Macht der Mitte

Die Europäische Union droht im digitalen Großmächte-Ringen an den Rand gedrängt zu werden. Dabei kann sie mit kluger Vernetzung und regulatorisch aus einer Position der Stärke manches bewegen. Und sie muss es auch.

Von Cathryn Clüver Ashbrook

Auch ohne den Blick in die ferne Zukunft ist klar: Wir haben in den vergangenen zwölf Jahren geopolitisches Neuland betreten. Wir erleben eine Zuspitzung des Wettrennens der Großmächte ohne Hegemonialmacht – die sogenannte G-Zero-Welt. Zugleich ist das multilaterale Institutionengefüge geschwächt, wobei es gerade dafür angelegt wurde, das Konfliktpotenzial zwischen Großmächten einzudämmen. Und der Wettbewerb zwischen den „großen Drei" – China, USA und Russland –verlagert sich: Der neue „Kriegsschauplatz" ist das Netz. Netzarchitektur, Daten- und Informationshoheit, KI und Edge-Technologie – ein neuer Machtpoker entsteht auf rasante Weise, ohne dass internationales Recht oder staatliche Regierungsbehörden kontrollierend mithalten können. Nationalstaatlich gelenkte Hacker-Angriffe wie NotPetya (russischer Geheimdienst) oder WannaCry (nordkoreanischer Geheimdienst) verursachen für staatliche Akteure und Unternehmen weltweit Schäden in mehrfacher Milliardenhöhe, zerstören kritische Infrastruktur und sorgen sogar in besonders betroffenen Gebieten für eine höhere Sterblichkeitsrate.

Machtmanipulation online: Für die Auswirkungen der technologisch-katalysierten Globalisierung sind die klassischen Nachkriegsinstitutionen nicht ausgelegt – nicht die nationalen Ministerien und noch weniger das multilaterale System. So wie sie heutzutage strukturell konzipiert sind, können sie den vielzähligen Herausforderungen auch kaum gerecht werden. Die multipolare Welt muss aus verschiedenen Gründen, nicht zuletzt auch wegen des Rückzugs der USA, ohne wirksamen Multilateralismus auskommen. China schafft sich eigene Institutionen; Russland blockiert, wo es kann, nutzt internationale Organisationen aus und widersetzt sich, wo es geht, internationalem Recht; die USA verlassen den Saal. Und Europa versucht zusammenzuhalten, was über 70 Jahre lang den eigenen Wohlstand und die Sicherheit garantiert hat, und das – wie die drei Szenarien von „Digitales Europa 2030" unterstreichen – im schlimmsten Fall mehr schlecht als recht, wenn sich Europa nicht jetzt schon gut vorbereitet. Diese „digitalen" Großmachtspannungen um Hardware (5G) und Plattformen haben ähnlich wie im Kalten Krieg auch ideologische Untertöne: Sowohl Europa, wie die Szenarien deutlich machen, aber auch der afrikanische Kontinent erleben den Wettlauf zwischen US- und chinesischen Technologiekonzernen hautnah.

Diesen Entwicklungen stehen die transnationalen Herausforderungen gegenüber, die global symmetrische Effekte erzeugen können: Klimawandel, Pandemien, Ressourcenknappheit, Massenmigration. Es sind Probleme der globalen öffentlichen Güter, die eine funktionale internationale Weltordnung im Sinne der Großkonfliktvermeidung lösen können müsste.

Die globalisierte Vernetzung erlaubt es auch anderen Akteuren, internationale Beziehungen auf neue Weise zu beeinflussen. Das Machtmonopol von Staaten im internationalen Gefüge wankt. Akteure, die sich plattformgetriebene Vernetzung zu eigen gemacht haben, fordern Nationalstaaten auf eigene Art heraus: Regierungen, Parteien, staatliche Rundfunkanstalten verlieren an Deutungshoheit, wenn immer mehr Menschen ihre Hauptinformationen von schwer regulierbaren Internetplattformen beziehen.

Unternehmen, Terrorgruppen sowie NGOs können es durch die gezielte Nutzung von Plattformvernetzung, Manipulation, Hacking, Trolling, Datendiebstahl, Cyberattacken, aber auch einfacher Präsenz und immer besser werdender KI-Ana-

Cathryn Clüver Ashbrook
ist Gründungsgeschäftsführerin des Projekts „Future of Diplomacy" an der Harvard Kennedy School in Cambridge, Massachusetts.

lyse schaffen, sich als internationale Akteure zu positionieren, mit denen man rechnen – besser noch, die man im Sinne der nationalen Sicherheit antizipieren muss.

Während die Verantwortung für Analyse und Entwicklung sowohl offensiver als auch defensiver Kapazitäten im cybermilitärischen Raum auf Verteidigungsministerien und die NATO entfällt, haben handels-, industrie-, regulations- und demokratieunterstützende Maßnahmen im digitalen Bereich auch eine außenpolitische Dimension. Um der nichtmilitärischen, digitalpolitischen Herausforderungen staatlicher und nichtstaatlicher Akteure Herr zu werden, braucht es eine engmaschige Koordinierung zwischen Fachministerien und den Partnern in der EU-Kommission, Nötig sind auch der Ausbau eigener Analyse-, Diagnose- und Antizipationskapazitäten, eine eigene digitale Infrastruktur (im Sinne der von der EU angestrebten „digitalen Souveränität") sowie eine Strategie der multilateralen Zusammenarbeit zur Entwicklung eines robusten Normen- und Standardkodexes auf der Basis ethischer Prinzipien und internationalen Rechts. Hier müssen sowohl die Außenministerien der EU-Mitgliedsländer und der Europäische Auswärtige Dienst die Koordinierungsrolle übernehmen: Spätestens seit Nord Stream 2 ist deutlich geworden, wie problematisch die Behandlung geopolitischer Situationen in einem rein wirtschaftlichen Kontext sein können. Sauber trennen lassen sich diese Bereiche heutzutage nicht mehr.

Zunächst die guten Nachrichten: Es hat sich in den letzten Jahren in Brüssel, aber auch in den Mitgliedstaaten, gerade in Paris, Kopenhagen und Berlin, auch institutionell einiges getan. Gegründet wurde ENISA, die zivile europäische Schirminstitution, die technologische Sicherheit mit Industriestrategie verbindet; es gibt cyber-außenpolitische Strategien; es gibt Digital-Botschafter im Silicon Valley (Frankreich, Dänemark) und in Berlin; europäische Think-Tanks überschlagen sich mit Analysen zu jedem Aspekt des digitalen Wettrennens und unterstützen als Konsortium sowohl die EU (EU Cyber Direct) als auch die internationale Finanzarchitektur. Der gesamte Themenkomplex ist von der Kommissionspräsidentin und europäischen Regierungen zur Chefsache erklärt worden. Doch es sind vornehmlich immer noch die Chinesen und die Russen, die bei den Vereinten Nationen die Impulse für international geltende Regeln im erweiterten Cyberraum geben – in ihrem Interesse. Und es gibt, wie es die Szenarien „Digitales Europa 2030" deutlich machen, immer noch zu viele europäische Länder – Griechenland, Italien, die Visegrád-Staaten –, die noch viel zu anfällig sind für internationale Einflussnahme.

Die EU wirkt in den Szenarien A und B außenpolitisch viel zu passiv

Die Szenarien A und B unterstreichen, wie weit die Konsequenzen reichen könnten, wenn Europa seine Pläne für die eigene digitale Souveränität nicht weiterverfolgt (dazu gehören der Ausbau von Edge Computing, die Umsetzung des KI-Weißbuchs und die Erweiterung von Gaia-X). Oder wenn Europa in der Diskussion um die EU-Digitalsteuer geopolitische und ökonomische Entscheidungen nicht genau gegeneinander abwägt, wenn es seine Kompetenz als global einflussreicher Digital-Regulator nicht voll ausschöpft.

Die EU sowie die außen- und handelspolitischen Institutionen ihrer Mitgliedsländer wirken in den Szenarien zu passiv: Im Zeichen der symmetrischen Herausforderungen durch Covid-19 ergeben sich für die europäische wie nationale Außenpolitik neue Möglichkeiten, auch im eigenen Institutionengefüge für Teile des digitalen Portfolios. Erstens in der klassischen Verhandlung und der nationalstaatlichen Kooperation, zweitens in der Möglichkeit, institutionell zu gestalten, drittens durch digital-diplomatische außenpolitische Analyse der demokratischen Erosion entgegenzuwirken.

Digitalbeziehungen neu gestalten

In beinahe keinem anderen politischen Bereich werden die Werteunterschiede zwischen Europa und den USA so deutlich wie in der Digitalpolitik. Die zurückliegenden zehn Jahre waren geprägt von den Auseinandersetzungen um Datensicherheit, Privatsphäre („the right to be forgotten"), von der Gestaltung der europäischen Datenschutz-Grundverordnung (General Data Protection Regulation/GDPR) und deren Auswirkungen auf US-Firmen sowie von den Diskussionen über eine EU-Richtlinie für digitale Dienstleistungen und einer EU-weiten Digitalsteuer. Zudem sehen Teile der politischen Elite in den USA die von der EU angestrebte „digitale Souveränität" – ähnlich wie das ältere Konzept der „strategischen Souveränität" – als amerikafeindlich oder zumindest als wenig hilfreich an, wenn es darum geht, den chinesischen Einfluss auf die Weltwirtschaft und die Geopolitik zurückzudrängen.

So reden Amerikaner und Europäer gerade in kritischen Punkten, wie der Nutzung von Huawei-Hardware beim Ausbau des europäischen 5G-Netzwerks, aneinander vorbei. Oder sie treffen weitreichende Entscheidungen im Alleingang, die dem transatlantischen Partner schaden. Anstatt auf diplomatische Vermittlung und regulären strategischen Austausch zu setzen, verlangt die US-Regierung den Abbau von Huawei-Technologie aus Netzen in ganz Europa (Huawei ist in allen EU-Netzen außer Slowenien verbaut) und erwägt die finanzielle Teilhabe an den „europäischen" Hardware-Riesen Ericsson und Nokia. Im direkten Angriff auf das chinesische Technologie-Imperium scheinen die USA ohne Rücksicht auf Verluste vorzugehen: Ihre Entscheidung, Ende August 2020 die Chip-Pipeline nach China (auch an den 5G-Riesen Huawei) einzustellen, hat Europas Mobilfunkunternehmen, die immer noch oder zumindest zum Teil auf Huawei im 5G-Ausbau setzen, kalt erwischt. Kurzum: Wenn Huawei keine amerikanischen Chips mehr verbauen kann, dann leidet darunter keiner mehr als die europäischen Telekommunikationsriesen. Die Tatsache, dass eine solche Ankündigung auch diplomatisch überraschend kam, zeugt davon, wie wenig zurzeit strategisch notwendiger Dialog zwischen den USA und Europa in der Digitalpolitik stattfindet.

Selbst wenn man das Verhalten der USA in diesen Fragen in den letzten drei Jahren als höchst undiplomatisch bezeichnet, sagt es doch einiges über

die Machtposition und Vorbildfunktion aus, die sich die EU in den vergangenen fünf Jahren erarbeitet hat: Vielen US-Unternehmen hat die europäische Datenschutz-Grundverordnung (GDPR) Zusatzkosten beschert. Dennoch wirkt die Richtlinie nachhaltig, nicht nur in ihrer eigentlichen Funktion, sondern auch als Vorlage. So hat sich beispielsweise der Bundesstaat Kalifornien in seiner eigenen Gesetzgebung zum Schutz der Privatsphäre (California Consumer Privacy Act) an der GDPR orientiert. Der Respekt vor der regulatorischen Macht Europas macht sich auch hier bemerkbar: Zwischen 2014 und 2019 haben amerikanische Technologieriesen ihr Lobbyingbudget verfünffacht.

Aus dieser Position der Stärke heraus kann die Europäische Union nun auch auf eine Neuverhandlung des EU-US-Datenschutzschilds pochen. Insgesamt könnten Spannungen ab- und Vertrauen aufgebaut werden. Dafür müsste es sowohl unter transatlantischen Fachministerien der einzelnen EU-Staaten und mit Teilen der Kommission und Interessengruppen aus der Digitalwirtschaft einen offenen Dialog geben, außerdem einen frühzeitigen transatlantischen Konsultationsprozess – gerade zu Künstlicher Intelligenz, Digitalbesteuerung oder Datenspeicherung.

Ein transatlantischer Digital-Rat müsste in Europa institutionell gut vorbereitet werden: ein besser koordinierter, interministerieller Austausch in den Mitgliedstaaten oder unter Ministerien mit ähnlichem bürokratischem und personellem Design und regem Austausch zur Kompetenzerhöhung in den verschiedenen Bereichen der Digitalpolitik. Hier können auch die europäischen Digital-Diplomaten im Silicon Valley eine entscheidende Rolle spielen. Schon jetzt hat das Team um US-Präsidentschaftskandidat Joe Biden angedeutet, die Digitalkapazität im Außenministerium wieder erhöhen zu wollen. Hier müssen sich die EU, ihre Mitgliedstaaten und die USA auf Augenhöhe begegnen können und institutionell nacharbeiten, um Interessenkonflikte diplomatisch zu lösen.

Multilaterale Diplomatie

Auf der multilateralen Ebene könnten EU-Mitgliedsländer und die EU an sich mehr zur Normen- und Rechtsarchitektur beitragen. Die Vorschläge der ursprünglich deutsch-französischen „Allianz für Multilateralismus“ zu digitalen Themen müssten schnell umgesetzt werden und über Grundsatzerklärungen hinausgehen. Auch hier bedarf es wegen des rapiden technologischen Wandels einer engen Zusammenarbeit mit Technologieunternehmen und einer neuen Generation von Diplomaten, die sowohl den Rechtsrahmen als auch die Technologie an sich verstehen. Die Öffnung der klassischen Außenpolitik für neue Rotationsexpertise und eine Vernetzung zu Think-Tanks, Unternehmen und Nichtregierungsorganisationen wären auch erforderlich.

Digitale Einflussnahme hat, wie die drei Szenarien zeigen, nicht nur nachhaltige Auswirkungen auf unsere Demokratien; sie zwingt uns auch grundsätzlicher, unsere Behördenstrukturen neu zu denken. Künstliche Intelligenz ist jetzt schon in der Konsulararbeit kanadischer Botschaften im Einsatz; in Zukunft wird auch die Meritokratie in Außenministerien infrage gestellt werden, wenn das substanzielle Hintergrundwissen, welches sich sonst aus einer langen Botschafterkarriere ergibt, einem diplomatischen Berufsanfänger per KI zur Verfügung gestellt werden kann.

Das „digitale Zuhören“ und die systematische Auswertung der verwertbaren Informationen aus gezielter digitaler Netzwerkbeobachtung gehören in manchen eu-

Regulatorisch befindet sich die EU in einer Position der Stärke

ropäischen Außenministerien schon heute zum Ausbildungsstoff. Nach dem Arabischen Frühling, der Grünen Revolution im Iran oder auch nach den gescheiterten TTIP-Verhandlungen erhofft man sich aus der engmaschigen Verfolgung einflussreicher Personen und Bewegungen ein Frühwarnsystem für humanitäre Vergehen oder antidemokratische Bewegungen.

Diese Analysekapazität ermöglicht aber auch das Erkennen von Mustern, wie die eigene Bevölkerung von außen beeinflusst werden kann. Immer mehr müssen diese Funktionen von Geheimdiensten, aber auch von Außenministerien übernommen werden, die so zum Beispiel radikale Bewegungen oder antidemokratische Desinformationen abfangen können. Dazu braucht es neue und erhöhte Kapazitäten innerhalb der Ministerien und eine bessere interministerielle Koordination.

In Deutschland könnten solche Funktionen auch in einem lang angedachten nationalen Sicherheitsrat gebündelt werden, um von dort aus wieder an relevante Fachministerien verteilt zu werden, die dann politische Handlungsrahmen entwickeln.

Außenministerien müssen auch selbst Desinformation aktiv entgegenwirken – sowohl auf den digitalen als auch in Person auf den realen Marktplätzen. Aus den EU-Kapazitäten zur Analyse von Desinformation müssen sich für relevante Fachministerien, europäische Parteien, Verbände, Wahlleiter und eine ganze Reihe ziviler Akteure neue Leitlinien entwickeln. Einem nationalen Außenministerium käme hier eine Mittlerfunktion zu. Hier gibt es ebenfalls eine transatlantische Dimension, die Außenministerien zwischen relevanten Ministerien koordinieren könnten, denn Europa und die USA eint, dass sie beide in ähnlicher Weise von Desinformation und digitaler Einflussnahme bedroht sind.

Auch im Aufbau neuer Rekrutierungsmaßnahmen oder im Ausbau der strategischen Kommunikation sollten sich EU-Außenministerien austauschen und Netzwerkeffekte nutzen, um effizient gegen Desinformation vorgehen zu können. Der Ausbau dieser Fähigkeiten in einem Ministerium sollte einhergehen mit verlässlichen und sicheren Technologieoptionen: Hier wird der in Szenario C besprochene, rapide wachsende GovTech-Sektor (z.B. tech4Germany) eine entscheidende Rolle spielen können.

Auch wenn das Risiko besteht, im Großmächte-Ringen um digitale Vorherrschaft ausgebremst zu werden, hat Europa sich einen Aktionsrahmen geschaffen, der eine gute Ausgangsposition ermöglicht. Dieser Rahmen ermöglicht nicht nur Regulierung, sondern auch gut vernetzte, koordinierte außenpolitische Maßnahmen m für mehr politische Gestaltung. Diese Chancen dürfen die EU und die digital führenden Mitgliedstaaten nicht aus den Augen verlieren. Die Konsequenzen sind zu dramatisch. IP