> mament. After 9/11, Arabic language skills, as well as expertise on the Middle East, offered an entrée into foreign policy. Today, students of foreign affairs should understand how the internet works on a technical level and study the varied threats that fall under the broad umbrella of so-called cyber issues.« (Burns und Cohen, 2017)

WissenschaftlerInnen haben immer wieder auf die besondere Komplexität des Untersuchungsgegenstands hingewiesen und die Bedeutung interdisziplinärer Expertise betont (Kello, 2013; Segal, 2016). Der Forschungsgegenstand Cybersicherheit hat, aufgrund der politischen Implikationen, daher in den vergangenen Jahren vermehrt Aufmerksamkeit auch jenseits der Informatik gefunden. Um den politischen Umgang mit Problemen der IT-Sicherheit geht es auch in der vorliegenden Untersuchung der deutschen und britischen Cybersicherheitspolitiken.

1.1 Untersuchungsgegenstand und Relevanz

Wenn im Folgenden von Cybersicherheitspolitiken gesprochen wird, dann liegt dem ein enges, an die Informatik angelehntes, Verständnis von IT-Sicherheit zugrunde. Es basiert auf einer Definition, auf die sich die beiden Untersuchungsstaaten bereits 1991 in internationalem Austausch mit den Niederlanden und Frankreich verständigt haben. Danach umfasst die IT-Sicherheit die Gewährleistung der Vertraulichkeit, Integrität sowie Verfügbarkeit von Daten bzw. datenverarbeitenden IT-Systemen (DTI, 1991, S. 1).[6] Ausgehend von dieser Definition wird im Folgenden untersucht, inwiefern die beiden Untersuchungsstaaten Cybersicherheit zu sicherheitspolitischen Zwecken (offensiv) unterminieren bzw. welche Praktiken sie als illegitim betrachten.[7]

Der Fokus auf die offensiven Cybersicherheitspolitiken ist angebracht, da diese national wie international besonders umstritten sind und wissenschaftlich bisher vergleichsweise wenig Aufmerksamkeit erfahren haben. International konnte im Rahmen einer Group of Governmental Experts der UN (UN GGE) zwar Einigkeit darüber erzielt werden, dass völkerrechtliche Regelungen und insbesondere die Charta der Vereinten Nationen prinzipiell auf den Cyberspace übertragbar sind (United Nations, 2013b), was das konkret bedeutet, ist aber nach wie vor unklar. So scheiterte im Jahr 2017 die letzte UN GGE. Zentraler Streitpunkt war dabei

6 Diese drei Schutzziele werden anhand der englischen Anfangsbuchstaben (confidentiality, integrity and availability) meist als CIA-Triad bezeichnet (Andress, 2014, S. 5-9).

7 Da es in dieser Untersuchung um die Entwicklung der Cybersicherheit in diesem engen Kernverständnis geht, ist die mitunter erhebliche extensionale Erweiterung, die der Begriff erfahren hat (bspw. im Kontext der Verbreitung von Desinformation), nicht Teil der Analyse (Schünemann und Steiger, 2019).

offenbar die Bedeutung des Selbstverteidigungsrechts im Cyberspace (Henriksen, 2019). Aber nicht nur bei der militärischen Nutzung des Internets besteht Unsicherheit. Die Snowden-Enthüllungen haben ferner gezeigt, dass Cyberangriffe zur Informationsgewinnung auch gegen befreundete Staaten eingesetzt werden (Spiegel, 2014b). Im Bereich des Strafrechts konnte zwar relativ schnell geklärt werden, was als unangemessenes Verhalten gewertet werden soll. International konnten mit der Convention on Cybercrime im Rahmen des Europarates auch strafrechtliche Regelungen harmonisiert werden. Domestisch ist aber nach wie vor umstritten, wann und in welchem Umfang staatliche Ermittlungsbehörden IT-Sicherheit unterminieren sollten (Roggan, 2018).

Das Internet als sicherheitspolitischer Handlungsraum mit globaler Architektur und universellen Protokollen, die nicht primär auf Sicherheitserwägungen fußen (s. Kapitel 2.4.1), stellt staatliche Praktiken vor besondere Herausforderungen. Denn einerseits wird die Trennung zwischen innerer und äußerer Sicherheit im globalen Netz problematisch, da Pakete stets auch über Knoten im Ausland geleitet werden können und andererseits befinden sich zentrale Infrastrukturen nicht in staatlicher Hand. Gleichzeitig ist das Netz mittlerweile für das Funktionieren nahezu aller bedeutenden gesellschaftlichen Infrastrukturen in Industriestaaten essenziell. Verkehrsleitsysteme können ebenso digital gesteuert werden wie die Wasser- oder Energieversorgung. Das Internet ist damit nicht nur selbst zu einer zentralen gesellschaftlichen Infrastruktur geworden. Es ist vielmehr zu der Infrastruktur geworden, von deren Funktionieren zahlreiche andere Infrastrukturen abhängen: »the Internet has become a backbone of backbones« (Choucri, 2012, S. 151).

Eindrückliche Vorfälle in jüngerer Vergangenheit haben offengelegt, dass diese Verwundbarkeiten auch praktisch nutzbar sind bzw. bereits genutzt werden. In der Ukraine verursachte ein Cyberangriff im Dezember 2016 einen kurzfristigen Stromausfall von dem mehr als 200.000 BürgerInnen betroffen waren (Wired, 2016). Die rasche Verbreitung des Wurms WannaCry im Mai 2017 traf unter anderem das britische Gesundheitssystem (National Health System (NHS)) und hatte zur Folge, dass Krankenhäuser ihre PatientInnen nicht mehr planmäßig versorgen konnten (National Audit Office, 2018).[8]

8 WannaCry steht auch exemplarisch für die unintendierten Konsequenzen, die mit staatlichen Cybersicherheitspolitiken verbunden sein können. Die Malware beruht auf einer Sicherheitslücke im Betriebssystem Windows, die von der NSA EternalBlue getauft wurde. Aufgrund der potenziellen Nützlichkeit für offensive Cyberoperationen wurde die Lücke geheimgehalten. Allerdings verlor die NSA die Kontrolle über dieses Wissen und die Gruppe Shadow Brokers verbreitete die Informationen im Netz. Die NSA hatte Microsoft zwar kurz nach Bemerken des Datenlecks über die Lücke informiert und Microsoft veröffentlichte im März 2017 ein entsprechendes Update, da dieses von NutzerInnen aber nur langsam instal-

Ein Angriff auf das Netz und insbesondere kritische Infrastrukturen kann für Gesellschaften dabei potenziell verheerende (kaskadierende) Folgen haben. Diese neue Verwundbarkeit hat Hollywoodfilme wie Stirb Langsam 4.0 schon früh dazu inspiriert, den digitalen Knockout vernetzter Gesellschaften auszumalen und auch in der (populär)wissenschaftlichen Auseinandersetzung mit der Thematik wird immer wieder mit Szenarien folgenschwerer Cyberangriffe argumentiert. Auch wenn es empirisch noch keine Vorfälle mit derart gravierenden Effekten gegeben hat. In Anbetracht der bisher kinetisch zumeist folgenlosen Cyberangriffe ist ein beständiges Skizzieren von Worst-Case-Szenarien kritisch hinterfragt worden (Dunn Cavelty, 2013; Schünemann und Steiger, 2019).

Aber auch wenn sich Horrorszenarien von kinetisch folgenreichen Cyberangriffen bisher nicht realisiert haben, haben Regierungen die wachsende Angriffsfläche zum Anlass genommen neue regulatorische Maßnahmen zu ergreifen, um mit den Risiken im Cyberspace umzugehen. Das Netz und die mit ihm verbundene Perzeption neuer Herausforderungen hat dementsprechend seit Ende der 1990er Jahre zentrale Bedeutung in sicherheitspolitischen Dokumenten erlangt. Sichtbarer Ausdruck sind unter anderem die Cybersicherheitsstrategien, die mittlerweile von zahlreichen Industrienationen ausgearbeitet und implementiert wurden (Bundesministerium des Innern, 2011; Cabinet Office, 2009). Auch in Deutschland und Großbritannien[9] haben die Regierungen dieses Problem adressiert und neue Kapazitäten zur offensiven Nutzung des Netzes aufgebaut.

Die Lektüre dieser Dokumente zeigt, dass sich staatliche Sicherheitspolitik in diesem Feld mit unterschiedlichen Spannungen konfrontiert sieht. Einerseits sind die Regierungen daran interessiert, das Netz als Wirtschaftsraum und IT als Mittel der Effizienzsteigerung möglichst umfassend zu nutzen. Sie sind aus dieser Warte an einem sicheren Cyberspace interessiert, der den Wirtschaftssubjekten nicht durch Unsicherheit die Bereitschaft zur Investition oder zum Handeln allgemein nimmt. Ferner fördern demokratische Regierungen die Nutzung des Internets zur freien Verbreitung von Informationen oder zur vertraulichen Kommunikation. Andererseits sehen Regierungen im Netz aber auch ein Mittel, mit dem klassische sicherheitspolitische Ziele erreicht werden können. Hierzu ist es aber mitunter nötig, IT-Sicherheit zu unterminieren, bspw. dann, wenn es darum geht, Kriminelle abzuhören, nachrichtendienstliche Aufklärung zu betreiben oder die Infrastruktur gegnerischer Staaten im Konfliktfall zu unterminieren. Durch die Geheimhaltung und Nutzung von Sicherheitslücken wird der Staat so selbst zum Akteur, der IT-Unsicherheit schafft (Nissenbaum, 2005).

---

liert wurde, konnte WannaCry im Mai trotzdem viele Rechner, darunter die des NHS, infizieren und lahmlegen (The Washington Post, 2017).

9 Mit Großbritannien ist im Folgenden stets das Vereinigte Königreich Großbritannien und Nordirland gemeint.

Die Cybersicherheitspolitiken stehen damit potenziell in Spannung mit dem Erhalt bzw. der Förderung volkswirtschaftlichen Wohlstands und der Gewährleistung demokratischer Freiheitsrechte. Beim Einsatz zumeist klandestiner Cyberoperationen stellt sich ferner die Frage, wie Exekutiven demokratisch kontrolliert werden können. Als globaler Handlungsraum stellt der Cyberspace damit nicht nur die internationalen Beziehungen vor Herausforderungen, sondern auch die domestischen Verhältnisse zwischen Regierungen, Parlamenten, Judikativen, Unternehmen, VertreterInnen der Zivilgesellschaft sowie BürgerInnen. Die Analyse von Cybersicherheitspolitiken ist somit empirisch nicht nur aufgrund der zunehmenden Vernetzung, der damit einhergehenden gesellschaftlichen Verwundbarkeit und der Zunahme qualitativ hochwertiger Angriffe relevant, sondern auch, weil sie zentrale demokratische und wirtschaftliche Abwägungen erfordern und damit soziale Relationen domestisch wie international berühren.

Die Regierungen haben ihre Cybersicherheitspolitiken dabei in unterschiedlichen Handlungsfeldern definiert. Das Untersuchungsinteresse dieser Studie bezieht sich konkret auf die Politikentwicklung in drei zentralen Bereichen. Erstens auf den Kontext der Strafverfolgung. Zur Regulation krimineller Handlungen haben die Regierungen explizite Regelungen akzeptablen Verhaltens etabliert und diese in ihre nationalen Strafrechtsordnungen integriert. Teilweise wurden diese auch auf internationaler Ebene harmonisiert. Im Kontext der polizeilichen Ermittlungspraktiken haben die Exekutiven in diesem Zusammenhang aber auch selbst Maßnahmen ergriffen, die die IT-Sicherheit unterminieren. Diese Praktiken wurden in den Strafprozessordnungen kodifiziert. Zweitens auf den Bereich der Nachrichtendienste. Die Snowden-Enthüllungen 2013 haben gezeigt, dass auch Demokratien das Netz umfassend zur Informationsgewinnung im Ausland nutzen (Signals Intelligence). Internationale (Cyber)Spionage ist rechtlich jedoch nicht reguliert. Was als akzeptables staatliches Verhalten gilt, ist folglich nicht expliziert, sondern ggf. nur aus etablierten Praktiken internationalen Rechts ableitbar (Buchan, 2016, 2019). Drittens auf die militärische Nutzung des Netzes. Regierungen haben sukzessive damit begonnen, militärische Cyberkapazitäten aufzubauen (Lewis und Neuneck, 2013). Abgesehen vom Konsens, dass internationales Recht und insbesondere die Charta der Vereinten Nationen prinzipiell auf den Cyberspace übertragbar ist (United Nations, 2013b), ist jedoch auch in diesem Kontext, das staatliche Verhalten weitgehend unreguliert.

Die drei Untersuchungsbereiche zeichnen sich damit durch unterschiedliche Akteurskonstellationen und Regelungsarrangements aus. Sie betreffen auch in unterschiedlicher Weise die internationalen Beziehungen sowie das Verhältnis zwischen domestischen AkteurInnen.

Zudem ist die Untersuchung theoretisch relevant, da mit dem Netz als sicherheitspolitischem Handlungsfeld neue theoretische Herausforderungen verbunden sind. Zentrale Analysekonzepte der Internationalen Beziehungen (IB) sind po-

tenziell schwierig auf den Cyberspace übertragbar. Die analytischen Potenziale etablierter Theorien der IB werden durch den neuen Handlungsraum infrage gestellt. Die Einschätzungen darüber, inwiefern tradierte Konzepte der IB auf den Cyberspace übertragbar sind, divergieren dabei erheblich. Während einige ForscherInnen davon ausgehen, dass erprobte Konzepte weiterhin tragfähig sind (Craig und Valeriano, 2018; Reardon und Choucri, 2012), werden die analytischen Potenziale von anderen WissenschaftlerInnen skeptisch beurteilt (Diersch und Schmetz, 2017; Mayer, 2017). Letztere Einschätzung bezieht sich oft auf das unklare Verhältnis zwischen technischen Infrastrukturen und den sozial handelnden AkteurInnen. Diese Beziehung ist erst in den letzten Jahren von Studien aufgegriffen und ein technischer Determinismus problematisiert worden (Carr, 2016; Dunn Cavelty, 2018; McCarthy, 2015).[10]

Illustrieren lässt sich die Problematik der Übertragbarkeit von IB-Theorien an einer für den Neorealismus entscheidenden Debatte über die Bedeutung von Macht im Cyberspace. Welche Staaten im Cyberspace mächtig sind, ist schwieriger zu beurteilen als in der analogen Welt. Realistisch argumentierende WissenschaftlerInnen haben darauf hingewiesen, dass konventionell überlegene Staaten durch Cyberkapazitäten nur marginale Vorteile gegenüber anderen Staaten erzielen könnten. Insbesondere wenn diese weniger abhängig von IT seien. Demgegenüber könnten unterlegene Staaten durch den Aufbau von Cyberfähigkeiten auch stärkere herausfordern und ihre Position so relativ verbessern (Lindsay, 2013). Die konventionell überlegenen und auch im Cyberspace ressourcenstärksten Staaten könnten so aufgrund ihrer IT-Abhängigkeit doch die schwächeren sein. Die realweltliche Machtverteilung wäre dann digital zumindest partiell invertiert. Das Verhältnis zwischen Macht on- bzw. offline ist aber nach wie vor ungeklärt (Craig und Valeriano, 2018, S. 90). Die Machtkonstellationen im Cyberspace und potenzielle Wechselwirkungen mit anderen Machtressourcen (bspw. einem vernetzten Militär) sind unklar. Damit sind neorealistisch auch nur bedingt systemische Verhaltenserwartungen ableitbar.

Eine wissenschaftliche Auseinandersetzung mit dem Untersuchungsgegenstand ist daher nicht nur aufgrund der praktischen gesellschaftlichen Implikationen relevant. Er ist auch wissenschaftlich bedeutsam, um theoretisch angemessen mit Cybersicherheit umgehen zu können und ein besseres Verständnis zu ermöglichen.

10 Ein theoretisches Defizit, das in Kapitel 2.4 näher beleuchtet wird.