Journal of Comparative Public Law
Homepage:http://cpl.qom.ac.ir
Online Issn: 3060-6004

# Assessment of the Legal and Legislative Capacities of the BRICS Alliance in Containing Terrorist Crimes Committed through Digital Platforms with the Implementation of Technological Sanctions

**Peyman Namamian** [1]

1 Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran (Corresponding Author), Email: P-namamian@araku.ac.ir

## Abstract

The BRICS alliance faces challenges in the realm of digital security, including the fight against terrorist crimes in the digital space. The misuse of digital platforms by terrorist groups for planning, communication, and propaganda threatens both the national security of BRICS member states and global security. By utilizing national and international legal capacities, BRICS member states can implement effective mechanisms such as multilateral legal cooperation, development of shared legal and legislative frameworks, and the establishment of international regulatory bodies. Technological sanctions are an effective tool for limiting terrorist groups' access to modern technologies and reducing digital threats. However, challenges such as political and economic conflicts of interest among BRICS members, legal differences in national systems, and the risk of human rights violations resulting from sanctions may reduce the effectiveness of these measures. This study, through a descriptive-analytical approach, aims to answer the question, "How can the BRICS alliance, considering the divergences in the domestic laws of its member states, create a common legal and legislative framework to combat terrorist crimes in the digital space?" Furthermore, it seeks to answer the question, "To what extent can technological sanctions be effective in limiting the exploitation of digital platforms by terrorist groups?" The study emphasizes the importance of international coordination in strengthening anti-terrorism regulations on digital platforms and reducing digital threats.

**Keywords**: Terrorist Crimes, Technological Sanctions, Digital Security, Digital Platforms, BRICS Alliance, International Cooperation.

**Received**: 05/08/2025; **Revised**: 05/09/2025; **Accepted**: 11/09/2025; **Published online**: 21/09/2025

**How To Cite**: Namamian, P (2025). Assessment of the Legal and Legislative Capacities of the BRICS Alliance in Containing Terrorist Crimes Committed through Digital Platforms with the Implementation of Technological Sanctions, *Journal of Comparative Public Law*, 2 (2).115-136. http://www.doi.org/10.22091/cpl.2025.13562.1060

**Published by:** University of Qom  **Article type:** Research

حقوق عمومی تطبیقی
شاپا الکترونیکی: ۶۰۰۴-۳۰۶۰
Homepage:http://cpl.qom.ac.ir

# سنجش ظرفیت‌های حقوقی و تقنینی ائتلاف کشورهای نوظهور (بریکس) در مهار جرائم تروریستی ارتکابی در سکوهای دیجیتالی با اجرای تحریم‌های فناورانه

**پیمان نمامیان**[1]

۱. دانشیار حقوق کیفری و جرم‌شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران، (نویسنده مسئول)، رایانامه: p-namamian@araku.ac.ir

## چکیده

ائتلاف کشورهای نوظهور (بریکس)، با چالش‌هایی حوزه در امنیت دیجیتال، ازجمله مقابله با جرائم تروریستی در فضای دیجیتالی مواجه است. سوءاستفاده گروه‌های تروریستی از سکوهای دیجیتالی برای برنامه‌ریزی و ارتباطات و تبلیغات، امنیت ملی کشورهای عضو بریکس و امنیت جهانی را به مخاطره می‌اندازد. کشورهای عضو بریکس با بهره‌گیری از ظرفیت‌های حقوقی ملی و بین‌المللی می‌توانند سازوکارهای مؤثر نظیر همکاری‌های حقوقی چندجانبه، توسعه چارچوب‌های حقوقی و تقنینی مشترک و ایجاد نهادهای نظارتی بین‌المللی را در این زمینه عملیاتی کنند. تحریم‌های فناورانه ابزار مؤثری برای محدودیت دسترسی گروه‌های تروریستی به فناوری‌های نوین و کاهش تهدیدهای دیجیتالی هستند. با این حال، چالش‌هایی نظیر تضاد منافع سیاسی و اقتصادی بین اعضای بریکس، تفاوت‌های حقوقی در نظام‌های ملی و خطر نقض حقوق بشر ناشی از تحریم‌ها، ممکن است کارایی این اقدام‌ها را کاهش دهد. این پژوهش ضمن سنجش ظرفیت‌های حقوقی بریکس در قبال جرائم تروریستی ارتکابی در سکوهای دیجیتالی و چالش‌های اجرایی و حقوقی مرتبط، سعی بر آن دارد تا با روش توصیفی‌تحلیلی به این پرسش که «چگونه ائتلاف بریکس می‌تواند با توجه به وجوه افتراق در قوانین داخلی کشورهای عضو، چارچوب حقوقی و تقنینی مشترکی برای مقابله با جرائم تروریستی در فضای دیجیتالی ایجاد کند؟» به‌علاوه، «تا چه حد تحریم‌های فناورانه در قبال بهره‌برداری گروه‌های تروریستی از سکوهای دیجیتالی می‌تواند اثرگذار باشد؟» پاسخ داده و بر اهمیت هماهنگی بین‌المللی برای تقویت مقررات ضدتروریستی در سکوهای دیجیتالی و کاهش تهدیدهای دیجیتالی تأکید دارد.

**واژگان کلیدی:** جرائم تروریستی، تحریم‌های فناورانه، امنیت دیجیتالی، سکوهای دیجیتال، ائتلاف بریکس، همکاری‌های بین‌المللی.

**تاریخ دریافت:** ۱۴۰۴/۰۵/۱۴؛ **تاریخ بازنگری:** ۱۴۰۵/۰۶/۱۴؛ **تاریخ پذیرش:** ۱۴۰۴/۰۶/۲۰؛ **تاریخ انتشار برخط:** ۱۴۰۴/۰۶/۳۰

**استناد:** نمامیان پیمان (۱٤۰٤). سنجش ظرفیت‌های حقوقی و تقنینی ائتلاف کشورهای نوظهور (بریکس) در مهار جرائم تروریستی ارتکابی در سکوهای دیجیتالی با اجرای تحریم‌های فناورانه، *حقوق عمومی تطبیقی*، ۲(۲)، ۲۳-۱۱۵. http://www.doi.org/10.22091/cpl.2025.13562.1060

**ناشر: دانشگاه قم**  **نوع مقاله: پژوهشی**

**مقدمه**

امنیت دیجیتالی به یکی از حوزه‌های حیاتی مورد توجه نهادهای نظارتی جهانی تبدیل شده است. کشورها در تلاش هستند تا دسترسی و وابستگی خود به فضای دیجیتالی را حفظ کرده و از آن محافظت کنند؛ اقدامی که اغلب نیازمند خروج از چارچوب‌های هنجاری اعم از حقوقی و تقنینی موجود است (Markopoulou, Papakonstantinou & De Hert, 2019: 6). از سال ۲۰۰۲، سازمان ملل متحد چندین قطعنامه را به منظور ترویج فرهنگ جهانی امنیت دیجیتالی تصویب کرده است.[1] با این حال، هنوز هیچ نهاد حقوقی بین‌المللی برای تضمین کنترل و نظارت مناسب بر این حوزه وجود ندارد (Khanna, 2018: 142). این خلأ نظارتی، موجب رقابت فزاینده‌ای بین کشورها برای دستیابی به اولویت در این عرصه شده است؛ اگرچه شورای امنیت سازمان ملل متحد وفق قطعنامه‌های ۲٤۱۹ (۲۰۱۸)، ۲٤٦۲ (۲۰۱۹) و ۲٤۹۰ (۲۰۱۹) و سایر قطعنامه‌ها اذعان داشته که فعالیت‌های افراد و نهادهای غیردولتی در حوزه دیجیتالی می‌تواند تهدیدی جدی برای صلح و امنیت بین‌المللی باشد (Douhan, 2022: 99).[2]

امنیت دیجیتالی برای حفاظت از داده‌ها و زیرساخت‌ها ضروری است و به پیشبرد سیاست‌های ملی و بین‌المللی کمک می‌کند. این امر نیازمند تقویت قوانین داخلی و هماهنگی با استانداردهای بین‌المللی است. البته چالش‌های حقوقی درزمینهٔ صلاحیت و مسئولیت‌های قانونی باید مورد توجه قرار گیرد (احمری، کحلکی و رحیم‌پور اصفهانی، ۱۳۹۵: ۳۲٤-۳۲۱). «ائتلاف کشورهای نوظهور» موسوم به «بریکس» مشتمل بر کشورهای برزیل، روسیه، هند، چین، آفریقای جنوبی و سایر کشورها مانند ایران و مصر باید به تقویت زیرساخت‌های دیجیتالی و تدوین سیاست‌های مناسب توجه کنند (Nikitin & Mensah, 2020: 66). بنابراین، با گسترش فناوری‌های نوین ارتباطی، جرائم تروریستی ارتکابی در سکوهای دیجیتالی به‌عنوان پدیده‌ای فراملی، مرزهای سنتی حاکمیت ملی را به چالش کشیده و به یکی از چالش‌های فزاینده در امنیت بین‌المللی تبدیل شده است. این شکل از تهدید، نه‌تنها زیرساخت‌های حیاتی کشورها را هدف قرار می‌دهد، بلکه موجب بی‌ثبات‌سازی نظام‌های سیاسی، اقتصادی و اطلاعاتی نیز می‌گردد (ر. ک: خاکزادشاهاندشتی و میربد، ۱٤۰۳: ۱۸۷-۱۸۵). در این بستر، کشورهای عضو بریکس، درصدد ایجاد یک چارچوب راهبردی مستقل در قبال تهدیدهای دیجیتالی است (Ovchinnikova, & Upadhyay, 2023: 18-19).

---

1. United Nations. (2003, January 31). Creation of a global culture of cybersecurity: Resolution/adopted by the General Assembly. United Nations Digital Library. https://digitallibrary.un.org/record/482184?ln=en

۲. این تهدیدها مشتمل بر حمله‌های دیجیتالی به زیرساخت‌های حیاتی، اختلال در سامانه‌های پرداخت برخط، انسدادسازی دسترسی به اینترنت و خدمات مختلف برخط مانند توییتر، اینستاگرام و غیره و نیز اجرای فعالیت‌های دیجیتالی در واکنش به سایر تهدیدهاست.

کشورهای عضو بریکس با تأکید بر اتخاذ سیاست کاهش وابستگی فناورانه به کشورهای غربی، به دنبال تدوین سیاست‌های هماهنگ دیجیتالی، توسعه ظرفیت‌های بومی در حوزه زیرساخت‌های دیجیتالی و بهره‌گیری از تحریم‌های فناورانه به‌عنوان ابزاری بازدارنده و هدفمند در قبال گروه‌های تروریستی دیجیتالی هستند (Iftimie, 2021: 57). این رویکرد، ضمن برخورداری از پشتوانه نظری در حوزه حقوق بین‌المللی فضای دیجیتال، در تلاش است تا الگویی جایگزین برای نظم دیجیتالی جهانی ارائه کند (علی‌پور و شکاری، ۱٤۰۰: ۸۱). ازاین‌رو، توسعه فناوری‌های دیجیتال تأثیر زیادی بر تحریم‌های یک‌جانبه داشته است، به‌ویژه که این تحریم‌ها بدون تصویب سازمان ملل اعمال می‌شوند و مشروعیت حقوقی آن‌ها مورد سؤال است. این تحریم‌ها ممکن است با اصول حاکمیت ملی و قوانین بین‌المللی مغایرت داشته باشند و استفاده از فناوری‌های دیجیتال، نظارت و ارزیابی آن‌ها را پیچیده‌تر کرده است. همچنین، این تحریم‌ها تأثیرات منفی بر حقوق بشر، شهروندان و اقتصادها دارد (Douhan, 2022: 114-115). به‌علاوه، بررسی تجربه بریکس در بهره‌گیری از ابزار تحریم فناورانه، به‌ویژه در قالب سازوکارهای جمعی و غیروابسته به ساختارهای نهادینه شده غربی، می‌تواند ابعاد نوینی از تعامل امنیت، حاکمیت فناوری و پاسخ‌های حقوقی به جرائم تروریستی ارتکابی در سکوهای دیجیتالی را آشکار سازد. به دیگر تعبیر، تجربه بریکس در بهره‌گیری از تحریم فناورانه در قبال جرائم تروریستی ارتکابی در سکوهای دیجیتالی، ترکیبی از اقدام‌های حقوقی و فناورانه است.[1] کشورهای عضو بریکس با تصویب قوانین ملی و تقویت همکاری‌های بین‌المللی، به محدودیت دسترسی گروه‌های تروریستی به زیرساخت‌ها و خدمات دیجیتالی می‌پردازند؛ در این بین باید اذعان داشت، روسیه و چین با کنترل فضای مجازی و انسداد سکوهای مرتبط با جرائم تروریستی، تلاش دارند امنیت دیجیتالی را تقویت کنند (Flonk, 2021: 1931-1932).

هدف این پژوهش، بررسی ظرفیت‌های حقوقی، تقنینی، امنیتی و فنی ائتلاف بریکس در قبال جرائم تروریستی ارتکابی در سکوهای دیجیتالی از طریق تحریم‌های فناورانه است. پژوهش به تحلیل چالش‌های حقوقی اجرای تحریم‌ها، ارزیابی تأثیر آن‌ها بر کاهش فعالیت‌های تروریستی در سکوهای دیجیتالی و بررسی امکان ایجاد چارچوب‌های حقوقی و تقنینی مشترک برای مقابله با آن می‌پردازد. ازاین‌رو، با پاسخ به این پرسش که با توجه به تفاوت‌های موجود در قوانین داخلی کشورهای عضو ائتلاف بریکس، چگونه می‌توان یک چارچوب حقوقی و تقنینی مشترک در قبال جرائم تروریستی در فضای دیجیتال ایجاد نمود؟ بر اهمیت هماهنگی بین‌المللی و تأثیر تحریم‌های فناورانه در مقابله با سوءاستفاده گروه‌های تروریستی از سکوهای دیجیتال تأکید دارد. به این ترتیب،

1.https://brics.br/en/news/use-of-artificial-intelligence-and-social-media-by-terrorist-groups-raises-concerns-among-brics-nations

این پژوهش می‌تواند به کشورهای عضو بریکس در تقویت ظرفیت‌های خود در قبال جرائم تروریستی ارتکابی در سکوهای دیجیتالی کمک کرده و سیاست‌های مؤثری برای اجرای تحریم‌های فناورانه ارائه دهد.

## ۱. شناخت مفاهیم

بهره‌گیری روزافزون از فناوری‌های دیجیتالی تهدیدهای جدی برای سامانه‌های حیاتی ایجاد کرده است، به‌ویژه زمانی که تروریست‌ها از آن سوءاستفاده می‌کنند. امنیت فضای دیجیتالی نیازمند اقدامات پیشگیرانه و واکنشی مانند روزآمدسازی سامانه‌ها، نصب نرم‌افزارهای امنیتی و ارزیابی نقاط ضعف است (ملکوتی و خلیل‌زاده، ۱٤۰۱: ۷۳-۷۵). افزایش حمله‌های دیجیتالی از سوی گروه‌های تروریستی با اهداف اعتقادی، پیچیدگی‌های بیشتری در تأمین امنیت دیجیتالی ایجاد کرده و می‌تواند به زیرساخت‌های حیاتی نظیر انرژی، حمل‌ونقل و خدمات بهداشتی آسیب برساند (Shaweorcid, McAndrew, 2023: 548).

با ظهور جامعه مبتنی بر اطلاعات، تهدیدهای نوینی از سوی تروریست‌های دیجیتال به وجود آمده است که قادرند از طریق آماج‌های رایانه‌ای به داده‌ها و زیرساخت‌های حیاتی آسیب بزنند. این آماج‌ها شامل آسیب به سامانه‌ها، سرورها و دستگاه‌های الکترونیکی است. «جرائم تروریستی در سکوهای دیجیتالی» به‌عنوان بهره‌گیری از فناوری‌ها برای ایجاد اختلال و تهدید به امنیت تعریف می‌شود. این تهدیدها به علت ناشناخته بودن، آثار روانی بیشتری نسبت به تهدیدهای شناخته‌شده دارند. تروریست‌ها با بهره‌گیری از ویروس‌ها و ابزارهای مخرب می‌توانند حمله‌های دیجیتال علیه دولت‌ها و زیرساخت‌ها ترتیب دهند که به اختلالات و تهدید جدی برای امنیت منجر می‌شود.[۱]

برای آنکه این دسته از جرائم به‌طور مؤثر در چارچوب مفهومی تروریسم قرار گیرد، لازم است واجد مؤلفه‌های اساسی این پدیده ازجمله سازمان‌یافتگی، هدفمندی در ایجاد رعب و وحشت و ایراد آسیب جدی به امنیت ملی، عمومی یا بین‌المللی باشد. بر همین اساس، محدوده شمول این جرائم به‌طور معمول بر پایه «محیط ارتکاب» آن (فضای مجازی به‌جای محیط فیزیکی) و نیز «رسانه یا ابزار» مورد استفاده، تعریف می‌شود (Kraft & Wang, 2009: 524). از این منظر، جرائم تروریستی در سکوهای دیجیتالی نه یک جرم مستقل و جداگانه، بلکه شکلی از تروریسم سنتی است که به‌طور صرف با بهره‌گیری از فناوری‌های دیجیتال و فضای مجازی محقق می‌شود (اصلانی و رنجبریان، ۱۳۹٤: ۲٦۸).

---

۱. در این زمینه، می‌توان به هکِ جایگاه‌های سوخت در ایران و اختلال در پمپ بنزین‌های مختلف کشور در تاریخ ۲۷ آذر ماه ۱۴۰۲ اشاره کرد. طبق اعلام مسئولین و گزارش‌های منتشر شده از سوی خبرگزاری‌های داخلی، این حمله دیجیتالی توسط گروه هکری صهیونیستی به نام «گنجشک درنده» صورت گرفته و این گروه مسئولیت هک سامانه سوخت‌رسانی ایران را بر عهده گرفته است. شایان ذکر است که پیش از این، در تاریخ چهارم آبان ۱۴۰۰، هکرها اطلاعات کارت سوخت شخصی را هدف قرار داده بودند؛ https://www.farsnews.ir/news/14020927000595/D8

با وجود این، تکیه بر «محیط ارتکاب» که همان فضای غیرواقعی یا مجازی بوده، به‌عنوان مبنای تمایز جرم تروریستی دیجیتالی است که می‌تواند محل تأمل و انتقاد باشد. به‌طور نمونه، حملات تروریستی از طریق هواپیماربایی (نظیر حوادث تروریستی ۱۱ سپتامبر ۲۰۰۱)[1] یا به‌کارگیری عامدانه از وسایل نقلیه برای ایجاد تلفات (نظیر حمله تروریستی در نیس فرانسه[2] در سال ۲۰۱٦)[3]، هر دو در فضای فیزیکی رخ داده‌اند، اما ماهیت تروریستی خود را از طریق شیوه اجرا از دست نداده‌اند. به همین قیاس، جرائم تروریستی در سکوهای دیجیتالی نیز واجد همان عناصر جرم تروریستی است، اما در بستری فناورانه و دیجیتالی تحقق می‌یابند (Lux, 2018: 12). ازاین‌رو، می‌توان گفت که تروریسم سایبری بازنمایی بسیاری از الگوهای شناخته‌شده تروریستی در بستر دیجیتال است و همان‌طور که در ادبیات مربوط به «کنشگری دیجیتالی»[4] (Milan & Hintz, 2013: 18-19) نیز اشاره شده، فعالیت‌های سیاسی و خشونت‌آمیز در فضای مجازی نوعی امتداد از کنش‌های دنیای واقعی محسوب می‌شوند. بنابراین، در شناسایی و تحلیل رفتارهای تروریستی آنچه اهمیت اساسی دارد، نه صرفاً وسیله یا محل ارتکاب، بلکه اهداف و آثار و انگیزه‌های پشت آن رفتار است که ماهیت تروریستی آن را احراز می‌سازد.

جرائم تروریستی دیجیتالی چالش‌های جدی در زمینه‌های حقوق بین‌المللی، امنیت و سیاست‌های جهانی به وجود آورده‌اند. مقابله با این تهدید نیازمند روزآمدسازی قوانین داخلی و تقویت همکاری‌های بین‌المللی است. این قوانین باید ابزارهایی مؤثر برای شناسایی، پیشگیری و مجازات عاملان این جرائم فراهم کنند. تحریم‌های فناورانه نیز می‌توانند به‌عنوان ابزاری برای محدودیت دسترسی گروه‌های تروریستی به فناوری‌های دیجیتال و فضای

---

۱. با ظهور اینترنت و گسترش فناوری‌های دیجیتال، ارتباط میان فضای مجازی و جرائم تروریستی پس از حوادث ۱۱ سپتامبر ۲۰۰۱ آشکار شد. این تحولات موجب انتقال مبارزه با جرائم تروریستی از سطح فیزیکی به الکترونیکی شد (ر.ک: عباسی و محسن‌پوراژیه، ۱۴۰۳: ۳۴۰-۳۳۹). با این حال، تاکنون تعریف جامع و بین‌المللی برای شناسایی جرائم تروریستی ارتکابی در سکوهای دیجیتالی، وجود ندارد. این نوع جرائم به‌عنوان ابزار خطرناک جرائم تروریستی مورد شناسایی قرار گرفته و گسترش سریع اینترنت، کنترل و شناسایی آن‌ها را دشوار کرده است؛ اگرچه این تهدیدها به‌طور جدی امنیت ملی و اقتصادی کشورها را به خطر انداخته و ضرورت اقداماتی مؤثر برای مقابله با آن را آشکار می‌کند.

2. https://transweb.sjsu.edu/sites/default/files/SP0518%20Vehicle%20Ramming%20Terrorism.pdf

۳. شهر نیس در جنوب فرانسه در تاریخ ۱۴ ژوئیه ۲۰۱۶، هم‌زمان با روز ملی فرانسه، هدف حمله تروریستی اسلام‌گرایان قرار گرفت. در این حمله، یک کامیون به جمعیت حاضر در خیابان نیس حمله کرده و موجب کشته شدن ۸۶ نفر، از جمله ۱۵ کودک و زخمی شدن ۴۵۸ نفر دیگر شد. بیش از ۳۰٬۰۰۰ نفر شاهد این رویداد وحشتناک بودند (Fernandez, 2023: 1).

٤. کنشگری دیجیتالی (Digital Activism) به استفاده از فناوری‌های دیجیتالی، به‌ویژه اینترنت، برای تحقق اهداف اجتماعی، سیاسی یا محیط‌زیستی و تأثیرگذاری بر سیاست‌ها و تحولات اجتماعی اشاره دارد. این نوع کنشگری از ابزارهایی مانند شبکه‌های اجتماعی، وب‌گاه‌ها و آدرس‌های الکترونیک برای سازماندهی، اطلاع‌رسانی و جلب حمایت استفاده می‌کند. از ویژگی‌های آن می‌توان به انتشار سریع پیام‌ها، مشارکت بدون محدودیت جغرافیایی، امکان فعالیت ناشناس و هزینه اندک اشاره کرد (Phillips, 2024: 33-35). کنشگری دیجیتالی می‌تواند ابزاری مشروع برای تقویت مشارکت عمومی و ارتقاء شفافیت باشد، مشروط بر آنکه مقررات ملی و بین‌المللی و موازین حقوق بشر رعایت شود.

مجازی، شامل محدودیت‌های واردات فناوری و ممنوعیت دسترسی به سکوهای برخط، به‌کار روند.[1] تهدیدهای موجود در سکوهای دیجیتالی مانند نقض داده‌ها، حملات باج‌افزاری و جاسوسی تحت حمایت دولت‌ها به‌طور فزاینده‌ای پیچیده و گسترده‌تر می‌شوند؛ بنابراین، نیاز به تدابیر حقوقی و همکاری بین‌المللی بیشتر ضروری است. مدیریت بحران دیجیتالی باید بر همکاری بین‌المللی، چارچوب‌های قانونی و آگاهی عمومی تمرکز کند. همکاری بین‌المللی برای تبادل اطلاعات و پیگرد قانونی جرائم سایبری ضروری است که در این زمینه «کنوانسیون بوداپست در مورد جرائم سایبری، مصوب ۲۰۰۱»[2] نقش کلیدی دارد. نهادهایی همچون سازمان همکاری و توسعه اقتصادی[3] و اتحادیه بین‌المللی مخابرات[4] نیز با تدوین استانداردهای جهانی به مقابله با تهدیدهای دیجیتالی کمک می‌کنند. در سطح بین‌المللی، اسناد حقوقی مانند کنوانسیون بوداپست و «کنوانسیون سازمان ملل متحد علیه جرائم سازمان‌یافته فراملی و پروتکل‌های الحاقی آن، مصوب ۲۰۰۳»[5] می‌توانند چارچوب قانونی برای همکاری در قبال جرائم تروریستی ارتکابی در سکوهای دیجیتالی را فراهم کنند. همچنین، تحریم‌های فناورانه می‌توانند به‌عنوان ابزار پیشگیرانه در مقابله با این تهدیدها عمل کنند که برای موفقیت آن‌ها باید در سطح جهانی هماهنگ و از طریق همکاری میان دولت‌ها، نهادهای بین‌المللی و بخش خصوصی اجرایی شوند (Radanliev, 2025: 57).

اجرای تحریم‌های فناورانه علیه جرائم تروریستی دیجیتال نیازمند درک فرامرزی بودن جرائم تروریستی دیجیتالی و همکاری بین‌المللی است. این همکاری باید با نهادهای بین‌المللی و استفاده از کنوانسیون بوداپست در مورد جرائم سایبری، برای ایجاد چارچوب قانونی صورت گیرد. تحریم‌های فناورانه باید به‌طور هماهنگ جهانی اعمال شوند تا دسترسی تروریست‌ها به فناوری‌های حساس محدود گردد. درنهایت، مقابله با این نوع از جرائم مستلزم رویکرد جامع و هماهنگ است که تحریم‌ها را به‌عنوان ابزاری مؤثر در نظر می‌گیرد.

راجع‌به مهار جرائم تروریستی از طریق سکوهای دیجیتال از طریق اجرای تحریم‌های فناورانه در کشورهای عضو بریکس با چالش‌های حقوقی و سیاسی خاصی مواجه است. این پیچیدگی‌ها به دلیل تفاوت‌های موجود در چارچوب‌های قانونی، نظام‌های سیاسی و رویکردهای امنیتی کشورهای عضو بریکس است که اجرای هماهنگ

1. https://www.moodys.com/web/en/us/kyc/resources/insights/cyber-risk-management-sanctions-evasion-in-the-cyberspace.html.

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

3. The Organization for Economic Co-operation and Development (OECD)

4. The International Telecommunication Union.

5.UN Convention against Transnational Organized Crime and the Protocols thereto, 29 September 2003, https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

و مؤثر تحریم‌ها را با مشکلات جدی روبه‌رو می‌سازد (Dmitrieva, Alshdaifat, & Pastukhov, 2023: 90-106). فقدان یک تعریف مشترک از جرم دیجیتالی و جرم تروریستی دیجیتالی، تفاوت در قوانین ملی و چالش‌های حقوق بشری مرتبط با آزادی‌های دیجیتال، ازجمله مواردی هستند که بر اجرای تحریم‌های فناورانه تأثیر منفی می‌گذارند. کشورهای عضو بریکس هریک چارچوب قانونی خاص خود را در قبال جرائم تروریستی دیجیتالی دارند که این امر به‌ویژه درزمینهٔ استخراج داده‌های فرامرزی و هماهنگی بین‌المللی، چالش‌هایی در اجرای مؤثر تحریم‌های فناورانه و مقابله با این جرائم ایجاد می‌کند (Belli, 2021: 273-275). افزون بر این، نگرانی‌های حقوق بشری، ازجمله نظارت بر فضای دیجیتال و محدودیت‌های آزادی‌های فردی، به‌ویژه در کشورهایی مانند چین، ممکن است تضادهایی با اصول حقوق بشر و آزادی اینترنت به وجود آورد.[1] ازاین‌رو، برای مقابله مؤثر با جرائم تروریستی و اجرای تحریم‌های فناورانه، کشورهای عضو بریکس نیازمند همکاری‌های بین‌المللی، ایجاد چارچوب‌های حقوقی و قانونی منسجم و تعاملات مستمر هستند؛ اگرچه این امر مستلزم مذاکرات طولانی‌مدت و پذیرش تغییرات در قوانین ملی جهت دستیابی به توافق جهانی و بهره‌برداری مؤثر از تحریم‌های فناورانه خواهد بود.[2]

به هر روی، تحریم‌های فناورانه زمانی که به‌طور یک‌جانبه از سوی دولت‌ها یا بلوک‌های منطقه‌ای اِعمال شوند، مشروعیت حقوقی آن‌ها قابل چالش است؛ زیرا ممکن است با اصول حقوق بین‌المللی، نظیر عدم مداخله و حق توسعه تضاد داشته باشند. کشورهای عضو بریکس مخالف تحریم‌های یک‌جانبه هستند و بر استقلال دیجیتال و حق توسعه فناورانه تأکید دارند. مشروعیت تحریم‌ها به شروطی نظیر وجود تهدید مشروع و تناسب بین ابزار و هدف و عدم نقض حقوق بشر بستگی دارد (Bogdanova, 2021: 267-268). ازاین‌رو، ائتلاف کشورهای عضو بریکس باید برای تقویت مشروعیت این تحریم‌ها، راهبردی مشترک در ارتقای امنیت سکوهای دیجیتالی، نهاد تحریمی با صلاحیت اجرایی و تضمین‌های حقوق بشری را ایجاد کند.[3]

1. https://as.nyu.edu/content/dam/nyu-as/ir/documents/Li-Huimin-ThesisFinal.pdf

2. See: The United Nations, Cyberspace and International Peace and Security, Responding to Complexity in the 21st Century, https://unidir.org/files/publication/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

3. BRICS. (2025, July 6). Strengthening global South cooperation for a more inclusive and sustainable governance. Rio de Janeiro, Brazil. https://brics.br/en/about-the-brics

## ۲. تحریم‌های فناورانه؛ راهبردی مؤثر در قبال جرائم تروریستی دیجیتالی

اجرای تحریم‌های فناورانه از سوی کشورهای عضو بریکس مجموعه‌ای از اقدامات محدودکننده است که در واکنش به تهدیدهای دیجیتالی، اقدام‌های مخرب دیجیتال یا نقض تعهدات بین‌المللی توسط برخی دولت‌ها یا نهادها اعمال می‌شود. این تحریم‌ها به‌طور عمده شامل ممنوعیت صادرات فناوری‌های پیشرفته، تجهیزات و خدمات دیجیتال است و اهدافی چون مقابله با تهدیدهای دیجیتالی، بازدارندگی در قبال حمایت از بازیگران دیجیتالی مخرب و اعمال فشار بر ناقضان حقوق بشر در فضای مجازی دارند (Jiang, & Belli, 2025: 227). از منظر حقوق بین‌المللی، مشروعیت این تحریم‌ها به رعایت اصولی مانند تناسب، احترام به حاکمیت دولت‌ها و اثبات مسئولیت دولت‌ها بستگی دارد. چالش‌هایی نظیر فقدان مجوز شورای امنیت و آثار منفی بالقوه می‌تواند مشروعیت این تحریم‌ها را مورد تردید قرار دهد. بنابراین، اثربخشی تحریم‌ها نیازمند هماهنگی بین‌المللی و انطباق با قواعد حقوقی بین‌المللی است (Hofer, 2019: 165).

### ۲-۱. مشروعیت اجرای تحریم‌های فناورانه

مشروعیت تحریم‌های فناورانه در چارچوب حقوق بین‌المللی منوط به رعایت اصولی ازجمله تناسب، هدفمندی، احترام به حاکمیت دولت‌ها، رعایت حقوق بشر، وجود ادله معتبر جهت انتساب فعالیت‌های دیجیتالی به دولت معین و در صورت امکان، اخذ مجوز از شورای امنیت سازمان ملل متحد است. تحریم‌هایی که منجر به آسیب گسترده به غیرنظامیان، زیرساخت‌های حیاتی یا حقوق اقتصادی و اجتماعی افراد شوند، از منظر حقوقی قابل توجیه نبوده و ممکن است مشروعیت خود را از دست دهند. افزون بر این، اقدام‌های یک‌جانبه فاقد مبنای حقوقی یا حمایت بین‌المللی، ازجمله مجوز شورای امنیت یا اجماع جهانی، در معرض تردیدهای حقوقی و سیاسی قرار می‌گیرند (Mallard, G, & Sun, 2024: 99-101). ازاین‌رو، تحریم‌های فناورانه تنها در صورتی از مشروعیت حقوقی برخوردار خواهند بود که در چارچوب اصول بنیادین حقوق بین‌الملل به‌ویژه قواعد حاکم بر مسئولیت دولت‌ها، اصل عدم مداخله در امور داخلی، اصل حاکمیت ملی و الزامات حقوق بشر بین‌المللی طراحی و اجرا شوند. در فقدان شواهد مستند، مبنای قانونی معتبر یا رعایت اصول تناسب و ضرورت، این اقدامات ممکن است با چالش‌های جدی در سطح بین‌المللی مواجه شوند (Rusinova, Martynova & Kurakina, 2020: 6-7). بنابراین، طراحی و اجرای تحریم‌های فناورانه مستلزم دقت، هدفمندی، هماهنگی حقوقی و دیپلماتیک و انطباق کامل با قواعد آمره حقوق بین‌الملل است تا ضمن حفظ مشروعیت، اثربخشی آن‌ها در مهار تهدیدهای فناورانه نیز تضمین گردد.

مشروعیت تحریم‌های فناورانه در بریکس برای مقابله با این نوع از جرائم به مسائل حقوقی، اقتصادی و سیاسی پیچیده‌ای مرتبط است. کشورهای عضو بریکس ممکن است در صورتی که این تحریم‌ها با اصول حقوق بین‌الملل مغایرت داشته باشند، با آن‌ها مخالفت کنند.[1] این تحریم‌ها به‌منظور مقابله با تهدیدهای ناشی از جرائم تروریستی ارتکابی در سکوهای دیجیتالی اعمال می‌شوند، اما ممکن است تأثیرات منفی بر توسعه فناوری‌های داخلی کشورهای بریکس بگذارند (Patra, S. K. & Muchie, 2020: 86-88). کشورهای عضو به دنبال راهکارهایی برای دور زدن این تحریم‌ها یا ارزیابی مشروعیت آن‌ها از نهادهای بین‌المللی هستند. به‌علاوه، یکی از زمینه‌های همکاری کشورهای عضو بریکس، مقابله با سوءاستفاده از فناوری‌های اطلاعات برای فعالیت‌های مجرمانه است. این همکاری شامل اقدامات مشترک برای پیشگیری از بهره‌برداری غیرقانونی از فناوری‌های پیشرفته و تقویت امنیت دیجیتالی است (فرشاسعید، جلالی و گودرزی، ۱٤۰۱: ۱٦۳). با این حال، تحریم‌های فناورانه در قبال این جرائم، مادام که با حقوق بین‌الملل یا منافع داخلی کشورهای عضو بریکس مغایرت داشته باشند، ممکن است با چالش‌هایی از حیث مشروعیت مواجه شوند (Ivanova, 2023: 69-71).

### ۲-۲. چالش انتساب و اثبات در بستر ارتکاب جرم

با توجه به وابستگی روزافزون زیرساخت‌ها و امنیت جهانی به فناوری‌های پیشرفته اطلاعاتی، اهمیت اتخاذ اقدامات قوی درزمینهٔ امنیت دیجیتالی به هیچ‌وجه قابل انکار نیست. افزایش جرائم ارتکابی در سکوهای دیجیتالی و طبیعت در حال تحول تهدیدهای تروریستی، ضرورت تلاش‌های هماهنگ بین‌المللی را بیش‌ازپیش آشکار می‌سازد.[2] کشورهای عضو بریکس با درک کامل از این چالش‌ها، آمادگی خود را برای ایفای نقشی محوری در قبال این تهدیدها اعلام کرده‌اند.[3] تحریم‌های فناورانه کشورهای عضو بریکس به‌منظور مقابله با جرائم تروریستی در بستر چالش‌های انتساب و اثبات در سکوهای دیجیتالی، می‌تواند نقشی کلیدی در کاهش تهدیدهای مجرمانه ایفا کند. با این حال، این اقدام با مسائل پیچیده‌ای مواجه است که مستلزم تدقیق و همکاری بین‌المللی گسترده است. البته چالش‌های انتساب و اثبات در فضای دیجیتالی به‌ویژه زمانی که تهدیدها به‌طور غیرمستقیم یا از طریق ابزارهای پیچیده و توزیع‌شده انجام می‌شوند، به مراتب پیچیده‌تر می‌شود. مرتکبان جرائم مزبور به‌طور معمول از فناوری‌های پیشرفته‌ای نظیر فیلترشکن‌ها، پروکسی‌ها و شبکه‌های توزیع‌شده برای پنهان‌سازی هویت خود بهره می‌برند (Mose, 2024: 1). در چنین شرایطی، تحریم‌های فناورانه می‌توانند به‌عنوان ابزاری مؤثر در محدودیت

1. https://economictimes.indiatimes.com/topic/cyber-terrorism

2. Azernews. (2024, September 12). BRICS to strengthen fight against terrorism and cybercrime. https://www.azernews.az/analysis/231138.html

3. https://www.fmprc.gov.cn/eng/wjb/zzjg_663340/ggjjs_665228/xwlb_665230/202504/t20250430_11613910.html

دسترسی به فناوری‌ها و ابزارهایی عمل کنند که به مرتکبان جرائم امکان پنهان‌سازی هویت یا تغییر ردپای دیجیتال خود را می‌دهند.

در چارچوب راهبرد کشورهای عضو بریکس، تحریم‌های فناورانه ممکن است شامل محدودیت‌هایی در دسترسی به فناوری‌های کلیدی نظیر نرم‌افزارهای پنهان‌سازی هویت یا ابزارهای پیشرفته برای اجرای حمله‌های دیجیتالی باشد. اعمال این تحریم‌ها می‌تواند به محدودیت بهره‌گیری از فناوری‌هایی که به پنهان‌سازی هویت یا دستکاری شواهد دیجیتال کمک می‌کنند، منجر شود و شفافیت بیشتری در فرایند شناسایی و پیگیری مرتکبان جرائم ایجاد کند.[1] به‌عنوان مثال، محدودیت دسترسی به ابزارهای فیلترشکن یا سرویس‌های پروکسی می‌تواند توانایی هکرها در اخفای هویت خود را کاهش دهد و فرآیند انتساب و اثبات جرم را تسهیل کند.[2] با این حال، به دلیل پیچیدگی‌های موجود در فضای دیجیتالی و نیاز به شواهد دیجیتال معتبر تحریم‌های فناورانه ممکن است چالش‌های نوینی ایجاد کنند. در صورتی که این تحریم‌ها به‌طور غیرمستقیم بر فناوری‌های داخلی کشورهای عضو بریکس تأثیر بگذارند، ممکن است مشکلاتی برای توسعه فناوری‌ها و اقتصاد این کشورها ایجاد شود. به‌علاوه، تفاوت‌های قانونی و قضائی میان کشورهای عضو می‌تواند فرایند جمع‌آوری و تحلیل شواهد دیجیتال و اجرای احکام را پیچیده‌تر سازد. بنابراین، تحریم‌های فناورانه باید به‌گونه‌ای طراحی شوند که افزون بر مقابله مؤثر با جرائم ارتکابی در سکوهای دیجیتالی، حقوق و منافع کشورهای عضو رعایت شود.[3]

به هر روی، برای مقابله مؤثر با چنین جرائمی در سطح جهانی، همکاری‌های بین‌المللی درزمینهٔ تبادل اطلاعات و ایجاد استانداردهای حقوقی و تقنینی مشترک ضرورت دارد. چنین همکاری‌هایی می‌تواند روند جمع‌آوری شواهد دیجیتال و سنجش حمله‌های دیجیتالی را تسهیل کرده و چالش‌های راجع‌به انتساب و اثبات جرم را در این بستر کاهش دهد (Ayodele & Petla, 2024: 5-6).

### ۲-۳. تأثیر تحریم‌های فناورانه بر حقوق بشر و تعهدات فراملی

همان‌گونه که در سطور قبلی تأکید شد، تحریم‌های فناورانه به‌عنوان ابزاری در قبال تهدیدهای امنیتی، ازجمله جرائم تروریستی ارتکابی در سکوهای دیجیتالی، از سوی کشورهای عضو بریکس مورد استعمال قرار می‌گیرد. این تحریم‌ها به‌طور عمده شامل محدودیت‌هایی در دسترسی به فناوری‌ها، سامانه‌های ارتباطی و تجهیزات

1.https://www.spglobal.com/commodity-insights/en/news-research/latest-news/crude-oil/052025-brics-criticize-sanctions-and-trade-restrictions-as-threat-to-energy-security.

2. https://neweconomy.expert/publications/256849/.

3.https://360mozambique.com/world/brics-condemn-unilateral-economic-sanctions-and-call-for-end-to-illegal-measures/.

دیجیتال است. هدف اصلی این تحریم‌ها، محدود کردن دسترسی به فناوری‌هایی بوده که ممکن است برای سازمان‌دهی، تبلیغ یا اجرای اقدام‌های تروریستی مورد استعمال قرار گیرند. با این حال، چنین اقدام‌های تحریمی می‌تواند به‌طور مستقیم بر حقوق بشر تأثیرگذار بوده و منجر به نقض حقوق بنیادین، ازجمله حق آزادی بیان و حق دسترسی آزاد به اطلاعات گردد (Fellmeth, 2023: 1). به‌علاوه، این تحریم‌ها می‌توانند موجب اختلال در ارتباطات بین‌المللی و همکاری‌های علمی و فناورانه میان کشورها شوند. علاوه بر موارد فوق، تحریم‌های فناورانه ممکن است دسترسی به فناوری‌های پزشکی و بهداشتی را نیز محدود سازند. در شرایط بحرانی، نظیر پاندمی‌ها، این محدودیت‌ها می‌توانند آثار منفی جدی بر حقوق بشر داشته باشند، به‌ویژه درزمینهٔ تأمین خدمات درمانی و بهداشتی دیجیتال (ر. ک: رضائی، رئیسی و راعی، ۱٤۰۱: ۱۵۳-۱۵۲). در این راستا، کشورهای عضو بریکس باید به تعهدات بین‌المللی خود درزمینهٔ حقوق بشر و امنیت جهانی توجه ویژه داشته باشند تا از نقض حقوق اساسی بشر پیشگیری شود. بنابراین، اعمال این تحریم‌ها باید با دقت و با توجه به پیامدهای آن‌ها بر حقوق بشر و همکاری‌های بین‌المللی صورت گیرد تا تأثیرات منفی آن‌ها به حداقل برسد (Šturma, 2024: 139-141).

افزون بر این، در چنین وضعیتی اثرات منفی تحریم‌های فناورانه ممکن است موجب تضعیف حقوق اقتصادی، اجتماعی و فرهنگی شهروندان شود. تحریم‌های فناورانه کشورهای عضو بریکس علیه جرائم تروریستی در سکوهای دیجیتالی حاکی از آن است که این تحریم‌ها باید با دقت و با در نظر گرفتن تأثیرات آن‌ها بر حقوق بشر و تعهدات فراملی تدوین و اجرا شوند.[1] در حالی که این تحریم‌ها می‌توانند ابزاری مؤثر در قبال تهدیدهای تروریستی موجود در سکوهای دیجیتالی باشند، باید دقت شود که اِعمال این تحریم‌ها موجب نقض حقوق اساسی بشر و کاهش سطح همکاری‌های بین‌المللی نشود. در ضمن، کشورهای عضو بریکس باید تلاش کنند تا میان اهداف امنیتی و حقوق بشر موازنه برقرار کنند. در حالی که تحریم‌های فناورانه می‌توانند ابزار مؤثری برای مقابله با جرائم ارتکابی باشند، اما نباید موجب نقض گسترده حقوق بشر شوند. به‌ویژه، این تحریم‌ها نباید منجر به کاهش سطح همکاری‌های بین‌المللی، محدودیت دسترسی به فناوری‌های پزشکی یا علمی و نقض حقوق اساسی شهروندان در کشورهای هدف شوند.

### ۳. همکاری‌های مشترک بریکس در ارتقای توانمندی‌های امنیت دیجیتالی

با تغییر مفهوم امنیت در حقوق بین‌الملل و ظهور جرائم تروریستی ارتکابی در سکوهای دیجیتالی به‌عنوان تهدیدی نوین، تحریم‌های فناورانه به‌عنوان ابزاری غیرنظامی و بازدارنده، جایگاهی مشروع در مقابله با این تهدید پیدا کرده‌اند. این تحریم‌ها، در چارچوب مسئولیت بین‌المللی دولت‌ها و دفاع مشروع، می‌توانند به‌صورت یک‌جانبه

1. https://afripoli.org/brics-and-the-human-rights-conundrum

یا چندجانبه برای پیشگیری از دسترسی گروه‌های تروریستی به فناوری‌های پیشرفته اعمال شوند (میر عباسی و کورکی‌نژاد قرایی، ۱۳۹۷: ۲۷۲-۲۷۱). در ضمن، برای مقابله مؤثر، بازنگری در قوانین، ایجاد سازوکارهای نوین و بهره‌گیری از ابزارهایی مانند تحریم‌های فناورانه و همکاری‌های بین‌المللی ضروری است تا امنیت جهانی در عصر دیجیتال تضمین شود (Alkharman, 2023: 16-17).

کشورهای عضو بریکس با بهره‌گیری از ظرفیت‌های اقتصادی، فناورانه و دیپلماتیک خود، از تحریم‌های فناورانه علیه کشورهای حامی جرائم تروریستی ارتکابی در سکوهای دیجیتالی بهره گرفته و با استفاده از فناوری‌های نوین و همکاری اطلاعاتی، در راستای شناسایی و مهار تهدیدهای دیجیتالی گام برمی‌دارد (Jiang, & Belli, 2025: 87-89). این رویکرد می‌تواند هم به ارتقای امنیت دیجیتالی اعضای بریکس منجر شود و هم الگویی برای اقدامات بین‌المللی در این رابطه باشد.

کشورهای عضو بریکس با توجه به ظرفیت‌های فناورانه و زیرساختی خود، در تلاش هستند تا رقابت‌پذیری اقتصادی و فناوری خود را در سطح جهانی افزایش دهند. این کشورها در حوزه‌هایی مانند فناوری اطلاعات، هوش مصنوعی، اینترنت اشیاء و... پیشرفت‌های چشمگیری داشته‌اند (Haryono, 2024: 85-86). طبق اعلامیه جهانی حقوق بشر، گسترش فناوری باید دسترسی یکسان به خدمات دیجیتال برای همه افراد، به‌ویژه در مناطق محروم فراهم کند و به حفظ محیط‌زیست توجه شود.[1] فناوری‌های نوین باید آزادی بیان، دسترسی به اطلاعات و حفظ حریم خصوصی افراد را تقویت کنند. کشورهای بریکس باید از حقوق بشر و رقابت عادلانه در توسعه فناوری‌ها، به‌ویژه امنیت سایبری و مالکیت معنوی، محافظت کنند. همچنین باید از نقض آزادی‌های فردی و حریم خصوصی با استفاده از فناوری‌های نظارتی پیشگیری نمایند و در همکاری‌های بین‌المللی استانداردهای حقوق بشر و حقوق حاکمیت ملی را رعایت کنند (Dyman, Gromova & Juchnevicius, 2021: 93-94).

در همکاری‌های دیجیتالی میان کشورهای عضو بریکس، رعایت حقوق بشر و حفظ حریم خصوصی افراد، ضروری است. این کشورها باید استانداردهای بین‌المللی حقوق بشر را در فرآیندهای نظارت و تبادل داده‌ها رعایت کرده و اقدامات امنیتی را مطابق با «مقررات عمومی حفاظت از داده‌ها اتحادیه اروپا»[2] اجرا کنند (Belli, 2020: 1). این دسته از همکاری‌ها، باید با احترام به حاکمیت ملی و استقلال دیجیتالی کشورهای عضو صورت پذیرد و از مداخله غیرقانونی در زیرساخت‌های داخلی دیگر کشورها اجتناب گردد. همچنین، توسعه فناوری‌های

---

۱. بر اساس ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی و ماده ۲۵ اعلامیه جهانی حقوق بشر، دسترسی برابر و بدون تبعیض به اطلاعات، خدمات دیجیتال و استانداردهای زندگی مناسب، از جمله حقوق اساسی افراد محسوب می‌شود.

2. General Data Protection Regulation (GDPR), https://gdpr-info.eu/

امنیتی باید با رعایت حقوق مالکیت فکری، رقابت عادلانه و ملاحظات زیست‌محیطی صورت گیرد. کشورهای عضو بریکس باید موافقت‌نامه‌های بین‌المللی شفاف و مبتنی بر حقوق بشر تدوین کنند تا با چالش‌های نوظهور در امنیت دیجیتالی مقابله کنند و نقش مؤثری در تقویت امنیت دیجیتالی جهانی در مواجهه با جرائم تروریستی ارتکابی در سکوهای دیجیتالی ایفا نمایند.[۱]

با این همه سیاست‌های ناظر بر تحریم‌های فناورانه کشورهای عضو بریکس در قبال جرائم تروریستی ارتکابی در سکوهای دیجیتالی باید مبتنی بر اصول حقوق بین‌الملل، حاکمیت ملی و حقوق بشر باشد. این سیاست‌ها باید به‌طور هدفمند از دسترسی گروه‌های تروریستی به فناوری‌های حساس مانند بلاک‌چین و رمزنگاری پیشگیری کنند، بدون آنکه به حقوق فردی یا خدمات اجتماعی آسیب بزنند. همکاری بین‌المللی با نهادهایی چون سازمان ملل متحد و اینترپل، نظارت مؤثر بر اجرای تحریم‌ها و حفظ رقابت عادلانه و حقوق مالکیت معنوی نیز ضروری است.[۲] البته، تمرکز بر توسعه فناوری‌های ایمن و پاسخگو برای مقابله با تهدیدهای دیجیتالی، نقش مهمی در موفقیت این سیاست‌ها خواهد داشت (Amoo, Atadoga, Abrahams, & Farayola, 2024: 213).

## ٤. چالش‌ها و موانع اجرایی در مهار جرائم تروریستی دیجیتالی

جرائم تروریستی ارتکابی در سکوهای دیجیتالی به‌عنوان تهدیدی پیچیده و فرامرزی در امنیت بین‌المللی و حقوق بین‌المللی دیجیتال مطرح است. تحریم‌های فناورانه برای محدودیت دسترسی گروه‌های تروریستی به فناوری‌های پیشرفته با چالش‌هایی همچون تفاوت قوانین ملی، استفاده از ابزارهای رمزنگاری و شبکه‌های غیرقابل شناسایی و آسیب‌پذیری زیرساخت‌های حیاتی مواجه است. مقابله با این تهدیدها نیازمند راهکارهای جامع فنی، حقوقی و دیپلماتیک است، اما نظارت بر اینترنت می‌تواند با اصول حقوق بشر در تضاد باشد.[۳] همچنین، عدم هماهنگی میان نهادهای داخلی و بین‌المللی و کمبود منابع اجرایی از موانع اصلی است.[٤] درنهایت، تحریم‌ها تنها در صورت

1. BRICS. (2023, August 23). XV BRICS Summit Johannesburg II Declaration: BRICS and Africa – Partnership for mutually accelerated growth, sustainable development and inclusive multilateralism. http://www.brics.utoronto.ca/docs/230823-declaration.html.

2.https://news.cgtn.com/news/2025-07-07/BRICS-denounces-unilateral-sanctions-violating-international-law-1EO6afHZklO/p.html.

3. https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

4. https://waccglobal.org/qatar-digital-surveillance-and-human-rights-abuse/

اجرای راهبرد هماهنگ و مبتنی بر همکاری‌های بین‌المللی و رعایت حقوق بشر مؤثر خواهند بود.[۱] بنابراین، چالش‌ها و موانع اجرایی در چارچوب حقوقی و قانونی اجرای تحریم‌های فناورانه بریکس در مهار جرائم تروریستی ارتکابی در سکوهای دیجیتالی، شامل تفاوت‌های حقوقی، فنی و سیاسی میان کشورهای عضو این گروه است.[۲] تفاوت‌های قانونی درزمینهٔ حریم خصوصی و رویکردهای مقابله با این دسته از جرائم، عدم هماهنگی میان نهادهای داخلی و بین‌المللی، کمبود منابع مالی و فنی و نگرش‌های متفاوت به حریم خصوصی، ازجمله مشکلات اصلی در این راستا محسوب می‌شوند.[۳] علاوه بر این، استفاده گروه‌های تروریستی از فناوری‌های پیشرفته مانند رمزنگاری و شبکه‌های غیرقابل شناسایی و آسیب‌پذیری زیرساخت‌های حیاتی کشورهای عضو در قبال تهدیدهای دیجیتالی، مقابله با این تهدیدها را پیچیده می‌سازد. برای مقابله مؤثر با جرائم تروریستی دیجیتالی و اجرای تحریم‌های فناورانه، کشورهای عضو بریکس نیازمند راهبردهای مشترک و هماهنگ، تقویت همکاری‌های بین‌المللی و رعایت اصول حقوق بشر در کلیه اقدام‌ها هستند (Ponomarenko, 2024: 553).

یکی از چالش‌های اساسی در فرایند مقابله با آماج‌های ناشی از ارتکاب جرائم تروریستی در سکوهای دیجیتالی، فقدان یک تعریف حقوقی جامع، شفاف و مورد اجماع بین‌المللی از مفهوم این جرم است (Stockton & Golabek-Goldman, 2024: 234-236). این خلأ مفهومی به‌ویژه در میان کشورهای عضو بریکس آشکار است؛ چراکه تنوع نظام‌های حقوقی، اختلاف در اولویت‌های امنیتی و تفاوت رویکردهای سیاسی در این کشورها وجود دارد. به‌طور مثال، چین و روسیه این جرائم را به‌طور عمده به‌مثابه تهدیدی علیه حاکمیت، امنیت ملی و زیرساخت‌های اقتصادی مدنظر قرار می‌دهند، در حالی‌که کشورهایی مانند هند بیشتر به ابعاد اجتماعی، انسانی و تأثیرات آن بر نظم عمومی توجه دارند. این تفاوت‌های مفهومی، به‌عنوان مانعی اساسی، روند تدوین سازوکارهای حقوقی و تقنینی مشترک و اجرای هماهنگ راهبرد تهاجمی، ازجمله اِعمال تحریم‌های فناورانه مؤثر را با چالش مواجه می‌سازد. فقدان یک تعریف واحد، نه‌تنها منجر به تفسیرهای متفاوت از مصادیق تهدید می‌شود، بلکه اجرای تحریم‌های فناورانه هدفمند علیه بازیگران غیردولتی دیجیتالی را نیز محدود می‌کند (Rahman & Das, 2024: 986-988). ازاین‌رو، تدوین یک چارچوب حقوقی بین‌المللی و مشترک برای تعریف و تعیین مصادیق جرائم در سکوهای دیجیتالی، به‌ویژه با رویکردهای تروریستی، به‌عنوان پیش‌نیازی ضروری برای

1. https://inclo.net/pillars/surveillance-and-digital-rights/

2. https://carnegieendowment.org/research/2025/03/brics-expansion-and-the-future-of-world-order-perspectives-from-member-states-partners-and-aspirants?lang=en

3. https://www.paho.org/en/news/17-6-2025-strengthening-cooperation-and-exchange-brics-countries-key-advance-priority-health

همکاری مؤثر میان کشورهای عضو بریکس و سایر بازیگران جهانی درزمینهٔ اِعمال تحریم‌های فناورانه و مدیریت تهدیدهای دیجیتالی، از اهمیت ویژه‌ای برخوردار است (Montasari, 2024: 146-147).

در ضمن تحریم‌های فناورانه، به‌ویژه در مواردی که به اعمال محدودیت بر ابزارهای ارتباطی و خدمات دیجیتال منجر می‌شوند، ممکن است با حقوق بشر دیجیتال و آزادی اطلاعات در تعارض قرار گیرند. اِعمال تحریم‌های گسترده در حوزه فناوری می‌تواند آثار منفی قابل توجهی بر دسترسی عموم مردم به اطلاعات، خدمات درمانی برخط و آزادی بیان بر جای گذارد. ازاین‌رو، این مسئله باید به‌عنوان یکی از چالش‌های اساسی حقوق بشری، در فرآیند تدوین و اجرای سیاست‌های کشورهای عضو بریکس درزمینهٔ مقابله با جرائم تروریستی ارتکابی در سکوهای دیجیتالی به‌طور جدی مورد توجه قرار گیرد (Ivanova, & Myltykbaev, 2022: 11-12). این در حالی است که کشورهای عضو بریکس به‌طور عمده فاقد زیرساخت‌های اجرایی کافی برای اِعمال تحریم‌های فناورانه به‌صورت هماهنگ و جهانی هستند. این کمبود می‌تواند منجر به کاهش کارآمدی و اثربخشی سیاست‌های تحریمی این گروه گردد. در حقیقت، در غیاب یک نهاد نظارتی بین‌المللی مستقل و معتبر برای پیگیری و اجرای تحریم‌های فناورانه، بسیاری از این اقدامات تنها به‌صورت داوطلبانه و محدود به حوزه‌های ملی و منطقه‌ای باقی خواهند ماند که موجب کاهش تأثیرگذاری آن‌ها خواهد شد.[1] با این همه مقابله مؤثر با جرائم تروریستی ارتکابی در سکوهای دیجیتالی مستلزم همکاری بین‌المللی، تدوین چارچوب‌های حقوقی و تقنینی مشترک، تقویت توان فنی و نهادی و رعایت اصول بنیادین حقوق بشر است. این رویکرد جامع قادر است به ایجاد محیطی امن‌تر در فضای دیجیتال، بهبود هماهنگی میان کشورهای عضو بریکس و پیشگیری مؤثر از تهدیدهای تروریستی در بستر فناوری‌های نوین کمک کند.[2]

## ۵. آینده‌انگاری و چشم‌انداز حفاظت از امنیت دیجیتالی با اجرای تحریم‌های فناورانه

چشم‌انداز کشورهای عضو بریکس در مهار جرائم تروریستی دیجیتالی از طریق اجرای تحریم‌های فناورانه، به توانایی آن‌ها در ایجاد هماهنگی مؤثر، تدوین چارچوب‌های حقوقی و تقنینی مشترک، تقویت زیرساخت‌های دیجیتالی و رعایت اصول حقوق بشر بستگی دارد. موفقیت این اقدام‌ها مستلزم تعریف دقیق و جامع از جرائم، تقویت همکاری‌های بین‌المللی در تبادل اطلاعات و طراحی سازوکارهای اجرایی هدفمند و مطابق با حقوق بشر

1. https://cihrs-rowaq.org/brics-and-human-rights-issues-impacts-and-expansion-scenarios/?lang=en

2. See: Ministry of Foreign Affairs & Social Communication Secretariat of the Presidency of the Republic of Brazil. (2025, June 9). Use of artificial intelligence and social media by terrorist groups raises concerns among BRICS nations. BRICS. https://brics.br/en/news/use-of-artificial-intelligence-and-social-media-by-terrorist-groups-raises-concerns-among-brics-nations

برای اِعمال تحریم‌ها است. در صورت تحقق این پیش‌نیازها، کشورهای عضو بریکس قادر خواهند بود نقش مؤثری در ارتقای امنیت دیجیتال و حکمرانی جهانی ایفا کنند (Ignatov, 2023: 317-319). بر این اساس، ایجاد یک سند بین‌المللی برای مقابله با جرائم ارتکابی در سکوهای دیجیتالی توسط کشورهای عضو بریکس می‌تواند به تقویت تحریم‌های فناورانه و ارتقای امنیت دیجیتالی جهانی کمک کند. یکی از چالش‌ها، عدم تعریف جامع و پذیرفته‌شده از جرائم ارتکابی است که تدوین آن می‌تواند مبنای حقوقی محکمی برای اقدامات قانونی و تحریم‌ها فراهم کند. به‌علاوه، لازم است سازوکارهای اجرایی و هماهنگ برای اعمال تحریم‌ها طراحی شود که مطابق با استانداردهای حقوق بشر باشد. تقویت همکاری‌های اطلاعاتی و اجرایی میان کشورهای عضو بریکس و دیگر کشورها، با رعایت حریم خصوصی نیز از ارکان مهم این کنوانسیون خواهد بود. این کنوانسیون می‌تواند الگویی برای سایر نهادها و کشورها باشد و همکاری‌های بین‌المللی در این زمینه را تقویت کند.[1] درنهایت، تدوین چنین سندی به جایگاه کشورهای عضو بریکس در حکمرانی دیجیتال جهانی کمک کرده و امنیت دیجیتالی و حقوق بشر در فضای موجود در سکوها را تقویت خواهد کرد (Haibin, 2025: 106-108).

کشورهای عضو بریکس باید همکاری‌های خود را با نهادهای بین‌المللی مانند گروه ویژه اقدام مالی، اینترپل و دفتر مبارزه با مواد مخدر و جرم سازمان ملل متحد تقویت کنند. این همکاری‌ها به تقویت ظرفیت‌های کشورهای بریکس در شناسایی، پیگیری و تحریم گروه‌های تروریستی دیجیتالی کمک خواهد کرد. همکاری با گروه ویژه اقدام مالی به شناسایی منابع مالی تروریسم در فضای دیجیتال و تنظیم تحریم‌های فناورانه کمک می‌کند. همکاری با اینترپل برای تبادل اطلاعات و شناسایی تروریست‌های دیجیتالی اهمیت دارد، به‌ویژه در

---

۱. وزرای امور خارجه کشورهای عضو بریکس در ۲۸ و ۲۹ آوریل ۲۰۲۵ در ریودوژانیرو گرد هم آمدند و ضمن بررسی تحولات جهانی و منطقه‌ای، بیانیه‌ای صادر کردند. در این بیانیه، از «پیش‌نویس کنوانسیون سازمان ملل متحد علیه جرائم سایبری» به‌عنوان دستاوردی مهم در چارچوب نظام حقوق بین‌المللی حمایت شد و بر نقش مؤثر کشورهای عضو بریکس در روند تصویب آن تأکید گردید. وزرا خواستار مشارکت کشورها در کمیته ویژه برای تدوین پروتکل تکمیلی کنوانسیون، امضای سریع آن در هانوی ۲۰۲۵ و همکاری بین‌المللی جهت مقابله با تهدیدهای دیجیتالی شدند؛

- https://brics.br/en/documents/2025-04-29_brics-mfa-chairs-statement.pdf

لازم به‌ذکر است، با توجه به تحولات دیجیتال و پیچیدگی‌های ناشی از آن، نظام حقوقی بین‌المللی نیازمند مقررات جدیدی برای مقابله با جرائم دیجیتالی است. در این راستا، پیش‌نویس کنوانسیون سازمان ملل متحد علیه جرائم سایبری پس از بیست سال تلاش تدوین و در سال ۲۰۲۳ به تصویب رسید. این معاهده که نخستین سند الزام‌آور در این حوزه به شمار می‌رود، کشورهای عضو را به همکاری در مبارزه با جرائم دیجیتال و تهدیدهای مرتبط با آن ترغیب می‌کند؛

- Explanation of Position of the United States on the Adoption of the Resolution on the UN Convention Against Cybercrime in UNGA's Third Committee - United States Mission to the United Nations

افزون براین، علی‌رغم چالش‌های موجود هم‌چون تفاوت‌های مقررات داخلی و مشکلات فنی، تقویت همکاری‌های بین‌المللی و توسعه فناوری‌های امنیتی به‌منظور ارتقای امنیت دیجیتالی، امری ضروری به نظر می‌رسد؛

- https://blog.prif.org/2024/12/09/between-a-rock-and-a-hard-place-the-un-cybercrime-convention/

شرایط بحران. همچنین، دفتر مبارزه با مواد مخدر و جرم سازمان ملل متحد می‌تواند با ارائه مشاوره حقوقی و فنی به کشورهای بریکس در تقویت زیرساخت‌های قانونی برای مقابله با این دسته از جرائم یاری رساند. این همکاری‌ها به کشورهای بریکس امکان می‌دهند تا اقدامات هماهنگ و حقوقی در مقابله با جرائم را اتخاذ کنند و از تناقضات حقوقی پیشگیری کنند. بنابراین، اتخاذ چنین رویکردی می‌تواند به کشورهای بریکس کمک کند تا در سطح جهانی به پیشگامان مبارزه با جرائم تروریستی ارتکابی در سکوهای دیجیتالی تبدیل شوند و امنیت دیجیتالی جهانی را ارتقا دهند.[1]

برای مقابله با جرائم تروریستی در سکوهای دیجیتالی، تقویت توانمندی‌های فناورانه داخلی برای کشورهای عضو بریکس از منظر حقوقی ضرورتی بنیادین اطلاق می‌شود. این کشورها باید با بومی‌سازی فناوری‌های پیشرفته، استقلال فناورانه و حاکمیت دیجیتالی خود را در قبال تحریم‌های یک‌جانبه حفظ کنند؛ اقدامی که در چارچوب حقوق بین‌الملل، مصداق اعمال مشروع حق حاکمیت است. توسعه این فناوری‌ها باید با رعایت اصول حقوق بشر، به‌ویژه حریم خصوصی، حفاظت از داده‌ها و شفافیت همراه باشد. به‌علاوه، نظارت مؤثر و پاسخگویی و پیشگیری از سوءاستفاده از فناوری باید تضمین گردد. در کنار توسعه داخلی، بهره‌گیری از همکاری‌های بین‌المللی نیز ضروری است، مشروط بر رعایت اصول برابری، شفافیت و حقوق بشر. ازاین‌رو، تحقق این اهداف نیازمند چارچوب‌های قانونی منطبق با تحولات فناورانه و اسناد بین‌المللی است تا امنیت دیجیتالی کشورهای عضو بریکس را به‌صورت پایدار، مشروع و مبتنی بر حقوق، تضمین کند (See: Jayan, 2013: 11-12).

## نتیجه‌گیری

کشورهای عضو بریکس، به‌عنوان یک ائتلاف چندجانبه نوظهور، از ظرفیت‌های حقوقی قابل توجهی برای مقابله با تهدیدهای ناشی از جرائم تروریستی ارتکابی در سکوهای دیجیتالی بهره‌مند هستند. در این راستا، بهره‌گیری از تحریم‌های فناورانه به‌عنوان ابزاری مؤثر در مدیریت تهدیدها، به همراه اجرای سیاست‌های تحریمی هدفمند، طراحی سازوکارهای همکاری مشترک و توسعه ظرفیت‌های بومی فناورانه، نقش کلیدی در مهار و کاهش اثرات این تهدیدها ایفا می‌کند. با این حال، تحقق این اهداف با چالش‌هایی حقوقی، سیاسی و اجرایی مواجه است. ازجمله این چالش‌ها می‌توان به عدم تعاریف مشترک از جرائم، تفاوت‌های رویکردهای ملی در قبال تحریم‌های فناورانه و محدودیت‌های موجود در چارچوب‌های حقوقی بین‌المللی اشاره کرد. بنابراین، کشورهای عضو بریکس

1. https://www.crimrxiv.com/pub/48bmtkg0/release/3

باید در کنار تقویت ظرفیت‌های داخلی خود، همکاری‌های بین‌المللی‌شان را گسترش داده و در راستای تدوین چارچوب‌های حقوقی نوین و منطبق با تحولات فناوری گام بردارند.

کشورهای عضو بریکس می‌توانند با بهره‌گیری از ظرفیت‌های فنی و امنیتی و حقوقی خود، به‌طور مؤثر با جرائم تروریستی ارتکابی در سکوهای دیجیتالی و تهدیدهای ناشی از آن‌ها مقابله کنند. این اقدام شامل بومی‌سازی فناوری‌ها، تقویت زیرساخت‌های دیجیتالی، استفاده از فناوری‌های نوین مانند هوش مصنوعی و بلاک‌چین و ایجاد سامانه‌های رصد تهدیدها است. به‌علاوه، تقویت همکاری‌های امنیتی و تدوین چارچوب‌های مشترک برای مقابله با تهدیدهای دیجیتالی و اِعمال تحریم‌ها با رعایت حقوق بشر ضروری است. از بُعد حقوقی، تدوین تعاریف مشترک از جرائم و روزآمدسازی مقررات داخلی برای تسهیل هماهنگی‌های بین‌المللی در مبارزه با این تهدیدها لازم است. همکاری‌های فنی و حقوقی می‌تواند به تقویت امنیت دیجیتالی جهانی کمک کند و تنها از طریق هم‌گرایی حقوقی و نهادی است که این ائتلاف می‌تواند نقش مؤثری ایفا کند.

## منابع


اصلانی، جبار و رنجبریان، امیرحسین (۱۳۹٤). «بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل». ***تحقیقات حقوقی***، دوره ۱۸، شماره ۷۱.

احمری، حسین؛ کحلکی، غلامرضا و رحیم‌پور اصفهانی، حامد (۱۳۹۵). «تحلیل سازه‌انگارانه تروریسم سایبری و رویکرد نظام حقوقی به آن». ***پژوهش‌های بین‌الملل***، دوره ۶، شماره ۱۹.

فرشاسعید، پرویز؛ جلالی، محمود و گودرزی، مهناز (۱٤۰۱). «ضرورت همکاری دولت‌ها در تقویت امنیت سایبری. مطالعات بین‌المللی»، دوره ۱۹، شماره ۲.

عباسی، بیژن و محسن‌پوراژیه، زهرا (۱٤۰۳). «دگردیسی نظام حقوقی درزمینهٔ فضای سایبر». ***مطالعات حقوق عمومی***، دوره ۵۴، شماره ۱.

علی‌پور، جواد و شکاری، حبیب (۱٤۰۰). «پدیده‌های نوظهور؛ تعاریف و مؤلفه‌ها، ابعاد، آثار، تهدیدات و راهکارهای مدیریت آن‌ها». ***مطالعات جنگ***، دوره ۳، شماره ۸.

خاکزاد شاهاندشتی، محسن و میربد، لیلا (۱٤۰۳). «خوانش نوین صلح و امنیت بین‌المللی در پرتو مبارزه با تروریسم سایبری». ***پژوهش‌های روابط بین‌الملل***، دوره ۱۴، شماره ۳.

رضائی، فاطمه؛ رئیسی، لیلا و راعی، مسعود (۱٤۰۱). «نقض حق بر سلامتی ناشی از تحریم‌های بین‌المللی و مسئولیت بین‌المللی دولت‌ها». ***مطالعات بین‌المللی***، دوره ۱۹، شماره ۲.

ملکوتی، رسول و خلیل‌زاده، مونا (۱٤۰۱). «راهکار حقوقی تأمین امنیت سایبری». ***رسانه***، دوره ۳۳، شماره ۱.

میرعباسی، سیدباقر و کورکی‌نژاد قرایی، مجید (۱۳۹۷). «قابلیت تحقق سایبر تروریسم و ارتباط آن با حق ذاتی دفاع مشروع مقرر در مادهٔ ۵۱ منشور سازمان ملل متحد». **مطالعات حقوق عمومی**، دوره ۴۸، شماره ۲.


## Refrences


Abbasi, B., Mohsenpourazieh, Z (2014). The transformation of the legal system in the field of cyberspace. Public Law Studies, 54(1), 353-331 (In persian).

Amoo, O. O., Atadoga, A., Abrahams, T. O., & Farayola, O (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205–217.

Ahmari, H., Kahlaki, G. & Rahimpour Esfahani, H (2016). Structural analysis of cyberterrorism and the legal system's approach to it. International Research, 6(19), 333-305 (In persian).

Alipour, J., Shekari, H (2021). Newly emerging phenomena; their definitions and components, dimensions, effects, threats and management strategies. War Studies, 3(8), 85-73 (In persian).

Alkharman, J. A., & Hassan, I (2023). Cyberterrorism and self-defense in the framework of international law. Journal of Law and Sustainable Development, 11(8), 1–21.

Aslani, J., Ranjbarian, A (2015). Comparative study and analysis of the definition of cyberattack from the perspective of doctrine, practice of countries and international organizations in international law. Legal Research, 18(71), 278-257 (In persian).

Ayodele, O., & Petla, V (2024). Leveraging the BRICS Digital Partnership for Collaborative Digital Governance. Journal of BRICS Studies, 3(1), 1–7.

Belli, L (2020). Data protection in the BRICS countries: Enhanced cooperation and convergence towards legal interoperability. SSRN. https://ssrn. com/abstract=4390979

Belli, L (2021). BRICS countries to build digital sovereignty. In L. Belli (Ed. ), CyberBRICS: Cybersecurity regulations in the BRICS countries (pp. 271–280). Springer Nature.

Bogdanova, I (2021). The potential of common concern of humankind. In T. Cottier & Z. Ahmad (Eds. ), Reshaping the law of economic sanctions for human rights enforcement: The prospects of common concern of humankind (pp. 247–291). Cambridge University Press.

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

Dmitrieva, A., Alshdaifat, S., & Pastukhov, P (2023). The features of the use of information technologies in criminal proceedings in the BRICS countries. BRICS Law Journal, 10(1), 88–108.

Dyman, Y., Gromova, E., & Juchnevicius, E (2021). Regulation of artificial intelligence in BRICS and the European Union. BRICS Law Journal, 8(1), 86–115.

Fernandez, A., Meurice, L., Franke, F., Vuillermoz, C., Gindt, M., Askenazy, F., & Vandentorren, S (2023). Impact of the 7/14/2016 Nice terrorist attack on pediatric emergency department visits thanks to syndromic surveillance: A descriptive study. Frontiers in Public Health, 11, Article 10616791. https://pmc. ncbi. nlm. nih. gov/articles/PMC10616791/

Farshasaid, P., Jalali, M. & Goodarzi, M (2013). The necessity of cooperation between states in strengthening cybersecurity. International Studies, 19(2), 178-163.

Fellmeth, A (2023). Unilateral sanctions under international human rights law: Correcting the record. Yale Journal of International Law. https://yjil. yale. edu/posts/2023-09-06-unilateral-sanctions-under-international-human-rights-law-correcting-the-record

Flonk, D (2021). Emerging illiberal norms: Russia and China as promoters of internet content control. International Affairs, 97(6), 1925–1944.

Hofer, A (2019). The efficacy of targeted sanctions in enforcing compliance with international law. American Journal of International Law, 113, 163–168.

Haryono (2024). BRICS in the digital age: Investigating technological innovation and knowledge sharing as catalysts for economic transformation. The Eastasouth Journal of Information System and Computer Science, 2(2), 84–91.

Iftimie, I. A (2020). Cyber sanctions. Journal of Information Warfare, 19(1), 48–61.

Ignatov, A (2023). Global governance of cyberspace: The BRICS agenda. In A. Baykov & E. Zinovieva (Eds. ), Digital International Relations (pp. 305–327). Springer Nature.

Ivanova, K., & Myltykbaev, M (2022). Implementing the right to information as a key element of freedom of expression in the BRICS countries. BRICS Law Journal, 9(2), 4–29.

Ivanova, L (2023). Criminal liability for cybercrimes in the BRICS countries. BRICS Law Journal, 10(1), 59–87.

Jayan, P. A (2013). BRICS: Advancing cooperation and strengthening regionalism. India Quarterly: A Journal of International Affairs, 64(4), 1–22.

Jiang, M., & Belli, L (Eds. ) (2025). Digital sovereignty in the BRICS countries: How the Global South and emerging power alliances are reshaping digital governance (pp. 39–102). Cambridge University Press.

Khanna, P (2018). State sovereignty and self-defence in cyberspace. BRICS Law Journal, 5(4), 139–158.

Khakzad Shahandeshti, M., Mirbod, L (2024). New reading of international peace and security in the light of combating cyber terrorism. International Relations Research, 14(3), 179-204 (In persian).

Kraft, E., & Wang, J (2009). Effectiveness of cyber bullying prevention strategies: A study on students' perspectives. International Journal of Cyber Criminology, 3(2), 513–535.

Lux, L. M (2018). Una definición de ciberterrorismo. Revista Chilena de Derecho y Tecnología, 7(2), 1–20.

Mallard, G., & Sun, J (2024). International law, security, and sanctions: A decolonial perspective on the transnational legal order of sanctions. Annual Review of Law and Social Science, 20, 97–116.

Malakouti, R., Khalilzadeh, M (2022). Legal strategy for ensuring cyber security. Media, 33(1), 97-69 (In persian).

Markopoulou, D., Papakonstantinou, V., & De Hert, P (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 1–15.

Milan, S., & Hintz, A (2013). Networked collective action and the institutionalized policy debate: Bringing cyberactivism to the policy arena?. Policy and Internet, 5(1), 7–26.

Mir Abbasi, S. B. Korkinezhad-Qaraei, M (2018). The possibility of cyber terrorism and its relationship with the inherent right of self-defense stipulated in Article 51 of the United Nations Charter. Public Law Studies, 48(2), 280-261 (In persian).

Mose, T. N (2024). Attribution and its challenges and the implications for state responsibility under international cyber security law. SSRN. https://ssrn. com/abstract=5087840

Montasari, R (2024). Cyberspace, cyberterrorism and international security in the Fourth Industrial Revolution: Threats, assessment and responses. Springer Nature.

Nikitin, E., & Mensah, C. M (2020). Unified digital law enforcement environment – Necessity and prospects for creation in the "BRICS countries". BRICS Law Journal, 7(2), 59–71.

Ovchinnikova, O., & Upadhyay, N. K (2023). The level of cybersecurity of the BRICS member countries in international ratings: Prospects for cooperation. BRICS Law Journal, 10(1), 7–34.

Patra, S. K., & Muchie, M (Eds. ) (2020). Science, technology and innovation in BRICS countries (1st ed. ). Routledge.

Phillips, C (2024). Digital communication and the rise of online activism. Journal of Communication, 5(3), 31–44.

Ponomarenko, S. V (2024). BRICS as an instrument of international cooperation in global crisis situations. Current Issues of the State and Law, 4(4), 552–558.

Rahman, M. M., & Das, T. K (2024). Countering cyberattacks: Gaps in international law and prospects for overcoming them. Journal of Digital Technologies and Law, 2(4), 973–1002.

Radinliev, P (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing. Journal of Cyber Security Technology, 9(1), 28–78.

Rezaei, F., Raisi, L. & Raei, M (2022). Violation of the right to health resulting from international sanctions and the international responsibility of states. International Studies, 19(2), 143-162 (In persian).

Rusinova, V., Martynova, E., & Kurakina, P (2020). Fighting cyber-attacks with sanctions: New threats, old responses. Higher School of Economics Research Paper No. WP BRP 96/LAW/2020. Available at SSRN: https://ssrn. com/abstract=3742751

Shaweorcid, R., & McAndrew, I. R (2023). Cybersecurity and domestic terrorism: Purpose and future. Journal of Software Engineering and Applications, 16(10), 548–560.

Šturma, P (Ed. ) (2024). International sanctions and human rights. Springer Nature Switzerland.

Stockton, P. N., & Golabek-Goldman, M (2014). Prosecuting cyberterrorists: Applying traditional jurisdictional frameworks to a modern threat. Stanford Law & Policy Review, 25, 211–268.