MARCIN BIELECKI/EPA/DPA-BILDFUNK

Will eine neue Teilstreitkraft aus dem Boden stampfen: Verteidigungsministerin Ursula von der Leyen hat Ende April die Schaffung des 13.500 Dienstposten umfassenden »Cyber- und Informationsraums« verkündet (hier am 14.4.2015 in Tallin beim »NATO Cooperative Cyber Defence Centre of Excellence«)

»Wehrfähigkeit stärken«

Die Bundeswehr legt sich eine Cyperspacearmee zu. Legitimiert wird die Befähigung zu digitalen Angriffen mit »hybrider Kriegsführung« der Feinde des Westens. **Von Peer Heinelt**

Prophetische Fähigkeiten sind nicht vonnöten, um zu wissen, was in dem vom Bundesverteidigungsministerium für den Sommer angekündigten »Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr« zu lesen sein wird. Mit Sicherheit werden sich weite Passagen des militärpolitischen Grundlagendokuments mit dem sogenannten Cyberwar, dem Krieg im World Wide Web, befassen. Schon Monate bevor Verteidigungsministerin Ursula von der Leyen (CDU) Ende April die Aufstellung einer 13.500 Dienstposten umfassenden Teilstreitkraft »Cyber- und Informationsraum« (CIR) bekanntgab, hatte sie bei einem »Expertenworkshop« zum neuen »Weißbuch« in Berlin entsprechende Absichten bekundet. Man werde einen »neuen Organisationsbereich« innerhalb der Truppe aufbauen und einem »Kommando CIR« unterstellen, ließ die Ressortchefin bei der Veranstaltung Mitte September letzten Jahres wissen. Das Ziel bestehe darin, die »vielfältigen Strukturen« und bis dato »zersplitterten Zuständigkeiten« auf dem Gebiet der Informationstechnik (IT) zusammenzuführen – »zu einer einheitlichen IT-Architektur«.

Zur Begründung erklärte von der Leyen, »Cyberangriffe« seien mittlerweile »fester Begleiter konventioneller Operationsführungen« und verwies auf die vermeintliche Aggression Russlands gegen die Ukraine. Zudem stärkten »Cybermittel« allerlei »asymmetrische Kräfte«, die sich zur Durchsetzung ihrer politisch-militärischen Ambitionen der Methoden des Guerillakampfes bedienten: »Cyberwaffen sind schlichtweg eine kostengünstige und effektive Möglichkeit, die Funktionsfähigkeit ganzer Gesellschaften und ihrer Streitkräfte anzugreifen.« Zunächst gehe es folglich um den »Selbstschutz« der »zunehmend digitalisierten Großorganisation Bundeswehr«, so die Ministerin – doch damit nicht genug: Da aus dem »Cyber- und Informationsraum« heraus für »gravierende Störungen und Zerstörungen« in den »anderen klassischen Dimensionen Land, Luft, See und Weltraum« gesorgt werden könne, benötige die Truppe nunmehr die »gesamte Palette an Fähigkeiten«, also auch die Fähigkeit zum Angriff auf feindliche Computernetze. Um Analogien war die Ressortchefin dabei nicht verlegen: Beim Krieg im »Luftraum« kämen schließlich ebenso »Aufklärungsdrohnen« wie Kampfjets »parallel« zum Einsatz, ließ sie ihre Zuhörer wissen.

Militärisch-industrielle Kooperation

Die Teilnehmer des besagten »Workshops« zum neuen »Weißbuch« dürften sich insbesondere über die Ankündigung von der Leyens gefreut haben, sie werde die »Kooperation mit Wissenschaft und Wirtschaft« im Bereich IT »intensivieren« und die »nationale Industrie« bei der Entwicklung dieser »Schlüsseltechnologie« nach Kräften unterstützen. Diese »nationale Industrie« wiederum war an der Planung und Durchführung der Veranstaltung maßgeblich beteiligt: Zu den Organisatoren zählte neben dem Innen- und dem Verteidigungsministerium auch der Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (Bitkom). Die Lobbyvereinigung vertritt nach eigenen Angaben mehr als 2.300 IT-Unternehmen, die mit ihren insgesamt 700.000 Beschäftigten jährlich Inlandsumsätze in Höhe von 140 Milliarden Euro erzielen und Waren im Wert von weiteren 50 Milliarden Euro exportieren. Unter den Mitgliedern des Verbandes finden sich nicht nur Konzerne wie die Deutsche Telekom und die deutschen Tochtergesellschaften von Google, Microsoft oder IBM, sondern auch Rüstungsfirmen wie Dassault und Rohde & Schwarz. Bitkom unterhält eigens einen »Arbeitskreis Verteidigung«, der sich die »Modernisierung der Bundeswehr« auf die Fahnen geschrieben hat und erklärtermaßen seinen »Beitrag« zur Aufstellung des neuen »Cyber- und Informationsraumkommando(s)« leisten will.

Unter Bezugnahme auf den »Expertenworkshop« zum neuen »Weißbuch« präsentierte der Bitkom-Arbeitskreis am 22. Februar ein »Positionspapier«, in dem er seine Vorstellungen über die »digitale Transformation« der Bundeswehr präzisiert. Dass eine solche zwingend erforderlich ist, steht für die Autoren außer Frage, ergäben sich hieraus doch »ganz neue Möglichkeiten im Bereich Effektivität und Dynamisierung« – beginnend mit der »Herstellung von Ersatzteilen direkt im Einsatzgebiet durch 3-D-Druck« über die »Datenerfassung und -analyse zur Informationsgewinnung« bis hin zur »moderne(n) Lagebilderstellung für das vernetzte Gefechtsfeld«, ganz zu schweigen von einem »effizientere(n) Personaleinsatz in Waffensystemen (z. B. Fregatten oder Panzern)«. Voraussetzung für eine entsprechende innovative Nutzung von »Schlüsseltechnologien« und die damit verbundene Erringung »digitale(r) Souveränität« sei allerdings die Etablierung eines »Chief Information Officers« (CIO) im Bundesverteidigungsministerium (BMVg). Dieser müsse sowohl über »planerische und haushälterische Eigenständigkeit« als auch über entsprechende »Weisungsbefugnisse« verfügen, da nur so eine »Gesamt-IT-Architektur« für die Truppe geschaffen werden könne, während gleichzeitig »uneffektive Insellösungen« vermieden würden, heißt es.

Dabei fehlt selbstverständlich nicht der Hinweis, dass IT im »zivilen Sektor« bereits »vielfältig eingesetzt wird und mit teilweise geringen Adaptionen an die militärischen Anforderungen angepasst werden kann«. Ebenso böten sich bei der Rekrutierung und Qualifizierung von geeignetem Fachpersonal »Ausbildungskooperationen mit Hochschulen und Unternehmen« an, erklärt der Bitkom-Arbeitskreis. Wie die Autoren weiter ausführen, komme die Bundeswehr mittelfristig zwar nicht um »eigene Laufbahn- und Besoldungsmodelle« für IT-Spezialisten herum, jedoch könnten in der Zwischenzeit »Kooperationsmodelle« entwickelt werden, »die über Auslagerung und externe Vergabe bestimmte Dienstleistungen zur Verfügung stellen«.

Grundsätzlich spricht sich der Branchenverband in seinem »Positionspapier« für eine »konsequente Zentralisierung« der staatlichen IT-Infrastruktur im Rahmen eines »ressortübergreifenden Ansatz(es)« aus. Ein solches Vorgehen habe nicht nur das »Potential für erhebliche Verbesserungen und Einsparungen«, sondern ermögliche der Bundeswehr darüber hinaus, »heute noch für behördliche Standardaufgaben gebundene Kapazitäten für verteidigungs- und sicherheitsrelevante Aufgaben ein(zu)setzen«, heißt es. Dies gelte »gerade im Hinblick auf die asymmetrische Bedrohungslage aus und im Cyberraum«.

»Nationale Schlüsseltechnologien«

Die von der IT-Lobby nicht zuletzt mit Blick auf das neue »Weißbuch« formulierten Forderungen finden sich nahezu eins zu eins im Abschlussbericht des von der Verteidigungsministerin eingesetzten »Aufbaustabes Cyber- und Informationsraum«. Das Gremium unter Leitung des stellvertretenden Generalinspekteurs der Bundeswehr, Generalleutnant Markus Kneip, und des »Beauftragten Strategische Steuerung Rüstung« im BMVg, Gundbert Scherf, legte seinen Report im April dieses Jahres vor. Gleich zu Beginn ist hier zu lesen, die »Verantwortung für die Themen Cyber und IT« innerhalb des Hauses von der Leyen würden nunmehr in der Hand eines »Chief Information Officers« (CIO) »gebündelt«: »Diese bzw. dieser steuert sowohl die technologische/technische Weiterentwicklung von Cyber/IT, einschließlich der IT-Architekturen, als auch Einsatz, Betrieb und Schutz der IT in der Bundeswehr sowie die BWI [Bundeswehr Informationstechnik GmbH – P. H.] als Inhouse-Gesellschaft. Ihm oder ihr muss dafür ein mit der Gesamtplanung der Bundeswehr harmonisiertes Budget zur Wahrnehmung seiner bzw. ihrer Planungsverantwortung eingeräumt werden.«

Auch die Ausführungen des »Aufbaustabes« über die »Einbeziehung der Wirtschaft« in die »Cyber-Verteidigung« tragen die Handschrift des Bitkom. Zwecks »Sicherung der digitalen Souveränität« Deutschlands und »Schaffung nationaler Schlüsseltechnologien« sei die »enge Verzahnung mit Behörden, Forschung, Lehre (und) Industrie« im IT-Bereich unabdingbar, heißt es. Zudem fordern die Autoren, bei der Beschaffung digitaler Rüstungsgüter verstärkt auf »marktverfügbare« Produkte kommerzieller Anbieter zurückzugreifen: »Dies spart Entwicklungszeit für aufwändige Speziallösungen, reduziert Kosten und ermöglicht damit eine schnellere Einführung von IT.«

Grundsätzliche Einigkeit mit den Vertretern der IT-Branche besteht auch hinsichtlich der »ressortübergreifende(n) Kooperation im Cyberraum«. So sprechen sich die Autoren des »Abschlussberichts« für einen »dauerhaften Dialog« aller »für innere und äußere Sicherheit zuständigen Ministerien« aus, um »Fragen überlappender Zuständigkeiten« zu klären und »Synergiepotentiale« auszuloten: »Mit der proaktiven, dauerhaften Kooperation und Zusammenarbeit mit anderen Ressorts bei der Aufgabenwahrnehmung in der gesamtstaatlichen Sicherheitsvorsorge bestehen gute Aussichten, die Verfügbarkeit informationstechnischer Systeme bei Cyberangriffen und Attacken gegen Staat, Wirtschaft und Gesellschaft übergreifend zu gewährleisten.«

Wie die Verteidigungsministerin will sich der »Aufbaustab Cyber- und Informationsraum« allerdings nicht auf eine rein defensive Rolle der »digitalen Kräfte« der Bundeswehr festlegen. Es gelte, »die gesamte Kette von Prävention zu Reaktion sowie von einfachen bis komplexen Angriffen zu beherrschen«, heißt es im »Ab-

schlussbericht« des Gremiums. Folgerichtig wird das World Wide Web denn auch als »Operationsraum« definiert, in dem die Truppe eine ganze Reihe von »Aufgaben« wahrnehmen soll. Diese reichen von der Absicherung des eigenen IT-Systems und anderer »kritischer« Infrastrukturen über die Erstellung eines politisch-militärischen »Lagebildes« und die Identifizierung feindlicher »Propaganda und Desinformation« bis hin zur Beeinflussung der »Meinungsbildung im Informationsumfeld der Interessengebiete der Bundeswehr und in mandatierten Einsätzen«. Explizit vorgesehen sind darüber hinaus »Maßnahmen des elektronischen Kampfes« und sogenannte Computer-Netzwerk-Operationen (CNO) – mithin gezielte Attacken auf IT-Einrichtungen des Gegners.

MAURIZIO GAMBARINI/DPA-BILDFUNK

NATO-Übung »Saber Strike« (Säbelschlag) gegen einen Gegner, gemeint ist Russland, dem man perfide Kriegsmethoden unterstellt (im vom Militär freigegebenen Bild ein deutscher Soldat, 19. Juni 2015)

»Verwundbarkeiten des Westens«

Legitimiert wird der Aufbau von Kapazitäten zum digitalen Angriff mit der vermeintlichen Perfidie des Feindes. Als besonders verwerflich gilt deutschen Militärplanern eine vor allem Russland zugeschriebene »hybride Kriegsführung«, die mit »Cyber-Angriffen« einhergeht. Laut dem von Verteidigungsministerin von der Leyen eingesetzten »Aufbaustab Cyber- und Informationsraum« basiert die »hybride Strategie« dabei auf »einer breiten, komplexen, anpassbaren und meistens hoch integrierten Kombination von konventionellen und/oder unkonventionellen Mitteln, offener und/oder verdeckter Aktivitäten von militärischen, paramilitärischen und/oder zivilen Akteuren, durchgeführt im gesamten Fähigkeitsspektrum, gezielt ausgerichtet auf die Entscheidungsfindung und das Erschweren eigener Aktivitäten«. Etwas konkreter wird ein in die aktuellen Weißbuchplanungen involviertes Autorenteam der von der Deutschen Gesellschaft für Auswärtige Politik (DGAP) herausgegebenen Zeitschrift *Internationale Politik* schon im Juni 2015. Nach Auffassung von James Hackett und Alexander Nicoll bedient sich Moskau gegenüber der Ukraine und den baltischen Staaten einer »synchronisierte(n) Mischung aus militärischem Druck, Spezialeinsätzen und Geheimdienstoperationen zusammen mit ziviler Revolte, feindseliger Propaganda, Informationsoperationen, Cyberattacken und ökonomischem Zwang«.

Folgerichtig machen sich Hackett und Nicoll denn auch ausgiebig Gedanken darüber, wie Deutschland und die NATO die vermeintliche Aggression Russlands »kontern« könnten. Unter anderem empfehlen sie den Einsatz neuer Überwachungs- und Analysetechniken sowie die Rekrutierung von Experten »mit einem langjährigen Wissen über Länder, Kulturen und Sprachen«, um »die Sicherheitsumgebung in fragilen Regionen und in potentiell oder tatsächlich feindseligen Staaten besser zu verstehen« und »Zeichen hybrider Aktivitäten in befreundeten Staaten früher (zu) erkennen«. Im Fokus der Beobachtung müssten dabei insbesondere »marginalisierte gesellschaftliche Gruppen« stehen, »die für äußere Einflüsse empfänglich sind«, heißt es. Des weiteren sprechen sich die Autoren für eine »agilere Informationspolitik« aus. So könnten etwa die NATO oder ihre Mitgliedsstaaten militärische »Verschlusssachen« der Öffentlichkeit zugänglich machen, »wenn diese überzeugende Beweise für feindselige Aktivitäten liefern«.

Überhaupt seien nunmehr »kluge Investitionen« gefordert, erklären Hackett und Nicoll: Ausgehend von einem »umfassenden Ansatz«, der »militärische, diplomatische, informationelle und ökonomische Aktivitäten« ebenso beinhaltet wie »Cyber- und Strafverfolgungsmaßnahmen«, fordern sie den verstärkten Aufbau von »Spezialeinheiten und schnelle(n) Eingreiftruppen«, um jederzeit »sowohl Angriffs- als auch Verteidigungsmaßnahmen ausführen zu können«. Dies gelte umso mehr, als »potentielle Feinde auf der ganzen Welt die Situation in der Ukraine genau beobachten und ihre Schlüsse ziehen, welche Taktiken funktionieren und wie die westlichen Regierungen und ihre Armeen auf Bedrohungen reagieren«.

In die gleiche Kerbe schlägt auch ein weiteres Autorenteam der *Internationalen Politik*, das wie seine Kollegen Hackett und Nicoll maßgeblich an der Erarbeitung des neuen »Weißbuchs« beteiligt ist: Claudia Major und Christian Mölling von der Berliner »Stiftung Wissenschaft und Politik« (SWP) fordern in einem Aufsatz die Entwicklung einer »hybride(n) Sicherheitspolitik«. Zur Begründung verweisen sie auf vier zentrale »Verwundbarkeiten« des Westens, zu denen ihrer Ansicht nach in erster Linie die »militärische Schwäche« der NATO im Vergleich zu Russland und dem »Islamischen Staat« zählt: »Die NATO selbst hat festgestellt, dass sie für einen großen zwischenstaatlichen Konflikt nicht ausreichend vorbereitet ist. Andere Akteure könnten versucht sein, diese Schwäche zu nutzen, um ihre Interessen militärisch durchzusetzen. Ein solches Szenario wird vor allem für das Baltikum befürchtet. Außerdem können sich die Europäer einem Konflikt an den eigenen Grenzen, sei es im Osten oder Süden, kaum entziehen – weil das Grenzgebiet destabilisiert, europäische Interessen berührt würden oder weil Kämpfe übergriffen.«

Eine weitere »Verwundbarkeit« sehen Major und Mölling in der »mangelnde(n) politische(n) Geschlossenheit« der EU. Während »in den baltischen Staaten die Erinnerung an ihre Annexion durch die Sowjetunion 1940 noch recht frisch« sei, so heißt es, betrachte etwa Frankreich Russland »nicht (als) das Hauptproblem«, sondern befasse sich lieber mit der »Instabilität der Sahel-Zone«: »Das birgt Spaltungspotential.« Des weiteren attestieren die Autoren dem Westen eine enorme »Abhängigkeit« von »internationalisierten Infrastrukturen und Strömen an Waren, Dienstleistungen, Personen und Kapital«: »Die Offenheit, von der Europa so profitiert, macht es auch anfällig für Störungen seiner globalen Interdependenzen.« Nach Auffassung von Major und Mölling ist zudem die »Pluralität der westlichen Gesellschaften« ein »wunde(r) Punkt«: »Die wesentliche Lehre aus der Ukraine-Krise lautet, dass der Beginn einer Eskalation derzeit wohl nicht in der Invasion einer Panzerdivision aus dem Osten bestehen würde, sondern darin, dass Staaten von innen destabilisiert werden, etwa indem Minderheiten aufgewiegelt werden.«

Als Therapeutikum gegen die von ihnen diagnostizierten »Verwundbarkeiten« empfehlen die Autoren einen »Dreiklang aus Abschreckung, Resilienz und Verteidigung«. »Abschreckung« verstehen sie dabei analog zur NATO-Doktrin aus der Zeit des Kalten Krieges gleichermaßen »konventionell« wie »nuklear«, ist ihrer Auffassung nach doch der »militärische Konflikt« mit Russland »ein Risiko, gegen das sich Europa wappnen muss«. Zudem habe Moskau mehrfach »demonstrativ« die Einsatzfähigkeit seiner Atomwaffen »unter Beweis gestellt«. »Resilienz« – Widerstandsfähigkeit – definieren Major und Mölling als Fähigkeit westlicher Gesellschaften, sich von Angriffen gleich welcher Art möglichst »rasch zu erholen«. Hierfür müsse insbesondere der soziale »Zusammenhalt« gestärkt werden, heißt es; gefragt sei eine »Migrations- und Integrationspolitik«, die »Zuwanderung steuert«, »Radikalisierungen« den Boden entzieht und »Minderheiten« so behandelt, »dass sie gegen Aufwiegelung unempfindlich werden«. Scheitere indes die »Abschreckung« potentieller Angreifer, bleibe die »Verteidigung von Territorium und staatlichen Institutionen« die »zentrale Aufgabe« des westlichen Militärs, erklären die SWP-Mitarbeiter – und warnen gleichzeitig davor, darüber das »Krisenmanagement« in aller Welt zu vernachlässigen: »Die EU- und NATO-Staaten können ihre Sicherheit nicht allein durch den Schutz von Territorium gewährleisten. Angesichts globaler Interdependenzen werden sie ihre Sicherheit auch künftig außerhalb Europas verteidigen müssen.«

Cyberwar gegen Russland

Entsprechend den zitierten Vorgaben äußerten sich die Teilnehmer eines »Expertenworkshops« zum neuen »Weißbuch«, der am 23. Juni letzten Jahres in Berlin stattfand und sich mit den »Perspektiven hybrider Kriegsführung« befasste. Unter den anwesenden 80 Fachleuten aus Politik, Thinktanks, Stiftungen, Wissenschaft und Militär mit Verteidigungsministerin von der Leyen an der Spitze herrschte laut einer Darstellung auf der Internetseite ihres Hauses Konsens darüber, dass Streitkräfte Teil der »Klaviatur der gesamtstaatlichen Sicherheitsvorsorge« sind. Der zugehörige »strategische Ansatz« wurde mit den Begriffen »Deter – Contain – Protect« beschrieben: »Abschrecken – Eindämmen – Schützen«.

Diesem Beitrag zufolge machten sich die Besucher des »Workshops« zudem ausgiebig Gedanken darüber, wie eine durch die Verbreitung von »Desinformation« im World Wide Web hervorgerufene »Destabilisierung« westlicher Gesellschaften zu verhindern ist. Dies sei umso dringlicher, als in den Staaten der EU ein weit verbreitetes »Misstrauen gegenüber der Politik« anzutreffen sei, das »hybride Krieger ausnutzen könnten«, so die einhellige Meinung. Der »Krisenfrüherkennung« wurde folglich »zentrale Bedeutung« beigemessen. Unter anderem kam man überein, Nichtregierungsorganisationen als »Sensoren« einzusetzen, um »möglichst breite und differenzierte Informationen« über die Haltung der jeweiligen Bevölkerung zu gewinnen. Als geradezu wegweisend erachtet das Verteidigungsministerium in diesem Zusammenhang offenbar das Entstehungsverfahren des neuen »Weißbuchs«. Die Einbindung ziviler Experten und die kontinuierliche Berichterstattung über deren Beratungen auf den Webseiten des Ministeriums trage wesentlich dazu bei, »sicherheitspolitische Prozesse transparenter und damit verständlicher zu machen«, heißt es – geht es doch erklärtermaßen darum, »Vertrauen« zu generieren.

En passant macht dieser Bericht über den besagten »Workshop« damit deutlich, was es mit dem neuen »Weißbuch« auf sich hat: Es handelt sich um ein Propagandainstrument, mit dessen Inhalten, wie der Generalinspekteur der Bundeswehr, Volker Wieker, unlängst so treffend formulierte, die »Wehrfähigkeit künftiger Generationen« erhalten und gestärkt werden soll. Erklärtes Ziel ist die Formierung eines nationalen Kollektivs, das sowohl die staatlichen »Sicherheitsbehörden« rückhaltlos unterstützt als auch »resilient« gegen informationelle Anfechtungen aller Art ist. Zu diesem Zweck werden Feindbilder konstruiert; als solche fungieren Russland und sogenannte asymmetrische Kräfte, die umstandslos mit den Massenmördern des »Islamischen Staats« gleichgesetzt werden. Ihnen werfen die Macher des »Weißbuchs« eine »hybride Kriegsführung« vor, die darauf angelegt ist, das Vertrauen der Menschen in die Politik der westlichen Metropolen zu untergraben. Vor diesem Hintergrund gerät die Fähigkeit zur Führung eines »Cyberwar«, eines Kriegs im virtuellen Raum, für die deutschen Militärstrategen zur entscheidenden Schnittstelle: Er ermöglicht nicht nur, die Medien und die Infrastruktur potentieller Feinde nachhaltig zu schädigen, sondern auch, die eigene Propaganda wirkungsvoll im World Wide Web zu plazieren. Das dafür notwendige Know-how liefert die deutsche IT-Industrie, die sich vor Begeisterung über die »digitale Transformation« der Bundeswehr schon seit längerem kaum halten kann.

■ Peer Heinelt schrieb an dieser Stelle zuletzt am 13.6.2015 über den »Tag der Bundeswehr«.

■ **Lesen Sie morgen auf den *jW*-Themaseiten:**

Kolonialistische Grenzziehung. 100 Jahre Sykes-Picot-Abkommen
Von Knut Mellenthin