Global Network
on Extremism & Technology

GNET-Umfrage zur Rolle von Technologie im gewalttätigen Extremismus und zum Stand der Beziehungen zwischen Forschungsgemeinschaft und Technologiebranche

Lydia Khalil

GNET ist ein Sonderprojekt des International Centre for the Study of Radicalisation, King's College London.

Die Autorin dieses Berichts ist Lydia Khalil, Research Fellow, Lowy Institute.

Danksagungen
Die Autorin dankt Dr. Maura Conway für ihren Rat bei der Ausarbeitung der Fragen, J. M. Berger für seine Einsichten, den Lowy-KollegInnen Natasha Kassam und Alex Oliver für ihre Erfahrungen und Erkenntnisse aus ihrer eigenen Entwicklung von Umfragen sowie Dr. Matteo Vergani für seinen Beitrag zu den Fragen. Ohne die Mitwirkung der vielen Wissenschaftler und Experten, die diese Umfrage trotz aller anderen Anforderungen an ihre Zeit und ihre Ressourcen bereitwillig beantwortet haben, wäre dieser Bericht nicht möglich gewesen. Etwaige Fehler bei der Gestaltung und Analyse der Umfrage liegen allein in der Verantwortung der Autorin.

KONTAKTANGABEN

Im Falle von Fragen oder zur Anforderung weiterer Exemplare wenden Sie sich bitte an:

ICSR
King's College London
Strand
London WC2R 2LS
Vereinigtes Königreich

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Wie alle anderen GNET-Publikationen kann auch dieser Bericht kostenlos von der GNET-Website unter www.gnet-research.org heruntergeladen werden.

Kurzfassung

Welche Rolle spielt Technologie, insbesondere die computergestützte Kommunikation, im gewalttätigen Extremismus? Dies ist die zentrale Frage hinter der Arbeit des Global Network on Extremism and Technology (GNET) als eine Initiative von Wissenschaft und Technologiebranche. Extremistische Akteure gehörten zu den frühesten Nutzern des Internets und erkannten schnell dessen Potenzial als Instrument für die Kommunikation und Mobilisierung. Fragen rund um die Rolle von Technologie und Extremismus beschäftigen Forscher seit Jahrzehnten, insbesondere jedoch seit dem Aufkommen des Islamischen Staates und der Zunahme von durch rechte Ideologien motiviertem gewalttätigem Extremismus sowie dem raschen Aufstieg gewalttätiger konspirativer extremistischer Bewegungen wie QAnon, der weitgehend durch das Internet begünstigt wurde.

Das Lowy Institute hat nun eine Umfrage unter Wissenschaftlern im Bereich Terrorismus und gewalttätiger Extremismus zu Facetten dieser Kernfrage durchgeführt, um bisherige Literaturübersichten zur Rolle von Internettechnologie und Extremismus zu ergänzen, um ein aktuelles Verständnis der Forschungserkenntnisse zu gewinnen, die möglicherweise nicht in der zuvor ausgewerteten Literatur enthalten sind, und um das Ausmaß der Zusammenarbeit der akademischen Forschungsgemeinschaft mit der Technologiebranche zu verstehen.

Wie die Ergebnisse der Umfrage zeigen, herrscht innerhalb der Forschungsgemeinschaft weitgehende Übereinstimmung, dass internetgestützte Kommunikations- und Social-Media-Plattformen „Schaden in der realen Welt unterstützen, fördern oder mobilisieren“. Laut den Antworten auf detailliertere Fragen ist die Analyse der Rolle von Technologie für den gewalttätigen Extremismus jedoch unglaublich komplex, vielschichtig und immer noch umstritten.

Antworten auf Fragen zu Kontakten von Forschern mit der Technologiebranche ergaben, dass dies ein potenziell fruchtbarer, aber auch heikler Bereich ist – ähnlich, wie es in der Terrorismusforschung Zwiespälte und Überlegungen zur Zusammenarbeit mit Regierungen und Sicherheitsbehörden sowie Bedenken hinsichtlich der Versicherheitlichung der akademischen Forschung gibt. Eine Reihe von Antworten lassen Zynismus hinsichtlich der Kontakte der Technologiebranche mit der akademischen Gemeinschaft erkennen und bringen diverse Bedenken zum Ausdruck, darunter die Undurchsichtigkeit und mangelnde Transparenz der großen Plattformen, ihre reaktive Natur, unterschiedliche Forschungsprioritäten im Vergleich zur Industrie und Skepsis darüber, wie ernsthaft und wirksam Social-Media-Plattformen gegen gewalttätigen Extremismus und schädliche Desinformation vorgehen.

Inhalt

1 Einleitung

Welche Rolle spielt Technologie, insbesondere die computergestützte Kommunikation, im gewalttätigen Extremismus? Dies ist eine derart weit gefasste Frage, dass sie Folgefragen praktisch erzwingt. Welche Rolle nimmt beispielsweise das Internet, einschließlich der sozialen Medien, im Radikalisierungsprozess ein? Hat die Verwendung sozialer Medien die Produktion von gewalttätigen extremistischen Inhalten und Narrativen sowie den Kontakt damit gesteigert, und werden Menschen durch einen solchen Kontakt bis zur Gewalt radikalisiert? Wird es durch die Verwendung von computergestützter Kommunikation und Social-Media-Plattformen einfacher, Menschen für gewalttätige extremistische Zwecke zu gewinnen oder zu mobilisieren? Sind es also gewisse Eigenschaften der Technologien und Plattformen selbst – ihre Gestaltung, Logik, Affordanz und Einschränkungen –, die zum Extremismus beitragen und ihn begünstigen? Ist die präzise Rolle der Technologie abhängig von der Art der extremistischen Ideologie oder Organisationsstruktur einer bestimmten Bewegung oder gar dem Geschlecht oder Hintergrund einer Person? Wie werden durch Internettechnologie und computergestützte Kommunikation Beziehungen begünstigt oder soziale Online-Ökologien entwickelt, die zum Extremismus beitragen? Selbst wenn eine Person infolge von Online-Kontakten mit extremistischen Narrativen und Inhalten oder der Teilnahme an Online-Subkulturen extremistische Überzeugungen äußert, muss dies zwangsläufig zu Gewalt, Militanz oder anderen Offline-Schäden führen?

Solche Fragen sind keinesfalls erschöpfend oder neu. Extremistische Akteure gehörten zu den frühesten Nutzern des Internets und erkannten schnell dessen Potenzial als Instrument für die Kommunikation und Mobilisierung. Diese und andere Fragen zur Rolle von Technologie und Extremismus beschäftigen Forscher seit Jahrzehnten, insbesondere jedoch seit dem Aufkommen des Islamischen Staates, da sein rasanter Aufstieg, seine globale Reichweite und seine geschickte Nutzung von sozialen Medien die Terrorismusforschung und Organe zur Terrorismusbekämpfung gleichermaßen vor Herausforderungen stellen.

An einem ähnlichen Punkt stehen wir nun mit dem Wachstum des gewalttätigen, durch rechte Ideologien und Verschwörungstheorien motivierten Extremismus. Rechtsextremer Terrorismus hat in den letzten fünf Jahren um 205 % zugenommen;[1] dazu kommt der rasche, durch das Internet begünstigte Aufstieg gewalttätiger konspirativer extremistischer Bewegungen wie QAnon. Obwohl es teilweise heißt, Befürchtungen hinsichtlich dieser auf Verschwörungstheorien gegründeten Bewegung seien möglicherweise übertrieben,[2] wurde

1 Global Terrorism Index (2020), Institute for Economics and Peace, https://www.visionofhumanity.org/global-terrorism-index-2020-the-ten-countries-most-impacted-by-terrorism/
2 CIVIQS (2021) „QAnon Support, Registered Voters“ Live-Umfrage, https://civiqs.com/results/qanon_support?uncertainty=true&annotations=true&zoomIn=true

QAnon vom FBI als inländische extremistische Bedrohung eingestuft[3] und hat in letzter Zeit eine Reihe gewalttätiger Angriffe ausgelöst.[4] Infolge der Corona-Pandemie leben viele Menschen unter einem Schatten der Angst und Unsicherheit und verbringen zugleich viel Zeit online. Der Anstieg der Internet-Nutzung hat (bislang unbelegte) Sorgen ausgelöst, dass dies das Risiko einer Online-Radikalisierung erhöht oder zumindest zu stärkeren Kontakten mit extremistischen Online-Inhalten geführt hat.[5]

Dr. Maura Conway förderte diese Diskussion über die Rolle von Technologie im gewalttätigen Extremismus mit ihrem Artikel „Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research“ von 2017.[6] Sie beschreibt darin, wie sich die Terrorismusforschung mit der Rolle des Internets auseinandersetzt. Doch wie Dr. Conway damals feststellte, gibt es „bislang unzureichende stichhaltige, empirisch fundierte sozialwissenschaftliche Forschung, um diese Fragen überzeugend beantworten zu können“.[7]

Wir haben weiterhin nur wenige definitive Antworten, doch seit der Veröffentlichung des Artikels hat die Extremismus- und Terrorismusforschung gewisse Fortschritte verzeichnet, was Fragen zur Rolle des Internets, zur Kausalität sowie zur Affordanz bestimmter Technologien oder Plattformen für gewalttätige extremistische Akteure betrifft. In den letzten fünf Jahren wurde viel zur Rolle des Internets und anderer Technologien im Extremismus und Terrorismus geforscht. Dabei gab es eine stärkere Zusammenarbeit zwischen Datenwissenschaftlern und Terrorismusforschern aus den Sozialwissenschaften. Im Bereich der Internetforschung erhalten Extremismus und Terrorismus nun mehr Aufmerksamkeit – ähnlich wie zu der Zeit, als die Medien- und Kommunikationswissenschaft und die Sozialpsychologie Verbindungen zur Terrorismusforschung aufbauten.

Allein die Gründung des Global Network on Extremism and Technology sowie die größere Bereitschaft der Technologiebranche einzugestehen (und sei es zögernd), dass ihre Plattformen und Technologien nicht nur von extremistischen Akteuren ausgenutzt werden, sondern dass ihre Affordanz auch zur schnellen Verbreitung extremistischer Ideologien beigetragen hat, haben unser Verständnis vorangebracht.[8] Mainstream-Plattformen befassen sich nun mit ihrer Rolle in der Schaffung extremistischer Online-Umgebungen[9] und ihrem Beitrag zu dem sich wandelnden Charakter des Extremismus und seiner Organisationsstruktur.[10] Auch geht die Industrie stärker auf die Forschung im Feld des gewalttätigen Extremismus ein.

---

3 Jana Winter (2019) „FBI document warns that conspiracy theories are a new domestic terrorism threat“, Yahoo News, https://news.yahoo.com/fbi-documents-conspiracy-theories-terrorism-160000507.html

4 Amarnath Amarasingham und Marc-André Argentino (Juli 2020) „The QAnon Conspiracy Theory: A Security Threat in the Making?“ *CTC Sentinel* Band 13 Nr. 7: S. 37–41, https://ctc.usma.edu/the-qanon-conspiracy-theory-a-security-threat-in-the-making/

5 Caleb Spencer (2020) „Children may have been radicalised during lockdown“, BBC News, https://www.bbc.com/news/uk-wales-53082476

6 Maura Conway (2017) „Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research“, *Studies in Conflict & Terrorism* Band 40 Nr. 1: S. 77–98, DOI: 10.1080/1057610X.2016.1157408

7 Ebd.

8 Mason Youngblood (2020) „Extremist ideology as a complex contagion: the spread of far-right radicalization in the United States between 2005 and 2017“, *Humanities and Social Science Communications* Band 7 Nr. 1: S. 1–10, https://www.nature.com/articles/s41599-020-00546-3

9 Department of Security Studies and Criminology (2020) „Mapping Networks and Narratives of Online Right-Wing Extremists in New South Wales“, http://doi.org/10.5281/zenodo.4071472

10 Bruce Hoffman und Colin Clarke (2020) „The Growing Irrelevance of Organizational Structure of Domestic Terrorism“, The Cipher Brief, https://www.thecipherbrief.com/article/united-states/the-next-american-terrorist

Es häufen sich in der Tat die Beweise dafür, dass Internettechnologie ein wichtiger Faktor für die Begünstigung von Extremismus sein kann. Gleichzeitig wird anerkannt, dass wir noch eingehender untersuchen müssen, was dies genau bedeutet. Nur dann kann eine so weit gefasste Schlussfolgerung überhaupt einen Sinn ergeben. Mittlerweile hat sich ein differenzierteres Verständnis dafür herausgebildet, dass die Internettechnologie gewalttätigen Extremismus zwar nicht unbedingt *verursacht*, aber dennoch *vielfältige* und *unterschiedliche* Rollen einnehmen kann, was die *Begünstigung* von Radikalisierung und Mobilisierung zu gewalttätigem Extremismus betrifft.[11]

Auch wissen wir jetzt, dass es bei konkreten gewalttätigen Verhaltensweisen, die durch extremistische Überzeugungen motiviert sind, „keine einfache Online- und Offline-Dichotomie“ gibt.[12] Und anstatt „Online-Radikalisierung“ pauschal zu konzeptualisieren, ist das Bewusstsein gewachsen, dass Internettechnologien unterschiedliche Rollen im Extremismus-Prozess spielen, diverse Nutzungsmöglichkeiten bieten und diverse Handlungen ermöglichen.[13]

Zudem wird anerkannt, dass sich die Rolle von Technologie in der Radikalisierung und Mobilisierung zur Gewalt im Laufe der Jahrzehnte verschoben hat, parallel zur Weiterentwicklung der Technologie selbst. Der Übergang extremistischer Akteure von statischen Websites und geschlossenen Foren zu öffentlichen sozialen Netzwerken und zurück zu Alt-Tech-Plattformen und dem verdeckten Agieren im „Dark Web“ oder „Deep Web“[14] hat die Rolle des Internets und anderer Technologien im Zusammenhang mit Extremismus erheblich verändert, abhängig von den Affordanzen der jeweiligen Plattform oder Technologie. Neue Technologien, die es in früheren Jahren noch nicht gab, wie z. B. durchgängig verschlüsselte Messaging-Dienste und Drohnentechnologie, haben sich auf die Taktiken, Kommunikation und Aktivitäten extremistischer Akteure ausgewirkt. Weitere technologische Entwicklungen werden ähnliche Veränderungen bewirken. In seinem Artikel über die Frage, ob das Internet zu einer Zunahme des transnationalen Terrorismus geführt hat, stellt David Benson Folgendes fest: „Das Internet ist allgegenwärtig, und deshalb wäre es seltsam, wenn die Terroristen von heute das Internet nicht nutzen würden, genauso wie es seltsam wäre, wenn frühere Terroristen nicht die Post oder das Telefon benutzt hätten.“[15] So wie technologische Fortschritte jeden Aspekt unseres Lebens verändern, nehmen sie auch Einfluss auf Extremismus und Terrorismus.

Bis vor Kurzem ging man davon aus, dass es sich bei der Internettechnologie um ein „unterstützendes Instrument“ handelt: Radikalisierung zur Gewalt, Rekrutierung, Mobilisierung und Anschlagsplanung können durch das Internet unterstützt werden, sind aber nicht unbedingt von ihm abhängig; auch verursacht das

11 Paul Gill, Emily Corner, Amy Thornton und Maura Conway (2015) „What are the roles of the internet in terrorism? Measuring online behaviours of convicted UK terrorists“, VOXPol Network of Excellence, https://www.voxpol.eu/download/vox-pol_publication/What-are-the-Roles-of-the-Internet-in-Terrorism.pdf

12 Paul Gill, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom und John Horgan (2017) „Terrorist Use of the Internet by the Numbers“, *Criminology and Public Policy* Band 16 Nr. 1: S. 99–117

13 Gill et al. „What are the roles of the internet in terrorism?“

14 Das Merriam-Webster Wörterbuch definiert das Dark Web als „eine Reihe von Webseiten im World Wide Web, die sich nicht von Suchmaschinen indexieren oder in Standard-Webbrowsern aufrufen lassen, die spezifische Mittel (wie spezialisierte Software oder Netzwerkkonfiguration) für den Zugriff erfordern und die verschlüsselt sind, um Anonymität und Datenschutz für Benutzer zu bieten“.

15 David C. Benson (2014) „Why the Internet Is Not Increasing Terrorism“, *Security Studies* Band 23 Nr. 2: S. 293–328, DOI: 10.1080/09636412.2014.905353

Internet keine Radikalisierung.[16] Dies mag weiterhin der Fall sein. Allerdings haben Sorgen um die Kausalität der Internettechnologie inmitten der Pandemie und vor allem nach dem Sturm auf das Kapitol in den USA an neuer Dringlichkeit gewonnen. Der Angriff auf das Kapitol brachte ein breites Spektrum an Netzwerken, Gruppierungen und Einzelpersonen zusammen – von organisierten militanten Gruppen bis hin zu individuellen QAnon-Anhängern und Pro-Trump-Aktivisten, vereint durch ihren Glauben an die weitgehend als Online-Desinformation verbreitete „große Lüge", die US-Präsidentschaftswahlen seien gefälscht worden. Diverse etablierte extremistische Gruppen hatten über Monate hinweg in Online-Foren den Boden für den Angriff bereitet,[17] und das offene Internet sowie die großen Social-Media-Plattformen waren überschwemmt von falschen Informationen über den Wahlhergang und die Wahlergebnisse.[18] Auch bei der Durchführung des Angriffs waren soziale Medien stark präsent: Ein vorläufiger Bericht des Program on Extremism der George Washington University ergab, dass 68 % der von den Strafverfolgungsbehörden angeklagten Teilnehmer „ihre mutmaßlichen Verbrechen im Kapitol in Echtzeit dokumentiert haben".[19]

Weiter heißt es in dem Bericht, dass soziale Medien „eine zentrale Rolle bei der Organisation des Angriffs und der Verbreitung von Material spielten, was dazu beitrug, zur Beteiligung anzuregen". Soziale Medien halfen zudem den verschiedenen Gruppen und Einzelpersonen, die am Angriff beteiligt waren, zu interagieren und sich schließlich am 6. Januar 2021 in Washington, D.C., zu versammeln.[20] Die in dem Bericht beschriebenen Fälle zeigen, wie soziale Medien die Bildung spontaner „Cluster" von zuvor nicht miteinander bekannten Personen erleichterten, die sich ohne große Planung fanden und gemeinsam auf den Weg nach Washington machten[21] – in etwa wie ausländische Anhänger, die in ISIS-Gebiete reisten, aber mit weniger Vorlaufzeit, Entfernung oder Barrieren für die Anreise.

Soziale Medien und algorithmische Technologien werden immer mehr Teil unseres täglichen Lebens. Ist es also denkbar, dass das Internet den gewalttätigen Extremismus nicht nur begünstigt, sondern aktiv ermöglicht? In ihrer Studie von 2015 über das Online-Verhalten verurteilter britischer Terroristen stellten Paul Gill, Emily Corner, Amy Thornton und Maura Conway fest, dass „das Internet nicht zu einem Anstieg des Terrorismus geführt hat. Es ist zumeist ein unterstützendes Instrument; Radikalisierung wird durch das Internet ermöglicht, anstatt davon abhängig zu sein."[22]

16 Alexander Meleagrou-Hitchens und Nick Kaderbhai (2017) „Research Perspectives on Online Radicalisation. A literature review, 2006–2016", VoxPol Network of Excellence, https://icsr.info/wp-content/uploads/2017/05/ICSR-Paper_Research-Perspectives-on-Online-Radicalisation-A-Literature-Review-2006-2016.pdf

17 Robert Evans (2021) „How the Insurgent and MAGA Right are Being Welded Together on the Streets of Washington D.C.", Bellingcat, https://www.bellingcat.com/news/americas/2021/01/05/how-the-insurgent-and-maga-right-are-being-welded-together-on-the-streets-of-washington-d-c/

18 Network Contagion Research Institute (2021) „NCRI Assessment of the Capitol Riots – Violent Actors and Ideologies Behind the Events of January 6, 2021", https://networkcontagion.us/wp-content/uploads/NCRI-Assessment-of-the-Capitol-Riots.pdf

19 Program on Extremism der George Washington University (2021) „This is Our House! A Preliminary Assessment of the Capitol Hill Siege Participants", https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/This-Is-Our-House.pdf

20 Ebd.

21 Ebd.

22 Gill et al. „What are the roles of the internet in terrorism?"

Erleben wir jedoch nun die Entstehung „einer neuen Art von Terrorismus, die ohne das Internet nicht existieren kann“?[23] War der Sturm auf das Kapitol ein Beispiel dafür, wie das Internet eine digitale Massenradikalisierung und -mobilisierung begünstigt und hervorruft?[24] Hat die Verwendung des Internets und der stetige Online-Kontakt mit extremistischen Narrativen und Desinformation bei einigen der am Angriff beteiligten Personen – vor allem solchen, die nicht zu bereits etablierten Organisationen gehören – den Prozess ihrer Radikalisierung zur Gewalt beschleunigt? War ihre Radikalisierung zur Gewalt in diesem Fall tatsächlich durch das Internet bestimmt oder davon abhängig? Hat die „Logik“ diverser Plattformen zum Wachstum des Extremismus beigetragen und spielt sie nun eine größere Rolle auf dem Pfad der Radikalisierung einer Person zur Gewalt?

José van Dijck und Thomas Poell haben sich damit beschäftigt, die neue Logik der sozialen Medien zu skizzieren und zu verstehen, wie Social-Media-Plattformen „tief in die Mechanik des Alltagslebens eingedrungen sind“, institutionelle Strukturen beeinflussen und sich auf menschliche Interaktionen auswirken. Dabei vergleichen sie die Logik der sozialen Medien mit der Logik der davor entstandenen Massenmedien und theorisieren, dass die sozialen Medien ein neues Ökosystem geschaffen haben, das „soziale Ordnungen oder Ereignisketten neu gestaltet“. Weil soziale Medien in der Lage sind, ihre Logik mittels der „Strategien, Mechanismen und Ökonomien, die der Dynamik von Social-Media-Plattformen zugrunde liegen“, über ihre Plattformen hinaus zu transportieren, wird die breitere Gesellschaft ihrer Logik und ihren Prinzipien unterworfen.[25]

Während van Dijck und Poell sich nicht spezifisch mit Extremismus befassen, hat der Extremismusforscher J. M. Berger ein ähnliches Argument dazu entwickelt, wie die Logik und der Charakter der computergestützten Kommunikation – und ganz besonders der sozialen Medien – die Bedingungen für soziale Interaktionen grundlegend verändert und unseren öffentlichen Raum auf eine Weise umgestaltet haben, die zu Extremismus geführt hat. Dieser Aufstieg des Internets, insbesondere der sozialen Medien, hat laut Berger „eine unbeständige und unwirtliche Umgebung für den Gedanken einer objektiven Wahrheit“ geschaffen und dadurch zu größerer Unsicherheit und einer zerfaserten „Konsensrealität“ beigetragen. Social-Media-Plattformen haben die Unsicherheit erhöht, weil sie die Verbreitung widersprüchlicher Informationen, Meinungen und Analysen beliebiger Art zugelassen haben.[26] Berger postuliert, dass „soziale Medien ein Umfeld schaffen, in dem mehrere alternative Wahrnehmungen der Realität Unterstützung gewinnen können, indem sie ein messbares Maß an Engagement gewinnen, das ausreicht, um vom Publikum als Konsens verstanden zu werden. Um die durch diese widersprüchlichen Standpunkte entstehende Unsicherheit zu lösen, neigen die Nutzer dazu, sich auf die Bestätigung der wahrgenommenen Realität durch die eigene Gruppe zu stützen, was oft mit Feindseligkeit gegenüber den Ansichten von Fremdgruppen einhergeht.“[27] Es liegt in der

23 Craig Timberg, Drew Harwell, Razzan Nakhlawi und Harrison Smith (2021), „Nothing can stop what's coming: far right forums that fomented Capitol riots voice glee in aftermath“, *The Washington Post*, https://www.washingtonpost.com/technology/2021/01/07/trump-online-siege/

24 Robert Pape und Keven Ruby (2021), „The Capitol Rioters Aren't Like Other Extremists“, *The Atlantic*, https://www.theatlantic.com/ideas/archive/2021/02/the-capitol-rioters-arent-like-other-extremists/617895/

25 José van Dijck und Thomas Poell (2013) „Understanding Social Media Logic“, *Media and Communication* Band 1 Nr. 1: S. 2–14, https://ssrn.com/abstract=2309065

26 J. M. Berger (2020) „Our Consensus Reality Has Shattered“, *The Atlantic*, https://www.theatlantic.com/ideas/archive/2020/10/year-living-uncertainly/616648/

27 Interview mit J. M. Berger, per Nachricht (6. April 2021).

menschlichen Natur, auf diese Zersplitterung der Konsensrealität mit einem entsprechenden Streben nach Gewissheit zu reagieren, und zwar mittels „exklusiver, allumfassender Identitäten – von denen viele toxisch und fragil sind und den Keim des gewalttätigen Extremismus in sich tragen“.[28] Extremismus entsteht auch deshalb, weil der Konsens einer Fremdgruppe als existenzielle Bedrohung wahrgenommen wird, der man entgegenwirken muss. Wie Berger weiter feststellt, gibt es kritische Unterschiede zwischen alten und neuen Medien, insbesondere in Bezug auf das Fehlen von Kontrollfunktionen oder Inhaltsregulierung, die niedrigen Produktionskosten und „Engagement-Metriken, die untrennbar mit der Verbreitung verbunden sind“.[29]

28 J. M. Berger, „Our Consensus Reality Has Shattered“
29 Interview mit J. M. Berger, per Nachricht (6. April 2021).

2 Die Rolle von Technologie im Extremismus

Eine Übersicht der vorhandenen Forschungsliteratur ist eine Möglichkeit, auf die anhaltenden Debatten über die Rolle der Technologie in Bezug auf gewalttätigen Extremismus zu reagieren und die neu auftretenden Themen und Fragen zu untersuchen. In der Tat gab es im Laufe der Jahre eine Reihe hochwertiger Literaturübersichten zur Rolle von Internet und Technologie bei der Radikalisierung und dem gewalttätigen Extremismus.

Der Stand der Literatur

Im Jahr 2013 erstellte RAND Europe eine Literaturübersicht im Rahmen der Studie *Radicalisation in the digital era*, die sich damit beschäftigte, wie das Internet von Personen im Prozess der Radikalisierung genutzt wird. Bei dieser Literaturübersicht, in Kombination mit Primärforschung, kam die Studie zu dem Ergebnis, dass das Internet „die Gelegenheiten zur Radikalisierung erweitert, da es vielen Menschen zur Verfügung steht und die Verbindung mit Gleichgesinnten aus der ganzen Welt rund um die Uhr ermöglicht". Festgestellt wurde zudem, dass das Internet als Echokammer fungieren kann und mehr Gelegenheiten zur Bestätigung extremistischer Überzeugungen bietet als Interaktionen in der realen Welt. Ein weiteres Ergebnis zum damaligen Zeitpunkt war jedoch, dass das Internet diese Radikalisierung nicht unbedingt beschleunigt und auch keinen Ersatz für die notwendige persönliche Interaktion während des Radikalisierungsprozesses darstellt.[30]

2017 erstellten Alexander Meleagrou-Hitchens und Nick Kaderbhai eine Literaturübersicht zur Online-Radikalisierung. Sie erkannten ebenfalls einen „Konsens, dass das Internet allein keine Ursache der Radikalisierung ist, sondern ein Vermittler und Katalysator für den Weg einer Person zu politischen Gewalttaten". Sie zitieren Literatur, die vor einer Überbetonung der Rolle des Internets warnt, wie z. B. Benson (2014). Dieser stellt fest, dass es vorhandenen Studien auch „an unabhängigen und abhängigen Variablen fehlt, die die Nutzung des Internets durch sowohl Terroristen als auch Staaten einschließen, wodurch sie negative Fälle auslassen, die helfen würden, ‚den Nettoeffekt des Internets auf den transnationalen Terrorismus zu ermitteln'".[31]

Wie Meleagrou-Hitchens und Kaderbhai ferner anmerken, ist die Literatur zur Rolle von Technologie und der Online-Umgebung für die Radikalisierung umstritten, weil das Konzept der Radikalisierung in der Extremismusforschung selbst umstritten bleibt. Es herrscht jedoch Konsens darüber, dass Radikalisierung zur Gewalt ein sozialer Prozess ist und dass das Internet, insbesondere soziale Medien, soziale Räume

30 Ines von Behr, Anais Reding, Charlie Edwards NS Luke Gribbon (o. D.) „Radicalisation in the digital era", RAND, https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf
31 Meleagrou-Hitchens und Kaderbhai, „Research Perspectives on Online Radicalisation"

bietet, die die Bildung von Eigengruppen und Fremdgruppen fördern, die Identitätsbildung unterstützen sowie Plattformen für Influencer und Anführer bieten.

Laut ihrer Schlussfolgerung „argumentiert die überwiegende Mehrheit der Autoren, dass das Internet zwar eine unterstützende Rolle spielt, die Person aber in den meisten Fällen auch noch mit Netzwerken in der realen Welt in Kontakt stehen muss. Eine Untersuchung des Wegs einer Person ist daher oft eine Untersuchung des einzigartigen Zusammenspiels zwischen Online- und Offline-Interaktionen."[32] Eine neuere Studie von Tinia Gaudette, Ryan Scrivens und Vivek Venkatesh aus dem Jahr 2020, die sich auf Tiefeninterviews mit ehemaligen gewalttätigen Extremisten in Kanada stützte, kam zu einem etwas anderen Ergebnis: „Unabhängig davon, wie Personen zuerst gewalttätigen extremistischen Ideologien und Gruppen begegnen, ist es das Internet, das letztendlich Prozesse der gewalttätigen Radikalisierung erleichtert, indem es ihnen ermöglicht, in extremistische Inhalte und Netzwerke einzutauchen – ein Ergebnis, das durch empirische Forschung zum Internet und seiner Begünstigung einer Reihe von gewalttätigen extremistischen Bewegungen im Allgemeinen und der rechtsextremen Bewegung im Besonderen belegt ist."[33] Diese Studie kanadischer ehemaliger Extremisten kommt damit zu ähnlichen Ergebnissen wie eine frühere Studie von Koehler aus dem Jahr 2014 über deutsche Ex-Extremisten und ihre Internetnutzung. Koehler stellt darin fest, dass „basierend auf dem verwendeten Material das Internet im Vergleich zu anderen ‚Sozialisationsinstitutionen' wie Offline-Gruppenaktivitäten, Musik und Konzerte, Kundgebungen und politischen Schulungen offenbar das wichtigste Element ist, das individuelle Radikalisierungsprozesse vorantreibt".[34]

Eine weitere systematische Übersicht aus dem Jahr 2018 befasste sich ausschließlich mit empirischen Studien, um die Frage zu beantworten, welche Zusammenhänge zwischen Online-Kontakten mit gewalttätigen radikalisierten Inhalten und gewalttätigen radikalen Online- oder Offline-Ergebnissen bestehen. Ihr Fazit: „Die Rolle des Internets scheint also eine entscheidungsfördernde zu sein, die in Verbindung mit Offline-Faktoren mit der Entscheidungsfindung assoziiert werden kann." Bei der Materialsuche im Zusammenhang mit dieser systematischen Übersicht wurden 5.182 Studien gefunden, von denen jedoch nur elf die Bedingungen für eine Aufnahme erfüllten[35] – eine schockierend niedrige Zahl, die den Mangel an empirisch fundierter Forschung zu dieser Zeit unterstreicht.

Im Jahr 2019 wurde eine weitere systematische Literaturübersicht durchgeführt; bei der Literatursuche, welche die Jahre 2000 bis 2019 abdeckte, fand man 88 geeignete Studien zur Untersuchung der Rolle des Internets im rechtsradikalen und dschihadistischen Extremismus. Allerdings ging es in diesen Studien um die Merkmale und Inhalte verwendeter Websites, nicht um die Internet-Gewohnheiten der Nutzer

32 Ebd.
33 Tiana Gaudette, Ryan Scrivens und Vivek Venkatesh (2020) „The Role of the Internet in Violent Extremism: Insights from Former Right-Wing Extremists", *Terrorism and Political Violence*, DOI: 10.1080/09546553.2020.1784147
34 Daniel Koehler (2014) „The Radical Online: Individual Radicalization Processes and the Role of the Internet", *Journal for Deradicalization*, Band Winter 2014/2015 Nr. 1: https://journals.sfu.ca/jd/index.php/jd/article/view/8/8
35 Ghadya Hassan et al. (2018) „Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence", *International Journal of Development Science* Band 12 Nr. 1–2: S. 71–88

selbst.[36] Die AutorInnen kamen zu dem Schluss, dass „bestehende Studien bisher die Nutzer der verfügbaren Seiten nicht ausreichend untersucht haben und auch nicht die kausalen Mechanismen betrachtet haben, die sich an der Schnittstelle zwischen dem Internet und seinen Nutzern entfalten". Es gibt nur sehr wenige Studien, die sich mit individuellen Nutzern, ihrem Nutzungsverlauf sowie ihren Motivationen und Online-Erfahrungen befassen.

In jüngerer Zeit erstellten Charlie Winter, Peter Neumann, Alexander Meleagrou-Hitchens, Magnus Ranstorp, Lorenzo Vidino und Johanna Fürst 2020 eine Literaturübersicht dazu, wie und für welche Zwecke das Internet von gewalttätigen Extremisten auf organisatorischer und individueller Ebene genutzt wird.[37] Darin stellten sie fest, dass das Internet genauso, wie es für alle Menschen von zentraler Bedeutung ist, auch „zu einer primären operativen Umgebung geworden ist, in der politische Ideologien verwirklicht, Angriffe geplant und soziale Bewegungen begründet werden".[38] Als Grund für diese Entwicklung führen sie an, dass „Online-Extremismus oft einfach eine intuitive Nutzung des Internets ist". Extremisten nutzen das Internet auf die gleiche Weise wie wir alle. Und während die Verbreitung und der gestiegene Konsum von extremistischer Propaganda im Internet allein nicht zu einer Radikalisierung führt, können Online-Räume als Foren für soziale Kontakte und Interaktionen dienen, die zu einer Radikalisierung und Mobilisierung zur Gewalt beitragen können.[39] Online-Räume sind soziale Räume; sie können Identität, Bestätigung, Gemeinschaft und Sinngehalt bieten und funktionieren damit ähnlich wie soziale Räume in der realen Welt. Die Übersicht kommt zu dem Schluss, dass zwar keine kausalen Zusammenhänge zwischen Internettechnologien und Extremismus gefunden oder strukturelle Schlussfolgerungen gezogen werden konnten, „es aber außer Frage steht, dass extremistische Organisationen ohne ihre geschickte Nutzung virtueller Terrains nicht so weit gekommen wären".

Einschränkungen und Daten

Diese und ähnliche systematische Übersichten leisten einen wichtigen Beitrag zum Verständnis des aktuellen Wissensstands und zur Bewertung der Rolle von Internettechnologien im gewalttätigen Extremismus durch die Forschung. Wie allerdings in vielen dieser Literaturübersichten festgestellt wurde, war die gesichtete Literatur stark auf die Untersuchung dschihadistischer Akteure ausgerichtet, weil hier ein Forschungsschwerpunkt liegt. Die Übersichten haben sich daher eher weniger mit anderen Ideologien beschäftigt, insbesondere rechtsgerichteten Ideologien, die inzwischen in vielen Ländern weltweit eine erhebliche Bedrohung darstellen und Gegenstand einer zunehmenden Anzahl neuer Forschungsarbeiten sind.[40] Dazu kommt, dass die Übersichten auf Forschungsliteratur aus der Zeit vor der Pandemie beruhen, so dass deren volle Auswirkungen auf die Gesellschaft und den Extremismus noch nicht untersucht wurden.

36 Ozen Odog, Anne Leiser und Klaus Boehnke (2019) „Reviewing the Role of the Internet in Radicalisation Processes", *Journal for Deradicalisation* Nr. 21, https://journals.sfu.ca/jd/index.php/jd/article/view/289
37 Charlie Winter et al. (2020) „Online Extremism: Research Trends in Internet Activism, Radicalization and Counter-strategies", *International Journal of Conflict Violence* Band 14
38 Ebd.
39 Department of Security Studies and Criminology, „Mapping Networks"
40 Meleagrou-Hitchens und Kaderbhai, „Research Perspectives on Online Radicalisation"

Anzumerken ist auch, dass Forschungsergebnisse immer nur so gut sind wie die zugrunde liegenden Daten, und eine Literaturübersicht ist weniger in der Lage, Fragen rund um den Datenzugang von Forschern angemessen zu beleuchten. Dies wiederum hat erhebliche Auswirkungen auf die Art und Qualität der gesichteten Literatur und das Ausmaß der Zusammenarbeit mit der Technologiebranche.

Frühe Bedenken über den Stand der Terrorismusforschung bezogen sich auf den mangelnden Zugang zu Daten und den fehlenden Datenaustausch von Regierungsseite.[41] Seit dieser anfänglichen Kritik an Terrorismus- und Extremismusstudien hinsichtlich des Mangels an datengestützter Forschung sind jedoch Fortschritte in der empirisch fundierten Forschung[42] und der Verwendung von Primärdaten[43] zu verzeichnen.[44] Doch obwohl das Internet von Daten überschwemmt ist, besteht nach wie vor ein Mangel an datengestützten Studien über die Rolle von Technologie, Extremismus und Online-Radikalisierung, wie viele der oben erwähnten Literaturübersichten zeigen.[45] In „Terrorist Use of the Internet by the Numbers", veröffentlicht im Jahr 2017, stellten die AutorInnen bei der Untersuchung von 200 Zusammenfassungen von Forschungsartikeln zum Thema „Online-Radikalisierung" fest, dass nur 6,5 % irgendeine Form von Daten verwendeten und nur 2 % davon Primärdaten.[46] Die oben erwähnten systematischen Übersichten von 2018 und 2019 kamen zu ähnlichen Ergebnissen.

In einem aktualisierten Artikel von 2020 zu der Frage, wie man bei der Erforschung der Rolle des Internets im gewalttätigen Extremismus weiterkommen kann, stellten Ryan Scrivens, Paul Gill und Maura Conway fest, dass es immer noch ein Problem mit dem Zugang zu Primärdaten, ihrer Sammlung und ihrer Interpretation gibt.[47] Ihre Vorschläge zur Wissensvermehrung in diesem Bereich konzentrieren sich hauptsächlich auf Daten. Zu ihren fünf Vorschlägen gehören „das Sammeln von Primärdaten über mehrere Arten von Populationen" und „die Bereitstellung von Archiven mit gewalttätigen extremistischen Online-Inhalten für Forscher und auf benutzerfreundlichen Plattformen".[48] Diese Probleme im Zusammenhang mit empirischen Beweisen haben Forscher daran gehindert, zu überzeugenden Schlussfolgerungen zu gelangen.[49]

Ironischerweise begannen genau zu dem Zeitpunkt, als die Terrorismusforschung anfing, Primärdaten aus der extremistischen Nutzung von Social-Media-Plattformen einzubeziehen, große Social-Media-Unternehmen damit, gewalttätige extremistische Akteure konsequenter und umfassender von ihren Plattformen auszuschließen und ihre Nutzungsbedingungen strenger durchzusetzen. Ein Hauptgrund dafür, dass Fragen zur Rolle des Internets weiterhin unbeantwortet bleiben, ist das Problem des Datenzugriffs, der weiterhin in den

41 M. Sageman (2014) „The stagnation in terrorism research", *Terrorism and Political Violence* Band 26 Nr. 4: S. 565–80, DOI: 10.1080/09546553.2014.895649
42 Sarah Knight und David A. Keatley (2020) „How can the literature inform counter terrorism practice? Recent advances and remaining challenges", *Behavioral Sciences of Terrorism and Political Aggression* Band 12 Nr. 3: S. 217–30, DOI: 10.1080/19434472.2019.1666894
43 Bart Schuurman (2020) „Research on Terrorism, 2007–2016 Review of Data, Methods, and Authorship", *Terrorism and Political Violence* Band 32 Nr. 5: S. 1011–1026, DOI: 10.1080/09546553.2018.1439023
44 Bart Schuurman und Quirine Eijkman (2013) „Moving Terrorism Research Forward: The Crucial Role of Primary Sources", ICCT Background Note, https://www.icct.nl/app/uploads/download/file/Schuurman-and-Eijkman-Moving-Terrorism-Research-Forward-June-2013.pdf
45 Gill et al., „Terrorist Use of the Internet by the Numbers"
46 Ebd.
47 Ryan Scrivens, Paul Gill und Maura Conway (2020) „The Role of the Internet in Facilitating Violent Extremism and Terrorism: Suggestions for Progressing Research", in T. J. Holt, A. M. Bossler (Hg.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, https://doi.org/10.1007/978-3-319-78440-3_61
48 Ebd.
49 Meleagrou-Hitchens und Kaderbhai, „Research Perspectives on Online Radicalisation"

Händen der Technologieunternehmen liegt. Der Versuch, zum aktuellen Verständnis der Rolle des Internets im Extremismus und Terrorismus beizutragen, erfordert also einen anderen Ansatz – insbesondere hinsichtlich der Zusammenarbeit der Forschungsgemeinschaft mit den Social-Media-Plattformen, die den Großteil der Daten übermitteln, die für die Untersuchung der Rolle der Technologie im Radikalisierungs- und Gewaltprozess relevant sind.

3 Umfrage

Das Lowy Institute hat eine Umfrage unter Wissenschaftlern im Bereich Terrorismus und gewalttätiger Extremismus durchgeführt, um bisherige Literaturübersichten zu Internettechnologie und Extremismus zu ergänzen, um ein aktuelles Verständnis der Forschungserkenntnisse zu gewinnen, die möglicherweise nicht in der zuvor ausgewerteten Literatur enthalten sind, und um das Ausmaß der Zusammenarbeit der akademischen Forschungsgemeinschaft mit der Technologiebranche zu verstehen.

Anhand mehrerer Quellen wurde dazu eine Datenbank von Wissenschaftlern und Experten erstellt, die in den Redaktionsausschüssen der führenden Fachzeitschriften für Terrorismus- und Extremismusforschung vertreten waren: *Studies in Conflict and Terrorism*, *Terrorism and Political Violence*, *Critical Studies on Terrorism*, *Journal for Policing Intelligence and Counterterrorism*, *CTC Sentinel*, *Perspectives on Terrorism*, *Journal of Democracy and Security*, *Journal for DeRadicalization*, *Behavioral Sciences of Terrorism and Political Aggression* sowie *Dynamics of Asymmetric Conflict*. Aufgenommen wurden ferner GNET Associate Fellows und Mitwirkende von GNET Insight, deren Arbeit sich auf das Internet und Extremismus konzentriert, sowie weitere Experten, die anerkannten Forschungsinstituten und -Netzwerken angehören, darunter das Program on Extremism der George Washington University, das Resolve Network, das Centre for the Analysis of Radical Right, Vox Pol, das Institute for Strategic Dialogue, das National Consortium for the Study of Terrorism and Responses to Terrorism, Hadayah, das AVERT Research Network, TSAS und andere. Neben etablierten Forschern wurden über Forschungskonferenzprogramme wie die TASM Conference on Terrorism and Social Media der Universität Swansea auch Forscher im Anfangsstadium ihrer Karriere und solche, die sich mit Themen rund um Terrorismus und Technologie beschäftigen, identifiziert.

Diese Personen in der Datenbank erhielten dann den webbasierten Fragebogen zusammen mit der Bitte, den Umfrage-Link auch an andere Personen mit einschlägigem Fachwissen weiterzuleiten. Teilnehmer konnten auf Wunsch anonym bleiben und waren nicht verpflichtet, ihren Namen oder ihre Zugehörigkeit anzugeben. Rund 158 Forscher im Bereich Terrorismus und gewalttätiger Extremismus nahmen an der Umfrage teil. Dieser Bericht fasst einige der Erkenntnisse aus der Umfrage zusammen und stellt die Ergebnisse zu einer Reihe von Fragen vor. Die gesamte Umfrage bestand aus 44 Fragen; dieser Bericht fasst die meisten, wenn auch nicht alle Antworten zusammen.

Der Ansatz der Expertenbefragung weist gewisse Einschränkungen auf. Die hier präsentierten Ergebnisse basieren auf einer nicht zufälligen Stichprobe und geben nur die Ansichten der Personen wieder, die den Fragebogen beantwortet haben. Abgesehen von den oben beschriebenen Kriterien für den Aufbau der Datenbank potenzieller Teilnehmer haben wir keine weitere Methode entwickelt, um zu ermitteln, inwieweit sich die einzelnen Teilnehmer mit den Themen Technologie und Extremismus beschäftigen. Angesichts

der Tatsache, dass viele Befragte anonym bleiben wollten, konnten wir das Niveau der Forschungskompetenz und -erfahrung bei der Beantwortung der Fragen nicht identifizieren und verifizieren. Dazu kommt, dass Forscher und Experten mit relevanter Forschungserfahrung zu diesen Themen möglicherweise nicht an der Umfrage teilgenommen haben.

Von den 84 Personen, die bereit waren, die Frage nach der „aktuellen Zugehörigkeit" zu beantworten, nannten 72 % Universitäten oder Wissenschaft als ihren primären Sektor. Weitere 12 % nannten Think Tanks oder politische Institute; die übrigen Antworten verteilten sich auf interne Forschung in Technologieunternehmen, Beratung sowie Nichtregierungsorganisationen und Organisationen der Zivilgesellschaft. Unter allen Befragten (n=158) ist die Politikwissenschaft für die meisten das primäre Fachgebiet (42 %); die restlichen Befragten nannten als primäres Fachgebiet hauptsächlich Soziologie, Kriminologie, Psychologie, Kommunikation und Geschichte.

Die Mehrheit der Befragten (n=158) gaben Nordamerika (44 %) und Europa (48 %) als ihren primären geografischen Forschungsschwerpunkt an. Die Befragten nannten auch den Nahen Osten (23 %), Asien (15 %) und Ozeanien (20 %) als geografische Forschungsschwerpunkte (die Befragten durften mehr als einen geografischen Schwerpunkt angeben). Der Fokus auf Nordamerika und Europa ist wahrscheinlich darauf zurückzuführen, dass die meisten Forscher in der Datenbank und damit die meisten Umfrageteilnehmer in Nordamerika und Europa ansässig sind oder aus diesen Regionen stammen. Ein weiterer Grund ist aber wahrscheinlich auch, dass der derzeitige Bedrohungsfokus der Forschungsgemeinschaft auf dem Rechtsextremismus aus Nordamerika, Europa und Ozeanien und in geringerem Maße auch aus Asien liegt.

Als Teilnehmer jedoch gefragt wurden „Zu welcher extremistischen Ideologie haben Sie geforscht?" und alle zutreffenden Antworten auswählen konnten, wählte der gleiche Prozentsatz „Dschihadismus" und „Rechtsextremismus" (79 % bzw. 80 %). Ein geringerer Prozentsatz der Teilnehmer wählte „rassistisch oder ethnisch motivierter gewalttätiger Extremismus" (41 %), „Linksextremismus" (29 %), „Incel" (22 %) und „Sonstige" (17 %).

Rolle des Internets und der sozialen Medien im Extremismus

Der erste Teil der Umfrage konzentrierte sich auf die Ansichten von Experten zur Rolle des Internets – und insbesondere der sozialen Medien – im Extremismus. Die Formulierung dieser Fragen war bewusst darauf ausgerichtet, keine Meinungen oder Eindrücke einzuholen. Vielmehr sollten die Teilnehmer ihre Antworten auf „empirisch fundierte Forschung" gründen, die sie entweder selbst durchgeführt oder in ihrer Arbeit verwendet haben.

In der ersten Frage ging es um die Einschätzung dazu, ob extremistische Online-Aktivitäten das Verlangen nach realen Handlungen befriedigen oder ob sie Personen vielmehr zu Offline-Handlungen anspornen,

ermutigen oder mobilisieren. Auf die Frage, ob die internetgestützte Kommunikation und Online-Aktivitäten extremistischer Akteure „Schaden in der realen Welt unterstützen, anregen oder mobilisieren", „ein Verlangen nach Aktion oder Teilnahme an Extremismus allein durch virtuelle Aktivitäten stillen" oder „beides", wählten die meisten Teilnehmer entweder „unterstützen, anregen oder mobilisieren" (60 %) oder „beides" (36 %); nur wenige waren der Ansicht, Online-Aktivitäten würden ein Verlangen nach Aktion oder Teilnahme an Extremismus allein auf virtuelle Weise stillen (unter 1 %). Laut den Kommentaren von Teilnehmern erleichtern Online-Aktivitäten die Planung und Ausführung von Angriffen (z. B. Logistik, Finanzierung, Humanressourcen), die Motivation oder Beeinflussung zur Ausübung von Gewalt und das Feiern oder Hochspielen vorheriger Angriffe, was andere zu ähnlichen Handlungen anregen könnte. Mehrere Teilnehmer wiesen zudem darauf hin, dass die „dschihadistischen Videos [zum Beispiel] im Besitz von Personen, die wegen Terrorismus verhaftet und angeklagt wurden, ein Indikator für die unterstützende Funktion des [Internets] sind", ebenso wie Studien zu gefassten Dschihadisten, die aussagen, die Kommunikationen hätten eine starke Wirkung auf sie gehabt. Diese Einschätzung der meisten Teilnehmer, dass Schäden in der realen Welt durch Online-Aktivitäten unterstützt, gefördert oder mobilisiert werden können, stimmt mit den jüngsten Ergebnissen einer repräsentativen Stichprobe in den USA überein, die „E-Partizipation" im weiteren Sinne untersuchte. Darin wurde festgestellt, dass „Formen des Ausdrucks und der Interaktion online mit einer stärkeren Bürgerbeteiligung offline verbunden sind".[50]

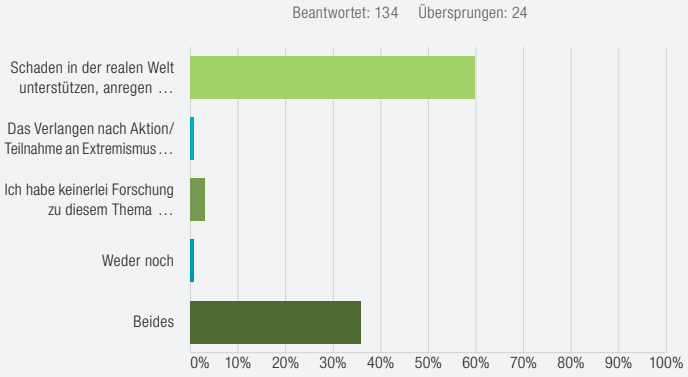
Die Mehrheit der Befragten stimmt also der Aussage zu, Online-Aktivitäten würden zu Offline-Schaden führen. Interessant ist dies, da einige Forschungsergebnisse – und einige Umfrageteilnehmer – darauf hinwiesen, dass manche Personen sich ausschließlich auf Online-Aktivitäten beschränken und kein Offline-Risiko darstellen, weil ihre Online-Aktivitäten das Bedürfnis gestillt hat, ihre Standpunkte zu artikulieren und zu verfechten und ihrem Unmut Luft zu machen.[51] Darüber hinaus haben frühere Studien über Dschihadisten ergeben, dass virtuelle Aktivitäten eine ähnliche Legitimität und Wirkung haben können wie Offline-Aktivitäten und somit möglicherweise die Notwendigkeit für dschihadistische Aktionen in der realen Welt verringern. Studien von Akil Awan und anderen haben gezeigt, dass der „virtuelle Dschihad" oder „mediale Dschihad" eine legitime und glaubwürdige Alternative zur realen Militanz darstellt.[52] So wurde beispielsweise das virtuelle Kalifat des Islamischen Staates als ebenso wichtig angesehen[53] wie das territoriale Kalifat in Syrien und im Irak; tatsächlich waren beide eng miteinander verwoben.[54]

Dazu kommt, dass Technologie immer mehr ein Teil unseres täglichen Lebens wird und die Dichotomie zwischen online und offline schwindet. Wie ein Teilnehmer feststellte, „kann Schaden in der realen Welt auch Handlungen in der digitalen Welt beinhalten. Online-Taten wirken sich auf die reale Welt aus. Das Swatting, Trollen, Stalken, Doxxing

50 K. Tai, G. Porumbescu und J. Shon (2020) „Can e-participation stimulate offline citizen participation: an empirical test with practical implications", DOI: 10.1080/14719037.2019.1584233
51 J. Suler (2004) „The online disinhibition effect", *Cyberpsychology and Behavior*, DOI: 10.1089/1094931041291295
52 A. Hoskins, A. Awan und B. O'Loughlin (2011) *Radicalisation and Media: Connectivity and Terrorism in the New Media Ecology* (1. Aufl.), Routledge, https://doi.org/10.4324/9780203829677
53 Charlie Winter (2015) „The Virtual Caliphate: Understanding Islamic State's Propaganda Strategy", Quilliam, https://www.stratcomcoe.org/charlie-winter-virtual-caliphate-understanding-islamic-states-propaganda-strategy
54 Haroro Ingram und Craig Whiteside (2017) „In Search of the Virtual Caliphate", *War on the Rocks*, https://warontherocks.com/2017/09/in-search-of-the-virtual-caliphate-convenient-fallacy-dangerous-distraction/

und Beschimpfen von Menschen online hat erhebliche Auswirkungen in der realen Welt." Internetgestützte Kommunikation und Aktivitäten haben digitale und reale Umgebungen miteinander verschmolzen.[55] Diese Verschmelzung zeigt zudem auf, dass es einer ganzheitlicheren Konzeptualisierung von Online und Offline bedarf. Andere Teilnehmer fügten ihren Antworten gewisse Vorbehalte hinzu; sie würden zwar die Schlussfolgerung unterstützen, dass Online-Aktivitäten zu Schäden in der realen Welt führen, dies sei aber kein „linearer oder unidirektionaler Prozess. Online- und Offline-Dynamiken unterstützen und erzeugen sich gegenseitig."

F7: Würden Sie auf Grundlage empirischer Forschung zu Extremismus und Technologie, die Sie durchgeführt oder gesehen haben, sagen, dass die internetgestützte Kommunikation und Online-Aktivitäten



ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Schaden in der realen Welt unterstützen, anregen oder mobilisieren	59,70 %	80
Das Verlangen nach Aktion/Teilnahme an Extremismus allein durch virtuelle Aktivitäten stillen	0,75 %	1
Ich habe keinerlei Forschung zu diesem Thema betrieben oder gesehen	2,99 %	4
Weder noch	0,75 %	1
Beides	35,82 %	48
SUMME		134

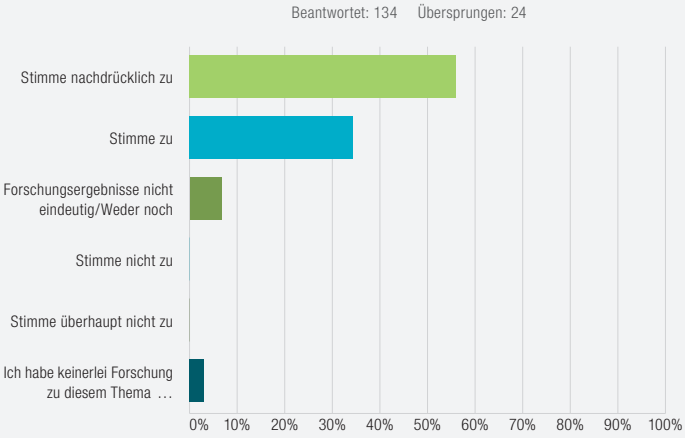
In den nachfolgenden Fragen, die sich auf die Nutzung des Internets durch Extremisten zur Mittelbeschaffung, Rekrutierung, Mobilisierung und Planung gewalttätiger Aktionen bezogen, wurde diese eher allgemeine Frage weiter aufgeschlüsselt.

Hinsichtlich der Rekrutierung und der Frage, ob die internetgestützte Kommunikation die Rekrutierung von Personen für extremistische Bewegungen erleichtert hat, gab es eine breite Zustimmung. Fast 90 % der Befragten stimmten zu bzw. stimmten nachdrücklich zu. Doch obwohl zu dieser Frage ein breiter Konsens zu bestehen scheint, ist die Definition und Begrifflichkeit von „Rekrutierung" im Online-Raum nicht eindeutig festgelegt. Dies könnte spezifische Rekrutierungsprozesse über computervermittelte

55 D. Valentini, A. M. Lorusso und A. Stephan (2020) „Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization"" *Frontiers in Psychology* Nr. 11: S. 524, https://doi.org/10.3389/fpsyg.2020.00524; B. Ducol (2015) „Radical sociability: in defense of an online/offline multidimensional approach to radicalization", in M. Bouchard (Hg.) *Social Networks, Terrorism and Counter-Terrorism: Radical and Connected* (New York, NY: Routledge): S. 82–104

Mechanismen bedeuten, aber auch breitere soziale Beeinflussung oder die Schaffung von Gemeinschaften durch strategische Kommunikationsbemühungen extremistischer Gruppen im Internet. Außerdem gibt es wenig bis gar keine vergleichende Forschung über das Umfeld vor und nach dem Internet hinsichtlich der Rekrutierung. Es besteht jedoch weitgehend Einigkeit darüber, dass das Internet – mehr als andere Technologien der Vergangenheit – die Reichweite extremistischer Botschaften erhöht und extremistischen Gruppen einen breiteren, schnelleren und effizienteren Zugang zu potenziellen Rekruten verschafft hat. Wie ein Teilnehmer feststellte: „Eine Reihe von Forschungsarbeiten hat gezeigt, wie soziale Medien es ansonsten nicht miteinander verbundenen Personen ermöglichen, extremistische Gruppen zu erreichen und von ihnen erreicht zu werden, und wie sie die Abhängigkeit von formalen Organisationsstrukturen als Mittel zur Rekrutierung beseitigen."

F9: Die Nutzung von internetgestützter Kommunikation und/oder Social-Media-Plattformen durch extremistische Akteure hat es einfacher gemacht, Personen für extremistische Bewegungen zu rekrutieren.



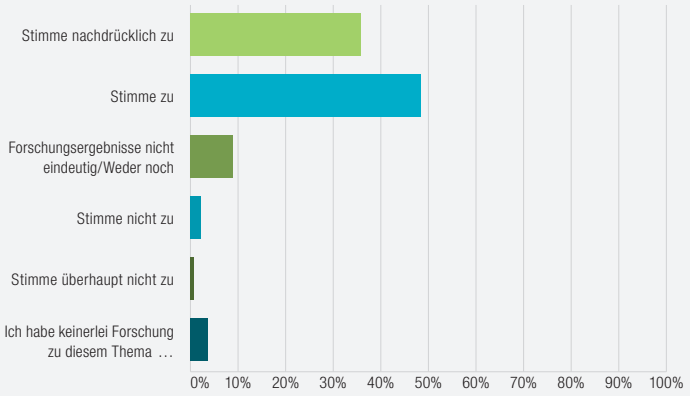
ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Stimme nachdrücklich zu	55,97 %	75
Stimme zu	34,33 %	46
Forschungsergebnisse nicht eindeutig/Weder noch	6,72 %	9
Stimme nicht zu	0,00 %	0
Stimme überhaupt nicht zu	0,00 %	0
Ich habe keinerlei Forschung zu diesem Thema betrieben oder gesehen	2,99 %	4
SUMME		134

Auch auf die Frage, ob das Internet die Planung von Anschlägen oder die Mobilisierung zu Gewalttaten erleichtert hat, erklärte die Mehrheit der Befragten (84 %) ihre Zustimmung bzw. nachdrückliche Zustimmung. Ein Befragter fasste die Rolle des Internets wie folgt zusammen: „Das Internet und insbesondere die verschlüsselte Kommunikation über soziale Medien haben den Fluss von Informationen, Ressourcen, taktischer und logistischer Unterstützung und Echtzeit-Kontakten verstärkt, was wiederum frühere Hindernisse für die Durchführung von Angriffen beseitigt oder abgeflacht hat".

Doch während das Internet einerseits das Recherchieren, Planen und Koordinieren von Gewalttaten erleichtert hat, profitieren andererseits auch die Strafverfolgungsbehörden davon. Zahlreiche geplante Anschläge konnten dank auf Online-Plattformen gesammelten Beweisen vereitelt oder strafrechtlich verfolgt werden. Viele der Befragten fügten Vorbehalte zu ihren Antworten hinzu; sie führten an, dass die internetgestützte Kommunikation, insbesondere verschlüsselte Kommunikation, zwar die Mobilisierung erleichtert haben mag, die detaillierte Planung von Anschlägen aber tatsächlich oft offline stattfindet, insbesondere bei ausgeklügelten Plänen.

F10: Die Nutzung von internetgestützter Kommunikation und/oder Social-Media-Plattformen durch extremistische Akteure hat es einfacher gemacht, gewalttätige Anschläge zu planen/zu mobilisieren.

Beantwortet: 134 Übersprungen: 24



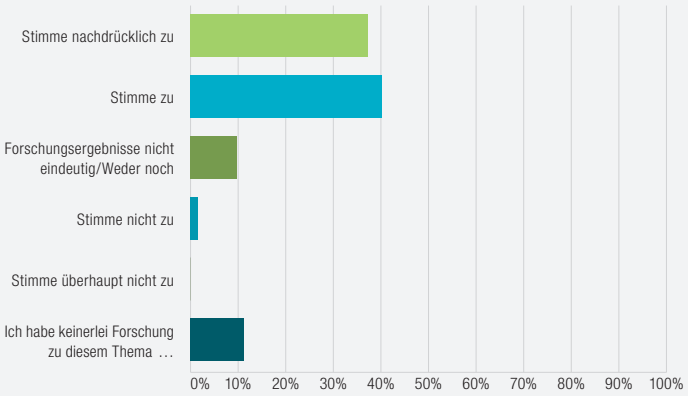
ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Stimme nachdrücklich zu	35,82 %	48
Stimme zu	48,51 %	65
Forschungsergebnisse nicht eindeutig/Weder noch	8,96 %	12
Stimme nicht zu	2,24 %	3
Stimme überhaupt nicht zu	0,75 %	1
Ich habe keinerlei Forschung zu diesem Thema betrieben oder gesehen	3,73 %	5
SUMME		134

Genauso erklärten die meisten Befragten (78 %) ihre Zustimmung bzw. nachdrückliche Zustimmung, dass es für extremistische Akteure mittels internetgestützter Kommunikation einfacher ist, sich Geld zu beschaffen. Das Internet ermöglicht Spenden durch Crowdfunding, den Verkauf von Merchandise, Werbeeinnahmen über Content-Kanäle und die Verwendung von Crypto-Währungen zur anonymen, sicheren Weiterleitung von Geldbeträgen. Ein Teilnehmer führte an, dass viele extremistische Gruppen oder Personen in der Tat eine geschäftliche Präsenz im Internet haben; für sie bestehen „monetäre

Anreize, Inhalte auf ihren Kanälen so sensationell und ansprechend wie möglich zu gestalten, aber gleichzeitig vage genug zu bleiben, um das größtmögliche Zielpublikum zu gewinnen“.

F11: Die Nutzung von internetgestützter Kommunikation und/oder Social-Media-Plattformen durch extremistische Akteure hat es einfacher gemacht, Geldmittel aufzubringen.

Beantwortet: 134 Übersprungen: 24



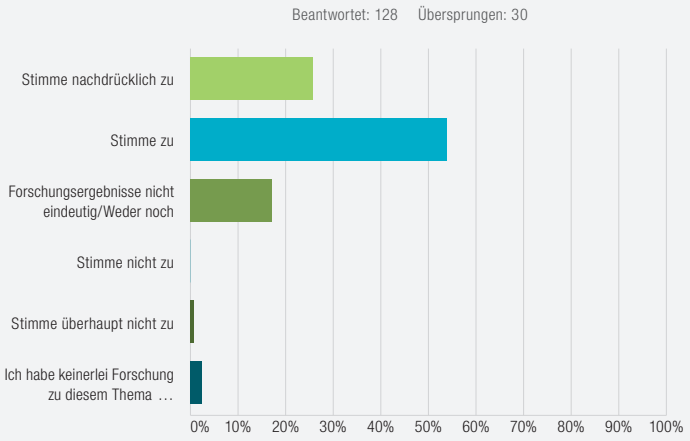
ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Stimme nachdrücklich zu	37,31 %	50
Stimme zu	40,30 %	54
Forschungsergebnisse nicht eindeutig/Weder noch	9,70 %	13
Stimme nicht zu	1,49 %	2
Stimme überhaupt nicht zu	0,00 %	0
Ich habe keinerlei Forschung zu diesem Thema betrieben oder gesehen	11,19 %	15
SUMME		134

Auf die spezifischere Frage, ob der Kontakt und die Interaktion mit extremistischen Inhalten zu Offline-Schäden führt, waren die Antworten der Umfrageteilnehmer weniger eindeutig. Wenn es spezifisch um den Kontakt mit Inhalten geht statt um „Online-Aktivitäten“ im weiteren Sinne (einschließlich Kommunikation, Mittelbeschaffung, Rekrutierung usw.), meinten die Teilnehmer, dass die Interaktion mit extremistischen Inhalten ein beitragender Faktor sein kann, aber kein kausaler, bestimmender oder ausreichender Faktor, genauso wie es die Literaturübersichten ergaben. Einem Teilnehmer zufolge „gibt es zahlreiche prädisponierende Faktoren, bevor eine Interaktion mit extremistischen Inhalten zu Offline-Aktionen führen kann, und der kausale Pfad wird nicht ersichtlich sein“.

Dieser Konsens könnte jedoch später in Frage gestellt werden, da – wie eine Mehrheit der Teilnehmer angab – die „Forschungsergebnisse nicht eindeutig“ sind. Viele Befragte merkten an, dass „wir nicht genug

Beweise dafür haben“, dass es „einfach nicht ausreichend gute Daten gibt“, dass „die Forschung auf sehr begrenzten Daten beruht“ oder dass „nur äußerst minimale empirische Untersuchungen vorliegen, die eindeutig einen Zusammenhang zwischen Kontakt/Interaktion mit extremistischen Inhalten und Offline-Schäden aufzeigen“. Auch diese Antworten spiegeln die seit Langem bestehenden Bedenken in diesem Bereich hinsichtlich des Zugangs zu Daten wider.

F13: Der Kontakt und die Interaktion mit extremistischen Inhalten online trägt zu Offline-Schäden bei.

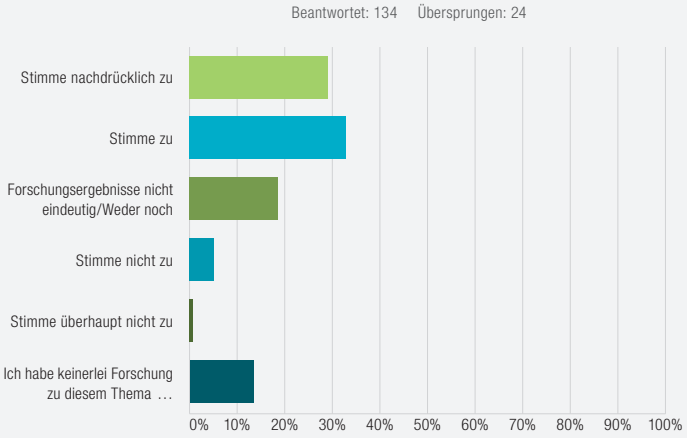


ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Stimme nachdrücklich zu	25,78 %	33
Stimme zu	53,91 %	69
Forschungsergebnisse nicht eindeutig/Weder noch	17,19 %	22
Stimme nicht zu	0,00 %	0
Stimme überhaupt nicht zu	0,78 %	1
Ich habe keinerlei Forschung zu diesem Thema betrieben oder gesehen	2,34 %	3
SUMME		128

Auf die Frage, wie bestimmte Personen auf extremistische Inhalte zugreifen oder diesen begegnen, insbesondere durch algorithmische Empfehlungsfunktionen von Social-Media-Plattformen, stimmten die Befragten zu, dass algorithmische Empfehlungen eine wichtige Rolle bei der Verbreitung von Inhalten spielen (62 % stimmten zu bzw. stimmten nachdrücklich zu). Sie waren jedoch zurückhaltender, was die Frage angeht, ob dies den Pfad einer Person zur Radikalisierung beeinflusst – auch mit dem Ausdruck „going down the rabbit hole“ (nach Alice im Wunderland) beschrieben. Viele wiesen auf die Tatsache hin, dass die Forschung nicht eindeutig ist oder dass es keine ausreichende Forschung darüber gebe, wie algorithmische Empfehlungen den Radikalisierungsprozess beeinflussen. Ein Teilnehmer kommentierte, dieses Thema erfordere „ein differenzierteres Verständnis der vernetzten Sozialität und der sozialen Ökonomien, wie Nutzergemeinschaften tatsächlich mit dem, was sie sich ansehen, umgehen und interagieren“.

Ein Großteil der Forschung zu extremistischen Inhalten und algorithmischen Empfehlungen konzentriert sich auf YouTube;[56] ein Teilnehmer, der nach eigenen Angaben Forschungen zu algorithmischen Empfehlungen durchgeführt hat, fand heraus, dass „Empfehlungsalgorithmen als zentraler Treiber für Rekrutierung, Radikalisierung und Propaganda dienen". Ein anderer kommentierte, dass „starke Beweise darauf hindeuten, dass Empfehlungsalgorithmen zumindest eine Desensibilisierung bewirken können, die wiederum die Hemmschwelle des Betrachters gegenüber Gewalt herabsetzen kann … die Forschung postuliert, dass die immersive Natur der sozialen Medien, einschließlich ihrer Empfehlungsalgorithmen, die Wahrnehmung der Realität durch den Betrachter verändern kann und oft ein Gefühl der Unmittelbarkeit entstehen lässt, was zu dem Gefühl führt, dass sofort gehandelt werden muss".[57]

F12: Empfehlungsalgorithmen von Technologieplattformen können auf dem Radikalisierungspfad einer Person ein wichtiger Faktor sein.



ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Stimme nachdrücklich zu	29,10 %	39
Stimme zu	32,84 %	44
Forschungsergebnisse nicht eindeutig/Weder noch	18,66 %	25
Stimme nicht zu	5,22 %	7
Stimme überhaupt nicht zu	0,75 %	1
Ich habe keinerlei Forschung zu diesem Thema betrieben oder gesehen	13,43 %	18
SUMME		134

Auf die Frage, ob die *Moderation von Inhalten – das Entfernen oder Unterdrücken extremistischer Inhalte* – ein wirksames Mittel zur Bekämpfung von Extremismus und zur Verringerung von Schäden in der realen Welt sei, neigten Teilnehmer, die sich des Themas bewusst waren oder Forschungen zu diesem Thema durchgeführt hatten, zu zwei Positionen: entweder „stimme nachdrücklich zu/stimme zu" (48 %) oder „Forschungsergebnisse sind nicht eindeutig" (37,5 %). Ein kleiner

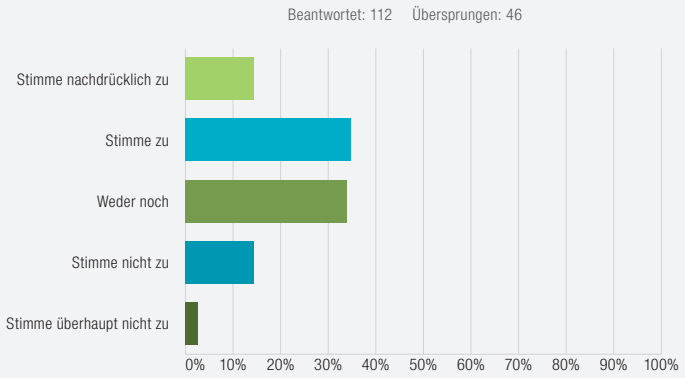
56 Ribeiro et al. (2019) „Auditing Radicalization Pathways on YouTube", *Computers and Society*; Derek O'Callaghan et al. und Tania Bucher vermuten einen starken Zusammenhang zwischen Algorithmen und sozialem Verhalten in YouTube.

57 J. Berger (2015) „The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion", *Perspectives on Terrorism* Band 9 Nr. 4, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/444

Anteil hatte keinerlei Forschung zu diesem Thema betrieben oder gesehen (7,8 %). Viele der Befragten, die die Moderation von Inhalten für ein wirksames Mittel zur Bekämpfung von Extremismus und zur Verringerung von Schäden in der realen Welt hielten, wiesen auch darauf hin, dass dies nur eines von vielen Mitteln zur Intervention sei; ein Befragter beschrieb sie als „ein Puzzleteil in einer umfassenden Strategie, aber allein wahrscheinlich nicht ausreichend, um eine wirksame Strategie zur Bekämpfung von Extremismus in der digitalen Sphäre darzustellen".

Etwa 49 % der Befragten waren jedoch der Meinung, dass die Moderation von Inhalten ihre Fähigkeit beeinträchtigt, auf Daten zuzugreifen und dieses Thema zu recherchieren, und 34 % waren unentschieden, was darauf hindeutet, dass dies nicht Teil ihrer Forschungsarbeit bildete. Einige Teilnehmer kommentierten, dass die Inhaltsmoderation eine Änderung des Forschungsschwerpunkts bewirkt habe und dass „blockierte, entfernte oder unzugänglich gemachte Inhalte nicht untersucht werden können". Viele Teilnehmer sprachen von der Notwendigkeit einer systematischeren Archivierung extremistischer Inhalte und Accounts. Ein Teilnehmer schlug vor, dass „Plattformen zugelassenen Forschern den Zugang zu moderierten Inhalten ermöglichen sollten". Die Terrorist Content Analytics Platform, entwickelt von Tech Against Terrorism und Public Safety Canada, ist eine solche Maßnahme, um Partner-Technologieunternehmen über terroristische Inhalte auf ihren Plattformen zu informieren, damit diese sowohl entfernt als auch zu Forschungszwecken in einer Datenbank verifizierter terroristischer Materialien archiviert werden können.[58]

F36: Die Moderation und/oder das Deplatforming von Inhalten hat meinen Zugang zu relevanten Forschungsdaten erschwert.

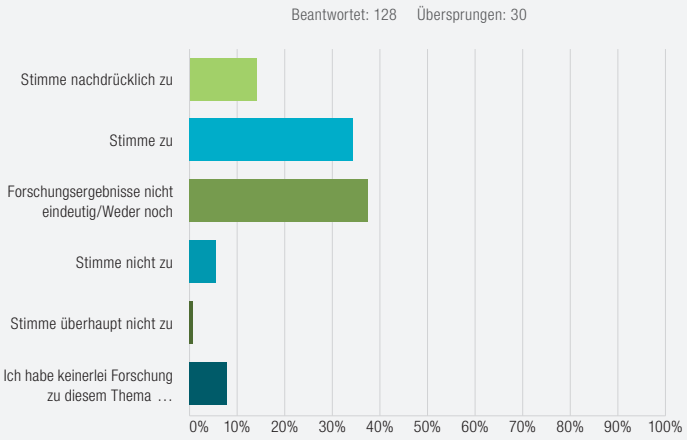


ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Stimme nachdrücklich zu	14,29 %	16
Stimme zu	34,82 %	39
Weder noch	33,93 %	38
Stimme nicht zu	14,29 %	16
Stimme überhaupt nicht zu	2,68 %	3
SUMME		112

58 https://www.terrorismanalytics.org/blog/tcap-newsletter-january-2021-jfwmj

Wie mehrere Teilnehmer anmerkten, kann die Moderation von Inhalten helfen, die Wirkung von Influencern oder die Zugänglichkeit von Informationshandbüchern zur Durchführung von Anschlägen einzuschränken, den Aufbau von Netzwerken zu verhindern und Personen vor zufälligen oder passiven Kontakten mit extremistischen Inhalten zu schützen. Allerdings geht die Moderation von Inhalten nicht auf die Treiber der Radikalisierung zur Gewalt ein und sollte nicht als einzige Lösung betrachtet werden, sondern als Teil einer breiteren Strategie zur Bekämpfung von gewalttätigem Extremismus. Ein Teilnehmer wies zudem darauf hin, dass die Moderation von Inhalten ein Spektrum abdecken sollte: Anstatt Inhalte zu entfernen, könnten schrittweise Formen der Moderation wie Demonetisierung, das Undurchsuchbarmachen bestimmter Inhalte, Shadow-Banning und die Einschränkung der Interaktion von Nutzern mit bestimmten Arten von Inhalten effektiver sein.

F14: Die Moderation von Online-Inhalten – das Entfernen oder Unterdrücken extremistischer Inhalte – reduziert Gewalt oder Schaden in der realen Welt und/oder ist ein wirksames Mittel zur Bekämpfung von Extremismus.

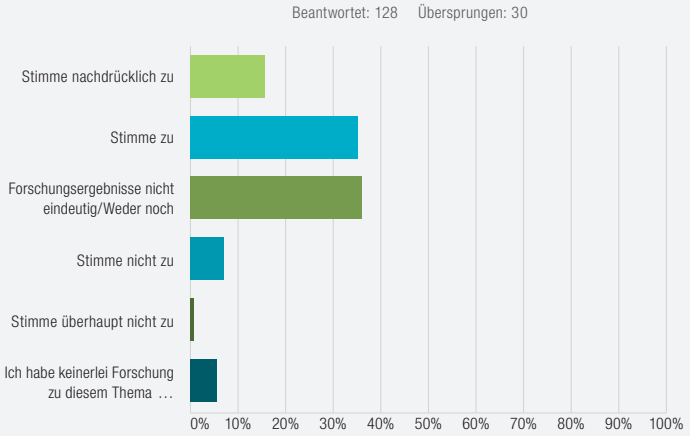


ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Stimme nachdrücklich zu	14,06 %	18
Stimme zu	34,38 %	44
Forschungsergebnisse nicht eindeutig/Weder noch	37,50 %	48
Stimme nicht zu	5,47 %	7
Stimme überhaupt nicht zu	0,78 %	1
Ich habe keinerlei Forschung zu diesem Thema betrieben oder gesehen	7,81 %	10
SUMME		128

In Bezug auf das Deplatforming extremistischer Akteure erklärte etwas mehr als die Hälfte (51 %) ihre Zustimmung oder nachdrückliche Zustimmung mit der Aussage, dass dies reale Schäden verringert und ein wirksames Mittel zur Bekämpfung von Extremismus ist. Etwa 41 % antworteten, die Forschung sei nicht eindeutig oder sie hätten keine Forschung in diesem Bereich gesehen. Nur 8 % stimmten der

Aussage, Deplatforming sei ein wirksames Mittel zur Bekämpfung von Extremismus, nicht oder überhaupt nicht zu.

F15: Das Deplatforming extremistischer Akteure von sozialen Medien und anderen Technologieplattformen reduziert den Schaden in der realen Welt und/oder ist ein wirksames Mittel zur Bekämpfung von Extremismus.



ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Stimme nachdrücklich zu	15,63 %	20
Stimme zu	35,16 %	45
Forschungsergebnisse nicht eindeutig/Weder noch	35,94 %	46
Stimme nicht zu	7,03 %	9
Stimme überhaupt nicht zu	0,78 %	1
Ich habe keinerlei Forschung zu diesem Thema betrieben oder gesehen	5,47 %	7
SUMME		128

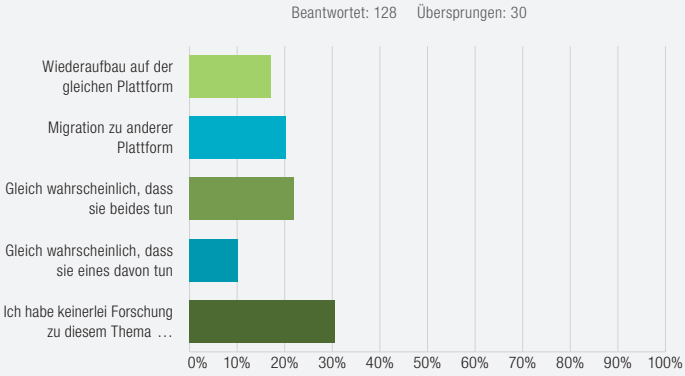
Die Kommentare der Teilnehmer betrafen grob zwei Themenbereiche. Deplatforming ist ein nützliches Instrument, indem es die Reichweite extremistischer Akteure, insbesondere von Influencern, einschränkt, weil diese dann auf Alt-Tech-Plattformen mit einer insgesamt geringeren Nutzerbasis ausweichen. Ein Teilnehmer stellte fest, dass „dies ihre Reichweite ernsthaft einschränkt, was automatisch ihr Publikum verringert. Und selbst wenn sie zurückkehren, wissen wir, dass sie oft nicht wieder die gleiche [Anzahl] von Followern erreichen." Es hilft auch, extremistische Konten zu demonetisieren, weil Geldmittel und Einkommensströme eingeschränkt werden. Wie bei der Moderation von Inhalten ist das Deplatforming nur Teil der breiteren Bemühungen zur Bekämpfung von gewalttätigem Extremismus.

Trotz alledem kann Deplatforming auch Gefühle von ungerechter Behandlung verstärken und extremistische Akteure auf unmoderierte, Nischen- und manchmal verschlüsselte Plattformen abdrängen, wo sie sich weiterhin mit extremistischen Inhalten und Netzwerken beschäftigen können. Die Ergebnisse zu einer damit verwandten Frage – und zwar, ob gefährliche oder extremistische Akteure nach einer zeitweiligen Sperrung (aber nicht einem endgültigen Deplatforming) eher zuerst auf eine andere Plattform abwandern oder den erneuten Aufbau auf der gleichen Plattform versuchen würden – deuten darauf hin, dass uns noch nicht genügend Daten oder Forschungsergebnisse vorliegen. Hier gab die Mehrheit der Befragten an, dass sie zu diesem Thema keine Forschung durchgeführt oder gesehen haben (30 %); die restlichen Antworten verteilten sich auf die sonstigen Antwortmöglichkeiten.

Die Kommentare einiger Befragter ließen zudem erkennen, dass sich hier die Situation verschoben hat. Während ausgeschlossene Akteure in früheren Jahren in der Regel versuchten, eine Präsenz auf derselben Plattform wiederherzustellen, wandern in jüngster Zeit ausgeschlossene Akteure in dem Versuch, ihre Anhängerschaft zu behalten, schon vor einem Verbot auf andere Plattformen ab. Ein Teilnehmer nannte das Beispiel von „Alt-Right-Influencern, die ein paar Verwarnungen erhalten hatten und strategisch ihre Migrationsabsicht verkündeten, bevor sie gesperrt wurden. Diese Influencer hatten ein großes Publikum und versuchten, es auf Plattformen wie BitChute mitzunehmen“, um so ihre Einkommensströme zu sichern und ihren Followern Zeit zu geben, sich an eine andere Plattform zu gewöhnen. Ein anderer Teilnehmer wies darauf hin, dass dies von der Plattform abhängig sei. Während der Islamische Staat letztendlich Twitter aufgab, hat er seine Präsenz auf Telegram hartnäckiger beibehalten, weil er die Funktionen dieser Plattform besonders nützlich findet.

Es besteht die Sorge, dass Deplatforming sogar als Push-Faktor für eine gewalttätige Radikalisierung wirken oder extremistische Ansichten verfestigen könnte. Diese Befürchtung wurde von mehreren Teilnehmern geäußert, wird aber möglicherweise durch die Forschung von Richard Rogers widerlegt, die ergab, dass ausgeschlossene Akteure, die zu anderen Plattformen wechseln, in ihrer Sprache gemäßigter werden.[59] Es ist allerdings festzuhalten, dass eine gemäßigtere Sprache nicht unbedingt auf gemäßigte Ansichten hindeutet; sie könnte bedeuten, dass diese Akteure ein anderes Kommunikationsbedürfnis ansprechen.

F16: Würden gefährliche/extremistische Akteure nach einer zeitweiligen Sperrung eines Accounts wahrscheinlich zuerst versuchen, ihre Social-Media-Präsenz auf der gleichen Plattform wieder aufzubauen, ODER würden sie zu einer anderen Plattform migrieren?



ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Wiederaufbau auf der gleichen Plattform	17,19 %	22
Migration zu anderer Plattform	20,31 %	26
Gleich wahrscheinlich, dass sie beides tun	21,88 %	28
Gleich wahrscheinlich, dass sie eines davon tun	10,16 %	13
Ich habe keinerlei Forschung zu diesem Thema betrieben oder gesehen	30,47 %	39
SUMME		128

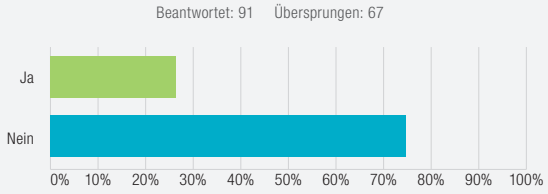
59 R. Rogers (2020) „Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media“, *European Journal of Communication* Band 35 Nr.3: S. 213–29, https://doi.org/10.1177/0267323120922066

Kontakte der Forschung mit der Technologiebranche

Im zweiten Teil der Umfrage lag der Schwerpunkt auf Kontakten der Forschung mit der Technologiebranche selbst. Von Interesse war, ob und wie Forscher mit Technologieunternehmen in Kontakt standen. Auf die Frage nach Art und Ausmaß der Kontakte eines Forschers mit Technologieunternehmen gab es sehr unterschiedliche Antworten, von enger Zusammenarbeit mit Technologieunternehmen, der gemeinsamen Produktion von Forschungsergebnissen und der Informierung über aktuelle Forschungsergebnisse bis hin zu überhaupt keinen Kontakten. Ein Großteil der Zusammenarbeit erfolgte über das GIFCT oder akademische Konferenzen. In mehreren Antworten kam auch Zynismus in Bezug auf die Kontakte der Technologiebranche mit der Forschergemeinschaft zum Ausdruck. So äußerte sich z. B. ein Teilnehmer wie folgt: „Tech-Firmen ‚beteiligen' sich nicht, sie lassen es nur so aussehen, als würden sie Probleme angehen, während sie mit vielen der gleichen Praktiken weitermachen, bis eine Krise Veränderungen erzwingt."

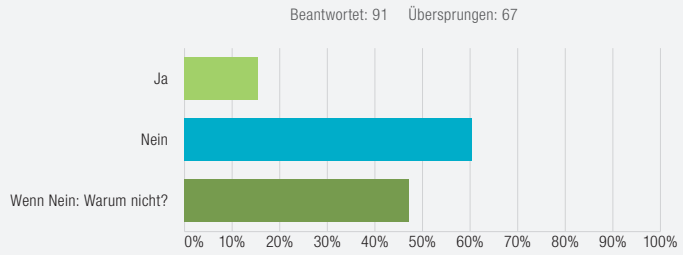
Eine Motivation für Forscher (47 % der Teilnehmer), mehr Kontakte zu Technologieunternehmen zu suchen – aber sicherlich nicht die einzige –, ist der Wunsch nach Datenzugriff. Auf die Frage, ob sie schon einmal an ein Unternehmen herangetreten sind, um Daten für ihre Forschung zu erhalten, antworteten allerdings 75 % mit Nein. Von denjenigen, die gefragt hatten, wurden den meisten die besagten Daten nicht bereitgestellt. Einige Teilnehmer, die angaben, Social-Media-Unternehmen zunächst nicht um Daten gebeten zu haben, wussten entweder, dass die Unternehmensrichtlinien dies in der Regel nicht zulassen, oder sie verfügten nicht über geeignete Kanäle für die Kontaktaufnahme mit Vertretern von Technologieunternehmen. Auf die Frage, ob sie klare Kontaktwege zu den entsprechenden Abteilungen in den Technologieunternehmen hatten, um die Forschung zu besprechen, oder ob sie wussten, wie Technologieunternehmen eine Forschungszusammenarbeit oder den Datenzugriff eventuell genehmigen würden, antwortete die Mehrheit der Teilnehmer (46 % bzw. 60 %) mit Nein. Einem Teilnehmer zufolge war das Anfrageverfahren für eine Forschungsbeteiligung oder die Bereitstellung von Daten „äußerst undurchsichtig". Zahlreiche Teilnehmer kommentierten, ihnen sei nicht klar, welche Möglichkeiten der Zusammenarbeit es gäbe, wen sie kontaktieren müssten und wie diese Personen erreichbar sind, oder sie gaben an, die Zusammenarbeit mit dem Technologiesektor habe einfach keine Priorität für sie.

F40: Sind Sie an ein Technologieunternehmen herangetreten, um Daten für Ihre Forschung zu erhalten?



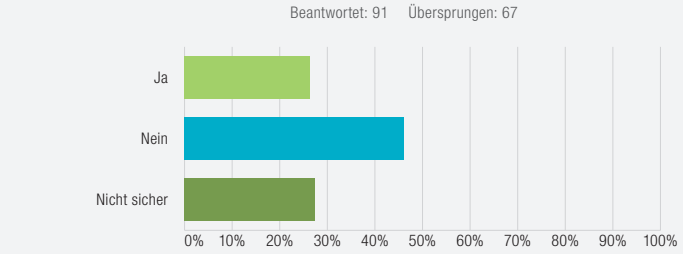
ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Ja	26,37 %	24
Nein	74,73 %	68
Antworten insgesamt: 91		

F41: Haben Sie diese Daten erhalten?



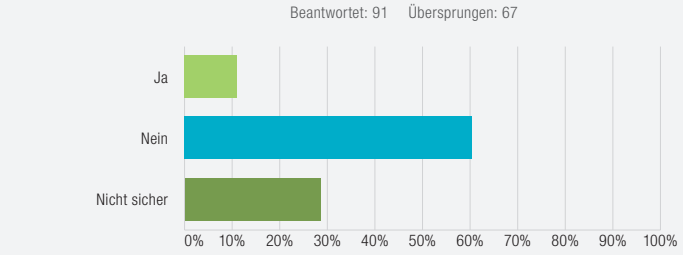
ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Ja	15,38 %	14
Nein	60,44 %	55
Wenn Nein: Warum nicht?	47,25 %	43
Antworten insgesamt: 91		

F42: Haben Sie klare Kontaktwege zu entsprechenden Abteilungen in den Technologieunternehmen, um die Forschung zu besprechen?



ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Ja	26,37 %	24
Nein	46,15 %	42
Nicht sicher	27,47 %	25
SUMME		91

F43: Wissen Sie, nach welchen Prüfungsverfahren Technologieunternehmen Forschungsarbeiten oder Datenzugriff genehmigen?



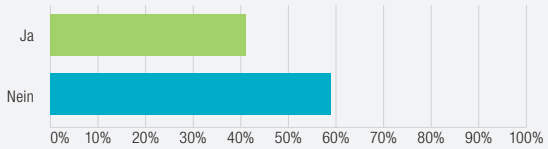
ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Ja	10,99 %	10
Nein	60,44 %	55
Nicht sicher	28,57 %	26
SUMME		91

Auf die Frage nach anderen Einschränkungen in Bezug auf Daten, z. B. ob sich akademische ethische Genehmigungsprozesse, Gesetze und Datenschutzüberlegungen auf den Datenzugriff auswirken, antworteten 59 % der Teilnehmer mit Nein und 41 % mit Ja. Diese abweichenden Antworten lassen sich teils dadurch erklären, dass Universitäten in verschiedenen Ländern unterschiedliche ethische Genehmigungsverfahren haben und nicht alle Forscher in einem universitären Umfeld arbeiten. Das Einholen einer ethischen Genehmigung war nicht die einzige Einschränkung. Teilnehmer verwiesen auf die Tatsache, dass bestimmte Gesetze den Besitz von terrorismusrelevantem Material unter Strafe stellen und dass das Studieren und/oder Erforschen solcher Materialien nicht als Verteidigung gilt. Auch Gesetze im Zusammenhang mit der DSGVO wurden angeführt. Wie ein Teilnehmer – der bejahte, dass ethische Genehmigungsprozesse und Datenschutzüberlegungen den Datenzugriff einschränken – kommentierte, hat dies im Ergebnis viele Forscher gezwungen, auf Sekundärdaten zurückzugreifen.

Mehrere Teilnehmer sprachen die Schwierigkeiten im Umgang mit Institutional Review Boards (IRB) oder Ethikkommissionen an. Ein Teilnehmer kommentierte: „Ich habe Forschungsfragen vermieden, die zu schwierigen Interaktionen mit IRB-Kommissionen führen würden." Viele IRBs erteilen eine ethische Genehmigung nur dann, wenn bei der Datenerhebung die Nutzungsbedingungen der Plattform eingehalten werden; angesichts der Bedingungen der meisten Plattformen bedeutet dies letztendlich, dass der Datenzugriff nicht möglich ist. Ein Teilnehmer merkte an, dass IRBs ein besseres Verständnis von Online-Daten für die Forschung benötigen, da viele IRBs laut den Teilnehmern eine „zu breite Definition von privatem Raum im Internet" haben und „Ethikkommissionen die Natur der Online-Forschung/Extremismusforschung nicht verstehen". Darüber hinaus ist es für Forscher auch wegen der Wartezeit auf eine ethische Genehmigung schwer, entweder auf Daten zuzugreifen oder über ihre Ergebnisse aus diesen Daten zu berichten, da die Daten bis zu dem Zeitpunkt, an dem die ethische Genehmigung erfolgt, möglicherweise bereits wieder entfernt wurden.

F32: Haben akademische ethische Genehmigungsprozesse und/oder Datenschutzüberlegungen, -richtlinien oder -gesetze Ihre Möglichkeiten für Datenzugriff beeinträchtigt?

Beantwortet: 112 Übersprungen: 46

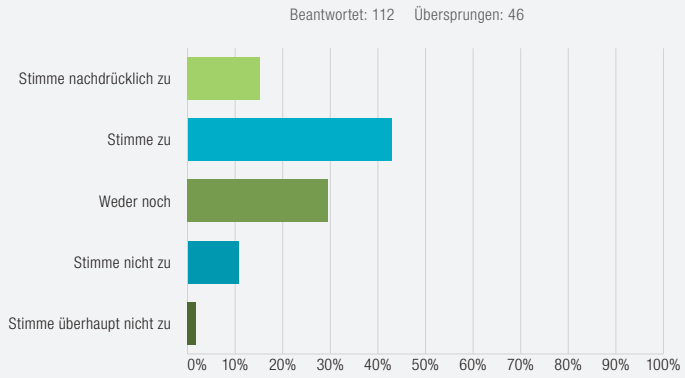


ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Ja	41,07 %	46
Nein	58,93 %	66
SUMME		112

Im Zusammenhang damit wurden die Teilnehmer allgemeiner gefragt, ob „akademische ethische Genehmigungsprozesse und/oder Datenschutzüberlegungen, -richtlinien oder -gesetze die Forschung über extremistische/gefährliche Akteure und Bewegungen auf Online-

Plattformen einschränken“. Die Bedenken der Befragten rund um die ethische Genehmigung wurden auch in der Arbeit von John Morrison, Andrew Silke und Eke Bont erwähnt. Sie stellen fest, dass „es bisher keine objektiven Kriterien gibt, die bei Prüfungen die Beurteilung von Risiko oder Nutzen der Terrorismusforschung unterstützen“. Aus diesem Grund haben sie ein jüngst veröffentlichtes Rahmenwerk für die Forschungsethik bei Terrorismusstudien entwickelt, das diese Lücke schließen kann.[60]

F31: Akademische ethische Genehmigungsprozesse und/oder Datenschutzüberlegungen, -richtlinien oder -gesetze schränken die Forschung über extremistische/gefährliche Akteure und Bewegungen auf Online-Plattformen ein.



ANTWORTMÖGLICHKEITEN	ANTWORTEN	
Stimme nachdrücklich zu	15,18 %	17
Stimme zu	42,86 %	48
Weder noch	29,46 %	33
Stimme nicht zu	10,71 %	12
Stimme überhaupt nicht zu	1,79 %	2
SUMME		112

Während viele Teilnehmer Kommentare zu den Schwierigkeiten von akademischen ethischen Genehmigungsverfahren abgaben, fanden einige diese Einschränkungen auch angemessen und notwendig. Kommentare lauteten: „Sie schränken in der Tat die Forschung ein – aber im Großen und Ganzen sind diese Einschränkungen angemessen“ und „Bei der Arbeit in diesen Bereichen ist es aus ethischen Gründen und zur Sicherheit der Forscher selbst wichtig, strenge Maßnahmen zu ergreifen. Ich weiß von Fällen, in denen unabhängige Forscher aufgrund der Art ihrer Kontakte mit den extremistischen Forschungssubjekten bedroht wurden.“

Datenschutzüberlegungen, ethische Genehmigungsverfahren, Nutzungsbedingungen der Plattformen und ähnliche Faktoren haben es Forschern äußerst schwer gemacht, die Online-Aktivitäten einer Person und/oder ihre Kontakte mit extremistischen Inhalten zu untersuchen. Wenn Teilnehmer dazu in der Lage waren, dann durch den Zugriff auf „Gerichtsunterlagen zu Fällen von terroristischen Aktivitäten“, über sekundäre, offen zugängliche Daten wie Zeitungsberichte,

60 John Morrison, Andrew Silke und Eke Bont (2021) „The Development of the Framework for Research Ethics in Terrorism Studies (FRETS)“, *Terrorism and Political Violence*, 33:2, 271–289, DOI: 10.1080/09546553.2021.1880196

Pressemitteilungen und so weiter. Andere Teilnehmer untersuchten die Online-Aktivitäten von Personen über direkte Fragebögen, die an Einzeltäter in Gefängnissen ausgegeben wurden, über Selbstauskünfte von freiwilligen Teilnehmern oder über Fokusgruppen zu den Fragen, warum und wie sich junge Menschen mit extremistischem Material beschäftigen. Nur eine Handvoll der Befragten war eigenen Angaben zufolge in der Lage, die Online-Aktivitäten von Personen eingehend zu analysieren und mittels Longitudinalstudien die Online-Aktivitäten von Personen zu verfolgen, bevor sie in militante Aktivitäten verwickelt wurden, sowie vergleichende Studien über das Posting-Verhalten von gewalttätigen und nicht gewalttätigen Extremisten anzustellen. Aus den Antworten der Teilnehmer geht hervor, dass es einige kürzlich veröffentlichte und bald zu erwartende Forschungsarbeiten in diesem Bereich gibt, wobei ein Teilnehmer erwähnte, man sei „an der Erfassung von Big Data aus verschiedenen Social-Media-Plattformen im Einklang mit einem genehmigten Ethikantrag beteiligt. Dies gewährt Einblicke in die Online-Aktivitäten von Personen in Bezug auf Inhalte, die mit gewalttätigen extremistischen Ideologien in Verbindung gebracht werden."

4 Schlussfolgerungen

Dieser Umfrage liegt die Hoffnung zugrunde, dass sie Literaturübersichten zur Rolle der Internettechnologie im gewalttätigen Extremismus ergänzen und als Ausgangspunkt für eine Betrachtung der Zusammenarbeit zwischen der Technologiebranche und der Forschungsgemeinschaft dienen wird. Eine wichtige Erkenntnis aus der Entwicklung der Umfrage und Auswertung der Antworten war, dass die Analyse der Rolle von Technologie für den gewalttätigen Extremismus unglaublich komplex, vielschichtig und immer noch umstritten ist. Die empirische Forschung in diesem Bereich ist noch begrenzt, nimmt aber zu.

Neben den Antworten auf die Fragen, die gestellt wurden, haben wir auch Erkenntnisse aus den Fragen gewonnen, die nicht gestellt wurden, und aus den Fragen, die zu unserem Ansatz eingingen. In der Tat wiesen einige Teilnehmer dieser Umfrage auf die Notwendigkeit hin, die Fragen spezifischer und präziser zu gestalten. Unsere Fragen bezogen sich allgemein auf „extremistische Akteure“, und viele Teilnehmer betonten, dass ihre Antworten von der Art des Akteurs und der Bewegung abhingen und dass eine Verallgemeinerung nicht möglich sei. Darüber hinaus waren viele der Fragen zu den Auswirkungen von Technologie, und speziell sozialen Medien, auf gewalttätigen Extremismus vergleichender Natur. Wie ein Teilnehmer jedoch anmerkte, gibt es wenig bis gar keine Forschung, die das Umfeld vor und nach dem Internet vergleicht. Dies ist eine Forschungslücke, die sich schwer schließen lässt und Auswirkungen auf die Gestaltung von zukünftigen Forschungs- und Erhebungsfragen zu diesen Themen haben wird.

Kontakte zwischen Forschern und Technologiebranche erwiesen sich als ein potenziell fruchtbarer, aber auch heikler Bereich – ähnlich, wie es in der Terrorismusforschung Zwiespälte und Überlegungen zur Zusammenarbeit mit Regierungen und Sicherheitsbehörden sowie Bedenken hinsichtlich der Versicherheitlichung der akademischen Forschung gibt. Einige Forscher hatten ähnliche Bedenken hinsichtlich der Kontakte und Zusammenarbeit mit der Technologiebranche und nannten weitere, darunter die Ethik von Beziehungen zu gewinnorientierten Unternehmen, die Undurchsichtigkeit und mangelnde Transparenz der großen Plattformen, ihre reaktive Natur, unterschiedliche Forschungsprioritäten im Vergleich zur Industrie sowie Skepsis darüber, wie ernsthaft und wirksam Social-Media-Plattformen gegen gewalttätigen Extremismus und schädliche Desinformation vorgehen. Zu hoffen ist, dass die in dieser Umfrage identifizierten Forschungslücken, Herausforderungen und Möglichkeiten hinsichtlich der Zusammenarbeit zwischen der Forschung und der Technologiebranche weiter untersucht und angegangen werden können.

Die politische Landschaft

Dieser Abschnitt wurde von Lucy Thomas und Constance Woollen, beide Research Associates am Policy Institute des King's College London, verfasst. Er bietet einen Überblick über den politischen Kontext des Berichtsthemas.

Einleitung

In diesem Bericht untersuchen wir die politische Landschaft und Gesetzgebung von neun Rechtssystemen hinsichtlich der Finanzierung von Forschung zur Terrorismusbekämpfung. Finanzielle Mittel haben unterschiedliche Formen und kommen aus unterschiedlichen Quellen, wie z. B. direkt von einem Regierungsministerium oder indirekt über beispielsweise einen Forschungsrat, wie es in Großbritannien und Frankreich der Fall ist. Die finanzierte Forschung ist zum Teil eindeutig politikorientiert; die Europäische Kommission, Neuseeland und die UNO finanzieren jeweils Forschung in Reaktion auf spezifische politische Erfordernisse bei der Terrorismusbekämpfung. In anderen Ländern wie Großbritannien und Frankreich ist die Finanzierung von Doktoranden weniger direkt in die aktuellen Strategien zur Terrorismusbekämpfung eingebunden, könnte jedoch für diese Studenten als Zugang zu einer Anstellung bei nationalen Sicherheitsbehörden dienen. Ebenfalls üblich ist, Netzwerke für den Austausch aktueller Forschungsergebnisse zur Terrorismusbekämpfung zu gründen; fünf der neun Rechtssysteme sind in den letzten zehn Jahren diesen Weg gegangen (Kanada, die Europäische Kommission, Frankreich, Neuseeland und die UNO).

Zum Abschluss erörtern wir die allgemeineren ethischen Herausforderungen, die mit der Zusammenarbeit zwischen Forschern und politischen Entscheidungsträgern einhergehen, und beschreiben die Schritte, die unternommen werden könnten, um sich einer ethischen Forschungsagenda zur Bekämpfung von gewalttätigem Extremismus („Countering Violent Extremism“ oder CVE) anzunähern. Dazu gehören (1) die Abkehr vom Paradigma der Lösungssuche, um vielmehr die Auswirkungen der Terrorismusbekämpfung auf rassifizierte und marginalisierte Gemeinschaften zu untersuchen, und die Abgabe von politischen Empfehlungen zur Änderung dieser Politik auf der Grundlage der Ergebnisse; (2) das Heranziehen der CVE-Forschung zur Unterstützung von Forderungen nach politischen Maßnahmen, die sich um eine Wiedergutmachung historischer und struktureller Gewalt bemühen; (3) die Untersuchung der Auswirkungen politischer Maßnahmen, die Gemeinschaften stärken, wie z. B. mehr Investitionen in Wohnraum und Maßnahmen zur Förderung der psychischen Gesundheit, und, resultierend daraus, die Verwendung von CVE-Forschung, um auf eine andere Art von Intervention in die Wege zur Gewalt zu drängen.

Staatlich finanzierte Forschung zur Bekämpfung von gewalttätigem Extremismus

Kanada

Die kanadische Regierung verfolgt eine umfassende Strategie zur Bekämpfung von Terrorismus und Radikalismus; diese umfasst die traditionellen Tätigkeiten der Nachrichten- und Sicherheitsbehörden, Beteiligung der Zivilgesellschaft, gemeinsame Initiativen mit der Industrie sowie gemeinschaftsorientierte Polizeiarbeit. Die sogenannte „National Strategy on Countering Radicalisation to Violence" verfolgt drei Richtungen: die Entwicklung von Gegennarrativen in der Zivilgesellschaft (Counter-Messaging), die Unterstützung der CVE-Forschung und die Partnerschaft mit internationalen Initiativen und Technologieunternehmen.[61]

Investitionen in die Forschung sind eines der erklärten Ziele der kanadischen Regierung, und deshalb unterhält sie von allen hier betrachteten Ländern eines der ausgereiftesten und engagiertesten Programme der staatlich finanzierten Forschung. Public Safety Canada, die kanadische Direktion für öffentliche Sicherheit und Notfallvorsorge, enthält das Canada Centre for Community Engagement and Prevention of Violence, das die Maßnahmen der Regierung zur Bekämpfung von gewalttätigem Extremismus leitet. Das 2017 ins Leben gerufene Canada Centre koordiniert eine Reihe von CVE-Aktivitäten, darunter politische Beratung, Zusammenarbeit mit Stakeholdern, Unterstützung von Initiativen und Interventionen sowie Finanzierung und Durchführung von Forschung. Die vom Canada Centre finanzierte Forschung umfasst Stipendien mit der Zielsetzung, „die Radikalisierung zu Gewalt und ihre Bekämpfung besser zu verstehen sowie Forschung den Personen nahezubringen, die sich an vorderster Front dafür einsetzen, die Radikalisierung zu Gewalt zu verhindern".[62]

In Verbindung mit dem Community Resilience Fund – einer Initiative, die mit Organisationen und lokalen Gemeinschaften zusammenarbeitet – hat das Canada Centre eine Reihe von Projekten finanziert, darunter Resilienz gegen Online-Hassreden, Wissen über die Incel-Community, Familien und Radikalisierung zu Gewalt, die extreme Rechte in Québec, Counter-Messaging-Initiativen und mehr. Zu den einbezogenen Partnern und Stakeholdern der geförderten Forschung gehören Hochschuleinrichtungen in Kanada und im Ausland, politische Akteure wie Moonshot CVE, Think Tanks wie das Institute for Strategic Dialogue, lokale und zivilgesellschaftliche Akteure wie das Boston Children's Hospital und andere.[63] Der letzte Aufruf zur Einreichung von Vorschlägen bezog sich auf den Zeitraum 2018-19; es ist also unklar, ob die kanadische Regierung über diesen Kanal auch zukünftig Forschung zur Bekämpfung von gewalttätigem Extremismus finanzieren wird.[64]

Darüber hinaus unterstützt das Canadian Network for Research on Terrorism, Security and Society (TSAS), das 2012 gegründet wurde, Forschung und deren Verbreitung in Bezug auf „die Bedrohung durch Terrorismus, die Reaktionen der Sicherheitsbehörden auf

61 „National Strategy on Countering Radicalization to Violence", Public Safety Canada. Abgerufen: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-en.aspx#s7
62 https://www.publicsafety.gc.ca/cnt/bt/cc/index-en.aspx
63 https://www.publicsafety.gc.ca/cnt/bt/cc/fpd-en.aspx
64 https://www.publicsafety.gc.ca/cnt/bt/cc/fnd-en.aspx

Terrorismus und die Auswirkungen von sowohl Terrorismus als auch Versicherheitlichung auf die kanadische Gesellschaft“.[65] TSAS ist eine unabhängige akademische Organisation, die bei der Forschung häufig mit staatlichen Stellen zusammenarbeitet.[66] Ihre Hauptziele sind die Unterstützung der Kommunikation und Zusammenarbeit zu diesen Themen zwischen Wissenschaftlern verschiedener Disziplinen, die Förderung von Kontakten und Zusammenarbeit zwischen Forschern und politischen Entscheidungsträgern sowie die Förderung einer neuen und breiteren Generation von Wissenschaftlern, die sich für diese Studienbereiche interessieren.[67]

Europäische Kommission

Für die Strategie der Europäischen Kommission zur Terrorismusbekämpfung ist die Generaldirektion Migration und Inneres (DG HOME) zuständig.[68] Die Kommission finanziert seit etwa 15 Jahren Forschung im Bereich der Terrorismusbekämpfung; Forschung zur Radikalisierung wurde erstmals unter dem Siebten Rahmenprogramm 2007-2013 eingeleitet.[69] In jüngerer Zeit hat die Europäische Kommission zwei Mitteilungen (Policy Papers) zur Prävention von Radikalisierung veröffentlicht, die politischen Entscheidungsträgern in den EU-Institutionen vorgelegt werden. Die Finanzierung von Forschung zur Terrorismusbekämpfung und insbesondere zur Radikalisierung steht im Mittelpunkt dieser beiden Mitteilungen, die zunehmend politik- und wirkungsorientierte Ziele enthalten.

2016 erschien in Reaktion auf die Terroranschläge in Europa die Mitteilung COM(2016)379,[70] in der es um die Frage geht, wie die EU „Mitgliedstaaten in ihren Bemühungen unterstützen kann, Radikalisierung zu verhindern, die zu extremistisch motivierter Gewalt und Terrorismus führt“.[71] Die Kommission führt in dieser Mitteilung an, dass jüngste Terroranschläge auf „neue Trends“ beim Radikalisierungsprozess verweisen, die genauer untersucht werden müssen. Um die „Kluft zwischen Sicherheitstheoretikern und -praktikern in diesem Bereich besser zu überbrücken“, stellte die Kommission Forschungsschwerpunkte vor.[72] Diese Forschung zu den Ursachen für Radikalisierung und Gewaltbereitschaft, die konkrete Instrumente hervorbringen und politische Interventionen ermöglichen soll,[73] wurde im Rahmen von Horizont 2020 mobilisiert, dem „größten EU-Förderprogramm für Forschung und Innovation je“, für das zwischen 2014 und 2020 nahezu 80 Mrd. Euro zur Verfügung standen.[74] Der Fokus der Kommission, ein breites Spektrum an Akteuren in ihre Strategie zur Terrorismusbekämpfung einzubinden, zeigt sich auch in der zusätzlichen Einrichtung des (mittlerweile stillgelegten) Radicalisation Awareness Network Centre of Excellence (RANCE), einem Netzwerk von Akteuren aus den Mitgliedsstaaten, das unter anderem dem Wissensaustausch über Radikalisierung dienen sollte.[75]

65 https://www.tsas.ca/about/
66 https://www.publicsafety.gc.ca/cnt/bt/cc/res-en.aspx Siehe Abschnitt unter „The Canadian Network for Research on Terrorism, Security and Society (TSAS)“
67 Ebd.
68 https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/radicalisation_en
69 https://ec.europa.eu/transport/themes/research/fp7_en
70 https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2016)379&lang=de, S. 2
71 Ebd., S. 3
72 Ebd., S. 5
73 Ebd., S. 6
74 https://ec.europa.eu/programmes/horizon2020//en/what-horizon-2020
75 https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2016)379&lang=de, S. 6

Im Jahr 2020 folgte eine weitere Mitteilung der Kommission, COM(2020)795, die eine umfassendere Agenda für die Terrorismusbekämpfung umreißt.[76] Aufbauend auf der vom Siebten Rahmenprogramm sowie von Horizont 2020 finanzierten Forschung enthält diese Agenda Pläne für eine Fortsetzung der Forschung zur Terrorismusbekämpfung. Ein zentrales Element dieser Mitteilung bestand darin, „EU-Maßnahmen im Bereich der Sicherheitsforschung [zu] finanzieren, um die Fähigkeit zur frühzeitigen Erkennung von Bedrohungen zu verbessern, und im Rahmen der EU-Städteagenda neue Technologien [zu] entwickeln".[77] Diese Forschung soll dazu beitragen, Fähigkeiten zur frühzeitigen Erkennung potenzieller terroristischer Bedrohungen mithilfe von künstlicher Intelligenz und Big-Data-Projekten zu verbessern; die Bekämpfung der Radikalisierung war erneut Bestandteil der Strategie.[78] Finanzielle Mittel für diese Forschung werden von Horizont Europa bereitgestellt, dem bis 2027 angelegten Nachfolgeprogramm von Horizont 2020.[79] Auch wenn Forscher, Wissenschaftler und Forschungseinrichtungen in der Mitteilung nicht ausdrücklich erwähnt werden, hat die EU eindeutig die Erwartung, dass diese Forschung wirkungsorientiert, tief in den Politikzyklus „Sicherheit" integriert und auf den Bedarf der Strafverfolgung ausgerichtet ist.[80] Neben der von Horizont Europa finanzierten Forschung unterstützt die Kommission in dieser Mitteilung auch den Austausch von Forschung und Wissen zur Terrorismusbekämpfung unter politischen Entscheidungsträgern, Akteuren aus der Praxis und Forschern. Sie schlägt die Einrichtung eines EU-Wissenszentrums zur Prävention von Radikalisierung vor, ähnlich wie RANCE.[81] Dies scheint nicht mit zusätzlichen Finanzmitteln verbunden zu sein, weist Forscher aber auf Fördermöglichkeiten im Rahmen mehrerer EU-Programme hin.[82]

Frankreich

In Frankreich ist das regierungsübergreifende Comité Interministériel de Prévention de la Délinquance et de la Radicalisation (CIPDR) für die Strategie zur Terrorismusbekämpfung verantwortlich.[83] Dieser interministerielle Ausschuss unter dem Vorsitz des Premierministers bringt u. a. Vertreter der Innen- und Justizministerien zusammen.[84, 85] Das CIPDR ist eine Quelle direkter Finanzierungsmittel für die Forschung. Die französische Regierung finanziert Forschung zur Terrorismusbekämpfung auch indirekt über ihre Agence nationale de la recherche (ANR). Während CIPDR-finanzierte Forschung am engsten mit der französischen Strategie zur Terrorismusbekämpfung verknüpft ist, scheint die ANR-Forschung weniger politikorientiert zu sein.

2016 veröffentlichte das CIPDR den zweiten Plan d'action contre la radicalisation et le terrorisme (PART) als eine aktualisierte Strategie zur Radikalisierungsprävention basierend auf sozialen sowie auch sicherheitsbezogenen Überlegungen.[86] Sowohl bei PART als auch

76 https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)795&lang=de
77 Ebd., S. 7
78 Ebd., S. 4
79 https://ec.europa.eu/info/horizon-europe_en
80 https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)795&lang=de, S. 5
81 Ebd., S. 10
82 Ebd.
83 https://www.cipdr.gouv.fr/wp-content/uploads/2019/04/PPPsept2018.pdf
84 https://www.cipdr.gouv.fr/pnpr/
85 https://www.cipdr.gouv.fr/wp-content/uploads/2019/04/PPPsept2018.pdf, S. 5
86 Ebd.

bei seinem Vorgängerdokument von 2014, dem Plan de lutte contre le terrorisme (PLAT), stand die Prävention im Mittelpunkt, bestehend aus Erkennung, Schulung und praktischer Intervention in Gesellschaft und Justizwesen sowie die Förderung der Forschung in diesem Bereich.[87] PART enthielt sieben übergreifende Ziele in Bezug auf Radikalisierung mit insgesamt 80 zugehörigen Maßnahmen.[88] Eines der Ziele (mit zehn zugehörigen Maßnahmen) war die Entwicklung von angewandter Forschung durch Einrichtung eines Forschungsnetzwerks für die Koordination und den Austausch von Erkenntnissen, die Förderung von Doktoranden[89] sowie die Finanzierung privater Initiativen, die einen kritischen Diskurs über die Ideologien der Radikalisierung oder einen offenen Diskurs zum Wissen über den Islam verbreiten.[90]

In jüngerer Zeit veröffentlichte das CIPDR 2018 den nationalen Plan zur Verhinderung von Radikalisierung, der PLAT und PART ersetzen soll.[91] Diese neueste Auflage umfasst insgesamt 60 Maßnahmen, eine davon mit spezifischer Relevanz für die Forschung. Sie betrifft die Bereitstellung von Finanzmitteln für Doktoranden[92] sowie Unterstützung für französische Anträge im Rahmen des Förderprogramms Horizont 2020 der Europäischen Kommission (siehe Abschnitt „Europäische Kommission“ für nähere Einzelheiten über die Förderung von Forschung zur Terrorismusbekämpfung). Die Forschungsergebnisse dieser CIPDR-Förderung werden nicht explizit genannt, sind jedoch mit der nationalen Strategie verknüpft und scheinen daher politik- und wirkungsorientiert zu sein.

Im Gegensatz dazu ist die ANR dem französischen Ministerium für Hochschulbildung, Forschung und Innovation unterstellt und finanziert im Allgemeinen projektbasierte Forschung, die eine Zusammenarbeit zwischen dem öffentlichen und privaten Sektor beinhaltet.[93] Die Ziele der ANR sind infolgedessen eher forschungsbezogen als fachspezifisch und konzentrieren sich z. B. auf die Förderung multidisziplinärer Forschung, anstatt Forschung in einem bestimmten Bereich wie der Terrorismusbekämpfung anzuregen. Zum Stand April 2021 wurden von der ANR zwischen 2011 und 2020 zehn Forschungsstudien zum Thema „violent extremism“ (gewalttätiger Extremismus)[94] sowie zwischen 2018 und 2020 drei Projekte zum Thema „counter-terrorism“ (Terrorismusbekämpfung) finanziert.[95] Diese Forschung wurde über die ANR indirekt von der französischen Regierung gefördert, scheint aber nicht explizit politikorientiert oder mit der staatlichen Strategie für Terrorismusbekämpfung verbunden zu sein.

Ghana

Die Republik Ghana hat zwar wenig Erfahrung mit Terroranschlägen im eigenen Land und daher auch keine nationale oder regionale Strategie zur Terrorismusbekämpfung,[96] aber dennoch ist ein klarer staatlicher Ansatz für Polizeiarbeit und Nachrichtendienste vorhanden.

87 Ebd.
88 https://www.cipdr.gouv.fr/announcement/second-plan-daction-contre-la-radicalisation-et-le-terrorisme-part/
89 https://www.gouvernement.fr/sites/default/files/document/document/2016/05/09.05.2016_dossier_de_presse_-_plan_daction_contre_la_radicalisation_et_le_terrorisme.pdf, S. 8
90 Ebd., S. 9
91 https://www.cipdr.gouv.fr/wp-content/uploads/2019/04/PPPsept2018.pdf
92 Ebd., S. 15
93 https://anr.fr/en/anrs-role-in-research/missions/
94 https://anr.fr/en/funded-projects-and-impact/funded-projects/?q=violent+extremism&id=1781&L=1
95 https://anr.fr/en/search/?q=counter-terrorism&id=1817&L=1
96 https://issafrica.org/iss-today/slow-progress-for-west-africas-latest-counter-terrorism-plan

Das Anti-Terror-Gesetz von 2008, das in Übereinstimmung mit den internationalen rechtlichen Verpflichtungen nach 9/11 verabschiedet wurde, ist „ein Gesetz, das erlassen wurde, um die Nutzung des ghanaischen Territoriums als Drehscheibe für Terroristen zu bekämpfen, zu unterdrücken und zu verhindern“.[97] Das Gesetz stellt das Verbrechen des Terrorismus unter Strafe und kriminalisiert in Übereinstimmung mit Resolution 1373 des UN-Sicherheitsrates die Terrorismusfinanzierung und terroristisches Material, den Besitz von terroristischem Eigentum sowie Anstiftung und Förderung einer terroristischen Agenda.[98]

Polizei und Justizsystem erhalten durch dieses Gesetz weitreichende Befugnisse zur Überwachung und Durchsuchung von Terrorismusverdächtigen. Laut Abschnitt 24 kann die Polizei physische Durchsuchungen einer Person durchführen und „„Räumlichkeiten aufbrechen und gewaltsam betreten“, wenn ein „begründeter Anlass“ für den Verdacht besteht, dass sich dort Eigentum befindet, das zur Durchführung einer terroristischen Handlung verwendet wird.[99] Vor allem aber kann die Polizei diese physischen Durchsuchungen durchführen, ohne einen Durchsuchungsbefehl zu erwirken oder einen Verdächtigen in Haft zu nehmen.[100] Das Gesetz gibt dem Staat zudem weitreichende Überwachungsbefugnisse, um Kommunikationen abzuhören, wenn ein „begründeter Verdacht“ auf Ausführung einer terroristischen Handlung besteht. Diese Gesetzgebung hat den Grundstein für zwei Entwicklungen in der ghanaischen Strategie zur Terrorismusbekämpfung gelegt: Erstens erfolgte 2012 eine Änderung des Gesetzes, wonach (in Übereinstimmung mit internationalen Best Practices) als terroristisch eingestufte Gruppen finanziellen Sanktionen und dem Einfrieren von Vermögenswerten unterworfen[101] und Einwanderungskontrollen mit der Strategie zur Terrorismusbekämpfung verflochten wurden.[102]

Zweitens – bedeutsam im Hinblick auf gewalttätigen Online-Extremismus – ebnete die verschärfte Anti-Terror-Gesetzgebung der Regierung den Weg für die Einbringung des Gesetzes zur Überwachung von Postverkehr und Telekommunikation Anfang 2016. Dieses Gesetz, auch als „Spy Bill“ bezeichnet, sollte die rechtliche Grundlage für „das Abfangen von Post und elektronischer oder Cyberspace-Kommunikation zum Schutz der nationalen Sicherheit im Kampf gegen das organisierte Verbrechen einschließlich des Terrorismus“ schaffen. Auffällig am Spy Bill war die mangelnde Rechenschaftspflicht oder Aufsicht, insbesondere weil Abschnitt 4(3) es der Regierung erlaubte, eine gerichtliche Anordnung oder Genehmigung für die Überwachung um 48 Stunden zu verschieben. Dies sowie das Fehlen eines Aufsichtsmechanismus leistete potenziellem Missbrauch und geheimer Überwachung Vorschub.[103] Auf Druck der Zivilgesellschaft wurde der Gesetzesentwurf zurückgenommen.[104]

97 https://heinonline.org/HOL/Page?handle=hein.journals/afjincol28&div=7&g_sent=1&casa_token=9lH5SXVmi30AAAAA:GB8E5gSXIg-UxFeFoW0D5MHaJkhBN0__swDl07Ot-ocLfkb60cbqF4qSyMCn3XTzQKg4-177Fw&collection=journals, S. 56
98 Ebd., S. 57
99 https://acts.ghanajustice.com/actsofparliament/anti-terrorism-act-2008-act-762/, Abschnitt 24
100 https://heinonline.org/HOL/Page?handle=hein.journals/afjincol28&div=7&g_sent=1&casa_token=9lH5SXVmi30AAAAA:GB8E5gSXIg-UxFeFoW0D5MHaJkhBN0__swDl07Ot-ocLfkb60cbqF4qSyMCn3XTzQKg4-177Fw&collection=journals, S. 58–9
101 https://www.mint.gov.gh/wp-content/uploads/2017/06/Anti-Terrorism-Reg-L.-I.-2181.pdf, Abschnitte 5 und 6
102 Ebd., Abschnitt 4
103 https://heinonline.org/HOL/Page?handle=hein.journals/afjincol28&div=7&g_sent=1&casa_token=9lH5SXVmi30AAAAA:GB8E5gSXIg-UxFeFoW0D5MHaJkhBN0__swDl07Ot-ocLfkb60cbqF4qSyMCn3XTzQKg4-177Fw&collection=journals, S. 60–61
104 https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Spy-Bill-withdrawn-from-Parliament-451805

Das repressive und missbrauchsanfällige Anti-Terror-Umfeld in Ghana ist Ausdruck eines breiteren Trends in postkolonialen Staaten, die paramilitärische Ansätze der Polizeiarbeit von ihren Kolonialherren – im Falle Ghanas von den britischen Kolonialbehörden – geerbt haben.[105] Trotz einer ressourcenreichen, wachsenden Produktions- und Exportwirtschaft bedeutet die fortgesetzte neokoloniale wirtschaftliche Abhängigkeit von westlichen Institutionen (wie dem Internationalen Währungsfonds), dass Korruption weit verbreitet ist und die Armutsraten hoch bleiben.[106]

In diesem Kontext überrascht es vielleicht nicht, dass die aktuelle CVE-Strategie in Ghana keine „weicheren" Elemente vorsieht, wie z. B. staatlich finanzierte Forschung. Forschungsarbeiten und Initiativen im Zusammenhang mit der Bekämpfung von gewalttätigem Extremismus werden eher von nicht-staatlichen Akteuren finanziert, darunter regionale Gruppen, zivilgesellschaftliche Gruppen und externe Regierungen. Zum Beispiel finanzierten das Kofi Annan International Peacekeeping Training Centre, das African Centre for the Study and Research on Terrorism und die spanischen Regierung 2016 einen hochkarätigen Workshop, der sich mit den Ursachen von gewalttätigem Extremismus befasste.[107] Aktivitäten für den Wissensaustausch im Bereich der Terrorismusbekämpfung in den Jahren 2019 und 2020 wurden vom UN Counter-Terrorism Executive Directorate[108] und dem Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung gemeinsam mit der deutschen Regierung finanziert.[109]

Japan

Ähnlich wie in Ghana beruht auch in Japan der interne Ansatz zur Bekämpfung von gewalttätigem Extremismus auf Kriminalisierung und Polizeiarbeit. Eine Erbe aus der Zeit des Kalten Krieges ist, dass die einheimischen nachrichtendienstlichen Aktivitäten, ausgerichtet auf die mutmaßliche kommunistische Bedrohung, weitgehend von den Strafverfolgungsbehörden koordiniert werden. Die Polizeibehörden der Präfekturen (unter Aufsicht der Nationalen Polizeibehörde) und der „Nachrichtendienst für öffentliche Sicherheit" (Japans nationaler Nachrichtendienst) stehen an der Spitze der nachrichtendienstlichen Erkennung und der Terrorismusabwehr auf japanischem Boden.[110]

In Reaktion auf inländischen Online-Terrorismus werden also traditionelle Polizeiarbeit und Sicherheitsarchitekturen mobilisiert.[111] Innovative technologische Entwicklungen sind für Japan ein Markenzeichen seiner wissenschaftlichen Forschung und seines Exporthandels, was sich auch in der Sicherheitsstrategie des Landes niederschlägt. Die japanische Regierung hat stark in Lösungen auf der Basis künstlicher Intelligenz (KI) investiert, darunter

105 https://journals.sagepub.com/doi/pdf/10.1177/1461355716638114
106 Siehe Walter Rodney (2018) *How Europe Underdeveloped Africa* (London: Verso Books); https://www.imf.org/en/News/Articles/2015/09/14/01/49/pr15159; https://www.tandfonline.com/doi/abs/10.1080/01900692.2011.598272; https://www.unicef.org/ghana/media/531/file/The%20Ghana%20Poverty%20and%20Inequality%20Report.pdf
107 https://caert.org.dz/Reports/Final%20Report%20for%20CVE%20Workshop_7-8Nov2016.pdf
108 https://www.un.org/sc/ctc/news/2019/10/04/cted-conducts-follow-visit-republic-ghana/
109 https://www.unodc.org/westandcentralafrica/en/2020-09-28-ghana-counter-terrorism.html
110 Ken Kotani (2013) „A Reconstruction of Japanese Intelligence: Issues and Prospects", in Philip H. J. Davies und Kristian C. Gustafson (Hg.), *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere* (Washington D.C.: Georgetown University Press): S. 181–99.
111 https://www.mofa.go.jp/files/000156881.pdf, Abschnitt zu „Domestic Counter-Terrorism Measures"

groß angelegte Systeme zur Gesichtserkennung, biometrischen Authentifizierung und automatischen Verhaltenserkennung.[112] Diese Lösungen lassen eine Lenkungsform erkennen, bei der Früherkennung und Prävention im Mittelpunkt stehen und durch traditionelle Polizei- und Sicherheitstaktiken realisiert werden.

In Reaktion auf eine Geiselnahme, bei der zwei japanische Staatsbürger vom Islamischen Staat in Syrien getötet wurden, gründete Japan 2015 eine Anti-Terror-Einheit, die vom Außen- und Verteidigungsministerium, der Nationalen Polizeibehörde sowie dem Nachrichten- und Untersuchungsbüro des Kabinetts besetzt ist.[113] Die Einheit deutet auf eine Stärkung der nationalen Geheimdienst- und Sicherheitskapazitäten hin. In der Tat setzte der japanische Premierminister Shinzō Abe im Parlament Mitte 2017 ein „brutales“[114] Anti-Terror-Gesetz durch.[115] Es kriminalisiert die Planung von über 270 „schweren Delikten“, unter anderem Sit-in-Proteste und Urheberrechtsverletzungen bei Musik; die Durchsetzbarkeit erstreckt sich auch auf die sozialen Medien.[116] Bürgerrechtsaktivisten haben ihre Besorgnis über die breite Anwendbarkeit und weitreichenden Überwachungs- und Kontrollbefugnisse für japanische Strafverfolgungsbehörden zum Ausdruck gebracht.[117]

Die internationalen Bemühungen Japans zur Terrorismusabwehr stehen im starken Kontrast zur innenpolitischen Fokussierung auf Kriminalisierung; sie sind durch einen regionalen Fokus, den Aufbau von Kapazitäten und Kooperation gekennzeichnet. Die Association of Southeast Asian Nations (ASEAN) – das Forum für viele der ausländischen Terrorabwehrbemühungen Japans[118] – hat eine Reihe von Erklärungen herausgegeben. Darin verpflichten sich die Mitglieder zur „Verhütung, Unterbindung und Bekämpfung des internationalen Terrorismus durch Informationsaustausch, gemeinsame Nutzung nachrichtendienstlicher Erkenntnisse und Aufbau von Kapazitäten“; dies schuf ein Vorbild für die regionale Zusammenarbeit bei der Bekämpfung von gewalttätigem Extremismus und Terrorismus.[119] Japan war zweimal Gastgeber des jährlich stattfindenden ASEAN-Japan Counter Terrorism Dialogue und hat bilaterale Gespräche mit einer Reihe von globalen Akteuren geführt.[120] So diskutierten z. B. Japan und das Vereinigte Königreich Ende 2019 „die gegenwärtige Lage des internationalen Terrorismus, innerstaatliche Maßnahmen zur Terrorismusabwehr und auch die

112 Japanische Regierung, „All is Ready for a Safe and Secure Tokyo Games“, https://www.japan.go.jp/tomodachi/2019/autumn-winter2019/tokyo2020.html; „NEC Becomes a Gold Partner for the Tokyo 2020 Olympic and Paralympic Games“, NEC Corporation, 2015, https://www.nec.com/en/press/201502/global_20150219_01.html; Kyodo News (29. Januar 2018) „Kanagawa police eye AI-assisted predictive policing before Olympics“, https://english.kyodonews.net/news/2018/01/5890d824baaf-kanagawa-police-eye-ai-assisted-predictive-policing-before-olympics.html

113 https://www.voanews.com/east-asia/japan-launches-anti-terrorism-unit-ahead-summit-olympics

114 B. Allen-Ebrahimian (16. Juni 2017) „Japan Just Passed a ‘Brutal,’ ‘Defective’ Anti-Terror Law“, *Foreign Affairs*, https://foreignpolicy.com/2017/06/16/japan-just-passed-a-brutal-defective-anti-terror-law/

115 Das Gesetz kam durch „den ungewöhnlichen Schritt des Überspringens einer Abstimmung im Oberhausausschuss für Justizangelegenheiten“ zustande. Japan Federation of Bar Associations (15. Juni 2017) „Statement on the Enactment of the Bill to Revise the Act on Punishment of Organized Crimes and Control of Crime Proceeds, including the Criminalization of Conspiracy“, https://www.nichibenren.or.jp/en/document/statements/170615.html

116 J. McCurry (15. Juni 2017) „Japan passes ‘brutal’ counter-terror law despite fears over civil liberties“, *The Guardian*, https://www.theguardian.com/world/2017/jun/15/japan-passes-brutal-new-terror-law-which-opponents-fear-will-quash-freedoms; J. Adelstein (15. Juni 2017) „Japan’s Terrible Anti-Terror Law Just Made ‘The Minority Report’ Reality“, *The Daily Beast*, http://www.thedailybeast.com/japans-terrible-anti-terror-law-just-made-the-minority-report-reality

117 Japan Federation of Bar Associations, „Statement on the Enactment of the Bill“

118 „Japan: Extremism & Counter Extremism“, Counter-Extremism Project, https://www.counterextremism.com/countries/japan

119 „ASEAN-Japan Joint Declaration for Cooperation to Combat International Terrorism“, ASEAN, https://asean.org/?static_post=asean-japan-joint-declaration-for-cooperation-to-combat-international-terrorism-2

120 „Japan: Extremism & Counter Extremism“

gegenwärtige Zusammenarbeit beim Aufbau von Kapazitäten zur Terrorismusbekämpfung, insbesondere in Dritt- (sic) Ländern [‚third *(sic)* countries']".[121]

In diesem Zusammenhang ist unklar, ob die japanische Regierung neben zivilgesellschaftlichen oder akademischen Partnern die CVE-Forschung hinsichtlich gewalttätiger extremistischer Online-Aktivitäten im Inland finanziert. Entsprechend der national-internationalen Aufteilung hat Japan jedoch Forschung und Workshops in Zusammenarbeit mit den Vereinten Nationen finanziert. So hat Japan beispielsweise gemeinsam mit dem Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung einen internationalen Leitfaden zur Verhinderung der Rekrutierung und Ausbeutung von Kindern durch gewalttätige extremistische Gruppen veröffentlicht[122] und mit UN Women zusammengearbeitet, um die geschlechtsspezifische Dynamik des gewalttätigen Extremismus zu untersuchen.[123] Diese Aktivitäten stärken das internationale Image Japans als kooperatives, fortschrittliches Land in Bezug auf CVE-Governance. Um jedoch die Freiheit und Privatsphäre seiner Bürger effektiv zu schützen, sollte Japan diese Anliegen berücksichtigen, wenn es Forschung in Auftrag gibt und Politik gestaltet.

Neuseeland

Die übergreifenden Maßnahmen gegen Terrorismus in Neuseeland werden zwischen mehreren Regierungsstellen, Kommunen und Organisationen des privaten Sektors koordiniert; sie stehen unter der Leitung des Cabinet External Relations and Security Committee sowie des Security and Intelligence Board. Die Gesamtstrategie ist in dem im Februar 2020 veröffentlichten Strategieplan zur Terrorismusbekämpfung beschrieben.[124] Der Christchurch-Anschlag vom März 2019 löste in Neuseeland mehrere Reaktionen zur Terrorismusbekämpfung aus, darunter der internationale Christchurch-Appell und der spezifisch auf Neuseeland ausgerichtete Bericht der Königlichen Kommission, in dem wiederholt auch die Forschung angesprochen wird.

Der Christchurch-Gipfel, eine globale Reaktion auf die Moscheenangriffe vom März 2019 unter dem gemeinsamen Vorsitz der neuseeländischen Premierministerin Jacinda Ardern und des französischen Präsidenten Emmanuel Macron,[125] brachte Vertreter von Regierungen und Internetunternehmen zu einem Treffen in Paris zusammen, bei dem Maßnahmen gegen den Missbrauch des Internets für terroristische Zwecke im Mittelpunkt standen.[126] Das Ergebnis dieses Gipfels war eine Vier-Phasen-Strategie zur Bekämpfung extremistischer Inhalte. Eine dieser Strategien betraf das „Verstehen, Kartieren und Analysieren der Forschung (durchgeführt oder mit dem Ziel, Lücken zu identifizieren) zu

121 Japanisches Außenministerium (4. Dezember 2019) „The 4th Japan-the UK Counter-Terrorism Dialogue", https://www.mofa.go.jp/fp/is_sc/page1e_000297.html.
122 https://www.unodc.org/unodc/en/frontpage/2019/March/unodc--japan-gather-countries-from-asia--the-middle-east-and-north-africa-to-protect-children-affected-by-terrorism-and-violent-extremism.html
123 https://thediplomat.com/2018/03/japan-helps-explore-the-gender-dynamics-of-violent-extremism/
124 Neuseeländische Regierung, Officials' Committee for Domestic and External Security Coordination, Counter-Terrorism Coordination Committee (Februar 2020), „Countering terrorism and violent extremism national strategy overview". https://dpmc.govt.nz/sites/default/files/2020-02/2019-20%20CT%20Strategy-all-final.pdf
125 Ebd.
126 https://www.gov.uk/government/news/pm-joins-christchurch-call-to-action-on-online-terror

gewalttätigem Extremismus im Internet“,[127] da es an Forschung und Fortschritten mangelte, was das Kartieren und Verstehen von Online-Extremismus betrifft.[128] Mit der Unterzeichnung des Christchurch-Appells verpflichteten sich die Regierungen zu einer Beschleunigung der Forschung und der Entwicklung von Werkzeugen mit dem Ziel, das Hochladen von terroristischen und extremistischen Inhalten zu verhindern und zu erkennen sowie solche Inhalte zu entfernen, und dabei auf die Expertise von Akademikern, Forschern und der Zivilgesellschaft zurückzugreifen.[129] In dieser Hinsicht könnte der Christchurch-Appell als Ausdehnung von Neuseelands Ansatz zur Terrorismusbekämpfung gesehen werden, der auf Gemeinschaften und die Zivilgesellschaft ausgerichtet ist, verglichen mit anderen Unterzeichnerländern wie Großbritannien und Frankreich, die zu traditionelleren Modellen tendieren.

Was die spezifisch auf Neuseeland ausgerichtete Finanzierung zur Terrorismusbekämpfung angeht, so enthielt der am 8. Dezember 2020 der Öffentlichkeit bereitgestellte Bericht der königlichen Untersuchungskommission,[130] die sich mit dem Terroranschlag auf die Moscheen in Christchurch am 15. März 2019 beschäftigte,[131] 44 Empfehlungen an die Regierung. Empfehlung 16 des Berichts betrifft die Finanzierung unabhängiger Forschung zu den Ursachen von gewalttätigem Extremismus und Terrorismus sowie diesbezüglichen Präventionsmaßnahmen.[132] Die beschriebene Forschung scheint politikorientiert zu sein, da die zugehörigen Bestimmungen zur Finanzierung des (vorgeschlagenen) nationalen Nachrichten- und Sicherheitsdienstes eine mehrjährige Mittelausstattung für die Forschungsförderung vorsehen; Forschungsprioritäten und Zuschussempfänger sollen von einem Gremium aus offiziellen Vertretern des neuen nationalen Nachrichten- und Sicherheitsdienstes ausgewählt werden.[133] Eine weitere Empfehlung war die Einrichtung eines Netzwerks aus relevanten staatlichen und örtlichen Regierungsbehörden, Gemeinden, der Zivilgesellschaft, dem privaten Sektor und der Forschung für den Informationsaustausch zur Bekämpfung von gewalttätigem Extremismus und Terrorismus.[134] Die Regierung hat alle Empfehlungen dieses Berichts formell akzeptiert. Die Umsetzung scheint jedoch langsam gewesen zu sein; in einer Rede vom 8. Dezember 2020 entschuldigte sich Jacinda Ardern im Namen der Regierung für die Versäumnisse bei der Umsetzung.[135] In ihrer Rede ging die Premierministerin nicht direkt auf die Auswirkungen der finanzierten Forschung ein, sagte aber, die Regierung werde einige Empfehlungen sofort umsetzen, während andere in Zusammenarbeit mit dem Parlament und den Neuseeländern geprüft würden.[136] Die Forschung, die finanziert werden soll, ist eindeutig politikorientiert und wird, sofern sie den Empfehlungen der Königlichen Kommission folgt, enge Verbindungen zu den nationalen Sicherheitsbehörden beinhalten. Die von der Königlichen Kommission

127 https://www.orfonline.org/research/one-year-since-the-christchurch-call-to-action-a-review/
128 https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/christchurch-call-to-eliminate-terrorist-and-violent-extremist-content-online
129 Ebd.
130 https://christchurchattack.royalcommission.nz/the-report/download-report/download-the-report/
131 https://christchurchattack.royalcommission.nz/assets/Report-Volumes-and-Parts/Ko-to-tatou-kainga-tenei-Volume-1-v2.pdf
132 https://christchurchattack.royalcommission.nz/assets/Report-Volumes-and-Parts/Ko-to-tatou-kainga-tenei-Volume-1-v2.pdf, S. 26
133 Ebd.
134 Ebd., S. 27
135 https://www.tvnz.co.nz/one-news/new-zealand/full-statement-jacinda-ardern-apologises-agrees-all-recommendations-in-christchurch-attack-report
136 Ebd.

vorgeschlagenen Maßnahmen umfassen daher offenbar sowohl konventionelle sicherheits- und nachrichtendienstliche Strukturen als auch Initiativen, die Zivilgesellschaft, Wissenschaft und politische Entscheidungsträger in ihrer Strategie zur Terrorismusbekämpfung zusammenbringen.

Vereinigtes Königreich

Im Vereinigten Königreich ist die Terrorismusbekämpfung auf gesetzgeberischer und politischer Ebene eine Aufgabe des Home Office (Innenministerium). Das National Security Council (NSC) unter Vorsitz des Premierministers ist das wichtigste Forum zum gemeinsamen Austausch über die Ziele der Regierung für die nationale Sicherheit.[137] Das NSC wiederum legt die Prioritäten für das Government Communications Headquarters (GCHQ) fest.[138] Die britische Regierung finanziert Forschung zur Terrorismusbekämpfung sowohl direkt als auch indirekt über diese verschiedenen Einrichtungen. Die Tatsache, dass Mittel (vorwiegend) indirekt bereitgestellt und Forschungsergebnisse über unabhängige Stellen veröffentlicht werden, ist angesichts der eher traditionellen CVE-Strategie des Vereinigten Königreichs nicht überraschend. Offenbar gibt es vier zentrale Wege, über die das Vereinigte Königreich Forschung zur Terrorismusbekämpfung finanziert, hier in der Reihenfolge von der höchsten bis zur geringsten direkten Finanzierung beschrieben.

Der Conflict, Stability and Security Fund (CSSF), der 2015 als Katalysator für eine stärker integrierte Reaktion der britischen Regierung auf Fragilität und Konflikte ins Leben gerufen wurde, ist ein regierungsübergreifender Fonds von jährlich 1,26 Mrd. GBP, an dem das Innenministerium und das Kabinettsbüro beteiligt sind.[139] Als Teil der CSSF wurde der Counter Terrorism Programmes Fund (CTPF) eingerichtet; das Enablers Programme ist eine seiner Umsetzungen. Das Enablers Programme sollte Forschung unterstützen, die das Verständnis der Regierung zum Terrorismus und gewalttätigen Extremismus verbessert.[140] Obwohl die Art der durchgeführten Forschung online nicht näher verdeutlicht wird, ist anzunehmen, dass sie mit der Terrorismusbekämpfung zusammenhängt, da dieser Teil des CTPF die Umsetzung von Aspekten der auslandsbezogenen Elemente von CONTEST unterstützen soll.[141]

CONTEST, die britische Strategie zur Terrorismusbekämpfung, die 2018 vom Innenministerium aktualisiert wurde,[142] enthält mehrere Verweise auf Forschung, insbesondere in Bezug auf einen ihrer „bewährten“ strategischen Aktionsbereiche, „Prevent“.[143] Prevent stützt sich auf „kontinuierliche Forschung und Evaluierung“.[144] Auch diese stützende Funktion wird nicht im Detail beschrieben, beinhaltet aber z. B. die Zusammenarbeit mit Forschungsorganisationen und Kontakte mit Wissenschaftlern, um besser zu verstehen, wie

137 https://www.gov.uk/government/groups/national-security-council
138 https://www.gchq.gov.uk/section/mission/overview
139 https://www.gov.uk/government/organisations/conflict-stability-and-security-fund/about
140 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875951/CTPF_Enablers_Programme_Summary.odt
141 Ebd.
142 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf
143 Ebd., S. 9
144 Ebd., S. 32

Terroristen das Internet zur Radikalisierung gefährdeter Personen verwenden.[145] Darüber hinaus beschreibt die Strategie die Rolle von „Wissenschaft, Technologie, Analyse und Forschung“ als Fundament der Terrorismusbekämpfung[146] und die zukünftigen Pläne des Innenministeriums, „die Zusammenarbeit mit der Wissenschaft und dem privaten Sektor zu verbessern, um sicherzustellen, dass sie Zugang zu den fortschrittlichsten Technologien, Ratschlägen und Lösungen für die Terrorismusbekämpfung haben und diese nutzen können“.[147]

Eine weniger explizite Finanzierung seitens der britischen Regierung erfährt das Centre for Research and Evidence on Security Threats (CREST), die britische „Drehscheibe für Verhaltens- und Sozialwissenschaften für die nationale Sicherheit“.[148] CREST erhielt sowohl direkt als auch indirekt staatliche Mittel, und zwar von den britischen Nachrichten- und Sicherheitsdiensten und dem Innenministerium[149] sowie vom Economic and Social Research Council (ESRC), Teil des öffentlichen Organs, das für die Unterstützung von Forschung und Wissensaustausch an englischen Hochschulen zuständig ist.[150] Seit Oktober 2015 hat CREST fast 12,5 Mio. GBP erhalten,[151] um sechs Partneruniversitäten in ganz Großbritannien zusammenzubringen und „ein interdisziplinäres Portfolio an Aktivitäten von Weltklasse zu liefern, das den Wert der Sozialwissenschaften für die Bekämpfung von Bedrohungen der nationalen Sicherheit maximiert“.[152] Im Rahmen der jüngsten Förderung werden auch sieben Doktoranden von CREST ausgebildet.[153] Die Projekte sind vielfältiger Art und ihre Themen reichen von „Understanding & Countering Online Behaviour“ bis hin zu einer Bewertung der Wirksamkeit von Maßnahmen zur Bekämpfung von gewalttätigem Extremismus.[154] Diese Förderberichte zeugen von den engen Verbindungen zwischen CREST und akademischen Partnern statt der britischen Regierung. Die Tatsache, dass CREST Mittel direkt vom Innenministerium erhält (sowie über das ESRC indirekt von der Regierung), bedeutet allerdings, dass die Verbindungen zur britischen Regierung und ihrer Politik der Terrorismusbekämpfung nicht zu leugnen sind.

Das Innenministerium arbeitet eng mit dem National Cyber Security Centre (NCSC) zusammen, der unabhängigen britischen Behörde für Cybersicherheit.[155] Das NCSC ist nicht speziell mit der Bekämpfung von gewalttätigem Extremismus betraut, aber es gehört zum GCHQ, dessen Prioritäten in Übereinstimmung mit dem National Security Council und der Nationalen Sicherheitsstrategie festgelegt werden,[156] in der die Terrorismusbekämpfung eine zentrale Rolle spielt. Über 19 Universitäten, die als Academic Centres of Excellence in Cyber Security Research anerkannt sind, fördert das NCSC seit 2012

145 Ebd., S. 33
146 Ebd., S. 8
147 Ebd., S. 80
148 https://www.lancaster.ac.uk/people-profiles/paul-j-taylor
149 https://crestresearch.ac.uk/about/
150 https://www.ukri.org/about-us/who-we-are/
151 https://gtr.ukri.org/projects?ref=ES%2FN009614%2F1#/tabOverview; https://gtr.ukri.org/projects?ref=ES%2FV002775%2F1
152 https://www.ukri.org/news/uk-hub-for-research-into-security-threats-awarded-5-3m-funding/; https://gtr.ukri.org/projects?ref=ES%2FN009614%2F1#/tabOverview
153 https://gtr.ukri.org/projects?ref=ES%2FV002775%2F1
154 https://crestresearch.ac.uk/projects/
155 https://www.ncsc.gov.uk/section/about-ncsc/what-we-do
156 https://www.gchq.gov.uk/section/mission/overview

Doktoranden, Cybersicherheitsforschung zu betreiben.[157, 158] Diese Universitäten werden gemeinsam vom NCSC und dem Engineering and Physical Sciences Research Council, einer indirekten staatlichen Fördereinrichtung, anerkannt. Genau wie Frankreich fördert also auch Großbritannien Doktoranden für die Forschung zur Terrorismusbekämpfung, wenn auch weniger direkt. Diese Verbindung mag etwas vage erscheinen, ist aber ein gut etablierter Finanzierungsstrom für zukünftige Akademiker, der auch als direkter Weg zu einer Anstellung im NCSC oder GCHQ dienen kann[159] und in die britische Politik zur Terrorismusbekämpfung einfließt.

Counter-Terrorism Committee Executive Directorate der Vereinten Nationen

Das Counter-Terrorism Committee Executive Directorate der Vereinten Nationen (UN CTED) wurde vom UN-Sicherheitsrat mit der Resolution 1535 (2004) eingerichtet, um als Expertengremium das Counter-Terrorism Committee (CTC) des Sicherheitsrats zu unterstützen.[160] Sein anfängliches Ziel bestand darin, die Implementierung von Anti-Terror-Resolutionen des Sicherheitsrats durch die UN-Mitgliedstaaten zu bewerten und diese Bemühungen im Wege eines Dialogs zu unterstützen.

Im Jahr 2015 gründete das CTED sein Global Counter-Terrorism Research Network (GRN). Das GRN bringt mehr als 100 Forschungseinrichtungen in aller Welt zusammen und verfolgt das Ziel, das CTED über neu entstehende Terrorismustrends zu informieren sowie Best Practices bei der Umsetzung der relevanten Resolutionen des Sicherheitsrats durch die Mitgliedstaaten zu identifizieren und zu verbreiten.[161] Der Wert des GRN wurde 2017 in einer UN-Resolution (2395) anerkannt, wie auch die Beziehungen des CTED zu relevanten Experten in der Wissenschaft und bei Think Tanks.[162] Es ist nicht klar, ob die durch das GRN verbreitete Forschung vom CTED oder einer anderen UN-Einrichtung finanziert wird. Das GRN veröffentlicht regelmäßig Berichte online, darunter längere Analysen, zum Beispiel über die Auswirkungen der Coronavirus-Pandemie auf Terrorismus, Terrorabwehr und CVE,[163] sowie kürzere „Trends Alerts“. Diese Alerts werden herausgegeben, um „das Bewusstsein sowohl innerhalb des CTC als auch bei den Organisationen der Vereinten Nationen und den politischen Entscheidungsträgern zu erhöhen“,[164] und enthalten Forschungsergebnisse aus dem gesamten GRN.[165] Wie bei der Forschung, die von der Europäischen Kommission finanziert wird, stehen auch beim GRN Politik und Wirkung im Mittelpunkt.

157 https://www.ncsc.gov.uk/information/academic-centres-excellence-phd-student-scheme
158 https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research
159 https://www.ncsc.gov.uk/information/academic-centres-excellence-phd-student-scheme
160 N. Chowdhury Fink (2012) „Meeting the challenge: A guide to United Nations counterterrorism activities“, International Peace Institute: S. 45, https://www.ipinst.org/wp-content/uploads/publications/ebook_guide_to_un_counterterrorism.pdf
161 https://spark.adobe.com/page/hMGmYTiTbbEag/
162 https://www.un.org/sc/ctc/news/2021/01/05/virtual-roundtable-global-research-network-20-years-research-emerging-threats-trends-developments-terrorism-counter-terrorism/
163 https://www.un.org/sc/ctc/wp-content/uploads/2020/06/CTED-Paper%E2%80%93-The-impact-of-the-COVID-19-pandemic-on-counter-terrorism-and-countering-violent-extremism.pdf
164 https://www.un.org/sc/ctc/wp-content/uploads/2020/04/CTED_Trends_Alert_Extreme_Right-Wing_Terrorism.pdf, S. 2
165 Ebd.

Das Entwicklungsprogramm der Vereinten Nationen, das zwar nicht direkt mit dem CTED zusammenhängt, hat zudem 2016 einen Aktionsplan zu Radikalisierung und gewalttätigem Extremismus veröffentlicht; dieser umfasst zwei Agendas, eine davon zu „Forschung, Politik und Advocacy".[166] Diese Forschungsagenda „wird vom [UN] Oslo Governance Centre gesteuert und in Zusammenarbeit mit den regionalen Drehscheiben sowie in Partnerschaft mit Hochschul- und Forschungseinrichtungen umgesetzt."[167] Die Agenda geht auch auf die Rolle des RESOLVE-Forschungsnetzwerks ein, das unabhängig vom GRN ist. Dieses Netzwerk zielt darauf ab, „eine Evidenzbasis für Programme und Politik zur Bekämpfung von gewalttätigem Extremismus"[168] zu schaffen, und organisiert eine jährliche Konferenz zum Austausch internationaler CVE-Forschung. Obwohl die damit verbundenen Finanzierungsströme nicht erwähnt werden, sollen auch hier die Forschungsergebnisse – wie der Titel der Agenda andeutet – politikorientiert sein.

USA

Unter der Trump-Regierung wurden die Aktivitäten und das Budget der USA zur Bekämpfung von gewalttätigem Extremismus drastisch reduziert. Die Countering Violent Extremism Task Force, die 2011 von der Obama-Regierung ins Leben gerufen wurde, um Bemühungen und Aktivitäten behördenübergreifend zu bündeln, wurde 2017 umstrukturiert[169] und Ende 2018 ganz geschlossen.[170] Die Regierung strich finanzielle Mittel für Initiativen, die mit Communitys und der Zivilgesellschaft arbeiteten, wie zum Beispiel Life After Hate, eine Initiative, die mit ihrer Arbeit Individuen dabei hilft, sich aus White-Supremacy- und Neonazi-Gruppen zu lösen.[171]

Trotz dieser Budgetkürzungen verdreifachte sich das Volumen der CVE-Finanzmittel für die Strafverfolgungsbehörden – insbesondere das Ministerium für Innere Sicherheit (Department of Homeland Security, DHS) – von 764.000 auf 2.340.000 USD.[172] Das DHS-Direktorat für Wissenschaft und Technologie gab eine Reihe von Forschungs-Roadmaps in Auftrag, um eine Bestandsaufnahme der aktuellen CVE-Forschung und -Stakeholder vorzunehmen und Empfehlungen für zukünftige Forschungslinien aufzustellen.[173] Die CVE-Forschung auf Bundesebene konzentriert sich auf „aufkommende soziale, psychologische, wirtschaftliche, rechtliche, politische und kulturelle Themen" sowie auf „Risikofaktoren, die zu gewalttätigem Extremismus führen, um den Partnern zu helfen, effektivere und effizientere Programme zu dessen Bekämpfung zu erstellen".[174]

166 https://www.undp.org/content/dam/norway/undp-ogc/documents/Discussion%20Paper%20-%20Preventing%20Violent%20Extremism%20by%20Promoting%20Inclusive%20%20Development.pdf, S. 33
167 Ebd.
168 Ebd., S. 34
169 J. Ainsley et al. (3. Februar 2017) „Exclusive: Trump to focus counter-extremism program solely on Islam – sources", *Reuters*, https://www.reuters.com/article/idUSKBN15G5VO?feedType=RSS&feedName=topNews&utm_source=twitter&utm_medium=Social
170 P. Beinart (29. Oktober 2018) „Trump Shut Programs to Counter Violent Extremism" *The Atlantic*, https://www.theatlantic.com/ideas/archive/2018/10/trump-shut-countering-violent-extremism-program/574237/
171 Life After Hate, „About Us", https://www.lifeafterhate.org/about-us-page
172 https://www.brennancenter.org/our-work/analysis-opinion/countering-violent-extremism-programs-trump-era
173 Siehe: https://www.dhs.gov/science-and-technology/developing-local-capabilities und speziell https://www.dhs.gov/sites/default/files/publications/861_OPSR_TP_CVE-Developing-Research-Roadmap_Oct2017.pdf
174 https://www.dhs.gov/sites/default/files/publications/861_OPSR_TP_CVE-Developing-Research-Roadmap_Oct2017.pdf, S. 11

Einige Kommentatoren meinen zwar, die Trump-Administration hätte in Bezug auf ihre CVE-Politik „schlimmer sein können“, und führen die Aufstockung der DHS-Forschungsmittel als positive Entwicklung an,[175] doch es ist klar, dass diese Forschungsprogramme auf spezifische Gemeinschaften ausgerichtet waren und Polizeiarbeit sowie Überwachungsaktivitäten innerhalb dieser Gemeinschaften verstärkt haben. Das Brennan Center for Justice, ein Institut für öffentliche Politik und Recht, analysierte die CVE-Finanzbeihilfen der Trump-Administration und stellte fest, dass „mindestens 85 % der CVE-Finanzbeihilfen und mehr als die Hälfte der CVE-Programme jetzt explizit auf Minderheitengruppen abzielen, darunter Muslime, LGBTQ-Amerikaner, Black Lives Matter-Aktivisten, Einwanderer und Flüchtlinge“.[176] Mehr als die Hälfte der Programme zielt auf Schulen und Schüler ab, teils schon ab einem Alter von fünf Jahren.[177] Viele CVE-Finanzbeihilfen wurden an Strafverfolgungsbehörden vergeben, die in nicht-weißen Gebieten tätig sind, wie „Minneapolis und seine somalischen Enklaven; das Alameda County Sheriff's Office, das Oakland, Kalifornien, umfasst“.[178]

Die Verwendung von Bundesmitteln für diese Art von Aktivitäten ist bedrohlich: Unter dem Deckmantel von Community Outreach und Forschung können die Strafverfolgungsbehörden „Informationen sammeln, mögliche Ziele für verdeckte Operationen identifizieren oder mögliche Informanten für die Rekrutierung finden“.[179] Dies erinnert an das umstrittene Prevent-Programm im Vereinigten Königreich, das zur Überwachung britischer muslimischer Gemeinschaften angeregt hat.[180] Solche Aktivitäten tragen zum Racial Profiling bestimmter Gemeinschaften bei, schaffen ein Klima der Angst und schränken das Recht auf freie Meinungsäußerung und Privatsphäre ein.

Es bleibt abzuwarten, wie die Strategie der neuen Biden-Administration in Bezug auf CVE aussehen wird. Angesichts der Tatsache, dass Biden unter Obama Vizepräsident war, könnte seine Strategie zur Terrorismusbekämpfung von dem militaristischen Ansatz im Ausland geprägt sein, den Obama favorisierte.[181] Sollte sich Biden von der rassistischen Politik der Trump-Regierung distanzieren wollen, wäre die Einstellung des CVE-Beihilfeprogramms ein Schritt in die richtige Richtung. Gelder, die bisher für schädliche CVE-Forschung verwendet wurden, könnten stattdessen in chronisch vernachlässigte und unterfinanzierte Gemeinschaften geleitet werden, um grundlegende Bedürfnisse zu decken.

175 https://www.brookings.edu/blog/order-from-chaos/2020/04/07/on-cve-the-trump-administration-could-have-been-worse/
176 https://www.brennancenter.org/our-work/analysis-opinion/countering-violent-extremism-programs-trump-era
177 https://www.brennancenter.org/our-work/research-reports/countering-violent-extremism-trump-era
178 https://theintercept.com/2018/06/15/cve-grants-muslim-surveillance-brennan-center/
179 Ebd.
180 Siehe vorigen GNET-Bericht „Untersuchung extremistischer Inhalte auf Social-Media-Plattformen: Datenschutz und Forschungsethik – Herausforderungen und Chancen“ https://gnet-research.org/wp-content/uploads/2021/02/GNET-Researching-Extremist-Content-Social-Media-Ethics-GERMAN.pdf, S. 32–37
181 https://www.cfr.org/election2020/candidate-tracker, Abschnitt zur Terrorismusbekämpfung

Politikrelevanz, Forschung und der Staat Ethische Überlegungen

Hinsichtlich der Entwicklung und Umsetzung der CVE-Politik lassen sich die Stakeholder in drei Hauptgruppen unterteilen: Wissenschaft, politische Entscheidungsträger/Praktiker und Technologiebranche. Die oben beschriebenen Umfrageergebnisse von Lydia Khalil konzentrieren sich auf die Kontakte von Forschern mit der Technologiebranche und zeigen ein unterschiedliches Niveau des Engagements mit Unternehmen. Dieser Unterabschnitt beleuchtet nun die Kontakte der Forscher mit politischen Entscheidungsträgern und Praktikern im CVE-Bereich und erörtert einige der breiteren ethischen Herausforderungen, die mit der Zusammenarbeit zwischen Wissenschaft und Politik verbunden sind.

Vor den Londoner Bombenanschlägen im Juli 2005 war die Strategie zur Terrorismusbekämpfung auf Sicherheitsbedrohungen durch den internationalen Terrorismus ausgerichtet, insbesondere Gruppen wie al-Qaida. Angesichts der Tatsache, dass drei der vier Londoner Bombenattentäter in Großbritannien geboren wurden, begann das Vereinigte Königreich, seine Aufmerksamkeit auf „homegrown extremism“ und die Bedrohung durch einheimischen Terrorismus zu richten. Die 2003 vom britischen Innenministerium eingeführte Prevent-Strategie zielte auf Personen ab, die als „anfällig“ für Radikalisierung galten, und griff in den sogenannten Radikalisierungspfad ein, bevor es zu kriminellen Handlungen kommen konnte.[182]

Die Strategie zeichnete sich besonders durch ihren gesamtgesellschaftlichen Ansatz aus: Zivilgesellschaftliche Einrichtungen wie Schulen, registrierte Kinderbetreuungseinrichtungen, Universitäten, Hochschulen, Gefängnisse, Bewährungsdienste, Gesundheitswesen, Sozialdienste und Einwanderungsbehörden wurden alle in die Strategie eingebunden. Diese Institutionen wurden dazu verpflichtet, mögliche Fälle von Radikalisierung vorherzusehen, zu beobachten und zu intervenieren, indem sie spezifische Anzeichen von Radikalisierung identifizieren und melden. Dieser Ansatz verlagerte die Anti-Terror-Strategie und -Kontrolle von den traditionellen sicherheits- und nachrichtendienstlichen Mechanismen auf öffentliche Räume und mehrere staatliche Behörden. Angeführt von Großbritannien wurde der Ansatz der Prevent-Strategie seitdem in vielen westlichen Staaten umgesetzt.[183]

Dieser gesamtgesellschaftliche und behördenübergreifende Ansatz zur Terrorismusbekämpfung wird oft als „Countering Violent Extremism“ oder CVE bezeichnet. CVE umfasst verschiedenste Aktivitäten „an der Basis“ zur Intervention in den Radikalisierungspfad, denen ideologische, psychologische oder kulturelle Vorstellungen von Radikalisierung zugrunde liegen.[184] Projekte in Gemeinschaften, wie Bildungs- oder Mentoring-Programme – oft auf junge Menschen oder spezifische

182 Prevent Strategy, HM Government, Juni 2011, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf
183 https://www.tandfonline.com/doi/pdf/10.1080/09546553.2020.1727450?needAccess=true, Fußnote 18
184 https://www.tandfonline.com/doi/pdf/10.1080/09546553.2020.1727450?needAccess=true, S. 3

Gemeinschaften ausgerichtet – sowie Programme zum Aufbau von Vertrauen und Kontakten mit der Polizei, sind typisch für eine CVE-Strategie.[185]

Das Office for Targeted Violence and Terrorism Prevention (TVTP; früher Countering Violent Extremism Task Force) des US-Heimatschutzministeriums verkörpert die Grundsätze der CVE-Strategie sehr anschaulich. Schwerpunkt der TVTP-Arbeit sind „proaktive Maßnahmen" zur Verhinderung von Terrorismus und gezielten Gewalttaten, die auf bestimmte Gemeinschaften ausgerichtet sind.[186] Diese Maßnahmen sollen „Gemeinschaften und Einzelpersonen stärken" und Resilienz gegen „gewalttätige Botschaften und Rekrutierung" aufbauen. Sie beinhalten öffentliche Bewusstseinsbildung, Aktivitäten in Gemeinschaften und Unterstützungsdienste.[187]

Entscheidend ist, dass Rahmenwerke für CVE-Strategie und Präventionsarbeit auf einem Paradigma der Bedrohungsbewertung und -abwehr beruhen. Laut dem TVTP bedeutet dies, „Pädagogen, Psychologen, Glaubensführer, medizinisches Personal, Strafverfolgungsbehörden und andere" innerhalb eines gesamtgesellschaftlichen Rahmens in die Bemühungen zur Terrorismusbekämpfung einzubeziehen.[188] Menschenrechtsgruppen haben diesen Ansatz stark kritisiert. Sie sind darüber besorgt, wie diese Form der Überwachung und polizeilichen Kontrolle von Gemeinschaften schädliche Annahmen darüber verfestigt, welche Gemeinschaften und rassischen Gruppen für Radikalisierung und Gewalt „anfällig" sind, sowie ein Klima der Angst und Feindseligkeit innerhalb von Gemeinschaften schafft.[189] Bei der Priorisierung der Bedrohungsbewertung und -abwehr stützt sich die CVE-Strategie auf „harte" Strafverfolgungs- und Sicherheitsapparate zur Kriminalisierung bestimmter Verhaltensweisen.

Im obigen Überblick zur Politik verschiedener Rechtssysteme haben wir untersucht, wie Bundesmittel in den USA dazu beitragen, diesen gesamtgesellschaftlichen Ansatz unter Einbeziehung von Strafverfolgungsbehörden, politischen Entscheidungsträgern und Wissenschaft zu operationalisieren. Wir stellten fest, dass „mindestens 85 % der CVE-Finanzbeihilfen und mehr als die Hälfte der CVE-Programme jetzt explizit auf Minderheitengruppen abzielen, darunter Muslime, LGBTQ-Amerikaner, Black Lives Matter-Aktivisten, Einwanderer und Flüchtlinge".[190] Mehr als die Hälfte der Programme zielt auf Schulen und Schüler ab, teils schon ab einem Alter von fünf Jahren.[191] Viele CVE-Finanzbeihilfen wurden an Strafverfolgungsbehörden vergeben, die in nicht-weißen Gebieten tätig sind, wie „Minneapolis und seine somalischen Enklaven; das Alameda County Sheriff's Office, das Oakland, Kalifornien, umfasst".[192]

185 Ebd., S. 5 und https://www.tandfonline.com/doi/full/10.1080/18335330.2015.1028772?casa_token=4VBOXUOQT3UAAAAA%3ABeegdWY62rzDh376WJQuY3Ssw6Z99i4QiU6NZkRWzkypPQ4OQ5Q9PkBzsIOXsdnrAVFp07xAQE4
186 Siehe: https://www.dhs.gov/tvtp
187 Ebd.
188 https://www.dhs.gov/tvtp, Abschnitt „Local Prevention Framework"
189 Siehe zum Beispiel Liberty: https://www.libertyhumanrights.org.uk/fundamental/prevent/
190 https://www.brennancenter.org/our-work/analysis-opinion/countering-violent-extremism-programs-trump-era
191 https://www.brennancenter.org/our-work/research-reports/countering-violent-extremism-trump-era
192 https://theintercept.com/2018/06/15/cve-grants-muslim-surveillance-brennan-center/

Ein besonders anschauliches Beispiel für die Zusammenarbeit zwischen Strafverfolgungsbehörden, Bundesbehörden und akademischen Forschern liefert eine CVE-Finanzbeihilfe, die dem Seattle Police Department gewährt wurde. Die Förderung in Höhe von 409.389 USD finanzierte Überstunden für Polizeibeamte zur Entwicklung und Umsetzung von „Micro Community Policing Plans“, die „Aktivitäten in Gemeinschaften, Daten zur Kriminalität und Polizeidienste zusammenbringen“. Die Pläne sind ausgerichtet auf die „afroamerikanischen, ostafrikanischen, philippinischen, koreanischen, lateinamerikanischen, muslimischen/sikh/arabischen, indianischen und südostasiatischen Gemeinschaften“, insbesondere auf Flüchtlingsfrauen und ihre Familien, 5- bis 18-Jährige und „ausgegrenzte Bevölkerungsgruppen“ in Seattle.[193] Die Förderung bringt die Strafverfolgungsbehörden von Seattle mit einem Rehabilitationszentrum, Schulen, der Stadt, glaubens- und gemeinschaftsbasierten Organisationen sowie Forschern der Seattle University zusammen. Forscher „werden das Programm durch Umfragen in der Bevölkerung, die die ‚Wahrnehmung der Polizei‘ und andere Faktoren messen, evaluieren“.

Durch die Partnerschaft mit einem Polizeiprogramm, das direkt auf bestimmte Gruppen abzielt, zeigt das obige Beispiel eine gefährliche Seite der Zusammenarbeit von Forschern mit CVE-Entscheidungsträgern und -Praktikern. Es wirft schwierige ethische Fragen in Bezug auf die Komplizenschaft mit problematischer staatlicher Überwachung, repressiver Polizeiarbeit und der Fortführung des Racial Profiling auf, was zu der überhöhten polizeilichen Kontrolle rassifizierter Gruppen beiträgt.

Richard Jackson, Gründungsherausgeber von *Critical Studies on Terrorism*, schreibt, der nach den Anschlägen vom 11. September 2001 in den USA begonnene „Krieg gegen den Terror“ habe „über eine Million Menschen getötet und verletzt … unermessliches Leid für Millionen weitere verursacht … und als eines der effektivsten Werkzeuge hegemonialer Herrschaft westlicher Staaten in der heutigen Zeit“ gedient. Weiter führt er aus, dass „das globale Anti-Terror-Regime in seiner Philosophie, seiner Praxis und seinen Auswirkungen inhärent gewalttätig, unterdrückend und lebensvernichtend ist“; man könne „unter solchen Bedingungen … argumentieren, dass die direkte Zusammenarbeit mit der staatlichen Terrorismusbekämpfung ähnlich ist wie Mediziner, die mit Folterern zusammenarbeiten, um das Wohlergehen der Gefangenen zu verbessern“.[194]

Forschung, die von staatlichen Behörden finanziert wird oder mit diesen kooperiert, wie die oben erwähnte Förderung der Polizei von Seattle und der Seattle University durch das DHS, ist in ihrem Spielraum stark eingeschränkt. Aus der Perspektive eines führenden Professors für kritische Terrorismusforschung heraus merkt Jackson an, dass kritische Terrorismusforscher „schon seit Jahren gewarnt und kritisiert und alternative Vorschläge gemacht haben, ohne eine messbare Wirkung zu erzielen; sie haben im aktuellen System der Terrorismusbekämpfung im Wesentlichen keine Stimme“. Er führt weiter aus, dass Forscher, die zur Konsultation und Beratung mit der Regierung herangezogen werden, in Wirklichkeit „in erster

193 https://www.dhs.gov/sites/default/files/publications/EMW-2016-CA-APP-00236%20Full%20Application.pdf
194 https://www.tandfonline.com/doi/pdf/10.1080/17539153.2016.1147771?needAccess=true, S. 121–2

Linie … vom Staat benutzt werden, um bereits beschlossene Vorgehensweisen zu legitimieren und sein öffentliches Ansehen zu stärken“.[195] Da sich der Forschungsrahmen akademischer Partnerschaften mit der Regierung auf die intellektuelle Legitimierung staatlicher Praxis beschränkt, verlagert sich die unabhängige kritische Analyse des Anti-Terror-Regimes oder darin enthaltener spezifischer Praktiken immer weiter fort vom Zentrum staatlicher Macht und Entscheidungsfindung.

Wie in den vorangehenden Umfrageergebnissen angemerkt, stellen ethische Genehmigungsprozesse und Datenschutz-Überlegungen, wie die Einhaltung der DSGVO-Gesetzgebung (Datenschutz-Grundverordnung) und der Nutzungsbedingungen von Social-Media-Unternehmen, große Hindernisse bei der CVE-Forschung dar. Diese Hindernisse führen zu erheblichen Verzögerungen bei der Forschung und den verfügbaren Daten und haben laut der Analyse der Umfrageergebnisse „viele Forscher gezwungen, auf Sekundärdaten zurückzugreifen“.

Wie kann die CVE-Forschung in einem solchen Forschungsklima, in dem Primärquellenanalysen schwierig zu erstellen sind und dazu dienen können, schädliche staatliche Anti-Terror-Praktiken zu legitimieren, auf ethische Weise politikrelevant sein? Erstens könnte die CVE-Forschung auf einem anderen Untersuchungsmodus aufbauen. Jackson argumentiert, dass Forschung, die auf orthodoxe Weise politikrelevant sein will, „uns dazu drängt, bestimmte Arten von Fragen zu stellen und nach bestimmten Arten von Fragen zu suchen. Sie formuliert die Forschungsfrage primär in einem ‚Problemlösungs‘-Modus“ und macht die Forschung dadurch konform mit der Art und Weise, wie politische Entscheidungsträger das „Problem“ artikulieren und das Lösungsspektrum definieren.[196] Eine ethische Forschungsagenda, in der das lösungsorientierte Paradigma weniger Gewicht erhält, könnte stattdessen die Auswirkungen von Terrorismusbekämpfung und CVE auf rassifizierte und marginalisierte Gemeinschaften untersuchen und anhand der Ergebnisse politische Empfehlungen zur Änderung dieser Politik abgeben. Dies würde zu einer Annäherung an ein Verständnis von Politikrelevanz beitragen, bei dem Forschung nicht einfach die staatliche Politik legitimiert, sondern direkt für die Gemeinschaften relevant ist, auf die sie abzielt.

Zweitens würde Forschungsarbeit, die historische, strukturelle und gesellschaftliche Erklärungen für Gewalt gegen Bürger und den Staat beleuchtet – statt lediglich individuelle, ideologische und rassistische Aspekte –, einen weiteren Strang innerhalb einer ethischen CVE-Forschungsagenda bilden. Durch die Ausdehnung des Forschungsspektrums auf Gewalt gegen Gemeinschaften, die traditionell als „anfällig für Radikalisierung“ gelten, kann die CVE-Forschung für politische Maßnahmen eintreten, die sich um eine Wiedergutmachung historischer und struktureller Gewalt bemühen. Indem beispielsweise das Inhaftierungs- und Abschieberegime als institutioneller Schaden gegen bestimmte Gemeinschaften verstanden wird, kann die CVE-Forschung beginnen, sich für den Abbau solcher Institutionen und für die Entwicklung politischer Maßnahmen zum Migrationsmanagement einzusetzen.

195 Ebd., S. 123
196 Ebd.

Schließlich könnte die CVE-Forschung durch die Entwicklung einer Forschungsagenda, die von Anti-Terror-Strategien betroffene Menschen in den Mittelpunkt stellt und stärkt, für eine Abkehr von einem gesamtgesellschaftlichen Ansatz plädieren, der eine überhöhte polizeiliche Kontrolle dieser Gemeinschaften begünstigt. Auf diese Weise könnte die CVE-Forschung die Auswirkungen von politischen Maßnahmen untersuchen, die Gemeinschaften stärken – beispielsweise mehr Investitionen in Wohnraum, die Förderung der psychischen Gesundheit, Gesundheitsversorgung und Beschäftigungsmöglichkeiten. Indem sie für Grundbedürfnisse wie solche sowie eine reduzierte Polizeipräsenz in den Gemeinschaften plädiert und dies mit einem Verständnis von struktureller Gewalt verbindet, kann die CVE-Forschung auf eine andere Art der Intervention in die Wege der Gewalt drängen.

Global Network
on Extremism & Technology

KONTAKTANGABEN

Im Falle von Fragen oder zur Anforderung weiterer Exemplare wenden Sie sich bitte an:

ICSR
King's College London
Strand
London WC2R 2LS
Vereinigtes Königreich

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Wie alle anderen GNET-Publikationen kann auch dieser Bericht kostenlos von der GNET-Website unter www.gnet-research.org heruntergeladen werden.