



A Comparative Assessment of the Balance between the Effectiveness of Economic Sanctions against Digital Terrorists on Social Networks and Compliance with Human Rights Standards

ARTICLE INFO

DOI: 10.48311/clr.2026.120416.82826

Article Type

Research Article

Authors:

¹ Peyman Namamian*

<https://orcid.org/0000-0001-7681-7293> 

² Jabar Issayan

<https://orcid.org/0000-0001-8780-4383> 

Affiliation:

¹ Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran

² Postdoctoral Researcher in International Sanctions Law, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran

Correspondence:

Email: p-namamian@araku.ac.ir

Article History:

Received: 2026/05/12

Received in Revised form: 2026/07/29

Accepted: 2026/08/09

Abstract

The rapid evolution of communication technologies and the dominance of social networks have fundamentally transformed social and political dynamics. They have also turned the digital ecosystem into an emerging arena for digital terrorists to propagate extremism, recruit operatives, organize operations, and facilitate financial flows. This development clearly exposes the inadequacy of traditional, hard-security-oriented models and renders the transition to comprehensive and interdisciplinary approaches inevitable. From an evaluative standpoint, although the implementation of targeted economic sanctions is considered a fundamental mechanism for blocking the financial lifelines of digital terrorists, the emergence of advanced financial instruments such as crypto-assets and decentralized systems has introduced novel technical and legal complexities to enforcing these restrictions. From a comparative perspective, contrasting unilateral, security-centric approaches with models grounded in multilateral governance indicates that the tension between security imperatives and the protection of users' digital rights can only be resolved through the deployment of smart monitoring technologies, the strengthening of cross-border cooperation, and the establishment of independent oversight bodies. In this manner, counter-terrorism measures—while striking a balance between security, justice, and international human rights standards—will not infringe upon privacy and freedom of expression, thereby preserving the digital space as a secure, free, and trustworthy environment for all.

Keywords: Communication Technologies, Digital Rights and Privacy, Targeted Economic Sanctions, Digital Terrorists, International Cooperation and Regulatory Bodies, Human Rights Standards





سنجش تطبیقی توازن میان کارآمدی تحریم‌های اقتصادی علیه تروریست‌های دیجیتالی در فضای شبکه‌های اجتماعی و رعایت موازن حقوق بشری

پیمان نامامیان^{۱*}، جبار عیسائییان^۲

۱. دانشیار حقوق کیفری و جرم‌شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران.
۲. پژوهشگر پس‌دکتری حقوق تحریم‌های بین‌المللی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران.

تاریخ پذیرش: ۱۴۰۵/۰۵/۱۸

تاریخ بازنگری: ۱۴۰۵/۰۵/۰۷

تاریخ ارسال: ۱۴۰۵/۰۲/۲۲

چکیده

تحول شتابان فناوری‌های ارتباطی و تسلط شبکه‌های اجتماعی، علاوه بر دگرگونی بنیادین در مناسبات اجتماعی و سیاسی، زیست‌بوم دیجیتالی را به بستر نوظهور گنجش‌گری تروریست‌های دیجیتالی برای اشاعه افراط‌گرایی، جذب نیرو، سازماندهی عملیات و تسهیل جریان‌های مالی بدل کرده است؛ امری که آشکارا ناکارآمدی الگوهای سنتی و سخت‌امنیت‌محور را آشکار ساخته و گذار به رویکردهای جامع و میان‌رشته‌ای را اجتناب‌ناپذیر می‌سازد. در مقام سنجش، اگرچه به‌کارگیری تحریم‌های اقتصادی هدفمند راهکاری بنیادین برای انسداد جریان‌های مالی تروریست‌های دیجیتالی محسوب می‌شود، ظهور ابزارهای پیشرفته مالی نظیر دارایی‌های رمزنگاری‌شده و نظام‌های غیرمتمرکز، پیچیدگی‌های فنی و حقوقی نوینی در مسیر اجرای این محدودیت‌ها پدید آورده است. از منظر تطبیقی، مقایسه رویکردهای امنیت‌گرایی یک‌جانبه با الگوهای مبتنی بر حکمرانی چندجانبه حاکی از آن است که تقابل میان الزامات

Email: p-namamian@araku.ac.ir

* نویسنده مسئول مقاله:



که‌ی‌رایت © ۲۰۲۶، انتشارات دانشگاه تربیت مدرس (TMU Press). این مقاله به‌صورت دسترسی آزاد منتشر شده و تحت مجوز بین‌المللی Creative Commons Attribution-NonCommercial 4.0 قرار دارد. بر اساس این مجوز، شما می‌توانید این مطلب را در هر قالب و رسانه‌ای کپی، بازتشر و بازآفرینی کنید و یا آن را ویرایش و بازسازی نمایید، به شرط آنکه نام نویسنده را ذکر کرده و از آن برای مقاصد غیرتجاری استفاده کنید.



دفاعی و صیانت از حقوق دیجیتال کاربران تنها از طریق به‌کارگیری فناوری‌های رصد هوشمند، تقویت همکاری‌های فرامرزی و ایجاد نهادهای مستقل نظارتی حل‌وفصل می‌شود؛ به‌گونه‌ای که تدابیر ضدتروریستی، ضمن برقراری تعادل میان امنیت، عدالت و موازین بین‌المللی حقوق بشر، حریم خصوصی و آزادی بیان را خدشه‌دار نکرده و فضای دیجیتال را به‌عنوان محیطی امن، آزاد و قابل‌اعتماد برای همگان حفظ نمایند.

واژگان کلیدی: فناوری‌های ارتباطی، حقوق دیجیتال و حریم خصوصی، تحریم‌های اقتصادی هدفمند، تروریست‌های دیجیتالی، همکاری‌های بین‌المللی و نهادهای نظارتی، موازین حقوق بشری.

۱. مقدمه

دگردیسی بنیادین در الگوهای ارتباطاتی و ظهور بی‌سابقه شبکه‌های اجتماعی در بسترهای نوین ارتباطی، زیرساخت‌های تعاملات جوامع معاصر را در ابعاد گوناگون مدنی، تجاری و حاکمیتی دستخوش بازتعریف عمیقی کرده است. این فضای مجازی تعاملی اگرچه مجاری نوینی را برای همگرایی‌های جهانی و جریان آزاد اطلاعات ایجاد نموده، هم‌زمان به بستری مناسب جهت زایش و بازتولید مخاطرات امنیتی غیرمتعارف تبدیل شده است؛ پدیده‌ای که در قالب «تروریسم دیجیتالی» تجلی یافته و در آن جریان‌های تکفیری و افراط‌گرا با سوءاستفاده از این شاهراه‌های ارتباطی، اهداف خرابکارانه خود را پیش می‌برند. این ساختارهای فرامرزی با به‌کارگیری هدفمند رسانه‌های اجتماعی، پیام‌رسان‌های رمزنگاری‌شده و درگاه‌های مبادلات مالی غیرمتمرکز، فرآیندهایی نظیر عضوگیری، ترویج اندیشه‌های رادیکال، هماهنگی‌های تاکتیکی و جذب منابع مالی را فراتر از حوزه‌های صلاحیت سرزمینی سنتی سازمان‌دهی می‌کنند. در تحلیل این فرآیند، آشکار می‌شود که راهبردهای کلاسیک مقابله با تروریسم که تمرکز محوری آن‌ها بر قدرت سخت نظامی و ابزارهای سخت‌افزاری امنیتی استوار بود، کارآمدی یکپارچه خود را در مواجهه با این تهدیدهای متکثر و سیال از دست داده‌اند و ضرورت طراحی و استقرار سازوکارهای همه‌جانبه، به‌ویژه در حوزه‌های حقوقی و مالی



بین‌المللی، بیش از پیش برجسته شده است (Pajuste, 2022: 31-34).

در این راستا، تحدید جریان‌های اقتصادی و اعمال تحریم‌های مالی هدفمند در زمرهٔ اساسی‌ترین راهبردهای صیانت امنیتی در دهه‌های اخیر قلمداد می‌شود که هدف بنیادین آن، فلج ساختن توان عملیاتی تروریست‌های دیجیتالی از طریق انسداد دسترسی آن‌ها به منابع پایدار مالی است. با وجود این، گذار ساختاری این شبکه‌های افراطی از سازوکارهای سنتی انتقال پول به اتمسفر تراکنش‌های دیجیتال، کاربست مؤثر این ابزارهای تنبیهی را با چالش‌های فنی و حقوقی نوظهوری روبه‌رو کرده است. تغییرپذیری و انعطاف‌پذیری رسانه‌های اجتماعی، سرعت آنی انتقال کلان‌داده‌ها و تکوین فناوری‌های زنجیره بلوکی و رمزارزهای ناشناس، کارشناسان را در ردیابی و انسداد شبکه‌های پشتیبانی مالی با بن‌بست‌های جدی مواجه ساخته است (Hussein, 2023: 114). ارزیابی‌های سنجشی نشان می‌دهند که سامانه‌های نظارتی گذشته که بر بستر بانکداری متمرکز دولتی قوام یافته بودند، در تحلیل رفتارهای مالی غیرمتمرکز در فضای دیجیتالی با کاهش کارایی مواجه شده و نیازمند بازنگری ساختاری هستند.

با وجود ضرورت مبارزه با این تهدیدها، اعمال تحریم‌های اقتصادی دیجیتال به‌طور اجتناب‌ناپذیری با اصول بنیادین حقوق بشر تلاقی پیدا می‌کند، چراکه در سناریوهای متعددی، این تحریم‌ها فراتر از دایرهٔ عاملان هدف عمل کرده و حقوق ارتباطی و معیشتی کاربران غیرنظامی و شهروندان عادی را به‌صورت فراگیر تحت تأثیر منفی قرار می‌دهند. این وضعیت نامطلوب سبب سلب حقوق اساسی، نظیر آزادی بیان، حریم خصوصی و دسترسی منصفانه به زیرساخت‌های حیاتی فناوری اطلاعات می‌گردد؛ از این‌رو، چالش اصلی این پژوهش چگونگی تعادل‌بخشی میان کارآمدی تدابیر امنیتی و پاسداشت حقوق شهروندی در بستر شبکه‌های اجتماعی است. از منظر روش‌شناختی و سنجشی، بررسی تجربه‌های تاریخی یک دههٔ گذشته نشان می‌دهد که حل این تعارض در گرو پی‌ریزی یک نظام همکاری چندجانبه میان دولت‌ها، ائتلاف بزرگ فناوری و نهادهای ناظر بین‌المللی است که در آن با به‌کارگیری فناوری‌های هوشمند، مانند تحلیل کلان‌داده‌ها و هوش مصنوعی، الگوهای تروریستی



به‌صورت دقیق و هدفمند شناسایی شوند تا ضمن مهار جریان‌های مالی تروریستی، تضمین‌های حقوق بشری صیانت شده و از رفتارهای انقباضی و اعمال تحریم‌های فراگیر پیشگیری به عمل آید.

این پژوهش با هدف سنجش تطبیقی توازن میان کارآمدی تحریم‌های اقتصادی علیه تروریست‌های دیجیتالی در شبکه‌های اجتماعی و رعایت موازین حقوق بشری، به بررسی ارتباط میان تروریسم دیجیتالی، بسترهای اجتماعی برخط و سازوکارهای تحریمی می‌پردازد. پرسش اصلی پژوهش این است که «چگونه می‌توان تحریم‌های اقتصادی علیه تروریست‌های دیجیتالی را در شبکه‌های اجتماعی به‌گونه‌ای طراحی و اجرا کرد که ضمن برخورداری از کارآمدی لازم در مهار منابع مالی آنان، با اصول و تضمین‌های بنیادین حقوق بشر نیز سازگار باشد؟». اهمیت این موضوع از آن‌روست که فقدان چارچوب‌های حقوقی و اجرایی روشن در این حوزه می‌تواند به اتخاذ تدابیری امنیتی منجر شود که پیامدهایی نظیر تحدید آزادی بیان، نقض حریم خصوصی و محرومیت ناعادلانه برخی کاربران از خدمات دیجیتال را به دنبال داشته باشد. از این‌رو، پژوهش حاضر با رویکردی توصیفی-تحلیلی و بر پایه مطالعه اسناد، مقررات و سیاست‌های بین‌المللی، همراه با تحلیل تطبیقی تجربه‌های یک دهه اخیر، تقریر یافته است. به‌علاوه، نقش همکاری میان دولت‌ها، شرکت‌های فناوری و نهادهای بین‌المللی، و نیز ظرفیت ابزارهایی مانند کلان‌داده و هوش مصنوعی در شناسایی و مهار جریان‌های مالی مرتبط با تروریسم دیجیتالی، مورد توجه قرار گرفته است. همچنین، یافته‌های پژوهش درصدد ارائه چارچوبی منسجم برای اعمال تحریم‌های هدفمند، شفاف و مسئولیت‌پذیر در این حوزه است.

۲. پیشینه و تحولات

تحولات شتابان فناوری اطلاعات و ارتباطات در دهه‌های اخیر، ماهیت تهدیدهای امنیتی را دگرگون کرده که در این میان، فعالیت‌های تروریست‌ها در سکوه‌های دیجیتالی به‌تدریج در کنار گونه‌های سنتی تروریسم مطرح شده و چارچوب‌های موجود تحلیل و تنظیم‌گری را با مسائل

نوینی مواجه کرده است (نمایان و شهبازی، ۱۴۰۴: ۸۵-۸۶). در الگوی سنتی، کنش‌های تروریستی به صورت عملیات فیزیکی، از قبیل بمب‌گذاری، هواپیماربابی یا حملات مسلحانه، تحقق می‌یافت و مقررات بین‌المللی نیز اغلب با فرض همین سنخ تهدیدها شکل گرفته بودند. با گسترش اینترنت و توسعه زیرساخت‌های ارتباطی جهانی در دهه ۱۹۹۰، به‌ویژه پس از تجاری‌شدن اینترنت در سال ۱۹۹۵، فضای دیجیتال به بستری برای بروز تهدیدهای نوین تبدیل شد. در این چارچوب، تروریسم دیجیتالی به معنای بهره‌گیری هدفمند از ابزارهای دیجیتال و فناوری‌های ارتباطی برای ایجاد هراس عمومی، اختلال در خدمات حیاتی، اثرگذاری بر افکار عمومی و تقویت ظرفیت عملیاتی تروریست‌های دیجیتالی تبیین می‌شود (Douhan, 2022: 126). این پدیده، مرز میان جرایم دیجیتالی، جنگ اطلاعاتی و اقدامات تروریستی را مبهم کرده و نظام‌های حقوقی را در تعیین مسئولیت‌ها، تعریف رفتارهای مجرمانه و احراز صلاحیت قضایی با دشواری مواجه ساخته است. «کنوانسیون بوداپست راجع به جرایم سایبری» مصوب ۲۰۰۱ شورای اروپا، از نخستین تلاش‌های بین‌المللی برای تقویت همکاری دولت‌ها در مقابله با جرایم مرتبط با فناوری اطلاعات به شمار می‌آید. با این حال، پاسخ حقوقی به تروریست‌های دیجیتالی، از جمله تحریم‌ها و سیاست‌های ضدتروریستی در محیط برخط، نباید به نقض حقوق بنیادین بشر منتهی شود و باید با رعایت حق حریم خصوصی، آزادی بیان و دسترسی به اطلاعات، و با اتکا به اسناد بین‌المللی، نظیر منشور ملل متحد و اعلامیه جهانی حقوق بشر پیگیری گردد (Razmetaeva, 2022: 51).

از سوی دیگر، تحریم‌های اقتصادی علیه تروریست‌های دیجیتالی و فعالیت آنان در شبکه‌های اجتماعی، به یکی از چالش‌های مهم بین‌المللی تبدیل شده است (نمایان، ۱۴۰۳: ۲۲۰-۲۲۱). از دهه ۲۰۰۰ و به‌ویژه پس از حملات ۱۱ سپتامبر ۲۰۰۱، دولت‌ها برای مقابله با تروریست‌ها به ابزار تحریم متوسل شدند و شورای امنیت نیز با قطعنامه ۱۳۷۳ دولت‌ها را به انسداد منابع مالی تروریست‌های دیجیتالی ملزم کرد.^۱ در گسترش فعالیت‌های تروریستی در

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



سکوهاى دیجیتالى، چند عامل نقش محوری دارد؛ نخست، افزایش وابستگى دولت‌ها و جوامع به زیرساخت‌هاى دیجیتالى، به‌گونه‌اى که شبکه‌هاى انرژی، نظام‌هاى بانكى، حمل‌ونقل و خدمات درمانى به سامانه‌هاى رایانه‌اى و شبکه‌هاى ارتباطى متكى شده و همین امر آسیب‌پذیرى آن‌ها را در قبال حملات دیجیتالى تشدید کرده است؛ حمله دیجیتالى به شبکه برق اوکراین در ۲۳ دسامبر ۲۰۱۵ که قطع برق حدود ۲۳۰ هزار نفر را در پی داشت، نمونه‌اى روشن از این وضعیت است. دوم، گسترش دسترسی به ابزارهاى نفوذ دیجیتالى و دانش فنى نسبت به گذشته است؛^۲ روندی که پس از انتشار مجموعه‌اى از ابزارهاى نفوذ آژانس امنیت ملی ایالات متحده توسط گروه هکری «شادوبروکرز»^۳ توجه گسترده کارشناسان امنیت دیجیتالى را برانگیخت. سوم، گسترش شبکه‌هاى اجتماعى و بسترهاى برخط، بسترسان انتشار پرشتاب اطلاعات، ساماندهى مخاطبان و بازتولید و تثبیت روایت‌هاى سیاسى شده است؛ ایجاد سکوهاى مانند فیس‌بوک در ۴ فوریه ۲۰۰۴، یوتیوب در ۱۴ فوریه ۲۰۰۵ و توییتر در ۲۱ مارس ۲۰۰۶، فضای دیجیتالى را به یکى از مهم‌ترین عرصه‌هاى اثرگذاری بر افکار عمومى

۲. در سال ۲۰۱۷ اوکراین هدف مجموعه‌اى از حملات دیجیتالى گسترده قرار گرفت که بخش‌هاى از زیرساخت‌هاى حیاتی، ازجمله شبکه برق این کشور را با اختلال مواجه کرد. این رویدادها به‌عنوان یکى از نمونه‌هاى مهم حملات دیجیتالى هدفمند علیه زیرساخت‌هاى حیاتی در سطح بین‌المللى مورد توجه قرار گرفته‌اند. <https://www.reuters.com/article/us-ukraine-cyber-attacks-idUSKBN19111J/> بررسی‌ها حاکی از سازمان‌دهى حملات دیجیتالى پیشرفته‌اى است که با فریب کاربران و نفوذ به زیرساخت‌هاى توزیع برق، موجب قطع گسترده جریان الکتریسیته شدند. این تهاجمات مخرب با از کار انداختن سامانه‌هاى کنترلى و انهدام داده‌هاى حیاتی، اطلاع‌رسانى به شهروندان را نیز مختل کردند. برآیند این اقدامات، تحمیل هزینه‌هاى سنگین مالی و توقف موقت خدمات عمومى در ابعاد وسیع بود

- Cybersecurity and Infrastructure Security Agency. (2021, July 20). Cyber-attack against Ukrainian critical infrastructure (IR-ALERT-H-16-056-01). Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>

۳. گروه «شادوبروکرز» (The Shadow Brokers)، گروهى هکری است که نخستین بار در تابستان سال ۲۰۱۶ ظاهر شد. این گروه چندین افشاگرى منتشر کرد که شامل ابزارهاى هک متعلق به آژانس امنیت ملی ایالات متحده (NSA) بود. این ابزارها در عملیات‌هاى نفوذ دیجیتالى استفاده مى‌شدند و انتشار آن‌ها توجه گسترده‌اى را در حوزه امنیت دیجیتالى برانگیخت؛

- <https://malpedia.caad.fkie.fraunhofer.de/actor>.

و انتشار پیام‌های سیاسی و اعتقادی تبدیل کرده است (Sharlamanov & Petreska, 2024: 8-9).

سنجش تجربه‌های عملی نشان می‌دهد که تروریست‌ها به‌طور فعال از این بسترها برای پیشبرد اهداف خود استفاده کرده‌اند. یکی از نمونه‌های بارز در این زمینه فعالیت‌های تروریست‌ها موسوم به «دولت اسلامی» (داعش) است که در فاصله ژوئن ۲۰۱۴ تا مارس ۲۰۱۹ از شبکه‌های اجتماعی و پیام‌رسان‌هایی مانند توئیتر، تلگرام و یوتیوب برای انتشار گسترده پیام‌های تبلیغاتی و جذب نیرو بهره برد (Karimi, Squicciarini & Forster, 2024: 17). وفق «گزارش وضعیت و روندهای تروریسم در اتحادیه اروپا»^۴، بخش قابل‌توجهی از فعالیت‌های تبلیغاتی این تروریست‌ها در محیط‌های برخط انجام شده است. وانگهی، برخی تحقیقات قضایی در کشورهای اروپایی نشان داده‌اند که تعدادی از عاملان حملات تروریستی، ازجمله عاملان حملات پاریس در ۱۳ نوامبر ۲۰۱۵، پیش از اجرای عملیات با محتوای افراطی منتشرشده در فضای دیجیتال در ارتباط بوده‌اند. در ضمن «داعش» در فاصله سال‌های ۲۰۱۴ تا ۲۰۱۹ با استفاده هم‌زمان از سکوهایی همچون توئیتر، تلگرام، یوتیوب و راکت‌چت^۵ راهبرد «ارتباط چندسکویی» را به کار گرفت تا پیام‌های تبلیغاتی، تصاویر ایدئولوژیک و فراخوان‌های جذب نیرو را در سکوهایی گوناگون منتشر کند^۶ (Bolpagni & Fisher, 2026: 17-18). شایان گفتن است داعش که در بستر بحران سوریه در سال ۲۰۱۴ و در پی انشعاب از القاعده قدرت گرفت، با ادعای تشکیل خلافت در بخش‌هایی از عراق و سوریه به دنبال گسترش نفوذ خود بود. این تروریست‌ها با وجود رویکرد ایدئولوژیک سخت‌گیرانه، به‌طور گسترده از فناوری‌های ارتباطی و شبکه‌های اجتماعی برای تبلیغات، ایجاد فضای روانی مبتنی بر ترس و جذب نیرو استفاده کرد. انتشار تصاویر خشونت‌آمیز و مدیریت حساب‌های متعدد در شبکه‌های اجتماعی، بخشی از

4. Europol. (2015). European Union terrorism situation and trend report 2015 (TE-SAT 2015). Publications Office of the European Union. <https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2015>.

5. <https://www.rocket.chat>

6. Digital jihad: Online communication and violent. Academia.edu. https://www.academia.edu/Digital_Jihad_Online_Com.



راهبرد رسانه‌ای آن برای تأثیرگذاری بر افکار عمومی و جذب نیرو از کشورهای مختلف بود (زمانی‌فراهانی، ۱۴۰۰: ۲۷؛ عبداللهی و دیگران، ۱۳۹۵: ۵).

در ادبیات اخیر، تحریم‌های اقتصادی دیگر به‌طور صرف «ابزار سیاست خارجی» اطلاق نمی‌شوند، بلکه به‌عنوان پدیده‌ای چندوجهی در پیوند با حقوق بین‌المللی، حقوق بشر و حکمرانی دیجیتال تحلیل می‌گردند. در این چارچوب، برخی پژوهشگران تحریم‌های یک‌جانبه را دارای پیامدهای انسانی و اجتماعی گسترده اطلاق و حتی آن را در قالب مفهوم «تروریسم اقتصادی» قابل‌تبیین می‌دانند؛ زیرا این اقدامات می‌تواند با اهداف منشور ملل متحد و قواعد مشروعیت در نظام بین‌المللی تعارض پیدا کند (حیدرقلی‌زاده و دیگران، ۱۴۰۳: ۱۱۱۳). هم‌زمان، تحلیل تحریم‌ها در عصر دیجیتال نشان می‌دهد که دامنه اثرگذاری آن‌ها از تحدید تجارت سنتی فراتر رفته و با شبکه‌های داده، زیرساخت‌های فناوری و سازوکارهای نوین مالی گره خورده است؛ به‌گونه‌ای که تحریم‌ها ماهیتی پیچیده‌تر، چندلایه و فناورمحور پیدا کرده‌اند (Douhan, 2022: 99). این تحول مفهومی، زمینه را برای بازاندیشی در ظرفیت‌های حقوق بین‌المللی در مهار اقدامات قهری اقتصادی و طراحی سازوکارهای پاسخگوتر فراهم می‌سازد. از سوی دیگر، مطالعات راجع به تهدیدهای دیجیتالی حاکی از آن است که مقابله با چنین تهدیدهایی بدون لحاظ حقوق بنیادین انسان‌ها، با خطر گسترش کنترل‌های نامتناسب و نقض کرامت انسانی مواجه است؛ بنابراین برخی از محققان اذعان می‌دارند سیاست‌های کیفی و امنیتی باید با معیارهای حقوق بشری هم‌تراز شود (قاسمی و باقرزاده، ۱۳۹۴: ۲۲۷). در ضمن، هم‌زمان، ادبیات بین‌المللی بر اثرگذاری سکوها دیجیتالی بر آزادی بیان و حریم خصوصی و ضرورت تنظیم‌گری دقیق‌تر تأکید دارد (Alexe, 2025: 9) و حتی از ایده به‌کارگیری تحریم‌ها برای «تنظیم» رفتار سکوها سخن می‌گوید (Miao, 2024: 396). در سطح امنیتی، هم‌گرایی فزاینده میان مجرمان دیجیتالی و تروریست‌ها و نقش رمزارزها و شبکه تاریک، ضرورت بازطراحی سیاست‌ها و همکاری منعطف با بخش خصوصی را تقویت می‌کند (Farber, 2025: 11)، در حالی که پراکندگی قواعد بین‌المللی جرایم دیجیتالی مانعی برای پاسخ هماهنگ اطلاق می‌شود (Ibid, 12). به‌طور کلی یافته‌های ناظر به پژوهش‌های منتشرشده نشان می‌دهد



شکاف اصلی، فقدان چارچوب تلفیقی برای نسبت‌سنجی «تحریم»، «سکوه‌های مجازی» و «مقابله با جنایات فناورانه تروریستی» است.

تمایز بنیادی این پژوهش با پیشینه مطالعاتی، در تغییر کانون تحلیل از ابزارشناسی تحریم به مدیریت بحران‌های امنیتی دیجیتال نهفته است. در حالی که ادبیات موجود با رویکردی معرفت‌شناختی، به کالبد شکافی تحولات ساختاری و حقوقی خود نهاد تحریم به‌عنوان پدیده‌ای فناورمحور می‌پردازد، این پژوهش بر سنجش گنشگری تروریستی در فضای دیجیتالی تمرکز دارد. در این سنج تطبیقی، توسعه فناوری به‌مثابه بستر زایش تهدید (تسهیل جذب نیرو و تأمین مالی) توصیف می‌شود؛ از این‌رو، تحریم‌های هدفمند اقتصادی نه موضوعی مستقل، بلکه بازویی مهارکننده در کنار الزامات حقوق بشری تحلیل می‌گردند. درواقع، این پژوهش با رویکردی سنجشی، کارآمدی تحریم‌های اقتصادی علیه تروریست‌های دیجیتالی در شبکه‌های اجتماعی را در توازن با صیانت از آزادی‌های بنیادین کاربران ارزیابی می‌کند، در حالی که پیشینه مطالعاتی پژوهش، به تنظیم‌گری ساختار تحریم‌ها معطوف بوده است.

۳. توازن بین تحریم اقتصادی و حقوق بشر در شبکه‌های اجتماعی

پدیده تروریسم دیجیتالی بازتعریف‌کننده الگوهای سنتی تهدید است؛ چراکه تروریست‌های دیجیتالی به‌مثابه گروه‌های افراطی با گذار از ساختارهای فیزیکی به فضای مجازی روی آورده‌اند تا به جذب نیرو، انتشار تبلیغات افراط‌گرایانه، آموزش اعضا، تأمین مالی، هماهنگی عملیات و ایجاد ارباب روانی در سطح گسترده بپردازند.^۷ در این میان، تروریست‌هایی نظیر داعش و القاعده با بهره‌گیری راهبردی از سکوه‌های توییتر، تلگرام و یوتیوب و انتشار ماهنامه‌های الکترونیک همسو مانند «دابق»، بستری نوین برای انتشار عقاید خود ایجاد کردند (Msall & Lary, 2022: 49). البته این پدیده نشان می‌دهد که فناوری ارتباطی علاوه بر ارائه مجرای برای تروریست‌ها، ابزار رهگیری و پیشگیری را نیز در اختیار نهادهای امنیتی قرار می‌دهد. در پاسخ به این بحران فزاینده، شورای امنیت سازمان ملل متحد با تصویب

7. <https://www.frontiersin.org> > fpos.2025.1718396



قطعه‌نامه‌های ۲۱۷۸ (۲۰۱۴) و ۲۳۵۴ (۲۰۱۷) تلاش کرده است چارچوبی هنجاری برای انسداد فعالیت‌های دیجیتالی این تروریست‌ها و الزام دولت‌ها به همکاری با بخش خصوصی فناوری تدوین کند.^۸ با این حال، تعارض میان ماهیت فرامرزی اینترنت و دکترین حاکمیت سرزمینی ملی، چالش‌های بی‌سابقه‌ای در حقوق بین‌المللی ایجاد کرده است. اگرچه پیشینه حقوقی مقابله با بهره‌گیری‌های مجرمانه از زیرساخت‌های فناوری به اواخر دهه ۱۹۹۰ میلادی بازمی‌گردد (Chertoff, Bury & Richterova, 2020: 1316)، قطعه‌نامه ۱۳۷۳ شورای امنیت با ایجاد نظام جامع تحریمی و الزام کشورها به اتخاذ تدابیر پیشگیرانه مالی، نقطه عطفی در مهار منابع مادی این جریان‌ها به شمار می‌رود. در مجموع، توصیف حقوقی این وضعیت نشان می‌دهد که مقابله با تهدیدهای دیجیتال نیازمند هماهنگی میان رژیم‌های حاکمیتی و قواعد ناظر بر قلمرو غیرفیزیکی است.

تنظیم‌گری حقوقی در زیست‌بوم دیجیتال به‌ناچار با ضرورت صیانت از آزادی‌های بنیادین اصطکاک پیدا می‌کند. در نظام بین‌المللی حقوق بشر، اسنادی بنیادین نظیر «اعلامیه جهانی حقوق بشر، مصوب ۱۹۴۸»^۹ و «میثاق بین‌المللی حقوق مدنی و سیاسی، مصوب ۱۹۶۶»^{۱۰} به‌عنوان سپرهای حمایتی از آزادی بیان و حریم خصوصی شناخته می‌شوند. تفسیر عمومی شماره ۳۴ کمیته حقوق بشر سازمان ملل با تسری مفاد ماده ۱۹ میثاق به قلمرو دیجیتال، بر این قاعده صحه می‌گذارد که تحدید دسترسی کاربران باید تنها وفق اصول ضرورت، تناسب و حاکمیت قانون صورت گیرد. سنجش انتقادی این چارچوب‌ها در تلاقی با تدابیر ضدتروریستی، نشان‌دهنده تعارض بنیادین ساختاری است؛ جایی که تلاش برای برقراری امنیت دیجیتالی می‌تواند به نقض حریم شخصی کاربران منجر شود. در این راستا، «کنوانسیون سازمان ملل متحد علیه جرایم سایبری ۲۰۲۴» با اتخاذ رویکردی هنجاری، به

8. <https://www.un.org> > etc

9. 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>

10. 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&mtmsg_no=IV-4&src=TREATY

دنبال توازن میان رمزنگاری داده‌ها، هویت‌زدایی دیجیتال و لزوم همکاری‌های قضایی فرامرزی است (Fidler, 2025: 764–766). سنجش این سند نشان می‌دهد که حقوق بین‌المللی معاصر در تلاش است تا با ایجاد معیارهای همسان، ضمن احترام به حاکمیت ملی، مانع از سوءاستفاده از شکاف‌های قانونی در فضای شبکه تاریک شود. برآیند مطالعه این مقررات تأیید می‌کند که امنیت پایدار در فضای برخپ بدون رعایت اصول آزادی‌های اساسی تحقق نخواهد یافت.

محدودیت‌های اقتصادی و تحریمی علیه تروریست‌های دیجیتالی به‌عنوان گزینه‌هایی کم‌هزینه و جایگزین اقدامات خشن نظامی مطرح هستند. این رهیافت‌های پیشگیرانه در اسنادی نظیر «کنوانسیون بین‌المللی راجع به سرکوب تأمین مالی تروریسم، مصوب ۱۹۹۹»^{۱۱} و «دستورالعمل‌های گروه ویژه اقدام مالی»^{۱۲} منعکس شده‌اند که هدفشان انسداد جریان‌های مالی تروریست‌ها در قالب رمزارزها و کانال‌های رمزگذاری شده است. قابلیت‌های فنی دارایی‌های دیجیتال نظیر گمنامی، ساختار غیرمتمرکز و تبادلات فرامرزی، بستر مالی نوینی را برای تروریسم دیجیتالی در شبکه‌های اجتماعی فراهم ساخته است. اعمال مؤثر تحریم‌های اقتصادی و تدابیر کیفری علیه این پدیده، مستلزم اصلاحات تقنینی، همکاری‌های بین‌المللی و ارتقای دادرسی تخصصی، هم‌گام با صیانت از موازین بنیادین حقوق بشر و دادرسی منصفانه است (نبوی و صابر، ۱۳۹۹: ۱۸۳). با وجود این، ارزیابی و سنجش عملکرد این نظام‌های تحریمی نشان‌دهنده نواقص جدی در حوزه حقوق شهروندی است؛ پرونده معروف به «کادی»^{۱۳} در دیوان دادگستری اروپا (۲۰۰۸) آشکار ساخت که چگونه سازوکارهای تحریمی

11. 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

12. 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>

۱۳. پرونده «کادی» (Kadi) که در ۳ سپتامبر ۲۰۰۸ توسط دیوان دادگستری اتحادیه اروپا (ECJ) صادر شد (پرونده‌های تجميع‌شده C-402/05 و C-415/05 P)، یکی از آرای برجسته در زمینه حمایت از حقوق بشر در قبال



مبتنی بر تصمیمات اداری و امنیتی می‌توانند فاقد حداقل‌های دادرسی منصفانه، حق دفاع یا سازوکارهای بازنگری مستقل باشند (Alexe, 2025: 8).^{۱۴} علاوه بر این، تحریم‌های اقتصادی اغلب دارای اثرات جانبی نامطلوبی هستند که به قطع دسترسی کاربران عادی به خدمات اساسی فناوری می‌انجامد. چالش مضاعف دیگر، واگذاری تدریجی وظایف حاکمیتی نظارت و حذف محتوا به غول‌های خصوصی فناوری اطلاعات است؛ نهادهایی که تصمیمات یکجانبه آن‌ها در انسداد حساب‌ها بدون وجود شفافیت ساختاری و مسئولیت‌پذیری عمومی اتخاذ می‌شود (Kuleshova, 2020: 162). وانگهی، تقابل میان کارآمدی تحریم‌های اقتصادی و تضمین حقوق متهمان همچنان یکی از پیچیده‌ترین مسائل حقوق بین‌المللی معاصر است.

۴. سنجش موازنه تحریم‌های اقتصادی در کارآمدی مهار تروریست‌های دیجیتالی

پیشرفت‌های نوین فناورانه، نظیر شبکه‌های اجتماعی، هوش مصنوعی و اینترنت اشیا، علاوه بر تسهیل فعالیت‌های مالی تروریست‌های دیجیتالی، چالش‌های بنیادینی برای حریم خصوصی پدید آورده‌اند. از این رو، کاربست ابزارهای نظارتی و اعمال تحریم‌های اقتصادی هدفمند مستلزم ایجاد توازنی دقیق میان افزایش کارآمدی امنیتی و صیانت از حقوق بنیادین اشخاص در زمینه حفاظت از داده‌های شخصی و آزادی‌های فردی است (شجاعی و رحمانی، ۱۴۰۵: ۵۰-۴۹).

دگردیدی در ساختار ارتباطات جهانی و اتکای تام ساختارهای زیستی و حاکمیتی به زیست‌بوم‌های دیجیتال، ساحت نوظهوری را برای بازتعریف و توسعه راهبردهای عملیاتی هسته‌های تروریستی ایجاد کرده است. جریان‌های افراطی با بهره‌گیری از فرصت‌های بی‌مرز محیط مجازی، اقدامات خود را در عرصه‌های پویایی نظیر مهندسی عملیات، سربازگیری

تحریم‌های اعمال‌شده از سوی سازمان ملل متحد علیه اشخاص، و نیز درباره رابطه میان حقوق بین‌الملل و حقوق اروپایی به شمار می‌رود.

14. <https://eu.vlex.com>



فرامرزی، ترویج گفت‌وگوهای ستیزه‌جویانه و به‌ویژه شبکه‌سازی مالی برای لجستیک خشونت سامان داده‌اند؛ پدیده‌ای که الگوهای سنتی تهدید را به ساختاری غیرمتمرکز، سیال و عاری از جغرافیا مبدل ساخته است (Baris, 2025: 68). در قبال این پویایی‌های مخاطره‌آمیز، جامعه بین‌المللی و دولت‌ها به طراحی و کاربست طیفی متکثر از ابزارهای هنجاری، اطلاعاتی و اقتصادی روی آورده‌اند تا مجاری تنفسی این تروریست‌ها را مسدود سازند. در میان منظومه این تدابیر، سیاست‌های تحریمی هدفمند پولی و مالی نقشی محوری ایفا می‌کنند؛ زیرا این رویکرد پیشگیرانه با هدف قرار دادن جریان‌های تغذیه‌کننده مالی و از کار انداختن شبکه‌های پشتیبانی لجستیکی، به‌طور مستقیم ظرفیت ساختاری و توان عملیاتی تروریست‌ها را در فضای واقعی و مجازی تحلیل می‌برد (حیدرقلی‌زاده و دیگران، ۱۴۰۳: ۱۱۳۸). بدین ترتیب، تقابل با تروریسم نوین از میدان‌های نبرد فیزیکی به بسترهای تبادل داده و جریان‌های پولی منتقل شده است که نیازمند ابزارهای واکنشی منعطف و متناسب با ماهیت پویای فناوری است.

گسترش پهنه فعالیت تروریست‌های دیجیتالی، چالش ظرفیتی را در برقراری توازن میان ضرورت‌های امنیتی حاکمیت و صیانت از آزادی‌های اساسی شهروندان پدید آورده است. مداخلات حاکمیتی در فضای مجازی متضمن آن است که راهبردهای ضدتروریستی با اصول حقوق بشر، ازجمله آزادی بیان، حریم خصوصی و حق دسترسی آزاد به اطلاعات هم‌پوشانی منفی نداشته باشند و منجر به تحدید غیرموجه آزادی‌های مدنی نشوند (شاهمرادی، ۱۴۰۱: ۷۹-۸۱). وفق این مبنا، اسناد چندجانبه بین‌المللی بر ارتقای همکاری‌های بین‌دولتی و یکپارچه‌سازی هنجارهای ملی اصرار می‌ورزند. در این میان، سه‌گانه «کنوانسیون پالمو، مصوب ۱۹۹۹»، «کنوانسیون بوداپست در مورد جرایم سایبری، مصوب ۲۰۰۱»^{۱۵} و «کنوانسیون سازمان ملل متحد علیه جرایم سایبری، مصوب ۲۰۲۴» ارکان اصلی معماری حقوقی بین‌الملل را تشکیل می‌دهند که هدفشان تسهیل به اشتراک‌گذاری شواهد دیجیتال، هم‌گرایی قضایی و تأسیس استانداردهای واحد حقوقی است (McKeever, 2021: 441-).

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



470). هم‌راستا با این روند، قطعنامه‌های ۲۳۵۴ و ۲۳۹۶ شورای امنیت در کنار قطعنامه‌های ۲۴۷/۷۴ و ۲۸۲/۷۵ مجمع عمومی سازمان ملل، بر ضرورت تعاملات اطلاعاتی پیشگیرانه و هماهنگی در مهار سوءاستفاده از سکوها‌های برخط پافشاری دارند. در این مسیر، «کنوانسیون بوداپست در مورد جرایم سایبری، مصوب ۲۰۰۱» و «کنوانسیون سازمان ملل متحد علیه جرایم سایبری، مصوب ۲۰۲۴» در پی ایجاد نقطه تعادل میان صیانت از حریم فضای دیجیتالی و پاسداشت حقوق بشر هستند؛ به‌گونه‌ای که کنوانسیون ۲۰۲۴ با درک دگرگونی‌های پرشتاب فناوریانه، الگوی جامع در قبال تروریست‌های دیجیتالی ارائه کرده و هرگونه اقدام امنیتی را منوط به رعایت اصول بنیادین حقوق بشر می‌داند (De Silva De Alwis, 2025: 31-34).

در قلمرو حقوق بین‌المللی، رژیم‌های تحریمی، به‌عنوان اهرم‌های صیانت از صلح جهانی، ذیل ماده ۴۱ منشور ملل متحد نقشی اساسی دارند. نقطه عطف این رویکرد پس از وقایع ۱۱ سپتامبر با صدور قطعنامه ۱۳۷۳ (۲۰۰۱) جهت انسداد دارایی‌های تروریستی رقم خورد و متعاقب آن با قطعنامه ۲۲۵۳ (۲۰۱۵) برای مقابله با روش‌های نوین تأمین مالی تروریست‌ها مانند تراکنش‌های رمزارزی و دیجیتالی شبکه‌های تکفیری نظیر داعش و القاعده تکامل یافت (Moslemzadeh, 2013: 212). این دگردیسی هنجاری مبین آن است که قلمرو تحریم‌ها از مرزهای فیزیکی فراتر رفته و بازارهای مالی مجازی را نیز دربرگرفته است؛ با این‌حال، نبود اجماع جهانی بر سر تعریفی واحد از تروریسم دیجیتالی و تعارض منافع میان دولت‌ها و پیشگامان صنعت فناوری پیرامون حاکمیت داده‌ها، مانعی جدی در مسیر هم‌گرایی بین‌المللی است (یوسفی و دیگران، ۱۴۰۳: ۶۷-۸۰). این تعارضات ساختاری مانع از شکل‌گیری جبهه عملیاتی واحدی در پاسخ به تهدیدهای دیجیتالی غیرمتمرکز می‌شود. از سوی دیگر، مشروعیت حقوقی این رژیم‌ها در گرو پای‌بندی به اصول ضرورت و تناسب است؛ چراکه تحریم‌های مبهم یا فراتر از حد مجاز می‌توانند حق دسترسی به اطلاعات را مخدوش کرده و به پالایش محتوا منجر شوند (Almakky, 2023: 57). نمونه عینی تلاش برای موازنه میان سرکوب محتوای تروریستی برخط و حفظ آزادی‌های دیجیتالی، در مقررات ۲۰۲۱/۷۸۴ اتحادیه اروپا تبلور یافته است که در عین الزام سکوها به حذف سریع محتوای مجرمانه، سازوکار دادرسی



و حق اعتراض را تضمین می‌کند^{۱۶} تا از سوءاستفاده‌های احتمالی پیشگیری نماید (Gherbaoui, 2023: 8-9). با وجود این دستاوردها، چالش تعریف مفاهیمی نظیر «محتوای تروریستی» و «جرایم تروریستی» همچنان خطر تفسیرهای موسع و تضییع آزادی بیان را زنده نگه می‌دارد (Ayasreh, 2023: 438–439).

در سطح داخلی، کشورها الگوهای متفاوتی را برای مهار تهدیدهای دیجیتال اجرا کرده‌اند. ایالات متحده با استناد به «قانون اختیارات اقتصادی در شرایط اضطراری بین‌المللی، مصوب ۱۹۷۷»^{۱۷} و دستورات اجرایی ریاست‌جمهوری، به‌ویژه «دستور اجرایی ۱۳۶۹۴، مصوب ۲۰۱۵»^{۱۸} و اصلاحات آن در سال ۲۰۱۶، الگوی تحریم‌های یکجانبه علیه بازیگران مخرب دیجیتال را توسعه داد. در نقطه مقابل، اتحادیه اروپا طی سال ۲۰۱۹ چارچوبی هنجاری برای مقابله با حمله‌های دیجیتال از طریق انسداد دارایی‌ها و ممنوعیت تردد عاملان حملات بزرگی مانند «واناکرای و نات‌پتیا»^{۱۹} ایجاد کرد که مؤید اتکای این بلوک به بازدارندگی حقوقی - امنیتی است.^{۲۰} تحلیل تاریخی این روندها نشان می‌دهد که موازنه میان صیانت از امنیت و پاسداشت حقوق شهروندی تا چه حد لغزنده است؛ تصویب «قانون میهن‌پرستی ایالات متحده»^{۲۱} در آمریکا

16. Defined in: Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online (O.J. L 172, 17 March 2021, p. 79) [hereinafter 'Regulation (EU) 2021/784'], Article 2 (1).

17. International Emergency Economic Powers Act, Pub. L. No. 95–223, 50 U.S.C. § 1701 et seq. (1977). <https://www.cbp.gov/trade/ieepa-duty-refunds>

این قانون، به مثابه یکی از قوانین فدرال ایالات متحده آمریکا است که به رئیس‌جمهور اختیار می‌دهد فعالیت‌های اقتصادی و مالی بین‌المللی را در شرایط اضطراری ملی تنظیم یا محدود کند.

18. Obama, B. (2015, April 1). Executive Order 13694—Blocking the property of certain persons engaging in significant malicious cyber-enabled activities. <https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-malicious-cyber-enabled-activities>.

دستور اجرایی ۱۳۶۹۴ که در یکم آوریل ۲۰۱۵ توسط باراک اوباما امضا شد، با هدف تحدید گسترش فعالیت‌های دیجیتالی مخرب و مقابله با تهدیدهای ناشی از حملات دیجیتالی علیه ایالات متحده صادر گردید.

19. WannaCry & NotPetya

20. <https://www.consilium.europa.eu/policies>

21. Bush, G. W. (2001, October 26). USA PATRIOT Act. The White House Archives. <https://georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011026-5.html>



پس از ۱۱ سپتامبر ۲۰۰۱ نمونه بارزی است که اگرچه ظرفیت‌های پایش و رهگیری اطلاعاتی دولت را ارتقا بخشید، به دلیل نقض حریم خصوصی با انتقادهای گسترده‌ای مواجه شد و افشاگری‌های سال ۲۰۱۳ نیز بحران بی‌اعتمادی به نظارت‌های بی‌ضابطه را عمق بخشید (Broman, 2024: 1176). در این میان، رژیم‌های هدفمندتر تحریمی می‌توانند تعادل بهتری میان صیانت از امنیت و آزادی‌های مدنی پدید آورند و کنوانسیون‌های چندجانبه‌ای چون کنوانسیون بوداپست بستر تعاملات قضایی امن را هموارتر می‌سازند (Farber, 2025: 9). از منظر نظریه‌های امنیت دیجیتال، تحریم‌ها با افزایش هزینه‌های رفتار مخرب در پی بازدارندگی هستند، اما نظریه تعادل هشدار می‌دهد امنیت مطلق سرابی بیش نیست و کارآمدی ابزارهای تنبیهی به‌طور صرف از مجرای شفافیت حقوقی، هدفمندی و همسویی با استانداردهای حقوق بشری میسر است (Douhan, 2022: 104). تفاوت در دیدگاه‌ها مشهود است؛ جایی که واشنگتن بر تحریم‌های فناورانه و اقتصادی تکیه دارد و بروکسل می‌کوشد راهبردهای ضدتروریستی خود را با رژیم‌های حفاظتی سخت‌گیرانه‌ای نظیر مقررات عمومی حفاظت از داده‌ها^{۲۲} پیوند بزند (Miao, 2024: 437). در ضمن، توفیق و مشروعیت این ابزارهای امنیتی در گرو اتخاذ رویکردی چندجانبه، مبتنی بر حاکمیت قانون و حامی آزادی‌های بنیادین بشر است.

۵. انطباق‌سنجی توازن تحریم‌های اقتصادی علیه تروریست‌های دیجیتالی و حفاظت از حقوق کاربران

۲۲. مقررات عمومی حفاظت از داده‌های اتحادیه اروپا یکی از مهم‌ترین چارچوب‌های حقوقی برای صیانت از داده‌های شخصی در فضای دیجیتال به شمار می‌رود که از سال ۲۰۱۸ لازم‌الاجرا شده است. این مقررات با تأکید بر اصولی مانند پردازش منصفانه و شفاف داده‌ها، محدودیت در هدف جمع‌آوری اطلاعات و تضمین امنیت داده‌ها، تلاش می‌کند میان بهره‌گیری از فناوری‌های نوین و حمایت از حقوق بنیادین افراد تعادل برقرار کند. در بستر سنجش تطبیقی کارآمدی تحریم‌های اقتصادی علیه تروریست‌های دیجیتالی در شبکه‌های اجتماعی، این چارچوب نشان می‌دهد که مقابله با تهدیدهای دیجیتالی و فعالیت‌های تروریستی نباید به تضعیف حریم خصوصی و حقوق داده‌ای کاربران منجر شود، بلکه سیاست‌های امنیتی باید هم‌زمان با الزامات حقوق بشری طراحی و اجرا شوند (نماین، ۱۴۰۴: ۱۶۵-۱۶۶).

تحریم‌های اقتصادی در عصر حاضر از مرزهای سنتی مالی و تجاری عبور کرده و گستره‌ای از زیرساخت‌های دیجیتال و فناوریانه را درنوریده است. این محدودیت‌های نوین، دامنه وسیعی از ابزارهای حیاتی، نظیر سامانه‌های پرداخت الکترونیک، بسترهای رایانش ابری، برنامه‌ها و نرم‌افزارهای کاربردی، و شبکه‌های اجتماعی را تحت تأثیر قرار داده و پیامدهای مستقیمی بر امنیت دیجیتالی و آزادی تبادل اطلاعات برجای گذاشته‌اند. چالش محوری در این میان، سنجش میزان اثربخشی تحریم‌ها در خنثی‌سازی توان مالی و شبکه‌های تبلیغاتی تروریست‌های دیجیتالی است، به نحوی که کمترین هزینه یا آسیب متوجه حقوق شهروندان غیرنظامی و کُشگران مدنی گردد؛ امری که موفقیت آن به‌طور تام به نحوه اجرا، نظارت و پایش دقیق بستگی دارد. از این‌رو، پرسش بنیادین این است که «آیا طراحی تحریم‌ها می‌تواند به گونه‌ای باشد که ضمن هدف قرار دادن کارآمد منابع جریان‌های تروریستی، تعرضی به حقوق اساسی مردم عادی و فعالان جامعه مدنی صورت نگیرد؟». پاسخ به این پرسش مطلق نیست، زیرا کیفیت عملکرد هر الگوی تحریمی به‌طور مستقیم در گرو مهندسی دقیق، دامنه نفوذ و سازوکارهای نظارتی آن است که در صورت فقدان دقت، می‌تواند از ابزاری بازدارنده به اهرمی برای سرکوب تبدیل شود.

در عرصه بین‌المللی، فقدان هماهنگی مقررات ملی، پیچیدگی ماهوی فناوری‌های نوظهور و ضعف ظرفیت‌های نهادی، موانع عمده‌ای بر سر راه ایجاد اجماع جهانی برای مدیریت تهدیدهای دیجیتال ایجاد کرده‌اند. علاوه بر این، ملاحظات سیاسی، فشار هزینه‌های اقتصادی و دغدغه‌های مربوط به حاکمیت نظارتی، همگی بر کارایی تدابیر جمعی اثرگذار هستند (Rabitz, 2025: 7). با وجود این، مقابله با تهدیدهای تروریستی در فضای مجازی به‌طور صرف از مسیر تقویت همکاری‌های فرامرزی و هماهنگی سیاست‌ها در بستری که امنیت و حقوق بشر را مکمل یکدیگر بدانند، امکان‌پذیر است. چنین توازنی ایجاب می‌کند که راهکارهای ضدتروریستی نه تنها از نظر فنی و عملیاتی کارساز باشند، بلکه باید از مشروعیت حقوقی و اخلاقی نیز برخوردار باشند. از منظر حقوق بین‌المللی، ماده ۴۱ منشور ملل متحد، تحریم‌ها را به مثابه ابزاری غیرنظامی برای صیانت از صلح و امنیت جهانی مجاز می‌داند. واکاوی



تجربیات تحریم‌های هدفمند علیه تروریست‌هایی نظیر القاعده و داعش ذیل قطعنامه‌های ۱۲۶۷، ۱۳۷۳ و ۲۲۵۳ نشان می‌دهد که تمرکز دقیق بر اشخاص و نهادهای مشخص، نسبت به تحریم‌های جامع، به مراتب کارآمدتر و از حیث انسانی موجه‌تر است. برخلاف تحریم‌های فراگیر که در دهه ۱۹۹۰ بر عراق اعمال شد و علی‌رغم فشار شدید اقتصادی، تأثیر چندانی بر تغییر رفتار امنیتی نداشت و تنها به تخریب معیشت عمومی، تضعیف خدمات درمانی و نقض وسیع حقوق بشر انجامید (Radanliev, 2025: 63)، تحریم‌های هوشمند که دسترسی تروریست‌ها به منابع مالی یا سکویهای تبلیغاتی را هدف قرار می‌دهند، می‌توانند توان عملیاتی آنان را به‌طور واقعی محدود کنند.

با وجود این، اجرای این سیاست‌ها مستلزم پای‌بندی به اصول شفافیت، نظارت مستقل و دادرسی منصفانه است تا اصل ضرورت و تناسب مخدوش نشود. مقررات ضدتروریستی و ابزارهای نظارت دیجیتال، در صورت فقدان کنترل‌های حقوقی، خطر نقض گسترده آزادی‌های اساسی را تشدید می‌کنند؛ بنابراین، قواعد حقوق بشر باید همواره مبنای تدوین این سیاست‌ها باقی بماند (Albader, 2020: 36). امنیت دیجیتال و حقوق بشر لزوماً در تقابل ذاتی نیستند؛ اگرچه مهار منابع مالی و تبلیغاتی تروریسم به تقویت امنیت عمومی می‌انجامد، نظارت‌های گسترده و انسداد گسترده و غیرتفکیکی، اعتماد اجتماعی و امنیت اطلاعاتی را متزلزل می‌سازد. سنجش حقوقی این حوزه وفق معیارهای مشروعیت، ضرورت و تناسب استوار است که در آن اصولی مانند کمینه‌سازی داده، محدودیت هدف و مسئولیت‌پذیری نهادی، اصول راهنمای سیاست‌گذاری متوازن محسوب می‌شوند.^{۲۳} برای سنجش کارآمدی تحریم‌های اقتصادی، باید هم‌زمان چهار معیار تکیه بر مستندات معتبر، تحلیل دقیق توان تروریست‌ها، پایش اثرات مخرب بر حریم خصوصی و وجود سازوکارهای اعتراضی را لحاظ کرد. برخلاف الگوهای فراگیر، راهکارهای هوشمند و انتخابی که حقوق‌محور و نظارت‌پذیر هستند، نتایج بهینه‌تری به بار می‌آورند. این رویکرد، ضمن تضعیف تهدیدها، از انسداد ارتباطات مشروع و خفگی فضای

23. <https://www.undp.org/sites/g/files/zskgke326/files/2023-03/>

مدنی پیشگیری می‌کند.^{۲۴} به هر روی، اتخاذ سیاست‌های عدالت‌محور و متناسب، یگانه ضامن برقراری تعادلی پایدار میان ضرورت‌های امنیتی و حقوق بنیادین بشری در بستر پیچیده فناوری‌های نوین جهانی خواهد بود.

۶. نتیجه‌گیری

توسعه شتابان فناوری‌های نوین ارتباطی و همگرایی بی‌سابقه در بستر شبکه‌های اجتماعی، فضای دیجیتالی را از ابزار ساده تعاملی به زیست‌بومی پیچیده و چندلایه بدل ساخته است؛ قلمرویی نوین که تروریست‌های دیجیتالی با بهره‌گیری هوشمندانه از قابلیت‌های فرامرزی آن، به تبلیغ گفتمان‌های افراطی، جذب مستمر نیروهای مستعد، سازماندهی عملیات‌های راهبردی و تسهیل جریان‌های مالی مبادرت می‌ورزند. این تحول بنیادین در ماهیت تهدیدهای فراملی، آشکارا ناکارآمدی الگوهای سنتی امنیت‌محور و پاسخ‌های سخت نظامی را آشکار ساخته و ضرورت گذار به رویکردهای جامع و چندبعدی را اجتناب‌ناپذیر کرده است. در این میان، تحریم‌های اقتصادی، به‌عنوان ابزاری تکمیلی و بازدارنده، وارد کارزار مقابله با این پدیده‌ها شده‌اند، اما ظهور روش‌های پرداخت الکترونیکی غیرمتمرکز و دارایی‌های رمزنگاری‌شده، اثربخشی این سازوکارها را با چالش‌های فنی و حقوقی جدی مواجه کرده است. افزون بر این، اعمال چنین محدودیت‌هایی همواره با خطر نقض حقوق بنیادین کاربران، به‌ویژه حق حریم خصوصی و آزادی بیان همراه بوده و ضرورت اتخاذ رویکردی متوازن میان الزامات امنیت ملی و صیانت از آزادی‌های مدنی را دوچندان می‌سازد.

سنجش همه‌جانبه کارآمدی تحریم‌های مالی در سپهر دیجیتال، نیازمند واکاوی تطبیقی اسناد بین‌المللی و مقررات ملی است تا توازن میان مهار تهدیدها و صیانت از حقوق شهروندان ارزیابی شود. در سطح فراملی، اسنادی نظیر کنوانسیون بوداپست راجع به جرایم دیجیتال و قطعنامه‌های شورای امنیت سازمان ملل متحد، رعایت حقوق اساسی بشر را به‌عنوان

24. <https://www.oas.org/en/sms/cicte/docs/National-Cybersecurity-Strategies-Lessons-learned-and-reflections-ENG.pdf>



پیش‌شرط مشروعیت و اثربخشی اقدامات پیشگیرانه معرفی می‌کنند. در تحلیل تطبیقی با رویکردهای ملی، نظام‌های حقوقی توسعه‌یافته مانند چارچوب‌های مقرراتی ایالات متحده و سیاست‌های تحریمی اتحادیه اروپا تلاش دارند تا از طریق تدوین استانداردهای متمایز، میان ضرورت‌های دفاعی و حفظ آزادی‌های فردی تعادل برقرار سازند؛ هرچند در عمل، این تدابیر اغلب به دلیل ماهیت فرامرزی داده‌ها دچار تداخل صلاحیت می‌شوند. تجارب پیشین حاکی از آن است که کاربست تحریم‌های کور و همه‌جانبه، نه تنها هدف اصلی را محقق نمی‌سازد، بلکه شهروندان عادی را از دسترسی به اطلاعات آزاد محروم می‌کند؛ وانگهی، جایگزینی تحریم‌های هوشمند و نقطه‌ای که به صورت متمرکز منابع مالی تروریست‌های دیجیتالی را هدف قرار می‌دهند، اثربخشی راهبردی را به حداکثر می‌رساند.

استقرار حکمرانی قانون‌مدار و پایدار در فضای مجازی مستلزم بازطراحی ساختارهای نظارتی منعطفی است که بر اصولی بنیادین، نظیر ضرورت، تناسب، شفافیت تقنینی و نظارت مستقل قضایی استوار باشند. تحقق این مهم نیازمند به‌کارگیری ابزارهای هوش مصنوعی و تحلیل داده‌های کلان جهت شناسایی الگوهای پیچیده تأمین مالی تروریست‌های دیجیتالی است، مشروط بر آنکه حریم خصوصی کاربران، به‌عنوان اصلی خدشه‌ناپذیر، صیانت شود. به‌علاوه، ایجاد نهادهای تخصصی مستقل برای پایش مستمر پیامدهای حقوقی محدودیت‌های دیجیتالی و انتشار گزارش‌های دوره‌ای، گامی اساسی در راستای مسئولیت‌پذیری نهادهای حاکمیتی و اصلاح سیاست‌های عمومی به شمار می‌رود. وانگهی، تقویت همکاری‌های بین‌المللی در زمینه تبادل سریع ادله الکترونیکی و ظرفیت‌سازی آموزشی مشترک، بسترساز برقراری تعادل میان امنیت جمعی و آزادی‌های مدنی در زیست‌بوم دیجیتال خواهد بود. تحریم‌های اقتصادی مادامی می‌توانند ابزاری مشروع در مبارزه با تروریست‌های دیجیتالی باشند که در چارچوب حاکمیت قانون، دادرسی عادلانه و استانداردهای حقوق بشری اعمال گردند تا ضمن صیانت از آزادی بیان، امنیت دیجیتالی جامعه را تضمین نمایند.

بیانیه هوش مصنوعی:

در نگارش این مقاله، از هوش مصنوعی استفاده نشده است.

سهم نویسندگان:

«جبار عیسائی» پژوهشگر پسادکتری، در طراحی مطالعه، گردآوری داده‌ها، ارزیابی منابع و اطلاعات پژوهش، تهیه پیش‌نویس نخستین و بازبینی محتوایی پژوهش مشارکت داشته است. به‌علاوه، «پیمان نمایان»، استاد راهنما و پیشنهاددهنده پژوهش، با ارائه مشاوره‌های علمی و نظارت مستمر بر روند اجرای مطالعه، بازبینی و اصلاح نسخه‌های مختلف پژوهش و تأیید چارچوب علمی آن را بر عهده داشته است. بدین ترتیب، فرآیند پژوهش با رعایت دقت علمی در تدوین مطالب و با هدف تضمین اعتبار و انسجام علمی آن انجام شده است و سهم مشارکت هریک از نویسندگان ۵۰٪ - ۵۰٪ می‌باشد.

تقدیر و تشکر:

نویسندگان مایل هستند از داوران ناشناس بابت دیدگاه‌های علمی و سازنده‌شان تشکر کنند.

حامی مالی:

این پژوهش فاقد هرگونه حمایت مالی از سازمان‌های دولتی، بخش‌های تجاری یا نهادهای انتفاعی است. پژوهش حاضر در چارچوب طرح پژوهشی شماره ۱۴۰۴/د/۴۳۸ به تاریخ ۱۴۰۴/۰۱/۱۹ در مقطع پسادکتری با موضوع «امکان‌سنجی اجرای تحریم‌های اقتصادی در مهار تروریست‌های دیجیتالی در شبکه‌های اجتماعی مجازی از دیدگاه موازن حقوق بشری» استخراج شده و در گروه حقوق دانشکده علوم اداری و اقتصاد دانشگاه اراک، به زیور طبع آراسته شده است.

تضاد منافع:

نگارندگان تصریح می‌کنند که در فرآیند اجرای پژوهش حاضر و انتشار یافته‌های آن،



هیچ‌گونه تعارض منافع مالی، نهادی، شخصی یا حرفه‌ای وجود نداشته است. این مطالعه در چارچوب طرح پژوهشی دوره پسادکتری به شماره ۴۳۸/د/۱۴۰۴ انجام شده و هیچ سازمان یا شخص دیگری در طراحی پژوهش، ارزیابی داده‌ها، تفسیر نتایج یا نگارش پژوهش مداخله‌ای نداشته است.

۷. منابع

۱-۷. منابع فارسی

الف) مقالات

۱. حیدرقلی‌زاده، جعفر و جلالی، محمود (۱۴۰۳). توسعه تدریجی حقوق بین‌الملل در مقابله با تحریم‌های اقتصادی. *فصلنامه مطالعات حقوق عمومی*، ۵۴(۲)، ۱۱۱۳-۱۱۳۶.
۲. زمانی فراهانی، محمدحسین (۱۴۰۰). تبیین نقش فضای سایبری در گسترش قلمرو ژئوپولیتیکی داعش در منطقه. *فصلنامه مطالعات جنگ*، ۳۶(۶۰)، ۲۵-۴۱.
۳. شاهمرادی، مهرانگیزسادات (۱۴۰۱). حریم خصوصی در فضای سایبر. در *دانشنامه رفتار سایبری*، به کوشش باقر شاملو، چاپ اول، ۷۹-۸۱، تهران: بنیاد حقوقی میزان.
۴. شجاعی، عبدالسعید و رحمانی، شهرام (۱۴۰۵). چهارچوب حقوقی حفاظت از حریم خصوصی در بستر دیجیتال: مطالعه تطبیقی در نظام‌های حقوقی ایالات متحده، اتحادیه اروپا و ایران. *پژوهش‌های حقوق تطبیقی*، ۳۰(۲)، ۳۷-۶۶.
۵. قاسمی، غلامعلی و باقرزاده، سجاد (۱۳۹۴). جایگاه حقوق بشر در مبارزه با سایبرتروریسم. *مجله حقوقی بین‌المللی*، ۳۲(۵۲)، ۲۲۷-۲۵۴.
۶. قدیر، محسن و کاظمی فروشانی، حسین (۱۳۹۸). بررسی تطبیقی حقوق کیفری ایران با اسناد بین‌المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری. *مجله حقوقی بین‌المللی*، ۳۶(۶۰)، ۲۳۷-۲۶۷.
۷. نبوی، مهدی و صابر، محمود (۱۳۹۹). مطالعه تطبیقی چالش‌های نظام عدالت کیفری ایران در دادرسی جرایم مرتبط با ارزش‌های مجازی. *پژوهش‌های حقوق تطبیقی*، ۲۴(۱)، ۱۸۳-۲۰۹.

۸. نامیان، پیمان (۱۴۰۴). مقابله با رایاجنگ‌های تخریب‌گر و مختل‌کننده امنیت زیرساخت‌های انرژی در اسناد بین‌المللی؛ با تحلیل تطبیقی مقررات ایران و قطر. *آموزه‌های حقوق کیفری کشورهای اسلامی*، ۲(۴)، ۱۷۷-۱۴۸.
۹. نامیان، پیمان و شهبازی، مهدی (۱۴۰۳). محافظت از امنیت سکویهای دیجیتالی در قبال جرایم تروریستی؛ راهبردی در ارتقای امنیت دیجیتالی دولت‌ها. *مطالعات و پژوهش‌های امنیت داخلی*، ۲(۱)، ۷۳-۹۱.
۱۰. نامیان، پیمان (۱۴۰۳). مقابله و پیشگیری از ارتکاب جرائم تروریستی در شبکه‌های اجتماعی مجازی. *حقوق فناوری‌های نوین*، ۵(۲)، ۲۱۵-۲۳۳.
۱۱. یوسفی، جمال؛ موثقی، حسن و رهبرفرش‌پیرا، ناصر (۱۴۰۳). رویه سازمان ملل متحد در مقابله با تروریسم سایبری. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۶(۴)، ۶۷-۸۰.

۲-۷. منابع لاتین

A) Books

1. Alexe, A. A.-M. S. (2025). *Impact of digital platforms on individual rights*. In J. Cremades & C. Hermida (Eds.), *Encyclopedia of contemporary constitutionalism*. Springer.
2. Pajuste, T. (Ed.). (2022). *Specific threats to human rights protection from the digital reality*. Tallinn University Press.

B) Articles

3. Albader, F. (2020). The digital war on human rights: Guilty until proven innocent in light of the Counter-Terrorism and Border Security Act of 2019. *Minnesota Journal of International Law*, 29(1), 21-41.
4. Almakky, R. (2023). The role of international organisations in the development of international law: An analytical assessment of the United Nations. *Law and World*, 9(28), 40-66.
5. Ayasreh, E. A. (2023). The relationship between science diplomacy and global governance in confronting global catastrophic risks. *University of Sharjah Journal of Humanities and Social Sciences*, 20(4), 438-476.
6. Barış Arı (2025). Human rights violations and public support for sanctions. *Journal of Peace Research*, 62(1), 68-84.



7. Bolpagni, A. & Fisher, A. (2026). Navigating beyond the digital safe haven': Mapping the course of proIslamic State propaganda on Rocket. Chat through a URL social network analysis. *Perspectives on Terrorism*, 20(1), 9–28.
8. Broman, M. M., et al. (2024). Cyberspace outlaws – Coding the online world. *International Journal of Semiotica Iuris*, 37(3), 1153–1183.
9. Chertoff, M., Bury, P. & Richterova, D. (2020). Bytes not waves: Information communication technologies, global jihadism, and counterterrorism. *International Affairs*, 96(5), 1305–1325.
10. 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.
11. Douhan, A. (2022). The changing nature of sanctions in the digital age. In A. Golia Jr., M. C. Kettemann, & R. Kunz (Eds.), *Digital transformations in public international law* (pp. 99–134). Nomos.
12. Farber, S. (2025). The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. *Security Journal*, 38(29), 1-23.
13. Fidler, M. (2025). Fragmentation of international cybercrime law. *Utah Law Review*, 3(4), 737–804.
14. Gherbaoui, T. & Martin S. (2023). A Dual Challenge to Human Rights Law: Online Terrorist Content and Governmental Orders to Remove it. *European Journal of Human Rights*, 2(1), 1-22.
15. Hussein, S. M., & Shima (2023). The differences between traditional terrorism and contemporary terrorism and its implications for global security. *The World Research of Political Science Journal*, 6(2), 113–124.
16. Karimi, Y., Squicciarini, A. & Forster, P. K. (2024). A longitudinal dataset and analysis of Twitter ISIS users and propaganda. *Social Network Analysis and Mining*, 14(1), 1-19.
17. 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.
18. McKeever, D. (2021). Revisiting Security Council action on terrorism: New threats; (a lot of) new law; same old problems?. *Leiden Journal of International Law*, 34(2), 441–470.
19. Mercy, C. (2019). The weaponization of social media: How social media can spark violence and what can be done about it. https://www.mercycorps.org/sites/default/files/2020-01/Weaponization_Social_Media_FINAL_Nov2019.pdf
20. Miao, M. (2024). The regulating digital platforms through sanctions. *Washington*



- International Law Journal*, 33(2), 389-452.
21. Moslemzadeh Tehrani, P. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. *Computer Law & Security Review*, 29(3), 207-215.
 22. Msall, K., & Lary, N. (2022). A link between radicalisation models and extremist propaganda. *Global Security: Health, Science and Policy*, 7(1), 44-50.
 23. Putra, M. D. (2016). New media and terrorism: Role of social media in countering cyber terrorism and cyber extremism. SSRN. <https://ssrn.com/abstract=2754370>
 24. Rabitz, F. F. (2025). A theory of international technology regulation. *Review of International Studies*, 1(1), 1-18.
 25. Radanliev, P. (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from AI, IoT, blockchains, and quantum computing. *Journal of Cyber Security Technology*, 9(1), 28-78.
 26. Razmetaeva, Y. (2022). The concept of human rights in the digital era: Changes and consequences for judicial practice. *Access to Justice in Eastern Europe*, 5(3), 41-56.
 27. Sharlamanov, K., & Petreska, J. (2024). How social media has changed politics. In *The Palgrave handbook of global social change* (pp. 1-17). Palgrave Macmillan.

C) Organizational/ Web Sources

28. Bush, G. W. (2001, October 26). *USA PATRIOT Act*. The White House Archives. <https://georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011026-5.html>
29. Council of Europe. (2001, November 23). *The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols*. <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
30. Cybersecurity and Infrastructure Security Agency. (2021, July 20). *Cyber-attack against Ukrainian critical infrastructure (IR-ALERT-H-16-056-01)*. <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>
31. European Parliament and Council of the European Union. (2021, April 29). *Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online*. Official Journal of the European Union, L 172/79.
32. Financial Action Task Force (FATF). (2021). *Opportunities and challenges of new technologies for AML/CFT*. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.html>
33. Frontiers in Political Science. (2025). [Title of Article].



- <https://www.frontiersin.org/fpos.2025.1718396>
34. *International Emergency Economic Powers Act*, 50 U.S.C. § 1701 et seq. (1977). <https://www.cbp.gov/trade/ieepa-duty-refunds>
 35. Obama, B. (2015, April 1). *Executive Order 13694—Blocking the property of certain persons engaging in significant malicious cyber-enabled activities*. Federal Register. <https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-malicious-cyber-enabled-activities>
 36. Reuters. (2017, June 27). *Ukraine cyber attacks*. <https://www.reuters.com/article/us-ukraine-cyber-attacks-idUSKBN19I1IJ/>
 37. 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
 38. United Nations Development Programme (UNDP). (2023). [Resource Document]. <https://www.undp.org/sites/g/files/zskgke326/files/2023-03/>
 39. 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>
 40. United Nations General Assembly. (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
 41. United Nations General Assembly. (2024, December 24). *Resolution 79/243: Resolution adopted by the General Assembly on the report of the Third Committee (A/79/460)*. <https://docs.un.org/en/A/AC.291/L.15>
 42. United Nations Security Council. (2001, September 28). *Resolution 1373 (2001) adopted by the Security Council at its 4385th meeting*. <https://digitallibrary.un.org/record/449020?v=pdf>
 43. United Nations Security Council Counter-Terrorism Committee (CTC). (n.d.). <https://www.un.org/ctc>

In Persian

B) Articles

1. Ghadir, M. & Kazemi Forushani, H. (2019). A comparative study of Iranian criminal law and international instruments in combating and preventing cyberterrorism. *International Legal Journal*, 36(60), 237–267.
2. Ghasemi, G. & Bagherzadeh, S. (2015). The position of human rights in



- combating cyberterrorism. *International Legal Journal*, 32(52), 227–254.
3. Heydargholizadeh, J. & Jalali, M. (2024). The gradual development of international law in confronting economic sanctions. *Quarterly Journal of Public Law Studies*, 54(2), 1113–1136.
4. Nabavi, M. & Saber, M. (2020). Comparative study of the challenges of the Iranian criminal justice system in the adjudication of crimes related to virtual currencies. *Comparative Law Research*, 24(1), 183–209.
5. Namamian, P. & Shahbazi, M. (2024). Protecting the security of digital platforms against terrorist crimes; A strategy to promote the digital security of governments. *Internal Security Studies and Researches*, 2(1), 73–91.
6. Namamian, P. (2024). Combating and preventing the commission of terrorist crimes in virtual social networks. *Journal of Modern Technology Law*, 5(2), 215–233.
7. Namamian, P. (2025). Confronting destructive cyber warfare disrupting energy infrastructure security in international instruments: A comparative analysis of the regulations of Iran and Qatar. *Teachings of Criminal Law of Islamic Countries*, 2(4), 148–177.
8. Shahmoradi, M. S. (2022). Privacy in Cyberspace. In *Encyclopedia of Cyber Behavior* (1st ed), with Bagher Shamloo, Mizan Legal Foundation, 79–81.
9. Shojaei, A. & Rahmani, Sh. (2026). Legal framework for the protection of privacy in the digital space: A comparative study in the legal systems of the United States, the European Union, and Iran. *Comparative Law Research*, 30(2), 37–66.
10. Yousefi, J., Moteghi, H. & Rahbarfarsh-Pira, N. (2024). The practice of the United Nations in combating cyberterrorism. *Comparative Research in Fiqh, Law and Politics*, 6(4), 67–80.
11. Zamani Farahani, M. H. (2021). Explaining the role of cyberspace in the expansion of ISIS's geopolitical sphere in the region. *Quarterly Journal of War Studies*, 36(60), 25–41.