Karlsruher Institut für Technologie

Trends der zukünftigen Technologienutzung im Kontext von Extremismus und Terrorismus: erste Erkenntnisse aus dem MOTRA-Technologiemonitoring

Christian Büscher, Isabel Kusche, Tim Röller, Florian Andres, Alexandros Gazos, Julia Hahn, Miltos Ladikas, Octavia Madeira, Georg Plattner, Constanze Scherz

Phänomenmonitoring

Zusammenfassung

*Dieser Beitrag beleuchtet technologische Trends, die für das Radikalisierungs- und Extremismusgeschehen relevant werden können. Technologien können von extremistischen Akteur*innen zur Kommunikation (Anbahnung, Koordination, Vernetzung, Verbreitung von Propaganda) oder als Stör-, Terror- oder Angriffsinstrument eingesetzt werden. Die Art und Weise, wie Technik zum Einsatz gebracht werden kann, unterscheidet sich wiederum deutlich, nämlich einmal in Form des Missbrauchs, ein anderes Mal in Form der Rekombination verschiedener technologischer Elemente oder gar als Erfindung neuer technischer Möglichkeiten. Um mehr darüber zu erfahren, ob und wie Technologien in naher Zukunft nützlich sein beziehungsweise zur Verfügung stehen könnten, haben wir eine Expert*innen-Befragung in Form eines zweistufigen Online-Delphis durchgeführt. Die Befragung erfasste in der ersten Runde Einschätzungen von internationalen Expert*innen zu zukunftsrelevanten Themen. In der zweiten Runde wurden die gleichen Fragen inklusive des Feedbacks zu den Ergebnissen der ersten Runde einbezogen. Die Ergebnisse werden zur Priorisierung der Technologien für eine detaillierte Analyse verwendet, die sich an dem Grad der Funktionalität und der Verfügbarkeit für extremistische Akteur*innen orientiert.*

*Ein weiterer Schwerpunkt unserer Arbeit zielt auf technologische Trends rund um die Möglichkeiten und Grenzen der Beobachtung von Personen und (physischen oder digitalen) Orten seitens der Organisationen mit Sicherheitsaufgaben ab. Auch in diesem Feld sind die technischen Entwicklungen enorm. Mithilfe von Sensoren, Kameras und Informationstechnik werden Unmengen an Daten generiert, aus denen handlungsweisende Informationen abgeleitet werden müssen. Diese Aufgabe wird in immer größerem Umfang mit Unterstützung von Algorithmen vorgenommen. Inwieweit die Ergebnisse einer automatisierten Auswertung als Entscheidungsgrundlage herhalten oder gar in übergeordnete Handlungsstrategien Einzug halten, hängt nicht nur von der Funktionalität und Zuverlässigkeit der Systeme ab. Auch die Kenntnisse der Anwender*innen im Umgang mit den komplizierten Systemen und das Vertrauen in die teilweise*

*intransparenten technischen Prozesse sind wesentliche Variablen. In einem Expert*innen-Workshop haben wir Einschätzungen zu den aktuellen Problemen mit bestimmten Beobachtungstechnologien erhoben. Dort wurden vor allem die funktionalen Grenzen aktueller Technik als Entscheidungs- und Handlungsunterstützung für Interventionen erörtert sowie die durch gesellschaftliche Diskurse vermittelten Grenzen für den Technikeinsatz.*

Stichworte

Radikalisierung | *Extremismus* | *Terrorismus* | *Technologien* | *Innovation* | *Technikfolgen* | *Delphi-Studie* | *Sicherheitsbehörden* | *Beobachtungstechnologien*

Einleitung

Das MOTRA-Technologiemonitoring beobachtet die Relevanz von Technologien im Problemfeld Radikalisierung und Extremismus in drei Schritten, die bei kontinuierlichem Monitoring immer wieder durchlaufen werden. In einem ersten Schritt – dem Grobradar – geht es darum, ein Überblickswissen zu einer Reihe technologischer Entwicklungen zu sammeln, die möglicherweise relevant sind. Die Einschätzung der tatsächlichen Relevanz wird im zweiten Schritt mithilfe von externen Expert*innen oder Stakeholdern vorgenommen, die im Rahmen von Workshops oder anderen Formaten mit Szenarien zu möglichen Effekten bestimmter Technologien im Themenfeld Radikalisierung und Extremismus konfrontiert werden. Ziel dieses zweiten Schrittes ist es, eine auf Expert*innenwissen basierende Priorisierung vorzunehmen, um jene Technologien zu identifizieren, die in vertiefenden Studien einer Feinanalyse unterzogen werden sollen. Dieser dritte Schritt nimmt als Feinradar ausgewählte Technologien genauer in den Blick, um ihre zukünftige Bedeutung für Radikalisierung, Extremismus und Akteur*innen ziviler Sicherheit, die auf diese Phänomene reagieren, auszuloten (Kusche et al. 2021).

In diesem Bericht präsentieren wir Ziele, Methoden und Ergebnisse unterschiedlicher Formate der Erhebung von Einschätzungen zu zukünftigen Entwicklungen von Technologien. Zum einen stellen wir heraus, wie wir mit einer Delphi-Studie zu Einsichten über relevante Technologieentwicklungen, die möglicherweise in Zukunft Extremist*innen beziehungsweise Terrorist*innen zur Verfügung stehen könnten, gekommen sind (Abschnitt 2). Zum anderen eruieren wir komplementär zu dieser Perspektive die Möglichkeiten und Probleme in der Nutzung von Beobachtungstechnologien auf Seiten der Akteur*innen der zivilen Sicherheit mithilfe eines Expert*innen-Workshops (Abschnitt 3). Zum Ende verweisen wir auf weitere Aktivitäten zur Detektion relevanter Technologietrends wie der Forcierung von extended reality und des „Metaverse“ (Abschnitt 4).

Delphi-Studie

Zielstellung

Die Zielstellung der Delphi-Studie ergibt sich aus dem übergeordneten Ziel, ein Technologiemonitoring im Problemfeld Radikalisierung und Extremismus durchzuführen, das neue Technologien und deren Folgen identifiziert, sofern sie für dieses Problemfeld relevant sind. Es gibt drei wesentliche Gründe für die Vermutung, dass es neue technologische Entwicklungen mit solcher Relevanz gibt (Kusche et al. 2021):

1. Extremistische Akteur*innen haben sich in den letzten Jahren solche Entwicklungen, insbesondere im Bereich des Internets, wiederholt zunutze gemacht, um ihre Ziele zu verfolgen.

2. Die zunehmende Vernetzung und Konvergenz von Technologien, die als Infrastrukturen viele gesellschaftliche Routinen überhaupt erst ermöglichen, schaffen potenzielle neue Vulnerabilitäten, die extremistische Akteur*innen ausnutzen könnten.

3. Neue Technologien können auch neue Handlungsmöglichkeiten für Sicherheitsbehörden schaffen, deren gesellschaftliche Wünschbarkeit aber einer kontinuierlichen kritischen Prüfung bedarf, denn das Streben nach mehr Sicherheit kann andere zentrale Werte demokratischer Gesellschaften schwächen oder sogar unterminieren.

Die mögliche Relevanz neuer technologischer Entwicklungen hängt sowohl von deren Verfügbarkeit (Technology-Push-Perspektive) als auch von dem Bedarf (Demand-Pull-Perspektive) ab, den die Akteur*innen im Problemfeld Radikalisierung und Extremismus an bestimmten Technologien haben.

Die Delphi-Studie konzentriert sich im Zuge des zweiten Schrittes des Monitoringprozesses mit dem Ziel einer Priorisierung von Technologien für vertiefende Analysen auf die Relevanz technologischer Entwicklungen für jene Akteur*innen, die extremistische oder gar terroristische Ziele verfolgen. Ausgangsannahme ist, dass Handlungen und Kommunikationen, die ausdrücklich Aspekte der freiheitlich demokratischen Grundordnung ablehnen oder gar Aktivitäten vorbereiten, die sich gewaltförmig gegen

diese Grundordnung richten, von bestimmten technologischen Entwicklungen in besonderer Weise profitieren können. Neue Technologien können es extremistischen und terroristischen Akteur*innen erleichtern, ihre Kommunikation einerseits selektiv Dritten – in Form von Propaganda – zugänglich zu machen und andererseits selektiv vor der Beobachtung durch Dritte – speziell Sicherheitsbehörden – zu schützen. Darüber hinaus können neue Technologien auch die Planung und Durchführung von Gewalttaten begünstigen. Für ein Technologiemonitoring ergibt sich damit eine doppelte Herausforderung. Zum einen kommt es darauf an, möglichst frühzeitig jene technologischen Entwicklungen zu identifizieren, die für extremistische und terroristische Akteur*innen nützlich sein könnten. Zum anderen ergibt sich eine mögliche Nützlichkeit nicht aus der vorgesehenen Funktions- und Verwendungsweise der Technologien selbst. Extremistische und terroristische Akteur*innen können – wie andere Akteur*innen auch, aber eben vor dem Hintergrund ihrer spezifischen Ziele – im Zuge der Technikverwendung Zwecke verändern, mehrere Technologien rekombinieren oder eine Technologie nicht bestimmungsgemäß innovativ gebrauchen.

Wissen zur zukünftigen Techniknutzung durch extremistische und terroristische Akteur*innen ist inhärent unsicher, sowohl wegen seines Zukunftsbezugs als auch, weil eine direkte Befragung solcher Akteur*innen zum Thema praktisch ausgeschlossen ist. Deshalb ist dieses unsichere Wissen im Überschneidungsbereich zweier Felder von Expertise angesiedelt. Zum einen ergibt sich solches Wissen aus einer technischen Expertise, die mögliche Verwendungsweisen neuer Technologien und den zeitlichen Horizont ihrer Verbreitung abschätzen kann. Zum anderen ist es mit Expertise aus dem Bereich der Forschung zu Radikalisierung, Extremismus und Terrorismus verknüpft, die die Nützlichkeit von Technologien für extremistische und terroristische Akteur*innen vor dem Hintergrund ihrer typischen Handlungs- und Organisationsmuster sowie wahrscheinlicher Handlungsalternativen einschätzen kann.

Methode

Die Delphi-Methode ist ein Verfahren, das aus der Zukunftsforschung stammt und ursprünglich für die Erstellung von Prognosen genutzt wurde. Die Grundidee ist, dass Expert*innen im Rahmen eines relativ stark

strukturierten Gruppenkommunikationsprozesses Sachverhalte bewerten, über die nur unsicheres, unvollständiges Wissen vorhanden ist (Häder 2014, 22). Expert*innen werden in mindestens zwei Runden zu Themen mit Zukunftsbezug und entsprechender Unsicherheit befragt. Dabei kommen meist sowohl geschlossene Fragen als auch offene Fragen zur Anwendung. In einer zweiten Runde werden den Befragten die in der ersten Runde gegebenen Antworten in geeigneter Form zurückgemeldet, woraufhin sie erneut darum gebeten werden, die Fragen zu beantworten. Dahinter steht die Annahme, dass sich die Einschätzungen zu unsicheren Sachverhalten im Verlauf einer Delphi-Befragung durch das Feedback in einer anonymen Kommunikationssituation verbessern (Häder 2014, 39-58). Die Anonymität mindert dabei spontane Gruppenprozesse zugunsten gezielter Modifikation und kontrollierter Bedingungen (Häder 2014, 61).

Seit ihren Anfängen hat sich die Delphi-Methode ausdifferenziert, sodass sich viele Varianten des Verfahrens etabliert haben, die mit unterschiedlichen Zielstellungen verbunden sind. Sie unterscheiden sich insbesondere darin, welchen Stellenwert eine mögliche Annäherung von Expert*innen-Meinungen im Verlauf des Delphi-Prozesses hat. Trotz der Vielfalt lassen sich vier grundlegende Typen von Zielen von Delphi-Studien unterscheiden (Häder 2014, 31–37): 1. Ideenaggregation, 2. Konsensbildung, 3. Ermittlung und Annäherung der Ansichten von Expert*innen über einen diffusen Sachverhalt, 4. Forecasting im Sinne einer möglichst exakten Vorhersage oder genauen Bestimmung eines unsicheren Sachverhaltes.

Die Frage nach der möglichen Relevanz neuer technischer Entwicklungen für extremistische und terroristische Akteur*innen entspricht der zuletzt genannten Zielstellung. Daraus ergeben sich bestimmte Konsequenzen für die Konzeption des Delphis und die Auswahl der teilnehmenden Expert*innen (Häder 2014, 107–112). Ausschlaggebend für diese Auswahl ist die Frage, wo Expertise zur Problemstellung zu erwarten ist. Die Bestimmung einer Grundgesamtheit von Expert*innen ist in diesem Zusammenhang kaum möglich. Außerdem steigt die Güte einer solchen Delphi-Studie nicht automatisch mit der Zahl der Befragten; sie hängt vielmehr davon ab, dass man jene Expert*innen identifiziert, die besonders gut zur Problemstellung Auskunft geben können, selbst wenn es sich dabei um eine relativ kleine Gruppe handeln sollte.

Die Funktion des Feedbacks von Befragungsergebnissen liegt in diesem Zusammenhang darin, zusätzliche kognitive Prozesse bei den Teilnehmer*innen auszulösen, sodass sie ihre ursprünglichen Urteile reflektieren und gegebenenfalls modifizieren. Fehlender Konsens auch nach Feedback zeigt große Unsicherheit der betreffenden zukunftsbezogenen Einschätzung an und kann nicht zuletzt als Hinweis auf die Notwendigkeit vertiefender Studien im Rahmen eines Technologiemonitorings verstanden werden.

*Auswahl und Rekrutierung von Expert*innen*

Als Teil des Technologiemonitorings stützte sich die Vorbereitung der Delphi-Studie auf die Auswertung einer Vielzahl von Literatur- und Internetquellen, die Beiträge zu und Hinweise auf relevante technologische Entwicklungen enthalten. Dazu gehören verschiedene Fachzeitschriften und periodische Veröffentlichungen zu den Themenfeldern Extremismus/Terrorismus einerseits und Technological Foresight andererseits, aber auch Internetblogs und Newsletter zum Thema Technologie und/oder Extremismus sowie Informationen von Nichtregierungsorganisationen. Die Auswertung dieser Quellen lieferte zum einen die Grundlage für die inhaltliche Konzeption der Studie. Zum anderen wurde sie genutzt, um einschlägige Expert*innen zu identifizieren, die für eine Teilnahme in Frage kamen. Dabei wurde eine enge Definition relevanter Expertise gewählt: Berücksichtigt wurden ausschließlich nationale und internationale Expert*innen, bei denen in Anbetracht ihrer eigenen Arbeiten oder ihrer Einbindung in entsprechende Projektzusammenhänge Expertise zur Rolle von Technologien im Feld von Extremismus und Terrorismus zu vermuten war.

Die Auswahl der in Frage kommenden Expert*innen erfolgte in einem strukturierten Prozess, der zu einem Pool von 64 Personen von allen Kontinenten führte, die per E-Mail zur Teilnahme an der Befragung eingeladen wurden. Trotz des Bemühens, auf Diversität des Pools zu achten, wies er ein klares Übergewicht männlicher Experten auf, die mit angelsächsischen Universitäten oder Thinktanks assoziiert waren; darin spiegelt sich im Wesentlichen die internationale Forschungslandschaft wider, wie sie in englischsprachigen Veröffentlichungen und institutionalisierten Forschungsnetzwerken zum Ausdruck kommt.

An der ersten Delphi-Runde nahmen 25 Personen – 21 Männer und vier Frauen – teil, die den Fragebogen vollständig ausfüllten. Von diesen 25 beteiligten sich wiederum 17 Personen – 15 Männer und zwei Frauen – auch an der zweiten und abschließenden Befragungsrunde bis zum Ende. Damit ergibt sich eine Rücklaufquote von 26,6 %. Das ist für eine Delphi-Befragung ungewöhnlich hoch und erklärt sich vermutlich aus der sehr gezielten Auswahl und Ansprache der Expert*innen, die dafür sorgte, dass Selbst- und Fremdwahrnehmung hinsichtlich relevanter Expertise sich besser deckten als bei anderen Delphi-Studien. Die geografische Verteilung der Teilnehmer*innen spiegelt das Ungleichgewicht im zugrunde gelegten Expertenpool wider (siehe Tabelle 1). Allerdings ist zu bedenken, dass die Nationalität der Expert*innen nicht unbedingt mit dem Land übereinstimmt, in dem sie tätig sind.

Tabelle 1
Verteilung der Befragten

Land, in dem die Befragten arbeiten	Anzahl 1. Runde	Anzahl 2. Runde
USA	9	6
Deutschland	4	3
Großbritannien	4	2
Australien	2	1
Norwegen	1	1
Polen	1	1
Rumänien	1	1
Spanien	1	1
Nigeria	1	1
Singapur	1	-

Operationalisierung

Zentrale Fragestellung der Delphi-Studie ist, welche neuen Technologien beziehungsweise technologischen Anwendungen in Zukunft für extremistische und terroristische Akteur*innen einerseits nützlich und andererseits

verfügbar sein werden. Auf der Grundlage von Literatur- und Internetrecherchen wurden dementsprechend relevante mögliche Verwendungsweisen neuer Technologien identifiziert, die in Form von geschlossenen Fragen in den Fragebogen aufgenommen wurden. Dabei handelt es sich um Anwendungen aus den folgenden Technologiekomplexen: künstliche Intelligenz/maschinelles Lernen, Blockchain, Internet der Dinge, Verschlüsselung und Anonymisierung von Kommunikation, 3D-Druck, Drohnen, synthetische Biologie sowie High-Performance Computing.

Die Benennung der Technologiekomplexe diente unter anderem dazu, zu Beginn des Fragebogens das Niveau der Expertise der Befragten bezüglich dieser Komplexe in Form von Selbsteinschätzungen zu erheben. Dabei gab es vier Optionen: Hohe Expertise war als aktive Arbeit zu dem jeweiligen Technologiekomplex definiert. Als mittleres Niveau von Expertise galt es, wenn Wissen auf dem Studium einschlägiger akademischer Publikationen oder dem Austausch mit Expert*innen beruhte. Sofern die Expert*innen mit dem Technologiekomplex nur durch Zeitungs- und populäre Zeitschriftenartikel vertraut waren, wurden sie gebeten, ihre Expertise als niedrig einzustufen. Befragte, die sich keine Expertise, das heißt kein Vorwissen, zu einem bestimmten Technologiekomplex zuschrieben, bekamen keine Fragen zu diesem gestellt.

In den geschlossenen Fragen zu den einzelnen Technologiekomplexen wurden die Expert*innen zum einen gebeten, die Nützlichkeit der Technologien für konkret benannte Zwecke einzuschätzen, die für extremistische Akteur*innen relevant sein können. Dazu wurden ihnen Aussagen vorgelegt, für die Antwortmöglichkeiten jeweils in Form einer fünfstufigen Likert-Skala präsentiert wurden, die von kompletter Zustimmung bis zu kompletter Ablehnung reichte. Zum anderen wurden die Expert*innen gebeten, den Zeithorizont einzuschätzen, innerhalb dessen die betreffenden Technologien für extremistische und terroristische Akteur*innen verfügbar sein werden. Hier gab es vier Antwortmöglichkeiten, die von „schon in Verwendung“ über „innerhalb der nächsten Dekade“ und „innerhalb der nächsten 25 Jahre“ bis „nicht in absehbarer Zukunft“ reichten. Ein Zeitraum von zehn Jahren entspricht dabei dem typischen Zeithorizont von Technikfolgenabschätzung und Prävention; ein Zeitraum von 25 Jahren ist typisch für Foresight-Studien.

Bei allen Fragen zur Nützlichkeit und Verfügbarkeit der untersuchten Technologieanwendungen hatten die Befragten jeweils auch die Möglichkeit, ihre Antwort mit einem Kommentar näher zu erläutern und zu begründen. Offene Fragen am Ende der Technologiekomplexe gaben allen Befragten darüber hinaus Gelegenheit, auch andere, bisher nicht genannte Technologien oder konkrete Anwendungen im betreffenden technologischen Feld zu benennen, die aus ihrer Sicht für extremistische und terroristische Akteur*innen relevant sein könnten. Zudem wurden die Expert*innen ganz am Ende des Fragebogens nach weiteren Technologien jenseits der thematisierten Technologiekomplexe gefragt, von denen sie glauben, dass sie in der Zukunft für extremistische und terroristische Akteur*innen nützlich und verfügbar sein werden, und sie wurden gebeten, ihre Antwort zu erläutern.

Die erste Befragungsrunde fand vom 25.9.20 bis 01.11.20 statt, die zweite vom 24.11.20 bis 11.01.21. In der zweiten Runde wurden den Befragten die Antworthäufigkeiten der ersten Runde zu Nützlichkeit und Verfügbarkeit mittels Balkendiagrammen angezeigt. Erläuterungen und Kommentare zu diesen Fragen wurden in Form von Synopsen in die zweite Runde eingespeist, ebenso die Antworten auf die offenen Fragen zu weiteren relevanten Technologien und Anwendungen.

Auswertung der Daten

Bei der Interpretation der Ergebnisse ist zu beachten, dass der relative Anteil von Expert*innen mit niedriger, mittlerer und hoher Expertise zwischen erster und zweiter Befragungsrunde nicht konstant ist. Das liegt zunächst daran, dass nicht alle Befragten auch an der zweiten Runde teilgenommen haben. Es gibt keine Anhaltspunkte dafür, dass diese Ausfälle systematisch sind, also zum Beispiel in der zweiten Runde Personen mit selbstzugeschriebener niedriger Expertise besonders häufig nicht mehr teilgenommen haben. Ein solches Muster war auch nicht zu erwarten, da die Expert*innen sich typischerweise je nach Technologiekomplex recht unterschiedlich einschätzen. Änderungen bei den relativen Anteilen der Expertiseniveaus können aber auch ein (erwünschter) Effekt des Delphi-Designs sein, das mit Lerneffekten rechnet. Befragte können ihre eigene Expertise in der zweiten Runde anders einstufen, weil sie zu diesem Zeitpunkt die Fragen bereits kennen und dieses Wissen in

ihre Selbsteinschätzung einfließt. Auch kann die Teilnahme an der ersten Delphi-Runde für Befragte ein Anlass gewesen sein, sich mit bestimmten Technologien genauer zu beschäftigen.

Für die Auswertung der Befragung wurden die Antworten auf die geschlossenen Fragen für jeden Komplex zusammenfassend visualisiert. Hierfür wurden für alle im Fragebogen abgefragten Anwendungen die Mittelwerte der Experteneinschätzungen zu Nützlichkeit und Verfügbarkeit gebildet und die Ergebnisse in einem Streudiagramm dargestellt (siehe Abbildung 1, exemplarisch für den Technologiekomplex maschinelles Lernen). Bei dieser Vorgehensweise handelt es sich lediglich um eine Heuristik, weil mit eigentlich ordinalskalierten Variablen gerechnet wird, als handele es sich um metrische. Das Resultat erlaubt aber eine einfache Orientierung, gerade wenn es um die übergreifende Aufgabe eines Technologiemonitorings geht, Priorisierungen für die vertiefende Beobachtung und Analyse vorzunehmen.

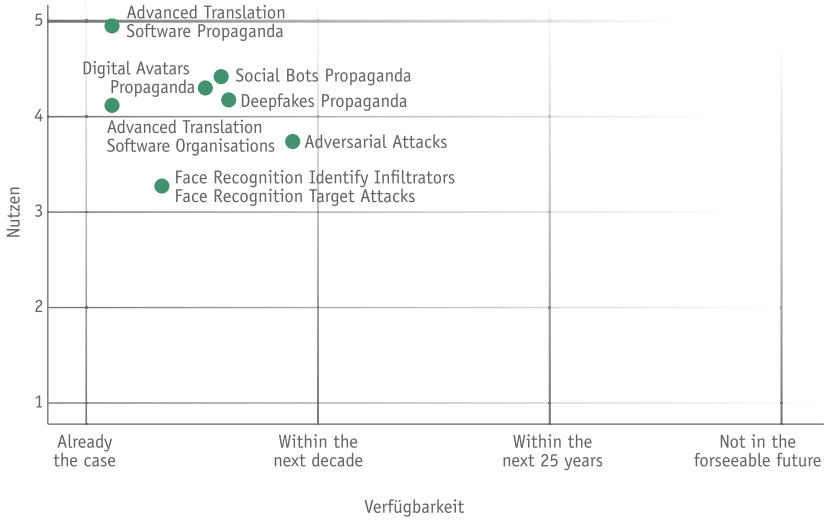

Abbildung 1: Technologieanwendungen im Bereich maschinelles Lernen

Um eine solche Priorisierung auch über alle betrachteten Technologiekomplexe hinweg einheitlich vorzunehmen, wird besonderes Augenmerk auf jene Anwendungen gelegt, die bei der Nützlichkeit im Durchschnitt

wenigstens den Wert 4 (von maximal 5) erreichen.[1] Diese recht hohe Wert ist dem Umstand geschuldet, dass die Einschätzungen zur Nützlichkeit in der Tendenz bei den meisten Items eher zustimmend sind. Das ist insofern nicht überraschend, da die Items auf der Basis von Literaturrecherchen formuliert wurden, eine zumindest vermutete Nützlichkeit einer Anwendung also bereits ein Kriterium dafür war, dass diese Anwendung überhaupt in den Fragebogen aufgenommen wurde. Bei der Verfügbarkeit bekommen jene Anwendungen besondere Aufmerksamkeit, die im Durchschnitt maximal den Wert 2 erreichen[2]. Das bedeutet, dass die Expert*innen tendenziell davon ausgehen, dass diese Anwendungen für extremistische und terroristische Akteur*innen entweder schon verfügbar sind oder das sehr bald sein werden. Priorisiert werden also technologische Anwendungen, die als besonders nützlich eingeschätzt werden und deren Einsatz für extremistische und terroristische Akteur*innen spätestens in naher Zukunft praktikabel wäre.

Für die Frage, welche Anwendungen einer detaillierteren Analyse unterzogen werden sollten, sind jedoch noch weitere Gesichtspunkte zu beachten. Dazu gehören die Kommentare der Expert*innen zu den geschlossenen Fragen, die Antworten auf die offenen Fragen nach weiteren relevanten Anwendungen, aber auch das von den Expert*innen selbst eingeschätzte Niveau ihrer Expertise zu bestimmten Technologiekomplexen. Hinzu kommt, dass Kombinationen bestimmter Anwendungen denkbar sind, die ihre Nützlichkeit für extremistische und terroristische Akteur*innen gegebenenfalls steigern oder auf neue Anwendungsfälle erweitern.

Diskussion der Ergebnisse

Durch die Ergebnisse der Delphi-Studie lassen sich die im Grobradar für extremistische und terroristische Akteur*innen als potenziell relevant ausgemachten technologischen Anwendungen im Hinblick auf eine Priorisierung für vertiefende Analysen eingrenzen. Im Folgenden werden die

[1] *Für Aussagen zur Nützlichkeit lauten die Antwortmöglichkeiten und Codewerte wie folgt: „completely agree" (5), „partly agree" (4), „neither agree nor disagree" (3), „partly disagree" (2), „completely disagree" (1).*

[2] *Für Aussagen zur Verfügbarkeit lauten die Antwortmöglichkeiten und Codewerte wie folgt: „already the case" (1), „within the next decade" (2), „within the next 25 years" (3), „not in the foreseeable future" (4).*

Ergebnisse, anhand der verschiedenen Technologiekomplexe gegliedert, kurz zusammenfassend dargestellt:

Für den Bereich des *maschinellen Lernens* ergibt sich auf der Basis der festgelegten Kriterien, dass Übersetzungssoftware – sowohl für Propagandazwecke als auch zur Erleichterung des Aufbaus transnationaler extremistischer oder terroristischer Organisationen –, Social Bots, Deepfakes und digitale Avatare besonders relevant sind. Weniger relevant hingegen ist die Nutzung von Gesichtserkennung zur Identifikation von Infiltratoren in den eigenen Reihen oder zur Erleichterung von Angriffen. Hinsichtlich der geringen Relevanz gilt Gleiches für die Möglichkeit von Angriffen auf KI-Systeme mittels Adversarial Attacks. In den offenen Fragen wird betont, dass sich Anwendungen maschinellen Lernens potenziell systematisch kombinieren lassen, um Propaganda und Desinformation strategisch für spezifische Kommunikationsziele oder soziale Disruption einzusetzen. Darüber hinaus handelt es sich um eine Technologie, die prinzipiell als Komponente in anderen Technologien Verwendung finden kann. So ist es beispielsweise denkbar, dass sich die Zielgenauigkeit von Drohnen über eine Kombination von algorithmenbasierter Gesichtserkennung und Geolokalisierung erhöhen lässt.

Bei den *Blockchain-Anwendungen* verdient insbesondere das Potenzial von Kryptowährungen für die Finanzierung von Aktivitäten eine genauere Betrachtung, während die Verwendung von Blockchain-Anwendungen zur Umgehung der Regulierung von Inhalten und die Nutzung von Smart Contracts für Zwecke der Koordination zunächst nicht relevant sind. Mittelfristig könnte darüber hinaus aber auch ein Wandel der Architektur des Internets hin zu dezentralen Apps[3], die auf Blockchains basieren, für das Themenfeld Extremismus und Terrorismus wichtig werden. Sollte sich ein solcher Umbau des Internets vollziehen, würde das die Rahmenbedingungen für Online-Kommunikation, gerade mit Blick auf die Möglichkeiten von Moderation oder Zensur, gravierend verändern.

[3] *Erläuterung: Dezentrale Apps (auch: dApps) sind dezentralisierte Anwendungen auf Basis von Blockchain-Technologie. Eine dApp wird, im Gegensatz zu einer klassischen App, nicht von einem einzelnen Anbieter betrieben, gewartet oder entwickelt, das heißt sie kann auch nicht von einem zentralen Kontrollmechanismus zensiert oder abgeschaltet werden. Da der Quellcode auf der Blockchain öffentlich ist, handelt es sich bei dezentralisierten Apps immer um Open-Source-Software, das heißt alle können sie für ihre Zwecke verwenden und weiterentwickeln [Schiller 2018].*

Das *Internet der Dinge* bietet terroristischen Akteur*innen schon heute oder in naher Zukunft eine Reihe von Gelegenheiten für neue Angriffsziele und ist gleichzeitig potenzielles Angriffsmittel. Die Möglichkeiten, das Internet der Dinge für Distributed-Denial-of-Service-Attacken (DDoS), für physische Attacken auf Individuen oder auf kritische Infrastrukturen sowie für das Schürfen von Kryptowährungen zu verwenden, sind für eine vertiefte Analyse relevant. Allerdings weist der Themenkomplex auch Überschneidungen mit Anwendungen von Blockchains und von maschinellem Lernen auf und könnte gegebenenfalls auch im Zusammenhang mit diesen vertiefend betrachtet werden.

Im Bereich *Verschlüsselung und Anonymisierung* sind kurzfristig eher keine Innovationen zu erwarten. Weder die Verwendung von selbst programmierten Instant Messengern, noch die Verwendung eines alternativen Onion-Routers für Aktivitäten im Darknet erweisen sich als hinreichend nützlich oder verfügbar. In den Kommentaren wird zudem deutlich, dass existierende Instant-Messenger-Dienste wie Telegram oder Signal für extremistische und terroristische Akteur*innen schon jetzt eine hohe Funktionalität haben. Langfristig ist in technologischer Hinsicht die Entwicklung von Quantencomputern relevant, weil sie aktuelle Verschlüsselungsverfahren aushebeln und so Innovationsdruck erzeugen würden – gerade für Akteur*innen, die ihre Kommunikation vor der Möglichkeit staatlicher Beobachtung schützen wollen.

Aus den Kriterien zur Priorisierung ergibt sich für den Bereich *Drohnen*, dass die meisten der im Fragebogen thematisierten Einsatzweisen eine hohe Priorität für vertiefende Betrachtungen haben. Im Einzelnen handelt es sich dabei um die Verwendung von Drohnen zum Filmen von Angriffen für Propagandazwecke, zur Beobachtung potenzieller Angriffsziele, zur Durchführung von gezielten tödlichen Angriffen auf bestimmte Personen und zur Durchführung von Angriffen auf kritische Infrastrukturen. Keine erhöhte Priorität haben Szenarien, in denen Drohnen eingesetzt werden, um eine größere Zahl an Menschen zu töten oder chemische beziehungsweise biologische Substanzen auszubringen. In den offenen Antworten verweisen die Expert*innen darauf, dass es zu diesen Zwecken einfachere und effektivere Alternativen als Drohnen gibt. In den Kommentaren wird von den Expert*innen jedoch die Bedeutsamkeit von prinzipiell bereits heute kommerziell verfügbaren Drohnen hervorgehoben, die sich so

modifizieren lassen, dass verschiedene andere Angriffsszenarien denkbar sind.

Hinsichtlich der Bewertungen zum *3D-Druck* ist zu berücksichtigen, dass in der Befragung kaum Expert*innen mit einem hohen Niveau an Expertise zu diesem Bereich vertreten waren. Die Einschätzung, dass die Verwendung von 3D-Druckern für die Herstellung von Waffen und sonstiger Ausrüstung hochrelevant ist, ist insofern mit etwas größerer Unsicherheit behaftet, aber plausibel. Wichtig in diesem Zusammenhang ist insbesondere der Hinweis aus den Kommentaren, dass die Herstellung einzelner Bauteile genügen kann, um vorhandene Waffen tödlicher zu machen. Langfristig könnte die Entwicklung des sogenannten 4D-Drucks[4], bei dem die angestrebte Form eines Bauteils sich erst unter bestimmten Bedingungen ausbildet, die Attraktivität der Technologie für terroristische Akteur*innen noch weiter erhöhen. Nicht relevant ist nach Einschätzung der Expert*innen der Effekt online verfügbarer CAD-Dateien für den 3D-Druck im Hinblick auf die Häufigkeit extremistischer Angriffe.

Zum Bereich *synthetische Biologie* hat die Befragung zwar das Ergebnis erbracht, dass synthetische biologische Waffen für terroristische Akteur*innen sehr nützlich sind und die Möglichkeit, sie selbst herzustellen, unmittelbar bevorsteht, wenn nicht schon gegeben ist. Hier besteht aber aus mehreren Gründen ein Bedarf an vertiefenden Analysen. Zum einen haben nur sehr wenige Expert*innen sich überhaupt für kompetent gehalten, zu diesem Thema Einschätzungen abzugeben, und diese schätzen ihre Expertise eher niedrig ein. Zum anderen deuten die abgegebenen Kommentare darauf hin, dass hier nicht in erster Linie an Angriffsszenarien zu denken ist, bei denen Menschen biologischen Agenten ausgesetzt werden, sondern etwa die landwirtschaftliche Produktion ein Angriffsziel sein könnte.

Einschätzungen zum *High-Performance Computing* sind wegen eher geringer Expertise der Befragten ebenfalls mit großen Unsicherheiten behaftet. Gefragt wurde nach der Verwendung von High-Performance Computing

[4] *4D-Druck beschreibt den Prozess, bei dem sich ein 3D-gedrucktes Objekt unter dem Einfluss von externen Energiequellen wie Temperatur, Licht oder anderen Umweltreizen in einer gewissen Zeit in eine andere, neue Form verwandelt. Zum 3D-Druck kommt also die vierte Dimension Zeit hinzu, also die Fähigkeit, dass sich die Form mit der Zeit selbst verändert [FutureBridge 2020].*

für verschiedene Zwecke wie Verschlüsselung von Kommunikation, Schürfen von Kryptowährungen oder Angriffe auf kritische Infrastrukturen, aber auch nach der Attraktivität von High-Performance-Computing-Anlagen als Angriffsziel. Allein aufgrund der hier abgegebenen Expert*innen-Urteile können wir nicht darauf schließen, dass es sich hier um Anwendungen handelt, die dringend vertiefender Betrachtung bedürfen, wenn es um Extremismus und Terrorismus geht. Gegebenenfalls bedeutsam ist die Kontrastierung mit dem Cloud-Computing, das im Fragebogen nicht berücksichtigt wurde, aber ein attraktives Angriffsziel für terroristische Akteur*innen sein könnte.

Weitere zukünftige Technologien

Auf die Frage nach für extremistische und terroristische Akteur*innen nützlichen und verfügbaren weiteren zukünftigen Technologien jenseits der thematisierten Technologiekomplexe wurden verschiedene konkrete technologische Anwendungen genannt. Mit dem Aufbau von 5G-Netzen sowie der Verfügbarkeit von Dienstleistungsangeboten im Bereich der künstlichen Intelligenz (AI as a Service[5]) sind Entwicklungen benannt, die im Zusammenhang mit dem Internet der Dinge beziehungsweise Anwendungen des maschinellen Lernens als Kontextbedingungen wichtig sind. Die Verfügbarkeit von Internet via Satelliten im Low-Earth-Orbit (siehe Elon Musks Starlink-Projekt) könnte eine weitere künftig relevante Kontextbedingung sein. Im Komplex der Fernerkundung und Raumfahrt werden zudem als künftig denkbare Möglichkeiten einerseits die Nutzung von Fernerkundungsdaten – etwa für die Planung von Anschlägen – genannt, andererseits der Einsatz eigener Satelliten oder die Übernahme der Kontrolle von strategischen Satelliten.

Vermutlich ebenfalls in fernerer Zukunft sind Technologien zur Wetteränderung anzusiedeln. Im Vergleich dazu greifbarer sind die Bereiche Virtual Reality oder Extended Reality. Sie könnten entweder als Medium für Propaganda genutzt werden oder für die Planung von Angriffen. Autonome Fahrzeuge könnten selbst Angriffsziel sein oder als Angriffswaffe

[5] *Artificial Intelligence as a Service (AIaaS) beschreibt das Angebot, künstliche Intelligenz an einen externen Anbieter, meist einen Cloud-Dienst, auszulagern. Der Vorteil liegt hierbei in der Einsparung von Ressourcen und Kosten (Gandorfer 2018).*

missbraucht werden. Darüber hinaus wird die Möglichkeit, elektromagnetische Wellen als Waffen zu verwenden, erwähnt.

Neben der Nennung konkreter Technologien finden sich in den Antworten zwei allgemeinere Zukunftsszenarien. Das eine Szenario rechnet mit einem generellen Trend von Hightech hin zu Lowtech, wenn es um terroristische Angriffe geht. Als Hintergrund dafür wird das Internet genannt, das es terroristischen Gruppen ermöglicht, auch gewaltbereite Anhänger*innen aus der Ferne zu rekrutieren. Diese haben aber nur begrenzte Ressourcen und begehen in der Regel nur einmalig einen Anschlag. Das bedeutet, dass weder individuelles noch institutionelles Lernen stattfindet, was aus Sicht der kommentierenden Person Angriffe mit wenig Technologieeinsatz wahrscheinlicher macht. Das zweite Szenario rechnet mit der Möglichkeit, dass die zunehmende Verbreitung systemischen Denkens künftig Attacken auf kritische Infrastrukturen wahrscheinlicher machen wird, die das Ziel haben, kaskadenartige Störungen und Zusammenbrüche auszulösen. Besonders gefährdet wären damit etwa Hochspannungsstromleitungen, Wasserwerke, Transformatoren oder Treibstoffdepots. Letztendlich, so ein weiterer Kommentar, hängt die Frage, ob neue Technologien in Zukunft für extremistische und terroristische Akteur*innen relevant werden, maßgeblich davon ab, wie weit diese Teil des alltäglichen Lebens werden und damit als Gelegenheitsstrukturen auch für illegale Aktivitäten zur Verfügung stehen.

Workshop zu „Beobachtungstechnologien“

Einführung und Zielstellung

Technologiemonitoring ist nicht nur im Kontext von extremistischen oder terroristischen Aktivitäten interessant, sondern auch hinsichtlich der Ausweitung des Möglichkeitsraums von Sicherheitsbehörden. Die Nutzbarmachung von Technik durch Sicherheitsbehörden ist ein Momentum im Rahmen einer Innovationsdynamik: Sicherheitsbehörden wollen Personen, Gruppen und Organisationen beobachten und gegebenenfalls intervenieren; diese wiederum wollen sich vor dieser Beobachtung und Intervention schützen, sich ihr entziehen oder diese stören. Im Weiteren

gehen mit der Beobachtung von Individuen, Gruppen oder Organisationen, beziehungsweise von physischen Orten oder digitaler Kommunikation, oftmals Eingriffe in die Grundrechte von Personen einher, weshalb auch hier ein ausgeprägtes Interesse an Technikfolgenabschätzung besteht (Aden/Fährmann 2020).

Aus diesem Grund waren die Beobachtung von Personen, Aktivitäten und Orten einerseits sowie die Interventionsmöglichkeiten durch Sicherheitsbehörden andererseits Gegenstand eines Workshops im Rahmen unseres Technologiemonitorings. Für die Konzeption des Workshops waren zwei Referenzprobleme ausschlaggebend. Ausgehend von multiplen System-Umweltbeziehungen lassen sich in einem abstrakten Sinne folgende Thesen formulieren:

1. Akteur*innen der zivilen Sicherheit müssen sich potenziell mit der Gesamtheit aller gesellschaftlichen Aktivitäten beschäftigen, wenn sie ihrer Aufgabe der Prävention nachkommen wollen.

2. Dadurch entsteht ein hoher Druck auf Seiten der Akteur*innen mit Sicherheitsaufgaben zur richtigen Selektion zwischen problematischen und unproblematischen Aktivitäten.

Bildgebende und nicht bildgebende Beobachtungstechnologien, sensorische Technologien, Internet- oder Social-Media-Beobachtung und die informationstechnische Auswertung von Daten versprechen den Sicherheitsbehörden mithilfe von lernenden Algorithmen neue Möglichkeiten der Überwachung und Prävention. Dadurch werden wiederum Probleme der "richtigen" Selektion generiert, die sich aus der Bewältigung von Datenmengen, der Notwendigkeit der Informationsgewinnung und der Erwartung möglichst eindeutiger Handlungsorientierung ergeben. Diesen Problemen der Funktionalität der Technik für die Zwecke von Sicherheitsbehörden haben sich die Teilnehmer*innen am ersten Tag des Workshops gewidmet.

Am zweiten Tag wurden die Workshop-Teilnehmer*innen aufgefordert, sich normativen Fragen zu stellen. Dahinter steckt die gesellschaftlich vehement debattierte Frage, ob das, was in diesem Zusammenhang technisch machbar wäre, auch gesellschaftlich wünschenswert ist. Dabei müssen

zunächst bereits bestehende rechtliche Regeln, etwa im Zusammenhang mit Datenschutz und informationeller Selbstbestimmung, in Betracht gezogen werden. Damit befassen sich sowohl Befürworter*innen neuer Überwachungsmöglichkeiten, wie zum Beispiel EU-Beamt*innen, die sich weitergehende Befugnisse für Behörden wünschen (Meister 2020), als auch Kritiker*innen, die bestehende Gesetze für zu schwach halten, um die Einhaltung demokratischer Grundrechte angesichts neuer technologischer Möglichkeiten noch zu gewährleisten (Kurz 2020). Hier ist die Reflexion zentraler demokratischer Werte, von denen Sicherheit nur einer ist, ein wichtiger Aspekt bei der Einschätzung von Verwendungsmöglichkeiten neuer Technologien.

Für den Workshop konnten wir Expert*innen gewinnen, die einen vertieften Einblick in die Funktionsweise von relevanten Technologien geben konnten oder den rechtlichen und politischen Kontext des Technikeinsatzes überblicken. Gleichermaßen wurden Personen eingeladen, die das Thema Radikalisierung (beziehungsweise auch Deradikalisierung) erforschen oder in der Praxis bearbeiten. Schlussendlich haben sich auch kritische Beobachter*innen des vermehrten Technikeinsatzes zur Teilnahme bereit erklärt.

Konzept: übergeordnetes Problem der Sicherheitsbehörden und Handlungstypen

Sicherheitsbehörden beziehungsweise Organisationen mit Sicherheitsaufgaben stellen einen besonderen Akteurstypus mit spezifischen Problemen dar. Diese Organisationen sollen qua gesetzlichem Auftrag in sehr vielen Lebensbereichen zur Erhöhung von Sicherheit beitragen, können aber gleichzeitig nicht in allen Lebensbereichen präsent sein. Sie sollen es auch nicht. Im Grunde muss eine die Sicherheit fördernde Relaistechnik (Luhmann 2005) angewendet werden, so unsere Vermutung: Allein die Erwartung, dass behördlicherseits beobachtet werden könnte, muss dazu führen, dass viele kriminelle beziehungsweise illegale Aktivitäten unterbleiben. Die selektive Präsenz muss ausreichen, um eine soziale Ordnung aufrechtzuerhalten. Eine Ordnung, in der alle Personen einer Gesellschaft erwarten können, innerhalb von generalisierten Beschränkungen frei und unbeschadet ihrem Leben nachgehen zu können. Das Referenzproblem aller Akteur*innen der zivilen Sicherheit ist daher das der richtigen Selektion von Präsenz, Beobachtung und Intervention. Diese Problemdefinition

ist hinreichend allgemein, dass sie für verschiedene Behörden passend zu sein scheint. Sie ist aber auch hinreichend konkret, dass sich Verbindungen zu Technologien herstellen lassen. Technologien bieten in diesem Zusammenhang mögliche Problemlösungen, die aber von Fall zu Fall nicht zwingend oder unvermeidlich sind. Wir gehen davon aus, dass mehrere äquivalente Lösungen, die in unterschiedlichem Maße (oder gar nicht) auf Technologien setzen, möglich sind. Vermutlich sind bestimmte Lösungen gleichermaßen funktional, aber nicht gleichermaßen wünschenswert mit Blick auf gesellschaftliche Normen und Werte.

Die Beobachtung menschlicher Aktivitäten ist darauf angewiesen, Adressen zu identifizieren. Zum einen sind dies Personen mit allen ihnen zugeschriebenen Eigenschaften wie Geschlecht, körperlichen Merkmalen, Staatsangehörigkeit, gemeldete postalische Adresse und so weiter. Zum anderen sind dies physische Orte, an denen sich Personen aufhalten, und sogenannte „virtuelle" Orte, an denen Personen Aktivitäten entfalten können, obwohl sie physisch woanders verortet sind.

Technologien können dann für die Zwecke der Beobachtung von Personen und Orten verwendet werden – aber auch für mögliche Interventionen in die beobachtete Situation. Es ist zu vermuten, dass es für diese funktionale Differenzierung unterschiedlicher Techniken beziehungsweise Technologien bedarf. Auch müssen bei der Beobachtung bestimmte Bedingungen erfüllt sein, um eine Intervention zu ermöglichen, wie beispielsweise die Zuverlässigkeit der aus den Daten ermittelten Informationen oder die Legalität der erhobenen Daten. Wir unterstellen, dass zwischen der Beobachtung von Personen beziehungsweise Orten und den möglichen Interventionen in das Verhalten von Personen keinerlei Kausalkette etabliert ist. Die Beobachtung einer Aktivität führt nicht „automatisch" zur Intervention. Interventionen sind immer ein Ergebnis von Selektionen aus einem Möglichkeitsraum, die wiederum durch eine komplexe rechtliche und polizeiliche Lage konditioniert sind. Wichtig ist die Annahme, dass die vorgenommenen Selektionen immer mit Unsicherheiten und mit Risikoverarbeitung verbunden sind.

Wir haben für die Zwecke des Workshops einige ausgewählte Technologien zur Diskussion gestellt. Wenn konkrete Personen oder Gruppen von Personen in ihren Aktivitäten beobachtet werden sollen (siehe Abbildung 2),

dann könnten zum Beispiel neue digitalisierte Infrastrukturen, sprich vernetzte Unterhaltungs-, Versorgungs-, oder Haushaltsgeräte, die über Kameras oder Mikrofone verfügen, in Zukunft ein Einfallstor nicht nur für Hacking, sondern auch für Beobachtungsbegehrlichkeiten des Staates werden – oder sie sind es bereits (Snijders et al. 2020).

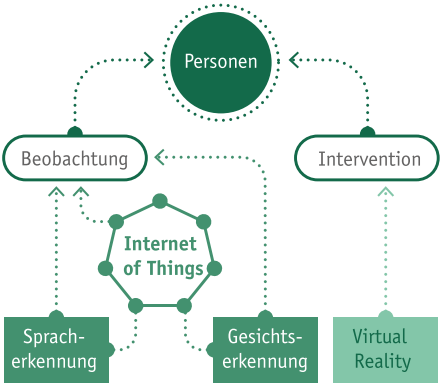

Abbildung 2: Die Beobachtung von Personen mit Hilfe von vernetzten Infrastrukturen

Für die Beobachtung physischer Orte ergeben sich folgende Differenzierungen. Es können menschliche Aktivitäten in konkreten Orten und Räumen adressiert werden, die öffentlich einsichtig sind und in denen sich Personen oder Gruppen aufhalten. Weiterhin können auch nicht öffentlich zugängliche Orte adressiert werden, in denen sich nur ausgesuchte Personen oder Gruppen aufhalten sollen. Darüber hinaus lassen sich auch Vorkommnisse in der realen Welt detektieren, die mittelbar auf Aktivitäten von Personen und Gruppen schließen lassen. Hier spielen alle möglichen bild- und tonaufnehmenden Technologien eine Rolle, aber auch Sensorik zur Messung physikalischer oder chemischer Eigenschaften der Welt, die auf Aktivitäten von Menschen hinweisen (siehe Abbildung 3).

Liegt der Fokus der Beobachtung dagegen auf virtuellen Orten, bedarf es der Technologien zur Erfassung digitalisierter Informationen. Auch hier lassen sich öffentlich zugängliche Orte und nicht öffentlich zugängliche Orte unterscheiden. Erstere umfassen Plattformen wie soziale Netzwerke und Foren, letztere umfassen Kommunikationsdienste (verschlüsselt

oder nicht verschlüsselt) wie WhatsApp, Telegram, Signal etc. oder private Speicher digitaler Informationen wie Cloud-Anbieter. In einer Vorselektion haben wir „Übersetzungssoftware“, „maschinelles Lernen“, „Deep Fakes“ (Kusche 2022) und „Social Bots“ als Beispiele für zukünftig relevante Technologieentwicklungen herangezogen, um das Potenzial der Beobachtung digitaler Räume zu eruieren (siehe Abbildung 4).

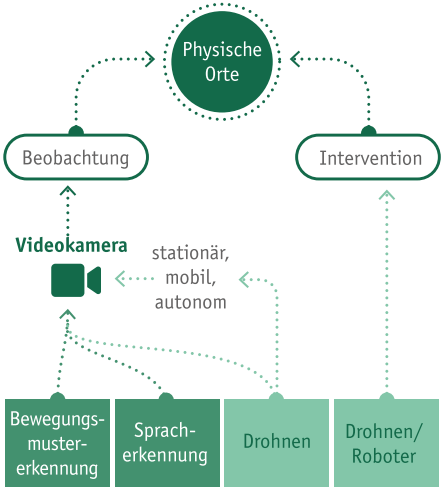

Abbildung 3: Die Beobachtung von physischen Orten durch Bildgebung und Sensorik

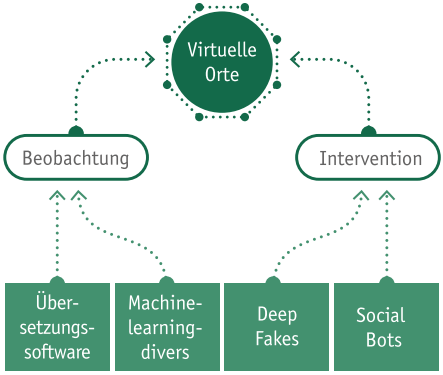

Abbildung 4: Die Beobachtung von virtuellen Orten

Diskussion der Ergebnisse

Die Diskussionen zwischen den Expert*innen bestätigen einen Trend, der in den letzten Jahren zu beobachten ist. Staatliche Organisationen verstärken ihre Bemühungen in der technikgestützten Analyse von Daten, um zu richtigen Selektionen zu gelangen. Damit gehen die staatlichen Aktivitäten über eine reine Echtzeitbeobachtung (surveillance) hinaus und verschieben sich in Richtung modellgestützter Analysen, um Muster in nicht erwünschtem, illegalem, kriminellem Verhalten zu entdecken (Hardy 2021) und darüber vorausschauend ein solches Verhalten eruieren zu können. Das Stichwort ist hier „Predictive Policing" (Pelzer 2018). Technologie ist in diesem Zusammenhang eine Ermöglicherin eines lang diskutierten Ziels, abweichendes Verhalten nicht nur zu beobachten, während es passiert, sondern bereits im Vorfeld mit einer Wahrscheinlichkeit zu belegen, dass dieses stattfinden könnte (Bröckling 2015). Damit soll die Handlungsfähigkeit auf Seiten der Organisationen mit Sicherheitsaufgaben im Vorfeld der möglichen Tat erhöht werden. Der frühere BKA-Präsident Horst Herold wird in einem Interview aus den 1980er Jahren wie folgt zitiert: „Meine Auffassung geht dahin, die Informationsleistung der Polizei zu verbessern, nicht um die Repression in den Vordergrund zu stellen, sondern eine gesellschaftliche Prävention" (Makropoulos 1990, 417). Um diese Vision nach und nach Wirklichkeit werden zu lassen, bedienen sich Organisationen mit Sicherheitsaufgaben verschiedenster Techniken: „DNA sequencing, metadata analysis, facial recognition technology and machine learning are becoming increasingly deployed by states [...] in the name of public safety and, especially, counterterrorism" (Clarke 2021, 132).

Ganz in diesem Sinne verliefen auch viele der Diskussionen unter den Teilnehmer*innen. Folgende Punkte möchten wir als Kondensat der Diskussionen herausstellen.

Chancen und Risiken der indiskriminatorischen Datenerhebung

Wir deuten die Einschätzung der Expert*innen dahingehend, dass durch die verstärkte Beobachtung von physischen und digitalen Orten einer indifferenten Datensammlung Vorschub geleistet wird. Zu Beginn der Beobachtung von Orten steht der Verdacht, dass jede Person, die sich im öffentlichen oder digitalen Raum bewegt, potenziell eine illegale, kriminelle

Tat begehen könnte. Für den digitalen Raum haben wir dies bereits am Beispiel des Tor-Projekts ausgeführt (Kusche/Büscher 2021). Auf der einen Seite erhöhen *.onion-Sites die Privatheit von Kontakten, weil sich interagierende Parteien im Tor-Netzwerk auf eine bessere Authentifizierung von Kommunikation verlassen können (Man-in-the-Middle-Attacken werden erschwert). Auf der anderen Seite bilden verborgene Websites (hidden services) ein sogenanntes Darknet, das für verschiedenste Zwecke genutzt werden kann: vor Repression geschützte Kommunikation, aber auch kriminelle, extremistische und terroristische Aktivitäten (Weimann 2019). Jede Person, die sich im Darknet bewegt, unterliegt daher dem Verdacht, illegale Aktivitäten anzubahnen oder durchzuführen. Eine ähnliche Entwicklung lässt sich nun im Zusammenhang mit Messenger-Diensten beobachten. Deren Verschlüsselungstechnologien erlauben es, sich des Mitlesens zu entziehen. Dies kann für legale und illegale Aktivitäten genutzt werden (Miller/Bossomaier 2021). Vor allem geraten aber einige Dienste in den Ruf, radikale beziehungsweise radikalisierende Kommunikation zu ermöglichen und damit extremistischen Gruppierungen eine operative Basis bereitzustellen (Guhl/Davey 2020). Es stellt sich die Frage, ob in naher Zukunft bereits die Nutzung von „Verschlüsselung" zu Verdachtsmomenten führt und staatliche Überwachungsbemühungen verstärkt.

Technisch unterstütze Detektion, Identifikation, Überwachung und Auswertung von Daten erlaubt einen Evolutionsschritt von der reaktiven (Wieder-)Herstellung von Sicherheit hin zu dem Versuch der präventiven Verhinderung sicherheitsgefährdender Aktivitäten. Dem daraus folgenden Modus Operandi der Gefahrenabwehr unterliegt eine Art Generalverdacht, eine „prospective form of risk management that is interested in strategic information and operates with a *generalised suspicion detached from individual cases*" (Kaufmann 2016, 82; Hervorhebung durch uns). Die Orientierung an einem Generalverdacht und die Ausdehnung sowie die Erhöhung des Auflösevermögens von technischer Beobachtung generieren einen selbstverstärkenden Effekt, möglichst viele Daten zu sammeln – gerade und auch, wenn aktuell noch nicht geklärt ist, wie diese Daten ausgewertet werden können (Aden/Fährmann 2019). Der technisch unterstützte Generalverdacht entwickelt sich in seiner Rationalität ähnlich wie die sogenannte „Datenökonomie" (Bundeszentrale für politische Bildung 2019). Es werden Daten überall dort gesammelt, wo sie abgegriffen werden können. Dies mit dem Versprechen, dass in Zukunft anhand dieser Daten

Verhaltensmuster erkannt werden können, die auf mögliche illegale Taten schließen lassen. Daran schließen sich weitere Fragen an, wie nach der Funktionalität von Technologien hinsichtlich der tatsächlichen Sicherheitsgewinne angesichts der unauflösbaren Spannung, mit falsch positiven (erfasste Informationen erweisen sich als nicht zutreffend) und falsch negativen (relevante Informationen werden nicht erfasst) Ergebnissen umgehen zu müssen. Damit ist das Problem des Vertrauens in die Reliabilität informationstechnischer Systeme angesprochen, wenn Akteur*innen mit deren Hilfe schwerwiegende Entscheidungen zu treffen haben. Vertrauen in abstrakte Systeme ist eine wichtige Variable in der Bestimmung der Handlungsfähigkeit der Organisationen mit Sicherheitsaufgaben.

Neben diesen technisch-funktionalen Aspekten spielen auch andere Faktoren eine Rolle, wenn es um die Herstellung von Handlungsfähigkeit geht. Technisch vermitteltes Handeln, das womöglich tiefgreifende Grundrechtseingriffe nach sich zieht, erfordert Rechtssicherheit bezüglich der dadurch berührten Rechtsnormen wie zum Beispiel des Rechts auf informationelle Selbstbestimmung und auf Vertraulichkeit sowie bezüglich der Integrität informationstechnischer Systeme. Zudem müssen Verantwortlichkeiten hinsichtlich von Datenbeständen, die durch private Unternehmen verwaltet werden, geklärt sein und damit der Schutz vor zweckentfremdeter Nutzung, offensichtlichem Missbrauch oder Datendiebstahl (Robbins 2021, 101). Nicht zuletzt müssen ethische Überlegungen der Grenzen des zu Beobachtenden trotz technischer Möglichkeiten angestellt werden und daran anschließend Definitionen von geschützten Personen und Orten vorgenommen sowie die tatsächliche Durchsetzung solcher selbst gesetzter Grenzen sichergestellt werden.

Es verbleibt der Eindruck, dass die umfassende Verarbeitung von Daten, indiskriminatorisch erhoben an physischen und digitalen Orten, vor allem die Intransparenz bei Entscheider*innen und bei Betroffenen erhöht, wie diese Daten verarbeitet werden (Stichwort: maschinelles Lernen) sowie welche Schlüsse gezogen und welche Entscheidungen getroffen werden, die wiederum die Grundrechte bestimmter Personen tangieren (Aden/Fährmann 2020).

Die Einschränkung des technisch Möglichen

Technologische Innovationen zur Erhebung von Daten, die menschliches Verhalten erfassen und im Weiteren analysieren können, haben in den letzten Jahrzehnten enorm an Vielfalt und Wirkmächtigkeit gewonnen. Der amerikanische Soziologe Gary T. Marx (2004, 19) diskutiert in diesem Zusammenhang den Begriff der „new surveillance", der zu Beginn des 20. Jahrhunderts aufgekommen ist, und benennt Beispiele: „video and audio surveillance, heat, light motion, sound and olfactory sensors, night vision goggles, electronic tagging, biometric access devices, drug testing, DNA analysis, computer monitoring including email and web usage and the use of computer techniques such as expert systems matching and profiling, data mining, mapping, network analysis, and simulation." Dennoch plädiert er dafür, genauer zwischen technischen Potenzialen und realer Anwendung zu unterscheiden. Nicht alles, was technisch möglich sei, müsse zwangsläufig auch zum Einsatz kommen. Er bezeichnet diese Diskrepanz als einen „surveillance slack". In einer dialektischen Entwicklung erscheinen mächtige technische Werkzeuge, die wiederum gesellschaftlich in ihrer Anwendung eingeschränkt werden können. Technik bestimmt Gesellschaft, ist aber gleichwohl wieder durch Gesellschaft bestimmt. „They do not enter a neutral culture, but one with informal and formal protections for personal information, as well one with value and organizational supports for collecting such information" (Marx 2004, 33).

Dieser gesellschaftliche Schub wirkt in beide Richtungen. In diesem Sinne wird von vielen Autor*innen mit den Terroranschlägen am 11. September 2001 in den USA eine Zäsur beobachtet. Die Anschläge haben die Grundlage für eine veränderte Motivlage geschaffen, die Argumenten für umfangreiche Maßnahmen zur Terrorabwehr Tür und Tor öffnete. Die Sammlung von Daten über die Aktivitäten von potenziell jeder Person, an physischen Orten oder in digitalen Netzen, wird aktuell nur noch durch technische Limitationen und Probleme der Datenverarbeitung eingehegt (Amoore/de Goede 2021; Kaufmann 2016). Im Anschluss an die Attacken wurden verstärkt Beobachtungstechnologien in Einsatz gebracht, die Finanztransaktionen, Warenaustausch oder Reiseaktivitäten erfassen können (Gerhold/Brandes 2021, 2). Die Enthüllungen von WikiLeaks und Edward Snowden haben der allgemeinen Öffentlichkeit vor Augen geführt, wie weit Regierungen die eigenen und fremde Staatsbürger*innen ausspionieren. In

diesem Sinne eruieren Forscher*innen die Wirkmächtigkeit von Zukunftsvorstellungen im Hinblick darauf, wie der weitere Umgang mit Technologie gesellschaftlich gestaltet werden kann: entweder als Sicherheit hypostasierende Gesellschaft, die nach umfangreichen technischen Lösungen sucht, oder als risikotolerante Gesellschaft, die kriminellen, extremistischen oder terroristischen Gefahren mit sozialen Innovationen begegnen will und gegenüber technischen Beobachtungsmöglichkeiten eine skeptische Haltung entwickelt (Gerhold/Brandes 2021).

Diese Argumentationslinien wurden auch unter den Teilnehmer*innen des Workshops verfolgt. Technisch sei alles möglich beziehungsweise Technik sei nicht mehr die begrenzende Variable in der Beobachtung von Personen und Orten. Für maschinelles Lernen seien geeignete Trainingsdaten, die sehr aufwendiges qualifizierendes Labeln verlangen, ein limitierender Faktor. Dazu brauche es wiederum den Einsatz menschlicher Intelligenz. Die Nutzung von Daten unterliege rechtlichen Einschränkungen, ebenso jede Form automatisierter Intervention. Durch Automatisierung der Datenauswertung komme es zur Vervielfältigung potenzieller Verdachtsmomente, wodurch ein „überschießender Verdacht" auch und gerade gegenüber Unbeteiligten entstehen könne. Auch auf Seiten der Organisationen mit Sicherheitsaufgaben könne man eine Diskrepanz zwischen den Prozessen der Polizeiarbeit und technischen Abläufen beobachten. Unterstützende Tools seien oft nicht an die Anforderungen (Use Case) der Nutzer*innen angepasst.

Informationslast in der Auswertung von Daten

Daten sind noch keine Informationen, Informationen sind noch nicht Wissen. So in etwa kann man allgemein die Problematik beschreiben, mit der alle Akteur*innen umgehen müssen, wenn sie sogenannte „Informations- und Kommunikationstechnik" oder automatisierte Prozesse der Datenanalyse einsetzen. In diesem Sinne besteht die größte technische Herausforderung in der Verwaltung und Handhabung der riesigen Datenmengen durch die stetig wachsende Zahl von Beobachtungssystemen. Hier haben die Teilnehmer*innen auf das Problem des „Data Lake", einer unstrukturierten Sammlung von Daten, und der Erzeugung eines „Data Warehouse" hingewiesen, das einen strukturierten Zugriff

unterschiedlicher Organisationen mit unterschiedlichen Use Cases erlauben soll.[6]

Aus dem Bereich der Terrorbekämpfung sind Gesichtserkennungstechnologien bekannt, die vor allem bei grenzüberschreitendem Personenverkehr eine Rolle spielen. Videobeobachtungssysteme werden aufgerüstet mit automatisierten Prozessen der Bildanalyse und -interpretation. Menschliche Beobachter*innen sollen unterstützt werden. Aufbereitung soll soweit maschinell vorgenommen werden, dass menschliche Beobachter*innen intuitiv reagieren können. Maschinelle Selektion (durch Menschen programmiert) soll mit menschlicher Informationsverarbeitung verbunden werden und trotzdem Sicherheit für Entscheidungssituationen herstellen beziehungsweise hinreichend Unsicherheit absorbieren, sodass das polizeiliche Personal sich auf Interventionshandeln festlegen kann.

Dazu braucht es Modelle für maschinelles Lernen (ML), „Algorithmen, die sich datengetrieben verbessern können" (Grünwald/Kehl 2020, 52 f.). Hier wird zwischen unterschiedlichen Formen des Lernens unterschieden:

1. Supervised Learning bezeichnet ein stark vordeterminiertes Lernen. Output-Kategorien werden vorgegeben. Input beziehungsweise Trainingsdaten werden korrekt anhand der Kategorien gelabelt, sodass der Algorithmus die Kategorisierungen nachvollziehen kann. Anschließend kann dieser die Kategorisierung selbstständig auf unbekannte Daten übertragen.

2. Bei Unsupervised Learning spielen bereits neue Freiheitsgrade eine Rolle. Anhand von statistischen Eigenschaften der Input-Daten werden Output-Kategorien vom Algorithmus selbst entwickelt. Das Ergebnis bedarf einer Reinterpretation durch menschliche Beobachter*innen.

3. Online lernende (selbstlernende) Systeme setzen das Training im laufenden Betrieb fort. Ein Algorithmus kann so „Erfahrungen" sammeln und eine eigene Historie entwickeln. Grünwald und Kehl (2020, 53) geben zu bedenken, dass solche Systeme „nichtintendierte Verhaltensweisen

[6] *Siehe dazu auch die Diskussion um das sehr umstrittene Softwareunternehmen „Palantir" (Hegemann et al. 2020; in 't Veld 2020; Monroy 2020) sowie die Bestrebungen der Polizei zur Konsolidierung unterschiedlicher Datenbestände (BMI 2018).*

lernen könnten und die Vorhersagbarkeit ihres Verhaltens im Laufe der Zeit gemindert würde". Die Einschätzungen der Workshop-Teilnehmer*innen gingen einheitlich in die Richtung, den aktuellen Einsatz von maschinellem Lernen noch als überwachtes Lernen zu qualifizieren.

Unter dem Stichwort „Predictive Policing" versammeln sich softwarebasierte Methoden, die im besten Falle Wahrscheinlichkeitsaussagen zu möglichen Aktivitäten generieren. Diese können aber nicht unmittelbar an polizeiliches Handeln gekoppelt werden. Es bedarf immer noch der Entscheidung an verantwortlicher Stelle beziehungsweise eines qualifizierten „peer reviews" (Pelzer 2018, 177). In der praktischen Anwendung von Predictive Policing (im angelsächsischen Raum) werden zunehmend Verfahren erprobt, die nicht mehr Vorhersagen für Räume („Heatmaps") machen, sondern Vorhersagen zum Verhalten von Individuen (Profiling, „Hotlists").

Treiber*innen dieser Entwicklungen sind Technologieunternehmen, die ihre Softwarelösungen bei Polizeibehörden anpreisen, woraus sich immer wieder Kooperationen ergeben, teils abseits der Öffentlichkeit und teils über nationale Grenzen hinaus (Beispiel: Clearview AI oder Palantir). Mit der Weiterentwicklung von Predictive-Policing-Software können zunehmend unterschiedlichste Datenbestände aus unterschiedlichsten Quellen miteinander verknüpft werden, um Vorhersagen zu treffen. Social-Media-Daten sind dabei eine Datenquelle unter vielen und werden zunehmend genutzt. Für die Anwendung von Predictive Policing in der polizeilichen Praxis spielen Aushandlungsprozesse eine große Rolle bei der Aneignung dieser Technologie. Auf der einen Seite berufen sich Hersteller*innen technischer Verfahren auf das Geschäftsgeheimnis und legen deshalb nicht dar, wie der eingesetzte Algorithmus funktioniert. Auf der anderen Seite entsteht ein erhebliches Interesse seitens der Betroffenen von Strafverfolgung, zu wissen, woher die Daten über Personen stammen und welche Schlussfolgerungen aus der Datenanalyse getroffen werden. Insgesamt generiert das Thema Predictive Policing vehemente Auseinandersetzungen zwischen Proponent*innen und Kritiker*innen darüber, inwieweit Big-Data-Verfahren eingesetzt werden sollten.

Ausblick

Für das Jahr 2022 werden wir das Technologiemonitoring auf Entwicklungen in der ferneren Zukunft ausrichten. Die Vision des „Metaverse" steht dabei im Mittelpunkt. Wichtige Proponent*innen wie META-CEO Mark Zuckerberg beschreiben das Metaverse als Nachfolger des mobilen Internets durch den Einsatz von Virtual Reality (VR) und Augmented Reality (AR). Durch diese Technologieschübe soll das Internet einer weitergehenden sinnlichen Erfahrung geöffnet werden („embodied internet"). Versprochen wird ein immersives Erleben seitens der Nutzer*innen, wodurch soziales Miteinander, mobiles Arbeiten, Lernen, aber auch Handel plattformübergreifend und weltweit möglich sein sollen. Hierbei wird betont, dass das Metaverse und seine Entwicklung aktiv von den Nutzer*innen mitgestaltet werden kann und auch muss. Das Metaverse wird in dieser Vision als omnipotente, weltumspannende Plattform skizziert, die sowohl in ihrem inhaltlichen als auch technischen Potenzial nahezu unbegrenzt wachsen soll: ein Freiraum mit unbegrenzten Möglichkeiten. Diese Vision ruft sofort Fragen der Sicherheit hervor, sprich des Schutzes vor Beleidigungen, Belästigungen, (psychischer) Gewalt oder vor radikalen und extremistischen Kommunikationsangeboten. Bislang ist der Schutz der Partizipierenden in der virtuellen Interaktivität allein in Bezug auf den jeweiligen individuellen virtuellen Space definiert.

Um das mögliche Potenzial für extremistische Kommunikationsangebote im Metaverse und die damit einhergehende Herausforderung für Sicherheitsbehörden einzuschätzen, wird mithilfe eines „Vision Assessments" ein Expert*innen-Workshop durchgeführt (Hausstein/Lösch 2020). Das Metaverse stellt eine Vision dar, die sich durch drei Kriterien von anderen Zukunftsvorstellungen abgrenzt:

1. Die Vision des Metaverse ist (noch) nicht institutionalisiert und einer breiten Öffentlichkeit unhinterfragt vertraut, sondern hat gegebenenfalls Befürworter*innen und Gegner*innen, weil sie eine konkrete, richtungsweisende Idee präsentiert.

2. Sie nimmt normative Setzungen vor, indem sie die vorgestellte Zukunft als wünschenswert auszeichnet, womit sie ein höheres Mobilisierungspotenzial aufweist.

3. Sie entstammt keiner wissenschaftlich reflektierten Entwicklung, die Orientierung bietet oder Entscheidungen ermöglicht. Vielmehr macht diese Vision durch ihre normativen Setzungen Alternativen gerade unsichtbar.

Ziel des Vision-Assessment-Workshops ist es, Szenarien zu entwickeln, die Alternativen sichtbar machen, Orientierung bieten und zum Austausch über kollektive Erwartungen sowie normative Setzungen anregen. Dieser Workshop soll die Basis für eine breitere Vertrautheit mit der Vision des Metaverse schaffen und erste Überlegungen zur Spannung von Freiheit und Sicherheit im Metaverse anstellen. Gerade in letzterer Hinsicht lohnt es sich, frühzeitig über die Potenziale im Metaverse für extremistische Inhalte und Aktivitäten zu reflektieren.

Extremistische Gruppen reagieren zumeist auf Visionen von außen: Auf der einen Seite grenzen sie sich von Visionen ab oder greifen sogar Technologien an, die zu Spannungen mit den eigenen ideologischen Prämissen führen, wie sich im Fall des rechtsextremen Akzelerationismus gezeigt hat (Loadenthal 2021). Auf der anderen Seite machen sie sich Visionen zu eigen, indem sie diese anhand der eigenen Ideologien modulieren oder erweitern, um damit die eigenen Ziele besser kommunizieren zu können, wie es die Taliban in ihrem Umgang mit den sozialen Medien eindrücklich demonstriert haben (Atiq 2021).

Die wichtigsten Felder, in denen extremistische Akteur*innen aktiv und kreativ bleiben müssen und die damit auch zur Anwendung prädestiniert sind, sind Grooming und Radikalisierung, extremistische Organisation (klandestine Kommunikation und Finanzierung) sowie extremistische Aktion (Zieldefinition, Aktionsformen, Aktionsdurchführung). Dies sind drei zentrale Handlungsbereiche extremistischer Organisationen, die mithilfe technologischer Innovation verbessert werden können. Inwieweit das Metaverse Potenziale für extremistische Kommunikationsangebote in allen drei Handlungsfeldern bietet, soll in dem Expert*innen-Workshop herausgearbeitet und bewertet werden.

Literatur

Aden, H. & Fährmann, J. (2019). *Defizite der Polizeirechtsentwicklung und Techniknutzung,* in: Zeitschrift für Rechtspolitik, 52(6), 175–178.

Aden, H.& Fährmann, J. (2020). *Datenschutz-Folgenabschätzung und Transparenzdefizite der Techniknutzung: Eine Untersuchung am Beispiel der polizeilichen Datenverarbeitungstechnologie,* in: TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, 29(3), 24–29.

Amoore, L. & de Goede, M. (2021). *Datawars: Reflections twenty years after 9/11,* in: Critical Studies on Terrorism, 14(4), 425–429.

Atiq, S. (2021). *The Taliban embrace social media: "We too want to change perceptions".* BBC News. Abrufbar unter: https://www.bbc.com/news/world-asia-58466939 [03.03.2022].

BMI. (2018). *Polizei 2020: White Paper. Bundesministerium des Inneren.* Abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/polizei-2020-white-paper.pdf?__blob=publicationFile&v=1 [14.03.2022].

Bröckling, U. (2015). *Der präventive Imperativ und die Ökonomisierung des Sozialen,* in: Public Health Forum, 21(4), 29–31.

Bundeszentrale für politische Bildung. (2019). *Datenökonomie. Aus Politik und Zeitgeschichte,* 69(24–26), 1–56.

Clarke, M. (2021). *"No Cracks, no Blind Spots, no Gaps": Technologically-Enabled "Preventative" Counterterrorism and Mass Repression in Xinjiang, China,* in: Henschke, A., Reed, S., Robbins, S. & Miller, S. (Hrsg.). Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism, Cham, 121–137.

FutureBridge. (2020). *4D Printing – The Technology of the Future. FutureBridge.* Abrufbar unter: https://www.futurebridge.com/industry/perspectives-mobility/4d-printing-the-technology-of-the-future/ [26.04.2021].

Gandorfer, S. (2018). *Was ist Artificial Intelligence- (AIaaS) oder Machine Learning as a Service (MLaaS)?* Abrufbar unter: https://www.it-business.de/was-ist-artificial-intelligence-aiaas-oder-machine-learning-as-a-service-mlaas-a-790408/ [26.04.2021].

Gerhold, L. & Brandes, E. (2021). *Sociotechnical imagineries of a secure future,* in: European Journal of Futures Research, 9:7, 1-19. Abrufbar unter: https://doi.org/10.1186/s40309-021-00176-1 [23.06.2021].

Grünwald, R. & Kehl, C. (2020). *Autonome Waffensysteme. Endbericht zum TA-Projekt.* TAB-Arbeitsbericht Nr. 187. Berlin. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB).

Guhl, J. & Davey, J. (2020). *A Safe Space to Hate: White Supremacist Mobilisation on Telegram.* Institute for Strategic Dialogue. Abrufbar unter: https://www.isdglobal.org/isd-publications/a-safe-space-to-hate-white-supremacist-mobilisation-on-telegram/ [08.03.2022].

Häder, M. (2014). *Delphi-Befragungen: Ein Arbeitsbuch (3. Aufl.).* Wiesbaden. VS Verlag für Sozialwissenschaften.

Hardy, J. (2021). *The Rise of the Modern Intelligence State,* in: Henschke, A., Reed, A., Robbins, S. & Miller, S. (Hrsg.). Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism, Cham, 105–120.

Hausstein, A. & Lösch, A. (2020). *Clash of Visions: Analysing Practices of Politicizing the Future.* BEHEMOTH – A Journal on Civilisation, 13(1), 83–97.

Hegemann, L., Sontheimer, L. & Becker, G. (2020). *Palantir Technologies: Die geheimnisvollen Datensortierer.* Die Zeit. Abrufbar unter: https://www.zeit.de/digital/internet/2020-09/palantir-technologies-daten-analyse-boersengang-peter-thiel-alex-karp/komplettansicht [14.02.2022].

In 't Veld, S. (2020). *Palantir is not our friend.* About:Intel. Abrufbar unter: https://aboutintel.eu/palantir-eu-independence/ [05.05.2022].

Kaufmann, S. (2016). *Security Through Technology? Logic, Ambivalence and Paradoxes of Technologised Security,* in: European Journal for Security Research, 1(1), 77–95.

Kurz, C. (2020). *Gesichtserkennung—Kampagne für ein dauerhaftes europaweites Verbot.* netzpolitik.org. Abrufbar unter: https://netzpolitik.org/2020/gesichtserkennung-kampagne-fuer-ein-dauerhaftes-europaweites-verbot/ [04.05.2022].

Kusche, I. (2022). *Politische Öffentlichkeit, Desinformation und das Problem von Deepfakes,* in: Bahr, A. & Fröhlich, G. (Hrsg.). Authentizität und Inauthentizität von (medialen) Artefakten, im Erscheinen.

Kusche, I., Andres, f., Büscher, C., Gazos, A., Hahn, J., Ladikas, M., Röller, T. & Scherz, C. (2021). *MOTRA-Technologiemonitoring,* in: Kemmesies, U., Wetzels, P., Austin, B., Dessecker, A., Grande, E., Kusche, I. & Rieger, D. (Hrsg.). MOTRA-Monitor 2020, Wiesbaden, 188–205.

Kusche, I., & Büscher, C. (2021). *Technologiemonitoring zur Prävention von Extremismus und terroristischer Gewalt,* in: Gesellschaft unter Spannung. Verhandlungen des 40. Kongresses der Deutschen Gesellschaft für Soziologie 2020. Abrufbar unter: https://publikationen.soziologie.de/index.php/kongressband_2020/article/view/1307 [14.12.2020].

Loadenthal, M. (2021). *Infrastructure, Sabotage, and Accelerationism. GNET.* Abrufbar unter: https://gnet-research.org/2021/02/15/infrastructure-sabotage-and-accelerationism/ [21.04.2022].

Luhmann, N. (2005). *Reflexive Mechanismen, in: Luhmann, N. (Hrsg.).* Soziologische Aufklärung 1: Aufsätze zur Theorie sozialer Systeme (7. Aufl.), Wiesbaden, 116–142.

Makropoulos, M. (1990). *Möglichkeitsbändigungen, Disziplin und Versicherung als Konzepte zur sozialen Steuerung von Kontingenz,* in: Soziale Welt, 41(4), 407–423.

Marx, G. T. (2004). *What's new about the "new surveillance"?: Classifying for change and continuity,* in: Knowledge, Technology & Policy, 17(1), 18–37.

Meister, A. (2020). *Gilles de Kerchove – Anti-Terror-Koordinator der EU fordert Gesetz gegen Verschlüsselung.* netzpolitik.org. Abrufbar unter: https://netzpolitik.org/2020/eu-beamter-fordert-gesetz-gegen-verschluesselung/ [04.05.2022].

Miller, S. & Bossomaier, T. (2021). *Privacy, Encryption and Counter-Terrorism,* in: Henschke, A., Reed, A., Robbins, S. & Miller, S. (Hrsg.). Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism, Cham, 139–154.

Monroy, M. (2020). *Rasterfahndung – Europol nutzt Palantir.* netzpolitik.org. Abrufbar unter: https://netzpolitik.org/2020/europol-nutzt-palantir/ [07.10.2020].

Pelzer, R. (2018). *Policing of Terrorism Using Data from Social Media,* in: European Journal for Security Research, 3(2), 163–179.

Robbins, S. (2021). *Facial Recognition for Counter-Terrorism: Neither a Ban Nor a Free-for-All,* in: Henschke, A., Reed, A., Robbins, S. & Miller, S. (Hrsg.). Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism, Cham, 89–104.

Schiller, K. (2018). *Was ist eine DApp (dezentralisierte App)?* Blockchainwelt. Abrufbar unter: https://blockchainwelt.de/dapp-dezentralisierte-app-dapps/ [26.04.2021].

Snijders, D., Biesiot, M., Munnichs, G. & van Est, R. (2020). *Citizens and sensors – Eight rules for using sensors to promote security and quality of life.* Den Haag, Rathenau-Institut.

Weimann, G. (2019). Going Darker? *The Challenge of Dark Net Terrorism.* Wilson Center. Abrufbar unter: http://cyber.haifa.ac.il/images/Publications/darkweb_Gabriel%20Weimann.pdf [04.04.2020].