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-

seits durch zunehmend ausgefeiltere Angriffe sowie andererseits durch Verweis auf die NATO-Partner ermöglicht, da die Bundesregierung die Kooperationsfähigkeit der deutschen Streitkräfte in diesem Gebiet verbessern wollte.

Die deutschen Bestrebungen zu einer insgesamt zurückhaltenden militärischen Nutzung des Netzes standen nicht nur in einem gewissen Spannungsverhältnis zum Aufbau eigener Kapazitäten, sie wurden auch international bspw. durch die britische Regierung herausgefordert, die sich früh gegen eine zu weitgehende Regulation militärischer Cyberkapazitäten stellte und als erste öffentlich die eigenen offensiven Kapazitäten bekanntgab. Die britische Regierung hat für sich stets in Anspruch genommen, alle Möglichkeiten nutzen zu können.

Beide Regierungen haben betont, dass für den Einsatz militärischer Cyberangriffe die gleichen Regelungen gelten sollten wie für konventionelle vergleichbare Einsätze des Militärs. In Deutschland hat die Bundesregierung dem Parlament versichert, dass ein konstitutives Mandat notwendig ist. In Großbritannien wurde das ISC mit der Kontrolle betraut. Mit Blick auf internationales Recht haben ebenfalls beide Regierungen darauf verwiesen, dass die völkerrechtlichen Vorgaben auch für den Einsatz von Cyberangriffen gelten. Sie haben in diesem Kontext ferner wiederholt das Prinzip der Sorgfaltsverantwortung betont und die Nutzung von Proxies verurteilt. Eine umfassende Kontrolle des Netzes zur Prüfung normkonformen Verhaltens wird aber durch die Rolle als Garant liberaler Grundrechte beschränkt.

Der Aufbau der Beschützer-Rolle wurde in beiden Staaten durch die Furcht vor folgenreichen Cyberangriffen und immer fähigeren AngreiferInnen begünstigt. Insbesondere nach Stuxnet wurde die Beschützer-Rolle durch Verweis auf diese Vulnerabilität gerechtfertigt. Beide Staaten waren in den letzten Jahren dann aber mit niedrigschwelligen Cyberangriffen staatlichen Ursprungs konfrontiert und haben hierauf unterschiedlich reagiert. Aufgrund der historischen Erfahrungen beim Einsatz der Streitkräfte, ist die Rolle der Bundeswehr jenseits der Landesverteidigung bzw. eines durch den Bundestag mandatierten Einsatzes nicht möglich. Debatten über einen niedrigschwelligeren Einsatz der Bundeswehr und einen neuen »Cyber-Verteidigungsfall« sind aufgrund verfassungsrechtlicher Bedenken und historischer Erfahrungen bislang ergebnislos geblieben. Außerdem ist die offensive Ausrichtung der Bundeswehr Kontestation auch aus dem Parlament ausgesetzt. Der deutschen Beschützer-Rolle fehlt eine klare Referenz (Schutz vor wem?) und Einsatzschwelle. Die Regierung scheint sich bisher noch nicht im Klaren darüber zu sein, ob bzw. wie sie die Kapazitäten angesichts niedrigschwelliger Angriffe verwenden soll und wie die Kompetenzen zwischen den unterschiedlichen Institutionen verteilt werden sollen. Die historisch gewachsene Ordnung der Beschützer-Rolle im deutschen Föderalismus sowie das Trennungsgebot stellen die Bundesregierung hier vor besondere Aufgaben.

In Großbritannien ist die militärische Beschützer-Rolle zwischen den Streitkräften und dem GCHQ geteilt. Dies wurde durch die positiven historischen Erfahrungen und den bereits im Bereich der Nachrichtendienste hervorgehobenen guten Ruf des GCHQs ermöglicht. Die britische Regierung hat im Rahmen dieser Kooperation Angriffstechniken entwickelt, die für folgenschwere Cyberangriffe genutzt werden können. Sie sieht diese Kapazitäten als Mittel zur Abschreckung. Um auf die niedrigschwelligen Angriffe verhältnismäßig zu reagieren, hat das GCHQ unterschiedliche Angriffsvarianten entwickelt. Die Referenz (Schutz vor wem?) der Rolle liegt mittlerweile auf Russland, das spätestens mit der Vergiftung von Sergei Skripal zu einem wesentlichen Referenzpunkt der Beschützer-Rolle wurde. Die britische Regierung hat die offensiven Kapazitäten aber auch zur Ergänzung des Einsatzes gegen den Islamischen Staat offensiv genutzt und sie so mit ihren konventionellen Fähigkeiten verschränkt.

Die wesentlichen Einflüsse, die die Entwicklung der Cybersicherheitspolitiken geprägt haben, sind in den Tabellen 7 und 8 schematisch dargestellt.

Tabelle 7: Schematische Darstellung der Einflüsse auf die Politikentwicklung im Bereich des Militärs in der Bundesrepublik Deutschland: Wirkung auf die Beschützer-Rolle, – = kontestierend, + = katalytisch. Quelle: Eigene Darstellung

	domestische Ebene				**internationale Ebene**	
	Historisches Selbst	Wirkung	Rollenbezüge	Wirkung	signifikante / organisierte Andere	Wirkung
Aufbau militärischer Kapazitäten (2000 - 2015)	Autokratische Erfahrungen	–			UN / OSZE / NATO	
(Schonende) Offensive und aktive Verteidigung (2015 - 2019)	Autokratische Erfahrungen	–	Garant liberaler Grundrechte	+	UN / NATO	+

Tabelle 8: Schematische Darstellung der Einflüsse auf die Politikentwicklung im Bereich des Militärs im Vereinigten Königreich: Wirkung auf die Beschützer-Rolle, – = kontestierend, + = katalytisch. Quelle: Eigene Darstellung

	domestische Ebene				**internationale Ebene**	
	Historisches Selbst	Wirkung	Rollenbezüge	Wirkung	signifikante / organisierte Andere	Wirkung
Aufbau militärischer Kapazitäten (2000 - 2015)	GCHQ, MoD	+			UN / NATO	
Einsatz der offensiven Kapazitäten (2015 - 2019)	GCHQ, MoD	+	Garant liberaler Grundrechte	+	UN / NATO / USA / RUS	+