Huawei im Spiegel der Geschichte: Großmachtpolitik und Telekommunikationsrisiko von 1840 bis 2021

Rush Doshi und Kevin McGuiness

Brookings Institution, März 2021

Zusammenfassung

Gegen Ende 2018 traf der kanadische Premierminister Justin Trudeau angesichts der amerikanischen Bedenken bezüglich einer möglichen Einbindung Huaweis in die kanadischen Telekommunikationsnetze eine Reihe von Aussagen, die weitgehend der gängigen Meinung im Großteil der Welt entsprachen. „Es sollte keine politische Entscheidung sein“, erklärte er damals, und Kanada würde „die Politik bei der Entscheidungsfindung“ bezüglich der Rolle von Huawei in seinem Netz „außen vor lassen“.[1]

Die Vorstellung, Telekommunikation und Machtpolitik ließen sich entkoppeln, war nicht nur optimistisch, sondern ignorierte auch die Geschichte der Telekommunikation. Dieser Bericht untersucht diese Geschichte und zeigt, wie Macht und Telekommunikation seit jeher eng miteinander verknüpft sind. Wenn Staaten diese Verquickungen ignorierten und hinsichtlich der Sicherheit Leichtsinn walten ließen, waren die Konsequenzen jeweils nachteilig und manchmal sogar verheerend.

In diesem Bericht werden mehrere prominente Beispiele für den Wettlauf zwischen Großmächten im Telekommunikationsbereich untersucht, die bis zu den ersten Anfängen der elektrischen Telekommunikation in den 1840er-Jahren zurückreichen. Diese Fälle zeigen, dass viele der Fragen, die sich den politischen Entscheidungsträgern heute stellen, klare Parallelen in der Vergangenheit haben. Die aktuelle Debatte über Netzwerksicherheit und 5G-Infrastruktur mag neuartig anmuten, hat aber vieles mit lang vergessenen Streitigkeiten gemeinsam, die bereits beim Aufkommen der elektrischen Telekommunikation vor ungefähr 150 Jahren auftauchten. Darüber hinaus wurden viele der wohlbekannten Aspekte des heutigen Telekommunikationswettbewerbs – wie z. B. der Einsatz von normsetzenden Gremien, staatlichen Subventionen, Leitungszugängen, Informationskriegsführung, den Märkten in Entwicklungsländern sowie Verschlüsselung zum eigenen Vorteil – vor mehr als einem Jahrhundert entwickelt, wobei sich für den aktuellen Diskurs wichtige Lehren daraus ziehen lassen.

Hier eine Liste dieser Lehren aus der Vergangenheit:

1. **Die Kontrolle über globale Telekommunikationsnetzwerke ist eine Form politischer Machtausübung.** Es wird damit gerechnet, dass 5G Netzwerke die Grundlage für eine intelligentere, vernetzte Wirtschaft bilden, die unzählige Geräte und Sensoren miteinander verbindet. China möchte diese Netzwerke weltweit aufbauen und subventioniert im Rahmen seiner Initiative „Digitale Seidenstraße“ seine führenden

5G-Unternehmen und 5G-Projekte auf der ganzen Welt. Diese Bemühungen entsprechen dem Streben Großbritanniens nach Netzdominanz in den Anfängen der elektrischen Telegrafie. Über sechs Jahrzehnte baute Großbritannien seinen Vorsprung aus, indem es andere Staaten in eine stetig steigende Abhängigkeit von seinen Netzen brachte – wobei es sogar auf Gebühren und wirtschaftliche Vorteile verzichtete, um die Verlegung von Kabeln durch Großbritannien zu fördern – und gleichzeitig seine eigene Abhängigkeit von ausländischen Netzen verringerte. Schließlich kontrollierte es mehr als die Hälfte des weltweiten Kabelverkehrs, das größte Funknetz und die größte Flotte von Kabellegern. Diese „Informationshegemonie" ermöglichte es Großbritannien, Deutschland im 1. Weltkrieg von so gut wie der gesamten globalen Telekommunikation abzuschneiden, und zwang Berlin dazu, den Nachrichtenverkehr über britische Leitungen abzuwickeln, die von den Briten überwacht werden konnten, was sich als entscheidend für die Niederlage Deutschlands erweisen sollte.

2. **Lange Zeiten von Frieden und Wohlstand führen in der Regel zu Nachlässigkeit hinsichtlich Telekommunikationsrisiken.** In den letzten 30 Jahren fielen der Frieden und die wirtschaftliche Globalisierung nach dem Kalten Krieg mit einer Zeit des raschen Fortschritts im Telekommunikationsbereich zusammen, der die Staaten dazu veranlasste, revolutionäre kommerzielle Vorteile gegenüber politischen und Sicherheitsrisiken zu priorisieren, wobei die Netze bisweilen sogar ausländischen Eigentümern oder Betreibern unterstanden. Eine ähnliche Entwicklung fand in den 1840er-Jahren in den Anfängen der Telekommunikation statt. Auch diese fielen in eine Phase relativen Friedens und der Globalisierung, die bis zum 1. Weltkrieg andauerte. Der Wunsch, das scheinbar magische wirtschaftliche Potenzial der neuen Kommunikationstechnologien zu nutzen, ließ damals Fragen im Zusammenhang mit der Abhängigkeit von ausländischen Netzen und Unternehmen in den Hintergrund treten. Großbritannien profitierte von der Nachlässigkeit anderer, indem es sich eine unangreifbare Schlüsselposition in den globalen Netzwerken aufbaute und diese dann ausnutzte, sodass die meisten anderen Großmächte von seinen Netzen abhängig waren.

3. **Wenn Staaten ihre Telekommunikationssicherheit nicht ernst nehmen, können die Ergebnisse verheerend sein und die Weltpolitik umschreiben.** Die jahrzehntelange Gleichgültigkeit Deutschlands gegenüber seiner Abhängigkeit von britischen Telekommunikationsleitungen führte dazu, dass der Zug bereits abgefahren war, als Berlin sich der Risiken dieser Abhängigkeit schließlich bewusst wurde. Beim Ausbruch des Ersten Weltkriegs kappte Großbritannien alle deutschen Leitungen und zwang Berlin, seinen Nachrichtenverkehr durch die britischen Netze zu leiten, obwohl das Risiko bestand, dass dieser abgehört würde. So kam die „Zimmermann-Depesche" ans Licht, die dabei half, die Vereinigten Staaten zum Kriegseintritt zu bewegen. In ähnlicher Weise ermöglichte es die russische Sorglosigkeit beim Funkverkehr den Deutschen, Nachrichten abzufangen, die Bewegungen der russischen Truppen in Echtzeit zu „sehen" und ihnen in der Schlacht von Tannenberg eine entscheidende Niederlage beizubringen. Im Zweiten Weltkrieg führte die Selbstüberschätzung der Nazis hinsichtlich ihrer Verschlüsselungstechnologie dazu, dass die Codes nur selten aktualisiert wurden. So konnte Großbritannien diese knacken und nachrichtendienstliche Informationen erlangen, von denen angenommen wird, dass sie den Krieg um zwei bis vier Jahre verkürzt haben.

Wissen ist Macht, und daher können selbst vereinzelte Anfälle von Sorglosigkeit oder Laschheit in der Signaltechnik den Lauf der Geschichte verändern.

4. **Neue Technologien führen immer zu neuen Bemühungen, die entsprechenden Informationsflüsse anzuzapfen.** Das Aufkommen von Unterwasserkabeln führte bereits im spanisch-amerikanischen Krieg zu Bemühungen, diese Linien zu kappen und anzuzapfen. Die Funkübertragung führte zu Bemühungen von Rivalen, Netzwerkknoten zu kontrollieren und Übertragungen abzufangen. Und die Einführung von ausgeklügelten Verschlüsselungstechniken führte zu Anstrengungen in industriellem Ausmaß, diese zu knacken. Dabei waren Mal für Mal jeweils einige überzeugt, der jüngste Quantensprung in der Kommunikationstechnik könnte diese weniger anfällig als frühere Technologien machen. Allerdings setzte sich der Zyklus aus Innovation und Missbrauch jedes Mal wieder fort.

5. **Telekommunikationsnetze waren niemals politisch neutral, vor allem nicht in Zeiten politischer Spannungen.** Im Jahr 2019 gelobte die Führung von Huawei: „Keine Hintertüren, keine Spionage!“. Sie versprach, dass sich das Unternehmen aus der Politik heraushalten würde, wobei sich die chinesische Regierung verpflichtete, dieses Versprechen zu respektieren. Doch schon vor mehr als hundert Jahren machten Telekommunikationsunternehmen und die Regierungen ihrer Länder ähnliche öffentliche Versprechungen, während sie diese im Geheimen brachen und in Friedens- wie in Kriegszeiten kollaborierten. So bewog die britische Dominanz bei Unterwasserkabeln die Franzosen, Deutschen und Amerikaner beispielsweise dazu, sich dafür einzusetzen, dass die Leitungen neutral blieben, sogar in Kriegszeiten. Britische Unternehmen erklärten öffentlich ihre Neutralität, fügten sich aber in Wirklichkeit den politischen Interessen Großbritanniens, insbesondere in Zeiten großer Spannungen, und gaben ihre Neutralität in Kriegszeiten überhaupt ganz auf. Der Machtgewinn, den die Störung oder das Abhören der Informationsflüsse von Rivalen mit sich bringt, war in der Regel so verlockend, dass selbst aufrichtige Bekenntnisse zur Neutralität nicht langfristig hielten.

6. **Oft versuchen Staaten, eigene führende Telekommunikationsunternehmen aufzubauen, wenn sie einmal erkannt haben, wie verwundbar sie sind, wenn sie sich auf die Unternehmen eines rivalisierenden oder feindlichen Staats verlassen.** In den USA gibt es derzeit keinen großen Hersteller von 5G-Basisstationen, was zu Debatten darüber geführt hat, ob das Land in seine eigenen Unternehmen investieren oder sich auf Unternehmen seiner Verbündeten verlassen sollte. Dabei kam es auch zu Unstimmigkeiten bezüglich der Frage, inwieweit Huawei selbst de facto ein staatsnahes Vorzeigeunternehmen sei. Diese Debatten haben einige Präzedenzfälle. Anfang des 20. Jahrhunderts begannen viele Staaten, die bei Telekommunikationsgeräten oder -netzen auf andere angewiesen waren, ihre eigenen Systeme zu entwickeln. Deutschland beispielsweise drängte zwei deutsche Unternehmen mit konkurrierenden Funkverkehrsinitiativen – Siemens & Halske und AEG – dazu, zusammen eine deutsche Alternative zur britischen Dominanz im Funkverkehr zu schaffen. Viele andere wichtige Staaten unterstützten Unternehmen, die zwar scheinbar privat waren, aber eng mit den Staaten verflochten waren, die sie unterstützten.

7. **Der Kampf um Telekommunikationsstandards kann den Ausschlag dafür geben, welche Staaten Macht über das Netz haben. Dafür ist oft die Mithilfe von Verbündeten und Partnern nötig.** Staaten, deren Technologie zum vorherrschenden Standard wird, können dies als Vorteil gegenüber anderen nutzen. Der aktuelle Wettbewerb um Standards in der Informationstechnologie ähnelt diesbezüglich dem britisch-deutschen Wettstreit im Bereich der Funknetze. Großbritannien war durch die von ihm unterstützte Marconi Company so dominant in der Funktechnik, dass alle anderen Großmächte ihre Nachrichten über das britische Funknetz weiterleiten mussten, das keine Kontakte mit anderen Funkstationen zuließ. Deutschland war letztendlich erfolgreich damit, diese Dominanz zu brechen, indem in einem Normsetzungsgremium diese „Nichtvernetzungspolitik" mit der Hilfe anderer Mächte, darunter die Vereinigten Staaten und Frankreich, verboten wurde – ein Beispiel, das zeigt, wie ähnliche Verbündungsstrategien heute liberalen Staaten dabei helfen könnten, günstige Informations- und Kommunikationstechnologiestandards (IKT-Standards) festzulegen oder zu bewahren, wenn sie an einem Strang ziehen.

8. **Staaten greifen auf Verschlüsselung zurück, wenn ihre Kommunikation leichter abgefangen werden kann, aber dieser Verschlüsselung sind aufgrund der Entschlossenheit der Gegner oder durch Anwenderfehler oft Grenzen gesetzt.** Manche argumentieren, die Befürchtungen hinsichtlich der Rolle von Huawei in Netzwerken oder der allgemeinen Angreifbarkeit von Geräten, die mit dem Internet verbunden sind, ließen sich durch moderne Verschlüsselungstechnik mindern. Diese Argumentationslinie kann auf eine lange Geschichte zurückblicken. Am Anfang der Telekommunikation vor einem Jahrhundert führte die Möglichkeit, dass Telegramme von anderen gelesen werden könnten, die die Netzknoten kontrollierten, oder dass der Funkverkehr von Abhörvorrichtungen abgefangen werden könnte, zu bedeutenden Fortschritten in der Verschlüsselungstechnik, die bisweilen auch eine gewisse Selbstüberschätzung nach sich zogen. Die komplexen Rotor-Chiffriermaschinen der Deutschen wurden als unentschlüsselbar angesehen, aber Anwenderfehler und seine in industriellem Maßstab vorangetriebenen Bemühungen ermöglichten es Großbritannien, die deutschen Codes zu knacken. Kostengünstige Aktualisierungen der deutschen Geräte und Chiffren hätten die Fortschritte Großbritanniens zunichte machen können, aber Berlins übertriebenes Vertrauen in seine Verschlüsselung verhinderte diese Änderungen. Dadurch konnten Informationen abgefangen werden, die den Verlauf des Krieges veränderten. End-to-End-Verschlüsselung ist deutlich stärker als frühere Verschlüsselungsbemühungen, aber die Vergangenheit zeigt, dass eine gewisse Bescheidenheit angebracht ist.

9. **Viele Staaten unterschätzen die außergewöhnlichen Anstrengungen, die ihre Widersacher möglicherweise unternehmen, um ihre Netze zu kompromittieren.** Vor dem Hintergrund der Debatten über moderne Telekommunikation ist zu bedenken, dass Staaten, die Komfort und Wirtschaftlichkeit höher werteten und dafür bei der Sicherheit Abstriche machten, oft unangenehm überrascht waren, zu welchen Anstrengungen ein entschlossener Widersacher bereit ist, um die entsprechenden Netze zu kompromittieren. Im Ersten Weltkrieg war Deutschland von der Geschwindigkeit und Kompromisslosigkeit Großbritanniens beim Durchtrennen aller von Deutschland

genutzten Leitungen überrumpelt; und nicht viel anders erging es den russischen Befehlshabern, als ihre Sorglosigkeit bei der Funktechnik ihnen die Niederlage von Tannenberg bescherte. Im Zweiten Weltkrieg rechnete Deutschland nicht damit, dass die Briten ein hochgradig zentralisiertes Entschlüsselungsprojekt in industriellem Maßstab entwickeln würden, das jeden noch so nebensächlichen oder flüchtigen Kommunikationsfehler der Deutschen ausnutzen sollte, um deren Codes zu knacken. Im Kalten Krieg wiederum verschlüsselten die Sowjets eine interne Unterwasser-Telefonleitung nicht, die ihrer Ansicht nach außerhalb der Reichweite der Vereinigten Staaten verlief. Doch Washington fand eine Möglichkeit, diese anzuzapfen – und so eine Informationsquelle von unschätzbarem Wert zu gewinnen.

10. **Netzwerksicherheit betrifft nicht nur die Möglichkeit des Abfangens von Nachrichten, sondern auch die der Sabotage.** Der Diskurs über die Rolle von Huawei in Netzwerken wirft gerne Fragen zur Datensicherheit auf, könnte aber bisweilen auch von einer stärkeren Berücksichtigung der Möglichkeit der Sabotage profitieren. Dies ist historisch ein wichtiger Aspekt des Wettbewerbs zwischen den Großmächten im Bereich der Telekommunikation. Am Beginn der Telegrafie versuchten Großmächte Kabel zu durchtrennen und die Kommunikation zu unmöglich zu machen, was in der beispiellosen und minutiös geplanten Initiative Großbritanniens gipfelte, weltweit alle Kabel zu durchtrennen, die Deutschland mit der Außenwelt verbanden. Bisweilen schadet sich ein Staat beim Verfolgen von Sabotagestrategien sogar selbst, tut dies aber dennoch, wenn er glaubt, dass der Schaden für seine Gegner größer ist.

Großmächte und die Telekommunikation

„Großreiche haben große Anstrengungen unternommen, um den Informationsfluss zu beschleunigen“, wird in einem Geschichtsbuch zur Telekommunikation vermerkt. „Die Römer bauten Straßen, die Perser und Mongolen errichteten Pferdetauschstationen, die Briten subventionierten Postschiffe.“[2] Doch so sehr die Staaten auch nach Wissen dürsteten, blieben die Informationsflüsse bis zur Erfindung des modernen Telegrafen doch begrenzt. Die Elektrifizierung von Informationsflüssen schuf die moderne Telekommunikation und die vertrauten Muster der zugehörigen Rivalität zwischen Großmächten.

Die ersten Jahrzehnte der modernen Telekommunikation von 1840 bis zum Ersten Weltkrieg haben wichtige Merkmale mit der heutigen Zeit gemeinsam. Dieser Zeitraum war, ganz wie die aktuelle Ära nach dem Kalten Krieg, einer des relativen Friedens zwischen den Großmächten. Dadurch waren die führenden Staaten „weniger sensibel“, was Fragen der Machtpolitik und Sicherheit in Telekommunikationsnetzen anbelangte.[3] Als die Großmächte im 19. Jahrhundert nationale und internationale Netze aufbauten, gaben sich viele anfänglich damit zufrieden, dies der Industrie zu überlassen, die Nationalität privater Unternehmen zu ignorieren und die Risiken herunterzuspielen, die mit der Kontrolle der Telekommunikationsnetze durch einen Widersacher einhergehen. Die Vorteile der revolutionären Neuerungen in der Telekommunikation – viele sprachen damals von der „Abschaffung von Zeit und Raum“ –[4] waren so offensichtlich und überwältigend, dass „die Eigentümerschaft an den Kabeln als nachrangige Frage angesehen wurde“.[5] Bei der Telegrafie sei es in diesem Zeitraum mehr um das Geschäft als um die Politik gegangen – diese Beobachtung eines Historikers ließe sich genauso gut auf die anfängliche Euphorie über die moderne Informationstechnologie und ihre jüngste Manifestation anwenden: 5G.[6]

Die Phase einer relativen Sorglosigkeit der Großmächte war nicht von Dauer. Staaten wie Peru im Jahr 1879 und dann die USA im Jahr 1898 gehörten zu den ersten, die die Telekommunikationsnetze eines Konkurrenten abschnitten. Als die Spannungen zwischen den Großmächten zunahmen, wurden die Staaten auf der ganzen Welt erschreckt gewahr, dass einige – insbesondere Großbritannien – den langen Frieden gut genutzt hatten und über ihre Privatunternehmen die Kontrolle über die internationale Kommunikation erlangt hatten.

Ländern wie Frankreich und Deutschland machte die Abhängigkeit vom britischen Unterwasser-Kabelnetz zunehmend Sorgen, und sie unterstützten die Entwicklung eigener Netze mit hohen Subventionen. Diese Entwicklung ist der heutigen Subventionierung und Verteidigung seiner führenden Informationstechnologieunternehmen wie Alibaba, Baidu, Tencent und Huawei durch China gar nicht so unähnlich. Wie die Historikerin Heidi Tworek dokumentiert, steckten auch die Rivalen Großbritanniens viel Geld in die Telekommunikationstechnologie der nächsten Generation – die „drahtlose Telegrafie“, besser bekannt als Funk –, um die Abhängigkeit von den britischen Unterwasser-Telegrafenkabeln zu verringern.[7] Die Briten warne hier zwar führend, doch Deutschland wollte sich nicht auf britische Netze verlassen. Das Land baute mit staatlich unterstützten Großunternehmen sein eigenes Netz auf und exportierte dieses in weniger gut vernetzte Teile der Welt – Lateinamerika, Afrika, Asien. Dem könnte man die heutige Expansion chinesischer Technologieunternehmen in die Entwicklungsländer und Beijings Entschlossenheit gegenüberstellen, die Grundlage für 5G-Netze zu schaffen.

Während dieser Zeit wurden viele der Elemente des Wettbewerbs zwischen den Großmächten im Bereich der Kommunikation, die heute bisweilen vernachlässigt werden, von den damaligen Staaten oft recht ernst genommen. Frustriert über die britische Dominanz im Funknetz, nutzte Deutschland ein Normsetzungsgremium, um die britische Dominanz zu brechen – eine Taktik, die zeigt, dass diese Institutionen in dieser Zeit nicht weniger wichtig waren als heute. Und da die Telekommunikation nun drahtlos erfolgte und noch einfacher abzuhören war, setzen die Großmächte ihr Vertrauen in die Verschlüsselung. Manchmal litt dabei allerdings die Disziplin beim Netzbetrieb selbst, weil davon ausgegangen wurde, dass „Chiffren" – detaillierte Schritte zum Verschlüsseln oder Entschlüsseln von Nachrichten – das Problem ohnehin lösen würden, eine Überzeugung, die sich aufgrund von Anwenderfehlern so gut wie immer als Fehlannahme erweisen sollte. Diese Sichtweise weist markante Parallelen mit den modernen Annahmen über die allgemeine Unsicherheit von Telekommunikationsnetzwerken und der in der Debatte immer wieder geäußerten Überzeugung auf, das Risiko, das sich aus dem Zugriff Chinas auf das eigene Telekommunikationsnetz ergebe, werde durch Verschlüsselung weitgehend ausgeschaltet.

Als der Frieden zwischen den Großmächten endete und der Krieg ausbrach, wurde die politische Bedeutung der Telekommunikation – die in Friedenszeiten nicht immer offensichtlich gewesen war – plötzlich deutlich. Der deutsche Erfolg beim Abfangen russischer Nachrichten im Zweiten Weltkrieg führte zum Sieg in der Schlacht von Tannenberg, der den Kriegsverlauf veränderte und Russlands Austritt aus dem Konflikt auslöste. Die britische Kontrolle der Unterwasserkabel im Ersten Weltkrieg war so allumfassend, dass Deutschland vom globalen Telekommunikationssystem abgeschnitten war, der deutschen Telegrammverkehr über britische Netze umgeleitet wurde und schließlich das Zimmermann-Telegramm entdeckt wurde, das die Vereinigten Staaten zum Kriegseintritt bewog. Im Zweiten Weltkrieg erzielte Großbritannien einen weiteren nachrichtendienstlichen Erfolg, indem die vermeintlich unknackbare deutsche Verschlüsselung geknackt wurde. Dies führte zur Erschließung einer beispiellosen Menge an Informationen, die nach Meinung der offiziellen Geschichtsbücher Großbritanniens den Krieg in Europa um Jahre verkürzte. Diese Fälle zeigen, dass die Telekommunikationssicherheit nicht nur eine Frage der Kriegstaktik ist, sondern auch des politischen Wettbewerbs, sondern dass sie ausschlaggebend für das Schicksal von Großmächten und den Verlauf der Weltgeschichte sein kann.

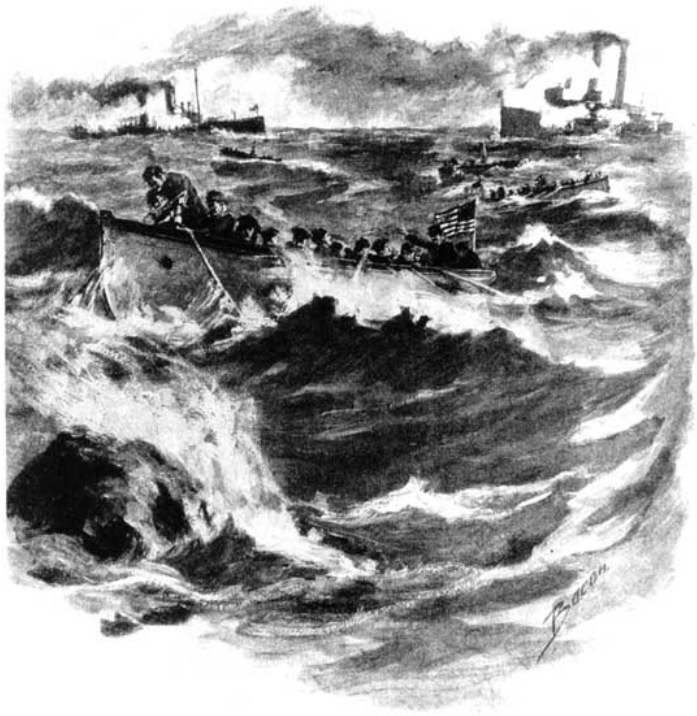
Als die Welt zum Kalten Krieg zwischen den USA und der Sowjetunion überging, ging der Vorsprung der Briten nicht nur durch den amerikanischen Einfluss, sondern auch durch technologische Verschiebungen verloren, die ältere Netzwerke weniger relevant machten. Dies zeigt, wie wichtig es für Großmächte ist, an der Spitze der Technologie zu bleiben. In dieser neuen Ära setzte sich der Telekommunikationswettlauf entlang vertrauter Linien fort. So entwickelten beispielsweise die USA neue Wege, um Unterwasserkabel anzuzapfen, die so tief vergraben waren und als so sicher angesehen wurden, dass die über sie versandten Nachrichten oft gar nicht verschlüsselt wurden. Der Wettbewerb verlagerte sich auch in weitere Bereiche – wie die Satelliten- und Internetinfrastruktur –, wobei ein Großteil dieser Geschichte erst noch geschrieben werden muss und die entsprechenden Quellen meistens noch der Geheimhaltung unterliegen.

Telekommunikation war, wie diese kurze Reihe von Fallbeispielen zeigt, schon immer politisch. Die Instrumentalisierung dieser Technologien und Fähigkeiten hat sich im Allgemeinen parallel

zu ihrer Entwicklung weiterentwickelt. Sobald neue Kommunikationsmethoden aufkamen, suchten die Großmächte im Allgemeinen nach Möglichkeiten, diese abzufangen oder zu sabotieren. „Elektrische Kommunikation wird oft als eine der großen Errungenschaften der Menschheit beschrieben“, merkt ein Telekommunikationshistoriker an, „aber wenn wir sie aus einer Sicherheitsperspektive betrachten, zeichnet sich ein völlig anderes Bild, denn Sicherheit ist kein technisches, sondern ein soziales und politisches Charakteristikum.“ Und „da die Politik keine Fortschritte gemacht hat“, merkt er an, „hat die Telekommunikation nach wie vor eine dunkle Seite.“[8]

Nun wollen wir uns den wichtigsten Themen dieses fast zwei Jahrhunderte währenden Telekommunikationswettlaufs zuwenden.

1. Der Spanisch-Amerikanische Krieg: Die Grenzen der Neutralität von Telegrafenkabeln



Eine Darstellung der US-amerikanischen Kabeltrennaktion in Cienfuegos, veröffentlicht 1907. Die Aktion zeigte, dass Unterwasser-Telegrafenkabel während eines bewaffneten Konflikts nicht als neutral behandelt werden, selbst von einer Großmacht, die einst zu den Befürwortern der Neutralität von Telegrafenkabeln gezählt hatte.

Quelle: Naval Historical Center Online Library[9]

Als im 19. Jahrhundert kreuz und quer durch die Welt Unterwasserkabel verlegt wurden, riefen mehrere Großmächte – darunter Frankreich, Deutschland und die Vereinigten Staaten – dazu auf, dies von der Weltpolitik getrennt zu halten. Im Jahr 1858 forderte US-Präsident James Buchanan Königin Victoria in einem der allerersten transatlantischen Telegramme auf, sicherzustellen, dass die neuen Telegrafenleitungen der Welt „für immer neutral bleiben …sogar während Kampfhandlungen“.[10]

Sobald jedoch Feindseligkeiten ausbrachen, wurden die hochtrabenden Neutralitätsprinzipien über Bord geworfen. Zwei Jahrzehnte nach Buchanans Botschaft durchtrennte Peru chilenische Telegrafenleitungen, die in strittige Gebiete führten.[11] Dieser Streitigkeit wurde wenig Aufmerksamkeit zuteil, aber als die Vereinigten Staaten – ein vormaliger Befürworter der Neutralität der Telegrafenkabel – im Spanisch-Amerikanischen Krieg sowohl im Atlantik als auch im Pazifik Telegrafenleitungen durchtrennten, wurde dies weltweit wahrgenommen.

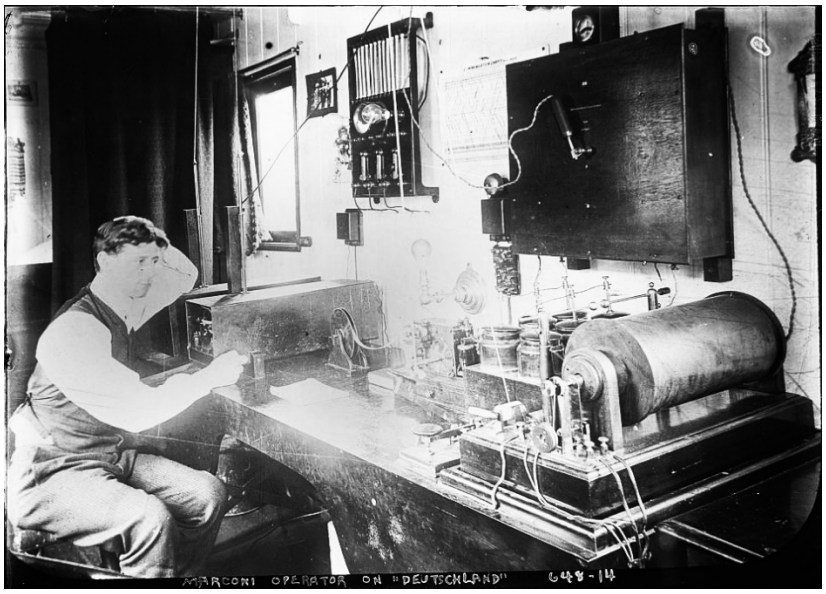
Das Kappen der Leitungen wurde schon im Vorfeld des Konflikts geplant. Auf dem Kriegsschauplatz im Atlantik hatten die Vereinigten Staaten gehofft, Spanien auf diese Weise von seinen Streitkräften in Kuba abzuschneiden. „Die Isolierung von Havanna war natürlich von

größter Bedeutung“, bemerkte damals ein Bericht in einer amerikanischen Zeitschrift. Dazu sei es nötig gewesen, dass die Vereinigten Staaten „Havanna von jeglicher telegrafischen Verbindung mit der Außenwelt abschnitten“.[12] In einem ersten Schritt unterbanden die Vereinigten Staaten den spanischen Telegrafenverkehr durch amerikanisches Hoheitsgebiet in Florida. Anschließend schickte man eine kleine amerikanische Vorhut nach Cienfuegos, um dort einen wichtigen Telekommunikationsknoten zu zerstören. Dadurch wurden die Stadt Havanna und der Großteil des Westens Kubas von Spanien abgeschnitten. Anschließend attackierten die Vereinigten Staaten verschiedene Kabelverbindungen im Osten Kubas sowie Leitungen in der Karibik, die Puerto Rico mit Spanien verbanden.[13] Das Kappen all dieser Verbindungen beeinträchtigte die Fähigkeit Spaniens, seine Kräfte in Kuba zu führen und zu befehligen, in der Summe erheblich.[14]

Im Pazifik durchtrennten die Vereinigten Staaten die einzige Unterwasserleitung zwischen Manila und Hongkong und schnitten die Philippinen damit effektiv von Spanien ab.[15] Diese Entscheidung schadet auch der US-amerikanischen Nachrichtenübermittlung selbst, doch man ging davon aus, dass die Kosten für die Spanier noch höher wären, und die USA konnten die Auswirkungen für sich selbst dadurch lindern, dass sie regelmäßig ein Schiff nach Hongkong schickten, um Mitteilungen nach Washington zu senden.[16] Die US-Kräfte kappten auch die Unterwasserkabel auf den Philippinen selbst, was die Fähigkeit Spaniens weiter beeinträchtigte, seine Kräfte zu befehligen.

Der Spanisch-Amerikanische Krieg war vielleicht der erste globale Konflikt, der sich auf mehrere Schauplätze erstreckte und in dem die elektrische Telekommunikation wichtig war. Es war auch das erste Mal, dass eine Großmacht versuchte, einer anderen den Zugang zu Unterwasserleitungen unmöglich zu machen. Vor dem Konflikt wurde die Telegrafie immer als vorwiegend kommerzieller Bereich angesehen, und viele hatten gehofft, dass die Leitungen von politischen und militärischen Rivalitäten nicht betroffen sein würden. Der Konflikt zeigte die Grenzen dieser Sichtweise auf und ließ erkennen, dass die Kontrolle über die Telekommunikationsinfrastruktur und die Fähigkeit, geopolitischen Rivalen diesen Vorteil zu verweigern, stets von entscheidender politischer Bedeutung war.

2. Die britisch-deutsche Rivalität: Netzaufbau und Normsetzung



Funker der Marconi Company im „Marconi-Raum" des deutschen Hochseeschiffs SS Deutschland. Der Einfluss der Marconi Company war so groß, dass ihre Funker in deutschen Funkräumen arbeiteten, obwohl Deutschland über die Abhör- und Sabotagerisiken besorgt war.

Quelle: Library of Congress, George Grantham Bain Collection[17]

Die technische Normsetzung und die damit verbundenen Netzwerkeffekte sind ein traditionsreiches und komplexes Schlachtfeld im Wettbewerb zwischen den Großmächten. Staaten, deren Technologie zum dominanten Standard wird, können diese Technologie gegenüber anderen nutzen – ein Punkt, der aufsteigenden Mächten wohl bewusst ist, die oft darauf hinarbeiten, ihre daraus resultierende Anfälligkeit durch die Schaffung paralleler Systeme zu reduzieren. Tatsächlich findet der aktuelle chinesisch-amerikanische Wettbewerb im IKT-Bereich seinen historischen Widerpart in einem jahrhundertealten Wettbewerb zwischen Deutschland und Großbritannien um die Dominanz in der damaligen IKT-Infrastruktur. Die Parallelen zur heutigen Zeit sind unheimlich, und wir können wichtige Lehren daraus ziehen.

Im späten 19. Jahrhundert schuf der italienische Ingenieur Guglielmo Marconi, unterstützt von der britischen Royal Navy, die drahtlose Telegrafie.[18] Die Erfindung war revolutionär. Während in der Vergangenheit Supermächte gegenseitig die Leitungen gekappt hatten und die Kommunikation zwischen und mit Schiffen schwierig gewesen war, konnte Marconis System diese Probleme lösen und war weniger anfällig für Störungen.[19] Marconi ging schlussendlich eine Partnerschaft mit Großbritannien ein und bescherte dem Land damit ein Monopol auf Funkübertragungen. In Kombination mit dem 60-prozentigen Anteil Großbritanniens am weltweiten Unterwasser-Kabelnetz dominierte Großbritannien damit den internationalen Nachrichtenverkehr. Der britische Vorsprung beunruhigte Deutschland, aber der Wettbewerb in der Funktechnik „bot Deutschland zugleich die Möglichkeit, die Kontrolle über eine neue internationale Infrastruktur zu übernehmen" und „die britischen Leitungen zu umgehen"; am Erfolg dieser Bemühungen hing großes machtpolitisches Kapital.[20]

Kaiser Wilhelm II bewilligte eine direkte staatliche Unterstützung für deutsche Wissenschaftler und Ingenieure, die die Technik Marconis kopierten, innerhalb Deutschlands patentieren ließen und ihre eigenen Funknetze aufbauten, die durch Verträge mit dem deutschen Militär finanziert wurden.[21] Dennoch setzte sich dank der überlegenen Funktechnik Marconis mit ihrer höheren Reichweite und ihrem „First-Mover Advantage" dessen von Großbritannien unterstütztes Unternehmen als weltweiter Standard durch, und Marconi nutzte diese Netzwerkeffekte, um eine „Nichtvernetzungspolitik" gegenüber anderen Funkbetreibern zu verfolgen. Deutsche Unternehmen und Hochseeschiffe wollten nicht von der globalen Kommunikation getrennt sein, daher bevorzugten sie das britische System gegenüber dem deutschen.

Kaiser Wilhelm II intensivierte die deutsche Industriepolitik, um den britischen Standard anzufechten. Er dekretierte umgehend, dass sich zwei große deutsche Elektrounternehmen mit konkurrierenden Funkprojekten Siemens & Halske und AEG, zusammenschließen sollten, um die definitive deutsche Alternative, Telefunken, zu etablieren. Die inländische Rivalität im Bereich der drahtlosen Telegrafie schwäche die Wettbewerbsfähigkeit Deutschlands, erklärte der Kaiser, und gebe der Marconi Company Gelegenheit, ein weltweites Monopol zu schaffen. Letzteres sei nicht im Interesse Deutschlands.[22] Unter Kaiser Wilhelm II verfolgte Deutschland eine protektionistische Politik, indem es die Marconi-Systeme teilweise verbot. Das Land versuchte, sich neue Märkte zu erschließen, indem es seine Technologie an Südamerika und Afrika verkaufte, um in diesen Regionen den Standard zu bestimmen und Umsätze zu sichern.

Als sich diese Bemühungen als unzureichend erwiesen, konnte Deutschland dafür in multilateralen Standardgremien Erfolge verzeichnen. Im Jahr 1906 brachte Deutschland die Großmächte zur ersten Radiotelegrafie-Konferenz zusammen, einer Konferenz über Standards im Funkbereich. Die Teilnehmerstaaten verboten dort die „Nichtvernetzungspolitik" von Marconi und brachen damit das britische Monopol. De facto führte dies zu einem britisch-deutschen Duopol.[23]

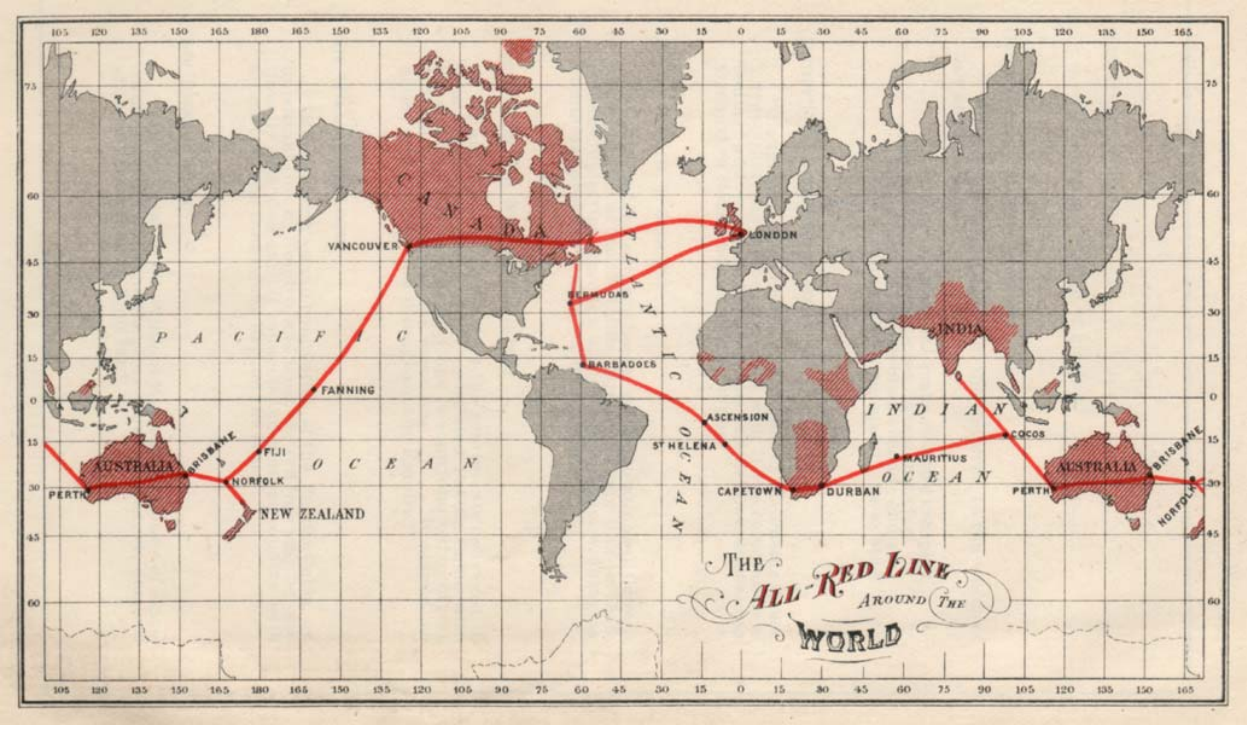
Der britisch-deutsche Wettbewerb zeigt, dass Normsetzungsgremien enorme strategische Wirkung haben. China wendet heute viele der Strategien an, die Deutschland vor einem Jahrhundert verwendet hat: staatlich geführte Industriepolitik, Staatsschutz, großzügige Staatsaufträge, Integration von zivilem und militärischem Bereich, Verbote von Konkurrenzprodukten, Zwangsfusionen, das Streben nach Expansion in Schwellenmärkten und sogar internationale Abkommen zur Festschreibung seiner Standards. All dies hat chinesischen Technologieunternehmen wie Alibaba und Tencent, den Eigentümern von WeChat und Alipay, geholfen, lokale Großunternehmen zu werden. Diese Unternehmen haben seitdem ins Ausland expandiert und zielen häufig nicht auf den US-Markt, sondern – wie zuvor die deutsche Telefunken – auf aufstrebende Märkte mit geringeren Gewinnen und geringerem Wettbewerbsdruck ab.[24]

China hat sich auch die Standards für Hardware-Infrastruktur für die Internetverbindungen als Schlachtfeld auserkoren. Die Regierung investiert Milliarden, damit chinesische Chiphersteller im Wettlauf um die Standards für das mobile 5G-Internet die amerikanischen Konkurrenten schlagen können. Ebenso erhalten chinesische Unternehmen wie Huawei und ZTE staatliche Darlehen, um die Hardware-Infrastruktur für Internetverbindungen in den Entwicklungsländern aufzubauen. Wie das britische Beispiel zeigt, machen diese Bestrebungen nicht nur chinesische

Technologie zum Standard, sondern bieten auch Überwachungsmöglichkeiten. Gleichzeitig macht es die Initiative „One Belt, One Road“ besser möglich, dass Standards für „intelligente Infrastruktur“ in ganz Asien, insbesondere für die relevanten Sensoren und die zugehörige Software, von China festgelegt werden und die Interoperabilität mit anderen Unternehmen verhindern, wodurch diese von Technologien wie dem autonomen Fahren und anderen Branchen ausgeschlossen würden.

Die britisch-deutsche Rivalität in der Telegrafie zeigt, dass Washington die staatlich gelenkte Herausforderung durch China ernst nehmen muss. Das Beispiel bietet aber auch eine Zukunftsperspektive. Genauso wie Deutschland internationale Konferenzen nutzte, um das britische Monopol in der Telegrafie zu brechen, könnten die USA durch multilaterale Vereinbarungen günstige IKT-Standards festlegen oder bewahren. Dies kann China daran hindern, durch Freihandelsabkommen, staatliche Großunternehmen oder Infrastrukturprojekte unilaterale Standards festzulegen.

3. Großbritannien im Ersten Weltkrieg: Informationshegemonie



Die „All Red Line", ein kostspieliges Netz britischer Unterwasserleitungen, das mit enormen Redundanzen gebaut und so angeordnet wurde, dass kein Teil das Gebiet eines Konkurrenten durchquerte. Deutschlands unzureichende Investitionen in ein eigenes, widerstandsfähiges globales Telekommunikationsnetz ermöglichten es Großbritannien, es weitgehend von der globalen Kommunikation abzutrennen, während Großbritannien selbst davon weitgehend unbeeinträchtigt blieb.

Quelle: George Johnson, Hsrg., The All Red Line: The Annals and Aims of the Pacific Cable Project / Internet Archive[25]

Die Bestrebungen Deutschlands, die britische Dominanz im Telekommunikationsbereich im frühen 20. Jahrhundert zu brechen, entsprangen keineswegs einem Verfolgungswahn. Nach dem Ausbruch des Ersten Weltkriegs nutzte Großbritannien seinen erheblichen Einfluss auf die Telekommunikationsnetze erfolgreich, um den Verlauf des Krieges zu bestimmen. Es kappte deutsche Kabelverbindungen, hörte deutsche Übertragungen ab und zwang den deutschen Nachrichtenverkehr in Netze, die von Großbritannien kontrolliert wurden. So wurde auch die Zimmermann-Depesche abgefangen, was zum Kriegseintritt der USA beitrug.[26]

Großbritannien war nicht die erste Großmacht, die Telekommunikationsnetze durchtrennte oder manipulierte. Peru hatte eine Verbindung zwischen Chile und Bolivien gekappt, die Vereinigten Staaten die spanischen Leitungen durchtrennt, und Großbritannien hatte in einer Krise die Buren von ihren europäischen Unterstützern abgeschnitten und in einer anderen den Telegrafenverkehr nach Frankreich manipuliert.[27] Im Ersten Weltkrieg jedoch wurden diese Bemühungen auf die Spitze getrieben.

Großbritannien war das erste Land, das ein ganzes Land von den weltweit gängigen Telekommunikationsnetzen trennte und dazu am ersten Tag des Krieges einen Plan umsetzte, der in Friedenszeiten sorgfältig vorbereitet worden war.[28] Innerhalb eines Jahres zerstörte Großbritannien deutsche Kabelverbindungen auf der ganzen Welt: im Ärmelkanal, in der Nordsee, im Nordatlantik, in Südamerika, im Großteil Afrikas, im Fernen Osten und sogar in neutralen Ländern, in denen deutsche Infrastruktur vorhanden war.[29]

Um dies zu kompensieren, versuchte Deutschland, das Funknetz zu erweitern, das Telefunken bereits ein Jahrzehnt früher in Lateinamerika und im „globalen Süden" errichtet hatte, um damit die Welt zu umspannen. In einer Anstrengung, die Parallelen zu Chinas moderner „digitalen Seidenstraße" aufweist, bot Berlin Regierungen, die an den „Entwicklungsvorteilen des Funkverkehrs" interessiert waren, Kredite und Investitionen für die Errichtung deutscher Kommunikationsknoten an. Als Reaktion darauf überzeugte oder bewog Großbritannien die meisten dieser Länder, keine deutschen Funknetzknoten zu unterstützen, oder sabotierte diese aktiv.[30]

Berlin blieb ohne eigene Netze und hatte während des Krieges keine andere Wahl, als auf das britische Netz zu vertrauen. Die Briten begannen zunächst damit, den gesamten Verkehr, der ihre Kabel passierte, unbemerkt zu überwachen und diesen Vorteil für den Informationskrieg gegen Deutschland zu nutzen, indem sie selektiv die peinlichsten deutschen Nachrichten durchsickern ließen, um Deutschlands Beziehungen zu neutralen Ländern zu schädigen. Als Deutschland ein Telegramm schickte, das eine militärische Allianz mit Mexiko gegen die Vereinigten Staaten vorschlug – die berüchtigte Zimmermann-Depesche –, ging auch diese Nachricht durch ein britisches Netz und wurde von Großbritannien abgefangen und entschlüsselt, das sie dann an die US-Regierung weitergab, die sie wiederum an die amerikanische Öffentlichkeit weitergab.[31] Dieser Vorfall trug dazu bei, die Vereinigten Staaten zum Kriegseintritt zu bewegen. Damit prägte er die Weltgeschichte und besiegelte letztlich die Niederlage Deutschlands.

Der britische Informationskrieg gegen Deutschland zeigt die Gefahren auf, die entstehen, wenn man einem Gegner die Möglichkeit gibt, den eigenen Nachrichtenverkehr zu überwachen oder einem den Zugang zu Telekommunikation zu verwehren. Außerdem lässt er erkennen, dass die Netze, die Großmächte in Friedenszeiten gerne als alltägliche Selbstverständlichkeiten ansehen, in Kriegszeiten oft abgeschaltet werden und der Kampf um Kommunikationsknoten unweigerlich auch Drittparteien und neutrale Länder in Mitleidenschaft zieht.

4. Der deutsche Sieg bei Tannenberg: Die Gefahren des Abhörens

Eine deutsche drahtlose Feldtelegrafenstation während des Ersten Weltkriegs. Russlands Unfähigkeit, die Kommunikation in seinen Feldstationen angemessen zu verschlüsseln, führte zu einer katastrophalen Niederlage, die den Kriegsverlauf prägte.

Quelle: C. O. Nordensvan und Valdemar Langlet, Det stora världskriget *[Der Große Krieg]*[32]

Auch Deutschland hatte im Informationskrieg Trümpfe in der Hand. Es durchtrennte russische Telegrafenleitungen an Land und unter Wasser, die Russland mit seinen wichtigsten Verbündeten verbanden, sowie mehrere transatlantische Kabel, auf die sich die Briten stützten, und nahm bei der Verwendung von U-Booten für diese Aufgaben eine Vorreiterrolle ein.[33] Angesichts der Redundanz britischer Netze waren diese Unternehmungen letztlich weniger verheerend, als die Deutschen gehofft hatten. Wesentlich folgenschwerer war der Einsatz funktechnischer Informationen durch Deutschland gegen Russland bei der Schlacht von Tannenberg im August 1914, dem ersten Kriegsmonat, der für die Russen in eine katastrophale Niederlage mündete. Ein deutscher Geheimdienstoffizier nannte den Vorfall den ersten in der Geschichte der Menschheit, bei dem das Abfangen der feindlicher Funksprüche eine entscheidende Rolle gespielt habe.[34]

Die Schlacht fand vor dem Hintergrund russischer Erfolge an der Ostfront statt. Als Russland tiefer in Ostpreußen eindrang, sah sich das Militär mit einer erheblichen Kommunikationsherausforderung konfrontiert, die die Voraussetzungen für eine verheerende Niederlage schuf. Die Deutschen hatten auf dem Rückzug ihre eigenen Telegrafenleitungen gekappt, und den voranschreitenden Russen fehlte ausreichend geschultes Personal, um über ihre ausgedehnte Formation hinweg eine kabelgebundene Kommunikation einzurichten. Die Funkübertragung bot eine Alternative, aber während die Russen für das militärische Kommando zwar bereits neue Funktechnologien eingeführt hatten, waren diese allerdings nicht ausreichend gesichert. Verschiedenen Gruppen wurden verschiedene Chiffren zugewiesen; die meisten hatten wenig Schulung mit der Codierung und Decodierung von Signalen; einige Codes wurden

bekanntermaßen geknackt; und die Codebücher standen in unzureichender Zahl zur Verfügung und waren zudem für viele der nicht schriftkundigen Rekruten unverständlich.[35] Das Ergebnis war, dass die russischen Befehlshaber sich gezwungen sahen, das Risiko der Verwendung von nicht codierten Funknachrichten einzugehen und zu hoffen, dass die Deutschen diese nicht sorgfältig überwachen würden.

Die Deutschen jedoch verfolgten die Funksprüche genau. Nachdem sie die fehlende Funkdisziplin der Russen im Krieg gegen die Japaner beobachtet hatten, wussten sie, dass deren uncodierte Funksprüche keineswegs Teil eines Täuschungsmanövers waren. Anschließend nutzten sie ihr Wissen über russische Echtzeitkommunikation, um den „Nebel des Kriegs“ zu lichten und den zahlenmäßig überlegenen Gegner rasch zu schlagen. Russland verlor eine ganze Armee, mit über 100.000 Gefallenen und 92.000 Gefangenen – die Deutschen hingegen hatten nur 13.000 Todesopfer zu beklagen.

5. Großbritannien im Zweiten Weltkrieg: Die Grenzen der Verschlüsselung

Nockenräder der Lorenz-Schlüsselmaschine, die im Zweiten Weltkrieg als faktisch unknackbar galt. Die Entschlüsselungsbemühungen der Briten gaben den Beamten Zugang zu Nachrichten, die die Deutschen auf hoher Ebene austauschten.

Quelle: Matt Crypto/Wikimedia Commons[36]

Die Neuerungen der drahtlosen Telegrafie und des Funks brachten im Vergleich zu physischen Kabeln mehr Komfort, machten aber auch das Abhören leichter. In beiden Weltkriegen bewegten sich die Großmächte in einem Umfeld, in dem davon ausgegangen wurde, dass Funksprüche von anderen mitgehört werden konnten. Und in einem solchen Umfeld – gar nicht unähnlich heutigen Annahmen über die Anfälligkeit moderner Computer- und Telekommunikationssysteme – wurde Verschlüsselung als sicherheitskritisch angesehen. Das Ergebnis, wie es ein amerikanischer Militärhistoriker formulierte, war ein „Kampf zwischen Kryptograf und Kryptoanalyst“.[37] Wenn die Großmächte in diesem Wettbewerb den Kürzeren zogen, konnte dies katastrophale Auswirkungen nach sich ziehen.

Um dies zu verhindern, wurden Chiffren verwendet, um das Risiko zu reduzieren, dass ein Mithören die Sicherheit beeinträchtigen würde. Außerdem ließ man „Funkdisziplin“ walten, um zu verhindern, dass Angreifer durch die Analyse des Funkverkehrs Erkenntnisse über Nutzungsmuster gewannen.

Die meisten Großmächte investierten in Anstrengungen in wahrhaft industriellem Ausmaß, um den feindlichen Funkverkehr zu studieren und, wenn möglich, die Chiffren zu knacken.

Großbritannien ging bei der Analyse der feindlichen Chiffren wesentlich zentralisierter vor als Deutschland, wo diese Aufgabe auf mehrere Behörden verteilt war. Und genau wie die britischen Erfolge in der Signalaufklärung und Kryptographie den Verlauf des Ersten Weltkriegs geprägt hatten, prägten sie auch den Verlauf des Zweiten Weltkriegs, als die britische Operation in Bletchley Park die deutschen Enigma- und Lorenz-Chiffren knackte.

Die Verschlüsselungssysteme Enigma und Lorenz verwendeten außergewöhnlich komplexe Rotormaschinen, um Nachrichten zu verschlüsseln, von denen Deutschland glaubte, dass sie daher „unentschlüsselbar" würden.[38] Jeder Tastenanschlag ersetzte ein Zeichen durch ein anderes, basierend auf den eindeutigen Einstellungen des Geräts. Diese Einstellungen – wobei die Anzahl der Möglichkeiten beim Lorenz-System die Gesamtzahl der Atome im Universum überschritt – mussten sowohl dem Absender als auch dem Empfänger bekannt sein, damit die Nachricht entschlüsselt werden konnte.[39] Enigma wurde vom Militär, der Gestapo und den Diplomaten genutzt, das Lorenz-System, das noch komplexer war, von Adolf Hitler und hochrangigen Nazis und Militärbeamten, die so miteinander kommunizierten.

Der britische Erfolg beim Knacken von Enigma und Lorenz war das Ergebnis mehrerer Entwicklungen. Erstens war er ein Produkt der geheimdienstlichen Zusammenarbeit zwischen den Alliierten und Polen, das einige deutsche Fehler ausgenutzt hatte, um einige einfachere Enigma-Maschinen zu knacken.[40] Wie ein damaliger britischer Kryptoanalyst es ausdrückte, hätte die Arbeit ohne die Beiträge Polens „erst gar nicht in die Gänge kommen können".[41]

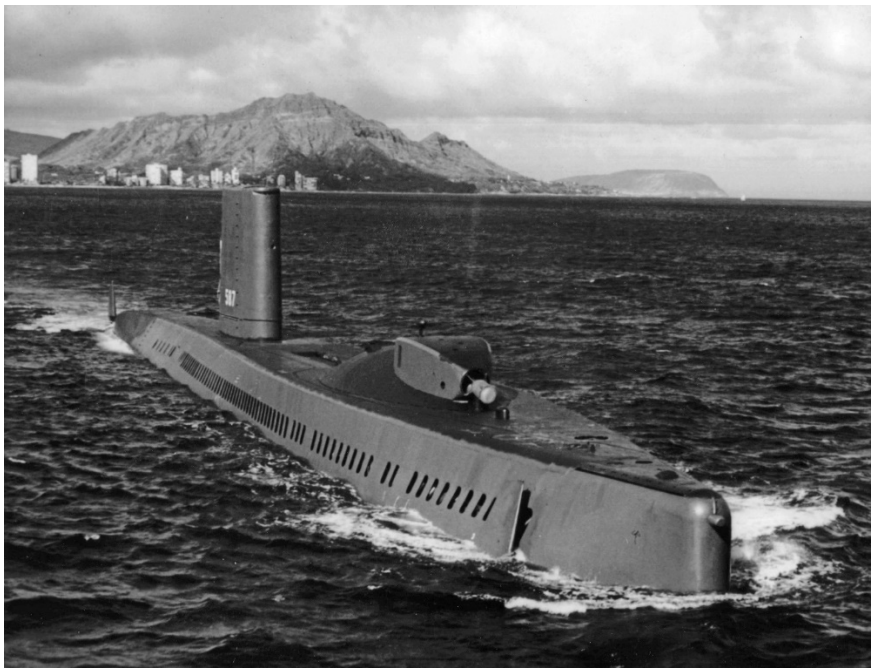
Zweitens war er ein Produkt der deutschen Selbstüberschätzung: Da Deutschland nie davon ausging, dass die Chiffren geknackt worden sein könnten, unterließ es selbst relativ einfache Modifikationen, die die Briten gezwungen hätten, wieder bei Null zu beginnen.[42] Andererseits war das Vertrauen der Deutschen in die Unknackbarkeit seiner Maschinen „beinahe gerechtfertigt", wie sich ein leitender Beamter in Bletchley Park erinnerte.[43]

Schließlich war er das Ergebnis eines einzigen, aber großen Ausrutschers in der deutschen „Funkdisziplin", der die Rekonstruktion der deutschen Chiffriersysteme erlaubte, ohne diese jemals selbst gesehen zu haben.[44] Selbst die ausgeklügeltsten Systeme waren anfällig auf Anwenderfehler, und ein wachsamer Gegner konnte diese ausnutzen.

Indem es das Enigma- und das Lorenz-System knackte, erhielt Großbritannien Zugang zu einigen der sensibelsten Übermittlungen der Deutschen. Winston Churchill hat dem Vernehmen nach die geheimdienstliche Arbeit als einen der Hauptgründe für den Sieg Großbritanniens im Krieg gesehen, und Dwight D. Eisenhower nannte sie „entscheidend".[45] Der offizielle Historiker des britischen Geheimdiensts, Sir Francis Harry Hinsey, argumentiert, dass diese Erfolge „den Krieg um nicht weniger als zwei Jahre und wahrscheinlich um vier Jahre verkürzt", die Anstrengungen von Feldmarschall Erwin Rommel in Afrika untergraben, alliierte Schiffsverluste durch deutsche U-Boote deutlich verringert und die Landungen in der Normandie erst ermöglicht hätten.[46] Außerdem konnten die Briten praktisch alle deutschen Spione identifizieren, die in das Land eindrangen, und sie oft dazu nutzen, fehlerhafte Nachrichten zurückzusenden, wobei der Programmleiter anmerkte, dass der britische Geheimdienst „das deutsche Spionagesystem in unserem Land de facto selbst betreibt und kontrolliert".[47] Nur wenige Länder hatten in Kriegszeiten derart genaue Kenntnisse übereinander.

Zusammengenommen bergen die Erfolge der britischen Anstrengungen gegen Deutschland, die Überwachung der deutschen Kommunikation durch Polen in Friedenszeiten und seine Entscheidung, Großbritannien an seinem diesbezüglichen Erfolg teilhaben zu lassen, Lehren, die sich auch auf die heutige Zeit anwenden lassen, wenn Großmächte Cyberaufklärung gegeneinander betreiben. Allgemein gilt, dass diejenigen, die argumentieren, Verschlüsselung verringere das Problem, dass ein Gegner Zugriff auf das eigene Telekommunikationsnetzwerk bekommen könnte, möglicherweise einen Fehler machen, wie es damals auch Deutschland tat: übermäßiges Vertrauen in die Technologie und unzureichende Berücksichtigung der stets vorhandenen Möglichkeit menschlicher Fehler.

6. Operation Ivy Bells: Die Tiefen der nachrichtendienstlichen Aufklärung



Die USS Halibut, die dem Vernehmen nach an der Anzapfung einer sowjetischen Telefonleitung beteiligt war.

Quelle: U.S. Navy / Wikimedia Commons[48]

Die Sowjetunion war bei ihrer Verschlüsselung viel vorsichtiger als die Nazis und baute dabei auf ihre eigene Version von Enigma – bekannt als Fialka –, die wesentlich komplexer war.[49] Aus diesem Grund hatten die riesigen Mengen strategischer nachrichtendienstlicher Informationen, die im Zweiten Weltkrieg ergattert wurden, nachdem die deutschen Chiffren geknackt worden waren, soweit bekannt, im Kalten Krieg kein Gegenstück. Angesichts dieser Schwierigkeit wurden nun andere Methoden zur Erschließung der feindlichen Kommunikation entwickelt. Eine der kühnsten unter diesen Bemühungen fand im Hinblick auf Unterwasserkabel statt.

Die Einführung von Unterwasserkabeln im 19. Jahrhundert hatte schließlich zu Bemühungen geführt, sie zu kappen und gelegentlich anzuzapfen, häufig in seichten Gewässern oder an Land, wo solche Aufgaben einfacher durchzuführen waren. Im Gegensatz dazu wurde die Durchführung dieser Arbeiten in tiefen Gewässern, die von einem Gegner kontrolliert werden, als praktisch unmöglich erachtet, insbesondere wenn sie verdeckt durchgeführt werden sollten. Seit dem 20. Jahrhundert waren die Briten und dann die weiteren Großmächte zu einer Gewissheit über die Sicherheit der Unterwasserkabel gelangt: Wenn die Landestellen gesichert seien und die Kabel keine neutralen oder feindlich gesinnten Länder durchquerten, seien sie in der Regel vor Abhöraktionen und Durchtrennungen gefeit, insbesondere in der Friedenszeit.[50]

Der Kalte Krieg jedoch änderte dieses Kalkül. Die Einführung nuklearer U-Boote eröffnete die Möglichkeit, Unterwasserkabel in der Tiefsee anzuzapfen. Aber die Aufgabe, Taucher für den

Zugang zu Kabeln zum Tiefseeboden zu schicken, war von der Komplexität her eher vergleichbar mit der Weltraumforschung als den bekannten Versuchen der Kabelmanipulation in früheren Epochen. Auch die Schaffung einer Abhörvorrichtung, die unter solchen Bedingungen installiert werden konnte, war eine technische Herausforderung.

Als die Vereinigten Staaten den Verdacht hegten, dass eine sowjetische Unterwasserleitung vom Marinestützpunkt in Wladiwostok zu einer U-Boot-Basis auf der Halbinsel Kamtschatka führen könnte, versuchten sie, diese Hindernisse zu überwinden. Dies zeigt, für wie wertvoll Signalaufklärung erachtet wurde.[51] Wenn man dieses 5-Zoll-Drahtbündel anzapfen könnte, würde dies, so dachte man, wichtige Informationen zu den sowjetischen Nuklearkräften erschließen.[52] Während die Sowjets den gesamten über die Luft gesendeten Datenverkehr verschlüsselten, gingen die Vereinigten Staaten davon aus, dass die Sowjets damit rechneten, dass ein Zugriff auf den Datenverkehr über das geschützte Unterwasserkabel praktisch unmöglich sei, und ihn daher nicht verschlüsselten. Außerdem seien „sowjetische Admirale und Generäle viel zu herrisch und ungeduldig, um sich mit einem Heer an Kryptografieexperten herumzuschlagen, das bereits von der Menge seiner Arbeit überfordert ist“, und würden selbst auf ungesicherter Sprachkommunikation bestehen.[53] Ein Anzapfen der Leitung würde somit einen raren Fundus an Informationen liefern, und die US-Marine brachte daher Operation Ivy Bells auf Schiene, um dies zu ermöglichen.

Vieles über den Abhörmechanismus und die damit erlangten Informationen ist bis heute geheim, aber offene Quellen liefern einige Details über die einzigartige und innovative Operation. Die USA sendeten ein nukleares U-Boot, die USS Halibut, um unbemerkt an der sowjetischen Marine vorbeizukommen und auf einer Fläche von 600.000 Quadratkilometern das Unterwasserkabel auszumachen.[54] Innovative Technologie wurde entwickelt, um sicherzustellen, dass Taucher über mehrere Stunden unter hohem Druck und bei extrem niedrigen Temperaturen arbeiten konnten. Ebenso wurden neue Methoden für die Installation einer Abhörvorrichtung in dieser anspruchsvollen Umgebung entwickelt.[55] All dies musste geschehen, ohne dass die Sowjets auch nur Verdacht schöpften. Sollte das Boot entdeckt werden, könnten die Sowjets es entern oder zerstören.

Die Operation erwies sich letztendlich als erfolgreich, und während der gesamten 70er-Jahre fing die U.S. Navy ungesichert über das Kabel übertragene Nachrichten ab und zeichnete sie auf. Alle paar Monate fuhren amerikanische U-Boote unbemerkt in sowjetische Gewässer, wichen Angriffen von U-Booten aus, brachten Taucher zu den Kabelanschlüssen und sammelten Bänder der sowjetischen Kommunikation ein – das war eine äußerst wertvolle und seltene Informationsquelle Während die Vereinigten Staaten zur Signalaufklärung ein „Netzwerk von Spionagesatelliten, -flugzeugen, -abhörstationen und -U-Booten“ aufgebaut hatten, um Signalintelligenz zu sammeln, konnten sie „nicht in eine festverdrahtete Telefonleitung eindringen“, die sich im Gebiet eines Gegners befand. Diese Anstrengungen illustrierten den allmählichen Wandel in der Telekommunikation, nämlich, dass ein bestimmter Akteur mit den richtigen Tools auf Daten und Signale zugreifen kann, die über jedes beliebige Medium oder Mittel übertragen werden. Auch wenn diese Abhörvorrichtung letztlich durch ein Leck beschädigt wurde, lieferten die damit abgefangenen Telekommunikationsdaten den USA und ihren Verbündeten militärische und politische Informationen von unschätzbarem Wert.[56]

Moderner Telekommunikationswettbewerb im historischen Kontext

Bis zum Ende des Kalten Krieges hatten die Vereinigten Staaten Großbritannien eindeutig als Informationshegemon abgelöst. Die Vereinigten Staaten verfügen heute über eine Knotenposition im globalen Internet, robuste Weltraumfähigkeiten, eine beherrschende Stellung in den meisten Internettechnologien und – laut öffentlichen Angaben – ausgeklügelte Fähigkeiten zum Abfangen oder zur möglichen Sabotage von feindlicher Kommunikation.

Dieser Vorsprung der USA wird zurzeit auf die Probe gestellt, wie es bei Großbritannien vor über einem Jahrhundert der Fall war. Russland und insbesondere China stellen nun die Dominanz der USA infrage. Während die USA bei vielen Datenströmen eine Knotenposition einnimmt, versuchen andere Mächte zunehmend, ihre Abhängigkeit von US-Netzen zu verringern. Gleichzeitig ist die zentrale amerikanische Position für das Abfangen weniger notwendig als im Fall Großbritanniens vor einem Jahrhundert. Das Internet ermöglicht das Eindringen in Netze ohne Kontrolle über die zugehörige physische Infrastruktur. Smartphones und Computernetzwerke können gehackt werden, und unabhängig davon, ob die sensible Kommunikation wie früher durch physische Angriffe oder wie heute durch virtuelle Angriffe beeinträchtigt wird, ist das Endergebnis das gleiche. Vernetzung schafft daher heute wahrscheinlich eine noch größere Angriffsfläche als im Zeitalter des Telegramms oder des Funks.

Besonders Russland ist beim Ausnutzen dieser Angriffsfläche an vorderster Front. Im Jahr 2007 startete Russland eine Welle von Cyberangriffen gegen estnische Institutionen, überwiegend verteilte Denial-of-Service-Angriffe.[57] Im Jahr 2008 wurden auch im russisch-georgischen Krieg Cyberangriffe verübt. Dazu wurden nicht nur Denial-of-Service-Angriffe unternommen, sondern auch Bemühungen, Regierungswebsites umzuleiten, georgische Regierungsserver zu übernehmen und den georgischen Internetverkehr über von Russland kontrollierte Server umzuleiten. Einige der Angriffe wurden bereits vor dem Konflikt vorbereitet, um dann zeitgleich mit dem militärischen Angriff Russlands umgesetzt zu werden.[58] 2014, als Russland die Krim eroberte, kombinierte es Cyberangriffe mit der physischen Kontrolle von Telekommunikationsnetzwerken. Die russischen Soldaten beschlagnahmten ukrainische Telekommunikationseinrichtungen und verwendeten sie, um die Kommunikationskanäle auf der Krim zu kappen und sogar Cyberangriffe und Störaktionen in anderen Teilen der Ukraine durchzuführen.[59] 2015 begann Russland eine Welle von Cyberangriffen auf die ukrainische Infrastruktur, die in zwei schwerwiegenden Fällen Hunderttausenden von Ukrainern den Strom abstellten. In den nächsten Jahren unternahm das Land eine Welle beispielloser Angriffe in der Ukraine, die sich auf „Medien, Finanzen, Verkehrswesen, Militär, Politik und den Energiesektor“ erstreckten – praktisch jedes Segment der ukrainischen Gesellschaft. Einige hielten dies für eine Übung im Hinblick auf einen ähnlichen Angriff auf die Vereinigten Staaten.[60] Gleichzeitig setzte das Land seine Angriffsserie im Baltikum fort und versuchte bekanntlich, die US-Wahlen 2016 und 2020 mit Desinformationskampagnen zu beeinflussen. Ähnliches wurde auch in anderen Ländern versucht.[61] Im Jahr 2021 bezichtigte die US-Regierung Russland offiziell eines Hackerangriffs auf das IT-Unternehmen SolarWinds. Es handelte sich um einen ausgeklügelten Angriff, der einen Großteil der Bundesverwaltung und mehrere große US-Unternehmen beeinträchtigte.[62]

Die andere Weltmacht, die erhebliche Investitionen in den Telekommunikationswettbewerb tätigt, ist China. Allerdings zielt China im Gegensatz zu Russland nicht nur darauf ab, die bestehende Internet-Infrastruktur zu nutzen, sondern auch Netzwerke und Infrastrukturen aufzubauen, die es beeinflussen und sogar kontrollieren kann. Wie Russland ist auch China in der Lage, bestehende Schwachstellen im Internet auszunutzen. Anfang der 2000er-Jahre begann China eine Welle von Angriffen auf die Netzwerke des US-Verteidigungsministeriums. Dieses bezeichnete dies als „Operation Titan Rain“.[63] Regierungen auf der ganzen Welt – in den USA, Großbritannien, Frankreich, Deutschland, Kanada, Australien, Japan, Südkorea, Taiwan, Indien und mehr als einem Dutzend anderer Länder – haben sich über das Eindringen von China in ihre Regierungsnetzwerke beschwert. Bei einigen der größten Cyberangriffe des letzten Jahrzehnts wurde vom amerikanischen Justizminister William Barr bestätigt, dass sie auf das Konto chinesischer Agenten gingen, darunter der Diebstahl von Aufzeichnungen aus dem U.S. Office of Personnel Management (Aufzeichnungen für 21 Millionen Menschen), von Marriott Hotels (über 400 Millionen), von Anthem Health Insurance (über 80 Millionen) und von Equifax (147 Millionen Menschen), um nur einige zu nennen.[64]

Gleichzeitig legt China auch das Fundament für die zukünftige Internet-Infrastruktur, und angesichts seiner bisherigen Bemühungen ist es unwahrscheinlich, dass diese Tätigkeiten derzeit rein kommerzieller Natur sind oder in Zukunft rein kommerzieller Natur bleiben werden. Am deutlichsten sind die chinesischen Investitionen in die 5G-Netze, die voraussichtlich die Grundlage für eine intelligentere, vernetzte Wirtschaft bilden werden, die unzählige Geräte und Sensoren miteinander verbindet. China möchte diese Netzwerke weltweit aufbauen und subventioniert seine 5G-Vorzeigeunternehmen und -projekte auf der ganzen Welt im Rahmen der Initiative „Digitale Seidenstraße“. Dank der wettbewerbsfähigen Preise konnten Unternehmen wie Huawei den Wettbewerb mit anderen großen 5G-Anbietern gewinnen und einen erheblichen globalen Marktanteil erreichen, wodurch China zum Marktführer beim Aufbau dieser Netzwerke wurde. Auch abseits der 5G-Technologie subventioniert die chinesische Regierung Bemühungen um den Aufbau von Internet- oder Kommunikationsinfrastruktur auf so gut wie allen Kontinenten. All diese Bemühungen werden durch eine Kampagne zur Gestaltung globaler Standards ergänzt. Dies ist eine wichtige politische Priorität für China, die in übergeordneten Planungsdokumenten verankert ist, die – wie die britisch-deutsche Rivalität in der Funktechnik vor einem Jahrhundert – die Zukunft der Telekommunikation auf eine Weise prägen könnten, die China in die Hände spielt. Zu diesem Zweck hat China kürzlich eine neue Initiative zur Datensicherheit vorgestellt.[65]

Einige befürchten, dass die Aktivitäten Chinas die Möglichkeit eröffnen, dass Beijing de facto die Kontrolle über diese Netzwerke hat und den Datenverkehr abfangen oder sabotieren kann. Über Chinas Bemühungen, eine solche Kontrolle zu übernehmen, liegen nur wenige öffentliche Informationen vor, aber die US-Regierung gab im Februar 2020 bekannt, dass Huawei sog. „Backdoors“ in seinen Netzgeräten hatte, und diese den relevanten Unternehmen, mit denen es Verträge abgeschlossen hat, nicht bekanntgegeben hatte. Diese Backdoors gingen über das hinaus, was Regierungen in den jeweiligen Ländern bisweilen im Rahmen gesetzlich gedeckter Überwachungsmöglichkeiten einforderten.[66] Darüber hinaus haben öffentliche Berichte zutage gefördert, dass Huawei Regierungen wie jene Ugandas und Sambias bei der Identifizierung von Dissidenten unterstützt hat.[67] Selbst über den Fall Huawei hinaus hat eine Cybersicherheitsfirma kürzlich Backdoors in obligatorischer Steuersoftware entdeckt, die ausländische Unternehmen in

China installieren müssen.[68] Unabhängig davon, ob diese Fälle darauf hindeuten, dass Huawei seine Position in diesen Netzwerken ausgenutzt hat, sind das Verhalten des Unternehmens und die Erfolgsbilanz Chinas im Bereich Cyberangriffe und Spionage Grund zur Sorge.

Den anderen wesentlichen Grund zur Besorgnis liefert die Geschichte – und das Verhalten, das selbst liberale Großmächte mit strengeren rechtsstaatlichen Grundsätzen an den Tag gelegt haben. Tatsächlich deuten die angeführten historischen Fälle stark darauf hin, dass die Art von Macht und Einfluss, die ein Unternehmen wie Huawei ausüben wird, wahrscheinlich von der chinesischen Regierung ausgenutzt wird, genau wie früher auch andere Großmächte oftmals die Stellung ihrer Unternehmen oder deren Fähigkeiten im Bereich der Telekommunikation ausgenutzt haben.

Aus dieser umfassenderen historischen Perspektive kommen viele Beobachter auf Basis der Beweislage möglicherweise zu dem Schluss, dass Vorsicht geboten ist, was die Rolle von Huawei in Telekommunikationsnetzen betrifft – selbst dann, wenn die Motive des Unternehmens selbst in der Tat rein kommerziell, sein Versprechen „Keine Hintertüren, keine Spionage“ glaubwürdig und Beijing in seinem Bekenntnis, diese Versprechen zu respektieren, aufrichtig sein sollten.

Im Großen und Ganzen haben, wie dieser Bericht zeigt, viele der Merkmale des Telekommunikationswettbewerbs zwischen den Großmächten, die heute als neuartig gelten, ihre Wurzeln bereits in der Vergangenheit. Im Laufe der Geschichte haben sich mehrere Leitmotive wiederholt:

- *Macht:* Die Kontrolle über Telekommunikationsnetze ist seit deren Anfängen vor über 150 Jahren eine Form politischer Machtausübung. Großbritannien hat seine Rolle im Telekommunikations- und Funkbereich ausgenutzt, die USA haben dies wahrscheinlich im modernen Internet-Zeitalter getan, und es besteht Grund zur Sorge, dass China dies heute seinerseits versuchen könnte.

- *Sorglosigkeit*: Lange Zeiten von Frieden und Wohlstand führen zu Sorglosigkeit hinsichtlich Telekommunikationsrisiken. Im 19. Jahrhundert gaben sich Großmächte damit zufrieden, sich auf ausländische Firmen und ausländische Netze zu verlassen, genau wie die Staaten heute bereit sind, chinesische Telekommunikationsausrüstung und -betreiber zu akzeptieren Doch schließlich erwies sich die Abhängigkeit von potenziellen Mitbewerbern oder gar Gegnern für Länder wie Deutschland als katastrophal und hat den Lauf der Weltgeschichte verändert.

- *Missbrauch:* Neue Telekommunikationstechnologien haben schon immer zu neuen Bemühungen geführt, Kommunikation abzufangen, zu sabotieren oder zu missbrauchen. Hinsichtlich der Hoffnung, dass die Verschlüsselungstechnologie die Bemühungen Chinas um das Abfangen moderner Kommunikationsdaten erschweren könnte, ist zu bedenken, dass die großen Hoffnungen, die in der Vergangenheit in Verschlüsselung gesetzt wurden, durch Anwenderfehler und die Entschlossenheit feindlicher Staaten zu deren Entschlüsselung zunichte gemacht wurden, wie es auch Deutschland erfahren musste, als Großbritannien seine angeblich „unknackbaren“ Chiffren knackte. Ein

entsprechendes Maß an Demut ist bei jeder neuen Welle vermeintlich sicherer Technologien das Gebot der Stunde.

- *Großunternehmen:* Staaten versuchen oft, ihre eigenen Telekommunikations-Vorzeigeunternehmen aufzubauen, besonders in Zeiten wachsender Spannungen. Die chinesische Regierung ist stolz auf die Erfolge von Huawei und setzt sich weltweit für das Unternehmen ein – dabei macht sie nicht vor Drohungen gegenüber Staaten Halt, die dessen Technologie ablehnen. Es wäre ungewöhnlich, dass ein Unternehmen, das der Regierung seines Landes so nahe steht, immun gegen staatlichen Druck wäre, wo doch so viele andere Telekommunikationsunternehmen in der Geschichte dies nicht geschafft haben.

- *Normen und Standards*: Telekommunikationsstandards können bestimmen, wer die Macht über das Netz hat. So nutzte Deutschland etwa ein Normsetzungsgremium, um die britische Dominanz in der Funktechnik zu brechen. Heute findet dieser Wettbewerb in Organisationen wie der Internationalen Fernmeldeunion statt, und die Rolle von Huawei darin legt die Frage nahe, ob ihre Standards China eine Neugestaltung der Telekommunikation ermöglichen werden.

- *Sabotage:* Bei der Netzsicherheit geht es nicht nur um Abhör- und Datensicherheit, sondern auch um die Verteilung des Zugriffs auf das gesamte Netz oder die Abschottung von anderen Netzen. Großbritannien trennte Deutschland von den weltweiten Telegrafennetzen, und die Rolle von Huawei in heutigen Netzen könnte es ihm ermöglichen, das Netz in Ländern, in denen seine Ausrüstung zum Einsatz kommt, auszuschalten, selbst wenn der Zugriff auf die Daten selbst nicht einfach ist.

- *Entschlossenheit:* Viele Staaten unterschätzen die außergewöhnlichen Anstrengungen, die seine Widersacher möglicherweise unternehmen, um ihre Netze zu kompromittieren, und erleben später eine unangenehme Überraschung. Die Fähigkeit Großbritanniens, im Zweiten Weltkrieg durch Bemühungen in industriellem Ausmaß die deutschen Chiffren zu entschlüsseln, und die Fähigkeit der USA, vermeintlich nicht anzapfbare interne sowjetische Unterwasserkabel anzuzapfen, zeigt, wie weit Großmächte gehen, um an wichtige nachrichtendienstliche Informationen zu gelangen. Auch China wird wahrscheinlich solche enormen Anstrengungen unternehmen, und selbst wenn Huawei seine Position in modernen Netzwerken nur schwer instrumentalisieren können sollte, ist es ein wiederkehrendes Motiv im Telekommunikationswettbewerb, den Einfallsreichtum und die Motivation eines entschlossenen Wettbewerbers wie China zu unterschätzen.

Wie dieser Bericht zeigt, bleiben viele der Merkmale des Kräftespiels zwischen den Großmächten im Bereich der Telekommunikation gleich, auch wenn die Spieler selbst wechseln.

Über die Autoren

Rush Doshi war Director der Brookings China Strategy Initiative und Fellow der Brookings Foreign Policy. Er war außerdem Fellow des Paul Tsai China Center der Yale Law School und gehört zu den ersten Stipendiaten der Wilson China Fellowship. Seine Forschung konzentrierte sich auf die übergeordnete chinesische Strategie sowie auf indopazifische Sicherheitsfragen. Doshi ist Autor des Buchs *The Long Game: Chinas Grand Strategy to Displace American Order*, das bei der Oxford University Press erscheinen wird. Derzeit ist er in der US-Regierung unter Joe Biden tätig.

Kevin McGuiness arbeitete vor kurzem als externer Mitarbeiter des Skillbridge Department of Defense Program mit Brookings zusammen. Er hat dort Beiträge zu verschiedenen Projekten im Center for East Asia Policy Studies geleistet. Er ist ein Veteran der Air Force und hat vor kurzem seine Tätigkeit als Fakultätsmitarbeiter an der United States Air Force Academy beendet, wo er Vorlesungen über internationale Beziehungen und Asienpolitik gab. In jüngerer Zeit arbeitete er außerdem als Forschungsassistent beim Institute for National Strategic Studies' Center for the Study of Chinese Military Affairs, wo er sich auf PLA-Modernisierung und -Sicherheit im indisch-pazifischen Raum konzentrierte.

Danksagungen

Die Autoren danken den ehemaligen Praktikanten Isabella Lu, Zijin Zhou und Gaoqi Zhang für ihre Forschungsunterstützung bei diesem Projekt, mehreren anonymen Prüfern, Claire Harrison und Ted Reinert für die Bearbeitung des Berichts sowie Chris Krupinski und Rachel Slattery für Layout und Webdesign. Brookings ist dem US-Außenministerium und dem Institute for War and Peace Reporting für die Finanzierung dieser Studie dankbar.

Dieser Bericht wurde vor der Aufnahme des Regierungsdienstes durch Rush Doshi erstellt, bezieht sich nur auf offene Quellen und spiegelt nicht unbedingt die offizielle Politik oder Position einer Behörde der US-Regierung wider.

Die Brookings Institution ist eine gemeinnützige Organisation, die sich unabhängiger Forschung und politischen Lösungen widmet. Ihre Mission besteht darin, qualitativ hochwertige, unabhängige Forschung durchzuführen und auf der Grundlage dieser Forschung innovative, praktische Empfehlungen für Politiker und die Öffentlichkeit zu geben. Die Schlussfolgerungen und Empfehlungen in Veröffentlichungen von Brookings sind ausschließlich die der jeweiligen Autoren und spiegeln nicht die Ansichten der Institution, ihrer Geschäftsleitung oder ihrer anderen Gelehrten wider.

[1] Steven Chase, Robert Fife und Barrie McKenna, „Trudeau Refuses to Let 'politics Slip into' Decision on Huawei", The Globe and Mail, 15. Oktober 2018, https://www.theglobeandmail.com/politics/article-trudeau-refuses-to-let-politics-slip-into-decision-on-huawei/; Greg Quinn und Josh Wingrove, „Trudeau Says Politics Won't Factor Into Huawei 5G Decision", Time, 19. Dezember 2018, https://time.com/5485141/justin-trudeau-huawei-5g-decision-politics/.

[2] Daniel R. Headrick, The Invisible Weapon: Telecommunications and International Politics, 1851-1945 (Oxford, Vereinigtes Königreich: Oxford University Press, 1991), Kapitel 1.
[3] Ibid., diese Beobachtung stammt von Headrick.
[4] Ibid.
[5] Ibid.
[6] Ibid., diese Beobachtung stammt von Headrick.
[7] Heidi Tworek, News from Germany: The Competition to Control World Communications, 1900–1945 (New York: Harvard Historical Studies, 2019).
[8] Daniel R. Headrick, The Invisible Weapon.
[9] „NH 79949 Cienfuegos Cable-Cutting Operation, 11. Mai 1898", Naval Historical Center Online Library, https://www.history.navy.mil/content/history/nhhc/our-collections/photography/us-people/b/baker-benjamin-f/nh-79949.html.
[10] ibid., Kapitel 5.
[11] Jonathan Winkler, „Information Warfare in World War I", The Journal of Military History 73, Nr. 3 (2009): 845–67, https://doi.org/10.1353/jmh.0.0324.
[12] Cameron McR. Winslow, „Cable-Cutting at Cienfuegos", The Century Illustrated Monthly Magazine 57 (1899): 708-717, https://books.google.com/books?id=Y7fPAAAAMAAJ&pg=PA708#v=onepage&q&f=false.
[13] Jonathan Winkler, „Silencing the Enemy: Cable-Cutting in the Spanish–American War", War on the Rocks, 6. November 2015, https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/; Rebecca Raines, „Manifesting Its Destiny: The U.S. Army Signal Corps in the Spanish-American War", *Army History* 46 (1998): 14–21, https://www.jstor.org/stable/26304991.
[14] Jonathan Winkler, „Silencing the Enemy".
[15] „Spanish American War: Telegraphy and Cable Cutting, Introductory Essay", Naval History and Heritage Command, https://www.history.navy.mil/research/publications/documentary-histories/united-states-navy-s/telegraphy-and-cable.html.
[16] Jonathan Winkler, „Silencing the Enemy".
[17] Library of Congress, George Grantham Bain Collection, https://www.loc.gov/pictures/item/2014683102/.
[18] Heidi Tworek merkt allerdings an, dass seine eigene Rolle bei der Entwicklung dieser Technologie häufig übertrieben wurde. Heidi Tworek, *News from Germany*.
[19] Marc Raboy, „The First Company That Wanted to 'Connect the World' Wasn't Google or Facebook", Media@LSE, 24. August 2016, https://blogs.lse.ac.uk/medialse/2016/08/24/the-first-company-that-wanted-to-connect-the-world-wasnt-google-or-facebook/.
[20] Heidi Tworek, News from Germany, 12–13.
[21] Michael Friedewald, „Telefunken vs. Marconi, or the Race for Wireless Telegraphy at Sea, 1896-1914", SSRN (9. Januar 2014): https://doi.org/10.2139/ssrn.2375755.
[22] Ibid.
[23] Marc Raboy, Marconi: The Man Who Networked the World (Oxford, Großbritannien: Oxford University Press, 2016), 226–28.
[24] So war Telefonunken auch in Regionen aktiv, in denen Deutschland nicht über eine große Kolonialpräsenz verfügte, wie etwa Lateinamerika.
[25] George Johnson, Hrsg., *The All Red Line: The Annals and Aims of the Pacific Cable Project* (Ottawa: James Hope and Sons, 1903), 10, im Internet Archive, https://archive.org/details/allredlineannals00johnuoft/page/n11/mode/2up.
[26] Gordon Corera, „How Britain Pioneered Cable-Cutting in World War One", BBC News, 15. Dezember 2017, https://www.bbc.com/news/world-europe-42367551.
[27] Jonathan Winkler, „Information Warfare in World War I", 847.
[28] P. M. Kennedy, „Imperial Cable Communications and Strategy, 1870-1914", The English Historical Review 86, no. 341 (1971): 728–52, https://www.jstor.org/stable/563928.
[29] Jonathan Winkler, „Information Warfare in World War I", 849.
[30] Ibid., 851.
[31] Gordon Corera, „Why Was the Zimmermann Telegram so Important?", BBC News, 17. Januar 2017, https://www.bbc.com/news/uk-38581861; Patrick Beesly, Room 40: British Naval Intelligence 1914-18 (San Diego: Harcourt Brace Jovanovich, 1982).
[32] C. O. Nordensvan und Valdemar Langlet, *Det stora världskriget* [Der Große Krieg] (1915), unter Wikimedia Commons, https://commons.wikimedia.org/wiki/File:German_WW_I_field_telegraph_002.jpg.
[33] Jonathan Winkler, „Information Warfare in World War I."

[34] Wilhelm Flicke, „The Beginnings of Radio Intercept in World War I: A Brief History by a German Intelligence Officer“, NSA Cryptologic Spectrum Artikel 8, Nr. 2 (1978): 21, https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/.
[35] Bruce Norman, Secret Warfare: The Battle of Codes and Ciphers (Newton Abbot, Großbritannien: David & Charles Ltd, 1973); Prit Buttar, Collision of Empires: The War on the Eastern Front in 1914 (Oxford, Großbritannien: Osprey Publishing, 2014).
[36] Matt Crypto, „The rotors of a Lorenz SZ42 cipher machine on display at Bletchley Park museum“, unter Wikimedia Commons, https://commons.wikimedia.org/wiki/File:SZ42-6-wheels.jpg.
[37] George I. Beck, „Military Communication - The Advent of Electrical Signaling“, Britannica, https://www.britannica.com/technology/military-communication.
[38] Harry Hinsley, „The Influence of ULTRA in the Second World War“, (Vortrag, Cambridge, Großbritannien, 19. Oktober 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.
[39] 1×10^{170} mögliche Einstellungen.
[40] „Bletchley Park Remembers Polish Code Breakers“, BBC News, 14. Juli 2011, https://www.bbc.com/news/uk-england-beds-bucks-herts-14141406.
[41] Gordon Welchman, The Hut Six Story: Breaking the Enigma Codes (Cleobury Mortimer, Großbritannien: Classic Crypto Books, 1997).
[42] Harry Hinsley, “The Influence of ULTRA.”
[43] Ibid.
[44] Vgl. beispielsweise Jerry Roberts, „Lorenz: Breaking Hitler’s Top Secret Code at Bletchley Park“ (Cheltenham, Großbritannien: History Press, 2017).
[45] F. W. Winterbotham, „The Ultra Secret“ (New York: Harper & Row, 1974), 154, 191.
[46] Harry Hinsley, „The Influence of ULTRA“.
[47] Calder Walton, „The Spies Who Came In From the Continent“, Foreign Policy, 27. April 2019, https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/.
[48] U.S. Navy, at Wikimedia Commons, https://commons.wikimedia.org/wiki/File:USS_Halibut_with_bow_thruster.jpg.
[49] Anna Borshchevskaya, „The Soviets’ Unbreakable Code“, Foreign Policy, 27. April 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.
[50] Daniel R. Headrick, The Invisible Weapon, Kapitel 4.
[51] Sherry Sontag, Christopher Drew und Annette Lawrence Drew, „Blind Man’s Bluff: The Untold Story of American Submarine Spionage“ (New York: Public Affairs, 1998), 222.
[52] Ibid.
[53] Ibid., 223.
[54] Ibid.
[55] Matt Blitz, „Navy Divers and Their Daredevil Mission to Spy on the Soviet Union at the Bottom of the Sea“, Popular Mechanics, 30. März 2017, https://www.popularmechanics.com/technology/security/a25857/operation-ivy-bells-underwater-wiretapping/.
[56] Michael J. Sulick, American Spies: „Espionage Against the United States from the Cold War to the Present“ (Washington, DC: Georgetown University Press, 2013), 109–14; Matt Blitz, „Navy Divers“.
[57] Damien McGuinness, „How a Cyber Attack Transformed Estonia“, BBC News, 27. April 2017, https://www.bbc.com/news/39655415; Rain Ottis, „Analysis of the 2007 Cyber Attacks Against Estonia From the Information Warfare Perspective“, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008), https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.
[58] David Hollis, „Cyberwar Case Study: Georgia 2008“, Small Wars Journal, 6. Januar 2011, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008; Ronald J. Deibert, Rafal Rohozinski, und Masashi Crete-Nishihata, „Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war“, Security Dialogue 43, no. 1 (2012): 3–24, https://journals.sagepub.com/doi/10.1177/0967010611431079.
[59] Pavel Polityuk und Jim Finkle, „Ukraine Says Communications Hit, MPs Phones Blocked“, Reuters, 4. März 2014, https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304; Sergey Sukhankin, „Russian Electronic Warfare in Ukraine: Between Real and Imaginable“, Jamestown Foundation, 24. Mai 2017, https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/.
[60] Andy Greenberg, „How an Entire Nation Became Russia’s Test Lab for Cyberwar“, Wired, 20. Juni 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; „Six Russian GRU Officers Charged in Connection

with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace“, U.S. Department of Justice, 19. Oktober 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[61] Constanze Stelzenmüller, „The impact of Russian interference on Germany’s 2017 elections“, (Aussage vor dem Kongress, 28. Juni 2017), https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

[62] Maggie Miller, „US intel agencies blame Russia for massive SolarWinds hack“, *The Hill,* 5. Januar 2021, https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack.

[63] „Connect the Dots on State-Sponsored Cyber Incidents - Titan Rain“, Council on Foreign Relations, https://www.cfr.org/cyber-operations/titan-rain.

[64] Garrett Graff, „China’s Hacking Spree Will Have a Decades-Long Fallout”, Wired, 11. Februar 2020, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.

[65] Chun Han Wong, „China Launches Initiative to Set Global Data-Security Roles“, *The Wall Street Journal,* 8. September 2020, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974.

[66] Bojan Pancevski, „U.S. Officials Say Huawei Can Covertly Access Telecom Networks“, The Wall Street Journal, 12. Februar 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

[67] Joe Parkinson, Nicholas Bariyo und Josh Chin, „Huawei Technicians Helped African Governments Spy on Political Opponents“, The Wall Street Journal, 15. August 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[68] William Turton, „Hidden Back Door Embedded in Chinese Tax Software, Firm Says“, Bloomberg, 25. Juni 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.