Economic Jurisprudence Studies
Review on New Researches of Jurisprudence and Law
2021 - 2022

Explain the situation of active governments in relation to cyber attack

Hamid Reza Aghababaian[1], Maryam Moradi[2*], Seyed Baqer MirAbbasi[3]

1. Department of International Law, Qeshm Branch, Islamic Azad University, Qeshm, Iran.
2. Assistant Professor, Department of Law and Political Science, Qeshm Branch, Islamic Azad University, Qeshm, Iran.
3. Professor, Department of Law and Political Science, Tehran Branch, University of Tehran, Tehran, Iran.

ARTICLE INFORMATION

Article Type: Original Research

Pages: 325-343

Article history:

Received: 18 Sep 2021

Edition: 6 Nov 2021

Accepted: 22 Jan 2022

Published online: 12 Mar 2022

Keywords:

Active Government, Cyber-Attacks, International Law, Cyberspace

Corresponding Author:
Maryam Moradi
Address:
Department of Law and Political Science, Qeshm Branch, Islamic Azad University, Qeshm, Iran.
Orchid Code:
0000-0003-1856-3947
Tel:
09126607291
Email:
moradimaryam@yahoo.com

ABSTRACT

Background and Aim: Cyber-attacks are one of the most complex security concerns in modern times. Given the importance of this issue, the present study seeks to examine the situation of active governments in relation to cyber-attacks.

Materials and Methods: The present article is theoretical, research method, qualitative and descriptive and analytical.

Ethical considerations: In the present study, ethical principles such as scientific referral and based on respect for authors' rights have been considered.

Results: Cyber-attacks as a harmful act, despite their widespread threats and high destructive power, are not prohibited according to international documents. Therefore, harmful actions caused by cyber threats are not prohibited, and this issue can be considered as a threat of such attacks.

Conclusion: The negative effects of a cyber-attack can affect other governments than the government against which the cyber-attack is designed. The fight against cyber-attacks and the damage caused by them must be organized in international law in line with the rights and interests of the affected country. Considering harmful cyber-attacks as war attacks is an international legal solution to eliminate the resulting threats.

Cite this article as: Aghababaian HR, Moradi M, MirAbbasi SB. Explain the situation of active governments in relation to cyber attack. *Economic Jurisprudence Studies 2021-2022*; Review on New Researches of Jurisprudence and Law.

This open-access article distributed under the terms of the Creative Commons Attribution NonCommercial 4.0 License (CC BY-NC 4.0).

مطالعات فقه اقتصادی
ویژه نامه جستارهای نوین فقه و حقوق ۱۴۰۰

فصلنامه مطالعات فقه اقتصادی، ویژه نامه جستارهای نوین فقه و حقوق، ۱۴۰۰

تبیین وضعیت دولت‌های کنشگر نسبت به حمله سایبری

حمیدرضا آقابابایی[۱]، مریم مرادی[*]، سید باقر میرعباسی[۳]

۱. گروه حقوق بین‌الملل، واحد قشم، دانشگاه آزاد اسلامی، قشم، ایران.

۲. استادیار گروه حقوق و علوم سیاسی، واحد قشم، دانشگاه آزاد اسلامی، قشم، ایران.

۳. استاد گروه حقوق و علوم سیاسی، واحد تهران، دانشگاه تهران، تهران، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۳۴۳-۳۲۵

سابقه مقاله:

تاریخ دریافت: ۱۴۰۰/۰۶/۲۷

تاریخ اصلاح: ۱۴۰۰/۰۸/۱۵

تاریخ پذیرش: ۱۴۰۰/۱۱/۰۲

تاریخ انتشار: ۱۴۰۰/۱۲/۲۱

واژگان کلیدی:

دولت کنشگر، حملات سایبری، حقوق بین‌الملل، فضای سایبری.

نویسنده مسوول:

مریم مرادی

آدرس پستی:

ایران، قشم، دانشگاه آزاد اسلامی، واحد قشم، گروه حقوق و علوم سیاسی.

تلفن:

۰۹۱۲۶۶۰۷۲۹۱

کد ارکید:

0000-0003-1856-3947

پست الکترونیک:

moradimaryam@yahoo.com

چکیده

زمینه و هدف: حملات سایبری از جمله نگرانی‌های پیچیده امنیتی در دوران معاصر هستند. با توجه به اهمیت موضوع، پژوهش حاضر به دنبال بررسی وضعیت دولت‌های کنشگر نسبت به حملات سایبری است.

مواد و روش‌ها: مقاله حاضر از نوع نظری، روش تحقیق، کیفی و از نوع توصیفی و تحلیلی است.

ملاحظات اخلاقی: در پژوهش حاضر اصول اخلاقی نظیر ارجاع‌دهی علمی و مبتنی بر رعایت حقوق مؤلفین مدنظر قرار گرفته است.

یافته‌ها: حملات سایبری به عنوان یک عمل زیانبار، علیرغم تهدیدات گسترده و قدرت تخریبی بالایی دارند، مطابق اسناد بین‌المللی منع نشده‌اند. بنابراین عمل زیانبار ناشی از تهدیدات سایبری ممنوع نیستند و همین موضوع باعث تهدید تلقی شدن اینگونه حملات باشند.

نتیجه: اثرات منفی ناشی از حمله سایبری می‌تواند گریبانگیر دولت‌های دیگری غیر از دولتی که حمله سایبری علیه او طراحی شده را دربر بگیرد. مبارزه با حملات سایبری و خسارات ناشی از آن می‌بایست در حقوق بین‌الملل و در راستای حقوق و منافع کشور خسارت‌دیده سامان داده شود. در نظر گرفتن حملات سایبری خسارت‌بار در زمره حملات جنگی، راهکار حقوقی بین‌المللی برای دفع تهدیدات ناشی از آن است.

© تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق بشر اسلامی ایران می‌باشد.

۱. مقدمه

هنگامی که یک حمله سایبری رخ می‌دهد، ممکن است دولت‌های مختلفی را تحت تأثیر قرار دهد. این دولت‌ها که در آن‌ها به عنوان کنشگران حملات سایبری یاد می‌شود، شامل دولت‌هایی است که از یک‌سو مبدأ حمله سایبری به شمار آمده و بازیگر اصلی این حمله محسوب می‌شوند و از سوی دیگر دولت یا دولت‌هایی که به طور مستقیم یا غیرمستقیم از این حمله سایبری تأثیر پذیرفته و به نوعی خسارت دیده‌اند. خطرها و زیان‌هایی که فعالیت‌های سایبری به خصوص حملات سایبری برای دولت‌ها در پی دارند دارای نمونه‌های متنوعی هستند. جبران خسارات فرامرزی که ناشی از فعالیت‌های خطرناک قانونی باشد، مسئله‌ای است که مشکلات زیادی را بین دولت‌ها ایجاد کرده و نیازمند تدوین قواعد شفاف و الزام‌آور در حقوق بین‌الملل است. معاهداتی چند سیستم‌های پرداخت غرامت را در موارد شایع و مهم خسارت‌های فرامرزی ایجاد کرده است. این سیستم‌ها به فعالیت‌های خاص مربوط بوده و مسئولیت را در درجه اول متوجه اشخاص و طرف‌های خصوصی می‌داند. این معاهدات خاص که بیشتر در حوزه آلودگی‌های زیست‌محیطی ایجاد شده است، بیانگر آنست که جامعه بین‌المللی به سمت توسعه قواعد حقوقی عام برای همه انواع فعالیت‌های پرخطر اما قانونی حرکت کرده است. از این رهگذر با اقتباس از قواعد مسئولیت مدنی در قوانین داخلی، رژیم مسئولیت مدنی بین‌المللی و به دنبال آن قواعد پیرامون مسئولیت محض بین‌المللی یا مسئولیت دولت‌ها در قبال اعمال منع‌نشده بین‌المللی مطرح شده است که هنوز هم به صورت قواعد عام الزام‌آور در قالب کنوانسیونی بین‌المللی درنیامده و تاکنون فقط دو طرح پیش‌نویس از سوی کمیسیون حقوق بین‌الملل در این خصوص تنظیم شده است که اصول آن جنبه توصیه‌ای دارد. با توجه به قابلیت‌های فراوان حملات سایبری این احتمال در آینده وجود دارد که این حملات بتواند خسارت فیزیکی و تخریبی گسترده‌ای را باعث شود. بر این اساس هدف اصلی پژوهش حاضر تبیین وضعیت دولت‌های کنشگر نسبت به حمله سایبری می‌باشد.

در تحقیقات متعددی، بحث حملات سایبری و ارتباط آن با جایگاه دولت‌ها مورد توجه قرار گرفت. از جمله در مقاله "بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل" که توسط اصلانی و رنجبریان (۱۳۹۴) نگارش شده است، تهدیدات سایبری را ناشی از گسترش همه‌جانبه تکنولوژی در زندگی انسان معاصر می‌دانند. به باور نویسندگان، فقدان یک اجماع حقوقی در جهان معاصر، حملات سایبری را به عنوان یک خطر جدی مطرح ساخته است. از این جهت حملات سایبری، آشکارا تهدیدی برای حاکمیت دولت‌ها در نظر گرفته می‌شود. در مقاله خلیلی‌پور رکن‌آبادی و نورعلی‌وند (۱۳۹۱)، با عنوان "تهدیدات سایبری و تأثیر آن بر امنیت ملی"، نیز بیان شده است که جلوه‌های تهدیدات امنیتی بسیار متنوع و گسترده شده است و بدلیل

تنوع و تغییرات ناشی از دنیای تکنولوژی، امکان مقابله دقیق و متناسب با این تهدیدات بسیار دشوار است.

قاسمی و بارین چهارپخش (۱۳۹۱) در مقاله "حملات سایبری و حقوق بین‌الملل"، به این نکته اشاره می‌کنند که در صورت وقوع خسارات مادی ناشی از حملات سایبری و بر مبنای آنچه وفق ماده ۵۱ منشور سازمان ملل متحد مطرح شده است، عامل این حملات خواه دولت، فرد و یا گروه خاصی باشد، ملزم به پرداخت خسارات است. ضمن اینکه در چنین شرایطی، دفاع کشور خسارت‌دیده، دفاعی مشروع است که برای دفع خطرات صورت می‌گیرد. اثری با عنوان "سایبر تروریسم؛ تروریسم در عصر اطلاعات" که توسط مرتضی نورمحمدی (۱۳۹۰) جمع‌آوری شده است، بیش از هر چیز بر عامدانه بودن جرایم اطلاعاتی در دوران معاصر و طراحی آن از سوی نظام‌های سیاسی و فرهنگی قوی برای شکست رقبا و حریفان خود در عرصه نظام بین‌الملل اشاره دارد. به نظر می‌رسد در این پژوهش، جنبه‌های فرصت‌آمیز فضای سایبر چندان مورد توجه نیست. مقاله "مسؤولیت کیفری در فضای سایبر" (۱۳۸۹) که توسط مهدی فضلی نگارش شده است، امکان و یا عدم امکان جرم‌انگاری در فضای سایبری را به بحث گذاشته است. بحث نویسنده بیش از هر چیز دشواری‌های جرم‌انگاری در فضای سایبر به دلیل نامعلوم بودن عاملان آن و عدم مکان‌مندی آنان متمرکز است.

با توجه به پژوهش‌های مطرح شده، برای تبیین وضعیت دولت‌های کنشگر نسبت به حملات سایبری پژوهشی جدی صورت نگرفته است. از این جهت پژوهش حاضر، نو و متمایز می‌باشد. سؤال پژوهش حاضر این است که با توجه به شرایط حاکم بر حملات سایبری، وضعیت دولت‌های مهاجم در قبال اَعمال خطرناک خود چگونه است؟ در این راستا، این فرضیه مطرح است که تبیین اَعمال خطرناک دولت‌ها از منظر حقوق بین‌الملل در زمینه حملات سایبری، بسیار دشوار و نیازمند شناسایی مصادیق حملات سایبری و ارائه قوانینی فراگیر و به‌روز است.

۲. مواد و روش‌ها

پژوهش حاضر از نوع نظری و کیفی است. با توجه به نوع پژوهش، پژوهشگر از روش توصیفی-تحلیلی برای بررسی موضوع استفاده نموده است.

۳. ملاحظات اخلاقی

نگارندگان با رعایت اصول امانتداری، ارجاع‌دهی دقیق و علمی و همچنین رعایت استناد به منابع مختلف، نسبت به جمع‌آوری و نگارش مطالب مربوط به پژوهش اقدام کردند.

۴. یافته‌ها

جامعه بین‌المللی در حیطه فضای سایبر، موفق به تدوین قواعد مشخصی که همه جوانب توسل به سلاح‌های سایبری را تعیین سازد، نشده اما همان طور که اشاره شد، حملات طراحی شده از این فضا قابلیت ایجاد خسارات گسترده‌تری را نسبت به سلاح‌های سنتی خواهند داشت، که به علت سهولت دسترسی به آن و کم هزینه‌تر بودن آن

دولت‌ها را برای توسل بـه ایـن ابرسلاح جریـح می‌سازد. امروزه تهدیدات موجود و بالقوه در فضای امنیتی اطلاعات در بین جدی‌ترین تعارضات قرن ۲۱ قرار دارند. تأثیرات این تهدیدات متضمن خطرات بسیاری برای امنیت عمـومی، امنیت دولت‌ها و در نهایت بقای جامعه بین‌المللی خواهد بود. بنابراین می‌توان امنیت موجود در این فضا را حق مسلمی برای همه جهانیان دانست و دولت‌ها را به نمایندگی از ملت‌شان منتفع از این حق شناخت و تأمین امنیت این فضا را یک تعهد جمعی شناخت و در غیاب یک نظام منسجم حاکم بر این حیطه با وام‌گیری از نظام‌های موجود مسئله را حل‌وفصل نمود. همان‌طور که اشاره شد، گفتیم که می‌توان با دیدی وسیع به منشور نگریست و حملات سایبری به تأسیسات بنیادین کشورها را در صورت برخورداری از شرایط لازمه ناقض اصول متعددی من‌جمله منع توسل به زور دانست و علاوه بر دولت‌های متضرر، دولت‌های ثالث را هم محق به استناد به مسئولیت دولت خاطی در این خصوص دانست.

برخی از تعهدات از درجه اعتبار و جایگاه ویژه‌ای برخوردار می‌باشد که در نتیجه، نگاه دولت‌ها و جامعه بین‌المللی به آن‌ها متفاوت از سایر تعهدات می‌باشد. این تعهدات هم جنبه عرفی و هم جنبه قراردادی دارند. در این نوع تعهدات، دولت مرتکب در برابر کل جامعه بین‌الملل مسئول است و این گونه نیست که فقط در برابر دولت صدمه‌دیده مسئول باشد. پذیرش چنین دیدگاهی به معنای ایجاد فصل جدیدی در روابط بین‌المللی به شمار می‌آید.

از جمله آثار حاصل از این نگاه، پذیرش اقدام متقابل در ارتباط با تعهدات چندجانبه برای کل دولت‌های جامعه جهانی است، در حالی که در معاهدات دوجانبه، این نوع اقدام متقابل تنها متعلق به دولت صدمه‌دیده است. اثر دیگر مربوط به نقض تعهد می‌باشد. نقض یک تعهد بین‌المللی چندجانبه به همان صورتی که نقض یک تعهد بین‌المللی رخ می‌دهد، تحقق می‌گیرد. بنابراین، رفتاری مغایر با آن تعهد بین‌المللی می‌تواند نقض آن تعهد را به دنبال داشته باشد. هرگاه یک حمله سایبری موجب نقض تعهد بین‌المللی چندجانبه و یا همه‌جانبه شود، هر دولتی می‌تواند به مسئولیت آن دولت استناد کند و از آن دولت بخواهد که بر اساس تعهدات خود عمل کند. اینکه چه معیاری توسط این دولت‌ها برای جلوگیری از نقض تعهد اتخاذ خواهد شد، باید بر اساس محتوای تعهد نقض شده صورت گیرد و نمی‌توان در این باره به یک فرمول کلی بسنده کرد. نکته قابل ذکر در ارتباط با این نوع تعهدات، ضرورت وجود یک رویه ناظر بر تعهدات بین‌المللی دولت‌هاست. اهمیت این نوع تعهدات، اقتضا می‌کنند که جامعه جهانی به وسیله ابزارهای خاص خود، مثل کمیته‌های بین‌المللی ناظر، عملکرد دولت‌ها را مدنظر قرار دهد. وجود یک رژیم خاص مسئولیت در ارتباط با این نوع تعهدات می‌تواند زمینه‌های پیش‌گیری از وقوع آن را افزایش دهد.

۵. بحث

۵-۱. حملات سایبری و اهمیت مقابله با تهدیدات ناشی از آنان

فضای سایبر، فضایی غیرملموس و غیرقابل مشاهده است که توسط شبکه‌ها و نظام اطلاعاتی انـجام می‌شود و دنیای مجازی را به عنوان دنیایی در کنار دنیای واقعی شکل داده است (فضلی، ۱۳۸۹، ۱۷). تأثیرگذاری فضای سایبری به حدی گسترده شده است که اغلب نظام‌های حقوقی بین‌المـللی، منطقه‌ای و داخلی درصدد اتخاذ راهکارهایی برای بهبود روش‌های مؤثر بهره‌مندی از این فضای نوین و دفع تهدیدات ناشی از آن هستند. نظارت بر فضای سایبر دشواری‌های خاص خود را دارد و به دلیل تنوع ناشی از حملات سایبری، جرم‌انگاری حملات سایبری همواره در حال تغییر و تحول است. یکی از دشواری‌های اساسی در این زمینه، عدم دسترسی و یا دشوار بودن دسترسی به مکانی است که جرم سایبری در آن رخ می‌دهد. به عنوان مثال، یک حمله سایبری که مدعی است از سوی کشور الف انجام می‌شود، ممکن است محل قرار گرفتن حمله‌کنندگان در آن کشور نباشد (برینر، ۲۰۰۶، ۴۲۴). بنابراین هم پی بردن به نقش عوامل اصلی تهدیدات سایبری و هم مدون بودن یک نظام حقوقی برای شناسایی و مجازات تهدیدکنندگان بخش مهمی از دشواری‌های ناشی از تهدیدات و حملات سایبری هستند. به این دلیل که در فضای حملات سایبری، ابهامات قانونی زیادی درباره پاسخگو کردن عاملان حملات سایبری وجود دارد (تهاری و رولینز، ۲۰۰۹، ۶۷). از این منظر، دستیابی به روش‌ها، راهکارها و سازوکارهای حقوقی برای پاسخگو کردن افراد و نهادها و همچنین پیشگیری از حملات خطرناک، بخش مهمی از دغدغه نظام حقوقی بین‌المللی در قبال حملات سایبری است.

۵-۲. روش‌های پیش‌بینی‌شده در طرح ۲۰۰۱ پیشگیری از آسیب فرامرزی

در حوزه فضای سایبری، پیشگیری از حملات سایبری، بهترین ابزار برای مدیریت خطرات احتمالی ناشی از آن است. در حقیقت در پیشگیری از ضرر و زیان ناشی از حملات سایبری، امنیت فضای سایبر ابزار اساسی و مهم محسوب می‌شود. مسئولیت بین‌المللی دولـت‌ها در نظام حقـوق بین‌الملل اساساً بر مبنای نقض تعهدات بین‌المللی آن‌ها استوار است، با این حال خسارات حاصله از اعمال منع نشده بین‌المللی در فقدان چنین نقض تعهدی به بار آمده و برای جبران آن‌ها باید در پی مبنای دیگری برای مسئولیت بود. علی‌رغم توانایی بالای حملات سایبری در تخـریب سامانـه‌ها و داده‌های رایانه‌ای کشورها، هنوز هم ممنوعیتی در نظام حقوقی بین‌المللی برای دولت‌ها و بازیگران غیردولتی در خصوص توسل به آن وجود ندارد. بنابراین اگر به دنبال طرح مسئولیت بین‌المللی دولت در این خصوص هستیم، باید مبنای مسئولیت را مسئولیت بدون تقصیر دانست. در عرصه بین‌المللی هم طرح تخصیص زیان در موارد آسیب فرامرزی ناشی از فعالیت‌های خطرناک، این مبنا را ملاک قرار داده است. کمیسیون حقـوق

بین‌الملل که به موجب بند الف ماده ۱۳ منشور و قطعنامه ذی‌ربط مجمع عمومی، وظیفه عهده‌دار تدوین و توسعه تدریجی حقوق بین‌الملل شده، رسماً از سال ۱۹۸۷ مسئله مسئولیت بین‌المللی دولت‌ها برای اعمال منع نشده دستورکار خود قرار داد که حاصل تلاش آن تصویب طرح ۲۰۰۱ پیشگیری از آسیب فرامرزی ناشی از فعالیت‌های خطرناک و طرح اصول تخصیص زیان در موارد آسیب فرامرزی ناشی از فعالیت‌های خطرناک در سال ۲۰۰۶ بوده است. دولت‌ها می‌بایست برای اطمینان از جبران خسارت فرامرزی، به اتخاذ تدابیر مقتضی از جمله تصویب قاعده حقوقی مشتمل بر مسئولیت بدون تقصیر برای متصدیان فعالیت‌های خطرناک بپردازند (عبداللهی، ۱۳۹۰، ۲۲۵). در سال ۲۰۰۱ کمیسیون حقوق بین‌الملل در پنجاه و سومین نشست خود، پیش‌نویس مواد راجع به جلوگیری از خسارت فرامرزی ناشی از فعالیت‌های خطرناک را تصویب کرد. این پیش‌نویس قلمرو مقررات خود را محدود به پیشگیری ضرر و زیان فرامرزی ناشی از فعالیت‌های خطرناک محدود کرده و شامل پیشگیری زیان‌های غیرفرامرزی نمی‌شود. به عبارت دیگر، ایجاد رویه حقوقی برای دولت‌ها جهت مقابله با تهدیدات سایبری چندان محل بحث نبوده است. همچنان که امروزه بخش زیادی از فعالیت‌ها و حملات سایبری رخ می‌دهد که کمتر از منظر حقوق جنگ تحلیل می‌شود (هاتوی و اونا، ۲۰۱۲، ۸۳۹). بدین معنا که اقدامات دولت‌ها برای بهره‌مندی از اصل دفاع مشروع چندان درباره حملات سایبری مصداق ندارد. آنچه از منظر حقوقی موجود است، مربوط به تهدیدات فرامرزی و بین‌المللی است که از سطح جامعیت و فراگیری بیشتری برخوردار است. در هر صورت از منظر پیش‌نویس مزبور، دولت منشأ فعالیت متعهد است که از ضرر و زیان فرامرزی پیشگیری کند و اگر توانایی ایفای چنین تعهدی را نداشت، در آن صورت ملزم است در جهت کاهش خطر بروز این ضرر و زیان اقدام کند.

۵-۲-۱. پیشگیری از طریق اعطای مج

براساس پیش‌نویس، اعطای مجوز به فعالیت ممنوع نشده از سوی دولت منشاء فعالیت اولین جزء از اجزاء پیشگیری زیان ناشی از فعالیت‌های ممنوع نشده محسوب می‌شود.[۱] اعطای مجوز به این فعالیت‌ها حق و تکلیف دولت منشاء فعالیت ممنوع نشده محسوب می‌شود که از این طریق نظارت خود بر این فعالیت‌ها استقرار می‌بخشد. پیش‌نویس در خصوص اعطای مجوز مطالب زیر را مطرح کرده است:

دولت منشأ فعالیت باید اجازه قبلی خود را نسبت به فعالیت‌های زیر الزامی کند:

۱. هر نوع فعالیت متضمن خطر فرامرزی در سرزمین یا مکان‌های تحت کنترل و صلاحیت.

۲. هر نوع تغییر عمده در این فعالیت‌ها.

[۱] پاراگراف ۱ ماده ۶ پیش‌نویس کمیسیون حقوق بین‌الملل راجع به پیشگیری از زیان ناشی از اعمال منع نشده بین‌المللی.

۳. هر نوع طرحی که هدف آن تغییر یک فعالیت به فعالیت متضمن خطر ضرر فرامرزی باشد.

در هر صورت باید به این نکته نیز اشاره نمود که مقابله با تهدیدات سایبری نیازمند در نظر گرفتن ابعاد و آثار خطر و همچنین سایر جوانب آن ازجمله هزینه‌های رو به تزاید آن است (تاباسکو، ۲۰۱۱، ۸۸). به همین دلیل، فضای سایبر و تهدیدات و خطرات ناشی از آن، همواره برای دولت‌ها مهم بوده است و دولت‌ها سعی می‌کنند تا با انجام اقدامات حقوقی هماهنگ در داخل و خارج، نسبت به رفع تهدیدات ناشی از این تهدیدات اقدام متناسبی انجام دهند.

۵-۲-۲. پیشگیری از طریق ارزیابی خطر

دولت منشأ می‌بایست قبل از اعطای مجوز برای انجام فعالیت‌های خطرناک، نسبت به ارزیابی‌های صورت گرفته در خصوص خطرات ناشی از فعالیت‌هایی که موجب زیان‌های فرامرزی می‌شوند اطمینان حاصل کند. در این رابطه، ماده ۷ پیش‌نویس اشعار داشته است: «هر نوع تصمیم در خصوص اجازه به یک فعالیت در چارچوب مواد حاضر، باید به ویژه، بر ارزیابی ضرر فرامرزی احتمالی ناشی از آن فعالیت، از جمله ارزیابی اثرات زیست‌محیطی آن، مبتنی باشد.»

۵-۲-۳. پیشگیری از طریق اعلام و اطلاع

چنانچه ارزیابی خطر، بر امکان خطر بروز ضرر فرامرزی دلالت کند در این صورت، دولت منشأ مکلف است این خطر و ارزیابی انجام‌شده را به موقع به دولت و یا دولت‌های متأثرشونده از خطر اطلاع داده و اطلاعات فنی و سایر اطلاعات مرتبط را به آن دولت یا دولت‌ها منتقل کند. در این حالت، دولت منشأ نباید ظرف ۶ ماه و تا زمان دریافت پاسخ از جانب آن دولت یا دولت‌ها، اقدام به صدور جواز نسبت به فعالیت موردنظر کند.

روش دیگر پیشگیری ضرر و زیان فرامرزی تبادل اطلاعات بین دولت‌های منشأ و احتمالاً متأثرشونده پیرامون فعالیت‌های متضمن ضرر و همینطور اطلاع‌رسانی از وضعیت این فعالیت‌ها به عموم است. در این خصوص ماده ۱۳ پیش‌نویس بیان می‌دارد: «دولت‌های مربوط از طرق مقتضی، باید هر نوع فعالیت چارچوب این پیش‌نویس را همراه با اطلاعات ذی‌ربط راجع به آن فعالیت، خطر و ضرر موجود در آنکه می‌تواند در دیدگاه‌های عموم مؤثر یا تعیین‌کننده باشد، در اختیار آن‌ها قرار دهند.» تعهد به تبادل اطلاعات پس از آغاز فعالیت، متضمن ضرر و زیان احتمالی است. در این حالت، هر دو دولت منشأ فعالیت و دولت احتمالاً متأثرشونده، ملزم به تبادل اطلاعات شده‌اند.

در برخی فعالیت‌ها مانند فعالیت‌های هسته‌ای، تعهد به پیشگیری، پس از خاتمه آن فعالیت نیز استمرار پیدا می‌کند. در حقیقت خطر ضرر و زیان نیروگاه هسته‌ای که به طور کامل تعطیل و تجهیزات آن جمع‌آوری شده، می‌تواند همچنان باقی بماند و تا زمانی که این وضعیت وجود داشته باشد، تبادل اطلاعات و استمرار آن ضرورت خواهد داشت.

لازم به ذکر است که تعهد دولت‌ها در تبادل اطلاعات به صورت مطلق در این پیش‌نویس بیان نشده است. بدین توضیح که پیش‌نویس در پاره‌ای از موارد این حق را به دولت‌ها اعطا کرده که از دادن اطلاعات به دیگر دولت‌ها امتناع ورزند. پیش‌نویس به دولت منشأ فعالیت اجازه داده است که در مواردی که اطلاعات به امنیت ملی یا اسرار تجاری یا مالکیت معنوی آن مربوط می‌شود از ارائه آن به دولت احتمالاً متأثرشونده خودداری کند. در این خصوص ماده ۱۴ پیش‌نویس بیان کرده است: «داده‌ها و اطلاعاتی که برای امنیت ملی دولت منشأ و یا برای حراست اسرار صنعتی آن حیاتی است یا به مالکیت معنوی مربوط می‌شود، می‌تواند ارائه نشود، اما دولت منشأ یا حسن‌نیت با دولت احتمالاً متأثر در مورد ارائه اطلاعات به قدر ممکن، تحت شرایطی همکاری خواهد کرد.»

۵-۳. مسئولیت متصدیان فعالیت‌های خطرناک در جبران خسارت

حملات سایبری در صورتی که منجر به ایجاد صدمات فیزیکی و ایجاد خسارت شوند، حتی می‌توانند به درگیری مسلحانه نیز منجر شوند (دورنان، ۲۰۰۴، ۳). بنابراین در صورت نادیده گرفتن فعالیت‌های ناشی از حملات سایبری، درگیر شدن منافع کشورها و بروز یک جنگ نیز محتمل است. به همین دلیل نباید حملات سایبری را به دلیل نامحسوس بودن و یا نامشخص بودن عاملان آن نادیده گرفت. از سوی دیگر، اساساً حقوق بین‌المللی عام، اصل تعهد مطلق به پیشگیری زیان ناشی از اعمال حق یا انجام فعالیت ممنوع نشده را تصدیق نمی‌کند، تعهد دولت‌ها به پیشگیری از زیان تعهد از نوع اعمال مراقبت‌های لازم یا به عبارت دیگر تعهد به وسیله است (رضایی، ۱۳۸۹، ۱۲۶). بدین توضیح که دولت‌ها اساساً تا حد توان و امکانات خود ملزم به پیشگیری زیان ناشی از فعالیت‌های پرخطر خود می‌باشند (مجموعه مقالات پیشگیری از فعالیت‌های خطرناک، ۲۰۰۱، ۳۹۱). در ارزیابی ایفا یا عدم ایفای تعهد دولت‌ها به پیشگیری زیان ناشی از اعمال حق یا انجام فعالیت ممنوع نشده لازم است عواملی از قبیل وسعت فعالیت، مکان آن، شرایط آب و هوایی خاص و مواد بکار رفته در آن فعالیت مدنظر قرار گیرد. آنچه ممکن است در یک مقطع زمانی معیار اعمال مراقبت لازم تلقی شود در مقطع زمانی دیگر ممکن است چنین نشود. پیشرفت‌های علمی و فنی می‌تواند در نحوه اعمال مراقبت‌های لازم مؤثر واقع شود. هر چند که در ایفای تعهد به اعمال مراقبت‌های مقتضی لازم است توانایی‌ها و امکانات متعهد در نظر گرفته شود. با وجود این، وضعیت امکانات و توان متعهد تحت هیچ شرایطی نمی‌تواند به طور مطلق را از تعهد خود معاف و مبرا سازد (همان، ۳۹۴).

پیشگیری کردن از تحمیل مسئولیت جبران خسارت‌های ناشی از فعالیت‌های پرخطر به متصدیان مربوط، رژیم‌های قراردادی بوده است. در ابتدا می‌توان شخص ثالث در زمینه انرژی هسته‌ای (کنوانسیون پاریس ۱۹۶۰) اشاره داشت. این کنوانیسیون متصدی فعالیت هسته‌ای اعم از این

که شخص خصوصی یا دولتی باشد را مسئول جبران هر گونه سلب حیات، جراحت، تخریب آسیب اموال دانسته و معتقد به مسئولیت محض متصدی بوده است (عبداللهی، ۱۳۹۰، ۲۴۲). همچنین بر طبق ماده ۴ کنوانسیون وین در خصوص مسئولیت مدنی ناشی از خسارات هسته‌ای، متصدی تأسیسات هسته‌ای برای خسارات هسته‌ای ناشی از نبرد نظامی، عملیات خصمانه، جنگ داخلی یا شورش مسئول نمی‌باشد (کنوانسیون وین درباره خطرات حملات هسته‌ای، ۴). ضمن اینکه متصدی برای خساراتی که از تشعشعات هسته‌ای به علت حوادث طبیعی که اوصاف استثنایی دارند به وجود آمده باشد مسئول نیست مگر این که قانون کشور دارای تأسیسات هسته‌ای مغایر آن مقرر کرده باشد این مورد بیانگر رویکرد مسئولیت مطلق نسبت به متصدی است.

کنوانیسون بعدی قابل ذکر در این خصوص، کنوانسیون بروکسل راجع به مسئولیت مدنی برای خسارت ناشی از آلودگی نفتی ۱۹۶۹ است که مسئولیت را متوجه مالک تانکرهای نفتی می‌کند. در کنوانسیون ۱۹۹۳ لوگانو در خصوص مسئولیت مدنی خسارت زیست‌محیطی ناشی از فعالیت‌های خطرناک هم متصدی را در قبال حوادثی که در زمان یا در خلال دوره‌ای که بر فعالیت موردنظر کنترل داشته، ایراد شود مسئول می‌شناسد. بند دوم ماده ۴ طرح ۲۰۰۶ تخصیص زیان ناشی از فعالیت‌های خطرناک نیز مسئولیت را به متصدی فعالیت مزبور تحمیل می‌کند. این موارد همگی حکایت از تمایل به خصوصی‌سازی مسئولیت و عدم تمایل دولت‌ها برای پذیرش مسئولیت خسارات ناشی از اعمال منع نشده دارد.

هر چند موارد ذکر شده صرفاً در خصوص خسارات زیست‌محیطی اعمال شده، اما می‌توان در خصوص خسارات ناشی از حملات سایبری نیز متصدیان مربوطه، شرکت‌ها و نهادهایی را که متولی ارائه خدمات اینترنتی هستند و بستر طراحی این حملات تقریباً به واسطه خدمات ارائه گردیده از سوی آن‌ها فراهم می‌شود، مسئول حفاظت از شبکه و نظارت درست بر فعالیت‌های خطرناکی که از رهگذر فضای سایبر صورت می‌گیرد، دانست. زیرا در واقع آن‌ها هستند که بستر فعالیت خطرناک را ایجاد کرده‌اند و در پی کسب منافع اقتصادی بوده‌اند، پس باید زیان ناشی از فعالیت خطرناک را متحمل شوند.

علاوه بر این، معاهدات راجع به جبران خسارت ناشی از فعالیت‌های خطرناک تمایل به تحمیل مسئولیت اولیه جبران خسارت بر متصدی فعالیت مربوطه داشتند. در عرصه فعالیت‌های زیست‌محیطی، متصدی یا بهره‌بردار کسی است که بر فعالیت موردنظر کنترل و نظارت دارد به عبارت دیگر بهره‌بردار کسی است که به موجب اصل «آلوده‌کننده باید بپردازد» مسئولیت دارد. دستورالعمل اتحادیه اروپا در خصوص مسئولیت خسارت زیست‌محیطی هم متصدی یا بهره‌بردار را شخص حقیقی یا حقوقی اعم از عمومی یا خصوصی قلمداد کرده که فعالیت حرفه‌ای را اجرا یا کنترل می‌کند یا اگر در قانون ملی پیش‌بینی شده باشد، شخصی است که قدرت اقتصادی مهم و

تعیین‌کننده بر کنترل فنی چنین فعالیتی به او واگذار شده و دارنده جواز فعالیت‌های مزبور را نیز دربرمی‌گیرد (گزارش پارلمان اروپا، ۲۰۰۴، ۶).

در عرصه فضای سایبر هم کنترل و نظارت فنی بر سرویس‌های اینترنتی در درجه اول به عهده شرکت‌های ارائه‌دهنده خدمات اینترنتی (ISPS) است، این‌ها شرکت‌هایی هستند که امکان دستیابی به اینترنت و سایر سرویس‌های وب را فراهم می‌نماید. مراکز ارائه‌دهنده خدمات اینترنت علاوه بر نگهداری و پشتیبانی از یک خط مستقیم به اینترنت، فعالیت‌های متعدد دیگری نظیر نگهداری و پشتیبانی از سرویس‌دهندگان وب را نیز انجام می‌دهند. با توجه به تعریف دستورالعمل اتحادیه اروپا که اشاره به دارنده مجوز هم کرده، می‌توان متصدیان کافی‌نت‌ها را نیز همانند شرکت‌ها مسئول شناخت. در اکثر جرایم اینترنتی رخ داده متصدیان کافی‌نت‌ها به دلیل عدم رعایت موارد قانونی قادر به معرفی کاربر موردنظر نخواهند بود و لاجرم مسئولیت اقدامات آن‌ها به عهده شخص متصدی کافی‌نت خواهد بود. رویکرد راجع به تحمیل مسئولیت بر متصدی ناشی از این تفکر است از فعالیت‌های خطرناک منتفع شده و در زمان وقوع خسارت بیشترین کنترل را بر فعالیت داشته، پس بار مسئولیت را اوست که باید به دوش کشد و غرامت را بپردازد. با این حال با توجه به حیله‌های هوشمندانه هکرها در طراحی حمله سایبری که گاه علی‌رغم تمام نظارت‌ها و کنترل‌ها صورت می‌گیرد، خسارات حاصله از حمله سایبری گاه می‌تواند از چنان وسعتی برخوردار باشد، که تحمیل آن بر متصدی از سویی ادامه فعالیت تجاری او را غیرممکن می‌سازد و از سوی دیگر به نحو کامل از زیان‌دیده جبران خسارت نگردد. در این حالت است که می‌توان دولت‌های مقر فعالیت خطرناک را واجد مسئولیت مکمل در این زمینه دانست.

در خصوص مسئولیت تکمیلی دولت مبدأ حمله سایبری در جبران خسارت، طرح کمیسیون ضمن شناسایی مسئولیت اولیه برای متصدیان فعالیت‌های خطرناک به منظور جبران کافی خسارت، مسئولیت دولت مقر فعالیت را در پله دوم نهاده است. در واقع چنانچه به هر دلیلی از شخص زیان‌دیده جبران خسارت نشود، مسئولیت نهایی و تکمیلی جبران خسارت به عهده دولت مبدأ خسارت یا دولت مقر می‌باشد. طرح ضمن شناسایی مسئولین اولیه برای متصدیان، دولت‌ها را ملزم ساخته که با اتخاذ تدابیر و اقدامات لازم جبران خسارت کافی و مناسب قربانیان را از طریق فعالیت‌هایی که در قلمرو یا تحت کنترلش صورت گرفته را تضمین دهد (مجوعه مقالات پیشگیری از آسیب‌های خطرناک، ۲۰۰۶، ۱۴). و اشاره داشته که در راستای اجرای این تدابیر باید مسئولیت را بر متصدیان یا بر حسب مورد شخص یا نهاد دیگر بار کند (همان، ۲۳). مسئولیت دولت‌ها در جبران ضرر و زیان‌های ناشی از فعالیت‌های منع نشده اساساً مسئولیت تضمینی است (داراب‌پور و زارع نعمتی، ۱۳۹۰، ۲۱۳).

۵-۴. دولت زیان‌دیده از حمله سایبری؛ رویه قضایی و کمیسیون حقوق بین‌الملل

برخی از اعمال متخلفانه بین‌المللی بر علیه کل جامعه جهانی انجام شده و در نتیجه برای دولت‌هایی که به صورت مستقیم صدمه ندیده‌اند نیز حق اقدام قانونی را فراهم می‌آورد. وابستگی‌های موجود و عدم مرزبندی در فضای سایبر می‌تواند موجب متأثر شدن چند دولت از یک حمله سایبری شود، لذا این امکان وجود دارد که دولت‌های دیگری غیر از دولتی که مستقیماً هدف حمله سایبری بوده است، بتوانند به عنوان زیان‌دیده به مسئولیت دولت متخلف استناد نمایند. دولت زیان‌دیده، دولتی است که حق معین او با ارتکاب فعل متخلفانه بین‌المللی انکار شده یا به آن خدشه وارد شده یا به گونه دیگر از آن متأثر شده است (ابراهیم گل، ۱۳۸۸، ۲۵۵). ضمن اینکه خسارات ناشی از حمله سایبری پیشرفته می‌تواند منافع کشورهای دیگری غیر از کشوری که حمله علیه او طراحی شده است، را تهدید و موجب ورود صدمه به آن‌ها نیز شود. در این صورت از اصل دفاع مشروع با استناد به رویه‌های حقوق بین‌الملل دنبال می‌شود (اسمیت، ۲۰۱۳، ۱۷۶). مهم‌ترین اصل توجیه‌گر در این زمینه همان اصل ۵۱ منشور سازمان ملل متحد است. بر مبنای این اصل، علاوه بر کشورهای هدف که مورد توجه حمله‌کنندگان سایبری هستند، سایر کشورهایی که به انحاء مختلف، از این حملات، دچار خسارت می‌شوند، می‌توانند از امکانات نظامی خود برای دفاع مشروع بهره ببرند.

از آن جایی که قابلیت‌های نوین فضای سایبر می‌تواند توانایی نقض تعهدات و قواعد بسیاری را به متصدیان مربوط و در رأس آن‌ها دولت‌ها اعطا نماید، طرح چنین مسئولیتی کاملاً یک بحث جدید و مهم تلقی می‌شود. لذا با تغییر و تحول در مفهوم حاکمیت شاهد آن هستیم که دامنه مسئولیت دولت نیز گسترش یافت، به گونه‌ای که در طرح ۲۰۰۱ کمیسیون حقوق بین‌الملل این مطلب مورد توجه جدی قرار گرفت.

در حقوق بین‌الملل می‌توان مواردی را مشاهده کرد که دایره طرف زیاندیده، گسترده‌تر از آن چیزی است که ابتدا تصور می‌شد در تفکرات آنزیلونی (راعی، ۱۳۸۷، ۶). رابطه حقوقی ایجادشده حاصل از نقض یک تعهد، تنها بین دو دولت، یعنی دولت مرتکب و دولت خسارت‌دیده شکل می‌گیرد. به اعتقاد او دولت‌ها حق و تکلیفی برای ممانعت از نقض حقوق بین‌الملل ندارند.

طرح مسئولیت در ماده ۴۸ با عبارت‌پردازی خود، نمود توسعه حقوق بین‌الملل را معین کرد. در این ماده مطرح شده است: هر دولتی غیر از دولت صدمه‌دیده حق دارد به مسئولیت دولت دیگر استناد کند، اگر تعهد نقض‌شده متعلق به گروهی از دولت‌ها باشد که این دولت نیز جزء آن‌ها به شمار می‌آید و آن تعهد نیز برای دفاع از منافع جمعی گروه تأسیس شده باشد و یا اینکه تعهد نقض‌شده متعلق به کل جامعه جهانی باشد. در بند دوم این ماده نیز به نوع ادعاهایی که این نوع دولت‌ها می‌توانند از دولت مرتکب داشته باشند، اشاره کرده است. خواسته‌هایی همانند توقف رفتار خلاف و

تضمین عدم تکرار، تعهد به پرداخت غرامت - مطابق آن چه در مواد قبل مطرح شده است- در راستای منافع دولت صدمه‌دیده و یا منتفعان از تعهد نقض‌شده، از مواردی می‌باشند که هر دولتی می‌تواند از دولت مرتکب بخواهد رعایت مواد ۴۳، ۴۴ و ۴۵ در ارتباط با هر دولتی نیز که قصد دارد به مسئولیت دولت مرتکب استناد کند، ضروری است (کراوفورد، ۲۰۰۲، ۳۳).

افزایش پیوندهای بین‌المللی واقعیات حاکم بر جامعه جهانی، به گونه‌ای شده است که نقض برخی از تعهدات تأثیرات فراگیر دارد. تقسیم‌بندی در نوع قواعد حقوقی یکی از دلایلی بود که تعیین طرف زیان‌دیده را اجتناب‌ناپذیر می‌کرد. اصولاً تعهدات بین‌المللی را می‌توان به دو دسته تقسیم کرد. برخی از این تعهدات مربوط به حفظ صلح می‌باشند و نقض آن‌ها منجر به نقض صلح و امنیت بین‌المللی است (منشور سازمان ملل متحد). این نوع قواعد از جایگاه مهمی برخوردار هستند؛ چرا که بنای جامعه بین‌المللی بر صلح و امنیت است و نقض این تعهدات به گونه‌ای است که می‌تواند به کل جامعه بین‌المللی لطمه وارد کند. پذیرش واکنش جمعی، حاکی از توجه جدی جامعه بین‌المللی به اهمیت این نوع تعهدات است (بووت، ۱۹۵۸، ۹۰). حقوق‌دانانی همچون تونکین (۱۹۶۲) معتقد بودند که اصولاً حقوق بین‌الملل پس از جنگ دوم، دسته از قواعد متمایز را پذیرفت (تانکین، ۱۹۷۴، ۶۰). پاراگراف دوم از بند اول ماده چهل و هشتم، طرح مسئولیت ناظر به این نوع تعهدات می‌باشد؛ یعنی تعهداتی که متعلق به کل جامعه جهانی است و نقض آن‌ها به کل جامعه جهانی لطمه می‌زند، در نتیجه کل جامعه بین‌المللی دولت‌ها، طرف زیان‌دیده به شمار خواهند آمد.

۵-۴-۱. مصادیق آرای قضایی درباره دولت صدمه‌دیده

در خصوص دولت زیان‌دیده در آرای قضایی بین‌المللی شاید مشهورترین رأی دیوان در این زمینه به سال ۱۹۶۰ برگردد. آرای سال‌های پیش از آن عملاً بر این نکته تکیه داشتند که طرف زیاندیده همان کسی است که مستقیماً صدمه‌دیده باشد و از گسترش مفهومی و مصداقی این موضوع عملاً خودداری می‌کردند. اما در سال ۱۹۶۰ دیوان در رأی خود کاملاً متفاوت عمل کرد. در سال ۱۹۶۰ دولت اتیوپی و لیبریا با استناد به ماده ۷ موافقتنامه سرپرستی، دادخواستی را علیه آفریقای جنوبی مطرح کردند و از دیوان خواستند که آفریقای جنوبی را به انجام تعهدات خود وادار کند و سیاست تبعیض نژادی را کنار بگذارد. آفریقای جنوبی به صلاحیت دیوان اعتراض و دیوان را فاقد صلاحیت برای رسیدگی به این دعوا دانست. آفریقای جنوبی معتقد بود مواردی که این دو کشور به عنوان مبنای صلاحیت مطرح می‌کنند ارتباطی با ماده ۷ ندارد.

دیوان در سال ۱۹۶۲ استدلال آفریقای جنوبی را رد کرد و اعلام کرد: مضمون مواد موافقتنامه سرپرستی به گونه‌ای است که کل جامعه جهانی را مخاطب قرار می‌دهد و آفریقای جنوبی با هدف

تأمین منافع جامعه جهانی، عهده‌دار این سمت شده است و طبیعتاً منفعت کل جامعه جهانی در این رابطه مطرح است و صلاحیت خود را احراز کرد. دیوان در امر صلاحیتی به یک نکته ماهوی نیز پرداخت. به عبارت دیگر، دیوان با ورود به ماهیت دعوا و مستند قرار دادن آن، به احراز صلاحیت خود پرداخت. این روش در آرای بعدی نیز دنبال شد البته دیوان در سال ۱۹۶۶ برخلاف اعلام نظر در سال ۱۹۶۲ تصمیم‌گیری کرد. شیوه این رأی، هفت برابر هفت بود که رأی رئیس دیوان، کار را به صورت دیگری تمام کرد.

دیوان در سال ۱۹۷۰ از این وضعیت غیرمعلوم و مبهم خود را بیرون آورد و در رأی بارسلونا تراکنش، نظر روشن‌تر خود را اعلام کرد. دیوان در سال ۱۹۹۵ در قضیه تیمور شرقی به تعیین مصادیق این نوع قواعد پرداخت و در واقع یک گام به جلوتر رفت. دیوان در این رأی اعلام کرد: حق تعیین سرنوشت، یک اصل بنیادین حقوقی و متعلق به کل جامعه جهانی است. دیوان در سال ۱۹۷۱ در رأی مشورتی خود درباره آثار حقوقی ادامه حضور آفریقای جنوبی در نامبیا اعلام کرد: ادامه سرپرستی آفریقای جنوبی، اشغال غیرقانونی این دولت است و منجر به مسئولیت بین‌المللی دولت آفریقا خواهد بود (گزارش دیوان بین‌المللی دادگستری، ۱۹۸۶). در خصوص حملات سایبری نیز به دلیل عدم وجود آرای خاص باید از همین رویه بین‌المللی که شرح آن گذشت استفاده نمود و در مواردی که می‌توان دولت ثالث را بر طبق قواعد بین‌المللی ذی‌نفع دانست، به وی اجازه طرح شکایت داده شود.

۵-۵. دولت صدمه‌ندیده از حمله سایبری

در خصوص وضعیت دولت صدمه‌ندیده در طرح کمیسیون ۲۰۰۱، بر اساس آن چه در پاراگراف اول ماده ۴۸ طرح مسئولیت آمده است، می‌توان گفت این طرح دایره دولت صدمه‌دیده را به شکل وسیع دیده است، به گونه‌ای که از دولت صدمه‌ندیده و حق آن دولت برای استناد به مسئولیت بین‌المللی دولت مرتکب سخن گفته است. در این خصوص ماده مذکور اعلام می‌کند:

الف. تعهدی که نقض آن منجر به مسئولیت می‌شود باید تعهدی باشد که مربوط و متعلق به گروهی است که این دولت نیز جزء آن گروه قرار می‌گیرد.

ب. تعهد در راستای حمایت و دفاع از منافع باشد. در این راستا، منشأ پیدایش تعهد، تفاوت‌ساز نمی‌باشد. این تعهد می‌تواند حالت دوجانبه و یا چندجانبه داشته باشد. چنانچه می‌تواند از نوع تعهدات عام‌الشمول باشد.

ج. تعهد مذکور باید یک تعهد جمعی باشد.

یادآوری این نکته ضروری است که ماده ۴۸ در صدد تعیین نوع منافع جمعی نیست، بلکه تنها به اصل موضوع نظر دارد. یکی از راه‌های کشف این موضوع، قصد دولت‌هاست؛ یعنی با در نظر گرفتن نیت آن‌ها، می‌توان فهمید که آیا معاهده مذکور با نیت دفاع از منافع جمعی به نگارش درآمده است و یا خیر. ابزار این کار می‌تواند دادرسی باشد.

با پذیرش این موضوع که در برخی از موارد رابطه مسئولیت می‌تواند به کل جامعه جهانی تسری پیدا کند، می‌توان این نتیجه را گرفت که حق اقدام متقابل برای همه دولت‌ها نیز می‌تواند وجود داشته باشد. طرح مسئولیت ۲۰۰۱، از مواد ۴۹ تا ۵۰ به حوزه اقدام متقابل می‌پردازد. با توسعه طـرف زیان‌دیده، دایره اعمال اقدام متقابل در حقـوق بین‌الملل نیز می‌تواند گسترش یابد و شرایط حاکم بر اقدام متقابل طرف زیان‌دیده، برای بقیه دولت‌ها نیز جاری است. برای مثال، اصل ممنوعیت توسل به زور (کراوفورد، ۲۰۰۲، ۵۲)، تعهد به خودداری از تهدید به زور مطابق آنچه در منشور آمده، تعهد برای حمایت از حقوق بنیادین بشری، تعهد به اجرای مقررات بشردوستانه که تلافی را ممنـوع می‌کنند، دیگر تعهدات دولت‌ها بر اساس فرم‌های اولیه حقوق بین‌الملل، اجرای تعهدی که از طرفین درخواست می‌کند اختلاف خود را مسالمت‌آمیز حل و فصل کنند، اصل احترام به نمایندگان کنسولی و دیپلماتیک و آرشیو و اسناد آن‌ها، همگی از محدودیت‌هایی است که نمی‌توان آن‌ها را در اقدام متقابل نادیده گرفت (همان، ۵۳). بدین ترتیب، رعایت اصل تناسب بر اساس ماده ۵۱ طرح، با لحاظ دو شرط گستردگی عمل خلاف و حق مورد بحث، ضروری است. این وضعیت از پذیرش نظام خاص مسئولیتی در حوزه چنین تعهداتی حاصل می‌شود.

۵-۶. حملات سایبری از منظر فقه

همانطور که گفته شد حملات سایبری یکی از تحولات نوین معاصر است و به دلیل نو بودن این تهدیدات، سازوکارهای حقوقی مرتبط با آن نیز از پیشینه چندانی برخوردار نیستند. زیرا حملات سایبری، پدیده ای مرتبط با قرن بیست و یکم است (قاسمی و نامدار، ۱۳۹۷، ۲۰۰). به همین دلیل، جست‌وجوی قوانین و مقررات مربوط به تحدید و یا مقابله با حملات سایبری، جدید و در عین حال متناسب با نوع و میزان تهدیدات سایبری است.

با عنایت به نو بودن حملات سایبری هم در عرصه عمل و هم در عرصه حقوق بین‌الملل، این موضوع در فقه امامیه نیز از منظر مختلف محل بحث است. اهمیت توجه به حملات سایبری در فقه به دلیل اهمیتی است که دین اسلام و آموزه‌های فقهی به برقراری امنیت و در نظر گرفتن این مسأله است که تخویف و ترساندن مردم از محرمات الهی است (حر عاملی، ۱۴۰۹، ۱۲، ۳۰۳). ایجاد ترس، دلهره، تهدید اموال و انفس و راه انداختن جنگ با هر ابزاری و وسیله‌ای، پذیرفته نیست و تأمین سازوکارهای لازم برای مقابله با این تهدیدات، دارای اهمیتی حیاتی است. این رویه شامل هر نوع وسیله و ابزار ترساندن مردم می‌شود که از مصادیق ناامنی روانی نیز محسوب می‌شود. زیرا اشتهار سلاح با هدف اخافه عمومی نهی شده است (نجفی، ۱۴۰۴، ۴۱، ۵۶۴). بدیهی است که فقه امامیه با در نظر گرفتن تحولات و شرایط کنونی، نسبت به حملات سایبری منفعل نبوده و راهکارهای خاصی خود را مطرح نموده است. از جمله اینکه حکومت

اسلامی موظف است تا با ایجاد سازوکارهای امنیتی، اعطای مجوز در قالب دفاع مشروع به آسیب‌دیدگان و همچنین ضرورت ایجاد امنیت حریم خصوصی و اطلاعات محرمانه کاربران، از بروز تهدیدات سایبری جلوگیری نموده و شرایط مناسبی را برای آحاد جامعه فراهم نماید (حسنی، ۱۳۹۹، ۴۰). به نظر می‌رسد بهره‌مندی از قواعد فقهی نظیر لاضرر، نفی سبیل، و برجسته کردن اصل امنیت در ابعاد مختلف آن، از جمله راهکارهایی است که می‌تواند تهدیدات سایبری را به عنوان تهدیدی جدی تلقی نموده و دست دولت اسلامی را برای دفع این تهدیدات باز بگذارد.

۶. نتیجه

بررسی حاضر نشان داد که اعطای مجوز، نظارت و کنترل بر آن و تبادل اطلاعات و اعلام خطرات احتمالی، زمینه‌ها و فرصت‌های ایراد خسارت ناشی از حملات سایبری نیازمند خنثی‌سازی و به حداقل‌رسانیدن خسارات ناشی از تهدیدات است. علاوه بر وظیفه دولت‌ها در پیشگیری از حمله سایبری، برای جبران خسارت نیز مسئولیت اصلی بر عهده متصدی فعالیت خطرناک بوده که به مسئولیت دولت مبدأ جلوه‌ای مکمل می‌دهد. با این حال، از آن جا که دولت‌ها در پذیرفتن مسئولیت اعمال منع شده طراحی شده از سرزمینشان اکراه دارند، این امر سبب می‌شود که تنها مسئولیت تکمیلی یا تضمینی را در قبال خسارت‌های وارده در اثر بی‌مبالاتی و اهمال متصدیان بپذیرند. در تبیین وضعیت دولت‌های زیان‌دیده از حملات سایبری نیز باید گفت که چنانچه این حملات در تناقض با تعهدات جمعی دولت‌ها یا به عبارت دیگر در تعارض با منافع جامعه جهانی باشد، سایر دولت‌ها غیر از دولت قربانی نیز محق به طرح دعوای مسئولیت دولت پشتیبان حمله می‌شوند. به طور کلی تعهد دولت‌ها می‌تواند از منابع مختلف حقوق بین‌الملل (معاهدات، عرف، اصول کلی) ناشی شود، مواردی هم می‌تواند وجود داشته باشد که در آن تعهدات دولت‌ها صرفاً از یک منبع نشأت بگیرد.

در حال حاضر، پیش‌نویس ۲۰۰۱ کمیسیون راجع به پیشگیری به آن درجه از توسعه نرسیده است که از منابع حقوق بین‌الملل تلقی شده و بر دولت‌ها الزام‌آور باشد. این پیش‌نویس آخرین وضعیت حقوق بین‌الملل عام در زمینه چگونگی پیشگیری زیان‌های ناشی از فعالیت‌های ممنوع شده، از جمله فعالیت‌های سایبری، محسوب می‌شود و تا زمانی که به یک سند الزام‌آور جهانی تبدیل نشده یا مقررات آن ماهیت عرفی جهانی پیدا نکرده است، نمی‌توان مدعی قواعد و مقررات بین‌المللی عام و الزام‌آور در زمینه چگونگی پیشگیری زیان‌های ناشی از فعالیت‌های ممنوع نشده، از جمله حملات سایبری شد. علیرغم خلاءهای موجود در حقوق بین‌الملل برای مقابله مؤثر با خطرات روزافزون ناشی از حملات سایبری می‌توان با استمداد از قواعد انسجام‌یافته حقوقی پیرامون مسئولیت دولت‌ها مبنای مستحکمی را در این خصوص یافت. لازمه این امر آن است که از نظر حقوقی، حملات سایبری و حملات مسلحانه را از نظر همپوشانی به

یکدیگر نزدیک نمود. در این زمینه می‌توان گفت از نظر حقوق بین‌الملل و حتی حقوق اسلامی که منبعث از فقه است، نیازمند اتخاذ تدابیری هستیم تا طیف بیشتری از فعالیت‌ها و حملات سایبری در قالب حقوق جنگ شناخته شده و قوانین حملات مسلحانه نیز بر آنان حاکم شود. در این صورت است که از نظر حقوقی، شرایط مطلوب‌تری برای دفاع مشروع در برابر تهدیدات و حملات سایبری فراهم می‌شود.

۷. سهم نویسندگان

نویسندگان مقاله حاضر به ترتیب حمیدرضا آقابابایان، مریم مرادی (نویسنده مسؤول) و سید باقر میرعباسی هستند که به صورت مشترک، مقاله را به رشته تحریر درآورده‌اند.

۸. تضاد منافع

در مقاله حاضر تضاد منافعی وجود ندارد.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

منابع

- ابراهیم گل، علیرضا، مسئولیت بین‌المللی دولت: متن و شرح مواد کمیسیون حقوق بین‌الملل، تهران، شهر دانش، ۱۳۸۸.

- حر عاملی، محمد بن حسن، وسائل الشیعه، جلد دوازدهم، قم، آل‌البیت، ۱۴۰۹.

- حسنی، سعید، «بررسی وجوب ایجاد امنیت در فضای سایبر؛ با رویکرد فقه حکومتی»، فصلنامه حکومت اسلامی، دوره بیست و پنجم، شماره یک، ۱۳۹۹.

- داراب‌پور، مهراب، زارع نعمتی، رویا، «تعهدات دولت‌ها در پیشگیری و جبران خسارت ناشی از حوادث اتمی»، مجله حقوقی بین‌المللی، دوره بیست و هشتم، شماره چهل و چهار، ۱۳۹۰.

- راعی، مسعود، «دولت لطمه‌دیده در حقوق بین‌الملل و مسئولیت ناشی از آن»، نشریه معرفت، صد و سی و چهار، ۱۳۸۷.

- رضایی، صالح، «مسئولیت بین‌المللی دولت‌ها در پیشگیری از زیان‌های ناشی از فعالیت‌های هسته‌ای صلح‌آمیز»، فصلنامه حقوق، دوره چهلم، شماره یک، ۱۳۸۹.

- عبداللهی، محسن، «رویکرد نظام مسئولیت بین‌المللی در جبران خسارت ناشی از اعمال منع نشده در حقوق بین‌الملل»، مجله تحقیقات حقوقی، شماره پنجاه و شش، ۱۳۹۰.

- فضلی، مهدی، مسؤولیت کیفری در فضای سایبر، تهران، نشر خرسندی، ۱۳۸۹.

- قاسمی، غلامعلی، نامدار، سعید، «بررسی مفهوم دفاع مشروع در پرتو حملات سایبری با تأکید بر حمله استاکس‌نت به تأسیسات هسته‌ای ایران»، فصلنامه مطالعات حقوقی دانشگاه شیراز، دوره دهم، شماره یک، ۱۳۹۷.

- نجفی، محمدحسن، جواهرالکلام فی شرایع الاسلام، بیروت، دارالاحیاه التراث العربیه، ۱۴۰۴.

منابع لاتین

- Boweet, P.W. Self Defence in International Law, 1958.

- Brenner, S.W. “At Light speed: Attribution and Response to Cyber Crime/ Terrorism/ warfare”, Journal of Criminal Law and Criminology, No. 97, 2006.

- Crawford, J. The International Law Commission's articles on state responsibility: introduction, text, and commentaries, Cambridge University Press, 2002.

- Dormann, K. Applicability of the Additional Protocols to Computer Network Attacks, International Committee of the Red Cross, Available at: https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf, Visited on 23 September 2004.

- Hathaway, A. Oona, R. The Law of Cyber-Attack California law rview. Vol. 100, 2012.

- Schmitt, M. “Reaction, Cyberspace and International Law: The Penumbral Mist of Uncertainty", Harvard Law Review Forum, Vol. 126, No. 176, 2013.

- Tabasco, L. “Basic Concepts in Cyber Warfare”, Military and Strategic Affairs, Vol. 3, No. 1, 2011.

2004 on Environment liability with regard to Prevention and Remedying of Environment Damage, Official Journal of European union, Art. 1, para. 6.

- Draft article on the Allocation of Loss in the case of Transboundary Harm arising out of Hazardous Activities, 2006, principle. 4(1).

- ICJ, Report. 1986.

- Text of the Draft Articles On Responsibility of States, 2001, Article. 48.

- Theohary, C.A., Rollins, J. Cyber Security: Current Legislation, 2009.

- Tunkin, G.I. Theory of International Law, Edited and translated by William E. Butler, 1974.

Documents:

- Commentaries to Draft Articles on Prevention of Harm from Hazardous Activities, Adopted by ILC, 2001, P. 391.

- Directive 2004/35/CE of the European Parliament and of the Council of 21 April

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی