verbot der UPP äußerst schwierig. Über das Ausmaß der Repression konnte ich mir selbst ein Bild machen. Ich hatte im Oktober 2016 südkoreanische Friedens- und Menschenrechtsaktivisten nach Berlin eingeladen, um beim Kongress des International Peace Bureau (IPB)[7] über die Situation in Südkorea zu berichten. Der Workshop war recht schlecht besucht, da die Situation auf der koreanischen Halbinsel zu diesem Zeitpunkt kaum auf der globalen politischen Agenda stand. Etwa ein Dutzend Menschen beteiligten sich an dem Workshop, aber darunter war offensichtlich auch der südkoreanische Geheimdienst. In den südkoreanischen Medien[8] wurde nahezu reißerisch darüber berichtet, dass in dem Workshop verurteilte Verbrecher als Friedensaktivisten bezeichnet worden wären. Tatsächlich ging es in dem Workshop um hunderte inhaftierte südkoreanische Kriegsdienstverweigerer, um die Proteste in Jeju, um die UPP, die sich intensiv für Friedensverhandlungen mit dem Norden eingesetzt hatte, und um den verhafteten Abgeordneten Lee Seok-ki. Als Quelle für das Transkript eines Audiomitschnitts wurde in den Zeitungsartikeln ein „Institut zur Erforschung der Geschichte“ angegeben. Nicht angegeben wurde, dass der Mitschnitt ohne Genehmigung erstellt wurde. Ein solches Institut gibt es zwar nicht, aber es taucht immer wieder in südkoreanischen Medien auf, wenn Informationen aus dubiosen Quellen (vermutlich Geheimdienstquellen) an die Öffentlichkeit geleakt werden sollen.

Auch wenn der „Leak“ aus dem IPB-Workshop völlig unspektakulär war, so war die Botschaft an die südkoreanischen Aktivisten jedoch ziemlich eindeutig. Wo auch immer auf der Welt sie sich um die Organisation von Solidarität bemühen, müssen sie auch damit rechnen, dass der Geheimdienst ebenfalls vor Ort ist. Glücklicherweise konnte weder die Repression in Südkorea noch die an anderen Orten der Welt die Empörung stoppen, die sich Ende 2016 in Südkorea gegen Präsidentin Park entlud. Millionen von Menschen gelang es, so viel Druck zu entfalten, dass Präsidentin Park des Amtes enthoben wurde und sie wegen Korruption zu einer mehrjährigen Haftstrafe verurteilt wurde. Die politischen Verwüstungen, die während ihrer Amtszeit entstanden, sind leider noch nicht alle beseitigt und nach wie vor sitzen Opfer ihrer Politik im Gefängnis.

WIE UMGEHEN MIT LEAKS?

Doch zurück zur politischen und medialen Situation hierzulande. Wie sollen wir mit Leaks umgehen? Wie bei anderen Informationen lohnen die Fragen danach, wem die Veröffentlichung nützt, wie vollständig sie ist, welche Aspekte eventuell fehlen und (soweit das möglich ist) welche Quelle die Daten veröffentlicht hat. Gibt es weitere Quellen, mit denen wir die Leaks wenigstens teilweise verifizieren (oder falsifizieren) können oder wollen wir die Nachricht vielleicht selbst einfach nur zu gerne glauben? Welche Zielgruppe wird mit der Information angesprochen? Gibt es einen Zusammenhang mit anderen regionalen oder globalen Entwicklungen? Welche politischen Schlussfolgerungen können oder müssen aus den Informationen gezogen werden und gibt dies wiederum eine Antwort auf die Frage, wem die Veröffentlichung nutzt? Ob damit die Daten als solche richtig sind oder falsch sind, wissen wir natürlich immer noch nicht. Mit meinem kurzen Blick auf Südkorea habe ich versucht, die Bedeutung von tatsächlichen und erfundenen Leaks zu zeigen. Diese Instrumentalisierung müssen wir bei allen Kämpfen um Transparenz und Informationsfreiheit immer mitdenken. Aber eine Forderung liegt auf jeden Fall klar auf der Hand: die Abschaffung von Geheimdiensten.

ANMERKUNGEN

1 „WikiLeaks hat sich mit den Regierungen verbündet“, Interview mit John Young, zeit.de vom 9.7.2018.

2 Justin McCurry: South Korea spy agency admits trying to rig 2012 presidential election, theguardian.com vom 4.8.2017.

3 Claudia Haydt: Neun Jahre Haft, IMI-Standpunkt 2014/041.

4 „South Korean undercover police crack down on peaceful resistance to Jeju Island naval base construction after increased international attention, Gangjeong Village mayor among those arrested“, cryptome.wikileaks.org vom 18.7.2011.

5 Choe Sang-Hun: Island’s Naval Base Stirs Opposition in South Korea, nytimes.com vom 18.7.2011.

6 Kim Zetter: The Evidence That North Korea Hacked Sony Is Flimsy, wired.com vom 17.12.2014.

7 Caught between Saber Rattling and Political Repression – The Parameters of Peace and Human Rights Politics in South Korea, ipb2016.berlin.

8 Beispiele hierfür finden sich u.a. unter http://www.munhwa.com/news/view.html?no=2016101001070109043001; http://www.munhwa.com/news/view.html?no=2016101101070930307001.

MASSENÜBERWACHUNG, HACKING UND DISKURSIVE INTERVENTIONEN VON GEHEIMDIENSTEN

VON: MORITZ TREMMEL

Der alte Scherz, NSA stünde für „No Such Agency“ (so eine Agentur gibt’s nicht), verlor im Sommer 2013 seine Pointe: Mit den Snowden-Leaks wurde NSA zum Schlagwort für eine umfassende, globale (Telekommunikations-) Überwachung, die viele bis dato für unmöglich gehalten hatten. Seither wird der umfangreiche Snowden-Fundus ausgewertet und es werden immer weitere Details und Überwachungsprogramme ans Licht gezogen.

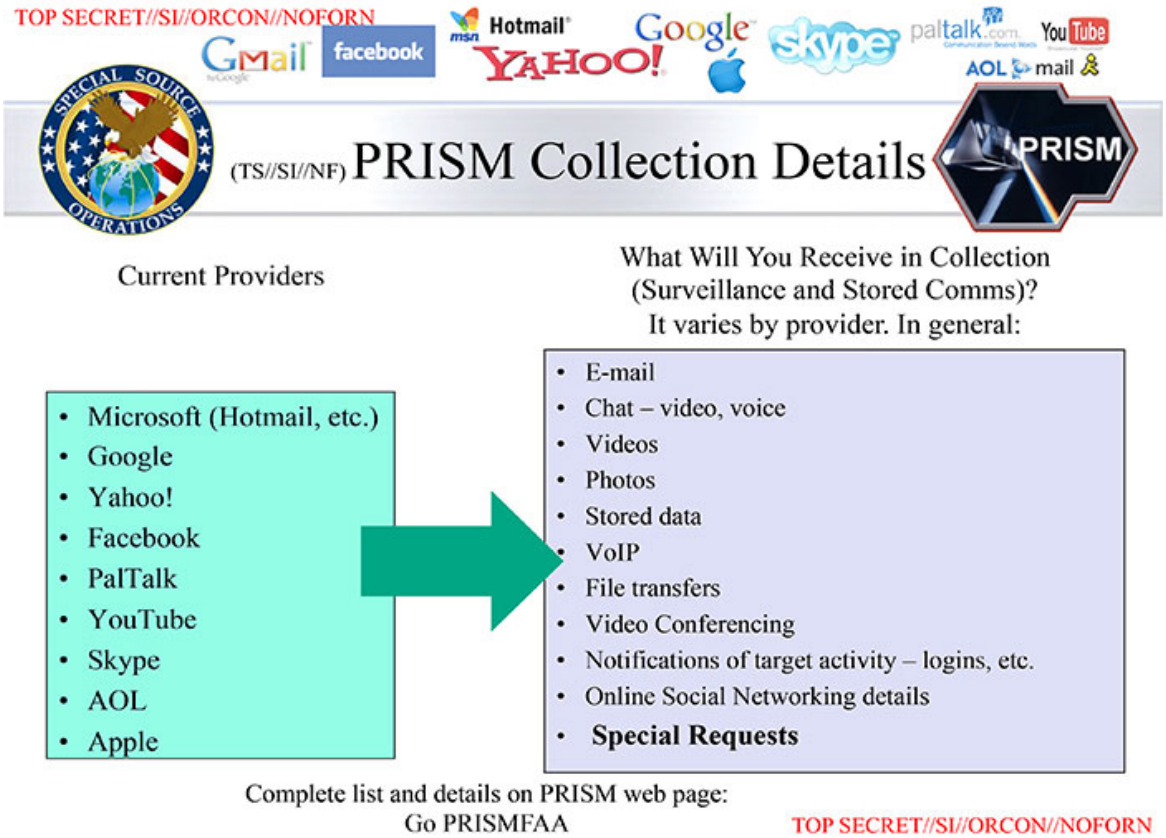
Teile der Leaks belegen die äußerst enge Zusammenarbeit der westlichen Geheimdienste im Bereich der Massenüberwachung. Sie betreiben gemeinsame Überwachungsprogramme, zum Teil ganze Überwachungszentren, teilen (Analyse-)Software und Daten untereinander. Das erklärte Ziel: „Collect it all“ (sammle alles). Jedwede Telekommunikation soll erfasst werden. Neben dieser Massenüberwachung verschaffen sich die Geheimdienste auch im großen Stil Zugang zu unseren Geräten (Hacking). Darüber hinaus nehmen sie auch Einfluss auf gesellschaftliche Diskussionen und Akteure. Diese drei Aspekte geheimdienstlicher Arbeit sollen im Folgenden näher beleuchtet werden.

MASSENÜBERWACHUNG: PRISM & UPSTREAM

Die Geheimdienste arbeiten bei der massenhaften Telekommunikationsüberwachung mit der sogenannten Heuhaufen-Theorie. Die relevanten Daten sind metaphorisch die Nadel. Um diese zu finden, braucht es den kompletten Heuhaufen - also jegliche Telekommunikation weltweit.[1]

Um diesen Heuhaufen möglichst umfassend abzugreifen, betreiben die Geheimdienste unzählige Überwachungsprogramme. Eines dieser Programme trägt den Namen PRISM und wird von der NSA eingesetzt. Es liefert den Zugriff auf unsere Daten bei neun amerikanischen Internet-Riesen: Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL und Apple. Die populären Plattformen werden von Abermillionen von Menschen genutzt. Allein durch dieses Programm erhält die NSA (und indirekt auch ihre befreundeten Geheimdienste) deren Internetsuchabfragen, E-Mails, Chats, Videos, Fotos, Internet(video)telefonie und weitere Daten, die die Nutzer_innen in ihren Onlinespeichern ablegen oder über die Plattformen teilen. PRISM ist ein zentraler Baustein in der Überwachungsarchitektur der NSA. Es liefert u.a. einen Großteil der Informationen für das tägliche Briefing des US-Präsidenten.[2]

Die Daten werden aber nicht nur bei den Telekommunikationsanbietern, sondern auch direkt an den Kabeln abgezapft. Besonders interessant sind hier die Unterseekabel, welche ganze Kontinente verbinden, sowie die Knotenpunkte, an denen verschiedene Internetanbieter und Re-



chenzentren ihre Netzwerke verbinden und die Daten untereinander austauschen. Hier kann das Internet im großen Stil überwacht werden. Die NSA nennt das entsprechende Programm UPSTREAM.

Zwischen 2006 und 2008 arbeiteten der BND (Bundesnachrichtendienst), die NSA und die Telekom zusammen und leiteten am Frankfurter Telekom-Knotenpunkt massenhaft Rohdaten aus.[3] Vorgefilterte Auszüge gab der BND an die Kooperationspartnerin NSA weiter. Seit 2009 greift der BND Daten am Internetknotenpunkt DE-CIX, ebenfalls in Frankfurt, ab.[4] Geschwärzte Listen im NSA Untersuchungsausschuss legen mindestens 12 weitere derartige Programme mit Beteiligung des BND nahe.

Auch der britische Überwachungsgeheimdienst GCHQ (Government Communications Headquarters) betreibt mit TEMPORA ein ähnliches Unterfangen. Er macht sich zunutze, dass wichtige Unterseekabel, die Europa mit den USA verbinden, in Großbritannien anlanden. Durch diese Kabel flossen 2010 ca. 25% des kompletten Internetverkehrs.[5] Diese Daten werden abgefangen und für drei Tage[6] komplett zwischengespeichert.

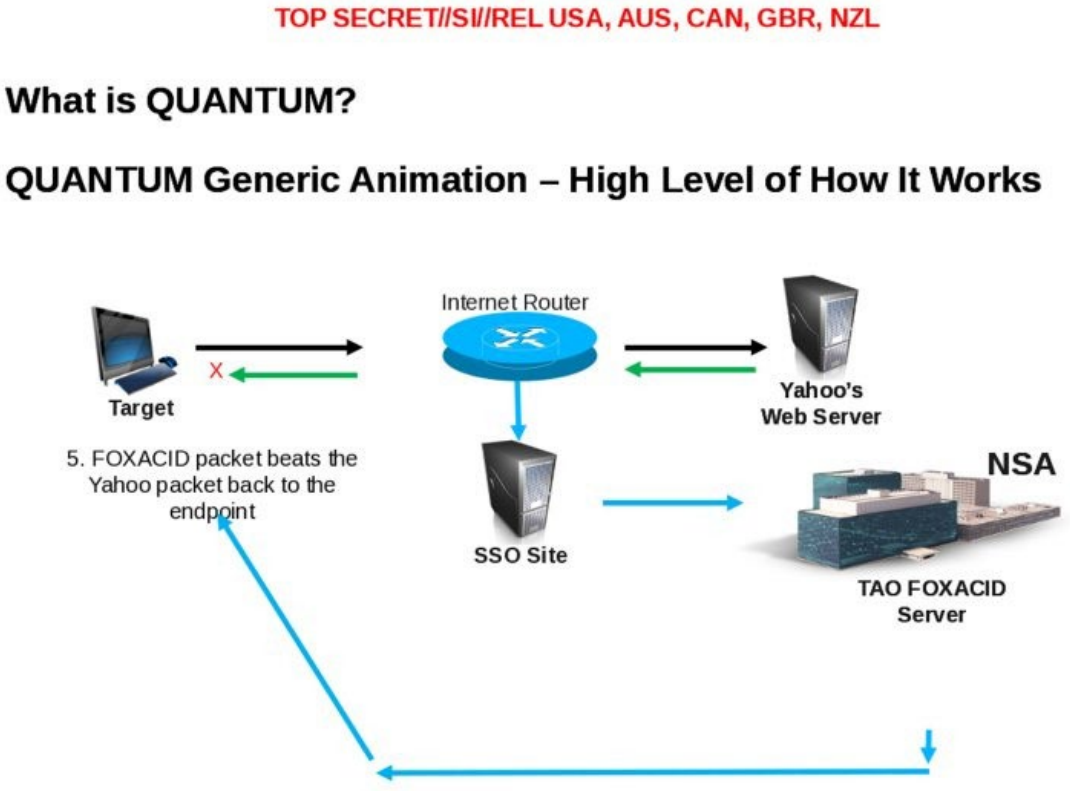
Die von den unzähligen Überwachungsprogrammen - hier konnte nur ein kleiner Ausschnitt gezeigt werden - abgefangenen Daten werden sortiert und in verschiedenen Datenbanken abgelegt. Anschließend können diese von Analyst_innen mit Programmen wie XKEYSCORE abgefragt und ausgewertet werden. Mit XKEYSCORE können Personen live oder rückwirkend im Internet beobachtet werden. Es lassen sich aber auch zu bestimmten Themen oder Gruppen umfangreiche Datensätze anzeigen. Dazu gehören privateste und intimste Informationen, die nur ein Klick entfernt sind.[7]

GEHEIMDIENSTLICHES HACKING: QUANTUM

Neben den überwachten Internetknotenpunkten betreibt die NSA häufig auch Server, um beispielsweise die abgefangenen Daten direkt speichern und für XKEYSCORE aufbereiten zu können. Die Kombination aus einer umfassenden Überwachung der Knotenpunkte und Server in unmittelbarer Nähe zu diesen nutzt sie mit dem QUANTUM-System aus.

Ruft eine Zielperson eine Webseite, beispielsweise die Startseite von Yahoo auf, muss die Anfrage üblicherweise durch mehrere Internetknotenpunkte, um letztlich bei einem Server von Yahoo anzukommen. Dieser schickt die angeforderte Webseite zurück. Die NSA sieht die Anfrage der Zielperson bereits an einem Internetknotenpunkt und schickt eine gefälschte mit Schadsoftware präparierte Yahoo-Seite von einem NSA-Server nahe des Knotenpunktes an die Zielperson. Das Ganze geschieht vollautomatisiert und in Millisekunden – doch es kommt darauf an, wer schneller ist: die echte Yahoo-Seite oder die NSA-Fälschung. Die Nähe zum Knotenpunkt verschafft der NSA dabei etwas Luft. Das reicht bei Weitem nicht immer, aber die NSA hat ja auch nicht nur einen Versuch.[8]

Die in die Webseite integrierte Schadsoftware kann eine Sicherheitslücke im Browser (z.B. Firefox) ausnutzen und anschließend den kompletten Rechner unter ihre Kontrolle bringen: Die Nutzer_in kann bei allem, was sie am



Computer oder Smartphone macht, überwacht werden: Der Bildschirm kann mitbetrachtet, Nachrichten mitgelesen (auch vor der Ver- bzw. nach der Entschlüsselung) und Dateien können aufgespielt oder heruntergeladen werden. Auch eine physische Überwachung ist möglich, wenn das integrierte Mikrofon und die Kamera aktiviert werden. Kurzum, sie kann die Dinge tun, die Schadsoftware klassischerweise kann.

DISKURSIVE INTERVENTIONEN: SQUEAKY DOLPHIN & JTRIG

Nachdem der GCHQ vom Arabischen Frühling komplett überrascht wurde, entwickelte er die Software SQUEAKY DOLPHIN. Das Programm soll gesellschaftliche Entwicklungen, wie etwa Proteste oder Revolutionen, weltweit prognostizieren. Um diese Vorhersagen treffen zu können, werden Social Media-Dienste wie Youtube, Facebook und Blogs bei Blogspot/Blogger in Echtzeit überwacht und nach Städten und Regionen ausgewertet. Hierdurch lassen sich automatisiert bestimmte Trends feststellen und Ableitungen treffen, was in diesen Städten und Regionen in naheliegender Zukunft passieren wird. Mit Hilfe von SQUEAKY DOLPHIN konnte der GCHQ die Proteste gegen die Regierung in Bahrain am 14. Februar 2012 schon einen Tag zuvor vorhersagen.[9]

Die Analyse und Prognose gesellschaftlicher Trends können wiederum die Grundlage vielfältiger geheimdienstlicher, militärischer und staatlicher Handlungen und Interventionen sein. Der GCHQ hat mit JTRIG (Joint Threat Research Intelligence Group) eine eigene Abteilung, die sich um diskursive Interventionen kümmert. Ziel ist es, Personen und Diskurse on- und offline in ihrem Sinne zu beeinflussen. Hierfür standen 2013 150 ausgebildete Mitarbeiter_innen zur Verfügung. Diese hatten unter anderem psychologische Schulungen erhalten, welche ihnen die Grundsätze der Verhaltenspsychologie vermittelten.

JTRIG versucht, auf vielfältige Art Einfluss auf gesellschaftliche Diskussionen zu nehmen. Eine Möglichkeit besteht darin, sich gezielt und planvoll – aber heimlich – in Diskussionen im Internet einzumischen, um diese in die gewünschte Richtung zu lenken. Eine andere Strategie ist der Ausschluss unliebsamer Diskursteilnehmer_innen aus selbigem. Hierzu können beispielsweise Widersprüche im Onlineverhalten (das natürlich überwacht wird) einer Person gesucht werden. Als Beispiel wird eine islamische Autorität genannt, die sich Pornografie ansieht. Eine Veröffentlichung der gefundenen – oder vom Geheimdienst erfundenen – Informationen kann das Ansehen der Person zerstören. Die Veröffentlichung kann dabei unter falscher Flagge, also im Namen von anderen oder erfunden Personen geschehen. Diese können die Informationen auf Blogs veröffentlichen oder belastende E-Mails an Freund_innen, Nachbar_innen oder Verwandte senden. Eine ähnliche Strategie wird mit sogenannten Honey Traps gefahren: Die unliebsamen Personen werden zum Besuch kompromittierender Webseiten verleitet oder es wird eine Online-Bekanntschaft aufgebaut, welche rufschädigend wirkt.

JTRIG kann ihre Opfer von der Telekommunikation abschneiden, indem sie deren Geräte mit SMS oder Anrufen bombardiert. Sie können Fax-Geräte blockieren, Viren oder Ransomware[10] auf Computer oder Smartphones aufspielen, DDoS-Angriffe[11] ausführen oder einfach die Online-Präsenz einer Person löschen. Durch Austausch von Fotos oder Profilbildern in sozialen Netzwerken soll die Paranoia der Opfer einer solchen JTRIG-Aktion oder -Kampagne erhöht werden.

JTRIG nutzt aber auch die klassischen Zersetzungsmethoden: Infiltration von Gruppen, Anstachelung zu Straftaten und verdeckte Ermittlungen. Dieses Methodenarsenal wird durchaus auch gegen Aktivist_innen ausgespielt. Bekannt geworden ist der Einsatz gegen Aktivist_innen während des Arabischen Frühlings sowie gegen die Hacktivist_innen von Anonymous.[12]

ANMERKUNGEN

1 Bruce Schneier: Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World. New York 2015, S. 138.
2 NSA: PRISM/US-984XN Overview. The SIGAD Used Most in NSA Reporting, snowdenarchive.cjfe.org, Folie 5f.; Glenn Greenwald: Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen. München 2014.
3 Die Operation firmiert unter dem Namen EIKONAL.
4 Georg Mascolo, Hans Leyendecker, John Goetz: Codewort Eikonal - der Albtraum der Bundesregierung, sueddeutsche.de, 04.10.2014.
5 GCHQ: Supporting Internet Operations. Special Source Access, snowdenarchive.cjfe.org, 2010, Folie 3; NSA: TEMPORA – „The World's Largest XKEYSCORE" – Is Now Available to Qualified NSA Users, snowdenarchive.cjfe.org, 2012, S. 2.
6 Die drei Tage wurden durch die begrenzte Speicherkapazität 2012 gesetzt und dürften mittlerweile höher liegen.
7 NSA: Introduction to XKS Application IDs and Fingerprints, snowdenarchive.cjfe.org, 2009.
8 Bruce Schneier (2013): Attacking Tor: how the NSA targets users' online anonymity, theguardian.com.
9 GCHQ: Psychology. A New Kind of SIGDEV, snowdenarchive.cjfe.org, 2012, Folie 27 ff.
10 Ransomware verschlüsselt die Daten auf einem betroffenen Gerät und macht es hierdurch unbenutzbar. Häufig wird ein Lösegeld (ransom) für die Entschlüsselung verlangt.
11 Bei einem DDoS-Angriff (Distributed Denial of Service) wird ein Computer oder Server mit extrem vielen Anfragen überhäuft, bis er unter der Last der Anfragen zusammenbricht.
12 GCHQ: Cyber Integration. „The Art of the Possible", snowdenarchive.cjfe.org, 2012, S. 7 ff.

DER INFORMATIONSRAUM AUS MILITÄRISCHER SICHT
CYBERWAR & CYBERPEACE

VON: HANS-JÖRG KREOWSKI

Während Albert Einstein zu einem denkbaren dritten Weltkrieg noch sagt: „Ich bin [mir] nicht sicher, mit welchen Waffen der dritte Weltkrieg ausgetragen wird, aber im vierten Weltkrieg werden sie mit Stöcken und Steinen kämpfen.“, legt sich Mandeep Singh Bhatia fest: „World War III: The Cyber War“ (Der Dritte Weltkrieg: Cyberkrieg, Titel eines Artikels im International Journal of Cyber Warefare and Terrorism, 2011). Wenn auch die meisten anderen Fachleute und KommentatorInnen nicht soweit gehen, zeigt die enorme Resonanz des Themas Cyberkrieg in den Printmedien, dass hier eine neue ernsthafte Bedrohung heraufzieht (siehe Abbildung 1 mit diversen Titelbildern zum Cyberkrieg).

Das Thema hat mit „Zero Days“: Hinter den Kulissen des Cyberkriegs von Alex Gibney auch die Filmwelt erreicht. Der Dokumentarfilm wurde auf der Berlinale 2016 gezeigt. Unter stern.de kann man mit Datum 19. August 2016 recht reißerisch lesen:

„Die Dokumentation von Alex Gibney fängt als Spurensuche über den Computervirus Stuxnet an. Und während IT-Sicherheitsexperten, Ex-NSA- und CIA-Chefs, ehemalige Mossad-Agenten und auch ein paar Whistleblower über das reden, worüber niemand reden darf, fällt der Satz, dass es sich gerade anfühle wie 1945, nachdem die USA zwei Atombomben über Japan gezündet haben: In dieser verwirrend coolen Spionage-Geschichte, die Sie permanent auf der Stuhlkante hält, geht es um mächtige, neue Waffen, über deren Reglementierung man dringend reden muss, wenn die Welt nicht noch mehr im Chaos versinken soll.“

Stuxnet ist aber nur ein Beispiel. Die Liste gravierender Cyberattacken ist lang. So hieß es bei Heise Security am 27. Juni 2017: „Rückkehr von Petya – Kryptotrojaner legt weltweit Firmen und Behörden lahm“, wobei Computersysteme verschlüsselt wurden mit dem Angebot, sie bei Zahlung von Lösegeld wieder zu entschlüsseln. Am 15. Mai 2015 hatte SPIEGEL ONLINE gemeldet: „Sicherheitsalarm im Parlament: Cyberangriff auf den Bundestag“, bei n-tv lautete die entsprechende Überschrift „Cyber-Attacke löst Alarm aus: Beispielloser Angriff auf den Bundestag“. Die Beseitigung des erheblichen Schadens hat über 100 Millionen Euro gekostet. Weitere Beispiele liegen weiter zurück: eine Angriffsserie auf US-amerikanische Computersysteme von Rüstungskonzernen, NASA und andere, die unter dem Namen Titan Rain bekannt wurde, die Denial-of-Service-Attacken auf estländische und georgische Regierungswebseiten, die tagelang außer Betrieb waren, die als Olympic Games bezeichnete und bisher vielleicht gravierendste Malwareattacke mit dem bereits angesprochenen Cyberwurm Stuxnet auf die nuklearen Wiederaufbereitungsanlagen des Irans, die dessen Atomwaffenprogramm um Monate zurückgeworfen hat. Die Entwicklung von Stuxnet hat nach Schätzungen von Fachleuten vielleicht bis zu einer Milliarde US-Dollar gekostet, zeigt aber, dass Cyberattacken zur Zerstörung technischer Anlagen führen können. Viele weitere Beispiele ähnlicher Art ließen sich anführen. Sie alle zeigen, dass sich Cyberangriffe mit Viren, Würmern, Trojanern und sonstiger Schadsoftware für Spionage, Propaganda und Informationsmanipulation verwenden lassen, dass man damit Service-Webseiten und Computersysteme insgesamt lahmlegen, infiltrieren und umfunktionieren kann, ja dass es sogar möglich ist, technische Geräte wie Kraftfahrzeuge, Flugzeuge bis hin zu ganzen Industrieanlagen fernzusteuern oder zu zerstören. Besonders bedroht sind kritische Infrastrukturen wie Energie- und Wasserversorgung, Krankenhäuser, Straßen-, Bahn- und Flugverkehr, Verwaltungseinrichtungen und militärische Einrichtungen. Je nach Ausmaß reichen die Konsequenzen von unbequem bis hin zu Elend und Tod.

ZUM BEGRIFF CYBERKRIEG

An dieser Stelle möchte ich einen Versuch wagen, den Begriff Cyberkrieg wenigstens ansatzweise zu definieren als Kriegsführung mit Informations- und Kommunikationstechnik (IKT) wie Computer, Netzwerke, Software als Waffen und militärische Systeme aller Art, deren Entwicklung und Betrieb des Einsatzes von Informatikmethoden bedürfen. Dabei ist schon umstritten, ob das IKT-Steuerung von militärischen Systemen wie Raketen, Drohnen, Luftabwehr, Panzer etc. einschließt. Ich würde das bejahen, weil es sich um dieselben oder zumindest sehr ähnliche methodische und technologische Grundlagen aus der Informatik sowie der Informations- und Kommunikationstechnik handelt.

Der Begriff Cyberkrieg ist noch relativ jung. Vieles, was darunter subsumiert wird, wurde früher als Informationskrieg bezeichnet. Ute Bernhardt und Ingo Ruhmann geben im Dossier 74 Information Warfare und Informationsgesellschaft – Zivile und sicherheitspolitische Kosten des Informationskriegs, das als Beilage der Zeitschriften Wissenschaft und Frieden 1-2014 und FIfF-Kommunikation 1/2014 erschien, einen umfassenden Überblick. Sie sehen die Anfänge in der Entschlüsselung der Enigma-Chiffriermaschinen, die vom deutschen Militär im Zweiten Weltkrieg für die Verschlüsselung des Nachrichtenverkehrs eingesetzt wurden. Ein Team von Fachleuten um den be-

Abb. 1: Auswahl an Titelbildern zum Thema Cyberkrieg

rühmten britischen Mathematiker Alan Turing in Blechley Park hat das mit Hilfe von Vorläufern heutiger Computer geschafft, was nicht ohne Einfluss auf den Kriegsverlauf blieb.

Die Bemühungen um Entschlüsselung des Funkverkehrs führten bereits damals zur Gründung der National Security Agency (NSA) in den USA und des Government Communication Headquarters (GCHQ) in Großbritannien, die beide bis heute eine entscheidende Rolle als Akteure des Cyberkriegs spielen. Einen ersten Höhepunkt des „Information Warefare“ war dann der Aufbau von C3I-Systemen (Control, Command, Communication, Intelligence) im Kalten Krieg in den USA, durch die die Kriegführungsebene auf Informations- und Kommunikationstechnik abgestützt wurde. Seitdem dazugekommen sind vor allem die Fähigkeiten, in gegnerische Systeme durch Hacking gezielt einzudringen, sie zu manipulieren und sie zu zerstören.

Auf der begrifflichen Seite muss beachtet werden, dass alle Varianten wie Cyberkrieg, Informationskrieg, Krieg im Informationsraum oder Krieg im Cyber- und Informationsraum den gemeinten Sachverhalt nur sehr bedingt treffen. So ist „cyber“, das vom Altgriechischen „ steuern und navigieren“ stammt, zu eng und als Synonym für „Computer- und Internet-gestützt“ zu nebulös. So ist „Information“ zu statisch, und der „Informationsraum“ ist überhaupt gar kein „Raum“, sondern ein riesiges Netz aus Computern und computergesteuerte Geräten, Anlagen, Maschinen etc. Tatsächlich geht es um programmierte, von Algorithmen getriebene Kriegsführung. Ich verwende den Begriff Cyberkrieg dennoch auch weiterhin, weil er inzwischen so etabliert ist, dass mit jeder anderen Bezeichnung Verständnisschwierigkeiten entstehen könnten.

WELTWEITES CYBERWETTRÜSTEN

Dass das als Cyberkrieg bezeichnete Phänomen ernst genommen werden muss und eine eklatante neue Bedrohung darstellt, ergibt sich aus der Tatsache der weltweiten gigantischen Aufrüstung in diesem Bereich. Mehr als 100 Staaten haben Cyberkriegseinheiten gebildet, die zudem überwiegend offensiv ausgerichtet sind. Die USA betreibt mit der NSA und dem United States Cyber Command (USCYBERCOM) die größte Einheit. China hat die „Blaue Armee“, eine Hackereinheit, die offiziell rein defensiv ausgerichtet ist. Russland wird verdächtigt, wiederholt offensiv Cyberangriffe zu betreiben oder zu unterstützen, was allerdings wohl nicht wirklich bewiesen ist. Der Iran brüstet sich damit, die weltweit zweitgrößte Einheit zu haben. Israel hat die Cyber Defense Taskforce, Großbritannien die Government Communication Headquarters (GCHQ) und so weiter und so weiter.

Auch Deutschland steht da nicht zurück, selbst wenn die Regierung erst spät systematisch auf die weltweite Entwicklung reagiert hat. Seit 2011 existiert der Nationale Cyber-Sicherheitsrat, der beim Beauftragten der Bundesregierung für Informationstechnik angegliedert ist. Im sel-

ben Jahr nahm das Nationale Cyberabwehrzentrum seine Arbeit auf, in dem die Cyberaktivitäten des Bundesamts für Sicherheit in der Informationstechnik (BSI), des Bundesamts für Verfassungsschutz und des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe koordiniert werden. Assoziierte Mitglieder sind das Bundeskriminalamt, der Bundesnachrichtendienst, die Bundespolizei, die Bundeswehr mit dem Militärischen Abschirmdienst sowie das Zollkriminalamt. Außerdem haben das BSI und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. 2012 die Allianz für Cybersicherheit geschmiedet. Die Strukturen dieser Einrichtungen sind allerdings eher intransparent und ihre Kontrolle ziemlich unklar.

Die Bundeswehr steht nicht abseits. Seit 2016 baut sie einen Organisationsbereich Cyber- und Informationsraum (CIR) mit rund 13.500 Dienstposten auf. Das Kommando CIR, die Führungsebene des Bereichs, wurde am 5. April 2017 offiziell durch die Verteidigungsministerin in Dienst gestellt. Es bildet ein Dach über Abteilungen, die vorher über viele Bereiche der Bundeswehr verteilt waren; insbesondere sind ihm das Kommando Strategische Aufklärung, das Kommando Informationstechnik der Bundeswehr (ehemals Führungsunterstützungskommando der Bundeswehr) und das Zentrum für Geoinformationswesen der Bundeswehr unterstellt. Aufgaben wie die Erstellung von Lageplänen, Weiterentwicklung, Ausbildung, nationale und internationale Zusammenarbeit im Cyber- und Informationsraum sowie die Informationssicherheit in der Bundeswehr liegen damit in einer Hand. Soweit ist das erst einmal unspektakulär. Aber der Organisationsbereich CIR bringt auch einige äußerst bedenkliche Entwicklungen mit sich. So hat die Bundeswehr neben Heer, Marine und Luftwaffe eine weitere Teilstreitkraft gebildet, was auch weltweit betrachtet eine neue Qualität darstellt. Defensive und offensive Cyberkriegsfähigkeiten sollen massiv ausgebaut werden. Dazu führt die Bundeswehr eine millionenschwere Werbekampagne zur Personalgewinnung durch und hat an der Universität der Bundeswehr München einen Masterstudiengang IT-Sicherheit eröffnet, dessen personelle Ausstattung jede zivile Hochschuleinrichtung vor Neid erblassen lässt.

... AUS MILITÄRISCHER SICHT

Cyberkrieg gilt als militärisch attraktiv, weil bei einem Angriff keine eigenen SoldatInnen direkt gefährdet sind, weil die Rückverfolgung schwierig und teilweise unmöglich ist, so dass der Angegriffene gar nicht weiß, wer angreift. Der Angriff auf meist zivile Ziele kann den Gegner empfindlich schwächen, während Cyberwaffen vergleichsweise billig zu haben sind. Die mangelhafte Rückverfolgung und Zuordnung von Cyberangriffen begünstigt Attacken auch unterhalb der Kriegsschwelle als „Nadelstiche“ oder Versuchsballon. Die Vorteile gelten allerdings nur für die Angreifer, für die Angegriffenen verkehren sie sich ins Gegenteil. Aber auch die Vorteile sind eher scheinbar und in vielfältiger Hinsicht eigentlich Nachteile. Weil zum Beispiel Cyberwaffen relativ leicht zu beschaffen oder zu entwickeln sind, können viele Staaten und auch größere Terrorgruppen sich das leisten, so dass die eigene Gefährdung wächst. Zudem ist das Angreifen mit Cyberwaffen wesentlich einfacher als das Verteidigen, weil dafür die Instrumente bekannt sind und man nur ein paar gute Computer und ein Team von Hackern braucht, die wissen, wie man die unzähligen Schwachstellen und Sicherheitslücken für die Installation von Schadsoftware nutzen kann. Cyberabwehr dagegen ist bei massiven und komplexen Angriffen technisch viel schwieriger und nur unzureichend beherrscht.

Dennoch wird Cyberrüstung von Politik und Militär für nötig erachtet mit der Begründung, dass alle im Cyberbereich rüsten, so dass man selbst nicht abseits stehen könne. Die Konsequenz ist eine gigantische weltweite Cyberrüstungsspirale, die insbesondere von den USA mit ungeheuren Geld- und Personalmitteln angetrieben wird. In ihrer Strategie für Operationen im Cyberspace (Strategy for Operating in Cyberspace) wird das damit begründet, dass die USA in diesem Bereich bei gleichzeitiger hoher Abhängigkeit von funktionierender Informationstechnik und hoher Verletzlichkeit durch Vernetzung, Zentralisierung, Standardisierung und Mobilität angreifbar und in der Defensive schwach wären. Man findet dort eine weit gefasste Definition eines Cyber-Angriffs: Denial-of-Service-Attacken, Sabotage von militärischen und zivilen Systemen (insbesondere von kritischen Infrastrukturen), Manipulation von Informationen, Wirtschaftsspionage und Diebstahl geistigen Eigentums. Hacktivismus, Cyberkriminalität und Cyberkriegführung werden undifferenziert als Bedrohungen der nationalen Sicherheit angesehen. Die Eintrittsschwelle für Gegenangriffe wird in diesem Strategiepapier sehr niedrig angesetzt, wobei ausdrücklich auch konventionelle Gegenschläge vorgesehen sind. Auch wenn dieser Vorbehalt bisher wohl nicht zur Anwendung gekommen ist, klingt er doch ziemlich besorgniserregend. Was auch Deutschland und die anderen NATO-Partner der USA in diesem Zusammenhang betrifft, ist die Frage, ob die USA im Falle eines Cyberangriffs den Bündnisfall ausrufen und so die ganze NATO in einen (Cyber-)Krieg hineinziehen können.

An einer anderen Stelle beschäftigt sich die NATO bereits mit einem wichtigen Aspekt der Cyberkriegsführung. Zwischen 2009 und 2012 wurde von einer internationalen Gruppe mit rund 20 Fachleuten am NATO Cooperative Cyber Defence Centre of Excellence in Tallinn eine rechtlich nicht bindende Studie erarbeitet, wie sich das Kriegsvölkerrecht (vor allem die Genfer Konventionen) auf Cyber-Konflikte und Cyberkrieg anwenden lässt. 2013 erschien Teil 1 des daraus hervorgegangenen Tallinn-Manuals bei Cambridge University Press. Der Fokus des ersten Teils liegt auf den massivsten Cyber-Operationen, die während bewaffneter Konflikte durchgeführt werden oder das Verbot von Gewalteinsatz in internationalen Beziehungen verletzen. Darin sind 95 Regeln zur Interpretation

einzelner Bestimmungen des Kriegsvölkerrechts hinsichtlich des Cyberkriegs aufgestellt worden. 2017 ist auch Teil 2 erschienen, in dem niederschwelligere Cyberangriffe behandelt werden.

CYBERPEACE

Ohne auf die Details einzugehen, sei daran erinnert, dass die Genfer Konventionen von Kriegsparteien verlangen, Opfer, Wehrlose und Unbeteiligte zu schützen, wobei insbesondere Angriffe auf Zivilpersonen verboten sind. Außerdem sollen zivile Einrichtungen und Kulturgüter verschont werden. Schon allein daraus ergibt sich, dass die außerordentliche Bedrohung von zivilen Infrastrukturen durch die Cyberkriegsrüstung völkerrechtlich inakzeptabel ist. Darüber hinaus sei auch angemerkt, dass die Charta der Vereinten Nationen, der fast alle Staaten der Welt zugestimmt haben, Krieg verbietet. In der Präambel heißt es dazu: „... fest entschlossen, künftige Geschlechter vor der Geißel des Krieges zu bewahren...“, und im Artikel 2 des ersten Kapitels steht: „Alle Mitglieder legen ihre internationalen Streitigkeiten durch friedliche Mittel so bei, dass der Weltfriede, die internationale Sicherheit und die Gerechtigkeit nicht gefährdet werden“. Im Grundsatz ist also Cyberkrieg wie auch Krieg ganz allgemein verboten.

Aus all diesen Fakten, Problemen, Vorkommnissen und allseitigen Bedrohungen wären die einzig richtigen Konsequenzen Cyberabrüstung und ein Verbot von Cyberwaffen, zumindest den offensiven. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) führt seit einigen Jahren eine Cyyberpeace-Kampagne durch, deren Ziel ein Gegenkonzept zum Cyberkrieg ist.

Angestrebt ist die Ächtung jeglicher Form von Cyberwaffen (zumindest von offensiven). Eine wesentliche Voraussetzung auf dem Weg dahin wäre ein demokratisch gestaltetes, demokratisch kontrolliertes und entmilitarisiertes Internet, das dem Frieden und nicht der Ausspähung sowie der Unterstützung militärischer Aktivitäten dient. Völlig utopisch ist das Ziel nicht, denn es gibt auf der Ebene de Vereinten Nationen ExpertInnen-Gespräche mit dem Ziel eines Cyberwaffen-Verbots oder wenigstens einer Regulierung. Aber auch auf nationaler Ebene lässt sich etwas tun. So könnte sich die Bundeswehr anders als momentan auf reine Cyberabwehr und dabei nur auf die Sicherheit ihrer eigenen Systeme beschränken. Außerdem könnte gesetzlich geregelt werden, dass alle im zivilen und militärischen Bereich entdeckten Sicherheitslücken und Schwachstellen in IT-Systemen aufgedeckt und beseitigt werden müssen, statt sie für den eigenen offensiven Gebrauch zu erwerben, zu nutzen und geheim zu halten.

cyberpeace

eine Kampagne des FIfF

Mehr zum Thema Cyberpeace findet man auf der Webseite https://cyberpeace.fiff.de.

Neben dem bereits genannten Dossier 74 der Zeitschrift Wissenschaft und Frieden möchte ich auf folgende Publikationen als weiterführende Literatur verweisen:

*Stefan Hügel, Hans-Jörg Kreowski und Dietrich Meyer-Ebrecht: Cyberwar and Cyberpeace. In: Handbook of Cyber-Democracy, Cyber-Development and Cyber-Defense, Springer, 2017, 25 Seiten.
*Sylvia Johnigk, Hans-Jörg Kreowski und Kai Nothdurft: Cyberwar – Schimäre oder reale Bedrohung?, FIfF-Kommunikation 4/2014, Seiten 74-77.
*Hans–Jörg Kreowski und Dietrich Meyer–Ebrecht: „Revolution in Military Affairs“. In: The Future Information Society, World Scientific Series in Information Studies, Band 8, 2017, Seiten 439-448.
*Dietrich Meyer-Ebrecht (Hg.): Kriegführung im Cyberspace, Dossier 79 in Wissenschaft und Frieden 3/2015 und FIfF-Kommunikation 3/2015.

Ganz besonders möchte ich schließlich das 5-minütige Video von Alexander Lehmann: Cyberpeace statt Cyberwar, aus dem Jahre 2017 empfehlen, das mit Unterstützung des FIfF entstanden ist und sowohl sehr anschaulich in das Thema Cyberkrieg einführt als auch die Grundidee von Cyberpeace vermittelt (https://vimeo.com/216584485, https://www.youtube.com/watch?v=St955HBD-7k).

BATTLE MANAGEMENT LANGUAGE.
SPRACHLOSE MYTHEN MILITÄRISCHER STRUKTUREN

VON: FRANZ WANNER

„Battle Management Language“ ist eine militärische Sprache zur Kommunikation von und mit autonomen Systemen. Das US-Militär begann 2001 mit ihrer Entwicklung. 2006 gründete sich die NATO-Forschungsgruppe „Battle Management Language“, zu der auch Deutschland gehört. Innerhalb Deutschlands wird sie vor allem am Fraunhofer-Institut in Wachtberg gepflegt. Dort erschien 2008 eine Veröffentlichung mit dem Titel „Entwurf einer Battle Management Language Bundeswehr“. Das Besondere dieser Sprache besteht in ihrer Behauptung, keine Mehrdeutigkeiten zu kennen und frei von Widersprüchen zu sein – ein linguistisches Wunder. Die Methode der „Battle Management Language“, Mehrdeutigkeit zu leugnen und Widersprüche zu ignorieren, ließe sich auf andere Bereiche erweitern: Wie schafft es eine Gesellschaft, sich selbst als liberale Demokratie zu erleben und gleichzeitig einen expansiven Militarismus zu betreiben, der Bindungen an eine Rechtsstaatlichkeit auflöst und das soziale Leben durchdringt? Um konstitutiven Brüchen wie diesem aus dem Weg zu gehen, sind ein Management und eine Verwendung von Sprache notwendig, die mehr mit Verschleierung zu tun haben, als mit der Absicht zu kommunizieren.

Information wird oft als wichtigste Ressource der Gegenwart beschrieben. Im Besonderen gilt das für den militärischen Bereich, der in der netzwerkorientierten Kriegführung den entscheidenden Vorteil gegenüber dem Feind in der Verarbeitung einer maximalen Informationsdichte in Echtzeit sieht.

Singapore Aerospace Manufacturing, Muttergesellschaft von Sitec Aerospace.
Still aus „DUAL-USE I: Global Cocktail“, 2016.

„Information ist Aberglaube“ sagte der Wiener Künstler und Aktivist Konrad Becker neulich in einem Vortrag und zitierte damit Peter Lamborn Wilson: „Information ist ein Ersatz für Gewissheit, ein übrig gebliebener Fetisch des Dogmatismus, ein Aberglaube, ein Gespenst“ („Information is a substitute for certainty, a leftover fetish of dogmatics, a super-stition, a spook”). Wilson beschreibt die Information nicht als Ressource, sondern als Aberglauben unserer Zeit. Hinter dem zeitgenössischen Zwang zum permanenten Informationskonsum vermutet er eine Angst; möglicherweise vor einer Stille. Die Sprachlosigkeit im Titel meines Beitrags bezieht sich nicht auf ein Schweigen, sondern auf eine Verwendung von Sprache, die weniger der Klärung und dem Austausch dient, als zugunsten bestimmter Techniken der Mythologisierung eine begriffliche Diffusion zu befördern. Dieses Verhindern von Lesbarkeit und Transparenz betrifft nicht nur begriffliche Sprache, sondern auch Bildsprache und andere kulturelle Texte.

Vor drei Jahren rief mich der Geschäftsführer der Rüstungsfirma Sitec Aerospace an. Am Telefon beschwerte er sich darüber, dass ich sein Unternehmen in einem Fernsehbeitrag als Rüstungsfirma bezeichnet hatte. Er warnte mich und erklärte, mit dieser Benennung würde ich ein hohes Risiko eingehen. Dadurch könne provoziert werden, dass ein Molotowcocktail durch die Scheibe seiner Produktionshalle fliege und zweihundert Familien wären vernichtet. Diese Beschreibung wirkte wie ein harter Schnitt, ein Cross-cut in eine andere Realität, hinein in ein Kampfgeschehen – vielleicht dorthin, wo die Produkte seiner Firma eingesetzt werden. Um das Risiko zu minimieren, sei der korrekte Begriff

für seine Branche nicht Rüstung, sondern „Dual-Use“. Ich schlug ihm vor, seinen Betrieb zu besuchen, um ihm die Möglichkeit zu geben, seine Vorstellung von Realitätsproduktion vor laufender Kamera offen zu legen. Darauf hat er sich eingelassen. So entstand der Film „Global Cocktail“.

Zu Bild 1: Sitec Aerospace wurde als Zulieferer für die Produktion des Kampfflugzeugs Tornado gegründet. Das Unternehmen wird von der Singapore Aerospace Manufacturing getragen und untersteht Temasek Holdings, die mit einem Portfolio von 150 Milliarden US-Dollar eine hohe Planungssicherheit bietet. Das steinzeitliche Arrangement am Firmeneingang entstand auf Anordnung des Geschäftsführers, um die Nähe seiner Produktionszusammenhänge zu Stonehenge zu untermauern. Seine Partnerfirma AgustaWestland produziert Kampfhubschrauber in Südengland. Im Sinne guter Geschäftsbeziehungen beauftragte er einen Dorfkünstler damit, den Mythos der Steinzeit nach Bayern zu transferieren. AgustaWestland wurde übernommen und ist in einem Konzern aufgegangen, der sich seit 2017 „Leonardo“ nennt – nach Leonardo da Vinci. Diese Anleihen lassen sich als Versuche deuten, die Banalität des Waffenhandels durch kulturelle Fassaden aufzuwerten. Die Strategie mag primitiv erscheinen. Sie ist aber nicht primitiv genug, als dass die lokale Presse nicht doch über das Stonehenge-Kunstwerk schreiben würde, anstatt über Militarisierungsprozesse. Seit der Gründung des Standorts vor neun Jahren wurde in der lokalen Berichterstattung der Begriff „Rüstungsindustrie“ nicht verwendet. Damit konfrontiert, erklärten die Redaktionen, man schreibe nicht schlecht über eine Firma, die der Gegend Aufschwung bringe. Christopher Schwitanski behandelt in seinem Beitrag die 200 ElitejournalistInnen, die exklusive Kurzschlüsse mit der Wirtschaft und der Nato bilden und zu den medialen Hauptverteilern gehören. Die Mitglieder der Lokalredaktionen zählen vermutlich nicht zu dieser so genannten Elite, deren Berufung es ist, sich in Wirtschaftsinteressen aufzulösen. Dennoch unterscheidet sich ihre Sprache nicht von der einer Dual-Use Imagebroschüre.

Zu Bild 2: Das Dispositiv der Drohne teilt den globalen Raum in zwei Bereiche: Die gesicherte Heimat und das feindliche Gebiet, das unter ständiger Beobachtung steht und als flexible Kampfzone nonlinear und feindzentriert verschoben wird. Die Ausführenden des staatlichen Vorsorgeterrorismus verüben durch bewaffnete Fernlenkvideos vom Büro aus Hinrichtungen aus der Luft. Die Tätigkeit lässt sie körperlich unverletzt, kann aber existenzielle Zweifel an ihrer Berufswahl auslösen. Im Gegensatz dazu sind autonome Systeme frei von Identität und funktionieren zweifellos.

Zu Bild 3 und 4: Die Installation DUAL-USE war 2016 im Lenbachhaus in München zu sehen. Sie besteht aus vier Videos, von denen jedes eine Hauptfigur zeigt. Die Tätigkeiten der ProtagonistInnen, die direkt oder indirekt mit der Herstellung oder dem Einsatz von Rüstungstechnologie zu tun haben, werden jeweils durch ein spezifisches Störgeräusch unterlaufen. Am Beispiel der US-Drohnenpilotin, die gleichzeitig als Model arbeitet, lässt sich dies beispielhaft verdeutlichen: Der Film über diese Frau ist auditiv und visuell mit einem Regeneffekt belegt, denn bei Niederschlag lassen sich weder der Strike noch das Shooting erfolgreich durchführen. Jedes der Videos enthält ein Störelement, das sich auf ähnliche Weise zu seiner Hauptfigur und ihrer homogenisierten Weltsicht verhält, wie der Regen zum Kampf-Modell. Ein Chemieprofessor sitzt im Explosionswind, während er seinen Rüstungsauftrag im deutschen Bildungssystem verteidigt. Der Geschäftsführer von Sitec Aerospace ist von Knallgeräuschen seiner eigenen Produkte irritiert. Eine Entwicklerin humanoider Roboter begegnet deren Potentialen zwischen Krieg und Kinderzimmer. Zusammen mit dem Informatiker Nando Schneider habe ich für die Installation eine Programmierung entwickelt, die in Echtzeit jedem der Videos das jeweilige Geräusch entnimmt. Auf Wahrscheinlichkeiten basierend kombiniert die Programmierung die Tonstücke in Bezug auf Lautstärke, Dauer und Gleichzeitigkeit und gibt sie im Raum wieder. Die ökonomisierten Ambitionen der Akteure lassen eine Art Dual-Use-Ambient entstehen. Das Grundrauschen der Weltverzweiflungsmaschine durchdringt den Raum wie ein kontinuierliches Störgeräusch, das unsere militarisierte Massenkultur permanent produziert und deshalb nicht mehr wahrnimmt. Der Programmcode, der dem Schallgebilde zugrunde liegt, läuft als großflächig projizierter Zeichenstrom unablässig über die Rückwand des Ausstellungsraums.

Neben den Videos und dem Code ist als Teil der Installation eine Publikation entstanden. Das Heft beschreibt in kurzen Texten die Produktionszusammenhänge, in denen sich die vier ProtagonistInnen bewegen. Eine Passage behandelt den Ludwig-Bölkow-Campus in München. Dort wird auf der Basis von ehemaliger NS-Rüstungsforschung ein Hightech-Standort betrieben, der Hochschulen integriert und militärische Technologien erforscht – auch Drohnen werden dort entwickelt. Die Installation DUAL-USE bewirkte eine parlamentarische Anfrage an die Bayerische Staatsregierung über diesen Campus. Die Prozedur einer Anfrage und ihrer Regierungsantwort sind ein eingespielter Mechanismus. Die Anfrage wird im Bewusstsein gestellt, ausweichende und faktisch unrichtige Antworten zu erhalten. Die Antworten treffen erwartungsgemäß formal korrekt und inhaltlich falsch ein. Diese nicht kommunikative Rhetorik gab den Impuls für meinen Film „From Camp to Campus“ über den Ludwig-Bölkow-Campus.

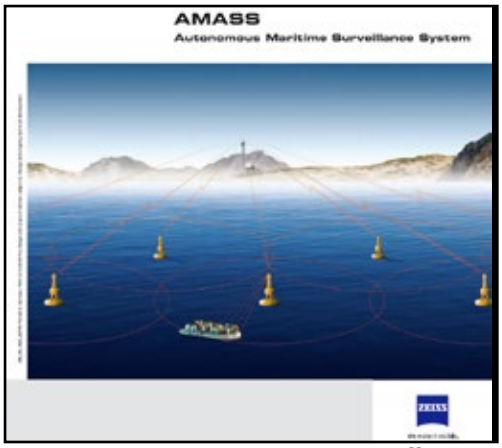
Um im Jahr 2013 bei der Benennung eines Campus den Namen eines NS-Ingenieurs zu wählen und sich gleichzeitig als Demokratie zu verstehen, ist ein hohes Maß an sprachlichem Battle Management notwendig. Dieser Herausforderung begegnet man durch verkürzte Bildungswege. Damit der Nachwuchs sich spätestens während des Studiums assimiliert, sind am Ludwig-Bölkow-Campus neben Firmen wie Airbus und Siemens auch die TU München, die Universität der Bundeswehr und die Hochschule München integriert. In dieser Konstellation wird auf dem Areal eine militärische Drohne entwickelt, die nach der griechischen Gottheit für Westwind benannt ist: Zephyr. Sie wird als erfolgreiches Hightech-Produkt beworben und an mehrere Armeen geliefert. Gleichzeitig informiert die Staatsregierung die Öffentlichkeit darüber, dass am Ludwig-Bölkow-Campus weder Drohnen noch Rüstungsprojekte existieren. Beide Angaben sind offiziell. Man findet sie auf der selben Website der Bayerischen Staatsregierung unter verschiedenen Links. Ich vermute, dass die beiden widersprüchlichen Informationen zwei entgegengesetzte Ansprüche eines Selbstverständnisses bedienen: Zum einen das bedingungslose ökonomische Wachstum, das militärisch gesichert und nicht verhandelbar ist. Zum anderen etwas wie eine Restmoral, die oft religiös pervertiert ist und vielleicht entfernt daran erinnert, dass es nicht das Beste sein kann, sein Leben auf Waffenhandel und Ausbeutungsmechanismen zu gründen. Beide Angaben koexistieren und lösen mehrheitlich keine Zweifel oder Widerstände aus, sondern befördern eine kollektive mentale Gespaltenheit, die es gerade erst ermöglicht, diesen Widerspruch als normal zu empfinden. Ein homogenisiertes Weltbild wird dadurch aufrechterhalten.

Zu Bild 5: Was heute Ludwig-Bölkow-Campus heißt, basiert auf der NS-Luftfahrtforschungsanstalt, für deren Bau zwei Zwangsarbeiterlager eingerichtet wurden. Die Grundmauern eines der beiden Arbeitslager liegen in Sichtweite des heutigen Campus. Ein Bachelorprogramm bildet die Studierenden dort zu Kampfpiloten aus. Zur Geschichte des Orts schreibt die Bayerische Staatsregierung 2016, diese sei nicht Inhalt der Forschungs- und Lehrtätigkeit. Die Broschüre des so genannten „Innovationscampus“ bewirbt fünf deutschlandweit einzigartige Studiengänge wie den „Master of autonomous Systems“, die tatsächlich gar nicht existieren und beschreibt die Arbeit am Campus als „Innovationsführerschaft“ und „traditionsreichste Hochtechnologie“. Die Konzentration auf technische und ökonomische Aspekte unter Vermeidung historischer, sozialer und kultureller Zusammenhänge führt zum objektorientierten Weltmodell:

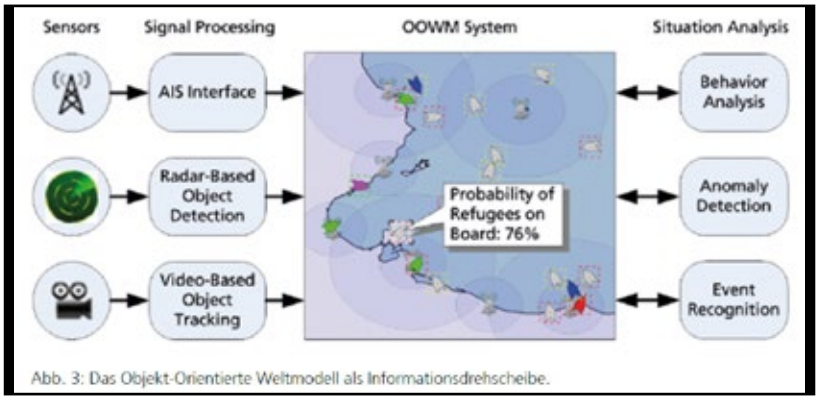
Die EU blockiert ihre Grenzen auf drei Niveaus. Ein Netz autonomer Sensorbojen erkennt Flüchtlingsboote vom Wasser aus, Drohnen überwachen das Mittelmeer aus der Luft und Satelliten leisten Fernaufklärung aus dem All. Ein Schaubild versieht Objekte mit Symbolen für detektierte Boote. Der Algorithmus sagt: „Wahrscheinlichkeit für Flüchtlinge an Bord: 76%“ („Probability of Refugees on Board: 76%“). Der Bereich für Wehrtechnik der Firma Carl Zeiss, der die optronische Präzision liefert, ist seit 2014 in Airbus integriert. Das Fraunhofer-Institut nutzt das All, den Luftraum und das Meer als Überwachungsschichten und fusioniert die Daten zum „Objektorientierten Weltmodell.“

Zu Bild 6: Eine Objektschutzstreife schützt die Mauer, die Münchner vor der Anwesenheit von Flüchtlingen schützen soll. Die abgelehnten Asylsuchenden aus Afghanistan, Mali und dem Kosovo werden in Einsatzgebiete der Bundeswehr zurückgeschickt. Ihre Heimatstaaten sind sicher genug, um sie dorthin abzuschieben, aber zu unsicher, um die deutsche Armee von dort abzuziehen. Mehrheitlich stellt man sich diese Regionen als Krisengebiete und gleichzeitig als ungefährliche Herkunftsländer vor.

Das Objektorientierten Weltmodell beschreibt die Flüchtlingsabwehr mit militärischen Mitteln. Die Publikation „visIT – Zivile Sicherheit“ des Fraunhofer IOSB vom Dezember 2012 interpretiert den Begriff der Immigration, indem sie sie als „illegal“ bezeichnet. Die Broschüre stellt Technologien vor, mit deren Hilfe diese „illegale Immigration“ abzuwehren sei. Das Fraunhofer-Institut unternimmt in einem Technikheft den Versuch, die Definitionsmacht essentieller gesellschaftlicher Begriffe für sich zu beanspruchen und die Immigration zu illegalisieren.



AMASS Autonomous Maritime Surveillance System, publica.fraunhofer.de (Abrufdatum: 18.11.2017).



„visIT – Zivile Sicherheit“, Broschüre des Fraunhofer IOSB, Dezember 2012.

Bild 1: Die Firma Sitec Aerospace sitzt seit 2007 in Bad Tölz.

Bild 2: Battle Management Drawing: Die Firma Sitec Aerospace aus der Drohnenperspektive.

Bild 3: Still aus DUAL-USE III - Kampfmodel, 2016.

Bild 4: Installation DUAL-USE, Lenbachhaus München, 2016.

Bild 5: Die Fundamente des NS-Arbeitslagers in München-Ottobrunn als Basis des Ludwig-Bölkow-Campus. Still aus „From Camp to Campus“, 2018.

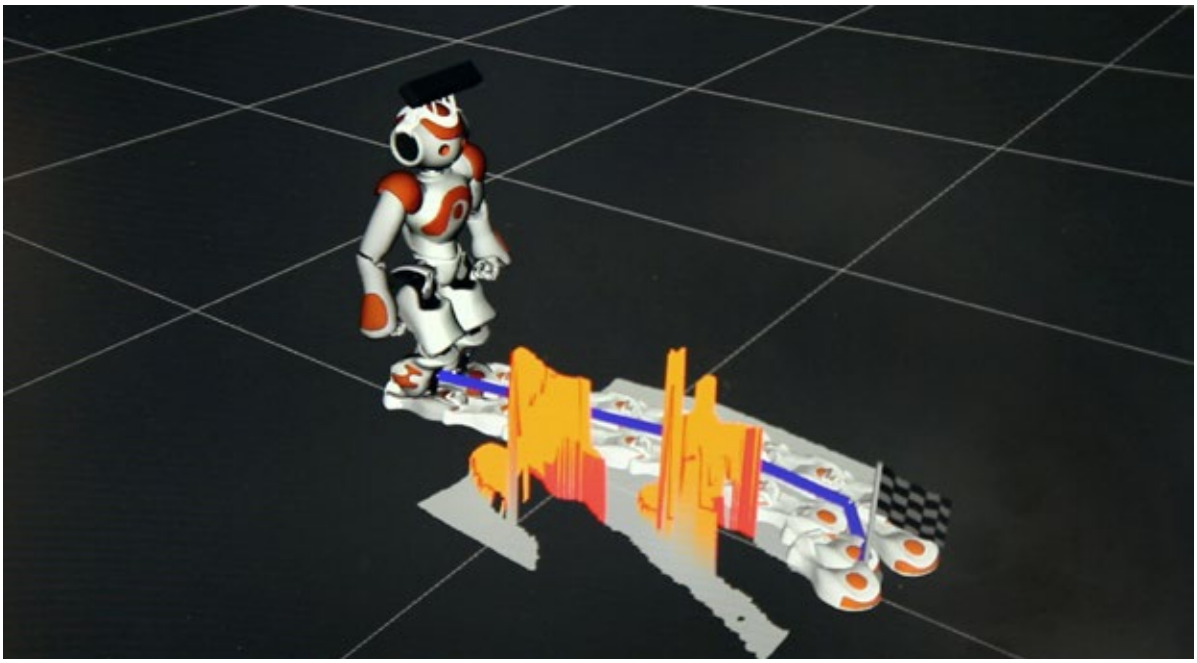
Bild 6: Battle Management Drawing – Schutzobjekt Objektschutz.

Bild 7: Battle Management Drawing – Das Radom des Fraunhofer FKIE in Wachtberg bei Bonn.

Bild 8: Battle Management Drawing – Das Radom in Wachtberg, im Vordergrund Lars (Lethal Autonomous Robots).

Das Karlsruher Institut für Technologie gibt Einblicke in Entscheidungsprozesse in Bezug auf die Verwendung von Bildern. Dort war ich 2016 mit einem Filmteam, um eine militärische Drohne aufzunehmen. Auf der Website des KIT wird sie als intelligent und autonom bezeichnet. Zu den Kooperationspartnern der Hochschule zählen Rüstungsunternehmen wie Airbus und Diehl. Meine Anfrage, im KIT einen Film zu drehen, beantwortete der Leiter des Drohnenprojekts, der vor seiner Lehrtätigkeit bei EADS tätig war, mit Interesse und erklärte sich und seine Forschungsgruppe zu filmischen Aufnahmen bereit. In Vorgesprächen äußerten die Wissenschaftler, eine Win-Win-Situation herzustellen, indem sie meine Filmaufnahmen für Imagezwecke nutzen möchten. Diese Vorstellung teilte ich nicht, stellte aber ein Bild in Aussicht, auf dem die Drohne gut getroffen ist. Vor laufender Kamera führten sie das Fluggerät vor, das sie zu selbstständigen Entscheidungen befähigen wollen. Es soll in der Lage sein, sich autonom, also ohne Fernsteuerung, durch Fenster und Türen in Innenräume zu navigieren und dort missionsorientierte Aufgaben durchzuführen. Das Interview mit zwei Entwicklern des Drohnenteams drehte sich um die Frage, ob „situationsbewusste“ Maschinen, die hohe Potenziale und Gefahren bergen, von situationsbewussten Forschern betreut werden sollten, die einen interdisziplinäre Austausch pflegen und philosophische wie soziale Aspekte in ihre Arbeit einbeziehen.

Zwei Tage nach dem Dreh erhielt ich eine Email von einem KIT-Mitarbeiter, der stellvertretend für das Institut das Einverständnis für die Aufnahmen nachträglich zurücknahm. Falls Bilder oder Zitate des Drehs an die Öffentlichkeit gelangen, müsse ich mit rechtlichen Folgen rechnen. Tatsächlich verwies das KIT damit auf das Recht am eigenen Abbild seiner Mitarbeiter und entzog einer Veröffentlichung die rechtliche Basis. Woran liegt es, dass die Nutzung von Bildern in Deutschland einfach und wirksam eingeschränkt werden kann, während militärische Forschung scheinbar nicht reglementierbar ist und Rüstungsgüter auf armierten Handelswegen frei flottieren? An das Verbot, die Bilder nicht zu veröffentlichen, habe ich mich gehalten – bis heute. Hat auch eine Drohne ein Persönlichkeitsrecht und Anspruch auf ihr eigenes Abbild, wenn man ihr Eigenschaften wie Autonomie, Situationsbewusstsein, Entscheidungsfähigkeit und Intelligenz zuspricht?



Still aus „DUAL-USE IV: Or do we have the same?“, 2016.

Zu Bild 7: Über die Vorgänge im Inneren des Radoms dringt wenig nach außen. Unter den Anwohnern in Wachtberg kursieren Gerüchte, die Militärforscher auf dem umzäunten Gelände unterhielten sich in Battle Management Language. Das Fraunhofer-Institut, das die Riesenkugel betreibt, entwickelt die „kontrollierte Sprache ohne Mehrdeutigkeiten“, um unbemannten Systemen Befehle zu erteilen.

Zu Bild 8: Ein mobiler Roboter registriert in einem gemeinsamen Projekt des Fraunhofer-Instituts und der Universität Bonn die Haut- und Haarfarbe von Menschen, um Individuen selbständig zu erkennen und zu verfolgen. Die Bewaffnung autonomer Systeme in Deutschland sei unumgänglich, besagt eine Studie des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag. Maschinen erweisen sich als fähig, eigenständig Waffen zu betätigen. Die Frage, ob sich Menschen als fähig erweisen, sich nicht wie Maschinen betätigen zu lassen, beantwortet Lars, der als unbewaffneter Rasenmäher in Wachtberg arbeitet, mit autonomen Battle Management Drawings.

DIE HYBRIDITÄT UND TERRITORIALITÄT DES INFORMATIONSRAUMS DER BUNDESWEHR

VON: CHRISTOPH MARISCHKA

Während manche militärische Angelegenheiten auf den ersten Blick transparenter behandelt werden, als man annehmen würde, stellen die Kommunikationsstrukturen der Bundeswehr einen Gegenstand dar, bei dem man sehr schnell auf Geheimhaltung stößt. Trotzdem können auch (nachrichten-)technische Laien – wie der Autor dieses Beitrages – ein annäherndes Verständnis verschiedener Komponenten des militärischen Informationsraumes entwickeln. Hierzu wurde – u.a. wegen der Geheimhaltung aktueller Strukturen – ein historischer und geografischer Zugang gewählt, der auch die Erkundung militärischer Landschaften beinhaltet. Dieser Ansatz erwies sich zumindest insofern als produktiv, als er veranschaulicht, dass es sich bei militärischer Kommunikation bereits historisch um eine hybride, zivil-militärische und staatlich-privatwirtschaftliche Struktur handelt und dass die räumliche Anordnung ihrer Komponenten mit der strategischen Ausrichtung der Streitkräfte in Zusammenhang steht und diese verdeutlichen kann.

Redundanz und das elektromagnetische Spektrum

Zunächst aber müssen wir uns mit jenem ‚Raum' vertraut machen, in dem ein großer Teil der militärischen Informationen zirkuliert: dem elektromagnetischen Spektrum. Dieses umfasst auch jene Frequenzbereiche elektromagnetischer Wellen, über die kommuniziert werden kann. Einen sehr kleinen Teil dieses Spektrums können wir als sichtbares Licht unmittelbar wahrnehmen, wobei uns die unterschiedlichen Frequenzen als verschiedene Farben erscheinen. Ein deutlich größerer Teil des elektromagnetischen Spektrums wird für die Übertragungen von Radiosendern genutzt, die durch einfache Technologie (Demodulation und Verstärkung) für uns hörbar und verständlich werden. Für viele Frequenzbereiche gibt es internationale Abkommen und Normen, in denen z.B. festgelegt wurde, auf welcher Frequenz Notsignale auf hoher See abgesetzt werden sollen. Insgesamt jedoch ist das elektromagnetische Spektrum mittlerweile nationalstaatlich reguliert und die Zuweisung bestimmter Frequenzen für bestimmte Akteure und Zwecke stellt einen zentralen Aspekt moderner staatlicher Souveränität dar. Dazu gehört auch die Fähigkeit, die widerrechtliche Nutzung von Frequenzen zu erkennen und den entsprechenden Sender zu lokalisieren.

Zumindest in den meisten westlichen Staaten wird das große, aber dennoch endliche und zunehmend umkämpfte elektromagnetische Spektrum in hunderte kleiner Frequenzbereiche aufgeteilt, von denen einige von einer zivilen und einige von einer militärischen Behörde (und manche auch gemeinsam) verwaltet werden. Die zivile Behörde ist im Falle Deutschlands die Bundesnetzagentur, die dem Telekommunikationsgesetz entsprechend laufend aktualisiert einen ‚Frequenzplan' veröffentlicht, der diese Bereiche, ihren jeweiligen Zweck und die Bedingungen der Nutzung ausweist. Ein Blick in den aktuellen Frequenzplan legt nahe, dass die Aufteilung in zivile und militärische Verwaltung eher historisch bedingt erscheint, da einige zivil verwaltete Frequenzbereiche ausschließlich oder teilweise militärisch genutzt werden und andersherum. So nutzen z.B. viele WLAN-Netzwerke eine Frequenz, die militärisch verwaltet wird, unter der Bedingung, dass eine gewisse Strahlungsleistung nicht überschritten und „[a]ndere Funkanwendungen [...] insbesondere Satelliten- und Radaranwendungen, nicht gestört werden." Ein anderer militärischer Frequenzbereich hingegen ist alleine für die „Überwachung von Verschiebungen von Bauwerken wie z.B. Dämmen, Brücken, Türmen" durch bodengestützte Radare reserviert, wobei es sich um eine zivile Anwendung handeln dürfte.[1] Wie das Licht, so weisen auch die anderen Frequenzen unterschiedliche Eigenschaften auf, v.a. hinsichtlich ihrer Reichweite bzw. ihres Verhaltens, wenn sie auf Hindernisse treffen.

Hilfreich bei der Auseinandersetzung mit militärischer Infrastruktur insgesamt und dem Informationsraum im Allgemeinen ist darüber hinaus ein Verständnis der angestrebten Redundanz, wie sie sich auch bei der Energieversorgung zeigt. Auch hier nutzen NATO und Bundeswehr gerne zivile Infrastrukturen und lassen sich von LKW über das Straßennetz mit Treibstoff beliefern. Für den Fall, dass dies nicht mehr möglich ist, unterhält die NATO jedoch über eine privatwirtschaftliche GmbH ein Netz von Pipelines und Depots, an das die wichtigsten Luftwaffenstandorte (und zivile Flughäfen) in Deutschland angebunden sind und das von Tankern in den Häfen von Marseille, Le Havre und Rotterdam aus gespeist wird.[2] Auch hier zeigt die Struktur des Netzes, dass eine Bedrohung bzw. ein Angriff von Osten her erwartet wurde. Auch bei der (zivilen) Kommunikation setzt man auf Redundanz: Das eigentliche Rückgrat des Telekom-Netzes ist das Kabelnetz, über das ein Großteil der Informationen fließt, das aber z.B. durch Bauarbeiten immer wieder beschädigt wird. Zwar ist bereits das Kabelnetz selbst auf Redundanz ausgelegt, trotzdem existiert zugleich ein Netz von Richtfunkverbindungen. Richtfunkverbindungen

sind günstiger und flexibler und können auch Orte anbinden, die sonst schwer erreichbar sind, zugleich ist ihre Übertragungskapazität deutlich geringer und kann z.B. durch das Wetter massiv beeinträchtigt werden.

GEHEIME ORTE: DIE GSVBWS

Eine mittlerweile aufgegeben Struktur des militärischen Informationsraumes der Bundeswehr stellen die sog. Grundnetzschalt- und Vermittlungsstellen der Bundeswehr (GSVBw) dar, die ab 1964 errichtet und bis Mitte der 1990er Jahre in Betrieb waren. Zwar hatte die Bundeswehr zunächst erwogen, ein eigenes Fernmeldenetz aufzubauen, dies wäre jedoch finanziell wie personell viel zu aufwendig gewesen. Also wurde auf das Netz aus Kabel- und Richtfunkverbindungen der Deutschen Bundespost gesetzt, das jedoch in mehrerlei Hinsicht den militärischen Anforderungen nicht entsprach: Zentrale Kabeltrassen liefen durch Innenstädte, Industriegebiete und über Brücken, die im Kriegsfalle naheliegende Ziele dargestellt hätten; die Verstärker- und Vermittlungsstellen waren oberirdisch und nicht gegen Waffenwirkung geschützt. Deshalb wurden über 30 Anlagen in Deutschland erbaut, welche sozusagen eine militärische Schnittstelle zum Netz der Bundespost darstellten und den Betrieb der angemieteten Übertragungswege auch im Kriegsfall ermöglichen sollten.

Mit einer Ausnahme waren diese Liegenschaften so konzipiert, dass sie theoretisch einen Angriff mit ABC-Waffen überstehen und für eine Dauer von 28 Tagen autark sein sollten. Vor allem aber sollten ihre Lage und Funktion geheim bleiben. Zusammen mit den militärischen Anforderungen und der Anbindung an das Netz der Bundespost ergaben sich hieraus die Standortkriterien. Die jeweilige GSVBw sollte die Anbindung mehrerer Bundeswehrstandorte an das Netz der Bundespost ermöglichen und dabei möglichst nahe an den Einspeisepunkten der Richtfunkverbindungen liegen. Die Liegenschaften mussten zwar möglichst weit von sonstiger Bebauung, insbesondere solcher mit „hoher Zielwertigkeit“,[3] entfernt sein, aber trotzdem an das Strom- und Verkehrsnetz angebunden sein. Außerdem war ein eigener Zugang zum Grundwasser vorgesehen. Von der Lage und Bebauung her erinnern die Standorte damit an Einsiedlerhöfe, einige hundert Meter von den Verbindungsstraßen kleinerer Orte gelegen. Überirdisch sichtbar waren ein Unterkunftsgebäude in etwa der Größe einer Scheune, ein überdachter Außenbereich, Hundezwinger und ggf. kleinere Lagerräume. Das eigentliche Fernmeldegebäude befand sich unterirdisch, Luftschächte wurden durch Anstrich und Umpflanzung getarnt, die Abgase des Generators über den Schornstein des zivil wirkenden Unterkunftsgebäudes abgeleitet.[4]

Eine solche Anlage für die Militärregion Stuttgart befindet sich mitten in einem Wald nahe dem beschaulichen Ort Waldenbuch im Schönbuch, östlich des Ortsrandes etwa 100 Meter oberhalb der Landstraße 1185 Richtung Nürtingen. Die unscheinbaren oberirdischen Gebäude werden heute von Künstlern genutzt, der militärisch anmutende Zaun ist erhalten. Wann genau die Anlage gebaut wurde, ist unklar, es wird jedoch zwischen 1964 und 1969 gewesen sein. 1969 wurde zwei Kilometer südlich der weithin sichtbare, 143 Meter hohe Fernmeldeturm Waldenbuch auf dem Betzenberg (497 m ü. NN) errichtet. Die zeitliche Abfolge verweist darauf, dass die Bundeswehr nicht nur eine ohnehin vorhandene zivile Struktur nutzte, son-

Die ehemalige GSVBw in einem Wald bei Rottweil wird heute von einem Künstler benutzt, der auf dem Gelände seine Skulpturen aufgestellt hat.

Hinter dem Neubau rechts war der Eingang in den Bunker, links vom Haupttor: das renovierte Unterkunftsgebäude.

Auch die ehemalige GSVBw bei Waldenbuch wird heute von Künstlern genutzt. Hier scheint das ursprüngliche Tor noch in Benutzung...

... ebenso wie der alte Zaun. Der Funkturm in wenigen hundert Metern Entfernung ziert den Umschlag dieser Broschüre.

dern sich die militärische Nutzung auch in die Struktur des Fernmeldenetzes eingeschrieben hat. So wurden über ein ‚Sonderbauprogramm' entsprechende Maßnahmen wie „Kabelumgehungsringe außerhalb von Großstädten und Industriegebieten sowie die Verlegung der Kabeltrassen von verkehrswichtigen Brücken" finanziert. In den jeweiligen Oberpostdirektionen wurden Bereichsfernmeldeführer der Bundeswehr stationiert, deren Aufgabe „die Beratung militärischer Stäbe, Truppen und Dienststellen bei der Inanspruchnahme von fernmeldetechnischen Einrichtungen und Leistungen" umfasste. Auf der anderen Seite wurden innerhalb der streng geheimen GSVBw „Verstärkerstellen (VrSt) der Deutschen Bundespost eingerichtet [...] die auch für die öffentliche Fernsprechkommunikation genutzt wurden. Der Betrieb und die Wartung dieser Anlagen erfolgte durch Mitarbeiter der Deutschen Bundespost."[5]

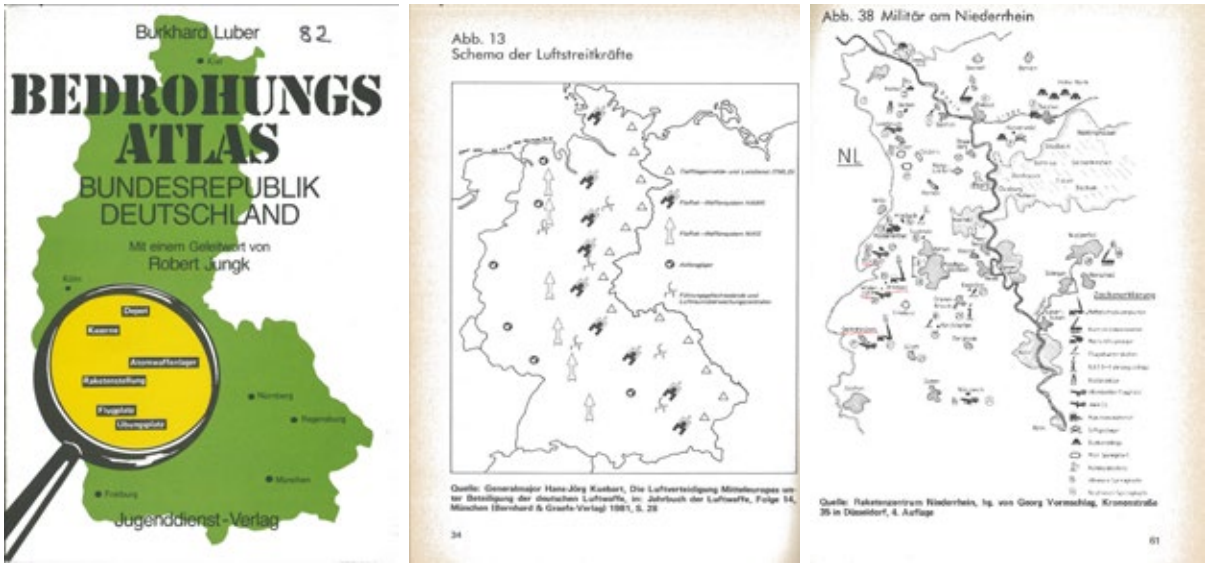
KABEL- UND RICHTFUNKNETZE: TERRITORIALARMEE

Neben der auf das Netz der Bundespost abgestützten Kommunikationsstruktur nutzten und nutzen die Militärs in Deutschland eigene Richtfunknetze und zwar in großer Vielfalt. Die NATO etwa unterhält grenzüberschreitende Netzwerke insbesondere zwischen Frankreich, Belgien und (West-) Deutschland. Auch die in Deutschland stationierte US-Army verfügt über eigene Richtfunknetzwerke. Innerhalb der Bundeswehr hatten Marine, Heer und Luftwaffe jeweils eigene Richtfunknetzwerke aufgebaut, selbst für einzelne Waffensysteme namentlich der Luftabwehr (Patriot, Nike) existierten eigene Netze. Betrieben wurden sie von den jeweiligen Fernmeldetruppen, deren Auftrag als ‚Führungsunterstützung' bezeichnet wird. Viele der engmaschig angelegten, tendenziell abgelegen und erhöht gebauten Sendeanlagen waren bemannt, umfassten also auch Unterkunftsgebäude und Sicherungsanlagen. Nach der Auflösung des Warschauer Paktes wurde die Führungsunterstützung Teil der 2000 geschaffenen Streitkäftebasis und die Fernmeldetruppen der Teilstreitkräfte weitgehend in diese integriert. Viele der Sendeanlagen wurden aufgegeben und häufig in das im Aufbau befindliche Mobilfunknetz privater Anbieter integriert.

Die fast schon chaotisch wirkende Vielfalt an Netzwerken und zugehörigen Truppenteilen spiegelt die strategische Ausrichtung der Bundeswehr als Territorialarmee wieder, die auf einen Angriff aus dem Osten ausgerichtet war. Die Richtfunknetze der Luftwaffe verbanden östlich gelegene Radarstationen mit den nach Westen versetzten Standorten der Flugabwehr, die wiederum Teil eines lokalen Netzwerks von Gefechtsständen und Depots waren. Noch weiter nach Westen versetzt befanden und befinden sich bis heute die Kommandos der Bundeswehr und der NATO. Ein Schema und Karten militärischer Standorte vom Niederrhein aus dem ‚Bedrohungsatlas' von 1983 veranschaulichen die Dichte von Luftwaffenstandorten, die so ihr Netz spannen.

Bei der Luftwaffe war bereits in dieser Konstellation der Inhalt der Kommunikation v.a. technischer Art (Position, Geschwindigkeit) und die Geschwindigkeit entscheidender Faktor, während in jede Entscheidungsstruktur die NATO unmittelbar auf höchster Ebene eingebunden sein musste. Das Netz des Heeres hatte andere Anforderungen (Inhalte, Reaktionszeiten) und weist entsprechend auch eine andere Struktur auf. Die schnelle und reibungslose Kommunikation zwischen den verschiedenen Teilstreitkräften, wie sie heute bei der ‚vernetzten Operationsführung' bzw. ‚netzwerkzentrierten Kriegführung' im Mittelpunkt steht, hatte demgegenüber keine Priorität. Die mit der Vielfalt von Netzwerken einhergehende großflächige Verteilung kleiner Standorte war in einer auf Wehrpflicht basierenden Territorialarmee geradezu zweckmäßig.

Darüber hinaus war diese Vielfalt jedoch auch technisch und politisch bedingt: Jedes Netzwerk war auf eine Art von Information ausgerichtet und darüber hinaus vom jeweiligen Stand der Zertifizierung innerhalb der NATO bestimmt. Eingeführt wurden sie im Zuge großer und langwieriger Beschaffungsvorhaben, die von miteinander



Der „Bedrohungsatlas" veranschaulicht das „Schema Luftwaffe" und die Dichte der zu vernetzenden Standorte

konkurrierenden, zunehmend internationalen Konsortien durchgeführt wurden. Flugzeuge verschiedener Hersteller oder Baureihen nutzen bis heute unterschiedliche Standards, analog gilt dies für Heer und Marine. Ein fliegendes Symbol für diese Vielstimmigkeit sind die häufig als ‚fliegende Kommandozentralen' beschriebenen AWACS der NATO, tatsächlich liegt ihre Funktion jedoch in der Führungsunterstützung: Mit ihren über 50 Antennen stellen sie den Informationsaustausch zwischen den Luftwaffen der verschiedenen NATO-Staaten und den Kommandostäben auf NATO-Ebene her.[6]

SATELLITENKOMMUNIKATION: INTERVENTIONSARMEE

Darüber hinaus stellen die AWACS die Funktion einer weiträumigen Luftraumüberwachung bereit, die innerhalb der NATO durch zivil anmutende (tatsächlich jedoch ist etwa die Deutsche Flugsicherung eine zivil-militärische Institution) bodengestützte Radar- und Leitstellen gewährleistet wird. Gegenüber den statischen Richtfunknetzen, die durch mobile Einheiten ergänzt werden können, weisen die AWACS einen offensiveren Charakter auf, der zumindest darauf abzielt, die Reichweite der auf „eigenem Territorium" errichteten Sensorik und Kommunikation darüber hinaus auszudehnen.

Die ‚vernetzte Operationsführung' und die damit im Kern gemeinte streitkräfteübergreifende Führungsstruktur ist ihrerseits ein offensives Konzept. Von der Rüstungsindustrie wird sie gerne so illustriert, dass aus dem sicheren Hinterland kommandierte Truppen an einer fremden Küste agieren – von See, Luft und Land aus – und dabei ständig miteinander in Kontakt stehen. Tatsächlich dürfte die Notwendigkeit, die Feuerkraft und Aufklärungsfähigkeiten der Teilstreitkräfte mehrerer Staaten (überraschend) auf einem Punkt zu konzentrieren oder in sonstiger Form zu koordinieren, bei offensiven Szenarien deutlich größer sein. Die Kommunikation mit den Kommandos im entfernten Heimatland wird dabei prinzipiell über Satelliten ermöglicht und durch Glasfaserkabel – sofern vorhanden – unterstützt. Solche Glasfaserkabel existieren in großer Menge zwischen den USA und Europa und wurden in den vergangenen Jahren zwischen Europa, insbesondere Italien, und Ostafrika bzw. der Arabischen Halbinsel ausgebaut. Über sie lief ein Großteil der militärischen Kommunikation zwischen den USA und ihren Einheiten in Irak und Afghanistan. Obwohl sie nahezu ausschließlich von Unternehmen betrieben werden, orientieren sich die Kabelstrecken an militärischen Anforderungen (die militärische Fokussierung der USA auf den Nahen und Mittleren Osten) bzw. spiegeln diese wider.

Dasselbe gilt auch für private Anbieter von Satellitenverbindungen. Unternehmen wie Horizon Teleports sind einerseits auf staatliche bzw. militärische Kundschaft ausgerichtet und platzieren ihre Satelliten zugleich so, dass sie im Kern ein Gebiet zwischen Westeuropa und Afghanistan abdecken.[7] Überspitzt gesagt, müsste sich die mittelfristige Konfliktsituation auch im Weltraum an einer erhöhten Konzentration von Satelliten ablesen lassen.

Die Entscheidung, dauerhaft Bandbreiten anzumieten und v.a. eigene militärische Kommunikationssatelliten zu entwickeln, ist gewissermaßen gleichzusetzen mit dem Aufbau der Interventionsfähigkeit und ihrer Reichweite. Über ein entsprechend globales Kommunikationsnetzwerk verfügen gegenwärtig nur die USA und stellen dies je nach Lage der NATO zur Verfügung. Eine Voraussetzung hierfür ist ein weitmaschiges, aber globales Netz von Militärbasen, über das ebenfalls aktuell nur die USA verfügen. Die Bundeswehr hat 1990 mit dem Aufbau entsprechender Kapazitäten begonnen, zunächst jedoch in Kooperation mit Frankreich und Großbritannien. An umfassende und offensive Auslandseinsätze außerhalb des NATO-Rahmens war in jener Zeit ohnehin noch nicht zu denken. 1999 dann begann die Bundeswehr ein eigenes Programm, das zunächst auf der Anmietung von Band-

Das Satellitenwerk des Airbus-Konzerns in Immenstaad...


... am Bodensee, mit der Frima ND Satcom direkt gegenüber.


Das Unternehmen Horizon Teleports in Moosburg an der Isar.

breiten bei privaten Anbietern setzte, jedoch die Schaffung eigener Kapazitäten vorsah. 2006 wurde ein entsprechender Vertrag mit den Unternehmen ND SatCom und EADS (heute: Airbus) unterzeichnet, welcher für fast 1 Mrd. Euro für zunächst 15 Jahre den Bau und Betrieb von zahlreichen Bodenstationen und zwei Bundeswehrsatelliten vorsah (SATCOMBw Stufe 2). Diese wurden am 1.10.2009 und am 21.5.2010 jeweils mit Ariane-Raketen in den Weltraum verbracht, am 1.4.2010 wurde das System feierlich in Dienst gestellt: General Manfred Engelhardt konnte als erster über eine bundeswehreigene Satellitenverbindung Kontakt mit der Fregatte Schleswig-Holstein in fernen Gewässern aufnehmen.

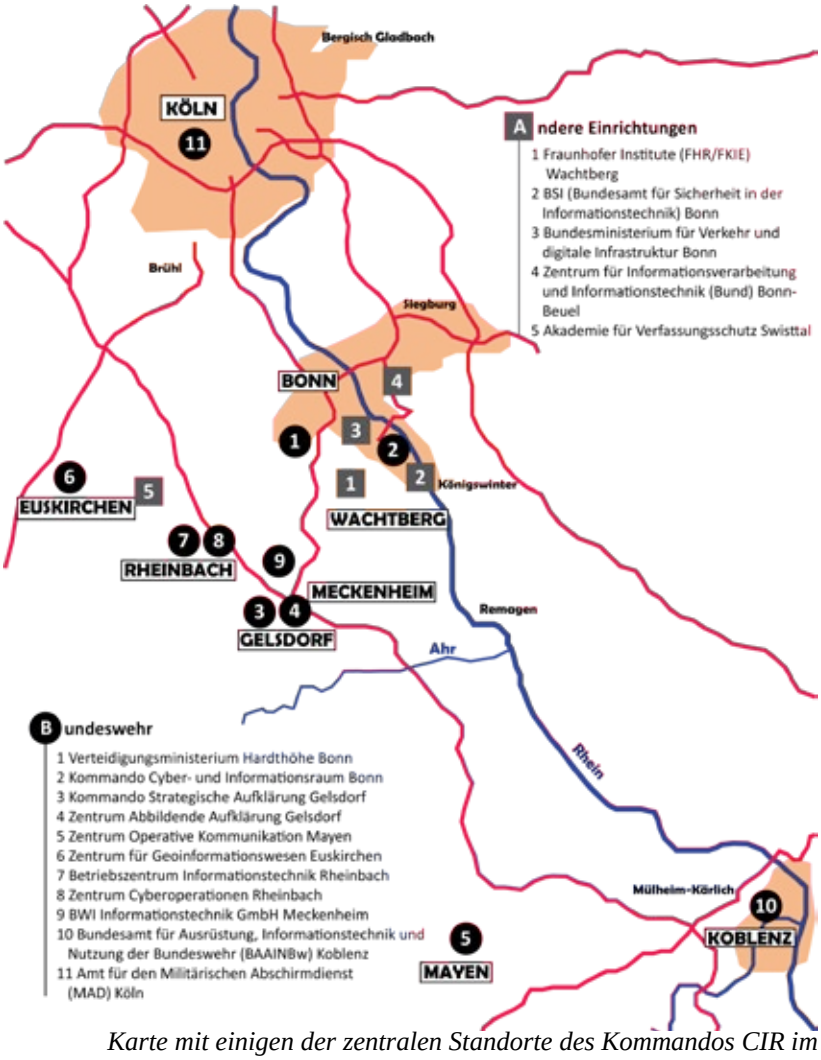
Das zur Umsetzung gegründete Airbus-Tochterunternehmen MilSat Services schreibt heute auf seiner Homepage: „Mit SATCOMBw wurden der Bundeswehr die Fähigkeiten zur Führungsunterstützung in den Einsatzgebieten bereitgestellt“. Neben den Satelliten umfasse das Programm „den Ausbau eines Netzes von festen Bodenstationen für Weitverkehr und Satellitenkontrolle, transportable Stationen sowie zu dessen Betrieb ein Führungs- und Kontrollsystem. Ergänzend leistet Airbus Defence and Space Dienstleistungen wie Anmietung ziviler Satellitenkapazität und Unterstützung bei Satelliten- und Netzwerkskontrolle.“ Eine schematische Grafik zweier Satelliten aus der Weltraumperspektive soll darstellen, wie einer dieser Satelliten die Verbindungen von Deutschland auf den afrikanischen Kontinent, ein anderer nach Zentral- und Südasien herstellt.[8] Die möglichen ‚Einsatzräume‘ der Bundeswehr sind damit auch durch die Position der Satelliten bestimmt und andersherum.

HYBRIDE STRUKTUREN

Wenn hier von bundeswehreigenen Kapazitäten die Rede ist, ist dies jedoch irreführend, denn betrieben werden viele der Komponenten auch heute von formal privaten Körperschaften, die unvorstellbare Summen damit verdienen, das kommunikationstechnische Rückgrat der ‚Armee im Einsatz‘ zu liefern. Ganz konkret profitieren u.a. die Standorte in Bremen, wo der Satellitenhersteller OHB und die Airbus-Tochter MiliSat ihren Sitz haben, Immenstaad, wo die Satelliten-Abteilung von Airbus und ND Satcom einander direkt gegenüberliegend an der B31 ihre Gebäude unterhalten, sowie der Hauptsitz von Airbus in Taufkirchen/Ottobrunn im Süden Münchens (siehe Beitrag von Franz Wanner). Gesteuert werden die SATCOMBw-Satelliten vom Raumfahrtkontrollzentrum in Oberpfaffenhofen bzw. von der damit verbundenen Bodenstation Weilheim als ‚Ankerstation‘ (beide westlich des Starnberger Sees, ebenfalls mit Wurzeln in der NS-Luftfahrt). Beides sind Einrichtungen des Deutschen Zentrums Luft- und Raumfahrt (DLR). Beim DLR handelt es sich formal um einen eingetragenen Verein (e.V.) mit Sitz in Köln, der 2015 knapp 8.000 Mitarbeiter*innen und ein Gesamtbudget von 888 Mio. Euro hatte. Unter verschiedenen unverdächtigen Stellenangeboten des DLR fand sich Ende 2017 zum Beispiel eine Ausschreibung „Technischer Ingenieur (m/w)“ für die „[b]etriebliche Projektsteuerung und technische Projektarbeiten für Projekt SATCOMBw“. Außer dem Kürzel am Ende verwies nichts in der Stellenbeschreibung darauf, dass ihr zentraler Zweck in der Optimierung der Kommunikation zwischen hiesigen Kommandos und den Out-of-Area-Einsätzen der Bundeswehr besteht.

Stellenausschreibung des Deutschen Zentrums Luft- und Raumfahrt für Mitwirkung an SatComBW.

Weitere zentrale Bodenstationen befinden sich hingegen in Bundeswehrliegenschaften in Kastellaun, Gerolstein und Rheinbach, allesamt linksrheinisch in bzw. am Rande der Eifel gelegen. Doch auch hier sind private Betreiber unmittelbar eingebunden. Im Herbst 2015 erhielt OHB aus Bremen den Auftrag, die Ankerstation in Gerolstein auszubauen, um, so das Unternehmen, „als Hauptauftragnehmer und Systemführer eine für die Bundeswehr einsatzwichtige Funktionalität und [...] damit die Führungs- und Kommunikationsfähigkeit der Bundeswehr in den Einsatzgebieten [zu] sichern“.[9] An den jeweiligen Standorten ist auch die BWI GmbH präsent, an der bis 2016 die Siemens AG und IBM beteiligt waren. Seit 2016 handelt es sich um eine Firma im alleinigen Besitz des Bundes, von deren 96 Standorten sich lediglich vier nicht auf militärischen Liegenschaften befinden bzw. an diese angegliedert sind. Von ihren gut 3.000 Mitarbeiter*innen waren im Mai 2017 505 am Hauptsitz in Meckenheim, 200 in Rheinbach und 577 in Bonn beschäftigt, wo im Verlauf desselben Jahres das Kommando Cyber- und Informationsraum (CIR) und der zugehörige Organisationsbereich im BMVg seine Arbeit aufnahm, zu dessen Aufgaben bzw. Befugnissen auch die unternehmerische Steuerung der BWI GmbH gehört.[10]



Karte mit einigen der zentralen Standorte des Kommandos CIR im Großraum Köln-Bonn.

CYBER-CLUSTER UND ANSATZPUNKTE FÜR PROTEST

Die räumliche Verteilung der großen Standorte der BWI GmbH verweist bereits auf eine bemerkenswerte Konzentration der Komponenten des Kommandos CIR auf die Eifel bzw. den Großraum Köln-Bonn. Neben dem Kommando selbst und den bereits genannten Führungsunterstützungsbataillonen (heute: Informationstechnikbataillone) in Kastellaun und Gerolstein befindet sich in Rheinbach mit dem Zentrum Cyberoperationen jene Einheit, die zumindest nach offen verfügbaren Quellen am ehesten für offensive Cyber-Operationen ausgerichtet ist, in unmittelbarer Nähe zu Meckenheim und dem Hauptsitz der BWI GmbH. Zudem untersteht dem CIR die strategische Aufklärung, deren zentrale Einrichtungen in Euskirchen (Zentrum für Geoinformationswesen) und Grafschaft-Gelsdorf (Zentrum Abbildende Aufklärung) liegen. Auch die entsprechenden – mit den Kommunikationssatelliten nicht zu verwechselnden, aber im selben Zeitraum aufgrund derselben strategischen „Notwendigkeiten“ implementierten – Aufklärungssatelliten der Bundeswehr werden in Zusammenarbeit mit Airbus, OHB und DLR betrieben. Die Antennen des prinzipiell eher geheim operierenden ehemaligen Zentrums für Nachrichtenwesen der Bundeswehr in Gelsdorf sind von der Autobahn A61 nahe dem Kreuz Meckenheim in südlicher Richtung bei guten Bedingungen sogar sichtbar. Wenige Kilometer weiter auf der A61 Richtung Koblenz kann auf der anderen Seite die Spitze eines Radoms erahnt werden, das zum gemeinsamen Gelände der Fraunhofer-Institute für Hochfrequenzphysik und Radartechnik (FHR) und für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) gehört, das im Auftrag des BMVg umfangreiche Forschungsarbeiten zu strategischer Aufklärung und Cybertechnologie durchführt (siehe Beitrag von Franz Wanner) und u.a. über eine „aktive Daten-Direkt-Verbindung“ zur Kaserne in Euskirchen an das Bundeswehrnetz angebunden sind.[11]

Darüber hinaus gehören auch das Zentrum Operative Kommunikation in Mayen und die Auswertezentrale Elektronische Kampfführung in Daun, die ihrerseits dem Kommando CIR unterstehen, in relativer Nähe zu Rheinbach bzw. Bonn. Ein weiterer, wenn auch deutlich kleinerer Cluster ergibt sich aus der Führungsunterstützungsschule der Bundeswehr in Pöcking (am Starnberger See) und dem Informationstechnikbataillon in Murnau (am Staffelsee) in Verbindung mit den DLR-Standorten Weilheim und Oberpfaffenhofen südwestlich von Murnau.

Über den von hier aus hergestellten Informationsraum sind weitere Standorte der Bundeswehr (quasi) in Echtzeit in die Auslandseinsätze der Bundeswehr einbezogen. Die Auswertung der von Israel geleasten Heron-Drohnen in Mali etwa erfolgt im Fliegerhorst Jagel, von wo aus die

Aufruf zu einer Kungebung in Jagel, wo die Aufklärungsdaten der Heron-Drohnen in Mali ausgewertet werden.

Das im Aufbau befindliche Kommando CIR in Bonn von vorne...

... und von hinten.

Ergebnisse – sicherlich unter Einbeziehung des Amts für Geoinformationswesen in der Eifel – wiederum nach Bamako und ins Camp Castor im Norden des westafrikanischen Landes geliefert werden. Die ‚vernetzte Operationsführung' von Deutschland aus unterstreicht somit einmal mehr, dass Krieg hier beginnt und hier Protest möglich und angebracht ist. Zum Beispiel am Standort Jagel in Schleswig-Holstein, wo schon mehrere Mahnwachen und Kundgebungen gegen den Krieg in Mali stattfanden, der von dort aus (mit-)geführt wird.[12]

ANMERKUNGEN

1 Bundesnetzagentur: Frequenzplan (Stand: April 2016), S.405 und S.477.
2 Jens Rüggeberg: NATO-Pipeline in Bodelshausen und anderswo, IMI-Standpunkt 2009/012
3 http://www.vorbei-ev.de/wwwa/virtuelles-gsvbw-museum-das-bundeswehrgrundnetz-bwgn/.
4 http://www.vorbei-ev.de/wwwa/virtuelles-gsvbw-museum-tarnung-einer-gsvbw/.
5 http://www.vorbei-ev.de/wwwa/virtuelles-gsvbw-museum-das-bundeswehrgrundnetz-bwgn/.
6 Eine relativ umfassende, öffentlich einsehbare Übersicht über die von Bundeswehr und NATO genutzten Kommunikationsstrukturen bietet eine Publikation des Instituts für technische Informatik der Universität der Bundeswehr in München: Prof. Dr. Gabi Dreo, Björn Stelte, Sebastian Hanigk (Hrsg.): „Militärische Funkkommunikation", Juni 2011.
7 Siehe z.B. „satellites" unter www.horizon-teleports.com.
8 „satcombw-stufe-2" unter www.milsatservices.de.
9 „OHB erhält Auftrag zum Ausbau der großen Bodenstation für Satellitenkommunikation (Ankerstation) der Bundeswehr in Gerolstein", Pressemeldung der Firma OHB System AG vom 11.11.2015.
10 BT-Drucksache 18/12277.
11 Ebd.
12 Im Aufruf zu einer „Mahnwache und Filmvorführung" am 14. Oktober 2017 heißt es u.a.: „Schon jetzt werden auf dem Fliegerhorst Jagel DrohnenpilotInnen im Simulator ausgebildet. Schon jetzt werden dort die über Mali von den Drohnen gesammelten Daten zu Zielkoordinaten ausgewertet." Weitere Aufrufe zu vergangenen und zukünftigen Aktionen rund um den Standort Jagel finden sich unter: http://bundeswehrabschaffen.de/cms/aktuelles.htm.

Zur Quellenlage:

Einige der Informationen über aufgegebene Strukturen stammen aus Ortsbegehungen und teils den Erzählungen von Anwohner_innen und sind entsprechend vage. Sehr gut aufbereitet sind die Informationen über die Grundnetzschalt- und Vermittlungsstellen der Bundeswehr durch den eingetragenen Verein ‚Vorbei e.V.', der u.a. die ehemalige GSVBw in Elmlohe erworben hat und versucht, diese möglichst originalgetreu wieder herzustellen und zu erhalten. Fast alle sachlich fundierten Informationen über die GSVBw stammen von der Webseite des Vereins vorbei-ev.de. Ohne ihn wäre bis heute so gut wie nichts über diese Struktur öffentlich bekannt.

Weitere Informationen, insbesondere zu den Richtfunknetzen, entstammen Foren, die sich mit ‚Lost Places' beschäftigen. Eine solche Quelle ist geschichtsspuren.de, wo sich auch (ehemalige) Soldaten der Fernmeldetruppen oft mit anekdotenhaften Berichten an der Diskussion beteiligen. Zugleich wird dort jedoch auch peinlichst darauf geachtet, keine aktuellen Strukturen offenzulegen.

SCHNITTSTELLE ZUM CYBERKRIEG - DER BRANCHENVERBAND AFCEA

VON: ANDREAS SEIFERT

Cyberkrieg ist eine wenig greifbare Kategorie. Die technischen Möglichkeiten der Manipulation von elektronischen Vorrichtungen, von Datenbeständen und Nachrichtenkanälen sind scheinbar endlos – jedes technisches Gerät kann in eine Waffe umgewandelt werden, kann beschädigt oder außer Funktion gesetzt werden. Was bei einer Geschirrspülmaschine oder dem Spiele-PC harmlos und ärgerlich wirken mag, stilisiert sich angesichts der Abhängigkeit jeder Gesellschaft von Mobilität, Kommunikation und Energie zu einer entgrenzten Drohkulisse hoch: Verkehrssteuerung, Wasserwerke, Kraftwerke und Telekommunikationsinfrastruktur funktionieren inzwischen ausnahmslos mit elektronisch gesteuerten Systemen.

Einen Schutzauftrag für sich reklamierend, schickt sich nun auch die Bundeswehr an, das Cyberfeld militärisch zu durchdringen. Sie rüstet sich für einen Krieg im Cyber- und Informationsraum, indem sie eine Teilstreitkraft mit 21.000 Planstellen aus der Taufe hebt und Geld in Überwachungsinfrastruktur und Technologie pumpt. Im Weißbuch zur Verteidigung wird eine allumfassende elektronische/digitale Bedrohung konstatiert und für die Bundeswehr ein Spektrum an Aufgaben abgeleitet:

Damit die Bundeswehr ihre Aufgaben im Cyber- und Informationsraum zukünftig wahrnehmen kann, gilt es darüber hinaus unter anderem,

- die gesamtstaatlichen Fähigkeiten auszubauen, also ressortübergreifend zu kooperieren und sich mit Wissenschaft, Industrie und Partnern zu vernetzen;
- bundeswehreigene Cyberfähigkeiten auszubauen, dabei die Sicherheitsarchitektur des IT-Systems der Bundeswehr zu konsolidieren und resilienter zu machen;
- Waffensysteme und Gefechtsstände sowie Lieferketten in der Rüstung, unter anderem durch den gezielten Rückgriff auf nationale Schlüsseltechnologien, zu härten;
- Spitzenpersonal durch Schaffung attraktiver Cyberkarrierepfade und innovativer Personalgewinnungsstrategien zu rekrutieren sowie sich zu öffnen für neue Partnerschaften und Kooperationen;
- die heute noch fragmentierten Zuständigkeiten und Strukturen für einen robusten Fähigkeitsaufbau zusammenzuführen, die IT-Fähigkeiten zur Digitalisierung der Streitkräfte zu bündeln sowie zentrale Ansprechpartner für andere Ressorts und multinationale Partner zu schaffen.

Jeder der fünf Spiegelstriche ergibt sich dabei aus der spezifischen militärischen Sicht und wäre im Sinne einer Kommentierung zu erweitern. Ließe sich der erste Spiegelstrich noch als offene Formulierung für eine auch zivil zu denkende Cyberabwehr von Gefahren und ein Monitoring krimineller Aktivitäten im Internet interpretieren, verortet sich die Bundeswehr im letzten Spiegelstrich als aktiver und zentraler Akteur (Ansprechpartner) in diesem Netz – gestärkt durch eine eigene Organisationseinheit: dem inzwischen geschaffenen Kommando Cyber- und Informationsraum. Spannender für die Diskussion hier sind allerdings die drei mittleren Punkte. Sie berühren die industriellen Kapazitäten, bzw. bilden, wie die Konsolidierung der IT-Infrastruktur der Bundeswehr, in sich auch relevante Ausgabenposten. Oder präziser: Hier wird auch Geld verdient.

Inzwischen werden die Cyberfähigkeiten der Bundeswehr ausgebaut und auch in der Kommandostruktur gebündelt. Das Kommando Cyber- und Informationsraum ist dabei nur die Fortsetzung dessen, was bereits unter anderen Strukturen begonnen wurde. Das IT-Netz der Bundeswehr, bisher fein säuberlich in eine grüne (militärische) und weiße („zivile“) Infrastruktur getrennt, wird dabei zusehends zu einem Raum verschmolzen und mit immer mehr Computertechnik ausgestattet. In wieweit man in den Spiegelstrich aus dem Weißbuch auch den Ankauf von Sicherheitslücken (zero day exploits etc.) oder die Konstruktion von Computerwürmern oder -viren verstehen kann, bleibt der Fantasie überlassen – ausgeschlossen wird es jedenfalls nicht.

Waffensysteme und Lieferketten in der Rüstung zu härten ist dank jahrelanger (Fehl)Planung und Beschaffungspraxis eine enorme Herausforderung. Das „Härten“ von Systemen gegen Angriffe bestand noch vor wenigen Jahren aus einer wie auch immer gearteten möglichst stabilen Verpackung. Beispiele wie die Toughbook-Computer der Firma Panasonic spiegelten lange Zeit die militärische Vorstellung von einem „sicheren“ Laptop wieder – massiv, stabil, un-kaputtbar. In Zeiten von Viren und Computer-Würmern ist das jedoch nur ein unzureichender Schutz. Das Verhältnis von stabiler Hülle und verletzlichem elektronischen Innenleben hat sich seit den letzten zwanzig Jahren deutlich verschoben. Nun zeigt sich, dass die Systeme in sich angreifbar sind. Das Ministerium sucht eine Lösung und findet sie in der lückenlosen Dokumentation aller einzelnen elektronischen Bauteile. Dabei setzt man auf nationale Produzenten – auch weil der Einkauf ausländischer Systeme das Risiko darin verbauter Schwachstellen und damit externer Zugriffsmöglichkeiten erhöht.

Darüber hinaus nimmt sich die Bundeswehr vor, attraktiver Arbeitgeber für Spitzenpersonal aus dem IT-Bereich zu werden. Angesichts von Fachkräftemangel und weltweiter Umstellung auf digitale Produktion handelt es sich hier um einen kostenintensiven Posten. Bei den „innovativen Personalgewinnungsstrategien“ soll in erster Linie auf die Kooperation mit der Wirtschaft gesetzt werden. Nicht

selten sind schon jetzt Stellenausschreibungen zu finden, deren Verbindung zur Bundeswehr – z.B. als Dienstleister für Radaranlagen oder Netzbetrieb – sich nur klein am Rande der Anzeige findet.

GROßPROJEKTE

Mit dem Cyberraum wird nicht erst in jüngster Geschichte auch Geld verdient. Früher unter dem Begriff der elektronischen Kampfführung (EloKa) bekannt, verlängert sich ein bisher bestehendes Geschäftsfeld in den Bereich des Virtuellen. Die Cybertruppe der Bundeswehr setzt sozusagen auf den physischen Hinterlassenschaften bereits installierter Kommunikations- und Datennetze und neuen Entwicklungen der Hardware auf und erweitert den eigenen Aufgabenbereich keineswegs nur in einer virtuellen Dimension.

Um den „Zustand“ zu skizzieren, ließen sich die großen Beschaffungsprogramme vergangener Jahrzehnte anführen – auch um gleich von vornherein darauf zu verweisen, dass es die Industrie ist, die hier schon immer mitverdient hat. Allein die Überarbeitung der zivilen IT-Infrastruktur im Zeitraum von 2006 bis 2016 hat über 7 Mrd. € verschlungen, die über eines der größten Projekte öffentlich-privater Partnerschaft (PPP) in Europa abgewickelt wurde. Vielsagend ist bereits der Name des Projekts: „Herkules“. Die hierfür gegründete BWI GmbH in Meckenheim mit den Beteiligten Siemens, IBM und dem Bund ist nach Ablauf des Ursprungsvertrages 2017 in eine hundertprozentige Bundesgesellschaft umgewandelt worden. Nun, so ist bei der Bekanntgabe der Umwandlung erwähnt worden, soll sich die BWI aber nicht mehr nur um die zivile IT-Infrastruktur der Bundeswehr kümmern, sondern auch als Ansprechpartner für den militärischen Teil fungieren. Damit nicht genug, will sich die BWI zudem als Dienstleister für andere Bundesbehörden andienen, womit eine an den Bundeswehrinteressen ausgerichtete Firma nun auch noch im Zivilen wildert – man könnte darin auch eine Militarisierung der Behörden-IT erkennen.

Auch eine andere Großausgabe – oder besser: einer der größeren Skandale –, die Beschaffung des Eurohawk durch die Bundeswehr, ist im Kontext der elektronischen Kriegsführung zu sehen. Notorisch fehlgeplant ist das Projekt an der Integration in den (zivilen) Luftraum gescheitert. Es wurde aber nicht, wie viele glauben, nach verschwendeten hunderten Millionen eingestampft, sondern ist schlicht umbenannt worden und wird auch weiterhin Gelder aus dem Bundeshaushalt ziehen. Zentral ist dabei nicht, wer die Drohne stellt, sondern wer die Elektronik für die Signalerfassende Aufklärung (Signals Intelligence, SIGINT) stellt: EADS/Airbus. Als Kernstück des gesamten Systems soll die Drohne hoch oben aus der Luft in einem Radius von über 200 Kilometern jedwede elektronische Kommunikation am Boden erfassen können. Ziel ist dabei weniger, die Inhalte von Telefongesprächen zu erfassen oder Personen zu identifizieren, als vielmehr die Struktur der Kommunikation zu erfassen und potentielle Schwachstellen auszumachen – böse Zungen behaupten, das hätte etwas mit Kriegsvorbereitung zu tun.

Im Zusammenhang mit Einsatzplanung ist auch die Anschaffung eines digitalen Höhenmodells der Erde zu sehen - mit 475 Mio € einer der größten Einzelposten unter der Führung der Verteidigungsministerin von der Leyen. Als Grundlage der Geoinformationssysteme, die bis zum Soldaten hinunter Verwendung finden, ersetzt dieses Modell zwar die Karte als Grundlage militärischer Planung und Aktionen nicht vollständig, doch ermöglicht es beispielsweise die zielgenaue Steuerung von Truppen oder Raketen. Vertrieben wird das Modell wiederum vom Unternehmen Airbus, das sich die kommerziellen Rechte daran gesichert hat – nachdem, so muss hinzugefügt werden, die Bundesrepublik die Erstellung des Modells mit mehreren hundert Millionen Euro überhaupt erst ermöglicht hat. Der Steuerzahler bezahlt es sozusagen doppelt.

SCHWACHSTELLE PERSONALGEWINNUNG

Allein die drei genannten Großprojekte stehen beispielhaft für die kontinuierlichen Investitionen in Kommunikations- und Dateninfrastruktur, Weiterentwicklung der Sensortechnologien zur Erfassung möglichst vieler Daten und die Investitionen in Big-Data, seien diese in Form von Datenmodellen oder Software zu deren Analyse. Diese werden längst nicht als autochthone Aufgaben der Bundeswehr allein begriffen, sondern oftmals in Modellen der Öffentlich-Privaten-Partnerschaft oder des Outsourcing betrieben. Die Bundeswehr plant hier schon längst mit industriellen Kooperationen und ist ganz wesentlich auf das Wissen und die Unterstützung durch Unternehmen angewiesen – sowohl auf die großen etablierten Unternehmen, wie auch auf kleine und mittlere Unternehmen mit einer besonderen Spezialisierung.

Neben der Infrastruktur, Erfassung und Auswertung von Daten stellt die Investition ins Personal eine vierte Dimension dar. Deshalb wurde die Cyberoffensive der Bundeswehr als mediales Ereignis inszeniert und auf Großplakaten wird mit sympathischen jungen Menschen für den Dienst am Computer geworben: Digitale Kräfte. Die Bundeswehr habe 21.000 Stellen im IT-Bereich, suche 700 Admins, stelle 800 IT-Soldaten allein im Jahr 2016 ein, habe 333 Studierenden ein IT-Studium in sieben Studiengängen ermöglicht, heißt es in einer der plakativen Onlineanzeigen. Die zusätzlichen Soldaten für den IT-Bereich decken jedoch absehbar nur einen Teil des über die „neuen Bedrohungen“ konstruierten „Bedarfs“ ab – einen nicht unerheblichen Teil der Aufgaben wird über industrielle Dienstleistungen zu erbringen sein. Dies ist ein Anlass, sich mit den IT- und elektronikbezogenen Firmen auseinander zu setzen, die im Umfeld der Bundeswehr auf Aufträge hoffen und ihre Angebote formulieren. Im Folgenden soll dies auf zwei Ebenen angegangen werden: Erstens auf der Ebene der Lobbyverbände, zum Zweiten auf der Ebene der Firmen selbst. Beides muss schlaglichtartig bleiben, da auch mit intensiven Recherchen bisher nur Teile der Akteure und ihrer Handlungen sichtbar gemacht werden können.

DER BRANCHENVERBAND AFCEA

Einen guten Ansatzpunkt bietet jedoch der Branchenverband AFCEA, der deutsche Zweig einer ursprünglich in den USA gegründeten Lobbyvereinigung, die als „Armed Forces Communications and Electronics Association“ aus ihrer Ausrichtung auf militärische Anwendungen keinen Hehl macht. Die „AFCEA Bonn e.V. - Das Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung“ hat ihren Sitz in Bonn, wo sich eines von zwei großen Zentren im IT-Bereich der Bundeswehr befindet; die Nähe zur Hardthöhe und zum Beschaffungsamt der Bundeswehr in Koblenz stellen weitere Standortvorteile dar. Unter dem Dach von AFCEA existieren in Deutschland sechs Unterkapitel, von denen das Bonner nur eines ist – ein zweites, ebenfalls von deutschen Unternehmern initiiert – befindet sich in München, ist aber weitgehend inaktiv. Die anderen vier Kapitel sind jeweils an US-amerikanischen Militäreinrichtungen in Deutschland angesiedelt und fokussieren in ihrer Arbeit auch auf die US-Truppen und ihre Angehörigen.

AFCEA hat bislang gegenüber der Deutschen Wehrtechnischen Gesellschaft oder dem Bundesverband deutscher Sicherheits- und Verteidigungsindustrie eher ein Schattendasein geführt – hat aber, was die thematische Abdeckung der Cyberkriegsoptionen anbetrifft, die Nase vorn.

Zu den Aktivitäten des Bonner Vereins gehören vielfältigste Veranstaltungen: Von Messen über Symposien und kleineren Gesprächsrunden bis hin zu gemeinsamen Tagungen z.B. mit der Bundeswehr oder den Fraunhofer Instituten. Ein über die Jahre hinweg immer umfangreicher gewordenes Nachwuchsförderprogramm umfasst z.B. auch Studienpreise für Abschlussarbeiten aus der angewandten IT, Nachrichtentechnik oder der Automatisierung. Von anfänglich einmal wenigen Tausend Euro ist inzwischen eine Summe von rund 17.000 € geworden, um die sich Studierende der

- Universität Bonn
- Hochschule Bonn-Rhein-Sieg
- Helmut-Schmidt-Universität Hamburg
- Universität Koblenz
- Hochschule Koblenz
- Universität der Bundeswehr München

bewerben können. Preisträger werden von einem Komitee ausgewählt, dem mit Dr. Michael Wunder ein Abteilungsleiter aus dem Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) in Wachtberg und Bonn vorsitzt. Auch wenn in der Auslobung des Preises ein direkter Bezug zu den (militärischen) Themen des Vereins nicht zwingend ist, zeigt sich doch bei vielen der eingereichten und prämierten Arbeiten eine Nähe hierzu.

DIALOG ZWISCHEN HERSTELLERN UND ANWENDERN

Die Veranstaltungen der AFCEA sind von besonderem Interesse, da hier Foren geboten werden, in denen sich Industrie, Ministerien und Militärs in einem direkten Austausch befinden. Es sind also nicht nur die Vertreter der Industrie, die hier ihre neuesten Produkte oder Vertreter der Bundeswehr, die ihre Anforderungskataloge präsentieren. Vielmehr befindet man sich im Dialog darüber, wohin sich die Technologie und Anforderungen entwickeln können. Die Grundkonstellation von Vertretern von Militär und Industrie wird dabei oft ergänzt durch Vertreter von weiteren Behörden und Ministerien mit Bezug zu Sicherheit – also auch Vertreter von Polizei, Verfassungsschutz oder den Innenministerien. Die Einbeziehung von Wissenschaftlern öffentlicher und privater Forschungseinrichtungen ermöglicht es, allen Akteuren früh Bedarfe wie Angebote auszurichten und liefert zudem die Blaupausen für die Legitimation gegenüber der Politik und der Öffentlichkeit. Diesen Foren kommt damit eine Rolle des Agenda Settings innerhalb des gesteckten Themenrahmens zu.

- 26. Jan.: AFCEA Mittagsforum mit Hitachi Data System: „Öffentliche Sicherheit mit intelligenter Videoüberwachung im Zeitalter der Digitalen Revolution“
- 26. Febr.: AFCEA Fachveranstaltung: „Digitalisierung im Einsatz - Herausforderungen für die Luftwaffe“
- 22. Mrz.: AFCEA Fachveranstaltung mit DBwV, Berlin: „Smart Mobility versus Mobility Security - Aktuelle Innovationen“
- 11./12. Apr.: 32. AFCEA Fachausstellung mit Symposium: „Digitale Zukunft gestalten - Intelligent. Vernetzt. Sicher.“
- 14. Mai: Parlamentarischer Abend, Berlin: „Digitalisierung Bundeswehr“
- 05. Jun.: Gemeinsame Veranstaltung AFCEA Bonn mit dem Heer: „Digitalisierung im Heer“
- 14. Jun.: AFCEA Fachveranstaltung mit Bitkom, Cebit: „Künstliche Intelligenz - Chancen und Herausforderungen für innere und äußere Sicherheit“
- 30. Aug.: Koblenzer IT-Tagung 2018: „Digitale Zukunft - Architekturen. Plattformen. Anwendungen.“
- 26. Sept.: Föderales IT-System - Vernetzte Verwaltung: „eGovernment und digitale Souveränität“
- 9./10. Okt.: Gemeinsame Veranstaltung AFCEA Bonn e.V. mit KdoCIR - CCF/ICOS
- 14. Nov.: AFCEA Technologieforum beim Fraunhofer FKIE: KI und Big Data zur Entscheidungsunterstützung“
- 23. Nov.: AFCEA Mittagsforum mit ESG: „Herausforderungen Digitalisierung: Verstehen - handeln - gemeinsam Mehrwert schaffen“
- 5. Dez.: AFCEA Fachveranstaltung: „Digitalisierung der Prozesse - Architekturen. Werkzeuge. Anwendungen.“

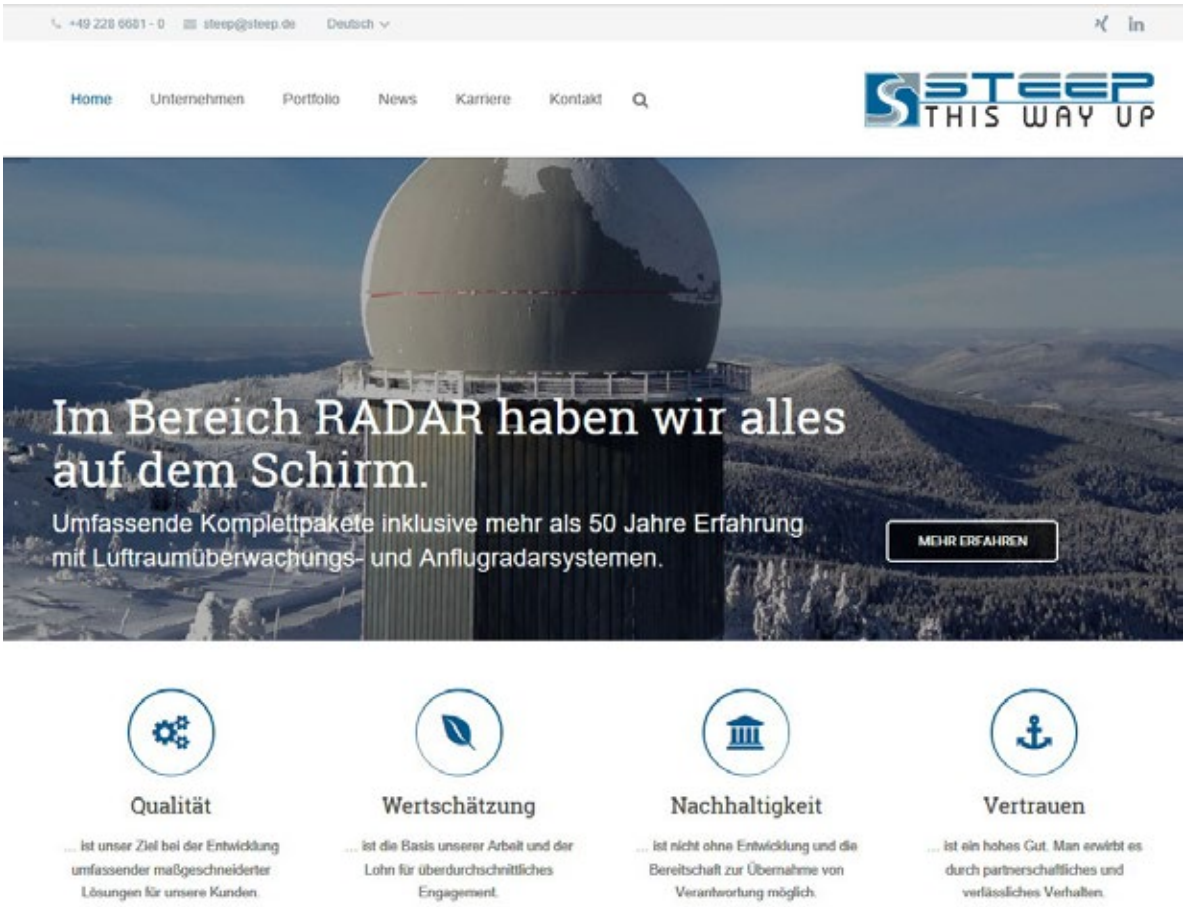
Die Liste der z.B. 2018 aufgeworfenen Themen ist dabei Beleg für die Breite, in der sich der Verband verortet und zeugt darüber hinaus von einem hohen Anspruch.

Der Blick zurück auf vergangene Veranstaltungen zeigt, dass ein jedes hier aufgeführte Thema immer unter mindestens drei, oftmals sogar vier Perspektiven der beteiligten Akteure aus Industrie, Militär, Politik (Regierung/ Behörde) und Forschung behandelt wird. Zudem wird bei allen Veranstaltungen die Möglichkeit zum „persönlichen Austausch“ geboten – eine Hohlfloskel für die Stärkung persönlicher Bindungen und Netzwerke. Die Veranstaltungen sind für alle Beteiligten ein Gewinn – die Industrie kann sich präsentieren, gleichzeitig den Kontakt zum Kunden pflegen und zudem noch Trends der Entwicklung erfahren; das Militär kann seine Bedürfnisse äußern, ohne großen Aufwand neue Anforderungen identifizieren und den Kontakt zu den Lieferanten aufrecht erhalten; die Regierungsstellen können zielgenaue, wissenschaftliche Expertise abgreifen, die Veränderung der Angebotspalette beobachten und spezifische Probleme zur Diskussion stellen; die Wissenschaftler können sowohl ihre eigene Unentbehrlichkeit unter Beweis stellen, wie auch neue Felder möglicher Forschung (und Forschungsförderung) identifizieren und in ihre Arbeit mit einbeziehen.

Ein Beispiel für eine Veranstaltung der AFCEA wäre z.B. die im September 2017 in Kooperation mit dem Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) – praktischerweise im nahegelegen Wachtberg – durchgeführte Tagung „Automatisierte Meinungsbeeinflussung – Manipulation in offenen Medien“. Hier lohnt ein genauerer Blick auf die vorgesehenen Themen und Referenten, darunter ein Vertreter des Verfassungsschutzes aus Niedersachsen zum Thema „Social Engineering“ und ein Redakteur des Behördenspiegels zum Umgang mit Fake-News. Ein weiterer Beitrag eines Oberstleutnants vom Zentrum Operative Kommunikation war unter dem dubiosen Titel „Die Bundeswehr und Katzenvideos? – Social Media als militärisches Wirkmittel“ vorgesehen. Ferner sollten zwei Unternehmensvertreter über die technischen Möglichkeiten der Analyse von Social Media und der Erkennung von Fake News vortragen. Aus dem Hochschulbereich finden sich Beiträge zu „Social Media“ und „Opinion Spam“. Den Abschluss bildet der Vortrag einer Bonner Professorin über die „Wahrheit aus philosophischer Sicht“.

ZUSAMMENSETZUNG DES BRANCHENVERBANDES

Die tiefgreifende Verzahnung des Verbandes mit Behörden, Militär und Forschung sollte dennoch nicht darüber hinwegtäuschen, dass AFCEA in erster Linie ein Branchenverband ist. Die auf der Homepage einsehbare Mitgliederliste der Bonner AFCEA ist im Laufe der letzten Jahre länger geworden – und umfasste Ende 2017 96 Mitgliedsfirmen und 900 Einzelmitglieder. Namentlich bekannt sind nur die Firmen, die die AFCEA-Homepage auch als Werbeplattform nutzen. Gerade bei den privaten

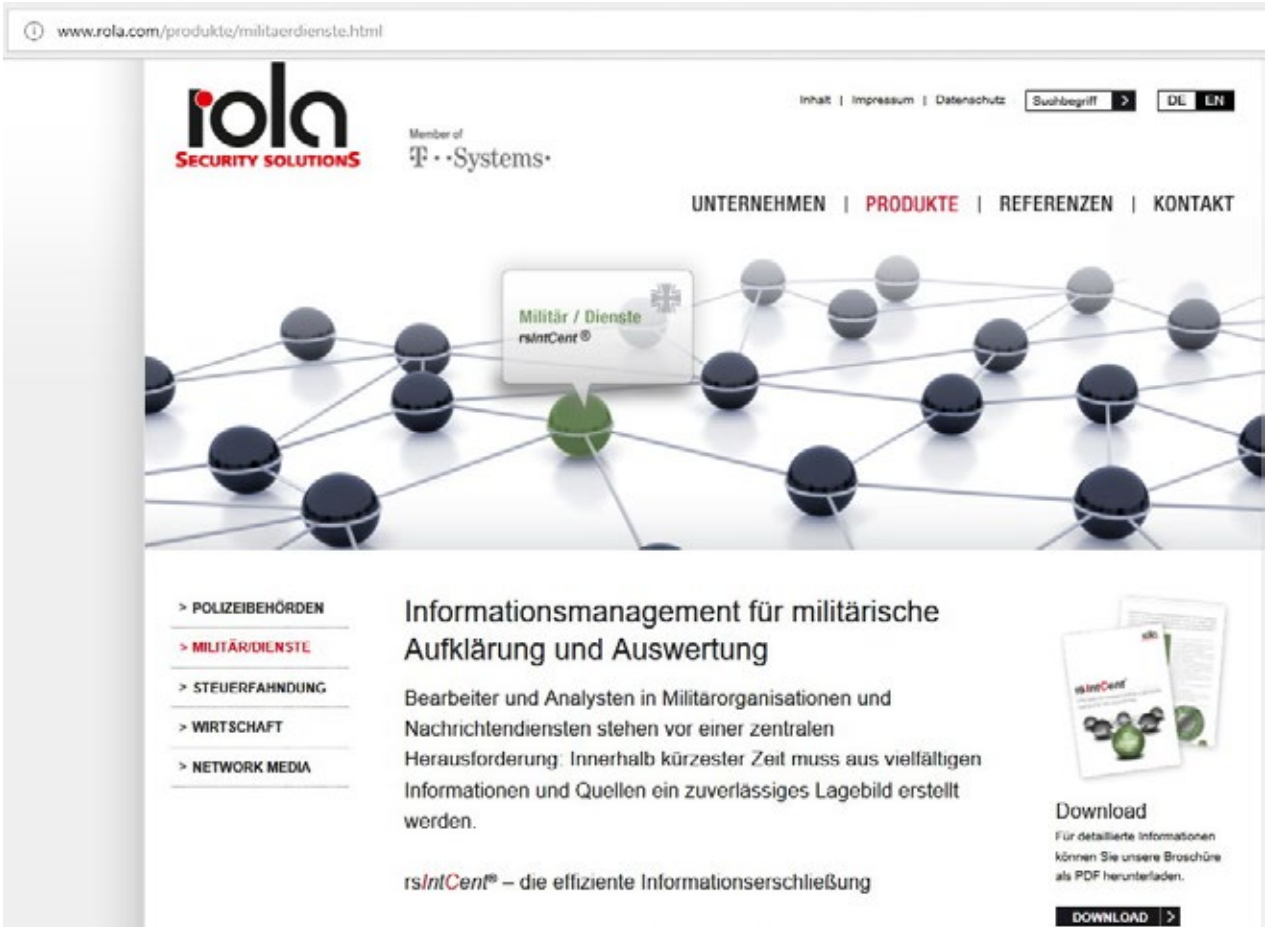


Mitgliedern ist dies nicht der Fall und es bleibt Spekulation, wie viele „Praktiker“ aus Militär oder Unternehmen sich hierunter befinden. Der Fokus der Betrachtung muss somit auf den Mitgliedsfirmen liegen. Hierunter finden sich selbstverständlich die bekannten großen Namen, die schon lange mit dem Militär zusammenarbeiten, wie Rohde&Schwarz, Telekom, ESG, Thales, IBM, etc. Aber auch eine ganze Reihe von kleineren Unternehmen, deren Geschäftstätigkeit mehr oder minder an einem der oben aufgeführten Punkte ansetzt, taucht hier auf. Auf der Karte erkennt man eine Ballung der Unternehmen im Rheinland und in München. Hauptstandorte sind tatsächlich Bonn und Köln – mit angeschlossenen Orten wie Siegburg, Hennef oder Hürth.

Exemplarisch seien an dieser Stelle ein paar Firmen angeführt – nicht um einen repräsentativen Querschnitt der Mitgliedsunternehmen zu bieten, als vielmehr das Spektrum aufzuzeigen, mit dem versucht wird, Geld zu verdienen.

Den Anfang macht dabei die Firma Steep aus Bonn, die in gewissem Sinne auch eine Brücke in die Vergangenheit elektronischer Kampfführung baut. Schon in den 1960er Jahren zum Zwecke der Betreuung der bundeswehreigenen Radaranlagen gegründet, war die Firma bis vor ein paar Jahren im Besitz des britischen Konzerns Serco. Im Verbund mit Serco ist die Betreuung ganzer Stützpunkte und Anlagen in das Portfolio aufgenommen worden und nach der Übernahme durch Mitarbeiter auch geblieben. Testzentren der Bundeswehr, aber auch privater Firmen wie der MBDA in Schrobenhausen werden dem Management von Steep unterworfen. Steep führt Tests im elektromagnetischen Bereich durch und hat, solange es ein Teil der britischen SERCO-Gruppe war, z.B. auch die Computer-Systeme der Projektorganisation OCCAR (Sitz in Bonn) gepflegt, die viele der großen europäischen Rüstungsprojekte (A400M, Eurofighter, etc.) betreut. Kerngeschäft ist aber nach wie vor die Betreuung der militärischen Luftraumüberwachung in Deutschland. Steep ließe sich somit auch als ein Modell anführen, wie originär bundeswehreigene Aufgaben dem Outsourcing unterworfen werden und in (scheinbar) zivile Unternehmen auch militärische Aufgaben verlagert werden können. Inzwischen bietet Steep auch Produkte, Schulungen und weitere Dienstleistungen für Netzwerke allgemein an - 2014 mit einem Umsatz von 110 Mio Euro. Steep ist damit noch einer der größeren Player im Geschäft mit der Bundeswehr. Etablierte Dienstleister in dieser Form für die Bundeswehr gibt es noch eine ganze Reihe – z.B. SQS aus Köln, die ein Testzentrum für die Produkte betreibt, die wir hier besprechen.

Ein ebenfalls großer Player ist die Software AG – genauso hätte man Microsoft, SAP, ATOS (alle Mitglieder von AFCEA) und andere anführen können. Die Software AG ist ein Beispiel für große Softwarehäuser, die Produkte für den militärischen Bereich entwickelt haben, die in erster Linie auf Lösungen basieren, die man für andere (zivile) Kunden entwickelt hat. Man preist diese Zweitverwertung auch oft als Vorteil an, da ein Umstieg von zivilen auf militärischen Nutzer leichter ist, als der Umgang mit kom-



plett neuen Oberflächen. Diese Produkte setzen oft bei den zivilen Produkten an (wie z.B. die SAP-Lösungen für Materiallogistik oder Buchhaltung, oder auch die Behördenplattform der Software AG), werden aber ins Militärische verlängert – die Software AG benennt hier z.B. die vernetzte Operationsführung als zusätzliche Komponente.

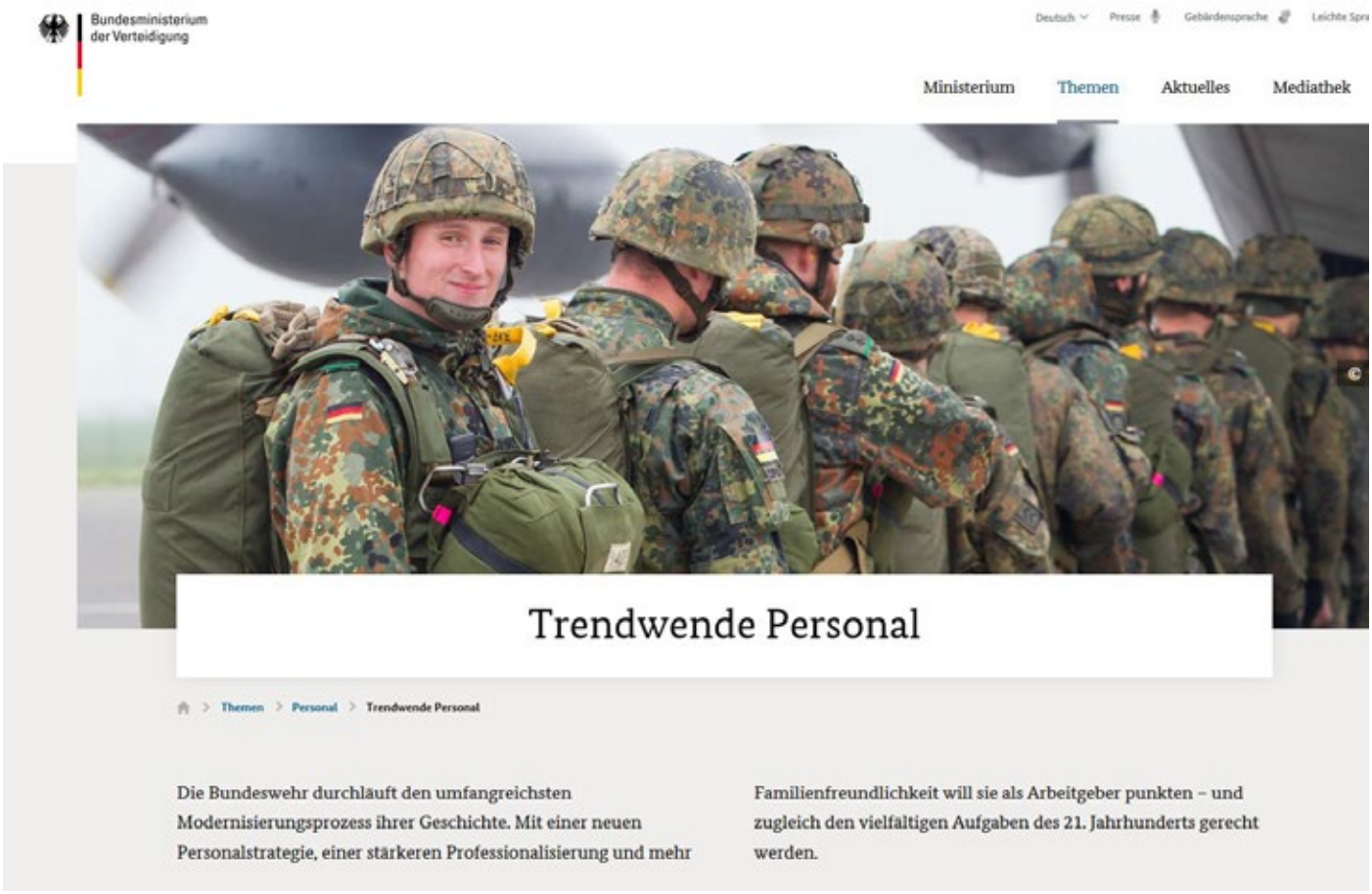
Eine weitere Mitgliedsfirma ist Systematic, die ihren Sitz in Köln hat und ein Ableger einer großen US-Firma ist. Systematic arbeitet mehrheitlich im Bereich E-learning und Healtcare, der Bereich Verteidigung ist daneben aber ebenfalls ausgeprägt. Das Unternehmen bietet ganze Software-Familien für den Einsatz in den Streitkräften an – von der Führung (Command and Control) über Kommunikation bis zur Logistik reicht das Aufgabenspektrum der Programmierung. Vorteil dieser Systeme mit internationalem Hintergrund ist die Interoperabilität mit anderen Staaten. Hier sind enge Verbindungen auch zu Geo-Informationssystemen zu sehen – wie sie z.B. von den Firmen esri (Bonn) und exelis (Harris Geospatial Solutions, Gilching) verkauft werden – Geoinformationssysteme, die wiederum an dem teuren Höhenmodell ansetzen, von dem oben die Rede war. Hierfür gibt es dann nicht nur kartenbasierte Anwendungen für den Handheld-Computer des „abgesessenen Kommandeurs“, sondern auch komplexe Analysetools, zugeschnitten auf den militärischen Bedarf. Damit kann man nicht nur die optimalen Überwachungsposten im Gefechtsfeld anhand der Höhenmodelle ermitteln, sondern über die geografisch basierte Analyse auch die Wahrscheinlichkeit von Bombenanschlägen vorhersagen.

In eine eine ganz ähnliche Richtung gehen auch die Produkte der Firma Rola aus Oberhausen – einer Firma aus dem Portfolio des Bonner Telekom-Konzerns – die sich an Polizeibehörden, Steuerfahndung, Network Media, Wirtschaft und das Militär wenden. Hier steht Informationsauswertung und -gewinnung im Vordergrund – nicht allein auf Basis von Geodaten, als vielmehr in der Auswertung großer unstrukturierter Datenbestände. Rola ist längst nicht die einzige Firma, die so etwas anbietet und auch hier verweise ich darauf, dass die entsprechenden Anwendungen leicht verändert für unterschiedliche Bereiche zur Verfügung stehen.

Als letzte Kategorie ließen sich Beraterfirmen anführen, die der Bundeswehr ihre Expertise in den Bereichen der Cybersicherheit anbieten wollen und deshalb auch in dem Verband vertreten sind. Oft sind es kleine Firmen, wie die Unternehmensberatung H&D aus München, die zum Teil erstaunlich weitreichende Angebote machen. Einige dieser Unternehmen bieten auch Penetrationstests an, mit denen die Strukturen der Bundeswehr auf Schwachstellen abgeklopft werden. Andere, wie die Firma Materna aus Dortmund, bieten auch die Konfiguration von Chatbots an, die zur automatisierten Kommunikation eingesetzt werden können.

SCHLUSSFOLGERUNGEN

Der Überblick zeigt, dass es die Bereitschaft auf Seiten der Bundeswehr zu geben scheint, viel Geld in Netze und Netzsoftware zu investieren und zwar sowohl physisch als



auch als Dienstleistung und als Wissen um Netzwerke – Kompetenzen werden erworben und lassen sich auch militärisch weiter verwenden. Es wird erhebliches Geld in die Auswertung von Informationen gesteckt, darunter Geoinformationssysteme, Datamining und Textanalyse sowie in die Verfügbarmachung dieses Wissens für den Soldaten vor Ort durch Mensch-Maschine-Schnittstellen. Der Blick auf den Branchenverband zeigt, dass die Industrie selbst an diesem Prozess und der Förderung der Bereitschaft zur militärischen Kooperation mitwirkt und diese in ihrem Sinne zu beeinflussen sucht. Dabei begibt sich die Industrie nicht nur in die Nähe des Militärs, sondern adaptiert deren Sichtweisen für die eigenen Produkte. Sie befördert den Umstand, dass das Militär in die Lage versetzt wird, die Privatsphäre aller auszuspionieren und Netzwerke zu überwachen/kontrollieren. Das Portfolio der Firmen zeigt zudem an, dass hier auch der Mittelstand bewusst und mit Nachdruck einbezogen werden soll – überall sonst spricht man von einer „Vereinheitlichung“ und „Reduktion der Marktakteure“, im Bereich „Cyber“ ist das Gegenteil der Fall: Je mehr Akteure, desto mehr unterschiedliche und damit flexible Lösungen.

Bezogen auf die Trendwende Personal kann man festhalten, dass die im Weißbuch eher vage angesprochenen neuen Modelle der Rekrutierung und Kooperation mit Wirtschaftsunternehmen zur Schließung eigener Fähigkeitslücken auf fruchtbaren Boden treffen. Wie diese Modelle aussehen, ist bisher noch weitgehend unspezifisch – da ist die zeitweise Übernahme von Mitarbeitern unterschiedlicher IT-Unternehmen durch die Bundeswehr genauso eine Überlegung, wie die Beauftragung von zivilen Unternehmen für spezifische Aufgaben.

Ganz entscheidend bei dem Gesagten ist für mich, dass die einstmals so hoch gehaltene Abgrenzung zwischen dem „zivilen“ Bedarf der Bundeswehr (weiße IT) und der grünen IT für das Militärische in der Auflösung begriffen ist. Sie war für „Herkules“ noch ausschlaggebend, verliert aber an Bedeutung. Mehr noch – die Bundeswehr schickt sich an, Kompetenzen zu erwerben oder eben auch als Dienstleistung einzukaufen, die die Übergänge in die zivile IT von Unternehmen, Behörden und Privatmenschen auflösen werden.

Der zweite wesentliche Punkt, der für mich aus den Recherchen folgt, ist nicht nur die technisch motivierte Entgrenzung, sondern auch die Idee, ein allumfassendes Lagebild erstellen zu wollen, das alle Faktoren des menschlichen Lebens umfassen soll. Die Cybertruppe ist sozusagen die Hilfstruppe zur Ausforschung aller Lebensumstände geworden – der technische Arm einer militärischen und damit weitgehend unkontrollierbaren geheimdienstlichen Tätigkeit. Für mich verblüffend ist es, dass zivile Firmen dies nicht nur mitmachen, sondern auch bereit sind, an dieser „Aufklärung“ mitzuwirken – und es sich bezahlen lassen.

REAL WAR AND FAKE NEWS: DIE KÄMPFE UM MOSSUL UND ALEPPO

VON: JOACHIM GUILLIARD

„Fake News“ sind in letzter Zeit zum Top-Thema geworden. Meist werden unter „Fake News“ nur frei erfundene oder stark verfälschte Nachrichten, also Falschnachrichten im engeren Sinne verstanden, die politisch motiviert und gezielt auf Täuschung angelegt sind. Sie werden zudem nur in den sogenannten „Sozialen Medien“ verortet, sowie in den Nachrichtenportalen gegnerischer Staaten. Geht es nach dem politischen Mainstream, so könnte man sie als die Falschmeldungen und Unwahrheiten definieren, die nicht von den etablierten Medien selbst verbreitet werden.

Nun steht natürlich außer Frage, dass die „Sozialen Medien“ einen besonders guten Nährboden für „Fake News“ bilden, wo sie sich leicht säen und sehr schnell verbreiten lassen. Wenn wir aber in der Geschichte zurückblicken, müssen wir feststellen, dass die Falschmeldungen, die die schlimmsten Schäden anrichteten, aus Politik und etablierten Medien selbst kamen bzw. von ihnen verbreitet wurden. Ein berühmt-berüchtigtes Beispiel dafür ist die sogenannte „Brutkasten-Lüge“, die von einer Werbeagentur kreierte Story über Babys, die irakische Soldaten 1990 in Kuwait aus Brutkästen gerissen hätten. Sie wurde damals von den meisten Medien weiter verbreitet und auch von Menschenrechtsorganisationen wie Amnesty International. Sie trug damals maßgeblich dazu bei, die öffentliche Meinung in den USA zugunsten des ersten US-Krieges gegen den Irak zu drehen. Weitere berühmte Beispiele sind die angeblichen Belege über irakische Massenvernichtungswaffen, die 2003 der damalige Außenminister Colin Powell dem UN-Sicherheitsrat vorlegte, oder die angeblichen Massaker im Kosovo und der „Hufeisenplan“, den Rudolf Scharping der jugoslawischen Regierung angedichtet hatte, um den NATO-Krieg gegen Jugoslawien zu rechtfertigen. Noch gut in Erinnerung sind sicherlich auch die Propagandameldungen über afrikanische Söldner und angeordnete Massenvergewaltigungen in Libyen, mit der Stimmung für den Libyenkrieg gemacht wurde.

Weit häufiger als mit eindeutigen Falschmeldungen, wird jedoch mit sehr einseitigen oder stark übertreibenden Beiträgen versucht, die gewünschte Stimmung für ein politisches Anliegen zu schaffen. Auch wenn es nicht so gewertet wird und auch leicht abzustreiten ist, ist das Weglassen essentieller Teile einer Geschichte, die zum Verständnis und zu ihrer Einordnung nötig sind, letztlich ebenfalls Fake, d.h. eindeutige, klare Desinformation. Dies wird besonders deutlich, wenn man sich die westliche Berichterstattung über die „Schlacht von Mossul“ im Irak zwischen Oktober 2016 und Juli 2017 im Vergleich zu den nahezu zeitgleich abgelaufenen Kämpfen um Ost-Aleppo in Syrien betrachtet.

Grünen-Chef Özdemir
"Assad und Putin bomben Syrien zurück in die Steinzeit"

"Anne Will" zum Syrienkrieg
Aleppo, Chiffre für moralisches Totalversagen

Offensive gegen IS-Miliz im Nordirak
"Die Befreiung Mossuls steht bevor"

29. September 2016, 16:24 Uhr Krieg in Syrien
"Assads Angriffe gelten Zivilisten, kein Zweifel"

Donnerstag, 20. Oktober 2016

IS auf dem Rückzug ins Stadtgebiet
Offensive auf Mossul geht weiter gut voran

Islamischer Staat
Iraker feiern "großen Sieg" in Mossul doch der IS scheint nicht ganz vertrieben

ALEPPO UND MOSSUL: BEISPIELE FÜR DOPPELMORAL UND PROPAGANDA

Wie stark solche Desinformationen zur Durchsetzung herrschender Politik hierzulande eingesetzt werden, lässt sich sehr gut am Umgang von Politik und Medien mit den Kämpfen um Mossul und Aleppo zeigen. Beide zählen zu den schlimmsten Schlachten in jüngster Zeit. Sie stehen aber nicht nur als drastische Beispiele für die Brutalität der Kriege in Syrien und dem Irak, sondern auch für eine extreme Doppelmoral in ihrer Bewertung und für eine Berichterstattung, die weit mehr an den strategischen Interessen der herrschenden Kreise im eigenen Land, als am tatsächlichen Kriegsgeschehen ausgerichtet ist. Wer Berichte über Mossul und Ost-Aleppo vergleiche, könne sehr viel über die Propaganda lernen, die wir konsumieren, rät der erfahrene Nahost-Korrespondent des britischen Independent, Patrick Cockburn.[1]

Die Ausgangslage war in den beiden großen Metropolen ähnlich. Sowohl Ost-Aleppo als auch Mossul standen unter Kontrolle radikaler islamistischer Kräfte. Beide wurden von Regierungstruppen mit ausländischer Unterstützung belagert, bombardiert und schließlich gestürmt. Die Darstellung von Politik und Medien hätte jedoch unterschiedlicher kaum sein können.

Die Schlacht um Mossul, wo sich nach Schätzung westlicher Geheimdienste 7.000 bis 10.000 Dschihadisten des sogenannten „Islamischen Staat“ (IS oder arab. despektierlich Daesch) unter rund eineinhalb Millionen Einwohnern verschanzt hatten, wurde durchgehend als Feldzug für die Befreiung begrüßt. Die Offensive zur Rückeroberung Ost-Aleppos hingegen, wo noch 150.000 bis 250.000 Bewohner verblieben waren, aus den Händen von rund 8.000 islamistischen Kämpfern, als ungerechtfertigter, grausamer, verbrecherischer Angriff auf die „Opposition“, die „Rebellen“ oder gar die gesamte Bevölkerung der Stadt verurteilt.

ALEPPO – „INBEGRIFF DES SCHRECKENS“

Den Charakter dieser „Opposition“ oder „Rebellen“ im Ostteil Aleppos blendete man dabei völlig aus, wie auch ihr tatsächliches Verhältnis zur Bevölkerung der Stadt. Man ließ so den Eindruck entstehen, es handele sich um fortschrittliche Kräfte und um Stadtviertel, die von der Mehrheit der Einwohner als „befreit“ angesehen würden. Ausgehend von diesem Narrativ, entwickelte sich die wohl größte Propagandaschlacht im Rahmen des Krieges in und gegen Syrien. „Aleppo!“ – der Name wurde in deutschen Medien, so Daniela Dahn, geradezu zum „Synonym für einen mythischen Kampf zwischen Gut und Böse.“[2]

Der Hintergrund für das Getöse war die enorme strategische Bedeutung, die der Kampf um die Hoheit über die zweitgrößte Stadt Syriens hatte. Die Niederlage der dortigen Milizen bedeutete faktisch das Ende des Regime-Change-Projektes und damit auch eine empfindliche Niederlage der NATO-Staaten und ihrer Verbündeten. Diese suchten daher den Preis für die syrische und russische Regierung so hoch wie möglich zu treiben, indem sie deren militärisches Vorgehen auf allen möglichen Ebenen skandalisierten. Mit Beginn der Offensive im September 2016 hatte die Berichterstattung im Westen nahezu einhellig nur noch den einen Tenor: Regierungstruppen und russische Luftwaffe lassen die Stadt in einem Inferno untergehen.

Aleppo wurde im Westen zum Inbegriff des Schreckens des Krieges in Syrien und für alle diejenigen, die ein direkteres Eingreifen des Westens anstreben, zum Symbol für eine hilflose internationale Gemeinschaft.[3] So überschrieb der Spiegel einen Artikel über eine Talk Show von Anne Will zum Thema „Ist Aleppo verloren?“ mit „Aleppo, Chiffre für moralisches Totalversagen“.[4]

Lauteten die Schlagzeilen zum Sturm auf Mossul „Die Offensive kommt schnell voran“ oder „die Befreiung steht bevor“, so titelte man über die syrische Offensive beispielsweise „Blut im grauen Staub Aleppos“ (Süddeutsche Zeitung[5]), „Außenminister Steinmeier: ‚Die Bilder aus Aleppo sind an Grausamkeit kaum zu überbieten‘“ (Spiegel Online[6]) oder „Grünen-Chef Özdemir: ‚Assad und Putin bomben Syrien zurück in die Steinzeit‘“ (Spiegel Online[7]). Zahlreiche hochrangige westliche Politiker nutzten die Berichte über Aleppo, um ihre Forderungen nach „Flugverbotszonen“ zu intensivierten, d.h. ausgedehnte Gebiete, die durch Androhung eines NATO-Krieges gegen Syrien den Kampfjets der US-Allianz vorbehalten bleiben sollten.[8]

Oft wurde nicht einmal erwähnt, dass sich die Offensive nur auf den Ostteil Aleppos richtete, in dem höchsten noch 15 Prozent der Einwohner lebten, und so der Eindruck erweckt, die ganze Stadt stehe vor dem Untergang, wie einst im Zweiten Weltkrieg – so ein häufig verwendeter Vergleich – Dresden.

ISLAMISTEN ALS »LETZTE HOFFNUNG«


SPIEGEL ONLINE POLITIK

Belagerte Stadt in Syrien: Die Islamisten sind Aleppos letzte Hoffnung

Von Christoph Sydow

Es war kein Geheimnis, dass die heroisierten Verteidiger (über die der SWR im November noch einmal den Propagandastreifen „Die letzten Männer von Aleppo“ zeigte[9]) überwiegend aus radikal-islamistischen und dschihadistischen Milizen bestanden, unter denen der syrische al-Qaida-Ableger, die in „Fatah asch-Scham“ umbenannte Al-Nusra Front, und Ahrar al Scham die dominierenden Kräfte waren. Gruppen also, die dem Daesch in Bezug auf reaktionäre islamistische Ideologie und Brutalität nicht viel nachstehen.

Westliche Medien scheuten sich jedoch nicht, sich ungeachtet dieses allgemein bekannten Hintergrunds offen hinter die al-Qaida nahen Kräfte zu stellen. So gab der Spiegel in einem Artikel durchaus an, dass die kampfstärksten Milizen „für einen syrischen Staat kämpfen, in dem ihre fundamentalistische Auslegung des islamischen Rechts, der Scharia“ gelten soll, bezeichnete sie aber dennoch als „Aleppos letzte Hoffnung“.[10]

Im Unterschied zu hiesigen Medien sah wohl kaum ein Bewohner Aleppos die von den Islamisten und Dschihadisten beherrschten Viertel als befreites Gebiet an. Die Enklave war auch keineswegs in Folge eines Aufstands in der Stadt selbst entstanden. In Aleppo hatte es 2011 keine nennenswerten Proteste gegen die Regierung gegeben. Die Metropole galt als Assad-Hochburg und blieb auch über ein Jahr lang von Unruhen verschont. Zum Verhängnis wurde ihr schließlich die Nähe zur Türkei. In der Grenzregion formierten sich die islamistischen Milizen und eroberten von dort aus den Osten der Stadt, bis zum Schluss über die nahe türkische Grenze gut versorgt. Das Gros der Bevölkerung der von ihnen besetzten Stadtteile flüchtete, die meisten in die von der Armee gehaltenen Viertel im Westen.

Allen Berichten von Betroffenen zufolge, die nicht mit den Islamisten sympathisieren – wie auch in der New York Times nachzulesen[11] – errichteten die Milizen ein islamistisches Terrorregime mit allem was dazugehört, vom Schleierzwang bis zu Scharia-Gerichten. Sie nutzten es als Basis, um unter Einsatz von Mörsern und Raketen, Autobomben und Selbstmordkommandos zu versuchen, in die benachbarten Viertel vorzustoßen. Die Mehrheit in Aleppo betrachtet daher die Vertreibung der „Terroristen“, wie sie in den Kommentaren und Interviews von Leuten aus Aleppo meist genannt werden, durchaus „als Befreiung“.[12]

NACHRICHTENHOHEIT DER DSCHIHADISTEN

Die romantisierende Darstellung der Dschihadisten als „Verteidiger der Freiheit“ der gesamten Stadt führte dazu, dass Quellen aus ihrem Umkreis eine enorme Glaubwürdigkeit zugebilligt bekamen – nicht nur bei den Medien, sondern auch bei Menschenrechtsorganisationen wie Amnesty International (AI) und Human Rights Watch (HRW). Dies führte beispielsweise dazu, dass HRW mehrfach Bilder zerstörter Gebäude und Straßenzüge zeigte, die die Auswirkungen von Fassbombenabwürfen demonstrieren sollten, die ganz woanders aufgenommen worden waren. Eines stammte z.B. aus dem kurdischen Kobani und eines sogar aus Gaza.[13]

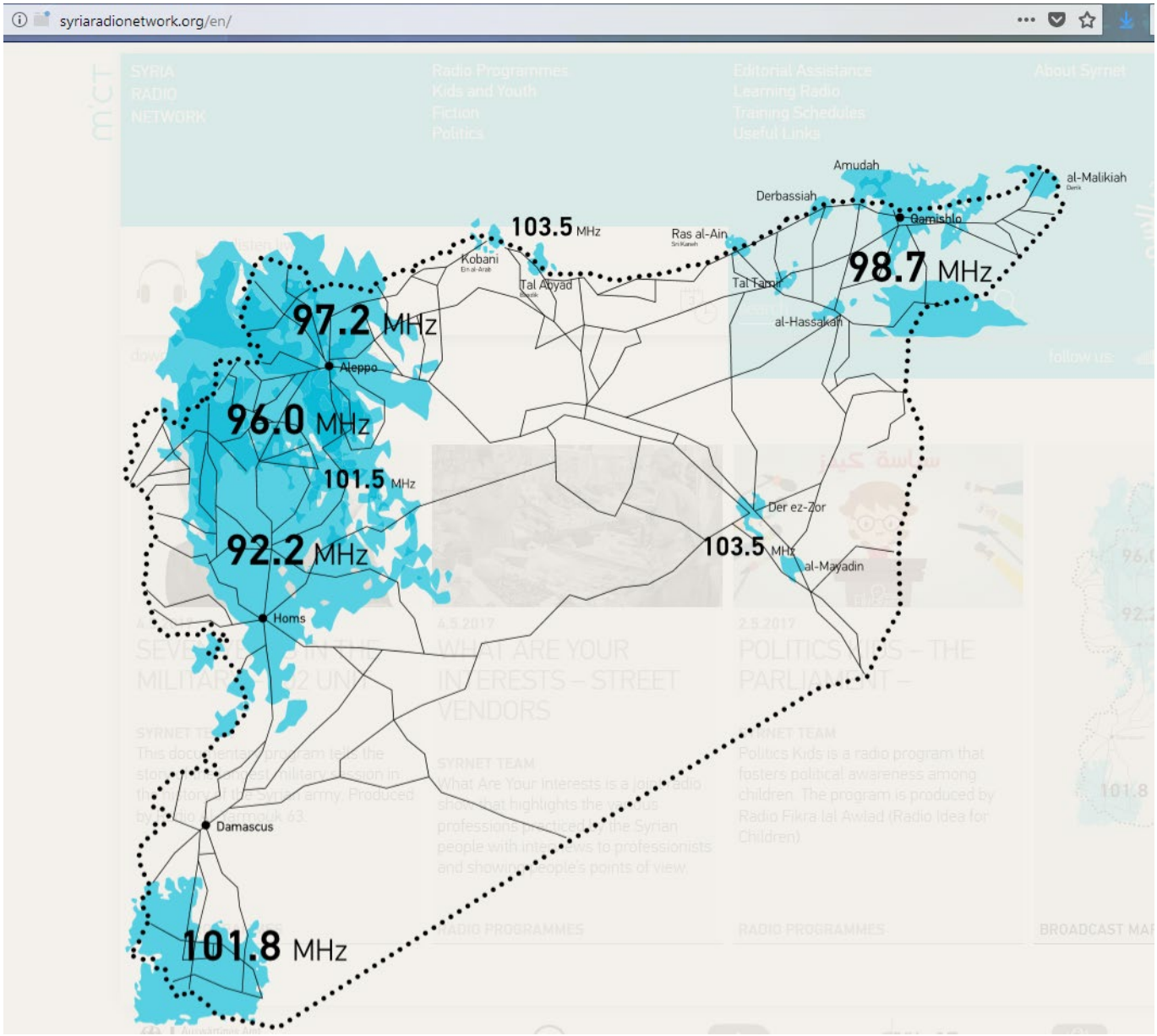
Egal ob es sich um Berichte über „Fassbomben-Abwürfe“, „Angriffe auf Krankenhäuser“ oder ähnliche Vorwürfe handelte, primäre Quellen waren in den meisten Fällen ausschließlich oppositionelle Gruppen, wie das „Aleppo Media Center“, die mehr oder weniger eng mit den Milizen verbandelt waren.

Unabhängige Journalisten hingegen konnten kaum in die von Regierungsgegnern kontrollierten Gebiete vordringen. In dieser Situation haben ausländische Medien – aus Naivität oder Eigeninteresse – zugelassen, wie früh schon Patrick Cockburn kritisierte, dass Leute, die nur mit dem Segen von al-Qaida-nahen Gruppen, wie Al Nusra-Front und Ahrar al-Sham vor Ort aktiv sein konnten oder gar direkt bei ihnen mitarbeiteten, die Berichterstattung dominierten.

PROFESSIONELLE PR-ARBEIT

Es wäre allerdings blauäugig anzunehmen, dass die ansprechende, professionelle und erfolgreiche PR-Arbeit allein das Werk der Milizen und verbündeter „zivilgesellschaftlicher Gruppen“ gewesen wäre. Arabische und westliche Regierungen haben von Beginn an ziemlich offen eine entscheidende Rolle bei der Finanzierung und Ausbildung regierungsfeindlicher Medieninitiativen gespielt. Häufig war, was als spontane Gründung eines unabhängigen Medienbüros durch lokale Journalisten, Bürgerrechtler, Hobbyfotographen und Medienaktivisten wirkte, von syrischen Exiloppositionsgruppen und westlichen NGOs in enger Zusammenarbeit mit westlichen Regierungsstellen aufgebaut worden. So wurde das Radio-Projekt „Syria Radio Network“ (Syrnet) von der Berliner Organisation „Media in Cooperation and Transition“ (MICT) mit Unterstützung des Auswärtigen Amtes entwickelt – kofinanziert u.a. vom Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, dem belgischen und französischen Außenministerium und der Friedrich-Ebert-Stiftung.[14]

Natürlich wird in allen Kriegen Desinformation betrieben, werden übertriebene Gräuelgeschichten produziert etc.. In Syrien aber, so das Fazit von Cockburn, der in den letzten Jahrzehnten viele Kriege und Konflikte beobachten



konnte, haben solche fabrizierten und absolut einseitige „Nachrichten“ die Berichterstattung zu einem Grad dominiert, wie vermutlich nie zuvor seit dem Ersten Weltkrieg.

DESINFORMATION UND FAKES IM MAINSTREAM

Im Fall Aleppo wurde hauptsächlich durch extreme Einseitigkeit und Weglassen wesentlicher Aspekte des Geschehens Stimmung gegen das Vorgehen der syrischen und russischen Streitkräfte gemacht. Die Folgen wurden mithilfe der Berichte, Bilder und Videos oppositioneller Gruppen massiv aufgebauscht, während die Angriffe der sogenannten „Rebellen“ unerwähnt blieben, oft sogar die Präsenz bewaffneter Gegner generell. Auf diese Weise entstand zwangsläufig der Eindruck, die Angriffe der Regierungstruppen und ihrer russischen Verbündeten würden sich durchweg auf zivile Ziele richten. Praktisch alle Opfer und Kriegsschäden wurden der syrischen und der russischen Regierung angelastet, so als würden diese allein Waffen einsetzen. Es wurde auch kein Gedanke darauf verschwendet, dass die Dauer und Intensität der Kämpfe nicht zuletzt eine Folge der fortgesetzten Unterstützung der islamistischen Milizen durch NATO-Staaten und ihre regionalen Verbündeten war.

Viele der von der „Opposition“ verbreiteten Berichte konnten aber auch direkt als Fälschung oder Irreführung entlarvt werden. Wenn man die Berichterstattung zu Aleppo überfliegt, so wird offensichtlich, dass ein wesentlicher Teil rein auf Emotionalisierung zielte und dies vor allem über Geschichten mit Kindern. So machte im Dezember 2016 das Bild eines tapferen kleinen Mädchens in den „Sozialen Medien“ die Runde, das in den Ruinen von Aleppo zwischen Leichen herumirrte. Das scheinbar aktuelle Foto entstand jedoch bereits 2014 im Libanon und stammt aus einem inszenierten Videoclip der libanesischen Sängerin Hiba Tawaji über den „Arabischen Frühling“.

Ein ähnlich lehrreiches Beispiel ist die Geschichte um das rührende Bild von Omran, dem „Jungen von Aleppo“, ein Bild, das, wie es Michael Lüders einmal beschrieb, „an emotionaler Wucht kaum zu überbieten“ ist. Es wurde im August 2016 geradezu zur Ikone der Schlacht um Aleppo. Es gab kaum eine Zeitung, die das Bild nicht veröffentlichte, oft sogar mehrfach.[15] Omran sei, so der Fotograf, durch einen syrischen oder russischen Luftangriff verletzt, von Helfern der sogenannten „Weißhelme“ aus den Trümmern geborgen und in ein Krankenhaus gebracht worden.

Sein Vater, Mohammad Daqneesh, bestritt allerdings die Geschichte umgehend: sein Sohn sei nur leicht verletzt gewesen und dies keineswegs durch einen Luftangriff. Er beschuldigte die „Weißhelme“ und die internationalen Medien, seinen Sohn für Propagandazwecke missbraucht zu haben.

Über den interessantesten Aspekt dieser Geschichte wurde auch später kaum berichtet: der Fotograf, Mahmud Raslan hatte kurz vor diesem Foto ein Selfie gepostet, das ihn grinsend mit Angehörigen der berüchtigten Dschihadistenmiliz „Harakat Nur ad-Din as-Sanki“ zeigte. Unter diesen wiederum waren zweifelsfrei auch zwei Männer, die vier Wochen zuvor den zwölfjährigen Jungen Abdallah Isa für ein Propagandavideo geköpft hatten. Dieser Raslan arbeitete im „Aleppo Media Center“ (AMC), das zu den wichtigstes Informationsquellen der westlichen Medien in Aleppo zählte. Gehandelt wird es als „unabhängiges Netzwerk“ sogenannter „Bürgerjournalisten“ – es steht jedoch fest im Lager der Regimegegner und ist eng vernetzt mit den Dschihadisten. Gegründet wurde es mit Hilfe der „Syrian Expatriates Organisation“ (SEO), die ihren Sitz in einer Straße Washingtons hat, in der sich die PR- und Lobbyfirmen in der US-Hauptstadt konzentrieren, und die wohl auch erhebliche Summen von US-amerikanischen Regierungsstellen erhält.[16] Laut ihrer Selbstdarstellung ist sie neben der finanziellen Hilfe seit Oktober 2012 auch für die Koordinierung des AMC und für die Bereitstellung technischer und logistischer Hilfe verantwortlich.[17] Weitere Geldgeber sind Paris und Brüssel, die das AMC über den „Syrian Media Incubator“ des „Canal France International“, einem Organ des französischen Außenministeriums, unterstützen.[18]

DIE „WEIßHELME“ - DAS ERFOLGREICHSTE PR-UNTERNEHMEN

Noch besser ausgestattet und wesentlich prominenter als das AMC ist die zweite Organisation, die bei der Inszenierung von Omran als Bomben-Opfer mitwirkte: die sogenannten „Weißhelme“. Auch sie versorgen die westlichen Medien fleißig mit Berichten und Bild-Material aus den Kampfgebieten. Entgegen ihrer Selbstdarstellung handelt es sich bei den „Weißhelmen“ nicht um eine originär syrische Organisation. Sie wurde von einem ehemaligen britischen Offizier, James Le Mesurier, gegründet, der zuvor in mehreren Kriegen in der Grauzone zwischen Spezialeinheiten und Geheimdiensten sowie bei privaten Militärdienstleistern tätig war und heute u.a. als Militärberater für Katar arbeitet.[19] Ihren Hauptsitz hat sie in Großbritannien. Das Geld kam zunächst aus den Golfstaaten, anschließend überwiegend aus Washington und London, die ihr jeweils bereits über 30 Millionen zukommen ließen.[20] Auch das deutsche Auswärtige Amt hatte Ende 2016 schon 12 Millionen Euro überwiesen, knapp ein Zehntel der deutschen – im Haushalt als „Stabilisierungsmittel“ ausgewiesenen – Gelder für die Umsturzbemühungen in Syrien in Höhe von 141 Millionen Euro.[21] Während etablierte Hilfsorganisationen mit sinkender staatlicher Unterstützung zu kämpfen haben, hat diese seltsame Zivilschutztruppe in den letzten vier Jahren insgesamt schon weit über 100 Millionen Euro erhalten. Einen großen Teil der Gelder investieren sie offensichtlich in die professionelle Medienarbeit.

Die „Weißhelme“ helfen zwar auch Verletzten, jedoch nur in Gebieten, die unter Kontrolle regierungsfeindlicher Milizen stehen mit denen sie auch personell eng verflochten sind. Auf zahlreichen Bildern und Videos sind sie mit Al-Nusra Fahnen zu sehen, wie sie zusammen mit islamistischen Kämpfern Erfolge gegen Regierungstruppen feiern oder mit „Victory-Zeichen“ über erschossenen Soldaten posieren.[22] Zudem kann man einige ihrer Aktivisten, die in Videos beim Einsatz in ihren weißen Uniformen zu sehen sind, auf anderen Fotos auch als bewaffnete Kämpfer erkennen.[23] Die „Weißhelme“ scheinen sogar bei Hinrichtungen und Folter zu assistieren. So zeigt ein im Internet kursierendes Video, wie einige von ihnen der Exekution eines Mannes durch Al Nusra-Kämpfer beiwohnen und anschließend seine Leiche wegtragen.[24] Ein Medienaktivist der Organisation Muawiya Hassan Agha filmte die Folterung zweier gefangener Soldaten, die anschließend ermordet wurden. Abu Jaber Shaykh, der Chef des von der Al-Nusra Front angeführten Bündnis Hai‘at Tahrir asch-Scham, scheint daher nicht übertrieben zu haben, als er die „Weißhelme“ anlässlich des sechsten Jahrestages des Krieges, als „verborgene Soldaten der Revolution“ pries.[25]

All dies schadete jedoch ihrer Popularität bisher so wenig, wie der häufige Nachweis, dass Bilder, die sie verbreiten, nicht das zeigen, was sie vorgeben.[26] Sie erhielten dennoch den Alternativen Nobelpreis und eine Kurz-Doku über sie einen Oscar. Im Dezember 2016, neun Monate nach ihrer Ehrung durch Dschihadisten-Führer Abu Jaber, überreichte der damalige Außenminister (Frank-Walter) Steinmeier ihrem Chef Raed al-Saleh den „Deutsch-französischen Preis für Menschenrechte und Rechtsstaatlichkeit“.[27]

DAS REALE KRIEGSGESCHEHEN IN ALEPPO

Auch wenn man die gesicherten Erkenntnisse über das Kriegsgeschehen in Aleppo betrachtet, so war die Offensive auf den Ostteil Aleppos mit Luftangriffen, Artilleriebeschuss und Straßenkämpfen für die verbliebene Bevölkerung selbstverständlich ein Horror, der große Verwüstungen in dieser Stadt mit ihrer jahrtausendealten Geschichte anrichtete und Tausende tötete. Horror waren aber auch die pausenlosen Raketen- und Mörserangriffe der vom Westen unterstützten „Rebellen“ auf die Stadtviertel im Westen gewesen.

Nach Einschätzung der UNESCO waren nach Ende der vier Jahre andauernden Kämpfe 60% der Altstadt, durch die die Front verlief, schwer beschädigt und bis zu 30% völlig zerstört.[28] Es ist jedoch bewusste Irreführung, wenn dafür ausschließlich die syrischen und russischen Streitkräfte verantwortlich gemacht werden. So wurde bei den

vielen anklagenden Bildern über die Zerstörungen in Aleppo völlig verschwiegen, dass ein erheblicher Teil der Schäden bereits im Sommer 2012 beim Eindringen der islamistischen Milizen nach Ostaleppo verursacht wurde. Teile der Altstadt waren damals bereits durch Feuer verwüstet und der berühmte Souk, das weltgrößte überdachte Marktviertel, von den Islamisten geplündert und gebrandschatzt worden.[29]

Die meisten neueren Schäden waren den Beobachtungen des schwedischen Konfliktforschers Jan Oberg zufolge, der die befreiten Gebiete nach Abzug der Milizen in Augenschein nahm und fotografierte, während der Straßenkämpfe entstanden. Er schätzt, dass – entgegen dem durch die Medien vermittelten Eindruck – höchsten 10 Prozent der Zerstörungen auf das Konto von Luftangriffen gingen.

Das Ende der Kämpfe hat bis Dezember 2017 bereits rund 500.000 aus Aleppo geflohene Einwohner zur Rückkehr bewegt. Über 300.000 wechselten auch wieder in den Ostteil. Die Ruinen sind dort zwar noch allgegenwärtig, die Infrastruktur ist aber genügend wiederhergestellt, so dass sie mit der Instandsetzung ihrer Häuser und Wohnungen beginnen konnten.

DAS GEGENSTÜCK: DIE „BEFREIUNG MOSSULS"

Von einer so raschen Rückkehr wie nach Aleppo können die früheren Bewohner des Westens von Mossul nur träumen. Das Ausmaß der Verwüstung ist wesentlich größer als in Ost-Aleppo. Hier wurden beim Sturm der Millionenstadt, die etwa so groß wie Hamburg ist, bis zu 80 Prozent der Gebäude zerstört.[30] Video-Aufnahmen und Fotos zeigen westlich des Tigris eine einzige Trümmerlandschaft.[31]

Nach Einschätzung der UNO stellt das Ausmaß der Zerstörungen alles Bisherige im Irak in den Schatten. Von den 54 Wohndistrikten Westmossuls wurden 15 völlig dem „Erdboden gleichgemacht" und dabei fast 32.000 Häuser komplett zerstört. In den 23 mittelschwer und 16 leicht beschädigten Distrikten kommen weitere 16.000 vollständig zerstörte Gebäude hinzu. Insgesamt wurden dadurch vermutlich Wohnungen für weit mehr als eine halbe Million Menschen zertrümmert. Die Lage in der einstigen Metropole, die wie Aleppo auf eine jahrtausende lange Geschichte zurückblickt, sei „die größte Herausforderung, der sich die UNO je gegenüber sah", so Lise Grande, die Humanitäre Koordinatorin der UNO im Irak.[32]

UM JEDEN PREIS – ZERSTÖRUNGEN UND ZIVILE OPFER DURCH US-ALLIANZ

Der größte Teil der Zerstörungen dürfte Berichten zufolge auf den Artillerie-Beschuss mit Mörsern und Raketen durch die irakischen Truppen zurückzuführen sein. Ein weiterer geht auch hier – wie in Aleppo – auf das Konto der Dschihadisten. Ein erheblicher Teil der betroffenen Gebäude war aber, wie Aufnahmen der betroffenen Viertel zeigen, eindeutig durch Bombardierungen aus der Luft zerstört worden.[33] Die US-geführte Allianz aus NATO-Staaten, Australien, Jordanien und Marokko hatte den Bodentruppen in den letzten Wochen den Weg Meter für Meter regelrecht freigebombt – ohne Rücksicht auf hunderttausende Bewohner, die in den dichten Stadtvierteln eingeschlossen waren. Viele konnten erst in den letzten Tagen aus dieser Hölle entkommen. Insgesamt wurden im Laufe des fast neun Monate dauernden Angriffs über eine Million Menschen aus der Stadt getrieben.

Die Trump-Regierung eskalierte den brutalen Luftkrieg weiter, indem sie Mitte Mai 2017 das „Einkreisen und Auslöschen" des Daesch als neue Taktik anordnete. In den NATO-Staaten gilt mittlerweile generell die Rückkehr ausländischer Kämpfer von Terrortruppen wie dem Daesch als größtes Sicherheitsrisiko. Durch eine sogenannte „Auslöschungskampagne", d.h. durch gezielten Abschuss vor Ort, will Washington dieses Risiko minimieren.[34]

Die Zahl der Opfer in Mossul ist schwer zu schätzen. Irakisch-kurdische Geheimdienste gehen von mindestens 40.000 Zivilisten aus. Einer Untersuchung der UN-Menschenrechtskommission zufolge wurde mindestens jeder vierte Zivilist, der bei den Kämpfen starb, durch Luftangriffe der US-geführten Koalition getötet.[35]

Während rund 200.000 Flüchtlinge aus dem bereits im Januar 2017 zurückeroberten und nicht so stark zerstörten Ostteil der Stadt mittlerweile zurückkehren konnten, sitzen noch über 750.000 Mossulaner in Zeltlagern fest – und das auf unbestimmte Zeit. Die flächendeckende Zerstörung von Wohnungen, Geschäften, Krankenhäusern, Schulen etc., macht eine baldige Rückkehr unmöglich.[37]

Betrachtet man die Berichterstattung zu Mossul so fällt hier das völlige Fehlen von Mitgefühl für die Eingeschlossenen auf, deren Zahl meist recht niedrig angesetzt wurde. Aus Mossul kamen so gut wie keine Bilder und Berichte über die Verwüstungen, die die massiven Bombardierungen anrichteten, keine Leidensgeschichte Betroffener und keine Bilder von toten oder verwundeten Kindern. Eingebettete Journalisten gaben meist nur die Erfolgsmeldungen beim Vorrücken weiter. Bilder zeigen feiernde Soldaten und schiitische oder kurdische Milizionäre.

Kaum erwähnt wurden die Konflikte zwischen der sunnitischen Bevölkerung in Mossul und Umgebung, die es dem Daesch überhaupt ermöglichten, sich festzusetzen und die daraus resultierende Abneigung gegen die „Befreier", insbesondere gegen die schiitischen und kurdischen Milizen. Absolut unkritisch wurde die Schlacht um Mossul als Kampf einer demokratisch gewählten Regierung gegen den Daesch dargestellt, für den sie völlig zu Recht die uneingeschränkte Unterstützung der US-geführten Anti-IS-Koalition erhalten habe. Trotz zahlreicher glaubwürdiger Berichte der UNO und von Menschenrechtsgruppen war keine Rede davon, dass dieser Kampf von schiitischen Kräften, die die Regierung dominieren und das Gros der Truppen stellten, durchaus als Kampf gegen die unbotmä-

ßigen Sunniten generell geführt wurde. Weitgehend ignoriert wurden auch die im Windschatten der Rückeroberung durchgeführten Vertreibungen von Sunniten aus ethnisch und konfessionell gemischten Gebieten.[38]

Die Berichterstattung war stattdessen – mit wenigen Ausnahmen – so ausgerichtet, dass eine Alternative zum Sturm Mossuls um jeden Preis – wie es Amnesty International bezeichnete[39] – schlicht nicht denkbar war.

ANMERKUNGEN

1 Patrick Cockburn: Compare the coverage of Mosul and East Aleppo and it tells you a lot about the propaganda we consume, independent.co.uk vom 21.10.2016.

2 Karin Leukefeld: Aleppo: Medien nach Scheitern des „syrischen Bengasi-Plans“ verstummt, deutsch.rt.com vom 26.1.2017.

3 Gudrun Harrer: Der Fall von Aleppo: Nicht das letzte Kapitel, derstandard.at vom 13.12.2016;
Dominic Johnson: Rolle des Westens im Syrien-Krieg: Nicht dieses Foto ist schrecklich, taz.de vom 19.8.2016.

4 Mathias Zschaler: „Anne Will“ zum Syrienkrieg: Aleppo, Chiffre für moralisches Totalversagen, spiegel.de vom 10.10.2016.

5 Paul-Anton Krüger: Syrien-Krieg: Blut im grauen Staub Aleppos, sueddeutsche.de vom 26.9.2016.

6 Außenminister Steinmeier „Die Bilder aus Aleppo sind an Grausamkeit kaum zu überbieten“, spiegel.de vom 9.8.2016.

7 Annett Meiritz und Roland Nelles: Grünen-Chef Özdemir: „Assad und Putin bomben Syrien zurück in die Steinzeit“, spiegel.de vom 15.10.2016.

8 Z.B. Norbert Röttgen (CDU), Vorsitzender des Auswärtigen Ausschusses des Bundestags bei Anne Will (Mathias Zschaler: „Anne Will“ zum Syrienkrieg: Aleppo, Chiffre für moralisches Totalversagen, spiegel.de vom 10.10.2016).

9 Die letzten Männer von Aleppo, ardmediathek.de vom 09.11.2017.

10 Christoph Sydow: Belagerte Stadt in Syrien: Die Islamisten sind Aleppos letzte Hoffnung, spiegel.de vom 2.8.2016.

11 Robert F. Worth: Aleppo After the Fall: As the Syrian civil war turns in favor of the regime, a nation adjusts to a new reality, nytimes.com vom 24.5.2017.

12 Bischof: „Aleppo ist wieder eine geeinte Stadt“, de.radiavaticana.va vom 14.12.2016; Krieg in Syrien - Teil eines Weltkriegs - Interview mit Erzbischof Joseph Tobji von Aleppo, nrhz.de vom 26.10.2016; Jan Oberg: Humans in liberated Aleppo - December 11-12, 2016, janoberg.me vom 29.12.2016.

13 Siehe Joachim Guilliard: „Fassbomben“ in Syrien: parteiische Berichte, einseitige Vorwürfe und Doppelmoral, jghd.twoday.net vom 26.1.2016.

14 Siehe „About“ auf der MICT-Homepage www.mict-international.org sowie Martin Schneider: Radio für Syrien - Der Kasten, der in den Krieg sendet, sueddetusche.de vom 21.10.2015.

15 Michael Lüders: Der Krieg in Syrien und die blinden Flecken des Westens, blaetter.de vom März 2017.

16 Tim Anderson: The Omran Deception, telesurtv.net vom 31.8.2016.

17 Siehe „Development & Support Committee” auf der SEO-Homepage syrian-expatriates.org.

18 Der Canal France International (CFI, www.cfi.fr), zunächst für Fernsehsendungen im frankophonen Afrika zuständig, kümmert sich heute um den Aufbau von Medien in Afrika und anderen Ländern im Süden. Zur Förderung oppositioneller syrischer Mediengruppen betreibt er den „Syrian media incubator”. Als Basis wurde aufgrund der Nähe zu Aleppo die türkische Grenzstadt Gaziantep gewählt. Sein wichtigstes Projekt ist das AMC (s. Aleppo Media Center set to launch its radio station in northern Syria, cfi.fr vom 18.12.2015 und Franz. Außenministerium: A new generation of journalists in Gaziantep, diplomatie.gouv.fr vom 18.9.2015).

19 Scott Ritter: The ‘White Helmets’ and the Inherent Contradiction of America’s Syria Policy, truthdig.com vom 5.10.2016 und Jan Oberg: Just how grey are the White Helmets and their backers?, blog.transnational.org vom 1.11.2016.

20 Supporting Syrians who are struggling for a future Syria based on democratic governance and respect for human rights, usaid.gov vom 12.6.2017 und Conflict, Stability and Security Fund. In: House of Lords Hansard. UK Parliament, Column 720 vom 2.11.2016

21 Factsheet – Hilfe für Syrien Stand 2016, auswaertiges-amt.de vom 30.3.2017.

22 Siehe u.a. Prof Marcello Ferrada de Noli (Swedish Professors & Doctors for Human Rights): Should UN consider White Helmets a politically neutral organization, and its allegations as credible sources by UN investigative panels on Syria?, theindicter.com vom 30.11.2017 und Vanessa Beeley: White Helmets: Hand in Hand with Al Qaeda and Extremist Child Beheaders in Aleppo, 21stcenturywire.com vom 12.3.2017.

23 Double Life of White Helmets: Volunteers by Day, Terrorists by Night (Photos), southfront.org vom 29.9.2016.

24 So-called “White Helmets” facilitate.an al Nusra execution, liveleak.com vom 6.5.2015.

25 Chef von Al-Qaida in Syrien lobt die Weisshelme als „versteckte Soldaten der Revolution“ (mit dt. u. engl. Untertiteln), antikriegTV (youtube.com) vom 9.5.2017.

26 Siehe u.a. Jens Bernert: Die Lügen der „Weißhelme“, rubikon.news vom 12.11.2017.

27 Reporter ohne Grenzen wollen kritische Pressekonferenz in Genf über syrische Weißhelme verhindern, de.rt.com vom 28.11.2017.

28 UNESCO: 30 percent of Aleppo’s ancient city destroyed, usnews.com vom 20.1.2017.

29 Souk burns as Aleppo fight rages, irishtimes.com vom 29.9.2012; Historische Stadt in Gefahr – Aleppo in Syrien - Feuer vernichtet Schatz der Menschheit, sueddetsche.de vom 1.10.2012.

30 Mosul’s capture sees ISIS vanquished – but at a terrible cost, airwars.org vom 1.7.2017.

31 Alexandra Genova: Picture Stories: Among the Ruins of Mosul, nationalgeographic.com vom 14.7.2017.

32 Iraq faces vast challenges in securing, rebuilding Mosul, arabnews.com vom 3.8.2017.

33 Siehe u.a. Patrick Cockburn: The massacre of Mosul: …, a.a.O., AI, At any cost: …

34 US plan to ‘annihilate IS’ raises questions over civilian toll, larger strategy, dw.com vom 21.5.2017.

35 Mehr zum Sturm auf Mossul siehe meine Artikel Befreiung um jeden Preis - Der Irak nach der verheerenden Schlacht um Mossul, jghd.twoday.net von August 2017 und Mossul in Ruinen – Konflikte verschärft, jghd.twoday.net vom September 2017.

36 UN Migration Agency Identifies Additional Displaced Population from West Mosul, iom.net vom 14.7.2017; UN Migration Agency: Over 830,000 Remain Displaced Outside Mosul, germany.iom.net vom 28.7.2017.

37 Humanitarian situation dire in ‘liberated’ Mosul, Level of destruction in Mosul’s Old City is almost total, aljazeera.com vom 10.7.2017; UNO: Mossul ist ein Schlachtfeld, swr.de vom 28.7.2017.

38 Mehr dazu in meiner ausführlichen Studie: Die Schlacht um Mossul – Der Irak zerrissen durch den Krieg gegen den „Islamischen Staat“, interne Konflikte und äußere Intervention, IMI, 3. Juli 2017, aktualisiert am 9. August 2017.

39 At any cost: The civilian catastrophe in West Mosul, Iraq, amnesty.org vom 11.7.2017.

Verzerrungen in der außenpolitischen Berichterstattung
Einige Erklärungsansätze

von: Christopher Schwitanski

Die Berichterstattung der deutschen Leitmedien über internationale Konflikte unter Beteiligung der Bundeswehr oder des Militärs anderer Nato-Staaten sowie die überwiegend unkritische Thematisierung der ökonomischen Ordnung haben in den vergangenen Jahren immer wieder zu Kritik an Medien und ihrer Berichterstattung geführt. Insbesondere im Zuge des Konflikts in der Ukraine kam es wieder zu massiver Kritik an der Berichterstattung.

Der Fokus des vorliegenden Beitrags wird vor diesem Hintergrund weniger auf der inhaltlichen Ebene der medialen Berichterstattung liegen, sondern verschiedene Erklärungsansätze darstellen, die sich aus einer kritischen Perspektive mit der medialen Nachrichtenproduktion auseinandersetzen und auf struktureller Ebene zu erklären versuchen, wie es zu Verzerrungen in der Berichterstattung kommen kann. Dabei können weder sämtliche Beiträge zu diesem Thema, noch die hier ausgewählten erschöpfend dargestellt werden, sondern es soll vielmehr ein erster Einstieg in die Thematik geboten werden.

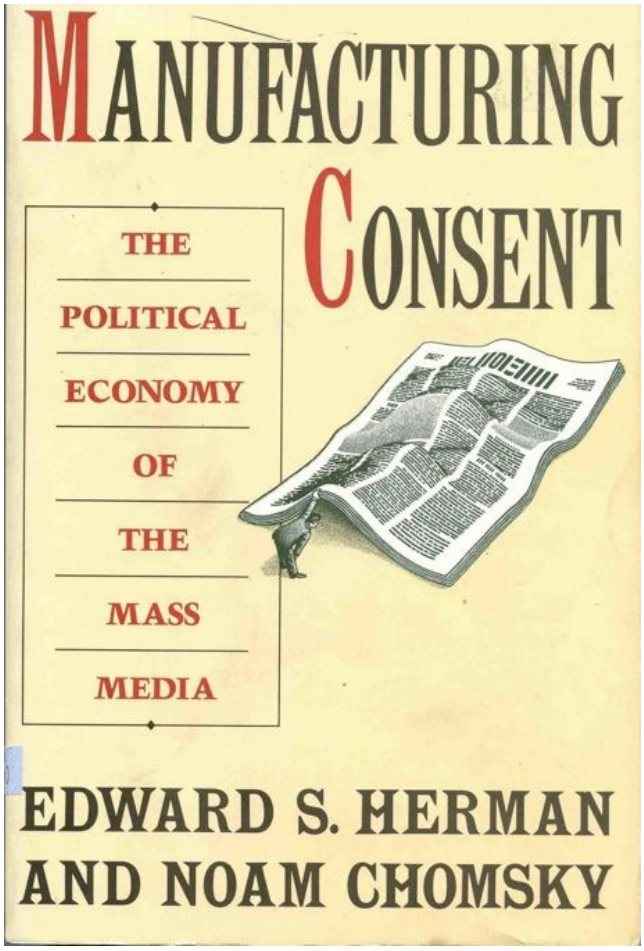
Die ökonomische Struktur der Massenmedien

Bezüglich der Frage, wie es zu Schieflagen in der medialen Berichterstattung kommt, finden sich zunächst im amerikanischen Raum verschiedene Untersuchungen und Erklärungsansätze.

So veröffentlichten der Ökonom und Medienanalyst Edward S. Herman und der Linguist Noam Chomsky 1988 das Buch „Manufacturing Consent: The political economy of the mass media“, dessen Kernthese zufolge das amerikanische Mediensystem primär den politischen und wirtschaftlichen Eliten des Landes als Sprachrohr dient und die Berichterstattung dementsprechend ideologischen Verzerrungen unterliegt. Als zentrale Ursache hierfür benennen die Autoren die ökonomische Struktur der Medien, aus welcher sie ein sogenanntes Propagandamodell ableiten. Dieses setzt sich aus fünf Filtern zusammen, die Informationen passieren müssen, ehe sie als Nachrichten publiziert werden.[1]

Den ersten Filter bilden die (wirtschaftlichen) Interessen der marktbeherrschenden Medienkonzerne und derer Anteilseigner sowie die Auswahl des führenden Personals in Einklang mit der ideologischen Ausrichtung des Konzerns. Der zweite Filter problematisiert die Abhängigkeit von Anzeigen und Werbetreibenden als Haupteinnahmequellen der Medien, aufgrund dessen sich die Publikationen stärker an den Interessen selbiger als an denen der Rezipienten orientieren. Der dritte Filter thematisiert die Abhängigkeit großer Medien von Informationen aus Regierungskreisen, Wirtschaft und regierungsnahen Experten. Hierzu gehören auch Institutionen, die nicht nur hochaktuelle (PR-)Informationen liefern, sondern darüber hinaus allgemein als vertrauenswürdig wahrgenommen werden. Dadurch könnten Kapazitäten für umfassende Faktenchecks eingespart und möglicher Kritik an abweichenden Berichten vorgebeugt werden, wodurch sich das Risiko erhöht, dass die Einschätzungen populärer Quellen unhinterfragt übernommen werden. Als weiteren Filter sehen Herman und Chomsky Möglichkeiten der direkten Einflussnahme und Bekämpfung unliebsamer Medienpositionen durch das Aufkündigen von Werbeverträgen, direkte Beschwerden und der Finanzierung von medialen Gegenkampagnen. Den fünften Kontrollmechanismus bildet (vor dem historischen Hintergrund der Publikation der Theorie) der Antikommunismus als zentrale staatliche Ideologie zur Bekämpfung unliebsamer Positionen und politischer Gegner. Eine Funktion, die im Rahmen des Modells heute in ähnlicher Weise der Krieg gegen den Terror erfüllt.

Das Modell von Herman und Chomsky berücksichtigt eine ganze Reihe möglicher Einflussfaktoren auf das mediale Geschehen, allerdings sei angemerkt, dass es u. a. aufgrund seiner beschränkten empirischen Nachweisbar-



keit umstritten ist. So konnten die Autoren zwar anhand zahlreicher Beispiele Auslassungen und einseitige Interpretationen politischer Ereignisse in den amerikanischen Leitmedien nachweisen, diese sind allerdings nicht notwendigerweise kausal auf die fünf attestierten Filter zurückzuführen.

INDEXING: DIE MEDIENBERICHTERSTATTUNG ALS SPIEGEL DES POLITISCHEN DISKURSES

Während das Propagandamodell die Ursachen für eine elitennahe Berichterstattung in der ökonomischen Struktur der Medien verortet, findet sich im amerikanischen Raum ein weiterer Ansatz, der diese über das Verhalten der Journalisten erklärt. Die vom Politikwissenschaftler W. Lance Bennett entwickelte Indexing-Hypothese geht davon aus, dass die amerikanischen Leitmedien sich in ihrer Berichterstattung primär auf die Wiedergabe von Positionen innerhalb des politischen (Eliten-)Diskurses beschränken.[2] Sind die politischen Parteien über ein Thema zerstritten, so bilden dem Modell zufolge auch die Medien mehr kontroverse und unterschiedliche Positionen zu diesem Thema ab. Stehen Regierung und Opposition dagegen geeint da, so sind auch auf Seiten der Medien wenige kritische Gegenpositionen zu erwarten. Ursächlich hierfür kann laut Bennett das intuitive Aufgreifen politischer Standpunkte sein, welches den jeweiligen Bericht vor Kritik schützt, da nur die Positionen der Politik wiedergegeben werden. Möglich ist weiterhin auch eine bewusste Entscheidung, sich auf die vorherrschenden politischen Positionen zu beschränken, sofern man diese als einzig relevante innerhalb des demokratischen Systems ansieht.

Die zentrale Vorhersage der Indexing-Hypothese konnte Bennett zunächst anhand der Berichterstattung der New York Times über die Finanzierung der Contras in Nicaragua durch die amerikanische Regierung bestätigten: Während der Widerstand gegen die Unterstützung der Contras durch die CIA Anfang der 80er Jahre im Kongress zunächst groß war, wurden auch in der Berichterstattung der New York Times häufig kritische Positionen wiedergegeben. Mit der Zerschlagung der Opposition im Kongress verschwand auch die kritische Perspektive aus der Berichterstattung, obwohl Meinungsumfragen zufolge nach wie vor die Bevölkerungsmehrheit eine Unterstützung der Contras ablehnte.[3] Zahlreiche weitere Untersuchungen konnten die inhaltlichen Vorhersagen aus Bennetts These an verschiedenen weiteren Beispielen und Medien bestätigen.[4]

Während die Entwicklung des Propagandamodells von Herman und Chomsky und auch die von Bennett entwickelte Indexing-Hypothese stets vor dem Hintergrund des US-amerikanischen politischen Systems und Mediensystems zu verstehen sind, konnten die Annahmen der Indexing-Hypothese auch im deutschen Kontext bestätigt werden. Untersucht wurde beispielsweise die Berichterstattung der überregionalen Tageszeitungen über die Einsätze der Bundeswehr im Rahmen des Kosovo- und des Afghanistan-Krieges.[5] In beiden Fällen herrschte im Bundestag mehrheitlich Konsens zwischen den größten Oppositionsparteien und der Regierung bezüglich der Kriegsbeteiligung, offene Ablehnung kam lediglich von der damaligen PDS. Vor dem Hintergrund dieser überwiegenden Einigkeit im Parlament konnte gezeigt werden, dass kritische Positionen, welche die Kriegseinsätze grundsätzlich infrage stellten, in den Medien marginalisiert waren und Kritik sich primär auf die performativ strategische Ebene der Kriegführung beschränkte. Der größte Anteil kritischer Beiträge fand sich dabei in den eher linken Zeitungen, insbesondere der taz.

Die Problematik der auf Bennett zurückgehenden Annahmen wird bei so weitreichenden politischen Entscheidungen wie einer Kriegsbeteiligung besonders deutlich. Werden infolge eines überwiegenden parlamentarischen Konsenses kritische Positionen außerparlamentarischer und zivilgesellschaftlicher Akteure nicht länger in relevantem Ausmaß wiedergegeben, so erfolgt eine Verengung des medialen Diskurses. Im Zuge dessen werden politische Entscheidungen kaum noch grundlegend kritisiert und hinterfragt, sondern als gegeben hingenommen.

DIE NÄHE DER JOURNALISTISCHEN ZUR POLITISCHEN UND WIRTSCHAFTLICHEN ELITE

Eine neue Perspektive auf die Situation der deutschen Medienberichterstattung eröffnete die 2013 veröffentlichte Arbeit „Meinungsmacht“ des Medienwissenschaftlers Uwe Krüger, deren zentrale Ergebnisse im Folgenden kurz vorgestellt werden.[6]

Im Rahmen seiner Untersuchung ging Krüger der Frage nach, wie eng führende deutsche Journalisten mit Eliten aus Politik und Wirtschaft in vertraulichem Austausch stehen und inwieweit die Medien die Meinung von Eliten auf Kosten der Perspektive anderer gesellschaftlicher Akteure wiedergeben. Dabei baut die Untersuchung auf bestehenden Erkenntnissen bezüglich der Nähe von Journalisten zur politischen Elite in Deutschland auf. So ist es in Berlin als Zentrum des politischen Journalismus üblich, dass Journalisten gezielt einzelne Politiker im Rahmen sogenannter Hintergrundkreise zum gemeinsamen Austausch einladen. Darüber hinaus gibt es kleinere vertrauliche Kreise, im Rahmen derer häufig Spitzenpolitiker ausgewählte Journalisten und Chefredakteure zu Gesprächen einladen. Das exklusivste Format bilden dabei Vier-Augen-Gespräche, zu welchen sich verabredet wird oder die sich am Rande von Veranstaltungen oder gemeinsamen Reisen ergeben. Allen diesen Treffen gemeinsam ist die Möglichkeit seitens der Beteiligten aus der Politik, gezielt Informationen an Journalisten weiterzugeben, welche entweder für die namentliche Veröffentlichung, anonyme Veröffentlichung oder zunächst als nicht zu publizierendes Hintergrundwissen bestimmt sind. Für Journalisten wiederum sind derartige Treffen interessant, da sie Zugang

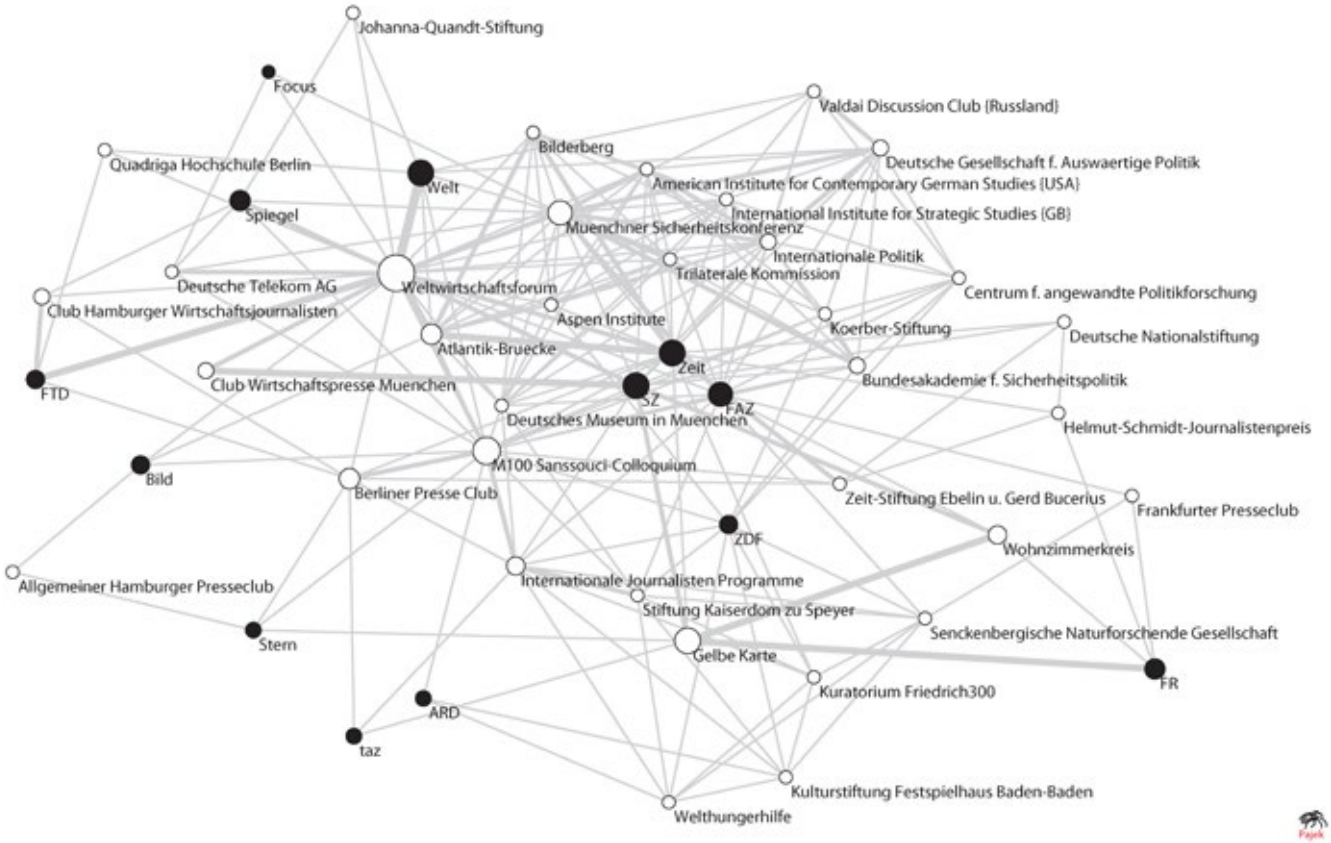
zu exklusiven Quellen und Informationen ermöglichen. Nicht zuletzt vor diesem Hintergrund war also die Annahme einer bedeutsamen Nähe zwischen Politikern und Journalisten naheliegend.

In der eigentlichen netzwerkanalytischen Untersuchung ging Krüger dann zunächst der Frage nach, inwiefern zwischen Eliten aus Journalismus, Politik und Wirtschaft Verbindungen in Form von gemeinsamer Mitgliedschaft in Gremien deutscher und internationaler Organisationen, Stiftungen, Denkfabriken, Konferenzen u. ä bestehen. Dabei wurde darauf geachtet, dass die Mitgliedschaft von Journalisten nicht unmittelbar mit ihrer journalistischen Tätigkeit in Form von Recherche oder Interviews zu tun hatte. Ergebnis dieser Analyse war, dass von zuvor ermittelten 219 führenden deutschen Journalisten 64 in einer oder mehreren Organisationen Mitglied waren, in denen Kontaktpotential zu Eliten aus Wirtschaft und Politik bestand. So fanden sich beispielsweise einzelne Journalisten im Beirat der Telekom AG und der Hypovereinsbank, sowie im Beirat der Bundesakademie für Sicherheitspolitik, welche u. a. in verschiedenen gesellschaftlichen Feldern für die Sicherheitspolitik der Bundesregierung wirbt.[7] Diese Beispiele machen die Brisanz der Untersuchungsergebnisse deutlich, da sich die Frage stellt, inwiefern derartige Mitgliedschaften die Berichterstattung über die besagten Konzerne oder auch die Bundesregierung beeinflusst, wenn man Teil eines Gremiums ist, welches eben jene berät.

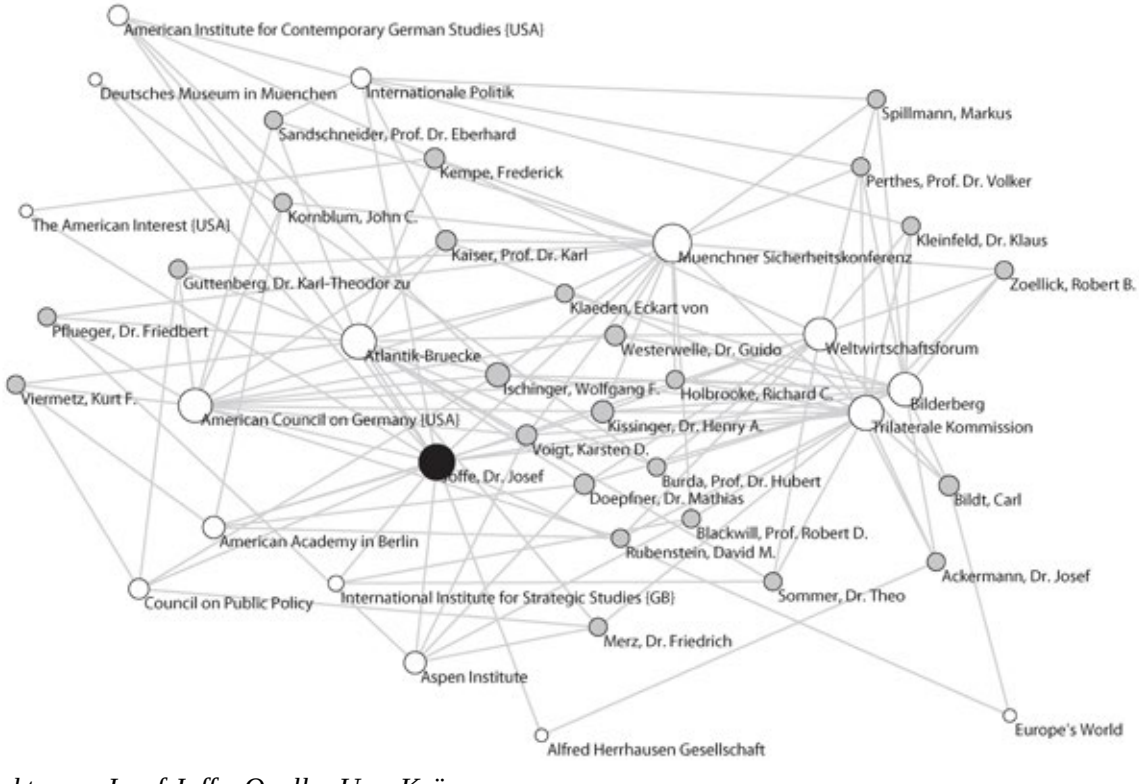
Eine besondere Auffälligkeit der Analyse war die Mitgliedschaft von vier Journalisten aus SZ, FAZ, Welt und Zeit in Organisationen aus dem außenpolitischen und transatlantischen Kontext, welche dementsprechend im Zeitraum der Untersuchung unter Eliten aus deutscher Politik und Wirtschaft, sowie der amerikanischen Wirtschaft und politiknaher Wissenschaft aus Deutschland und den USA verkehrten. In einer folgenden inhaltsanalytischen Auswertung der Artikel jener Journalisten zu den Themen Sicherheit, Verteidigung und Auslandseinsätze wurde deutlich, dass sich die Berichterstattung inhaltlich innerhalb des Deutungsrahmens der jeweiligen Eliten-Organisationen bewegte, im Kontrast zu einer – laut Umfragen – deutlich kritischeren Bevölkerungsmehrheit.

In einer hieran anschließenden Untersuchung der Berichterstattung über die Münchener Sicherheitskonferenz, die parallel stattfindende Friedenskonferenz und die Proteste in den Jahren 2007 bis 2010 konnte Krüger weiterhin zeigen, dass die elitennahe Berichterstattung nicht bloß ein individuelles Phänomen darstellt.[8] Die Beiträge in Welt, FAZ und SZ gaben ausführlich und unkritisch den Diskurs auf der Sicherheitskonferenz wieder und kritisierten die Gegenveranstaltungen, ohne inhaltlich näher auf diese einzugehen. FR und taz dagegen boten auch der Friedenskonferenz und den Protesten mehr Raum und berichteten neutraler über diese, gingen dabei aber auch nicht näher auf die konkreten Inhalte des dortigen Diskurses ein.

Es gilt an dieser Stelle zu beachten, dass sich aus Krügers Analysen keine einfachen kausalen Ursachenzuschreibungen ableiten lassen. Die Einbindung verschiedener Journalisten in das politische und wirtschaftliche Elitenmilieu muss nicht für eine Einflussnahme auf die Berichterstattung sprechen. Denkbar ist ebenso ein Zustandekommen enger Beziehungen aufgrund geteilter Überzeugungen



Das von Uwe Krüger untersuchte Gesamtnetzwerk. Quelle: Uwe Krüger.



Kontakte von Josef Joffe. Quelle: Uwe Krüger.

und Wertvorstellungen, die sich dann auch in der Berichterstattung widerspiegeln. Weiterhin gilt, dass die inhaltliche Elitenorientierung je nach Medium auch dem gesellschaftlichen Status der Kunden und deren antizipierten Interessen geschuldet ist. Deutlich wird anhand von Krügers Arbeit aber sowohl eine große Nähe zur gesellschaftlichen Elite in Teilen des führenden deutschen Journalismus sowie eine große inhaltliche Nähe zum Elitendiskurs, wie sie auch in den zuvor dargestellten Ansätzen prognostiziert wurde.

FAZIT

Die drei besprochenen Arbeiten eint eine kritische Perspektive auf die Nachrichtenproduktion in den jeweils untersuchten Mediensystemen. Gemeinsam ist ihnen weiterhin, dass die Annahmen, auf die sie sich jeweils stützen, weder die Entstehung der medialen Berichterstattung, noch ihre Verzerrung vollständig erklären können. Trotz dieser Einschränkung ermöglichen sie eine kritische Reflexion verschiedener für die Nachrichtenproduktion relevanter Faktoren und verbunden damit der Frage, wie es zu Verzerrungen und Schieflagen in der medialen Berichterstattung kommen kann - eine Frage, die ebenso wie die damit verbundene Medienkritik für eine friedenspolitische Perspektive so lange unverzichtbar sein wird, wie Medien an der Konstruktion von Feindbildern und der einseitigen Betrachtung von Konflikten beteiligt sind und einen politischen Status quo stützen, der die gegenwärtigen Konfliktlagen ermöglicht und befördert.

ANMERKUNGEN

1 Herman, Edward S.; Chomsky, Noam: Manufacturing consent: The political economy of the mass media, Random House, 1988.
2 Bennett, W. Lance: Toward a theory of press-state relations in the United States, Journal of communication, 40(2), 103-127, 1990.
3 Ebd.
4 Siehe z. B. bezüglich der Berichterstattung über Folter in amerikanischen Militärgefängnissen: Bennett, W. Lance; Lawrence, Regina G.; Livingston, Steven: None dare call it torture: Indexing and the limits of press independence in the Abu Ghraib scandal, Journal of Communication, 56(3), 467-485, 2006.
5 Eilders, Christiane; Lüter, Albrecht: Gab es eine Gegenöffentlichkeit während des Kosovo-Krieges? Eine vergleichende Analyse der Deutungsrahmen im deutschen Mediendiskurs, In: Albrecht, Ulrich; Becker, Jörg (Hrsg.): Medien zwischen Krieg und Frieden, Nomos, 2002, S. 103–122. Pohr, Adrian: Indexing im Einsatz: Eine Inhaltsanalyse der Kommentare überregionaler Tageszeitungen in Deutschland zum Afghanistankrieg 2001, M&K Medien & Kommunikationswissenschaft, 53(2-3), 261-276, 2005.
6 Krüger, Uwe: Meinungsmacht: der Einfluss von Eliten auf Leitmedien und Alpha-Journalisten: eine kritische Netzwerkanalyse, Halem, 2013.
7 Auf der Website der Bundesakademie für Sicherheit heißt es: „Sie trägt dazu bei, ein umfassendes Verständnis für die langfristigen sicherheitspolitischen Ziele Deutschlands zu schaffen. […] Die Bundesakademie fördert ein gemeinsames Verständnis nationaler und internationaler Sicherheitspolitik – bei Angehörigen von Politik, Behörden, Wissenschaft, Wirtschaft und gesellschaftlichen Organisationen sowie in der breiteren Öffentlichkeit.“ baks.bund.de (Zugriff 14.02.2018).
8 Krüger, Uwe 2013.

DIE FABELHAFTE WELT DES MALIBOT

DIE NEUE MALI-WERBEKAMPAGNE DER BUNDESWEHR

VON: ALEXANDER KLEIß

Nach der Youtube-Serie „Die Rekruten“ im vergangenen Jahr startete die Bundeswehr im Oktober 2017 eine neue Werbekampagne. Diese beschäftigt sich mit dem Auslandseinsatz der Bundeswehr in Mali und stellt diesen im Sinne der Bundeswehr dar. Ähnlich wie bei „Die Rekruten“ steht im Mittelpunkt der Werbekampagne wieder eine Youtube-Serie. Diese ist im Reality-TV-Format gehalten und dementsprechend inhaltlich eher seicht, aber technisch aufwändig und professionell produziert. Die Serie ist aber nur ein Mosaikstein der Werbekampagne, die von einem sehr breiten Bündel anderer Werbemaßnahmen begleitet wird. Dies umfasst zum einen die konventionelle flächendeckende Werbung im öffentlichen Raum, aber auch eine Werbeoffensive auf sämtlichen gängigen Social Media: Neben YouTube wirbt die Bundeswehr auch auf Instagram und Spotify. Auch Facebook wird von Bundeswehr-Werbung nicht verschont. Dort ist u.a. die Möglichkeit vorgesehen, sich mit einem Chat-Bot der Bundeswehr, also einem Softwareprogramm, welches mit den Nutzer_innen chattet und Fragen beantwortet, zu unterhalten.

Dieses Programm nennt sich Malibot und schickt Facebook-Nutzer_innen, die das Programm abonniert haben, täglich mehrere in Militärsprache gehaltene Nachrichten, Bilder und Videos (meist in eher schlechter Qualität) der „Kameraden“ aus Mali. Die Bundeswehr versucht sich hierbei ein teils heldenhaftes, teils seriöses, teils eher flapsiges Image zu geben, wobei vor allem letzteres oft eher zu unangenehmer Fremdscham bei den Betrachtenden führt, so z.B. die „lustige“, sexistische Aussage eines in Mali stationierten Soldaten: „Bei Blindgängern gibt es eine Grundregel: Wenn du mit ihm umgehst wie mit einer Frau, dann explodiert er auch nicht“.[1]

Insgesamt ist die Aufmachung der Werbekampagne so gehalten, dass sie sehr stark an einen Action-Film oder einen Egoshooter erinnert, wodurch eine Ästhetisierung von Krieg und Militär stattfindet. Außerdem soll durch die Aufmachung vor allem ein junges Publikum angesprochen werden. Dies wird auch durch die Wahl der verwendeten Medien sichtbar: So sind z.B. 86% der Nutzer_innen von Snapchat unter 34, mehr als die Hälfte ist zwischen 16 und 24 Jahre alt.[2] Das macht die Werbeoffensive besonders gefährlich, da vor allem Minderjährige die vermeintlich seriösen Informationen oft nicht adäquat einordnen und als Propaganda entlarven können und die Bundeswehr vorwiegend „deren“ Kommunikationskanäle nutzt.

Dies lässt sich die Bundeswehr einiges kosten: 6,5 Mio. Euro gaben die Zuständigen für die Kampagne aus, die intern unter der Bezeichnung „Arbeitgebermarke Bundeswehr“ läuft. Die Produktionskosten der Videos haben daran mit zwei Millionen Euro noch den geringsten Anteil. 4,5 Millionen Euro wurden für die „Medialeistungsbewerbung“ ausgegeben.[3]

Die Bundeswehr versucht, ihr Vorgehen zu rechtfertigen, indem sie behauptet, die Kampagne diene der Nachwuchswerbung, was nach der Aussetzung der Wehrpflicht nötig sei, um alle Dienstposten zu besetzen. Dabei wird allerdings nicht erwähnt, dass momentan zunehmend neue Dienstposten geschaffen werden, obwohl die bisher angepeilte Stellenzahl mangels Interessent_innen jetzt schon nicht mehr besetzt werden kann.[4] Eine Reduzierung der Dienststellen wäre insofern eine gute Alternative zur Mali-Werbekampagne. Stattdessen wird versucht, bei den kriegsmüden jungen Menschen wieder Kriegsbegeisterung zu schaffen. Die Soldat_innen werden zu Held_innen stilisiert, die – so die Bundeswehr – „auch dein Leben sicherer“[5] machen. Vor allem durch die hohe Frequenz und die Aufmachung der ständigen Nachrichten des Malibots auf Facebook wird suggeriert, diese kämen z.B. von einer guten Freundin aus Mali. Junge Menschen sollen an den Smartphones und Bildschirmen mit „unseren“ Jungs und Mädels an der Front mitfiebern, als handle es sich beim Einsatz der Bundeswehr in Mali ganz banal um die neuste Staffel des Dschungelcamps. Die Tatsache, dass in Mali jedoch Menschen sterben, ist lediglich eine Randnotiz und dient eher der zusätzlichen Heroisierung der Soldat_innen statt einer kritischen Auseinandersetzung mit der Thematik.

Die ausgiebigen Werbebemühungen der Bundeswehr scheinen bei der Zielgruppe jedoch zu verfangen: Im Sendezeitraum der Youtube-Serie „Die Rekruten“ stieg die Zahl der Zugriffe auf die Karriereseite der Bundeswehr um 40%. Auch die Zahl der tatsächlichen Bewerbungen stieg.[6] Ähnliches ist auch für die aktuelle Werbekampagne zu erwarten. Insgesamt sank die Zahl der Bewerbungen für eine militärische Laufbahn bei der Bundeswehr im Vergleich zum Vorjahr jedoch leicht, wobei die Zahl der Bewerbungen für eine Laufbahn als Zeitsoldat_in um 3% leicht ansteigt. Im Schnitt brechen 27 Prozent der Rekrut_innen in den ersten sechs Monate wieder ab. Unter den Zeitsoldat_innen beenden im Schnitt 18 Prozent ihren Dienst in der Probezeit.[7] Spätestens während der Ausbildung merken also viele, dass eine Karriere bei der Bundeswehr weder Heldentum noch Abenteuer, sondern Krieg und somit Tod bedeutet.

ANMERKUNGEN

1 Facebook: Bundeswehr Exclusive im Chatverlauf. 10.11.2017, 19:07.
2 Statista: Verteilung der Snapchat-Nutzer nach Altersgruppen weltweit im 2. Quartal 2015.
3 Zeit Online: Bundeswehr Exclusive. Werde Soldat, yo! 25.10.2017.
4 Bundesministerium der Verteidigung: Bundeswehr schafft noch mehr neue Stellen. 21.02.2017.
5 Bundeswehr-Werbereklame im öffentlichen Raum: „Ihre Mission macht auch dein Leben sicherer“.
6 Zeit Online: Bundeswehr Exclusive. Werde Soldat, yo! 25.10.2017.
7 FAZ: Bewerberzahlen für freiwilligen Wehrdienst brechen ein. 25.11.2017.

HERAUSFORDERUNGEN FÜR EINEN KRITISCHEN JOURNALISMUS

VON: ANNA HUNGER

„In Demokratien erfüllen Medien grundlegende Funktionen: Sie sollen das Volk informieren, durch Kritik und Diskussion zur Meinungsbildung beitragen und damit Partizipation ermöglichen.“ So definiert die Bundeszentrale für Politische Bildung den Begriff „Medien“. Subtrahiert man davon die Vorwürfe um „Fake News“ und „Lügenpresse“, bleibt nur wenig übrig von der hübschen Definition. Zwischen Ideal und Totalverriss klafft eine ganze Schlucht. Die Realität ist komplizierter.

Natürlich gibt es Leerstellen und Ungleichgewichte der Medienberichterstattung. Warum wurde selbst in so genannten Leitmedien so wenig über Cum-Ex- und Cum-Cum-Geschäfte berichtet – den größten Steuerskandal der Geschichte? Andererseits gab es die Panama-Papers, den Abhöhr-Skandal rund um Edward Snowden und auch #MeToo wäre ohne Medienbeteiligung nicht so groß geworden. Zudem gibt es engagierten Journalismus auf lokaler oder regionaler Ebene.

„Die Presse“ ist kein homogenes Gebilde. Journalistinnen und Journalisten sind auch nur Menschen. Mit Meinungen, guten und schlechten Tagen, Gesprächspartnern, Geschichten, Ideen, mit eigenen Assoziationen, Prägungen und Charakteren, politischen Haltungen. Es gibt sehr kluge Medienmachende und sehr dumme, es gibt solche mit mehr oder weniger Leidenschaft. Andere, die es sich einfach machen, oder natürlich solche, die sich beeinflussen lassen, weil sie einen Vorteil daraus ziehen – Presserabatte, irgendwann einen hochbezahlten Job als PressesprecherIn in der Wirtschaft oder die Eitelkeit, sich im inneren Kreis hoher Politik bewegen zu wollen.

Allerdings ist der Anspruch, anders als beim Steuerberater oder der Dachdeckerin, die Wahrheit zu publizieren. Lässt man Aspekte wie Gerechtigkeit oder politische Haltung beiseite, gibt es die eine reine Wahrheit aber nur selten.

Allerdings ist die Realität, die es abzubilden gilt, auch kein frei flottierendes Gut, das beliebig interpretiert werden kann. Es gibt Fakten, um der Wahrheit möglichst nahe zu kommen. Und die müssen nach bestem Wissen und Gewissen geprüft werden. Um über Flüchtlingspolitik zu diskutieren, braucht es belastbare Zahlen. Denn mit Zahlen wird Politik gemacht. Die Aufgabe der Presse ist es, diese Zahlen zu überprüfen oder zu korrigieren. Wenn ein Geflüchteter ein Verbrechen begangen haben soll, überprüft guter Journalismus den Sachverhalt und recherchiert die Hintergründe – mit Ortsbesuchen, Gesprächen mit Polizei, Beteiligten, ExpertInnen und so weiter. Aber die Realität ist selten einfach und aufrichtige Recherche dauert - und kostet.

Die Presse leidet unter einem immer vehementeren ökonomischen Druck, weil die Print-Verlage den Wandel zu Online verschlafen haben und jetzt auf Klickzahlen angewiesen sind, damit sich Werbung lohnt. Was wiederum heißt: möglichst reißerisch, möglichst schnell, möglichst viel, möglichst kurz. Hintergrundberichterstattung fällt da oft flach.

Dass es immer weniger eigenständige Lokal- oder Regionalzeitungen gibt, die nicht zu der einen Hand voll großer, renditeorientierter Pressekonzerne in Deutschland gehören, tut sein Übriges dazu. Redaktionen werden kaputtgespart, anstatt sie liquider und damit besser zu machen, feste RedakteurInnen werden gekündigt, stattdessen wird verstärkt auf freie Mitarbeitende gesetzt, die manchmal finanziell regelrecht gemolken werden. RedakteurInnen müssen in der Print-Berichterstattung auf die Befindlichkeiten der wenigen verbliebenen Anzeigenkunden achten. Aus Zeit- oder Geldmangel wird häufig auf Agentur-Meldungen zurückgegriffen, die in selber Ausführung zeitgleich hunderte Deutscher Redaktionen erreichen. Vielfalt bleibt auf der Strecke.

In der außenpolitischen Berichterstattung ist es noch schwieriger. Ich kenne einige KollegInnen, die in Kriegs- oder Krisengebieten arbeiten oder gearbeitet haben, zuverlässige, kompetente Menschen, die ihr Leben riskieren für gute Berichterstattung. Aber weniger finanzielle Spielräume in Redaktionen bedeuten weniger Korrespondentinnen und Korrespondenten, weniger Reiseetat. Und so passiert es, dass oft eine einzige kompetente Person für einen Bauchladen an Zeitungen schreibt, andere vom Schreibtisch aus recherchieren, im schlimmsten Fall mit wenig Ahnung.

Pressekonzentration und Unterfinanzierung führen zum Rückgang von Meinungsvielfalt und damit zu Einheitsbrei und der widerspricht der eigentlichen Aufgabe von Presse – Meinungsvielfalt zu ermöglichen, um Diskussion und Teilhabe zu generieren. Das ist der Grundgesetzauftrag. Um es mit Heribert Prantl, dem Leitartikler der Süddeutschen Zeitung, zu sagen: „Journalismus ist das Brot der Demokratie.“

Journalismus heute braucht Haltung, Mut und Courage, um seine ureigene Aufgabe der Kritik an herrschenden Umständen aller Art zu erfüllen. Gegenwind auszuhalten, braucht Rückgrat und manchmal einen guten Anwalt, um Versuche, Berichterstattung zu verhindern, abzuwehren. Und vor allem braucht Journalismus gutes Handwerk. Deshalb ist er ein Beruf, den man lernen muss. Nicht nur das Schreiben, sondern vor allem das Recherchieren, den Umgang mit Information und deren Vermittlung. Irgendwie die Schale einer Zwiebel abzupopeln kriegt auch ein Laie hin. Aber das sorgfältig zu tun und womöglich hinterher noch ein gutes Zwiebel-Gericht daraus zu kochen, das kann eben nicht jeder. Journalismus, der hinter die Kulissen schaut und damit den Mächtigen in Wirtschaft und Politik auf die Finger, braucht gute Ausbildung. Wo aber Redaktionen an RedakteurInnen sparen und stattdessen unerfahrene, aber günstige Volontäre einsetzen, kann das nichts werden.

RESONANZ CON(TRA)SENS

PERSPEKTIVEN AUS DEM FREIEN RADIO: SUBJEKTIV, POLITISCH UND DESHALB AUTHENTISCH.

VON: JUDITH LAUTERBACH

Freie Radios haben den Anspruch und den Auftrag, kritische Medienkompetenz zu vermitteln, d.h. die Fähigkeiten zu sozialer und journalistischer, aber auch technischer Medienproduktion quasi „unter die Leute zu bringen“. Die Wüste Welle, das Freie Radio für die Region Tübingen/Reutlingen, ist basisdemokratisch organisiert, hat keine finanziellen Interessen und kann politisch unabhängig agieren. Alle Menschen, die nicht in irgendeiner Weise menschenfeindliche oder diskriminierende Werte vertreten, sind eingeladen, auf Sendung zu gehen und sich im Radio frei nach ihren Interessen zu beteiligen. Dies alles spiegelt sich im Begriff der Freien Kommunikation wider: als Medienschaffende treten wir für eine transparente und offene Kommunikation ein und verstehen uns als Instrument zur Demokratisierung der Öffentlichkeit. Dabei möchten wir sowohl bei den Hörer*innen als auch bei den Sendungsmachenden die politische Meinungsbildung fördern.

Die Sendung, in der ich aktiv bin, nennt sich „Resonanz Con(tra)sens“. Der Name soll ein Wortspiel sein mit dem Teil „Resonanz“ für Anklang und Widerhall, und den Teilen „Contra“ und „Konsens“, die für kritische und solidarische politische Inhalte stehen sollen.

Die Berichte für Resonanz Con(tra)sens schreiben wir nur zu einem kleinen Teil völlig selbst. Dafür nutzen wir sowohl herkömmliche Medien wie Tageszeitungen, als auch Medienplattformen wie Indymedia und das Archiv der Freien Radios (freie-radios.net). Die Zensur und Repression gegen die Nachrichtenplattform Indymedia Linksunten betrifft uns daher nicht nur ideell als Teil einer gemeinsamen Gegenöffentlichkeit, sondern auch ganz direkt als Nutzerin und Leserin.

Der Großteil unserer Beiträge speist sich aus Interviews oder persönlichen Berichten – von Demonstrationen und Aktionen oder mit Personen, die sich sozial oder politisch engagieren. Es kommen also Menschen selbst zu Wort, und was sie erzählen, sind ihre Bedürfnisse, Probleme, Ideen, Initiativen. Mitzubekommen, was andere bewegt und was sie an der Gesellschaft stört, führt zu einer authentischen Berichterstattung. Oft geht es dabei nicht um reine Fakten, sondern um Diskurse: wie werden von wem welche Sachverhalte bewertet; welche Veränderungen wären hilfreich für eine freie, demokratische Gesellschaft; welche Gruppierungen engagieren sich für was, und so weiter. Ein solcher Kontext hält die Gefahr für „Fake News“ oder Falschmeldungen klein, vielmehr hilft er bei der Einschätzung der Gesellschaft von unten – letztlich bei der politischen Meinungsbildung. Die Inhalte mögen dadurch einseitig und punktuell sein. Als Teil eines Lokalsenders mit einer alternativen bzw. linken Stammhörer*innenschaft haben wir allerdings nicht den Anspruch, Massenmedium zu sein. Durch die Glaubwürdigkeit, die persönliche Berichte auszeichnet, hoffen wir trotzdem einen Anklang auch außerhalb des explizit linken Spektrums zu finden.

Mehr und mehr sind auch die Radiosender mit den neuen Kanälen im Informationsraum („Social Media“ usw.) konfrontiert. In der Wüsten Welle werden die anstehenden Veränderungen aus unterschiedlichen Blickwinkeln betrachtet. Während viele der über 120 Sendungsmachenden ihre Kernkompetenz und Freude im analogen UKW-Bereich haben, sehen andere auch die Chancen, welche die Digitalisierung mit sich bringt: sei es die bessere Erreichbarkeit durch Internetradio und Internetauftritte oder eine erhöhte Präsenz der Wüsten Welle durch Vernetzung über soziale Medien.

Die sozialen Medien und ihre Nutzung sind von zentraler Bedeutung bei der Frage, inwieweit das „Zeitalter“ von Cyberwar und das sogenannte postfaktische miteinander verknüpft sind. Dass eine Digitalisierung des Zusammenlebens zwangsläufig eine Verschärfung der geführten Diskurse und die daraus genährte Annahme, es gäbe so etwas wie „alternative Fakten“, mit sich bringt, ist zu bezweifeln. Hier in unserer Gesellschaft sind die Vermittlung von Ereignissen und Diskursen, die alltägliche Kommunikation und Digitalisierung jedoch eng miteinander verknüpft.

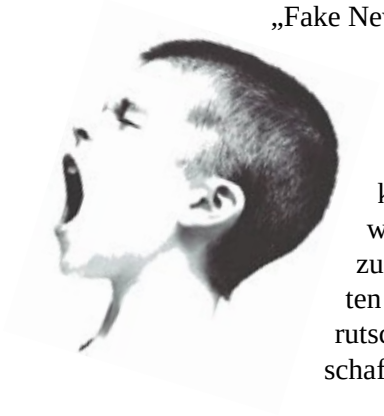
Dabei spielen die sozialen Medien im Informationsraum die größte Rolle: die meistgenutzte „Quelle“ für Nachrichten ist inzwischen Facebook. Über soziale Medien lassen sich schnell und unmittelbar Nachrichten und Berichte verbreiten, und wir haben schon während des Arabischen Frühlings gesehen, wie hilfreich sie für Vernetzung und Organisierung von Unten sein können. Menschen, die direkt vor Ort sind, teilen ihre Berichte weltweit. Ein Hinweis auf die Effizienz sozialer Medien ist die Zensur, die in vielen Staaten genau diese Kanäle trifft. Aus dieser Perspektive lassen sich soziale Medien als eine Sorte Gegenöffentlichkeit betrachten, die der Demokratisierung einer Gesellschaft zugute kommen können.

Problematisch ist allerdings, dass die meisten Nutzer*innen sich damit abfinden, Teil eines kommerziellen Unternehmens zu sein. Facebook gehört zu den fünf wertvollsten Unternehmen der Welt. Durch unbekannte Quellcodes bleiben die Algorithmen, mit denen soziale Medien (und auch andere Internetkonzerne) arbeiten, intransparent. Dies allein schon stellt eine Gefährdung des demokratischen Miteinanders dar: wer nicht weiß, wie Medien und Informationen produziert werden, kann sie auch nicht richtig einschätzen und sich schlecht orientieren. Ein Stichwort dazu lautet Filterblase: anstatt sich selbständig um Informationsquellen zu kümmern, erscheint auf dem Display scheinbar ganz von alleine eine Nachrichtenmeldung. Bedenklich dabei ist die automatische Anpassung an zuvor gelesene Inhalte. Alles, was der Algorithmus als außerhalb des eigenen Interesses erkennt, wird aussortiert. Wer sich also nur auf seine Filterblase verlässt und das eigene Recherchieren und Diskutieren vernachlässigt, hat es schwer, seine Informationen mit anderen abzugleichen. Wem der Abgleich fehlt, beruft sich schnell auf nur eine bestimmte Wahrheit. Dass Wahrheiten jedoch nie absolut sind und der Diskurs über Geschehnisse stets aus verschiedenen Perspektiven geführt wird, gehört zu einem demokratischen Bewusstsein und zu einer kritischen Medienkompetenz. Wenn diese Kompetenzen nicht vorhanden sind, kann die Vorstellung entstehen, dass es sich bei Berichten außerhalb der eigenen Filterblase um Lügen und „falsche Fakten“ handele. Der Neologismus „postfaktisch“ zeugt zugleich von einem irreführenden Sprachgebrauch: während „Fakten“ physisch reale Ereignisse bezeichnen, kann das Darüber-Reden sehr unterschiedlich ausfallen und soziale Realität verändern.

Es darf nicht vergessen werden, dass auch in den bürgerlichen Medien und schon lange vor der Zeit des Internets nur bestimmte Inhalte verbreitet wurden und werden. Monopole von Medienkonzernen und interessengeleitete Berichterstattungen sind in der Lage, gesellschaftliche Diskurse zu lenken und Wertvorstellungen zu beeinflussen. Sie können demzufolge als eine Art große Filterblase gedacht werden. Diese ist jedoch weniger ausgeprägt als die digitale Filterblase: innerhalb der Riege der großen öffentlichen und privaten Medien besteht ein Spielraum, der gesellschaftlich relevante Themen von (links) Unten aufnehmen kann. Digitale Filterblasen dagegen funktionieren automatisiert und werden von weniger Akteuren bestimmt. Sie wirken dadurch viel selektiver und haben einen selbstverstärkenden Effekt, der extreme und sogar menschenfeindliche Inhalte begünstigen kann.

Wenn wir eine Sensibilität dafür entwickeln, wer wie über etwas redet und was von wem gesagt wird – und noch viel wichtiger: was nicht gesagt wird – dann sind wir auch in der Lage, uns in der Vielfalt der Medien besser zu orientieren und politische Zusammenhänge besser zu erkennen. Anders als die Battle Management Language (siehe Beitrag von Franz Wanner) ist unsere natürliche Sprache zu Recht in sehr vielen Fällen mehrdeutig – aber wir besitzen die Fähigkeit, Mehrdeutigkeiten und Lücken in Diskursen ausfindig zu machen, Meldungen mit unserem sonstigen Wissen abzugleichen und somit „Fake News“, politische Meinungsmache und Verschwörungstheorien leichter zu identifizieren.

Unsere Gesellschaft erfährt einen Wandel hin zu einer größeren und undurchsichtigeren Medienlandschaft, gepaart mit der Digitalisierung vieler Bereiche. Der Informationsraum ist dabei nur ein Teil. Je komplexer die Nachrichtenquellen sind, desto bedeutender ist das Wissen darüber, dass es die eine Wahrheit noch nie gab, „Fake News“ und Propaganda dagegen eine lange Tradition haben, und ebenso die Kompetenz, sich trotz Filterblasen und antidemokratischer Kommunikationskultur darin zurechtzufinden.



In fast allen gesellschaftlichen Bereichen ist die maschinelle Verarbeitung auf dem Vormarsch, sodass die Digitalisierung den Anschein eines totalitären Systems entwickeln kann, in dem Algorithmen die Entscheidungs- und Handlungsfreiheit im Einzelfall – das, was Menschlichkeit ausmacht – unterbinden. Diese Algorithmen als unpersönlichen Feind zu betrachten, wäre allerdings der falsche Weg. Was unsere Gesellschaft braucht, um in Zeiten von Cyberwar und Strategischer Kommunikation nicht vollends ins Postfaktische abzurutschen, ist mehr Transparenz in Politik,Wirtschaft und Medien(diskursen) und mehr gesellschaftliche Partizipation auf allen Ebenen – und eben auch in den Medien.

MILITÄR-WERBUNG BIS ZUR KENNTLICHKEIT VERÄNDERN

VON: MICHAEL GODE

Seit November 2015 drängt die Bundeswehr mit millionenschweren Werbeaufträgen in den öffentlichen Raum. So verstörend das zunächst erscheinen mag, ist das militärische Streben nach Aufmerksamkeit auch eine Chance. Denn wer die Öffentlichkeit sucht, muss sie auch ertragen. Dass die Bundeswehr damit ihre Probleme hat, zeigte sich immer wieder bei den polizeistaatlichen Reaktionen auf Proteste anlässlich von öffentlichen Gelöbnissen oder Tagen der offenen Tür. Ähnlich angreifbar ist die Werbung der Bundeswehr im öffentlichen Raum. Die Protestform, die sich explizit mit dem Umdeuten von Werbung beschäftigt, nennt sich Adbusting. Dieses Kunstwort aus den englischen Begriffen Advertising (Werbung) und to bust (stören, kaputt machen) beschreibt das gezielte Verändern von Werbung, oder, wie die Adbuster*innen sagen würden: „Wir entstellen die Werbung bis zur Kenntlichkeit".

BEISPIEL: ADBUSTINGS AM KRIEGSMINISTERIUM

Wie das funktioniert, lässt sich an einer Aktion am Kriegsministerium im Dezember 2017 zeigen. Schräg gegenüber des Bendlerblocks am Lützow-Ufer gibt es eine Plakatwand. Diese wird regelmäßig durch die von den Militärs angeheuerte Werbeagentur genutzt, um dort gut sichtbar für alle ministerialen Schreibtischtäter*innen die jeweils aktuelle Militär-Werbung präsentieren zu können. Doch im letzten Dezember überklebten Unbekannte diese Plakate mit antimilitaristischen Verbesserungen. Auf der Abbildung einer Soldat*in vor einem U-Boot steht nun statt „Nicht jede Führungskraft hat ein Büro": „Nicht jede Führungskraft befiehlt Schikane". Das Bild einer Jet-Pilot*in zierte ursprünglich der Spruch „Nicht jeder Entscheider hat einen Dienstwagen". Nach der Verbesserung heißt es wahlweise „Nicht jeder Entscheider hat die Lizenz zum Töten" oder „Nicht jeder Entscheider träumt vom Führer".

GEZIELTE ÜBERSPITZUNG

Das Beispiel macht deutlich, wie Adbusting-Künstler*innen das Vorgefundene überspitzen. In der Original-Version versuchen die Militärs bei der Suche nach neuen Offiziersanwärter*innen gegen die sogenannte „freie Wirtschaft" beim Werben um Nachwuchs zu konkurrieren. Dabei übernehmen die Militär-Werber*innen deren neoliberales Gerede von „Führungskräften" und „Entscheidern" und die daran gebundenen Vorstellungen von Statussymbolen wie Dienstwagen und Büros. Da die Bundeswehr aber genau hier nicht mithalten kann, wird die Erwartungshaltung der Betrachtenden gebrochen, indem das Büro durch ein U-Boot und der Dienstwagen durch ein Kampfjet ersetzt wird. Diese Bilder- und Begriffswelt soll auf der einen Seite mit den positiv besetzten Begriffen „Führungskraft" und „Entscheider" eine Gleichrangigkeit zu anderen Berufen beanspruchen, gleichzeitig mit dem offensiven Zeigen von Waffen wie U-Booten und Kampfjets deutlich machen, dass der Job beim Bund viel interessanter sei.

MIT DEM ARBEITEN, WAS DA IST

Diese Trennung von „ziviler" und „militärischer" Welt nehmen die Adbustings auf. Doch statt die militärische Welt mit ihrer Waffentechnik und Macht verheißenden Mordsmaschienen positiv zu setzen, wird dieser Effekt ins Gegenteil verkehrt. Der Spruch „Nicht jeder Entscheider hat die Lizenz zum Töten" erinnert die Betrachter*in daran, dass man in der zivilen Wirtschaft meistens allenfalls indirekt für das Sterben von Menschen verantwortlich ist. „Nicht jede Führungskraft befiehlt Schikane" macht der Betrachter*in deutlich, dass es auch Arbeitsverhältnisse gibt, in denen das Einführen von Tampons in den After nicht zum Ausbildungsprogramm gehört. „Nicht jeder Entscheider träumt vom Führer" erinnert an die sehr wohl regelmäßig an die Wehrmacht anknüpfende zweifelhafte Traditionspflege der deutschen Militärs.

AUF DER GRENZE ZWISCHEN GLAUBWÜRDIGKEIT UND ÜBERTREIBUNG

Besonderen Effekt hat ein Adbusting, wenn es den Duktus der zu persiflierenden Werbung aufnimmt und bis hart an die Grenze der Glaubwürdigkeit überspitzt. Ein Beispiel dafür ist die Veränderung „Nicht jeder Entscheider hat die Lizenz zum Töten". Der Spruch arbeitet mit der von den Militärs bereits aufgemachten Trennung von „ziviler" und „militärischer" Welt, er ändert jedoch die Konnotation des Ganzen. Das aus der Popkultur entlehnte James-Bond-Zitat sorgt für Glaubwürdigkeit, da die Werbeagentur ebenfalls Anleihen bei der Popkultur macht. Die Thematisierung von Töten als Bestandteil des Militärs irritiert jedoch. Die Chancen stehen gut, dass so ein Slogan zu Irritation und Nachdenken bei den Betrachter*innen führt. Davon zeugen auch die Reaktionen in den sogenannten „Sozialen Medien", wo solche Aktionen regelmäßig zusätzlich zu den Passant*innen auf der Straße noch ein weiteres Publikum finden.

BUNDESWEHR BISHER BETONT COOL

Bisher reagiert die Bundeswehr betont cool auf derartige Aktionen. Als der Journalist Peter Nowak für das „Neue Deutschland“ im April 2016 im Kriegsministerium bezüglich der Bundeswehr-Adbustings nachfragte, teilte ihm Pressesprecher Jörg Franke Folgendes mit: „Wir sehen bislang keinen Anlass, Strafanzeigen zu erstatten“. Die Bundeswehrplakatkampagne habe zum Ziel gehabt, „provokative Denkanstöße“ auszulösen. Nun sorgten die Adbusting-Aktionen für Kontroversen, die wiederum dazu beigetragen hätten, die Bundeswehrkampagne bekannter zu machen.

LÄSSIGKEIT IN DEN SOZIALEN MEDIEN

Auch in den sogenannten „Sozialen Medien“ agieren die Propagada-Soldat*innen nicht ungeschickt. Im Herbst 2015 wurde die Fassade des „Bundeswehr-Ladens“ – einer öffentlichkeitswirksamen Rekrutierungsstelle am Berliner Bahnhof Friedrichstraße – von oben bis unten mit blutroter Farbe markiert. Neben diesen Anblick stellten die Soldat*innen ein Poster mit dem Slogan „Wir kämpfen dafür, dass Du gegen uns sein kannst“ und verbreiteten das Bild auf ihren Kanälen. Fast alle Berliner Tageszeitungen griffen das Motiv auf und feierten die Besatzung der Rekrutierungsstelle für ihr Propaganda-Geschick.

BALI STATT MALI

In einer Werbeanzeige in digitalen und analogen Magazinen greift die PR-Agentur der Bundeswehr ein Adbusting sogar explizit auf. Es handelt sich um ein Adbusting aus München. Auf das große M von Mali wurde dabei ein B geklebt, sodass dort nach der Veränderung „Bali“ statt ursprünglich „Mali“ steht. Den abgebildeten Soldat*innen wurden Blumen an die Helme geklebt und der Slogan um eine Bierflasche ergänzt. In ihrer Werbeanzeige nutzte die Bundeswehr dieses Arrangement wiederum, um es mit ihrem Logo und dem schon vom BW-Laden bekannten Slogan „Wir kämpfen auch dafür, dass du gegen uns sein kannst“ zu ergänzen.

PLAKATIVE PROBLEME

Hier deuten sich einige Probleme der Aktionsform Adbusting an. Die inhaltliche Rückeroberung der Adbustings durch die Bundeswehr nutzt die im Medium Plakat angelegte plakative Phrasenhaftigkeit. Die Bali-Aktion greift zwar durch eine Umdekodierung der im ursprünglichen Plakat verwendeten graphischen Symbole geschickt die Vorlage auf. Sie bleibt inhaltlich aber eher beliebig. Die Veränderung von „Mali“ zu „Bali“ suggeriert, dass der „Auslandseinsatz“ eher ein gut bezahlter Ferienurlaub als ein brutal geführter Krieg sei. Und genau diese inhaltlich zahnlose Kritik ermöglicht der Bundeswehr die Wieder-Aneignung.

INHALT WEITERHIN WICHTIG

Bei poppiger Kommunikationsguerilla stellt sich immer die Frage nach dem Inhalt. Nur weil die Form der Aktion bestimmte Vorteile gegenüber anderen politischen Interventionsformen bietet, sind sie aus einer emanzipatorischen Perspektive trotzdem keine Selbstläufer. Die Plakatveränderungen der Adbusting-Aktivist*innen sind sehr anfällig für Vereinnahmungen aller Art. Das liegt u.a. daran, dass sie zwar für Erregungskorridore sorgen können, aber aufgrund der wenigen Buchstaben und der Einfachheit der Botschaft, die ein gelungenes Plakat nun einmal ausmachen, wenig Inhalt transportieren können. Darüber hinaus müssen Plakat-Veränderungen zumindest in einem gewissen Grade die vorgedruckte Vorgabe ihrer Gegner*innen nutzen. Gerade deshalb ist ein radikaler Inhalt bei Kommunikationsguerilla sehr wichtig, weil nur das einen relativen Schutz vor einer Rück-Aneignung bietet.

WESHALB KRITISIEREN WIR DIE BUNDESWEHR EIGENTLICH?

Ein anderes Beispiel für die Probleme inhaltlich eher problematischer Kommunikationsguerilla blieb die relativ bekannt gewordene Fake-Homepage des Peng-Collectives. Unter der Domain „machwaszaehlt.de“ kopierten die Berliner Aktivist*innen täuschend echt die Bundeswehr-Seite „machwaswirklichzaehlt.de“. Unter dem Slogan „Mach was zählt“ warben sie im Bundeswehr-Design für einen Job in der Altenpflege, im Krankenhaus oder in der Entwicklungszusammenarbeit. Doch auch das bewahrt nicht vor dem Schicksal der Vereinnahmung. So beurteilt Phillipp Fritz, Volontär bei der Berliner Zeitung, die Homepage-Cover-Aktion des Peng-Collectives deshalb als unterstützenswert, weil sie keine grundsätzliche Systemkritik leistet: „Kritik an der deutschen Armee ist keine Systemkritik. Kritik an ihren Kampagnen kann auch geübt werden, wenn jemand die Notwendigkeit einer deutschen Verteidigungsarmee sieht. Die ‚Mach, was wirklich zählt‘-Kampagne jedoch versucht die Bundeswehr als etwas zu verkaufen, was sie nicht ist – als einen Abenteuerspielplatz. Genau das entlarvt die Gegenkampagne von Peng.“

KOMMUNIKATIONSGUERILLA ALS OPTIMIERUNG DES NORMALVOLLZUGS?

Eine genaue Betrachtung zeigt: Herr Fritz hat Recht. Denn die Gegenkampagne entlarvt auch das Peng-Kollektiv als lammfrom: Mehr Humanitäre Hilfe? Das leistet die Bundeswehr gerade beim Thema „Geflüchtetenhilfe“ mit dem größten (und unkritisiertesten!) Inlandseinsatz ihrer Geschichte. Weniger Sexismus in der Armee? Hier handelt es sich um ein explizites Anliegen der aktuellen Kriegsministerin. Kritische Aufarbeitung der Nazi-Vergangenheit im deutschen Militär? Auch das ist ein Anliegen deutscher Außenpolitiker*innen (denn wenn man aus der Vergangenheit lernt, kann man mit moralischer Überlegenheit überall in der Welt „intervenieren“). Zu jeder Forderung des Peng-Collectives kann das Militär also theoretisch laut „Ja!“ sagen. Eine radikale Politik sollte mehr als Optimierung des kapitalistischen Normalvollzugs sein.

MEHR INFOS IM INTERNET

Wer sich mit der Kunstform des Adbustings mehr beschäftigen möchte, findet dafür im Netz reichlich Ratschläge und Anschauungsmaterial. Auf dem Blog maqui.blogsport.eu finden sich neben ausführlichen Aktionsanalysen zu Kommunikationsguerilla-Aktionen auch viele Bilder von Adbustings zum Thema „Militär“.

ACHTUNG SATIRE:
ROHDE UND SCHWARZ ZUM FÜNFUNDACHZIGSTEN

DER HERR ROHDE UND DER HERR SCHWARZ DIE GRÜNDETEN FLEIßIG
IHRE FIRMA IM UNVERDÄCHTIGEN JAHR 1933
ZUM ENDE DES KRIEGES HATTEN SIE SCHON MEHRERE FABRIKEN
UND BEKAMEN BESUCH VON DER US-AIRFORCE UND DEN BRITEN
DOCH ANSTATT DAS UNTERNEHMEN ZURECHTZUSTUTZEN
WOLLTEN AUCH DIE DEUTSCHE MILITÄRFUNK-TECHNIK NUTZEN

WAS ROHDE UND SCHWARZ SO MACHEN?
VOR ALLEM SO ELEKTROMAGNETISCHE SACHEN.
SIE UNTERSUCHEN BANDBREITEN NACH ABSTRAHLUNGEN
UND DAMIT GRUNDLAGEN FÜR MILITÄRISCHE ENTSCHEIDUNGEN
UM DANN DAS KOMMANDO ZU ÜBERTRAGEN
BAUEN SIE AUCH DIE FUNKANLAGEN
WER IMMER DIE BEFEHLE ENTSCHLÜSSELT VERSTEHT
HAT ROHDE UND SCHWARZ IM EMPFANGSGERÄT
SIGNALE DES FEINDES WERDEN ZUGLEICH GESTÖRT
UND DIE SOCIAL MEDIA ABGEHÖRT.
LIEFERUNGEN AN DIKTATUREN ÜBERNEHMEN GERN,
TOCHTERFIRMEN VOM KONZERN.

DEN BND GIBT ES SEIT NEUNZEHNSECHSUNDFÜNFZIG
UND AUCH MIT DEM VERDIENT DAS UNTERNEHMEN ZÜNFTIG
WO GENAU DIE GRENZEN ZWISCHEN BEIDEN LIEGEN,
IST GAR NICHT SO GENAU HERAUSZUKRIEGEN.
NACHRICHTENTECHNIKER DER STASI ETWA NACH DER WENDE,
FANDEN DORT ANSTELLUNG OHNE ENDE
UND DABEI KAM IHR VERDIENST
DIREKT VOM DEUTSCHEN NACHRICHTENDIENST.

WER ES MIT DER WAHRHEIT ZU ENG NIMMT,
KANN ZWEIFELN OB ALL DAS GENAU SO STIMMT.
DOCH IM PRINZIP BESTEHT KEINE WAHL,
OHNE ROHDE UND SCHWARZ GIBTS KEIN SIGNAL.

KRIEG IM INFORMATIONSRAUM
DOKUMENTATION DES 21. KONGRESS DER
INFORMATIONSSTELLE MILITARISIERUNG
MÄRZ 2018. IMI-ONLINE.DE PREIS:5€

IMI Informationsstelle Militarisierung e.V.