Kontrolle ist besser

Statt über die Vertrauensfähigkeit chinesischer Netzwerkanbieter zu diskutieren, sollte Europa an der Sicherheit der eigenen digitalen Infrastrukturen arbeiten

Von Jan-Peter Kleinhans

Sind Mobilfunkkomponenten chinesischer Netzwerkausrüster eine Gefahr für unsere nationale Sicherheit? Sollte Europa beim voranschreitenden 5G-Ausbau weiterhin auf chinesische Ausrüster wie Huawei oder ZTE setzen?

Bisher gibt es auf diese Fragen keine befriedigenden Antworten; von Strategien, die Regierungen sinnvollerweise verfolgen könnten, ganz zu schweigen. Das liegt daran, dass im Fall von 5G zwei völlig verschiedene Probleme aufeinandertreffen und eine neuartige außen- und wirtschaftspolitische Herausforderung schaffen: Es geht einerseits um die technische Sicherheit und Vertrauenswürdigkeit unserer Kommunikationsnetze und andererseits um eine langfristige technologische Abhängigkeit Europas von China. Beide Probleme erfordern jedoch vollkommen unterschiedliche Maßnahmen. Gerade deswegen ist es so wichtig, beide getrennt voneinander zu betrachten – auch, da ähnliche Fragestellungen künftig ebenso in anderen Technologiebereichen wie Künstlicher Intelligenz oder autonomem Fahren aufkommen werden.

Zu komplex, um sicher zu sein

Heutige Informations- und Kommunikationssysteme (IKT), seien es Basisstationen der Mobilfunknetze, Smartphones oder Server, haben eine unvorstellbare Komplexität erreicht – hundert Millionen Zeilen Quellcode und mehrere Milliarden Transistoren. Komplexität aber ist der Feind der IT-Sicherheit, wie der amerikanische Kryptologe und IT-Sicherheitsexperte Bruce Schneier betont. Bei heutigen IKT-Systemen lässt sich unmöglich nachweisen, dass in den Millionen Zeilen Quellcode nicht doch ein Fehler liegt oder gar eine absichtliche Schwachstelle versteckt wurde. Gleiches gilt für die Hardware.

Hinzu kommt, dass die Suche nach Schwachstellen und Attestierung gewisser Sicherheitsanforderungen weiterhin durch Software-Updates erschwert werden. Denn IT-Sicherheitsanalysen und Überprüfungen des Quellcodes,

etwa im Rahmen einer Produktzertifizierung, verlieren mit jedem nachfolgenden Software-Update an Aussagekraft: Wie viel ist eine Produktzertifizierung wert, die vor einem halben Jahr durchgeführt wurde, wenn der Hersteller mittlerweile mehrere Sicherheitsupdates veröffentlicht hat? Unsere wirtschaftliche Prosperität fußt daher in wachsendem Maße auf komplexen, voneinander abhängigen, sich ständig verändernden, softwaredefinierten Systemen, deren Sicherheit kaum abschätzbar ist. Das ist nichts Neues, und es hindert uns auch nicht daran, kritische Infrastrukturen wie Krankenhäuser, Kraftwerke oder Banken mit zu vernetzen.

Es zeigt jedoch, wie verkürzt die 5G-Debatte derzeit oft geführt wird. Die Mobilfunknetze werden nicht erst durch chinesische Hersteller unsicher – sie sind es schon. Wie vertrauenswürdig und widerstandsfähig ein Mobilfunknetz ist, hängt derzeit in erster Linie vom jeweiligen Betreiber ab: Manche achten sehr stark auf IT-Sicherheit, viele andere kaum. Bei der fünften Mobilfunkgeneration sollte es vorrangig um ein ganzheitliches, herstellerunabhängiges Risikomanagement gehen. Das wird schwierig genug.

Eindeutige Anforderungen, europäischer Austausch

Sowohl der Ansatz der Europäischen Kommission als auch die „Prager Empfehlungen“, ein Memorandum von 30 NATO- und EU-Staaten zum Ausbau zukünftiger 5G-Netzwerke, gehen hier in die richtige Richtung. Um die Vertrauenswürdigkeit und die Widerstandsfähigkeit unserer Mobilfunknetze zu erhöhen, müssen zunächst einmal die Anforderungen an Betreiber und Hersteller eindeutig formuliert werden. Daneben geht es um einen verstärkten Austausch zwischen Betreibern auf europäischer Ebene – nicht nur über die Netzwerkplanung, sondern auch über eine möglichst sichere Konfiguration des Netzwerks. Großbritannien hat hier durch die Arbeit des National Cyber Security Centers (NCSC) schon langjährige Erfahrung und führt seit Ende 2018 ebenso eine Risikoanalyse der Lieferketten von Telekommunikationsanbietern durch.

Ob mit Huawei oder ohne: Unsere Netze sind bereits unsicher

Die angesprochenen Maßnahmen auf der Ebene von Standardisierung, Implementierung, Konfiguration und Prozessen bei Betreibern und Herstellern führen natürlich lediglich zu einer Risikominimierung – ein Restrisiko wird immer bestehen bleiben. Dieses Restrisiko ist aus europäischer Perspektive bei chinesischen Herstellern größer. Nicht weil Netzwerkkomponenten von Huawei oder ZTE von minderer Qualität gegenüber europäischen Anbietern wie Ericsson oder Nokia wären. Sondern weil chinesische Unternehmen im Zweifelsfall den Anweisungen der Kommunistischen Partei Chinas unterliegen.

Genau deswegen fordern etwa die Unterzeichner der Prager Empfehlungen, die rechtlichen Rahmenbedingungen des Herkunftslands des Herstellers zum Teil der nationalen Risikoanalyse zu machen. Dies ist sinnvoll und notwendig, da heutige IKT-Systeme aufgrund ihrer Komplexität nicht abschließend vertrauenswürdig sind. Man muss sich also darauf verlassen, dass ein Hersteller sein Gerät konstant mit Sicherheitsupdates versorgt und seine Privilegien nicht missbraucht, um beispielsweise absichtlich einen Schadcode einzuführen. Dieses Vertrauen in den Hersteller hängt wiederum davon ab, aus welchem

Bild nur in Printausgabe verfügbar

rechtlichen System heraus er operiert. Das bedeutet nicht automatisch, dass chinesische Hersteller aufgrund von Mängeln des chinesischen Rechtssystems ausgesperrt werden müssten. Wohl aber, dass sie sich mit den Schwächen konstruktiv auseinandersetzen müssen. Ein Beispiel ist hier das russische IT-Sicherheitsunternehmen Kaspersky: Aufgrund von Vorwürfen der USA, Kaspersky würde mit dem russischen Geheimdienst kooperieren, büßte das Unternehmen auch in Europa viel Vertrauen ein. Im Zuge dessen wurde ein Rechenzentrum in der Schweiz aufgebaut, in dem nun die Daten europäischer Kunden verarbeitet werden – statt sie, wie bisher, zur Analyse zurück nach Russland zu schicken. Immerhin hat Huawei in den vergangenen Jahren mehrere Cybersecurity Center in Europa aufgebaut, um dort Einsicht in das Equipment und den Quellcode zu gewähren.

Die rechtlichen Rahmenbedingungen, denen ein Hersteller im eigenen Land unterliegt, beeinflussen die Vertrauenswürdigkeit der IKT-Systeme dieses Herstellers. Daran wird sich auf absehbare Zeit wenig ändern. Genau deswegen lässt sich die derzeitige Debatte über die Vertrauenswürdigkeit chinesischer Netzwerkausrüster nicht auf 5G und Mobilfunknetze beschränken. Wenn die chinesische 5G-Basisstation tatsächlich eine Gefahr für die nationale Sicherheit ist, was ist mit dem chinesischen 5G-Modul in einem selbstfahrenden Auto? Was ist mit dem Prozessor für Rechenzentren, den Huawei im Winter 2018 vorgestellt hat? Was ist mit KI-Algorithmen von chinesischen Unternehmen wie Alibaba oder Tencent? Fakt ist: China spielt eine immer dominantere Rolle in einer Vielzahl von IKT-Lieferketten. Und die Frage, wie wir mit chinesischen IKT-Systemen in unseren digitalen Infrastrukturen umgehen, wenn wir dem chinesischen Staat in letzter Instanz nicht vertrauen, bleibt ungeklärt.

Europa hat sich an die Technologieführerschaft der USA in weiten Teilen der IKT gewöhnt. Während europäische Unternehmen noch bei 2G (GSM) in Führung lagen, wurde die vierte Mobilfunkgeneration eindeutig durch US-Unternehmen dominiert. 4G hat überhaupt erst mobiles Internet ermöglicht und damit die Voraussetzung für weite Teile der App-Industrie und Sharing-Plattformen geschaffen. Auch bei Cloud-Diensten hat man sich in Europa mit der Dominanz amerikanischer Unternehmen abgefunden. Letztlich stammen beide mobilen Betriebs- und Ökosysteme, Apple iOS und Google Android, von amerikanischen Unternehmen. Die Liste ließe sich beliebig fortsetzen.

Die Technologieführerschaft der USA wird auch durch Standardisierungsarbeit in den relevanten Gremien sichergestellt. Qualcomm, Cisco, HP, Google und viele andere senden massiv Personal in internationale Ausschüsse, um dort durch Mitarbeit an technischen Standards eigene Entwicklungen am Markt zu etablieren, Geschäftsmodelle abzusichern und letztlich Technologie und Spielregeln zu definieren.

Zweierlei Maß?

Diese Abhängigkeit hatte mit den Snowden-Enthüllungen ihre vielleicht bisher stärkste Belastungsprobe erfahren. Die Snowden-Dokumente haben gezeigt, dass die USA ihre Vormachtstellung bei IKT ausnutzen, um mit ihren Geheimdiensten umfassend in fremde Netzwerke einzudringen und Datenverkehr im Internet zu überwachen. So ist belegt, dass die National Security Agency Netzwerkequipment, unter anderem von Cisco, auf dem Postweg abgefangen hat. Das Equipment wurde dann mit speziellem Schadcode infiziert, um es dem Geheimdienst später zu erleichtern, das Netzwerk, in dem das Equipment zum Einsatz kommt, zu infiltrieren. Nachdem man den Schadcode aufgespielt hatte, wurden die Netzwerkkomponenten wieder verpackt und auf die weitere Reise zum Endkunden geschickt – ohne dass der Hersteller davon wusste.

Trotz NSA-Skandals blieb US-Equipment in Europas Netzen

Trotz umfassender medialer Berichterstattung wurde seinerzeit nicht ernsthaft erwogen, amerikanisches Netzwerkequipment aus deutschen oder europäischen Netzen zu verbannen. Einer der Gründe hierfür war und ist das Vertrauen in den US-Rechtsstaat und ein gemeinsames Werteverständnis. So ziehen US-Unternehmen gegen Regierung und Strafverfolgungsbehörden vor Gericht, um gegen Praktiken der Datenherausgabe oder verpflichtende „Hintertüren“ in IKT-Systemen zu klagen. Wie sähe das in China aus? Es ist zumindest mehr als fraglich, ob Huawei, Alibaba oder Baidu sich vor einem chinesischen Gericht gegen eine Anordnung der Regierung wehren würden. Gerade weil weder der Regierung noch dem Rechtssystem Chinas vertraut wird, verläuft die derzeitige Debatte um den 5G-Ausbau in Europa so anders als die damalige Debatte nach den Snowden-Enthüllungen um amerikanische Hersteller – zu Recht.

Huawei ist vielleicht das erste chinesische Unternehmen, das es in einer bestimmten IKT-Sparte zum Weltmarktführer geschafft hat. Es ist jedoch keineswegs das einzige. Huawei avancierte im sogenannten Radio Access Network (RAN), also den Basisstationen und Antennen, die das eigentliche Mobilfunknetz ausmachen, zum Weltmarktführer, weil es die gesamte Klaviatur bespielt:

Es ist eines der aktivsten Unternehmen innerhalb der 3GPP, den zentralen Standardisierungsgremien für 5G, und arbeitet in unzähligen Arbeitsgruppen mit, um zukünftige Technologie zu definieren. Weiterhin versteht es die strategische Relevanz der Patentierung und hat 2017 die meisten Patente in Europa erhalten. Huawei hat in den vergangenen Jahren so viel für Forschung und Entwicklung ausgegeben wie Nokia und Ericsson zusammen – allein 2018 nach eigenen Angaben über 15 Milliarden Dollar. So behauptete sich Huawei durch innovative Produkte erfolgreich in einem Hochtechnologiemarkt.

All dies wird durch die chinesische Regierung massiv unterstützt und subventioniert. Gerade bei IKT und Halbleitern ist es das Ziel, möglichst zügig weitestgehend unabhängig von den USA zu werden, die beispielsweise beim Chipdesign weiterhin Technologieführer sind. China fördert gezielt Innovationen im eigenen Land und schafft nationale Champions, die im riesigen chinesischen Binnenmarkt sehr lange wachsen können. Wie abhängig von den USA man allerdings derzeit etwa bei Halbleitern noch ist, zeigt der derzeitige Handelskrieg: 2018 haben die USA durch Exportkontrolle jegliche Zusammenarbeit zwischen ZTE und US-Unternehmen unterbunden – wodurch das Unternehmen fast bankrott gegangen wäre. 2019 ist Huawei Ähnliches widerfahren, was massive Kollateralschäden nach sich zog. Als Reaktion hat die chinesische Regierung eine eigene Exportkontrolle ins Leben gerufen, um so zukünftig ebenso Druck auf IKT-Lieferketten ausüben zu können. Das könnte dann auch Europa treffen.

ZTE wäre im Handelskrieg beinahe pleite gegangen

Eigene digitale Strukturen stärken, Abhängigkeiten verringern

5G ist nur der Anfang. China ist nicht mehr die „Fabrik der Welt“; es gestaltet durch Unternehmen wie Huawei, Alibaba, Tencent und ZTE Technologie aktiv mit – auf Höchstniveau. Für Europa bedeutet das, immer abhängiger von Technologie zu werden, deren Herkunftsland wir teils als „Systemrivalen“ sehen. Erstens gilt es daher, die Vertrauenswürdigkeit und Widerstandsfähigkeit unserer digitalen Infrastrukturen zu stärken. Zweitens sollten wir in bestimmten IKT-Bereichen eigene Kompetenzen aufbauen und Abhängigkeiten verringern.

Die Vertrauenswürdigkeit unserer Netze lässt sich durch eine Vielzahl von Maßnahmen deutlich erhöhen – viele davon sind auch derzeit im Gespräch: So sollten Betreiber und nationale Sicherheitsbehörden europaweit geltende Best Practices zur sicheren Konfiguration von Netzwerkequipment erarbeiten. Ebenso sollte es europaweit einheitliche Regelungen für bestimmte kritische Prozesse des Betreibers geben, wie etwa das Aufspielen von Software-Updates oder Wartungsarbeiten mit Fernzugriff durch den Netzwerkausrüster.

Ein Mindestmaß an Sicherheit auf Ebene der Komponenten kann daneben durch schlanke und einheitliche IT-Sicherheitszertifizierung gewährleistet werden, um zumindest die gröbsten Fehler auszuschließen. Mit dem Network Equipment Security Assurance Scheme entwickelt die GSMA, der weltweite Verband der Telekommunikationsanbieter, seit einigen Jahren ein entsprechendes Evaluationssystem, das sich zurzeit in der Pilotphase befindet.

Durch starke Verschlüsselung auf Anwendungsebene muss der Datenverkehr außerdem so weit wie möglich von Netzwerkkomponenten abgeschirmt

und vor ihnen geschützt werden – ähnlich, wie dies schon seit Langem beim Datenverkehr im Internet der Fall ist. Das führt zu einem Zielkonflikt zwischen Interessen der Strafverfolgung, also der öffentlichen Sicherheit, und IT-Sicherheit: Entweder lässt sich das Netz leicht überwachen oder es ist vertrauenswürdig – Regierungen werden sich für eines entscheiden müssen.

Um die Widerstandsfähigkeit des Netzes zu erhöhen, reicht es aber nicht aus, die IT-Sicherheit einzelner Komponenten zu stärken oder auf sichere Konfigurationen bei Betreibern zu bestehen: Risikomanagement, Netzwerkplanung und Krisenmanagement der Betreiber sollten mit den nationalen Regulierungsbehörden abgestimmt werden – das bedeutet, dass auch auf behördlicher Seite entsprechende Kompetenzen aufgebaut werden müssen.

Der Schlüssel für einen effektiven Schutz gegen flächendeckende Sabotage des Netzwerks heißt Diversität der eingesetzten Komponenten – eine „Multi-Vendor-Strategie“. Wenn ein Betreiber etwa im Radio Access Network zu 70 Prozent auf Komponenten eines einzigen Netzwerkausrüsters setzt, ist das gefährlich. Daher ist eine der Anforderungen in Deutschland, dass Betreiber eine Multi-Vendor-Strategie konsequent umsetzen. Das ist jedoch in vielen EU-Mitgliedstaaten noch nicht vorgeschrieben. „Nationales Roaming“, die Möglichkeit, Infrastruktur eines anderen Betreibers zu nutzen, erhöht ebenso die Widerstandsfähigkeit des Netzwerks, da einzelne Netzausfälle durch andere Betreiber kompensiert werden können.

Wer sich auf einen Netzwerkausrüster verlässt, ist anfällig

Dies sind nur einige Beispiele, um zu verdeutlichen, dass die technischen Risiken, die mit dem 5G-Ausbau einhergehen, durchaus zu bewältigen sind. Viel schwerwiegender und wichtiger ist die Frage, welche Rolle Europa langfristig in Sachen IKT und Halbleiter zwischen den USA und China spielen will. Wir bewegen uns bei Schlüsseltechnologien – KI, Quantencomputer, 5G, Internet der Dinge – immer stärker hin zu einer bipolaren Welt, in der Technologie vorrangig durch die USA, aber immer stärker auch durch China definiert wird.

Brüssel und manche Mitgliedstaaten erkennen erst langsam, dass es gerade bei IKT einer strategischen Industriepolitik bedarf, um langfristig in Kernbereichen nicht allzu abhängig zu sein. Ein erster Schritt ist hier die Schaffung des Important Project of Common European Interest (IPCEI) für Mikroelektronik, das europäische Halbleiterunternehmen gezielt subventioniert. Ebenso braucht es eine Weiterentwicklung der Instrumente, um besonders den europäischen Mittelstand im IKT-Bereich vor ausländischen Direktinvestitionen zu schützen und Technologietransfer zu verhindern – ohne Innovationskraft und Wachstum zu begrenzen. Bei der gesamten Debatte um eine technologische Abhängigkeit Europas fehlt es bisher an guten Ideen, die über den „nächsten Airbus“ hinausgehen – und gleichzeitig ist dies mittel- und langfristig eine der zentralen Herausforderungen, um Europas wirtschaftliche Prosperität zu sichern.

Jan-Peter Kleinhans
ist Projektleiter IT-Sicherheit und Geopolitik bei der Stiftung Neue Verantwortung.