1. Einleitung

Die rasante globale Verbreitung des Internets[1] hat in den vergangenen 25 Jahren tiefgreifende wirtschaftliche sowie gesellschaftliche Veränderungen ermöglicht. Aus einem Netzwerk, das ursprünglich den militärischen sowie wissenschaftlichen Informationsaustausch sicherstellen bzw. erleichtern sollte, wurde nach der kommerziellen Öffnung zu Beginn der 1990er Jahre zunächst ein »Spielplatz« für Nerds und dann ein zentraler Wirtschaftsraum sowie ein Ort des kulturellen Austauschs. Heute gibt es in modernen Staaten kaum noch Lebensbereiche, die nicht von digitalen Technologien durchdrungen werden. BürgerInnen konsumieren und kommunizieren über globale Plattformen, die mit dem Internet neue Geschäftsmodelle erschlossen bzw. etablierte Unternehmenspraktiken auf den neuen Handlungsraum übertragen haben. Die nächste Entwicklungsstufe – das Internet of Things (IoT) – beginnt rasch Gestalt anzunehmen. Viele Gegenstände des täglichen Gebrauchs werden dann ebenso flächendeckend online sein, wie die Steuerungssysteme zentraler gesellschaftlicher Infrastrukturen. Die nächste industrielle Revolution, die durch die Vernetzung und die gezielte Nutzung erzeugter Daten effizientere Wirtschaftsprozesse ermöglicht, hat laut Ansicht einiger ExpertInnen bereits begonnen. Die Entwicklung künstlicher Intelligenz hat

1 Als Internet wird im Folgenden das mittels TCP/IP verbundene Netzwerk verschiedener (Teil-)Netze (Autonomer Systeme) bezeichnet. Dieser Zusammenschluss von Rechnern ermöglicht es theoretisch zwischen allen verbundenen Punkten Informationen in Form von Datenpaketen auszutauschen. Im Folgenden werden die Begriffe Internet, Netz und Cyberspace synonym verwendet. Es ist aber darauf hinzuweisen, dass der Begriff Cyberspace konzeptionell umfassender ist, da er auch jene digital vernetzten Geräte einschließt, die nicht mit dem Internet verbunden sind (air gap). Das Internet ist damit nur ein (großer) Teil des Cyberspace, der daneben noch zahllose weitere Netzwerke privater, wirtschaftlicher und staatlicher Akteure umfasst, die nicht mit dem Internet verbunden sind und damit auch nicht unmittelbar über das Internet erreicht und angegriffen werden können (Tabansky, 2011). Sofern nicht explizit darauf hingewiesen wird, ist im Folgenden auch mit der Bezeichnung Internet dieses weite Verständnis gemeint.

dabei das Potenzial den Arbeitsmarkt und damit die Gesellschaftsordnung der Zukunft nachhaltig zu verändern (Frey und Osborne, 2017).[2]

Das IoT droht aber auch zu einem sicherheitspolitischen Problem zu werden, da viele Geräte technisch schlecht gegen Angriffe geschützt sind. Eine Studie hat bspw. ein Szenario skizziert, in dem AngreiferInnen durch die Übernahme von besonders energieintensiven Geräten Verbrauchsschwankungen erzeugen und dadurch weitreichende Stromausfälle auslösen könnten (Soltan, Mittal und Poor, 2018). Das Mirai-Botnet[3] hat gezeigt, dass IoT-Geräte wie IP-Kameras oder Fernseher für Angriffe gekapert und missbraucht werden können. Mit einem großen DDoS-Angriff[4] legte das Botnet im Oktober 2016 einen zentralen DNS-Dienst[5] lahm und sorgte so dafür, dass große Teile des Internets für viele NutzerInnen nicht mehr erreichbar waren (Mansfield-Devine, 2016).

Das Internet ist im Zuge seiner sozialen Integration aber nicht erst mit dem Aufkommen des IoT zu einer Quelle gesellschaftlicher Unsicherheit und zum Medium des Konfliktaustrages geworden. Während in der Frühphase des Netzes Schadsoftware noch oft von individuellen AkteurInnen aus technischer Neugier oder zur Reputationssteigerung in einer relativ kleinen (Peer-)Gruppe von HackerInnen eingesetzt wurde, gehen aktuelle Schätzungen davon aus, dass (organisierte) Cyberkriminalität weltweit jährlich Schäden in Höhe von bis zu 600 Milliarden US-Dollar verursacht (McAfee und CSIS, 2018, S. 4). Die Geschäftsmodelle reichen dabei vom Handel mit illegalen Gütern wie Waffen oder Drogen im Darknet, über den massenhaften Versand von Spam- und (Spear)Phishingmails, bis zur Verbreitung von Erpressungstrojanern (Ransomware), die die Geräte der Opfer verschlüsseln und nur gegen Lösegeldzahlung wieder zugänglich machen.

---

2 Eine umfassende Vernetzung ist weder als wünschenswerter teleologischer Endpunkt der Entwicklung zu verstehen – derartige Tendenzen bleiben immer durch die AkteurInnen umkehrbar (möglicherweise unter Inkaufnahme erheblicher Opportunitätskosten) – noch als sich den AkteurInnen aufzwingender Prozess eines technischen Determinismus (s. dazu Kapitel 2.4).

3 Ein Botnet bezeichnet ein Netz von Rechnern, die von AngreiferInnen übernommen und zentral ferngesteuert werden. Meist handelt es sich hierbei um Rechner, die aufgrund veralteter Software angreifbar sind (Singer und Friedman, 2014, S. 44). Das Mirai-Botnet nutzte schlecht gesicherte IoT-Geräte, um Angriffe durchzuführen.

4 (D)DoS-Angriffe sorgen dafür, dass ein Zielsystem systematisch überlastet wird. Die Überlastung kann dabei auf verschiedene Ressourcen zielen bspw. die Rechenleistung oder die Internetanbindung. Ein Dienst ist in der Folge für NutzerInnen nicht mehr erreichbar.

5 Die Abkürzung DNS steht für Domain Name System und bezeichnet die Infrastruktur, die für die eindeutige Zuordnung zwischen maschinenlesbaren IP-Adressen und URLs benötigt wird (Singer und Friedman, 2014, S. 295). Der Ausfall eines DNS-Dienstes führt dazu, dass NutzerInnen Internetseiten nicht mehr erreichen können, da die Zuordnung zwischen URL und IP-Adresse nicht erfolgen kann.

Es sind aber nicht nur Kriminelle, die die neuen Verwundbarkeiten der digitalen Gesellschaft ausnutzen. Auch politische Konflikte finden Widerhall im Netz. Die Bandbreite angreifender AkteurInnen ist dabei ebenso zahl- und facettenreich wie die verschiedenen Angriffsmöglichkeiten. Politisch motivierte nichtstaatliche Hacktivists nutzen das Netz, um durch öffentlichkeitswirksame Aktionen, wie bspw. (D)DoS-Angriffe oder die Veröffentlichung gestohlener Dokumente (doxing), ein größeres Publikum auf ihre Anliegen aufmerksam zu machen (Karatzogianni, 2015; Sauter, 2014). Terrororganisationen greifen auf Cyberangriffe zurück, um bspw. Finanzmittel zu generieren oder propagandistische Botschaften zu verbreiten (Schweitzer, Siboni und Yogev, 2013). Regierungen erweitern und komplementieren durch Cyberangriffe ihr außen- und sicherheitspolitisches Handlungsrepertoire. Die Möglichkeiten reichen dabei von umfassenden Spionageaktivitäten gegen Staaten, Unternehmen und gesellschaftliche Akteure – wie sie bspw. durch die Snowden-Enthüllungen 2013 aufgedeckt wurden – über kinetisch folgenreiche Angriffe – etwa zur Unterminierung des iranischen Nuklearwaffenprogramms durch den Wurm Stuxnet – bis zur Verschränkung konventioneller Kriegführung mit Cyberangriffen – bspw. im Zuge des Kaukasuskrieges 2008. BeobachterInnen gehen davon aus, dass in zukünftigen Konflikten mit einer zunehmenden Verknüpfung von konventionellen Mitteln des Konfliktaustrags, Cyberangriffen und Maßnahmen zur Informationsmanipulation zu rechnen ist (Libicki, 2017). Regierungen delegieren Angriffe dabei mitunter an nichtstaatliche Akteure (sog. Proxies), um die eigene Urheberschaft systematisch abstreiten zu können (Maurer, 2018).

Diese Ausdifferenzierung auf der Akteursseite ist mit einer qualitativen Weiterentwicklung der Cyberangriffe und der quantitativen Zunahme von Vorfällen verbunden. War Malware in der Frühphase der Netzentwicklung noch häufig Analogon zum konventionellen Scherzartikel, ist Schadsoftware heute meist deutlich komplexer und potenziell folgenreicher. Möglich wird der Einsatz von Schadsoftware durch die zahlreichen Sicherheitslücken (vulnerabilities), die in Hard- als auch Software vorhanden sind und die teilweise durch AngreiferInnen gezielt ausnutzbar sind (exploits). Da die Anforderungen an Funktionalität und Interoperationalität von IT immer anspruchsvoller werden, wächst auch deren Fehleranfälligkeit (Gaycken, 2011).

Sicherheitspolitik wird zudem durch die Globalität des Internets und die technischen Charakteristiken vor neue Herausforderungen gestellt (bspw. durch das Attribtutionsproblem). Diese Situation hat aber nicht nur dazu geführt, dass Staaten neue regulatorische Maßnahmen zum Umgang mit Cybersicherheit ergriffen haben, auch wissenschaftlich erfährt die Thematik zunehmend Aufmerksamkeit:

> »In previous generations, young people who wanted to be relevant in the foreign-policy establishment studied Russian or learned about nuclear disar-

> 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).