Global Network
on Extremism & Technology

Migrationsdynamik: die Nutzung von Instant-Messaging-Anwendungen durch Extremisten

Bennett Clifford

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

Der Autor dieses Berichts ist Bennett Clifford, Senior Research Fellow, Program on Extremism at George Washington University

Das Global Network on Extremism and Technology (GNET) ist eine akademische Forschungsinitiative mit Unterstützung des Global Internet Forum to Counter Terrorism (GIFCT), einer unabhängigen, aber von der Wirtschaft finanzierte Initiative mit dem Ziel, die Nutzung von Technologie für terroristische Zwecke besser zu verstehen und einzudämmen. GNET wird einberufen und geleitet vom International Centre for the Study of Radicalisation (ICSR), einem akademischen Forschungszentrum innerhalb des Department of War Studies am King's College London. Die in diesem Dokument enthaltenen Ansichten und Schlussfolgerungen sind den Autoren zuzuschreiben und sollten nicht als die ausdrücklichen oder stillschweigenden Ansichten und Schlussfolgerungen von GIFCT, GNET oder ICSR verstanden werden.

KONTAKTANGABEN

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

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

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

Twitter: **@GNET_research**

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

© GNET

Kurzfassung

- Extremisten verschiedenster Couleur – darunter dschihadistische Anhänger von al-Qaida und des „Islamischen Staates (IS) in Syrien und im Irak sowie verschiedene rechtsextreme Gruppen – nutzen derzeit den Instant-Messaging-Dienst Telegram als zentrales Koordinationsforum für Online-Aktivitäten. Aufgrund der neuen Richtlinien von Telegram, der Zusammenarbeit mit den Strafverfolgungsbehörden und anderen Branchenpartnern sowie der konsequenteren Durchsetzung seiner Nutzungsbedingungen erfahren Extremisten jedoch allmählich erheblichen Druck auf ihr Telegram-basiertes Ökosystem.

- Dschihadisten und Rechtsextremisten im Internet experimentieren daher immer wieder mit anderen Instant-Messaging-Diensten als möglichen Alternativen zu Telegram. Dennoch ist die vollständige Verlagerung auf eine andere Plattform auf kurze Sicht unwahrscheinlich. Aufgrund bestimmter Eigenschaften und Funktionen von Telegram, des Bekanntheitsgrads in extremistischen Kreisen und der im Vergleich zur Konkurrenz einfachen Verwendung wird die extremistische Ausnutzung der Plattform den neuen Durchsetzungsregeln des Unternehmens zum Trotz wahrscheinlich weitergehen.

- Im Zuge der Schwierigkeiten der Anhänger extremistischer Gruppen, sich auf Telegram zu halten, versuchen oder planen die Gruppen, Präsenzen bei anderen Instant-Messaging-Diensten zu etablieren. Hierbei haben extremistische Gruppen in den vergangenen zwei Jahren sechs Plattformen (BCM, Gab Chat, Hoop Messenger, Riot.im, Rocket.Chat und TamTam) als mögliche Alternativen zu Telegram ins Auge gefasst.

- Die folgende Analyse zeigt, dass sich Extremisten von diesen Plattformen aufgrund ihrer Eigenschaften und Funktionen, ihrer einfachen Verwendung und dem Verhalten der jeweiligen Betreiber hinsichtlich der Themen Datenschutz, Sicherheit und Regulierung extremistischer Inhalte angezogen fühlten.

- Für die Zukunft zeichnen sich in der extremistischen Ausnutzung von Instant-Messaging-Diensten zwei Trends ab:

    - Die Anhänger extremistischer Gruppen, die auf Telegram eine massive Präsenz aufgebaut haben, werden wahrscheinlich nach Plattformen Ausschau halten, die sehr ähnliche Eigenschaften und Funktionen, Möglichkeiten und Gestaltungselemente wie Telegram haben.

    - Die Anhänger extremistischer Gruppen werden voraussichtlich weiterhin versuchen, Instant-Messaging-Plattformen auszunutzen, die dezentrale Server und Datenspeicherung anbieten.

- Um dem extremistischen Missbrauch von Instant-Messaging-Diensten Einhalt zu gebieten, könnten branchenweite Initiativen wie das Global Internet Forum to Counter Terrorism erwägen, zwecks Zusammenarbeit und Informationsaustausch die Anbieter von Instant-Messaging-Diensten einzelnen Foren zuzuordnen. Generell sollten Forschung, Politik und Praxis der Extremismusbekämpfung im Internet in Erwägung ziehen, sich bei der Bewertung der extremistischen Ausnutzung digitaler Kommunikationstechnologien stärker auf bestimmte Merkmale zu konzentrieren als auf individuelle Plattformen.

Inhalt

1 Einleitung: Extremisten, Telegram und Verlagerung

Der vorliegende Bericht untersucht den Flickenteppich der bei dschihadistischen und rechtsextremen Gruppen beliebtesten Instant-Messaging-Dienste. Im Wesentlichen geht es dabei um eine Darstellung besonderer technischer Eigenschaften und Möglichkeiten sowie das Verhalten ihrer jeweiligen Betreiber im Hinblick auf die Themen Schutz der Privatsphäre ihrer Nutzer, Sicherheit und Regulierung. Zu diesem Zweck analysiert der Bericht sechs Online-Messaging-Dienste (BCM, Gab Chat, Hoop Messenger, Riot.im, Rocket.Chat und TamTam), die von extremistischen Gruppen über Telegram hinaus bereits genutzt wurden oder genutzt werden können.

Zurzeit konzentrieren sich viele Anhänger verschiedenster extremistischer Gruppen auf den Online-Instant-Messaging-Dienst Telegram, wobei einige auch versuchen, auf andere Plattformen vorzudringen.[1] Telegram wird immer wieder als „Lieblingsplattform" der Dschihadisten im Internet bezeichnet, insbesondere der Anhänger des „Islamischen Staates" (IS) im Irak und in Syrien, aber auch bei rechtsextremen Bewegungen ist der Dienst seit jeher populär.[2] Analysten und Wissenschaftler, die sich mit Extremismus im Internet befassen, sowie zahlreiche Regierungen betrachten Telegram aufgrund seiner besonderen Funktionen und Eigenschaften (u. a. verschlüsselte Ende-zu-Ende-Kommunikation für seine Anwender sowie Garantien für Anonymität und Schutz der Privatsphäre) als eine stabile Kommunikationsplattform für extremistische Gruppen unterschiedlicher Couleur.[3] Extremisten nutzen Telegram-Kanäle und -Gruppen als Inszenierungsort für eine Multiplattformstrategie, bei der Medieninhalte von Telegram auf andere Messaging-Plattformen und öffentliche Websites weitergeleitet werden.[4]

Allerdings schmälern die jüngsten Änderungen der Nutzungsbedingungen und Datenschutzrichtlinien von Telegram die Möglichkeiten, die die Plattform extremistischen Gruppen bietet. So ergänzte Telegram beispielsweise im April 2018 seine Datenschutzerklärung um Abschnitt 8.3. Abweichend von Telegrams früherer Absage an die Informationsweitergabe an staatliche Behörden besagt dieser Abschnitt: „wenn Telegram ein gerichtlicher Beschluss vorgelegt wird, wonach ein Terrorverdacht vorliegt,

1 Clifford, Bennett, und Helen Powell. 2019. „Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram." Washington, D.C.: Program on Extremism. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/EncryptedExtremism.pdf; Bloom, Mia, Hicham Tiflati, und John Horgan. 2019. „Navigating ISIS's Preferred Platform: Telegram." Terrorism and Political Violence 31 (6): 1242–1254. https://doi.org/10.1080/09546553.2017.1339695; Bloom, Mia, und Chelsea Daymon. 2018. „Assessing the Future Threat: ISIS's Virtual Caliphate." Orbis 62 (Mai). https://doi.org/10.1016/j.orbis.2018.05.007; „Telegram: The Latest Safe Haven for White Supremacists." 2019. Anti-Defamation League. 2. Dezember 2019. https://www.adl.org/blog/telegram-the-latest-safe-haven-for-white-supremacists.

2 Anti-Defamation League, „Telegram: The Latest Safe Haven for White Supremacists".

3 Clifford und Powell, „Encrypted Extremism".

4 Ebd.

können wir Ihre IP-Adresse und Telefonnummer an die zuständigen Behörden weitergeben“.[5] Zeitgleich mit der Änderung seiner Datenschutzerklärung begann Telegram auch mit der Teilnahme an „Referral Action Days“ (RAD) von Europol und einzelnen Strafverfolgungsbehörden in der Europäischen Union.[6] Während der elften RAD beschränkte sich Telegram darauf, den Prozess der europäischen Strafverfolgungsbehörden zur Auffindung und Identifizierung terroristischer Inhalte zu beobachten.[7] Während der sechzehnten RAD im November 2019 arbeitete Telegram jedoch mit Europol und den Branchenpartnern Google, Twitter und Instagram zusammen.[8] Gemeinsam entfernten die Plattformen insgesamt 26.000 IS-Propaganda-Objekte wie Accounts, Kanäle, Gruppen, Videos und andere Publikationen von ihren Plattformen.[9] In einer Stellungnahme zu der Aktion behauptete der Sprecher der belgischen Staatsanwalt Eric Van Der Sypt, dass der IS infolge der Massenlöschung „vorerst aus dem Internet getilgt“ sei.[10]

Van Der Sypts anfänglicher Einschätzung zum Trotz blieben extremistische Gruppen allerdings auch nach den RAD auf Telegram präsent. Zwar versetzte die Aktion den IS-Anhängern auf Telegram vorübergehend einen Schlag, doch ergaben Analysen des Global Network on Extremism and Technology, dass „ein hartnäckiger Überrest der Kernpräsenz“ sich auf der Plattform halten konnte und „die Verbreitung sowohl offizieller als auch inoffizieller Propaganda kontinuierlich weitergeht“.[11] Die IS-Anhänger (als einzige bekannte Zielgruppe dieser Aktion), bauten sehr schnell Präsenzen auf diversen anderen Instant-Messaging-Plattformen auf. Hierdurch gelang es den IS-Anhängern, im Internet präsent zu bleiben, da „die Verteilung auf diese mehr als ein Dutzend Plattformen die Verbreitung dschihadistischer Propaganda weiter dezentralisiert hat“ und der IS durch das großflächige Verteilen seines Contents im Web seinen „Bekanntheitsgrad noch erhöhen konnte“.[12] Im Juli 2020 kam eine Einschätzung durch Europol zu dem Ergebnis, dass „die Bestrebungen, eine IS-Präsenz im Internet einzurichten, auf mehreren Plattformen – einschließlich Telegram – fortgesetzt werden“.[13] Mitarbeiter, die an den Telegram-RAD beteiligt waren, gaben an, dass sich die Anstrengungen hauptsächlich auf IS-Anhänger konzentriert hätten, sodass andere dschihadistische Gruppen und gewaltbereite Extremisten von den Löschungen weitgehend verschont geblieben seien.[14]

5 Ebd.
6 Amarasingam, Amarnath. 2020. „A View from the CT Foxhole: An Interview with an Official at Europol’s EU Internet Referral Unit.“ CTC Sentinel 13 (2). https://ctc.usma.edu/view-ct-foxhole-interview-official-europols-eu-internet-referral-unit/.
7 „Referral Action Day with Six EU Member States and Telegram.“ 2018. Europol. 5. Oktober 2018. https://www.europol.europa.eu/newsroom/news/referral-action-day-six-eu-member-states-and-telegram.
8 „Europol and Telegram Take on Terrorist Propaganda Online.“ 2019. Europol. 25. November 2019. https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.
9 Ebd.
10 Zialcita, Paolo. 2019. „Islamic State ‚Not Present On The Internet Anymore‘ Following European Operation“. NPR.Org. 25. November 2019. https://www.npr.org/2019/11/25/782712176/islamic-state-not-present-on-the-internet-anymore-following-european-operation.
11 Gluck, Raphael. 2020. „Islamic State Adjusts Strategy to Remain on Telegram.“ Insight. Global Network on Extremism and Technology. https://gnet-research.org/2020/02/06/islamic-state-adjusts-strategy-to-remain-on-telegram/; Creizis, Meili. 2020. „Telegram’s anti-IS Campaign: Effectiveness, Perspectives, and Policy Suggestions.“ Insight. Global Network on Extremism and Technology. https://gnet-research.org/2020/07/30/telegrams-anti-is-campaign-effectiveness-perspectives-and-policy-suggestions/
12 „Jihadists Presence Online Decentralizes After Telegram Ban.“ 2020. Flashpoint. 17. Januar 2020. https://www.flashpoint-intel.com/blog/terrorism/jihadists-presence-online-decentralizes-after-telegram-ban/.
13 „Online Jihadist Propaganda: 2019 in Review.“ 2020. Europol. 28. Juli 2020. https://www.europol.europa.eu/sites/default/files/documents/report_online_jihadist_propaganda_2019_in_review.pdf.
14 Amarasingam, „A View from the CT Foxhole.“

Während IS-Inhalte auf Telegram systematisch gelöscht wurden, blieben die großen Präsenzen rechtsextremer Gruppen auf der Plattform weitgehend unbehelligt.[15] Diese Tendenz könnte sich jedoch allmählich ändern. In diesem Sommer organisierte Telegram Massenlöschungen bekannter rechtsextremer Kanäle und Gruppen auf seiner Plattform.[16] Telegram sperrte einige der aggressivsten und bösartigsten rechtsextremen Kanäle, darunter Terrorwave Refined, eine „Drehscheibe" für die gewaltbereiten Rechtsextremen auf Telegram, sowie Kanäle in Verbindung mit Misanthropic Division und RapeKrieg.[17] Die meisten rechtsextremen Kanäle auf Telegram blieben jedoch unangetastet, und die Administratoren der gelöschten Kanäle versuchen weiterhin, Inhalte auf der Plattform zu posten.[18] Es bleibt abzuwarten, ob Rechtsextremisten auf Telegram ernsthaft die Nutzung anderer Plattformen in Erwägung ziehen und ob die Bemühungen von Telegram überhaupt fortgesetzt werden.

15 Katz, Rita. 2020. „Neo-Nazis Are Running Out of Places to Hide Online." WIRED, 9. Juli 2020. https://www.wired.com/story/neo-nazis-are-running-out-of-places-to-hide-online/.
16 Ebd.
17 Ebd.
18 Ebd.

2 Instant-Messaging-Dienste: Analysekategorien

Auf kurze Sicht ist ein vollständiger Rückzug der Online-Extremisten von Telegram und eine massenhafte Migration auf eine andere Plattform unwahrscheinlich. Dennoch besteht die Notwendigkeit, auch alternative Messaging-Plattformen zu kennen, die extremistische Gruppen zusätzlich zu Telegram nutzen. Extremisten legen sich nicht auf eine Plattform fest; vielmehr missbrauchen sie häufig mehrere Plattformen gleichzeitig.[19] So wie Extremisten Telegram bereits ausprobiert haben, als Twitter und Facebook ihnen noch ein weitgehend komfortables Umfeld geboten haben, ist davon auszugehen, dass sie auch dann mit alternativen Messaging-Plattformen experimentieren werden, wenn Telegram ihnen gewogen bleibt. Darüber hinaus kann eine Analyse dieser alternativen Plattformen im Vergleich zu Telegram Aufschluss darüber liefern, welche Merkmale Messaging-Plattformen attraktiv für extremistische Gruppen machen. Geht man davon aus, dass Telegram sich weiterhin bemühen wird, Extremisten durchgreifend und rigoros von der Plattform zu entfernen, muss die Praxis die alternativen Plattformen kennen. Nur so lassen sich die indirekten Folgen von Tilgungskampagnen unter Kontrolle halten, beispielsweise die Migration von Extremisten zu Plattformen mit schwächerer Regulierung, mit besseren Eigenschaften und Möglichkeiten für ihre Zwecke oder mit Datenschutz- und Sicherheitsrichtlinien, die extremistische Inhalte vor Strafverfolgungsbehörden, Nachrichtendiensten oder den Betreibern selbst verbergen.

Die sechs in dieser Analyse betrachteten Plattformen stellen selbstverständlich keine vollständige Liste der Instant-Messenger dar, der sich extremistische Gruppen heutzutage bedienen. Sie alle hatten jedoch in den vergangenen Jahren mit extremistischem Missbrauch ihres Angebots zu tun. Ein Vergleich dieser Plattformen kann dazu beitragen, einige der Eigenschaften und Möglichkeiten zu identifizieren, die für extremistische Gruppen bei der Auswahl ihrer Messaging-Plattformen wesentlich sind. Im Einzelnen untersucht der vorliegende Beitrag für jede der Plattformen fünf Faktoren, die ihren generellen Umgang mit extremistischen Inhalten charakterisieren: extremistische Nutzung, Umfang an Eigenschaften und Funktionen, einfache Anwendung, Datenschutz und Sicherheit sowie die ideologischen/regulatorischen Bedingungen. Jede dieser fünf Kategorien umfasst mehrere Kernfragen zur Nutzung von Instant-Messaging-Plattformen durch extremistische Gruppen:

- *Extremistische Nutzung:* Welche Arten von extremistischen Gruppen nutzen die Plattform? Seit wann nutzen sie die Plattform? Nutzen sie die Plattform gegenwärtig? In welchem Ausmaß wird die Plattform von Extremisten genutzt?

19 Prucha, „IS and the Jihadist Information Highway"; Alkhouri, Laith, und Alex Kassirer. 2016. „Tech for Jihad: Dissecting Jihadists Digital Toolbox." Flashpoint. https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf; Conway, Maura. 2006. „Terrorism and the Internet: New Media – New Threat?" Parliamentary Affairs 59 (2): 283–98. https://doi.org/10.1093/pa/gsl009.

- *Umfang an Eigenschaften und Funktionen:* Welche Eigenschaften und Funktionen bietet diese Plattform? In welchen dieser Eigenschaften und Funktionen unterscheidet sie sich vom Wettbewerb, insbesondere im Hinblick auf die extremistische (missbräuchliche) Nutzung der Plattform?

- *Einfache Anwendung:* Wie einfach ist die Plattform zu nutzen? Welche Schritte sind notwendig, um einen Account anzulegen und auf bestimmte Inhalte zuzugreifen? Mit welchen Protokollen läuft das System? Kommt es auf der Plattform zu Störungen, Hacking-Versuchen oder anderen Denial-of-Service-Angriffen?

- *Datenschutz und Sicherheit:* Was sehen die Nutzungsbedingungen im Hinblick auf den Schutz der Daten der Anwender vor? Bietet die Plattform Datenverschlüsselung an? Wo werden die Benutzerdaten gespeichert? Welche Drittparteien haben potenziell Zugang zu Benutzerdaten?

- *Ideologische/regulatorische Bedingungen:* Welche Ideologie vertritt die Plattform, wenn es um die Entfernung terroristischer und extremistischer Inhalte geht? Legt sie Transparenzberichte vor? Wo ist die Plattform registriert, und welchen Gesetzen zur Regulierung von Online-Inhalten unterliegt sie? Wie steht sie zu behördlichen Aufforderungen zur Herausgabe von Benutzerdaten?

Im letzten Abschnitt hebt der Bericht wesentliche gemeinsame Merkmale dieser Plattformen hervor, um Hinweise darauf zu finden welche Merkmale für extremistische Gruppen besonders attraktiv sind. Des Weiteren plädiert er dafür, sich bei der Analyse und Bekämpfung der extremistischen Nutzung des Internets stärker auf bestimmte Angebotsmerkmale als auf bestimmte Plattformanbieter zu konzentrieren.

3 Extremistische Nutzung alternativer Instant-Messaging-Dienste

In diesem Abschnitt werden sechs Instant-Messaging-Plattformen analysiert, die Extremisten im Zuge der konsequenteren Durchsetzung der Nutzungsbedingungen durch Telegram ausgenutzt haben oder ausnutzen könnten. Sechs Monate nach den Referral Action Days bei Telegram kam ein Bericht von Europol zu dem Ergebnis, dass nach der Tilgungswelle die IS-Sympathisanten im Internet „zu TamTam und Hoop Messenger strömten“ und darüber hinaus „Nischenanwendungen wie den Blockchain-Messenger BCM, RocketChat und die kostenlose Messenger-Software Riot“ testeten.[20] Auch die Anhänger anderer dschihadistischer Gruppen sowie rechtsextremer Gruppen haben auf mehreren dieser Plattformen eigene Experimente gestartet. Neben diesen fünf Plattformen analysiert dieser Abschnitt eine weitere Plattform, Gab Chat, die derzeit noch in der Entwicklung ist, aber aufgrund ihrer Eigenschaften und Möglichkeiten sowie der Geschichte des Betreibers für Rechtsextremisten attraktiv sein könnte.[21]

BCM Messenger

BCM (Because Communication Matters) war eine dezentrale Messaging-App, die sowohl private Chats als auch Gruppen-Chats für bis zu 100.000 Teilnehmer anbot.[22] Zwar liegen die Ursprünge des Unternehmens im Dunkeln, doch wurde die Plattform von chinesischen Entwicklern geschaffen und auf den Britischen Jungferninseln als dezentrale Alternative zur chinesischen Messaging-Plattform WeChat registriert.[23] Mehrere Beobachter extremistisch genutzter Online-Medien stellten fest, dass IS-Anhänger nach den Referral Action Days (RAD) 2019 zunehmend mit der Anwendung experimentierten.[24] So richtete beispielsweise im Dezember 2019 eines der wichtigsten dem IS angeschlossenen Online-Mediennetzwerke, die Nashir News Agency, mehrere Kanäle auf der Plattform ein.[25] Im Februar 2020 teilte das Unternehmen den Nutzern mit, dass es seinen Messaging-Dienst eingestellt habe.[26]

20 Europol, „Online Jihadist Propaganda: 2019 in Review“.
21 Morse, Jack. 2020. „Police are worried about white extremists organizing on Gab Chat, leaked documents show.“ 13. Juli 2020. https://mashable.com/article/law-enforcement-documents-violent-white-extremists-encrypted-gab-chat/.
22 „BCM Messenger.“ ohne Jahr. BCM Messenger. Abgerufen am 1. April 2020. „Privacy Policy“, ohne Jahr. BCM Messenger. Abgerufen am 1. April 2020. Der BCM-Dienst ist inzwischen eingestellt. Zugängliche Versionen der Seite und die Datenschutzerklärung von BCM finden sich in der Wayback Machine unter https://web.archive.org/web/20200215082731/https://bcm.social/index.html und https://web.archive.org/web/20191016053505/https://bcm.social/license/policy.html.
23 Ebd.; Yuan, Lanny, Huaibing Jian, Peng Liu, Pengxin Zhu und ShanYang Fu. 2018. „AME Blockchain: An Architecture Design for Closed-Loop Fluid Economy Token System.“ White Paper.
24 Smith, Brenna. 2019. „Terrorists Use a New Blockchain Messaging App after Telegram Crackdown.“ Bellingcat CryptOSINT. 10. Dezember 2019. https://mailchi.mp/7884c14d5fb9/terrorists-use-a-new-blockchain-messaging-app-after-telegram-crackdown.
25 Ebd.; Flashpoint, „Jihadists Presence Online Decentralizes After Telegram Ban“; Gluck, „Islamic State Adjusts Strategy to Remain on Telegram“; Webb, Sam, und Colin Rivet. 2019. „Terror Group ISIS Testing Blockchain Messaging App“. 16. Dezember 2019. https://finance.yahoo.com/news/terror-group-isis-testing-blockchain-150028142.html.
26 Mitteilung an die BCM-Teilnehmer, 22. Februar 2020. https://postimg.cc/3dWTwGmp.

BCM unterschied sich in mehrfacher Hinsicht von Telegram und anderen Instant-Messengern. Insbesondere arbeitete der Dienst mit dezentralen Servern. Im Gegensatz zu anderen Messenger-Diensten, die Benutzerdaten und -inhalte auf zentralen Servern speichern, über die der Dienstanbieter die Kontrolle hat, verteilten BCM und andere dezentrale Plattformen die Serverknoten über das Benutzernetzwerk, sodass jeder Benutzer selbst über die Speicherung seiner Daten und deren Zugänglichkeit bestimmen kann.[27] Während einige Instant-Messenger für bestimmte (aber nicht alle) Kommunikationsformen Ende-zu-Ende-Verschlüsselung anbieten und zum Teil nur auf Nachfrage, wurden über BCM gesendete Mitteilungen standardmäßig verschlüsselt.[28] Ansonsten ähnelte BCM im Funktionsumfang (Privat- und Gruppen-Chats) und dem verwendeten Verschlüsselungsalgorithmus Telegram.[29]

Um bei BCM einen Account zu erstellen, konnten potenzielle Benutzer einfach die Anwendung herunterladen und sich mit einer Benutzer-ID registrieren. Anders als bei Telegram war für die Registrierung keine Telefonnummer erforderlich.[30] Für den Zugang zu bestimmten Gruppen brauchte man einen URL-Link zu den Inhalten, und für die direkte Kontaktaufnahme mit anderen Benutzern musste man deren BCM-Public-Key oder Benutzer-ID kennen. BCM basierte auf einer „dezentralen Infrastruktur- und Anwendungsplattform“ namens AME, die nach dem Prinzip „Null Vertrauen“ aufgebaut ist: „die BCM-App vertraut niemandem außer sich selbst, nicht einmal dem BCM-Server.“[31] Außenstehenden, einschließlich dem BCM-Server, war es nicht möglich, zwischen Benutzern gesendete Mitteilungen zu entschlüsseln. BCM bietet außerdem eine Wallet für Kryptowährungen an, die auch nach der Abschaltung des Messaging-Diensts weiterhin zur Verfügung steht.[32] Daher wird gelegentlich fälschlicherweise behauptet, dass der Messenger auf einer Blockchain basiert habe, was aber nur für die digitale Wallet zutrifft.[33]

Laut der Datenschutzerklärung von BCM wird das Unternehmen „ohne Ihre vorherige Zustimmung keine [Benutzerdaten] verwenden oder an Dritte weitergeben“.[34] Das dezentrale Netzwerk und die standardmäßige Ende-zu-Ende-Verschlüsselung für die gesamte Kommunikation machten es dem Unternehmen selbst unmöglich, zwischen den Nutzern ausgetauschte Mitteilungen zu entschlüsseln. Da die Benutzerdaten auf einzelnen Knoten im Netzwerk gespeichert sind, wäre es für Strafverfolgungsbehörden äußerst schwierig, Serverzugang zu verlangen.[35] Das Unternehmen machte keinerlei Angaben dazu, wie es gegen terroristische oder extremistische Inhalte vorzugehen gedenke, ein Unternehmenssprecher ließ jedoch verlauten, dass man sich zwar an das jeweils geltende Recht halten, aber „unter keinen Umständen Aufforderungen zur Entschlüsselung nachkommen oder Hintertüren zur Überwachung von Inhalten öffnen“ werde.[36]

27 Yuan et. al. „AME Blockchain: An Architecture Design for Closed-Loop Fluid Economy Token System.“
28 „FAQ.“ ohne Jahr. BCM Messenger. Abgerufen am 1. April 2020. https://web.archive.org/web/20200115224708/https://bcm.social/faq.html.
29 Ebd.
30 Ebd.
31 Ebd.
32 Ebd.
33 Ebd.
34 BCM Messenger, „Privacy Policy.“
35 Ebd.
36 Ebd.

Gab Chat

Gab wurde 2016 als Twitter-„Alternative für freie Meinungsäußerung“ gegründet. Mitbegründer Andrew Torba nannte ein „linksgerichtetes Big-Social-Monopol“ als Hauptbeweggrund für die Schaffung der Plattform.[37] Gab wurde als Koordinationsstelle für Rechtsextremisten im Internet berüchtigt und geriet ins Visier, als bekannt wurde, dass der Attentäter, der im Oktober 2018 in der Tree-of-Life-Synagoge in Pittsburgh mehrere Menschen erschoss und verletzte, Mitglied einer Randgruppe von Neonazis auf der Plattform war.[38] Seitdem haben mehrere Internetdienstanbieter die Zusammenarbeit mit Gab eingestellt.[39] Nach mehreren Anbieterwechseln gibt es auf Gab noch immer über 1.000.000 Accounts und eine stabile rechtsextreme Community.[40]

Ende Januar 2020 gab Gab bekannt, dass man dabei sei, eine Telegram ähnliche Instant-Messaging-Plattform namens Gab Chat einzuführen.[41] Der Dienst wird als „verschlüsselter Messaging-Dienst mit öffentlichen und privaten Chat-Räumen“ beworben.[42] Torba gab an, dass, wie bei Telegram, die Kommunikation in den öffentlichen Chat-Räumen nicht standardmäßig verschlüsselt werde, aber es gebe eine End-to-End-Verschlüsselung für private Chats: „In den verschlüsselten Räumen kann niemand außer den Mitgliedern im Raum mitlesen, nicht einmal Gab.“[43] Außerdem werde die App für Gab Chat nur auf der Website von Gab angeboten und nicht in den beliebten App-Stores von Google und Apple.[44]

Der Hauptvorteil von Gab als Plattform für Extremisten ist die Zusicherung des Unternehmens, dass keine Content-Moderation oder Entfernung von Content stattfinde. Sie betrachtet die Redefreiheit als unantastbar und ist stolz auf ihre grundsätzliche Ablehnung jeglicher Zensur.[45] Sollte jedoch „eine unrechtmäßige Bedrohung auf der Plattform entdeckt werden oder wir Kenntnis von gravierendem gewalttätigem Verhalten außerhalb der Plattform durch eine Person erhalten, die möglicherweise ein Account auf unserer Website eingerichtet hat“, wird das Unternehmen „eng mit den Strafverfolgungsbehörden auf Bundes-, Kommunal- und Bundesstaatsebene [kooperieren] und [kommunizieren] ..., um bei der Verhinderung schwerer Straftaten zu helfen.“[46]

Gab Chat befindet sich noch im Beta-Stadium.[47] Angesichts der Beliebtheit von Gab bei Rechtsextremisten als Alternative zu den stärker der Öffentlichkeit zugewandten Social-Media-Anbietern wie Twitter und Facebook ist jedoch zu erwarten, dass Rechtsextreme Gab Chat in gewissem Umfang annehmen werden. Hierfür spricht

37 Lorenz, Taylor. 2018. „The Pittsburgh Suspect Lived in the Web’s Darkest Corners.“ The Atlantic. 27. Oktober 2018. https://www.theatlantic.com/technology/archive/2018/10/what-gab/574186/.
38 Ebd.
39 Jurecic, Quinta. 2018. „Gab Vanishes, and the Internet Shrugs.“ Lawfare. 29. Oktober 2018. https://www.lawfareblog.com/gab-vanishes-and-internet-shrugs.
40 „When Twitter Bans Extremists, GAB Puts Out the Welcome Mat.“ 2019. Anti-Defamation League. 11. März 2019. https://www.adl.org/blog/when-twitter-bans-extremists-gab-puts-out-the-welcome-mat.
41 Torba, Andrew. 2020. „AG Barr Is Wrong On Encryption. Introducing Gab Chat: An Open Source Encrypted Messaging Platform.“ Gab News (Blog). 31. Januar 2020. https://news.gab.com/2020/01/31/ag-barr-is-wrong-on-encryption-introducing-gab-chat-our-open-source-encrypted-messaging-platform/.
42 Ebd.
43 Ebd.
44 Ebd.
45 Torba, Andrew. 2019. „Gab’s Policies, Positions, and Procedures for Unlawful Content And Activity On Our Social Network.“ Gab News (Blog). 23. August 2019. https://news.gab.com/2019/08/23/gabs-policies-positions-and-procedures-for-unlawful-content-and-activity-on-our-social-network/.
46 Ebd.
47 Torba, „AG Barr is Wrong on Encryption.“

auch die Popularität von Telegram und Telegram ähnlichen Diensten bei Rechtsextremisten. Wenn Gab Chat unter dem Banner von Gab ähnliche Dienste anbietet wie Telegram, ist es denkbar, dass Rechtsextremisten es als einen ihnen entgegenkommenden Instant-Messaging-Dienst betrachten und versuchen werden, die Plattform auszunutzen, sobald sie voll funktionsfähig ist.

Hoop Messenger

Hoop Messenger ist eine Instant-Messaging-App, die, ähnlich wie Telegram, Kommunikationsmöglichkeiten in Form von privaten Chats, Chatrooms und One-to-many-Kanälen bietet. Der Dienst wird von einem kleinen Unternehmen in Kanada betrieben.[48] Im Anschluss an die von Europol koordinierten Löschaktionen von IS-Medien richteten im Dezember 2019 mehrere offizielle und inoffizielle IS- und al-Qaida-Medien auf Hoop Messenger Kanäle ein, nachdem einige Anhänger die Plattform als sichere Alternative zu Telegram propagiert hatten.[49] Einige Tage später entfernte das Unternehmen jedoch eine große Anzahl von IS-Kanälen von seiner Plattform.[50] Ende Januar 2020 warnte eine dem IS nahestehende Medienstiftung ihre Anhänger vor der Verwendung von Hoop Messenger mit der Behauptung, die Plattform sammle in großem Umfang persönliche Daten und Informationen von Nutzern.[51]

Auch heute gibt es noch eine erhebliche IS-Präsenz auf Hoop Messenger. Einige namhafte IS-Anhänger sehen das Angebot als die derzeit möglicherweise attraktivste Alternative zu Telegram. Anfang Juni 2020 schickte ein Kanal der Nashir News Agency auf Telegram eine „dringende" Botschaft an seine Follower, wonach Hoop Messenger die bevorzugte Plattform für die Verbreitung von Nachrichten sei.[52] Diese Botschaft erfolgte im Zuge des anhaltenden Drucks auf dem IS nahestehende Kanäle auf Telegram. In den Tagen nach der Botschaft importierten Anhänger zahlreiche dem IS nahestehende Kanäle von Telegram in Hoop Messenger.[53] Die dem IS angegliederte Stiftung Electronic Horizons Foundation, die für die Produktion von Inhalten zur digitalen und funktionalen Sicherheit zuständig ist, gab für ihre Abonnenten ein Handbuch heraus, wie Hoop Messenger sicher zu verwenden sei.[54] Diesen Bemühungen zu Trotz reagierte Hoop Messenger erneut und startete eine weitere Kampagne, um Pro-IS-Inhalte von der Plattform zu tilgen.[55]

48 „FAQ." ohne Jahr. Hoop Messenger. Abgerufen am 1. April 2020. http://hoopmessenger.com/faq/.
49 Amarasingam, Amarnath. 2019. „Telegram Deplatforming ISIS Has Given Them Something to Fight For." Vice. 5. Dezember 2019. https://www.vice.com/en_us/article/vb55bd/telegram-deplatforming-isis-has-given-them-something-to-fight-for; Bloom, Mia. 2019. „No Place to Hide, No Place to Post: Lessons from Recent Efforts at ‚De-Platforming' ISIS." Just Security. 5. Dezember 2019. https://www.justsecurity.org/67605/no-place-to-hide-no-place-to-post-lessons-from-recent-efforts-at-de-platforming-isis/; Seldin, Jeff. 2019. „IS Struggles to Regain Social Media Footing After Europe Crackdown." Voice of America. 4. Dezember 2019. https://www.voanews.com/europe/struggles-regain-social-media-footing-after-europe-crackdown.
50 Ebd.
51 „Pro-ISIS Media Foundation Warns ISIS Supporters Against Using Hoop Messenger." 2020. MEMRI. 27. Januar 2020. https://www.memri.org/cjlab/pro-isis-media-foundation-warns-isis-supporters-against-using-hoop-messenger.
52 „ISIS Media Outlet Announces Shift To Canadian Hoop Messenger App After Wave Of Account Deletions On Telegram." 2020. MEMRI. 5. Juni 2020. https://www.memri.org/cjlab/isis-media-outlet-announces-shift-canadian-hoop-messenger-app-after-wave-account-deletions.
53 Ebd.
54 Gluck, Raphael. 2020. „Aus dem jüngsten AFAQ-Angebot – Eine Anleitung zur sicheren Nutzung von Hoop Messenger – die neue App der Wahl des IS nach anhaltenden Löschungen auf Telegram. – Die Zeitschrift ‚The Supporters Security' bemüht sich um höheres Sicherheitsbewusstsein bei ‚Tastatur-Kriegern' – Debian-Video-Tutorial." Tweet, 3. Juli 2020. https://twitter.com/einfal/status/1279124715957891072.
55 Alkhouri, Laith. 2020. „Mehrere offizielle und inoffizielle #ISIS-Kanäle wurden von Hoop Messenger, der bevorzugten Kommunikations-/Propaganda-Plattform der Gruppe, entfernt. Dies hatte jedoch kaum Auswirkungen auf die Medienverbreitung der Gruppe, die sich frühzeitig Dutzende von Backup-Kanälen geschaffen hat." Tweet, 6. August 2020. https://twitter.com/MENAanalyst/status/1291415487453302790.

Was Hoop Messenger von anderen Instant-Messaging-Diensten unterscheidet, ist der „Vault“ (Tresorraum), ein passwortgeschütztes Dateispeichersystem, in dem Benutzer Chats, Fotos, Videos und andere Dateien ablegen können. Sobald ein Benutzer ein Passwort erstellt hat, werden alle Chats und Dateien im Vault durchgehend verschlüsselt, und zwar sowohl auf dem Gerät des Benutzers als auch in der Cloud. Ansonsten gibt es für Kanäle und alle anderen Chats keine End-to-End-Verschlüsselung.[56] Benutzer können zudem „Fake“-Passwörter für ihren Vault erstellen, die bei der Eingabe zur Selbstzerstörung der Inhalte im Vault führen.[57] Über die Website des Dienstes besteht für Benutzer außerdem die Möglichkeit, ihren Account aus der Ferne zu löschen. Hierdurch werden alle Daten des Benutzeraccounts und die auf seinem Smartphone gespeicherten persönlichen Daten endgültig gelöscht.[58] Dem Unternehmen zufolge sind die Dummy-Passwörter für den Vault und dessen Selbstzerstörung sehr hilfreich, wenn „Sie sich in Bereiche begeben, in denen Sie Ihr Handy abgeben müssen ... Löschen Sie Hoop einfach und laden Sie es wieder herunter, sobald Ihr Gerät wieder sicher in Ihren Händen ist.“[59]

Die Erstellung eines Accounts in Hoop Messenger erfordert die Registrierung mit einer Telefonnummer und/oder E-Mail-Adresse. Anders als bei anderen Plattformen können Benutzer mehrere Benutzer-IDs für denselben Account erstellen.[60] Für die End-to-End-Verschlüsselung von Chats ist ein Opt-in-Verfahren vorgesehen, was nur durch den Vault möglich ist. Hoop Messenger bietet jedoch auch einen integrierten VPN-Browser (Virtual-Private-Network-Browser), sodass Benutzer aus der Anwendung heraus anonym im Netz surfen können.[61] In der Gestaltung und Funktionalität ähnelt die Plattform Telegram.

Abschnitt 9, 10 und 11 der Nutzungsbedingungen von Hoop Messenger regeln den Umgang des Dienstes mit schädlichen Inhalten. Der Dienst verbietet „anstößiges Verhalten und für uns inakzeptable Inhalte“ und weist darauf hin, dass das Unternehmen Inhalte oder Benutzerkonten entfernt, die gegen die Nutzungsbedingungen verstoßen.[62] Im Dezember 2019 stellte das Unternehmen klar, dass diese Vorgehensweise auch für terroristische Inhalte gelte und gab an, dass das Unternehmen „auch weiterhin dem IS nahestehende Gruppen schließen“ werde, nachdem es zahlreiche mit dem IS sympathisierende Kanäle und Chats von der Plattform gelöscht hatte.[63] Aufgrund des koordinierten Vorgehens des Unternehmens gegen IS-Inhalte und -Konten scheinen einige Sympathisanten von Hoop Messenger abgerückt zu sein und warnen vor dessen Verwendung.[64] Dessen ungeachtet sind andere IS-Anhänger nach wie vor davon überzeugt, dass die Plattform die zweckdienlichste Telegram-Alternative ist.

56 Hoop Messenger, „FAQ“.
57 Ebd.
58 Ebd.
59 „Hoop Messenger.“ ohne Jahr. Hoop Messenger. Abgerufen am 1. April 2020. http://hoopmessenger.com/.
60 Ebd.
61 Ebd.
62 „Privacy & Terms.“ ohne Jahr. Hoop Messenger. Abgerufen am 1. April 2020. http://hoopmessenger.com/legal/.
63 @HoopMessenger, 2019. „Wir werden weiterhin dem IS nahestehende Gruppen schließen. Wir rufen dazu auf, uns verdächtige Kanäle per E-Mail zu senden. Da unser Team relativ klein ist, sind wir auf die Mithilfe der Öffentlichkeit angewiesen. Wenn Sie Fragen haben, wenden Sie sich bitte per E-Mail oder Direktnachricht an unser Team.“ 5. Dezember 2019. https://twitter.com/HoopMessenger/status/1202698188160811008.
64 MEMRI, „Pro-ISIS Media Foundation Warns ISIS Supporters Against Using Hoop Messenger.“

Riot.im

Riot.im (im Juli 2020 umbenannt in Element) ist eine dezentrale Chat-Anwendung im Matrix-Netzwerk.[65] Sie bietet Kommunikation in Form von Eins-zu-eins-Chats und Gruppen, einige File-Sharing-Funktionen und lässt den Nutzern die Wahl hinsichtlich der Zugriffsmöglichkeiten auf die Kommunikation.[66] Riot.im wurde ursprünglich als Plattform für die virtuelle Office-Kollaboration konzipiert und ähnelt vom Aufbau her anderen Instant-Messenger-Apps in dieser Kategorie (z. B. Slack, Twist, Microsoft Teams).[67] Während einer Phase des Experimentierens mit dezentralen Web-Plattformen begannen IS-Anhänger im September 2017 zunächst damit, Gruppen auf der Plattform zu gründen. Kurz darauf folgten al-Qaida und andere Dschihad-Anhänger.[68] Diese Gruppen sind seit 2017 durchgehend auf der Plattform vertreten.[69] Da sich jedoch die meisten Sympathisanten für die Speicherung der Kommunikation auf dem öffentlichen Server des Unternehmens entschieden, kommt es durch Löschung von Content und Accounts immer wieder zu Störungen der dschihadistischen Netzwerke auf den Servern von Riot.im.[70] Beobachter rechtsextremer Gruppen im Internet stellen auch fest, dass einige prominente rechtsextreme Kanäle auf Telegram damit beginnen, auf Riot.im eine Präsenz aufzubauen.[71]

Da Riot.im dezentrale Kommunikation über die Matrix-Protokolle anbietet, befürchteten Beobachter extremistischer Online-Aktivitäten, dass Riot.im „die nächste verbesserte Version von Telegram werden könnte“, wenn Extremisten beginnen, ihre eigenen Server zu hosten.[72] Zum Speichern ihrer Kommunikation bietet Riot.im seinen Benutzern die Wahl zwischen dem öffentlichen Server matrix.org, einem kostenpflichtigen Premium-Server, der von dem jeweiligen Benutzer (bzw. seiner Organisation) gehostet wird, anderen öffentlichen Servern, die von den Benutzern von Riot.im eingerichtet wurden, oder individuell zugeschnittenen Servern.[73] Die Plattform bietet zwar dezentralisierte Server an, verlangt allerdings, dass sich der einzelne Benutzer anmeldet und dann den Server verwaltet. Unabhängig davon, ob die Kommunikation auf einem zentralen, öffentlichen oder einem dezentralen Server liegt, können Riot.im-Benutzer eine Ende-zu-Ende-Verschlüsselung für ihre Kommunikation aktivieren.[74]

Das Anlegen eines Riot.im-Accounts erfordert die Festlegung eines Benutzernamens und eines Passworts. Eine E-Mail-Adresse kann freiwillig angegeben werden.[75] Nach der Erstellung eines Accounts kann der Eigentümer eines Chats dessen Einstellungen ändern, sodass entweder nur ausgewählte Benutzer teilnehmen

65 „Features.“ ohne Jahr. Riot.im. Abgerufen am 1. April 2020. https://about.riot.im/features.
66 Ebd.
67 Ebd.
68 Flashpoint, „Jihadists Presence Online Decentralizes After Telegram Ban“; Gluck, „Islamic State Adjusts Strategy to Remain on Telegram“.
69 Ebd.
70 King, Peter. 2019. „Islamic State Group’s Experiments with the Decentralized Web.“ Europol. https://www.europol.europa.eu/publications-documents/islamic-state-group%E2%80%99s-experiments-decentralised-web.
71 Kommunikation mit Jon Lewis, Program on Extremism, 1. April 2020.
72 Bodo, Lorand. 2018. „Decentralised Terrorism: The Next Big Step for the so-Called Islamic State (IS)?“ VOX – Pol. 12. Dezember 2018. https://www.voxpol.eu/decentralised-terrorism-the-next-big-step-for-the-so-called-islamic-state-is/.
73 Riot.im, „Features“.
74 Ebd.
75 Ebd.

können, dass nur Benutzer mit einem URL-Link auf den Chat zugreifen können oder dass der Chat öffentlich gemacht wird.[76] Die Teilnehmer können zudem die Ende-zu-Ende-Verschlüsselung für Mitteilungen aktivieren.

Riot.im ist auf der Matrix-Plattform aufgebaut, und seine öffentlichen Server werden im Matrix-Netzwerk gehostet. Beide Dienste haben ihren Sitz im Vereinigten Königreich.[77] Die Beziehung zwischen Riot.im und Matrix hat merklichen Einfluss darauf, wie Extremisten den Schutz der Privatsphäre und die Sicherheit auf der Plattform wahrnehmen. Vor allem entscheiden sich extremistische Riot.im-Nutzer häufig dafür, die Kommunikation auf den öffentlichen Matrix-Standardservern zu hosten, anstatt ihre eigenen dezentralen Server einzurichten und zu verwalten.[78] Das bedeutet, dass ihre Kommunikation unter die Nutzungsbedingungen von Matrix fällt und den strengen Vorschriften hinsichtlich extremistischer Online-Inhalte im Vereinigten Königreich unterliegt. Die Nutzungsbedingungen von Matrix verbieten die Nutzung des Dienstes „für ungesetzliche Zwecke oder zur Unterstützung von nach britischem/EU-Recht illegalen Aktivitäten“, einschließlich terroristischer Inhalte.[79] Das Unternehmen entfernt somit regelmäßig extremistische Inhalte und Accounts von seinen Plattformen. Wenn extremistische Gruppen Inhalte auf dezentralen Servern von Drittanbietern hosten, haben sie es häufig mit unzuverlässigem Service und unabhängigen Löschaktionen kleiner Plattformbetreiber zu tun.[80] Bislang haben nur wenige Extremisten die Initiative ergriffen, Chats auf Riot.im auf selbstverwalteten Servern zu hosten.[81]

Rocket.Chat

Rocket.Chat ist eine dezentrale Instant-Messaging-Plattform, die es ihren Nutzern ermöglicht, Inhalte und Kommunikation auf ihren eigenen Servern zu hosten oder Material auf dem öffentlichen Rocket.Chat-Server zu speichern.[82] Bemerkenswert ist, dass das zentrale IS-Medium im Dezember 2018 mit der Verwaltung eines eigenen Servers für die Kommunikation auf Rocket.Chat experimentierte. Dies war einer der ersten Versuche von Dschihadisten, die Vorteile dezentraler Web-Plattformen voll auszuschöpfen.[83] Die Nashir News Agency des IS hostete mehrere Rocket.Chat-Kanäle auf einem Server namens Techhaven, der laut Benutzerhinweisen den Zweck hatte, „ein offenes Forum für Diskussionen, digitale Privatsphäre und Innovation für unterdrückte Nutzer in Konfliktzonen zu bieten, die wegen ihrer Überzeugungen von den autoritären Regimen des Westens verfolgt werden.“[84] Seitdem haben der IS und andere dschihadistische Gruppen, darunter al-Qaida, Kanäle und Gruppen auf Rocket.Chat eingerichtet.[85]

76 Ebd.
77 „Privacy Notice.“ ohne Jahr. Riot.im. Abgerufen am 1. April 2020. https://riot.im/privacy.
78 King, „Islamic State Group’s Experiments with the Decentralized Web“.
79 Riot.im, „Privacy Notice“.
80 King, „Islamic State Group’s Experiments with the Decentralized Web“.
81 Ebd.; Bodo, „Decentralized Terrorism“.
82 „Rocket.Chat“. ohne Jahr. Rocket.Chat. Abgerufen am 1. April 2020. https://rocket.chat/.
83 BBC News. 2019. „Europol Disrupts IS Propaganda Machine.“ 25. November 2019, Sektion Naher Osten. https://www.bbc.com/news/world-middle-east-50545816.
84 King, „Islamic State Group’s Experiments with the Decentralized Web“.
85 Flashpoint, „Jihadists Presence Online Decentralizes After Telegram Ban“.

Unter den in diesem Bericht untersuchten Plattformen ist Rocket.Chat insofern Riot.im am ähnlichsten, als es sich bei beiden um Messaging-Plattformen handelt, die ursprünglich für Teams in Büroumgebungen konzipiert wurden und den Nutzern die Wahl zwischen zentral verwalteten Servern und nutzerverwalteten, dezentralen Servern bieten.[86] Dabei ist es auf Rocket.Chat einfacher, einen Server zu erstellen und zu verwalten, als auf Riot.im. Um einen Account auf dem öffentlichen Rocket.Chat-Server einzurichten oder sich bei einem privat gehosteten Server anzumelden, sind ein Benutzername, ein Passwort und eine E-Mail-Adresse erforderlich.[87] Sobald der Account eingerichtet ist, kann der Nutzer mit anderen Nutzern direkt chatten und öffentliche oder nur auf Einladung zugängliche Kanäle einrichten. Die Plattform umfasst zudem einige besondere Funktionen, die für extremistische Gruppen unter Umständen attraktiv sind, z. B. die automatische Übersetzung von fremdsprachigen Beiträgen.[88]

Die Option, dezentrale Server zu hosten, stellt für extremistische Gruppen eine Schwierigkeit dar. Wenn sie ihre Rocket.chat-Kommunikation auf dem zentralen Server des Unternehmens hosten, kann das Unternehmen entweder Kanäle entfernen, die gemäß den Nutzungsbedingungen Extremismus fördern, oder es ist unter Umständen „verpflichtet, Ihre persönlichen Daten offenzulegen, wenn das Gesetz es verlangt, oder im Falle einer zulässigen Aufforderung durch die Behörden.“[89] Die Kommunikation stattdessen auf einem dezentralen Server zu hosten, kann zeitaufwendig sein. Es erfordert ein gewisses technisches Know-how und kann für extremistische Gruppen noch andere Probleme mit sich bringen.[90] Drei Monate, nachdem die Nashir News Agency ihre Kanäle auf dem Techhaven-Server eingerichtet hatte, erfuhr der Host eine von zahlreichen anderen Rechnern ausgehende Dienstblockade (Distributed Denial of Service, DDoS), die die meisten Rocket.chat-Kanäle funktionsunfähig machte.[91] Die Einrichtung eines eigens für extremistische Propaganda vorgesehenen Servers kann diesen zur Zielscheibe für digitale Angriffe machen. Im Falle erfolgreicher DDoS-Aktionen können extremistische Gruppen auf dezentralen Plattformen wie Rocket.chat sich gezwungen sehen, von Server zu Server zu springen, was den Nutzen der Plattform als stabile Basis für Propaganda einschränkt.

86 Rocket.Chat, „Rocket.Chat“.
87 Ebd.
88 Ebd.
89 „Rocket.Chat Privacy Policy.“ ohne Jahr. Rocket.Chat. Abgerufen am 1. April 2020. https://rocket.chat/privacy.
90 King, „Islamic State Group’s Experiments with the Decentralized Web“.
91 Ebd.

TamTam

Der Online-Instant-Messenger TamTam wird von der Mail.ru Group verwaltet. Das Unternehmen hält den größten Anteil am russischsprachigen Internet und betreibt auch die beliebten Social-Media-Plattformen Vkontakte und Odnoklassniki.[92] Im Funktionsumfang ist TamTam fast identisch mit Telegram aufgebaut. Der Messenger bietet Chats, öffentliche Kanäle, private Kanäle und Gruppen-Chats.[93] Die Ähnlichkeit zwischen Telegram und TamTam ist beabsichtigt. Während der fortgesetzten Bemühungen der russischen Regierung, Telegram-IP-Adressen im russischen Internet zu blockieren, schuf die Mail.ru Group TamTam als Telegram-Alternative.[94] Die Mail.ru Group unterhält enge Beziehungen zur russischen Regierung und ist angeblich eher bereit, Aufforderungen der russischen Strafverfolgungsbehörden zur Herausgabe von Nutzerdaten nachzukommen, als Telegram.[95]

Im Anschluss an die von Europol koordinierte Aktion auf Telegram im Dezember 2019 richteten IS-Anhänger eine beträchtliche Anzahl von Kanälen und Gruppen auf TamTam ein.[96] TamTam handelte umgehend gegen den Aufwärtstrend bei IS-Inhalten.[97] Ein Unternehmenssprecher sagte gegenüber Vice News, TamTam sei „entschieden gegen die Präsenz jeglicher Art von Inhalten terroristischer Organisationen auf unserer Plattform“ und forderte seine Nutzer auf, Inhalte und Accounts, die terroristische Gruppen unterstützen, zu melden.[98] Nach den Tilgungsmaßnahmen bei TamTam begannen dschihadistische Gruppen, ihren Anhängern von der Nutzung der Plattform abzuraten.[99] So postete zum Beispiel im Februar 2020 eine Gruppe englischsprachiger IS-Anhänger namens „Lions of Tawheed“ auf Rocket.Chat: „die russische Regierung hat Zugang zu allen TamTam-Accounts ... schützen Sie sich, indem Sie TamTam von Ihrem Smartphone bzw. Computer entfernen. Verwenden Sie sichere Anwendungen wie Riot, Rocket.Chat und Telegram.“[100]

Die Vorgehensweise zur Erstellung eines Accounts und für den Zugang zu Inhalten ist bei TamTam dieselbe wie bei Telegram. Der Dienst bietet den gleichen Funktionsumfang wie Telegram, mit Optionen für Eins-zu-eins-Chats, One-to-many-Kanäle und Chats in großen Gruppen.[101] Nutzer können Chats und Kanäle öffentlich oder privat auf Einladung zugänglich machen.[102] Die Ähnlichkeiten von TamTam mit Telegram erstrecken sich sogar auf den Domainnamen. Die verkürzten Hyperlinks von Telegram sind über den Domain-Namen t.me zugänglich; TamTam benutzt

92 „Some Messenger Called ‚TamTam‘ Is Trying to Replace Telegram in Russia. What the Heck Is It?“ 2018. Meduza. 17. April 2018. https://meduza.io/en/feature/2018/04/17/some-messenger-called-tamtam-is-trying-to-replace-telegram-in-russia-what-the-heck-is-it.
93 Ebd.
94 Ebd.
95 Ebd.
96 Flashpoint, „Jihadists Presence Online Decentralizes After Telegram Ban“; Gluck, „Islamic State Adjusts Strategy to Remain on Telegram“; Amarasingam, „Telegram Deplatforming ISIS Has Given Them Something to Fight For“; Bloom, „No Place to Hide, No Place to Post.“
97 Ebd.
98 Gilbert, David. 2019. „The Russian Social Network Letting ISIS Back Online.“ Vice. 3. Dezember 2019. https://www.vice.com/en_us/article/d3ane7/islamic-state-cant-find-an-online-home-so-they-might-build-their-own-app.
99 „Pro-ISIS Outlet Lists ‚Safe‘ Messaging Apps, Advises Against Using Chinese, Russian Apps.“ 2020. MEMRI. 18. März 2020. https://www.memri.org/cjlab/pro-isis-outlet-lists-safe-messaging-apps-advises-against-using-chinese-russian-apps.
100 Ebd.
101 „About TamTam.“ ohne Jahr. TamTam. Abgerufen am 1. April 2020. https://about.tamtam.chat/en/index.html.
102 Ebd.

hierfür tt.me.[103] Das Unternehmen vermarktet auf dem russischen Markt aktiv seine Kompatibilität mit Telegram, indem es auf populären russischen Telegram-Kanälen offen mit seiner Ähnlichkeit zu Telegram wirbt.[104]

Der Hauptunterschied zwischen Telegram und TamTam betrifft den Schutz der Privatsphäre und Sicherheit. TamTam ist in der Russischen Föderation registriert, und seine Datenschutzrichtlinien „werden in Übereinstimmung mit den Gesetzen der Russischen Föderation umgesetzt".[105] Das heißt, dass TamTam, im Gegensatz zu Telegram, aktiv russisches Recht befolgt, wonach Dienstanbieter dem Inlandsgeheimdienst (FSB), der zentralen Strafverfolgungsstelle in der Russischen Föderation, Backdoor-Access gewähren muss.[106] Zwar bietet TamTam Verschlüsselung an, doch gehen Experten davon aus, dass Kopien der TamTam-Verschlüsselungsschlüssel dem FSB übergeben wurden.[107] TamTams Nutzungsvereinbarung verbietet ausdrücklich, „Extremismus oder Terrorismus [zu propagieren], Feindseligkeit aufgrund von Rasse, ethnischer oder nationaler Identität zu schüren" oder „dem Wesen nach extremistische Informationen" zu veröffentlichen.[108] Man darf annehmen, dass IS-Anhänger, die in der Folge der Europol Referral Action Days 2019 versuchten, TamTam auszunutzen, dies wegen der Ähnlichkeit mit Telegram taten und nicht wegen der Maßnahmen zum Schutz der Privatsphäre und der Sicherheit.

103 Meduza, „Some Messenger Called ‚TamTam' Is Trying to Replace Telegram in Russia."
104 Ebd.
105 „TamTam Messenger Confidentiality Policy." ohne Jahr. TamTam. Abgerufen am 1. April 2020. https://about.tamtam.chat/en/policy/index.html.
106 Ebd.
107 Ebd.
108 „TamTam Messenger End User License Agreement." ohne Jahr. TamTam. Abgerufen am 1. April 2020. https://about.tamtam.chat/en/license/index.html.

Abbildung 1: Vergleich der von Extremistengruppen verwendeten Instant-Messaging-Plattformen

Plattform	Extremistische Nutzung	Land der Eintragung	Eigenschaften und Funktionen	Sicherheit	Kooperationsbereitschaft mit politischen/ gesetzlichen Forderungen
Telegram	Dschihadistischer Extremismus (IS, al-Qaida), Rechtsextremismus	Britische Jungferninseln / Vereinigte Arabische Emirate	• Eins-zu-eins-Chats • Gruppen-Chats • Öffentliche und private Chats	• Ende-zu-Ende-Verschlüsselung für Eins-zu-eins-Chats • Selbstzerstörung von Accounts/Daten	• Sagt die Entfernung „terroristischer“ öffentlicher Inhalte (Bots und öffentliche Kanäle) zu • Sagt zu, auf gerichtliche Anordnung in Fällen von Terrorverdacht den Strafverfolgungsbehörden Nutzerdaten zur Verfügung zu stellen
BCM*	Dschihadistischer Extremismus (IS)	Britische Jungferninseln	• Eins-zu-eins-Chats • Gruppen-Chats	• Ende-zu-Ende-Verschlüsselung • Selbstzerstörung von Accounts/Daten • Option dezentraler Server	• Keine bekannten Grundsätze zur Entfernung oder Moderation extremistischer Inhalte • Keine Offenlegung von Nutzerdaten gegenüber Strafverfolgungsbehörden
Gab Chat**	Rechtsextremismus	Vereinigte Staaten von Amerika	• Eins-zu-eins-Chats • Gruppen-Chats	• Ende-zu-Ende-Verschlüsselung auf dem Gerät • Nachrichtenlöschung auf dem Server nach 30 Tagen	• „Beleidigende“ und „hasserfüllte“ Rede ist kein Grund für die Entfernung von Inhalten, nur „illegale Inhalte und Aktivitäten“ • Sagt zu, bei rechtmäßiger Abfrage von Benutzerdaten im Rahmen von Untersuchungen mit der US-Regierung zusammenarbeiten, nicht jedoch mit anderen Regierungen oder Dritten
Hoop Messenger	Dschihadistischer Extremismus (IS, al-Qaida)	Kanada	• Eins-zu-eins-Chats • Gruppen-Chats • Öffentliche und private Kanäle	• Ende-zu-Ende-Verschlüsselung aller Chats und der Dateien im passwortgeschützten „Vault“ • Fernlöschung von Accounts und Inhalten im Vault	• Zusicherung des Unternehmens: „[wir] werden Inhalte entfernen, die wir nach unserem alleinigen Ermessen für ungesetzlich, obszön, beleidigend, bedrohlich, verleumderisch, diffamierend oder anderweitig inakzeptabel halten”

Plattform	Extremistische Nutzung	Land der Eintragung	Eigenschaften und Funktionen	Sicherheit	Kooperations-bereitschaft mit politischen/ gesetzlichen Forderungen
Riot.im	Dschihadistischer Extremismus (IS, al-Qaida), Rechts-extremismus	Vereinigtes Königreich	• Eins-zu-eins-Chats • Gruppen-Chats	• Ende-zu-Ende-Verschlüsselung durch den Nutzer zu aktivieren • Option dezentraler Server	• Das Unternehmen kann Inhalte auf öffentlichen Servern entfernen, die „ungesetzlichen Zwecken dienen oder nach britischem/ EU-Recht illegale Aktivitäten unterstützen“.
Rocket.Chat	Dschihadistischer Extremismus (IS, al-Qaida)	Vereinigte Staaten von Amerika / Brasilien	• Eins-zu-eins-Chats • Gruppen-Chats • Öffentliche und private Kanäle	• Ende-zu-Ende-Verschlüsselung durch den Nutzer zu aktivieren • Option dezentraler Server	• Das Unternehmen ist „verpflichtet, Ihre personenbezogenen Daten offenzulegen, wenn dies gesetzlich vorgeschrieben ist, oder auf rechtmäßiges Verlangen öffentlicher Behörden“.
TamTam	Dschihadistischer Extremismus (IS, al-Qaida)	Russische Föderation	• Eins-zu-eins-Chats • Gruppen-Chats • Öffentliche und private Kanäle	• „Verschlüsselung“ (Protokoll unklar)	• Das Unternehmen verbietet die Propagierung von „Extremismus, Terrorismus, Erregung von Feindseligkeit aufgrund von Rasse, ethnischer oder nationaler Identität“ sowie die Veröffentlichung von „Informationen extremistischer Natur“ • „Nutzerdaten werden in Übereinstimmung mit den Gesetzen der Russischen Föderation verarbeitet“, woraus sich die obligatorische Offenlegung von Informationen und Verschlüsselungs-schlüsseln gegenüber den russischen Strafverfolgungs-behörden ergibt

* Dienst eingestellt, Februar 2020
** Derzeit in der Beta-Phase

4 Analyse: Die extremistische Nutzungshistorie der Instant-Messaging-Dienste

Das Experimentieren von Extremisten mit internetbasierten Instant-Messaging-Diensten ist ein wichtiger Aspekt ihrer Bemühungen um die Nutzung neuer Technologien. Auf die Schwierigkeiten bei Telegram folgt die extremistische Nutzung alternativer Messaging-Anwendungen im Allgemeinen dem, was Daveed Gartenstein-Ross, Matt Shear und David Jones als „Technologieaneignungskurve gewaltbereiter nichtstaatliche Akteure (violent non-state actors, VNSA)“ bezeichnen.[109] In der Anfangsphase der Aneignung unternehmen Extremisten (in der Regel erfolglose) Versuche, sich aufkommende Technologie zunutze zu machen.[110] In der Iterationsphase verbessern sie ihre Fähigkeit zur Nutzung der Technologie, während zugleich neue Produkte auf den Markt kommen, die ihre Bemühungen unterstützen.[111] Nach der Iteration kann extremistischen Gruppen ein Durchbruch gelingen – sie finden eine bestimmte Methode zur Nutzung der Technologie, von der ihre Strategien in hohem Maße profitieren.[112] Unweigerlich müssen sich extremistische Gruppen mit Abwehrmaßnahmen von staatlicher Seite oder durch Dienstanbieter auseinandersetzen.[113] Eine konsequente Abwehr kann die Aneignungskurve neu starten, diesmal für Alternativen zur ursprünglichen Technologie. Somit sind sie gezwungen, als Early Adopters mit neuen Technologien zu experimentieren.[114]

Der Durchbruch, der Extremisten im Zeitraum 2015–17 mit der Telegram-Nutzung gelungen ist, geht augenscheinlich in die Phase der Abwehr über. Im vergangenen Jahr hat Telegram in Zusammenarbeit mit Regierungsstellen begonnen, der extremistischen Nutzung der Plattform ernsthaft entgegenzutreten. Dies veranlasste Extremisten unterschiedlicher Couleur, sich für diverse Telegram-Alternativen wieder in die frühe Aneignungsphase zu begeben.[115] Der VNSA-Technologieaneignungskurve zufolge können wir davon ausgehen, dass ein Großteil der derzeitigen Bemühungen extremistischer Gruppen, eine nachhaltige und sichere Alternative zu Telegram zu finden, keinen Erfolg hatte. Allerdings können extremistische Gruppen auch eine Erfolgsbilanz vorweisen, wenn es um schnelles organisatorisches Lernen zwecks Nutzung neuer

109 Gartenstein-Ross, Daveed, Matt Shear und David Jones. 2019. „Virtual Plotters. Drones. Weaponized AI?: Violent Non-State Actors as Deadly Early Adopters.“ Washington, D.C.: Valens Global. http://valensglobal.com/virtual-plotters-drones-weaponized-ai-violent-non-state-actors-as-deadly-early-adopters/.
110 Ebd.
111 Ebd.
112 Ebd.
113 Ebd.
114 Ebd.
115 Flashpoint, „Jihadists Presence Online Decentralizes After Telegram Ban“; Gluck, „Islamic State Adjusts Strategy to Remain on Telegram“; Amarasingam, „Telegram Deplatforming ISIS Has Given Them Something to Fight For“; Bloom, „No Place to Hide, No Place to Post”.

Social-Media-Plattformen geht.[116] Mit dem Wechsel extremistischer Gruppen von Telegram zu neu aufkommenden und immer stabileren Instant-Messaging-Alternativen, die neue Eigenschaften in puncto Schutz der Privatsphäre und Sicherheit mitbringen, lautet die Frage nicht mehr „ob", sondern „wann" und „welche".

Unterschiedliche Gruppen von Extremisten werden sich wahrscheinlich zu unterschiedlichen Zeiten von Telegram abwenden, da sie auf der Plattform derzeit eine uneinheitliche Abwehr erfahren. Die gegen Extremisten auf Telegram gerichteten Maßnahmen seitens des Betreibers und staatlicher Stellen, von der Löschung von Content und Accounts bis hin zu Überwachungsmaßnahmen, konzentrieren sich weitgehend auf IS-Sympathisanten.[117] Derweil sehen sich die Anhänger anderer extremistischer Gruppen, darunter Rechtsextremisten und andere dschihadistische Gruppen, nur begrenzter Abwehr ausgesetzt und haben daher einen geringeren Anreiz, sich von der Plattform abzuwenden.[118] Nur IS-Anhänger werden sich wahrscheinlich auch weiterhin intensiv darum bemühen, neu aufkommende Instant-Messaging-Plattformen als Alternative zu Telegram auszutesten. Wenn Telegram jedoch beginnt, auch gegen andere Arten extremistischer Aktivitäten auf seiner Plattform hart durchzugreifen, könnte ein breiteres Spektrum von Dschihadisten und rechtsextremen Gruppen nachziehen.

Eine vorläufige Bewertung, ausgehend von den oben aufgeführten Plattformen, kann Hinweise auf einige der Merkmale liefern, auf die extremistische Gruppen bei einem Ersatz für Telegram Wert legen werden. Innerhalb dieser Gruppe von Instant-Messenger-Apps, die sich extremistische Gruppen im Zuge der intensivierten Abwehrmaßnahmen auf Telegram angeeignet haben, zeigen sich auffällige Ähnlichkeiten und Trends. Erstens bieten viele von ihnen ganz ähnliche Kommunikationsoptionen und Gestaltungsmerkmale wie Telegram. Es ist kein Zufall, dass in den Tagen nach den Europol-RAD-Maßnahmen TamTam eine der ersten Plattformen war, auf denen IS-Sympathisanten Follower um sich scharen konnten.[119] Die Anwendung ist eine nahezu identische Kopie von Telegram und wirbt sogar damit. Trotz der praktisch nicht existenten Sicherheits- und Datenschutzfunktionen zog TamTam aufgrund der großen Ähnlichkeit sofort extremistische Telegram-Nutzer an. In der Frühphase der Suche nach einem Ersatz sahen extremistische Gruppen die Ähnlichkeit mit Telegram als Vorteil an, weil sich die Anhänger durch einfache Handhabung und Vertrautheit schnell an die neue Plattform gewöhnen konnten.

Die obige Analyse zeigt auch, dass extremistische Gruppen zunehmend mit Instant-Messaging-Plattformen experimentieren, die dezentrale Server und Datenspeicherung anbieten. Bislang scheinen die meisten Gruppen die Möglichkeit der dezentralen

116 Shapiro, Jacob N. 2015. The Terrorists Dilemma: Managing Violent Covert Organizations. Reprint edition. Princeton University Press; Kenney, Michael. 2010. „Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists." Terrorism and Political Violence 22 (2): 177–97. https://doi.org/10.1080/09546550903554760; Gartenstein-Ross et al., „Virtual Plotters. Drones. Weaponized AI?"; Alexander, „Digital Decay."

117 Amarasingam, „A View from the CT Foxhole"; Conway, Maura, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson und David Weir. 2019. „Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts." Studies in Conflict & Terrorism 42 (1–2): 141–60. https://doi.org/10.1080/1057610X.2018.1513984; Conway, Maura, Ryan Scrivens und Logan Macnair. 2019. „Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends." Den Haag, Niederlande: International Centre for Counter-Terrorism. https://icct.nl/wp-content/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf.

118 Amarasingam, „Telegram Deplatforming ISIS Has Given Them Something to Fight For".

119 King, „Islamic State Group's Experiments with the Decentralized Web"; Bodo, „Decentralized Terrorism".

Datenspeicherung bei Plattformen wie BCM, Riot.im oder Rocket.Chat noch nicht voll ausgeschöpft zu haben.[120] Die Verwaltung unabhängiger Server für diese Plattformen kann zeitaufwändig und ressourcenintensiv sein und – wie die Nashir News Agency bei ihrem Versuch, einen dezentralen Rocket.chat-Server für ihre Propagandakanäle einzurichten, feststellen musste – zusätzliche Ziele für staatliche Stellen, Konkurrenten und unabhängige Hacker schaffen.[121] In der Anfangsphase sind diese neuen Plattformen und rudimentären Ausnutzungsversuche durch Extremisten von Pannen, Denial of Service und andere technische Probleme gekennzeichnet. Neue Plattformen, wie ZeroNet, Matrix und andere, machen das dezentrale Server-Hosting für Verbraucher jedoch wesentlich einfacher, was diese Plattformen unweigerlich auch für extremistische Gruppen zugänglicher machen wird.[122]

So kann eine Instant-Messaging-Plattform, die auf dem dezentralen Web aufbaut, dennoch ein guter Ersatzkandidat für Telegram sein, insbesondere wenn sie für Extremisten leicht zugänglich und einfach zu bedienen ist. Lorand Bodo schreibt, dass „das dezentrale Web der nächste logische Schritt zu sein scheint, nicht nur für den IS, sondern auch für andere (gewaltbereite) Extremisten im Internet, die versuchen, den Behörden und der Löschung zu entgehen“.[123] Der Grund für die Bevorzugung dezentraler Web-Plattformen ist einfach: Extremisten im Internet sehen sich Bedrohungen sowohl durch staatliche Stellen ausgesetzt, die versuchen, potenzielle Terroristen zu überwachen, zu identifizieren und zu sperren, als auch durch die Technologieanbieter, die versuchen, extremistische Propaganda auf ihren Plattformen auszuschalten.[124] Durch Telegram und andere Dienste sind Extremisten nun in der Lage, Funktionen wie Ende-zu-Ende-Verschlüsselung zum maximalen Schutz ihrer Anonymität zu nutzen, mühen sich auf den Plattformen aber mit der Aufrechterhaltung der Netzwerkstabilität ab.[125] Wenn die Gruppen in der Lage wären, Daten auf ihren eigenen Servern abzulegen, würde dies in der Tat den Erfolg der Bemühungen seitens der Technologieunternehmen zur Beseitigung der Inhalte schmälern, weil so ein unabhängiges, dezentrales Speichernetzwerk außerhalb der Reichweite der Dienstanbieter entstünde.[126]

120 Ebd.
121 Ebd.
122 Ebd.
123 Bodo, „Decentralized Terrorism“.
124 Ebd.
125 Ebd.
126 Ebd.

5 Empfehlungen: Hinwendung zu einer merkmalzentrierten Strategie gegen Online-Extremismus

Die Dominanz Telegram ähnlicher Messenger und dezentraler Anwendungen unter den Chat-Apps, die von Extremisten im Zuge der konsequenteren Abwehr auf Telegram genutzt werden, zeigt, dass eine bestimmte Funktionalität maßgebliche Anziehungskraft auf extremistische Gruppen ausübt. Daraus folgt, dass sich die Extremismusbekämpfung nicht mehr länger nur auf bestimmte Plattformen oder Anwendungen konzentrieren darf. Vielmehr gilt es, plattformübergreifend bestimmte funktionale Merkmale unter die Lupe zu nehmen, wenn man die Ausnutzung digitaler Kommunikationstechnologien durch Extremisten verhindern will. Forschung und Politik richten ihr Augenmerk verstärkt auf eine Reihe bestimmter „Problem"-Plattformen – in den vergangenen Jahren Twitter und Telegram – während sie ein wesentlich breiteres Ökosystem der extremistischen Kommunikation im Internet übersehen.[127] Diese Dynamik manifestiert sich in gezielten Online-Razzien wie den Referral Action Days von Europol, die einige Politiker sogar dazu veranlasst haben, die Entfernung von Content auf bestimmten Plattformen als Gesamtsieg gegen den Online-Extremismus darzustellen. Wie dieser Beitrag zeigt, kann die daraus resultierende dezentrale Plattformnutzung die positiven Auswirkungen dieser Operationen aber wieder zunichtemachen.[128]

Generell würde die Extremismusbekämpfung im Internet von einem merkmalorientierten Ansatz profitieren, weil dann die Reaktionsstrategie der Art und Weise entspräche, wie Extremisten ihrerseits Nutzung des Internets konzeptionieren. Wenn die Abwehr des extremistischen Missbrauchs sich an Merkmalen statt an einzelnen Plattformen orientiert, können die Anbieter zudem leichter gleichgesinnte Unternehmen finden, um sich über Maßnahmen und neue Möglichkeiten auszutauschen. Die Daten mehrerer Studien zu bestimmten Plattformen legen die Vermutung nahe, dass Extremisten nicht aufgrund des Markennamens oder der Legitimation von diesen Anwendungen angezogen wurden, sondern wegen der angebotenen Eigenschaften und Funktionen.[129]

Bei der Bekämpfung des extremistischen Missbrauchs des Internets neigen die europäischen und amerikanischen Verfolgungsbehörden

127 Alexander, Audrey und Bill Braniff. 2018. „Marginalizing Violent Extremism Online." Lawfare. 21. Januar 2018. https://www.lawfareblog.com/marginalizing-violent-extremism-online.; Fisher, Ali, Prucha, Nico und Emily Winterbotham. 2019. „Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability." Global Research Network on Terrorism and Technology: Paper Nr. 6, Juli 2020. https://rusi.org/sites/default/files/20190716_grntt_paper_06.pdf.
128 Alexander und Braniff, „Marginalizing Violent Extremism Online".
129 Ebd.

dazu, bestimmte Plattformen zu selektieren und sie mit Regulierungsdruck, gezielten Abschreckungsmaßnahmen und Fristsetzungen ins Visier zu nehmen. In manchen Fällen sind diese Maßnahmen sicher notwendig. Es gibt leider Plattformen mit einer überaus schlechten Erfolgsbilanz in Bezug auf Online-Extremismus, die auf unzureichende Durchsetzung von Nutzungsbedingungen, gravierende Kapazitätslücken, ein schlechtes regulatorisches Umfeld oder sogar Sympathien für bestimmte extremistische Gruppen zurückzuführen sein kann, die einem Eingreifen entgegensteht. Dass diese Plattformen gezielt angegangen werden, ist erforderlich für die Rechtsdurchsetzung. Weit verbreitet ist extremistischer Missbrauch jedoch auch auf Plattformen, die trotz redlicher Bemühungen, Inhalte zu moderieren bzw. zu entfernen, aufgrund ihrer Merkmale oder ihrer Erreichbarkeit für ein Massenpublikum für Extremisten attraktiv sind. Ein merkmalorientierter Ansatz, der plattformübergreifend die Ausnutzung bestimmter Möglichkeiten durch Extremisten bewertet, würde den Entscheidungsträgern helfen, zwischen Plattformen mit Governance- bzw. Moderationsproblemen und solchen zu unterscheiden, die einfach aufgrund ihrer Merkmale Extremisten anziehen. Bei der ersten Gruppe ist die Ausübung von Druck aussichtsreich, bei der zweiten eher nicht.

Einrichtungen zur Bekämpfung von Extremismus im Internet wie dem Global Internet Forum to Counter Terrorism (GIFCT) könnte die Gruppierung gleichartiger Plattformen helfen, plattformübergreifende, ganzheitliche Ziele der Extremismusbekämpfung auf bestimmte Merkmale abzustimmen, die diesen Plattformen gemeinsam sind. Ali Fisher, Nico Prucha und Emily Winterbotham schreiben, dass „die Konzentration auf das Multiplattform-Kommunikationsparadigma statt auf einzelne Plattformen entscheidend für die Entwicklung eines neuen Online-Abwehrkonzepts für die Zukunft“ sei.[130] Der Austausch von Best Practices, Reaktionsmöglichkeiten und Ideen zwischen Plattformen, die ähnliche Funktionen anbieten, wie z. B. File-Sharing-Plattformen, Instant Messenger oder Social-Media-Sites, ermöglicht eine wirksamere Zusammenarbeit und Innovation. Dies kann den bereits bestehenden Informationsaustausch, wie z. B. URL-Hash-Sharing-Datenbanken, dadurch aufwerten, dass verschiedene Plattformen die Verbreitung extremistischer Inhalte von einer Plattform zur anderen verfolgen können.[131]

Schließlich kann eine stärkere Zusammenarbeit zwischen Plattformen mit ähnlichen Merkmalen vor allem als Frühwarnsystem vor Extremisten dienen, die auf eine andere Plattform umziehen wollen. So hätte beispielsweise eine Instant-Messaging-Plattform, die einem Konsortium zum Informationsaustausch mit anderen Plattformen angehört, einen direkten Kanal zur Benachrichtigung der anderen, wenn sie durchgreifende Maßnahmen zur Ausschaltung extremistischer Inhalte und Netzwerke auf ihrer Plattform plant. Die vorab informierten Instant-Messaging-Plattformen können dann Abwehrmaßnahmen für den Fall vorbereiten, dass extremistische Gruppen versuchen, zu einem anderen Anbieter „umzuziehen“. Dienstanbieter, die in der Lage sind, extremistischen Missbrauch ihres Angebots bereits in der frühen Iterationsphase empfindlich zu stören, können wirkungsvoll dafür sorgen, dass es Extremisten nicht so schnell und einfach gelingt, sich auf neuen Plattformen in Stellung zu bringen.

130 Fisher et al. „Mapping the Jihadist Information Ecosystem“.
131 Ebd.

Wenn das GIFCT in den kommenden Jahren seine Mitgliedschaft auf neue Unternehmen ausweitet, sollte es erwägen, seine derzeitigen breit angelegten Möglichkeiten der Zusammenarbeit mit kleineren Arbeitsgruppen zu kombinieren, die sich bestimmten Kategorien von Dienstanbietern widmen. Nachdem der vorliegende Beitrag zeigt, dass dieses Modell der Zusammenarbeit für Instant-Messaging-Plattformen nützlich sein könnte, wäre durch weitere Forschung und Experimente zu ermitteln, ob andere Arten von Dienstangeboten, wie Social Media, File-Sharing oder E-Commerce, ebenfalls von einer merkmalbasierten Gruppierung innerhalb des GIFCT profitieren könnten. Ein Vorstoß mit diesem Ansatz seitens des GIFCT könnte außerdem politische Entscheidungsträger und die Forschung dazu bewegen, die Bedeutung bestimmter Merkmalkombinationen für die Anpassungsbemühungen von Extremisten sorgfältig zu evaluieren und ihre politischen Reaktionen sowie die Forschungsarbeit so aufzustellen, dass breitere Bereiche des extremistischen Ökosystems im Internet erfasst werden. Generell könnte das merkmalorientierte Paradigma Technologieunternehmen, politischen Entscheidungsträgern, Theoretikern und Praktikern helfen, die Kurve der Aneignung digitaler Kommunikationstechnologien durch Extremisten flacher zu halten.

Die politische Landschaft

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

Einleitung

Die Nutzung und der Missbrauch des Internets durch Terroristen stellt seit langem politische Entscheidungsträger, Strafverfolgungsbehörden und Technologieunternehmen gleichermaßen vor Herausforderungen. Auf der einen Seite gibt es die sehr öffentlichen Fälle von Technologiemissbrauch: das Livestreaming eines Terroranschlags in Neuseeland ist ein Extrembeispiel. Aber ein weiteres potenzielles Problem sind Terroristen oder terroristische Organisationen, die Private-Messaging-Anwendungen zur Planung und Rekrutierung für ihre Aktivitäten nutzen. Dabei verwenden terroristische Organisationen immer häufiger Messaging-Apps mit Ende-zu-Ende-Verschlüsselung, gerade weil sie ein sehr gut geheim zu haltendes Kommunikationsmittel darstellen, an das die Strafverfolgungsbehörden nicht so leicht herankommen. Dieses Problem hat in den vergangenen Jahren bei der Messaging-App Telegram zugenommen, aber auch bei neueren Telegram-Alternativen, die Terroristen ausprobieren, um sich den Strafverfolgungsbehörden zu entziehen.

In diesem Bericht werden einige der zentralen Herausforderungen dargelegt, mit denen sich die nationalen Regierungen im Umgang mit durchgehend verschlüsselten Messaging-Apps auseinandersetzen müssen. Für neun Länder werden die wichtigsten Gesetze und Prozessbeteiligten sowie die Herausforderungen für die politischen Entscheidungsträger bei der Verhinderung des Missbrauchs von Messaging-Apps dargestellt, ebenso wie die verschlüsselungsbedingten Schwierigkeiten der Strafverfolgungsbehörden bei Nachforschungen. Er wird auch einige der Herausforderungen anreißen, die sich aus der Hinwendung zu dezentralen Messaging-Plattformen ergeben, sowie mögliche Ansätze zu deren Überwindung.

Instant-Messaging-Apps und Terrorabwehr: Umgang mit den Herausforderungen und Beurteilung neuer Entwicklungen

Kanada

Die kanadische Regierung verfolgt eine umfassende Strategie zur Bekämpfung von Terrorismus und Radikalismus; diese umfasst die traditionellen Tätigkeiten der Nachrichten- und Sicherheitsbehörden, Beteiligung der Zivilgesellschaft, gemeinsame Initiativen mit der Technologiebranche sowie gemeinschaftsorientierte Polizeiarbeit. Ihre Strategie zur Bekämpfung von Radikalisierung und Gewaltbereitschaft (National Strategy on Countering Radicalisation to Violence) verfolgt

drei Richtungen: die Entwicklung von Gegennarrativen in der Zivilgesellschaft (Counter-Messaging), die Unterstützung der Forschung zur Terrorabwehr und die Partnerschaft mit internationalen Initiativen und Technologieunternehmen.[132]

Kanada hat von allen hier untersuchten Ländern die vielleicht am weitesten entwickelte Strategie des Counter-Messaging und der zivilgesellschaftlichen Beteiligung. Extreme Dialogue ist eine Counter-Messaging-Initiative der kanadischen Regierung und des Institute of Strategic Dialogue. Das Projekt gibt Praktikern und jungen Menschen pädagogische Ressourcen in Form von Filmmaterial an die Hand, das die negativen Auswirkungen von Extremismus veranschaulicht.[133] Das Canada Centre for Community Engagement and Prevention of Violence ist Träger diverser gemeinschaftsbasierter Interventionsprojekte zur Abwehr von Radikalisierung zur Gewaltbereitschaft. In Calgary arbeitet beispielsweise das ReDirect-Programm mit dem Calgary Police Service und den City of Calgary Community & Neighborhood Services sowie den Gesundheits- und Sozialdiensten zusammen, um frühzeitig in Radikalisierungsprozesse einzugreifen. ReDirect arbeitet mit unterschiedlichen Strategien wie Meldung, Aufklärung und Beratung von Personen, die nach einer Möglichkeit suchen, aus einer gewaltbereiten extremistischen Gruppe auszusteigen.[134]

Was die Forschung zur Terrorabwehr angeht, so hat Kanada 2019 Tech Against Terrorism, eine internationale, von der UNO geförderte Initiative, die mit der globalen Technologiebranche zusammenarbeitet, mit der Entwicklung einer Terrorist Content Analytics Platform (TCAP) beauftragt, einer Datenbank, die verifiziertes terroristisches Material und Inhalte aus bestehenden Datenbeständen und offenen Quellen enthält.[135] Die Plattform kann als Echtzeitwarnsystem für kleinere Internetplattformen fungieren, die unter Umständen nicht über die Kapazitäten oder Ressourcen verfügen, um den behördlichen Vorgaben zur Entfernung bösartiger und extremistischer Inhalte nachzukommen.

Schließlich ist Kanada auch noch an einer Reihe von internationalen und sektorübergreifenden Initiativen beteiligt. Nach dem Terroranschlag auf zwei Moscheen in Christchurch im März 2019 schloss sich Premierminister Justin Trudeau dem Christchurch-Appell (Christchurch Call to Action) an, einer gemeinsamen Initiative der Staaten und Technologiebranche zur „Tilgung von terroristischen und gewalttätigen extremistischen Inhalten im Netz“.[136] Neben der finanziellen Unterstützung technischer Entwicklungen zur Auffindung und Löschung extremistischer Inhalte – wie der GIFCT-Hash-Datenbank[137] – verpflichtet der Appell die Regierungen zur Unterstützung des Aufbaus von Strukturen und Kapazitäten sowie Aufklärungskampagnen, um der Nutzung von Online-Diensten zur Verbreitung terroristischer und gewalttätiger extremistischer Inhalte entgegenzuwirken.

132 „National Strategy on Countering Radicalization to Violence“, Public Safety Canada. Abgerufen: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-en.aspx#s7
133 Siehe: https://extremedialogue.org/
134 Siehe: http://redirect.cpsevents.ca/
135 Die Terrorist Content Analytics Platform (TCAP) wurde auch im Abschnitt „Die politische Landschaft“ des GNET-Berichts „Hass decodieren: Klassifizierung terroristischer Inhalte mittels experimenteller Textanalyse“ beschrieben. Abgerufen: https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Decoding-Hate-Using-Experimental-Text-Analysis-to-Classify-Terrorist-Content_GERMAN.pdf
136 Siehe: https://www.christchurchcall.com/
137 Siehe: https://www.gifct.org/joint-tech-innovation/

Europäische Kommission

Bei Europol angesiedelt ist das European Counter Terrorism Centre (ECTC), das nach dem Pariser Anschlag auf Mitarbeitende der Satirischezeitschrift *Charlie Hebdo* im Jahr 2015 eingerichtet wurde, wie in der Europäischen Sicherheitsagenda der Europäischen Kommission empfohlen. Das ECTC hat die Aufgabe, „den Informationsaustausch und die operative Unterstützung der Ermittler der Mitgliedstaaten zu verbessern".[138] Die Kommission hat 2015 außerdem das EU-Internetforum ins Leben gerufen, das Regierungen, Europol sowie Technologie- und Social-Media-Unternehmen zusammenführt, damit illegale Inhalte so schnell wie möglich beseitigt werden können.[139]

Die Europäische Kommission hat erkannt, dass nicht nur die großen Technologiefirmen von terroristischen Organisationen genutzt und missbraucht werden, sondern auch kleinere Anbieter, die „verschiedene Arten von Hosting-Diensten" anbieten.[140] Datenverschlüsselung und der Zugriff auf persönliche bzw. personenbezogene Daten hat sich bei Ermittlungen als eine Herausforderung für die Strafverfolgung erwiesen.

Europol hat mehrere große Kampagnen gestartet, um IS-Nutzer und Nutzer aus dem IS-Umfeld von Telegram zu entfernen. Im Laufe mehrerer Tage im November 2019 nahm Europol insgesamt 5.055 Accounts und Bots aus dem Netz, gegenüber einem Tagesdurchschnitt von 200 bis 300 Accountlöschungen zu anderen Zeiten.[141] Im Dezember 2018 wurden laut Telegram 3.276 Accounts an einem einzigen Tag entfernt, und bereits im April des Jahres hatte Europol einen Tag mit ähnlicher Bilanz.[142] Obwohl diese Einzelereignisse die Aktivitäten des IS empfindlich stören, ist ohne kontinuierliches Vorgehen ein dauerhafter Erfolg unwahrscheinlich.

Im Nebeneffekt zu diesen Tagen des harten Durchgreifens hat eine Zusammenarbeit zwischen Telegram und Europol bessere Instrumente für die Meldung von Inhalten hervorgebracht, d. h. über eine Meldefunktion in Gruppen und Kanälen kann jeder Nutzer Inhalte melden, die er für unangebracht hält.[143]

Frankreich

Gemeinsam mit Deutschland hat Frankreich die Europäische Kommission aufgefordert, als Mittel zur Terrorismusbekämpfung, verschlüsselte Messaging-Anwendungen zu regulieren.[144] Konkret forderte Matthias Fekl als französischer Innenminister,

138 European Commission, Migration and Home Affairs, *Counter-terrorism and radicalisation.* https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism_en

139 European Commission, Press Office, *EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online.* 3. Dezember 2015. https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243

140 Europäische Kommission, „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Verbreitung terroristischer Online-Inhalte", COM(2018) 640. 2018/0331. 12. September 2018. S. 1 https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-640-F1-DE-MAIN-PART-1.PDF

141 BBC Monitoring, „Europol disrupts Islamic State propaganda machine", *BBC News*. 25. November 2019. https://www.bbc.com/news/world-middle-east-50545816

142 Ebd.

143 Europol, *Europol and Telegram take on terrorist propaganda online.* Pressemitteilung. 25. November 2019. https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online

144 Französische Regierung, Innenministerium, „Initiative franco allemande sur la securite interieure en Europe". 23. August 2016. https://www.interieur.gouv.fr/Archives/Archives-des-actualites/2016-Actualites/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe

dass die Polizei bei Online- und Technologieanbietern dieselben Zugriffsrechte haben sollte wie bei Telekommunikationsanbietern.[145]

Infolge des Drucks von Frankreich und Deutschland schlägt die Europäische Kommission vor, die EG-Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie) dahingehend zu ändern, dass die nationalen Regierung bestimmte Datenschutzvorkehrungen umgehen dürfen, wenn die nationale Sicherheit bedroht ist – hiermit ist allerdings nicht die Verschlüsselung reguliert.[146] Das Problem für die nationalen Strafverfolgungsbehörden ist das Fehlen rechtlicher Instrumente, um Technologieunternehmen zur Herausgabe verschlüsselter Daten zu zwingen.[147] Seit der Veröffentlichung der Vorschläge der Europäischen Kommission im Januar 2017 sind die Verhandlungen auf Ratsebene jedoch ins Stocken geraten, woran sich auch unter der deutschen EU-Ratspräsidentschaft bislang nichts geändert hat.[148]

In Frankreich sind Verschlüsselungsanbieter derzeit verpflichtet, „Vereinbarungen mit der Regierung zu treffen, um den Zugang zu den von ihnen verschlüsselten Daten zu ermöglichen; anderenfalls drohen Bußgelder".[149] Darüber hinaus hat der Premierminister die Befugnis, „Verschlüsselungsdienste zu verbieten, die ihren gesetzlichen Verpflichtungen nicht nachkommen".[150]

Ghana

Da Ghana sehr wenig Erfahrung mit Terroranschlägen hat – seit 1970 gab es lediglich 21 Vorfälle mit 23 Todesopfern[151] – hat die ghanaische Regierung kein robustes Regelwerk für gewalttätigen Extremismus im Internet entwickelt.[152]

Anders als Ghana hat das nahegelegene westafrikanische Nigeria seit Jahren mit schweren Terroranschlägen zu kämpfen. Gruppen wie Boko Haram und „Islamischer Staat Provinz Westafrika" (ISWAP) haben berüchtigte Anschläge verübt, wie die Verschleppung von Schülerinnen im April 2014[153] und die Massaker vom Januar 2015, beide im Bundesstaat Borno.[154] Boko Haram hat begonnen, Social-Media-Plattformen zu nutzen, um Propaganda zu verbreiten und neue Mitglieder für seine Zwecke anzuwerben. Die Gruppe nutzt vor allem traditionelle Social-Media-Plattformen wie Twitter, Facebook und YouTube, um zu Zwecken der Rekrutierung Fotos von Soldaten zu veröffentlichen, Enthauptungen und Entführungen bekannt

145 Stupp, C. „EU to propose new rules targeting encrypted apps in June", *Euractiv.* 29. März 2017. https://www.euractiv.com/section/data-protection/news/eu-to-propose-new-rules-on-police-access-to-encrypted-data-in-june/
146 Ebd.
147 Ebd.
148 Europäisches Parliament, *Legislative Train Schedule: Proposal for a regulation on privacy and electronic communications.* https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform
149 Lewis, J. A., Zheng, D. E., Carter, W. A. „The effect of encryption on lawful access to communications and data", *CSIS Technology Policy Program.* Februar 2017. S. 20 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf
150 Ebd.
151 Global Terrorism Database, START. Abgerufen: https://www.start.umd.edu/gtd/
152 Siehe auch: Abschnitt „Die politische Landschaft" des vorherigen GNET-Berichts, „Künstliche Intelligenz und Terrorabwehr: Eine Einführung". Abgerufen: https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Artificial-Intelligence-and-Countering-Violent-Extremism-A-Primer_GERMAN.pdf
153 Mbah, F. (2019), „Nigeria's Chibok schoolgirls: Five years on, 112 still missing", Al Jazeera. Abgerufen: https://www.aljazeera.com/news/2019/4/14/nigerias-chibok-schoolgirls-five-years-on-112-still-missing
154 Amnesty International (2018), „Boko Haram Baga attacks: satellite images reveal destruction." Abgerufen: https://www.amnesty.org.uk/nigeria-boko-haram-doron-baga-attacks-satellite-images-massacre

zu machen und regierungsfeindliche Nachrichten zu verbreiten.[155] In den vergangenen Jahren hat Boko Haram jedoch begonnen, verschlüsselte Instant-Messaging-Apps wie Telegram zu verwenden, um Propagandamaterial zu veröffentlichen und andere Gruppen zu denunzieren.[156] Aufgrund der Zunahme des Terrorismus im Land verschärfte die nigerianische Regierung 2013 ihre Anti-Terror-Gesetze und -Politik. Über die Stärkung der staatlichen Institutionen zur Terrorismusbekämpfung hinaus kann die Regierung nun auch Terrorverdächtige festnehmen und strafrechtlich verfolgen sowie gegen Personen, die einen terroristischen Akt begangen oder geplant haben, die Todesstrafe verhängen.[157]

Im Hinblick auf die Regulierung von Telegram und seiner Alternativen hat sich Ghanas großer Nachbar in der Region für eine traditionelle, vom Staat ausgehende und nach unten gerichtete Politik entschieden. Diese Lenkungsform stützt sich stärker auf gesetzgeberische Maßnahmen als auf sektorübergreifende Initiativen oder Einbeziehung der Zivilgesellschaft. Zudem hat die vom Staat ausgehende Strategie schon zu nicht intendierten, gefährlichen Resultaten geführt, z. B. zur Abschaltung des Internets durch die Regierung oder zur Ausnutzung sozialer Medien zur Unterdrückung politisch Andersdenkender.[158] Regierungen in Afrika haben brutale, aus der Kolonialzeit stammende Gesetze, die historisch zur Beschneidung von Bürgerrechten verwendet wurden, schon dazu ausgenutzt, um „viele ... Versuche zu legitimieren, außergesetzliche Forderungen an den privaten Sektor zu stellen".[159] Social-Media-Plattformen und Internetdienstanbieter mussten bereits regierungsseitigen, außergesetzlichen Abschaltforderungen nachkommen, was den Verdacht auf Zensur und Verletzung des Rechts auf freie Meinungsäußerung aufkommen lässt.[160]

Zivilgesellschaftliche Gruppen und Journalisten haben ihre Besorgnis über die Zukunft Ghanas im Hinblick auf die Regulierung des Internets und der Social-Media-Plattformen zum Ausdruck gebracht.[161] Im Vorfeld der Präsidentschafts- und Parlamentswahlen 2016 hatte der ghanaische Polizeichef beispielsweise eine mögliche Abschaltung der sozialen Medien angekündigt (zum Glück erfolglos).[162] Außerdem lassen großzügig ausgelegte Gesetze zur Meinungsfreiheit in Ghana digitale Räume offen für Missbrauch wie Hassreden und Cyberbullying (insbesondere gegen Frauen gerichtet).[163] Die Forderungen nach einer strengeren Regulierung von Social-Media-Plattformen nehmen daher zu.

155 UN Development Programme and RAND (2018), „Social Media in Africa." Abgerufen: https://www.africa.undp.org/content/rba/en/home/library/reports/social-media-in-africa-.html

156 Zenn, J. (2017), „Electronic Jihad in Nigeria: How Boko Haram is Using Social Media", *Terrorism Monitor*, Bd. 15, Nr. 23. Abgerufen: https://www.refworld.org/docid/5b728ca2a.html

157 „Nigeria: Extremism & Counter Extremism", Counter-Extremism Project. Abgerufen: https://www.counterextremism.com/countries/nigeria

158 Ilori, T. (2020), „Content Moderation Is Particularly Hard in African Countries", Information Society Project at Yale Law School. Abgerufen: https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/moderate-globally-impact-locally-content-moderation-particularly-hard-african-countries

159 Ilori, T. (2020), „Stemming digital colonialism through reform of cybercrime laws in Africa", Information Society Project at Yale Law School. Abgerufen:https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/stemming-digital-colonialism-through-reform-cybercrime-laws-africa

160 Ranking Digital Rights, „2019 RDR Corporate Accountability Index." Abgerufen: https://rankingdigitalrights.org/index2019/assets/static/download/RDRindex2019report.pdf

161 Majama, K. (2019) „Africa in urgent need of a homegrown online rights strategy", Association for Progressive Communications. Abgerufen: https://www.apc.org/en/news/africa-urgent-need-homegrown-online-rights-strategy

162 Olukotun, D. „President of Ghana says no to internet shutdowns during coming elections", *AccessNow*, 16. August 2019. Abgerufen: https://www.accessnow.org/president-ghana-says-no-internet-shutdown-elections-social-media/

163 Endert, J. (2018) „Digital backlash threatens media freedom in Ghana", DW Akademie. Abgerufen: https://www.dw.com/en/digital-backlash-threatens-media-freedom-in-ghana/a-46602904

Ghana hat daraufhin 2019 ein Gesetz über das Recht auf Information verabschiedet, das den Zugang zu Informationen im Besitz öffentlicher Institutionen garantiert.[164] Der Gesetzentwurf signalisiert, dass die ghanaische Regierung mit digitalen Rechten transparent und verantwortungsbewusst umgehen und ein Gleichgewicht zwischen dem Schutz der Nutzer vor Schaden und dem Recht der Nutzer auf freie Meinungsäußerung finden will. Nichtsdestotrotz könnte die ghanaische Regierung ihre Strategie zur Terrorabwehr breiter aufstellen, um sich gemeinsam mit der Zivilgesellschaft und Community-Guppen besser zu wappnen.

Japan

Bei den Anstrengungen der japanischen Regierung zur Terrorismusbekämpfung besteht eine strikte Trennung zwischen dem, was sie als ausländische und was als inländische terroristische Aktivitäten wahrnimmt. Mit der entsprechend aufgeteilten institutionellen Zuständigkeit gehen zwei unterschiedliche Ansätze zur Bekämpfung des gewalttätigen Extremismus im Internet einher.

Was innerstaatliche Bedrohungen angeht, wie im Zusammenhang mit den Olympischen Spielen 2021 in Tokio oder durch die japanische extreme Rechte, wird die staatliche Abwehr weitgehend durch die Strafverfolgungsbehörden koordiniert. Die kommunistischen Subversionsaktivitäten aus der Zeit des Kalten Krieges haben die Art und Weise beeinflusst, wie Japan mit innerstaatlichen Bedrohungen umgeht: Die Polizeibehörden der Präfekturen (unter Aufsicht des Nationalen Polizeibehörde) und der „Nachrichtendienst für öffentliche Sicherheit“ (Japans nationaler Nachrichtendienst) stehen an der Spitze der nachrichtendienstlichen Erkennung und der Terrorismusabwehr auf japanischem Boden.[165]

Die inländischen Maßnahmen zur Terrorismusbekämpfung konzentrieren sich daher auf Polizeiarbeit und traditionelle Sicherheitsarchitekturen. Aufgrund seiner Affinität zur technischen Innovation ist Japan mit Lösungen auf der Basis künstlicher Intelligenz (KI) vorgeprescht, darunter groß angelegte Systeme zur Gesichtserkennung, biometrischen Authentifizierung und automatischen Verhaltenserkennung.[166] Diese Lösungen lassen eine Lenkungsform erkennen, bei der Früherkennung und Prävention im Mittelpunkt stehen, die durch traditionelle Polizei- und Sicherheitstaktiken realisiert werden.

164 Yahya Jafru, M. „Right to information – RTI bill passed into law“, *Graphic Online*, 26. März 2019. Abgerufen: https://www.graphic.com.gh/news/politics/ghana-news-rti-bill-passed.html

165 Kotani, K., „A Reconstruction of Japanese Intelligence: Issues and Prospects“, in Philip H. J. Davies & Kristian C. Gustafson (eds.), *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere* (Washington D.C.: Georgetown University Press, 2013), S. 181–99.

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

Um diese Bemühungen weiter zu unterstützen, setzte der japanische Premierminister Shinzō Abe Mitte 2017[167] ein Anti-Terror-Gesetz durch, das von Japans Oppositionsführer als „brutal" bezeichnet wurde.[168] Die Gesetzgebung kriminalisiert bereits die Intention, eines von über 270 „schweren Delikten" zu begehen, unter anderem auch Sit-in-Proteste und Urheberrechtsverletzungen bei Musik, und ihre Durchsetzbarkeit erstreckt sich auch auf die sozialen Medien.[169] Bürgerrechtsaktivisten und zivilgesellschaftliche Gruppen sind angesichts des weit gefassten Geltungsbereichs und der Befugnis, Online-Aktivitäten zu überwachen und zu sanktionieren, zutiefst besorgt über das Gesetz.[170]

Was die internationalen Bemühungen Japans zur Terrorismusabwehr anbelangt, so besteht hier eine Diskrepanz zur innenpolitischen Fokussierung auf Kriminalisierung. Japans Anstrengungen zur Terrorismusabwehr außerhalb des eigenen Landes sind durch Zusammenarbeit in der Region, den Aufbau von Kapazitäten und Kooperation gekennzeichnet. Konkret sind viele der Terrorabwehrbemühungen des Landes Bestandteil der Association of Southeast Asian Nations (ASEAN),[171] die von den Mitgliedern eine Reihe von Absichtserklärungen verlangt, die der „Verhütung, Unterbindung und Bekämpfung des internationalen Terrorismus durch Informationsaustausch, gemeinsame Nutzung nachrichtendienstlicher Erkenntnisse und Aufbau von Kapazitäten" verlangt und damit ein Vorbild für die Zusammenarbeit in einer Region bei der Bekämpfung von gewaltbereitem Extremismus und Terrorismus geschaffen hat.[172]

Japan war zweimal Gastgeber des jährlich stattfindenden ASEAN-Japan Counter Terrorism Dialogue und führte bilaterale Gespräche mit einer Reihe von globalen Akteuren.[173] Ende 2019 führten Japan und das Vereinigte Königreich Gespräche über „die gegenwärtige Lage des internationalen Terrorismus, innerstaatliche Maßnahmen zur Terrorismusabwehr und auch über die gegenwärtige Zusammenarbeit beim Aufbau von Kapazitäten zur Terrorismusbekämpfung, insbesondere in Dritt- (sic) Ländern [„third *(sp.)* countries]".[174]

Die Bekämpfung der Nutzung von Telegram und seiner Alternativen durch Extremisten in Japan wird wahrscheinlich diesem kombinierten Ansatz folgen: eine nach außen gerichtete Strategie der Zusammenarbeit in der Region und der Agendasetzung, begleitet von einer Durchführung im eigenen Land mittels herkömmlicher Sicherheits-, Polizei- und Überwachungsaktivitäten.

---

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

168 Allen-Ebrahimian, B., „Japan Just Passed a ‚Brutal', ‚Defective' Anti-Terror Law", *Foreign Affairs*, 16. Juni 2017. Abgerufen: https://foreignpolicy.com/2017/06/16/japan-just-passed-a-brutal-defective-anti-terror-law/

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

170 Japan Federation of Bar Associations, „Statement on the Enactment of the Bill to Revise the Act on Punishment of Organized Crimes and Control of Crime Proceeds, including the Criminalization of Conspiracy", 15. Juni 2017. Abgerufen: https://www.nichibenren.or.jp/en/document/statements/170615.html

171 „Japan: Extremism & Counter Extremism", Counter-Extremism Project. Abgerufen: https://www.counterextremism.com/countries/japan

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

173 „Japan: Extremism & Counter Extremism", Counter-Extremism Project. Abgerufen: https://www.counterextremism.com/countries/japan

174 Japanisches Außenministerium, „The 4th Japan-the UK Counter-Terrorism Dialogue", 4. Dezember 2019. Abgerufen: https://www.mofa.go.jp/fp/is_sc/page1e_000297.html

Neuseeland

Neuseelands im Februar 2020 veröffentlichter Gesamtstrategieplan zur Terrorismusbekämpfung macht deutlich, dass die Lenkung der Bekämpfung von gewalttätigem Extremismus im Internet die Koordination zahlreicher Stellen und Gremien erfordert.[175] Dazu gehören, ähnlich wie in Kanada (siehe oben), das Cabinet External Relations and Security Committee, die Polizei, Nachrichtendienste und Stellen für Sicherheitskommunikation sowie die Behörden für auswärtige Angelegenheiten, Handel, Verteidigung, Verkehr, Innovation und Entwicklung.

Neuseeland hat internationale Aufmerksamkeit für seine Führungsrolle bei länder- und sektorübergreifenden Initiativen erlangt. Insbesondere nach dem Attentat in den Moscheen in Christchurch im März 2019 brachten die Regierungen Neuseelands und Frankreichs unter dem Christchurch Call to Eliminate Terrorist and Violence Extremist Content Online („Christchurch-Appell") eine Koalition von Staatsoberhäuptern mit Social-Media- und Technologieunternehmen zusammen.[176] Die Unterzeichner des Appells verpflichten sich zur Durchsetzung von Gesetzen, die die Verbreitung terroristischer und gewalttätiger extremistischer Inhalte im Internet verbieten, aber zugleich dem Recht auf freie Meinungsäußerung und Schutz der Privatsphäre Rechnung tragen. Die Länder arbeiten auch daran, Rahmenbedingungen, Kapazitätsaufbau und Sensibilisierungsmaßnahmen zu unterstützen, um der Nutzung von Online-Diensten zur Verbreitung terroristischer und gewalttätiger extremistischer Inhalte entgegenzuwirken.

Der Christchurch-Appell verpflichtet auch Unternehmen wie Amazon, Facebook, Google, Twitter und YouTube zu mehr Rechenschaftspflicht und Transparenz in der Branche. Die Unternehmen müssen ihre Community-Standards und Nutzungsbedingungen durchsetzen, indem sie Maßnahmen zur Content-Moderation und Entfernung von Inhalten Priorität einräumen und Inhalte in Echtzeit zur Überprüfung und Bewertung identifizieren. Gemeinsam entwickeln die Länder und Unternehmen mit der Zivilgesellschaft Maßnahmen, um von der Community ausgehende Aktivitäten zu fördern und so in die Prozesse der Online-Radikalisierung einzugreifen.

Der Appell fungierte auch als Vehikel für die Modernisierung des GIFCT, dessen Aufgabenbereich erweitert wurde und nun auch eine Reihe von Präventions-, Reaktions- und Bildungsaktivitäten zur Bekämpfung des gewalttätigen Extremismus im Internet umfasst.[177]

Die Bemühungen Neuseelands, eine Reihe sektorübergreifender globaler Initiativen mit zu unterstützen, zeigen eine eher horizontale Strategie zur Kontrolle der Nutzung technischer Plattformen durch Extremisten. Die Herangehensweise umfasst sowohl konventionelle Sicherheits- und nachrichtendienstliche Strukturen als auch Initiativen, die Praxis, Forschung, Politik und technische Führungskräfte zusammenbringen, um Reaktionen auf neue Bedrohungen durch gewaltbereiten Extremismus im Internet auszuarbeiten.

175 Neuseeländische Regierung, Officials' Committee for Domestic and External Security Coordination, Counter-Terrorism Coordination Committee, „Countering terrorism and violent extremism national strategy overview", Februar 2020. https://dpmc.govt.nz/sites/default/files/2020-02/2019-20 CT Strategy-all-final.pdf

176 Siehe: https://www.christchurchcall.com/

177 Global Internet Forum to Counter Terrorism, „Next Steps for GIFCT", 23. September 2019. Abgerufen: https://gifct.org/press/next-steps-gifct/

Vereinigtes Königreich

Die Strategie des Vereinigten Königreichs zur Bekämpfung der extremistischen Nutzung von Online-Plattformen folgt einer traditionellen Lenkungsform, die sich auf staatliche Institutionen konzentriert. Die zentrale Institution, die für die Gesetzgebung zur Terrorismusbekämpfung zuständig ist, ist das Innenministerium (Home Office), das sich auch mit dem Government Communications Headquarters, dem Nachrichten- und Sicherheitsdienst des Landes, abstimmt. Darüber hinaus hat das Home Office Kooperationsgremien mit anderen Regierungsinstitutionen (vor allem mit dem Department for Digital, Culture, Media, and Sport) und dem Parlament geschaffen, wie beispielsweise das UK Council for Internet Safety, das National Counter Terrorism Security Office und die Commission on Countering Extremism.[178]

Ähnlich wie Japan (siehe oben) verfolgt auch Großbritannien bei der Bekämpfung von gewalttätigem Extremismus im Internet einen zweigleisigen Ansatz. Die eine Gruppe von Maßnahmen konzentriert sich auf die Regulierung von sozialen Medien und Technologieplattformen. Das im April 2019 veröffentlichte Online Harms White Paper der Regierung begründet ausführlich, warum eine stärkere nationale Regulierung der sozialen Medien notwendig sei.[179] Dieser neue Rechtsrahmen erlegt Social-Media- und Technologieunternehmen eine neue gesetzliche Sorgfaltspflicht gegenüber ihren Nutzern auf, die über die britische Medienaufsichtsbehörde (Office of Communications, Ofcom) durchsetzbar ist. Bei Nichteinhaltung des rechtlichen Rahmens und Verstößen gegen die gesetzliche Sorgfaltspflicht verhängt Ofcom finanzielle und technische Strafen über die Plattformen – Websites könnten auf ISP-Ebene gesperrt und mit Bußgeldern von bis zu 4 % ihres weltweiten Umsatzes belegt werden.[180] Zum Zeitpunkt dieser Niederschrift war die Online Harms Bill, die gesetzgeberische Umsetzung des White Paper bereits um mehrere Jahre verzögert.[181]

Die zweite Maßnahmengruppe im Vereinigten Königreich konzentriert sich auf die konventionellen Polizei-, Sicherheits- und Geheimdienstinstitutionen mit Beihilfe durch Antiterrorgesetze und eine starke öffentliche Unterstützung. Im Frühjahr 2020 brachte das Parlament einen neuen Gesetzesvorschlag zur Terrorismusbekämpfung ein, das auf Terrorverdächtige abzielt. Das neue Gesetz sieht vor, dass auch Verdächtige. „die nicht wegen eines Vergehens verurteilt wurden, unter Umständen mit umfassenderen und intensivierten Überwachungsmaßnahmen rechnen müssen".[182] Diese Überwachungsmaßnahmen wären nicht länger auf maximal zwei Jahre begrenzt. Darüber hinaus werden Maßnahmen zur Prävention und Untersuchung des Terrorismus (Terrorism Prevention and Investigation Measures, TIMs), einschließlich Zwangsumzug, elektronische Überwachung, Betretens- und Aufenthaltsverbote sowie Beschränkungen der Reise- und Versammlungsfreiheit, der

178 Gov.uk, UK Council for Internet Safety. Abgerufen: https://www.gov.uk/government/organisations/uk-council-for-internet-safety; Gov.uk, Commission for Countering Extremism. Abgerufen: https://www.gov.uk/government/organisations/commission-for-countering-extremism; Gov.uk, National Counter Terrorism Security Office. Abgerufen: https://www.gov.uk/government/organisations/national-counter-terrorism-security-office

179 Britische Regierung, „Online Harms White Paper", April 2019. Abgerufen: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

180 Crawford, A. „Online Harms bill: Warning over ‚unacceptable' delay", *BBC*, 29. Juni 2020. Abgerufen: https://www.bbc.co.uk/news/technology-53222665

181 Ebd.

182 „United Kingdom: Extremism & Counter Extremism", Counter-Extremism Project. Abgerufen: https://www.counterextremism.com/countries/unitedkingdom

Inanspruchnahme von Finanzdienstleistungen und der Nutzung von Kommunikationsmitteln, unter der vorgeschlagenen geringeren ausreichenden Beweislast nun leichter durchsetzbar sein.[183]

Diese strengeren Maßnahmen zur Terrorismusbekämpfung folgen auf die Anschläge in der Nähe der Fishmongers' Hall in der Londoner City im November 2019 und in der Streatham High Road im Februar 2020[184], nachdem die öffentliche Meinung eine strengere Gesetzgebung befürwortete.[185] Angesichts dieses permissiven Zeitgeistes können Strategien zur Bekämpfung des gewalttätigen Extremismus im Internet, und insbesondere die Nutzung von Anwendungen wie Telegram und seinen Alternativen, sich von ordnungspolitischen Maßnahmen stärker der strafrechtlichen Ahndung zuwenden. Der Gesetzentwurf sieht vor, dass die Beweislast, die die Unterwerfung eines Bürgers oder einer Bürgerin unter TPIMs-Maßnahmen ermöglicht, auf „begründeten Verdacht („reasonable grounds“) reduziert wird.[186] Unklar ist, ob die Nutzung von Apps wie Telegram und anderen dezentralen und verschlüsselten Instant-Messengern für den Zugriff auf oder die Verbreitung von extremistischen Inhalten als „begründeter Verdacht“ anzusehen ist.

Counter-Terrorism Committee Executive Directorate der Vereinten Nationen

Die Generalversammlung der Vereinten Nationen verabschiedete 2006 einstimmig die globale Strategie der Vereinten Nationen zur Terrorismusbekämpfung (United Nations Global Counter-Terrorism Strategy). Seitdem hat der Sicherheitsrat eine Reihe von Resolutionen zur Terrorabwehr verabschiedet, die die Mitgliedstaaten zur uneingeschränkten Zusammenarbeit im Kampf gegen den Terrorismus verpflichten. Die Resolutionen 1373 (2001) und 1566 (2004) „fordern von allen Mitgliedstaaten gesetzgeberische Maßnahmen zur Bekämpfung des Terrorismus, insbesondere auch durch verstärkte Zusammenarbeit mit anderen Regierungen“.[187] Die Resolution 1963 (2010) bestätigt die zunehmende Nutzung des Internets durch Terroristen für terroristische Zwecke.[188]

Der Kampf gegen die Nutzung dezentraler Plattformen durch terroristische Vereinigungen stellt die Strafverfolgungsbehörden vor besondere Herausforderungen. Über diese Plattformen können Nachrichten zwischen Sender und Empfänger ohne Vermittlung ausgetauscht werden, was die Verfolgung von (mutmaßlichen) Terroristen sehr schwierig macht.[189]

183 Grierson, J., „Unconvicted terrorism suspects face indefinite controls under UK bill“, *The Guardian*, 20. Mai 2020. Abgerufen: https://www.theguardian.com/politics/2020/may/20/unconvicted-terrorism-suspects-face-indefinite-controls-under-uk-bill

184 Department of Justice, „Press release: 14-year minimum jail terms for most dangerous terror offenders“, 20. Mai 2020. Abgerufen: https://www.gov.uk/government/news/14-year-minimum-jail-terms-for-most-dangerous-terror-offenders

185 In einem Bericht vom September 2017 über eine Meinungsumfrage zu extremistischen Inhalten im Internet sprachen sich fast drei Viertel der Befragten für eine neue Gesetzgebung aus, die den Besitz und Konsum von extremistischen Online-Inhalten unter Strafe stellt. Siehe: Frampton, M. (2017), „The New Netwar: Countering Extremism Online“, *Policy Exchange*. Abgerufen: https://policyexchange.org.uk/wp-content/uploads/2017/09/The-New-Netwar-1.pdf

186 Amnesty International UK, „Counter-Terrorism and Sentencing Bill 2019-21: Submission to the Public Bill Committee“, Juni 2020. Abgerufen: https://publications.parliament.uk/pa/cm5801/cmpublic/CounterTerrorism/memo/CTSB07.pdf

187 UNODC, *The use of the Internet for terrorist purposes*. Vereinte Nationen, 2012. S. 16 https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

188 Ebd.

189 Tech Against Terrorism, *Analysis: ISIS use of smaller platforms and the DWeb to share terrorist content.* April 2019. https://www.voxpol.eu/isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content/

Die Vereinten Nationen haben die nationalen Regierungen aufgefordert, eine „klare rechtliche Grundlage für die Verpflichtungen der Parteien des privaten Sektors“ zu schaffen, wonach Technologieunternehmen und -plattformen bei Ermittlungen mit den Strafverfolgungsbehörden kooperieren müssen.[190]

USA

Der politische Ansatz der USA zur Bekämpfung des Missbrauchs von Technologieplattformen kann als uneinheitlich bezeichnet werden. Was die beteiligten staatlichen Stellen anbelangt, so stehen unter anderem das Ministerium für Innere Sicherheit (Department of Homeland Security, DHS), das Justizministerium (Department of Justice, DOJ), das Federal Bureau of Investigation (FBI), das National Counter Terrorism Center (NCTC), der Nationale Sicherheitsrat (National Security Council, NSC) und der Kongress in vorderster Linie der Abwehr.[191] Es wurden bereits eine Reihe von Methoden ausprobiert: „Gegenbotschaften, Aufklärungskampagnen, Partnerschaften und Gesetze.“[192]

Eine solche Methode war die Co-Förderung von globalen, sektorübergreifenden Initiativen. Die Terrorabwehrstrategie der USA verpflichtet sich zur Zusammenarbeit mit der Wirtschaft und IT-Branche, um die Anwerbung von Terroristen, Geldbeschaffung und Radikalisierungsprozesse im Internet zu bekämpfen. Was länderübergreifende Initiativen betrifft, so arbeiten die USA mit Initiativen wie Tech Against Terrorism und dem Global Counterterrorism Forum zusammen, das in Partnerschaft mit anderen Unterzeichnern, der Zivilgesellschaft und dem Technologiesektor mittel- und langfristige Konzepte zur Bekämpfung von gewalttätigem Extremismus im Internet entwickelt.

Auf breiterer Ebene rief die Obama-Administration 2011 die Countering Violent Extremism Task Force ins Leben, um „die inländische Terrorabwehr zu vereinigen.”[193] Die Task Force soll Praktiker aus den oben genannten Gremien zusammenbringen, um die Einbeziehung der Zivilgesellschaft zu koordinieren, Interventionsmodelle zu entwickeln, in die Forschung zu investieren und Kommunikations- sowie digitale Strategien zu kultivieren.[194] Angesichts der bis dato sporadischen Bemühungen der USA hätte ein einheitliches Konzept zur Bekämpfung des gewalttätigen Extremismus im Internet die Bemühungen zur Bekämpfung des Missbrauchs von Plattformen wie Telegram unterstützt.

Anfang 2017 erwog Präsident Trump jedoch eine Umstrukturierung der Task Force dahingehend, dass der White-Supremacy-Terrorismus aus ihrem Aufgabenbereich entfernt und das Programm in „Countering Radical Islamic Extremism“ umbenannt werden sollte.[195] Darüber

190 UNODC, 2012. S. 135
191 Alexander, A. (2019), „A Plan for Preventing and Countering Terrorist and Violent Extremist Exploitation of Information and Communications Technology in America“, *George Washington University Program on Extremism*, S. 5. Abgerufen: https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/A%20Plan%20for%20Preventing%20and%20Countering%20Terrorist%20and%20Violent%20Extremist.pdf
192 Ebd.
193 Department of Homeland Security, „Countering Violent Extremism Task Force.“ Abgerufen: https://www.dhs.gov/cve/task-force
194 Ebd.
195 Ainsley, J. et al., „Exclusive: Trump to focus counter-extremism program solely on Islam – sources“, *Reuters*, 3. Februar 2017. Abgerufen: https://www.reuters.com/article/idUSKBN15G5VO?feedType=RSS&feedName=topNews&utm_source=twitter&utm_medium=Social

hinaus wurden im Frühjahr 2017 in einem Etat alle Mittel für Programme zur Bekämpfung von gewalttätigem Extremismus gekürzt.[196] Ende Oktober 2018 hatte die Task Force ihre Arbeit eingestellt: die Finanzierung lief aus, und „die Mitarbeiter kehrten in ihre alten Behörden und Abteilungen zurück".[197]

Die Aktionen von Trump offenbaren eine tiefe Abwehrhaltung gegenüber Bemühungen der Terrorabwehr im Allgemeinen, aber insbesondere gegenüber Maßnahmen, die auf den gemeinschaftlichen Diskurs und die Einbeziehung der Zivilgesellschaft auf lokaler Ebene oder den rechtsextremen und White-Supremacy-Terror abzielen. Einer der Empfänger von DHS-Mitteln war zum Beispiel Life After Hate, eine Initiative, die mit ihrer Arbeit Individuen dabei hilft, sich aus White-Supremacy- und Neonazi-Gruppen zu lösen.[198] Die Streichung der Finanzierung und die Beschneidung des Aufgabenbereichs, um White-Supremacy-Bestrebungen aus der Abwehrarbeit der USA auszuschließen, kann als ein eklatantes Signal verstanden werden, dass die Trump-Administration nicht gegen Terror dieser Gruppe und rassistische Terrorakte vorgehen wird.

Diese Entwicklung hat große Bedeutung für den Kampf gegen den Missbrauch von Telegram und anderen verschlüsselten und dezentralen Instant-Messaging-Anwendungen. Wie Bennett Clifford oben zeigt, nutzen rechtsextreme Gruppen viele dieser Plattformen zur Koordinierung von Aktivitäten. Wenn sich der Umgang der Regierung mit diesen Plattformen jetzt als „politisch motiviert und gefährlich" erweist,[199] haben wir Grund zur Sorge um die Zukunft der Terrorabwehr. Die letzte Verteidigungslinie gegen den Missbrauch dieser Plattformen ist dann ein erhöhter Druck auf ihre Gründer, den Anordnungen der Strafverfolgungsbehörden und Gerichte Folge zu leisten, ein Ansatz, der sicher zu kurz und zu spät greift.

Dezentrale Lenkungsformen für dezentrale Plattformen?

Im oben stehenden Bericht warnt Bennett Clifford vor der Hinwendung Telegram ähnlicher Anwendungen zu einem dezentralen Server-Hosting. Diese im Zuge des Web 2.0 aufgekommene Option würde es Nutzern ermöglichen, direkt miteinander zu kommunizieren und zentralisierte Dienste von Unternehmen wie Google, Amazon, Microsoft und Facebook zu umgehen.[200] Das dezentrale Modell „kehrt das derzeitige Modell des Dateneigentums (Data Ownership) um", sodass die Nutzer uneingeschränkten Zugang und Verfügungsgewalt über ihre Daten haben.[201]

196 Ainsley, J., „White House budget slashes ‚countering violent extremism' grants", *Reuters*, 23. Mai 2017. Abgerufen: https://www.reuters.com/article/us-usa-budget-extremism-idUSKBN18J2HJ

197 Beinart, P. „Trump Shut Programs to Counter Violent Extremism", *The Atlantic*, 29. Oktober 2018. Abgerufen: https://www.theatlantic.com/ideas/archive/2018/10/trump-shut-countering-violent-extremism-program/574237/

198 Life After Hate, „About Us." Abgerufen: https://www.lifeafterhate.org/about-us-page

199 Southern Poverty Law Center, „Trump's planned changes to government's ‚Countering Violent Extremism' program are politically motivated, dangerous", 2. Februar 2017. Abgerufen: https://www.splcenter.org/news/2017/02/02/splc-trumps-planned-changes-governments-countering-violent-extremism-program-are

200 Corbyn, Z. „Decentralisation: The Next Big Step for the World Wide Web", *The Guardian*, 8. September 2018. Abgerufen: https://www.theguardian.com/technology/2018/sep/08/decentralisation-next-big-step-for-the-world-wide-web-dweb-data-internet-censorship-brewster-kahle

201 Bodó, L. „Decentralised Terrorism: The Next Big Step for the So-Called Islamic State (IS)?" *VoxPol*, 12. Dezember 2018. Abgerufen: https://www.voxpol.eu/decentralised-terrorism-the-next-big-step-for-the-so-called-islamic-state-is/

Die zentrale Diensterbringung in Regierungshand bietet hingegen reichlich Gelegenheit für Missbrauch, Überwachung und Zensur. So verhängte beispielsweise die indische Regierung im Zusammenhang mit den seit Jahrzehnten andauernden antimuslimischen Gewalt und Gräueltaten in Indien in Kaschmir die weltweit längste Internetabschaltung.[202] Die 192 Tage dauernde Abschaltung ist Teil einer umfassenderen, beunruhigenden Haltung gegenüber den digitalen Rechten in Indien: der Minister für Kommunikations- und Informationstechnologie stellte das Recht der Bürgerinnen und Bürger auf das Internet in Frage und verkündete: „Das Recht auf das Internet ist zwar wichtig, aber die Sicherheit des Landes ist ebenso wichtig ... Können wir leugnen, [dass] das Internet von Terroristen missbraucht wird?“[203]

Ebenso sind Fälle bekannt, in denen Unternehmen die Daten ihrer Nutzer missbraucht haben. Im Jahr 2018 griff die politische Beratungsfirma Cambridge Analytica die persönlichen Daten von Millionen von Facebook-Nutzern für politische Werbung ab.[204] Die Datenpanne, die größte in der Geschichte von Facebook, wurde von Präsidentschaftskandidat Donald Trump 2016 genutzt, um als Wechselwähler identifizierte Facebook-Nutzer mit passgenauer Wahlwerbung zu erreichen (Microtargeting).[205] Da die Daten der Nutzer zentralisiert auf den Facebook-Servern liegen, kann die Plattform die sensiblen und personenbezogenen Daten von Milliarden von Menschen monetarisieren, überwachen und missbrauchen.[206]

Ein dezentrales Internetmodell, das die Daten zwar vor unbefugtem Zugriff schützt, bringt dafür andere Herausforderungen mit sich. Insbesondere können dezentrale und verschlüsselte Instant-Messaging-Anwendungen wie Telegram und seine Alternativen eine sichere Umgebung für extremistische Inhalte darstellen. Wie Clifford oben schreibt, macht die Möglichkeit eines dezentralen Server-Hostings bei neu aufkommenden Plattformen „diese Plattformen unweigerlich zugänglicher für extremistische Gruppen“. Dezentrale Plattformen können sich wesentlich leichter der Überwachung und Intervention sowohl durch Selbstregulierung als auch die Strafverfolgung entziehen, da sich die Daten nicht mehr in den Händen des Anbieters befinden.

Der Kampf gegen die Ausnutzung und den Missbrauch von dezentralen Instant-Messaging-Plattformen wirft dringende und schwierige Fragen für das entsprechende politische und unternehmerische Vorgehen auf. Wie sollten Regierungen und Unternehmen auf die extremistische Nutzung eines dezentralen Internets reagieren? Wie können die Rechte der Nutzer auf Privatsphäre und freie Meinungsäußerung gegen die Ausnutzung von Plattformen zur Verbreitung von Propaganda und Desinformation, zur Rekrutierung für terroristische Zwecke und zur Planung von Anschlägen abgewogen werden?

202 Pandit, I. „India is escalating Kashmir conflict by painting it as terrorism“, *openDemocracy*, 2. Dezember 2019. Abgerufen: https://www.opendemocracy.net/en/openindia/india-escalating-kashmir-conflict-painting-it-terrorism/

203 Shastry, V. „Asia's Internet Shutdowns Threaten the Right to Digital Access“, *Chatham House*, 18. Februar 2020. Abgerufen: https://www.chathamhouse.org/2020/02/asias-internet-shutdowns-threaten-right-digital-access

204 Confessore, N. „Cambridge Analytica and Facebook: The Scandal and the Fallout So Far“, *The New York Times*, 4. April 2018. Abgerufen: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

205 Hilder, P. und Lewis, P. „Leaked: Cambridge Analytica's Blueprint for Trump's Victory“, *The Guardian*, 23. März 2018. Abgerufen: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory

206 Kamyshev, P. „Facebook's Political Problems are Inherent to Centralized Social Media“, *Palladium Magazine*, 14. Februar 2019. Abgerufen: https://palladiummag.com/2019/02/14/facebooks-political-problems-are-inherent-to-centralized-social-media/

Innerhalb der gegenwärtigen Lenkungsformen gibt es drei mögliche Strategien, die grob betrachtet jeweils in einem bestimmten Stadium eines linearen Radikalisierungsprozesses ansetzen.

Der erste Ansatz – die frühzeitige Prävention – zielt darauf ab, in den frühen Stadien der Radikalisierung einzugreifen, um Menschen davon abzuhalten, sich mit terroristischen Inhalten auseinanderzusetzen. Im Hinblick auf Telegram ähnliche Anwendungen würde eine frühzeitige Prävention verhindern, dass Menschen versuchen, mit extremistischen Inhalten, Gruppen und Kanälen auf der Plattform zu interagieren. Der Vorteil dieses Ansatzes besteht darin, dass er die ressourcenintensive Überwachung der Plattform reduziert und die Online-Präsenz von Extremisten schwächt, während die Meinungsfreiheit und der Schutz der Privatsphäre der Nutzer gewahrt bleiben.

Derartige Präventionsprogramme bergen jedoch selbst eine Vielzahl ethischer, politischer und rechtlicher Fallstricke. Das vielleicht umstrittenste Präventionsprogramm ist die 2003 eingeführte Prevent Strategy des britischen Innenministeriums (Home Office). Die Strategie zielt ab auf „Personen, die anfällig für Rekrutierungen sind“, insbesondere innerhalb von Institutionen wie denjenigen des staatlichen Gesundheitssystems (National Health Service, NHS), an Schulen und Universitäten sowie in anderen lokalen Gemeinschaften und zivilgesellschaftlichen Gruppen.[207] Bürgerrechtsgruppen kritisieren Prevent seit seiner Einführung: Shami Chakrabarti, ehemalige Vorsitzende der prominenten Bürgerrechtsgruppe Liberty, bezeichnete Prevent als „das größte Spionageprogramm Großbritanniens in der jüngeren Vergangenheit“, da die über so genannte schutzbedürftige Personen gesammelten Informationen politische und religiöse Ansichten sowie Daten über die psychische Gesundheit und sexuelle Aktivitäten einschlössen.[208] Prevent ziele sehr selektiv auf britische Muslime; das Programm schüre dadurch Islamophobie und vermische „legitimen politischen Widerstand unter jungen britischen Muslimen“ mit „Anzeichen für gewalttätigen Extremismus“.[209]

Die zweite Lenkungsstrategie konzentriert sich auf Ausstiegsangebote und Gegenbotschaften (Counter-Messaging). Personen, die bereits online auf extremistische Inhalte zugreifen und diese konsumieren, können mit Gegennarrativen angesprochen werden, die „ein überzeugendes alternatives Weltbild sowie andere Orientierungs- und Handlungsoptionen als die in gewaltbereiten extremistischen Kreisen zirkulierenden“ anbieten und Werte wie Toleranz, Offenheit, Freiheit und Demokratie propagieren.[210] Für Instant-Messaging-Plattformen wie Telegram könnte dies die Infiltration von Kanälen und Gruppen beinhalten, um alternative Narrative zu posten, in der Hoffnung, einige Personen vom Weg der Radikalisierung abzubringen.

207 Britisches Innenministerium, „Counter-Terrorism Strategy: The Four Ps: Pursue, Prevent, Protect, Prepare“. Abgerufen: https://web.archive.org/web/20090711105017/http://security.homeoffice.gov.uk/counter-terrorism-strategy/about-the-strategy1/four-ps/; Britische Regierung, „CONTEST: The United Kingdom's Strategy for Countering Terrorism“, Juni 2018. Abgerufen: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf

208 Dodd, V. „Government anti-terrorism strategy ‚spies' on innocents“, *The Guardian*, 16. Oktober 2009. Abgerufen: https://www.theguardian.com/uk/2009/oct/16/anti-terrorism-strategy-spies-innocents

209 Abbas, T. (2019) „Implementing ‚Prevent' in Countering Violent Extremism in the UK: A Left-Realist Critique“, *Critical Social Policy* 39, Nr. 3: S. 396–412

210 Waldman, S. und Verga, S. (2016) „Countering violent extremism on social media“, Centre for Security Science, Defence Research and Development Canada, S. 7. Abgerufen: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805091_A1b.pdf

Counter-Messaging hat Potenzial, aber die staatliche strategische Kommunikation ist bisher weitgehend erfolglos[211] und hatte unbeabsichtigte negative Folgen. Das Programm „Think Again Turn Away“ des US-Außenministeriums, das Counter-Messaging-Material verbreitete und auf Twitter Dispute mit IS- und Pro-IS-Accounts führte, provozierte Gegenreaktionen und Zorn.[212] Eine Untersuchung durch Demos ergab, dass die europäischen Counter-Messaging-Seiten auf Facebook insgesamt sehr wenig frequentiert wurden.[213] Staatliche Initiativen zur strategischen Kommunikation leiden an der so genannten „Glaubwürdigkeitslücke“. Hierbei wird die gewaltbereite extremistische Botschaft durch Darstellung der Kluft zwischen den staatlich propagierten Werten und ihrem Handeln noch verstärkt.[214]

Seitdem heben Counter-Messaging-Initiativen weniger auf staatliche Beteiligung ab und stärker auf Branchenengagement. Google und sein Mutterunternehmen Alphabet haben mit einem „Verfahren für Content-Umleitung (Content-Redirect)“ Neuland beschritten, das sich an Personen richtet, die online nach IS-Inhalten suchen, und sie zu kuratierten Videos auf YouTube umleitet, die der gewaltbereiten extremistischen Propaganda entgegenwirken.[215] Der kuratierte Videoinhalt konfrontiert anfällige und radikalisierte Personen mit Narrativen, die auf Werte wie Toleranz, Diversität und Inklusivität abheben. Alphabets gewichtiger Partner für die Content-Redirect-Methode ist Moonshot CVE, das in über achtundzwanzig Ländern und in fünfzehn Sprachen Counter-Messaging-Kampagnen durchführt.[216] Die in den USA ansässige Anti-Defamation League kooperiert mit Moonshot CVE, um White-Supremacy- und dschihadistischen Aktivitäten im Netz entgegenzuwirken.[217]

Zwar sind Aktivitäten wie diejenigen von Moonshot CVE unter Umständen geeignet, den Radikalisierungsprozess zu unterbrechen, doch bergen privatwirtschaftliche Lösungen für tiefsitzende gesellschaftspolitische Probleme ein eigenes Konfliktpotenzial. Moonshot CVE unterliegt als unabhängiges Unternehmen keiner staatlichen oder zivilgesellschaftlichen Aufsicht oder Rechenschaftspflicht. Das Unternehmen legt lediglich allgemeine Daten über seine Geschäftstätigkeit offen, und es ist nicht klar, wann und nach welchen Kriterien die Weiterleitung („Redirect“) greift.[218]

Die dritte Lenkungsstrategie – die Regulierung der Plattformen – greift erst am Ende des Radikalisierungsprozesses. Im obigen Bericht beschreibt Clifford die Bemühungen der Strafverfolgungsbehörden, Plattformen wie Telegram unter Druck zu setzen, damit sie Gerichtsbeschlüssen aufgrund mutmaßlicher terroristischer Aktivitäten nachkommen. So verweist Clifford auf Seite 6 auf die von Europol veranstalteten Referral Action Days, mit denen erreicht wurde, dass Telegram seine Datenschutzerklärung durch eine Klausel ergänzte, wonach die Plattform in Fällen mutmaßlich extremistischen Inhalts Nutzerdaten zu Identifikationszwecken an die Behörden

211 Bartlett, J. und Krasodomski-Jones, A. (2015) „Counter-Speech: examining content that challenges extremism online“, *Demos*. Abgerufen: https://www.demos.co.uk/wp-content/uploads/2015/10/Counter-speech.pdf
212 Katz, R. (2014) „The State Department's Twitter War with ISIS is Embarrassing“, *Time*. Abgerufen: https://time.com/3387065/isis-twitter-war-state-department/
213 Bartlett und Krasodomski-Jones, „Counter-Speech“
214 Romaniuk, P. (2015) „Does CVE Work? Lessons Learned from the Global Effort to Counter Violent Extremism“, *Global Center on Cooperative Security*. Abgerufen: https://www.globalcenter.org/wp-content/uploads/2015/09/Does-CVE-Work_2015.pdf, S. 33
215 Siehe: https://redirectmethod.org/
216 Siehe: http://moonshotcve.com/work/
217 „ADL and Partners Counter White Supremacists Online Through Google Search“, *Anti-Defamation League*. Abgerufen: https://www.adl.org/news/press-releases/adl-and-partners-counter-white-supremacists-online-through-google-search
218 Siehe: http://moonshotcve.com/work/

weitergeben darf. Andere im obigen Bericht beschriebene Plattformen arbeiten in mehr oder weniger großem Umfang mit Regierungen und Strafverfolgungsbehörden zusammen, um die Verbreitung extremistischer Inhalte zu bekämpfen.

Die besondere Schwierigkeit bei dieser Herangehensweise besteht darin, dass Politik und Strafverfolgung hiermit eine Sisyphusarbeit verrichten: Sobald sich eine Plattform den Anordnungen beugt, entsteht an ihrer Stelle eine andere Plattform, die den Nutzern einen besseren Schutz der Anonymität bietet. So zieht der obige Bericht folgendes Fazit: „Mit dem Wechsel extremistischer Gruppen von Telegram zu neu aufkommenden und immer stabileren Instant-Messaging-Alternativen, die neue Eigenschaften in puncto Schutz der Privatsphäre und Sicherheit mitbringen, lautet die Frage nicht mehr ‚ob', sondern ‚wann' und ‚welche'".

Ein merkmalorientierter Ansatz zur Bekämpfung des Online-Extremismus, wie er auf den letzten Seiten des vorstehenden Berichts skizziert wird, eröffnet die Möglichkeit einer neuen Lenkungsform, die über die drei hier beschriebenen Ansatzpunkte hinausgeht. Alle der oben genannten Konzepte beruhen auf einer vertikalen, abwärts gerichteten Lenkungsform, oft durch staatliche Stellen, die sich auf eine gesetzgeberische Rechtfertigung stützen.[219] Prävention, Counter-Messaging und Regulierung unterliegen jeweils einer „Kommando- und Lenkungsstruktur", in der bestimmte Stellen (Regierungen, Unternehmen, Strafverfolgungsbehörden, Nachrichtendienste) von oben herab das Vorgehen bestimmen.

Ein dezentrales Web, das durch die Eigenschaften und Funktionen charakterisiert ist, die es den Nutzern bietet, verlangt unter Umständen eine andere Strategie. Statt einer vertikalen Lenkungsform könnte sich ein horizontales Strategiekonzept, das den Aufbau eines dezentralen Internets nachahmt, als wirksam erweisen. Sektorübergreifende Initiativen, wie z. B. ein erweitertes GIFCT, wie Clifford es oben auf Seite 29 beschreibt, das ein breites Spektrum von Dienstanbietern mit politischen Entscheidungsträgern und wissenschaftlichen Experten zusammenbringt, sind ein gutes Beispiel für einen eher dezentralen Ansatz.

Ein früherer GNET-Bericht, *„Künstliche Intelligenz und Terrorabwehr",* empfahl eine unabhängige Regulierungsstelle bei der Moderation schädlicher Online-Inhalte als möglicherweise sehr effektiv.[220] Eine Co-Regulierung durch Zivilgesellschaft, Staat, Industrie und Dienstanbieter, die von einem internationalen und unabhängigen Gremium überwacht wird, entspräche einer weiter in die Breite gehenden und stärker integrativen Strategie bei der Terrorabwehr. Dieses Gremium könnte sich im Aufbau in der Tat an den Eigenschaften und Merkmalen dezentraler Plattformen und gewalttätiger extremistischer Inhalte im Netz orientieren, wie Clifford oben vorschlägt, um „Abwehrmaßnahmen vorzubereiten ... [und] den extremistischen Missbrauch des Angebots bereits in der frühen Iterationsphase empfindlich zu stören". Eine solche dezentrale Lenkungsform könnte sich bei der Anpassung und Bewältigung der Herausforderungen eines Trends zu einem dezentralen Internet als sehr wirksam erweisen.

219 Zwitter, A. und Hazenberg, J. (2020), „Decentralized Network Governance: Blockchain Technology and the Future of Regulation", *Frontiers in Blockchain*. Abgerufen: https://www.frontiersin.org/articles/10.3389/fbloc.2020.00012/full

220 GNET, „Künstliche Intelligenz und Terrorabwehr: eine Einführung", S. 41. Abgerufen: https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Artificial-Intelligence-and-Countering-Violent-Extremism-A-Primer_GERMAN.pdf

Global Network
on Extremism & Technology

KONTAKTANGABEN

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

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

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

Twitter: **@GNET_research**

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

© GNET