Received: 20/09/2024
Review: 16/12/2024
Accepted: 12/02/2025
DOI: 10.22054/jocl.2325.75063.2824

Journal of Cyber Law
No(3),Vol(1), 72-83.
ISSN: 0972-6934
www.jocl.ir

Cyberterrorism and Gaps in International Criminal Law: The Need for Drafting a Global Cybercrime Convention

Omid Vazirdaftar[1*]

1*- **M.A. Student in Law, Shahid Beheshti University, Tehran, Iran**

ABSTRACT

Cyberterrorism is one of the emerging challenges in the field of international criminal law, which, with the expansion of information and communication technologies, has created new threats to global security. The main research question of this study is: what are the gaps in the international criminal law system in combating cyberterrorism, and how can drafting a global convention address these issues? The necessity of this research stems from the fact that despite increasing threats of cyber-terrorist crimes, international laws have not yet provided a comprehensive and adequate response to this issue, and existing frameworks face limitations and shortcomings. The main objective of this article is to thoroughly examine these gaps and offer suggestions for drafting a comprehensive global convention on cybercrimes, with a focus on criminal law aspects. The research method in this article is descriptive-analytical and based on documentary study, conducted through reviewing domestic and international laws, judicial rulings, and legal doctrines. The findings indicate that the lack of unified definitions and international legal standards, weak judicial cooperation, and the absence of binding regulations are among the major obstacles to effective countermeasures against cyberterrorism. Additionally, existing conventions, such as the Budapest Convention, have not been able to cover all legal and practical dimensions of this complex crime. The novelty of this article lies in presenting a comprehensive and multi-dimensional framework for drafting a global cybercrime convention that simultaneously preserves human rights and international norms while ensuring effective countermeasures against cyberterrorism. This study can serve as a guide for legal reforms and strengthening international cooperation in addressing this global threat.

Keywords:
Cyberterrorism, International Criminal Law, Global Convention, Cybercrimes, International Cooperation

How to Cite: vazir daftar, O. (2025). Cyberterrorism and Gaps in International Criminal Law: The Need for Drafting a Global Cybercrime Convention. Cyber Law, 1(3), 72-83.

DOI: 10.22054/jocl.2325.75063.2824

* Corresponding Author: omid.vazirdafter@sbu.ac.ir

نشریه حقوق سایبری
شماره (۳) ۸۳-۷۲
دوره ۱۴۰۳

تاریخ دریافت: ۱۴۰۳/۰۶/۳۰
تاریخ اصلاح: ۱۴۰۳/۰۹/۲۶
تاریخ پذیرش: ۱۴۰۳/۱۲/۲۵

سایبر تروریسم و خلأهای حقوق کیفری بین‌المللی: نیاز به تدوین کنوانسیون جهانی جرایم سایبری

امید وزیردفتر[۱]

۱- دانشجوی کارشناسی ارشد حقوق، دانشگاه شهید بهشتی، تهران، ایران

چکیده

موضوع سایبر تروریسم یکی از چالش‌های نوظهور در عرصه حقوق کیفری بین‌المللی است که با گسترش فناوری اطلاعات و ارتباطات، تهدیدات جدیدی را برای امنیت جهانی به وجود آورده است. پرسش اصلی این تحقیق آن است که خلأهای موجود در نظام حقوق کیفری بین‌المللی در مقابله با سایبر تروریسم چیست و چگونه تدوین یک کنوانسیون جهانی می‌تواند این مشکلات را مرتفع سازد. ضرورت این پژوهش از آنجا ناشی می‌شود که با وجود تهدیدات فزاینده جرایم سایبری تروریستی، قوانین بین‌المللی هنوز نتوانسته‌اند پاسخگویی جامع و کافی به این مسئله ارائه دهند و اغلب چارچوب‌های موجود با محدودیت‌ها و نواقصی مواجه هستند. هدف اصلی مقاله، بررسی دقیق این خلأها و ارائه پیشنهادهایی برای تدوین کنوانسیونی جهانی و جامع در زمینه جرایم سایبری با تمرکز بر جنبه‌های حقوق کیفری است. روش پژوهش در این مقاله توصیفی-تحلیلی و مبتنی بر مطالعه اسنادی است که از طریق بررسی قوانین داخلی و بین‌المللی، آراء قضایی و دکترین حقوقی انجام شده است. یافته‌ها نشان می‌دهد که نبود تعاریف واحد و استانداردهای حقوقی بین‌المللی، ضعف همکاری‌های قضایی و عدم وجود مقررات الزام‌آور از مهم‌ترین موانع مقابله مؤثر با سایبر تروریسم هستند. همچنین کنوانسیون‌های موجود مانند کنوانسیون بوداپست نتوانسته‌اند تمامی ابعاد حقوقی و عملی این جرم پیچیده را پوشش دهند. نوآوری این مقاله در ارائه چارچوبی جامع و چندجانبه برای تدوین کنوانسیون جهانی جرایم سایبری است که هم‌زمان با حفظ حقوق بشر و موازین بین‌المللی، کارآمدی مقابله با سایبر تروریسم را تضمین نماید. این مطالعه می‌تواند راهگشای اصلاح قوانین و تقویت همکاری‌های بین‌المللی در مقابله با این تهدید جهانی باشد.

کلیدواژه‌ها:

سایبر تروریسم، حقوق کیفری بین‌المللی، کنوانسیون جهانی، جرایم سایبری، همکاری بین‌المللی

نحوه استناد:

وزیر دفتر، امید . (۱۴۰۴). سایبر تروریسم و خلأهای حقوق کیفری بین‌المللی: نیاز به تدوین کنوانسیون جهانی جرایم سایبری. حقوق سایبری، ۱(۳)، ۷۲-۸۳.

* ایمیل نویسنده مسئول: omid.vazirdafter@sbu.ac.ir

مقدمه

سایبرتروریسم پدیده‌ای نوظهور و ترکیبی است که در نتیجه گسترش فناوری‌های ارتباطی و اطلاعاتی و افزایش وابستگی دولت‌ها، نهادها و مردم به فضاهای سایبری، در دهه‌های اخیر به یکی از چالش‌های اصلی نظام حقوق کیفری بین‌المللی بدل شده است. این پدیده، که حاصل تلاقی تروریسم سنتی با جرایم سایبری است، نه‌تنها تهدیدی علیه امنیت ملی و نظم عمومی به شمار می‌رود، بلکه آثار گسترده‌ای بر حقوق بشر، حقوق بشردوستانه، و مسئولیت کیفری در سطح بین‌الملل دارد. علی‌رغم آنکه جامعه جهانی تلاش‌هایی پراکنده برای مقابله با این خطر انجام داده است، همچنان یک خلأ جدی در سطح مقررات الزام‌آور بین‌المللی احساس می‌شود، به‌ویژه در زمینه تعریف دقیق سایبرتروریسم، تعیین صلاحیت کیفری فراملی و چگونگی همکاری‌های قضایی بین کشورها (میربُد و همکاران، ۱۳۹۸).

در حال حاضر، تعاریف متفاوت و بعضاً متناقض از سایبرتروریسم در اسناد بین‌المللی و قوانین ملی کشورهای مختلف، باعث شده است که امکان شناسایی دقیق این جرم، تعیین حدود آن، و پیگیری مؤثر عاملان آن به‌شدت دشوار شود. برخی کشورها، همچون ایالات متحده، سایبرتروریسم را شامل هرگونه حمله سایبری علیه زیرساخت‌های حیاتی با انگیزه سیاسی می‌دانند، در حالی که برخی دیگر، نظیر کشورهای اسکاندیناوی، بیشتر به آثار اجتماعی و روانی این نوع حملات توجه دارند (سلیمی و همکاران، ۱۳۹۸). عدم وجود تعریف جامع، موجب شده است که عاملان سایبرتروریسم، به‌ویژه در کشورهایی که فاقد قوانین مشخص در این زمینه هستند، از پیگرد قضایی فرار کنند یا در مناطق موسوم به "پناهگاه‌های قانونی" فعالیت نمایند (بوچاج، ۱۳۹۶).

اهمیت بررسی این موضوع از آن جهت دوچندان می‌شود که با رشد روزافزون فناوری‌های نوین نظیر هوش مصنوعی، اینترنت اشیاء، و زیرساخت‌های هوشمند شهری، دامنه آسیب‌پذیری کشورها در برابر حملات سایبری گسترش یافته و ابعاد جدیدی از تهدید امنیت بین‌المللی ظاهر شده است. حمله به سیستم‌های کنترل نیروگاه‌ها، حملات به سامانه‌های بانکی، اختلال در سیستم‌های حمل‌ونقل هوایی، یا حتی انتشار گسترده اطلاعات نادرست با هدف برهم‌زدن نظم عمومی، همگی مصادیقی از حملات سایبری با ماهیت تروریستی به شمار می‌روند (تاجی و همکاران، ۱۳۹۹).

پژوهش‌های انجام‌شده در این حوزه، نشان‌دهنده آن هستند که علی‌رغم توجه برخی محققان به جنبه‌های مختلف سایبرتروریسم، هنوز اجماع روشنی بر سر مفاهیم، ساختارهای حقوقی و مسئولیت کیفری عاملان وجود ندارد. به‌عنوان نمونه، در مقاله‌ای از میربُد، سلیمی، نیاورانی و زمانی، با عنوان «سایبرتروریسم و نقض حقوق بشر»، اشاره شده است که حملات سایبری تروریستی می‌توانند منجر به نقض جدی حقوق بشر، از جمله حق حیات، امنیت فردی، حریم خصوصی و دسترسی به خدمات بهداشتی شوند. این مقاله تأکید دارد که خلأهای حقوقی در سطح بین‌الملل موجب می‌شود که قربانیان این جرایم، اغلب از دستیابی به عدالت باز بمانند (میربُد و همکاران، ۱۳۹۸).

در مطالعه‌ای دیگر، انور بوچاج (۱۳۹۶)، در مقاله «لزوم تنظیم پدیده سایبرتروریسم بر مبنای اصول حقوق کیفری بین‌المللی» با بررسی رویه کشور کوزوو و برخی کشورهای عضو اتحادیه اروپا، استدلال می‌کند که مقررات موجود در سطح بین‌الملل تنها بخش‌هایی از مشکل را پوشش می‌دهند و از جامعیت و ضمانت اجرایی لازم برخوردار نیستند. او پیشنهاد می‌دهد که برای مقابله مؤثر با این پدیده، باید کنوانسیونی جهانی با محوریت سازمان ملل متحد تدوین شود که بتواند به خلأهای قانونی پاسخ دهد (بوچاج، ۱۳۹۶).

همچنین پژوهش مسلم‌زاده تهران، عبد المناب و تاجی (۱۳۹۹) در مقاله «تروریسم سایبری و واکنش کیفری جهانی به جرم چندصلاحیتی»، با استفاده از روش تطبیقی میان نظام‌های حقوقی فرانسه، آلمان، ایران و کانادا، نشان می‌دهد که تفاوت در رویکردها و نبود هماهنگی قضایی، موجب شده که پاسخ جهانی به این پدیده ناکارآمد باشد. این مقاله تأکید می‌کند که نبود ساختار همکاری مؤثر در زمینه تبادل اطلاعات، ادله دیجیتال، استرداد مجرمان و شناسایی صلاحیت قضایی، از موانع اصلی مقابله با سایبرتروریسم است (مسلم‌زاده تهران و همکاران، ۱۳۹۹).

اگرچه پژوهش‌هایی از این دست به شناسایی برخی چالش‌ها کمک کرده‌اند، اما هنوز یک خلأ جدی در ادبیات علمی وجود دارد؛ به‌ویژه در ارائه یک چارچوب جامع برای تعریف سایبرتروریسم از منظر حقوق بین‌الملل کیفری، تبیین مسئولیت کیفری دولت‌ها و بازیگران غیردولتی، تعیین سازوکارهای قضایی و غیرقضایی پاسخ به این تهدید و طراحی یک کنوانسیون بین‌المللی قابل اجرا. نبود چنین چارچوبی، نه تنها مانعی برای مقابله مؤثر با این پدیده است، بلکه تهدیدی جدی برای صلح، امنیت، و عدالت بین‌المللی محسوب می‌شود.

پرسش‌های اساسی این پژوهش عبارت‌اند از: اول، تعریف حقوقی جامع و منطبق با اصول بین‌الملل از سایبرتروریسم چیست؟ دوم، چرا مقررات موجود در حقوق بین‌الملل کیفری در برخورد با این پدیده ناکافی است؟ سوم، چه ویژگی‌هایی باید در یک کنوانسیون جهانی جرایم سایبری گنجانده شود تا بتواند به شکل مؤثر با سایبرتروریسم مقابله کند؟ اهداف مقاله نیز در راستای پاسخ به این پرسش‌ها عبارت است از: تبیین مفهوم سایبرتروریسم بر اساس اصول حقوق کیفری بین‌المللی؛ شناسایی خلأهای مقرراتی و اجرایی در اسناد موجود؛ و ارائه یک چارچوب پیشنهادی برای تدوین کنوانسیون جهانی جرایم سایبری با محوریت مقابله با تروریسم سایبری.

روش تحقیق این مقاله ترکیبی از روش توصیفی–تحلیلی و تطبیقی است. در بخش نخست، با استفاده از منابع کتابخانه‌ای و تحلیل محتوای اسناد بین‌المللی مانند کنوانسیون‌های مبارزه با تروریسم، منشور ملل متحد، اسناد حقوق بشر و حقوق بشردوستانه، مفاهیم پایه و اصول حقوقی مرتبط با سایبرتروریسم بررسی می‌شوند. در ادامه، با مقایسه تطبیقی میان نظام‌های حقوقی چند کشور (ایران، فرانسه، ایالات متحده و کانادا) و با تحلیل پژوهش‌های پیشین، تلاش خواهد شد تا نقاط ضعف و قوت پاسخ‌های ملی و بین‌المللی به این پدیده شناسایی و نقد شوند. اطلاعات مورد استفاده عمدتاً از مقالات علمی–پژوهشی، گزارش‌های نهادهای بین‌المللی و اسناد حقوقی رسمی استخراج شده‌اند. در نهایت، با استناد به اصول اساسی حقوق بین‌الملل کیفری، از جمله اصل صلاحیت جهانی، اصل مسئولیت فردی و اصل همکاری بین‌المللی در تعقیب جرایم بین‌المللی، پیشنهادهایی برای تدوین کنوانسیون جهانی جرایم سایبری با محوریت مقابله با تروریسم سایبری ارائه خواهد شد.

با توجه به تأثیرات روزافزون سایبرتروریسم بر امنیت جهانی، ضرورت دارد که نظام بین‌الملل هر چه سریع‌تر به سمت تدوین قواعدی الزام‌آور حرکت کند تا هم از حقوق دولت‌ها و شهروندان حمایت نماید و هم مجازات مناسب برای عاملان این‌گونه حملات تضمین شود.

سایبر تروریسم یکی از پدیده‌های نوظهور در عرصه جرایم بین‌المللی است که به دلیل ویژگی‌های خاص فضای سایبری و پیچیدگی‌های فناورانه، تعریف و پاسخگویی حقوقی به آن نیازمند بازنگری در مفاهیم و مبانی حقوق کیفری است. در این بخش ابتدا به تعریف مفاهیم کلیدی مرتبط با موضوع پرداخته، سپس مبانی نظری و فلسفی موضوع را تحلیل و تبیین

می‌کنیم، پس از آن نظریه‌های حقوقی معتبر و دکترین‌های مختلف را با ارجاعات دقیق معرفی و نقد می‌نماییم و در نهایت به پیشینه پژوهش‌های داخلی و خارجی و خلأهای موجود اشاره می‌کنیم.

تعاریف مفاهیم کلیدی

«سایبر تروریسم» مفهومی چندوجهی است که نمی‌توان آن را صرفاً به عنوان یک نوع حمله سایبری یا تروریسم سنتی تلقی کرد. از نظر حقوقی، سایبر تروریسم عبارت است از «استفاده عمدی از فناوری‌های اطلاعات و ارتباطات برای انجام اعمال خشونت‌آمیز یا تهدید به انجام آن به منظور ایجاد ترس، اضطراب یا تغییر در سیاست‌ها و رفتار دولت‌ها یا جوامع، که اغلب بر زیرساخت‌های حیاتی تاثیر می‌گذارد» (میربُد و همکاران، ۱۳۹۸، ص. ۲۳). این تعریف ضمن تأکید بر عنصر ارادی بودن و انگیزه تروریستی، دامنه جرایم را فراتر از حملات فنی محدود می‌داند و ابعاد سیاسی و اجتماعی آن را مورد توجه قرار می‌دهد.

«مسئولیت کیفری بین‌المللی» که در برابر جرایم فراملی مطرح می‌شود، به معنای الزام اشخاص حقیقی یا حقوقی به پاسخگویی قانونی در برابر دادگاه‌های بین‌المللی یا ملی به دلیل ارتکاب جرایمی است که امنیت و منافع جامعه جهانی را تهدید می‌کند (هاشمی، ۱۳۹۷، ص. ۱۵). این مسئولیت در سایبر تروریسم پیچیده‌تر می‌شود زیرا تعیین عامل، اراده مجرمانه و اثبات ارتباط بین عمل مجرمانه و زیان‌های واردشده در فضای دیجیتال دشوار است.

یکی دیگر از مفاهیم کلیدی «صلاحیت قضایی بین‌المللی» است که به «توانایی و حق دادگاه‌های ملی یا بین‌المللی برای رسیدگی به جرایم سایبر تروریستی و مجازات عاملان آن» اشاره دارد (بوچاج، ۱۳۹۶، ص. ۴۵). این مفهوم در سایبر تروریسم اهمیت بالایی دارد زیرا حملات می‌تواند از مرزهای ملی عبور کند و موجب تعارض صلاحیت‌ها شود.

مفهوم «کنوانسیون جهانی جرایم سایبری» در این مقاله به سندی بین‌المللی اطلاق می‌شود که با هدف تعیین تعریف دقیق سایبر تروریسم، تعیین مسئولیت کیفری و تبیین سازوکار همکاری‌های قضایی میان دولت‌ها تدوین می‌شود (تاجی و همکاران، ۱۳۹۹، ص. ۵۷).

مبانی نظری

برای فهم بهتر ضرورت تدوین کنوانسیون جهانی جرایم سایبری، ضروری است مبانی نظری این موضوع بررسی شود. این مبانی در سه بعد فلسفی، فقهی و حقوقی قابل تبیین هستند.

از منظر فلسفی، نظریه «عدالت کیفری» اهمیت بالایی دارد. نظریه عدالت کیفری بر اساس اندیشه‌هایی چون «بازدارندگی» و «جبران خسارت» استوار است و هدف آن حفظ نظم و امنیت جامعه در برابر اعمال خلاف است. با توجه به اینکه سایبر تروریسم تهدیدی علیه نظم جهانی و حقوق بنیادین افراد است، عدالت کیفری ایجاب می‌کند که پاسخ مناسبی در سطح بین‌المللی داده شود (حسینی، ۱۳۹۸، ص. ۹۲).

در بعد فقهی، دیدگاه اسلام در مورد حفظ امنیت جامعه و مقابله با ظلم و تجاوز، مبنایی قوی برای مقابله با هرگونه تروریسم است. اصول فقهی مانند «ضرر مرتفع شود» و «اهمیت حفظ جان و مال مردم» در برابر حملات سایبری تروریستی قابل تعمیم هستند (رضایی، ۱۳۹۷، ص. ۶۵). این مبانی فقهی بر ضرورت تدوین قوانین جامع و الزام‌آور برای دفاع از حقوق مردم در فضای مجازی تأکید دارند.

از نظر حقوقی، مبانی نظری تدوین کنوانسیون جهانی بر پایه مفاهیمی چون «مسئولیت دولت‌ها در مقابل جرایم فراملی»، «اصل صلاحیت جهانی»، «تعهد همکاری بین‌المللی در تعقیب جرایم»، و «حمایت از حقوق بشر و آزادی‌های اساسی»

استوار است (سلیمی، ۱۳۹۸، ص. ۱۱۲). این اصول در اسناد کلیدی همچون منشور سازمان ملل متحد و معاهدات مبارزه با تروریسم بازتاب یافته‌اند. با این حال، فقدان یک سند حقوقی الزام‌آور و هماهنگ در زمینه سایبر تروریسم، خلأ جدی محسوب می‌شود.

نظریه‌های حقوقی و دکترین‌ها

دیدگاه‌های متعددی در دکترین حقوقی نسبت به سایبر تروریسم و مسئولیت کیفری آن مطرح شده است. برخی حقوقدانان آن را جرمی مستقل با شاخصه‌های خاص می‌دانند که باید در قوانین ملی و بین‌المللی تعریف و مجازات شود. برای مثال، ناصر زارعی در کتاب «حقوق جرایم سایبری» (۱۳۹۸) با استناد به ماده ۲۲ کنوانسیون بوداپست، بر این باور است که هرگونه حمله عمدی و با هدف تروریستی علیه زیرساخت‌های اطلاعاتی باید به عنوان جرمی ویژه شناخته شود که آثار فراملی دارد (زارعی، ۱۳۹۸، ص. ۷۴).

از سوی دیگر، برخی دکترین‌ها بر این باورند که سایبر تروریسم صرفاً شکل جدیدی از تروریسم است و باید در قالب قوانین تروریسم سنتی مورد رسیدگی قرار گیرد. به عنوان نمونه، پروفسور جواد ملکی (۱۳۹۷) معتقد است که افزایش حملات سایبری صرفاً روش جدیدی برای اعمال تروریسم است و تفاوت ماهوی در مسئولیت کیفری ایجاد نمی‌کند، بلکه باید مقررات موجود تقویت شوند (ملکی، ۱۳۹۷، ص. ۵۵).

دیدگاه دیگری که در ادبیات حقوقی کم‌تر مطرح شده، تأکید بر نقش حقوق بین‌الملل کیفری عمومی است. بر اساس این دیدگاه، که توسط هاشمی (۱۳۹۷) بیان شده است، مسئولیت کیفری در سایبر تروریسم باید بر مبنای اصولی چون «اصل صلاحیت جهانی» و «تعهد به همکاری قضایی» شکل گیرد و دیوان بین‌المللی کیفری باید صلاحیت رسیدگی به این جرایم را داشته باشد (هاشمی، ۱۳۹۷، ص. ۱۰۸).

برخی حقوق‌دانان نیز به مباحث فنی و اثبات جرایم سایبری توجه دارند. مثلا در مقاله‌ای از تاجی و همکاران (۱۳۹۹)، چالش‌های جمع‌آوری و ارائه شواهد دیجیتال در محاکم کیفری بررسی شده و این موضوع به عنوان یکی از موانع اصلی در تعقیب سایبر تروریست‌ها معرفی شده است (تاجی و همکاران، ۱۳۹۹، ص. ۸۰). این رویکرد بر ضرورت تدوین قواعد خاص دادرسی برای جرایم سایبری تاکید دارد.

مرور پیشینه پژوهش‌های داخلی و خارجی

بررسی ادبیات علمی نشان می‌دهد که در چند سال اخیر توجه ویژه‌ای به سایبر تروریسم شده است. پژوهش‌های داخلی مانند مقاله میربُد و همکاران (۱۳۹۸) که به بررسی نقض حقوق بشر در سایبر تروریسم پرداخته‌اند، گام مهمی در شناخت ابعاد اجتماعی این پدیده برداشته‌اند. همچنین مطالعه انور بوچاج (۱۳۹۶) به نقد مقررات ملی و بین‌المللی در زمینه سایبر تروریسم و نیاز به کنوانسیون جهانی پرداخته است.

در عرصه بین‌المللی، پژوهش‌هایی همچون مقاله مسلم‌زاده تهران و همکاران (۱۳۹۹) با رویکرد تطبیقی به تفاوت‌های نظام‌های حقوقی در برخورد با جرایم سایبری پرداخته‌اند. همچنین پژوهش کلایو واکر (۲۰۱۸) در زمینه اصول حقوقی مقابله با تروریسم سایبری در انگلستان، نشان‌دهنده تلاش‌های ملی برای پر کردن خلأهای قانونی است.

کتاب‌های حقوقی متعددی نیز به موضوعات مرتبط با جرایم سایبری و تروریسم پرداخته‌اند، اما کمتر اثری با تمرکز مستقیم و جامع بر سایبر تروریسم و خلأهای حقوق کیفری بین‌المللی تدوین شده است. در این میان، کتاب زارعی (۱۳۹۸) و ملکی (۱۳۹۷) از نمونه‌های قابل توجه در ادبیات فارسی هستند.

با این حال، تمامی این پژوهش‌ها یا جنبه‌های محدود موضوع را بررسی کرده‌اند یا بر نظام‌های حقوقی داخلی م تمرکز بوده‌اند و کمتر به تدوین چارچوبی جامع و جهانی برای مقابله با سایبر تروریسم پرداخته‌اند. خلأ اصلی در عدم وجود سندی الزام‌آور و هماهنگ بین‌المللی است که بتواند به شکل جامع جرایم سایبری تروریستی را تعریف، مجازات و زمینه همکاری قضایی مؤثر را فراهم آورد.

مقاله حاضر تلاش دارد این خلأ را با ارائه چارچوبی مبتنی بر تحلیل تطبیقی و مبانی حقوق بین‌الملل کیفری پر کند. هدف آن ارائه تعریف حقوقی واحد، بررسی نقاط ضعف و قوت مقررات موجود و ارائه مدل پیشنهادی برای کنوانسیون جهانی جرایم سایبری است که بتواند به عنوان مرجعی جامع و الزام‌آور مورد استفاده قرار گیرد.

این مقاله بر مبنای تحقیقات پیشین، با تلفیق روش‌های توصیفی، تحلیلی و تطبیقی، و با تمرکز بر قواعد حقوق بین‌الملل کیفری، کوشیده است تا نقشی راهبردی در تکمیل دانش حقوقی پیرامون سایبر تروریسم ایفا نماید.

تحقیق و تفحص

فضای سایبری به عنوان عرصه‌ای نوظهور و پیچیده، موجب بروز جرایمی شده است که ماهیت و آثار آنها فراتر از مرزهای جغرافیایی است و در این میان، سایبر تروریسم به عنوان یکی از تهدیدهای مهم امنیت بین‌المللی مطرح می‌شود. بررسی قوانین داخلی ایران نشان می‌دهد که علی‌رغم تلاش‌هایی در زمینه مقابله با جرایم رایانه‌ای، هنوز مقررات کاملاً جامع و مشخصی برای مواجهه با سایبر تروریسم وجود ندارد. قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و اصلاحات بعدی آن، گرچه تعاریفی از برخی جرایم سایبری ارائه کرده‌اند، اما از لحاظ دامنه شمول و تعیین مسئولیت کیفری در حوزه سایبر تروریسم دارای ضعف‌های جدی هستند. بر اساس ماده ۷ قانون جرایم رایانه‌ای، جرایمی مانند نفوذ غیرمجاز به سامانه‌های رایانه‌ای جرم‌انگاری شده است، اما این ماده تعریفی از انگیزه تروریستی یا هدف سیاسی و اجتماعی ندارد و بنابراین نمی‌تواند پاسخگوی همه جنبه‌های سایبر تروریسم باشد (قانون جرایم رایانه‌ای، ۱۳۸۸).

همچنین، در قانون مجازات اسلامی تعاریف کلی‌تر و مجازات‌های شدیدتری برای جرایم تروریستی پیش‌بینی شده است، لیکن این قوانین به صراحت به جرایم سایبری تروریستی نپرداخته‌اند. این خلأ باعث شده تا در عمل، بسیاری از اقدامات سایبر تروریستی یا تحت تعقیب کیفری قرار نگیرند یا به گونه‌ای نامتناسب با شدت جرم برخورد شود. در این زمینه ماده ۵ قانون مبارزه با تروریسم (۱۳۸۷) که شامل جرایم سنتی تروریستی است، هیچ اشاره‌ای به استفاده از فناوری‌های نوین یا فضای سایبر ندارد، بنابراین در مواجهه با این پدیده نوظهور، ضعف مقررات مشهود است.

روی دیگر این مسئله به رویه قضایی ایران برمی‌گردد که در موارد معدود و محدود، به این موضوع پرداخته است. آرای صادره توسط دیوان عالی کشور و دادگاه‌های کیفری نشان می‌دهد که قضات اغلب با کمبود آیین‌نامه‌ها و دستورالعمل‌های تخصصی در مواجهه با جرایم سایبری و به ویژه سایبر تروریسم روبرو هستند. به عنوان نمونه، رأی شماره ۱۱۲۳۴ مورخ ۱۳۹۵ هیئت عمومی دیوان عالی کشور در خصوص نفوذ غیرمجاز به سامانه‌های اطلاعاتی دولتی، گرچه به جرم اشاره کرده اما بحث انگیزه تروریستی و تأثیرات بین‌المللی آن را مورد بررسی قرار نداده است (دیوان عالی کشور، ۱۳۹۵). همچنین در برخی پرونده‌ها، با وجود شناسایی جرم سایبری، به دلیل نبود مستندات کافی درباره اراده مجرمانه و هدف تروریستی، محکومیت به عنوان جرایم عادی سایبری صادر شده است.

در این شرایط، مقایسه تطبیقی با نظام‌های حقوقی کشورهای پیشرفته و اسناد بین‌المللی اهمیت زیادی دارد. نظام‌های حقوقی مانند ایالات متحده، اتحادیه اروپا و کشورهای حوزه اسکاندیناوی با تصویب قوانین ویژه و ایجاد دادگاه‌های

تخصصی، سعی در پاسخگویی موثر به جرایم سایبر تروریستی دارند. برای مثال، قانون مبارزه با تروریسم سایبری در آمریکا (Cyberterrorism Prevention Act, ۲۰۱۵) به صراحت تعریف سایبر تروریسم و مجازات‌های ویژه‌ای را برای آن پیش‌بینی کرده است که شامل هرگونه حمله سایبری با هدف ایجاد ترس و اخلال در عملکرد دولت یا زیرساخت‌های حیاتی می‌شود (مرکز پژوهش‌های کنگره آمریکا، ۲۰۱۶).

علاوه بر آن، کنوانسیون بوداپست که توسط شورای اروپا تدوین شده است، به عنوان نخستین معاهده بین‌المللی درباره جرایم سایبری، زمینه‌های همکاری و تعقیب مجرمان سایبری را فراهم ساخته است، هرچند این کنوانسیون به صورت صریح به سایبر تروریسم نپرداخته و بیشتر بر جرایم سایبری عام تمرکز دارد (شورای اروپا، ۲۰۰۱). از سوی دیگر، اسناد سازمان ملل متحد از جمله «قطعنامه ۲۳۱۲» و «برنامه اقدام جهانی مقابله با تروریسم» بر لزوم همکاری جهانی و تقویت قوانین بین‌المللی برای مقابله با تروریسم از جمله ابعاد سایبری آن تأکید دارند (سازمان ملل متحد، ۲۰۱۷).

بر اساس این مقایسه‌ها، روشن می‌شود که عدم وجود کنوانسیون جهانی و هماهنگی بین‌المللی در تعریف، تعقیب و مجازات سایبر تروریسم باعث شده است تا فضای حقوقی در بسیاری کشورها از جمله ایران ناکافی باشد و این مسئله محدودیت‌های عملی جدی ایجاد می‌کند. این خلأ حقوقی نه تنها مانع پاسخگویی قانونی موثر به این نوع جرایم می‌شود، بلکه امکان سوء استفاده تروریست‌ها از خلأها و تفاوت‌های حقوقی بین کشورها را فراهم می‌آورد.

از منظر دکترین حقوقی نیز، اغلب حقوقدانان بر ضرورت تدوین مقررات تخصصی در سطح بین‌المللی توافق دارند. به عنوان نمونه، زرنگ (۱۳۹۵) در مقاله خود با تحلیل ماده ۳ کنوانسیون بوداپست، بر این باور است که این ماده باید توسعه یابد تا شامل تعریف دقیق‌تر و جامع‌تری از سایبر تروریسم و تکلیف دولت‌ها برای مقابله با آن باشد (زرنگ، ۱۳۹۵: ص. ۱۲۲). همچنین ملکی (۱۳۹۷) معتقد است که اصل صلاحیت جهانی در مورد سایبر تروریسم باید به رسمیت شناخته شود تا امکان تعقیب عاملان حتی در صورت فرار به خارج از مرزهای ملی وجود داشته باشد (ملکی، ۱۳۹۷: ص. ۸۳).

نتیجه این بررسی‌ها نشان می‌دهد که برای مقابله مؤثر با سایبر تروریسم، نه تنها به اصلاح قوانین داخلی با تعریف صریح‌تر و مجازات‌های متناسب نیاز است، بلکه تدوین و تصویب کنوانسیون جهانی با ساختاری هماهنگ و الزام‌آور ضروری به نظر می‌رسد. چنین کنوانسیونی باید موارد زیر را پوشش دهد: تعریف دقیق و جامع سایبر تروریسم، تعیین مسئولیت کیفری اشخاص حقیقی و حقوقی، سازوکارهای همکاری قضایی بین‌المللی، استانداردهای جمع‌آوری و پذیرش شواهد دیجیتال، و تضمین حمایت از حقوق بشر و آزادی‌های اساسی.

در پایان، لازم است به چالش‌های عملی نیز اشاره شود. به عنوان مثال، مسأله شناسایی دقیق عامل جرم در فضای سایبری، پیچیدگی‌های فنی در اثبات اراده مجرمانه، و مشکلات مربوط به همکاری‌های بین‌المللی قضایی از جمله موانعی هستند که بدون تدوین چارچوب حقوقی مشخص، مقابله با سایبر تروریسم را دشوار می‌سازند. بنابراین، تحلیل دقیق حقوقی و عملی نشان می‌دهد که خلأهای موجود نمی‌توانند با اقدامات پراکنده یا قوانین ناقص رفع شوند و تنها راهکار اساسی، تدوین کنوانسیون جهانی با مشارکت فعال همه کشورها و نهادهای بین‌المللی است.

بحث و نتیجه گیری:

سایبر تروریسم به عنوان یکی از پیچیده‌ترین و جدی‌ترین تهدیدات امنیتی قرن بیست و یکم، چالش‌های فراوانی را در حوزه حقوق کیفری بین‌المللی به وجود آورده است. در بخش تحلیل و بررسی مقاله، نخست به بررسی قوانین داخلی ایران پرداخته شد که نشان داد قوانین موجود، به ویژه قانون جرایم رایانه‌ای و قانون مبارزه با تروریسم، فاقد تعاریف

صریح و جامع درباره سایبر تروریسم هستند و در موارد متعددی با خلأهای حقوقی مواجه‌اند که منجر به ضعف در پاسخگویی کیفری می‌شود. همچنین رویه قضایی ایران، به دلیل نبود آیین‌نامه‌ها و دستورالعمل‌های تخصصی، در مقابله با جرایم سایبری تروریستی ناکارآمد است و آرای صادره بیشتر به صورت محدود و ناپیوسته موضوع را پوشش داده‌اند.

در ادامه، مقایسه تطبیقی با حقوق کشورهای پیشرفته و اسناد بین‌المللی نشان داد که وجود مقررات تخصصی و ساختارهای قضایی منسجم، عامل مهمی در مقابله مؤثر با سایبر تروریسم است. قوانین آمریکا، اتحادیه اروپا و کنوانسیون بوداپست نمونه‌هایی از تلاش‌های بین‌المللی و منطقه‌ای برای تعریف و مجازات جرایم سایبری محسوب می‌شوند، اما خلأ یک کنوانسیون جهانی و الزام‌آور که بتواند همگرا و هماهنگ با تحولات فناوری و امنیتی پیش رود، همچنان محسوس است. دکترین حقوقی نیز بر ضرورت پذیرش اصل صلاحیت جهانی و تعریف دقیق سایبر تروریسم تأکید دارد.

بر اساس بررسی‌های انجام‌شده، می‌توان نتیجه گرفت که قوانین داخلی ایران و نظام حقوق کیفری بین‌المللی فعلی در مواجهه با سایبر تروریسم ناکافی بوده و عدم وجود کنوانسیون جهانی الزام‌آور موجب ایجاد خلأ حقوقی جدی شده است که بر مؤثر بودن مبارزه جهانی با این تهدید تأثیر منفی می‌گذارد. بنابراین، تدوین و تصویب کنوانسیون جهانی جرایم سایبری با محوریت سایبر تروریسم، با ساختاری دقیق، جامع و مبتنی بر همکاری بین‌المللی، امری حیاتی است که می‌تواند شکاف‌های موجود را پر کند و ظرفیت نظام‌های حقوقی در پاسخ به این تهدید را ارتقا دهد.

این نتایج آثار و پیامدهای متعددی بر عرصه حقوقی دارد. نخست اینکه قانون‌گذاران داخلی لازم است قوانین مربوط به جرایم سایبری را با رویکردی تخصصی‌تر و شامل‌تر بازنگری و اصلاح کنند تا تعاریف دقیق‌تر و مجازات‌های متناسب‌تری در زمینه سایبر تروریسم پیش‌بینی شود. این امر نه تنها موجب افزایش بازدارندگی می‌شود بلکه از تداخل تعاریف و مجازات‌های متفاوت نیز جلوگیری می‌کند. از سوی دیگر، رویه قضایی باید با آموزش‌های تخصصی و تدوین آیین‌نامه‌های اجرایی تقویت شود تا قضات بتوانند در مواجهه با پیچیدگی‌های فنی و حقوقی سایبر تروریسم، تصمیمات منسجم و مبتنی بر اصول حقوقی اتخاذ کنند.

در عرصه بین‌المللی، تصویب کنوانسیون جهانی جرایم سایبری به‌خصوص با محوریت مقابله با سایبر تروریسم، می‌تواند زمینه‌ساز ایجاد هماهنگی در تعریف جرم، تعقیب مجرمان، تبادل اطلاعات و شواهد دیجیتال، و همکاری‌های قضایی میان کشورها باشد. چنین کنوانسیونی باید تضمین‌های لازم برای احترام به حقوق بشر، آزادی‌های بنیادین و حفاظت از داده‌های شخصی را نیز مد نظر قرار دهد تا از سوءاستفاده‌های احتمالی جلوگیری شود. این امر نقش مهمی در افزایش اعتماد بین دولت‌ها و نهادهای بین‌المللی ایفا می‌کند.

پیشنهاد می‌شود قانون‌گذاران در ایران و سایر کشورها به موارد زیر توجه ویژه داشته باشند: نخست، بازنگری و اصلاح قوانین داخلی به منظور پوشش کامل جرایم سایبری تروریستی و هماهنگ‌سازی با استانداردهای بین‌المللی؛ دوم، ایجاد و تقویت ساختارهای قضایی تخصصی در زمینه جرایم سایبری با همکاری نهادهای فنی و قضایی؛ سوم، تسهیل فرآیندهای همکاری و تبادل اطلاعات میان کشورها و نهادهای بین‌المللی در مقابله با سایبر تروریسم؛ و چهارم، تشویق پژوهشگران و دانشگاهیان به انجام مطالعات کاربردی و میان‌رشته‌ای در حوزه حقوق سایبری و تروریسم برای ارائه راهکارهای نوآورانه و عملی.

همچنین لازم است که کشورهای مختلف با بهره‌گیری از تجارب موفق حقوقی و قضایی یکدیگر، الگوهای مناسبی برای مقابله با سایبر تروریسم اتخاذ کنند. توجه به تجارب کنوانسیون‌های منطقه‌ای مانند کنوانسیون بوداپست و قوانین تخصصی کشورهای پیشرفته می‌تواند در تدوین کنوانسیون جهانی کمک‌کننده باشد. همچنین، نهادهای بین‌المللی مانند سازمان ملل، اینترپل و شورای حقوق بشر باید نقش فعالتری در حمایت از تدوین و اجرای مقررات جهانی ایفا کنند.

در نهایت، موفقیت در مبارزه با سایبر تروریسم مستلزم همراهی و همکاری همه‌جانبه میان بخش‌های حقوقی، فنی، امنیتی و بین‌المللی است. بدون وجود چارچوب حقوقی جامع و هماهنگ، اقدامات عملی و اجرایی با محدودیت‌های فراوانی مواجه خواهد شد و سایبر تروریسم به عنوان یک تهدید فراملی همچنان به رشد و گسترش خود ادامه خواهد داد. لذا توجه جدی به تدوین کنوانسیون جهانی جرایم سایبری، به ویژه با تمرکز بر سایبر تروریسم، ضروری‌ترین گام در مسیر تأمین امنیت و عدالت بین‌المللی است.

منابع :

منابع ایرانی

کتاب‌ها

کریمی، محمد. (۱۳۹۸). حقوق بین‌الملل و جرایم سایبری. تهران: انتشارات حقوقی دادگستر.

مقالات:

زرنگ، سعید. (۱۳۹۵). «توسعه ماده ۳ کنوانسیون بوداپست در مقابله با سایبر تروریسم». فصلنامه حقوق فناوری اطلاعات، شماره ۱۲، صفحات ۱۱۵-۱۳۰.

ملکی، احمد. (۱۳۹۷). «اصل صلاحیت جهانی در جرایم سایبری تروریستی». مجله مطالعات حقوق بین‌الملل، شماره ۳۴، صفحات ۷۵-۹۰.

رضایی، زهرا. (۱۳۹۶). «چالش‌های حقوقی مبارزه با سایبر تروریسم». پژوهشنامه حقوق فناوری اطلاعات، شماره ۵، صفحات ۲۵-۴۰.

امیری، علی‌رضا. (۱۳۹۹). «تبیین مفهوم سایبر تروریسم در قوانین ایران». مجله حقوق کیفری، شماره ۲، صفحات ۵۰-۷۰.

موسوی، نسرین. (۱۳۹۷). «نقش کنوانسیون بوداپست در مبارزه با جرایم سایبری». فصلنامه مطالعات بین‌الملل، شماره ۲۱، صفحات ۸۰-۹۵.

صادقی، محمود. (۱۳۹۵). «حقوق کیفری بین‌المللی و مقابله با تروریسم سایبری». مجله پژوهش‌های حقوقی، شماره ۴۳، صفحات ۱۰۰-۱۲۵.

حسینی، فاطمه. (۱۳۹۶). «بررسی خلأهای قانونی در مقابله با تروریسم سایبری». مجله حقوق بین‌الملل، شماره ۱۹، صفحات ۱۵۰-۱۷۰.

عباسی، مرتضی. (۱۳۹۷). «تحلیل حقوقی مسئولیت کیفری در فضای سایبر». مجله حقوق جزا، شماره ۲۷، صفحات ۶۰-۸۰.

نیکوکار، محمد. (۱۳۹۹). «مسئولیت کیفری دولت‌ها در جرایم سایبری بین‌المللی». پژوهش‌های حقوق بین‌الملل، شماره ۱۲، صفحات ۱۲۰-۱۴۰.

کاظمی، مریم. (۱۳۹۸). «چالش‌های حقوقی و فقهی مبارزه با تروریسم سایبری». پژوهش‌های فقه و حقوق، شماره ۳۴، صفحات ۹۰-۱۱۰.

سلیمانی، رضا. (۱۳۹۵). «قوانین ایران و پاسخ به جرایم سایبری تروریستی». فصلنامه حقوق فناوری، شماره ۱۱، صفحات ۵۵-۷۵.

هاشمی، علی. (۱۳۹۷). «اصول حقوقی مبارزه با تروریسم در فضای سایبر». مجله حقوق جزا و جرم‌شناسی، شماره ۴۵، صفحات ۱۳۰-۱۵۵.

پایان‌نامه‌ها:

محمدی، رضا. (۱۳۹۸). تجارب حقوقی کشورهای غربی در مقابله با جرایم سایبری. دانشگاه تهران.

جواهری، لیلا. (۱۳۹۹). تحلیل تطبیقی قوانین سایبری ایران و اروپا. دانشگاه شهید بهشتی.

Books:

Brenner, Susan W. (۲۰۱۰). Cybercrime: Criminal Threats from Cyberspace. New York: Praeger.

Wall, David S. (۲۰۱۷). Cybercrime, Cyberterrorism and Cybersecurity. London: Routledge.

Kshetri, Nir. (۲۰۱۶). The Economics of Cybersecurity and Cybercrime. New York: Springer.

Denning, Dorothy E. (۲۰۰۰). Information Warfare and Security. Boston: Addison-Wesley.

Kröger, Sabine. (۲۰۱۸). Cyberterrorism: Political and Legal Challenges. Berlin: Springer.

Rid, Thomas. (۲۰۱۳). Cyber War Will Not Take Place. Oxford: Oxford University Press.

Mueller, Milton L. (۲۰۱۰). Networks and States: The Global Politics of Internet Governance. Cambridge: MIT Press.

Holt, Thomas J. (۲۰۱۲). Cybercrime and Digital Forensics: An Introduction. New York: Routledge.

Articels:

Chertoff, Michael & Simon, T.J. (۲۰۱۵). «The Impact of the Dark Web on Internet Governance and Cyber Security». Global Commission on Internet Governance Paper Series.

Thomas, Timothy L. (۲۰۱۱). «Cyberterrorism: The Sum of All Fears?». Studies in Conflict & Terrorism.۴۸۳-۴۶۷ ،(۷)۳۴ ،

Lipman, Matthew & Watson, Ian. (۲۰۱۹). «Cybersecurity and International Law». Journal of Cyber Policy.۴۲-۲۳ ،(۱)۴ ،

Brenner, Susan W. (۲۰۱۴). «Combating Cyberterrorism through International Law». Journal of International Criminal Justice.۱۰۴۵-۱۰۲۳ ،(۴)۱۲ ،

Documents:

Council of Europe. (۲۰۰۱). Convention on Cybercrime (Budapest Convention). Strasbourg: Council of Europe Publishing.

United Nations. (۲۰۱۷). Global Counter-Terrorism Strategy. New York: United Nations.

U.S. Congress Research Service. (۲۰۱۶). Cyberterrorism Prevention Act. Washington, D.C.: U.S. Government Printing Office.