Cyber an die Front –
Zur Handlungsfähigkeit der Bundeswehr im Cyber- und Informationsraum

Ralph D. Thiele

Juni 2016

Zusammenfassung

Die Zahl staatlicher und nichtstaatlicher Akteure im Cyber- und Informationsraum wächst atemberaubend schnell. Während die Bundeswehr bislang ordentlichen Abstand zur Spitze des Fortschritts in Sachen Cyber hält, behandeln die NATO und etliche Partnerländer den Cyber- und Informationsraum schon länger als einen eigenen Operationsraum. Verteidigungsministerin von der Leyen hat angekündigt, mit dem Kommando Cyber- und Informationsraum bis zum April 2017 eine neue Teilstreitkraft der Bundeswehr aufzubauen. Sie will die IT-Kompetenz in der Bundeswehr bündeln und effektiver nutzen. Zugleich sollen der Schutz der Truppe und gegebenenfalls auch der Schutz der Bevölkerung verbessert werden. Auf dem Weg ins digitale Zeitalter besteht für die Bundeswehr allerdings noch erheblicher Handlungsbedarf. Relevanten Überlegungen stehen strukturelle Mängel, zu kurz gesprungene konzeptionelle Grundlagen, eine Kannibalisierung bestehender Strukturen und unzulängliche Investitionen gegenüber. Die neue Aufstellung im Cyber- und Informationsraum sollte sich mit Priorität daran orientieren, dass die Bundeswehr als eine kombattante Organisation politisch-parlamentarische Zwecke im Einsatz erfolgreich umsetzen soll.

Das ISPSW

Das Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung (ISPSW) ist ein privates, überparteiliches Forschungs- und Beratungsinstitut.

In einem immer komplexer werdenden internationalen Umfeld globalisierter Wirtschaftsprozesse, weltumspannender politischer, ökologischer und soziokultureller Veränderungen, die zugleich große Chancen, aber auch Risiken beinhalten, sind unternehmerische wie politische Entscheidungsträger heute mehr denn je auf den Rat hochqualifizierter Experten angewiesen.

Das ISPSW bietet verschiedene Dienstleistungen – einschließlich strategischer Analysen, Sicherheitsberatung, Executive Coaching und interkulturelles Führungstraining – an.

Die Publikationen des ISPSW umfassen ein breites Spektrum politischer, wirtschaftlicher, sicherheits- und verteidigungspolitischer Analysen sowie Themen im Bereich internationaler Beziehungen.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analyse

1. Abstand zur Spitze

China tut es. Israel und die USA haben es getan. Jetzt gründen auch die deutschen Streitkräfte ein eigenes Kommando für die Operationsführung im Cyberraum. Mit ordentlichem Medien-Auftrieb hat Ministerin von der Leyen angekündigt, mit dem Kommando Cyber- und Informationsraum bis zum April 2017 eine neue Teilstreitkraft der Bundeswehr aufzubauen.

Die Zahl staatlicher und nichtstaatlicher Akteure im Cyber- und Informationsraum wächst atemberaubend schnell. Sie verfolgen erfolgreich kriminelle und andere schadhafte Absichten. Digitale Wirtschaftsspionage und Internet-Kriminalität gehören zum Alltag. Doch die Grenzen zwischen simpler Kriminalität im Netz und staatlich gesteuerter Cyber-Spionage sind nicht leicht zu erkennen, denn auch Staaten sind Auftraggeber krimineller Akteure.

Besonders perfide für die nationale und internationale Sicherheit sind sogenannte *hybride Bedrohungen* unterhalb der Schwelle eines militärischen Angriffs. Hierzu zählen Cyber-Operationen für Spionage, Informationsmanipulation, mögliche Cyber-Terrorakte bis hin zu groß angelegten Sabotage-Attacken z.B. auf kritische Infrastrukturen. Die russischen Cyber-Attacken im Kontext der Georgien-Krise 2008, der Ukraine-Krise, aber auch beim Hacker-Angriff auf das Netz des Deutschen Bundestages geben erste Eindrücke über das Spektrum der Möglichkeiten. Aber Russland steht hier ebenso wenig allein, wie zuvor die USA im Dunst der Snowden-Enthüllungen. Israel und China, Nordkorea und Taiwan, England und Frankreich und andere mehr sind ebenfalls schlagkräftig aufgestellt.

Während die Bundeswehr bislang ordentlichen Abstand zur Spitze des Fortschritts in Sachen Cyber hält, behandeln die NATO und etliche Partnerländer den Cyber- und Informationsraum schon länger als einen eigenen Operationsraum. Sie prägen konsequent eigene Cyber-Fähigkeiten in zweckbestimmten Organisationsformen aus. Die USA haben schon vor sechs Jahren ihr Cyber-Kommando eingerichtet. Das Atlantische Bündnis begreift Cyber-Fähigkeiten geradezu als *Game Changer*, also als eine Fähigkeit, die etablierte Macht- und Kräfteverhältnisse zwischen Staaten auf den Kopf stellen kann.[1]

In Abstimmung mit der Europäischen Union (EU) entwickelt die NATO zur Abwehr der hybriden Bedrohungen gerade eine neue Strategie. Wir werden beim bevorstehenden NATO-Gipfel in Warschau mehr darüber hören. Die EU hat ihre diesbezüglichen Vorstellungen bereits veröffentlicht. Zu den Schlüsselthemen zählen KRITIS, Energie und Cyber. Man sorgt sich insbesondere vor Cyberangriffen, die zu erheblichen Störungen der digitalen Dienste in der EU führen. Für den digitalen Binnenmarkt gilt es deshalb, die Resilienz der Kommunikations- und Informationssysteme in Europa zu stärken. Inzwischen zeichnet sich auch eine Intensivierung der Zusammenarbeit zwischen EU und NATO ab. Diese konzentriert sich absehbar neben der Verbesserung des Bewusstseins für hybride Bedrohungen auf die Stärkung der Resilienz sowie auf Prävention, Krisenreaktion und Rückkehr zur Normalität.

[1] So Dr. Jamie Shea, NATO Deputy Assistant Secretary General und zuständig für künftige Sicherheitsherausforderungen.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

2. Handlungsfähig werden

Tagtäglich finden Cyberangriffe auf die Bundeswehr statt. Im ersten Halbjahr 2015 wurden bei Einsätzen über 100.000 sicherheitsrelevante Ereignisse bei den Rechnern der Bundeswehr registriert. Zum Teil sind dies gezielte, individuell zugeschnittene Angriffe. Sie werden mit hohem Aufwand geplant, vorbereitet und durchgeführt. Nicht immer werden sie sofort erkannt und abgewehrt. Statistisch dauerte es 2015 selbst bei schwerwiegenden Attacken im Schnitt 205 Tage, bis Cyberangriffe überhaupt erkannt wurden. Die Lösung der daraus resultierenden Probleme dauerte dann durchschnittlich noch einmal 32 Tage. Diese Statistiken geben Anlass zur Sorge.

Noch mehr Sorge muss bereiten, dass nicht nur die Administration und Büroorganisation der Streitkräfte bedroht sind. In alten und neuen Waffensystemen finden sich zahllose Prozessoren, Interfaces, Chips und Computer. Viele dieser Systeme wurden bereits oder werden derzeit vom informationstechnischen Fortschritt überrollt und sind professionellen Cyber-Angriffen hilflos ausgesetzt. Im Umkehrschluss lassen sich hochentwickelte Cyber-Fähigkeiten auch zur Unterstützung der Einsätze der Bundeswehr einsetzen. Bits und Bytes können nicht nur die Kommunikation und Entscheidungsfindung eines Gegners beeinflussen, sondern ggf. den Einsatz kinetischer Kampfkraft klassischen Zuschnitts ermöglichen, verstärken oder auch ersetzen. Wenn ich ein Raketensystem auch ohne Waffenwirkung ausschalten kann, vermeide ich sowohl die Gefährdung eigener Kräfte im Zuge eines erforderlichen Einsatzes wie auch denkbare Kollateralschäden.

Vor diesem Hintergrund ist das Grundrational der Verteidigungsministerin durchaus überzeugend: *„Staat, Wirtschaft und Gesellschaft sind in einer zunehmend vernetzten, digitalisierten Welt für Angriffe im Cyber- und Informationsraum (CIR) verwundbarer geworden. Diese digitale Verwundbarkeit der Gesellschaft haben sich in den letzten Jahren staatliche und nichtstaatliche Akteure – insbesondere im Rahmen der hybriden Kriegsführung – zu Nutze gemacht. ... Die zunehmend komplexeren Angriffe erfordern den Ausbau der staatlichen Handlungsfähigkeit zum Schutze unseres demokratischen Systems und seiner wirtschaftlichen Grundlagen.“*[2]

Bereits zum Oktober 2016 wird im Verteidigungsministerium eine eigenständige Abteilung eingerichtet. Der vormalige ThyssenKrupp-Manager Klaus-Hardy Mühleck übernimmt hier als Chief Information Officer mit Budgethoheit die Verantwortung für die Themen Cyber und IT. Als IT-Architekt der gesamten Bundeswehr soll er zunächst einmal die bislang verzettelte materielle und personelle IT-Infrastruktur unter ein Dach bringen und die Bundeswehr-Informationstechnikgesellschaft als Systemhaus steuern. Ob dann noch Zeit, Kraft und zielführende Vision für die zukunftsweisende Gestaltung der roten Netze des militärischen Nachrichtenwesens, für die recht komplexe Waffensystem IT sowie die leistungsfähige Ausprägung einer neuen Teilstreitkraft mit ganz neuen Fähigkeiten bei rechtlich unübersichtlichen Rahmenbedingungen bleibt?

Bis Anfang April 2017 wird zudem ein Kommando für den Cyber- und Informationsraum (CIR) aufgestellt mit den Aufgaben Cyber, Informationstechnologie, militärisches Nachrichtenwesen, Geoinformationswesen, operative Kommunikation und elektronische Kampfführung. Insgesamt 13.500 Dienstposten werden hierzu von den anderen Teilstreitkräften und Organisationsbereichen in die neue Struktur wechseln – 12.800 davon allein aus der Streitkräftebasis.

Die Ministerin will mit diesen Maßnahmen die IT-Kompetenz in der Bundeswehr bündeln und effektiver nutzen. Zugleich sollen Effizienz und Schlagkraft der Bundeswehr im dynamisch wachsenden Feld der Informa-

[2] BMVg, Abschlussbericht Aufbaustab Cyber- und Informationsraum, April 2016, S. 2, https://www.google.de/search?q=Abschlussbericht+Aufbaustab+Cyber-+und+Informationsraum&biw=1440&bih=708&noj=1&source=lnt&tbs=qdr:m&sa=X&ved=0ahUKEwjG9czT3c7MAhWmK8AKHetBAlwQpwUIFQ

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

tionstechnologie verbessert werden, ebenso der Schutz der Truppe – auch im Einsatz – und gegebenenfalls auch der Schutz der Bevölkerung. Denn die Bundeswehr stellt sich darauf ein, bei Cyber-Angriffen von katastrophalen Ausmaßen an der Seite der Spezialisten der Polizei und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in die Abwehr einzugreifen. Eingebettet in einer ressortübergreifenden Gesamtstrategie der Bundesregierung sollen dann die Cyber-Fähigkeiten der Bundeswehr in enger Abstimmung vor allem mit dem Bundesinnenministerium agieren.

In diesem Kontext stellt sich natürlich die Frage, welche Rahmenbedingungen - faktisch und rechtlich – im internationalen Einsatz sowie beim Schutz von Bevölkerung, Wirtschaft und der verletzlichen Infrastruktur der Heimat auf dem digitalen Gefechtsfeld gelten. Welcher Mix aus defensiven und offensiven Fähigkeiten ist notwendig? Welcher ist erlaubt? Wo sind rechtliche Grenzen gesetzt?

In der Bundeswehr erwartet man, dass solche Fragen im Falle eines Auslandseinsatzes durch ein Bundestagsmandat geklärt werden. Einsatzmöglichkeiten jenseits der Firewall eines fremden Servers kommen für sie – außer im Verteidigungsfall – nur infrage, wenn sie für den jeweiligen Einsatz vom Bundestag mandatiert sind. Bei Angriffen auf die eigenen Computersysteme im Inland darf sich die Bundeswehr zwar schützen, sie überlässt die erforderlichen Gegenmaßnahmen jedoch dem im Inland zuständigen Bundesamt für Sicherheit in der Informationstechnik. Ob das in der Praxis gut geht?

3. Großbaustelle

Man könnte die Ministerin für ihre Weitsicht in Sachen Cyber loben. Allerdings wurden die bedrohlichen Cyber-Herausforderungen in der Bundeswehr doch bemerkenswert spät wahrgenommen. In den vergangenen Jahren hat man in Deutschland den Kopf in den Sand gesteckt, während Freund und Feind einen Wettlauf um die beste Aufstellung im Cyberraum begonnen haben. Wer die Details der deutschen Planung prüft, entdeckt viele gute Absichten und viel weniger gute Taten. Was die Ministerin inhaltlich verspricht, trifft frühestens 2020 ein, vermutlich erst viel später. Das Geld reicht nicht. Das Personal reicht nicht. Die Strukturüberlegungen geben in erster Linie bestehenden Organisationen einen neuen Namen und eine neue Unterstellung – alter Wein in neue Schläuche. Viel spricht für eine weitere Großbaustelle der Bundeswehr mit Namen Cyber.

Bereits jetzt sorgt sich der Wehrbeauftragte des Bundestages vor einem flächendeckenden Burnout in der Bundeswehr. Das Weißbuch 2016 spricht im gegenwärtigen Entwurfsstand selbstkritisch von *„schleichender Überalterung des Materials“* und von Streitkräften, die im Grundbetrieb vermehrt aus der Substanz leben müssten. Dies ist eine freundliche Umschreibung für die Kannibalisierung von Ersatzteilen aus Waffensystemen, Fahrzeugen, Flugzeugen und Schiffen, früher ein klassifizierendes Merkmal von Drittweltstaaten. *„Aufgaben, Kräfte und Mittel befinden sich nicht mehr in einer ausgewogenen Balance“*.[3] Gemeint sind Panzer, die nicht fahren, Flugzeuge, die nicht fliegen, Kompanien ohne Personal.

Die bestehende Planung hat sich bereits ohne die Cyber-Herausforderungen als überholt und ineffizient erwiesen. Nun kommt also das Thema *Cyber* hinzu. Will man hier keine bösen Überraschungen im Einsatz erleben, müsste man die laufenden Rüstungsplanungen, natürlich auch die im Dienst befindlichen Rüstungsgüter, dringend auf ihre Cyberverwundbarkeit prüfen und entsprechend anpassen. Da dies absehbar teuer wird und zudem die bestehende Planung weiter kompliziert, vermied man bislang selbstkritische Analysen und stellt sich dieser Aufgabe erst in der Zukunft.

[3] Werner Sonne. Weißbuch zur Sicherheitspolitik Deutschland ist nur bedingt einsatzfähig. Kölner Stadtanzeiger. 26.05.16, 21:10 Uhr http://www.ksta.de/politik/weissbuch-zur-sicherheitspolitik-deutschland-ist-nur-bedingt-einsatzfaehig-24124356

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Nun ventiliert man derzeit die Überlegung, den Problemen der Gegenwart durch eine beschleunigte Beschaffung von IT nach dem Grundsatz - *IT schneller als Rüstung* - zu enteilen. Es ist sicherlich gut gemeint, dass IT-Beschaffung nicht hinter den Innovationszyklen in der Computerindustrie hinterherhechelt. Und zugleich ist es realitätsfremd. IT ist Bestandteil von Rüstung. Zunehmend prägt sie erst die Wirksamkeit hochkomplexer Waffensysteme. IT muss insbesondere auch der einsatzbezogenen Nutzung von Rüstungsgütern dienen. Wenn der IT-Bereich mit der sogenannten *2-speed-IT* eine zusätzliche Überholspur erhält, wird ein Fokus auf die *weiße IT* erkennbar, die sich um die Bürokommunikation bis hin zum Druck von Broschüren dreht. Das ist die Welt, aus der von außerhalb der Bundeswehr hinzugezogene IT-Experten kommen und in der sich diese zu Hause fühlen. Der Bund stellt aber keine Streitkräfte auf, damit deren Bürokommunikation funktioniert. Wenn die *weiße IT* die den Einsatz prägende *grüne IT* überholt, sind die Streitkräfte in Gefahr. Ein einziger Eurofighter fliegt beispielsweise mit hundert Kilometer Kabel an Bord, damit seine 80 Computer das Fliegen und Feuern beherrschen.

Bereits seit langem liefert Beschaffung nicht, was sie verspricht. Das hat sich auch in der laufenden Legislaturperiode nicht merklich verändert. Hierfür gibt es viele Gründe. Eine Ursache ist seit Jahrzehnten bekannt: die in Streitkräfte und Bundeswehrverwaltung gespaltene Aufgabenwahrnehmung der Bundeswehr. Es war ein gut gemeinter[4], aber dennoch struktureller Webfehler bei der Aufstellung der deutschen Streitkräfte, deren Aufgaben grundgesetzlich durch die Teilung in Grundgesetz (GG) Art. 87a[5] und in GG Art. 87b[6] zu veruneinheitlichen. Die durch GG Art. 87a adressierten Streitkräfte erhalten als sogenannte Bedarfsträger von den durch GG Art. 87b adressierten Mitarbeitern der Bundeswehrverwaltung als sogenannte Bedarfsdecker allzu oft Rüstungsgüter, die wesentlich zu spät ausgeliefert werden und zudem auch nicht den Ansprüchen der Truppe im Einsatz genügen. Der Lufttransporter A400M liefert als aktuelles Beispiel immer neue Belege hierfür. Die Bundeswehrverwaltung hat sich zu einem Bremsschuh und Verursacher von *Bauchlandungen* bei vielen neuen Rüstungsprojekten etabliert. Nun klebt dieses Image an ihr, selbst wo dies sachlich nicht zutrifft. Die neue Cyber-Teilstreitkraft wird ein neuer Leidtragender sein, denn viele ihrer künftigen taktischen und operativen Leistungen werden – auch IT technisch – im vernetzten und hochintegrierten Verbund mit den klassischen Rüstungsgütern zu erbringen sein.

Seit 25 Jahren hat es sich eingebürgert, dass erforderliche Investitionen durch vermiedene Ausgaben erwirtschaftet werden sollen. Zugleich fressen hohe Personalkosten Löcher in Betrieb und Ausrüstungsbedarf. Und natürlich leidet auch die Ausbildung unter dem Geldmangel. Die seit Jahrzehnten mangelhafte finanzielle Unterlegung von Reformen und Innovation hat nicht nur die Substanz der Bundeswehr entkernt, sondern untergräbt zugleich erfolgreichen, rechtzeitigen Wandel. Trotz der jüngsten Aufstockung des Verteidigungsetats herrscht in der Bundeswehr weiterhin Geldmangel. Dringende Beschaffungsvorhaben bleiben bis auf weiteres nicht finanzierbar. Die Bundeswehr hat für ihren Haushalt zu viel Personal. Wie da die Überlegungen nach einer Aufstockung um 14.300 zusätzlichen Soldaten und 4.400 Zivilisten für die nächsten sieben Jahre hineinpassen ist ein Rätsel, zumal auch die Demografie gegen die Pläne der Verteidigungsministerin arbeitet. Der Arbeitsmarkt deckt schon jetzt nicht den Bedarf der Bundeswehr an jungen Menschen.

Das Thema Personal ist auch jenseits der demografischen Herausforderungen ein problematisches Feld. Bislang fehlt der Bundeswehr das hoch qualifizierte Personal, das für den Betrieb und insbesondere für das Erkennen und letztendlich die Abwehr von Cyberangriffen zuständig ist. Insbesondere sind die komplexen Waffensys-

[4] Die Kriegsheimkehrer sollten in der mit 500.000 Obergrenze gedeckelten Bundeswehr eine zivile Beschäftigung finden
[5] In Artikel 87a des Grundgesetzes heißt es: „Der Bund stellt Streitkräfte zur Verteidigung auf."
[6] In Artikel 87b des Grundgesetzes heißt es: „Die Bundeswehrverwaltung wird in bundeseigener Verwaltung mit eigenem Verwaltungsunterbau geführt."

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

teme zu schützen und auf aktuellem Stand zu halten. Das ist aufgrund der hohen Innovationszyklen der Informationstechnologie eine große Herausforderung. Demgegenüber verlassen seit Jahrzehnten hochqualifizierte IT-Experten die Bundeswehr in Scharen, weil deren Expertise insbesondere in den ersten Dienstjahren nach deren Studienabschluss ignoriert wird und bei fachfremden Tätigkeiten zu verkümmern droht. Werdegangsmodelle lassen Förderung in der IT-Expertise bislang nur unzureichend zu. Auf der anderen Seite ignoriert man den Bedarf von IT-Kompetenz in operativen Schlüsselverwendungen und schiebt befähigte Allrounder unter dem Hinweis auf nicht besetzte Dienstposten gerne in berufliche IT-Sackgassen. Damit fehlt dann wiederum die adäquate IT-Kompetenz im Umfeld der militärischen und politischen Spitzenentscheider.

Also Experten von außen anwerben? Auch dieser Ansatz stößt auf Hindernisse. Zum einen kann die Bundeswehr den Wettbewerb mit der IT-Industrie um geeignetes Personal nicht gewinnen, da sie nicht mit den Gehältern der Privatwirtschaft mithalten kann. Zum anderen haben die *Nerds* der zivilen Welt nicht selten eine problematische Vergangenheit. Wer in sicherheitsempfindlichen Bereichen arbeitet muss überprüft werden. Die gesuchten Experten wollen aber nicht überprüft werden. Und die Bundeswehr kann schlecht Experten mit Sicherheitsrisiken in sensitive Verwendungen bringen. Die Bundeswehr sucht deshalb nach neuen Wegen. Unter anderem will man eigene Studiengänge und Fachkarrieren aufbauen, um Menschen zu gewinnen und zu halten. Man will aber auch zugleich mit Industrie und Universitäten in „Cyber-Clustern" kooperieren, um die nötige Expertise zu bekommen. An der Universität der Bundeswehr München wird dafür ein eigener Studiengang für Cybersicherheit eingerichtet. Schnelle Ergebnisse wird man hier nicht erwarten können.

Und die im Entwurf für das Weißbuch 2016 diskutierte Option, EU-Ausländer für die Bundeswehr zu rekrutieren, wird ggf. neue Probleme mit sich bringen. Der Soldat der Bundeswehr schwört nämlich mit seinem Eid, *„... der Bundesrepublik Deutschland treu zu dienen und das Recht und die Freiheit des deutschen Volkes tapfer zu verteidigen ...“*. Was wird der EU-Ausländer schwören oder geloben? Geht die EU-Einstellungswelle mehr in Richtung ausländischer ziviler Mitarbeiter wird es erst richtig interessant, wenn sich diese ebenfalls wie viele zivile deutsche Mitarbeiter heute als hausinterner Primat der Politik missverstehen. Die Steuerung der Bundeswehr durch EU-Ausländer – eine erfrischende Perspektive?

Ein bisher sträflich vernachlässigtes, aber vielversprechendes Feld sind Cyber-Spezialisten aus dem Reservistenbereich – vormalige Soldaten mit fortgesetzter Affinität zu den Streitkräften. Statt sie nach den bisher angelegten Maßstäben für den Reservistendienst in klassischen militärischen Funktionen einzusetzen, können sie als IT-Fachleute in Deutschland in Rechenzentren und Gefechtsständen mitarbeiten und z.B. Auslandseinsätze im Zuge des sogenannten *Reach-Back*[7] unterstützen.

Auch konzeptionell gibt es Wachstumspotenzial. Schon die Absicht der Ministerin, die Cyber-Fähigkeiten der Bundeswehr im Weißbuch 2016 zu definieren – Entwürfe zirkulieren bereits in Medien und bei internationalen Partnern – , belegt die Leichtfüßigkeit des vorgestellten Cyber-Ansatzes. Ein Weißbuch ist von seinem Charakter her eher eine Kommunikationsbroschüre, die der Öffentlichkeit die Sicherheitspolitik der Bundesregierung erklärt. Es ist eben kein konzeptionelles Dokument, das aus einer nationalen Sicherheitsstrategie und einer daraus abgeleiteten militärstrategischen Zielsetzung Konsequenzen für die Planung der Bundeswehr ableitet. Wenn eine Kommunikationsbroschüre konzeptionelle Ansätze ersetzt, weiß der Fachmann, dass inhaltlich kleine Brötchen gebacken werden.

Insbesondere das vorherrschende geistige Maginot-Denken, sich auf die Cyber-Abwehr zu konzentrieren und auf offensive Cybereinsätze weitestgehend zu verzichten, ist im Lande eines Carl von Clausewitz geradezu

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

unfassbar. Bereits vor 200 Jahren lernte man in deutschen Landen zwischen taktischen, operativen und strategisch-politischen Ebenen zu differenzieren. Noch im Kalten Krieg wusste und übte man in Deutschland, wie man einen strategischen Angriff des Warschauer Paktes, durch kleine offensive Gegenangriffe auf taktischer Ebene und Luftangriffe auf die Versorgungs- und Verbindungslinien im Rückraum des angreifenden Gegners ausbremsen konnte. In der Cyber-Domäne ist der Angreifer klar im Vorteil. Sich hier einseitig defensiv auszurichten, bedeutet nichts anderes als sich auf Niederlagen und Großschäden einzustellen.

Will man künftig wirklich immer wieder eigene Informations- und Kommunikationsnetze solange beschädigen lassen, wie es ein Angreifer wünscht? Will man die ausgeprägten IT-Aktivitäten von ISIS und Taliban auch künftig möglichst ungehindert und störungsfrei zur Entfaltung kommen lassen? Wie will man forensisch dem Täter auf die Spur kommen, ohne sein Wirken bis an den Ursprungsort zu verfolgen? Selbstverständlich müssen Mandatierungs- und Rechtsfragen geklärt werden. Dennoch: Wer sich gegen Cyberangriffe effektiv schützen will, muss auch in der Lage sein, einen Angriff auszuführen. Die Fachkenntnis ist ohnehin identisch. Ohne eigene taktische und operative Offensiv-Fähigkeiten macht die Cyber-Truppe keinen Sinn.

Der Weg ins digitale Zeitalter beginnt für die Bundeswehr absehbar mit selbstgemachten Hindernissen. Relevanten Überlegungen stehen strukturelle Mängel, zu kurz gesprungene konzeptionelle Grundlagen, eine Kannibalisierung bestehender Strukturen und unzulängliche Investitionen gegenüber. Drei Empfehlungen sollen diesen Beitrag schließen:

- Eine Vision ohne entsprechende Investition ist eine Halluzination. Die neue Teilstreitkraft Cyber- und Informationsraum braucht eine Mittelausstattung, die es ermöglicht, zentrale Zielsetzungen zu erreichen.
- Die neue Aufstellung im Cyber- und Informationsraum sollte sich mit Priorität daran orientieren, dass die Bundeswehr als eine kombattante Organisation politisch-parlamentarische Zwecke im Einsatz erfolgreich umsetzen soll.
- Alle Teilstreitkräfte – auch das neue Kommando Cyber- und Informationsraum – müssen über einen Mix an offensiven und defensiven Fähigkeiten verfügen. Taktisch und operativ brauchen die Streitkräfte ein den Aufgaben angemessenes Fähigkeitendispositiv, um ihre Einsätze im Sinne der politischen Vorgaben erfolgreich zu gestalten. Dies steht der politisch-strategischen Vorgabe einer strategisch defensiven Ausrichtung der deutschen Streitkräfte im digitalen Zeitalter ebenso wenig entgegen wie zu Zeiten des Kalten Krieges.

***

Anmerkungen: Der Beitrag gibt die persönliche Auffassung des Autors wieder. Die Erstveröffentlichung erfolgte am 27. November 2015 als Gastbeitrag in der *WirtschaftsWoche* unter dem Titel „Bundeswehr gegen IS-Terror. Mit Daten siegen".

[7] Hier werden Einsatzfunktionen, die nicht unbedingt im Einsatzland wahrgenommen werden müssen, aus Deutschland ausgeübt. Damit spart man erheblich an Personal in Auslandseinsätzen.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Über den Autor dieses Beitrags

Oberst a.D. und Diplom-Kaufmann Ralph D. Thiele ist Vorsitzender der Politisch-Militärischen Gesellschaft e.V. (pmg), Berlin und CEO von StratByrd Consulting. In seiner militärischen Laufbahn war Herr Thiele in bedeutenden nationalen und internationalen, sicherheits- und militärpolitischen, planerischen und akademischen Verwendungen eingesetzt, darunter im Planungsstab des Verteidigungsministers, im Private Office des NATO-Oberbefehlshabers, als Chef des Stabes am NATO Defense College, als Kommandeur des Zentrums für Transformation und als Direktor Lehre an der Führungsakademie der Bundeswehr.

Eine Vielzahl von Publikationen, regelmäßige Vorträge in Europa, Amerika und Asien sowie eine intensive Forschungstätigkeit im Kontext deutscher, österreichischer und europäischer Sicherheitsforschung unterstreichen sein ausgeprägtes Kompetenzspektrum.

Ralph D. Thiele ist Mitglied im Beirat Deutscher Arbeitgeber Verband e.V., Wiesbaden und im Defence Science Board, das von Gerald Klug, Verteidigungsminister der Republik Österreich, geleitet wird.

Ralph D. Thiele

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de