Cyber-Reserve der Bundeswehr

Nachschub für den Kampf um den Informationsraum

von Jürgen Wagner

Die Auseinandersetzungen um die Kontrolle des Cyber- und Informationsraums nehmen an Bedeutung und Schärfe zu und spielen auch und gerade in den Planungen der Bundeswehr eine immer größere Rolle. Gleichzeitig ist es dieser Bereich, in dem die Bundeswehr mit die größten Nachwuchsschwierigkeiten plagen, die wenigstens in Teilen über eine „Cyber-Reserve“ behoben werden sollen.

Bundeswehr auf Cyberkurs

Ohne Begriffe wie „Digitalisierung“, „Künstliche Intelligenz“ oder auch den „Cyber- und Informationsraum“ geht seit einiger Zeit in der Bundeswehr überhaupt nichts mehr. Das Weißbuch der Bundeswehr stufte Cyberangriffe bereits 2016 als eine ernste Bedrohung ein:

„Die Auswirkungen von Cyberangriffen können denen bewaffneter Auseinandersetzungen entsprechen und in die nichtvirtuelle Welt eskalieren.“

Mit der Einrichtung des in Bonn beheimateten „Kommando Cyber- und Informationsraum“ (KdoCIR) im Jahr darauf wurde der virtuelle Raum den Dimensionen Land, Luft, Weltraum und See gleichgestellt und erhielt seinen eigenen Organisationsbereich. Im kommenden Jahr soll das KdoCIR den vollen Personalumfang erreichen, der auf der Homepage des Verteidigungsministeriums folgendermaßen beziffert wird: „Bis 2021 soll der gesamte Organisationsbereich Cyber- und Informationsraum seine volle Einsatzbereitschaft erreichen. Dazu wird der Organisationsbereich auf etwa 14.500 Dienstposten aufwachsen.“

Gleichzeitig fällt es der ohnehin unter chronischer Personalnot leidenden Bundeswehr besonders schwer, an die zunehmend gefragten IT-ExpertInnen zu gelangen, was wohl ein zentraler Grund für die Aufstellung der Cyber-Reserve sein dürfte.

Cyber-Reserve

Ganz taufrisch ist die Idee einer Cyber-Reserve nicht, erste Überlegungen in diese Richtung scheinen bereits vor fast zehn Jahren angestellt worden zu sein – so zumindest die Bundesregierung in einer Antwort auf eine Kleine Anfrage am 15. Oktober 2020: „Erste Überlegungen eine Cyber-Reserve zu etablieren wurden in der Cyber-Sicherheitsstrategie für Deutschland 2011 formuliert.“

Mit dem (nicht-öffentlichen) „Konzept für die personelle Unterstützung der Cyber-Community der Bundeswehr“ wurde die „Cyber-Reserve“ im März 2017, wohl nicht von ungefähr kurz bevor auch das KdoCIR an den Start ging, ins Leben gerufen – die Bundesregierung schreibt: „Mit der Aufstellung des Kommando Cyber- und Informationsraum (KdoCIR) und der Unterstellung von bereits existierenden Dienststellen, wie dem Kommando Strategische Aufklärung oder dem Kommando Informationstechnik der Bundeswehr, wurden existente Reservestrukturen für den Bereich Cyber/IT-Dienst in die Cyber-Reserve integriert.“

Das Aufgabenprofil der Cyber-Reserve besteht vor allem darin, an zusätzliche Exemplare der raren, aber gefragten IT-Experten zu gelangen. In der ausführlichen Variante wird dies auf der Homepage des Reservistenverbandes mit folgenden Worten beschrieben:

„Absicht ist es, gezielt eine hoch qualifizierte und schlagkräftige Cyber-Reserve zur bedarfsorientierten Unterstützung des aktiven Cyber-Personals der Bundeswehr sukzessive aufzubauen und für das Aufgabenfeld Cyber- und Informationsraum geeignete und interessierte Reservistinnen und Reservisten zu gewinnen. Nur so kann benötigte Fachexpertise in einem hoch innovativen und sich ständig weiterentwickelnden Bereich aktuell gehalten werden und die Effektivität der Bundeswehr im Cyber- und Informationsraum verbessert werden. Zudem soll die Cyber-Reserve gemeinsame Übungen von Cyber-Spezialisten

aus Behörden, Gesellschaft und Wirtschaft zur Cyber-Verteidigung ermöglichen und einen Wissenstransfer fördern."

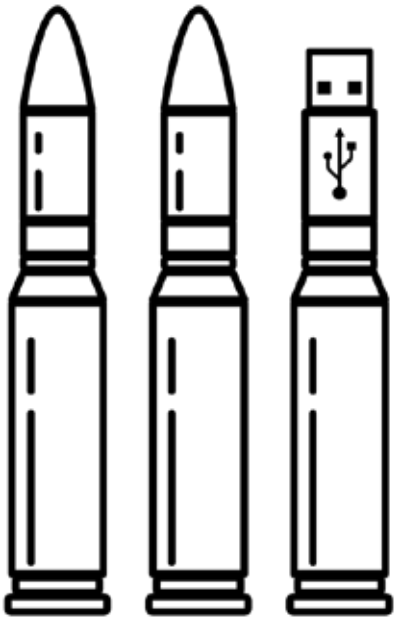
Laut der im Oktober 2020 erschienenen „Weisung für Reservistenarbeit in den Jahren 2020 bis 2022" wird diesem Reserve-Bereich hohe Bedeutung zugemessen: „Die Implementierung und Einsatzbereitschaft der Cyber-Reserve ist schon jetzt mit Blick auf das neue Konfliktbild (hybride Einflussnahme und Kriegsführung) im Rahmen der gesamtstaatlichen Sicherheitsvorsorge für den Grundbetrieb zu priorisieren."

Allerdings waren die diesbezüglichen Anstrengungen bislang nur bedingt von Erfolg gekrönt. Die Bundesregierung gibt in ihrer Antwort vom Oktober 2020 an, aktuell seien lediglich 283 von 523 Dienstposten besetzt (Stand: 18. September 2020). Die Bundeswehr hinkt also jetzt schon ihren Zielen hinterher – und das, obwohl sich die Zielgröße laut derselben Quelle noch einmal fast verdoppeln soll: „Als Folge der in der Strategie der Reserve festgelegten Grundbeorderung aller ausscheidenden Soldatinnen und Soldaten soll der Umfang der DP für die Cyber-Reserve im OrgBer KdoCIR auf 931 anwachsen." Es ist also davon auszugehen, dass die Bemühungen, IT-ReservistInnen zu gewinnen, noch einmal deutlich intensiviert werden dürften.

In der Cyber-Offensive

Das BMVg betont auf seiner Website, dass alle Cyberaktivitäten der Bundeswehr an die Vorgaben des Grundgesetzes gebunden seien – insinuiert wird damit, Offensivaktionen wären enge Grenzen gesetzt: „Der Einsatz der Bundeswehr im Cyberraum unterliegt denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte. Rechtsgrundlage für die Einsätze und Verwendungen der Bundeswehr sind die einschlägigen Regelungen des Grundgesetzes. Die rechtliche Zulässigkeit von konkreten Operationen im Cyberraum ist – wie bei anderen militärischen Maßnahmen auch – in jedem Einzelfall zu prüfen."

Dennoch wurde bereits im April 2015, damals noch von Verteidigungsministerin Ursula von der Leyen, die als Verschlusssache eingestufte „Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg" erlassen. In der von netzpolitik.org veröffentlichten Leitlinie wird Cyberattacken ganz ungeniert das Wort geredet: „Der Cyber-Raum stellt mit seinen Chancen und Risiken eine Herausforderung dar, der sich die Bundeswehr intensiver stellen muss, um ihre Zukunftsfähigkeit zu erhalten. […] Neben den klassischen Räumen Land, Luft, See und Weltraum ist auch der Cyber-Raum somit ein Operationsraum. […] Offensive Cyber-Fähigkeiten der Bundeswehr sind als



Quelle: Skye Selbiger/thenounproject.

unterstützendes, komplementäres oder substituierendes Wirkmittel anzusehen. Sie haben zum Einen das Potenzial, in der Regel nicht-letal und mit hoher Präzision auf gegnerische Ziele zu wirken, zum Anderen kann diese Wirkung im Gegensatz zu kinetischen Wirkmitteln unter Umständen sogar reversibel sein. Offensive Cyber-Fähigkeiten der Bundeswehr haben grundsätzlich das Potenzial, das Wirkspektrum der Bundeswehr in multinationalen Einsätzen signifikant zu erweitern."

Nur ein Jahr später hieß es auch im Weißbuch der Bundeswehr, nun auch ohne viel Aufhebens für Interessierte nachlesbar: „Die Verteidigung gegen derartige [Cyber-]Angriffe bedarf auch entsprechender defensiver und offensiver Hochwertfähigkeiten, die es kontinuierlich zu beüben und weiterzuentwickeln gilt."

Es ist diese Offensivstrategie, in die die Cyber-Reserve als integraler Bestandteil eingebettet ist und die inzwischen auch von ExpertInnen offen benannt wird. So wird beispielsweise Matthias Schulze von der ansonsten in der Regel selten sonderlich kritischen „Stiftung Wissenschaft und Politik" im Deutschlandfunk mit den Worten zitiert: „Also mindestens seit 2016 haben wir eine offensivere Gangart in der deutschen IT-Sicherheitspolitik. Davor war das Ganze in erster Linie zivil und defensiv orientiert. Mit 2016 haben wir das neue Weißbuch, was einen offensiveren Touch hat, wir haben den Aufbau des Kommandos CIR, wir haben die Schaffung der ZITIS. Und das sind alles Pflöcke, die da eingeschlagen werden, um in eine offensivere Richtung zu gehen."