DiDaT

Die verantwortungsvolle Nutzung
Digitaler Daten als Gegenstand
eines Transdisziplinären Prozesses

Konzeptskizzen zu den Vulnerabilitätsräumen

6. Mai 2019

Herausgegeben von
Ortwin Renn,
Roland W. Scholz und
Verena van Zyl Bulitta

IASS POTSDAM
DONAU UNIVERSITÄT KREMS
b-tu Brandenburg University of Technology Cottbus - Senftenberg
Fraunhofer FOKUS
STIFTERVERBAND

Inhaltsverzeichnis

Vorwort

In welchem Zusammenhang mit anderen Dokumenten, Arbeitsphasen und Produkten von DiDaT steht das Booklet «Konzeptskizzen»

Dieses Booklet mit der Sammlung aller **Konzeptskizzen** stellt – nach der DiDaT Broschüre (Oktober 2018) und dem DiDaT Newsletter (März 2019) – das dritte Dokument aus der ***Initiierungsphase*** des Projekts DiDaT «Verantwortungsvoller Umgang mit digitalen Daten als Gegenstand eines transdisziplinären Prozesses» dar. Die sieben Konzeptskizzen liefern erste Vorschläge zum Gegenstand, den Systemgrenzen, der Ziele, etc. in den verschiedenen Vulnerabilitätsräumen. Die Konzeptskizzen machen zusammen mit der **DiDaT Broschüre**, dem DiDaT Newsletter 01 und der auf der 1. Stakeholder Konferenz am 25. Juni 2019 vorzulegenden **Grobplanung** die Hauptprodukte der Initiierungsphase von DiDaT aus. Bis Ende des Jahres 2019 wird dann in der sogenannten ***Planungsphase*** die **Detailplanung** erstellt, die auf der 2. Stakeholderkonferenz im Januar 2020 diskutiert werden soll. Damit soll dann eine in einem diskursiven Prozess erarbeitete Arbeitsplanung für die ***Hauptphase*** vorhanden sein, in der ein **Weissbuch** zum «Verantwortungsvollen Umgang mit digitalen Daten» erstellt wird.

Weitere Informationen zur Planung finden sich in DiDaT Newsletter 01 und in Newsletter 02 (Juni 2019). Um die Ziele und die Funktion von der Konzeptskizzen Vulnerabilitätsräume besser zu verstehen, möchten wir an dieser Stelle eine zusammenfassende Formulierung der Ziele von DiDaT präsentieren, die auf dem Kickoff Meeting erarbeitet wurde.

> *Ausgehend von einer Analyse der Vulnerabilitäten, werden Möglichkeits- bzw. Options- und Handlungsräume betrachtet, die es erlauben, soziale und technologische Innovationen (einschließlich der dazu notwendigen Diskurse) für einen verantwortungsvollen Umgang mit digitalen Daten zu entwickeln und zu realisieren.*

Wer hat die Konzeptskizzen erstellt?

An der Erstellung dieser Konzeptskizzen waren rund 50 WissenschaftlerInnen und PraktikerInnen beteiligt. Ein erster Entwurf wurde von 10 Personen aus der DiDaT Steuerungsgruppe und dem gegenwärtigen Projektteam kritisch begutachtet, auf dem 1. Kickoff Meeting am 27.3.2019 von 35 Personen gemeinsam diskutiert und revidiert und danach erneut begutachtet und angepasst. Dies ist aber erst ein erster Schritt. Es wird angestrebt, eine zusätzliche Grobplanung unter Beteiligung von je zwei bis vier PraktikerInnen für jeden Vulnerabilitätsraum zu erstellen.

Mit der Erstellung der Grobplanung (die auch eine Stakeholder Analyse beinhaltet) wird sichtbar, welches Wissen (und welche WissenschaftlerInnen) und welche RepräsentantInnen von welchen Stakeholdergruppen, die verschiedenen Interessen und Kompetenzen von Praxisakteuren am besten repräsentieren, für die Hauptphase gebraucht werden. Die Arbeitsgruppen der Vulnerabilitätsräume (siehe die Graphik auf Seite 4) werden dann auf der 3. Stakeholderkonferenz im Januar 2020 mit je sechs WissenschaftlerInnen und PraktikerInnen besetzt sein.

Ortwin Renn, Roland W. Scholz, Verena van Zyl Bulitta
Potsdam und Krems, Mai 2019

Organigramm DiDaT

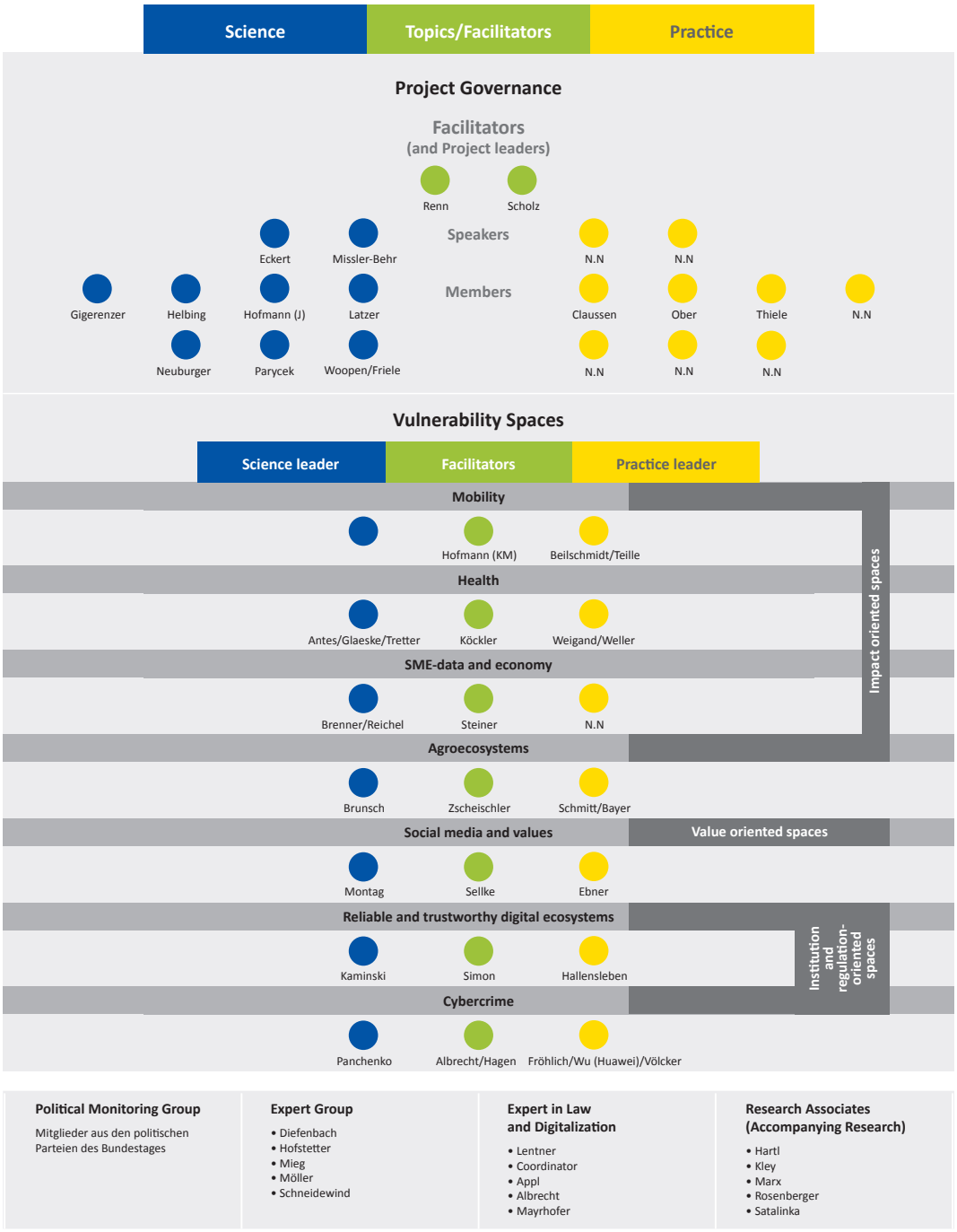


Abbildung: Organigramm von DiDaT (Stand 4.5.2019). In den Vulnerabilitätsräumen gibt es mehr Teilnehmer als in dieser Graphik (siehe z.B. die Liste der Autoren zu den Konzeptskizzen). Wir haben jeweils ein oder zwei Personen aufgeführt, die als Sprecher fungieren. Die LeiterInnen Wissenschaft und Praxis werden im Laufe des Jahres bestimmt.

01 Vulnerabilitätsraum: «Digitale Mobilitätssysteme»

Autoren: M. Hofmann (NETWORK institute), D. Beilschmidt (Deutsche Bahn), K. Teille (VW AutoUni), T. Thiele (Deutsche Bahn), W. Palmetshofer (Open Knowledge Foundation) u.a.

1. Titelvorschlag Bezeichnung/deutscher (und englischer) Titel

Vernetzte Mobilitäts-Service Systeme (Advanced Mobility Service Systems)

2. Kurzbeschreibung

Mobilität ist ein gesellschaftliches Grundbedürfnis, das unter Nutzung von Infrastruktur-Systemen durch unterschiedliche Verkehrsmittel und Dienste ermöglicht wird. Digitalisierung und Vernetzung verändern Technologien für Fahrzeuge und Infrastruktur, ermöglichen neue Marktstrukturen und Handlungsoptionen im Mobilitätsektor. Digital könnten Angebot und Nachfrage dynamisch, sicher und energieeffizient koordiniert werden. Gleichzeitig entstehen komplexe Systemabhängigkeiten und neue Marktstrukturen. DiDaT untersucht Auswirkungen auf Mobilitätsverhalten, Umwelt sowie die neuen Wertschöpfungs-Netzwerke und entwickelt Vorschläge für gesellschaftlich nachhaltige Rahmenbedingungen für die Mobilitäts-Akteure.

3. Erster Entwurf der Leitfrage (Guiding Question)

Wie können Daten zu einer nachhaltigen Systemoptimierung genutzt und individuelle, institutionelle und kommerzielle Interessen und Rechte der Marktteilnehmer ausgewogen gestaltet werden? Welche Rahmenbedingungen und Anreize sind förderlich, um bei der zunehmenden Digitalisierung des Mobilitätssektors soziale, ökonomische oder ökologische Auswirkungen aus volkswirtschaftlicher und europäischer Perspektive in Einklang zu bringen – unter Wahrung der noch zu definierenden «Privatheitsphäre»? Wie wirkt die Automatisierung der Fahrfunktion qualitativ auf die Beziehungen Mensch ↔ Maschine, Bevölkerung ↔ Umwelt und Nutzer ↔ Eigentum am Fahrzeug? Neben der Europäischen Perspektive sollen auch die mögliche Leitfunktion und Interdependenzen im globalen Markt für Fahrzeugtechnik und Mobilitätsdienste betrachtet werden.

4. Beschreibung von möglichen/wichtigen unbeabsichtigten Nebenfolgen (unseens)

Unsere Analyse mit Fragestellungen zu Auswirkungen der Digitalisierung im Mobilitätssektor fokussiert sich auf die technisch-funktionale Ebene, die soziale und personale Ebene, die rechtlich institutionelle, die ökonomische sowie die physisch-ökologische Ebene:

a. Technisch-Funktionale Ebene:

Als Folge der Digitalisierung im Mobilitätssektor könnten Plattformen zu einer Monopolbildung beitragen und damit Abhängigkeit der Nutzer/Reisenden und der öffentlichen Hand von wenigen Daten-Infrastruktur-Anbietern führen. Mangelnde europäische Aktivitäten und ein "Verschlafen" des Digitalisierungspotenzials können eine Monopolbildung zu Lasten Europas bewirken. Neben der Safety-Funktion für Fahrzeug und Nutzer ist auch die Security im digitalen und physischen Raum auf höchstem Niveau zu gewährleisten.

Die Frage des Zugangs, der Nutzung, des Eigentums und des Wertes von Daten eines Fahrzeuges oder Verkehrsteilnehmers wird zum Schlüssel für eine ökonomisch und ökologisch nachhaltige Gestaltung von Verkehrsräumen, Infrastrukturen und attraktiven und stärker automatisierten Mobilitätsangeboten sowie für die intermodale Verrechnung von Mobilitätsleistungen (Mobility as a Service, MaaS).

b. Soziale und personale Ebene:

Die Digitalisierung im Mobilitätssektor könnte zu Rebound Effekten führen wie Mehrverkehr, z.B. durch Logistik- und Leerfahrten, zu negativen Umwelteffekten und einer Verschlechterung der öffentlichen Gesundheit z.B. durch Bewegungsmangel, Lärm oder Schadstoffe. Auch personalisierte und preiswerte Mobilitätsangebote (free, flat rate) können zu negativen Auswirkungen auf Bewegung und Gesundheit führen.

Die Gestaltung von Städten als soziale Räume, Siedlungsstrukturen und die Gestaltung der öffentlichen Verkehrsräume (auch ruhender Verkehr) wirken auf Mobilitätsverhalten und Umwelt, dabei sind Formen der aktiven Mobilität zu fördern und diskriminierungsfrei in digitale Mobilitätsassistenten einzubeziehen.

Darüber hinaus sind parallel mit der Technologie Regulierungsmechanismen zu entwickeln, die Potenziale für Nachhaltigkeit der Mobilität fördern.

c. Rechtliche und institutionelle Ebene:

Anpassung Verkehrs- und Infrastrukturrecht, Schaffung eines fehlendes Rechtsrahmen für organisierten und vernetzten Individualverkehr. Die Digitalisierung der Mobilität kann durch Monitoring des Verkehrs und Überwachungen des öffentlichen Raums zur Gefahrenprävention zu einer Erosion des Datenschutzes und der Selbstbestimmung der Bürger (Datensouveränität, Mobilitäts-Souveränität) führen. Dieses Risiko erhöht sich überproportional, wenn durch Dritte oder aufgrund mangelnder Compliance die Anonymität des Verkehrsteilnehmers nicht mehr geschützt wird. Eine mobilitätsspezifische Taxonomie für «öffentliche» und «private» Daten könnte zwischen Raum, Zeit, Objekt, Kapital, Institutionen und Personendaten differenzierte Regelwerke mit spezifischen Rechten und Pflichten für Infrastrukturbetreiber, Diensteanbieter und Nutzer als sinnvoll erscheinen lassen.

d. Ökonomische Ebene:

Die mit der Digitalisierung verbundene Vernetzung im Mobilitätssektor ermöglicht den Eintritt neuer Anbieter, mit servicebasierten Geschäftsmodellen, und verändert die traditionellen Angebotsstrukturen. Ein Rückgang der Anbietervielfalt insbesondere im ländlichen Raum kann somit zu einem Verlust der zivilgesellschaftlichen Gestaltungsmöglichkeiten führen. Hier gilt es eine sinnvolle Abgrenzung von legitimen Geschäftsinteressen, individuellen Nutzungsrechten und Belangen der öffentliche Daseinsvorsorge und einen verantwortlichen Umgang mit Gemeingütern (Städte, öffentlicher Raum, Gesundheit, Mobilität??) zu finden.

e. Physische und ökologische Ebene:

Mobilität ist immer physisch und bedarf daher besonderer Schutzmechanismen für Leib und Leben (safety) die höchsten Anforderungen entsprechen. Jede Mobilität erfordert Energie, so dass Grundbedürfnisse nach Mobilität bei vollständiger Digitalisierung im Falle von Naturkatastrophen, Blackout, Terror- oder Verteidigungsfall und Ausfall der Übertragungsnetze stark eingeschränkt werden könnten.

Die Digitalisierung des Mobilitätssektors ermöglicht – wie Industrie 4.0 – eine sehr vollständige Rückverfolgung der Transporte und Mehrwertschöpfung in intermodalen Mobilitätsnetzwerken. Dies verringert den Anteil der Wertschöpfung durch den Transporteur und lokale Unternehmer und je nach Gestaltung der Nutzungsbedingungen die verfügbaren Mittel für Infrastruktur-Systeme.

5. Beschreibung der zentralen Stakeholder-Gruppen (und der gewünschten/vorgeschlagenen Repräsentant*innen)

- Öffentliche Hand (Kommunal, Ministerien, Städtetag) [z.B. FHH Hamburg, Wolfsburg]
- Verkehrs-Infrastruktur Betreiber, Telekommunikations- und Datennetze-Betreiber
- Mobilitätsanbieter, Fahrzeughersteller, Energieversorger
- Emerging Mobility Services (Car-, Ride, bike- Sharing, MDM, Plattformen)
- Umweltorganisationen, Stadtplaner, Architekten, Kommunen
- Mobilitäts-Nutzer aller Verkehrsmodi, Pendler, Berufskraftfahrer, Mobilitätseingeschränkte, Senioren, Kinder
- Konsumenten-Verbände, NGOs /alternative Sichtweisen (VCD, BUND, Open Data Vertreter…)

6. Ideen und Finanzierung zur Vertiefungsforschung in den Vulnerabilitätsräumen

Für die Gestaltung digitaler UND öffentlicher Mobilitätsräume sollten sowohl die öffentliche Hand (EU, Bund, Länder, Städtetag) als auch die die beteiligten Unternehmen im Sinne einer aktiven Rolle für Co-Finanzierung zu gewinnen sein. Es ist geplant, Szenarien zu erstellen, die Entwicklungsvarianten für Vulnerabilitätsrisiken anhand definierter Parameter (Umweltwirkung, Individualität, Automatisierung) gegenüberstellen. Für den Roll-Out der Level des automatisierten Fahrens sowie die Entwicklung von Rechten und Pflichten digitaler Subjekte erfolgen eigene szenarische Überlegungen. Auch könnten spezifische Befragungen, transdisziplinäre Workshops zu priorisierten offenen Themen und ggf. explorative (Delphi) oder vertiefende qualitative Untersuchung (mit kleinem N) zum Umgang mit schwierigen Tradeoffs benötigt und finanziert werden.

7. Auflistung der drei bis fünf „most critical problems and challenges“ in Stichworten aus der Sicht des Vulnerabilitätsraumes

(1) Welches Systemmodell legt man für den öffentlichen Verkehrsraum, Fahrzeuge und Nutzer und das entsprechenden Datenmanagement zu Grunde?
(2) Welche Bereiche des Mobilitätssektors werden mit welcher Intensität angeschaut?
(3) Kann eine Differenzierung von personen-, raum- objekt- und infrastrukturspezifischen Daten Risiken im

	Vulnerabilitätsraum reduzieren und rechtlich, auch sektor- und grenzübergreifend, sichergestellt werden? (4) Welche Rolle spielen Vernetzung und «Digitale Subjekte», die raumspezifische Entscheidungen beeinflussen/ treffen und wie kann Datenqualität und -integrität einerseits und Datensouveränität der Nutzer und Betreiber andererseits gewährleistet werden? (5) Welche kommerziellen, ethischen und technischen Auswirkungen (Unseens) damit verbunden sein können ist unklar. Wie mit diesem Punkt umgegangen wird, muss diskutiert werden.

8.	Weitere zentrale Anmerkungen/Inputs zum Kick-Off-Meeting
	Die Vorbereitung dieses Dokuments basiert auf Recherchen und Inputs u.a. vom Münchner Kreis, KIT, Mobilitätsanbietern, Herstellern, kommunalen Institutionen und Wissenschaftlern.

02 Vulnerabilitätsraum: «Gesundheit und Digitalisierung»
Autoren: Heike Köckler (HSG Bochum), Gerd Antes (Uni Freiburg), Lisa Rosenberger (Uni Wien), Felix Tretter (LMU München), Marcel Weigand (APS)

1.	Titelvorschlag Bezeichnung/deutscher (und englischer) Titel
	Gesundheit und Digitalisierung (Health and Digitalisation)

2.	Kurzbeschreibung (50 bis 80 Worte),
	Der VR Gesundheit umfasst aus einer Systemperspektive Gesundheit und Krankheit, Prävention, Gesundheits-förderung und -versorgung. Gesundheit wird entsprechend dem Verständnis der WHO als ein Zustand des vollständigen körperlichen, geistigen und sozialen Wohlergehens und nicht nur als Fehlen von Krankheit oder Gebrechen gesehen. Zentral ist hier das Verständnis eines Gesundheitskontinuums. Zentrale Akteure sind Individuen, nicht nur als Patienten und Patientinnen, in Gesundheitsberufen Tätige (insbesondere Ärzte, Therapeuten, Apotheker, Pharmazeuten, Public Healther), Krankenkassen, Unternehmen (Pharma, Medizintechnik, Abrechnungswesen, …). Digitalisierung im Bereich Gesundheit reicht von der digitalen Patientenakte, über Gesundheitsportale/-Apps bis hin zu KI-gestützter Diagnostik und therapieorientierter Robotik.

3.	Erster Entwurf der Leitfrage (Guiding Question)
	Welche negativen Auswirkungen können aus unintendierten und unerwünschte Nebenfolgen einer Digitalisierung im Gesundheitsbereich auf einzelne Menschen (Gesunde und Patient*innen), Tätige in Gesundheitsberufen, Forschende und das Gesundheitssystem mit seinen Institutionen und Organisationen im Ganzen resultieren?

4.	Beschreibung von möglichen/wichtigen nicht intendierten, unbeabsichtigten Nebenfolgen (unseens)
	Die digitale Revolution (siehe Scholz 2016)[1] kommt im Handlungsfeld Gesundheit in verschiedenen Bereichen zum Tragen. Hierzu zählen unter anderem: <u>Auf den einzelnen Menschen ausgerichtete Digitalisierungsprozesse</u> Diese orientieren sich teilweise an einer Individualisierung von Gesundheitsverantwortung und einer Optimierung im Sinne von Kosteneinsparung und individueller ökonomischer Leistungssteigerung (siehe unten). Hierbei spielen derzeit Gesundheits-Apps eine zentrale Rolle. Diese Optimierung orientiert sich nicht immer im Sinne eines Empowerment an individuellen Zielen. *Wie wird das Recht auf individuelle Entwicklung und Selbstbestimmung sichergestellt?* <u>Auf Gesundheitsberufe gerichtete Digitalisierungsprozesse</u> Eine Unterstützung von Ärzten, Therapeuten, Pharmazeuten und Laboreinrichtungen bei Diagnose, Prävention, Gesundheitsförderung und Therapie, bspw. durch Datenbanken und/oder künstlicher Intelligenz sowie ggf. Robotik. *Wie wird Qualität im Sinne einer evidenzbasierten Diagnose und Therapie, insbesondere im Kontext der künstlichen Intelligenz sichergestellt? Wer versteht und kontrolliert die Algorithmen? Welchen Einfluss haben Interessen jenseits der Evidenz (Pharmaunternehmen, …)?* <u>Auf eine ökonomische Optimierung des Gesundheitssystems gerichtete Digitalisierungsprozesse</u> Kosten im Krankenversorgungs-/Gesundheitssystem sollen durch Digitalisierung verringert werden. *Ist die Kostenersparnis im Sinne einer gesundheitsökonomischen Kalkulation belegt? Welche Wirkungen hat der Primat der Kostenreduktion?* <u>Apps als Materialisierung des Digitalisierungsprozesses</u> Die Anzahl sogenannter Gesundheits-Apps beläuft sich im Apple und Google-Play Store laut Statista auf jeweils über 1. Mio. Daher ist es wichtig, dass einheitliche Vorgaben an Qualität und Transparenz bestehen, Die Interessen für das Anbieten von Apps schließen auch Aspekte wie Kostenoptimierung (insbesondere aus der Sicht der Krankenkassen), Generierung von Daten (bspw. Internetkonzerne) oder die Werbung für eigene Produkte (Unternehmen) mit ein. *Wie wirkt sich die Nutzung von Apps auf den*

[1] Scholz, R. W. (2016). *Sustainable Digital Environments: What Major Challenges Is Humankind Facing?, Sustainability,8, 726,* http://doi.org/10.3390/su8080726

Gesundheitszustand von Individuen und die anderen Akteure des Gesundheitssystems aus? Welche Vorgaben an Qualität und Transparenz sind erforderlich und können wie umgesetzt werden?

Auf Forschungsmethodik ausgerichtete Digitalisierung

Derzeit werden Forschungsprozesse durch die Möglichkeiten der Digitalen Revolution überformt, so dass die Grundlagen einer P4 Gesundheitsforschung (predictive, personalised, preventive, participatory) vernachlässigt werden. Im Ergebnis kann dies zu epistemischen Schwächen führen, da sich bestimmte Phänomene und Prozesse nur aus analoger Sicht verstehen lassen. «*Wie wirkt sich die digitale Revolution im Hinblick auf Forschungsprozesse aus?».*

Auf Kommunikation und Austausch gerichtete Digitalisierungsprozesse

Zwischen den einzelnen Systemelementen (Individuum, Arzt/Therapeut, Dritte wie die KV, Abrechnungsstelle, Labor), findet regelmäßig Austausch von Informationen statt. Dieser wird zunehmend digitalisiert (Stichwort «Digitale Patientenakte»). Die Erhebung von persönlichen Gesundheitsdaten auf individueller Ebene, bietet Möglichkeiten Arzt- und Therapietermine intensiver zu nutzen. Allerdings stehen Sicherheit der Datenübertragung und Souveränität im Umgang mit Daten und Ergebnissen im Fokus. *Wie sind hier Datensicherheit und Recht auf informationelle Selbstbestimmung sichergestellt?* Patient*innen informieren sich eigenständig («Dr. Google», diverse Apps). Dies ersetzt teilweise die Kommunikation zwischen Gesundheitsexperten und Patienten. *Wie wird die Evidenzbasierung und Unabhängigkeit von Werbung (Pharmaindustrie, Gesundheitswirtschaft) in dieser Form der Wissensverbreitung sichergestellt? Wie wirken sich Wege der individualisierten digitalen Information auf die Gesundheitskompetenz aus?*

Auf Behandlungsmethoden ausgerichtete Digitalisierungsprozesse

An der Schnittstelle zwischen Individuum/Mensch, Therapeut/Arzt/Pharmazeut und Gesundheitssystem liegen spezifische digitale Behandlungsmethoden (von der Insulinpumpe über Apps gegen Depression oder Chats, die Behandlungsprozesse/Monitoring unterstützen und den realen Kontakt ergänzen und teilweise ersetzen). *Wie wird hier mit Datensicherheit, Eigentum an Daten, wirtschaftlichem Nutzen, Zugang und Nutzung umgegangen?*

Weiter zu berücksichtigen sind gesundheitliche Folgen der Digitalisierung als gesellschaftliches Phänomen

Macht Digitalisierung krank? Hier gibt es mehrere Synergien mit anderen Vulnerabilitätsräumen: *In welchen weiteren Bereichen hat Digitalisierung Gesundheitsbezug und unerwünschte Nebeneffekte?* Die Bearbeitung der hier skizzierten Fragen ist konsequent aus einer Systemperspektive zu beantworten. Ein Systemmodell zum Bereich Digitalisierung und Gesundheit wird in der weiteren Zusammenarbeit entwickelt.

5. Beschreibung der zentralen Stakeholder-Gruppen (und der gewünschten/ vorgeschlagenen Repräsentant*innen)

- Tätige in Gesundheitsberufen, Ärzte, Therapeuten, Pharmazeuten, Apotheker, Public Healther
- Patienten und deren Verbände
- Gesunde (Verbraucherschutz)
- Krankenkassen
- Pharmaunternehmen
- Entwickler von Gesundheitstechnologien
- …

6. Ideen und Finanzierung zur Vertiefungsforschung in den Vulnerabilitätsräumen

Ideen zur Vertiefungsforschung umfassen «case-based learning» in verschiedenen Settings und Akteurskonstellationen zur Beantwortung der oben skizzierten Fragen.

Nutzung bestehender Förderlinien, um oben skizzierten Fragen nachzugehen wären neben anderen: Innovationsfonds https://innovationsfonds.g-ba.de/; Förderlinien des BMBF; EU Horizon; Kooperation mit den wissenschaftlichen Instituten der Krankenkassen

7.	Auflistung der drei bis fünf „most critical problems and challenges“ in Stichworten aus der Sicht des Vulnerabilitätsraumes
	(1) Welches Verständnis von Gesundheit liegt zu Grunde? (2) Wie werden Datensicherheit, Eigentum an Daten, wirtschaftlicher Nutzen, Zugang und Nutzung für Individuen aber auch der in Gesundheitsberufen Tätigen gesichert?

8.	Weitere zentrale Anmerkungen/Inputs zum Kick-Off-Meeting
	Gerade in der Vorbereitung wurden Nutzen und Nebeneffekte von künstlicher Intelligenz sehr kontrovers diskutiert. Sie reichen von einer «Vergrößerung des Heuhaufens bei gleichbleibender Anzahl an Nadeln» (Antes) bis zu dem Wunsch einer breiten Anwendung der KI für eine Vielzahl an Patienten (Weigand). Der Bereich Gesundheit weist zu verschiedenen VR Räumen im DiDaT Projekt Synergien in der Bearbeitung auf. Diese gilt es noch herauszuarbeiten.

03 Vulnerabilitätsraum: SME
Autoren: G. Steiner (F), D. Baier, B. Brenner, B. Hartl, W. Hofmann, M. Missler- Behr, A. Reichel, L. Satalkina, R.W. Scholz

1	Titelvorschlag Bezeichnung/deutscher (und englischer) Titel
	Small and Medium sized enterprises (KMUs, SMEs)

2	Kurzbeschreibung (50 bis 80 Worte),
	A distinction between data-driving and data-dependent companies may help to map out vulnerabilities of SMEs. Whereas representatives within the first category are either generating, synthesizing, utilizing, interpreting, and providing data as part of their business model, the second category is mainly dependent on data (e.g., for market penetration and market strategies for their consumer goods). SMEs can easily become under danger regarding data availability, -access, and affordability in case of 'data absorption' through large companies. And operating in the cloud and utilizing cloud tools induces threats of losing control about data, (software) tools, and price dynamics.

3	Erster Entwurf der Leitfrage (Guiding Question)
	What changes and threats (unseens) of digitalization cause vulnerabilities for what type of German SME (e.g., domains of craft, commerce and industry)? What adaptive capacity (e.g., in integrative data analytics) and new competences (including security management) are needed to keep short-, mid, and long-term competitive power with large-scale firms?

4	Beschreibung von möglichen/wichtigen nicht intendierten, unbeabsichtigten Nebenfolgen (unseens)
	As established by the ERT, the relationship between ownership of data, economic value of data and use and access to data are major source of unseens [1]. Excessive use of digital data and an increasing concentration of power in the hands of a few digital hub firms have been changing competitive dynamics. Platform firms – which offer digital services to connect producers and consumers or to improve intra- and inter-organizational production processes by outsourcing process steps – have become powerful players by accumulating and exploiting data. This may offer opportunities but also cause risk. Large Industrie 4.0-based business players may show craftsman-like flexibility in production, and large platform economy services may not only be interested in trade management but offer products by themselves. The German IT branch, for instance, is a SME-shaped industry. The current transition to large cloud- platform based IT support will change the qualification of IT experts. Simplified, we may see a trend from programming to cloud tools-based design and architecture (in a similar way as the Job of an "Autoschlosser" turned to a "Automechaniker" and now to "Auto-Mechatroniker") asks for severe adaptation and new business models in many branches. This may offer opportunities but also cause risk. Large Industrie 4.0-based business players may show craftsman-like flexibility in production, and large platform economy services may not only be interested in trade management but offer products by themselves. The German IT branch, for instance, is a SME-shaped industry. The current transition to large cloud- platform based IT support will change the qualification of IT experts. Simplified, we may see a trend from programming to cloud tools-based design and architecture (in a similar way as the Job of an "Autoschlosser" turned to a "Automechaniker" and now to "Auto-Mechatroniker") asks for severe

adaptation and new business models in many branches. [2].

The surge of users in the digital environment rendered large samples possible that contain a plethora of traces of demand-side human behaviour, communication and social interactions [3] as well as supply-side production and maintenance processes along the product lifecycles [7]. Essentially mining 'big data' allows to understand individuals, groups, societies, and processes by extracting patterns and predicting real-life outcomes. Building on machine learning and analytics to predict individual action, such as consumer choice, big data analytics are going beyond analysing patterns but attempt to predict the likelihood of events [4].

For example, digital footprints tracked on social media allow for precise prediction of personality traits, digital footprints of tracked production and usage processes allow for valuable product and process improvements. This opens up novel analytics–based avenues of influencing individual opinions and/or consumer choice or to improve production. Smaller firms, who may not be able to afford computational scientists for scrutinizing their customer base may be put at a disadvantage.

Information and communication technologies are transforming data-driven innovation [5]. Traditional industrial contexts have recently been dealing with a number of digital leverages that show mutually reinforcing effects. Key technologies, such as mobile cloud computing, big data, and the internet of Things (IoT) spurred technological advances and disrupted industries. Essentially, eight technologies are considered to matter most for business, across every industry over the next three to five years, including artificial intelligence (AI), augmented reality (AR), blockchain, drones, Internet of Things (IoT), robotics, virtual reality (VR) and 3-D Printing. While these technologies continue to mature and be used in novel ways, they are also combined in new ways that might become the next wave of innovation [6]. All of these are data-driven technologies, which underscores the importance of data ownership, access and use as a basis for future competitive advantage of firms.

5 Beschreibung der zentralen Stakeholder-Gruppen (und der gewünschten/vorgeschlagenen Repräsentant*innen)

- Industrie- und Handelskammer (IHK)
- Handwerkskammer (HDK)
- KfW Mittelstandspanel (repräsentatives KMU Panel D)
- Institut für KMU-Forschung (kleine und mittlere Unternehmen in Ö)
- Betriebswirtschaftliches Forschungszentrum für Fragen der mittelständischen Wirtschaft, Bayreuth, ODER Institut für Mittelstandsforschung, Bonn (KMU in D)
- Förderkreis Gründungs-Forschung e.V., Krefeld (Startups D)

6 Ideen und Finanzierung zur Vertiefungsforschung in den Vulnerabilitätsräumen

We just want to mention two issues: The classification of vulnerabilities of branches of SME asks for an (Delphi study-based) structuring to develop smart adaptation strategies
Empirical evidence on the effects of big data on SMEs in is scarce. Based on the transdisciplinary key stakeholder conferences, questionnaires that capture potential vulnerabilities and challenges can be drafted. Systematic surveys of SMEs in cooperation with may help to gain a better and more representative picture of the challenges involved.

- Survey on Startups (i.e. based on the I2B database) and/or secondary data analysis of existing business plans

	- Joint effort with the KfW Mittelstandspanel to cover data and digitalization in the SME Panel.

7	Auflistung der drei bis fünf „most critical problems and challenges“ in Stichworten aus der Sicht des Vulnerabilitätsraumes
	SMEs but also larger enterprises need to be analyzed to adequately look for size and industry effects of data access, ownership and use. SMEs are torn back and forth: Should they digitalize their production and sales processes alongside the valuable offers of platform firms and so improve internal and external innovativeness, productivity and convenience (open model, e.g. open innovation or own digital sales channels)? Or should they avoid this usage (closed model, e.g. closed innovation or usage of platform sales channels) since this may weaken their competitiveness in the future?

8	Weitere zentrale Anmerkungen/Inputs zum Kick-Off-Meeting
	The first draft has been written by the first four authors and has been adapted, based on the feedback, e.g. of the Kickoff meeting.

1. Scholz, R., et al., *Unintended Side Effects of the Digital Transition: European Scientists' Messages from a Proposition-Based Expert Round Table.* Sustainability, 2018. **10**(6): p. 2001.
2. Van Alstyne, M.W., G.G. Parker, and S.P. Choudary, *Pipelines, platforms, and the new rules of strategy.* Harvard Business Review, 2016. **94**(4): p. 54-62.
3. Kosinski, M., et al., *Mining big data to extract patterns and predict real-life outcomes.* Psychological Methods, 2016. **21**(4): p. 493-506.
4. George, G., M.R. Haas, and A. Pentland, *Big data and management.* Academy of Management Journal, 2014. **57**(2): p. 321-326.
5. OECD, *OECD Digital Economy Outlook 2017* 2017, OECD: Paris
6. PWC *The Essential Eight - your guide to the emerging technologies revolutionizing business now*. 2018.
7. Li, L., Tao, F., Cheng, Y., Zhao, L., *Big data in product lifecycle management,* The International Journal of Advanced Manufacturing Technology, **81**, p. 667-684, 2015.

04 Vulnerabilitätsraum: «Landwirtschaft und Digitalisierung»
Autoren: J. Zscheischler (ZALF), R. Brunsch (Leibniz Institut ATB), W. Haefeker (DBIB)[2], R.W. Scholz (DUK)

1.	Titelvorschlag Bezeichnung/deutscher (und englischer) Titel
	Agrar-Ernährungskette (Agro-food system)

2.	Kurzbeschreibung
	Die Digitalisierung erzeugt wesentliche Veränderungen in der landwirtschaftlichen Produktion sowie im Verhältnis zwischen «farm and food» regional und global. Unter dem Begriff «precision agriculture» (auch Landwirtschaft 4.0) werden für landwirtschaftliche Betriebe aktuell die Unterstützung und Optimierung der technischen Steuerung sowie von Entscheidungsprozessen mittels digitaler Technologien und „Big Data“ verstanden. Dies umfasst den Pflanzenbau, die Betreibung von Gewächshäusern, die Tierproduktion und andere Bereiche der Landwirtschaft. Für die Zukunft der Landwirtschaft werden Szenarien diskutiert, die in ihren Grundannahmen und jeweiligen Auswirkungen weit auseinander gehen. Eine Möglichkeit ist, dass der aktuell zu beobachtende Trend immer größere, stärkere und breitere (auch teurere) Agrartechnik sowie weniger und größerer Betriebe sich fortsetzt. Ein anderes Szenario setzt auf die Möglichkeiten durch kleinere, intelligentere und effizientere Feldroboter. Sie ermöglichen eine an den Standort angepasste, kleinteiligere sowie auf Multifunktionalität ausgelegte Bewirtschaftung und ermöglichen auch kleineren Betrieben zu partizipieren. Die Änderungen in der Kette zwischen «farm und table» sind schwerer abzuschätzen und können unter dem Gesichtspunkt «precision nutrition» und der Optimierung von Stoffwechselprozessen («agrigenomics, nutrigenomics, nutriprotenomics, and nutrimetabolism») auch neue Märkte, Produktionsketten und industrielle Wertschöpfungsketten bilden.

3.	Erster Entwurf der Leitfrage (Guiding Question)
	Welche Auswirkungen (negative + positive) der Digitalisierung der Landwirtschaft und Lebensmittelkette auf Umwelt, sozioökonomische Systeme und eine faire Beteiligung aller beteiligten Unternehmen entlang der Lebensmittelkette (beginnend bei den bäuerlichen Klein- und Mittelbetrieben, über den Transport, die Verarbeitungsstufen bis hin zum Handel und schließlich den Konsumenten) gibt es und wird es geben? Wie muss der Rahmen gesetzt werden, um die Vorteile für Gesellschaft und Umwelt zu steigern und die Risiken zu minimieren?

4.	Beschreibung von möglichen/wichtigen nicht intendierten, unbeabsichtigten Nebenfolgen (unseens)
	Trotz unterschiedlicher Ansichten über zukünftige Entwicklungen werden für beide Zukunftstrends die Bedeutung der Datenrechte hervorgehoben. Risiken ergeben sich hier aus den möglichen Geschäftsmodellen. Dazu gehören Fragen der Erhebung, Nutzung, des Zugangs zu, des Besitz und der Sicherheit von Daten. Hier wird von den Akteuren ein wichtiger aktueller Gestaltungsraum beschrieben, der „spielentscheidend“ die weitere Entwicklung prägen wird. Noch ist offen, ob sich „offene Systeme“ (in Form von Daten-Allmenden) gegenüber den Interessen großer (möglicherweise agrarfremder und ganz neuer) Datenkonzerne (mit „geschlossenen“ Service-Angeboten) durchsetzen werden. Im Zusammenhang mit Letzterem wird auch das Risiko einer Vollautomatisierung landwirtschaftlicher Prozesse für den Landwirt thematisiert, der sich in starke Abhängigkeit und Kontrolle durch Agrarkonzerne begibt. Zugleich wird sich das Selbstverständnis der Landwirte verändern. Es gilt folgende Thesen zu diskutieren und zu überprüfen: Die Auseinandersetzung mit Fragen zur Digitalisierung in der Landwirtschaft und über die gesamte

[2] Der Vorschlag, Landwirtschaft zu einem Vulnerabilitätsraum zu machen, wurde erst nach Beginn der Initiierungsphase von Seiten des NABU unterbreitet. Nach einem Prüfprozess mit verschiedenen Schlüsselakteuren wurde auf dem Kickoff Meeting am 27. März befunden, dass der Vorschlag des NABU weiterverfolgt werden sollte.

Lebensmittelkette konzentriert sich auf die betriebswirtschaftlich ökonomische (und vornehmlich an der produzierten Biomasse orientierten) Optimierung einer industriellen Landwirtschaft von Gross-/Megabetrieben in Pflanzenbau und Tierproduktion. Dies führt (an vielen Stellen) zu einer mangelhaften Betrachtung ökosystemarer kleinräumiger ökologischer Funktionen und zu dem Verlust nachhaltiger kleinräumiger, die Artenvielfalt erhaltender landwirtschaftlicher Kleinbewirtschaftung.

Die mit der Digitalisierung verbundene zunehmende Rationalisierung der Landwirtschaft führt zu einer weiteren Abnahme landwirtschaftlicher Betriebe, einem Rückgang der Akteursvielfalt im ländlichen Raum und somit zu einem weiteren Verlust der zivilgesellschaftlichen Gestaltungskraft.

Die Digitalisierung führt zur weiteren Marktkonzentration und Monopolbildung und damit zur stärkeren Abhängigkeit des Landwirts von Agrarkonzernen. Die Frage des Besitzes, des Zugangs, der Nutzung und des Wertes von Daten eines landwirtschaftlichen Betriebes für eine ökonomisch gute und ökologisch nachhaltige Bewirtschaftung (einschliesslich der Erhebung von «Feebates» für Düngung, Pestizide, und Herbizide) kann für den Landwirt die Arbeit wesentlich erschweren.

Durch die Digitalisierung verändert sich das Qualifikationsprofil des Landwirts. Er wird zum technologieabhängigen Datenmanager, der in grosser Abhängigkeit zu digitalen, agrotechnischen und Lebensmittel produzierenden wirtschaftlichen Schlüsselakteuren steht. Das ursprüngliche, aber weiterhin wichtige, erfahrungsbasierte, direkt durch Interaktionen mit dem organismischen Boden-Pflanze-Tiersystem erworbene Wissen eines (traditionellen mittel-Europäischen) Landwirts geht verloren.

Die Digitalisierung ermöglicht – wie Industrie 4.0 – eine sehr vollständige Rückverfolgung der Erträge und Mehrwertschöpfung der landwirtschaftlichen Lebensmittelkette. Dies verringert den Anteil der Wertschöpfung durch den landwirtschaftlichen Unternehmer.

Personalisierte (DNA-Analyse-basierte) Ernährungsoptimierung entbehrt bislang (abgesehen von bestimmten, weniger gut untersuchten Krankheiten) einer ausreichenden wissenschaftlichen Grundlage. Die Kopplung von «precision nutrition»-Ansätzen mit «precision farming»-Ansätzen könnte jedoch zur einseitigen Übernutzung von Landressourcen führen.

5. Beschreibung der zentralen Stakeholder-Gruppen (und der gewünschten/vorgeschlagenen Repräsentant*innen)

- Staatliche Akteure (Verwaltung, Kontrollorgane)
  Landwirte (Verbände oder einzelne Unternehmer?)
- Agrochemische Grossbetriebe
- Landwirtschaftsmaschinen-Hersteller
- Schlüsselakteure der Lebensmittelkette (Erzeugung, Lagerung, Verarbeitung, Transport, Groß- und Einzelhandel, Verbraucher, z.B. Oetker)
- Umweltorganisationen
- Konsumenten-Verbände, alternative Sichtweisen (WWF, Oxfam)

6. Ideen und Finanzierung zur Vertiefungsforschung in den Vulnerabilitätsräumen

Die Reflektion zu «Unseens» bezogen auf die Digitalisierung der Landwirtschaft ist relevant aber kaum entwickelt. Es ist anzunehmen, dass sich die Situation in landschaftlich vergleichsweise homogenen, grossflächigen Nutzungsstrukturen im Norden/Osten anders darstellt als in landschaftlich kleingliedrigeren Systemen. Auch sind die verschiedenen Zweige der Landwirtschaft zu differenzieren.

Deshalb braucht es für alle Bereiche angemessene Systemmodelle, auf deren Grundlage sich potentielle Rebounds und «Unseens» identifizieren lassen. Dies wäre schon einmal eine Arbeit für die Planungsphase, die mit einem Papier (Grössenordnung 20k €) zu finanzieren wäre (oder als «in kind» von wissenschaftlichen oder privaten Forschungseinrichtungen durchzuführen wäre).

Die Veränderung der Produktionskette zwischen «farm and table» sind bislang wenig erforscht. In welcher Weise sie einbezogen werden wird im Verlauf der Erstellung des Grobkonzeptes in einem transdisziplinären Dialog zwischen Wissenschaft und Stakeholdern spezifiziert werden.

Welche Vertiefungsforschung in der Hauptphase zu machen wäre, ist gegenwärtig noch offen.

Es gibt hier verschiedene Möglichkeiten:

- Experten-Delphi zur Wirkung von «Unseens» auf die Ertragsfunktion des Landwirtes, die Veränderung der landwirtschaftlichen Wertschöpfungskette und die Umweltqualität

	- Formative Szenarienkonstruktion (mit den Experten und weiteren Beteiligten) über verschiedene Wege der Digitalisierung der Landwirtschaft und deren Wirkungen auf wirtschaftliche, ökomische und andere Systeme; Bewertung der Szenarien mittels multikriterieller Bewertung durch verschiedene Stakeholder-Gruppen, um Hypothesen über Wahrnehmung und Expertenurteile zu messen - Fallbezogenes Lernen: Betrachtung bestimmter Agrarprodukte oder Produktionsketten

7.	Auflistung der drei bis fünf „most critical problems and challenges“ in Stichworten aus der Sicht des Vulnerabilitätsraumes
	(1) Welches Systemmodell (Agro-ecosystem; Agro-food chain, etc.) legt man zu Grunde? (2) Welche Sektoren der Landwirtschaft werden mit welcher Intensität angeschaut? (3) Welche Rolle die Digitalisierung des Organismischen (d.h., DNA-basierte Optimierung der landwirtschaftlichen Produktion, personalisierte Ernährung als Geschäftsmodell, GMO, etc.) spielt und welche Wirkungen und «Unseens» damit verbunden sind, ist unklar. a. Wie mit diesem letzten Punkt umgegangen wird, muss diskutiert werden.

8.	Weitere zentrale Anmerkungen/Inputs zum Kick-Off-Meeting
	In der Vorbereitung dieses Dokuments wurden Telefoninterviews mit S. Ober (NABU) P.-A. Schmidt und S. Schraff (Bayer) sowie H. Paetow (DLG) geführt

05 Vulnerabilitätsraum: «Social Media and Values»
Autoren*innen: C. Montag (Uni Ulm), F. Ebner (Mecodia), H. Gleiß (Nettz); B. Köhler (Frieda Frauenzentrum/Cyberstalking)

1.	Titelvorschlag Bezeichnung/deutscher (und englischer) Titel
	Social Media und Werte; vlt. Auswirkung und Verantwortung von Social Media auf die Demokratie, Werte und Gesundheit (Impact and responsibility of social media on democracy, values and health)

2.	Kurzbeschreibung
	Social Media/Messenger Applikationen sind für viele Menschen unmittelbar mit ihrem Alltag verknüpft und haben in kurzer Zeit großen Einfluss auf Kommunikation, Marketing und demokratische Prozesse genommen. Dies wird unter anderem durch den Konzern Facebook illustriert: Facebook wurde beispielsweise erst im Jahr 2004 gegründet und zählt im März 2019 in etwa 2,3 Milliarden Nutzer. Zum Facebook Konzern gehören auch andere wichtige App-Services wie die Plattform Instagram oder der Messenger-Dienst WhatsApp. Dadurch zeigt sich auch die relative Monopolstellung von Facebook und Google.

3.	Erster Entwurf der Leitfrage (Guiding Question)
	Welche negativen Auswirkungen entstehen aus der großen Macht der Social Media Plattformen in Bereich Demokratie und (psychische) Gesundheit?

4.	Beschreibung von möglichen/wichtigen nicht intendierten, unbeabsichtigten Nebenfolgen (*unseens*)
	Themengebiet 1: Social Media und Verantwortung für Demokratie ***Systemdesign von Plattformen wie WhatsApp oder Facebook, genauso wie die Bezahlmodelle des Silicon Valley, lenken Wahrnehmung und Verhalten von Menschen.*** **Dadurch kommt es auch zum Wandel der individuellen Realitätskonstruktionen** (im Vergleich zu „traditionellen“ Realitätskonstruktionen, geprägt durch klassische Massenmedien) durch digitalisierte bzw. algorithmisierte Alltagshandlungen - und dem sich daraus ergebenden **Wandel von sozialer Ordnung** auf gesellschaftlicher Ebene Ein wirkungsmächtiger Mechanismus in diesem Wandel-Prozess kann als **Individualisierung/Personalisierung** zusammengefasst werden. Damit verbunden kann es einerseits zu **digitalen Echoräumen/Filterblasen** bzw. der Problematik von **Verzerrungen/Bias** kommen, der vermuteten **Reduktion von Vielfalt (silencing effect) in der Meinungsbildung** mit demokratiepolitischen Konsequenzen. Andererseits sind mögliche **politische und kommerzielle Manipulationen** zu beachten, die personalisiert mittels **Microtargeting** und **Social Bots** unterstützt werden. In diesem Zusammenhang ist auch die Problematik zunehmender **Desinformation** (u.a. als **Fake News** diskutiert) zu beachten. Demokratiepolitische Konsequenzen hat zudem eine **Deterritorialisierung**, etwa durch eine Entkoppelung von lokalen Werten oder in Form von globalisierten Einflussnahmen. Die voranschreitende **Datafizierung** kann nicht nur zu einer verstärkten **Kommerzialisierung von Lebensbereichen** führen; die wahrgenommenen **Datenschutzverletzungen** und ein permanentes **Überwachungsgefühl** können auch zu **Chilling Effekten** führen, zu einer Selbstzensur der **Meinungs- bzw. Kommunikationsfreiheit** mit demokratiepolitisch sensiblen Wirkungen. Auswirkungen auf die **Kommunikationsfreiheit** ergeben sich durch die spezifischen Ausprägungen der **Inhalts-Moderation** der einzelnen Anbieter sozialer Medien (algorithmisch und manuell) bzw. durch rechtliche Rahmenbedingungen etwa zu Uploadfiltern und Netwerkdurchsetzungsgesetz. Die genannten Plattformen sind Wirtschaftsunternehmen, denen es primär um Gewinnerzielung geht – dementsprechend werden auch die Algorithmen gestaltet und programmiert. Neben den hier genannten Plattformen (vor allen Dingen solche von Facebook) sei erwähnt, dass es auch an anderer Stelle demokratieschädliche Prozesse im World Wide Web gibt, die sich z. B in extremistischen Gruppen auf Discord oder auf Telegram abspielen und auf welche das NetzDG keinen Zugriff hat. In diesem Kontext ist auch die Neuausrichtung von Facebook bemerkenswert und dringend zu untersuchen, die explizit nun die Privatheit der Kommunikation stärker in den Vordergrund rücken will. Durch die *peer zu peer encyrption* wird es hier schwieriger werden, demokratiefeindliche Prozesse zu entlarven.

Themengebiet 2: Social Media und Verantwortung für (psychische) Gesundheit

Insgesamt stellt sich die Frage nach Auswirkungen auf das **Wohlbefinden**, wobei die Indikatoren vielfältig sind und u.a. auch **problematische Nutzung**, **Overuse** und **Social Pressure** inkludieren. Letzteres muss unter anderem im Kontext von sozialen Vergleichsprozessen beforscht werden, die zu negativem Affekt führen können. Besondere Vulnerabilitätsgruppen müssen herausgearbeitet werden, beispielsweise sind junge Frauen besonders anfällig für das ständig verbreitete Schönheitsbild von sehr schlanken Models. Dieses kann zu Essstörungen führen. Cybermobbing bei Jugendlichen sowie die Betroffenheit und die psychischen Auswirkungen von Hate Speech, Doxing etc. führen die Liste fort und führen u.a. zu Depressionen, Aggressionen etc.).

Dabei bieten sich auch mehrere Perspektiven an, aus welchen Maßnahmen zur Verbesserung des Well-Being/Wohlbefindens angestoßen werden können. Unter anderem die **gesellschaftliche Perspektive**, wobei die Frage gestellt werden muss, was Entscheidungsträger aus **Politik und Wirtschaft** diesbezüglich unternehmen können, wie zum Beispiel E-Mails nach Feierabend zu minimieren oder gänzlich zu unterbinden. Des Weiteren bietet sich in der **individuelle Perspektive** an, darüber nachzudenken, was ein jeder Einzelne tun kann, um im digitalen Zeitalter sein eigenes Wohlbefinden und Gesundheit zu erhalten. Mögliches Themengebiet kann hier zum Beispiel sein, wie eine Struktur im digitalen Alltag geschaffen werden kann, um Zeiten auf Social Media Apps zu regulieren, um beispielsweise ausreichend Schlaf zu finden und ungestörte Arbeitszeiten zu generieren.

5. Beschreibung der zentralen Stakeholder-Gruppen (und der gewünschten/vorgeschlagenen Repräsentant*innen)

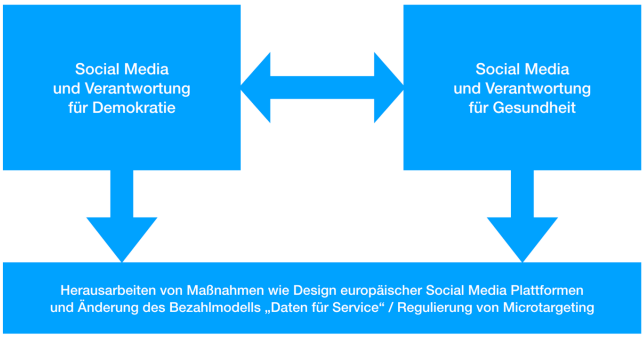
- Nutzer von Social Media Plattformen (direkte Mitglieder der Social Media Plattformen)
- Besucher von Social Media Plattformen ohne Mitglied zu sein (Log Dateien werden trotzdem gesammelt)
- Indirekt sind alle Bundesbürger von einigen Auswirkungen der Social Media Plattformen betroffen
- Gestalter digitaler Angebote (Digitalagenturen, wie Influencer-Netzwerke oder Werbeagenturen, welche Targeting-Maßnahmen nutzen)
- Weitere Interessengruppen wie Beratungsstellen für digitale Gewalt oder Well-Being Angebote im Digitalzeitalter (siehe die Time Well Spent Initiative in den USA)

6. Ideen und Finanzierung zur Vertiefungsforschung in den Vulnerabilitätsräumen

Die Probleme, die aus den Themenbereichen Social Media und Verantwortung für Demokratie/Gesundheit resultieren, sind bereits relativ gut umrissen, können aber empirisch nur unzulänglich beforscht werden. Ein Grund dafür ist, dass momentan nur unzureichend das Verhalten von Menschen auf diesen Plattformen untersucht werden kann, da die hierfür benötigten Schnittstellen nur eingeschränkt verfügbar sind. Wichtig wäre die Öffnung von Plattformen wie Facebook für unabhängige-öffentliche Forschung, um eine entsprechende Abschätzung der Social Media Wirkung auf die benannten Themenbereiche herausarbeiten zu können. Solche Forschung muss unter den aktuell höchsten ethischen Standards durchgeführt werden, da sich unter anderem bereits in 2018 der Cambridge Analytica Datenskandal das Ausmaß der Manipulationsmöglichkeiten durch Microtargeting offenbart hat. Als Anmerkung: Erste Initiativen sind von Facebook in 2018 bereits entstanden, um solche Forschung zu ermöglichen. Allerdings stecken diese Entwicklungen noch in den Kinderschuhen.
Die Finanzierung solcher Forschung sollte durch Plattformen wie Facebook, durch öffentliche Forschungsgelder wie der DFG und Stiftungen wie von Volkswagen oder Daimler ermöglicht werden.

7. Auflistung der drei bis fünf „most critical problems and challenges“ in Stichworten aus de Sicht des Vulnerabilitätsraumes

(1) Beantwortung der Frage ob es Filterblasen tatsächlich gibt und wie groß das Problem von Filterblasen und Echokammern auf die politische Meinungsbildung tatsächlich ist.
(2) Kausalität in dem Zusammenhang zwischen exzessiver Social Media Nutzung und Angst-/Depressions-erkrankungen.
(3) Bildungsaspekte für Digitale Natives und Immigrants: Aufklären über die Funktionsweisen der Plattformen, etc., Probleme des sozialen Vergleichs online, etc.; wie kann Bildung generell stattfinden (schulische und außerschulische Bildung zu Medienkompetenz).
(4) Regulierung von Microtargeting-Maßnahmen zum Schutz der Demokratie und das Schaffen ge-

	setzlicher Rahmenbedingungen, um Digital Phenotyping im Gesundheitssektor zu ermöglichen.
8.	Weitere zentrale Anmerkungen/Inputs zum Kick-Off-Meeting
	Besonders bedeutsam wird es sein, die Wechselwirkungen zwischen beiden Themenkomplexen herauszuarbeiten, um am Ende die richtigen Implikationen für den politischen Prozess herauszuarbeiten sowie um sich inhaltlich gut mit der AG zur Desinformation abzustimmen. Zu dieser Konzeptskizze hat Michael Latzer, Uni Zürich und Mitglied der Steuerungsgruppe des Projekts bei er Erstellung der ersten Skizze und der Revision wesentliche Inputs gegeben. 

06 Vulnerabilitätsraum: «Vertrauenswürdigkeit von Informationen im digitalen Raum»

Autoren: S. Hallensleben (VDE) mit Input von, A. Kaminski (Uni Stuttgart), M. Reißig (IASS), R. W. Scholz (Donau Uni Krems), K.-H. Simon (Uni Kassel)

1. Titelvorschlag Bezeichnung/deutscher (und englischer) Titel

Vertrauenswürdigkeit von Informationen im digitalen Raum (Reliable and Trustworthy Digital Ecosystems)

2. Kurzbeschreibung

Ein vertrauensvolles Miteinander, die Möglichkeit faktenbasierter Diskurse und die Symbiose von Anonymität und Identität sind essenzielle Grundlagen des Zusammenlebens in demokratischen und rechtsstaatlichen Gesellschaften. Trends zur breiten Verfügbarkeit von Werkzeugen zur Fälschung von Informationen im digitalen Raum und die zunehmende Verlagerung unserer Kommunikation in den digitalen Raum stellen diese Grundlagen und damit die Form unseres Zusammenlebens jedoch in Frage. Der Vulnerabilitätsraum soll diese Problematik untersuchen und konsensfähige Lösungsansätze entwickeln.

3. Erster Entwurf der Leitfrage (Guiding Question)

Wie können wir Informationsökosysteme so gestalten, dass ein fakten- und wertebasierter*, gesellschaftlicher, wissenschaftlicher und politischer Diskurs möglich bleibt? Wie kann auch künftig mündige politische Meinungsbildung ablaufen? Wie sorgen wir mit einer Kombination aus sozialen und technischen Ansätzen dafür, dass ein Dialog Führen und ggf. auch eine mühsame Konsensfindung attraktiver bleiben als das Verharren auf extremen Positionen? Welche Anreize für die Wahrheitsfindung und -verbreitung können wir schaffen?
*) „Werte“ meint hier v.a. Konsistenz, Verantwortung, und Veränderungsoffenheit.

4. Beschreibung von möglichen/wichtigen nicht intendierten, unbeabsichtigten Nebenfolgen (unseens)

(1) <u>Disruption der Vertrauenswürdigkeit im digitalen Raum</u>

Videos galten bisher als das weitgehend unbestechliche digitale Äquivalent des Augenscheins. Seit 2018 sind jedoch mit künstlicher Intelligenz ausgestattete Werkzeuge (v.a. Deep Fake[3],[4],[5]) verfügbar, mit denen praktisch jedermann beliebige Video- und Audioaufnahmen fälschen kann. Mit entsprechender Rechenleistung sind diese Fälschungen sogar in Echtzeit möglich. Auch überzeugende „Fotos“ nichtexistenter Menschen lassen sich mittlerweile mit minimalem Aufwand generieren[6].

Parallel zu dieser technologischen Entwicklung sinkt der Einfluss der traditionellen Massenmedien und ihrer Filter- und Verifizierungsfunktion für Informationen. Inhalte, egal, ob echt oder gefälscht, können sich in sozialen Netzwerken rasend schnell verbreiten, oft gezielt vorangetrieben durch kommerzielle Dienstleister[7]. Die Werbewirtschaft und manche politischen Akteure haben sich bereits auf diese neuen Verbreitungsmöglichkeiten eingerichtet. Über gezielte Einflussnahmen beispielsweise der russischen „Internet Research Agency“ (IRA) [8] [9] sowie Wahlmanipulation durch Cambridge Analytica[10] ist ausführlich berichtet worden.

Eine Flut falscher Informationen hat das Potenzial, Fakten in der Wahrnehmung zu verdrängen. Dies geschieht nicht nur durch eine bewusste Entscheidung des Rezipienten, dieser oder jener Information eher zu vertrauen, sondern auch durch eine unbewusste Überlagerung bereits abgespeicherten Wissens[11].

[3] https://gizmodo.com/researchers-come-out-with-yet-another-unnerving-new-de-1828977488
[4] https://www.theregister.co.uk/2018/09/11/ai_fake_videos/
[5] https://www.youtube.com/watch?v=gLoI9hAX9dw
[6] https://www.theregister.co.uk/2018/12/14/ai_created_photos/ (man beachte auch das eingebettete Video im Artikel)
[7] https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf
[8] https://www.nytimes.com/2015/06/07/magazine/the-agency.html
[9] https://www.economist.com/briefing/2018/02/22/inside-the-internet-research-agencys-lie-machine
[10] https://www.bbc.com/news/av/world-43472347/cambridge-analytica-planted-fake-news
[11] https://www.researchgate.net/publication/8045738_Searching_for_the_neurobiology_of_the_misinformation_effect

(2) Gefährdung des demokratischen Gemeinwesens als Konsequenz

Wenn nun selbst Videos überzeugend gefälscht werden können und damit die letzte Bastion der Tatsachenprüfung durch Augenschein fällt, dann sind sämtliche Onlineinhalte fragwürdig. **Wahrheit und Lüge werden ununterscheidbar**. Nicht nur gefälschte Informationen können für echt gehalten werden, sondern auch echte Informationen können in Zweifel gezogen werden. Aviv Ovadya hat für diese Entwicklung den Begriff „Infokalypse" geprägt[12], der inzwischen auch an anderen Stellen aufgenommen wurde, allerdings bisher nur in Form einzelner Zwischenrufe an die breitere Öffentlichkeit gelangt ist [13] [14].

Traditionelle Massenmedien können zwar weiterhin versuchen, als Filter und Prüfer zu agieren, sind aber der emotionalen Wirkung und der rasend schnellen Verbreitung einer gefälschten „Nachricht" gegenüber machtlos. Sie können ihre Filterfunktion im extrem beschleunigten Online-Nachrichtenfluss nur noch schwer oder verzögert ausüben. **Wenn sich Wahrheit und Lüge für den Einzelnen aber nicht mehr mit realistischem Aufwand trennen lassen, dann ist das Konstrukt des „mündigen Bürgers" bzw. eines „mündigen Volkes"** als Ausgangspunkt aller staatlichen Gewalt (vgl. Artikel 20, Absatz 2 des Grundgesetzes) **faktisch unmöglich geworden**. Das demokratische Gemeinwesen verliert seine Grundlage. Die Auseinandersetzung mit der Vertrauenswürdigkeit von Informationen im digitalen Raum wird so zur dringlichen Notwendigkeit.

Neben der Gefährdung demokratischer Systeme durch die informationelle Entmündigung des Bürgers sind weitere schwerwiegende Folgen realistisch, darunter die Infragestellung der Zuverlässigkeit polizeilicher Untersuchungen oder Gerichtsprozesse durch die Fälschbarkeit von Informationen; Manipulation der Finanzmärkte mit realen Auswirkungen auf die Weltwirtschaft etc.

Verschärft wird die Situation durch **kommerzielle Anreize**, denn für Onlineinhalte dominiert als Geschäftsmodell die Werbefinanzierung. Dies führt dazu, dass die Auswahl und Darstellung von Inhalten allein auf eine hohe Aufmerksamkeit der Nutzer (z.B. gemessen durch Klicken oder Teilen) gerichtet ist (vgl. z.B. diese Tipps einer Werbeagentur[15]). Da extreme und/oder emotional erschütternde Nachrichten eine besonders hohe Aufmerksamkeit erregen, besteht ein hoher Anreiz für Plattformen, diese besonders prominent anzuzeigen. Gefälschte Informationen können genau dieses Muster besonders einfach bedienen und verbreiten sich daher besonders leicht.

5. Beschreibung der zentralen Stakeholder-Gruppen (und der gewünschten/vorgeschlagenen Repräsentant*innen)

- Schwerpunkt technische Perspektive: Experten für Künstliche Intelligenz, Deep Fakes, IT-Sicherheit, Zertifikatswesen, auch Datenwissenschaftler/ Bibliothekare
- Schwerpunkt gesellschaftliche/politische/rechtliche Perspektive: Publizisten wie Journalisten, Verlagsinhaber, Blogger, Medienwissenschaftler; Juristen für Internetrecht, Datenschützer, Normungsspezialisten; auch Politiker
- Schwerpunkt philosophische Perspektive: Wissenschafts- und Technikphilosophen, Historiker; Psychologen
- Schwerpunkt ökonomische Perspektive: Wirtschaftswissenschafter; Akteure im Online Marketing, Product Information Management, Content-Plattformen

6. Ideen und Finanzierung zur Vertiefungsforschung in den Vulnerabilitätsräumen

Es ist unklar, wie eine Infrastruktur für eine breit anerkannte, nicht staatlich beeinflusste Zertifizierung von Informationsquellen technisch aussehen könnte, insbesondere für „Marken", die nicht bereits aus dem Offline-Bereich bekannt waren. Die Vergabe von SSL-Zertifikaten für elektronische Signaturen kann ein Ausgangspunkt der Überlegungen sein, ist aber nur begrenzt übertragbar und hat zahlreiche Schwächen. Wichtig ist auch, dass eine anonyme (bzw. irreversibel pseudonyme) Kommunikation möglich bleibt. Zur Erarbeitung und idealerweise Demonstration technisch realisierbarer Vorschläge sollte Vertiefungsforschung im Umfang von 1 Personenjahr eingeplant werden.
Mehrere weitere Vertiefungsprojekte sind denkbar.

[12] https://www.buzzfeed.com/charliewarzel/the-terrifying-future-of-fake-news
[13] https://www.wiwo.de/politik/deutschland/schlusswort-laesst-sich-die-infocalypse-noch-abwenden/20989742.html
[14] https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth
[15] https://blog.hootsuite.com/de/facebook-algorithmus-organische-reichweite/

7.	Auflistung der drei bis fünf „most critical problems and challenges“ in Stichworten aus der Sicht des Vulnerabilitätsraumes
	1. Bisherige primär technologische Gegenmaßnahmen gegen Fake News wie die KI-gestützte Untersuchung von Videos oder die internen Netzwerkaktivitätsanalysen großer Internetplattformen sind letztlich nur ein Wettrüsten mit immer besseren Fälschungswerkzeugen und -methoden. Das zugrundeliegende erkenntnistheoretische Verständnis von Vertrauenswürdigkeit liefert bestenfalls partielle Lösungen. 2. Das Vertrauen in Informationen fußt fast immer auf dem Vertrauen in die Person/Institution, die sie verbreitet. Die Mechanismen zur Genese dieses Vertrauens (z.B. Andocken an den Augenschein in der realen Welt, Transfer, Crowdansätze etc.) sollten daher einen Schwerpunkt bilden (im Gegensatz zu Punkt 1 steht dahinter ein Anerkennungsmodell von Vertrauenswürdigkeit). Die Frage ist, wie eine institutionelle Infrastruktur des Vertrauens als ein „Gerüst der Wahrheit“ aussehen könnte. 3. Die Auseinandersetzung „Anonymität vs. Pseudonymität vs. Klarnamen“ im Netz ist ein künstlich konstruierter Konflikt. Jeder der drei Ansätze ist in bestimmten Kontexten sinnvoll und muss für Menschen zugänglich sein. Die Verantwortlichkeit für eigene Inhalte ebenso wie für das Teilen von Fremdinhalten muss neu gedacht werden. 4. Der Nachweis einer Lüge genügt nicht. Gesellschaftliche Konventionen und andere Faktoren bestimmen den Umgang mit ertappten Lügnern (vgl. Trump vs. Relotius). Vgl. auch das Phänomen „Reality Apathy“. Wir benötigen eine pragmatische Auseinandersetzung zur Existenz „objektiver“ Fakten oder einer objektiven Wahrheit[16] sowie der Frage, inwieweit Wahrheit tatsächlich gewollt ist, auch mit Blick auf psychologische Mechanismen. 5. Gängige Geschäftsmodelle für Onlineinhalte – vor allem die Werbefinanzierung – stehen im Zielkonflikt mit Vertrauenswürdigkeit und müssen vermutlich weiterentwickelt bzw. ersetzt werden; gleichzeitig ist zu erwarten, dass nicht alle Lösungsvorschläge kommerziell tragfähig und stattdessen bspw. staatlich zu finanzieren sind. Letzteres wirft wiederum die Frage auf, inwieweit diese im Kontext repressiver Regime funktionieren würden. „Vertrauen ist akzeptierte Vulnerabilität“ (Kaminski). Eine **komplette** Beseitigung von Vulnerabilität würde also Vertrauen obsolet machen. Dies kann nicht das Ziel sein. Es geht hier darum, in einer komplexen Gratwanderung das richtige Maß von Vulnerabilität zu finden und nachhaltig zu verwirklichen. Das betrifft auch das Verständnis von Demokratie als eines inhärent vulnerablen Systems.

8.	Weitere zentrale Anmerkungen/Inputs zum Kick-Off-Meeting
	Zwei Facetten zum methodischen Vorgehen: **(1)** Die Wirksamkeit und Sinnhaftigkeit von Lösungsansätzen soll anhand einer Reihe frühzeitig definierter **Test Cases** geprüft werden. Jeder Test Case beschreibt eine – bereits beobachtete oder auch konstruierte – problematische Situation, für die der Effekt eines Lösungsansatzes durchgespielt werden kann. – Beispiele: „Der gewählte Präsident eines einflussreichen Landes bestreitet offensichtliche Fakten und ermutigt Gewalt gegen kritische Journalisten“ oder „Ein Massenmedium stellt reißerische ‚Nachrichten‘ ohne Rücksicht auf deren Wahrheitsgehalt in den Vordergrund, um Aufmerksamkeit und Werbeeinnahmen zu generieren.“ oder „Ein bestechlicher Politiker bestreitet die Echtheit von Videodokumenten und lässt gleichzeitig ein falsches Video seines politischen Gegners herstellen und streuen, in dem diesem abstoßende Aussagen in den Mund gelegt werden.“ oder „Ein repressives Regime unterdrückt eine unabhängige Presse mit der Behauptung, sie würde ‚fake news‘ verbreiten.“ oder „Der Diskurs zu einer gesamtgesellschaftlichen Herausforderung zerfällt in fragmentierte Öffentlichkeiten.“ Mit der Formulierung von Test Cases wird frühzeitig ein Rahmen für die gemeinsame Arbeit und Diskussion gesetzt und ein Konsens zum Zielkorridor hergestellt. **(2)** Im Fokus dieses Vulnerabilitätsraums stehen Informationsökosysteme wie die klassischen Nachrichtenmedien, Plattformen für nutzergenerierte Inhalte (Twitter, Facebook, YK, Wordpress, Medium etc.) sowie Fachpublikationen (auch in der Wissenschaft). Gleichzeitig können jedoch weitere Ökosysteme herangezogen werden, um technologische Eigenschaften und Regulierungsmechanismen zu verstehen und ggf. durch Analogieschlüsse Handlungsmöglichkeiten für die Informationsökosysteme zu identifizieren. Beispiele für dieses Umfeld sind App-Ökosysteme (Google, Apple), Datenökosysteme im Industrie-4.0-Bereich (z.B. Bosch IOTA), Zertifikatökosysteme (SSL klassisch bzw. mit CaCERT), Digitale Währungen oder Peer-to-Peer-Dateiaustausch-Ökosysteme (z.B. BitTorrent).

[16] unter Berücksichtigung der bereits vorhandenen philosophischen Erkenntnisse und Traditionen

07 Vulnerabilitätsraum: «Cybercrime/-security im Cyberspace»

Autoren: Eike Albrecht (BTU), Veselko Hagen (BTU), Martin Fröhlich (IT-Compliance Solutions), Dirk Marx (BTU), Hinrich Völcker (Deutsche Bank), Haiying Wu (Huawei)

1. Titelvorschlag Bezeichnung/deutscher (und englischer) Titel

"Cybercrime/-security in Cyberspace", "Cyberkriminalität/-sicherheit im Cyberspace"

2. Kurzbeschreibung und terminologische Grundlagen

Die Nutzung digitaler Systeme im Cyberspace erleichtert die Begehung von Straftaten oder ermöglicht diese erst und stellt eine zunehmende Herausforderung für die öffentliche Sicherheit und Ordnung dar (Falk 2017; Leitner 2019). Dolose Handlungen nach Siepermann (2017) und alle anderen unrechtmäßigen Handlungen im digitalen Raum *Cyberspace* erfordern im Rahmen der Zuordnung *Cybercrime, Cybersecurity* Antworten auf Fragen, die teils noch gar nicht gestellt sind (Goeken und Fröhlich 2018). Neue Gesetze, angepasste Organisationsstrukturen und geänderte Verhaltensweisen, verbunden mit dem Ziel, die *Resilienz* der Gesellschaft und des Staates gegen die nachteiligen Auswirkungen der Digitalisierung zu erhöhen, erfordern «*socially robust orientations*»[17] wertneutral in diesem Teilprojekt zu entwickeln. Die im Rahmen der Abwägung zwischen verschiedenen Rechtsgütern (Freiheit vs. Sicherheit) und Gesellschaftskonzepten (Selbstverantwortlichkeit vs. staatlich-gesellschaftlich organisierter Schutz) erfolgende Gewichtung muss daher Gegenstand einer gesellschaftlichen Aushandlung sein, vor allem vor dem Hintergrund nicht vorhersehbarer und nicht gewollter Nebeneffekte (Scholz 2019). Angriffe auf staatliche digitale Infrastruktur und Daten sind regelmäßig strafbar, aber schwer nachweisbar. Digitale Spuren sind flüchtig und selten mit den für den klassischen Strafrechtsbereich geltenden Beweisanforderungen zu belegen (Miebach 2016). Manifestationen von Verhalten, Verständnissen und Praktiken (beispielsweise Korruption) erzeugen eine Art perspektivische Zweischneidigkeit, dazu, wie, wann und wo Handlungen im Cyberspace entscheidend als kriminell entdeckt und erkannt werden (Carraro et al., 2011; Del Monte und Papagni, 2001).

3. Zweiter Entwurf der Leitfrage (Guiding Question)

Ist es möglich, ein *suffizientes Gesamtbild* über unerwünschte *Rebound-Effekte* der Digitalisierung in Deutschland als Beitrag zu einer *resilienten Gestaltung* der Gesellschaft – zu identifizieren, zu beschreiben und zu bewerten?

Zu klären ist in diesem Teilprojekt, inwieweit die derzeit verfolgten Rechtskonzepte zur Bewältigung der Herausforderung der Digitalisierung geeignet sind, den Herausforderungen der Digitalisierung zu begegnen (Lentner 2019). Das betrifft zum einen den Rechtsrahmen insgesamt, daneben auch organisationsbezogene Antworten, aber auch die strukturell zu beobachtende Verlagerung von originär staatlichen Aufgaben auf Private (Scholz 2019; Ebert und Maurer 2017). Diese Verlagerung erfolgt bislang einzelfallbezogen und ohne eine Überprüfung von Nebeneffekten und vor allem ohne eine ausreichende gesellschaftliche Diskussion. Hier ist zu klären, ob und inwieweit und unter welchen Voraussetzungen die Verlagerung von solchen staatlichen und für den Einzelnen, die Wirtschaft und die Gesellschaft als Ganzes auch relevanten Aufgaben stattfinden soll.

Die Frage ist somit, wie dieser gesellschaftliche Aushandlungsprozess auch mit Blick auf unsere Praxispartner und durch sie vorgestellten *Projekte im VR Cyberspace*, beispielhaft zu organisieren ist. Dabei sind die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit - CIA-Triade -[18] der Informationssicherheit mit denen der Cybersicherheit deckungsgleich; Informations- und Kommunikationstechnologie stellt sich als die wesentliche Schwachstelle heraus und ist deshalb als Querschnittsthema zu behandeln. (Whitman und Mattord 2012, S. 8; von Solms und van Niekerk 2013; Godbole 2016).

[17] DiDaT Newsletter 01, Februar 2019, www.iass-potsdam.de (abgerufen am 05.05.2019); IASS DiDaT-Broschüre 2018, S.6 DOI: 10.2312/iass.2018.010

[18] „confidentiality, integrity, and availability"; Sicherheitslücken im Internet - www.informatik.uni-oldenburg.de (abgerufen am 02.05.2019)

4.	Beschreibung von möglichen/wichtigen nicht intendierten, unbeabsichtigten Nebenfolgen (unseens)

(a) Rechtsrahmen wie z.B. das IT-Sicherheitsgesetz

Mit zunehmender Digitalisierung in verschiedensten Bereichen besteht die Gefahr von Insellösungen und Einzelfallregelungen, wobei eine rechtliche Gesamtstrategie auf der Grundlage gesellschaftlich ausgehandelter Rechtskonzeptionen erforderlich erscheint und somit bekannte Risikomanagementsysteme Vulnerabilitätsbeurteilungen bereits beinhalten (Albrecht und Küchenhoff, 2015, Rdnr. 145; Albrecht 2008; Albrecht und Woll, 2010).

(b) Organisationsbezogene Fragen

Der Staat reagiert auf die Herausforderungen der Digitalisierung auf unterschiedliche Weise und auf unterschiedlichen Ebenen. Das Bundesamt für Sicherheit und Informationstechnik – BSI – sowie die Einrichtung der Agentur für Cybersicherheit in Leipzig aber auch durch die Zustimmung Verantwortlichkeiten auf überstaatliche, vor allem europäische Einrichtungen, wie z. B. der Agentur der Europäischen Union für Netz- und Informationssicherheit ENISA, zu verlagern.

(c) Zunehmende Privatisierung von originär staatlichen Aufgaben

Zunehmend werden Aufgaben des Staates auf Private verlagert. Das gilt besonders für den Bereich der Digitalisierung, die als Gruppen *Benutzer* und *Anwender* (Unternehmen, Behörden, private Nutzer) *Governance* (Regierungen und sonstige staatliche Stellen), Netz- und Internet-Service-Provider (ISP), Hersteller und Dienstleister (wie z.B. IT-Sicherheitsfirmen, Hobby-Hacker (Scriptkidis) und Hacktivisten), Strafverfolgungsbehörden sowie CERTs (Computer Emergency Response Teams), deren Hauptzwecke nicht nur die Gewinnerzielung ist, sondern die zunehmend für staatliche Aufgaben eingesetzt werden, identifiziert (Pospisil et al. 2017).

(d) Zunehmende Verlagerung von Entscheidungen auf automatisierte Verfahren (KI)

Digitalisierung, die zum guten Teil auch mit *Automatisierung* übersetzt werden kann, erfordert -nahezu unbemerkt- gravierende Verhaltensänderungen der Nutzer und Anwender, und auch in großem Umfang, die Verlagerung von Entscheidungen weg von Menschen, hin zu Maschinen. Beispiele dazu sind Partnerbörsen, die Personalgewinnung und somit ein zunehmender Einsatz künstlicher Intelligenz (KI); Stichworte hier sind das Internet der Dinge (IOT), Industrie 4.0, oder die gerade der Öffentlichkeit vorgestellten autonom handelnden und automatisierten Waffensysteme.

(e) Cybersecurity bei staatlicher digitaler Infrastruktur

„Hacker oder Cyberkriminelle können die kritische Infrastruktur eines Landes – wie das Stromnetz oder Anwendungssysteme eines Krankenhauses – über den Cyberspace angreifen. Dies könnte entweder indirekt, z.B. durch Beeinflussung der Verfügbarkeit von Informationen mittels Denial-of-Services-Angriffen, oder direkt durch einen Angriff auf die kritische Infrastruktur selbst (z.B. durch sog. Ransomware) geschehen“ (Goeken und Fröhlich 2018, S. 5). Zu den heutigen Angreifern müssen auch die organisierte Kriminalität und sogar Staaten gerechnet werden. Gerade die letztgenannte Gruppe zeichnet sich durch nahezu unerschöpfliche personelle und finanzielle Ressourcen aus (Eckert 2017, S. 141). Verstärkt wird diese Entwicklung dadurch, dass wenig transparente Privatunternehmen, wie die amerikanische Softwarefirma „Palantir“ private, aber auch staatliche Kundschaft bedient und Software und Technologie zum Ausspähen und zum Ordnen von Massendaten liefert. Wird von „Palantir“ entwickelte Software eingesetzt, bedeutet dies, dass aus der Analyse von „big data“ sicherheitsrelevante, personenbezogene oder anderweitig sensible Informationen in nicht-kontrollierte (und kontrollierbare) Sphären gelangen.

5.	Beschreibung der zentralen Stakeholder-Gruppen (und der gewünschten/vorgeschlagenen Repräsentant*innen)

- Schwerpunkt Rechtsrahmen: Verfassungsjuristen, Strafrechtler
- Schwerpunkt Organisationsbezogene Fragen bei Cybercrime: Staatsanwaltschaften, Verwaltungswissenschaftler
- Schwerpunkt Zunehmende Privatisierung von originär staatlichen Aufgaben: Private Unternehmen in den beschriebenen Bereichen (Internet-Provider, Social-Media-Plattformen, Banken & Versicherung
- Schwerpunkt Zunehmende Verlagerung von Entscheidungen auf automatisierte Verfahren: Unternehmen, die automatisierte Verfahren verwenden (Banken, Versicherungen, Partnerbörden, etc.; Arbeitsrechtler)

- Schwerpunkt Cybersecurity bei staatlicher digitaler Infrastruktur: Sicherheitsbehörden, z.B. BSI sowie die Agentur für Cybersicherheit und der Geheimdienst BND, Bundesamt für Verfassungsschutz und Terrorismusbekämpfung in Österreich

6. Ideen und Finanzierung zur Vertiefungsforschung in den Vulnerabilitätsräumen

Alle fünf in diesem VR benannten „unseens" sind zwar schon beschrieben, aber nur in Teilbereichen erforscht. Gelingt die Verknüpfung mit Fragen des Strukturwandels, ist eine Forschungsförderung über die Strukturwandelprogramme für die Lausitz denkbar.

7. Herausforderungen durch neue Akteure und Technologien: Auflistung der drei bis sechs „most critical problems and challenges" in Stichworten aus der Sicht des Vulnerabilitätsraumes

(a) Im Bereich Cybercrime gelingt es den Strafverfolgungs- und Sicherheitsbehörden zunehmend weniger, entsprechende präventive und repressive Maßnahmen zu ergreifen. Es werden zur besseren Bekämpfung von Cyberangriffen zwingend neue Kooperationen zwischen dem BSI, den LKAs, dem BKA und den Strafverfolgungsbehörden mit der Industrie erforderlich.
(b) Die hohe Geschwindigkeit der Änderungen durch Digitalisierung ist eine erhebliche Herausforderung für den Gesetzgeber, der entweder bestimmte problematische Handlungsweisen nicht schnell genug rechtlich reguliert, oder bei anderen Fragen nicht schnell genug die rechtlichen Grundlagen für deren Einsatz schafft.
(c) Mit der Verlagerung von Entscheidungen auf technische Prozesse und Algorithmen geht eine zunehmende Entpersönlichung von Entscheidungen einher.
(d) Die Frage nach der Sicherheit der KI (-Systeme) gegen Eingriffe von außen als Frage der Cybersecurity gilt im besonderen Maße für autonome automatisierte Waffensysteme.
(e) Die Verlagerung sensibler staatlicher Aufgaben auf Private könnte zum einen nicht gewollter technischer Möglichkeiten erst zum technischen oder gesellschaftlich akzeptiertem Durchbruch verhelfen (Stichwort: Upload-Filter), zum anderen diese Privaten zum Gegenstand von Begehrlichkeiten anderer Unternehmen machen, die ein eigenes kommerzielles (oder sonstiges, auch drittstaatliches) Interesse an bestimmten Informationen und Daten haben. (Stichwort: Huawei beim 5-G-Netzaufbau als Grundlage für diverse neue technologische Lösungen).
(f) Möglicherweise müssten die Anforderungen an die Überzeugung des Richters bei Cyberangriffen nach § 261 StPO den o.g. Schwierigkeiten beim Nachweis von entsprechenden Handlungen neu justiert werden, um einen ausreichenden strafrechtlichen Schutz bei Angriffen über die digitale Infrastruktur zu gewährleisten.

8. Literatur

Albrecht, E., Küchenhoff, B. (2015): Staatsrecht, 3. Aufl. Erich Schmidt, Berlin.
Albrecht E., Woll, R. (2010): Modelle, Methoden und Werkzeuge zum Risikomanagement, BTU, Bericht.
Albrecht, E. (2008): Risikomanagement nach REACH, StoffR (2), S. 64-69.
Carraro, L., Castelli, L. (2011): Ideology is related to basic cognitive processes involved in attitude formation. Journal of Experimental Social Psychology, Vol. 47, Issue 5, S. 1013-1016.
Del Monte, A., Papagni, E. (2001): Public expenditure, corruption, and economic growth: the case of Italy. European Journal of Political Economy, vol. 17, issue 1, 1-16.
Ebert, H., Maurer, T. (2017): Cyber Security. In: Patrick James (ed.): Oxford Bibliographies in International Relations. Oxford University Press, New York.
Eckert, C. (2017): Cybersicherheit beyond 2020. Informatik-Spektrum 40 (2017), Nr. 2, S. 141-146.
Falk, M. (2017): Cyber Security. Der blinde Fleck auf der CEO-Agenda. Entscheidern fehlt das «Big Picture» in der Diskussion um Cyber-Risiken. www.klardenker.kpmg.de (abgerufen am 02.05.2019).
Freiling, F., Grimm, R., Großpiesch, K.-E., Keller, H.B., Mottok, J., Münch, I., Rannenberg, K., Saglietti, F. (2014): Technische Sicherheit und Informationssicherheit. Unterschiede und Gemeinsamkeiten. Informatik-Spektrum 37, Nr. 1, S. 14-24.
Godbole, S. (2016): From Information Security to Cyber Security. www.isaca.org (abgerufen am 02.05.2019)
Goeken, M., Fröhlich, M. (2018): Sicherheit im Cyberraum – Stand der Dinge, Herausforderungen, Lösungsansätze. IT-Governance 27, S. 3-9.
Lentner, G. M. (2019). *Comparative Legal Analysis on Digital Data as subject of the European/German, US-American and Hongkong Law*.
Mertens, P., Barbian, D., Baier, S. (2017): Digitalisierung und Industrie 4.0 – eine Relativierung. Springer Wiesbaden.
Miebach, K. (2016), § 261, Rn. 58 f., in: Knauer, C., Kudlich, H., Schneider, H. (Hrsg.), Münchener Kommentar zur StPO, Beck, München.
Pospisil, B., Gusenbauer, M., Huber, E., Hellwig, O. (2017): Cyber-Sicherheitsstrategien – Umsetzung von Zielen durch Kooperation. Datenschutz und Datensicherheit – DuD, Ausgabe 10.
Scholz , R. W., u. Kley, M. (2019): Stocks and Flows-based Stakeholder Analysis of Digital Data – Basic concepts, tools for analysis, data, and the role of digital data infrastructure providers. Kreuzlingen: STTM.
Siepermann, M. (2017): Stichwort «IT Security». In: Gabler Wirtschaftslexikon online. www. wirtschaftslexikon.gabler.de (abgerufen am 02.05.2019)
Von Solms, R., van Niekerk, J. (2013): From information security to cyber security. Computers u. Security, Vol. 38, 10/2013, S. 97-102.
Whitman, M., Mattord, H. (2012): Principles of Information Security. 4th ed., Boston.

Institute for Advanced Sustainability Studies (IASS) e. V.

Das IASS forscht mit dem Ziel, Transformationsprozesse hin zu einer nachhaltigen Gesellschaft aufzuzeigen, zu befördern und zu gestalten, in Deutschland wie global. Der Forschungsansatz des Instituts ist transdisziplinär, transformativ und ko-kreativ: Die Entwicklung des Problemverständnisses und der Lösungsoptionen erfolgen in Kooperationen zwischen den Wissenschaften, der Politik, Verwaltung, Wirtschaft und Gesellschaft. Ein starkes nationales und internationales Partnernetzwerk unterstützt die Arbeit des Instituts. Zentrale Forschungsthemen sind u.a. die Energiewende, aufkommende Technologien, Klimawandel, Luftqualität, systemische Risiken, Governance und Partizipation sowie Kulturen der Transformation. Gefördert wird das Institut von den Forschungsministerien des Bundes und des Landes Brandenburg.

DiDaT: Die verantwortungsvolle Nutzung Digitaler Daten als Gegenstand eines Transdisziplinären Prozesses

Institute for Advanced Sustainability Studies Potsdam (IASS) e. V.
Berliner Straße 130
14467 Potsdam
Tel: +49 (0) 331-28822-300
Fax: +49 (0) 331-28822-310
E-Mail: media@iass-potsdam.de
www.iass-potsdam.de

Autoren:
Ortwin Renn und Roland W. Scholz

Kontakt:
Ortwin Renn: Ortwin.Renn@iass-potsdam.de
Roland W. Scholz: Roland.Scholz@donau-uni.ac.at
oder Roland.Scholz@iass-potsdam.de

ViSdP:
Prof. Dr. Dr. Ortwin Renn,
Geschäftsführender Wissenschaftlicher Direktor

Förderung des Projekts DiDaT:
DiDaT ist ein Projekt des IASS. Es wird in Kooperation mit der Donau Universität Krems und ggf. anderen Institutionen durchgeführt. Eine finanzielle Förderung soll durch Institutionen/ Organisationen der Praxis und der öffentlichen Hand vorgenommen werden. Eine erste Förderung für die Initiierung erfolgte durch die Bernhard und Ursula Plettner Stiftung.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
FONA Forschung für nachhaltige Entwicklungen
BMBF
LAND BRANDENBURG
Ministerium für Wissenschaft, Forschung und Kultur