Bundesakademie
für Sicherheitspolitik

Arbeitspapier Sicherheitspolitik, Nr. 24/2017

Informationskriege:
Eine Herausforderung für die Bundeswehr

von Carolin Busch und Nadine Düe

Information war schon immer eine wichtige Währung im Krieg. Nachdem das russische Militär diese wieder verstärkt auf seine Agenda gesetzt hat, ziehen nun auch westliche Streitkräfte und Militärbündnisse nach. Die Bundeswehr reagiert mit der Aufstellung des Kommandos Cyber- und Informationsraum jedoch vor allem auf die steigende Anzahl von Cyberangriffen. Diese sind jedoch nur ein Aspekt, der an Relevanz gewinnt. Es gilt ebenso, den Blick auf die kritische Rolle von Information zu werfen.

Anfang der 2000er Jahre ließen sich Sicherheitsexperten zuweilen noch dazu hinreißen, den Cyberraum als in keiner Weise vergleichbar zu anderen Operationsräumen, wie Land, Luft, See und Weltraum abzutun. So äußerte Dr. James Lewis, Direktor des *Center for Strategic and International Studies*, noch 2003 in einem Interview, dass Cyber-Angriffe eher „weapon of mass annoyance" denn „weapon of mass destruction" gleichkämen. Dieser Trend hat sich mittlerweile ins Gegenteil verkehrt. Die Ausschreitungen im estnischen Tallinn 2007 wurden von Cyber-Attacken begleitet, ebenso wie der Kaukasuskrieg 2008 zwischen Russland und Georgien. Weitere Beispiele sind der Cyber-Angriff auf das iranische Atomprogramm mittels des Computerwurms *Stuxnet* 2010 oder jüngst der Angriff mit der Schadsoftware *WannaCry*. Die Gefahren, die im und durch den Cyberraum entstehen, führten zu einer sogenannten „Cyberfizierung":[1] Allein die Nennung des Begriffs löst Assoziationen einer diffusen, allgegenwärtigen Bedrohungslage aus. Das Schlagwort *Cyber* wird zum Treiber einer engagiert geführten Debatte und zunehmend handlungsanleitend für Politik und Militär. Dabei sollte der Cyberraum nur als ein Teil des Informationsraums angesehen werden, dem zwar die Rolle eines Transmissionsriemens in Informationskriegen gleichkommt und ohne den *information warfare* heutzutage nicht mehr gedacht werden kann, der jedoch nicht den Blick auf die Natur von Informationskriegen verstellen sollte.

Die Bundeswehr hat sich diesen neuen Herausforderungen progressiv mit der Gründung eines eigenen militärischen Organisationsbereichs gewidmet: dem Cyber- und Informationsraum (CIR). Der Name legt es nahe, und bei der Berichterstattung über den beginnenden Aufbau des gleichnamigen Kommandos im April 2017 wird deutlich, dass der Schwerpunkt aktuell auf der Absicherung gegen Cyberangriffe liegt. Dass dieser Aspekt wichtig ist und die Bundeswehr hier Nachholbedarf hatte, steht außer Frage. Es gilt jedoch das „I" im CIR stärker in den Blickpunkt zu rücken und dementsprechend Fähigkeiten weiter aus- und aufzubauen.

Zumindest in Russland existiert bereits seit Jahren ein breiteres Verständnis. So spricht beispielsweise die russische Regierung nicht von sogenannter *Cyber Security*, sondern vielmehr von *Information Security*, was einen viel breiteren Ansatz impliziert. Die Technik selbst wird nur als einer von vielen Aspekten – und nicht als der

[1] Wagner, Ben / Vieth, Kilian (2016): Was macht Cyber? Epistomologie und Funktionslogik von Cyber, in: *Zeitschrift für Außen- und Sicherheitspolitik* 2, S. 213–222.

 | ISSN 2366-0805

wichtigste – der *Information Security* gesehen. Folgerichtig ist das Ziel Russlands, primär auch das Wissen sowie die Kultur des Landes zu schützen und den freien Fluss an Informationen zu gewährleisten – ein Aspekt, der über Cybersicherheit weit hinausgeht und der durch die russische Regierung aggressiv verfolgt wird.[2] Im Umkehrschluss sollte das nicht bedeuten, dass westliche Streitkräfte denselben Ansatz verfolgen sollten. Primär geht es zunächst darum, das sich daraus ergebende Bedrohungspotential für westliche Gesellschaften besser zu verstehen und darauf aufbauend gegebenenfalls entsprechende schützende Maßnahmen zu entwickeln.

Informationskriege der Zukunft

Der russische Einmarsch 2014 auf der Krim war vor allem ein Propagandaerfolg. Das systematische und konstante Leugnen der Präsenz russischer Truppen („little green men" ohne nationale Hoheitsabzeichen) führte dazu, dass sowohl die NATO als auch Journalisten die militärische Besetzung der Halbinsel zunächst unterschätzten. Generalmajor Gordon Davis, damals *Deputy Chief of Staff Operations & Intelligence* des obersten NATO Hauptquartiers SHAPE, gab zu, dass er und seine Kollegen aufgrund der russischen Dementis nicht auf Anhieb die Größe und das Ausmaß der russischen Truppenbewegungen begriffen. Auch im digitalen Informationsumfeld spannen (pro-)russische Akteure ein Netz aus Alternativdarstellungen, propagandistischen Narrativen und Falschinformationen.

Zwei sich einander bedingende Trends treffen hier aufeinander: erstens die Art und Weise, wie Auseinandersetzungen geführt werden und zweitens die zunehmende Vernetzung und Digitalisierung der Welt, welche die Auswirkungen von Konflikten verschärfen und die Zivilbevölkerung in einem bislang ungekannten Maße mit in den „Kampf der Narrative" ziehen beziehungsweise sie selbst zum Ziel machen.

1. Die Annexion der Krim hat Europa und der Welt vor Augen geführt, was schon lange bekannt, jedoch in der jüngsten Vergangenheit selten so machtvoll demonstriert wurde: Information selbst ist ein Angriffsziel und Mittel der Kriegsführung. 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. Besonders kritisch wirkt sich darauf außerdem die zunehmend unklare Abgrenzung von Krieg und Frieden aus. Heutigen Gesellschaften fällt es bisweilen sehr schwer, feindliche Propaganda als solche zu erkennen. Russische „Trolle" und „Bots" agieren konstant im digitalen Informationsumfeld. Die russische Propaganda in den baltischen Staaten, die vor allem die dort lebenden russischen Minoritäten adressiert, ist ein aktuelles Beispiel; es hat das Potential, bestehende Spannungen in den baltischen Gesellschaften zu verschärfen und sie zwischen pro-russischen Gruppen und denjenigen, die die Zukunft in Europa sehen, zu spalten.

Clausewitz hat die Natur des Krieges als eine „wunderliche Dreifaltigkeit" dargestellt. Eine der drei Komponenten beschrieb er als „Hass" und „Feindschaft", welche er dem Akteur des Volkes zuordnete, denn – so heißt es weiter in seinem Standardwerk – die „Leidenschaften, welche im Kriege entbrennen sollen, müssen schon in den Völkern vorhanden sein". 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. Experten sind sich weitgehend darin einig, dass aktuelle Formen der Kriegführung in weiten Teilen nichts Neues sind. Einige der Methoden Russlands in der Ukraine, wie Desinformation, sind beispielsweise aus der Sowjetunion und ihrem Geheimdienst, dem KGB, bekannt.

[2] Gady, Franz / Austin, Greg (2010): *Russia, The United States and Cyber Diplomacy. Opening the Doors*, EastWest Institute, S.5.

2. 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. Die zunehmende Verbreitung von Mobiltelefonen und Internetzugängen und das steigende Ausmaß ihrer Nutzung setzen Gesellschaften in ebenso steigendem Maße den Bedrohungen aus dem Cyberraum aus. Laut Statistiken der Internationalen Fernmeldeunion leben sieben Milliarden Menschen (und damit 95 Prozent der Weltbevölkerung) in Gegenden, die von Mobilfunknetzen abgedeckt werden. 84 Prozent der Weltbevölkerung leben in Gegenden mit mobilen Breitbandnetzen (3G oder mehr), die Internetzugang ermöglichen. In Europa sind nur 21 Prozent der Bevölkerung offline und die Verbreitung von Internetzugängen und billigen Smartphones wird die Zahl der Nutzer auch in anderen Teilen der Welt in den kommenden Jahren stark ansteigen lassen. Im selben Maße wird auch die Exponierung der Bevölkerung gegenüber digitaler Propaganda, *hate speech* oder Verschwörungstheorien zunehmen.

Der US-Wahlkampf im letzten Jahr eröffnete dabei eine neue Dimension. Die gehackten E-Mails von Hillary Clinton gelten als russische Sabotageaktion. Für weitere Aufregung sorgte eine von Donald Trumps Team beauftragte Datenanalysefirma, Cambridge Analytica: Sie soll Wählergruppen durch maßgeschneiderte Werbung gezielt beeinflusst haben. In einem Umfeld, das so gespalten ist wie die politische Landschaft der USA finden externe Akteure leicht einen fruchtbaren Boden, um Differenzen innerhalb der Bevölkerung auszunutzen. Das Netz polarisiert.

Verstärkend trägt dazu auch das Phänomen der sogenannten Filterblasen bei: Internetnutzer werden, zuvorderst in sozialen Onlinemedien, nur Inhalten ausgesetzt, die mit den eigenen Ansichten übereinstimmen. Basierend auf den besuchten Webseiten, der Verweildauer, den *Likes* und den Aktivitäten der vernetzten Freunde und *Follower* in sozialen Netzwerken erstellen Unternehmen wie Google oder Facebook mittels Algorithmen ein Datenprofil des Nutzers, welches zu personalisierten Suchergebnissen führt und gegenläufige Informationen herausfiltert. In der Folge ist der Nutzer immer seltener anderen Darstellungen und Werten als den eigenen ausgesetzt – bis er, wie der Internetaktivist Eli Pariser schreibt, in seiner „Informationsblase“ isoliert ist und nur noch in seinen bereits bestehenden Meinungen bestärkt wird.

Beide Trends haben in ihrer Verbindung viele, teils bislang vernachlässigte Folgen für die Sicherheitspolitik und die Streitkräfte, die sich je nach Szenario unterscheiden: In militärischen Operationen geringer oder mittlerer Intensität wie KFOR seit 1999 im Kosovo oder ISAF bis 2014 in Afghanistan spielt die Deutung des Konflikts in der Öffentlichkeit eine entscheidende Rolle. Vergangene Szenarien haben gezeigt, dass die NATO ihre eigenen politischen Ziele nicht oder nur kaum erreichte. Das digitale Informationsumfeld bietet neue Chancen, indem es beispielsweise einen direkteren Zugang zu der Lokalbevölkerung in (potenziellen) Einsatzländern ermöglicht. Es steht für Streitkräfte nicht mehr zur Debatte, ob sie in den digitalen Medien präsent sind, sondern auf welche Art und Weise. Gruppen wie der sogenannte Islamische Staat haben gezeigt, welches Potential in darin liegt: Eine Terrorgruppe in Syrien und dem Irak schaffte es, unter anderem über soziale Netzwerke tausende Rekruten für ihren Krieg zu gewinnen. Streitkräfte können es sich nicht leisten, dieses „Schlachtfeld“ nicht zu beachten. Dabei reicht das theoretische Spektrum eigener Möglichkeiten von der Nutzung sozialer Medien bis hin zum Aufbau und Verfügbarmachen von Funknetzen und dem Zugang hierzu in Gegenden, in denen kaum digitale Anbindung besteht.

In einem hochintensiven Konfliktszenario wie einem Krieg zwischen Industriestaaten stellt sich die Frage, welchen Beitrag Streitkräfte zur vielzitierten Resilienz von Gesellschaften gegen gegnerische Propaganda und Desinformationskampagnen beitragen können. Ein Einsatz von Streitkräften im Rahmen von Landes- oder Bündnisverteidigung wird andere Informationskampagnen und eine andere Mediennutzung mit sich bringen. Gerade in einem Konfliktszenario mit einem technologisch fortgeschrittenen, nichtdemokratischen Staat stellt sich zudem die Frage, wie dessen Bevölkerung und Streitkräfteangehörige überhaupt noch erreicht werden können, wenn der Gegner digitale Abschirmungsmaßnahmen ergreift. In solch einem Fall dürften Soldaten beispielsweise kein privates Smartphone mit sich tragen. Laut russischer Medien hat Russlands Militär beispielsweise ein eigenes, geschlossenes „Internet“, das nicht an das globale Internet ange-

schlossen ist. 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.

Doktrinäre Landschaft der Bundeswehr

Das Weißbuch 2016 leistet Vorarbeit in der Definition des Cyber- und Informationsraums als sicherheitspolitisches Handlungsfeld: „Die sichere und gesicherte sowie freie Nutzung des Cyber- und Informationsraums ist elementare Voraussetzung staatlichen und privaten Handelns in unserer globalisierten Welt." Die „Ungehinderte Nutzung von Informations-, Kommunikations-, Versorgungs-, Transport- und Handelslinien" sei eine strategische Priorität. Damit zielt das Weißbuch vor allem auf den Aspekt des Zugangs ab. Tatsächlich sind unsere Kommunikationsinfrastrukturen unverzichtbarer Bestandteil unserer Gesellschaft geworden. Ein flächendeckender Ausfall beispielsweise des Internets würde mittlerweile großen wirtschaftlichen Schaden verursachen.

Weniger betont das Weißbuch hingegen die Information selbst. Informationskriege haben die materiellen Aspekte des Kriegs überschritten. Die Beeinträchtigung und physische Zerstörung von Informationsinfrastruktur und IT trägt eine große Bedrohung in sich: Trojaner, Viren und Versuche, Daten zu löschen, fallen in diese Kategorie. Allerdings muss eine weitere Dimension durchdrungen werden: Immateriell wird der Informationskrieg immer dann, wenn es darum geht, in Gesellschaften Zweifel beispielsweise an Darstellungen der politischen Eliten oder der Medien (Stichwort „Fake News") zu säen. 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. Die vielen Versuche Russlands, beispielsweise die Einheit der Europäischen Union durch gezielte Falschinformationen und -darstellungen zu unterminieren folgen nicht primär dem Ziel, dass die Europäer die russische Darstellung als die richtige ansehen, sondern dass sie jener der eigenen politischen Eliten zu zweifeln beginnen. Nach dem Abschuss der Passagiermaschine MH17 in der Ostukraine im Sommer 2014 beispielsweise kehrte die russische Regierung mit ihren teilweise widersprüchlichen und an Verschwörungstheorien grenzenden Erklärungen über die genauen Ursachen und die Täterschaft die Beweislast um. Verschiedene Organisationen, Behörden und Think Tanks wiesen daraufhin nach bisweilen akribischer Arbeit die Beteiligung Russlands nach. Diese Arbeiten sind teilweise noch immer nicht abgeschlossen.

Die Verteidigungspolitischen Richtlinien von 2011 warnen, dass Entwicklungen im Bereich der Telekommunikations- und Informationstechnologie auch Extremisten „vielfältige Chancen für Desinformation und Radikalisierung und Destabilisierung" eröffnen. Die zunehmende Zersplitterung des Internets, das heißt die teilweise extrem unterschiedlichen nationalen Gesetzgebungen im Netz – unter anderem durch Bestrebungen Russlands und Chinas, das „eigene" Internet stark zu zensieren – führen dazu, dass manche Gesellschaften auf medialer Ebene in der eigenen Filterblase isoliert leben und nur die eigenen Narrative erzählt bekommen, in der die eigenen (Vor-)Urteile permanent bestätigt werden können.

Auch wenn Deutschland mit der Einrichtung eines Kommandos Cyber- und Informationsraum diesem Thema einen hohen Stellenwert einräumt, so hinkt die nationale Umsetzung vieler der benötigten Antworten auf neue Herausforderungen, gerade im Bereich Digitalisierung und Informationskrieg, anderen Nationen hinterher. Die Erfolgsformel der Zukunft liegt in der Fähigkeit, die verschiedenen Teilmengen des Cyber- und Informationsraums nicht mehr getrennt voneinander zu betrachten, sondern die technischen Komponenten in Verbindung mit sicherheitspolitischen Interessen und Diskursen zu betrachten. Eine Reaktion darauf muss diese Bandbreite an komplexen Herausforderungen abdecken. Diesen Weg verfolgt beispielsweise das US Central Command, um die Terrororganisation Islamischer Staat weiter zu schwächen und seine Anwerbungsbemühungen zu unterbinden. Ziel ist es dabei, die digitale Informationsumgebung zu nutzen und im eigenen Sinne zu beeinflussen.

Mit dem Aufbau des Organisationsbereichs Cyber- und Informationsraum bildet die Bundeswehr die Voraussetzung, den militärischen Risiken und Bedrohungen aus dem Cyber- und Informationsraum zu begegnen und die mit dieser Dimension verbundenen Chancen und Möglichkeiten zu nutzen. Große Herausforderungen liegen jetzt beispielsweise in der Entwicklung von militärischen Fähigkeiten, um auf die neuen Bedrohungen zu antworten, der Weiterentwicklung der Konzeptlandschaft und in der Anpassung der Ausbildung – nicht nur im Bereich Cyber, sondern gerade auch den Informationsraum betreffend.

Sowohl im Bereich Nationale Krisenvorsorge als auch in den Einsätzen der Bundeswehr steht eine tiefergehende Befassung mit dem Thema digitale Medien sowie eine entsprechende Fähigkeitsentwicklung und -umsetzung noch aus. Weitere zu klärende Fragen betreffen den Beitrag, den die Bundeswehr zur gesamtstaatlichen Sicherheitsvorsorge im Cyber- und Informationsraum stellt und wie ein solcher Beitrag mit zivilen Behörden koordiniert und von ihnen abgegrenzt werden müsste. Die Behandlung und Beantwortung dieser und weiterer Fragen sind eine unabdingbare Grundlage für das erfolgreiche Begegnen von Bedrohungen und Risiken sowie das zielgerichtete Nutzen von Chancen und Möglichkeiten, die mit dem Cyber- und Informationsraum verbunden sind. Dies umfasst das Identifizieren und die Priorisierung von national oder gemeinsam mit Partnern zu beherrschenden Schlüsseltechnologien, die gezielte Steuerung von Forschung und Technologie, aber vor allem auch eine realistische Roadmap für den Fähigkeits- und Personalaufbau der Bundeswehr (und ihrer Partner), beispielsweise im Bereich der Kommunikation, und eine praxisnahe Ausbildung der Soldatinnen und Soldaten.

Dr. Carolin Busch und Nadine Düe sind Analystinnen und Beraterinnen im Bereich „Verteidigung & Sicherheit“ der IABG mbH. Die Autorinnen geben ihre persönliche Meinung wieder.