Defense Policy

131

Vol. 34
Summer 2025
P.P: 11-31

Research Paper

Received:
2024-09-02
Revised:
2024-10-15
Accepted:
2025-10-20
Published:
2025-10-20

ISSN: 1025-5087
E-ISSN: 2654-4971

Preemptive Self-Defense in Cyber Attacks in International Law

Seyed Abolghaseem Naghibi[1*] | Masoud Nakhaei Moghadam [2] | Seyed Mohammadsadegh Mousavi[3]

Abstract

With the expansion of cyberattacks and the increase in associated threats, the concept of preemptive defense in international law has entered a new phase. This research aims to examine the legal foundations for the use of the doctrine of preemptive defense in response to cyberattacks and to align it with traditional principles of international law. The methodology of this study is descriptive-analytical, utilizing reputable international legal sources, including the United Nations Charter and international judicial decisions, for analysis.

In this research, the doctrine of preemptive defense is examined as a theoretical basis in international law, and an effort is made to analyze its applicability to cyberattacks. Additionally, the challenge of identifying the sources of cyberattacks and the indirect nature of the damages resulting from these attacks are recognized as key legal challenges in this area.

The findings of this study indicate that, although there are general principles in international law that permit the doctrine of preemptive defense under specific conditions, significant legal and interpretative gaps still exist in the context of cyberattacks. Notably, due to the technical complexities and non-physical nature of cyberattacks, more precise regulations are needed. Therefore, the development of more accurate and updated legal frameworks at the international level to address cyber threats is deemed essential so that states can respond to these threats based on clear and internationally compliant principles.

Keywords: Cyberattacks, Preemptive Defense, International Law, United Nations Charter.

1. Corresponding author: Professor of the Department of jurisprudence and private law of the Faculty of Humanities, Shahid muthari University, Tehran, Iran. Email: da.naghibi@motahari.ac.ir
2. Doctoral student in the field of jurisprudence and the foundations of Law, Faculty of Humanities of Shahid muthari University, Tehran, Iran.
3. Associate Professor of Private Jurisprudence and Law, Higher School and Shahid Motahari of TehranUniversity , Tehran, Iran.

۱۳۱

سال سی وچهارم
تابستان ۱٤۰٤
صص: ۳۱-۱۱

مقاله پژوهشی

تاریخ دریافت: ۱٤۰۳/۰٦/۱۲
تاریخ بازنگری: ۱٤۰۳/۰۷/۲٤
تاریخ پذیرش: ۱٤۰٤/۰۷/۲۸
تاریخ انتشار: ۱٤۰٤/۰۷/۲۸

شاپا چاپی: ۵۰۸۷-۱۰۲۵
الکترونیکی: ٤۹۷۱-۲۶۵٤

حق دفاع پیش دستانه در حملات سایبری در حقوق بین الملل

سید ابوالقاسم نقیبی*[۱] | مسعود نخعی مقدم[۲] | سیدمحمدصادق موسوی[۳]

چکیده

با گسترش حملات سایبری و افزایش تهدیدات ناشی از آنها، مفهوم دفاع پیش‌دستانه در حقوق بین‌الملل وارد مرحله جدیدی شده است. این پژوهش با هدف بررسی مبانی حقوقی استفاده از دکترین دفاع پیش‌دستانه در واکنش به حملات سایبری و تطبیق آن با اصول سنتی حقوق بین‌الملل انجام شده است. روش این تحقیق توصیفی-تحلیلی بوده و از منابع معتبر حقوقی بین‌المللی، از جمله منشور سازمان ملل و آراء قضایی بین‌المللی، برای تحلیل استفاده شده است.

در این پژوهش دکترین دفاع پیش‌دستانه، به‌عنوان یک مبنای نظری در حقوق بین‌الملل، مورد بررسی قرار می‌گیرد و تلاش می‌شود تا قابلیت انطباق این دکترین بر حملات سایبری تحلیل شود. همچنین، مسئله شناسایی منبع حملات سایبری و ماهیت غیرمستقیم آسیب‌های ناشی از این حملات به‌عنوان چالش‌های حقوقی اصلی در این حوزه شناخته شده است.

نتایج این مطالعه نشان می‌دهد که اگرچه اصول کلی در حقوق بین‌الملل وجود دارد که در شرایط خاص دکترین دفاع پیش‌دستانه را مجاز می‌شمارد، اما در حوزه حملات سایبری هنوز خلأهای حقوقی و تفسیری زیادی وجود دارد. به‌ویژه اینکه حملات سایبری به دلیل پیچیدگی‌های فنی و ماهیت غیر فیزیکی آنها، به قواعد دقیق‌تری نیاز دارند. بر این اساس، توسعه چارچوب‌های حقوقی دقیق‌تر و به‌روزتر در سطح بین‌المللی برای مواجهه با تهدیدات سایبری ضروری به نظر می‌رسد تا دولت‌ها بتوانند با اتکا به اصول روشن و منطبق با حقوق بین‌الملل، به این تهدیدات پاسخ دهند.

کلیدواژه‌ها: حملات سایبری، دفاع پیش‌دستانه، حقوق بین‌الملل، منشور سازمان ملل.

۱. نویسنده مسئول: استاد گروه فقه و حقوق خصوصی دانشکده علوم انسانی، دانشگاه شهید مطهری، تهران، ایران.
Email: da.naghibi@motahari.ac.ir
۲. دانشجوی دکتری تخصصی رشته فقه و مبانی حقوق، دانشکده علوم انسانی دانشگاه شهید مطهری، تهران، ایران.
۳. فقه و حقوق خصوصی، مدرسه عالی و دانشگاه شهید مطهری تهران، تهران، ایران.

ناشر: دانشگاه جامع امام حسین (ع)

مقدمه

در نظام حقوقی بین‌المللی، برای حملات سایبری که باعث نقض قاعده منع توسل زور گردیده و یا تهدیدی علیه صلح و امنیت کشورها به‌حساب می‌آیند، نخستین استثنای وارد بر منع توسل به زور، یعنی حق دفاع مشروع مقرر در ماده ۵۱ منشور موضوعیت پیدا می‌کند. ماده مذکور مقرر می‌دارد:

درصورت وقوع حمله مسلحانه علیه یک عضو ملل متحد تا زمانی که شورای امنیت اقدامات لازم برای حفظ صلح و امنیت بین‌المللی را به‌عمل آورد، هیچ‌یک از مقررات این منشور به حق ذاتی دفاع مشروع، خواه به‌طور فردی و خواه دسته‌جمعی لطمه‌ای وارد نخواهد کرد.

منشور سازمان ملل متحد، یکی از موارد استفاده مجاز از زور را در ماده ۵۱ خود به شرح زیر بیان می‌نماید:

درصورت وقوع تهاجم مسلحانه علیه یک عضو ملل متحد، تا زمانی‌که شورای امنیت اقدامات لازم را برای حفظ صلح و امنیت بین‌المللی به‌عمل آورد هیچ‌یک از مقررات این منشور به حق ذاتی دفاع از خود، خواه فردی یا دسته‌جمعی لطمه‌ای وارد نخواهد کرد. اعضاء باید اقداماتی را که در اعمال این حق به‌عمل می‌آورند فورا به شورای امنیت گزارش دهند. این اقدامات به‌هیچ‌وجه در اختیار و مسئولیتی که شورای امنیت برطبق این منشور دارد و به‌موجب آن برای حفظ و اعاده صلح و امنیت بین‌المللی و در هر موقع که ضروری تشخیص دهد اقدام لازم به‌عمل خواهد آورد تاثیری نخواهد داشت.

یکی از موضوعات کلیدی در این زمینه، مسئله **حق دفاع پیش‌دستانه** در برابر حملات سایبری است. این مسئله به‌ویژه از آنجا اهمیت می‌یابد که حملات سایبری ممکن است بدون خسارات فیزیکی مستقیم، تأثیرات ویرانگر بر امنیت ملی و بین‌المللی داشته باشند.(Gegout & Granholm, 2021)

منشور سازمان ملل متحد به‌طور سنتی دفاع مشروع را در برابر حملات مسلحانه تعریف می‌کند، اما تفسیر مفهوم "حمله مسلحانه" در عصر دیجیتال محل مناقشه است. برخی از محققان معتقدند که اصول موجود در حقوق بین‌الملل همچنان باید بر حوزه سایبری نیز اعمال شوند، به شرط آنکه حمله سایبری به سطح یک حمله مسلحانه سنتی برسد. به عبارت دیگر، اگر یک حمله سایبری به‌طور مؤثری به همان میزان خسارات فیزیکی یا اقتصادی که حملات نظامی سنتی ایجاد می‌کنند، منجر شود، می‌توان دفاع پیش‌دستانه را موجه دانست .(Kastenberg, 2022) این دیدگاه بر

اصول **ضرورت** و **تناسب** در حقوق بین‌الملل تأکید دارد که به دولت‌ها اجازه می‌دهد تنها زمانی که یک تهدید فوری و جدی وجود دارد و هیچ جایگزین مناسبی برای جلوگیری از آن نیست، از زور استفاده کنند.

از سوی دیگر، برخی از پژوهشگران بر این باورند که ماهیت غیرشفاف و فرامرزی حملات سایبری باعث ایجاد مشکلات عملی در استفاده از دفاع پیش‌دستانه می‌شود. به‌طور مشخص، مسئله **شناسایی دقیق عاملان** حملات سایبری یکی از چالش‌های اصلی است که دولت‌ها با آن مواجه هستند. در بسیاری از موارد، مشخص کردن اینکه یک دولت خاص پشت یک حمله سایبری قرار دارد یا اینکه حمله توسط گروه‌های غیردولتی یا هکرهای مستقل انجام شده، ممکن است به زمان و تحقیقات پیچیده نیاز داشته باشد .(Roscini, 2020) این امر موجب می‌شود که استفاده از دفاع پیش‌دستانه در زمان مناسب و با توجیهات حقوقی معتبر، دشوارتر شود.

همچنین برخی محققان پیشنهاد می‌کنند که جامعه بین‌المللی باید چارچوب‌های حقوقی جدیدی را برای حملات سایبری توسعه دهد تا به این پدیده پیچیده به‌طور جامع‌تری پاسخ داده شود. تدوین **قواعد بین‌المللی ویژه** برای مدیریت حملات سایبری و تعیین حدود استفاده از زور در این حوزه می‌تواند به کاهش ابهامات حقوقی و جلوگیری از سوءاستفاده‌های احتمالی کمک کند .(Nasu & Fahey, 2021) این قواعد باید به دولت‌ها اجازه دهد تا به‌طور مسئولانه و بر اساس شواهد معتبر به تهدیدات سایبری پاسخ دهند، در حالی که از تشدید تنش‌ها و درگیری‌های بین‌المللی جلوگیری شود.

زیرساخت های غیرنظامی حیاتی که امکان ارائه خدمات ضروری را فراهم می کند، به طور فزاینده ای بر سیستم های دیجیتالی شده متکی است. حفاظت از چنین زیرساخت‌ها و خدماتی در برابر حملات سایبری یا آسیب‌های اتفاقی برای محافظت از مردم غیرنظامی ضروری است.

حقوق بشردوستانه بین المللی بدون در نظر گرفتن نوع عملیات مضر، حفاظت خاصی از زیرساخت‌های خاص، مانند خدمات پزشکی و اشیاء ضروری برای بقای جمعیت فراهم می‌کند.[1] با این حال، اکثر قوانین ناشی از اصول تمایز، تناسب و اقدامات احتیاطی، که حفاظت عمومی را برای غیرنظامیان و اشیاء غیرنظامی ارائه می‌کند، فقط برای عملیات‌های نظامی اعمال می‌شود که به

1 See text in relation to footnotes 16 and 15 above. With regard to the latter, they must not be attacked, destroyed, removed or rendered useless.

عنوان «حمله» مطابق با تعریف حقوق بشردوستانه بین المللی اعمال می‌شوند.[1] ماده ۴۹ پروتکل الحاقی یک، حملات را به عنوان «اعمال خشونت علیه دشمن، چه در حمله و چه در دفاع» تعریف می‌کند. بنابراین، این سؤال که مفهوم «حمله» با توجه به عملیات سایبری چقدر گسترده یا محدود تفسیر می‌شود، برای کاربرد این قوانین و حفاظتی که از غیرنظامیان و زیرساخت‌های غیرنظامی انجام می‌دهند ضروری است.

بنابراین، نیاز به تدوین و توسعه ابزارهای حقوقی جدید برای مقابله با چالش‌های حقوقی حملات سایبری در حقوق بین‌الملل بیش از پیش احساس می‌شود. در حالی که حقوق بین‌الملل کنونی چارچوبی کلی برای استفاده از زور در مواجهه با حملات فراهم کرده است، به‌وضوح کاستی‌هایی در تفسیر و تطبیق این اصول با واقعیت‌های مدرن دیجیتال وجود دارد که نیازمند اصلاح و تقویت است.

تبیین دکترین دفاع پیش دستانه

در یک نگاه کلی دفاع پیش دستانه[2] به برخورد اولیه ای[3] اطلاق می شود که به منظور متوقف سازی حملاتی که قریب الوقوع[4] فرض می شوند، طرح ریزی شده است. (هندرسون، ۲۰۱۰: ۲۲۴.) نهاد دفاع پیش دستانه با این ادعا که ماده ۵۱ منشور مانع قواعد عرفی موجود پیش از منشور نیست، مطرح شده است و توسط تعدادی از حقوقدانان برجسته امریکایی و بریتانیایی توسعه یافته و توسط اسرائیل در سال ۱۹۸۱ در شورای امنیت سازمان ملل متحد مطرح گردیده است (آنتونیو کاسسی، ۲۰۰۱: ۳۵۸.). این تئوری معتقد است که اگر تهدید مسلحانه واقعی، قریب الوقوع[5] و درهم شکننده و همه جانبه[6] باشد، آنگاه توسل به دفاع پیش دستانه مجاز است. به عنوان مثال: تمرکز انبوه و مستمر سربازان خارجی در طول مرز کشور همسایه می تواند زمینه دفاع پیش دستانه

1 The notion of attack under IHL, defined in Art. 49 of the 1977 First Additional Protocol, is different from and should not be confused with the notion of 'armed attack' under Art. 51 of the UN Charter, which belongs to the realm of jus ad bellum. To affirm that a specific cyber operation, or a type of cyber operations, amounts to an attack under IHL does not necessarily mean that it would qualify as an armed attack under the UN Charter.
2 Anticipatory Self-defence
3 First strike
4 Imminent
5 Imminent
6 Overwhelming

را به وجود آورده و قبل از اقدام قطعی و حمله عملی آن ها دست به کار شود. پس می توان بر این اساس شرایط موجه کننده دفاع پیش دستانه را این گونه برشمارد:

۱- دولت باید هدف فعالیت های خصمانه دولت دیگر باشد؛

۲- دولت تهدید شده هیچ راهکار دیگری برای حفاظت از خود نداشته باشد؛

۳- خطر قریب الوقوع باشد؛

۴- اقدامات دفاعی متناسب با حملات احتمالی باشد. (والاس، ۲۰۰۵: ۲۸۴.)

در اسناد مختلف حقوق بین الملل و هم چنین تألیفات حقوقدانان بزرگ از سه نهاد دفاع پیش دستانه[1]، دفاع پیش گیرانه[2] و دفاع قطع کننده[3] با معانی متفاوتی استفاده شده است و برخی هر سه را برابر یکدیگر دانسته اند، فلذا آن ها را به جای یکدیگر به کار برده اند و به نوعی موجبات خلط مبحث را ایجاد کرده اند. عده ای دیگر هم هر یک تعبیر خاص خود را برای این مفاهیم داشته اند. اما مشکل اصلی در خصوص دفاع پیش دستانه و دفاع قطع کننده می باشد. برای حل این مسئله، پروفسور مالکوم شاو۴ از اساتید برجسته حقوق بین الملل عمومی، دو پیشنهاد ارائه می کند. که در ذیل به هر یک جداگانه و با قدری فاصله می پردازیم:

پیشنهاد اول این است که مفهوم دفاع پیش دستانه را مربوط به جایی دانسته که یک حمله مسلحانه قابل پیش بینی است و در مقابل مفهوم دفاع قطع کننده را نیز مرتبط با مواقعی فرض نموده که یک حمله مسلحانه قریب الوقوع و غیرقابل اجتناب باشد. (شاو، ۲۰۱۷: ۱۱۳۹) این راه حل بر این استدلال استوار است که هر دو مفهوم دفاع پیش دستانه و دفاع قطع کننده وجوه متفاوتی از یک مفهوم (یعنی حق دفاع پیش دستانه) هستند و در مقابل آن ها تئوری دفاع پیش گیرانه قرار دارد که کاملاً مردود و غیرقانونی است.

تفکیک میان دفاع مشروع پیش دستانه و دفاع پیشگیرانه را می توان در گزارش ۲۱ مارس ۲۰۰۵ دبیر کل سازمان ملل متحد ملاحظه نمود (موسوی، ۱۳۹۱: ۱۰۵). در بند ۱۲۴ این گزارش آمده است که: «ماده ۵۱ که از حق ذاتی کشورهای مستقل برای دفاع از خود در برابر حمله

1 Anticipatory Self-defence
2 Pre-emptive Self-defence
3 Interceptive
4 Malcolm N. Shaw

مسلحانه محافظت می کند، به تهدیدهای قریب الوقوع به طور کامل پوشش می دهد. حقوق دانان از مدت ها پیش پذیرفته اند که این ماده حمله قریب الوقوع و هم چنین حمله ای را که صورت پذیرفته، پوشش می دهد.» (موسوی، ۱۳۹۱: ۱۰۶) دبیر کل در بند ۱۲۵ گزارش خود تهدید بالقوه (مورد استناد در دفاع پیش گیرانه) را از تهدید قریب الوقوع (مورد استناد در دفاع پیش دستانه) تفکیک می نماید. همین معیار برای تمایز دفاع پیش دستانه از پیش گیرانه کافی است. اساسا دبیر کل تهدید بالقوه را مسبب مداخله شورا می داند. البته به نظر می رسد که ذکر این بند از گزارش ضرورتی نداشت، چون ماده ۳۹ منشور سازمان ملل متحد[1] مؤید این وظیفه ی شورا است (موسوی، ۱۳۹۱: ۱۰۷). براساس ماده ۳۹ منشور ملل متحد این شورای امنیت است که وقوع تهدید بر ضد صلح، نقض صلح و تجاوز را بر عهده دارد (بیگ زاده، ۱۳۸۵: ۲۲۲). بر این اساس، شروع یک حمله نظامی به استناد اینکه دولت مقابل یک تهدید بالقوه برای صلح و امنیت کشور مهاجم (یا سایر کشورهای دیگر است) داخل در تئوری دفاع پیش گیرانه بوده و غیرمشروع است. دبیر کل همچنین در ادامه بند ۱۲۵ بیان می کند که «هر جا که تهدیدها، نه قریب الوقوع بلکه بالقوه است، منشور به شورای امنیت اختیار کامل می دهد تا از نیروهای نظامی، از جمله به صورت پیش گیری برای حفظ صلح و امنیت بین المللی استفاده کنند. اما آیا نسل کشی[2]، پاک سازی قومی[3] و سایر این گونه جنایات علیه بشریت، نیز تهدیدی برای صلح و امنیت بین الملل محسوب نمی شوند که بشریت در برابر آن ها نتوانند که برای انجام تدابیر امنیتی، به شورای امنیت چشم بدوزند؟» (موسوی، ۱۳۹۱: ۱۰۶)

اما در پایان اگر تئوری دفاع پیش دستانه و شرایط آن به درستی شناخته شود، ایجاد تمایز آن با سایر مفاهیم آسان به نظر می رسد. در این خصوص پروفسور آنتونیو کاسسه (حقوقدان برجسته حقوق بین الملل عمومی) به دقت شرایط دفاع پیش دستانه را بیان نموده است. منشور سازمان ملل «تهدید یا استفاده از زور» توسط یک کشور علیه کشور دیگر را در ماده ۲ (۴) ممنوع کرده است.[4]

---

۱ منشور سازمان ملل متحد، ماده ۳۹.

2 Genocide
3 Ethnic cleaning

۴ ماده ۲ منشور ملل متحد ، پاراگراف ۴:

این ممنوعیت، حقوق بین‌الملل عرفی تلقی می‌شود و برای همه ملت‌ها اعم از امضاکننده یا غیر قابل اجرا است. یورام دینشتاین، تهاجم جنگ و دفاع شخصی ۹۵ (ویرایش پنجم ۲۰۱۱).

با این حال، ماده ۵۱ به صراحت «حق ذاتی دفاع مشروع فردی یا جمعی را در صورت وقوع حمله مسلحانه علیه یکی از اعضای سازمان ملل» به رسمیت می شناسد.[۱] در ظاهر، این زبان به نظر می‌رسد که ایجاب می‌کند که یک دولت قبل از توسل به دفاع از خود، ابتدا باید مورد حمله قرار گیرد. (رایسمن و آرمسترانگ، ۲۰۰۶: ۵۲۵-۵۵۰.)

علیرغم عبارت ماده ۵۱، بسیاری از دولت ها این زبان را به عنوان یک هنجار حقوق بین الملل عرفی به عنوان سهل گیرانه تر و شامل اقدامات پیش بینی کننده تفسیر می کنند. (بارکر و گرانت، ۲۰۱۳: ۳۴-۳۵.) بر اساس این دیدگاه، یک دولت "نیازی ندارد قبل از اینکه بتواند برای دفع حمله قریب الوقوع به استفاده از زور در دفاع از خود متوسل شود، اولین ضربه را جذب کند.". (اشمیت، ۲۰۰۲: ۵۱۳، ۵۳۵) در واقع، حتی کسانی که از تفسیر دقیق ماده ۵۱ حمایت می‌کنند، می‌پذیرند که تاریخ مملو از مواردی است که دولت‌ها برای دفاع از خود به اقدامات پیش‌بینی‌کننده متوسل شده‌اند. (دینشتاین، ۲۰۱۷: ۱۹۵) از این میان، حادثه کارولین بیشتر مورد اشاره است. (سادوف، ۲۰۰۸: ۳۷-۳۸)

در سال ۱۸۳۷ نیروهای بریتانیایی که خارج از کانادا فعالیت می کردند به نیویورک رفتند و کارولین (کشتی بخاری که توسط شورشیان کانادا و حامیان آمریکایی آنها استفاده می شد) را تصرف کردند، آن را به آتش کشیدند و آن را در حال سقوط به سوی آبشار نیاگارا فرستادند.[۲] در سال ۱۸۴۲، دانیل وبستر، وزیر امور خارجه ایالات متحده، به ادعای بریتانیایی ها مبنی بر اینکه این اقدام دفاع شخصی مناسب بود، پاسخ داد. (اشمیت، ۲۰۰۲: ۵۲۹-۳۰) وبستر اظهار داشت: «در حالی که پذیرفته شده است که استثنائات ناشی از قانون بزرگ دفاع از خود وجود دارد، این استثناها باید به مواردی محدود شود که در آن «ضرورت آن دفاع شخصی فوری، طاقت‌فرسا است و هیچ انتخابی باقی نمی‌گذارد». وسیله، و هیچ لحظه ای برای مشورت نیست.»[۳]

اما مسئله دیگر این است که در مورد حملات فیزیکی وحشت حمله قریب الوقوع ملموس تر می باشد. به این بیان که هر گاه دولتی اقدام به تبلیغات گسترده دعوت به جنگ نماید یا اینکه اظهارات جنگ طلبانه نموده و یا اینکه نیروهای خود را تا مرز کشور دیگر حرکت داده و آن ها را

---

۴. ماده ۵۱ منشور ملل متحد

2 Hunter William, Yale Law School's Avalon Project: Documents in Law, History and Diplomacy, BritishAmerican Diplomacy, The Caroline Case, at http://avalon.law.yale.edu/19th _centrury/br-1842d.asp [hereinafter Avalon Project, Caroline Case].

۳ نامه دانیل وبستر به لرد اشبرتون، (۶ اوت ۱۸۴۲)، پروژه آوالون، کارولین مورد ۱۷.

بسیج کرده و هم چنین میزان نیروهای خود را در زمینه های گوناگون افزایش دهد و یا به وسیله جاسوسان خود به طور سری نهادهای نظامی دولت دیگر را رصد نماید. همگی نشانه های یک حمله قریب الوقوع هستند که شاید بسته به شرایط، یکی از آن ها و یا مجموع آن ها جامعه جهانی را متقاعد نماید که حمله ای مسلحانه در شرف وقوع است. (رابرتسون، ۲۰۰۲: ۱۳۸)

اما در خصوص حملات سایبری کار قدری متفاوت تر است. چرا که گاهی ادقات خود حملات سایبری موضوع نبوده و بلکه وقوع آن ها پیش زمینه ای برای تدارک یک حمله فیزیکی گسترده می باشد. در شرایطی دیگر کاملاً برعکس امکان دارد که کشف یک ویروس در یک سخت افزار نشان آن باشد که دولت ارسال کننده ویروس قصد دارد که در آینده نزدیک با فعال کردن آن ویروس موجب خسارت جدی به زیرساخت های حیاتی دولت قربانی یا ایجاد تلفات گسترده باشد. منتهی آنچه مورد اهمیت است، رعایت تناسب میان حمله آتی و دفاع پیش دستانه می باشد. (رابرتسون، ۲۰۰۲: ۱۳۸)

با تمام بحث هایی که در مورد دفاع پیش دستانه وجود دارد. باید این را پذیرفت که در صورت وجود چنین حقی، تقریباً همه وفاق دارند که معیارها و شرایط کارولین باید در دفاع پیش دستانه رعایت شود.(دافی، ۲۰۱۸: ۱۵۷) در واقع رعایت مفاهیم کلیدی ضرورت و تناسب الزامی است و به نوعی مشروعیت توسل به دفاع پیش دستانه به رعایت آن ها بستگی دارد. (گرانت، کرانت و بارکر، ۲۰۰۹: ۵۴۹)

در ۱۰ اوت ۱۹۹۸ در پی بمب گذاری های سفارت امریکا در کنیا و تانزانیا در ۷ اوت ۱۹۹۸. (موسوی، ۱۳۹۱: ۱۹۷)

در قضایای نامبرده، اعتراض مداوم کشورها مانع شکل گیری چنین عرفی شده است. (موسوی، ۱۳۹۱: ۱۹۷)

در واقع برای شکل گیری عرف آنی، تکرار عنصر مادی شرط نیست و صرف الزام حقوقی و به وقوع پیوستن حتی یک دفعه ای عمل کافی است. طرفداران این نظریه پیش تر توجه خود را به پاسخ امریکا و متحدانشان به حملات ۱۱ سپتامبر معطوف نمودند و وجود یک عنصر قوی حقوقی در این پاسخ ها را علت شکل گیری عرف آنی می دانند. (موسوی، ۱۳۹۱: ۱۱۲)

در تحلیل حقوقی دکترین دفاع پیش‌دستانه در برابر حملات سایبری، نخست باید به مفهوم **ضرورت** توجه کرد. در حقوق بین‌الملل سنتی، دولت‌ها تنها زمانی می‌توانند به استفاده از زور متوسل شوند که حمله‌ای قریب‌الوقوع و اجتناب‌ناپذیر در شرف وقوع باشد و هیچ راه حل جایگزین دیگری برای جلوگیری از آن موجود نباشد. در مورد حملات سایبری، شناسایی تهدیدات قریب‌الوقوع بسیار پیچیده‌تر از تهدیدات سنتی نظامی است، زیرا حملات سایبری معمولاً در فضای مجازی رخ می‌دهند و آثار فیزیکی مستقیم ندارند. این امر باعث شده که تعریف و احراز ضرورت در چنین مواردی نیاز به بازنگری داشته باشد .(Nasu, 2021) به عنوان مثال، ممکن است یک حمله سایبری مدت‌ها پیش از آشکار شدن اثرات آن رخ داده باشد، و همین تأخیر در شناسایی حمله، چالش بزرگی برای دولت‌ها در واکنش به آن ایجاد می‌کند.

از سوی دیگر، مفهوم **تناسب** نیز به‌عنوان یکی از شروط اساسی دفاع پیش‌دستانه باید بررسی شود. در حقوق بین‌الملل سنتی، هرگونه استفاده از زور باید متناسب با تهدیدی باشد که با آن مواجه است. این اصل در مورد حملات سایبری نیز به شکل پیچیده‌تری مطرح می‌شود، چرا که میزان و دامنه خسارات ناشی از یک حمله سایبری معمولاً به‌طور مستقیم قابل ارزیابی نیست و آثار آن ممکن است تدریجی و نامحسوس باشد .(Roscini, 2020) برای مثال، حمله‌ای که به یک سیستم بانکی سایبری انجام می‌شود، ممکن است تأثیر فوری و گسترده‌ای نداشته باشد، اما در طول زمان خسارات اقتصادی شدیدی به دولت هدف وارد کند. در چنین مواردی، تعیین میزان تناسب میان واکنش دولت و حمله سایبری چالش بزرگی محسوب می‌شود.

همچنین، یکی از موضوعات کلیدی در تحلیل حقوقی دفاع پیش‌دستانه در حوزه سایبری، **شناسایی عاملان حمله** است. در حملات سایبری برخلاف حملات نظامی سنتی، عاملان حمله معمولاً ناشناخته هستند و ردیابی دقیق آنان ممکن است ماه‌ها یا حتی سال‌ها طول بکشد (Hollis, 2020). در نتیجه، واکنش سریع و پیش‌دستانه به این حملات به دلیل مشکل در شناسایی منابع حمله، به‌طور جدی به چالش کشیده می‌شود. این مسئله به‌ویژه هنگامی که دولت‌ها یا بازیگران غیردولتی پشت حمله قرار دارند، اهمیت بیشتری پیدا می‌کند.

از منظر حقوق بین‌الملل، تفسیر ماده ۵۱ منشور سازمان ملل نیز به چالش کشیده شده است. این ماده به دولت‌ها اجازه می‌دهد که در صورت وقوع یک حمله مسلحانه، از حق دفاع مشروع

برخوردار باشند. با این حال، مسئله این است که آیا یک حمله سایبری می‌تواند به‌عنوان **حمله مسلحانه** در چارچوب ماده ۵۱ تلقی شود؟ برخی از حقوقدانان معتقدند که اگر یک حمله سایبری به‌اندازه‌ای خسارت‌بار باشد که همانند حملات مسلحانه فیزیکی تأثیرگذار باشد، می‌تواند دفاع مشروع را توجیه کند .(Schmitt, 2017) با این حال، این دیدگاه همچنان مورد مناقشه است و تفسیرهای متفاوتی درباره معیارهای لازم برای شمول حملات سایبری تحت ماده ۵۱ وجود دارد.

بنابراین، بررسی دکترین دفاع پیش‌دستانه در حملات سایبری نشان می‌دهد که چارچوب حقوقی کنونی با چالش‌های جدی در این حوزه مواجه است. تطبیق اصول سنتی ضرورت، تناسب، و شناسایی عاملان حمله با واقعیت‌های نوین سایبری نیازمند بازنگری و تدوین قواعد حقوقی جدید است که بتوانند به‌طور مؤثر به این تهدیدات پاسخ دهند. عدم وجود چارچوب‌های روشن و توافقات بین‌المللی در این زمینه، خطر تشدید تنش‌ها و سوءاستفاده از مفهوم دفاع پیش‌دستانه را به‌ویژه در فضای سایبری افزایش می‌دهد.

دفاع مشروع در برابر حملات سایبر تروریستی و چالش های پیش روی آن

بعد از حادثه ۱۱ سپتامبر تحولی عظیم در زمینه دفاع مشروع در برابر حملات تروریستی بوجود آمد .و نظریه پردازی های زیادی در نقطه مقابل نظریه سنتی دفاع مشروع قوت گرفت. بخصوص استناد نظریه پردازان مخالف با دفاع مشروع سنتی به قطعنامه هایی بود که شورای امنیت بعد واقعه ۱۱ سپتامبر به تصویب رسانید.

همان طور که قبلا گفته شد »در منشور ملل متحد دو استثنا بر اصل ممنوعیت توسل به زور موجود است: «دفاع مشروع فردی و جمعی و دوم توسل به زور در قالب سیستم امنیت دست جمعی. منشور ملل متحد با اولویت دادن به نظام امنیت دسته جمعی اقدامات شورای امنیت در راستای حفظ صلح و امنیت بین المللی را استثنای اصلی ،اصل منع توسل به زور تلقی کرده است و تا زمانی که این استثنا فعلیت نیافته است ،دفاع مشروع فردی و جمعی را حق ذاتی و طبیعی دولتها می داند.» همچنین قبلا اشاره شده بود که «ماده ۵۱ در واقع قاعده ی جدیدی را به وجود نیاورده است ،بلکه از حقوق بین الملل عرفی گرفته شده است به عبارت دیگر این ماده تنها بخشی از ضوابط توسل به دفاع مشروع را مورد توجه قرار داده است و به منظور بررسی سایر شرایط حاکم

بر اعمال دفاع مشروع از جمله ضرورت و تناسب وهم چنین مفهوم حمله مسلحانه باید به حقوق عرفی موجود در این خصوص رجوع کرد». (کدخدایی و زرنشان، ۱۳۸۶: ۸۸) از طرفی منشا حمله های مسلحانه علیه دولتها در ماده ۵۱ مشخص نشده است. همین امر باعث شده که حقوق بین الملل با چالش های زیادی در ارتباط با نقش بازیگران غیر دولتی در حملات مسلحانه روبرو باشد. این در حالی است که در دیوان بین المللی دادگستری در نظر مشورتی خود در قضیه دیوار حائل توسل به دفاع مشروع را منوط به قابل انتساب دانستن وقوع حمله مسلحانه به یک دولت خارجی دانسته اند. (گزارش دیوان بین المللی دادگستری، ۲۰۰۴: بند ۱۳۹)

در مورد دفاع مشروع در برابر حملات تروریستی دو نظر وجود دارد. یک نظر مربوط به تفسیر مضیق از ماده ۵۱ وتفسیر دیگر موسع است. که دفاع مشروع پیشگیرانه و پیش دوستانه را هم در بر می گیرد. مفاهیمی که بعد یازده سپتامبر دکترین حقوقی آن را حمایت کردند.

در تفسیر مضیق از ماده ۵۱ منشور می گویند دفاع مشروع صرفا در برابر حمله مسلحانه و نظامی از سوی یک دولت علیه دولت دیگر آن هم تا زمان اقدام شورای امنیت در قالب اقدام دسته جمعی و با رعایت تناسب و ضرورت و حقوق بشر دوستانه مجاز می باشد.

پروفسور باوت در خصوص ماده ۵۱ بیان می فرماید که «(برخی معتقدند) دفاع مشروع مندرج در منشور ملل متحد همان دفاع موجود در حقوق عرفی گذشته است ،یعنی دفاع مشروع پیشگیرانه حفظ مصالح و منافع کشور و غیره اما به نظر می رسد چنین تفسیری اصلا مورد قبول نیست وتنها تفسیر مورد قبول همان تفسیر مضیق است». (ابراهیمی، ۱۳۸۴: ۹۳-۹۴) اما با بررسی ماده ۹۴منشور و حقوق بین الملل عرفی این نتیجه بدست می آید که توسل به زور برای دفاع مشروع حق ذاتی است اما بی قید وشرط هم نیست. اول اینکه اصل ضرورت ،فوریت ،اجتناب ناپذیری ،نداشتن انتخاب دیگر و نداشتن فرصتی برای مذاکره وجود دارد دیوان بین المللی دادگستری اصل ضرورت را به عنوان یک قاعده عرفی بین المللی تائید کرده است. (گزارش های دیوان بین المللی دادگستری، ۱۹۹۶: ۴۱) «هم چنین دیوان در قضیه نیکاراگوا اظهار می دارد که اصل ضرورت ،توسل به نیروی مسلحانه را به حصول اهداف نظامی مشروع محدود می کند چنان چه نابودی نیروهای متجاوز و دفاع در سرزمین دولت متجاوز برای اعمال دفاع مشروع ضروری باشد یک

دولت می تواند به انجام آن مبادرت ورزد[1]» حث فوریت حمله وهم چنین نبود گزینه ای دیگر نیز از بحث های بسیار مهم در زمینه حقوق بین الملل است. اینکه فوریت یک حمله چگونه باید محاسبه شود بسته به شرایط حمله و نیز پاسخگویی دارد وحداقل فاصله زمانی طبق عرف باید موجود باشد. اما توسل به زور باید برای دفع حمله مسلحانه باشد و هر گونه اقدامات تلافی جویانه توسط دولت ها ممنوع می باشد.

اصل بعدی ،اصل تناسب است در حقوق مخاصمات مسلحانه اصل تناسب بر پایه یک اصل مبنایی قرار دارد. این اصل می گوید که طرفین متخاصم در استفاده از ابزار برای ضربه زدن به دشمن انتخاب نامحدودی ندارد .بنابراین دیدیم که در تفسیر مضیق فقط اجازه دفاع مشروع و آن هم با رعایت شرایط آن در برابر حملات مسلحانه داده شده است. (محمدعلیپور، ۱۳۸۱: ۳۵)

در حال حاضر در حوزه دفاع مشروع ،دکترینی مطرح شده اندکه دفاع مشروع رادر وضعیت های خاص مجاز می شمارند. این ها به دفاع مشروع پیش دستانه معروف شده اند. طبق این دکترین پاسخ مسلحانه به حملات قریب الوقوع و یا زمانی که حمله ای وقوع یافته و دولت قربانی در یافته است که حملات بیشتری در حال طراحی است مجاز است. در این دکترین دفاع مشروع در چند حالت مجاز است اول زمانی که شواهد متقاعده کننده ای نه صرفا مبنی بر تهدید یا خطر بالقوه بلکه مبنی بر حمله ای قریب الوقوع وجود داشته باشد و احتمال حمله مسلحانه وقوع یابد حالت دوم این است که دولتی یکبار مورد حمله مسلحانه قرار گرفته باشد و در حال حاضر شواهد اشکاری مبنی بر حمله دوباره باشد. پس از حمله ۱۱ سپتامبر امریکا و بریتانیا اقداماتی علیه افغانستان انجام دادند آن ها به وجود شواهدی مبنی بر وقوع حملات بیشتر اشاره می کردند. (موسوی و حاتمی، ۱۳۸۵: ۳۰۵-۳۱۵)

دفاع مشروع پیشگیرانه به مواردی گفته می شود که یک دولت برای سرکوب هر گونه احتمال حمله آتی توسط دولتی دیگر به زور متوسل می شود. دفاع مشروع پیشگیرانه در حقوق بین الملل جاری ،غیر قانونی است. هرچند دولت هایی مثل امریکا از این که دیگر دولت ها به سلاح های کشتار جمعی دسترسی یابند نگرانند واستدلال می کنند که صرف داشتن چنین سلاح هایی می توانند توسل به زور طبق دفاع مشروع را توجیه کند.

---

۱ پرونده نیکاراگوئه، بند ۳۵

اما طرفدارانی که معتقدبه تفسیر موسع از مقررات منشور هستند استناد به قطعنامه ۱۳۶۸و ۱۳۷۳ شورای امنیت می کنند. شورای امنیت پس از وقوع حملات۱۱ سپتامبر اقدام به صورت این دو قطعنامه کرده است. شورای امنیت در مقدمه قطعنامه ۱۳۶۸[1]، اقدامات تروریستی را به عنوان تهدیدی علیه صلح و امنیت بین الملل مطرح می کند و حق ذاتی دفاع مشروع فردی یا جمعی طبق منشور را به رسمیت می شناسد. شورا هم چنین در مقدمه ۱۳۷۳[2] بار دیگر حملات ۱۱ سپتامبر را تهدیدی علیه صلح و امنیت بین المللی دانسته و آن را محکوم کرد و بار دیگر حق دفاع مشروع را به رسمیت شناخت .شورای امنیت هم چنین تلاش کرد بین مفهوم حمله تروریستی و حمله مسلحانه مندرج در ماده ۵۱ ارتباط بر قرار کند.

قبل از حوادث ۱۱ سپتامبر عموم دولتها تفسیر مضیقی از ماده ۵۱ منشور داشتند. اکثریت دولتها حق دفاع مشروع علیه شبکه های تروریستی مستقر در سرزمین دولتها ی دیگر را مورد شناسایی قرار نمی دادند. دفاع مشروع به عنوان پاسخی فوری به حمله مسلحانه موجود در نظر گرفته می شد واز دید اکثریت دولتها ،دفاع مشروع پیش دستانه یا پیشگیرانه غیر قانونی بود هر چند موضوع آمریکا و اسرائیل درست برعکس بود.

اما بعد حمله ۱۱ سپتامبر ادعاهای جدیدی مطرح شد برخی از حقوقدانان معتقدند که قاعده سنتی دفاع مشروع تغییر کرده و اصلاح شده است اوبرینگ معتقد است که رویه دولت ها بین ۱۲ سپتامبر تا ۱۰ اکتبر ۲۰۰۱ (قطعنامه های شورای امنیت ،اعلامیه های ناتو ،اظهارات حمایتی اتحادیه اروپا و اعلامیه سازمان کنفرانس اسلامی) نشان می دهد که قاعده سنتی دفاع مشروع اصلاح شده و دامنه آن توسعه یافته است. هیچ یک از اعضا ی شورای امنیت به تفسیر جدید ماده ۵۱ اعتراض نکرده اندو بدین ترتیب تفسیر موسع ماده ۵۱ مشروع می باشد.[3]

شرط دیگر دفاع مشروع تناسب بین حمله و دفاع است. در واقع باید بین عمل دفاع و حمله تناسبی حداقل نسبی موجود باشد. در حوزه سایبر در عمل واکنش یکسانی به حمله سایبری را نمی توانیم متصور شویم. دلیل آن هم این است که سرعت پیشرفت تکنولوژی بالاست ولی این وضعیت در همه کشورها یکسان نیست. کشورهای غربی اغلب دارای تکنولوژی پیشرفته تری

1 S.c. Ress1368,12sep,2001
2 S.c.Ress1373 ,28sep.2001
3 Ove Bring, Military Defence against International Terrorism availiable on http//: www .kkrva. se/eng / rsawspj/016/ brings.html

هستند. همچنین گاهی گروه های تروریستی از چنان دانشی در حوزه فناوری اطلاعات برخوردارند که شاید یکسری از کشورها هنوز به آن دانش نرسیده باشند. (گرین برگ، ۱۹۹۸) در این فرضیه آیا می شود تصور کرد در مقابل از کار انداختن سیستم گازرسانی یک کشور از طریق حمله سایبری به کشوری که گروه تروریستی درآن است حمله مسلحانه فیزیکی یا سایبری کرد؟ قطعا پاسخ این سوال نمی تواند مثبت باشد. درست است که گاهی حملات حوزه سایبر درصد تخریبی وسیع تری از حملاتی که بصورت فیزیکی اتفاق می افتد دارد ولی در حملات باید سلاح ها وابزار بکارگرفته شده تناسب داشته باشد. اما دکترین انباشت رویداد که توسط امریکا واسرائیل حمایت می شود، معتقد است که چند حمله مرزی کوچک و با شدت اندک می شود در مجموع یک حمله مسلحانه تلقی شود. در حوزه سایبر هم همین قاعده اجرا می شود. (زمنک، ۲۰۱۰)

به هرحال این ها شرایطی است که در دفاع مشروع علیه حملات سایبری در نظر گرفته می شود .چالش های پیش روی کشور ها دررعایت دقیق این ضوابط، بسیار است.

اما در ارتباط با موضع اتخاذ شده کشورها در این زمینه ، کشور هایی که موضع دفاع مشروع پیش دستانه و پیش گیرانه را در نوع سنتی تروریسم دارند، در مورد تروریسم سایبری نیز همین عقیده را دارند «آنها معتقد به امکان دفاع مشروع در برابر حملات سایبر تروریستی هستند و معتقدند چون در هر حال دفاع مشروع بعد ۱۱ سپتامبر در برابر حملات تروریستی صورت میگیرد، در برابر حملات سایبر تروریستی نیز می توان دفاع مشروع انجام داد. ایالات متحده آمریکا در خصوص حق دفاع مشروع در تقابل با حملات سایبری مواضعی را اتخاذ نموده است. براساس ارزیابی وزارت دفاع این کشور ،کشور حامی حملات سایبری ،حق توسل به دفاع مشروع را برای طرف مقابل ایجاد می کند. از منظر این وزارت خانه هرگاه یک حمله ی شبکه ای رایانه ای هماهنگ سیستم کنترل ترافیک هوایی یک کشور و یا سیستم های بانک داری و مالی آن را مختل کند دریچه چندین سد را باز کند و هر کدام تلفات گسترده غیر نظامیان و صدمات اقتصادی و مالی داشته باشد کشور را چند قربانی حمله مسلحانه است.» (راهنمای تالین در مورد حقوق بین الملل قابل اجرا در جنگ سایبری، دفاع عالی سایبری تعاونی ناتو، ۲۰۱۳: ۵۲-۶۰.)

اما به نظر می رسد باید بیشتر به این گونه حملات و ویژگی خاص درون آنها توجه کرد.

حمله ها یا تهدید به حمله های سایبر تروریستی از طریق فضای سایبر اتفاق می افتد. حمله هایی که ممکن است توسط یک فرد به صورت مستقل و به طریق تروریستی یا توسط یک گروه تروریستی اتفاق می افتد. یا حمله هایی که یک هکر بدون انگیزه های تروریستی انجام دهد.

چگونه می توان علیه یک حمله قطع سرویس دهی که سیستم بانکی یک کشور را مختل می کند دفاع مشروع انجام داد آیا کشوری که مورد حمله قرار گرفته، توانایی مختل کردن سیستم بانکی کشور مقابل را دارد ؟آیا اجازه ی این را دارد که بدون در نظر گرفتن اینکه حمله از طریق چه گروهی یا فردی اتفاق افتاده به کشوری حمله کنند؟

حملات سایبر تروریستی که اثر آن ابعاد تخریبی مثل نوع سنتی عملیات تروریستی داشته باشد را می توان حمله مسلحانه در نظر گرفت. ارسال یک تروجان به سیستم یک هواپیما و اختلال در پرواز که منجر به سقوط آن می شود در حد یک حمله تروریستی هوایی است. اما مشکل اساسی در حملات سایبر تروریستی و مقابله با آن مفاهیمی که موجود است، این است که ویژگی فضای سایبر ناشناس بودن در آن است. حتی برای کشورهایی با توان و ظرفیت تکنولوژیکی بالا امکان بر آورد اینکه حمله از طرف چه کشوری بوده بسیار سخت است .اگر همهی کشورها به این جایگاه برسند که بتوانند کشوری که حمله از طریق آن صورت گرفته را تشخیص دهند چطور می توان ثابت کرد که حمله از طریق مقامات آن کشور بوده است یا اینکه آن کشور حامی گروه تروریستی است و مسئولیت حمایت دارد و اینکه آن کشور با حمایت از گروه های تروریستی اجازه ی حمله به کشور قربانی را صادر کرده ومی توان علیه آن دفاع مشروع انجام داد؟

برای بارزتر کردن این مساله باید تاکید کرد که اولا سنجیدن این مساله که حمله سایبری تا چه حد می تواند موضوع حمله مسلحانه مقرر در ماده ۵۱ را تشکیل دهد بسیار بحث برانگیز است. مصادیق حمله مسلحانه در قطعنامه تعریف تجاوز و بعد طبق بعضی اعمالی که در طول سالیان تا حمله ۱۱ سپتامبر اتفاق افتاد می تواند محدوده ای از حملات تروریستی را مشخص کند.

ما در مورد حملات مسلحانه سایبر تروریستی هیچ قاعده و معیاری وجود ندارد اینکه چطور می توان یک حمله را مسلحانه تلقی کرد را باید با توسل به قواعد علم کامپیوتر در نظر گرفت. چرا که حملاتی که از طریق حوزه ی سایبر اتفاق می افتد دارای شدت و ضعف است مثلا درصد

تخریبی یک تروجان دارد را یک حمله قطع سرویس دهی ندارد به هر حال به نظر می رسد در هر مورد که حمله اتفاق می افتد با توجه به شدت حمله واثراتی که دارد باید آن را دنبال کرد.

معمولا در نوع سنتی تروریسم گروه های تروریستی و کشورهایی که حامی هستند مشخص هستند و شواهد و قراین زیادی وجود دارد و گاه خود گروه های مسئولیت ناشی از حمله تروریستی را می پذیرند.

در فرض حمله از طریق فضای سایبری به یک کشور که توسط گروه های تروریستی انجام می شود ممکن است حمله توسط یک فرد از یک گروه تروریستی در همان کشوری که قربانی حمله است اتفاق بیفتد در این باره تکنولوژی کمک زیادی می تواند به کشور قربانی کند اما می توان گفت می توان دفاع مشروع علیه گروه تروریستی مستقر در یک کشور دیگر را ترتیب داد ؟ باز هم مشکل تعدد کشورهایی موجود است که گروه های تروریستی در آن جا مستقر هستند. با گسترش عمل رادیکالیزه کردن اتاق اینترنت شاید به جرأت بتوان گفت در اکثر کشور های دنیا عضو گیری می شود. آیا می توان علیه اکثر کشور های دنیا حمله سایبری انجام داد؟

در این باره باید گفت انتساب اینکه چه کشوری حامی گروه تروریستی بوده و عمل گروه تروریستی می تواند عمل آن کشور تلقی شود کاری غیر قابل تصور و یا با درصد انتساب بسیار پایینی است. نمی توان صرف وجود یک گروه تروریستی را عاملی برای دفاع مشروع در برابر حملات سایبر تروریستی دانست و حمله سایبر تروریستی به کشور مورد نظر کرد. در ویژگی های حملات سایبر تروریستی گفته شد حتی یک کشور نمی داند که حملات از طریق سرور های آن کشور اتفاق می افتد.

از طرفی ویژگی های حقوق بین المللی عرفی و معاهداتی مثل منشور برای دفاع مشروع در نظر گرفته است مثل ضرورت ، تناسب .به طور مثال ارسال تروجان به سیستم بانکی یک کشور که موجب خسارت شدیدی می تواند باشد. این تناسب و چگونگی حمله ها چندان مقیاس درستی ندارد. هم چنین در باب فوریت باید گفت که اگر کشور قربانی امکانات تکنولوژی لازم برای دفاع مشروع نداشته باشد نمی تواند این فرض را متصور شد که پنج یا شش سال بعد پس از بدست آوردن فناوری علیه گروه تروریستی که در کشور دیگری قرار دارد حمله نماید.

«به دیگر سخن باید دقت نمود که هر حمایت و پشتیبانی، اگر چه ممکن است مسؤلیت بین المللی دولت حامی یا پشتیبان را بوجود آورد، ولی نمی تواند اعمال وبه ویژه حملات مسلحانه تروریست ها را به دولت حامی و به طور دقیق تر به دولت میزبان آن ها منتسب نماید. برای اثبات چنین رابطه ای لازم است که یک دولت خارجی یا در حملات و اعمال تروریستی مسلحانه مشارکت داشته باشد، یا چنین حملاتی را تصدیق نموده باشد، و یا بر گروه و سازمان های تروریستی مربوط آنچنان درجه ای از کنترل را داشته باشد که از نقطه نظر حقوقی بتوان اعمال گروه یا سازمان های تروریستی را در حقیقت اعمال خود آن دولت در نظر گرفت.» بنابراین مسولیت کشور ها نیز از بابت اعمال سایبر تروریستی یا با احراز شرایط بالا و یا بدلیل عدم کنترل سیستم های امنیتی کشورشان است.

نتیجه گیری

نتیجه‌گیری در زمینه دفاع پیش‌دستانه در برابر حملات سایبری نشان می‌دهد که حقوق بین‌الملل با چالشی اساسی برای تطبیق با تهدیدات مدرن مواجه است. دکترین دفاع پیش‌دستانه به‌عنوان یکی از ابزارهای کلیدی دولت‌ها برای واکنش به تهدیدات فوری و قریب‌الوقوع، در شرایط سنتی نظامی بر اساس معیارهای مشخص ضرورت و تناسب استوار است. اما در عصر دیجیتال، این معیارها با پیچیدگی‌های فراوانی روبرو هستند. حملات سایبری اغلب به‌صورت نامرئی و غیرمستقیم انجام می‌شوند و تشخیص فوری تهدید یا میزان آسیب‌های احتمالی آن‌ها دشوار است. همین امر باعث شده که بسیاری از اصول سنتی حقوق بین‌الملل به‌ویژه در زمینه شناسایی حمله، ضرورت واکنش، و تعیین تناسب با محدودیت‌های عملی مواجه شوند.

از یک سو، اصول حقوق بین‌الملل همچنان بر ممنوعیت استفاده از زور تأکید دارد، مگر در موارد مشخص دفاع مشروع، که بر اساس ماده ۵۱ منشور سازمان ملل به‌عنوان واکنش به یک حمله مسلحانه تعریف شده است. اما تطبیق مفهوم حمله مسلحانه با حملات سایبری، همچنان محل مناقشه است و حقوق بین‌الملل به‌روشنی نتوانسته این مسئله را حل‌وفصل کند. در مواردی که حملات سایبری به زیرساخت‌های حیاتی دولت‌ها آسیب‌های گسترده و جدی وارد می‌کنند، به‌عنوان مثال حملات به شبکه‌های انرژی، مالی یا حتی نظامی، می‌توان آن‌ها را تحت شرایط

خاصی به‌عنوان حمله مسلحانه تعریف کرد. با این حال، اختلاف‌نظرها درباره میزان و شدت خسارات لازم برای احراز این تعریف، همچنان پابرجاست.

مسئله شناسایی دقیق عاملان حمله نیز یکی دیگر از چالش‌های اصلی در استفاده از دفاع پیش‌دستانه است. در موارد حملات سایبری، دولت‌ها اغلب نمی‌توانند به‌سرعت و با دقت عاملان اصلی حمله را شناسایی کنند. این مشکل به‌ویژه در مواردی که بازیگران غیردولتی یا دولت‌های ثالث در پشت حملات قرار دارند، شدیدتر می‌شود. عدم توانایی در شناسایی فوری منبع حمله، به‌طور جدی واکنش‌های پیش‌دستانه را به چالش می‌کشد و ممکن است منجر به استفاده نادرست از این دکترین شود. به همین دلیل، برخی از محققان و کشورها معتقدند که باید چارچوب‌های حقوقی جدید و بین‌المللی برای مقابله با تهدیدات سایبری تدوین شود تا امکان واکنش مشروع و منطبق با حقوق بین‌الملل فراهم شود.

با توجه به این تحلیل‌ها، مشخص است که حقوق بین‌الملل به قواعد و اصول جدیدی نیاز دارد که به‌طور خاص به تهدیدات سایبری بپردازد. ایجاد تعاریف دقیق‌تری برای حملات سایبری که بتوانند به‌عنوان حمله مسلحانه محسوب شوند، شفاف‌سازی معیارهای ضرورت و تناسب در واکنش به این حملات، و تدوین چارچوب‌های بین‌المللی برای شناسایی عاملان حملات سایبری از جمله اقداماتی هستند که جامعه بین‌المللی باید به آن‌ها توجه کند. بدون چنین اصلاحات و تحولات حقوقی، دولت‌ها همچنان با عدم قطعیت‌های حقوقی مواجه خواهند بود که می‌تواند تنش‌های بین‌المللی و خطر تشدید درگیری‌ها را افزایش دهد.

در نهایت به نظر می‌رسد، بحث حملات سایبری و دفاع پیش‌دستانه نشان می‌دهد که تحول و تطبیق حقوق بین‌الملل با تهدیدات مدرن نه‌تنها ضروری است، بلکه نیازمند همکاری گسترده بین‌المللی و ایجاد توافقات جدید میان دولت‌هاست. به موازات پیشرفت‌های فناورانه، حقوق بین‌الملل نیز باید به‌روز شود تا بتواند به‌طور مؤثر و مسئولانه به تهدیدات سایبری پاسخ دهد و از تشدید تنش‌ها و بحران‌های بین‌المللی جلوگیری کند.

فهرست منابع

ابراهیمی، نصر الله، تجاوز دفاع مشروع در حقوق بین الملل، مجله حکومت اسلامی، قم، پاییز و زمستان ۱۳۸۴.

ارفعی، عالیه و دیگران، حقوق بشر از دیدگاه مجامع بین‌المللی، زیر نظر محمدرضا دبیری، چاپ اول، موسسه چاپ و انتشارات وزارت امور خارجه، تهران، ۱۳۷۲ ه ش.
اسکندری، محمد حسین، قاعده مقابله به مثل در حقوق بین‌الملل از دید اسلام، چاپ اول، مرکز انتشارات دفتر تبلیغات اسلامی حوزه علمیه قم، قم، ۱۳۷۹ ه ش.
آقابخشی، علی اکبر، افشاری راد، مینو، فرهنگ علوم سیاسی، نشر چاپار، چاپ دوم، ۱۳۸۷.
آقابخشی، علی، افشاری راد، مینو، فرهنگ علوم سیاسی، نظر چاپار، تهران، ۱۳۷۹ ه ش.
آکهرست، مایکل، حقوق بین‌الملل نوین، ترجمه بهمن آقایی، چاپ دوم، دفتر خدمات حقوقی بین‌المللی جمهوری اسلامی ایران، تهران، ۱۳۷۶ ه ش.
بیگ زاده، ابراهیم، جزوه حقوق بین‌الملل عمومی ۲، دانشگاه شهید بهشتی، سال تحصیلی ۸۴-۸۵.
پلینو، جک سی، التون، روی، فرهنگ روابط بین‌الملل، ترجمه حسن پستا، چاپ اول، انتشارات فرهنگ معاصر، تهران، ۱۳۷۵ ه ش.
جوادی عاملی، عبد الله، حماسه و عرفان، چاپ اول، مرکز نشر اسراء، قم، ۱۳۸۱ ه ش.
حجازی، محمدعلی، حقوق اسیران جنگی، چاپ اول، نشر میزان، تهران، ۱۳۸۷ ه ش.
حسینی ژرفا، سید ابوالقاسم، جهاد و حقوق بین‌الملل، چاپ دوم، سازمان انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی، ۱۳۸۶ ه ش.
حمیدالله، محمد، سلوک بین‌المللی دولت اسلامی، ترجمه سید مصطفی محقق داماد، چاپ سوم، مرکز نشر علوم اسلامی، تهران، ۱۳۸۴ ه ش.
خسرو شاهی، قدرت الله، فلسفه قصاص از دیدگاه اسلام، چاپ اول، انتشارات دفتر تبلیغات اسلامی حوزه علمیه قم، قم، ۱۳۸۰ ه ش.
خلیلیان، سید خلیل، حقوق بین‌الملل اسلامی، چاپ هشتم، دفتر نشر فرهنگ اسلامی، تهران، ۱۳۷۸ ه ش.
زمانی، سید ابوالقاسم، حقوق بین‌الملل و کاربرد سلاح‌های شیمیایی در جنگ عراق علیه جمهوری اسلامی ایران، چاپ اول، بنیاد حفظ آثار و ارزش‌های دفاع مقدس، تهران، ۱۳۷۶ ه ش.
شبرنگ، محمد، منشور ملل متحد، چاپ اول، نشر دانشور، ۱۳۸۲.
ضیایی بیگدلی، محمدرضا، حقوق بین‌الملل عمومی، انتشارات گنج دانش، چاپ ۵۱، ۱۳۹۴.
عظیمی شوشتری، عباسعلی، حقوق بین‌الملل اسلام، انتشار دادگستر، ۱۳۹۲.
عمید، حسن، فرهنگ فارسی، چاپ ۲۳، نشر امیرکبیر، ج ۲، ۱۳۸۳.
عمید زنجانی، عباسعلی، فقه سیاسی، انتشارات امیرکبیر، چاپ اول، ۱۳۸۲.
محمدعلیپور، فریده، دفاع مشروع، مجلس و پژوهش، ۱۳۸۱، شماره ۳۵.
مسائلی، محمود، ارفعی، عالیه، جنگ و صلح از دیدگاه حقوق و روابط بین‌الملل، اداره نشر وزارت امور خارجه، چاپ دوم، ۱۳۷۳.

معین، محمد، فرهنگ فارسی، ج ۲، ۱۳۵۱.

موسوی، سیدافضل، حاتمی، مهدی، دفاع مشروع پیش دستانه در حقوق بین‌الملل، مجله دانشکده حقـوق و علـوم سیاسی دانشگاه تهران، ۱۳۸۵، شماره ۷۲.

موسوی، سید فضل اله، اندیشه‌های حقوقی ۷ (حقوق بین‌الملل)، تهران: انتشارات مجد، چاپ اول، ۱۳۹۱.

Bowett, D.W. Self Defence in International Law; Manchester University Press, 1958.

Bring, Ove. Military Defence against International Terrorism, available at http://www.kkrva.se/eng/rsawspj/016/brings.html.

Cassese, Antonio. Terrorism is also Disrupting some Crucial Legal Categories of International Law. Available at http://ejil.org/forum-wte-cassese-02.html.

Dinstein, Y. War, Aggression and Self-Defence. Cambridge University Press, 2017.

Duffy, H. "Foreign Terrorist Fighters": A Human Rights Approach? Security and Human Rights, 29(1-4), 120-172,
2018.

Erakat, Noura S. New Imminence in the Time of Obama: The Impact of Targeted Killings on the Law of Self-Defense, 56 ARIZ. L. REV., 2014.

Greenberg, L.T. Information Warfare and International Law, Mishawaka: National University Press, 1998.

Hunter, William. Yale Law School's Avalon Project: Documents in Law, History and Diplomacy, British-American Diplomacy, The Caroline Case. Available at http://avalon.law.yale.edu/19th_century/br-1842d.asp.

ICRC. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 2011, p. 37; International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 2015.

John J. Merriam. Natural Law and Self-Defense, 206 MIL. L. REV. 43, 59-61 (2010); Schmitt, supra, note 14, at 529-530.

Legality of The Use of Force by the State of Nuclear Weapons in Armed Conflict Advisory Opinion, ICJ Report (1996).

MICHAEL WALZER. Just and Unjust Wars: A Moral Argument with Historical Illustrations, 74-75 (4th ed., 2006).

NATO Cooperative Cyber Defense of Excellence. Tallinn Manual on The International Law Applicable to Cyber Warfare, 2013.

O'Connell, Mary Ellen. The Myth of Pre-emptive Self-Defence, The American Society of International Law Task Force on Terrorism, August 2002.

Parry, C., Grant, J. P., & Barker, J. C. Parry & Grant Encyclopaedic Dictionary of International Law, Oxford University Press, 2009.

Prosecutor v. Kupreskic, Case No. IT-95-16, judgment (Int'l Crim. Trib. for the Former Yugoslavia 14 January 2000), para. 520.

Reisman, W. M., & Armstrong, A. (2006). The Past and Future of the Claim of Preemptive Self-Defense. American Journal of International Law, 100(3), 525-550.

Robertson, Horace B., Jr. Self-Defense against Computer Network Attack under International Law, International Law Studies, U.S. Naval War College, Vol. 76, (2002).

Sadoff, D. A. (2008). A Question of Determinacy: The Legal Status of Anticipatory Self-Defense. Geo. J. Int'l L., 40, 523.

Schmitt, M. N. (2002). Preemptive Strategies in International Law. Mich. J. Int'l L., 24, 513.

Shaw, M. N. International Law, Cambridge University Press, 2017.

Tallinn Manual on The International Law Applicable to Cyber Warfare, The NATO Cooperative Cyber Defense of Excellence, 2013.
Use of Internet for Terrorist Purposes, CTITF, 2011.
Wallace, R. M., & Martin-Ortega, O. International Law, Sweet and Maxwell, 2020.
Zemenek, K. Armed Attack, Max Plank Encyclopedia of Public International Law, Oxford University Press, 2010.
Gegout, C., & Granholm, N. (2021). Cybersecurity and International Law: A Call for a More Comprehensive Approach. International Security Review.
Kastenberg, J. (2022). Cyber Conflict and the Law of War: A Legal Perspective on the Use of Force in Cyberspace. Global Cyber Law Journal.
Roscini, M. (2020). Cyber Operations and the Use of Force in International Law. Oxford University Press.
Nasu, H., & Fahey, J. (2021). The Future of Cyber Law: International Governance in a Connected World. Cambridge University Press.
Hollis, D. (2020). Attribution in Cyberspace: Problems and Solutions. Global Cyber Law Review.
Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.