Interdisciplinary Legal Research
Jun 2025, 6(3): 61-73
Available online on: www. ilrjournal.ir
e-ISSN:2717-1795

ORIGINAL RESEARCH PAPER

Legal Analysis of Cyber Attacks on Critical Infrastructures; Responsibility of States and International Institutions

Ali Yazdani [1], ***Nazafarin Nazemi**** [2]

Received:
30 Jun 2025
Revised:
31 Agu 2025
Accepted:
10 Sep 2025
Available Online:
22 Sep 2025

Keywords:
Cyber Attacks, Critical Infrastructure, International Responsibility, States, International Law, Compensation.

Abstract

With the increasing dependence of states on new information and electronic technologies, cybersecurity has become one of the main challenges in maintaining the critical infrastructures of countries. Cyber-attacks that are carried out with the intention of destroying, disrupting or unauthorized access to critical systems can lead to widespread damage in the economic, security, political and social spheres. In this regard, analyzing the responsibility of states and international institutions from the perspective of international law in the face of these attacks is of particular importance. Based on the fundamental principles of international law, every state is responsible for its actions that lead to a violation of international obligations; even in situations where it has indirectly aided or assisted the attacking state in carrying out the attacks. Article 16 of the Draft International Responsibility of States and other similar documents provide frameworks for determining responsibility arising from cooperation or facilitation in cyber-attacks. Meanwhile, if the state's action violates principles such as the prohibition of the use of force or aggression against the sovereignty of another state, not only the attacking state, but also the supporting states will be obliged to compensate for the damage. Also, the issue of criminalizing cyber-attacks, recognizing the responsibility of states in the form of international responsibility, and the possibility of using human rights and humanitarian instruments such as the Additional Protocol to the Geneva Convention are among the topics raised in this research. Finally, the necessity of creating coordinated and effective legal systems for preventing, responding to, and compensating for damage caused by cyber-attacks is emphasized. The method of the present article is descriptive-analytical and the tools used are library and documentary.

1 M.A Student, Shi.C, Islamic Azad University, Shiraz, Iran.
2* Assistant Professor, Shi.C, Islamic Azad University, Shiraz, Iran.
(Corresponding Author) Email: *dr.n.nazemi@gmail.com*

Please Cite This Article As: Yazdani, A & Nazemi, N (2025). "Legal Analysis of Cyber Attacks on Critical Infrastructures; Responsibility of States and International Institutions".*Interdisciplinary Legal Research*, 6 (3): 61-73.

مقاله پژوهشی
(صفحات ۶۱-۷۳)

تحلیل حقوقی حملات سایبری به زیرساخت‌های حیاتی؛ مسؤولیت دولت‌ها و نهادهای بین‌المللی

علی یزدانی [۱]، نازآفرین ناظمی*[۲]

۱. دانشجوی کارشناسی ارشد، واحد شیراز، دانشگاه آزاد اسلامی، شیراز، ایران
۲. استادیار، واحد شیراز، دانشگاه آزاد اسلامی، شیراز، ایران. (نویسنده مسؤول)

Email: dr.n.nazemi@gmail.com

دریافت: ۱۴۰۴/۰۴/۱۰ ویرایش: ۱۴۰۴/۰۶/۱۵ پذیرش: ۱۴۰۴/۰۶/۲۰ انتشار: ۱۴۰۴/۰۷/۰۱

چکیده
با گسترش وابستگی دولت‌ها به فناوری‌های نوین اطلاعاتی و الکترونیکی، امنیت سایبری به یکی از چالش‌های اصلی در حفظ زیرساخت‌های حیاتی کشورها تبدیل شده است. حملات سایبری که به قصد تخریب، اختلال یا دسترسی غیرمجاز به سامانه‌های حیاتی صورت می‌گیرند، می‌توانند منجر به خسارات گسترده‌ای در حوزه‌های اقتصادی، امنیتی، سیاسی و اجتماعی شوند. در این راستا، تحلیل مسؤولیت دولت‌ها و نهادهای بین‌المللی از منظر حقوق بین‌الملل در مواجهه با این حملات از اهمیت ویژه‌ای برخوردار است. براساس اصول بنیادین حقوق بین‌الملل، هر دولتی نسبت به اعمال خود که منجر به نقض تعهدات بین‌المللی شود، مسؤولیت دارد؛ حتی در شرایطی که به شکل غیرمستقیم به دولت مهاجم در اجرای حملات کمک یا مساعدت کرده باشد. ماده ۱۶ پیش‌نویس طرح مسؤولیت بین‌المللی دولت‌ها و سایر اسناد مشابه، چارچوب‌هایی برای تعیین مسؤولیت ناشی از همکاری یا تسهیل در حملات سایبری ارائه می‌دهند. در این میان، اگر فعل دولت موجب نقض اصولی مانند ممنوعیت توسل به زور یا تعرض به حاکمیت کشور دیگر شود، نه‌تنها دولت مهاجم، بلکه دولت‌های حامی نیز موظف به جبران خسارت خواهند بود. همچنین، موضوع جرم‌انگاری حملات سایبری، شناسایی مسؤولیت دولت‌ها در قالب مسؤولیت بین‌المللی، و امکان بهره‌گیری از اسناد حقوق بشری و بشردوستانه نظیر پروتکل الحاقی کنوانسیون ژنو، ازجمله مباحث مطرح‌شده در این تحقیق هستند. نهایتاً، ضرورت ایجاد نظام‌های حقوقی هماهنگ و اثربخش برای پیشگیری، پاسخ‌گویی و جبران خسارت ناشی از حملات سایبری، مورد تأکید قرار می‌گیرد. روش مقاله حاضر توصیفی-تحلیلی و ابزار مورد استفاده نیز کتابخانه‌ای و اسنادی است.
کلمات کلیدی: حملات سایبری، زیرساخت‌های حیاتی، مسؤولیت بین‌المللی، دولت‌ها، حقوق بین‌الملل، جبران خسارت.

مقدمه

۱- بیان مسأله

با پیشرفت فناوری‌های اطلاعاتی و گسترش کاربرد سامانه‌های رایانه‌ای در مدیریت زیرساخت‌های حیاتی کشورها، حوزه امنیت سایبری به یکی از مهم‌ترین و پیچیده‌ترین چالش‌های جهانی تبدیل شده است. زیرساخت‌های حیاتی شامل تأسیسات و سامانه‌هایی است که عملکرد صحیح و مستمر آنها برای امنیت ملی، اقتصاد، سلامت و رفاه عمومی یک کشور ضروری است. در این زمینه، حملات سایبری به این زیرساخت‌ها، به‌عنوان یک تهدید نوظهور، می‌تواند پیامدهای مخربی ازجمله اختلال در خدمات حیاتی، خسارت‌های مالی و جانی و حتی بی‌ثباتی سیاسی–اجتماعی به همراه داشته باشد. از منظر حقوق بین‌الملل، مسأله تعیین مسؤولیت دولت‌ها و نهادهای بین‌المللی در قبال این حملات، یکی از پیچیده‌ترین و در عین حال ضروری‌ترین مباحث است. دولت‌ها به‌عنوان بازیگران اصلی در نظام بین‌الملل، علاوه‌بر وظیفه حفظ امنیت و حراست از زیرساخت‌های حیاتی خود، باید در چارچوب قوانین و تعهدات بین‌المللی عمل کنند و از هرگونه فعالیت سایبری که منجر به نقض حقوق سایر دولت‌ها یا ایجاد خسارت شود، خودداری نمایند. با این حال، پیچیدگی‌های ماهیت فناوری‌های سایبری، عدم شفافیت کامل در شناسایی عامل حمله و گاهی مشارکت یا مساعدت دولت‌های مختلف در انجام این حملات، چالش‌های حقوقی قابل توجهی را به وجود آورده است.

از سوی دیگر، نهادهای بین‌المللی نیز به‌عنوان بازیگران تأثیرگذار در تنظیم قواعد و چارچوب‌های حقوقی جهانی، نقش مهمی در تعیین حدود مسؤولیت و نحوه پاسخگویی به حملات سایبری دارند. اما فقدان توافقات جامع و الزام‌آور در زمینه جرایم سایبری و ضعف سازوکارهای اجرایی، موضوع مسؤولیت و جبران خسارت در این حوزه را پیچیده‌تر ساخته است. بنابراین، مسأله اصلی تحقیق، بررسی دقیق ابعاد حقوقی حملات سایبری به زیرساخت‌های حیاتی، تحلیل چارچوب‌های موجود مسؤولیت دولت‌ها و نهادهای بین‌المللی و تعیین راهکارهای حقوقی مؤثر برای پیشگیری، مقابله و جبران خسارات ناشی از این حملات است. این تحلیل می‌تواند ضمن روشن ساختن مبانی حقوقی و اصول حاکم، به ایجاد سازوکارهای هماهنگ‌تر و کارآمدتر در سطح بین‌المللی برای مدیریت تهدیدات سایبری کمک کند و به امنیت پایدار فضای سایبری در جهان معاصر منجر شود. پرسش محوری این است که مسؤولیت دولت‌ها و نهادهای بین‌المللی از منظر حقوقی در زمینه حملات به زیرساخت‌های حیاتی چیست؟

۲- روش تحقیق: توصیفی- تحلیلی.

بحث و نظر

۱- حملات سایبری و پیامدهای آنان

حملات سایبری چه از طرف دولت یا از طرف شهروندان یک دولت صورت گیرند، مسؤولیتی برای آن دولت در پی خواهد داشت. به همین دلیل از مسؤولیت بین‌المللی دولت در موارد متعدد سخن گفته شده است. بحث حقوقی در ارتباط با مسؤولیت بین‌المللی دولت در مواد ۱ و ۲ طرح کنوانسیون مسؤولیت بین‌المللی دولت به این شرح آمده است:

ماده ۱– هر فعل متخلفانه بین‌المللی دولت موجب مسؤولیت بین‌المللی آن دولت می‌شود، یعنی نقض مقررات حقوق بین‌الملل توسط یک دولت موجبات مسؤولیت بین‌المللی آن دولت خواهد بود (ابراهیم گل، ۱۳۹۰: ۲۶). این اصل در مواردی که اعمال دولت باعث تهدید و تخریب منابع یک کشور شود، مشمول اصل توسل به زور تلقی می‌گردد که مسؤولیتی برای دولت ایجاد کرده و جبران خسارت از سوی دولت مهاجم بخشی از این رویکردهای حقوقی است. در همین راستا دیوان دائمی دادگستری بین‌المللی اصل مندرج در ماده ۱ را در تعداد زیادی از قضایایی که در آن دیوان مطرح شده اعمال کرده است، دیوان در قضیه مراکش بیان داشته است، زمانی‌که دولتی علیه دولت دیگر مرتکب فعل متخلفانه بین‌المللی می‌شود بلافاصله بین آن دو دولت رابطه مسؤولیت بین‌المللی ایجاد می شود. همچنین دیوان بین‌الملل دادگستری در قضیه کانال کورفو و قضیه فعالیت‌های نظامی و شبه نظامی ایالات متحده آمریکا در نیکاراگوئه و قضایای دیگر به این اصل استناد نموده

است.[۱] همچنین دیوان در قضایای جبران خسارات، تفسیر معاهدات صلح، مرحله دوم نظریه مشورتی خود بیان داشته است که عدم ایفای یک تعهد معاهداتی، مسؤولیت بین‌المللی درپی خواهد داشت.[۲] یکی از مواردی که مسؤولیت بین‌المللی دولت را ایجاد می‌کند، حملات سایبری است که به هر حال بر مبنای نظریه مشورتی، عدم پایبندی به تعهدات دولت در قبال تعامل سازنده با سایر دولت‌ها در نظام بین الملل است.

اما در ارتباط با بیان فعل متخلفانه دولت به‌نحوی باعث خروج از تعهدات و وظایف آن شده و این ترک فعل منجر به خسارت یا زیان به دیگری شود، اصولی بیان شده است که در ارتباط با حملات سایبری به‌مثابه نقض تعهدات یک دولت و خسارت به دیگری نمود پیدا می‌کند. در همین راستا، ماده ۲ مقرر داشته است: فعل متخلفانه بین‌المللی دولت هنگامی محقق می‌شود که رفتاری اعم از فعل یا ترک فعل. در این ماده دو اصل و یا رویکرد نیز قابل طرح است: الف) به موجب حقوق بین‌الملل قابل انتساب به آن دولت باشد. ب) نقض تعهد بین‌المللی آن دولت محسوب شود. همچنان که نقش نهادهای بین‌المللی در این زمینه ازجمله در عرصه مقابله با حمله به زیرساخت‌های حیاتی نیز مهم است که محور مباحث آتی خواهد بود.

۲- حملات سایبری به زیرساخت‌های حیاتی و نقش دولت‌ها

دولت‌ها به‌عنوان اصلی‌ترین بازیگران بین‌المللی نقش مهمی در حمایت از زیرساخت‌های حیاتی خود درصورت وقوع حمله سایبری یا رعایت مقرراتی برای جلوگیری از تعرض یا حمله و وارد کردن خسارت به سایر بازیگران دولتی و غیر دولتی دارند که به برخی از این مسؤولیت‌های حقوقی اشاره می‌شود.

۲-۱- مسؤولیت یک کشور در ارتباط با اعمال دولت دیگر در حملات سایبری

حسب اصول اولیه و اساسی حقوق بین‌الملل هر دولتی مسؤول رفتار و عملکرد متخلفانه بین‌المللی خود خواهد بود، یعنی زمانی که کشوری با رفتارش یک تعهد بین‌المللی را نقض نموده و این عمل قابلیت انتساب به آن دولت را داشته باشد، از این اصل تحت عنوان اصل مسؤولیت مستقل نیز یاد می‌شود با این وجود رفتار متخلفانه بین‌المللی اغلب موارد ناشی از همکاری چند دولت انجام می‌شود تا یک دولت مستقل لذا ماده ۱۶ طرح مسؤولیت بین‌المللی دولت برهمین مبنا و ضع گردید که در آن دولتی به‌منظور ارتکاب فعلی متخلفانه توسط دولت دیگر به او کمک و مساعدت می‌کند (ابراهیم گل، ۱۳۹۰: ۱۱۵). با این حال و در راستای تشریح بیشتر این بحث، ماده ۱۶ درخصوص کمک یا مساعدت در ارتکاب فعل متخلفانه بین‌المللی مقرر می دارد:

دولتی که در ارتکاب فعل متخلفانه بین‌المللی توسط دولت دیگر به او مساعدت یا کمک می‌کند درصورت وجود شرایط زیر مسؤولیت بین‌المللی دارد:

الف- آن دولت با آگاهی از شرایط فعل متخلفانه بین‌المللی به این کار اقدام کند؛ و

ب- فعل مزبور اگر توسط خود آن دولت هم ارتکاب می‌یافت، فعل متخلفانه بین‌المللی محسوب می‌شد.

یکی از موارد مهم نقض تعهد بین‌المللی، تعهد عدم توسل به زور در روابط بین‌المللی است که ممنوعیت توسل به زور هم در مواد منشور ملل متحد تصریح شده[۳] و هم در حال حاضر بعنوان یک «قاعده آمره بین‌المللی»[۴] از سوی همه کشورها تلقی می‌شود. بنابراین اگر کشوری متوسل به زور و تجاوز علیه کشور دیگر گردد در این صورت مسؤولیت مستقل آن دولت را درپی خواهد داشت، حال ممکن است کشورهای دیگر، آن کشور متجاوز را در اعمال متخلفانه‌اش کمک، مساعدت و یاری نمایند، باز در این صورت، مسؤولیت جبران خسارت را بر عهده خواهد داشت. بدین ترتیب باید گفت که در حملات سایبری، اگر فعل متخلف یک دولت در قالب نقض اصول و قواعد

---

[۱] – به نقل از:
Military and Paramilitary Activities in and against Nicaragua, Merits, Reports 1949. P. 174 -

- Interpretation of Peace Treaties wich Bulgaria, Hungary and Romania, Second Phase, I.C.J. Reports 1950, P. 221

[۳]– از جمله بند ۴ ماده ۲ منشور ملل متحد.

[2] - Jus Cogens

بین‌المللی انجام شود، مسؤولیت جبران خسارت نیز بر عهده دولت متجاوز خواهد بود.

این موضوع درباره حملات سایبری به میزانی که خسارت ایجاد می‌کنند، صادق است. همچنان که در نظر گرفتن حملات سایبری به‌عنوان عاملی برای بروز خسارت نیازمند تلقی آنان در قالب جنگ سایبری است یا حتی حملاتی است که منجر به بروز خسارت مالی و جانی به طرف مقابل شود. زیرا در تعریف حمله سایبری نیز همین موارد مدنظر قرار گرفته است. بخشی از تجهیزات و ابزارهایی که با استفاده از رایانه یا ابزارهای الکترونیکی منجر به خسارت فیزیکی و غیر مستقیم می‌شود در این دسته جای می‌گیرند. اگر درگیری میان بازیگران ملی یا غیرملی با هدف ورود خسارت باشد و منجر به خسارت فیزیکی به تجهیزات یا افراد یا خرابکاری یا خسارت مستقیم به سامانه‌های اطلاعاتی حساس و استراتژیک شود، بخشی از حملات سایبری محسوب می‌شوند (Stefano, 2013: 9). در این صورت توسل به زور، نقض مسؤولیت و تعهد دولت و همچنین بر عهده گرفتن مسؤولیت برای پذیرش جبران خسارت، ازجمله اصول حقوقی برای رفع مشکلات و پیامدهای ناشی از حملات سایبری خواهد بود.

۲-۲- جرم‌انگاری حملات سایبری و مسؤولیت دولت

همان طور که گفته شد مسؤولیت بین‌المللی یکی از اصول اساسی حقوق بین‌الملل است که در اثر ماهیت سیستم حقوقی بین‌المللی و دکترین حاکمیت و ثبات کشورها رشد کرده است، طبق این سیستم هرگاه یک تابع حقوق بین‌الملل یک عمل متخلفانه و یا غیر قانونی بین‌المللی علیه تابع دیگر حقوق بین‌الملل مرتکب شود مسؤولیت بین‌المللی بین آن دو برقرار می‌شود و درصورتیکه یک تعهد بین‌المللی نقض شود باید غرامت پرداخت شده و جبران خسارت شود (Fitzmaurice and D.Sarooshi, 2003: 14). از این منظر، فعل دولت یک جرم تلقی شده و برای مقابله با این جرم، جبران خسارت تعبیه شده است. زیرا پیامدهای ناشی از حملات سایبری منجر به خسارت مادی و معنوی به دولت زیان دیده شده و باید به‌نحوی جبران شود.

ماهیت اساسی مسؤولیت بین‌المللی بر مبنای چند عنصرشکل گرفته است، اول وجود یک تعهد حقوقی بین‌المللی بین دو تابع حقوق بین‌الملل، دوم وقوع یک فعل یا ترک فعل که آن تعهد را نقض کرده باشد و قابلیت انتساب به دولت مسؤول را داشته باشد و در آخر، از دست دادن و یا وقوع خسارتی در اثر یک فعل یا ترک فعل غیر قانونی رخ داده باشد. در همین راستا نیز می‌توان گفت که دیوان در رأی ماهیتی خود به سال ۱۹۲۸ بیان نمود که: اصل مهمی در رویه بین‌المللی و به‌ویژه تصمیمات دیوان‌های داوری و مراجع قضایی بین‌المللی بر آن تاکید شده است این است که جبران خسارت باید تا جایی که همه آثار آن عمل غیر قانونی را پاک نماید ادامه پیدا کرده و وضعیتی را بوجود آورد که اگر آن عمل خلاف حقوق بین‌الملل اتفاق نمی‌افتاد، آن وضع وجود نمی‌داشت؛ مانند برگرداندن عین پا پرداخت غرامت و جبران خسارات، این موارد معیارها و اصولی هستند که درصورت وقوع یک عمل خلاف حقوق بین‌الملل و ورود خسارت باید از آنها الهام گرفت (فیوضی، ۱۳۷۹: ۳۱۴). در اینکه مبنای مسؤولیت تئوری خطا و تقصیر است یعنی مبنای مسؤولیت ذهنی می‌باشد یعنی همین که یک عمل خلاف حقوق بین‌المللی صورت گرفت صرف‌نظر از اینکه سوء نیت و تقصیر در ارتکاب وجود داشته یا نه دولت مسؤول خواهد بود و یا اینکه مبنی تئوری خطر و ریسک است یعنی مبنای مسؤولیت عینی می‌باشد باید سهل‌انگاری و تقصیر دولت ثابت شود تا مسؤولیت آن دولت مستقر گردد.

اما برای رسیدگی به موارد مشابه در این باره، نظرات متفاوتی ارائه شده است و دیوان‌های داوری و مراجع قضایی در هر مورد آراء متفاوتی صادر نموده‌اند، هرچند که در بسیاری از موارد مراجع فوق تمایل خود را نسبت به اعمال تئوری عینی یعنی مسؤولیت مطلق نشان داده‌اند (Brownlie, 1983: 573). اما با این وجود، بحث جبران خسارت هم در طرح مسؤولیت بین‌المللی دولت از مواد ۳۱ تا ۳۹ و هم در طرح مسؤولیت سازمان‌های بین‌المللی از مواد ۳۱ تا ۴۰ به‌طور مفصل آمده است، به علت اینکه مفاد مواد این دو طرح در بسیاری از موارد عیناً مطابق یکدیگر بوده فقط به جای دولت، سازمان بین‌المللی لحاظ شده است لذا به خاطر تقدم تدوین در بررسی‌های آتی بیشتر استناد به طرح مسؤولیت دولت درخصوص جبران

خسارت خواهد بود که قابل اطلاق به حملات سایبری و نقض تعهدات دولت‌ها به‌عنوان اعضای منشور ملل متحد و یا مواردی ازجمله رعایت مسؤولیت بین‌المللی دولت خواهد بود. به هر حال، جرم‌انگاری حملات سایبری هم در قالب منشور سازمان ملل متحد و اصل ۵۱ و هم در قالب سایر اسناد بین‌المللی قابل بررسی است. ازجمله می‌توان به ماده ۳۶ پروتکل الحاقی کنوانسیون ۱۹۴۹ ژنو اشاره نمود. در این راستا و بر مبنای تفاسیر موجود از ماده ۳۶ پروتکل الحاقی یکم، چهار رکن ماده مزبور به همین موضوع اختصاص داده شده است. ازجمله می توان به کشورهای مشمول بررسی، سلاح‌های مشمول بررسی، مقررات حاکم بر بررسی و فعالیت‌ها پس از بررسی حقوقی است. اطلاع داشتن از این ارکان، به بررسی و رسیدگی حقوقی برای قابلیت‌های فضای سایبری ذیل ماده ۳۶ پروتکل الحاقی کمک می‌رساند (شریفی طراز کوهی، ۱۳۹۹: ۱۲۴).

علاوه‌بر بحث جرم‌انگاری و جبران خسارت در حملات سایبری، مسؤولیت تضامنی یا ثانوی پشتوانه اعاده و جبران خسارت برای دولت قربانی یا زیان دیده ناشی از حملات سایبری است. در این راستا باید گفت که مبنای رژیم مسؤولیت تضامنی یا متقارن این است که کشور زیان دیده از عمل یک سازمان بین‌المللی حق خواهد داشت که به انتخاب خود برای جبران خسارت یا اقامه دعوا به سازمان یا اعضای آن و یا همزمان به هر دوی آنها مراجعه نماید، هدف از تبیین چنین رژیمی این است که کشور متضرر فرصت جبران خسارت از ناحیه سازمان بین‌المللی را داشته و از این طریق استقلال شخصیت حقوقی آن سازمان نیز حفظ خواهد شد و از طرف دیگر چنانچه سازمان بین‌المللی توان جبران خسارات را نداشته یا از پرداخت غرامت خودداری ورزد، کشور زیان دیده بدون جبران رها نشده که این مطلب با این اصل حقوقی که هیچ خسارتی نباید بدون جبران باقی بماند سازگارتر است (زمانی، ۱۳۸۷: ۱۷۸-۱۷۷). به همین دلیل جبران خسارت هم از جنبه حقوقی و هم از جنبه جرم‌انگاری و مطابق اصول و قواعد بین‌المللی، راهی برای اعاده حیثیت، جبران خسارت و تلفات برای دولت زیان‌دیده و قربانی و همچنین اثبات و نشان دادن مسؤولیت دولت‌ها نسبت به تعهدات خود در عرصه بین‌المللی است.

۳- حملات سایبری به زیرساخت‌های حیاتی و نقش نهادهای بین‌المللی

وجه مهم و بارز حقوق سایبری معطوف به نقش سازمان‌های بین‌المللی ازجمله منشور ملل متحد است که از دیرباز به عدم مداخله، استقلال و صلح و امنیت بین‌المللی توجه نشان داده و در قبال حمله به زیرساخت‌های حیاتی، اقداماتی حقوقی در نظر گرفته است. در این صورت، هر نوع تهدیدی که اهداف یاد شده را با خطر روبه‌رو سازد، مشمول قوانین بین‌المللی شده و نیازمند رسیدگی حقوقی است. در همین راستا نیز سازمان‌های بین‌المللی ازجمله نهادهایی هستند که به‌صورت غیر مستقیم و در برخی موارد به‌طور مستقیم تحت تأثیر حملات سایبری قرار می‌گیرند. به این دلیل که سازمان‌های یاد شده چیزی جز تشکیل اعضای خود نیستند و هنگامی که اعضا مورد تهدید سایبری واقع می‌شوند، سازمان‌ها نیز برای حمایت از اعضا یا حل مشکلات میان آنان وارد عمل شده و از منظر حقوقی نسبت به آن ورود می‌کنند. لذا با توجه به اهداف اصلی و وظیفه‌ای که در مقابل اعضاء خود دارند، در صدد آنند که چاره‌ای برای مقابله با اینگونه حملات بیاندیشند که در ذیل به برخی از آنها اشاره می‌گردد.

۳-۱- سازمان ملل متحد

با شروع قرن بیست و یکم، سازمان ملل سعی کرده اهداف اولیه خود؛ یعنی ایجاد تعامل بین دول و ملل جهان؛ را عملی و جدی‌تر سازد و به همین دلیل مبادلات علمی، فرهنگی و ارتباطات را ابزار مؤثری در راه دستیابی به صلح، امنیت و توسعه بین‌المللی می‌داند و به همین منظور نه‌تنها یک «اتحادیه بین‌المللی ارتباطات» تأسیس شده، بلکه سایر ارکان و کارگزاری‌های این سازمان نیز در توسعه ارتباطات بین‌المللی فعالیت شایانی داشته‌اند (Burkadze, 2020: 12). از آنجایی که در دو دهه اخیر حملات سایبری، مهم‌ترین هدف سازمان ملل متحد؛ که همانا صلح و امنیت بین‌المللی بوده؛ را به مخاطره انداخته است، لذا ارکان سازمان ملل نیز ساکت نبوده و از طریق مجمع عمومی و شورای امنیت و دیگر سازمان‌های وابسته به

تحقیق و پژوهش و اقدام در مقابل ناامنی سایبری در سطح جهانی پرداخته‌اند.

مجمع عمومی تاکنون چندین قطعنامه[۱] در این خصوص صادر نموده که البته دارای ابهاماتی نیز بوده‌اند. در ماه اوت سال ۱۹۹۹، سازمان ملل متحد یک نشست بین‌المللی تحت عنوان " درک مفاهیم امنیت اطلاعاتی در حال ظهور" در ژنو با حضور کارشناسان خبره برگزار نمود و به دنبال آن در سال ۲۰۰۲ قطعنامه مجمع عمومی درخصوص " تحولات در زمینه اطلاعات و ارتباطات از راه دور در حوزه امنیت بین‌المللی" را صادر نمود که البته مقدار کار انجام شده بر روی آن بسیار کم بود و در پی آن اجلاس جهانی جامعه اطلاعاتی برگزار گردید. این سازمان در سال ۲۰۱۰ یک گام بزرگ به جلو برداشت و دبیر کل سازمان ملل متحد از متخصصان امنیت سایبری پانزده کشور برتر سایبری دعوت نمود تا همایشی با عنوان " ارائه مجموعه‌ای از توصیه‌های ابتدایی در جهت ساخت چارچوب بین‌المللی برای امنیت و ثبات" بر گزار نمایند. دستور جلسه برای این همایش عبارت بود از:

– تبادل نظر میان کشورهای حاضر در جلسه پیرامون موضوع مطروحه؛

– اعتماد سازی، ثبات و اقدامات احتیاطی جهت کاهش خطر و تبادل دیدگاه‌های ملی در استفاده از فن‌آوری اطلاعات و ارتباطات در جنگ؛

– ظرفیت سازی در کشورهای کمتر توسعه یافته و اقدامات لازم برای حمایت از آن‌ها؛

– ارائه تعریفی واحد از مفاهیم بنیادین.

تلاش‌های مذکور توسط سازمان ملل متحد نشان دهنده پیشرفت تدریجی در غلبه بر ابهامات موجود در استفاده از فضای سایبر می‌باشد (Hathaway, 2012: 34). به‌علاوه اینکه یکی دیگر از ارکان سازمان ملل متحد که در رابطه با حملات سایبری و ارتباطات، صلاحیت اظهارنظر و تصمیم گیری دارد، شورای امنیت است که در ادامه بررسی می‌گردد.

با توجه به گسترش استفاده از رسانه‌ها و فناوری‌های نوین همچون پهپادها، این فناوری‌ها به همان نسبت که می‌تواند در جهت حفظ صلح به کار آیند، می‌توانند موجب تهدید صلح نیز باشند (نورمحمدی و طالبی آرانی، ۱۳۹۶: ۸۵)، چراکه همان‌گونه که کشورها با استفاده از این رسانه‌ها و فناوری‌ها می‌توانند باعث نزدیک شدن روابطشان شوند، ممکن است کشوری مجهز به ابزار نوین اطلاع رسانی باشد و ضمن به‌کارگیری آن، امنیت ملی کشورهای دیگر را با تهدید مواجه کند، به گونه‌ای که وضعیتی تحمل ناپذیر برای آنان فراهم آورد. در حقیقت چنین کشوری فروپاشی صلح را هدف قرار داده، چراکه این امر جز تهدید صلح جهانی، مفهوم دیگری نخواهد داشت. در چنین شرایطی شورای امنیت می‌تواند وضعیت را به‌عنوان بحرانی در روابط بین‌الملل به گونه‌ای که احتمالاً بروز جنگ را قریب‌الوقوع نموده است تعریف کند و آن را مشمول ماده ۳۹ منشور به‌شمار آورد.

بنابراین می‌توان این‌گونه برداشت کرد که طبق ماده ۳۹ منشور اگر دولتی به واسطه رسانه‌ها و فناوری‌های اطلاع رسانی، باعث ایجاد بحران و تنش جدی بین خود و سایر دولت‌ها شود و امنیت بین‌المللی و جهانی را به مخاطره اندازد، شورای امنیت این اختیار را خواهد داشت که جهت مقابله با این‌گونه تهدیدات، مسؤولیت خود ناشی از فصل هفتم منشور را احراز کرده و با دولت یا دولت‌های خاطی برخورد جدی داشته باشد (طیبی و همکاران، ۱۳۹۸: ۱۶). در این رویکرد تهدید صلح و امنیت بین‌المللی یک خطر جدی است و گروهها یا دولت‌هایی که با اقدامات خود ازجمله حملات سایبری برای تهدید دیگری اقدام کنند، مشمول مقررات و قوانین شده و ازجمله می‌توان با استناد به اصل منع توسل به زور به مقابله با آنان برخاست.

یکی دیگر از چالش‌های فناوری‌های نوین، استفاده از این فناوری‌ها جهت اختلال در امنیت بین‌المللی است، چراکه این فناوری‌ها توانایی اثرگذاری بر افکار عمومی را داشته و می‌توانند با تبلیغات، مردم را بر ضد حکومت تحریک کرده و سبب ایجاد اختلاف میان کشورها شود. اگرچه صلاحیت و وظایف برخی از

---

[۱]– از جمله قطعنامه‌های مرتبط با این موضوع، قطعنامه‌های: ۳۲/۵۸، ۶۱/۵۹، ۴۵/۶۰، ۵۴/۶۱، ۱۷/۶۲، ۳۷/۶۳، ۲۵/۶۴، ۲۵۲/۶۰ می‌باشد.

نهادهای حقوقی بین‌المللی در چارچوب تنظیم و ضابطه‌مند کردن حملات سایبری نبوده و نیست اما به‌طور غیرمستقیم می‌توانند بر این پدیده نوین اعمال نظر و یا کارهایی از این قبیل نمایند. مهم‌ترین این قواعد حقوقی عبارتند از: قوانین بین‌المللی حاکم بر ارتباطات راه دور، قواعد حاکم بر حمل و نقل هوایی، قواعد حاکم بر فضا و دریاها. در این صورت نیز نقش شورای امنیت سازمان ملل متحد به‌عنوان نهاد متولی صلح و امنیت بین المللی بسیار برجسته بوده و سازوکارهایی در نظر گرفته است. هرچند باید بیان کرد که این رژیم‌های حقوقی قبل از ظهور حملات سایبری تا حد زیادی شکل گرفته‌اند و به همین دلیل به‌صورت مستقیم رابطه‌ای با تنظیم مقررات در حملات سایبری ندارند اما تجربه حقوق‌دانان و صاحب نظران عرصه بین‌الملل این بوده که می‌توان از کارکرد این‌گونه سازمان‌ها در راستای قاعده‌مند کردن حملات سایبری بهره برد چراکه این سازمان‌ها و نهادها بر حملات سایبری تأثیر دوسویه‌ای دارند به این معنا که از طرفی حملات سایبری بر عملکرد آن‌ها تأثیرگذار می‌باشد و از سوی دیگر این سازمان‌ها می‌توانند بر ضابطه‌مند کردن این‌گونه عملیات نظارت داشته باشند.

۳-۲- «اتحاد بین‌المللی حفاظت از امنیت سایبری» (ICSPA)

در راستای مقابله با تهدیدات و خطرات حملات سایبری نباید از نقش سازمان‌های غیردولتی غفلت ورزید. به این دلیل که افزایش جرایم سایبر، بسیاری از کشورهای جهان را به فکر مقابله جدی‌تر انداخته است. به همین دلیل اکثر کشورها بخش ویژه مبارزه با جرایم و حملات سایبری را راه‌اندازی کرده‌اند. اما تلاش‌های انفرادی نتایج عملی و قابل توجهی در پی نخواهد داشت. لذا به موازات تلاش‌های انفرادی و گروهی در قالب اتحادهای دفاعی–امنیتی، سازمان‌های غیردولتی نیز پا به عرصه مقابله با حملات سایبری نهاده‌اند. یکی از این سازمان‌های نوبنیاد، سازمان غیردولتی «اتحاد بین‌المللی حفاظت از امنیت سایبری» می‌باشد که در سال ۲۰۱۴ میلادی با هدف مبارزه با جرایم سایبری تأسیس شده است (Eichensehr, 2020:19-36). در این سازوکار هم کوشش برای آگاهی افراد و دولت‌ها از حملات سایبری و هم ایجاد یک ائتلاف بین المللی برای مشارکت گروههای غیردولتی برای مقابله با تهدیدات سایبری دیده می‌شود که هریک می‌توانند باعث ایجاد هم افزایی و مشارکت جهانی برای مقابله با تروریسم سایبری شوند که خود بخشی از رویه حقوقی در این زمینه خواهد بود و اقدامات آنان به مرور پشتوانه فرهنگی برای حقوق سایبری در جهان خواهد شد.

مطابق وظایف و اهداف این نهاد غیردولتی، برای مبارزه با جرایم و تروریسم سایبری نیاز است تا قوانین بین‌المللی تازه‌ای برای مبارزه با جرایم سایبری و مجرمین سایبری تعریف گردد و قوانین حمایتی از شرکت‌های تجاری فعال در حوزه فن‌آوری را ارتقاء دهد. ریاست فعلی این سازمان غیردولتی برعهده دیوید بلانکت، وزیر کشور سابق انگلیس است. بودجه این سازمان بین‌المللی را اتحادیه اروپا و دیگر کشورهایی که قصد پیوستن به این نهاد را دارند، تأمین خواهند کرد. اعضای این اتحاد بین‌المللی را دولت‌ها، شرکت‌های اینترنتی و فن‌آوری بین‌المللی و نهادهای قانونی متولی مبارزه با جرایم سایبر ازجمله "پلیس بین‌الملل"(Interpol) تشکیل می‌دهند. اما از جهت مشارکت نهادهای تخصصی در این زمینه، شرکت‌های فعال در زمینه امنیت رایانه‌ای و سایبری ازجمله "مک‌آفی" و "ترند مایکرو" نیز که در زمینه تولید آنتی ویروس‌ها فعال هستند، به عضویت "اتحاد بین‌المللی حفاظت از امنیت سایبر" درآمده‌اند. دلیل اصلی تأسیس این اتحادیه این است که میزان وقوع جرایم سایبری در جهان در سال ۲۰۱۰ نسبت به سال‌های قبل، افزایشی ۹۳ درصدی داشته است و در سال‌های ۲۰۱۱ الی ۲۰۲۱ نیز افزایشی بالغ بر ۴ برابر داشته است.

بخشی از وظایف این سازمان غیردولتی، کمک به کشورهایی خواهد بود که با بیشترین حجم حملات سایبری مواجه بوده و نیاز به کمک‌های مالی و تخصصی سایر کشورها دارند. دست‌اندرکاران تشکیل این سازمان اعلام کرده‌اند که قرار نیست این نهاد فقط مختص به کشورهای اروپایی باشد؛ آن‌ها از همه دولت‌ها می‌خواهند که برای مبارزه با حملات سایبری، به عضویت این نهاد درآیند. بنابراین به مرور و با درک خطرات ناشی از تهدیدات و خطرات حملات سایبری، استفاده از رسانه‌های آزاد و مستقل و آگاهی از طریق شبکه‌های اجتماعی،

نوعی کوشش فرهنگی در سطح جهان شکل خواهد گرفت که نهاد غیردولتی مزبور به دنبال حضور و مشارکت سایر بازیگران دولتی و غیردولتی در این زمینه است.

۳-۳- مقررات بین‌المللی مخابرات راه دور

یکی از سازمان‌های قدیمی و فعال در زمینه مخابرات راه دور، اتحادیه بین‌المللی مخابرات (ITU) است که امروزه در عرصه مبارزه با جرایم سایبری نیز تلاش‌هایی انجام می‌دهد. این اتحادیه از نقطه نظر ساختار وظیفه‌ای از سه بخش استانداردسازی مخابرات، ارتباطات رادیویی و توسعه مخابرات تشکیل گردیده است. از آنجایی‌که یکی از عمده‌ترین زیرساخت‌های این اتحادیه مرتبط با فناوری اطلاعات و فضای سایبر می‌باشد، حملات سایبری می‌تواند هم از طریق امکانات این سازمان انجام گردد و هم بر عملکرد این سازمان تأثیرگذار باشد. لذا این اتحادیه نیز به‌طور غیرمستقیم می‌تواند و در برخی موارد بایستی به قضیه مطروحه وارد شده و تمام جوانب این‌گونه عملیات را بررسی نموده و درصورت لزوم به تدوین قواعد مختلف مرتبط با دسترسی به فضای سایبر بپردازد. در این زمینه و در راستای تشریح اقدامات این نهاد غیردولتی باید گفت که اگر و درصورت اخلال در پخش برنامه‌های رادیویی یا مخابراتی توسط یک عضو یا غیرعضو، اعم از دولتی یا غیردولتی، دبیر کل این اتحادیه می‌تواند طبق اساسنامه، اقداماتی درخصوص شخص خاطی اتخاذ نماید. البته باوجود محدودیت‌های فوق، اساسنامه این اتحادیه به‌طور خاص استفاده از ارتباطات راه دور برای مقاصد نظامی را منع نکرده است. لذا به نظر می‌رسد که حملات سایبری نیز شامل این عدم ممنوعیت باشد اما با توجه به اهداف موجود در حملات سایبری، می‌توان گفت که اگر یک حمله سایبری در چارچوب یک حمله نظامی بوده باشد این سازمان با قوانین فعلی نمی‌تواند بر روی آن اعمال نظر نماید اما اگر به‌صورت غیرقانونی انجام شده باشد قضیه متفاوت بوده و اتحادیه می‌تواند به دلیل "تداخل مضر در مخابرات" به خاطی هشدار دهد. بنابراین حیطه اختیارات این نهاد به‌نحوی است که با هشدار به طرف خاطی و یا مهاجم، نقشی پیشگیرانه ایفا کرده و از بروز یک خطر جدی جلوگیری می‌کند. ضمن اینکه فعالیت مخابرات بین‌المللی از راه دور از جهت شناسایی عامل یا عاملین در حملات سایبری بسیار مهم و حیاتی است که درصورت ارجاع یک پرونده مرتبط با حملات سایبری می‌توان از داده‌های آن در راستای شناسایی عاملین حملات سایبری بهره برد. در این صورت به نظر می‌رسد حضور در این نهاد و ایفای نقشی مهم و پررنگ‌تر توسط آن خواهد توانست بخشی از پیچیدگی‌های ناشی از حملات سایبری را حل نماید. در این باره باید اشاره کرد که تاکنون چندین بار این اتحادیه سعی نموده که به‌صورت مستقیم به قضیه اینترنت و فضای سایبر ورود کرده و بخشی از آن را تحت مدیریت خود قرار دهد که با مخالفت دولت‌هایی همچون آمریکا و انگلیس و شرکت‌هایی همچون"آیکان"(ICAN) مواجه شده است.[1] به هر حال اگر بتوان نقش مؤثر و در حال گسترش نهاد اخیر را در راستای مقابله با حملات سایبری یا دریافت اطلاعات جهت شناسایی حملات سایبری به کار گرفت، پی بردن به حملات سایبری از حیث حقوقی و توجه به جبران خسارت نیز گسترش خواهد یافت.

۳-۴- قواعد حمل و نقل هوایی

برای جلوگیری از خسارت و یا حمله به زیرساخت‌های حیاتی، تلاش برخی از دولت‌ها این بوده است تا از قواعد حقوق فضایی برای مقابله با تهدیدات سایبری بهره ببرند. اگر بتوان این قواعد را به عرصه فضای مجازی و سایبری تسری داد، سازوکار حقوقی دیگری برای شناسایی حملات سایبری و جبران خسارت برای دولت قربانی فراهم خواهد شد. به هر حال باید گفت که ازجمله پدیده‌های نوین در عرصه فناوری اطلاعات، "اینترنت اشیاء" **(IOT)** می‌باشد. این فناوری تأثیرات زیادی بر روی کار و زندگی بشر ایجاد نموده است. هر دستگاهی که قابلیت ارتباط با اینترنت یا یک دستگاه دیگر را داشته باشد یک نوع IoT است. همه دستگاه‌ها ازجمله گوشی‌های هوشمند، ماشین‌های لباس‌شویی، یخچال‌ها و سایر تکنولوژی‌های پوششی در حال حاضر توان بالقوه ارتباط با اینترنت یا دستگاه

---

[1]- THE WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS,Dubai, 2012:14(

دیگر را دارا هستند و همه این‌ها در بستری در شبکه قرار خواهند داشت که مبنای "اینترنت اجسام و اشیاء" را تشکیل می‌دهند.

هم‌اکنون حجم بسیار بالایی از سیستم‌های تکنولوژیک در حال کار، از آدرس‌های IP استفاده می‌کنند تا قادر به دسترسی از خارج شبکه باشند. به این ترتیب نه‌تنها یک اداره یا نهاد به تنهایی می‌تواند هدف یک حمله سایبری قرار گیرد، بلکه از این طریق کل یک زیرساخت همچون شبکه حمل و نقل هوایی یا شبکه انتقال برق و سایر سیستم‌های اتوماسیون می‌تواند مورد حمله و سوءاستفاده قرار بگیرد.

امروزه صنعت حمل و نقل هوایی بدون سیستم‌های مخابراتی و سایبری قابلیت استفاده ندارند لذا برخی از هکرها و یا اشخاص خاص این بخش را هدف خود برای حملات سایبری قرار داده‌اند که در مقابله با این‌گونه حملات، نظام حقوقی بین‌المللی در سه بخش بر اعمال غیرقانونی این‌چنینی قابل اعمال می‌باشد:

کنوانسیون ۱۹۴۴ هواپیمایی کشوری (Convention on International Civil Aviation, 1944:2)، کنوانسیون ۱۹۷۱ در جلوگیری از اعمال غیرقانونی علیه حمل‌ونقل هوایی (کنوانسیون مونترال (Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 1971:4)، و پروتکل ۱۹۸۸ برای جلوگیری از اعمال غیرقانونی خشونت‌آمیز در فرودگاه‌هایی که در خدمت هواپیمایی کشوری می‌باشند (پروتکل مونترال) Protocol for the Suppression of Unlawful acts of Violence at Airports serving international civil aviation, 1988:5).

با توجه به اینکه احتمالاً حملات سایبری به خصوص به روش "اینترنت اجسام و اشیا" به بخش حمل و نقل هوایی زیاد شده و شاید رژیم حقوقی فعلی کارآیی کافی نداشته باشد. لذا در دهه اخیر چندین جلسه و کنفرانس توسط گروه حمل و نقل هوایی بین‌المللی برای مبارزه با جرایم سایبری تشکیل گردیده و در نهایت یک توافق‌نامه امضا کرده‌اند تا راهکارهای مبارزه با این شیوه جدید هک و مقابله با حوادث احتمالی پیش آمده و کنترل آن را پیدا کنند (Hathaway, 2012: 37). بدین ترتیب اگر بتوان از قواعد حقوقی مرتبط با هوا و فضا در زمینه مقابله با حملات سایبری بهره برد، یک رویه حقوقی دیگری برای مقابله با حملات و خطرات ناشی از تهدیدات سایبری ایجاد خواهد شد که در نهایت به یک تلاش بین المللی دیگر منجر خواهد شد.

۳-۵- رژیم حقوقی بین‌المللی فضای ماوراء جو

حقوق فضا به‌عنوان جدیدترین شاخه از دانش حقوق بین‌الملل با توسعه خیره کننده علمی و فنی از همان ابتدای تشکیل و تکامل، با سؤالات مهم و بنیادین چندی از قبیل تعیین مرز هوا و فضا، تعیین وضعیت حقوقی اشیاء هوا-فضایی و پیشگیری از گسترش مخاصمات مسلحانه به فضای ماورای جو مواجه بوده است. اما بدون تردید یکی از مهم‌ترین این چالش‌ها تعیین حدود حاکمیت دولت‌ها در پهنه بیکران فضای ماورای جو است.

چالش مذکور از آن رو قوت می‌گیرد که اصل منع تصاحب، تملک و تصرف فضا و ممنوعیت طرح هرگونه ادعای حاکمیت بر قلمرو در معنای سنتی آن، یکی از اصول بنیادین و پذیرفته شده حاکم بر کاوش و بهره‌برداری از فضا است. با توجه به اینکه، حملات سایبری می‌تواند بر روی اجسام فضایی همچون ماهواره‌ها و ارتباطات راه دور اجسام فضایی تأثیر گذار باشد، لذا برخی از محققین بر این باور هستند که معاهدات مربوط به حقوق فضا برای حملات سایبری قابل اعمال می‌باشند اما به نظر می‌رسد در این بخش از حقوق بین‌الملل نیز کمبود قوانین مرتبط با حملات سایبری احساس می‌شود (جعفری، ۱۳۹۴: ۷۰). در کنار معاهداتی همچون معاهده فضای ماورای جو ۱۹۶۷ که فقط به فعالیت‌های فضایی و فضای ماورای جو اختصاص داشته است، جامعه بین‌المللی توافق‌نامه‌ها و معاهدات دیگری را نیز ایجاد کرده‌اند که گاهی حاوی مواد و نکات مهمی در مورد فعالیت‌های فضایی و فضای ماورای جو می‌باشند، که می‌توان از این میان به یکی از مهم‌ترین آن‌ها یعنی ممنوعیت استفاده نظامی یا هرگونه استفاده خصمانه از فنون تعدیلات محیطی، استفاده از این شیوه‌ها را با هدف تغییر در دینامیک، ترکیب یا ساختار فضای ماورای جو ممنوع می‌کند. کنوانسیون مخابرات بین‌المللی نیز حاوی موادی در ارتباط با مخابرات فضایی است. با این حال، نباید پنداشت که کنوانسیون‌ها و معاهدات یاد شده نیاز جامعه بین‌المللی را به استمرار در

قانون‌سازی و قانون‌گذاری در زمینه‌های فضای ماورای جو و فعالیت‌های فضایی برآورده کرده است. حتی با پیشرفت قابل توجه در این زمینه نیز بسیاری از مسائل حل نشده باقی می مانند (Bada, & Nurse, 2012: 34). اما به هر حال قوانین یاد شده در عرصه فعالیت‌های فضایی یا قوانینی که به آسمان کشورها در سطح داخلی و مخصوصاً بین‌المللی مربوط است، نقش مهمی در ایجاد یک سازوکار حقوقی جهت بررسی مسائل و چالش‌های پیش‌روی حملات سایبری خواهند داشت. به‌طور ساده باید گفت که اگر حملات سایبری به‌طور نامحسوس وارد حریم و حاکمیت یک کشور شوند، قوانین فضایی می‌توانند نسبت به حمل قوانین این عرصه بر حملات سایبری برخوردار هستند یا اینکه از چنین ظرفیتی برخوردار نیستند. بر این اساس باید گفت که قوانین ارتباط از راه دور، حمل و نقل هوایی، رژیم حقوقی حاکم بر پروازها و... یا قوانینی که در حوزه ارتباطات هستند، از چنین ظرفیتی برای تحلیل وضعیت حملات سایبری برخوردار هستند.

با نگاهی اجمالی به قوانین بین‌المللی حاکم بر ارتباطات راه دور، حمل و نقل هوایی، فضا، و دریا، که در بالا اشاره کوتاهی به آن‌ها شد می‌توان به این نتیجه رسید که برخی از مفاد قانونی در این حوزه‌ها، ابزار بالقوه مؤثری برای مقابله با برخی از انواع حملات سایبری که در حوزه‌های مربوطه اتفاق می‌افتد کاربرد دارند با این حال هیچ یک مکانیسم منسجمی برای مقابله با حملات سایبری را فراهم نمی‌نمایند بنابراین باز هم به این نتیجه می‌رسیم که نیاز به قوانین منسجم و یکپارچه‌ای در این خصوص حس می‌شود (جعفری،۱۳۹۸:۲۱۳). بنابراین باید گفت که مباحث حقوقی مرتبط با جرایم سایبری هنوز در ابتدای راه است، اما با توجه به سرعت تحول در ابزارها و خطرات ناشی از حملات سایبری، تجمیع رویکردهای حقوقی برآمده از فعالیت بازیگران دولتی، نهادهای بین‌المللی و نهادهای غیردولتی می تواند زمینه را برای ایجاد یک سازوکار حقوقی مدون جهت شناسایی، مقابله و پیشگیری از حملات سایبری ارائه نماید.

نتیجه‌گیری

حملات سایبری به زیرساخت‌های حیاتی، یکی از مهم‌ترین چالش‌های امنیتی عصر حاضر است که می‌تواند تبعات جبران‌ناپذیری بر امنیت، اقتصاد و ثبات کشورهای مختلف و حتی امنیت بین‌المللی داشته باشد. در این میان، دولت‌ها به‌عنوان اصلی‌ترین بازیگران عرصه بین‌الملل، نقش کلیدی و بی‌بدیلی در حفاظت از این زیرساخت‌ها و همچنین پیشگیری و مقابله با حملات سایبری بر عهده دارند. براساس اصول بنیادین حقوق بین‌الملل، هر دولت مسؤول رفتارهای خود و اعمالی است که به آن نسبت داده می‌شود و درصورت ارتکاب عمل متخلفانه یا نقض تعهدات بین‌المللی، مسؤول جبران خسارات ناشی از آن خواهد بود. حتی در شرایطی که دولت‌ها در ارتکاب یک عمل متخلفانه همکاری یا مساعدت کنند، براساس ماده ۱۶ طرح مسؤولیت بین‌المللی دولت‌ها، مسؤولیت مشترک برای جبران خسارت بر عهده آنان قرار می‌گیرد. این اصل به‌ویژه در مواردی که حملات سایبری به زیرساخت‌های حیاتی منجر به خسارات مالی، جانی یا تخریب فیزیکی شود، اهمیت و کاربرد بیشتری پیدا می‌کند.

مسأله توسل به زور، به‌خصوص در قالب حملات سایبری که آثار ویرانگر فیزیکی یا اقتصادی برجای می‌گذارند، یکی از موارد بارز نقض تعهدات بین‌المللی است که در منشور ملل متحد و قواعد آمره بین‌المللی منع شده است. بنابراین، هرگونه حمله سایبری که ماهیت تجاوز یا استفاده از زور داشته باشد، نه‌تنها مسؤولیت حقوقی و بین‌المللی برای دولت مهاجم ایجاد می‌کند، بلکه جبران خسارات وارده نیز از اصول اساسی حاکم بر روابط بین‌الملل محسوب می‌شود. در بحث جرم‌انگاری حملات سایبری نیز، مسؤولیت بین‌المللی دولت‌ها یک اصل پایه و اساسی است که بر مبنای آن، هر عمل متخلفانه‌ای که منجر به نقض تعهدات و وارد آمدن خسارت شود، جرم تلقی شده و مستلزم جبران خسارت است. این مسؤولیت حتی در مواردی که سوءنیت یا تقصیر اثبات نشود، براساس نظریه مسؤولیت مطلق (مسؤولیت عینی) نیز اعمال می‌شود. همچنین، در موارد پیچیده‌تر، نهادهای بین‌المللی و دیوان‌های داوری نیز به‌صورت موردی و براساس شواهد و معیارهای حقوقی، تصمیمات متناسبی برای جبران خسارت و تعیین مسؤولیت صادر می‌کنند.

سازمان ملل متحد به‌عنوان مهم‌ترین نهاد بین‌المللی با هدف حفظ صلح و امنیت جهانی، در طول سال‌های اخیر تلاش‌های چشمگیری در جهت تنظیم و تدوین چارچوب‌های حقوقی و سیاسی مرتبط با امنیت سایبری انجام داده است. برگزاری نشست‌ها و همایش‌های تخصصی، تصویب قطعنامه‌ها، و ایجاد بسترهای تعامل بین دول عضو، ازجمله اقداماتی است که این سازمان به‌منظور مقابله با تهدیدات سایبری در پیش گرفته است. با این وجود، چالش‌های ناشی از پیچیدگی و ابهامات فضای سایبری و تفاوت دیدگاه‌ها میان کشورها، اجرای کامل و مؤثر این قوانین را با محدودیت‌هایی مواجه ساخته است. شورای امنیت سازمان ملل نیز، به‌عنوان نهادی مسؤول در مقابله با تهدیدات علیه امنیت بین‌المللی، می‌تواند در شرایط بحرانی و خطرناک وارد عمل شده و با استناد به مفاد منشور ملل متحد، اقدامات لازم را برای مقابله با حملات سایبری اتخاذ کند.

نقش نهادهای غیر دولتی نیز در این عرصه قابل توجه است؛ به ویژه «اتحاد بین‌المللی حفاظت از امنیت سایبری» (ICSPA)که نمونه‌ای از تلاش‌های جهانی برای مقابله با جرایم و تروریسم سایبری از طریق همکاری دولت‌ها، شرکت‌ها و نهادهای تخصصی است. این سازمان غیردولتی با هدف ایجاد هم‌افزایی و افزایش آگاهی جهانی درباره تهدیدات سایبری شکل گرفته و می‌تواند به‌عنوان مکمل و تقویت‌کننده اقدامات بین‌المللی رسمی عمل کند. اتحادیه بین‌المللی مخابرات (ITU) نیز با توجه به تخصص و ساختار خود، به‌عنوان یکی از ارکان مهم در زمینه مخابرات و فناوری اطلاعات، به‌صورت غیرمستقیم اما مؤثر در مقابله با اختلالات و حملات سایبری نقش ایفا می‌کند. توانایی این اتحادیه در شناسایی عوامل اختلال در ارتباطات بین‌المللی و تنظیم قواعد مرتبط می‌تواند بخشی از راهکارهای پیشگیرانه در برابر تهدیدات سایبری باشد.

از سوی دیگر، قواعد و معاهدات بین‌المللی مرتبط با حمل و نقل هوایی، حقوق فضای ماوراء جو و قوانین حاکم بر فضای مجازی، اگرچه به‌صورت مستقیم برای مقابله با حملات سایبری تدوین نشده‌اند، اما ظرفیت بالقوه‌ای برای تنظیم و پاسخگویی به این تهدیدات دارند. فناوری‌های نوین همچون «اینترنت اشیاء (IoT) «باعث افزایش پیچیدگی و گستردگی حملات سایبری شده‌اند، که این امر نیازمند توسعه قوانین بین‌المللی منسجم‌تر و جامع‌تر است. در این میان، جلسات و توافق‌نامه‌های بین‌المللی که به مقابله با جرایم سایبری در بخش حمل و نقل هوایی می‌پردازند، نمونه‌ای از تلاش‌ها برای به‌روزرسانی نظام حقوقی در جهت پاسخ به تهدیدات جدید هستند.

در مجموع، می‌توان گفت که مبارزه با حملات سایبری به زیرساخت‌های حیاتی، نیازمند رویکردی چندجانبه و هماهنگ بین نهادهای دولتی، بین‌المللی و غیر دولتی است. تدوین و تقویت قواعد حقوقی بین‌المللی منسجم، ایجاد سازوکارهای نظارتی و اجرایی مؤثر، و افزایش همکاری‌های بین‌المللی در زمینه تبادل اطلاعات و ظرفیت‌سازی، از مهم‌ترین ارکان این مبارزه به‌شمار می‌روند. با توجه به سرعت پیشرفت فناوری و پیچیدگی‌های فضای سایبری، بدون شک این حوزه در آینده‌ای نزدیک نیازمند قوانین پویا و به‌روز خواهد بود که بتواند پاسخگوی تحولات و تهدیدات نوین باشد.

ملاحظات اخلاقی: در تمام مراحل نگارش پژوهش حاضر، صداقت و و امانتداری رعایت شده است.

تعارض منافع: در این مقاله هیچگونه تضاد منافعی وجود ندارد.

سهم نویسندگان: نگارش مقاله مشترکاً توسط نویسندگان صورت گرفته است.

تشکر و قدردانی: از کلیه کسانی که در معرفی منابع و تهیه این مقاله ما را یاری رساندند، تشکر و قدردانی می‌نماییم.

تأمین اعتبار پژوهش: این پژوهش فاقد تأمین کننده مالی بوده است.

منابع و مآخذ

الف. منابع فارسی

– ابراهیم گل، علیرضا (۱۳۹۰). مسؤولیت بین‌المللی دولت، متن و شرح مواد کمیسیون حقوق بین‌الملل. تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش.

– جعفری، افشین (۱۳۹۸). «حاکمیت بر فضای سایبر از منظر حقوق بین‌الملل و نظام حقوقی جمهوری اسلامی ایران». *فصلنامه رهیافت انقلاب اسلامی*، ۴۹.

– زمانی، سید قاسم (۱۳۸۷). *حقوق سازمان بین‌المللی، شخصیت، مسؤولیت، مصونیت*. تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش.

– شریفی طرازکوهی، حسین و برمکی، جعفر (۱۳۹۹). «چالش‌های حقوقی قابلیت‌های فضای سایبری در پرتو ماده ۳۶ پروتکل یکم الحاقی ۱۹۷۷». *مجله حقوقی بین‌المللی*، ۶۲.

– طیبی، سبحان؛ زمانپور، بهاره و طیبی، سجاد (۱۳۹۸). «مسؤولیت بین‌المللی دولت‌ها نسبت به نقض هنجارهای حقوقی و عدم پیروی معاهداتی». *فصلنامه تخصصی حقوق فارس*، ۲(۵): ۲۷–۹.

– نورمحمدی، مرتضی و طالبی آرانی، روح‌الله (۱۳۹۵). «گسترش فناوری‌های اطلاعات و ارتباطات؛ رویکردهای نظری و ملاحظات امنیتی جمهوری اسلامی ایران». *فصلنامه پژوهش‌های راهبردی سیاست*، ۱۶.

ب. منابع انگلیسی

- Bada, A., & Nurse, J. R. C. (2019). Cybersecurity and international law: The Budapest Convention and beyond. *Journal of Cyber Policy*, 4(3), 383-405.

- Brownlie, System of the Law of nations, State Vespansibility, Part I, Oxford, 1983.

- Burkadze, K. (2020). International Legal Basis For The Right To Defense In The Cyber Era. *Law and World*, 3(2), 1-18.

- Fitzmaurice and D.Sarooshi, Issues of State responsibility before International Judicial Institutions, Oxford, 2003,P.14

- Hathaway, O. A., & Crootof, R. (2012). The Law of Cyber-Attack. *California Law Review*, 100(4), 817-885. https://doi.org/10.2139/ssrn.1977974

- Mele, S, "Cyber Weapons: Legal and Strategic Aspects", Italian Institute of Strategic Studies, Rome, 2013.p9.

- Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 1971.

- Protocol for the Suppression of Unlawful acts of Violence at Airports serving international civil aviation, 1988.

- Convention on International Civil Aviation, 1944.