Das verborgene Rückgrat der digitalen Souveränität:

Warum Europa sich für Internetrouter interessieren muss

IEF

SAFENet
SOVEREIGNTY ALLIANCE FOR EUROPEAN NETWORK TECHNOLOGY

iconomy

Inhalt

Vorwort

ALS MESSDIENER in meiner Kindheit erhielt ich einen unvergesslichen Ratschlag bezüglich meiner Rolle als junger Helfer des Priesters am Altar: Niemand bemerkt einen Messdiener, es sei denn, er macht einen Fehler. Als wir mit der Arbeit an diesem Artikel begannen, ging mir dieser Gedanke immer wieder durch den Kopf, denn das vorliegende Thema – Router – ist wie die unsichtbaren Helfer unseres täglichen Lebens im Internet. Sie sind überall, aber in vielerlei Hinsicht unsichtbar und unbeachtet. Normalerweise begegnen wir ihnen erst dann, wenn wir Ärger mit unserer Internetverbindung haben.

Normalerweise wäre das kein Problem, doch die jüngsten politischen Entwicklungen haben die Geopolitik in alle Bereiche der Technologiebranche Einzug halten lassen. Europa und die Vereinigten Staaten haben beispielsweise große Anstrengungen unternommen, um den Einsatz chinesischer Hardware in kritischen 5G-Netzen zu debattieren oder diese sogar zu entfernen. Viele diskutieren noch immer darüber, ob die Bedrohung den ergriffenen Maßnahmen entspricht, doch die Öffentlichkeit und die Gesetzgeber sind zunehmend bereit, für die Interessen Europas einzutreten. Bislang hat sich diese Wachsamkeit seltsamerweise nicht bis zum Endgerät des Nutzers erstreckt. Dieser Beitrag soll dies ändern.

Die Innovate Europe Foundation setzt sich seit langem für mehr Souveränität durch die Entwicklung eines europäischen Technologie- und Digitalökosystems ein. Wie viele andere haben auch wir uns oft auf Plattformen und die darauf aufbauenden digitalen Dienste konzentriert, bis wir begannen, unsere Aufmerksamkeit verstärkt auf die darunter liegenden Infrastrukturebenen zu richten. Bereits in unserem Cloud-Computing-Artikel aus dem Jahr 2018 wiesen wir auf das Risiko kritischer Abhängigkeiten in der Cloud-Infrastruktur hin.

Nun, da sich Europas Bestrebungen nach mehr technologischer Souveränität weit verbreitet haben, möchten wir bescheiden darauf hinweisen, dass es noch eine weitere Technologieebene gibt, die allzu oft ignoriert wurde: die Router und Repeater, die in den meisten Haushalten und Unternehmen die grundlegende Infrastruktur bilden. Bislang sind sich nur wenige bewusst, a) dass diese Geräte überwiegend nicht aus Europa stammen und b) welches Risiko damit potenziell verbunden ist. Glücklicherweise wird derzeit eine neue europäische Koalition namens SAFENet gegründet, um das Bewusstsein für diese Schwachstelle zu schärfen.

Gemeinsam mit unseren Freunden von SAFENet und iconomy hat das IE.F daher ein Hintergrundpapier erstellt, von dem wir hoffen, dass es den Blick auf einen der letzten noch nicht untersuchten Bereiche unserer gemeinsamen Technologie-Stacks öffnet. Wir hoffen, dass dieses Papier einen wertvollen Beitrag zur öffentlichen Debatte über dieses Thema leistet, und freuen uns besonders darauf, zu sehen, wie sich die neue SAFENet-Koalition als einheitliche Stimme für diesen wichtigen Teil des europäischen Hardware-Ökosystems etabliert.

Clark Parsons
Geschäftsführer der Innovate Europe Foundation

Zusammenfassung

KRITISCHE DIGITALE INFRASTRUKTUR ist die vorderste Front geworden, an der die prägendsten geopolitischen und wirtschaftlichen Konflikte unserer Zeit ausgetragen werden. Regierungen in den Vereinigten Staaten, in China und weltweit sind zu dem Schluss gekommen, dass die Hardware und Software, die kritische Systeme antreiben, nicht länger als gewöhnliche Handelsgüter behandelt werden können. Diese Technologie-Lieferketten werden nun als Instrumente des geopolitischen Wettbewerbs und der nationalen Sicherheit verstanden, was zu Importkontrollen, Marktbeschränkungen und Sicherheitsklassifizierungen führt – Maßnahmen, die einst als undenkbar galten. Die Zunahme staatlich geförderter Cyberangriffe auf kritische Infrastrukturen hat diesen Wandel noch verstärkt und die Sicherheit digitaler Systeme zu einer Frage der nationalen Verteidigung und Souveränität gemacht.

Dennoch hat es die Europäische Union versäumt, sich an diese neue strategische Realität anzupassen. Ihre Märkte bleiben offen für Hardware- und Softwareimporte, die strategische Abhängigkeiten und Sicherheitslücken in kritischen Infrastrukturen schaffen und gleichzeitig Europas eigene digitale Lieferketten untergraben. Besonders besorgniserregend ist, dass einige der grundlegendsten Ebenen der europäischen digitalen Infrastruktur weitgehend außerhalb des Geltungsbereichs einer sinnvollen Politik zur Wahrung der Souveränität und zur Sicherung der Lieferketten bleiben.

In den letzten zehn Jahren hat die Europäische Union eines der weltweit ehrgeizigsten Regelwerke für digitale Regulierung und Cybersicherheit geschaffen. Die Datenschutz-Grundverordnung, der Data Act, die Funkgeräterichtlinie, die KI-Verordnung, die NIS2-Richtlinie, der Cyberresilienz-Verordnung und die 5G-Cybersicherheits-Toolbox befassen sich jeweils mit unterschiedlichen Aspekten der Regulierung digitaler Produkte, Dienste und Infrastrukturen im Binnenmarkt. Zusammengenommen spiegeln diese Instrumente einen **hart erkämpften politischen Konsens** wider, **wonach kritische digitale Systeme einer aktiven Regulierung bedürfen.**

Innerhalb dieser Architektur wird jedoch die Lieferkettendimension einer kritischen Infrastrukturebene nach wie vor nur unzureichend berücksichtigt. Die **Router und Heim-Gateway-Geräte,** die in Hunderten von Millionen europäischer Haushalte, kleiner und mittlerer Unternehmen, öffentlicher Verwaltungen, Schulen und Einrichtungen des Gesundheitswesens installiert sind – also die physische Hardware, über die etwa **93 % des europäischen Internetverkehrs fließen** –, operieren weitgehend außerhalb des umfassenderen Rahmens der EU für Souveränität und Lieferkettensicherheit. Während Europa Gesetze zur Cloud-Souveränität und zu Halbleiter-Lieferketten erlassen hat, wurde der buchstäbliche erste und letzte Hardware-Knotenpunkt der europäischen digitalen Aktivitäten zu einem kritischen blinden Fleck in der Lieferkette. Diese Geräte, die in fast allen europäischen Haushalten und Unternehmen installiert sind und direkt von Internetdienstanbietern bereitgestellt werden, ohne dass die Verbraucher eine Wahl hinsichtlich des Herstellers haben, stehen unkontrolliert im Zentrum der digitalen Infrastruktur Europas. Standardmäßig als vertrauenswürdig angesehen und in der Praxis unsichtbar, stellen sie ein potenzielles Trojanisches Pferd dar, das derzeit von keinem koordinierten Rahmenwerk zur Lieferkettensicherheit berücksichtigt wird.

In diesem Papier wird dargelegt, dass Kundennetzwerkgeräte – darunter Router, Heim-Gateways sowie WLAN-Mesh- und Repeater-Geräte – die **mit Abstand auffälligste Lücke in der Architektur der digitalen Souveränität der EU** darstellen und dass deren Schließung zu den politischen Maßnahmen mit der geringsten Reibung und der größten Hebelwirkung gehört, die der Kommission und den Mitgliedstaaten in der aktuellen Legislaturperiode zur Verfügung stehen.

Der vorliegende Sachverhalt stützt sich auf vier Säulen: die Größenordnung und die zentrale Bedeutung von Routern, über die der Großteil des europäischen Internetverkehrs abgewickelt wird; einen konzentrierten Markt, auf dem chinesische Hersteller 37 % der Heimnetzwerkgeräte in der Europäischen Union halten; dokumentierte Cybersicherheitsrisiken, die sich aus Botnetzen, Firmware-Hintertüren und den durch das chinesische Nationale Geheimdienstgesetz auferlegten Verpflichtungen ergeben; sowie eine zunehmende regulatorische Inkonsistenz angesichts der Bereitschaft Europas, gegen risikoreiche Lieferanten in anderen kritischen Hardware-Sektoren vorzugehen.

Um diese Lücke zu schließen, mangelt es der Europäischen Union weder an regulatorischen Kapazitäten noch an Analyseinstrumenten. Eine robuste

Architektur rund um die Sicherheit der digitalen Infrastruktur ist bereits vorhanden. Bestehende und geplante Instrumente befassen sich mit Cybersicherheitsgrundlagen, Risiken in der Lieferkette, Beschaffungspräferenzen und der Widerstandsfähigkeit kritischer Infrastrukturen in einer Vielzahl von Sektoren und Technologien. Wie in diesem Papier ausführlich dargelegt wird, hat diese Architektur die strategischen Risiken und die Risiken in der Lieferkette, die mit Heim- und KMU-Netzwerkausrüstung verbunden sind, bislang nur unzureichend berücksichtigt. Europa hat – am deutlichsten durch die 5G-Cybersicherheits-Toolbox – bewiesen, dass es weiß, wie dieses Problem anzugehen ist. Die Frage ist, warum es dies noch nicht getan hat.

Die Notwendigkeit regulatorischer Maßnahmen wird durch die öffentliche Stimmung weiter untermauert. Aktuelle Umfragedaten aus den EU-Mitgliedstaaten zeigen einen deutlichen Stimmungsumschwung in der Öffentlichkeit gegen den Einfluss ausländischer Technologieanbieter auf die europäische digitale Infrastruktur. Dieselben Bürger, die diese Skepsis äußern, sind sich größtenteils nicht bewusst, dass der Router, der von ihrem Internetdienstanbieter bei ihnen zu Hause installiert wurde, möglicherweise von genau den Unternehmen hergestellt wurde, denen sie misstrauen. Sobald diese Wissenslücke durch die unten empfohlenen Transparenzmaßnahmen geschlossen ist, wird es sehr schwer, die politische Logik für weitere Maßnahmen zu ignorieren. Die öffentliche Meinung ist dem regulatorischen Rahmen bereits voraus. Die in diesem Papier identifizierten Probleme weisen auf vier Bereiche hin, in denen europäische Institutionen und die Regierungen der Mitgliedstaaten handeln können, wobei jeder Bereich einen anderen Hebel, einen anderen Akteur und ein anderes positives Ergebnis für die Europäische Union widerspiegelt.

- **Transparenz** ist der kostengünstigste Ansatzpunkt und derjenige, der sich mit bereits geltenden Instrumenten am schnellsten umsetzen lässt. Die Verpflichtung zur Offenlegung der Herkunft der Hardware, der Zuständigkeit für die Firmware und der Verantwortung für den Update-Kanal bei allen auf dem EU-Markt in Verkehr gebrachten Netzwerkgeräten – einschließlich der von Internetdienstanbietern bereitgestellten und der White-Label-Geräte – schafft die Informationsgrundlage, ohne die eine Reform des öffentlichen Beschaffungswesens und die Steuerung der Lieferkette nicht funktionieren können. Internetdienstanbieter sollten verpflichtet werden, ihren Kunden die Herkunft klar mitzuteilen, und eine koordinierte Initiative zur Sensibilisierung der Öffentlichkeit durch die ENISA sollte die Kluft zwischen den Geräten, denen die Bürger misstrauen, und dem Gerät, das sie uninformiert in ihren Haushalten installiert haben, schließen.

- **Die Reform des öffentlichen Beschaffungswesens** ist der direkteste Hebel auf der Nachfrageseite, der heute zur Verfügung steht. Die Anwendung der „Buy Trusted"-Anforderungen auf Behörden, Betreiber kritischer Infrastrukturen und öffentlich finanzierte Einrichtungen – gestützt durch eine auf die Lieferkette ausgerichtete Zertifizierungsgrundlage für von Internetdienstanbietern bereitgestellte Router im Rahmen des Europäischen Zertifizierungsrahmens für Cybersicherheit – würde die Marktanreize neugestalten, ohne auf ein neues horizontales Rechtsinstrument warten zu müssen. Strukturierte Austauschanreize, nach dem Vorbild derer, die für den Ausstieg aus Huawei-Geräten im 5G-Bereich genutzt wurden, sollten vorrangige Bereiche beim Übergang weg von risikoreicher Hardware unterstützen.

- **Die Steuerung der Lieferkette** ist die strukturell bedeutsame Option, und die institutionellen Voraussetzungen für Maßnahmen sind bereits gegeben. Erstens bietet der bevorstehende Trilog zum Cybersicherheitsgesetz (CSA2) eine konkrete Gelegenheit, Heimnetzwerkgeräte in die Debatte über Lieferkettenrisiken einzubeziehen. Parallel dazu hat die NIS-Kooperationsgruppe im Rahmen von NIS2 den Auftrag, einer koordinierten Risikobewertung der Router-Lieferkette Priorität einzuräumen, und die 5G-Cybersicherheits-Toolbox liefert bereits das operative Modell dafür, was diese Bewertung hervorbringen sollte: eine gemeinsame Risikomethodik und einen Mechanismus zur Einstufung von Lieferanten mit hohem Risiko, der in allen Mitgliedstaaten anwendbar ist.

- **Die industrielle Kapazität** ist die Voraussetzung für eine langfristige Perspektive. Investitionen im Rahmen von InvestEU und IPCEI, verbunden mit der Harmonisierung der Freiheit der Router-Wahl im gesamten Binnenmarkt, würden die europäische Produktionskapazität stärken und die Marktsegmente erweitern, in denen europäische Hersteller bereits erfolgreich im Wettbewerb stehen..

1
DIE UNVOLLENDETE AGENDA ZUR SOUVERÄNITÄT

EUROPA HAT IN DEN LETZTEN ZEHN JAHREN BEDEUTENDE FORTSCHRITTE im Bereich der digitalen Souveränität erzielt. Die KI-Verordnung, das Datengesetz, das Gesetz über digitale Märkte, die NIS2-Richtlinie, die Cyberresilienz-Verordnung, der vorgeschlagene „Industrial Accelerator Act“ und das „Tech Sovereignty Package“ sowie die 5G-Cybersicherheits-Toolbox befassen sich jeweils mit einzelnen Aspekten der Regulierung digitaler Systeme im Binnenmarkt. Das EuroStack-Konzept – also das mehrschichtige System europäischer digitaler Fähigkeiten, das von der Konnektivität an der Basis bis hin zu Anwendungen an der Spitze reicht – hat die jüngsten strategischen Analysen zu diesem Thema geprägt.

Zusammengenommen zeigen diese Instrumente, dass digitale Souveränität kein einheitliches, sondern ein mehrschichtiges Konzept ist, das sich über vier unterschiedliche, sich jedoch gegenseitig verstärkende Dimensionen erstreckt. Bei der **Souveränität der Lieferkette** geht es um die Frage, wer die Hardware herstellt und welche Staaten die Hersteller rechtlich zur Zusammenarbeit verpflichten können. Bei der **Souveränität in Bezug auf Know-how und geistiges Eigentum** geht es darum, ob europäische Unternehmen die Design- und Softwarekompetenzen behalten, die die langfristige Wettbewerbsunabhängigkeit bestimmen. Bei der **Sicherheitssouveränität** geht es um die Frage, ob Europa seine Systeme gegen Cyberangriffe, Schwachstellen und kriminelle Ausnutzung von außen verteidigen kann. Die **Souveränität der Infrastruktur** befasst sich mit der Frage, ob bereits in Europa installierte Systeme von innen heraus gegen Europa selbst als Instrument für Spionage, Sabotage oder Nötigung durch ausländische Staaten eingesetzt werden können. Jede Dimension verstärkt die anderen, und eine Schwäche in einer einzelnen Dimension wirkt sich auf die übrigen aus. Eine glaubwürdige Souveränitätsagenda muss daher alle vier Dimensionen berücksichtigen – und zwar auf jeder Ebene des digitalen Stacks.

Der Großteil der Debatte um digitale Souveränität hat sich jedoch auf Europas Abhängigkeit von der Software US-amerikanischer Hyperscaler in den oberen Schichten des digitalen Technologie-Stacks konzentriert. Cloud-Dienste, KI-Systeme und Online-Plattformen haben in Brüssel und

den Hauptstädten der Mitgliedstaaten große Aufmerksamkeit auf sich gezogen. Die Hardware-Infrastruktur in der Basisschicht, insbesondere die Netzwerkausrüstung für Verbraucher und KMU, über die die europäischen digitalen Aktivitäten tatsächlich abgewickelt werden, ist in der öffentlichen Debatte auf der Strecke geblieben.

Die einflussreichsten strategischen Studien zur EU, wie der Draghi-Bericht über die Zukunft der europäischen Wettbewerbsfähigkeit, der Bericht des Europäischen Parlaments über europäische technologische Souveränität und digitale Infrastruktur[1] sowie der „Competitiveness Compass" der Europäischen Kommission[2] , weisen jeweils auf wachsende Bedenken hinsichtlich technologischer Abhängigkeit, asymmetrischen industriellen Wettbewerbs und der Aushöhlung der europäischen digitalen Souveränität hin.

In jüngerer Zeit haben sich diese Bedenken durch neue Anzeichen für einen „zweiten China-Schock"[3] verstärkt und gezeigt, dass deren Auswirkungen auf den europäischen Industrie- und Technologiesektor immer gravierender werden. Eine aktuelle Analyse des Centre for European Reform schätzt, dass allein in Deutschland bereits mehr als 400.000 Arbeitsplätze aufgrund des Einbruchs der Exporte nach China verloren gegangen sein könnten, und warnt gleichzeitig davor, dass chinesische Überkapazitäten in der Industrie und das Exportwachstum strategische Sektoren in ganz Europa zunehmend beeinträchtigen[4] . Trotz der zunehmenden Betonung von digitaler Souveränität und industrieller Widerstandsfähigkeit wurde der Netzwerkzugangsebene und der Lieferkette für Kundennetzwerkgeräte bislang nur wenig regulatorische Aufmerksamkeit gewidmet.

Ein souveränes europäisches Cloud- und Datenökosystem bleibt gefährdet, wenn die Hardware-Gateways, die eine Verbindung dazu herstellen, anfällig für Angriffe auf die Lieferkette, für Datenabfang oder Störungen sind, die über Software ausgeführt werden, die von Akteuren außerhalb der EU kontrolliert wird.

Die Folgen dieser Vernachlässigung sind erheblich. Router für Privathaushalte und KMU sind Massenprodukte mit langer Lebensdauer, die in mehr als 100 Millionen europäischen Haushalten und in zig Millionen kleinen und mittleren Unternehmen installiert sind. Sie bilden zudem die am stärksten exponierte Ebene der Telekommunikationslieferkette, für die derzeit kein koordinierter EU-Rahmen gilt. Der 5G-Kern ist zwar in Bezug auf die Umsetzung noch nicht lückenlos gesichert, unterliegt jedoch zumindest seit 2019 einem gemeinsamen Ansatz zur Risikoklassifizierung sowie politischer Rechenschaftspflicht auf EU- und nationaler Ebene.

Die Ebene der Netzwerkgeräte nimmt in der Regulierungslandschaft eine Sonderstellung ein. Sie ist gleichzeitig ein Verbraucherprodukt und Teil der kritischen digitalen Infrastruktur, die über fragmentierte Einzelhandels- und Internetdienstanbieter-Kanäle verkauft wird, in denen kommerzielle Kostenüberlegungen historisch gesehen Vorrang vor der Sicherheit der Lieferkette hatten. Im Gegensatz zu professionellen Netzwerkgeräten befinden sie sich in den Händen von Endnutzern, die ein berechtigtes Interesse daran haben, ihre eigenen Geräte auszuwählen, und jede regulatorische Maßnahme sollte diese Freiheit erweitern, anstatt sie einzuschränken. Gleichzeitig bedeuten der Umfang des Einsatzes und das Fehlen eines koordinierten EU-Rahmens, dass Millionen von Geräten, die von Unternehmen hergestellt werden, die der Gerichtsbarkeit ausländischer Staaten unterliegen, in europäischen Haushalten und Unternehmen installiert sind, ohne dass es einen Mechanismus gibt, um das von ihnen ausgehende Risiko zu bewerten oder zu mindern.

1 Die Zukunft der europäischen Wettbewerbsfähigkeit, Europäische Kommission, abrufbar unter: https://commission.europa.eu/topics/competitiveness/draghi-report_en; Bericht über technologische Souveränität und digitale Infrastruktur, Europäisches Parlament, abrufbar unter: https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

2 Wettbewerbsfähigkeitskompass, Europäische Kommission, abrufbar unter: https://commission.europa.eu/topics/competitiveness/competitiveness-compass_en

3 „Deutschland ist das Epizentrum des zweiten China-Schocks", von Handelsblatt, abrufbar unter: https://www.handelsblatt.com/politik/deutschland/china-deutschland-ist-das-epizentrumdes-zweiten-china-schocks-01/100226122.html

4 China-Schock 2.0 – Der Preis für Deutschlands Selbstgefälligkeit, Centre for European Reform, abrufbar unter: https://www.cer.eu/sites/default/files/pb_BS_ST_china_shock_2.0_18.5.26.pdf

Dieses Papier beleuchtet die Komplexitäten und aktuellen Schwachstellen auf der Ebene der Netzwerkgeräte und untersucht, warum Router als sicherheitskritische Infrastruktur von Bedeutung sind, wie der aktuelle Markt gestaltet ist, wie die Bedrohungslage aussieht und welche regulatorischen Impulse bereits bestehen, die ausgeweitet werden können, um diese Lücke zu schließen. Es stützt sich auf den legislativen Präzedenzfall der 5G-Toolbox sowie auf ein in zahlreichen anderen Sektoren zu beobachtendes Handlungsmuster, um zu argumentieren, dass Router den nächsten logischen und notwendigen Schritt in Europas Souveränitätsagenda darstellen.

Die politischen Rahmenbedingungen für ein Handeln sind ungewöhnlich günstig. Der Beschluss der Kommission vom Mai 2026, die EU-Förderung für Projekte einzustellen, bei denen Solarwechselrichter aus Hochrisikoländern zum Einsatz kommen[5] – unter Berufung auf das explizite Risiko einer koordinierten Fernmanipulation der Firmware, die zu einem netzweiten Stromausfall führen könnte –, schafft sowohl den rechtlich-politischen Präzedenzfall als auch den institutionellen Willen, eine entsprechende Logik auf die Netzinfrastruktur auszuweiten. Der vorgeschlagene „Cybersecurity Act 2“[6] und der „Industry Accelerator Act“ weisen auf gesetzgeberischer Ebene in dieselbe Richtung: Ersterer durch die Einführung eines horizontalen Sicherheitsrahmens für die ITK-Lieferkette, der ein direktes Argument dafür liefert, Netzwerkausrüstung in den Geltungsbereich aufzunehmen; Letzterer durch die Beseitigung der wirtschaftlichen Nachteile, denen europäische Hersteller gegenüber staatlich subventionierten Wettbewerbern ausgesetzt sind. Beide Gesetzgebungsvorhaben stellen eine konkrete Chance dar, sicherzustellen, dass Heimnetzwerkausrüstung ausdrücklich als vorrangiger Sektor anerkannt wird. Die Rahmenbedingungen für Maßnahmen im Bereich der Router werden nicht günstiger sein als derzeit.

Dieses Momentum findet sein deutlichstes Beispiel im „Tech Sovereignty Package“[7] , das Cloud, KI, Halbleiter und Rechenzentren unter einem einzigen Souveränitätsrahmen zusammenfasst. Es handelt sich um eine wegweisende Initiative, die in diesem Papier begrüßt wird. Aber es ist auch – wieder einmal – ein Rahmen, der bei Heimnetzwerkgeräten nicht weit genug geht. Souveräne Halbleiter erfordern geschützte Transportwege. Souveräne Cloud-Infrastrukturen sind auf widerstandsfähige Zugangspunkte angewiesen. Souveräne KI lässt sich nur auf einer zuverlässigen Infrastruktur skalieren. Die Netzwerkschicht, die all dies miteinander verbindet, bleibt unberücksichtigt, und genau diese Lücke soll mit diesem Papier geschlossen werden.

SAFENet (Sovereignty Alliance for European Network Technology), ein strategisches Bündnis führender europäischer Netzwerktechnologieunternehmen, fordert die EU-Institutionen und die Regierungen der Mitgliedstaaten auf, Router für Privathaushalte und KMU als kritische Infrastruktur zu behandeln, dieselbe risikobasierte Lieferkettenlogik anzuwenden, die sich bereits bei 5G bewährt hat, und zu handeln, bevor sich das Zeitfenster für die Unabhängigkeit schließt.

5 Kommission blockiert EU-Fördermittel für Solar-Technologie von Huawei, berichtet von Politico, abrufbar unter: https://www.politico.eu/article/commission-blocks-eu-funding-for-huawei-solar-tech

6 Vorschlag für eine Verordnung zum EU-Cybersicherheitsgesetz, abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act

7 Stärkung der technologischen Souveränität Europas, Europäische Kommission, abrufbar unter: https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty

2
WARUM ROUTER ALS VERSTECKTE ZUGANGS-PORTALE VON BEDEUTUNG SIND

2.1 Die Architektur des europäischen Internetverkehrs

Die Diskussion über die digitale Infrastruktur in Europa wird von sichtbaren, viel beachteten Anlagen dominiert. Dazu gehören Rechenzentren, Unterseekabel, 5G-Basisstationen und Satelliten. Der Router, ein kleines Netzwerkgerät, das im Flur, im Keller oder hinter einem Fernseher steht, findet dagegen kaum vergleichbare Beachtung. Und doch ist der Router in der Praxis eines der wichtigsten Einzelgeräte im gesamten europäischen digitalen Ökosystem. Die Abbildung auf der nächsten Seite veranschaulicht, warum das so ist.

Die digitale Infrastruktur Europas ist als mehrschichtiger Stack aufgebaut, von Anwendungen und Plattformen an der Spitze über Cloud-Dienste und die Betriebsinfrastruktur in der Mitte bis hin zur physischen Basisebene. Jede Schicht ist von der darunterliegenden Schicht abhängig. Und ganz unten in diesem Stack durchlaufen alle Daten einen Router, bevor sie einen Cloud-Dienst, eine Plattform oder eine Anwendung erreichen. Jede Banküberweisung, jede Krankenakte, jede private Nachricht, jeder Login bei Behörden, jeder Videoanruf im Homeoffice, jedes Smart-Home-Gerät – alles, was ein Haushalt oder ein Unternehmen über das Internet sendet oder empfängt, fließt durch dieses eine Gerät. Über die Daten hinaus umfasst dies auch die gesamte lokale Kommunikation innerhalb des WLANs oder LANs, die vom Router verwaltet wird, wie zum Beispiel das Ausdrucken eines Briefes vom PC auf dem Drucker, das Senden von Fotos vom Smartphone an einen Fernseher oder die Steuerung von Heizungsthermostaten über eine App, um nur einige Beispiele zu nennen.

Er ist das unverzichtbare Tor, durch das der gesamte Datenverkehr in beide Richtungen fließen muss – für jeden Nutzer und jedes Gerät. Ein kompromittiertes Rechenzentrum betrifft die Nutzer dieses Rechenzentrums. Ein kompromittierter Router betrifft jedes Gerät, jeden Dienst und jede Kommunikation aller damit verbundenen Nutzer – lautlos, beharrlich und ohne dass der Nutzer jemals davon erfährt.

Abbildung 1: Die drei Schichten und drei Grundlagen des digitalen Ökosystems[8]

Schicht 1 **Vermittlungsinfrastruktur**

Branchenspezifische Apps
Förderung eines nutzerzentrierten Designs für Apps lokaler Start-ups in bestimmten Branchen, z. B. Energiemanagement, Mobilität und Gesundheit

E-Commerce
Schutz der Verbraucherrechte gewährleisten und offene Standards für Transaktionsnetzwerke oder APIs für den E-Commerce schaffen

Search & Social
Investitionen in eine gemeinsame Infrastruktur für soziale Medien und Suchmechanismen, die algorithmischen Pluralismus unterstützen

Kompetenz & Mobilität
Investitionen in digitale Kompetenzen, einen Talentpool und in die Verbesserung der Mobilität hochqualifizierter Arbeitskräfte

Schicht 2 **Immaterielle/logische Infrastruktur**

Plattformen
Gewährleistung der Wettbewerbsfähigkeit digitaler Plattformen wie Mobil-, Desktop- und Server-Betriebssysteme, Clouds, APIs und Browser

Sichere Datenräume
Sichere Speicherung sensibler personenbezogener Daten und Gewährleistung eines auf Einwilligung basierenden Zugriffs

Digitale Zahlung
Entwicklung öffentlicher Zahlungsinfrastrukturen zur Förderung eines inklusiven digitalen Binnenmarkts

Digitale Identität
Entwicklung datengeschützte Lösungen für digitale Identitäten zur biometrischen Authentifizierung

Cloud, KI & Daten
Entwicklung von Lösungen für souveräne Clouds, Unterstützung der Bereitstellung von Rechenkapazität und des Einsatzes von KI

Schicht 3 **Physische Infrastruktur**

Geräte & Hardware
Sichere „physische Schnittstellen“ für die digitale Wirtschaft, einschließlich IoT, Hardware und vernetzter Geräte

Netzwerke & Kabel
Förderung eines wettbewerbsorientierten Telekommunikationsmarkts und Investitionen in Netze und Kabel der nächsten Generation (6G-Standards und Unterseekabel)

Datenzentren
Vergrößerung der Kapazitäten von Rechenzentren und Cloud-Diensten und Investitionen in Edge Computing

Chips & Quanten
Resilienz digitaler Lieferketten – einschließlich Halbleitern – sowie kritische Forschung und Entwicklung im Bereich Quantentechnologie

CRM, Energie & Wasser
Sicherstellung eines nachhaltigen und diversifizierten Zugangs zu kritischen Rohstoffen (critical raw materials, CRM) zur Versorgung mit erneuerbaren Energien und zu Wasser

8 Der „europäische Weg“ – Ein Konzept zur Rückeroberung unserer digitalen Zukunft, Seite 17, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5251254&download=yes
Basierend auf „The Technology Stack“ von Gautam Kamath, ECDPM, 2025

Basierend auf Daten der Bundesnetzagentur, dem „State of Wi-Fi“-Bericht von ASSIA und Analysen der GSMA[9] verarbeiten Router und Heim-Gateway-Geräte etwa 93 % des gesamten europäischen Internetdatenverkehrs. Mobilfunknetze, die Gegenstand intensiver regulatorischer Aufmerksamkeit und erheblicher öffentlicher Investitionen sind, machen die restlichen 7 % aus.

Router wickeln 93 % des europäischen Internetverkehrs ab. Die ihnen gewidmete regulatorische Aufmerksamkeit steht in keinem Verhältnis zu ihrer Rolle in der digitalen Wirtschaft.

2.2 Was Router tatsächlich leisten

Ein moderner Heimrouter oder ein Home-Gateway leistet weit mehr, als nur Pakete und sensible Informationen weiterzuleiten. Er ist das Nervenzentrum der digitalen Aktivitäten in Haushalten und KMU: Er verwaltet WLAN-Netzwerke, koordiniert Smart-Home-Geräte, wickelt VoIP-Telefonie ab, wendet Kindersicherungen und Netzwerkfilter an und verarbeitet in immer mehr Fällen Datenverkehr im Zusammenhang mit Remote-Arbeit, Telemedizin und digitalen Behördendiensten. Funktional gesehen handelt es sich um einen kleinen Server, der permanent dem öffentlichen Internet ausgesetzt und ständig mit den sensibelsten Daten aus dem digitalen Leben des Nutzers verbunden ist.

Entscheidend ist, dass der Router ununterbrochen in Betrieb ist und ständigen Zugriff auf alle Daten hat, die das Netzwerk durchlaufen. Eine Browser-Anwendung lässt sich innerhalb weniger Minuten überprüfen, aktualisieren oder ersetzen. Im Gegensatz dazu wird die Router-Software in der Regel nur unregelmäßig, oft gar nicht aktualisiert, und das Gerät selbst bleibt möglicherweise fünf bis zehn Jahre lang im Einsatz. Anders als ein Smartphone, das die meisten Nutzer alle zwei bis drei Jahre ersetzen, ist ein Router selten eine bewusste Anschaffung. Er wird im Rahmen

9 Berechnung basierend auf folgenden Quellen: Bundesnetzagentur; ASSIA: „State of Wi-Fi Reporting“, 8. Juni 2021, abrufbar unter: https://dynamicspectrumalliance.org/wp-content/uploads/2021/06/ASSIA-DSA-Summit-Presentation-v7.8.pdf; GSMA: „The Importance of 6 GHz to Mobile Evolution“, September 2024, abrufbar unter: https://www.gsma.com/connectivity-for good/spectrum/wp-content/uploads/2024/09/GSMA_Mobile-Evolution-in-6-GHz.pdf

eines Internetanbietervertrags mitgeliefert und bleibt so lange im Einsatz, bis er kaputtgeht.

Für die Zwecke dieses Artikels ist es wichtig, Router nicht als einzelnes Gerät zu betrachten, sondern als drei unterschiedliche Ebenen, von denen jede ihren eigenen Ursprung, ihren eigenen Eigentümer und ihre eigene Exposition gegenüber ausländischer Gerichtsbarkeit hat.

1. **Die physische Hardware** ist das Gerät selbst, das in einer Produktionsstätte in einem bestimmten Land zusammengebaut wird.
2. **Die Firmware und das Betriebssystem** sind die in dieser Hardware eingebettete Software, die in der Regel vom Markenhersteller oder einem vorgelagerten Original Design Manufacturer (ODM) entwickelt wird und in der sich der Großteil der Sicherheitsrisiken konzentriert.
3. **Der Verwaltungskanal** ist die Fernverbindung, über die der Hersteller nach der Installation Änderungen an das Gerät überträgt und die eine effektive, fortlaufende Kontrolle über das Gerät während seiner gesamten Lebensdauer darstellt.

Eine Kompromittierung einer einzelnen Ebene reicht aus, um das gesamte System zu gefährden. Dies bedeutet auch, dass die Souveränität über einen Router nicht erreicht werden kann, indem nur eine dieser Ebenen berücksichtigt wird. Ein Gerät, das in Europa montiert wurde, aber mit einer unter ausländischer Gerichtsbarkeit entwickelten Firmware läuft und Updates über im Ausland kontrollierte Server erhält, bleibt grundsätzlich gefährdet. Vor dem Hintergrund dieser Architektur können wir nun die drei Risikokategorien untersuchen, auf die jede ernsthafte regulatorische Maßnahme eingehen muss.

2.3 Drei zentrale Risiken

Die oben beschriebene dreischichtige Architektur – Hardware, Firmware und Update-Kanal – schafft drei unterschiedliche Risikokategorien, die jede ernsthafte regulatorische Maßnahme berücksichtigen muss.

- **Datenabfang (Firmware-Ebene).** Der Datenverkehr, der einen kompromittierten Router durchläuft, kann überwacht, kopiert und umgeleitet werden. Dies gilt unmittelbar für unverschlüsselten Datenverkehr und kann durch ausgefeiltere Angriffe auf Firmware-Ebene potenziell auch verschlüsselte Kommunikation betreffen.[10] Da der Router vor jedem Gerät im Netzwerk angesiedelt ist, verschafft eine einzige Kompromittierung einem Angreifer Einblick in die gesamten digitalen Aktivitäten eines Haushalts oder Unternehmens.

- **Nutzung für Cyberangriffe (Hardware- und Firmware-Ebene).** Kompromittierte Router sind der wichtigste Baustein von Botnets – großen Netzwerken aus gekaperten Geräten, die dazu dienen, Distributed-Denial-of-Service-Angriffe zu starten, Malware zu verbreiten und groß angelegten Diebstahl von Zugangsdaten durchzuführen. Da eine einzige Firmware-Sicherheitslücke alle Geräte desselben Herstellers gleichzeitig betreffen kann, verstärkt die Marktkonzentration dieses Risiko direkt.

- **Kill-Switch und Infrastrukturstörungen (Ebene des Update-Kanals).** Auf der Ebene des Update-Kanals spitzt sich dieses Risiko am stärksten zu. Ein Hersteller, der der Gerichtsbarkeit eines ausländischen Staates unterliegt, behält über den Update-Kanal eine effektive, fortwährende Kontrolle über jedes Gerät, das er jemals ausgeliefert hat. Ein staatlicher Akteur mit rechtlicher Autorität über diesen Internetdienstanbieter und/oder Hersteller kann diesen grundsätzlich anweisen, ein Firmware-Update zu veröffentlichen oder eine bereits integrierte, vorinstallierte Funktion zu aktivieren, die Millionen von Routern gleichzeitig deaktiviert, stört oder als Waffe einsetzt.

Gerade weil diese Risiken struktureller Natur und nicht nur zufällig sind, ist die Frage, wer europäische Router herstellt und liefert, keine Marktfrage: Es ist eine Sicherheitsfrage. Das Verständnis des aktuellen Zustands des europäischen Marktes für Netzwerkgeräte ist daher der notwendige Ausgangspunkt für jede ernsthafte politische Reaktion.

10 ENISA Threat Landscape 2024, Agentur der Europäischen Union für Cybersicherheit, Oktober 2024, abrufbar unter https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
ENISA Threat Landscape 2023, Agentur der Europäischen Union für Cybersicherheit, Oktober 2023, abrufbar unter https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

3
WER BEHERRSCHT DIE EUROPÄISCHEN NETZWERKE

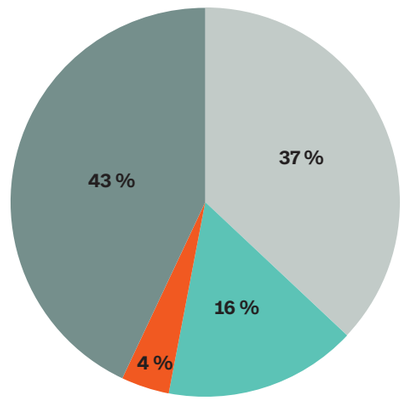
3.1 Marktstruktur bei Routern

Um die von Routern in Privathaushalten und KMU ausgehenden Risiken zu verstehen, bedarf es eines klaren Bildes des aktuellen europäischen Marktes. Die von der YouGov-Verbraucherumfrage 2025 zusammengestellten und durch GfK-Point-of-Sale-Paneldaten[11] ergänzten Daten liefern die umfassendste verfügbare Momentaufnahme.

Die Ergebnisse zeigen einen Markt, auf dem Hersteller mit Sitz in der Volksrepublik China neben europäischen und taiwanesischen Anbietern einen erheblichen Marktanteil halten. Auf Hersteller aus der EU und anderen Ländern entfallen etwa 43 % aller in europäischen Haushalten installierten Router und Repeater. Zu diesen Unternehmen zählen sowohl große Anbieter im ISP-Bereich wie Sagemcom und Vantiva als auch Marken, die direkt im Einzelhandel und in Fachsegmenten konkurrieren, darunter FRITZ!, Devolo, Lancom, Icotera, MikroTik und Teltonika. Chinesische Hersteller, darunter ZTE, Huawei, TP-Link, Xiaomi und Tenda, machen etwa 37 % der Geräte aus, was einer installierten Basis in schätzungsweise 95 Millionen europäischen Haushalten entspricht. Taiwanesische Anbieter, darunter Sercomm, Arcadyan, ASUS, D-Link und Zyxel, halten weitere 16 %, während die USA mit 4 % nur geringfügig vertreten sind und sich dabei auf das Einzelhandelssegment konzentrieren. Insgesamt machen Anbieter aus Nicht-EU-Ländern mehr als die Hälfte aller Router- und Repeater-Installationen in ganz Europa aus.

11 Zusammenstellung auf Basis der YouGov-Verbraucherumfrage 2025 (DE, AT, CH, NL, IT, UK); der internen ISP-CPE-Datenbank von FRITZ!; der GfK-Point-of-Sale-Panel-Daten 2025; sowie der Context-POS-Panel-Daten für ES, FR, BE, DK, NO, SE, FI (07/2023–06/2024). Für die übrigen europäischen Mitgliedstaaten wurde eine feste Annahme zugrunde gelegt. Die Zahlen dienen als Anhaltspunkte.

Router und Repeater in der EU nach Herstellerstandort



Quelle: YouGov-Umfrage 2025 in DE, AT, CH, NL, IT, UK: Bei ISP-Routern wurde die Aufschlüsselung nach Herstellungsländern anhand einer internen Wissensdatenbank zu ISP-CPEs ermittelt. Weitere Länder (CZ, DK, ES, FI, FR, GR, NO, PL, SE): Bei ISP-Routern wurde die Aufschlüsselung nach Herstellungsländern anhand einer internen Wissensdatenbank zu ISP-CPEs ermittelt. GFK-Daten zu den Marktanteilen von Repeatern

Herkunft der Hersteller	Die meisten Hersteller
Europäisch	Sagemcom und Vantiva sind im ISP-Kanal stark vertreten; FRITZ!, Devolo, Lancom, Icotera, MikroTik, Teltonika und weitere nationale Hersteller im Einzelhandel und in Fachgeschäften
Volksrepublik China	ZTE, Xiaomi, Huawei, TP-Link, Tenda, Reyee als White-Label-Produkte für Internetdienstanbieter und als Verbrauchermarken im Einzelhandel
Taiwan	Sercomm, Arcadyan, Compal, ASUS, D-Link, Zyxel – häufig als White-Label-Produkte für Internetdienstanbieter und teilweise auch als Verbrauchermarken
Vereinigte Staaten	Vor allem Netgear und eero (Amazon) konzentrieren sich auf den Einzelhandel. Cisco, Linksys, Ubiquiti, Belkin, Google und Starlink sind ebenfalls Internetanbieter.

Hinter diesen Marktanteilszahlen verbirgt sich eine Vertriebsdynamik, die die meisten europäischen Verbraucher nie zu Gesicht bekommen. Wie ein Router in einen Haushalt gelangt, bestimmt zu einem großen Teil, wessen Router es sein wird.

3.2 Wie Router zu europäischen Verbrauchern gelangen

Netzwerkgeräte für Privathaushalte und KMU gelangen über zwei unterschiedliche Vertriebskanäle zu den europäischen Nutzern, und der Unterschied zwischen diesen Kanälen prägt sowohl das Sicherheitsprofil der installierten Geräte als auch die politischen Hebel, die zur Verfügung stehen, um darauf einzuwirken.

Der erste Kanal ist **die Bereitstellung** durch **Internetdienstanbieter**. In den meisten europäischen Märkten erhalten die meisten Haushalte ihren Hauptrouter im Rahmen ihres Breitbandvertrags. Das Gerät wird vom Internetdienstanbieter im Rahmen einer kommerziellen Beschaffung ausgewählt, bei der Aktivierung installiert und bleibt dort in der Regel für die Dauer des Vertrags, oft über Jahre hinweg. Der Verbraucher spielt bei der Auswahl der Geräte keine Rolle und weiß in vielen Fällen nicht, wer das in seinem Haushalt installierte Gerät hergestellt hat.

Der zweite Kanal ist **der Kauf im Einzelhandel**. Verbraucher und kleine Unternehmen erwerben Router, Mesh-Systeme und Repeater direkt bei Elektronikfachhändlern, auf Online-Marktplätzen und bei Spezialanbietern. Zwar sind Informationen über die Herkunft in der Lieferkette und den Sitz des Herstellers auch in diesem Kanal nicht systematisch verfügbar, doch ist der Verbraucher zumindest an der Entscheidung beteiligt, neigt dazu, sich aktiver damit auseinanderzusetzen, und unterhält eine direkte Beziehung zum Gerät und dessen Hersteller.

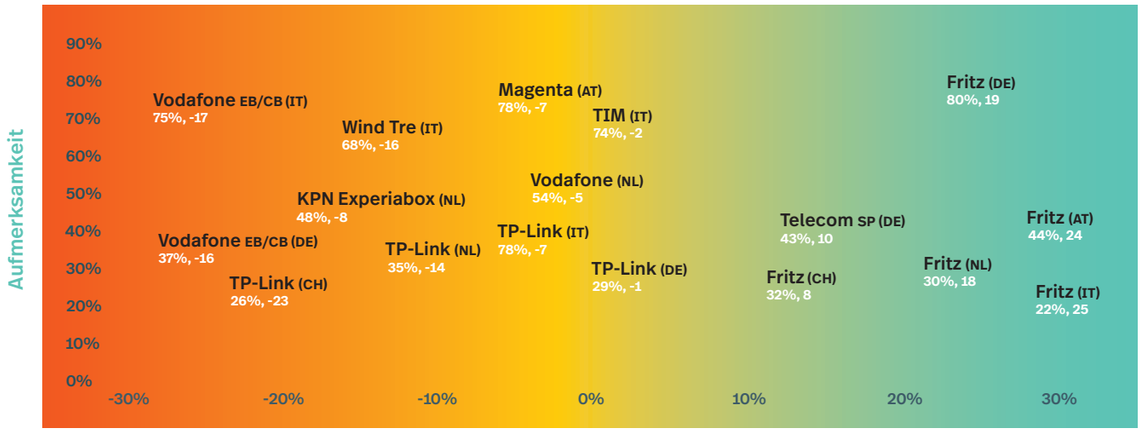
Diese beiden Vertriebskanäle führen zu systematisch unterschiedlichen Marktergebnissen. Dort, wo die Wahlfreiheit der Verbraucher stärker ausgeprägt ist – insbesondere in Märkten, in denen spezielle Gesetze zur Routerfreiheit erlassen wurden –, berichten die Verbraucher von einer höheren Zufriedenheit mit ihren Netzwerkgeräten und entscheiden sich überproportional häufig für Hersteller mit Hauptsitz in Europa.

Das europäische Recht erkennt bereits den Grundsatz an, dass Verbraucher ihre Endgeräte selbst wählen können sollten. Artikel 3 Absatz 1 der Verordnung über die Rechte der Nutzer elektronischer Kommunikationsdienste[12] legt das Recht der Endnutzer fest, bei der Anbindung an ein elektronisches Kommunikationsnetz Endgeräte ihrer Wahl zu verwenden. Die Mitgliedstaaten haben diesen Grundsatz mit unterschiedlicher Strenge umgesetzt. Das deutsche Gesetz zur freien Wahl von Telekommunikationsendgeräten aus dem Jahr 2016, bekannt als „Freie Routerwahl“[13] , stellte die strengste nationale Umsetzung dar und verpflichtete Internetdienstanbieter, ihren Kunden die Nutzung eigener Router zu gestatten und die dafür erforderlichen Zugangsdaten bereitzustellen. Italien hat 2018 vergleichbare Bestimmungen verabschiedet[14] , und in anderen Mitgliedstaaten gelten ähnliche Vorschriften mit unterschiedlichem Geltungsbereich. Andere europäische Märkte, darunter das Vereinigte Königreich, haben keine gleichwertigen Schutzmaßnahmen umgesetzt.

Bei der Betrachtung von Daten auf Markenebene in Verbindung mit der Marktstruktur zeichnet sich ein Muster ab. Wie die Grafik auf der nächsten Seite verdeutlicht, erzielen Marken, für die sich Verbraucher in Märkten mit effektiver Routerfreiheit entscheiden, durchweg positive Net Promoter Scores, während von Internetanbietern bereitgestellte und in China hergestellte Geräte unabhängig von ihrem Bekanntheitsgrad im negativen NPS-Bereich liegen. Die Marken, für die sich Verbraucher aktiv entscheiden, wenn sie die Wahl haben, genießen nicht nur mehr Vertrauen, sondern haben auch überwiegend ihren Hauptsitz in Europa. Dort, wo die Kaufentscheidung beim Verbraucher liegt, gehen Zufriedenheit und die Präferenz für europäische Hersteller Hand in Hand.

Die Daten weisen auf etwas hin, was die Zahlen zur Marktstruktur allein nicht erfassen: nämlich eine widerstandsfähige und von den Verbrauchern geschätzte europäische Industrie, die **dort** effektiv konkurriert**, wo die Bedingungen dies zulassen.** Wenn ihnen eine echte Wahlmöglichkeit und ausreichende Informationen geboten werden, tendieren europäische Verbraucher zu europäischen Produkten. Internetdienstanbieter handeln nicht rechtswidrig. Sie treffen rationale Beschaffungsentscheidungen innerhalb eines Rahmens, der von ihnen nicht verlangt, die Rechtsordnung des Herstellers, die Herkunft der Firmware oder Risiken in der Lieferkette abzuwägen. Die in diesem Papier dargelegten Empfehlungen sollen sicherstellen, dass Verbraucher, Internetdienstanbieter und öffentliche Einrichtungen alle über dieselben Informationen zu den Geräten verfügen, die in europäische Haushalte gelangen, und dass Hersteller aus Europa und Drittländern unter wirklich transparenten Wettbewerbsbedingungen konkurrieren. Wo diese Informationen vorliegen und Verbraucher darauf reagieren können, hat der Markt bereits gezeigt, in welche Richtung die Verbraucher tendieren.

Abbildung 2: Markenbekanntheit vs. Net Promoter Score nach Router-Hersteller



Quellen: Bekanntheit: Umfrage von M&R, 2024; NPS: Umfrage von YouGov, 2025

12 Verordnung (EU) 2015/2120, abrufbar unter: https://eur-lex.europa.eu/eli/reg/2015/2120/oj/eng

13 Freie Routerwahl, Bundesministerium für Wirtschaft und Energie der Bundesrepublik Deutschland, abrufbar unter https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Artikel/ Digitale-Welt/freie-routerwahl.html

14 Beschluss 348/18/CONS, Autorità Per Le Garanzie Nelle Comunicazioni, abrufbar unter https://www.agcom.it/provvedimenti/delibera-348-18-cons

Doch die Widerstandsfähigkeit europäischer Hersteller in den Segmenten, in denen sie heute konkurrieren, sollte nicht mit struktureller Sicherheit verwechselt werden. Aktuelle Markttrends, die von der im folgenden Abschnitt untersuchten Preisdynamik und der industriellen Unterstützung angetrieben werden, untergraben aktiv die Bedingungen, die diesen Wettbewerb erst möglich machen. Wenn sich diese Trends ungehindert fortsetzen, wird sich das Zeitfenster, in dem europäische Alternativen rentabel bleiben, verengen – und mit ihm die Auswahlmöglichkeiten für Verbraucher, die die Europäer so schätzen.

3.3 Ein Markt im Wandel

Die oben beschriebenen Marktanteile stellen kein statisches Bild dar. Sie spiegeln einen Markt wider, der sich aktiv in Richtung einer stärkeren Konzentration in den Händen von Herstellern mit Hauptsitz in der Volksrepublik China verschiebt, und die Dynamik, die diesen Wandel antreibt, beschleunigt sich.

Chinesische Hersteller von Netzwerkgeräten werden untersucht, ob sie von der chinesischen Regierung subventionierten Preisen profitieren, die den Markt zum Nachteil westlicher Hersteller von Kommunikationsgeräten in unfairer Weise beeinflusst haben. Das US-Justizministerium hat eine strafrechtliche kartellrechtliche Untersuchung eingeleitet, um zu prüfen, ob TP-Link durch den Verkauf von Routern unter Selbstkostenpreis Preisdumping betrieben hat[15] – eine Preisgestaltung, die, sollte sie sich bestätigen, jene Art struktureller staatlicher Unterstützung widerspiegeln würde, die privat finanzierte europäische und taiwanesische Hersteller weder abfedern noch mit der sie gleichziehen können. Sollte sich dies bestätigen, wäre die Folge eine schrittweise Verdrängung europäischer und vertrauenswürdiger außereuropäischer Hersteller aus einem Segment, das die Grundlage der digitalen Wirtschaft bildet.

Diese Verdrängung wird nun durch externen Druck noch verstärkt. Nach der Entscheidung der US-amerikanischen Federal Communications Commission vom März 2026, alle im Ausland hergestellten Verbraucher-Router aus Gründen der nationalen Sicherheit zu verbieten, stellen die vom US-Markt ausgeschlossenen chinesischen Hersteller erhebliche industrielle Kapazitäten dar, die nun keinen anderen Weg mehr haben, als auf andere offene Märkte auszuweichen. Hohe US-Zölle auf Importe aus China haben bereits zu einem messbaren Anstieg der chinesischen Exporte in die EU geführt, wobei die europäischen Märkte die umgeleiteten Kapazitäten in einer Reihe von Produktkategorien aufnehmen.[16] Wenn Europa sich seiner Anfälligkeit nicht bewusst wird und keine Maßnahmen ergreift, wird es zum natürlichen Ziel für eine Flut chinesischer Router werden, die selbst die Vereinigten Staaten als zu großes Sicherheitsrisiko erachten, um sie in ihren eigenen Netzwerken zuzulassen. Die Frage ist, was diese Anfälligkeit tatsächlich für die europäische Sicherheit bedeutet – dies ist das Thema des nächsten Abschnitts.

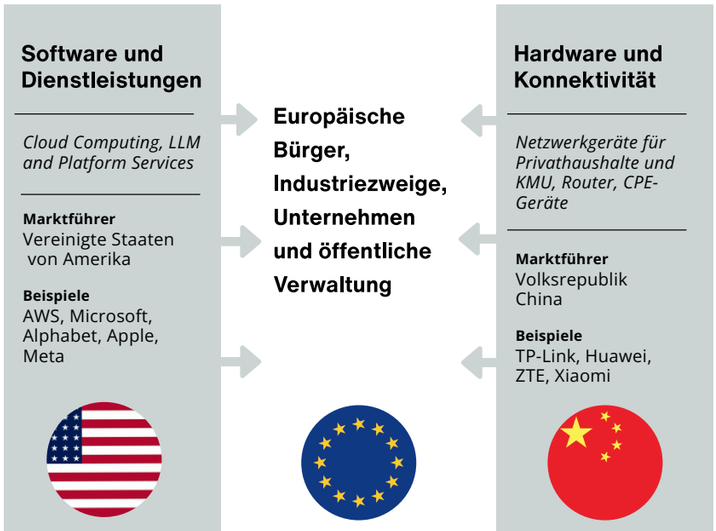
15 Bloomberg, Router-Hersteller TP-Link steht vor strafrechtlicher kartellrechtlicher Untersuchung in den USA, 24. April 2025, abrufbar unter https://www.bloomberg.com/news/articles/2025-04-24/router-maker-tp-link-faces-us-criminal-antitrust-investigation

16 CEPR VoxEU, Zölle, Handelsströme, Umleitungseffekte und Chinas Exporte in die EU, Februar 2026, abrufbar unter cepr.org/voxeu/columns/tarifs-trade-fows-diversion-efects-and-chinas-exports-eu

4
DIE BEDROHUNGS-LAGE

WIE BEREITS DARGESTELLT, befindet sich Europa in einer strukturell anfälligen Position innerhalb der digitalen Infrastruktur. In den oberen Schichten werden Cloud-Computing, KI-Infrastruktur und Plattformdienste von US-amerikanischen Unternehmen dominiert – eine Abhängigkeit, die seit einem Jahrzehnt zu Reaktionen in der Regulierungs- und Industriepolitik geführt hat. Auf der Hardware-Basisebene wird die Herstellung von Netzwerkgeräten für Endverbraucher zunehmend von Unternehmen mit Hauptsitz in der Volksrepublik China dominiert. Die europäischen Bürger und Institutionen befinden sich zwischen diesen beiden außereuropäischen Technologiepolen und sind einerseits von dem einen für ihre Software und andererseits von dem anderen für die Hardware abhängig, über die all dies läuft.

Die doppelte Abhängigkeit Europas
von amerikanischer Software und chinesischer Hardware



In den folgenden Abschnitten wird untersucht, was die im vorangegangenen Abschnitt dokumentierte Marktkonzentration von Hardwareherstellern mit Sitz in China für die europäische Sicherheit und Souveränität in drei unterschiedlichen, aber miteinander verbundenen Dimensionen bedeutet: dabei werden konventionelle Cybersicherheitsbedrohungen, geopolitische und staatliche Risiken sowie strukturelle Risiken für die industrielle Souveränität Europas behandelt.

4.1 IT-Sicherheit.
Botnetze, Schwachstellen und kriminelle Ausnutzung

Router aller Hersteller können Schwachstellen enthalten und tun dies auch. Die ENISA hat Router, Netzwerkgeräte und andere mit dem Internet verbundene Netzwerkinfrastrukturen wiederholt als bedeutende Angriffsflächen innerhalb der europäischen Cyberbedrohungslandschaft identifiziert[17] . Öffentliche Schwachstellendatenbanken, darunter das MITRE CVE[18] -Programm und die US-amerikanische National Vulnerability Database (NVD)[19] , dokumentieren zudem einen anhaltenden Strom offengelegter Schwachstellen, von denen Router und eingebettete Netzwerkgeräte verschiedener Hersteller betroffen sind.

Eine in Kürze erscheinende Studie der Gesellschaft für Informatik (GI), Deutschlands führendem Fachverband für Informatik, liefert die bislang detaillierteste Schwachstellenbewertung auf Anbieterebene für den deutschen Markt. Bei der Analyse der NVD für den Zeitraum 2020–2025 identifizierte die Studie 2.190 eindeutige Common Vulnerabilities and Exposures (bekannte Schwachstellen und Anfälligkeiten, CVEs), die die Router-Produkte der führenden Anbieter in Deutschland betreffen: Netgear (USA), D-Link (Taiwan), TP-Link (China) und AVM FRITZ! (Deutschland). Die Verteilung ist auffällig. Auf Netgear entfallen 1.016 CVEs (46 %) und auf D-Link 955 (44 %), während TP-Link 218 (10 %) aufweist. Der deutsche Hersteller FRITZ! verzeichnet über den gesamten Sechsjahreszeitraum hinweg nur eine einzige CVE. Die Unterschiede werden noch deutlicher, wenn man den Schweregrad betrachtet. Von den als „kritisch“ eingestuften CVEs – also solchen mit einem CVSS-Wert (Common Vulnerability Scoring System) von 9,0 oder höher, was auf nicht authentifizierten Fernzugriff, vollständige Systemübernahme oder die Ausführung von beliebigem Code hindeutet – entfallen 280 auf D-Link (29 % seiner Gesamtzahl), TP-Link 60 (28 % seiner Gesamtzahl) und Netgear 149 (15 % seiner Gesamtzahl). Fast jede dritte der für D-Link offengelegte Schwachstelle erreicht die höchste Schweregradklasse. Die Studie stellt fest, dass TP-Link trotz einer geringeren absoluten CVE-Anzahl im Vergleich zu Netgear einen fast doppelt so hohen relativen Anteil an kritischen Schwachstellen aufweist, was eher auf strukturelle Schwächen in grundlegenden Sicherheitsmechanismen wie Authentifizierung und Eingabevalidierung hindeutet als auf zufällige oder nebensächliche Mängel.

Das spezifische Risiko, das mit Anbietern mit hohem Marktanteil verbunden ist, ist das der Konzentration. Wenn die Firmware-Architektur eines einzelnen Herstellers eine Schwachstelle enthält – ob fahrlässig oder absichtlich eingeführt–, ist das Ausmaß der Gefährdung proportional zum Marktanteil. Eine Schwachstelle bei einem Anbieter, der 20 bis 50 % der Router-Installationen in Europa kontrolliert, bietet eine potenzielle Angriffsfläche, die sich gleichzeitig auf mehrere zehn Millionen vernetzte Geräte erstreckt. Die Malware-Kampagne „VPN Filter“, die von US-amerikanischen und britischen Behörden russischen staatlichen Akteuren zugeschrieben wird, demonstrierte genau diese Dynamik durch eine einzige koordinierte Operation, bei der Router verschiedener Herstellerplattformen kompromittiert und Hunderttausende von Geräten in 54 Ländern betroffen waren[20] . Der Angriff auf die Router-Infrastruktur der Deutschen Telekom im Jahr 2016, bei dem eine Schwachstelle in der Fernverwaltungsfunktion zum Absturz von etwa 900.000 Geräten führte

17 Internet-Infrastruktur: ENISA-Bedrohungslage, abrufbar unter: https://www.enisa.europa.eu/sites/default/files/all_files/Detailed%20Mind%20Map%20for%20Internet%20Infrastructure%20Assets.pdf

18 Verfügbar unter: https://www.cvedetails.com

19 Nationale Schwachstellendatenbank, abrufbar unter: https://nvd.nist.gov

20 US-CERT-Warnung TA16-288A, Erhöhte DDoS-Bedrohung durch Mirai und andere Botnetze, US-Behörde für Cyberabwehr, abrufbar unter https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

und fast eine Million Kundenverbindungen unterbrach[21] , bietet ein vergleichbares Beispiel auf nationaler Ebene.

Das Ausmaß der auf Routern basierenden Cyberkriminalität ist beträchtlich. Botnetze, die auf kompromittierten Routern aufbauen, waren für einige der größten DDoS-Angriffe verantwortlich, die jemals verzeichnet wurden, darunter anhaltende Angriffe auf kritische nationale Infrastrukturen, Finanzdienstleister und Gesundheitssysteme. Das Mirai-Botnetz, das 2016 große Teile der Internetinfrastruktur in den Vereinigten Staaten und Europa kurzzeitig lahmlegte, basierte hauptsächlich auf kompromittierten vernetzten Geräten, wobei Router einen wesentlichen Bestandteil darstellten[22],[23]. Nachfolgende Botnetz-Familien wie Meris, Mantis und deren Nachfolger haben dieselbe Schwachstellenarchitektur in noch größerem Umfang demonstriert.

Über groß angelegte Angriffe hinaus ermöglicht die Übernahme einzelner Router eine dauerhafte, gezielte Überwachung. Ein kompromittierter Router, der sich im Haus oder Büro einer hochrangigen Zielperson wie beispielsweise eines Regierungsbeamten, eines Journalisten, eines Rechtsanwalts oder eines Unternehmensleiters befindet, verschafft einem Angreifer dauerhaften, kaum erkennbaren Zugriff auf alle Netzwerkaktivitäten. Im Gegensatz zu Endpunkt-Malware sind Schwachstellen auf Firmware-Ebene bei Routern extrem schwer zu erkennen und können routinemäßige Neustarts des Geräts überstehen.

Auch die Bedrohungslandschaft entwickelt sich weiter. Da Tools der künstlichen Intelligenz zunehmend zugänglich werden, steigt entsprechend die Fähigkeit, kompromittierte Infrastruktur in großem Maßstab auszunutzen. Ein Botnetz aus Millionen kompromittierter Router, das durch KI-gestützte Befehls- und Kontrollmechanismen koordiniert wird, stellt eine qualitativ andere Bedrohung dar als dasselbe Botnetz, das mit herkömmlichen Mitteln betrieben wird. KI-Fähigkeiten werden zudem zur Erkennung von Schwachstellen eingesetzt, was in der Praxis dazu führt, dass die Zeitspanne zwischen der Bekanntwerdung einer Schwachstelle in der Router-Firmware und ihrer Ausnutzung in großem Maßstab immer kürzer wird. Die heute geltenden Sicherheitsüberlegungen werden sich mit der zunehmenden Verbreitung von KI-Fähigkeiten verschärfen, was die Notwendigkeit von Maßnahmen untermauert, solange die Konzentration der Marktanteile noch durch gewöhnliche politische Instrumente angegangen werden kann.

4.2 Geopolitische Risiken und Risiken auf staatlicher Ebene. Die rechtliche Architektur der Abhängigkeit

Die oben beschriebenen Cybersicherheitsrisiken gelten in unterschiedlichem Maße für jeden Hersteller mit unzureichenden Sicherheitspraktiken. Die speziell mit Herstellern mit Hauptsitz in der Volksrepublik China verbundene Besorgnis hat strukturelle Ursachen. Das rechtliche und politische Umfeld, in dem diese Unternehmen tätig sind, schafft Verpflichtungen, die durch keinen noch so großen guten Willen des Unternehmens und keine vertraglichen Vereinbarungen außer Kraft gesetzt werden können. Die zuvor zitierte GI-Studie stellt auf der Grundlage von Experteninterviews fest, dass die Zuordnung in diesem Bereich strukturell dadurch erschwert wird, dass dieselben Akteursgruppen häufig gleichzeitig als kriminelle Vereinigungen und als staatlich gelenkte Akteure agieren, was die binäre Unterscheidung zwischen kommerzieller Cyberkriminalität und geopolitischem Risiko erschwert.

Das Nationale Geheimdienstgesetz (2017) und das Spionageabwehrgesetz (2023) der VR China[24] erlegen allen Personen und Organisationen in der VR China rechtlich bindende Verpflichtungen auf, die staatlichen Geheimdienstaktivitäten der VR China zu unterstützen, ihnen Beistand zu leisten und mit ihnen zusammenzuarbeiten. Diese Verpflichtungen

21 Weltweiter Internetangriff, berichtet von der Deutschen Welle, abrufbar unter: https://www.dw.com/en/deutsche-telekom-hack-part-of-global-internet-attack/a-36574934

22 Offizielle Warnmeldung zu Mirai, CISA, abrufbar unter: https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

23 Was ist das Meris-Botnetz?, Erläuterung von Akamai zu Meris, abrufbar unter: https://www.akamai.com/glossary/what-is-the-meris-botnet

24 Gesetz der Volksrepublik China über den nationalen Nachrichtendienst (2017), Artikel 7 und 14; Spionageabwehrgesetz der Volksrepublik China (überarbeitet 2023), abrufbar unter: https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017

gelten für Unternehmen aus der VR China unabhängig davon, wo sie tätig sind. Ein Router-Hersteller mit Hauptsitz in der VR China, der einen Anteil von 20 bis 25 % am europäischen Markt hält, ist nach chinesischem Recht ein potenzielles Instrument des staatlichen Nachrichtendienstes der VR China, und dieser Status spiegelt eine rechtliche Verpflichtung wider, die nicht vertraglich ausgeschlossen werden kann.

Der Fall Huawei hat diese Bedenken im Zusammenhang mit der 5G-Infrastruktur so deutlich gemacht, dass er koordinierte politische Maßnahmen in der gesamten Europäischen Union und bei ihren wichtigsten Verbündeten ausgelöst hat. Huawei ist selbst ein Hersteller von Routern für Privathaushalte und KMU, die über europäische Einzelhandels- und ISP-Kanäle vertrieben werden. Die rechtliche Analyse, die die Beschränkungen für Huawei bei Kernnetzwerkausrüstung stützte, gilt mit derselben Logik auch für chinesische Hersteller von Routern für Privathaushalte und KMU. Die relevante Frage ist, ob der für einen Hersteller geltende Rechtsrahmen eine strukturelle Voraussetzung für eine potenzielle Zwangsausübung schafft, die mit den Sicherheitsanforderungen kritischer Infrastrukturen unvereinbar ist.

Das „Kill-Switch"-Szenario stellt den extremsten Ausdruck dieses Risikos dar und ist keine hypothetische Sorge. Wie bereits erwähnt, machen chinesische Hersteller zusammen etwa 37 % des gesamten europäischen Marktes für Router und Repeater aus, was bedeutet, dass eine koordinierte Firmware-Anweisung, die über diese installierte Basis verbreitet wird, gleichzeitig die Internetverbindung für Dutzende Millionen europäischer Haushalte und KMU unterbrechen könnte. Ein Hersteller mit Hauptsitz in der VR China, der über eine derart starke Marktpräsenz verfügt, der der staatlichen Aufsicht der VR China unterliegt und Geräte mit der Möglichkeit zur Fernaktualisierung der Firmware betreibt, stellt einen potenziellen Vektor für koordinierte Infrastrukturstörungen auf nationaler oder europäischer Ebene dar. Die Entscheidung der Kommission vom Mai 2026, die Finanzierung von Projekten mit chinesischen Solarwechselrichtern einzustellen, wobei ausdrücklich das Risiko einer koordinierten Fernmanipulation zur Verursachung von Netzinstabilität angeführt wurde, zeigt, dass europäische Entscheidungsträger diesen Bedrohungsvektor bereits als real und handlungsrelevant anerkennen.

Staatlich geförderte Cyberoperationen, die die Router-Infrastruktur ausnutzen, wurden wiederholt dokumentiert. In der gemeinsamen Warnung der US-Behörden NSA, CISA, FBI und der „Five Eyes"-Partner aus dem Jahr 2023 wurde eine anhaltende Kampagne zur Ausnutzung von Routern Akteuren zugeschrieben, die mit dem chinesischen Staat in Verbindung stehen. Es wurde festgestellt, dass im Rahmen der „Volt Typhoon"-Kampagne von 2024 über kompromittierte Network-Edge-Geräte Schadcode in kritischen Infrastrukturen der Vereinigten Staaten platziert worden war.[25] Im Jahr 2025 schrieb das tschechische Außenministerium einen anhaltenden Cyberangriff öffentlich staatlichen Akteuren der VR China zu. Im selben Jahr bestätigten US-Behörden, dass die „Salt Typhoon"-Kampagne, die staatlichen Hackern der VR China zugeschrieben wurde, die Telekommunikationsinfrastruktur in mindestens 80 Ländern kompromittiert hatte.[26]

Eine kurze Anmerkung zu Taiwan ist angebracht, da taiwanesische Hersteller einen vergleichbaren Marktanteil halten. Taiwan verfügt über eine demokratische Verfassungsordnung und eine unabhängige Justiz, ohne dass es ein Äquivalent zum chinesischen Nationalen Geheimdienstgesetz von 2017 gibt, das private Unternehmen zur verdeckten Zusammenarbeit mit staatlichen Geheimdienstoperationen verpflichtet. Im Rahmen der EU-Strategie zur Risikominderung und wirtschaftlichen Sicherheit wird Taiwan eher als Partner denn als systemischer Rivale behandelt. Taiwans geopolitische Abhängigkeit von der VR China und die weit verbreitete Verwendung von Firmware aus der VR China in Produkten taiwanesischer Marken sind nach wie vor aktuelle Überlegungen; aus diesem Grund beziehen sich die Empfehlungen in Abschnitt 7 neben dem Herkunftsort der Hardware-Baugruppen auch auf die Herkunft der Firmware und die Kontrolle der Update-Kanäle.

25 Gemeinsame Cybersicherheitswarnung – Von der Volksrepublik China staatlich geförderte Cyberakteure nutzen Netzbetreiber und Geräte aus. NSA, CISA, FBI und Partner, abrufbar unter: CISA – Von der Volksrepublik China staatlich geförderte Cyberakteure nutzen Netzbetreiber und Geräte aus (AA22–158A)

26 US-Behörden: Chinesische Telekom-Hacker in 80 Ländern aktiv, Deutschlandfunk, abrufbar unter: https://www.deutschlandfunk.de/us-behoerden-chinesische-telekom-hacker-in-80-laendern-aktiv-102.html

4.3 Strategische Souveränität und die Dimension der Wettbewerbsfähigkeit

Die dritte Dimension der Bedrohungslandschaft ist weniger unmittelbar, aber nicht weniger folgenreich. Wer die physische Hardware herstellt, bestimmt nicht nur, wer den wirtschaftlichen Wert des Marktes für Netzwerkgeräte für sich beansprucht, sondern auch, wer die Grundlage kontrolliert, auf der die Ebenen der Firmware und der Update-Kanäle beruhen. Der Verlust der Hardware-Ebene bedeutet den Verlust der Fähigkeit, die darüber liegenden Ebenen zu steuern.

Europäische Routerhersteller konkurrieren auf einem offenen Markt mit Anbietern, deren Kostenstrukturen eher eine anhaltende staatliche Unterstützung widerspiegeln als allein den Marktwettbewerb. Die Einschätzung der Rhodium Group vom Mai 2025 kam zu dem Schluss, dass Chinas Strategie darin bestand, seine Dominanz in fortschrittlichen Fertigungssektoren systematisch auszubauen – durch eine Kombination aus staatlichen Subventionen, bevorzugtem Marktzugang und dem Ausschluss ausländischer Wettbewerber vom heimischen Markt.[27] Die Folge für europäische Hersteller von Netzwerkgeräten ist eine schrittweise Verdrängung aus einem Markt, der sowohl wirtschaftlich bedeutend als auch strategisch kritisch ist.

Die unterschiedlichen Ansätze der USA und Europas verstärken diese Dynamik noch. Chinesische Hersteller, die vom US-Markt ausgeschlossen sind, haben ihren Fokus verstärkt auf den europäischen Markt gerichtet und damit genau jene Konzentrationsdynamik beschleunigt, die Sicherheitsrisiken mit sich bringt. Die europäische Infrastruktur wird zur globalen Ausnahme – als einzige große Industrienation, die ihre Türen für Anbieter offen hält, die anderswo aus Sicherheitsgründen ausgeschlossen werden. Europa verfügt nach wie vor über eine bedeutende Produktionspräsenz auf dem Router-Markt. Dieses Fenster wird jedoch nicht auf unbestimmte Zeit offen bleiben.

27 „Was Made in China 2025 Successful?“, erstellt für die US-Handelskammer, abrufbar unter rhg.com/wp-content/uploads/2025/05/Was-MIC25-Successful.pdf

Die Marktanalyse des GI-Berichts zum deutschen Router-Segment liefert einen anschaulichen Gegenpol. In Deutschland, wo die Abschaffung des Routerzwangs im Jahr 2016 den Verbrauchern das gesetzliche Recht einräumte, ihren eigenen Router zu wählen, konkurrieren europäische Hersteller erfolgreich auf der Grundlage der Vorzüge ihrer Produkte. Unternehmen wie Devolo, FRITZ! und Lancom behaupten starke Positionen im Einzelhandel und im Fachhandel, während der größte Breitbandanbieter, die Deutsche Telekom, trotz eines Anteils von mehr als 40 % an den Breitbandanschlüssen nur 19 % des Routermarktes hält. Diese Asymmetrie verdeutlicht, dass europäische Hersteller dort, wo die Wahlfreiheit der Verbraucher greift, bedeutende Marktanteile gegenüber Anbietern halten und verteidigen können, die ausschließlich über den Preis konkurrieren. Umgekehrt führen in Segmenten und Rechtsräumen, in denen keine Wahlfreiheit der Verbraucher besteht, die strukturellen Vorteile staatlich subventionierter Wettbewerber direkter zu einer Verdrängung vom Markt.

Die drei in diesem Abschnitt beschriebenen Risikodimensionen bilden in ihrer Gesamtheit ein Profil, mit dem europäische Entscheidungsträger bereits zuvor konfrontiert waren und für das sie bereits gezeigt haben, dass sie es bewältigen können. Die rechtliche Möglichkeit zur Zwangsverpflichtung ausländischer Hersteller, die Konzentration von Marktanteilen in den Händen von Anbietern aus einem einzigen nicht verbündeten Rechtsraum und die strukturelle Schwierigkeit, Abhängigkeiten wieder aufzulösen, sobald sie sich vertieft haben, waren genau die Bedingungen, die die Debatte über die 5G-Netzinfrastruktur zwischen 2018 und 2020 geprägt haben. Europa begegnete dieser Herausforderung mit einem koordinierten, risikobasierten Rahmen, der sich als sowohl praktikabel als auch als wirksam erwiesen hat.

In den folgenden Abschnitten wird untersucht, wie dieses Rahmenwerk aufgebaut wurde, wie es seitdem auf andere Sektoren ausgeweitet wurde und warum derselbe Ansatz, angewandt auf Router, zu derselben Schlussfolgerung führt.

5
DIE 5G-ANALOGIE UND EIN HANDLUNGS-MODELL

5.1 Wie die EU die Sicherheit der 5G-Lieferkette angegangen ist

Der Ansatz der Europäischen Union zur Sicherheit der 5G-Lieferkette stellt den relevantesten Präzedenzfall für die in diesem Papier empfohlenen Maßnahmen dar. Er ist zudem ein konkreter Beweis dafür, dass koordinierte, risikobasierte Regulierungsmaßnahmen im Bereich der Netzinfrastruktur erfolgreich sein können.

Die „5G-Cybersicherheits-Toolbox“, die im Januar 2020 von der NIS-Kooperationsgruppe verabschiedet und in der Mitteilung der Europäischen Kommission zu „Secure 5G“ befürwortet wurde, schuf einen Rahmen, der auf drei sich gegenseitig verstärkenden Elementen basiert. Erstens eine gemeinsame Methodik zur Risikobewertung, die die Mitgliedstaaten auf ihre 5G-Lieferketten anwenden mussten. Zweitens ein Bündel strategischer Maßnahmen, darunter die Identifizierung von Lieferanten mit hohem Risiko und die Möglichkeit, solche Lieferanten in Kern- und sensiblen Teilen des Netzes einzuschränken oder auszuschließen. Drittens einen koordinierten Umsetzungsprozess in den Mitgliedstaaten, der durch Leitlinien der Kommission unterstützt wurde und de facto zum Ausschluss von Huawei und ZTE aus der zentralen 5G-Netzinfrastruktur in der überwiegenden Mehrheit der EU-Mitgliedstaaten führte. Beide Unternehmen sind zudem als Hersteller von Netzwerkgeräten für Privathaushalte und KMU vertreten und verfügen zusammen über einen erheblichen Marktanteil in den europäischen Einzelhandels- und ISP-Kanälen.

Die wichtigste Erkenntnis aus der 5G-Toolbox ist, dass die EU nicht nachweisen musste, dass ein konkreter Verstoß vorlag. Eine risikobasierte Bewertung, ob die rechtlichen, technischen und geopolitischen Rahmenbedingungen eines bestimmten Anbieters ein inakzeptables Risiko für kritische Infrastrukturen darstellten, reichte aus. Auf dieser Grundlage wurden Maßnahmen ergriffen und die Märkte effektiv umgestaltet. Das Zusammenspiel von Sicherheitsklassifizierung, Beschaffungsvorschriften und Marktsignalen führte zu einem Ergebnis, das kein einzelnes Instrument allein hätte erzielen können.

Die 5G-Toolbox wartete nicht auf einen Sicherheitsverstoß. Es wurde ein risikobasierter Rahmen eingesetzt, um einen solchen zu verhindern. Die Anwendung desselben Rahmens auf Router führt zu derselben Schlussfolgerung und derselben Handlungsnotwendigkeit.

Das gleiche analytische Rahmenwerk, angewandt auf Router für Privathaushalte und KMU, führt zu derselben Schlussfolgerung. Die rechtlichen Rahmenbedingungen für Router-Hersteller mit Hauptsitz in der VR China sind identisch mit denen für 5G-Ausrüster mit Hauptsitz in der VR China. Die Risikovektoren, darunter Datenabfang, „Kill-Switch"-Fähigkeit und Möglichkeit zur Zwangsverpflichtung durch den Staat, sind strukturell analog. Die Marktkonzentration ist dokumentiert. Das Zeitfenster für Maßnahmen, bevor die Abhängigkeit unumkehrbar wird, besteht jetzt, so wie es 2019 und 2020 bei 5G der Fall war.

5.2 Ein einheitliches Handlungsmuster über alle Sektoren hinweg

Der Fall 5G ist keineswegs ein Einzelfall. Bei einer branchenübergreifenden Betrachtung zeigt sich in der Politik der EU und der Mitgliedstaaten eine kohärente und zunehmend angewandte Logik. Dort, wo chinesische Hersteller einen bedeutenden Marktanteil bei Hardware mit Fernzugriffsmöglichkeiten und Auswirkungen auf die kritische Infrastruktur halten, hat Europa Maßnahmen ergriffen, um diese einzuschränken, zu regulieren oder Risiken zu mindern. Der Fall der Router stellt dabei eine auffällige Ausnahme dar.

Die Tabelle auf den folgenden Seiten gibt einen Überblick über dokumentierte Maßnahmen der EU und der Mitgliedstaaten in verschiedenen Sektoren, in denen Risiken in der chinesischen Lieferkette zu regulatorischen Reaktionen geführt haben.

Tabelle 1. Sektorübergreifender Vergleich der Maßnahmen der EU und ihrer Partnerländer hinsichtlich der Präsenz von Lieferanten aus Hochrisikoländern in kritischen Hardwarekategorien, 2020 bis 2026

Sektor	Begründung	Maßnahmen der EU	Entsprechungen außerhalb der EU
Solarwechselrichter	Risiko einer koordinierten Fernmanipulation der Firmware, die zu Störungen im gesamten Stromnetz führen könnte. Der Großteil der in der EU installierten Wechselrichter wird in China hergestellt.[28]	Beschluss der Kommission von April–Mai 2026, die EU-Finanzierung im Rahmen der Kohäsions- und Wiederaufbauinstrumente für Projekte einzustellen, bei denen Wechselrichter aus Hochrisikoländern, darunter die VR China, Russland, Iran und Nordkorea, zum Einsatz kommen; Mitteilung an die Finanzinstitute ab dem 1. Mai 2026 und Formalisierung in den Leitlinien der Kommission vom 13. Mai 2026.[29]	**China:** Inländische Hersteller wie Huawei, Sungrow und Ginlong haben auf dem globalen Wechselrichtermarkt eine marktbeherrschende Stellung erreicht, unterstützt durch die Industriepolitik „Made in China 2025", die von staatlichen Unternehmen gesteuerte Beschaffung sowie strukturelle Größenvorteile[30] , die die Wettbewerbsposition europäischer Anbieter auf dem chinesischen Markt erheblich eingeschränkt haben. **USA:** Über 54 Republikaner im Repräsentantenhaus forderten im November 2025 offiziell Einfuhrbeschränkungen für chinesische Wechselrichter und verwiesen dabei auf kritische Risiken für die Netzsicherheit, darunter die Entdeckung nicht genehmigter Kommunikationsgeräte in in China hergestellten Wechselrichtern, die einen Fernzugriff auf die Netzinfrastruktur ermöglichen könnten.[31] **Japan:** Das METI und die ANRE widmen den Risiken für die Lieferkette und die Cybersicherheit im Energiesektor verstärkt Aufmerksamkeit und veröffentlichten im Juni 2025 Leitlinien zur Lieferkettensicherheit für Stromsteuerungssysteme. Gemäß dem Gesetz zur Förderung der wirtschaftlichen Sicherheit von 2022 unterliegen ausgewiesene Betreiber kritischer Infrastrukturen in Sektoren wie dem Energiesektor einer Vorabmeldepflicht und einer staatlichen Überprüfung, bevor sie bestimmte kritische Anlagen installieren – ein Rahmenwerk, das auch in Stromversorgungssystemen verwendete Geräte, einschließlich Wechselrichter, umfassen kann.[32]

FORTSETZUNG ►

28 Kommission blockiert EU-Fördermittel für Huawei, Politico, abrufbar unter: https://www.politico.eu/article/commission-blocks-eu-funding-for-huawei-solar-tech

29 Euronews-Bericht über risikoreiche Wechselrichter, abrufbar unter: https://www.euronews.com/my-europe/ 2026/05/04/eu-moves-to-ban-high-risk-inverters-from-china-over-cybersecurity-threats

30 Die Umwälzungen in Chinas Solarindustrie werden globale Auswirkungen haben, abrufbar unter: https://www.csis.org/analysis/chinas-solar-industry-upheaval-effects-will-be-global

31 US-Republikaner drängen Trump, Importe chinesischer Wechselrichter zu blockieren, abrufbar unter: https://rsc-pfluger.house.gov/media/press-releases/rsc-calls-out-chinese-solar-inverters-security-risk-us-energy-infrastructure

32 Leitfaden zu Maßnahmen zur Sicherheit der Lieferkette für Leistungssteuerungssysteme veröffentlicht, METI, abrufbar unter: https://www.meti.go.jp/english/press/2025/0603_007

Sektor	Begründung	Maßnahmen der EU	Entsprechungen außerhalb der EU
5G Kernnetz	Rechtliche Verpflichtbarkeit von Herstellern nach chinesischem Staatsrecht, Möglichkeit zur Fernaktualisierung von Firmware, konzentriertes Lieferantenrisiko	5G-Toolbox 2020. Beschränkungen für risikoreiche Lieferanten durch die Mitgliedstaaten, de facto Ausschluss von Huawei und ZTE in den meisten Mitgliedstaaten[33]	**China:** Nach der Überarbeitung der chinesischen „Cybersecurity Review Measures“ im Jahr 2022[34] , durch die die Aufsicht der CAC auf die Beschaffung durch Betreiber kritischer Informationsinfrastrukturen ausgeweitet wurde, wurden Verträge von Nokia und Ericsson einer Überprüfung im Hinblick auf die nationale Sicherheit unterzogen, deren Kriterien nicht offengelegt wurden. Der gemeinsame Marktanteil beider Anbieter in Chinas Mobilfunknetzen sank von etwa 12 % im Jahr 2020 auf rund 3 % bis 2025. Der Umsatz von Nokia in der Region „Greater China“ ging zwischen 2019 und 2025 um 58 % zurück, von etwa 2,2 Mrd. € auf 913 Mio. €.[35] **USA:** „Secure and Trusted Communications Networks Act“ von 2019 und die „FCC Covered List“, in der Huawei und ZTE aufgeführt sind; „Secure Equipment Act“ von 2021, der weitere FCC-Genehmigungen für gelistete Geräte verbietet.[36] **Großbritannien:** Verbot neuer Huawei-Geräte im 5G-Netz ab 2021, vollständige Entfernung bis Ende 2027. **Australien:** Huawei und ZTE sind seit 2018 ausgeschlossen. **Kanada:** Huawei und ZTE sind ab Mai 2022 für 5G und 4G verboten, Entfernung 2027.
Elektrofahrzeuge in der Nähe kritischer Standorte	Fernmessung, dauerhafte Standortbestimmung, Erfassung von Bordsensordaten sowie die Möglichkeit der Fernabschaltung oder -störung; Möglichkeit zur Zwangsverpflichtung von Herstellern mit Hauptsitz in der VR China gemäß staatlichem Recht der VR China.	Polen (Federführung), weitere Mitgliedstaaten erarbeiten Beschränkungen für in der VR China hergestellte Elektrofahrzeuge in der Nähe sensibler Infrastruktur [37]	**China:** Ab 2021 verboten die chinesischen Behörden den Zugang von Tesla-Fahrzeugen zu Militärstützpunkten, Regierungsgebäuden, Flughäfen und einer wachsenden Zahl staatlicher Einrichtungen, wobei sie Bedenken hinsichtlich der Datensicherheit im Zusammenhang mit den Sensoren und der Konnektivität der Fahrzeuge anführten. Tesla blieb von den meisten staatlichen Beschaffungslisten ausgeschlossen und durfte ohne behördliche Genehmigung keine Fahrzeugdaten außerhalb Chinas übertragen.[38] **USA:** Endgültige Verordnung des Handelsministeriums vom Januar 2025 im Rahmen der Zuständigkeit für Informations- und Kommunikationstechnologie und -dienste, die den Import und Verkauf vernetzter Fahrzeuge verbietet, die mit der Volksrepublik China oder Russland verbundene Fahrzeugvernetzungssysteme (Hardware und Software) sowie Software für automatisierte Fahrsysteme enthalten; schrittweise Einführung ab dem Modelljahr 2027 (Software) und dem Modelljahr 2030 (VCS-Hardware).[39] **Großbritannien:** Die Regierung führt derzeit eine Untersuchung durch, nachdem im Januar 2023 Berichte über in Regierungsfahrzeugen eingebaute, in der VR China hergestellte Ortungsgeräte bekannt wurden.[40]

FORTSETZUNG ►

33 EU-5G-Toolbox und Mitteilung der Kommission zu Huawei und ZTE: https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation5g-cybersecurity-toolbox
34 China hat neue Maßnahmen für die Cybersicherheitsprüfung im Jahr 2022 erlassen, abrufbar unter: https://www.whitecase.com/insight-alert/china-issued-new-measures-cybersecurity-review-2022
35 Ericsson und Nokia verzeichnen einen drastischen Umsatzrückgang in China, abrufbar unter: https://www.lightreading.com/5g/ericsson-and-nokia-see-their-sales-in-china-fall-of-a-clif
36 Gesetz über sichere und vertrauenswürdige Kommunikationsnetze von 2019, abrufbar unter https://www.congress.gov/bill/116th-congress/house-bill/4998
FCC-Liste der betroffenen Unternehmen (Einträge zu Huawei und ZTE), abrufbar unter: https://www.fcc.gov/supplychain/coveredlist
Gesetz über sichere Ausrüstung von 2021, abrufbar unter: https://www.congress.gov/bill/117th-congress/ house-bill/3919

37 Polen verbietet chinesische Autos auf Militärgeländen: https://www.fdd.org/analysis/2026/02/20/ poland-bans-chinese-cars-from-military-sites-over-spying-fears
38 Tesla-Fahrzeuge sehen sich in China weiteren Einfuhrverboten gegenüber, da „Sicherheitsbedenken“ zunehmen, abrufbar unter: https://asia.nikkei.com/spotlight/supply-chain/tesla-cars-face-more-entry-bans-in-china-as-security-concerns-accelerate
39 US-Bundesregister, abrufbar unter: https://www.federalregister.gov/documents/2025/01/16/2025-00592/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles
40 Verstecktes chinesisches Ortungsgerät „in Fahrzeug der britischen Regierung gefunden“ löst Befürchtungen um die nationale Sicherheit aus, abrufbar unter: https://inews.co.uk/news/hidden-chinese-tracking-device-government-car-national-security-2070152

Sektor	Begründung	Maßnahmen der EU	Entsprechungen außerhalb der EU
Netzwerkgeräte (Router für Privatkunden und KMU)	**Identische Risikofaktoren wie in den oben genannten Sektoren:** rechtliche Durchsetzbarkeit der Möglichkeit von Fern-Firmware-Updates durch Hersteller mit Hauptsitz in der VR China, eine zum Zeitpunkt der EU-Maßnahmen vergleichbare oder höhere Marktkonzentration als bei 5G-Kernnetzen sowie eine wesentlich größere installierte Basis.	**Für Netzwerkgeräte für Privatkunden und KMU gilt kein koordinierter EU-Rahmen, der mit der 5G-Toolbox vergleichbar wäre.** Horizontale Instrumente wie der Cyber Resilience Act und der delegierte Rechtsakt zur Funkgeräterichtlinie gelten zwar für Router für Privatkunden, bieten jedoch keinen Mechanismus zur Risikoklassifizierung der Lieferkette. Der vorgeschlagene Cybersecurity Act 2 führt einen solchen Mechanismus für kritische ITK-Lieferketten ein, erstreckt sich jedoch in der derzeitigen Fassung nicht auf Netzwerkgeräte für Privatkunden und KMU.	**China:** Im Jahr 2014, nach den Enthüllungen von Snowden über die Überwachung von im Ausland verkauften Geräten durch die NSA, strich das chinesische Zentrale Beschaffungszentrum für die Regierung Cisco, Apple, Intel, McAfee und Citrix von seiner Liste zugelassener Lieferanten.[41] **USA:** Entscheidung der FCC[42] vom 23. März 2026, alle im Ausland hergestellten Router für Endverbraucher in die „FCC Covered List“ aufzunehmen und die Zulassung neuer Modelle zu verbieten; bestehende Geräte unterliegen einer Bestandsschutzregelung, wobei für Hersteller eine Ausnahmeregelung für Software-Updates bis zum 1. März 2027 gilt. Ende 2024 wurde vom US-Justizministerium eine strafrechtliche kartellrechtliche Untersuchung gegen TP-Link eingeleitet.[43] **Großbritannien, Kanada und Australien** haben jeweils Leitlinien oder Betriebsbeschränkungen für risikoreiche Netzwerkgeräte herausgegeben; in jeder dieser Rechtsordnungen werden derzeit formelle Regulierungsrahmen für Router entwickelt.

41 China streicht US-Technologiegiganten von der Zulassungsliste, abrufbar unter: https://www.bbc.com/news/ technology-31640539

42 FCC aktualisiert Liste der betroffenen Geräte um im Ausland hergestellte Verbraucher-Router und verbietet die Zulassung neuer Modelle, abrufbar unter: https://docs.fcc.gov/public/attachments/DOC-420034A1.pdf

43 USA führen strafrechtliche kartellrechtliche Ermittlungen gegen TP-Link durch, abrufbar unter: https://www.reuters.com/technology/tp-link-faces-us-criminal-antitrust-investigation bloomberg-news-reports-2025-04-25

Das länderübergreifende juristische Bild ist auffällig. In jedem der oben aufgeführten Bereiche hat die Europäische Union im Einklang mit ihren wichtigsten demokratischen Partnern gehandelt, mit einer Ausnahme: Bei Netzwerkgeräten steht Europa unter den großen Industrienationen allein da, wenn es darum geht, den offenen Marktzugang für Anbieter aufrechtzuerhalten, die anderswo aus identischen Sicherheitsgründen eingeschränkt wurden – insbesondere im Hinblick auf die Netzwerksicherheit. Dies ist keine neutrale Position. Die Anwendung der Risikologik der „5G-Toolbox“ auf Mobilfunknetze bei gleichzeitiger Nichtregulierung von Netzwerkgeräten ist eine Inkonsistenz, für deren Beibehaltung sich keine verbündete Rechtsordnung entschieden hat – und die mit jedem Monat schwerer zu rechtfertigen ist.

Abbildung 3: Ein Sonderfall unter Gleichgesinnten: Die EU verfügt über keinen Rahmen für die Sicherheit von Heimnetzwerkgeräten

	Mobilfunk/5G	Netzwerkgeräte
China	! Einschränkungen bestehen	! Einschränkungen bestehen
USA	! Einschränkungen bestehen	! Einschränkungen seit 04/2026
EU	! 5G Toolbox 2020	– Kein koordinierter Rahmen

Die EU hat im Jahr 2020 die Logik der Lieferkettensicherheit auf 5G angewendet. Bei Breitband-Heimnetzgeräten für das Festnetz hat sie diese Logik jedoch nicht angewandt. Alle vergleichbaren Rechtsordnungen sind Europa voraus oder bewegen sich in diese Richtung.

Dieser strukturelle Widerspruch lässt sich auch öffentlich nur schwer rechtfertigen. Europa schränkt den Einsatz chinesischer Solarwechselrichter ein, um das Stromnetz zu schützen, beschränkt den Einsatz chinesischer Geräte in 5G-Netzen, um die Kommunikationsinfrastruktur zu schützen und erwägt Einschränkungen für chinesische Fahrzeuge in der Nähe sensibler Standorte – erlaubt jedoch den uneingeschränkten Einsatz chinesischer Router, die die Internetverbindung jedes europäischen Privathaushalts und Unternehmens verwalten.

6
WAS BEREITS IN BEWEGUNG IST

DIE ARGUMENTE FÜR MASSNAHMEN zur Netzwerksicherheit erfordern keinen Neuanfang bei der Regulierung. Es gibt bereits ein umfangreiches EU-Recht, das Teile des Problems behandelt, entsprechende Verpflichtungen schafft und in mehreren Fällen auf die Lücke hinweist, die ein spezielles Instrument zur Routersicherheit schließen würde. Zu verstehen, was bereits in Gang ist, ist ebenso wichtig wie zu erkennen, was fehlt.

Tabelle 2. EU-Rechtsakte zur Sicherheit der Lieferkette von Netzwerkgeräten: Analyse der Beiträge und Lücken

Rechtsakt	Relevanz	Beitrag und Lücke
Cybersicherheitsgesetz 2 (Vorschlag, COM(2026) 11)	Sehr hoch	Befindet sich derzeit in der Anfangsphase des ordentlichen Gesetzgebungsverfahrens. Schafft einen Rahmen für eine vertrauenswürdige ITK-Lieferkette mit der Möglichkeit, Lieferanten als risikoreich einzustufen und Verbote zu erlassen. Das Gesetzgebungsinstrument, durch das die langfristige Empfehlung in diesem Papier umgesetzt werden kann.
Gesetz zur Förderung der Industrie (Vorschlag)	Hoch	Vorschlag der Kommission, veröffentlicht im März 2026 im Rahmen der Umsetzung des „Clean Industrial Deal“ und des „Competitiveness Compass“. Setzt die Beschaffungspräferenzen für „Made in EU“-Produkte fort, der Anwendungsbereich ist jedoch auf energieintensive Industrien (Stahl, Zement, Aluminium), Elektrofahrzeuge und Netto-Null-Technologien beschränkt. Router und ITK-Geräte fallen derzeit nicht in den Anwendungsbereich; eine Einbeziehung von Netzwerkgeräten erfordert einen spezifischen politischen Beschluss.
Überarbeitung der Richtlinien über das öffentliche Auftragswesen	Hoch	Die Überarbeitung der Richtlinie 2014/24/EU ist in Vorbereitung. Sie bildet die wichtigste Rechtsgrundlage für branchenneutrale Beschaffungspräferenzen und durch nationale Sicherheitsinteressen gerechtfertigte Ausschlüsse, unter anderem für Netzwerkgeräte.
TPaket zur technologischen Souveränität	Mittel	Mitteilung der Kommission und begleitende Maßnahmen, 2026. Legt den strategischen Rahmen für bereichsübergreifende Maßnahmen zur digitalen Souveränität im gesamten Zuständigkeitsbereich der Kommission fest. Netzwerkgeräte werden derzeit nicht als vorrangiger Arbeitsschwerpunkt genannt.
Cyberresilienz-Verordnung	Sehr hoch	Verbindliche Mindestanforderungen an die Cybersicherheit für vernetzte Produkte einschließlich Router. Herkunftsneutral. Befasst sich damit, ob sich ein Gerät sicher verhält; es geht nicht darum, ob der Hersteller dazu gezwungen werden kann, das Verhalten des Geräts zu ändern.
NIS2-Richtlinie	Mittel	Verpflichtet Telekommunikationsbetreiber, Risiken in der Lieferkette zu managen. Die Verpflichtungen sollten nicht am Netzabschlusspunkt enden und erstrecken sich daher nicht auf die Beschaffungsentscheidung für Netzwerkgeräte.
RED-Delegierter Rechtsakt und Verordnung über das offene Internet	Mittel	Die delegierte RED-Verordnung schreibt vor, dass drahtlose Geräte die Nutzerdaten und den Netzwerkbetrieb schützen müssen; diese Vorschrift gilt ab August 2025. Artikel 3 Absatz 1 der Internet-Verordnung legt das Recht des Nutzers auf freie Wahl der Endgeräte fest. Bietet die rechtliche Grundlage für Transparenzpflichten bei von Internetdienstanbietern bereitgestellten Routern.
SAFE-Verordnung und STEP	Mittel	Beschaffungspräferenzen für in der EU hergestellte kritische Technologien und Investitionsmechanismen für strategische Technologien. Die Ausweitung auf Router für den Massenmarkt erfordert einen spezifischen politischen Beschluss.
5G-Cybersicherheits-Toolbox	Hoch (analog)	Der definitorische Präzedenzfall, bestehend aus der risikobasierten Einstufung von Lieferanten mit hohem Risiko, der Umsetzung durch die Mitgliedstaaten und der Befugnis zur Markteinschränkung. Direkt als Umsetzungsbeispiel anwendbar.

6.1 Warum das Gesetz zur Cyberresilienz allein nicht ausreicht

Der am ehesten zu erwartende institutionelle Einwand gegen die Empfehlungen in diesem Papier lautet, dass die Cyberresilienz-Verordnung (Cyber Resilience Act[44]), die im Dezember 2024 in Kraft trat und ab Dezember 2027 gilt, bereits grundlegende Cybersicherheitsanforderungen für vernetzte Produkte einschließlich Router und Heim-Gateways vorschreibt. Wenn ein Router den Anforderungen des CRA entspricht, so lautet das Argument, warum sind dann weitere Maßnahmen erforderlich?

Dieser Einwand vermischt zwei grundlegend unterschiedliche Risikobereiche. Der CRA befasst sich damit, ob sich ein Gerät im Normalbetrieb sicher verhält. Er schreibt „Secure-by-Design“-Prinzipien, den Umgang mit Schwachstellen, die Dokumentation der Software-Stückliste sowie eine

44 Verordnung (EU) 2024/2847 vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyber Resilience Act).

Konformitätsbewertung vor. Dies sind notwendige und begrüßenswerte Verpflichtungen. Die Lieferketten-Steuerung befasst sich hingegen mit der Frage, ob der Hersteller rechtmäßig von einem ausländischen Staat angewiesen werden kann, das Verhalten des Geräts zu ändern. Sie befasst sich mit dem rechtlichen Rahmen, der den Akteur regelt, der die Firmware des Geräts über dessen gesamte Lebensdauer kontrolliert, und nicht mit dem Standardverhalten des Geräts.

Ein Netzwerkgerät, das von einem Unternehmen hergestellt wird, das dem Nationalen Geheimdienstgesetz der VR China unterliegt, kann alle technischen Anforderungen des CRA vollständig erfüllen und dennoch rechtlich gesehen ein potenzielles Instrument des staatlichen Geheimdienstes der VR China bleiben. Die Konformitätsbewertung nach dem CRA erfolgt anhand des zu einem bestimmten Zeitpunkt beobachtbaren Verhaltens des Geräts. Aufgrund ihrer Konzeption kann sie die rechtliche Möglichkeit zur Zwangsverpflichtung des Akteurs, der den Update-Kanal des Geräts kontrolliert, nicht bewerten. Die CRA ist ein technologieneutrales Instrument zur Produktsicherheit, das bewusst herkunftsunabhängig ist. Die 5G-Cybersicherheits-Toolbox wurde 2020 gerade deshalb verabschiedet, weil die Konformitätsbewertung allein nicht in der Lage war, nicht-technische Risiken zu erfassen. Der Vorschlag für das Cybersicherheitsgesetz 2 vom Januar 2026 spiegelt dieselbe Erkenntnis wider und schafft einen horizontalen Rahmen für die Lieferketten-Steuerung, der über der bestehenden Produktsicherheitsarchitektur steht und diese ergänzt.

Der bestehende EU-Rahmen befasst sich mit der Frage, ob ein Gerät sicher ist. Ein am Vorbild der 5G-Toolbox ausgerichtetes Instrument zur Lieferketten-Steureung ist erforderlich, um zu klären, ob der Hersteller dazu veranlasst werden kann, das Gerät unsicher zu machen.

6.2 Die kumulative Lücke und die politische Dynamik

Die Argumente für eine Lieferketten-Steuerung beruhen nicht allein auf einer rechtlichen Analyse. Die öffentliche Meinung hat sich in die gleiche Richtung wie die Rechtsarchitektur bewegt und ist ihr in mancher Hinsicht sogar vorausgeeilt. Ein Blick auf die bestehende Regulierungsarchitektur offenbart ein einheitliches Muster. Jedes Instrument befasst sich mit wichtigen Aspekten der Gerätesicherheit, des Marktzugangs oder der Netzresilienz. Keines befasst sich jedoch mit der spezifischen Kombination von Faktoren, die Netzwerkgeräte unter der Gerichtsbarkeit der VR China zu einem strategischen Risiko machen können: **dem Zusammenspiel von hoher Marktkonzentration, Fernzugriffsmöglichkeiten und der potenziellen Zwangsverpflichtung von Herstellern gemäß den chinesischen Gesetzen zur nationalen Sicherheit und zum Nachrichtendienst.** Über die formale Regulierungsarchitektur hinaus ist das allgemeine politische Umfeld innerhalb der Europäischen Union zunehmend günstig für Maßnahmen geworden, die darauf abzielen, strategische Abhängigkeiten in kritischen Sektoren zu verringern.

Dieser Wandel spiegelt sich in der Gemeinsamen Mitteilung zur Europäischen Wirtschaftssicherheitsstrategie[45] wider, in der wirtschaftliche Sicherheit, die Widerstandsfähigkeit der Lieferketten und der Schutz kritischer Infrastrukturen als zentrale strategische Prioritäten der Union identifiziert werden. Der Schwerpunkt der Strategie auf Risikominderung, technologischer Widerstandsfähigkeit und dem Schutz sensibler Infrastrukturen liefert eine umfassendere politische Begründung für eine verstärkte Überprüfung von im Ausland hergestellten Netzwerkgeräten in strategisch bedeutenden Kommunikationsumgebungen.

Die politischen Rahmenbedingungen werden durch die öffentliche Meinung weiter verstärkt. Laut einer im März 2026 durchgeführten POLITICO European Pulse-Umfrage unter 6.698 Europäern geben rund 84 % der Befragten an, dass sie US-Technologieunternehmen ihre personenbezogenen Daten nicht anvertrauen, während 93 % dieselbe Ansicht in Bezug auf chinesische Unternehmen vertreten. In Deutschland gehört das Misstrauen zu den höchsten in der Stichprobe[46]. Eine im Mai dieses Jahres veröffentlichte

45 GEMEINSAME MITTEILUNG AN DAS EUROPÄISCHE PARLAMENT, DEN EUROPÄISCHEN RAT UND DEN RAT ZUR „EUROPÄISCHEN STRATEGIE FÜR WIRTSCHAFTLICHE SICHERHEIT“, abrufbar unter https://op.europa. eu/de/publication-detail/-/publication/3948446b-101c-11ee-b12e-01aa75ed71a1

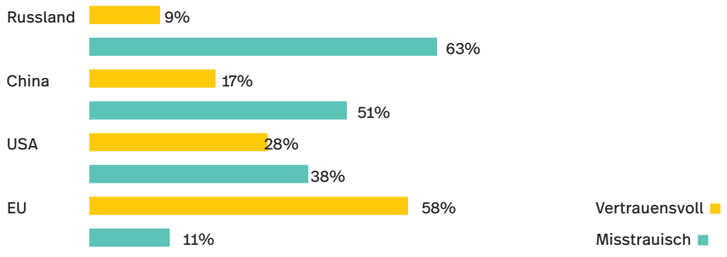
46 POLITICO: 8 von 10 Europäern vertrauen US-amerikanischen und chinesischen Unternehmen nicht, was ihre Daten angeht, abrufbar unter: https://www.politico.eu/article/8-in-10-europeans-dont-trust-us-chinese-frms-with-data

„eupinions"-Studie der Bertelsmann Stiftung[47] kommt zu dem Ergebnis, dass 61 % der Europäer Chinas globalen Einfluss negativ bewerten. Dieselbe Studie berichtet, dass 67 % der Befragten glauben, ihr Land sei wirtschaftlich von China abhängig. Unter denjenigen, die eine solche Abhängigkeit wahrnehmen, befürworten 77 % deren Verringerung, selbst wenn dies mit wirtschaftlichen Kosten verbunden ist. Diese Ergebnisse deuten sowohl auf eine weit verbreitete Besorgnis über Chinas globale Rolle als auch auf eine starke öffentliche Unterstützung für Maßnahmen hin, die darauf abzielen, die strategische und wirtschaftliche Abhängigkeit zu verringern.

Das Misstrauen der Öffentlichkeit gegenüber ausländischen Technologieunternehmen erstreckt sich direkt auf die Geräte, die europäische Heimnetzwerke verwalten. Eine YouGov-Umfrage aus dem Jahr 2025 unter mehr als 16.000 Befragten in den EU-Mitgliedstaaten ergab, dass eine klare Mehrheit speziell gegenüber chinesischen und russischen Router-Herstellern Misstrauen äußerte und diese unter allen vorgestellten Herstellerherkünften als die am wenigsten vertrauenswürdigen Anbieter von Heimnetzwerkausrüstung einstufte.

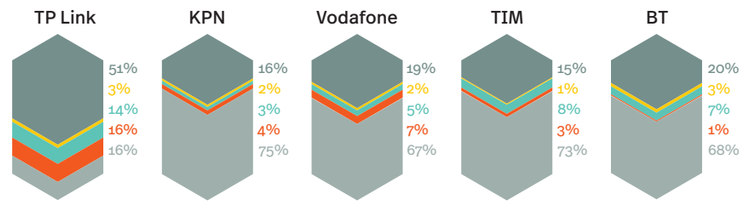
Es überrascht vielleicht nicht, dass die meisten europäischen Verbraucher bei der Frage nach der Herkunft ihres vom Internetdienstanbieter bereitgestellten Routers davon ausgehen, dass das Gerät in ihrem Haushalt aus Europa stammt. Dieselben Bürger, die starke Skepsis gegenüber chinesischer Technologie äußern, sind sich größtenteils nicht bewusst, dass ihr Router möglicherweise von genau den Unternehmen hergestellt wurde, denen sie misstrauen. Sobald diese Wissenslücke durch die in diesem Papier empfohlenen Transparenzmaßnahmen geschlossen ist, wird es sehr schwer, sich der politischen Logik für weitere Maßnahmen zu widersetzen. In dieser Frage ist die öffentliche Meinung dem regulatorischen Rahmen bereits einen Schritt voraus.

Vertrauen und Misstrauen gegenüber Router-Herstellern (gewichtet)

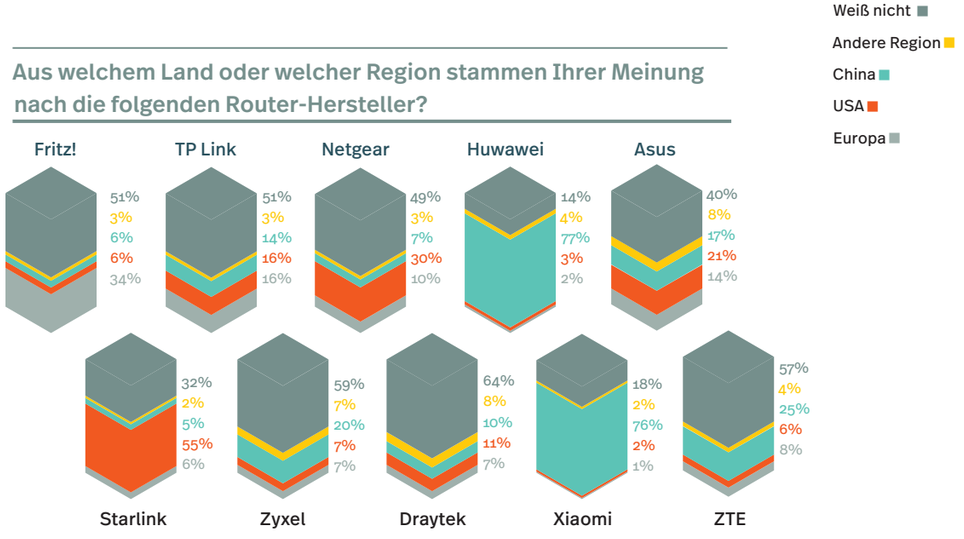


47 Studie „Europas Forderung nach größerer Unabhängigkeit", abrufbar unter: https://bst-europe.eu/europe-in-the-world/europes-call-for-greater-independence

Aus welchem Land oder welcher Region stammen Ihrer Meinung nach die Router der folgenden Internetdienstanbieter?



Aus welchem Land oder welcher Region stammen Ihrer Meinung nach die folgenden Router-Hersteller?



7 EMPFEHLUNGEN

DIE SAFENET-KOALITION präsentiert einen vierteiligen Aktionsrahmen, der die gesamte Bandbreite der Hebel abdeckt, die den europäischen Institutionen und den Regierungen der Mitgliedstaaten zur Verfügung stehen, um die Lücke in der Router-Souveränität zu schließen. Die vier Bereiche **Transparenz, Reform des öffentlichen Beschaffungswesens, Steuerung der Lieferkette und industrielle Kapazitäten** werden – wenn sie gemeinsam und konsequent umgesetzt werden – sicherstellen, dass Netzwerkausrüstung für Privathaushalte und KMU in die Architektur der digitalen Souveränität Europas eingebunden wird und dass die 93 % des europäischen Internetverkehrs, die über Netzwerkgeräte geleitet werden, keine ungelöste Lücke mehr darstellen.

7.1 Transparenz und Sensibilisierung

Europäische Bürger, Unternehmen und Behörden können keine fundierten Entscheidungen über Netzwerkgeräte treffen, die sie nicht identifizieren können, und Regulierungsbehörden können keine Märkte regulieren, die sie nicht überblicken können. Wir empfehlen folgende Maßnahmen:

Verpflichtende Kennzeichnung des Herkunftslandes und der Gerichtsbarkeit für Netzwerkgeräte

Hersteller und Vertreiber von Routern und Netzwerkgeräten für Privathaushalte und KMU sollten verpflichtet werden, klar und in einem standardisierten Format das Herstellungsland der Gerätehardware, das Land, dessen Rechtsordnung für den Firmware-Entwickler gilt, sowie das Land, dessen Rechtsordnung für den Betreiber des Update-Kanals gilt, anzugeben. Diese Kennzeichnung sollte am Verkaufsort, in den Vertragsbedingungen der Internetdienstanbieter und auf der Geräteverpackung erfolgen.

Offenlegungspflichten für Internetdienstanbieter bezüglich der Herkunft von Hardware und Firmware

Internetanbieter, die im Rahmen von Breitbandverträgen Netzwerkgeräte an Privatkunden und KMU liefern, sollten verpflichtet werden, in einer für Verbraucher verständlichen Sprache die Herkunft des Geräteherstellers, die für den Hersteller zuständige Gerichtsbarkeit sowie die Lieferkette der Firmware offenzulegen. Diese Anforderung sollte sich nicht nur auf die physische Hardware beschränken, sondern auch auf die Firmware-

und Betriebssystemebene erstrecken, wo die Herkunft oft selbst für die Internetanbieter undurchsichtig ist.

Verpflichtende Software-Stückliste (SBOM) für die Firmware von Netzwerkgeräten

Hersteller von Netzwerkgeräten, die Geräte auf dem EU-Markt in Verkehr bringen, sollten verpflichtet werden, für die gesamte Firmware eine Software-Stückliste (Software Bill of Materials, SBOM) vorzulegen, die den vollständigen transitiven Abhängigkeitsgraphen abdeckt und nicht nur die Abhängigkeiten auf oberster Ebene, um Risiken in der Lieferkette zu adressieren, die durch die aktuellen Anforderungen in Anhang I, Teil II(1) des Cyber Resilience Act nicht vollständig abgedeckt sind, und diese SBOM neben den Marktüberwachungsbehörden auch Internetdienstanbietern und großen institutionellen Einkäufern zugänglich zu machen. Diese Anforderung ergänzt die Offenlegungspflicht zur Herkunft der Hardware und befasst sich mit der Firmware-Ebene, auf der das Betriebsrisiko einer Fernmanipulation am größten ist.

Initiative zur Sensibilisierung der Verbraucher für die Sicherheit von Routern

Die Kommission und die Kommunikationsbehörden der Mitgliedstaaten sollten eine gezielte Aufklärungskampagne unterstützen, die in Abstimmung mit der ENISA und den nationalen Cybersicherheitsbehörden durchgeführt wird und sich mit den sicherheitsrelevanten Auswirkungen der Herkunft von Heimroutern befasst. Die Kampagne sollte die Kluft zwischen den Bedenken der Verbraucher hinsichtlich chinesischer Technologie und dem Bewusstsein der Verbraucher über die tatsächliche Herkunft der von ihrem Internetdienstanbieter bereitgestellten Geräte thematisieren. Im Zusammenhang mit der DSGVO und der Cybersicherheitshygiene hat sich gezeigt, dass Aufklärungskampagnen zu bedeutenden Veränderungen im Verbraucherverhalten führen können.

7.2 Reform des Beschaffungswesens

Transparenzmaßnahmen schaffen Sichtbarkeit, eine Reform des Beschaffungswesens schafft die wirtschaftlichen Anreize, die für eine Veränderung der Marktstruktur erforderlich sind. Die EU ist der größte Einzelabnehmer von Netzwerkausrüstung auf dem europäischen Markt, wenn man die Beschaffungen in den Bereichen öffentliche Verwaltung, Gesundheitswesen, Bildung und kritische Infrastruktur zusammenfasst, und die Bedingungen, die sie an diese Beschaffung knüpft, beeinflussen direkt die Anreize für die Anbieter.

Kauf von vertrauenswürdigen Bedarfen im öffentlichen Sektor und für Beschaffungen für kritische Infrastrukturen

Behörden, Betreiber regulierter kritischer Infrastrukturen und öffentlich finanzierte Einrichtungen sollten verpflichtet werden, Netzwerkgeräte von Herstellern zu beschaffen, die nicht der rechtlichen Möglichkeit zur Zwangsverpflichtung unterliegen, die im Kontext der 5G-Toolbox als Ausschlusskriterien identifiziert wurden. Bis zur Einrichtung eines formellen Mechanismus zur Einstufung von Lieferanten mit hohem Risiko gemäß der Empfehlung zur Lieferketten-Steuerung unter 7.3 können öffentliche Auftraggeber die Risikokriterien der 5G-Toolbox analog anwenden. Die Anforderung sollte durch das künftige Gesetz über das öffentliche Beschaffungswesen und spezifische NIS2-Umsetzungsleitlinien zu Lieferkettenrisiken bei Netzwerkgeräten umgesetzt werden. Der Grundsatz sollte in erster Linie „Buy Trusted“ lauten, mit einer Präferenz für „Buy European“, sofern vertrauenswürdige europäische Anbieter die funktionalen und wirtschaftlichen Anforderungen erfüllen. Diese Kriterien können für Router verbindliche Wirkung erlangen, sobald das CSA2-Rahmenwerk in Kraft tritt.

Europäische Cybersicherheitszertifizierungsgrundlage für Netzwerkgeräte

Die ENISA sollte in Zusammenarbeit mit der Kommission und den nationalen Cybersicherheitsbehörden ein spezielles europäisches Cybersicherheits-Zertifizierungssystem für Router im Rahmen des europäischen Cybersicherheits-Zertifizierungsrahmens entwickeln, das auf den im Cyber Resilience Act festgelegten Sicherheitsanforderungen aufbaut und die für Funkanlagen gemäß der Funkanlagenrichtlinie geltenden grundlegenden Anforderungen ergänzt, jedoch um Kriterien zur Herkunft in der Lieferkette und zur Einstufung von Lieferanten mit hohem Risiko erweitert wird.

Strukturierte Anreize für den Austausch von risikoreicher Hardware in vorrangigen Bereichen

Strukturierte finanzielle Anreize, analog zu denen, die zur Erleichterung des Ausbaus von Huawei-Geräten aus 5G-Netzen eingesetzt wurden, sollten bereitgestellt werden, um den Austausch von Netzwerkgeräten mit hohem Risiko in vorrangigen Sektoren wie der öffentlichen Verwaltung, dem Gesundheitswesen, dem Bildungswesen und bei Betreibern kritischer Infrastrukturen zu unterstützen. Das Instrument kann über den STEP-Mechanismus, über nationale Wiederaufbau- und Resilienzpläne oder durch gezielte Zuweisungen aus der Fazilität „Connecting Europe“ bereitgestellt werden.

7.3 Steuerung der Lieferkette

Transparenz und Beschaffung sind notwendig, aber nicht ausreichend. Ein Rahmenwerk für die Steuerung der Lieferkette, vergleichbar mit dem, das die EU zwischen 2019 und 2020 für 5G geschaffen hat, ist das geeignete Instrument, um die zugrunde liegende Möglichkeit zur Zwangsverpflichtung von Herstellern, die strukturelle Konzentration des Router-Marktes und das Problem der grenzüberschreitenden Koordinierung zwischen den Mitgliedstaaten anzugehen, das entsteht, wenn jedes nationale Beschaffungsumfeld Entscheidungen isoliert trifft.

Einbeziehung von Heim- und KMU-Netzwerkausrüstung in die Gesetzgebungsdebatte zum Cybersecurity Act 2

Während das Cybersicherheitsgesetz 2 den Gesetzgebungsprozess durchläuft, sollten das Parlament und der Rat Möglichkeiten prüfen, wie Risiken in der Lieferkette für Router angegangen werden können. Das CPE-Segment wirft Fragen zur Möglichkeit zur Zwangsverpflichtung auf, die denselben Charakter haben wie jene, für deren Lösung die 5G-Toolbox konzipiert wurde, und die sich abzeichnende Architektur des CSA2-Rahmens bietet ein naheliegendes Instrument, mit dem diese Fragen untersucht werden können. Der Gesetzgebungsprozess bietet die Gelegenheit sicherzustellen, dass die Lieferkettenaspekte von Netzwerkausrüstung für Privathaushalte und KMU nicht standardmäßig außerhalb des Geltungsbereichs des horizontalen ITK-Sicherheitsrahmens der EU bleiben.

Eine Empfehlung der Kommission zur Risikobewertung der Lieferkette von Routern

Die Kommission kann gemäß Artikel 292 AEUV eine Empfehlung aussprechen, in der sie die Mitgliedstaaten anweist, die Risikobewertungslogik der 5G-Toolbox auf die Lieferketten von Routern anzuwenden, ohne den Abschluss des Gesetzgebungsverfahrens abzuwarten. Parallel dazu kann die ENISA im Rahmen ihres jährlichen Arbeitsprogramms gemäß dem Cybersicherheitsgesetz beauftragt werden, eine spezielle Bedrohungslageanalyse für Risiken in der Lieferkette von Netzwerkgeräten zu erstellen und damit die analytische Grundlage für Maßnahmen der Kooperationsgruppe nach deren eigenem Zeitplan zu schaffen.

Eine „Router Security Toolbox“

Die EU sollte eine „Router-Sicherheits-Toolbox“ entwickeln, die sich ausdrücklich an der 5G-Cybersicherheits-Toolbox orientiert. Die Toolbox sollte eine gemeinsame Risikobewertungsmethodik für die Lieferketten von Netzwerkgeräten, einen Mechanismus zur Einstufung von Lieferanten mit hohem Risiko und zum Ausschluss ihrer Produkte aus sicherheitskritischen Einsatzbereichen sowie einen koordinierten Umsetzungsprozess in den Mitgliedstaaten festlegen. Das CSA2-Rahmenwerk bietet nach seiner Verabschiedung die rechtliche Grundlage, auf der die Maßnahmen der Toolbox als verbindliche Durchführungsrechtsakte gemäß den Artikeln 101 bis 104 umgesetzt werden können. Im Gegensatz zur 5G-Toolbox, die in erster Linie für professionelle Netzbetreiber galt, muss die Router-Sicherheits-Toolbox die massenmarktbezogene, verbraucherorientierte Dimension des Router-Marktes berücksichtigen.

Mechanismus zur Einstufung von Lieferanten mit hohem Risiko

Aufbauend auf der CSA2-Anerkennung und der Router-Sicherheits-Toolbox sollte die EU einen Mechanismus zur Einstufung von Lieferanten mit hohem Risiko für die Router-Lieferkette einrichten. Der Mechanismus sollte den risikobasierten Ansatz zur Lieferantenbewertung der 5G-Toolbox auf den Kontext der Netzwerkgeräte anwenden und damit eine Rechtsgrundlage für differenzierte Zertifizierungs- und Beschaffungsanforderungen schaffen, die die Gerichtsbarkeit des Herstellers berücksichtigen.

7.4 Transformation der industriellen Kapazitäten

Regulatorische Maßnahmen auf der Nachfrageseite müssen mit Investitionen auf der Angebotsseite und mit dem Ausbau der Marktsegmente einhergehen, in denen europäische Hersteller bereits erfolgreich im Wettbewerb stehen. Das Ziel ist nicht die europäische Autarkie bei Netzwerkgeräten, sondern die Gewährleistung, dass vertrauenswürdige europäische und verbündete Hersteller auf einem Markt, der derzeit durch asymmetrische staatliche Unterstützung geprägt ist, effektiv konkurrieren können.

Kurzfristig: Nachfragebelebung durch Harmonisierung der Routerfreiheit

Der am schnellsten verfügbare Hebel auf der Angebotsseite erfordert keine neuen Ausgaben. Eine Harmonisierung der Routerfreiheit in allen Mitgliedstaaten nach dem Standard, der durch die deutsche „Freie Routerwahl" und die italienischen Bestimmungen von 2018 festgelegt wurde, würde die Marktsegmente erweitern, in denen europäische Hersteller bei der Verbraucherpräferenz bereits besser abschneiden als chinesische Wettbewerber. Dort, wo die Kaufentscheidung beim Verbraucher liegt, behaupten sich europäische Hersteller. Die Beschleunigung der vollständigen Umsetzung von Artikel 3 Absatz 1 der Verordnung 2015/2120 in den noch hinterherhinkenden Mitgliedstaaten ist daher sowohl die kostengünstigste als auch die am schnellsten wirksame verfügbare Maßnahme auf der Angebotsseite.

EU-Investitionen in die Produktionskapazitäten für europäische Router

Regulatorische Maßnahmen auf der Nachfrageseite müssen von Investitionen auf der Angebotsseite begleitet werden, um sicherzustellen, dass vertrauenswürdige europäische Alternativen die Marktnachfrage decken können. Die Kommission und die Mitgliedstaaten sollten eine Industriestrategie für die europäische Router-Fertigung entwickeln, einschließlich gezielter Unterstützung durch die Mechanismen von InvestEU, den Wichtigen Vorhaben von gemeinsamem europäischem Interesse (Important Projects of Common European Interest, IPCEI) und Rahmenwerken für öffentlich-private Partnerschaften. Europäische Hersteller wie FRITZ!, Sagemcom, Vantiva und Lancom zeigen, dass bereits eine wettbewerbsfähige industrielle Basis existiert, die es zu verteidigen gilt. Das Ziel ist nicht die europäische Autarkie bei Netzwerkgeräten, sondern die Gewährleistung, dass vertrauenswürdige europäische und verbündete Hersteller auf einem Markt, der derzeit durch asymmetrische staatliche Unterstützung geprägt ist, effektiv konkurrieren können.

Ein Vier-Säulen-Rahmen zur Sicherung der Netzwerkausrüstung für Privathaushalte und KMU in Europa

Transparenz
Fundierte Entscheidungen

Kennzeichnung von Herkunft und Rechtsordnung
Verpflichtung zur Offenlegung der Herkunft der Hardware, der für die Firmware-Entwickler zuständigen Rechtsordnung sowie des Betreibers des Update-Kanals am Verkaufsort in den Verträgen der Internetanbieter und auf der Verpackung.
Mittel – CRA / Verträge der Internetanbieter / Verpackung

Offenlegung der ISP-Herkunft
Verpflichtung der Internetanbieter, die Herkunft des Herstellers, die zuständige Rechtsordnung und die Firmware-Lieferkette in verständlicher Sprache offenzulegen.
Mittel – Breitbandverträge

Anforderung an die Firmware-SBOM
Verpflichtung zur vollständig transitiven Software-Stückliste (SBOM) für die gesamte Firmware, die Lieferrisiken über die Anforderungen von CRA Anhang I, Teil II hinaus abdeckt.
Mittel – CRA Anhang I, Teil II (erweitert)

Aufklärungskampagne für Verbraucher
Eine öffentliche Aufklärungskampagne zu Router-Sicherheit und -Herkunft durchführen, koordiniert mit der ENISA und den nationalen Behörden.
Mittel – ENISA / nationale Programme

Reform des Beschaffungswesens
Umverteilung der Marktmacht

Anforderungen an vertrauenswürdige Beschaffung
Behörden und Betreiber kritischer Infrastrukturen müssen Netzwerkgeräte von Herstellern beschaffen, die keinen rechtlichen Zwangsmaßnahmen unterliegen (analog zu den Kriterien der 5G-Toolbox).
Mittel – Gesetz über das öffentliche Beschaffungswesen / NIS2-Leitlinien

Grundsatz – Zuverlässige Produkte zuerst beschaffen; nach Möglichkeit europäische Produkte beschaffen

EU-Zertifizierung für Cybersicherheit
Die ENISA soll innerhalb des EU-Zertifizierungsrahmens für Cybersicherheit ein spezielles europäisches Zertifizierungssystem für Router entwickeln, das auf der CRA aufbaut und die Funkgeräterichtlinie ergänzt.
Mittel – EUCCF-Referenzrahmen

Anreize zum Austausch
Strukturierte finanzielle Anreize für den Austausch von Hochrisikogeräten in vorrangigen Sektoren: öffentliche Verwaltung, Gesundheitswesen, Bildungswesen und kritische Infrastruktur.
Mittel – STEP/RRP / Fazilität „Connecting Europe"

Steuerung der Lieferkette
Langlebige Regeln schaffen

Netzwerkgeräte für Privathaushalte und KMU in die CSA2-Gesetzgebungsdebatte einbeziehen
Sicherstellen, dass Netzwerkgeräte für Privathaushalte und KMU in die Debatte um den Rechtsakt zur Cybersecurity 2 und den entstehenden Rahmen für die ITK-Sicherheit einbezogen werden.
Mittel – CSA2-Gesetzgebungsprozess

Empfehlung der Kommission zur Risikobewertung der Lieferkette für Router
Anwendung der Logik zur Risikobewertung der 5G-Lieferkette auf Router durch eine Empfehlung der Kommission, während das Gesetzgebungsverfahren voranschreitet.
Mittel – Artikel 292 TFEU

Router-Sicherheits-Toolkit
Entwicklung eines dedizierten Router-Sicherheits-Toolkits mit einer einheitlichen Risikobewertungsmethodik, Lieferantenbewertung und koordinierter Umsetzung.
Mittel – CSA2 Artikel 101–104

Mechanismus zur Einstufung von Hochrisiko-Lieferanten
Einrichtung eines EU-Mechanismus zur Einstufung von Hochrisiko-Lieferanten von Routern auf der Grundlage von Risikofaktoren in der Lieferkette, die mit der jeweiligen Rechtsordnung zusammenhängen.
Mittel – Router-Sicherheits-Toolbox / CSA2

Industrielle Kapazität
Vertrauenswürdige Bezugsquellen ermöglichen

Harmonisierung der Router-Freiheit
Beschleunigung der vollständigen Umsetzung von Art. 19 Abs. 7 der EU-Verordnung 2015/2120 in den Mitgliedstaaten, die hierbei im Rückstand sind, um Endnutzern die Wahl ihres Routers zu ermöglichen.
Mittel – Verordnung 2015/2120

Investitionen in die Fertigung innerhalb der EU
Umsetzung einer Industriestrategie zur Förderung der europäischen Fertigung von Teilnehmerendgeräten über InvestEU- und IPCEI-Mechanismen.
Mittel – InvestEU / IPCEI

Die vier Säulen verstärken sich gegenseitig. Transparenz ermöglicht Beschaffung; Beschaffung schafft Nachfrage nach Steuerung der Lieferkette; Steuerung macht Industrieinvestitionen tragfähig.

8
FAZIT – VOM BEWUSSTSEIN ZUM HANDELN

EUROPA MUSS JETZT HANDELN. Sicherheitsrisiken, technische Souveränität und die wirtschaftlichen Gründe für die Unterstützung der europäischen Technologieindustrie erfordern sofortiges Handeln. Europa hat die institutionellen Rahmenbedingungen, die Rechtsinstrumente, die Koordinierungsmechanismen und – mit der 5G-Toolbox – das bewährte operative Handbuch geschaffen. Die analytische These, dass Router für Privathaushalte und KMU eine kritische Infrastrukturlücke in der Architektur der digitalen Souveränität Europas darstellen, wird von niemandem bestritten, der die Beweise, die Marktdaten, die Dokumentation der Bedrohungen, die rechtlichen Risiken und die eklatante Inkonsistenz mit bereits in anderen Sektoren ergriffenen Maßnahmen prüft.

Nun ist politischer Wille gefragt, der sich auf die spezifische Frage der Router-Sicherheit konzentriert. Diese Frage wurde in aufeinanderfolgenden Arbeitsprogrammen der Kommission, in Debatten zur Umsetzung von NIS2 und in den Verhandlungen zur Cyberresilience-Verordnung von größeren, sichtbareren und in mancher Hinsicht weniger leicht zu bewältigenden Herausforderungen der digitalen Souveränität verdrängt. Auch wenn KI-Steuerung und Cloud-Abhängigkeit zu Recht große Aufmerksamkeit auf sich ziehen, darf nicht zugelassen werden, dass die kritischen Komponenten der zugrunde liegenden Netzwerkinfrastruktur, durch die der gesamte digitale Wert fließt, weiterhin nur eine untergeordnete Rolle spielen. Router befinden sich buchstäblich am Zugangspunkt zu jedem europäischen Haushalt und jedem europäischen Unternehmen. Sie sind das Hardware-Gateway, über das auf die gesamte Architektur der digitalen Souveränität zugegriffen wird, und die einzige Ebene dieser Architektur, die derzeit von keinem koordinierten europäischen Rahmenwerk abgedeckt wird.

Die Kosten der Untätigkeit sind extrem hoch. Jedes Jahr, das ohne einen Sicherheitsrahmen für Router verstreicht, ist ein Jahr, in dem chinesische Hersteller ihre Marktposition festigen, in dem Beschaffungsentscheidungen von Internetdienstanbietern risikoreiche Hardware für ein weiteres Jahrzehnt der Nutzungsdauer festschreiben und in dem die durch die Abschottung des US-Marktes getriebene Konzentrationsdynamik die Gefährdung Europas verstärkt. Das Zeitfenster für kosteneffiziente,

präventive Maßnahmen – das Zeitfenster, das 2019 für 5G bestand – ist jetzt offen. Es wird nicht auf unbestimmte Zeit offen bleiben.

Europa verfügt über die Instrumente, den Präzedenzfall und das politische Momentum. Die Frage ist, ob es handeln wird, bevor die Abhängigkeit unumkehrbar wird.

Die SAFENet-Koalition fordert die EU-Institutionen und die Regierungen der Mitgliedstaaten auf, Router in Privathaushalten und KMU als den kritischen Punkt in der Lieferkette digitaler Dienste zu behandeln, der sie sind, dieselbe kohärente Logik von Sicherheit und Souveränität anzuwenden, die bereits überall sonst angewendet wurde, und zu handeln, bevor sich das Zeitfenster schließt. Die in der SAFENet-Koalition vertretenen europäischen Hersteller, Cybersicherheitsorganisationen und Verfechter digitaler Rechte verfolgen ein gemeinsames Ziel: Ein Europa, in dem die grundlegende Infrastruktur des digitalen Lebens mit der Ernsthaftigkeit und Weitsicht geregelt wird, die ihre Rolle erfordert.

9
ÜBER DIESES PAPIER

9.1 Über die SAFENet-Koalition

Die „Sovereignty Alliance for European Network Technology“ (SAFENet) ist ein strategisches Bündnis führender europäischer Netzwerktechnologieunternehmen. SAFENet versteht Netzwerktechnologie als das Rückgrat des digitalen Ökosystems. Das Bündnis vertritt die Interessen europäischer Hersteller in politischen und regulatorischen Prozessen und trägt damit zur digitalen Souveränität und zur langfristigen Sicherheit der eigenen digitalen Infrastruktur Europas bei. Sein Ziel ist ein digitales Europa, das selbstbestimmt, widerstandsfähig und zukunftssicher ist.

9.2 Über die Innovate Europe Foundation (IE.F)

Die IE.F ist ein unabhängiger Thinktank, der von einem Kreis führender Persönlichkeiten aus der europäischen Tech-Welt getragen wird, die sich zusammengeschlossen haben, um für den Platz Europas in der Weltwirtschaft einzutreten. Als in Berlin ansässiger Forumveranstalter und Dialogpartner fördert sie die Interessen der europäischen Digital- und Tech-Wirtschaft.

9.3 Über iconomy

iconomy ist ein in Berlin ansässiges Beratungsunternehmen und Startup-Förderer, das an der Schnittstelle zwischen europäischer Industriepolitik und digitaler Regulierung tätig ist. Tief eingebettet in das europäische Startup- und Scaleup-Ökosystem und an der Schnittstelle zwischen Venture Building und digitaler Regulierung, berät iconomy Kunden und unterstützt Gründer in kritischen Phasen auf den strategisch wichtigsten Technologiemärkten Europas.

9.4 Urheberrecht und Zitierweise

 Dieses Papier kann zitiert werden als: IE.F und SAFENet-Koalition, „Who Controls Europe’s Internet? | Home Routers, Supply Chain Risk and the Case for European Action“ (IE.F, Mai 2026).

Herausgeber

Innovate Europe Foundation (IE.F)
Schonhauser Allee 43a
10435 Berlin
www.ie.foundation

Autoren

Clark Parsons
IE.F

Gustav Robrahn
iconomy

Kira Terstappen-Richter
SAFENet

Kontakt

Clark Parsons
Innovate Europe Foundation (IE.F)
c.parsons@ie.foundation

Veröffentlichung
Juni 2026