

# **China als „Cyber-Großmacht“: die zwei Sprachen Pekings in der Telekommunikation**

Rush Doshi, Emily de La Bruyère, Nathan Picarsic und John Ferguson

März 2021

## **Zusammenfassung**

Die chinesische Außenpolitik und chinesische Werbebotschaften rund um das Thema Informationstechnologie (IT) sprechen eine gemeinsame Sprache. Im Inland hört man jedoch eine andere, zweite Sprache. Erstere spricht von freien Märkten, Offenheit, Zusammenarbeit und Interdependenz, d. h. Themen, die nahelegen, dass Huawei und andere chinesische Unternehmen genau wie alle anderen globalen Akteure des Privatsektors behandelt und in ausländischen Netzwerken begrüßt werden sollten. Indessen drehen sich kommerzieller, akademischer und innenpolitischer Diskurs in China um die *Grenzen* freier Märkte und die Gefahren der Abhängigkeit von ausländischen Technologien – und dementsprechend um die Notwendigkeit von Industriepolitik und staatlichen Kontrollen zum Schutz von Technologien, Unternehmen und Netzwerken. Der nationale chinesische Diskurs deutet außerdem darauf hin, dass kommerzielle Kommunikationsnetzwerke, Telekommunikationssysteme eingeschlossen, dazu genutzt werden könnten, Macht und Einfluss aggressiv zu demonstrieren sowie, dass internationale technische Standards eine Möglichkeit bieten, diese Macht und diesen Einfluss zu festigen, und vor allem, dass IT-Architekturen ein Nullsummenwettbewerb sind.

Der Eindruck, dass die Botschaften der chinesischen Außenpolitik und chinesischer Unternehmen unaufrichtig sein könnten, ist keineswegs neu. Die wesentlichen Unterschiede zwischen diesen Botschaften und der internen Diskussion zu IT in China sind jedoch weitgehend undokumentiert – trotz des steigenden Einflusses Chinas auf internationale IT-Infrastrukturen, -Technologien und -Normen und der zunehmenden Entwicklung derselben in China selbst. Der vorliegende Bericht zielt darauf ab, diese Lücke zu füllen und die Spannungen zwischen der von China geführten externen und internen Diskussion zu Telekommunikation sowie IT im weiteren Sinne zu dokumentieren. Der Bericht beleuchtet auch interne Diskurse, um Einblicke in Absicht, Ambitionen und Strategie Pekings zu gewinnen. Dieser Bericht sollte Fragen zu Chinas staatlichen und wirtschaftlichen Botschaften sowie dazu aufwerfen, was diese möglicherweise zu verschleiern versuchen.

Motivation für die Erstellung des vorliegenden Berichts sind Chinas wachsender Einfluss auf den Telekommunikationssektor und die damit einhergehende zunehmende Kontroverse. Allerdings sind Telekommunikationsressourcen, Ambitionen und strategischer Rahmen Chinas mit denen des weiteren IT-Umfelds verflochten. Aus diesem Grund werden in diesem Bericht sowohl der innenpolitische, kommerzielle und akademische Diskurs zu IT im Allgemeinen als auch zur Telekommunikation im Besonderen behandelt. Der vorliegende Bericht betrachtet überdies den weiter gefassten Kontext der chinesischen Bemühungen, sich zu einer „Cyber-Großmacht“ bzw. „Netzwerk-Großmacht“ zu entwickeln, d. h. Chinas Bestrebungen, bestehende Branchenführer zu überholen und die Architektur der digitalen Revolution zu prägen.

Eine neue technologische Landschaft nimmt Form an. China arbeitet daran, diese Landschaft zu prägen. Es ist wichtiger denn je, die Ambitionen Chinas genau zu dokumentieren.

# Einführung

2020 wandte sich das chinesische Telekommunikationsunternehmen Huawei an eine bekannte westliche Zeitschrift mit einer Anfrage: Es wurde darum gebeten, eine Serie von zehn Artikeln zur Unterstützung von Huawei zu veröffentlichen, da das Unternehmen in der westlichen Welt unter Druck geraten war.<sup>1</sup> Huawei schlug eine Reihe von Themen für diese Artikel vor, darunter den vorgeblichen Respekt des Unternehmens gegenüber geistigem Eigentum, die Vorzüge, die staatliche Zuwendungen gegenüber Huawei der Welt boten, seine Rolle als verantwortungsvoller Akteur mit Vertrauen in den freien Marktwettbewerb und seinen Status als Unternehmen im Mitarbeiterbesitz, unabhängig vom staatlichen Einfluss Chinas. Huawei schlug firmeneigene Wissenschaftler und Mitarbeiter für Interviews vor. Das Unternehmen bot auch Beratungen mit ausgewählten Vertretern an, die Huawei nicht angehörten. Huawei erbat sich, Materialien vor ihrer Veröffentlichung einer abschließenden Überprüfung unterziehen zu können.

Bemühungen zur Einflussnahme auf die öffentliche Berichterstattung sind bei großen Unternehmen in China wie auch andernorts nicht ungewöhnlich. Das Vorgehen von Huawei hebt sich jedoch von ähnlichen Bemühungen ab. Es zeichnet sich durch ein Zusammenwirken mit gleichzeitigen Vorstößen der chinesischen Regierung aus, den globalen Diskurs zum Thema Telekommunikation und Informationsnetzwerke zu beeinflussen. Diese nach außen gerichteten Botschaften – sowohl im Namen des Unternehmens als auch der Regierung – stehen in klarem Kontrast zum kommerziellen, akademischen und innenpolitischen Diskurs in China.

Die chinesische Außenpolitik und chinesische Werbebotschaften rund um das Thema Informationstechnologie (IT) sprechen eine gemeinsame Sprache. Ihr inländisches Pendant offenbart jedoch eine radikal andere zweite Sprache. Genau wie in den von Huawei vorgeschlagenen Artikeln ist in ersterer von freien Märkten, Offenheit, Zusammenarbeit und Interdependenz die Rede, also von Themen, die nahelegen, dass Huawei und andere chinesische Unternehmen wie alle anderen globalen Akteure des Privatsektors behandelt und in ausländische Netzwerke eingebunden werden sollten. Indessen betont der inländische Diskurs die *Grenzen* freier Märkte und damit die Notwendigkeit von Industriepolitik und staatlichen Kontrollen zum Schutz von Technologien, Unternehmen und Netzwerken, die Gefahr der Abhängigkeit von ausländischen Technologien, den Wettbewerbswert der Festlegung internationaler Standards und, was all dem zugrunde liegt, der Unvermeidbarkeit eines Nullsummenwettbewerbs im IT-Bereich.

Der Eindruck, dass die Botschaften der chinesischen Außenpolitik und chinesischer Unternehmen unaufrichtig sein könnten, ist keineswegs neu. Die wesentlichen Unterschiede zwischen diesen Botschaften und der internen Diskussion zu IT in China sind jedoch weitgehend undokumentiert – trotz des steigenden Einflusses Chinas auf internationale IT-Infrastrukturen, -Technologien und -Normen und der zunehmenden Entwicklung derselben in China selbst. Der vorliegende Bericht zielt darauf ab, diese Lücke zu füllen und die Spannungen zwischen der von China geführten externen und internen Diskussion zu Telekommunikation sowie IT im weiteren Sinne zu dokumentieren. Der Bericht beleuchtet auch interne Diskurse, um Einblicke in Absicht, Ambitionen und Strategie Pekings zu gewinnen. Dieser Bericht sollte Fragen zu Chinas staatlichen und wirtschaftlichen Botschaften sowie dazu aufwerfen, was diese möglicherweise zu verschleiern versuchen.

Motivation für die Erstellung des vorliegenden Berichts sind in erster Linie Chinas wachsender Einfluss auf den Telekommunikationssektor und die damit einhergehende zunehmende Kontroverse. Allerdings sind Telekommunikationsressourcen, Ambitionen und strategischer Rahmen Chinas mit denen des weiteren IT-Umfelds verflochten. Aus diesem Grund werden in diesem Bericht sowohl der innenpolitische, kommerzielle und akademische Diskurs zu IT im Allgemeinen als auch zur Telekommunikation im Besonderen behandelt. Dieser Bericht betrachtet überdies den weiter gefassten Kontext der chinesischen Bemühungen, China zu einer „Cyber-Großmacht“<sup>2</sup> zu machen, d. h. seiner Ambitionen, bestehende Branchenführer zu überholen und die Architektur der digitalen Revolution zu prägen. Der Bericht legt mehrere primäre Erkenntnisse dar:

1. **China spricht intern zwar wiederholt über seine Ambitionen als „Cyber-Großmacht“, lässt diese aber nur selten in der Kommunikation nach außen durchscheinen.** Der Begriff „Cyber-Großmacht“ ist ein Schlüsselkonzept, das die chinesische Strategie in den Bereichen Telekommunikation sowie IT im weiteren Sinne leitet. Der Begriff findet sich im Titel fast jeder bedeutenden Rede Xi Jinpings über Chinas Telekommunikations- und Netzwerkstrategie, die er seit 2014 an inländische Zielgruppen gerichtet hat. Er taucht jedoch selten in Botschaften auf, die sich an externe Zielgruppen richten, und wurde in sechs Jahren nur einmal von Sprechern des Außenministeriums verwendet. Dies deutet darauf hin, dass Peking die Diskussionen über seine Ambitionen absichtlich verwässert, um ausländische Zielgruppen nicht in Alarmbereitschaft zu versetzen.
2. **Während die chinesische Regierung ausländische Zielgruppen zum Kauf von Huawei-Produkten ermutigt, warnen ihre Funktionäre das inländische Publikum vor den Gefahren, die sich aus der Abhängigkeit von fremder Technologie ergeben.** Jahre vor dem Handelskrieg und den unter Präsident Trump verhängten Beschränkungen für Huawei vertrat Xi bereits die Ansicht, dass „die Kontrolle der Kerntechnologien durch andere die größte versteckte Gefahr für uns darstellt“. Ausländern die Kontrolle solcher Kerntechnologien zu überlassen, sei laut ihm, „wie ein Haus auf dem Fundament eines anderen zu bauen“.<sup>3</sup> Er streicht heraus, dass „China über eigene Technologie verfügen muss, und zwar über eine starke Technologie.“<sup>4</sup>
3. **Die chinesische Regierung fordert ausländische Gruppen, die Huawei skeptisch gegenüberstehen, zur Einhaltung der Marktprinzipien auf. Gleichzeitig warnt die Regierung das inländische Publikum davor, dass die Entwicklung von IT-Netzwerken industriepolitische Eingriffe erfordert und nicht Marktkräften anvertraut werden darf.** Xi hat explizit erklärt, dass „die Börse uns keine Kerntechnologien bringen und Geld keine Kerntechnologien kaufen kann“.<sup>5</sup>
4. **Peking nennt die Sicherheitsbedenken aus dem Ausland in Bezug auf Huawei „lahme Ausrede[n]“ und reine „Politik“.<sup>6</sup> Gleichzeitig äußert China im Inland ähnliche Bedenken hinsichtlich der Integration ausländischer Technologien in seine Netzwerke.** Sicherheit ist für Xi von entscheidender Bedeutung. So hat er wiederholt erklärt, dass es „ohne Cybersicherheit keine nationale Sicherheit geben kann“.<sup>7</sup> Dementsprechend plädiert er nur für die Einführung ausländischer Technologie, die „kontrollierbar“ ist, während Funktionäre des Ministeriums für Industrie und Informationstechnologie (MIIT) betonen, dass ausländische Technologienetzwerke in der Regel nicht „kontrollierbar“ sind.<sup>8</sup> China müsse daher eigene Netze aufbauen, die „unabhängig und kontrollierbar“ sind.<sup>9</sup>

5. **Kommerzielle und akademische chinesische Quellen deuten darauf hin, dass die Sicherheitsbedenken der internationalen Community in Bezug auf die chinesische Telekommunikation möglicherweise nicht fehl am Platz sind und Peking Telekommunikationsnetzwerke sowie sonstige kommerzielle Netzwerke als Mittel sehen könnte, um weltweit offensiv Macht zu demonstrieren.** Xi präsentiert IT als wesentlichen Bestandteil der militärisch-zivilen Fusionsstrategie Chinas: 2018 sagte er: „Die militärisch-zivile Fusion in den Bereichen Cybersicherheit und Informatisierung ist Schlüssel und Grenze der militärisch-zivilen Fusion im Allgemeinen.“<sup>10</sup> Auch Qin An, Direktor des China Institute of Cyberspace Strategy, vertrat 2016 die Ansicht, dass „es aufgrund der stark monopolistischen Natur von Informationstechnologiesystemen unwahrscheinlich ist, dass es zwei verschiedene Systeme für die militärische und zivile Nutzung geben wird ... Insbesondere [für China] ist es notwendig, militärische und zivile Ressourcen durch ein militärisch-ziviles Fusionssystem zu integrieren.“<sup>11</sup>
  
6. **Bei der Diskussion von Standards mit ausländischen Zielgruppen betont die chinesische Regierung den beiderseitigen Nutzen der Zusammenarbeit. Der Diskurs im Inland rückt jedoch den Wettbewerbswert von Standards für die Erlangung technologischer Dominanz in den Vordergrund, und damit die Notwendigkeit, den „Machtdiskurs“ bei der globalen IT-Entwicklung aufzubauen.** Xi vertritt die Meinung, dass das „Spiel der großen Mächte“ in den Bereichen Cybersicherheit und Telekommunikation „nicht nur ein Spiel der Technologie, sondern auch ein Spiel der Ideen und des Machtdiskurses ist“ – ein Verweis auf Internet-Governance und -Standards.<sup>12</sup> Weitere Quellen bauen auf Xis Thematik auf und erwähnen, dass China bestrebt ist, im Bereich 5G und auch allgemeiner in der IT neue Standards zu setzen, um den Westen zu überholen, was wirtschaftliche und militärische Vorteile mit sich brächte. Kurz gesagt: „Wer über die Standards bestimmt, bestimmt über die Welt.“<sup>13</sup>

Der vorliegende Bericht beginnt mit einem Überblick über den strategischen Rahmen, in den sich die Telekommunikationsziele Pekings einfügen: das Konzept der „Cyber-Großmacht“, das erstmals im Jahr 2014 von Xi vorgestellt wurde und umfassende Ambitionen zur Umsetzung der vierten industriellen Revolution beinhaltet. Auf dieser Grundlage untersuchen die nächsten Abschnitte spezifische Elemente der Diskurse Pekings zu Telekommunikation und IT sowie den Kontrast zwischen der externen und internen Kommunikation. Der erste Abschnitt konzentriert sich auf ein relativ defensives Element: Die Gefahr der Abhängigkeit von ausländischen „Kerntechnologien“ und der Notwendigkeit von Industriepolitik anstelle der Abhängigkeit von Marktkräften, um diese Gefahr zu beseitigen. Im nächsten Abschnitt geht es um die Themen Netzwerk- und Cybersicherheit in China: Einerseits verurteilt Peking ausländische Sicherheitsbedenken bezüglich chinesischer Systeme und Technologien, andererseits herrscht Sorge über die Cyber- und Netzwerksicherheit und die Rolle, die inländische Beiträge darin spielen. Überspitzt ausgedrückt betrachtet Peking internationale, kommerzielle Informationsnetzwerke tatsächlich als Mittel aggressiver Machtprojektion. Der letzte Abschnitt befasst sich mit Chinas Ambitionen bezüglich der Definition von Standards sowie dem entsprechenden Wettbewerb um strukturelle Macht.

## Ein Hinweis zur Methodik

Bei der Beurteilung des nach außen gerichteten Diskurses stützt sich der Bericht in erster Linie auf offizielle diplomatische Aussagen und Bemerkungen der Sprecher des chinesischen Außenministeriums. Diese sind für ausländische Zielgruppen gedacht.

In Bezug auf den nach innen gerichteten Diskurs greift der Bericht auf eine breitere Palette an Quellen zurück, darunter Reden und Artikel von Xi und anderen führenden Persönlichkeiten der chinesischen Regierung, die sich an inländische Zielgruppen richten, sowie Dutzende von autoritativen Zeitschriften, die mit Elementen des Parteistaats verbunden sind, vom MIIT bis zur Volksbefreiungsarmee (VBA).

Quellen, die Xi selbst nicht zugeschrieben werden können, müssen als weniger aussagekräftig betrachtet werden und bieten daher einen geringeren Erklärungswert als von ihm persönlich bewilligte Quellen. Selbst innerhalb des zentralisierten Regierungssystems Chinas dürften Beamte der höheren Ebenen eine Vielfalt von Ansichten widerspiegeln. Auch innerhalb der relativ stark kontrollierten akademischen Gemeinschaft Chinas (z. B. der Chinesischen Akademie der Wissenschaften) können die Meinungen von Experten von denen der Regierung abweichen. Trotz dieser Einschränkungen halten die Autoren des vorliegenden Berichts solche inoffiziellen oder weniger offiziellen Quellen für bedeutsam, um das Wettbewerbsverständnis und die Ambitionen Chinas zu verstehen. In Äußerungen von Xi sind keine detaillierten Aussagen zu bestimmten Technologien oder technologischen Anwendungen zu erwarten. Beamte des MIIT oder des Ministeriums für Wissenschaft und Technologie treffen solche Aussagen hingegen durchaus. Hochrangige Regierungsbeamte, deren Äußerungen einer regelmäßigen Prüfung unterliegen, gehen voraussichtlich weniger auf sensible Themen ein (z. B. militärische Anwendungen von 5G), als es bei isolierten akademischen und kommerziellen Quellen der Fall ist. Regierungsverlautbarungen spiegeln in der Regel die politische Sichtweise wider, die sich bereits gebildet hat. Akademische und kommerzielle Abhandlungen können einen Einblick in die Entwicklung und aufkommende Trends bei relevanten Denkweisen geben.

Der vorliegende Bericht bemüht sich um die Quadratur des Kreises, indem er die Aussagekraft aller verwendeten Quellen überprüft und dabei Kontext bereitstellt. Die Aussagekraft von Quellen wurde anhand ihrer Autoren, Herausgeber und des Ausmaßes beurteilt, mit dem Argumente anderer Positionen innerhalb des chinesischen strategischen Diskurses vertreten wurden. Eine solche Methodologie geht nicht davon aus, dass eine einzelne Quelle einen perfekten Erklärungswert bietet. Vielmehr besteht das Ziel darin, eine relativ umfassende, unverfälschte Sammlung von Quellen zu präsentieren, die zusammen Chinas strategischen internen Diskurs zu Telekommunikation und IT widerspiegeln.

# Ziel: China als „Cyber-Großmacht“

*„Der Aufbau Chinas zu einer ‚Cyber-Großmacht‘ ist ein langfristiges, komplexes und systematisches strategisches Projekt, das alle Aspekte der Wirtschaft und der Gesellschaft umfasst.“*

– Chen Zhaoxiong, stellvertretender Minister des Ministeriums für Industrie und Informationstechnologie, 2017<sup>14</sup>

Xi führte im Februar 2014 das Konzept einer „Cyber-Großmacht“ (网络强国), auch als „Netzwerk-Großmacht“ übersetzt,<sup>15</sup> mit der Gründung der ranghöchsten Organisation für Internetthemen in der Kommunistischen Partei Chinas ein: die Zentrale Führungsgruppe für Cybersicherheit und Informatisierung.<sup>16</sup> Darauf führte Xi die Entwicklung zu einer „Cyber-Großmacht“ als einen Eckpfeiler der chinesischen Internetpolitik ein, und damit als einen wichtigen Schritt zur Verwirklichung der Hundertjahres-Parteiziele – große Meilensteine, die die Partei hofft, bis zu den Hundertjahresjubiläen ihrer Gründung (2021) und ihres Siegs im Chinesischen Bürgerkrieg (2049) zu erreichen.<sup>17</sup> Seitdem hat sich das Konzept der „Cyber-Großmacht“ im offiziellen Diskurs in China verbreitet. Das Konzept hat sich als Schlüsselfaktor der chinesischen Strategie im Telekommunikations- und IT-Bereich herauskristallisiert. Der Begriff „Cyber-Großmacht“ erscheint im Titel fast jeder wichtigen Rede Xis zur chinesischen Telekommunikations- und Netzwerkstrategie, die er seit 2014 an inländische Zielgruppen gerichtet hat.

Allerdings ist der Begriff in Botschaften, die sich an externe Zielgruppen richten, selten zu finden. Er wurde in sechs Jahren nur einmal von Sprechern des Außenministeriums verwendet.<sup>18</sup> Die wenigen Verweise auf „Cyber-Großmacht“ in externen Botschaften deuten darauf hin, dass Peking seine Ambitionen bei der Kommunikation mit ausländischen Zielgruppen absichtlich herunterspielt. Diese Vorsicht ist durchaus gerechtfertigt: Basierend auf den Vorträgen von Xi und den Verlautbarungen relevanter Funktionäre kommt der Abschnitt zum Schluss, dass das Konzept der „Cyber-Großmacht“ genau solche weitreichenden, wettbewerbsorientierten Ambitionen nahelegt, die im Ausland Besorgnis erregen dürften.<sup>19</sup>

Xi betont ausdrücklich, dass es sich bei seinem Programm um ein globales Programm handelt: Eine Cyber-Großmacht hat globalen Einfluss. Auf der Welt-Internet-Konferenz im Jahr 2015 erklärte er, dass „China energisch eine Strategie umsetzen wird, um das Land zu einer Cyber-Großmacht zu machen“, unter anderem durch den Aufbau einer „Gemeinschaft der gemeinsamen Ziele im Cyberspace“, einer globalen Internet-Infrastruktur und entsprechender Internet-Governance-Normen.<sup>20</sup> In ähnlicher Weise beschreibt ein Artikel von Beamten der Cyberspace Administration of China (CAC) in der führenden Parteipublikation Qiushi aus dem Jahr 2017<sup>21</sup> die Intensivierung des Einflusses Chinas auf die globale Internet-Governance als ein Hauptziel bei der Entwicklung des Status als „Cyber-Großmacht“.<sup>22</sup>

Diese Vision einer globalen Cyber-Großmacht beruht auf einer Wettbewerbsorientierung. Xi betrachtet die Informationsrevolution als Chance, den relativen Nachteil Chinas in den vergangenen industriellen Revolutionen aufzuholen. Er schlägt das Cyber-Großmachtkonzept als Fahrplan dafür vor. In einer weitreichenden Rede von 2016 erklärt Xi, wie wichtig es ist, vor dem Hintergrund der Demütigung Chinas in den Opiumkriegen und dem Scheitern des Landes bei der Industrialisierung im 20. Jahrhundert, das Land in eine Cyber-Großmacht zu verwandeln.<sup>23</sup> Er merkt an, dass China die industrielle Revolution verpasst hätte, die Informationsrevolution jedoch nutzen würde. In diesem Wettbewerb um den Cyberspace sagt Xi: „Die Gewinner werden sich freuen und die Verlierer werden zusammenbrechen.“<sup>24</sup>

Chinesische Beamte haben diese Betrachtungsweise übernommen. Beispielsweise argumentiert Chen Zhaoxiong, der stellvertretende Minister des MIIT, in einem 2019 im Journal of Military-Civil Fusion in Cyberspace veröffentlichten Artikel, dass die Welt einen Moment von historischer Bedeutung erlebe, der die Machtverhältnisse in der globalen Politik und Wirtschaft neu definieren könne – und dementsprechend einen Moment, in dem China die Gelegenheit hat, Macht hinzuzugewinnen. „Die aktuelle und zukünftige Phase stellt eine wichtige strategische Gelegenheit für China dar, um sich von einem großen Produktionsland und Cyber-Land in eine Produktions-Großmacht und Cyber-Großmacht zu verwandeln“<sup>25</sup>, schreibt er. Er stellt dies in einem weiter gefassten strategischen Kontext dar: „In der gesamten Geschichte der Zivilisation haben alle technologischen Revolutionen und industriellen Wandel unschätzbare Auswirkungen und Einflüsse auf die menschliche Gesellschaft herbeigeführt und tiefgreifende Anpassungen der weltweiten wirtschaftlichen und politischen Struktur ausgelöst.“ In solchen Zeiten des Wandels können diejenigen, die „den historischen Trend verstehen“ und „den ersten Schritt tun“ einige „Entwicklungsstufen überspringen“ und Wettbewerbsvorteile gewinnen.<sup>26</sup>

In einem 2017 veröffentlichten Artikel in der People's Daily betont Chen außerdem, dass der Cyberspace-Wettbewerb einer der großen Wettbewerbe um die Macht sei, und dass das Projekt „Cyber-Großmacht“ vom Sieg Chinas in diesem Wettbewerb abhängt. Er erklärt, dass der „Cyberspace zu einer neuen Arena für führende Länder geworden“ sei und viele „führende Länder der Welt das Internet als strategische Richtung des zukünftigen Wettbewerbs betrachten“. Daher werden sie „neue Generationen von Netzwerk-Informationstechnologie fördern und anwenden“ und „um eine Führungsrolle im Cyberspace konkurrieren“.<sup>27</sup> China sei hier keine Ausnahme: Vor dem Hintergrund „zunehmender internationaler Konkurrenz muss [China] die neuen Chancen in diesem neuen Zeitalter mit einem Gefühl der Dringlichkeit wahrnehmen“ und „den Aufbau neuer Vorteile im internationalen Wettbewerb“ sowie die Zusammenarbeit im digitalen Zeitalter beschleunigen. China müsse „eine Führungsposition im technologischen Wettbewerb langfristig und bezogen auf die Gesamtsituation erobern“.<sup>28</sup>

Diese Logik – dass die Informationsrevolution eine Gelegenheit für China darstelle, im Wettbewerb um die Entwicklung an die Spitze der globalen Ordnung zu gelangen – wird insbesondere in Diskussionen rund um die Telekommunikation deutlich. „5G hat sich zunehmend zu einer strategischen Führungsposition entwickelt, über die der langfristige Wettbewerbsvorteil des Landes zu sichern ist“, schreibt Duan Weilun,<sup>29</sup> stellvertretender Direktor des Büros der Führungsgruppe für die umfassende Reformvertiefung der Datang Telecom Group in einem Artikel aus dem Jahr 2020.<sup>30</sup>

Ein Artikel aus dem Jahr 2020 im Party & Government Forum, einem Journal der Parteischule der Kommunistischen Partei Chinas (CCP), formuliert es direkter: „Vor dem Internetzeitalter spielten europäische und amerikanische Länder eine führende Rolle bei der Bildung der neuen Weltwirtschaftsordnung, der politischen Ordnung und Rechtsordnung“, aber „im Zeitalter des Internets, insbesondere in der neuen Ära der Informatisierung, an deren Spitze 5G steht, ist es für China absolut möglich, voranzuschreiten und größere Beiträge zu leisten.“ Auch dieser Artikel lässt keine Zweifel daran, was die Beiträge Chinas mit sich bringen werden: „Wer im Internetzeitalter die Macht über den Diskurs [话语权] und die Macht über die Erstellung von Regeln [规则制定权] hat, hat die Macht, die Dominanz über die Zukunft [主导权] zu übernehmen.“ Aus dieser Perspektive bietet 5G eine „historische Chance“, auch in anderen Bereichen als Technologie eine Führungsposition einzunehmen und eine Chance, „Chinas internationale Wettbewerbsfähigkeit zu verbessern“, obwohl ähnliche revolutionäre Veränderungen in der Vergangenheit verpasst wurden.<sup>31</sup>

# Indigenisierung: Abhängigkeit als „versteckte Gefahr“ für China

*„Die Kontrolle der Kerntechnologien durch andere ist unsere größte versteckte Gefahr.“*  
– Xi Jinping, 2016<sup>32</sup>

Externe Diskurse zu Chinas digitalen Plänen verharmlosen chinesische Ambitionen, sich zu einer Cyber-Großmacht zu entwickeln. Die Bestandteile dieser Pläne werden in der Regel sogar völlig falsch dargestellt. Ein offensichtliches und anschauliches Beispiel dafür findet sich im Fokus, den Peking auf inländische Kerntechnologien und die Unzulänglichkeit der Marktmechanismen zum Schutz dieser Technologien legt.

Bei nach außen gerichteten Mitteilungen argumentieren die chinesische Regierung und Unternehmen häufig, dass freie Märkte anstelle von Politik die Telekommunikationslandschaft bestimmen sollten. Beispielsweise weisen Sprecher des Außenministeriums gegenüber ausländischen Zielgruppen häufig auf die Bedeutung von Marktprinzipien für Technologieentscheidungen hin. Mehrere Sprecher haben argumentiert, dass ein „fares, einfaches, offenes und nicht diskriminierendes Geschäftsumfeld“ nicht mit Einschränkungen oder Bedenken gegenüber Huawei vereinbar sei.<sup>33</sup> Die Sprecherin des Außenministeriums, Hua Chunying, erklärte im Juli 2020, dass solche Beschränkungen „offensichtlich gegen die Grundsätze der Marktwirtschaft und die Freihandelsregeln“ verstießen, und die Entscheidung des Vereinigten Königreichs, derartige Beschränkungen umzusetzen, zeige, dass die Briten „gegen die internationale Gemeinschaft“ seien.<sup>34</sup> In einer anderen Pressekonferenz argumentierte sie, dass „das, was die USA getan haben, deutlich zeigt, dass das Prinzip der Marktwirtschaft und des fairen Wettbewerbs, für das sie sich einsetzen, nichts anderes als ein Feigenblatt ist“ und dass das Verhalten der USA „gegen die Regeln des internationalen Handels verstößt“.<sup>35</sup>

Die innenpolitischen Aussagen Xis sowie die anderer Persönlichkeiten der chinesischen Regierung und Unternehmenswelt schlagen jedoch einen anderen Ton an. Sie unterstreichen, wie wichtig es ist, die Abhängigkeit von ausländischen Quellen der Kerntechnologien (核心技术) und den entsprechenden Beschränkungen durch freie Märkte zu reduzieren. Entsprechend unterstreichen sie die Notwendigkeit der Umsetzung von Industriepolitik. Diese Industriepolitik soll sich auf Fertigung und Lieferketten sowie auf Forschung und Entwicklung konzentrieren. Sie soll zudem eine enge Zusammenarbeit zwischen der Regierung und dem privaten Sektor bei nationalen und internationalen Geschäftstätigkeiten ermöglichen.

Xi hat wiederholt Kerntechnologien mit starker Entwicklung im eigenen Land und relativer Unabhängigkeit von anderen Ländern als Schlüsselfaktoren für den Aufbau einer Cyber-Großmacht betont. Dies obwohl China fortlaufend selbst Technologie exportiert, die internationale Abhängigkeiten erzeugt. In seiner ersten Hauptansprache 2014, die das Konzept einer „Cyber-Großmacht“ darlegt, betont Xi die Notwendigkeit, die Abhängigkeit von ausländischer Technologie zu verringern und „die einheimische Innovation (自主创新) in Kerntechnologien und Infrastrukturaufbau zu stärken“.<sup>36</sup> Er vertritt die Meinung, dass „China über eigene Technologie verfügen muss, und zwar über eine starke Technologie, um zur Cyber-Großmacht aufzusteigen“.<sup>37</sup> Wichtig ist, dass diese Rede – und damit auch Chinas Diskussion über die Auflösung der gegenseitigen technologischen Abhängigkeit – vor der Wahl von Donald Trump, dem Handelskrieg und der US-Rhetorik stattfand, die sich auf eine „Entkopplung“ konzentrierte.



Xi ging in einer wichtigen Rede zur Internetpolitik im Jahr 2016, ebenfalls vor der US-Wahl, auf seinen Kerntechnologiefokus ein. In dieser Rede formulierte Xi eine breite Definition des Begriffs „Kerntechnologie“: „Meiner Meinung nach besteht sie aus drei Aspekten. Der erste ist die grundlegende Technologie und die allgemeine Technologie, der zweite ist die asymmetrische Technologie oder die ‚Geheimwaffen‘-Technologie (杀手锏), der dritte ist modernste Technologie und revolutionäre Technologie.“<sup>38</sup> In einem bemerkenswerten Nachtrag erklärt Xi, dass der Schlüssel darin liege, dass „wir in diesen Bereichen an der gleichen Startlinie wie andere Länder stehen. Wenn wir unsere Lösung vor ihnen bereitstellen und uns auf die Forschung konzentrieren können, haben wir eine reale Chance, uns von unserer Schlusslichtposition vorzukämpfen und an die Spitze zu setzen.“<sup>39</sup> Mit anderen Worten: Kerntechnologieelemente werden nicht nur aufgrund ihres grundlegenden Charakters ins Auge gefasst, sondern auch aufgrund der aktuellen Position Chinas im internationalen Wettbewerb in diesem Bereich und des Potenzials, China letztendlich in Führung zu bringen.

Trotz dieser positiven Gesamtprognose weist Xi in der Rede auch auf die anhaltenden technologischen Defizite Chinas hin. „Im Vergleich zum fortschrittlichen Niveau der Welt und unserem strategischen Ziel, uns in eine Cyber-Großmacht zu verwandeln, sind wir bei vielen Aspekten immer noch im Rückstand“, sagt er, und fügt hinzu: „Der größte Rückstand besteht bei den Kerntechnologien.“<sup>40</sup> Er betont die damit einhergehenden Gefahren. „Die Kerntechnologie des Internets ist unsere größte ‚Hauptschlagader‘“, erklärt Xi und verwendete dabei einen Begriff (命门), der sich auf den lebenswichtigen Bereich des Körpers bezieht, der für Atmung, Verdauung und Fortpflanzung verantwortlich ist.<sup>41</sup> „Die Kontrolle der Kerntechnologie durch andere ist die größte versteckte Gefahr für uns.“<sup>42</sup>

China müsse daher unbedingt seine Kerntechnologien stärken. „Wenn wir bei Chinas Internetentwicklung die Initiative ergreifen und Internetsicherheit sowie nationale Sicherheit gewährleisten möchten, müssen wir das Problem der Kerntechnologien aus der Welt schaffen und versuchen, in bestimmten Bereichen in der Kurve zu überholen“<sup>43</sup>.<sup>44</sup> Die Begründung, die Xi für diese Behauptung gibt, bezieht sich sowohl auf die Abhängigkeit des Auslands von China als auch auf die Abhängigkeit Chinas von anderen::

Ganz gleich, wie groß ein Internetunternehmen und wie hoch sein Marktwert auch ist: Wenn es für seine Kernkomponenten stark von ausländischen Staaten abhängig ist und wenn die „Hauptschlagader“ der Lieferkette in den Händen anderer liegt, ist es so, als würde man ein Haus auf dem Fundament eines anderen bauen. So groß und schön es auch sein mag, hält es möglicherweise Sturm und Regen nicht stand, sondern fällt beim ersten Windstoß in sich zusammen.<sup>45</sup>

Zu diesem Zweck fordert Xi eine robuste Industriepolitik. China müsse „mehr Personal-, Material- und Finanzressourcen in die Forschung und Entwicklung von Kerntechnologien investieren“ sowie „unsere besten Kräfte sammeln und strategische Vorkehrungen treffen“, um der Zukunft zu begegnen. China müsse „einen Entwurf für die Entwicklungsstrategie von Kerntechnologien und -ausrüstung im Informationsbereich“ sowie „einen Fahrplan, einen Zeitplan, eine Liste von Aufgaben sowie kurzfristige, mittelfristige und langfristige Ziele formulieren.“ Und China müsse sich „genau darauf konzentrieren, eine strategische Führungsposition einzunehmen“.<sup>46</sup>

Nach Xis Dafürhalten sollte China dies auf einem Mittelweg zwischen absolutem Protektionismus<sup>47</sup> und Integration in die freie Marktwirtschaft anstreben<sup>48</sup>. „Kerntechnologien sind die wichtigste Waffe des Landes und die wichtigsten Kerntechnologien müssen auf einheimischer Innovation und Eigenständigkeit basieren“, erklärte er. Die freie Marktwirtschaft sei als Mittel dafür unzureichend. „Die Börse kann uns keine Kerntechnologien bringen und Geld keine Kerntechnologien kaufen. Wir müssen uns auf eigene Forschung und Entwicklung verlassen.“ Gleichzeitig sei jedoch in einem globalisierten Umfeld nicht zu erwarten, dass derartige Forschung und Entwicklung „hinter verschlossener Tür“ stattfinden können. Xi erklärt, dass „wir den Rückstand nur ermitteln können, wenn wir gegen die Besten antreten“.<sup>49</sup> China „würde keine neuen Technologien ablehnen“. Vielmehr würde das Land strategisch entscheiden, „welche davon [aus dem Ausland] eingeführt, aufgeschlossen, absorbiert und dann neu erfunden werden können“ und „welche davon durch eigene Innovation entwickelt werden müssen“.<sup>50</sup>

Xi stellt ferner klar, dass die chinesische Industriepolitik Lieferketten, die Produktionsbasis sowie Forschung und Entwicklung anleiten und unterstützen werde. Er erklärt, dass Kapazität ohne eine solide Produktionsbasis für Kerntechnologien „Arbeitsverschwendung“ wäre. „Im globalen Informationsbereich hat sich die Fähigkeit zur Integration von Innovationsketten, Produktionsketten und Wertschöpfungsketten zunehmend zum Schlüssel für Erfolg oder Misserfolg entwickelt“, und dies erfordere, dass „das Endergebnis der Technologieforschung und -entwicklung in der Kerntechnologie nicht nur technische Berichte, wissenschaftliche Forschungsarbeiten und Laborproben sein sollten, sondern [auch] Marktprodukte, technische Stärke und industrielle Stärke.“<sup>51</sup> Anders ausgedrückt: Wissenschaftliche Forschung wirft nur dann ausreichende Renditen ab, wenn sie von Lieferketten und der Stärke des verarbeitenden Gewerbes unterstützt wird.

Sowohl in der inländischen als auch in der internationalen Anwendung würde eine derartige Industriepolitik eine enge Zusammenarbeit zwischen der chinesischen Regierung und den Unternehmen des Landes erfordern. Xi erklärt in seiner Rede von 2016, dass „das Schicksal von [Technologie-]Unternehmen eng mit der Entwicklung des Landes verbunden ist“, dass private Unternehmen somit den Staat ebenfalls benötigten. „Ohne staatliche Unterstützung, ohne die Unterstützung der [chinesischen] Massen, ohne einen Dienst für das Land und die Menschen zu leisten, ist es für Unternehmen schwierig, stärker zu werden oder zu wachsen.“<sup>52</sup> Die staatliche Unterstützung würde sich auch auf den Betrieb der Unternehmen im Ausland erstrecken: Wie Xi im Jahr 2016 verdeutlicht, „müssen wir Chinas Internetunternehmen ermutigen und dabei unterstützen, global tätig zu werden ... und sich aktiv am Projekt „One Belt, One Road“ zu beteiligen. So können wir das Prinzip umsetzen, dass ‚[unsere] Informatisierung[stechnologie] alle Bereiche abdeckt, in denen unsere nationalen Interessen liegen‘.“<sup>53</sup> Xi hat sich noch nicht mit der Frage befasst, ob derartige globale Ambitionen für den Rest der Welt die gefährlichen Abhängigkeiten von ausländischer – in diesem Fall chinesischer – Technologie schaffen, die Peking im Inland so vehement zu vermeiden versucht.

In einem Artikel von Chen Zhaoxiong aus dem Jahr 2019 wird besonders auf die Defizite der Marktkräfte bei der Entwicklung von Kerntechnologien und damit auf die Notwendigkeit einer entsprechenden Industriepolitik hingewiesen. „Geld und die Marktwirtschaft“, so Chen, hätten „weder die Kerntechnologien eines Betriebssystems entwickelt“, noch es erlaubt, dass Technologie „aufgeschlossen, aufgenommen und neu erfunden“ wurde. China habe daher keine andere Wahl als die „einheimische Innovation“ zu unterstützen, um „ein sicheres und kontrollierbares Informationstechnologiesystem aufzubauen“.<sup>54</sup>

Andere chinesische Quellen wenden diesen Rahmen direkt auf 5G an. Ein Artikel in der dem MIT nahestehenden Zeitschrift *Communications World* aus dem Jahr 2017 ermutigt die Regierung beispielsweise, „Betreiber und zugehörige Abteilungen zu koordinieren, um einen nationalen Versuchsplan zur Vorbereitung auf die kommerzielle Nutzung von 5G effizient umzusetzen“ – ein Plan, mit dessen Implementierung China schließlich 2020 begann.<sup>55</sup> Auch Autoren der Shanxi University mahnen in einem Artikel des Magazins *International Economics and Trade* aus dem Jahr 2020 an, dass der Ausbau einer 5G-Branche einen „Top-Level-Entwurf“ der nationalen Verwaltungsabteilungen des Landes erfordere und die Regierung „auch finanzielle Unterstützung“ leisten müsse. Sie führen dies auf „langfristige Entwicklung und Erforschung“ in High-Tech-Branchen wie 5G zurück, die „große Summen kostet“. Anders gesagt: „Der Staat führt den Top-Level-Entwurf auf strategischer Ebene durch und setzt die branchenspezifischen Mittel rational ein.“<sup>56</sup>

## Cyber- und Netzwerksicherheit: „Offensiv wie defensiv“

*„Ohne Cybersicherheit gibt es keine nationale Sicherheit.“*

– Xi Jinping, 2014<sup>57</sup>

Chinesische externe Mitteilungen zu Cyber- und Netzwerksicherheit spielen auch die Risiken herunter, die ausländische Technologien wie die von Huawei für Informationssysteme darstellen könnten. Im Gegensatz dazu legt die chinesische Regierung im inländischen Diskurs Priorität auf die Sicherheit – und stellt „unabhängige und kontrollierbare“<sup>58</sup> IT-Systeme als Mittel dar, um diese zu erreichen. In China deuten akademische und kommerzielle Diskussionen über offensive Anwendungen von Informationsnetzwerken darauf hin, dass Sicherheitsbedenken bezüglich chinesischer Systeme durchaus gerechtfertigt sind. Peking könnte kommerzielle Telekommunikation und andere IT-Netzwerke als Mittel betrachten, um militärische Macht zu demonstrieren, sowie als Mittel zur Prägung von globalen Systemen und Diskursen nach seinen Interessen.

Hua Chunying, Sprecherin des Außenministeriums, beschreibt Bedenken hinsichtlich der Cyber- und Netzwerksicherheit als ein Beispiel dafür, wie Länder versuchen würden, „wirtschaftliche und technologische Probleme um jeden Preis zu politisieren“. In einer Rede im Jahr 2020 behauptet sie, dass Einschränkungen für Huawei „nicht nationaler Sicherheit, sondern politischer Manipulation“ dienen.<sup>59</sup> Noch eindeutiger formuliert Hua dies, als sie die „Förderung der nationalen Sicherheit“ als „lahme Ausrede der USA“ bezeichnet und behauptet, dass ausländische Bedenken von politisierten, „nicht vorhandenen Risiken“<sup>60</sup> getrieben würden, die auf einem „übertriebenen Konzept der nationalen Sicherheit“ beruhen.<sup>61</sup>

## *Unabhängige, kontrollierbare Technologien für die Cyber- und Netzwerksicherheit*

Auch wenn die USA möglicherweise das Konzept der nationalen Sicherheit überstrapaziert haben, so weist der nach innen gerichtete Diskurs in China auf eine gleichartige Haltung Pekings hin. Dieser Diskurs betont die entscheidende Bedeutung von Sicherheit in Informationsnetzwerken, die die Einführung unabhängiger, kontrollierbarer Technologien erfordert. In der Rede im Jahr 2014, in der Xi das Konzept einer „Cyber-Großmacht“ vorstellt und eine kleine Führungsgruppe mit der Aufgabe ins Leben ruft, dieses Ziel umzusetzen, erklärt er: „Ohne Cybersicherheit [oder Netzwerksicherheit]<sup>62</sup> gibt es keine nationale Sicherheit.“<sup>63</sup> Er führt zudem einen Satz ein, der sich zu einem Hauptbestandteil des chinesischen Telekommunikationsdiskurses entwickelt hat: „Cybersicherheit und Informatisierung sind zwei Flügel des gleichen Körpers und zwei Zahnräder des gleichen Motors“, sagte er. „Sie müssen auf einheitliche Weise geplant, bereitgestellt, erweitert und umgesetzt werden.“<sup>64</sup> Mit anderen Worten: Sicherheit steht im Mittelpunkt der digitalen Ambitionen Chinas. Diese wichtige Rolle der Sicherheit beim Aufbau einer „Cyber-Großmacht“ zieht sich nahezu konstant durch die wichtigsten Reden von Xi zum Thema.<sup>65</sup>

Der Diskurs, der auf diese Äußerungen Xis folgt, legt diesen Schwerpunkt auf die Sicherheit speziell in der Telekommunikation. Forscher am Investigation Technology Center of the Political and Legal Committee of the Central Military Commission (军委政法委侦查技术中心) betonen die Wichtigkeit von Sicherheit bei 5G:

Als moderne Kommunikationstechnologie von heute wird die Verbreitung von 5G neue Veränderungen in der Produktion und im Leben der gesamten Gesellschaft mit sich bringen. Die Sicherheit der zugehörigen Technologien und Anwendungen stehen in Bezug zur öffentlichen Sicherheit sowie zu militärischen Interessen und sollten aus Sicht der allgemeinen nationalen Sicherheit in die wesentlichen Überlegungen einbezogen werden.<sup>66</sup>

Der nationale chinesische Diskurs verweist auf „kontrollierbare“ (可控) Technologien und Systeme, um Sicherheit zu erreichen. Xi erklärt 2016, dass China vor der Einführung neuer Technologien überprüfen sollte, ob diese „sicher und kontrollierbar“ seien.<sup>67</sup> Auch im Jahr 2016 sagt er, China müsse „ein sicheres und kontrollierbares IT-System aufbauen“.<sup>68</sup>

Andere Quellen betonen die Notwendigkeit heimischer Technologien noch stärker. In einem Artikel in der Fachzeitschrift *Military-Civil Fusion in Cyberspace* aus dem Jahr 2019 argumentiert Chen Zhaoxiong, dass China „ein sicheres und kontrollierbares Informationstechnologiesystem aufbauen“ müsse, und zwar durch „einheimische Innovation“.<sup>69</sup> In einem Artikel aus dem Jahr 2015 erläutert ein Forscher an der Shanghai Academy of Social Sciences die Sicherheitsrisiken, die sich aus der Abhängigkeit von ausländischen Technologien in der IT ergeben: „Wir sind erst spät zur Informationstechnologie hinzugestoßen und vertrauen bei Kerntechnologien wie Chips und Betriebssystemen auf westliche Technologien.“ Dies führe zu einer Schwachstelle: „Die westlichen Länder unter der Führung der USA nutzen die technologische Industrie zur Entwicklung und Anpassung verschiedener Cyberwaffen, um Cyber-Überwachung, Cyber-Angriffe und Cyber-Abschreckung zu erreichen.“ Er kommt zum Schluss: „Wenn die Kerntechnologie nicht unabhängig und kontrollierbar ist, wird das von uns erschaffene Netzwerk ein ‚ungeschütztes Netzwerk‘ sein.“<sup>70</sup>

## *Militarisierte IT-Netzwerke*

Auf der nächsten Ebene zeigt die Analyse von akademischen und kommerziellen Quellen, dass Sicherheitsbedenken ausländischer Investoren in Bezug auf chinesische Technologien und Systeme möglicherweise nicht unangebracht sind. Peking könnte kommerzielle und zivile IT-Netzwerke als Werkzeuge zur offensiven Machtprojektion betrachten.<sup>71</sup> Diese Machtprojektion kann viele Formen annehmen. Auf herkömmlichster Ebene wird in China immer wieder über Informationsnetzwerke, Telekommunikationsnetzwerke eingeschlossen, als militärisch-zivile Fusionssysteme sowie über militärische Anwendungen von 5G gesprochen.

Militärisch-zivile Fusion bezieht sich auf die Integration militärischer und ziviler Ressourcen und Akteure sowie die gemeinsame Positionierung zur Verfolgung eines einheitlichen Ziels.<sup>72</sup> Xi erhob 2015 die militärisch-zivile Fusion zur Strategie auf nationaler Ebene.<sup>73</sup> Er hat wiederholt die wichtige Rolle der IT innerhalb dieser Strategie unterstrichen. Auf der Nationalen Arbeitskonferenz für Cybersicherheit und Informatisierung im Jahr 2018 erklärt Xi: „Die militärisch-zivile Fusion in den Bereichen Cybersicherheit und Informatisierung sind Schlüssel und Grenze der militärisch-zivilen Fusion im Allgemeinen. Darüber hinaus versprechen sie die größte Dynamik und das größte Potenzial für Fortschritte bei der militärisch-zivilen Fusion.“<sup>74</sup>

Nachgelagerte Diskussionen in China machen noch weniger einen Hehl aus der Beziehung zwischen Informationsnetzwerken und der militärisch-zivilen Fusion, sondern weisen explizit darauf hin, dass kommerzielle Netzwerke zu militärischen Zwecken eingesetzt werden können. Beispielsweise vertritt Qin An 2016 die Auffassung, dass „es aufgrund der stark monopolistischen Natur von Informationstechnologiesystemen unwahrscheinlich ist, dass es zwei verschiedene Systeme für die militärische und zivile Nutzung geben wird“, weshalb die beiden Systeme stattdessen tatsächlich ein einziges System formen würden. Darüber hinaus sei es angesichts Chinas „derzeitiger technologischer Grundlagen [...] für China äußerst schwierig, ein System zu entwickeln, das dem weltweiten Standard standhalten kann. Daher „ist es [für China] besonders wichtig, militärische und zivile Ressourcen über ein militärisch-ziviles Fusionssystem ineinander zu integrieren.“<sup>75</sup>

In diesem Sinne fordert Duan Weilun 2020 China auf, „die grundlegenden gemeinsamen Technologien des 5G-Netzwerksystems für die militärische und zivile Nutzung zu stärken und die tiefgreifende Entwicklung der militärisch-zivilen Fusion von 5G und seiner technologischen Entwicklung zu unterstützen sowie die großflächige Anwendung von autonomen und kontrollierbaren 5G-Technologien in militärischer Ausrüstung zu ermöglichen.“<sup>76</sup>

Ein Artikel in der Zeitschrift *National Defense* von Forschern der Academy of Military Science führt den Fusionsgedanken noch einen Schritt weiter. Die Autoren schlagen vor, dass „die militärische Anwendung von 5G-Technologie den evolutionären Gesetzen der Informatisierung folgen sollte“, zu denen die „globale Verbreitung“ von 5G-Technologie und die „umfassende Verknüpfung“ zwischen militärischen und zivilen Ressourcen gehören. Dementsprechend argumentieren sie, dass der Ausbau von 5G in China „eine enge Verbindung zwischen Friedenszeit und Kriegszeit“ schaffen sollte.<sup>77</sup>

Diese Darstellung lässt darauf schließen, dass chinesische Ansätze für 5G und andere Informationsnetzwerke sowie die darauf aufbauenden Technologien und Anwendungen militärische Zwecke von Anfang an beinhalten könnten. Zusätzliche Quellen bieten einen Einblick in spezifische militärische Anwendungsbereiche.

Informationsfähigkeiten bilden das Herzstück des militärischen Modernisierungsprogramms in China.<sup>78</sup> Zheng Anqi von der China Academy of Information and Communications Technology drückt es 2020 so aus: „Wenn moderne Streitkräfte über eine starke Informationsmacht verfügen, verfügen sie auch über eine starke militärische Macht.“<sup>79</sup> Laut Zheng muss das Militär „das Thema des Zeitalters im militärischen Informationskontext verstehen, während das Land die Strategie zum Aufbau einer Cybermacht umsetzt, brandneue Informationstechnologien und -konzepte aufnehmen und daraus lernen und die Entwicklung der 5G-Technologie nutzen, um vom Internet der Dinge, Big Data und Cloud Computing zu profitieren.“<sup>80</sup> Zheng fasst zusammen: „Die Grundlage einer Informationsmacht ist das Netzwerk. Ohne die Unterstützung allgegenwärtiger Breitband- und mobiler Netzwerke ist eine leistungsstarke Informationsarmee nichts als leere Worte.“<sup>81</sup> Ebenso erklären Forscher an der Academy of Military Sciences 2020, dass China „den Funktionen zukünftiger Kommunikationstechnologien, einschließlich großer Verbindungen, geringer Latenz, hoher Bandbreite und breiter Abdeckung, vollen Spielraum geben wird, um das intelligente Kampfsystem unseres Militärs mit leistungsstärkerer wissenschaftlicher und technologischer Unterstützung zu stärken.“<sup>82</sup>

Ein Artikel aus dem Jahr 2019 in der chinesischen Zeitschrift National Defense von Militärfunktionären und permanenten Fakultätsangehörigen der Academy of Military Sciences bietet eine aussagekräftige Zusammenfassung der militärischen Anwendungen von 5G. Sie schreiben, dass „5G-Technologie einen hohen Wert für militärische Anwendungen hat. Es ist von großer strategischer Bedeutung, die Chancen der militärischen Anwendung von 5G-Technologie zu nutzen.“<sup>83</sup> In ausschweifenden Worten gehen sie sowohl auf die militärisch-zivile Fusionsstrategie als auch die Informatisierung des Militärs ein und argumentieren, dass „die Mobilkommunikationstechnologie der fünften Generation (5G-Technologie) einen neuen Motor für die Modernisierung der militärisch-zivilen Fusion von Netzwerkinformationen darstellt und neue Unterstützung für ein starkes Militär durch Informationen bietet.“<sup>84</sup> Die Autoren weisen ferner darauf hin, dass der militärische Wert von 5G für offensive Zwecke verwendet werden sollte. Dabei muss China „die 5G-Technologieentwicklungsstrategie unserer Armee zur Abwehr des Gegners sorgfältig studieren sowie umfassend demonstrieren und formulieren“.<sup>85</sup>

Diese Autoren beschreiben eine Reihe von Anwendungsfällen für 5G. Erstens: Verbindungshaltung im Gefecht sowie Befehlsführung und Lenkung: Sie stellen fest, dass das chinesische Militär nach „der umfassenden Integration von Netzwerksystemen“ suche. In der Praxis besteht das Ziel darin, „gemeinsame Operationen [über] dreidimensionale Informationsnetzwerke an Land, zur See, in der Luft und im Weltraum sicher, schnell und nahtlos in jede Kampfeinheit und sogar Waffenplattform, Sensoren und andere Kampfausrüstung zu integrieren.“ Diese Ziele sind langfristig, aber die Autoren betonen, dass 5G die erforderlichen Funktionen bietet, um diese Vision eines vernetzten Schlachtfelds umzusetzen: „Die 5G-Technologie bietet technische Bedingungen für die Vernetzung verschiedener Waffensysteme, Informationssysteme und Befehlssysteme.“<sup>86</sup>

Zweitens: Fortschrittliche militärische Werkzeuge: Die Autoren der Zeitschrift National Defense skizzieren eine Fülle von Möglichkeiten, die 5G eröffnen könnte – von „projizierten virtuellen holografischen Bildern“ über das militärische Internet der Dinge bis hin zu militärischen Robotern.<sup>87</sup>

Drittens und allgemeiner: Kommunikation auf dem Schlachtfeld: „Verschiedene mobile Endgeräte können direkt 5G-Kommunikationsnetzwerke für die verschlüsselte Datenkommunikation verwenden, um dem Militär im Gefecht eine integrierte Kommunikation mit breiter Abdeckung, hoher Geschwindigkeit und hoher Kompatibilität zu bieten.“ Diese mobilen Endgeräte können in traditionellere militärische Netzwerke und Geräte integriert werden, z. B. „militärische Kommunikationssatelliten, Frühwarnflugzeuge und andere Ressourcen“, sodass „die Kommunikation nahezu störungsfrei ist, was die Kosten des Militärbetriebs erheblich senken kann.“<sup>88</sup>

Ein Artikel aus dem Jahr 2019 in der Zeitschrift Business Observation des General Managers für den Cloud-Computing-Geschäftszweig von China Telecom vertritt ebenfalls die Ansicht, dass „der qualitative Sprung in Übertragungsraten und Stabilität von 5G es aus militärischer Sicht ermöglicht, die Anforderungen zukünftiger Kommunikationsaufgaben im Gefecht problemlos zu erfüllen.“<sup>89</sup> 5G-Netzwerke könnten sogar zur Unterstützung einer global entsendeten VBA verwendet werden:

Sobald das 5G-Kommunikationssystem global bereitgestellt ist, wird es gleichwertige oder noch bessere Servicefähigkeiten im Vergleich zu militärischen Kommunikationssystemen bieten. Neben dem Zugriff auf taktische militärische Kommunikationsnetzwerke können verschiedene mobile Endgeräte für den militärischen Einsatz auch direkt 5G-Kommunikationsnetzwerke zur verschlüsselten Datenkommunikation nutzen, wodurch das Militär über integrierte Luft-Boden-Backup-Kommunikationsfunktionen verfügt, die die Informationsunterstützungsfunktionen im Gefecht erheblich verbessern können.<sup>90</sup>

Experten der Academy of Military Sciences haben in einem Artikel aus dem Jahr 2020 die Logistik als weitere militärische Anwendung hinzugefügt: „Die 5G-Technologie bringt Änderungen bei Modellen, Effizienzverbesserungen und wirtschaftliche Vorteile im Bereich ziviler Logistik mit sich. Es ist vorhersehbar, dass sie eine wichtige unterstützende Rolle beim Aufbau der intelligenten Logistik unseres Militärs spielen wird.“<sup>91</sup>

Sun Bolin vom Expert Advisory Working Committee of Chinese Society of Automation fasst den Wert dieser militärischen Anwendungen in einem Artikel aus dem Jahr 2020 zusammen und beschreibt ein Szenario für ein 5G-unterstütztes Kriegsszenario, das die Bedrohung eines militarisierten Telekommunikationsnetzwerks betont:

In der Anfangsphase eines Kriegs könnte 5G-Technologie das Befehlssystem und Logistikunterstützungssystem des Gegners komplett lahmlegen. So stünde das Ergebnis bereits fest, noch bevor es zu Kampfhandlungen gekommen ist. Die 5G-Kommunikationstechnologie stellt dem Militär ein integriertes Luft-Boden-Informationenkommunikationsnetzwerk mit einer breiten Abdeckung, Hochgeschwindigkeitsübertragung und starker Kompatibilität bereit, wodurch die Informationsunterstützung im Gefecht erheblich verbessert wird.<sup>92</sup>

## Informationsnetzwerke und eine neue Art von Sicherheitsbedrohung

Die Art der 5G-befähigten Machtprojektion geht weit über den herkömmlichen Sicherheitsbereich hinaus. Die Diskussion über Cyber- und Netzwerksicherheit in China basiert auf einem umfassenden Konzept dazu, was Sicherheit genau bedeutet und welche Sicherheitslücken die IT schafft. In dieser Konzeption der Netzwerk- und Cybersicherheit spielen wirtschaftliche, soziale und informative Bereiche neben dem militärischen Bereich eine Rolle. In diesen Bereichen können Informationsnetzwerke zu Einflussnahme, Ausübung von Druck oder Zerstörungen sowie für direkte Angriffe eingesetzt werden, beispielsweise durch die Verbreitung von Propaganda oder durch die Beeinflussung der Kapitalmärkte.

Chen Baoguo vom International Institute of Technology des Staatsrates erklärt in einem Artikel aus dem Jahr 2010, dass die Fortschritte in der IT mehr Einwirkung externer Akteure mit sich brächten, was die Souveränität eines Staates einschränken könnte:

Die neue Generation der Revolution der Informationstechnologie hat ... die gegenseitige Durchdringung und Abhängigkeit von Ländern erhöht ... Es ist für Länder schwierig geworden, ihre Souveränität in inneren Angelegenheiten, Diplomatie und Militär auf traditionelle und absolute Weise zu genießen. Im Zeitalter der Informatisierung und wirtschaftlichen Integration können Entscheidungen eines Landes kaum eigene Entscheidungen sein. In der Ära der neuen Generation revolutionärer Informationstechnologie werden absolute Souveränität und Unabhängigkeit, die ein Land traditionell genießt, durch eben diese neue Generation der Informationstechnologie intern und extern zunehmend untergraben und geschwächt.<sup>93</sup>

Zur Unterstützung seines Standpunktes erläutert Chen die Abhängigkeit nationaler und sozialer Systeme von Informationsnetzwerken und dementsprechend die Schwachstellen, die von diesen Netzwerken hervorgerufen werden:

Eine neue Generation revolutionärer Informationstechnologie hat dazu geführt, dass die nationalen Sicherheitsprobleme nicht mehr auf die militärische und wirtschaftliche Sicherheit beschränkt sind. Stattdessen wird die gesamte Gesellschaft immer stärker vom Internet abhängig. Eine neue Generation der IT-Revolution ist zum Rückgrat der Gesellschaft des 21. Jahrhunderts geworden – und das Internet zum Nervenzentrum eines Landes. Finanzen, Handel, Transport, Kommunikation, Bildung und Gesundheitssysteme, die über das Internet betrieben werden, bilden heute die Grundlage der nationalen wirtschaftlichen und gesellschaftlichen Entwicklung.<sup>94</sup>

Kurz gesagt bieten Informationsnetzwerke mehr Raum für Konflikte und Verbindungen und vergrößern so die Anfälligkeit. Ein Netzwerkangriff könnte die „Finanz-, Handels-, Transport-, Kommunikations-, Bildungs- und Gesundheitssysteme, die das Netzwerk nutzen“ bedrohen.<sup>95</sup>

Andere Quellen gehen über die Betrachtung der von Netzwerken erzeugten Schwachstellen hinaus und untersuchen die *Arten* von Bedrohungen, die in diesen Netzwerken entstehen. Dabei befassen sie sich nicht nur mit direkten Konfrontationen, sondern verweisen auch auf das Risiko, dass Informationssysteme verwendet werden könnten, um nationale Angelegenheiten in einer Weise zu beeinflussen, die die nationale Sicherheit und Autonomie beeinträchtigt. Liu Honglin von der Parteischule der Kommunistischen Partei Chinas in Shanghai warnt 2011 vor der „kulturellen Durchdringung, ideologischen Infiltration und politischen Infiltration“, die durch die IT begünstigt werden könnte:



Im Informationszeitalter gibt es mehrere Kulturen und viele Ideen. Westliche Länder nutzen die Vorteile der Informationstechnologie für kulturelle Durchdringung, ideologische Infiltration und politische Infiltration, um politische Ziele zu erreichen. Dies wird sich zweifellos auf die Ideologie und die ideologische Grundlage der Partei auswirken. Darüber hinaus hat das Informationsnetzwerk die einseitige Top-down-Kommunikation herkömmlicher Medien unterbrochen. Wie kann unsere Partei den Marxismus aufrechterhalten und entwickeln, dem Einfluss von Gedanken widerstehen und die Attraktivität der Parteiideologie stärken, wenn sie für ein noch größeres interaktives Informationsumfeld geöffnet wird?<sup>96</sup>

Ebenso beschreibt ein 2020 veröffentlichtes Projekt des National Social Science Fund die Gefahr von ideologischer Subversion und „kultureller Erosion“, die sich aus 5G und anderen neuen, grenzüberschreitenden technologischen Systemen ergibt: „Im neuen Zeitalter der Innovation und Anwendung neuer Technologien wie KI und 5G, ... steht die nationale kulturelle Sicherheit vor zahlreichen Herausforderungen, wie unzureichenden Innovationen in der Kulturtheorie, Schwächen in der Verbreitung der Mainstream-Ideologie und mangelnder Fähigkeit, die erodierenden Auswirkungen der westlichen Kultur zu beseitigen.“ Als Antwort darauf, so der Bericht, „sollte unser Land ausgehend von einem übergreifenden makrostrategischen Plan für die nationale Sicherheit ... ein nationales System zur Gewährleistung der kulturellen Sicherheit für ‚interne und externe Verknüpfungen‘ (内外联动) aufbauen, ‚sowohl offensiv als auch defensiv‘ (攻守兼备).“<sup>97</sup> Diese Idee, Angriff und Verteidigung zu verschmelzen, könnte darauf hindeuten, dass Peking nicht nur vor äußeren Einflüssen durch Informationsnetze schützen, sondern diese auch zur Projektion seiner eigenen Einflüsse nutzen will.

Im Jahr 2020 deutet der Sprecher des Außenministeriums Zhao Lijian an, dass die Verwendung von Geräten von Huawei durch andere Länder Spionage durch die USA verhindern würde: „Der Grund, warum die USA Huawei unterdrücken, könnte darin liegen, dass sie befürchten, nicht mehr ‚durch die Hintertür‘ lauschen zu können, wenn andere Länder Huawei verwenden.“<sup>98</sup> Diese Zeile ist ein Eingeständnis der Sicherheitsvorteile, die durch ausländische Informationsnetze gewonnen werden können. Sie wirft auch die Frage auf, wie sich dieses Sicherheitsbild entwickelt, wenn derartige Vorteile von einem Akteur beansprucht werden, der kommerzielle Netzwerke als Kriegsschauplatz für militärische und ideologische Konfrontationen betrachtet.

Ein Artikel aus dem Jahr 2017 von Long Zaiye, einem Forscher des Cyberspace Military-Civil Fusion Strategy Forum, liefert ein überzeugendes Porträt der Fusion von Angriff und Verteidigung in Bezug auf Netzwerk- und Cybersicherheit in China:

Auf dem Weg von einer Cyber-Macht zu einer Cyber-Großmacht war China lange Zeit in mühsame Kämpfe mit verschiedenen Oppositionskräften verwickelt. Wir müssen ... Fragen der Netzwerksicherheit koordinieren und erkennen, dass das Internet unsere Feinde und bewaffnete Konflikte näher gebracht hat. Unter den aktuell vorherrschenden Bedingungen haben wir den Kampf gegen Widersprüche und Konflikte gewonnen, Hindernisse beseitigt ... und mit dem Netzwerk-Inspektionsmodell effektiv auf die Fragen der öffentlichen Sicherheit der Informationsgesellschaft reagiert. Die konkrete Umsetzung konzentriert sich auf drei Aspekte: Erstens die globale Zielerhebung. Aufklärungsscreening und Clusteranalyse im Dragnet-Stil werden weltweit an vernetzten Zielen durchgeführt, und temporäre Sicherheitsbereiche und wichtige Inspektionsbereiche werden ausgewiesen. Der zweite Aspekt ist eine detaillierte Untersuchung feindseliger Ziele. Für nationale Ziele, die [China] als großen strategischen Gegner betrachten oder Feindseligkeiten ausgesetzt waren, werden wir Schlüsselinspektionen und stichprobenartige Inspektionen durchführen, um diese zu identifizieren. Der dritte Aspekt ist die Überprüfung der Kampfziele. Wir müssen regelmäßige Inspektionen von Ländern, Unternehmen oder persönlichen Zielen durchführen, die eine Gefahr für [China] darstellen könnten, und uns jederzeit die Möglichkeit vorbehalten, mit dem Ziel der Zerstörung zu kämpfen.<sup>99</sup>

## Definition von Standards: Chinas Suche nach „Diskursmacht“

*„Gegenwärtig ist das Cybersicherheitsspiel der Großmächte nicht nur ein Spiel der Technologie, sondern auch ein Spiel der Ideen und der Diskursmacht.“*

– Xi Jinping, 2016<sup>100</sup>

Informationstechnologien bieten eine subtilere, systemischere Form der Machtprojektion sowie der Definition von Standards. Der nach innen gerichtete Diskurs in China deutet auf wettbewerbsorientierte Ambitionen hin, internationale technische Standards zu setzen, um die globale Macht zu stärken.

Diese Ambitionen sucht man bei Diskussionen mit der Außenwelt vergeblich. Die nach außen gerichtete Kommunikation Pekings stellt die Definition von Standards als einen für beide Seiten vorteilhaften Bereich dar und fordert eine Zusammenarbeit und gemeinsame Entwicklung von Regeln. Bei der Erörterung der Global Data Security Initiative im Jahr 2020 behauptet der Sprecher des Außenministeriums, Zhao Lijian, China habe versucht, „einen Entwurf für die Formulierung globaler Standards“ zu liefern, indem es sich auf integrative Konzepte von „gegenseitigem Respekt und gemeinsamer Governance“ stütze, um „gegenseitiges Vertrauen aufzubauen und die Zusammenarbeit zu vertiefen“ sowie „Multilateralismus“ und neue Wege zur „Zusammenarbeit mit anderen“ zu unterstützen. Zhao erklärt, dass „umfassende Beratung und ein gemeinsamer Beitrag zum gemeinsamen Nutzen der richtige Weg ist“, wenn China „eine Gemeinschaft mit einer gemeinsamen Zukunft im Cyberspace“ aufbauen will.<sup>101</sup> In einem Artikel in der People’s Daily von 2016 heißt es ebenfalls: „China und die Vereinigten Staaten brauchen eher Netzwerkzusammenarbeit als Konfrontation ... für eine Win-Win-Zusammenarbeit und gemeinsame Erarbeitung von Verhaltenskodizes im Netzwerk.“<sup>102</sup>

Chinas intern ausgerichteter Diskurs erzählt jedoch eine ganz andere Geschichte. Die Definition von Standards ist ein Mittel, um zukünftige Technologien anzuführen oder sogar zu dominieren – und damit die neue Weltordnung anzuführen oder zu dominieren. Standards werden durchgehend als Nullsummen-, Wettbewerbs- und Instrumente nationaler Macht definiert. Ein Artikel aus dem Jahr 2015 in der *Zhejiang Daily* des damaligen stellvertretenden Direktors des Policy Research Office des Parteikomitees der Provinz Zhejiang, der sich deutlich von der öffentlichen Linie des Außenministeriums unterscheidet, liefert ein kurzes Beispiel für den wettbewerbsorientierten strategischen Wert, den China Standards zuweist:

Im Rahmen der wirtschaftlichen Globalisierung und der modernen Marktwirtschaft ... bedeuten Standards die Führungsposition, die Diskursmacht und die Macht zur Kontrolle. Daher gilt: Wer den Standard prägt, prägt die Welt („得标准者得天下“), und: Erstklassige Unternehmen verkaufen Standards, zweitklassige Unternehmen verkaufen Marken und drittklassige Unternehmen verkaufen Produkte („一流企业卖标准、二流企业卖品牌、三流企业卖产品“).<sup>103</sup>

Die höchsten Ebenen der Partei, einschließlich Xi, haben diesen Schwerpunkt auf Standards ebenfalls aufgegriffen. Sie haben auch eine Rolle der Regierung bei der Leitung der Bemühungen zur Festlegung technischer Standards umrissen. 2016 erklärt Xi, China werde „eine Standardisierungsstrategie aktiv umsetzen“<sup>104</sup>, um die chinesischen technischen Standards zu stärken und zu exportieren.<sup>105</sup> „Wir müssen die internationale Diskurs- und Regelmacht Chinas im Cyberspace beschleunigen und unermüdliche Anstrengungen unternehmen, um das Ziel des Aufbaus einer Cyber-Großmacht zu erreichen“, so Xi damals.<sup>106</sup> Im März 2018 startete Peking das Projekt „China Standards 2035“ unter der Leitung der Chinese Academy of Engineering.<sup>107</sup> Nach einer zweijährigen Forschungsphase entwickelte sich dieses Projekt im Januar 2020 zur National Standardization Development Strategy Research weiter.<sup>108</sup> In den vom National Standardization Committee Chinas im März 2020 herausgegebenen „Hauptpunkten der Standardisierungsarbeit im Jahr 2020“ wurden die Absichten dargelegt, „die Interaktion zwischen der Standardisierungsstrategie und den wichtigsten nationalen Strategien zu stärken.“<sup>109</sup>

Der Diskurs in China deutet ebenfalls nicht darauf hin, dass die Definition von Standards kooperativ erfolgen soll. Ein Direktor der Chinesischen Akademie der Wissenschaften erklärt 2016, dass die verschiedenen von Xi vorgebrachten „Prinzipien“ für die Steuerung des Cyberspace „auch von allen Ländern der Welt anerkannt werden und zu den grundlegenden Standards für die Internet-Governance in allen Ländern werden sollten“.<sup>110</sup>

Chinas Standardisierungsambitionen erstrecken sich auf alle Felder. Sie gelten sowohl für Hochgeschwindigkeitszüge als auch für die Telekommunikation. Peking scheint sich jedoch besonders auf aufstrebende Bereiche zu konzentrieren, d. h. Bereiche, in denen noch keine globalen Standards definiert wurden und China daher die Möglichkeit hat, etablierte Mächte auszuhebeln.<sup>111</sup> Die Hauptpunkte der nationalen Standardisierungsarbeit im Jahr 2020 umfassen beispielsweise Anstrengungen in aufstrebenden Branchen (z. B. intelligente Fertigung, neue Energie und energieeffiziente Transportsysteme, fortschrittliche Materialien) aufkommende Prioritäten (z. B. COVID-19-Prävention und -Kontrolle), Biotechnologie (z. B. biobasierte Materialien und fortschrittliche medizinische Geräte), Service-Infrastruktur (z. B. E-Commerce, Finanzen, Sozialkredite und Logistik) und Informationstechnologie (z. B. das Internet der Dinge, Cloud Computing, Big Data, 5G, Smart Citys, geografische Informationen).<sup>112</sup>

Wie aus dieser Taxonomie hervorgeht, spielen 5G und Informationstechnologie im weiteren Sinne eine zentrale Rolle in Chinas Agenda zur Definition von Standards. Die chinesische Regierung unterstützt und organisiert die Verbreitung von Telekommunikationsstandards. Xi erklärt 2016, dass China „die Reform des globalen Internet-Governance-Systems fördern“ wird, sowohl über bestehende Institutionen wie die Vereinten Nationen als auch über neue, in China geführte Mechanismen wie die Initiative „One Belt, One Road“ und untergeordnete Projekte wie die „Digitale Seidenstraße“.<sup>113</sup> Zhao Dachun, ein Abgeordneter des Nationalen Volkskongresses und stellvertretender Generaldirektor von China Mobile, verdeutlicht 2018 die zentrale Rolle des Staates bei der Organisation und Förderung von Telekommunikationsstandards. „Im Hinblick auf die Definition der Standards für 5G, die Zuweisung von Bandbreiten, die Ausstellung von Lizenzen, die technische Verifizierung und die industrielle Verbreitung“, erklärt er, „werden die Regierung und die zuständigen Abteilungen ein Design der obersten Ebene anfertigen und relevante politische Unterstützung bereitstellen, um die Entwicklung der 5G-Branche zu beschleunigen.“<sup>114</sup>

Ein weiteres Mal wird die Rolle des Staates bei der Definition von Standards und dem Schwerpunkt auf 5G durch Tong Guohua, Vorsitzender und Sekretär des Party Committee of China Information and Communication Technology Group, 2018 aufgegriffen, als er verspricht, dass „wir für die zukünftige Richtung der Industrieentwicklung den Anweisungen des Generalsekretärs Xi und des strategischen Einsatzes der staatlichen Kommission für die Überwachung und Verwaltung von Vermögenswerten des Staatsrates zur Bildung von sechs Industrielayouts folgen, die sich unter anderem auf 5G-Standards konzentrieren“.<sup>115</sup>

In einem Artikel aus dem Jahr 2020 beschreibt Duan Weilun den Erfolg dieses Ansatzes:

Nach jahrelangen Bemühungen, [anderen] bei 2G zu folgen, bei 3G aufzuholen und uns [mit anderen] bei 4G abzustimmen, hat China die Führungsgruppe bei der 5G-Entwicklung erreicht und die Führung in der technologischen Innovation übernommen. Chinesische Unternehmen waren vollumfänglich an der Formulierung internationaler 5G-Standards beteiligt, haben die internationale Kooperationen bei 5G gestärkt und mit internationalen Unternehmen zusammengearbeitet, um die Definition eines weltweit einheitlichen 5G-Standards zu fördern.<sup>116</sup>

Duan unterstützt die Behauptung mit empirischen Ermittlungen: „Im April 2019 lag die Anzahl der SEP-Anträge (Standards-Essential Patents) für 5G-Kommunikationssysteme chinesischer Unternehmen mit 34 % an der ersten Stelle der Welt.“<sup>117</sup> Die wichtigsten Akteure, die diese Anträge eingereicht haben, waren Huawei, ZTE und das –Institute of Telecommunications Science and Technology.<sup>118</sup> Anschließend stellt Duan Bemühungen vor, mit denen China seine Erfolge bei Standards fördern könnte, und fordert chinesische Unternehmen auf, die International Standardization Organization, die International Electrotechnical Commission und die International Telecommunications Union einzubeziehen, um „aktiv an der Formulierung von 5G und anderer internationaler Standards für Informationstechnologie und Netzwerksicherheit der nächsten Generation teilzunehmen ... und Chinas internationale Stimme und seinen Einfluss bei der Formulierung internationaler Standards für die Sicherheit des Netzwerkraums weiter zu verbessern.“<sup>119</sup>

Der chinesische Diskurs beschreibt klar die globalen Wettbewerbsambitionen, die diesen staatlich geführten Bemühungen zur Gestaltung von Telekommunikationsstandards zugrunde liegen. Ein Artikel von Autoren der Academy of Military Sciences<sup>120</sup> in der chinesischen Zeitschrift National Defense aus dem Jahr 2019 bietet eine klare Zusammenfassung dessen, was auf dem Spiel steht:

Die Kerntechnologie von 5G ist fast völlig neu. Wer das Modell, die Architektur und die Standards der 5G-Technologie zuerst beherrscht, hat das Recht, im zukünftigen Mobilfunknetz zu sprechen, und sichert den Vorteil des frühen Vogels in der Industriekette. Diese ermöglicht eine strategische Führungsposition im künftigen wirtschaftlichen Handel und im militärischen Wettbewerb.<sup>121</sup>

Diese Zeilen deuten darauf hin, dass nur ein einziger Beteiligter diese „strategische Führungsposition“ beanspruchen kann. Dies wird auch an anderer Stelle explizit betont. Shenzhen Commercial Daily nannte 5G im Jahr 2019 „Winner takes all“ (赢家通吃).<sup>122</sup> Miao Wei, Leiter des Ministeriums für Industrie und Informationstechnologie, hat dieses Argument selbst bestätigt. In einer Rede von 2020 sagt Miao Wei: „Im Zeitalter von 3G gab es drei globale Standards, im Zeitalter von 4G zwei globale Standards und im Zeitalter von 5G einen einheitlichen globalen Standard.“<sup>123</sup>

Warum sind diese „Winner takes all“-Standards von 5G strategisch so wichtig? Zum Teil, so argumentiert Tong Guohua, weil China, wenn es diese Standards definieren kann, seine Technologie und Netzwerke besser kontrollieren und so die nationale Autonomie unterstützen kann. „Die Standards selbst zu beherrschen und Netzwerke selbst aufzubauen“, schreibt er 2018, „bedeutet große Garantien für Informationen und sogar für die nationale Sicherheit.“<sup>124</sup>

Aber 5G-Standards – und die der Informationstechnologie im weiteren Sinne – bieten auch strategischere, potenziell offensivere und grundlegendere Vorteile. Der chinesische Diskurs legt nahe, dass die IT-Standards die Architektur der neuen IT-Welt bestimmen werden. Die Definition dieser Standards bietet daher die Möglichkeit, die Regeln der zukünftigen Welt zu schreiben und dabei die westliche Ordnung auszuhebeln oder gar zu ersetzen. Ein Artikel aus dem Jahr 2020 in der Chinese Cadres Tribune macht es deutlich:

Wer im Internetzeitalter die Macht über den Diskurs und Macht über die Erstellung von Regeln hat, hat die Macht, die Dominanz über die Zukunft zu übernehmen ... Vor dem Internetzeitalter spielten europäische und amerikanische Länder eine führende Rolle bei der Bildung der neuen Weltwirtschaftsordnung, der politischen Ordnung und Rechtsordnung, aber im Zeitalter des Internets, insbesondere in der neuen Ära der Informatisierung, an deren Spitze 5G steht, ist es für China absolut möglich, voranzuschreiten und größere Beiträge zu leisten. Die historische Chance, die das Internet bietet, wird sicherlich zu einem wichtigen Schub für die Verbesserung der internationalen Wettbewerbsfähigkeit Chinas.<sup>125</sup>

Diese Beschreibung der „Ära der Informatisierung, an deren Spitze 5G steht“ ist von entscheidender Bedeutung. Sie erklärt die übergroße Bedeutung, die China 5G offenbar bei seinen größeren Anstrengungen zur Definition der Architektur des Informationszeitalters zuweist. 5G wird als eine Art Standard der Standards beschrieben – ein System, das eine Reihe von Technologien, Funktionen und Standards unterstützt und somit das IT-Ökosystem im Allgemeinen definiert. In einem Interview aus dem Jahr 2018 erklärt Zhao Dachun dies ganz sachlich:

Die Forschung an und Entwicklung von 5G ist eine wichtige Maßnahme zum Aufbau der Cybermacht und zur Entwicklung der digitalen Wirtschaft. Sie kann die Entwicklung des Internets der Dinge, des industriellen Internets der Dinge usw. vorantreiben, die digitale Transformation der gesamten Industrie ermöglichen und starke Unterstützung beim Aufbau einer intelligenten Gesellschaft leisten.<sup>126</sup>

Im selben Jahr drückt Tong Guohua<sup>127</sup> es etwas anders aus:

Die große Bedeutung von 5G für die Entwicklung des Landes [China] besteht darin, dass es Anwendungen in verschiedenen Branchen obsolet machen wird und dann die Entstehung neuer Standards und Ökosysteme in verschiedenen Branchen auslösen wird. Man kann sagen, dass der Wettbewerb um die führende Position der 5G-Technologie für das Wirtschaftswachstum und die Wettbewerbsfähigkeit des Landes oberste Priorität hat.<sup>128</sup>

Chen Baoguo fügt dem Bild in einem vorausschauenden Artikel aus dem Jahr 2010 eine weitere Ebene hinzu und stellt fest, dass das Ökosystem von Standards und Netzwerken, das 5G stärken soll, nicht nur die virtuelle, sondern auch die physische Informationswelt umfassen wird:

Die Technologie des Internets der Dinge ermöglicht es, die reale Welt über das Netzwerk zu steuern ... In der Vergangenheit wurde die physische Infrastruktur im Allgemeinen als getrennt von der Informationstechnologie-Infrastruktur betrachtet: Flughäfen, Autobahnen, Gebäude einerseits und andererseits Rechenzentren, PCs, Breitband usw. Im Zeitalter des Internets der Dinge werden Stahlbeton, Kabel, Chips und Breitband zu einer einheitlichen Infrastruktur zusammengefasst. In diesem Sinne sind Netzwerk und Realität zu einem integralen Ganzen geworden.“<sup>129</sup>

Die Welt, die durch die Festlegung von 5G-Standards definiert werden kann, erstreckt sich über die reale und die virtuelle Welt und gewährt nicht nur Macht über die Bewegung von Informationen, sondern auch über den physischen Raum.

All diese Punkte – die Rolle des Staates bei der Festlegung von 5G-Standards, ihre „Winner takes all“-Natur, ihre Rolle bei der Förderung der größeren Ökosysteme, die das Informationszeitalter bestimmen, und die Kontrolle, die diese Ökosysteme über die virtuelle und physische Welt bieten, – verbinden sich im chinesischen Diskurs, um 5G-Standards als wettbewerbsorientierte und strategisch bestimmende Domäne zu definieren. „China dominiert weiterhin den globalen Standard der mobilen Kommunikation“, so Tong Guohua in einem Interview aus dem Jahr 2017. Er fährt fort: „Das Überholen im 5G-Zeitalter bieten uns eine seltene historische Chance.“<sup>130</sup>

China hat außerdem die Chance, den USA und dem Westen die Zügel bei den internationalen Standards aus der Hand zu nehmen und so deren Einfluss zu untergraben. Die Kontrolle über globale Standards – und insbesondere der Informationstechnologie-Standards – wird konsequent als das Herzstück der weltweiten Macht der USA und des Westens beschrieben. Yang Zhen, damals Vorsitzender des Council of Jiangsu Institute of Communications, sagt im Jahr 2010:

Die Standards und Kerntechnologien des Internets werden von den USA festgelegt. Das Internet ist nur eine virtuelle Welt, und das Internet der Dinge ist ein riesiges System, das alle Dinge der Welt verbindet ... Wenn die wichtigsten Technologien und Hauptstandards des Internets der Dinge in den westlichen Industrieländern liegen und [China] keine unabhängigen geistigen Eigentumsrechte hat, dann hat China keine Chance, seinen friedlichen Aufstieg und eine nationale Verjüngung zu erreichen.<sup>131</sup>

## Schlussfolgerung

Eine neue digitale Architektur nimmt Form an. Diese Architektur wird Kommunikations- und Ressourcenflüsse, Sicherheit und Wohlstand, globale Normen und Informationen prägen. Sie wird die Grundlage für das internationale Kräfteverhältnis und die Art und Weise bilden, wie Macht innerhalb dieses Systems eingesetzt werden kann.

Peking bereitet sich darauf vor, eine zentrale Rolle bei der Entwicklung dieser Architektur zu spielen – und diese Entwicklung sogar anzuführen. Dabei verbreitet die chinesische Regierung eine Reihe von Annahmen und Zielen nach außen, die im Widerspruch zur internen Botschaft stehen. Dass China zwei Sprachen spricht, ist keine neue Erkenntnis. Die wesentlichen Unterschiede zwischen diesen Sprachen in der IT sind jedoch weitgehend undokumentiert – trotz des zunehmenden Einflusses Chinas auf internationale IT-Infrastrukturen, -Technologien und -Normen.

## 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.

**Emily de La Bruyère** ist Mitbegründerin von Horizon Advisory, einem geopolitischen Beratungsunternehmen, sowie Senior Fellow der Foundation for Defense of Democracies (FDD). Ihre Arbeit konzentriert sich auf Chinas Standardisierungsambitionen, die militärisch-zivile Fusionsstrategie und die Plattform-Geopolitik sowie deren Auswirkungen auf die globale Sicherheit und Wirtschaftsordnung. Sie besitzt einen Bachelor of Arts *summa cum laude* von der Princeton University und einen Master of Arts *summa cum laude* von Sciences Po, Paris, wo sie Michel David-Weill-Fellow war.

**Nathan Picarsic** ist Mitbegründer von Horizon Advisory, einem geopolitischen Beratungsunternehmen, sowie Senior Fellow der Foundation for Defense of Democracies (FDD). Seine Forschung konzentriert sich auf die Entwicklung von Wettbewerbsstrategien als Reaktion auf die asymmetrische Ausrichtung der Kommunistischen Partei Chinas im globalen Wirtschafts- und Sicherheitswettbewerb. Er hat einen Bachelor of Arts des Harvard College und absolvierte Executive Education-Programme der Harvard Business School und der Defense Acquisition University.

**John Ferguson** ist ein ehemaliger Praktikant von Brookings beim Center for East Asia Policy Studies und der China Strategy Initiative. Er wird im Mai 2022 seinen Abschluss an der Harvard University machen und gleichzeitig in vier Jahren sowohl einen Bachelor of Arts in Government als auch einen Master of Arts in Regional Studies-East Asia abschließen. Zuvor war er Forschungspraktikant beim Director des Carnegie-Tsinghua Center for Global Policy und leitete die Harvard Undergraduate Foreign Policy Initiative.

## Danksagungen

Die Autoren möchten den ehemaligen Praktikanten Isabella Lu, Gaoqi Zhang und Zijin Zhou für ihre Forschungsunterstützung bei diesem Projekt, Anna Newby und Ted Reinert für die Korrektur dieser Abhandlung und Chris Krupinski für das Layout danken. 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.*

## Referenzen

---

<sup>1</sup> Das Untersuchungsteam der vorliegenden Abhandlung erhielt Kopien der E-Mails zwischen dem Beratungsservice der Zeitschrift und Autoren, die man mit dem Verfassen von Inhalten im Namen von Huawei zu beauftragen hoffte.

<sup>2</sup> Der Begriff „Cyber“ (网络) in „Cyber-Großmacht“ kann auch als „Netzwerk“ übersetzt werden. Dieser Bericht stützt sich auf die Übersetzung „Cyber-Großmacht“, erkennt jedoch an, dass hier Interpretationsspielraum besteht. Tatsächlich bevorzugt mindestens einer der Autoren die Übersetzung „Netzwerk-Großmacht“, basierend auf den Anstrengungen, die am häufigsten mit den Bemühungen um dieses Konzept assoziiert werden. (Siehe: Emily de La Bruyère, „The Network Great Power Strategy: A Blueprint for China’s Digital Ambitions“, The National Bureau of Asian Research, Veröffentlichung im Laufe von 2021.)

<sup>3</sup> 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung], (Rede, Peking, 25. April 2016), [http://www.xinhuanet.com/politics/2016-04/25/c\\_1118731175.htm](http://www.xinhuanet.com/politics/2016-04/25/c_1118731175.htm).

<sup>4</sup> 习近平 [Xi Jinping], „习近平：把我国从网络大国建设成为网络强国-高层动态-新华网“ [Xi Jinping: Entwicklung Chinas von einem führenden Cyber-Land zu einer Cyber-Großmacht], Xinhua, 27. Februar 2014, [http://www.xinhuanet.com/politics/2014-02/27/c\\_119538788.htm](http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm).

<sup>5</sup> 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung].



- 
- <sup>6</sup> Hua Chunying, „Reguläre Pressekonferenz der Sprecherin des Außenministeriums Hua Chunying am 15. Juli 2020“, (Rede, Peking, 15. Juli 2020), [https://www.fmprc.gov.cn/mfa\\_eng/xwfw\\_665399/s2510\\_665401/t1797967.shtml](https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1797967.shtml); Hua Chunying „Reguläre Pressekonferenz der Sprecherin des Außenministeriums Hua Chunying am 11. Dezember 2020“ (Rede, Peking, 11. Dezember 2020), [https://www.fmprc.gov.cn/mfa\\_eng/xwfw\\_665399/s2510\\_665401/2511\\_665403/t1839583.shtml](https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1839583.shtml).
- <sup>7</sup> „中央网络安全和信息化领导小组第一次会议召开“ [Erstes Treffen des Führungskomitees für zentrale Cybersicherheit und Informatisierung hat stattgefunden], 中央政府门户网站 [Portal der Zentralregierung], 27. Februar 2014, [http://www.gov.cn/ldhd/2014-02/27/content\\_2625036.htm](http://www.gov.cn/ldhd/2014-02/27/content_2625036.htm).
- <sup>8</sup> „习近平称努力让关键核心技术自主可控 促产业迈向全球价值链中高端“ [Xi Jinping kündigte Bemühungen an, wichtige Kerntechnologien unabhängig und kontrollierbar zu gestalten und die Branche zu ermutigen, sich dem oberen Ende der globalen Wertschöpfungskette zuzuwenden], Reuters, 28. Mai 2018, <https://cn.reuters.com/article/china-xi-jinping-tech-value-chain-0528-idCNKCS1I10XT>; 陈肇雄 [Chen Zhaoxiong], „推进工业和信息化高质量发展“ [Förderung der hochwertigen Entwicklung der Branche und Informatisierung], 网信军民融合 [Militärisch-zivile Zusammenarbeit im Cyberspace], 9. Juli 2019, CNKI: F424;F49.
- <sup>9</sup> „习近平称努力让关键核心技术自主可控 促产业迈向全球价值链中高端“ [Xi Jinping kündigte Bemühungen an, wichtige Kerntechnologien unabhängig und kontrollierbar zu gestalten und die Branche zu ermutigen, sich dem oberen Ende der globalen Wertschöpfungskette zuzuwenden], Reuters.
- <sup>10</sup> 习近平 [Xi Jinping], „习近平：自主创新推进网络强国建设“ [Xi Jinping: Unabhängige Innovationen begünstigen den Aufbau einer Cybermacht], 新华 [Xinhua], 21. April 2018, [http://www.xinhuanet.com/politics/2018-04/21/c\\_1122719810.htm](http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm).
- <sup>11</sup> 秦安 [Qin An], „网络强国的意识认识共识“ [Bewusstsein, Verständnis und Konsens einer Cybermacht], 中国信息技术安全评估中心 [China Information Security], 9 (2016), CNKI: TP393.08.
- <sup>12</sup> 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung].
- <sup>13</sup> 郭占恒 [Guo Zhanheng], „习近平标准化思想与浙江实践“ [Xi Jinpings Standardisierungsgedanke und Herangehensweise für Zhejiang], 浙江日报 [Zhejiang Daily], 25. September 2015, CNKI: F203;F092.7. Beide zitierten Sätze sind bei der Erörterung von Standards in chinesischen Unternehmen und in der Politik häufig zu finden.
- <sup>14</sup> 陈肇雄 [Chen Zhaoxiong], „加快推进新时代网络强国建设“ [Beschleunigen des Aufbaus einer Cybermacht in der neuen Ära], *People's Daily*, 17. November 2017, <http://opinion.people.com.cn/n1/2017/11/17/c1003-29651140.html>.
- <sup>15</sup> Siehe Endnote 2.
- <sup>16</sup> Das Führungskomitee für zentrale Cybersicherheit und Informatisierung wird als 中央网络安全和信息化领导小组 bezeichnet und im März 2018 in ein Amt umgewandelt: 中央网络安全和信息化委员会.
- <sup>17</sup> „中央网络安全和信息化领导小组第一次会议召开“ [Erstes Treffen des Führungskomitees für zentrale Cybersicherheit und Informatisierung hat stattgefunden] 中央政府门户网站 [Portal der Zentralregierung].“
- <sup>18</sup> Der Service Oriprome wurde verwendet, um den Ausdruck 网络强国 zu suchen. Xi Jinping und Wang Huning, langjähriges Mitglied des ständigen Ausschusses des Politbüros, haben diesen Ausdruck bei der Welt-Internet-Konferenz mindestens zweimal verwendet, jedoch mit viel weniger Details als in Reden, die auf das inländische Publikum abzielen, und nicht in letzter Zeit.
- <sup>19</sup> Eine Liste der relevanten Reden und Zitate von Xi finden Sie unter: 习近平 [Xi Jinping], „习近平谈加快建设网络强国-中共中央网络安全和信息化委员会办公室“ [Xi Jinping spricht über die Beschleunigung des Baus eines Cyberpower-Büros des CPC-Zentralkomitees für Cybersicherheit und Informationstechnologie], 9. September 2019, [http://www.cac.gov.cn/2019-09/11/c\\_1569738113999057.htm](http://www.cac.gov.cn/2019-09/11/c_1569738113999057.htm); siehe auch Paul Triolo, Lorand Laskai, Graham Webster und Katharin Tai, Xi Jinping Puts ‘Indigenous Innovation’ and ‘Core Technologies’ at the Center of Development Priorities“, *New America*, 1. Mai 2018, <http://newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/>.
- <sup>20</sup> 习近平 [Xi Jinping], „习近平在第二届世界互联网大会开幕式上的讲话“ [Rede von Xi Jinping zur Eröffnungszereemonie der zweiten Welt-Internet-Konferenz], (Rede, Wuzhen, 16. Dezember 2015), [http://www.xinhuanet.com/politics/2015-12/16/c\\_1117481089.htm](http://www.xinhuanet.com/politics/2015-12/16/c_1117481089.htm).

- 
- <sup>21</sup> Die CAC ist die Internetaufsicht Chinas. Der Artikel stützt sich auf Analysen der Aussagen Xi Jinpings.
- <sup>22</sup> „深入贯彻习近平总书记网络强国战略思想 扎实推进网络安全和信息化工作“ [Eingehende Umsetzung des strategischen Denkens von Generalsekretär Xi Jinping in Bezug auf die Stärkung des Landes durch das Internet und solide Weiterentwicklung der Netzwerksicherheit und Informatisierung], *求是 [Qiushi]*, 15. September 2017, [http://www.qstheory.cn/dukan/qs/2017-09/15/c\\_1121647633.htm](http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm).
- <sup>23</sup> 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung].
- <sup>24</sup> Ibid. Im selben Jahr griff der stellvertretende Direktor der Cyberspace-Verwaltung Chinas Zhuang Rongwen dieses Thema auf: „Wir haben unsere Chancen während der industriellen Revolution verpasst ... Wir dürfen in der neuen Wettbewerbsrunde niemals hinterherhinken.“ Siehe: Mandy Zuo, „China Aims to Become Internet Superpower by 2050“, *South China Morning Post*, 28. Juli 2016, <https://www.scmp.com/news/china/policies-politics/article/1995936/china-aims-become-internet-cyberpower-2020>.
- <sup>25</sup> 陈肇雄 [Chen Zhaoxiong], „推进工业和信息化高质量发展“ [Förderung der hochwertigen Entwicklung von Industrie und Informatisierung].
- <sup>26</sup> Ibid.
- <sup>27</sup> Ibid.
- <sup>28</sup> 陈肇雄 [Chen Zhaoxiong], „加快推进新时代网络强国建设“ [Beschleunigen des Aufbaus einer Cybermacht in der neuen Ära], *人民网—人民日报 [People's Daily]*, 17. November 2017, <http://theory.people.com.cn/n1/2017/11/17/c40531-29651453.html>.
- <sup>29</sup> Duan verfasste seinen Text mit einem Co-Autor, Han Xiaolu, der ebenfalls der Datang Group angehört.
- <sup>30</sup> 段伟伦 [Duan Weilun] und 韩晓露 [Han Xiaolu], „全球数字经济战略博弈下的 5G 供应链安全研究“ [Forschung zur Sicherheit der 5G-Lieferkette im Rahmen des strategischen Spiels der globalen digitalen Wirtschaft], *信息安全研究 [Information Security Research]* 6, Nr. 1 (2020): 46-51, <http://www.sicris.cn/CN/abstract/abstract715.shtml>.
- <sup>31</sup> 许正中 [Xu Zhengzhong], „网络空间治理的任务与挑战“ [Die Aufgaben und Herausforderungen der Cyberspace-Governance ], *中国党政干部论坛 [Party & Government Forum]*, Nr. 1 (2020): 36-37, CNKI: D669. Der Autor ist Mitglied des ständigen Ausschusses der Parteiorganisation in Hubei und Verwaltungsratsmitglied der Parteiorganisation der Propagandaabteilung.
- <sup>32</sup> 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung].
- <sup>33</sup> Zhao Lijian, „Reguläre Pressekonferenz des Sprechers des Außenministeriums Zhao Lijian am 19. November 2020“, (Rede, Peking, 19. November 2020), [https://www.fmprc.gov.cn/mfa\\_eng/xwfw\\_665399/s2510\\_665401/t1833798.shtml](https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1833798.shtml).
- <sup>34</sup> Hua Chunying, Reguläre Pressekonferenz der Sprecherin des Außenministeriums Hua Chunying am 15. Juli 2020.“
- <sup>35</sup> Zhao Lijian, „Reguläre Pressekonferenz des Sprechers des Außenministeriums Zhao Lijian am 18. August 2020“, (Rede, Peking, 18. August 2020), [https://www.fmprc.gov.cn/mfa\\_eng/xwfw\\_665399/s2510\\_665401/t1807193.shtml](https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1807193.shtml).
- <sup>36</sup> 习近平 [Xi Jinping], „习近平：把我国从网络大国建设成为网络强国-高层动态-新华网“ [Xi Jinping: Entwicklung Chinas von einem führenden Cyber-Land zu einer Cyber-Großmacht].
- <sup>37</sup> Ibid.
- <sup>38</sup> 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung].
- <sup>39</sup> Ibid.
- <sup>40</sup> Ibid.
- <sup>41</sup> Wörtlich bedeutet dieser Begriff „Lebenstor“ oder „Tor der Vitalität“, aber da er hier im Chinesischen metaphorisch verwendet wird, haben wir uns für eine entsprechende deutsche Metapher entschieden.
- <sup>42</sup> 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung].
- <sup>43</sup> Ein Ausdruck, der sich darauf bezieht, einen Konkurrenten auf der Außenseite einer Kurve zu überholen.
- <sup>44</sup> 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung].
- <sup>45</sup> Ibid.

- 
- <sup>46</sup> 习近平 [Xi Jinping], „习近平在第二届世界互联网大会开幕式上的讲话“ [Rede von Xi Jinping zur Eröffnungszereemonie der zweiten Welt-Internet-Konferenz].
- <sup>47</sup> Xi sagte: „Eine Ansicht ist, dass wir die Tür schließen, neu anfangen, die Abhängigkeit von ausländischer Technologie vollständig beseitigen und uns auf einheimische Innovationen verlassen müssen, um uns weiterzuentwickeln. Andernfalls werden wir immer anderen folgen und niemals aufholen.“
- <sup>48</sup> Xi sagte: „Wir müssen uns öffnen und unsere eigene Technologie auf den Schultern von [ausländischen] Riesen entwickeln.“
- <sup>49</sup> 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung].
- <sup>50</sup> Ibid.
- <sup>51</sup> Ibid.
- <sup>52</sup> Ibid.
- <sup>53</sup> Ibid.
- <sup>54</sup> 陈肇雄 [Chen Zhaoxiong], „推进工业和信息化高质量发展“ [Förderung der hochwertigen Entwicklung von Industrie und Informatisierung].
- <sup>55</sup> 墨翡 [Mo Fei], „英国高调发布 5G 战略 意欲成为全球领导者“ [Großbritannien startet hochkarätige 5G-Strategie und strebt die weltweite Führungsrolle an], *通信世界 [Communications World]*, Nr. 21 (2017), CNKI: F627.
- <sup>56</sup> 乔龙 [Qiao Long], 任天舒 [Ren Tianshu] und 刘优 [Liu You], „中国高新技术产业应对贸易摩擦的影响研究 – 以 5G 产业为例“ [Untersuchung der Auswirkungen der chinesischen Hightech-Industrie auf Handelsstreitigkeiten am Beispiel der 5G-Branche], *国际经贸 [International Economics and Trade]*, 5 (2020), CNKI: F276.44;F752.02.
- <sup>57</sup> „中央网络安全和信息化领导小组第一次会议召开“ [Erstes Treffen des Führungskomitees für zentrale Cybersicherheit und Informatisierung hat stattgefunden] 中央政府门户网站 [Portal der Zentralregierung].“
- <sup>58</sup> „习近平称努力让关键核心技术自主可控 促产业迈向全球价值链中高端“ [Xi Jinping kündigte Bemühungen an, wichtige Kerntechnologien unabhängig und kontrollierbar zu gestalten und die Branche zu ermutigen, sich dem oberen Ende der globalen Wertschöpfungskette zuzuwenden].
- <sup>59</sup> Hua Chunying, Reguläre Pressekonferenz der Sprecherin des Außenministeriums Hua Chunying am 15. Juli 2020.“
- <sup>60</sup> Hua Chunying, Reguläre Pressekonferenz der Sprecherin des Außenministeriums Hua Chunying am 11. Dezember 2020.“
- <sup>61</sup> Hua Chunying, „Reguläre Pressekonferenz der Sprecherin des Außenministeriums Hua Chunying am 9. Oktober 2020“ (Rede, Peking, 9. Oktober 2020), [https://www.fmprc.gov.cn/mfa\\_eng/xwfw\\_665399/s2510\\_665401/t1822871.shtml](https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1822871.shtml).
- <sup>62</sup> Der chinesische Begriff für „Cyber“ (网络) in „Cybersicherheit“ kann auch als „Netzwerk“ übersetzt werden. Für die Zwecke dieses Berichts werden die zitierten Verwendungen des Begriffs als „Cybersicherheit“ und nicht als „Netzwerksicherheit“ übersetzt. Im Allgemeinen verwendet der Bericht jedoch den Begriff „Cyber- und Netzwerksicherheit“.
- <sup>63</sup> „中央网络安全和信息化领导小组第一次会议召开“ [Erstes Treffen des Führungskomitees für zentrale Cybersicherheit und Informatisierung hat stattgefunden] 中央政府门户网站 [Portal der Zentralregierung].“ Zudem gab der dem Führungskomitee, das bei dieser Veranstaltung ins Leben gerufen wurde, den Namen „Führungskomitee für zentrale Cybersicherheit und Informatisierung“ und definierte damit seine Rolle in Sachen Sicherheit.
- <sup>64</sup> Ibid.
- <sup>65</sup> 2018 wiederholte Xi beispielsweise erneut, dass es „ohne Cybersicherheit keine nationale Sicherheit geben kann“. Siehe: 习近平 [Xi Jinping], „习近平：自主创新推进网络强国建设“ [Xi Jinping: Unabhängige Innovationen begünstigen den Aufbau einer Cybermacht].
- <sup>66</sup> 刘棟 [Liu Li], 孟宪民 [Meng Xianmin] und 李阳 [Li Yang], „5G 安全及网络监管问题探析“ [Analyse von 5G-Sicherheits- und Netzwerküberwachungsproblemen], *国防科技 [National Defense Technology]* 41, Nr. 3 (2020): 76-79, CNKI: TN929.5;TN915.08.
- <sup>67</sup> 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung].

---

<sup>68</sup> 习近平 [Xi Jinping], „习近平: 加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力“ [Xi Jinping: Beschleunigung der unabhängigen Innovation der Netzwerkinformationstechnologie und Vornahme unermüdlicher Anstrengungen, um das Ziel des Aufbaus einer Cybermacht zu erreichen], (Rede, Peking, 10. Oktober 2016), <http://cpc.people.com.cn/n1/2016/1010/c64094-28763907.html>.

<sup>69</sup> 陈肇雄 [Chen Zhaoxiong], „推进工业和信息化高质量发展“ [Förderung der hochwertigen Entwicklung von Industrie und Informatisierung].

<sup>70</sup> 轩传树 [Xuan Chuanshu], „正确认识网络强国建设所面对的成就\_问题和影响“ [Die Leistungen beim Aufbau einer Cybermacht richtig verstehen: Probleme und Auswirkungen], *中国信息安全 [China Information Security]*, 2 (Februar 2015), CNKI: TP393.08;E86.

<sup>71</sup> Es ist unwahrscheinlich, dass diese Art offensiver und aggressiver Wortwahl in der öffentlichen Rhetorik von Xi Jinping oder in Bekanntmachungen anderer Regierungsstellen vorkommt, die ihre Äußerungen an ein externes Publikum richten und einer internationalen Prüfung unterliegen. Der Abschnitt stützt sich daher in erster Linie auf weniger offizielle Quellen. Natürlich sind diese mit Einschränkungen hinsichtlich ihrer Aussagekraft verbunden: Diese sollten nicht als offizielle Anweisungen oder Strategien der chinesischen Regierung betrachtet werden, sondern vielmehr als Reflexion der vorherrschenden Denkweise in chinesischen Analysekreisen.

<sup>72</sup> Detaillierte Informationen zur militärisch-zivilen Fusionsstrategie Chinas finden Sie unter: Emily de La Bruyère and Nathan Picarsic, „Military-Civil Fusion: China’s Approach to R&D, Implications for Peacetime Competition, and Crafting a US Strategy“, USN/NPS Acquisition Research Symposium, Mai 2019, <https://nps.edu/web/gsdm/acquisition-research-program>.

<sup>73</sup> „《2015 年中国军民融合发展报告》呈现五大亮点“ [Fünf Höhepunkte des „Berichts über die Entwicklung der militärisch-zivilen Fusion 2015“], *中国日报 [China Daily]*, 24. September 2015, [https://cn.chinadaily.com.cn/2015-09/24/content\\_21968926.htm](https://cn.chinadaily.com.cn/2015-09/24/content_21968926.htm).

<sup>74</sup> 习近平 [Xi Jinping], „习近平: 自主创新推进网络强国建设“ [Xi Jinping: Unabhängige Innovationen begünstigen den Aufbau einer Cybermacht].

<sup>75</sup> 秦安 [Qin An], „网络强国的意识认识共识“ [Bewusstsein, Verständnis und Konsens einer Cybermacht].

<sup>76</sup> 段伟伦 [Duan Weilun] und 韩晓露 [Han Xiaolu], „全球数字经济战略博弈下的 5G 供应链安全研究“ [Forschung zur Sicherheit der 5G-Lieferkette im Rahmen des strategischen Spiels der globalen digitalen Wirtschaft], CNKI: F623;TN929.5.

<sup>77</sup> 郭超 [Guo Chao], 于川信 [Yu Chuanxin], and 王景芳 [Wang Jingfang], „对第五代移动通信技术军事应用的几点认识“ [Einige Ansichten zur militärischen Anwendung der Mobilkommunikationstechnologie der fünften Generation], *国防 [Nationale Verteidigung]*, Nr. 1 (2019): 27-29, CNKI: E962;TN929.5.

<sup>78</sup> Siehe beispielsweise Xis Rede bei der 22. Studiensitzung des Politbüros der Kommunistischen Partei Chinas im Juli 2020, in der er zur Beschleunigung der „Informatisierung und Intelligensierung“ zur Stärkung des chinesischen Militärs aufruft: „习近平在中央政治局第二十二次集体学习时强调 统一思想坚定信心鼓足干劲抓紧工作 奋力推进国防和军队现代化建设“ [Während der 22. kollektiven Studiensitzung des Politbüros des Zentralkomitees betonte Xi Jinping die Einheitlichkeit des Denkens, festes Vertrauen und Begeisterung und die großen Anstrengungen dahingehend, die Modernisierung der nationalen Verteidigung und des Militärs voranzutreiben], *新华 [Xinhua]*, 31. Juli 2020, [http://www.xinhuanet.com/politics/leaders/2020-07/31/c\\_1126310486.htm](http://www.xinhuanet.com/politics/leaders/2020-07/31/c_1126310486.htm).

<sup>79</sup> 郑安琪 [Zheng Anqi], „立足现实基础推动我国网络强国建设“ [Förderung des Aufbaus der Netzmacht meines Landes auf der Grundlage der Realität], *通信管理与技术 [Kommunikationsmanagement und -technologie]* 3 (2020), CNKI: F49.

<sup>80</sup> Ibid.

<sup>81</sup> Ibid.

<sup>82</sup> 李峰 [Li Feng], 马方方 [Ma Fangfang], 刘海 [Li Hai] und 李凯 [Li Kai], „浅析 5G 技术在现代军事物流中的应用“ [Analyse der Anwendung von 5G-Technologie in der modernen Militärlogistik], *物流技术 [Logistiktechnologie]* 39, Nr. 4 (2020.): 133-37, CNKI: TN929.5;E075.

<sup>83</sup> 郭超 [Guo Chao], 于川信 [Yu Chuanxin], and 王景芳 [Wang Jingfang], „对第五代移动通信技术军事应用的几点认识“ [Einige Ansichten zur militärischen Anwendung der Mobilkommunikationstechnologie der fünften Generation Verteidigung].

<sup>84</sup> Ibid.

<sup>85</sup> Ibid.

<sup>86</sup> Ibid.

<sup>87</sup> Ibid.

---

<sup>88</sup> Ibid.

<sup>89</sup> 王峰 [Wang Feng], „军民融合热度渐升 A 股酝酿主题行情“ [Die Begeisterung für die militärisch-zivile Fusion nimmt zu und A-Aktien führen zu einer Entwicklung von Themenmärkten], *商业观察 [Geschäftsbeobachtung]* 8 (2019): 42-47, CNKI:F426.48;E25;F832.51.

<sup>90</sup> Ibid.

<sup>91</sup> 李峰 [Li Feng], 马方方 [Ma Fangfang], 刘海 [Li Hai] und 李凯 [Li Kai], „浅析 5G 技术在现代军事物流中的应用“ [Analyse der Anwendung von 5G-Technologie in der modernen Militärlogistik].

<sup>92</sup> 孙柏林 [Sun Bolin], „5G 赋能现代军事“ [5G befähigt das moderne Militär], *计算机仿真 [Computersimulation]* 37, Nr. 1 (2020): 1-6, CNKI: TN929.5;E11.

<sup>93</sup> 陈宝国 [Chen Baoguo], „新一轮信息技术革命浪潮对我国的影响“ [Die Auswirkungen der neuen Welle der Revolution der Informationstechnologie auf unser Land], *科学决策 [Wissenschaftliche Entscheidungsfindung]* 11 (2010): 1-25, CNKI: F49.

<sup>94</sup> Ibid.

<sup>95</sup> Ibid.

<sup>96</sup> 刘红凛 [Liu Honglin], „信息化发展对党的建设的多重影响“ [Die vielfältigen Einflüsse der Entwicklung der Informatisierung auf den Aufbau der Partei], *中共中央党校学报 [Zeitschrift der zentralen Parteischule der Kommunistischen Partei Chinas]* (Dezember 2011), CNKI: TP399-C2.

<sup>97</sup> 易华勇 [Yi Huayong] und 邓伯军 [Deng Bojun], „新时代中国国家文化安全策论“ [Chinas nationale Politik der kulturellen Sicherheit in der neuen Ära], *江海学刊 [Akademische Fachzeitschrift Jianghai]* (2020), CNKI: TP18;TN929.5;G120.

<sup>98</sup> Zhao Lijian, „Reguläre Pressekonferenz des Sprechers des Außenministeriums Zhao Lijian am 19. Oktober 2020“, (Rede, Peking,

19. Oktober 2020), [https://www.fmprc.gov.cn/mfa\\_eng/xwfw\\_665399/s2510\\_665401/t1825131.shtml](https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1825131.shtml).

<sup>99</sup> 龙在野 [Long Zaiye], „网络强国和信息治国的网信军民融合路径探悉“ [Untersuchung der militärisch-zivilen Fusion im Bereich Cyberinformationen zum Aufbau einer Cyber-Macht und Information Governance], *网信军民融合 [Militärisch-zivile Fusion im Cyberspace]* (Oktober 2017), CNKI: E25.

<sup>100</sup> 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung].

<sup>101</sup> Zhao Lijian, „Reguläre Pressekonferenz des Sprechers des Außenministeriums Zhao Lijian am 8. September 2020“, (Rede, Peking, 8. September 2020),

[https://www.fmprc.gov.cn/mfa\\_eng/xwfw\\_665399/s2510\\_665401/t1813183.shtml](https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1813183.shtml).

<sup>102</sup> „网络空间战略论坛‘三载路：网络强国理论高地行“ [Der Drei-Jahres-Plan des Cyberspace-Strategieforums: Auf dem Weg zur Cyber-Großmacht].

<sup>103</sup> 郭占恒 [Guo Zhanheng], „习近平标准化思想与浙江实践“ [Xi Jinpings Standardisierungsgedanke und Herangehensweise für Zhejiang], *浙江日报 [Zhejiang Daily]*, 25. September 2015, CNKI: F203;F092.7. Beide zitierten Sätze sind bei der Erörterung von Standards in chinesischen Unternehmen und in der Politik häufig zu finden.

<sup>104</sup> „‘标准化’作用何在？习近平为你一一讲来“ [Welche Rolle spielt die Standardisierung? Xi Jinping erklärt es Ihnen], *中国日报 [China Daily]*, 13. September 2016, [https://china.chinadaily.com.cn/2016-09/13/content\\_26783549.htm](https://china.chinadaily.com.cn/2016-09/13/content_26783549.htm). Dieser Schwerpunkt war für Xi nicht neu: Bereits 2006, als Sekretär des Parteikomitees der Provinz Zhejiang, schlug Xi vor, „die Strategie der Rechte des geistigen Eigentums und der Standardisierung aktiv umzusetzen“ und bezeichnete die „Standardisierung“ als „strategische Anhöhe“ für die wirtschaftliche und soziale Entwicklung. Siehe: 郭占恒 [Guo Zhanheng], „习近平标准化思想与浙江实践“ [Xi Jinpings Standardisierungsgedanke und Herangehensweise für Zhejiang].

<sup>105</sup> Weitere Informationen zu Chinas Ambitionen bei der Standardsetzung finden sich in folgenden Artikeln: Emily de La Bruyère und Nathan Picarsic, „China Standards 2035: Beijing’s Platform Geopolitics and Standardization Work in 2020“, *Horizon Advisory*, April 2020, <https://www.horizonadvisory.org/china-standards-2035-introduction>; Emily de La Bruyère, „Platform Geopolitics: The New Metrics for Building Geopolitical Power in a New World,“ *The National Interest*, 12. April 2020, <https://nationalinterest.org/feature/new-metrics-building-geopolitical-power-new-world-143147>.

<sup>106</sup> 习近平 [Xi Jinping], „中共中央政治局就实施网络强国战略进行第三十六次集体学习“ [Das Politbüro des Zentralkomitees der KP Chinas führt die 36. kollektive Studie zur Umsetzung der Strategie zum Aufbau einer Cybermacht durch], *新华 [Xinhua]*, 9. Oktober 2016, [http://www.gov.cn/xinwen/2016-10/09/content\\_5116444.htm](http://www.gov.cn/xinwen/2016-10/09/content_5116444.htm).

- <sup>107</sup> 金英果 [Jin Yingguo], “‘中国标准 2035’项目” [Projekt „China Standards 2035“], *中国标准话 [Chinesische Standardisierung]* 1 (2019): 38-43, CNKI: F203.
- <sup>108</sup> „‘中国标准 2035’项目结题会暨‘国家标准化发展战略研究’项目启动会在京召开“ [Projektabschluss des Projekts „China Standards 2035“ und Auftakttreffen des Projekts „Nationale Strategieentwicklungsstrategieforschung“ in Peking], *铁道技术监督 [Technische Überwachung der Eisenbahn]* 2 (2020): 16, CNKI: F203.
- <sup>109</sup> „2020 年全国标准化工作要点“ [Hauptpunkte der nationalen Standardisierungsarbeit im Jahr 2020], 国家标准化管理委员会 [Nationales Verwaltungskomitee für Standardisierung].
- <sup>110</sup> 孙强 [Sun Qiang], „乌镇讲话彰显习近平网络强国战略的思想内核“ [Die Rede von Wuzhen betont den ideologischen Kern von Xi Jinpings Strategie zum Aufbau einer Cybermacht], *人民日报 [People's Daily]*, Januar 2016, CNKI: TP393.4.
- <sup>111</sup> Dieses Kalkül ähnelt dem zuvor in diesem Bericht zitierten Punkt von Xi Jinping, dass Kerntechnologien Bereiche sind, in denen China „an der gleichen Startlinie“ wie andere Länder stehen. „Wenn wir unsere Lösung vor ihnen bereitstellen und uns auf die Forschung konzentrieren können, haben wir eine reale Chance, uns von unserer Schlusslichtposition vorzukämpfen und an die Spitze zu setzen.“ Siehe: 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表“ [Vollständiger Text der Rede Xi Jinpings beim Forum zur Cybersicherheit und Informatisierung].
- <sup>112</sup> „2020 年全国标准化工作要点“ [Hauptpunkte der nationalen Standardisierungsarbeit im Jahr 2020], 国家标准化管理委员会 [Nationales Verwaltungskomitee für Standardisierung].
- <sup>113</sup> 习近平 [Xi Jinping], “习近平：加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力” [Xi Jinping: Beschleunigung der unabhängigen Innovation der Netzwerkinformationstechnologie und Unternehmung von unermüden Anstrengungen, um das Ziel des Aufbaus einer Cybermacht zu erreichen, *People's Daily*]
- <sup>114</sup> 高超 [Gao Chao], „加快 5G 进程助力网络强国建设“ [Beschleunigung des 5G-Prozesses zum Aufbau einer Cybermacht], *通信产业报 [Nachrichten aus der Kommunikationsbranche]*, 12. März 2018, <http://www.qikan.com/article/txcy20180928.html>.
- <sup>115</sup> 童国华 [Tong Guohua], „立足自主 重点布局 探索网络空间内生安全“ [Auf der Grundlage der Unabhängigkeit auf das Layout konzentrieren und die endogene Sicherheit des Cyberspace erkunden], *保密科学技术 [Vertrauliche Wissenschaft und Technologie]* 11 (2018): 33, CNKI: TP393.08.
- <sup>116</sup> 段伟伦 [Duan Weilun] und 韩晓露 [Han Xiaolu], „全球数字经济战略博弈下的 5G 供应链安全研究“ [Forschung zur Sicherheit der 5G-Lieferkette im Rahmen des strategischen Spiels der globalen digitalen Wirtschaft]. Duan schrieb gemeinsam mit einem Mitautor, Han Xiaolu, der ebenfalls der Datang Group angehört.
- <sup>117</sup> Ibid.
- <sup>118</sup> Ibid.
- <sup>119</sup> Ibid.
- <sup>120</sup> Der Artikel wurde von einem Oberstleutnant an der Graduiertenschule der Akademie der Militärwissenschaften, einem Professor an der Akademie der Militärwissenschaften und einem Oberst in der Einheit 93605 erstellt. Siehe: 郭超 [Guo Chao], 于川信 [Yu Chuanxin], and 王景芳 [Wang Jingfang], „对第五代移动通信技术军事应用的几点认识“ [Einige Ansichten zur militärischen Anwendung der Mobilkommunikationstechnologie der fünften Generation Verteidigung].
- <sup>121</sup> Ibid.
- <sup>122</sup> 胡蓉 [Hu Rong], „发展 5G，深圳使命在肩“ [Shenzhens Mission: Die Entwicklung von 5G], *深圳商报 [Shenzhen Commercial Daily]*, 29. April 2019, [http://www.sznews.com/news/content/mb/2019-04/29/content\\_21705204.htm](http://www.sznews.com/news/content/mb/2019-04/29/content_21705204.htm).
- <sup>123</sup> 苏德悦 [Su Deyue], „苗圩在国务院新闻发布会上表示稳步推进 5G 网络建设 深化 5G 应用发展“ [Miao Wei sagte bei der Pressekonferenz des Staatsrats, dass der Bau von 5G-Netzwerken und die Entwicklung von 5G-Anwendungen kontinuierlich vertieft werden müsse], *人民邮电报 [Volkspost und Telegraph]*, 21. Januar 2020, [http://www.cnii.com.cn/sy/tt/202001/t20200121\\_150863.html](http://www.cnii.com.cn/sy/tt/202001/t20200121_150863.html).
- <sup>124</sup> 童国华 [Tong Guohua], „立足自主 重点布局 探索网络空间内生安全“ [Auf der Grundlage der Unabhängigkeit auf das Layout konzentrieren und die endogene Sicherheit des Cyberspace erkunden].
- <sup>125</sup> 许正中 [Xu Zhengzhong], „网络空间治理的任务与挑战“ [Die Aufgaben und Herausforderungen der Cyberspace-Governance].
- <sup>126</sup> 高超 [Gao Chao], „加快 5G 进程助力网络强国建设“ [Beschleunigung des 5G-Prozesses zum Aufbau einer Cybermacht].

---

<sup>127</sup> Tong, ebenfalls oben zitiert, ist Vorsitzender und Sekretär des Parteikomitees der chinesischen Gruppe für Informations- und Kommunikationstechnologie.

<sup>128</sup> 童国华 [Tong Guohua], „立足自主 重点布局 探索网络空间内生安全“ [Auf der Grundlage der Unabhängigkeit auf das Layout konzentrieren und die endogene Sicherheit des Cyberspace erkunden].

<sup>129</sup> 陈宝国 [Chen Baoguo], „新一轮信息技术革命浪潮对我国的影响“ [Die Auswirkungen der neuen Welle der Revolution der Informationstechnologie auf unser Land].

<sup>130</sup> 童国华 [Tong Guo], „大唐电信集团董事长兼总裁童国华：不忘初心 牢记使命，做引领 5G 发展的国家队“ [Vorsitzender und Präsident der Datang Telecom Group: Vergessen Sie nie Ihre ursprünglichen Ziele, behalten Sie Ihre Mission im Auge und werden Sie das nationale Team, das die Entwicklung von 5G anführt], *中国电子报* [Chinesische Nachrichten aus der Elektronik], 21. November 2017, <http://www.cena.com.cn/infocom/20171121/90412.html>.

<sup>131</sup> 杨震 [Yang Zhen], „物联网：引领新一轮信息技术革命“ [Das Internet der Dinge: Führung einer neuen Runde der Revolution der Informationstechnologie], *江苏通信* [Jiangsu Communications] 3 (2010): 12113, CNKI: F49;F426.6.