IPG

CYBER-SICHERHEIT 04.08.2016 | Thomas Reinhold

Vom Hindukusch zum Cyberspace

Wie die Bundeswehr unsere Sicherheit im virtuellen Raum verteidigen will.

Für die Bundeswehr wird nun auch formell der virtuelle Raum, der Cyberspace, zu einem relevanten Thema. Davon zeugt zum einen das Mitte Juli offiziell vorgestellte Weißbuch. Darin werden die Fähigkeiten der Bundeswehr sowohl zur Verteidigung im Cyberspace als auch für die Offensive gegenüber dem letzten Weißbuch von 2006 erstmals detailliert diskutiert. Zum anderen wurde wenige Wochen vor der Vorstellung des Weißbuchs der Aufbau eines eigenen Organisationsbereichs „<link kommentar artikel cyber-gedoens-1404>Cyber- und Informationsraum“ beschlossen, der den bestehenden Teilstreitkräften Heer, Marine und Luftwaffe sowie dem Sanitätsdienst gleichgestellt sein soll. Damit will das Bundesverteidigungsministerium (BMVg) auf die Bedrohungen durch die vielfältigen gesellschaftlichen Abhängigkeiten von der Informationstechnologie (IT) und die zunehmende Militarisierung des virtuellen Raumes reagieren.

Eine Studie des „United Nations Institute for Disarmament Research“ (UNIDIR) aus dem Jahr 2013 kommt etwa zu dem Schluss, dass mindestens 47 Staaten den Cyberspace als militärische Domäne auffassen und zehn dieser Staaten am Aufbau offensiver Cyber-Fähigkeiten arbeiten. Diese Zahl dürfte seitdem gestiegen sein, und mit der Ankündigung der USA, den Kampf gegen den „Islamischen Staat“ (IS) auch aktiv im Cyberspace zu führen, gibt es die weltweit ersten offiziellen offensiven militärischen Cyber-Aktivitäten.

Auch wenn bei Cyber-Angriffen auf kritische Infrastruktur oder staatliche Einrichtungen, wie im vergangenen Jahr die Hacking-Kampagne gegen das interne Kommunikationssystem des Bundestages, staatliche Angreifer oft nur vermutet werden können, unterstreichen die zunehmenden Cyber-Angriffe die Notwendigkeit eines besseren nationalen Schutzes in diesem Bereich. Das BMVg und die Bundeswehr versuchen, diesen Herausforderungen durch die bessere Steuerung und eine rasche Umsetzung von IT-Projekten seitens des Ministeriums sowie eine Zusammenfassung bestehender Kapazitäten in der Truppe zu begegnen.

Mit Blick auf die rasante und dynamische Entwicklung von Hardware und Software und die heterogene IT-Landschaft der Bundeswehr bei Kommunikations- und Verwaltungssystemen sowie Einsatz- und Waffensystemen ist es grundsätzlich begrüßenswert, dass die Gewährleistung von IT-Sicherheit zu einer Kernaufgabe wird. Die in den Umstrukturierungsmaßnahmen anvisierte zentrale Steuerung von IT-Angelegenheiten kann bei einer konsequenten Umsetzung sicher helfen, ein „internes Lagebild“ der IT-Sicherheit aufzubauen, diese zu verbessern und regelmäßig auf den Prüfstand zu stellen.

Hinsichtlich Regeln, Grenzen und Kontrollmöglichkeiten des militärischen Engagements im Cyberspace gestaltet sich die Anwendung etablierter Maßnahmen schwierig.

Hinsichtlich Regeln, Grenzen und Kontrollmöglichkeiten des militärischen Engagements im Cyberspace und einer einheitlichen internationalen Sichtweise auf diese Fragen gestaltet sich die Anwendung etablierter Maßnahmen jedoch schwierig. Trotz dieser Unklarheiten baut die Bundeswehr seit 2006 mit der Einheit „Computer Network Operations“ eigene Cyber-Kräfte auf, die sich auf das offensive Wirken in fremden Netze vorbereiten. Offizielle Aussagen über das strategische Konzept dieser Einheit, ihre Zusammenarbeit mit anderen nationalen oder internationalen Behörden sowie den Umgang des BMVg mit der völkerrechtlich problematischen Situation gibt es jedoch nach wie vor nicht. Es bleibt zu hoffen, dass die im Rahmen des Weißbuchs und der Umstrukturierungen angestoßenen Prozesse und das klare Bekenntnis zur Parlamentsbeteiligung bei Entscheidungen über Cyber-Einsätze zur Klärung beitragen und die Möglichkeiten der parlamentarischen Kontrolle verbessern.

Bisher deuten die Planung und die im neuen Weißbuch beschriebenen Herausforderungen der Bundeswehr vor allem auf eine Ausweitung der Angriffsfähigkeiten, Planungen zum Einsatz der Bundeswehr für die Cyber-Abwehr im Inneren sowie eine engere Verzahnung mit dem militärischen Nachrichtenwesen und den Geheimdiensten hin. Ähnlich wie bei konventionellen Waffen benötigen mögliche Operationen im Cyberspace eine exakte Lagebildaufklärung und strategische Planungen. Im Cyberspace würde dies jedoch ein Navigieren in fremden Netzen sowie die Identifizierung potenzieller Zielsysteme und deren

Schwachstellen voraussetzen. Dies sind extraterritoriale Aufgaben, die der Bundeswehr aus guten Gründen in Friedenszeiten untersagt sind.

Es steht zu befürchten, dass diese Aufgaben zukünftig dem Bundesnachrichtendienst zufallen – dessen Mitarbeiter bereits zu zehn Prozent aus Reihen der Bundeswehr stammen – und sich damit weitestgehend der parlamentarischen Kontrolle entziehen. Erste Berichte über eine neue Cyber-Sicherheitsstrategie der Bundesregierung weisen darauf hin, dass es bereits Planungen gibt, für diese Zwecke eine eigene „Beschaffungsdienststelle“ aufzubauen, um offiziell Schadsoftware und „Cyber-Waffen“ zu entwickeln und bereitzustellen.

Ähnlich wie bei konventionellen Waffen benötigen mögliche Operationen im Cyberspace eine exakte Lagebildaufklärung und strategische Planungen.

Das größere Augenmerk auf Fähigkeiten der Bundeswehr im Cyberspace könnte auch den Beschlüssen der NATO-Staaten beim letzten Gipfeltreffen in Warschau Anfang Juli 2016 geschuldet sein. Dort wurde die Abwehr von Cyber-Angriffen als weitere wesentliche Aufgabe der kollektiven Verteidigung aufgenommen und der Aufbau nationaler Kapazitäten beschlossen. Doch auch die Erweiterung der Verteidigungsfähigkeiten sollte angesichts der im Cyberspace schwierigen Abgrenzung zwischen Verteidigung und Angriff – die Hilfsmittel sind in aller Regel dieselben – mit Blick auf die außenpolitische Wirkung kritisch hinterfragt werden. Zudem sollte sie durch eine klare außenpolitische Linie der Vertrauensbildung begleitet sein. Laut Weißbuch sollen derlei Anstrengungen vor allem im Rahmen der Organisation für Sicherheit und Zusammenarbeit in Europa weiter vorangetrieben werden. Allerdings haben diese Bekenntnisse angesichts der wiederholten Betonung, wie wichtig die Ausrichtung auf ein „Wirken im gesamten Einsatzspektrum“ sei, nicht das angemessene Gewicht. Dies gilt insbesondere beim Ausbau der Forschung für das offensive Wirken im Cyberspace. Dieser Forschung muss unbedingt Forschung für die Friedenssicherung, wie Abrüstung und Rüstungskontrolle, gegenübergestellt werden.

Angesichts der zunehmenden Vereinnahmung des Cyberspace durch Militär und Nachrichtendienste, denen nur zum Teil an der friedlichen Weiterentwicklung des Cyberspace und der besseren Absicherung von IT gelegen ist, muss die Informatik als primäre gestaltende Kraft dieser Technologie zukünftig noch stärker in die Pflicht genommen werden. Das reflexhafte <link kommentar artikel cyber-gedoens-1404>Belächeln der „Cyber“-Wortwahl deutscher Entscheidungsträger ist hier leider wenig hilfreich. Stattdessen sollten Fragen der moralischen Verantwortung für das eigene Tun und kontinuierlichen Überprüfung der erschaffenen Technologie in den Vordergrund gestellt und in die gesamte IT-Community getragen werden. Denn wie am Projekt „Digitale Kräfte“ der Bundeswehr deutlich wird, ist die Nachfrage nach IT-Fachkräften im militärischen und im Rüstungsbereich hoch und wird weiter steigen. Die Freiheit wird, wie es in der Kampagne „Digitale Kräfte“ der Bundeswehr heißt, schließlich auch „im Cyberspace verteidigt“.

Thomas Reinhold
Hamburg

Thomas Reinhold ist IT-Freelancer und Wissenschaftler am Institut für Friedensforschung und Sicherheitspolitik der Universität Hamburg. Schwerpunkte seiner Forschung sind insbesondere die Themen Cybersecurity, Bedrohungen im Cyberspace und Cyberwar.

4 LESERBRIEFE

Benedikt Rübenkopf schrieb am 09.08.2016

»Deutschlands Freiheit wird auch im Cyberraum

verteidigt«: Abgesehen davon, dass dieser von »Deutschlands Freiheit wird auch am Hindukusch verteidigt« abgewandelte Satz eben deshalb negative Assoziationen hervorruft, da der Afghanistan-Einsatz wirklich nicht uneingeschränkt als erfolgreich betrachtet werden kann, liegt der entscheidende Fehler in der Grundannahme der Kampagne, dass der Cyberraum ein Raum sei. Selbst wenn sich das Eine oder Andere mit Parallelen aus dem »real life« erklären ist, so kann das gewohnte dreidimensionale Denken im »Cyberkampf« verheerende Folgen haben.

Thomas Reinhold schrieb am 14.08.2016

Hallo Herr Rübenkopf

Ihrer Einschätzung der Probleme einer Übertragung konventioneller Konzepte stimme ich vollends zu - das Zitat war daher auch bewusst in Gänsefüßchen gesetzt. Nichts desto trotz setzen die Strategen im BMVg und auch in internationalen Debatten aber genau an diesem Punkt an, eben weil etablierte Konzepte stark auf dem Vorhandensein eines "Raumes" aufbauen ... und scheitern daher bislang ein tragfähigen Lösungen. Die Frage ist

daher, wie der Cyberspace als Domäne mit unterschiedlichsten Akteuren in Begriffen und Konzepten abgebildet werden kann, die unter anderem auch Aspekte wie Verantwortlichkeiten und Souveränität erfassen. Da fehlt es bislang an Ansätzen und m.M.n. auch an Forschung.

Kurt Theobald schrieb am 29.08.2016

Interessant ist die Frage nach dem Konzept des Denkens bezueglich des Internets.
Einmal nach der Frage der Souveraenitaet der Staaten: Haben sie die nicht schon an beliebige Firmen wie google, microsoft oder amazon verloren? Steuerhoheit, Produktqualitaet etc.!
Man koennte natuerlich auch das Internet als ein "eine Welt" Konzept auffassen und daraus die Konsequenz ziehen, dass man eine internationale Regulierungsbehoerde schafft, die Zugang und Nutzung regelt und auch das Recht auf Ausschluss ausueben kann, sowohl fuer einzelne Personen, als auch fuer Firmen oder auch Staaten.
Das haette dann zur Folge, dass Staaten die irgendeine Art von Angriff fuehren ausgeschlossen werden.

Es ist vielleicht sinnvoller in dieser Richtung zu denken, als in form von Verteidigung und Angriff.

Thomas Reinhold schrieb am 30.08.2016

Hallo Herr Theobald

"Es ist vielleicht sinnvoller in dieser Richtung zu denken, als in form von Verteidigung und Angriff."

Da stimme ich Ihnen zu, zumal ohnehin bereits sehr viele Staaten, deren Gesellschaften und Wirtschaft am Wohl und Wehe des "einen Raumes Internet" hängen und die leider immer noch üblichen Versuchen nationaler Eingrenzungen eher auf verlorenem Posten stehen. Entsprechende erste Bestrebungen der UN die Regulierung des Internets in globale Hände zu legen gibt es bereits, allerdings sperren sich aktuell bisher ICANN und IANA sehr dagegen.
