ISD | Powering solutions to extremism, hate and disinformation

CASM technology

Erforschung des sich im Wandel begriffenen Online-Ökosystems: Telegram, Discord und Odysee

Henry Tuck, Jakob Guhl, Julia Smirnova, Lea Gerster and Oliver Marsh

WARNUNG: Dieser Bericht enthält Abbildungen und Darstellungen von Beiträgen, die als hochgradig verstörend wahrgenommen werden könnten. Insbesondere handelt es sich dabei um Aufrufe zur Gewalt, die Verherrlichung von Terrorismus und die Entmenschlichung von Minderheiten.

Übersicht

Akteur:innen die Extremismus, Hass und Desinformation verbreiten nutzen eine Vielzahl an digitalen Räumen, um schädliche Ideologien zu verbreiten und Menschenrechte und Demokratie online zu untergraben. Daher ist es entscheidend, die Ideen, Online-Netzwerke und Aktivitäten dieser Akteur:innen besser zu verstehen, um auf Grundlage einer evidenzbasierten Faktenlage wirksame und verhältnismäßige Gegenmaßnahmen zu entwickeln. Die Schaffung einer solchen Evidenzbasis kann jedoch aufgrund von begrenzten technischen Möglichkeiten, Ressourcen und sogar ethischen und rechtlichen Grenzen eine große Herausforderung darstellen. Wir sind besorgt, dass sich all diese Herausforderungen verschlimmern könnten, während die Möglichkeiten zur Verbreitung von schädlichen Inhalten im Internet zunehmen.

Es ist daher besorgniserregend, dass es in vielen Fällen immer schwieriger wird, digitale Forschung systematisch, ethisch und rechtlich zulässig zu betreiben. Dies führt zu einer Situation, in der schwierige Abwägungen getroffen werden müssen zwischen konkurrierenden Interessen, einschließlich des Wunsches nach einem besseren Verständnis von schädlichen Inhalten und Verhaltensweisen im Internet, der Wahrung der Privatsphäre und der Einhaltung rechtlicher Vereinbarungen. Wir argumentieren in diesem Bericht, dass dies nicht der Fall sein muss; Lösungen sind vorhanden, und es sollten so schnell wie möglich Maßnahmen ergriffen werden, um ein zukünftiges Szenario sicherzustellen, in dem Forscher über die notwendigen Instrumente zur systematischen, ethischen und legalen Beobachtung, Nachverfolgung und Analyse von schädlichen Inhalten und Verhalten im Internet verfügen.

In diesem Bericht werden die Ergebnisse der Forschungsphase eines vom Institute for Strategic Dialogue (ISD) und CASM Technology durchgeführten und vom Omidyar Network finanzierten Projekts vorgestellt. Ziel des Projekts ist es, Forschungsmethoden zur Beobachtung und Analyse kleiner, geschlossener oder kaum moderierter Plattformen zu ermitteln und zu testen. Das Projekt präsentiert die Grenzen und Dilemmata, auf die unsere Forscher dabei stießen. In drei kleinen Forschungs-Fallstudien, die sich auf Telegram, Discord und Odysee konzentrieren, versuchen wir, verschiedene methodische Ansätze anzuwenden, um Plattformen zu analysieren, die in erster Linie technologische, ethische, rechtliche oder Fragmentierungs-Barrieren aufweisen.

Über die Autoren

Jakob Guhl ist Senior Research Manager beim ISD, wo er in der Digital Research Unit und für das ISD Germany arbeitet. Seine Forschungsschwerpunkte sind Rechtsextremismus, islamistischer Extremismus, Hassrede, Desinformation und Verschwörungsideologien. Als ISD-Experte wurde Jakob mehrfach eingeladen, seine Forschungen dem Bundesministerium der Justiz vorzustellen und dem Bundesminister für Inneres und für Heimat seine Handlungsempfehlungen zur Prävention von Rechtsextremismus und Antisemitismus auszusprechen.

Lea Gerster war Analystin beim ISD und ISD Germany. Sie arbeitete an einer Reihe von Projekten bezüglich der Verbreitung von extremistischen Ideologien und Desinformation im deutschen und englischen Sprachraum. Zuvor arbeitete sie zwei Jahre im Bereich der digitalen Extremismusbekämpfung am TRD Policy und dem Centre on Radicalisation and Terrorism. Sie arbeitete auch als Praktikantin für das Schweizer Außenministerium und als Freiwillige auf einer japanischen Teefarm. Sie ist die Co-Autorin des ISD-Berichts "Krise und Kontrollverlust: Deutschsprachiger digitaler Extremismus im Kontext der der COVID-19-Pandemie". Sie hat einen Master in War Studies vom King's College London und einen Bachelor in Geschichte, Japan-Studien und Politikwissenschaften.

Julia Smirnova arbeitet als Senior Analystin beim ISD und ISD Germany wo sie zur Verbreitung von Desinformationen, Verschwörungsmythen, Hassrede und extremistischen Ideologien im Internet forscht. Sie ist Co-Autorin der ISD-Berichte „Digitale Gewalt und Desinformation gegen Spitzenkandidat:innen vor der Bundestagswahl 2021", „Ein Virus des Misstrauens: Der russische Staatssender RT DE und die deutsche Corona-Leugner-Szene" and „Desinformationskampagnen gegen die Wahl: Befunde aus Sachsen-Anhalt". Zuvor arbeitete Julia als Journalistin, unter anderem für Der Spiegel und Die Zeit. Als Moskau-Korrespondentin für Die Welt berichtete sie über die Politik Russlands, die Annexion der Krim und den Krieg in der Ostukraine. Sie hat einen Master in Conflict, Security and Development vom King's College London.

Oliver Marsh ist Gründer des Beratungsunternehmens The Data Skills Consultancy, das die Arbeit an der Schnittstelle von Datenkompetenz und Soft Skills unterstützt. Zuvor war er als Regierungsbeamter am Aufbau der Rapid Response Unit der britischen Regierung und im Ministerium für Digitales, Kultur, Medien und Sport an der Schaffung von Datenzuverlässigkeit nach dem Brexit beteiligt. Er ist Fellow der Denkfabrik Demos, Policy Fellow der Royal Academy of Engineering und Honorary Research Associate der Abteilung für Wissenschaft und Technologie an der University College London.

Henry Tuck ist Head of Digital Policy beim ISD, wo er die Arbeit zur digitalen Regulierung und zu den Maßnahmen von Technologieunternehmen gegen Terrorismus, Extremismus, Hass sowie Des- und Miss-Information im Internet leitet. Henry betreut das Projekt Digital Policy Lab (DPL) des ISD und führt Beratungen zu wichtigen Vorschlägen im Bereich der digitalen Regulierung in Europa und den Five-Eyes-Ländern durch. Er arbeitet mit der Digital Analysis Unit des ISD zusammen, um Forschungsergebnisse in umsetzbare Empfehlungen für die digitale Politik zu übersetzen.

Danksagungen

Dieser Bericht wäre ohne die finanzielle Unterstützung durch das Omidyar Network nicht möglich gewesen. Wir möchten uns bei Wafa Ben-Hassine, Anamitra Deb und Emma Leiken für ihre Vision, ihre kontinuierliche Unterstützung und ihr aufschlussreiches Feedback bedanken. Die Autoren möchten auch Nestor Prieto Chavana, Jack Pay and Carl Miller von CASM danken, deren technische Expertise und Ratschläge für diese Forschung von entscheidender Bedeutung waren.

ISD | Powering solutions to extremism and polarisation

Amman | Berlin | London | Paris | Washington DC

www.isdglobal.org

Inhalt

Executive Summary

Aktuell entsteht im Internet ein immer breiteres Spektrum an digitalen Räumen, in denen schädliche Inhalte verbreitet und Menschenrechte und demokratische Werte untergraben werden. Zur Entwicklung wirksamer und angemessener Gegenmaßnahmen auf der Grundlage einer breiteren Evidenzbasis ist ein Verständnis solcher Online-Netzwerke und Aktivitäten von entscheidender Bedeutung. Die Schaffung einer solchen Evidenzbasis kann für die Forschung jedoch eine große Herausforderung darstellen. Das gilt sowohl in Bezug auf die technischen Möglichkeiten als auch auf die verfügbaren Ressourcen und nicht zuletzt die ethischen und rechtlichen Rahmenbedingungen. Aufgrund der zunehmenden Optionen zur Verbreitung schädlicher Inhalte im Internet befürchten wir eine weitere Verschärfung dieser Bedrohungen.

Diese Herausforderung, digitale Forschung systematisch, ethisch und rechtskonform zu betreiben, führt zu einer Situation, in der zwischen konkurrierenden Interessen abgewogen werden muss. Neben dem Wunsch, schädliche Inhalte und Verhaltensweisen im Internet zu verstehen und zu bekämpfen, gilt es, die geltenden Datenschutzvorschriften und rechtlichen Vereinbarungen einzuhalten. In diesem Bericht argumentieren wir, dass dieses Dilemma nicht unüberwindbar ist. Es gibt Lösungen, die ein schnelles Ergreifen von Maßnahmen ermöglichen und ein zukunftssicheres Szenario schaffen können, in dem Forscher:innen die Instrumente zur Verfügung stehen, mit denen schädliche Inhalte und Verhaltensweisen auf systematische, ethische und rechtmäßige Weise beobachtet, nachverfolgt und analysiert werden können.

Dieser Bericht fasst die Ergebnisse der Forschungsphase eines Projektes des Institute for Strategic Dialogue (ISD) und CASM Technology zusammen. Im Rahmen dieses vom Omidyar Network finanzierten Projektes sollen Forschungsmethoden für die Beobachtung und Analyse kleiner, geschlossener oder kaum moderierter Plattformen identifiziert und getestet werden. Der Report zeigt anhand von Praxisbeispielen auf, welchen Einschränkungen und Hindernissen die Forscher:innen gegenüberstehen. In drei kurzen Fallstudien zu den Plattformen Telegram, Discord und Odysee (auf Deutsch, Englisch bzw. Französisch) wenden wir verschiedene methodische Ansätze zur Analyse von Plattformen an, die in erster Linie technologische, ethische und rechtliche Hindernisse oder eine ausgeprägte Fragmentierung aufweisen.

Wichtigste Ergebnisse: Forschungshindernisse

- **Insgesamt ist es trotz einiger Schwierigkeiten möglich, digitale Forschung auf Plattformen wie Telegram, Discord und Odysee auf eine Weise durchzuführen, die gleichzeitig systematisch, ethisch und rechtskonform ist**. Während ethische Erwägungen in Bezug auf datenschutzrechtliche Vorgaben und Erwartungen uns daran hindern, schädlichere Communities auf Telegram zu untersuchen, halten uns rechtliche Bedenken hinsichtlich einer Verletzung von Vertragsbestimmungen davon ab, systematisch Daten von Discord-Servern zu erfassen. Insofern schränken ethische und rechtliche Hindernisse die Möglichkeiten von Forscher:innen ein, Communities mit schädlichen Inhalten und Verhaltensweisen auf diesen Plattformen systematisch zu untersuchen. Bei der Untersuchung von Odysee gab es wegen des öffentlichen Charakters der Plattform zwar weniger ethische Bedenken. Jedoch wurde eine gründlichere Analyse aufgrund einer Kombination aus technischer Komplexität und unklaren Nutzungsbedingungen (Terms of Service, TOS) ebenfalls erschwert.
- **Auf Telegram können Administrator:innen von vermeintlich öffentlichen Bereichen mithilfe der Plattformfunktionalitäten die systematische Untersuchung von Communities mit schädlichen Inhalten und Verhaltensweisen verhindern**. Auf Telegram haben Nutzer:innen die Möglichkeit, „private" Gruppen und Kanäle zu erstellen, die nicht systematisch gefunden und untersucht werden können. Dass diese Kanäle Tausende Mitglieder haben können, strapaziert die Auslegung des Begriffs „privat" deutlich. Zudem entstehen ethische Bedenken, wenn Forscher:innen ihre Identität verschleiern müssen, um Zugang zu diesen Kanälen zu erhalten.
- **Auf Discord ist der Umfang unserer Forschungsarbeit durch Fragmentierung sowie durch ethische und rechtliche Hindernisse eingeschränkt**. Die Programmierschnittstelle (Application Programming Interface, API) von Discord und die intransparenten Suchfunktionen der Plattform sowie Software von Drittanbietern stellen Forschungshindernisse durch Fragmentierung dar. Gleichzeitig untersagen die Nutzungsbedingungen von Discord die Erfassung von Daten der Nutzer:innen über die API der Plattform, woraus sich juristische Risiken für die Forscher:innen ergeben. Auch beim Ausfüllen von Formularen für den Beitritt zu einzelnen Gruppen ist oft ein

erheblicher Grad von Täuschung oder die Unterstützung problematischer Überzeugungen erforderlich, was uns davon abhält, uns Zugang zu vielen untersuchungswürdigen Servern zu verschaffen.

- **Das auf Blockchain basierende Design von Odysee (ein technologisches Hindernis) stellt weniger unüberwindbare Barrieren für die Forschung dar, als zu erwarten**. Zusätzliche Datenpunkte liefern Transaktionen mit der Kryptowährung LBC, die tatsächlich öffentlich sichtbar sind. Dies erfordert jedoch technisches Fachwissen und einen erheblichen Aufwand, damit verschiedene Tools untersucht und zusammengeführt werden können. Da es sich noch um eine sehr junge Technologie handelt, verfügen viele Organisationen möglicherweise nicht über dieses Fachwissen zur Blockchain-Technologie; zudem sind unter Umständen weniger Open-Source-Tools verfügbar. Die audiovisuelle Ausrichtung der Plattform stellt eine weitere Herausforderung dar, da die Forscher:innen die Inhalte manuell sichten müssen. Die unklaren Nutzungsbedingungen von Odysee sorgen zudem für Unsicherheit darüber, was angemessen oder rechtlich zulässig ist.
- **Die technologischen, ethischen und rechtlichen Hindernisse und die Fragmentierung von Telegram, Discord und Odysee sind folglich eng miteinander verknüpft**. So hindern uns beispielsweise rechtliche Bedenken daran, fragmentierungsbedingte Hindernisse durch systematische Suchmethoden auf Discord zu überwinden. In ähnlicher Weise werfen die technischen Funktionen von Telegram ethische Hindernisse auf.

Wichtigste Ergebnisse: Implikationen für Forscher:innen

Unsere Forschungsarbeit im Rahmen dieses Projekts zeigt auf, wie Plattformen absichtlich oder unabsichtlich die im öffentlichen Interesse liegende Forschung auf verschiedene Weise behindern können.

- **Technologische Handlungsspielräume der Plattformen können den Zugang zu Daten oder gehosteten Inhalten verhindern oder die Datenerfassung aus technischer Sicht unnötig erschweren**. Das geschiet beispielsweise, wenn die Front-End- oder Back-End-Architekturen der Plattformen fragmentiert sind oder schlecht gepflegt werden, bzw. wenn die für den Datenzugriff verfügbaren Tools schlecht dokumentiert sind. Insbesondere in der Zivilgesellschaft verfügen möglicherweise nicht alle Forscher:innen über das erforderliche Fachwissen zur Erforschung der technischen Möglichkeiten einer Vielzahl verschiedenartiger Plattformen.
- **Unklar formulierte Nutzungsbedingungen von Plattformen können zusätzliche Nachteile oder Risiken für Forscher:innen mit sich bringen und die Kosten und Eintrittsbarrieren für die Online-Forschung erhöhen**. Dank des Zugangs zu externer, kostenloser Rechtsberatung waren wir glücklicherweise in der Lage, die Nutzungsbedingungen der Plattformen und die sich daraus ergebenden rechtlichen Risiken im Zusammenhang mit dem Datenzugang genauer zu bewerten.
- **Zur Rechtfertigung von Einschränkungen des Zugangs zu Daten durch Forscher:innen können sich Plattformen gezielt auf rechtliche oder ethische Bedenken berufen, beispielsweise mit Verweis auf den Datenschutz oder das Recht der Nutzer:innen auf Privatsphäre**. Dies kann selbst dann der Fall sein, wenn Nutzer:innen aktiv in die Weitergabe und Verwertung ihrer Daten für bestimmte, begrenzte Forschungszwecke eingewilligt haben. Ebenso kann dies der Fall sein, wenn die Ausweisung von Online-Räumen als private Bereiche zu ethischen Unsicherheiten führen kann, wenn sie in der Praxis sowohl für Nutzer:innen als auch für Forscher:innen leicht und weitgehend zugänglich sind.
- **Es besteht die Gefahr, dass die knappen Ressourcen der Forschungsgemeinschaft zur Bewältigung dieser Herausforderungen unkoordiniert und isoliert eingesetzt werden**. Ohne solide Mechanismen und Anreize für eine stärkere Zusammenarbeit werden folglich Möglichkeiten zur Ausschöpfung von Skalierungseffekten verpasst.
- **Hindernisse für die Online-Forschung können für Forscher:innen problematische Anreize schaffen, wenn es darum geht, verschiedene rechtliche und ethische Risiken abzuwägen oder zu umgehen**. Zum Beispiel könnten die rechtlichen Risiken für Forscher:innen unter Rückgriff auf Täuschungen reduziert werden, wenn sie

für Forschungszwecke Tools von Drittanbietern nutzen, die gegen die Nutzungsbedingungen der Plattformen verstoßen. Wenn Plattformen oder Nutzer:innen nicht bemerken, dass eine Datenerfassung stattfindet, ist die Wahrscheinlichkeit deutlich geringer, dass rechtliche Schritte gegen Forscher:innen angestrengt werden.

- **Die Anwendung von Drittanbieter-Tools oder unseriösen Methoden kann Forscher:innen davon abhalten, ihre Arbeit zu veröffentlichen und/oder sie dazu verleiten, nicht nachvollziehbare Angaben zu ihren Forschungsmethoden zu veröffentlichen**. Dies wirkt sich wiederum nachteilig auf die Qualität, Vergleichbarkeit und Reproduzierbarkeit der Online-Forschung zu wichtigen gesellschaftlichen Themen aus und kann zu einem zunehmenden Verlust des Vertrauens der Plattformen in die Forschungsgemeinschaft führen.

Wichtigste Ergebnisse: Extremistische Communities auf Telegram, Discord und Odysee

- **Auf Telegram identifizierten die Forscher:innen des ISD sechs deutschsprachige private Kanäle und 80 private Gruppen, die mit Rechtsextremismus und schädlichen Verschwörungstheorien assoziiert sind**. Der größte dieser Kanäle zählt 12.049 Mitglieder. Aus unseren Ergebnissen geht hervor, dass selbst diese größeren, vorgeblich privaten Räume für schädliche Aktivitäten genutzt werden, darunter Aufrufe zur Gewalt gegen Politiker:innen, Verbreitung von Falschinformationen und Koordinierung der Offline-Mobilisierung.
- **Auf Discord identifizierten die Forscher:innen des ISD 31 englischsprachige Server mit katholisch-extremistischen Inhalten und insgesamt 9.585 Mitgliedern sowie 16 mit islamischem Extremismus assoziierte Server mit insgesamt 4.757 Mitgliedern**. Auf diesen Servern fanden wir erhebliche Mengen extrem menschenfeindlicher Inhalte, die sich gegen die LGBTQ-Gemeinschaft, jüdische Menschen und Frauen richteten. Sowohl katholische als auch islamistische Extremist:innen äußerten antidemokratische Ansichten, riefen zur Errichtung totalitärer religiöser Staaten auf und teilten gewaltorientierte Inhalte bis hin zur Unterstützung von Terrorist:innen und terroristischen Organisationen.
- **Auf Odysee identifizierten die Forscher:innen des ISD 8.690 französischsprachige Videos mit rechtsextremen monarchistischen Inhalten und 6.035 neofaschistische Videos, sowie 4.084 katholisch-fundamentalistische Videos**. Die Analyse dieser Videos deutet auf das Bestehen ausgeprägter antidemokratischer Ideologien innerhalb der französischsprachigen Communities auf Odysee hin. Dazu gehört auch Material, in dem der Holocaust geleugnet und der Nationalsozialismus verherrlicht werden – beides potenzielle Straftatbestände in Frankreich.

Empfehlungen

Auf der Grundlage der in diesem Bericht dargestellten Ergebnisse, Implikationen für Forscher:innen und Darstellungen über den Stand der bisherigen politischen Regulierungsanstrengungen haben wir eine Reihe von übergreifenden Empfehlungen für alle Online-Plattformen, politischen Entscheidungsträger:innen und Aufsichtsbehörden sowie zivilgesellschaftliche und akademische Forscher:innen formuliert. Diese Empfehlungen sollen dazu dienen, die verschiedenen technologischen, ethischen und rechtlichen Hindernisse sowie die bei der Forschungsarbeit häufig festgestellte Fragmentierung zu überwinden.

Uns ist bewusst, dass manche unserer Empfehlungen zusätzlichen Aufwand bedeuten – insbesondere für kleinere Plattformen mit weniger Ressourcen oder geringen technischen Möglichkeiten. Gegenwärtig stellen die Plattformen jedoch eher praktische Funktionen zur Erleichterung der Kommunikation und Koordinierung von schädlichen Akteur:innen bereit, während sie nur eingeschränkte oder unzureichende Funktionen für die im öffentlichen Interesse liegende Forschung in Bezug auf diese Online-Räume bieten. Dieses Ungleichgewicht gilt es aus unserer Sicht zu beseitigen.

Technologische Hindernisse

- Plattformen sollten Drittanbietern, die im öffentlichen Interesse liegende Forschung betreiben, einen autorisierten Datenzugang – beispielsweise über APIs – anbieten. Begleitend müsste eine klare, konsistente

und öffentlich zugängliche Dokumentation bereitgestellt werden, die Angaben zu den Datentypen enthält, die erfasst werden können. Zum Schutz der Privatsphäre der Nutzer:innen sollte gleichzeitig die Erfassung sensibler personenbezogener Daten ausreichend begrenzt werden.

- Bei der Ausarbeitung zukünftiger Bestimmungen sollten die politischen Entscheidungsträger:innen und Aufsichtsbehörden einen präzisen, zuverlässigen und für die im öffentlichen Interesse liegende Forschung ausreichenden Datenzugang für alle Plattformen vorschreiben. Dies würde nicht nur die derzeit größten Plattformen betreffen, sondern auch das breite Spektrum kleinerer und mittlerer Online-Plattformen mit einbeziehen.
- Akademische und zivilgesellschaftliche Forscher:innen sollten sich über wirksame Ansätze und Instrumente zur Datenerfassung sowie über die Erfahrungen austauschen, die sie beim Zugriff auf die wachsende Vielfalt von Plattformen im sich entwickelnden Online-Ökosystem gemacht haben.

Hindernisse durch Fragmentierung

- Plattformen sollten einen systematischen Datenzugang bereitstellen, der es Forschern:innen ermöglicht, zuverlässig auf akkurate Daten aus allen öffentlichen Bereichen der Plattform zuzugreifen, damit die Forscher:innen untersuchungswürdige Online-Räume oder Communities nicht erst manuell identifizieren müssen. Unabhängig davon, ob für die systematische Suche plattformeigene oder Drittanbieter-Tools eingesetzt werden, müsste die Zuverlässigkeit, Vollständigkeit und Genauigkeit solcher Tools beispielsweise durch eine unabhängige Prüfung nachgewiesen werden.

Ethische Hindernisse

- Plattformen sollten eine angemessene Grenze für die Anzahl der in privaten Gruppen und Kanälen teilnehmenden Nutzer:innen festlegen und Online-Bereiche mit einem großen Nutzerkreis ab einem bestimmten Schwellenwert als öffentlich deklarieren. Inhalte, für die keine berechtigten Erwartungen an den Datenschutz bestehen, weil sie beispielsweise auf öffentlichen Seiten gepostet werden, sollten über einen überprüften API-Zugang zugänglich gemacht werden.
- Falls die Plattformen solche Veränderungen auf freiwilliger Basis nicht umsetzen, könnten die politischen Entscheidungsträger:innen in Erwägung ziehen, verbindliche Anforderungen für die Unternehmen festzulegen. Diese sollten sie dazu verpflichten, klarzustellen, welche Bereiche ihrer Plattformen tatsächlich öffentlicher oder privater Natur sind, und angemessene Schwellenwerte zur Begrenzung der Zahl der Nutzer:innen bestimmen, die an privaten Online-Räumen teilnehmen.
- Die Forschungsgemeinschaft müsste sich dafür einsetzen, ethische Ansätze für die wissenschaftliche Untersuchung öffentlicher, halbprivater und privater Online-Räume zu formalisieren. Sie sollten sowohl der potenziellen Gefährlichkeit dieser Räume gerecht werden als auch das Recht der Nutzer:innen auf Privatsphäre respektieren.

Rechtliche Hindernisse

- Die Plattformen sollten in ihren Nutzungsbedingungen nicht nur die zulässigen Arten von Inhalten und Aktivitäten definieren, sondern auch eindeutige Vorgaben für die Anwendung dieser Nutzungsbedingungen auf den Datenzugriff durch Forscher:innen festlegen. Anschließend könnten diese konsequent durchgesetzt werden.
- Die politischen Entscheidungsträger:innen müssten Rechtsschutz für Forscher:innen gewährleisten, die unter Wahrung der Datenschutzvorkehrungen im öffentlichen Interesse liegende Online-Forschung betreiben.
- Akademische und zivilgesellschaftliche Forscher:innen sollten die Chance nutzen, ihre Expertise über die rechtlichen Implikationen beim Zugang zu Plattformdaten zu teilen oder zu bündeln.

Glossar

Der Begriff „**Alt-Tech**“ bezeichnet („alternative“) Social-Media-Plattformen, die von Gruppen und Einzelpersonen genutzt werden, die der Meinung sind, dass ihre politischen Ansichten auf den großen Social-Media-Plattformen nicht erwünscht sind. Dazu gehören Plattformen, die zu bestimmten politischen Zwecken aufgebaut wurden, libertäre Plattformen, die ein breites Spektrum politischer Positionen sowie auch Hass und Extremismus tolerieren, aber auch Plattformen, die zu ganz anderen, nicht-politischen Zwecken wie beispielsweise für Computerspiele (Gaming) aufgebaut wurden.

Programmierschnittstellen (Application Programming Interfaces, APIs) sind Softwareschnittstellen, die eine Kommunikation zwischen zwei Anwendungen ermöglichen. Die Anwendungsmöglichkeiten sind vielfältig. In diesem Bericht sind APIs gemeint, die Forscher:innen per Anfrage den Zugriff auf bestimmte Daten von bestimmten Online-Plattformen gestatten. Als zwischengeschaltete Instanz stellen APIs eine zusätzliche Sicherheitsebene bereit, indem sie einen direkten Zugriff auf Daten verhindern und das Volumen und die Häufigkeit der Anfragen protokollieren, verwalten und kontrollieren.

Verschwörungstheorien sind Versuche, ein Phänomen zu erklären, indem man sich auf eine geheime Absprache zwischen mächtigen Akteur:innen beruft. Verschwörungen werden als geheim oder esoterisch dargestellt, wobei sich die Verfechter:innen des jeweiligen Narrativs als die wenigen Eingeweihten sehen, die Zugang zu verborgenem Wissen haben. Die Anhänger:innen von Verschwörungstheorien sehen sich in der Regel in direkter Opposition zu den Kräften, die das Verschwörungsmuster inszenieren, wobei es sich typischerweise um staatliche Akteur:innen oder einflussreiche Personen handelt.

Bei **Crowdsourcing- und Umfragemethoden melden Nutzer:innen von Online-Plattformen** freiwillig bestimmte Inhalte an Forscher:innen. Hierfür verwenden die Nutzer:innen Mechanismen wie Browser-Plugins oder Formulare.
Das ISD definiert Desinformation als falsche oder irreführende Inhalte, die mit der Absicht verbreitet werden, zu täuschen oder wirtschaftliche oder politische Vorteile zu erwirken und der Öffentlichkeit Schaden zufügen können. Wenn wir uns dagegen auf Inhalte beziehen, die ohne eine solche Absicht verbreitet werden, verwenden wir den Begriff Misinformation.

Verschlüsselung bezeichnet den **Prozess der Informationscodierung**, bei dem die verschlüsselten Daten nur für die intendierten Empfänger:innen verständlich sind.

Ethnographie bzw. ethnografische Forschungsmethoden sind soziologische Forschungsmethoden, die eine tiefe und langfristige Auseinandersetzung mit bestimmten Bevölkerungsgruppen beinhalten. Anstatt sich auf Technologien zur Datenerfassung zu stützen, verfolgen die Forscher:innen hierbei einen auf den Menschen ausgerichteten Ansatz, indem sie Online-Räume weniger als virtuelle, sondern als soziale Räume betrachten und beobachten.

Das ISD definiert **Extremismus** als das Eintreten für eine Weltanschauung, welche die Überlegenheit und Dominanz einer identitätsbasierten Eigengruppe (Ingroup) über alle Fremdgruppen (Outgroups) für sich beansprucht. Extremismus fördert eine entmenschlichende, ausgrenzende Denkweise, die mit Pluralismus und universellen Menschenrechten unvereinbar ist.

Unter **fragmentierten Plattformen** verstehen wir solche, bei denen Online-Inhalte theoretisch zwar ohne technologische oder ethische Hindernisse zugänglich sind, aber dennoch nicht schnell oder systematisch – beispielsweise über eine API – durchsucht werden können. Somit müssen relevante Inhalte inmitten einer Unmenge von anderem Datenmaterial gefunden manuell werden.

Als **schädliche Inhalte und Verhaltensweisen** (harmful content and behaviour) bezeichnen wir ein breites Spektrum von Online-Aktivitäten, die negative Auswirkungen auf die Menschenrechte, die Gesellschaft und/oder die Demokratie haben können. Dazu gehören gezielte Anfeindungen von Personen, die Aufhetzung zur Gewalt gegen eine bestimmte Gruppe oder die Verbreitung von Desinformationen und schädlichen Verschwörungstheorien. In einigen Fällen kann das Schadenspotenzial durch den Inhalt selbst zurückzuführen sein, wobei das damit

verbundene Risiko durch verstärkende Mechanismen vergrößert wird. In anderen Fällen kann der Schaden durch umfassende Verhaltensmuster und nicht durch die Art des Inhalts selbst verursacht werden. Je nach geografischem und rechtlichem Rahmen sind verschiedene Formen von schädlichen Inhalten und Verhaltensweisen rechtswidrig oder nicht. Je nach Plattform können diese auch in den Geltungsbereich der Community-Richtlinien, Standards oder unternehmenseigenen Regeln fallen oder nicht.

Unter Hass verstehen wir Überzeugungen oder Praktiken, die eine ganze Gruppe von Menschen aufgrund bestimmter Charaktermerkmale wie ethnische Zugehörigkeit, Religion, Geschlecht, sexuelle Orientierung oder Behinderung angreifen, verleumden, diskreditieren oder ausgrenzen. Mit Hassakteur:innen sind Einzelpersonen, Gruppen oder Communities gemeint, die sich aktiv und offen an den oben genannten Aktivitäten beteiligen, sowie diejenigen, die implizit Personengruppen angreifen, indem sie beispielsweise Verschwörungstheorien und Desinformationen verbreiten. Hassaktivitäten werden als Gegensatz zu Pluralismus und der universellen Anwendung der Menschenrechte verstanden.

Offene Plattformen sind Social-Media-Plattformen, auf denen Inhalte für Nutzer:innen ohne weitere Überprüfung sichtbar und oft über Suchmaschinen zugänglich sind. Im Gegensatz dazu sind Inhalte auf **geschlossenen Plattformen** nicht ohne Weiteres über Suchmaschinen zugänglich und können oft nur nach einer zusätzlichen Authentifizierung oder auf Einladung aufgerufen werden. Plattformen weisen häufig offene und geschlossene Elemente auf. So gibt es bei Facebook beispielsweise öffentliche und private Gruppen.

Systematische Suchmethoden nutzen Technologien, mit denen große Mengen an Daten und Metadaten direkt aus Online-Plattformen extrahiert werden können. Zu den Daten gehören beispielsweise der Inhalt von Online-Texten, Beziehungen zwischen Online-Konten und Metadaten wie der Zeitstempel oder geografische Standort von Posts. Viele Social-Media-Plattformen erleichtern den Zugang zu Daten, indem sie APIs bereitstellen, mit denen Forscher:innen direkt auf verschiedene Arten von Plattformdaten zugreifen können, ohne selbst einen Code von Grund auf neu zu entwickeln. Die Entwicklung von KI-basierten Ansätzen ermöglicht darüber hinaus immer komplexere Analysemethoden. So werden beispielsweise zunehmend Methoden der Computerlinguistik (Natural Language Processing, NLP) eingesetzt, um in großen Online-Textmengen Trends, Stimmungen und namentlich erwähnte Entitäten zu erkennen.

Einleitung

Aktuell entsteht im Internet ein immer breiteres Spektrum an digitalen Räumen, in denen schädliche Inhalte verbreitet und Menschenrechte und demokratische Werte untergraben werden. Um wirksame und angemessene Gegenmaßnahmen zu entwickeln, die auf einer breiteren Evidenzbasis beruhen, ist ein Verständnis ihrer sich entwickelnden Auffassungen, Online-Netzwerke und Aktivitäten entscheidend. Die Schaffung einer solchen Evidenzbasis kann für die Forschung jedoch eine große Herausforderung darstellen, was die technischen Möglichkeiten, die Ressourcen und nicht zuletzt die ethischen und rechtlichen Rahmenbedingungen betrifft. Aufgrund der zunehmenden Optionen, schädliche Inhalte im Internet zu verbreiten, befürchten wir ebenfalls eine weitere Verschärfung dieser Bedrohungen.

Diese Herausforderung, digitale Forschung systematisch, ethisch und rechtskonform zu betreiben, führt zu einer Situation, in der zwischen konkurrierenden Interessen abgewogen werden muss. Neben dem Wunsch, schädliche Inhalte und Verhaltensweisen im Internet zu verstehen und zu bekämpfen, gilt es, die geltenden Datenschutzvorschriften und rechtlichen Vereinbarungen einzuhalten. In diesem Bericht argumentieren wir, dass dieses Dilemma nicht unüberwindbar ist. Es gibt Lösungen, die ein schnelles Ergreifen von Maßnahmen ermöglichen und ein zukunftssicheres Szenario schaffen können, in dem Forscher:innen die Instrumente zur Verfügung stehen, um schädliche Inhalte und Verhaltensweisen systematisch, ethisch und rechtmäßig zu beobachten, nachzuverfolgen und zu analysieren.

Dieser Bericht fasst die Ergebnisse der Forschungsphase eines Projektes des Institute for Strategic Dialogue (ISD) und CASM Technology zusammen. Im Rahmen des vom Omidyar Network finanzierten Projektes sollen Forschungsmethoden für die Beobachtung und Analyse kleiner, geschlossener oder kaum moderierter Plattformen identifiziert und getestet werden. In dem Bericht über die Phase I dieses Projektes wurden die Ergebnisse der Scoping-Phase zur Ermittlung von relevanten Plattformen und Forschungsmethoden vorgestellt.[1] Dazu gehörte die Beschreibung der wichtigsten Hindernisse, die diese Plattformen für die Erforschung und Bekämpfung schädlicher Inhalte und Verhaltensweisen aufwerfen, sowie die Untersuchung bestehender Forschungsmethoden und Tools zur Bewältigung dieser Hindernisse. Auf dieser Grundlage haben wir drei übergeordnete Kategorien von Hindernissen entwickelt und sie unter den Begriffen „technologische Hindernisse", „ethische und rechtliche Hindernisse" sowie „Fragmentierung" zusammengefasst.

- **Technologische Hindernisse** können in Form von Verschlüsselung, KI-generierten Inhalten, Blockchain, dezentralen Plattformstrukturen oder schwer systematisch zu analysierenden Inhaltsformaten auftreten (insbesondere im audiovisuellen Bereich).
- **Ethische und rechtliche Hindernisse** können sich aus der Erwartung an die Privatsphäre, aus rechtlichen Einschränkungen, aus Schwierigkeiten bei der Einholung einer informierten Zustimmung oder sogar aus den Nutzungsbedingungen der Plattformen ergeben, wenn diese eine ansonsten legitime Forschung im öffentlichen Interesse verbieten. Einige Plattformen weisen ausschließlich ethische oder ausschließlich rechtliche Hindernisse auf.
- **Hindernisse durch Fragmentierung** entstehen bei Plattformen, bei denen Online-Inhalte theoretisch zwar ohne technologische oder ethische Hindernisse zugänglich sind, aber dennoch nicht schnell oder systematisch durchsucht werden können – beispielsweise über eine API. Somit müssen relevante Inhalte manuell inmitten einer Unmenge von anderem Datenmaterial gefunden werden.

Im genannten Bericht weisen wir darauf hin, dass die Abwanderung von etablierten Social-Media-Plattformen hin zu weniger moderierten Online-Räumen die Erforschung und Bekämpfung schädlicher Online-Aktivitäten erschweren kann. Diese Feststellung beruht auf der Beobachtung, dass viele dieser Plattformen technologische, ethische und rechtliche Hindernisse für die Forscher:innen aufweisen, die ihre Möglichkeiten zur systematischen Untersuchung von Communities mit schädlichen Inhalten und Verhaltensweisen einschränken..

Der vorliegende Bericht über die zweite Phase baut auf dem genannten Bericht auf. Er zeigt anhand von Praxisbeispielen, welchen Einschränkungen und Hindernissen die Forscher:innen gegenüberstehen. In drei kurzen Fallstudien wenden wir verschiedene methodische Ansätze an, um Plattformen zu analysieren, die in erster Linie technologische, ethische

und rechtliche Hindernisse oder eine ausgeprägte Fragmentierung aufweisen. Dafür haben wir Online-Communities auf Telegram, Discord und Odysee in deutscher, englischer bzw. französischer Sprache untersucht. Ziel dieser Forschung war es, sowohl das wissenschaftliche Verständnis bezüglich der Anwendbarkeit von Methoden in diesen Online-Räumen zu erweitern als auch praktische Beispiele für die Arten von Hindernissen zu liefern, mit denen Forscher:innen konfrontiert werden können, beim Versuch, auf Daten von Online-Plattform zuzugreifen.

Wie in diesen Fallstudien immer wieder deutlich wird, überlagern sich diese Hindernisse oft oder sind miteinander verknüpft, wobei sie sich auf den verschiedenen Plattformen auf unterschiedliche Weise bemerkbar machen. So können rechtliche Erwägungen es unmöglich machen, die Barrien der Fragmentierung durch systematische Suchmethoden zu überwinden. Auch können bestimmte technische Funktionen ethische Hindernisse mit sich bringen. Schließlich führen unklare Nutzungsbedingungen oder das Fehlen einer API mitunter zu Unsicherheit darüber, was technisch machbar oder rechtlich zulässig ist. Wir beschränken uns bewusst auf drei Plattformen.

Die Erkenntnisse dieser Forschung werden in die dritte Phase des Projekts einfließen, in der es darum geht, praktische, technische und aufsichtsrechtliche Lösungen für den Datenzugang und die Transparenz für diese Arten von Online-Räumen zu finden, ohne die Rechte der Nutzer:innen zu verletzen. Weiterhin werden wir unsere Ergebnisse mit den betreffenden Stakeholdern wie Forschungsexpert:innen und Vertreter:innen von Technologieunternehmen diskutieren, die sich mit den Aspekten Datenzugang und Transparenz befassen. Auf der Grundlage unserer Ergebnisse wird zu überlegen sein, wie die gesetzlichen und aufsichtsrechtlichen Rahmenbedingungen angepasst werden müssen. Ziel ist es, mit der zunehmenden Bandbreite und technologischen Vielfalt der Online-Plattformen Schritt zu halten und gleichzeitig die grundlegenden Rechte auf Privatsphäre, Sicherheit und Anonymität im Internet zu respektieren und zu schützen.

Eine der größten Herausforderungen, die sich bei diesem Projekt herauskristallisiert hat, ist die Frage, wie das Recht auf Privatsphäre geschützt werden, während gleichzeitig Forschung im öffentlichen Interesse über Communities mit schädlichen Inhalten und Verhaltensweisen erfolgen. Dieser Bericht befasst sich ebenfalls mit ethischen und rechtlichen Bedenken in Zusammenhang mit berechtigten Erwartungen an die Privatsphäre. Leider gibt es für die Bezeichnung „privater Raum" keine einheitliche Begriffsbestimmung, sodass es für Forscher:innen schwierig ist, zu bestimmen, welche Räume als privat und welche als öffentlich zu betrachten sind. Andererseits erlaubt das Fehlen einer solchen Definition den Plattformen, die Transparenz und den Zugang zu vermeintlich privaten Räumen zu beschränken, die jedoch wegen des relativ problemlosen Zugangs einen eher öffentlichen Charakter haben. Wie wir bereits dargelegt haben, sollten Faktoren wie die Größe, der Zweck, die Zugänglichkeit und die Art der Beziehungen zwischen den Nutzern:innen eines Kanals oder einer Community bei der Klassifizierung von öffentlichen oder privaten Räumen berücksichtigt werden.[2] Zudem besteht die Gefahr, dass diese Zweideutigkeit die Bedeutung der Verschlüsselung tatsächlich privater Online-Räume und -Kommunikationsmittel untergräbt.

Der Bericht stellt drei Fallstudien vor und beginnt jeweils mit einer Einführung zur betreffenden Plattform und ihren wichtigsten Funktionen. Anschließend beschreibt er, wie diese Funktion bislang von bestimmten Online-Communities für schädliche Inhalte und Verhaltensweisen ausgenutzt wurden. Anschließend befassen wir uns mit den konkreten Ideologien und Online-Communities, die wir auf den einzelnen Plattformen untersucht haben, einschließlich der Gründe für deren Auswahl. Nachfolgend dokumentieren wir die Ergebnisse jeder Fallstudie und konzentrieren uns dabei auf die Gefahren, die von den verschiedenen Communities ausgehen. Schließlich diskutieren wir die Eignung und die Einschränkungen der in der Phase I des Projekts identifizierten Methoden zur Überwindung der vorhersehbaren Hindernisse sowie alle zusätzlichen oder unerwarteten Hindernisse, auf die wir während der eigentlichen Forschungsarbeit gestoßen sind. Dazu gehört auch eine Thematisierung von Methoden, die technisch zwar machbar sind, aus ethischen, sicherheitstechnischen oder rechtlichen Gründen allerdings nicht angewendet worden sind. Im letzten Abschnitt untersuchen wir, ob die in Phase I getroffenen Annahmen bezüglich der drei Kategorien für Forschungshindernisse und die Forschungsmethoden zutreffen und welche Auswirkungen dies auf die Datenerfassung, zukünftige Forschungsanstrengungen und Bemühungen zur Bekämpfung schädlicher Inhalte und Verhaltensweisen auf diesen Plattformen hat. Der Schwerpunkt liegt dabei auf den Auswirkungen auf die zukünftige politische und regulatorische Gestaltung digitaler Räume.

Fallstudie 1: **Telegram**

Wichtigste Ergebnisse

- Auf Telegram können Nutzer:innen private Gruppen und Kanäle erstellen. Die dort eingestellten Inhalte können nicht systematisch durchsucht und überprüft werden, sodass ihrer wissenschaftlichen Erforschung fragmentierungsbedingte Hindernisse entgegenstehen. Da diese Räume als private Räume klassifiziert sind, entstehen zudem ethische Bedenken, wenn Forscher:innen ihre Identität verschleiern müssen, um sich zur Teilnahme anzumelden.
- Gleichwohl können diese Gruppen Tausende Teilnehmer:innen haben, was ihre Klassifizierung als „private Online-Räume" fragwürdig erscheinen lässt. Ferner gibt es Belege dafür, dass sie für schädliche Zwecke eingesetzt werden, einschließlich der Planung potenziell gewalttätiger Handlungen gegen deutsche Politiker:innen.
- Wir empfehlen daher, dass Telegram Gruppen und Kanäle mit einer bestimmten Anzahl von Nutzer:innen als öffentlich deklariert, sodass diese folglich den Nutzungsbedingungen der Plattform unterliegen. Wir empfehlen außerdem, dass Telegram diese Bereiche proaktiver moderiert und Anfragen zur Löschung illegaler Inhalte oder Aktivitäten in diesen Bereichen entgegennimmt.

Im Rahmen dieser Fallstudie hat das ISD deutschsprachige Communities auf Telegram untersucht, die mit rechtsextremen und verschwörerischen Inhalten assoziiert werden. Während über Gruppen und Kanäle, die als öffentlich gekennzeichnet sind, in der Regel relativ umfangreiche Daten verfügbar sind, stehen der Erforschung von Gruppen und Kanälen, die von der Plattform als privat eingestuft werden, sowohl ethische als auch fragmentierungsbedingte Hindernisse entgegen. Dies beginnt bereits damit, dass strittig ist, ob diese Gruppen und Kanäle aufgrund ihrer Größe und ihres Zwecks überhaupt als „private Räume" bezeichnet werden können. Für die Zwecke dieser Forschungsarbeit wurden zunächst Hochrisikogruppen und die als privat eingestuften Kanäle mittels einer quantitativen Link-Analyse identifiziert. Anschließend erfolgte eine qualitative ethnografische Analyse dieser Communities.

Wie viele andere Social-Media-Plattformen hat auch Telegram keinen konkreten Schwellenwert dafür festgelegt, ab welcher Anzahl an Nutzer:innen ein bestimmter Online-Raum nicht mehr als privat gilt. Stattdessen können die Admins der Gruppen und Kanäle bestimmen, ob sie privat sind – unabhängig von ihrer Größe. Daraus ergeben sich mehrere wichtige Konsequenzen für die Art und Weise, wie die Plattform genutzt wird. Da die Nutzungsbedingungen von Telegram beispielsweise nur für Kanäle gelten, die als öffentlich gekennzeichnet sind, entsteht ein Schlupfloch, das es Nutzern:innen ermöglicht, die ohnehin schon begrenzten Inhaltsmoderationsmaßnahmen der Plattform zu umgehen. Obgleich sich Telegram dieser Tatsache offensichtlich bewusst ist und in seinen FAQ erklärt, dass „ein privater Kanal wie ein öffentlicher Kanal behandelt wird, sobald ein privater Kanal einen öffentlich zugänglichen Link hat"[3], gibt es keine Anhaltspunkte dafür, dass die Plattform private Kanäle proaktiv moderiert. Die Funktionsweise privater Kanäle ermöglicht es Administrator:innen auch, durch sogenannte Paywalls, die den Zugang zu diesen privaten Bereichen beschränken, Geld einzunehmen.

Auch für Forscher:innen ergeben sich daraus problematische Konsequenzen. Indem sie eine Gruppe als privat deklarieren, können Administrator:innen die Sichtbarkeit früherer Nachrichten für neue Nutzer:innen einer Gruppe oder eines Kanals auf die letzten einhundert Nachrichten beschränken und/oder das Speichern oder Herunterladen von Inhalten einschränken. Zwar besteht die technische Möglichkeit, als Mitglied der Gruppe oder des Kanals über die Telegram-API auf diese Nachrichten zuzugreifen, doch könnte dies nicht nur gegen die Nutzungsbedingungen der Plattformen verstoßen, sondern auch potenzielle ethische Risiken mit sich bringen. Administrator:innen können diesen Zugriff auf frühere Nachrichten auch deaktivieren und können auf die Aktivitäten von Forscher:innen aufmerksam

gemacht werden, die diese technischen Möglichkeiten nutzenen, was die Erforschung extremistischer Online-Communities weiter erschwert. Aufgrund dieser Hindernisse, die wir in die Kategorie der fragmentierungsbedingten Forschungshindernisse einordnen, ist es den Forscher:innen kaum möglich, systematisch festzustellen, ob es schädliche Inhalte in privaten Gruppen oder Kanälen gibt. Das gilt auch für Gruppen und Kanäle, deren Größe und Zweck stark darauf hindeuten, dass die Nutzer:innen wahrscheinlich keine berechtigten oder realistischen Erwartungen an die Privatsphäre haben. Da ein systematischer Suchansatz mit entsprechend umfangreicher Datenerfassung somit nicht möglich war, haben wir die Inhalte und Verhaltensweisen in diesen Gruppen und Kanälen mit ethnografischen Methoden untersucht. Eine Beschreibung der Methoden erfolgte in unserem Bericht über die Phase I.

Sobald private Gruppen auf Telegram zum Gegenstand ethnografischer Untersuchungen gemacht werden, entstehen ethische Bedenken. Um sich für die Teilnahme an den Gruppen anmelden zu können, müssen neue Mitglieder häufig Fragen beantworten oder sich vorstellen. Dabei müssen sie mitunter detaillierte personenbezogene Angaben machen. Die Beantwortung dieser Fragen kann ein gewisses Maß an Verschleierung von Seiten der Forscher:innen erfordern, obwohl sich dieses Problem in der unten beschriebenen Discord-Fallstudie wesentlich deutlicher stellt. Schließlich überprüfen die Administrator:innen die Mitglieder je nach ihrem Verhalten und geben Links zu vertraulicheren Gruppen möglicherweise nur an Mitglieder weiter, die sie für vertrauenswürdig halten. Das bedeutet, dass Forscher:innen eine trügerische Persona vortäuschen und sich entsprechend berechnend verhalten müssten, um Glaubwürdigkeit und Zugang zu kleineren Gruppen mit mutmaßlich schädlichen Inhalten und Verhaltensweisen zu erlangen. Die Konsequenz ist eine schwierige Abwägung: Je bedenklicher eine private Gruppe von außen erscheint, desto legitimer erscheint es, vortäuschende Mittel einzusetzen, um ihr beizutreten. Andererseits lassen sich derartige Mittel umso schwieriger rechtfertigen, wenn damit der Beitritt zu Räumen bezweckt wird, in denen die Grenze zwischen privat und öffentlich verschwimmt.

Diese ethischen Hindernisse und Bedenken hielten uns letztlich davon ab, in kleinere Gruppen und Kanäle vorzudringen. Insofern beschränken sich unsere Erkenntnisse auf größere Communities, zu denen die Forscher:innen sich vergleichsweise einfach Zugang verschaffen konnten. Unsere Ergebnisse legen nahe, dass selbst diese größeren, vergleichsweise leicht zugänglichen Räume für schädliche Aktivitäten genutzt werden – darunter Aufrufe zur Gewalt gegen Politiker:innen, Verbreitung von Falschinformationen und Koordinierung der Offline-Mobilisierung.

In den folgenden Abschnitten gehen wir auf die Hintergründe und Funktionsweise von Telegram ein und beschreiben die identifizierten und angewendeten Forschungsansätze sowie die in der Praxis aufgetretenen Forschungshindernisse. Abschließend stellen wir die Ergebnisse unserer Analyse vor.

Überblick über die Plattform

Telegram ist eine Messaging-App mit einigen Funktionen einer Social-Media-Plattform. Nach eigenen Angaben hat die Plattform 700 Millionen aktive monatliche Nutzer:innen (Stand: September 2022).[4] Sie wurde 2013 von den russischen Unternehmern Pavel und Nikolai Durov gegründet. Wenngleich das ursprünglich erklärte Ziel der Gründer darin bestand, eine sichere Kommunikation ohne staatliche Überwachung zu ermöglichen, hat sich die Messaging-App im Laufe der Zeit zu einer Plattform entwickelt, die bei einem breiten Spektrum von Akteur:innen beliebt ist, darunter auch Regimekritiker:innen und Aktivist:innen in undemokratischen oder autoritären Gesellschaften. Telegram-Kanäle sind chronologisch geordnete Nachrichten-Feeds, die Nutzer:innen abonnieren können. Sie sind zu einer beliebten Medienplattform für Akteur:innen geworden, die ihre Inhalte einem breiten Publikum zugänglich machen wollen. Das Spektrum der Kanäle reicht von klassischen Nachrichtenkanälen über staatliche Propagandaorgane bis hin zu Influencer:innen, die Verschwörungstheorien verbreiten.

Die Nutzungsbedingungen von Telegram untersagen neben Spam und betrügerischen Aktivitäten lediglich die Verbreitung von illegalen pornografischen Inhalten sowie die Anstiftung zur Gewalt durch öffentliche Kanäle und Bots.[5] Obwohl die Plattform Kanäle mit Bezug zum Terrorismus teilweise in Zusammenarbeit mit den Strafverfolgungsbehörden gelöscht hat, widmet sie anderen illegalen und schädlichen Aktivitäten wenig bis gar keine Aufmerksamkeit, sodass diese unmoderiert bleiben.[6] Dadurch ist Telegram besonders attraktiv für Extremist:innen

und Akteur:innen, die von anderen Social-Media-Plattformen wegen ihrer schädlichen Inhalte oder Verhaltensweisen bereits verbannt wurden.[7]

Wichtige Funktionen

Nutzer:innen von Telegram haben die Möglichkeit, öffentliche und private Gruppen und Kanäle zu erstellen und ihnen beizutreten. Öffentliche Kanäle können über die Suchfunktion von Telegram gefunden werden. Ein Beitritt ist allen Personen uneingeschränkt möglich. Die Inhalte der Kanäle sind auch sichtbar, wenn man den Kanälen nicht beigetreten ist. Für den Beitritt zu privaten Gruppen oder Kanälen ist dagegen ein Einladungslink erforderlihc, der von Administrator:innen (Admins) bereitgestellt wird. Außerdem kann ein Admin neue Mitglieder manuell hinzufügen. Obwohl Telegram Gruppen oder Kanäle als „privat" definiert, wenn diese nicht über die Suchfunktion gefunden und der Zugang nicht ohne einen Einladungslink möglich ist, hängt der tatsächliche Grad der Privatsphäre in der Praxis von den Handlungen und Entscheidungen der Administrator:innen ab.[8] So können Administrator:innen beispielsweise verschiedene Einladungslinks mit unterschiedlichen Bedingungen erstellen. Für jeden spezifischen Link können sie festlegen, ob eine Person, die der Gruppe oder dem Kanal beitritt, eine zusätzliche Freigabe durch die Administrator:innen benötigt. Sie können auch ein Zeitlimit für die Gültigkeit des Links und/oder die Anzahl der Nutzer:innen festlegen, die der Gruppe oder dem Kanal beitreten können. Schließlich kann auch das Umfeld, in dem ein Link zu einer privaten Gruppe oder einem Kanal gepostet wird, auf den Datenschutz und die Beitrittsbedingungen auswirken. So können Links zu privaten Gruppen in öffentlichen Gruppen und Kanälen mit einer hohen Anzahl von Mitgliedern geteilt werden, oder die Administrator:innen können beschließen, diese Links nur in privaten Nachrichten oder gar nicht zu teilen und stattdessen neue Mitglieder manuell hinzuzufügen, indem sie sie aus ihren Kontakten auswählen.

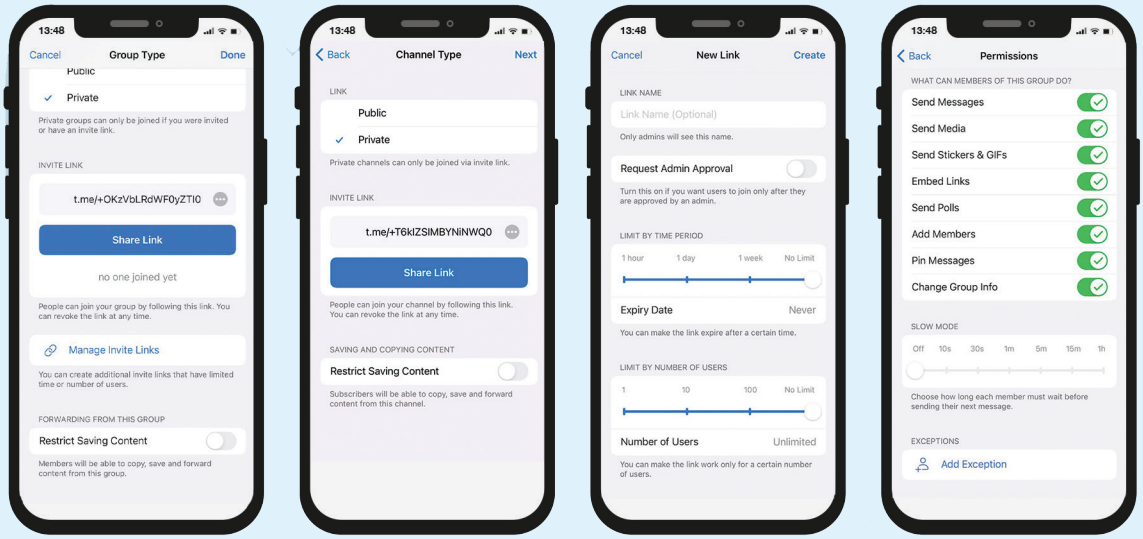


Abbildung 1: Einstellungen, die Administrator:innen für Gruppen und Kanäle auf Telegram vornehmen können

Private Gruppen auf Telegram können bis zu 200.000 Mitglieder haben. Große Gruppen mit mehreren tausend Mitgliedern, die alle Einladungslinks im öffentlichen Raum teilen können, mögen zwar nach den Kriterien von Telegram als privat angesehen werden – nicht jedoch nach der allgemeinen Begriffsauffassung. Das beliebte russische Tool TGStat zur Analyse von Inhalten auf Telegram enthält sowohl öffentliche als auch private Gruppen in seiner Datenbank und listet regelmäßig die beliebtesten privaten Kanäle für ausgewählte Länder auf, wobei sowohl deren Namen als auch die Einladungslinks angezeigt werden.[9] TGStat erfasst Daten aus diesen privaten Gruppen und Kanälen, u. a. die Anzahl der Teilnehmer:innen sowie Erwähnungen anderer Gruppen und Kanäle. Dies hat bereits Kritik ausgelöst, insbesondere von Nutzern:innen in Weißrussland, wo die Behörden Menschen festgenommen haben, nur weil sie oppositionelle Telegram-Kanäle abonniert hatten, die von der Regierung als „extremistisch" eingestuft wurden.[10] TGStat gibt an, dass private Gruppen und Kanäle nur dann in der Datenbank enthalten sind, wenn

sie von Nutzer:innen oder Admins, die an Statistiken interessiert sind, hinzugefügt werden oder wenn Links zu diesen Gruppen und Kanälen häufig öffentlich geteilt werden.[11]

Die Datenschutz-Einstellungen bei Telegram ermöglichen nicht nur einen relativ geschützten Kommunikationsraum, sondern können auch als Paywall verwendet werden. Der deutsche Verschwörungsideologe und Influencer Oliver Janich[12] betreibt zum Beispiel mehrere öffentliche Telegram-Kanäle sowie einen privaten Kanal, der nur für zahlende Abonnent:innen zugänglich ist.[13] Gegen eine etwas höheren Preis für das Abo erhalten Nutzer:innen Zugang zu einem privaten Telegram-Chat, in dem sie die Möglichkeit haben, direkt mit Janich zu kommunizieren. Im Oktober 2022 konnte man die Zahlung der Abonnementskosten mit Kryptowährungen vornehmen. Trotz Janichs Festnahme im August 2022 auf den Philippinen funktionieren seine verschiedenen Telegram-Kanäle weiterhin – vermutlich, da sie von seinem Team gepflegt werden.

Daraus lässt sich ableiten, dass viele Gruppen, die nach der eigenen Definition von Telegram zwar als privat gelten, in Wirklichkeit – ähnlich wie einige andere Kommunikationsräume im Internet – in eine Grauzone fallen.[14] Der Grad der Privatsphäre bei Telegram hängt nicht nur von den technischen Funktionen ab, sondern auch von der Größe der Gruppe und den Entscheidungen der Admins. Die nachstehende Tabelle verdeutlicht die Bandbreite für das Maß an Privatsphäre in verschiedenen Arten von Kommunikationsräumen auf Telegram.

← Eher öffentlich				Eher privat →
Öffentliche Gruppen und Kanäle	Große private Gruppen, deren Links in öffentlichen Kanälen und auf anderen Social-Media-Plattformen veröffentlicht werden.	Kleinere private Gruppen, deren Links nur in anderen privaten Gruppen für eine begrenzte Zeit veröffentlicht werden; für den Beitritt ist gegebenenfalls eine Genehmigung des Admins erforderlich.	Private Gruppen, deren Links nicht auf einer Social-Media-Plattform gepostet werden, sondern in privaten Nachrichten zwischen einzelnen Nutzer:innen ausgetauscht werden; Administrator:innen können festlegen, dass nur Mitglieder aus ihren vertrauenswürdigen Kontakten ausgewählt werden..	Private Nachrichten zwischen zwei Nutzer:innen

Abbildung 2: Bandbreite für das Maß an Privatsphäre für verschiedene Arten von Gruppen und Kanäle auf Telegram

Schädliche Aktivitäten auf Telegram

Da auf der Plattform kaum Eingriffe zur Inhaltsmoderation stattfinden, hat sich Telegram zu einer zentralen Social-Media-Plattform für internationale Extremist:innen aus dem gesamten ideologischen Spektrum entwickelt. Unter anderem wird sie von deutschsprachigen Akteur:innen und Communities mit rechtsextremistischen und verschwörungsideologischen Inhalten und Verhaltensweisen sowie von Gegner:innen der sogenannten Corona-Maßnahmen genutzt.[15] So gaben die deutschen Behörden im April 2022 bekannt, dass sie geplante Anschläge und Entführungen vereiteln konnten, bei denen extremistische Akteur:innen, die sich über eine Telgram-Chatgruppe organisiert hatten, den deutschen Gesundheitsminister und andere bekannte Personen ins Visier genommen hatten.[16] In einem anderen Fall leiteten die Behörden strafrechtliche Ermittlungen ein, nachdem journalistische Recherchen ergeben hatten, dass Mitglieder einer örtlichen rechtsextremen privaten Telegram-Gruppe in Dresden sich über einen möglichen Mordanschlag auf den sächsischen Ministerpräsidenten austauschten.[17] Auch andere journalistische Arbeiten haben zahlreiche Gewaltaufrufe in Gruppen und Kanälen auf Telegram dokumentiert.[18] Kriminalbeamte auf Bundes- und Landesebene konnten in Deutschland und Österreich außerdem Telegram-Gruppen identifizieren, die dem Verkauf von Drogen, Waffen, gefälschten Dokumenten und gestohlenen Daten dienten.[19] Obwohl damit bereits eindeutige Belege dafür vorliegen, dass Telegram für rechtswidrige und schädliche Aktivitäten genutzt wird, steht eine systematische Untersuchung über Umfang und Art dieser Aktivitäten in privaten Gruppen bisher noch aus.

Untersuchungen auf Telegram

Technologische Hindernisse

Aus technologischer Sicht sind die Daten in privaten Gruppen auf Telegram leicht zugänglich, nachdem die Forscher:innen ihnen beigetreten sind. Als Mitglieder geschlossener Gruppen können sie in den Gruppeneinstellungen über die Option „Chatverlauf exportieren" Gesprächsverläufe und Listen der Gruppenmitglieder herunterladen und speichern. Dies ermöglicht auch den Zugriff auf ältere Text- und Sprachnachrichten sowie auf alle Bilder, Videos und Dokumente, die in der Gruppe ausgetauscht wurden. Wie oben bereits erwähnt, können Administrator:innen die Sichtbarkeit früherer Nachrichten für neue beitretende Nutzer:innen einer Gruppe oder eines Kanals leidglich auf die letzten hundert Nachrichten beschränken. Trotz der Positionierung als Plattform, die hohen Wert auf die Sicherheit und den Schutz der Privatsphäre ihrer Nutzer:innen legt, bietet Telegram keine Ende-zu-Ende-Verschlüsselung der Gruppenchats an. Die Verschlüsselung ist nur für „geheime Chats" zwischen zwei Nutzern:innen verfügbar. Sie ist keine standardmäßige Voreinstellung, sondern muss manuell ausgewählt werden.

Einige Eigenschaften von Telegram stellen jedoch eine technologische Herausforderung für die systematische Erforschung der Plattform dar. Sprachnachrichten und andere Formen audiovisueller Inhalte, die bei Telegram sehr beliebt sind, lassen eine automatische Analyse nur sehr bedingt zu. Darüber hinaus bietet Telegram Sprach- und Videoanrufe in Gruppen an, die man nicht analysieren kann, ohne selbst darin Mitglied zu sein.

Eine weitere Funktion, die auf Telegram (und vielen anderen Plattformen) verfügbar ist und eine Herausforderung für Forscher:innen darstellt, sind sogenannte selbstlöschende Nachrichten, die nur für eine begrenzte Zeit sichtbar bleiben. In einer der beobachteten Gruppen aktivierten die Admins vorübergehend die Funktion zum automatischen Löschen von Nachrichten, was es unmöglich machte, die gelöschten Nachrichten mit der Funktion zum Exportieren des Chatverlaufs zu erfassen. Außerdem begrenzten sie den Zeitraum, in dem die Chatmitglieder darauf zugreifen konnten. Diese Funktion kann einerseits eine wichtige Rolle beim Schutz der Privatsphäre der Nutzer:innen spielen, stellt aber andererseits auch eine große Herausforderung für die digitale Forschung dar.

Hindernisse durch Fragmentierung

Ein weiteres Hindernis für die Forschung auf Telegram besteht in der Schwierigkeit, relevante Gruppen aufzufinden. Sie wird bedingt durch ein Merkmal der Plattform, das wir hier als Fragmentierung bezeichnen. Private Gruppen und Kanäle auf Telegram sind weder für die plattformeigene Suchfunktion noch für Suchmaschinen zugänglich. Es ist daher nicht möglich, sie durch Eingabe bestimmter Schlüsselwörter zu finden. Ein Lösungsansatz besteht darin, dass Forscher:innen eine systematische Linkanalyse in den öffentlichen Gruppen und Kanälen auf Telegram durchführen, denen sie bereits beigetreten sind, und dann nach Links zu privaten Gruppen oder Kanälen filtern oder in Datenbanken, bzw. auf anderen Plattformen nach entsprechenden Links suchen. Alternativ könnten Forscher:innen auch manuell von einer Gruppe oder einem Kanal in eine andere Gruppe oder einen anderen Kanal wechseln und manuell überprüfen, wo Links zu anderen privaten Gruppen oder Kanälen gepostet werden. Dies ist jedoch sehr viel zeitaufwendiger als die Verwendung der Suchfunktion. Darüber hinaus werden Links zu einigen besonders versteckten Gruppen womöglich nie in öffentlichen Bereichen gepostet und bleiben somit unzugänglich.

Ethische Hindernisse

Die Erforschung schädlicher Online-Aktivitäten, insbesondere von gewalttätigen extremistischen Communities, wirft eine Reihe von ethischen Konflikten auf, die sowohl von Forscher:innen und Akademiker:innen als auch von Jurist:innen, Regierungs- und Aufsichtsbehörden ausführlich debattiert werden.[20] Zwar besteht ein öffentliches Interesse daran, die Dynamik der Radikalisierung zu verstehen und die Kommunikation von Communities zu analysieren, die gewalttätige Anschläge planen oder in andere Straftaten involviert sind. Jedoch kann es Forscher:innen schnell in eine schwierige ethische Lage bringen, wenn sie öffentliches Interesse mit den Rechten der Personen abwägen müssen, die Gegenstand der Untersuchung sind.

Derartige Abwägungen erschweren die Erforschung schädlicher Inhalte und Verhaltensweisen in privaten Gruppen auf Telegram erheblich. Schließlich müssen die Nutzer:innen, die dort Informationen austauschen, davon ausgehen

können, dass sie dies ohne externe Beobachtung tun können. Wenn Forscher:innen eine Einverständniserklärung einholen wollen, um die untersuchten Personen und ihr Recht auf Privatsphäre in vollem Umfang zu respektieren, müssen sie in Bezug auf ihre Identität und Ziele transparent sein. Sie müssten alle Gruppenmitglieder bitten, der Anwesenheit bestimmter Forscher:innen im Chat zuzustimmen sowie der möglichen Speicherung und Analyse ihrer Daten und Nachrichten. Es liegt in der Natur der Sache, dass eine solche Zustimmung nicht zu erwarten ist – insbesondere nicht im Fall von extremistischen Online-Chats. Wenn die Mitglieder dieser Gemeinschaften sich der Beobachtung bewusst wären, änderten sie womöglich auch ihr Verhalten und würden potenziell rechtswidrige Inhalte vermeiden, bzw. die Gruppe einfach ganz verlassen. Nutzer:innen von Gruppen mit verschwörungsideologischen Inhalten, die akademische Institutionen und Denkfabriken als Teil einer intellektuellen Intrige der globalen Eliten betrachten, würden einer potenziell kritischen Beobachtung wahrscheinlich nicht zustimmen. Schließlich müssen aber auch die Risiken für die Forscher:innen selbst berücksichtigt werden. Wenn ihre Identität und institutionelle Zugehörigkeit potenziell schädlichen Akteur:innen gegenüber offengelegt werden, könnten sie nicht nur im Internet zur Zielscheibe von Missbrauch, Belästigung oder Doxing werden, sondern müssten auch Übergriffe im wirklichen Leben befürchten.

Wenn Forscher:innen feststellen, dass eine vollständig transparente Durchführung ihrer Arbeit entweder unmöglich oder zu riskant ist, könnten sie entscheiden, dass der Nutzen der Untersuchung einer bestimmten privaten Gruppe die potenziellen Bedenken in Bezug auf das Recht auf Privatsphäre, eine Forschung ohne vorherige Einwilligungserklärung oder bestimmte Formen der Täuschung überwiegen. Dabei sollten Forscher:innen auch die Konsequenzen berücksichtigen, die sich aus der Unterlassung einer Erforschung von potenziell gewalttätigen und schädlichen Gruppen ergeben kann, die wiederum ebenfalls die Rechte anderer verletzen oder Gewalttaten vorbereiten könnte.

Während einige geschlossene Telegram-Gruppen leicht zugänglich und de facto halb-öffentlich sind, zählen andere nur eine Handvoll Mitglieder. Der Beitritt zu diesen Gruppen erfordert üblicherweise die Zustimmung der Admins, die potenzielle neue Mitglieder zusätzlich befragen. Im erstgenannten Fall können die Forscher:innen normalerweise als passive Beobachter:innen agieren und bräuchten keine aktive Täuschung anzuwenden. Andernfalls werden sie wahrscheinlich nach ihren Beweggründen für den Beitritt zur Gruppe gefragt und müssten abwägen, ob eine täuschende Antwort zu diesem Zweck gerechtfertigt ist.

Forschungsmethodik

Um Einladungslinks zu privaten Gruppen und Kanälen zu finden, sind die Forscher:innen des ISD einer Seed-List von öffentlichen Kanälen beigetreten. Diese Liste von 253 deutschsprachigen öffentlichen Kanälen mit rechtsextremen und verschwörungsideologischen Inhalten und Verhaltensweisen wurde während der Arbeit an einem Projekt des ISD über Extremismus in Deutschland zusammengestellt und für dieses Projekt aktualisiert.[21] Es sei darauf hingewiesen, dass dieser Ansatz nur Forscher:innen vorbehalten ist, die Zugang zu bestehenden und aktuellen Listen von Gruppen und Kanälen haben, deren Erstellung und Pflege schwierig sein kann, was ein weiteres Hindernis für die Forschung darstellt.

Die auf diesen Kanälen im Zeitraum vom 1. Januar 2022 bis zum 18. August 2022 veröffentlichten Nachrichten sind erfasst worden. Anschließend wurden die Links automatisch aus den Nachrichten extrahiert. Um potenzielle Einladungslinks zu identifizieren, überprüften die Forscher:innen des ISD manuell Links zur Domain t.me von Telegram – ein gängiges Format für Links, die zu Kanälen, Gruppen und Nachrichten auf Telegram führen. So konnte auch ohne Beitritt zu diesen Gruppen oder Kanälen festgestellt werden, ob der Link aktiv war oder nicht. Weiterhin wurden auf diese Weise die Namen der privaten Gruppen oder Kanäle erfasst, deren Profilbild und Beschreibung (falls vorhanden) sowie jeweils die Anzahl der Mitglieder (bei Gruppen) bzw. Abonnenten (bei Kanälen).

Diese Analyse lieferte im Ergebnis eine Liste von 80 privaten Gruppen und sechs privaten Kanälen. Die Anzahl der Mitglieder oder Abonnent:innen variierte zwischen acht in der kleinsten Gruppe und 12.049 Abonnent:innen im größten Kanal.

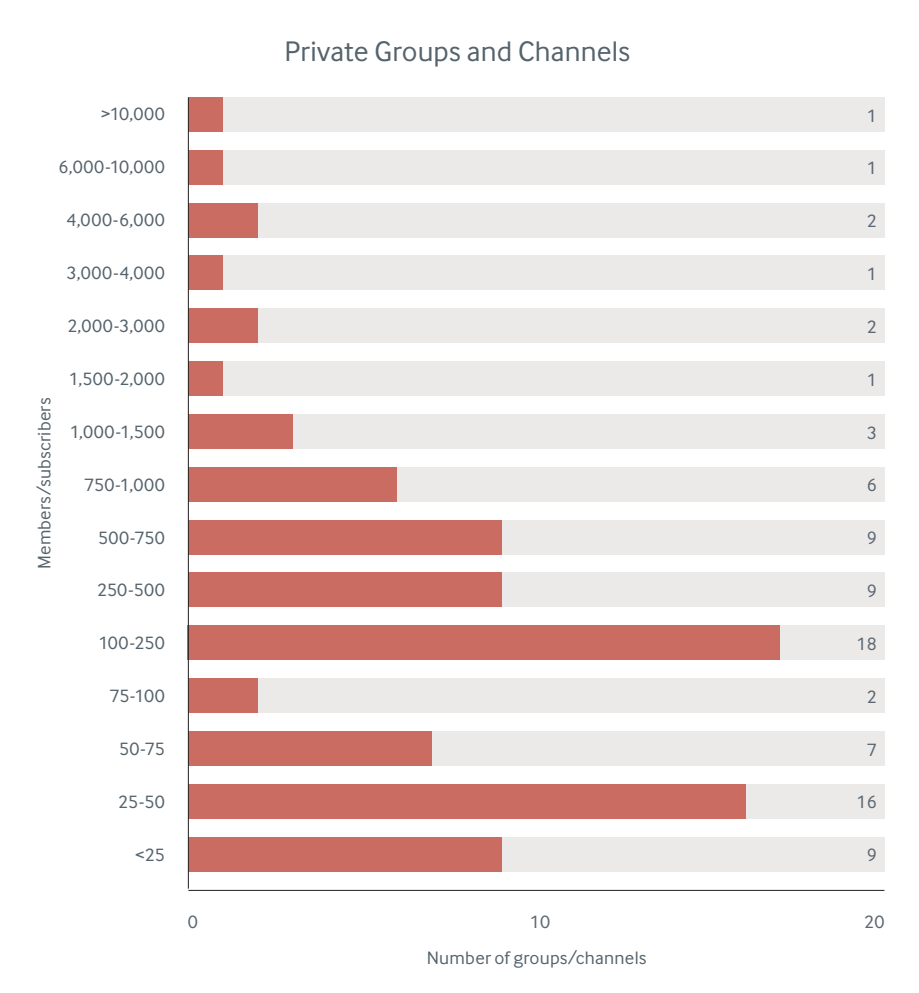


Abbildung 3: Größe der privaten Gruppen und Kanäle in der untersuchten Stichprobe

Während einige Einladungslinks im ursprünglichen Datensatz häufig geteilt wurden, wurden andere nur einmal geteilt und verzeichneten eine geringe Anzahl von Aufrufen. Der am häufigsten geteilte Einladungslink führte zu einer privaten Chatgruppe für die Abonnent:innen eines verschwörungsideologischen Telegram-Kanals. Er wurde 1.843fach geteilt und über 35 Millionen Mal aufgerufen. Diese Gruppe hatte 2.852 Mitglieder und konnte damit kaum als vollkommen privater Kommunikationsraum angesehen werden.

Soweit sich dies aus den Namen und einigen der verfügbaren Beschreibungen ableiten ließ, waren die privaten Gruppen und Kanäle im Datensatz auf folgende Themen spezialisiert:

1. Mobilisierung von Protesten in bestimmten deutschen Regionen und Städten: Während einige Gruppen den Namen des Protests in der Gruppenbeschreibung oder im Gruppennamen aufführten, verwendeten andere allgemeine Phrasen wie „Wir stehen auf" oder bezogen sich auf sogenannte Montagsspaziergänge. Dieser Begriff, der ursprünglich eine Form des demokratischen Protests in der ehemaligen DDR bezeichnete, wurde in jüngster Zeit häufig von rechtsextremen Akteur:innen und Covid-19-Skeptiker:innen gekapert;
2. Debatten über die Covid-19-Pandemie: Aus den Beschreibungen geht hervor, dass diese Gruppen Impfgegner:innen und Menschen zusammenbrachten, die den Corona-Maßnahmen skeptisch gegenüberstanden, wenngleich einige Namen und Beschreibungen eher beschönigende Formulierungen verwendeten und sich auf „gesunde Freidenker" oder den Schutz von Kindern (vermutlich vor Impfungen und anderen Covid-19-Maßnahmen) bezogen;.

3. Regionale Hilfe für Fernfahrer aus Russland: Diese Gruppen wurden nach dem Beginn der russischen Invasion in der Ukraine erstellt. Einladungslinks dazu wurden häufig von öffentlichen Kanälen mit rechtsextremen und verschwörungsideologischen Inhalten und Verhaltensweisen verbreitet;
4. Spezielle Veranstaltungen, bei denen es sich nicht um Proteste handelt (z. B. Treffen), oder kommerzielle esoterische Veranstaltungen (z. B. Seminare zum Thema spirituelles Wachstum);
5. Verschwörungstheorien, einschließlich QAnon;
6. Esoterische Themen, wie etwa alternative Medizin oder spirituelles Wachstum;
7. Regionales Netzwerken ohne jeglichen Bezug zum Diskussionsgegenstand;
8. Andere Themen oder Gruppen mit unklaren Absichten.

Bei der Auswahl der Gruppen und Kanäle, denen wir beitreten wollten, haben wir entweder die beliebtesten mit einer großen Anzahl von Mitgliedern oder Abonnent:innen vorgezogen oder solche, die aufgrund ihrer Namen und Beschreibungen besonders extreme Inhalte und Verhaltensweisen erwarten ließen (einschließlich bekannter extremistischer Gruppen oder solcher, die wahrscheinlich schädliche Verschwörungstheorien verbreiten). Allerdings war es nicht immer möglich, das Thema und das Gefahrenpotenzial der Gruppen oder Kanäle richtig einzuschätzen, ohne ihnen vorher beizutreten. So enthielt unser Datensatz zum Beispiel Links zu einer privaten Gruppe und einem privaten Kanal, die von rechtsextremen Kanälen geteilt wurden und den Anschein erweckten, als hätten sie einen Bezug zu einer Neonazi-Band. Tatsächlich handelte es sich um einen sogenannten Hoax (engl.: Falschmeldung oder Scherz) von antifaschistischen Aktivist:innen, der zeigen sollte, wie rechtsextreme Musik auf Musik-Streaming-Plattformen verbreitet wird.[22] Auf der anderen Seite trug ein weiterer privater Kanal im Datensatz den irreführenden Namen „Tierschutz ist Ehrensache". Da der Link zu diesem Kanal von dem prominenten deutschen Rechtsextremisten und Verschwörungs-Influencer Attila Hildmann geteilt wurde, beschlossen wir, ihm beizutreten. Der Kanal erwies sich tatsächlich als einer von Hildmanns Reservekanälen, die er eingerichtet hatte, um die von Telegram auferlegten Einschränkungen für seine Hauptkanäle zu umgehen.[23]

Beitrittsanforderungen

Für den Beitritt zu mehreren größeren Gruppen mit mehreren hundert Mitgliedern mussten die Forscher:innen lediglich einfache CAPTCHAs lösen (ein Test, um festzustellen, ob die Anfrage durch einen echten Menschen erfolgt), um Nachrichten schreiben zu können.

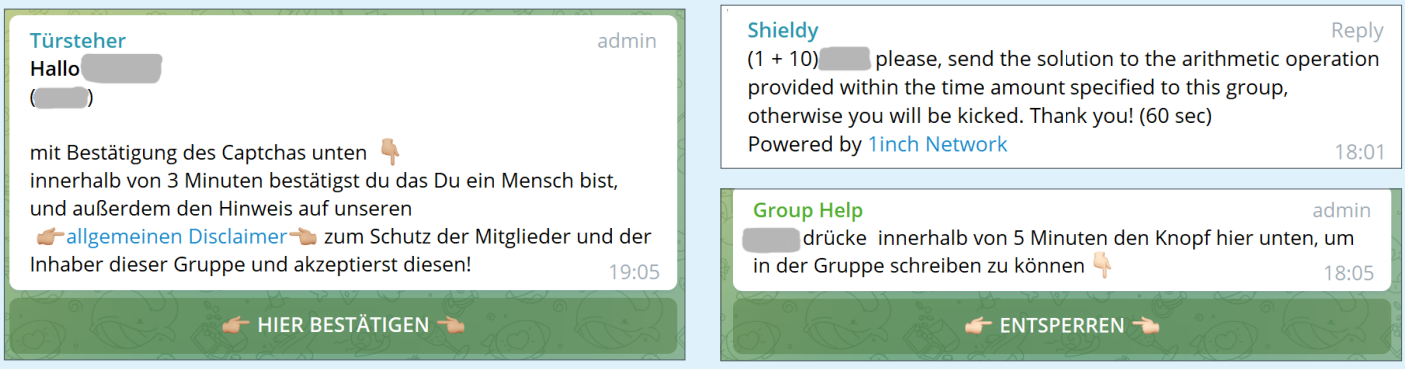


Abbildung 4: CAPTCHAs für den Beitritt zu privaten Gruppen auf Telegram

In einer Gruppe mit über 2.000 Mitgliedern bat ein Bot neue Mitglieder, innerhalb von drei Minuten anzugeben, warum sie der Gruppe beitreten möchten. Zur Auswahl standen folgende Antworten: 1) „Keine Ahnung", 2) „Ist das wichtig?" und 3) „Ich bin neugierig". Nutzer:innen, die die erste oder zweite Option gewählt hatten, wurden automatisch aus der Gruppe ausgeschlossen und konnten ihr nicht mehr beitreten.

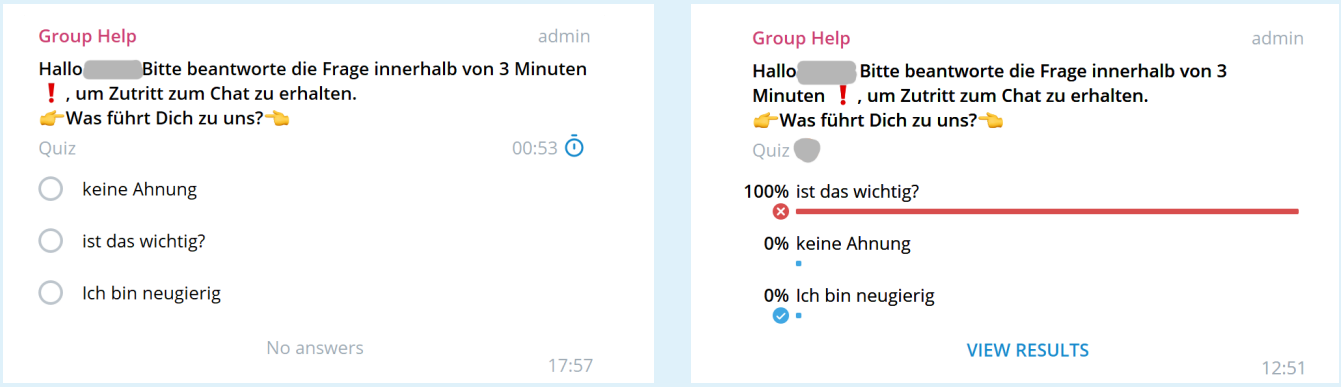


Abbildung 5: Von einem Bot gestellte Fragen als Einstiegshürde für den Beitritt zu einer Telegram-Gruppe

In einer der kleineren geschlossenen Gruppen – einem regionalen Chat mit dem erklärten Ziel, ehemalige Soldat:innen zu vernetzen – wurden neue Mitglieder von einem Bot aufgefordert, sich vorzustellen und einige persönliche Daten anzugeben. Diese regionalen Gruppen waren mit einem öffentlichen Telegram-Kanal für Veteran:innen verbunden, der über 14.000 Abonnent:innen hatte. Auf diesem wurden regelmäßig kremlfreundliche Desinformationen über den Krieg in der Ukraine veröffentlicht, die unter anderem vom russischen Staatssender RT stammten. Hinzu kamen falsche und irreführende Informationen über die Covid-19-Pandemie und Aufrufe zu Protesten gegen die Gesundheitsmaßnahmen sowie die Russland-Sanktionen der Bundesregierung. Der Kanal war mit einer öffentlichen Gruppe mit mehr als 600 Mitgliedern verbunden, die auch als Diskussionsforum für den Kanal fungierte.[i] In dieser öffentlichen Gruppe posteten die Mitglieder Aufrufe zur Gewalt gegen Politiker:innen, zum Waffenkauf sowie zum „Aufstand" gegen die deutsche Regierung anstelle von „sinnlosen Demos". Bemerkenswert ist, dass die Nutzungsbedingungen von Telegram kein ausdrückliches Verbot von Gewaltaufrufen in den Gruppen enthalten, unabhängig davon, ob es sich um öffentliche oder private Gruppen handelt. In den FAQ der Plattform schreibt Telegram auf die Frage, wie sich illegale Inhalte löschen lassen, lediglich Folgendes: „Alle Telegram- und Gruppenchats sind die Privatsache der jeweiligen Nutzer. Wir bearbeiten keine diesbezüglichen Anfragen."[24]

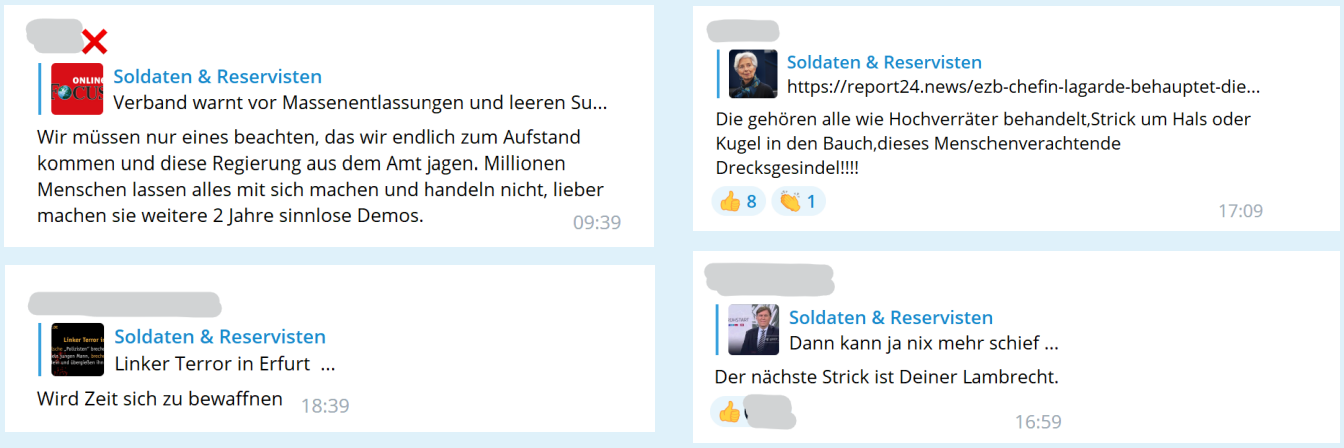


Abbildung 6: Aufrufe zu Gewalt und zum „Aufstand" in einer öffentlichen Gruppe für Veteran:innen

Nachdem sie der öffentlichen Gruppe für Veteran:innen beigetreten waren, konnten die Forscher:innen Einladungslinks zur Vernetzung in regionalen geschlossenen Gruppen sehen, die deutlich kleiner waren (Mitgliederzahlen im September 2022: zwischen sieben und 100). Die Entscheidung, kleinen geschlossenen Gruppen wie diesen beizutreten, birgt ein ethisches Konfliktpotenzial. In diesem Fall befürchteten die Forscher:innen jedoch, dass diese

i Um Kommentare zu Beiträgen in einem Telegram-Kanal zu ermöglichen, müssen die Administrator:innen den Kanal mit einer Gruppe verbinden.

Communities angesichts der Gewaltaufrufe im öffentlichen Chat und der Tatsache, dass die Gruppen und Kanäle auf ehemalige Militärangehörige abzielten, potenziell schädlich und gewalttätig sein könnten. Die Forscher:innen traten einer der regionalen Gruppen bei, in der neue Mitglieder von einem Bot aufgefordert wurden, sich vorzustellen, die ersten Ziffern ihrer Postleitzahl zu nennen und Angaben zu ihrer Dienstzeit beim Militär zu machen. Gemäß den Regeln der Gruppe wären neue Mitglieder, die sich nicht innerhalb von 48 Stunden vorstellten, aus dem Chat geworfen worden. Diese Regeln wurden in der Praxis jedoch nicht streng umgesetzt. Den Forscher:innen gelang es, passiv in der Gruppe zu verweilen, wobei sie keine irreführenden Antworten gaben oder zum Chat beitrugen.

Insgesamt waren die Eintrittsbarrieren für den Beitritt zu großen privaten Gruppen, deren Links öffentlich geteilt wurden, relativ niedrig. Forscher:innen konnten oft Gruppen beitreten und als passive Beobachter:innen in ihnen verweilen, ohne sich aktiver Täuschung zu bedienen. Für die vorliegende Forschungsarbeit haben wir beschlossen, kleineren Gruppen nur dann beizutreten, wenn es überzeugende Hinweise für deren Beteiligung an potenziell gewalttätigen Aktivitäten gab. Ferner verzichteten wir auf die Art der aktiven Täuschung, die erforderlich gewesen wäre, damit die Accounts und Personas der Forscher:innen als zugehörige Insider:innen in den Communities akzeptiert und als solche zu den vertraulicheren Gruppen eingeladen werden konnten. Folglich konnten nur relativ offene Gruppen in unsere Betrachtungen einbezogen werden.

Analyse von Communities auf Telegram: Wichtigste Ergebnisse

Zunächst mussten wir entscheiden, auf welche der privaten Gruppen und Kanäle, die wir durch unsere Link-Analyse erfasst hatten, wir unsere ethnografische Arbeit konzentrieren wollten. Angesichts der Belege für Gewaltaufrufe und rechtswidrige Aktivitäten – insbesondere von deutschsprachigen Gruppen, die mit Rechtsextremismus, Protesten gegen die Corona-Maßnahmen und Verschwörungsideologien in Verbindung gebracht werden können – haben wir uns bei unserer Arbeit auf bekannte extremistische Gruppen und solche Communities konzentriert, die zu Gewalt aufrufen und möglicherweise auch in der realen Welt Proteste und gewalttätige Aktivitäten planen könnten. Insgesamt traten die Forscher:innen 28 privaten Gruppen und zwei privaten Kanälen bei.

Im Beobachtungszeitraum August bis Oktober 2022 gab es in den Gruppen wiederholt Aufrufe zu Protesten oder einem „Generalstreik" gegen alle verbleibenden Maßnahmen des öffentlichen Gesundheitssystems zur Bekämpfung der Covid-19-Pandemie, einschließlich der damit verbundenen Impfungen, und zunehmend auch gegen die steigenden Lebenshaltungskosten und die Sanktionen gegen Russland. Mitglieder dieser Gruppen leiteten häufig Nachrichten von verschwörungsideologischen oder rechtsextremen Kanälen weiter und posteten Links zu alternativen Medien oder russischen Staatsmedien wie RT oder RT DE. Nachdem die EU infolge des Angriffs auf die Ukraine Sanktionen gegen russische Staatsmedien verhängt hatte, gaben Nutzer:innen in den beobachteten Gruppen Tipps zur Umgehung der Sanktionen und posteten Links zu alternativen RT-Domains. Die Mitglieder der Gruppen veröffentlichten zudem Flugblätter über bevorstehende Events sowie Bilder und Videos von Veranstaltungen. Dabei machten sie nicht nur auf Veranstaltungen in ihrer jeweiligen unmittelbaren Nähe aufmerksam, sondern auch in anderen Regionen – vermutlich um das Gefühl der Dringlichkeit zu verstärken und den Eindruck von weit verbreiteten Protesten durch Gleichgesinnte zu erwecken.

Zur Mobilisierung für die Proteste machten sich die Verfasser:innen der Beiträge häufig Ausdrucksformen des antiautoritären Widerstands zu eigen, indem sie erklärten, sie würden für „Freiheit", „Menschenrechte" oder „Frieden" protestieren. Im Gegensatz dazu wurde der deutsche Staat üblicherweise als „Diktatur" oder „Corona-Regime" dargestellt. Mitglieder der Gruppen verbreiteten Falschinformationen, wonach die Regierung plane, die Bundeswehr

Abbildung 7: Handzettel und Fotos von Protesten, die in privaten Gruppen geteilt wurden

gegen Demonstrant:innen einzusetzen oder auf sie zu schießen. Die Bundesregierung wurde zudem so dargestellt, als würde sie von externen Kräften oder einer „globalen Finanzmafia" gesteuert – ein antisemitischer Dog Whistle.

Für eine der privaten Gruppen hat das ISD den gesamten Chatverlauf heruntergeladen, um die Einsatzmöglichkeiten einer automatischen Analyse zu testen. Hierbei handelte es sich um die Telegram-Gruppe einer regionalen extremistischen Gruppierung, die wegen des Verdachts der „verfassungsschutzrelevanten Delegitimierung des Staates" vom Landesamt für Verfassungsschutz Sachsen-Anhalt beobachtet wurde.[25] Dieser neue Phänomenbereich wurde aufgrund der Erfahrungen rund um das Protestgeschehen gegen die Corona-Schutzmaßnahmen eingerichtet, um gegen Akteur:innen vorzugehen, die den Staat und öffentliche Einrichtungen delegitimieren und sabotieren.[26] Nachdem sie der Gruppe beigetreten waren, konnten die Forscher:innen den Chatverlauf ab einem bestimmten Datum (in diesem Fall dem 1. Januar 2022) speichern. Im Zeitraum zwischen dem 1. Januar 2022 und dem 3. Oktober 2022 haben 767 individuelle Nutzer:innen 22.165 Nachrichten in der Gruppe veröffentlicht. Das Nachrichtenaufkommen war von Januar bis März 2022 besonders hoch. In dieser Zeit konzentrierten sich die meisten Nachrichten auf den Widerstand gegen Maßnahmen im Bereich der öffentlichen Gesundheit oder auf den Beginn des russischen Großangriffs auf die gesamte Ukraine. Im Mai und Juni 2022 nahm die Aktivität der Gruppe ab, um dann im Herbst – wenn auch nicht mehr auf das Niveau wie zu Beginn des Jahres – wieder anzusteigen.

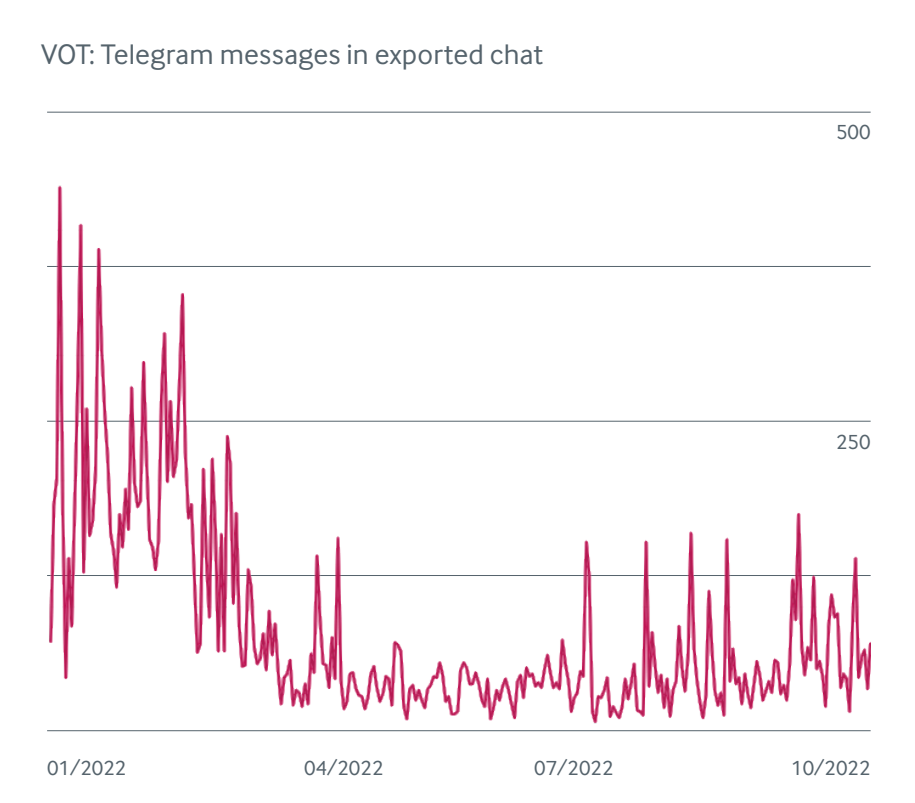


Abbildung 8: Gesamtzahl der Nachrichten im Chatverlauf der Gruppe, deren Daten exportiert wurden

Die Mehrzahl der Nachrichten im Chat wurde von einer kleinen Gruppe hochaktiver Nutzer:innen gepostet. Die 76 aktivsten von ihnen (10 % aller individuellen Nutzer:innen, zu denen solche gezählt wurden, die 90 oder mehr Nachrichten gepostet haben), waren für 78,7 % des gesamten Nachrichtenaufkommens in der Gruppe verantwortlich. Allein die drei aktivsten Nutzer:innen haben jeweils über eintausend Nachrichten gepostet. Im auffälligen Gegensatz dazu hat über die Hälfte aller individuellen Nutzer:innen während des beobachteten Zeitraums nur drei oder weniger Nachrichten gepostet.

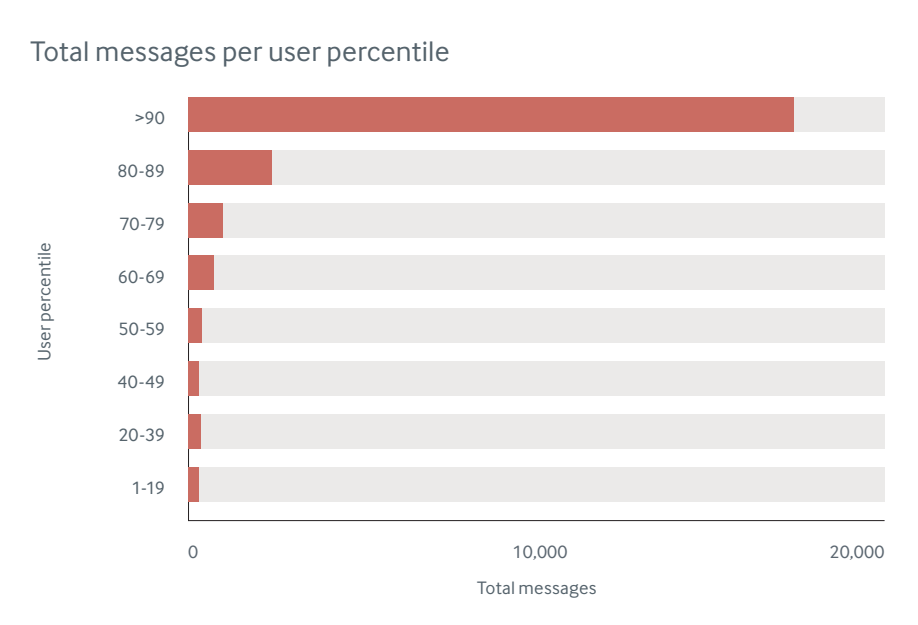


Abbildung 9: Gesamtanzahl der Nachrichten pro User-Quantil

Die Mitglieder der Gruppe veröffentlichten zudem eine beträchtliche Menge an audiovisuellen Inhalten, die sich nur schwer mit automatischen Verfahren auswerten ließen. Insgesamt enthielt der Chatverlauf – beginnend mit der ältesten Nachricht vom 28. April 2020 bis zum 20. Oktober 2022 – 6.428 Bilder, 3.128 Videos, 179 Sprachnachrichten, 85 Audiodateien und 603 sonstige Dateien wie PDFs und Word-Dokumente. Aufgrund der Menge an audiovisuellen Daten war ihre ausführliche Analyse eine große Herausforderung, auch wenn sich diese Arbeit nur auf eine einzige Gruppe bezog.

Ergebnisse und Empfehlungen

Ein umfassendes System zur Inhaltsmoderation fehlt auf der Plattform Telegram weiterhin. Obwohl die Plattform sporadisch rechtswidrige oder gewaltverherrlichende Inhalte entfernt, greifen diese Maßnahmen nach wie vor zu kurz und werden nicht konsequent durchgesetzt. Private Gruppen bieten ein zusätzliches Schlupfloch, um die zwischenzeitlich in Deutschland und anderen Ländern eingeführten gesetzlichen Bestimmungen zur Entfernung rechtswidriger Inhalte auszuhebeln. Inhalte, die in privaten Telegram-Gruppen gepostet werden, können nicht automatisch über externe Suchmaschinen, die Telegram-eigene Suchfunktion oder API gefunden werden. Stattdessen müssen die Gruppen und Kanäle durch eine systematische Analyse der Einladungslinks identifiziert werden, was arbeitsaufwendig und damit kostenintensiv sein kann. Besonders schwierig wird es für Forscher:innen, wenn sie nicht über Listen mit Gruppen verfügen, die mit schädlichen Inhalten und Verhaltensweisen assoziiert sind, bzw. diese nicht beschaffen können.

Forscher:innen müssen privaten Gruppen beitreten, um Zugang zu deren Inhalten zu erhalten. Dabei ergeben sich ethische Konflikte. Um Zugang zu den vertraulichsten und gefährlichsten Gruppen zu erhalten, müssten Forscher:innen eine aktive Täuschung betreiben. Das bedeutet: Um als vertrauenswürdige Mitglieder der Community wahrgenommen zu werden müssten sich sich gruppenkonform verhalten, indem sie Hassrede einsetzen, extreme Nachrichten posten, Abo-Gebühren oder Spenden an schädliche Akteur:innen zahlen . Obwohl diese Methode gelegentlich von investigativen Journalist:innen[27] oder staatlichen Strafverfolgungsbehörden und Nachrichtendiensten angewandt wird, haben wir uns aus ethischen Gründen dagegen entschieden, Extremist:innen zu finanzieren oder aktive Täuschung zu betreiben.[28]

Aufgrund der fragmentierungsbedingten und ethischen Hindernisse beschränkten sich unsere Untersuchungen der Communities mit schädlichen Inhalten und Verhaltensweisen daher auf größere private Gruppen, zu denen Links in öffentlichen Kanälen geteilt wurden. Wir stellten fest, dass einige dieser größeren Communities aufgrund der Zahl ihrer Mitglieder und der Tatsache, dass Einladungslinks aktiv in öffentlichen Kanälen geteilt werden, die Auslegung des Begriffs „privat" weit überstrapazieren. Selbst diese halböffentlichen digitalen Räume wurden für Aufrufe zu Gewalt, Verbreitung von schädlichen Verschwörungstheorien und zur Offline-Mobilisierung genutzt.

Die Tatsache, dass die Nutzungsbedingungen von Telegram nur für öffentliche, nicht aber für private Gruppen (die bis zu 200.000 Mitglieder haben können), noch für private Kanäle gelten, macht diese Räume zu einem attraktiven Online-Umfeld für Akteur:innen, die zu Gewalt aufrufen, Falschinformationen verbreiten oder Gemeinschaften für Offline-Aktionen mobilisieren möchten.

Um diese Schwachpunkte zu beheben, sollte Telegram einen angemessenen Grenzwert festlegen für die Anzahl der Nutzer:innen , die in privaten Gruppen und Kanälen teilnehmen. Online-Bereiche mit einem großen Nutzerkreis sollten ab einem bestimmten Schwellenwert als öffentlich deklariert werden, sodass sie den Nutzungsbedingungen von Telegram unterliegen. Telegram sollte sich zudem verpflichten, diese Bedingungen konsequenter und wirksamer durchzusetzen, um die Menge an rechtswidrigen oder schädlichen Inhalten, Verhaltensweisen und Communities auf der Plattform zu begrenzen. Schließlich müsste Telegram dafür sorgen, dass Forscher:innen auf diese öffentlichen Online-Räume zugreifen und Daten abrufen können, während der Schutz der Privatsphäre und der Datenschutz durch angemessene Vorkehrungen gewährleistet blieben.

Fallstudie 2: **Discord**

Wichtigste Ergebnisse

- Discord stellt Forscher:innen vor ähnliche Herausforderungen wie Telegram. Um auf Inhalte zugreifen zu können, ist der Beitritt zu einer Community oder einem Server erforderlich. Dies stellt ein Hindernis für die systematische Forschungsarbeit dar und birgt potenzielle ethische und rechtliche Bedenken im Zusammenhang mit täuschendem Verhalten und der Datennutzung.
- Auch bei Discord gibt es ähnliche Probleme in der Abgrenzung zwischen öffentlichen und privaten Bereichen. Darüber hinaus weisen die Tagging- und Suchfunktionen von Discord, die den Nutzer:innen helfen sollen, die Server zu finden, die ihren Interessen entsprechen, verschiedene Defizite auf und liefern im Vergleich zu Alternativen von Drittanbietern inkonsistente Ergebnisse. Auf den Servern findet man oft sowohl schädliche als auch unauffällige Inhalte und soziale Verhaltensweisen, was das Auffinden von relevantem Material noch schwieriger macht.
- Dennoch konnten wir eine eingeschränkte Untersuchung von zwei verschiedenen religiös-extremistischen Communities durchführen, in denen jeweils katholisch- bzw. islamistisch-extremistische Inhalte und Verhaltensweisen festgestellt wurden. In beiden Gruppen beobachteten wir vergleichbare schädliche Inhalte, darunter Hassrede gegen Angehörige der LGBTQ-Gemeinschaft, Antisemitismus und Aufrufe zur Bildung religiös-fundamentalistischer Staaten.

In dieser Fallstudie untersuchten Forscher:innen des ISD englischsprachige Online-Communities auf Discord, in denen jeweils katholisch- bzw. islamistisch-extremistische Inhalte und Verhaltensweisen festgestellt wurden. Auf Discord bestehen Forschungshindernisse in erster Linie aufgrund einer ausgeprägten Fragmentierung. Zur Überwindung dieser Hindernisse wählten die Forscher:innen zwei verschiedene methodische Ansätze: 1) systematischer Zugriff auf Daten mit Beschränkung auf untersuchungsrelevante Server und 2) ethnografische Forschungsmethoden.

Auf Discord bestehen in zweifacher Hinsicht Hindernisse durch Fragmentierung. Erstens ist das Durchsuchen und Herunterladen von Nachrichten über die Discord-API zwar technisch möglich, aber nur auf der Ebene der einzelnen Server. Das bedeutet, dass Forscher:innen einerseits wissen müssen, wo sie nach schädlichen Inhalten suchen müssen, und dass sie andererseits Mitglied der betreffenden Server sein müssen. Zweitens wird die Suche nach relevanten Inhalten oder Communities durch die begrenzten und intransparenten Suchfunktionen der Plattform und der Software von Drittanbietern erschwert.

Neben den Hindernissen, die die Fragmentierung von Discord mit sich bringt, stellt die Plattform Forscher:innen auch vor erhebliche rechtliche und ethische Hindernisse. Da die Nutzungsbedingungen von Discord die Erfassung von Nutzerdaten über die plattformeigene API untersagen, würde jede Zuwiderhandlung gegen das Vertragsrecht verstoßen und das Risiko möglicher rechtlicher Schritte seitens der Plattform nach sich ziehen. In diesem Moment ist es unerheblich, ob ethische Bedenken gegen die Erfassung solcher Daten bestehen oder nicht, da bereits die rechtlichen Risiken dem Einsatz systematischer Suchmethoden zur Überwindung der Fragmentierung entgegenstehen. Umgekehrt wirken sich ethische Hindernisse auf den Einsatz qualitativer Methoden zur Untersuchung von Communities mit schädlichen Inhalten und Verhaltensweisen auf Discord aus, auch wenn dieser rechtlich zulässig ist. Die Fragen, die in der Regel in Form von Formularen beantwortet werden müssen, um Gruppen beitreten zu können, können die Forscher:innen dazu zwingen, täuschende Angaben zu machen. Schlimmstenfalls müssen sie sich als Unterstützer:innen problematischer Überzeugungen ausgeben. Dies ist insbesondere bei kleineren Servern der Fall, da nicht klar ist, wo die Schwelle für „berechtigte Erwartungen" in Bezug auf die Privatsphäre liegt.

Diese Hindernisse schränken den Spielraum und die Ergebnisse unserer Forschungsarbeit insofern ein, als dass sie sich hauptsächlich auf qualitative und nicht systematisierte Analysen von Inhalten und Verhaltensweisen auf Servern stützt, von denen wir aus ethischen Gründen nicht von vornherein ausgeschlossen waren. Gleichwohl zeigen diese Ergebnisse, dass hetzerische, antidemokratische und gewalttätige Inhalte in diesen Communities weit verbreitet sind.

In den folgenden Abschnitten gehen wir auf die Hintergründe und Funktionsweise von Discord ein und beschreiben die identifizierten und angewendeten Forschungsansätze sowie die in der Praxis aufgetretene Forschungshindernisse. Abschließend stellen wir die Ergebnisse unserer Analyse vor.

Überblick über die Plattform

Discord wurde 2015 als kostenlose Plattform für Video-Gaming ins Leben gerufen und sollte Nutzer:innen ermöglichen, beim Spielen miteinander zu kommunizieren. Seitdem hat sich die Zahl der Nutzer:innen von Discord weltweit dramatisch vergrößert; sie wird derzeit auf 6,7 Millionen aktive Server und 140 Millionen monatlich aktive Nutzer:innen geschätzt.[29]

Wichtige Funktionen

Mit Discord können Nutzer:innen in Echtzeit über Text-, Sprach- und Videochats miteinander kommunizieren. Chat-Räume, die als Server bezeichnet werden, können von allen Nutzer:innen erstellt werden. Der Zweck des Servers muss keinen Bezug zum Gaming haben. Server können auch für das Networking, die Organisation von Events und Wettkämpfen, thematische Diskussionen und das Zusammentragen und Teilen von Inhalten genutzt werden, die für die Mitglieder des jeweiligen Servers von Interesse sind. Die Server können auch für sogenannte Überfälle (Raids) eingesetzt werden. Dabei handelt es sich um organisierte Kampagnen, die das Spamming oder Trolling anderer Server oder Nutzer:innen auf anderen Plattformen beinhalten.

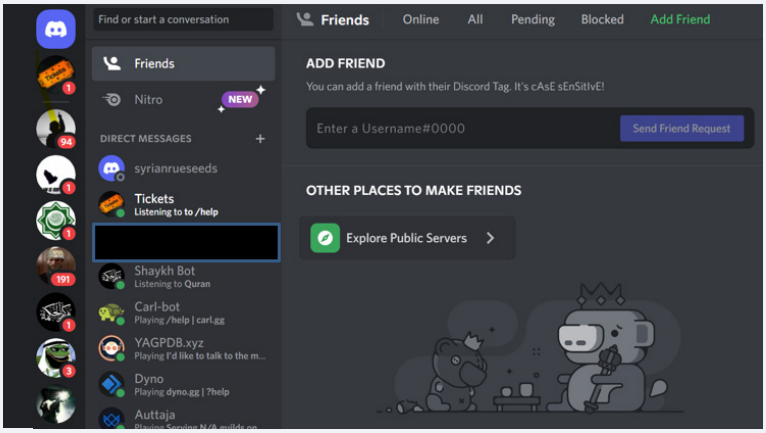


Abbildung 10: Benutzeroberfläche von Discord

Viele dieser Server sind privat. Daneben gibt es auch öffentliche Server, für deren Beitritt jedoch ein Anmeldename (username) erforderlich ist. Die größten öffentlichen Server können Hunderttausende von Mitgliedern haben.[30] Während sich viele öffentliche Server mit Gaming oder Anime befassen, dienen andere zur Diskussion über soziale oder politische Themen, wobei teilweise explizit Themen und Aspekte diskutiert und aufgegriffen werden, die denen anderer Plattformen wie 4chan ähneln.[31]

Schädliche Aktivitäten auf Discord

Obwohl sich Discord in erster Linie an die Gaming-Community richtet und für nichtpolitische Zwecke konzipiert ist, haben Forscher:innen belegt, dass die App inzwischen auch von verschiedenen extremistischen Gruppen genutzt wird. Im Vorfeld der Kundgebung weißer Rassist:innen in Charlottesville im US-Bundesstaat Virginia, bei der ein rechtsextremer Aktivist im August 2017 eine Gegendemonstrantin ermordete, als er absichtlich mit einem Auto in eine Menschenmenge fuhr, nutzten die Organisator:innen Discord, um den Protest zu planen und zu koordinieren sowie um ideologisches Propagandamaterial auszutauschen.[32]

Nach Berichten über die Verwendung von Discord durch Rechtsextremist:innen und insbesondere nach den Ereignissen in Charlottesville begann Discord, die Präsenz dieser Gruppierungen auf seiner Plattform strenger zu

ahnden.[33] 2021 erklärte Discord, mehr als 2.000 extremistische Server entfernt zu haben.[34] Allerdings ergab eine Untersuchung des ISD später im selben Jahr, dass Discord nach wie vor als Anlaufstelle für den Aufbau rechtsextremer Communities genutzt wird. Dabei ist unklar, inwieweit das Thema Gaming selbst eine Rolle bei ernstzunehmenden Strategien zur Radikalisierung und Rekrutierung neuer Einzelpersonen auf der Plattform spielte.[35] Bei Untersuchungen wurden auf Servern von Discord außerdem Unterstützungsbekundungen für die rechtsextremen Gruppierungen „Atomwaffen Division" und „Sonnenkrieg Division" gefunden, die beide in Großbritannien, Kanada und Australien als terroristische Organisationen eingestuft werden.[36]

Zwar scheint Discord bei Rechtsextremist:innen besonders beliebt zu sein, jedoch wird Discord auch von Mitgliedern einer jüngeren Gemeinschaft islamistischer Extremist:innen der Generation Z genutzt, die salafistische Überzeugungen[ii] mit rechtsextremen Motiven und Gaming-Subkulturen vermischen.[37] Die Bedeutung von Discord für eine Reihe von Online-Subkulturen, die durch Extremismus und Gewalt auffallen, wurde 2022 durch den Anschlag in Buffalo im US-Bundesstaat New York und den Amoklauf bei der Highland Park Parade in der gleichnamigen US-amerikanischen Kleinstadt noch deutlicher. In beiden Fällen fanden sich im digitalen Fußabdruck der Angreifer Nachrichten, die sie auf Discord hinterlassen hatten, darunter auch Inhalte, die die Planung und Vorbereitung ihrer Angriffe dokumentierten.[38]

Untersuchungen auf Discord

Forschungsmethodik

Discord stellt die Forscher:innen vor allem bei der Analyse privater Gruppen mit quantitativen und qualitativen Methoden sowohl vor rechtliche als auch vor ethische Hindernisse. Zusätzlich wird die Untersuchung sowohl von öffentlichen als auch von privaten Gruppen durch eine ausgeprägte Fragmentierung in der Form behindert, als dass die Untersuchung auf der Plattform nur serverweise und nicht global bzw. systematisch erfolgen kann. Zur Überwindung dieser Hindernisse wählten die Forscher:innen zwei verschiedene methodische Ansätze: 1) systematischer Zugriff auf Daten mit Beschränkung auf untersuchungsrelevante Server und 2) ethnografische Forschungsmethoden.

Wie bereits erwähnt, ergab eine frühere Untersuchung des ISD zur Plattform Discord, dass sowohl islamistische Extremist:innen als auch Rechtsextremist:innen auf der Plattform präsent sind. Die Forscher:innen des ISD zogen in Erwägung, eine umfassende Analyse rechtsextremer Gruppen zum Gegenstand dieses Projekts durchzuführen, da frühere Forschungen zu Discord auf eine signifikante rechtsextreme Präsenz auf der Plattform hindeuteten. Es wurde jedoch entschieden, dass eine engere und gezieltere Untersuchung spezifischer Untergemeinschaften innerhalb der rechtsextremen Szene mehr zu den laufenden Forschungsarbeiten beitragen könnte, die darauf abzielen, die Vielfalt extremistischer Communities und Radikalisierungsdynamiken auf Discord zu verstehen. Angesichts der Hinweise auf ein wachsendes Interesse US-amerikanischer Rechtsextremist:innen an Konzepten wie dem katholischen Integralismus und dem Traditionalismus – auch unter den Anhängern der rechtsextremen America-First- und Groyper-Bewegungen, die sich auf Discord mobilisiert haben[39] – beschloss das ISD, sich auf Hass- und Gewaltinhalte auf Servern zu konzentrieren, die mit katholischen integralistischen und traditionalistischen Inhalten und Verhaltensweisen assoziiert waren.[iii] Darüber

ii Der Salafismus ist eine Form des sunnitischen Islams, deren Anhänger:innen für eine Rückkehr zu den Praktiken der ersten drei Generationen von Muslim:innen (die Salaf, deutsch „die Altvorderen") eintreten, die unmittelbar nach dem Propheten Mohammed lebten. Innerhalb des Salafismus gibt es verschiedene Strömungen, die sich in ihrer Auslegung der heiligen Schriften des Islams und deren Bedeutung für das politische Handeln deutlich unterscheiden. Salafist:innen werden oft untergliedert in quietistische Salafist:innen, die politischen Aktivismus ablehnen, politische Salafist:innen, die sich aktiv für die Umgestaltung der Gesellschaft nach ihren ideologischen Vorstellungen einsetzen, und Salafi-Dschihadist:innen, die Gewalt als legitimes Mittel zur Durchsetzung ihrer Auffassung des islamischen Glaubens ansehen.

iii Der katholische Integralismus ist eine Strömung innerhalb des Katholizismus, deren Anhänger:innen die Trennung zwischen weltlicher und religiöser Macht ablehnen. Da deren übergeordnete religiöse Ziele für wichtiger gehalten werden als „zeitliche", vertreten Integralist:innen die Ansicht, dass die Lehren der Kirche eine am Gemeinwohl orientierte Politik bestimmen sollten. Zwar ist der katholische Integralismus kein neuer Trend, allerdings haben diese Ansichten in den letzten Jahren in englischsprachigen rechtsextremen (Online-)Gemeinschaften an Boden gewonnen. Es gibt einige Überschneidungen mit katholischen Traditionalist:innen, die die teilweise Öffnung der katholische Kirche zur Moderne nach dem Zweiten Vatikanischen Konzil zwischen 1962 und 1965 nicht akzeptieren. Die größten Diskrepanzen gibt es seitdem bei Themen wie Religionsfreiheit, Geschlechterrollen und Menschenrechte sowie in Bezug auf liturgische Auffassungen, wobei einige Traditionalist:innen auch die Legitimität der nachfolgenden Päpste und/oder ihrer Lehren nicht länger anerkennen. So erklären die Sedevakantist:innen, dass das Amt des Papstes seit dem Zweiten Vatikanischen Konzil nicht mehr besetzt sei, während der Sedeprivationismus davon ausgeht, dass der Papst zwar rechtmäßig gewählt wurde, aber aufgrund von doktrinären Fehlern keine Autorität beanspruchen kann. Aufgrund ihrer antisäkularen, antiliberalen und antipluralistischen Ausrichtung sowie ihrer Ablehnung der Reformen des Zweiten Vatikanischen Konzils kann es zu gewissen Überschneidungen zwischen den unterschiedlichen Strömungen des Sedevakantismus und des Integralismus kommen. Katholische integralistische Ansichten werden nicht nur auf Discord, sondern auch auf vielen anderen Plattformen verbreitet.

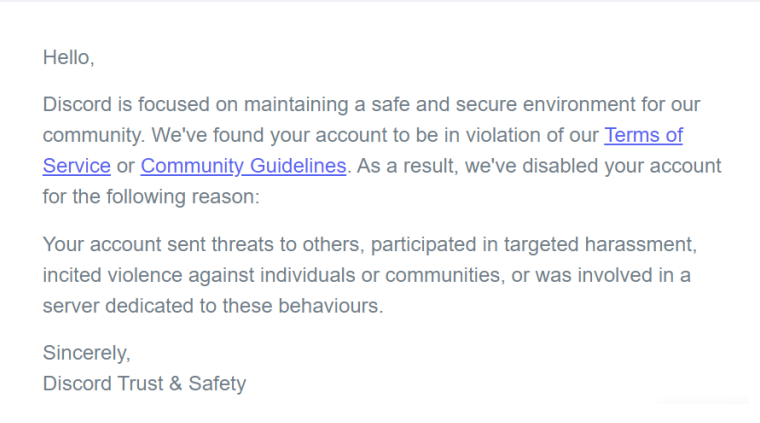
hinaus wurden auch islamistisch-extremistische Communities auf Discord untersucht. An diesen Beispielen ist die Eignung der Methoden für den Zugriff auf Daten von zuvor identifizierten Communities mit schädlichen Inhalten und Verhaltensweisen untersucht worden. Die dabei aufgetretenen Forschungshindernisse wurden ebenfalls dokumentiert.

Die Identifizierung von Servern, die mit katholischem und islamistischem Extremismus assoziiert sind, erfolgte in zwei Schritten. Zunächst erstellten die Forscher:innen Listen mit Schlüsselwörtern (keywords), die mit katholischem und islamistischem Extremismus im Internet in Verbindung gebracht werden. Dazu nutzten sie die Suchfunktionen von Discord und das Open-Source-Tool Disboard, das unabhängig von Discord ist, aber Nutzern:innen hilft, Server zu finden.[40] Die Auswahl der Schlüsselwörter für diese Listen erfolgte auf der Grundlage zuvor abgeschlossener Forschungsarbeiten des ISD über islamistischen Extremismus, nach Auswertung der vorhandenen Veröffentlichungen und Berichte über katholischen Extremismus in englischsprachigen Ländern.

Aufbauend auf dem ersten Schritt führten die Forscher:innen eine manuelle Suche auf der Plattform nach dem Schneeballprinzip durch, indem sie ausgehend von den ersten Fällen neue Fälle identifizierten und untersuchten. Dabei zielten sie auf Server – insbesondere auf sogenannten Partnerserver (partnership servers) – ab, die in extremistischen Kreisen empfohlen wurden. In „Partnerschafts-Chats" innerhalb von Servern werden gleichgesinnte Server aufgelistet, die sich gegenseitig bei ihren Mitgliedern empfehlen, wobei man von einem gegenseitigen Interesse ausgeht. Die Beschreibungen der Partnerserver sind in der Regel sehr viel umfangreicher als die Beschreibungen innerhalb von Disboard und erlauben es den Forschenden zumeist, aussagekräftige Rückschlüsse auf den wahrscheinlichen ideologischen Hintergrund zu ziehen.

Mit dieser Vorgehensweise konnten 31 katholisch-extremistische und 16 islamistisch-extremistische Server identifiziert werden. Um die Ideologie der Server zu klassifizieren, bewerteten die Forscher:innen des ISD deren Namen, Tags auf Disboard und/oder Beschreibungen. Oft gibt es innerhalb eines Servers keine einheitliche Ideologie, sondern eine Mischung aus verschiedenen Stimmen, die erhebliche Meinungsverschiedenheiten austragen, aber auch über andere, harmlosere Themen diskutieren. Aus diesem Grund ist es treffender, die Mehrheit der von uns untersuchten Server nicht per se als „extremistische Server", sondern als Communities zu bezeichnen, in denen extremistische Stimmen präsent sind.

Für die vorliegende Fallstudie wurden zwei Accounts erstellt. Damit sollte vermieden werden, dass den Nutzer:innen der untersuchten Server Ungereimtheiten bezüglich der Forschungsaccounts auffallen. Da diese einsehen können, bei wie vielen (und welchen) anderen Servern ein Account Mitglied ist, könnten Forscher:innen, die bereits in der katholisch-extremistischen Community vertreten sind, Verdacht erregen, wenn sie Servern mit islamistisch-extremistischen Inhalten und Verhaltensweisen beitreten.


Hello,

Discord is focused on maintaining a safe and secure environment for our community. We've found your account to be in violation of our Terms of Service or Community Guidelines. As a result, we've disabled your account for the following reason:

Your account sent threats to others, participated in targeted harassment, incited violence against individuals or communities, or was involved in a server dedicated to these behaviours.

Sincerely,
Discord Trust & Safety

Abbildung 11: Benachrichtigung von Discord über die Entfernung des vom ISD für Forschungszwecke eingerichteten Accounts

Dazu ist anzumerken, dass der von uns zur Untersuchung katholisch-extremistischer Communities auf Discord erstellte Account zwei Monate nach dem Beitritt zu den identifizierten Servern gesperrt wurde. Als Begründung

erklärte Discord, der Account habe „gegen die Nutzungsbedingungen oder Community-Richtlinien der Plattform verstoßen". Wenngleich kein konkreter Grund angegeben wurde, geht aus der Liste der Verhaltensweisen hervor, dass die Sperrung darauf zurückzuführen ist, dass andere Mitglieder der betreffenden Server Drohungen verschickt haben, an gezielten Anfeindungen beteiligt waren oder zu Gewalt aufgerufen haben. Allerdings hätten zahlreiche der im Rahmen der vorliegenden Arbeit untersuchten Server einen oder mehreren dieser Beschreibungen entsprochen. Insofern ist es bedauerlich, dass keine Informationen darüber bereitgestellt wurden, welcher Server zu dieser Entscheidung geführt hat und ob der Server selbst gelöscht wurde. Mehrere der 31 Server mit katholisch-extremistischen Communities, denen die Forscher:innen des ISD beigetreten waren, waren zum Zeitpunkt des Abschlusses der Datenerfassung nicht mehr über die Suchfunktion von Discord oder das Disboard verfügbar. Dabei blieb unklar, ob sie vom Plattformbetreiber entfernt wurden.

Da Discord über eine öffentlich zugängliche API verfügt, prüften wir die Möglichkeit, für weitere Analysen systematisch auf die Daten der Server zuzugreifen, die wir durch die oben beschriebenen Schritte als untersuchungswürdig identifiziert hatten. In den folgenden Abschnitten werden die fragmentierungsbedingten sowie die rechtlichen und ethischen Hindernisse beschrieben, auf die wir bei unserer Arbeit gestoßen sind.

Hindernisse durch Fragmentierung
Auf Reddit, Facebook und anderen Plattformen kann über die API auf Chats in öffentlichen Gruppen zugegriffen werden. Dadurch können Forschende schnell Erwähnungen relevanter Stichwörter in einer Vielzahl von öffentlichen Gruppen finden. Ähnlich weitreichende Funktionen sind über die API von Discord leider nicht verfügbar. Das Suchen und Herunterladen von Nachrichten über die API von Discord ist zwar möglich, jedoch nur indivduell Server für Server. Einige Nutzer:innen konnten diese Funktion zwar automatisieren, um sie im größeren Maßstab anzuwenden.[41] Es scheint jedoch, dass die Forscher:innen die zu durchsuchenden Kanäle im Voraus festlegen müssen. Angesichts der riesigen Vielfalt der Kanäle auf Discord und der Tatsache, dass Kanäle, die schädliche Inhalte oder Verhaltensweisen enthalten, manchmal gelöscht und/oder umbenannt werden, kann eine systematische Suche sehr schwierig sein. Es geht also keineswegs darum, dass die relevanten Informationen versteckt wären. Sie wären sogar leicht zu finden – allerdings müssten Forscher:innen im Voraus wissen, wo sie danach suchen müssen. Diese Forschungshindernisse auf Discord sind daher auf die ausgeprägte Fragmentierung der Daten zurückzuführen.

Darüber hinaus ist nicht transparent, wie die Suchfunktionen von Discord oder Disboard funktionieren, wie ihre Suchergebnisse ermittelt werden, wie umfassend diese sind und welche Ergebnisse fehlen (siehe Erläuterung unten). Disboard gruppiert die Server zudem nach Tags, die einen Hinweis darauf geben, welche von ihnen für schädliche Ideologien relevant sein könnten (z. B. IS, Dschihad, Taliban, Kalifat, Salafisten). Die einzelnen Servernamen und -beschreibungen wurden manuell überprüft, um festzustellen, ob sie für dieses Projekt relevant sein könnten.

Zwei Faktoren weisen darauf hin, dass weder die Suchfunktionen von Discord noch die von Disboard vollumfängliche Ergebnisse liefern. Erstens gibt es große Unterschiede zwischen den jeweils gelieferten Ergebnissen, wobei Disboard in der Regel eine sehr viel höhere Anzahl von Suchtreffern anzeigt. Zweitens gibt es auch bei den Ergebnissen von Disboard oft unerklärliche Abweichungen zwischen der Anzahl der vermeintlich identifizierten und der tatsächlich angezeigten Server. Es ist daher nicht auszuschließen, dass die Suchfunktionen Defizite aufweisen, welche die Genauigkeit der von ihnen gelieferten Daten beeinträchtigen und damit unsere Ergebnisse möglicherweise verzerren.

Ethische und rechtliche Hindernisse
Die Forschungsarbeit auf Discord bringt verschiedene ethische und rechtliche Hindernisse mit sich. Dabei könnten die spezifischen ethischen Hindernisse, auf die wir bei der Erforschung von Discord gestoßen sind, auch auf einer Plattform ohne dieselben rechtlichen Hindernisse bestehen, und umgekehrt.

Ethische Hindernisse

Ähnlich wie bei Telegram ist es auch auf Discord üblich, Mitglieder, die einer speziellen Community beitreten wollen, anhand von Online-Beitrittsformularen zu überprüfen. Um diese Hürde zu bewältigen, können Forscher:innen sich

daher gezwungen sehen, bei der Beantwortung der Fragen falsche Angaben zu machen. Täuschende Antworten auf solche Kontrollfragen sind vor allem bei kleineren Servern problematisch, bei denen die Nutzer:innen „berechtigte Erwartungen" an den Schutz ihrer Privatsphäre als betroffene Personen haben können.

Bei der Einrichtung von Accounts zu Forschungszwecken und bei der anschließenden ethnografischen Forschung ist das ISD stets darauf bedacht, täuschende Verhaltensweisen zu minimieren. Profilbilder oder Informationen über das Geschlecht oder die persönlichen Interessen werden nur dann bereitgestellt, wenn dies im Einzelfall nachweislich notwendig ist. Außerdem müssen die Account-Namen Pseudonyme sein. Dies dient neben dem Schutz der Forscher:innen auch dem Schutz Dritter. Anhand der für die Accounts verwendeten Pseudonyme oder sonstigen Informationen, die nach den obigen Grundsätzen bereitgestellt werden, sollte es nicht möglich sein, real existierende Personen zu identifizieren.

Wenn Nutzer:innen die Verifizierung für deren Beitritt nicht bestehen, verbleiben sie in einem Wartebereich. Der Umfang der Informationen über den Server, die bereits im Wartebereich sichtbar sind, ist sehr unterschiedlich. Auf den meisten Servern gibt es ein Formular zur Verifizierung neuer Nutzer:innen. Lediglich acht der 47 von uns untersuchten Server verwendeten keinen Verifizierungsprozess. Die Beitrittsformulare enthalten in der Regel etwa ein halbes Dutzend an Fragen. Nach Auswertung dieser Formulare hat das ISD sie in verschiedenen Kategorien zusammengefasst, die ausdrücken, welcher Grad an Täuschung und Ideologie für deren Beantwortung jeweils nötig ist.

- **Stufe 1**: Fragen, die keine Informationen über die politischen und/oder religiösen Ansichten der Nutzer:innen erfordern.
- **Stufe 2**: Fragen nach wenig konfliktbehafteten Angaben zur Identität der Nutzer:innen (z. B. „Was ist Ihre Religion?" oder „Auf welchem Kontinent leben Sie?").
- **Stufe 3**: Fragen, die sich nach der Identität der Nutzer:innen erkundigen und zusätzlich Antworten einfordern, die näher auf ihre religiösen, politischen oder ideologischen Einstellungen eingehen (z. B. „Bitte schildern Sie Ihre politischen Ansichten." oder „Üben Sie Ihre Religion aktiv aus?").
- **Stufe 4**: Spezifische und konfliktbehaftete Fragen zur Identität der Nutzer:innen, die Antworten zur Bestätigung religiöser, politischer oder ideologischer Übereinstimmung erfordern (z. B. „Befürworten Sie Selbstmordattentate?" oder „Stimmen Sie zu, dass jegliche Sünde und Entartung zu verabscheuen ist?").

Die Forscher:innen des ISD beantworteten im Allgemeinen Fragen, die in die Kategorien 1 oder 2 fielen (21 Server). Bis auf eine Ausnahme konnte das ISD auf diese Weise allen ausgewählten Servern beitreten. In dem einen Fall, in dem den Forscher:innen kein Zugang gewährt wurde, stellten die Admins des Servers weitere Fragen zu politischen und religiösen Überzeugungen, deren Beantwortung ein unvertretbares Maß an Täuschung erfordert hätte.
Ein damit verbundenes ethisches Problem ist, dass Nutzer:innen in diesen Befragungen oft nach ihrer Zustimmung zu den Regeln des Servers befragt werden. Die Regeln selbst können höchst problematisch sein, beispielsweise wenn sie bestimmte Religionen oder politische Bewegungen ausgrenzen oder die Geschlechtertrennung befürworten. Wenn die Befragten diesen Regeln zustimmen, kann dies als Befürwortung aufgefasst werden.

Ein weiteres ethisches Grundproblem, das sich bei kleineren Servern stellt, ist die Frage, wo die Schwelle für „berechtigte Erwartungen" (reasonable expectations) an den Datenschutz beginnt. Dieses Problem stellt sich nicht nur in Bezug auf Discord: WhatsApp-Gruppen sind auf 256 Mitglieder beschränkt. Signal erlaubt sichere Messaging-Gruppen mit bis zu zehn Mitgliedern und Gruppen mit bis zu tausend Mitgliedern. Facebook-Profile können bis zu 5.000 Freunde haben. Diese Online-Umgebungen können alle als privat betrachtet werden (vorausgesetzt, dass im Falle von Facebook entsprechende Einstellungen gewählt wurden). Dies verdeutlicht, dass die Grenze zwischen öffentlichen und privaten Räumen unscharf sein kann, da es keinen einheitlichen numerischen Schwellenwert gibt, ab dem ein privater Raum zu einem öffentlichen Raum wird. Die Größe der Server auf Discord variiert erheblich, wobei die größten Server mit nicht-politischen Inhalten Hunderttausende von Mitgliedern haben. Häufiger sind jedoch kleinere Server

mit Hunderten oder Tausenden von Mitgliedern. Bei den meisten Server, die das ISD untersucht hat, mit religiös-extremistischen Inhalten und Verhaltensweisen, bewegten sich die Mitgliedzahlen im zwei- bis dreistelligen Bereich. Folglich gibt es zwar keine objektive Norm für die Unterscheidung zwischen eindeutig privaten und öffentlichen Kommunikationskanälen anhand der Anzahl der Nutzer:innen oder Mitglieder. Es ist jedoch unverkennbar, dass viele der extremistischen Communities auf Discord in einer Grauzone agieren, wenn es darum geht, wann ein Online-Raum nach vernünftigem Ermessen als privat angesehen werden kann.

Rechtliche Hindernisse

Der API-Client von Discord ermöglicht es Nutzern:innen, sich mit einem Server zu verbinden und auf diesem Kanal nicht nur Nachrichten in Echtzeit zu erfassen, sondern auch frühere Nachrichten aus dem Verlauf. Um sich mit einem Server zu verbinden, müssen sich die Forscher:innen über eine von zwei Optionen identifizieren. Die erste Möglichkeit ist ein sogenannter Bot-Account, der manuell von einem Admin (beispielsweise dem Ersteller des Servers oder einem anderen Mitglied mit entsprechenden Berechtigungen) in einen Server aufgenommen werden muss, der diesen Zugang aber auch verweigern kann. Der Bot wird in der Nutzerliste zudem eindeutig als solcher gekennzeichnet, was einen Verdacht erwecken könnte – insbesondere bei Communities, die sensible oder umstrittene Themen diskutieren, rechtswidrige Inhalte teilen oder illegale Aktivitäten durchführen.

Eine zweite Möglichkeit wäre die Automatisierung normaler Benutzerkonten (im Allgemeinen als „Self-Bots" bezeichnet). In diesem Fall treten die Forschenden den Servern zunächst als normale Nutzenden bei und gebrauchen hierzu beispielsweise einen Einladungslink. Anschließend gibt sich der Bot als diese Nutzerin oder dieser Nutzer aus. Die Verwendung von „Self-Bots" stellt ein täuschendes Verhalten dar und ist nach den Nutzungsbedingungen von Discord verboten.42 Die Nutzungsbedingungen von Discord verweisen auch auf die Entwicklerrichtlinie (Developer Policy). Nach dieser Richtlinie ist ein Gebrauch der API für das Scraping bzw. die massenhafte Erfassung von Daten von einem Discord-Server verboten.[43] Als Voraussetzung für die Erforschung einer Gruppe auf Discord mittels ethnografischer Methoden müssen die Forscher:innen ein Benutzerkonto erstellen, um als Beobachter:innen oder Teilnehmer:innen an der Gruppe teilzunehmen. Bei der Registrierung auf Discord erklären sich die Nutzer:innen mit den Nutzungsbedingungen der Plattform einverstanden. Damit birgt jede Forschungsarbeit auf Discord, die entgegen dem in den Nutzungsbedingungen geregelten Verbot über die API-Daten der relevanten Kanäle erfasst, das juristische Risiko, von der Plattform wegen eines Verstoßes gegen die Nutzungsbedingungen belangt zu werden.

Analyse von Communities auf Discord: Wichtigste Ergebnisse

Wie in den vorausgehenden Abschnitten dargelegt wurde, war der Umfang unserer Forschungsarbeit auf Discord durch Fragmentierung sowie durch ethische und rechtliche Hindernisse eingeschränkt. Die Ergebnisse stützen sich daher hauptsächlich auf qualitative und nicht systematisierte Analysen von Inhalten und Verhaltensweisen auf Servern, von denen wir aus ethischen Gründen nicht von vornherein ausgeschlossen waren. Gleichwohl zeigen die in den nachstehenden Abschnitten vorgestellten Ergebnisse, dass hetzerische, antidemokratische und gewalttätige Inhalte in diesen Communities stark verbreitet sind.

Überblick über die Server

In den folgenden Abschnitten werden die Ergebnisse unserer ethnografischen Erforschung von katholisch- und islamistisch-extremistischen Communities auf Discord zusammengefasst. Wir beginnen mit einem allgemeinen Überblick über die Größe, die Art und den Umgangston in diesen Communities. Anschließend führen wir Beispiele für die von uns identifizierte Hass- und Gewaltrhetorik an.

Ende August 2022 identifizierten die Forscher:innen des ISD auf Discord 31 englischsprachige Server mit katholisch-extremistischen Inhalten und insgesamt 9.585 Mitgliedern sowie 16 mit islamistischem Extremismus assoziierte Server mit insgesamt 4.757 Mitgliedern. An dieser Stelle sei noch einmal ausdrücklich darauf hingewiesen, dass der Aufbau von Communities zwar zu den Hauptzielen der Server auf Discord zählt, dass es jedoch innerhalb der Server eine große Vielfalt an Themen gibt. Es ist daher eher zutreffend zu konstatieren, dass sich unsere Analyse auf die Aktivitäten des katholischen Integralismus und des islamistischen Extremismus auf Servern von Discord konzentrierte, auf denen darüber hinaus auch andere Themen diskutiert werden. Es handelt sich also nicht um Server, die sich ausschließlich auf den katholischen Integralismus oder den islamistischen Extremismus beschränken.

Davon abgesehen bestimmen die Serverregeln oft, dass Kommentare nicht gegen religiöse Anschauungen verstoßen, Gläubige beleidigen oder religiöse Instanzen angreifen dürfen, und dass Nutzer:innen bei Verstößen gegen diese Regeln ausgeschlossen werden können. Darüber hinaus sind die Verhaltensmuster Ironisierung und Gamification

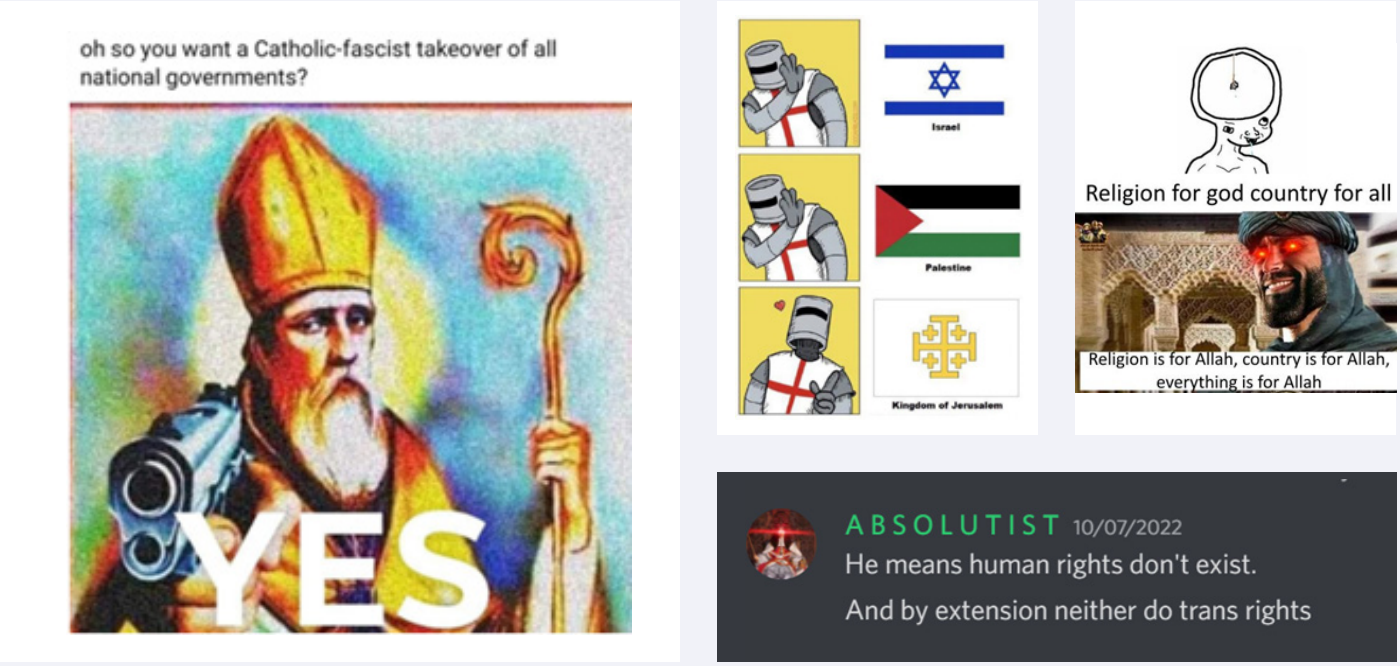


Abbildung 12: Katholisch- und islamistisch-extremistische Inhalte und Memes, die auf Servern von Discord geteilt wurden und sich gegen Menschenrechte und Trans-Rechte aussprechen bzw. einen totalitären religiösen Staat propagieren

auf den meisten Servern verbreitet. Letzterer Begriff bezeichnet die Verwendung von Videospiel-Elementen bei der Radikalisierung, zur Förderung extremistischer Ansichten oder zur Gestaltung extremistischer oder terroristischer Inhalte. Dabei bleibt oft unklar, ob die jeweiligen Nutzer:innen autoritäre religiöse Staaten oder Bewegungen tatsächlich unterstützen oder sie lediglich aus ästhetischen Gründen interessant oder „cool" finden.[44]

Sowohl auf den katholisch- als auch auf islamistisch-extremistischen Servern ist häufig zu beobachten, dass Nutzer:innen ihre Vorstellungen einer idealen Gesellschaft skizzieren. Mitunter beschreiben die Admins diese Ideale auch in den Serverregeln. In diesen utopischen Visionen wird im Allgemeinen die Überlegenheit und Dominanz einer identitätsbasierten katholischen bzw. muslimischen Eigengruppe (Ingroup) über alle Fremdgruppen (Outgroups) vertreten. Die dabei zu Tage tretende Weltsicht ist mit pluralistischen Grundwerten und den universellen Menschenrechten nicht mehr vereinbar, womit die Definition des ISD für Extremismus erfüllt wird (vgl. Glossar). Die genaue Form des idealen katholischen Staates ist unklar. Die Forscher:innen stießen auf Nutzer:innen, die unter anderem mit Vorstellungen des linken antikapitalistischen Integralismus, Faschismus, Monarchismus und christlichen Nationalismus sympathisierten.

Unter islamistischen Extremist:innen sind auch Aufrufe zur Wiedererrichtung einer totalitären modernen Version des Kalifats verbreitet, das alle Muslim:innen vereinen würde. In diesem Kalifat würden alle Lebensbereiche, einschließlich sämtlicher politischer, wissenschaftlicher und spiritueller Belange, den islamistisch-extremistischen Interpretationen des Islam unterworfen. Dazu gehört eine strenge juristische Auslegung der Scharia, die neben Prügelstrafen auch Einschränkungen der Glaubens- und Meinungsfreiheit sowie der Rechte sexueller und religiöser Minderheiten vorsieht. Sunnitische islamistische Extremist:innen brachten auf den untersuchten Discord-Servern besondere Verachtung für schiitische und liberale Muslim:innen, Sufis und Atheist:innen zum Ausdruck.

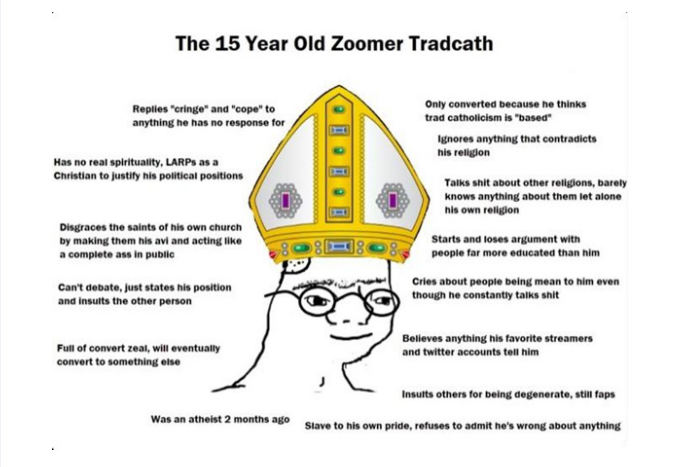


Abbildung 13: Ironische Memes, die sich über die Vorurteile gegenüber katholisch-extremistischen Subkulturen im Internet lustig machen

Hassrhetorik

Im folgenden Abschnitt werden verschiedene Arten von hasserfüllten und beleidigenden Inhalten gegenüber bestimmten Gruppen beschrieben, die auf verschiedenen Servern identifiziert wurden. Neben hitzigen Debatten über gesellschaftliche Visionen zielen viele Inhalte auf bestimmte politische Feindbilder und Fremdgruppen ab. Dabei scheint die Abgrenzung durch eine gruppeneigene Identität und die damit verbundene interne Bestätigung dessen, was vermeintlich „die Norm" oder „das Richtige" darstellen sollte, für die Herausbildung einer Eigengruppe (Ingroup) entscheidend zu sein.[iv]

iv In den USA hat sich zum Ausdruck dieses Selbstverständnisses, „normale" oder „richtige" Überzeugungen zu vertreten, der Begriff „based" durchgesetzt, der ursprünglich auch für eine Abhängigkeit von Crack stand. Der Begriff wurde dann zuerst von dem Rapper Lil B als Synonym für „authentisches Verhalten" umgeprägt und später von Rechtsextremist:innen im Internet aufgegriffen, um Dinge zu beschreiben, die mit ihren eigenen Werten übereinstimmen.

Die Admins einiger Server scheinen sich bewusst zu sein, dass die ideologische Ausrichtung ihrer Communities gegen die Richtlinien von Discord in Bezug auf die Anwendung von Hassrede oder die Verbreitung gewalttätiger extremistischer Inhalte verstoßen könnte. So forderten beispielsweise zwei Server mit katholischen Communities die Mitglieder in ihren Regeln auf, keine geschützten Gruppen oder Mitglieder einer schwarzen, asiatischen oder ethnischen Minderheit (in Großbritannien, wo der Server vermutlich beheimatet ist, häufig mit dem Akronym BAME bezeichnet) anzugreifen, um einen Verstoß gegen die Nutzungsbedingungen von Discord zu vermeiden.v
Als Gemeinsamkeit vereint die extremistisch-katholischen und extremistisch-islamistischen Nutzer:innen auf Discord der Hass gegen Angehörige der LGBTQ-Gemeinschaft. Trotz der ideologischen Divergenzen zwischen den Servern in vielen anderen Fragen scheint es einen weitgehenden Konsens in der Ablehnung von Homosexualität und Trans-Rechten zu geben. Die Anhänger der katholisch- und islamistisch-extremistischen Communities nutzen die Kommunikation auf den entsprechenden Servern im Allgemeinen dafür, Positionen zum Ausdruck zu bringen, die sie als die normative Doktrin ihrer jeweiligen Religion ansehen.

Abbildung 14: LGBTQ-feindliche Kommentare und Memes: Verherrlichung von Gewalt gegen Homosexuelle, die vom Dach eines Hochhauses gestoßen werden (links); Verspotten von Ansichten, nach denen die islamischen Schriften mit LGBTQ-Rechten vereinbar seien (rechts)

Darüber hinaus sind auch antisemitische Inhalte auf Discord-Servern von katholisch- und islamistisch-extremistischen Communities gleichermaßen nachweisbar. Mitglieder beider Communities bringen häufig einen religiös begründeten Antisemitismus zum Ausdruck, der sich auf fortbestehende historische Formen des Antisemitismus stützt. Während antisemitische Äußerungen unter islamistischen Extremist:innen manchmal mit dem Hass auf Israel in Verbindung stehen, haben die meisten antisemitischen Inhalte sowohl bei katholischen als auch bei islamistischen Extremist:innen auf Discord keinen erkennbaren Bezug zu Israel. Vielmehr stellen sie Jüdinnen und Juden als Satanist:innen (oder sogar als Personen mit Macht über Satan), als Dämonen, gierig oder nicht-menschlich dar. In den in Abbildung 15 dargestellten Beiträgen wird außerdem unterstellt, das Judentum sei nicht nur dämonisch, sondern auch mit dem Eintreten für die Rechte von Transsexuellen verbunden. Dies ist ein beliebtes Argument in rechtsextremen Kreisen, dem zufolge Jüdinnen und Juden angeblich versuchen, patriarchale Gesellschaften zu schwächen, indem sie die binären Geschlechternormen in Frage stellen.

Die Ablehnung des Feminismus ist ein weiterer Faktor, der katholisch- und islamistisch-extremistische Server auf Discord sowohl unter- als auch miteinander verbindet. Nutzer:innen machen sich oft über Frauenrechtler:innen lustig oder werfen ihnen vor, sie würden durch ihre Ansichten über Geschlechternormen provoziert werden. Eine verbreitete Angriffstaktik gegen den Feminismus ist die Behauptung, dass traditionelle Geschlechter- und Familiennormen Frauen tatsächlich glücklicher machen, während feministische Werte im Alter kinderlose, einsame und reuevolle Frauen hervorbringen.

v In den Community-Richtlinien von Discord heißt es: „Du darfst keine Hassrede oder andere hasserfüllte Verhaltensweisen verwenden. „Es ist nicht zulässig, eine Person oder eine Gemeinschaft aufgrund von Merkmalen wie Rasse, ethnischer Zugehörigkeit, Kaste, nationaler Herkunft, Geschlecht, Geschlechtsidentität, Geschlechtsdarstellung, sexueller Orientierung, Religionszugehörigkeit, Alter, schwerer Krankheit, Behinderung oder anderer geschützter Merkmale anzugreifen.“ Discord Community-Richtlinien (Februar 2023). Discord. URL: https://discord.com/guidelines.

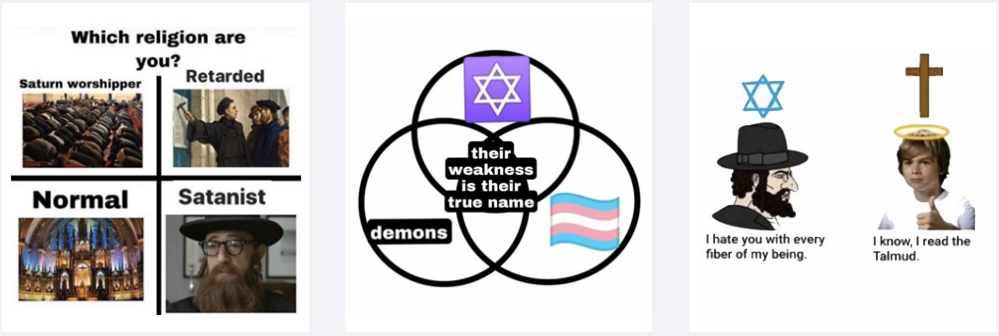


Abbildung 15: Memes, mit denen Juden:Jüdinnen, Protestant:innen, Muslim:innen und Trans-Menschen angegriffen werden

Abbildung 16: Meme, das sich über die fiktive Zukunft von Frauen lustig macht, die sich nicht an die traditionellen Geschlechterrollen halten (links); Screenshot eines Videos, in dem darüber fantasiert wird, die Frauenrechtlerin Malala Yousafzai zu ermorden (rechts)

Ein weiterer Kritikpunkt am Feminismus und der Frauenrechtsbewegung, der häufiger auf Servern mit katholisch-extremistischen Communities zu finden ist, zeigt sich in einer Ablehnung der Abtreibung. Demgegenüber gibt es zwar sowohl innerhalb des Islams als auch unter Islamist:innen eine gewisse Vielfalt an Ansichten, wobei eine strikte Ablehnung von Schwangerschaftsabbrüchen jedoch relativ selten geäußert wird. Nutzer:innen auf Servern mit katholischen Communities begrüßten im Allgemeinen die Aufhebung der Entscheidung Roe v. Wade im Juni 2022, die den Frauen das Recht gab, über Abbruch oder Fortführung einer Schwangerschaft selber zu entscheiden. Auf einem Server, der mit Linksintegralismus assoziiert war, gingen Nutzer:innen sogar so weit, das Recht auf Abtreibung als „individualistisch und mit dem Liberalismus verknüpft" zu verurteilen und zu behaupten, dass dies der Grund sei, warum Nikita Chruschtschow in den 1950er Jahren im Rahmen seiner „Entstalinisierungs"-Reformen die Abtreibung legalisiert habe. Auf einigen islamistisch-extremistisch geprägten Servern, auf denen Taliban-Unterstützer:innen aktiv sind, sprachen sich die Nutzer:innen zudem gegen das Recht der Frauen auf Bildung aus. Ein Video fantasierte von einer Zeitreise in die Vergangenheit, in der die Männer, die das Attentat auf Malala Yousafzais verübt haben, besser ausgebildet worden wären, mit dem Ziel, Malala Yousafzais nicht nur zu verletzen – wie geschehen –, sondern sie tatsächlich auch zu ermorden.[vi]

vi Malala Yousafzai ist eine pakistanische Menschenrechtsaktivistin und Friedensnobelpreisträgerin, die 2012 bei einem von den Taliban verübten Attentat durch Schüsse schwer verletzt wurde, weil sie sich für das Recht aller Kinder – insbesondere auch der Mädchen – auf Bildung einsetzte.

Gewaltrhetorik

Bei der Klassifizierung von gewalttätigen Inhalten ist zu berücksichtigen, dass die Haltung der Nutzer:innen in Bezug auf deren Befürwortung von Gewalt keine binäre Variable ist, sondern sehr unterschiedliche Ausprägungen innerhalb eines breiten Spektrums annehmen kann. Dieses Spektrum reicht von einem implizierten Bedürfnis nach Gewalt, der Verherrlichung von oder Solidarität mit bekannten Gewalttätern oder -gruppen, über Aufrufe, sich gewalttätigen Bewegungen anzuschließen oder unspezifische Aufrufe zur Gewalt, bis hin zur Verbreitung von Lehrmaterial und Informationen, die Einzelpersonen oder Gruppen der Gewalt aussetzen könnten.

Wenngleich nur wenige konkrete Gewaltaufrufe gefunden wurden, stellten die Forscher:innen eine Reihe von unspezifischen Aufrufen zu Gewalt und gewaltverherrlichenden Beiträgen fest. Insbesondere auf Discord-Servern mit islamistisch-extremistischen Communities gab es darüber hinaus vermehrt Beiträge, die ein Bedürfnis nach Gewalt andeuteten. So äußerten Nutzer:innen die Hoffnung, dass Gott (Allah) den Mudschaheddin erlauben würde, Homosexuelle und ihre Anhänger:innen zu töten oder einen ernsthaften Aufstand gegen den pakistanischen Staat zu initiieren. Einige Memes zeigten die Ermordung von Menschen aus der westlichen Welt oder die Hinrichtung von Hindus (dargestellt als „Pepe der Frosch"-Figuren mit dem Namen Pajeet – eine im Internet häufig verwendeter und abwertender Begriff für Inder:innen).

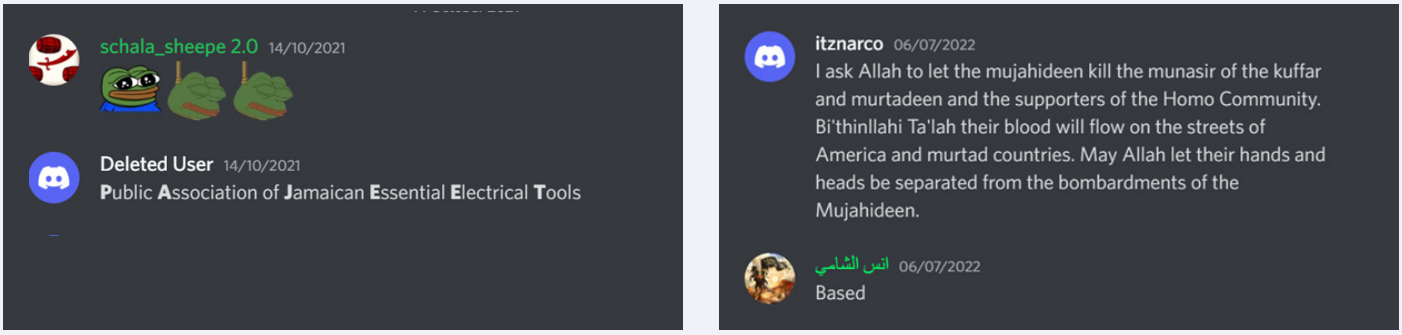


Abbildung 17: Äußerungen, in denen zur Hinrichtung von Inder:innen aufgerufen wird (symbolisiert durch den Begriff Pajeet) und in denen Gott angerufen wird, Homosexuelle und deren Unterstützer:innen zu töten

Nutzer:innen der Server mit islamistisch-extremistischen Bezügen äußerten darüber hinaus ihre Unterstützung für extremistische und terroristische Organisationen, darunter der IS, al-Qaida, die Taliban und Hamas. Dazu gehörte das Teilen von offiziellen Inhalten des IS und den Taliban (einschließlich Hinrichtungsvideos) und die Erstellung eigener Memes und Videospielgrafiken, die extremistische oder terroristische Gruppen verherrlichen. Interessanterweise scheinen Inhalte und Kommentare, die Solidarität mit dem Islamischen Staat (IS) ausdrücken, besonders umstritten zu sein und eher kritische Reaktionen auszulösen als Beiträge zur Unterstützung anderer islamistisch-extremistischer Bewegungen. So genießen zum Beispiel die Taliban offenbar mehr Unterstützung, wobei eine Vielzahl von Memes freudige Zustimmung zur erfolgreichen Wiedererrichtung des Islamischen Emirats Afghanistan im September 2021 zum Ausdruck brachte.

Dabei ist zu beachten, dass daraus nicht auf eine einheitliche Ideologie innerhalb der analysierten Server geschlossen werden kann. Erstens sind die verschiedenen extremistischen Gruppen oft miteinander verfeindet. Die Taliban, Al-Qaida und Hamas etwa sind alle Gegner des IS. In Afghanistan zum Beispiel bekämpfen sich die Taliban und ISIS-K (der afghanische Ableger des IS) gegenseitig militärisch. Zweitens kommen auf den Servern, wie bereits erwähnt, oft unterschiedliche ideologische Ansichten zum Ausdruck, wobei Meinungsverschiedenheiten zwischen den Nutzern:innen an der Tagesordnung sind.

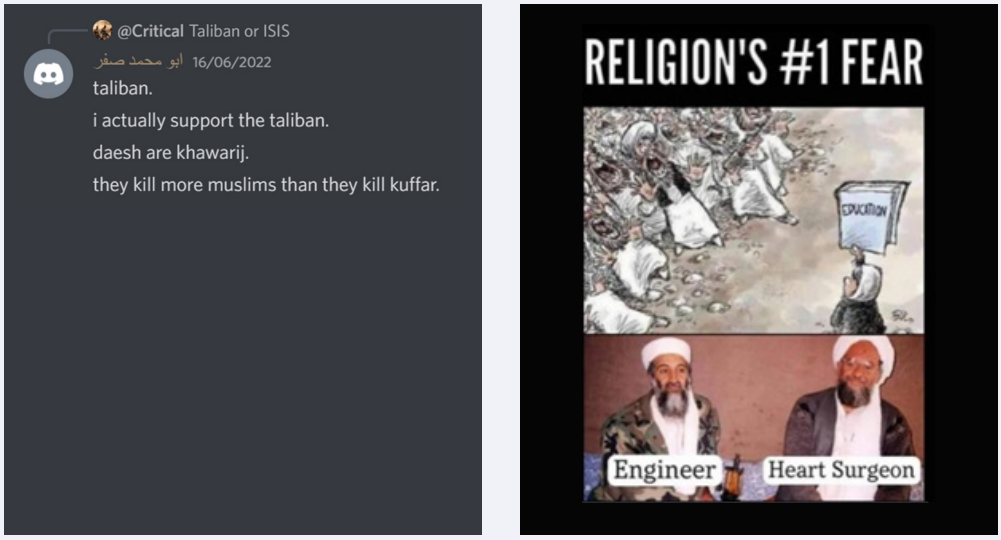


Abbildung 18: Beitrag, in dem die Unterstützung für die Taliban zum Ausdruck gebracht wird (links); Karikatur, mit der die These lächerlich gemacht werden soll, nach der die religiöse Führung durch Bildung untergraben werden könnte, indem auf die Ausbildung der Al-Qaida-Führer Osama bin Laden und Ayman al-Zawahiri als Ingenieur bzw. Herzchirurg verwiesen wird (rechts)

Abbildung 19: Memes und Videospielgrafiken, die Solidarität mit den Taliban zum Ausdruck bringen

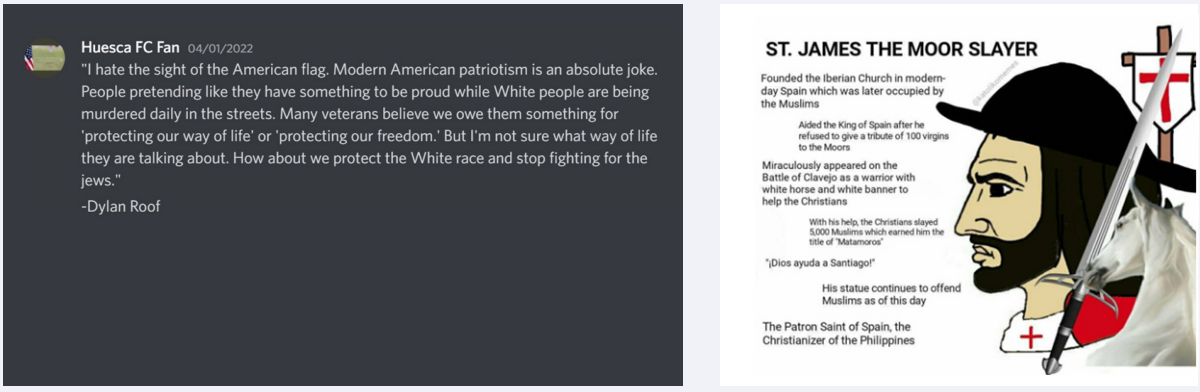


Abbildung 20: Inhalt, der sich um die mythische Figur des Sankt Jakobus des Maurentöters dreht und die Tötung von Muslimen verherrlicht (oben); Zitat des Attentäters von Charleston, Dylann Roof (unten)

Auf den untersuchten Servern mit katholisch-integralistischen Communities wurden Beispiele von Gewaltrhetorik weniger häufig beobachtet. Nutzer:innen und Admins vertraten jedoch zuweilen die Ansicht, dass Gewalt im Kampf gegen „Entartung (Degeneration) und die moderne Gesellschaft" unverzichtbar sei. In einem Fall hat ein:e Nutzer:in ein Zitat von Dylann Roof verbreitet, dem Attentäter, der in einer Kirche im US-amerikanischen Charleston neun Menschen erschoss. Darin werden die Leser:innen aufgefordert, für die „weiße Rasse" zu kämpfen und nicht für angebliche jüdische Interessen (vgl. Abschnitt über Hassrhetorik oben). Zudem wurden einige Memes geteilt, die sich um die mythische Figur des Sankt Jakobus des Maurentöters drehten und die Tötung von Muslimen verherrlichten.

Ergebnisse und Empfehlungen

Unsere Analyse von Servern auf Discord, auf denen katholisch- und islamistisch-extremistische Communities aktiv sind, deutet darauf hin, dass es eine kleine, aber signifikante Präsenz von Communities mit schädlichen Inhalten und Verhaltensweisen gibt, die zuweilen sehr extreme, hasserfüllte, antidemokratische und gewalttätige Inhalte teilen. Da Forschungshindernisse aufgrund einer ausgeprägten Fragmentierung, ethischer Bedenken und rechtlicher Risiken eine systematische Analyse verhindern, sind unsere Forschungsergebnisse qualitativer Natur und bilden möglicherweise nur einen Bruchteil des tatsächlichen Ausmaßes von vergleichbaren Aktivitäten auf der Plattform ab

Dabei sind die ethischen Überlegungen im Zusammenhang mit dem Schutz der Privatsphäre und der Menschenrechte nachvollziehbar. Dennoch sollten politische Entscheidungsträger:innen, Plattformen und Menschenrechtsaktivist:innen zusammenarbeiten, um einfachere und praxistauglichere Definitionen von öffentlichen und privaten Räumen zu entwickeln, die diese Bedenken gegen das öffentliche Interesse an der Erforschung von Extremismus und anderen schädlichen Online-Aktivitäten abwägen.

Wir sind der Meinung, dass die rechtlichen Risiken im Zusammenhang mit möglichen Verstößen gegen die Nutzungsbedingungen von Discord eine im öffentlichen Interesse liegende legitime Erforschung von Communities mit schädlichen Inhalten und Verhaltensweisen verhindern. Es wäre begrüßenswert, wenn die Plattformen, einschließlich Discord, ihre Nutzungsbedingungen ändern würden, um systematische Untersuchungen im öffentlichen Interesse zu ermöglichen, anstatt sich der öffentlichen Beobachtung zu entziehen. Idealerweise sollten Forscher:innen durch neue Gesetze vor rechtlichen Risiken geschützt werden, wenn sie im öffentlichen Interesse liegende Forschung über Communities mit schädlichen Inhalten und Verhaltensweisen betreiben, die in öffentlichen Online-Räumen agieren. Schließlich sollten Discord und Disboard gemeinsam daran arbeiten, erstens die Suchfunktionen zu verbessern und zweitens proaktiv Server zu identifizieren und zu moderieren, die rechtswidrige Inhalte und Verhaltensweisen aufweisen oder gegen die Nutzungsbedingungen von Discord verstoßen, indem sie die Tagging-Funktion von Disboard nutzen.

Fallstudie 3 : **Odysee**

Wichtigste Ergebnisse

- Odysee ist eine primär audiovisuelle Plattform, die auf der Blockchain-Technologie basiert. Untersuchungen auf Odysee bieten sich daher potenziell stellvertretend zur Analyse technologischer Forschungshindernisse an.
- Dabei stellten wir fest, dass die Blockchain-gestützte Funktionsweise von Odysee weniger unüberwindbare Hindernisse darstellte, als wir im Vorfeld erwartet hatten. Tatsächlich lieferten Transaktionen mit der Kryptowährung LBC, die öffentlich sichtbar sind, sogar zusätzliche Datenpunkte. Allerdings ist für die Untersuchungen und Zusammenführung der verschiedenen Tools neben technischem Fachwissen auch ein erheblicher Arbeitsaufwand vonnöten. Die Ausrichtung der Plattform auf audiovisuelle Inhalte bedeutete zusätzlich einen erheblichen Forschungsaufwand für die manuelle Sichtung der Inhalte.
- Da Odysee im Vergleich zu YouTube und anderen gängigen Plattformen für audiovisuelle Inhalte weniger streng moderiert wird und darüber hinaus auch Möglichkeiten bereitstellt, Inhalte zu monetarisieren und Videos von YouTube zu importieren, bietet sich die Plattform potenziell für die Verbreitung extremistischer oder verschwörungsideologischer audiovisueller Inhalte an.

Im Rahmen der Fallstudie untersuchte das ISD französischsprachige neofaschistische und rechtsextreme monarchistische Communities sowie eine mit diesen Communities verbundene Gruppe katholisch-extremistischer Fundamentalisten auf Odysee und traf dabei in erster Linie auf technologische Forschungshindernisse. Da dezentrale und/oder Blockchain-basierte Plattformen wie Odysee in der Online-Forschung bisher relativ wenig erforscht sind, wollten wir zunächst eruieren, ob systematische Suchmethoden anwendbar sind, auf welche Daten damit zugegriffen werden kann und welche zusätzlichen Hindernisse während des Prozesses entstehen.

Zu Beginn dieses Forschungsprojekts war unklar, welche Arten von Daten von Odysee über die LBRY-API (siehe Erläuterung unten) verfügbar sein würden und ob der dezentrale Charakter der Plattform zu Problemen bei der Synchronisierung von Datenpunkten führen könnte. Wie sich herausstellte, ermöglicht LBRY den Zugriff auf Daten über Krypto-Wallets, Blöcke (blocks), Kanäle und Videos. Allerdings bestehen dennoch technologische Forschungshindernisse. So ist beispielsweise nicht unmittelbar ersichtlich, ob ein Video von einer anderen Plattform wie YouTube importiert oder ursprünglich auf Odysee eingestellt wurde, wobei nur unvollkommene Methoden existieren, mit denen sich dies nachprüfen lässt.

Im Rahmen unserer Arbeit stießen wir zusätzlich auf rechtliche Hindernisse bei der Erforschung von Odysee. Die Nutzungsbedingungen der Plattform schränken die Erfassung personenbezogener Daten ein, ohne jedoch eindeutig und rechtssicher zu definieren, was in diesem Zusammenhang darunter zu verstehen ist. Da die betreffenden Daten öffentlich zugänglich und auch ohne Anmeldung mit einem Odysee-Account einsehbar sind, spielen ethische Bedenken hinsichtlich des Datenschutzes nur begrenzt eine Rolle. Trotzdem bleibt unklar, ob die Erfassung von Daten, die Odysee als personenbezogen definiert, gegen das Vertragsrecht verstößt.

Diese Hindernisse schränken nicht nur die möglichen Datenpunkte ein, die für diese Fallstudie erfasst werden, sondern auch die Art und Weise, wie diese später präsentiert werden können. Für die Zwecke dieser Untersuchung haben wir uns entschieden, öffentlich gepostete Daten wie Videos oder Kommentare zu erfassen und nach Nutzer:innen-Kategorien zusammenzufassen. Die Ergebnisse deuten auf das Bestehen ausgeprägter antidemokratischer Ideologien innerhalb der französischsprachigen Communities auf der Plattform hin. Dazu gehören auch Inhalte, in denen der Holocaust geleugnet und der Nationalsozialismus verherrlicht werden – beides Straftatbestände in Frankreich.

In den folgenden Abschnitten gehen wir auf die Hintergründe und Funktionsweise von Odysee ein und beschreiben die identifizierten und angewendeten Forschungsansätze sowie die in der Praxis aufgetretenen Forschungshindernisse. Abschließend stellen wir die Ergebnisse unserer Analyse vor.

Überblick über die Plattform

Odysee ist eine Videoplattform, die sich als Alternative zu YouTube positioniert. Laut Angaben der Plattform belief sich die Zahl der Nutzer:innen im Dezember 2020 auf 8,7 Millionen.[45] Die Plattform wird nicht ausschließlich von Extremist:innen und Verschwörungstheoretiker:innen genutzt. Da Odysee jedoch mit einem weniger stringenten Ansatz der Inhaltsmoderation wirbt, ist die Plattform zunehmend bei Nutzer:innen beliebt, die von größeren Videoplattformen wegen Verstößen gegen deren Nutzungsbedingungen gesperrt wurden.[46] Auf die Frage, warum Odysee dem russischen Sender RT (der inzwischen in der EU sanktioniert wurde) erlaubt, seinen Dienst weiter zu nutzen, erklärte das Unternehmen, dass es „konkurrierende Stimmen im Journalismus zulassen" wolle.[47] Ein kürzlich veröffentlichter Bericht von ISD Germany zeigte jedoch auf, dass Odysee Inhalte übertrieben einschränkte, indem ganze Accounts wegen einiger weniger Videos, die gegen die Richtlinien verstießen, komplett blockiert wurden. Zugleich wurden teils illegale Inhalte übersehen und blieben für deutsche IP-Adressen weiterhin abrufbar.[48] Odysee distanziert sich von der Bezeichnung „Alt-Tech", die eine ideologische Nähe zum Rechtsextremismus suggeriert, und zieht die Bezeichnung „New Tech" vor.[49]

Odysee ist der Nachfolger der Videoplattform LBRY.tv und baut auf dem Netzwerk LBRY auf, einem Blockchain-basierten Filesharing- und Zahlungsprotokoll im Besitz von LBRY Inc.. Laut Eigenaussage auf der Website will LBRY für das Hosting von Online-Inhalten das ermöglichen, „was Bitcoin für den Zahlungsverkehr getan hat", und verspricht damit eine dezentrale Alternative zu den etablierten Plattformen zu schaffen, um den Nutzer:innen mehr Kontrolle über ihre Produktionen zu geben.[50] Da das Netzwerk LBRY ein Blockchain-Protokoll ist, bedeutet theoretisch, dass Inhalte nicht von einer zentralen Stelle aus moderiert werden können, wenngleich Odysee in der Praxis einige Inhalte moderiert. LBRY verfügt darüber hinaus über eine eigene Währung namens LBRY Coin (LBC), die Nutzer:innen durch das Hochladen von Videos und Interaktionen mit ihren Inhalten verdienen können. Für Forscher:innen ist dabei von Bedeutung, dass diese Finanztransaktionen einsehbar sind, da es sich bei LBRY um eine öffentliche Blockchain handelt. Im weiteren Verlauf des Berichts werden wir darauf eingehen, wie dieser Sachverhalt genutzt werden kann.

Jeremy Kauffman, CEO von LBRY Inc., war Kandidat der Libertarian Party bei den Senatswahlen 2022 in New Hampshire (USA).[51] Der dadurch entstehende Bezug von LBRY zum Libertarismus könnte dazu beitragen, dass die Nutzer:innen Odysee als libertäres Unternehmen wahrnehmen und von einer zurückhaltenden Inhaltsmoderation der Plattformbetreiber ausgehen.[52] Im Oktober 2021 gab Odysee bekannt, die weitere Geschäftsentwicklung unabhängig von LBRY vorantreiben zu wollen. Das Protokoll und die Kryptowährung sollten aber weiterverwendet werden. Seitdem wird Odysee über eine LBRY-Tochtergesellschaft namens Odysee Holdings Inc. betrieben, deren neuer CEO der ehemalige TikTok-Mitarbeiter Julian Chandra ist.[53] Er verfolgt offenbar das Ziel, Odysee aus der libertären Nische zu holen und für ein Mainstream-Publikum zu öffnen, um die Plattform so profitabel zu machen.[54]

Wichtige Funktionen

Wie Odysee Inhalte bereitstellt (Hosting)

Odysee wird überwiegend zum Hochladen von Videos genutzt, kann aber auch für die Verbreitung anderer Formate wie Text- oder Audiodateien verwendet werden. Um Inhalte hochladen oder mit ihnen interagieren zu können, müssen Nutzer:innen einen Account erstellen und dabei den Nutzungsbedingungen von Odysee zustimmen.[55] Trotzdem gibt es auf der Plattform mitunter auch Videos ohne Zuordnung zu individuellen Nutzer:innen. Das bedeutet, dass man auf Videomaterial von anonymen Bereitsteller:innen (Uploader) treffen kann, deren Accounts nicht mehr aufrufbar sind. Nutzer:innen können ihre Videos von YouTube importieren, indem sie ihre Kanäle bei der Anmeldung auf Odysee synchronisieren.

Im Allgemeinen wird auf der Startseite von Odysee eine große Vielfalt an Inhalten präsentiert, die nur teilweise einen Bezug zu politischen Themen haben. Es erscheinen jedoch auch gelegentlich Beiträge umstrittener politischer Persönlichkeiten, was den Eindruck verstärkt, dass extremistische Ideologien und Desinformationen auf der Plattform toleriert werden. Die Seitennavigation von Odysee enthält verschiedene Inhaltskategorien, von denen sich viele auf Hobbies und Lifestyle beziehen. Unter der Rubrik „News & Politics" (Nachrichten und Politik) erscheinen jedoch Inhalte von Kanälen wie RT, Sputnik und The Alex Jones Channel, was den Eindruck verschärft, dass Odysee Inhalte, die nachweislich und absichtlich unrichtige Informationen enthalten, nicht moderiert.

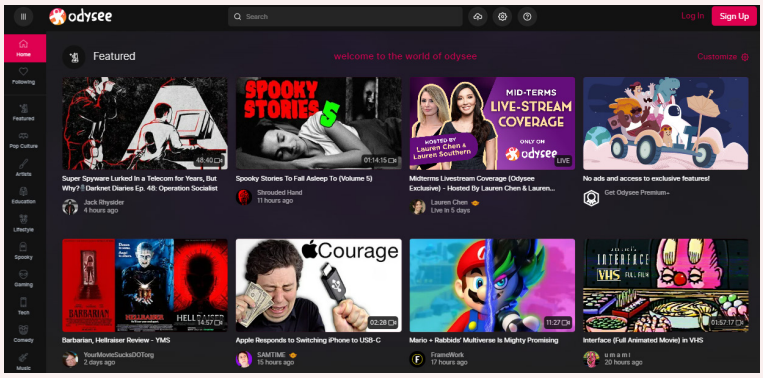


Abbildung 21: Startseite von Odysee (03.11.2022)

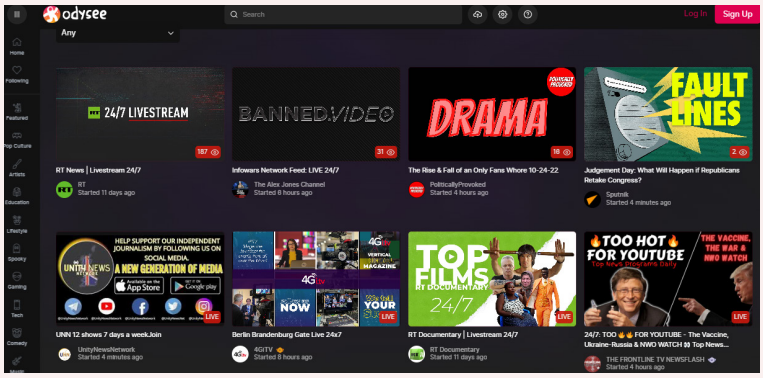


Abbildung 22: Inhalte aus der Rubrik „Nachrichten und Politik" (News & Politics) auf Odysee (englischsprachige Seite, aufgerufen am 08.11.2022)

Monetarisierung

Auf Odysee können die Inhaltsproduzent:innen (sogenannte Creators) ihre Inhalte mit der bereits erwähnten Kryptowährung LBC monetarisieren. LBC Credits können auf Handelsplattformen für Kryptowährungen gegen offizielle Währungen wie den US-Dollar gehandelt werden. Ende Oktober 2022 hatte 1 LBC lediglich einen Gegenwert von 0,02 US-Dollar. Da die Transaktionen über die Blockchain von LBRY öffentlich sind, lassen sich die Einnahmen der einzelnen Nutzer:innen auf Odysee in LBC nachvollziehen. Zu jedem Account gehört eine Wallet für LBC Credits. Außerdem ist jedes Video über eine Transaktions-ID identifizierbar.

Die Nutzung der Blockchain durch Odysee, mit der die Credits leichter von einer Wallet zu den Inhaltsersteller:innen auf derselben Plattform übertragen werden können, senkt die Schwelle für die Monetarisierung im Vergleich zu Plattformen wie YouTube, die nicht auf Kryptowährungen basieren. Diese Plattformen erfordern formelle Geschäftspartnerschaften mit den Inhaltsersteller:innen, um eine Monetarisierung zu ermöglichen. Dabei kann die

Plattform den Inhaltsersteller:innen auch die Möglichkeit zur Monetarisierung ihrer Inhalte verweigern, wenn diese als nicht werbefreundlich eingestuft werden. Die Nutzung der Blockchain durch Odysee steigert daher potenziell die Attraktivität der Plattform bei Nutzer:innen, die ihre Inhalte auf anderen Plattformen nicht monetarisieren können.

Ursprünglich schaltete Odysee keine Werbung. Im Oktober 2021 kündigte das Unternehmen an, zukünftig Werbung in Videos zu schalten, und verband dies mit dem Versprechen, im Vergleich zu konkurrierenden Plattformen einen geringeren Anteil an den Einnahmen einzubehalten.[56] Die Plattform bietet auch einen Premium-Tarif mit werbefreier Anzeige und verschiedenen anderen Funktionen.

Schädliche Aktivitäten auf Odysee

Viele selbsternannte „unzensierte" bzw. „zensurfreie" Plattformen neigen dazu, Nutzer:innen anzuziehen, die von anderen Plattformen aufgrund der Veröffentlichung von extremistischen Inhalten oder Desinformationen verbannt wurden. Dass derart positionierte Plattformen wie Odysee sich entscheiden, diese Nutzer:innen nicht zu entfernen, kann aus ideologischer Überzeugung und mit der bewussten Absicht geschehen, neue Nutzer:innen zu gewinnen, insbesondere wenn die Follower:innen der gesperrten Accounts ihnen auf die neue Hosting-Plattform folgen. Eine alternative Erklärung wäre, dass ihnen einfach die Ressourcen oder das Fachwissen fehlen, um einen umfassenderen Ansatz zur Moderation umzusetzen. In den französischen Medien hat Odysee negative Aufmerksamkeit als bevorzugte Plattform von Anhänger:innen von Verschwörungstheorien erregt, die zuvor wegen der Verbreitung von falschen Behauptungen über die Covid-19-Pandemie von YouTube gesperrt worden waren. So erschien auch die französischsprachige Desinformations-„Dokumentation" mit dem Titel „Hold Up" auf Odysee, nachdem sie von YouTube entfernt worden war. Mehrere führende Vertreter:innen der extremen Rechten wie der Politiker Florian Philippot sowie bekannte Desinformationskanäle wie France-Soir haben Kanäle auf Odysee eingerichtet. Auch wenn der aktuelle Wechselkurs für LBC Credits recht niedrig ist, stellt Odysee auch insofern ein mögliches Risiko dar, als dass die Plattform allen Nutzer:innen eine Monetarisierung von Inhalten ermöglicht und somit zur Finanzierung antidemokratischer Aktivitäten ausgenutzt werden kann.

Untersuchungen auf Odysee

Forschungsmethodik

Auch wenn es keine speziell für Odysee eingerichtete API zu geben scheint, konnten die für die Analysen auf Odysee benötigten Daten über APIs beschafft werden, die für LBRY entwickelt wurden. Wir untersuchten zwei der Tools, die LBRY für die Interaktion mit der LBRY-Blockchain und dem Netzwerk bereitstellt: Chainquery und LBRY SDK.

- **Chainquery**: Hierbei handelt es sich um ein Tool zur Abfrage von Transaktionsdaten in der Blockchain. Chainquery ist zwar für Forscher:innen einfach zu handhaben, muss jedoch auf eine lokale Kopie der LBRY-Blockchain zugreifen, deren Einrichtung und Pflege mit einigen Schwierigkeiten verbunden ist und u. a. besonders leistungsstarke Hardware erfordert. Der Beitritt zum LBRY-Netzwerk ist mit zusätzlichen sicherheitstechnischen und ethischen Bedenken verbunden, da dies die Reaktion auf die Anfragen anderer Nutzer an die Blockchain erfordert und somit eine aktive Teilnahme am Netzwerk darstellt.
- **LBRY SDK**: Dieses Tool stellt Entwickler:innen Ressourcen bereit, zur Erstellung eigener Anwendungen für die Interaktion mit der Blockchain. Neben Suchanfragen haben Forscher:innen auch die Möglichkeit, mit den Daten zu interagieren. So können beispielsweise alle Teile eines Videos gefunden und heruntergeladen werden, das zuvor gesplittet wurde. Mit dem LBRY SDK können sich Nutzer:innen mit dem Netzwerk verbinden und auf Informationen über Inhalte und Transaktionen sowie die dazugehörigen Metadaten zugreifen. Die Erstellung von Datenzugriffsanfragen über die LBRY SDK API kann zwar im Vergleich zu Chainquery zeitaufwendiger sein. Dafür ist der Aufwand für die Einrichtung und Pflege der Daten geringer.

Für das vorliegende Projekt haben wir den letzteren Ansatz gewählt und Odysee über die LBRY SDK API mit dem Analysetool Method52 untersucht. Keines der LBRY-Tools ermöglicht den Zugriff auf Kommentare, die auf Odysee veröffentlicht wurden. Der Zugriff erfolgt über ein separates System namens Commentron, das direkt vom Odysee-Team verwaltet wird. Dieses System stellt auch eine API bereit, die ähnlich wie das LBRY SDK funktioniert. Um für unsere Forschungszwecke Zugriff auf die Videokommentare zu erhalten, mussten wir diese API in Method52 integrieren.

Forscher:innen können Odysee auf ähnliche Weise analysieren wie andere Videoplattformen. Dazu gehören manuelle Sichtungen von Videoinhalten, Untersuchungen des persönlichen Hintergrundes von Kanalinhaber:innen und das Einholen von Statistiken, die die Plattform allen Nutzer:innen zur Verfügung stellt, wie beispielsweise die Anzahl der Abonnent:innen und Uploads. Die manuelle Überprüfung von Videoinhalten kann jedoch bei einer größeren Anzahl von Inhalten und Accounts sehr aufwendig werden. Eine detailliertere systematische Analyse, wie die Untersuchung von Aktivitätsspitzen in bestimmten Zeiten, ist damit in der Regel ebenfalls nicht möglich.

Durch die manuelle Untersuchung von Finanztransaktionen relevanter Akteure:innen sind Forscher:innen in der Lage, Krypto-Wallets und deren Guthaben identifizieren. Bei der Untersuchung einer großen Anzahl an Accounts wird auch diese Arbeit sehr aufwendig. Außerdem gibt es einige Einschränkungen bei der Analyse der Guthaben von mehreren Wallets. Da die Nutzer:innen mehrere Wallets besitzen können, kann es schwierig sein, die tatsächlichen finanziellen Einnahmen einzelner Nutzer:innen auf der Plattform zu überblicken. Wenn die beobachteten Kanäle sich gegenseitig Guthaben senden, werden diese LBC-Credits möglicherweise doppelt gezählt, solange man nur den Anfangs- und Endsaldo einzelner Wallets vergleicht.

Um die Erfassung von Einnahmen in Form von LBC-Credits zu automatisieren, hat CASM eine Komponente für Method52 entwickelt, die detaillierte Informationen über ein Video erfassen kann – darunter die Wallet-IDs und die LBC-Credits, die die jeweiligen Nutzer:innen mit ihren Videos eingenommen haben. Ein zusätzlicher Vorteil dieses Ansatzes zur automatischen Erfassung hoher Datenvolumen besteht darin, dass die Wallet-IDs den Accounts mit größerer Sicherheit zugeordnet werden können. Mit dem LBRY Block Explorervii lässt sich nicht erkennen, welche Wallet-ID zu welchem Kanal gehört. Forscher:innen, die einen manuellen Ansatz verwenden, müssen Beziehungen zwischen Nutzer:innen und Wallets ermitteln, indem sie die einzelnen Transaktions-IDs von Videos analysieren. Dies ist nicht nur zeitaufwendig, sondern liefert auch keinen belastbaren Nachweis dafür, welche Wallet-IDs zu welchem Kanal gehören.

Technologische Hindernisse

Blockchain ist noch immer eine sehr junge Technologie. Dementsprechend gibt es bislang nur wenige systematische, datengestützte Untersuchungen über Blockchain-basierte Social-Media-Plattformen. Infolgedessen kann die Verwendung neuartiger Methoden zur Datenerfassung unerwartete Ergebnisse hervorbringen, wobei die dezentrale Natur der Technologie zu Verzerrungen in den erfassten Daten führen kann, wie sie das ISD bereits bei der Untersuchung der Plattform PeerTube feststellte. Die Nutzung von Blockchain-Technologien durch Extremist:innen wird von Forscher:innen in anderen Zusammenhängen als zunehmend bedenklich empfunden. Das betrifft u. a. die Nutzung von non-fungible tokens (NFT's, Blockchain-basierte digitale Vermögenswerte) zur Erstellung nicht löschbarer Terrorpropaganda durch IS-Anhänger:innen.[57] Beobachter:innen haben sich jedoch weitgehend auf die Verwendung von Kryptowährungen konzentriert und nicht auf die Verwendung von Blockchain-basierten Plattformen für Propagandazwecke.

Odysee bietet zwar auch die Möglichkeit, Textdateien wie beispielsweise PDFs hochzuladen, ist jedoch in erster Linie eine Videoplattform. Audiovisuelle Inhalte stellen eine spezielle Herausforderung dar, da es schwieriger und arbeitsintensiver ist, eine große Menge dieser Inhalte systematisch zu analysieren. Sofern keine Untertitel verfügbar sind, beschränkt sich die textbasierte Analyse in der Regel auf Videotitel, Beschreibungen und Kommentare.

vii Der LBRY Block Explorer ist ein öffentlich zugängliches Online-Tool, mit dem Nutzer:innen sowohl in Echtzeit als auch im historischen Zeitverlauf Informationen über eine Blockchain aufrufen können, einschließlich Daten zu Blöcken, Transaktionen oder Adressen.

Allerdings können insbesondere automatisch generierte Untertitel aufgrund von undeutlichem Audiomaterial oder der Übersetzung in mehrere Sprachen ihrerseits Probleme verursachen.

Bei der Datenerfassung gab es einige Schwierigkeiten, die mit der Konfiguration von Odysee als Plattform zusammenhingen. Aufgrund einer bewussten Entscheidung oder eines unbeabsichtigten Fehlers im Design der Plattform werden auf Odysee nur 1.000 Videos pro Kanal angezeigt, so dass wir zunächst nur maximal 1.000 Videos eines Kanals erfassen konnten. Der Hintergrund ist, dass ältere Videos zwar nicht entfernt werden, aber auf dem Kanal nicht mehr sichtbar sind. Um Zugriff auf die nicht angezeigten Videos zu erhalten, musste die Methode zur Datenerfassung angepasst werden.

Im Vergleich zu vielen anderen Online-Plattformen, die eine besser aufeinander abgestimmte Palette von Tools für den Datenzugriff bereitstellen, ist das Software-Ökosystem rund um Odysee außerdem weder kohärent noch frei von Überschneidungen. Für die Interaktion mit Odysee gibt es zwar eine Reihe offizieller Tools wie LBRY SDK und Chainquery (siehe oben). Die analytische Arbeit mit diesen Tools erfordert jedoch viel Zeit und erhebliche technische Vorkenntnisse. Diese Tools sind vergleichsweise schlecht dokumentiert und ihre Implementierung kann daher beträchtliche Zeit in Anspruch nehmen. Beide Tools bieten viele identische Funktionen und Datenzugriffsoptionen, unterscheiden sich jedoch in anderer Hinsicht, sodass es schwierig ist, zu entscheiden, welches Tool für den jeweiligen Forschungszweck am besten geeignet ist. Um beispielsweise Zugang zu Video- und Kommentardaten zu erhalten, mussten zwei verschiedene APIs integriert werden, da diese Systeme von der Plattform getrennt behandelt werden.

Insgesamt waren die technischen Hindernisse für die Erforschung von Odysee weniger gravierend, als wir anfangs erwartet hatten. Bei früheren Untersuchungen der Plattform hatte das ISD entsprechend auf technologiebasierte Ansätze verzichtet. Letztlich konnten wir über technologische Mittel auf Daten der Plattform zuzugreifen.

Ethische und rechtliche Hindernisse

Da die meisten Inhalte auf Odysee öffentlich zugänglich sind, auch ohne sich über einen Account einzuloggen, bestehen nur begrenzte datenschutzrechtliche Risiken. Es darf berechtigterweise davon ausgegangen werden, dass die Nutzer:innen wissen, dass ihre Inhalte von jedem eingesehen werden können, der sie findet. Der LBRY Block Explorer, der die Wallets der Nutzer:innen aufzeichnet, ist ebenfalls öffentlich einsehbar und zeigt die Salden der Wallets an, ohne dass eine Registrierung oder Anmeldung bei Odysee oder einem LBRY-Konto erforderlich ist.

Ethische und rechtliche Bedenken beziehen sich hauptsächlich auf die Nutzungsbedingungen von Odysee, die das Auslesen (harvesting) oder anderweitige Erfassen von Informationen über Nutzer:innen, einschließlich E-Mail-Adressen, ohne deren Zustimmung untersagen.[58] Aus dem Wortlaut der Nutzungsbedingungen geht nicht eindeutig hervor, welche Arten der verfügbaren Daten als personenbezogen eingestuft werden und daher nicht erfasst werden dürfen. Dabei sind E-Mail-Adressen auf Odysee nicht öffentlich und können nicht über die verfügbaren offiziellen Tools abgerufen werden. Dennoch stellt sich die Frage, inwieweit es rechtlich und ethisch zulässig ist, die verschiedenen Arten von verfügbaren Daten – wie beispielsweise Uploads und Aufrufe bei Aktivitäten auf öffentlichen Kanälen – zu erfassen, sofern die betreffenden Nutzer:innen anonymisiert werden.

Für die Zwecke dieses Projekts haben das ISD und CASM beschlossen, unter Berücksichtigung der von Odysee selbst festgelegten Nutzungsbedingungen Daten über die offizielle API von LBRY zu erfassen. Nachdem ermittelt wurde, welche Arten von Daten über die verfügbare API erfasst werden konnten, haben wir festgelegt, welche als personenbezogene Daten gelten sollten. Wir haben uns entschieden, für dieses Projekt öffentlich gepostete Daten wie Videos oder Kommentare zu erfassen und sie in Nutzer:innen-Kategorien zusammenzufassen. Durch diese Vorgehensweise wurde sichergestellt, dass keine Identifizierung von Einzelpersonen anhand der Daten möglich war und die potenziellen ethischen und rechtlichen Bedenken, die sich aus den Nutzungsbedingungen von Odyssee in Bezug auf die Erhebung personenbezogener Daten ergaben, ausgeräumt werden konnten. Auf der anderen Seite verhinderte dieser Ansatz jedoch die Analyse bestimmter Datenpunkte, die ein detaillierteres Bild des Nutzungsverhaltens auf der Plattform ermöglicht hätten.

Analyse von Communities auf Odysee: Wichtigste Ergebnisse

Auf Odysee existiert ein breites, aber ideologisch zersplittertes Ökosystem französischsprachiger Communities, die mit Rechtsextremismus und Desinformation assoziiert werden. Da dieses Spektrum zu breit und ideologisch zu uneinheitlich ist, um es vollständig zu analysieren, haben wir uns stattdessen auf drei spezifische Untergruppen des französischen Rechtsextremismus konzentriert, die ideologische Verbindungen zueinander haben, auch wenn ihre Anschauungen teilweise auseinandergehen. Bei diesen ideologischen Fraktionen handelt es sich um rechtsextreme Monarchist:innen (far-right royalists), Neofaschist:innen (neo-fascists) und katholische Fundamentalist:innen (catholic fundamentalists). Die Gruppe der rechtsextremen Monarchist:innen wurde aufgrund ihrer historischen Bedeutung für den Ultranationalismus und wegen ihrer ablehnenden Haltung gegenüber der derzeitigen politischen Ordnung in Frankreich ausgewählt. Die Gruppe der Neofaschist:innen wurde ausgewählt, da sie häufig rechtswidrige Inhalte postet und dabei beispielsweise im Zweiten Weltkrieg begangene Verbrechen gegen die Menschlichkeit leugnet. Katholische Fundamentalist:innen wurden einbezogen, da sie bekanntermaßen eine ideologische Brücke zwischen den beiden erstgenannten Gruppen bilden können. Sie unterstützen sowohl den Ethnonationalismus als auch den Widerstand gegen den Säkularismus und verbreiten gleichzeitig Verschwörungstheorien und Desinformationen, die sich beispielsweise gegen Impfangebote richten. Da alle diese Gruppen dazu neigen, Verschwörungstheorien über vermeintliche mysteriöse Eliten zu streuen, und häufig ethnische oder religiöse Minderheiten diffamieren, könnten sie sich zu der Plattform hingezogen fühlen, aufgrund der als vergleichsweise lax geltenden Moderationspraktiken von Odysee.

Rechtsextreme Monarchist:innen lehnen die politische Ordnung ab, die in Frankreich nach der Französischen Revolution entstanden war – insbesondere die während dessen beschlossene Trennung von Kirche und Staat. Der radikalere Zweig der französischen Monarchist:innen befürwortet gar eine Rückkehr zur „Herrschaft durch göttliches Recht" und zum Absolutismus, bei dem der Monarch Gott allein Rechenschaft schuldig ist. Solche Vorstellungen sind von Natur aus antidemokratisch.Keine weltliche Macht, weder der französischen Senat, noch das Parlament, könnte den Regenten zur Verantwortung ziehen. Demokratische Entscheidungen oder Instanzen könnten übergangen werden. Der Ausdruck „extreme Rechte" wurde im französischen Kontext zuerst für unnachgiebige Monarchisten verwendet, die während der Zweiten Restauration (1815-1830) auf der rechten Seite der französischen Abgeordnetenkammer saßen.[59]

Neofaschist:innen sind nicht unbedingt dem katholischen Fundamentalismus zuzuordnen, da sie teilweise das Christentum zugunsten neoheidnischer Ansichten ablehnen (Neopaganist:innen). Dennoch gibt es eine deutliche Überschneidung zwischen beiden Gruppen, insbesondere wenn Neofaschist:innen das französische Volk als katholisch und rein französischstämmig definieren und Verschwörungstheorien verbreiten, die Freimaurer:innen sowie jüdische Menschen schädlicher Machenschaften beschuldigen oder eine vermeintliche satanische Unterwanderung der Gesellschaft unterstellen.

Die Kanäle auf Odysee, die wir als katholisch-fundamentalistisch eingestuft haben, konzentrieren sich in erster Linie auf religiöse Inhalte (häufig in Form von Verschwörungstheorien), teilen aber oft auch den Wunsch der Monarchist:innen nach einer Abschaffung des Säkularismus und die Unterstützung der Neofaschist:innen für den Ethnonationalismus. Mitunter verbreiten sie sogar Inhalte, die den Holocaust oder andere während des Zweiten Weltkriegs begangene Verbrechen leugnen. Gemeinsam ist allen diesen Gruppierungen die Ablehnung der aufklärerischen Ideen des Universalismus und der Persönlichkeitsrechte, die die Französische Revolution inspirierten und die Fünfte Französische Republik bis heute prägen.

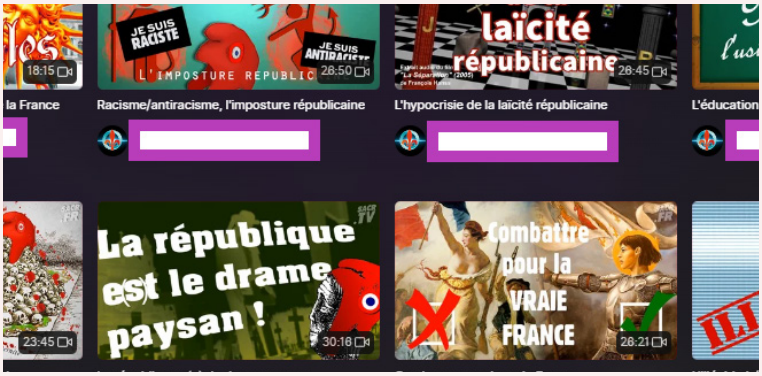


Abbildung 23: Beispiele für einen Kanal mit rechtsextrem-monarchistischen Inhalten auf Odysee

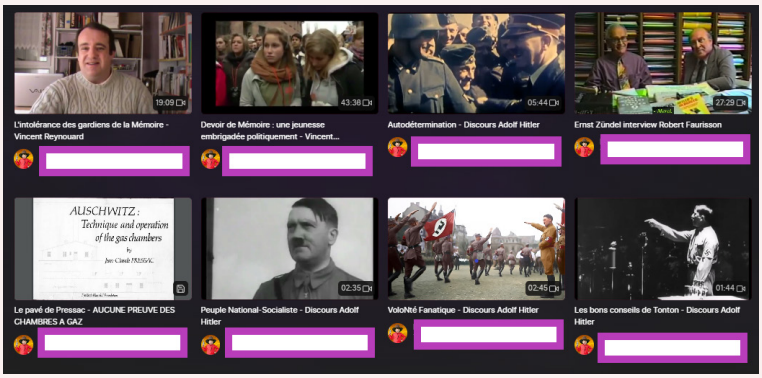


Abbildung 24: Beispiele für einen Kanal mit neofaschistischen Inhalten auf Odysee

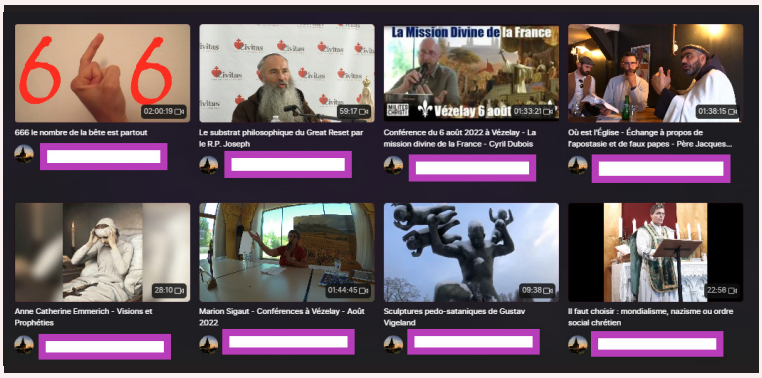


Abbildung 25: Beispiele für einen Kanal mit katholisch-fundamentalistischen Inhalten auf Odysee

Nutzung der Plattform und Nutzer:innen-Engagement

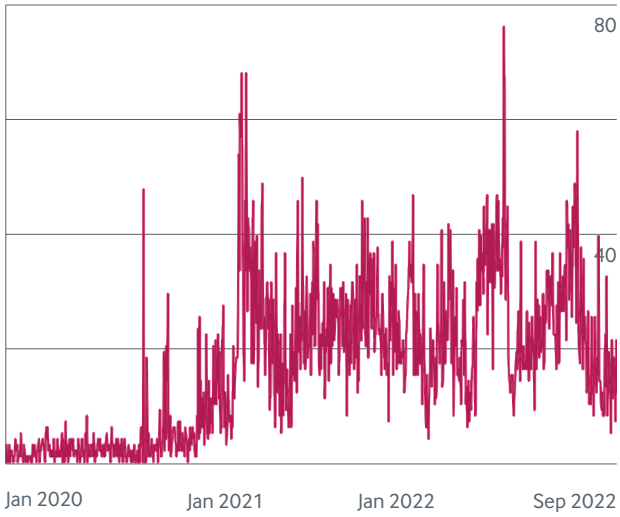
Die systematische Analyse der in den vorgenannten Communities anzutreffenden Inhalte stellt selbst bei der relativ kleinen Stichprobe, die dieser Studie zugrunde lag, eine große Herausforderung dar. Während Text problemlos mittels Computerlinguistik (NLP) analysiert und mit einem geeigneten Programm klassifiziert werden kann, müssen audiovisuelle Inhalte zunächst transkribiert werden. Die Qualität der Transkriptionen kann von Sprache zu Sprache und je nach Tool variieren. Videos, in denen mehrere Personen gleichzeitig oder in verschiedenen Sprachen sprechen, stellen die Transkriptionsprogramme in der Regel vor erhebliche Probleme. Darüber hinaus besteht das Risiko, dass visuelle Bilder – auch sogenannte Dog-Whistles –, die einen wichtigen zusätzlichen Kontext in Bezug auf ideologische Zugehörigkeiten oder die verwendeten Narrative liefern könnten, bei diesem Ansatz unberücksichtigt bleiben. Aus diesem Grund beschränkt sich der folgende Abschnitt auf die Daten, die über die API von LBRY erfasst werden konnten. Dabei handelt es sich hauptsächlich um Kanal- und Videostatistiken sowie um Informationen über Einnahmen in Form von LBC-Credits.

Die Analyse der im Zeitraum vom 1. Januar 2020 bis 15. September 2022 erfassten Daten zeigt einen ersten nennenswerten Anstieg der Aktivitäten im Sommer 2020 – also etwa zu der Zeit, als Odysee als Nachfolger von LBRY.tv eingeführt wurde. Die Daten zeigen, dass die Aktivität der beobachteten Konten auf LBRY.tv minimal war. Die anfänglichen Spitzen in der Aktivität nach dem Start von Odysee scheinen hauptsächlich auf Uploads aus der Kategorie der neofaschistischen Communities zurückzuführen zu sein. Die Daten für alle Nutzerkategorien insgesamt zeigen, dass es seit dem ersten Anstieg der Uploads im Spätsommer 2020 mehrmals zu weiteren Anstiegen der täglichen Upload-Aktivitäten gekommen ist, wobei sich die Zahl meist zwischen zehn und fünfzig Videos pro Tag bewegte.

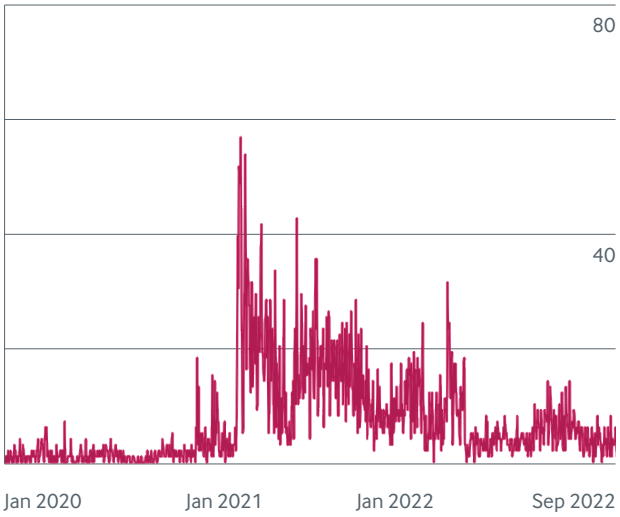
Auffällig an den Daten ist, dass ein Großteil der Upload-Aktivitäten im Jahr 2021 zunächst von Kanälen mit extremistisch-monarchistischen Inhalten und Verhaltensweisen ausging, die jedoch im Jahr 2022 die am wenigsten aktive Gruppe waren. Dessen ungeachtet haben sie innerhalb des Beobachtungszeitraums von etwas mehr als zweieinhalb Jahren mit 8.690 Videos im Vergleich zu allen anderen Nutzerkategorien die meisten Inhalte hochgeladen. An zweiter Stelle folgten die Kanäle mit neofaschistischen Communities, auf denen im beobachteten Zeitraum 6.035 Videos veröffentlicht wurden. Von den drei Kategorien haben sie seit dem offiziellen Start von Odysee am regelmäßigsten Beiträge veröffentlicht, wobei im Spätsommer 2020, im Herbst 2021 und im Sommer 2022 Phasen erhöhter Aktivität zu beobachten waren.

Die Kanäle mit katholisch-fundamentalistischen Communities haben dagegen lediglich 4.084 Videos veröffentlicht, wenngleich sie ihre tägliche Upload-Rate zum Ende des Beobachtungszeitraum deutlich erhöht haben. Nachdem für diese Nutzerkategorie in den Jahren 2020 und 2021 nur wenige Uploads zu verzeichnen waren, wurden sie im Laufe des Jahres 2022 recht aktiv. Besonders auffallend ist ein sprunghafter Anstieg der Aktivität gegen Februar und März 2022. Insgesamt kann man aus diesen Daten schlussfolgern, dass die Nutzung von Odysee im Zeitverlauf und je nach Nutzerkategorie variiert. Während das Interesse der Monarchist:innen an der Plattform anscheinend zurückgegangen ist, ist das der katholisch-fundamentalistischen Communities zunehmend gestiegen.

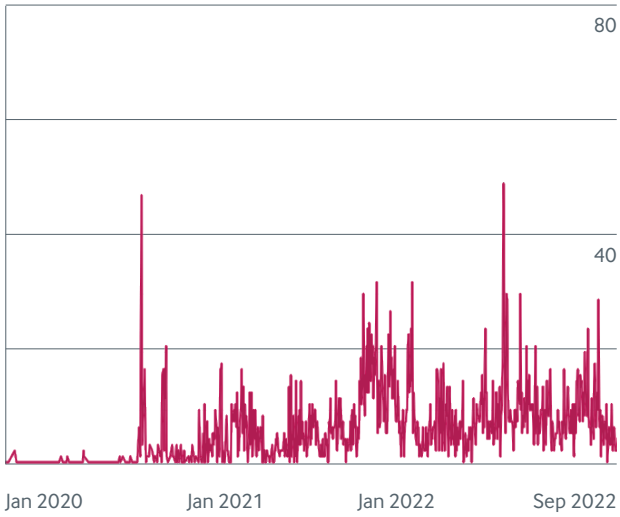
Odysee all channel videos: volume over time



Odysee Royalist channel videos: volume over time



Odysee Neo-Fascist channel: videos volume over time



Odysee Catholic Fundamentalist channel videos: volume over time

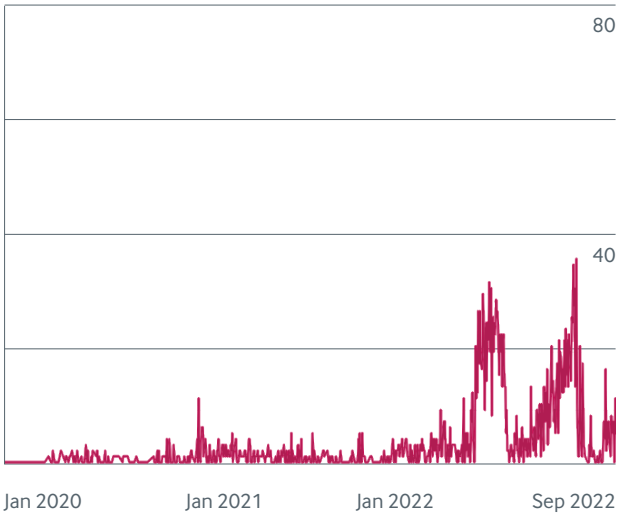
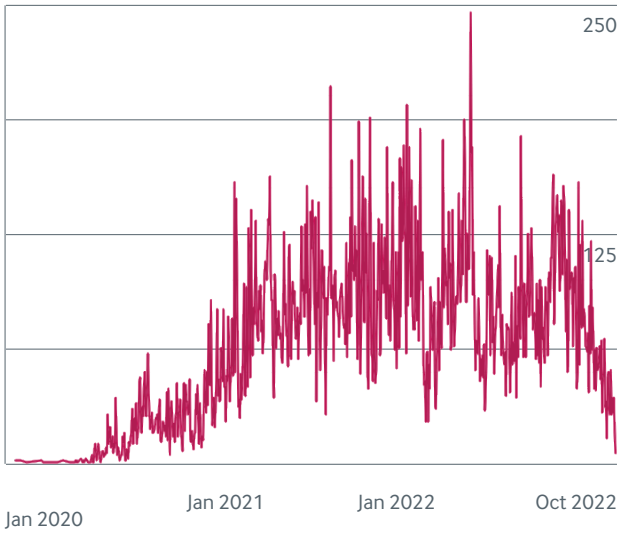
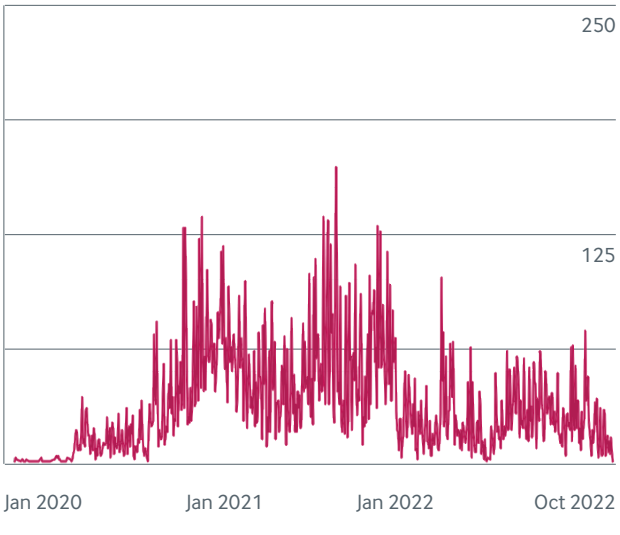


Abbildung 26: Darstellungen von Verläufen für die Anzahl der Video-Uploads im Zeitraum zwischen dem 01.01.2020 und dem 15.09.2022 für alle Kategorien insgesamt und aufgeschlüsselt nach Nutzerkategorien (monarchistische, neofaschistische, katholisch-fundamentalistische Communities)

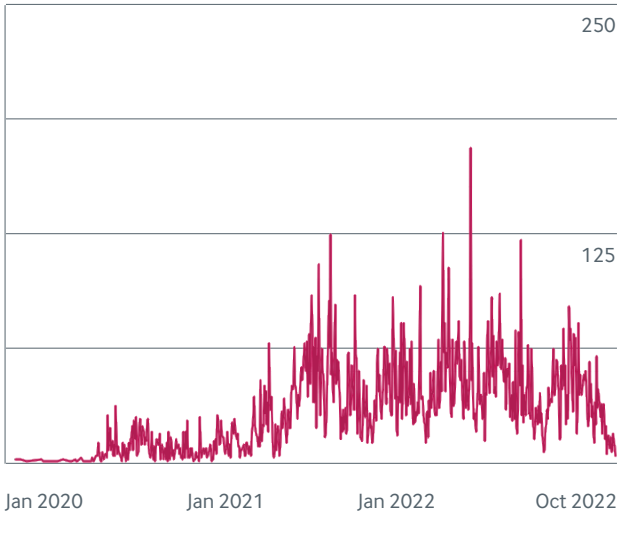
Odysee all channel comments: volume over time



Odysee Royalist channel comments: volume over time



Odysee Neo-Fascist channel comments: volume over time



Odysee Catholic Fundamentalist channel comments: volume over time

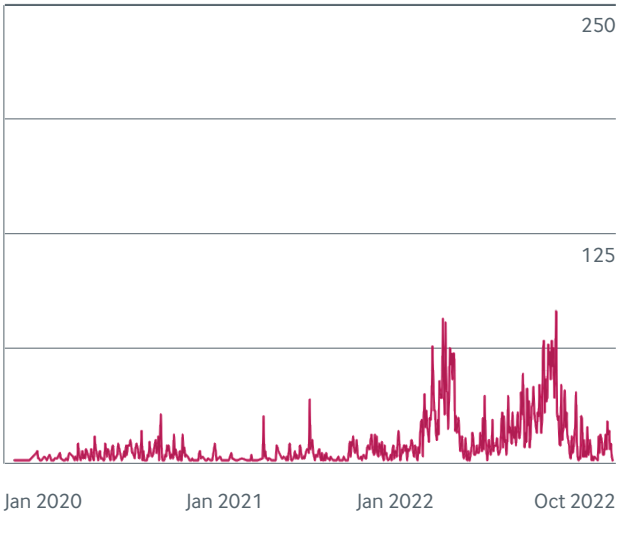


Abbildung 27: Darstellungen von Verläufen für die Anzahl der veröffentlichten Kommentare und Antworten im Zeitraum zwischen dem 13.08.2020 und dem 15.09.2022 für alle Kategorien insgesamt und aufgeschlüsselt nach Nutzerkategorien (monarchistische, neofaschistische, katholisch-fundamentalistische Communities)

Die Anzahl der Kommentare ist über eine separate API erfasst worden und wird erst ab Mitte 2020 dargestellt. Auch hier sind Unterschiede zwischen den Nutzerkategorien sichtbar, wobei die durchschnittliche Anzahl der Kommentare und Antworten vergleichsweise gering ist. Videos von neofaschistischen Kanälen erhielten im Durchschnitt 3,3 Kommentare, die der Monarchist:innen 2,4 und die der katholischen Fundamentalist:innen 1,5. Dies zeigt, dass die Upload-Rate nicht unbedingt mit der Anzahl der Kommentare in einer bestimmten Nutzer:innenkategorie korreliert.

Es wäre zu erwarten, dass die Anzahl der Kommentare im Zeitverlauf tendenziell mit der Zahl der Video-Uploads korreliert, auch wenn beide Verläufe nicht völlig deckungsgleich sind. Während die Kanäle mit extremistisch-monarchistischen Communities Anfang 2021 sehr viele Videos hochluden, spiegelt sich diese hohe Aktivität nicht in der Anzahl der veröffentlichten Kommentare wider. Nichtsdestotrotz ging mit ihrer rückläufigen Uploadrate auch die Anzahl der Kommentare entsprechend zurück. Videos, die auf neofaschistischen Kanälen veröffentlicht wurden, verzeichneten ab Herbst 2021 eine konstant bleibende Anzahl an Kommentaren. Davor war die Anzahl der Kommentare vergleichsweise gering. Es gibt gelegentlich Ausreißer, bei denen an einem einzigen Tag eine besonders große Anzahl von Kommentaren verzeichnet wurde. Der deutlichste Zusammenhang zwischen der Anzahl der Uploads und der Kommentare ist bei der Kategorie der katholischen Fundamentalist:innen zu beobachten, die im Spätwinter und Sommer 2022 eine erhöhte Aktivität aufwiesen.

Insgesamt gibt es Hinweise, die darauf schließen lassen, dass die untersuchten französischsprachigen rechtsextremistischen Communities Odysee als Alternative zu YouTube nutzen. Theoretisch könnten sie auf der Plattform mit ihren Inhalten leichter Einnahmen erzielen als auf Plattformen, die keine Kryptowährungen anbieten. Angesichts des recht geringen Wertes der LBC-Credits scheint jedoch die Erwartungshaltung der Nutzer:innen, dass Odysee Inhalte zulässt, die auf anderen Plattformen wegen Verletzung der Nutzungsbedingungen entfernt würden, derzeit eine wichtigere Rolle zu spielen.

Darüber hinaus bietet Odysee Optionen, die auf vielen anderen Videoplattformen fehlen. Inhalte anderer Nutzer:innen können mit der Funktion „Repost" geteilt und dabei erneut veröffentlicht werden. Dabei werden diese Inhalte anschließend auf der eigenen Kanalseite angezeigt. Mithilfe dieser Funktion können die Forscher:innen ideologische Affinitäten und gemeinsame Ansichten zwischen den Communities beobachten und die Narrative identifizieren, die sie miteinander verbinden. Dazu gehören insbesondere antisemitische Verschwörungstheorien und angebliche Intrigen zur Untergrabung des Katholizismus und des französischen Volkes sowie globale Verschwörungstheorien im Zusammenhang mit dem sogenannten „Great Reset" oder der „Neuen Weltordnung". Auf Odysee können neben Videos auch andere Dateiformate hochgeladen werden. Vor allem neofaschistische Gruppierungen nutzen diese Funktion, um Dokumente hochzuladen, die angeblich den Holocaust widerlegen sollen und antisemitische Verschwörungstheorien verbreiten.

Abbildung 28: Beispiel für das Re-Posting eines antisemitischen Videos (rot markiert) von einem katholisch-fundamentalistischen Kanal, das auf einem neofaschistischen Kanal wiederveröffentlicht wird

Eine weitere wichtige Funktion von Odysee ist die Möglichkeit, Inhalte direkt von anderen Videoplattformen wie YouTube zu importieren. Diese Funktion hatte einen Einfluss auf die von uns erfassten Daten, da einige Videos ein

Hochladedatum aufwiesen, das aus einer Zeit datierte, in der Odysee oder die Vorgängerplattform LBRY.tv noch nicht existierten. Aus unseren Daten ist nicht unmittelbar ableitbar, ob ein Video von einer anderen Plattform importiert wurde. Um abzuschätzen, wie viele Videos von YouTube importiert wurden, wurden alle Videobeschreibungen nach der Zeichenfolge ‚www.youtube.com/watch?v=' durchsucht und ihre Anzahl im Zeitverlauf für die Analyse zusammengestellt. Videos, die von YouTube importiert wurden, sollten einen Link zur Ursprungs-URL des Videos unter einem Dreipunkt am Ende der Videobeschreibung enthalten. Diese Methode kann zwar einen Anhaltspunkt dafür liefern, wie viele Videos im Zeitverlauf importiert wurden, aber sie ist auch mit Fehlern behaftet. Erstens kann es vorkommen, dass eine Videobeschreibung zwar die Zeichenfolge ‚www.youtube.com/watch?v=' enthält, aber keine Angabe der Ursprungs-URL darstellt, sondern die Verlinkung eines beworbenen anderen Videos. Außerdem bezieht sich das Veröffentlichungsdatum auf den Upload des Originalvideos auf YouTube und nicht auf das Datum, an dem ein bestimmtes Video in Odysee importiert wurde. Entsprechend gehen diese Upload-Zeitpunkte in den grafischen Darstellungen der Uploads im Zeitverlauf durcheinander.

Die Existenz der Importfunktion wirft die Frage auf, ob die beobachteten Akteur:innen versuchen, ihr Publikum von YouTube zu Odysee umzuleiten, wobei sie letztere Plattform möglicherweise als sichereren Hosting-Anbieter für ihr konfliktbehaftetes Material ansehen, für den Fall dass die größeren Plattformen gegen ihre Kanäle vorgehen. Auf der Grundlage von manuellen Analysen und empirischen Beobachtungen konnten in Bezug auf die Nutzung der Plattform zwei verschiedene Trends identifiziert werden, die auf unterschiedliche Typen von Akteur:innen hinweisen. Der erste Typ sind Akteur:innen, die de facto als alternative Medientreibende fungieren und eigene Inhalte wie Podcasts oder Nachrichtenkommentare produzieren. Diese verfolgen in der Regel eine Multiplattform-Strategie, bei der Odysee als eine von mehreren Hosting-Alternativen zu etablierteren Plattformen genutzt wird. Diese Akteur:innen verknüpfen ihre Profile in der Regel sowohl auf den Mainstream-Plattformen als auch auf Alt-Tech-Plattformen wie Gettr, Telegram und Rumble und nutzen häufig die Importfunktion, um ihre Videos plattformübergreifend zu synchronisieren. Dabei ist zu beachten, dass diese relativ gut organisierten Akteur:innen in der Regel mehr Abonnent:innen und Aufrufe auf YouTube haben als auf Odysee. Insofern scheint es, als ob diese Kanäle Odysee hauptsächlich als eine unter diversen anderen Backup-Lösungen nutzen, um ihre Inhalte online zu halten, falls ihr Account auf einer größeren Plattform gesperrt würde.

Der zweite Typ sind Akteur:innen, die von YouTube zu Odysee gewechselt sind oder (soweit nachvollziehbar) schon immer nur auf Odysee aktiv waren. Über diese Accounts werden häufig Inhalte veröffentlicht, die nicht nur gegen die Nutzungsbedingungen vieler Plattformen, sondern potenziell auch gegen französisches Recht verstoßen. Darunter fallen Inhalte, die den Holocaust leugnen und den Nationalsozialismus verherrlichen. Im Gegensatz zum oben beschriebenen Typ 1 haben diese Akteur:innen mehr Abonnent:innen auf Odysee als zuvor auf YouTube. Während sie auf YouTube ein paar Dutzend und manchmal weniger als zehn Abonnent:innen hatten, geht die Zahl ihrer Follower:innen auf Odysee oft in die Tausende. Damit scheint die Zielgruppe dieser Kanäle zunächst überschaubar. Allerdings handelt es sich nach Angaben von SimilarWeb bei Odysee mit 23,4 Millionen monatlichen Aufrufen (monthly visits) um eine erheblich kleinere Plattform als YouTube, wo die vergleichbare Metrik im September 2022 ganze 33 Milliarden erreichte.[60] Kanäle, die mit Videos auf der Startseite von Odysee vertreten sind – bei denen also davon ausgegangen werden kann, dass sie die meistbesuchten Inhalte der Website zeigen –, haben oft nur etwa zehntausend Abonnent:innen. Kanäle, die unter diesen Typ fallen, importieren in der Regel keine Inhalte aus ihren YouTube-Kanälen, von denen die meisten zum Zeitpunkt der Untersuchung bereits seit Monaten inaktiv waren. Stattdessen haben diese Akteur:innen direkt damit begonnen, ihre Inhalte auf Odysee hochzuladen, womit sie sich offenbar ein neues Publikum erschließen konnten.

Anders als die erste Gruppe von Akteur:innen verwenden die Betreiber:innen dieser reinen Odysee-Accounts in der Regel Pseudonyme. Diese anonymen Accounts laden häufig Material von anderen Personen hoch, darunter Interviews mit bekannten Holocaust-Leugner:innen oder historisches Filmmaterial, in dem das Dritte Reich verherrlicht wird. Eine Ausnahme stellt ein bekannter Neonazi-Aktivist dar, der in Frankreich bereits wegen Leugnung des Holocausts verurteilt wurde, aber dennoch offen seinen eigenen Kanal auf Odysee betreibt, ohne ein Pseudonym zu verwenden. Die Daten wurden wie oben beschrieben nach der Anzahl der YouTube-Links in der Videobeschreibung analysiert. Demnach verzeichneten die Kanäle der Monarchist:innen offenbar die meisten Videoimporte (3.595), die der

katholischen Fundamentalist:innen die zweitmeisten (1.807) und die der Neofaschist:innen die wenigsten (680). Eine mögliche Erklärung für diese Unterschiede ist, dass viele Accounts der Monarchist:innen zu organisierten Gruppen und Medientreibenden gehören, die eine Multiplattform-Strategie verfolgen. Im Gegensatz dazu könnten Neofaschist:innen davor zurückschrecken, ihre Inhalte auf YouTube hochzuladen, wo die Wahrscheinlichkeit größer ist, dass sie moderiert werden. Da viele dieser Konten anonym sind und größtenteils nicht zugeordnet werden können, sind sie vermutlich weniger daran interessiert, sich über eine Multiplattform-Strategie zu profilieren.

In jedem Fall scheint Odysee für diese speziellen Communities in erster Linie dazu zu dienen, Verbote auf strenger moderierten Plattformen zu umgehen. Für Organisationen und Medientreibende scheint Odysee ein Mittel zu sein, um ihre Inhalte zu schützen, falls ihre Konten auf anderen Plattformen gesperrt werden. Für diejenigen, die offen extreme Inhalte posten, ist Odysee zu einem wichtigen Medium zur Verbreitung dieser Inhalte geworden. Obwohl Inhalte sich auf Odysee sehr viel einfacher monetarisieren lassen als auf YouTube und ein Großteil der untersuchten Inhalte auf den großen Plattformen wahrscheinlich nicht monetarisiert werden würde, sind die potenziellen finanziellen Vorteile für die beobachteten Communities wahrscheinlich nicht der ausschlaggebende Faktor für ihre Entscheidung, die Plattform zu nutzen. Die Einnahmen in Form von LBC-Credits, die von diesen Kanälen seit Beginn unserer Datenerhebung im Januar 2020 erzielt werden konnten, sind insgesamt unerheblich. Insgesamt erzielten die beobachteten Kanäle in etwa zweieinhalb Jahren weniger als 500 US-Dollar für fast 20.000 Videos, was darauf schließen lässt, dass Odysee allein (noch) kein tragfähiges Geschäftsmodell für diese Nutzer:innen bietet.

Nutzer:innen-Kategorie	Anz. der Videos seit 01/01/20	Einnahmen seit 01/01/2020 in LBC	Umrechnung in USD (22/09/22)
Monarchist:innen	8 690	4 266,733 714	94,66 $
Neofaschist:innen	6 035	7 979,900 723	177,03 $
Katholische Fundamentalist:innen	4 084	7 736,055 632	171,62 $

Ergebnisse und Empfehlungen

Odysee ist bestrebt, sich als Alternative zu Mainstream-Online-Videoplattformen wie YouTube zu positionieren – durch die Verwendung der Blockchain-Technologie, die Auszahlung von Kryptowährungen sowie durch weniger strenge Standards der Inhaltsmoderation. Unsere Ergebnisse zeigen, dass sich die Plattform für einige französischsprachige rechtsextreme Communities als attraktiv erwiesen hat, obwohl ihre Präsenz im Vergleich zu anderen Plattformen immer noch relativ gering ist und sie offenbar nicht in der Lage sind, nennenswerte Einnahmen aus dem Hosting ihrer Inhalte auf der Plattform zu generieren. Da die Nutzungsbedingungen von Odysee durchaus die Verbreitung von Hass- und Gewaltinhalte untersagen, die sich gegen bestimmte Gruppen aufgrund von ethnischer Zugehörigkeit, Religion, Nationalität oder anderer Merkmale richten, ist das Auffinden von offen rassistischem, antisemitischem und faschistischem Material ein Hinweis auf die mangelnde Durchsetzung dieser Regeln.[61] Da einige dieser Inhalte wahrscheinlich in verschiedenen Staaten gegen geltende Gesetze verstoßen, könnte Odysee zunehmend unter Druck geraten, diese zu entfernen.

Insgesamt hat sich die Blockchain-Technologie, die Odysee zugrunde liegt, nicht als das erwartet gravierende Hindernis für den Datenzugriff erwiesen. LBRY stellt zu diesem Zweck eine Vielzahl von Tools für Entwickler:innen bereit. Die Anwendung der verfügbaren Tools zur Erforschung dieser Blockchain-basierten Plattform war jedoch äußerst zeitaufwendig und erforderte technologisches Fachwissen, das vielen anderen Organisationen möglicherweise nicht zur Verfügung steht. Komplikationen ergaben sich aus der Fragmentierung der Technologie, die Odysee zugrunde liegt. Dies erforderte die Erprobung und Integration mehrerer Tools, bevor auf die für die vorliegende

Forschungsarbeit benötigten Daten zugegriffen werden konnte. Darüber hinaus waren nicht alle diese Tools gut dokumentiert oder wurden nach denselben Standards gepflegt, was die Anforderungen an das technologische Fachwissen und den Zeitbedarf noch weiter erhöhte. Kleinere Plattformen wie Odysee verfügen in der Regel über weniger Personal und finanzielle Mittel als größere Technologieunternehmen, um diese Dienste zu pflegen. Das kann zu technischen Herausforderungen und Inkonsistenzen bei der Erhebung von Daten für Forschungszwecke führen. Die Verwendung neuartiger Technologien wie der Blockchain kann das Problem noch verschärfen, da die geringere Zahl der vorhandenen Expert:innen und Tools die Forscher:innen zur Anwendung weniger gut entwickelter und dokumentierter Ansätze zwingen könnte. Wo immer möglich, sollte die Plattform versuchen, diese Palette von Tools zu optimieren und eine umfangreichere, konsistentere und leichter zugängliche Begleitdokumentation bereitzustellen.

Die Nutzungsbedingungen von Odysee waren insbesondere in Bezug auf die Auslegung des Begriffs „personenbezogene Daten" (personal data) unklar und schufen damit potenzielle rechtliche Hindernisse für die im öffentlichen Interesse liegende Erforschung der Plattform. In Verbindung mit der Verfügbarkeit einer Vielzahl unterschiedlicher Kategorien und Arten von Daten führte dies dazu, dass wir bei der Datenerfassung und -analyse einen konservativeren Ansatz wählten, als technisch möglich gewesen wäre. Die Plattform sollte ihre Erwartungen präzisieren, hinsichtlich der Verwendung von Daten, die durch Dritte erhoben worden sind. Dies würde den Forscher:innen mehr Sicherheit geben und den Nutzer:innen ein besseres Verständnis über mögliche Verwendungen ihrer Daten vermitteln.

Fazit und Empfehlungen

Die diesem Bericht zugrunde liegenden Forschungsarbeiten zeigen, dass die digitale Forschung auf Plattformen wie Telegram, Discord und Odysee zwar grundsätzlich möglich ist, in der Praxis jedoch auf Hindernisse stößt, die ihre systematische, ethische und rechtskonforme Durchführung erschweren. Trotzdem konnten im Rahmen dieser Arbeit , nützliche Erkenntnisse gewonnen werden, insbesondere mit manuellen oder ethnografischen Methoden, die teilweise durch umfangreichere und systematischere Methoden zur Datenerfassung und -analyse ergänzt wurden.

Allerdings gab es auf den einzelnen Plattformen auch erhebliche Einschränkungen, die den Einsatz noch umfangreicherer Forschungsmethoden und -ansätze verhindert haben. Auf der einen Seite hinderten uns ethische Erwägungen in Bezug auf datenschutzrechtliche Vorgaben und Erwartungen daran, kleinere und besonders schädliche Communities auf Telegram zu untersuchen. Andererseits hielten uns rechtliche Bedenken hinsichtlich einer Verletzung der Nutzungsbedingungen (Verstöße gegen das Vertragsrecht) davon ab, systematisch Daten von Discord-Servern zu erfassen. Bei der Untersuchung von Odysee gab es wegen des öffentlichen Charakters der Plattform zwar weniger ethische Bedenken. Jedoch wurde eine gründlichere Analyse aufgrund einer Kombination aus technischer Komplexität und unklaren Nutzungsbedingungen ebenfalls erschwert.

Diese technologischen, ethischen, rechtlichen und fragmentierungsbedingten Hindernisse, auf die wir bei Telegram, Discord und Odysee gestoßen sind, sind zudem eng miteinander verknüpft und überschneiden sich teilweise. So hinderten uns beispielsweise rechtliche Bedenken daran, fragmentierungsbedingte Hindernisse durch systematische Suchmethoden auf Discord zu überwinden. Einige technologischen Besonderheiten bei Telegram haben wiederum erhebliche ethische Hindernisse aufgeworfen. Die komplizierte Integration mehrerer Tools für den Zugriff auf Daten von Odysee stellt ein weiteres potenzielles Hindernis dar. Darüber hinaus geht aus den Nutzungsbedingungen der Plattform nicht eindeutig hervor, ob es sich bei den durch die verschiedenen Tools bereitgestellten Daten um personenbezogene Daten im Sinne der angewandten Definition handelt, was zusätzlich zu ethischen und rechtlichen Unsicherheiten bei der Forschungsarbeit führt. Insofern schränken ethische und rechtliche Hindernisse die Möglichkeiten von Forscher:innen ein, Communities mit schädlichen Inhalten und Verhaltensweisen auf diesen Plattformen systematisch zu untersuchen, selbst wenn entsprechende technologische Mittel zur Verfügung stehen.

Implikationen für Forscher:innen

Unsere Forschungsarbeit hat aufgezeigt, wie Plattformen im öffentlichen Interesse liegende Forschung auf verschiedene Weise behindern können, wobei unklar ist ob die absichtlich oder unabsichtlich geschieht. Wie bereits erwähnt, können unklare rechtliche Rahmenbedingungen zu zusätzlichen Belastungen oder Risiken für Forscher:innen führen. Technologische Handlungsspielräume der Plattformen können den Zugang zu Daten oder gehosteten Inhalten verhindern oder die Datenerfassung aus technischer Sicht unnötig erschweren, beispielsweise wenn die Front-End- oder Back-End-Architekturen der Plattformen fragmentiert sind oder schlecht gepflegt werden, oder wenn die für den Datenzugriff verfügbaren Tools unzureichend dokumentiert sind. Auch die genaue Ausgestaltung der Plattformen kann zu ethischen Bedenken führen, beispielsweise wenn Online-Plattformen oder -Räume als privat bezeichnet werden, in der Praxis aber sowohl für Nutzer:innen als auch für Forscher:innen leicht und umfassend zugänglich sind.

Um die technologischen Möglichkeiten von Discord und insbesondere Odysee für die Forschung nutzbar zu machen, konnte sich unsere Arbeit an diesem Projekt auf die Expertise von CASM stützen. Dieses Fachwissen steht möglicherweise nicht allen Forscher:innen zur Verfügung, insbesondere nicht in der Zivilgesellschaft. Zudem waren wir dank des Zugangs zu externer, kostenloser Rechtsberatung in der Lage, die Nutzungsbedingungen der Plattformen und die sich daraus ergebenden rechtlichen Risiken im Zusammenhang mit dem Datenzugang sorgfältiger zu bewerten. Diese Faktoren erhöhen unter anderen Umständen zweifellos die Kosten und die Einstiegshürden für die Erforschung dieser Plattformen. Angesichts der beträchtlichen Vielfalt und Kombinationsmöglichkeiten, mit denen diese Hindernisse die Forschung erschweren können, stehen die Forscher:innen vor einzigartigen und komplexen Herausforderungen. Um die Tragweite der Herausforderung für die Forscher:innen zu veranschaulichen, sei auf

den im Rahmen der ersten Phase dieses Projekts veröffentlichten Bericht verwiesen. Dort hatten wir insgesamt 81 individuelle Plattformen oder Online-Dienste identifiziert, die von den von uns untersuchten englisch-, französisch- und deutschsprachigen extremistischen Communities genutzt werden. Ohne solide Mechanismen und Anreize für eine stärkere Zusammenarbeit innerhalb der Forschungsgemeinschaft besteht die Gefahr, dass ihre knappen Ressourcen zur Bewältigung dieser Herausforderungen unkoordiniert und isoliert eingesetzt und folglich Möglichkeiten zur Ausschöpfung von Skalierungseffekten verpasst werden.

Hinzu kommt, dass Plattformen sich gezielt auf rechtliche oder ethische Bedenken – beispielsweise in Bezug auf den Datenschutz oder das Recht der Nutzenden auf Privatsphäre – berufen, um externe Erforschung zu verhindern. Dies gilt mitunter sogar, wenn die Nutzer:innen der Weitergabe und Nutzung ihrer Daten für bestimmte, begrenzte Forschungszwecke ausdrücklich zugestimmt haben.[62] Ein solches Verhalten von Plattformen sowie unklar formulierte oder explizit gegen die Forschung im öffentlichen Interesse gerichtete Nutzungsbedingungen können problematische Anreize für Forscher:innen schaffen, wenn es darum geht, verschiedene rechtliche und ethische Risiken abzuwägen oder zu umgehen. .So kann es beispielsweise vorkommen, dass technologische Mittel zur Erfassung von Plattformdaten in Form von APIs von Drittanbietern, Scrapern oder Plugins für Crowdsourcing zur Verfügung stehen, deren Verwendung jedoch durch die Nutzungsbedingungen der Plattform untersagt ist. Dies kann Forscher:innen dazu veranlassen, zur Verbindung mit der Plattform täuschende Mittel einzusetzen. Das ist insbesondere dann ein ethisch fragwürdiger Ansatz, wenn die Plattform oder deren Nutzer:innen nicht über die Datenerhebung informiert wurden oder ihr nicht zugestimmt haben.

In diesen Fällen könnten die rechtlichen Risiken für Forscher:innen durch Täuschungen reduziert werden. Wenn Plattformen oder Nutzer:innen nicht bemerken, dass die Datenerfassung stattfindet, ist die Wahrscheinlichkeit deutlich geringer, dass rechtliche Schritte gegen Forscher:innen angestrengt werden. Die Anwendung solcher Methoden kann Forscher:innen jedoch auch davon abhalten, ihre Ergebnisse zu veröffentlichen, oder sie – im Falle einer Veröffentlichung – dazu veranlassen, unvollständige Angaben zu ihren Forschungsmethoden zu machen. Dies wirkt sich wiederum nachteilig auf die Qualität, Vergleichbarkeit und Reproduzierbarkeit der Online-Forschung zu wichtigen gesellschaftlichen Themen aus. Ebenso kann es zu einem allgemeinen Verlust des Vertrauens der Plattformen in die Forschungsgemeinschaft führen.

Insgesamt besteht ein dringender Bedarf für grundlegende Standards, die den Zugang zu Plattformdaten durch Forscher:innen sowohl in Bezug auf die Daten, auf die zugegriffen werden darf, als auch in Bezug auf die Art und Weise regeln, wie auf sie zugegriffen werden kann. Dies betrifft insbesondere die Erforschung neuer oder neu entstehender Online-Plattformen. Solche Standards würden dazu beitragen, das bestehende Ungleichgewicht im Kräfteverhältnis zwischen den Plattformen und den Forscher:innen auszugleichen.

Digitalpolitischer Kontext

Unabhängig von diesem Projekt sind wir auch bei der Erforschung von zahlreichen weiteren Plattformen im sich ständig weiterentwickelnden Online-Ökosystem auf vergleichbare Herausforderungen gestoßen.[63] Wie es aus dem Plattform-Scoping in Phase I des vorliegenden Projekts hervorgegangen ist, gibt es eine Vielzahl weiterer kleinerer und mittelgroßer Online-Plattformen, die ebenfalls von Extremist:innen und anderen schädlichen Akteur:innen genutzt werden. Wir gehen davon aus, dass sich dieser Trend noch verstärken wird, wenn größere Plattformen für diese Art von Communities und Aktivitäten weiter an Attraktivität verlieren, insbesondere wenn Regulierungsmaßnahmen wie das Gesetz über digitale Dienste (Digital Services Act, DSA) der EU greifen.[64] Es ist auch denkbar, dass einige Plattformen zumindest kurzfristig und/oder in Ländern, in denen der Datenzugang nicht gesetzlich reguliert ist, die bestehenden Möglichkeiten des Datenzugangs weiter einschränken oder zurücknehmen werden. Ohne strenge regulatorische Anforderungen an den Datenzugang könnten Plattformen dazu verleitet werden, sich der Beobachtung durch eine unabhängige Forschung zu entziehen, oder versuchen, von der Bereitstellung des Datenzugangs zu profitieren. So kündigte Twitter im Februar 2023 Änderungen an, die den freien Zugang zur plattformeigenen API einschränken. In diesem Zusammenhang wurde berichtet, dass Meta plane, den bestehenden Zugang zu Daten über das eigene Analysetool CrowdTangle zu sperren.[65]

Obwohl sich viele der vorgeschlagenen Maßnahmen zur Regulierung in erster Linie auf die größten und marktbeherrschenden Plattformen konzentrieren, können sich Änderungen der regulatorischen Rahmenbedingungen für Online-Plattformen bis zu einem gewissen Grad auch auf kleinere und mittlere Online-Plattformen auswirken. Je nach Rechtsprechung werden diese Plattformen dadurch verpflichtet, gegebenenfalls umfassendere und konsistentere Nutzungsbedingungen, mehr Transparenz und/oder einen besseren Zugang zu den Daten für Aufsichtsbehörden oder unabhängige Forscher:innen bereitzustellen. Sie müssen womöglich auch über Systeme verfügen, mit denen sie schnell und wirksam auf Meldungen über illegale Inhalte oder Aktivitäten auf ihren Plattformen reagieren können. Im Falle von Telegram könnte das gewaltige Wachstum der Plattform in den letzten Jahren dazu führen, dass diese bald den gleichen Anforderungen unterworfen wird wie andere etablierte große Plattformen. Zur Erfüllung dieser Anforderungen wären erhebliche Änderungen gegenüber der derzeitigen Funktionsweise erforderlich. Wenn mittelgroße Plattformen wie Discord in den kommenden Jahren weiter wachsen, könnten sie ebenfalls mit zusätzlichen regulatorischen Verpflichtungen konfrontiert werden, die größere Investitionen in die Inhaltsmoderation, Transparenz und den Datenzugang erfordern.

Kleinere Plattformen wie Odysee, die sich als „zensurfreie" Alternativen zu größeren, etablierten Tech-Unternehmen positioniert haben, werden wahrscheinlich ebenfalls vor eine Entscheidung gestellt: Wenn sie wachsen und langfristig rentabel wirtschaften wollen, müssen sie wahrscheinlich höhere regulatorische Anforderungen und Kontrollmaßnahmen erfüllen und benötigen zusätzliche technische und personelle Ressourcen, damit ihre Plattform die zunehmende Aktivität bewältigen kann. Dabei ist fraglich, inwieweit diese Entwicklungen bei den bestehenden Nutzer:innen, die diese Plattformen oft gerade wegen ihrer nachlässigen Umsetzung von Inhaltsmoderationsmaßnahmen wählen, auf Zustimmung stoßen werden. Sollten die Plattformen stattdessen versuchen, die Erwartungen der betreffenden Nutzer:innen oder Gemeinschaften zu befriedigen, indem sie sich der Einhaltung regulatorischer oder rechtlicher Anforderungen verweigern, müssen sie unter Umständen den Betrieb in bestimmten Ländern einstellen und/oder mit rechtlichen Schritten, bzw. Geldstrafen seitens der Aufsichtsbehörden rechnen, die versuchen, das Ausmaß der durch sie geförderten schädlichen Inhalte oder Verhaltensweisen einzudämmen.

Eine genaue Analyse der Regelungen und der Schwellenwerte für die Zahl der Nutzer:innen in den bestehenden oder geplanten Rechtsvorschriften der wichtigsten Rechtssysteme lässt erahnen, dass viele der in diesem Bericht angesprochenen Herausforderungen nicht vollständig bewältigt werden können. Die regulatorischen Maßnahmen stellen maßgeblich auf die Metrik „monatlich aktive Nutzer:innen" als zentrale Kennzahl ab. Bei Überschreitung eines bestimmten Schwellenwertes greifen die strengsten regulatorischen Anforderungen. Viele kleinere Plattformen, die dennoch ein erhebliches Online-Risiko darstellen, wären demnach auch weiterhin nicht verpflichtet, bestehende Hindernisse für den Datenzugang zu beseitigen. Der folgende Abschnitt gibt einen ersten Überblick über bestehende oder geplante Regulierungsmaßnahmen in den wichtigsten Rechtsordnungen sowie eine kurze Einschätzung, ob sie sich auf bestehende Forschungshindernisse auf kleinen und mittleren Online-Plattformen auswirken könnten. In der dritten und letzten Phase dieses Projekts werden wir die politischen Implikationen der von uns identifizierten Herausforderungen beim Datenzugang genauer untersuchen.

EU: Gesetz über digitale Dienste (Digital Service Act, DSA) und gestärkter Kodex zur Bekämpfung von Desinformation

Gemäß dem vom EU-Parlament im Juli 2022 verabschiedeten Gesetz für digitale Dienste (im Folgenden: Digital Services Act oder DSA) werden Plattformen als „sehr große Online-Plattformen" (VLOPs) bezeichnet, wenn sie ihre Dienste für aktive Nutzer:innen in der Union erbringen, deren durchschnittliche monatliche Zahl sich auf mindestens 45 Millionen Personen beläuft. Die Anbieter dieser sehr großen Online-Plattformen müssen den Zugang zu Daten in Echtzeit ermöglichen, sofern dies technisch machbar ist und die Daten öffentlich zugänglich sind (Art. 40). Zu den dort aufgezählten öffentlich zugänglichen Metriken zählen Daten zu „aggregierten Interaktionen mit Inhalten von öffentlichen Seiten, öffentlichen Gruppen (...), einschließlich Daten zu Wahrnehmung und Interaktion, wie z. B. die Anzahl der Reaktionen, Teilungen und Kommentare". Demnach müssten die Plattformen den Zugang zu den Daten

auf Verlangen der als Koordinator für digitale Dienste (Digital Services Coordinator, DSC) zuständigen staatlichen Aufsichtsbehörde am jeweiligen Niederlassungsort des Unternehmens in der EU oder der Europäischen Kommission (EC) innerhalb einer angemessenen Frist gewähren. Der DSC und die EC dürfen die bereitgestellten Daten dabei ausschließlich zur Überwachung und Bewertung der Einhaltung des DSA verwenden und müssen die Rechte und Interessen von Anbietern und Nutzer:innen berücksichtigen, einschließlich des Schutzes personenbezogener Daten und vertraulicher Informationen (Geschäftsgeheimnisse) sowie der Aufrechterhaltung der Sicherheit des Dienstes. Der Datenzugang müsste über geeignete Schnittstellen wie Online-Datenbanken oder APIs gewährt werden, die auf Verlangen des DCS oder der EC anzugeben wären.

Ebenso müssen die Anbieter zugelassenen Forscher:innen (vetted researchers) auf begründetes Verlangen des DSC Zugang zu Daten gewähren, die zur Aufspürung, zur Ermittlung und zum Verständnis der im DSA genannten systemischen Risiken in der Union beitragen. Die zugelassenen Forscher:innen (vetted researchers) müssen einer Forschungseinrichtung angeschlossen und von kommerziellen Interessen unabhängig sein sowie bestimmte mit dem Verlangen verbundene Anforderungen an den Datenschutz und die Datensicherheit erfüllen können. Forscher:innen müssen in ihren Anträgen die Notwendigkeit und Verhältnismäßigkeit des Datenzugangs für ihre Forschungsarbeiten nachweisen, ihre Finanzierung offenlegen und ihre Forschungsergebnisse frei und öffentlich zugänglich machen. Im Rahmen zukünftiger delegierter Rechtsakte (Sekundärrecht der Europäischen Union) sollen weitere Bedingungen, Verfahren und unabhängige Beratungsmechanismen zur Unterstützung der Datenweitergabe an externe Forscher:innen ergänzt werden. Anbieter werden personenbezogene Daten anonymisieren oder pseudonymisieren müssen, es sei denn, dies würde den verfolgten (und legitimen) Forschungszweck unmöglich machen.

Im Jahr 2022 führte die EU ferner den neuen gestärkten Kodex zur Bekämpfung von Desinformation (Strengthened Code of Practice on Disinformation) ein. Dabei handelt es sich um einen freiwilligen Verhaltenskodex mit derzeit 34 Unterzeichner:innen, darunter eine Reihe von Organisationen, die ein Interesse an der Bekämpfung von Desinformation haben: große Tech-Unternehmen wie Meta (Facebook und Instagram), Google (YouTube), TikTok, Microsoft und Twitch sowie eine Reihe kleinerer Unternehmen wie Clubhouse und Vimeo.[66] Im Abschnitt VI, in dem es um die Befähigung der Forschungsgemeinschaft geht (Empowering the Research Community) enthält der Kodex eine Reihe von Regeln für den Datenzugang, darunter die Verpflichtung Nr. 26 für die unterzeichnenden Plattformen, nicht-personenbezogene Daten und anonymisierte, aggregierte oder öffentliche Daten für die Zwecke der Forschung über Desinformation bereitzustellen. Wie beim DSA sollten die Plattformen maschinenlesbare Daten in Echtzeit (oder nahezu in Echtzeit) über APIs oder andere offene und zugängliche technische Mechanismen zur Verfügung stellen und sicherstellen, dass angemessene Instrumente und Prozesse implementiert sind, mit denen die Risiken des Missbrauchs (z. B. durch böswillige oder kommerzielle Nutzung von Daten) minimiert werden sollen. Um sich zu qualifizieren, müssen beantragte Forschungsvorhaben ethischen und methodischen Best Practices entsprechen, wie sie beispielsweise im Entwurf des Verhaltenskodex der Europäischen Beobachtungsstelle für digitale Medien (EDMO) für den Zugang zu Plattformdaten (Code of Conduct on Access to Platform Data) beschrieben sind. Den Forschungsteams können dabei sowohl Personen aus zivilgesellschaftlichen als auch aus akademischen Organisationen angehören.[67] Außerdem enthält der gestärkte Kodex zur Bekämpfung von Desinformation die Verpflichtung Nr. 27 zur Schaffung einer unabhängigen Stelle für die Zulassung von Forscher:innen und Forschungsvorschlägen.

Von den in diesem Bericht bewerteten Plattformen wird voraussichtlich keine den im DSA festgelegten Schwellenwert erreichen, ab dem diese Anforderungen zu erfüllen sind.[viii] Daraus ergibt sich, dass die Anforderungen des DSA zwar einen signifikanten Beitrag dazu leisten würden, die derzeitigen Forschungshindernisse auf größeren Plattformen abzubauen. Zur Lösung der in dem vorliegenden Bericht beschriebenen Herausforderungen im Zusammenhang mit kleineren oder mittelgroßen Plattformen könnten sie jedoch kaum beitragen. Ebenso wenig hat bisher eine der in diesem Bericht untersuchten Plattformen den gestärkten Kodex zur Bekämpfung von Desinformation unterzeichnet. Das bedeutet, dass auch der Kodex die Forschungshindernisse auf kleineren und mittleren Plattformen wie Telegram, Discord oder Odyssee nicht beseitigen wird, solange diese sich nicht selbst zur Einhaltung der Verhaltensregeln verpflichten.

viii Telegram beziffert die Zahl seiner Nutzer:innen auf 38,5 Millionen und liegt damit unterhalb des in der EU geltenden Schwellenwertes von 45 Millionen Nutzer:innen, ab dem die Plattform zu den VLOPs zählen würde. FAQ. *Telegram.* URL: https://telegram.org/faq.

USA: Platform Transparency and Accountability Act (PATA) und Digital Services Oversight and Safety Act (DSOSA)

Ähnlich wie der DSA der EU sehen auch die Gesetzesentwürfe in den USA wie PATAix und DSOSAx Schwellenwerte für die Zahl der monatlich aktiven Nutzer:innen vor und machen damit die gesetzlichen Verpflichtungen der Plattformen von deren Größe abhängig. Gemäß PATA müssten Plattformen, die nutzergenerierte Inhalte hosten, mindestens 25 Millionen monatlich aktive Nutzer:innen in den USA haben, um unter die Regelung zu fallen (vgl. PATA Section 2). Nach dem Gesetz soll die National Science Foundation (NSF) bestimmen, welche Daten und Informationen die Plattformen den zugelassenen Forscher:innen zur Verfügung stellen müssen. Die Bereitstellung muss für die Plattform machbar sein, in einem angemessenen Verhältnis zu den Forschungsbedürfnissen stehen und darf keine unzumutbaren Belastungen für die Plattform darstellen (Section 4). Gemäß PATA müssen qualifizierte Forscher:innen einer Universität angehören und bei der National Science Foundation (NSF) einen Antrag für ihren spezifischen Forschungsvorhaben (research proposal) einreichen (Section 2). Die NSF soll darüber hinaus ein Verfahren zur Annahme von Forschungsanträgen von Forscher:innen einrichten und Richtlinien und Kriterien zur Bewertung dieser Anträge festlegen (Section 4).

Ferner soll nach dem Gesetzentwurf innerhalb der Federal Trade Commission (FTC) ein Platform Accountability and Transparency Office (PATO) eingerichtet werden, das die Plattformen über Forschungsanträge informiert und Schutzmaßnahmen für den Datenschutz und die Cybersicherheit bei der Weitergabe der betreffenden Daten festlegt. Zu diesen Maßnahmen kann beispielsweise die Verschlüsselung oder Anonymisierung von Daten zum Schutz der Privatsphäre einzelner Nutzer:innen zählen (Section 4). Bevor sie ihre Ergebnisse veröffentlichen könnten, müssten die Forscher:innen der betreffenden Plattform und dem PATO eine Vorabversion zur Bewertung vorlegen, um zu bestätigen, dass bei der Veröffentlichung der Forschungsarbeit keine personenbezogenen Daten, Betriebsgeheimnisse oder vertraulichen Geschäftsinformationen offenlegt werden (Section 5). Der PATA würde Forscher:innen durch die Schaffung eines „sicheren Hafens" zusätzlichen Schutz bieten, um zu verhindern, dass Plattformen rechtliche Schritte gegen Forscher:innen einleiten, die einvernehmlich und unter Wahrung sonstiger Datenschutzmaßnahmen Zugang zu Informationen erhalten (Section 11). Schließlich würde es der Gesetzentwurf der FTC auch ermöglichen, Transparenzberichte oder meldepflichtige Angaben anzufordern, die für die Öffentlichkeit zugänglich und nachvollziehbar oder für die Analyse durch Forscher:innen, Journalist:innen und die Öffentlichkeit über Mechanismen wie APIs zugänglich sind. Dazu könnten Werbe-Bibliotheken (Ad-Libraries), Informationen über weit verbreitete Inhalte und Entscheidungen zur Inhaltsmoderation, bzw. Angaben zu den Algorithmen gehören (Section 12).

Der DSOSA, der in gewissem Maße dem DSA der EU nachempfunden ist, legt die Schwelle für Plattformen, die den Regelungen für große Plattformen unterliegen (large covered platforms), auf 66 Millionen monatlich aktive Nutzer:innen und für darin regulierte Plattformen (covered platforms) auf 10 Millionen fest. Analog zum Entwurf für den PATA würde der Gesetzentwurf die FTC dazu verpflichten, Regeln für die Arten von Daten zu erlassen, die zertifizierten Forscher:innen zur Verfügung gestellt werden sollten (Section 10 (c)). Die FTC müsste dabei auch die Arten und Mechanismen des Datenzugriffs festlegen und dabei unter anderem die Größe der Datensätze und die Erfassungsmethoden berücksichtigen, mit denen sie erstellt werden. Die nach dem Gesetzentwurf als „large covered platforms" eingestuften Plattformen müssten außerdem eine detaillierte Werbe-Bibliothek bereitstellen (Section 10(f)). Auch müssten sie Metriken für öffentliche Inhalte mit hoher Reichweite und hohem Engagement bereitstellten sowie transparente Angaben über Inhalte machen, die über die Mechanismen der Plattform verstärkt werden (Section 10(g)). Die FTC könnte die Einrichtung eines staatlich finanzierten Forschungs- und Entwicklungszentrums (Federally Funded Research and Development Center, FFRDC) veranlassen, um den Informationsaustausch zwischen den regulierten Plattformen und zertifizierten Forscher:innen zu erleichtern. Die FTC müsste auch sicherstellen, dass der Datenzugriff die berechtigten Erwartungen der Nutzer:innen an deren Privatsphäre nicht verletzt (beispielsweise indem die Plattformen verpflichtet werden, alle Informationen zu anonymisieren, die nicht als öffentliche Inhalte gelten) und den Einsatz datenschutzfreundlicher Technologien erwägen (Section 10 (c)).

ix PATA – Der Wortlaut des Gesetzentwurfes ist hier abrufbar. Eine Zusammenfassung der einzelnen Sections des Gesetzentwurfes ist hier abrufbar.
x DSOSA – Der Wortlaut des Gesetzentwurfes ist hier abrufbar. Eine Zusammenfassung der einzelnen Abschnitte des Gesetzentwurfes ist hier abrufbar.

Der Gesetzentwurf sieht ebenfalls die Schaffung einer Einrichtung zur Förderung der unabhängigen Forschung (Office of Independent Research Facilitation) bei der FTC vor. Forscher:innen aus Wissenschaft und Zivilgesellschaft, die die Auswirkungen von Inhaltsmoderationsprozessen, Produktdesignentscheidungen und Algorithmen auf die Gesellschaft und die Politik sowie auf die Verbreitung von Hass, Hetze und Extremismus, die Sicherheit, den Datenschutz sowie die körperliche und geistige Gesundheit untersuchen, würden von dieser Einrichtung zertifiziert werden (Sec. 10 (a)). Als qualifizierungsberechtigte Forschungseinrichtungen gelten Hochschuleinrichtungen oder gemeinnützige Organisationen (501(c)(3)), zu deren Aufgaben es gehört, das Verständnis für die Auswirkungen von Plattformen auf die Gesellschaft zu vertiefen. Sie müssen dazu in der Lage sein, sowohl die Regeln für den sicheren Zugang für Forscher:innen einzuhalten als auch geeignete datenwissenschaftliche sowie investigative und qualitative Forschungsmethoden und Best Practices anzuwenden (Section 10 (b)). Der Gesetzentwurf würde auch den Schutz zertifizierter Forscher:innen gewährleisten, wenn diese ausschließlich für ein Forschungsprojekt Accounts auf Plattformen einrichten oder Informationen erfassen, die von Nutzer:innen zu Forschungszwecken zur Verfügung gestellt werden (beispielsweise über eine Browsererweiterung oder ein Plugin), wenn die jeweiligen Nutzer:innen ihre Einverständniserklärung gegeben haben (Section 10(c)).

Wie beim DSA im EU-Kontext werden die in diesen Entwürfen festgelegten Schwellenwerte wahrscheinlich dazu führen, dass viele kleinere Plattformen nicht unter die Regelungen fallen. Während einige mittelgroße Plattformen wie Telegram oder Discord den niedrigeren Schwellenwert von 10 Millionen Nutzer:innen erreichen und im Sinne des DSOSA als Plattformen dieser Größe (covered platforms) bestimmten Regelungen unterliegen, zielen die einschneidendsten Anforderungen an den Datenzugang auf große Plattformen (large covered platforms) ab. Infolgedessen würde keiner der beiden Entwürfe die Forschungshindernisse, auf die wir bei unserer Arbeit für diesen Bericht auf kleineren Plattformen gestoßen sind, wirksam abbauen. Ferner ist anzumerken, dass die Wahrscheinlichkeit, dass diese Gesetzesentwürfe auf US-Bundesebene im Kongress verabschiedet werden, gering ist, da die Exekutive ein größeres Interesse an Gesetzen hat, die sich auf den Schutz der Privatsphäre und den Wettbewerb konzentrieren. Außerdem gibt es parteipolitische Differenzen über die weitere Vorgehensweise bei der Regulierung der sozialen Medien (abgesehen von der Regulierung, die speziell auf den Schutz der Online-Sicherheit von Kindern abzielt, die bessere Aussichten haben könnte). Dies lässt vermuten, dass die USA zumindest kurz- bis mittelfristig bei der Einführung neuer Vorschriften für den Datenzugang gegenüber anderen Rechtsordnungen zurückbleiben könnten.

Großbritannien: Online Safety Bill (OSB)

Dem Gesetzesentwurf für die Online Safety Bill (OSB) fehlt es in seiner aktuellen Form (Stand Februar 2023) noch an Klarheit über eine mögliche zukünftige Datenzugriffsregelung. Als zuständige Aufsichtsbehörde könnte das Office of Communications (Ofcom) Daten von den Plattformen anfordern und diese möglicherweise mit ausgewählten Drittorganisationen teilen, um unterstützende Forschungsarbeiten durchzuführen. Innerhalb von zwei Jahren nach Verabschiedung des Gesetzes müsste das Ofcom außerdem einen Bericht erstellen, in dem erläutert wird, wie und in welchem Umfang diejenigen, die unabhängige Forschungen zur Online-Sicherheit betreiben, zu diesem Zeitpunkt Informationen von regulierten Plattformen erhalten können. In dem Bericht sollen auch rechtliche und andere Aspekte erörtert werden, die derzeit den Zugang zu den Daten beschränken, sowie eine Bewertung, inwieweit ein besserer Zugang erreicht werden könnte. Nach der Veröffentlichung des Berichts könnte Ofcom zusätzliche Leitlinien für regulierte Plattformen und Forscher:innen erstellen. Im Vergleich zum DSA enthält die OSB relativ schwache Bestimmungen und bietet wenig Klarheit über die Datenzugangsregelungen für Forscher:innen, die möglicherweise erst in einigen Jahren nach Inkrafttreten der neuen Regelung geklärt werden. Es bleibt daher unklar, inwieweit die OSB geeignet sein wird, den in diesem Bericht angesprochenen Forschungshindernissen für den Datenzugang auf großen, mittleren oder kleinen Plattformen entgegenzuwirken.

Deutschland: Netzwerkdurchsetzungsgesetz (NetzDG)

Das erstmals 2017 vorgestellte und 2021 aktualisierte NetzDG ist ein Beispiel für eine frühere Generation der inhaltsorientierten Digitalpolitik, die sich auf die Entfernung von illegalen Online-Inhalten in Deutschland konzentriert.[68] Auch dieses Gesetz sieht einen Schwellenwert für die Zahl der Nutzer:innen vor, ab dem die

Plattformen in seinen Geltungsbereich fallen. Dieser liegt bei zwei Millionen oder mehr registrierten Nutzer:innen in Deutschland. Das Gesetz enthält in § 5a verschiedene Regelungen zum Datenzugang, die es Forscher:innen ermöglichen, vom Plattformanbieter qualifizierte Auskünfte zu verlangen. Dazu gehören Informationen über die Verbreitung von Inhalten, die Gegenstand von Beschwerden waren oder die vom Anbieter gesperrt oder entfernt worden sind, Informationen darüber, welche Nutzer:innen in welcher Weise mit den Inhalten interagiert haben, sowie die „Trainingsdaten von Verfahren zur automatisierten Erkennung von Inhalten, die entfernt oder gesperrt werden sollen". Die angeforderten Daten müssen „für Vorhaben einer im öffentlichen Interesse liegenden wissenschaftlichen Forschung zu Art, Umfang, Ursachen und Wirkungsweisen öffentlicher Kommunikation in sozialen Netzwerken und den Umgang der Anbieter hiermit" erforderlich sein. Darüber hinaus gibt es keine Beschränkungen für die Arten von Organisationen oder Forscher:innen, die diese Regelungen in Anspruch nehmen können.

Das Gesetz sichert den Anbietern eines sozialen Netzwerks gegenüber den Forscher:innen einen Anspruch auf Erstattung der durch die Auskunftserteilung entstehenden Kosten von bis zu 5.000 Euro (in Ausnahmefällen kann dieser Betrag überschritten werden) zu. Um Auskünfte zu erhalten, müssen die Forscher:innen dem Anbieter ein Datenschutzkonzept vorlegen. Dieses Schutzkonzept beinhaltet beispielsweise „eine Beschreibung der Vorkehrungen, um eine anderweitige Verwendung der Informationen zu verhindern" und „eine Beschreibung der technischen und organisatorischen Maßnahmen, die den Schutz der personenbezogenen Daten sicherstellen". Soweit dies ohne Gefährdung des Forschungszwecks möglich ist, müssen die Anbieter die Daten anonymisiert oder zumindest pseudonymisiert übermitteln. Die genauen Mechanismen für die Datenfreigabe (z. B. über eine API) sind jedoch nicht spezifiziert. Auch wurden die Regelungen des NetzDG für den Datenzugriff von Forscher:innen bisher noch nicht in großem Umfang genutzt, möglicherweise wegen der damit verbundenen Kosten. Damit hat sich das NetzDG auch nach mehreren Jahren seines Bestehens nicht als wirksam erwiesen, wenn es darum geht, den Datenzugang für Forscher:innen auf großen, mittleren oder kleineren Plattformen zu erleichtern.

Empfehlungen

Auf der Grundlage der in diesem Bericht dargestellten Ergebnisse und Implikationen für Forscher:innen sowie der Darstellungen über den Stand der bisherigen politischen Regulierungsanstrengungen sprechen wir in diesem Abschnitt eine Reihe von übergreifenden Empfehlungen für Anbieter von Online-Plattformen, politische Entscheidungsträger:innen und Aufsichtsbehörden sowie für zivilgesellschaftliche und akademische Forscher:innen aus. Diese Vorschläge sollen dazu beitragen, die verschiedenen technologischen, ethischen und rechtlichen Hindernisse sowie die bei der Forschungsarbeit häufig festgestellte Fragmentierung zu überwinden.

Uns ist bewusst, dass manche unserer Empfehlungen insbesondere für kleinere Plattformen mit weniger Ressourcen oder geringen technischen Möglichkeiten zusätzlichen Aufwand bedeuten. Gegenwärtig stellen die Plattformen jedoch eher praktische Funktionen zur Erleichterung der Kommunikation und Koordinierung von schädlichen Akteur:innen bereit, während sie nur eingeschränkte oder unzureichende Funktionen für die im öffentlichen Interesse liegende Forschung in Bezug auf diese Online-Räume bieten. Dieses Ungleichgewicht gilt es aus unserer Sicht zu beseitigen.

Technologische Hindernisse

In modernen Online-Räume werden in kürzester Zeit immer größere Inhaltsmengen produziert, was ihre Erforschung vor gewaltige Herausforderungen stellt. Ein technologischer Ansatz für den Zugriff auf relevante Daten wird oft bewusst verhindert oder ist wegen komplizierter Plattformstrukturen oder unzureichend dokumentierter Technologien nicht anwendbar. Dies hat erhebliche Auswirkungen auf die im öffentlichen Interesse liegende Forschung, insbesondere für Organisationen mit begrenztem Zugang zu entsprechenden Technologien. Mit der zunehmenden Verbreitung neuartiger Technologien wie Blockchain erhöht sich diese Komplexität weiter, während davon auszugehen ist, dass immer weniger Forscher:innen über die erforderlichen technologischen Werkzeuge und das erforderliche Fachwissen zur effektiven Untersuchung der betreffenden Plattformen verfügen.

- **Plattformen sollten Drittanbietern, die im öffentlichen Interesse liegende Forschung betreiben, einen autorisierten Datenzugang – beispielsweise über APIs – bereitstellen**. Begleitend sollte eine klare, konsistente und öffentlich zugängliche Dokumentation verfügbar gemacht werden, die Angaben zu den Datentypen enthält, die erfasst werden können. Zum Schutz der Privatsphäre der Nutzer:innen sollte gleichzeitig die Erfassung sensibler personenbezogener Daten ausreichend begrenzt werden. Soweit möglich, sollten die Plattformen die Anwendungsfreundlichkeit ihrer Tools optimieren, die sie direkt für den Datenzugriff bereitstellen, sodass Forscher:innen nicht mehrere Tools mit sich überschneidenden Funktionen verwenden müssen.
- **Die politischen Entscheidungsträger:innen und Aufsichtsbehörden sollten einen präzisen, zuverlässigen und für die im öffentlichen Interesse liegende Forschung ausreichenden Datenzugang für alle Plattformen vorschreiben. Dies würde nicht nur die derzeit größten Plattformen betreffen, sondern das breite Spektrum kleinerer und mittlerer Online-Plattformen mit einbeziehen**. Das ist von entscheidender Bedeutung, um ein besseres Verständnis darüber zu gewinnen, wie rechtswidrige oder schädliche Online-Aktivitäten zunehmend auf kleineren und mittelgroßen Plattformen stattfinden oder koordiniert werden, die trotz geringerer Reichweite erhebliche Risiken darstellen können. Soweit möglich, sollten die politischen Entscheidungsträger:innen auch länderübergreifend zusammenarbeiten, um einheitliche Anforderungen an den Datenzugang für Plattformen zu schaffen und im Laufe der Zeit optimierte Verfahren sowohl für Plattformen als auch für Forscher:innen zu entwickeln. Dadurch könnten auch unverhältnismäßige Belastungen für kleinere Unternehmen vermieden werden.
- **Akademische und zivilgesellschaftliche Forscher:innen sollten sich über wirksame Ansätze und Instrumente zur Datenerfassung sowie über die Erfahrungen austauschen, die sie beim Zugriff auf die wachsende Vielfalt von Plattformen im sich entwickelnden Online-Ökosystem gemacht haben**. Bei Plattformen, die mehr technisches Fachwissen für den Zugriff auf Daten erfordern, kann ein erheblicher Zeitaufwand für das Testen potenzieller Optionen anfallen. Die Forschungsgemeinschaft (und ihre Finanzierenden) sollte vermeiden, dass Forschungsarbeit nicht reproduzierbar ist oder Forscher:innen die Vorarbeit anderer nicht nutzen können. Wo immer möglich, sollten sie stattdessen Skaleneffekte anstreben und die Hürden für die gemeinsame Nutzung von Methoden, Tools und Ansätzen abbauen. Dies könnte durch sektorübergreifende Initiativen wie die Coalition for Independent Tech Research oder durch neu entstehende unabhängige Datenzugangsstellen koordiniert werden, wie sie vom European Digital Media Observatory (EDMO) oder der Carnegie Endowment for International Peace (CEIP) vorgeschlagen wurden.[69]

Hindernisse durch Fragmentierung

Neben der folgenden spezifischen Empfehlung in Bezug auf systematische Suchfunktionen auf Plattformen würden die vorstehenden Empfehlungen zur Überwindung technologischer Hindernisse ebenfalls dazu beitragen, die von uns identifizierten fragmentierungsbedingten Hindernisse zu beseitigen.

- **Plattformen sollten einen systematischen Datenzugang bereitstellen, der es Forschern:innen ermöglicht, zuverlässig auf akkurate Daten aus allen öffentlichen Bereichen der Plattform zuzugreifen**, damit die Forscher:innen untersuchungswürdige Online-Räume oder Communities nicht erst manuell erkunden müssen. Dies würde nicht nur einen größeren Umfang, sondern auch eine gezieltere Forschung ermöglichen, da die relevanten Communities (und damit die Daten) leichter identifiziert werden könnten. Unabhängig davon, ob für die systematische Suche plattformeigene oder Drittanbieter-Tools eingesetzt werden, sollte die Zuverlässigkeit, Vollständigkeit und Genauigkeit solcher Tools beispielsweise durch eine unabhängige Prüfung nachgewiesen werden, die durch Forscher:innen oder Aufsichtsbehörden durchgeführt werden könnte.

Ethische Hindernisse

Als eine der größten Herausforderungen bei diesem Projekt hat sich die Frage herauskristallisiert, wie das Recht auf Privatsphäre geschützt werden und gleichzeitig eine im öffentlichen Interesse liegende Forschung über Communities mit schädlichen Inhalten und Verhaltensweisen erfolgen kann. Leider gibt es für die Bezeichnung „privater Raum“

keine einheitliche Begriffsbestimmung, sodass es für Forscher:innen schwierig ist, private und öffentlichen Räume zu unterscheiden. Andererseits erlaubt das Fehlen eines solchen gemeinsamen Verständnisses darüber, was einen privaten Raum ausmacht, den Plattformen, die Transparenz und den Zugang zu vermeintlich privaten Räumen zu beschränken, die wegen des relativ problemlosen Beitritts dennoch einen eher öffentlichen Charakter haben.

Wie wir bereits dargelegt haben, sollten Faktoren wie die Größe, der Zweck, die Zugänglichkeit und die Art der Beziehungen zwischen den Nutzern:innen eines Kanals oder einer Community bei der Klassifizierung als öffentlicher oder privater Raum berücksichtigt werden.[70] Zudem besteht die Gefahr, dass rechtswidrige oder schädliche Online-Aktivitäten, die offen in vermeintlich privaten Online-Räumen stattfinden, zu Unsicherheit führen und die Argumente für den Schutz der Privatsphäre (z. B. durch Verschlüsselung) in tatsächlich privaten Online-Räumen und Kommunikationsmitteln untergraben.

- **Plattformen sollten eine angemessene Grenze für die Anzahl der in privaten Gruppen und Kanälen teilnehmenden Nutzer:innen festlegen und Online-Bereiche mit einem Nutzerkreis ab einem bestimmten Schwellenwert als öffentlich deklarieren**. Dies sollte auch dazu beitragen, sowohl den Nutzer:innen der Plattformen als auch den unabhängigen Forscher:innen mehr Klarheit darüber zu verschaffen, was in diesen Bereichen zulässig ist und welche Arten von Daten mit angemessenen Vorkehrungen zum Schutz der Privatsphäre und des Datenschutzes für Dritte zugänglich sein können. Inhalte, für die keine berechtigten Erwartungen an den Datenschutz bestehen, weil sie beispielsweise auf öffentlichen Seiten gepostet werden, sollten einschließlich der relevanten Metriken zu deren Reichweite (reach), Impressionen (impressions) und Engagement über einen zugelassenen API-Zugang zugänglich gemacht werden.
- **Falls die Plattformen solche Veränderungen auf freiwilliger Basis nicht umsetzen, sollten die politischen Entscheidungsträger:innen in Erwägung ziehen, verbindliche Anforderungen für die Unternehmen festzulegen, die sie dazu verpflichten, klarzustellen, welche Bereiche ihrer Plattformen tatsächlich öffent licher oder privater Natur sind, und angemessene Schwellenwerte zur Begrenzung der Zahl der Nutzer:innen bestimmen, die an privaten Online-Räumen teilnehmen**. Anstatt pauschale Schwellenwerte in diesem Bereich festzulegen, könnten die Unternehmen im Rahmen der Regulierung verpflichtet werden, ihrerseits klare und angemessene Grenzwerte festzulegen, die sich nach der Art ihrer Plattformen richten und auf Risikobewertungen basieren, die die spezifischen Merkmale oder Funktionen der betreffenden Plattform (z. B. Verschlüsselung) sowie die Risiken und potenziellen Schwachstellen berücksichtigen. Im Rahmen der Regulierung könnten die Plattformen darüber hinaus angehalten werden, den Nutzer:innen deutlich zu machen, welche Aspekte ihrer Plattformen eher öffentlich oder eher privat sind, und welche Konsequenzen dies für die Privatsphäre der Nutzer:innen und den Zugriff von Forscher:innen oder Dritten auf ihre Daten hat. Eine unabhängige Aufsichtsbehörde könnte schließlich auf der Grundlage der Risikobewertung beurteilen, ob der von der Plattform festgelegte Grenzwert angemessen ist und die festgestellten Risiken oder Schäden ausreichend mindert.
- **Die Forschungsgemeinschaft sollte sich dafür einsetzen, ethische Ansätze für die wissenschaftliche Untersuchung öffentlicher, halbprivater und privater Online-Räume zu formalisieren. Diese sollten der potenziellen Schwere der Risiken gerecht werden, die von diesen Räumen ausgehen können**. Solche Ansätze müssen das Recht auf Privatsphäre mit den Rechten derer abwägen, die geschädigt werden könnten, wenn diese Bereiche für Forscher:innen unzugänglich bleiben. Dies ist umso wichtiger, je größer diese Räume sind und je weniger gründlich deren Inhalte moderiert werden. Solche Anstrengungen sollten auf der bestehenden und gut etablierten Ethik der Online-Forschung aufbauen. Die Koordinierung könnte durch bestehende Initiativen wie die Association of Internet Researchers (AoIR) oder die bereits erwähnten potenziellen zukünftigen unabhängigen Datenzugangsstellen (z. B. EDMO) erfolgen.[71]

Rechtliche Hindernisse

- **Die Plattformen sollten in ihren Nutzungsbedingungen nicht nur die zulässigen Arten von Inhalten und Aktivitäten definieren, sondern auch eindeutige Vorgaben festlegen für die Anwendung dieser**

Nutzungsbedingungen auf den Datenzugriff durch Forscher:innen. Anschließend sollten diese konsequent durchgesetzt werden. Die Nutzungsbedingungen sollten nicht dazu dienen, die Plattform wirksam vor einer öffentlichen Beobachtung abzuschirmen, sondern sie die im öffentlichen Interesse liegende Forschung unter Wahrung des Datenschutzes ermöglichen. Eindeutigere Nutzungsbedingungen würde auch klare Erwartungen hinsichtlich der Verwendung der durch Dritte erfassten Daten schaffen. Dies würde den Forscher:innen mehr Sicherheit geben und den Nutzer:innen ein besseres Verständnis hinsichtlich der potentiellen Verwendungen ihrer Daten ermöglichen.

- **Die politischen Entscheidungsträger:innen sollten Rechtsschutz für Forscher:innen gewährleisten, die unter Wahrung der Datenschutzvorkehrungen im öffentlichen Interesse liegende Online-Forschung betreiben**. Sofern Forscher:innen verhältnismäßige Methoden und Ansätze verwenden und geeignete Vorkehrungen treffen, um die Privatsphäre der Nutzer:innen zu schützen, sollten sie nicht dem potenziellen Risiko rechtlicher Schritte seitens der Plattformen ausgesetzt werden, wenn sie wichtige gesellschaftliche Fragenstellungen in Bezug auf das Ausmaß und die Folgen rechtswidriger oder schädlicher Aktivitäten im öffentlichen Online-Raum erforschen. Dies ist besonders dann wichtig, wenn die Nutzungsbedingungen einer Plattform unvollständig, unklar oder missverständlich sind. Plattformen sollten sich der Kontrolle nicht völlig entziehen können, indem sie den Datenzugriff in ihren Nutzungsbedingungen pauschal verbieten. Anstelle von staatlich eingeführten gesetzlichen Schutzmaßnahmen für Forscher:innen sollten verantwortungsbewusste Plattformen freiwillige Ausnahmen in ihren Nutzungsbedingungen vorsehen, um Forschungsmethoden wie eine Datenerfassung über Crowdsourcing (unter Einholung einer Einverständniserklärung der Nutzer:innen durch die Forscher:innen) zu ermöglichen.
- **Akademische und zivilgesellschaftliche Forscher:innen sollten ebenfalls die Chance nutzen, ihre Expertise über die rechtlichen Implikationen beim Zugang zu Plattformdaten zu teilen oder zu bündeln**. Die rechtliche Überprüfung der Nutzungsbedingungen einer Plattform und anderer damit verbundener Bedingungen oder Bestimmungen kann zeitaufwendig, ressourcenintensiv und oft länderspezifisch sein. In Anbetracht der Tatsache, dass Forscher:innen mitunter keinen Zugang zu externer datenschutz- und vertragsrechtlicher Beratung haben, könnte eine stärkere Koordinierung und gemeinsame Nutzung von Ressourcen und Expertisen dazu beitragen, rechtliche Risiken und Einstiegshürden für die Online-Forschung zu verringern und damit die Chancengleichheit unter den Forscher:innen zu erhöhen. Wie bei den vorstehenden Empfehlungen zum Abbau der technologischen und ethischen Forschungshindernisse sollte auch diese Art der sektorübergreifenden Zusammenarbeit nach Möglichkeit durch bestehende Initiativen erleichtert werden.

Ausblick

Insgesamt ist gegenwärtig noch immer unklar, wie sich die Bedingungen für den Zugang zu Plattformdaten für wissenschaftliche Zwecke in Zukunft entwickeln werden. Obwohl die bestehenden und geplanten Regulierungsmaßnahmen in den wichtigsten Rechtsordnungen vielversprechend sind, was die Verbesserung der Transparenz der Plattformen und des externen Datenzugriffs insbesondere für die größten Plattformen angeht, bestehen für Plattformen Anreize, den Zugang zu Daten zu verwehren oder in vielen Fällen weiter einzuschränken. Es bleibt abzuwarten, ob die Regulierungsmaßnahmen in wichtigen Rechtsordnungen wie der EU einen Übertragungseffekt haben werden, indem Plattformen in diesem Zusammenhang dazu übergehen, einen ähnlichen Zugang auch in Staaten zu gewähren, in denen sie gesetzlich nicht dazu verpflichtet sind.

Die geplanten Regulierungsmaßnahmen werden den Status quo in Bezug auf viele kleinere oder mittelgroße Plattformen nicht wesentlich verbessern, da diese den schärferen Anforderungen an den Datenzugang nicht unterliegen werden. Dies dürfte dazu führen, dass die Benachteiligung von Forscher:innen gegenüber vielen Plattformen fortbestehen wird, wobei es kaum Garantien dafür gibt, dass sich diese Situation nicht noch verschlechtert. So könnten einige Unternehmen versuchen, den Datenzugriff mit technischen oder rechtlichen Mitteln einzuschränken, um weitere aufsichtsbehördliche oder unabhängige Untersuchungen schädlicher Inhalte oder Verhaltensweisen und der damit verbundenen Risiken auf ihren Plattformen zu vermeiden. Unabhängig davon, wie sich die Bedingungen für den Datenzugang entwickeln, wird sich das Online-Ökosystem zwangsläufig weiterentwickeln.

Damit erhöhen sich die Anzahl, Vielfalt und Komplexität der Online-Plattformen, deren Daten für Forscher:innen von Interesse sein könnten.

Um in der gegenwärtigen Situation eine Verbesserung herbeizuführen, sollten die politischen Entscheidungsträger:innen mindestens die Einführung gesetzlicher Ausnahmen oder Schutzmaßnahmen für Forscher:innen erwägen, die unter Wahrung des Datenschutzes eine im öffentlichen Interesse liegende Online-Forschung betreiben. Politische Entscheidungsträger:innen sollten versuchen, Plattformen verstärkt durch nicht regulatorische Mittel anzuregen und zu unterstützen, damit diese freiwillig Tools bereitstellen, die strukturierte und genaue Daten liefern. Dies betrifft insbesondere Plattformen, die unterhalb der regulatorischen Schwellenwerte liegen und damit nicht unter die Regelungen für strengere Anforderungen an den Datenzugang fallen würden. Viel wünschenswerter wäre überdies ein Szenario, in dem die Forschungshindernisse nicht nur durch zusätzliche Regulierung deutlich abgebaut werden, sondern in dem auch die Plattformen den Forscher:innen einen einvernehmlichen, standardisierten und die Privatsphäre wahrenden Datenzugang mit garantierten Mindeststandards für die Genauigkeit und klar formulierten Nutzungsbedingungen bieten, die eine im öffentlichen Interesse liegende Forschung unterstützen. Um dies sicherzustellen, müssten kleinere Plattformen gegebenenfalls mit den nötigen Ressourcen unterstützt werden. Gleichzeitig muss eine anerkannte unabhängige Vermittlungsstelle geschaffen werden, welche die kontinuierliche Qualität der Daten sicherstellt und sie den Forscher:innen auf standardisierte Weise und unter Wahrung der Privatsphäre zur Verfügung stellen kann. Forscher:innen und Finanzierende der Online-Forschung sollten verstärkt versuchen, Skaleneffekte in diesem Bereich zu realisieren. Dies würde die derzeitigen Einstiegshürden abbauen, die einer Entwicklung hin zu einer gerechteren, vielfältigeren globalen Forschungsgemeinschaft im Weg stehen.

Endnotes

1 Guhl, Jakob, Marsh, Oliver & Tuck, Henry. Erforschung des sich im Wandel begriffenen Online-Ökosystems: Hindernisse, Methoden und zukünftige Herausforderungen. Institute for Strategic Dialogue. Juli 2022 https://www.isdglobal.org/isd-publications/erforschung-des-sich-im-wandel-begriffenen-online-okosystems-hindernisse-methoden-und-zukunftige-herausforderungen/.

2 Extracts From ISD's Submitted Response to the UK Government Online Harms White Paper. Institute for Strategic Dialogue. Juli 2019. https://www.isdglobal.org/isd-publications/extracts-from-isds-submitted-response-to-the-uk-government-online-harms-white-paper/.

3 Channels FAQ (Fragen und Antworten zu Kanälen). Telegram. URL: https://telegram.org/faq_channels

4 700 Million Users and Telegram Premium. Telegram. Juni 2022. URL: https://telegram.org/blog/700-million-and-premium.

5 Terms of Service. Telegram. URL: https://telegram.org/tos.

6 Europol and Telegram take terrorist propaganda online. Europol. November 2019. URL: https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.

7 Gerster, Lea et al. (17. Dezember 2021). Stützpfeiler Telegram. Wie Rechtsextreme und Verschwörungsideolog:innen auf Telegram ihre Infrastruktur ausbauen. Institute for Strategic Dialogue. URL: https://www.isdglobal.org/isd-publications/stutzpfeiler-telegram-wie-rechtsextreme-und-verschworungsideologinnen-auf-telegram-ihre-infrastruktur-ausbauen/.

8 FAQ – F: Wie unterscheiden sich öffentliche und private Kanäle? Telegram. URL: https://telegram.org/faq_channels#wie-unterscheiden-sich-ffentliche-und-private-kanle.

9 Ratings of Telegram groups. TGStat. URL: https://tgstat.com/ratings/chats.

10 Belarus Carries Out Wave Of Detentions For Subscribing to "Extremist" Telegram Channels. Radio Free Europe/Radio Liberty. Oktober 2021. URL: https://www.rferl.org/a/belarus-telegram-extremist-detentions/31530720.html.

11 Через сервис TGStat стали доступны данные о протестных приватных чатах и их участниках. Mediazona. April 2022: URL: https://mediazona.by/news/2022/04/28/tgstat.

12 Frühling, Milla (2020, Oktober). OLIVER JANICH – QANON-DESINFORMATIONEN AUF ALLEN KANÄLEN. Belltower.News. URL: https://www.belltower.news/social-media-rechtsaussen-oliver-janich-qanon-desinformationen-auf-allen-kanaelen-105577/.

13 Telegram-Kanal Oliver Janich Investigativ. URL: https://www.oliverjanich.de/telegram-messenger.

14 Institute for Strategic Dialogue (Juli 2019). Ebd.

15 Gerster et al. (Dezember 2022). Ebd.

16 Rogers, Iain (April 2022). Germany Foils Plot to Sabotage Democracy, Kidnap Health Minister. Bloomberg UK. URL: https://www.bloomberg.com/news/articles/2022-04-14/germany-foils-plot-to-sabotage-democracy-kidnap-health-minister.

17 Raid due to murder plans against Kretschmer. ZDFheute. Dezember 2021. URL: https://www.zdf.de/nachrichten/politik/razzia-telegram-mordplan-kretschmer-100.html.

18 Täglich Tötungsaufrufe auf Telegram. Tagesschau. Januar 2021. URL: https://www.tagesschau.de/investigativ/funk/ todesdrohungen-telegram-101.html.

19 Ermittler decken illegalen Handel auf. Tagesschau. Oktober 2020. URL: https://www.tagesschau.de/inland/telegram-illegaler-handel-105.html.

20 Vgl. z. B.: Sold, Manjana und Junk, Julian (2021). Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities. Global Network on Extremism and Technology. URL: https://gnet-research.org/wp-content/uploads/2021/01/GNET-Report-Researching-Extremist-Content-Social-Media-Ethics.pdf; Conway, Maura (März 2021). Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, and the Need for Tailored Guidelines, Terrorism and Political Violence. Terrorism and Political Violence, 33 (2), pp. 367–380. 10.1080/09546553.2021.1880235; "Internet Research: Ethical Guidelines 3.0. AoIR. Oktober 2019. URL: https://aoir.org/reports /ethics3.pdf; A Guide to Internet Research Ethics. NESH. Juni 2019. URL: https://www.forskningsetikk.no/en/guidelines/social-sciences-humanities-law-and-theology/a-guide-to-internet-research-ethics/.

21 Projekt Radikalisierung in rechtsextremen Online-Subkulturen entgegentreten. Institute for Strategic Dialogue Germany. URL: https://isdgermany.org/projekt-bmj/.

22 Nazi-Song ist Antifa-Experiment. Taz. Januar 2022. URL: https://taz.de/Rechte-Musik-auf-Streaming-Plattformen/!5828978/.

23 Dockery, Wesley (September 2022). Germany cracks down on far-right Telegram users. Deutsche Welle. URL: https://www.dw.com/en/germany-cracks-down-on-far-right-telegram-users/a-60715438.

24 FAQ – F: Ich habe illegale Inhalte auf Telegram gefunden. Wie kann ich diese löschen lassen? Telegram. URL https://telegram.org/faq/de?setln=de#f-ich-habe-illegale-inhalte-auf-telegram-gefunden-wie-kann-ich-d.

25 Antwort der Landesregierung auf eine Kleine Anfrage zur schriftlichen Beantwortung. Landtag von Sachsen-Anhalt. URL: https://www.landtag.sachsen-anhalt.de/fileadmin/files/drs/wp8/drs/d1519aak.pdf.

26 Efforts to delegitimise the state. Bundesamt für Verfassungsschutz. URL: https://www.verfassungsschutz.de/EN/topics/efforts-to-delegitimise-the-state/efforts-to-delegitimise-the-state_node.html

27 Mit Haftbefehl gesuchter Hetzer Attila Hildmann sieht sich als Nachfolger von Adolf Hitler. RTL. Oktober 2022. URL: https://www.rtl.de/cms/attila-hildmann-von-stern-reportern-in-der-tuerkei-aufgespuert-er-wird-mit-haftbefehl-gesucht-5013127.html.

28 Steinke, Ronen (September 2022). Office for the Protection of the Constitution: Alone among false friends. Süddeutsche Zeitung. URL: https://www.sueddeutsche.de/projekte/artikel/politik/verfassungsschutz-rechtsextreme-social-media-telegram-virtuelle-agenten-reichsbuerger-coronaleugner-rassismus-antisemitismus-verschwoerungsideologie-e222942/?reduced=true.

29 Curry, David (Januar 2023). Discord Revenue and Usage Statistics. Business of Apps. URL: https://www.businessofapps.com/data/discord-statistics/.

30 Top 100 Biggest Discord Servers. Discord. URL: https://discords.com/servers/top-100.

31 Discord servers tagged with 4Chan. Discord. URL: https://disboard.org/servers/tag/4chan.

32 Roose, Kevin (August 2017). This Was the Alt-Right's Favorite Chat App. Then Came Charlottesville. The New York Times. URL: https://www.nytimes.com/2017/08/15/technology/discord-chat-app-alt-right.html; Davey, Jacob & Ebner, Julia (Oktober 2017). The Fringe Insurgency – Connectivity, Convergence and Mainstreaming of the Extreme Right. Institute for Strategic Dialogue. URL: https://www.isdglobal.org/isd-publications/the-fringe-insurgency-connectivity-convergence-and-mainstreaming-of-the-extreme-right/.

33 Alexander, Julia (Februar 2018). Discord is purging alt-right, white nationalist and hateful servers. Polygon. URL: https://www.polygon.com/2018/2/28/17061774/discord-alt-right-atomwaffen-ban-centipede-central-nordic-resistance-movement.

34 Allyn, Bobby (April 2021). Group-Chat App Discord Says It Banned More Than 2,000 Extremist Communities. NPR. URL: https://www.npr.org/2021/04/05/983855753/group-chat-app-discord-says-it-banned-more-than-2-000-extremist-communities.

35 Gallagher, Aoife et al (August 2021). Gaming and Extremism: The Extreme Right on Discord. Institute for Strategic Dialogue. URL: https://www.isdglobal.org/isd-publications/gaming-and-extremism-the-extreme-right-on-discord/.

36 Ebd.

37 Ayad, Moustafa (November 2021). Islamogram: Salafism and Alt-Right Online Subcultures. Institute for Strategic Dialogue. URL: https://www.isdglobal.org/isd-publications/islamogram-salafism-and-alt-right-online-subcultures/.

38 Wong, Wilson (Juli 2022). Discord chat app faces moderation questions after mass shooting suspects are linked to platform. NBC News. URL: https://www.nbcnews.com/tech/tech-news/highland-park-shooting-suspect-bobby-e-crimo-iii-discord-server-raises-rcna36659.

39 Joyce, Kathryn & Lorber, Ben (Mai 2022). Traditional Catholics and white nationalist "groypers" forge a new far-right youth movement. Salon. URL: https://www.salon.com/2022/05/13/trad-catholics-and-nationalist-groypers-forge-a-new-far-right-youth-movement/.

40 Disboard. https://disboard.org/.

41 Channel Resources. Discord. URL: https://discord.com/developers/docs/resources/channel - get-channel-messages; Dracovian/Discord-Scraper. Github (via Internet Archive). URL: https://web.archive.org/web/20220727182403/https://github.com/Dracovian/Discord-Scraper.

42 Terms of Service. Discord. URL: https://discord.com/terms.

43 Discord Developer Policy. Discord. URL: https://discord.com/developers/docs/policies-and-agreements/developer-policy. Anmerkung: Die Entwicklerrichtlinie für die Nutzung der API von Discord wurde im September 2022 aktualisiert; die betreffende Passage und enthält aktuell den folgenden Wortlaut: „You may not mine or scrape any data, content, or information available on or through Discord services".

44 Schlegel, Linda (Sommer 2020). Jumanji Extremism? How games and gamification could facilitate radicalization processes. Journal for Deradicalization, 23. S. 1 – 44.

45 Vogel, William (April 2023). People-first video platform Odysee Launches out of Beta, Enabling Creators to Reclaim Power and Monetization. Cision PRWeb. URL: https://www.prweb.com/releases/peoplefirstvideoplatformodyseelaunchesoutof-betaenablingcreatorstoreclaim-powerandmonetization/prweb17586549.htm.

46 Odysee @OdyseeTeam (30. September 2021): Big tech censorship has gone too far! Use Odysee as your alternative to YouTube. We're not perfect, but getting better. FYI. Livestream with us, and make more money than yt/twitch in donations. Twitter. URL: https://twitter.com/OdyseeTeam/status/1443642146280509464.

47 Odysee @Odysee (März 2022). Odysee & Freedom of the Press: A Letter From Our CEO. Odysee. URL: https://odysee.com/@Odysee:8/freedomofthepress:0.

48 Matlach, Paula, Hammer, Dominik & Schwieter, Christian (August 2022). Auf Odysee: Die Rolle von Blockchain-Technologie für die Monetarisierung im rechtsextremen Onlinemilieu. Institute for Strategic Dialogue. URL: https://www.isdglobal.org/wp-content/uploads/2022/08/ISD_auf-odyssee_220810_digital.pdf.

49 Odysee @OdyseeTeam (3. August 2021). We aren't alt tech, we're new tech Alt tech = inferior version of what's come before with no selling points other than free speech New tech = better version of what's come before with the added benefit of free speech. Twitter. URL: https://twitter.com/OdyseeTeam/status/1422629329905848322.

50 LBRY. URL: https://lbry.com/.

51 Jeremy Kauffman: Leadership For New Hampshire. https://jeremy4nh.com/home/

52 Matlach, Paula, Hammer, Dominik & Schwieter, Christian (August 2022). Ebd.

53 New breed of video sites thrive on misinformation and hate. Rappler. August 2022. URL: https://www.rappler.com/technology/features/new-breed-video-sites-thrive-misinformation-hate/.

54 Marshall, Andrew R. C. & Tanfani, Joseph (August 2022). New breed of video sites thrives on misinformation and hate. Reuters. URL: https://www.reuters.com/investigates/special-report/usa-media-misinformation/.

55 Sign-up. Odysee. URL: https://odysee.com/$/signup?redirect=/.

56 Odysee @Odysee (Oktober 2021). Creators Will Be Earning From Ads Soon. Odysee. URL: https://odysee.com/@Odysee:8/creator-earnings:7.

57 Talley, Ian (September 2022). Islamic State Turns to NFTs to Spread Terror Message. The Wall Street Journal. URL: https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800.

58 'Terms of Service. Odysee. URL: https://odysee.com/$/tos.

59 Les origins de l'extrême-droite. herodote.net. Oktober 2022. URL: https://www.herodote.net/Les_origines_de_l_extreme_droite-article-2715.php.

60 Odysee.com. Similar Web (via Internet Archive). https://web.archive.org/web/20221018123152/https://www.similarweb.com/website/odysee.com/; Youtube.com. Similar Web (via Internet Archive). https://web.archive.org/web/20221018122916/https://www.similarweb.com/website/youtube.com/#overview.

61 Declaration of Indifference: Community Guidelines. Odysee. Februar 2022. https://help.odysee.tv/communityguidelines/.

62 Vgl. beispielsweise: Mir, Rory & Doctorow, Cory (August 2021). Facebook's Attack on Research is Everyone's Problem. EFF. URL: https://www.eff.org/deeplinks/2021/08/facebooks-attack-research-everyones-problem.

63 Vgl. beispielsweise: Hammer, Dominik, Gerster, Lea & Schwieter, Christian (Februar 2023). Im digitalen Labyrinth: Rechtsextreme Strategien der Dezentralisierung im Netz und mögliche Gegenmaßnahmen. Institute for Strategic Dialogue. URL https://www.isdglobal.org/wp-content/uploads/2023/01/im_digitalen_Labyrinth.pdf.

64 Digital Services Act. European Parliament. https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.pdf.

65 Twitter API Changes Set to Disrupt Public Interest Research. Tech Policy Press. Februar 2023. URL: https://techpolicy.press/twitter-api-changes-set-to-disrupt-public-interest-research/; Lawler, Richard (Juni 2023). Meta reportedly plans to shut down CrowdTangle, its tool that tracks popular social media posts. The Verge: URL: https://www.theverge.com/2022/6/23/23180357/meta-crowdtangle-shut-down-facebook-misinformation-viral-news-tracker.

66 Signatories of the 2022 Strengthened Code of Practice on Disinformation. European Commission. Juni 2022. URL: https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation.

67 EDMO releases report on researcher access to platform data. European Digital Media Observatory. Mai 2022. URL: https://edmo.eu/2022/05/31/edmo-releases-report-on-researcher-access-to-platform-data/.

68 Bundesministerium der Justiz (2017). Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act, NetzDG). Basic Information. URL: https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html.

69 Coalition for Independent Technology Research. URL: https://independenttechresearch.org/; European Digital Media Observatory (May 2022). Ebd.; Wanless, Alicia & Shapiro, Jacob N (November 2022). A CERN Model for Studying the Information Environment. Carnegie Endowment for International Peace. URL: https://carnegieendowment.org/2022/11/17/cern-model-for-studying-information-environment-pub-88408.

70 Institute for Strategic Dialogue (Juli 2019). Ebd.

71 Ethics. AoIR. URL: https://aoir.org/ethics/.

ISD | Powering solutions to extremism and polarisation

Amman | Berlin | London | Paris | Washington DC

www.isdglobal.org