Technologiemonitoring zur Prävention von Extremismus und terroristischer Gewalt

Isabel Kusche und Christian Büscher

Beitrag zur Veranstaltung »Die Logik des Verdachts I. Prävention als gesellschaftliche Selbstverständlichkeit« der Sektion Soziale Probleme und soziale Kontrolle

Einleitung

Die Überlegungen, die wir im Folgenden vorstellen möchten, sind im Rahmen des Verbundprojektes „Monitoringsystem und Transferplattform Radikalisierung" (MOTRA) entstanden, das im Dezember 2019 gestartet ist. Das Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) des KIT ist in diesem Verbund mit einem Teilprojekt vertreten, das die Rolle von Technologien im Zusammenhang mit Radikalisierung und Terrorismus beleuchten soll. Ziel ist es, aktuelle und zukünftige Technologieentwicklungen mit Blick darauf einzuschätzen, welchen Unterschied sie für die Kommunikation extremistischer Akteure, die Beobachtungsmöglichkeiten der Sicherheitsbehörden sowie für Störungen und Angriffe auf Schutzgüter machen. Gefördert wird der Verbund im Rahmen des Programms der Bundesregierung „Forschung für die zivile Sicherheit 2018–2023".

Diese Verankerung verweist auf Sicherheit als Wert der modernen Gesellschaft, die dennoch und eben deshalb ständig mit Unsicherheit umgehen muss. Sicherheitserwartungen werden insbesondere an die Politik adressiert, die oft auf Wissen setzt, das selbst unsicher ist. Die Sicherheitsforschung allgemein und der MOTRA-Verbund im Besonderen illustrieren diese Verschränkung von Sicherheit als anzustrebendem Zustand und der Suche nach neuem und deshalb unsicherem Wissen für den Umgang mit Unsicherheit im Zusammenhang mit Terrorismus, aber auch Naturkatastrophen oder Kriminalität.

Gleichzeitig ist hier offensichtlich nicht Sicherheit in allen Belangen des Lebens gemeint, insbesondere nicht ökonomische Sicherheit. Pat O'Malley (2009) spricht von unterschiedlichen Regimen der Sicherheit, die in derselben Gesellschaft zur gleichen Zeit Möglichkeiten und Grenzen politischen Handelns zu bestimmten Themen abstecken können. Am Beispiel der USA weist er für die Jahre nach dem 11. September auf den Kontrast hin, der zwischen einer Fülle technokratischer illiberaler Maßnahmen besteht, die mit dem Ziel der Terrorismusbekämpfung gerechtfertigt wurden, und einer ungebrochen neo-liberalen Wirtschafts- und Sozialpolitik. Letztere geht davon aus, dass Unsicherheit nötig ist, um Unternehmergeist anzuregen und die wirtschaftliche Entwicklung voranzutreiben. In jüngster Zeit steht insbesondere das Silicon Valley für diese Verknüpfung von Unsicherheit und Innovationskraft. Das illustrieren Buchtitel wie *The Silicon Valley Edge: A Habitat for Innovation and Entrepreneurship* (Lee et al. 2000), *The Silicon Valley Model: Management for Entrepreneurship* (Steiber, Alänge 2016) oder

Silicon Valley als unternehmerische Inspiration: Zukunft erforschen – Wagnisse eingehen – Organisationen entwickeln" (Müller-Friemauth, Kühn 2016).

Nun sind es eben jene technischen Innovationen, die mit dem Silicon Valley verbunden sind, die zunehmend dafür verantwortlich gemacht werden, dass sich extremistisches Gedankengut verbreiten kann, terroristische Netzwerke von den Sicherheitsbehörden schwer aufzuspüren sind und Einzelpersonen ohne direkte Kontakte zu Terrorist*innen willens und in der Lage sind, Anschläge zu begehen. Vor diesem Hintergrund ist es einerseits folgerichtig, im Rahmen eines Monitorings von Radikalisierungsprozessen auch ein Technologiemonitoring zu betreiben, das die Rolle von Technologien und technologischen Innovationen in diesem Zusammenhang in den Blick nimmt. Andererseits impliziert ein solches Technologiemonitoring unvermeidlich, dass zwei Regime der Sicherheit miteinander in Berührung kommen, die sonst durch die vertraute Einteilung von Politikfeldern auseinandergehalten werden: nämlich das Regime der zivilen Sicherheit, das auf Prävention nach der Logik des Verdachts setzt, und ein liberales Regime der ökonomischen (Un-)Sicherheit, das Zukunftsoffenheit als Voraussetzung für weitere Innovation prämiiert. Unsere These ist, dass sich die Technikfolgenabschätzung, anders als andere Präventionsbemühungen, schon seit langem in diesem Spannungsfeld zwischen Verdacht und bejahter Zukunftsoffenheit[1] bewegt und Prävention mit einer Selbstreflexion kombiniert, die über die Logik des Verdachts hinausreicht.

Technikfolgenabschätzung als Ansatz der Prävention

Die Institutionalisierung von Technikfolgenabschätzung (TA) in Form von Organisationen, Konferenzen, Zeitschriften und Projekten lässt sich – etwas verkürzt – als Reaktion auf einen grundsätzlichen Verdacht gegen neue Technologien verstehen. Dieser Verdacht hat, mit unterschiedlichen Schwerpunkten und zu unterschiedlichen Zeitpunkten, ab Ende der 1960er Jahre in Nordamerika und verschiedenen Ländern Westeuropas Fuß gefasst. Er speiste sich aus der Erfahrung von unerwarteten und zum Teil schwerwiegenden Technikfolgen, die im Vorhinein nicht oder nicht hinreichend berücksichtigt worden waren.

Die Ursprungsgeschichte der Technikfolgenabschätzung ist daher mit der Erwartung verbunden, die sozialen, ethischen und politischen Konsequenzen neuer Technologien umfassend zu analysieren (Sadowski 2015, S.10). TA entwickelt dazu Theorien und Methoden, um etwas anderes zu sehen, als diejenigen Zwecksetzer, die erfinden, finanzieren oder nutzen (Bechmann 2007, S.35). TA operiert deshalb mit einer dreifachen Unterscheidung von Risiko, Gefahr und Chance. Jeder Technikeinsatz ist mit Chancen und Risiken verbunden, also Entscheidungen über die Entwicklung, Implementierung und den Betrieb von technischen Anlagen. Die Folgen dieser Entscheidungen sind nicht immer präzise abschätzbar, vor allem bei sogenannten *new emerging technologies* (Nanotechnologie, Synthetische Biologie etc.), die nicht immer ausschließlich in geschützten Räumen auf ihre Sicherheit hin erschöpfend getestet werden können, die in komplexe ökologische oder organische Systeme eingreifen, oder deren Gefahrenpotenziale erst in mittelbarer Zukunft erkennbar werden. In vielen Fällen müssen Entscheider*innen mit einem gehörigen Maß an Nicht-Wissen rechnen, das auch und gerade durch das stetig steigende Auflösevermögen der Wissenschaft immer weiter in das Bewusstsein vorrückt und dadurch kognitive und moralische Herausforderungen evoziert (Luhmann 1992).

[1] Anders ausgedrückt (Makropoulos 1990): zwischen Kontingenzbewältigung als Kontingenzvermeidung und Kontingenzverarbeitung als Kontingenzmanagement

Gängige Charakterisierungen des Modus präventiven Handelns beschreiben insofern zunächst auch die Perspektive der TA durchaus treffend. So hält etwa Ulrich Bröckling fest, dass „[d]as vorbeugende Verhältnis zur Zukunft […] gekennzeichnet [ist] durch einen aktivistischen Negativismus: Nicht Fortschritt zum Besseren, sondern Vermeidung künftiger Übel" (Bröckling 2015, S.30). Aber auch wenn diese Haltung den Ausgangspunkt von TA treffend erfasst, ist sie mit Blick auf Technologieentwicklung mit zwei Schwierigkeiten konfrontiert. Erstens stößt ein Denken in Populationen und Wahrscheinlichkeiten, wie es für den präventiven Blick sonst typisch ist, hier an Grenzen. Der Blick auf neue Technologien ist notwendig ein individualisierender, der die einzelne Technologie – wie schwierig auch immer eine solche Abgrenzung konkret sein mag – nicht dadurch bewerten kann, dass er sie mit einer Vielzahl ähnlicher Fälle vergleicht und auf dieser Basis Risiken probabilistisch erfasst. Die mit neuen Technologien verbundene Unsicherheit über ihre Folgen verweigert sich der Kalkulation.

Hinzu kommt ein zweiter Punkt: Den Verdacht gegenüber einer neuen Technologie darin zu gründen, dass man es mit der Abweichung von einer zur Norm gewordene Normalität zu tun hat, wäre gleichbedeutend damit, technologische Innovationen, die ja durch ihre Neuheit unvermeidlich abweichend sind, generell zum Problem zu erklären. Eben eine solche Innovationsfeindlichkeit ist der TA tatsächlich gerne vorgeworfen worden. Konzeptionell reagiert sie auf diesen Vorwurf bzw. dessen Antizipation mit dem Hinweis darauf, dass Technikfolgen neben Risiken immer auch Chancen umfassen (Bechmann 2007; Grunwald 2008), oder mit dem Verfolgen von Ansätzen wie Responsible Research and Innovation (Nierling, Udén 2020). TA verweist insofern stets auf das Problem des Entscheidens unter Unsicherheit, die positive wie negative Folgen von Technologien und von Entscheidungen für oder gegen eine bestimmte Technologie umfasst.

Dabei sind zwar bestimmte Basiserwartungen aus politischer und rechtlicher Sicht klar, nämlich einerseits die der Gefahrenabwehr und andererseits die der Nicht-Verhinderung nützlicher Innovationen. Aber die Unterscheidung zwischen (nützlichen) Zwecken und zu vermeidenden Nebenfolgen einer Technologie ist kaum durchzuhalten, sobald mitbedacht wird, dass sich im Laufe der Technikgenese und -verwendung Zwecke verändern, mehrere Technologien rekombinieren lassen oder eine Technologie innovativ – im Sinne von nicht-bestimmungsgemäß – gebraucht werden kann. Risiko ist unter solchen Umständen kein Rationalisierungskalkül, sondern eine Frage der Zurechnung von Entscheidungen und damit von Verantwortung.

Der Struktur gebende Gegenwert von Risiko steckt in dem Begriff der Gefahr (Luhmann 1991). Während Risiken auf die Folgen des eigenen Entscheidens zugerechnet werden, werden Gefahren externen Faktoren (Natur) oder den Entscheidungen anderer zugerechnet. Daraus leiten sich unterschiedliche Beobachterperspektiven ab, nämlich die der Entscheider und der Betroffenen. Für beide ergeben sich jeweils andere kommunikative Anschlussmöglichkeiten und Folgenbewertungen, und zwar bezogen auf dieselbe Situation (risikobehaftete Zweckverfolgung auf der einen und Gefahrenablehnung auf der anderen Seite).

Technologiegebrauch im Kontext von Extremismus und Terrorismus

Was bedeutet es nun, wenn man sich der Rolle von Technologien für die Prävention von Extremismus und Terrorismus aus der Perspektive der TA nähert? Zunächst wird der Bezug zu Entscheidungen und damit verbundenen Risiken augenfällig, und zwar unabhängig davon, ob man im Interesse von Innovation für Zukunftsoffenheit als Wert optiert oder für Sicherheit. Auf den ersten Blick scheint ausschließlich Innovation einen bias in Richtung Risiko aufzuweisen, das zur Gefahr für andere werden kann,

wenn etwa ein Messenger-Dienst wie Telegram zum Tummelplatz für extremistische und terroristische Akteure wird. Auf den zweiten Blick kann man aber erkennen, dass auch Akteure der zivilen Sicherheit gezwungen sind, riskante Entscheidungen zu treffen. Die rechtlich festgelegte Aufgabe (Verantwortlichkeit) und die Erwartungen einer politisierten Öffentlichkeit und einer öffentlichkeitssensiblen Machtpolitik treibt Sicherheitsbehörden dazu, umfangreiche Zweckprogramme aufzusetzen. Belohnt wird hier die erfolgreiche Abwehr von Gefahren (wenn auch nur symbolisch in der Darstellung von Handlungsfähigkeit oder in geschönten Statistiken). Riskant ist insbesondere Untätigkeit, da diese keinen Schutz gegen die Diagnose des Versagens bietet, falls Schadensereignisse und abweichendes Verhalten nicht verhindert werden. Diese Präferenz für Sicherheit aber kann ebenfalls zur Gefahr werden.

Beispiel Tor-Projekt

Da wir mit unserem Technologiemonitoring noch am Anfang stehen, möchten wir die von der TA inspirierte Perspektive hier erst einmal retrospektiv ausprobieren, und zwar für das Beispiel des Tor-Browsers. Dabei handelt es sich um eine Software, die zweierlei leistet: Erstens ermöglicht sie es, sich im normalen Internet anonym zu bewegen, also konventionelle Adressen im World Wide Web anzusteuern, ohne dass diese oder Dritte die IP-Adresse beobachten können, von der der Zugriff erfolgt. Zweitens erlaubt Tor das Hosten von Diensten, die als verborgene Websites mit der Endung *.onion mit normalen Browsern und Suchmaschinen nicht gefunden werden können. Die ursprüngliche Idee dahinter war, einen effektiven Schutz gegen Denial-of-Service-Attacken anzubieten. *.onion-Sites bieten aber auch zusätzliche Vorteile in Sachen Sicherheit: Sie erhöhen die Privatheit von Kontakten, weil beide Parteien sich dabei im Tor-Netzwerk aufhalten; sie verbessern die Authentifizierung von Kommunikation, weil sie sogenannte Man-in-the-Middle-Attacken sehr viel schwieriger machen. Daher bieten beispielsweise Zeitungen dort Whistleblower*innen die Möglichkeit, mit ihnen in Kontakt zu treten und Informationen weiterzugeben (Moore, Rid 2016, S.28). Die verborgenen Websites (hidden services) bilden also ein Darknet, das für verschiedenste Zwecke genutzt werden kann. Dazu gehören insbesondere Drogenhandel und Kinderpornographie. Ein Beispiel für die Nutzung durch Terrorist*innen ist eine *.onion-Site, die der IS 2015 als Archiv für Propagandamaterial eingerichtet hat (Weimann 2016, S.41).

Tor wurde ursprünglich vom US-amerikanischen Naval Research Laboratory (NRL) in Kooperation mit dem Free-Haven-Projekt, einer Non-Profit-Organisation, entwickelt (Moore, Rid 2016, S.16). Dem NRL ging es darum, Angehörigen des Militärs während Operationen im Ausland anonyme Kommunikation im Internet zu ermöglichen. 2003 wurde Tor als Open-Source-Browser der Öffentlichkeit zur Verfügung gestellt. Die Idee dahinter war, die militärische Kommunikation inmitten einer Vielzahl ziviler Nutzer*innen verbergen zu können (Chertoff 2017, S.27). Gleichzeitig wurde auf diese Weise ein dezentralisiertes, anonymisiertes Netzwerk geschaffen, wie es den Ideen des Free-Haven-Projektes entsprach. Aus der Perspektive der Entwickler*innen ist die Nutzung des Netzwerkes für kriminelle oder terroristische Zwecke insofern ein Fall von nicht-bestimmungsgemäßem Gebrauch der Technologie. Es ist aber klar, dass das für die Bewertung der Technikfolgen keine Rolle spielt. Was ex ante insbesondere niemand vorhersah, war die Kombination von Tor mit einer anderen Technologie, die erst einige Jahre später erfunden wurde, nämlich Bitcoin, eine pseudonyme Kryptowährung, die kriminelle Transaktionen im Darknet erst richtig praktikabel machte (Chertoff 2017, S.28).

Allen Einschätzungen und den vom Tor-Projekt selbst gemachten Angaben zufolge nutzt die weit überwiegende Zahl der Tor-Nutzer die Software, um Seiten im normalen Internet anonym anzusteuern. Der Anteil der verborgenen Dienste am gesamten Tor-Verkehr wird nur auf 3–6% geschätzt (Moo-

re, Rid 2016, S.16). Hinzu kommt, dass die Größe des Darknets im Vergleich zum sichtbaren Internet geradezu winzig ist. Verschiedene Studien schätzen die Zahl der zu einem beliebigen Zeitpunkt aktiven *.onion-Adressen auf nicht mehr als 30.000 bis 45.000 (Jardine 2018, S.2829).

In einer Umfrage unter mehr als 17.000 Internetnutzer*innen aus 17 Ländern 2016 sprachen sich allerdings 73% der Befragten dafür aus, das Darknet komplett abzuschaffen, nachdem ihnen dessen legitime und illegitime bzw. illegale Verwendungsweisen genannt worden waren. Das Ergebnis der Umfrage bekam große Medienaufmerksamkeit und floss in laufende Debatten zum Umgang mit Verschlüsselungstechnologien in verschiedenen Ländern ein (Jardine 2018, S.2826). In die Medienberichterstattung eines interessierten Nischenpublikums schafften es Meldungen, dass Geheimdienste in der Lage sind, auch Tor-Nutzer zu de-anonymisieren, oder dass die amerikanische National Security Agency (NSA) bereits das Herunterladen des Tor-Browsers registriert und als Verdachtsmoment behandelt (Meister 2017).

Insgesamt entsteht so das Bild einer verdächtigen Technologie. Entsprechend niedrig sind die weltweiten Nutzerzahlen: Tor Metrics (o. J.) zufolge schwanken sie zwischen zwei und drei Millionen. Die Prävention von extremistischen, terroristischen und anderen Straftaten ist unter diesen Bedingungen schwierig, weil das insgesamt genügend Aktivität bedeutet, um Kommunikationen im Zusammenhang mit illegalen Handlungen in der Masse der anonymen Nutzer*innen verbergen zu können. Insofern wäre ein plausibles Minimalziel aus dieser präventiven Perspektive, dass sich die Nutzung von Tor nicht noch stärker verbreitet. Damit wird allerdings auch erhebliches Innovationspotential verschenkt, wenn man bedenkt, dass das Geschäftsmodell der wenigen großen Internetkonzerne, die inzwischen dominieren, darauf beruht, dass Nutzer*innen im Internet nicht anonym browsen, sondern mit Hilfe von verschiedenen Tracking-Technologien identifiziert und mit personalisierter Werbung versorgt werden (Zuboff 2019). Zugegebenermaßen stehen der Verwendung des Tor-Browsers durch eine Mehrheit der Internetnutzer*innen nach jetzigem Stand auch technische Probleme der Kapazität und Stabilität entgegen. Aber diese wären vielleicht längst gelöst, wenn die Technologie nicht selbst als verdächtig gelten würde. Falls diese (oder andere) Anonymisierungstechniken weite Verbreitung gefunden hätten, könnte die Gestalt des digitalen Kapitalismus eine ganz andere sein.

Ausblick

Es stellt sich also die Frage, wie die möglichen Folgen (voraussichtlich) nützlicher Technologie hinsichtlich Gefährdungen ziviler Sicherheit abgeklärt werden können. Aus den gerade skizzierten Überlegungen ergibt sich zunächst, welche Unterscheidungen dafür ungeeignet sind: Zunächst ist das die Unterscheidung norm(al)/abweichend, die weder auf der Basis einer vorab fixierten Norm noch im Sinne statistischer Muster in der Lage ist, Orientierung zu bieten, wenn es um technologische Innovationen geht. Als ebenso ungeeignet erweist sich allerdings auch die klassische Unterscheidung der Technikfolgenabschätzung zwischen intentionalen und nicht-intentionalen Folgen von Technologien. Im Zusammenhang mit Extremismus und Terrorismus geht es schließlich um intentionale Folgen der Rekombination von Technologien und des (im Sinne der Entwicklerinnen und Entwickler) „nicht-bestimmungsgemäßen Gebrauchs“. Unser Vorschlag ist eine funktionale Perspektive, die danach fragt, inwieweit neu entstehende Technologien soziale Koordinationsprobleme lösen, die für extremistische und terroristische Akteure zentral sind. Das Problem anonymer und gleichzeitig authentifizierbarer Kommunikation, für das das Tor-Netzwerk eine Lösung darstellt, ist dafür ein Beispiel.

Literatur

Bechmann, Gotthard. 2007. Die Beschreibung der Zukunft als Chance oder als Risiko? – TA zwischen Innovation und Prävention. *TATuP* 16:34–44.

Bröckling, Ulrich. 2015. Der präventive Imperativ und die Ökonomisierung des Sozialen. *Public Health Forum* 21:29–31.

Chertoff, Michael. 2017. A public policy perspective of the Dark Web. *Journal of Cyber Policy* 2:26–38.

Grunwald, Armin. 2008. Technikfolgenabschätzung als wissenschaftliche Politikberatung. In *Politikberatung. Ein Handbuch*. Stuttgart: Lucius & Lucius.

Jardine, Eric. 2018. Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies. *New Media & Society* 20:2824–2843.

Lee, Chong-Moon, William F. Miller, und Marguerite Gong Hancock, Hrsg. 2000. *The Silicon Valley edge: a habitat for innovation and entrepreneurship*. Stanford, Calif: Stanford University Press.

Luhmann, Niklas. 1992. Ökologie des Nichtwissens. In *Beobachtungen der Moderne*, 149–220. Opladen: Westdeutscher Verlag.

Luhmann, Niklas. 1991. *Soziologie des Risikos*. Berlin; New York: W. de Gruyter.

Makropoulos, Michael. 1990. Möglichkeitsbändigungen: Disziplin und Versicherung als Konzepte zur sozialen Steuerung von Kontingenz. *Soziale Welt* 41:407–423.

Meister, Andre. 2017. Der BND hat das Anonymisierungs-Netzwerk Tor angegriffen und warnt vor dessen Nutzung. https://netzpolitik.org/2017/geheime-dokumente-der-bnd-hat-das-anonymisierungs-netzwerk-tor-angegriffen-und-warnt-vor-dessen-nutzung/ (Zugegriffen: 01. Juni 2021).

Moore, Daniel, und Thomas Rid. 2016. Cryptopolitik and the Darknet. *Survival* 58:7–38.

Müller-Friemauth, Friederike, und Rainer Kühn. 2016. Silicon Valley als unternehmerische Inspiration: Zukunft erforschen – Wagnisse eingehen – Organisationen entwickeln. Wiesbaden: Springer Fachmedien Wiesbaden.

Nierling, Linda, und Maria Udén. 2020. There is no all-in-one solution – The challenges of inclusive and sustainable innovation processes. In *Die neutrale Normativität der Technikfolgenabschätzung. Konzeptionelle Auseinandersetzung und praktischer Umgang*, Hrsg. Linda Nierling und Helge Torgersen, 139–153. Baden-Baden: Edition Sigma, Nomos.

O A. o. J. Tor Metrics. https://metrics.torproject.org/ (Zugegriffen: 28. Juli 2020).

O'Malley, Pat. 2009. "Uncertainty makes us free". Liberalism, risk and individual security. *BEHEMOTH – A Journal on Civilisation* 2:24–38.

Sadowski, Jathan. 2015. Office of Technology Assessment: History, implementation, and participatory critique. *Technology in Society* 42:9–20.

Steiber, Annika, und Sverker Alänge. 2016. *The Silicon Valley Model: Management for Entrepreneurship*. 1st ed. 2016. Cham: Springer International Publishing: Imprint: Springer.

Weimann, Gabriel. 2016. Terrorist Migration to the Dark Web. *Perspectives on Terrorism* 10:40–44.

Zuboff, Shoshana. 2019. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: PublicAffairs.