Auflösungs-erscheinungen

Die digitale Transformation erzwingt das Zusammendenken von Wirtschafts-, Sicherheits- und Wertefragen. Deutsche und europäische Außenpolitik müssen lernen, damit umzugehen.

Von Kaan Sahin

Wer über „digitale Souveränität“ spricht, kommt kaum ohne den Verweis auf die Auswirkungen der digitalen Transformation auf die politische, wirtschaftliche und militärische Wettbewerbsfähigkeit von Staaten aus. Innovationen in Sachen Künstliche Intelligenz, Cloud Computing, 5G oder Halbleiter eröffnen Regierungen und Unternehmen enorme Gestaltungsmöglichkeiten.

Der Spagat zwischen Sicherheit und „Bequemlichkeit“ ist jedoch schon bei der Wahrung „individueller Souveränität“ schwierig. Sei es die Nutzung des Kurznachrichtendiensts WhatsApp oder die für viele lästigen Website-Pop-ups, die der EU-Datenschutzgrundverordnung genüge tun sollen, die richtige Balance definiert jeder anders. Auf die politische Ebene übertragen, bestehen auf dem Weg zu „digitaler Souveränität“ viele solcher Zielkonflikte: Innovationskraft und schnelle Marktreife hier, Cybersicherheit und Datenschutz dort. Für Europa und Deutschland, die gegenüber den Tech-Mächten USA und China im Aufholmodus sind, ist es entscheidend, diese Gratwanderung erfolgreich zu absolvieren, gerade mit Blick auf das Selbstverständnis als sichere und „human-centered“ Alternative im digitalen Raum. Dabei lassen sich Fragen der Wirtschaftspolitik, der Sicherheit und der eigenen Werte nicht mehr voneinander trennen.

5G als Weckruf

Diese neue Verwobenheit wirtschaftlicher und sicherheitspolitischer Interessen zeigte sich vor allem in der Debatte um 5G und Huawei. Zunächst

Bild nur in Printausgabe verfügbar

in Berlin als rein technische Angelegenheit abgetan, wurde die Komplexität der Entscheidung, ob der staatsnahe chinesische Telekommunikationsriese Huawei zentrale 5G-Komponeneten für das deutsche Infrastrukturnetz liefern darf, in der Folge immer größer.

Telekommunikationsbetreiber wie die Deutsche Telekom oder Vodafone und auch Stimmen aus dem Bundeswirtschaftsministerium beschworen ein Worst-Case-Szenario herauf: Ohne Huawei werde der 5G-Ausbau um Jahre zurückgeworfen, Deutschland verlöre den Anschluss bei Industrie 4.0-Innovationen oder dem autonomen Fahren. Die Opposition, wichtige Stimmen aus den Regierungsparteien selbst und auch das Auswärtige Amt machten dagegen Sicherheitsbedenken geltend und verwiesen unter anderem auf das enge Verhältnis zwischen der Kommunistischen Partei Chinas und Huawei sowie auf die Rechtslage in der Volksrepublik, die die Zusammenarbeit zwischen „privaten" Unternehmen und den Geheimdiensten vorschreibt.

Das 2021 schließlich auf den Weg gebrachte IT-Sicherheitsgesetz 2.0 sieht nun neben einer technischen Überprüfung von IT-Komponenten auch eine sicherheitspolitische Bewertung der Hersteller und ihrer Vertrauenswürdigkeit vor. Das anfängliche Primat der technischen Verfügbarkeit und des kurzfristigen wirtschaftlichen Nutzens wurde um die notwendige sicherheitspolitische Komponente ergänzt.

Wie Infrastruktur schützen, ohne an Innovationskraft zu verlieren oder Beziehungen zu anderen Staaten zu beeinträchtigen, lautet die Kernfrage.

Die 5G-Diskussion ist Weckruf und Fingerzeig zugleich für bestehende und kommende komplexe Entscheidungen im digitalen Kontext. Wie können die digitale Infrastruktur und Daten der Bürgerinnen und Bürger sowie staatlicher Stellen geschützt werden, ohne damit wirtschaftliche Wertschöpfung und Innovationskraft einzubüßen? Diese Frage stellt sich für die Bundesregierung wie für die Europäische Union auf praktisch allen Technologiefeldern wie Künstliche Intelligenz und Cloud Computing. Stets schwingen auch Fragen der Ethik und Werte als auch die mögliche Verschlechterung von Beziehungen zu anderen Staaten mit.

Europa in der Zwickmühle

Es wäre zu kurz gegriffen, das Spannungsverhältnis auf die Anschaffung von IT-Komponenten von ausländischen Partnern zu reduzieren. Die EU ist gerade auf der Suche nach einem digitalen Leitbild, das neben dem profitorientierten Silicon-Valley-Ansatz der USA und dem autoritären staatskapitalistischen Modell Chinas Bestand haben soll. Der von der EU bereits in Dokumenten und Reden skizzierte, aber noch nicht definierte „menschenzentrierte dritte Weg" soll Europas Markenkern werden. Angesichts dieser selbstgewählten Marschroute brachte die

Kaan Sahin
war bis Ende 2021 Technology Fellow und Strategischer Berater für Cyber-Diplomatie für die deutsche EU-Ratspräsidentschaft im Auswärtigen Amt.

Europäische Kommission verschiedene Initiativen und Gesetzesvorschläge auf den Weg, unter anderem einen zur Verordnung über ein europäisches Konzept für KI. Auch hier warnen Wirtschaftsvertreter, die vorgebrachten Regulierungsansätze würden mögliche KI-Innovationen behindern und der Aufbau von Datenpools, die für das Trainieren von KI-Algorithmen wichtig sind, wäre eingeschränkt. Dagegen kritisieren NGOs mit Fokus auf digitale Menschenrechte den Entwurf: Zu niedrig seien die gesetzlichen Schranken für den Schutz der Bürger und ihrer Daten beispielsweise bei KI-Überwachung. Gerade dieses Beispiel zeigt, wie schwierig die richtige Balance aus potenzieller Wirtschaftlichkeit und sicheren Daten ist, von einem EU-Markenzeichen ganz zu schweigen.

Auch bei der Exportkontrolle verkomplizieren aufkommende Technologien die Abwägungsentscheidungen. So können Fortschritte bei Bilderkennungsalgorithmen, die für kommerzielle Zwecke genutzt werden können, auch für die Massenüberwachung oder die Identifizierung von Objekten auf einem Schlachtfeld verwendet werden. Ähnliches gilt für Quantencomputer, deren Einsatz für Industriezweige wie die Chemie-, Pharma-, Automobil- und Finanzbranche wichtig sein wird, die aber auch sicherheitspolitisch unter anderem mit Blick auf Verschlüsselungssysteme von hoher Relevanz sind.

Die potenzielle Nutzung technologischer Innovationen sowohl für zivile als auch für militärische Zwecke ist zwar schon seit Jahrzehnten ein Element der Exportkontrolle, doch benötigen heute viele technologische Hilfsmittel wie KI-Systeme keine großen industriellen Vorbedingungen mehr und lassen sich viel leichter verbreiten. Im Gegensatz beispielsweise zur Raketentechnologie während des Kalten Krieges, die durch ihre enormen logistischen Anforderungen und eine langwierige Herstellungsphase gekennzeichnet waren, lassen sich viele Innovationen heute nicht mehr so einfach mit den Werkzeugen der Exportkontrolle begutachten.

KI-Systeme lassen sich heute viel leichter verbreiten als beispielsweise Raketentechnik während des Kalten Krieges

Wie reagieren?

Entscheidend ist nun, wie politisch Verantwortliche mit der Komplexität und Verwobenheit von wirtschaftlichen, sicherheitspolitischen und wertebasierten Aspekten rund um die digitale Souveränität umgehen werden. Die notwendigen Abwägungen lassen sich nicht länger verschieben oder auslagern. Und isoliert betrachtet, wird wirtschaftlich oder sicherheitspolitisch immer ein bestimmtes Unbehagen mitschwingen. Im Prinzip sind solche Entscheidungen in einer Art Matrix zu betrachten, in der Ergebnisse oft nicht optimal sein können.

Eine theoretische Alternative bestünde darin, sich technologisch und digital abzuschotten und jegliche Innovationen selbst herzustellen. Dazu ist Europa jedoch nicht imstande – die USA und China sind es aber auch nicht. Auch würden die weltweite Vernetzung und die globalen Wertschöpfungsketten dem entgegenstehen. Digitale und technologische Abkopplungsprozesse würden eine Abkehr von einem globalen Innovationssystem bedeuten.

Doch auch bei dem Setzen eigener Regeln wird sich das Spannungsverhältnis zwischen Wirtschafts- und Sicherheitsinteressen nicht auflösen. Die ideale Mischung wird in einer Art „Trial and Error"-Prinzip immer wieder zwischen Politik, Wirtschaft und Zivilgesellschaft ausgehandelt und gegebenenfalls nachjustiert werden müssen. Jedoch besteht die Gefahr, dass die bürokratischen Mühlen zu langsam mahlen und der Staat, wenn die Regulierungsvorschläge schließlich gereift sind, bereits vor vollendeten Tatsachen steht, weil die rasanten Innovationen – die noch dazu meist jenseits von Europa stattfinden – diese immer wieder neu schaffen.

Schon aus diesem Grund müssen die technologischen Entscheidungen und Aushandlungsprozesse auch institutionell aufgefangen und bearbeitet werden. Das immer enger werdende Wechselverhältnis von Technologie und Geopolitik wird von der bestehenden Ressortlogik nicht optimal aufgefangen. Wäre ein Digitalministerium in diesem Punkt ein Schritt in die richtige Richtung gewesen? Selbst wenn die neue Bundesregierung ein solches Ministerium ins Leben gerufen hätte, hätten andere Ministerien, nicht zuletzt das Auswärtige Amt, ihre unterschiedlichen Interessen und Blickwinkel einbringen müssen. Denn es ist schlichtweg unmöglich, Themenfelder wie KI oder 5G allein einem Ministerium oder einer Regierungsstelle gänzlich und im Voraus zuzuschreiben. Die aus den Technologiefeldern resultierenden wirtschafts-, sicherheits- und wertepolitischen Implikationen müssen effektiv und sachgerecht von den jeweiligen Ministerien und ihren Fachreferaten bearbeitet werden.

Um die neue Komplexität besser zu begreifen, müssen zunächst die Ministerien selbst mehr Expertise aufbauen. Das gilt insbesondere für den Nexus Wirtschaft-Sicherheit bei digitalen Technologien. Für das Auswärtige Amt würde es bedeuten, diese Aspekte zunächst selbst stärker in der Attaché-Ausbildung zu thematisieren und insgesamt mehr Personal für die Bearbeitung dieser Themen abzustellen. Neben bestehenden Referaten wie dem für Exportkontrolle oder dem Cyber-Koordinierungsstab wäre es denkbar, ein eigenes Referat für den Themenkomplex „Emerging Technologies" (aufkommende Technologien) aufzubauen. Zudem sollten die Auslandsvertretungen stärker genutzt werden, um beispielsweise für die Bewertung der rechtlichen Lage in Herkunftsländern von Zulieferern wichtiger Komponenten Informationen zu liefern.

Und auch das leidige Thema der interministeriellen Koordinierung muss in Angriff genommen werden. Denkbar, wenn auch praktisch nicht so leicht umsetzbar, wäre es, sogenannte Cluster-Teams zu bilden, in denen Referenten aus verschiedenen Ministerien dauerhaft zu diesen Themen zusammenarbeiten.

Ob es um die Beschaffung von im Ausland hergestellten IT-Komponenten geht, um das Setzen von Regeln für Innovationen oder um Exportkontrolle – das Zusammenspiel von Wirtschaft und Sicherheit bei der Digitalisierung und bei neuen Technologien wird nicht nur die neue Bundesregierung inhaltlich und institutionell herausfordern, sondern auch die EU. Das beginnt bereits beim Austarieren der Verhältnisse zwischen Kommission, Europäischem Auswärtigen Dienst und den einzelnen Mitgliedstaaten. Dies ist beim Streben nach digitaler Souveränität, die sich am Ende in eigener Handlungsfähigkeit manifestiert, in unserem digitalen und technologischen Zeitalter aber unabdingbar. IP