DIGITALE TRANSFORMATION UND ÖFFENTLICHE SICHERHEIT

1 DIGITALE TRANSFORMATION

In geradezu atemberaubender Geschwindigkeit haben sich moderne Gesellschaften rund um den Globus in den letzten Jahrzehnten gewandelt. Die Digitalisierung nahezu aller Bereiche des Lebens und Arbeitens ist eine der fundamentalsten Veränderung in der Menschheitsgeschichte. Dies wirft eine Vielzahl von Problemen auf, die für die öffentliche Sicherheit relevant sind, insbesondere die Frage nach der Beherrschbarkeit von datengetriebenen Prozessen, die mit hoher Geschwindigkeit ablaufen und sich damit tendenziell einer Kontrolle durch menschliche Akteure entziehen. Die Kernelemente dieser Transformation können folgendermaßen zusammengefasst werden:

- Digitalisierung geht mit einer Steigerung der Komplexität einher, da viele Prozesse nunmehr von technischen Systemen übernommen werden und oftmals automatisiert ablaufen. Entscheidungen werden von technischen Systemen in sehr kurzen Zeiträumen und in hoher Geschwindigkeit getroffen, wodurch die Undurchschaubarkeit komplexer, digitalisierter Systeme zunimmt.
- Mit der digitalen Repräsentation von Wirklichkeit geht der direkte, unmittelbare Bezug zum operativen Geschehen verloren.
- Die Datafizierung sämtlicher Prozesse hat darüber hinaus erhebliche Auswirkungen auf den Datenschutz und die Privatsphäre, weil nunmehr sämtliche Prozesse aufgezeichnet und überwacht werden können.
- Mit der Digitalisierung hält eine Logik der Kontrolle in viele Bereiche des Arbeitens und Lebens Einzug, die ursprünglich aus den Bereichen Militär und Logistik stammt. Diese Logik der Kontrolle wird nun aber in gesellschaftliche Lebensbereiche transferiert, die durch eine Balance von Autonomie und Kontrolle geprägt sind, deren Bewahrung ein Teil unserer freiheitlichen Grundordnung ist.
- Schließlich tangiert die Digitalisierung von Entscheidungsprozessen in komplexen soziotechnischen Systemen auch die politische Öffentlichkeit. Wenn Algorithmen Entscheidungen treffen, könnte dies tendenziell zu einer Erosion von Politik und deren Ersetzen durch eine „Algokratie“ führen.

Die digitalisierte Gesellschaft ist zwar einerseits effizienter und sicherer geworden, zugleich hat aber ihre Abhängigkeit von Technik und damit auch ihre Verletzlichkeit zugenommen. Moderne, digitale, oftmals sogar autonome Technik trägt dazu bei, die Sicherheit komplexer soziotechnischer Systeme zu erhöhen und „alte“ Risiken sowie damit einhergehende Unsicherheiten zu bewältigen.

Zugleich ergeben sich aber auch neuartige Gefährdungen und Bedrohungen, beispielsweise im Falle eines Versagens der Technik, sowie eine erhöhte Anfälligkeit, die sich zu Katastrophen

aufschaukeln können, weil kein Mensch mehr in der Lage ist, derartige Störfälle manuell zu beherrschen. Diese Risiken betreffen nicht nur den Einzelnen und dessen berechtigte Schutzinteressen, sondern auch das Gemeinwesen als Ganzes, ist die Gesellschaft doch auf das Funktionieren kritischer Infrastruktursysteme existenziell angewiesen.

So paradox es klingen mag: Digitalisierte sozio-technische Systeme sind sicherer, zugleich aber auch riskanter. In Erwartung einer hohen Zuverlässigkeit und perfekter Performance verlassen wir uns nämlich nicht nur auf derartige Systeme bei der Bewältigung bisheriger Aufgaben, sondern dehnen zudem die Grenzen unseres Handelns immer weiter aus.

2 MENSCH UND TECHNIK IM DIGITALEN ZEITALTER

Die Digitalisierung des privaten Alltags wie auch der Arbeitswelt schreitet in großen Schritten voran. Was in der Luftfahrt mit dem computergestützten Fliegen begann, setzt sich im Straßenverkehr und mittlerweile auch im Bereich „Gesundheit und Fitness“ fort. Smarte Geräte werden immer mehr zu unseren Begleitern, die uns bei vielfältigen Prozessen unterstützen bzw. unsere Handlungen ersetzen. Menschliche Bediener bzw. Nutzer befinden sich zunehmend in hybriden Konstellationen, in denen die Handlungsträgerschaft auf Menschen und (zunehmend) autonome Technik verteilt ist. Wie genau dieses Zusammenspiel funktioniert, ist noch unzureichend erforscht.

3 TECHNIK UND GESELLSCHAFT IM DIGITALEN ZEITALTER

In Organisationen, die kritische Infrastruktursysteme betreiben, ist ein funktionierendes Risikomanagement eminent wichtig. Katastrophen der jüngeren Zeit zeigen jedoch eindrucksvoll, was alles misslingen kann; sie deuten zudem auf die Stellschrauben und Einflussfaktoren hin, an denen man „drehen“ kann, um die öffentliche bzw. zivile Sicherheit zu erhöhen. Ein ganz wesentlicher Faktor ist eine funktionierende Organisationskultur, die es den Mitarbeitenden ermöglicht, auch in kritischen Situationen das Richtige zu tun. Hier tragen Organisationen, die kritische Infrastruktursysteme betreiben, offenbar eine große Verantwortung, der sie nicht immer hinreichend gerecht werden.

Der Überblick über unterschiedliche Konzepte und Strategien zum Umgang mit Unsicherheit hat zudem gezeigt, dass es wenig Sinn macht, die Debatte um das Risikomanagement mit abstrakten Modellen und mit pauschalen Zuordnungen ganzer Technologiebereiche zu bestimmten Risiko-Kategorien zu führen. Das Design des sozio-technischen Systems sollte immer eine wesentliche Komponente einer sozialwissenschaftlichen Risikoanalyse sein, aber nicht im Sinne abstrakter Generalisierungen, sondern gestützt auf eine realistische Modellierung und Simulation des jeweils konkreten Systems. Auf diese Weise lassen sich Szenarien entwickeln und Simulationsexperimente konzipieren, mit deren Hilfe sich Schwachstellen und Fehlerquellen im betreffenden System identifizieren lassen.

4 VERTRAUEN IN AUTOMATION

Gerade angesichts des unaufhörlichen Vordringens autonomer Technik stellt sich jedoch die Frage, ob Transparenz und Nachvollziehbarkeit noch gegeben sind und ob der Mensch noch in der Lage ist, die Entscheidungen autonomer Systeme nachzuvollziehen.

Vertrauen in (autonome) Technik kann definiert werden als die Bereitschaft, Kontrolle über Dinge oder Prozesse – zumindest zeitweise – abzugeben und sich darauf zu verlassen, dass eine andere Person oder ein technisches Gerät die betreffenden Aufgaben zuverlässig ausführt.

Besonders im Falle autonomer technischer Systeme sind die menschlichen Operierenden (z.B. Pilotinnen und Piloten) bzw. die Nutzenden von Dienstleistungen (z.B. Online-Käuferinnen und -Käufer), kaum noch in der Lage, eine vollständige Kontrolle auszuüben bzw. die Kontrolle im Notfall komplett zu übernehmen.

5 POLITIK IM DIGITALEN ZEITALTER

In der digitalen Gesellschaft wird ein neuer Governance-Modus praktiziert, der sich als die zentrale Steuerung dezentraler Systeme beschreiben lässt, die sich in Echtzeit vollzieht. Auf der operativen Ebene funktioniert dies bereits im Bereich der Verkehrssteuerung; und die Planungen für künftige intelligente Stromnetze zeigen in eine ähnliche Richtung.

Welche Folgen dies für die Politik hat, ist noch nicht absehbar. Auf jeden Fall wird deutlich, dass Politik nicht mehr mit dem traditionellen Repertoire interventionistischer Steuerung operieren kann, sondern neue Formen und Verfahren intelligenter Steuerung entwickeln muss, die unterschiedliche Konzepte und Instrumente kombinieren und auf das Zusammenspiel unterschiedlicher Akteure in Mehrebenen-Systemen setzen. Dem Staat kommt auch im digitalen Zeitalter die Aufgabe zu, die öffentliche wie die zivile Sicherheit zu gewährleisten; aber die Verfahren und Instrumentarien werden sich radikal wandeln müssen.

6 AUSBLICK UND HANDLUNGSFELDER

Die Digitalisierung führt zu einer enormen Beschleunigung und Verdichtung sämtlicher Prozesse in Wirtschaft und Gesellschaft, die weitgehend automatisiert ablaufen. Gestützt auf eine große Menge verfügbarer Daten, finden viele Prozesse, die früher Stunden oder Tage gedauert haben, nunmehr in Echtzeit statt. Damit verschwimmen die Grenzen von Planung und Handlung; denn es ist nunmehr möglich, ad hoc zu planen und mehrere Prozesse parallel stattfinden zu lassen, statt sie – wie früher – sequenziell nacheinander abzuarbeiten.

Die Digitalisierung der Welt ist Teil einer Sicherheitsstrategie, die Unsicherheiten zu bewältigen und Risiken durch Kontrolle und Überwachung zu vermeiden versucht, damit aber zugleich auch Spielräume einengt, die einerseits eine Ressource für flexibles Handeln sind, andererseits aber auch Freiheiten beinhalten, die durch datengetriebene Prozesse tendenziell eingeschränkt werden. Die prekäre Balance von Autonomie und Kontrolle, die Teil unserer freiheitlichen Gesellschaft ist, droht so, aus dem Gleichgewicht zu geraten.

Ein wesentlicher Teil des Diskurses über die Risiken der Digitalisierung dreht sich um Fragen des zukünftigen Funktionserhalts von Infrastrukturen und des Datenmissbrauchs bzw. des Schutzes der Privatsphäre.

Die Infrastruktursysteme der Zukunft sind durch vielfältige und teilweise neuartige Interaktionen technischer, sozialer, organisationaler, regulatorischer und normativer Komponenten geprägt; sie gewinnen dadurch beträchtlich an Komplexität. Komplexe Systeme bestehen typischerweise aus einer großen Anahl von Komponenten, deren Interaktionen nur schwer zu durchschauen sind. Hier benötigt es zukünftig mehr Forschung, um neue Erkenntnisse zu generieren.

Denn die Ursachen übersteigerten Vertrauens verweisen auf eine Ironie der Automation: Je zuverlässiger die Systeme werden, desto weniger Konsequenzen hat eine nachlässige Kontrolle der automatischen Systeme und desto seltener werden die Risiken eines derartigen Verhaltens sichtbar. Damit wächst aber die Gefahr, dass die Operierenden sich in falscher Sicherheit wiegen.

Der Diskurs zum Schutz privater Daten ist wichtig und es werden dringend Lösungen für die anstehenden Probleme gefunden werden müssen, doch ebenso wichtig ist es auch, den Blick auf die neuartigen Möglichkeiten der Echtzeit-Steuerung komplexer sozio-technischer Systeme zu werfen. Hier liegt ein gewaltiges Potenzial, das sich mit der Digitalisierung und Vernetzung der Prozesse in komplexen Systemen ergibt.

Die Frage, wie eine intelligente politische Steuerung der Echtzeit-Gesellschaft aussehen könnte, ist noch weitgehend ungeklärt. Die Rolle des Staates besteht darin, dafür zu sorgen, dass die Funktionsfähigkeit kritischer Infrastruktursysteme aufrechterhalten wird. Aber er kann dies nicht mehr mit klassischen obrigkeitsstaatlichen Instrumenten tun, sondern er muss neue Formen einer intelligenten Steuerung und Regulierung entwickeln, die der Komplexität der Echtzeit-Gesellschaft gerecht werden.

Johannes Weyer (2018). Digitale Transformation und öffentliche Sicherheit.
Schriftenreihe Sicherheit, Nr. 23. Forschungsforum Öffentliche Sicherheit, Freie Universität Berlin.

Print: 978-3-96110-040-8 Online: 978-3-96110-041-5
Die Vollversion der Studie ist erhältlich unter www.schriftenreihe-sicherheit.de

---

Das 2009 an der Freien Universität Berlin gegründete Forschungsforum Öffentliche Sicherheit (www.sicherheit-forschung.de) führt Forschung unterschiedlicher Disziplinen zu sicherheitsrelevanten Themen zusammen und trägt dazu bei, zukünftig relevante Forschungsthemen zu identifizieren. Hauptsächlich geschieht dies durch Workshops und Expertisen zu verschiedenen Facetten der Sicherheitsforschung. Ziel ist es, wissenschaftliche Handlungsempfehlungen aus diesem heterogenen Feld zu generieren und für Politik, Industrie, und Organisationen der Sicherheit zugänglich zu machen. Die Idee zu diesem Projekt entstand auf Anregung des am Bundestag gegründeten Zukunftsforums Öffentliche Sicherheit e.V., dem Abgeordnete aller Parteien sowie Stakeholder aus Behörden, Wirtschaft und Wissenschaft angehören.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Forschungsforum Öffentliche Sicherheit

Freie Universität Berlin

Impressum: Forschungsforum Öffentliche Sicherheit
Freie Universität Berlin
Carl-Heinrich-Becker-Weg 6–10
12165 Berlin

Tel: +49 - (0)30 - 838 573 67
Fax: +49 - (0)30 - 838 4 573 67
www.schriftenreihe-sicherheit.de
kontakt@schriftenreihe-sicherheit.de