Für mehr Cybersicherheit muss Deutschland risikoreiche chinesische Technologien entfernen

Weber, Valentin

Veröffentlichungsversion / Published Version
Stellungnahme / comment

DGAP MEMO 02

Deutsche Gesellschaft für Auswärtige Politik e. V.

Nr. 7 | April 2024

Für mehr Cybersicherheit muss Deutschland risikoreiche chinesische Technologien entfernen

Valentin Weber

Mit Blick auf Cybersicherheit wird der Druck aus den USA auf Deutschland zunehmen, sich zu chinesischen Technologien im 5G-Bereich und darüber hinaus zu positionieren. Um dem zuvorzukommen, muss Deutschland eine systemweite Risikoanalyse anstoßen und risikoreiche chinesische Technologien gezielt identifizieren und entfernen, wie etwa Hikvision-Überwachungskameras am Flughafen BER. So würde Berlin nicht mehr als sicherheitspolitischer Nachzügler gewertet, sondern als Partner auf Augenhöhe gesehen werden – unabhängig davon, wer nächster US-Präsident wird.

Die transatlantischen Beziehungen im Cyberraum sind derzeit stark abhängig von den USA und deren Verhältnis zu China. Dementsprechend können die USA Druck auf Europa ausbauen, damit es stärker auf chinesische Technologie verzichtet, die ein Cybersicherheitsrisiko darstellt. Wenn chinesische Technologieunternehmen von den USA sanktioniert werden, können somit auch europäische Unternehmen gewisse Güter nicht mehr an die Volksrepublik liefern, etwa an Huawei.

Im Gegensatz zur EU hat sich in den letzten Jahren die Haltung der USA gegenüber China im Bereich Cybersicherheit drastisch verändert. Seit Beginn der 2000er beschuldigten die USA China der wirtschaftlichen Cyberspionage. Mitte der 2010er Jahre herrschte in den USA die Annahme vor, dass Cyberwirtschaftsspionage nur eines der Probleme war. China ist schließlich zu dieser Zeit zur Technologiemacht aufgestiegen und trumpfte auf mit Giganten wie Huawei oder ZTE, welche die Internetinfrastruktur in großen Teilen Afrikas aufbauten, in verschiedenen Kontinenten Unterseekabel verlegten und sich auch tief in europäischen Netzwerken ausbreiteten.

In Europa ließ dies jedoch nicht die Alarmglocken läuten. Politische Verantwortliche waren der Ansicht, Industriespionage könnte abgewandt und das Risiko chinesischer Technologien in kritischen Infrastrukturen durch technische Maßnahmen auf ein akzeptables Maß reduziert werden. Eine Annahme, die wenig erfolgsversprechend war. Einerseits sind 5G-Netzwerke zu komplex, um jedes Update grundlegend auf Schadsoftware zu prüfen, andererseits zerrütteten US-Sanktionen die Lieferketten von Huawei, was eine gründliche Prüfung dieser Systeme unmöglich machte. Trotz großer Sicherheitsbedenken gibt es in Deutschland und anderen europäischen Staaten bis heute keine klare Position zur Entfernung von Huawei-Ausrüstung in kritischen Netzwerken.

Und obwohl beide das Ziel der Risikoreduzierung gegenüber chinesischen Technologien haben, könnte ihre Politik jeweils gänzlich andere Auswirkungen auf die transatlantischen Beziehungen im Cyberbereich haben.

Kurz: In den letzten Jahren hat sich in der transatlantischen Haltung bezüglich der Risiken, die von chinesischen Technologien ausgehen, sowie darüber, wie diese gehandhabt sollten, ein Graben aufgetan. Diese konfrontativere Entwicklung der USA gegenüber China hat unter Donald Trump begonnen und sich unter Joe Biden gesteigert.

SZENARIEN

TRUMP 2.0: ÖFFENTLICHE ANPRANGERUNG UND WILLKÜR

Die besten Indikatoren für die Entwicklungen unter einer Amtszeit von Biden beziehungsweise Trump sind ihre ersten Amtszeiten.

Unter Trump lag das Hauptaugenmerk von Aspekten der Cybersicherheit mit Blick auf China auf 5G. Das wiederholte Anprangern der Positionen von Alliierten zu 5G war unter Trump die Norm. So wurde das Clean Network Program ins Leben gerufen, welches die Ausscheidung von chinesischen Technologien aus kritischen Netzwerken zum Ziel hatte. Telefónica Deutschland schien als einziger Dienstleister hierzulande Teil dieses Programms zu sein. Deutschland wurde angedroht, dass es weniger nachrichtendienstlich relevante Informationen von den USA bekommen würde, falls es den Gebrauch von Huawei nicht einschränkt. Gleichzeitig drohte China der deutschen Autoindustrie mit Vergeltung, falls es Huawei aus deutschen 5G-Netzen ausschließt.

Doch die oft willkürliche Politik Donald Trumps spiegelt sich auch in puncto Cybersicherheit wider. Im Rahmen der Anti-China-Linie versuchte seine Administration, beispielsweise TikTok zu verbieten. Dieses Vorhaben zog sich jedoch aus rechtlichen Gründen über Jahre und verlor unter Biden weiter an Geschwindigkeit. Vor Kurzem erwähnte Biden, dass er ein Gesetz, das zum Verbot des Videoportals führen könnte, unterschreiben würde. Daraufhin gab sich Trump als Gegner eines solchen Verbots. Dies geht auch auf das Lobbying von einigen republikanischen Persönlichkeiten zurück, die kommerzielle Interessen an einem Weiterbestehen von TikTok haben. Mittlerweile hat Biden das Gesetz unterschrieben.

Die Lehre aus den Fällen 5G und Apps zeigt, dass es bei Infrastruktur für ein potenziell härteres Durchgreifen überparteilichen Konsensus gibt. Auch unter einer Administration Trump II würde Infrastruktur verstärkt ins Visier geraten. Chinesische Apps wie TikTok werden hingegen stärker politisiert, was innenpolitisch in den USA weiterhin viel Hin und Her erwarten lässt. Bezüglich von Apps wird wohl weniger Druck auf transatlantische Partner ausgeübt werden als in Bezug auf Infrastrukturen wie etwa 5G oder elektrische Autos aus China. Für die Sicherheit Deutschlands ist dies schlecht, da die regierende KPCh Einfluss auf diese Apps ausüben kann. Von deutscher Seite wird es ohne transatlantischen Druck keine wesentlichen risikoreduzierenden Maßnahmen geben.

BIDEN 2.0: KONSEQUENTER DRUCK HINTER VERSCHLOSSENEN TÜREN

Unter Präsident Biden hat sich der Fokus auf cybersicherheitsrelevante Technologien verstärkt. Das Cybersicherheitsrisiko wird breiter und systematischer definiert als bei Trump. Mittlerweile gelten auch vernetzte Elektroautos, die mit fahrenden Mobiltelefonen verglichen werden, als Gefahr für die nationale Sicherheit. Für die Bundesregierung bedeutet dies, dass die Biden-Regierung sie zukünftig stärker anregen wird, sich von China zu distanzieren. Auch wenn dies Herausforderungen mit sich bringen wird, kann Bidens Politik langfristig leichter eingeschätzt und begegnet werden als einer möglichen zweiten Amtszeit Donald Trumps. Vernetzte Hafenkräne aus China sind ebenso ins Visier der amtierenden US-Behörden geraten. Was den Fall TikTok angeht, wird konkret ein Verbot angedroht, falls die Muttergesellschaft Bytedance ihre Anteile an der Firma nicht an einen US-Eigentümer veräußert. Einige dieser Punkte werden verstärkt vom US-Kongress gefördert, wie zum Beispiel vom Sonderausschuss des US-Repräsentantenhauses zur KPCh, der bis vor Kurzem vom ehemaligen republikanischen Abgeordneten Mike Gallagher geleitet wurde und überparteilich ist.

Bezüglich 5G und anderer cyberrelevanter Infrastruktur gab es unter Biden I – und würde es höchstwahrscheinlich auch unter Biden II – genauso viel Druck wie unter Trump geben. Dieser Druck wurde und wird jedoch direkt an deutsche Behörden kommuniziert und nicht öffentlichkeitswirksam über die Medien gespielt.

Es gibt auch Bereiche, wie multilaterale Cyberverhandlungen, auf die mit großer Wahrscheinlichkeit weder Trump noch Biden starken Einfluss ausüben werden. Darunter die UN Open-Ended Working Group zu internationaler Cybersicherheit. Gänzlich ausgeschlossen werden kann dies jedoch nicht. Möglich ist, dass vor allem unter Trump eine vermehrte und konfrontativere Auseinandersetzung mit China in multilateralen Foren angeregt wird, was sich auch auf die Positionen von Alliierten auswirken könnte. Alliierte der USA sowie internationale Partner hatten sich in öffentlichen Verhandlungen vor allem konfrontativ gegenüber Russland positioniert, dagegen jedoch weniger gegenüber China.

Kurz gesagt: Es ist zu erwarten, dass unter Donald Trump der Druck auf Alliierte konfrontativer und launenhafter wird und unter Joe Biden der Sicherheitsbegriff weiter und systematischer gefasst werden wird, wobei Kooperation und Dialog fortgesetzt werden würden.

EMPFEHLUNGEN

CYBERPOLITISCHE STRATEGIEN FÜR DEUTSCHLAND UND DIE EU

Um sich am besten auf die divergierenden Szenarien eines Wahlsiegs von Trump einerseits oder von Biden andererseits vorzubereiten, sollte Deutschland die folgenden Strategien befolgen:

EINE 5G-ENTSCHEIDUNG FÄLLEN

Unabhängig, wer die Wahl gewinnt, muss Deutschland chinesische Technologien aus den 4G- und 5G-Netzwerken entfernen. Umso früher dies geschieht, desto billiger wird der Umstieg zu sichereren Technologielieferanten. Die nationale Sicherheit wird durch einen Ausschluss von Huawei aus kritischen Netzwerken gestärkt. Zwar ist davon auszugehen, dass China Vergeltungsmaßnahmen ergreifen wird, falls es zu einem Ausschluss kommt, doch in diesem Fall könnte argumentiert werden, dass in China ebenso wenig ausländische 5G-Anbieter in Kernnetzwerken präsent sein dürfen. Der Anteil von Nokia und Ericsson ist allgemein in chinesischen Netzen aufgrund des staatlichen chinesischen Einflusses sehr gering. Zudem hat China Behinderungen von ausländischen Unternehmen im technologischen Bereich in den letzten Jahren mit der Begründung von nationaler Sicherheit intensiviert. So dürfen zum Beispiel Tesla-Fahrzeuge in zahlreichen öffentlichen Gebäuden nicht einfahren.

EINE SYSTEMATISCHE UND FORTLAUFENDE RISIKO-ANALYSE VON KRITISCHEN TECHNOLOGIEN ERSTELLEN

Das Thema Sicherheit von Technologien aus China hört nicht bei 5G auf, sondern umfasst alle vernetzten Geräte. Wie in den USA kürzlich zu beobachten, können dies Kräne in Häfen sein, die ein Sicherheitsrisiko darstellen. In Australien wiederum wurde eine systematische Kartierung von chinesischen Überwachungskameras in Ministerien und anderen staatlichen Institutionen vollzogen. So konnten die Behörden herausfinden, wo chinesische Hikvision- oder Dahua-Kameras in Netzwerken verbaut waren und als Konsequenz diese Kameras aus öffentlichen Einrichtungen entfernen. Deutschland ist noch weit entfernt von solchen Maßnahmen. Auf dem Parkplatz des Flughafens Berlin Brandenburg sind etwa noch Hikvision-Kameras zu sehen, die die Volksrepublik dazu nützen könnte, Bewegungsmuster von als interessant erachteten Personen zu erstellen. So könnte zum Beispiel herausgefunden werden, wann BND-Mitarbeitende verreisen, wohin sie fliegen und wann sie heimkehren. Diese chinesischen Überwachungskameras sollten mit Hinblick auf mögliche Spionageaktivitäten so schnell wie möglich entfernt werden. Sicherheitsanalysen sollten kontinuierlich und systemweit in Deutschland stattfinden und somit gezielt das Sicherheitsrisiko, welches von chinesischen Technologien ausgeht, reduzieren. Dabei geht es ausschließlich um öffentliche Einrichtungen oder kritische Infrastrukturen, private Nutzerinnen und Nutzer könnten weiterhin chinesische Überwachungskameras und Drohnen verwenden. Zu beachten ist jedoch, dass Öffentliches und Privates vor allem bei sich bewegenden Objekten schwer voneinander zu trennen sind. Dies ist bei hochvernetzten chinesischen elektrischen Fahrzeugen der Fall, die theoretisch Zugang zu militärischen Basen oder Ministeriumsgeländen haben könnten und bedeutet, dass auch dies unterbunden werden müsste. Gleichzeitig sind solche Objekte und Kameras auf der Autobahn sowie in Städten unterwegs und sammeln dort zahlreiche Daten. Hier sollte eine Risikoanalyse angestoßen werden, um zu evaluieren in welchen Gebieten diese Fahrzeuge verboten werden sollten. Fahrzeuge, die mit zahlreichen Kameras ausgestattet sind, dürfen somit nicht anders behandelt werden als fest installierte Hikvison- und Dahua-Kameras.

EINE PARTNERSCHAFT AUF AUGENHÖHE MIT DEN USA ANSTREBEN.

Mithilfe der oben genannten Maßnahmen könnte Deutschland eine faktenbasierte Politik verfolgen, um das Risiko chinesischer Technologien zu reduzieren. Gleichzeitig müsste die Bundesregierung dann nicht mehr fortwährend versuchen, in die Fußstapfen der USA zu treten, da sie vorab eigene Analysen erstellen würde. Diese könnten im nächsten Schritt mit den USA geteilt und Deutschland damit zum engagierten Akteur werden. So könnten die Partner kooperativ systemische Risiken reduzieren. Eine systemweite Analyse könnte dazu führen, dass Deutschland Vorreiter im Bereich der systemweiten Cybersicherheitsanalyse wird. Etwas, was bereits vor Jahren hätte geschehen können, wenn dieser Problematik ausreichend Aufmerksamkeit geschenkt worden wäre. Auf EU-Ebene könnte Deutschland zudem diese Frage im Rahmen des US-EU Trade and Technology Councils (TTC) stärker in der Arbeitsgruppe Cybersicherheit und Wettbewerbsfähigkeit thematisieren. Dies wäre ein guter Weg, deutsche Erkenntnisse auch europaweit zu platzieren.

Weder eine zweite Amtszeit von Donald Trump noch von Joe Biden wird den Druck auf Europa in Bezug auf China und Cybersicherheit abschwächen. Der Unterschied wäre, dass Trump diesen Druck konfrontativ und willkürlich, Biden kooperativ und systematisch ausüben würde. Mit den genannten Handlungsoptionen kann Deutschland schon jetzt die Initiative ergreifen und sich auf beide Präsidentschaftsszenarien angemessen vorbereiten.

Mit der Memo-Reihe „Weichenstellung für die transatlantischen Beziehungen" blicken DGAP-Expertinnen und -Experten im Vorfeld der US-Präsidentschaftswahl 2024 aus verschiedenen Perspektiven – Sicherheits-, Handels-, Geo- und Klimaaußenpolitik – auf die möglichen Wahlausgangsszenarien. Sie skizzieren, je nachdem, ob es zu einer zweiten Amtszeit von Joe Biden oder Donald Trump kommen wird, die zu erwartenden Folgen für die transatlantischen Beziehungen und formulieren Empfehlungen für Deutschland und Europa, um bereits heute die Weichenstellungen für eine gute und nachhaltige Partnerschaft zu stellen.

DGAP
Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin

Tel. +49 30 254231-0

info@dgap.org
www.dgap.org
@dgapev

Die Deutsche Gesellschaft für Auswärtige Politik e.V. (DGAP) forscht und berät zu aktuellen Themen der deutschen und europäischen Außenpolitik. Dieser Text spiegelt die Meinung der Autorinnen und Autoren wider, nicht die der DGAP.

Die DGAP ist gefördert vom Auswärtigen Amt aufgrund eines Beschlusses des Deutschen Bundestages.

Herausgeber
Deutsche Gesellschaft für Auswärtige Politik e.V.

ISSN 749-5542

Redaktion Jana Idris

Layout Lara Bührer