Karlsruher Institut für Technologie

MOTRA-Technologiemonitoring

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

Zusammenfassung

*Das Technologiemonitoring hat als Teil des MOTRA-Monitoringsystems die Aufgabe, die Rolle neuer technologischer Entwicklungen für das Radikalisierungsgeschehen in Deutschland zu beleuchten. Dies geschieht in einem auf Technikfolgen spezialisierten Forschungskontext, der berücksichtigt, dass die Zwecke, für die Technologien genutzt werden, nicht feststehen. Zwecke verändern sich im Laufe von Technikentwicklung und -verwendung und Technologien lassen sich auf innovative Weise kombinieren oder gebrauchen. Ziel des Technologiemonitorings ist es, neue Technologien zu identifizieren, die für das Problemfeld Extremismus und gewaltaffine Radikalisierung relevant sind, mitsamt ihren Folgen, sofern sie auf dieses Problemfeld zurückwirken. Dazu gehören sowohl die Technologienutzung durch extremistische oder gewaltaffine Akteure als auch die Technologienutzung durch Akteure der zivilen Sicherheit und deren rechtliche und ethische Folgen. Der Prozess des Technologiemonitorings besteht aus drei Schritten, die bei kontinuierlichem Monitoring immer wieder durchlaufen werden: (1) Ein Grobradar sammelt Überblickswissen zu einem Pool potenziell relevanter technologischer Entwicklungen; (2) Ein Selektionsmechanismus, der systematisch Expert*innen einbezieht, mündet in Entscheidungen darüber, welche Entwicklungen besonders intensiv untersucht werden müssen; (3) Feinanalysen nehmen solche Untersuchungen für ausgewählte Technologien vor.*

Stichworte

Radikalisierung | Extremismus | Terrorismus | Technologien | Innovation | Technikfolgen

Warum ein Technologiemonitoring?

Vielleicht war es noch nie so offensichtlich wie heute: Wenn Extremist*innen ihr Gedankengut verbreiten oder gar terroristische Anschläge vorbereiten, koordinieren und durchführen, sind Technologien im Spiel. Im Internet finden sich Anleitungen zum Bombenbau (Stenersen 2013) und zur Herstellung von Schusswaffen mit Hilfe von 3D-Druckern (Flade und Mascolo 2020). Messenger-Dienste wie Telegram bieten sowohl die Möglichkeit, propagandistische Botschaften breit zu streuen, als auch verschlüsselt mit wenigen Vertrauten zu kommunizieren (Clifford und Powell 2019) und sich zu Anschlägen zu verabreden oder Attentäter*innen aus der Ferne zu dirigieren.

Gleichzeitig sind bestimmte Technologien längst zur unabdingbaren Grundlage gesellschaftlicher Funktionen geworden. Eine wachsende gesellschaftliche Abhängigkeit von solchen Technologien sowie ihre Vernetzung und Konvergenz untereinander haben dazu geführt, dass sie zu den kritischen Infrastrukturen einer modernen Gesellschaft gehören. Die gesellschaftlichen Auswirkungen einer Störung oder eines Ausfalls dieser Infrastrukturen zeigen sich am offensichtlichsten bei Technologien, die eine reibungslose Energieversorgung (Petermann et al. 2011) und digitale Vernetzung (Gandorfer 2020) ermöglichen. Extremistische Akteure könnten diese und andere Vulnerabilitäten mit potenziell verheerenden Folgen ausnutzen und angreifen.

Daneben bieten Technologien wie Drohnen oder die Gesichtserkennung mit Hilfe von lernenden Algorithmen den Sicherheitsbehörden aber auch neue Möglichkeiten der Überwachung und Prävention. Damit stellt sich immer wieder die Frage, ob das, was in diesem Zusammenhang technisch machbar wäre, auch gesellschaftlich wünschenswert ist. Rechtliche Regeln, etwa im Zusammenhang mit Datenschutz und informationeller Selbstbestimmung, werden potenziell in Frage gestellt. Das tun sowohl Befürworter*innen neuer Überwachungsmöglichkeiten, 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 der neuen technologischen Möglichkeiten noch zu gewährleisten (Kurz 2020). Hier ist die Reflexion auf zentrale demokratische Werte, von denen Sicherheit nur

einer ist, ein wichtiger Aspekt bei der Einschätzung von Verwendungsmöglichkeiten neuer Technologien.

Es gibt also drei zentrale Gründe dafür, im Rahmen eines Monitoringsystems, das sich auf Entwicklungen im Zusammenhang mit Radikalisierung und Extremismus konzentriert, auch ein Monitoring neuer technologischer Entwicklungen zu betreiben:

1. Extremistische Akteure haben sich in den letzten Jahren solche Entwicklungen immer wieder zunutze gemacht, um ihre Ziele zu verfolgen.

2. Die zunehmende Vernetzung und Konvergenz von Technologien, die als Infrastrukturen viele gesellschaftliche Routinen überhaupt erst ermöglichen, schafft potenziell neue Vulnerabilitäten, die extremistische Akteure 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.

Aus dem ersten Punkt ergibt sich für das MOTRA-Technologiemonitoring eine enge Zusammenarbeit mit dem Modul Internetmonitoring im Rahmen von MOTRA. Ein erheblicher Teil jener technologischen Innovationen, die für extremistische Akteure potenziell interessant sind, betrifft die Kommunikation im Internet, z. B. Möglichkeiten der Verschlüsselung und Anonymisierung. Für die anderen MOTRA-Teilprojekte liefert das Technologiemonitoring wichtige Hintergrundinformationen, die unter anderem Hinweise zu möglichen künftigen Protestanlässen (z. B. die Ablehnung von Überwachung) oder strategischen Zielen extremistischer Akteure liefern können.

Zum Verhältnis von Technikfolgenabschätzung und MOTRA-Technologiemonitoring

Das MOTRA-Technologiemonitoring wird am Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) durchgeführt, also in einem auf Technikfolgenforschung spezialisierten Forschungskontext. Solche

Forschungskontexte haben sich mit unterschiedlichen Schwerpunkten und zu unterschiedlichen Zeitpunkten seit dem Ende der 1960er Jahre in Nordeuropa und verschiedenen westeuropäischen Ländern etabliert. Sie reagieren auf die Erfahrung von unerwarteten und zum Teil schwerwiegenden Technikfolgen, die vor der Verbreitung von Technologien nicht, oder nicht hinreichend, berücksichtigt worden waren (Grunwald 2019).

Technikfolgenabschätzung (TA) ist vor diesem Hintergrund mit der allgemeinen Erwartung verbunden, die sozialen, ethischen und politischen Konsequenzen neuer Technologien umfassend zu analysieren. TA entwickelt dazu Theorien und Methoden, um etwas anderes zu sehen als diejenigen Zwecksetzer, die erfinden, finanzieren oder nutzen (Bechmann 2007, p. 35). Erwartungen an ein Technologiemonitoring im Rahmen von MOTRA sind grundsätzlich ähnlich gelagert, aber nicht deckungsgleich. Die intuitive Unterscheidung zwischen (nützlichen) Zwecken und zu vermeidenden Nebenfolgen sowie nicht-bestimmungsgemäßem Gebrauch einer Technologie ist wenig hilfreich, sobald mitbedacht wird, dass sich im Laufe der Technikgenese und -verwendung Zwecke verändern, mehrere Technologien rekombinieren lassen und viele Innovationen mit dem nicht-bestimmungsgemäßen Gebrauch schon vorhandener Technologien verbunden sind. Für MOTRA sind zum einen insbesondere intentionale Folgen der Rekombination von Technologien und ihres (im Sinne der Entwickler*innen) nicht-bestimmungsgemäßen Gebrauchs durch extremistische Akteure relevant. Bei der Technologienutzung durch Akteure der zivilen Sicherheit sind zum anderen rechtliche und ethische Folgen zu berücksichtigen.

Für das Ziel eines Technologiemonitorings im Bereich Extremismus und Radikalisierung ergeben sich daraus hohe Anforderungen an die Breite des Monitorings sowie ein Selektionsproblem, was die Auswahl bestimmter Entwicklungen für eine vertiefende Betrachtung angeht. Zur Lösung orientieren wir uns an einem Monitoringprozess, der im Rahmen des ITAS-Projektes „Zukünftige Themen der Innovations- und Technikanalyse (ITA)“ (Decker et al. 2012) entwickelt wurde. Bestand dessen Ziel darin, neue Themen für die Innovations- und Technikanalyse zu identifizieren, ist das Ziel unseres Technologiemonitorings, neue Technologien zu identifizieren, die für das Problemfeld Radikalisierung und Extremismus relevant sind, mitsamt ihren Folgen, sofern sie auf dieses Problemfeld zurückwirken.

Der Monitoring-Prozess besteht aus drei Schritten, die bei kontinuierlichem Monitoring immer wieder durchlaufen werden (vgl. Abbildung 1). Für die Zwecke des MOTRA-Technologiemonitorings geht es im ersten Schritt – dem Grobradar – darum, Überblickswissen mit Bezug auf einen Pool technologischer Entwicklungen zu sammeln, die möglicherweise relevant sind. Die Einschätzung der tatsächlichen Relevanz wird im zweiten Schritt mit Hilfe von externen Expert*innen/Stakeholdern vorgenommen, die im Rahmen von Workshops oder anderen Formaten mit Szenarien zu möglichen Effekten bestimmter Technologien auf Radikalisierungsprozesse und dem Umgang von Akteuren ziviler Sicherheit mit diesen konfrontiert werden. Ziel dieses zweiten Schrittes ist es, eine auf Expertenwissen 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 Akteure ziviler Sicherheit, die auf diese Phänomene reagieren, auszuloten.

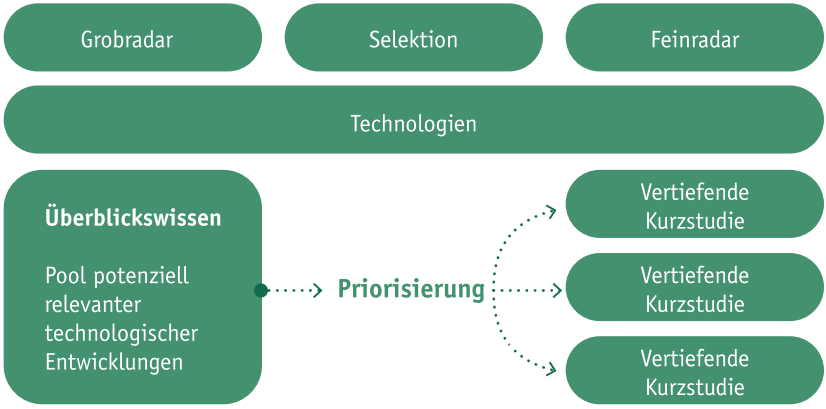

Abbildung 1: Monitoringprozess

Zur theoretischen und methodischen Konzeption des Grobradars

Der Grobradar orientiert sich an der Unterscheidung zwischen der Verfügbarkeit von Technologien (Technology-Push-Perspektive) und dem Bedarf an bestimmten Technologien (Demand-Pull-Perspektive). Bezugspunkt ist dabei die zentrale Akteurskonstellation im Themenfeld Radikalisierung und Extremismus, nämlich das Gegeneinander von extremistischen Akteuren einerseits und Sicherheitsbehörden andererseits. Jede Seite reagiert dabei auf die Strategien der jeweils anderen. Für jede Seite ergeben sich aus dieser Konstellation typische Dauerprobleme, für deren Lösung sie gegebenenfalls auf Technologien zurückgreifen (vgl. Abbildung 2).

Betrachten wir zunächst die Seite der Sicherheitsbehörden. Für sie ist das Problem zentral, wie radikalisierende Akteure sich beobachten lassen, um extremistische Radikalisierungen und Gewalttaten verhindern zu können. Mögliche Lösungen dieses Problems werfen hinsichtlich gesamtgesellschaftlicher Folgen oft rechtliche, politische und ethische Fragen auf, nicht zuletzt weil Radikalisierung nicht automatisch in Extremismus und Gewaltbereitschaft mündet (etwa: Gaspar et al. 2018, Kemmesies in diesem Band).

Umgekehrt ist für extremistische Akteure das Problem des Schutzes ihrer Kommunikation vor Beobachtung zentral. Im Falle der Verbreitung extremistischen Gedankenguts geht es ihnen darum, ihre Identität zu verschleiern, im Falle einer gemeinschaftlichen Planung von Gewalttaten darüber hinaus darum, den Inhalt ihrer Kommunikation vor Beobachtung durch Dritte zu schützen. Sofern extremistischen Akteuren Angriffe auf vulnerable Schutzgüter gelingen, können ihre Aktivitäten massive gesamtgesellschaftliche Folgen haben.

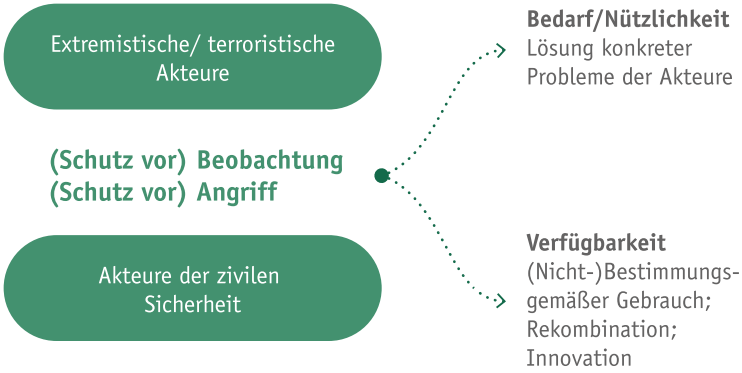

Abbildung 2: Akteurskonstellation

Unser Modell stellt in mehreren Hinsichten eine Vereinfachung gegenüber der komplexen Wirklichkeit dar. Es ist ausgeschlossen und für MOTRA auch nicht zielführend, sämtliche Probleme, die in der täglichen Praxis der Sicherheitsbehörden auftreten, in die Betrachtung einzubeziehen. Ebenso wenig praktikabel ist es, alle Probleme zu betrachten, mit denen extremistische Akteure umgehen müssen. Das Technologiemonitoring konzentriert sich auf die Rolle neuer Technologien bei jenen Problemen, die sich aus dem aufeinander bezogenen Handeln von staatlichen Akteuren ziviler Sicherheit einerseits und extremistischen Akteuren andererseits ergeben. So besteht das Problem des Schutzes von Kommunikation vor Beobachtung für extremistische Akteure eben nur, weil und insofern diese Kommunikation entweder selbst gegen Gesetze verstößt oder Hinweise auf künftige Gesetzesverstöße enthält. Komplementär dazu ergibt sich das Problem der Beobachtung extremistischer Akteure für die Sicherheitsbehörden nur, weil und insofern diese gegen Gesetze verstoßen oder erwartet wird, dass sie das in der Zukunft tun werden.

Wir vereinfachen auch die Bezüge zwischen dieser zentralen Akteurskonstellation und ihrer gesellschaftlichen Umwelt. So ist es unmöglich, dem Anspruch einer Technikfolgenabschätzung gemäß sämtliche gesellschaftliche Folgen zu betrachten, die sich daraus ergeben können, dass staatliche Akteure der zivilen Sicherheit zur Lösung ihres zentralen Problems bestimmte Technologien verwenden. Wir konzentrieren uns deswegen auf

zwei Folgenkomplexe: mögliche Folgen für die Grundrechte und Folgen, die zwar rechtskonform sind, unter ethischen Gesichtspunkten aber dennoch problematisch. Andere Folgenkomplexe, z. B. mögliche wirtschaftliche Folgen, die die Nachfrage nach bestimmten Technologien hat, klammern wir aus.

Auch die gesellschaftlichen Folgen der Nutzung bestimmter Technologien durch extremistische Akteure können wir nicht erschöpfend betrachten. So ist z. B. denkbar, dass das Wissen darum, dass extremistische Akteure bevorzugt bestimmte Technologien nutzen, die Technologienutzung anderer Akteure beeinflusst, oder das Kommunikationsverhalten extremistischer Akteure in sozialen Netzwerken – etwa die Nutzung von Social Bots zur Verbreitung von Botschaften, wie sie im nächsten Abschnitt skizziert wird – Folgen für das allgemeine Vertrauen in solche Netzwerke hat. Wir konzentrieren uns beim Technologiemonitoring dagegen auf Folgen, die die Nutzung von Technologien durch extremistische Akteure für vulnerable Schutzgüter, insbesondere kritische Infrastrukturen, hat.

Für den Grobradar werten wir eine Vielzahl von Literatur- und Internetquellen daraufhin aus, welche Hinweise sie zu für MOTRA relevanten technologischen Entwicklungen enthalten. Dazu gehören verschiedene Fachzeitschriften und periodische Veröffentlichungen zu den Themenfeldern Extremismus/Terrorismus einerseits und Technological Foresight andererseits. Auch das ITAS selbst sowie das Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB) veröffentlichen immer wieder Berichte, die für MOTRA interessante Informationen enthalten. Hinzu kommen Internetblogs und Newsletter zum Thema Technologie sowie unregelmäßige Publikationen für das Themenfeld relevanter Organisationen und Netzwerke, wie etwa die Nichtregierungsorganisation AlgorithmWatch oder das Global Network on Extremism and Technology. Auch Ergebnisse anderer MOTRA-Teilprojekte sollen künftig in den Grobradar einfließen (Abbildung 3).

Ist eine bestimmte technologische Entwicklung oder Neuerung als potenziell relevant identifiziert, wird eine genauere Literaturrecherche dazu durchgeführt, gegebenenfalls ergänzt durch Interviews mit einschlägigen Expert*innen. Leitgesichtspunkt ist dabei jeweils die beschriebene zentrale Akteurskonstellation, also die Frage, wie eine technologische Entwicklung sich auf die Möglichkeiten von bzw. den Schutz vor Überwachung sowie die Möglichkeiten von bzw. den Schutz vor Angriffen auswirken könnte. Die daraus entwickelten Hypothesen lassen sich dann in Form von Miniszenarien oder zugespitzten Aussagen den Expert*innen präsentieren, die im zweiten Schritt des Monitoring-Prozesses eine zentrale Rolle spielen.

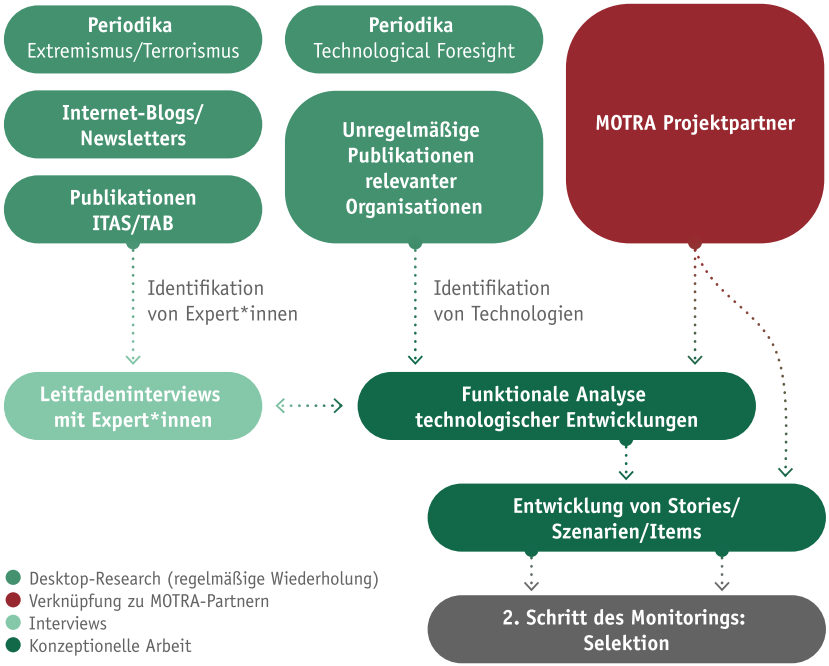

Abbildung 3: Grobradar

Ein Beispiel aus dem Grobradar: Social Bots

Social Bots werden häufig als Mittel für Desinformationskampagnen und automatisierte Propaganda gesehen. Der Begriff *Social Bot* wird allerdings verschieden gebraucht. Nach gängigem Verständnis handelt es sich um eine Unterkategorie von Bots, also von automatisierten Computerprogrammen, die bestimmte, vorher festgelegte Aufgaben erfüllen (Reuter 2019). Social Bots werden als solche bezeichnet, da sie hauptsächlich auf Social-Media-Plattformen agieren, um dort anderen Accounts zu folgen, Inhalte hervorzuheben oder auch maschinell erstellte Beiträge wie Kommentare, Antworten oder Posts zu generieren. Da Social Bots durch Fake-Accounts mit anderen Nutzer*innen einer Plattform in Interaktion treten, sind sie manchmal schwer als Computerprogramm zu erkennen und können so Diskurse und Meinungen beeinflussen (Kind et al. 2017). Auch extremistisches Gedankengut lässt sich auf diese Weise verbreiten.

Expert*innen sind sich hinsichtlich der Definition uneinig darüber, wie viel „realer Mensch" in einem Social Bot enthalten sein kann. Das MOTRA-Technologiemonitoring konzentriert sich aber auf maschinelle Social Bots. Einfache Social Bots können schon mit geringen Programmierkenntnissen erstellt werden. Die erforderlichen Programmcodes und Anleitungen sind im Internet leicht zu finden und frei zugänglich (Kind et al. 2017). Bots können aber auch einzeln oder in größerer Anzahl bei verschiedenen Anbietern im Internet gekauft werden (Hegelich 2016, p. 3; Reuter 2019). Dabei hängen Aufwand oder Preis stark von der Komplexität des Bots ab. Die meisten Social Bots sind sehr einfach aufgebaut und können dementsprechend auch nur einfache Aktionen ausführen. Sie suchen in den Sozialen Medien nach zuvor festgelegten Keywords. Beispielsweise scannen sie Twitter-Timelines oder Facebook-Posts nach bestimmten Wörtern und Hashtags. Wird ein passendes Wort oder Hashtag gefunden, wird der Bot aktiv und liked, teilt oder kommentiert den Beitrag mit vorgefertigten Antworten (Bundeszentrale für politische Bildung 2017).

In großer Anzahl sind gerade diese Bots sehr effizient, da sie gewisse Inhalte und Beiträge hervorheben und somit deren Relevanz künstlich verstärken (können). Umgekehrt können sie Beiträge und Diskussionen, die den Akteuren hinter den Bots unangenehm sind, mit irrelevanten, provozierenden oder beleidigenden Kommentaren überfluten. Durch diese

Überlastung werden die beteiligten realen Personen abgelenkt oder abgeschreckt und ein Austausch erschwert (Bundeszentrale für politische Bildung 2017).

Es ist aber auch möglich, komplexe Social Bots herzustellen, deren Aktivitäten einem realen Social-Media-Account sehr ähnlich sind. Solche Bots können zum Beispiel eigene Texte schreiben und diese posten oder mit anderen Nutzer*innen in Kontakt treten und einen Austausch aufbauen. Sie nutzen dabei nicht vorgefertigte Antworten, sondern erschaffen durch ein generatives Dialogsystem eigene Texte (Pricewaterhouse Coopers 2017, pp. 13–16). Generative Systeme bauen meist auf künstlichen neuronalen Netzen auf und müssen erst mit Dialogen trainiert werden, um selbst „kommunizieren" zu lernen. Der technische Vorteil von generativen Systemen liegt darin, dass die Zuordnung von Eingabe und Antwort nicht durch Regeln konditioniert werden muss, da ein neuronales Netz diese Zusammenhänge selbstständig erlernt, wenn es große Mengen an Trainingsdaten zur Verfügung hat (Pricewaterhouse Coopers 2017) .

Einfache Social Bots lassen sich oft anhand bestimmter Merkmale gut erkennen (Bundeszentrale für politische Bildung 2017). Sehr neue Accounts, das Fehlen eines Profilbilds oder das Absetzen extrem vieler Botschaften pro Tag können Hinweise darauf sein, dass es sich um Bots handelt. Darauf aufbauende technische Klassifizierungstools sind allerdings bislang sehr ungenau und liefern viele falsch negative und falsch positive Ergebnisse. Daher sind auch Schätzungen, wie hoch der Anteil von Social Bots an Aktivitäten im Netz ist, unsicher (Rauchfleisch und Kaiser 2020).

Die sozialwissenschaftliche Literatur diskutiert Social Bots als mehr oder weniger fragwürdiges Instrument in Wahlkampagnen sowie generell als mögliches Instrument zur Beeinflussung öffentlicher Debatten. Die Befürchtung ist nicht, dass Personen ihre politischen Überzeugungen ändern, weil sie Mitteilungen von Social Bots ausgesetzt sind. Aber wenn durch Bots beispielsweise massenhaft radikale Inhalte in einem Diskussionskontext verbreitet werden, kann das dazu führen, dass sich gemäßigte Personen zurückziehen. Personen, die eine radikal entgegengesetzte Position zu den Bot-Nachrichten vertreten, fühlen sich dagegen herausgefordert. So kann ein aufgeheiztes Diskussionsklima entstehen,

das Personen, die tendenziell für radikale Positionen empfänglich sind, ermutigt (Hegelich 2016, pp. 3-4).

Auf den Schirm des Grobradars geraten Social Bots also zunächst, weil sie verschiedenste Inhalte in Sozialen Medien verbreiten können, darunter auch extremistisches Gedankengut. Dabei deutet sich im Zusammenhang mit der zunehmenden Verbreitung von Anwendungen künstlicher neuronaler Netze an, dass Social Bots künftig immer schwerer von echten Nutzer*innen zu unterscheiden sein könnten. Das wäre ein Problem nicht nur für die individuellen Nutzer*innen, die über die Urheberschaft von Botschaften getäuscht werden, sondern auch für Beobachter*innen, z. B. aus der Wissenschaft oder auch aus dem Internetmonitoring von Behörden, die nachvollziehen wollen, wie und durch wen Debatten zu bestimmten Themen geprägt werden.

Vom Grobradar zur Selektion: Internationaler Expertensurvey als Delphi-Befragung

Ziel des zweiten Schrittes im Monitoring-Prozess ist es, unter den technologischen Entwicklungen, die der Grobradar als potenziell relevant identifiziert hat, Prioritäten zu setzen und auszuwählen, welche Technologien samt ihrer möglichen Folgen vertiefend analysiert werden sollten. Die zentralen Kriterien ergeben sich aus der theoretischen Konzeption, die bereits dem Grobradar zugrunde liegt: die erwartete Nützlichkeit und Verfügbarkeit von Technologien, besonders gravierende ethische Implikationen sowie besonders hohes Störungspotenzial für kritische Infrastrukturen. Die Ergebnisse des Grobradars beeinflussen aber nicht nur, mit welchen Inhalten sich die Expert*innen im Schritt der Selektion auseinandersetzen, sondern auch in welcher Weise das am besten geschieht und welche Expert*innen geeignet erscheinen, eine Selektion vorzunehmen. Umgekehrt beeinflusst das Format, das für den Schritt der Selektion gewählt wird, in welche Form die Ergebnisse des Grobradars gebracht werden müssen.

Mit der SARS-CoV-2-Pandemie hat ein Faktor, der mit der Konzeption des Monitoring-Prozesses gar nichts zu tun hat, erhebliche Bedeutung für die Methodenwahl im Projekt bekommen. Die Durchführung eines internationalen Expert*innenworkshops, wie er für den Schritt der Selektion

eigentlich geplant war, ist auf absehbare Zeit nicht möglich. Stattdessen haben wir eine Online-Befragung internationaler Expert*innen konzipiert. Die Befragung zielt auf Einschätzungen zur Nützlichkeit und künftigen Verfügbarkeit verschiedener technologischer Anwendungen. Damit der Fragebogen nicht zu kompliziert wird, sind die Fragen ausschließlich auf die Perspektive der extremistischen Akteure bezogen. Nützlichkeit und Verfügbarkeit von Technologien für die Sicherheitsbehörden und die damit zusammenhängenden ethischen Fragen mussten erst einmal ausgeklammert werden.

Die im Fragebogen formulierten Fragen und zu bewertenden Aussagen sind aus dem ersten Durchlauf des Grobradars abgeleitet. Sie decken daher Technologien ab, die im Prinzip schon existieren, allerdings nicht unbedingt breit verfügbar sind bzw. bei der Verwendung erhebliche Spezialkenntnisse voraussetzen. Expert*innen werden zum einen gebeten, den Grad der Nützlichkeit dieser Technologien für konkret benannte Zwecke einzuschätzen, die für extremistische Akteure relevant sein können. Zum anderen werden Expert*innen darum gebeten einzuschätzen, wann extremistische Akteure tatsächlich Zugriff auf die entsprechende Technologie haben könnten. So wird das oben beschriebene Phänomen der Social Bots in der Befragung als ein Anwendungsfall von Verfahren maschinellen Lernens gefasst, also auf die mögliche Entwicklung komplexer Bots zugespitzt, die natürliches Sprachverhalten täuschend echt imitieren können. Die Expert*innen werden erstens um eine Einschätzung dazu gebeten, wie nützlich solche komplexen Social Bots für extremistische Akteure bei der Verbreitung extremistischer Propaganda wären. Zweitens werden sie danach gefragt, ob und wann extremistische Akteure vermutlich Zugriff auf solche komplexen Social Bots haben werden.

Da es sich hier um unvermeidlich unsichere Einschätzungen handelt, ist die Befragung als Delphi-Studie mit zwei Runden konzipiert (Häder 2014). Das heißt, in einer zweiten Befragungsrunde, die ca. einen Monat nach Abschluss der ersten Runde starten soll, werden die gleichen Fragen noch einmal gestellt, verbunden mit einer Rückmeldung über die Ergebnisse der ersten Runde. So können sich die Expert*innen bei ihren Einschätzungen an anderen orientieren und deren Urteile in die eigenen unsicheren Bewertungen miteinbeziehen.

Der Pool an Expert*innen, die wir für die Befragung kontaktiert haben, speist sich erstens aus Autor*innen von Artikeln in Fachzeitschriften, Blogs und anderen Publikationen, die im Rahmen des Grobradars als einschlägig identifiziert wurden. Zweitens wurde die institutionelle Anbindung dieser Expert*innen daraufhin geprüft, ob in der betreffenden Organisation weitere Personen mit für uns einschlägiger Expertise arbeiten. Drittens wurden bestehende Kontakte aus anderen einschlägigen Projektzusammenhängen einbezogen.

Ausblick auf 2021

Die zweite Erhebungsrunde der Delphi-Studie wurde Anfang Januar 2021 abgeschlossen. Die Ergebnisse werden eine wichtige Arbeitsgrundlage für das gesamte Jahr 2021 sein. Vertiefende Interviews mit ausgewählten Expert*innen werden sich auf Befunde aus der Online-Befragung stützen und unterschiedliche Einschätzungen dazu einholen, welche Schlussfolgerungen aus ihnen zu ziehen sind. Nachdem die Delphi-Studie sich auf die Frage des zukünftigen Technologiegebrauchs durch extremistische Akteure konzentriert hat, sollen dabei Perspektiven von Vertreter*innen der Sicherheitsbehörden in den Fokus gerückt werden. Hier sollen neben den funktionalen Aspekten bestimmter technologischer Entwicklungen, also Fragen der Nützlichkeit und Verfügbarkeit, insbesondere auch ethische Probleme thematisiert werden. Als Expert*innen werden in diesem Zusammenhang auch Vertreter*innen von Nichtregierungsorganisationen einbezogen, die sich kritisch mit staatlicher und nicht-staatlicher Überwachung von Bürger*innen befassen.

Darüber hinaus soll 2021 mit dem *Vision Assessment* eine am ITAS entwickelte Methode zum Einsatz kommen, die die Wirkmacht von Leitbildern und Visionen in Innovations- und Transformationsprozessen untersucht. Die Hypothese ist, dass gegenwärtige Visionen soziotechnischer Zukünfte auch für die Rolle von Technologien im Themenfeld Extremismus und Radikalisierung von Bedeutung sind. Das *Vision Assessment* ergänzt mit Blick auf die Priorisierung von Technologien für vertiefende Studien die Delphi-Befragung. Es nimmt die Verknüpfung und gegebenenfalls auch Vermischung mehrerer technologischer Entwicklungen im Rahmen von Leitbildern ernst, die gegenwärtige Entscheidungen orientieren, aus

denen sich Folgen für die zukünftige Verfügbarkeit und gesellschaftliche Erwünschtheit bestimmter technologischer Anwendungen ergeben.

Literatur

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

Bundeszentrale für politische Bildung (2017). *Was sind Social Bots?* [WWW Document]. bpb.de. URL https://www.bpb.de/252585/was-sind-social-bots (accessed 10.9.20).

Clifford, B., Powell, H.C. (2019). *Encrypted Extremism. Inside the English-Speaking Islamic State Ecosystem on Telegram.*

Decker, M., Fleischer, T., Schippl, J., Weinberger, N. (2012). *Zukünftige Themen der Innovations- und Technikanalyse: Methodik und ausgewählte Ergebnisse – Einführung (No. 7605)*, KIT Scientific Reports. https://doi.org/10.5445/KSP/1000025609

Flade, F., Mascolo, G. (2020). *Tod aus dem 3-D-Drucker.* Süddeutsche Zeitung.

Gandorfer, S. (2020). *Digitaler Schutz des öffentlichen Lebens.*

Gaspar, H.A., Daase, C., Deitelhoff, N., Junk, J., Sold, M. (2018). *Was ist Radikalisierung? Präzisierungen eines umstrittenen Begriffs* (PRIF Report No. 5/2018). Frankfurt.

Grunwald, A. (2019). *Technology assessment in practice and theory.* Routledge, Taylor & Francis Group, London; New York.

Häder, M. (2014). *Delphi-Befragungen: ein Arbeitsbuch,* 3. Auflage. ed, Springer-Lehrbuch. Springer VS, Wiesbaden.

Hegelich, S. (2016). *Invasion der Meinungs-Roboter. Analysen & Argumente 9.*

Kind, S., Jetzke, T., Weide, S., Ehrenberg-Silies, S., Bovenschulte, M. (2017). *Social Bots. TA-Vorstudie (No. 3),* Horizon-Scanning. TAB – Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag.

Kurz, C. (2020). *Gesichtserkennung – Kampagne für ein dauerhaftes europaweites Verbot.* netzpolitik.org. URL https://netzpolitik.org/2020/gesichtserkennung-kampagne-fuer-ein-dauerhaftes-europaweites-verbot/ (accessed 9.30.20).

Meister, A. (2020). Gilles de Kerchove – *Anti-Terror-Koordinator der EU fordert Gesetz gegen Verschlüsselung.* netzpolitik.org. URL https://netzpolitik.org/2020/eu-beamter-fordert-gesetz-gegen-verschluesselung/ (accessed 5.18.20).

Petermann, T., Bradke, H., Lüllmann, A., Poetzsch, M., Riehm, U. (2011). *Was bei einem Blackout geschieht. Folgen eines langandauernden und großflächigen Stromausfalls.,* Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag. Nomos Verlag, Berlin.

Pricewaterhouse Coopers (2017). *Social Bots: Gefahr für die Demokratie? White Paper mit Handlungsempfehlungen für Unternehmen,* Medien und Politik.

Rauchfleisch, A., Kaiser, J. (2020). *The False Positive Problem of Automatic Bot Detection in Social Science Research.* SSRN Journal. https://doi.org/10.2139/ssrn.3565233

Reuter, M. (2019). *Social Bots: Was nicht erkannt werden kann, sollte nicht reguliert werden.* netzpolitik.org. URL https://netzpolitik.org/2019/social-bots-was-nicht-erkannt-werden-kann-sollte-nicht-reguliert-werden/ (accessed 6.10.20).

Stenersen, A. (2013). *‚Bomb-Making for Beginners': Inside al Al-Qaeda E-Learning Course.* Perspectives on Terrorism, 7, 13.