Journal of
Comparative Criminal Jurisprudence
www.jccj.ir

Volume 5, Issue 4, 2025

Feasibility of Combating Digital Terrorism through the Application of Pattern Design in Criminal Justice for Mitigating Climate Change Sustainability

Peyman Namamian*[1], Sobhan Tayebi[2]

1. Associate Professor Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran. (Corresponding Author)

2. Postdoctoral Researcher, International Criminal Environmental Law, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: 69-90

Corresponding Author's Info
ORCID: *0000-0001-7681-7293*
TELL: *+988632620000*
Email: *p-namamian@araku.ac.ir*

Article history:
Received: *06 May 2025*
Revised: *20 Aug 2025*
Accepted: *04 Oct 2025*
Published online: *22 Dec 2025*

Keywords:
Digital Ecoterrorism, Climate-Related Crimes, Mitigation Strategies, Criminal Justice.

ABSTRACT

This study examines the role and functions of criminal justice mechanisms in addressing digital ecoterrorism and its impacts on the climate system. Given that environmentally destructive actions in electronic contexts can directly or indirectly disrupt climate processes, strengthening legal and criminal tools to prevent and counteract such criminal behaviors is an indispensable necessity. Within this framework, the development and harmonization of international regulations, the use of advanced technologies for monitoring and evidence collection and the enhancement of transnational cooperation are among the key requirements for identifying and prosecuting offenders. Findings from the review of legal documents and authoritative sources indicate that controlling digital ecoterrorism cannot rely solely on environmental policies; it requires the establishment of a coherent criminalization framework, efficient oversight institutions and enforceable international mechanisms. The analyses further suggest that synergy among criminal justice, ecodiplomacy and emerging technologies can play a significant role in mitigating digital threats to the environment. Consequently, the study emphasizes that the establishment of a robust and deterrent criminal justice structure is a fundamental condition for safeguarding ecosystem sustainability and enhancing the effectiveness of other global strategies to combat climate change.

This is an open access article under the CC BY license. © 2025 The Authors.

How to Cite This Article: Namamian, P & Tayebi, S (2025). "Feasibility of Combating Digital Terrorism through the Application of Pattern Design in Criminal Justice for Mitigating Climate Change Sustainability". *Journal of Comparative Criminal Jurisprudence*, 5(4): 69-90.

فصلنامه فقه جزای تطبیقی
www.jccj.ir
انجمن علمی فقه جزای تطبیقی ایران
فصلنامه فقه جزای تطبیقی

دوره پنجم، شماره چهارم، زمستان ۱۴۰۴

امکان‌سنجی مقابله با تروریسم دیجیتالی با کاربست طراحی الگو در عدالت کیفری برای مهار پایداری تغییرات اقلیمی

پیمان نمامیان*[۱]، سبحان طیبی[۲]

۱. دانشیار حقوق کیفری و جرم‌شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران. (نویسنده مسؤول)

۲. پژوهشگر پسادکتری حقوق بین‌الملل کیفری زیست‌محیطی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۶۹-۹۰

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۰-۰۰۰۱-۷۶۸۱-۷۲۹۳

تلفن: ۰۰۰۰ ۳۲۶۲ ۸۶۳ ۹۸+

ایمیل: p-namamian@araku.ac.ir

سابقه مقاله:

تاریخ دریافت: ۱۴۰۴/۰۲/۱۶

تاریخ ویرایش: ۱۴۰۴/۰۵/۲۹

تاریخ پذیرش: ۱۴۰۴/۰۷/۱۲

تاریخ انتشار: ۱۴۰۴/۱۰/۰۱

واژگان کلیدی:

اکوتروریسم دیجیتالی، جرایم اقلیمی، راهبردهای مهار، عدالت کیفری.

چکیده

این پژوهش به بررسی جایگاه و کارکرد سازوکارهای عدالت کیفری در مواجهه با اکوتروریسم دیجیتالی و آثار آن بر نظام اقلیمی می‌پردازد. نظر به این‌که اقدامات مخرب زیست‌محیطی در بسترهای الکترونیکی می‌توانند روندهای اقلیمی را به‌طور مستقیم یا غیرمستقیم مختل سازند، تقویت ابزارهای حقوقی و کیفری برای پیشگیری و مقابله با این دسته از رفتارهای مجرمانه ضرورتی اجتناب‌ناپذیر است. در این چهارچوب، توسعه و انسجام‌بخشی به مقررات بین‌المللی، بهره‌گیری از فناوری‌های نوین در رصد و گردآوری ادله و نیز تقویت همکاری‌های فراملی از مهم‌ترین الزامات شناسایی و تعقیب مرتکبان محسوب می‌شود. یافته‌های حاصل از بررسی اسنادی و منابع معتبر حقوقی نشان می‌دهد که کنترل اکوتروریسم دیجیتال صرفاً با اتکای به سیاست‌های زیست‌محیطی کفایت نمی‌کند و مستلزم ایجاد نظام جرم‌انگاری منسجم، نهادهای نظارتی کارآمد و سازوکارهای الزام‌آور بین‌المللی است. تحلیل‌ها همچنین بیانگر آن است که هم‌افزایی میان عدالت کیفری، اکودیپلماسی و فناوری‌های نوظهور می‌تواند نقش مهمی در کاهش مخاطرات دیجیتالی وارد بر محیط‌زیست ایفا کند، در نتیجه پژوهش بر این نکته تأکید دارد که استقرار یک ساختار کیفری توانمند و بازدارنده، شرطی اساسی برای صیانت از پایداری بوم‌سازگان و تقویت کارآمدی دیگر راهبردهای جهانی مقابله با تغییرات اقلیمی است.

خوانندگان این مجله، اجازه توزیع، ترکیب مجدد، تغییر جزئی و کار روی حاضر به صورت غیرتجاری را دارند.

© تمامی حقوق انتشار این مقاله، متعلق به نویسنده می‌باشد.

مقدمه

هنگامی که تروریسم با عوامل مختلف محیطی، ازجمله زیست‌محیطی، اجتماعی، فرهنگی، فناوری، سیاسی، امنیتی و اقتصادی درآمیخته شود، پیامدهای مخربی به‌دنبال دارد. تروریسم با بهره‌گیری از تمامی ابزارهای محیطی اهداف خود را دنبال می‌کند و مسیر فعالیت‌های خود را به‌صورت سازمان‌یافته و توسعه‌یافته هموار می‌سازد. این روند با سرعت و هماهنگی با فناوری‌های نوین همراه است و از فضاهای دیجیتال مانند سکوها، شبکه‌های اجتماعی، رسانه‌های نوین و برنامه‌های کاربردی هوشمند برای پیشبرد اهداف خود بهره می‌برد. اهداف مذکور می‌تواند شامل تبلیغات، اطلاع‌رسانی برای ایجاد ارعاب، جذب و آموزش نیروهای انسانی، تسهیل عملیات تروریستی، تأمین منابع مالی و خلق راهکارهای خلاقانه برای توسعه فعالیت‌های مجرمانه باشد (Baldassarre, 2023: 457).

این وضعیت به‌دلیل ضعف زیرساخت‌های فنی، کمبود هماهنگی‌های منطقه‌ای و بین‌المللی، ناکافی‌بودن مقررات پیشگیرانه و محدودیت اقدامات پیش‌دستانه تشدید می‌شود و امنیت ملی، منطقه‌ای و بین‌المللی و نیز امنیت شهروندان را با تهدید جدی مواجه می‌سازد. ضعف چهارچوب‌های قانونی و شکاف‌های عملکردی دولت‌ها، شرایط مناسبی برای ترویج تروریسم دیجیتال فراهم می‌آورد و ضرورت بررسی راهکارهای مقابله‌ای را آشکار می‌سازد (Fathi al-Rai *et al*, 2024: 461).

یکی از راهکارهای مؤثر در این زمینه، تقویت مسؤولیت کیفری در قالب عدالت کیفری است که می‌تواند با اعمال مجرمانه تروریسم مقابله جدی داشته باشد. همچنین همکاری‌های بین‌المللی می‌تواند دسترسی تروریست‌ها به فناوری‌ها و منابع دیجیتال را محدود کند و با وضع مقررات و تعهدات الزام‌آور، زمینه پیشگیری از اقدامات مخرب را فراهم سازد و نهادهای ملی را به ایجاد ساختارهای قانونی مقابله با تروریسم ترغیب نماید (Iftikhar, 2024: 781).

امروزه توافق کلی بر این است که هر نوع اقدام تروریستی، چه سنتی و چه دیجیتال، درصورتی‌که آثار مخرب زیست‌محیطی داشته باشد، تهدیدی جدی برای حیات زیست‌کره محسوب می‌شود. تروریسم، چه در شرایط صلح و چه در زمان جنگ، آثار زیان‌باری بر محیط زیست دارد و شکل‌گیری پدیده‌هایی همچون «جنگ سبز» و جنایات زیست‌محیطی ناشی از ترکیب تروریسم و تخریب محیطی، نمونه‌ای از این پیامدهاست. هر فعل یا ترک فعلی که موجب آسیب شدید به محیط زیست و ایجاد مخاطرات اقتصادی، اجتماعی، بهداشتی و سلامت انسان‌ها شود، جرم زیست‌محیطی تلقی می‌گردد (پورهاشمی و همکاران، ۱۳۹۴: ۱۷۸).

استفاده از بسترهای دیجیتال سبب شده است که سوءاستفاده از منابع طبیعی، دستکاری ژنوم، دسترسی به مواد خطرناک و تجارت آن‌ها در فضای برخط، تأثیرات مخربی بر اقلیم و محیط زیست داشته باشد. این اقدامات می‌تواند به تخریب منابع طبیعی، تهدید تنوع زیستی و افزایش آلودگی‌ها منجر شود. بر این اساس، مهار مخاطرات ناشی از تروریسم دیجیتالی اقلیمی به یک ضرورت تبدیل شده است و پژوهش حاضر در پی آن است تا نقش عدالت کیفری در کاهش و کنترل این تهدیدات را مورد واکاوی قرار دهد.

پژوهش حاضر مبتنی‌بر ساختاری است که به بررسی مفهومی عدالت کیفری در مقابله با تروریسم دیجیتالی و ارائه چهارچوبی برای مهار و کنترل این پدیده می‌پردازد. در ادامه، آثار تروریسم در محیط‌های دیجیتالی بر تغییرات اقلیمی با تمرکز بر جنبه‌های مستقیم و غیرمستقیم مورد واکاوی قرار می‌گیرد. اهمیت این مطالعه زمانی برجسته می‌شود که مقابله با تروریسم دیجیتالی – اقلیمی از سطح امکان‌سنجی تا دستاوردهای حقوقی بین‌المللی بررسی شده و باتوجه به رخداد دوسویه اکوتروریسم دیجیتالی و سیاست‌گذاری فعال نهادهای تصمیم‌ساز تحلیل می‌گردد. ازاین‌رو، رویکرد اصلی پژوهش بر مهار اثرات تروریسم دیجیتالی بر تغییرات اقلیمی متمرکز است و سازوکارهای عملیاتی شامل تقویت اکودیپلماسی، ارتقای آگاهی عمومی و بهره‌گیری از فناوری‌های محیط زیستی نوین (اکوفناوری) را دربر می‌گیرد. همچنین راهبردهای مهار اثرات تروریسم دیجیتال بر تغییرات اقلیمی با تأکید بر اثربخشی جرم‌انگاری به‌عنوان ابزار پیشگیری و تضمین حفاظت از اقلیم

مورد تحلیل قرار می‌گیرد. این پژوهش با روش توصیفی – تحلیلی و براساس مطالعات کتابخانه‌ای و منابع علمی معتبر انجام شده است. به‌منظور غنای بحث، استناد به معاهدات و سازوکارهای بین‌المللی، توان پژوهش را در تحلیل ابعاد حقوقی و عملیاتی موضوع افزایش داده است. مطالعه حاضر در چهارچوب امکان‌سنجی عدالت کیفری طراحی شده تا ظرفیت آن برای مهار سوءاستفاده تروریسم از ابزارهای دیجیتالی که تهدیدی برای حیات طبیعی و اقلیم محسوب می‌شوند، ارزیابی گردد.

۱- نقش نظام عدالت کیفری در عصر دیجیتال: چهارچوب پیشگیرانه، یکپارچه و چندلایه برای مقابله با تروریسم دیجیتالی

نظام عدالت کیفری نقش چندوجهی در جامعه ایفا می‌کند و هدف اصلی آن حفظ نظم عمومی، تضمین عدالت و حمایت از حاکمیت قانون است. تروریسم دیجیتالی شامل حملاتی با انگیزه سیاسی یا ایدئولوژیک است که از طریق ابزارهای دیجیتال مانند هک، بدافزار یا نقض داده‌ها انجام می‌شوند و هدفشان ایجاد آسیب، ترس یا اختلال اجتماعی است. این حملات اغلب فراملی هستند و تحقیقات و تعقیب قانونی را پیچیده می‌سازند. چهارچوب‌های قانونی جهانی هنوز پراکنده‌اند و هیچ معاهده متمرکزی به‌طور اختصاصی به تروریسم دیجیتالی نمی‌پردازد، اگرچه برخی کشورها قوانین ملی خاصی تصویب کرده‌اند. تعقیب قانونی همچنین باید تعادل میان امنیت و آزادی‌های مدنی را حفظ کند و اطمینان حاصل نماید که اقدامات ضدتروریسم به حریم خصوصی یا آزادی بیان تجاوز نمی‌کند. همکاری بین‌المللی، ازجمله از طریق اینترپل ضروری است، اما اختلافات حاکمیتی می‌تواند مانع آن شود. اقدامات پیشگیرانه شامل مشارکت دولتی –خصوصی، تشخیص تهدید مبتنی‌بر هوش مصنوعی و ایمن‌سازی زیرساخت‌های حیاتی است. واکنش مؤثر نیازمند چهارچوب‌های قانونی به‌روز، همکاری جهانی تقویت‌شده و رعایت اصول اخلاقی است تا بتوان با تروریسم دیجیتالی مقابله نمود بدون تضعیف حقوق اساسی (Berk *et al*, 2018: 21; Liu, 2024: 16; Onat, *et al*, 2021: 901).

چالش‌های اصلی نظام کیفری شامل اختلافات قضایی ناشی از حملات فرامرزی، استانداردسازی شواهد دیجیتال و تعیین مجازات‌های متناسب با شدت آسیب و قصد مرتکب است. جوامع دموکراتیک باید میان امنیت و آزادی‌های مدنی تعادل برقرار کنند و از سوءاستفاده از قوانین ضدتروریسم جلوگیری نمایند. واکنش‌های قضایی مؤثر نیازمند دادگاه‌های سایبری تخصصی، دستورالعمل‌های روشن برای ارزیابی شواهد دیجیتال، چهارچوب صدور حکم تدریجی و سازوکارهای نظارتی قوی است (Fakhoury, 2024: 611).

نظام‌های عدالت کیفری جهانی در حال شکل‌گیری به یک چهارچوب چندلایه برای مقابله با تروریسم دیجیتالی هستند که ابعاد حقوقی، فناوری و مشارکتی را ادغام می‌کند. در هسته این ساختار، اصول کیفری سنتی برای جرایم دیجیتال تطبیق می‌یابند و قوانین جدید برای جرم‌انگاری اقدامات تروریسم دیجیتالی تدوین می‌شوند. در این مسیر، تحقیقات مبتنی‌بر فناوری‌های پیشرفته، نفوذ به شبکه‌های ناشناس و همکاری بین‌المللی در زمان واقعی از طریق واحدهای جرایم دیجیتالی اینترپل انجام می‌شود. دادگاه‌های سایبری تخصصی با قضات ماهر و پروتکل‌های استاندارد برای رسیدگی به شواهد دیجیتال، اطمینان از محاکمه عادلانه و صدور مجازات متناسب با شدت جرم را تضمین می‌کنند (Bastug & Onat, 2024: 7; Corliss, 2023: 76).

چهارچوب این نظام شامل شش محور اصلی است:

۱- مبانی حقوقی: تعریف جرایم دیجیتال و تعیین مجازات‌ها با استناد به قوانین ملی و معاهدات بین‌المللی مانند کنوانسیون بوداپست؛

۲- تحقیق و انتساب: ردیابی حملات تا عاملان از طریق همکاری فرامرزی و اشتراک‌گذاری اطلاعات، باتوجه به چالش‌های ابزارهای ناشناس و پروکسی‌های دولتی؛

۳- تعقیب قانونی: برقراری تعادل میان الزامات امنیتی و حقوق متهم، تضمین شواهد دیجیتال معتبر و دادگاه‌های تخصصی سایبری؛

۴- محکومیت و بازدارندگی: صدور مجازات متناسب با شدت آسیب و تمایز بین هکرهای آماتور و شبکه‌های سازمان‌یافته تروریسم دیجیتال؛

۵- همکاری بین‌المللی: استفاده از معاهدات استرداد، کمک‌های حقوقی متقابل و هماهنگی قوانین برای پرکردن شکاف‌های قضایی؛

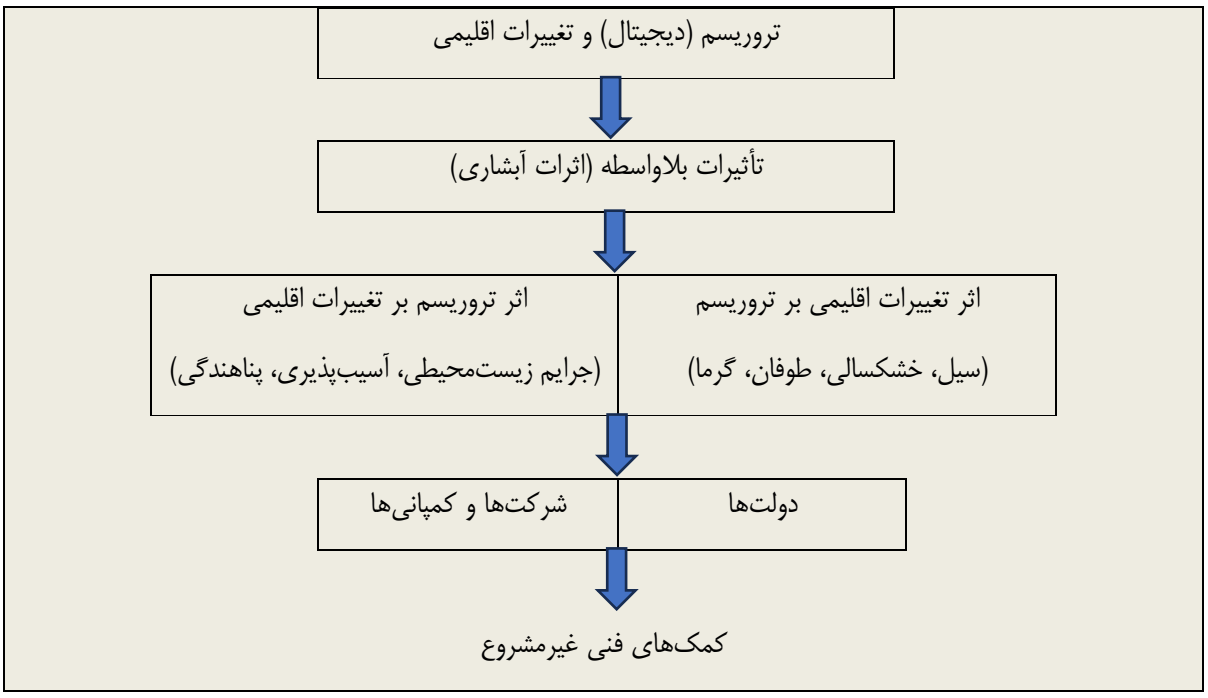
۶- عدالت پیشگیرانه: اقدامات نظارتی و ضدتروریسم با رعایت استانداردهای حقوق بشر و مشارکت دولتی - خصوصی و هوش مصنوعی برای کاهش تهدیدات.

ادغام این اجزا، نظام عدالت کیفری را از نهادی واکنشی به چهارچوبی چابک، پیشگیرانه و مبتنی‌بر قانون تبدیل می‌کند که قادر است با چالش‌های امنیتی عصر دیجیتال مقابله نموده و اصول «انصاف، پاسخ‌گذاری و تناسب» را حفظ کند (Seth Harrison, 2018: 30).

۲- آثار تروریسم در سکوهای دیجیتالی بر تغییرات اقلیمی

۲-۱- سویه‌های آثار مستقیم

تروریسم و تغییرات اقلیمی اثرات دوسویه مستقیم بر یکدیگر دارند. فراتر از تهدیدهایی که ایمنی و امنیت انسان در اثر سیل، خشکسالی ایجاد می‌شود، تغییرات آب و هوایی خطراتی را برای زندگی و رفاه انسان، ازجمله بحران‌های بهداشت عمومی. کمبود سوخت و انرژی، ناامنی غذایی، نابسامانی‌های امنیت ملی، جرایم سازمان‌یافته، جمعیت‌های آسیب‌پذیر، مهاجرت اجباری همراه با «پناهندگان» اقلیمی که از زوال محیطی و اجتماعی در جستجوی امنیت و ثبات و تخریب زیرساخت‌های حیاتی فرار می‌کنند، ایجاد کرده است (Lydon *et al*, 2024: 26). فرآیند اثرات مستقیم تروریسم دیجیتالی و تغییرات اقلیمی به‌صورت آبشاری است که کاملاً همه‌گیر است و بیشترین آثار وخامت را در پی دارد.

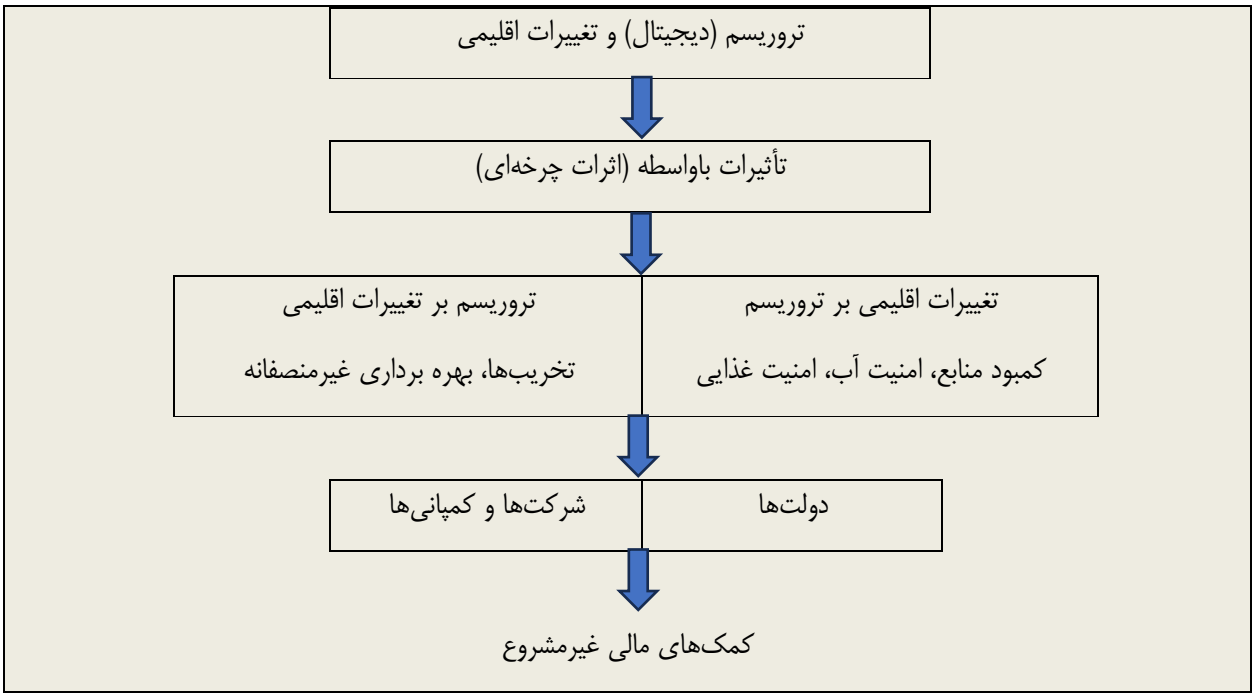


شکل ۱: اثرات بلاواسطه (پژوهشگرمحور)

اگرچه تروریسم حیات سبز زیست کره را با مخاطره جدی روبه رو ساخته، اما تغییرات اقلیمی محرک اصلی تروریسم آینده است. در حال حاضر توسط بسیاری از کشورها به‌عنوان یک تهدید امنیتی راهبردی شناخته شده است، اگرچه نقش بالقوه ای که می‌تواند در برافروختن، تسهیل یا تشدید درگیری‌های تروریستی ایفا کند، نسبتاً ناشناخته مانده است. با این حال، نشانه‌های فزاینده‌ای وجود دارد که نشان می‌دهد تغییرات آب و هوایی – چه از طریق تأثیرات مستقیم یا غیرمستقیم – باید به‌عنوان یک محرک مهم تروریسم در سطح کلان در نظر گرفته شود. مسلماً به خوبی ثابت شده است که علل تروریسم می‌تواند شامل فرآیندهای ژئوپلیتیکی در مقیاس بزرگ و در عین حال عوامل شخصی بسیار پایین‌تر در سطح فردی باشد. در این راستا، عوامل مهم تأثیر تغییر اقلیم بر تروریسم را می توان در مواردی همچون رشد جمعیت، قطبی‌شدن اجتماعی، الگوهای مهاجرت و همچنین توسعه فناوری مشاهده نمود (Silke, 2022: 885). تروریسم دیجیتال قلمرو وسیعی را پوشش می‌دهد که در ادامه مباحث پیش رو مورد تحلیل دقیق تری قرار می‌گیرد.

۲-۲- سویه‌های آثار غیرمستقیم

برخی از سیاست‌گذاران در سراسر جهان، تغییرات آب و هوایی را به‌عنوان یک تهدید امنیتی فزاینده به رسمیت می‌شناسند و به‌طور فزاینده‌ای به تغییر اقلیم به‌خصوص تروریسم اقلیمی اشاره می‌کنند. اثرات با واسطه بین تغییرات آب و هوایی و مواردی مانند کمبود منابع، ازدست‌دادن فرصت‌های اقتصادی و بی‌ثباتی سبب این اتفاق می‌شود. ازاین‌رو تغییرات آب و هوایی به‌طور غیرمستقیم از طریق تأثیر آن بر شرایطی که اغلب به‌عنوان محرک‌های تروریسم است، در نظر گرفته می شوند که منجر به تروریسم می‌شود (Mavrakou *et al*, 2022: 899). فرآیند اثرات غیرمستقیم تروریسم و تغییرات اقلیمی به‌شکل چرخه‌ای است که این مهم چرخه حیاتی طبیعی را با مشکل مواجه ساخته و حقوق نسل‌های آینده در معرض تضییع قرار می‌گیرد.



شکل ۲: اثرات باواسطه (پژوهشگرمحور)

این روند نشان می‌دهد که تروریسم و تغییرات اقلیمی منابع مورد احتیاج انسان‌ها را تهدید می‌کند و بهره‌برداری‌های نامعقول باعث برهم‌خوردن توازن جهانی به‌لحاظ امنیت اقتصادی و اجتماعی می‌شود، اگرچه تغییرات اقلیمی محرک مستقیمی برای درگیری یا افراط‌گرایی خشونت‌آمیز نیست، اما می‌تواند محرک‌های هر دو را تشدید کند و به‌عنوان یک «ضریب خطر» عمل نماید. این عوامل شامل تعامل پیچیده بین عوامل تاریخی، اجتماعی، اقتصادی و سیاسی است که با تغییرات اقلیمی به‌شکل رویدادهای شدید آب و هوایی مکرر و شدید، مانند خشکسالی و قحطی تشدید می‌شود. واکنش‌های امنیتی سخت برای سرکوب درگیری‌ها و ظهور اقتصادهای غیرقانونی می‌تواند سختی‌ها و رنج‌های بیشتری را در چنین نقاط حساس اقلیمی و امنیتی به‌همراه داشته باشد که به نوبه خود می‌تواند باعث جذب نیرو، چه از روی ضرورت معیشت و چه از روی افزایش نارضایتی‌ها شود. به‌عنوان نمونه در منطقه دارفور سودان، درگیری بر سر منابع طبیعی به بحرانی یک دهه‌ای در منطقه‌ای تبدیل شد که بخشی از مسیر اصلی ردیابی و قاچاق انسان و اسلحه (با رویکرد فناورانه) به لیبی را تشکیل می‌دهد. جایی که برنامه توسعه سازمان ملل متحد همچنان بر تخریب منابع طبیعی نظارت دارد و تمام مخازن آب طی دهه گذشته خشک شده‌اند و این امر مستثنی‌کردن ملاحظات تغییرات اقلیمی از تثبیت اوضاع را غیرممکن می‌سازد.

۳- مقابله با تروریسم دیجیتالی – اقلیمی؛ از امکان‌سنجی تا دستاوردهای حقوقی بین‌المللی

۳-۱- رخداد دوسویه اکوتروریسم دیجیتالی

الگوی در حال تکامل جرایم تروریستی اقلیمی دیجیتال و اکوتروریسم دیجیتال دوطرفه، چالش‌های بی‌سابقه‌ای را ایجاد می‌کند که معاهدات بین‌المللی اخیر از طریق چهارچوب‌های قانونی نوآورانه شروع به پرداختن به آن‌ها کرده‌اند (Lu, 2024: 508). پیش‌نویس کنوانسیون جرایم سایبری سازمان ملل متحد در سال ۲۰۲۳، مقرراتی را دربر می‌گیرد که آسیب‌های زیست‌محیطی از طریق ابزارهای دیجیتالی را به عنوان یک عامل تشدیدکننده به رسمیت می‌شناسد و براساس ماده ۶ کنوانسیون بوداپست، اکنون به‌صراحت حملات علیه نظام‌های نظارت بر محیط زیست پوشش می‌یابد. هم‌زمان، دستورالعمل‌های اجرایی توافق‌نامه پاریس (تصمیم ۱۲ COP26) پروتکل‌هایی را برای محافظت از زیرساخت‌های داده‌های اقلیمی در قبال دستکاری دیجیتالی ایجاد می‌کند و چنین مداخله‌ای را به‌عنوان تهدیدی برای تعهدات جهانی آب و هوا به رسمیت می‌شناسد. رویه قضایی نوظهور دادگاه کیفری بین‌المللی در مورد جنگ زیست‌محیطی (براساس قطع‌نامه ICC-ASP/21/Res.5) در حال تدوین اصولی برای تعقیب قانونی عملیات دیجیتالی است که باعث آسیب گسترده زیست‌محیطی می‌شوند، به‌ویژه هنگامی که سامانه‌های کشاورزی هوشمند یا فناوری‌های جذب کربن را هدف قرار می‌دهند. ابتکار عمل اینترپل نشان می‌دهد که چگونه همکاری چندجانبه، مفاد «پیمان آسه‌آن راجع‌به جرایم زیست‌محیطی» را برای بررسی حملات دیجیتالی فرامرزی علیه تصفیه‌خانه‌های آب و شبکه‌های انرژی تجدیدپذیر اعمال می‌کند. دستورالعمل اصلاح‌شده اتحادیه اروپا در مورد حفاظت از زیرساخت‌های حیاتی (COD 2022/0347) به‌طور خاص پایگاه‌های داده تحقیقات اقلیمی و سامانه‌های هشدار اولیه را به‌عنوان دارایی‌های رده یک طبقه‌بندی می‌کند و استانداردهای امنیت دیجیتالی را که با دستورالعمل‌های مرکز دفاع سایبری مشترک ناتو در مورد تهدیدات زیست‌محیطی ترکیبی هم‌سو هستند، الزامی می‌کند (Lee & Choi, 2022: 171). با این حال، شکاف‌های قابل توجهی در اعمال اصل صلاحیت جهانی (مطابق با کنوانسیون‌های ژنو) در مورد موارد دستکاری داده‌های اقلیمی، به‌ویژه هنگامی که بازیگران تحت حمایت دولت از ابهامات قانونی پیرامون فناوری‌های تغییرات اقلیمی تحت «کنوانسیون ممنوعیت به‌کارگیری فنونِ تغییرِ محیط‌زیست برای مقاصد نظامی یا هر هدفِ خصمانهٔ دیگر، مصوب ۱۹۷۶»[1] سوءاستفاده می‌کنند، باقی مانده است. فرآیند اخیر هیروشیما در مورد امنیت دیجیتالی – محیطی گروه هفت، روش‌های استانداردی را برای نسبت‌دادن آسیب‌های زیست‌محیطی به عملیات دیجیتالی خاص پیشنهاد می‌کند که

[1]- https://www.fedlex.admin.ch/eli/cc/1988/1888_1888_1888/it

از چهارچوب‌های اثباتی توسعه‌یافته تحت کنوانسیون سازمان ملل متحد در مورد جرایم سازمان‌یافته فراملی گرفته شده است (Darwish, 2024: 449). این چشم‌انداز در حال تحول در معاهدات، نشان‌دهنده اجماع فزاینده‌ای است که حملات دیجیتالی که ثبات اقلیمی را به خطر می‌اندازند، جرایم بین‌المللی متمایزی را تشکیل می‌دهند، اگرچه چالش‌ها در هماهنگ‌سازی رژیم‌های حقوقی متفاوت در سراسر کنوانسیون‌های حقوق سایبری، حقوق محیط زیست و مبارزه با تروریسم برای مبارزه مؤثر با این تهدید چندبعدی همچنان ادامه دارد (Macklin, 2022: 982).

تلاقی عملیات دیجیتال و تروریسم مرتبط با اقلیم، نشان‌دهنده یک قانون ویژه نوظهور در حقوق بین‌الملل است که نیازمند تحلیل دقیق دکترین است. چهارچوب‌های قانونی فعلی توسط سه متغیر متحول‌کننده، در معرض آزمون‌های سختی قرار گرفته‌اند: ۱- تسلیحاتی‌شدن سامانه‌های کنترل محیطی مبتنی بر اینترنت اشیا؛ ۲- دستکاری الگوریتمی مدل‌های اقلیمی؛ ۳- ظهور شبکه‌های اکوتروریسم هماهنگ‌شده با بلاکچین (Shackelford, 2016: 667). در این راستا، کتابچه راهنمای تالین، اولین تلاش معتبر[1] برای طبقه‌بندی عملیات دیجیتالی منجر به آسیب زیست‌محیطی به‌عنوان نقض بالقوه حقوق بین‌الملل بشردوستانه است که براساس شرط **مارتنس** برای حفاظت از محیط طبیعی تهیه شده است. این با پیش‌نویس اصول حفاظت از محیط زیست در رابطه با درگیری‌های مسلحانه کمیسیون حقوق بین‌الملل در سال ۲۰۲۲ تلاقی دارد که اکنون به‌صراحت زیرساخت‌های دیجیتال ضروری برای ثبات اقلیم را به‌عنوان اشیای محافظت‌شده تحت چهارچوب ماده ۵۶ کنوانسیون‌های ژنو در نظر می‌گیرد (Christensen, 2024: 181).

ازاین‌رو چالش‌های انتساب، شکاف‌های مهمی را در قطع‌نامه ۳۷/۷۷ مجمع عمومی سازمان ملل متحد راجع‌به «پایداری سایبری و امنیت آب و هوایی» آشکار می‌کند[2]، درحالی‌که این قطع‌نامه سازوکارهای گزارش‌دهی برای مداخلات دیجیتالی – زیست‌محیطی تحت حمایت دولت را تعیین می‌کند، اما به پیچیدگی‌های فنی بی‌اعتنا بوده است، ازجمله این بی‌اعتنایی می‌توان به تمایز قائل‌شدن بین هک مجرمانه و فعالیت زیست‌محیطی قانونی طبق ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی، اعمال اصل احتیاط (اصل ۱۵ اعلامیه ریو) برای عملیات دیجیتالی پیشگیرانه علیه تروریسم اقلیمی، محاسبه ضرایب آسیب اکولوژیکی برای صدور حکم طبق مفاد جدید جرایم زیست‌محیطی اساسنامه رم اشاره داشت. با این وصف، تلاش‌ها برای استانداردسازی و پیشگامی درخصوص تروریسم اقلیمی دیجیتالی ضروری به‌نظر می‌رسد (Farber, 2025: 21).

[1]- The Tallinn Manual 3.0's Rule 92bis.

[2]- UN General Assembly's Resolution 77/37 on “Cyber stability and Climate Security”.

جدول ۱: پیشگامی در مهار تروریسم اقلیمی دیجیتالی(پژوهشگرمحور)

نهاد اقدام‌کننده	نوع اقدام	بازه زمانی
کمیته کنوانسیون جرایم سایبری شورای اروپا[1]	– پروتکل‌های زنجیره نگهداری برای جریان‌های داده‌های اقلیمی دستکاری‌شده؛ – تحلیل قانونی نفوذهای سامانه SCADA در تأسیسات انرژی تجدیدپذیر؛ – روش‌های انتساب ردیابی IP با مدل‌سازی اثرات زیست‌محیطی.	از سال ۲۰۲۱ ادامه دارد.
دیوان بین‌المللی دادگستری	– گسترش مسؤولیت دولت تحت داوری Trail Smelter برای آلودگی دیجیتال فرامرزی؛ – اعمال تعهدات مربوط به بررسی‌های لازم از پرونده Pulp Mills به امنیت دیجیتالی سامانه‌های نظارت بر آب و هوا؛ – بازتعریف «حمله مسلحانه» طبق ماده ۵۱ منشور سازمان ملل متحد برای شامل‌کردن اختلال نظام‌مند در زیرساخت‌های ترسیب کربن.	رویه قضایی نوظهور با دستور موقت سال ۲۰۲۳ در پرونده کاستاریکا علیه نیکاراگوئه (پرونده دستکاری داده‌های اقلیمی).
ضمیمه‌های فنی توافق نامه پاریس	– استانداردهای امنیتی مبتنی‌بر ISO/IEC 27032 برای مخازن تحقیقات آب و هوا؛ – مسؤولیت‌های مشترک، اما متمایز (CBDR) برای ظرفیت‌سازی امنیت دیجیتالی در کشورهای آسیب‌پذیر؛ – مکانیسم‌های گزارش‌دهی مبتنی‌بر بلاکچین تحت چهارچوب شفافیت ماده ۱۳.	از سال ۲۰۱۵ ادامه دارد.
گروه ویژه مشترک مؤسسه بین‌المللی یکسان سازی حقوق خصوصی و برنامه محیط زیست ملل متحد	- ایجاد ماتریس‌های مسؤولیت براساس محاسبات خسارت معادل کربن با معیارهای سهل‌انگاری در امنیت دیجیتالی؛ - ایجاد شعب تخصصی در دادگاه کیفری بین‌المللی برای قضاوت در مورد جرایم دیجیتالی اقلیمی؛ - تدوین پروتکل‌های یکسان برای ارزیابی اثرات زیست‌محیطی کدهای مخرب براساس تجزیه و تحلیل چرخه عمر دستورالعمل NIS2 اتحادیه اروپا (الزامات).	Lex Cyber-Clima پیشنهادی از سال ۲۰۲۱ ادامه دارد.

[1]- The Council of Europe's Cybercrime Convention Committee (T-CY)

با این وصف به‌نظر می‌رسد در مورد پیشگیری از آسیب فرامرزی ناشی از عملیات دیجیتالی علیه زیرساخت‌های حیاتی اقلیمی بایستی تلاش‌های مؤثری همچون رژیم‌های مسؤولیت سخت‌گیرانه برای بازیگران دولتی تأمین‌کننده سامانه‌های کنترل زیست‌محیطی، تعهد به کمک‌های فنی طبق اصل نگرانی مشترک بشریت، صلاحیت شبه‌جهانی برای حملاتی تشدی‌کننده آسیب زیست‌محیطی را مد نظر قرار داد. با این توصیف، این تحولات در مجموع نشان‌دهنده ظهور یک رژیم جدید موسوم به «حقوق محیطزیست مبتنی بر شبیه‌سازی‌ها و الگوسازی‌های رایانه‌ای»[1] یا «حقوق محیطزیست در گستره دیجیتال» است که اساساً مفاهیم سنتی نظیر دکترین دفاع از خود در مواجهه با حملات دیجیتالی اقلیمی، استانداردهای فناوری طبق پیش‌نویس معاهده تجارت و حقوق بشر، اعمال دکترین آسیب مداوم به بدافزارهای پایدار در شبکه‌های حسگر محیطی را پیکربندی می‌کند. به هر ترتیب، جامعه حقوقی اکنون باید با این موضوع دست و پنجه نرم کند که آیا چهارچوب‌های موجود مانند کنوانسیون ممنوعیت به‌کارگیری فنونِ تغییرِ محیطزیست برای مقاصد نظامی یا هر هدفِ خصمانهٔ دیگر، مصوب ۱۹۷۶» می‌توانند این ابعاد دیجیتال را در خود جای دهند یا این‌که یک کنوانسیون تخصصی جدید با عنوان دیجیتالیسم برای سامانه‌های اقلیمی برای رسیدگی به این همگرایی بی‌سابقه به‌واسطه تهدیدات فناوری و زیست‌محیطی مورد نیاز است. ازاین‌رو پیش‌آهنگ‌بودن در این مسیر امری کاملاً ضروری است.

۳-۲- سیاست‌گذاری تهاجمی نهادهای تصمیم‌ساز

استانداردسازی درخصوص تروریسم دیجیتالی یک فرآیند آسان نبوده و قدمت آن به سال ۱۹۶۰ برمی‌گردد، اما به‌لحاظ چهارچوبی و توسعه آن به سال ۱۹۹۰ به بعد برمی‌گردد. ازاین رو در سال ۲۰۰۱ کنوانسیون جرایم رایانه‌ای و تقویت این کنوانسیون در سال ۲۰۰۴، قطع‌نامه ۲۳۴۱ سال ۲۰۱۷ درخصوص راهبردهای جهانی مبارزه با تروریسم، برنامه جهانی مبارزه با تروریسم راجع به امنیت سایبری و فناوری‌های نوین ۲۰۲۰ (نمامیان و شهبازی، ۱۴۰۳: ۸۴) و کنوانسیون چهارچوبی شورای اروپا در مورد هوش مصنوعی و حقوق بشری دموکراسی و حاکمیت قانون ۲۰۲۴ (CETS225) و قوانینی که در سطوح ملی است، وجود دارد (بهادری جهرمی و همکاران، ۱۴۰۳: ۱۹). در این خصوص تلاش‌های فراوانی در کمیته اجرایی شورای مبارزه با تروریسم سازمان ملل[2] انجام پذیرفته و تلاش‌های اصلاحی دیگر نیز انجام گرفته که ماهیت جهانی دارند که ناشی از ابتکارات دولتی و منطقه‌ای بوده که در قالب موافقت‌نامه ارائه گردیده است. هریک از این ابتکارات در مرحله متفاوتی از توسعه هستند و هر کدام نیاز مهمی را برطرف می‌کنند، اما هریک لایه جدیدی از پیچیدگی را برای وضعیت داده‌های فرامرزی ایجاد می‌کند.

جدول ۲: تلاش‌های عمده برای اصلاحات (CTED, 2022: 18)

ابتکارات چندجانبه	
کنوانسیون سازمان ملل متحد علیه جرایم سایبری؛ تقویت همکاری‌های بین‌المللی برای مبارزه با برخی جرایم ارتکابی از طریق سامانه‌های فناوری اطلاعات و ارتباطات و به اشتراک‌گذاری مدارک به‌صورت الکترونیکی جرایم جدی[3]	کنوانسیون سازمان ملل متحد علیه جرایم سایبری توسط مجمع عمومی سازمان ملل متحد در ۲۴ دسامبر ۲۰۲۴ در نیویورک با قطع‌نامه ۲۴۳/۷۹ به تصویب رسید.

[1] Jus in Silico Ambientale

[2]- CTED: Counter-Terrorism Committee Executive Directorate

[3]- United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (2024).

شورای اروپا: دومین پروتکل الحاقی به «کنوانسیون بوداپست[۱]»	کنوانسیون بوداپست سال ۲۰۰۲ به تصویب رسید و پروتکل الحاقی دوم سال ۲۰۲۲ به تصویب رسید.
ابتکارات منطقه‌ای و فرامنطقه‌ای	
اتحادیه اروپا: مقررات مدارک الکترونیکی[۲]	سال ۲۰۱۹ به تصویب رسید.
چهارچوب حقوق مدنی برزیل برای اینترنت[۳]	سال۲۰۱۴ به تصویب رسید و قانون حفاظت از داده‌ها در برزیل به سال ۲۰۲۱ اجرایی شد.
چین؛ قانون امنیت داده‌ها و قانون حفاظت از اطلاعات شخصی[۴]	سال ۲۰۱۷ تصویب شد و سال ۲۰۲۱ به‌روزرسانی گردیده است.
هند؛ لایحه حفاظت از داده‌های شخصی[۵]	سال ۲۰۲۱ به تصویب رسید.
فدراسیون روسیه: قانون بومی‌سازی داده‌ها[۶]	سال ۲۰۱۵ به تصویب رسید.
ایالات متحده آمریکا؛ قانون شفاف‌سازی استفاده از داده‌ها در خارج از کشور[۷]	سال ۲۰۱۸ به تصویب رسید.
ابتکارات سازمان ملل متحد	
ابتکار جهانی اداره اجرایی کمیته مبارزه با تروریسم (CTED)، دفتر مواد مخدر و جرم سازمان ملل متحد (UNODC) و انجمن بین‌المللی دادستان‌ها (IAP)[۸]	طی قطع نامه‌های ۲۳۲۲ (۲۰۱۶) و ۲۳۹۶ (۲۰۱۷) شورای امنیت درخصوص تشویق به همکاری دولت‌ها با بخش خصوصی درخصوص دستیابی به داده‌های دیجیتال و امنیت آن است.
دفتر مبارزه با مواد مخدر و جرم سازمان ملل متحد (UNODC)[۹]	مرکز مدارک الکترونیکی سال ۲۰۰۷
نقشه راه دبیرکل برای همکاری دیجیتال[۱۰]	از سال ۲۰۱۸ با تشکیل هیأت بلندپایه همکاری‌های دیجیتال در عصر وابستگی متقابل دیجیتال که تابه‌حال نیز ادامه دارد که بر طیف وسیعی از مسائل، ازجمله حقوق بشر دیجیتال، هویت دیجیتال، حریم خصوصی و حفاظت از داده‌ها اشاره دارد.
مرکز مبارزه با تروریسم سازمان ملل متحد (UNCCT) دفتر مبارزه با تروریسم سازمان ملل متحد (UNOCT) و سازمان بین‌المللی پلیس جنایی (INTERPOL)[۱۱]	ارائه هندبوک با عنوان استفاده از اینترنت و رسانه‌های اجتماعی برای تحقیقات ضد تروریسم[۱۲] در سال ۲۰۲۱
ابتکارات پراهمیت	

1- Council of Europe: Second Additional Protocol to “Budapest Convention”.
2- European Union: e-Evidence regulation.
3- Brazilian Civil Rights Framework for the Internet.
4- China: Data Security Law and Personal Information Protection Law.
5- India: Personal Data Protection Bill 2021.
6- Russian Federation: Data-Localization Law.
7- United States: Clarifying Lawful Overseas Use of Data Act (CLOUD Act).
8- CTED: The Counter-Terrorism Committee Executive Directorate; UNODC: The United Nations Office on Drugs and Crime; IAP: The International Association of Prosecutors.
9- UNODC: United Nations Office on Drugs and Crime.
10- Secretary-General’s Roadmap for Digital Cooperation.
11- UNCCT: United Nations Counter-Terrorism Centre; UNOCT: The United Nations Office of Counter-Terrorism; INTERPOL: The International Criminal Police Organization.
12- Using the Internet and Social Media for Counter-Terrorism Investigations.

پروژه مشترک اتحادیه اروپا و یوروپل درخصوص همکاری عدالت کیفری و اجرای قانون[1]	با محوریت بهره‌برداری از دانش داده‌ها سال ۲۰۲۱ تصویب شد.
شبکه جرایم سایبری گروه ۸[2]	از سال ۱۹۹۷ تابه‌حال با رویکرد داده‌های اضطراری و حفظ داده‌ها ادامه دارد.
اینترنت و شبکه سیاست قضایی[3]	از سال ۲۰۲۰ تا به حال با رویکرد اینترنت و خطومشی قضایی ادامه دارد.

این‌ها نشان می‌دهند که چه تلاش‌های مؤثری درجهت مقابله جدی با تروریسم دیجیتالی در سطح جهانی انجام پذیرفته و چه رویکردهایی مد نظر بوده است و قطعاً این اصلاحات نتایج مثبتی نیز دربر داشته است. ازجمله این نتایج متحدالشکل‌کردن انواع مقابله با روش‌های متفاوت و متعدد تروریسم، همکاری چندجانبه سازمان‌های بین‌المللی در دستیابی به رویکرد واحد برای تقابل با تروریسم دیجیتالی می‌باشد. در این راستا چالش‌ها متعددی نیز در سایه این همکاری‌های جهانی نیز وجود دارد.

جدول ۳: روندها و چالش‌ها (CTED, 2022)

چندپارگی قانونی	توسعه چهارچوب‌های قانونی، پیچیدگی‌هایی به‌همراه دارد و هم‌زیستی چندین رژیم حقوقی مشترک موجب چندپارگی مقررات وتلاش‌های دیپلماتیک شود.
کاهش قابلیت همکاری	تعارض در اجرای مقررات با عنایت به رویکرد داخلی دولت‌ها به‌واسطه منافع ملی.
بومی‌سازی	گسترش اینترنت و دسترسی به داده‌ها در قالب مقررات داخلی و ساختار محلی.
نگرانی‌های بین‌المللی حقوق بشری	نگرانی از عدم تضمین حقوق بشر در جریان حفظ داده‌ها و مقابله با تروریسم.
رویه بخش خصوصی	رویکرد امنیت اطلاعات و داده‌ها و حفظ آن‌ها بستگی به تمکن و قدرت شرکت‌های بزرگ و کوچک دارد.

تمرکز ارائه‌دهندگان کمک‌های فنی برای پیشرفت و پرداختن به چالش‌ها باید بر تضمین قابلیت همکاری و گسترش ظرفیت مجریان اجرای قانون در حال توسعه بین رژیم‌های مختلف باشد (Terzi, 2019: 236). همچنین واضح است که تضمین احترام و رعایت قوانین بین‌المللی حقوق بشر و آزادی‌های اساسی از اجزای ضروری اصلاحات و تلاش‌های ظرفیت‌ساز هستند.

[1]- Eurojust: The European Union Agency for Criminal Justice Cooperation; Europol: The European Union Agency for Law Enforcement Cooperation.

[2]- The G7 24/7 Cybercrime Network Began under the Auspices of the Group of Eight (G8).

[3]- I&JPN: Internet and Jurisdiction Policy Network.

جدول ۴: نگاه به آینده (پژوهشگرمحور)

ضمانت	فرصت	چالش	مصلحت	رژیم
تضمین قابلیت همکاری	افزایش ظرفیت	مقابله با تروریسم‌شویی	صلح‌گرایی و صلح‌پذیری	نظم دیجیتال
ایجاد چهارچوب جهانی با استناد به معاهدات بنیادین مانند میثاق بین‌المللی حقوق مدنی و سیاسی سازمان ملل متحد.	با در نظرگرفتن ساختارهای معاهداتی بین‌المللی و رعایت شئونات داده‌ها و افزایش راهکارهای عدم دسترسی تروریسم به ساختارهای دیجیتالی.	رویکردی در رویارویی و سرکوب تعامل و به‌رسمیت‌شناختن تروریست‌ها و گروه‌های تروریستی.	نگاه جهانی به تعاملات مثبت دولت‌ها برای دورشدن از فضای تنش‌های مخرب و جمع شدن بساط ساختارهای سوءاستفاده‌گر مانند تروریسم.	شامل رکن مالی، تجاری، سیاسی، امنیتی، فرهنگی و دیجیتالی با رویکرد طرح‌های برون‌مرزی شامل زیرساخت‌های مالی، ابتکارات فناوری و سلامت است.

خوشبختانه، این تلاش‌ها می‌تواند نقاط عطف مهمی در حل جرایم دیجیتالی فرامرزی و زمینه‌ساز توسعه همکاری‌ها در مورد بهره‌مندی صحیح از سکوهای دیجیتال باشد و این مهم سبب می‌شود که به درخواست‌های جهانی اجرای قانون برای دسترسی به شواهد الکترونیکی کمک کند. ازاین‌رو با یک چشم‌انداز روشن می‌توان به حق بر دسترسی امن و کم‌چالش به اطلاعات و داده‌ها و کنترل دسترسی‌ها ناصواب نزدیک شد که این مسأله قابلیت همکاری‌ها را افزایش می‌دهد. در این میان، تلاش‌های مداوم باعث می‌شود که یک چشم‌انداز حقوقی فرامرزی برای رفع موانع مقابله با تروریسم دیجیتالی و اثرات نامعقول آن ترسیم گردد. با این وصف به‌نظر می‌رسد با تقویت قوانین چه از بعد فنی و چه از بعد حقوقی، زمینه جرم انگاری جرایم دیجیتالی فراهم شده و این باعث می‌شود که پاسخ‌گذاری و تعقیب قانونی مؤثرتر انجام پذیرد.

۴- مهار اثرگذاری تروریسم دیجیتالی بر تغییرات اقلیمی؛ سازوکارهای عملیاتی

۴-۱- تقویت اِکودیپلماسی و آگاهی‌بخشی بشری

دیپلماسی زیست‌محیطی و آگاهی بشردوستانه نقش مهمی در پرداختن به تلاقی تروریسم و تغییرات اقلیمی ایفا می‌کنند، زیرا هر دو موضوع پیامدهای گسترده‌ای برای ثبات جهانی و سلامت محیط زیست دارند. یکی از جنبه‌های اساسی دیپلماسی زیست‌محیطی شامل تقویت همکاری بین‌المللی برای مبارزه با جرایم زیست‌محیطی مرتبط با تروریسم است. بسیاری از گروه‌های تروریستی عملیات خود را از طریق قطع غیرقانونی درختان، قاچاق حیات وحش و قاچاق نفت تأمین مالی می‌کنند که اکوسیستم‌ها را ویران کرده و تغییرات اقلیمی را تسریع می‌کنند. تلاش‌های دیپلماتیک باید بر تقویت توافق‌نامه‌های جهانی، مانند کنوانسیون سازمان ملل متحد علیه جرایم سازمان‌یافته فراملی، متمرکز شوند تا شامل مقررات سخت‌گیرانه‌تری علیه بهره‌برداری از محیط زیست توسط گروه‌های مسلح باشد. علاوه‌بر این، کشورهای آسیب‌پذیر در برابر فعالیت‌های تروریستی باید در نظارت و حفاظت از منابع طبیعی، ازجمله نظارت ماهواره‌ای و اشتراک‌گذاری اطلاعات مرزی برای پیشگیری از تجارت غیرقانونی، حمایت شوند (Tayebi, 2020: 18).

آگاهی بشردوستانه نیز به‌همان اندازه مهم است، زیرا جوامع آسیب‌دیده از تروریسم اغلب با بحران‌های پیچیده‌ای، ازجمله فروپاشی محیط زیست مواجه می‌شوند. افزایش آگاهی در مورد پیامدهای زیست‌محیطی اقدامات تروریستی می‌تواند حمایت محلی و بین‌المللی را برای تلاش‌های بهبودی بسیج کند. سازمان‌های بشردوستانه باید توان‌بخشی محیط زیست را در برنامه‌های کمکی خود بگنجانند و اطمینان حاصل کنند که جمعیت‌های آواره به منابع پایدار دسترسی دارند و اکوسیستم‌های آسیب‌دیده احیا می‌شوند. کمپین‌های آموزشی همچنین می‌توانند با برجسته‌کردن این‌که چگونه تخریب محیط زیست، بقا و رفاه بلندمدت آن‌ها را تضعیف می‌کند،

جوامع را برای مقاومت در برابر جذب تروریست‌ها توانمند سازند (Montasari, 2024: 89).

یکی‌دیگر از راهبردهای مهم، ارتقای تاب‌آوری اقلیمی در مناطق مستعد درگیری است. گروه‌های تروریستی اغلب از حکومت ضعیف و کمبود محیط زیست برای کسب نفوذ، به‌ویژه در مناطقی که از خشکسالی، جنگل‌زدایی یا تخریب خاک رنج می‌برند، سوءاستفاده می‌کنند. با سرمایه‌گذاری در پروژه‌های کشاورزی پایدار، احیای جنگل‌ها و انرژی‌های تجدیدپذیر، دولت‌ها و سازمان‌های غیردولتی می‌توانند آسیب‌پذیری‌هایی را که تروریست‌ها از آن‌ها سوءاستفاده می‌کنند، کاهش دهند. دیپلماسی زیست‌محیطی می‌تواند مشارکت بین ملت‌ها را برای به اشتراک‌گذاشتن فناوری و تخصص در سازگاری با آب و هوا تسهیل کند و اطمینان حاصل شود که مناطق شکننده کمتر در معرض تهدیدات زیست‌محیطی و امنیتی قرار می‌گیرند (Shackelford, 2016: 671).

پرداختن به علل ریشه‌ای تروریسم – مانند فقر، نابرابری و حاشیه‌نشینی سیاسی – می‌تواند به‌طور غیرمستقیم تأثیر زیست‌محیطی آن را کاهش دهد. تلاش‌های بشردوستانه‌ای که توسعه اقتصادی، آموزش و شمول اجتماعی را در اولویت قرار می‌دهند، جوامع پایدارتری را ایجاد می‌کنند که احتمال کمتری دارد تحت تأثیر گروه‌های افراطی قرار گیرند. در همین حال، دیپلماسی زیست‌محیطی می‌تواند تضمین کند که سیاست‌های اقلیمی حساس به منازعه هستند و از اقداماتی که ممکن است ناخواسته تنش‌ها را تشدید کنند، مانند تصرف زمین در مقیاس بزرگ برای حفاظت از محیط زیست که باعث جابه‌جایی جمعیت محلی می‌شود، اجتناب شود (نمامیان، ۱۴۰۳: ۲۱۸).

با این توصیف، مهار تأثیر جنایات تروریستی بر تغییرات اقلیمی نیازمند ترکیبی از تعامل دیپلماتیک، اقدامات بشردوستانه و نظارت بر محیط زیست است. با ادغام این راهبردها، جامعه بین‌المللی می‌تواند ظرفیت‌های مالی و عملیاتی گروه‌های تروریستی را تضعیف کند و در عین حال از اکوسیستم‌ها محافظت کرده و از جمعیت‌های آسیب‌دیده حمایت کند. ماهیت به هم پیوسته این چالش‌ها، نیازمند یک پاسخ هماهنگ است که در آن پایداری و امنیت زیست‌محیطی به‌عنوان اهداف تقویت‌کننده متقابل و نه مسائل جداگانه دنبال می‌شوند.

۴-۲- بهره‌مندی از اکوفناوری

تلاقی تروریسم و تغییرات اقلیمی، چالش جهانی پیچیده‌ای را ایجاد می‌کند که در آن بازیگران غیردولتی از طریق تخریب عمدی، بهره‌برداری غیرقانونی از منابع و اختلال در تعادل اکولوژیکی، تخریب محیط زیست را تشدید می‌کنند. فناوری زیستی – کاربرد فناوری‌های نوآورانه و پایدار برای مشکلات زیست‌محیطی – مسیری امیدوارکننده برای کاهش این تأثیرات با مختل‌کردن تأمین مالی تروریسم، احیای اکوسیستم‌های آسیب‌دیده و ایجاد تاب‌آوری اقلیمی در مناطق آسیب‌پذیر ارائه می‌دهد (Rose, 2022: 166). سازمان‌های تروریستی اغلب برای تأمین مالی عملیات خود به فعالیت‌های مخرب زیست‌محیطی، ازجمله قطع غیرقانونی درختان، معدن‌کاری و سرقت نفت متکی هستند. این فعالیت‌ها نه‌تنها اکوسیستم‌های محلی را ویران می‌کنند، بلکه به میزان قابل توجهی در انتشار کربن جهانی نیز نقش دارند. فناوری زیستی می‌تواند از طریق مکانیسم‌های پیشرفته نظارت و اجرا با این شیوه‌ها مقابله کند. تصویربرداری ماهواره‌ای، نظارت پهپادی و تجزیه و تحلیل داده‌های مبتنی‌بر هوش مصنوعی، ردیابی بلادرنگ فعالیت‌های غیرقانونی زیست‌محیطی را امکان‌پذیر می‌سازد. به‌عنوان مثال، سازمان دیده‌بان جنگل جهانی از فناوری ماهواره‌ای برای شناسایی نقاط مهم جنگل‌زدایی استفاده می‌کند و به مقامات اجازه می‌دهد قبل از وقوع خسارات گسترده مداخله کنند. به‌طور مشابه، سامانه‌های ردیابی مبتنی بر بلاکچین می‌توانند به تأیید قانونی‌بودن صادرات منابع طبیعی کمک کنند و یک جریان درآمد اساسی برای گروه‌های تروریستی را قطع کنند. یکی‌دیگر از کاربردهای حیاتی فناوری زیستی در اصلاح محیط زیست پس از جنگ است. حملات تروریستی اغلب میدان‌های نفتی، خطوط لوله و تأسیسات صنعتی را هدف قرار می‌دهند که منجر به نشت فاجعه‌بار و آلودگی سمی می‌شود. زیست‌پالایی – استفاده از میکروارگانیسم‌ها برای تجزیه آلاینده‌ها – یک راه حل مقرون‌به‌صرفه و پایدار برای پاک‌سازی خاک و آب آلوده ارائه می‌دهد. در مناطق جنگی مانند عراق و نیجریه، جایی که

داعش و بوکوحرام خرابکاری‌های نفتی گسترده‌ای انجام داده‌اند، استقرار باکتری‌های مهندسی ژنتیک‌شده یا گیاه‌پالایی (استفاده از گیاهان برای جذب سموم) می‌تواند بهبود را تسریع کند. سامانه‌های تصفیه آب با انرژی خورشیدی همچنین می‌توانند دسترسی به آب آشامیدنی تمیز را در مناطقی که زیرساخت‌ها تخریب شده‌اند، بازیابی کنند (Rawat, 2023: 897).

فناوری‌های انرژی تجدیدپذیر می‌توانند آسیب‌پذیری جوامع را در برابر سوءاستفاده تروریستی بیشتر کاهش دهند. بسیاری از گروه‌های تروریستی در مناطقی با فقر انرژی رشد می‌کنند، جایی که جمعیت‌ها به منابع کمیاب و مورد مناقشه وابسته هستند (Johnson, 2024: 522). ریزشبکه‌های خورشیدی غیرمتمرکز، توربین‌های بادی و سامانه‌های بیوگاز، انرژی قابل اعتماد و خارج از شبکه را فراهم می‌کنند و کنترلی را که گروه‌های مسلح بر منابع سوخت اعمال می‌کنند، کاهش می‌دهند. برای مثال، در سومالی، جایی که الشباب از قاچاق زغال چوب سوءاستفاده کرده است، ابتکارات انرژی خورشیدی، معیشت جایگزینی را برای قاچاقچیان سابق ارائه داده و در عین حال جنگل‌زدایی را کاهش داده است (Olumoye, 2013: 14).

فناوری زیست‌محیطی می‌تواند سامانه‌های هشدار اولیه را برای بلایای اقلیمی و تهدیدات امنیتی تقویت کند. تجزیه و تحلیل پیش‌بینی‌کننده، با ترکیب داده‌های اقلیمی با ارزیابی ریسک درگیری، می‌تواند مناطقی را شناسایی کند که در آن‌ها استرس محیطی ممکن است منجر به افزایش فعالیت تروریستی شود. این امر امکان مداخلات پیشگیرانه بشردوستانه و صلح‌آفرین را فراهم می‌کند (Sieber, 2006: 437). به‌عنوان مثال، در ساحل، جایی که بیابان‌زایی باعث تشدید درگیری‌ها بر سر زمین می‌شود، ادغام نظارت بر آب و هوای ماهواره‌ای با شبکه‌های امنیتی محلی می‌تواند به کاهش تنش‌ها قبل از تبدیل‌شدن به خشونت کمک کند، درنتیجه فناوری زیست‌محیطی یک ابزار چندبعدی برای پرداختن به پیوند تروریسم و تغییرات اقلیمی فراهم می‌کند. این نوآوری‌ها با افزایش نظارت بر محیط زیست، تسریع بازیابی اکوسیستم، ترویج انرژی‌های تجدیدپذیر و تقویت تاب‌آوری اقلیمی، می‌توانند تأمین مالی تروریسم را مختل کنند، از جوامع آسیب‌پذیر محافظت کنند و به ثبات زیست‌محیطی بلندمدت کمک کنند (Sarkar & Shukla, 2024: 9).

۵- راهبردهای مهار اثرات تروریسم دیجیتالی بر تغییرات اقلیمی

۵-۱- اثربخشی جرم‌انگاری به‌مثابه اقدامی پیشگیرانه

تأثیر تروریسم دیجیتال بر تغییرات اقلیمی از طریق چندین مسیر آشکار می‌شود، ازجمله حملات دیجیتالی به شبکه‌های برق که باعث وابستگی به منابع انرژی کثیف‌تر می‌شود، دستکاری داده‌های انتشار گازهای گلخانه‌ای برای تضعیف سیاست‌های اقلیمی و هک‌کردن سامانه‌های کنترل زیست‌محیطی در صنایعی مانند نفت و گاز برای ایجاد نشت‌های عمدی (میرمحمدصادقی و قدیری بهرام‌آبادی، ۱۳۹۴: ۳۳). این اقدامات اغلب در مناطق خاکستری قانونی قرار می‌گیرند، زیرا بسیاری از قوانین جرایم دیجیتالی موجود با در نظرگرفتن پیامدهای زیست‌محیطی طراحی نشده‌اند. یک رویکرد جرم‌انگاری راهبردی شامل تعریف دسته‌های جدیدی از «جرایم زیست‌محیطی - دیجیتالی» در قوانین حقوقی بین‌المللی و داخلی است که به‌صراحت اعمالی را که در آن‌ها نفوذهای دیجیتال منجر به آسیب زیست‌محیطی قابل اثبات می‌شوند، مجازات می‌کند. کنوانسیون بوداپست در مورد جرایم دیجیتالی می‌تواند گسترش یابد تا شامل پروتکل‌هایی شود که اختلال در سامانه‌های انرژی تجدیدپذیر یا شبکه‌های نظارت بر آب و هوا را جرم‌انگاری می‌کنند، مشابه نحوه برخورد فعلی با نقض داده‌ها و جرایم مالی (GCTF, 2025: 7-14).

در سطح ملی، قانون‌گذاران باید قوانین مجازات را به‌روزرسانی کنند تا آسیب‌های زیست‌محیطی را به‌عنوان یک عامل تشدیدکننده در پرونده‌های تروریسم دیجیتالی بگنجانند. به عنوان مثال، هکری که سیستم‌های سیل‌خیز را در یک منطقه آسیب‌پذیر غیرفعال می‌کند، نه‌تنها به‌دلیل دسترسی غیرمجاز، بلکه به‌دلیل به خطرانداختن بی‌ملاحظه اکوسیستم‌ها و جوامع نیز باید با اتهاماتی روبه‌رو شود. اصل قانونی «قصد دوگانه» که در آن مرتکبان هم به‌دلیل جرم دیجیتال و هم به‌دلیل

پیامدهای زیست‌محیطی پیش‌بینی‌شده آن تحت تعقیب قانونی قرار می‌گیرند، می‌تواند بازدارنده‌های مطلوب و داری اثرگذاری قوی ایجاد کند.

در این راستا، همکاری بین‌المللی حیاتی است، زیرا تأثیرات اقلیمی تروریسم دیجیتال اغلب از مرزها عبور می‌کند. یک تلاش هماهنگ از طریق برنامه جرایم زیست‌محیطی اینترپل و دفتر مبارزه با مواد مخدر و جرایم سازمان ملل می‌تواند واحدهای تخصصی برای بررسی جرایم زیست‌محیطی – دیجیتالی ایجاد کند. معاهدات کمک‌های حقوقی متقابل باید به‌روزرسانی شوند تا در مواردی که حملات بر اکوسیستم‌های فرامرزی تأثیر می‌گذارند، مانند زمانی که هکرها کنترل‌های سد را در یک کشور دستکاری می‌کنند تا به محیط زیست پایین‌دست در کشور دیگری آسیب برسانند، به اشتراک‌گذاری شواهد دیجیتال اولویت دهند (Shandler *et al*, 2022: 861).

جرم‌انگاری راهبردی همچنین باید به ساختارهای تأمین مالی که این حملات را ممکن می‌سازند، بپردازد. بسیاری از گروه‌های تروریستی دیجیتالی که در خرابکاری‌های زیست‌محیطی مشارکت دارند، از طریق معاملات ارزهای دیجیتال مرتبط با قاچاق غیرقانونی منابع تأمین مالی می‌شوند. گروه ویژه اقدام مالی می‌توانند ارائه‌دهندگان خدمات دارایی مجازی را ملزم به اجرای پروتکل‌های «انطباق سبز» کنند و تراکنش‌های مرتبط با جرایم مشکوک زیست‌محیطی – دیجیتالی را درست مانند آن‌چه برای تأمین مالی تروریسم انجام می‌دهند، مسدود کنند. شرکت‌های تجزیه و تحلیل بلاکچین که قبلاً برای ردیابی تجارت غیرقانونی حیات وحش استفاده می‌شدند، می‌توانند ابزارهای خود را برای نظارت بر تراکنش‌های مشکوک تأمین مالی حملات به زیرساخت‌های اقلیمی تطبیق دهند (Spadaro, 2020: 73).

۵-۲- اقلیم زنده و اقدامات حفاظتی

پیچیدگی روزافزون تروریسم دیجیتال، تهدیدی منحصر به فرد و فزاینده برای ثبات اقلیمی جهانی ایجاد می‌کند و مستلزم راهبردهای حفاظتی نوآورانه برای محافظت از سامانه‌های محیطی آسیب‌پذیر فعلی است. با افزایش تغییرات اقلیمی، بازیگران مخرب از آسیب‌پذیری‌های دیجیتال برای تشدید آسیب‌های زیست‌محیطی، مختل‌کردن تلاش‌های کاهش اثرات اقلیمی و تبدیل آن‌ها به سلاح بی‌ثباتی زیست‌محیطی سوءاستفاده می‌کنند. این شکل نوظهور از جنگ هیبریدی نیازمند یک راهبرد دفاعی جامع است که تاب‌آوری فناوری، اصلاح سیاست‌ها و همکاری بین‌المللی را برای محافظت از زیرساخت‌های حیاتی اقلیمی و سیستم‌های داده در برابر خرابکاری‌های دیجیتالی ترکیب کند.

تأثیر تروریسم دیجیتال بر سامانه‌های اقلیمی از طریق چندین بردار عمل می‌کند که هر کدام نیاز به اقدامات حفاظتی متناسب دارند. حملات به زیرساخت‌های انرژی، به‌ویژه شبکه‌های انرژی تجدیدپذیر، اتکای موقت به سامانه‌های پشتیبان کربن‌محور را ضروری می‌کند و در دوره‌های بحرانی، انتشار گازهای گلخانه‌ای را به‌طور مصنوعی افزایش می‌دهد. حمله دیجیتالی به خط لوله استعماری در سال ۲۰۲۱ نشان داد که چگونه، حتی اهداف غیر زیست‌محیطی می‌توانند از طریق اختلال در زنجیره‌های تأمین و سوزاندن سوخت اضطراری، آسیب‌های زیست‌محیطی آبشاری ایجاد کنند. راهبردهای حفاظتی باید ایمن‌سازی شبکه‌های هوشمند و سامانه‌های مدیریت انرژی تجدیدپذیر را با رمزگذاری مقاوم در قبال کوانتوم، تشخیص ناهنجاری در زمان واقعی و کنترل‌های پشتیبان‌گیری بدون وقفه که عملیات را در طول حوادث دیجیتالی حفظ می‌کنند، در اولویت قرار دهند. توسعه پروتکل‌های امنیت دیجیتالی «آگاه از آب و هوا» که حفاظت از سیستم‌ها را براساس تأثیر بالقوه کربن آن‌ها درصورت به خطرافتادن، اولویت‌بندی می‌کنند، می‌تواند به تخصیص مؤثرتر منابع کمک کند (Sydes *et al*, 2023: 55).

سیستم‌های نظارت و پیش‌بینی آب و هوا، خط مقدم آسیب‌پذیر دیگری هستند که نیاز به حفاظت بیشتر دارند. شبکه‌های ماهواره‌ای، شناورهای اقیانوسی و حسگرهای جوی که داده‌های حیاتی آب و هوا را جمع‌آوری می‌کنند، به‌طور فزاینده‌ای برای تحریف درک علمی یا غیرفعال‌کردن سامانه‌های هشدار اولیه برای رویدادهای شدید آب و هوایی هدف قرار می‌گیرند. نقض سازمان اروپایی بهره‌برداری از

ماهواره‌های هواشناسی طی سال ۲۰۲۰ نشان داد که چگونه داده‌های آب و هوایی به‌خطرافتاده می‌توانند تلاش‌های جهانی برای سازگاری را تضعیف کنند. محافظت از این سامانه‌ها نیازمند پروتکل‌های تأیید چند لایه، احراز هویت داده‌های مبتنی‌بر بلاکچین و راه‌حل‌های ذخیره‌سازی غیرمتمرکز است که حتی درصورت نقض سامانه‌های اولیه، یکپارچگی اطلاعات را حفظ می‌کنند. ایجاد استانداردهای بین‌المللی برای امنیت داده‌های آب و هوایی، شاید از طریق یک چهارچوب جدید تحت نظر سازمان جهانی هواشناسی، به همگام‌سازی اقدامات حفاظتی در سراسر مرزها کمک خواهد کرد (Asaka, 2021: 86).

زیرساخت‌های مالی که از اقدامات اقلیمی پشتیبانی می‌کنند، همچنین نیاز به محافظت در برابر تداخل دیجیتال دارند. بازارهای اعتبار کربن، سکوهای سرمایه‌گذاری سبز و سامانه‌های پرداخت صندوق آب و هوا، همگی دستکاری‌های مختلفی را از جبران خسارت‌های جعلی گرفته تا حملات باج‌گیری به پروژه‌های پایداری تجربه کرده‌اند. سوءاستفاده از پروتکل توکان در سال ۲۰۲۲ که ۳ میلیون دلار اعتبار کربن را به خطر انداخت، نشان داد که چگونه حملات مالی می‌توانند مستقیماً تلاش‌های کاهش انتشار گازهای گلخانه‌ای را با شکست مواجه کنند. پیاده‌سازی احراز هویت بیومتریک برای تراکنش‌های مالی اقلیمی، ایجاد ذخایر پشتیبان مجزا برای پروژه‌های مهم کاهش اثرات مخرب تغییرات اقلیمی و توسعه محصولات بیمه دیجیتالی به‌طور خاص برای طرح‌های زیست‌محیطی می‌تواند به محافظت از این سازوکارهای اقتصادی ضروری در برابر اختلال دیجیتال کمک کند (Henkin *et al*, 2022: 3).

حفاظت از اقلیم در برابر تروریسم دیجیتال مستلزم شناخت این است که سامانه‌های زیست‌محیطی به حوزه جدیدی از درگیری ترکیبی تبدیل شده‌اند. با افزایش مداوم سطح CO_2 اتمسفر، آسیب‌های احتمالی ناشی از حملات دیجیتال به‌موقع به همان سامانه‌هایی که سعی در معکوس‌کردن روند دارند نیز افزایش می‌یابد. این راهبردی باید پیشگیرانه باشد نه واکنشی، پیش‌بینی کند که چگونه آسیب‌پذیری‌های فناوری می‌توانند علیه ثبات اقلیمی به سلاح تبدیل شوند و بر این اساس، دفاع ایجاد کند (Asaka, 2021: 89). این امر مستلزم همکاری بی‌سابقه‌ای بین اقلیم‌شناسان، متخصصان امنیت دیجیتالی، سیاست‌گذاران و متخصصان امنیتی است – همگرایی رشته‌هایی به همان اندازه سامانه‌هایی که به‌دنبال محافظت از آن‌ها هستند، به هم پیوسته. در عصری که بیت‌ها و بایت‌ها می‌توانند بر سرنوشت یخچال‌های طبیعی و جریان‌های جوی تأثیر بگذارند، حفاظت از ابعاد دیجیتال آب و هوای ما ممکن است به اندازه کاهش انتشار گازهای گلخانه‌ای حیاتی باشد. با این وصف تسهیل اجرای سیاست‌های اقلیمی و نقشه راه را می توان در پرتو ارائه الگوی مقابله با تروریسم دیجیتالی برای مهار پایداری تغییرات اقلیمی و تحقق عدالت توصیف نمود.

جدول ۵: الگوی راهبردی (پژوهشگرمحور)

یکم: نقشه راه برای مقابله با تغییراقلیم
خلاقیت در ایجاد راهکارهای بهسازی محیط زیست؛ تعالی پیروی از قوانین در سطح ملی و معاهداتی در سطح بین‌المللی؛ حرکت سریع به‌سمت جایگزینی انرژی‌های تجدیدپذیر؛ الزام به تأمین و تسهیل مالی و اقدام برای پیشگیری سریع؛ تقلای سریع به سوی تنظیم اقلیم و تجدید اقلیم.
دوم: نقشه راه برای تحقق کاربست سیاستی

تلقی محیط زیست به‌عنوان یک نگرانی مهم از منظر سیاست عمومی؛ آزمایشگاه دموکراسی و فعال‌نمودن جامعه مدنی؛ حفاظت از محیط زیست به روش علمی؛ دیپلماسی عمومی و دیپلماسی زیست‌محیطی؛ توسعه پایدار سیاسی و توسعه پایدار محیط زیست؛ آموزش و آگاهی‌رسانی؛
سوم: نقشه راه برای تروریسم‌زدایی اقلیمی
کاربردپذیری مقررات در سطح ملی و بین‌المللی؛ ساختار مسؤولیت در قبال ورود خسارت و الزام به جبران؛ شفافیت در اجرای حقوق کیفری بین‌المللی؛ جرم‌انگاری باتوجه به وضعیت روز و موقعیت مقتضی؛ تعقیب جدی اکوسیستم کشی.
چهارم: نقشه راه برای مقابله با تروریسم دیجیتالی
تلاش‌های فردی و جمعی زیر چتر امنیت دیجیتالی؛ نامشروع‌تلقی‌نمودن تروریسم دولتی و حمایت‌های نافرجام؛ زیرساخت‌های متحد تحت تأثیر معاهده؛ حفاظت از شبکه‌ها و ایجاد کدهای رمزی برای پیشگیری و بهره‌برداری نامشروع؛ ایجاد و مطالعه مدل‌های تجربی برای بهره‌برداری کشورها؛
پنجم: نقشه راه برای مقابله با اثرگذاری سکوهای دیجیتال بر تغییر اقلیم
کنترل منطقی کاربران از طریق موبایل، کامپیوتر، لپتاب، سایر دستگاه‌های ارتباطی دیجیتالی؛ تقویت دیتاسنترها و وجود مقررات فوق سری برای پیشگیری از سوءاستفاده‌های احتمالی؛ حفاظت از شبکه‌ها و داده‌ها برای پیشگیری از داده‌های جعلی و غیر متقن؛ حفاظت از محیط زیست در مقابل زباله‌های الکترونیکی؛ طراحی انرژی‌های سبز مصرفی ابزارهای دیجیتال.

این ساختار نشان می‌دهد که عدالت کیفری برای تحقق در سطح ملی نیازمند کاربست سیاستی و در سطح بین‌المللی نیازمند نقشه راه است که با تلاش‌های معاهداتی درجهت مقابله با اکوتروریسم دیجیتالی – اقلیمی تحقق خواهد یافت.

نتیجه‌گیری

تغییرات اقلیمی به‌عنوان عاملی اساسی در تشدید خشونت‌ها و ناپایداری‌های اجتماعی مطرح بوده و افزایش دما می‌تواند شدت پیامدهای آن را تشدید کند. کاهش دسترسی به منابع حیاتی مانند آب، گسترش بیابان‌زایی در مناطق کشاورزی و افزایش دمای عمومی، ثبات سیاسی را تضعیف کرده و شکنندگی ساختارهای دولتی را افزایش می‌دهد. فشارهای محیطی می‌توانند به ابزاری برای جذب نیرو و کنترل جوامع تبدیل شوند و بازیگران دولتی و غیردولتی ممکن است از آن بهره‌برداری کنند؛ گاهی این بهره‌برداری با تخریب محیط زیست از طریق اقدامات خشونت‌آمیز یا تروریستی صورت می‌گیرد، پدیده‌ای که تحت عنوان «تروریسم زیست‌محیطی» شناخته می‌شود. این نوع تروریسم که پیش‌تر عمدتاً محدود به فعالیت‌های مدنی و فشار بر سیاست‌های زیست‌محیطی بود، اکنون با حضور در فضای دیجیتال و افزایش سرعت انتشار اطلاعات، پیچیدگی و دامنه وسیع‌تری یافته است. نمونه‌هایی از این روند شامل فعالان محیط زیستی تحت فشار است که جذب گروه‌هایی با رویکردهای مخرب می‌شوند، حتی در مناطقی با منابع کافی، محدودیت‌های حقوقی می‌توانند شرایط ظهور گونه‌های نوین تروریسم زیست‌محیطی را فراهم آورند.

تغییرات اقلیمی علاوه‌بر ایجاد بستر رشد تروریسم زیست‌محیطی، زمینه‌ساز شکل‌گیری ایدئولوژی‌های افراطی ضدپیشرفت نیز هستند، ازجمله «اکوفاشیسم» که توسط گروه‌های راست‌گرای افراطی شکل می‌گیرد. شواهد نشان می‌دهد تروریسم در مسیر مدرن‌سازی قرار داشته و حوزه‌های محیط زیست، تغییرات اقلیمی و فناوری‌های دیجیتال را تحت تأثیر قرار می‌دهد. ابزارهای دیجیتال علاوه‌بر تسهیل فعالیت‌های تروریستی، می‌توانند به‌طور غیرمستقیم بر تغییرات اقلیمی اثرگذار باشند و تهدیدات نوینی ایجاد کنند. در این زمینه، نظام عدالت کیفری می‌تواند نقش اساسی در تضمین پاسخ‌گذاری و مسؤولیت‌پذیری جهانی ایفا کند. جرم‌انگاری اقدامات تروریستی مرتبط با تغییرات اقلیمی و فناوری‌های دیجیتال، با استناد به اسناد بین‌المللی و منابع معاهداتی، امکان پیگیری قانونی و جلوگیری از فرار از مسؤولیت را فراهم می‌آورد. مقابله با تروریسم دیجیتال – اقلیمی می‌تواند از سه محور اصلی دنبال شود: ۱- بهره‌گیری از معاهدات و همکاری‌های بین‌المللی؛ ۲- اعمال ابزار جرم‌انگاری در برابر تهدیدات دیجیتال – اقلیمی؛ ۳- تقویت صلاحیت‌های جهانی شامل بازنگری در فهرست جرایم علیه بشریت و ارتقای عملکرد دیوان بین‌المللی کیفری.

پیشنهادات عملی برای تقویت این مقابله شامل تدوین معاهده بین‌المللی ویژه تروریسم دیجیتال و تغییرات اقلیمی، بومی‌سازی آن در سطح ملی با هدف ارتقای نقش دولت‌ها و طراحی چشم‌انداز امنیت دیجیتالی همراه با ایجاد کمیته تخصصی مقابله با تروریسم دیجیتال – اقلیمی برای شفاف‌سازی مسؤولیت نهادها و تقویت پدافند غیرعامل است. اجرای این اقدامات می‌تواند به کاهش آسیب‌پذیری جهانی و مدیریت تهدیدات پیچیده و نوظهور کمک کند.

ملاحظات اخلاقی: در این پژوهش کلیه ملاحظات اخلاقی رعایت گردیده است.

تعارض منافع: نگارندگان ابراز می‌دارند که در ارتباط با اجرای این پژوهش، نگارش نتایج آن و انتشار این متن، هیچ‌گونه تعارض منافعی اعم از مالی، سازمانی، شخصی یا حرفه‌ای، وجود ندارد. به‌علاوه، هیچ نهادی، به‌جز طرح پژوهشی پسادکتری شماره ۱۴۰۳/د/۳۱۹۶۲، در طراحی، تحلیل، نتیجه‌گیری یا گزارش این پژوهش نقشی نداشته است.

سهم نویسندگان: سبحان طیبی به‌عنوان پژوهشگر پسادکتری، مسئولیت اصلیِ طراحی پژوهش، گردآوری داده‌ها، تحلیل مطالب، نگارش پیش‌نویس اولیه و بازنگری محتوایی متن را بر عهده داشته است. در عین حال، پیمان نمامیان به‌عنوان استاد راهنما (پیشنهاد دهنده)، راهنمایی علمی، نظارت بر مراحل اجرای پژوهش، بررسی و اصلاح نسخه‌های مختلف

پژوهش و تأیید نهایی چارچوب علمی آن را به‌عهده داشته است.

تشکر و قدردانی: «این پژوهش حاصل همکاری و پشتیبانی های علمی ارزشمند گروه حقوق دانشکده علوم اداری و اقتصاد و معاونت پژوهش و فناوری دانشگاه اراک است. نگارندگان بدین‌وسیله سپاس خود را از همراهی‌ها، راهنمایی‌ها و حمایت‌های همکارانی که در مراحل مختلف طراحی، تدوین و تکمیل این پژوهش نقش‌آفرین بوده‌اند، ابراز می‌دارند.

تأمین اعتبار پژوهش: این پژوهش مستخرج از طرح پژوهشی به‌شماره ۳۱۹۶۲/د/۱۴۰۳ دوره پسادکتری با عنوان «واکاوی ابعاد عدالت کیفری در مواجهه با جرایم تروریستی از طریق سکوهای دیجیتالی در جهت مهار اثرگذاری آن بر تغییرات اقلیمی» بوده که در گروه حقوق دانشکده علوم اداری و اقتصاد دانشگاه اراک اجرا شده است.

منابع و مآخذ

الف. منابع فارسی

– بهادری، علی؛ فراهانی، محمدصادق؛ جعفریان، محمدمهدی و قاسمی‌پور، رضا (۱۴۰۳). «رویه‌های نوین ضدرقابتی در سکوهای فضای مجازی». *فصلنامه مطالعات حقوق عمومی دانشگاه تهران*، ۱–۳۱.

– پورهاشمی، سیدعباس؛ نامیان، پیمان و طیبی، سبحان (۱۳۹۴). «جرم‌انگاری تروریسم زیست‌محیطی؛ چالش‌ها، هنجارها و راهبردها». *فصلنامه علوم و تکنولوژی محیط زیست*، ۱(۱۷): ۱۶۷–۱۸۲.

– میرمحمدصادقی، حسین و قدیری بهرام‌آبادی، رشید (۱۳۹۴). «نقش و جایگاه سیاست در عدالت کیفری حاکم بر جرایم تروریستی». *فصلنامه پژوهش حقوق کیفری*، ۴(۱۳): ۹–۴۱.

– نامیان، پیمان (۱۴۰۳). «مقاله و پیشگیری از اتکاب جرایم تروریستی در شبکه‌های اجتماعی مجازی». *مجله حقوق فناوری‌های نوین*، ۵(۱۰): ۲۱۵–۲۳۳.

– نامیان، پیمان و شهبازی، مهدی (۱۴۰۳). «محافظت از امنیت سکوهای دیجیتالی در قبال جرایم تروریستی؛ راهبردی در ارتقای امنیت دیجیتالی دولت‌ها». *فصلنامه مطالعات و پژوهش‌های امنیت داخلی*، ۲(۱): ۷۳–۹۱.

ب. منابع انگلیسی

- Asaka, JO (2021). “Climate Change - Terrorism Nexus? A Preliminary Review/Analysis of the Literature”. *Perspectives on Terrorism*, 15(1): 81-92.

- Baldassarre, S (2023). “Cyberterrorism and Religious Fundamentalism: New Challenges for Europe in the Age of Universal Internet Access”. *Religions*, 14(4): 451-467.

- Bastug, MF & Onat, I (2024). *Cyberterrorism*. Oxford: Oxford University Press.

- Berk, R; Heidari, H; Jabbari, S; Kearns, M & Roth, A (2018). “Fairness in Criminal Justice Risk Assessments: The State of the Art”. *Sociological Methods & Research*, 50(1): 3-44.

- Christensen, CB (2024). “Ecofascism and Green Nazis in Denmark 1920-2020”. *Scandinavian Journal of History*, 50(2): 174-196.

- Corliss, C (2023). “Digital Terror Crimes”. *Columbia Journal of Transnational Law*, 58(1): 58-112.

- Darwish, M (2024). “Fascism, Nature and Communication: A Discursive-Affective Analysis of Cuteness in Ecofascist Propaganda”. *Feminist Media Studies*, 25(2): 443-463.

- Fakhoury, A (2024). “The Role of Digital Technology in Countering Terrorism”. *Pakistan Journal of Criminology*, 16(3): 609-618.

- Farber, SH (2025). “The Evolving Nexus of Cybercrime and Terrorism: A Systematic Review of Convergence and Policy Implications”. *Security Journal*, 38(J): 4-23.

- Fathi Al-Rai, A; Alomran, NM & Al-Ansari, MA (2024). “The Crime of Digital Promotion of Terrorism through Digital Platforms and New Media: A Comparative Study of Jordanian and Emirati Laws”. *International Journal of Electronic Governance*, 16(4): 453-467.

- Montasari, R (2024). *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses*. Cham: Springer.

- Olumoye, MY (2013). "Cyber Crime and Technology Misuse: Overview, Impacts and Preventive Measures". *European Journal of Computer Science and Information Technology*, 1(3): 10-20.

- Onat, I; Guler, A; Kula, S & Bastug, MF (2021). "Fear of Terrorism and Fear of Violent Crimes in the United States: A Comparative Analysis". *Crime & Delinquency*, 69(5): 891-914.

- Rawat, R (2023). "Logical Concept Mapping and Social Media Analytics Relating to Cyber-Criminal Activities for Ontology Creation". *International Journal of Information Technology*, 15(2): 893-903.

- Rose, G (2022). "Environmental Terrorism: Not Yet an International Crime". *Environmental Policy and Law*, 52(2): 161-170.

- Sarkar, G & Shukla, SK (2024). "Reconceptualizing Online Offenses: A Framework for Distinguishing Cybercrime, Cyberattacks and Cyberterrorism in the Indian Legal Context". *Journal of Economic Criminology*, 4(1): 1-17.

- Seth Harrison, ET (2018). "Evolving Tech, Evolving Terror". *Center for Strategic and International Studies*, 15: 28-33.

- Shackelford, SJ (2016). "On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems". *Vanderbilt Journal of Entertainment and Technology Law*, 18(4): 653-711.

- Shandler, R; Gross, ML; Backhaus, S & Canetti, D (2022). "Cyber Terrorism and Public Support for Retaliation - a Multi-Country Survey Experiment". *British Journal of Political Science*, 52(2): 850-868.

- Sieber, U (2006). "International Cooperation Against Terrorist Use of the Internet". *Revue Internationale de Droit Pénal*, 77(3): 395-449.

- Global Counterterrorism Forum (GCTF) (2025). *Understanding the Risks of Climate Change's Relationship with Violent Extremism Conducive to Terrorism and Building Solutions*.

- Henkin, S; Boyd, MA & Romm, M (2022). "A Climate of Terror? Part I: Approaches to the Study of Climate Change and Terrorism". *START*, 1-7.

- Iftikhar, S (2024). "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures". *Peer J Computer Science*, 10(e1): 772-793.

- Johnson, SHD (2024). "Identifying and Preventing Future forms of Crimes Using Situational Crime Prevention". *Security Journal*, 37(1): 515-534.

- Lee, H & Choi, KS (2022). *Interrelationship between Bitcoin, Ransomware and Terrorist Activities: Criminal Opportunity Assessment Via Cyber-Routine Activities Theoretical Framework*. In: The New Technology of Financial Crime. London: Routledge.

- Liu, J (2024). "The Relationism Theory of Criminal Justice: A Paradigm Shift". *Asian Journal Criminology*, 19(1): 1-25.

- Lu, Y (2024). "The Influence of Cognitive and Emotional Factors on Social Media Users' Information-Sharing Behaviours during Crises: The Moderating Role of the Construal Level and the Mediating Role of the Emotional Response". *Behavioral Sciences*, 14(6): 495-515.

- Lydon, D; Hallenberg, K & Kapageorgiadou, V (2024). "This is not a Drill': Police and Partnership Preparedness for Consequences of the Climate Crisis". *International Journal of Police Science & Management*, 27(1): 16-30.

- Macklin, G (2022). "The Extreme Right, Climate Change and Terrorism". *Terrorism and Political Violence*, 34(5): 979-996.

- Mavrakou, S; Chace-Donahue, E; Oluanaigh, R & Conroy, M (2022). "The Climate Change-Terrorism Nexus: A Critical Literature Review". *Terrorism and Political Violence Journal*, 34(5): 894-913.

- Silke, A & Morrison, J (2022). "Gathering Storm: An Introduction to the Special Issue on Climate Change and Terrorism". *Terrorism and Political Violence*, 34(5): 883-889.

- Spadaro, PA (2020). "Climate Change, Environmental Terrorism, Eco-Terrorism and Emerging Threats". *Journal of Strategic Security*, 13(4): 58-80.

- Sydes, M; Hine, L; Higginson, A; McEwan, J; Dugan, L & Mazerolle, L (2023). "Criminal justice Interventions for Preventing Radicalization, Violent Extremism and Terrorism: An Evidence and Gap Map". *Campbell Systematic Reviews*, 19(4): 43-69.

- Tayebi, S (2020). "Diplomacy and Environment; Conflict of Interest or Need for a Legal Regime?". *International Social Science Practice and Research*, 1(1): 17-31.

- Terzi, M (2019). "E-Government and Cyber Terrorism: Conceptual Framework, Theoretical Discussions and Possible Solutions". *TESAM Akademi Dergisi*, 6(1): 213-247.

- United Nation Development Programme Policy Brief (2020). *The Climate Security Nexus and the Prevention of Violent Extremism: Working at the Intersection of Major Development Challenges*.

- United Nation Security Council Counter-Terrorism Committee Executive Directorate (CTED) (2022). "The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspectives". *CTED Trends Report January, Germany*, 1-33.