6. Krieg im Cyberspace? Die militärische Nutzung des Netzes

Eine wachsende Zahl von Staaten hat damit begonnen, den Cyberspace auch als militärische Domäne zu erschließen und damit ihre Sicherheitspolitiken zu komplementieren (Lewis und Neuneck, 2013). Spätestens seit den Cyberangriffen auf Estland im Jahr 2007 wird immer wieder über die Möglichkeit eines Cyberwars debattiert. Dem Cyberspace wird dabei immer wieder eine Begünstigung konventionell unterlegener Akteure zugesprochen. Außerdem sei das Netz ein Ort in dem die Offensive der Defensive stets überlegen sei. Aufgrund des Attributionsproblems sei es ferner kaum verlässlich möglich, AngreiferInnen zu identifizieren. Durch diese strategischen Eigenschaften ist der Cyberspace ein sicherheitspolitischer Handlungsraum, der die internationalen Beziehungen und den Konfliktaustrag potenziell verändert. Wie die beiden Untersuchungsstaaten mit den militärischen Herausforderungen des Netzes umgegangen sind, wird im Folgenden näher untersucht.

Im folgenden Kapitel wird nachvollzogen, inwiefern die beiden Untersuchungsstaaten begonnen haben, offensive Fähigkeiten aufzubauen und durch welche Einflüsse dies ermöglicht wurde. Ferner wird in diesem Zusammenhang analysiert, welche (völker)rechtlichen Positionen die Staaten mit Blick auf den Einsatz von militärischen Cyberkapazitäten entwickelt haben.

6.1 Deutschland

6.1.1 Der Aufbau militärischer Kapazitäten: Defensive Ausrichtung und Schutz der eigenen Systeme

Verstärkte Aufmerksamkeit erfuhr die IT-Sicherheit der Streitkräfte, als Ende der 1990er Jahre die Sicherheit kritischer Infrastrukturen eingehender debattiert wurde. Die potenziellen Folgen der Beeinträchtigung von militärischer Infrastruktur durch Cyberangriffe wurde in diesem Kontext auch von einer Enquete-

Kommission des Bundestags problematisiert und die Komplexität der Gefahrenlage diskutiert:

> »Bedrohungen können von kriminellen Einzeltätern, von Terroristen, von kriminellen Organisationen oder auch von feindlichen Staaten ausgehen. Insofern wird die Unterscheidung zwischen ziviler und militärischer Bedrohung sowie zwischen innerer und äußerer Sicherheit immer verschwommener.« (Deutscher Bundestag, 1998b, S. 84)

In einer Auseinandersetzung im Cyberspace sei daher immer weniger zwischen Krieg und Frieden zu unterscheiden. Angriffe könnten das gezielte Handeln der gegnerischen Partei massiv einschränken, ohne die Schwelle eines bewaffneten Angriffs zu erreichen. Zu derartigen Angriffen könnten, so die Einschätzung der Kommission, auch weniger ressourcenstarke Akteure in der Lage sein, so dass asymmetrische Konfliktlagen entstünden. Um der neuen Verwundbarkeit vernetzter Gesellschaften und der Streitkräfte zu begegnen, solle auf Defensivmaßnahmen gesetzt werden, da etablierte Konzepte wie Abschreckung nur sehr begrenzt anwendbar seien (ebd., S. 84).

Die Bundeswehr setzte, wie viele andere Streitkräfte, auf das militärische Potenzial von IT, um in Gefechtssituationen informationelle Vorteile zu erlangen bzw. diese ausnutzen zu können. So wurde auch in der Bundeswehr unter der Bezeichnung vernetzte Operationsführung ein Konzept der network centric warfare entworfen (heise.de, 2006). Im Weißbuch von 2006 wurde die militärische Bedeutung des Cyberspace in einem zentralen militärischen Strategiedokument erwähnt. Hier betonte die Bundesregierung ebenfalls, dass Cyberangriffen vorrangig mit zivilen Mitteln begegnet werden müsse (Bundesministerium der Verteidigung, 2006, S. 19). Die militärische Beschützer-Rolle war damit zunächst defensiv angelegt und auf den Schutz der bundeswehreigenen Infrastrukturen bzw. (Waffen-)Systeme gerichtet.

In der Folge wurde aber auch die Möglichkeit erprobt, den Cyberspace zur Durchführung offensiver militärischer Operationen zu nutzen. Ersten institutionellen Ausdruck fanden die Bestrebungen zur offensiven militärischen Nutzung des neuen Handlungsraums im Jahr 2007 als im Kommando Strategische Aufklärung eine Einheit zur Durchführung von Computer Network Operations (CNO) gegründet wurde. Auftrag dieser neuen Einheit war und ist es, in gegnerischen Netzwerken zu wirken und ggf. konventionelle militärische Maßnahmen zu begleiten. Ein eigenständiges, losgelöstes Wirken im Sinne eines »Cyberwar« wurde durch das Verteidigungsministerium aber als unwahrscheinlich eingeschätzt (Deutscher Bundestag, 2014c, S. 1165). Damit legte die Bundesregierung den Grundstein zum Aufbau einer offensiven militärischen Beschützer-Rolle.

Die Bundesregierung sah in einem durch militärische Feindseligkeit geprägten Cyberspace aber auch ein erhebliches Risiko und plädierte dafür, internationa-

le Regeln zur Selbstbeschränkung zu fördern, um eine »Kultur der Zurückhaltung zu schaffen« (Deutscher Bundestag, 2010a, S. 5). Zu dieser Kultur der Zurückhaltung gehörte aus Sicht der Bundesregierung die Präzisierung völkerrechtlicher Vorgaben sowie die freiwillige Selbstbeschränkung der Staatengemeinschaft (ebd., S. 5). Die Bundesregierung unterstrich die eigene Zurückhaltung bspw. dadurch, dass die Bundeswehr keine Schadsoftware entwickeln sollte bzw. dass die Streitkräfte keine Cyberangriffe gegen Ziele im Ausland durchführten (ebd., S. 5). Diese Position stand in offensichtlichem Widerspruch zur Etablierung eigener CNO-Kräfte, die zur Infiltration gegnerischer Netze auf den Einsatz von Schadsoftware angewiesen sind.

Entsprechend den Einschätzungen im Weißbuch 2006, wurde in der ersten Cybersicherheitsstrategie der Bundesregierung 2011 deren zivile Ausrichtung betont:

> »Zivile Ansätze und Maßnahmen stehen bei der Cyber-Sicherheitsstrategie im Vordergrund. Sie werden ergänzt durch die Maßnahmen der Bundeswehr zum Schutz ihrer eigenen Handlungsfähigkeit und im Rahmen zugrunde liegender Mandate, um auf diese Weise Cyber-Sicherheit als Teil gesamtstaatlicher Sicherheitsvorsorge zu verankern.« (Bundesministerium des Innern, 2011, S. 5)

Dem Gedanken staatlicher Selbstbeschränkung folgend, wurde das Aufgabengebiet der Bundeswehr defensiv beschrieben. Im Fokus stand der Schutz der eigenen militärischen Netze. Diese Ausrichtung ist auch aus der Haltung der Bundesregierung ableitbar, dass die in der Strategie skizzierten Maßnahmen keine parlamentarische Mandatierung erforderten (Deutscher Bundestag, 2011a, S. 4). Dennoch wurde auch hier darauf hingewiesen, dass vernetzte Gesellschaften erheblichen Risiken aus dem Cyberspace ausgesetzt seien. Die neue Verwundbarkeit wurde wiederum insbesondere mit Bezug zu kritischer Infrastruktur hergestellt. Als Beispiel für eine solche Attacke wurde unter anderem auf den Wurm Stuxnet verwiesen, der in Iran Zentrifugen zur Urananreicherung manipuliert hatte (Bundesministerium des Innern, 2011, S. 3).[1]

Die Beschützer-Rolle blieb somit zwar defensiv ausgerichtet, allerdings rückte mit der kritischen Infrastruktur und dem Szenario eines potenziell folgenreichen Cyberangriffs ein neues Referenzobjekt sowie die Frage der Landesverteidigung in den Blick.

In den Verteidigungspolitischen Richtlinien 2011 wurde die militärische Gefahr, die von Cyberangriffen ausging, dann auch zentraler aufgegriffen. Hier heißt es:

1 Für weitere Informationen zu Stuxnet s. bspw. Zetter (2014).

> »Informationsinfrastrukturen gehören heute zu den kritischen Infrastrukturen, ohne die das private und öffentliche Leben zum Stillstand käme. Angriffe darauf können aufgrund ihrer engen Verflechtung zur Destabilisierung auch unseres Staates mit gravierenden Auswirkungen für die nationale Sicherheit führen. Mit der Bedrohung aus dem Informationsraum werden Staaten ihre bisherigen Vorstellungen über Konflikte und ihre Lösungsmöglichkeiten anpassen.« (Bundesministerium der Verteidigung, 2011, S. 9)

Insbesondere die Möglichkeit, die Urheberschaft von Angriffen ex post abstreiten zu können, wurde von der Regierung in diesem Kontext problematisiert, so entstünden potenziell asymmetrische Konfliktlagen, die es ohne diese neue Vulnerabilität nicht geben würde. Unter Bezugnahme auf Artikel 51 der UN-Charta, hat die Bundesregierung aber bereits 2011 die Einschätzung vertreten, dass auch ein Cyberangriff, der in seinen Folgen einem konventionellen Angriff vergleichbar ist, als bewaffneter Angriff bewertet werden und folglich das Recht zur Selbstverteidigung auslösen könne (Deutscher Bundestag, 2011a, S. 4).

Auf internationaler Ebene versuchte die Bundesregierung weiterhin, ein militärisches Wettrüsten zu vermeiden und auf staatliche Zurückhaltung hinzuwirken. Die Abschlusserklärung beim NATO-Gipfel in Lissabon, in der die Bedrohung durch Cyberangriffe prominent erwähnt wurde und in der von allen Mitgliedsstaaten mehr Engagement gefordert wurde, wurde von der Regierung und dem Bundestag debattiert (Bundesministerium der Verteidigung, 2011, S. 9 bzw. 17). Dass eine Cyberattacke automatisch unter Artikel 5 des Nordatlantik-Vertrags fallen könne, wurde in einer öffentlichen Anhörung des Auswärtigen Ausschusses kritisch beurteilt. Die Abgeordneten bevorzugten die Konsultation eines solchen Vorfalls unter Artikel 4 (Deutscher Bundestag, 2011c, S. 14-16). Diese Auffassung wurde gleichsam von der Bundesregierung und der Opposition in einer Debatte des neuen strategischen Konzepts der NATO im Bundestag zum Ausdruck gebracht (Deutscher Bundestag, 2010b, S. 7600, 7608 bzw. 7610). Auf internationaler Ebene setzte sich die Bundesregierung daher erfolgreich dafür ein, Cyberangriffe innerhalb der NATO nicht automatisch nach Artikel 5 zu behandeln. Ziel dieses Vorstoßes war es, einen dezidiert zivilen Ansatz beim Umgang mit diesen neuen Gefahren zu entwickeln (Deutscher Bundestag, 2010c, S. 8097).[2]

Im Rahmen der Vereinten Nationen plädierte die Bundesregierung wiederholt für die Etablierung internationaler Normen zum Umgang mit Cyberangriffen. Der Fokus lag hierbei einerseits auf Verbesserungen bei der Attribtution

2 Die Debatte um die Anwendbarkeit von Artikel 5 war nach den Angriffen auf Estland im April und Mai 2007 verstärkt geführt worden (The Guardian, 2007). 2014 legte die NATO fest, dass ein Cyberangriff potenziell Artikel 5 auslösen könne. Ein Automatismus wurde allerdings nicht etabliert ebenso wenig definierte die Allianz eine Schwelle für einen solchen Angriff (Reuters, 2016).

von Angriffen, die durch internationale Kooperation verlässlicher werden sollte, sowie auf der Sorgfaltsverantwortung der Staaten für den Cyberspace. Staaten sollten Angriffe unterbinden, die von ihrem Territorium ausgingen (United Nations, 2011, S. 10). Die Regierung wies in diesem Kontext darauf hin, dass Staaten dem Völkergewohnheitsrechts entsprechend Verantwortung trügen »for internationally wrongful cyber activity attributable to them, including the internationally wrongful activity in cyberspace of any State-backed proxies acting on the State's instructions or under its direction or control […]« (United Nations, 2013a, S. 9). Regierungen müssten daher darauf hinwirken, dass ihr Territorium nicht für Cyberangriffe genutzt werde (ebd., S. 9).

Auch wenn die Bundesregierung international versuchte, eine Kultur der Zurückhaltung zu fördern, wurden die eigenen Kapazitäten nach 2010 immer weiter ausgebaut und auch institutionell verankert. Weiterhin hat die Bundesregierung ihre Haltung zur militärischen Nutzung des neuen Handlungsraumes entwickelt. Bereits mit der Schaffung der CNO-Kräfte vertrat die Regierung die Auffassung, dass der Aufbau und Einsatz von Schadsoftware durch die Bundeswehr kein grundsätzliches rechtliches Problem darstelle. Eine Einschätzung die innerstaatlich später auch durch ein Gutachten des Wissenschaftlichen Dienstes des Bundestages prinzipiell bestätigt wurde (Deutscher Bundestag, 2015h). Eine erste theoretische Einsatzfähigkeit erreichten diese Kräfte 2012 (Augen Geradeaus!, 2012). Der Verteidigungsausschuss des Bundestages wurde von der Regierung über diese neuen Fähigkeiten 2012 bzw. 2013 informiert (Deutscher Bundestag, 2014c, S. 1165). Damit war auch ein relevanter Gegenrollenträger offiziell in die Entwicklung offensiver Fähigkeiten der militärischen Beschützer-Rolle eingebunden.

6.1.2 (Schonende) Offensive und aktive Verteidigung

Im Jahr 2015 wurde in Deutschland immer häufiger auch über offensive militärische Maßnahmen im Cyberspace debattiert. Auslöser hierfür war unter anderem die Einschätzung der Bundesregierung, dass Cyberangriffe immer häufiger durchgeführt würden und dass sie hierbei einen Qualitätssprung vollzogen hätten (Deutscher Bundestag, 2015d, S. 3). Diese Einschätzung fand auch in einem gewachsenen und immer deutlicher formulierten militärischen Schutzanspruch Ausdruck. Während der Aufgabenbereich der Bundeswehr in der ersten Cybersicherheitsstrategie noch zurückhaltend formuliert wurde und auf den Schutz der eigenen militärischen Infrastruktur bezogen blieb, zeigte sich in der Folgezeit deutlicher, dass die Bundeswehr den Cyberspace als weiteren militärischen Handlungsraum konzipiert hatte. Auch in diesem Raum sollte die Bundeswehr ihren verfassungsmäßigen Aufgaben nachkommen:

> »Die Verteidigung gegen Cyber-Angriffe, die einen bewaffneten Angriff auf Deutschland darstellen bzw. einen solchen vorbereiten oder begleiten können. Die Ausübung von Cyberfähigkeiten im Rahmen von Auslandseinsätzen nach Artikel 24 Absatz 2 des Grundgesetzes.« (Deutscher Bundestag, 2015d, S. 3)

Damit fand die Beschützer-Rolle erstmals konkrete offensive Bezüge. Im Falle eines bewaffneten Angriffs nach Artikel 51 der UN-Charta sollte die Bundeswehr die Landesverteidigung übernehmen. Außerdem sollten Cybermaßnahmen mandatierte Auslandseinsätze komplementieren.

Die Strukturen bei der Bundeswehr waren aus Sicht der Regierung diesen Herausforderungen nicht mehr gewachsen und mussten daher reformiert werden. Die Exekutive betonte hierbei aber, dass der Einsatz der Streitkräfte den gleichen Erfordernissen unterliege wie eine konventionelle Dislozierung. Die CNOs sollten aus Sicht der Regierung einerseits die eigenen Kräfte schützen sowie deren Wirken unterstützen (ebd., S. 3f.).

KritikerInnen aus der Netzgemeinde sahen in der zunehmend offensiven Ausrichtung der Bundeswehr ein Problem für das Netz allgemein, da Cyberangriffe wie »Streubomben« wirken könnten, die viele, auch unbeabsichtigte, Ziele treffen könnten. Diese Analogie wurde von der Bundesregierung aber als unangemessen zurückgewiesen, da die kinetischen Folgen deutlich unterschiedlich seien. Außerdem seien die Angriffe genau auf Zielsysteme zuschneidbar. Dies sei besonders wichtig, da die Bundeswehr durch das Völkerrecht verpflichtet ist, Kollateralschäden zu minimieren (ebd., S. 5).

Während KritikerInnen potenziell unbeherrschbare Folgen der Beschützer-Rolle bspw. durch das Überspringen von Malware auf Systeme jenseits des eigentlichen Ziels fürchteten, wurde der Cyberspace von der Regierung als besonders »schonende« Domäne für den militärischen Einsatz bewertet.

In der Folge gestand die Bundesregierung auch ein, dass die CNO-Kräfte zum Wirken in fremden Netzen auf Schwachstellen zurückgreifen müssten und daher Schadsoftware bzw. Exploits benötigten (Deutscher Bundestag, 2015b). Die Regierung argumentiert zwar, dass im Sinne eines Vulnerabilities Equities Process Sicherheitslücken, »deren Nutzung weitreichende Auswirkungen auf die Sicherheit der Bevölkerung bzw. des Staates haben, gemeldet werden sollen«, schränkte aber ein, dass dabei die zur Aufrechterhaltung der Schutzfunktion notwendigen Kapazitäten nicht negativ beeinträchtigt werden dürften (Deutscher Bundestag, 2018c, S. 10). Ob bzw. inwiefern die Bundeswehr beim Aufspüren und der Nutzbarmachung von Schwachstellen (Zero-Day-Exploits) mit privatwirtschaftlichen Unternehmen kooperiert bzw. diese Lücken dort bezieht, beantwortet die Regierung nicht öffentlich (ebd., S. 10).

In diesem Bereich wird die Ablehnung einer Beschützer-Rolle für das gesamte Internet besonders deutlich. Die Auswirkungen einer Sicherheitslücke werden mit Blick auf die nationalen Gegebenheiten evaluiert. Ein Schutz der globalen Infrastruktur, wie er zur Kontestation der Beschützer-Rollen in fast allen Bereichen von der Netzgemeinde gefordert wird, findet bei der Regierung keine Unterstützung.

Die Bundesregierung nutzte die neuen Kapazitäten der Beschützer-Rolle bereits im Herbst 2015. 2016 berichteten Medien darüber, dass die Bundeswehr 2015 den ersten Einsatz ihrer CNO-Kräfte durchgeführt habe. Im Rahmen der Befreiung einer in Afghanistan entführten Entwicklungshelferin, hatten sich die Streitkräfte, nach Anfrage aus dem Krisenstab des Auswärtigen Amts, in das Netz eines afghanischen Telekommunikationsdienstleisters gehackt und die Bewegungen der EntführerInnen mittels Handydaten verfolgt. Offiziell bestätigt wurde diese Operation allerdings nicht (Spiegel, 2016).

Bei einem Blick auf die Einsatzdoktrin der CNO-Kräfte der Bundeswehr wird ferner ein Trend deutlich, der, sofern er von allen Staaten geteilt wird, das Ziel einer internationalen Kultur der Zurückhaltung deutlich schwieriger erreichbar macht. Während das Völkerrecht für den Einsatz staatlicher Streitkräfte die sichtbare Unterscheidung zwischen Kombattanten und Nicht-Kombattanten vorsieht, betont die Bundesregierung, dass das völkerrechtliche Unterscheidungsgebot »bei der Nutzung technischer Einrichtungen und Aktivitäten im Cyber-Raum nicht [verlange, Anm. d. Verf.], die Zurechenbarkeit zu einem bestimmten Staat offenzulegen« (Deutscher Bundestag, 2015d, S. 11). Die SoldatInnen, die CNOs durchführen, tragen daher Uniformen mit Hoheitsabzeichen und sind damit als Kombattanten im Sinne des Völkerrechts erkennbar (Deutscher Bundestag, 2015a, S. 5), die technischen Infrastrukturen, über die ein Angriff erfolgt, attribuieren den Angriff aber nicht eindeutig. Die Nutzung falscher Identitäten, um den Verdacht bspw. auf andere Akteure zu lenken, ist aus Sicht der Bundesregierung aber untersagt (Deutscher Bundestag, 2015b, S. 2). Der Aufbau einer verifizierbaren Kultur der Zurückhaltung im Cyberspace ist dadurch dennoch erschwert. Insgesamt zeigt die Bundesregierung auch kein Interesse daran, offensive Fähigkeiten mit anderen Staaten zu teilen. Die Beurteilung von Cyberangriffen soll ebenfalls, auch innerhalb der EU, den Nationalstaaten überlassen bleiben (Deutscher Bundestag, 2018a).

Im Kontext der Debatte um den Aufbau offensiver Kapazitäten definierte die Bundesregierung weiterhin gegen welche Ziele die neuen Mittel eingesetzt werden dürften. Hierbei orientierte sie sich an etablierten völkerrechtlichen Normen. Ziele von militärischen Cyberangriffen können aus Sicht der Bundesregierung nur Objekte sein,

> »[…] die aufgrund ihrer Beschaffenheit, ihres Standorts, ihrer Zweckbestimmung oder ihrer Verwendung wirksam zu militärischen Handlungen beitragen und deren gänzliche oder teilweise Zerstörung, deren Inbesitznahme oder Neutralisierung unter den im betreffenden Zeitpunkt des Angriffs gegebenen Umständen einen eindeutigen militärischen Vorteil darstellen.« (Deutscher Bundestag, 2015a, S. 2)

Dies könne aber auch »nicht als militärisch klassifizierte Gegner« einschließen, sofern rechtlich zulässig mit militärischen Mitteln gegen diese vorgegangen werden dürfe (Deutscher Bundestag, 2015d, S. 6).

Die parlamentarische Opposition verlangte Auskunft darüber, ob aus Sicht der Bundesregierung offensive Cybermaßnahmen ein konstitutives Mandat des Bundestages benötigten. Die Regierung stellte in der Folge klar, dass für offensive Einsätze der CNO-Kräfte die gleichen Regeln wie für den konventionellen Einsatz deutscher Truppen gelten. Damit sicherte die Regierung dem Parlament die tradierten Kontrollrechte auch für CNOs zu:

> »Der Einsatz militärischer Cyber-Fähigkeiten durch die Bundeswehr unterliegt denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte. Grundlagen für Einsätze der Bundeswehr sind die einschlägigen Regelungen des Grundgesetzes sowie des Völkerrechts, Maßnahmen des Sicherheitsrates nach Kapitel VII der VN-Charta (Mandate), völkerrechtliche Vereinbarungen mit dem betreffenden Staat und das Parlamentsbeteiligungsgesetz.« (Ebd.)

Damit bestätigte die Bundesregierung die Regelungen nach Artikel 87a GG. Außerdem betonte die Regierung, dass Artikel 26 GG Deutschland auch im Cyberspace einen Angriffskrieg verbiete (ebd., S. 7). Der Einsatz der neuen Fähigkeiten der militärischen Beschützer-Rolle sollte aus Sicht der Regierung damit domestisch wie international den etablierten rechtlichen Regeln folgen und parlamentarisch mandatiert werden.

Ebenfalls 2015 begann das Verteidigungsministerium mit der Arbeit an einem neuen Weißbuch zur deutschen Sicherheitspolitik. In diesem Zusammenhang wurde das Thema Cybersicherheit zu einem zentralen Themengebiet, das in einem eigenen Workshop bearbeitet wurde. Zur Eröffnung dieser Veranstaltung skizzierte die Verteidigungsministerin die Gefahrenlage im Cyberspace sowie die potenziellen Herausforderungen für die Streitkräfte. Sie betonte dabei, dass Cyberoperationen zu etablierten Komponenten militärischer Auseinandersetzungen geworden seien. In diesem Kontext habe insbesondere der Konflikt zwischen Russland und Georgien 2008 gezeigt, wie die beiden Komponenten verknüpft werden könnten. Das Attributionsproblem mache aber eine Kartierung der Konfliktparteien schwierig, dies liege an der grenzen- und hierarchielosen

Organisation des Netzes. Zur Illustration der vielfältigen Einsatzmöglichkeiten von Cyberangriffen wies die Ministerin auf den Bundestagshack 2015 hin. Mit Blick auf die Konfliktkonstellationen im Cyberspace betonte die Ministerin, Cyberangriffe ermöglichten konventionell unterlegenen Akteuren asymmetrisch gegen andere vorzugehen (Bundesministerium der Verteidigung, 2015a).

Die Aufgaben der Bundeswehr umfassten nach Einschätzung der Bundesregierung daher zwei wesentliche Bereiche: erstens den Schutz der bundeswehreigenen IT-Systeme. Dies sei auch mit Blick auf die zunehmend vernetzten Waffensysteme wie den Eurofighter von zentraler Bedeutung, um im Ernstfall das Funktionieren der konventionellen Streitkräfte sicherzustellen und den Schutzauftrag erfüllen zu können. Zweitens stelle der Cyberspace neben Land, See, Luft und Weltraum einen eigenen militärischen Handlungsraum dar, in dem die Bundeswehr agiere und daher die entsprechenden Fähigkeiten aufbauen und vorhalten müsse. Um dieses Ziel zu erreichen sollte ein eigener Organisationsbereich Cyber- und Informationsraum die vorhandenen Kapazitäten bündeln und Partnerstaaten als zentraler militärischer Ansprechpartner in Fragen der militärischen Cybersicherheit dienen. Die Ministerin setzte daher einen Aufbaustab ein, der mit der konzeptionellen Entwicklung dieses neuen Organisationsbereichs betraut wurde (ebd.). Zudem beschloss das Verteidigungsministerium schon im April 2015 die »Strategische Leitlinie zur Cyber-Verteidigung im Geschäftsbereich BMVg« (Bundesministerium der Verteidigung, 2015b). Der Spiegel berichtete im Juli 2015 über das eingestufte Dokument und Netzpolitik.org veröffentlichte zeitgleich den Volltext (Netzpolitik.org, 2015; Spiegel, 2015b).[3]

In den Leitlinien verwies das BMVg zunächst auf die gestiegene Abhängigkeit von IT, die staatliche, wirtschaftliche und gesellschaftliche Akteure gleichermaßen betreffe. Explizit leiste die Bundeswehr in diesem Zusammenhang »Beiträge zum Heimatschutz auch durch die Verteidigung gegen Cyber-Angriffe, die einen bewaffneten Angriff auf Deutschland darstellen, vorbereiten oder begleiten können« (Netzpolitik.org, 2015). Außerdem sei in künftigen Konfliktlagen davon auszugehen, dass komplementär zu konventionellen Operationen, die gegnerische Nutzung des Cyberspace beeinträchtigt oder ganz unterbunden werden müsse. Dabei müsse stets die eigene Handlungsfähigkeit gesichert werden. Die Notwendigkeit in diesem Bereich verstärkt aktiv zu werden, wurde neben der gewachsenen Vulnerabilität auf die gestiegene Angriffshäufigkeit sowie auf die qualitativ immer ausgefeiltere Durchführung zurückgeführt. Die Leitlinien weisen aber auch darauf hin, dass die Bundeswehr allein möglicherweise nicht dazu in der Lage sei, das nötige Know-How vorzuhalten, so dass evtl. auf Ressourcen aus der Reserve

3 Das veröffentlichte Dokument verfügt über keinerlei Paginierung mehr, weshalb in folgenden Referenzen auf den Text Verweise auf Seitenzahlen fehlen.

zurückgegriffen und Personal aus der Wirtschaft temporär eingebunden werden müsse (Netzpolitik.org, 2015).

Offensive Cyberoperationen stellten aus Sicht des BMVg besonders effektive Mittel zur Zielerreichung dar, da sie präzise gegen bestimmte Ziele eingesetzt werden könnten und zumeist keine kinetischen Folgen hätten, also keine Menschenleben gefährdet würden. Ferner seien deren Effekte nicht von Dauer:

> »Offensive Cyber-Fähigkeiten der Bundeswehr sind als 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.« (Ebd.)

Rollentheoretisch gesprochen waren CNOs aus Sicht der Bundesregierung damit ein geeignetes Mittel, die militärische Beschützer-Rolle möglichst ohne Kollateralschäden und physische Zerstörung zu erfüllen. Cyberangriffe sind damit ein besonders »schonendes« und präzises Mittel zur Erreichung militärischer Ziele.

Die Leitlinien stießen sowohl bei der parlamentarischen Opposition als auch bei VertreterInnen der Zivilgesellschaft auf Kritik. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) erkannte in der Bevorratung von Sicherheitslücken zur offensiven Nutzung eine Unterminierung der Sicherheit des Netzes im Allgemeinen. Außerdem wurde bemängelt, dass die Leitlinien erhebliche rechtliche Probleme aufwürfen, da sie ein Wirken gegen IT-Infrastrukturen vorsehen, die potenziell nicht in staatlicher Hand seien und ggf. keine legitimen Ziele für militärische Angriffe darstellten. Aus dieser Sicht verstieß die Bundesregierung mit den Plänen gegen die Genfer Konventionen und würde internationales Recht brechen (FIfF, 2015). Ferner wies sowohl das FIfF als auch die deutsche Gesellschaft für Informatik darauf hin, dass die Bundesregierung mit Blick auf den Bundestagshack 2015 gezeigt habe, dass der Schutz essenzieller Infrastrukturen nicht gewährleistet sei. Daher sei der Ausbau defensiver Maßnahmen begrüßenswert, der Ausbau offensiver Kapazitäten aber unangemessen (Gesellschaft für Informatik, 2015). Auch die Grünen bemängelten die zu offensive Ausrichtung der Leitlinien als kontraproduktiv, da Deutschland auf diesem Weg einer zunehmend konfliktiven Dynamik im Cyberspace folge (Brugger, 2015).

Diese Kontestationen wurden von der Bundesregierung aber nicht aufgenommen und blieben folgenlos. Im April 2016 legte der Aufbaustab Cyber- und Informationsraum seinen Abschlussbericht vor. Trotz der Kontestationsprozesse wurde in diesem Dokument der Ausbau der militärischen Kapazitäten befürwortet. Dabei wurde auf die nationale Sicherheit, auf die Manipulation von Wahlen sowie auf die wirtschaftliche Prosperität verwiesen: »Die zunehmend komplexeren Angriffe erfordern den Ausbau der staatlichen Handlungsfähigkeit zum Schutze

unseres demokratischen Systems und seiner wirtschaftlichen Grundlagen« (Bundesministerium der Verteidigung, 2016, S. 1).

Die militärische Beschützer-Rolle hatte im Zuge der Debatten um Wahlmanipulationen durch russische Cyberangriffe während des US-Präsidentschaftswahlkampfs mit dem demokratischen System ein zusätzliches neues Referenzobjekt erhalten. In diesem Kontext wirkte die Rolle als Garant liberaler Grundrechte katalytisch auf den Ausbau der Beschützer-Rolle, da die Freiheiten notfalls auch militärisch zu schützen seien.

Die Notwendigkeit, einen eigenen militärischen Organisationsbereich einzurichten, wurde neben einem »Qualitätssprung in der Bedrohungslage« mit dem Verweis auf internationale Partner sowie Entwicklungen in der NATO begründet (ebd., S. 1f. sowie 13f.). Die NATO hatte den Cyberspace 2016 auf dem Gipfel von Warschau als »a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea« definiert (NATO, 2016). Der Aufbaustab empfahl daher, entsprechend der Ankündigung der Ministerin, analog zu Verbündeten einen eigenen Organisationsbereich mit InspekteurIn zu etablieren (Bundesministerium der Verteidigung, 2016, S. 1).

Zur Verdeutlichung des gestiegenen Risikopotenzials verwies der Aufbaustab unter anderem auf Stuxnet, der die Angreifbarkeit von kritischen Infrastrukturen gezeigt habe sowie auf den OPM- und Bundestagshack, die potenziell sensible Informationen zum Ziel hatten.[4] Das Netz mit seinen technischen Besonderheiten und seiner globalen Architektur stelle dabei sowohl die Unterscheidung zwischen Krieg und Frieden als auch die Differenzierung innerer und äußerer Sicherheit vor Herausforderungen. Für den Einsatz der Streitkräfte im Cyberspace gelten aber dennoch die gleichen Regelungen wie für deren konventionellen Einsatz (Parlamentsbeteiligungsgesetz) (ebd., S. 5). Der Aufbaustab erklärte, es sei das Ziel mit dem neuen Organisationsbereich »Informationsdominanz im Operationsraum zu erreichen, um Entscheidungsprozesse zu optimieren und Einsatzwirkung zu maximieren« (ebd., S. 5). Dazu müsse sowohl das Personal besser geschult als auch das institutionelle Gefüge der Bundeswehr angepasst werden (ebd., S. 16f.). Im Oktober 2016 wurde dazu im Ministerium eine neue Abteilung Cyber- und Informationstechnik aufgestellt (Bundeswehr, 2020).

Neben dem Umgang mit qualitativ immer höherwertigen Angriffen, wurde mit der Reform der Beschützer-Rolle auch, die internationale Kooperationsfähigkeit verbessert. Ferner wurden zur Rechtfertigung des Aufbaus auch auf die eigenen Erfahrungen mit Cyberangriffen verwiesen.

---

4 2014/15 wurde das amerikanische Office of Personnel Management (OPM) Opfer eines Cyberangriffs bei dem persönliche Daten von mehr als 20 Millionen Bediensteten und BewerberInnen gestohlen wurden (The New York Times, 2015). Ebenfalls 2015 wurde der Bundestag zum Ziel eines Angriffs, auch hierbei wurden Daten entwendet (Spiegel, 2015c).

Aufgrund der Sorge vor folgenreichen Angriffen auf kritische Infrastrukturen arbeitete die Bundesregierung auf internationale Normen hin. Im Rahmen der OSZE setzte sich die Bundesregierung 2016 erfolgreich für eine Kultur der Zurückhaltung ein. Mit einem zweiten Bündel von vertrauensbildenden Maßnahmen wurde unter deutschem Vorsitz empfohlen, dass Staaten auf freiwilliger Basis dazu beitragen sollten, Cyberangriffe auf kritische Infrastrukturen zu vermeiden, da diese auch Folgen für benachbarte Staaten haben könnten (OSCE, 2016a,b). Diese Maßnahmen sind Teil der Bemühungen eine Norm des Nicht-Angriffs auf kritische Infrastrukturen zu etablieren, die allerdings bis heute nicht allgemein anerkannt ist. 2019 drängte der Bundesaußenminister erneut auf die Spezifizierung einer solchen Norm, die konkret Angriffe auf weltweite Handelsströme, das Bankensystem oder die zivile Luftfahrt ächten solle. Heiko Maas bemängelte, dass hierzu aber »der ernsthafte politische Wille« fehle (Auswärtiges Amt, 2019).

Eingeleitet durch den Prozess der Erarbeitung eines neuen Weissbuches, setzte sich auch der Verteidigungsausschuss des Bundestages Anfang 2016 mit der militärischen Nutzung des Internets auseinander. Hier wurde durch die Sachverständigen unter anderem auf Probleme bei der Parlamentsbeteiligung hingewiesen. Angeführt wurde bspw. der Umstand, dass der Einsatz von deutschen Tornados zur Aufklärung zustimmungspflichtig sei, obwohl kein Waffeneinsatz erfolge. Für Cyberoperationen bedeute das, dass auch die Aufklärung feindlicher Netze, also der erste Zugriff eigentlich durch den Bundestag mandatiert werden müsse (Deutscher Bundestag, 2016a, S. 25). Mehrere Gutachter sprachen sich ferner gegen die Entwicklung von Schadsoftware durch die Bundesrepublik aus. Dies berge stets das Risiko, dass diese Werkzeuge von Dritten zweckentfremdet würden, dass damit die globale Unsicherheit steige und dass gegnerische Systeme permanent ausgekundschaftet werden müssten, um die Zuverlässigkeit der Exploits sicherzustellen (ebd., S. 20 bzw. 27). Insbesondere letztgenannter Aspekt widerspreche »der deutschen Kultur der militärischen Zurückhaltung« (ebd., S. 27). Die Vertreterin des BMVg teilte diese Kritik allerdings nicht. Mit Blick auf die potenzielle Proliferation von Wissen über Schwachstellen sah die Staatssekretärin des BMVg aber keine Probleme, da die Bundeswehr die eigenen Wissensbestände »im Griff« habe (ebd., S. 40).

In dieser Anhörung wurde ferner darüber debattiert, wie weitreichend eine staatliche Sorgfaltsverantwortung für den Cyberspace reichen könne und ob damit ggf. umfassende Überwachungsmaßnahmen verbunden seien (ebd., S. 37f.). Eine umfassende Kontrolle von Internetverkehr, um Angriffe aufzuspüren, stand somit prinzipiell im Widerspruch zur Rolle als Garant liberaler Grundrechte.

Darüber hinaus bestanden bei der Opposition Bedenken, inwiefern Cyberoperationen überhaupt parlamentarisch kontrollierbar seien, da keine physischen Truppenbewegungen entständen und die Operationen stets klandestin ablaufen könnten. Ferner könne das Attributionsproblem auch gegen die parlamentari-

schen KontrolleurInnen verwendet werden (ebd., S. 50-54). Die Frage, ab wann die Bundesregierung einen Cyberangriff als bewaffneten Angriff werten und damit ein Recht auf Selbstverteidigung beanspruchen würde, wurde von der Vertreterin des Verteidigungsministeriums nicht beantwortet; auch unter Verweis, dass dadurch »die Grauzone« entfallen würde, die ggf. Entscheidungsspielraum gewähren oder abschreckend wirken könne (ebd., S. 53). Ähnlich argumentierte die Bundesregierung auch in der Antwort auf eine parlamentarische Anfrage. Konkrete Maßstäbe oder Schwellen zur Beurteilung eines Vorfalls nannte sie auch hier nicht (Deutscher Bundestag, 2015d, S. 10 bzw. 11). Sollte die Regierung zu der Auffassung gelangen, dass ein Angriff das Selbstverteidigungsrecht auslöse, würde sie sich aber vorbehalten, »mit allen zulässigen militärischen Mitteln [zu; Anm. d. Verf.] reagieren« (Deutscher Bundestag, 2018e, S. 6).

Sichtbar kulminiert ist der domestische Aufbau von Cyberkapazitäten im Jahr 2017 als die Bundeswehr das Kommando Cyber- und Informationsraum (Kdo CIR) mit etwa 14.500 Dienstposten etablierte. Diesem untersteht unter anderem das Kommando Strategische Aufklärung sowie das 2018 gegründete Zentrum Cyber-Operationen (Bundesministerium der Verteidigung, 2020; Bundeswehr, 2020). Ebenfalls 2018 wurde beschlossen in Kooperation zwischen dem BMI und BMVg die Agentur für Innovation in der Cybersicherheit zu gründen. Sie soll dazu beitragen die technologische Souveränität der Bundesrepublik bei Schlüsseltechnologien sicherzustellen (Bundesregierung, 2019a). Mit dem Kdo CIR wurde der Cyberspace als militärischer Handlungsraum auch institutionell fest verankert.

Einerseits hat sich die Bundesregierung bei diesem Schritt maßgeblich an den internationalen Partnern orientiert und die Kooperationsfähigkeit verbessert. Insbesondere die Entwicklungen und Erfordernisse in der NATO wurden in diesem Kontext immer wieder angeführt. Andererseits wurden die zunehmend häufiger auftretenden und in ihrer Qualität immer besseren Cyberangriffe zur Rechtfertigung der neuen Kapazitäten herangezogen. Gegen die internationalen Dynamiken blieben die domestischen Kontestationen folgenlos. Eine von der parlamentarischen Opposition (insbesondere den Grünen und Linken) immer wieder angemahnte Lücke bei der Kontrolle militärischer Cyberkapazitäten, wurde von der Bundesregierung ebenfalls bestritten (Deutscher Bundestag, 2018c, S. 3).

Trotz Kritik aus den Reihen des Parlaments konnte die Regierung auf die Zustimmung der Mehrheit der Abgeordneten zählen. So konnte die Regierung auch die parlamentarische Zustimmung zu einer Budgeterhöhung für den Aufbau des neuen Kommando Cyber- und Informationsraum gewinnen. Um die parlamentarische Kontrolle der CNO-Kräfte zu verbessern, wird darüber diskutiert, einen spezifischen parlamentarischen Unterausschuss zu etablieren (Deutscher Bundestag, 2017b, S. 53f.).

Besonders problematisiert wurde die, aus Sicht der Opposition, unklare Aufgabenteilung zwischen dem Bundesnachrichtendienst und der Bundeswehr beim

Einsatz in gegnerischen Netzen (Deutscher Bundestag, 2016a, S. 39). Diese Frage wurde explizit auch mit der Thematik eines digitalen Gegenschlags als Reaktion auf einen Cyberangriff (Hackback) debattiert. Da in diesem Kontext die Frage offen war, wer diese Maßnahme durchführen solle (ebd., S. 45). Die Regierung verwies in diesem Kontext auf das 2011 gegründete Nationale Cyber-Abwehrzentrum in dem die wesentlichen Akteure (BKA, Nachrichtendienste und Streitkräfte) vertreten seien und in dem eine Entscheidung über die angemessene Reaktion und die durchführende Stelle getroffen werden könne (ebd., S. 62).

Da aus Sicht der Bundesregierung zwischen Krieg und Frieden im Cyberspace nicht mehr eindeutig unterschieden werden konnte, weil die Angriffe praktisch nie die Schwelle eines bewaffneten Angriffs überschreiten und so das Selbstverteidigungsrecht gemäß Artikel 51 der UN-Charta auslösen könnten, plädierten VertreterInnen der Bundeswehr für eine neue gesetzliche Regelung zum »digitalen Verteidigungsfall«, die einen Einsatz der Streitkräfte im Cyberspace unterhalb der Schwelle eines bewaffneten Angriffs ermöglicht und die innerstaatlichen Prozesse zur Amtshilfe (Art. 35 GG) durch die Bundeswehr vereinfacht (Augen Geradeaus!, 2019). Aus Sicht des Inspekteurs des Kdo CIR, kommt es bei schwerwiegenden Cyberangriffen

> »[…] buchstäblich auf Minuten an. Die derzeitigen Prozesse des Bundes und der Länder sind darauf nicht ausgelegt. Allein die Unkenntnis des Angreifers und die damit verbundene Frage der Zuständigkeit, das bisher fehlende gesamtstaatliche Cyber-Lagebild und die Verfahren zur Anforderung von Amtshilfe oder die fehlende direkte Zusammenarbeit mit beispielsweise den Internet Service Providern ermöglichen aktuell keine optimale Reaktion in solch einem Szenario.« (Ebd.)

Im Juni 2019 konstatierte Verteidigungsministerin von der Leyen in einem Interview, dass die Möglichkeit zu digitalen Gegenschlägen »zur Abschreckung« benötigt werde, dass Reaktionen aber nicht zwangsläufig digital sein müssten, sondern bspw. durch Sanktionen erfolgen könnten (t-online.de, 2019).

Damit versuchte die Bundesregierung die Einsatzschwelle der militärischen Beschützer-Rolle zu senken. Dies war aus Sicht der Streitkräfte nötig, da die etablierten Voraussetzungen durch Cyberangriffe kaum erreicht werden. Einem Verschwimmen der Trennung zwischen Krieg und Frieden, wie er immer wieder debattiert wurde, würde dann durch eine niedrigere Schwelle zum Einsatz der militärischen Beschützer-Rolle korrespondieren.

Unklar ist die konkrete Aufgabe der Bundeswehr in diesem Kontext auch in einer maßgeblich vom Innenministerium im Mai 2019 angestoßenen, noch nicht beendeten, Debatte um digitale Gegenschläge im Falle eines Cyberangriffs – KritikerInnen sprechen in diesem Zusammenhang von Hackback, die Bundesregierung bezeichnet das Vorgehen als aktive Cyberabwehr. Im Ernstfall sollte

aus Sicht des Innenministers der BND auf einen Angriff bspw. auf kritische Infrastrukturen, wie im Falle WannaCry, reagieren und die entsprechenden Gegenmaßnahmen ausführen, dieser Vorstoß erfolgte Presseberichten zufolge nach Absprache mit dem Bundeskanzleramt. Um ein solches Vorgehen zu ermöglichen, bedürfte es aber einer Grundgesetzänderung, da es sich hierbei um polizeiliche Maßnahmen zur Gefahrenabwehr handelt, für die die Bundesländer zuständig sind (Deutschlandfunk, 2019a; ZDF, 2019). Ein Vertreter des Innenministeriums sagte dazu:

> »Wenn man bei solchen Szenarien zu dem Ergebnis kommt, dass es die Länder alleine nicht schultern können, gehört es zu unserer Pflicht, uns auf eine solche Situation rechtlich vorzubereiten. Wenn wir sie nie brauchen, wäre es mir am liebsten.« (Deutschlandfunk, 2019a)

Diese Position vertrat die Bundesregierung auch bei einer parlamentarischen Anfrage im November 2018. Inwiefern diese neue Herausforderung eine Neubalancierung zwischen Bund und Ländern erfordere, würde noch geprüft (Deutscher Bundestag, 2018e, S. 3). Eine Entscheidung zugunsten des BND könnte ferner das Trennungsgebot unterminieren (Deutschlandfunk, 2019a).

Ein Gutachten der Wissenschaftlichen Dienste des Bundestages kam zu dem Schluss, dass es völkerrechtlich zunächst nicht relevant sei, ob die Gegenmaßnahme durch einen Nachrichtendienst oder die Streitkräfte erfolge, da die Handlung dem Staat zugeschrieben würde. Allerdings dürften militärische Gegenmaßnahmen (also Angriffe, die signifikante Schäden verursachen) »nur durch Kombattanten, also Mitglieder der Streitkräfte, ausgeführt werden« (Deutscher Bundestag, 2018f). Die durchführende Instanz müsste also durch Art des Einsatzes bestimmt werden, ganz allgemein fehle den Nachrichtendiensten aber eine Befugnis jenseits der Aufklärung (ebd.).

In einem regierungsinternen Papier, aus dem der Bayerische Rundfunk zitierte, wurde ein vierstufiges Vorgehen beschrieben, um massiven Cyberangriffen aus dem Ausland zu begegnen. In einer ersten Reaktion (Stufen eins und zwei) könnten die Netzbetreiber oder Polizeien damit beginnen den Netzwerkverkehr zu blockieren oder die Routen zu verändern. Hierbei fände noch keine offensive Maßnahme außerhalb der eigenen Netze statt. Auf der dritten Stufe soll es der zuständigen Behörde erlaubt sein, auf fremde Netzwerke zuzugreifen und »Daten zu verändern oder Daten zu löschen« (Bayerischer Rundfunk, 2019). Dieser Schritt war ein Desiderat nachdem beim Bundestagshack 2015 sensible Daten abgegriffen worden waren, die später auf Rechnern in Osteuropa gefunden wurden. Aufgrund einer fehlenden Rechtsgrundlage, durften die Informationen dort aber nicht gelöscht werden. Die vierte Stufe der Reaktion sah dann ein Eingreifen in die Systemfunktionen des angreifenden Rechners vor, um einen laufenden Angriff zu beenden. Über das Vorgehen sollte im Cyber-Abwehrzentrum beraten

werden, inwiefern »ein erheblicher Cyber-Angriff aus dem Ausland vorliegt«, der nicht durch andere Maßnahmen beendet werden kann (Bayerischer Rundfunk, 2019). In der Folge sollte ein Gremium aus VertreterInnen des Kanzleramts, des Auswärtigen Amts, des Justiz-, des Verteidigungs- und des Innenministeriums über eine Reaktion entscheiden. Mit der Durchführung des Gegenangriffs sollte dann der BND betraut werden (ebd.).

Der Innenminister rechtfertigte die Maßnahmen unter Verweis auf die potenziell verheerenden Folgen eines umfassenden Cyberangriffs:

> »Wenn Sie sich einen größeren Angriff auf kritische Infrastruktur vorstellen – nicht nur Energieversorgung, sondern Krankenhäuser und ähnliches und alles gleichzeitig –, dann kann eine solche Situation eintreten, wo eben die herkömmlichen Abwehrmöglichkeiten nicht mehr ausreichen.« (Deutschlandfunk, 2019a)

Kontestationen gegen die Pläne gab es sowohl vom Koalitionspartner als auch von der parlamentarischen Opposition, die insbesondere vor einem Rüstungswettlauf warnte und das Risiko von Kollateralschäden hervorhob. Um die unerwünschten Folgen eines Cyberangriffs zu illustrieren, verwies ein Vertreter der FDP auf das Risiko eines »Cyber-Kundus« (ZDF, 2019).[5] Im September 2019 wurde über ein eingestuftes Gutachten des Wissenschaftlichen Dienstes des Bundestages berichtet, das ebenfalls mit Verweis auf potenzielle Eskalationsdynamiken Probleme bei den Plänen zu einem digitalen Gegenschlag feststellte (Zeit, 2019).

Bislang ist unentschieden, welche Institution, in welcher Form digitale Gegenschläge führen sollte. Die militärische Beschützer-Rolle der Bundeswehr wurde zwar ausgebaut, es bleibt aber unklar, wann diese Kapazitäten eingesetzt werden. Klar ist nur, dass dies bei einem bewaffneten Angriff, der das Selbstverteidigungsrecht nach Artikel 51 der UN-Charta evoziert und im Rahmen von mandatierten Einsätzen der Streitkräfte möglich wäre. Wie ein digitaler Verteidigungsfall aussehen könnte, der diese Hürden unterschreitet, ist dagegen noch nicht geklärt.

6.2 Vereinigtes Königreich

6.2.1 Der Aufbau militärischer Kapazitäten: Neue offensive Möglichkeiten

Offensive Cyberkapazitäten zum militärischen Einsatz wurden durch das GCHQ bereits Anfang der 2000er Jahre im Rahmen des Einsatzes in Afghanistan aufge-

5 Am 4. September 2009 befahl ein deutscher Oberst den Luftangriff auf zwei von den Taliban entführte Tanklaster. Bei diesem Angriff starben mindestens 90 ZivilistInnen (Deutschlandfunk, 2019b).