Modern Technologies Law

University of Science and Culture

http://doi.org/10.22133/MTLJ.2023.367059.1136

International Responsibility of States For Cyber Attacks of Non-State Actors

Parviz Farshasaid[1]*, Mahmood Jalali[2]

[1] Ph.D student In Public International Law, Department of International law, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran

[2] Associate Professor, Department of Law, University of Isfahan, Iran

Article Info

Original Article

Received:
24-10-2022
Accepted:
07-01-2023

Keywords:
Cyber attacks
International responsibility of states
Effective control standard
Overall control standard
Due diligence standard

***Corresponding author**
e-mail: parvizfarshasaid@yahoo.com

Abstract

Due to the widespread dependence of all human affairs on cyberspace and the Internet, the risk of cyber attacks threatens international peace and security more than ever. From time to time, some news is spread in the media and social networks that a cyber attack has been carried out against a state. Still, due to the complexities of cyberspace, it is difficult to determine the perpetrator of the cyber attack. What can act as a strong barrier against the state's violations of the rules and principles of international law is the rules of the international responsibility of the states. Currently, there are two standards of responsibility for states against cyber attacks of Non-State Actors, one of which is the standard of effective control, and the other is the standard of general control. In this article, the advantages and disadvantages of these two standards for determining the international responsibility of states for cyber attacks by Non-State Actors are discussed. It is concluded that due to the special characteristics of cyber technologies, these two standards are not appropriate to prove the responsibility of states for Non-state actors' cyber attacks. The standard of due diligence must be considered by states because, based on the characteristics of this standard, it seems easier to prove the international responsibility of states against cyber attacks by Non-state Actors.

How to Cite:
Farshasaid, P., & Jalali, M. (2022). International Responsibility of States For Cyber Attacks of Non-State Actors. *Modern Technologies Law*, *3*(6), 173-184.

Published by University of Science and Culture https://www.usc.ac.ir
Online ISSN: 2783-3836

حقوق فناوری‌های نوین

http://doi.org/10.22133/MTLJ.2023.367059.1136

مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی

پرویز فرشاسعید[1]*، محمود جلالی[2]

[1] دانشجوی دکتری حقوق بین‌الملل عمومی، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، اصفهان، ایران

[2] دانشیار گروه حقوق دانشگاه اصفهان، اصفهان، ایران

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۱/۸/۲

تاریخ پذیرش:
۱۴۰۱/۱۰/۱۷

واژگان کلیدی:
حملات سایبری
مسئولیت بین‌المللی دولت‌ها
معیار کنترل کلی
معیار کنترل مؤثر
معیار مراقبت بایسته

***نویسندهٔ مسئول**

رایانامه: parvizfarshasaid@yahoo.com

نحوهٔ استناددهی:

فرشاسعید، پرویز و جلالیان، محمود (۱۴۰۱). مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی. *حقوق فناوری‌های نوین*، ۳ (۶)، ۱۸۴-۱۷۳.

ناشر: دانشگاه علم و فرهنگ https://www.usc.ac.ir

شاپای الکترونیکی: ۳۸۳٦-۲۷۸۳

چکیده

به‌علت وابسته‌شدن گستردهٔ تمامی امورات بشر به فضای سایبر و اینترنت، خطر حملات سایبری صلح و امنیت بین‌المللی را بیش‌ازپیش تهدید می‌کند. گاه‌گاهی اخباری در رسانه‌ها و شبکه‌های مجازی منتشر می‌شود مبنی بر این‌که حملهٔ سایبری علیه دولتی انجام گرفته است، ولی به‌علت پیچیدگی‌های فضای سایبر مشخص‌نمودن عامل حملهٔ سایبری مشکل است. آنچه می‌تواند در برابر تخلفات دولت‌ها از قواعد و اصول حقوق بین‌الملل همچون سدی استوار عمل کند قواعد مسئولیت بین‌المللی دولت‌ها است. در حال حاضر دو معیار مسئولیت برای دولت‌ها در قبال حملات سایبری عوامل غیردولتی وجود دارد که یکی معیار کنترل مؤثر و دیگری معیار کنترل کلی است. در این مقاله به مزایا و معایب این دو معیار برای تعیین مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی پرداخته و نتیجه‌گیری شده است که به‌علت ویژگی‌های خاص فناوری‌های سایبری این دو معیار برای اثبات مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی مناسب نیست و باید معیار مراقبت بایسته مدنظر دولت‌ها قرار گیرد؛ زیرا، بر اساس ویژگی‌های این معیار، اثبات مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی ساده‌تر به‌نظر می‌رسد.

مقدمه

حملات سایبری چالش‌های جدیدی را برای حقوق بین‌الملل ایجاد کرده است. در گذشته و هنگامی‌که دولت‌ها برای واردکردن خسارات به رقبایشان از سلاح‌های سنتی استفاده می‌کردند، مشخص‌کردن عامل این حملات تا حدی ساده بود. قرن بیست‌ویکم عصر حاکمیت اینترنت بر تمامی عرصه‌های زندگی بشر است، به حدی که تمدن و حیات کنونی بشر به این فناوری مدرن و بااهمیت وابسته شده است. در سایهٔ این وابستگی، دولت‌هایی که فناوری‌های پیشرفته‌ای در این عرصه دارند به دنبال کسب منافع سیاسی، اقتصادی و سایر منافعی هستند که دست‌یابی به آن‌ها با این فناوری ساده‌تر و راحت‌تر شده است. بدین سبب، همه‌روزه شاهد انتشار اخباری دربارهٔ حملات سایبری به دولت‌های متعدد و حتی کشورهایی مانند ایالات متحدهٔ آمریکا، روسیه، چین و سایر کشورهایی هستیم که دارای فناوری‌های بسیار پیشرفته‌ای در حوزهٔ سایبرند. تمامی حوزه‌های تمدن و حیات بشری، از مراکز دولتی گرفته تا دانشگاه‌ها و مراکز پژوهشی، بخش صنعت و انرژی و...، در معرض حملات سایبری قرار دارند. به‌علت ماهیت حملات سایبری، اثبات مسئولیت بین‌المللی این حملات همواره یکی از چالش‌هایی بوده که حقوق بین‌الملل موجود با آن مواجه بوده است و بحث مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی شایستهٔ اعتنا و توجه بیشتری است؛ زیرا بیشتر دولت‌ها برای فرار از مسئولیت بین‌المللی چنین حملاتی را توسط عوامل غیردولتی انجام می‌دهند. در حقوق بین‌الملل، اصطلاح عوامل غیردولتی طیف گسترده‌ای از کنشگران را در سطح بین‌المللی، از سازمان‌های غیردولتی گرفته تا شرکت‌های چندملیتی، دربر می‌گیرد. فناوری رایانه، در کنار همهٔ مطلوبیت‌ها و پیشرفت‌هایی که داشته است، چالش‌ها و مشکلاتی را برای جهانیان ایجاد کرده و زنگ خطر جدیدی پس از وحشت به‌کارگیری سلاح‌های هسته‌ای به‌شمار می‌آید (قرشی سروندانی، ۱۳۹۱، ص ۵). امکان بروز آسیب و خسارت گسترده باعث می‌شود جامعهٔ جهانی در برابر این تهدید احساس وظیفه کند و برای مقابله با آن چاره‌ای بیندیشد. رشد فزایندهٔ فناوری در حوزهٔ اطلاعات و ارتباطات تهدیدهایی نیز به دنبال داشته است که حملهٔ سایبری نمونهٔ بارز چنین تهدیدی است. تبعات چنین حملاتی به حدی جدی است که کنشگران بین‌المللی به‌ویژه دولت‌ها را برای اتخاذ رویه‌های مناسب و مواضع سیاسی‌حقوقی به تکاپو واداشته است (اصلانی و رنجبریان، ۱۳۹۴، ص ۲۵۷). مهم‌ترین و مؤثرترین اقدام در رویارویی با حملات سایبری ایجاد نظام حقوقی مسؤلیت بین‌المللی است، زیرا بدون یافتن مسئول واقعی حملات سایبری نمی‌شود به‌راحتی چگونگی واکنش به آنها را مشخص نمود. در این مقاله به تجزیه‌وتحلیل دو رژیم حقوقی مسئولیت دولت برای حملات سایبری عوامل غیردولتی موجود می‌پردازیم: نخست معیار کنترل مؤثر[1] که موارد برجستهٔ استفاده از آن در رأی دیوان بین‌المللی دادگستری دربارهٔ قضیهٔ نیکاراگوئه[2] در ۱۹۸۶ و رأی سال ۲۰۰۷ در قضیهٔ نسل‌زدایی بوسنی[3] بود و معیار کنترل کلی[4] که در رأی سال ۱۹۹۹ دیوان بین‌المللی یوگسلاوی سابق در قضیهٔ تادیچ[5] مدنظر دیوان قرار گرفت. با بررسی این دو رژیم مسئولیت بین‌المللی به این سؤال پاسخ خواهیم داد که با توجه به ماهیت پیچیدهٔ حملات سایبری آیا این دو معیار در رویارویی با حملات سایبری عوامل غیردولتی مؤثر خواهد بود و جلوی فرار از مسئولیت دولت‌هایی را که در پشت حملات سایبری قرار دارند خواهد گرفت یا باید رژیم حقوقی دیگری تعیین شود.

۱. حملات سایبری پدیدهٔ خطرناک قرن بیست‌ویکم

قرن بیست‌ویکم را باید عصر فناوری اطلاعات بنامیم. اختراع و گسترش شبکهٔ جهانی اینترنت باعث شده است که تمامی عرصه‌های زندگی و تمدن بشر به این فناوری‌ها وابسته شود. از نیروگاه‌های برق گرفته تا فرودگاه‌ها و سامانه‌های کنترل پرواز هواپیماها، سامانه‌های دفاعی و موشکی، تجارت و بانک‌داری، همه و همه به این فناوری‌ها وابسته‌اند. با این پدیده شاهد ظهور نوعی جدید از حملات بین‌المللی علیه دولت‌ها هستیم؛ حملاتی که به سبک قدیمی و با سلاح‌های سنتی صورت نمی‌گیرد، بلکه فناوری‌های حوزهٔ سایبر یعنی ویروس‌ها،کرم‌ها و سایر ابزارهای مرتبط

1. Effective Control
2. Nicaragua case
3. Bosnia Genocide Case
4. Overall control
5. Tadić case

با این حوزه را به خدمت می گیرد. اختراع کامپیوتر و اینترنت باعث شد نوع و سبک حملات علیه دولت‌ها تغییر یابد. در گذشته، هنگامی‌که حملاتی علیه دولت‌ها شکل می‌گرفت، شاهد پرواز هواپیماها، پرتاب موشک‌ها، خمپاره‌ها و شلیک گلوله‌ها و بلافاصله به دنبال آن شاهد تخریب اماکن و جراحت و مرگ اشخاص بودیم. شناسایی چنین حملاتی نیز به‌راحتی ممکن بود و دولت‌ها می‌توانستند در برای این حملات اقدام به دفاع مشروع نمایند. بنابراین، دولت‌ها تا حد امکان از انجام حملات علیه دولت‌ها و کشورهای دیگر اجتناب می‌ورزیدند، زیرا چنین حملاتی احتمال جنگ و درگیری را بین آن‌ها افزایش می‌داد. بر اساس بند ۴ مادهٔ ۲ منشور سازمان ملل متحد، اعضا در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر روش دیگری که با مقاصد ملل متحد مباینت داشته باشد خودداری خواهند کرد. فناوری‌های حوزهٔ سایبر مفهوم زور را نیز به چالش کشیده است. زور در گذشته به معنی استفاده از سلاح‌ها و تجهیزات نظامی بود، ولی امروزه شاهد حملاتی هستیم که بدون چکاندن ماشه‌ای خسارت‌های بسیار زیادی را به کشورها وارد می‌کند. در چند سال گذشته، شاهد حملات متعدد سایبری در جهان بوده‌ایم و روزبه‌روز به تعداد این حملات افزوده می‌شود. چنین وضعیتی باعث شده است که قرن بیست‌ویکم را قرن حملات سایبری نام‌گذاری کنیم. ازآنجاکه توسعهٔ جامعهٔ بین‌المللی با هدف ساختن جامعهٔ اطلاعاتی بین‌المللی صورت می‌گیرد، مسئلهٔ امنیت سایبری و دفاع مشروع قانونی دارای اهمیت بسیاری است (Kulesza, 2009, p.3). در بحث دفاع مشروع، بر اساس مادهٔ ۵۱ منشور سازمان ملل متحد، در صورت وقوع حملهٔ مسلحانه علیه یك عضو سازمان مجوز دفاع مشروع داده شده است. البته باید گفت که مواد منشور سازمان ملل متحد پیش از عصر سایبر تهیه شده و منظور از حملهٔ مسلحانه حملات با سلاح‌های سنتی است، ولی فناوری‌های حوزهٔ سایبر حقوق بین‌الملل را به چالش کشیده است؛ زیرا مواجه با حملاتی هستیم که بدون استفاده از ابزار و سلاح‌های سنتی و به سبکی دیگر و با ابزارهای بسیار متفاوتی انجام می‌گیرد. حتی فضای ارتکاب حملات سایبری فضایی جدید و ناملموس است و فقط نتایج آن قابل مشاهده است. با توجه به مادهٔ ۵۱ منشور سازمان ملل متحد، اگر حملات سایبری به حد حملهٔ مسلحانه برسند، یعنی باعث ایجاد جراحت یا مرگ اشخاص و خسارت و تخریب اشیا شوند، می‌توان در برابر آن‌ها دفاع مشروع کرد. با توجه به حملات سایبری، می‌شود دریافت که بیشتر حملات سایبری به آستانه‌ای که در مادهٔ ۵۱ بیان شده است نمی‌رسند.تنها راه‌حل برای مواجهه با حملات سایبری کنکاش در قواعد مسئولیت بین‌المللی دولت‌ها است، زیرا این قواعد هم چگونگی واکنش به حملات سایبری را برای دولت‌ها مشخص و آشکار می‌نماید و هم باعث ایجاد نظم و ثبات بین‌المللی می‌شود. در حقیقت، فناوری سایبری مرزهای سیاسی و فرهنگی را نادیده می‌گیرد و دسترسی نامحدود به کنشگران خصوصی ایجاد می‌کند (Liu, 2017, p.256). چنین ویژگی این حملات باعث شده است که حملات سایبری متعددی در جهان شکل گیرد که یافتن انگیزهٔ واقعی مرتکبان آن‌ها بسیار دشوار است. اگرچه دولت‌ها از انجام و هدایت حملات سایبری انگیزه‌های متعددی دارند، مهم‌ترین انگیزه برای ارتکاب این حملات واردکردن خسارت و آسیب به دولت‌های رقیب است.

۲. مسئولیت بین‌المللی دولت‌ها در برابر اعمال متخلفانهٔ بین‌المللی

مسئولیت بین‌المللی، به‌مثابهٔ نهاد حقوقی بین‌المللی، عبارت است از الزام به جبران خسارت مادی یا معنوی وارد بر تابعان حقوق بین‌الملل، که این خسارت باید ناشی از عمل یا خودداری از عمل غیرمشروع و مخالف حقوق بین‌الملل با یکی از موضوعات یا تابعان حقوق بین‌الملل باشد. برای تحقق مسئولیت بین‌المللی هر دولت، تخلف بین‌المللی باید قابلیت انتساب به آن دولت را نیز داشته باشد (ضیایی بیگدلی، ۱۳۸۴، ص۴۶۹). حملات سایبری بیشتر به‌منزلهٔ نقض‌های تعهدات بین‌المللی به حساب می‌آیند که به مسئولیت بین‌المللی دولت منجر می‌شوند. بر اساس مادهٔ ۱ طرح کمیسیون حقوق بین‌الملل دربارهٔ مسئولیت بین‌المللی دولت، هر تخلف بین‌المللی یک دولت موجب مسئولیت بین‌المللی آن دولت می‌شود. دیوان‌های بین‌المللی در پرونده‌های متعددی به اصل مذکور استناد کرده‌اند. دیوان دائمی دادگستری بین‌المللی در پروندهٔ فسفات مراکش نظر داد که وقتی دولتی مرتکب تخلفی بین‌المللی علیه دولتی دیگر می‌شود مسئولیت بین‌المللی برقرار می‌گردد.[1] دیوان بین‌المللی

1. Phosphates in Morocco, Judgment (1938), P. C. I. J. Series A/B, No. 74,para 28

دادگستری نیز در پرونده‌های متعددی مانند تنگهٔ کورفو،[1] قضیهٔ نیکاراگوئه[2] و طرح گابچیکو ـ ناگی ماروس[3] به اصل مزبور استناد کرده است. همچنین، در پروندهٔ رینبو وارير،[4] دیوان داوری نظر داد که تخلف هر دولتی از هر تعهدی، صرف‌نظر از منشأ آن، موجب مسئولیت دولت می‌شود.[5] ازآنجاکه روابط حقوقی ناشی از وقوع تخلف اساساً رابطه‌ای دوجانبه یعنی فقط مربوط به مناسبات دولت مسئول و دولت صدمه‌دیده است، دیوان بین‌المللی دادگستری در قضیهٔ بارسلونا تراکشن رأی داد که باید بین تعهداتی که یک دولت در برابر کل جامعهٔ بین‌المللی دارد و تعهداتی که ناشی از حمایت سیاسی در قبال یک دولت دیگر است به نحو اساسی قائل به تفکیک شد. ماهیت ذاتی دستهٔ اول این است که تعهدات مزبور مربوط به تمامی دولت‌ها است و به‌علت اهمیت حقوقی که در آن‌ها مطرح است، همهٔ دولت‌ها در آن‌ها ذی‌نفع‌اند، یعنی تعهداتی تخطی‌ناپذیر به حساب می‌آیند.[6]

عناصر تشکیل‌دهندهٔ تخلف بین‌المللی دولت‌ها

تخلف بین‌المللی دولت زمانی محرز می‌شود که فعل یا ترک فعل تشکیل‌دهندهٔ اقدام الف) طبق حقوق بین‌الملل قابل‌انتساب به آن دولت باشد و ب) موجب نقض تعهد بین‌المللی آن دولت باشد.

دیوان بین‌المللی دادگستری در پرونده‌های متعددی به عناصر دوگانهٔ مذکور اشاره کرده است. برای مثال، در پروندهٔ کارکنان کنسولی و سیاسی آمریکا در تهران، دیوان رأی داد که نخست باید معلوم شود که از لحاظ قانونی تا چه حد اعمال موردبحث قابل‌انتساب به دولت ایران است. دوم، باید انطباق یا مغایرت آن اعمال را با تعهداتی که ایران طبق عهدنامه‌های معتبر یا هر قاعدهٔ قابل‌اعمال دیگر حقوق بین‌الملل در این خصوص بر عهده دارد بررسی کرد.[7]

اقدام منتسب به دولت می‌تواند شامل فعل‌ها یا ترک فعل‌ها یا ترکیبی از هر دو باشد. مواردی که مسئولیت بین‌المللی یک دولت بر اساس ترک فعل مورد استناد قرار گرفته دست‌کم به همان تعدادی است که بر اساس مبادرت به فعل‌ها مورد استناد واقع شده است و از لحاظ اصول هیچ تفاوتی بین این دو مورد وجود ندارد (حلمی، ۱۳۸۷، ص ۳۶). در بحث شرط دوم که نقض یک تعهد بین‌المللی دولت است سابقه‌ای طولانی دارد و هم تعهدات عهدنامه‌ای و هم تعهدات غیرعهدنامه‌ای را دربر می‌گیرد. در حقوق بین‌الملل، غالباً نقض یک تعهد معادل اقدامی مغایر با حقوق سایرین تلقی شده است (حلمی، ۱۳۸۷، ص ۳۷). در این خصوص که در حملات سایبری چه تعهد بین‌المللی نقض می‌شود، باید به بند ۴ مادهٔ ۲ منشور سازمان ملل متحد مراجعه کنیم. بر اساس این بند، کلیهٔ اعضا در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه یکپارچگی سرزمینی یا استقلال سیاسی هر کشوری که با مقاصد ملل متحد مباینت داشته باشد خودداری خواهند کرد. اگرچه استفاده از ابزار سایبری برای هدایت و ارتکاب حملات سایبری علیه دولت‌های دیگر کاربرد زور به حساب می‌آید، ولی همهٔ حملات سایبری به آستانهٔ موردنظر برای دفاع مشروع در حقوق بین‌الملل نمی‌رسند. در حقوق بین‌الملل، بر اساس مادهٔ ۵۱ منشور سازمان ملل متحد، فقط در برابر حملهٔ مسلحانه حق دفاع مشروع داده شده است.

در منشور سازمان ملل متحد، برای حملهٔ مسلحانه تعریفی ارائه نشده است. بنابراین، برای یافتن تعریف حملهٔ مسلحانه باید به قطعنامهٔ ۳۳۱۴ سازمان ملل دربارهٔ تعریف تجاوز مراجعه کنیم. بر اساس مادهٔ ۳ قطعنامهٔ تعریف تجاوز، تهاجم نیروهای مسلح کشوری به سرزمین

1. Corfu Channel Case
2. Military and Paramilitary Activities in and against Nicaragua
3. Gabcikovo - Nagymaros
4. Rainbow Warrior
5. Rainbow Warrior Case, (NEW ZEALAND v. FRANCE),France-New Zealand Arbitration Tribunal. 30 April 1990
6. I. C. J. Reports 1970, Case Concerning the Barcelona Traction, Light and Power Co (Belgium v. Spain) , order of 10 April 1961,para 33
7. I. C. J. Reports 1981 ,Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran); Order, 12 V 81, International Court of Justice (ICJ), 12 May 1981,para 56

کشور دیگر تجاوز به حساب می‌آید. همچنین، عمل دولتی که سرزمین خود را در اختیار دولت دیگر قرار داده است و اعزام دسته‌ها و گروه‌های مسلح یا نیروهای غیرمنظم یا سربازان مزدور برای انجام عملیات علیه کشور دیگر تجاوز را شکل می‌دهد.[1]

اصل عدم‌مداخله در امور داخلی کشورها ازجمله اصولی است که در بند ۷ مادهٔ ۲ منشور سازمان ملل متحد به‌صراحت آمده است. بر اساس این بند، هیچ‌یک از مقررات مندرج در این منشور ملل متحد را مجاز نمی‌کند در اموری که ذاتاً جزو صلاحیت داخلی هر کشوری است دخالت کند و اعضا را نیز ملزم نمی‌کند چنین موضوعاتی را تابع مقررات این منشور قرار دهند. در اعلامیهٔ اصول حقوق بین‌الملل دربارهٔ روابط دوستانه و همکاری میان دولت‌ها، بر اساس منشور سازمان ملل متحد، هرگونه مداخلهٔ مستقیم یا غیرمستقیم به هر دلیلی در امور داخلی یا خارجی هر دولت نقض حقوق بین‌الملل به حساب می‌آید.[2]

بنابراین، اگر حملات سایبری نتایج و عواقبی شبیه به نتایج و عواقب سلاح‌های سنتی داشته باشند، حملات مسلحانه به حساب می‌آیند و حق دفاع مشروع در برابر چنین حملاتی وجود خواهد داشت. اگر حملات سایبری نتایج و عواقبی مانند نتایج و عواقب سلاح‌های سنتی نداشته باشند، مداخله در امور داخلی کشورها به حساب می‌آیند و مسئولیت بین‌المللی دولت‌ها را بر مبنای نقض اصل عدم‌مداخله در پی خواهد داشت. این‌که چگونه و با چه معیاری بتوان مسئولیت بین‌المللی دولت‌ها را در برابر حملات سایبری اثبات کرد اقدام بسیار مهمی در حفظ صلح و امنیت بین‌المللی خواهد بود. با توجه به این‌که موضوع بحث ما دربارهٔ مسئلهٔ مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری عوامل غیردولتی است، در این قسمت به بررسی و کنکاش پیرامون معیار مناسب برای اثبات مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری عوامل غیردولتی خواهیم پرداخت.

۳. مسئلهٔ انتساب و معیار کنترل در برابر حملات سایبری عوامل غیردولتی

فرض گمنامی و ناشناخته‌بودن عامل حملهٔ سایبری ابهامات و پرسش‌های روزافزونی را درخصوص انتساب حمله ایجاد کرده است. در شرایطی که معلوم نیست حملهٔ سایبری از طرف دولت یا گروه غیردولتی خاصی صورت گرفته باشد، طبعاً انتساب آن به دولت یا نهادی دولتی یا حتی فردی خاص غیرممکن خواهد بود (امیری و حیدری فرد، ۱۳۹۷، ص ۱۶۲). انتساب حمله‌ای سایبری به یک دولت مهم‌ترین عنصر برای ایجاد رژیم حقوقی کاربردی برای حوزهٔ سایبر است. در حقوق بین‌الملل موجود، بر اساس مادهٔ ۸ طرح مواد کمیسیون حقوق بین‌الملل راجع‌به مسئولیت دولت‌ها برای افعال متخلفانهٔ بین‌المللی سال ۲۰۰۱، دو معیار برای مسئولیت بین‌المللی دولتها وجود دارد. در مادهٔ ۸ این مواد آمده است که رفتار شخص یا گروهی از اشخاص به‌موجب حقوق بین‌الملل فعل دولت تلقی می‌شود، در صورتی که شخص یا اشخاص مزبور در انجام رفتار مزبور به دستور تحت هدایت یا کنترل دولت عمل کنند.[3] واژهٔ کنترل به مواردی اشاره دارد که دولت بر انجام رفتار خلاف تسلط و غلبه دارد و این غلبه ناشی از غفلت و بی‌توجهی نیست. بنابراین، با توجه به اشراف و تسلطی که بر دولت دیگر یا گروه و اشخاص دارد و با علم به این غلبه، رفتاری را به خود مرتبط می‌کند. در مقابل، واژهٔ هدایت فقط شامل تحریک یا پیشنهاد برای عمل خلاف است که این معنی شامل هدایت واقعی و ضمنی مؤثر هم است (راعی، ۱۳۸۸، ص ۱۵۵). اگرچه تعریف دقیقی از کنترل برای تفسیر به دادگاه واگذار شده است، نخستین معیاری که دادگاه‌ها ارائه داده‌اند معیار کنترل مؤثر دیوان بین‌المللی دادگستری در قضیهٔ نیکاراگوئه است. دیوان در قضیهٔ نیکاراگوئه نظر داد که برای آن‌که مسئولیت دولت آمریکا در قبال اقدامات کنتراها به‌وجود آید، باید این نکته ثابت شود که دولت آمریکا نسبت به این نیروها دارای کنترل مؤثر داشته است و این کنترل به‌گونه‌ای بوده است که نقض‌های بشردوستانه واقع شده را به دولت آمریکا منسوب کند (راعی، ۱۳۸۸، ص ۱۵۳). بر اساس این رأی، کنترل یک دولت بر شبه‌نظامیان یا دیگر عوامل غیردولتی فقط وقتی ایجاد می‌شود که کنشگران موردبحث وابستگی کامل به

1. Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX), 2319th plenary meeting, 14 December 1974,art 3
2. United Nations General Assembly Resolution 2625 (XXV) Declaration on Principles of International Law Concerning Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations ,Adopted at the 1883rd plenary meeting ,October 24, 1970.
3. Draft articles on Responsibility of States for Internationally Wrongful Acts, 2001: Art 8

دولت برای انجام فعل متخلفانه داشته باشند. اکثریت کارشناسان حقوق بین‌الملل رأی دیوان بین‌المللی دادگستری در قضیهٔ نیکاراگوئه را این‌گونه تفسیر کرده‌اند که برای این‌که اعمال مسلحانهٔ گروهی به دولتی انتساب یابد آن دولت باید کنترل مؤثری بر عملیات آن گروه داشته باشد.

همچنین، دیوان دربارهٔ معیار کنترل چنین اظهار داشت: باید محرز شود که رابطهٔ شورشیان با دولت ایالات متحده از یک طرف به میزان وابستگی و از طرف دیگر به حد کنترل رسیده است تا از لحاظ حقوقی، نیروهای کنترا رکن دولت ایالات متحده یا عامل آن دولت قلمداد شوند.[1] دیوان با تکیه بر اصل نظارت و کنترل مؤثر ابراز داشت: به‌رغم کمک‌های مالی گسترده و دیگر حمایت‌هایی که ایالات متحده از کنتراها به عمل آورده است، هیچ دلیل روشنی وجود ندارد مبنی بر این‌که ایالات متحده چنین درجه‌ای از کنترل مؤثر دولت را بر تمامی زمینه‌ها اعمال کرده باشد.[2] کنترل مؤثر به کنترل دولت بر اعمالی خاص در جریان عملیات خاصی که در طول آن نقض‌هایی صورت گرفته است مربوط می‌شود.[3]

در رأی سال ۲۰۰۷ دیوان بین‌المللی دادگستری درخصوص قضیهٔ نسل‌زدایی و مجازات مرتکبان نیز، دیوان با تکیه بر معیار کنترل مؤثر به‌منزلهٔ عاملی برای تحقق مسئولیت دولت به این قضیه پرداخته است. در این رأی، دیوان اعمال شبه‌نظامیان صرب را به دولت صربستان انتساب نداد و دلیل دیوان این بود که دولت صربستان بر نیروهای نظامی صرب دولت بوسنی کنترل مؤثر نداشته است (راعی، ۱۳۸۸، ص ۱۵۳).

دومین معیار، معیارکنترل کلی است که در رأی دادگاه بخش تجدیدنظر کیفری یوگسلاوی سابق دربارهٔ قضیهٔ تادیچ مطرح شد. منظور از کنترل کلی، طبق نظر شعبهٔ تجدیدنظر دادگاه کیفری یوگسلاوی سابق، این است که کنترل از صرف تجهیز و تأمین مالی نیروها و مشارکت در برنامه‌ریزی و نظارت بر عملیات نظامی آن‌ها فراتر رود.[4] دادگاه کیفری یوگسلاوی کنترل کلی دولت بر گروه‌های سازمان‌یافتهٔ شبه‌نظامی را موجب تبدیل آن‌ها به ارکان عملی دولت می‌داند و با تشبیه آن‌ها به نیروهای مسلح منظم و قانونی دولت را در هر صورت، ازجمله اجرای دستورات و تخطی از حیطهٔ اختیارات، مسئول قلمداد می‌کند. دیوان منطق وضع چنین مقرره‌هایی را اجتناب از گریز دولت‌ها از مسئولیت بین‌المللی قرار داد (نصیری محلاتی، ۱۳۸۹، ص ۶۸).

همچنین، از نظر بخش تجدیدنظر، آستانه‌ای که در حقوق بین‌الملل برای بین‌المللی تلقی‌کردن یک مخاصمه لازم است کنترل کلی است. کنترل واقعی همان تأمین مالی و تجهیز این نیروها است و شامل شرکت در عملیات غیرنظامی و حمایت از آن می‌شود (راعی، ۱۳۸۸،ص ۱۵۶). ضابطه‌های دیوان بین‌المللی دادگستری و دادگاه کیفری یوگسلاوی سابق در درجهٔ کنترل لازم برای انتساب عمل به دولت متفاوت است. ضابطهٔ دیوان به اثبات وابستگی کامل یا کنترل مؤثر نیازمند است، درحالی‌که ضابطهٔ دادگاه کیفری یوگسلاوی سابق انتساب را حتی برای هماهنگی یا کمک به طرح کلی فعالیت‌های نظامی اشخاص غیردولتی تجویز می‌کند (ملکی‌زاده، ۱۳۹۲، ص ۱۷۴).

۴. معایب معیار کنترل مؤثر برای مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری عوامل غیردولتی

دیوان بین‌المللی دادگستری در قضیهٔ نسل‌زدایی دربارهٔ معیار کنترل مؤثر چنین نظر داد: نخست آن‌که ضروری نیست نشان داده شود افرادی که ادعا شده است حقوق بین‌الملل را نقض کرده‌اند به‌طور کلی ارتباطی از نوع وابستگی تام با دولت خوانده داشته اند ، بلکه لازم است ثابت شود که ایشان طبق دستورات دولت مذکور یا تحت کنترل مؤثر آن عمل می‌کرده‌اند. بااین‌حال، باید نشان داده شود که چنین کنترل مؤثری بر هریک از عملیاتی که در خلال نقض‌های ادعایی صورت‌گرفته اعمال یا صادر شده است، نه این‌که صرفاً در زمینهٔ کلیت اعمالی که افراد یا گروه‌های مرتکب نقض‌های مذکور در پیش گرفته‌اند صادر یا اعمال شده باشد.[5] دیوان بین‌المللی دادگستری برای احراز این وابستگی و کنترل معیارهایی ارائه داده است: الف) رکن غیردولتی واقعاً توسط دولت ایجاد شده باشد.[6] ب) دخالت دولت به آموزش و کمک مالی بیشتر از حد منجر شده

1. I. C. J. Reports 1986, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits), Judgement of 27 June 1986,para 109
2. Ibid: 109
3. Ibid:277
4. prosecutor v. Tadic. Judgment. (Appeals chamber ICTY)15 July 1999,para 145
5. I. C. J. Reports 2007, Case Concerning Application of Convention on the Prevention and Punishment of the Crime of Genocide,(Bosnia and Herzegovina v Serbia and Montenegro) Judgment of 26 of February 2007:para 115
6. I. C. J. Reports 1986, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits), Judgement of 27 June 1986, ,Para 93&94

باشد. به عبارت دیگر، کافی نیست که حمایت دولت از گروهی قطعی باشد، بلکه این رابطه باید وابستگی کاملی باشد.[1] ج) دولت موردنظر باید واقعاً کنترل را اعمال کند.[2] د) دولت موردنظر رهبران گروه سیاسی را انتخاب کند.[3] ه) اساساً ضابطهٔ کنترل نیازمند این است که گروه وابسته و مجزا از دولت کنترل‌کننده اختیار واقعی نداشته باشد.[4] اگر این معیارهای ارائه‌شده از سوی دیوان دادگستری بین‌المللی درخصوص حملات سایبری را تجزیه و تحلیل کنیم، با مشکلات فراوان و متعددی روبه‌رو می‌شویم. به‌علت ماهیت پنهان حملات سایبری و این‌که برخلاف سلاح های سنتی همهٔ افراد و گروه‌ها به طور مساوی به فناوری های این حوزه دسترسی دارند، اثبات این مسئله که آیا این حملات توسط یک فرد یا گروه سازمان‌یافته ارتکاب یافته مشکل است. اگر عامل این حملات فردی از افراد جامعه است، آیا برای این حملات از دولتی دستور گرفته و تحت کنترل و هدایت دولتی بوده است یا خودسرانه و برای اهداف شخصی اقدام به انجام و هدایت چنین حملات سایبری کرده است. همچنین، اگر این حملات توسط گروه غیردولتی ارتکاب یافته‌اند، آیا چنین گروه غیردولتی توسط دولتی ایجاد شده و تحت کنترل و دستور آن دولت بوده و اوامر آن دولت را اجرا کرده است یا گروهی مخالف یک دولت و بدون ارتباط با سایر دولت‌ها و فقط به دلیل مخالفت با چنین دولتی اقدام به انجام و هدایت حملات سایبری کرده است؟ همچنین، آیا چنین فرد یا گروهی توسط دولتی آموزش دیده و حمایت مالی شده است و حمایت به‌گونه‌ای بوده که بین این فرد یا گروه وابستگی کامل ایجاد کرده است؟ اثبات چنین رابطه‌ای بین عاملان حملات سایبری و دولت‌ها بسیار مشکل است، زیرا حملات سایبری به صورت پنهانی و ناشناس انجام می‌گیرند و ارتباط بین دولت‌ها و اشخاصی که در پشت حملات سایبری قرار دارند بسیار محرمانه است و حتی کمک‌های مالی به این افراد و گروه‌ها از طریق کانال‌های سری و مخفی انجام می‌گیرد که شناسایی چنین رابطه‌ای تقریباً غیرممکن است. در بحث این‌که دولت موردنظر باید واقعاً کنترل را اعمال کند، مشکل این است که چگونه می‌توان وابستگی کامل یا مؤثر دولت‌ها را اثبات کرد. اگر با این معیار به دنبال انتساب مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری عوامل غیردولتی باشیم راه به جایی نخواهیم برد ، زیرا دولت‌ها ادعا خواهند کرد که حملات سایبری از خاک آن‌ها از طریق افراد و گروه‌های تبهکاری انجام گرفته است که هیچ‌گونه وابستگی به این دولت‌ها نداشته‌اند و تحت امر و دستور آن‌ها نبوده‌اند. بنابراین، نمی‌توان این دولت‌ها را طبق این معیار مسئول دانست.

فناوری‌های حوزهٔ سایبر به‌گونه‌ای است که با سلاح‌های سنتی تفاوت بسیاری دارد. درخصوص سلاح‌های سنتی در کشورهای متعددی قوانین خاصی وجود دارد و همهٔ افراد و شهروندان نمی‌توانند به‌آسانی به چنین سلاح‌هایی دسترسی داشته باشند. اگرچه در بعضی از کشورها مانند ایالات متحدهٔ آمریکا مالکیت سلاح‌های سبک به رسمیت شناخته شده است، افراد و شهروندان چنین کشوری نیز حق مالکیت سلاح‌های سنگین را ندارند و چنین سلاح‌هایی فقط در اختیار نهادها و ارگان‌های نظامی است که از آن‌ها به‌شدت محافظت می‌شود. هنگامی‌که حمله‌ای مسلحانه با سلاح‌های سنگین علیه دولتی ارتکاب می‌یابد ، دولت قربانی به‌راحتی می‌تواند عامل حمله را شناسایی کند ، زیرا یا دولتی در پشت این حمله قرار دارد یا گروه یا سازمانی مرتبط با دولتی مرتکب چنین حملاتی شده است. اما فناوری‌های حوزهٔ سایبری تمدن کنونی بشر را به چالش کشیده اند. این فناوری‌ها در دسترس همهٔ شهروندان قرار دارند و امروزه ، با توجه به پیشرفت‌های فناوری‌های عرصهٔ رایانه و اینترنت ، حتی در دورافتاده‌ترین نقاط و روستاها مردم به آن دسترسی دارند. چنین وضعیتی باعث می‌شود هر فرد یا گروهی توان انجام و هدایت حملات سایبری را در هر گوشه‌ای از جهان داشته باشد. همچنین، مکان هدایت حملات سایبری با مکان هدایت حملات به وسیلهٔ سلاح‌های سنتی متفاوت است. در گذشته، حملات مسلحانهٔ گروه‌های شبه‌نظامی علیه دولت‌ها از سوی گروه‌های مسلح مستقر در خاک آن‌ها انجام می‌گرفت ولی امروزه حملات سایبری از هر نقطه از جهان هدایت می‌شود، بدون این‌که به‌راحتی بتوان کنترل مؤثر یک دولت را بر این گروه‌ها اثبات کرد. بنابراین، با توجه با ماهیت و ویژگی‌های این فناوری، معیار کنترل مؤثر به چالش کشیده شده است.

1. Ibid para 110
2. Ibid
3. Ibid para 112
4. Ibid para 114

۵. معایب معیار کنترل کلی برای مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری عوامل غیردولتی

دیوان بین‌المللی دادگستری، در رویهٔ قضایی‌اش درخصوص پرونده‌های مرتبط مانند قضیهٔ نیکاراگوئه و قضیهٔ نسل‌زدایی، ضابطهٔ کنترل مؤثر را لحاظ کرده است، ولی شعبهٔ تجدیدنظر دادگاه یوگسلاوی سابق در قضیهٔ تادیچ و آرای مرتبط دیگری معیار کنترل کلی را به‌کار برده است. شعبهٔ تجدیدنظر در این قضیه رأی داد که به‌منظور انتساب اعمال گروه نظامی یا شبه‌نظامی به دولت باید اثبات کرد که دولت نه‌تنها با کمک مالی به گروه، بلکه با همکاری و کمک در طراحی کلی فعالیت‌های آن گروه بر آن کنترل کلی داشته است. فقط در این صورت دولت مسئول سوءرفتار گروه قلمداد می‌شود، اگرچه ضروری نیست دولت دستورالعمل‌هایی را برای ارتکاب اعمال خاص که در تضاد با حقوق بین‌الملل است صادر کند.[1] اگر معیار کنترل کلی را برای مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری عوامل غیردولتی به‌کار ببریم نیز راه به جایی نخواهیم برد، زیرا باید اثبات کنیم که علاوه بر کمک مالی دولت به افراد یا گروه‌هایی که در پشت حملات سایبری قرار دارند، در طراحی حملات سایبری نیز با آن‌ها همکاری داشته و به آن‌ها کمک کرده است. نخستین معضل در بحث حملات سایبری مطابق این معیار یافتن این است که دولت چگونه و از چه طریقی به گروه‌ها و افراد هدایت‌کنندهٔ حملات سایبری کمک مالی کرده است و مهم‌تر از اثبات مسئلهٔ کمک مالی اثبات همکاری و کمک در طراحی حملات سایبری است. ارتکاب حملات سایبری به‌گونه‌ای است که از مدت‌ها قبل چنین حملاتی طراحی و پس از ماه‌ها و حتی سال‌ها هدایت می‌شوند. ازآنجاکه این حملات با فناوری‌های حوزهٔ سایبری انجام می‌گیرند و ابزار مورداستفاده ویروس‌ها، کرم‌ها و سایر ابزار مرتبط با این حوزه است، حتی طراحی این حملات با طراحی حملات با استفاده از سلاح‌های سنتی بسیار متفاوت است. ممکن است حملات سایبری در کشوری طراحی شوند و با استفاده از حافظه‌های جانبی و به‌صورت کاملاً نامرئی به کشور هدف انتقال داده شوند. یکی از روش‌هایی که مورداستفادهٔ هکرها و سایر طراحان حملات سایبری قرار می‌گیرد انداختن فلش مموری‌های آلوده به ویروس در پارکینگ‌های خودروی بعضی از شرکت‌ها است و گاه کارکنان بی‌تجربه و ناشی این فلش مموری ها را برداشته و از کامپیوترهای شرکت‌ها استفاده می‌کنند. پس از مدتی، ویروس به همین سادگی وارد سیستم‌های کامپیوتری می‌شود و کامپیوترهای بسیاری را در شرکت آلوده می‌کند. چنین ظرفیت فناوری سایبری باعث می‌شود که به‌هیچ‌وجه نتوان عامل و فاعل حملات سایبری را مشخص نمود.

۶. معیار مؤثر برای اثبات مسئولیت دولت‌ها در برابر حملات سایبری عوامل غیردولتی

معیارهای انتساب اقدامات گروهی غیردولتی به دولت پیش از عصر اینترنت و همراه شدن حملات سایبری با حملات مسلحانه تعیین‌شده است (Collion, 2013, p.55). معیارهای ارائه‌شده در قضایای نیکاراگوئه و تادیچ راه حل مؤثری برای حملات سایبری ارائه نمی دهند. کارشناسان متعددی به دنبال ارائهٔ راهکاری برای حل مشکل اثبات مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری بوده‌اند. مارگلیز در مقاله‌ای با عنوان «حاکمیت و حملات سایبری: چالش‌های فناوری برای حقوق مسئولیت دولت» معیار کنترل مجازی[2] را ارائه کرده است و عقیده دارد که این معیار می‌تواند در بحث اثبات مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری مؤثرتر باشد. مطابق این معیار، دولتی که کمک مالی یا کمک‌های دیگری را برای گروه‌های غیردولتی فراهم کرده است مسئولیت دارد (Margulies, 2013, p. 496). البته مشکل معیار مطرح‌شده از سوی ایشان اثبات نقش دولت‌ها در کمک مالی یا سایر کمک‌ها است؛ یعنی چگونه می‌توان اثبات نمود که واقعاً دولتی به عوامل خصوصی برای ارتکاب حملات سایبری کمک مالی کرده یا کمک‌های دیگری را فراهم آورده است. چنین چالشی معیار کنترل مجازی را هم برای اثبات مسئولیت دولت‌ها بی‌اثر می‌نماید. دولت‌ها، هنگام تعیین معیار جدید مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری عوامل غیردولتی، باید مشکل شناسایی دولتی را که حملات سایبری از خاک آن انجام می‌گیرد درنظر داشته باشند، زیرا با تعیین محل هدایت حملات سایبری تا حدی می‌توان به سرنخ‌هایی دربارهٔ مرتکبان این حملات دست یافت. بنابراین، بهترین راه‌حل در بحث اثبات مسئولیت بین‌المللی دولت‌ها در

1. prosecutor v. Tadic. Judgment . (Appeals chamber ICTY)15 July 1999 : para 124
2Test of Virtual Control

برابر حملات سایبری عوامل غیردولتی توجه به این نکته است. یکی از اصول حقوق بین‌الملل اصل مراقبت بایسته[1] است که بارها در دیوان‌های بین‌المللی تأیید شده و به معنای هوشیاری لازم در انجام تعهد حقوقی است. مطابق این اصل، اگر دولت در اجرای تعهدات خود فاقد مراقبت بایسته باشد، این اصل مبنایی برای مسئولیت بین‌المللی ایجاد خواهد کرد (حدادی و مرادیان، ۱۳۹۸، ص ۱۶۵). تعهدات مراقبت بایسته مبنایی برای ایجاد مسئولیت دولت‌ها است و ریشه در اصول کلی حقوق دارد و با نوشته‌های گروسیوس و واتل وارد ادبیات حقوقی شده است. این مفهوم در تمامی حوزه‌های حقوق بین‌الملل نظیر حقوق مسئولیت دولت، حقوق بین‌الملل سرمایه‌گذاری و حقوق بین‌الملل محیط‌زیست وارد شده است و کشورها را به اقدامات مبتنی بر هوشیاری مداوم ملزم می‌کند (حدادی و مرادیان، ۱۳۹۸، ص ۱۶۶). اصطلاح مراقبت بایسته در لغت به معنای مراقبت مقتضی یا احتیاط منطقی است. در مفهوم حقوقی به معنای مراقبت و هوشیاری است که به‌طور منطقی از کسی انتظار می‌رود و عرفاً در اوضاع و احوال خاصی از سوی فرد متعارفی که به دنبال اجرای تعهد حقوقی است انجام می‌پذیرد.[2] اصل مراقبت بایسته بیشتر در بحث مسئولیت دولت‌ها در حوزهٔ حقوق بین‌الملل محیط‌زیست مطرح شده است. در قضیهٔ تریل اسملتر، دیوان داوری رأی دادکه تحت اصول حقوق بین‌الملل و حقوق ایالات متحده هیچ کشوری حق ندارد از سرزمین خود به‌گونه‌ای استفاده کند یا اجازهٔ استفاده دهد که آثار ناشی از آن موجب ایراد آسیب به سرزمین، اموال یا اشخاص دولت دیگر شود.[3] بر اساس این رأی دیوان داوری، دولت‌ها برای اعمال اشخاص خصوصی در خاک خود و عدم پیشگیری از ورود خسارت به سایر کشورها مسئولیت دارند. این اصل مهم و اساسی، یعنی اصل پیشگیری که در دعوای تریل اسملتر مطرح شد، در قضیهٔ کانال کورفو نیز مورد نظر دیوان بین‌المللی دادگستری قرار گرفت. در این قضیه، دیوان بین‌المللی دادگستری رأی داد که همهٔ کشورها متعهدند که عالمانه اجازه ندهند از خاک آن‌ها برخلاف حقوق سایر کشورها استفاده شود.[4] همچنین، در پیش‌نویس کنوانسیون حقوق بین‌الملل دربارهٔ مسئولیت دولت در آسیب‌های فرامرزی ناشی از فعالیت‌های خطرناک (۲۰۰۱) نیز بیان شده است که دولت‌ها موظفند از ورود آسیب‌های ناشی از فعالیت‌هایی که در حقوق بین‌الملل منع نشده اما نتایج فیزیکی آن‌ها ممکن است موجب ورود آسیب فرامرزی عمده شود پیشگیری کنند.[5] بنابراین، چنان‌که مشاهده می‌شود ، دولت‌ها بر اساس حقوق بین‌الملل از آسیب زدن به محیط زیست سایر کشورها منع شده‌اند. حوزهٔ محیط زیست شباهت بسیار زیادی با حوزهٔ سایبر دارد، زیرا خسارات این دو حوزه بدون استفاده از سلاح‌های سنتی وارد می‌شوند. در هر دو حوزه ممکن است عوامل غیردولتی اقدامات مخربی را بدون اطلاع دولت سرزمینی انجام دهند، اما ممکن است خسارات بسیار فراوانی به دولت همسایه وارد شود. فناوری‌های حوزهٔ سایبری به‌گونه‌ای است که از هر جای جهان امکان هدایت حملات سایبری وجود دارد. تنها چیزی که می‌تواند به حل مشکل حملات سایبری در جهان کمک کند نظارت و کنترل دقیق دولت‌ها برقلمرو سرزمینی آن‌ها به‌منظور پیشگیری از انجام حملات سایبری علیه دولت‌های دیگر است.

نتیجه‌گیری

به‌علت پیشرفت‌های گستردهٔ فناوری اطلاعات و ارتباطات در قرن بیست‌ویکم و وابستگی روزافزون دولت‌ها به فناوری‌های این حوزه، این قرن را می‌توان قرن فناوری اطلاعات نامید. وابستگی تمدن و حیات بشری به فناوری‌های این حوزه به حدی است که نمی‌توان هیچ حوزه‌ای از تمدن و حیات بشری را مستقل از این فناوری ها تصور نمود. این وابستگی توجه دولت ها را به استفاده از این فضا برای مقاصد سیاسی و اقتصادی معطوف کرده است. دولت‌ها، برای طفره‌رفتن از مسئولیت بین‌المللی، حملات سایبری را به‌وسیلهٔ عوامل غیردولتی انجام می‌دهند. همچنین، چون حملات سایبری پنهانی انجام می‌گیرند، ردیابی آن‌ها بسیار مشکل است. چنین امری انگیزه‌ای دوچندان به دولت‌ها برای استفاده از مزایای این حوزه داده است، تا جایی که امروزه شاهد ارتکاب میلیون‌ها حملهٔ سایبری در جهان هستیم که باعث هرج‌ومرج در روابط بین دولت‌ها شده

1. Due Diligence
2. Black's Law Dictionary, “Due Diligence” entry, 8th ed. , 1990, p. 488.
3. Trail Smelter case (USA v. Canada), Arbitration Judgment, 11 March1941, Reports of International Arbitral Awards (RIAA), vol. III, p. 1965, available at: http://legal. un. org/riaa/cases/vol_III/1905-1982. pdf,p.1965
4. I. C. J. Reports 1949,Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania), 1949, ICJ Report,p.22
5. International Law Commission (ILC), Draft Articles on Prevention of Trans-boundary Harm from Hazardous Activities, 2001,art 1

است. برای سروسامان‌دادن به وضعیت آشفته‌بازار کنونی جهان، در قدم اول باید دولت‌ها با همکاری هم رژیم حقوقی مناسبی برای اثبات مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری عوامل غیردولتی تدوین کنند، زیرا بدون چنین رژیمی نمی‌شود به این وضعیت آشفته سروسامان داد. رژیم‌های کنونی مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری عوامل غیردولتی شامل معیارهای کنترل مؤثر و کنترل کلی است که به‌علت معایبشان برای حوزهٔ سایبر مناسب نیستند؛ زیرا حملات سایبری به‌گونه‌ای پنهان و ناشناس انجام می‌گیرند که یافتن ارتباط بین دولت‌ها و اشخاصی که در پشت حملات سایبری قرار دارند مشکل است و اثبات مسئلهٔ کنترل مؤثر و کنترل کلی بسیار دشوار است. تنها معیار مناسب برای اثبات مسئولیت بین‌المللی دولت‌ها در برابر حملات سایبری معیار مراقبت بایسته است، زیرا بر اساس آن هیچ کشوری حق ندارد از سرزمین خود به‌گونه‌ای استفاده کند یا اجازهٔ استفاده دهد که آثار ناشی از آن موجب ایراد آسیب به سرزمین، اموال یا اشخاص دولت دیگر شود. پذیرش چنین معیاری از طرف جامعهٔ جهانی باعث می‌شود که دولت‌ها نظارت و کنترل بیشتری بر سرزمین خود داشته باشند. این کنترل تأثیری مثبت و بسیار مهم در کاهش حملات سایبری در جهان خواهد داشت.

منابع

اصلانی، جبار و رنجبریان، امیرحسین (۱۳۹۴). بررسي تطبيقي و تحليل تعريف حملهٔ سايبری از منظر دكترين، رويهٔ كشورها و سازمان‌های بين‌المللی در حقوق بين‌الملل. *تحقیقات حقوقی*، *۱۸* (۷۱)، ۲۵۷-۲۷۸.

امیری، علی و حیدری‌فرد، مهدی (۱۳۹۷). جنگ‌های سایبری: چالش‌ها و راهکارهای تعامل در پرتو مقررات توسل به زور». *سیاست خارجی*، ۳۲ (۳)، ۱۸۲-۱۵۳.

حدادی، مهدی و مرادیان، بهرام (۱۳۹۸). مفهوم مراقبت بایسته در حقوق بین‌الملل و مقررات گروه ویژه اقدام مالی. *مجله حقوق بین‌المللی*، ۳۶ (۶۱)، ۲۰۲-۱۶۵.

حلمی، نصرت‌الله (مترجم) (۱۳۸۷). *مسئولیت بین‌المللی دولت و حمایت سیاسی*. تهران: نشر میزان، چاپ اول.

راعی، مسعود (۱۳۸۸). کنترل کلی یا مؤثر عاملی برای تحقق مسئولیت بین‌المللی دولت‌ها؟. *مطالعات حقوق خصوصی*، ۳۹ (۳)، ۱۵۱-۱۶۴.

ضیایی بیگدلی، محمدرضا (۱۳۸۴). *حقوق بین‌الملل عمومی*. تهران: انتشارات گنج دانش، چاپ بیست‌ویکم.

قرشی سروندانی، سیده‌نرگس (۱۳۹۱). *مسئولیت بین‌المللی دولتها در قبال حملات سایبری*. پایان‌نامهٔ کارشناسی ارشد، دانشکدهٔ حقوق دانشگاه بهشتی.

ملکی‌زاده، امیرحسین (۱۳۹۲). ضابطهٔ کنترل در نظام مسئولیت بین‌المللی؛ وحدت یا تعارض رویهٔ قضایی بین‌المللی. *مجله حقوقی دادگستری*، *۷۷* (۸۲)، ۱۹۱-۱۶۰.

نصیری محلاتی، ژوبین (۱۳۸۹). *بررسی انطباق تصمیمات محاکم آمریکا در انتساب اعمال افراد و گروه‌ها به دولت ایران*. پایان‌نامهٔ کارشناسی ارشد، دانشگاه شهید بهشتی.

Collin, S. A. (2013). Attribution issues in cyberspace. *Chicago-Kent Journal of International and Comparative Law*, *13*(2), 57-82.

Kulesza, J. (2009). State Responsibility for Cyberattacks on International Peace and Security. *Polish Yearbook of International Law*, (29), 139-152.

Liu, I. Y. (2017). State Responsibility and Cyberattacks: Defining Due Diligence Obligations. *The Indonesian Journal of International and Comparative Law*, *4*, 191.

Margulies, P. (2013). Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility. *Melbourne Journal of International Law*, *14*(2), 496-519.