Stefan Engelbrecht, Jens Gerber, Michael Gyollai, Philipp Rosch, Cord C. Schulz, Annika Selzer

# Digitalisierung in Deutschland

## Ein Vergleich zu Südkorea und Singapur

Im Februar 2023 beschäftigten sich Führungskräfte aus der Verwaltung, der Industrie und der angewandten Forschung im Rahmen einer Feldstudie mit der Digitalisierung in Deutschland. Die in Deutschland gewonnenen Erkenntnisse zum Digitalisierungsstand wurden mit den Bestrebungen Südkoreas und Singapurs in diesem Themenfeld verglichen. Im Rahmen des vorliegenden Beitrags sollen wichtige Erkenntnisse der Feldstudie zusammengetragen und somit ein Beitrag zur politischen und gesellschaftlichen Diskussion geleistet werden.

**Stefan Engelbrecht**

Chief Security Officer, RWE AG
E-Mail: stefan.engelbrecht@rwe.com

**Jens Gerber, M.Sc. (WU)**

Nachwuchsführungskraft in der Konzernsicherheit eines DAX-Unternehmens

**Michael Gyollai**

Vertriebsleiter für die Bundebehörden in Deutschland bei der Cisco Systems GmbH
E-Mail: mgyollai@cisco.com

**Philipp Joachim Rosch (LL.M.)**

Chief Information Security Officer des Ressorts beim Bundesministerium für Bildung und Forschung
E-Mail: mail@philipp-rosch.de

**Cord C. Schulz**

Leiter des Büros, Dr. Marie-Agnes Strack-Zimmermann MdB, Vorsitzende des Verteidigungsausschusses
E-Mail:
marie-agnes.strack-zimmermann.ma01@bundestag.de

**Dr. Annika Selzer**

Abteilungsleiterin am Fraunhofer SIT und Co-Forschungsbereichskoordinatorin sowie Principal Investigator in ATHENE
E-Mail: annika.selzer@sit.fraunhofer.de

### 1 Digitalisierung in Deutschland, Südkorea und Singapur[1]

Unter dem Begriff der Digitalisierung wird die Einbeziehung digitaler Technologien in Prozesse sozialer, politischer und ökonomischer Relevanz verstanden. Ziel der Digitalisierung ist es, diese Prozesse zu verbessern, indem sie u.a. verschlankt und modernisiert, vor allem aber digitalisiert werden und somit der breiten Masse zur Verfügung stehen. So bieten z.B. eine Vielzahl von Unternehmen ihren Kunden mittlerweile bereits die Möglichkeit, ihre Kundendaten über personengebundene Zugänge in ihrem Kundenportal (z.B. nach einem Umzug) selbstständig zu ändern oder machen ihren Kunden ihre eigene Rechnungshistorie über das Kundenportal zugänglich. Auch Behörden und soziale Einrichtungen bieten Bürgern digitalisierte Prozesse an, z.B. zur Beantragung bestimmter Dokumente wie Geburtsurkunden oder die Beantragung eines Kinderbetreuungsplatzes. Für die Industrie birgt die Digitalisierung darüber hinaus u.a. die Möglichkeit, Fertigungsprozesse digital abzubilden und über diese digitalen Abbildungen („digitale Zwillinge") bereits Probleme in der Fertigungskette zu erkennen und auf diese reagieren zu können, bevor sie im realen Fertigungsprozess auftreten. Gesellschaftspolitisch bewegt sich die Digitalisierung somit zwischen den Eckpunkten der politischen Strategieentwicklung und dem gesamtgesellschaftlichen Kulturwandel.

Im Februar 2023 beschäftigten sich Führungskräfte aus der Verwaltung, der Industrie und der angewandten Forschung im Rahmen einer 15-tägigen Feldstudie mit der Digitalisierung. Ziel der Feldstudie war es, die Bestrebungen Deutschlands[2] zur Digitalisierung mit den Bestrebungen Südkoreas[3] und Singa-

1 Der Beitrag gibt die persönliche Meinung der Autoren wieder. Die Autoren danken den weiteren Teilnehmern der Feldstudie für ihre wichtigen inhaltlichen Diskussionsbeiträge, die in den vorliegenden Beitrag eingeflossen sind.

2 In Deutschland erfolgten über 10 Besuche und Fachgespräche, u.a. im Auswärtigen Amt, im Bundeskanzleramt und bei verschiedenen Branchenverbänden.

3 In Südkorea erfolgten über 10 Besuche und Fachgespräche, u.a. im Korean Institute of Foreign Affairs and National Security, in der Korean Internet & Security Agency und bei koreanischen Wirtschaftsvertretern.

purs[4] in diesem Themenfeld zu vergleichen und daraus Rückschlüsse für möglichen Handlungsbedarf in Deutschland abzuleiten. Basierend auf dieser Feldstudie gibt der vorliegende Beitrag neun konkrete Anregungen (Kapitel 2.1-2.9) für den Digitalisierungsfortschritt in Deutschland.

## 2 Erkenntnisse der Feldstudie

### 2.1 Fokus auf Usability, Informationssicherheit und Datenschutz

Deutschland sollte bei der Digitalisierung bestehender Prozesse die Nutzungsfreundlichkeit – unter Berücksichtigung von Datenschutz und Informationssicherheit by Design – in den Vordergrund stellen. Die Prozesse sollten verschlankt bzw. vereinfacht werden. Insbesondere bei der Digitalisierung behördlicher Verwaltungsprozesse sind neben einer hohen Nutzerfreundlichkeit die Bedürfnisse einzelner Benutzergruppen nach Veränderungsbegleitung zu berücksichtigen (z.B. durch Angebote von entsprechenden Schulungen, digitale Lotsen, kostenlose Nutzung von internetangebundenen Computern für die Nutzung digitaler Verwaltungsprozesse).

Bei der Digitalisierung bestehender Prozesse – sowohl innerhalb als auch außerhalb der behördlichen Verwaltung – darf die Digitalisierung der Prozesse kein Selbstzweck sein, sondern sollte sich an der Angemessenheit und dem zu erwartenden Nutzen der Umsetzung orientieren.

### 2.2 Ausbau von Bildungsangeboten

Deutschland braucht einen Ausbau von Bildungsangeboten für alle Altersgruppen, insbesondere Fachunterricht zum Erlernen des (vertieften) Umgangs mit digitalen Diensten. Nur wer sicher mit digitalen Diensten umgehen kann, wird diese nutzen wollen und ohne ungewollte Einschränkungen von Grundrechten und -Freiheiten nutzen können.

Das Angebot sollte auch entsprechende Aus- und Fortbildungen im Bereich der englischen Sprache beinhalten, insbesondere auch frühzeitige Angebote des bilingualen Unterrichts in Schulen, um eine der Verkehrssprachen der digitalen Welt zu fördern und zu verbreiten.

### 2.3 Fachkräftemangel beheben

Der in Deutschland fortbestehende Fachkräftemangel bremst die Digitalisierung aus. Zielgerichtete Aus- und Fortbildungsangebote im Bereich der Digitalisierung würden eine umfassende Ausbildung von Fachkräften ermöglichen und zur Behebung des Fachkräftemangels beitragen. Darüber hinaus sollte Deutschland danach streben, digitale Berufe und Karrieren attraktiver zu gestalten, um international wettbewerbsfähig zu bleiben. Hierzu gehören neben Flexibilität des Arbeitsortes und der Arbeitszeiten auch attraktive Vergütungsmodelle im öffentlichen Dienst. Nur wenn in- und ausländische Fachkräfte aufgrund der bestehenden (Arbeits-)Bedingungen gewillt sind, in Deutschland zu arbeiten, kann ein kontinuierlicher Zustrom zum Arbeitsmarkt erreicht werden.

### 2.4 Investition in Digitalisierung

Deutschland sollte mehr in die Digitalisierung investieren und hierbei einen Fokus auf den Ausbau der Konnektivität und moderner technologischer Infrastruktur legen. Um den heutigen Anforderungen an digitale Konnektivität und Sicherheit gerecht zu werden, benötigen wir Anreizstrukturen für Investitionen und einen stärkeren Fokus auf den Ausbau digitaler Infrastruktur. Zusätzlich ist es erforderlich, moderne Netzwerke als Herzstück für die Digitalisierung zu fördern. Hierzu zählen insbesondere die Schaffung und der Ausbau von leistungsstärkeren Breitband-Anschlüssen und von Internetzugängen in den Haushalten. Eine entscheidende Rolle spielen unter anderem Schlüsseltechnologien wie Wi-Fi 6/7, 5G/6G und der Zugang zu Daten.

Weitere Investitionen betreffen u.a. den Bereich der gezielten (längeren) Förderung von Start-Ups, die branchenabhängig einen großen Beitrag zur Förderung der Digitalisierung leisten. Es braucht eine Strategie, die mehr privates Kapital für die Wachstumsphase erschließt. Hierbei sollte das Einbringen von Wagniskapital gefördert und staatlich begünstigt werden. Auch die Forschung im Bereich der Digitalisierung – insbesondere in den o.g. Kernbereichen der Nutzungsfreundlichkeit, des Datenschutzes und der Informationssicherheit – sollte (noch) stärker gefördert werden.

### 2.5 Schaffen einer digitalen Identität

Deutschland sollte das Vertrauen in digitale Identitäten stärken sowie die technische Infrastruktur und die organisatorische Umsetzung einer digitalen Identität vorrangig sicherstellen. Die bestehenden Ansätze sollten übergreifend koordiniert und Teil einer einheitlichen Strategie werden. Ziel ist eine frühzeitige Entwicklung der notwendigen technischen Funktionalitäten und nahtlose Einbindungsoptionen in bestehende und zukünftige Produkte und Services. Es braucht einen pragmatischen Ansatz, der bestehende Nutzungsszenarien und die Bedürfnisse der Nutzerinnen und Nutzer in den Blick nimmt. Die Lösung muss sich an ihrer Nutzerfreundlichkeit, Datenschutzkonformität, (Informations-)Sicherheit, Rechtssicherheit und Wirtschaftlichkeit messen lassen.[5]

### 2.6 Informationssicherheit als integralen und gleichberechtigten Bestandteil der Digitalisierung begreifen

Deutschland sollte die Informationssicherheit nicht als Anhang zu technologischer Infrastruktur oder Digitalisierungsprojekten begreifen, sondern sie im Sinne eines umfassenden Risikomanagements in jeder Projektphase gleichberechtigt mitdenken. Die vehemente Zunahme gezielter und erfolgreicher Cyberangriffe auf Institutionen der Verwaltung, der Wirtschaft und auf den Bildungs- und Forschungsbereich sowie die enormen finanziellen Schäden, die allein durch Ransomware jedes Jahr entstehen, ma-

4 In Singapur erfolgten über 5 Besuche und Fachgespräche, u.a. in der Maritime and Port Authority of Singapore, der Cybersecurity Agency of Singapore und mit Interpol.

5 Skierka, Sachverständigenstellungnahme für die Sitzung des Bundestagsausschusses für Digitales am 04.07.2022 zum Thema „Digitale Identitäten", über: https://www.bundestag.de/resource/blob/902266/ 55d480a952db3dde1444fb21ca59b452/Skierka-data.pdf.

chen beispielhaft deutlich, dass Informationssicherheit nicht länger als ein Teilaspekt unter vielen des IT-Betriebs verstanden werden darf. Möchte Deutschland auf eine resiliente und verlässliche digitale Infrastruktur zurückgreifen, bedarf es vielmehr eines starken Informationssicherheitsmanagements, das sich sowohl durch eine umfassende Beteiligung an Digitalisierungsvorhaben als auch durch eine entsprechend einflussreiche Verortung in der jeweiligen Aufbauorganisation manifestiert.

### 2.7 Einheitliches Begriffsverständnis zur aktiven Cyberabwehr

Deutschland braucht zeitnah ein zwischen Politik, Wirtschaft, Forschung und Zivilgesellschaft vereinheitlichtes Begriffsverständnis zur aktiven Cyberabwehr. Das Verständnis des Begriffs der aktiven Cyberabwehr sollte diejenigen technischen Maßnahmen umfassen, die dazu erforderlich sind, einen akuten Cyberangriff abzuwehren und aufzuklären. Von der aktiven Cyberabwehr ist der Begriff des Hackbacks abzugrenzen. Dieser umfasst Maßnahmen, die ergriffen werden, um für einen vorangegangenen Cyberangriff Vergeltung in Form eines Cybergegenangriffs auszuüben.[6] Dieses einheitliche Verständnis ist nicht nur die Grundlage für (1) die fortgesetzte Sicherstellung eines hohen Niveaus der Cybersicherheit unter Nutzung von Maßnahmen der aktiven Cyberabwehr, die dazu führt, u.a. die Privatheit des Einzelnen zu bewahren und Kritische Infrastrukturen in Deutschland zu schützen, sondern auch die Grundlage, um (2) den gesamtgesellschaftlichen Konsens zu stärken und unbegründete Ängste und Unsicherheiten zu nehmen, die auf einem falschen Begriffsverständnis der aktiven Cyberabwehr beruhen (z.B. dass aktive Cyberabwehr Cyberracheakte darstellt).

### 2.9 Interdisziplinäres Verständnis zwischen Recht und Technik

Deutschland sollte in den Bereichen Technik und Recht ein tiefgehendes interdisziplinäres Verständnis fördern, z.B. durch spezielle Aufbaustudiengänge und Traineeprogramme. Nur ein gegenseitiges Verständnis beider Disziplinen füreinander ermöglicht es, dass Chancen und Nutzen neuer Technologien in angemessener Weise austariert werden — das Recht darf gesellschaftlichen Nutzen durch technische Entwicklung nicht aufhalten, die Technik darf nicht in unangemessener Weise in die Grundrechte und -Freiheiten der Bürger eingreifen.

### 2.10 Rechtsrahmen für die Cybersicherheitsforschung

Deutschland braucht einen klaren Rechtsrahmen für die Erforschung von Cybersicherheitslücken und die (aktive) Abwehr von Cyberangriffen. Bei der offensiven Cybersicherheitsforschung nutzen Forschende die gleichen Methoden und Werkzeuge, wie sie auch für Cyberangriffe genutzt werden. Anders als zur Nutzung für Cyberangriffe nutzen die Forschenden diese Methoden und Werkzeuge jedoch, um IT-Schwachstellen aufzuspüren und wiederum Methoden und Werkzeuge abzuleiten, mit denen diese Schwachstellen geschlossen werden können. Des Weiteren fallen Maßnahmen der aktiven Cyberabwehr unter diesen Begriff.[7]

Die in Deutschland derzeit bestehenden Rechtsnormen, die im Rahmen der offensiven Cybersicherheitsforschung beachtet werden müssen, sind nicht vor dem Hintergrund entstanden, diese spezielle Forschung zu regeln. Dies führt zu großer Rechtsunsicherheit, sodass Cybersicherheitsforschende häufig vor der Wahl stehen, entweder mit Hilfe ihrer Forschung einen wichtigen Beitrag zur Verbesserung und zum Erhalt der Cybersicherheit zu leisten oder aber gegen geltendes Recht zu verstoßen und somit Gefahr zu laufen, für ihre Tätigkeit rechtlich belangt zu werden. Vor diesem Hintergrund braucht die offensive Cybersicherheitsforschung adäquate Regeln, welche einerseits die besonderen Bedürfnisse der Forschung berücksichtigen und andererseits den verantwortungsvollen Umgang der Forschenden im Rahmen ihrer Forschung sicherstellen.[8]

## 3 Fazit

Die neun in diesem Beitrag benannten, konkreten Anregungen ergänzend seien zwei übergeordnete Erkenntnisse, die im weiteren Verlauf der Digitalisierungsbestrebungen Deutschlands in sämtlichen Bereichen mitgedacht werden sollten:

1. In Singapur und Südkorea sind die Digitalisierungsziele des Staates klar formuliert, sie sind den Bürgern bekannt und werden von diesen unterstützt. Dies scheint ein wichtiger Erfolgsfaktor für einen schnellen Digitalisierungsfortschritt zu sein. Fördernde Faktoren sind dabei ein Maß an gegenseitigem Vertrauen zwischen Staat und Bürgern sowie der erlebte (gesellschaftliche und persönliche) Mehrwert von Maßnahmen.
2. Zum anderen scheint in Singapur und Südkorea sowohl in staatlichen Einrichtungen als auch in Unternehmen ein hohes Maß an Verständnis dafür zu herrschen, dass der Digitalisierungserfolg eng mit Agilität, Kreativität, Mut und Innovationsförderung verbunden ist und hierfür die entsprechenden Bedingungen geschaffen werden müssen.

In der digitalen Weiterentwicklung sollten wir Technologien für positive Transformationen nutzen und demokratische-menschenrechtsbasierte, rechtsstaatliche Ansätze als handlungsleitenden Rahmen betrachten. Dies stützt eine offene Gesellschaft und damit eine unserer Stärken, da Meinungsvielfalt und politischer Diskurs als Korrektiv wirken, Transparenz schaffen, Missbrauch entgegenwirken und so unsere Sicherheit und Resilienz fördern.

6 Shulman/Waidner, Aktive Cyberabwehr, über: https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf.

7 Shulman/Waidner, Aktive Cyberabwehr, über: https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf.

8 Selzer/Spiecker gen. Döhmann, Warum es einen Rechtsrahmen für die offensive Cybersicherheitsforschung braucht, über: https://background.tagesspiegel.de/cybersecurity/warum-es-einen-rechtsrahmen-fuer-die-offensive-cybersicherheitsforschung-braucht.