Bundesakademie
für Sicherheitspolitik

1/20

#BAKS Arbeitspapier

Von Firewall bis Hackback: Das Spektrum militärischer Cyberoperationen

von Dr. Carolin Busch

Die Begriffe Cyberangriff und Cyberattacke werden in den Medien geradezu inflationär genutzt. Am Rande der Diskussion sprechen Kritiker außerdem von sogenannten Hackback-Plänen der Bundesregierung. In den Konzepten und Strategien von Streitkräften auf der ganzen Welt einschließlich der Bundeswehr ist wiederum oft von Cyberoperationen die Rede. Doch was sind Cyberoperationen aus Sicht des Militärs? Und wie grenzen diese sich vom Begriff des Cyberangriffs ab?

Von Kleinkriminalität bis hin zu militärischen Angriffen

Mit der Einrichtung eines neuen militärischen Organisationsbereichs Cyber- und Informationsraum (CIR) sowie einem Kommando CIR (KdoCIR) hat die Bundeswehr deutlich gemacht, dass sie Cyberbedrohungen sehr ernst nimmt. Unter der damaligen Verteidigungsministerin Ursula von der Leyen wurde hier ein wichtiger politischer Schwerpunkt gesetzt. Geplant ist, dass das KdoCIR im Jahr 2021 seine „Full Operational Capability", also die Zielstruktur erreicht und voll einsatzfähig ist. Noch ist viel zu tun, sowohl was politische Fragen als auch die militärische Fähigkeitsentwicklung angeht. Die Entwicklungen rund um die Bundeswehr werden in den Medien allerdings nur sporadisch dargestellt. Werden dort die Begriffe Cyberangriff oder -attacke genutzt, so sind in der Regel nicht militärische Cyberoperationen gemeint. In den wenigsten Fällen handelt es sich bei den medial erwähnten Angriffen um Vorfälle eines solchen Schweregrades, dass militärische Akteure dafür zuständig wären. Sprechen die Medien von Cyberangriff, so meinen sie damit Aktivitäten, die von Kleinkriminalität (zum Beispiel mittels *Phishing*) bis hin zu organisierter Kriminalität (beispielsweise das Eindringen in Bankennetzwerke) reichen, von Cybervandalismus (das Entstellen von Webseiten) bis hin zu gezielten Angriffen auf kritische Infrastrukturen.

Diese Cyberangriffe können zwar einen hohen finanziellen Schaden verursachen oder auch Hardware zerstören, kosten jedoch keine Menschenleben. Außerdem werden sie in der Regel von Kriminellen oder Hacktivisten (eine Wortmischung aus Hacker und Aktivist) begangen. Für die meisten der oben aufgelisteten Fälle ist die Bundeswehr nicht zuständig, sondern in der Regel die Polizei, in Teilen das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die Geheimdienste. Dies darf allerdings nicht der Ausgangspunkt für sicherheitspolitische Bewertungen oder Überlegungen über militärische Cyberoperationen sein. Bei Cybervorfällen, die durch ausländische staatliche Akteure durchgeführt werden und die die deutsche Souveränität untergraben oder solche, die gar die Schwelle bewaffneter Gewalt überschreiten, ist – unter bestimmten Bedingungen – die Bundeswehr zuständig.

Cyberangriffe im Völkerrecht

In der Diskussion unter Experten und vor allem in der rechtlichen Bewertung sind die meisten Vorfälle, welche die Medien als „Cyberangriffe" bezeichnen, nicht als Angriffe im völkerrechtlichen Sinn zu werten – und in der Regel begründet erst ein solcher Fall die Zuständigkeit von Streitkräften. Sind allerdings Bundeswehrnetzwerke oder internationale Einsätze betroffen, so ist die Bundeswehr selbstverständlich auch unterhalb der Schwelle eines Angriffs (im völkerrechtlichen Sinn) zuständig. Erst wenn ein Cyberangriff in seiner Intensität und seinen Auswirkungen einem bewaffneten Angriff gleicht, kann man völkerrechtlich von einem Angriff sprechen.[1] Hier liegt bereits die erste Schwierigkeit: Es gibt im Völkerrecht keine allgemein geteilte Definition eines „bewaffneten Angriffs". Völkerrechtler teilen die Auffassung, dass ein „bewaffneter Angriff" eine massive Gewaltanwendung darstellen muss und dass der Angriff von außerhalb des angegriffenen Landes stattfinden muss. Uneinigkeit besteht darüber, ob bereits kleine und wiederholte Angriffe im Sinne von „Nadelstichen" darunterfallen. Erst ein bewaffneter Angriff eröffnet Staaten eine Ausnahme vom ansonsten generellen Gewaltverbot in ihren internationalen Beziehungen (Artikel 51 der UN Charta).

Cyberoperationen *können* die Schwelle eines solchen „bewaffneten Angriffs" überschreiten – wenn sie zu Toten sowie großflächiger materieller Zerstörung führen. In der Regel werden sich Cyberoperationen allerdings unterhalb dieser Schwelle bewegen. Einer der bekanntesten Fälle – gleichzeitig aber auch bislang einzigartig, was seine komplexe Entwicklung anging – war der Computerwurm Stuxnet, der sich gegen das iranische Atomprogramm richtete und es laut Einschätzungen um Jahre zurückwarf. Experten sind sich nicht einig, ob dies bereits als Angriff im völkerrechtlichen Sinne zu werten war.

Cyberoperationen: ein breites Spektrum

In der Regel wird eine Cyberoperation verstanden als militärisches Wirken im oder durch den Cyberraum. Denkbar ist hier ein breites Spektrum an Möglichkeiten, das im Nachfolgenden näher betrachtet werden soll, um die Bandbreite dessen aufzuzeigen, worüber staatliche Akteure im Themenkomplex Cyberoperationen nachdenken. Dabei wird deutlich, dass die tradierte Unterscheidbarkeit zwischen „offensiv" und „defensiv" sowie zwischen Spionage und militärischem Handeln im Bereich der Cyberoperationen oft nicht gegeben ist. Stattdessen sollten diese konzeptionell in Form eines Spektrums gesehen werden und nicht in strikte Kategorien, wie eben „defensiv" und „offensiv", einsortiert werden.

Eine mögliche Perspektive auf dieses Spektrum ist der fließende Übergang von defensivem Vorgehen, zum Beispiel mittels Firewalls, hin zu offensivem Vorgehen, das heißt dem Eindringen in fremde Systeme und deren Ausspionieren. Die schon erwähnte Diskussion um eine aktive Cyberabwehr – von Kritikern auch Hackback genannt – nimmt das offensive Ende dieses Spektrums in den Blick. Waren vergangene deutsche Strategien noch rein defensiv ausgelegt (siehe zum Beispiel die ausschließlich zivile erste Cybersicherheitsstrategie von 2011), so ist spätestens mit der Aufstellung des Bundeswehr-Organisationsbereichs Cyber- und Informationsraum 2017 klar, dass die Bundesregierung auch offensives Vorgehen nicht außenvorlässt.

Ohne Scheuklappen argumentierte beispielsweise der Abschlussbericht des Aufbaustabs CIR, der den Grundstein für den neuen Organisationsbereich legte: „Hat ein Akteur die Fähigkeit zur Verteidigung, so kann er auch weltweit angreifen." Dementsprechend schlussfolgert der Bericht, dass „zur Durchführung wirkungsvoller Cyber-Maßnahmen immer defensive und offensive Fähigkeiten erforderlich sind".[2] Diese offene Einschätzung, der eine Vielzahl an Cyberexperten zustimmen würde, war für Deutschland ein durchaus mutiger Schritt und keineswegs selbstverständlich. Sie zeugt von einem realpolitischen Verständnis.

[1] Siehe dazu ausführlich Schmitt (Hrsg.) (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.
[2] Bundesministerium der Verteidigung (2016): *Abschlussbericht Aufbaustab Cyber- und Informationsraum*, online: https://www.bmvg.de/resource/blob/11412/868d0f8c03b84846f6bb959618a5518f/c-26-04-16-download-auftrag--cyber-verteidigung-data.pdf.

Allerdings ist auch bei offensivem Vorgehen eine große Bandbreite vorhanden. Die US-amerikanischen Soldaten und Autoren Owen Tullos und Gary Brown schlugen schon 2012 vor, zwischen „Cyber Disruption" (etwa Stören/Unterbrechen) und „Cyber Attack" zu unterscheiden.[3] „Cyber Disruption" sind beispielsweise Unterbrechungen im Betrieb und verursachen keinen materiellen Schaden, schon gar keine Toten. Die Autoren argumentieren, dass das „Zusammenwerfen von verschiedenen Aktivitäten in eine zu inklusive Kategorie wie *computer network attacks*", wie es das US-amerikanische Verteidigungsministerium gemacht hat, die konzeptionelle Weiterentwicklung des Themas lähmt. „Es ist schlicht unmöglich, entsprechende Handlungsanweisungen zu entwickeln, wenn alle negativen Cyberaktivitäten gleichbehandelt werden, egal, ob es sich um das Stilllegen einer Website handelt oder die komplette Zerstörung eines Computersystems", schreiben Tullos und Brown.

Rechtmäßigkeit und Zuständigkeiten

Eine weitere Frage in der Diskussion um die Zulässigkeit von Cyberoperationen ist die rechtliche. Gerade die Pläne einer aktiven Cyberabwehr (bis hin zu einem offensiven Vorgehen) werden von vielen Aktivisten und Journalisten als rechtswidrig kritisiert, und aufwendige juristische Bewertungen werden dabei verkürzt dargestellt. So fasst beispielsweise das Portal netzpolitik.org einen Bericht des Wissenschaftlichen Dienstes des Bundestages dahingehend zusammen, dass sogenannte Hackbacks im Ausland verfassungswidrig seien, während dieser selbst zu einer deutlich differenzierteren Bewertung kommt.[4]

Dabei ist auch hier das Spektrum an möglichen Handlungen zu betrachten. Laut einer Analyse des Juristen Christian Marxsen ist zwischen Cyberaktivitäten der Bundeswehr im Inneren und Einsätzen im Äußeren zu unterscheiden. Im Inneren sind unterstützende und beratende Tätigkeiten der Bundeswehr (Stichwort Amtshilfe) rechtlich erlaubt. Läge hingegen ein Zwangs- und Einsatzcharakter vor, „so wären Cybermaßnahmen im Inneren nur in den explizit verfassungsrechtlich geregelten Konstellationen, allem voran zur Verteidigung, denkbar," schreibt Marxsen.[5] Hier müsste ein Cyberangriff – wie oben beschrieben – in seiner Intensität und seinen Auswirkungen mit einem bewaffneten Angriff auf die Bundesrepublik vergleichbar sein. Der Angriff müsste aus dem Ausland kommen und idealerweise einem Staat zurechenbar sein. Bei der Mitwirkung der Bundeswehr bei der Erstellung eines Cyberlagebilds gemeinsam mit anderen Behörden ist die rechtliche Lage nicht mehr ganz so klar, denn laut Marxsen bedingt die Natur des Cyberraums, dass hier mit hoher Wahrscheinlichkeit in Grundrechte eingegriffen wird, „insbesondere in das Fernmeldegeheimnis (...), aber auch in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme".

Ob allerdings erst die Schwelle bewaffneter Gewalt überschritten werden muss, damit die Bundeswehr handeln kann, muss angesichts hybrider Bedrohungen neu diskutiert werden. Schließlich ist es ein Merkmal hybrider Bedrohungen, dass sie bewusst unterhalb der Schwelle von bewaffneter Gewalt und damit entsprechender politischer Entsperrungen wie in Deutschland dem vom Bundestag festzustellenden Spannungs- und Verteidigungsfall bleiben. In diese Richtung stieß auch die Aussage des Inspekteurs CIR General Ludwig Leinhos: „Wir brauchen etwas, welches ich in der Diskussion gerne als ‚digitalen Verteidigungsfall' bezeichne, unterhalb der Schwelle eines klassischen Verteidigungsfalls."[6] Anders ausgedrückt: Wann kann die Bundeswehr zur Cyberverteidigung Deutschlands beitragen, wenn kein Angriff im völkerrechtlichen Sinn vorliegt, aber die Situation eine wie auch immer geartete Verteidigung erfordert? Laut der Konzeption der Bundeswehr sind die deutschen Streitkräfte unter anderem für „Verteidigungsaspekte der gesamtstaatlichen Cybersicherheit" zuständig. Konzeptionell gesehen ist unklar, was genau darunter zu verstehen ist. Kritiker, wie

[3] Tullos/Brown (2012): On the Spectrum of Cyberspace Operations, *Small Wars Journal*, 11. Dezember, online: http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations.
[4] Siehe zum Beispiel: Netzpolitik (2018): Wissenschaftliche Dienste des Bundestages: „Hackbacks" im Ausland sind verfassungswidrig, 19. Juni, online: https://netzpolitik.org/2018/wissenschaftlichen-dienste-des-bundestages-hackbacks-im-ausland-sind-verfassungswidrig/.
[5] Marxsen (2017): Verfassungsrechtliche Regeln für Cyberoperationen der Bundeswehr, *Juristenzeitung* 11, S. 551.
[6] Wiegold (2019): Bundeswehr plädiert für digitalen Verteidigungsfall zur besseren Cyber-Abwehr, *Augen Geradeaus*, 12. Juni, online: https://augengeradeaus.net/2019/06/bundeswehr-plaediert-fuer-digitalen-verteidigungsfall-zur-besseren-cyber-abwehr/

beispielsweise die Autoren von netzpolitik.org, argumentieren, dass eine Rolle der Bundeswehr in der gesamtstaatlichen Sicherheit außer im Verteidigungsfall nicht vorgesehen ist. Befürworter einer stärkeren Rolle der Bundeswehr argumentieren hingegen, dass es die Natur des Cyberraums (beispielsweise extrem schnelle Datenübertragung, möglicherweise großer materieller Schaden innerhalb von Stunden und ohne Vorwarnung) sowie hybride Bedrohungen es notwendig machen, dass die Bundeswehr nicht erst dann eingreifen darf, wenn es bereits zu spät ist und zum Beispiel große Teile des deutschen Stromnetzes lahmgelegt worden sind.

Was auswärtige Einsätze angeht, so sind Cyberoperationen, die sich *nicht* ausdrücklich in das betreffende Einsatzmandat eingliedern (wie beispielsweise in Afghanistan), laut Christian Marxsen folgendermaßen zu bewerten: „Vor dem Hintergrund des für Cyberkonflikte bestehenden Eskalationsrisikos und des Grundsatzes, dass die Parlamentsbeteiligung im Zweifel weit auszulegen ist, sind (...) kaum Konstellationen denkbar, in denen Cyberoperationen generell ohne Parlamentsbeteiligung, das heißt per bloßer Regierungsentscheidung zulässig wären."[7] Das Parlamentsbeteiligungsgesetz von 2015 erlaubt allerdings „Einsätze bei Gefahr im Verzug, die keinen Aufschub dulden" *ohne* eine vorherige Zustimmung des Bundestags, wenn diese unverzüglich nachgeholt wird. Dies würde es zumindest erleichtern, die Schnelligkeit von Cyberangriffen besser zu adressieren. Doch ganz unabhängig davon wird die Bundesregierung nicht umhinkommen, über die gegenwärtige Gesetzeslage nachzudenken, wenn die Bundeswehr tatsächlich auch unterhalb der Schwelle des Verteidigungsfalls zur gesamtstaatlichen Sicherheit substantiell und regelmäßig (das heißt nicht nur im Rahmen von sporadischer Amtshilfe) beitragen soll.

Aufgaben der Bundeswehr

Eine weitere Perspektive auf das Thema Cyberoperationen sind die in der Konzeption der Bundeswehr klar definierten Aufgaben der Bundeswehr. Sie reichen von der Landes- und Bündnisverteidigung über Krisenmanagement und – wie bereits erwähnt – Verteidigungsaspekte der gesamtstaatlichen Cyber-Sicherheit bis hin zum Grundbetrieb der Bundeswehr. Weniger prominente Aufgaben sind Unterstützungsleistungen zum Erhalt und zur Weiterentwicklung nationaler Schlüsseltechnologiefelder oder Partnerschaft und Kooperation auch über EU und NATO hinaus. Bekanntes Territorium aus Cyberperspektive ist sicherlich der Grundbetrieb, das heißt das Sichern der eigenen Netzwerke sowie die Aus- und Weiterbildung von Bundeswehrpersonal. Dies wird seit Jahren gemacht, wobei im sich im Bereich Aus- und Weiterbildung durch die Aufstellung des Organisationsbereich CIR vieles stark weiterentwickelt hat. Das Forschungsinstitut CODE (Cyber Defence) an der Universität der Bundeswehr in München wurde zwar bereits 2013 gegründet. Doch mit der Neuaufstellung des Organisationsbereich CIR wurden hier Schwerpunkte gesetzt und es zeichnet sich ab, dass CODE nicht nur deutschlandweit, sondern auch europaweit eine große Rolle in der Forschungs- und Ausbildungslandschaft rund um Cyber spielen wird. Neuland und nur in Szenarien durchdacht ist die Rolle der Bundeswehr bei der Landesverteidigung im Cyberraum; die oben dargestellte Aussage von General Leinhos wurde in Deutschland, beispielsweise im parlamentarischen Raum, bislang viel zu wenig diskutiert. In Einsätzen hingegen hat die Bundeswehr bereits Erfahrungen mit Cyberoperationen gemacht: Eines der wenigen bekannten Beispiele war das Hacken eines afghanischen Mobilfunkbetreibers im Jahr 2015, um Informationen über eine entführte deutsche Entwicklungshelferin zu erlangen.

Nur im Cyberraum?

Eine weitere spannende Perspektive auf das Thema Cyberoperationen betrifft die sehr praktische Frage, ob reine Cyberoperationen überhaupt die Regel sind. Anders ausgedrückt: werden Cyberfähigkeiten nicht öfters im Verbund (oder innerhalb von *Joint Operations*) Anwendung finden? Der Blick auf einige bekannte Beispiele zeigt, dass Cyberfähigkeiten im Verbund gut funktionieren und eine Querschnittsaufgabe haben oder erst die Voraussetzung zum Einsatz kinetischer Gewalt schaffen:

[7] Marxsen (2017): Verfassungsrechtliche Regeln für Cyberoperationen der Bundeswehr, *Juristenzeitung* 11, S. 552.

- Im Mai 2019 machten die Streitkräfte Israels Schlagzeilen mit einem Luftschlag gegen das sogenannte Cyberhauptquartier der Hamas. Auf Twitter schrieb das israelische Militär: „We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed."

- 2015 wurde der Hacker Junaid Hussain der Terrorgruppe Islamischer Staat in einem Drohnenangriff der amerikanischen Streitkräfte getötet, unter anderem aufgrund seiner Hackingaktivitäten.

- 2015 wurde durch eine Cyberoperation auf Informationssysteme von drei ukrainischen Energieversorgungsunternehmen die Stromversorgung in der Westukraine für eine bis sechs Stunden unterbrochen. Teil der Operation war ein Denial-of-Service-Attacke auf das Kundencenter der Energieversorgungsunternehmen. Dabei wurden Telefonanlagen stark überlastet, sodass Kunden, welche die Unterbrechung melden wollten, durch belegte Leitungen blockiert wurden. Die Angreifer konnten nicht eindeutig identifiziert werden. Die ukrainische Regierung verdächtigte jedoch die russische Hackergruppe „Sandworm-Team".

- 2007 bombardierte die israelische Luftwaffe in Syrien den nuklearen Forschungsreaktor in Dayr az-Zawr. Israel hielt sich bedeckt, was die Vorgänge anging und so konnte der Angriff nur teilweise rekonstruiert werden. Weit vor den Angriffen kam es zur Ausspähung des Computers eines hohen syrischen Regierungsvertreters durch ein Trojanisches Pferd. Dem Luftschlag gingen unmittelbar Maßnahmen der elektronischen Kampfführung sowie vermutlich ein Cyberangriff voraus. So wurde die Generierung eines aktuellen Luftlagebilds erschwert und zum Eindringen der israelischen Kampfjets in den syrischen Luftraum beigetragen. In Deutschland unterstehen auch Kräfte zur Elektronischen Kampfführung (EloKa) dem Organisationsbereich Cyber- und Informationsraum.

Nichtsdestotrotz gibt es auch viele Beispiele reiner Cyberoperationen. Einen exzellenten Überblick über bekannte Vorfälle mit staatlichen Tätern bietet die *Cyber Operations Tracker Database* des Council on Foreign Relations.[8] Die schiere Bandbreite möglicher Cyberoperationen und -aktvitäten bedingt, dass gegenwärtig mehr Fragen gestellt als beantwortet werden können. Dringender Handlungsbedarf besteht beispielsweise in der Definition des Bundeswehrbeitrags zur gesamtstaatlichen Sicherheit. An dieser Stelle muss sich der Gesetzgeber auch überlegen, ob das gegenwärtige rechtliche Rahmenwerk der vernetzten, schnellen Welt, in der wir heute leben, angemessen ist.

Darüber hinaus muss eine Bestandsaufnahme stattfinden, welche Fähigkeiten dafür noch aufgebaut werden müssen. Leider wird in der öffentlichen Debatte meist zu kurz und polarisierend gedacht, und vermeintlich illegale Hackback-Fähigkeiten stehen im Zentrum der Debatte. Es ist es an der Zeit, dass das Thema Cyberoperationen sowohl in der oben dargestellten Breite als auch in der Tiefe konzeptionell durchdrungen wird, um offene, auch politische, Fragen zu beantworten und besser auf die Zukunft vorbereitet zu sein.

Dr. Carolin Busch ist Analystin und Beraterin. Sie arbeitet für ein mittelständisches Unternehmen im Bereich Verteidigung und Sicherheit. Die Autorin gibt ihre persönliche Meinung wieder.

[8] Council on Foreign Relations: Cyber Operations Tracker Database, online: https://www.cfr.org/interactive/cyber-operations#CyberOperations (eingesehen 2020).