فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲
وبگاه مجله: https://cyberlaw.maragheh.iau.ir

Right to "Self-Defense" against Cyber-attacks with an Emphasis on the Attacks of the United States of America

Saeid Eid Koshayesh
Ph.D. Student in Public International Law, Maragheh Branch, Islamic Azad University, Maragheh, Iran
Hossein Sorayaii Azar*
Assistant Professor of International Law, Maragheh Branch, Islamic Azad University, Maragheh, Iran
Jahangir Bagheri
Assistant Professor of Political Science, Maragheh Branch, Islamic Azad University, Maragheh, Iran
hosseinsorayaiiazar@iau-maragheh.ac.ir

DOI 10.30495/CYBERLAW.2023.701877

Keywords:
Self-Defense, Cyber-attacks, United States Government , Safe Haven, Digital Defense, Cyber War.

Abstract

Hostile actions and resorting to coercive force in the cyberspace fields are very important issues that could challenge fundamental principles of the international law. Many States consider the cyberspace as a battlefield and intend to inflict damages through it to their opponent states. United States is considered an avant-garde in these issues. The United States possess many advanced technologies in cyberspace field. In this respect, the necessity of self-defense (legitime defense) against cyber-attacks seems inevitable, although from "treaty law" point of view it lacks the basic internationally supported legislations. It remains to be clarified whether the 51th Article of the United Nations Charter could be used as a legal base for cyber self-defense or not and if that could be entitled self-defense or not. This study employs descriptive-analytical method through data analyzing system. Findings of this study indicate that in the event of a cyber-attack by a State or its agents, a cyber-self-defense could be legally justifiable provided that the legal conditions of the self-defense such as compatibility of self-defense with the attacks and some other international law principles (principle of non-use of force for example) are met, Of course, in the path of self-defense, the principle of proportionality must be observed as the main rule, and as soon as the Security Council effectively intervenes in the crisis, the defense must be terminated.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

حق بر «دفاع مشروع» در قبال حملات سایبری با تاکید بر حملات ایالات متحده آمریکا

سعید عید کشایش

دانشجوی دوره دکتری حقوق بین الملل عمومی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.

حسین ثریائی آذر*

استادیار، گروه حقوق دانشکده علوم انسانی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.

جهانگیر باقری

استادیار، گروه حقوق دانشکده علوم انسانی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.

hosseinsorayaiiazar@iau-maragheh.ac.ir

تاریخ دریافت: ۳۰ آذر ۱۴۰۱ تاریخ پذیرش: ۲۵ فروردین ۱۴۰۲

چکیده

اقدامات خصمانه و توسل به‌زور در فضای سایبر موضوع بسیار مهمی است که توانایی مواجه کردن حقوق بین‌الملل با چالش‌هایی اساسی را دارد؛ چراکه دولت‌های مختلف فضای مذکور را به‌عنوان میدان جنگ تلقی نموده و در راستای ایراد خسارت به دیگرانی هستند که آن را دشمن خود خطاب می‌نمایند، یکی از مهم‌ترین و تأثیرگذارترین این کشورها ایالات‌متحده آمریکا است که با استفاده از تجهیزات فوق پیشرفته خود به این اقدامات علیه دولت‌های دیگر دست می‌یازد. در این راستا ضرورت انجام دفاع مشروع در مقابل این حملات اجتناب‌ناپذیر جلوه می‌نماید؛ اما سؤال اساسی آن است که با توجه به قواعد موجود بین‌المللی و به‌طور خاص ماده ۵۱ منشور ملل متحد می‌توان به این اقدام دست یازید و از آن به دفاع مشروع سایبری یادکرد یا خیر. این پژوهش با روش توصیفی–تحلیلی به مطالعه منابع مرتبط با موضوع و گردآوری اطلاعات پرداخته است. نتایج تحقیق نشان می‌دهد که در صورت انجام حمله سایبری از جانب بازیگر دولتی یا انتساب آن به دولت با رعایت شرایط دفاع مشروع درزمینه انتساب، شدت درجه نقض اصل عدم توسل به‌زور و گزارش به شورای امنیت سازمان ملل متحد؛ می‌توان به دفاع مشروع سایبری دست یازید؛ البته در مسیر دفاع مشروع باید اصل تناسب به‌عنوان ضابطه اصلی رعایت گردیده و به‌محض ورود مؤثر شورای امنیت در بحران، دفاع خاتمه یابد.

کلید واژگان: دفاع مشروع، حملات سایبری، ایالات‌متحده آمریکا، پناهگاه امن، دفاع دیجیتالی، جنگ سایبری.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

مقدمه

با فراگیر شدن اینترنت، افراد و سازمان‌ها صرف‌نظر از مکانشان، به یکدیگر نزدیک‌تر شده‌اند. علی‌رغم مزایای آشکار این فضا که ما را قادر ساخته است رشد سریع اقتصاد جهان را شاهد باشیم، شاهد جنبه‌های تاریک اینترنت و پیامدهای منفی تأثیر اینترنت بر انسان نیز هستیم. در فضای موجود، جریان اطلاعات و ارتباطات محدود به مرزهای جغرافیایی و دولتی نیست و این وضعیت مملو از خطر سلب امنیت برای دولت و جامعه است. ظهور انواع جدید جرائم و ارتکاب جرائم سنتی به روش‌های جدید، نتیجه ورود گسترده فناوری اطلاعات به زندگی ماست. نیاز به مقررات قانونی در فضای مجازی واضح است، بااین‌حال، ماهیت فرامرزی، از راه دور و غیر شفاف بودن آن، مشکلات خاصی را ایجاد می‌نماید (Schmitt, 2017: 215). امروزه هر دولتی می‌تواند باانگیزه‌های مختلف و بدون در نظر گرفتن هنجارهای بین‌المللی، به انجام توسل به‌زور در فضای سایبری اقدام نماید و این خود به وجود آورنده اقدامات تلافی جویانه خواهد بود؛ حال مساله این است که این استفاده غیرقانونی از زور یا تهدید به آن نقض قوانین بین‌المللی محسوب می‌شود یا نه؟ به‌منظور ارائه تعریفی از توسل به‌زور در فضای سایبر باید جامعه بین‌المللی به اجماعی برسد که تاکنون حاصل نگردیده است. در معنای چنین فعالیت‌هایی در سایه‌روشن منشور سازمان ملل متحد به‌طور خاص بند ۴ ماده ۲، باید دید که گستره این مقرره در باب منع توسل به‌زور متوجه توسل به‌زور در فضای سایبر نیز می‌شود یا باید مقرره‌های دیگری را تدوین نمود. البته باید بیان نمود که توسل به‌زور علیه تمامیت ارضی یا استقلال سیاسی هر کشوری که به‌طورکلی مغایر ارزش‌ها و اهداف سازمان ملل باشد، ممنوع است.

نه‌تنها ممنوعیت استفاده از زور، بلکه تهدید به‌زور نیز قبلاً در قوانین بین‌المللی به‌طور قاطع ذکرشده است. در بند ۴ ماده ۲ منشور سازمان ملل متحد آمده است: «همه اعضا باید در روابط بین‌المللی خود از تهدید یا استفاده از زور علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر طریق دیگری که با اهداف سازمان ملل متحد مغایرت داشته باشد، خودداری کنند». این ماده یکی از اصول اساسی حقوق بین‌الملل را بیان می‌کند که در اعلامیه اصول حقوق بین‌الملل در مورد روابط دوستانه و همکاری بین دولت‌ها، مصوب مجمع عمومی سازمان ملل متحد در سال ۱۹۷۰، تصریح شده است. چندین نقطه مهم در این تعریف خودنمایی می‌کند که به‌عنوان‌مثال، این ممنوعیت در مورد روابط بین‌المللی دولت‌ها اعمال می‌شود. این امر عمدتاً به این امر مربوط می‌شود که در گذشته نظراتی وجود داشت که موضوعات استعمار و مبارزات آزادی‌بخش ملی متعلق به امور داخلی دولت است و ازنظر مفهومی مشمول این اصل نمی‌شود. امروز این جریان فکری منسوخ‌شده است و حتی در صورت اقدامات سرکوبگرانه علیه ملتی که حق تعیین سرنوشت خود را اعمال می‌کند، نقض اصل منع تهدید به‌زور یا توسل به‌زور خواهد بود. بااین‌حال، این ممنوعیت نه‌تنها بر اقداماتی باهدف تمامیت ارضی یا استقلال سیاسی کشورها متمرکز است، بلکه در مورد هر روش دیگری که با اهداف سازمان ملل متحد مذکور در ماده ۱ منشور ناسازگار است نیز اعمال می‌شود. توسل زور توسط هر کشوری علیه کشور دیگر از منظر اسناد بین‌المللی ازجمله منشور سازمان ملل محکوم است و تنها یک کشور زمانی می‌تواند از زور استفاده نماید که مورد تجاوز واقع‌شده باشد و در مقام دفاع از خود متوسل به‌زور شود (رضایی، میر عباسی و کمالی، ۱۳۹۸: ۱۱۹). پس به‌طورکلی تنها دو استثناء پذیرفته‌شده برای ممنوعیت توسل به‌زور وجود دارد که عبارت‌اند از: ۱. اقدامات انجام‌شده بر اساس قطعنامه شورای امنیت سازمان ملل متحد مطابق با فصل هفتم منشور سازمان ملل متحد ، ازجمله اقدامات مسلحانه انجام‌شده توسط سازمان‌های منطقه‌ای تحت به‌اصطلاح موافقت‌نامه‌های منطقه‌ای با مجوز یا موافقت شورای امنیت سازمان ملل؛ ۲. دفاع مشروع انفرادی یک دولت و دسته‌جمعی چندین دولت[1].

در همین راستا مساله اصلی که باید با توجه به موضوعات مذکور موردتوجه قرار بگیرد حق کشورها در استفاده از «دفاع مشروع» در مقابل حملات سایبری و چگونگی اعمال این حق احتمالی است؛ لذا مقاله حاضر با یاری جستن از روش توصیفی-تحلیلی به بررسی

[1] ماده ۵۱ منشور سازمان ملل متحد

دانشگاه آزاد اسلامی واحد مراغه

حق دفاع مشروع اعضا سازمان ملل متحد مصرح در ماده ۵۱ منشور در مقابل حمله سایبری مخرب کشورها (با تأکید بر حملات سایبری ایالات‌متحده امریکا) پرداخته و کم و کیف آن را تحلیل می‌نماید.

۱. توسل به‌زور[۲] در جنگ سایبری

بشر در طول گذران تاریخ خود مراحل مختلفی را طی نموده است و از بدو خلقت در این کره خاکی به دنبال ارتباط باهم نوع خود بوده است. عمر این ماجرا را می‌توان از روزی که بشر با شوق فراوان با ایماء و اشاره با همنوع خود ارتباط برقرار ساخت تا اختراع خط و... متصور شد. ولی در سده ۲۰ میلادی بشر با فراگیر شدن ارتباطات در بستری جدید، محیطی نو در مقابل خویشتن مشاهده کرد و برای اولین بار مساله‌ای به نام «فضای مجازی»[۳] برایش مطرح گردید (پور قهرمانی و صابر نژاد، ۱۳۹۴: ۲). که شاید تا آن زمان تصوّر کردن چنین چیزی برای آدمی محال بود. مساله‌ای که در این فضا ذهن بشری را به خود جلب کرد این بود که آیا قواعد سابق اجتماع، در این عرصه نیز می‌تواند مصداق داشته باشد یا نه؟ و در صورت امکان، هنجارهای آن به چه نحوی تبیین خواهد شد؟

درباره مفهوم توسل به‌زور که صراحتاً در بند ۴ ماده ۲ منشور ملل متحد منع گردیده است و کم و کیف آن نظر مشترکی در جامعه بین‌المللی وجود ندارد. از سویی کارایی منشور ایجاب می‌کند که بند ۴ ماده ۲ چنان در نظر گرفته شود که همه انواع تهدید به‌زور یا استفاده از آن را منع نماید، مگر در مواردی که خود منشور به‌صراحت اجازه کاربرد آن را داده باشد (مصفا، ۱۳۶۵: ۸۰) ولی به‌طورکلی و در مرحله عمل در تفسیر و تحلیل تحریم توسل به‌زور در منشور اختلاف‌نظرهایی وجود دارد، چراکه برخی آن موارد مجاز کاربرد زور را کاملاً استثنایی می‌دانند و عده‌ای دیگر موارد بیشتری را مجاز قلمداد می‌نمایند (حیدری، ۱۳۷۶: ۷۰).

در مواردی برخی از کشورها، معمولاً کشورهای درحال‌توسعه و در طول جنگ سرد اغلب کشورهای حامی بلوک شرق اصرار بر این داشتند که معنای توسل به‌زور، شامل فشارهایی از نوع سیاسی، اقتصادی و چنین تهدیدهایی علیه کشورها می‌گردد؛ بحث‌های مشابهی درباره‌ی تعریف توسل به‌زور در حملات نظامی در بند ۴ ماده ۲ و هم‌چنین در مفهوم دفاع مشروع در ماده‌ی ۵۱ وجود دارد؛ مجمع عمومی سازمان ملل متحد و ایالات‌متحده آمریکا در بحث تعریف «تجاوز»[۴] نیز چنین رویکردهایی داشته‌اند، آمریکا یک تعریف بسیار مضیقی از تجاوز که محدود به تجاوز نظامی می‌شود ارائه می‌دهد، درصورتی‌که کشورهای درحال‌توسعه یک تعریف موسعی ارائه داده و آن را حتی شامل فشارهای اقتصادی نیز می‌دانند. تاریخ جنگ سرد درباره تعارضات در مفهوم توسل به‌زور در بند ۴ ماده ۲، درباره رشد فنّاوری‌ها بر روی جنگ و تنظیم مقررات آن چند درس را به ما آموخت (waxman, 2011: 428-429). اول: توسعه دادن اثرات فنّاوری های جدید در مناقشات و پذیرش آن به‌صورت «اجماعی»[۵] از طرف اعضای جامعه بین‌المللی آهسته و دشوار خواهد بود؛ دوم: بعضی فنّاوری‌ها یا مدل‌های خاصی از آنان تعارضات و نکته ضعف‌های خاصی دارند که مانع حکمرانی قوانین سابق بر آن‌ها می‌گردد.

از سوی دیگر باید به خاطر داشت که یکی از ویژگی‌های مهم فضای سایبر که آن را از دنیای واقعی متمایز و با مشکلات اساسی روبرو نمی‌نماید، ناشناس بودن (ناپیدا بودن) کاربر است که مشکل شناسایی و محرمانگی از آن ناشی می‌شود. به‌عنوان‌مثال، تلاش برای منطقه‌بندی فضا بر اساس محدودیت سنی به دلیل اینکه در فضای مجازی، جداسازی بر اساس سن، جنسیت یا معیارهای دیگری که جداسازی آن در دنیای واقعی کاملاً آسان است، بسیار دشوار و پرهزینه است، شکست‌خورده و بنابراین اعمال هنجارهای حقوقی موجود در حل این مشکل بی‌تأثیر است[۶] و لذا در خصوص توسل به‌زور در این فضا شدیداً مشکل شناسایی متوسل به‌زور احساس خواهد شد.

با توجه به دلایل مطروحه، می‌توان به این نتیجه دست‌یافت که جنگ در این عرصه جدید ویژگی‌هایی دارد که به‌سختی می‌توان آن را در مقررات منشور ازجمله در بند ۴ ماده ۲ و ماده ۵۱ درباره دفاع مشروع گنجاند، اهم این تفاوت‌ها عبارت‌اند از این‌که تحت شمول قرار دادن حملات سایبری در زیرمجموعه این مقرره به دلایل فنی، حقوقی، سیاسی و استراتژیک مشکل خواهد بود؛ به خاطر این‌که این حملات به‌طور مشخص از نکته‌ای انجام می‌گیرند که به خاطر سرعت و بسترهای خاص ماهیت اطلاعات دیجیتال تشخیص آن بسیار

---

[۲] Use of force
[۳] Virtual space
[۴] Aggression
[۵] Consensus
[6] See: It's about the case Reno v. American Civil Liberties Union, 521US844(1997). https://supreme.justia.com/cases/federal/us/521/844/

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

سخت و دشوار است؛ که این می‌تواند زمینه تهدیدها و متهم کردن‌های نابجا را فراهم آورد.

از سوی دیگر حتی در صورت تشخیص، در یک حمله بین‌المللی از فضای سایبر، ممکن است بین اصول فیزیکی حاکم بر این فضا و حقوق بین‌الملل تعارضی پیش بیاید؛ به‌عنوان نمونه الکترون‌ها[۷] می‌توانند از یک مرز بین‌المللی در شبکه برای جنگ به کار گرفته شوند، درصورتی‌که حاکمیت یا یک عامل حکومتی در آن دخیل باشد. علاوه بر این در بحث بازدارندگی و دفاع مشروع نیز مشکلات خاصی در این فضا وجود دارد و به دلیل اینکه اگر شما نمی‌توانید مجرم را شناسایی کنید نمی‌توانید او را تهدید یا با او مقابله‌به‌مثل کنید و از سوی دیگر نمی‌توانید قانون را اعمال نمایید؛ چراکه سد راه شدن برای «قابلیت دسترسی»[۸] ناشناخته، خیلی دشوار است (waxman, 2011: 430). با همه این تعابیر به‌خوبی پیداست که نمی‌توان اعمال مقررات منشور بر این جنگ را مدعی شد، چراکه این جنگ ویژگی‌های خاص خود را دارد و توجه خاصی نیز می‌طلبد؛ درواقع ویژگی‌های خاصی در فضای سایبر و تحول به‌زور در آن مهم بوده و توجه خاصی را می‌طلبد و می‌توان چنین گفت که شاید همین ویژگی‌ها هستند که توسل به‌زور را در همین فضا مهم و قابل‌اعتنا می‌نمایند؛ که اهم این ویژگی‌ها چنین‌اند:

الف) تعدد بازیگران در فضای سایبری: هزینه کم فن‌آوری رایانه‌ای، اتصال گسترده به اینترنت و سهولت ایجاد یا به دست آوردن نرم‌افزارهای مخرب به این معناست که تقریباً هرکسی می‌تواند به این فضا وارد شود. این بازیگران شامل افراد، گروه‌های سازمان‌یافته جنایی، گروه‌های تروریستی، شرکت‌های خصوصی و دولت–کشور هستند (Charney, 2009: 6).

ب) هزینه کم ورود، صرف زمان کم و سرعت‌بالای اقدام: هر فرد برای انجام حمله سایبری تنها به یک رایانه، یک ارتباط اینترنتی و دانش فنی محدود درزمینه فضای سایبری نیاز دارد؛ درنتیجه، فضای سایبری شرایطی را فراهم کرده است که با هزینه پایین می‌توان اقدامات خطرناکی را در مدت‌زمان کم و با سرعت بالایی انجام داد؛ البته، انجام حملات پیچیده‌تر سایبری نیازمند صرف هزینه‌های بالاتری است (Lord and Sharp, 2011: 20).

پ) ناشناس ماندن بازیگران و عدم قابلیت ردیابی: اینترنت به‌عنوان سیستم نامتمرکز طراحی‌شده و کاربران آن، غالباً شناخته‌شده نیستند؛ همین ناشناختگی باعث می‌شود هیچ اثری از برخی از حمله‌های سایبری باقی نماند. افراد فعال در عرصه اینترنت می‌توانند از اقصی نقاط دنیا، بدون هشدار و در عرض چند ثانیه و بدون آنکه اثر یا نامی از خود بر جای بگذارند، اهداف دیجیتالی را مورد هدف قرار دهند (Lord and Sharp, 2011: 22).

ت) حجم شگرف تأثیرگذاری: ماهیت خاص فضای سایبری شرایطی را به وجود آورده است که بروز هر اختلال یا وقفه می‌تواند تأثیرات و پیامدهای به‌مراتب بیشتری از حادثه اولیه در پی داشته باشد. وقوع حمله‌های سایبری و درنتیجه آن، بروز اختلال در شبکه‌ها می تواند موجب ایجاد خسارت به اموال، زمان، محصولات و تولیدات، اعتبار، اطلاعات حساس و حتی از دست دادن جان انسان‌ها شود، زیرا در این‌گونه مواقع، زیرساخت‌ها و سامانه‌های مهم دچار آسیب می‌شوند (Lord and Sharp, 2011: 24).

ث) کمرنگ شدن نقش جغرافیا: فضای سایبری سرعت انتقال به سراسر جهان را در لحظه کوتاهی فراهم کرده است. بنابراین، تهدیدکنندگان قادر به فراتر رفتن از محدوده جغرافیایی خود و رسیدن به اهداف کلیدی‌شان هستند.

ج) ساختار فضای اینترنت: اینترنت، دامنه مشترک و یکپارچه است. استفاده از این فضا توسط شهروندان، شرکت‌ها و دولت‌ها به شیوه‌ای است که جداسازی آن‌ها بسیار دشوار است. توانایی محدود برای جدا کردن بازیگران و فعالیت‌های آن‌ها، پاسخ مناسب به تهدید را دشوارتر کرده است؛ از سوی دیگر، ساختار اینترنت، دولت‌ها و شرکت‌های خصوصی را با عدم اطمینان در قبال خطرات فضای اینترنتی مواجه کرده است. این عدم قطعیت ناشی از پیچیدگی این فضا است (Haller and Other, 2010: 4).

چ) پیچیدگی در مجازات اعمال مجرمانه در فضای سایبر: احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری پایین است. درنتیجه، افراد و سازمان‌ها نیز این فضا را در مقایسه با گزینه‌های جایگزین غیر سایبری مطمئن‌تر و دارای خطرات کمتری می‌بینند (Lord and Sharp, 2011: 25).

با تحقیق در ویژگی‌هایی که مختص توسل به‌زور در این فضا است که شرح آن گذشت بی‌شک توسل به‌زور در این فضا به علت

[۷] Electrons

[۸] Accountable

سهولت و دیگر عوامل توضیح داده‌شده، در میان دولت‌ها جلوه‌ی خاصی به خود خواهد گرفت و همین مسائل است که ضرورت توجهی درخور و زیرساختی به این مساله را ناگزیر می‌نماید؛ چراکه اگر توسل به‌زور در این فضا مورد بی‌مهری قرار بگیرد و حدودوثغور آن مشخص نشود، بالطبع استثنائات عدم توسل به‌زور ازجمله دفاع مشروع[۹] موردتوجه نبوده و زمینه‌ساز ناهنجاری‌هایی خواهد بود که کل جهان را غرق در ناامنی خواهد نمود.

ح) تهدیدات سایبری و آستانه شروع جنگ در آن: ماهیت فراگیر و گستره جهانی فضای سایبر، زمینه‌ای برای ایجاد تهدیدات سایبری در ابعاد سیاسی، اقتصادی، اجتماعی، فرهنگی، زیست‌محیطی و دفاعی–نظامی فراهم نموده است. تهدیدات سایبری در حوزه نظامی و دفاعی برخلاف سایر ابعاد آن، رویکردی سخت و چهره‌ای خشن دارد. بسیاری از این تهدیدات، به خاطر محدودیت‌های بین‌المللی به‌صورت بالقوه وجود دارد و تنها جنبه بازدارندگی دارد. در صورت افزایش تنش و تخاصم میان کشورها این تهدیدات به مرحله عملیاتی و جنگ منجر می‌شود. در یک دسته‌بندی کلی ویژگی‌های تهدیدات سایبری را می‌توان شامل موارد زیر در نظر گرفت (هلیلی، ۱۴۰۰: ۱۱۲).

الف) منشأ تهدید: مزدوران سایبری یا گروه‌های تحت حمایت پنهان دولت‌ها، دولت‌های متخاصم، تروریست‌های سایبری، جاسوسان سایبری، مجرمین سازمان‌یافته سایبری، هکرهای دارای انگیزه سیاسی

ب) پیامد تهدید: مخاطره سایبری (احتمال بهره‌برداری یک تهدید سایبری، از آسیب‌پذیری سایبری موجود در یک سرمایه سایبری) و تهاجم سایبری (اقدام عملی تهدید برای بهره‌برداری از آسیب‌پذیری سایبری)

پ) سطح تهدید: زیرساختی، سازمانی، ملی و فراملی

ت) احتمال وقوع تهدید: احتمال بهره‌برداری تهدید از آسیب‌پذیری ایجاد مخاطره سایبری شامل: خیلی کم (مخاطره سایبری غیرمحتمل)، کم (مخاطره سایبری غیرمحتمل)، متوسط (مخاطره سایبری ممکن) و زیاد (مخاطره سایبری محتمل)

ث) شدت تهدید: شدت خیلی کم (تهدید منجر به خسارات محدود و قابل‌کنترل)، کم (تهدید سایبری حادثه‌آفرین)، متوسط (تهدید منجر به حادثه امنیتی)، شدت زیاد (بحران و خسارات گسترده سایبری مانند اختلال در شبکه بانکی)، خیلی زیاد (تهدیدات فاجعه‌بار مانند ازکارافتادن شبکه برق سرتاسری)

با تدقیق در همین خصوصیات تهدیدها می‌توان بیان داشت که آستانه شروع جنگ در این فضا نیز هدف‌گیری زیرساخت‌های حیاتی و حساس مانند اهداف نظامی، خدمات اجتماعی، سامانه‌های حمل‌ونقل، انرژی، مخابرات و... است؛ که به شبکه‌های رایانه‌ای دشمن نفوذ کرده و موجب تخریب، اختلال و یا عدم‌کارآیی آن‌ها می‌شود.[۱۰]

در همین راستا است که می‌توان بیان داشت نبرد مجازی یا جنگ سایبری به‌نوعی از نبرد اطلاق می‌گردد که طرفین در آن از رایانه و شبکه‌های رایانه‌ای (به‌خصوص شبکه اینترنت) به‌عنوان ابزار استفاده کرده و نبرد را در فضای مجازی جاری می‌سازند. درواقع جنگ سایبری بر اساس قوانین حاکم بر اطلاعات و از طریق دنیای اطلاعات صورت می‌گیرد.

۲. حملات سایبری ایالات‌متحده آمریکا و دفاع مشروع در مقابل آن

استراتژی نظامی ملی ایالات‌متحده آمریکا در خصوص عملیات فضای سایبری، عبارت است از استفاده منسجم از توانمندی‌های جنگ الکترونیکی، عملیات شبکه‌ای رایانه‌ای، عملیات روانی، حیله‌های نظامی و عملیات هماهنگ باقابلیت‌های پشتیبانی که به‌منظور تأثیرگذاری، متوقف کردن، تخریب یا سرقت اطلاعات طرف مقابل و درعین‌حال پشتیبانی از فرایندهای تصمیم‌گیری نهادهای ملی صورت می‌گیرد؛ هدف همه عملیات‌های سایبری، ایجاد اختلال، ممانعت، تنزل دادن یا تخریب اطلاعات موجود در رایانه‌ها و شبکه‌های رایانه‌ای است (Roscini, 2014: 13). نکته‌ی قابل‌توجه در مورد حملات سایبری کشورها آن است که این حملات و در مفهوم عام‌تر جنگ

---

[۹] Legitimate Defence (Self Defence)

[۱۰] در همین راستا است که می‌توان بیان داشت نبرد مجازی یا جنگ سایبری به نوعی از نبرد اطلاق می‌گردد که طرفین در آن از رایانه و شبکه‌های رایانه‌ای (به‌خصوص شبکه اینترنت) به‌عنوان ابزار استفاده کرده و نبرد را در فضای مجازی جاری می‌سازند. درواقع جنگ سایبری بر اساس قوانین حاکم بر اطلاعات و از طریق دنیای اطلاعات صورت می‌گیرد (جیستان و جیستان، ۱۳۹۳:ص۴).

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

سایبری[۱۱] شکل کاملاً جدیدی از رزم است که بازتاب آن را هنوز به‌طور کامل نتوانسته‌ایم درک کنیم (Clark, 2009: 32). اما درباره این موضوع، آنچه به ذهن متبادر می‌گردد این است که به نظر می‌رسد این نوع جنگ با اشکال سابق جنگ تفاوت چندانی ندارد و فضای سایبر را نیز به عرصه‌های سنتی‌تر افزوده است ولی با این تعریف آنچه از چشم پنهان می‌ماند پس‌زمینه جاری حمله سایبری به‌عنوان بخشی از برنامه‌ای کل‌نگر و هماهنگ برای دستیابی به اهداف سیاسی، اقتصادی و اجتماعی کشورهاست (Michael, 2013:1). که در حملات سایبری ایالات‌متحده به‌وفور مشاهده می‌گردد. باوجوداین باید به این نکته توجه کرد که برخلاف دیپلماسی نیروی نظامی و جنگ اقتصادی در این عرصه، موضوع اصلی مساله کشورها و وجود آن‌ها برای تخاصم بین‌المللی به چالش کشیده می‌شود. درواقع فضای سایبر این امکان را برای سوژه‌های[۱۲] غیردولتی نظام بین‌المللی، سازمان‌های تجاری و حتی افراد فراهم می‌کند که وسایل و انگیزه برای فعالیت جنگ‌طلبانه را کسب کنند (Conrnish, 2010: 32). و همین مساله موجب شده است که در سطح بین‌المللی نیز جهان شاهد چندین حمله سایبری باشیم؛ که برخی از مهم‌ترین آن‌ها به دولت ایالات‌متحده منتسب است.[۱۳]

اگرچه آمریکا به‌عنوان توسعه‌دهنده اصلی فضای سایبری، کشوری پیشرو در این عرصه تلقی می‌شود. توسعه همه‌جانبه اینترنت و وابستگی بیش‌ازحد زیرساخت‌های حساس امریکا به فناوری اطلاعات آن را در معرض انواع تهدیدات سایبری قرار داده است. شبکه بانکی و مالی تا خدمات عمومی، شبکه‌های مدنی و نظامی همگی به شبکه وابسته بوده در صورت اختلال سایبری همگی آن‌ها از کار می‌افتند (صانعیان، ۱۳۹۸: ۱۹۱). لذا تشکیل تأسیساتی در مقابله با این خطرات بهانه‌ی خوبی بوده است که این کشور ارتش سایبری مقتدری فراهم آورد که اکثر حملات سایبری علیه کشورهایی را که هم‌مسلک سیاسی آن نیستند را راهبری نماید[۱۴]؛ ولی نکته‌ای که شایان

---

۱۱ Cyber war

۱۲ Subjects

۱۳ مهم‌ترین این حملات به‌قرار ذیل می‌باشند:

۱. دهه ۸۰ میلادی حمله آمریکا به زیرساخت‌های نظامی کره شمالی که به ایالات‌متحده آمریکا منتسب شده است.

۲. سال ۱۹۹۹ حمله آمریکا به تأسیسات حیاتی یوگسلاوی هم‌زمان با بمباران یوگسلاوی توسط ناتو

۳. سال ۱۹۹۹ حمله آمریکا به شبکه‌های رایانه‌ای صرب

۴. سال ۲۰۰۱ حمله آمریکا به تأسیسات و زیرساخت‌های دولتی چین

۵. سال ۲۰۰۱ حمله آمریکا به روسیه

۶. سال ۲۰۱۰ حمله ویروس «استاکس نت» به تأسیسات نطنز (مرکز پدافند غیرعامل فاوا، ۱۳۸۸: ۵۵)

۷. «عملیات ابابیل» (Ababil Operation) که در سال ۲۰۱۲ انجام شد و مؤسسات مالی مختلف آمریکایی را هدف قرار داد و توسط گروهی که خود را جنگجویان سایبری «عزالدین القسام» می‌نامید، انجام شد.

۸. حملات سایبری ۲۰۱۳ سنگاپور در پاسخ به مقررات سانسور وب در کشور سنگاپور که ادعای دست داشتن ایالات‌متحده آمریکا در آن مطرح شده است.

۹. حمله سایبری ۲۰۱۳ کره جنوبی که به عناصری در داخل کره شمالی نسبت داده می‌شود.

۱۰. هک شبکه برق اوکراین در سال ۲۰۱۵ که به یک گروه تهدید دائمی پیشرفته روسی معروف به «کرم شنی» (Sandworm) نسبت داده می‌شود.

۱۱. حمله سایبری ۲۰۱۶ کیف، که باعث قطع برق گسترده شد.

۱۲. حملات سایبری کمیته ملی دموکرات، علیه کمیته ملی دموکرات توسط گروه‌های جاسوسی سایبری تحت حمایت روسیه، احتمالاً برای کمک به کمپین ریاست جمهوری ۲۰۱۶ دونالد ترامپ (Washington Post. Retrieved, 2019: 04-01).

۱۳. حملات سایبری به اکراین در ۲۷ ژوئن ۲۰۱۷ که وب‌سایت‌های سازمان‌های اوکراینی ازجمله بانک‌ها، وزارتخانه‌ها، روزنامه‌ها و شرکت‌های برق را تحت تأثیر قرارداد.

۱۴. حملات سایبری ۲۰۱۹،۲۰۲۰ و ۲۰۲۱ که به ۱۰ وب‌سایت ملی این کشور حمله شده بود و منشأ آن ناشناخته باقی ماند.

۱۵. حملات سایبری ۲۰۲۲ اوکراین، که در آستانه حمله نظامی روسیه به اوکراین انجام شد و بی‌تردید منتسب به روسیه است (Howcroft, 2022).

۱۶. حمله پهپادی سال ۲۰۲۳ به تأسیسات نظامی اصفهان که با ابزار سایبری بوده و به اسرائیل منتسب است ر.ک:
https://ir.voanews.com/a/international-media-reports-on-crackdown-of-protesters-and-artists-and-the-impact-of-israeli-drone-attack-on-isfahan/6946797.html

۱۴ لذا مرکز «فرماندهی سایبری ایالات‌متحده یا واحد فرماندهی امنیت سایبری ایالات‌متحده» یکی از یازده واحد فرماندهی وزارت دفاع ایالات‌متحده است. فرماندهی سایبری در اواسط سال ۲۰۰۹ در دفتر مرکزی آژانس امنیت ملی در «فورت جورج جی. مید» مریلند تشکیل شد. این واحد با شبکه آژانس امنیت ملی همکاری می‌کند

توجه است اینکه آیا در مقابل این حملات می‌توان به دفاع مشروع مصرح در ماده‌ی ۵۱ منشور سازمان ملل دست یازید یا خیر؟ به نظر می‌رسد پاسخ به این سؤال نیازمند تدقیق در دو مفهوم ویژگی‌های حملاتی که می‌تواند مستوجب دفاع مشروع باشد و از سوی دیگر شرایط تحقق همین دفاع مشروع مستتر باشد که در ادامه خواهد آمد.

۱،۲. ویژگی حملات سایبری مستوجب دفاع مشروع

پیشرفت فناوری موجب مواجهه روزافزون دولت‌ها با حملات سایبری شده است. بیشترین حملات سایبری که دولت‌ها با آن مواجه‌اند، از نوع حملات سایبری نفی یا محروم‌سازی از سرویس توزیع شده اینترنتی است. این‌گونه حملات آثار مخرب مستقیم و آنی ندارند، به همین دلیل ارزیابی آن‌ها در قالب ممنوعیت توسل به‌زور و حملات مسلحانه قرار نمی‌گیرد و معمولاً دولت‌ها نیز با توجه به‌شدت کمتر آن‌ها در برخی موارد حتی از پیگیری و شناسایی عاملان حملات صرف‌نظر می‌کنند. بااینکه قواعد مستقیم و صریحی در مورد حملات سایبری و نظم بخشیدن به آن‌ها وجود ندارد، نظر به تبعات چنین حملاتی حتی با شدت کم و اقتضای ارزیابی حقوقی این حملات، با بررسی مقررات فعلی حقوق بین‌الملل به این نتیجه می‌رسیم که بعضی ازاین‌گونه حملات غیر مخرب را می‌توان با اصل ممنوعیت مداخله به نظم درآورد و در صورت احراز عاملان و انتساب آن حملات به دولت، مسئولیت بین‌المللی دولت‌ها را در مراجع بین‌المللی مطرح کرد (اسمعیل زاده ملاباشی و عبدالهی، ۱۳۹۹: ۷۱۱) وجود برخی از ویژگی‌ها در حملات سایبری می‌تواند آن را تبدیل به حملاتی نماید که درنهایت بتوان در مقابل آن به دفاع مشروع تأسی جست. اصولاً اقدام مداخله آمیز غیرمجاز سایبری شامل دو عنصر است: «۱. عنصر تداخل با امور داخلی یا خارجی دولت هدف؛ ۲. قهری بودن عملیات سایبری حادث (Tallinn Manual 2.0, 2017: 314)».

در رأی مربوط به قضیه نیکاراگوئه–ایالات متحده آمریکا، دیوان بین‌المللی دادگستری، زمانی که ابراز داشت مداخله ممنوعه باید مداخله‌ای باشد که مقولاتی که وفق اصل حاکمیت، هر دولتی در اتخاذ تصمیم راجع به آن‌ها آزاد است را تحت‌الشعاع قرار می‌دهد (Nicaragua judgment, Para 205). تأکید کرد که مداخله، بر حوزه اختصاصی یک دولت تأثیر می‌گذارد؛ به‌طور خاص، چنین مقولاتی، شامل انتخاب نظام سیاسی، اقتصادی، اجتماعی و فرهنگی و صورت‌بندی سیاست خارجی، می‌گردند (Nicaragua judgment, Para 205). مطابق اعلامیه مربوط به روابط دوستانه، سازمان‌دهی، تحریک، مساعدت، تأمین مالی یا مشارکت در آشوب داخلی یا تروریسم در دولت دیگر یا پذیرش بی‌قیدوشرط فعالیت‌های سازمان‌یافته در قلمرو خود که برای ارتکاب چنین اقداماتی ترتیب داده شده‌اند، در شمار مصادیق مداخله هستند (Declaration on Friendly Relations, Para. 1-3). در این راستا، نیازی نیست که مداخله چه به‌صورت طبیعی یا سایبری در حوزه داخلی یک دولت، علیه زیرساخت دولتی هدایت شده باشد یا فعالیت‌های دولتی را شامل شود، بلکه، کلید تحقق عنصر ابتدایی مداخله که می‌تواند دفاع مشروع را در پی داشته باشد، این است که عمل موردنظر می‌بایست به‌منظور تضعیف اقتدار دولت بر حوزه اختصاصی خود طراحی شده باشد (Tallinn Manual 2.0, 2017: 315-316). و به تعبیری بهتر بتواند حاکمیت را نقض کرده و به‌عنوان «توسل به‌زور غیرقانونی» جلوه‌گری نماید.

اشاره دیوان بین‌المللی دادگستری به «تصمیم‌گیری آزادانه» در رأی قضیه نیکاراگوئه، ما را به این مطلب هدایت می‌کند که عملیات‌های سایبری معین استفاده شده جهت وادار ساختن دولتی دیگر برای پایبندی به تعهدات حقوقی بین‌المللی خویش، از دامنه اعمال این قاعده حذف می‌شوند و نمی‌توان در مقابل آن به دفاع مشروع مصرح در ماده ۵۱ منشور دست یازید. این امر به این خاطر است که متعهد بودن یک دولت در قبال دولت دیگر، دست‌کم در قبال دولت دوم، موضوع را از دایره حوزه اختصاصی، خارج می‌سازد. درواقع، حقوق بین‌الملل

و از زمان تشکیل این نیرو به‌طور هم‌زمان ریاست آن با مدیر آژانس امنیت ملی بوده است. اگرچه در ابتدا یک واحد با مأموریت دفاعی در ذهن ایجاد شده، اما به‌طور فزاینده‌ای به‌عنوان یک نیروی تهاجمی موردتوجه قرارگرفته است و حتی در مرحله عمل در ۱۸ آگوست ۲۰۱۷ اعلام شده است که به یک فرماندهی جنگی متحد کامل و مستقل ارتقا می‌یابد و این موضوع در ۴ می ۲۰۱۸ انجام‌یافته است. ر.ک.:

https://dod.defense.gov/page-not-found?original_path=/News/Special-Reports/0415_Cyber-Strategy

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

اقدامات متفاوتی، نظیر دفاع مشروع، یا اقدامات متقابل را که برای قادر ساختن یک دولت به مجبور کردن دولت دیگر جهت محترم شمردن تعهدات حقوقی بین‌المللی خویش طراحی شده‌اند، مجاز می‌شمارد (Tallinn Manual 2.0, 2017: 317).

۲،۲. ظرفیت‌های اجرایی ماده ۵۱ منشور سازمان ملل متحد در مقابله با حملات سایبری

در چارچوب سنتی حقوق بین‌الملل، در مورد دفاع مشروع اختلافات قابل‌توجهی بین دولت‌ها و دکترین وجود دارد (Gray, 2018: 126). بااین‌حال، همه کشورها موافق‌اند که در صورت وقوع حمله مسلحانه، حق دفاع از خود طبق ماده ۵۱ منشور ملل متحد به وجود می‌آید. بااین‌حال، در مورد اینکه چه چیزی یک حمله مسلحانه به معنای مستتر در منشور سازمان ملل متحد است، اختلاف‌نظر وجود دارد. به‌طور سنتی، یک حمله مسلحانه مستلزم تلفات جانی و یا تخریب گسترده اموال صرف‌نظر از ابزار مورداستفاده است (Woltag, 2014: 214).

اگرچه مورد متعارف یک حمله مسلحانه، تهاجم نیروهای مسلح سازمان‌دهی شده یک دولت به قلمرو دولت دیگر است، اما تحولات اخیر ویژگی ترکیبی یا نامتقارن فزاینده‌ای از جنگ و درگیری را نشان می‌دهد (Schrof & et al, 2009:102). که این تضادهای ترکیبی معمولاً شامل انواع بازیگران دولتی و غیردولتی و نیز تاکتیک‌های مختلف می‌شود (Schroefl & Kaufman, 2014: 421). از منظر حقوق بین‌الملل تحولات مربوط به پیامدهای حملات ۱۱ سپتامبر، بحث اساسی را در مورد اینکه آیا الزامات دفاع از خود را می‌توان با حملات بازیگران غیردولتی برآورده کرد، مطرح نمود. برخی از دولت‌ها تمایل دارند که ازنظر کیفی دامنه دفاع مشروع را به روش‌های رادیکال در این زمینه گسترش دهند (Anand, 2009: 114). این تحولات با توجه به امکانات فنی جدید حملات سایبری، وزن ویژه‌ای پیداکرده؛ چراکه هر وقت پیامدهای پشتیبانی حیاتی کنترل‌شده توسط رایانه از طریق یک حمله سایبری باعث تلفات مقدار قابل‌توجهی از حملات می‌شود، به‌طور خطرناکی به محدوده ماده ۵۱ منشور ملل متحد نزدیک می‌شویم. اهمیت این بحث زمانی که به دلیل ناشناس بودن گسترده در فضای مجازی، ساختارهای گروهی مشکوک و گریزان در درگیری‌ها مطرح می‌شود، بیشتر جلوه‌گری می‌نماید و درنتیجه، این سؤال که آیا الزامات قانونی برای دفاع از خود را می‌توان با حملات بازیگران غیردولتی برآورده کرد، درزمینه سایبری نیز به‌صراحت موردبحث قرار می‌گیرد. گسترش حق دفاع مشروع با درج رفتار بازیگران خصوصی می‌تواند در قلمرو سایبری منجر به حملات سایبری توسط هکرهای فردی شود که با ابزار نظامی پاسخ داده می‌شود و ممکن است آزادی عمل مشکل‌ساز برای دفاع مشروع را ایجاد نماید. علاوه بر این، حتی یک‌رویه دولتی پذیرفته‌شده و تصمیمات سیاسی دولت‌های قدرتمند نیز نمی‌تواند تحلیل حقوقی اقدامات انجام‌شده را دور بزند.

تحولات ذکرشده نشان می‌دهد که نه‌تنها ویژگی‌های خاص حملات سایبری، بلکه پراکنده شدن نظرات در مورد محدوده مشخص ماده ۵۱ منشور ملل متحد، سؤال‌های مهمی در مورد کاربرد مفهوم حمله مسلحانه سایبری را ایجاد می‌نماید؛ ازاین‌رو جای تعجب نیست که زمینه سایبری موضوع مورد مناقشه را پیچیده‌تر می‌کند. بر این اساس، قانون دفاع مشروع یکی از موضوعات موردبحث درزمینه حملات سایبری است (Rosciini, 2014: 14). به‌طورکلی، کاربرد حق دفاع مشروع در برابر حملات سایبری چندین بار به‌طور ضمنی و صریح تأیید شده است. حتی برخی از کشورها به‌صراحت حق دفاع از خود را در صورت حملات سایبری حفظ می‌کنند. اگرچه به‌طور گسترده‌ای شکی نیست که حملات سایبری دارای پتانسیل واجد شرایط بودن به‌عنوان یک حمله مسلحانه بر اساس منشور هستند، زیرا ممکن است پیامدهای فاجعه‌بار و مخربی در دنیای واقعی داشته باشند. تاکنون، هیچ دولتی رسماً یک حمله سایبری را اعلام نکرده است که طبق ماده ۵۱ منشور سازمان ملل متحد به‌عنوان یک حمله مسلحانه شناخته شود، دولت‌ها هنوز رویه دقیق دولتی یا اجماع در مورد قوانین این حوزه را ایجاد نکرده‌اند. با توجه به بحث مقررات بین‌المللی جاری و ماهیت ناشناس فضای سایبری، به نظر می‌رسد طرح این سؤال که در صورت وجود چه درجه‌ای از دخالت دولت برای انجام یک حمله مسلحانه ضروری است و شدت پیامدهای آن به چه میزان موردنیاز است که اجتناب‌ناپذیر می‌نماید؛ که در ادامه تحلیل می‌گردد.

۱،۲،۲. معیار شدت و اهمیت

اکثر کشورها تصریح می‌کنند که حملات سایبری باید به آستانه حمله مسلحانه با همان مقیاس و اثر قابل‌مقایسه با حملات سنتی که به سطح موردنیاز افزایش می‌یابد؛ برسند (Tallinn-Manual 2.0, 2017: 323). ازاین‌رو، این‌که آیا یک عملیات سایبری یک حمله مسلحانه را تشکیل می‌دهد، به‌شدت نتایج و پیامدهای آن بستگی دارد.

رویکرد «مقیاس و آثار» که ازلحاظ تاریخی توسط دیوان بین‌المللی دادگستری در پرونده نیکاراگوئه در سال ۱۹۸۶ تأسیس شده است، بر روی مقیاس یا به‌عبارت‌دیگر شدت تأثیرات یک حمله متمرکز است. البته از کلمه خاص «مسلح»[۱۵] در ماده ۵۱ منشور مشخص است که همه اقدامات واجد شرایط به‌عنوان نیروی مذکور در ماده ۲(۴) منشور، ممکن است یک حمله مسلحانه تلقی گردد. دامنه ماده ۵۱ منشور در مقایسه با نیروی مسلح طبق ماده ۲ (۴) منشور بسیار مضیق بوده و نیاز به خسارت جسمی یا صدمات در سطح جدی‌تر دارد. بر این اساس، یک دولت توانایی واکنش خودکار به‌اجبار و تهدید نظامی را ندارد و واکنش نظامی به‌شدت محدود به کنش حمله مسلحانه است (Dinstein, 2017: 216). که این موضوع دقیقاً باید در فضای سایبر و حملات سایبری مصداق یابد.

۲،۲،۲. معیار انتساب حقوقی

اگرچه سناریوهایی مانند حملات سایبری که زیرساخت‌های مهم را هدف قرار می‌دهد منجر به عواقب ویرانگر در دنیای فیزیکی یا تعداد قابل‌توجهی از مرگ‌ومیر می‌گردد؛ الزامات بیشتر حمله مسلحانه که اغلب موردتوجه کمتری قرار می‌گیرد مانند میزان موردنیاز درگیری دولت، نیز باید در نظر گرفته شود. همچنین مواردی همچون مشارکت افراد و سازمان‌های غیردولتی در فحوای ماده ۵۱ منشور که در مخاصمات معمولی موردتردید است؛ اصلاً در جنگ‌های سایبری قابلیت طرح نخواهد داشت (Ramírez, 2017: 324). به‌طور سنتی، یک حمله مسلحانه طبق ماده ۵۱ منشور سازمان ملل متحد جانب یک دولت به قلمرو دولتی دیگر آغاز شود؛ که این موضوع ناشی از ماهیت حقوق بین‌الملل است که در درجه اول روابط بین کشورها را به‌عنوان تابعان اصلی حقوق بین‌الملل تنظیم می‌نماید. در اصل، دفاع مشروع نیز درزمینه کشورها وارد منشور شده است و ارتباطی به تابعان دیگر ندارد. بااین‌حال چهره تغییریافته مخاصمات و بازیگری تابعان دیگر در این زمینه به‌طور ویژه در مخاصمات داخلی، توجه دکترین حقوق بین‌المللی را به‌حق دفاع مشروع در این موارد جلب می‌نماید؛ البته، اگر حملات سایبری توسط افراد خصوصی، گروه‌ها یا بازیگران غیردولتی دیگر به‌وسیله نظامی پاسخ داده شود، این حملات نه‌تنها ازنظر فنی بلکه به‌طور قانونی به یک کشور نسبت داده می‌شود. اگر حمله بازیگران غیردولتی با توجه به ماده ۵۱ منشور به یک کشور نسبت داده شود؛ مطابق دکترین «پناهگاه امن»[۱۶] که البته تئوری توسعه‌یافته‌ای نیست و موردبحث است (O'Connell, 2019: 512). یک کشور ممکن است مسئول بازیگران غیردولتی باشد که در صورت عدم تمایل یا عدم امکان جلوگیری از انجام این بازیگران در برابر دولت قربانی، حملات فرامرزی از قلمرو آن آغازشده است (Tibori, 2016: 98). ناگفته پیداست که این تئوری به خاطر تفسیر موسع استثنای اصل توسل به‌زور مستقر در ماده ۵۱ منشور ملل متحد شدیداً موردانتقاد است. علیرغم ابهام دکترین مذکور، به‌منظور فرض مشارکت قانونی، برای شروع کار باید شواهد فنی دیگری وجود داشته باشد و در ارتباط با فضای سایبر این واقعیت مصداق بیشتری دارد؛ چراکه حملات سایبری بسیار متفاوت است و حتی اگر بتوان قلمرویی برای انجام این حملات شناسایی نمود، باز این بحث مطرح خواهد بود که آیا این حملات توسط یک دولت کشور انجام پذیرفته است یا نه.

از سوی دیگر حملات سایبری به‌طور هم‌زمان از چندین سرزمین دولتی بیرون می‌آیند؛ چراکه می‌تواند در مسیر تداوم مخاصمه‌ای، از چندین «آی پی»[۱۷] مختلف انجام پذیرد (Friedman, 2014: 695). در این حالت اغلب هویت شخص ناشناس باقی می‌ماند و حتی اگر

---

[۱۵] Armed

[۱۶] Safe-haven

[17] Internet Protocol(IP)

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

در فرض غیرمحتمل‌تر هویت او آشکار گردد قابلیت انتساب عمل به دولت خاص غیرقابل اثبات به نظر می‌رسد (Schulze, 2015: 218). علاوه بر این، ازآنجاکه بدافزار نه‌تنها ممکن است سیستم هدف را به‌خودی‌خود آلوده کند بلکه ممکن است در سایر رایانه‌ها نیز در سراسر جهان گسترش یابد و وضعیت پیچیده‌تری را ترسیم نماید. در جمع‌بندی این مبحث می‌توان عنوان داشت ازآنجایی‌که موضوع دفاع از خود در برابر بازیگران خصوصی و غیردولتی در مخاصمات سنتی ازنظر قانونی بحث‌برانگیز است، مطمئناً توسعه آن به حملات سایبری به‌طریق‌اولی مبهم و یا حتی غیرممکن خواهد بود؛ ولی در فرضی که این حملات توسط دولت انجام‌گرفته و اثبات گردد اعمال ماده ۵۱ منشور ملل متحد در خصوص دفاع مشروع در این زمینه متصور است.

نتیجه‌گیری

حملات سایبری افسارگسیخته در جامعه بین‌المللی به‌عنوان چالشی اساسی برای حقوق بین‌الملل جلوه‌گری می‌نماید. با وضعیت فعلی حاکم بر جامعه جهانی، بی‌تردید برخی از حملات سایبری ایالات‌متحده علیه کشورهای دیگر مصداق بارز نقض اصل عدم‌مداخله است و در قاعده ۶۶ راهنمای دوم تالین[۱۸] موضوع عدم‌مداخله مدنظر قرارگرفته و ویژگی‌ها و عناصر یک مداخله و انواع مداخله با استفاده از ابزار سایبری را برشمرده شده است. بر این اساس، استفاده یک دولت از ابزارها و عملیات‌های سایبری به‌منظور تغییر آراء الکترونیکی از راه دور و دست بردن در انتخابات از طریق آن، مداخله محسوب می‌شود؛ این حملات اکثراً علاوه بر اجبار عناصری شبیه آموزش، تسلیح و تجهیز برخی نیروهای معاند داخلی را دارد که در این خصوص در فضای حقیقی در قضیه نیکاراگوئه در خصوص مداخله غیرمجاز مورد تأیید دیوان بین‌المللی دادگستری بوده است.

از سویی دیگر چالش اعمال ماده ۵۱ منشور ملل متحد درزمینه مخاصمات سایبری وجود دارد و در این زمینه باید تمام جنبه‌های حمله مذکور و چگونگی انتساب به دولت خاطی سنجیده شود. خطر ذاتی که در این فضا برای انتساب حملات به یک دولت و درنهایت پیش کشیدن بحث دفاع مشروع وجود دارد موضوع ردیابی فنی به‌موقع برای شناسایی مبدأ حمله است؛ که با توجه به امکان استفاده از «آی پی» های گوناگون و خارج از قلمرو کشور صاحب آن بسیار چالش‌برانگیز می‌نماید.

اگرچه درزمینه اعمال ماده ۵۱ منشور ملل متحد در خصوص حملات سایبری سند بین‌المللی خاصی مشاهده نمی‌گردد ولی دکترین حقوق بین‌الملل همان‌گونه که مخاصمات را به چالش‌های اقتصادی ازجمله تحریم‌های یک‌جانبه‌ی فراقانونی گسترش داده‌اند علاقه ویژه‌ای به گسترش این موضوع به فضای سایبری دارند. به‌طورکلی گسترش اعمال ماده ۵۱ در موارد خاصی منوط به اینکه شرایط انتساب و انجام توسل به‌زور به‌درستی اثبات گردیده و وضعیت به شورای امنیت گزارش شود، می‌تواند در جهت تحقق صلح بین‌المللی مؤثر باشد؛ که فضای سایبر و حملات سایبری از این موضوع مستثنا نمی‌باشند؛ اما باید دولت‌ها در راستای انجام گفتگوهای سازنده مقررات و راهکارهای خاصی برای فضای مذکور بیندیشند. با همه این موارد نکته‌ی خاصی که وجود دارد ضرورت رعایت تناسب در بحث دفاع مشروع سایبری است که باید اقدامات دفاع دیجیتالی متناسب باشد که احراز این موضوع با توجه به مباحث فنی بسیار پیچیده، بعید به نظر می‌رسد.

منابع

- اسمعیل زاده ملاباشی، پرستو و عبدالهی، محسن. (۱۳۹۹). «حملات سایبری و نقض اصل عدم‌مداخله»، فصل‌نامه مطالعات حقوق عمومی، دوره ۵۰، شماره ۲.

- باستانی، برومند. (۱۳۸۳). جرایم کامپیوتری و اینترنتی، جلوه‌ای نوین از بزهکاری، تهران: انتشارات بهنامی.

[۱۸] Tallinn

– بای، حسین‌علی و پور قهرمانی، بابک. (۱۳۸۸). بررسی فقهی و حقوقی جرایم رایانه‌ای، قم: پژوهشگاه علوم و فرهنگ اسلامی.

– پور قهرمانی، بابک و صابر نژاد، علی. (۱۳۹۴). حریم خصوصی در فضای سایبر از منظر حقوق بین‌الملل، تهران: انتشارات مجد.

– جیستان، ذبیح‌الله و جیستان، حسین. (۱۳۹۳)، «مفهوم جنگ سایبری و بررسی ابعاد مختلف»، ،نهمین سمپوزیوم بین المللی پیشرفتهای علوم و تکنولوژی،مشهد.

– حیدری، حمید. (۱۳۷۶). توسل به‌زور در روابط بین‌الملل، تهران: انتشارات اطلاعات.

– رضایی، محمدحسن، میر عباسی، سید باقر و کمالی، علی. (۱۳۹۸). «مبانی توسل به‌زور و ممنوعیت آن در حقوق بین‌المللی با تأکید بر منشور سازمان ملل متحد»، فصل‌نامه تحقیقات حقوقی بین‌المللی، دوره ۱۲، شماره ۴۵.

– صابر نژاد، علی و هاشم‌پور حمیدی، هادی. (۱۳۹۲). «جنگ سایبری و تحول مفهوم توسل به‌زور در حقوق بین‌الملل»، پنجمین همایش مجازی بین‌المللی تحولات جدید ایران و جهان، قزوین،دانشگاه بین‌المللی امام خمینی

– صانعیان، علی. (۱۳۹۸). «امنیت سایبری در آمریکا، ساختارها و روندها»، فصل‌نامه سیاست خارجی، دوره ۳۳، شماره ۱۲۹.

– مرکز پدافند غیرعامل فاوا. (۱۳۸۸). «جنگ سایبری»، مجله پردازشگر، دوره ۷، شماره ۶۴.

– مسعودی، امیر. (۱۳۸۳). «امنیت اطلاعات در فضای سایبر»، تهران، نشریه کتاب ماه

– مصفا، نسرین، طارم سری، مسعود و مستقیمی، بهرام. (۱۳۶۵). مفهوم تجاوز در حقوق بین‌الملل، تهران: انتشارات دانشگاه تهران.

– هلیلی، خداداد. (۱۴۰۰). «فناوری‌های نوظهور سایبری و تهدیدات ناشی از به‌کارگیری آن‌ها در سازمان‌های دفاعی- نظامی»، فصل‌نامه مطالعات جنگ، دوره ۳، شماره ۱۱.

- Anand, Ruchi. (2009). Self-Defense in International Relations, New York: Palgrave Macmillan.

- Charney, Scott. (2009). “Rethinking the Cyber Threat A Framework and Path Forward”, Microsoft Corp. One Microsoft Way Redmond, WA 98052-6399 USA,14(2).

- Clark, Richard. (2009). e,War from Cyberspace, the National Interest ,Chicago.

- Cornish, Paul & David Livingstone. (2010). On Cyber Warfare, a Chatham House Report, The Royal Institute of International Affairs.

- Dinstein, Yoram. (2017). War Aggression and Self-Defence, 6th ed Cambridge: Cambridge University.

- Friedman, Allan. (2014). Cybersecurity and Cyberwar, What Everyone Needs to Know,London, Oxford University.

- Gray, Christine. (2018). International Law and the Use of Force, 4th ed Oxford: Oxford University Press.

- Haller, John, Merrell, Samuel, Butkovic, Matthew J. & Willke, Bradford J. (2010). “Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability”, Software Engineering Institute,9(2).

- Howcroft, Elizabeth. (2022). available at: https://www.reuters.com/technology/hackers-steal-around-100-million-cryptocurrency-binance-linked-blockchain-2022-10-07/

- Lord,kristin m.&sharp, Travis. (2011). “America’s Cyber future Security and Prosperity in the Information Age”, Center for a New American Security, Vol 1,at: https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS_Cyber_Volume-I_0.pdf?mtime=20160906081238&focal=none

- Michael, Schmitt N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare, New York: Cambridge University Press.

- Nakashima, Ellen. (2016). “Obama to be urged to split cyberwar command from NSA”. The Washington Post. Archived from the original on 14 September 2016

- O'Connell, C. & Tams, D,Tladi. (2019). Self-Defence against Non-State Actors, Max Planck Trialogues, Cambridge, Cambridge University Press.

- Ramírez, J.M. & García-Segura, L.A. (2017). Cyberspace: Risks and Benefts for Society, Security and Development, Cham: Springer

- Roscini, Marco. (2014). Cyber Operations and the Use of Force in International Law, London,,Oxford University Press.

- Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed).Cambridge: Cambridge University Press. Glossary.

- Schroefl, Josef & Kaufman, Stuart. (2014). Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War, Washington, D.C, Studies in Conflict and Terrorism

- Schrofl,Josef, Cox, Sean Michael,Pankratz,Thomas. (2009). Winning the Asymmetric War, Political,Social and Military Responses, Frankfurt: Peter Lang.

- Schulze, Hendrik. (2015). "Cyber War", Testfall der Staatenverantwortlichkeit, Tübingen: Mohr Siebeck.

- Tallinn Manual 2.0 On The International Law Applicable To Cyber Operation. (2017). Perpared by International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Center of Excellence, Cambridg: Cambridg university press.

- Tibori, Szabó Kinga. (2016). The "Unwilling or Unable" Test and the Law of Self-Defence, Washington, D.C

- Woltag, Johann. (2014). Cyber Warfare: Military Cross-Border Computer Network Operations under International Law, Cambridge: Cambridg university press.

-Waxman, Matthew C. (2011)."Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", Yale Journal of International Law,15(4). Vol. 36

Documents

- Declaration on Friendly Relations. (1970).

- I.C.J Reports, Nicaragua judgment. (1986).

- Washington Post. Retrieved. (2019-04-01), available at:

https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidentialcampaign/2016/12/09/31d6b300-be2a-11e6-94ac 3d324840106c_story.html

- https://supreme.justia.com/cases/federal/us/521/844/

-https://ir.voanews.com/a/international-media-reports-on-crackdown-of-protesters-and-artists-and-the-impact-of-israeli-drone-attack-on-isfahan/6946797.html