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).

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

baut. Hierbei stützte sich der Nachrichtendienst auf eine erprobte Kooperation mit dem Verteidigungsministerium. Dabei sind offensive Cybermaßnahmen zum Einsatz gekommen, die direkte Folgen für den Konfliktverlauf in der realen Welt gehabt haben (GCHQ, 2018c). Diese Einsätze wurden aber erst weit nach deren Durchführung eingeräumt.

Entsprechend der offensiven Ausrichtung der militärischen Beschützer-Rolle sprach sich die britische Regierung international bereits 2004 explizit gegen ein Verbot der militärischen Nutzung des Netzes aus. Die völkerrechtlichen Vorgaben zum Einsatz militärischer Mittel seien zur Verhinderung eskalativer Dynamiken ausreichend. Außerdem könne ein solches Verbot im Widerspruch zum Prinzip des freien Informationsflusses im Netz stehen, da zur Verifikation Kontrollen von und ggf. Eingriffe in Datenströme notwendig werden könnten. In der ersten Risikoeinschätzung kam die britische Exekutive zu der Auffassung, dass Staaten keine maßgeblichen Gefahren im Netz darstellten (United Nations, 2004, S. 11).

Die militärische Beschützer-Rolle unterscheidet sich hier bereits deutlich von der deutschen. Schon in der Frühphase nutzte die britische Regierung offensive Cyberkapazitäten um die eigenen Streitkräfte zu unterstützen. Eine zusätzliche Kontrolle war aus Sicht der Exekutive nicht notwendig, da rechtliche Regelungen übertragbar seien. Eine Kontrolle der Rolle könne ferner im Widerspruch zum freien Fluss von Informationen im Netz stehen. Restriktionen der Beschützer-Rolle waren aus rollentheoretischer Sicht nicht mit der Rolle als Garant liberaler Grundrechte vereinbar.

Die Gefahreneinschätzung mit Blick auf staatliche Akteure revidierte die britische Regierung in ihrer ersten Cyber Security Strategy 2009 (Cabinet Office, 2009, S. 13). Da Staaten nun doch als Risiken für die nationale Cybersicherheit gesehen wurden, wurde dem Verteidigungsministerium bereits 2008 die Aufgabe zugeschrieben, die Entwicklungen im Bereich der Cybersicherheit zu überwachen und die potenziellen Risiken zu evaluieren (Cabinet Office, 2008, S. 44). Cybersicherheit wurde in der folgenden National Security Strategy (NSS) 2009 zu den emergenten Problemfeldern der Sicherheitspolitik gezählt. Die Regierung ging davon aus, dass Staaten zunehmend damit beginnen würden, militärische Kapazitäten in diesem Bereich zu entwickeln. Anstelle von militärischen Interventionen könnten dann Cyberangriffe genutzt werden, um Schäden zu verursachen (UK Government, 2009, S. 13, 65).

In der ersten Cyber Security Strategy von 2009 wies die Regierung darauf hin, dass der Cyberspace auch genutzt werden sollte, um gegen Gegner vorzugehen. Cyberangriffe gegen Großbritannien könnten sowohl von Staaten als auch Terrororganisationen ausgehen. Die Regierung müsse daher in der Lage sein, falls nötig, offensive Maßnahmen zu ergreifen (Cabinet Office, 2009, S. 13-16). Der Cyberspace sei die neue Domäne, die es zum Erhalt der Sicherheit und des Wohlstands zu verstehen und nutzen gelte:

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

> »Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our position in cyber space.« (Cabinet Office, 2009, S. 21)

Die britische Beschützer-Rolle fand damit neben dem Schutz der eigenen Netze bereits früh eine Referenz (Schutz vor wem?) auf den (Cyber)Aktivitäten feindlicher Staaten und von Terrorgruppen. Ähnlich wie in der Bundesrepublik wurde die Notwendigkeit militärischer Handlungsfähigkeit auch durch potenzielle Angriffe auf kritische Infrastrukturen gerechtfertigt.

Die militärische Einschätzung verschärfte sich 2010 nach dem Wahlsieg der Tories. In diesem Kontext rückte die Offensive zunehmend in den Fokus der Aufmerksamkeit. In der neuen NSS sah der National Security Council in Cyberangriffen eine der vier größten sicherheitspolitischen Herausforderungen für das Vereinigte Königreich. Angriffe könnten dabei von Staaten, Terrororganisationen oder Kriminellen ausgehen (UK Government, 2010, S. 11 sowie 27). Zur Illustration möglicher Angriffe auf kritische Infrastrukturen und deren »potentially devastating real-world effect«, verwies die britische Regierung auf den Wurm Stuxnet (ebd., S. 30).

Die Kompetenzen des GCHQ sollten bei der Entwicklung offensiver Fähigkeiten genutzt werden, um auch militärische Kapazitäten auszubauen. In der Cyber Security Strategy von 2011 wurde dies institutionell verankert. Die Regierung etablierte hierzu eine Joint Cyber Unit, die die Kooperation zwischen dem Nachrichtendienst und den Streitkräften im Bereich der Cybersicherheit verstetigte. Zusätzlich zu dieser Einheit beim GCHQ etablierten die Streitkräfte eine weitere, eigene Joint Cyber Unit in Corsham. Auf militärischer Seite wurde die Verantwortung beim neuen Joint Forces Command angesiedelt. Etwa 320 Millionen britische Pfund erhielt das GCHQ für den Aufbau weiterer Cyberkapazitäten. Mit den neuen Fähigkeiten sollten Angriffe abgeschreckt und abgewehrt werden (Cabinet Office, 2011, S. 26f.).

Dieser Schritt wurde mit der wachsenden Verwundbarkeit und der gestiegenen Zahl immer komplexerer Angriffe gerechtfertigt. Mit Blick auf internationale Konflikte konstatierte die Regierung: »In times of conflict, vulnerabilities in cyberspace could be exploited by an enemy to reduce our military's technological advantage, or to reach past it to attack our critical infrastructure at home« (ebd., S. 15). Auch ein terroristischer Angriff auf kritische Infrastrukturen wurde in diesem Zusammenhang als potenzielles Risiko debattiert. Dies alles vollziehe sich in einem grenzenlosen Raum, in dem die Attribution von Angriffen und die Unterscheidung zwischen Gegnern schwierig sei. Der Cyberspace war aus Sicht der Regierung zu einem neuen Raum geworden, in dem auch entscheidende militärische Vorteile gewonnen werden könnten. Das Bestreben einiger Staaten, Angriffe

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

abstreitbar durchzuführen berge hierbei besonders große Risiken (ebd., S. 15 bzw. 17). Für das Vereinigte Königreich sei es daher notwendig, proaktiv im Cyberspace zu agieren und diesen für die eigene Sicherheitspolitik besser zu nutzen. Dies stimme auch mit den Vorgaben des neuen Strategischen Konzepts der NATO überein (ebd., S. 26). Die Regierung war zu diesem Zeitpunkt der Auffassung, dass ein Cyberangriff auf kritische Infrastrukturen verheerende Folgen nach sich ziehen könnte. Ein Vertreter des Verteidigungsministeriums verglich Cyberoperationen mit kinetischen Folgen mit dem Einsatz von Marschflugkörpern. Mit Blick auf die Kontrolle der neuen Kapazitäten betonte die Regierung, ähnlich wie die deutsche, dass die neuen Möglichkeiten durch die etablierten Regeln nationalen und internationalen Rechts reguliert werden sollten (UK Government, 2011).

Innerhalb kurzer Zeit rückte damit, begünstigt durch den Wechsel der RollenträgerInnen in der Exekutive sowie durch den Verweis auf die Aktivitäten anderer Staaten und die Folgen von Cyberangriffen, die offensive Ausrichtung der Beschützer-Rolle in den Vordergrund.

Ebenfalls 2011 wurde in britischen Medien darüber berichtet, dass die Regierung damit begonnen habe, die Fähigkeit zu Cyberangriffen auszubauen. Der Parlamentarische Staatssekretär im Verteidigungsministerium Nick Harvey gab gegenüber dem Guardian an, dass Cyberoperationen zu einem wichtigen Bestandteil des militärischen Arsenals geworden wären. Sorgen, dass diese Militarisierung des Netzes einen aggressiveren Einsatz dieser Kapazitäten zur Folge haben könnte, teilte er nicht:

> »I don't think that the existence of a new domain will, in itself, make us any more offensive than we are in any other domain. The legal conventions within which we operate are quite mature and well established.« (The Guardian, 2011)

Auch wenn die Unterscheidung zwischen Krieg und Frieden aus Sicht der britischen Regierung im Netz schwieriger wurde, sollte das nicht zu einem offensiveren Einsatz der entsprechenden Beschützer-Rolle führen.

Die Verantwortung für die Entwicklung der neuen Fähigkeiten wurde wiederum dem GCHQ übertragen, politisch war das Cabinet Office zuständig. Das Verteidigungsministerium sollte den Prozess begleiten und die militärischen Anforderungen einbringen. Harvey führte aus, dass der Westen seine Technologieführerschaft nicht als garantiert betrachten sollte und dass Staaten wie China vehement an der Modernisierung ihrer Streitkräfte arbeiteten (ebd.).

Diesen Aussagen folgend, verkündete der Verteidigungsminister im September 2013 öffentlich, dass Großbritannien »a full-spectrum military cyber capability, including a strike capability« aufbaue (UK Government, 2013a). Dabei würde auch auf die Expertise von ReservistInnen zurückgegriffen. Die britische Regierung war damit die erste, die die Entwicklung eines offensiven Cyberarse-

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

nals ankündigte (Financial Times, 2013). Im Dezember 2013 legte das Verteidigungsministerium ein erstes Strategiedokument vor, das sich ausschließlich mit militärischen Aspekten der Cybersicherheit befasste. Nachdem die Aufgabe des Militärs, ähnlich wie in Deutschland, zuvor primär im Schutz militärischer IT-Infrastruktur gesehen wurde, wies der Verteidigungsminister im Vorwort darauf hin, dass dies nicht mehr ausreiche:

> »Cyber is the new frontier of defence. For years, we have been building a defensive capability to protect ourselves against these cyber attacks. That is no longer enough. You deter people by having an offensive capability.« (Ministry of Defence, 2013, S. iii)

Die größte Gefahr für folgenschwere und komplexe Cyberangriffe ging zu diesem Zeitpunkt aus Sicht der Regierung von anderen Staaten aus, die mit ihren Fähigkeiten wirtschaftliche aber auch militärische Ziele verfolgten (ebd., S. 1-9). Eine Definition offensiver Maßnahmen oder wie diese eingesetzt werden könnten, beinhaltete dieses Dokument allerdings nicht. Betont wurde lediglich, dass der Einsatz den tradierten Vorgaben des Kriegsvölkerrechts entsprechen müssten (ebd., S. 1-24).

Die öffentliche Ankündigung, Cyberangriffskapazitäten aufzubauen, wurde in der Folge auch im Parlament diskutiert. Die Opposition sprach sich nicht prinzipiell gegen den Aufbau aus, forderte von der Regierung aber, eine klare Einsatzdoktrin vorzulegen. Ein gänzlich klandestines Vorgehen berge das Risiko, dass Maßnahmen als illegitim wahrgenommen würden. Außerdem wurde kritisiert, dass die parlamentarische Kontrolle der Exekutive im Bereich verdeckter Operationen nicht ausreichend sei. Die Zuständigkeit des ISC sei in diesem Kontext noch nicht definiert (House of Commons, 2014a, S. 794f., 816f.). Ferner ging es darum, deutlich zu machen, dass Maßnahmen stets verhältnismäßig seien:

> »Proportionality is at the gutes of the whole business of international law, human rights and legitimacy. We have to show that proportionality is there and that we have mechanisms and systems to ensure that it is. Simply claiming that it is there will not be good enough.« (Ebd., S. 795)

Die meisten Abgeordneten teilten aber die Einschätzung, dass die Regierung in diesem Bereich aktiv werden müsse, da das Gefahrenpotenzial durch die wachsende Vernetzung stark gestiegen sei. Ein Cyberangriff könne die wirtschaftliche Prosperität nachhaltig beschädigen und im Extremfall sogar zum partiellen Zusammenbruch der Gesellschaft führen (ebd., S. 796f. ebenso 806, 809, 812–815).

Ferner begrüßten Abgeordnete, dass Cyberangriffe zur Erreichung militärischer Ziele genutzt werden könnten, ohne dabei das Leben britischer Soldaten

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

zu riskieren (ebd., S. 796f.). Aus Sicht der Regierungsabgeordneten waren Cyberkapazitäten zu einem »battle-winning asset« geworden (ebd., S. 804). Das Parlament erwarte daher, dass die Exekutive die entsprechenden Fähigkeiten aufbaue. Russland, China, Nordkorea, Iran und Syrien seien bislang durch Cyberangriffe aufgefallen, die sowohl Regierungen als auch Unternehmen getroffen hätten. Die Exekutive könne diesem Trend nicht tatenlos begegnen (ebd., S. 805, 811).

Um die parlamentarische Kontrolle der neuen Fähigkeiten zu gewährleisten, legte die Regierung Ende 2014 in einem erneuerten Memorandum of Understanding mit dem Intelligence and Security Committee fest, dass das ISC auch mit der Kontrolle offensiver Cybermaßnahmen betraut sein sollte (Intelligence and Security Committee, 2014a, S. 12).

Die Entscheidung, kein eigenständiges Kommando für den Cyberspace zu etablieren, wie bspw. die USA, wurde vereinzelt kritisiert (House of Commons, 2014a, S. 814). Dies liegt maßgeblich darin begründet, dass das Militär eng mit dem GCHQ kooperiert und dass bspw. beim Kampf gegen den Islamischen Staat Cyberangriffe durch den Nachrichtendienst ausgeführt wurden. Die Regierung institutionalisierte die Kooperation zwischen Verteidigungsministerium und GCHQ 2014 in einem National Offensive Cyber Programme (NOCP) (The Times, 2018b). Die Regierung verwies darauf, dass sich diese Zusammenarbeit historisch bewährt habe und auch im Cyberspace erfolgreich sein werde (The Telegraph, 2018).

Die offensive Referenz (Schutz vor wem?) der Beschützer-Rolle wurde mit Verweis auf verschiedene Staaten konkretisiert und deren Notwendigkeit unterstrichen. Kontestationen aus dem Parlament bezogen sich auf die Kontrolle der neuen Fähigkeiten durch das ISC. Dieser Forderung kam die Regierung zügig nach und räumte dem ISC die Zuständigkeit ein. Damit wurde auch aus Sicht vieler Abgeordneter ein wichtiger Schritt zur Wahrung der Rolle als Garant liberaler Grundrechte vollzogen. Bei der konkreten Ausgestaltung des Programms zum Aufbau der Kapazitäten konnte die Regierung wiederum auf historische Erfolge der Streitkräfte und des Nachrichtendienstes hinweisen.

Bereits bei ersten parlamentarischen Fragen danach, wer im Ernstfall digitale Gegenmaßnahmen gegen einen Angriff ergreifen sollte, verwies die Regierung 2014 auf das GCHQ. Nach Analyse im Cyber Security Operations Centre und Rücksprache mit dem Cabinet Office, sollte der Nachrichtendienst ggf. die Reaktionen durchführen (House of Commons, 2013a, S. 41-43). In Anhörungen wurden von VertreterInnen der Streitkräfte darauf hingewiesen, dass Cyberangriffe ein potentes Mittel zu Erreichung militärischer Ziele sein könnten, dass für einen effizienten Angriff aber genaues Wissen über die Ziele vorhanden sein müsse, die daher vorher ausgespäht werden müssten. Ein schneller Gegenschlag könne daher schwierig sein, wenn nicht bereits zuvor in die Systeme eingegriffen wurde (ebd., Ev 14f.). In der Folge verlangten die Abgeordneten des Verteidigungsaus-

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

schusses von der Regierung eine klarere Positionierung darüber, unter welchen Bedingungen diese Fähigkeiten genutzt werden sollten:

> »There is clearly still much work to be done on determining what type or extent of cyber attack would warrant a military response. Development of capabilities needs to be accompanied by the urgent development of supporting concepts. We are concerned that the then Minister's responses to us betray complacency on this point and a failure to think through some extremely complicated and important issues.« (Ebd., S. 4)

Die Abgeordneten erkannten an, dass Cyberangriffe eine Möglichkeit darstellten militärische Operationen auszuführen, ohne dabei das Leben britischer Soldaten zu gefährden. Die Regierung müsse aber klarstellen, wie diese neue Fähigkeit genutzt werden solle. Außerdem wiesen die Mitglieder des Verteidigungsausschusses darauf hin, dass der Einsatz offensiver Cyberfähigkeiten problematisch werden könne, wenn es um die Abwägung der Verhältnismäßigkeit sowie die sichere Attribution der Angriffe gehe (House of Commons, 2014b, S. 41f.).

Die Regierung beantwortete Fragen nach dem Einsatz nicht direkt, sondern verwies darauf, dass Reaktionen im Einzelfall geprüft werden müssten. So sollte ein Ermessensspielraum gewahrt werden, der auch abschreckend wirken könne. Gegenmaßnahmen erfolgten aber immer unter Vorgaben des Kriegsvölkerrechts (House of Commons, 2013b, S. 7f.).

Bürgerrechtsorganisationen kritisierten den Aufbau militärischer Kapazitäten als eine unangemessene Militarisierung des Netzes, die zu erheblichen Kollateralschäden führen könnte. Ferner sei es bedenklich, dass die offensiven Kapazitäten klandestin entwickelt würden und sich so weitgehend parlamentarischer Kontrolle entzögen (Open Rights Group, 2016a, S. 1, 5).

Diese Kontestation blieb allerdings folgenlos, da sie auch vom Parlament nicht geteilt wurde. Bis Ende 2014 hatte die britische Regierung damit offensive Kapazitäten aufgebaut und dies auch öffentlich eingeräumt. Ermöglicht wurde dies, durch die Referenz (Schutz vor wem?) zu feindlichen Staaten sowie Terrororganisationen und Verweise auf potenzielle physische Folgen von Cyberangriffen. Mit dem Bezug zu Russland wurde die Referenz der Beschützer-Rolle ab 2015 weiter konkretisiert.

6.2.2 Einsatz der offensiven Kapazitäten und Russland als neuer Referenzpunkt

Die Notwendigkeit verstärkt auch offensiv im Cyberspace tätig zu werden, wurde 2015 von den Streitkräften unter Verweis auf die Verschränkung konventioneller und digitaler Maßnahmen durch Russland in Estland, Georgien und der Ukraine gerechtfertigt. Diese neue Situation lasse eine klare Unterscheidung zwischen

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

Krieg und Frieden nicht mehr zu (Ministry of Defence, 2015). Einen Monat nach diesen Aussagen wurde die Verantwortlichkeit für folgenschwere Cyberangriffe vom Cabinet Office auf das Verteidigungsministerium übertragen (House of Commons, 2015c, S. 650).

Die Mitglieder des Verteidigungsausschusses forderten im November 2015 von der Regierung, angesichts der russischen Cyberaktivitäten flexibel auf Angriffe zu reagieren und neue Konzepte zu entwickeln, da eine konventionelle Vergeltungsdrohung für Cyberangriffe, die zumeist keine kinetischen Folgen hätten, wenig glaubhaft sei. Russland habe seine feindseligen Absichten durch Angriffe auf Estland, Georgien, die Ukraine, Deutschland sowie den französischen Fernsehsender TV5 Monde deutlich gemacht (House of Commons, 2015a, S. 12f.). Die Aktivitäten zielten dabei stets darauf, unterhalb der Schwelle eines bewaffneten Angriffs zu bleiben und so auch Artikel 5 des Transatlantikvertrages zu unterlaufen bzw. dessen Anwendbarkeit infrage zu stellen (House of Commons, 2016e, S. 18, 26).

Im Gegensatz zu Deutschland, wo die Absenkung der militärischen Einsatzschwelle auch durch den Bundestag besonders kritisch gesehen wird, unterstützten in Großbritannien viele Abgeordnete ein flexibles digitales, notfalls auch militärisches, Vorgehen.

Auf die neuen offensiven Kapazitäten sowie deren Einsatz ging George Osborne ebenfalls im November 2015 in einer Rede vor MitarbeiterInnen des GCHQ ein. Er verknüpfte hierbei ausdrücklich die nationale und ökonomische Sicherheit: »[…] there will be no economic security for our country without national security. Nowhere is that more true than when it comes to cyber« (UK Government, 2015a). Osborne wies darauf hin, dass mit der gestiegenen Vernetzung und der wachsenden NutzerInnenschaft des Netzes das ursprüngliche vertrauensvolle Verhältnis zwischen den NutzerInnen nicht mehr bestünde. Dies werde durch die Aktivitäten feindlicher Staaten oder Terrororganisationen immer deutlicher. Mit Blick auf die Verantwortung für die Sicherheit des Vereinigten Königreichs, sei es für die Regierung unerlässlich offensive Cyberfähigkeiten zu entwickeln und vorzuhalten, da durch Cyberangriffe mittlerweile auch Menschenleben in Gefahr seien. Die Regierung nehme diese Verantwortung sehr ernst und begegne damit den immer ausgefeilteren Angriffen. Terrorgruppen seien zwar noch nicht in der Lage verheerende Angriffe gegen kritische Infrastrukturen durchzuführen, strebten diese Fähigkeit aber an. Nur die Regierung sei in der Lage, Schutz gegen diese besonders komplexen Angriffe zu gewähren. Der Cyberspace stelle aber einen Raum dar, in dem Angriff stets einfacher sei als Verteidigung. Daher sei es notwendig ein Abschreckungspotenzial aufzubauen. Hierzu gehöre es, ein möglichst schwer zu treffendes Ziel zu sein, Normen für Cyberangriffe zu entwickeln – bspw. die staatliche Sorgfaltsverantwortung – sowie im Ernstfall dazu in der Lage zu sein, zurückzuschlagen (ebd.).

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

> »We reserve the right to respond to a cyber attack in any way that we choose. And we are ensuring that we have at our disposal the tools and capabilities we need to respond as we need to protect this nation, in cyberspace just as in the physical realm. We are building our own offensive cyber capability – a dedicated ability to counter-attack in cyberspace.« (UK Government, 2015a)

Bei der Entwicklung dieser Fähigkeiten wurde weiterhin auf die Expertise des Verteidigungsministeriums und des GCHQs zurückgegriffen, um zu den besten Ergebnissen zu gelangen. Diese Kapazitäten seien für die Kriegführung im 21. Jahrhundert essenziell (ebd.).

Im Juli 2016 veröffentlichte das Verteidigungsministerium die zweite Auflage des sogenannten Cyber Primer in dem weitere militärische Aspekte der Cybersicherheitspolitik debattiert wurden. Fehlte in der vorangegangenen Auflage noch eine Definition offensiver Cyberoperationen, wurden diese nun erstmals beschrieben:

> »Offensive cyber operations include activities that project force to create, deny, disrupt, degrade and destroy effects in and through cyberspace. These operations may transcend the virtual domain into effects in the physical and cognitive domains.« (Ministry of Defence, 2016a, S. 54)

Die Cyberkapazitäten dienten dabei im Wesentlichen der Konfliktprävention, dem Schutz des Vereinigten Königreichs sowie dem Anspruch, schnell überall auf der Welt Einfluss nehmen zu können. So könnten Cyberangriffe dazu genutzt werden, Ziele zu erreichen die sonst nicht angreifbar wären, ohne eine massive Eskalation nach sich zu ziehen. Als Beispiel hierfür verwies die Regierung auf Stuxnet (ebd., S. 2 bzw. 65).

Die Fähigkeit zur digitalen Abschreckung wurde auch in der Cyber Security Strategy 2016 hervorgehoben. Angreifer müssten damit rechnen, dass die britische Regierung offensive Maßnahmen zur Abwehr von Cyberangriffen anwende (UK Government, 2016f, S. 9f.). Besonders besorgniserregend war aus Sicht der Regierung, dass es eine kleine aber wachsende Anzahl feindlicher Staaten gäbe, die auch destruktive Cyberangriffe entwickelten. Dies stelle eine neue Qualität in der Gefahrenlage dar:

> »[…] a small number of hostile foreign threat actors have developed and deployed offensive cyber capabilities, including destructive ones. These capabilities threaten the security of the UK's critical national infrastructure and industrial control systems. Some states may use these capabilities in contravention of international law in the belief that they can do so with relative impunity, encouraging others to follow suit.« (Ebd., S. 18)

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

Zur Illustration eines solchen Szenarios verwies die Regierung auf den Angriff auf ukrainische Energieversorger im Dezember 2015, durch den ein Stromausfall ausgelöst wurde, von dem etwa 220.000 BürgerInnen betroffen waren (ebd., S. 21). Die technischen Fähigkeiten von Terrororganisationen reichten nach Einschätzung der Exekutive noch nicht aus, um folgenschwere Angriffe gegen kritische Infrastrukturen durchzuführen (ebd., S. 50). Es sei daher die wichtigste Aufgabe der Administration, das Vereinigte Königreich vor den Angriffen feindlicher Staaten zu schützen, da deren Angriffe die nationale Sicherheit, politische Stabilität sowie wirtschaftliche Leistungsfähigkeit unterminieren könnten. Das NOCP und die Kooperation zwischen GCHQ und Streitkräften sollten daher ausgebaut werden. Weiterhin verfolgte die Regierung das Ziel, das Verhalten von Staaten durch eine offensive Attributionspraxis zu beeinflussen und so nicht-normkonformes Verhalten öffentlich anzuprangern (ebd., S. 26 bzw. 49-51).

Die offensiven Fähigkeiten wurden bei der Vorstellung der neuen Strategie dann direkt mit den Fähigkeiten zur Attribution verknüpft »because the ability to detect, trace and retaliate in kind is likely to be the best deterrent« (UK Government, 2016a). Würde das Vereinigte Königreich auf den Aufbau offensiver Kapazitäten verzichten, bliebe im Ernstfall nur die Wahl, entweder gar nicht zu reagieren oder konventionell zu vergelten. Da aus Sicht der Regierung zwischenstaatlichen Spannungen zukünftig immer Cyberangriffe zur Unterminierung der Verteidigungsfähigkeit vorausgehen würden, wäre der Verzicht auf Vergeltung durch Cyberangriffe unverantwortlich (ebd.).

Eine flexible militärische Beschützer-Rolle war damit sowohl aus Sicht des Parlaments als auch der Regierung essenziell, da die AngreiferInnen gezielt niedrigschwellige Operationen durchführten, die sonst nicht angemessen vergolten werden könnten. Die Aktivitäten Russlands dienten hierzu als mahnendes Beispiel.

Aus Sicht des Verteidigungsministeriums stellte der Cyberspace, den wegweisenden neuen Handlungsraum des 21. Jahrhunderts dar und damit die Nachfolge des Luftraums. Es sei nur eine Frage der Zeit, bis Großbritannien den ersten folgenschweren Cyberangriff erlebe, da eine Vielzahl verschiedener Akteure offensive Fähigkeiten entwickle. Daher sei es wichtig, offensiv handlungsfähig zu sein: »It is important that our adversaries know there is a price to pay if they use cyber weapons against us, and that we have the capability to project power in cyberspace as in other domains« (Ministry of Defence, 2016b).

Gegenüber dem ISC führten VertreterInnen des GCHQ aus, dass im Rahmen des NOCP verschiedene Fähigkeiten aufgebaut würden. Dies umfasse auch Angriffsoptionen mit schwerwiegenden Folgen, die gegen Staaten eingesetzt werden könnten, möglicherweise aber nie zum Einsatz kämen. Primärer Effekt sollte die Abschreckung potenzieller Angreifer sein. Mit Blick auf den Einsatz von Cyberangriffen führten VertreterInnen des GCHQ aus, dass offensive Cyberoperatio-

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

nen den gleichen rechtlichen Anforderungen unterlägen wie konventionelle militärische Einsätze. Die Abgeordneten stimmten den Einschätzungen des GCHQ weitgehend zu und befürworteten auch den Aufbau offensiver Kapazitäten (Intelligence and Security Committee, 2017, S. 44f.). Sachverständige hatten weiterhin die unklare parlamentarische Kontrolle der offensiven Fähigkeiten bemängelt. Um die Aufsicht zu verbessern, sollte das ISC aus Sicht der ExpertInnen unter anderem personell gestärkt und (auch schon vor Operationsbeginn) detaillierter unterrichtet werden (International Centre for Security Analysis, 2017, S. 3f. bzw. 6f.).

Aus Sicht der Abgeordneten waren die Bestrebungen der Regierung mit Blick auf die Aktivitäten Russlands aber nachvollziehbar, da bspw. Angriffe im Zusammenhang mit den amerikanischen Präsidentschaftswahlen dafür sprächen, dass die bisherige Zurückhaltung staatlicher Akteure zunehmend erodiere. Es sei daher für die Sicherheit unerlässlich gegen derartige Angriffe vorzugehen, weil auch Großbritannien zum Ziel von Angriffen werden könne. In diesem Kontext begrüßten die Abgeordneten ausdrücklich das Angebot des GCHQ Parteien und Abgeordneten bei der Sicherung ihrer Kommunikation zu unterstützen (Intelligence and Security Committee, 2017, S. 31-34).

Auf internationaler Ebene wies die britische Regierung auf drei Entwicklungen hin, die aus ihrer Sicht besonders besorgniserregend waren. Erstens nehme die staatliche Nutzung von Proxies zur Ausführung von Cyberangriffen zu. Zweitens nutzten Staaten Cyberangriffe immer häufiger in Verbindung mit anderen Mitteln des Konfliktaustrages. Dies würde drittens besonders häufig zur Destabilisierung von anderen Staaten eingesetzt und bleibe stets unterhalb der Schwelle eines bewaffneten Angriffs (Foreign & Commonwealth Office, 2017, S. 3).

Die Notwendigkeit im Cyberspace schlagkräftig zu sein, wurde von VertreterInnen der Regierung daher unter Verweis auf derartige staatliche Aktivitäten begründet. Nach der Vergiftung von Sergei Skripal im März 2018 in Salisbury verwies der Direktor des GCHQ explizit auf die Aktivitäten Russlands im Cyberspace:

> »For decades, we have collected intelligence on Russian state capabilities, on their intent and on their posture. And for over twenty years, we've monitored and countered the growing cyber threat they pose to the UK and our allies. […] We'll continue to expose Russia's unacceptable cyber behaviour, so they're held accountable for what they do.« (GCHQ, 2018c)

Mit Blick auf die russischen Aktivitäten konstatierte Fleming, dass die Maßnahmen die Distinktion zwischen Kriminalität und staatlichem Handeln zunehmend verwischten. Insbesondere wies er auf den Einsatz von NotPetya gegen Banken, Energieversorger und staatliche Einrichtungen in der Ukraine hin. Die Operationen Nordkoreas seien ein weiterer Beleg dafür, dass feindliche Staaten den

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

Cyberspace maßgeblich für ihre Belange einsetzten, WannaCry stehe beispielhaft hierfür. Das GCHQ arbeite daher auch weiterhin eng mit dem Verteidigungsministerium zusammen, um die eigenen Kapazitäten sukzessive zu erweitern (ebd.).

Die Sicht der britischen Regierung auf das Völkerrecht und den Einsatz von Cyberangriffen skizzierte Jeremy Wright im Mai 2018. Hierbei machte er deutlich, dass ein Cyberangriff unter der Schwelle eines bewaffneten Angriffs nicht illegitim sei und auch das staatliche Souveränitätsprinzip (Artikel 2(7)) nicht notwendigerweise verletze.

> »Some have sought to argue for the existence of a cyber specific rule of a ›violation of territorial sovereignty‹ in relation to interference in the computer networks of another state without its consent. […] Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.« (UK Government, 2018b)

Diese Interpretation deckt auch die Praxis offensiven nachrichtendienstlichen Hackens, wie sie von Großbritannien praktiziert wird. Eine illegale Intervention liegt aus Sicht der britischen Regierung erst dann vor, wenn Staaten nicht mehr »free from external, coercive intervention in the matters of government« seien, sie also bspw. bei politischen Wahlen beeinflusst würden (ebd.).[6]

Außerdem betonte Wright die staatliche Sorgfaltsverantwortung für Angriffe auch von »individuals acting under its instruction, direction or control« (ebd.). Dieser Verantwortung könnten sich Staaten nicht durch die Nutzung von Proxies entziehen. Die Regierung verfolge daher die Praxis, Cyberangriffe öffentlich zu attribuieren, sofern sie dies für zielführend erachte, um regelgeleitetes Verhalten im Cyberspace zu fördern. Wright verwies in diesem Zusammenhang explizit auf den Wurm WannaCry, der das britische NHS substanziell beeinträchtigt hatte sowie auf die Ransomware NotPetya. Die britische Regierung forderte andere Staaten auf, sich diesen Bemühungen anzuschließen, um die Glaubwürdigkeit der Zuschreibungen zu erhöhen (ebd.). Die Regierung hatte bereits im Dezember 2017 offiziell die Lazarus Group bzw. Nordkorea für WannaCry verantwortlich gemacht. Aus Sicht der Exekutive nutzte das Regime in Pjöngjang Cyberangriffe, um Sanktionen zu umgehen. Ein Vertreter des britischen Außenministeriums

6 Diese Bezugnahme ist auch Ergebnis der britischen Erfahrungen während des Referendums zum Austritt aus der Europäischen Union. In diesem Kontext gab es den Verdacht, Russland habe die Abstimmung zu manipulieren versucht (The Guardian, 2019a; The New York Times, 2017).

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

betonte, dass dieses Verhalten inakzeptabel sei und dass die nordkoreanische Regierung dafür mit Gegenmaßnahmen zu rechnen habe (UK Government, 2017a).

Die britische Regierung vertrat ferner die Ansicht, dass auf einen Cyberangriff nicht in gleicher Weise reagiert werden müsse, sondern, dass alle Maßnahmen zulässig seien, die notwendig und verhältnismäßig seien (UK Government, 2018b). Das Risiko eines durch militärische Offensivkapazitäten geprägten Cyberspace, sah die britische Regierung nicht. Vielmehr betonte sie, dass es das Recht eines jeden Staates sei, solche Fähigkeiten aufzubauen, da die Staaten bei deren Einsatz an das Völkerrecht gebunden seien. Wright illustrierte dies am Beispiel eines Angriffs auf zivile Flugleitsysteme, der egal mit welchen Mitteln er ausgeführt würde, einen klaren Bruch des Völkerrechts darstelle. Genauso verhalte es sich bei Angriffen auf medizinische Einrichtungen. Legitim seien aber Angriffe im Rahmen bewaffneter Auseinandersetzungen wie bspw. gegen Terrororganisationen, um deren Kampffähigkeit zu beeinträchtigen (ebd.).

Wie die deutsche Regierung erkannte auch die britische Exekutive keine wesentlichen Regulierungslücken im internationalen Recht.

Der Ankündigung, Cyberangriffe künftig häufiger öffentlich zu attribuieren, folgten noch im gleichen Jahr mehrere Zuschreibungen. Im März hatte die US Regierung eine Gruppe iranischer HackerInnen beschuldigt, unter anderem Angriffe gegen Universitäten durchgeführt zu haben. Die britische Regierung teilte diese Einschätzung und begrüßte das Vorgehen der US-Administration (UK Government, 2018a). Im September 2018 wies Premierministerin Theresa May auf die russischen Cyberaktivitäten unter anderem zur Beeinflussung von demokratischen Wahlen hin (House of Commons, 2018c, S. 169). Medienberichten zufolge, plante die Regierung nach der Vergiftung von Sergei Skripal in Salisbury Vergeltungsmaßnahmen im Cyberspace. Treffen sollten diese Angriffe den russischen Militärgeheimdienst GRU sowie assoziierte (kriminelle) Gruppen. Sie sollten darauf ausgerichtet sein, deren Operationsfähigkeit einzuschränken oder den Zugang zu Finanzmitteln zu begrenzen (The Times, 2018a). Im Parlament räumte die Premierministerin diese Möglichkeiten zumindest theoretisch ein (House of Commons, 2018a, S. 633). Der Direktor des GCHQ bezeichnete die Bedrohung durch Russland als sehr real. Um Russland in seinen Bestrebungen, die internationale Ordnung zu unterminieren, zu stoppen, müsse der Herausforderung mit unterschiedlichen Maßnahmen begegnet werden (GCHQ, 2018a).

Im Oktober 2018 gab das NCSC bekannt, dass nach Auffassung der britischen Sicherheitsbehörden der russische Militärgeheimdienst GRU für eine Reihe prominenter Cyberangriffe verantwortlich war, darunter Attacken zur Destabilisierung von Demokratien. Nach Einschätzung der britischen Regierung war der GRU unter verschiedenen Namen bekannt, darunter APT 28, Fancy Bear, Sofacy, Pawnstorm, Sednit, CyberCaliphate, Cyber Berkut, Voodoo Bear, BlackEnergy Ac-

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

tors, STRONTIUM, Tsar Team, Sandworm.[7] Die Angriffe verstießen aus Sicht des Außenministers offensichtlich gegen internationales Recht:

> »The GRU's actions are reckless and indiscriminate: they try to undermine and interfere in elections in other countries; they are even prepared to damage Russian companies and Russian citizens. This pattern of behaviour demonstrates their desire to operate without regard to international law or established norms and to do so with a feeling of impunity and without consequences. [...] Our message is clear: together with our allies, we will expose and respond to the GRU's attempts to undermine international stability.« (UK Government, 2018d)

Im Dezember 2018 gab die britische Regierung ferner bekannt, dass die Gruppe APT 10, die für zahlreiche Spionageangriffe verantwortlich gemacht wurde, für die chinesische Regierung arbeite bzw. sehr enge Verbindungen zum Ministerium für Staatssicherheit habe. Mit den Angriffen verstoße die chinesische Regierung in flagranter Weise gegen ein bilaterales Abkommen mit dem Vereinigten Königreich sowie gegen Ziele der G20, die den Diebstahl geistigen Eigentums verbieten (UK Government, 2018c). Für Angriffe gegen Georgien im Oktober 2019 machte der britische Außenminister wiederum den russischen Militärgeheimdienst GRU verantwortlich (UK Government, 2020).

Die offensive Attribution wurde damit auch durch die Rollen als Garant liberaler Grundrechte und Wohlstandsmaximierer ermöglicht, die die Gewährleistung demokratischer Wahlen und die wirtschaftliche Wettbewerbsfähigkeit beinhalten. Sie wirkten damit katalytisch auf den Ausbau der Beschützer-Rolle. Die Fähigkeit zur Attribution und zur Vergeltung im Cyberspace wurden ferner zu einem wesentlichen Teil der flexiblen militärischen Beschützer-Rolle im Cyberspace. Die Regierung folgte damit den Praktiken der vermeintlichen Angreifer und versuchte deren Operationen zu kontern.

International war die britische Regierung in diesem Zuge die erste, die 2018 der NATO offensive Cyberfähigkeiten angeboten hat (House of Commons, 2019, S. 1200).

Für die Jahre 2018-2020 wurden dem Verteidigungsministerium zusätzlich 1,8 Mrd. Pfund zur Verfügung gestellt, die für die Entwicklung offensiver Cybermaßnahmen sowie die Bekämpfung von U-Booten und das Nuklearwaffenarsenal vorgesehen wurden (Treasury, 2018, S. 76).

---

7 Die deutsche Regierung schloss sich der Einschätzung, dass die russische Regierung für die Angriffe (darunter der Bundestagshack 2015) verantwortlich sei, offiziell an. Zuvor wurde dies nur in deutschen Geheimdienstkreisen für sehr wahrscheinlich gehalten (Spiegel, 2018; Zeit, 2018).

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

Ebenfalls 2018 wurde öffentlich bekannt, dass im Kampf gegen Daesh in Kooperation zwischen GCHQ und den Streitkräften systematisch offensive Cyberoperationen durchgeführt worden waren. Diese hätten sowohl die Kommunikations- als auch Operationsfähigkeit der Terrororganisation substanziell unterminiert: »This is the first time the UK has systematically and persistently degraded an adversary's online efforts as part of a wider military campaign« (GCHQ, 2018c). In diesem Kontext sei eine ganze Reihe unterschiedlicher Angriffstechniken zum Einsatz gekommen. Die Attacken reichten dabei von der Blockade von Diensten, bis zur Zerstörung von technischem Equipment.[8] Aus Sicht des GCHQ waren die Maßnahmen dabei sehr erfolgreich. Jeremy Fleming betonte, dass die Angriffe stets im Rahmen der nationalen und internationalen rechtlichen Regelungen durchgeführt wurden und dass die demokratische Kontrolle der Operationen gewährleistet sei. KritikerInnen, die dies bestritten hatten, warf er vor, die Wertvorstellungen sowohl im Geheimdienst als auch bei den Streitkräften nicht verstanden zu haben (ebd.).

Um auch in Zukunft offensiv im Cyberspace aktiv sein zu können, bedürfe es eines kontinuierlichen Trainings der eigenen Kräfte. Dies geschehe im Vereinigten Königreich regelmäßig in der Kooperation zwischen dem Verteidigungsministerium und dem GCHQ. Nur auf diesem Weg ließe sich lernen, wie die eigenen Fähigkeiten im Ernstfall am besten eingesetzt werden sollten. Letztlich ging es darum, die Sicherheit des Vereinigten Königreichs zu gewährleisten, Daher sei es wichtig, »[..] to make the UK harder to attack, better organised to respond when we are, and able to push back if we must« (ebd.). Mit Blick auf die Gefahrenlage verwies die Regierung erneut auf die russischen Aktivitäten (Foreign & Commonwealth Office, 2019). Die besondere Bedeutung der Abschreckung, insbesondere gegenüber Russland, betonte im März 2019 auch Außenminister Jeremy Hunt. Er verwies in diesem Kontext explizit darauf, dass die westlichen Staaten die Kapazitäten aufbauen müssten, um ihre demokratischen Systeme vor externen Einflussnahmen zu schützen. Vergeltung müsse dabei nicht immer durch Cyberangriffe erfolgen, eine erfolgreiche Abschreckung müsse aber verschiedene Optionen glaubwürdig abdecken können (UK Government, 2019b).

Die enge Kooperation zwischen dem Nachrichtendienst und den Streitkräften wird in naher Zukunft weiter ausgebaut. Die britische Regierung hat angekündigt, eine neue National Cyber Force bestehend aus VertreterInnen des GCHQ und den Streitkräfte zu gründen (Ministry of Defence, 2019). Die neue Einheit soll offensive Cybermaßnahmen entwickeln und durchführen. Der Kommandeur des Joint Forces Command betonte, dass der Aufbau der neuen Kräfte für die

8 Medienberichten zufolge führte das GCHQ im Zusammenspiel mit Spezialkräften bspw. Angriffe auf Systeme von IS-Kommandeuren aus, um deren Kommunikation zu manipulieren und sie dann in Hinterhalte zu locken (Sky News, 2018).

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -

sicherheitspolitische Handlungsfähigkeit besonders wichtig sei: »By adopting offensive cyber techniques in the UK we are levelling the playing field and providing new means of both deterring and punishing states that wish to do us harm« (Sky News, 2018).

KritikerInnen bemängelten die geheime Natur der neuen Einheit und den fehlenden demokratischen Diskurs über den Einsatz von CNOs (The Guardian, 2020).

Neben der flexiblen militärischen Beschützer-Rolle, die durch die Maßnahmen hybrider Kriegführung Russlands ermöglicht wurde, hat die britische Regierung zudem die offensiven Kapazitäten zur Unterstützung militärischer Operationen ausgebaut und genutzt. Die Einsätze gegen den Islamischen Staat stehen exemplarisch hierfür.

6.3 Zwischenfazit

Beide Untersuchungsstaaten haben in den vergangenen 20 Jahren die militärischen Beschützer-Rollen ausgebaut und Kapazitäten zum offensiven Wirken in gegnerischen Netzen etabliert. Sowohl in der Bundesrepublik als auch in Großbritannien lag die Referenz (Schutz für wen?) der Rolle zunächst auf dem Schutz militärischer Infrastrukturen und verschob sich dann durch Bezugnahmen zur kritischen Infrastruktur zunehmend hin zur Landesverteidigung. Wie im Vereinigten Königreich wurde auch in Deutschland nach 2016 auf die Notwendigkeit des Schutzes des demokratischen Systems verwiesen, sodass der Ausbau der Beschützer-Rolle auch unter Verweis auf die Rolle als Garant liberaler Grundrechte begünstigt wurde.

Deutschland hat sich international früh für eine Kultur der Zurückhaltung im Cyberspace ausgesprochen. Im Rahmen der OSZE konnte die Bundesregierung erfolgreich für eine emergente Norm zum Nichtangriff von kritischen Infrastrukturen werben. Die Unterstützung einer Kultur der Zurückhaltung stand aber von Beginn an in einem Spannungsverhältnis zum Aufbau eigener CNO-Kräfte und der Etablierung der offensiven Beschützer-Rolle. Wie diese agieren sollten, ohne Schadsoftware zu entwickeln bzw. zu verwenden, blieb von Beginn an unklar. Auch die später von der Regierung entwickelte Einsatzdoktrin, die die Nutzung von Verschleierungstechniken zum verdeckten Operieren in gegnerischen Netzen vorsieht, konterkariert eine verifizierbare Kultur der Zurückhaltung. Mit Blick auf den Aufbau offensiver Kapazitäten hat die Regierung auf die besondere Präzision und die vergleichsweise geringen kinetischen Effekte von digitalen Maßnahmen verwiesen. Cyberangriffe sind aus dieser Perspektive ein besonders schonendes Mittel zur Erfüllung der militärischen Beschützer-Rolle, die sonst einen konventionellen Angriff nötig gemacht hätte. Die Etablierung des Kdo CIR wurde einer-

https://doi.org/10.14361/9783839460641-027 - am 13.02.2026, 08:41:15. https://www.inlibra.com/de/agb - Open Access -