CEP POLICY PAPER

Terrorismusfinanzierung und soziale Medien

April 2020

Dr. Hans-Jakob Schindler

COUNTER EXTREMISM PROJECT

COUNTER EXTREMISM PROJECT

Über CEP und den Autor

Das Counter Extremism Project (CEP) ist eine gemeinnützige, überparteiliche, internationale Organisation, die das Ziel verfolgt, der Bedrohung durch extremistische Ideologien entgegenzuwirken und pluralistisch-demokratische Kräfte zu stärken. CEP übt durch eigene Recherchen und Studien Druck auf finanzielle und materielle Unterstützungsnetzwerke von extremistischen Organisationen aus, arbeitet den Narrativen von Extremisten und ihren Rekrutierungstaktiken im Internet entgegen, und wirbt für effektive Regulierungen und Gesetze.

Dr. Hans-Jakob Schindler ist Senior Director von CEP und leitet das Büro in Berlin. Er ist der ehemalige Koordinator des *ISIL, Al-Qaida and Taliban Monitoring Team* des Sicherheitsrates der Vereinten Nationen.

Bei Fragen zu diesem Papier oder den Aktivitäten von CEP kontaktieren Sie bitte **Marco Macori**, CEP Research Fellow: mmacori@counterextremism.com; Tel. (030) 300 149 3369

Terrorismusfinanzierung und soziale Medien

Im Januar und März 2020 untersuchte das Counter Extremism Project (CEP) in zwei Schritten die aktuell bestehenden Abwehrmechanismen großer Plattformen, um zu testen, ob diese in Bezug auf den Missbrauch ihrer Systeme durch Financiers des internationalen Terrorismus effektiv sind. Zunächst teste CEP die Möglichkeit der durch den Sicherheitsrat der Vereinten Nationen weltweit öffentlich enttarnter Financiers von al-Qaida und dem Islamischen Staat, weiterhin auf großen Plattformen aktive Profile zu unterhalten und daher unter Umständen ihre Aktivitäten über die sozialen Medien weiterzuführen. Dabei stellte CEP fest, dass rund ein Duzend dieser weltweit bekanntesten und wichtigsten Financiers im Januar 2020 weiterhin anscheinend aktive Profile unterhielten.

Weiterhin untersuchte CEP die Nutzungsbedingungen[1] großer Plattformen. Ein Bericht aus 2019 des Global Research Network on Terrorism and Technology, welches ein Teil der Global Internet Forum to Counter Terrorism (GIFCT) ist, hatte aufgezeigt, dass diese Nutzungsbedingungen Lücken aufweisen und Terrorismusfinanzierung nicht explizit ausschließen.[2] CEP konnte im März 2020 keine generelle Verbesserung der Situation seit dem Bericht 2019 feststellen. Da die jeweiligen Nutzungsbedingungen die Prioritäten der internen weltweiten Inhaltsüberwachung durch die Plattformen festlegen, deutet dies darauf, dass Plattformen diese Art des Missbrauchs möglicherweise weiterhin nicht prioritär behandeln.

Der Missbrauch von sozialen Medien und anderen Dienstleistungen im Internet wird spätestens seit dem Erstarken des Islamischen Staates (IS) ab 2014 regelmäßig sowohl in den Medien als auch in Fachliteratur diskutiert. Seit einigen Jahren bemühen sich die großen

[1] Dieser werden je nach Plattform unterschiedlich bezeichnet als „Community Standards", „Rules" oder „Terms of Service" und legen fest, welche Inhalte auf der jeweiligen Plattform geduldet werden und welche nicht.

[2] Tom Keatinge, Florence Keen, Social Media and Terrorism Financing. What are the Vulnerabilities and How Could Public and Private Sector Collaborate Better? Global Research Network on Terrorism and Technology: Paper No. 10, Royal United Services Institute 2019. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.

Plattformen den durch diesen Missbrauch erlittenen Reputationsschaden durch öffentlichkeitswirksame Maßnahmen zu begegnen. So gründeten zu Beispiel 2017 Facebook, Microsoft, Google und Twitter GIFCT, welches das Ziel verfolgt den Missbrauch dieser Plattformen durch Terroristen zu stören.[3] Als Teil dieser Arbeit etablierte GIFCT auch das Global Research Network on Terrorism and Technology, welches zur Aufgabe hat, durch akademische Forschung Impulse zur Weiterentwicklung der Abwehrmechanismen der Firmen zu geben.[4] Ein Teilgebiet dieser Arbeit betrifft die Finanzierung des Terrorismus mittels Internet Dienstleistungen, inklusive sozialer Medien. Der Bericht des GIFCT Research Networks von 2019 enthält eine Reihe grundlegender Empfehlungen, wie Plattformen ihre Abwehrmechanismen speziell zu diesem Risikofeld erhöhen könnten.[5]

Die von CEP im Januar und März 2020 durchgeführten Tests deuten darauf hin, dass bei den Abwehrmechanismen globaler Plattformen gegen den Missbrauch ihrer Systeme durch Terrorfinanciers und zur Finanzierung des Terrorismus weiterer Verbesserungsbedarf besteht.

CEP hat daher zwei grundlegende Empfehlungen:

A) **Da die Finanzierung des Terrorismus die Grundlage jeden terroristischen Handelns darstellt, sollte sich die Industrie diesem Risiko pro-aktiv stellen.** Ein System, welches darauf vertraut, dass von außen Organisationen wie CEP die potentiellen Profile der wichtigsten globalen Financiers des Terrorismus auf den globalen Plattformen finden und die Plattformen anmahnen, deren Aktivitäten zu unterbinden kann diese Gefahr nicht effektiv bekämpfen. Hier müssen, insbesondere Firmen mit einem weltweiten Kundenstamm pro-aktiv und effektiver vorgehen.

B) **Die Plattformen sollten ihre Nutzungsbedingungen, wie schon in dem vom Global Research Network on Terrorism and Technology im Bericht von 2019 vorgeschlagen, anpassen und damit auch die internen Systeme der Inhaltsüberwachung zu diesem Thema besser sensibilisieren.** Die Financiers des weltweiten Terrorismus brauchen für ihre Tätigkeiten einen möglichst großen Wirkungsrahmen, damit sie Spender und Unterstützer erreichen können. Finanzierung des Terrorismus sollte daher, insbesondere bei globalen Plattformen in den Nutzungsbedingungen explizit angesprochen und ausgeschlossen werden. Dies ist insbesondere wichtig für Crowdfunding Plattformen.

[3] https://www.gifct.org/about/
[4] https://www.gifct.org/partners/
[5] Tom Keatinge, Florence Keen, Social Media and Terrorism Financing. What are the Vulnerabilities and How Could Public and Private Sector Collaborate Better? Global Research Network on Terrorism and Technology: Paper No. 10, Royal United Services Institute 2019. Seite 17f. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.

Risikoanalyse

Das Aufkommen der sozialen Medien wurde von terroristischen Gruppen und Organisationen nicht ignoriert, sondern bilden mittlerweile einen zentralen Teil ihrer strategischen Fähigkeiten. Seit dem Aufstieg des IS wurden zahlreiche Berichte veröffentlich, welche vor dem Missbrauch von sozialen Medien, durch diese Terrorgruppe warnen.[6] Diese und andere Terrororganisationen nutzen sehr geschickt diese neue Medienlandschaft, um Terrorwissen und -fähigkeiten zu verbreiten, zu radikalisieren, zu rekrutieren, und operativ zu kommunizieren.

Seit 2014 dokumentiert dass ISIL, Al-Qaida and Taliban Monitoring Team des Sicherheitsrates der Vereinten Nationen diesen Missbrauch.[7] Das Team beobachtet im Auftrag des Sicherheitsrates Terrorgruppen und Individuen, welche zu den weltweiten Netzwerken von IS, al-Qaida und den Taliban gehören und berät sowohl den Sicherheitsrat als auch den Generalsekretär der Vereinten Nationen in Bezug auf globale Gegenmaßnahmen, um die Gefahr, welche von diesen Gruppen ausgeht, einzudämmen.

Bei der Bekämpfung dieser Art von Missbrauch durch die Industrie wurden mittlerweile einige erste Fortschritte erzielt. Zum Beispiel kooperierten erfolgreich mehrere Plattformen mit EUROPOL am 16th Referral Action Day, welcher von European Union Internet Referral Unit koordiniert wurde.[8] Diese Fortschritte beruhen auch auf öffentlichen Druck durch die Zivilgesellschaft,[9] sowie Maßnahmen einzelner Regierungen,[10] einschließlich der Europäischen Union.[11]

Ein spezieller Missbrauch der sozialen Medien durch Terrorgruppen, die Finanzierung mittels dieser Plattformen, hat bislang weniger öffentliche Aufmerksamkeit erhalten. Der anhaltende Missbrauch von Internet- und sozialen Mediendiensten durch terroristische Organisationen zur Finanzierung ihrer Aktivitäten wurde in der Fachwelt in den letzten Jahren immer wieder

---

[6] Siehe zum Beispiel: S/2014/815 vom 14.11.2014, Paragraphen 27 und 90, https://www.undocs.org/S/2014/815.

[7] S/2014/770 vom 29.10.2014, Paragraphen 17 – 22. https://www.undocs.org/S/2014/770
Die regelmäßigen Berichte des Monitoring Teams sind hier erhältlich:
https://www.un.org/securitycouncil/sanctions/1267/monitoring-team/reports
https://www.un.org/securitycouncil/sanctions/1988/monitoring-team/reports

[8] EUROPOL, Referal Action Day Against Islamic State Online Terrorist Propaganda, 22.11.2019, https://www.europol.europa.eu/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda.

[9] Zum Beispiel die Digital Disruption Campaign des Counter Extremism Projects (CEP), https://www.counterextremism.com/digital-disruption

[10] In diesem Zusammenhang ist insbesondere das Netzwerkdurchsetzungsgesetz (NetzDG) herauszustellen. NetzDG war der weltweit erste Versuch eines westlichen Staates, Grundregeln für die Nutzung sozialer Medien einzuführen. Schon im Dezember 2018 veröffentlichte CEP eine erste detaillierte Studie zu den Auswirkungen des NetzDG, siehe: Williams Echikson and Oliva Knodt, Germany's NetzDG: A key test for combatting online hate. CEPS and Counter Extremism Project, 09. November 2018. https://www.counterextremism.com/sites/default/files/CEP-CEPS_Germany%27s%20NetzDG_020119.pdf

[11] Eine neue Richtline der Europäischen Union zur Entfernung terroristischer Inhalte aus dem Netz ist mittlerweile in den letzten Stadien der Entscheidungsfindung. Siehe: http://www.europarl.europa.eu/legislative-train/theme-civil-liberties-justice-and-home-affairs-libe/file-preventing-the-dissemination-of-terrorist-content-online. CEP begleitet diesen Prozess in Brüssel aktiv, siehe: https://www.counterextremism.com/press/cep-statement-tech-companies'-transparency-reports-required-under-german-law-and-european-0

dokumentiert. Zum Beispiel stellte die amerikanische Regierung in ihrer neuen nationalen Risikoanalyse zur Goldwäsche und Terrorismusfinanzierung im Jahr 2018 heraus, dass dieses Risiko in Bezug auf mehrere Terrororganisationen besteht, insbesondere der Islamische Staat (IS), al-Qaida, al-Qaida auf der Arabischen Halbinsel (AQAP) und al-Shabaab.[12]

Zuletzt hat die Asia Pacific Group (APG) in Zusammenarbeit mit der Financial Action Task Force für den Nahen Osten und Nordafrika (MENA FATF) einen gemeinsamen Analyse- und Typologiebericht[13] zu diesem Thema veröffentlicht. Der Bericht macht deutlich, dass Finanziers des Terrorismus soziale Medien weiterhin hauptsächlich als Instrument nutzen, um Gelder einzuwerben und Informationen zu Finanztransfers, wie Kontonummern für Spenden oder Adressen von Geldwechselstuben und Hawallah-Büros zu verbreiten. Der Bericht hebt jedoch auch hervor, dass diese Aktivitäten „*in hohem Maße sichtbar sind und kein ausgeklügeltes Verständnis für die Verwendung von Verschlüsselungstools haben*“.[14] Diese Einschätzungen wird auch von anderen Experten geteilt.[15]

Risikoabwehr durch Plattformen anscheinend unzureichend

Zur Abwehr des Risikos, dass Plattformen der sozialen Medien zur Terrorfinanzierung missbraucht werden, stehen zwei grundlegende Mechanismen zur Verfügung. Einerseits könnten die Plattformen erkennen, dass Terrorfinanziers ihre Dienste missbrauchen, in dem sie aktive Profile unterhalten. Andererseits könnten die Plattformen erkennen, dass Aktivitäten auf ihren Plattformen ablaufen, die der Finanzierung des Terrorismus dienen. Beim zweiten Mechanismus ist wichtig, dass Plattformen ihre Beobachtungen der ablaufenden Aktivitäten mittels ihrer Nutzungsbedingungen auf solche Aktivitäten hin fokussieren. CEP hat diese beiden Mechanismen im Januar und März 2020 stichprobenartig getestet.

Aufgrund des relativ offenen Vorgehens bei diesen Aktivitäten sollte ihre Aufdeckung sowohl für Staatsanwälte als auch für Plattformanbieter keine großen Herausforderungen darstellen. Leider scheinen hier jedoch auf Seiten der Plattformbetreiben noch einige wichtige Lücken zu bestehen. CEP unternahm im Januar 2020 eine rudimentäre Suche, welche sie ausschließlich auf Personen und Organisationen konzentrierte, die an der Finanzierung des Terrorismus beteiligt sind und vom Sicherheitsrat der Vereinten Nationen auf seiner ISIL- und Al-Qaida Sanktionsliste stehen und auf der Liste eindeutig als Finanziers des Terrorismus identifiziert wurden.

Die ISIL & al-Qaida Sanktionliste des Sicherheitsrates der Vereinten Nationen wird durch das ISIL & al-Qaida Sanktionskomitee des Sicherheitsrates verwaltet.[16] Individuen und Organisationen werden nur dann auf dieser Liste aufgeführt, wenn im Konsens aller 15 Mitglieder des Sicherheitsrates beschlossen wurde, dass sie Teil des globalen ISIL oder al-

[12] United States of America Treasury, National Terrorist Financing Risk Assessment 2018, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf
[13] Als Typologien werden im Finanzsektor Betrugs- und Missbrauchsschemata bezeichnet. Diese Schemata werden verwendet, um die Abwehrmechanismen im Finanzsektor fortwährend weiter zu entwickeln und zu justieren.
[14] APG/MENA FATF, Social Media and Terrorism Financing, Januar 2019, Seite 6, http://www.apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142
[15] Siehe zum Beispiel: The Camstoll Group, Use of Social Media by Terrorist Fundraisers & Financers, April 2016, https://www.camstoll.com/wp-content/uploads/2016/04/Social-Media-Report-4.22.16.pdf
[16] https://www.un.org/securitycouncil/sanctions/1267

Qaida Netzwerkes sind und eine weltweite Gefahr darstellen.[17] Individuen und Organisationen auf dieser Liste unterliegen drei Sanktionsbeschränkungen: totale und globale Finanzsanktionen, ein totales und globales Reiseverbot, ein totales und globales Waffenembargo.[18]

Da die Liste Teil des globalen Anti-Terror Sanktionsregimes des Sicherheitsrates ist, welches nach Kapitel VII der Charter der Vereinten Nationen verabschiedet wurde, ist die Liste rechtlich verbindlich für alle Mitgliedsstaaten der Vereinten Nationen.[19] Diese sind dazu aufgerufen, die vereinbarten Sanktionen gegen die auf dieser Liste befindlichen Personen und Organisationen umzusetzen. Die Mitgliedstaaten müssen auch sicherstellen, dass Wirtschaftsunternehmen in ihrer Jurisdiktion diese Sanktionen nicht umgehen und wissentlich oder durch nicht-Wissen über die Inhalte Sanktionsbestimmungen den sanktionierten Personen und Organisationen Leistungen bereitstellen.[20] Damit stellt diese Liste die einzige Liste terroristischer Personen und Organisationen dar, welche den Konsens der Weltgemeinschaft abbildet und zweifelsfrei von allen Mitgliedsstaaten der Vereinten Nationen anerkannten Bereich des globalen Terrorismus verbindlich definiert.[21]

Im Januar 2020 extrahierte CEP aus dieser Sanktionsliste nur diejenigen Individuen, welche explizit mit der Finanzierung des Terrorismus in Verbindung gebracht werden und die Organisationen, auf der Liste, welche als terroristische Hilfsorganisationen ausgewiesen werden. Für diese Gruppe von Individuen und Organisationen wurde geprüft, ob sie möglicherweise aktive Profile auf verschiedenen globalen Plattformen unterhalten. CEP verwendete für diese einfache Internetsuche ausschließlich die Identifikationsinformationen, welche auf der Sanktionsliste des Sicherheitsrates der Vereinten Nationen öffentlich erhältlich sind. CEP entschied sich bewusst dazu, keine spezielle Suchtechnologie, wie z.B. die CEP-eGLYPH-Software[22] einzusetzen, um sicher zu stellen, dass das Erkennen von eventuellen Accounts ohne technischen Aufwand der Plattformbetreiber möglich ist.

Trotz dieser Beschränkungen auf eine kleine Anzahl von Fällen der weltweit durch den Sicherheitsrat bekannt gemachten Financiers des Terrorismus und einfachste technische Suchmechanismen fanden die Mitarbeiter von CEP in mehreren Fällen anscheinend aktive Accounts dieser auf der öffentlichen Sanktionsliste des Sicherheitsrates ausgewiesenen Terrorismusfinanziers.[23] Nach der Veröffentlichung der CEP Presseerklärung im Januar 2020[24] waren ab Mitte Februar 2020 die CEP auf Facebook erkannten Accounts nicht mehr erreichbar. YouTube sperrte bis Ende März 2020 eines der von CEP bei der Internetsuche erkannten und in seiner Presseerklärung veröffentlichten Videos. Die anderen

[17] https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/guidelines_of_the_committee_for_the_conduct_of_its_work_0.pdf, Seite 2.
[18] https://www.un.org/securitycouncil/sanctions/1267#sanction_measures
[19] https://www.un.org/securitycouncil/sanctions/1267#background_info
[20] https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/eot_assets_freeze_-_english.pdf
[21] Die Sanktionsliste ist hier erhältlich: https://scsanctions.un.org/r/?keywords=al-qaida
[22] https://www.counterextremism.com/german/eglyph-extremismus-im-netz-bekämpfen
[23] Abgleich der öffentlichen Indentifikationsinformationen der Individuen und Organisationen auf der Sanktionsliste des Sicherheitsrates der Vereinten Nationen mit den auf den Profilen öffentlich angegebenen Informationen.
[24] Counter Extremism Project, U.N.-Designated Individuals Maintain Social Media Presence, 22. Januar 2020, https://www.counterextremism.com/blog/un-designated-individuals-maintain-social-media-presence.

Plattformbetreiber zeigten bis zur Verfassung dieses Berichtes Ende März 2020 keine Reaktion.

Die internen Abwehrmechanismen der Plattformanbieter gegen den Missbrauch ihrer Dienste zur Finanzierung des Terrorismus scheinen daher noch nicht ausreichend auf dieses Thema ausgerichtet zu sein.

Eines der zentralen Instrumente der Industrie für die Moderation des Inhaltes von sozialen Medien sind die Nutzungsbedingungen der jeweiligen Plattform. Diese setzen wichtige thematische Prioritäten für die Moderation der Plattformbetreiber. Hier scheint es ebenfalls wichtige Lücken zu geben. In einem Bericht des Royal United Services Institute (RUSI) im Auftrag des GIFCT Global Research Network on Terrorism and Technology wurde 2019 dargestellt, dass in den Nutzungsbedingungen auf mehreren wichtigen Plattformen die Frage der Terrorismusfinanzierung nicht explizit erwähnt wurde.[25] Damit besteht die Gefahr, dass die Moderation der Inhalt auf den jeweiligen Plattformen durch die Betreiber eine spezifische Suche nach Inhalten in Bezug auf Finanzierungsaktivitäten nicht einschließt, zumindest jedoch keine Priorität darstellt.

Eine Überprüfung der Nutzungsbedingungen der größten globalen Plattformen, ergab, dass noch im März 2020 dieses Problem von den jeweiligen Plattformbetreibern nicht behoben und die Formulierungen ihrer Nutzungsbedingungen nicht angepasst wurden.[26] Das dies auch bei globalen Plattformen möglich ist, zeigt z.B. Twitter. Die Plattform schließt die Finanzierung des Terrorismus in seinen Nutzungsbedingungen explizit aus.[27] Damit ist leider festzustellen, dass einige globale Plattformen weiterhin wichtige Impulse ihrer Partner zu diesem Thema nicht umzusetzen scheinen.

Mit ein speziellem Missbrauchsrisiko sehen sich Crowdfunding-Webseiten konfrontiert. Diese sind für die Einwerbung von Geldern und Spenden technisch konzipiert. Auch dieses Risiko ist nicht neu. Bereits im Jahr 2015 wies die Europäische Wertpapier- und Marktaufsichtsbehörde auf das Risiko hin, dass Crowdfunding-Plattformen im Investmentbereich zur Finanzierung des Terrorismus missbraucht werden könnten, insbesondere *„wenn Plattformen nur eine begrenzte oder keine Due Diligence Prüfungen[28] für*

[25] Tom Keatinge, Florence Keen, Social Media and Terrorism Financing. What are the Vulnerabilities and How Could Public and Private Sector Collaborate Better? Global Research Network on Terrorism and Technology: Paper No. 10, Royal United Services Institute 2019, Seite 13f. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.

[26] Es wurden folgende Nutzungsbedingungen von CEP überprüft:
https://www.facebook.com/communitystandards/dangerous_individuals_organizations
Bemerkenswert ist, dass während die Nutzungsbedingungen von Facebook Finanzierung des Terrorismus nicht erwähnen, schließen sie jedoch Geldwäsche explizit aus:
https://www.facebook.com/communitystandards/fraud_deception
https://help.instagram.com/477434105621119
https://support.google.com/youtube/answer/9229472?hl=en&ref_topic=9282436
https://www.tumblr.com/policy/en/community

27 https://help.twitter.com/en/rules-and-policies/violent-groups

[28] Due Dilligence-Prüfungen sind Hintergrundrecherchen zu potenziellen Geschäftspartnern, welche vor dem Abschluss des Geschäftes veranlasst werden, um sicher zu stellen, dass alle möglichen Risiken erkannt und weitgehend ausgeschlossen werden, um u.a. Betrug und Missbrauch zu verhindern. Dabei wird u.a. überprüft, ob Geschäftspartner möglicherweise auf nationalen oder internationalen Sanktionslisten stehen durch einen Abgleich der Indentifikationsinformationen des Geschäftspartners mit den Informationen auf den jeweiligen Sanktionslisten.

Projektinhaber und ihre Projekte durchführen". [29] In diesem Zusammenhang ist insbesondere der Missbrauch von Crowdfunding-Plattformen von vermeintlichen gemeinnützigen Organisationen zu erwähnen, welche unter Vorgabe angeblicher humanitärer Aktivitäten Spenden für Terrororganisationen sammeln.

Der Missbrauch gemeinnütziger Spenden zur Finanzierung des Terrorismus ist einer der zentralen Finanzierungsströme für viele terroristische Organisationen. [30] Mehrere Fälle des Missbrauchs von Crowdfunding-Websites für mutmaßliche wohltätige Zwecke, von denen letztendlich terroristische Gruppen profitierten, wurden in den letzten Jahren von den Aufsichtsbehörden dokumentiert.[31] Die besondere Herausforderung für Aufsichtsbehörden und Ermittler ist der Mangel an Informationen auf den Plattformen über die Organisatoren solchen Kampagnen.[32] Dies behindert die Ermittlungen erheblich. Auch für diese Kategorie von Plattformanbietern scheinen sich die Nutzungsbedingungen nicht konsequent auf das Risiko eines Missbrauchs für die Terrorismusfinanzierung zu konzentrieren und signifikante Lücken aufzuweisen.

CEP führte im März 2020 eine Überprüfung der aktuellen Nutzungsbedingungen einiger der weltweit größten Crowdfunding Webseiten durch. Dabei stellte sich heraus, dass einige das Risiko ausschließlich auf die Nutzer abwälzten und diese lediglich aufforderten, das bestehende Recht ihres Heimatlandes einzuhalten.[33] Einige Plattformen erklärten, dass sie keine Nutzer zulassen, welche einen terroristischen Hintergrund haben oder aufgrund terroristischer Vergehen verurteilt wurden.[34] Dies deckt sich mit den Erkenntnissen des RUSI-Berichtes von 2019.[35] Daher scheint es auch in diesem Bereich bislang scheinbar zu keiner Verbesserung der Abwehrmechanismen gekommen zu sein.

---

[29] European Securities and Markets Authority, Questions and Answers. Investment-based crowdfunding: money laundering/terrorist financing, ESMA/2015/1005, 1 July 2015, Seite 4. https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2015_1005_qa_crowdfunding_money_laundering_and_terrorist_financing.pdf

[30] Empfehlung 8 zur Abwehr vonTerrorismusfinanzierung und Finanzierung der Proliferation der Financial Action Task Force (FATF), dem globalen Regulierungsgremium der globalen Finanzwirtschaft, hebt dieses Risiko besonders hervor. Die FATF hat schon 2014 einen ausführlichen Bericht zu diesem Thema veröffentlicht, siehe: FATF, Risk of Terrorist Abuse in Non-Profit Organisations, 2014, https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf

[31] Siehe: APG/MENA FATF, Social Media and Terrorism Financing, January 2019, Seite 11f, http://www.apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142

[32] Siehe: Alexandra Posadzki, Hard to identify crowdfunding platforms financing terrorism. The Canadian Press, 18 May 2017, https://www.thestar.com/business/2017/05/18/hard-to-identify-crowdfunding-platforms-financing-terrorism.html

[33] Siehe:
https://www.kickstarter.com/terms-of-use?ref=global-footer
https://www.indiegogo.com/about/terms?utm_source=learn&utm_medium=referral&utm_campaign=ent-trustandsafety&utm_content=bodylink
https://www.countable.us/about/community-guidelines?utm_source=causes&utm_content=tos.

[34] Siehe:
https://www.patreon.com/policy/guidelines
https://www.gofundme.com/terms

[35] Tom Keatinge, Florence Keen, Social Media and Terrorism Financing. What are the Vulnerabilities and How Could Public and Private Sector Collaborate Better? Global Research Network on Terrorism and Technology: Paper No. 10, Royal United Services Institute 2019, Seite 14f. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.

Zusammenfassung

Es kann nach dem aktuellen Sachstand kann nicht davon ausgegangen werden, dass gegenwärtig die internen Abwehrmechanismen der verschiedenen globalen Plattformen einen ausreichenden Schutz vor dem Missbrauch dieser Dienste zur Terrorismusfinanzierung bieten. Daher ist es wichtig, dass die Plattformbetreiber weitere Maßnahmen ergreifen, um intern die verschiedenen Missbrauchsrisiken zur Terrorismusfinanzierung besser zu verstehen. Weiterhin kann auch im Bereich staatlicher Regulierungen noch Optimierungen vorgenommen werden.

Ein interessanter Vorschlag von Tom Keatinge und Florence Keen, den Autoren des RUSI-Berichtes von 2019, ist auf den jeweiligen Terrorismussanktionslisten auch Informationen bzgl. der Präsenz der sanktionierten Gruppierungen und Individuen im Internet und auf den sozialen Medien einzufügen. Dies könnte u.a. folgende Informationen betreffen: E-Mail-Adressen, IP-Adressen und Account-Informationen auf den sozialen Medien. Natürlich können diese Informationen durch die betroffenen Nutzer relativ leicht verändert werden, sie würden jedoch wichtige Ersthinweise darstellen, die für die internen Überprüfungen der Plattformbetreiber verwendet werden könnten.[36] Der Sicherheitsrat der Vereinten Nationen forderte in seiner jüngsten Resolution zur Finanzierung des Terrorismus *„wirksame Partnerschaften mit dem Privatsektor, darunter […], Internet-Unternehmen und den sozialen Medien“*,[37] um dieser Bedrohung entgegenzuwirken.

Aufgrund der globalen Reichweite der führenden Plattformen unabdingbar, dass Plattformen pro-aktive Maßnahmen ergreifen, um den Missbrauch ihrer Dienste zur Finanzierung des Terrorismus zu verhindern. Das aktuelle System, welches anscheinend darauf beruht, dass kleine Organisationen wie CEP einen solchen Missbrauch durch die weltweit führenden und durch den Sicherheitsrat der Vereinten Nationen öffentlich identifizierten Finanziers des globalen Terrorismus entdecken und öffentlich anmerken, erscheint keine ausreichend effektive Abwehrmaßnahme.

Weiterhin scheint eine Anpassung der Benutzerrichtlinien der Plattformen als erster wesentlicher Schritt unabdingbar und ist mittlerweile eine längst überfällige Maßnahme. Terrorismusfinanzierung ist die Basis jeglichen terroristischen Handelns. Daher sollte die Industrie in ihren jeweiligen Nutzungsbedingungen klar zum Ausdruck bringen, dass ihre Plattformen für solche Aktivitäten nicht offen sind. Eine klar formulierte Ausschließung solcher Aktivitäten in den Nutzungsbedingungen wäre wichtig, um die internen Abwehrsysteme auf diesen Missbrauch hin zu fokussieren. Dies gilt insbesondere für die Nutzungsbedingungen von Crowdfunding Plattformen, da diese aufgrund ihrer Struktur einem besonderen Risiko unterliegen als potentielles Instrument der Spendengenerierung für terroristische Gruppierungen missbraucht zu werden.

[36] Tom Keatinge, Florence Keen, Social Media and Terrorism Financing. What are the Vulnerabilities and How Could Public and Private Sector Collaborate Better? Global Research Network on Terrorism and Technology: Paper No. 10, Royal United Services Institute 2019, Seite 17. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf
[37] Resolution 2462 (2019), Paragraph. 22, https://www.un.org/depts/german/sr/sr_19/sr2462.pdf