FinanzRESILIENZ stärken –

Technologischen Wandel und geopolitische Spannungen meistern!

VORWORT

Dr. Peter Robejsek
Geschäftsführer Mastercard Deutschland

Simone Wießmeyer
Director Public Policy, Head of DACH Region, Mastercard

Mit dem Whitepaper FinanzRESILIENZ stärken – Technologischen Wandel und geopolitische Spannungen meistern! wollen wir eine Grundlage für eine neue und breiter angelegte Diskussion zum Thema Resilienz im Finanzsektor anstoßen. Für dieses Projekt haben wir Expertinnen und Experten eingeladen, sich über die Herausforderungen für Politik, Wirtschaft und Aufsicht Gedanken zu machen und Maßnahmen aufzuzeigen, um die Resilienz des Finanzsystems in Deutschland und Europa – aber auch im Zusammenspiel mit unseren globalen Partnern – zu stärken.

Die Ihnen hier vorliegende Sammlung von Beiträgen bietet einen kaleidoskopartigen Blick auf Finanzresilienz.

Ob aus einer wissenschaftlichen oder aus einer praktischen Perspektive verfasst, viele Beiträge stützen sich auf eine Grunddefinition von Resilienz, um die eigenen Gedanken aus einer spezifischen Perspektive (Innovationen, Geopolitik, Regulatorik, etc.) zu entwickeln. Doch, wie ein Kaleidoskop, ermöglicht die unterschiedliche Refraktion des Lichts, Muster und Gemeinsamkeiten zu erkennen. Auf diese Weise kommt dieses Whitepaper zu einem eigenen, gemeinsamen Verständnis von Finanzresilienz.

Im Sinne einer Zusammenfassung fällt uns auf, dass sich Resilienz, vor allem Finanzresilienz, durch ein Vorgehen und einen Anspruch auszeichnet, der vor allem maßvoll ist. Dort wo Potenziale nicht bis zum Maximum ausgereizt werden und wo Spielräume bleiben, kann reagiert werden. Analog einem Gelenk, das bis zur Grenze der Artikulation flexibel ist. Wird die Grenze überschritten, ist es leicht verwundbar und es besteht das Risiko von Verletzungen. Die verschiedenen Perspektiven der Autorinnen und Autoren zeigen Wege auf, wie wir unser Finanzsystem maßvoll und damit resilient gestalten können.

Einer dieser Wege ist eine auf den Kriterien der sozialen Marktwirtschaft basierende Regulatorik, die unternehmerische Eigenverantwortung nicht zurückdrängt. Wird das Maß der Regulierung und Intervention jedoch überschritten, droht das Korsett die Innovationskraft und Widerstandsfähigkeit der Wirtschaft zu beeinträchtigen. Innovation findet insbesondere dort statt, wo Unternehmen verlässliche Rahmenbedingungen vorfinden und die Politik einen fairen Wettbewerb für alle Marktakteure fördert.

„In einer Zeit des beispiellosen technologischen Wandels und zunehmender geopolitischer Spannungen steht die globale Finanzstabilität vor neuen und komplexen Herausforderungen. Als internationales Technologieunternehmen im Zahlungsverkehr nimmt Mastercard eine entscheidende Rolle in dieser sich nachhaltig verändernden Lebensrealität ein. Mit rund 7.000 Mitarbeitenden in Europa, leistet Mastercard täglich einen wichtigen Beitrag zur Sicherheit und Resilienz des Finanzsystems."

Dr. Peter Robejsek, Geschäftsführer Mastercard Deutschland

Ebenso ist Resilienz eine Funktion der Größe. Große homogene Markträume, wie der EU-Binnenmarkt es mit dem geeigneten Rahmenwerk darstellen kann, sind ein Beispiel. Aber auch gerade im Umfeld des Zahlungsverkehrs sind gegen immer schärfere Cyberrisiken abgesicherte Netzwerke nur dann wirtschaftlich zu betreiben, wenn sie Skalen einnehmen und internationale Standards und Trends berücksichtigen. Insbesondere im Zusammenspiel mit Regierungen, beispielsweise durch Public-Private-Partnerships, und eingebettet in ein durch ein robustes Aufsichtsregime prosperierendes Ökosystem mit anderen Anbietern und Netzen, entsteht ein gegen externe Schocks resilient aufgestelltes System.

„Cyberangriffe machen nicht vor nationalen Grenzen halt und Technologien wie generative künstliche Intelligenz sind globale Phänomene. Aus diesem Grund lässt sich auch das Thema Finanzresilienz nicht aus einer rein lokalen Perspektive betrachten – für ein widerstandsfähiges Gesamtsystem sind die Zusammenarbeit mit globalen Partnern, internationale Standards zur Vermeidung von Fragmentierung und der grenzüberschreitende Informations- und Datenaustausch von entscheidender Bedeutung."

Simone Wießmeyer, Director Public Policy, Head of DACH Region, Mastercard

Resilienz ist ebenfalls durch gemeinsames Handeln beschrieben. Nur Systeme, in denen integrierte Partner sich auch aufeinander verlassen, sind in der Lage die Schwäche des Einen mit der Stärke des anderen zu kompensieren. Wie die Autorinnen und Autoren andeuten oder explizit machen, befinden wir uns in einer Zeit in der das „sich Besinnen" auf die natürlichen Allianzen, Kooperationen und Partnerschaften wichtiger ist denn je um Resilienz sicherzustellen. Das gilt sowohl im geopolitischen Sinne, als auch für Public-Private-Partnerships und emergente Ökosysteme von Startups.

Wir sind überzeugt, dass der Gedanken- und Ideenaustausch dieses Whitepapers dazu beitragen wird, neue Perspektiven auf das Thema Finanzresilienz zu eröffnen und gemeinsame Strategien und Lösungen zu skizzieren, um so die Finanzresilienz in Deutschland und Europa zu stärken. An dieser Stelle möchten wir uns herzlich bei den Autorinnen und Autoren für Ihre wertvollen Beiträge bedanken.

In diesem Sinne wünschen wir Ihnen eine interessante Lektüre

Dr. Peter Robejsek
Geschäftsführer Mastercard Deutschland

Simone Wießmeyer
Director Public Policy, Head of DACH Region, Mastercard

INHALTSVERZEICHNIS

1. Innovation und Finanzresilienz – ein Widerspruch?

Christoph Bornschein
President Digital Strategy, Business Development & Growth Omnicom Deutschland, sowie Gründer und Chairman von TLGG

In Zeiten der Disruption ist Evolution nur in Kooperation möglich

„This is the beginning of an exciting journey and I'm looking forward to sharing more soon" schrieb Mark Zuckerberg am 18. Juni 2019 in einem Facebook-Post. Die Reise, die er meinte, war die Entwicklung und Etablierung einer Facebook-Währung namens Libra. Ein Konsortium aus 27 Partnern, darunter Paypal, Stripe, Visa und Spotify, sollte das Projekt vorantreiben. Manch einer belächelte die Ambitionen Zuckerbergs, und die folgenden Monate sollten den Zweiflern Recht geben: Paypal stieg schon nach zwei Monaten wieder aus, andere Konsortiumsmitglieder folgten. Das Buhlen um regulatorische Zuneigung brachte dem Projekt auch unter dem neuen Namen „Diem" und mit deutlich eingedampften Ambitionen keinen Erfolg. Anfang 2022 schließlich kaufte die US-Bank Silvergate die Reste des Projekts auf, um auf seinen Trümmern eigene Lösungen zu entwickeln. So weit, so gescheitert.

Die tatsächliche Bedeutung der Facebook-Ankündigung ließ sich 2019 jedoch an den so raschen wie ratlosen Reaktionen der Finanzaufsichten ablesen. Nur Stunden nach der offiziellen Libra-Ankündigung forderte die damalige Vorsitzende des Ausschusses für Finanzdienstleistungen im US-Repräsentantenhaus, Maxine Waters, eine Einstellung der Arbeit an Libra, um den Regulierungsbehörden Zeit für die Analyse des Projekts zu geben. Der damalige Bafin-Chef Felix Hufeld klang auch eine Woche später noch alarmiert: „Ich kann nur hoffen, dass es uns gelingt, mindestens europäisch, wenn nicht global ein paar Grundstandards zu entwickeln." Angesichts der Tatsache, dass der Betreiber einer datenerfassungintensiven Plattform mit damals rund 2,5 Milliarden Nutzern weltweit gerade erklärt hatte, die Übernahme einer der Kernfunktionen des Staatswesens anzustreben, scheint die milde Überforderung, die aus einem solchen Statement spricht, verständlich

Die Leistung liegt in der Problemerkennung

Kaum fünf Jahre später scheint all das ewig her: 2019, das war nicht nur vor Krankheit, Krieg und Krise, sondern auch vor Bitcoin-Rekordhoch, WallStreetBets, NFT-Hype, Wirecard und FTX. Im Finanzsektor war und ist Bewegung, und staatliche Akteure und Regulatoren sind weiterhin milde überfordert – daran kann allen gewonnenen Erkenntnissen und allen Bemühungen um staatliche Antworten und Lösungen zum Trotz kein Zweifel bleiben.

Neue Technologien und ihre Entwickler und Proponenten fordern den Staat heute in zweien seiner Kernfunktionen heraus: der Kontrolle der Währung und der damit eng verbundenen Kontrolle der Identität seiner Bürger. Auf beide Herausforderungen haben Staaten bislang keine valide Antwort gefunden.

Das griffigste Beispiel für die Herausforderung des Staates durch private Akteure ist aktuell WorldCoin, das Kryptowährungs- und ID-Projekt des OpenAI-Mitgründers und -CEOs Sam Altman. WorldCoin verfolgt den Ansatz, seine Nutzer durch Iris-Scans mit einer digitalen ID zu erfassen und ihnen damit Zugriff auf eine handelbare Kryptowährung zu geben. Umgesetzt wird die Iris-Erfassung durch dystopisch anmutende Scan-Interfaces, die aktuell nicht zuletzt in finanzschwachen Gegenden und mit konkreten finanziellen Anreizen für zukünftige Nutzer eingesetzt werden. Es läuft nicht eben umwerfend: Der formelle Launch in den USA ist alles andere als gesichert, im August 2023 untersagte mit Kenia eines der ersten Launch-Länder WorldCoin den Betrieb, die Nutzerbasis wächst eher schleppend. Bislang liegt WorldCoin, was praktischen Nutzen und Ansehen angeht, hinter anderen Alternativwährungen weit zurück, ob nun Bitcoin, Dogecoin oder Chiemgauer. Es wirkt alles in allem undurchdacht und unseriös. Der Reflex, auch hier wieder Ambitionen zu belächeln, ist völlig verständlich.

Wer aber nur lächelt, dem entgeht, was Sam Altman offensichtlich verstanden hat: Spätestens mit den von ihm und OpenAI sowie weltweit immer mehr Organisationen ermöglichten Entwicklungssprüngen künstlicher Intelligenz stellt sich die Frage nach der Identifizierbarkeit echter Menschen im digitalen Raum mit einer neuen Dringlichkeit. Sam Altman ist davon überzeugt, dass der Siegeszug der künstlichen Intelligenz auch zu einem digitalen Vertrauensverlust führt, der wiederum eine neue Form von ID nötig macht. Er schafft und erkennt das Problem und versucht sich an einer Lösung, auch wenn die Umsetzung seiner Erkenntnisse noch an vielen Punkten zu wünschen übriglässt. Ein Unternehmen, das mit offenbar dem Puzzle-Shooter „Portal" entlehnten Irisscannern durch die Straßen von Lagos zieht und Leuten ihre ID-Daten für einen schmalen Taler abkauft, demonstriert ein eher zweifelhaftes Verständnis von Vertrauen.

Tech- und Finance-Hypes sind nur Symptome eines systemischen Wandels

WorldCoins noch mangelhafter Lösungsansatz sollte jedoch kein Grund dafür sein, das von Altman diagnostizierte Problem anzuzweifeln. Der technologische Fortschritt allgemein und künstliche Intelligenz im Besonderen sind dabei, unsere vielfach herausgeforderte Welt noch einmal auf den Kopf zu stellen. Neben den DeepFake- und Desinformationspotenzialen, die bereits in aktuellen KI-Modellen angelegt sind, bringt ihr wirtschaftliches Potenzial auch die gewohnte Macht- und Marktverteilung der Welt ins Schwanken. Längst legen etwa die VAE und Saudi-Arabien die Grundlagen für eine neue, tech-basierte Wirtschaftsrelevanz. Sie schaffen neue Wirtschaftszonen, machen sich attraktiv für etablierte Tech-Player und halten es längst nicht mehr für nötig, ihren Gestaltungs- und Relevanzanspruch herunterzuspielen. Dazu kommt, dass diese Gestaltungsansprüche finanziell bestens unterfüttert sind.
Das bringt uns zurück zu Felix Hufelds Prinzip Hoffnung angesichts des Libra-Launches. Denn ob Libra, WorldCoin, WallStreetBets, Bitcoin, Bitcoin-ETFs, NFTs, ChatGPT, KI, sie werden von den Akteuren noch viel zu oft als isolierte Hypes betrachtet, auf die man entweder reagiert oder halt nicht. Wie sehr sie Symptom einer systemischen Herausforderung sind, die so gut wie alle etablierten Prozesse und Methoden betrifft, wird dabei oft verkannt.

In Kombination mit den längst nicht mehr ausreichenden IT-Beschaffungskompetenzen des Staates und den Legacy-Methoden seiner Partner entstehen aus diesem Problemverständnis immer wieder nur unzureichende Insellösungen, die weder sinnvolle Antworten auf umfassende Herausforderungen noch attraktive Angebote für die Bürger von heute sind. Betrachten wir Deutschland und Europa: Verimi, DeMail, PayDirekt, elektronischer Personalausweis, Gaia-X – alles grundsätzlich nicht völlig verkehrt, aber unzureichend im Design, in der Handhabung, in der Entwicklung, im Einsatz. Selbst Altmans Iris-Orbs wirken attraktiver und problemadäquater.

Zukunft braucht Kooperationen und Bewertungskompetenz

Die Kompetenz, die den bisherigen Gewinnern der Globalisierung heute fehlt, ist es, vorausdenkend gute und ineinandergreifende Lösungen für antizipierte und zusammenhängende Probleme zu schaffen. Staaten, zumal europäische Staaten, sind Verwaltungsstaaten, geschaffen für die überwiegend lineare Fortschreibung gegenwärtiger Zustände. Dies jedoch findet so nicht mehr statt. Die Lösung kann deshalb nur in neuen, informierten, problembewussten Partnerschaften liegen.
Allgemein kann Evolution in einer disruptiven und volatilen Welt nur in Partnerschaften funktionieren, da sich jede Veränderung ins Gesamtsystem auswirkt. „Partnerschaften" wiederum kann nicht heißen, dass staatliche Institutionen nach Dienstleistern suchen, denen sie ihre jeweiligen Probleme und Projekte full-stack überhelfen können. Um es anders zu formulieren und noch einmal Gaia-X zu bemühen: Braucht Europa eine souveräne Cloud? Ja. Sagt das etwas über jede damit verbundene Schnittstelle, jede Anwendungsschicht, jedes damit verbundene Infrastrukturelement? Nein. Souveränität ist nicht Ausschluss: Staaten brauchen strategische Allianzen mit sehr klarem Blick fürs Was, fürs Warum, fürs Mit-Wem. Welche kritische Infrastruktur lassen wir von Huawei bauen und welche nicht? Mit wem entwickeln wir den digitalen Euro und was machen wir eigentlich damit, wenn er fertig ist?

Antworten auf Fragen wie diese entstehen nicht in isolierten 1:1-Kollaborationen, sondern in Partner-Ökosystemen, in denen staatliche und nichtstaatliche Akteure voneinander profitieren und miteinander wachsen. Diese Ökosysteme wiederum setzen eine verbesserte Bewertungs- und Koordinationskompetenz staatlicher Institutionen voraus. Deren Aufgabe muss es zukünftig stärker sein, Herausforderungen zu analysieren, Teilprobleme zu entkoppeln und in Kooperation mit eng vernetzten Lösungsanbietern Teillösungen zu entwickeln – ohne das große Ganze aus den Augen zu verlieren. Teile des Koalitionsvertrages 2021 lassen vermuten, dass die grundsätzlichen Kompetenzen dafür durchaus existieren. Es wäre schön, sie in relevanten Positionen eingesetzt zu sehen.
Das grundsätzliche Problem wurde nun schon so oft, so detailliert, so präzise und stets aktuell und doch so folgenlos beschrieben, dass ich fast das Gefühl habe, mich bei den Lesern und Leserinnen dieses Textes dafür entschuldigen zu müssen, hier auch nur ein Update der Problem- und Lösungsskizze liefern zu können. Lassen Sie mich deshalb mit positiven Worten enden.
Denn was immer sich 2024 im Segment Finanzen, Banken, Payment und ID konkret tun wird: Es wird „the beginning of an exciting journey" sein.

Christian Rau
Senior Vice President Fintech and Crypto Enablement Europe

Die neue Finanzinfrastruktur? Was die Blockchain Technologie für die Resilienz des digitalen Zahlungsverkehrs bedeutet

Beim Stichwort „Finanz-Resilienz stärken" werden wahrscheinlich bei vielen Beobachtern aus Politik, Wirtschaft und Gesellschaft die Worte „Finanzkrise" und „Schuldenkrise" vor dem inneren Auge aufscheinen. Auch wenn seit der Insolvenz von Lehman Brothers im September 2007 und der sogenannten Eurokrise, und deren Höhepunkte im Jahre 2010, einiges an Zeit verstrichen ist: die Erfahrungen hallen weiterhin nach und sind präsent.

Was vor dem Hintergrund der oben genannten Ereignisse gerne in den Hintergrund gerät: auch der digitale Zahlungsverkehr spielt beim Thema Finanz-Resilienz eine entscheidende Rolle.
Mit der zunehmenden Digitalisierung der Gesellschaft und Wirtschaft, die wir täglich an unserem eigenen Verhalten ablesen können, und beschleunigt durch die Covid 19 Pandemie und die damit einhergehenden Lockdowns wird zunehmend klar, dass für eine moderne, resiliente, effiziente und auf Partizipation ausgerichtete Volkswirtschaft das digitale (und damit oft nichtbare) Bezahlen essenziell ist.

Apps akzeptieren typischerweise kein Bargeld, der E-Commerce kennt weniger nationale Grenzen und dafür umso mehr internationale Standards und Konsumenten nutzen zunehmend das Handy zum Bezahlen. So hat beispielsweise die Zentralbank der Niederlande kommuniziert, dass bereits im Jahr 2022 die Nutzung des Handys zum Bezahlen im stationären Einzelhandel die Bargeldzahlungen überholt hat; dem Volumen nach lag das Bargeld bei 15% und die mobilen Zahlungen bei 19% (DNBulletin, 2023).

All diese Innovationen und Herausforderungen werden durch das bestehende System des digitalen Zahlungsverkehrs erfreulich unaufgeregt, effizient, sicher und global skalierend abgebildet bzw. adressiert.

Nie hatten europäische und deutsche KonsumentInnen und Händler mehr Zahloptionen als heute; eine Handvoll Buy-Now-Pay-Later Lösungen, Debit und Kredit Karten im 3- und 4-Parteien System, Wallets, (Echtzeit)überweisungen und natürlich Bargeld und Rechnungskauf bieten Wahlfreiheit und Optionen und tragen damit unmittelbar zur Resilienz und dem Funktionieren der Realwirtschaft bei.

Auch wenn diese Veränderungen noch nicht in gleichem Maße überall angekommen sind und Deutschland sich hier eher im Mittelfeld bewegt: der Zug hat den Bahnhof verlassen und viele der Erneuerungen und Veränderungen werden bleiben und sich eher beschleunigen als revidiert werden.

Teile der Payment-, Finanz- und Technologiewelt schauen währenddessen bereits seit einiger Zeit auf die nächste große Veränderung und der Themenkomplex Tokenization, Blockchain, Digital Assets, Crypto und Centralbank Digital Currencies nimmt in der öffentlichen Debatte zunehmend mehr Raum ein.

Neben dem Aufstieg und Preisverfall verschiedener Kryptowährungen und vielen Irrungen und Wirrungen im Markt hat das Thema CBCD oder Central Bank Digital Currency mittlerweile global Fahrt aufgenommen.

Selbstverständlich liegen Kryptowährungen und CBDCs, durch eine Zentralbank emittiertes digitales Geld als komplementäres Angebot zu Münzen und Scheinen, an komplett unterschiedlichen Enden des Spektrums des digitalen „Geldes", aber man sollte sie trotzdem holistisch betrachten.

Mitte 2023 lag die Anzahl der Länder, die sich aktiv mit dem Thema CBDC beschäftigen bei 130, darunter alle G20 Staaten mit Ausnahme von Argentinien. Mit Indien und Brasilien haben zwei große Wachstumsvolkswirtschaften die Einführung ihrer jeweiligen CBDCs in Aussicht gestellt. Der digitale Euro ist im November 2023 nach zweijähriger Investigativphase in die zweijährige Vorbereitungsphase übergangen (Jones, 2023; Reuters, 2023; Partz, 2023; Deutsche Bundesbank, 2023).

Auch wenn nicht alle CBDCs auf Blockchain Technologie basieren und man zwischen sogenannten Retail und Wholesale CBDCs unterscheiden muss, bleibt festzuhalten: privatwirtschaftliche und Zentralbank Initiativen zur Tokenisierung des Geldes bewegen gemeinsam den Markt.

Diverse Zahlungsdienstleister, Banken und Asset Manager experimentieren mit der Blockchain Technologie.

So hat PayPal im August 2023 einen eigenen, US-Dollar denominierten, Stable Coin eigeführt und die DWS kommunizierte im Dezember 2023 die Intention, einen Euro denominierten Stable Coin einzuführen.

Auch die Europäischen Regulatoren haben erkannt, dass das Thema „Krypto" gekommen ist, um zu bleiben und somit wird mit der sogenannten MiCAR Regulierung mit Ende Juni bzw. Ende des Jahres 2024 eines der umfassendsten und modernsten Regelwerke greifen, um Konsumenten zu schützen und Stable Coins zu regulieren (DeVon, 2023; DWS, 2023).

All diese Initiativen zielen darauf ab die nächste Evolutionsstufe der Finanzinfrastruktur zu etablieren und das Thema Resilienz schwingt häufig mit: höhere Resilienz durch Dezentralisierung und den Wegfall eines „Single Point of Failure", Risikominimierung von Settlement Risiken durch sogenannte Smart Contracts, mehr Freiheit, Selbstbestimmung und geringere Kosten für Konsumenten und mehr Transparenz, Effizienz und geringere Risken bei grenzüberschreitenden B2B Payments, um nur einige zu nennen.

Was bedeutet all dies unter dem Strich für das Thema „Finanz-Resilienz"?

Eine Technologie, die ursprünglich die etablierten Finanzinstitute ersetzen wollte, privates digitales Geld in Form von Stablecoins und die nächste Stufe des, nun digitalen, Zentralbank Geldes erstmals nutzbar für Konsumenten treffen auf ein Marktumfeld, dass ohnehin durch Veränderungen und wichtige Fragen wie Verschuldung und Inflation geprägt ist.

Mastercard ist überzeugt, dass die Blockchain Technologie, richtig eingesetzt und eingebettet in ein entsprechendes regulatorisches Rahmenwerk, zur Wahlfreiheit, technologischen Diversifikation und somit auch zur Resilienz und Innovationskraft der deutschen und europäischen Finanzwelt beitragen kann.

Wir sind überzeugt, dass eine ausgewogene Regulierung in Form von MiCAR den europäischen Standort stärken kann, so wie es die DSGVO im Bereich Datenschutz und die PSD2 für Open Banking und die Kundenauthentifizierung vorgemacht haben.

Als global tätiges Unternehmen im digitalen Zahlungsverkehr nehmen wir unsere Rolle wahr, gemeinsam mit unseren Kunden und Partnern die neuen Möglichkeiten für einfaches, sicheres und bequemes Bezahlen auszuloten ohne essentielle Werte und Konzepte wie Konsumentenschutz, Wertstabilität und das Einhalten von Geldwäschen und Compliance Richtlinien außer Acht zu lassen.

Wie jeder Technologiesprung birgt das Aufkommen von Krypto, Blockchain und CBDCs enorme Chancen, auch für die Resilienz, sofern er richtig umgesetzt wird.

Dr. Sven Herpig
Leiter „Cybersicherheitspolitik und Resilienz", Stiftung Neue Verantwortung e.V.

Sicherheit und Resilienz von Maschinellem Lernen

Schutz Künstlicher Intelligenz: Zwischen Safety und Security

Zwischen Regierungen und auf internationalen Konferenzen wird derzeit viel über die Sicherheit von Künstlicher Intelligenz gesprochen, wie zum Beispiel kürzlich auf dem AI Safety Summit in Bletchley Park (AI Safety Summit, 2023). Der Name dieses Gipfels deutet schon an, was hier und auch anderswo meist gemeint ist: der Safety-Aspekt. Safety bedeutet in diesem Zusammenhang, dass eine Anwendung, die auf maschinellem Lernen basiert (ML-Anwendung), unfallfrei das tut, was sie tun soll. Ein auf dem Parkett der internationalen Politik deutlich seltener beleuchteter Punkt ist jedoch die Sicherheit im Sinne von Security. Security beschreibt die Sicherheit von ML-Anwendungen – Foundation Models und anderen – vor böswilligen Dritten, die Modelle unberechtigt kopieren (und weiternutzen) oder manipulieren wollen. Kriminelle, Nachrichtendienste und andere böswillige Akteure versuchen dies beispielsweise über Data Poisoning, Model und Data Extraction, Backdooring oder Prompt Injection zu erreichen (Herpig, 2020).

Sicherheit allein wird nicht reichen, es braucht Resilienz

Da ML-Anwendungen in Zukunft auch zunehmend in Bereichen eingesetzt werden, die elementar für das Funktionieren der Gesellschaft sind, ist die Absicherung dieser Anwendungen unabdingbar. Ein internationaler Zusammenschluss von Cybersicherheitsbehörden hat Ende 2023 Richtlinien dazu veröffentlicht, wie eine bessere Security bei der Entwicklung von ML-Anwendungen über die gesamte Lieferkette hinweg erreicht werden kann (Herpig, 2020; NCSC & CISA, 2023). Von 2020 bis 2023 beschäftigte sich damit bereits eine internationale Arbeitsgruppe unter Leitung der europäischen Cybersicherheitsbehörde ENISA, die entsprechende Analysen und Handlungsempfehlungen veröffentlichte (ENISA, 2023). Folgt man jedoch der Gefährdungslogik der letzten Jahre, wird eine reine Absicherung von ML-Anwendungen nicht ausreichen. Denn die Frage ist nicht, ob eine ML-Anwendung von Dritten manipuliert wird, sondern nur wann. Beispiele gibt es bereits genug. So wurden zum Beispiel der Chatbot Tay von Microsoft und Tesla's Autopilot bereits 2016 manipuliert (Vincent, 2016; Greenberg, 2016). Blackberry's IT-Sicherheitssoftware Cylance wurde 2019 komplett ausgehebelt und zuletzt wurden Wege gefunden, Sicherheitsbeschränkungen bei Large Language Models, wie etwa bei Open AI's ChatGPT, zu umgehen (Skylight Cyber, 2019; Liu et al., 2023). Zwar haben sich die hier genannten Beispiele nicht in the wild abgespielt, Menschen waren nicht direkt gefährdet; die Manipulation von Teslas Autopilot zum Beispiel fand unter Laborbedingungen statt. Dennoch ist der Weg vorgezeichnet. Böswillige Akteure werden ML-Anwendungen in kritischen Infrastrukturen erfolgreich manipulieren, um ihr Ziel – zum Beispiel Lösegelderpressung oder Disruption – zu erreichen. Es darf daher nicht nur über die Sicherheit von ML-Anwendungen gesprochen werden. Es muss auch über die Resilienz von ML-Anwendungen gesprochen werden.

Wie kann Resilienz bei ML-Anwendungen aussehen

Das Nationale Institut für Normen und Technologie der Vereinigten Staaten, NIST, definiert cyber resilience als: „The ability to anticipate [vorhersagen], withstand [widerstehen], recover [erholen] from, and adapt [anpassen] to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." Zwar wird schon daran gearbeitet, die Cyberresilienz zu erhöhen, aber für ML-Anwendungen gibt es einen Anpassungsbedarf (Herpig, 2023; NIST, 2024).

Um eine Vorhersage zu ermöglichen, müssen die zuständigen Stellen, zum Beispiel Cybersicherheitsbehörden und ML-Entwickler:innen, die aktuelle Gefährdungslage im Auge behalten. Gleichzeitig bedarf es bei jeder ML-Anwendung, das merkt unter anderem auch die Bletchley Declaration an, einer Risikoanalyse und -mitigation. Der verantwortungsvolle Umgang mit gefundenen Schwachstellen in ML-Anwendungen ist ein weiterer Aspekt, der eine gute Vorhersage unterstützt (Nasr et al., 2023).

Dem Aspekt des Widerstands gegen Schadensereignisse kommt bei ML-Anwendungen eine besondere Rolle zu. Denn: ML soll für Geschwindigkeit, Skalierbarkeit und Automatisierung sorgen. Kann dem Schadensereignis bei einer ML-Anwendung nicht widerstanden werden, drohen im schlimmsten Fall sich schnell fortsetzende Kaskadeneffekte (Herpig, 2020). Es bedarf hier daher neben robusten Algorithmen und der Absicherung der gesamten ML-Lieferkette, inklusive Validierung und Verifizierung, weiterer Maßnahmen wie Notausfall-Schalter und adäquater menschlicher Aufsicht (Human-on-the-Loop).

Sich von einem Schadensereignis zu erholen, bedeutet unter anderem herauszufinden, wie es eingetreten ist. Solange der Algorithmus eine Blackbox und die Lieferkette nur in Teilen transparent ist, wird es schwierig. Daher ist eine Erholung vom Schadensereignis nur dann umfangreich möglich, wenn die im Einsatz befindliche ML-Anwendung auf Basis von erklärbaren oder interpretierbaren Ansätzen – explainable and interpretable AI – entwickelt wurde. Auch bereits im Gesamtsystem integrierte forensische Maßnahmen können ihren Teil dazu beitragen, dass sich IT-Infrastrukturen nachhaltig von einem Schadensereignis erholen können.

Die Anpassung von ML-Anwendungen kann je nach zugrunde liegenden Schwachstellen weitaus umfangreicher sein als bei Nicht-ML-Anwendungen. Bei Letzteren hilft oftmals die Veränderung von Konfigurationen und das Einspielen von Patches. Sollte die Schwachstelle aber in der ML-Anwendung liegen, ist ein einfacher Patch, zum Beispiel die Einführung weiterer Guardrails, nicht unbedingt ausreichend. Im schlimmsten Fall muss die Anwendung weitertrainiert oder von einer vorherigen, vor-trainierten Version erneut trainiert werden. Anschließend sollten dann weitere Sicherheitstests zur Validierung durchgeführt werden. Hierbei schließt sich der Kreis zum Anfang. Wenn eine spätere Anpassung aufwändig und komplex ist, sollte bereits bei der Entwicklung von ML-Anwendungen noch mehr Augenmerk auf die Sicherheit gelegt werden.

Die Fehler der Vergangenheit nicht wiederholen

Der Fehler, dass die Verantwortlichen die Absicherung und Resilienz von Software nicht von Anfang an zur Priorität machen, fällt uns jeden Tag aufs Neue auf die Füße. Dafür muss man sich nur die einschlägigen Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik oder des Bundeskriminalamts anschauen (BSI, 2023; BKA 2023). Derzeit gibt es ein Momentum, dass wir diesen Fehler nicht in gleichem Maße bei ML-Anwendungen wiederholen. Diese Chance sollte von Politik und Industrie genutzt werden, um das notwendige Sicherheitsniveau von ML-Anwendungen zu gewährleisten und für Schadensfälle durch entsprechende Resilienz direkt mitzuplanen.

Marcus W. Mosen
Payment & Fintech-Experte,
Aufsichtsratsvorsitzender N26 AG

Mehr Wachstum bei digital Payment und Banking in Europa wagen

Digital, nachhaltig, resilient – das sind die aktuellen Anforderungen an die Lenker in der Wirtschaft. Die Veränderungen reichen jedoch viel weiter und betreffen nicht nur Unternehmen und ihre Kunden, sondern die gesamte Gesellschaft. Der technologische Fortschritt und das Internet haben dazu geführt, dass Individuen, Unternehmen, Politik und Gesellschaft eng miteinander vernetzt sind. Zugleich spielen Daten, Analytik und Technologie eine immer zentralere Rolle in der Entwicklung und der Bereitstellung neuer Produkte. Wer zudem in der Lage ist, Daten über Ökosysteme intelligent miteinander zu verknüpfen und auszutauschen, ist noch besser positioniert, die immer digitaler werdende Gesellschaft mitzugestalten und in ihr zu bestehen. Die Finanzdienstleistungsbranche ist in vielen Bereichen des wirtschaftlichen Handelns auf die Nutzung von Daten und zunehmend auf den Einsatz digitaler Lösungen und modernster Technologien angewiesen.

Finanzdienstleister sichern Risiken ab, stellen Finanzierungsinstrumente zur Verfügung, vermitteln Kapitalanlagen und wickeln Zahlungen ab. Sie stehen damit im Zentrum allen wirtschaftlichen Geschehens. Insbesondere die Branche, die sich mit der Bereitstellung von digitalen Zahlungsdiensten befasst, hat in den letzten beiden Jahrzehnten tiefgreifende Veränderungen durchlaufen. Die sogenannte „Payment-Industry" war in den letzten Jahren besonders stark vom technologischen Wandel – insbesondere durch die verstärkte Nutzung der Internettechnologie – geprägt. Die Erfahrungen in der Corona-Pandemie haben das bargeldlose, digitale Bezahlen deutlich vorangebracht und gleichzeitig auch verstärkt in die öffentliche Diskussion gerückt. Die in allen Lebensbereichen voranschreitende Digitalisierung zeigt gerade im digitalen Zahlungsverkehr sowohl bei den Dienstleistern, aber auch beim Zahlungsverhalten der Konsumenten eine hohe transformatorische Wirkung. Bei vielen Verbraucherinnen und Verbrauchern - vor allem bei jüngeren Generationen - ist es heute selbstverständlich, dass Bankdienstleistungen zunehmend mit einer Banking-App statt in einer Bankfiliale getätigt werden und dass am Point of Sale mit dem Smartphone oder der Smartwatch bezahlt wird. Die Bereitstellung und Erbringung dieser Paymentdienste setzt eine enge Zusammenarbeit zwischen regulierten und nicht regulierten Dienstleistern voraus. Paymentservices stellen einen wichtigen Teil der Lösungsangebote im gesamten Finanzökosystem dar und gewinnen aufgrund des weltweiten Wachstums digitaler Zahlungen zunehmend an Bedeutung. Der Paymentservices-Teil des Ökosystems hat sich in den letzten Jahren stark verändert. Auch hier stehen wir vor einem Wendepunkt, der strategische Weichenstellungen bei vielen Akteuren erfordert, um die Markt- und Kundenbedürfnisse auch in Zukunft resilient bedienen zu können.

In den letzten zehn Jahren hat sich das Payment-Ökosystem, also die verschiedenen Dienstleister, die Zahlungen im Handel, E-Commerce oder zwischen Privatpersonen und Unternehmen ermöglichen, stark verändert. Traditionelle Anbieter standen und stehen unter dem Druck, ihre Digitalisierungsprojekte schneller voranzutreiben und haben häufig ihre geographische Präsenz durch Firmenübernahmen erweitert, um so Skaleneffekte zur Kostenoptimierung oder zum Ausbau ihrer Wettbewerbsposition zu erzielen. Beispiele hierfür sind die europäischen Paymentdienstleister Worldline (mit Sitz in Frankreich) und Nexi (mit Sitz in Italien). Beide Unternehmen sind durch ambitionierte Unternehmenszukäufe u. a. auch in Deutschland heute europaweit marktführende Anbieter. Aus deutscher Sicht muss man konstatieren, dass es keinen einzigen deutschen Payment Services Provider mehr gibt, der eine marktführende oder relevante Marktposition in Deutschland oder mit einer europäischen Dimension hat. Die Gründe hierfür sind vielfältig. Letztlich liegt es daran, dass keine der etablierten deutschen Bankengruppen ein strategisches Interesse an dieser Form der Paymentdienstleistung in den letzten Jahren entwickelt hat bzw. bereit war, signifikant in diese Geschäftsaktivitäten zu investieren. Dies hängt sicherlich auch damit zusammen, dass keine deutsche Bank oder Bankengruppe im Retail-Payment oder Retail-Banking außerhalb Deutschlands nennenswert aktiv ist. Dementsprechend haben sie sich im Verlauf der letzten ca. 15 Jahre von fast allen Payment-Unternehmen oder Beteiligungen in diesem Bereich getrennt. In der Konsequenz ist die „Deutsche Kreditwirtschaft" daher heute nicht wirklich in einer gestaltenden Position bei der Entwicklung und Umsetzung strategisch neuer, europäischer Zahlungsverkehrsstrukturen.

Traditionelle Paymentunternehmen bzw. traditionelle Banken stehen zudem häufig vor der Herausforderung, ihre historisch gewachsenen Strukturen und IT-Systeme mit erheblichen Investitionen in Digitalisierungsprojekte zu erneuern. Dies hat zwar dazu geführt, dass mittlerweile fast alle Banken inzwischen ihren Kunden eine Banking-App anbieten. Hinter diesen Apps stehen jedoch oftmals jahrzehntealte Bankbetriebssysteme, die eine sehr gute Customer Experience, Innovation oder Skalierung nicht in dem Maße zulassen, wie es beispielsweise cloudbasierte Plattformen heute viel besser ermöglichen. Erschwerend kommt für den deutschen Bankensektor hinzu, dass er die niedrigste Kosteneffizienz in Europa aufweist, was unter anderem auf den stark fragmentierten, traditionell dreigeteilten deutschen Bankensektor zurückzuführen ist.

Auf der anderen Seite ist seit einigen Jahren eine rasante Entwicklung etablierter, international agierender Paymentanbieter wie z. B. Mastercard, Visa oder Paypal zu beobachten. Auch sogenannte Fintechs, die zum Teil erst vor 10-15 Jahren gegründet wurden, haben sich als marktführende Payment- oder Banking-Anbieter positioniert. Beispiele sind im Payment das börsennotierte niederländische Unternehmen Adyen oder das durch Venture Kapital finanzierte US-amerikanische Unternehmen Stripe. Im Banking bieten junge Digitalbanken wie Bunq aus den Niederlanden oder N26 aus Deutschland Plattformen an, bei denen digitale Zahlungs- und Bankingdienstleistungen im Mittelpunkt eines rein digitalen Geschäftsmodells stehen.

Die weltweit führenden Paymentunternehmen kommen heute überwiegend aus den USA oder aus Asien und zeichnen sich durch Plattformstrategien mit unterschiedlicher Wertschöpfungstiefe aus. Während beispielsweise die chinesische Plattform Alipay umfassende Zahlungs- und Finanzdienstleistungen für Konsumenten und Händler in einem eigenen Ökosystems anbietet, ist das Geschäftsmodell der amerikanischen Kartenorganisationen Mastercard und Visa mit ihren globalen Plattformen auf die Zusammenarbeit mit Banken und Paymentdienstleistern angewiesen.

In Europa bieten heute alle Retailbanken Debit- oder Kreditkarten an, die auf Kartenlösungen von Mastercard oder Visa basieren und aufgrund der globalen Akzeptanz fast überall auf der Welt von Händlern akzeptiert werden. Der amerikanische Payment-Wallet-Anbieter PayPal verfolgt dagegen ein Geschäftsmodell, bei dem sowohl Händler als auch Konsumenten über eine Plattform bedient werden. Allein in Deutschland haben bereits über 32 Millionen Kunden diesen Service genutzt.

Neben den internationalen Payment-Anbietern sind es aber vor allem die fünf High-Tech-Unternehmen Alphabet, Meta, Apple, Amazon und Microsoft, die mit ihren Plattformen die Entwicklung des Payments und der digitalen Gesellschaft insgesamt in Nordamerika und Europa gestalten, manche sagen sogar „dominieren". Diese „Big Techs" sind häufig „Gamechanger" und „Enabler", wenn es um die Digitalisierung – auch im Zahlungsverkehr – in Wirtschaft und Gesellschaft geht. So hat Apple mit seinem Produkt „Apple Pay" den Standard für das mobile Bezahlen mit dem Smartphone gesetzt. Als „Apple Pay" vor fünf Jahren auch in Deutschland eingeführt wurde, waren es vor allem junge Digitalbanken, die „Apple Pay" vom ersten Tag an ihren Kunden anboten. Viele traditionelle Banken haben damals den Kundenwunsch nach einer solchen Form des Bezahlens am Point of Sale nicht erkannt. Sie zogen erst im Laufe der Zeit aufgrund des zunehmenden Kunden- und Marktdrucks nach.

In Politik und Medien wird immer wieder der Ruf nach eigenen, europäischen Angeboten bzw. Plattformlösungen laut. Im Zahlungsverkehr wird dieser Wunsch mit der öffentlichen Initiative des „Digitaler Euro" sowie der privatwirtschaftlich getragenen „European Payment Initiative" (EPI) in Verbindung gebracht. Beide Initiativen werden von ihren Protagonisten häufig als notwendige Konkurrenz zu den amerikanischen Paymentplattformen positioniert. Da beide Initiativen auf eine „Instant-Payment" Lösung setzen, unterscheiden sie sich tatsächlich von den bestehenden Zahlungsinstrumenten der Debit- oder Kreditkarte, wie wir sie in Deutschland von Mastercard, Visa oder der Girocard kennen. Die Big Tech Unternehmen und große Payment Services Provider haben jedoch den Trend hin zu den innovativen Technologien, wie z. B. der Blockchain-Technologie, Open Banking oder künstlicher Intelligenz jedoch längst erkannt und schaffen es auch hier, (Fort)Schrittmacher im Finanzökosystem zu sein. Während wir uns hierzulande in mehrjährigen Vorbereitungsphasen befinden, entwickeln die Big Techs mit erheblichen Investitionen Produkte und setzen oft die Marktstandards. Dies gilt auch für den klaren Trend hin zu Digital-Wallet-basierten Zahlungen, die in Zukunft vermehrt als „Instant-Payment" und nicht mehr zwingend auf Basis einer im Wallet hinterlegten Debit- oder Kreditkarte erfolgen werden.

So ist es nun auch für den digitalen Euro sowie für EPI geplant, diese Form der Sofortzahlung den Bürgern in digitalen Wallets anzubieten – sei es als eigenständiges oder als Wallet in der persönlichen Banking-App. Während Instant-Payment in einigen Ländern als Fortschritt gegenüber kartenbasierten Zahlungen oder Bargeldzahlungen gesehen wird, weil es z. B. in digitalen Geschäftsmodellen die Zahlung hinsichtlich Sicherheit und Garantie für Konsumenten und Händler verbessert, verlangen viele Banken in Deutschland heute für „Echtzeit-Überweisungen" ein zusätzliches Entgelt von bis zu 1,50 € pro Überweisung. Es stellt sich die Frage, ob dies nicht eher eine prohibitive und damit nicht zukunftsfähige Preisgestaltung ist.

Die großen Big-Tech-Plattformen sind heute in vielen Bereichen die treibende Kraft für die Entwicklungen von Ökosystemen, dies gilt insbesondere für das Finanzökosystem. Es ist daher folgerichtig, dass wir in Europa darüber diskutieren, in welchen rechtlichen und regulatorischen Strukturen sich insbesondere große Technologieplattformen, Finanzdienstleister und Payment-Anbieter bewegen können bzw. dürfen. Auf der anderen Seite sollten wir aber davon ausgehen, dass sich der Erfolg von europäischen Zahlungsverkehrsinitiativen nicht gegen die sogenannten Big Tech, sondern vielmehr in geeigneten Formen der Zusammenarbeit mit ihnen erreicht werden kann. Zudem muss den Akteuren, die neue digitale Bezahlverfahren entwickeln und dem Handel und den Kunden bereitstellen, ein profitables Geschäftsmodell ermöglicht werden. Ein Aspekt, den die Politik und die Regulierung an manchen Stellen ausblenden. Um die Erfolgsaussichten dieser europäischen Initiativen zu erhöhen, müssen sie Teil eines offenen Ökosystems für verschiedene Wallet-Anbieter werden, das mit der Integration weiterer Dienste, wie digitale Identität oder digitale Signatur, einhergeht.

1.200 Mrd.$

Wurden in den letzten 10 Jahren wurden weltweit in den Fintech-Sektor investiert

ca. 400

Neobanken gibt es mittlerweile Weltweit

Fintech-Unternehmen leisten mittlerweile einen wichtigen und wachsenden Beitrag zur Innovationskraft und Resilienz des Finanzsektors. Diese technologiegetriebenen Fintech-Plattformen konkurrieren inzwischen vielfach erfolgreich mit dem traditionellen Bankensektor oder ermöglichen im Rahmen von Partnerschaften Innovationen bei den klassischen Finanzdienstleistern. In den letzten 10 Jahren wurden weltweit ca. 1.200 Mrd. USD in den Fintech-Sektor investiert worden, davon sind über 50 % in Fintech-Unternehmen in Amerika geflossen (Statista 2023). Weltweit gibt es mittlerweile rund 400 Neobanken. Sie sind einer der wichtigsten „Innovations-Inkubatoren" für die Finanzbranche, da ihre Geschäftsmodelle zumeist ausschließlich digital aufgestellt sind und damit die Kundenerlebnisse im Payment- und Banking revolutionieren. Beschränkten sich die Geschäftsmodelle der Neobanken zunächst auf Konto- und Zahlungsverkehrsprodukte, bieten diese App-basierten Digitalbanken zunehmend neue Dienstleistungen für beispielsweise alternative digitale Zahlungen, für Aktien- und Fondssparen, für Kredite, für den Handel mit Kryptowährungen oder für das persönliche Finanzmanagement an. Wenn diese Fintech-Banken jedoch eine europaweite Plattformstrategie verfolgen, stoßen sie heute noch auf verschiedene Defizite im europäischen Binnenmarkt. So gibt es beispielsweise das Problem, dass eine deutsche IBAN von einem ausländischen Unternehmen oder einer Behörde nicht akzeptiert wird.

Dies liegt u.a. an der unterschiedlichen Umsetzung von Geldwäschevorschriften bzw. an fehlenden digitalen Kommunikationsstrukturen zwischen den Behörden in den verschiedenen Ländern, die für eine effiziente Geldwäschebekämpfung notwendig wären. Resilienz im Zahlungsverkehr setzt daher auch eine resiliente, grenzüberschreitende Struktur in der Betrugsbekämpfung voraus. Eine weitere Harmonisierung und Angleichung nationaler Besonderheiten an europäische Standards ist nicht nur wünschenswert, sondern eine wichtige Voraussetzung für europäisch ausgerichtete Geschäftsmodelle im digitalen Zahlungsverkehr und Banking.

Die Vereinheitlichung der regulatorischen Anforderungen im Zahlungsverkehr innerhalb der Europäischen Union (EU) ist noch stark verbesserungsbedürftig. Die EU verfolgt mit ihren Richtlinien und gesetzlichen Vorgaben zwar das Ziel einer stärkeren Vernetzung von Plattformen, die dann auch den Zugang zu paneuropäischen digitalen Payment- oder Banking-Plattformen erlauben. In der konkreten Umsetzung stoßen diese Ziele jedoch auf national unterschiedliche Prinzipien und Auslegungen, die Entwicklungen oftmals verlangsamen und damit nicht die Wettbewerbsposition europäischer Unternehmen stärken. Wenn die globalen Trends im digitalen Zahlungsverkehr in Europa nicht erkannt und mehr an Gemeinsamkeit im Payment und Banking in Europa umgesetzt wird, dürfen wir uns auch nicht wundern, wenn sich europäische Fintech-Plattformen nicht mit der Dynamik entwickeln können, die für diese Geschäftsmodelle notwendig sind, um auch gegen die Global Player bestehen zu können.

Der digitale Zahlungsverkehr steht im kommenden Jahrzehnt vor nachhaltigen technologiegetriebenen Veränderungen. Die meisten Menschen stehen diesen Entwicklungen im digitalen Zahlungsverkehr und Banking offen bis positiv gegenüber. Es gibt aber auch Teile der Gesellschaft, die diese Entwicklungen kritisch sehen oder ablehnen. Wenn wir aber in Europa die Digitalisierung von Finanzdienstleistungen nicht energisch und transparent vorantreiben, überlassen wir wichtige Instrumente zur weiteren Ausgestaltung der digitalen Gesellschaft zunehmend anderen. Denn eines ist sicher: Die Gesellschaft wird digitaler – so oder so.

Prof. Dr. Helmut Schönenberger
CEO UnternehmerTUM

Jennifer Kaiser-Steiner
Referentin des CEO

Technologie und Innovation - Start-ups als Beitrag zur Resilienz

Deutschland ist nach vielen Jahrzehnten des Wohlstands, des technischen Fortschritts, der Globalisierung und der militärischen Entspannung wieder mit tiefgreifenden gesellschaftlichen, ökologischen und wirtschaftlichen, aber auch sicherheitspolitischen Herausforderungen konfrontiert. Zudem sucht unsere Gesellschaft nach Wegen, eine nachhaltige Form des Wirtschaftens zu finden, die im Einklang mit der Natur steht, den Klimawandel aufhält und mit den beschränkten globalen Ressourcen haushält.

Technologie und Wandel

Vor diesem Hintergrund gewinnen die Entwicklung und der Einsatz innovativer Technologien als unverzichtbarer Teil des Lösungswegs in Richtung einer nachhaltigen Zukunft immer mehr an Bedeutung. Mit der zunehmenden Dringlichkeit zum Wandel nimmt auch der Druck zu, konkrete Lösungen zu liefern. Umsetzbare Anwendungen müssen skaliert werden, damit sie signifikant zur Resilienz beitragen und eine positive Wirkung auf das Wirtschafts- und Finanzsystem haben. Ein zentrales Element dieses Ansatzes ist, dass mit dem technischen Fortschritt die Wertschöpfung, der Wohlstand aber auch die Widerstandsfähigkeit der Gesellschaft steigen. Dies wird zum Beispiel durch die Gewinnung von günstigem Strom durch erneuerbare Energie, durch Effizienzsteigerungen mit der Automatisierung von Prozessen oder der Weiterentwicklung von Künstlicher Intelligenz erreicht. Zudem kann Resilienz durch eine verbesserte Widerstandsfähigkeit bzw. Anpassungsfähigkeit von Böden, Pflanzen, Tieren und Menschen erzielt werden, indem beispielsweise innovative Wirkstoffe zum Einsatz kommen oder auf eine regenerative Landwirtschaft umgestellt wird. Resilienz kann auch durch den Ausbau einer robusten Infrastruktur gesteigert werden, die die effiziente Mobilität von Personen und Gütern und die Verfügbarkeit von Daten und Energie sicherstellt.

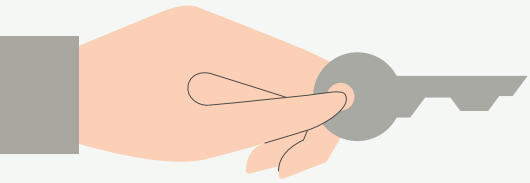
Start-ups sorgen für Fortschritt, Souveränität und Wettbewerbsfähigkeit

Auch die Finanzwelt wird stark vom technologischen Fortschritt beeinflusst. Speziell die Nutzung von Kommunikationstechnologie ist die Grundlage der modernen Finanzwelt. Gleichzeitig bringt diese immer neue Gefahren wie Hackerangriffe oder Datenmissbräuche mit sich. Neue Technologien wie die Quantenverschlüsselung und Quantumcomputing ermöglichen wiederum ganz neue Sicherheitslösungen und innovative Geschäftsmodelle.

Im Wettrennen um technologischen Fortschritt, Souveränität und Wettbewerbsfähigkeit spielen Start-ups mit ihrer Schnelligkeit und Fähigkeit, disruptive Innovationen hervorzubringen, eine herausragende Rolle. Start-ups fungieren als effektives Bindeglied zwischen Forschung und Wirtschaft und tragen entscheidend dazu bei, neuartige Technologien rasch auf den Markt zu bringen. Ihr Beitrag als Beschleuniger für Innovation hat insbesondere in den letzten Jahrzehnten massiv zugelegt. Das Silicon Valley hat dabei als besonders dynamisches und leistungsstarkes Innovationscluster eine herausragende Rolle als Vorbild eingenommen.

Deutschlands Innovationsfähigkeit bedroht

Deutschland zeigt als eine der führenden globalen Technologie- und Innovationsnationen nach wie vor in Branchen wie der Automobilindustrie, dem Maschinenbau und der Chemie eine starke wirtschaftliche Präsenz. Gleichzeitig fehlt es im Vergleich zu anderen Wirtschaftsnationen an Wachstumsdynamik, bei der Entwicklung von Spitzentechnologien und der Digitalisierung hinkt Deutschland im internationalen Vergleich hinterher. Damit schwindet auch der Zugang zu wichtigen Ressourcen, um die Zukunft aktiv zu gestalten. Das betrifft insbesondere den Zugang zu Top-Talenten, aber auch zu Rohstoffen, zu Schlüsselprodukten wie Halbleitern, den Zugang zum Weltall, zu Daten, zu Rechenleistung oder zu günstiger Energie. All diese Rückstände gefährden die Resilienz Deutschlands enorm!



Ökosysteme als Garant für Resilienz

Der Schlüssel zur effektiven Förderung von Innovationen liegt in einem vernetzten Ökosystem, das etablierte Unternehmen, Universitäten, Forschungseinrichtungen, Start-ups, Investoren und die Politik miteinander verbindet. Nur so können Synergien genutzt, Stärken kombiniert und eine kritische Masse an Ressourcen gebündelt werden. Dies ist die Voraussetzung für die Bildung starker und widerstandsfähiger Innovationscluster.

Die Metropolregion München ist in Europa ein herausragendes Beispiel für ein gut vernetztes und dynamisches Innovationsökosystem. Mit Spitzenuniversitäten wie der TUM (Technische Universität München), außeruniversitären Forschungseinrichtungen wie der Max-Planck-Gesellschaft, globalen Unternehmen, Mittelständlern, agilen Start-up-, sowie Investoren-Szene schafft München zusammen mit der bayerischen Staatsregierung ein attraktives unternehmerisches Umfeld, das kontinuierlich Talente und Spitzenkräfte aus der ganzen Welt anzieht und kontinuierlich wächst. TUM, als eine der führenden europäischen Eliteuniversitäten, und UnternehmerTUM, als größtes europäisches Gründungszentrum, übernehmen darin eine zentrale Rolle als Innovationsplattform und große Quelle für neue Unternehmungen.

Systematischer Ausgründungsprozess in München

Gegründet im Jahr 2002 mit Hilfe der Unternehmerin Susanne Klatten, hat UnternehmerTUM einen systematischen Ausgründungsprozess etabliert und gilt heute als größte Start-up Fabrik in Europa. In den Jahren 2021 bis 2023 hat der Einfluss von TUM und UnternehmerTUM als Geburtsstätte für wachstumsstarke Tech-Unternehmen einen neuen Höchststand erreicht: Über 20 Prozent des deutschen Wagniskapitalvolumens – jährlich rund zwei bis drei Milliarden Euro - flossen in Start-ups, die von TUM und UnternehmerTUM unterstützt wurden. Zu den Erfolgsgeschichten gehören „Einhörner" und Tech-Unternehmen wie Celonis, Lilium, Flixbus und Personio. Diese können insbesondere die Stärke des industriellen Münchner Clusters hebeln und mit den etablierten Unternehmen vor Ort Kunden-, Lieferanten-, Investment-Beziehungen oder andere strategische Partnerschaften eingehen.

Europäische Kräftebündelung

Trotz aller regionaler Clusterbildung ist es für die heimischen Wachstumsunternehmen wichtig, die Zusammenarbeit über lokale oder nationale Grenzen hinweg zu forcieren, um internationale Absatz- und Kapitalmärkte für das eigene Unternehmen zu gewinnen und weitere Lieferanten-, Talente-, Partner- und Technologienetzwerke für den Unternehmenserfolg zu nutzten. In Zeiten einer nach wie vor stark vernetzten globalen Wirtschaft und vieler gemeinsamen Herausforderungen ist es unerlässlich, auch zwischen einzelnen Innovationsclustern resiliente Netzwerke aufzubauen. Das gilt insbesondere auf europäischer Ebene: Nur gemeinsam kann in Europa nachhaltiger Wohlstand erreicht werden.

Ein Beispiel für die aktive Schaffung eines europäischen Innovationsclustern ist Rise Europe. Die Initiative, die von UnternehmerTUM, dem dänischen DTU Skylab und dem Pariser Inkubator Agoranov gestartet wurde, ist ein paneuropäisches Netzwerk führender Entwickler lokaler Start-up Ökosysteme. Ziel ist es, gemeinsam neue europäische Technologie- und Marktführer zu fördern und ihnen überregional die Unterstützung sowie Ressourcen bereitzustellen, die sie benötigen, um im globalen Wettbewerb erfolgreich zu sein. Vertreter aus 14 Ländern arbeiten inzwischen im Rahmen von Rise Europe zusammen, um das Wachstum ihrer Start-up Teams über die nationalen Grenzen hinweg zu beschleunigen und damit zur technologischen Souveränität Europas beizutragen. Rise Europe adressiert auch Herausforderungen wie die Klimakrise und die Ressourcenknappheit. Durch die Unterstützung von technologieorientieren Start-ups, die sich einer wohlhabenden und zukunftsorientierten Gesellschaft in Europa verschrieben haben, strebt das Netzwerk eine positive Wirkung sowohl auf europäischer als auch auf globaler Ebene an. Mittels eines strategischen Wissensaustauschs, gemeinsamen Mentorenprogrammen und Zugang zu einem umfangreichen Ressourcennetzwerk positioniert sich Rise Europe als Katalysator für nachhaltige Veränderungen und Beschleuniger der nächsten Generation europäischer, nachhaltiger Technologieunternehmen.

Ausblick in Richtung einer resilienten Zukunft

Start-ups, die sich durch ihre Schnelligkeit, Anpassungsfähigkeit und ihren Zugang zu Spitzentechnologie auszeichnen, werden auch in Zukunft eine zentrale Rolle bei der Schaffung nachhaltiger Innovation und somit bei der Resilienz-Steigerung spielen. Führende Cluster wie das Silicon Valley zeigen, welches enorme Potenzial Start-ups als Motoren für Wirtschaftswachstums und technologischen Fortschritt haben. Durch die Optimierung der Rahmenbedingungen und die Etablierung von Innovationsplattformen wie der Stanford University oder der TUM und UnternehmerTUM in Deutschland kann ein Umfeld geschaffen werden, das die unternehmerische Dynamik massiv beschleunigt.

Um das unternehmerische Ökosystem um Hochschulen systematisch zu stärken und den nahtlosen Übergang von Spin-off-Teams aus dem akademischen Bereich in die Industrie zu erleichtern, ist es erforderlich, die bestehenden Unterstützungsstrukturen und -prozesse auszuweiten und zu professionalisieren. Dazu gehört die Entwicklung eines umfassenden Unterstützungssystems, das diesen aufkeimenden Start-ups Anleitung, Mentoring und Ressourcen bietet und sicherstellt, dass sie sich in der komplexen Unternehmenslandschaft zielorientiert und kompetent bewegen.

Aufbau weiterer Start-up Fabriken

Zur weiteren Optimierung der deutschen Gründungsszene hat die Bundesregierung eine umfassende Start-up-Strategie entwickelt. Eine zentrale Maßnahme ist es, in Deutschland bis zu zehn weitere Start-up Fabriken nach dem Vorbild von UnternehmerTUM zu schaffen.

Neben der Förderung hochschulnaher Gründungen und des Transfers von geistigem Eigentum aus Universitäten, ist die Verbesserung der Start-up Finanzierungslandschaft in Europa ein wichtiger politischer Fokus. Ein funktionierender Kapitalmarkt für nachhaltige Innovationen ist ein entscheidender Faktor für den Aufbau einer starken europäischen Innovationsszene. Um dies zu erreichen, ist es wichtig, dass mehr Risikokapital für Start-ups in Deutschland und Europa zur Verfügung gestellt wird. Dies könnte beispielsweise durch die Erschließung von Finanzmitteln von Versicherungen, Pensionsfonds und Stiftungen erreicht werden. Mit einer gemeinsamen Anstrengung zur Verbesserung des europäischen Innovationsökosystems lässt sich das gesamte unternehmerische Potenzial Europas heben. So kann eine neue Generation resilienter Markt- und Technologieführer entstehen, die wiederum Treiber für Wachstum und Wohlstand sind.

2. Regulatorik und Aufsicht als Garant für Finanzresilienz?

Dr. Lea Marie Siering
Managing Director, Token GmbH

Finanzresilienz in der Aufsicht - Regulatorische Maßnahmen für ein tragfähiges, stabiles Finanzsystem

Was ist Resilienz

Charles Darwin hat gesagt, dass „nicht die stärkste Spezies [überlebt], auch nicht die intelligenteste, sondern diejenige, die am besten auf Veränderungen reagiert." Er beschreibt dabei nichts anderes als Resilienz - ein Begriff, der in den letzten Jahren eine hohe Popularität bei der Formulierung wirtschafts- und finanzpolitischer Zielsetzungen erlangt hat. Angesichts einer raschen Abfolge gravierender Krisen kann der Aufstieg dieses Begriffs nicht überraschen.

Resilienz ist ein Begriff, der in vielen verschiedenen wissenschaftlichen Kontexten verwendet wird. Naturwissenschaftliche, sozialwissenschaftliche, betriebswirtschaftliche und rechtswissenschaftliche Disziplinen verwenden ihn. Der Begriff findet seinen Ursprung im Lateinischen: „resilire", was zurückspringen heißt. Der Begriff Resilienz passt damit auch zur Finanzwirtschaft. Er drückt sowohl die Krisentragfähigkeit als auch die nach der Krise notwendige Zukunftsfähigkeit aus.

Betriebswirtschaftlich wird in Bezug auf Resilienz davon ausgegangen, dass Unternehmen über die Fähigkeit verfügen müssen, auf krisenhafte Situationen reagieren zu können. Resilienz für Organisationen wird demnach als die Fähigkeit definiert, Krisen zu überleben oder sogar gestärkt aus ihnen hervorzugehen.

Nicht nur in Bezug auf die Finanzbranche wurde Resilienz in den vergangenen Jahren nachhaltig auf die Probe gestellt. Nach der Corona Krise, dem Angriff Russlands auf die Ukraine oder zuletzt dem Terrorangriff der Hamas aus Israel sowie weiteren geopolitischen Konflikten, braucht „man" ebenso wie Finanzdienstleister vor allem eines: die Fähigkeit, schwierige Lebenssituationen wie Krisen oder Katastrophen ohne dauerhafte Beeinträchtigung zu überstehen. Dies erfolgt regelmäßig, indem mögliche Risiko-Szenarien erkannt und sich auf diese präventiv vorbereitet werden.

Resilienz als Grundvoraussetzung für unsere Wirtschaft

Finanzresilienz ist wichtiger denn je; denn sie braucht es, finanzielle Schocks, Unsicherheiten, systemische Risiken oder andere widrige Umstände zu bewältigen, ohne dabei ernsthafte finanzielle Schäden zu erleiden. Es ist die Fähigkeit, auftretende Schocks absorbieren zu können. Es geht im Kern darum, widerstandsfähig gegenüber wirtschaftlichen Turbulenzen, Krisen oder unvorhersehbaren Ereignissen oder Risiken zu sein. Das Finanzsystem muss auch in Stressphasen so kapitalisiert und liquide sowie gegenüber Risiken wie etwa Cyber- und politischen Risiken oder Risiken aus Unsicherheit und dem Strukturwandel wie insbesondere infolge des Klimawandels und damit verbundenen, notwendigen klimapolitischen Maßnahmen wie einer kohlenstoffarmen Wirtschaft, mithin Net-Zero - ausgestattet sein, dass es besteht.

Resilienz ist aufgrund ihrer tragenden Bedeutung des Finanzsektors für die Stabilität der Wirtschaft und damit einhergehend für den Wohlstand einer Volkswirtschaft unabdingbar; sie spielt angesichts steigender Risiken und Herausforderungen auch im Bankaufsichtsrecht eine herausragende Rolle. Denn Resilienz und eine robuste Finanzinfrastruktur sind entscheidend für den Schutz von Wohlstand, Wirtschaft, Staat und Gesellschaft. Diese Bedeutung ist in den vergangenen Jahren stetig gewachsen angesichts steigender Risiken und Bedrohungen, wie etwa geschickten Betrugsmethoden - weitgehend über das Internet -, Social Engineering oder Cyberangriffen mit Hilfe künstlicher Intelligenz, aber auch klimapolitischen Maßnahmen oder Auswirkungen aus der Pandemie der vergangenen Jahre.

Resilienz Quo Vadis

Finanzresilienz ist nicht nur von nationalen Faktoren, sondern im Zuge einer fortschreitenden Globalisierung im Besonderen auch von wirtschaftlichen Entwicklungen abhängig. Entsprechend hat die Europäische Union in den vergangenen Jahren auch verstärkte Bemühungen verfolgt, die Finanzstabilität innerhalb der EU zu verbessern. Bestandteil hiervon war u.a. die Einführung von Maßnahmen zur Bankenunion und zur Harmonisierung der Bankenregulierung.

Die deutsche Volkswirtschaft ist seit Jahrzehnten vielfältigen langfristigen Veränderungen ausgesetzt. Der Strukturwandel, ausgelöst insbesondere durch technologischen Fortschritt, aber auch durch den demografischen Wandel und die Transformation hin zu einer klimaneutralen Wirtschaft, ist eine große Herausforderung. Dies insbesondere, da solche Unsicherheiten aufgrund geopolitischer Spannungen, veränderten Rahmenbedingungen, Klimarisiken, oder ähnlichem, Investoren verunsichern und zu Kapitalflucht führen kann, was wiederum die Liquidität des Finanzsystems beeinträchtigen und die Kosten für Kapital erhöhen kann. Auch können geopolitische Ereignisse zu Volatilität an den Finanzmärkten führen.

Angesichts geopolitischer Unsicherheiten ist ein effektives Risikomanagement auf mikroprudenzieller Ebene entscheidend. Unternehmen und Investoren sollten Strategien entwickeln, um sich vor negativen Auswirkungen abzusichern, sei es durch Diversifikation, Versicherungen oder andere Absicherungsmechanismen. Makroprudenziell ist die Stabilität des Finanzsystems als Ganzes zu überwachen. Die Wirtschaftspolitik ist entsprechend gefordert, die mit der Corona-Pandemie begonnene Krise zu bewältigen, die ökonomische und aufsichtliche Resilienz in Deutschland und Europa zu stärken und damit das dringend erforderliche Wachstumspotenzial zu erhöhen.

Finanzresilienz in Deutschland

Wo steht Deutschland im Hinblick auf technische Innovationen heute und auch im Vergleich zu anderen europäischen Ländern? Ist dies ausreichend, um die Resilienz des Finanzsystems tatsächlich zu gewährleisten?

Deutschland hat eine der größten und zugleich stabilsten Volkswirtschaften in der Europäischen Union. Entsprechend müssen deutsche Finanzinstitute robust und gut kapitalisiert sein. Die Aufsichtsbehörden in Deutschland, d. h. die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und die Bundesbank, spielen eine entscheidende Rolle bei der Überwachung und Regulierung der Finanzinstitute, um die Stabilität des Finanzsystems zu gewährleisten. Die Überwachung erfolgt dabei makroprudenziell, d. h. die Stabilität des Finanzsystems wird aufsichtlich als Ganzes überwacht.

Veränderte technologische Realität

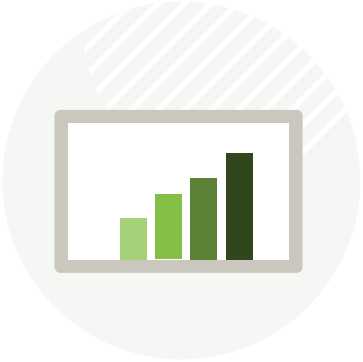
Der technologische Wandel und insbesondere ein zunehmendes Maß an Digitalisierung führen durch neue Geschäftsmodelle und Produktionsprozesse zu tiefgreifenden Veränderungen im Finanzsektor bzw. bei den Finanzinstituten der Wirtschaft. Ein ähnlich umfassender Strukturwandel steht durch die geplante Reduktion der Treibhausgasemissionen an, die eine Transformation hin zu einer klimaneutralen Wirtschaft notwendig macht. Hiervon betroffen sind ebenfalls Finanzinstitute. Es sind Rahmenbedingungen notwendig, die einerseits einen anhaltenden Aufschwung und langfristiges Wachstum sicherstellen, andererseits aber auch Resilienz wahren.

Anstieg von Cyberrisiken

Die verstärkte Abhängigkeit von komplexen IT-Systemen, Softwareanwendungen und Betriebssystemen, die zunehmende Vernetzung von Geräten, Systemen und Infrastrukturen, sowie auch zum Teil bestehende mangelnde Sicherheitsmaßnahmen führen zu einer erhöhten Angriffsfläche für Cyberangriffe. Auch ist zunehmend eine Professionalisierung von Cyberkriminellen zu beobachten; etwa durch Verfügbarkeit von Cybercrime-Tools im Darknet, wodurch es auch weniger erfahrenen Akteuren ermöglicht wird, Angriffe durchzuführen. Nicht zuletzt fungieren Cyberangriffe als moderne Kriegswaffe: Einige Staaten setzen Cyberangriffe als Mittel zur Spionage oder zur Durchsetzung

politischer Ziele ein. Dies hat zu einer Zunahme von hochentwickelten Angriffen geführt, die oft schwieriger zu erkennen und abzuwehren sind. Die Risiken für betriebliche Störungen durch (auch politisch motivierte) Cyberangriffe zur Schwächung der Wirtschaft sind angesichts des geopolitischen Umfelds gestiegen. Verwenden Banken etwa veraltete IT-Systeme und IT-Sicherheitsstandards oder verfügen sie nicht über gut ausgebildetes Personal, macht dies sie gegenüber Cyberrisiken verwundbar. Investitionen in eine resiliente IT-Infrastruktur und Schutz gegen Cyberrisiken sollten daher Priorität haben.

Die Jahresberichte des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Lage der IT-Sicherheit belegen in den vergangenen Jahren gleiches: in den letzten Jahren spitzte sich die Risikolage fortwährend zu; das BSI bewertet die „Gefährdungslage im Cyber-Raum" seit 2022 als so hoch, wie noch nie zuvor.



Diese steigende Komplexität und Vernetzung der digitalen Welt sowie die aktuellen geopolitischen Krisen erfordern eine kontinuierliche Verbesserung von Sicherheitspraktiken, die Zusammenarbeit zwischen verschiedenen Akteuren und eine ständige Anpassung an neue Bedrohungen.

Regulatorische Sicherstellung von Resilienz

Für die Resilienz von Instituten spielt also auch der Umgang mit jedweden operationellen Risiken eine tragende Rolle. Dies wird auch durch regulatorische Vorgaben sichergestellt. Besonders in den letzten Jahren konnte vermehrt ein Anstieg an entsprechenden Vorgaben beobachtet werden:

Auf nationaler Ebene hat die Bundesregierung etwa im Juni 2023 ihre erste Nationale Sicherheitsstrategie vorgelegt, in deren Mittelpunkt die geopolitischen Herausforderungen und die Resilienz der deutschen Wirtschaft stehen. In einer zunehmend global vernetzten Wirtschaft betont die Bundesregierung dabei die gemeinsame Verantwortung staatlicher und privater Akteure.

Auf europäischer Ebene arbeiten die Mitgliedstaaten bereits seit Jahren gemeinsam daran, den Rechtsrahmen der Finanzwelt robuster gegen Angriffe auf IT-Systeme zu machen. Seit 2017 gibt es die EU-Cybersicherheitsstrategie, 2018 traten die NIS Directive zum Schutz kritischer Infrastruktur – also auch den Finanzsektor betreffend – sowie ein Fintech-Aktionsplan in Kraft, mit dem Ziel, der Finanzindustrie zu helfen, den rasanten technologischen Fortschritt zu nutzen und dabei gleichzeitig die Cybersicherheit zu stärken.

Diese Maßnahmen scheinen allesamt zu wirken. So schreibt etwa die Deutsche Bundesbank in ihrem jährlich veröffentlichten Finanzstabilitätsbericht, dass sich das deutsche Finanzsystem im aktuellen makrofinanziellen Umfeld bislang als stabil erweist. Sie verweist aber auch darauf, dass die Herausforderungen der Zinswende und der gedämpften konjunkturellen Entwicklungen weiterhin groß seien. Demgemäß, so führt sie ebenfalls aus, sei die Weiterentwicklung des Regulierungsrahmens zum Umgang mit Liquiditätsrisiken bei Banken, Versicherern und Fonds von zentraler Bedeutung. Ausdrücklich wird in dem Zusammenhang durch die Bundesbank aber auch darauf hingewiesen, dass Banken ihre Anstrengungen zur Erhöhung der Widerstandsfähigkeit gegenüber operationellen Risiken wie Cyberrisiken aufrechterhalten und intensivieren müssen.

DORA

Der jüngste regulatorische Vorstoß ist der sogenannte Digital Operational Resilience Act (DORA). Die Europäische Kommission hatte den Legislativvorschlag zu DORA bereits am 24. September 2020 als Teil des Pakets zur Digitalisierung des Finanzsektors vorgelegt. Die Verordnung bezweckt, die Vorgaben zur IT-Resilienz europaweit zu harmonisieren und die Finanzbranche künftig besser gegen diese Risiken zu schützen. Die Europäische Union hat mit DORA eine finanzsektorweite Regulierung für die Themen Cybersicherheit, IKT-Risiken und digitale operationale Resilienz geschaffen und trägt damit wesentlich dazu bei, den europäischen Finanzmarkt gegenüber Cyberrisiken und Vorfällen der Informations- und Kommunikationstechnologe (IKT) langfristig zu stärken. Spannend ist auch, dass DORA als Verordnung unmittelbar in den Mitgliedstaaten zur Anwendung kommt, ohne dass es eines Umsetzungsgesetzes bedarf. Es besteht durch DORA in der EU damit Vollharmonisierung in den von DORA umfassten Bereichen wie etwa Vorgaben zum IKT-Risikomanagement, ein vereinheitlichtes Meldewesen zu sog. IKT-Vorfällen und wesentlichen Cyberbedrohungen, dieselben Regelungen zum Testen der digitalen operationellen Resilienz einschließlich Threat-led Penetration Testing (TLPT) sowie zum IKT-Drittparteirisikomanagement. Darüber hinaus wird es ein Europäisches Überwachungsrahmenwerk für kritische IKT-Drittdienstleister, EU-weites Information Sharing sowie Cyberkrisen- und Notfallübungen geben.

DORA wird eine große Zahl der Finanzunternehmen in der EU zu Vorkehrungen und Prozessen im Kampf gegen IT-Störungen und Cyberattacken verpflichten. Geschätzt wird die Anzahl der betroffenen Unternehmen auf rund 22.000. Durch einheitliche Standards und Regeln für das IT-Risikomanagement, das Management von IT-Drittdienstleistern, als auch für Cloud-Service-Anbieter soll Resilienz erhöht werden.

Kritisiert wird insbesondere der damit verbundene hohe Aufwand für betroffene Unternehmen. In einer ohnehin angespannten und herausfordernden Wirtschafts- bzw. Marktlage seien solche kostenintensiven Maßnahmen oftmals unzumutbar.

Ausblick

Trotz umfassender Maßnahmen bleiben Fragen bestehen: Reichen die vorstehend skizzierten Maßnahmen aus? Muss und - sofern der Fall - wie kann Resilienz insbesondere durch Regulierung und technologische Innovationen weiter gestärkt werden? Welche politischen Maßnahmen sind notwendig, um sich an die veränderte technologische Realität anzupassen und das Ziel eines resilienten Finanzsystems zu erreichen? Wie kann jeder einzelne beitragen?

Die Fragen sind aufgrund ihrer Komplexität nicht, oder jedenfalls nicht leicht zu beantworten. Zweifelsohne erfordert die Stärkung der Finanzresilienz in Deutschland und der EU eine fortlaufende Beobachtung der Risiken und Rahmenbedingungen und dann eine integrierte Herangehensweise, wie die hier skizzierten regulatorischen Vorhaben, wie jüngst DORA oder eine nachhaltige und verantwortungsvolle Finanzpolitik.

Prof. Dr. Guntram Wolff
Direktor und CEO der DGAP

Elanur Alsa
Studentische Hilfskraft im Leitungsbüro der DGAP

Das Finanzsystem der EU im Visier: Abwer von Cyber- und Hybridbedrohungen

Cyberrisiken und hybride Bedrohungen stellen eine sicherheitspolitische Herausforderung dar. Wirtschaftssysteme und Gesellschaften können durch Cyberangriffe direkt betroffen sein. Eine hybride Attacke, in der verschiedene Angriffe im Informationsbereich und in den Energiesystemen mit Attacken auf physische Infrastruktur kombiniert werden, können dabei zusätzlich destabilisierend wirken. Dabei handelt es sich nicht um rein theoretische Überlegungen, sondern gut dokumentierte Ereignisse, zum Beispiel in Estland (Demertzis & Wolff, 2020). Ein besonderer Bereich der kritischen Infrastruktur ist das Finanzsystem. Unsere moderne Gesellschaft funktioniert nicht ohne Vertrauen in das Finanzsystem und verlässliche Zahlungs- und Kreditströme. Ein paar Tage ohne ein funktionierendes Zahlungssystem würde schnell die Versorgung mit Grundgütern zum Erliegen bringen. Der Schutz des Finanzsystems ist daher von herausragender Bedeutung.

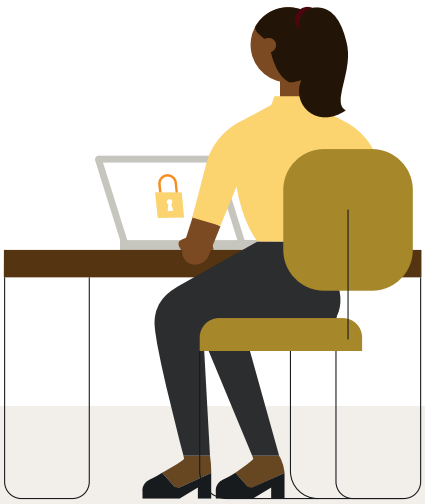
Aktuelle Studien zeigen, dass Cyberattacken gegen Unternehmen zunehmen. So findet zum Beispiel der Hiscox Cyber Readiness Report 2023, dass die Zahl der Angriffsversuche und erfolgreichen Angriffe von 2022 auf 2023 von 6 auf 10 pro Medianunternehmen in einer repräsentativen Stichprobe zugenommen haben (Hiscox, 2023). Dabei waren die Angriffe für jedes fünfte Unternehmen potenziell existenzbedrohend. Cyberangriffe stellen in Deutschland weiterhin das größte Unternehmensrisiko dar (ebd.). Die Analyse von SonicWall Cyber Threat dokumentiert ebenfalls einen Anstieg der Cyberrisiken und zeigt auch, dass Finanzinstitutionen zu den vier am meisten betroffenen Bereichen gehören (SonicWall, 2023). Eine dritte Studie von Verizon wiederum findet, dass es mehr als 1800 Vorfälle im Finanz- und Versicherungssektor in den 81 von Anfang November 2021 bis Ende Oktober 2022 untersuchten Ländern gab (Verizon, 2023). Informationen über hybride Angriffe werden hingegen weniger systematisch erfasst.

Im integrierten europäischen Finanzsystem ist es besonders wichtig, dass mögliche Attacken auf einzelne Institutionen oder Länder frühzeitig erkannt werden und Maßnahmen ergriffen werden können, die Risiken für die Finanzstabilität der gesamten EU effektiv abwehren kann. Dabei ist ein grundsätzliches Problem, dass zwar das Finanzsystem und die Finanzarchitektur inzwischen stark integriert ist, die Sicherheitsbehörden aber weitestgehend national agieren und ihre Arbeiten nur recht lose koordinieren.

Ein Versuch, Sicherheitsbedrohungen im europäischen Finanzsektor durch Cyberangriffe und Ähnliches effektiver entgegenzutreten, ist die im Januar 2023 in Kraft getretene Verordnung über digitale Betriebsstabilität der Europäischen Union (EU) „Digital Operational Resilience Act" (DORA) (EurLex, 2022). Sie zielt darauf ab, ein umfassendes und harmonisiertes Rahmenwerk für die digitale operative Widerstandsfähigkeit von EU-Finanzunternehmen und ihren IKTDienstleistern einzuführen. Darin enthalten sind unter anderem Anforderungen in Bezug auf die Verbesserung des IKT-Risikomanagements, die Klassifizierung und Berichterstattung IKTbezogener Vorfälle und eines EU-weit einheitlichen Aufsichtsrahmen für kritische IKTDrittdienstleister. Besonderen Fokus legt DORA auf die Etablierung eines umfangreichen Drittanbieter-Risikomanagements, um den einschlägigen europäischen Aufsichtsbehörden die Überprüfung ausgelagerter Dienstleistungen zu ermöglichen. Erfolgen soll die Umsetzung der Vorgaben bis Januar 2025 (EurLex, 2022).

Mit der Harmonisierung von Regelungen in Bezug auf Betriebsstabilität und Cybersicherheit im europäischen Finanzsektor sowie der Einbeziehung von kritischen, auch außerhalb der EU ansässigen, IKT-Drittdienstleister enthält DORA wesentliche Maßnahmen, um regulatorische Fragmentierung zur reduzieren. Dennoch bleibt die Verantwortung zur Definition und Überprüfung des IKT-Risikomanagements beim Leitungsorgan des jeweiligen Finanzunternehmens (EurLex, 2022). Welche Strafen und Maßnahmen bei Nicht-Einhaltung und Verstößen der in DORA festgelegten Vorschriften durch EU-Finanzunternehmen erfolgen, sind derzeit nicht konkretisiert. Die Definition und Vergabe von Sanktionen sind weiterhin den einzelnen Mitgliedsstaaten überlassen (EurLex, 2022).

DORA ist ein Schritt in Richtung einer größeren Kongruenz zwischen wirtschaftlicher Integration und weitestgehend nationaler Sicherheitsarchitektur. Weitergehende Schritte werden aber wahrscheinlich notwendig sein.



Peer Steinbrück
Bundesfinanzminister a.D.

Kommentar: Finanzresilienz stärken – Technologischen Wandel und geopolitische Spannungen meistern

Die Debatte über die Stabilität des Finanzsystems oszilliert zwischen zwei Zuspitzungen. Der einen liegt die Zuspitzung zugrunde, dass aus der Bankenkrise 2008/2009 allenfalls völlig unzureichende Konsequenzen zur Regulierung gezogen worden seien. Die andere liegt in der Unterschätzung oder Verharmlosung nach wie vor bestehender Risiken.

Tatsächlich ist das Bankensystem durch eine Reihe von Maßnahmen, die von strengeren Kapital- und Liquiditätsstandards, sowie der Einführung einer Verschuldensquote (Leverage Ratio) für Banken über die Etablierung eines einheitlichen Mechanismus der Aufsicht über die Großbanken in der Eurozone (als erster Säule einer europäischen Bankenunion) und einen einheitlichen Mechanismus der Bankenabwicklung (der zweiten Säule) bis zu einer Bilanzbereinigung vieler Banken reichen, einiges getan worden, um das Bankensystem weitaus robuster gegen Schocks aufzustellen. Die dritte Säule einer europäischen Bankenunion mit einem gemeinsamen Einlagensicherungssystem steht aus und dürfte wegen der Widerstände gegen eine Vergemeinschaftung von Bankenverlusten eher auf die Verabschiedung gemeinsamer Standards für die nationalen Systeme der Einlagensicherung hinauslaufen. Die kritischen Stimmen, die insbesondere eine deutliche Erhöhung der Eigenkapitalquoten auf 20% bis 30% dringen, die Banken ihren Aktivitäten unterlegen sollen, verschweigen meistens die damit verbundenen massiven Auswirkungen auf die Finanzierungsfunktion der Banken für die Realwirtschaft. Der Bankenstresstest der EZB vom Juli 2023 weist immerhin aus, dass die europäischen Banken eine schwere dreijährige Rezession durchstehen würden.

Umgekehrt sind eine ganze Reihe von Risiken für die Stabilität des Finanzsystems nicht zu ignorieren und durchkreuzen jede Beruhigung, eine Krise wie 2008/2009 sei unwahrscheinlich. Die Beschwörung eines solchen Gespenstes im Zuge einer drohenden Illiquidität einiger US-Regionalbanken und der eskalierenden Probleme der Credit Suisse Anfang 2023, war allerdings eher einer schnell einsetzenden Erregungstendenz geschuldet, als substanziell begründet. In dem einen Fall handelte es sich bei steigenden Leitzinsen um ein Fristentransformationsproblem zwischen länger laufenden Forderungen und kurzfristigem Refinanzierungsbedarf und in dem anderen Fall führte das obskure Geschäftsmodell einer Bank außerhalb des Single Supervisory Mechanism der EZB zum Kollaps.

Die ernst zu nehmenden Risiken für die Stabilität des Finanzsystems liegen

- in dem sogenannten Schattenbankenmarkt, auf dem sich Hedgefonds und andere Kapitalsammelstellen außerhalb einer Finanzmarktaufsicht tummeln und inzwischen allein in der Eurozone über 30 Billionen (!) Euro bewegen,

- in einem digitalen Bankrun im Zusammenwirken von Onlinebanking und Social Media, wie er sich nach der Kommunikation der Probleme einiger US-Regionalbanken im Zuge sprunghaft gestiegener Leitzinsen erstmals darstellte und die US-Zentralbank zu massiven Liquiditätshilfen geradezu zwang,

- in der hohen Verschuldung mancher Staaten mit den spiegelbildlich hohen Anteilen von Staatsanleihen auf den Bilanzen mancher Banken, ebenso wie den mit privaten Schulden aufgeblähten Märkten, wenn man insbesondere an den Gewerbeimmobilienmarkt denkt;

- bei allen Geschäftsmodellen von Banken oder auch Pensionskassen, bei denen die Laufzeiten ihrer Forderungen und jene ihrer Schulden nicht aufeinander abgestimmt sind.

Am Anfang jeder Überlegung zur weiteren Stabilisierung des Finanzsystems steht, dass unser Wirtschaftssystem auf leistungsfähige, profitable und wettbewerbsfähige Banken angewiesen ist. Das gilt für Deutschland, in dem der Finanzsektor in einem gewissen Missverhältnis zur starken Realwirtschaft in ihrer globalen Orientierung steht, und das gilt für Europa insgesamt, dessen Bankensystem mit wenigen Ausnahmen gegenüber der Potenz und Reichweite US-amerikanischer Banken weit hinterherhinkt. Wenn von Deutschlands Abhängigkeit von Energie- und anderen Rohstoffen sowie Lieferketten und von europäischer Souveränität auch in der Technologieentwicklung die Rede ist, dann sollte eine zunehmende Abhängigkeit von den Finanzdienstleistungen US-amerikanischer Banken nicht ausgeblendet werden.

Insofern ist die Errichtung einer europäischen Kapitalmarktunion von zentraler Bedeutung. Sie würde einen entsprechend großen Verbriefungsmarkt schaffen, erhebliches Kapital grenzüberschreitend freisetzen und Kreditpotentiale öffnen, die nicht nur, aber insbesondere mit Blick auf den enormen Finanzierungsbedarf einer Klimatransformation erforderlich sind. Es spricht viel für die These, dass die Finanzierung der Klimatransformation angesichts der klammen Haushaltslage vieler EU-Mitgliedstaaten weder aus staatlichen Töpfen noch denen der EU zu bewältigen ist, sondern dass es maßgeblich auf eine Mobilisierung privaten Kapitals ankommt. Dazu und als Antwort auf den US-Finanzmarkt bedarf es einer europäischen Kapitalmarktunion. Umso bedauerlicher ist es, dass dafür die Bremsklötze immer noch nicht beseitigt werden konnten.

Die ausstehenden Antworten auf die genannten Risiken liegen in einer strengen Regulierung des Schattenbankensektors und von Geldmarktfonds, der Einführung eines Trennbankensystems, welches das risikoreichere Investmentbanking von den restlichen Geschäftsfeldern trennt, und einer Begrenzung der engen Verknüpfung zwischen Banken und den Staatsschulden ihrer Heimatländer (der sogenannte Sovereign-Bank-Nexus). Die Gefahr eines digitalen Bankruns fordert Politik und Zentralbanken auf, nach einem Abwehrmechanismus zu suchen.

Angesichts der Zeitenwende, die von Kriegen, Kriegsdrohungen, der Tendenz zu einer neuen Systemkonkurrenz zwischen autoritären Staaten und dem globalen Westen einschließlich einer Blockbildung und tendenziellen Deglobalisierung, einer Umwälzung von Gesellschaft, Wirtschaft und Medien durch die Künstliche Intelligenz sowie die Notwendigkeit einer Klimatransformation geprägt ist, unterliegt das Finanzsystem massiven externen Einflüssen. Jenseits möglicher Schocks wird der Finanzsektor allein aus dem Wandel von Investitions-, Produktions- und Konsummustern herausgefordert und zu einer hohen Anpassungsfähigkeit gezwungen.

Die Antwort in einer zunehmenden „Weltunordnung" liegt für die Politik und die Wirtschaft – wie nicht weniger für die Zivilgesellschaft insgesamt – in einer größeren Resilienz gegenüber abrupten Veränderungen und der Minimierung von „Verwundbarkeiten". Die unpopuläre, aber ehrliche Ansage der Politik sollte lauten, dass es schwieriger wird, nicht leichter.

Dr. Miriam Sinn
TIBER Cyber Team (Z 16),
Deutsche Bundesbank

Das Euro Cyber Resilienz Board für Finanzmarkt-infrastrukturen

In der sich ständig wandelnden Landschaft der Finanztechnologie und der zunehmend herausfordernden geopolitischen Lage ist die Cyberresilienz zu einem zentralen Anliegen für die Stabilität des europäischen Finanzsystems geworden. Das Euro Cyber Resilienz Board (kurz: ECRB), eine Initiative der Europäischen Zentralbank (EZB) und der nationalen Notenbanken, spielt hierbei eine entscheidende Rolle.

Das ECRB, ein Teil der Eurosystem Cyber Resilienz Strategie für Finanzmarktinfrastrukturen, fungiert als ein Forum für den Austausch von Best Practices, Wissen und Erfahrungen im Bereich der Cybersicherheit. Es bringt wichtige Akteure aus dem privaten und öffentlichen Sektor zusammen, um gemeinsame Herausforderungen zu identifizieren und kollektive Maßnahmen zu koordinieren. Für die Bundesbank, die eine zentrale Rolle im deutschen und europäischen Finanzsystem spielt, ist die Mitarbeit im ECRB von strategischer Bedeutung, da es nicht nur die Sicherheit des deutschen Finanzsystems, sondern auch die des gesamten Euro-Währungsgebiets fördert.

Der Austausch von Informationen über Cyberbedrohungen und Sicherheitsvorfälle ist ein wesentlicher Pfeiler für die Stärkung der Cyberresilienz. Aus diesem Grund hat das ECBR die Initiative CISII-EU (Cyber Information and Intelligence Sharing Initiative) ins Leben gerufen. CISII-EU zielt darauf ab, die Effektivität des Informationsaustausches zu steigern, indem es eine strukturierte Plattform für den Austausch von strategischen und operativen Cyberinformationen bietet. Durch gezielte Maßnahmen wie regelmäßige Treffen und aufbereitete Informationen fördert CISII-EU die Koordination und den Informationsfluss zwischen den Mitgliedern des ECRB und darüber hinaus.

Durch diesen Austausch können Finanzmarktinfrastrukturen von den Erfahrungen anderer lernen, ihre eigenen Sicherheitsmaßnahmen bewerten und verbessern sowie sich auf neue und sich entwickelnde Bedrohungen vorbereiten. Auch die Bundesbank bringt ihre Expertise und ihre Erfahrungen in den Informationsaustausch ein und profitiert gleichzeitig von den Erkenntnissen anderer Mitglieder. Dieser Austausch ist entscheidend, um die Resilienz gegenüber Cyberbedrohungen zu verbessern und ein sicheres Finanzumfeld in Deutschland und Europa zu gewährleisten.

Neben der bahnbrechenden Arbeit der CISII-EU Initiative engagiert sich das ECRB weiterhin aktiv in anderen Schlüsselbereichen der Cybersicherheit. Ein solcher Arbeitsstrang betrifft die Entwicklung eines Protokolls für Krisenkommunikation. In der schnelllebigen Welt der Cyberbedrohungen ist eine effektive Kommunikation während eines Sicherheitsvorfalls von entscheidender Bedeutung. Das ECRB arbeitet daran, ein Protokoll zu etablieren, das eine klare, koordinierte und zeitnahe Krisenkommunikation ermöglicht, um die Auswirkungen von Cyberangriffen zu minimieren.

Ein weiterer bedeutender Fokus liegt auf der Bewältigung von Drittparteien-Risiken („third-party risk"). In einer vernetzten Finanzlandschaft sind Institutionen oft von externen Dienstleistern abhängig, was neue Einfallstore für Cyberbedrohungen eröffnet. Das ECRB setzt sich aktiv dafür ein, Strategien und Best Practices zu entwickeln, um die Risiken im Zusammenhang mit Drittparteien zu mindern.

Diese Initiativen verdeutlichen das ganzheitliche Engagement des ECRB im Streben nach Cyberresilienz. Durch die Zusammenarbeit in verschiedenen Arbeitssträngen wie CISII-EU, Krisenkommunikation und Drittparteien-Risiken trägt das ECRB dazu bei, den europäischen Finanzsektor gegen die wachsenden Herausforderungen der Cyberwelt zu wappnen.

Trotz der Fortschritte bleiben Herausforderungen bestehen. Dazu gehören die ständige Entwicklung von Cyberbedrohungen, der Schutz sensibler Informationen und die Förderung einer Kultur des Vertrauens und der Zusammenarbeit. Die Bundesbank sieht in der Weiterentwicklung des ECRB und der Vertiefung der Zusammenarbeit eine Chance, diesen Herausforderungen effektiv zu begegnen und die Cyberresilienz weiter zu stärken.

Wolfgang Steiger
Generalsekretär,
Mitglied des Präsidiums,
Wirtschaftsrat der CDU e.V.

Wirksame Fiskalregeln als zentraler Baustein der Finanzstabilität

Vor dem Hintergrund der außergewöhnlich expansiven Geldpolitik haben massive Schulden in den letzten Jahren scheinbar ihren Schrecken verloren. Als Folge ist die globale Verschuldung auf ein unglaubliches Rekordniveau angewachsen. Das gilt nicht nur für Schwellen- und Entwicklungsländer, sondern insbesondere auch für Industrieländer. Im Anbetracht der geldpolitischen Wende - weg von der Null- und Negativzinswelt - sehen sich viele Staaten absehbar mit einer drastischen Verschärfung der Haushaltslage konfrontiert. In den USA etwa werden sich die gestiegenen Zinsen im Markt für Staatsanleihen in massive Mehrkosten zwischen einer und drei Billionen Dollar in den kommenden zehn Jahren niederschlagen.

Doch obwohl die Niedrigzinsphase zu Ende geht, negieren zahlreiche politische Akteure den Handlungsbedarf und empfehlen sogar noch höhere Staatsausgaben und Schulden. Das ist eine geradezu unverantwortliche Strategie. Schon heute stufen die Europäischen Kommission und der IWF die Schuldentragfähigkeit einiger entwickelter Länder als problematisch ein. Die Bevölkerungsalterung und ein sinkendes Potenzialwachstum können einen weiteren Schub der Sozialausgaben verursachen. Krisen und ökonomische Schocks könnten durch den nicht vorhandenen fiskalischen Handlungsspielraum dann zu tieferen Verwerfungen führen. Bereits während der Pandemie war sichtbar, dass einige hoch verschuldete Länder in der EU ohne externe EU-Garantien oder Anleihekaufprogramme der EZB kaum genug „fiscal space“ besaßen, um größere Krisenprogramme national zu finanzieren.

Wieso sind europäische und nationale Schuldenregeln in der aktuellen Debatte dennoch so verpönt? Aus unserer Sicht liegt das an zwei eklatanten Fehlannahmen der Fiskalregelkritiker, die beständig fordern, dass es doch angesichts der Herausforderungen von Klimawandel und Transformation, verteidigungspolitischer Zeitenwende und dem Zuschnappen der Demografie-Falle gerade jetzt geboten sei, endlich die selbst angelegten Ketten von Stabilitätspakt und Schuldenbremse zu sprengen und entschlossen und schuldenfinanziert Zukunft zu gestalten. Erstens wird suggeriert, dass die Schuldenregeln eine künstliche Grenze setzen, wo ansonsten keine Restriktionen bestünden. Zweitens wird unterstellt, dass mehr staatliche Ausgaben, Schulden und Interventionen für mehr Wachstum sorgen. Beide Annahmen sind keineswegs überzeugend.

ab 90%

Schuldenquote des BIP inmmt das Wachstum einer Volkswirtschaft tendenziell ab

Die ungedeckten Steuerpläne der britischen Regierung, die Premierministerin Liz Truss den Posten kosteten, sind nur ein aktuelleres Beispiel, dass kein Land einen unbegrenzten Verschuldungsspielraum besitzt. Unter anderem Rogoff / Reinhart haben zudem nachgewiesen, dass Staatsschulden ab einem gewissen Umfang zunehmend negative Auswirkungen mit sich bringen und ab einer Schuldenquote von etwa 90 Prozent des BIP das Wachstum einer Volkswirtschaft tendenziell abnimmt. Der fiskalische Handlungsspielraum zur Bewältigung von Schocks und zur Gestaltung von Zukunftsaufgaben geht verloren.

Die Aufgabe von Schuldenregeln wie dem Stabilitätspakt und der Schuldenbremse ist es, Länder eben nicht zu nah an diese Schuldengrenze rücken zu lassen.

Der Blick nach Europa zeigt in aller Deutlichkeit, dass politische Wachstumsprogramme keine Wundermittel sind und regelmäßig ihre Ziele verfehlen. Als „Hamilton-Moment", „historische Chance für Europa" und „kopernikanische Wende" wurde der EU-Wiederaufbaufonds noch vor kurzem bezeichnet. Erstmalig erhielt die EU eine eigene Verschuldungskompetenz und hunderte Milliarden sollten den EU-Staaten bei der Transformation und zum wirtschaftlichen Aufschwung helfen. Wie bei den Vorgängerprogrammen wurde die Wachstumswirkung massiv überschätzt. Nach der Finanzkrise startete Europa im Juli 2009 bereits den sogenannten „European Economic Recovery Plan." Ein Konjunkturprogramm und Stimulus von 1,5 Prozent des Bruttoinlandsproduktes, um „Millionen von Arbeitsplätzen" zu schaffen und dafür zu sorgen, dass Europa gestärkt aus der Krise kommt. Der Juncker Plan wurde kurz danach als „Investment Plan für Europa" gefeiert und hat 360 Milliarden Euro mobilisiert. Das Ergebnis all dieser Programme war niederschmetternd. Die Wachstumsraten schwach, Produktivitätssteigerungen kaum vorhanden, Investitionstätigkeiten nahmen keine Fahrt auf.

Zusätzliche Ausgaben sind also offensichtlich keineswegs ein Garant für Wachstum und auch nicht für bessere staatliche Leistungen. Eine Kernfrage ist auch die Qualität der staatlichen Ausgaben und der Abruf der Mittel – es gibt enorm viel Spielraum für „better spending", für mehr Effizienz beim Staat. Die Infrastrukturschwächen vieler Industrieländer würden meist nicht zusätzliches öffentliches Geld, sondern die Reform schwerfälliger Planungs- und Entscheidungsprozesse erfordern, so eine IMF-Studie. Auch für Themen wie Bildung und Gesundheit spielt die Höhe der Staatsausgaben im internationalen Vergleich nicht die entscheidende Rolle für gute Performanz-Indikatoren. Statt mehr Staat sollte der Fokus auf einem besseren und effizienteren Staat liegen, der sich auf seine Kernaufgaben und auf eine regelbasierte Politik konzentriert.

Erfolgsmodell Schuldenbremse

Sowohl in Deutschland als auch in der Schweiz - dem Mutterland der Schuldenbremse – hat das Regelwerk dazu beigetragen, die konjunkturellen Schwankungen und Herausforderungen der letzten krisengeprägten Jahre zu meistern. Im Kontrast mit anderen Ländern wird dies besonders deutlich. Im Jahr 2007 hatten die USA, Frankreich und Deutschland alle Staatsschuldenquoten von etwa 65 Prozent, die dann in den Folgejahren signifikant auseinanderliefen. In Frankreich und USA blieben die Ausgaben und Haushaltsdefizite auch im Aufschwung konstant auf hohem Niveau, und die Schuldenquoten explodierten bis 2020 auf 131 Prozent (USA) bzw. 118 Prozent (Frankreich). Nur in Deutschland konnte durch die Umsetzung der Schuldenbremse das Vorkrisenniveau wieder erreicht werden. Genau diese Entwicklung wird der Schuldenbremse nun jedoch zum Vorwurf gemacht, da die angeblich aufgezwungene Austerität wichtige Investitionen ausbremse. Diese Interpretation ist angesichts der Entwicklung von Ausgaben und Staatsquote schlicht nicht haltbar. Von 2010 bis 2022 sind die Gesamtausgaben der öffentlichen Hand um rund 70 Prozent (!) gestiegen. In der Dekade davor betrug der Anstieg lediglich 15 Prozent.

Geld ist heute mehr als genug da. Die Steuereinnahmen sind die höchsten, die der deutsche Staat jemals seinen Bürgern und Unternehmen abverlangt hat – das gilt absolut genauso wie relativ zum BIP. Gerade in Krisen bläht die Politik den Haushalt auf und richtet sich anschließend dauerhaft auf dem hohen Niveau ein. Es zeugt von einem ökonomischen Unverständnis von „Austerität" oder „rigider Sparpolitik" zu sprechen, wenn Staatsausgaben wieder auf ein Normalmaß zurückgefahren werden, nachdem sie in einer Krise kurzfristig sprunghaft angestiegen sind. 2019 hatten wir einen Haushalt von 350 Mrd. Euro, 2022 dann von 550 Mrd. Euro. Für 2023 und 2024 waren jeweils Haushalte über 480 Mrd. Euro vorgesehen. Der Bundesrechnungshof hat vorgerechnet, dass das tatsächlich vorgesehene Ausgabenvolumen einschließlich der Nebenetats sogar bei 539 Milliarden Euro gelegen habe. Das heißt, die Corona-induzierten Mehrausgaben wurden nicht wieder heruntergefahren. Die Politik gewöhnt sich an Sondersituationen und die Ausnahme wird zur Normalität, so dass selbst Rekordeinnahmen nicht mehr ausreichen.

Auch der Vorwurf, dass die Schuldenbremse eine Investitionsbremse sei, ist nicht haltbar. Die Nullzinsen des letzten Jahrzehnts waren für die öffentlichen Haushalte ein gewaltiges Geschenk, das gerade nicht für Investitionen genutzt wurde. Die Staatsausgaben sind unter der Schuldenbremse nicht gesunken, es wurden vielmehr die öffentlichen Investitionen durch konsumtive und redistributive Ausgaben verdrängt. Schaut man in den Klimatransformationsfonds, sieht man auch dort wenig investive Ausgaben und viele Subventionen.

In der Tat gäbe es einen erheblichen Bedarf an Investitionen in Deutschland. Wer jedoch wirklich den Investitionsstau anpacken will, der bellt mit der Schuldenbremse den vollkommen falschen Baum an. Das Volumen privater Investitionen ist etwa neunmal so hoch wie das der öffentlichen. In erster Linie gilt es deshalb, die Rahmenbedingungen für die privaten Investitionen endlich zu verbessern. Denn hier erleben wir einen atemberaubenden Abstieg, über den es kaum eine öffentliche Debatte gibt. Wir verzeichnen gerade die höchsten Nettoabflüsse von Unternehmenskapital, die es in Deutschland je gab! Im internationalen Vergleich ist die Steuerlast zu hoch, es braucht eine verlässliche Versorgung der Industrie mit bezahlbarem Strom, ebenso wie eine Verbesserung von Abschreibungsmöglichkeiten, den Abbau von Bürokratie und Regulierungshemmnissen und endlich wieder Konstanz in der Wirtschaftspolitik.

Fazit

Glaubwürdige Fiskalregeln und ihre Einhaltung sind heute angesichts der hohen Schuldenstände zur Vertrauensbildung absolut notwendig. Eine gegenläufige Politik würde dagegen destabilisierend wirken. Bei der Diskussion über die Möglichkeiten und Grenzen staatlicher Ausgabenprogramme brauchen wir mehr Ehrlichkeit und Differenzierung. Ausgaben für dringende Aufgaben wie Verteidigung, soziale Konvergenz und auch die grüne Transformation sind fraglos notwendig – sie erhöhen jedoch nicht das Wachstumspotenzial und sollten deshalb auch nicht defizitfinanziert werden. Die Gedankenspiele in Deutschland, die Schuldenbremse zu unterlaufen, lassen sich auch nicht isoliert betrachten. Sie treffen auf demografische Herausforderungen und ungeklärte Fragen zur Altersvorsorge. Sie fallen in eine Zeit, da sich die Menschen erstmals seit mehr als einer Generation ohnehin mit rasanten Preissteigerungen konfrontiert sehen. Sie treffen auf einen suspendierten EU-Stabilitätspakt und zahlreiche Forderungen, die europäische Haftungsgemeinschaft etwa über die Perpetuierung des Wiederaufbaufonds, weiter auszubauen. Die Frage, wie die Bundesregierung mit dem Bundesverfassungsgerichtsurteil zur Schuldenbremse umgeht, besitzt deshalb eine Strahlkraft, die weit über Deutschland hinausgeht.

Rechtsanwalt Prof. Dr. Joachim Wuermeling LL.M. Professor Digitales Finanzwesen an der European School of Management and Technology, Berlin; Rechtsanwalt bei der Kanzlei Allen&Overy, Frankfurt, bis Ende 2023 Mitglied des Vorstandes der Deutschen Bundesbank

Der digitale Euro: Ein neuer Anker für finanzielle Resilienz?

Finanzielle Resilienz ist nicht gerade das erste Stichwort, das bei der Diskussion um den digitalen Euro genannt wird. Und dennoch: Jenseits des Fokus der öffentlichen Debatte auf den Erhalt des Bargelds und auf die Vertraulichkeit von Zahlungsdaten eröffnet die Herausgabe des öffentlichen Geldes in digitaler Form noch viele weitreichendere Dimensionen bis hin zu finanzieller Resilienz.

In dem folgenden Beitrag wird zunächst die Funktionsweise des digitalen Euro kurz erklärt (I.). Sodann wird erörtert, welche strategischen Ziele die EU neben der Verbesserung des Zahlungsverkehrs erreichen möchte (II.). In dem folgenden Kernabschnitt wird dargelegt, wie digitales Zentralbankgeld sich auf Resilienz auswirken kann (III.), bevor schließlich auf mögliche neue Risiken durch digitales Zentralbankgeld eingegangen wird.

I. Der digitale Euro: Was ist das Neue daran?

Das Geld der Europäischen Zentralbank gibt es bisher in zwei Formen, als Banknoten und als Zentralbankguthaben für Finanzinstitutionen. Einlagen auf Bankkonten sind hingegen Ansprüche gegen Banken und kein Zentralbankgeld

Mit dem digitalen Euro wird eine dritte Art von Zentralbankgeld geschaffen. Der digitale Euro repräsentiert einen Anspruch gegen die EZB in Form eines Datenpakets. Gehalten wird der digitale Euro in einer Wallet; übertragen wird er durch einen von der EZB validierten, direkten digitalen Transfer von einer Wallet in eine andere.

Für den Aspekt der Resilienz sind folgende Unterschiede zu dem traditionellen Zentralbankgeld relevant: Erstens wird mit dem digitalen Euro ein öffentliches Zahlungsmittel im Netz verfügbar. Zuvor konnte dort nur mit Kryptowährungen wie Bitcoin oder Dollar Stable Coins wie USDC bezahlt werden. Zwar muten auch Zahlungen mit einer Kreditkarte oder PayPal digital an; jedoch wird dort die eigentliche Zahlung nicht im Netz, sondern auf den traditionellen Kontosystemen vollzogen.

Zweitens sind Transaktionen mit dem digitalen Euro autark europäisch und bedürfen keinerlei Einbindung von Dienstleistern aus anderen Teilen der Welt.

Und drittens ist der Euro in digitaler Form nicht ortsgebunden, sondern netzbasiert und deshalb im Prinzip weltweit verfügbar.

II. Verfolgt die EU mit dem digitalen Euro strategische Ziele?

Digitales Zentralbankgeld ist eine Basisinnovation, die unterschiedlichen Zielen dienen kann, z. B. der finanziellen Inklusion, wie in Schwellenländern oder der Überwachung der Bürger, wie in China.

Für die Europäische Zentralbank steht der Erhalt des staatlichen Geldes als monetärer Anker im Vordergrund. So formulierte EZB-Direktor Fabio Panetta: „Das Projekt zum digitalen Euro hatte für uns immer eine klare Priorität: die Funktion des öffentlichen Geldes im alltäglichen Zahlungsverkehr zu erhalten" (Panetta, 2023). Zugleich sollte dem Bürger ein einfaches Zahlungsmittel für die digitale Welt zur Verfügung gestellt werden. Beim Eintritt der EZB in die Vorbereitungsphase erklärte die Präsidentin Christine Lagarde: „We envisage a digital euro as a digital form of cash that can be used for all digital payments free of charge" (EZB, 2023a).

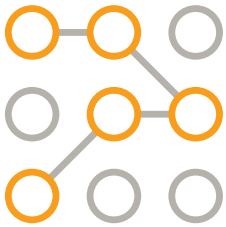
Nur am Rande und eher in Überschriftenform tauchten Gründe auf, die mit der Resilienz des Finanzsystems in Zusammenhang stehen. So begründete die Europäische Kommission ihren Verordnungsvorschlag zum digitalen Euro mit der „Aufrechterhaltung der Finanzstabilität" (Lagarde, 2022). Zudem sollte die „Widerstandsfähigkeit in einer immer stärker digitalisierten EU-Wirtschaft gefördert" (Lagarde, 2022) werden. Schließlich wird der digitale Euro auch als ein „Element der Strategie der Kommission zur Unterstützung der offenen strategischen Autonomie der EU" identifiziert (Lagarde, 2022).

III. Kann der digitale Euro zu finanzieller Resilienz beitragen?

Die Abfolge von Finanzkrisen seit Jahrhunderten hat gezeigt, dass das Finanzsystem stark verwundbar ist. Finanzielle „Resilienz" soll dem entgegenwirken, ist dabei aber eher eine programmatische Forderung als ein klar definierter Begriff. Resilienz bezeichnete ursprünglich die „Menge an externen Einflüssen, die ein Ökosystems absorbieren kann, bevor es in einen anderen Zustand wechselt." (Holling, 1973, S1. ff).

Finanzielle Resilienz ist deshalb stark mit der „Möglichkeit einer Anpassungs- und Lernfähigkeit des Finanzsystems verbunden" (Nagel, 2020). Für den Zweck dieses Artikels mag die Vorstellung ausreichen, dass jedwede Maßnahme, welche gegenwärtige Verwundbarkeiten des Finanzsystems reduziert, die finanzielle Resilienz stärkt.

Der digitale Euro adressiert drei wesentliche Verwundbarkeiten des gegenwärtigen europäischen Finanzsystems: Erstens die Disruption des staatliche Geldsystems durch Kryptoassets, zweitens die Ausfallrisiken im Zahlungsverkehr und drittens die Abhängigkeit von außereuropäischen Dienstleistern.



1. Disruption des staatlichen Geldsystems

Transaktionen jeglicher Art verlagern sich in den digitalen Raum: Finanzielle Assets oder tokenisierte Gegenstände werden auf Blockchains direkt transferiert – ohne jegliche Intermediäre. Als Gegenleistung steht dort aber staatliches Geld nicht zur Verfügung, weil es Zentralbanken bisher nur in physischer Form oder kontobasiert bereitgestellt haben. Marktmächtige Big Techs wie Facebook haben zudem versucht, mit privatem Alternativgeld das öffentliche Geldsystem herauszufordern. Verlieren aber der Staat und die Zentralbank die Hoheit über das Geld, das in Deutschland mit dem Notenbankprivileg vor 150 Jahren geschaffen wurde, ist das Vertrauen in das Finanzsystem und damit seine Funktionsfähigkeit vor allem in Krisensituationen massiv gefährdet. Als „Lender of last resort" können Zentralbanken nur Zentralbankgeld, nicht aber privates Geld zur Verfügung stellen. Die Geldmenge kann nicht mehr kontrolliert und bei weiter Verbreitung des neuen Geldes auch Inflation nicht mehr bekämpft werden.

EZB-Präsidentin Christine Lagarde formuliert es so: „In the absence of a public anchor, the emergence of new kinds of digital assets could harbour instability and confusion among citizens about what is money and what is not." (Lagarde, 2022).

Mit der Schaffung von digitalem Zentralbankgeld wie dem digitalen Euro wird die Resilienz, die staatliches Geld weltweit produziert, in den digitalen Raum übertragen. Das digitale Äquivalent der staatlichen Währung „kann die Gesellschaft auf etwas vorbereiten, das (sonst) nicht kontrolliert werden kann" (Demertzis & Martins, 2023).

2. Ausfallrisiken im Zahlungsverkehr

Eine signifikante Verwundbarkeit des Finanzsystems als Ganzes, sowie des einzelnen Marktteilnehmers ist das Risiko, dass eine initiierte Zahlungstransaktion nicht endgültig vollzogen wird. Kontobasierte Transaktionen brauchen Zeit und können scheitern, vor allem im internationalen Handel. Ganze Geschäftszweige sind tätig, diese Risiken zu minimieren oder auch zu übernehmen, ob Kreditkartenunternehmen wie Mastercard, Zahlungsdienste wie PayPal oder Korrespondenzbanken.

Die Zahlung mit dem digitalen Euro ist hingegen direkt und wird unmittelbar vollzogen. Es gibt weder einen Zeitverzug noch spielen Mittler eine Rolle, auf die man sich verlassen können muss. Die Zahlung mit dem digitalen Euro kann Zug um Zug gegen die Erbringung der Leistung erfolgen wie bei einer Bargeldzahlung.

Darüber hinaus ermöglicht ein digitaler Euro auf einer Blockchain, Zahlungen an digitale Signale wie Geodaten, die das Eintreffen einer Ware signalisieren, oder Laufzeiten von Maschinen zu knüpfen. Die Zahlung erfolgt dann automatisch, wenn das digitale Signal gesendet wird.

So können mit dem digitalen Euro Ausfallrisiken im Zahlungsverkehr aus dem Finanzsystem extrahiert werden. Das Finanzsystem wird resilienter.

Der digitale Euro soll auch ohne Netzverbindung funktionieren, durch die so genannte „Offline-Funktion." Im Falle von Nichtverfügbarkeit oder gar eines Ausfalls von Elektrizität oder Internet stünde mit dem digitalen Euro offline eine begrenzte Ausweichmöglichkeit zur Verfügung, die allerdings voraussetzt, dass sich der Zahler und der Empfänger am gleichen Ort aufhalten.

3. Internationale Abhängigkeiten

Innereuropäische Kartenzahlungen werden zu 70% von nicht europäischen Dienstleistern abgewickelt (EZB, 2023b). Das Funktionieren des Zahlungsverkehrs als Rückgrat des Handels für die Verbraucher und die Unternehmen kann somit nicht von Europa selbst sichergestellt werden. Das verursacht eine erhebliche Abhängigkeit und stellt eine signifikante Verwundbarkeit des europäischen Finanzsystems dar.

Die geopolitischen und geoökonomischen Krisen der vergangenen Jahre haben uns deutlich vor Augen geführt, welche dramatischen Folgen solche Dependenzen haben können. Im Finanzwesen führen sie nicht nur zu einer Anfälligkeit des Systems, sondern öffnen das Tor für extraterritoriale Übergriffe von Drittstaaten in innereuropäische Angelegenheiten, wie z. B. bei der Durchsetzung von Sanktionen.
Auch Störungen anderer Art in den leistungserbringenden Drittländern, seien es wirtschaftliche oder technische, auf die wir keinen Einfluss haben, beeinträchtigen die Funktionsfähigkeit der Systeme bei uns.

Die Transaktion mit einem digitalen Euro wird hingegen ausschließlich in der Eurozone vollzogen. Jedwede Zahlung an jedweden Partner in jedwedem System kann mit dem digitalen Euro ohne Einbindung eines nicht-europäischen Dienstleisters abgewickelt werden. Neben der Vereinfachung für den Verbraucher macht sich die Eurozone damit im Zahlungsverkehr unabhängiger.

Entsprechend erklärte die EZB bei dem Eintritt in die Vorbereitungsphase für die Schaffung des digitalen Euro: „It would ensure that there is a pan-European payment solution for the euro area under European governance. It would rely on its own infrastructure, thereby strengthening resilience" (EZB, 2023a).

Digitales Zentralbankgeld erleichtert insgesamt grenzüberschreitende Zahlungen und damit den internationalen Handel (Bank of England, 2023), weil Zahlungen ohne komplexe Infrastrukturen und eine Vielzahl von Intermediären direkt, sicher und kosteneffizient geleistet werden können. Wird die Abwicklung internationaler Geschäfte jedoch einfacher, sollte der Handel intensiver werden. Auch Lieferabhängigkeit können besser verringert und Diversifikation kann erleichtert werden. Auch wenn diese Wirkung indirekt ist, stärkt digitales Zentralbankgeld letztlich auch die Resilienz des globalen Wirtschaftssystems.

Kurz angesprochen werden soll hier noch eine mögliche Verringerung der Abhängigkeit Europas vom Dollar durch den digitalen Euro. Im internationalen Zahlungsverkehr liegt der Anteil der in Dollar denominierten Transaktionen mittlerweile bei fast 50 Prozent (Buchholz, 2023).

Bislang sind staatliche Währungen gebunden an den Währungsraum und können ihn – abgesehen in der Form von Bargeld - nicht verlassen. Digitales Zentralbankgeld hingegen kann überall verwandt werden, wo es ein digitales Netz gibt, also auch außerhalb des Euroraums.

Die EU-Kommission ist in ihrem Gesetzesvorschlag bei der internationalen Verwendung des digitalen Euro noch vorsichtig. Das soll nur dann möglich sein, wenn es dazu eine Vereinbarung mit dem betroffenen Drittstaat gibt (EUKOM, 2023). Deshalb könnte der digitale Euro vielleicht nicht sofort, aber doch mittelfristig einen Weg öffnen, die internationale Verwendung des Euro als Zahlungsmittel zu steigern.

Nicht umsonst haben die EU-Spitzen anlässlich des 25-jährigen Bestehens des Euro angesichts zunehmender geopolitischer Spannungen zu einer Stärkung des Euro aufgerufen. Dafür müsse die Währung fit für das digitale Zeitalter gemacht werden, auch durch die Schaffung eines digitalen Euro (Council of the EU, 2022). Entsprechend begründet die EU-Kommission ihren Gesetzesvorschlag zum digitalen Euro als ein Element "to support the EU´s open strategic autonomy" (Lagarde, 2022; Lagarde et al., 2023).

4. Neue Risiken für die Finanzresilienz?

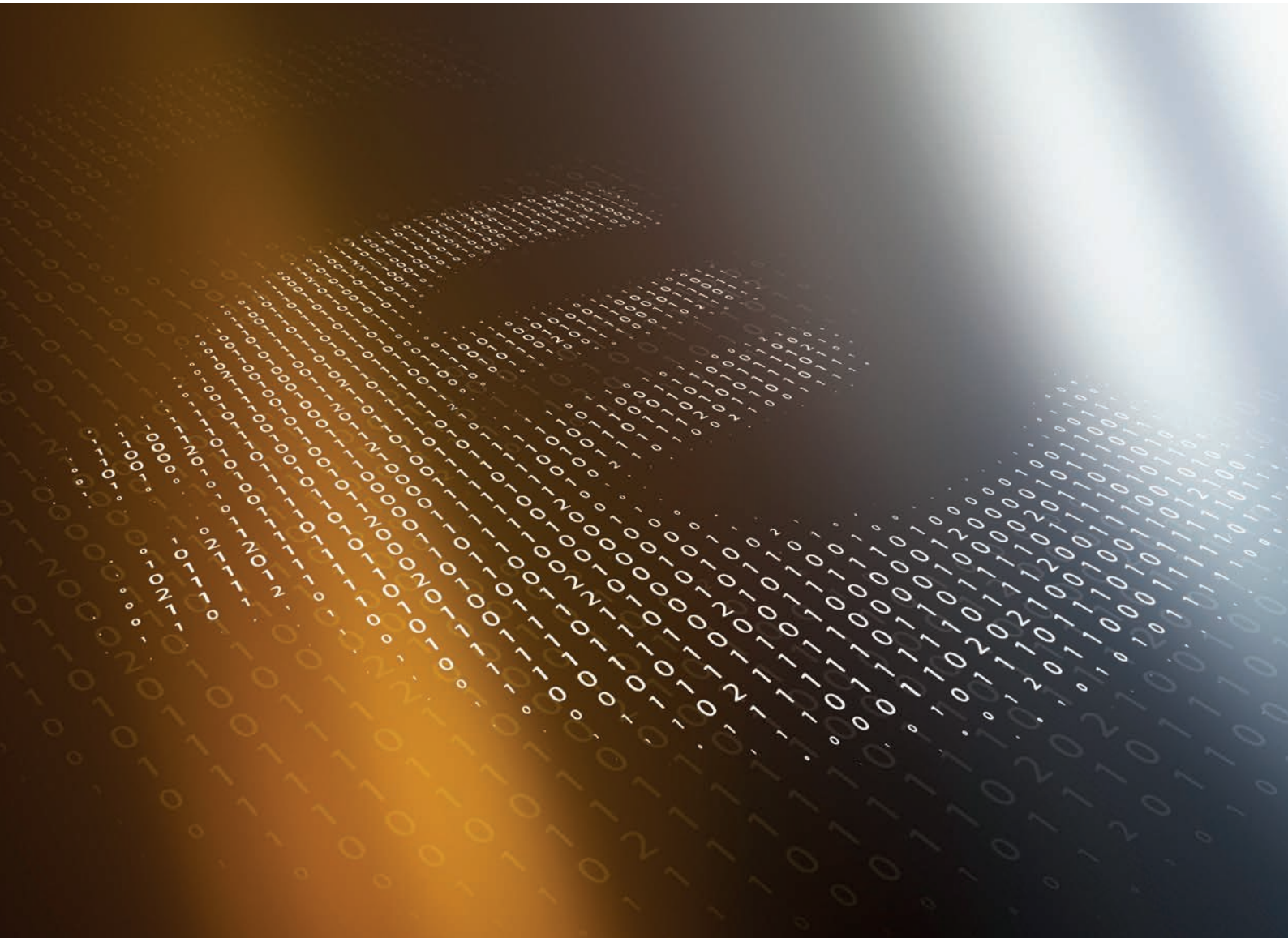
Digitales Zentralbankgeld kann für das Finanzsystem disruptive Wirkungen entfalten. Damit können auch neue Risiken für die Finanzresilienz entstehen. Diese sind bereits vielfach erörtert worden und werden hier nur kurz angeschnitten (Bofinger & Haas, 2023).

So könnten Verbraucher und Unternehmen ihre Einlagen von ihren Bankkonten abziehen und als digitale Euro in ihren Wallets halten. Damit stünden sie den Banken nicht mehr als kostengünstiges Mittel zur Refinanzierung von Krediten zur Verfügung.

In Finanzkrisen könnten die Bankkunden ihre Kontoguthaben schnell in sichere Wallets verschieben und so Liquiditätsprobleme bei den Banken auslösen. Beidem könnte durch Haltelimits für die Wallets vorgebeugt werden, wie sie EU-Kommission und EZB erwägen.

Der digitale Euro existiert nur digital und ist damit IT-Sicherheitsrisiken ausgesetzt. Das gilt allerdings für alle klassischen Bank- und Anwendungen jeder anderen Art auch. Die Verlässlichkeit der Systeme und die Cyber-Sicherheit muss überall und auch beim digitalen Euro durch adäquate Vorsorge sichergestellt werden.

Allerdings würde auch der Verzicht auf eine Digitalisierung von Zentralbankgeld Risiken mit sich bringen. Wenn andere Geldformen überhandnähmen, können die Zentralbanken nicht mehr für Preisstabilität sorgen. Die Emittenten des privaten Geldes unterlägen nicht der hiesigen Beaufsichtigung. Womöglich würde die staatliche Währung als Rechnungseinheit in Frage gestellt (Demertzis & Martins, 2023)



Fazit

Der digitale Euro kann die Finanzresilienz in dreierlei Hinsicht stärken, indem er das durch verlässliches staatliches Geld geschaffene Vertrauen in das Finanzsystems auf die digitale Finanzwelt erweitert, indem er Transaktionen des Zahlungsverkehrs sicherer macht und die Autonomie Europas stärkt. Zugleich gehen mit der Herausgabe eines digitalen Euro neue Risiken einher, die aber beherrschbar sein sollten.

3. Finanzresilienz als geopolitischer Sicherheitsfaktor?

Dr. Benedikt Franke
Stellvertretender Vorsitzender und CEO der Münchner Sicherheitskonferenz (MSC)

Kommentar: Finanzresilienz stärken – Technologischen Wandel und geopolitische Spannungen meistern

Die letzten fünf Jahre haben uns (wieder einmal) vor Augen g eführt, dass unsere liberale Ordnung und das Wirtschaftssystem, das sie ermöglicht und stützt, auf tönernen Füßen stehen. Die Pandemie, der Überfall Russlands auf die Ukraine und der Hamas auf Israel oder die Angriffe der jemenitischen Huthis auf Frachtschiffe im Golf von Aden bilden dabei nur die Spitze eines enormen Eisbergs. Die Münchner Sicherheitskonferenz (MSC) warnt seit längerem, dass wir als westliche Welt an diesem Eisberg zu zerschellen drohen, wenn wir nicht schnell besser darin werden, unsere einseitigen Abhängigkeiten zu reduzieren, unsere Schwächen zu beheben, und mehr aus unseren Vorteilen und Stärken zu machen. Gesunde Finanzen und insbesondere deren strategischer Einsatz und nachhaltiger Schutz spielen hier eine außerordentlich wichtige Rolle.

Wir haben es uns über die letzten Jahrzehnte in der Annahme bequem gemacht, dass unsere vielfältigen Abhängigkeiten uns fest in einer globalisierten Ordnung verankern und damit einen Beitrag zur internationalen Stabilität liefern. Unsere Theorie war, dass die zunehmenden Verschränkungen mit Dritten und die wachsende Anzahl an Berührungspunkten langsam aber sicher zu einer Annäherung der verschiedenen Systeme und Ideologien und damit gleichsam einem „Ende der Geschichte" führen würden. Es war für uns offensichtlich kein Problem, dass unsere Sicherheit von den USA, unsere Energie von Russland, und unsere Wirtschaft von China abhängig geworden waren, weil wir glaubten, dass die andere Seite damit jeweils auch von uns abhängig sei und damit jeder ein Interesse an der Perpetuierung des Status Quo haben sollte. Wie sehr wir daneben lagen, wissen wir nun alle. Die zunehmende Instrumentalisierung, dieser am Ende leider doch eher einseitigen Abhängigkeiten, ist zu einem enormen Risiko für Europa und insbesondere Deutschland geworden.

Es ist daher kein Wunder, dass die von Bundeskanzler Olaf Scholz attestierte und ausgerufene Zeitenwende, und die daraus geborene erste Nationale Sicherheitsstrategie, die Reduzierung dieser Abhängigkeiten zu einer Kernaufgabe der nächsten Dekade erklärt hat. Dass diese Aufgabe leichter gestellt als erledigt ist, dürfte niemanden überraschen. Wie gut wir damit aber in einigen Bereichen vorankommen, schon: Auch durch die tatkräftige Hilfe einiger Unternehmen ist es der Bundesregierung innerhalb eines Jahres gelungen, Deutschlands Abhängigkeit von russischem Öl, Gas und Kohle auf null herunterzufahren. Dass dadurch zwar die Abhängigkeit von Norwegen, Aserbaidschan und Katar auf absehbare Zeit weiter gestiegen ist, ist sicherlich wahr, dass die grüne Transformation und damit die langfristige energetische Unabhängigkeit Deutschlands dadurch massiv beschleunigt worden ist, aber auch.

Das gleiche gilt, wobei mit Einschränkungen, für unsere bisherige Abhängigkeit im Bereich der Halbleiterproduktion, in der wir zu über 90 Prozent von den Produkten einer einzigen taiwanesischen Firma abhängig geworden sind. Hier konnte durch geschickte Subventionen und anderer Incentivierungen der Bau mehrerer Produktionsstätten in Europa ermöglicht werden. Ein resilientes Finanzsystem war das Herzstück dieser, und vieler anderer notwendiger, Kurskorrekturen der letzten Jahre.

Gerade weil uns unser Finanzsystem so verlässlich durch die Krisen der letzten Jahre getragen und uns vor den schlimmsten Auswirkungen der vielen exogenen Schocks geschützt hat, gilt es, dieses System in besonderem Maße zu schützen. Dies wird aber immer schwerer. Neben den beinahe schon traditionellen Herausforderungen wie der Bedrohung aus dem Cyberraum oder der Überregulierung, sind durch die globalen Dynamiken zusätzliche Risiken entstanden, seien es zunehmende Versuche der Entdollarisierung oder die Etablierung alternativer, digitaler Währungssysteme durch die Gegner der westlichen Welt.

Unser Finanzsystem ist aber nicht nur unser bestes Schild, es eignet sich auch als Schwert im Wettstreit mit autoritären Regimen und anderen illiberalen Kräften: Richtig incentiviert erlaubt es uns, Innovationen voranzutreiben und das Rennen um Kerntechnologien zu gewinnen. Richtig abgesichert erlaubt es uns, Investitionen in Infrastruktur und Märkte, die sich zwar nicht kurzfristig auszahlen, uns aber langfristig einen großen Vorteil verschaffen. Und richtig eingesetzt, erlaubt es uns, unsere Unternehmen im globalen Wettbewerb zu stärken und es ihnen zu ermöglichen, durch ihre Investitionen wichtige Strukturveränderungen voranzutreiben und entwicklungspolitische Ziele zu erreichen, die wiederum die Stabilität der internationalen Ordnung erhöhen.

Richtig ist natürlich aber auch, dass wir nicht von Firmen und Banken erwarten dürfen, dass sie die Welt alleine retten. Diese Verantwortung liegt am Ende des Tages vor allem bei unseren politischen Entscheidungsträgern, die wir durch unsere Wahl damit beauftragt haben. Es liegt an ihnen, unser Finanzsystem zu schützen, unsere Abhängigkeiten zu erkennen und zu reduzieren, unsere Schwächen dezidiert anzugehen und das meiste aus unseren vielen Stärken und Vorteilen zu machen.

Was dazu von Nöten ist, wissen wir: Wir wissen zum Beispiel ganz genau, dass wir die ESG-Kriterien anpassen müssen, wenn wir Investitionen in unsere Verteidigungsfähigkeit nicht weiter künstlich kleinhalten wollen. Wir wissen auch, dass wir das Investitionsrisiko im Globalen Süden durch staatliche Garantien reduzieren müssen, wenn wir nachhaltige Entwicklung und die Diversifizierung unserer Absatzmärkte ermöglichen wollen. Und wir wissen, dass wir private Investitionen in die grüne Transformation unserer Industrien und Gesellschaften lenken müssen, wenn wir irgendeine Chance haben wollen, den vielfältigen Herausforderungen des Klimawandels erfolgreich begegnen zu können.

Besonders wichtig ist dabei aber, dass wir uns besser mit unseren Alliierten und Partnern abstimmen. Aktuell liegen wir oft stärker im Wettbewerb untereinander als mit unseren Rivalen und Gegnern. Der Inflation Reduction Act der Amerikaner wird von den Europäern als Wettbewerbsverzerrung verteufelt, genauso wie der Digital Markets Act der Europäischen Union amerikanischen Technologieunternehmen das Leben immer schwerer macht und damit nichtwestlichen Alternativen Tür und Tor öffnet. Solange wir uns mehr aneinander reiben als gemeinsam den wachsenden Herausforderungen und Bedrohungen zu begegnen, solange hilft uns auch eine steigende Resilienz unseres Finanzsystems nichts.

Julia Friedlander
CEO Atlantik-Brücke

Finanzen sind ein Instrument der modernen Kriegsführung

Kürzlich kursierte ein Video vom September 2022 in den sozialen Medien. Darin rät die schwedische Zentralbank der Bevölkerung, sich für den Fall einer Krise, etwa eines Krieges oder eines Cyberangriffs, mit mehreren Zahlungsmitteln einzudecken. In Schweden sind die Finanztransaktionen fast vollständig digitalisiert, sogar die Abschaffung des Bargelds ist regelmäßig im Gespräch.

In Sachen Finanztechnologie sowie bei der Einschätzung hybrider Bedrohungen sind die nordischen Länder zukunftsweisend. In einem Land mit einer schlankeren Regierung oder einer konzentrierteren wirtschaftlichen Basis – Schweden hat beispielsweise nur zehn Millionen Einwohner oder Estland gar nur etwas über als eine Million – mag die Interdisziplinarität selbstverständlich sein. Doch langsam kommt auch in größeren, komplizierteren Ländern etwas in Bewegung.

Deutschlands derzeitige Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Claudia Plattner, ist selbst ehemalige Leiterin der technischen Sicherheit bei der Europäischen Zentralbank. Für ein Land wie Deutschland, das bekanntermaßen krampfhaft an Bargeld festhält und seine Datensysteme von den Nachrichtendiensten abschottet, könnte die Ernennung ein Zeichen für eine neue, differenziertere Interpretation der Reichweite moderner Kriegsführung sein. Ein Trend, der zu begrüßen ist.

Die westlichen Finanzsysteme, sowohl ihre positiven als auch ihre negativen Seiten, gehören durchaus in das Venn-Diagramm der nationalen Sicherheit. Doch je mehr sich der internationale Sicherheitsapparat und der Finanzsektor seit der Zeit des Wirtschaftsliberalismus in den 1980er Jahren weiterentwickelt haben, desto mehr haben sie Brandmauern zwischen sich errichtet. Praktiker argumentieren, dass solche strikten Unterteilungen die Außenpolitik davor schützen, von Finanz- oder Geschäftsinteressen „korrumpiert" zu werden, oder umgekehrt, dass der private Sektor von staatlichen Eingriffen „losgelöst" bleiben kann.

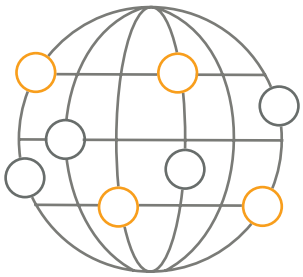
Das ist nobel, aber die viel banalere Erklärung ist, dass Institutionen im Laufe der Zeit ihre eigenen Grundprinzipien und Kulturen entwickeln. Ein Gang vom Nationalen Sicherheitsrat der USA zum Internationalen Währungsfonds – obgleich räumlich ein kurzer Spaziergang durch Washington – verwandelt sich so in einen intellektuellen Wirbelsturm. Eine derart große Wegstrecke, dass Sie Ihr Telefon ebenso gut in den Flugmodus versetzen könnten.

Doch die Ereignisse der vergangenen fünf Jahre haben diese Grenzen Stück für Stück niedergerissen.

Erstens werden die defensiven Firewalls immer höher. Der Fortschritt in der Finanztechnologie bietet viele Möglichkeiten zur Erleichterung des Handels und der persönlichen Vorlieben.

Er beinhaltet aber auch ein akutes Risiko von Cyberkriminalität und hybriden Angriffen. Die Bequemlichkeit des Bezahlens mit dem Smartphone, sei es beim Kauf einer Limonade an der Tankstelle oder gar eines Autos, hat ihre nüchterne Kehrseite: Was passiert, wenn das alles plötzlich nicht mehr funktioniert und Kunden, Unternehmen oder sogar Regierungen keinen Zugang mehr zu Geldmitteln haben?

Finanzielle Hardware ist vergleichbar mit unterirdischen Seekabeln oder Telekommunikation: Sie sind physische Eckpfeiler der nationalen Sicherheit. Bargeld unter der Matratze oder Goldbarren im Kleiderschrank sind keine Lösung, aber es ist erstaunlich selten, wie oft das Risiko eines finanziellen Zusammenbruchs in hitzigen Debatten über den Schutz kritischer Infrastrukturen erwähnt wird. In ähnlicher Weise stellt die Entwicklung digitaler Währungen eine neue Reihe von Herausforderungen dar: ob Kryptowährungen oder von der Regierung ausgegebene digitale Zentralbankwährungen – ein Bereich, der nicht zufällig auch von den Schweden und, was noch besorgniserregender ist, von den Chinesen beherrscht wird.



Das zweite Element ist die offensive finanzielle Kriegsführung. Seit den Anschlägen vom 11. September 2001 haben die USA und ihre Partner ihren legislativen und regulatorischen Spielraum zur Bestrafung des Verhaltens ausländischer Akteure (sei es wegen Terrorismus, Korruption oder der Invasion von Nachbarländern) mit finanziellen Mitteln stetig erweitert.

Putins Behauptung, die Maßnahme der G7-Staaten, Russlands Devisenreserven Anfang 2022 einzufrieren, sei ein kriegerischer Akt gewesen, ist eine glaubwürdige Anschuldigung, auch wenn westliche Regierungen viele Umschreibungen gefunden haben, um dies nicht zuzugeben. Die Sperrung des Zugangs zu Russlands Krediten ging jeder militärischen Unterstützung für die Ukraine voraus und sollte Russlands Kriegsmaschinerie lahmlegen und das Land noch während des Einmarsches in Echtzeit in den Bankrott treiben. Die Finanzmechanismen wurden taktisch eingesetzt, kaum hatten sich die Panzer in Bewegung gesetzt. Das war übrigens kein Einzelfall. Die jahrzehntelange finanzielle Isolierung des Irans hat viele politische Zyklen überdauert und den Ruf nach einer militärischen Intervention abgewehrt, um die Entwicklung von Atomwaffen in Teheran zu stoppen. Je mehr der Wille des Westens, gegen Assad in Syrien zu intervenieren, schwand, desto mehr westliche Sanktionen traten in Kraft. Die Liste ließe sich beliebig fortsetzen.

Doch im Zuge der kreativen Kapitalkontrollen und Sanktionsumgehungstechniken Russlands haben Analysten eine intensive Kosten-Nutzen-Analyse durchgeführt: Inwieweit führen solch umfangreiche Markteingriffe zu finanziellen und wirtschaftlichen Verzerrungen, die den strategischen Nutzen der Sanktionen überwiegen? Es gibt starke Argumente in beide Richtungen, aber eines ist klar: Finanzen sind unbestreitbar zu einem primären Instrument der modernen Kriegsführung geworden.

Kürzlich, als die Huthis mit ihren Angriffen auf Handelsflotten im Roten Meer begannen und Verlader um das Kap der Guten Hoffnung schickten, setzte die Biden-Administration die Einstufung der Gruppe als terroristische Organisation wieder in Kraft, ein Schritt, der – im Idealfall – Finanzinstitutionen daran hindern sollte, mit dem Jemen Geschäfte zu machen.

Damit sollte unterbunden werden, dass militärische Maßnahmen jenseits von Luftangriffen notwendig werden. Man bediente sich einfach der Finanzwirtschaft als Akteur in der Kriegsführung.

Der dritte Faktor ist der strategische Vorteil eines globalen Finanzsystems, das überwiegend von westlichen Institutionen und Währungen verwaltet und reguliert wird. Es wäre eine Fehleinschätzung, dass die Amerikaner die Hauptprofiteure sind, wie manche behaupten. Als der französische Präsident Valéry Giscard d'Estaing 1965 beklagte, dass die USA das „exorbitante Privileg" des US-Dollars als führende Reservewährung genössen, war der Euro noch eine ferne Hoffnung. Heute dominieren die G7-Währungen weiterhin sowohl die Emission von Schulden als auch die Abwicklung internationaler Transaktionen. Doch in einer Ära der chinesischen „Schuldenfallen-Diplomatie" hat sich die Fähigkeit, Kredite zu vergeben, schnell zu einer Arena des internationalen Wettbewerbs entwickelt. Große Volkswirtschaften stärkt das, aber auch schwächere Empfängerländer bekommen so eine Wünschelrute in die Hand, um souveräne Gläubiger und internationale Kreditinstitute gegeneinander auszuspielen und bessere Konditionen zu erhalten. Das Gleichgewicht verschiebt sich.

Bei der Kreditvergabe geht es schließlich nicht nur um die Bilanz eines Landes, sondern oft auch um den Zugang zu natürlichen Ressourcen oder Sicherheitsvorkehrungen. Und für die kreditgebenden Länder ist die Fähigkeit, Kredite aufzunehmen und Kapital zu beschaffen, ebenfalls zu einer Herausforderung geworden. Nachdem Jahrzehnte lang unzureichend in die Infrastruktur, den technologischen Fortschritt und die Energiewende investiert wurde, sind höhere Zinsen und eingeschränkte Kapitalmärkte in Europa zu einer strategischen Herausforderung für einige der wohlhabendsten Volkswirtschaften der Welt geworden. Diese erkennen nun, dass es sich kaum noch lohnt, mitzuhalten. In diesem Sinne ist die bisherige Unfähigkeit der EU, eine effektive Kapitalmarktunion zu schaffen und internationale Investitionen anzulocken, wahrscheinlich der größte selbstverschuldete Nachteil für ihre strategische Wettbewerbsfähigkeit.

Die Bretton-Woods-Institutionen, wie der IWF und die Weltbank, wurden gleichzeitig mit dem Sicherheitsrahmen der Nachkriegszeit gegründet. Damals sahen die Architekten der internationalen Finanzinstitutionen den Dollar als wichtigsten globalen Stabilisator an, genauso wie die Vereinten Nationen als Vermittler in der Politik. Konzeptionell gab es nur wenige Brandmauern zwischen der militärischen und der finanziellen Welt. Auch wenn heute gelegentlich gefordert wird, eine „Wirtschafts-NATO“ zu schaffen, um die westlichen Volkswirtschaften vor Raubzügen Chinas zu schützen, oder die Nutzung westlicher Technologie für militärische Zwecke einzudämmen, so ist der Schutz der Finanzinfrastruktur heute vielleicht genauso wichtig wie die territoriale Verteidigung.

Ob es nun darum geht, die physische Infrastruktur zu sichern, in Kriegszeiten Finanzsanktionen zu verhängen oder die Kapital- und Kreditmärkte zu stützen – es ist unbestreitbar, dass das Finanzwesen mit der Sicherheitspolitik eng verflochten ist. Und langsam werden sowohl Regierungen als auch die Wirtschaft wach.

QUELLENVERZEICHNIS

1. AI Safety Summit (2023), „AI Safety Summit Hosted by the UK", AI Safety Summit, https://www.aisafetysummit.gov.uk/
2. Bank of England (2023), „The Digital Pound: A New Form of Money for Households and Businesses?", Bank of England and HM Treasury
3. BKA (2023), „Bundeslagebild Cybercrime 2022", Bundeskriminalamt, https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html
4. Bofinger P. und Haas T. (2023), „The Digital Euro (CBDC) as a Monetary Anchor of the Financial System", SUERF Policy Note, 309
5. BSI (2023), „Die Lage der IT-Sicherheit in Deutschland 2023", Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410
6. Buchholz K. (2023), „U.S. Dollar Defends Role as Global Currency", Statista, https://www.statista.com/chart/30838/share-us-us-dollar-in-global-economy-global-financial-transactions/
7. Council of the EU (2022), „Council Adopts Conclusions on Strategic Autonomy of the European Economic and Financial Sector", Council of the EU, https://www.consilium.europa.eu/en/press/press-releases/2022/04/05/council-adopts-conclusions-on-strategic-autonomy-of-the-european-economic-and-financial-sector/
8. Demertzis M. and Martins C. (2023), „The Value Added of Central Bank Digital Currencies: A View from the Euro Area", Bruegel Policy Brief, 13(23): 1-19
9. Demertzis M. and Wolff G. (2020), „Hybrid and Cyber Security Threats and the EU's Financial System", Journal of Financial Regulation, 6(2): 306-316
10. Deutsche Bundesbank (2023), „Digital euro: Eurosystem moves to the next phase", Deutsche Bundesbank, https://www.bundesbank.de/en/tasks/topics/digital-euro-eurosystem-moves-to-the-next-phase-912766#:~:text=The%20digital%20euro%20project%20was,%2C%20based%20on%20users'%20needs
11. DeVon C. (2023), „Paypal is diving deeper into crypto by launching its own stablecoin – what investors should know", CNBC, https://www.cnbc.com/2023/08/10/paypal-launches-its-own-dollar-backed-stablecoin.html
12. DNBulletin (2023), „Paying with mobile as popular as cash at checkout", DeNederlandscheBank, https://www.dnb.nl/en/general-news/dnbulletin-2023/paying-with-mobile-as-popular-as-cash-at-checkout/
13. DWS (2023), „DWS, Flow Traders and Galaxy announce the intention to launch AllUnity", DWS, https://www.dws.com/en-gb/our-profile/media/media-releases/dws-flow-traders-and-galaxy-announce-the-intention-to-launch-allunity/
14. Edwards J. (2023), „Bitcoin's Price History", Investopedia, https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp
15. ENISA (2023), „Ad-Hoc Working Group on Artificial Intelligence Cybersecurity", European Union Agency for Cybersecurity, https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence/ad-hoc-working-group
16. EUKOM (2023), „Verordnung des Europäischen Parlaments und des Rates zur Einführung des Digitalen Euro", Europäische Kommission, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52023PC0369
17. EurLex (2022), „Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011", EUR-Lex
18. EZB (2023a), „Eurosystem Proceeds to Next Phase of Digital Euro Project", EZB, https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr231018~111a014ae7.en.html
19. EZB (2023b), „The EU's Open Strategic Autonomy from a Central Banking Perspective", EZB, 311: 1-189
20. Greenberg A. (2016), „Hackers Fool Tesla S's Autopilot to Hide and Spoof Obstacles", WIRED, https://www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles/
21. Herpig S. (2020), „Understanding the Security Implications of the Machine-Learning Supply Chain", Transatlantic Cyber Forum

22. Herpig S. (2023), „Mehr Resilienz für Deutschlands IT-Systeme", Tagesspiegel Background: Cybersecurity, https://background.tagesspiegel.de/cybersecurity/mehr-resilienz-fuer-deutschlands-it-systeme
23. Hiscox (2023), „Hiscox Cyber Readiness Report 2023", Hiscox
24. Holling C.S. (1973), „Resilience and Stability of Ecological Systems", Annual Review of Ecology and Systematics, 4: 1-23; zitiert nach Behringer, Finanzielle Resilienz, KSI 4/20, S. 155
25. Jones M. (2023), „Study shows 130 countries exploring central bank digital currencies", Reuters, https://www.reuters.com/markets/currencies/study-shows-130-countries-exploring-central-bank-digital-currencies-2023-06-28/
26. Kriptomat (2024), „Bitcoin Kurs", Kriptomat, https://kriptomat.io/de/kryptowaehrungen-kurse/bitcoin-btc-kurs/#:~:text=Der%20Marktrang%20von%20Bitcoin%20ist,BTC%20Kurs%20ist%2051.30%20%E2%82%AC
27. Lagarde C. (2022), „Digital Euro: A Common European Project", EZB, https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp221107~dcc0cd8ed9.en.html
28. Lagarde C., Donohoe P., Metsola R., Michel C., von der Leyen U. (2023), „Euro at 25: The Value of Unity in a Changing World", EZB, https://www.ecb.europa.eu/press/blog/date/2023/html/ecb.blog231230~23675beac3.en.html#:~:text=25%20years%20ago%2C%20on%201,million%20people%20in%2020%20countries.
29. Liu Y., Deng G., Xu Z., Li Y., Zheng Y., Zhang Y., Zhao L., Zhang T., Liu Y. (2023), „Jailbreaking ChatGPT via prompt Engineering: An Empirical Study", arXiv
30. Nagel S. (2020), „Stabilität und Resilienz des Finanzmarkts", In: Nachhaltigkeit und Finanzmarkt, Wirtschaft + Gesellschaft, Springer VS, Wiesbaden
31. Nakamoto S. (2008), „Bitcoin: A Peer-to-Peer Electronic Cash System", Bitcoin.de, https://www.bitcoin.de/de/bitcoin-whitepaper-deutsch
32. Nasr M., Carlini N., Hayase J., Jagielski M., Feder Cooper A., Ippolito D., A. Choquette-Choo C., Wallace E., Tramer F., Lee K. (2023), „Extracting Training Data from ChatGPT", arXiv
33. NCSC and CISA (2023), „Guidelines for Secure AI System Development", UK National Cyber Security Centre & US Cybersecurity and Infrastructure Security Agency, https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf
34. NIST (2024), „Cyber Resiliency", Computer Security Resource Center, https://csrc.nist.gov/glossary/term/cyber_resiliency
35. Panetta F. (2023), „Der digitale Euro: unser Geld, egal wo und wann wir es brauchen", EZB, https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230123~2f8271ed76.de.html
36. Partz H. (2023), „India in 'no hurry' for CBDC as digital rupee pilot onboards 50K users", Cointelegraph, https://cointelegraph.com/news/india-in-no-hurry-for-cbdc-as-digital-rupee-pilot-onboards-50k-users
37. Reuters (2023), „Brazil central bank names its digital currency 'DREX', scheduled for 2024 launch", Reuters, https://www.reuters.com/technology/brazil-central-bank-names-its-digital-currency-drex-scheduled-2024-launch-2023-08-07/
38. Skylight Cyber (2019), „Cylance, I Kill You", Skylight Cyber, https://skylightcyber.com/2019/07/18/cylance-i-kill-you/
39. SonicWall (2023), „Sonicwall Cyber Threat Report: Tracking Cybercriminals into the Shadows", SonicWall
40. Verizon (2023), „Data Brech Investigations Report", Verizon
41. Vincent J. (2016), „Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day", The Guardian, https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racistGreenberg A. (2016), „Hackers Fool Tesla S's Autopilot to Hide and Spoof Obstacles", WIRED, https://www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles/
42. Herpig S. (2020), „Understanding the Security Implications of the Machine-Learning Supply Chain", Transatlantic Cyber Forum
43. Herpig S. (2023), „Mehr Resilienz für Deutschlands IT-Systeme", Tagesspiegel Background: Cybersecurity, https://background.tagesspiegel.de/cybersecurity/mehr-resilienz-fuer-deutschlands-it-systeme
44. Hiscox (2023), „Hiscox Cyber Readiness Report 2023", Hiscox
45. Holling C.S. (1973), „Resilience and Stability of Ecological Systems", Annual Review of Ecology and Systematics, 4: 1-23; zitiert nach Behringer, Finanzielle Resilienz, KSI 4/20, S. 155
46. Jones M. (2023), „Study shows 130 countries exploring central bank digital currencies", Reuters, https://www.reuters.com/markets/currencies/study-shows-130-countries-exploring-central-bank-digital-currencies-2023-06-28/

47. Kriptomat (2024), „Bitcoin Kurs", Kriptomat, https://kriptomat.io/de/kryptowaehrungen-kurse/bitcoin-btc-kurs/#:~:text=Der%20Marktrang%20von%20Bitcoin%20ist,BTC%20Kurs%20ist%2051.30%20%E2%82%AC
48. Lagarde C. (2022), „Digital Euro: A Common European Project", EZB, https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp221107~dcc0cd8ed9.en.html
49. Lagarde C., Donohoe P., Metsola R., Michel C., von der Leyen U. (2023), „Euro at 25: The Value of Unity in a Changing World", EZB, https://www.ecb.europa.eu/press/blog/date/2023/html/ecb.blog231230~23675beac3.en.html#:~:text=25%20years%20ago%2C%20on%201,million%20people%20in%2020%20countries.
50. Liu Y., Deng G., Xu Z., Li Y., Zheng Y., Zhang Y., Zhao L., Zhang T., Liu Y. (2023), „Jailbreaking ChatGPT via prompt Engineering: An Empirical Study", arXiv
51. Nagel S. (2020), „Stabilität und Resilienz des Finanzmarkts", In: Nachhaltigkeit und Finanzmarkt, Wirtschaft + Gesellschaft, Springer VS, Wiesbaden
52. Nakamoto S. (2008), „Bitcoin: A Peer-to-Peer Electronic Cash System", Bitcoin.de, https://www.bitcoin.de/de/bitcoin-whitepaper-deutsch
53. Nasr M., Carlini N., Hayase J., Jagielski M., Feder Cooper A., Ippolito D., A. Choquette-Choo C., Wallace E., Tramer F., Lee K. (2023), „Extracting Training Data from ChatGPT", arXiv
54. NCSC and CISA (2023), „Guidelines for Secure AI System Development", UK National Cyber Security Centre & US Cybersecurity and Infrastructure Security Agency, https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf
55. NIST (2024), „Cyber Resiliency", Computer Security Resource Center, https://csrc.nist.gov/glossary/term/cyber_resiliency
56. Panetta F. (2023), „Der digitale Euro: unser Geld, egal wo und wann wir es brauchen", EZB, https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230123~2f8271ed76.de.html
57. Partz H. (2023), „India in 'no hurry' for CBDC as digital rupee pilot onboards 50K users", Cointelegraph, https://cointelegraph.com/news/india-in-no-hurry-for-cbdc-as-digital-rupee-pilot-onboards-50k-users
58. Reuters (2023), „Brazil central bank names its digital currency 'DREX', scheduled for 2024 launch", Reuters, https://www.reuters.com/technology/brazil-central-bank-names-its-digital-currency-drex-scheduled-2024-launch-2023-08-07/
59. Skylight Cyber (2019), „Cylance, I Kill You", Skylight Cyber, https://skylightcyber.com/2019/07/18/cylance-i-kill-you/
60. SonicWall (2023), „Sonicwall Cyber Threat Report: Tracking Cybercriminals into the Shadows", SonicWall
61. Verizon (2023), „Data Brech Investigations Report", Verizon
62. Vincent J. (2016), „Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day", The Guardian, https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist

IMPRESSUM

Herausgegeben von:

Mastercard Representative Office Germany
Taunusanlage 9-10
60329 Frankfurt am Main
Deutschland
Vertretungsberechtigter: Dr. Peter Robejsek

Mastercard Europe ist eine Tochtergesellschaft von Mastercard Incorporated, der Holding-Gesellschaft von Mastercard. Mastercard Incorporated ist eine private Aktiengesellschaft nach US-amerikanischem Recht und berichtet an die amerikanische Börsenaufsicht (SEC).
Mastercard Europe SA
Chaussée de Tervuren 198A
B-1410 Waterloo
Belgium
Vertretungsberechtigter: Mark Barnett
R.P.M (Registre des Personnes Morales) Nivelles, 0448.038.446
Mehrwertsteuer-Identifikationsnummer Mastercard Europe SA: TVA BE 0448.038.446.