Kurzauswertung des Weißbuchs 2016 hinsichtlich der strategischen Planungen im Cyberspace

Stand: 12.07.2016, weitere Aktualisierungen auf cyber-peace.org[1]

Thomas Reinhold, Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, reinhold@ifsh.de, http://cyber-peace.org

Nachfolgende Auswertung bezieht sich auf den von der taz veröffentlichten Weißbuch-Entwurf mit Stand vom 24.Mai 2016[2]. Die finale, im Bundestag abgestimmte Version kann demzufolge noch Änderungen enthalten.

In Ergänzung zur Auswertung des Abschlußberichts zum Aufbau des neuen Bundeswehr-Organisationsbereiches "Cyber- und Informationsraum"[3] wird nachfolgend der Entwurf des Bundeswehr-Weißbuchs 2016 mit Blick auf die strategischen Planungen der Bundeswehr im Cyberspace analysiert. Den umfangreichen Änderungen im Rahmen des Abschlußberichts und insbesondere der anvisierten Aufstockung der offensiven Cyberfähigkeiten der Bundeswehr standen im Bericht wenige strategische Erläuterungen gegenüber. Dies betraf insbesondere die Aspekte in welcher Form die neuen Fähigkeiten eingesetzt werden sollen, auf welche Szenarien die Bundeswehr sich damit vorbereitet, wie die neuen Aufgaben angesichts der engen gesetzlichen Grenzen und der Parlamentsbeteiligung wahrgenommen werden sollen und welche institutionelle Kooperationen für die Erfüllung der Aufgaben im Cyberspace angestrebt werden.

Allgemeine Vorbemerkungen

Insgesamt ist es erfreulich, dass mit dem neuen Weißbuch erstmals strategische Erläuterungen zu den Herausforderungen, Aufgaben und Ziele der Bundeswehr in der Domäne Cyberspace gegeben werden. Beispielsweise existiert die für offensive Cybereinsatz trainierende Einheit Computer Network Operations[4] bereits seit 2006 ohne dass offiziellen Dokumenten zu entnehmen war, welche strategischen Aufgaben mit dem Aufbau dieser Einheit verfolgt wurden. Ebenso ist es grundsätzlich positiv zu bewerten, dass mit dem neuen Weißbuch der Cyberspace und IT allgemein als grundlegender Bestandteil der Bundeswehr bewertet und die Modernisierung, Harmonisierung und Sicherung dieser Ressourcen elementare Aufgabe auch im Bereich der Bundeswehr ist. In diesem Zusammenhang ist Betrachtungsweise von Sicherheit auch im Bereich der Bundeswehr-IT als Prozess, nicht als Zustand (Abschnitt 4.1.d) die richtige Herangehensweise um IT zukunftsfähig zu machen und zu halten.

---

[1] http://cyber-peace.org/2016/07/12/auswertung-weissbuch-2016-und-der-cyberspace
[2] http://taz.de/static/pdf/Weissbuch_Bundeswehr_Stand_240516.pdf
[3] http://cyber-peace.org/2016/04/27/auswertung_aufbaustab_cirk/
[4] http://www.kommando.streitkraeftebasis.de/portal/a/kdoskb/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK94uyk-OyUfL3s4kQwLk1NSi0qzSvWL8h2VAQAQvOGXA!!/

Ebenso hilfreich ist, dass mit dem Weißbuch (Abschnitt 2.2.b) eine konkrete Definition des bereits im Aufbaubericht hinlänglich verwendeten, jedoch eher knapp erklärten[5] Begriffs des "Cyber- und Informationsraumes" als strategische Domäne abgegeben wird. Allerdings enthält die Definition im Weißbuch-Entwurf nicht mehr die Nennung des "Elektromagnetische[n] Spektrum[s]" als Bestandteil des Cyberraums.

Zur Erläuterung der Herausforderungen durch den Cyberspace (Abschnitt 2)

Hinsichtlich der im Weißbuch erläuterten Herausforderungen wird sowohl auf Qualitäts- wie auf Quantitätssprünge der Bedrohungen durch den Cyberspace hingewiesen, auf die Diversität der potentiellen Akteure durch die einfache Verbreitung von Schadsoftware und entsprechenden Software-Werkzeugen und die gestiegenen Möglichkeiten relativ einfach umfangreiche Schäden zu verursachen (Abschnitt 2.2.b). Diese Argumentation ist jedoch nur insofern korrekt, als dass es relativ leicht ist im Cyberspace nach einem beliebigen verwundbaren Ziel zu suchen und dieses zu attackieren - analog zu blinden Vandalismus gegen zufällige Ziele. Sofern es sich um spezifische, strategisch relevante Ziele handelt sind die Möglichkeiten der Schädigungen erheblich eingegrenzt, da diese ein umfangreiches Wissen über das Ziel und möglichen Schwachstellen sowie ggf. ein verborgenes Vorgehen erfordern. Bei den im Weißbuch bezeichneten "Hochwertzielen" kann dabei mit notwendigen Ressourcen auf Seiten der Angreifer gerechnet werden, die in aller Regel nur durch Staaten aufzubringen sind. Exemplarisch wird für Stuxnet von einer mehrjährigen Entwicklungszeit[6], einem hochgradigen Entwicklerteam sowie dem Aufbau einer Testanlage ausgegangen. Das Spektrum der im Cyberspace angreifbaren Ziele grenzt daher die möglichen Akteurs-Gruppen signifikant ein.

Hinsichtlich der Bedrohungen durch den Cyberspace verweist das Weißbuch (Abschnitt 2.2.b) auf zahlreiche Vorfälle von Cyberangriffen "auf Staaten und kritische Infrastrukturen" sowie den Umstand, dass Cyberoperationen bereits heute "Bestandteil kriegerischer Auseinandersetzungen" sind. Ohne den Verweis auf konkrete Beispiele, die jeweils durchgeführten Attacken und eine Bewertung der verursachten Schäden ist eine solche Argumentation jedoch schwer nachvollziehbar. Bisher gibt es noch keinen Fall der - auf Basis öffentlich verfügbarer Informationen - nachweislich eine staatliche Cyberattacke gewesen ist und auch die Liste mutmaßlicher Vorfälle mit konkreten Schäden ist eher kurz. Beispielsweise wurden bei den Attacken in Estland (2007) und im Kaukasus-Krieg (2008) kein nachhaltigen Schäden verursacht sondern Dienste "nur" unterbunden. Tatsächliche IT-Schäden wurden nachweisbar durch Stuxnet (2010) und den BlackEnergy/KillDisk-Attacken auf ukrainische Kraftwerke (2015) verursacht.

Bei der Analyse der Herausforderungen verweist das Weißbuch auf den Umstand, dass im Bereich Cyber innere und äußere Sicherheit so eng zusammenfallen wie "in wenigen Bereichen" (Abschnitt 2.2.b). Aus diesem Umstand wird unter anderen die gemeinsame Verantwortung für den Schutz kritischer Infrastrukturen vor Cyberattacken abgeleitet,

---

[5] siehe Abschnitt 2. des Abschlussbericht Aufbaustab Cyber- und Informationsraum
[6] http://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/stuxnet/

während die Argumentationsgrundlage nicht näher erläutert wird. Dies wäre angesichts der Sensibilität eines Einsatzes der Bundeswehr im Inneren jedoch geboten zumal angesichts im Rahmen der Cybersicherheits-Strategien bereits klare Regelungen bestehen und u.a. mit dem BSI eine zentrale zivile Institution für diese Aufgaben existiert.

Zur Erläuterung der Strategien und Gestaltungsfelder im Cyberspace (Abschnitt 3 / 4)

Das Weißbuch verweist mehrfach auf die Herausforderungen bei völkerrechtlichen Fragen im Cyberspace angesichts neuer Eigenschaften dieser Domäne und den Schwierigkeiten bei der Übertragung etablierter Konzepte. Obgleich bei der Erläuterung der Verantwortung und der Gestaltungsmöglichkeiten im internationalen Umfeld (Abschnitt 4.1.e) sowie explizit im Rahmen der OSZE (Abschnitt 4.2.d und 4.2.f) auf die Förderung der Modernisierung etablierter Konzepte hingewiesen wird, lässt das Weißbuch eine klare Aussage offen, auf Basis welcher Grundlagen der aktuelle Ausbau der Bundeswehr im Bereich der offensiven Cyberfähigkeiten erfolgt und welche Regelungen der Einsatz derartiger Mittel unterliegt. Auf Konzepte wie sie bereits im Rahmen des NATO-Exzellenzzentrums CCDCOE entwickelt wurden, wie das nicht-bindende Tallinn-Manual wird nicht verwiesen. Die Unklarheiten im Rahmen der sicherheitspolitischen Bewertung von potentiellen Cybervorfällen durch die Bundesregierung sowie den Grundlagen und Grenzen eigenen offensiven Agierens im Cyberspace bleiben damit offen. Angesichts des im weiteren Verlauf starken Bekenntnis zur Notwendigkeit des Wirkens in Cyberspace, der eine international noch sehr uneinheitliche Sichtweise auf die Regeln staatlichen Agierens im Cyberspace gegenübersteht[7] wäre eine Klärung oder der Hinweis auf entsprechende nationale Bestrebungen wünschenswert gewesen.

Der unter anderem in den Abschnitten 4.2.e und 4.2.f zum Ausdruck gebrachte Wille zur Modernisierung von Maßnahmen der Vertrauensbildung und der Rüstungskontrolle ist grundsätzlich positiv zu bewerten. Angesichts der bereits kurz angesprochenen Anwendungs-Schwierigkeiten eines Großteils der etablierten Konzepte insbesondere im Bereich praktischer Maßnahmen wie der Verifikation auf den Cyberspace wären genauere Ausführungen wünschenswert, wie explizit diese Herausforderungen begegnet werden soll und in welchem nationalen Umfang die zivile naturwissenschaftliche Forschung der Informatik als wesentliche Gestalter der Domäne Cyberspace eingebunden werden.

Zu den Erläuterungen über die Zukunft der Bundeswehr (Abschnitte 5 bis 8)

Die Ausführungen zu den strategischen Planungen der Bundeswehr sind geprägt von einem klaren Bekenntnis zum Willen des militärischen Wirkens - defensiv und offensiv - im Cyberspace. Das Weißbuch betont an diversen Stellen immer wieder die

[7] Vgl. dazu exemplarisch die Sichtweise auf die Domäne “Cyberspace” im Rahmen eines Vorschlages für einen “UN International code of conduct for information security” durch China , Kasachstan, Kirgisistan , der Russischen Föderation, Tadschikistan und Usbekistan vom 9.01.2015

Notwendigkeit und die Ausrichtung auf ein "Wirken im gesamten Einsatzspektrum" (Abschnitt 5.1) der Bundeswehr und klammert dabei Cyberoperationen nicht aus. "*Die Befähigung zum bundeswehrgemeinsamen Wirken in allen Dimensionen (..) ist der übergeordnete Maßstab*" (Abschnitt 7.) und eine "Wirkungsüberlegenheit muss über alle Intensitätsstufen hinweg erzielt werden können" (Abschnitt 7.3).

Hinsichtlich der Landes- und Bündnis-Verteidigung im Rahmen der NATO und der EU wird der Cyberspace dabei als Einsatzdomäne nicht explizit erwähnt, sondern nur implizit über den Verweis auf die Verteidigung "in allen Dimensionen" (Abschnitt 5.3). Darüber hinaus wird der Kampf gegen Bedrohungen aus dem Cyber- und Informationsraum als Bestandteil des Beitrags zum internationalen Krisenmanagement aufgenommen (Abschnitt 5.3).

Hinsichtlich der Entwicklung und des Ausbaus von Fähigkeiten für das Wirken im Cyberspace verweist Abschnitt 5.3. wörtlich auf die Notwendigkeit dass es im Rahmen der Verteidigung auf Cyberangriffe der Entwicklung und des Trainings defensiver und offensiver "Hochwertfähigkeiten" bedarf. Dafür ist es im Rahmen der bereitgestellten Finanzierung, der Kooperation mit nationalen Institutionen und Unternehmen sowie internationalen Partner notwendig entsprechende Technologien zu erschließen. Dass gerade bei Technologie in Bereich der IT-Sicherheit kaum eine klare Grenze zwischen dem Erwerb defensiver und offensiver Fähigkeiten zu ziehen ist und die Ausrichtung der Bundeswehr auf ausschließliche Verteidigungsaufgaben damit konterkariert, wird nicht erwähnt oder konzeptionell aufgegriffen.

Zur Wahrung der gewachsenen Aufgaben definiert das Weißbuch die Notwendigkeit zur Aufklärung und Lagebilderstellung im gesamten Spektrums des nationalen und internationalen Krisenmanagements, also auch wie in Abschnitt 5.3 definiert zu Bedrohungen im Cyberspace. Damit wird jedoch erneut die Frage aufgeworfen, wie das Agieren in fremden Netzen in Friedenszeiten angesichts der betonten parlamentarischen Kontrollen geregelt werden soll, ob dies überhaupt möglich und wünschenswert ist. Andererseits wäre eine Lagebilderstellung ohne ein Agieren und Sondieren in fremden Netzwerken kaum sinnvoll umsetzbar. Möglicherweise sollen derartige Schwierigkeiten über Kooperation mit dem dafür rechtlich befugten Bundesnachrichtendienst (darauf deutet der aktuelle Stand der neuen Cybersicherheits-Strategie hin[8]). Allerdings ist diskussionswürdig ob und inwieweit das verstärkte Wirken von parlamentarisch schwer zu kontrollierenden Diensten und die Kooperationen mit militärischen Bereichen wünschenswert ist. Trotz erneutem Verweis auf den Bestand der Parlamentsbeteiligung auch bei Cyber-Einsätzen der Bundeswehr (Abschnitt 8) bietet das Weißbuch zu dieser Frage keine Antworten an.

---

8 http://cyber-peace.org/2016/07/12/verbindung-der-neuen-cybersicherheits-strategie-zu-den-militaerischen-cyber-plaenen/

Angesichts der anstehenden Publikation des Weißbuches nach der Veröffentlichung des Aufbauberichts zum neuen Cyberbereich der Bundeswehr schließen die Ausführungen einige Lücken über die strategischen Absichten hinter diesen Restrukturierungs-Maßnahmen und wirken ein wenig wie eine rückwirkende Erläuterung und strategischen Einordnung dieser Vorhaben.