Stefan Heumann

Die Bundeswehr im Cyberraum: quo vadis?

Die Digitalisierung verändert nicht nur die Arbeits- und Lebenswelt, sie wirkt sich zunehmend auf militärische Strategien und die Formen der Kriegsführung aus – auch bei der Bundeswehr. Digitale Waffen erlauben es, mit vergleichsweise wenig Aufwand große Schäden hervorzurufen, insbesondere in der zivilen Infrastruktur eines gegnerischen Landes. Wie weit sich die Konventionen und politischen wie rechtlichen Regulierungsversuche des Militärischen auf diese neue Form der Auseinandersetzung übertragen lassen, und welche neuen Probleme und Streitfragen dabei auftreten, erläutert der folgende Beitrag von Stefan Heumann.

Wie militärische Konflikte im Zeitalter des Internets aussehen, beschäftigt schon seit vielen Jahren Verteidigungsexperten auf der ganzen Welt. Während militärische Großmächte wie die Vereinigten Staaten, Russland und China seit Jahren ihre Fähigkeiten für die Kriegsführung im Cyberraum ausbauen, gab es in Deutschland vergleichsweise wenig öffentliche Aufmerksamkeit für die Rolle der Bundeswehr im Cyberraum. Ein wichtiger Meilenstein für das Verteidigungsministerium war der im April 2016 fertiggestellte „*Abschlussbericht Aufbaustab Cyber- und Informationsraum*." Auch das jüngste Weißbuch (2016) des Bundesministeriums der Verteidigung (BMVg) zur Sicherheitspolitik und zur Zukunft der Bundeswehr erkennt in der Abwehr beziehungsweise Bekämpfung von Bedrohungen aus dem Cyberraum ein zentrales Handlungsfeld.[1] Die Einrichtung des neuen *Kommandos Cyber- und Informationsraum* der Bundeswehr zum 1. April 2017 mit dem Ziel einer zukünftigen Personalstärke von 13.500 Cyber-Soldatinnen zeigt, wie ernst man dieses Handlungsfeld mittlerweile nimmt.[2]

Mit der Einrichtung des Cyber-Kommandos ist die Bundeswehr nun auch in einer breiteren, öffentlichen Debatte um offensive Cyber-Operationen angekommen. Im Zentrum steht vor allem die Frage, was Einsätze im Cyberraum eigentlich für die Bundeswehr bedeuten. Um diese Frage beantworten zu können, ist es wichtig, klar herauszuarbeiten, was Cyber-Operationen eigentlich sind und wie sie sich von anderen Waffengattungen unterscheiden. Der Einsatz militärischer Mittel ist an gesetzliche und verfassungsrechtliche Vorgaben sowie das Völkerrecht gebunden. Wenn es sich bei Cyber-Operationen wirklich um eine neue Art der Kriegsführung handelt, brauchen wir dringend eine breite Diskussion, welche Regeln für das Militär hier gelten sollen.

Ursprünge der digitalen Revolution im Militär liegen im Kalten Krieg

Die Revolution der Informations- und Telekommunikationstechnologie sowie die globale Vernetzung von IT-Systemen über das Internet hat selbstverständlich auch das Militär stark verändert. Das Militär war allerdings nicht einfach ein Rezipient des technologischen Wandels, sondern hat die Entwicklung von Computern und ihre Vernetzung selbst vorangetrieben. Das hieraus einmal ein eigenes, neues Gebiet für militärische Operationen entsteht, ist eine Entwicklung, die erst nach dem Ende des Kalten Krieges richtig Fahrt aufgenommen hat. Um zu verstehen, was Cyber-Operationen für das Militär heute bedeuten, ist ein kurzer Rückblick auf die historischen Wurzeln hilfreich.

Wie Thomas Rid (2016) eindrücklich nachgezeichnet hat, liegen die Ursprünge von dem, was wir heute als Cyberraum verstehen, in militärischen Forschungen zur automatisierten Zielerfassung in der Luftabwehr während des Zweiten Weltkriegs. Ausgehend von diesem konkreten Problem wurde das Potenzial von Computern in der Kriegsführung schnell erkannt. Die Steigerung der Rechenleistung von Computern ermöglichte die Verarbeitung großer Informationsmengen und die Durchführung komplexer Rechenleistungen innerhalb kürzester Zeit. Computerbasierte Berechnungen bildeten die Grundlage für Raketenangriffs- und Abwehrstrategien, die nach Ende des Zweiten Weltkriegs den Rüstungswettlauf zwischen den Vereinigten Staaten und der Sowjetunion prägten.

Die wachsende Bedeutung von Computern für Forschung und Entwicklung im Rüstungssektor war der entscheidende Treiber für die Entwicklung des Vorläufers des heutigen Internets, dem sogenannten ARPANET (Kaplan 2016: 7-11). Die *Advanced Research Projects Agency* (ARPA) ist eine Behörde des US-Verteidigungsministeriums. Sie hat den Auftrag, neue rüstungsrelevante Technologien für das Pentagon zu identifizieren und deren Entwicklung zu fördern. Die ARPA trieb Anfang der 1980er Jahre die Entwicklung des ARPANET voran. Über ARPANET wurden die Computer von Forschungsinstituten, Rüstungsunternehmen und Universitäten miteinander verbunden, um schneller und einfacher Forschungsergebnisse und -daten miteinander austauschen zu können. Darüber hinaus sollte das ARPANET mit Hilfe von schneller, dezentraler Kommunikation die Zweitschlagfähigkeiten der Vereinigten Staaten in einem möglichen Nuklearkrieg erhöhen. Die Computer bauten hierzu Verbindungen über Telefonleitungen auf. Die dafür entwickelten technischen Protokolle und Standards bilden bis heute die Grundlage des Internets. Aus dem ARPANET ging ein Forschungsnetzwerk hervor, welches sich vor allem dank nutzerfreundlicher Webtechnologien in den 1990er Jahren zu einem globalen Kommunikationsnetzwerk entwickelte. Militärs sehen in diesem Kommunikationsnetzwerk, dem Internet, und dem mit ihm verbundenen informationstechnischen Systemen ein neues Operationsgebiet, den sogenannten Cyberraum.

Was bedeuten Operationen im Cyberraum für die Bundeswehr?

Laut Weißbuch des BMVg besteht der Cyberraum aus allen „*weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme(n). Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann*“ (Bundesministerium der Verteidigung 2016, 36). Das aus dem ARPANET hervorgegangene Internet ist auf effizienten Datenaustausch in einem dezentralen Netzwerk ausgelegt. Jeder Punkt im Netz soll sich möglichst einfach und ohne zentrale Koordination mit jedem beliebigen anderen Punkt im Netz verbinden können. Die darauf ausgerichteten technischen Protokolle bieten jedoch wenig Kontrolle über das Netzwerk selbst und sind nicht auf IT-Sicherheit ausgelegt.

Dezentralität und effizienter Datenaustausch machen den Erfolg des Internets aus. Überall auf der Welt können sich Computer mit dem Netz verbinden, solange sie bestimmte technische Standards einhalten. In den vergangenen Jahrzehnten ist das Internet rasant gewachsen. Heute befinden wir uns in einer Welt, in der vernetzte Informations- und Telekommunikationstechnologien nicht nur Wirtschaft und Gesellschaft, sondern auch das Militär in allen Bereichen – von der Logistik über Informations- und Befehlsstrukturen bis zu den Waffensystemen – durchdringen. Computer und Internet sind aus dem militärischen genauso wie aus dem zivilen Alltag schon lange nicht mehr wegzudenken.

Was heißt das für militärische Operationen im Cyberraum? Grundsätzlich gilt für militärische IT-Systeme die gleiche Logik wie für zivile IT-Systeme. Die Abhängigkeit von IT-Systemen bringt auch für Militärs neue Verwundbarkeiten mit sich. Ohne funktionierende IT hebt kein moderner Kampfflieger mehr ab. Cyber-Angreifer können daher heutzutage nicht nur Kraftwerke oder Krankenhäuser lahm legen. Sie können auch Waffensysteme außer Gefecht setzen, wenn es ihnen gelingt, in die entsprechenden IT-Steuerungssysteme einzudringen. Und wie bei Cyber-Angriffen auf zivile IT-Systeme werden hierbei Sicherheitslücken in der eingesetzten Soft- und Hardware als Einfallstore ausgenutzt. Sogenannte „Cyberwaffen“ sind daher schwerlich mit herkömmlichen Waffensystemen zu vergleichen. Im Kern handelt es sich um Software, die es einem Angreifer ermöglicht (oft unter Ausnutzung einer Sicherheitslücke), in ein fremdes IT-System einzudringen, um es zu überwachen, zu manipulieren oder außer Betrieb zu nehmen.

Aber Militärs können Cyber-Operationen nicht nur nutzen, um Flugabwehrsysteme auszuschalten oder streng geheime Angriffspläne zu stehlen. IT-Experten können im Auftrag des Militärs auch Schadsoftware entwickeln, um die Stromversorgung oder den Schienenverkehr zu stören. Computer steuern nicht nur Waffensysteme, sondern auch unsere gesamte zivile Infrastruktur. Cyber-Operationen bieten hier ganz neue Möglichkeiten, die Wirtschaft eines Landes zum Erliegen zu bringen, ohne eine einzige Bombe abzuwerfen. Nach Angaben des Whistleblowers Edward Snowden war es ein misslungener Versuch der *National Security Administration* (NSA), Zugriff auf den wichtigsten Telekommunikationsdienstleister Syriens zu erlangen, der das gesamte Land vom Internet trennte.[3] Durch einen Cyber-Angriff lassen sich Fehlfunktionen in einem Kraftwerk auslösen, die zu dessen Zerstörung führen können; können Züge zum Entgleisen gebracht, schwerwiegende physische Schäden ausgelöst und Menschen ge-

tötet werden. Aufgrund dieser Implikationen müssen wir uns Gedanken darüber machen, welche Regeln für den Cyberraum gelten sollen. Und vor allem brauchen wir klare Grenzen für militärische Operationen im Cyberraum.

Lehren des Kalten Kriegs gelten nicht für den Cyberraum

Die Herausforderung, die destruktiven technischen Möglichkeiten nicht auszuschöpfen und militärischen Operationen im Cyberraum zu begrenzen, wird oft mit der Verhinderung des Einsatzes von Nuklearwaffen im Kalten Krieg verglichen. Die Herausforderung mag ähnlich groß und bedeutsam für unsere Zivilisation sein. Allerdings helfen uns zentrale Konzepte zur Vermeidung von Atomkonflikten – etwa die gegenseitige Abschreckung oder die Rüstungskontrolle – im Cyberraum nur bedingt weiter. Um hier zu Lösungen zu kommen, müssen wir uns von der Logik des Kalten Krieges verabschieden und uns auf die Logik von Cyber-Konflikten einlassen.

Ein zentraler Unterschied zu Atomwaffen sind die vergleichsweise geringen Entwicklungskosten für sogenannte Cyberwaffen. Einfache Schadsoftware ist frei im Internet verfügbar. Wer selbst nicht in der Lage ist, Sicherheitslücken in gängigen Betriebssystemen zu identifizieren, kann diese auch für im Vergleich zu konventionellen Waffen wenig Geld einkaufen. Letztendlich arbeiten Cyber-Kriminelle, die in Firmennetzwerke eindringen, um sich zum Beispiel Kreditkarteninformationen von Kunden zu besorgen, mit den gleichen Mitteln wie Cyber-Söldner, die sich im Auftrag des Militärs Zugang zu IT-Systemen feindlicher Staaten verschaffen. Hierin liegt noch ein weiterer großer Unterschied zum Kalten Krieg: Der Einsatz von Atomwaffen ist sofort nachweisbar und lässt sich in der Regel leicht einzelnen Akteuren zuordnen. Dies ist bei Cyber-Operationen völlig anders.

Mitarbeitenden des iranischen Nuklearprogramms war über Monate hinweg gar nicht bewusst, dass der Ausfall der Zentrifugen zur Urananreicherung in Natanz im Jahr 2010 auf den eigens hierfür entwickelten Computervirus Stuxnet zurückzuführen war. Obwohl es zahlreiche Indizien und Berichte gibt, dass Stuxnet von den Vereinigten Staaten von Amerika, wahrscheinlich in Kooperation mit Israel, entwickelt und eingesetzt worden ist, wurde dies bis heute nicht von offizieller Seite bestätigt.[4]

Stuxnet ist ein besonderer Fall. Der Virus ist so hochkomplex und aufwändig, dass letztendlich nur staatliche Akteure für seine Entwicklung in Frage kommen. Er musste physisch in die Aufbereitungsanlage eingeschleust werden, da deren Computersysteme nicht mit dem Internet verbunden sind. Dies ist aber heutzutage selbst bei kritischen Infrastrukturen und Militäranlagen immer seltener der Fall. Wenn eine Internetverbindung besteht, kann die Attacke von jedem beliebigen, mit dem Internet verbundenen Computer ausgelöst werden. Cyber-Operationen können auch über Server in Drittstaaten gesteuert werden (um die Ursprünge zu verschleiern). Zudem können die Militärs bei ihren Attacken mit nicht-staatlichen Akteuren zusammenarbeiten. All das macht eine eindeutige Identifizierung der Urheber eines Cyber-Angriffs enorm schwierig und nicht selten sogar unmöglich.

Es gibt noch weitere Unterschiede, die gegen eine einfache Übertragung von bekannten Konzepten der Rüstungskontrolle auf den Rüstungswettlauf im Cyberraum

sprechen. Für Rüstungskontrolle ist ein gewisses Maß an Transparenz über militärische Fähigkeiten und Waffen notwendig. Da Cyberwaffen meistens auf der Ausnutzung von Sicherheitslücken beruhen, beruht der Wert dieser Waffen auf strengster Geheimhaltung. Wird eine Sicherheitslücke bekannt, so wird sie in der Regel auch geschlossen. Damit verlieren alle, die von dieser Lücke wussten, einen möglichen Angriffsvektor. Allerdings gibt es auch zahlreiche bekannte Sicherheitslücken, die nicht geschlossen sind, oder mögliche Zielcomputer sind angreifbar, da sie veraltete Software nutzen.

Der „*Wanna Cry*"-Wurm hat uns diese Problematik gerade eindrücklich vor Augen geführt. Der Erpressungstrojaner basiert auf einer von der NSA identifizierten Sicherheitslücke in alten Windows-Betriebssystemen. Diese Informationen wurden von Servern der NSA gestohlen und von einer Gruppe namens *Shadow Brokers* veröffentlicht.[5] Die Entwickler von „*Wanna Cry*" nutzten diese Schadsoftware und profitierten davon, dass selbst zwei Monate nachdem Microsoft ein Update zur Schließung der Sicherheitslücke zur Verfügung gestellt hatte, noch Zehntausende von Rechnern verwundbar waren.[6] Zusätzlich ist die Verbreitung von Cyberwaffen viel schwieriger zu kontrollieren. Standort und Transport von Raketen oder Panzern lassen sich nur schwer verheimlichen. Eine Schadsoftware lässt sich hingegen beliebig kopieren und über das Internet verbreiten. Als physischer Speicherträger reicht ein einfacher USB-Stick.

Für Staaten gibt es allerdings gute Gründe, sich bei der Jagd nach Sicherheitslücken und dem Einsatz von Cyberwaffen zurückzuhalten. Alle Schwachstellen, die nicht gemeldet werden, um sie als Angriffsvektoren zu nutzen, gehen auch zu Lasten der eigenen Cybersicherheit. Gerade bei Angriffen auf gut gesicherte IT-Systeme ist man auf die Ausnutzung solcher, den Herstellern nicht bekannter Sicherheitslücken angewiesen. Das heißt aber auch, dass diese Schwachstellen in der Infrastruktur des eigenen Landes nicht geschlossen werden können. Kriminelle oder ausländische Staaten, die auch von dieser Schwachstelle wissen, können diese ebenfalls ungehindert nutzen.[7]

Staaten haben auch gute Gründe, sich bei Cyber-Operationen, die über das bloße Ausspähen hinausgehen und darauf ausgelegt sind, IT-Systeme zu manipulieren, zu stören oder zum Ausfall zu bringen, zurückzuhalten. Je weiter unsere Abhängigkeit von digitaler Infrastruktur und informationstechnischen Systemen zunimmt, um so mehr wird ein solcher Einsatz zu einer Gefahr für uns alle. Digitale Supermächte wie die Vereinigten Staaten verfügen zwar über hohe Fähigkeiten zur Durchführung von Cyber-Operationen. Die Vereinigten Staaten sind hier allerdings zugleich auch extrem verwundbar. Ein Cyber-Angriff auf die Elektrizitätsversorgung oder die Börse kann der US-amerikanischen Wirtschaft großen Schaden zufügen. Cyber-Angriffe auf Krankenhäuser könnten die Gesundheitsversorgung der US-Bevölkerung stark beeinträchtigen. Daher überrascht nicht, dass die Vereinigten Staaten und China schon Gespräche über Beschränkungen beim Einsatz von Cyberwaffen geführt haben, insbesondere bezüglich ziviler Infrastruktur.[8] Mit zunehmenden Risiken von IT-Ausfällen wird international das Interesse weiter zunehmen, Normen zum staatlichen Verhalten im Cyberraum zu entwickeln.

Der Weg zu internationalen Normen ist schwierig und umstritten

Dass Analogien aus dem Kalten Krieg nur begrenzt anwendbar sind, heißt nicht, dass wir bei der Diskussion um internationale Regeln für Cyber-Konflikte bei Null anfangen müssten. So initiierte die NATO 2009 als Reaktion auf die Cyber-Attacken gegen ihr Mitglied Estland zwei Jahre zuvor eine Expertengruppe, die sich insbesondere mit der Anwendung des internationalen Kriegsrechts auf Cyber-Angriffe befasste. Das Ergebnis, das im Jahr 2013 veröffentlichte „*Tallinn Manual on the International Law Applicable to Cyber Warfare*“, analysiert, wie bestehendes internationales Recht auf Kriegsführung im Cyberraum anzuwenden ist. Das Tallinn-Handbuch ist zwar rechtlich nicht bindend. Es macht aber deutlich, dass Staaten im Cyberraum nicht in einem rechtsfreien Raum operieren und zeigt, wie internationales Kriegsrecht hier zur Anwendung kommen kann.

Das Tallinn-Handbuch befasst sich vor allem mit der Anwendung internationalen Rechts auf Cyber-Operationen, die von ihren Auswirkungen her bewaffneten Auseinandersetzungen gleichzusetzen sind. Allerdings ist diese Schwelle bisher kaum überschritten worden. Dennoch gehören staatliche Cyber-Operationen mittlerweile zum Alltag. Vor allem Geheimdienste dringen zur Informationsbeschaffung ständig in IT-Systeme anderer Staaten ein. Aber handelt es sich hierbei um völkerrechtlich gedeckte Spionage oder eine völkerrechtswidrige Verletzung der territorialen Integrität anderer Staaten? Diesen und ähnlich gelagerten Fragen widmet sich eine umfangreiche Erweiterung des Handbuchs mit dem Namen „*Tallin 2.0*“. Aber insbesondere bei der Frage, wo bei Cyber-Operationen die Grenze zwischen „legitimer“ Informationsbeschaffung und illegitimer Verletzung völkerrechtlicher Normen verläuft, ist international alles andere als geklärt. Hier gab es unter den Autoren der zweiten Version des Handbuchs erhebliche Differenzen. Und auch wenn man sich in der *Group of Governmental Experts* mittlerweile auf UN-Ebene mit diesen Fragen befasst, ist nicht zu erwarten, dass zu den umstrittensten Fragen zum staatlichen Verhalten im Cyberraum in naher Zukunft ein internationaler Konsens erzielt werden kann.

Die Bundeswehr im Cyberraum: auf Kernaufgaben beschränken

Selbstverständlich muss sich die Bundeswehr mit den neuen Herausforderungen von Cyber-Operationen befassen. Die im neuen Cyber-Kommando gebündelte Expertise und Ressourcen werden dringend benötigt, um sich auf neue Formen von Angriffen und Kriegsführung einzustellen. IT-Systeme durchdringen mittlerweile alle Bereiche der Bundeswehr: von den Waffensystemen über die Befehlssteuerung bis hin zur Logistik. Die Bundeswehr sollte sich zuerst einmal vor allem mit der Verwundbarkeit ihrer eigenen Systeme befassen und ihre eigene IT-Sicherheit erhöhen. Auch mit den Möglichkeiten, digitale Verwundbarkeiten in gegnerischen Militärs auszunutzen, wird man sich beschäftigen müssen. So hat das US-Militär im Irakkrieg mit Hilfe von Cyber-Operationen die Kommunikationsinfrastruktur des irakischen Militärs gestört. Solche Methoden sind selbstverständlich auch für die Bundeswehr interessant. Das Ausschalten beziehungsweise Stören gegnerischer Kommunikations- und Waffensys-

teme durch Cyber-Operationen kann den Verlust menschlichen Lebens in militärischen Auseinandersetzungen verringern. Gleichzeitig sollte die Bundeswehr die Etablierung internationaler Normen stärken – etwa zum Schutz kritischer ziviler Infrastrukturen. Hierzu sind klare Einsatzregeln notwendig. Der Schutz von Zivilisten muss auch bei Operationen im Cyberraum höchste Priorität haben.

Schwieriger ist die Frage, wie die Bundeswehr mit Sicherheitslücken umgehen soll. Obwohl viele Vorfälle in jüngster Zeit verdeutlichen, dass wir vor allem ein Problem mit der IT-Sicherheit haben, investiert die Bundesregierung derzeit stark in ihre Fähigkeiten, sich in IT-Systeme zu hacken. Neben dem Bundesnachrichtendienst und der sich im Aufbau befindenden Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), die Sicherheitsbehörden unter anderem Zugang zu verschlüsselter Kommunikation verschaffen soll, wäre das Cyber-Kommando bereits die dritte bedeutende staatliche Einheit, die auf Jagd nach Sicherheitslücken geht.[9] Wie problematisch das Zurückhalten von Sicherheitslücken sein kann, zeigen jüngste Vorfälle aus den Vereinigten Staaten. Die NSA hortet nicht nur Sicherheitslücken. Sie musste auch hilflos mit ansehen, wie ihre auf diesen Lücken beruhenden Hacking-Werkzeuge und Schadprogramme im Internet veröffentlicht und beispielsweise in der „*Wanna Cry*"-Attacke durch Dritte eingesetzt wurden. Wenn sich schon die mächtige NSA mit dem Schutz ihrer Werkzeuge so schwer tut, wie ist es dann um den Schutz der Cyberwaffen bestellt, die die Bundeswehr entwickeln will?

Es gibt noch ein weiteres Problem. Die Leaks über von der NSA genutzte Sicherheitslücken haben eine kontroverse Debatte über den staatlichen Umgang mit solchen Lücken ausgelöst. Die NSA ist nicht nur für Cyber-Operationen, sondern auch für die Sicherheit von IT-Systemen verantwortlich. Dies erzeugt ein Dilemma: Wie soll die NSA beide Aufgaben – die Sicherheit von IT-Systemen, die das Stopfen von Schwachstellen erfordert, und die Fähigkeit zu Cyber-Operationen, die auf dem Geheimhalten und Ausnutzen dieser Schwachstellen beruht – unter einen Hut bringen? Republikanische und Demokratische Abgeordnete haben einen Gesetzentwurf in den US-Kongress eingebracht, der diesen Abwägungsprozess auf eine gesetzliche Grundlage stellen will.[10] Neben den Militärs und Geheimdiensten sollen auch jene Behörden in die Beratungen einbezogen werden, die primär für den Schutz der IT-Systeme zuständig sind. Die Leitung des Prozesses soll nicht mehr die eher auf Cyber-Operationen setzende NSA, sondern das für den Schutz der zivilen Infrastrukturen zuständige Heimatschutzministerium übernehmen.

In Deutschland baut man zurzeit an seinen offensiven Cyber-Fähigkeiten, ohne sich ausreichend diesen schwierigen Fragen zu stellen. Dabei besteht hier dringender Handlungsbedarf. Die Kontroverse um die NSA zeigt, dass wichtige Sicherheitsinteressen auf dem Spiel stehen. Während man in den Vereinigten Staaten diskutiert, wie man mehr Kontrolle und Transparenz in den Umgang mit Sicherheitslücken bringen kann, scheint die Widersprüchlichkeit des eigenen Vorgehens von den politisch Verantwortlichen in Deutschland noch gar nicht erkannt zu sein. Zumindest verkauft die Bundeswehr ihre Aufrüstung in der Cyber-Domäne als eine Maßnahme zur Stärkung der Cyber-Sicherheit, ohne dass man von der Regierung viel über die hier angesprochenen Unsicherheiten, die das mit sich bringt, hört.

Anstatt sich diesen Fragen zu stellen, geht vielen das Mandat des neuen Cyber-Kommandos noch nicht weit genug. Sie wollen das Cyber-Kommando auch für den Schutz kritischer Infrastrukturen verantwortlich machen und zum sogenannten „Hack Back" befähigen.[11] Diese Forderung schießt nicht nur über das Ziel hinaus, sie ist auch gefährlich. IT-Sicherheitsvorfälle haben in der Regel eines gemeinsam: Es ist nicht klar, wer hinter ihnen steckt. Trotzdem fordern einige Experten, dass die Bundeswehr bei einem Angriff auf ein Stromnetz den Angriff nicht nur in fremde Server zurückverfolgen, sondern auch zurückschlagen und diese lahmlegen darf. Das hieße: wir wissen gar nicht, wer verantwortlich ist, aber wir schlagen mit unserem Militär zurück. Ein solches Eingreifen der Bundeswehr in die IT-Infrastruktur im Ausland würde nicht ohne Folgen bleiben. Andere Staaten könnten darin einen militärischen Angriff sehen und entsprechend antworten; und das alles aufgrund eines Vorfalls, hinter dem auch kriminelle Hacker stecken könnten. Wenn eine kriminelle Organisation von Dänemark nach Deutschland kommt, um Banken zu überfallen, antworten wir auch nicht mit einem Angriff der Bundeswehr auf ihr Versteck hinter der Grenze. Ansonsten würden aus grenzüberschreitender Kriminalität ohne Not zwischenstaatliche Konflikte gemacht. Das kann nicht in unserem Interesse sein.

An der Debatte um den „Hack Back" wird deutlich, dass die Rolle der Bundeswehr im Cyberraum notwendigerweise auf Einsätze im Rahmen eines Auslandsmandats und zur Selbstverteidigung begrenzt sein muss.[12] Der größte Teil unserer Computer, IT-Systeme und Telekommunikationsinfrastruktur ist in privater Hand. Anders als bei einem Angriff feindlicher Panzer bekommt es die Bundeswehr in der Regel gar nicht mit, wenn Cyber-Angriffe auf zivile Infrastrukturen stattfinden. Das heißt nicht, dass der Staat hier keine Verantwortung übernehmen soll. Um einen Angriff überhaupt zeitnah identifizieren und entsprechende Gegenmaßnahmen ergreifen zu können, ist eine enge und vertrauensvolle Kooperation zwischen Unternehmen und Sicherheitsbehörden dringend erforderlich. Aber hierfür braucht es zivile, auf IT-Sicherheit fokussierte Behörden, denn die Zusammenarbeit zwischen Staat und Wirtschaft in Fragen der IT-Sicherheit benötigt vor allem eines: Vertrauen. Die Grundlage für dieses Vertrauen ist bei Behörden mit offensiven Auftrag nicht gegeben. Sie haben ein Interesse, Wissen um Schwachstellen für die Entwicklung eigener Hacking-Fähigkeiten zurückzuhalten. Das heißt: der beste Schutz vor Cyber-Angriffen besteht darin, die zivilen Institutionen zu stärken, die bereits mit der Sicherheit unserer IT-Systeme befasst sind – allen voran das Bundesamt für die Sicherheit in der Informationstechnik (BSI). Die Weiterentwicklung des BSI zu einer starken und unabhängigen Behörde für IT-Sicherheit wäre der nächste konsequente Schritt, um den Schutz unserer zivilen Infrastruktur vor Cyber-Angriffen zu verbessern.

Die Einrichtung des neuen Kommando Cyber- und Informationsraum ist ein Meilenstein für die Bundeswehr. Allerdings brauchen wir eine breitere gesellschaftliche und verteidigungspolitische Diskussion, wie der Auftrag der Bundeswehr im Cyberraum genau aussehen soll. Es stehen hier nichts weniger als zentrale und bewährte Grundsätze der zivilen Ausrichtung unserer Sicherheitspolitik auf dem Spiel. Statt IT-Sicherheit zu militarisieren und damit die internationale Eskalationspotenziale zu erhöhen, sollte die Rolle der Bundeswehr auf ihre verteidigungspolitischen Kernaufgaben beschränkt bleiben. Für den alltäglichen Umgang mit IT-Sicherheitsfällen

brauchen wir weiterhin einen zivilen Ansatz. IT-Sicherheitsgesetz und Stärkung des BSI sind hier die richtigen Hebel. Denn beim Schutz unser zivilen Infrastrukturen gilt: Cyber-Angriff ist nicht die beste Verteidigung.

STEFAN HEUMANN PhD, Jahrgang 1978, ist Mitglied des Vorstands der Stiftung Neue Verantwortung. Stefan Heumann hat in den vergangenen Jahren die Weiterentwicklung der Stiftung Neue Verantwortung zum *Think Tank* für die Gesellschaft im technologischen Wandel mitvorangetrieben und beschäftigt sich insbesondere mit den Auswirkungen neuer Technologien auf internationale Beziehungen, nationale Sicherheit und Bürgerrechte..

Literatur:

Bundesministerium der Verteidigung (2016): Abschlussbericht Aufbaustab Cyber- und Informationsraum, Berlin

Bundesministerium der Verteidigung (2016): Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr, Berlin

Kaplan, Fred (2016): Dark Territory: The Secret History of Cyber War, New York

Rid, Thomas (2016): Maschinendämmerung: Eine kurze Geschichte der Kybernetik, Berlin

Anmerkungen:

1 Zuvor wurde die Positionierung der Bundeswehr im Cyberraum vor allem unter Ausschluss der Öffentlichkeit diskutiert, s. https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/.
2 Um diese Zahl in Kontext zu setzen: Derzeit arbeiten etwa 60 Männer und Frauen an offensiven Cyber-Fähigkeiten. https://www.golem.de/news/verteidigungsministerium-ursula-von-der-leyen-will-13500-cyber-solaten-einstellen-1604-120565.html.
3 S. https://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war.
4 S. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.
5 S. https://mobile.nytimes.com/2017/05/16/us/nsa-malware-case-shadow-brokers.html?smid=tw-share&referer=.
6 S. https://www.heise.de/newsticker/meldung/WannaCry-Angriff-mit-Ransomware-legt-weltweit-Zehntausende-Rechner-lahm-3713235.html.
7 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2928758.

8 S. https://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyber-space.html?_r=0.
9 Bundeskriminalamt und die Polizeieinheiten der Länder und Bundes- sowie Landesämter für Verfassungsschutz sind hier auch bereits aktiv. ZITiS soll zukünftig als zentrale Anlaufstelle für alle dienen, so dass die einzelnen Sicherheitsbehörden die notwendige technische Expertise nicht gesondert aufbauen müssen.
10 S. https://lawfareblog.com/patch-debating-codification-vep.
11 S. https://causa.tagesspiegel.de/politik/darf-die-bundeswehr-cyber-attacken-zur-verteidigung-nutzen/eine-cyber-armee-braucht-auch-einen-auftrag.html.
12 S. https://causa.tagesspiegel.de/politik/darf-die-bundeswehr-cyber-attacken-zur-verteidigung-nutzen/warum-cyber-gegenangriffe-gefaehrlich-sind.html.