Innovative Technologien und Extremisten: Das DWeb als neue Internet-Realität?

Lorand Bodo und Inga Kristina Trauthig

Kurzfassung und Übersicht

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

Die Autoren dieses Berichts sind
Lorand Bodo und Inga Kristina Trauthig

Das Global Network on Extremism and Technology (GNET) ist eine akademische Forschungsinitiative mit Unterstützung des Global Internet Forum to Counter Terrorism (GIFCT), eine unabhängige, 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
Vereinigtes Königreich

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

Twitter: **@GNET_research**

Diese Kurzfassung und Übersicht ist auf Arabisch, Englisch, Französisch, Deutsch, Indonesisch und Japanisch erhältlich. Wie alle anderen GNET-Publikationen können diese Kurzfassung sowie der vollständige Bericht auf Englisch kostenlos von der GNET-Website unter www.gnet-research.org heruntergeladen werden.

Kurzfassung

Das World Wide Web hat sich seit seiner Erfindung durch Sir Tim Berners-Lee im Jahr 1989 zu einem Ökosystem entwickelt, in dem Milliarden von Nutzern von relativ wenigen, aber großen Konzernen abhängig sind. Die Verwendung einer Suchmaschine, das Posten in den sozialen Medien, die Kommunikation mit anderen oder das Speichern von Daten in der Cloud – alles sind Beispiele, wie diese Unternehmen für Milliarden von Menschen echten Nutzen bieten. Mit der Nutzerbasis wächst jedoch im Laufe der Jahre auch deren Macht. Die Rückverlagerung der Macht von diesen wenigen, großen Konzernen in die Hände der Nutzer ist für Befürworter des dezentralen Internets („Decentralised Web" oder kurz „DWeb") entscheidend. Eine solche „Re-Dezentralisierung" sollte den Nutzern zudem mehr Kontrolle über ihre Daten geben. Das DWeb befindet sich auch im Blickfeld extremistischer Akteure, die nach innovativen Wegen suchen, ihre Propaganda zu verbreiten und das Entfernen von Accounts und Inhalten zu erschweren. Dieser Bericht bietet einen kurzen Überblick über den aktuellen Stand des DWeb und erörtert die bestehende sowie mögliche zukünftige Ausbeutung des DWeb durch Extremisten. Unser Augenmerk liegt hierbei auf Rechtsextremisten (RE) und dem sogenannten Islamischen Staat (IS), da diesen beiden extremistischen Bewegungen in vielen Teilen der Welt das höchste Bedrohungspotenzial zugeschrieben wird. Wir analysieren eine Stichprobe von 30 Telegram-Kanälen, die anhand unserer Kategorienmerkmale dem rechtsextremen Spektrum zuzuordnen sind. Der zweite Datensatz erlaubt eine kritische Untersuchung der DWeb-Nutzung durch den sogenannten Islamischen Staat. Dieser Datensatz wurde von „Tech Against Terrorism" bereitgestellt, einer von der UNO unterstützten und von Regierungen und der Privatwirtschaft gemeinschaftlich finanzierten Initiative.

Auf Grundlage der Literaturübersicht, durchgeführter Interviews sowie der Datenanalyse stellen wir Folgendes fest:

- Da Extremisten jede Technologie für ihre Zwecke ausbeuten möchten, ist das DWeb ebenfalls in ihr Blickfeld geraten. Ein wichtiger Grund für seine Attraktivität ist, dass sich „im DWeb" gehostete Inhalte nicht entfernen lassen, da das DWeb nicht von einer zentralen Behörde kontrolliert wird.

- Die Analyse zeigt jedoch, dass die betroffenen Akteure derzeit noch andere existierende Technologien bevorzugen.

- Insgesamt besteht für die Ausbeutung von DWeb-Diensten durch RE- und IS-Akteure ein mittleres Risiko.

- Dazu kommt, dass extremistische Akteure nicht unbedingt das DWeb benötigen, um ihre Inhalte zu hosten, zu verteilen und zu kontrollieren, weil dafür bereits andere Dienste existieren.

- Schließlich können DWeb-Dienste die Risiken einer derartigen Ausbeutung begrenzen, wodurch das DWeb nicht unbedingt einen sicheren Hafen für Extremisten darstellt.

Übersicht

Begriffe rund um das dezentrale Internet (DWeb) – wie Web3 oder Bitcoin – scheinen gleichbedeutend mit Blockchains und Kryptowährung geworden zu sein. Insgesamt kreisen die wichtigsten Fragen zum dezentralen Internet um zwei grundlegende Themen: (1) Ist ein dezentrales Internet für genügend Menschen realistisch und attraktiv genug? Und: (2) Was ist das Wesen dieses „neuen Internets“? Oder anders ausgedrückt: Wird es die negativen Aspekte des vorhandenen Internets – das schließlich regelmäßig für Online-Radikalisierung oder die Erstarkung autoritärer Bewegungen verantwortlich gemacht wird – vermeiden können? Könnte das DWeb stattdessen positive Aspekte fördern, wie z. B. sein Potenzial für Aktivisten, sich mithilfe dieser Technologie außer Sichtweite staatlicher Zensoren zu organisieren?

Dieser Bericht trägt zu beiden Themenkreisen bei, indem er hinterfragt, wie Extremisten das DWeb bereits ausbeuten und wie sie es in Zukunft ausbeuten könnten. Warum ist das dezentrale Internet entweder „gut“ oder „schlecht“? Warum nutzen Menschen es? Wird diese Version des Internets durch den kleinen Anteil der Nutzer, der es missbraucht, bereits gefährdet? Was könnten Entwickler in ihre Erwägungen einbeziehen, wenn man die vorhandenen Beweise betrachtet? Was müssen politische Entscheidungsträger bei der Ausarbeitung gesetzlicher Maßnahmen rund um Technologie beachten? Wissenschaftler und Journalisten haben das DWeb bereits in vielerlei Hinsicht untersucht; dies reicht von Fragen der politischen Ökonomie bis hin zu den normativen Auswirkungen einer ethischen Grundeinstellung unter Web3-Entwicklern, dass man „Big Tech“ nicht vertrauen kann. Für die Zwecke dieses Berichts liegt der Schwerpunkt auf den Implikationen für extremistische Akteure sowie den entsprechenden Sicherheitsimplikationen für die Gesellschaft als Ganzes.

Unser Forschungsansatz beruht auf einer dreigleisigen Strategie. Zunächst haben wir eine systematische Literaturübersicht zu dem vorhandenen Material über das DWeb erstellt; unser Augenmerk lag insbesondere auf der Moderation von Inhalten sowie dem Extremismus. Zweitens haben wir Belege dafür gesammelt und organisiert, dass Rechtsextremisten und Organisationen des Islamischen Staates mit dem DWeb experimentieren. Schließlich haben wir teilstrukturierte Interviews mit Befürwortern, Kritikern und Entwicklern des DWeb geführt, um unser Verständnis für dieses sich entwickelnde Thema zu vertiefen. Bezeichnend für diesen Bericht ist sein Sondierungscharakter, der direkt mit der Tatsache zusammenhängt, dass das DWeb für die meisten Menschen auf der Welt derzeit eher eine Idee als eine Realität darstellt.

Ein großes Risiko im Zusammenhang mit gewalttätigem Online-Extremismus und -Terrorismus besteht darin, dass DWeb-Technologie für die Speicherung und Bereitstellung von Daten missbraucht werden könnte. In diesem Fall „[...] könnten dezentralisierte Methoden der Datenspeicherung es einer einzelnen Instanz schwierig oder gar praktisch unmöglich machen, Inhalte zu zensieren“.[1] Infolgedessen lassen sich extremistische Inhalte nicht einfach entfernen und sind somit für jeden zugänglich, der weiß, wo man sie findet.

Unsere Literaturübersicht ergab, dass sich DWeb-Technologien schon seit geraumer Zeit im Blickfeld extremistischer Gruppierungen befinden, aber die begrenzten Funktionen und die damit verbundene eingeschränkte Publikumsreichweite ihre Nutzung durch solche Gruppen beschränkt haben. Die vordringliche Sorge ist allerdings, dass die allgemeine Ausbreitung des DWeb mit einer verstärkten Ausbeutung durch extremistische Akteure einhergehen könnte.

Die vier Haupterkenntnisse aus unseren RE-Daten sind folgende:

(1) DWeb-Dienste treten nicht in nennenswertem Maße in Erscheinung.

(2) Der Großteil der weiterführenden Links führt zu zwei großen Social-Media-Plattformen.

(3) Die rechtsextreme Stichprobe teilte mehr Links zu unzuverlässigen Nachrichten und Blogs als zu zuverlässigeren Nachrichtenquellen.

(4) Archivierungsdienste werden ebenso häufig genutzt wie DWeb-Dienste.

Die drei Haupterkenntnisse aus unseren IS-Daten sind folgende:

(1) Dezentrale Dienste werden genutzt, aber nicht im gleichen Ausmaß wie zentralisierte Dienste.

(2) Dienste für Filehosting und -sharing sind vorrangige Ziele.

(3) Bei Diensten für Filehosting und -sharing, Archivierung und Pasting gibt es mehr verifizierte terroristische Inhalte als in sozialen Medien.

1 Barabas, Chelsea, Neha Narula und Ethan Zuckerman. „Defending Internet Freedom through Decentralization: Back to the Future?“ The Center for Civic Media & The Digital Currency Initiative MIT Media Lab, August 2017. https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/59ae908a46c3c480db42326f/1504612494894/decentralized_web.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
Vereinigtes Königreich

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

Twitter: **@GNET_research**

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