Received: 15 /04/2025
Review: 17/07/2025
Accepted: 08 /09/2025
DOI: 10.22054/jocl.2025.85063.2954

Journal of Cyber Law
No(2),Vol(2), 1-13.
ISSN: 0972-6934
www.jocl.ir

The Role of Cyber Law in Defining State Responsibility for Cross-Border Cyberattacks

Behroz Sharifi [1], Parvindokht farahmandpur [*2]

1- M.A. Student in Law, Payame Noor University, Shiraz, Iran

2*- M.A. Student in Law, Payame Noor University, Shiraz, Iran

ABSTRACT

With the expansion of cyberspace and the growing dependence of states on information technology-based critical infrastructures, cross-border cyberattacks have become one of the most pressing security and legal challenges of the modern era. The main research question of this study is to what extent cyber law provides a framework for defining state responsibility for such attacks and whether it can offer effective mechanisms for obligations and enforcement. The significance of this research lies in the fact that cyberattacks, due to their transnational nature, the difficulty of attribution, and technical complexities, have created substantial gaps in traditional international law, making a reconsideration of the foundations of state responsibility inevitable. The primary aim of this paper is to analyze the role of cyber law, as an emerging branch of international law, in addressing state accountability for harmful cyber operations. The research method is descriptive-analytical, based on documentary study, drawing upon international legal instruments, treaties, and state practice. The findings indicate that although existing international instruments—such as the Tallinn Manual and certain UN resolutions—represent important steps in recognizing state responsibility, significant shortcomings remain in clarifying attribution criteria and establishing enforcement mechanisms. The main conclusion is that cyber law can serve as a complementary framework to traditional international law by elaborating principles such as non-intervention, sovereignty, and the necessity of recognizing new customary norms, thereby paving the way toward a more coherent legal regime on state responsibility for cross-border cyberattacks. The novelty of this article lies in its systematic analysis of cyber law's role in bridging the gaps of classical international law and in proposing an integrated framework to address the current challenges.

Keywords:
Cyber law, State responsibility, Cyberattacks, International law, Cybersecurity

How to Cite: sharifi, B. and farahmandpur, P. (2025). The Role of Cyber Law in Defining State Responsibility for Cross-Border Cyberattacks. Journal of Cyber Law (JOCL), 2(2), 1-13.

DOI: 10.22054/jocl.2025.85063.2954

* Corresponding Author: parvindokht.farhamandpur@pnu.ac.ir

نشریه حقوق سایبری
شماره (۲) ۱-۱۳
دوره ۱٤۰٤

تاریخ دریافت: ۱٤۰٤/۰۱/۳۱
تاریخ اصلاح: ۱٤۰٤/۰٤/۲۵
تاریخ پذیرش: ۱٤۰٤/۰٦/۲۲

جایگاه حقوق سایبری در تبیین مسئولیت دولت‌ها نسبت به حملات سایبری برون‌مرزی

بهروز شریفی[۱] ، پروین دخت فرهمندپور[۲*]

۱- دانشجوی کارشناسی ارشد حقوق، دانشگاه پیام نور شیراز، ایران

۲ - دانشجوی کارشناسی ارشد حقوق، دانشگاه پیام نور شیراز، ایران

چکیده

با گسترش فضای مجازی و افزایش وابستگی دولت‌ها به زیرساخت‌های حیاتی مبتنی بر فناوری اطلاعات، حملات سایبری برون‌مرزی به یکی از مهم‌ترین چالش‌های امنیتی و حقوقی عصر حاضر تبدیل شده است. پرسش اصلی این پژوهش آن است که حقوق سایبری چه جایگاهی در تبیین مسئولیت دولت‌ها نسبت به چنین حملاتی دارد و تا چه حد می‌تواند ابزاری برای تعیین حدود تعهدات و ضمانت‌های اجرایی فراهم کند. اهمیت بررسی این موضوع از آن جهت است که حملات سایبری، به دلیل ماهیت فرامرزی، عدم شفافیت در شناسایی منبع و پیچیدگی‌های فنی، خلأهای جدی در قواعد سنتی حقوق بین‌الملل ایجاد کرده و نیازمند بازاندیشی در مبانی مسئولیت بین‌المللی دولت‌هاست. هدف اصلی مقاله تحلیل جایگاه حقوق سایبری به عنوان شاخه‌ای نوظهور از حقوق بین‌الملل در پاسخگویی به چالش‌های مسئولیت دولت‌ها در برابر اقدامات مخرب سایبری است. روش پژوهش توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی بوده و از بررسی منابع حقوق بین‌الملل، اسناد بین‌المللی مرتبط و رویه‌های عملی دولت‌ها برای تحلیل استفاده شده است. یافته‌های تحقیق نشان می‌دهد که هرچند اسناد بین‌المللی موجود، از جمله دستورالعمل‌های تالین و برخی قطعنامه‌های سازمان ملل، گامی مهم در جهت شناسایی مسئولیت دولت‌ها محسوب می‌شوند، اما همچنان کاستی‌های جدی در زمینه شفاف‌سازی معیارهای انتساب اعمال سایبری و تعیین ضمانت‌های اجرایی وجود دارد. نتیجه‌گیری اصلی پژوهش آن است که حقوق سایبری می‌تواند به عنوان چارچوبی مکمل برای حقوق بین‌الملل سنتی عمل کند و با تبیین اصولی چون منع مداخله، اصل حاکمیت و ضرورت شناسایی قواعد عرفی جدید، مسیر توسعه یک رژیم حقوقی منسجم‌تر در حوزه مسئولیت دولت‌ها نسبت به حملات سایبری برون‌مرزی را هموار سازد. نوآوری این مقاله در ارائه تحلیلی نظام‌مند از نقش حقوق سایبری در پر کردن خلأهای حقوق بین‌الملل کلاسیک و پیشنهاد چارچوبی تلفیقی برای پاسخگویی به چالش‌های موجود است.

کلیدواژه‌ها:

حقوق سایبری، مسئولیت دولت‌ها، حملات سایبری، حقوق بین‌الملل، امنیت سایبری

نحوه استناد:

شریفی, بهروز و فرهمندپور, پروین دخت . (۱۴۰۴). جایگاه حقوق سایبری در تبیین مسئولیت دولت‌ها نسبت به حملات سایبری برون‌مرزی. حقوق سایبری, ۲(۲), ۱-۱۳

* ایمیل نویسنده مسئول: parvindokht.farhamandpur@pnu.ac.ir

مقدمه

در عصر حاضر، فضای سایبری به عنوان حوزه‌ای نوظهور در تعاملات بین‌المللی مطرح شده است که دولت‌ها را هم به صورت مستقیم و هم به صورت غیرمستقیم در معرض تهدیدهای جدّی قرار می‌دهد. یکی از مسائل کلیدی در این زمینه، مسئولیت دولت‌ها در قبال حملات سایبری برون‌مرزی است؛ پرسش محوری این است که "حقوق سایبری" به چه نحوی می‌تواند مبنایی برای تعیین مسئولیت بین‌المللی دولت‌ها در برابر این حملات فراهم کند. در حقوق بین‌الملل متعارف، مسئولیت دولت‌ها بر مبنای دو عنصر اصلی بنیاد نهاده شده است: نخست، تخلف بین‌المللی یعنی نقض یک تعهد بین‌المللی، و دوم، انتساب عمل به دولت (Articles on Responsibility of States for Internationally Wrongful Acts, ILC) که در ماده ۲ و بندهای آن آمده است. برای نمونه، منشور ملل متحد در ماده ۲ بند ۴ منع توسل به زور را مقرر داشته است که حملات سایبری شدید ممکن است مشمول آن شود. اگر حمله سایبری به گونه‌ای باشد که آثارش معادل توسل به زور قلمداد شود یا مخاصمه مسلحانه ایجاد کند، آن‌گاه دولت مهاجم مسئول شناخته خواهد شد(صفری ،۱۴۰۴،ص۷۸). در نظام حقوق ایران نیز اگرچه قانون معینی که مسئولیت بین‌المللی دولت در زمینه حملات سایبری را با مواد و تبصره‌های روشن تنظیم کند، کمابیش در حال شکل‌گیری است، با این حال نهادهایی همچون قانون جرائم رایانه‌ای مصوب ۱۳۸۸ و دستورالعمل‌ها یا آیین‌نامه‌های مرتبط نشان می‌دهند که مسأله انتساب عامل حمله و تمیز آن از رفتار غیرمخاطره‌آمیز برای قضات و مراجع حقوقی اهمیت یافته است.اهمیت این موضوع به دلیل چالش‌های متعدد حقوقی و اجتماعی روز فزاینده است؛ نخست، بسیاری از حملات سایبری امکان فیزیکی وارد آوردن خسارت، تعطیلی زیرساخت‌های حیاتی مانند انرژی یا آب، انتقال بیماری‌ها یا اختلال در تأمین خدمات سلامت را دارند(رحمتی ،۱۴۰۱،ص۶۹)؛ دوم، تکنولوژیِ شناسایی عامل یا منبع حمله سایبری هنوز کامل نبوده و دولت‌های قربانی در درخواست جبران خسارت یا توقیف عملی مسئول دچار دشواری‌اند؛ سوم، فقدان قواعد الزام‌آور بین‌المللی که با جامعیت انتساب، معیارهای کنترل مؤثر یا معیار مراقبت لازم را در زمینه سایبری مقرر دارند، باعث شده است خلأهای عرفی و حقوقی قابل توجهی در این عرصه وجود داشته باشد.

پیشینه تحقیق نشان می‌دهد که موضوع مسئولیت دولت‌ها در حملات سایبری برون‌مرزی پیش از این نیز مورد توجه اندیشمندان داخلی و بین‌المللی بوده است. پرستو اسمعیل‌زاده ملاباشی و همکاران در مقاله "حملات سایبری و اصول حقوق بین‌الملل بشردوستانه (مطالعهٔ موردی: حملات سایبری به گرجستان)" به تحلیل این پرسش پرداخته‌اند که آیا قواعد حقوق مخاصمات مسلحانه سنتی قابلیت تسری به فضای مجازی را دارند یا خیر، و به این نتیجه رسیده‌اند که بخش‌هایی از این قواعد نیاز به تفسیر جدید دارند (اسمعیل‌زاده و همکاران، ۱۳۹۶، ص. ۵۴۰-۵۵۰). مقاله "مسئولیت بین‌المللی دولت‌ها و مسئله انتساب حملات سایبری" توسط رضا رحمتی نتیجه گرفته است که انتساب حمله سایبری به دولت تابع معیارهای کنترل کلی یا کنترل مؤثر است، ولی این معیارها در بسیاری موارد عملی قابل اثبات نیستند و نیاز به معیار مراقبت بایسته احساس می‌شود (رحمتی، ۱۴۰۱، ص. ۶۵-۷۵). در سطح بین‌المللی،(Węgliński,2016.p.123) به بررسی استانداردهای انتساب از جمله ارتباط با ماده ۲ ARSIWA پرداخته و نشان داده است که عرف بین‌المللی هنوز در بسیاری از موارد در شناسایی عمل متخلفانه ضعیف است .همچنین (William Banks,2020.p.45-60) تأکید کرده است که نبود اجماع بر سر معیارهای حقوقی انتساب، پاسخ بین‌المللی به حملات سایبری را تضعیف کرده است .اثر شراز به طور خاص به چالش‌های انتساب رفتار گروه‌های غیردولتی و کنترل فعّال دولت بر آنها پرداخته است

(Sheraz,2021,p.1230) چارچوب مفیدی برای تحلیل مسئولیت دولت‌ها با تأکید بر الزامات قانونی، امکانات و محدودیت‌ها پیشنهاد کرده است.

با وجود این خلأهایی قابل مشاهده‌اند: اولاً، هنوز یک چارچوب حقوقی یکپارچه و شناخته‌شده بین‌المللی برای انتساب حملات سایبری به دولت وجود ندارد که معیارهای کنترل مؤثر، انتساب دولتی و الزامات مراقبت لازم را با هم جمع کند؛ ثانیاً، بیشتر تحقیقات به بررسی نظری معیارهای حقوقی پرداخته‌اند و کمتر به موردکاوی‌هایی با تحلیل رویه عملی دولت‌ها یا عملکرد قضایی پرداخته شده است؛ ثالثاً، بررسی نقش حقوق سایبری به عنوان شاخه مستقل حقوق بین‌الملل، در ترکیب با حقوق عرفی، حقوق معاهدات و منشور سازمان ملل در تعیین مسئولیت دولت‌ها به طور نظام‌مند کمتر صورت گرفته است.پرسش‌های اصلی این تحقیق بدین ترتیب‌اند:

۱. حقوق سایبری چه نقشی در تعیین مسئولیت دولت‌ها نسبت به حملات سایبری برون‌مرزی دارد؟

۲. چه معیارهایی برای انتساب عمل سایبری به دولت وجود دارند و کدام یک کارآمدتر است؟

۳. چه ضمانت‌های اجرایی بین‌المللی برای اعمال مسئولیت دولت‌ها در برابر چنین حملاتی موجود است یا باید ایجاد شود؟

اهداف این مقاله به شرح زیراند: نخست تحلیل مفهومی حقوق سایبری و تعیین جایگاه آن در حقوق بین‌الملل؛ دوم شناخت و بررسی معیارهای انتساب و مسئولیت دولت‌ها در مواجهه با حملات سایبری برون‌مرزی؛ سوم شناسایی خلأهای حقوقی و ارائه پیشنهادهایی برای تقویت ضمانت‌های اجرایی و ایجاد یک چارچوب تلفیقی حقوقی.

روش پژوهش در این مقاله توصیفی-تحلیلی است؛ داده‌ها و مواد تحقیق از منابع اسنادی گردآوری شده‌اند شامل معاهدات بین‌المللی، قطعنامه‌ها، منشور ملل متحد، رویّه قضایی بین‌المللی، اسناد کارشناسی چون Tallinn Manual و مقالات حقوقی معتبر داخلی و خارجی. تطبیق بین حقوق معاصر و عرف بین‌الملل و بررسی موردی در کشورهایی که سابقه قابل توجهی در حملات سایبری داشته‌اند نیز مورد استفاده قرار خواهد گرفت تا جنبه عملی و حقوقی موضوع روشن‌تر شود. این روش به ما امکان می‌دهد تا نه تنها نظریه‌های حقوقی را بازنمایی کنیم بلکه نقد آنها را با توجه به واقعیت‌های سیاسی و فنی موجود بررسی نماییم و پیشنهادهایی عملی برای بهبود وضعیت فعلی عرضه کنیم.

حقوق سایبری

به عنوان شاخه‌ای نوظهور از حقوق بین‌الملل و حقوق داخلی، به مجموعه قواعد و مقررات حقوقی اطلاق می‌شود که رفتارها و روابط انسانی در فضای دیجیتال و شبکه‌های رایانه‌ای را تنظیم می‌کند و بر مسئولیت دولت‌ها، سازمان‌ها و افراد در استفاده از فناوری اطلاعات تأثیر می‌گذارد (Kuner, 2013, p. 27). این حوزه حقوقی، هم قواعد الزام‌آور بین‌المللی و هم قواعد قراردادی و داخلی را در بر می‌گیرد و مرز مشخصی میان مقررات عرفی و قانونی در آن وجود ندارد. حمله سایبری به هرگونه اقدام عمدی گفته می‌شود که از طریق شبکه‌های رایانه‌ای یا ارتباطات دیجیتال، با هدف تخریب، اختلال، دسترسی غیرمجاز یا سوءاستفاده از داده‌ها و زیرساخت‌های حیاتی انجام می‌شود (Schmitt, 2017, p. 63). در دستورالعمل تالین ۲٫۰، روشن شده است که حمله سایبری در صورتی می‌تواند معادل استفاده از زور تلقی شود که آثار آن مشابه حمله مسلحانه باشد و به طور جدی به زیرساخت‌های حیاتی یا امنیت ملی کشورها آسیب وارد کند (Tallinn Manual 2.0, Rule 69).حقوق سایبری نقش تعیین‌کننده‌ای در تعیین مسئولیت دولت‌ها ایفا می‌کند. مطابق اصول ARSIWA، هر اقدام متخلفانه‌ای که به دولت قابل انتساب باشد، موجب مسئولیت بین‌المللی آن

دولت است (ILC, 2001, p. 35). در زمینه سایبری، دشواری انتساب حملات، ناشی از استفاده مهاجمان از واسطه‌ها، شبکه‌های توزیع شده و فناوری‌های ناشناس‌ساز است، بنابراین تدوین چارچوب حقوق سایبری برای روشن‌سازی حدود مسئولیت، الزامی است. این چارچوب شامل معیارهای شناسایی عامل، تعیین حدود صلاحیت دولت‌ها برای پاسخ، و استانداردهای مراقبت لازم در جلوگیری یا پاسخ به حملات است.

در سطح داخلی ایران، حقوق سایبری بخشی از قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و آیین‌نامه‌ها و دستورالعمل‌های مرتبط است. این مقررات گرچه بیشتر مسئولیت کیفری افراد را پوشش می‌دهند، ولی به تدریج پایه‌ای برای بررسی مسئولیت دولت‌ها و سازمان‌ها در مواجهه با تهدیدات سایبری فراهم می‌کنند(رحمانی ،۱۴۰۰ ص۶۸). اصول حقوق سایبری بر مبانی اخلاقی، امنیتی و اقتصادی نیز استوار است؛ از منظر فلسفه حقوق، تضمین مسئولیت و پاسخگویی، کارآمدی نظام حقوقی بین‌الملل را در برابر تهدیدات نوین حفظ می‌کند (Kelsen, 1967, p. 120)، و از منظر اقتصادی، حملات سایبری می‌تواند خسارات گسترده‌ای به زیرساخت‌ها و اقتصاد ملی وارد کند و نیاز به چارچوب حقوقی قوی را افزایش می‌دهد (OECD, 2019, p. 88).

مسئولیت دولت‌ها

دولت ها نیز به عنوان یک نهاد ریشه‌دار در حقوق بین‌الملل، بر مبنای مواد کمیسیون حقوق بین‌الملل در خصوص مسئولیت دولت‌ها برای اعمال متخلفانه بین‌المللی (ARSIWA) تعریف می‌شود. ماده ۲ این اسناد بیان می‌دارد که هر فعل یا ترک فعل دولت که با نقض تعهدات بین‌المللی همراه باشد و به دولت قابل انتساب باشد، موجب مسئولیت بین‌المللی آن خواهد بود (ILC, 2001, p. 35). در حوزه سایبری، انتساب از دشوارترین مسائل است زیرا ماهیت حملات معمولاً ناشناس یا از طریق واسطه‌های متعدد صورت می‌گیرد. در حقوق داخلی ایران نیز مفهوم مسئولیت در جرائم رایانه‌ای در مواد ۱ و ۵ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ مورد توجه قرار گرفته است، هرچند این قانون بیشتر بر مسئولیت کیفری افراد متمرکز است تا مسئولیت بین‌المللی دولت‌ها.

حاکمیت

مفهوم حاکمیت به عنوان یکی از اصول بنیادین حقوق بین‌الملل، پایه و اساس تعیین مسئولیت دولت‌ها در زمینه حملات سایبری است. بر اساس منشور ملل متحد، ماده ۲ بند ۱، دولت‌ها دارای برابری حاکمیتی هستند و هیچ کشوری حق دخالت در امور داخلی دولت دیگر را ندارد (UN Charter, 1945, p. 7). این اصل در حقوق سایبری نیز اهمیت خود را حفظ می‌کند، چرا که حمله به زیرساخت‌های حیاتی یک کشور—مانند شبکه‌های برق، سامانه‌های ارتباطات یا سیستم‌های مالی—نقض حاکمیت دولت تلقی می‌شود، حتی اگر این حمله به سطح مخاصمه مسلحانه نرسد (Schmitt, 2017, p. 65). بر اساس دکترین حقوق بین‌الملل، دولت‌ها حق دارند اقدامات دفاعی یا پیشگیرانه‌ای را علیه فعالیت‌های سایبری تهدیدکننده امنیت ملی خود اتخاذ کنند، مشروط بر اینکه این اقدامات با اصول شناخته‌شده بین‌المللی هماهنگ باشد و به کشور ثالث آسیب نامتناسب نرساند (Kelsen, 1967, p. 120; Shaw, 2017, pp. 52–55).تحلیل حقوقی حاکمیت در حوزه سایبری نشان می‌دهد که مفهوم حاکمیت و مسئولیت دولت‌ها به یکدیگر متصل هستند. حملات سایبری می‌تواند موجب مسئولیت بین‌المللی دولت مهاجم شود، چه آن حمله توسط نهادهای رسمی دولت انجام شده باشد و چه توسط گروه‌های غیردولتی که تحت حمایت یا سکوت دولت مورد نظر قرار گرفته‌اند (Banks, 2020, pp. 45–50; Sheraz, 2021, pp. 1230–1233). همچنین، مفاهیم حقوق سایبری

جدید مانند «انتساب حملات» و «اقدام متقابل محدود» به دولت‌ها امکان می‌دهد چارچوب حقوقی برای پاسخگویی به تهدیدات سایبری داشته باشند، بدون اینکه اصول حاکمیت کشورها زیر پا گذاشته شود (Saaishri & Ravi, 2023, pp. 2418–2426). در نتیجه، احترام به حاکمیت دولتی و همزمان شناسایی مسئولیت بین‌المللی در حملات سایبری، محور اصلی توسعه سیاست‌ها و مقررات بین‌المللی در زمینه امنیت سایبری محسوب می‌شود و پایه‌ای برای ایجاد رویه قضایی و قوانین ملی در این حوزه فراهم می‌آورد.

از حیث مبانی نظری، فلسفه حقوقی مسئولیت دولت‌ها در قبال حملات سایبری بر اصل مسئولیت اخلاقی و سیاسی مبتنی است. اندیشمندان فلسفه حقوق همچون هانس کلسن معتقد بودند که هر نظام حقوقی بدون وجود ضمانت اجرای مسئولیت نمی‌تواند معنا داشته باشد (Kelsen, 1967, p. 120). از این منظر، اگر دولت‌ها مسئولیتی در قبال رفتارهای سایبری نداشته باشند، نظام حقوقی بین‌الملل در برابر تهدیدات جدید کارآمدی خود را از دست می‌دهد. در فقه اسلامی نیز اصل «لاضرر و لاضرار فی الاسلام» (وسائل‌الشیعه، ج ۱۷، ص. ۳۴۰) به عنوان مبنای مسئولیت شناخته می‌شود و می‌تواند در تحلیل فقهی حملات سایبری که موجب زیان‌های گسترده به اموال و جان انسان‌ها می‌شود، مورد استناد قرار گیرد. همچنین قاعده «تسبیب» در فقه که بیان می‌کند هرکس سبب ورود ضرر شود ضامن است (شهید ثانی، ۱۴۱۰ق، ج ۲، ص. ۲۱۷)، قابل تطبیق بر مواردی است که دولت‌ها از سرزمین خود برای انجام حملات سایبری علیه دیگران غفلت ورزند.

از دیدگاه حقوقی، حقوق آمره در حوزه حقوق بین‌الملل جایگاهی ویژه دارد. اصولی همچون منع توسل به زور و اصل احترام به تمامیت ارضی و استقلال سیاسی دولت‌ها در شمار قواعد آمره شناخته شده‌اند (Shaw, 2017, p. 52). اگر حمله سایبری به سطحی برسد که معادل استفاده از زور باشد، نه تنها نقض یک تعهد عادی بلکه نقض یک قاعده آمره محسوب می‌شود و مسئولیت شدیدتری برای دولت مهاجم به دنبال دارد. در قانون اساسی جمهوری اسلامی ایران نیز اصول متعددی وجود دارد که به مسئولیت دولت در قبال امنیت عمومی و روابط بین‌المللی اشاره دارد. برای مثال اصل ۱۵۲ قانون اساسی سیاست خارجی ایران را بر اساس نفی هرگونه سلطه‌گری و سلطه‌پذیری تعریف می‌کند و این اصل در حوزه سایبری نیز قابل تفسیر است. همچنین اصل ۷۷ مقرر می‌دارد که عهدنامه‌ها و مقاوله‌نامه‌های بین‌المللی باید به تصویب مجلس شورای اسلامی برسند، که نشان‌دهنده نقش حقوق داخلی در تنظیم روابط بین‌المللی حتی در عرصه سایبری است.

از حیث مبانی اقتصادی، حملات سایبری پیامدهای گسترده‌ای بر اقتصاد ملی و بین‌المللی دارند. خسارات ناشی از حملات سایبری به زیرساخت‌های انرژی، حمل‌ونقل یا سیستم‌های مالی می‌تواند میلیاردها دلار زیان ایجاد کند و این امر ضرورت مسئولیت دولت‌ها را دوچندان می‌سازد (OECD, 2019, p. 88). علاوه بر این، اقتصاد دیجیتال جهانی به همکاری میان دولت‌ها وابسته است و در نبود چارچوب مسئولیت، اعتماد متقابل در تجارت و تبادل داده‌ها آسیب خواهد دید.بنابراین، مبانی نظری و مفهومی نشان می‌دهند که حقوق سایبری، مسئولیت دولت‌ها، اصل حاکمیت، قواعد آمره، و مبانی فقهی و اقتصادی همگی چارچوبی چندوجهی برای تبیین مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری برون‌مرزی فراهم می‌کنند.

نظریه‌های حقوقی مرتبط با مسئولیت دولت‌ها در حملات سایبری برون‌مرزی بر پایه اصول بنیادین حقوق بین‌الملل و شاخه نوظهور حقوق سایبری استوار هستند. یکی از مهم‌ترین نظریه‌ها، نظریه مسئولیت دولتی بر اساس انتساب عمل است

که در مواد ۲ و ۴ ARSIWA به وضوح بیان شده است. ماده ۲ این اسناد تصریح می‌کند که هر فعل یا ترک فعلی که از جانب دولت انجام شود و با نقض تعهدات بین‌المللی همراه باشد، موجب مسئولیت بین‌المللی دولت خواهد شد (ILC, 2001, p. 35). ماده ۴ ARSIWA نیز بیان می‌دارد که اقدامات سازمان‌های دولتی و هر عمل خصوصی که به عنوان نماینده دولت انجام شده باشد، قابل انتساب به دولت است. این نظریه به خصوص در حقوق سایبری اهمیت دارد، زیرا بسیاری از حملات از طریق گروه‌های غیردولتی یا هکرهای ناشناس انجام می‌شود و تعیین انتساب قانونی نیازمند معیارهای روشن حقوقی است (Banks, 2020, pp. 48-52).نظریه دوم، معیار مراقبت لازم است که بر اساس آن، دولت‌ها موظف‌اند از سرزمین خود برای آسیب نرساندن به دیگر کشورها مراقبت کنند. این اصل در رویه قضایی بین‌المللی و همچنین در اسناد حقوقی مانند دستورالعمل تالین مورد تأکید قرار گرفته است(Schmitt ,2017, pp. 67-70) توضیح می‌دهد که اگر یک دولت از انجام اقدامات پیشگیرانه لازم برای جلوگیری از حملات سایبری به دیگر کشورها غفلت کند، مسئولیت آن دولت فعال می‌شود حتی اگر حمله به صورت مستقیم توسط دولت انجام نشده باشد. این نظریه با اصول فقهی قاعده «تسبیب» همخوانی دارد که هرکس سبب ورود ضرر شود، ضامن است (شهید ثانی، ۱۴۱۰ق، ج ۲، ص. ۲۱۷).از منظر حقوق داخلی ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸، ماده ۵، دولت و نهادهای عمومی را موظف کرده است تا از سامانه‌های حیاتی و زیرساخت‌ها حفاظت کنند و اقدامات پیشگیرانه انجام دهند. این ماده به شکل غیرمستقیم با نظریه «مراقبت لازم» همسو است و نشان می‌دهد که حقوق داخلی در برخی حوزه‌ها با اصول بین‌المللی تلفیق می‌شود. علاوه بر آن، اصول ۷۷ و ۱۲۵ قانون اساسی ایران، که به تصویب معاهدات بین‌المللی و تعهدات دولت در روابط خارجی اشاره دارد، امکان استناد به استانداردهای بین‌المللی حقوق سایبری و مسئولیت دولت‌ها را فراهم می‌آورد.دیدگاه‌های دکترین حقوقی نیز تنوع گسترده‌ای دارند. (Konrad Węgliński ,2016, pp. 125-130) معتقد است که معیارهای سنتی انتساب در ARSIWA برای فضای سایبری کافی نیست و نیاز به استانداردهای جدید مبتنی بر شواهد فنی و دیجیتال وجود دارد. از سوی دیگر، William Banks ,2020, pp. 55-60)) بر این باور است که تعیین مسئولیت در حقوق سایبری باید به ترکیبی از معیارهای حقوقی و تحلیل‌های فنی متکی باشد و صرفاً اتکا به ارتباط رسمی با دولت کافی نیست. (Sheraz ,2021, pp. 1232-1235) نیز به مسأله رفتار گروه‌های غیردولتی در عملیات سایبری پرداخته و تاکید می‌کند که دولت‌ها ممکن است مسئول باشند حتی اگر کنترل مستقیم بر این گروه‌ها نداشته باشند، مشروط بر اینکه از انجام اقدامات پیشگیرانه کوتاهی کرده باشند.نظریه دیگری که اهمیت دارد، نظریه اقدام متقابل است. بر اساس ماده ۲۲ ARSIWA، دولت‌ها می‌توانند در برابر اعمال متخلفانه دیگر دولت‌ها اقدام متقابل کنند، مشروط بر اینکه این اقدامات متناسب و مطابق با اصول حقوق بین‌الملل باشد (ILC, 2001, p. 64). در حقوق سایبری، این نظریه به دولت‌ها اجازه می‌دهد تا در برابر حملات سایبری پاسخ محدود و قانونی ارائه دهند، اما باید دقت شود که اقدام متقابل نباید به سطح استفاده از زور برسد، زیرا در این صورت مسئولیت جدی‌تری ایجاد می‌شود.

در زمینه حقوق آمره، حملات سایبری که معادل تجاوز یا نقض تمامیت ارضی کشورها باشد، مشمول قواعد آمره می‌شود و دولت مهاجم مسئولیت کامل خواهد داشت (Shaw, 2017, pp. 53-55). حقوق سایبری به عنوان شاخه‌ای که تعامل میان مقررات داخلی، معاهدات بین‌المللی و عرف بین‌المللی را سامان می‌دهد، امکان تحلیل دقیق این نوع حملات و تعیین مسئولیت دولت‌ها را فراهم می‌کند.رحمانی (۱۴۰۰، ص. ۶۵-۷۵) و اسمعیل‌زاده ملاباشی (۱۳۹۶،

ص. ۵۴۰-۵۵۰) بر این باورند که تحلیل مسئولیت دولت‌ها در حملات سایبری باید مبتنی بر ترکیب معیارهای حقوقی بین‌المللی، اسناد داخلی و شواهد فنی باشد و صرفاً اتکا به ارجاعات عرفی یا تجربی کافی نیست. این دیدگاه‌ها نشان می‌دهند که در ادبیات داخلی نیز تلاش برای تلفیق دکترین و معیارهای عملی در حوزه حقوق سایبری صورت گرفته است، اما همچنان خلاهایی وجود دارد که مقاله حاضر به دنبال پر کردن آن‌هاست.

در نتیجه، نظریه‌های حقوقی مرتبط با حقوق سایبری و مسئولیت دولت‌ها در حملات برون‌مرزی شامل سه محور اصلی است: انتساب عمل، مراقبت لازم، و اقدام متقابل. هر کدام از این نظریه‌ها با مواد و تبصره‌های ARSIWA و حقوق داخلی ایران قابل تحلیل است و چارچوب قانونی برای مسئولیت بین‌المللی دولت‌ها فراهم می‌کند. این تحلیل نظری، پایه‌ای محکم برای بررسی پیشینه پژوهش‌ها و شناسایی خلأهای موجود فراهم می‌سازد و مسیر توسعه چارچوب حقوق سایبری جامع برای مسئولیت دولت‌ها را روشن می‌کند.

پیشینه پژوهش در حوزه حقوق سایبری و مسئولیت دولت‌ها در حملات سایبری برون‌مرزی نشان می‌دهد که این موضوع از سال‌های اخیر مورد توجه پژوهشگران داخلی و بین‌المللی قرار گرفته است، اما همچنان خلاهای قابل توجهی وجود دارد. در سطح بین‌المللی، (Schmitt (2013, pp. 15-40 به تحلیل کاربرد قواعد سنتی حقوق بین‌الملل در عملیات سایبری پرداخته و نشان داده است که بسیاری از اصولی مانند منع توسل به زور و اصل حاکمیت، در حوزه سایبری نیاز به تفسیر دقیق‌تر دارند. وی همچنین تأکید می‌کند که نبود معیارهای روشن برای انتساب حمله، چالشی اساسی در تعیین مسئولیت دولت‌هاست (Banks ,2020, pp. 45-60) با بررسی نظریه‌های انتساب و معیارهای مراقبت لازم، به این نتیجه رسید که تعیین مسئولیت در فضای سایبری نیازمند تلفیق تحلیل‌های حقوقی و شواهد فنی است و صرفاً اتکا به معیارهای حقوقی سنتی ناکافی است(Sheraz ,2021, pp. 1230-1238) نیز بر مسأله رفتار گروه‌های غیردولتی تأکید دارد و نشان می‌دهد که دولت‌ها حتی در نبود کنترل مستقیم بر این گروه‌ها، در صورت کوتاهی در اعمال اقدامات پیشگیرانه، مسئول شناخته می‌شوند. (Ravi ,2023, pp. 2418-2426) چارچوبی تحلیلی ارائه کرده‌اند که با تلفیق مقررات داخلی و بین‌المللی، امکان شناسایی مسئولیت دولت‌ها در عملیات سایبری را فراهم می‌کند، اما این چارچوب بیشتر جنبه نظری دارد و بررسی موردی محدودی ارائه می‌دهد.در سطح داخلی، تحقیقات متعددی به بررسی ابعاد حقوقی حملات سایبری پرداخته‌اند. اسمعیل‌زاده ملاباشی و همکاران (۱۳۹۶, ص. ۵۴۰-۵۵۰) با مطالعه حملات سایبری به گرجستان، تحلیل کرده‌اند که قواعد حقوق مخاصمات مسلحانه سنتی تا چه حد قابلیت تسری به حملات سایبری را دارند و نتیجه گرفته‌اند که بخشی از این قواعد نیازمند تفسیر نوین است. رحمتی (۱۴۰۱, ص. ۶۵-۷۵) نیز بر موضوع انتساب حملات سایبری به دولت‌ها تمرکز کرده و معتقد است که معیارهای کنترل مؤثر و استانداردهای مراقبت لازم هنوز در عمل قابل اثبات نیستند و خلأهای حقوقی قابل توجهی وجود دارد. رحمانی (۱۴۰۰, ص. ۶۵-۷۵) با بررسی مسئولیت بین‌المللی دولت‌ها و چارچوب قانونی ایران، نشان داده است که حقوق داخلی با وجود مواد محدود در قانون جرایم رایانه‌ای، هنوز فاقد یک نظام جامع برای انتساب و پاسخ به حملات سایبری برون‌مرزی است.تحلیل این پیشینه پژوهشی نشان می‌دهد که بیشتر تحقیقات بین‌المللی به تحلیل نظری و توسعه چارچوب‌های اصولی حقوق سایبری پرداخته‌اند و تحقیقات داخلی نیز عمدتاً بر مبنای تطبیق قواعد بین‌المللی با حقوق ایران و مطالعه موردی محدود تمرکز داشته‌اند. نقاط قوت این تحقیقات شامل ارائه نظریه‌های دقیق حقوقی، تحلیل معیارهای انتساب و مراقبت لازم، و اشاره به الزامات حقوق آمره و حاکمیت دولت‌هاست. اما نقاط ضعف آن‌ها نیز آشکار است: اولاً فقدان چارچوب عملی و

یکپارچه برای تلفیق معیارهای حقوقی، شواهد فنی و رویه عملی دولت‌ها؛ ثانیاً محدود بودن بررسی‌های تطبیقی میان حقوق داخلی و بین‌المللی در زمینه حملات سایبری؛ ثالثاً کمبود تحلیل نظام‌مند بر نقش حقوق سایبری به عنوان شاخه مستقل که بتواند خلأهای موجود در حقوق بین‌الملل کلاسیک را پر کند.مقاله حاضر در صدد است این خلأها را پر کند و جایگاه حقوق سایبری را در تبیین مسئولیت دولت‌ها نسبت به حملات سایبری برون‌مرزی به صورت نظام‌مند و تلفیقی تحلیل نماید. نوآوری این پژوهش در چند محور است: نخست، تحلیل جامع و همزمان حقوق بین‌الملل، حقوق داخلی ایران و اصول فقهی مرتبط با مسئولیت دولت‌ها در حوزه سایبری؛ دوم، ارائه چارچوب تحلیلی برای شناسایی انتساب عمل، تعیین حد اقدامات متقابل و بررسی استانداردهای مراقبت لازم در حملات سایبری؛ سوم، بررسی خلأهای عملی و حقوقی موجود در پیشینه پژوهش‌های داخلی و خارجی و ارائه پیشنهادهایی برای تقویت ضمانت‌های اجرایی و توسعه استانداردهای حقوقی.این رویکرد امکان می‌دهد که جایگاه تحقیق حاضر در میان ادبیات موضوع به وضوح مشخص شود: در حالی که پژوهش‌های پیشین بیشتر بر تحلیل نظری و بررسی موردی محدود تمرکز داشته‌اند، مقاله حاضر با تلفیق مبانی نظری، قوانین داخلی و بین‌المللی، دکترین حقوقی و تحلیل عملی، چارچوبی جامع و عملی برای مسئولیت دولت‌ها در حملات سایبری برون‌مرزی ارائه می‌دهد. این چارچوب می‌تواند به سیاست‌گذاران، نهادهای حقوقی و پژوهشگران کمک کند تا بر اساس یک نظام حقوقی منسجم، تصمیم‌گیری و اعمال حقوقی در مواجهه با تهدیدات سایبری را انجام دهند.

تحلیل مسئولیت دولت‌ها در حقوق داخلی ایران

در حقوق داخلی ایران، مسئولیت دولت‌ها در قبال حملات سایبری برون‌مرزی به‌طور مستقیم در قوانین مشخصی پیش‌بینی نشده است. با این حال، برخی از مواد قانونی می‌توانند به‌طور غیرمستقیم به این موضوع مرتبط باشند. برای مثال، ماده ۲ قانون جرایم رایانه‌ای جمهوری اسلامی ایران (مصوب ۱۳۸۸) به‌صراحت به "حملات رایانه‌ای" اشاره کرده است، اما این ماده بیشتر بر جرایم داخلی تمرکز دارد و به مسئولیت دولت‌ها در سطح بین‌المللی نمی‌پردازد.همچنین، در قانون اساسی جمهوری اسلامی ایران، اصولی مانند اصل ۷۷ که به تصویب قراردادهای بین‌المللی اشاره دارد، می‌تواند مبنای مسئولیت دولت در قبال تعهدات بین‌المللی باشد. با این حال، در خصوص حملات سایبری برون‌مرزی، خلأ قانونی مشهودی وجود دارد که نیازمند تدوین قوانین خاص در این زمینه است.

تحلیل رویه قضایی ایران

در رویه قضایی ایران، تاکنون پرونده‌های مشخصی در خصوص مسئولیت دولت‌ها در قبال حملات سایبری برون‌مرزی وجود ندارد. این موضوع به‌دلیل نو بودن و پیچیدگی‌های فنی و حقوقی آن است. با این حال، در پرونده‌هایی مانند حملات سایبری به زیرساخت‌های هسته‌ای ایران، دادگاه‌ها و مقامات قضایی ایران بر لزوم پاسخگویی و مسئولیت‌پذیری در برابر چنین حملاتی تأکید کرده‌اند(رحمتی ،۱۴۰۱،ص۶۹). این موارد نشان‌دهنده توجه نظام قضایی ایران به موضوع مسئولیت دولت‌ها در قبال حملات سایبری است، هرچند که هنوز رویه منسجمی در این زمینه شکل نگرفته است.

مقایسه با حقوق بین‌الملل و سایر کشورها

در سطح بین‌المللی، مسئولیت دولت‌ها در قبال حملات سایبری برون‌مرزی موضوعی پیچیده و در حال توسعه است. اسناد بین‌المللی مانند گزارش گروه کارشناسان دولتی سازمان ملل متحد (GGE) و نظرات مشورتی دیوان بین‌المللی دادگستری، بر لزوم اعمال حقوق بین‌الملل به فضای سایبری تأکید دارند. به‌عنوان مثال، در گزارش GGE، آمده است

که "حقوق بین‌الملل باید به‌طور کامل در فضای سایبری اعمال شود" (GGE Report, 2015, p. 4).در حقوق برخی کشورها مانند ایالات متحده و کشورهای عضو اتحادیه اروپا، قوانین خاصی برای مقابله با حملات سایبری وجود دارد. برای مثال، در ایالات متحده، قانون "قانون جرایم رایانه‌ای و سوءاستفاده از آن" (CFAA) به‌صراحت به جرایم سایبری اشاره دارد و مجازات‌های مشخصی برای آن‌ها تعیین کرده است. این در حالی است که در حقوق ایران، چنین قوانینی به‌طور خاص برای حملات سایبری برون‌مرزی وجود ندارد.

با توجه به خلأهای موجود در حقوق داخلی ایران و مقایسه با حقوق بین‌الملل و سایر کشورها، پیشنهاد می‌شود که جمهوری اسلامی ایران نسبت به تدوین قوانین خاص در زمینه مسئولیت دولت‌ها در قبال حملات سایبری برون‌مرزی اقدام کند. این قوانین باید با توجه به اصول حقوق بین‌الملل و تجربیات سایر کشورها، به‌گونه‌ای تنظیم شوند که هم‌راستا با تحولات فناوری و تهدیدات جدید سایبری باشند.همچنین، ایجاد رویه قضایی منسجم در این زمینه می‌تواند به شفافیت و پیش‌بینی‌پذیری در برخورد با حملات سایبری کمک کند. این رویه باید بر اساس اصول حقوقی پذیرفته‌شده بین‌المللی و با توجه به واقعیت‌های فنی و امنیتی فضای سایبری شکل گیرد.می توان چنین بیان نمود که ، مسئولیت دولت‌ها در قبال حملات سایبری برون‌مرزی نه‌تنها یک موضوع حقوقی، بلکه یک مسئله امنیتی و استراتژیک است که نیازمند توجه جدی و اقدامات مؤثر در سطح ملی و بین‌المللی است. با تدوین قوانین مناسب و ایجاد رویه‌های قضایی منسجم، می‌توان از تهدیدات سایبری کاست و امنیت ملی را در برابر این نوع حملات تأمین کرد.

بحث و نتیجه‌گیری

مقاله حاضر با تمرکز بر جایگاه حقوق سایبری در تبیین مسئولیت دولت‌ها نسبت به حملات سایبری برون‌مرزی، نشان می‌دهد که این حوزه حقوقی در حال شکل‌گیری و توسعه است و می‌تواند خلأهای موجود در نظام حقوقی بین‌المللی و داخلی را پر کند. از تحلیل حقوق داخلی ایران، رویه قضایی، و مقایسه با حقوق بین‌الملل مشخص شد که هرچند قوانین داخلی ایران همچون قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و اصول قانون اساسی نظیر اصل ۷۷ و ۱۲۵ به طور محدود به مسئولیت دولت‌ها و الزامات مرتبط با تعهدات بین‌المللی اشاره دارند، اما به‌طور مستقیم به حملات سایبری برون‌مرزی نمی‌پردازند و خلأ قابل توجهی در این زمینه وجود دارد. این خلأ نشان می‌دهد که در مواجهه با تهدیدات سایبری فراملی، نظام حقوقی داخلی فاقد چارچوبی جامع و کاربردی است که بتواند مسئولیت دولت را روشن کند و تضمین‌کننده پاسخگویی حقوقی باشد.

تحلیل رویه قضایی ایران نشان داد که تاکنون پرونده‌های مشخصی در این زمینه شکل نگرفته است، هرچند اصول کلی و حقوقی، از جمله لزوم رعایت تعهدات بین‌المللی و حفاظت از امنیت ملی، می‌تواند مبنای پاسخگویی قضایی در آینده باشد. بررسی تجارب سایر کشورها و اسناد بین‌المللی مانند گزارش GGE سازمان ملل، دستورالعمل تالین و ARSIWA نشان می‌دهد که در سطح بین‌المللی، چارچوب‌های اصولی و معیارهای انتساب و مراقبت لازم به صورت دقیق و مرحله‌ای تعریف شده‌اند و دولت‌ها ملزم به رعایت آن‌ها هستند. این امر نه تنها باعث پاسخگویی دولت‌ها می‌شود، بلکه شفافیت و پیش‌بینی‌پذیری حقوقی را در برخورد با حملات سایبری افزایش می‌دهد.بر اساس بررسی‌های انجام‌شده، می‌توان نتیجه گرفت که حقوق سایبری به عنوان یک شاخه مستقل و مکمل، نقش کلیدی در تبیین مسئولیت دولت‌ها ایفا می‌کند و می‌تواند چارچوب قانونی و عملی برای پاسخگویی دولت‌ها در برابر حملات سایبری برون‌مرزی فراهم آورد. این مسئولیت شامل سه محور اصلی است: انتساب عمل، که تعیین می‌کند دولت چه زمانی مسئول حمله‌ای

است که از سرزمین یا منابع آن انجام شده است؛ مراقبت لازم، که الزامی است برای پیشگیری از استفاده از سرزمین یا منابع دولتی برای حملات سایبری علیه دیگر کشورها؛ و اقدام متقابل، که امکان پاسخ قانونی و متناسب به حملات متخلفانه را فراهم می‌کند.

آثار و پیامدهای حقوقی این نتایج قابل توجه است. از منظر قانون‌گذاری، روشن شدن مسئولیت دولت‌ها در حملات سایبری نیازمند اصلاح قوانین داخلی و تدوین مقررات جامع است. این قوانین باید به صراحت معیارهای انتساب، استانداردهای مراقبت لازم و حدود پاسخ قانونی دولت‌ها را مشخص کنند. از منظر رویه قضایی، ایجاد پرونده‌ها و تصمیمات قضایی منسجم در زمینه حملات سایبری می‌تواند به شکل‌گیری الگوی قضایی پایدار و افزایش ضمانت اجرایی قوانین کمک کند. همچنین، برای حقوق شهروندان، شفافیت در مسئولیت دولت‌ها به معنای تضمین امنیت اطلاعات، زیرساخت‌ها و خدمات حیاتی است و اعتماد عمومی به دولت و نظام حقوقی را افزایش می‌دهد.

در مقایسه با تجربیات بین‌المللی، مطالعه نشان داد که کشورهای پیشرو در حوزه حقوق سایبری، مانند ایالات متحده و اعضای اتحادیه اروپا، چارچوب‌های حقوقی و اجرایی دقیق و عملی دارند که همزمان امکان پاسخ قانونی و پیشگیری از حملات را فراهم می‌کند. بنابراین، تجربه این کشورها می‌تواند برای قانون‌گذاران و نهادهای قضایی ایران مفید باشد و راهنمایی‌هایی برای تدوین مقررات داخلی ارائه کند. استفاده از استانداردهای بین‌المللی، دستورالعمل‌های تخصصی و معیارهای دکترین حقوقی، به ویژه در زمینه شناسایی مسئولیت دولت‌ها و نحوه پاسخ قانونی، می‌تواند خلاهای موجود در نظام حقوقی ایران را کاهش دهد و چارچوبی عملیاتی برای مدیریت تهدیدات سایبری ایجاد کند.پیشنهادهایی که از تحلیل حاضر به دست می‌آید شامل موارد زیر است: نخست، اصلاح قانون جرایم رایانه‌ای و گنجاندن مواد مشخص درباره مسئولیت دولت‌ها در حملات سایبری برون‌مرزی؛ دوم، تصویب مقررات تکمیلی و آیین‌نامه‌های اجرایی برای تعیین معیارهای انتساب، الزامات مراقبت لازم و حدود اقدامات متقابل؛ سوم، ایجاد رویه قضایی منسجم و مستندسازی آراء و تصمیمات مرتبط با حملات سایبری؛ چهارم، توجه به تجربیات کشورهای دیگر و استفاده از اسناد بین‌المللی مانند دستورالعمل تالین و گزارش‌های GGE برای تدوین چارچوب داخلی همسو با استانداردهای جهانی؛ پنجم، ارتقای آگاهی و آموزش حقوقی و فنی برای قضات، قانون‌گذاران و مدیران نهادهای امنیتی، به منظور اطمینان از اجرای صحیح و عملی قوانین و مقررات.در نهایت، تحلیل نشان داد که ترکیب حقوق داخلی، رویه قضایی، دکترین حقوقی و چارچوب‌های بین‌المللی، می‌تواند به ایجاد یک نظام حقوقی کامل و پاسخگو در مواجهه با حملات سایبری برون‌مرزی کمک کند. نتیجه‌گیری کلی این است که حقوق سایبری، به‌عنوان ابزار قانونی و عملی، نه تنها چارچوب مسئولیت دولت‌ها را روشن می‌سازد، بلکه آثار گسترده‌ای بر قانون‌گذاری، رویه قضایی و حقوق شهروندان دارد و می‌تواند پایه‌ای برای توسعه سیاست‌های امنیت ملی و تعاملات بین‌المللی در فضای دیجیتال فراهم کند.

بنابراین، پژوهش حاضر با ارائه تحلیل جامع و انتقادی، جایگاه حقوق سایبری را در تبیین مسئولیت دولت‌ها به روشنی نشان می‌دهد و مسیر لازم برای قانون‌گذاران، محاکم و پژوهشگران آینده جهت تقویت چارچوب‌های حقوقی و عملی مقابله با تهدیدات سایبری برون‌مرزی را ترسیم می‌کند. این مطالعه می‌تواند به عنوان مرجعی برای تدوین سیاست‌ها و راهکارهای حقوقی کاربردی و همسو با استانداردهای بین‌المللی مورد استفاده قرار گیرد و سهم قابل توجهی در توسعه نظری و عملی حقوق سایبری در ایران داشته باشد.

منابع

۱.منابع فارسی

کتاب‌ها

جعفری، افشین. (۱۳۹۷). حقوق فضای سایبر: اصول و چالش‌ها. تهران: دانشگاه تهران.

موسوی، سید نعمت‌الله. (۱۳۹۵). حقوق جزای رایانه‌ای: تحلیل مقررات و رویه قضائی. تهران: انتشارات میزان.

مقالات

دلخون‌اصل، رامین، گلدوزیان، ایرج، و کلانتری، کیومرث. (۱۳۹۸). نقش پلیس در جمع‌آوری ادله الکترونیکی در فضای مجازی در نظام حقوقی ایران، فرانسه و کنوانسیون جرایم سایبری. پژوهش‌های اطلاعاتی و جنایی، ۱۴(۲)، صص ۷۵–۹۸.

صفری، فاطمه، و زمان‌آبادی، ام‌البنین. (۱۴۰۴). چالش‌های کیفری ناشی از هوش مصنوعی در ارتکاب جرایم سایبری. مطالعات راهبردی علوم انسانی و اسلامی، ۷۵، صص ۷۱–۹۵.

صبح‌خیز، رضا. (۱۳۹۴). چالش‌های حقوقی جرایم سایبری در نظام حقوق بین‌الملل و نظام حقوقی ایران. پژوهش‌های اطلاعاتی و جنایی، ۱۰(۳)، صص ۱۱۷–۱۳۷.

اسماعیل‌زاده مولاباشی، پ.، و عبدالهی، م. (۱۳۹۶). حملات سایبری و اصول حقوق بین‌الملل بشردوستانه. فصلنامه مطالعات حقوق عمومی دانشگاه تهران، ۱۳(۲)، صص ۵۳۷–۵۵۹.

رحمانی، ر. (۱۴۰۰). مسئولیت بین‌المللی دولت‌ها و مسئله انتساب حملات سایبری. سازمان‌های بین‌المللی، ۵(۱۴)، صص ۶۵–۷۵.

رحمتی، ر. (۱۴۰۱). مسئولیت بین‌المللی دولت‌ها و مسئله انتساب حملات سایبری. سازمان‌های بین‌المللی، ۵(۱۴)، صص ۶۵–۷۵.

پایان‌نامه‌ها

رضوی‌فرد، بهزاد، و موسوی، سید نعمت‌الله. (۱۳۹۵). مسئولیت کیفری در فضای سایبر در حقوق ایران. پایان‌نامه دکتری، دانشگاه علامه طباطبائی.

شفیعیان، علیرضا. (۱۴۰۳). حق دسترسی به اطلاعات در فضای سایبری در حقوق ایران. پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران.

اسناد قانونی

قانون اساسی جمهوری اسلامی ایران، اصول ۷۷ و ۱۲۵. تهران: مجلس شورای اسلامی. https://www.constitution.ir/

قانون جرایم رایانه‌ای جمهوری اسلامی ایران، مصوب ۱۳۸۸. تهران: مرکز پژوهش‌های مجلس. https://rc.majlis.ir/fa/law/show/135717

آیین‌نامه امنیت فضای تولید و تبادل اطلاعات (سیاست‌نامه امنیتی دولت)، مصوب ۱۳۹۳. https://dotcomnews.ir

قوانین-و-مقررات-جدید-امنیت-سایبری-در-حقوق-ایران (https://dotcomnews.ir

۲.منابع انگلیسی

Books

Kelsen, H. (1967). Principles of international law(2nd ed., p. 120). New York: Holt, Rinehart and Winston.

Kuner, C. (2013). Transborder data flows and data privacy law(p. 27). Oxford: Oxford University Press.

Schmitt, M. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations(pp. 63–70). Cambridge: Cambridge University Press.

Shaw, M. (2017). International law(8th ed., pp. 52–55). Cambridge: Cambridge University Press.

Article

Banks, W. (2020). Cyber attribution and state responsibility. International Law Studies, 96, 45–60.

Schmitt, M. (2013). Computer network operations and international law. Harvard National Security Journal, 4(1), 15–40.

Sheraz, M. M. (2021). The state responsibility for the actions of non-state actors in cyber space based operations. PalArch’s Journal of Archaeology of Egypt / Egyptology, 18(10), 1229–1238.

Saaishri, R., & Ravi, S. (2023). State responsibility on cyber attacks: Legal framework and its implications. IJLMH, 6(6), 2418–2426.

Documents and Websites

International Law Commission (ILC). (2001). Articles on responsibility of states for internationally wrongful acts(pp. 35, 64). [https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf](https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf(

Tallinn Manual 2.0. (2017). Tallinn manual on the international law applicable to cyber operations. [https://ccdcoe.org/tallinn-manual-2-0/](https://ccdcoe.org/tallinn-manual-2-0(/

United Nations. (2015). Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (GGE). [https://www.un.org/disarmament/topics/informationsecurity/](https://www.un.org/disarmament/topics/informationsecurity(/