CEP POLICY PAPER

Financing of Terrorism and Social Media Platforms

April 2020

Dr. Hans-Jakob Schindler

COUNTER EXTREMISM PROJECT

COUNTER EXTREMISM PROJECT

About CEP and the Author

The Counter Extremism Project (CEP) is a non-profit, non-partisan international organization that aims to counter the threat of extremist ideologies and to strengthen pluralistic-democratic forces. CEP deals with extremism in all forms – including Islamist extremism/terrorism as well as right-wing and left-wing extremism/terrorism. To this end, CEP exerts pressure on financial and material support networks of extremist and terrorist organizations through its own research and studies, works against extremist and terrorist narratives and their online recruitment tactics, develops good practices for the reintegration of extremists and terrorists, and promotes effective regulations and laws.

In addition to offices in the United States, CEP has an office and a separate legal entity, Counter Extremism Project Germany gGmbH, in Berlin, and maintains a representation in Brussels. CEP's activities are led by an international group of former politicians, senior government officials and diplomats. CEP supports policymakers to develop laws and regulations to effectively prevent and combat extremism and terrorism, particularly in the area of combating terrorist financing.

More information can be found here: www.counterextremism.com/german.

Dr. Hans-Jakob Schindler is Senior Director at CEP and former Coordinator of the ISIL, al-Qaida and Taliban Monitoring Team of the United Nations Security Council.

If you have any questions relating to this policy paper, please contact **Marco Macori**, CEP Research Fellow: Email: mmacori@counterextremism.com; Phone: +49 30 300 149 3369

Financing of terrorism and social media platforms

In January and March 2020, the Counter Extremism Project (CEP) conducted a study to evaluate the current defense mechanisms of large social media platforms against the misuse of their services by financiers of international terrorism or for the financing of terrorism. This involved two steps. First, CEP tested whether major financiers of al-Qaida and the Islamic State in Iraq and the Levant (ISIL), as identified by the United Nations Security Council, are able to maintain profiles on large platforms where they could possibly continue their activities via social media. In January 2020, CEP found that around a dozen of the most notorious financiers apparently continued to maintain social media profiles.

Secondly, CEP examined the community standards[1] of global social media platforms. In 2019 a report by the Global Research Network on Terrorism and Technology, which is part of the Global Internet Forum to Counter Terrorism (GIFCT), highlighted that these community standards have gaps and do not explicitly exclude terrorist financing.[2] CEP reviewed these

[1] Depending on the platform, these are referred to differently as “Community Standards”, “Rules” or “Terms of Service” and determine which content is tolerated on the respective platform and which is not.
[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

guidelines in March 2020, and saw no overall improvement compared to the situation described in the research network's 2019 report. Given that a company's community standards reflect its content moderation priorities of each platform, the lack of improvement indicates that social media platforms appear to not prioritize protecting their sites against terrorist financing.

The misuse of social media and other internet services by terrorist organizations, including for financing activities, has been regularly discussed in the media and among experts. This issue became particularly prevalent since the emergence of ISIL from 2014 onwards. For the last few years, major platforms have been trying to mitigate the reputational damage caused by this misuse by publicly announcing a range of counter measures and initiatives. For example, in 2017, Facebook, Microsoft, Google, and Twitter founded GIFCT, which aims to disrupt the misuse of these platforms by terrorists.[3] As part of this work, GIFCT also established the Global Research Network on Terrorism and Technology. The network is tasked with developing academic research and providing policy recommendations to help prevent terrorists' misuse of technology.[4] A part of this work concerns the financing of terrorism through internet services, including social media. The 2019 report of the GIFCT-supported research network contains several basic recommendations on how platforms could strengthen their defensive mechanisms against the financing of terrorism.[5]

The study conducted by CEP in January and March 2020 indicated that there is still room for improvement in social media platforms' defense mechanisms against the misuse of their sites by terrorist financiers and against the misuse of their services to finance terrorism.

CEP has two fundamental recommendations to improve the defensive mechanisms of platforms:

A) **Since terrorist financing is the basis of any terrorist operation, the tech industry should proactively counter the risk that their services are misused for this purpose and search for profiles and accounts of terror financiers on their platforms.** A system that seems to depend on relatively small organizations like CEP to manually locate potential social media profiles of the most notorious global terrorist financiers and notify the respective companies is unlikely effective to prevent such misuse. Companies, especially those with a worldwide user base, have to act proactively and more effectively.

B) **Social media platforms should revise their community standards, as suggested in the Global Research Network on Terrorism and Technology's 2019 report, and subsequently increase awareness of terrorism financing risks among their internal content monitoring and moderation teams.** The financiers of international terrorism need the broadest possible public reach so that they can connect to potential donors and supporters. Financing terrorism should therefore be explicitly addressed and prohibited in the social media platforms' community standards. This is particularly important also for crowdfunding platforms.

and Technology: Paper No. 10, Royal United Services Institute 2019. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.

[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, page 17f. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.

COUNTER EXTREMISM PROJECT

Risk analysis

The emergence of social media has become a central part of terrorist groups' strategic capabilities. Since the rise of ISIL, numerous reports have been published warning of the group's ongoing abuse of social media.[6] ISIL and other terrorist organizations use this new media landscape very skillfully to disseminate, radicalize, recruit, operationally communicate, and disseminate terrorist knowledge and skills.

Since 2014, the ISIL, Al-Qaida and Taliban Monitoring Team of the United Nations Security Council have documented this misuse.[7] On behalf of the Security Council, the team monitors terrorist groups and individuals belonging to the global networks of ISIL, al-Qaida, and the Taliban and advises both the Security Council and the U.N. Secretary General on global countermeasures to address the risks posed by these groups.

Some progress has been made in combating terrorists' misuse of social media. For example, several platforms cooperated with EUROPOL on the 16th Referral Action Day, which was coordinated by the European Union Internet Referral Unit.[8] This progress was in part achieved after public pressure from civil society,[9] as well as action by governments,[10] including the European Union.[11]

The specific misuse of social media by the financiers of terrorism in recent years has received less public attention. However, the continuing misuse of internet and social media services by terrorist organizations to finance their activities has been regularly documented by various experts and governments. For instance, in its updated national risk assessment concerning financing of terrorism, the U.S. government highlighted in 2018 that cases of financing activities via social media were observed across multiple terrorist organizations, in particularly ISIL, al-Qaida, al-Qaida in the Arabian Peninsula (AQAP), and al-Shabaab.[12]

[6] See for example: S/2014/815 from 14 November 2014, paragrahs 27 and 90, https://www.undocs.org/S/2014/815.
[7] S/2014/770 from 29 October 2014, paragraphs 17 – 22. https://www.undocs.org/S/2014/770
The reports of the Monitoring Team can be found here:
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 November 2019, https://www.europol.europa.eu/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda.
[9] For example, the Digital Disruption Campaign of the Counter Extremism Projects (CEP), https://www.counterextremism.com/digital-disruption
[10] In this context, the Network Enforcement Act (NetzDG), in force in Germany since 2018 played a significant role. NetzDG was the world's first attempt by a western state to introduce basic rules for social media platforms. In December 2018, CEP published a first detailed study on the effects of the NetzDG, see: 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] A new regulation of the European Union focusing on the removal of terrorist content online is in the last stages of the adoption process. See: http://www.europarl.europa.eu/legislative-train/theme-civil-liberties-justice-and-home-affairs-libe/file-preventing-the-dissemination-of-terrorist-content-online. CEP actively supports this process in Brussels, see: https://www.counterextremism.com/press/cep-statement-tech-companies'-transparency-reports-required-under-german-law-and-european-0
[12] United States of America Treasury, National Terrorist Financing Risk Assessment 2018, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf

The Asia Pacific Group (APG), in cooperation with the Financial Action Task Force for the Middle East and North Africa (MENA FATF), recently published a joint analysis and typology report on this topic.[13] The report highlights that terrorist financiers continue to use social media primarily as a tool to raise funds and disseminate information on financial transfers, such as account numbers for donations or addresses of currency exchange offices and *hawala* (informal money transfer establishments) offices. The report also emphasizes that these activities are conducted "highly visible, and without sophisticated understanding of computing and use of encryption tools."[14] This assessment is also shared by other experts.[15]

Defensive systems of social media platforms appear inadequate

Social media platforms can use two basic mechanisms to avert the risk of being misused for terrorist financing. Platforms can work to proactively identify terrorist financiers' social media profiles or accounts. Additionally, platforms can analyze patterns of activities that indicate that the financing of terrorism is ongoing. For this second mechanism to be effective, it is crucial that companies specifically focus their content moderation on this topic. The community standards of the respective platforms play a central role in this regard, as they outline the companies' priorities for content monitoring. In January and March 2020, CEP conducted a study to evaluate these two mechanisms.

Financing of terrorism via social media is often conducted in a relatively open manner, without using sophisticated encryption tools. It should not be a challenge for global social media platforms to detect such activities. Unfortunately, however, there still seem to be some important gaps in the defensive mechanisms of the platform operators. In January 2020, CEP carried out a rudimentary search that focused only on individuals and organizations involved in terrorist financing, which are listed on the public United Nations Security Council's ISIL and al-Qaida sanctions list and for whom the sanctions list clearly indicates that they are financiers of terrorism.

This particular sanctions list is administered by the Security Council's ISIL & al-Qaida Sanctions Committee.[16] Individuals and organizations will only appear on this list if all 15 members of the Security Council agree that they are part of the global ISIL or al-Qaida networks and pose a worldwide threat.[17] Individuals and organizations on this list are subject to three sanction measures: a total and global asset freeze, a total and global travel ban, and a total and global arms embargo.[18]

Since this sanctions list is part of the Security Council's global anti-terror sanctions regime, which was adopted in accordance with Chapter VII of the U.N. Charter, the list is legally binding for all member states of the United Nations.[19] It is the responsibility of the member states to

[13] Fraud and abuse schemes are referred to as typologies in the financial sector. These typologies are used to develop, adjust and improve compliance mechanisms in the financial sector.
[14] APG/MENA FATF, Social Media and Terrorism Financing, January 2019, page 6, http://www.apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142
[15] See for example: 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
[17]https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/guidelines_of_the_committee_for_the_conduct_of_its_work_0.pdf, page 2
[18] https://www.un.org/securitycouncil/sanctions/1267#sanction_measures
[19] https://www.un.org/securitycouncil/sanctions/1267#background_info

implement the three sanction measures against the individuals and organizations on the list. Member states must also ensure that business entities in their jurisdiction do not circumvent these sanctions and that these businesses do not provide sanctioned individuals and organizations knowingly or unknowingly with goods or services that are prohibited by the three sanctions measures.[20] This global sanctions list is unique since it represents the consensus of the global community concerning which individuals or entities are considered terrorists. Therefore, this list, which is legally recognized by all member states of the United Nations, also acts as a global definition of what phenomena are considered terrorism.[21]

In January 2020, CEP identified those individuals from the list who were explicitly associated with the financing of terrorism, and only those organizations on the list that were identified as terrorist aid organizations. For this subgroup of individuals and entities, CEP checked whether they maintained potentially active profiles on different global social media platforms. In this simple internet search, CEP only used the identification information that is publicly available on the sanctions list of the United Nations Security Council. CEP deliberately decided not to use any special search technology, such as use CEP's eGLYPH software,[22] to ensure that any potential accounts could be identified without any technical effort on the part of the respective platform operators.

Despite limiting the search to only a small number of infamous terrorist financiers, which are publicly identified by the Security Council, and despite the technical limitations of the search methodology, CEP located accounts apparently belonging to or established in support of several of these terrorist financiers.[23] CEP published a press release concerning its findings in January 2020.[24] By mid-February 2020, the Facebook accounts that CEP had identified were no longer available. YouTube blocked one of the videos identified by CEP at the end of March 2020. The other platforms had no response at the time of writing this report at the end of March 2020.

It seems that the internal defensive mechanisms of the various platform providers against misuse of their services by international financiers of terrorism are not yet sufficiently focused on this issue. They apparently failed to internally recognize that some of the most well-known financiers of terrorism held potentially active profiles on their platforms.

One of the crucial guiding instruments for content moderation of social media platforms is their community standards. These set important thematic priorities for content monitoring and moderation by platform operators. These community standards appear to have significant gaps as far as countering the financing of terrorism is concerned. A 2019 report by the Royal United Services Institute (RUSI) on behalf of the GIFCT Global Research Network on Terrorism and Technology highlighted that the community standards of several major social media platforms

[20] https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/eot_assets_freeze_-_english.pdf
[21] The sanctions list can be found here: https://scsanctions.un.org/r/?keywords=al-qaida
[22] https://www.counterextremism.com/video/how-ceps-eglyph-technology-works
[23] Comparison of the public identification information of the individuals and organizations on the sanctions list of the United Nations Security Council with the information given publicly on the social media profiles.
[24] Counter Extremism Project, U.N.-Designated Individuals Maintain Social Media Presence, 22 January 2020, https://www.counterextremism.com/blog/un-designated-individuals-maintain-social-media-presence.

did not mention terrorism financing as an unacceptable activity.[25] Consequently, it is likely that content moderation and analysis of these platforms does not include specific searches for content relating to such financing activities, or at least, that such activities are not a priority for content moderators.

In March 2020, a review by CEP of the community standards of the largest global platforms showed that each platform operator did not yet resolve this problem – failing to adjust their community standards to clearly forbid terrorism financing activities since the issue was highlighted in 2019.[26] A clear focus on the issue of terrorism financing is possible for global platforms, as demonstrated by the community standards (termed "rules and policies") of Twitter. The platform explicitly excludes the financing of terrorism in its rules and policies.[27] Unfortunately, it seems that other major social media platforms did not implement the recommendations of the Global Research Network on Terrorism and Technology, the academic partner of GIFCT.

Crowdfunding websites are faced with a particular risk for misuse since these platforms are specifically designed for fundraising and to collect donations. The abuse of fundraising platforms for the financing of terrorism is also not a new problem. As early as 2015, the European Securities and Markets Authority pointed out that crowdfunding platforms in the investment sector could be misused to finance terrorism, especially if "platforms carry out limited or no due diligence[28] on project owners and their projects."[29] In this context, the misuse of crowdfunding platforms by non-profit organizations, which under the cover of alleged charitable work could collect donations for terrorist organizations, is an important risk.

The misuse of charitable donations to finance terrorism is an important funding stream for many terrorist organizations.[30] In recent years, several cases of the misuse of crowdfunding

[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, page 13f. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.
[26] CEP checked the following community standards:
https://www.facebook.com/communitystandards/dangerous_individuals_organizations
Interestingly, while Facebook's community standards do not mention financing of terrorism, they explicitly exclude money laundering: 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 diligence checks involve background research on potential business partners, which are initiated before the transaction is concluded to ensure that all possible risks are identified and largely excluded, e.g. to prevent fraud and abuse. This includes, among other issues, checks whether business partners are possibly sanctioned on national or international sanction lists by comparing the identification information of the business partner with the information provided on the respective sanction lists.
[29] European Securities and Markets Authority, Questions and Answers. Investment-based crowdfunding: money laundering/terrorist financing, ESMA/2015/1005, 1 July 2015, page 4. https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2015_1005_qa_crowdfunding_money_laundering_and_terrorist_financing.pdf
[30] Recommendation 8 concerning combating terrorist financing and financing of proliferation of the Financial Action Task Force (FATF), the regulatory body of the global financial industry, highlights this risk. Already in 2014 the FATF published a report on this issue, see: FATF, Risk of Terrorist Abuse in

websites for alleged charitable purposes that ultimately benefited terrorist groups, have been documented by regulators.[31] The particular challenge for regulators and investigators is the lack of information available on crowdfunding platforms concerning the organizers of such campaigns.[32] This significantly impedes investigations. Unfortunately, the community standards for this category of platform providers do not seem to consistently focus on the risk of the misuse of their services for the financing of terrorism.

In March 2020, CEP conducted a review of the current community standards of some of the world's largest crowdfunding websites. This audit revealed that some platforms merely passed the problem along to the users by simply asking them to comply with existing laws in their respective home countries.[33] This would mean that financiers of terrorism would have to self-identify as such to the platform moderators, which is very unlikely to ever be the case. Some platforms stated that they do not allow users who have a terrorist background or have been convicted of terrorist offenses.[34] However, it is not clear how platform moderators could identify and confirm that a user had such a background or had been convicted for such offences. These results confirm the findings of the RUSI report from 2019.[35] Currently, it seems that there has been no improvement of the defensive mechanisms of this category of platforms.

Social media platforms should strengthen their defense mechanisms

Given the results of CEP's analysis in January and March 2020, it is clear that the internal defense mechanisms of the various global social media platforms do not offer adequate protection against the misuse of their services for the financing of terrorism. Therefore, it is important that platform operators undertake further measures to better understand the various risks related to this issue. Furthermore, improvements could also be made by government regulators to support due diligence processes by social media companies.

Tom Keatinge and Florence Keen, the authors of the 2019 RUSI report, suggest that regulators should include information on sanctions lists concerning the activities of sanctioned groups and individuals on the internet and on social media. This could include the provision of the following information of sanctioned individuals and entities: email addresses, IP addresses, and social media account information. Of course, this information could be changed relatively

Non-Profit Organisations, 2014, https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf

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

[32] See: 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] See:
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] See:
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, page 14f. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.

easily by the sanctioned individuals and entities. However, such data could serve as important initial indicators which could be used for internal reviews and searches conducted by platform operators.[36] In its latest resolution concerning the combatting the financing of terrorism, the U.N. Security Council called on member states " to continue to establish effective partnerships with the private sector, including (…) internet and social media companies,"[37] to address this threat.

Given the global reach of leading social media services, it is crucial that platforms take proactive measures to prevent the misuse of their services for the financing of terrorism. The tech industry should proactively search for profiles and accounts of terror financiers on their platforms. The current system, which appears to require small organizations such as CEP to manually search for, identify, and notify misuse by the world's leading global terrorism financiers, even when they have already been publicly identified by the U.N. Security Council, does not appear to be a sufficiently effective mechanism.

Moreover, adjustments to the community standards of these platforms seems to be an essential first step and a long overdue measure. Terrorism financing is the basis of all terrorist activities. Therefore, the tech industry should clearly state in their respective community standards that their platforms are not open to such activities. A clearly formulated prohibition of such activities in the community standards is important in order to focus platforms' internal defensive systems on this type of abuse. This applies in particular to the community standards of crowdfunding platforms, because their services are at particular risk of being misused as a potential instrument to generate donations for terrorist groups and organizations.

[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, page 17, https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf

[37] Resolution 2462 (2019), paragraph. 22, https://undocs.org/en/S/RES/2462(2019)