حاکمیت دولت‌ها در فضای سایبر و اصل عدم مداخله: چالش‌های حقوق بین‌الملل در مواجهه با عملیات سایبری فرامرزی

فهیمه حشمت (نویسنده مسئول)
دانشجوی دکتری حقوق بین الملل، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.
F_Heshmat@Sbu.ac.ir
محمد حسین رمضانی قوام آبادی
دانشیار، گروه حقوق بین‌الملل، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.
ramazanighavam@yahoo.com

چکیده

گسترش فناوری‌های اطلاعاتی و ارتباطی و افزایش وابستگی دولت‌ها به زیرساخت‌های دیجیتال، فضای سایبر را به یکی از مهم‌ترین حوزه‌های امنیت ملی، ثبات اقتصادی و حاکمیت سیاسی تبدیل کرده است. با این حال، ماهیت فرامرزی، غیرمتمرکز و بدون مرز فضای سایبر، چالش‌های اساسی برای اصول سنتی حقوق بین‌الملل، به‌ویژه حاکمیت دولت‌ها و اصل عدم مداخله ایجاد کرده است. بر این اساس، سؤال اصلی پژوهش آن است که چارچوب‌های حقوق بین‌الملل تا چه اندازه توانایی تنظیم رفتار دولت‌ها در عملیات سایبری فرامرزی را دارند و این عملیات‌ها چه چالش‌هایی را برای اصول حاکمیت و عدم مداخله ایجاد کرده‌اند؟ در پاسخ به این سؤال، فرضیه پژوهش بر این مبنا استوار است که اگرچه حقوق بین‌الملل موجود چارچوبی بنیادین برای تنظیم رفتار دولت‌ها در فضای سایبر فراهم می‌کند، اما ماهیت پیچیده و فرامرزی عملیات سایبری موجب شده است که این قواعد با محدودیت‌های اجرایی، ابهام مفهومی و خلأهای حقوقی مواجه شوند و در نتیجه، نیاز به توسعه تدریجی قواعد حقوق بین‌الملل سایبری بیش از پیش احساس شود. این پژوهش با روش تحلیل دکترینال حقوقی و رویکرد تطبیقی، اسناد بین‌المللی، از جمله منشور سازمان ملل متحد و دستورالعمل تالین ۲٫۰ را بررسی می‌کند. یافته‌های پژوهش نشان می‌دهد که قواعد و اصول بنیادین حقوق بین‌الملل مانند حاکمیت دولت‌ها و اصل عدم مداخله در فضای سایبر کارآمدی محدودتری داشته باشند. علاوه بر این، اختلاف دیدگاه دولت‌ها درباره آستانه نقض حاکمیت و مداخله سایبری، موجب پراکندگی در کاربرد قواعد حقوقی شده و خطر تشدید تنش‌های سایبری را افزایش داده است.

واژگان کلیدی: حاکمیت سایبری، اصل عدم مداخله، عملیات سایبری فرامرزی، چالش‌های حقوق بین‌الملل، دستورالعمل تالین ۲٫۰.

۱- مقدمه

تحولات فناورانه در دهه‌های اخیر، به‌ویژه گسترش فناوری‌های اطلاعاتی و ارتباطی، موجب شکل‌گیری فضای جدیدی در روابط بین‌الملل تحت عنوان فضای سایبر شده است. انقلاب دیجیتال آغازگر عصر اطلاعات بوده و قدرت سیاسی، اقتصادی و نظامی را بیش از پیش به توانایی مدیریت داده‌ها و زیرساخت‌های دیجیتال وابسته ساخته است. در نتیجه، تهدیدات سایبری به یکی از نگرانی‌های عمده جامعه بین‌المللی تبدیل شده و فضای سایبر به عرصه‌ای مهم برای رقابت و تعامل دولت‌ها بدل گردیده است. در چنین شرایطی، عملیات سایبری از حاشیه امنیت بین‌المللی به هسته اصلی سیاست‌ورزی دولت‌ها منتقل شده و علاوه بر جاسوسی، به ابزاری برای نفوذ، اخلال و ارسال پیام‌های راهبردی در شرایط صلح و بحران تبدیل شده است. این تحول را می‌توان در چارچوب روند تاریخی حقوق بین‌الملل نیز تحلیل کرد؛ به‌گونه‌ای که همانند دوره‌های گذشته، فناوری‌های نوین موجب طرح مسائل امنیتی جدید و ضرورت تطبیق قواعد حقوق بین‌الملل شده‌اند. در همین راستا، بسیاری از مطالعات اولیه درباره حقوق بین‌الملل قایل اعمال در فضای سایبر، بر حملات سایبری‌ای تمرکز داشته‌اند که ممکن است مقررات مربوط به منع توسل به زور و دفاع مشروع در منشور سازمان ملل متحد را نقض کنند. در دوره‌های اولیه شکل‌گیری فضای سایبر، دیدگاه‌های سایبرخوش‌بینانه بر این باور بودند که این فضا فراتر از قلمرو حاکمیت دولت‌ها قرار دارد؛ با این حال، افزایش تهدیدات سایبری و پیامدهای امنیتی ناشی از آن، موجب تغییر این برداشت شد، به‌گونه‌ای که امروزه قابلیت اعمال اصول و قواعد حقوق بین‌الملل در فضای سایبر به یک اجماع نسبی تبدیل شده است. در همین چارچوب، مجمع عمومی سازمان ملل متحد از سال ۱۹۹۸ قطعنامه‌هایی درباره امنیت اطلاعات تصویب کرده و تشکیل گروه کارشناسان دولتی و گروه کاری با عضویت باز[1] نیز نشان‌دهنده تلاش جامعه بین‌المللی برای تدوین قواعد و هنجارهای رفتاری در فضای سایبر است (Guerriero et al., 2024: 1 and 4).

با این حال، ویژگی‌های خاص فضای سایبر، از جمله فرامرزی بودن، ناشناس بودن کاربران و عدم وابستگی به مرزهای جغرافیایی، مفاهیم سنتی حقوق بین‌الملل را با چالش‌های جدی مواجه کرده است. افزایش عملیات سایبری فرامرزی، مانند حملات به زیرساخت‌های حیاتی، جاسوسی سایبری و مداخله در فرآیندهای سیاسی، بدون عبور فیزیکی از مرزها انجام می‌شود و همین امر موجب ابهام در مفهوم حاکمیت دولت‌ها شده است(Schmitt, 2017: 81). این وضعیت، از یک سو مسئولیت دولت‌ها برای حفاظت از فضای سایبر را افزایش داده و از سوی دیگر، کنترل کامل این فضا را دشوار ساخته است. علاوه بر این، عملیات سایبری در محیطی همراه با ابهام فنی، پراکندگی صلاحیتی و درهم‌تنیدگی حوزه‌های نظامی و غیرنظامی انجام می‌شود. این ویژگی‌ها موجب شده است که کاربرد اصول سنتی حقوق بین‌الملل، به‌ویژه حاکمیت و عدم مداخله، با پیچیدگی بیشتری مواجه شود. همچنین، مرز میان مداخله و عدم مداخله در فضای سایبر به‌وضوح مشخص نیست و اقداماتی مانند انتشار اطلاعات نادرست[2]، مداخله در انتخابات یا حملات سایبری به زیرساخت‌های حیاتی می‌تواند به‌عنوان نوعی مداخله تلقی شود، در حالی که تعیین عامل این حملات با دشواری‌های فنی و حقوقی همراه است.

بر این اساس، افزایش عملیات سایبری فرامرزی و ویژگی‌های خاص فضای سایبر، ضرورت بازنگری در قواعد حقوق بین‌الملل را برجسته ساخته است. در چنین شرایطی، بررسی چالش‌های حاکمیت دولت‌ها در فضای سایبر و تحلیل وضعیت اصل عدم مداخله در مواجهه با عملیات سایبری فرامرزی اهمیت ویژه‌ای یافته است. ساختار مقاله حاضر به شرح زیر سازماندهی شده است: در بخش اول، چارچوب نظری پژوهش ارائه می‌شود که بر سه رویکرد اصلی نظریه حاکمیت در حقوق بین‌الملل، نظریه مسئولیت بین‌المللی دولت‌ها و نظریه حکمرانی جهانی فضای سایبر استوار است. در بخش دوم، چارچوب‌های حقوقی حاکم بر رفتار دولت‌ها در فضای سایبر بررسی می‌شود. در اینجا، کاربرد منشور سازمان ملل متحد و به ویژه ماده ۲(۴) درباره منع توسل به زور، همچنین دستورالعمل تالین ۲،۰ به عنوان مهم‌ترین منبع تفسیری تحلیل می‌گردد. در بخش سوم، اصل عدم مداخله در فضای سایبر مورد کنکاش قرار می‌گیرد. در بخش چهارم، عملیات سایبری فرامرزی و نسبت آن با نقض حاکمیت دولت‌ها واکاوی می‌گردد. در بخش پنجم، سه چالش اصلی حقوق بین‌الملل در مواجهه با عملیات سایبری فرامرزی تبیین می‌گردد: مشکل انتساب و مسئولیت دولت‌ها، چالش صلاحیت قضایی، و خلأهای حقوقی همراه با نبود اجماع بین‌المللی. در

---

[1]. Establishment of the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG)

[2]. Dissemination of misinformation

پایان، نتیجه‌گیری مقاله به جمع‌بندی یافته‌ها، ارائه تحلیل نهایی و پیشنهادهایی برای توسعه تدریجی حقوق بین‌الملل سایبری اختصاص یافته است.

۲- چارچوب نظری پژوهش

تحلیل حقوقی عملیات سایبری فرامرزی مستلزم بهره‌گیری از چارچوب نظری چندبعدی است که بتواند ابعاد حقوقی، سیاسی و امنیتی این پدیده را به صورت هم‌زمان بررسی کند. در این پژوهش، چارچوب نظری بر سه رویکرد اصلی استوار است: نظریه حاکمیت در حقوق بین‌الملل، نظریه مسئولیت دولت‌ها و نظریه حکمرانی جهانی فضای سایبر. این سه رویکرد نظری امکان تحلیل جامع چالش‌های پیش‌روی حاکمیت دولت‌ها در مواجهه با عملیات سایبری فرامرزی را فراهم می‌سازند.

۲-۱- نظریه حاکمیت در حقوق بین‌الملل و تحول آن در فضای سایبر

حاکمیت دولت یکی از بنیادی‌ترین مفاهیم حقوق بین‌الملل محسوب می‌شود و بسیاری از قواعد اساسی این نظام حقوقی بر آن استوار است. از منظر حقوق بین‌الملل، حاکمیت به صلاحیت حقوقی دولت‌ها برای اعمال اقتدار در قلمرو سرزمینی خود و همچنین تعامل برابر با سایر دولت‌ها در عرصه بین‌المللی اشاره دارد. به همین دلیل، حاکمیت به عنوان «اصل بنیادین و ساختاری حقوق بین‌الملل» شناخته می‌شود (Crawford, 2012: 447).

اسناد بنیادین حقوق بین‌الملل نیز بر اهمیت اصل حاکمیت تأکید کرده‌اند. بند ۱ ماده ۲ منشور سازمان ملل متحد اصل برابری حاکمیتی دولت‌ها را مورد تأکید قرار داده است (مجتهدی و همکاران،۱۴۰۲: ۵۴). همچنین، اعلامیه روابط دوستانه ۱۹۷۰ مجمع عمومی سازمان ملل متحد تصریح می‌کند که هر دولت دارای حقوق ناشی از حاکمیت کامل است. این اسناد نشان می‌دهند که حاکمیت یکی از اصول بنیادین نظم حقوقی بین‌المللی محسوب می‌شود. رویه قضایی بین‌المللی نیز جایگاه مهم حاکمیت را تأیید کرده است. دیوان بین‌المللی دادگستری در قضیه تنگه کورفو اعلام کرد که احترام به حاکمیت سرزمینی یکی از اصول بنیادین روابط بین‌الملل است(Chircop, 2019: 3). همچنین در پرونده نیکاراگوئه علیه ایالات متحده آمریکا، دیوان تأکید کرد که اصل احترام به حاکمیت شامل قلمرو زمینی، آب‌های سرزمینی و فضای هوایی دولت‌ها می‌شود (قاسمی،۱۳۹۵: ۱۴۴). در این چارچوب، حاکمیت دارای دو بعد اساسی است: حاکمیت داخلی و حاکمیت خارجی. حاکمیت داخلی به کنترل دولت بر قلمرو سرزمینی و جمعیت خود اشاره دارد، در حالی که حاکمیت خارجی به استقلال دولت در روابط بین‌المللی مربوط می‌شود (Brownlie, 2008: 289) .

پس از جنگ جهانی دوم، مفهوم سنتی وستفالیایی حاکمیت دچار تحول شد. در گذشته، حاکمیت به معنای اقتدار مطلق دولت‌ها تلقی می‌شد، اما در حقوق بین‌الملل معاصر، حاکمیت با مجموعه‌ای از حقوق و تکالیف همراه شده است. دولت‌ها علاوه بر برخورداری از حقوق، دارای مسئولیت‌های بین‌المللی نیز هستند. در این چارچوب، حاکمیت دارای دو بعد عمودی و افقی است. بعد عمودی به سازمان‌دهی اقتدار در داخل دولت اشاره دارد، در حالی که بعد افقی به روابط برابر میان دولت‌ها مربوط می‌شود. این تحول نشان می‌دهد که حاکمیت دیگر یک مفهوم مطلق نیست، بلکه در چارچوب قواعد حقوق بین‌الملل محدود شده است (Guerriero et al., 2024: 23). در برداشت معاصر، حاکمیت شامل مجموعه‌ای از اختیارات است که عبارت‌اند از:

- اعمال اقتدار بر قلمرو سرزمینی
- کنترل تعاملات فرامرزی
- اقدام مستقل در عرصه بین‌المللی

این تحولات نشان می‌دهد که مفهوم حاکمیت از یک مفهوم صرفاً سرزمینی به مفهومی چندبعدی تبدیل شده است (Guerriero et al., 2024: 23).

در این چارچوب، مفهوم «حاکمیت سایبر[1]» مطرح شده است. حاکمیت سایبری به معنای توانایی دولت‌ها در اعمال کنترل بر زیرساخت‌های دیجیتال و جریان اطلاعات در قلمرو خود است. با این حال، تحقق این مفهوم با چالش‌های جدی مواجه است، زیرا فضای سایبر به شدت وابسته به زیرساخت‌های جهانی و بازیگران خصوصی است (DeNardis, 2014: 55) .

[1]. Cyber Governance

بر اساس دستورالعمل تالین ۲٫۰ نیز، نقض حاکمیت در فضای سایبر زمانی رخ می‌دهد که عملیات سایبری موجب دخالت در عملکرد دولت یا ایجاد اثرات قابل توجه در قلمرو یک کشور شود. بر اساس قاعده ۶۹ دستورالعمل تالین ۲٫۰، یک عملیات سایبری زمانی مصداق «توسل به زور» تلقی می‌شود که مقیاس و آثار آن با عملیات‌های غیرسایبری که در حقوق بین‌الملل به سطح توسل به زور می‌رسند، قابل مقایسه باشد (Schmitt, 2017: 320 and 330). این موضوع نشان می‌دهد که مفهوم حاکمیت در فضای سایبر در حال تحول است و نیازمند تفسیر جدیدی در چارچوب حقوق بین‌الملل است.

۲-۲- نظریه مسئولیت بین‌المللی دولت‌ها در عملیات سایبری

یکی دیگر از مبانی نظری مهم این پژوهش، نظریه مسئولیت بین‌المللی دولت‌ها[1] در حقوق بین‌الملل است. بر اساس این نظریه، دولت‌ها در صورت نقض تعهدات بین‌المللی مسئول شناخته می‌شوند و باید خسارات ناشی از اقدامات خود را جبران کنند. این اصل در مواد ۱ و ۲ پیش‌نویس مواد مسئولیت دولت‌ها برای اعمال متخلفانه بین‌المللی مصوب کمیسیون حقوق بین‌الملل مورد تصریح قرار گرفته است. همچنین، مطابق ماده ۳۱ این پیش‌نویس، دولت مسئول مکلف به جبران کامل خسارات ناشی از عمل متخلفانه بین‌المللی خود است. از این رو، در صورت انتساب عملیات سایبری به یک دولت و احراز نقض تعهدات بین‌المللی، آن دولت مسئول پیامدهای حقوقی ناشی از عمل خود بوده و ملزم به جبران خسارات وارده خواهد بود (Crawford, 2013: 45-48). در واقع، در فضای سایبر، اعمال مسئولیت بین‌المللی دولت‌ها با چالش‌های متعددی مواجه شده است. مهم‌ترین این چالش‌ها شامل مشکل انتساب، نقش بازیگران غیردولتی و دشواری اثبات خسارت است.

الف) مشکل انتساب

یکی از مهم‌ترین چالش‌های حاکمیت در فضای سایبر، مسئله انتساب حملات سایبری است. حملات سایبری می‌توانند از طریق سرورهای متعدد در کشورهای مختلف انجام شوند و همین امر تعیین مسئولیت بین‌المللی دولت‌ها را دشوار می‌کند (Rid, 2020: 117). بر اساس دستورالعمل تالین ۲٫۰، انتساب عملیات سایبری باید بر اساس قواعد عمومی مسئولیت بین‌المللی دولت‌ها انجام شود. این بدان معناست که اگر یک دولت کنترل مؤثر بر عملیات سایبری داشته باشد، مسئول آن شناخته می‌شود.(Schmitt, 2017: 95)

ب) نقش بازیگران غیردولتی

در فضای سایبر، بسیاری از عملیات توسط گروه‌های هکری، شرکت‌های خصوصی یا سازمان‌های غیردولتی انجام می‌شود. این مسئله مسئولیت بین‌المللی دولت‌ها را پیچیده‌تر کرده است. با این حال، حقوق بین‌الملل دولت‌ها را موظف می‌کند که از قلمرو خود برای انجام عملیات سایبری علیه سایر دولت‌ها جلوگیری کنند(Koh, 2012: 4) . دستورالعمل تالین ۲٫۰ این موضوع را در قواعد مربوط به انتساب رفتار دولت‌ها مورد بررسی قرار داده است. بر اساس قواعد ۱۴ و ۱۷، چنانچه اشخاص یا گروه‌های غیردولتی تحت هدایت، کنترل یا دستور یک دولت عمل کنند، یا دولت رفتار آنان را به‌عنوان رفتار خود بپذیرد، اقدامات مزبور به دولت منتسب شده و مسئولیت بین‌المللی آن دولت محقق می‌شود. افزون بر این، مطابق قاعده ۶ دستورالعمل تالین ۲٫۰، دولت‌ها موظف‌اند با اعمال مراقبت مقتضی از استفاده قلمرو، زیرساخت‌ها یا سامانه‌های سایبری تحت صلاحیت خود برای انجام عملیات سایبری زیان‌بار علیه سایر دولت‌ها جلوگیری کنند. در نتیجه، حتی در مواردی که عملیات سایبری مستقیماً توسط بازیگران غیردولتی انجام می‌شود، دولت‌ها ممکن است به دلیل انتساب رفتار یا قصور در انجام تعهد مراقبت مقتضی، مسئول شناخته شوند (Schmitt, 2017: 14-16).

ج) دشواری اثبات خسارت

یکی دیگر از چالش‌های عملیات سایبری، دشواری اثبات خسارت است. بسیاری از حملات سایبری موجب خسارات غیرملموس مانند اختلال در خدمات یا سرقت اطلاعات می‌شود که اثبات آن ها در چارچوب حقوق بین‌الملل دشوار است (Dinstein, 2020: 112).

۲-۳- نظریه حکمرانی جهانی فضای سایبر

[1]. The theory of international responsibility of states

نظریه حکمرانی جهانی[1] فضای سایبر یکی دیگر از چارچوب‌های نظری مهم در این پژوهش محسوب می‌شود. این نظریه بر این فرض استوار است که فضای سایبر نیازمند همکاری بین‌المللی و تنظیم قواعد مشترک است. بر اساس این دیدگاه، هیچ دولتی نمی‌تواند ادعای حاکمیت کامل بر فضای سایبر داشته باشد. دستور العمل تالین نیز تأکید می‌کند که هیچ دولتی نمی‌تواند بر کل فضای سایبر حاکمیت داشته باشد (Tanzi et al., 2021: 5). بر اساس این نظریه، حکمرانی فضای سایبر دارای ماهیت چندبازیگری است و شامل دولت‌ها، سازمان‌های بین‌المللی و بازیگران خصوصی می‌شود.(DeNardis, 2014: 72)

الف) نقش دولت‌ها

برخی پژوهشگران معتقدند که دولت‌ها همچنان می‌توانند بر زیرساخت‌ها، کاربران و داده‌های فضای سایبر اعمال حاکمیت کنند. از این منظر، فضای سایبر کاملاً خارج از حاکمیت دولت‌ها نیست (Guerriero et al., 2024: 25). دولت‌ها همچنان بازیگران اصلی در تنظیم فضای سایبری محسوب می‌شوند. بسیاری از کشورها در سال‌های اخیر استراتژی‌های ملی امنیت سایبری تدوین کرده‌اند که نشان‌دهنده اهمیت این حوزه است(Tsagourias & Buchan, 2021: 41) . برای مثال، ایالات متحده «استراتژی ملی امنیت سایبری ۲۰۲۳» را با تأکید بر دفاع از زیرساخت‌های حیاتی، مسئولیت‌پذیری بازیگران فضای سایبری و همکاری بین‌المللی منتشر کرد(White House, 2023) . اتحادیه اروپا نیز از طریق «استراتژی امنیت سایبری اتحادیه اروپا برای دهه دیجیتال» در سال ۲۰۲۰ بر تقویت حاکمیت سایبری، امنیت شبکه‌ها و افزایش تاب‌آوری سایبری تأکید کرده است(European Commission, 2020) . همچنین، بریتانیا در «استراتژی ملی سایبری ۲۰۲۲» حفاظت از منافع ملی در فضای سایبری و توسعه توانمندی‌های دفاع سایبری را از اولویت‌های اصلی خود معرفی کرده است (UK Government, 2022). این اسناد نشان می‌دهند که دولت‌ها فضای سایبری را بخشی از قلمرو حاکمیتی و امنیت ملی خود تلقی کرده و نقش فعالی در تنظیم و مدیریت آن ایفا می‌کنند.

ب) نقش سازمان‌های بین‌المللی

سازمان ملل متحد نقش مهمی در توسعه قواعد سایبری ایفا کرده است. گروه کارشناسان دولتی سازمان ملل متحد در گزارش‌های خود تأکید کرده است که حقوق بین‌الملل موجود در فضای سایبر نیز قابل اجرا است.(UN GGE, 2015: 12)

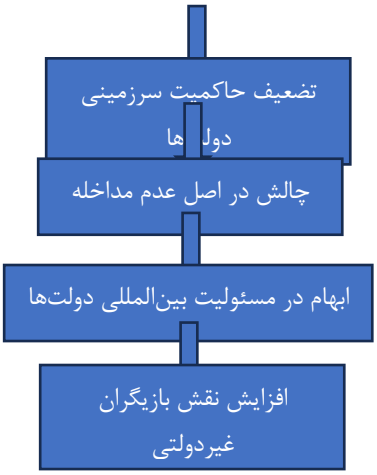
ج) نقش بازیگران غیردولتی

شرکت‌های فناوری مانند ارائه‌دهندگان خدمات اینترنتی[2] و شرکت‌های نرم‌افزاری نقش مهمی در مدیریت فضای سایبر دارند. این مسئله موجب شده است که حکمرانی فضای سایبر ماهیتی چندسطحی پیدا کند.(DeNardis, 2014: 89)

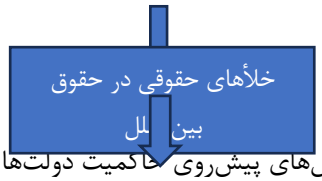
در مجموع، چارچوب نظری پژوهش بر ترکیب سه رویکرد نظری حاکمیت، مسئولیت بین‌المللی دولت‌ها و حکمرانی جهانی فضای سایبر استوار است. این چارچوب امکان تحلیل جامع چالش‌های حقوق بین‌الملل در مواجهه با عملیات سایبری فرامرزی را فراهم می‌سازد.

مدل مفهومی پژوهش

عملیات سایبری فرامرزی



[1]. Global Governance Theory
[2]. Internet service providers



در این مدل مفهومی، عملیات سایبری فرامرزی به‌عنوان متغیر مستقل در نظر گرفته شده است که از طریق متغیرهای میانجی شامل اصل عدم مداخله، مسئولیت بین‌المللی دولت‌ها، خلأهای حقوقی و نقش بازیگران غیردولتی، بر چالش‌های حاکمیت دولت‌ها تأثیر می‌گذارد. این مدل نشان می‌دهد که عملیات سایبری فرامرزی موجب تحول در مفهوم سنتی حاکمیت شده و حقوق بین‌الملل را با چالش‌های جدیدی مواجه ساخته است.

۳- چارچوب‌های حقوقی حاکم بر رفتار دولت‌ها در فضای سایبر

با گسترش فضای سایبر و افزایش عملیات‌های سایبری میان دولت‌ها، یکی از مهم‌ترین پرسش‌های حقوق بین‌الملل معاصر این است که چه چارچوب‌های حقوقی بر رفتار دولت‌ها در فضای سایبر حاکم است. در این میان، منشور سازمان ملل متحد همچنان مهم‌ترین سند حقوقی برای تنظیم استفاده از زور در روابط بین‌الملل محسوب می‌شود. اگرچه این منشور در سال ۱۹۴۵ و پیش از ظهور فناوری‌های دیجیتال تدوین شده است، اما اصول بنیادین آن همچنان مبنای تحلیل حقوقی عملیات‌های سایبری قرار می‌گیرد، به‌ویژه در مواردی که این عملیات‌ها می‌توانند خسارت‌های فیزیکی یا اختلالات گسترده ایجاد کنند (Gul et al., 2025: 124).

بر اساس ماده ۲(۴) منشور سازمان ملل متحد، دولت‌ها از تهدید یا استفاده از زور علیه تمامیت ارضی یا استقلال سیاسی سایر دولت‌ها منع شده‌اند. این اصل یکی از مهم‌ترین قواعد آمره حقوق بین‌الملل محسوب می‌شود و تنها دو استثنای محدود دارد: نخست، حق دفاع مشروع بر اساس ماده ۵۱ منشور، و دوم، اقداماتی که شورای امنیت سازمان ملل متحد در چارچوب فصل هفتم منشور مجاز اعلام می‌کند. این چارچوب حقوقی، اساس تحلیل مشروعیت عملیات‌های سایبری در نظام حقوق بین‌الملل معاصر را تشکیل می‌دهد. با این حال، اعمال این قواعد در فضای سایبر با چالش‌های متعددی همراه است. یکی از مهم‌ترین پرسش‌ها این است که آیا عملیات‌های سایبری می‌توانند مصداق «توسل به زور» محسوب شوند یا نه. در سال‌های اخیر، نوعی اجماع نسبی میان برخی دولت‌ها[۱] در حال شکل‌گیری است که عملیات‌های سایبری که منجر به مرگ، جراحت یا تخریب فیزیکی قابل توجه شوند، می‌توانند در چارچوب ماده ۲(۴) منشور به‌عنوان توسل به زور تلقی شوند. برای مثال، حملات سایبری که موجب از کار افتادن شبکه برق، اختلال در سیستم‌های بیمارستانی یا آسیب به زیرساخت‌های حیاتی شوند، می‌توانند از نظر حقوقی در سطح استفاده از زور قرار گیرند (Gul et al., 2025: 124-125).

در این زمینه، دستور العمل تالین ۲,۰ درباره حقوق بین‌الملل قابل اعمال بر عملیات‌های سایبری، نقش مهمی در ارائه چارچوب تحلیلی ایفا کرده است. این دستورالعمل که توسط کارشناسان حقوقی و فنی تهیه شده، اگرچه الزام‌آور نیست، اما یکی از مهم‌ترین منابع تفسیری در حوزه حقوق بین‌الملل سایبری محسوب می‌شود. اهمیت این سند از آن روست که نخست، جامع‌ترین تلاش نظام‌مند برای تطبیق قواعد سنتی حقوق بین‌الملل با چالش‌های ناشی از فناوری‌های سایبری را ارائه می‌کند؛ دوم، در حوزه‌ای که هنوز فاقد معاهده جامع و اختصاصی بین‌المللی است، چارچوبی منسجم برای تفسیر اصولی همچون حاکمیت، عدم مداخله، مسئولیت بین‌المللی دولت‌ها، توسل به زور و دفاع مشروع فراهم می‌آورد؛ سوم، تحلیل‌های آن مبتنی بر اجماع نسبی گروهی از حقوقدانان و متخصصان برجسته بین‌المللی است؛ و چهارم، استدلال‌ها و قواعد مطرح‌شده در آن به‌طور گسترده در آثار دانشگاهی، گزارش‌های تخصصی و حتی مواضع رسمی برخی دولت‌ها مورد استناد قرار گرفته‌اند. از این رو، تالین ۲,۰ به‌رغم فقدان ماهیت الزام‌آور، به یکی از مهم‌ترین مراجع تفسیری برای فهم و تبیین حقوق بین‌الملل در فضای سایبری تبدیل شده است (Schmitt, 2017: 4-5; Tsagourias & Buchan, 2021: 11-12). نسخه نخست این

---

[۱]. برای مثال: ایالات متحده آمریکا، بریتانیا، هلند و فرانسه

راهنما در سال ۲۰۱۳ منتشر شد و بر مخاصمات سایبری تمرکز داشت. سپس نسخه دوم در سال ۲۰۱۷ منتشر شد که دامنه وسیع‌تری را پوشش داد و عملیات‌های سایبری زیر آستانه توسل به زور را نیز بررسی کرد (Pray, 2021: 53). پیرو این موضوع، راهنمای تالین ۳٫۰ نیز در حال تدوین است. بر اساس این راهنماها، یک عملیات سایبری زمانی می‌تواند «توسل به زور» محسوب شود که مقیاس و آثار آن با عملیات‌های نظامی سنتی قابل مقایسه باشد. در این ارزیابی، معیارهای مختلفی مورد توجه قرار می‌گیرد، از جمله:

- شدت و گستره پیامدها؛
- فوریت و مستقیم بودن اثرات؛
- ماهیت نظامی عملیات؛
- میزان نفوذ به قلمرو یک دولت دیگر.

این معیارها نشان می‌دهد که ارزیابی عملیات سایبری به‌صورت موردی انجام می‌شود و هیچ آستانه مشخص و قطعی برای تشخیص توسل به زور وجود ندارد. علاوه بر این، از آنجا که دستور العمل تالین ۲٫۰ ماهیت غیرالزام‌آور دارد، دولت‌ها همچنان در مورد تفسیر و کاربرد آن اختلاف نظر دارند (Gul et al., 2025: 124).

چالش مهم دیگر در این حوزه، تمایز میان «توسل به زور» و «حمله مسلحانه» است. این تمایز اهمیت زیادی دارد، زیرا تنها در صورت وقوع حمله مسلحانه، دولت‌ها می‌توانند به حق دفاع مشروع طبق ماده ۵۱ منشور استناد کنند. در حقوق بین‌الملل سنتی، حمله مسلحانه شدیدترین شکل استفاده از زور محسوب می‌شود، اما در فضای سایبر تعیین این آستانه دشوارتر است. برای مثال، وارد کردن بدافزار به یک تأسیسات هسته‌ای که منجر به انفجار یا خسارت گسترده شود، می‌تواند به‌عنوان حمله مسلحانه تلقی شود. در مقابل، جاسوسی سایبری یا سرقت داده‌ها در مقیاس گسترده—معمولاً به سطح حمله مسلحانه نمی‌رسد. این تمایز نشان‌دهنده پیچیدگی حقوقی عملیات‌های سایبری در چارچوب منشور سازمان ملل متحد است (Meyer, 2020; Khan et al., 2020).

علاوه بر این، برخی دولت‌ها در سال‌های اخیر عملیات‌های سایبری را در دکترین‌های دفاع ملی خود وارد کرده‌اند. این تحول نشان می‌دهد که دولت‌ها به‌طور فزاینده‌ای تهدیدهای سایبری را در چارچوب حقوق توسل به زور[1] مورد توجه قرار می‌دهند. به عبارت دیگر، فضای سایبر به‌عنوان حوزه‌ای جدید برای رقابت‌های امنیتی و حتی درگیری‌های احتمالی میان دولت‌ها مطرح شده است (Gul et al., 2025: 124). با این حال، نبود مقررات معاهده‌ای مشخص در زمینه عملیات سایبری، موجب شده است که حدود حقوقی استفاده از زور در فضای سایبر همچنان مبهم باقی بماند. همچنین، فقدان رویه قضایی الزام‌آور در این حوزه، موجب شده است که دولت‌ها تفسیرهای متفاوتی از قواعد حقوق بین‌الملل ارائه دهند. این وضعیت می‌تواند خطر سوءبرداشت، تشدید تنش‌ها و حتی درگیری‌های بین‌المللی را افزایش دهد. از سوی دیگر، عملیات‌های سایبری حتی بدون ایجاد خسارت فیزیکی نیز می‌توانند در شرایط خاص به‌عنوان توسل به زور تلقی شوند. برای مثال، حمله سایبری گسترده به سیستم مالی یک کشور یا اختلال در شبکه‌های حیاتی ارتباطی می‌تواند پیامدهای جدی اقتصادی و امنیتی داشته باشد. با این حال، هنوز اجماع روشنی در این زمینه وجود ندارد و این موضوع یکی از چالش‌های مهم حقوق بین‌الملل سایبر محسوب می‌شود (Lahmann, 2021; Khan et al., 2020).

در مجموع، منشور سازمان ملل متحد همچنان چارچوب بنیادین برای ارزیابی مشروعیت عملیات‌های سایبری فراهم می‌کند. با این حال، ویژگی‌های خاص فضای سایبر -از جمله سرعت بالا، ناشناس بودن و فقدان مرزهای جغرافیایی- موجب شده است که اعمال قواعد سنتی حقوق بین‌الملل با دشواری‌هایی همراه شود. در نتیجه، بسیاری از پژوهشگران بر ضرورت توسعه تدریجی حقوق بین‌الملل سایبری و تدوین استانداردهای جدید تأکید کرده‌اند. در نهایت، روشن شدن آستانه توسل به زور در فضای سایبر برای حفظ صلح و امنیت بین‌المللی اهمیت اساسی دارد. بدون وجود قواعد روشن و مورد توافق، خطر تشدید تنش‌های سایبری میان دولت‌ها افزایش خواهد یافت. بنابراین، توسعه حقوق بین‌الملل سایبر و ایجاد چارچوب‌های حقوقی شفاف برای تنظیم رفتار دولت‌ها در فضای سایبر، یکی از مهم‌ترین چالش‌های حقوق بین‌الملل در قرن بیست‌ویکم محسوب می‌شود

---

[1]. jus ad bellum

۴- اصل عدم مداخله در فضای سایبر

۴-۱- مفهوم سنتی اصل عدم مداخله در حقوق بین‌الملل

اصل عدم مداخله یکی از اصول بنیادین حقوق بین‌الملل است که ریشه در اصل برابری حاکمیتی دولت‌ها دارد. این اصل به‌عنوان «پیامد آشکار آزادی و استقلال ملت‌ها» شناخته می‌شود و مداخلات قهرآمیز در اموری را که دولت‌ها بر اساس حقوق بین‌الملل در انتخاب آن‌ها آزاد هستند، ممنوع می‌کند (Guerriero et al., 2024: 41). در واقع، اصل عدم مداخله تضمین‌کننده استقلال تصمیم‌گیری دولت‌ها در نظام بین‌الملل است و از تحمیل اراده دولت‌های دیگر جلوگیری می‌کند. با وجود اهمیت این اصل، منشور سازمان ملل متحد به‌طور مستقیم و صریح از واژه «مداخله» استفاده نکرده است و تنها ماده ۲(۷) منشور به این موضوع اشاره دارد. این ماده مقرر می‌کند که هیچ‌یک از مفاد منشور سازمان ملل متحد به این سازمان اجازه نمی‌دهد در اموری که اساساً در صلاحیت داخلی دولت‌ها قرار دارد مداخله کند. همچنین اعضای سازمان ملل متحد نیز ملزم نیستند چنین موضوعاتی را برای حل‌وفصل در چارچوب منشور ارائه دهند (Guerriero et al., 2024: 47). این امر نشان می‌دهد که اصل عدم مداخله از همان ابتدا با نوعی ابهام مفهومی همراه بوده است.

از منظر حقوق عرفی نیز اصل عدم مداخله به‌عنوان یک «اصل» و نه یک «قاعده دقیق» شناخته شده است. به همین دلیل، تعیین دقیق اینکه چه اقداماتی مداخله ممنوع محسوب می‌شود، همواره دشوار بوده است. به گفته آنتونیو کاسسه، زمانی که دولت‌ها درباره یک وضعیت مهم به توافق نمی‌رسند اما همچنان نیاز به راهنما وجود دارد، اصول کلی شکل می‌گیرند. بنابراین، اصل عدم مداخله نیز به‌عنوان یک اصل کلی با دامنه‌ای نسبتاً مبهم باقی مانده است. در چارچوب نظریه هوفلد، اصل عدم مداخله را می‌توان به‌صورت یک رابطه حق و تکلیف تفسیر کرد. بر این اساس، هر دولت دارای حق اداره امور داخلی خود بدون مداخله خارجی است و سایر دولت‌ها نیز دارای تکلیف خودداری از چنین مداخله‌ای هستند. این اصل در واقع از حاکمیت تصمیم‌گیری دولت‌ها در برابر اجبار دولت‌های دیگر حمایت می‌کند. بنابراین، زمانی که اجبار در موضوعی اعمال نشود که دولت هدف در آن آزادانه تصمیم می‌گیرد، آن اقدام خارج از حوزه ممنوعه اصل عدم مداخله قرار می‌گیرد (Guerriero et al., 2024: 51).

دیوان بین‌المللی دادگستری نیز در پرونده نیکاراگوئه علیه ایالات متحده آمریکا(۱۹۸۶) اصل عدم مداخله را به‌عنوان یک قاعده عرفی حقوق بین‌الملل تأیید کرد. دیوان اعلام کرد که مداخله زمانی ممنوع است که در حوزه‌هایی صورت گیرد که دولت‌ها بر اساس اصل حاکمیت حق تصمیم‌گیری آزادانه درباره آن‌ها را دارند و این مداخله ماهیت قهرآمیز داشته باشد. این حوزه‌ها شامل تصمیمات سیاسی، اقتصادی و نظامی دولت‌ها می‌شود (Shaw, 2017: 116). با این حال، اصل عدم مداخله همواره با چالش‌هایی همراه بوده است. برخی پژوهشگران معتقدند که این اصل از نظر عملی به‌خوبی اجرا نشده است و ابهام در مفهوم «اجبار» موجب محدود شدن کاربرد آن شده است. به‌طور سنتی، مداخله زمانی رخ می‌دهد که دولت مداخله‌کننده، دولت هدف را مجبور کند اقدامی را انجام دهد که در شرایط عادی انجام نمی‌داد (Cora & Mikail, 2026: 8). این ابهام موجب شده است که دولت‌ها در بسیاری از موارد به جای استناد حقوقی به اصل عدم مداخله، از ابزارهای سیاسی مانند تحریم‌ها یا واکنش‌های دیپلماتیک استفاده کنند (Nye, 2010).

علاوه بر این، برخی پژوهشگران معتقدند که اصل عدم مداخله در طیف اعمال متخلفانه بین‌المللی در موقعیتی میانی قرار دارد. در یک سوی این طیف، ممنوعیت توسل به زور قرار دارد و در سوی دیگر نقض ساده حاکمیت قرار دارد. اصل عدم مداخله میان این دو قرار می‌گیرد و از نظر شدت، نه شدیدترین تخلف محسوب می‌شود و نه کم‌اهمیت‌ترین آن (Watts, 2014: 1). این موقعیت میانی موجب شده است که تعیین آستانه نقض این اصل دشوار باشد.

۴-۲- تحول اصل عدم مداخله در فضای سایبر

گسترش گسترش فضای سایبر موجب شده است که اصل عدم مداخله به یکی از مهم‌ترین قواعد حقوق بین‌الملل در تنظیم رفتار دولت‌ها در محیط دیجیتال تبدیل شود. عملیات‌های سایبری این امکان را فراهم کرده‌اند که دولت‌ها بدون توسل به زور نظامی، بر امور داخلی سایر کشورها تأثیر بگذارند. برای مثال، مداخله در فرآیندهای انتخاباتی، انتشار اطلاعات نادرست، دستکاری داده‌ها، عملیات نفوذ در شبکه‌های اجتماعی و تضعیف نهادهای دولتی می‌تواند در صورت برخورداری از ماهیت

قهرآمیز، نقض اصل عدم مداخله تلقی شود (Gul et al., 2025: 125). در حقوق بین‌الملل، اصل عدم مداخله به‌عنوان «حق دولت‌ها برای اداره امور داخلی خود بدون مداخله خارجی» و در مقابل «تعهد سایر دولت‌ها به خودداری از مداخله اجبارآمیز» شناخته می‌شود. بر این اساس، آنچه «دخالت» را از «مداخله ممنوع» متمایز می‌کند، وجود دو عنصر اساسی است: نخست، دخالت در حوزه‌هایی که دولت‌ها بر اساس حقوق بین‌الملل در انتخاب آن‌ها آزاد هستند و دوم، وجود عنصر اجبار(Guerriero et al., 2024: 65). دیوان بین‌المللی دادگستری نیز در قضیه نیکاراگوئه بر همین دو معیار تأکید کرده و مداخله غیرقانونی را مستلزم دخالت در حوزه صلاحیت انحصاری دولت و برخورداری از ماهیت اجبارآمیز دانسته است (Moulin, 2020: 1). این معیارها امروزه مبنای اصلی ارزیابی عملیات‌های سایبری از منظر اصل عدم مداخله به شمار می‌روند.

تحولات فناوری اطلاعات و ارتباطات، چارچوب سنتی این اصل را با چالش‌های جدیدی مواجه ساخته است. دولت‌ها اکنون قادرند از طریق ابزارهای دیجیتال نفوذ خود را فراتر از مرزهای جغرافیایی اعمال کرده و بر سیاست داخلی، اقتصادی و امنیتی سایر کشورها تأثیر بگذارند. در نتیجه، برای اعمال نفوذ مؤثر بر حوزه صلاحیت یک دولت دیگر، دیگر لزوماً نیازی به ابزارهای سنتی اجبار وجود ندارد (Guerriero et al., 2024: 64). از همین رو، بسیاری از حقوقدانان و دولت‌ها بر این باورند که قاعده عرفی ممنوعیت مداخله به فعالیت‌های سایبری نیز تسری می‌یابد، هرچند حدود و ثغور دقیق آن هنوز به‌طور کامل مشخص نشده است (Kilovaty, 2021: 97). در سال‌های اخیر، ظهور عملیات‌های سایبری تحت حمایت دولت‌ها، به‌ویژه کارزارهای سایبری با شدت پایین که آثار تخریبی فیزیکی ندارند، اهمیت این اصل را دوچندان کرده است. این عملیات‌ها اگرچه معمولاً پایین‌تر از آستانه توسل به زور قرار می‌گیرند، اما می‌توانند تأثیرات عمیقی بر حاکمیت و استقلال سیاسی دولت‌ها بر جای بگذارند. با این حال، یکی از مهم‌ترین چالش‌های موجود، نبود اجماع درباره مفهوم «اجبار» در فضای سایبر است. دولت‌ها هنوز در خصوص اینکه چه نوع عملیات سایبری می‌تواند مصداق اجبار محسوب شود، توافق روشنی ندارند و همین امر موجب تداوم ابهام در تعیین دامنه اصل عدم مداخله در فضای سایبری شده است (Watts, 2014: 1).

از منظر حقوقی، اسناد بین‌المللی متعددی امکان اعمال اصل عدم مداخله در فضای سایبر را فراهم می‌کنند. منشور سازمان کشورهای آمریکایی، قطعنامه‌های ۲۱۳۱، ۲۶۲۵، ۳۲۸۱ و ۳۶/۱۰۳ مجمع عمومی سازمان ملل متحد و همچنین سند نهایی هلسینکی، تفاسیر گسترده‌ای از اصل عدم مداخله ارائه کرده‌اند که قابلیت انطباق با محیط سایبری را دارند. در تمامی این اسناد، دو عنصر بنیادین مداخله ممنوع، یعنی دخالت در امور صلاحیتی دولت‌ها و وجود فرآیند اجبارآمیز، همچنان معیار اصلی تشخیص محسوب می‌شوند (Guerriero et al., 2024: 65). در همین راستا، دستورالعمل تالین ۲٫۰ تلاش کرده است دامنه کاربرد اصل عدم مداخله در فضای سایبر را روشن‌تر سازد. مطابق این سند، عملیات سایبری زمانی مداخله غیرقانونی محسوب می‌شود که در کارکردهای ذاتاً حاکمیتی یک دولت، از جمله برگزاری انتخابات، حفظ نظم عمومی یا تدوین سیاست خارجی، به‌صورت قهرآمیز مداخله کند (Schmitt, 2017: 312). علاوه بر این، ویژگی‌های خاص فضای سایبری، از جمله ناشناس بودن عاملان حملات و امکان انکارپذیری عملیات‌ها، اجرای اصل عدم مداخله را با دشواری‌های جدی مواجه کرده است. در بسیاری از موارد، انتساب حملات سایبری به یک دولت مشخص و اثبات مسئولیت بین‌المللی آن بسیار پیچیده است و همین مسئله از کارآمدی بازدارنده این اصل می‌کاهد (Tsagourias, 2021). به طوری که، دیجیتالی شدن موجب افزایش استناد دولت‌ها به اصل عدم مداخله شده است. در گذشته، این اصل بیشتر توسط دولت‌های ضعیف‌تر مورد استفاده قرار می‌گرفت، اما امروزه دولت‌های غربی نیز به آن استناد می‌کنند (Willmer, 2023: 509).

بحث‌های گروه کارشناسان دولتی سازمان ملل متحد[1] و گروه کاری باز[2] نیز نشان می‌دهد که دولت‌ها درباره نحوه اعمال این اصل در فضای سایبر اختلاف نظر دارند. برخی دولت‌ها تفسیر محدودتری ارائه می‌دهند، در حالی که برخی دیگر تفسیر گسترده‌تری دارند (Willmer, 2023: 512). برای مثال، ایران در بیانیه ۲۰۲۰ خود مفهوم گسترده‌ای از مداخله ارائه داده و حتی مهندسی افکار عمومی در آستانه انتخابات را نیز مصداق مداخله دانسته است (Ossof, 2021: 315). همچنین، کشورهایی مانند فرانسه و هلند معتقدند، حتی عملیات‌های سایبری فاقد خسارت فیزیکی نیز ممکن است ناقض اصل عدم مداخله باشند،

---

1. GGE
2. OEWG

در حالی که برخی دولت‌ها رویکرد محدودتری اتخاذ کرده‌اند (Bechara & Schuch, 2021). با وجود این چالش‌ها، طی یک دهه گذشته اجماع فزاینده‌ای در سطح بین‌المللی درباره قابلیت اعمال اصل عدم مداخله در فضای سایبر شکل گرفته است. گروه کارشناسان دولتی سازمان ملل متحد در گزارش سال ۲۰۱۳ اعلام کرد که حقوق بین‌الملل، از جمله منشور سازمان ملل متحد، در فضای سایبری نیز قابل اعمال است. این موضع در گزارش ۲۰۱۵ تقویت شد و بر اعتبار اصول حاکمیت و عدم مداخله در محیط سایبری تأکید گردید. گزارش‌های بعدی، از جمله گزارش سال ۲۰۲۱ و همچنین اسناد گروه کاری با عضویت باز، همین رویکرد را تکرار کرده و بر ضرورت رعایت اصل عدم مداخله در فضای سایبر تأکید نموده‌اند (Sardu, 2025: 7). بنابراین، اگرچه اصل عدم مداخله همچنان یکی از مهم‌ترین ابزارهای حقوقی برای مقابله با مداخلات سایبری محسوب می‌شود، اما تحولات فناورانه، ابهام در مفهوم اجبار، دشواری انتساب حملات و اختلاف دیدگاه دولت‌ها درباره حدود این اصل، موجب شده است که تفسیر و اجرای آن در فضای سایبری همچنان با چالش‌های قابل توجهی روبه‌رو باشد.

۵- عملیات سایبری فرامرزی و نقض حاکمیت دولت‌ها

فضای سایبر به‌عنوان حوزه‌ای جدید، چالش‌های جدی برای اعمال حاکمیت سرزمینی ایجاد کرده است. داده‌ها می‌توانند در چندین کشور ذخیره شوند و عملیات سایبری نیز می‌تواند از چندین قلمرو مختلف انجام شود. این ویژگی‌ها موجب شده است که تعیین قلمرو حقوقی عملیات سایبری دشوار شود (Pray, 2021: 43). ارزیابی وزارت دفاع ایالات متحده آمریکا در سال ۱۹۹۹ نیز بر این پیچیدگی تأکید کرده بود و بیان داشت که نفوذ الکترونیکی غیرمجاز ممکن است در برخی موارد نقض حاکمیت تلقی شود، اما این مسئله به شرایط خاص هر مورد بستگی دارد. این دیدگاه نشان می‌دهد که اعمال اصل حاکمیت در فضای سایبری به شدت وابسته به زمینه و شرایط عملیاتی است (Pray, 2021: 52).

۵-۱- تحول تاریخی رویکرد حقوق بین‌الملل به عملیات سایبری

در اواخر دهه ۱۹۹۰، جامعه حقوق بین‌الملل با شکل جدیدی از منازعه مواجه شد که در آن زمان «حمله به شبکه‌های رایانه‌ای» یا «عملیات اطلاعاتی» نامیده می‌شد. این تحول موجب شد که نهادهای نظامی و حقوقی، به‌ویژه وزارت دفاع ایالات متحده آمریکا، بررسی ابعاد حقوقی عملیات سایبری را آغاز کنند. در سال ۱۹۹۹، دفتر مشاور حقوقی وزارت دفاع ایالات متحده آمریکا گزارشی با عنوان «ارزیابی مسائل حقوق بین‌الملل در عملیات اطلاعاتی[1]» منتشر کرد که در آن، قابلیت اعمال قواعد حقوق توسل به زور و حقوق در زمان جنگ، حقوق فضا، حقوق مخابرات، حقوق جاسوسی و سایر رژیم‌های حقوقی بر عملیات سایبری مورد بررسی قرار گرفت. این گزارش بر این فرض استوار بود که حقوق بین‌الملل موجود در فضای سایبر نیز قابل اعمال است؛ دیدگاهی که تا سال‌ها رویکرد اصلی ایالات متحده آمریکا باقی ماند (Schmitt & Vihul, 2017: 1639).

با این حال، آنچه در سال‌های بعد تغییر کرد، موضع ایالات متحده آمریکا درباره نقش اصل حاکمیت در فضای سایبر بود. در ارزیابی سال ۱۹۹۹، فرض بر این بود که نقض حاکمیت یک قاعده ماهوی حقوق بین‌الملل است و چالش اصلی تنها تعیین آستانه نقض آن در فضای سایبر بود (Schmitt & Vihul, 2017: 1640). اما در سال ۲۰۱۷، وزارت دفاع ایالات متحده آمریکا موضع متفاوتی اتخاذ کرد و اعلام نمود که بسیاری از عملیات‌های سایبری با شدت پایین که به سطح توسل به زور یا مداخله قهرآمیز نمی‌رسند، ممکن است تحت حقوق بین‌الملل موجود ممنوع نباشند. این دیدگاه عملاً نشان‌دهنده برداشت محدودتر از نقش اصل حاکمیت در فضای سایبر بود (Sean & Theodore, 2018: 828).

در مقابل این دیدگاه محدودکننده، نهادهای بین‌المللی تلاش کردند بر قابلیت اعمال اصل حاکمیت در فضای سایبر تأکید کنند. در این زمینه، گروه کارشناسان دولتی سازمان ملل متحد در گزارش سال ۲۰۱۵ خود اعلام کرد که دولت‌ها در استفاده از فناوری اطلاعات و ارتباطات باید اصول حقوق بین‌الملل از جمله حاکمیت، برابری حاکمیتی و عدم مداخله را رعایت کنند. این گزارش تأکید کرد که تعهدات موجود حقوق بین‌الملل در فضای سایبر نیز قابل اعمال هستند. همچنین در سال ۲۰۱۶، کشورهای عضو سازمان همکاری شانگهای بیانیه‌ای صادر کردند که در آن خواستار ایجاد فضای اطلاعاتی امن و صلح‌آمیز بر

[1]. Assessing International Legal Issues in Information Operations

اساس اصول احترام به حاکمیت و عدم مداخله شدند. این موضع نشان‌دهنده تلاش دولت‌ها برای تقویت مفهوم حاکمیت در فضای سایبر بود (Schmitt & Vihul, 2017: 1667).

با این حال، برخی پژوهشگران معتقدند که این اسناد بیشتر جنبه سیاسی دارند و نمی‌توان آن‌ها را به عنوان قواعد الزام‌آور حقوقی تلقی کرد. کورن و تیلور استدلال می‌کنند که گزارش‌های گروه کارشناسان دولتی سازمان ملل متحد بیشتر بیانگر اصول کلی هستند و نه قواعد دقیق حقوقی که بتوانند مبنای ممنوعیت عملیات‌های سایبری کم‌شدت قرار گیرند (Corn & Taylor, 2017: 282).

کمیته بین‌المللی صلیب سرخ نیز تعریف گسترده‌ای از عملیات سایبری ارائه کرده است. از نظر این نهاد، عملیات سایبری شامل هرگونه فعالیت علیه یا از طریق سیستم‌های رایانه‌ای با هدف نفوذ، استخراج داده‌ها، تخریب یا تغییر اطلاعات و یا دستکاری فرایندهای تحت کنترل سیستم‌های رایانه‌ای است. چنین عملیات‌هایی می‌توانند زیرساخت‌های حیاتی مانند صنایع، شبکه‌های مالی، ارتباطات و سامانه‌های دولتی را تحت تأثیر قرار دهند(Bannelier & Christakis, 2017: 29) . این تعاریف نشان می‌دهد که عملیات سایبری می‌تواند دامنه‌ای از اقدامات از جاسوسی اطلاعاتی تا تخریب زیرساخت‌های حیاتی را شامل شود. با این حال، تمامی این اقدامات الزاماً نقض اصل عدم مداخله محسوب نمی‌شوند. در حقوق بین‌الملل، تحقق مداخله ممنوع مستلزم وجود عنصر اجبار در حوزه صلاحیت انحصاری دولت هدف است؛ بنابراین برخی عملیات‌های سایبری ممکن است صرفاً نقض حاکمیت تلقی شوند، در حالی که برخی دیگر در صورت برخورداری از ماهیت اجبارآمیز می‌توانند ناقض اصل عدم مداخله باشند.

این گستردگی مفهومی موجب شده است که تعیین واکنش حقوقی مناسب نسبت به عملیات سایبری پیچیده شود. در حقوق بین‌الملل، واکنش دولت‌ها معمولاً بر اساس شدت خسارت تعیین می‌شود. با این حال، شدت خسارت تنها معیار تعیین واکنش نیست. در برخی موارد، حتی حملات جدی نیز ممکن است امکان واکنش قاطع حقوقی را فراهم نکند، به‌ویژه زمانی که حمله توسط بازیگران غیردولتی انجام شده و انتساب آن به یک دولت مشخص قابل اثبات نباشد؛ زیرا در چنین وضعیتی استناد به مسئولیت بین‌المللی دولت و طرح ادعای نقض قواعدی نظیر اصل عدم مداخله با دشواری جدی مواجه خواهد شد.

۲-۵- مسئولیت بین‌المللی در عملیات سایبری

واکنش حقوقی به عملیات سایبری زمانی امکان‌پذیر است که یک عمل متخلفانه بین‌المللی رخ داده باشد. در چنین شرایطی، اصل مسئولیت بین‌المللی دولت‌ها اعمال می‌شود. مطابق مواد ۱ و ۲ پیش‌نویس مواد مسئولیت دولت‌ها برای اعمال متخلفانه بین‌المللی، هر فعل یا ترک فعل منتسب به یک دولت که ناقض تعهدات بین‌المللی آن باشد، موجب مسئولیت بین‌المللی آن دولت خواهد شد. در این صورت، دولت زیان‌دیده می‌تواند توقف عمل متخلفانه و ارائه تضمین عدم تکرار آن را مطالبه کند (ماده ۳۰) و همچنین خواستار جبران کامل خسارات ناشی از عمل متخلفانه بین‌المللی شود (مواد ۳۱ و ۳۴ تا ۳۷) (International Law Commission, 2001). این قواعد در فضای سایبر نیز قابل اعمال هستند، اما چالش اصلی در اثبات انتساب حمله سایبری به یک دولت خاص است.

به طوری که، بحث درباره ماهیت حاکمیت در فضای سایبر موجب شکل‌گیری دو دیدگاه اصلی شده است. دیدگاه نخست، حاکمیت را به‌عنوان یک قاعده مستقل حقوقی در نظر می‌گیرد که نقض آن می‌تواند به‌خودی‌خود موجب مسئولیت بین‌المللی دولت‌ها شود. این دیدگاه در قاعده ۴ دستورالعمل تالین ۲,۰ منعکس شده است. بر اساس تفسیر اکثریت کارشناسان تالین، عملیات سایبری که موجب مداخله در کارکردهای ذاتی دولت یا آثار قابل توجه در قلمرو دولت دیگر شود، می‌تواند نقض حاکمیت تلقی گردد و حتی در صورت نرسیدن به آستانه مداخله ممنوع یا توسل به زور، مسئولیت بین‌المللی دولت مرتکب را در پی داشته باشد.(Schmitt, 2017) . در مقابل، دیدگاه دوم حاکمیت را صرفاً یک اصل بنیادین می‌داند که از طریق قواعد دیگر مانند ممنوعیت توسل به زور و اصل عدم مداخله اجرا می‌شود (Pray, 2021: 43). کورن و تیلور[1] از دیدگاه دوم حمایت می‌کنند. آن‌ها استدلال می‌کنند که اصل حاکمیت به‌تنهایی یک قاعده مستقل نیست و نقض حاکمیت تنها زمانی رخ می‌دهد که قواعد مشخصی مانند ممنوعیت توسل به زور یا عدم مداخله نقض شوند. از نظر آن‌ها، عملیات‌های سایبری با

[1]. Corn and Taylor

شدت پایین که به این آستانه‌ها نمی‌رسند، لزوماً نقض حقوق بین‌الملل محسوب نمی‌شوند (Safi, 2019: 47). برای مثال، دیوان در قضیه کانال کورفو (۱۹۴۹) حاکمیت را به‌عنوان یکی از مبانی اساسی روابط بین‌الملل توصیف کرد، اما آن را به‌عنوان یک قاعده مستقل مسئولیت‌آور مورد شناسایی قرار نداد. همچنین در قضیه نیکاراگوئه علیه ایالات متحده (۱۹۸۶)، دیوان تخلفات بین‌المللی را بر اساس قواعد مشخصی همچون منع توسل به زور و عدم مداخله تحلیل کرد (Corn & Taylor, 2017).. از این رو، طرفداران این دیدگاه معتقدند که رویه قضایی بین‌المللی از شناسایی حاکمیت به‌عنوان یک قاعده مستقل که هرگونه نقض آن به‌خودی‌خود موجب مسئولیت بین‌المللی شود، حمایت روشنی به عمل نیاورده است(Safi, 2019: 50).

۳-۵- عملیات سایبری فرامرزی و چالش حاکمیت سرزمینی

دولت‌ها از یک سو، بر حق حاکمیتی خود برای تنظیم فضای سایبر تأکید دارند و از سوی دیگر، ماهیت فرامرزی فضای سایبر، نیازمند همکاری بین‌المللی گسترده است. این وضعیت موجب ایجاد تنش میان حاکمیت ملی و امنیت جمعی سایبری شده است(Gul et al., 2025: 127) . در این راستا، یکی از مهم‌ترین اشکال عملیات سایبری، جاسوسی سایبری است. جاسوسی همواره بخشی از روابط بین‌الملل بوده و در حقوق بین‌الملل به‌طور صریح ممنوع نشده است. بنابراین، جاسوسی سایبری به‌خودی‌خود نقض حقوق بین‌الملل محسوب نمی‌شود. با این حال، شیوه انجام جاسوسی ممکن است موجب نقض قواعد حقوق بین‌الملل شود، به‌ویژه زمانی که با نفوذ به زیرساخت‌های حیاتی همراه باشد(Guerriero et al., 2024: 34) .

در این راستا، یکی از مهم‌ترین اشکال عملیات سایبری، جاسوسی سایبری[1] است. جاسوسی از دیرباز بخشی از روابط میان دولت‌ها بوده و با وجود آنکه اغلب دولت‌ها آن را در قوانین داخلی خود جرم‌انگاری کرده‌اند، حقوق بین‌الملل تاکنون ممنوعیت عام و صریحی برای آن وضع نکرده است. به همین دلیل، بسیاری از حقوقدانان معتقدند که صرف جمع‌آوری مخفیانه اطلاعات از طریق ابزارهای سایبری، به‌خودی‌خود نقض حقوق بین‌الملل محسوب نمی‌شود. با این حال، میان «هدف جاسوسی» و «شیوه انجام جاسوسی» باید تمایز قائل شد؛ زیرا هرچند کسب اطلاعات فی‌نفسه ممنوع نیست، اما روش‌های مورد استفاده برای دستیابی به اطلاعات ممکن است ناقض قواعد حقوق بین‌الملل باشند. برای مثال، اگر عملیات جاسوسی سایبری مستلزم نفوذ غیرمجاز به سامانه‌های دولتی، شبکه‌های نظامی یا زیرساخت‌های حیاتی دولت دیگر باشد، این اقدام ممکن است از منظر اصل حاکمیت دولت‌ها محل ایراد تلقی شود. همچنین چنانچه عملیات مزبور موجب اختلال در عملکرد سامانه‌های دولتی، شبکه‌های برق، تأسیسات هسته‌ای، سامانه‌های حمل‌ونقل یا مراکز درمانی شود، احتمال نقض حاکمیت یا حتی سایر قواعد حقوق بین‌الملل از جمله اصل عدم مداخله افزایش می‌یابد. افزون بر این، جاسوسی سایبری در بسیاری از موارد با نصب بدافزار، ایجاد دسترسی مخفیانه و استقرار طولانی‌مدت در شبکه‌های هدف همراه است؛ وضعیتی که می‌تواند زمینه را برای عملیات‌های مخرب بعدی فراهم کند و از این جهت نگرانی‌های امنیتی و حقوقی گسترده‌ای ایجاد نماید. دستورالعمل تالین ۲٫۰ نیز اگرچه جاسوسی سایبری را به‌عنوان یک فعالیت ذاتاً غیرقانونی تلقی نمی‌کند، اما تأکید دارد که مشروعیت حقوقی هر عملیات باید بر اساس آثار و پیامدهای آن ارزیابی شود. از این رو، جاسوسی سایبری که صرفاً به جمع‌آوری اطلاعات محدود باشد، معمولاً خارج از قلمرو ممنوعیت‌های حقوق بین‌الملل قرار می‌گیرد؛ اما اگر با نفوذ عمیق به سامانه‌های حیاتی، اخلال در عملکرد دولت یا نقض سایر تعهدات بین‌المللی همراه شود، می‌تواند مسئولیت بین‌المللی دولت مرتکب را در پی داشته باشد (Schmitt, 2017: 19-20).

۴-۵- عملیات سایبری و نمونه‌های واقعی نقض حاکمیت سایبری

دولت‌ها از عملیات سایبری برای اهداف مختلفی مانند جمع‌آوری اطلاعات، تأثیرگذاری سیاسی و اختلال در زیرساخت‌های رقبا استفاده می‌کنند. این عملیات به دلیل هزینه پایین، قابلیت انکار و دشواری انتساب، جذابیت زیادی برای دولت‌ها دارد. بسیاری از این عملیات‌ها در «منطقه خاکستری» میان صلح و جنگ انجام می‌شوند و تعیین وضعیت حقوقی آن‌ها دشوار است. این وضعیت موجب شده است که مفهوم سنتی حاکمیت دولت‌ها با تحول اساسی مواجه شود.

---

[1]. Cyber Espionage

الف) حمله سایبری استونی ۲۰۰۷

حملات سایبری علیه استونی در سال ۲۰۰۷ یکی از مهم‌ترین نقاط عطف در تاریخ امنیت سایبری و حقوق بین‌الملل سایبری محسوب می‌شود. این حملات در پی تنش‌های سیاسی میان استونی و روسیه بر سر انتقال بنای یادبود «سرباز برنزی» از مرکز شهر تالین آغاز شد. تصمیم دولت استونی برای جابه‌جایی این یادبود که نماد پیروزی اتحاد جماهیر شوروی در جنگ جهانی دوم تلقی می‌شد، با واکنش شدید روسیه و بخشی از جمعیت روس‌تبار استونی مواجه گردید. در فاصله آوریل تا مه ۲۰۰۷، موج گسترده‌ای از حملات محروم‌سازی از خدمت توزیع‌شده‌علیه زیرساخت‌های دیجیتال استونی صورت گرفت. این حملات وب‌سایت‌های نهادهای دولتی، پارلمان، وزارتخانه‌ها، بانک‌ها، رسانه‌های خبری، شرکت‌های مخابراتی و ارائه‌دهندگان خدمات اینترنتی را هدف قرار داد. حجم ترافیک مخرب به اندازه‌ای بود که بسیاری از سامانه‌های حیاتی کشور برای ساعت‌ها یا حتی روزها از دسترس خارج شدند. از آنجا که استونی یکی از پیشرفته‌ترین دولت‌های دیجیتال جهان محسوب می‌شد و بخش مهمی از خدمات عمومی، بانکی و ارتباطی آن به بستر اینترنت وابسته بود، آثار این حملات به‌طور گسترده در زندگی روزمره شهروندان مشاهده شد. با وجود گستردگی حملات، هیچ خسارت فیزیکی یا تلفات انسانی گزارش نشد و حملات عمدتاً به ایجاد اختلال در دسترسی به خدمات منجر گردید. به همین دلیل، بسیاری از حقوقدانان این رویداد را نمونه‌ای از یک عملیات سایبری زیر آستانه «توسل به زور» دانسته‌اند. با این حال، حمله استونی اهمیت فراوانی در تحول مباحث حقوقی و امنیتی فضای سایبر داشت؛ زیرا نشان داد که حتی بدون استفاده از نیروی نظامی متعارف نیز می‌توان عملکرد دولت، اقتصاد و خدمات عمومی یک کشور را مختل کرد. از منظر حقوق بین‌الملل، حمله استونی پرسش‌های مهمی درباره انتساب عملیات سایبری به دولت‌ها، مسئولیت بین‌المللی دولت‌ها، آستانه توسل به زور و حق دفاع مشروع مطرح کرد. اگرچه بسیاری از تحلیلگران روسیه را عامل یا حامی این حملات می‌دانستند، اما به دلیل دشواری انتساب فنی و حقوقی، استونی نتوانست مسئولیت بین‌المللی دولت خاصی را به‌طور قطعی اثبات کند. همین مسئله بعدها به یکی از مباحث محوری در تدوین دستورالعمل تالین و ادبیات حقوق بین‌الملل سایبری تبدیل شد. اهمیت این رویداد تا حدی بود که پس از آن، سازمان پیمان آتلانتیک شمالی (ناتو) توجه ویژه‌ای به امنیت سایبری معطوف کرد و در سال ۲۰۰۸ مرکز عالی دفاع سایبری تعاونی ناتو در تالین تأسیس شد. این مرکز بعدها مسئولیت هدایت پروژه تدوین دستورالعمل تالین را بر عهده گرفت. از این رو، حمله سایبری استونی نه تنها یک حادثه امنیتی مهم، بلکه نقطه آغاز بسیاری از مباحث نظری و حقوقی معاصر درباره جنگ سایبری، مسئولیت دولت‌ها و حکمرانی فضای سایبر به شمار می‌رود (Baezner, 2018: 4).

ب) حمله سایبری استاکس‌نت

ویروس استاکس‌نت در سال ۲۰۱۰ تأسیسات هسته‌ای ایران را هدف قرار داد و به‌عنوان نخستین حمله سایبری علیه زیرساخت‌های فیزیکی شناخته شد (Baezner, 2018: 4) که توانست خسارات فیزیکی واقعی به تجهیزات صنعتی وارد کند. استاکس‌نت با دستکاری سامانه‌های کنترل صنعتی و تغییر سرعت چرخش سانتریفیوژها، موجب آسیب به بخشی از تجهیزات مورد استفاده در فرایند غنی‌سازی اورانیوم شد(عیدکشایش و همکاران،۱۴۰۳: ۵۸-۶۲). تا آنجا که استاکس‌نت، نقطه عطفی در تحول جنگ سایبری تصور می شود؛ زیرا نشان داد عملیات‌های سایبری می‌توانند آثار فیزیکی مشابه برخی عملیات‌های متعارف نظامی ایجاد کنند. از منظر حقوق بین‌الملل، استاکس‌نت یکی از مهم‌ترین نمونه‌های مورد استناد در مباحث مربوط به حاکمیت، توسل به زور و آستانه حمله مسلحانه در فضای سایبری محسوب می‌شود.(Schmitt, 2017: 334)

ج) حملات سایبری به انتخابات

یکی از مهم‌ترین نمونه‌های نقض اصل عدم مداخله، مداخله سایبری در انتخابات است. مداخله در انتخابات ۲۰۱۶ ایالات متحده آمریکا یکی از مهم‌ترین نمونه‌های مداخله سایبری محسوب می‌شود (Rid, 2020: 133). تحقیقات نشان می‌دهد که در انتخابات ۲۰۱۶ ایالات متحده آمریکا، فعالیت‌های سایبری برای تأثیرگذاری بر افکار عمومی انجام شد و این مسئله به‌عنوان نمونه‌ای از مداخله سایبری در امور داخلی کشورها مطرح شد (Badawy et al., 2018: 5). همچنین گزارش کمیته اطلاعاتی سنا نشان داد که بازیگران سایبری مرتبط با روسیه تلاش کردند به زیرساخت‌های انتخاباتی ایالات متحده نفوذ کنند (Senate Report, 2019).

با توجه به مطالب فوق، نفوذ به زیرساخت‌های حیاتی، حملات سایبری به سیستم‌های دولتی و سرقت داده‌ها از جمله معیارهای نقض حاکمیت سایبری هستند. نمونه‌های واقعی مانند حمله سایبری استونی، حمله به شبکه برق اوکراین و مداخله سایبری در انتخابات نشان می‌دهد که فضای سایبری به عرصه جدیدی برای رقابت قدرت‌ها تبدیل شده است.

۶- چالش‌های حقوق بین‌الملل در مواجهه با عملیات سایبری فرامرزی

مهم‌ترین چالش‌های حقوق بین‌الملل در مواجهه با عملیات سایبری فرامرزی را می‌توان در سه حوزه اصلی شامل مشکل انتساب، مسئله صلاحیت قضایی و خلأهای حقوقی و نهادی بررسی کرد.

۱-۶- مشکل انتساب و مسئولیت دولت‌ها در عملیات سایبری

یکی از مهم‌ترین چالش‌های حقوق بین‌الملل در فضای سایبر، مسئله انتساب عملیات سایبری به دولت‌ها است. در حقوق بین‌الملل سنتی، انتساب رفتار غیرقانونی به دولت‌ها معمولاً از طریق شواهد مستقیم یا کنترل مؤثر امکان‌پذیر است؛ اما در فضای سایبر، ناشناس بودن عاملان و استفاده از زیرساخت‌های پراکنده، این فرآیند را بسیار پیچیده کرده است. در دستورالعمل تالین ۲،۰، مسئله انتساب و مسئولیت دولت‌ها در عملیات سایبری بر اساس قواعد حقوق بین‌الملل عرفی و پیش‌نویس مواد مسئولیت دولت‌ها تنظیم شده است. مطابق این چارچوب، رفتار بازیگران غیردولتی در صورتی به دولت منتسب می‌شود که تحت هدایت، کنترل یا دستور آن دولت انجام شده باشد، یا در صورتی که نهاد مزبور عناصر اقتدار حکومتی را اعمال کند، و همچنین هنگامی که دولت رفتار انجام‌شده را به‌صراحت بپذیرد و به‌عنوان عمل خود معرفی کند. در کنار این اشکال انتساب مستقیم، تالین ۲،۰ تعهد «مراقبت مقتضی» را نیز مورد تأکید قرار می‌دهد؛ به این معنا که دولت‌ها موظف‌اند از استفاده از قلمرو و زیرساخت‌های تحت صلاحیت خود برای انجام عملیات سایبری زیان‌بار علیه سایر دولت‌ها جلوگیری کنند. در نتیجه، حتی در مواردی که عملیات سایبری به‌طور مستقیم قابل انتساب به دولت نباشد، قصور در پیشگیری از فعالیت‌های سایبری مخرب نیز می‌تواند مبنای مسئولیت بین‌المللی دولت قرار گیرد و در صورت تحقق انتساب و نقض تعهد بین‌المللی، قواعد عام مسئولیت دولت‌ها مطابق مواد ۱ و ۲ پیش‌نویس کمیسیون حقوق بین‌الملل اعمال شده و دولت مسئول ملزم به توقف عمل متخلفانه، تضمین عدم تکرار و جبران خسارت خواهد بود (Schmitt, 2017: 105-106).

در این زمینه، نیکلاس تسگوریاس و مایکل فارل[1] تأکید می‌کنند که عملیات سایبری اغلب چندمرحله‌ای بوده و از سرورها و شبکه‌های مختلف در کشورهای متعدد عبور می‌کنند، که این امر شناسایی عامل واقعی حمله را دشوار می‌سازد (Tsagourias & Farrell, 2020: 944). مایکل اشمیت و لیس ویهول[2] نیز معتقدند که استفاده دولت‌ها از بازیگران نیابتی و غیردولتی، فرآیند انتساب را پیچیده‌تر کرده و شکاف‌هایی در نظام مسئولیت دولت‌ها ایجاد کرده است (Schmitt & Vihul, 2017: 22). در همین راستا، تانییلدیزی[3] بیان می‌کند که معیارهای سنتی مانند «کنترل مؤثر» یا «کنترل کلی» در فضای سایبر کارایی محدودی دارند، زیرا دولت‌ها می‌توانند از گروه‌های هکری مستقل یا شرکت‌های خصوصی برای اجرای عملیات سایبری استفاده کنند (Tanyildizi, 2017: 18).

مطالعات جدید همچنین نشان می‌دهد که انتساب سایبری دارای سه بعد فنی، سیاسی و حقوقی است و حتی در صورت امکان‌پذیر بودن انتساب فنی، اثبات مسئولیت حقوقی دولت‌ها همچنان دشوار باقی می‌ماند (Spáčil, 2024: 155). گزارش مشترک گروه کارشناسی چین و اروپا نیز بر این نکته تأکید می‌کند که تفاوت میان این سطوح انتساب موجب پیچیدگی بیشتر مسئولیت دولت‌ها در فضای سایبری شده است (Chen et al., 2025: 9).

در این راستا، ناشناس بودن یکی از مهم‌ترین عوامل دشواری انتساب محسوب می‌شود. حملات سایبری معمولاً از طریق شبکه‌ای از سرورها، بات‌نت‌ها و سیستم‌های آلوده انجام می‌شوند که در کشورهای مختلف قرار دارند. این وضعیت موجب می‌شود که شناسایی عامل اصلی حمله بسیار دشوار باشد (Rid, 2020: 112). افزون بر این، عملیات «پرچم دروغین[4]» که در آن مهاجم تلاش می‌کند حمله را به دولت دیگری نسبت دهد، پیچیدگی تعیین مسئولیت بین‌المللی را افزایش داده است

---

1. Nicholas Tsagourias and Farrell Michael
2. Michael Schmitt and, Liis Vihul
3. Tanyildizi
4. False Flag

(Schmitt, 2017: 82). علاوه بر این، حملات پراکسی نیز یکی دیگر از چالش‌های مهم انتساب محسوب می‌شود. در این نوع حملات، دولت‌ها از گروه‌های واسطه یا بازیگران ثالث برای اجرای عملیات سایبری استفاده می‌کنند. این گروه‌ها می‌توانند شامل شرکت‌های خصوصی، گروه‌های هکری یا حتی سازمان‌های جنایی باشند. این وضعیت ارتباط مستقیم میان دولت و عملیات سایبری را دشوار کرده و مسئولیت حقوقی دولت‌ها را پیچیده‌تر می‌کند (Schmitt & Vihul, 2017: 8؛ Nye, 2010: 108). در نتیجه، نقش گسترده بازیگران غیردولتی و پراکسی‌ها موجب شده است که چارچوب سنتی مسئولیت بین المللی دولت‌ها در حقوق بین‌الملل با چالش‌های جدی مواجه شود (Roscini, 2014: 51؛ Tanyildizi, 2017: 21).

۲-۶- چالش صلاحیت قضایی در عملیات سایبری فرامرزی

یکی دیگر از چالش‌های مهم حقوق بین‌الملل در عملیات سایبری، مسئله صلاحیت قضایی است. در فضای سایبر، حمله ممکن است از یک کشور آغاز شود، از طریق چند کشور عبور کند و در کشور دیگری تأثیر بگذارد. این ویژگی تعیین صلاحیت قضایی را دشوار کرده و موجب تعارض میان دولت‌ها می‌شود (Schmitt, 2017: 51). صلاحیت سرزمینی یکی از اصول سنتی حقوق بین‌الملل است که بر اساس آن دولت‌ها بر فعالیت‌های انجام‌شده در قلمرو خود صلاحیت دارند. با این حال، در فضای سایبر تعیین محل وقوع حمله دشوار است، زیرا عملیات سایبری ممکن است از چندین سرور در کشورهای مختلف انجام شود. این مسئله موجب تعارض صلاحیت میان دولت‌ها شده است (Batarseh, 2022: 301).

برخی پژوهشگران پیشنهاد کرده‌اند که حملات سایبری شدید در چارچوب صلاحیت جهانی بررسی شوند، به‌ویژه در مواردی که امنیت بین‌المللی تهدید می‌شود (Schmitt, 2017: 55). با این حال، بسیاری از دولت‌ها با این رویکرد مخالف هستند، زیرا اعمال صلاحیت جهانی در فضای سایبری می‌تواند موجب تعارض‌های سیاسی و حقوقی شود (Nye, 2010: 114).

در همین راستا، صلاحیت فراسرزمینی نیز به‌عنوان راهکار دیگری مطرح شده است. بر اساس این رویکرد، دولت‌ها می‌توانند عملیات سایبری خارج از قلمرو خود را بررسی کنند، در صورتی که این عملیات امنیت ملی آن‌ها را تحت تأثیر قرار دهد. با این حال، این رویکرد نیز با مخالفت برخی دولت‌ها مواجه شده است، زیرا ممکن است نقض حاکمیت تلقی شود (Schmitt, 2017: 58؛ Shaw, 2017: 692).

۳-۶- خلأهای حقوقی و نبود اجماع بین‌المللی

یکی دیگر از چالش‌های مهم حقوق بین‌الملل در فضای سایبر، وجود خلأهای حقوقی و نبود قواعد صریح بین‌المللی است. اگرچه اصول کلی حقوق بین‌الملل مانند حاکمیت، عدم مداخله و مسئولیت دولت‌ها در فضای سایبر نیز قابل اعمال هستند، اما نحوه اجرای این اصول همچنان مبهم باقی مانده است (Schmitt, 2017: 5). مارکو روسچینی[1] نیز تأکید می‌کند که تعیین آستانه استفاده از زور در عملیات سایبری همچنان موضوعی بحث‌برانگیز است و دولت‌ها دیدگاه‌های متفاوتی در این زمینه دارند (Roscini, 2014: 45). همچنین دستورالعمل تالین ۲,۰ در مقدمه خود تأکید می‌کند که بسیاری از قواعد سنتی حقوق بین‌الملل برای مواجهه با ویژگی‌های خاص فضای سایبر طراحی نشده‌اند و در نتیجه، در کاربرد آن‌ها در این حوزه با ابهام‌ها و خلأهای تفسیری مواجه هستیم. با این حال، هدف این دستورالعمل ایجاد حقوق جدید نیست، بلکه تفسیر و اعمال قواعد موجود حقوق بین‌الملل در بستر عملیات‌های سایبری است(Schmitt, 2017: 3) . این رویکرد نشان می‌دهد که چالش اصلی در حقوق بین‌الملل سایبری نه فقدان قواعد، بلکه دشواری در تفسیر و انطباق قواعد موجود با ماهیت غیرمادی، فرامرزی و ناشناس فضای سایبر است. از این رو، یکی از مهم‌ترین خلأهای حقوقی، نبود معاهده جامع بین‌المللی در زمینه عملیات سایبری است. برخلاف حوزه‌هایی مانند حقوق دریاها یا حقوق هوافضا، هنوز معاهده جهانی جامعی برای فضای سایبر وجود ندارد. تلاش‌هایی مانند گزارش‌های گروه کارشناسان دولتی سازمان ملل انجام شده است، اما این اسناد الزام‌آور نبوده و بیشتر جنبه توصیه‌ای دارند (UN GGE, 2021: 7).

علاوه بر این، اختلاف دیدگاه دولت‌ها نیز مانع شکل‌گیری قواعد مشترک شده است. برخی دولت‌ها مانند ایالات متحده آمریکا معتقدند که حقوق بین‌الملل موجود برای فضای سایبر کافی است، در حالی که برخی دیگر مانند چین و روسیه خواستار تدوین معاهده جدید هستند (Nye, 2010: 120). این اختلاف دیدگاه‌ها موجب شده است که اجماع بین‌المللی درباره قواعد

---

[1]. Marco Roscini

حقوقی فضای سایبری شکل نگیرد. از سوی دیگر، نبود سازکار اجرایی مؤثر نیز یکی از چالش‌های اساسی محسوب می‌شود. حتی در مواردی که مسئولیت یک دولت مشخص شود، اجرای حقوق بین‌الملل در فضای سایبر دشوار است.
در مجموع، عملیات سایبری فرامرزی چالش‌های بنیادینی برای حقوق بین‌الملل ایجاد کرده است. مشکل انتساب، پیچیدگی صلاحیت قضایی، نقش بازیگران غیردولتی، خلأهای حقوقی و نبود اجماع میان دولت‌ها از مهم‌ترین این چالش‌ها هستند. این تحولات نشان می‌دهد که چارچوب‌های سنتی حقوق بین‌الملل برای مواجهه با تهدیدهای سایبری کافی نیستند و توسعه تدریجی قواعد جدید حقوق بین‌الملل سایبری برای حفظ ثبات و امنیت بین‌المللی ضروری به نظر می‌رسد.

نتیجه‌گیری

مقاله حاضر کوشید تا نشان دهد که حقوق بین‌الملل موجود، علیرغم داشتن ظرفیت نظری برای تنظیم رفتار دولت‌ها در فضای سایبر، در عمل با سه مانع بنیادین مواجه است: ابهام مفهومی در اصول حاکمیت و عدم مداخله، دشواری ساختاری انتساب عملیات به دولت‌ها و نبود نهاد داوری تخصصی و الزام‌آور. این موانع نه از جنس فقدان قاعده، بلکه از جنس «شکاف اجرا و تفسیر» هستند. آنچه امروز فضای سایبر را به «منطقه خاکستری حقوقی» تبدیل کرده است، نبود قاعده نیست؛ بلکه نبود اراده سیاسی برای پذیرش رویه قضایی الزام‌آور و نبود اجماع بر سر مصادیق عملیاتی اصولی همچون «اجبار» و «مداخله» است. نکته نوآورانه‌ای که این پژوهش بر آن تأکید دارد، آن است که اصل عدم مداخله در فضای سایبر دچار «بحران مصداق‌یابی» شده است. در حقوق بین‌الملل کلاسیک، مداخله با معیارهایی نسبتاً روشن مانند حضور فیزیکی، استفاده از زور یا اجبار آشکار قابل تشخیص بود. اما در فضای سایبر، عملیاتی مانند مهندسی افکار عمومی، انتشار گسترده اطلاعات نادرست در آستانه انتخابات، یا نفوذ بلندمدت به زیرساخت‌های غیرنظامی، بدون آنکه به‌وضوح مصداق «اجبار» باشند، می‌توانند حاکمیت و استقلال تصمیم‌گیری یک دولت را به شدت تضعیف کنند. در چنین شرایطی، توسل صرف به تعریف سنتی «اجبار» راهگشا نیست و نیاز به بازتعریف عملیاتی این مفهوم در عصر دیجیتال به یکی از اولویت‌های حقوق بین‌الملل معاصر تبدیل شده است. از دیگر یافته‌های تحلیلی مهم این پژوهش، شناسایی یک تناقض ساختاری در موضع‌گیری دولت‌هاست. از یک سو، دولت‌ها در مجامع بین‌المللی همچون گروه کارشناسان دولتی و گروه کاری با عضویت باز بر قابلیت اعمال حقوق موجود در فضای سایبر تأکید می‌کنند و از اصول حاکمیت و عدم مداخله دفاع می‌نمایند. از سوی دیگر، در عمل، همین دولت‌ها از پذیرش هرگونه مرجع داوری فراقوه‌ای یا قاعده عرفی مشخص که رفتار خودشان را محدود کند، خودداری می‌ورزند. این دوگانگی، به‌ویژه در مورد قدرت‌های بزرگ سایبری (آمریکا، روسیه، چین) مشهود است. ایالات متحده با تفسیر مضیق از اصل حاکمیت، عملیات زیرآستانه را عمدتاً مجاز می‌داند؛ روسیه و چین نیز با وجود تأکید بر حاکمیت سایبری در بیانیه‌های سیاسی، در عمل از بازیگران غیردولتی و پراکسی به‌طور گسترده استفاده می‌کنند. نتیجه این وضعیت، «بازی بدون قاضی» در فضای سایبر است که در آن هر دولت هم‌زمان هم بازیکن است و هم مفسر قواعد. بررسی سه نمونه عمده این مقاله مانند حمله استونی (۲۰۰۷)، استاکس‌نت (۲۰۱۰) و مداخله در انتخابات آمریکا (۲۰۱۶)، به‌روشنی نشان می‌دهد که حقوق بین‌الملل در هیچ‌یک از این موارد نتوانسته است به تعیین مسئولیت قاطع و الزام‌آور منجر شود. در استونی، به دلیل دشواری انتساب، هیچ دولتی به‌طور رسمی مسئول شناخته نشد. در استاکس‌نت، حتی با وجود خسارت فیزیکی آشکار، جامعه بین‌المللی از هرگونه اعلام رسمی نقض حاکمیت خودداری کرد. در انتخابات ۲۰۱۶، با وجود گزارش‌های متقن درباره نقش بازیگران مرتبط با روسیه، واکنش عمدتاً سیاسی و تحریمی بود، نه حقوقی. این سه مورد نشان می‌دهند که حقوق بین‌الملل سایبری در مرحله «پیش‌رویه‌قضایی» باقی مانده است و تا زمانی که یک پرونده نمادین با انتساب قطعی و واکنش حقوقی رسمی شکل نگیرد، بازدارندگی هنجاری اصولی مانند عدم مداخله بسیار محدود خواهد بود. در پاسخ به این وضعیت، مقاله پیشنهاد می‌کند که مسیر پیشرفت حقوق بین‌الملل سایبری نباید صرفاً بر تدوین معاهده جامع متمرکز شود (که به دلیل اختلافات ژئوپلیتیک بعید به نظر می‌رسد)، بلکه باید از راهبرد ترکیبی سه‌لایه پیروی کند: لایه نخست، تقویت هنجارهای نرم رفتاری با تمرکز بر شفافیت و اقدامات اعتمادساز میان دولت‌ها (مانند تبادل اطلاعات در خصوص بدافزارها و کانال‌های ارتباطی بحران). لایه دوم، ایجاد یک نهاد تخصصی فنی-حقوقی انتساب با مشارکت بخش خصوصی و دانشگاهیان که بتواند در زمان واقعی، گزارش‌های قابل استناد دادگاهی از مبدأ حملات ارائه دهد؛ بدون آنکه الزاماً جایگزین تصمیم سیاسی دولت‌ها

شود. لایه سوم، توسعه تدریجی رویه عرفی از طریق «اقدامات متقابل هماهنگ منطقه‌ای»؛ به این معنا که دولت‌های هم‌عقیده می‌توانند در قالب گروه‌هایی مانند اتحادیه اروپا یا ناتو، پاسخ‌های حقوقی مشخصی به انواع خاصی از عملیات سایبری (مثلاً مداخله در انتخابات) تعریف کرده و با تکرار این پاسخ‌ها، به تدریج عرف بین‌المللی جدیدی خلق کنند. در نهایت، این پژوهش به این نتیجه می‌رسد که حقوق بین‌الملل بدون نهاد، ناقص است و فضای سایبر بدون رویه، بی‌قاعده. اجماع نظری بر «قابلیت اعمال» قواعد موجود، اگر به اجماع عملی بر «نحوه اعمال» تبدیل نشود، نه تنها از کارآمدی بازدارندگی می‌کاهد، بلکه می‌تواند به ابزاری در دست دولت‌های قدرتمند برای توجیه عملیات‌های یک‌طرفه تبدیل گردد. از این رو، آینده حقوق بین‌الملل سایبری نه در انتظار معاهده‌ای جامع و دست‌نیافتنی، بلکه در نهادینه‌سازی تدریجی فرآیندهای انتساب، شفافیت و پاسخ‌گویی رقم خواهد خورد. اصل عدم مداخله در فضای سایبر همچنان یک اصل بنیادین باقی خواهد ماند، اما تا زمانی که مصادیق عملیاتی آن مورد توافق حداقلی دولت‌ها قرار نگیرد و سازوکاری برای داوری بی‌طرفانه درباره نقض‌های آن وجود نداشته باشد، این اصل بیشتر به «بیانیه سیاسی مطلوب» شبیه خواهد بود تا «قاعده حقوقی الزام‌آور». بنابراین، مهم‌ترین چالش پیشِ روی جامعه بین‌المللی، نه فقدان قاعده، بلکه فقدان نهاد و فقدان اراده سیاسی برای پذیرش محدودیت‌های داوطلبانه به نام ثبات جمعی است.

منابع

عیدکشایش و همکاران (۱۴۰۳)، تعارض حمالت سایبری با اصل عدم مداخله در حقوق بین الملل با تمرکز بر اقدامات ایاالتمتحده آمریکا، مطالعات حقوقی فضای مجازی، دوره ۳، شماره ۲.

قاسمی، غلامعلی (۱۳۹۵)، چالش‌های اصل عدم مداخله و جایگاه آن در حقوق بین‌الملل، آفاق امنیت، شماره ۳۳.

مجتهدی، محمدرضا و همکاران (۱۴۰۲)، معناشناسی اصل عدم مداخله از منظر تعاملات این مفهوم با دیگر اصول بنیادین حقوق بین الملل، پژوهش های حقوق تطبیقی، شماره ۲۲.

Badawy, Adam et al(2018), "Analyzing Russian Interference in the 2016 Election", Journal of Information Warfare.

Baezner, Marie (2018), Cyber and Information Warfare in the Ukrainian Conflict, ETH Zurich.

Bannelier, karine and christakis, théodore (2017), Cyber-Attacks Prevention-Reactions: The Role of States and Private Actors, the Committee for National Defence Studies.

Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatorychallenges. Journal of Financial Crime, 28(2).

Brownlie, Ian (2008), Principles of Public International Law, Oxford University Press.

Chen, Hui et al (2025), The Attribution of Cyber Operations to States in International Law, Sino-European Expert Working Group on the Application of International Law in Cyberspace.

Chircop, luke (2019), Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0, Melbourne Journal of International Law, Vol 20.

Cora, hakan and mikail, elnur hasan (2026), cybersecurity, sovereignty, and international law: normative challenges in the digital age, veredas do direito, v.23, e234381.

Corn, Gary P.; Taylor, Robert (2017), Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0: Concluding Observations on Sovereignty in Cyberspace, The American Journal of International Law Unbound, Vol. 111.

Crawford, James (2013). State Responsibility: The General Part. Cambridge University Press.

Crawford, James R (2012), Brownlie's Principles of Public International Law (Oxford University Press.

DeNardis, Laura (2014). The Global War for Internet Governance. Yale University Press.

Dinstein, Yoram (2020). Cyber War and International Law. Cambridge University Press.

European Commission. (2020). The EU's Cybersecurity Strategy for the Digital Decade. Brussels: European Commission.

Guerriero, Alessandro et al (2024), States' cyber-interferences in International Law: a reconstruction of the Principles of Sovereignty, Nonintervention and Self-Determination and their applicability in cyber context, Corso di laurea in Giurisprudenza.

Gul, Seema et al (2025), Cybersecurity and sovereignty: the role of internationallawin governing state behaviour in cyberspace, Policy Journal of Social Science Review, Vol. 3 No. 5.

International Law Commission. (2001). Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries. Yearbook of the International Law Commission, Vol. II, Part Two. United Nations.

Khan, A. et al (2020). TheEvolution of Human Rights Law in the Age of Globalization. Pakistan journal of law, analysis and wisdom.

Kilovaty, Ido (2021), Chapter 5: The international law of cyber intervention, in Research Handbook on International Law and Cyberspace, Edward Elgar Publishing.

Koh, Harold (2012). International Law in Cyberspace. USCYBERCOM Inter-Agency Legal Conference.

Lahmann, H. (2021). On the politics and ideologies of the sovereignty discourseincyberspace. Duke J. Comp. & Int'l L., 32, 61.
Meyer, P. (2020). Norms of responsible state behaviour in cyberspace. The ethics of cybersecurity.
Moulin, Thibault (2020), Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward, Journal of Conflict and Security Law 25(3).
Nye, Joseph Samuel Jr. (2010). *Cyber Power*. Oxford University Press.
Ossof, William (2021), Hacking the Domaine R´eserv´e: The Rule of Non-Intervention and Political Interference in Cyberspace, Volume 62, Number 1.
Pray, corey (2021), it's the principle: defining sovereignty in the context of cyber operations, national security 44 law journal, vol. 7:2.
Rid, T. (2020). Active Measures. Farrar, Straus and Giroux.
Roscini, Marco (2014), Cyber Operations and the Use of Force in International Law, Oxford University Press.
Safi, Sam (2019), Master's Thesis in Public International Law, Sovereignty in Cyberspace A Study on Customary International Law on the Principle of Sovereignty, Cover: Illustration by VIN JD. Licensed under Pixabay.
Sardu, Alessandra (2025), Non-intervention and cyberspace, QIL, Zoom-in 110.
Schmitt, Michael N. (2017), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press.
Schmitt, Michael N. and Vihul, Liis (2017), Respect for Sovereignty in Cyberspace, Texas Law Review, Vol. 95.
Sean, Watts and Theodore, Richard (2018), Baseline Territorial Sovereignty and Cyberspace (Lewis & Clark Review, Vol. 22, Issue 3.
Shaw, Malcolm N. (2017), International Law, Cambridge University Press.
Tanyildizi, Emrah (2017), State Responsibility in Cyberspace, Law & Justice Review.
Tanzi, Attila et al (2021), international law and cyberspace, Ministry of Foreign Affairs and International Cooperation.
Tsagourias, N. (2021). The legal status of cyberspace: sovereignty redux?. In ResearchHandbook on International Law and Cyberspace (pp. 9-31). Edward Elgar Publishing.
Tsagourias, Nicholas & Buchan, Russell (2021). Research Handbook on International Law and Cyberspace. Edward Elgar.
Tsagourias, Nicholas & Farrell, Michael (2020), Cyber Attribution: Technical and Legal Approaches and Challenges, European Journal of International Law, Vol. 31.
UK Government. (2022). National Cyber Strategy 2022. London: HM Government.
United Nations Group of Governmental Experts (2015), Report of the UN GGE.
US Senate Intelligence Committee (2019), Russian Interference in the 2016 Election, Washington DC.
Watts, Sean (2014), Low-Intensity Cyber Operations and the Principle of Non-Intervention, Creighton University School of Law; Lieber Institute for Law & Land Warfare, West Point.
White House. (2023). National Cybersecurity Strategy. Washington, DC: The White House.
Willmer, Lukas (2023), Does Digitalization Reshape the Principle of Non-Intervention?, German Law Journal , International Law and Digitalization, Volume 24 , Special Issue 3.

State Sovereignty in Cyberspace and the Principle of Non-Intervention: Challenges of International Law in the Face of Cross-Border Cyber Operations

Abstract

The expansion of information and communication technologies and the increasing reliance of states on digital infrastructures have transformed cyberspace into one of the most critical domains of national security, economic stability, and political sovereignty. However, the transnational, decentralized, and borderless nature of cyberspace has posed fundamental challenges to the traditional principles of international law, particularly state sovereignty and the principle of non-intervention. Accordingly, the main question of this research is to what extent international legal frameworks are capable of regulating state behavior in cross-border cyber operations, and what challenges these operations pose to the principles of sovereignty and non-intervention? In response to this question, the research hypothesis posits that although existing international law provides a foundational framework for regulating state behavior in cyberspace, the complex and transnational nature of cyber operations has subjected these rules to enforcement limitations, conceptual ambiguities, and legal vacuums. Consequently, the need for the progressive development of international cyber law is felt more than ever. Employing a doctrinal legal analysis method and a comparative approach, this study examines international instruments, including the United Nations Charter and the Tallinn Manual 2.0. The findings of the research indicate that fundamental rules and principles of international law, such as state sovereignty and the principle of non-intervention, have limited efficacy in cyberspace. Furthermore, diverging state perspectives regarding the threshold of sovereignty violation and cyber intervention have led to fragmentation in the application of legal rules and increased the risk of escalating cyber tensions.

Keywords: Cyber Sovereignty, Principle of Non-Intervention, Cross-Border Cyber Operations,Tallin Manual, Challenges of International Law.