United Nations A/HRC/49/NGO/137

General Assembly

Distr.: General
17 February 2022

English only

Human Rights Council
Forty-ninth session
28 February–1 April 2022
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Written statement* submitted by Human Rights Advocates Inc., a non-governmental organization in special consultative status

The Secretary-General has received the following written statement which is circulated in accordance with Economic and Social Council resolution 1996/31.

[7 February 2022]

* Issued as received, in the language of submission only. The views expressed in the present document do not necessarily reflect the views of the United Nations or its officials.

Countering Digital Financing for the Effort to Counter Terrorism

Since 1963, the international community has elaborated 19 international legal instruments to prevent terrorist acts through the UN, but there's been little mobility in the text that adequately covers the current evolvement of terrorism through specific language. Unchanging, however, is the desire for terrorist groups to acquire power.

Recent years of study in International Relations have provided scholars with the opportunity to distinguish power into two major categories: hard and soft power.(1) The former is most traditionally referenced by political spectators to measure hegemony: wars, sanctions, military force, military arms, nuclear weapons, etc. Hard power "is achieved through military threat or use," and "soft power works through the persuasive potency of ideas that foreigners find attractive."(1) Since the rise of technology, notably social media, the ability to spread soft power has multiplied exponentially.(1) Through the nexus of technology, the world is influenced by ideas much quicker, which, in turn, creates the ability to achieve ultimate hard power goals: buying weapons by militarized groups through financial backing that legitimizes their extremist efforts. Soft and hard power authority synergistically creates a much stronger front that attracts followers. Thus, the ability to gain both power in arms and power in influence has catastrophic potential.

Soft power seeks to achieve influence by building networks and communicating compelling narratives. Individual sources of soft power are manifold and varied, and thus have the ability to osmose subtly without liability.(1) As such, terrorist ideology has the capacity to seamlessly integrate into daily lives with a less forceful approach. In recent years, terrorist groups have used this approach in their social media campaigns that lure soldiers and financiers alike through the appeal of being a part of a "brethren."(2) This language appeals to individuals not by instilling fear or coerced threats but a welcome that appeals to those who want to be part of an ideological family that is bigger than themselves– feeding into the martyr mentality.

Even so, during the rise of terrorism, the UN and states have mostly narrowly focused on the hard power war against terrorism. Over the past decade, especially during Covid-19, illicit actors have increasingly diversified their financial portfolio to include virtual funding through their broad social media efforts to gain followers. The question of whether governments should require tech companies to conduct counterterrorism operations is politically important; yet, many companies have voluntarily made efforts to counter terrorism.(3) Even so, these reports are often not officiated by the government or the UN in their operations to shut down financing terrorism. For example, in 2018, Facebook removed 14.3 million pieces of content related to the Islamic State, al-Qaeda, and their affiliates, only 41,000 of which were flagged by external sources.(4) Funding exposes platforms such as PayPal, Venmo, and Western Union as attractive to such violent extremists. Digital payments crime is continuously expanding as it sophisticates with criminals' innovations of new types of malware.(3) Through social engineering and social media curation, recruitments to finance terrorist acts have only become easier with time. Terrorists have used digital payments to achieve money laundering or direct payment to finance terrorist attacks. Exemplified in the March 2018 conviction of the United States of America citizen Mohamed Elshinawy, the Islamic State received over $8,000 from supporters via PayPal. He achieved these finances ostensibly for sales of printers through his eBay account, as many others have through similar schemes.(4) It was confirmed that these funds were intended to support future operational attacks in the United States of America.

In the past decade, illicit actors have slowly but steadily diversified their funding sources by incorporating virtual assets known as cryptocurrencies.(5) Through cryptocurrency, there is the elimination of geographic limitations to transfer funds, the finality of settlement, lower transaction costs compared to other forms of payment, and the ability to verify transactions publicly. While cryptocurrency is used for legitimate, legal transactions, "it appeals to violent extremists because of its pseudonymity, varying oversight and regulatory requirements by country, convenience, and quick transfer speeds."(5) First responder situational awareness and recognition of illicit use of cryptocurrencies can largely prevent terrorist-related fundraising.(5)

In 1999, the INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM was adopted in recognition of the increasing issue of financial terrorism support, and yet the issue is more prevalent than ever. According to the recently updated report on the impact of the Covid-19 pandemic on terrorism:

"Most pandemic-related trends in the areas of terrorism and counter-terrorism have overlapped across regions. Terrorist groups have sought to exploit pandemic-related socio-economic grievances and political tensions (...) to expand their influence, drive their recruitment efforts, and undermine State authority. Terrorists and violent extremists have also sought to exploit pandemic-related sociocultural restrictions that have led people around the world to spend increasing time online by strengthening their efforts to spread propaganda, recruit, and radicalize via virtual platforms (including gaming platforms)."(6)

To adequately combat terrorism, the UN needs to prioritize the squashing of soft power efforts in order for terrorist groups to be unable to gain hard power traction. While this issue isn't region specific per se, it's apparent that this has been an issue in the United States of America, Afghanistan, the Syrian Arab Republic, Yemen, and the Russian Federation. There are three major areas that need to be administratively investigated through specific tactics and requirements: cryptocurrency, social media (Twitter, Facebook, Instagram, TikTok, YouTube, video game platforms, etc.), and digital banking services (PayPal, Venmo, Western Union, etc.). Although separate, they are interrelated and dependent upon one another in a terrorism financing scheme.

There needs to be more aggressive means to determine why the abuse of the named digital tools are more successful than ever, despite companies and states being aware of this strategy. All parties cooperating in this form of terrorist aid must be held accountable. Building on the International Convention for the Suppression of the Financing of Terrorism (1999) and Security Council resolution 1373 (2001), S/RES/2462 (2019) "call[s] on States to prevent and suppress the financing of terrorism," without a clear notion of how or the scope.(6)

Following this resolution, S/RES/2482 (2019), still does not adequately address online financing of terrorist activity, even with the Forty FATF Recommendations on Combating Money Laundering, and the Financing of Terrorism and Proliferation.(7) Adopted language that "urges" investigations is not specific nor strong enough to enforce both private and state compliance with regulating online activity on digital banking platforms, social media, and cryptocurrency in order to eradicate online terrorist financing. The use of these technological platforms is a means to violate human rights and, therefore, their misusage is a violation of human rights itself.

Recommendation to the Human Rights Council by Human Rights Advocates:

There needs to be stronger cooperation between digital services and their state government. the United Nations should adopt stricter resolution language that speaks directly to these major suspicious activities and specifically outlines the need for private tech companies to communicate with both their home countries and the UN in order to collaboratively combat terrorism. Digital monitoring needs to be implemented in tandem with public policy while still requesting that States hold terrorists, tech companies, and states accountable for their active role in allowing this type of activity. Specific language in the resolution will help further investigation and prosecution of responsible individuals. It will also allow the UN to hold accountable other non-state and state actors for either their complacency or sponsorship of terrorism.

---

1. Gray, C. (2011). (Rep.). Strategic Studies Institute, the United States of America Army War College. www.jstor.org/stable/resrep11431

2. AlSarayreh, Ata. (2019). How Isis Uses Social Media for Recruitment. https://www.cfc.forces.gc.ca/259/290/22/305/AlSarayreh.pdf

3. Fishman, Brian. (2019). Crossroads: Counter-terrorism and the Internet. https://tnsr.org/2019/02/crossroads-counter-terrorism-and-the-internet/
4. Adams, John. (2019). Behind Western Union's billion dollar war on fraud. https://www.americanbanker.com/payments/news/behind-western-unions-billion-dollar-war-on-fraud
5. Department of the United States of America Homeland Security. (2021). Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists. https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/119s_-_First_Responders_Toolbox_-_Identifying_and_Preventing_Illicit_Use_of_Cryptocurrency_by_Terrorists.pdf
6. The UN Security Council Counter-Terrorism Committee Executive Directorate. (2020). The Impact of The Covid-19 Pandemic on Terrorism, Counter-Terrorism, and Countering Violent Extremism. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Dec/cted_covid19_paper_dec_2021.pdf
7. Security Council Resolution 2482. (2019). Threats to international peace and security. http://unscr.com/en/resolutions/2482