Scientific Journal of Political Law Approaches

Scientific J. Pol. L. App., 2(2) (2025) 19-34
DOI: 10.22084/qjpla.2025.31386.1036

Bu-Ali Sina University

Imperatives for Strengthening Legal Capacities Regarding the Implementation of International Sanctions Against Technological Crimes Committed by Terrorists on Virtual Platforms

Peyman Namamian*

Associate Professor, Department of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran.

ABSTRACT: International sanctions against the commission of technological crimes by terrorists on virtual platforms constitute one of the complex and emerging challenges in international law, requiring a precise analysis and evaluation of the existing legal capacities in this area. Given the increasing technological threats and the growing use of the internet and virtual platforms to commit terrorist crimes, the international community is seeking strategies to address these threats and limit the activities of terrorists on virtual platforms. In this context, economic, financial, and trade sanctions against individuals directly or indirectly involved in the commission of technological terrorist crimes are recognized as an effective tool to counter these threats. However, several legal challenges exist regarding international sanctions, including difficulties in identifying and accurately assessing the commission of technological crimes by terrorists, coordination among states, methods of enforcing sanctions, and ensuring the protection of human rights during the implementation of these sanctions. These issues must be addressed in the development and implementation of an effective and comprehensive legal framework. In this regard, international organizations such as the United Nations, the European Union, and other member states are working to establish the necessary rules and guidelines for the effective imposition of sanctions against individuals and terrorist groups involved in technological crimes on virtual platforms. However, challenges such as a lack of transparency, consistency, and coordination in enforcing these sanctions still persist, necessitating enhanced international cooperation and a revision of the existing legal structure.

Review History:

Received: Oct. 06, 2024
Revised: Dec. 08, 2024
Accepted: Mar. 12, 2025
Available Online: Mar. 19, 2025

Keywords:

Technological Crimes by Terrorists
Virtual Platforms
International Sanctions
Virtual Platform Security.

HOW TO CITE THIS ARTICLE

Namamian, P., (2025). Imperatives for Strengthening Legal Capacities Regarding the Implementation of International Sanctions Against Technological Crimes Committed by Terrorists on Virtual Platforms, *Scientific Journal of Political Law Approaches*, *2*(2), 19-34. https://doi.org/10.22084/qjpla.2025.31386.1036

Online ISSN 3092-6394

*Corresponding author's email: p-namamian@araku.ac.ir

نشریه علمی رویکردهای حقوق سیاسی

نشریه علمی رویکردهای حقوق سیاسی، دوره ۲، شماره ۲، پاییز و زمستان ۱۴۰۳، صفحات ۱۹ تا ۳۴
(مقاله پژوهشی)
DOI: 10.22084/qjpla.2025.31386.1036

بایسته‌های تقویت ظرفیت‌های حقوقی ناظر به اتخاذ سیاست اجرای تحریم‌های بین‌المللی علیه ارتکاب جنایات فناورانه از سوی تروریست‌ها در سکوهای مجازی

پیمان نمامیان*

دانشیار، گروه حقوق کیفری و جرم شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران.

خلاصه: تحریم‌های بین‌المللی علیه ارتکاب جنایات فناورانه توسط تروریست‌ها در سکوهای مجازی، یکی از چالش‌های پیچیده و نوظهور در حقوق بین‌الملل به‌شمار می‌آید که تحلیل و ارزیابی دقیق ظرفیت‌های حقوقی موجود در این حوزه امری ضروری است. با توجه به گسترش روزافزون تهدیدات فناورانه و استفاده فزاینده از اینترنت و سکوهای مجازی برای ارتکاب جنایات تروریستی، جامعه بین‌المللی به دنبال راهکارهایی برای مقابله با این تهدیدات و محدودسازی فعالیت‌های تروریست‌ها در سکوهای مجازی است. در این زمینه، تحریم‌های بین‌المللی علیه اشخاصی که به‌طور مستقیم یا غیرمستقیم در ارتکاب جنایات فناورانه تروریستی نقش دارند، به‌عنوان ابزار مؤثری برای مقابله با این تهدیدات شناخته می‌شود. با این حال، چالش‌های حقوقی متعددی در زمینه تحریم‌های بین‌المللی وجود دارد؛ از جمله دشواری‌های شناسایی و ارزیابی دقیق ارتکاب جنایات فناورانه توسط تروریست‌ها، هماهنگی میان کشورها، شیوه‌های اعمال تحریم‌ها و رعایت حقوق بشر در فرآیند اجرای این تحریم‌ها. این مسائل باید در تدوین و اجرای یک چارچوب حقوقی مؤثر و جامع مورد توجه قرار گیرند. در این راستا، نهادهای بین‌المللی هم‌چون سازمان ملل متحد، اتحادیه اروپا و دیگر کشورهای عضو، در تلاشند تا قواعد و دستورالعمل‌های لازم برای اعمال تحریم‌های مؤثر علیه افراد و گروه‌های تروریستی و جنایات فناورانه آنان در سکوهای مجازی تدوین کنند. با این حال، هنوز چالش‌هایی همچون فقدان شفافیت، وحدت رویه و هماهنگی در اجرای این تحریم‌ها وجود دارد که ایجاب می‌کند همکاری‌های بین‌المللی تقویت شده و ساختار حقوقی موجود مورد بازنگری قرار گیرد.

تاریخچه داوری:
دریافت: ۱۴۰۳/۰۷/۱۵
بازنگری: ۱۴۰۳/۰۹/۱۸
پذیرش: ۱۴۰۳/۱۲/۲۲
ارائه آنلاین: ۱۴۰۳/۱۲/۲۹

کلمات کلیدی:
جنایات فناورانه تروریست‌ها
سکوهای مجازی
تحریم‌های بین‌المللی
امنیت سکوهای مجازی

۱- مقدمه

بهره‌گیری از سکوهای مجازی به‌عنوان ابزارهایی برای گسترش ایدئولوژی‌های تروریستی و تأمین منابع مالی، تهدیدات جدی برای امنیت جهانی ایجاد کرده است (Passalacqua, 2024, p 6). به‌طور خاص، گسترش فعالیت‌های تروریستی در سکوهای مجازی تهدیدات پیچیده‌ای را برای امنیت جهانی به‌وجود آورده است. تروریست‌ها از سکوهای مجازی به‌منظور تبلیغ ایدئولوژی‌های افراطی، جذب نیرو و تأمین منابع مالی خود بهره‌برداری می‌کنند. این فعالیت‌ها به‌دلیل عدم شناخت و سرعت بالای فضای مجازی، شناسایی و سرکوب آن ها را دشوار می‌سازد (Alavi, 2024, p 15-17). از این‌رو، تحریم‌های بین‌المللی به‌عنوان ابزاری مؤثر برای محدودیت منابع تروریست‌ها طراحی شده‌اند که مشتمل بر انسداد دارایی‌ها، محدودیت‌های ورود و خروج از قلمرو حاکمیتی کشورها و غیره می‌شود.

ارتکاب جنایات فناورانه از سوی تروریست‌ها در سکوهای مجازی به‌ویژه با استفاده از فناوری‌های نوین مانند اینترنت، رمزارزها، شبکه‌های اجتماعی و ابزارهای هکری، تهدیدی جدی برای زیرساخت‌های حیاتی و امنیت جهانی به‌شمار می‌آید. تروریست‌ها از سکوهای مجازی به‌منظور گسترش افکار افراطی، جذب نیرو و تأمین مالی استفاده می‌کنند. به‌علاوه، این نوع از فعالیت‌های تروریستی می‌توانند به سرقت اطلاعات حساس یا تخریب داده‌ها منجر شوند (Kuzior et al., 2024, p 231-232). در این سکوها، تروریست‌ها از فناوری‌های نوینی هم‌چون پهپادها و رُبات‌ها برای انجام حملات بهره می‌برند. فضای تاریک اینترنت[1] نیز به‌عنوان بستری برای گسترش آموزش‌ها و فروش غیرقانونی سلاح‌ها شناخته می‌شود (Adel & Norouzifard, 2024, p 18-19).

* نویسنده عهده‌دار مکاتبات: p-namamian@araku.ac.ir

1. Dark Web

سرکوب این تهدیدات نیازمند همکاری جهانی، ایجاد قوانین جدید و نظارت دقیق بر سکوها است[۱]. تروریست‌ها از فناوری‌هایی چون اینترنت، شبکه‌های اجتماعی، نرم‌افزارهای هکری و پهپادها برای تبلیغ افراطی‌گری، جذب نیرو، تأمین مالی و ارتکاب فعالیت‌های تروریستی استفاده می‌کنند[۲]. به‌دلیل عدم شناخت و سرعت فضای مجازی، سرکوب این تهدیدات دشوار است. به‌همین جهت، تحریم‌های بین‌المللی و چارچوب‌های حقوقی در سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی ضروری است. سازمان‌های بین‌المللی از جمله شورای امنیت سازمان ملل متحد با تحریم‌های مالی و محدودیت‌های ورود و خروج از قلمرو حاکمیتی، کشورهای عضو را ملزم به کاهش تهدیدات می‌کنند (Bogdanova, 2022, p 71-73).

چالش‌های حقوقی مانند تفاوت‌های مقررات داخلی کشورها، تضاد با حقوق بشر و نیاز به هماهنگی بین‌المللی برای نظارت بر سکوها همچنان وجود دارد. سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی نیازمند رویکردی چندجانبه، همکاری‌های قضائی و حفظ تعادل میان امنیت و حقوق بشر است (Afina et al., 2024, p 36-37). از این‌رو، برای سرکوب این تهدیدات، ضرورت هماهنگی بین‌المللی، تبادل اطلاعات و تقویت چارچوب‌های قانونی روزآمد و جامع امری انکارناپذیر است. به‌علاوه، قطعنامه‌های شورای امنیت ملل متحد، کشورهای عضو را ملزم به اتخاذ تدابیر مؤثر برای سرکوب فناوری‌های تروریستی کرده است (Pytlak & Lad, 2024, p 1)[۳]. در عین حال، اتحادیه اروپا و ایالات متحده از سال ۲۰۱۹ تحریم‌های هدفمند علیه تروریست‌ها اعمال کرده‌اند (Giumelli et al., 2021, p 11-12) و در سال ۲۰۲۴، آمریکا تحریم‌هایی علیه «گروه هکری ارتش سایبری روسیه»[۴] اعمال نمود(Antoniuk, 2024, p 1)[۵].

این پژوهش با سنجش کاربرد و اجرای تحریم‌های بین‌المللی و ابزارهای حقوقی بین‌المللی در سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی برای تعقیب کیفری تروریست‌ها، و شناسایی چالش‌ها و فرصت‌های مرتبط با اجرای این ابزارها در سکوهای مجازی، به بررسی تأثیر این اقدامات در کاهش تهدیدات تروریستی می‌پردازد. از این‌رو، با بهره‌گیری از روش پژوهش توصیفی تحلیلی به این پرسش که «چگونه تحریم‌های بین‌المللی و ابزارهای حقوقی بین‌المللی می‌توانند به‌طور مؤثر در سرکوب این جنایات در سکوهای مجازی عمل کنند؟» و «چه چالش‌ها و موانعی در مسیر اعمال تحریم‌ها و اجرای تصمیمات قضائی بین‌المللی برای سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی وجود دارد و آیا این اقدامات قادر به کاهش تهدیدات تروریستی خواهند بود؟» پاسخ دهد.

۲- پیشینهٔ تحولات حقوقی؛ تهدیدهای تروریستی در سکوهای مجازی و ضرورت پاسخ‌گذاری‌های بین‌المللی

در سال‌های اخیر، با گسترش فناوری‌های نوین و استفاده روزافزون از سکوهای مجازی، جنایات فناورانه در سکوهای مجازی به یکی از تهدیدات عمده امنیت بین‌المللی تبدیل شده است (Farber, 2025, p16). تروریست‌ها، ازجمله داعش و القاعده، به‌طور فزاینده‌ای از این سکوها برای جذب نیرو، تأمین منابع مالی، آموزش و برنامه‌ریزی عملیات‌های تروریستی بهره‌برداری کرده‌اند. این روند ضرورت پاسخ‌گویی حقوقی و اتخاذ تدابیر قانونی مؤثر برای سرکوب تهدیدات تروریستی در سکوهای مجازی را بیشتر از پیش برجسته می‌کند (Tsesis, 2017, p 624). به‌عنوان مثال، گروه داعش از شبکه‌های اجتماعی نظیر تلگرام، فیس‌بوک و توییتر برای تبلیغات و جذب نیروهای جدید بهره برده و عملیات‌های تروریستی خود را، به‌ویژه در کشورهای غربی و خاورمیانه، برنامه‌ریزی کرده است (Al-Qarawee, 2015, p 157)[۶]. هم‌چنین، در افغانستان و عراق، تروریست‌ها به‌طور گسترده‌ای از این فضا برای تبلیغات و جذب منابع مالی استفاده کرده‌اند[۷].

تلاش‌ها برای سرکوب جنایات فناورانه از سوی تروریست‌ها در سکوهای مجازی به اواخر دهه ۱۹۹۰ میلادی برمی‌گردد (Chertoff et al., 2020, p 1316). از این رو، یکی از مهم‌ترین ابزارهای حقوقی در قبال فعالیت‌های تروریستی، تحریم‌های بین‌المللی است که تحت نظارت سازمان ملل متحد و نهادهای بین‌المللی اعمال می‌شود. به‌عنوان مثال، شورای امنیت

1. https://www.odni.gov/files/NCTC/documents/jcat first responders toolbox/134s_-_First_Responders_Toolbox_-_Emerging_Technologies_May_Heighten_Terrorist_Threats.pdf
2 .https://ec.europa.eu/programmes/erasmus-plus/project-result-content/b63fe787-88d2-443e-a9ac-e0adbac2e214/UNSC-Study-Guide_final.pdf
3. https://www.ohchr.org/en/press-releases/2009/10/security-council-unanimously-adopts-wide-ranging-anti-terrorism-resolution
4. Cyber Army of Russia; https://www.s-rminform.com/cyber-intelligence-briefing/cyber-intelligence-briefing-26-july-2024
5. https://www.pravda.com.ua/eng/news/2024/07/19/7466559/

۶. پس از وقوع حملات گسترده‌ای نظیر تیراندازی به «مجله طنز شارلی ابدو» (Attentat contre Charlie Hebdo) در پاریس طی هفتم ژانویه سال ۲۰۱۵ و انفجار ۲۲ مِی سال ۲۰۱۷ پس از اجرای کنسرت در خارج از سالن «منچسترآرنا» در منچستر بریتانیا، موجب شد تا کشورهای اروپایی و البته ایالات متحده آمریکا نسبت به تصویب مقررات سخت‌گیرانه‌تری در حوزه مبارزه با فعالیت‌های تروریستی برخط اقدام‌های جدی‌تری داشته باشند؛

-https://journals.cambridgemedia.com.au/application/files/6016/8359/7173/Maloney_Paris_2019.pdf
7. https://unipd-centrodirittiumani.it/en/topics/terrorism-propaganda-and-human-rights-in-the-islamic-state

سازمان ملل متحد با تصویب قطعنامه ۱۳۷۳، از کشورهای عضو خواسته است تا با اعمال تحریم‌های اقتصادی و سیاسی علیه تروریست‌ها، این تهدیدات را کاهش دهند[۱]. تحولات اخیر در نیز شامل تصویب قطعنامه‌های جدیدی است که بر لزوم مقابله کشورهای عضو با بهره‌گیری غیرقانونی و نامشروع تروریست‌ها از سکوهای مجازی تأکید دارند. به‌عنوان نمونه، در پی حملات تروریستی ۱۱ سپتامبر ۲۰۰۱ در ایالات متحده، شورای امنیت سازمان ملل متحد قطعنامه ۱۳۷۳ را تصویب کرد که بر لزوم تقویت همکاری‌های بین‌المللی در مبارزه با تروریسم تأکید داشت[۲]. این قطعنامه از دولت‌ها خواست تا تدابیر قانونی و مالی لازم را برای مقابله با تروریسم اتخاذ کرده و تحریم‌های اقتصادی و مالی علیه افراد، گروه‌ها و کشورهای حامی تروریسم اِعمال نمایند (Tran, 2018, p 425). قطعنامه ۱۳۷۳ به‌عنوان نقطه آغازین استفاده از تحریم‌ها در مبارزه با تروریسم به‌شمار می‌آید. با این حال، با توجه به پیشرفت‌های فناوری و گسترش سکوهای مجازی، تحریم‌های نوینی علیه تهدیدات ناشی از ارتکاب جنایات فناورانه از سوی تروریست‌ها در سال‌های بعد به تصویب رسید[۳]. افزون بر این، شورای امنیت سازمان ملل متحد در قطعنامه ۲۳۵۴، از دولت‌ها خواسته شده است تا اقدامات خود را برای سرکوب فعالیت‌های تروریستی در سکوهای مجازی تقویت کنند[۴]. این قطعنامه بر لزوم ایجاد چارچوب‌های حقوقی برای نظارت و شناسایی این نوع از فعالیت‌های تروریستی تأکید می‌کند. علاوه بر این، گسترش مفهوم چنین فعالیت‌هایی در سکوهای مجازی و توسعه ابزارهای قانونی برای تعقیب و مجازات مرتکبان از دیگر تحولات مهم این حوزه به‌شمار می‌آید.[۵] این ابزارها شامل استفاده از مقررات داخلی و تقویت همکاری‌های بین‌المللی برای تعقیب و مجازات افرادی است که از سکوهای مجازی برای تبلیغات تروریستی و جذب منابع استفاده می‌کنند (Fidler, 2016, p 471). البته شورا وفق قطعنامه ۲۴۸۲ مجدد به تهدیدات تروریستی در سکوهای مجازی پرداخته و از کشورهای عضو خواسته است تا از سوءاستفاده اینترنتی در جنایات تروریستی پیشگیری کرده و تحریم‌های اقتصادی و مالی علیه جنایات فناورانه از سوی تروریست‌ها اعمال کنند. همچنین، بر لزوم تقویت همکاری‌های بین‌المللی و روزآمدسازی مقررات داخلی تأکید شده است[۶]. وانگهی، در هشتم دسامبر ۲۰۲۰، اتحادیه اروپا تحریم‌هایی علیه گروه‌های تروریستی که از فناوری‌های نوین و سکوهای مجازی برای جنایات تروریستی استفاده می‌کنند، اِعمال کرد[۷]؛ این تحریم‌ها مشتمل بر انسداد دارایی‌ها، ممنوعیت سفر و محدودیت‌های مالی بود (Lemnitzer, 2020, p 796-999). البته وزارت خزانه‌داری ایالات متحده آمریکا در ۲۴ جولای ۲۰۲۰، تحریم‌هایی علیه شبکه‌های تروریستی که از سکوهای مجازی برای ترویج فعالیت‌های تروریستی استفاده می‌کنند، وضع کرد[۸]. فرانسه از ابتکارات بین‌المللی برای مقابله با جنایات فناورانه تروریست‌ها حمایت کرده و به‌ویژه از «قانون خدمات دیجیتال، مصوب ۲۰۲۲[۹]» اتحادیه اروپا پشتیبانی نموده است[۱۰]. این مقررات بر مسئولیت سکوها در حذف سریع محتوای تروریستی تأکید دارد و فرانسه از سکوها می‌خواهد که از سوءاستفاده تروریستی پیشگیری کنند. به‌علاوه، فرانسه مسئولیت‌پذیری بازیگران در سکوهای مجازی را در قبال سوءاستفاده برای اهداف تروریستی ترویج می‌دهد و این موضوع را در نشست‌های «گروه هفت[۱۱]» و اتحادیه اروپا مطرح کرده و از تصویب پیش‌نویس «مقررات خدمات دیجیتال» که در دسامبر ۲۰۲۰ توسط کمیسیون اروپا ارائه و در نوامبر ۲۰۲۲ در شورای اروپا تصویب شد[۱۲]، حمایت نموده است[۱۳].

---

۱. در عصر حاضر، اینترنت و گستره سکوهای مجازی می‌تواند وفق ماده ۴۱ منشور سازمان متحد تحت تحریم‌های بین‌المللی قرار گیرند. با این حال، تاکنون شورای امنیت ملل متحد راهبرد مشخصی در این زمینه نداشته است و بیشتر تحریم‌ها به‌طور یک‌جانبه و بدون مجوز قانونی از سوی دولت‌ها اِعمال می‌شود. تنها در صورت ورود کشورهای هدف به حوزه قدرت‌های کلان بین‌المللی، این تحریم‌ها ممکن است از جنبه ضمانت اجرایی به ماهیت مجرمانه تبدیل شوند (خالقی و ثقفی، ۱۴۰۱، ص ۱۰۵).

2. United Nations. (2001, September 28). *Resolution 1373 (2001) adopted by the Security Council at its 4385th meeting* (S/RES/1373). https://digitallibrary.un.org/record/449020?v=pdf

3. Access Now. (2024, June). *Wavering resolutions: The UN Security Council on digital rights: Digital, cyber, and human rights in the language of UN Security Council resolutions between 2001-2023*. https://www.accessnow.org/wp-content/uploads/2024/07/UN-Security-Council-in-the-digital-age-technical-report.pdf

4. United Nations. (2017). *Resolution 2354 (2017)*. S/RES/2354. Security Council Distr.: General, 24 May 2017. https://digitallibrary.un.org/record/1289209?v=pdf

5. https://www.undp.org/sites/g/files/zskgke326/files/2024-12/final-analysis-tf-gbv.pdf

6. United Nations. (2019, July 19). *Resolution 2482 (2019) adopted by the Security Council at its 8582nd meeting*. https://docs.un.org/en/S/RES/2482(2019)

7. https://www.consilium.europa.eu/en/policies/sanctions-against-terrorism/

8. https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf

9. European Commission. (2022, October 19). *The Digital Services Act*. European Union. https://www.eu-digital-services-act.com/Digital_Services_Act_Articles.html

10. https://cds.thalesgroup.com/en/hot-topics/french-cyber-community-forefront-european-security

11. https://www.g7italy.it/en/

12.https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020PC0825

13. United Nations. (2019, June 24). *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General* (A/74/120, p. 25). https://docs.un.org/en/A/74/120

با این همه، چین و روسیه به‌طور مُجدانه تهدیدات تروریستی در سکوهای مجازی را مورد توجه قرار داده و اقدامات قانونی متعددی برای مقابله با این تهدیدات اتخاذ کرده‌اند. چین با تصویب « قانون مبارزه با تروریسم جمهوری خلق چین، مصوب ۲۰۱۵[۱]» و « قانون امنیت سایبری جمهوری خلق چین، مصوب ۲۰۱۶[۲]»، به تقویت امنیت سکوهای مجازی و پیشگیری از سوءاستفاده گروه‌های تروریستی از فناوری‌های نوین پرداخته است (Li, 2019, p 347-352)[۳]. از سوی دیگر، روسیه نیز با تصویب مقرراتی مشابه نظیر «قانون فدرال راجع‌به مقابله با تروریسم، مصوب ۲۰۰۶[۴]»، «قانون اطلاعات، فناوری اطلاعات و حفاظت از اطلاعات و قانون ارتباطات از جمله الزامات احراز هویت کاربر، لازم‌الاجرا ۲۰۲۵[۵]» و «دستورالعمل‌های سرویس امنیت فدرال روسیه برای نظارت بر فضای مجازی[۶]»، به سرکوب تهدیدات ناشی از جنایات فناورانه از سوی تروریست‌ها در سکوهای مجازی پرداخته است (Kuleshova, 2020, p 158-161). علاوه بر این، هر دو کشور در سطح بین‌المللی همکاری‌هایی را در زمینه شناسایی و انسداد محتوای تروریستی و تقویت ظرفیت‌های اجرایی در قبال تهدیدات ناشی از ارتکاب جنایات فناورانه از سوی تروریست‌ها دارند.

با این حال، چالش‌هایی همچون حاکمیت ملی، تعارض‌های قضائی و محدودیت‌های اجرایی تحریم‌ها همچنان مانع از تحقق کامل اهداف حقوقی در سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی است (Purcell et al., 2023, p 139-141). به‌عنوان مثال، برخی کشورها به‌دلایل سیاسی از همکاری با سازمان‌های بین‌المللی در زمینه سرکوب فعالیت‌های تروریستی در سکوهای مجازی پرهیز می‌کنند یا اجرای تحریم‌ها را به‌دلیل مسائل سیاسی به تأخیر می‌اندازند[۷]. برای نمونه، در سال‌های اخیر، روسیه و چین با انتقاد از برخی سیاست‌های غربی در زمینه تحریم‌های ضدتروریسم، همکاری‌های محدودی با نهادهای بین‌المللی در این زمینه داشته‌اند.[۸] این مسائل نیازمند اصلاحات در چارچوب‌های بین‌المللی و تقویت همکاری‌های بین‌دولتی است تا بتوان به‌طور مؤثر با تهدیدات تروریستی در سکوهای مجازی سرکوب کرد. در ضمن، این تحولات و چالش‌ها، اهمیت بازنگری در سیاست‌ها و چارچوب‌های حقوقی بین‌المللی را آشکار می‌سازد تا از این طریق با همبستگی جهانی و وضع قوانین مؤثر، مقابله‌ای جامع و هماهنگ با تهدیدات تروریستی فناورانه در سکوهای مجازی به‌عمل آید.

۳- مصادیق و مفهوم‌شناسی تحریم‌ها

تحریم‌ها به‌عنوان ابزارهایی مؤثر در سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی شناخته می‌شوند. از منظر حقوق بین‌الملل، این تحریم‌ها باید با اصول حقوق بشر سازگار بوده و به‌طور متناسب با تهدیدات واقعی و خطرات ناشی از آن ها اعمال گردند[۹]. اعمال تحریم‌های یک‌جانبه می‌تواند منجر به بروز اختلافات حقوقی میان دولت‌ها شود؛ بنابراین، نظارت و هماهنگی از سوی سازمان‌های بین‌المللی به‌ویژه شورای امنیت ملل متحد ضروری است تا از هرگونه سوءاستفاده و تبعیض احتمالی پیشگیری شود[۱۰]. بر این اساس، با توجه به امکان سرکوب جنایات فناورانه تروریست‌ها و حتی نظارت و کنترل آن ها در سکوهای مجازی از طریق اِعمال تحریم‌های

1. Standing Committee of the National People's Congress. (2015, December 27). *Counter-terrorism law of the People's Republic of China* (amended 2018, April 27). National People's Congress. http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm
2. Standing Committee of the National People's Congress. (2016, November 7). *Cybersecurity law of the People's Republic of China* (Order No. 53 of the President). Lawinfochina. https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3
3. http://www.scio.gov.cn/zfbps/zfbps_2279/202401/t20240123_829679.html
4. Federal Assembly of the Russian Federation. (2006, March 6). *Federal law No. 35-FZ of 6 March 2006 on counteraction against terrorism*. https://rm.coe.int/ct-legislation-russian-federation/16806415f5
5. Digital Policy Alert. (n.d.). *Implemented law No. 406-FZ amending the Act on Information, Information Technologies and Information Protection and Act on Communications including user authentication requirement*. https://digitalpolicyalert.org/event/18087-implemented-implemented-law-no-406-fz-amending-act-on-information-information-technologies-and-information-protection-and-act-on-communications-including-user-authentication-requirement
6. Britannica. (n.d.). *Federal Security Service of the Russian Federation*. Encyclopædia Britannica. https://www.britannica.com/topic/Federal-Security-Service
7. https://carnegie-production-assets.s3.amazonaws.com/static/files/Carnegie_Countering_Disinformation_Effectively.pdf
8. https://www.marshallcenter.org/en/publications/clock-tower-security-series/strategic-competition-seminar-series/russia-and-china-central-asia
9. https://luissuniversitypress.it/wp- content/uploads/2021/04/9_de-Lauro_completo.pdf?srsltid=AfmBOoqXC1kHGbQ0C1rXfxYs-DGV2C7CArvBzPaA-62FIQ1adl8VkBki
10. https://watermark.silverchair.com/130063.pdf

بین‌المللی اعم از اقتصادی و غیر اقتصادی[۱]، تنوع و اقسام گوناگون آن ها که مرتبط به جنایات ارتکابی است، در ذیل مورد مداقه قرار می‌گیرند:

الف) تحریم‌های اقتصادی، تجاری و مالی[۲]؛ اجرای این تحریم‌ها علیه جنایات فناورانه تروریست‌ها به‌عنوان ابزارهای مؤثر در حقوق بین‌الملل برای سرکوب تروریست‌ها و پیشگیری از سوءاستفاده آن ها از فناوری‌های نوین شناخته می‌شوند.[۳] این تحریم‌ها به‌طور معمول با هدف تحدید منابع مالی، تجاری و فناورانه تروریست‌ها وضع می‌گردند و ممکن است شامل انسداد دارایی‌ها، محدودیت‌های تجاری و مالی، و نظارت بر واردات و صادرات فناوری‌ها باشند (Bogdanova, 2022, p 71-73). این اقدامات به‌ویژه در سکوهای مجازی مؤثر است، چرا که تروریست‌ها ممکن است از ابزارهای دیجیتالی برای تأمین مالی و پیشبرد اهداف خود بهره‌برداری کنند. تحریم‌ها باید با رعایت اصول حقوق بشر و به‌طور متناسب با تهدیدات واقعی اعمال گردند تا از آسیب به حقوق افراد غیرمرتبط پیشگیری شود. از منظر حقوق بین‌الملل، تحریم‌های اقتصادی باید مطابق با استانداردهای بین‌المللی و اصول حقوق بشر برای سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی وضع شوند (Douhan, 2022, p 118-119). در ضمن، ممنوعیت دسترسی تروریست‌ها به بازارهای مالی جهانی از طریق تحریم‌های تجاری و مالی، یکی از اقدامات مؤثر در سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی به شمار می‌رود. این تحریم‌ها به‌منظور تحدید منابع مالی تروریست‌ها و پیشگیری از تأمین مالی فعالیت‌های آن ها از طریق سامانه‌های مالی جهانی اعمال می‌شوند. تحریم‌های تجاری و مالی ممکن است شامل انسداد دسترسی تروریست‌ها به سامانه‌های بانکی، خدمات مالی، و ارزهای مجازی باشد (گوردون، اسمیت و کورنل، ۱۴۰۰، ص ۴۳). وفق چارچوب موازین و قواعد بین‌المللی، اعمال این تحریم‌ها باید مطابق با اصول حقوق بشر و متناسب با تهدیدات واقعی باشد. همچنین، تحریم‌ها باید به‌صورت شفاف و منصفانه اجرا شوند تا از آسیب به حقوق افراد غیرمرتبط و نقض حقوق انسانی پیشگیری گردد (Lombardo & El Khoury, 2023, p 95-96).

ب) تحریم‌های ممنوعیت ورود و خروج (ممنوعیت سفر[۴])؛ این نوع از تحریم‌ها، به‌مثابه یکی از ابزارهای بین‌المللی در سرکوب فعالیت‌های تروریستی در سکوهای مجازی، محدودیت‌هایی را بر سفر افراد خاص، از جمله سرکردگان تروریست‌ها، وضع می‌کنند[۵]. این تحریم‌ها مشتمل بر ممنوعیت ورود یا خروج افرادی است که به تسهیل یا ارتکاب فعالیت‌های تروریستی در سکوهای مجازی پرداخته‌اند (ماتام‌فارال، ۱۳۹۹، ص۱۲۶). هدف از اِعمال این تحریم‌ها محدودیت تحرک این افراد و پیشگیری از گسترش فعالیت‌های تروریستی از طریق سکوهای مجازی است، همچنین پیشگیری از دسترسی آنان به منابع مالی و فناوری در کشورهای مختلف[۶]. این تحریم‌ها تحریم‌های می‌توانند به‌طور غیرمستقیم در پیشگیری از استفاده تروریست‌ها از سکوهای مجازی برای سازمان‌دهی حملات مؤثر واقع شوند[۷]. با این حال، این تحریم‌ها ممکن است با حقوق بشر، به‌ویژه حق آزادی حرکت و حفاظت از زندگی خصوصی، در تضاد قرار گیرند؛ به‌ویژه زمانی که افراد هنوز در محاکم بین‌المللی به‌طور رسمی به فعالیت‌های تروریستی متهم نشده‌اند. علاوه بر این، شناسایی دقیق ارتباط افراد با فعالیت‌های تروریستی در سکوهای مجازی به دلیل استفاده از هویت‌های مستعار و روش‌های پیچیده ارتباطی چالش‌برانگیز است. بنابراین، تحریم‌های ممنوعیت ورود و

۱. تحریم‌های سازمان ملل متحد را می‌توان به «اقتصادی» و «غیراقتصادی» تقسیم کرد؛ بر این اساس، «تحریم‌های اقتصادی» مشتمل بر «تحریم‌های اقتصادی فراگیر»، «تحریم‌های اقتصادی خاص» مشتمل بر «تحریم تسلیحاتی»، «تحریم علیه سلاح‌های کشتار جمعی»، «تحریم‌های نفتی»، «تحریم آزبست، سنگ‌آهن، شکر، چرم، کروم، چدن خام، تنباکو، مس، کوشت و حتی فرآورده‌های گوشتی»، «تحریم الماس»، «تحریم‌های شیمیایی»، «تحریم الوار» و «تحریم کالاهای لوکس» بوده و «تحریم‌های مالی»، است. «تحریم‌های غیراقتصادی» شامل «تحریم حمل‌ونقل»، «تحریم سفر»، «تحریم هوایی»، «تحریم ورزشی»، «تحریم علمی و فرهنگی»، «تحریم مخابراتی»، است(ر.ک: ماتام‌فارال، ۱۳۹۹: ۱۲۸-۱۱۳). این تحریم‌ها ممکن است بر صنایع خاصی نظیر نفت، شیمیایی یا حتی کالاهای لوکس تأثیر بگذارند. از سوی دیگر، تحریم‌های غیراقتصادی عمدتاً به محدودسازی ارتباطات و فعالیت‌های غیرمستقیم می‌پردازند، از جمله تحریم‌های حمل‌ونقل، سفر، یا همکاری‌های علمی و فرهنگی. هدف از این نوع تحریم‌ها معمولاً وارد ساختن فشار بر روابط بین‌المللی و فرهنگی کشورها به‌منظور تحقق تغییرات سیاسی مطلوب است. این اقدامات در راستای تأثیرگذاری بر رفتار دولت‌ها و دستیابی به اهداف سیاسی از طریق ابزارهای غیرمستقیم طراحی و اعمال می‌شوند.

2. Economic, Rrade and Financial Sanctions

۳. تحریم‌های اقتصادی در قرن بیست و یکم به‌عنوان ابزاری اساسی در سیاست‌های بین‌المللی شناخته شده‌اند و دولت‌های عمده‌ای نظیر ایالات متحده، اتحادیه اروپا و سازمان ملل متحد از آن ها در قبال خشونت‌های دولتی، نقض حقوق بشر، تروریسم و گسترش سلاح‌های هسته‌ای بهره‌برداری می‌کنند. این تحریم‌ها به‌ویژه در چارچوب مبارزه با تروریسم مؤثر واقع شده و نقشی حیاتی در حفظ امنیت بین‌المللی ایفا می‌کنند. افزون بر این، تحریم‌های اقتصادی به‌عنوان راهبردی برای احیای حقوق بشر و حمایت از اصول بنیادین آن مورد استفاده قرار می‌گیرند(نمامیان و حسینی، ۱۴۰۲: ۱۴۹).

4. Sanctions Prohibiting Entry and Exit (Travel Ban)

۵. شورای امنیت ملل متحد، قطعنامه ۲۷۳۴ (۲۰۲۴) را به‌منظور مقابله با تهدیدات امنیتی نوظهور در سکوهای مجازی و سرکوب جنایات فناورانه تروریست‌ها اتخاذ شده است. این قطعنامه به‌ویژه به تحریم‌های ممنوعیت سفر برای اشخاص و نهادهایی اشاره دارد که به‌طور مستقیم یا غیرمستقیم در فعالیت‌های تروریستی در سکوهای مجازی مشارکت دارند. هدف اصلی این تحریم‌ها اعمال فشار بر دولت‌ها و گروه‌هایی است که از فناوری‌های نوین با هدف تغییر رفتارهای مخرب و تهدیدآمیز در سکوهای مجازی برای ترویج خشونت، تهدید امنیت بین‌المللی یا نقض حقوق بشر استفاده می‌کنند؛

- United Nations. (2024, June 10). Resolution 2734 (2024) [S/RES/2734 (2024)]. Security Council. https://documents.un.org/doc/undoc/gen/n24/164/83/pdf/n2416483.pdf?_gl=1*1def6i9*_ga*ODA3MjM3ODkwLjE1ODkzNjgwMzc.*_ga_TK9BQL5X7Z*czE3NTQ2NDUyMzckbzQ5JGcwJHQxNzU0NjQ1MjM3Jo2MCRsMCRoMA

6. https://main.un.org/securitycouncil/sites/default/files/eot_travel_ban_english.pdf

7. https://esil-sedi.eu/wp-content/uploads/2018/04/Birkhauser.pdf

خروج باید مطابق با اصول حقوقی، مشروعیت و تناسب در حقوق بین‌الملل اعمال شوند.

ج) تحریم‌های فناوری اطلاعات[1]؛ این دسته از تحریم‌ها، به‌عنوان ابزاری مؤثر برای محدودیت توان تروریست‌ها در بهره‌برداری از فناوری‌های نوین و سکوهای مجازی جهت ارتکاب جرایم تروریستی شناخته می‌شوند. این تحریم‌ها با تحدید دسترسی به فناوری‌ها، نرم‌افزارها، ابزارهای ارتباطی و منابع اطلاعاتی خاص، تلاش دارند تا از برنامه‌ریزی و سازمان‌دهی عملیات تروریستی در سکوهای مجازی پیشگیری کنند (Jayawickrama, 2017, p 476-477). با این حال، تحریم‌های مذکور ممکن است با برخی حقوق بشر، نظیر حق آزادی بیان و دسترسی آزاد به اطلاعات، در تضاد قرار گیرند. علاوه بر این، چالش‌هایی نظیر احتمال سوءاستفاده از تحریم‌ها، پیچیدگی‌های فناوری و لزوم همکاری‌های بین‌المللی برای اجرای مؤثر آن ها وجود دارد (McDonnell, 2024, p 136-138). تحریم‌های فناوری اطلاعات باید با رعایت اصول حقوقی، مشروعیت و تناسب در موازین بین‌المللی اعمال شوند تا از تأثیرات منفی بر افراد بی‌گناه پیشگیری گردد (ماتام‌فارال، ۱۳۹۹، ص ۱۲۸). در نهایت، این تحریم‌ها می‌توانند در سرکوب فعالیت‌های تروریستی در سکوهای مجازی مؤثر باشند، اما اجرای آن ها باید با دقت، رعایت حقوق بشر و اصول قانونی همراه باشد.

د) تحریم‌های رسانه‌ای و ارتباطی[2]؛ این تحریم، به‌مثابه راهبردی مؤثر برای سرکوب ترویج خشونت و فعالیت‌های تروریستی از طریق رسانه‌ها و شبکه‌های اجتماعی به‌کار می‌روند. این تحریم‌ها به محدودیت دسترسی به سکوها و ابزارهای ارتباطی خاصی می‌پردازند که تروریست‌ها از آن ها برای تبلیغات، جذب نیرو و سازمان‌دهی عملیات‌های تروریستی استفاده می‌کنند (Davis, 2021, p 69). هدف اصلی این تحریم‌ها پیشگیری از انتشار پیام‌های تروریستی و خشونت‌آمیز در سکوهای مجازی است[3]. علاوه بر این، پیشرفت‌های فناوری و استفاده از فنون رمزگذاری می‌تواند اجرای این تحریم‌ها را با چالش‌هایی مواجه سازد (نمامیان و حسینی،۱۴۰۳، ص ۱۶۹). از این‌رو، تحریم‌های رسانه‌ای و ارتباطی باید به‌طور متناسب با تهدیدات تروریستی و با رعایت کنوانسیون‌های بین‌المللی اعمال شوند تا از آسیب به حقوق و آزادی‌های اساسی پیشگیری گردد[4].

1. IT Sanctions
2. Media and Communication Sanctions
3. https://www.un.org/unispal/document/report-special-rapporteur-23aug24/
4. https://www.ohchr.org/en/special-procedures/sr-terrorism/international-standards-promotion-and-protection-human-rights-and-fundamental-freedoms-while

هـ) تحریم‌های تسلیحاتی[5]؛ اجرای این نوع از تحریم‌ها، اقدامی بین‌المللی برای سرکوب تهدیدات تروریستی، به‌منظور محدودیت دسترسی تروریست‌ها به سلاح و تجهیزات نظامی اطلاق می‌شوند[6]. این تحریم‌ها در زمینه سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی نیز تأثیرگذارند، زیرا تروریست‌ها ممکن است از فناوری‌های نوین برای سازمان‌دهی و اجرای عملیات تروریستی استفاده کنند[7]. در این راستا، تحدید تأمین تسلیحات به این تروریست‌ها می‌تواند از گسترش خشونت و تهدیدات علیه امنیت جهانی پیشگیری کند. با این حال، تحریم‌های تسلیحاتی باید به‌طور دقیق و متناسب با تهدیدات موجود اعمال شوند تا از نقض حقوق بشر و آزادی‌های اساسی پیشگیری گردد (Faraji Dizaji & Murshed, 2024, p 8-9). در برخی موارد، تروریست‌ها ممکن است از فناوری‌های پیچیده مانند شبکه‌های خصوصی مجازی یا رمزگذاری برای دور زدن این تحریم‌ها استفاده کنند. این امر نیازمند نظارت دقیق و همکاری‌های بین‌المللی مستمر است (گوردون و همکاران، ۱۴۰۰، ص ۴۴). البته تحریم‌های تسلیحاتی باید مطابق با اصول قانونی، مشروعیت و تناسب اعمال شوند. به‌ویژه در زمینه استفاده از فناوری‌های مجازی برای تسهیل فعالیت‌های تروریستی، تحریم‌ها باید به‌گونه‌ای طراحی گردند که به‌طور مستقیم با تهدیدات فناورانه سرکوب کنند، بدون آنکه حقوق فردی و آزادی‌های اساسی افراد بی‌گناه را نقض نمایند (Erickson, 2020, p 14-15).

5. Arms Sanctions (or Arms Embargo)

۶. شورای امنیت ملل متحد تا سال ۲۰۲۳، تحریم‌های تسلیحاتی اجباری علیه چهارده کشور از جمله عراق، سومالی، لیبریا، ساحل عاج و جمهوری آفریقای مرکزی اعمال کرده است. برخی از این تحریم‌ها تا سال ۲۰۲۵ تمدید شده‌اند، مانند تحریم‌های علیه جمهوری آفریقای مرکزی و سودان جنوبی. همچنین، اتحادیه اروپا تا سال ۲۰۲۳، ۲۲ تحریم تسلیحاتی علیه کشورهایی مانند بلاروس، روسیه، سوریه، ونزوئلا و زیمبابوه برقرار کرده است که برخی از آن ها تا سال ۲۰۲۶ تمدید شده‌اند. این تحریم‌ها شامل اقدامات الزامی و سیاسی هستند و عمدتاً به دلیل تهدیدات امنیتی، نقض حقوق بشر یا رفتارهای غیرقانونی ادامه و تمدید می‌شوند؛

-https://www.sipriyearbook.org/view/9780198890720/sipri-9780198890720-chapter-012-div1-003.xml?utm_source=chatgpt.com

۷. قطعنامه ۲۴۲۸ شورای امنیت سازمان ملل متحد که در تاریخ ۳۰ ژوئیه ۲۰۱۸ تصویب گردید، بر تحریم‌های تسلیحاتی و سایر محدودیت‌ها علیه جمهوری آفریقای مرکزی تأکید دارد. این قطعنامه به‌ویژه به سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی و پیشگیری از سوءاستفاده از فناوری برای ترویج خشونت و تهدیدات امنیتی پرداخته است. هدف اصلی این قطعنامه، ایجاد ثبات در جمهوری آفریقای مرکزی و مقابله با خشونت‌های فرقه‌ای و تروریستی، به‌ویژه از طریق استفاده غیرمجاز از سکوهای مجازی، می‌باشد. این اقدام بخشی از تلاش‌های بین‌المللی برای حفظ صلح و امنیت و مقابله با فعالیت‌های تروریستی در این کشور است؛

- United Nations Security Council. (2018, July 13). *Resolution 2428 (2018)*. https://docs.un.org/en/S/RES/2428(2018)

ر) تحریم‌های دیپلماتیک یا سیاسی (تحریم‌های مقامات دولتی)[1]؛ اِعمال این مصداق از تحریم‌ها برای اِعمال فشار سیاسی و تحدید فعالیت‌های دولتی در سرکوب جنایات تروریستی، نقش مهمی در ساختار و محتوای اسناد بین‌المللی ایفا می‌کنند. بنابراین، مشتمل بر قطع روابط دیپلماتیک، محدودیت‌های سفر و تعلیق مشارکت در سازمان‌های بین‌المللی هستند[2]. هدف اصلی تحریم‌های سیاسی، وارد کردن فشار به هدف برای تغییر اقدامات، سیاست‌ها یا شیوه‌های حکمرانی سیاسی آن است؛ این تحریم‌ها اغلب به واکنش به مسائلی هم‌چون تجاوز، فساد یا رفتار غیردموکراتیک اِعمال می‌شوند[3]. اِعمال تحریم‌های دیپلماتیک باید وفق اصول حقوقی بین‌الملل، مشروعیت و تناسب در اعمال فشار انجام گیرد (گوردون و همکاران، ۱۴۰۰، ص ۴۵). این تحریم‌ها ممکن است با حقوق بشر و آزادی‌های اساسی در تضاد قرار گیرند، به‌ویژه زمانی که بدون شواهد قانونی مستند بر مقامات یا افراد با ارتباطات غیرمستقیم با فعالیت‌های تروریستی اِعمال شوند[4]. به‌علاوه، این تحریم‌ها باید با دقت و به‌طور مؤثر اجرا شوند تا از سوءاستفاده و آسیب به افراد بی‌گناه پیشگیری گردد[5]. در نهایت، تحریم‌های دیپلماتیک ابزاری ضروری در سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی هستند، اما باید با رعایت اصول حقوقی و دقت کافی به‌منظور پیشگیری از نقض حقوق بشر و مقابله مؤثر با تهدیدات تروریستی اعمال شوند (Miao, 2024 p 421).

با این همه، تحریم‌های بین‌المللی به‌عنوان ابزارهای حقوقی مؤثر در سرکوب سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی شناخته می‌شوند و در قالب‌های مختلف اقتصادی، تجاری، مالی، سفر، فناوری اطلاعات، رسانه‌ای، تسلیحاتی و دیپلماتیک اعمال می‌گردند. این تحریم‌ها با هدف تحدید دسترسی تروریست‌ها به منابع مالی، فناوری‌های نوین و سکوهای مجازی طراحی می‌شوند. اعمال این تحریم‌ها باید متناسب با تهدیدات موجود و با رعایت اصول حقوق بین‌الملل، حقوق بشر و آزادی‌های اساسی صورت پذیرد.

٤- چالش‌ها و موانع اجرای تحریم‌های بین‌المللی

تحریم‌های بین‌المللی به‌عنوان یکی از ابزارهای اساسی برای سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی شناخته می‌شوند، اما در راستای استفاده مؤثر از این ابزار، چالش‌های متعددی وجود دارد. از جمله مهم‌ترین موانع می‌توان به تفاوت‌های حاکم در مقررات داخلی کشورها و عدم تطابق آن ها با مفاد تحریم‌ها، مشکلات اجرایی در سکوهای مجازی نظیر ردیابی منابع مالی و انسداد محتوا، و پیچیدگی‌های ناشی از روش‌های دور زدن تحریم‌ها توسط تروریست‌ها اشاره کرد[6]. علاوه بر این، اختلافات سیاسی میان دولت‌ها و عدم همکاری برخی کشورها با نهادهای بین‌المللی، موجب محدودیت در اجرای مؤثر تحریم‌ها می‌شود. برای دستیابی به مقابله مؤثر با جنایات فناورانه تروریست‌ها، ضروری است اصلاحات در چارچوب‌های حقوقی بین‌المللی صورت پذیرد و همکاری‌های بین‌دولتی تقویت شود تا تهدیدات تروریستی در سکوهای مجازی به‌طور مؤثر و جامع سرکوب گردد.

تروریست‌ها با بهره‌گیری از فناوری‌های نوین، از جمله رمزارزها، شبکه‌های پنهان و ارتباطات رمزگذاری‌شده، به‌طور مؤثر از تحریم‌های بین‌المللی فرار می‌کنند. این شیوه‌ها موجب بروز مشکلات قابل توجهی در ردیابی و انسداد منابع مالی فعالیت‌های تروریستی می‌شوند. رمزارزها انتقال منابع مالی را بدون نظارت نهادهای مالی ممکن می‌سازند، شبکه‌های پنهان برای خرید و فروش سلاح و مواد شیمیایی مورد استفاده قرار می‌گیرند و ارتباطات رمزگذاری‌شده به تروریست‌ها این امکان را می‌دهند که از نظارت دولتی اجتناب کنند. این روش‌ها به‌ویژه در کشورهای تحت تحریم به‌طور مؤثری عمل می‌کنند و مقابله با آن ها نیازمند اصلاحات قانونی و تقویت همکاری‌های بین‌المللی است (Burgess et al., 2024, p 216-218). برای سرکوب این تهدیدات، اجرای تحریم‌های بین‌المللی باید به‌طور مؤثرتری صورت پذیرد و همکاری‌های بین‌دولتی در زمینه تبادل اطلاعات و بهره‌برداری از ابزارهای نظارتی پیشرفته تقویت گردد.

نظارت بر اجرای تحریم‌ها در سکوهای مجازی و جهانی با چالش‌های قابل توجهی مواجه است. ویژگی‌هایی چون عدم شناخت و سرعت فزاینده

1. Diplomatic or Political Sanctions (Sanctions by Government Officials)

2. Old Dominion University. (2020). *ODUMUNC 2020 Issue Brief: UN General Assembly Fourth Committee: Disarmament – The Role of the Sanctions in Diplomacy*. ODU United Nations Society. https://www.odu.edu/sites/default/files/documents/ib-4th-sanctions-in-diplomacy.pdf

3. Sanction Scanner. (2025, June 20). *Economic sanctions vs. political sanctions: Definitions and differences*. Sanction Scanner. https://www.sanctionscanner.com/blog/economic-sanctions-vs-political-sanctions-924

4. https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-human-rights-and-cybercrime-law.html

۵. با ظهور تروریسم بین‌المللی و ضعف تحریم‌های سنتی، تحریم‌های هوشمند به‌وجود آمد که عمده آن ها علیه بازیگران غیردولتی و اشخاص حقیقی اِعمال می‌شود. این نوع تحریم‌ها چالش‌های نوینی را در حقوق بین‌الملل ایجاد کرده‌اند؛ به‌ویژه این‌که تحریم‌های اِعمال‌شده علیه برخی اتباع ایرانی به‌دلیل فعالیت‌های هسته‌ای، موشکی و نقض حقوق بشر، ممکن است با اصولی مانند مصونیت اموال دولتی، مصونیت دیپلماتیک و حق بر مالکیت خصوصی در تضاد باشند. رویه قضایی ملی و منطقه‌ای مؤید آن است که این تضادها می‌تواند منجر به بی‌اعتباری برخی قطعنامه‌ها و تصمیمات شورای امنیت شود (ضیایی و محمدی‌ثقفی، ۱۳۹۳، ص ۱۵).

6. https://www.lawfaremedia.org/article/sounding-the-alarm-on-digitally-enabled-sanctions-evasion

انتقال اطلاعات در این سکوها، نظارت بر فعالیت‌های تروریستی را پیچیده می‌سازد. تروریست‌ها از فناوری‌هایی مانند رمزارزها و شبکه‌های پنهان برای اجتناب از نظارت بهره می‌برند. علاوه بر این، تفاوت‌های قانونی میان کشورها و عدم هماهنگی میان نهادهای بین‌المللی، اجرای مؤثر تحریم‌ها را با مشکل مواجه می‌کند (Theodore, 2017, p 231). افزون بر این، تحریم‌های بین‌المللی به‌عنوان واکنشی به جنایات فناورانه تروریست‌ها، ممکن است تأثیرات منفی قابل توجهی بر مردم عادی و آزادی‌های فردی داشته باشند. این تحریم‌ها به‌ویژه محدودیت‌هایی در دسترسی به فناوری‌های ارتباطی و اطلاعاتی ایجاد می‌کنند که می‌تواند به نقض حقوق بشر منجر شود. علاوه بر این، این تحریم‌ها تأثیرات منفی بر رفاه اجتماعی و اقتصادی مردم عادی دارند، به‌ویژه در زمینه‌های ارتباطات، آموزش و خدمات پزشکی (Moiseienko, 2024, p 27-29). این چالش‌ها به‌ویژه در ایجاد توازن میان امنیت جهانی و حقوق فردی مطرح می‌شوند و ضرورت اتخاذ تدابیر مناسب برای پیشگیری از آسیب به مردم عادی و حفظ حقوق بشر را ایجاب می‌کنند؛ وانگهی، محدودیت‌های تحریمی ممکن است دسترسی به خدمات ارتباطی را محدود کند و نظارت گسترده تهدیدی برای آزادی‌های فردی، به‌ویژه در کشورهای با وضعیت حقوق بشری ضعیف، باشد. برای مقابله با این چالش‌ها، نیاز به توازن میان امنیت و حقوق بشر و طراحی راهکارهایی است که از یک‌سو مانع بهره‌برداری تروریست‌ها شود و از سوی دیگر حقوق افراد حفظ گردد.

با این همه، تحریم‌های بین‌المللی در سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی با چالش‌هایی نظیر حاکمیت ملی، تفاوت‌های قوانین داخلی و مشکلات اجرایی در سکوهای مجازی مواجه هستند[۱].

۵- توازن میان امنیت سکوهای مجازی و حقوق بشر در رویکردهای حقوقی اسناد بین‌المللی

اسناد بین‌المللی، به‌ویژه «کنوانسیون بوداپست در مورد جرایم سایبری، مصوب ۲۰۰۱[۲]» و «کنوانسیون سازمان ملل متحد علیه جرایم سایبری، مصوب ۲۰۲۴[۳]»، به‌طور عمده بر ایجاد توازنی میان تضمین امنیت سکوهای مجازی و صیانت از حقوق و آزادی‌های بنیادین بشر تأکید دارند. کنوانسیون سازمان ملل متحد علیه جرایم سایبری با توجه به تحولات شتابان فناوری اطلاعات و ظهور تهدیدهای پیچیده مجازی، چارچوبی جامع و به‌روز برای سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی و سوءاستفاده از سکوهای مجازی ارائه می‌دهد؛ به‌نحوی‌که اجرای تدابیر امنیتی باید هم‌راستا با الزامات حقوق بشری انجام گیرد (De Silva De Alwis, 2025, p 31-34).

اسنادی نظیر «کنوانسیون بین المللی راجع به سرکوب تأمین مالی تروریسم، مصوب ۱۹۹۹[۴]» و «دستورالعمل‌های گروه ویژه اقدام مالی[۵]» بر شناسایی و انسداد مسیرهای تأمین مالی فعالیت‌های تروریستی، به‌ویژه از طریق فناوری‌های نوین مانند رمزارزها، شبکه‌های تاریک و سامانه‌های رمزگذاری‌شده، تمرکز دارند. عمده این اقدامات در قالب تحریم‌های مالی و اقتصادی هدفمند علیه اشخاص و نهادهای مظنون به فعالیت‌های تروریستی اعمال می‌شوند. با این حال، از منظر حقوقی، چنین تدابیری می‌توانند به‌صورت غیرمستقیم منجر به تحدید حقوق کاربران عادی و دسترسی مشروع آنان به فناوری‌های مجازی شوند؛ مسأله‌ای که کنوانسیون سازمان ملل متحد علیه جرایم سایبری درصدد پیشگیری از آن، از طریق طراحی سازوکارهای نظارتی شفاف، پاسخ‌گو و متناسب با اصول حقوق بشری است.

قطعنامه‌های شورای امنیت سازمان ملل متحد، از جمله قطعنامه‌های ۱۳۷۳[۶] و ۱۶۲۴[۷]، بر ضرورت تقویت همکاری‌های بین‌المللی و تدوین مقررات هماهنگ جهت سرکوب فعالیت‌های تروریستی در سکوهای مجازی تأکید دارند. کنوانسیون سازمان ملل متحد علیه جرایم سایبری نیز با اذعان به این ضرورت، توسعه چارچوب‌های حقوقی هم‌راستا میان دولت‌ها را در حوزه‌هایی نظیر اشتراک‌گذاری داده‌ها، هم‌افزایی اطلاعاتی، و ارتقای ظرفیت‌های

۱. در حال حاضر، به‌طور گسترده‌ای این اصل پذیرفته شده است که اعمال حاکمیت بر فضای مجازی ملی باید تمامی ابعاد آن، از ابعاد سخت‌افزاری تا نرم‌افزاری، را دربرگیرد. در این راستا، ابعاد سخت‌افزاری حاکمیت بر فضای مجازی در حال حاضر با استفاده بهینه از تجهیزات و نرم‌افزارها به‌طور فزاینده‌ای مورد توجه قرار می‌گیرد (علوی، حسینی و رامک، ۱۴۰۲، ص ۳۵).

2. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols, https://www.coe.int/en/web/cybercrime/the-budapest-convention

3. United Nations General Assembly. (2024, December 24). Resolution adopted by the General Assembly on the report of the Third Committee (A/79/460, para. 15): 79/243, https://docs.un.org/en/A/AC.291/L.15

4. United Nations. (1999, December 9). *International Convention for the Suppression of the Financing of Terrorism*. https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-11&chapter=18&clang=_en

5. Financial Action Task Force (FATF). (2021). *Opportunities and challenges of new technologies for AML/CFT*. FATF. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.html

6. United Nations Security Council. (2001, September 28). *Resolution 1373 (2001)*. Adopted at the 4385th meeting. https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf

7. United Nations Security Council. (2005, September 14). *Resolution 1624 (2005)*. Adopted at the 5261st meeting. https://digitallibrary.un.org/record/556538?v=pdf

نظارتی و قضایی داخلی مورد توجه قرار داده است. با این وجود، اجرای چنین تدابیری در برخی کشورها، به‌ویژه دولت‌هایی با وضعیت شکننده در حوزه حقوق بشر، می‌تواند زمینه‌ساز سوءاستفاده از ابزارهای نظارتی برای سرکوب مخالفان سیاسی، نقض آزادی بیان و تحدید حریم خصوصی گردد.

در سطح بین‌المللی، «اعلامیه جهانی حقوق بشر، مصوب ۱۹۴۸[1]» و «میثاق بین‌المللی حقوق مدنی و سیاسی، مصوب ۱۹۶۶[2]» به‌صراحت بر لزوم رعایت حقوق بشر در اقدامات ضدتروریستی تأکید دارند. در همین چارچوب، کنوانسیون ۲۰۲۴ نیز با اتخاذ رویکردی مبتنی بر حقوق بشر و اصل تناسب، تلاش کرده است استثناهای ممکن بر این حقوق را در روند سرکوب فعالیت‌های تروریستی در سکوهای مجازی تحدید سازد و آن ها را به‌طور صرف در چارچوب اصول ضرورت، تناسب و قانونی بودن تنظیم کند. از منظر اجرایی، کنوانسیون سازمان ملل متحد علیه جرایم سایبری به چالش‌های موجود در پیاده‌سازی تحریم‌ها و اقدامات نظارتی در بستر سکوهای مجازی، از جمله ناشناس‌بودن کاربران، پیچیدگی‌های رمزنگاری، تنوع قوانین داخلی کشورها و امکان دور زدن تحریم‌ها از طریق فناوری‌های پیشرفته، اشاره کرده است. در پاسخ به این چالش‌ها، این کنوانسیون بر تدوین استانداردهای جهانی، ارتقای توانمندی نهادهای ملی، و تقویت همکاری‌های چندسطحی قضایی و پلیسی در سطح بین‌المللی تأکید دارد (Fidler, 2025, p 764-766).

به‌طور کلی، اسناد بین‌المللی، به‌ویژه کنوانسیون بوداپست در مورد جرایم سایبری و کنوانسیون سازمان ملل متحد علیه جرایم سایبری، بر استفاده از ابزارهای حقوقی نظیر تحریم‌های هدفمند، رصد مالی مجازی، انسداد محتوای تروریستی و توسعه همکاری‌های حقوقی و فنی بین‌المللی برای سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی تمرکز دارند. با این حال، تحقق توأمان امنیت سکوهای مجازی و صیانت از حقوق بشر مستلزم تدوین سیاست‌های حقوقی منسجم، ایجاد سازوکارهای پاسخ‌گو و التزام به اصل حاکمیت قانون در سطوح ملی و فراملی است (ماتام‌فارال، ۱۳۹۹، ص۸۹-۸۶).

٦- تقویت همکاری‌های بین‌المللی در اجرای مؤثر تحریم‌ها؛ بایسته‌ها و ظرفیت چارچوب‌های حقوقی

ارتکاب جنایات فناورانه از سوی تروریست‌ها، شامل به‌کارگیری ابزارهای دیجیتالی به‌منظور برنامه‌ریزی، برقراری ارتباطات و جذب نیرو به گروه‌های تروریستی می‌باشد. سکوهای مجازی به‌عنوان ابزارهای اصلی در این فعالیت‌ها، برای نشر افکار افراطی و تأمین مالی به‌کار گرفته می‌شوند. این نوع فعالیت‌ها طبق چارچوب کنوانسیون بوداپست در خصوص جرایم سایبری و کنوانسیون سازمان ملل متحد علیه جرایم سایبری، به‌عنوان جرایم سایبری با اهداف تروریستی طبقه‌بندی می‌گردند.

به‌رغم این، اجرای مؤثر این تحریم‌ها با چالش‌هایی نظیر تعادل میان تأمین امنیت ملی و رعایت حقوق بشر، و همچنین تفاوت‌های سیاسی و حقوقی میان کشورهای مختلف، مواجه است. بنابراین، تقویت همکاری‌های بین‌المللی و هماهنگی در وضع و اجرای تحریم‌ها می‌تواند در کاهش این چالش‌ها و افزایش اثربخشی اقدامات پیشگیرانه تأثیرگذار باشد.

۶- ۱- همکاری‌های بین‌المللی در اجرای تحریم‌ها

در دنیای معاصر، استفاده از سکوهای مجازی به‌منظور گسترش فعالیت‌های تروریستی و تأمین منابع مالی، تهدیدات جدی برای امنیت جهانی به‌وجود آورده است[3]. موازین بین‌المللی کشورهای عضو را موظف به همکاری در سرکوب فعالیت‌های تروریستی در پرتو پذیرش کنوانسیون‌های بین‌المللی، نظیر کنوانسیون بین المللی راجع به سرکوب تأمین مالی تروریسم و کنوانسیون بوداپست در مورد جرایم سایبری، می‌سازد. این کنوانسیون‌ها کشورها را ملزم می‌کنند تا مقررات داخلی خود را به‌گونه‌ای تنظیم نمایند که سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی تسهیل شود[4].

تحریم‌های بین‌المللی، شامل انسداد دارایی‌ها و محدودیت‌های سفر، به‌عنوان ابزار مؤثری برای سرکوب تأمین منابع مالی تروریست‌ها به‌کار گرفته می‌شوند. با این حال، چالش‌هایی نظیر تضاد با حقوق بشر و تفاوت‌های مقررات ملی هم‌چنان باقی است که نیازمند هماهنگی بین‌المللی و توسعه چارچوب‌های قانونی هماهنگ و به‌روز می‌باشد. برای سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی، همکاری و تبادل اطلاعات میان کشورها ضروری است تا از یک‌سو امنیت جهانی تأمین گردد و از سوی دیگر، حقوق بشر نیز رعایت شود (Packin & Volovelsky, 2024, p 87-89).

1. United Nations General Assembly. (1948, December 10). *Universal Declaration of Human Rights* (General Assembly resolution 217 A). https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf
2. United Nations. (1966, December 16). *International Covenant on Civil and Political Rights*. United Nations Treaty Series. https://treaties.un.org/PAGES/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=TREATY
3. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
4. https://www.unodc.org/documents/terrorism/Publications/Legislative_Guide_Universal_Legal_Regime/English.pdf

کشورهای عضو وفق اسناد بین‌المللی موظف به همکاری در سرکوب جنایات تروریستی از طریق پذیرش و اجرای کنوانسیون‌های بین‌المللی هستند. از جمله مهم‌ترین این کنوانسیون‌ها، می‌توان به کنوانسیون بین‌المللی راجع به سرکوب تأمین مالی تروریسم و کنوانسیون بوداپست در مورد جرایم سایبری اشاره کرد که کشورهای عضو را ملزم به تنظیم قوانین داخلی به‌منظور پیشگیری از تأمین مالی فعالیت‌های تروریستی در سکوهای مجازی می‌سازند. شورای امنیت سازمان ملل متحد با تصویب تحریم‌های بین‌المللی علیه تروریست‌ها، نقش حیاتی در سرکوب تهدیدات تروریستی ایفا می‌کند. این تحریم‌ها به‌ویژه در زمینه سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی مؤثر بوده و می‌توانند شامل انسداد دارایی‌ها، محدودیت‌های سفر و ممنوعیت تعاملات اقتصادی باشند. وفق ماده ۳۹ منشور ملل متحد، در صورت شناسایی تهدیدات جهانی، شورای امنیت می‌تواند تحریم‌هایی را به‌طور الزامی علیه دولت‌ها و تروریست‌ها اعمال کند[1]. در ضمن، شورای امنیت با تصویب تحریم‌ها علیه تروریست‌ها، قادر است منابع مالی و فنی آن ها را تحدید کند (Wood, 2013, p 321-325).

مجمع عمومی سازمان ملل متحد در سرکوب فعالیت‌های تروریستی در سکوهای مجازی نقش مؤثری ایفا کرده است؛ اگرچه این نهاد قدرت اجرایی شورای امنیت را ندارد، اما از طریق تصویب قطعنامه‌ها و تسهیل همکاری‌های بین‌المللی، به تقویت سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی می‌پردازد[2]. مجمع عمومی در چارچوب هدف ایجاد توازنی میان امنیت جهانی و حقوق فردی، بر رعایت حقوق بشر و آزادی‌های فردی تأکید کرده و از کشورهای عضو می‌خواهد تا قوانین لازم برای انسداد محتوای تروریستی و پیشگیری از تأمین مالی فعالیت‌های تروریستی در سکوهای مجازی را تصویب کنند[3].

در عین حال، تضاد با حقوق بشر و پیچیدگی‌های فرامرزی سکوهای مجازی به‌عنوان یکی از چالش‌ها، ضرورت همکاری‌های بین‌المللی و هماهنگی قضائی را می‌طلبد. از اینرو، برای مؤثر بودن این تحریم‌ها، ضروری است که کشورها همکاری نزدیک و تبادل اطلاعات مستمر داشته باشند (Gul & Ullah, 2024, p 603-604). وانگهی، دولت‌ها باید چارچوب‌های قانونی هماهنگ و شیوه‌های نظارتی مؤثر بر سکوهای مجازی را توسعه دهند تا از بهره‌برداری تروریست‌ها از فناوری‌های نوین پیشگیری کنند.

اتحادیه اروپا در سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی، از طریق تقویت چارچوب‌های قانونی و نظارت بر سکوهای مجازی، اقدامات مؤثری اتخاذ کرده است[4]. بر اساس «قانون خدمات دیجیتال، مصوب ۲۰۲۲[5]»، اتحادیه اروپا سکوهای مجازی را موظف به شناسایی، حذف و پیشگیری از بازنشر محتوای تروریستی می‌کند[6]. علاوه بر این، در راستای مقابله با تأمین مالی فعالیت‌های تروریستی، اتحادیه اروپا اقدام به وضع قوانینی برای شفافیت مالی و تحدید دسترسی تروریست‌ها به منابع مالی نموده است[7]. اتحادیه اروپا همچنین تحریم‌های هدفمند علیه تروریست‌ها اعمال می‌کند که شامل انسداد دارایی‌ها و محدودیت‌های سفر می‌باشد. این اقدامات به‌ویژه در محدودیت استفاده تروریست‌ها از سکوهای مجازی مؤثر است. اتحادیه اروپا با تقویت همکاری‌های بین‌المللی و ظرفیت‌های نظارتی، به سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی پرداخته و در عین حال به حفظ حقوق بشر، از جمله آزادی بیان و حریم خصوصی، توجه ویژه دارد (Nave & Lane, 2023, p 9-10).

سازوکارهای اجرایی تحریم‌ها برای سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی به نظارت و اجرای مؤثر تحریم‌ها وابسته است. این تحریم‌ها عمدتاً از سوی نهادهای بین‌المللی نظیر سازمان ملل متحد و اتحادیه اروپا به‌منظور تحدید دسترسی تروریست‌ها به فناوری‌ها و سکوهای مجازی اعمال می‌شوند[8]. نظارت بر این تحریم‌ها توسط کمیته‌های ویژه و نهادهای نظارتی مستقل صورت می‌گیرد که انسداد دسترسی به سکوهای مجازی، رصد منابع مالی و نظارت بر تحریم‌های مرتبط با فناوری را شامل می‌شود. کشورهای عضو موظف به اجرای مؤثر تحریم‌ها مطابق با اصول

1. United Nations. (n.d.). *United Nations Charter, Chapter VII: Action with respect to threats to the peace, breaches of the peace, and acts of aggression (Article 39)*. https://www.un.org/en/about-us/un-charter/chapter-7

2. United Nations. (2018, April 20). *The United Nations Global Counter-Terrorism Strategy: Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy* (A/72/840). https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/a_72_840.pdf

3. United Nations. (2023, December 22). *Terrorism and human rights* (A/RES/78/210). Seventy-eighth session, agenda item 71(b). https://docs.un.org/en/A/RES/78/210

4. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

5. Digital Services Act (DSA), 2022.

6. European Union. (2022, October 19). *Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)*. PE/30/2022/REV/1. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/ita

7. https://edri.org/our-work/eu-attempt-to-regulate-big-tech/

8. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1711?p=emailAm8BW05SKQlvU&d=/10.1093/law:epil/9780199231690/law-9780199231690-e1711

حقوق بین‌الملل هستند و باید از سازوکارهای ملی برای نظارت و اجرای این تحریم‌ها بهره‌برداری کنند (Dowlah, 2025, p 52-54). اعمال تحریم‌ها باید با رعایت حقوق بشر و آزادی‌های اساسی انجام پذیرد و از نقض حقوق افراد غیرمرتبط پیشگیری شود.

به‌هر روی، در اجرای تحریم‌های بین‌المللی علیه جنایات فناورانه تروریست‌ها در سکوهای مجازی، حفظ تعادل میان امنیت جهانی و حقوق بشر از اهمیت حیاتی برخوردار است[1]. از یک سو، شورای امنیت سازمان ملل متحد و سایر نهادهای بین‌المللی برای سرکوب تهدیدات تروریستی ناشی از فناوری‌های نوین، به‌ویژه در سکوهای مجازی، تحریم‌هایی نظیر انسداد دارایی‌ها، محدودیت‌های سفر و ممنوعیت تعاملات اقتصادی را اعمال می‌کنند تا منابع مالی و فنی تروریست‌ها را تحدید سازند[2]. این تحریم‌ها به‌ویژه در زمینه سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی و استفاده از اینترنت برای تبلیغ، جذب نیرو و تأمین منابع مالی مؤثر واقع می‌شوند[3]. در ضمن، چالش اصلی در اجرای این تحریم‌ها، حفظ حقوق بشر، به‌ویژه آزادی‌های فردی و حریم خصوصی، است. نظارت بر فعالیت‌های برخط، تحدید دسترسی به اطلاعات و انسداد سکوها می‌تواند منجر به نقض حقوق اساسی شهروندان و آزادی‌های فردی گردد. به علاوه، اقدامات نظارتی و تحریمی باید به‌گونه‌ای طراحی شوند که از نقض حقوق بشر پیشگیری کرده و در عین حال با موازین بین‌المللی، به‌ویژه در زمینه آزادی بیان، حریم خصوصی و دادرسی منصفانه، هم‌راستا باشند (Stănciulescu Alexe, 2025, p 6-7). از این‌رو، برای پیشگیری از نقض حقوق بشر در اجرای تحریم‌ها، ضروری است که اقدامات حقوقی با دقت و توجه به اصل تناسب و ضرورت، و با رعایت تعادل میان هدف‌های امنیتی و محدودیت‌های اعمال‌شده بر حقوق فردی، انجام گیرد. همچنین، نظارت بین‌المللی بر اجرای تحریم‌ها و تقویت همکاری‌های قضائی میان کشورها می‌تواند به حفظ این تعادل کمک کند.

۶- ۲- همکاری‌های بین‌المللی برای ظرفیت‌سازی و تقویت تحریم‌ها

تحریم‌های بین‌المللی، به‌ویژه از طریق شورای امنیت ملل متحد و گروه ویژه اقدام مالی، با هدف تحدید منابع مالی و فناوری تروریست‌ها و پیشگیری از فعالیت‌های مجرمانه در سکوهای مجازی وضع می‌شود[4]. این تحریم‌ها شامل انسداد تراکنش‌ها، تحدید دسترسی به خدمات دیجیتالی و شبکه‌های مخفی است. با این حال، این تدابیر ممکن است با چالش‌هایی نظیر نقض حقوق بشر مواجه شوند. کنوانسیون‌های بین‌المللی نظیر کنوانسیون بوداپست و کنوانسیون سازمان ملل متحد در تلاش‌اند تا تدابیر امنیتی را با رعایت حقوق بشر هماهنگ کنند. همکاری‌های بین‌المللی در زمینه تبادل داده‌ها و تقویت ظرفیت‌های نظارتی و قضایی نیز به سرکوب فعالیت‌های تروریستی در سکوهای مجازی کمک می‌کند[5].

همکاری‌های اطلاعاتی و مالی میان دولت‌ها نقش حیاتی در شناسایی و انسداد منابع مالی جنایات فناورانه تروریست‌ها در سکوهای مجازی دارد و به‌طور عمده وفق قطعنامه‌های شورای امنیت و استانداردهای گروه ویژه اقدام مالی انجام می‌شود. این همکاری‌ها با تمرکز بر تبادل داده‌ها، ردیابی تراکنش‌های مشکوک و مهار جریان‌های مالی در بستر سکوهای مجازی، به مهار تأمین مالی فعالیت‌های تروریستی در سکوهای مجازی کمک می‌کنند[6]. با این حال، اجرای این تدابیر باید در چارچوب اصول حقوق بین‌الملل، از جمله حفظ حریم خصوصی و رعایت اصل تناسب، صورت گیرد[7]. نیل به موفقیت در راهبردهای مزبور، مستلزم توازن میان کارآمدی امنیتی و رعایت حقوق بشر است.

مؤسسات مالی و رمزارزها نقش اساسی در شناسایی تراکنش‌های مشکوک و تحدید دسترسی تروریست‌ها به سامانه‌های مالی دارند. بر اساس استانداردهای گروه ویژه اقدام مالی، این مؤسسات موظف به گزارش تراکنش‌های مشکوک هستند و باید با استفاده از فناوری‌های پیشرفته، از جمله ابزارهای شفاف‌سازی تراکنش‌ها، از سوءاستفاده‌های تروریستی پیشگیری کنند[8]. تحریم‌های بین‌المللی، به ویژه از سوی شورای امنیت و گروه ویژه اقدام مالی، در انسداد دارایی‌های تروریستی و محدودیت دسترسی

1. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_establishing_law_enforcement_web.pdf
2. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ict_oct_2021.pdf
3. https://discovery.ucl.ac.uk/id/eprint/10054303/1/Kavanagh%20Carr%20Bosco%20and%20Hadley%20final%20submitted%20copy.pdf.pdf
4. United Nations Security Council. (2019, March 28). *S/PV.8496: Seventy-fourth year, 8496th meeting*. https://docs.un.org/en/S/PV.8496
5. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted-technical-guide-2017.pdf
6. United Nations Security Council. (2025, January 10). *Letter dated 9 January 2025 from the President of the Security Council acting in the absence of a Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council* (S/2025/22). https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/n2500570.pdf
7. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_analytical_brief_on_ppps_cft_2023.pdf
8. https://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/FATF-Annual-Report-2021-2022.pdf

به سامانه‌های مالی مؤثر هستند. با این حال، اعمال این تدابیر باید با رعایت حقوق بشر، از جمله حریم خصوصی و اصل تناسب، انجام شود. کنوانسیون‌های بین‌المللی مانند کنوانسیون بوداپست در مورد جرایم سایبری و کنوانسیون سازمان ملل متحد علیه جرایم سایبری بر لزوم طراحی تدابیر نظارتی شفاف و متناسب تأکید دارند[1].

ایجاد برنامه‌های آموزشی و ظرفیت‌سازی برای مقامات حقوقی و مالی کشورهای مختلف، به‌ویژه در مواجهه با تهدیدات فناورانه، نقش اساسی در تقویت نظارت و اجرای مؤثر تحریم‌های بین‌المللی دارد. این برنامه‌ها، مطابق با استانداردهای بین‌المللی مانند گروه ویژه اقدام مالی و قطعنامه‌های شورای امنیت، به مقامات کمک می‌کنند تا توانمندی‌های خود را در شناسایی و سرکوب تهدیدات تروریستی بهبود بخشند. به منظور سرکوب تهدیدات ناشی از جنایات فناورانه تروریست‌ها در سکوهای مجازی، تحریم‌های بین‌المللی، به‌ویژه از طریق شورای امنیت سازمان ملل متحد و گروه ویژه اقدام مالی، برای تجدید منابع مالی و فناوری تروریست‌ها اعمال می‌شود[2] . این اقدامات ممکن است منجر به نقض حقوق بشر، به ویژه در زمینه حریم خصوصی، شوند (Ferreira, 2024, p 76). کنوانسیون‌هایی همچون کنوانسیون بوداپست در مورد جرایم سایبری و کنوانسیون سازمان ملل متحد علیه جرایم سایبری در تلاش‌اند تا تدابیر امنیتی را با رعایت حقوق بشر ترکیب کنند. همکاری‌های بین‌المللی در زمینه تبادل داده‌ها و تقویت نظارت، نقش حیاتی در شناسایی و انسداد منابع مالی فعالیت‌های تروریستی ایفا می‌کند. مؤسسات مالی و رمزارزها نیز به‌عنوان بازیگران اصلی در شناسایی تراکنش‌های مشکوک و تحدید دسترسی تروریست‌ها به سامانه‌های مالی شناخته می‌شوند. افزون بر این، توسعه برنامه‌های آموزشی برای مقامات حقوقی و مالی کشورهای مختلف، به‌ویژه در مواجهه با تهدیدات فناورانه، به تقویت توانمندی‌های اجرایی و نظارتی در این زمینه کمک خواهد کرد (Abikoye et al., 2024, p 1839-1840).

۷- نتیجه‌گیری

تروریست‌ها از طریق ارتکاب جنایات فناورانه، به بهره‌گیری از فناوری‌های نوین برای تبلیغ، جذب نیرو و اجرای عملیات تروریستی اطلاق می‌شود. تحریم‌ها علیه تروریست‌ها استفاده‌کننده از این فناوری‌ها، به‌طور معمول مشتمل بر محدودیت‌های اقتصادی و انسداد دسترسی به منابع فناورانه می‌باشند. عمده این تحریم‌ها از سوی نهادهایی مانند شورای امنیت سازمان ملل متحد و اتحادیه اروپا اعمال می‌شوند. البته، اجرای تحریم‌ها در سکوهای مجازی با چالش‌هایی همراه است؛چرا که تروریست‌ها می‌توانند از فناوری‌های رمزنگاری برای دور زدن این تحریم‌ها بهره‌برداری کنند.

بنابراین، برای اجرای مؤثر تحریم‌ها نیازمند همکاری بین‌المللی گسترده و توسعه ابزارهای نظارتی پیشرفته هستیم. سکوهای مجازی به دلیل غیرمتمرکز بودن و استفاده تروریست‌ها از فناوری‌های پیچیده، نظارت و اجرای تحریم‌ها را دشوار می‌سازد. برای مؤثر بودن تحریم‌ها، همکاری بین‌المللی و توسعه فناوری‌های شناسایی و نظارتی ضروری است. در این راستا، تقویت چارچوب‌های حقوقی و هماهنگی میان قوانین ملی و بین‌المللی به منظور سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی و اجرای تحریم‌ها در سکوهای مجازی از اهمیت قابل ملاحظه‌ای برخوردار است. به‌دلیل جهانی بودن اینترنت، هیچ کشوری به تنهایی قادر به سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی نیست و تحریم‌ها تنها در صورت هماهنگی و همکاری بین‌المللی و تبادل اطلاعات می‌توانند مؤثر واقع شوند. همکاری کشورها باید شامل تقویت ابزارهای نظارتی دیجیتالی، به اشتراک‌گذاری اطلاعات و آموزش نهادهای اجرایی باشد تا تحریم‌ها به‌طور مؤثرتر و سریع‌تر اعمال شوند.

همکاری‌های بین‌المللی در تبادل اطلاعات و ایجاد چارچوب‌های حقوقی هماهنگ نیز برای افزایش اثربخشی نظارت و سرکوب جنایات فناورانه تروریست‌ها در سکوهای مجازی حیاتی است. در ضمن، سرکوب چنین فعالیت‌هایی در سکوهای مجازی و تحریم‌های فناوری اطلاعات و نیز تحریم‌های رسانه‌ای و ارتباطی باید به‌گونه‌ای باشد که هم‌زمان امنیت جهانی را تأمین کند و حقوق بشر، به ویژه آزادی بیان و حریم خصوصی، را نیز رعایت نماید. به این ترتیب، مقررات و سیاست‌های متوازن باید برای سرکوب تهدیدات امنیتی و در عین حال حفظ حقوق اساسی افراد وضع شود.

منابع

[۱] خالقی، ابوالفتح و ثقفی، پریسا (۱۴۰۱). تحریم اینترنتی: کُنش یا واکنش کیفری در سطح حقوق بین‌الملل. پژوهش حقوق کیفری، ۱۱(۴۰)، ۱۲۵-۱۰۵.

[۲] ضیایی، سیدیاسر و محمدی‌ثقفی، علیرضا (۱۳۹۳). تحریم اشخاص حقیقی از منظر حقوق بین‌الملل با تأکید بر تحریم برخی اتباع ایرانی. مجله حقوقی دادگستری، ۷۸(۸۸)، ۱۷۸-۱۴۵.

1. https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention
2. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.coredownload.pdf

[۳] علوی، سیدحسین، حسینی، محمدرضا و رامک، مهراب (۱۴۰۲). بررسی چگونگی اِعمال حاکمیت بر قلمرو سایبری ملی به‌مثابه قدرت نَرم در پرتو حقوق بین‌الملل. مطالعات قدرت نَرم، ۱۳(۴)، ۵۴–۳۵.

[۴] گوردون، ریچارد، اسمیت، میشل و کورنل، تام (۱۴۰۰). حقوق تحریم. ترجمه سعید باغبان‌کندری. چاپ اول. تهران: اداره چاپ و انتشارت وزارت امورخارجه.

[۵] ماتام‌فارال، جرمی (۱۳۹۹). تحریم‌های سازمان ملل متحد و حاکمیت قانون. ترجمه مجید عباسی و احمدرضا عصاری. چاپ اول. تهران: بنیاد حقوقی میزان.

[۶] نمامیان، پیمان و حسینی، میرهادی (۱۴۰۲). سرکوب اقدام‌های تروریستی با تحریم‌های اقتصادی سازمان ملل متحد. پژوهش‌های حقوق اقتصادی و تجاری، ۱(۲)، ۱۷۲–۱۴۹.

[۷] نمامیان، پیمان و حسینی، میرهادی (۱۴۰۳). رویکردها و سازوکارهای رویارویی با پول‌شویی دیجیتالی در موازین بین‌المللی. پژوهش‌های حقوق مالی و اقتصادی، ۱(۲)، ۱۷۲–۱۴۹.

[8] Abikoye, B., Ebunlomo, U., Stanley Chidozie, A., Adesola O., & Ayodele, O. (2024). Regulatory compliance and efficiency in financial technologies: Challenges and innovations. World Journal of Advanced Research and Reviews, 23(1), 1830-1844.

[9] Adel, A. & Norouzifard, M. (2024). Weaponization of the growing cybercrimes inside the dark net: The question of detection and application. Big Data Cognition and Computation, 8(91), 1-37.

[10] Afina, Y., Buchser, M., Krasodomski, A., Rowe, J., Sun, N. & Wilkinson, R. (2024). Towards a global approach to digital platform regulation: Preserving openness amid the push for internet sovereignty (Research Paper). Chatham House, the Royal Institute of International Affairs. Digital Society Initiative.

[11] Antoniuk, D. (2024, July 19). US sanctions two members of Russian ‘Cyber Army’ hacktivist group. The Record. https://therecord.media/cyber-army-russia-us-sanctions

[12] Alavi, S.H.R. (2024). The evolution of cyber conflicts and its impact on international security: A comprehensive analysis [Tesi di laurea, Università degli Studi di Padova, Scuola di Economia e Scienze politiche, European and Global Studies]. https://thesis.unipd.it/retrieve/9ecfb519-e683-4fb6-8a26-a8d1d129bc21/Thesis-SeyedhamidrezaAlavi.pdf

[13] Al-Qarawee, H.H. (2015). The discourse of ISIS: Messages, propaganda, and indoctrination. In Monica Maggioni & Paolo Magri (Eds.), Twitter and jihad: The communication strategy of ISIS (pp. 145-166). ISPI. Via Clerici, 5.

[14] Bogdanova, I. (2022). The legality of unilateral economic sanctions under public international law. In Unilateral sanctions in international law and the enforcement of human rights: The impact of the principle of common concern of humankind (Vol. 9, pp. 59–158). Brill Nijhoff.

[15] Burgess, A., Hamilton, R. & Leuprecht, C. (2024). Terror on the blockchain: The emergent crypto-crime-terror nexus. In Doron Goldbarsht & Louis de Koker (Eds.), Financial crime, law and governance: Navigating challenges in different contexts (pp. 203-227). Springer.

[16] Chertoff, M., Bury, P. & Richterova, D. (2020). Bytes not waves: Information communication technologies, global jihadism, and counterterrorism. International Affairs, 96(5), 1305–1325.

[17] Davis, S. (2021). Economic sanctions, communication infrastructures, and the destruction of communicative sovereignty. In Sanctions as war: Anti-imperialist perspectives on American geo-economic strategy (Vol. 212, pp. 63–76). Brill.

[18] Dowlah, C. (2025). Economic and financial sanctions of the United States: Legal perspectives. In Economic and financial sanctions under international law (pp. 28-69). Cambridge University Press.

[19] Douhan, A. (2022). The changing nature of sanctions in the digital age. In Digital transformations in public international law (1st ed., Vol. 317, pp. 99–132). https://sanctionsplatform.ohchr.org/record/20981?ln=en&v=pdf

[20] De Silva De Alwis, R. (2025). Gendering the new international convention on cybercrimes and new norms on artificial intelligence and emerging technologies. Washington Journal of Law, Technology & Arts, 20(2), 1-41.

[21] Erickson, J.L. (2020). Punishing the violators? Arms embargoes and economic sanctions as tools of norm enforcement. Review of International Studies, 46(1), 96-120.

[22] Passalacqua, M. (2024). Online radicalization and cybersecurity: Case study - Belgium [PDF]. University of Bologna. Prepared for Cybersecurity & Cyber Warfare Courses.

[23] Packin, N.G. & Volovelsky, U. (2024). Digital assets, anti-money laundering, and counter financing of terrorism: An analysis of evolving regulations and enforcement in the era of NFTs. In N. G. Packin (Ed.), The Cambridge Handbook of Law and Policy for NFTs (pp. 78-102). Cambridge University Press.

[24] Purcell, J., Schantz, D. & Shire, J. (2023). Terrorism-related targeted financial sanctions. In C. A. El Khoury (Ed.), Countering the financing of terrorism: Good practices to enhance effectiveness (pp. 113-152). International Monetary Fund.

[25] Pytlak, A. & Lad, S. (2024). The UN Security Council discusses cyber threats to international security: Highlights and takeaways from a Security Council meeting on the cyber threat landscape and implications for international peace and security. The Henry L. Stimson Center. (April 15). https://www.stimson.org/2024/un-security-council-cyber-threats-to-international-security/

[26] Giumelli, F., Hoffmann, F. & Książczaková, A. (2021). The when, what, where and why of European Union sanctions. European Security, 30(1), 1-23.

[27] Gul, S. & Ullah, N. (2024). Cybersecurity and international law: Addressing state responsibility in a digitally interconnected world. International Journal of Human and Society (IJHS), 4(3), 601-609.

[28] Jayawickrama, N. (2017). The right to freedom of movement. In The judicial application of human rights law: National, regional and international jurisprudence (pp. 448–489). Cambridge University Press.

[29] Kuleshova, G. (2020). The legal basis of countering cyber-terrorism in Russia and in other countries from the standpoint of its social and political dimension. Russian Journal of Criminology, 14(1), 156-165.

[30] Kuzior, A., Tiutiunyk, I., Zielińska, A. & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies, 17(2), 220-239.

[31] Nave, E. & Lane, L. (2023). Countering online hate speech: How does human rights due diligence impact terms of service? Computer Law & Security Review, 51, 105884, 1-18.

[32] McDonnell, E. (2024). Challenging externalisation through the lens of the human right to leave. Netherlands International Law Review, 71(2), 119–154.

[33] Miao, M. (2024). Regulating digital platforms through sanctions. Washington International Law Journal, 33(2), 389-452.

[34] Moiseienko, A. (2024). Crime and sanctions: Beyond sanctions as a foreign policy tool. German Law Journal, 25(1), 17-47.

[35] Faraji Dizaji, S. & Murshed, S.M. (2024). External arms embargoes and their implications for government expenditure, democracy, and internal conflict. World Development, 173, 106410, 1-17.

[36] Farber, S. (2025). The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. Security Journal, 38(29), 1-23.

[37] Fidler, D.P. (2016). Cyberspace, terrorism and international law. Journal of Conflict and Security Law, 21(3), 463-485.

[38] Fidler, M. (2025). Fragmentation of international cybercrime law. Utah Law Review, 3(4), 737–804.

[39] Ferreira, I.C. (2024). Description of the Financial Action Task Force. In The legal status of the Financial Action Task Force in the international legal system (Vol. 7, pp. 8-120). Brill Nijhoff.

[40] Tsesis, A. (2017). Social media accountability for terrorist propaganda. Fordham Law Review, 86(3), 605-631.

[41] Lombardo, G. & El Khoury, C. (2023). Investigating, prosecuting, and sanctioning terrorist financiers. In

Chady El Khoury (Ed.), Countering the financing of terrorism: Good practices to enhance effectiveness (pp. 89–112). International Monetary Fund.

[42] Lemnitzer, J.M. (2022). Back to the roots: The laws of neutrality and the future of due diligence in cyberspace. The European Journal of International Law, 33(3), 789–819.

[43] Li, E. (2019). Fighting the “Three Evils”: A structural analysis of counter-terrorism legal architecture in China. Emory International Law Review, 33(4), 311-365.

[44] Theodore, O. (2017). How international law can deal with lack of sanctions and binding targets in the Paris Agreement. Journal of Sustainable Development, 10(5), 225-241.

[45] Tran, D. (2018). The law of attribution: Rules for attributing the source of a cyber-attack. Yale Journal of Law & Technology, 20(3), 376-441.

[46] Wood, M. (2013). The role of the UN Security Council in relation to the use of force against terrorists. In Larissa van den Herik & Nico Schrijver (Eds.), Counter-terrorism strategies in a fragmented international legal order: Meeting the challenges (pp. 317-333). Cambridge University Press.

[47] Stănciulescu, A. & Andreea, A.M. (2025). Impact of digital platforms on individual rights. In Encyclopedia of contemporary constitutionalism (pp. 1–10). Latest edition.