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

Possible Responses to Cyber Attacks from the perspective of International Law

Azar Givkey*

PhD in International Law, Department of International Law, Qom Branch, Islamic Azad University, Qom, Iran

azarg1359@gmail.com

DOI 10.30495/CYBERLAW.2023.701823

Keywords:
Cyber Attacks, State Responsibility, Accountability, Cyber Law, Cyber Defense.

Abstract

Cyber-attacks, while as easy as pushing a button, can have devastating and possibly catastrophic consequences such as the destruction, disabling or malfunctioning of critical infrastructure. Such an inevitable action certainly has to be timely and appropriately responded by the affected states. Although the issue of international responsibility of states, as a broad concept of cyber-attacks, faces many challenges, assuming that the aggrieved State is able to identify the source of the cyber-attack and also able to attribute the same to a country, the question that arises is: what legal solutions exist for the aggrieved government in order to respond appropriately and realize its right. In this article, which has employed library studies and analytical and descriptive methodology, we intend to examine the types of possible responses to cyber-attacks by the aggrieved governments and the conditions for using each of the possible responses.

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

پاسخ‌های ممکن نسبت به حملات سایبری از منظر حقوق بین‌الملل

آذر گیوکی*

دانش آموخته دکتری حقوق بین‌الملل، گروه حقوق بین‌الملل، واحد قم، دانشگاه آزاد اسلامی، قم، ایران

azarg1359@gmail.com

تاریخ دریافت: ۲۰ آذر ۱۴۰۱ تاریخ پذیرش: ۱۹ فروردین ۱۴۰۲

چکیده

حملات سایبری، در عین سهولت به‌اندازه فشردن یک دکمه، ممکن است آثار مخرب و شاید فاجعه‌باری، همچون تخریب، از کار انداختن یا اختلال در کارکرد زیرساخت‌های مهم و حیاتی، در پی داشته باشند و این مسأله غیرقابل‌اغماض، قطعاً باید با پاسخگویی صحیح و به‌موقع از سوی دولت زیان‌دیده، مواجه شود. اگرچه، مبحث مسئولیت بین‌المللی دولت‌ها، به‌عنوان یک مفهوم گسترده درباره حملات سایبری، با چالش‌های بسیار مواجه است، اما با فرض اینکه دولت زیان‌دیده، قادر به شناسایی منشأ حمله سایبری باشد و بتواند حمله را به دولتی منتسب نماید؛ این سؤال مطرح می‌شود که چه راهکارهای حقوقی پیش روی دولت زیان‌دیده، در راستای پاسخ مناسب و احقاق حق آن وجود دارد؟ در این نوشتار که با استفاده از مطالعات کتابخانه‌ای و با روش توصیفی و تحلیلی، تهیه شده است، بر آنیم که انواع پاسخ‌های ممکن به حملات سایبری از سوی دولت زیان‌دیده را بررسی کرده و شرایط استفاده از هر یک را بیان نماییم.

کلید واژگان: حملات سایبری، مسئولیت دولت، شورای امنیت، دیوان بین‌المللی دادگستری، پدافند سایبری.

مق

عدم اطمینان عمیقی در مورد برخورد با فضای مجازی به‌عنوان یک فضای فیزیکی دیگر مانند زمین، هوا یا دریا وجود دارد؛ اینکه کدام کشورها ممکن است کنترل حاکمیت آن را در دست داشته باشند؛ چنین رفتاری با توجه به توصیف فضای مجازی به‌عنوان سرزمین مجازی، واقعاً بحث‌انگیز است. اگرچه وجود زیرساخت‌های فیزیکی در داخل قلمرو دولت به آن‌ها اجازه می‌دهد تا حدی کنترل بر روی کاربران نهایی، ایستگاه‌های مسیریاب، سرورها، جریان داده‌ها و موارد مشابه داشته باشند، اما اجرای چنین کنترلی دشوار است؛ زیرا این امر عمدتاً در برخورد با حقوق اساسی بشر و اصول حفظ حریم خصوصی، آزادی بیان و تشکل‌ها و اقتصاد بازار آزاد موردقبول واقع نمی‌شود. با توجه به تردیدهایی که به نظر می‌رسد بسیاری از مقامات دولتی، در مورد مفاد مقرراتی واحد دارند که بتواند به بهترین وجه، منافع کشورهایی را که درگیر عملیات سایبری هستند تضمین کند و ظرفیت‌های نابرابر دولت‌ها در این زمینه و کمبود نهادهای بین‌المللی مؤثر برای انتساب مسئولیت بر مبنای هنجارهای حقوق بین‌الملل را شناسایی کند، جای تعجب نیست که علیرغم فقدان یک کنوانسیون واحد، تلاش برای قاعده‌مند سازی فضای مجازی از طریق ترجمه مفاهیم سنتی دولت، ازجمله حاکمیت، تمامیت ارضی و مسئولیت بین المللی، با برخی از بدبینی‌ها و مقاومت‌ها روبرو شده و فقط تا حدی از رویه دولت شکل می‌گیرد. آنچه تاکنون، در رابطه با قاعده‌مند سازی فضای سایبر، مورد وفاق است، این است که قواعد حقوق بین‌الملل موجود، بر عملیات‌های سایبری، حاکم است، کشورها، حاکمیت یا کنترل بخشی از فضای سایبر را در دست دارند؛ هم‌چنین، قواعد حقوق توسل به زور و حقوق مخاصمات مسلحانه، در حوزه جنبشی، بر حملات سایبری قابل‌اعمال هستند و دولت‌ها، نه‌تنها مسئولیت اعمال خود در این فضا، بلکه گاه، مسئولیت مجرمان سایبری خصوصی را تحت شرایطی متحمل می‌شوند. از سویی، نبود حقوق سخت و عدم تناسب میان اصول سنتی موجود حقوق بین‌الملل حاکم بر اعمال قدرت دولت در داخل و خارج از قلمرو آن و تنظیم فضای مجازی، دلیلی برای ترجیح برخی از کشورهای درگیر در عملیات سایبری به حفظ سیاست سکوت و ابهام در رابطه با حملات سایبری، ارائه می‌دهد؛ در این برهه از زمان، دولت‌ها ترجیح می‌دهند در عملیات سایبری با آستانه پایین و عملیات جاسوسی شرکت‌کننده و با توسعه مسیرهای موازی محدود، انتقام‌جویی پنهانی و مقابله‌به‌مثل آشکار و منوط به شرایط خاصی از تناسب، فعلاً درجه‌ای از ثبات را در فضای سایبری حفظ کنند. آنچه در این پژوهش که با روش توصیفی-تحلیلی، انجام شده است، موردنظر است، پاسخ به این سؤال است که دولت‌ها، مطابق قواعد حاضر، مجاز به چه انواعی از پاسخگویی در مقابل حملات سایبری هستند؟ این تحقیق، می‌کوشد پاسخ‌های مختلف موجود در حقوق بین‌الملل حاضر ازجمله، حل‌وفصل مسالمت-آمیز اختلافات، ارجاع به شورای امنیت، اقدام متقابل و دفاع مشروع را در عملیات‌های سایبری، بررسی نماید.

۱. حل‌وفصل مسالمت‌آمیز اختلافات

لزوم حل‌وفصل اختلافات بین‌المللی به شیوه‌های مسالمت‌آمیز در حقوق بین‌الملل، در معاهدات چند و دوجانبه، مورد پشتیبانی قرارگرفته،[۱] در تصمیمات دیوان بین‌المللی دادگستری اعمال گردیده[۲] و در قطعنامه‌های مجمع عمومی ملل متحد، نیز تصدیق شده است.[۳] از جهتی، کاملاً پذیرفته‌شده که این تعهد، واجد ماهیتی عرفی است (Nicaragua Judgment, 1986 :290).[۴] مواد ۲(۳) و ۳۳(۱) منشور ملل متحد،

---

۱ از جمله این معاهدات، می‌توان به موارد زیر اشاره کرد:

American Treaty on Pacific Settlement (Pact of Bogotá), 30 April 1948, 30 UNTS 55; European Convention for the Peaceful Settlement of Disputes, 29 April 1957, 320 UNTS 243

۲ ازجمله می‌توان به آرای زیر اشاره کرد:

Fisheries Jurisdiction (Spain v. Can.) judgment, 1998 ICJ 432, Para. 56 (4 December); Aerial Incident judgment, Para. 53.

۳ ازجمله، اصل ۲ از اعلامیه روابط دوستانه که «اصل حل‌وفصل اختلافات به شیوه‌های مسالمت‌آمیز توسط دولت‌ها به‌گونه‌ای که صلح و امنیت بین‌المللی و عدالت به مخاطره نیفتد» را تصدیق می‌نماید.

۴ See also UN GGE 2015 Report, Paras26, 28(b).

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

تأکید دارند که «طرفین هر اختلافی که احتمال می‌رود تداوم آن حفظ صلح و امنیت بین‌المللی را به مخاطره افکند، پیش از هر چیز از طریق مذاکره، تحقیق، میانجی‌گری، سازش، داوری، حل‌وفصل قضایی، توسل به نهادها یا ترتیبات منطقه‌ای یا دیگر شیوه‌های منتخب خویش، درصدد یافتن راه‌حل برآیند» (UN Charter, Art. 33(1)). هم‌چنین، «تمامی اعضا، اختلافات بین‌المللی خود را از طریق شیوه‌های مسالمت‌آمیز حل‌وفصل می‌کنند به‌گونه‌ای که صلح و امنیت بین‌المللی و عدالت به مخاطره نیفتد»؛ بدین ترتیب، تعهد کوشش برای حل‌وفصل مسالمت‌آمیز اختلافات، تنها زمانی الزامی است که احتمال به خطر افتادن صلح و امنیت بین‌المللی از رهگذر اختلاف موردنظر وجود داشته باشد. این اختلاف، می‌تواند عدم توافق بر سر مقوله‌ای حکمی یا موضوعی، تعارض دیدگاه‌های حقوقی یا تعارض منافع میان طرفین باشد (Mavrommatis Palestine Concessions, 1924: 2).[۵] به‌عنوان‌مثال، ادعای یک دولت، دایر بر نفوذ دولت دیگر در زیرساخت سایبری او به‌گونه‌ای که اصل حاکمیت را نقض می‌کند، اختلاف میان دو دولت به شمار می‌رود؛ هم‌چنین عدم توافق میان آن‌ها بر سر کفایت قانون داخلی، وفق موافقت‌نامه‌ای دوجانبه راجع به تعقیب جرائم سایبری نیز به این شکل است. اختلاف، صرف وجود تنشی کلی میان دولت‌ها نیست؛ بلکه متضمن ادعایی خاص، از جانب یک دولت است که توسط دولتی دیگر رد می‌شود (The Charter of United Nations: A Commentary, at 192).

قاعده ۶۵ دستورالعمل تالین ۲، در این راستا، مقرر داشته است «(الف) دولت‌ها باید بکوشند اختلافات بین‌المللی مشتمل بر فعالیت‌های سایبری خود که صلح و امنیت بین‌المللی را به مخاطره می‌افکنند، از طریق شیوه‌های مسالمت‌آمیز حل‌وفصل کنند. (ب) اگر دولت‌ها بکوشند اختلافات بین‌المللی مشتمل بر فعالیت‌های سایبری خود را که صلح و امنیت بین‌المللی را به مخاطره نمی‌اندازند، حل‌وفصل نمایند، می‌بایست از طریق شیوه‌های مسالمت‌آمیز به این امر مبادرت ورزند». این قاعده، صرفاً بر اختلافات بین‌المللی و نه اختلافات کاملاً داخلی، اعمال می‌گردد؛ اختلاف بین‌المللی، عبارت است از اختلافی که میان دو یا چند دولت وجود دارد. باوجوداین، اختلاف میان اعضای یک اتحاد نظامی، در باب تعهدات معاهداتی مربوط به خود آن‌ها، راجع به پدافند سایبری مشترک، واجد این وصف است. هم‌چنین، در پاره‌ای مواقع، ممکن است یک اختلاف داخلی، به اختلافی بین‌المللی مبدل شود (The Charter of United Nations: A Commentary, at 193).

در حل‌وفصل اختلاف بین‌المللی مشتمل بر فعالیت‌های سایبری، دولت تنها می‌تواند به «شیوه‌های مسالمت‌آمیز» متوسل شود و باید این کار را «به شیوه‌ای که صلح و امنیت بین‌المللی و عدالت به خطر نیفتد»، انجام دهد؛ انتخاب شیوه‌ها مقوله‌ای است که به تصمیم دولت‌ها بستگی دارد. حتی اگر شیوه‌های مرضی‌الطرفینی رسیدگی به اختلاف بین‌المللی اغلب به‌واسطه دلایل سیاسی و دیگر علل ترجیح داشته باشند، به اقدام یک‌جانبه موافق قواعد بین‌المللی یک دولت، در زمان ورود به اختلافی بین‌المللی خدشه‌ای وارد نمی‌سازد. برای نمونه، یک دولت می‌تواند به‌منظور اثرگذاری بر حل‌وفصل اختلاف به سود خود، تحریم‌های تجاری را در زمینه واردات تجهیزات مربوط به فناوری اطلاعات وضع کند. این قاعده، اتخاذ اقدامات متقابل قانونی را ممنوع نمی‌کند (Tallinn Manual 2.0 Rule 65, 2017: 11).

۲. پاسخ‌های دیپلماتیک

نوع دیگری از پاسخ در مقابل حملات سایبری، اعتراضات دیپلماتیک است که می‌تواند به‌صورت یک بیانیه دیپلماتیک، به دولتی که ادعا می‌شود حمله را مرتکب شده است، به‌صورت محرمانه یا علنی، ابلاغ شود، این بیانیه هم‌چنین ممکن است به‌صورت یک بیانیه عمومی یا از سوی یک یا چند سازمان منطقه‌ای یا بین‌المللی صورت گیرد. علاوه بر بیانیه، اعتراضات دیپلماتیک می‌تواند با اخراج یک یا برخی از دیپلمات‌ها یا سایر مقامات نماینده دولت متهم، تقویت شود. این نوع پاسخ، علاوه بر اینکه به اعتبار بین‌المللی دولت متهم آسیب وارد

۵ See also Case Concerning Certain Property (Liech. v. Ger.) judgment on preliminary objections, 2005 ICJ 6, Para 24 (10 February).

می‌کند، به‌خوبی مؤید این است که کشور موردتهاجم، قادر به شناسایی مهاجمان سایبری است و برای کشور مهاجم، آسیب چندانی به بار نخواهد آورد. اعتراضات دیپلماتیک را می‌توان یک واکنش نمادین در نظر گرفت (Van Der Meer, 2018: 3).

۳. پاسخ‌های حقوقی

اقدامات حقوقی، با متهم کردن سازمان‌ها یا افراد، پیامی آشکار و عمومی ارسال می‌کند که مهاجمان سایبری شناسایی شده‌اند و با عواقب عمل ارتکابی، روبرو خواهند شد. این اقدامات ممکن است به‌واسطه برخی آسیب‌های اعتبار بین‌المللی، اثر بازدارندگی داشته باشد. کیفرخواست، عموماً در سطح ملی، صادر می‌شود که بااینکه این اقدامات، اغلب حالتی نمادین دارند اما درصورتی‌که افراد متهم از کشور صادرکننده کیفرخواست بازدید کنند، امکان دستگیری دارند. در حال حاضر، دخالت سازمان‌های قضایی بین‌المللی مانند دیوان بین‌المللی دادگستری یا دیوان کیفری بین‌المللی، کمی دور از ذهن به نظر می‌رسد (Van Der Meer, 2018: 4). که در ادامه به این موارد اشاره‌ای خواهیم داشت.

۱،۳. مراجعه به دادگاه‌های بین‌المللی

چنانچه دولت مهاجم، شناسایی شده و حمله، به او منتسب شده باشد، می‌توان با استناد به نقض بند ۴ ماده ۲ منشور ملل متحد و اصل عدم‌مداخله و به‌منظور جبران خسارت، علیه وی در یک دادگاه بین‌المللی، مانند دیوان بین‌المللی دادگستری اقامه دعوا نمود. باید در نظر داشت که ازآنجاکه دیوان، مانند سایر دادگاه‌های بین‌المللی فاقد صلاحیت اجباری است، بنابراین دو طرف باید با توافق و قبول صلاحیت دیوان، مسئله را به این مرجع، ارجاع نمایند. از سوی دیگر، ارزیابی مجموع خسارات وارده در اثر حمله سایبری، ممکن است دشوار باشد، زیرا دولت‌ها به دلیل مسائل امنیتی و منافع ملی، تمایلی به ارائه اطلاعات مربوط به تأسیسات مهم خود و حتی نوع حمله و میزان خسارات وارده، ندارند. به‌علاوه، دیوان، در مسیر رسیدگی خود به هر قضیه، با پایبندی به ماده ۳۸ اساسنامه، بر مبنای منابعی مانند، معاهدات بین‌المللی، عرف بین‌المللی، اصول کلی حقوق بین‌الملل و تصمیمات قضایی و عقاید برجسته‌ترین مبلغین ملل که به‌عنوان وسیله‌ای فرعی برای تعیین قواعد حقوقی مورداستفاده قرار می‌گیرد، نسبت به حل‌وفصل اختلاف، تصمیم‌گیری می‌نماید؛ در مورد عملیات‌های سایبری، باید متذکر شد که حقوق سخت در قالب معاهده و قرارداد، هنوز شکل نگرفته است، هم‌چنین، حقوق عرفی که با رویه دولت‌ها و التزام آن‌ها به یک‌رویه خاص یا حتی با توجه به عملکرد دیوان بین‌المللی دادگستری در رسیدگی به قضایای ارجاع شده، قابل‌تعریف خواهد بود، تاکنون قوام نیافته است، از طرفی، شاهد سند غیر الزام‌آوری هستیم که تحت عنوان دستورالعمل تالین ۲، به بیان قواعد موجود حقوق بین‌الملل در رابطه با فضای سایبری، پرداخته است و توان ایجاد یک قانون خاص در رابطه با عملیات‌های سایبری را ندارد؛ به‌این‌ترتیب، مستندی قانونی که با تکیه بر آن عملیات‌های سایبری، مورد رسیدگی قرار گیرند، هنوز موجود نیست. از سوی دیگر، درخواست نظریه مشورتی از دیوان بین‌المللی دادگستری، در خصوص مشروعیت حملات سایبری طبق ماده ۹۶ منشور می‌تواند باوجوداینکه این ویژگی غیر الزام‌آور دارد، اما در مسیر شکل‌گیری حقوق عرفی، مؤثر واقع شود.

برخی صاحب‌نظران پیشنهاد کرده‌اند که حملات سایبری منتهی به تجاوز، موجب طرح مسئولیت کیفری بین‌المللی اشخاص مسئول شود. کنفرانس بازبینی اساسنامه دیوان بین‌المللی کیفری (ICC) نهایتاً تعریفی از جرم تجاوز را بر اساس قطعنامه ۳۳۱۴ مصوب سال ۱۹۷۴ مجمع عمومی ارائه داد؛ هرچند برخی از موارد برشمرده شده در ماده ۸ مکرر اساسنامه دیوان بین‌المللی کیفری، حملات سایبری خاصی را از طریق قیاس با حملات سنتی تحت پوشش قرار می‌دهد؛ اما به نظر می‌رسد که چنین تفسیری با ماده ۲۲ که تفسیر از طریق قیاس را ممنوع نموده، در تضاد است.

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

۲،۳. ارجاع به شورای امنیت سازمان ملل

به‌طورکلی می‌توان دو دیدگاه را در خصوص اینکه آیا حمله سایبری می‌تواند مشمول عنوان «توسل به زور» باشد، بیان داشت. یک دیدگاه، بر آن است که ممنوعیت توسل به زور، تنها محدود به حمله مسلحانه و با سلاح‌های سنتی است و بنابراین حمله سایبری، خارج از شمول بند ۴ ماده ۲ منشور قرار می‌گیرد. این رویکرد، رویکردی مضیق به قواعد ایجاد شده توسط جامعه بین‌المللی است و مقرر می‌دارد هر چیزی که خارج از این ممنوعیت قرار بگیرد، قانونی است.

دیدگاه دیگر، رویکردی موسع است و مقرر می‌دارد ازآنجاکه یکی از اهداف منشور، حفظ صلح و امنیت بین‌المللی است و منشور، هرگونه توسل به زور را که صلح و امنیت بین‌المللی را به مخاطره اندازد، ممنوع نموده است؛ تمام انواع زور، در یک سلسله قرار دارند و حاصل آن‌ها عوامل چندی است که حداقل نظم جهانی را متأثر می‌سازد.

مطابق این رویکرد و نیز با اشاره به دستورالعمل تالین ۲، حملات سایبری که دارای شرایط ذکر شده برای توسل به زور محسوب شدن حملات سایبری باشند و زیرساخت‌های حیاتی یک دولت را هدف قرار داده و موجب خسارت‌های گسترده مالی و جانی شوند، می توانند در محدوده بند ۴ ماده ۲ منشور قرار گیرند. بر این اساس، هدف نویسندگان منشور، تنها ممنوع ساختن تعارضات مسلحانه نبوده، بلکه هر اقدامی که می‌توانسته صلح و امنیت بین‌المللی را به مخاطره اندازد، موردنظر بوده است؛ بند ۴ ماده ۲ منشور، توسل به زور را به هر طریقی که مغایر با اهداف منشور باشد، ممنوع می‌نماید. از سوی دیگر، این ماده، دولت‌ها را از توسل به زور علیه تمامیت ارضی دولت دیگر منع نموده است. عبارت تمامیت ارضی را می‌توان به طرق گوناگونی تفسیر نمود، ازجمله اینکه تمامیت ارضی یک دولت، فضای سایبری او را هم در برمی‌گیرد و بنابراین هرگونه خرابکاری گسترده در این فضا، تجاوز به تمامیت ارضی آن دولت است (گیوکی، ۱۴۰۰: ۱۲۳-۱۲۴). چنانچه دولت قربانی حمله سایبری، معتقد باشد که حمله یا حملات صورت گرفته از شدت قابل‌توجهی برخوردار بوده و بیم آن می‌رود که صلح و امنیت بین‌المللی را به مخاطره اندازد، می‌تواند طبق پاراگراف اول ماده ۳۵ منشور ملل متحد، موضوع را به شورای امنیت سازمان ملل ارجاع دهد؛ مطابق قاعده ۷۶ دستورالعمل تالین ۲، «اگر شورای امنیت ملل متحد، تعیین کند که یک عملیات سایبری موجب شکل‌گیری تهدید صلح، نقض صلح یا عمل تجاوز شده است، می‌تواند اجازه اتخاذ اقدامات غیر قهری متقابل و ازجمله انجام عملیات‌های سایبری را بدهد. درصورتی‌که شورای امنیت چنین اقداماتی را ناکافی قلمداد نماید، می‌تواند در خصوص اقدامات قهرآمیز ازجمله اقدامات سایبری اتخاذ تصمیم کند». این قاعده، بر فصل هفتم منشور ملل متحد استوار است. ماده ۳۹ منشور به شورای امنیت این اختیار را می‌دهد که «درصورتی‌که وجود هرگونه تهدید علیه صلح، نقض صلح یا عمل تجاوز را تعیین کند در راستای حفظ یا اعاده صلح و امنیت بین‌المللی، توصیه‌هایی را صادر یا در خصوص اقداماتی که باید وفق مواد ۴۱ و ۴۲ اتخاذ شوند تصمیم‌گیری نماید».

شورای امنیت، دو پدیده حائز اهمیت تروریسم بین‌المللی[۶] و اشاعه تسلیحات کشتارجمعی[۷] را تهدید علیه صلح نامیده است؛ هم‌چنین این شورا در قالب قطعنامه ۲۳۴۱، از کشورهای عضو درخواست می‌نماید که به خطر حملات تروریستی، ازجمله حملات سایبری تروریستی علیه زیرساخت‌های حیاتی رسیدگی نمایند؛ نیز، قطعنامه ۲۳۷۰ را در سال ۲۰۱۷ در رابطه با جلوگیری از دستیابی تروریست‌ها به سلاح، ازجمله سلاح سایبری، به تصویب رسانده است. علاوه بر این عملیات‌های سایبری، در نشست‌های موسوم به «فرمول آریا» شورای امنیت، به‌طور مشخص، در ۲۶ آگوست ۲۰۲۲، طی نشستی با عنوان حملات سایبری علیه زیرساخت‌های حیاتی، در ۲۲ مه ۲۰۲۰،

۶ See, e.g. SC Res. 1373, UN Doc. S/RES/2001 (28 September 2001).

۷ See, e.g. SC Res. 1540, UN Doc. S/RES/1540 (28 April 2004).

دانشگاه آزاد اسلامی واحد مرند

در نشستی تحت عنوان ثبات سایبری، پیشگیری از درگیری و ظرفیت‌سازی، در ۲۳ نوامبر ۲۰۱۶ و تحت عنوان امنیت سایبری و صلح و امنیت بین‌المللی، موضوع بحث و تبادل‌نظر قرارگرفته است.

باوجود این‌که مصادیق تهدید علیه صلح و نقض صلح، توسط شورای امنیت، مشخص گردیده است و مسلم است که شورای امنیت اقتدار تشخیص هرگونه عملیات ازجمله عملیات‌های سایبری به‌عنوان نقض صلح یا تهدید علیه صلح را دارد اما تاکنون، هیچ عملیات سایبری را، واجد شرایط تهدید علیه صلح، نقض صلح یا عمل تجاوز تشخیص نداده است.

شورای امنیت می‌تواند تصمیم بگیرد که انواع خاصی از عملیات‌های سایبری به‌صورت انتزاعی و پیش‌فرض، یعنی بدون اشاره به اقدامات خاصی که رخ‌داده یا در شرف وقوع‌اند، تهدید علیه صلح، نقض صلح یا عمل تجاوز به شمار می‌آیند؛ برای نمونه، تعیین اینکه عملیات‌های سایبری هدایت شده علیه سامانه‌های بانکی ملی یا زیرساخت‌های ملی حساس واجد چنان وصفی هستند، ذیل اقتدار شورای امنیت قرار دارد؛ هم‌چنین، هرکجا عملیات‌های سایبری یک دولت مداخله ممنوعه به شمار آید، صلح و امنیت بین‌المللی درخطر است. شورای امنیت، به‌مجرد انجام امر مقرر شده در ماده ۳۹، می‌تواند اتخاذ اقدامات وفق ماده ۴۱ را مدنظر قرار دهد. این ماده مقرر می‌دارد که «شورا، برای عملی ساختن تصمیمات خود، می‌تواند نسبت به اقداماتی که مستلزم به کار بردن نیروی مسلح نیست، اتخاذ تصمیم نماید و می‌تواند اعضای ملل متحد را به اعمال چنین اقداماتی فرابخواند. این اقدامات، ممکن است توقف کلی یا جزئی روابط دیپلماتیک و ارتباطات ریلی، دریایی، هوایی، پستی، تلگرافی، رادیویی و سایر شیوه‌های ارتباطی و قطع روابط دیپلماتیک را در برگیرد». اقدامات غیر قهری اقداماتی هستند که به سطح توسل به زور نمی‌رسند؛ لازم به ذکر است که همان‌طور که در پاراگراف ۳۵ رأی قضیه تادیچ اشاره شده است، فهرست اقدامات مورداشاره در ماده ۴۱ منشور حصری نیست. اشاره به «توقف کلی یا جزئی ... ارتباطات پستی، تلگرافی، رادیویی و سایر شیوه‌های ارتباطی» در ماده ۴۱، در حوزه سایبر از اهمیت ویژه‌ای برخوردار است. این مقرره، در پرتو حاشیه صلاحدید گسترده شورا، مؤید آن است که شورای امنیت می‌تواند در خصوص توقف کلی یا جزئی ارتباطات سایبری با یک دولت یا بازیگر غیردولتی اتخاذ تصمیم کند[۸]. از طرفی، کلیه دولت‌های عضو ملل متحد، ملزم به اجرای تصمیمات شورای امنیت که از توصیه‌ها متمایز هستند، ذیل فصل هفتم منشور ملل متحد می‌باشند (UN Charter, Art. 25). به‌طورکلی، قطعنامه‌های شورای امنیت، تصمیم‌گیری راجع به شیوه‌های خاصی که دولت‌ها با آن‌ها تعهد خویش دایر بر اجرای تصمیمات شورا در سطح داخلی را ایفا می‌کنند را به خود ایشان واگذار می‌کند. در مورد تحریم‌های مشتمل بر ارتباطات سایبری، اجرای داخلی امری ناگزیر خواهد بود. برای نمونه، ممکن است الزام ارائه‌دهندگان خدمات اینترنت (دولتی و خصوصی به یک‌شکل) به اتخاذ اقدامات محدودکننده مانند تهیه لیست سیاه نام دامنه یا فیلترینگ مسیریابی بسته‌ها برای پایبندی به قطعنامه الزام‌آور شورای امنیت، ضروری باشد. بر این اساس، امکان دارد دولت‌ها مجبور شوند قانون یا مقرراتی داخلی را به تصویب برسانند که ارائه‌دهندگان خدمات اینترنتی تحت صلاحیت، آنان را به اتخاذ اقدام ضروری وادار سازند (Tallinn Manual 2.0 Rule 76, 2017: 5). قاعده ۷۶ دستورالعمل تالین ۲، هم‌چنین بر ماده ۴۲ منشور استوار است. زمانی که شورا تشخیص دهد که تهدید علیه صلح، نقض صلح یا عمل تجاوز وجود دارد و اقدامات غیر قهری برای حفظ یا اعاده صلح و امنیت بین‌المللی ناکافی بوده یا عدم‌کفایت آن‌ها اثبات شده است، می‌تواند مجوز توسل به زور و ازجمله از طریق ابزارهای سایبری را صادر کند. وضعیتی را در نظر بگیرید که در آن یک دولت درحال‌توسعه توانمندی تسلیحات هسته‌ای خویش است. آن دولت، خواسته‌های شورای امنیت برای پایان دادن به فعالیت‌های خویش را نادیده گرفته و در معرض تحریم‌های اقتصادی مجاز وفق ماده ۴۱ قرارگرفته است. شورای امنیت می‌تواند به دولت‌های عضو اجازه دهد به عملیات‌های سایبری طراحی شده برای قطع برنامه تسلیحاتی مزبور علیه آن دولت دست بزنند. شورای

---

۸ برای نمونه، در سال ۲۰۰۱، سازکار پایش تحریم‌ها علیه اتحادیه ملی استقلال کامل آنگولا، احتمال اتخاذ اقداماتی در راستای توقف اتصالات اینترنتی با اتحادیه ملی استقلال کامل آنگولا را مطرح ساخت.

Monitoring Mechanism on Sanctions against UNITA Report, appended to Letter from the Chairman of the Security Council Committee established pursuant to Resolution 864 to the President of the Security Council, Paras64–69, UN Doc. S/2001/966 (12 October 2001).

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

امنیت اغلب مقرر می‌دارد که برای اجرای یک قطعنامه، باید «کلیه اقدامات ضروری» اتخاذ گردند؛ عبارت مربوطه، از اقتدار و اختیار به‌کارگیری عملیات‌های سایبری در سطح توسل به زور علیه دولت یا موجودیتی که هدف قطعنامه موردنظر است حکایت دارد که اتخاذ اقدام فیزیکی علیه توانمندی‌های سایبری آن دولت یا موجودیت را نیز در برمی‌گیرد. بی‌گمان، هر اقدام اتخاذی می‌بایست در چارچوب حکم یا مجوز قطعنامه ذی‌ربط قرار داشته باشد. لازم به ذکر است که شورای امنیت تحت هیچ شرایطی نمی‌تواند از قواعد واجد ماهیت آمره تخطی کند (Tallinnn Manual 2.0 Rule 76, 2017: 6-7).

دستورالعمل تالین ۲، هم‌چنین در قاعده ۷۷، اشاره دارد که «سازمان‌ها، ترتیبات یا نهادهای بین‌المللی واجد ماهیت منطقه‌ای می‌توانند وفق حکم یا مجوز شورای امنیت ملل متحد، به انجام اقدامات اجرایی در پاسخ به عملیات‌های سایبری مبادرت جویند»؛ این قاعده بر فصول هفتم و هشتم منشور ملل متحد استوار است که از رهگذر آن شورای امنیت می‌تواند برای اتخاذ اقدام اجرایی تحت اقتدار خود، به ترتیبات یا نهادهای منطقه‌ای روی آورد.

۳.۳. تحریم سیاسی و اقتصادی

یکی دیگر از ابزارهای دیپلماتیک، تحریم است. برای مثال، تحریم‌های سیاسی می‌توانند شامل تهیه لیست سیاه از افراد و سازمان‌های درگیر در حمله سایبری، محدود کردن سفر یل انجام تراکنش‌های مالی بین‌المللی را شامل شود. از سوی دیگر، تحریم‌های اقتصادی، ممکن است معاملات خاصی را با کشوری که در پشت حمله سایبری قرار دارد را ازلحاظ انجام واردات یا صادرات برخی کالاها، با مشکل مواجه سازد. اقدامات تلافی‌جویانه این‌چنینی، قطعاً ارزش بازدارندگی خواهد داشت و تا زمانی که دستورالعمل‌های روشنی در مورد چگونگی لغو تحریم‌ها نباشد، دولت تحریم شده، باید بتواند تغییر رفتار خود را اثبات نماید (Van Der Meer, 2018: 5).

۴. اقدام متقابل، به‌عنوان یک پاسخ

به‌موجب حقوق بین‌الملل، وصف متخلفانه عملیات سایبری یک دولت زیان‌دیده، درصورتی‌که عملیات مربوطه واجد شرایط اقدام متقابل باشد، رفع می‌شود. اقدامات متقابل که تنها در پاسخ به اعمال متخلفانه بین‌المللی در دسترس قرار دارند، فعل یا ترک فعل‌های یک دولت زیان‌دیده هستند که علیه دولت مسئول هدایت می‌شوند و جز در قالب اقدام متقابل، تعهد دولت نخست در قبال دولت دوم را نقض می‌کنند. هم دیوان بین‌المللی دادگستری و هم محاکم داوری، قانونی بودن اقدامات متقابل به‌موجب حقوق بین‌الملل را به رسمیت شناخته‌اند (Nicaragua Judgment, 1986: 24)[۹].

ماده ۲۲ طرح کمیسیون حقوق بین‌الملل ۲۰۰۱، درباره اقدامات متقابل در برابر فعل متخلفانه بین‌المللی، به‌عنوان یکی از معاذیر رافع مسئولیت بین‌المللی مقرر داشته است «درصورتی‌که فعل مغایر با تعهد بین‌المللی دولت، نسبت به دولتی دیگر به‌عنوان اقدام متقابل علیه دولت اخیر انجام شده باشد در صورت صحت اقدام مذکور و تا حدی که فعل مذکور مطابق فصل دوم بخش سوم اتخاذ شده باشد وصف متخلفانه بین‌المللی آن زایل می‌گردد». در برخی شرایط، ارتکاب فعل متخلفانه بین‌المللی توسط دولت می‌تواند توجیهی برای دولت زیان‌دیده باشد که برای توقف آن فعل و جبران خسارت وارده به اقدامات متقابل غیر قهری مبادرت ورزد (ابراهیم گل، ۱۳۹۲: ۱۳۹).

قاعده ۲۰ دستورالعمل تالین ۲، نیز، در جهت معرفی اقدام متقابل، مقرر داشته است «یک دولت می‌تواند در پاسخ به نقض یک تعهد حقوقی بین‌المللی که دولت دیگر در قبال او بر دوش دارد، مستحق اتخاذ اقدامات متقابل با ماهیتی سایبری یا غیر سایبری باشد»؛ هم‌چنین،

۹ See also Gabčíkovo-Nagymaros judgment, paras82–83; Naulilaa arbitral award, at 1025–1026

دیوان در رأی قضیه گابچیکو و ناگیماروس، اعلام کرد که برای آنکه اقدام متقابل توجیه‌پذیر باشد شرایط چندی لازم است: شرط اول آن است که این اقدام در پاسخ به یک رفتار خلاف بین‌المللی قبلی دولت دیگر باشد و مستقیماً علیه آن دولت هدایت شود (Gabčíkovo-Nagymaros Judgment, Para. 83). هم‌چنین، بر مبنای همین قاعده از دستورالعمل تالین ۲، «اقدامات متقابل، تنها می‌توانند از سوی دولت زیان‌دیده برای مجبور ساختن یا واداشتن دولت مسئول به ازسرگیری پایبندی به تعهدات حقوقی بین‌المللی خویش، به اجرا درآیند»؛ بند اول از ماده ۴۹ طرح مسئولیت ۲۰۰۱، هدف از اقدام متقابل را چنین معرفی نموده است «دولت زیان‌دیده، تنها می‌تواند علیه دولت مسئول، دست به اقدام متقابل بزند و هدف از این کار نیز وادار کردن آن دولت است که بر اساس تعهدات بین‌المللی خود عمل کند». قاعده ۲۱ دستورالعمل تالین ۲، نیز، در راستای بیان هدف از اقدامات متقابل، مقرر می‌دارد، «اقدامات متقابل، با ماهیتی سایبری یا غیر سایبری، تنها می‌توانند برای واداشتن دولت مسئول به پایبندی به تعهدات قانونی خویش در قبال دولت زیان‌دیده اتخاذ شوند»؛ بند اول ماده ۴۹ طرح مسئولیت ۲۰۰۱ (Articles on State Responsibility, Art. 49(1)). نیز هدف از اقدامات متقابل را وادار کردن دولت مسئول به متوقف ساختن فعل یا ترک فعل غیرقانونی خویش و هنگام ضرورت، ارائه تأمین و تضمین و جبران خسارت می‌داند؛ این اقدامات، مستمسکی هستند که به‌منظور بازگشت به روابط قانونی میان دولت‌های مربوطه طراحی شده‌اند. ازآنجایی‌که هدف از اقدامات متقابل، تشویق ازسرگیری تعاملات قانونی، یعنی سوق دادن به‌سوی متوقف ساختن یک عمل متخلفانه در حال انجام است، مخاطره تشدید وضعیت را باید حین اتخاذ تصمیم راجع به اتخاذ یا عدم اتخاذ اقدامات متقابل و چگونگی مبادرت به این کار، مدنظر قرارداد؛ در این رابطه، اقدامی که صرفاً وضعیت را به وخامت می‌کشاند، تلافی صرف بوده و بر این مبنا غیرمجاز است.

هم‌چنین، قاعده ۲۴ دستورالعمل تالین ۲، تأکید می‌کند «تنها یک دولت زیان‌دیده می‌تواند مبادرت به اتخاذ اقدامات متقابل سایبری یا غیر سایبری بنماید»؛ به‌این‌ترتیب، در نگاه اول متوجه خواهیم شد که تنها دولت‌ها می‌توانند به اتخاذ اقدامات متقابل دست بزنند. از دیگر سو، هرچند یک دولت باید «هدف و موضوع» اقدام متقابل باشد، اما نیازی نیست اقدامات متقابل، ارکان دولتی یا زیرساخت سایبری دولت را هدف قرار دهند. لازم به ذکر است که اقدامات متقابل در پاسخ به عملیاتی سایبری که توسط یک بازیگر غیردولتی انجام شده باشد، قابل‌اعمال نیستند، مگر اینکه عملیات مربوطه، به یک دولت قابل انتساب باشد.

نهادهای غیردولتی ممکن است مبادرت به عملیات‌هایی سایبری کنند که موجب نقض تعهداتی همچون ممنوعیت توسل به زور و احترام به حاکمیت دولت‌ها که بنا به ادعا در مقابل آن‌ها دارند بشوند. از رهگذر این دیدگاه، به میزانی که بازیگران غیردولتی در قبال دیگر دولت‌ها، دارای تعهدات قانونی هستند، دولت‌های «زیان‌دیده» حق‌دارند در هنگام نقض چنین تعهداتی علیه بازیگران غیردولتی مزبور به اتخاذ اقدامات متقابل دست بزنند؛ موردی را در نظر بگیرید که در آن یک گروه تروریستی مستقر در یک دولت، علیه دولت دیگر دست به عملیات‌های سایبری می‌زند و عملیات‌های مربوطه به ایراد خسارت فیزیکی به سخت‌افزارهای موجود در قلمرو دولت دوم می‌انجامند. اگر عملیات‌ها توسط یک دولت صورت می‌پذیرفتند، دست‌کم حاکمیت دولت دوم را نقض می‌نمودند. دولت نخست، همگام با تکلیف خود دایر بر اعمال مساعی مقتضی، تمامی اقدامات ممکن برای پایان دادن به عملیات‌های سایبری گروه مربوطه از قلمرو خویش را اتخاذ می‌نماید، ولی نهایتاً ناکام می‌ماند و عملیات‌ها ادامه پیدا می‌کنند. دولت هدف که کماکان از آسیب ناشی از فعالیت‌های آن گروه رنج می‌برد، وفق مؤلفه‌های این رویکرد می‌تواند علیه گروه مربوطه نسبت به اتخاذ اقدامات متقابل اقدام کند، هرچند آن اقدامات ممکن است از حاکمیت دولت نخست عدول کنند.

همان‌گونه که در داوری قضیه خدمات هوایی ابراز گردیده است، «اقدامات متقابل... باید بر مبنای عقلانیت و نه ضعف طرف دیگر باشند. آن‌ها باید باروح میانه‌روی مورداستفاده قرار گیرند و با تلاش واقعی برای حل‌وفصل اختلاف همراه گردند» (Air Services arbitral award, Para. 91). این بیان هشدارآمیز به‌ویژه در رابطه با اقدامات متقابل سایبری، موضوعیت دارد، زیرا سرعتی که عملیات‌های سایبری

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

متخلفانه می‌توانند با آن بروز یابند، خطر تبادل تلافی‌جویانه سریعی را به وجود می‌آورد که مجال اندکی را برای بررسی دقیق پیامدهای احتمالی باقی می‌گذارد.

اقدامات متقابل که هدف آن‌ها واداشتن دولت مسئول به پایبندی به تعهدات قانونی خویش است، ماهیتاً واکنشی هستند و نه معطوف به آینده. همان‌گونه که دیوان بین‌المللی دادگستری در رأی قضیه گابچیکو و ناگیماروس ابراز داشت، «این اقدامات باید در پاسخ به یک عمل متخلفانه بین‌المللی پیشین از جانب دولتی دیگر اتخاذ شوند» (Gabčíkovo-Nagymaros Judgment, Para. 83). هیچ اقدام متقابلی که با دفاع از خود پیش‌دستانه علیه یک حمله سایبری یا فیزیکی مسلحانه فوری، برابری کند، وجود ندارد؛ هم‌چنین اقدامات متقابل نباید برای اهداف پیشگیرانه به کار گرفته شوند.

اقدامات متقابل، عموماً با عنوان اقداماتی موقتی توصیف می‌شوند و بنابراین، طبق نظر کمیسیون حقوق بین‌الملل، «باید آثار آن‌ها ازلحاظ روابط حقوقی آتی میان دو کشور تا جایی که ممکن است بازگشت‌پذیر باشند» (Articles on State Responsibility, chapeau to Chapter II of Part 3, Para. 6). دیوان بین‌المللی دادگستری، با انعکاس این هدف، تأیید نموده است که اقدامات متقابل می‌بایست حتی‌الامکان به شیوه‌ای اتخاذ گردند که اجازه ازسرگیری ایفای تعهدات نقض شده مبنای اقدامات متقابل را بدهند (Articles on State Responsibility, Art. 49(3)). به‌عنوان‌مثال، عملیات قطع توزیعی خدمات، نوعاً قابل بازگشت است، درحالی‌که حذف داده‌هایی که دولت اتخاذکننده اقدامات متقابل از ذخیره نشدن آن‌ها اطلاع دارد را نمی‌توان بازگشت‌پذیر دانست. بایسته برگشت‌پذیری، موسع بوده و مطلق نیست، چون با قید صرفاً تا جایی که امکان دارد انعکاس یافته است، برای مثال، اقدام متقابل معطوف به قطع توزیعی خدمات را می‌توان پایان داد و خدمت مربوطه را بازگرداند، ولی امکان دارد فعالیت‌هایی که مختل شده‌اند را نتوان درزمانی دیگر به انجام رساند؛ این امر موجب ممنوعیت اقدام متقابل نمی‌گردد. مسأله ضروری دیگری که از هدف مبنای اقدامات متقابل ناشی می‌شود، لزوم مطلع ساختن دولت مسئول، توسط دولتی است که قصد اتخاذ اقدامات متقابل دارد، شامل استناد به مسئولیت، تصمیم به مبادرت به اقدامات متقابل و پیشنهاد مذاکره (Articles on State Responsibility, Art. 52(1)). یک اعلان واحد با چنین مضمونی می‌تواند برای تحقق بایسته مربوطه کفایت کند (Articles on State Responsibility, Art. 52, Para. 5). در برخی شرایط، امکان دارد اقدام فوری در راستای حراست از حقوق دولت و اجتناب از ورود زیان برای دولت زیان‌دیده ضرورت داشته باشد، در هنگام بروز چنین شرایطی، دولت زیان‌دیده می‌تواند بدون اعلان قصد خود به این کار، مبادرت به «اقدامات متقابل فوری» بنماید (Articles on State Responsibility, Art. 52(2)). با توجه به سرعتی که می‌توانند پیامدهای یک حمله سایبری بروز کنند، این وضعیت به‌شدت محتمل است؛ به‌این‌ترتیب، اگر اعلام قصد اتخاذ اقدام متقابل احتمالاً موجب بی‌معنا و بی‌ثمر ساختن آن اقدام گردد، نیازی به چنین اعلامی نیست (Articles on State Responsibility, Art. 52(6)). از دیگر سو، حقوق بین‌الملل عرفی و بر مبنای ماده ۵۴ طرح مسئولیت دولت، دولت زیان‌دیده را ملزم می‌سازد تا پیش از اتخاذ اقدامات متقابل، درصدد مذاکره برآید. ازآنجاکه دولت زیان‌دیده می‌تواند پیش از آن‌که درصدد مذاکره برآید مبادرت به اقدامات متقابل نماید، اقدامات متقابل در خلال مذاکرات مجاز هستند. اگر اختلاف موردنظر در حال رسیدگی در یک دیوان یا یک دادگاه بوده که ممکن است در خصوص مقوله مربوطه مبادرت به صدور تصمیمی الزام‌آور نماید و فعالیت متخلفانه بین‌المللی خاتمه یافته باشد، اقدامات متقابل را نباید اتخاذ نمود و در صورت اتخاذ باید آن‌ها را به حالت تعلیق درآورد (Articles on State Responsibility, Art. 52(3)). هم‌چنین، وفق ماده ۵۳ کنوانسیون وین راجع به حقوق معاهدات، اقدامات متقابل نباید متضمن اعمالی باشند که هنجارهای آمره، نظیر ممنوعیت نسل زدایی را نقض می‌کنند؛ چنانکه این ماده اشاره کرده است «یک قاعده حقوق بین‌الملل عام قاعده‌ای است که از سوی جامعه بین‌المللی در کل به‌عنوان قاعده‌ای که هیچ عدولی از آن جایز نیست و تنها می‌تواند به‌وسیله قاعده‌ای متعاقب در حقوق بین‌الملل با ماهیتی مشابه تعدیل شود، پذیرفته شده و مورد شناسایی قرارگرفته است»؛ هم‌چنین، اقدامات متقابلی که تعرض ناپذیری دیپلماتیک و کنسولی را مورد تخطی قرار می‌دهند، ممنوع هستند (Articles on State Responsibility, Art. 50(2) (b)). باید توجه داشت که اقدام متقابل، نمی‌تواند به

سطح یک حمله مسلحانه برسد، تعهد دایر بر خودداری از توسل به زور، محدودیتی کلیدی بر دولت زیان‌دیده در هنگام انجام اقدامات متقابل است (Articles on State Responsibility, Art. 50(1) (a)). این موضع، هم‌چنین، با رویه قضایی دیوان بین‌المللی دادگستری در قضیه کانال کورفو و قضیه نیکاراگوئه[۱۰] سازگار است.

اقدامات متقابل قهرآمیز، در پاسخ به استفاده متخلفانه از زوری که خود فاقد وصف یک حمله مسلحانه است با ابزارهای سایبری یا غیر سایبری، مناسبت دارد. دولت مواجه با استفاده از زور سایبری که به آستانه حمله مسلحانه نرسیده است نمی‌تواند با عملیات‌های سایبری یا غیر سایبری قهرآمیز به آن پاسخ دهد؛ به‌عبارت‌دیگر، دولت زیان‌دیده به پاسخ از طریق اقدامات متقابل سایبری که پایین‌تر از سطح استفاده از زور قرار می‌گیرند محدود خواهند شد و درنتیجه از ارائه پاسخی متناسب محروم خواهند گردید. دولت قربانی حملات سایبری می‌تواند علیه دولت مهاجم متوسل به اقدامات متقابل غیرنظامی شود. هرچند اقدام متقابل رفتار غیردوستانه‌ای است که با تعهدات بین‌المللی دولتی که به آن مبادرت می‌ورزد مغایر است؛ اما مقابله‌به‌مثل[۱۱] رفتار دولت در مغایرت با تعهدات بین‌المللی‌اش است که در پاسخ به یک فعل متخلفانه بین‌المللی صورت می‌گیرد و بنا بر اعلام دیوان بین‌المللی دادگستری، چنین اقداماتی اگرچه به‌خودی‌خود غیرقانونی است؛ اما چنانچه در پاسخ به یک عمل متخلفانه دولت دیگر صورت گیرد، جایز شمرده می‌شود (Gabacikovo-Nagymaros, PP.55-56). بنابراین دولت قربانی حملات سایبری زمانی می‌تواند به این اقدامات متوسل شود که عملیات و حملات سایبری انجام‌گرفته علیه او طبق موازین حقوق بین‌الملل غیرقانونی محسوب و فعل متخلفانه بین‌المللی قلمداد شود. حملات سایبری صورت گرفته باهدف وارد آوردن صدمات به دولت قربانی به دلیل مغایرت با اصل ممنوعیت توسل به زور و اصل عدم‌مداخله در امور داخلی دولت دیگر، غیرقانونی محسوب شده و به دولت قربانی حق اعمال اقدام متقابل متناسب مطابق با شروط و محدودیت‌های بیان‌شده در مواد ۵۰، ۵۱ و ۵۲ طرح مسئولیت دولت‌ها مورخ ۱۲ دسامبر ۲۰۰۱ را می‌دهد (Roscini, 2010: 114). در خصوص حمله سایبری که به حد حمله مسلحانه می‌رسد، مسلم است که دولت قربانی هم حق پاسخ سایبری و هم حمله مسلحانه را دارد، اما درجایی که حمله سایبری به آستانه حمله مسلحانه نمی‌رسد، دولت تنها حق توسل به اقدام متقابل غیرنظامی را دارد.

ازآنجاکه دولت‌ها در مقابل عمل متخلفانه بین‌المللی دولت دیگر از قبیل حمله سایبری مادامی‌که به آستانه حمله مسلحانه نرسد، حق توسل به زور به‌گونه‌ای که مغایر با منشور باشد را ندارند؛ فشارهای اقتصادی و سیاسی دو شکل عمده اقدامات متقابل هستند که مشمول این ممنوعیت نمی‌شوند. اخراج خبرنگاران، فشارها و تحریم‌های اقتصادی، قطع روابط دیپلماتیک، مسدود نمودن دارایی‌ها و اموال دولت خاطی نمونه‌ای ازاین‌دست اقدامات است که هیچ‌یک مسئولیتی برای دولت ایجاد نمی‌کند و ممنوعیتی ندارد. هر دولتی حق دارد وضعیت حقوقی خود را نسبت به سایر دولت‌ها ارزیابی نماید و در برابر وضعیتی که در آن نقض تعهد بین‌المللی توسط یک دولت دیگر صورت گرفته، حق خود را از طریق اقدام متقابل غیرنظامی استیفا نماید[۱۲].

۵. دفاع مشروع، پاسخی در مقابل حمله سایبری

اصل ممنوعیت توسل به زور، به‌عنوان یکی از اصول بنیادین جامعه بین‌المللی همچنان، بر روابط دولت‌ها حاکم است و به‌موجب منشور، دولت‌ها مکلف شده‌اند ضمن خودداری از توسل به زور و حتی تهدید به توسل به زور، اختلافات خود را از طریق روش‌های مسالمت‌آمیز حل‌وفصل نمایند. دفاع مشروع به‌عنوان مهم‌ترین استثناء بر اصل ممنوعیت توسل به زور پذیرفته شده است.

۱۰ Corfu Channel judgment, at 35; Nicaragua judgment, Para. 249.

۱۱ Reprisal.

۱۲ رأی داوری تفسیر توافقنامه میان فرانسه و ایالات‌متحده در مورد حمل‌ونقل هوایی ۱۹۸۷، مجموعه آراء داوری، جلد ۲، ص ۴۱۷.

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

ماده ۵۱ منشور ملل متحد در رابطه با دفاع مشروع، مقرر می‌دارد «در صورت حمله مسلحانه یک عضو سازمان ملل متحد تا زمانی که شورای امنیت اقدامات لازم را برای حفظ صلح و امنیت بین‌المللی به عمل آورد، هیچ‌یک از مقررات این منشور به حق دفاع مشروع انفرادی یا جمعی اعضاء لطمه‌ای وارد نخواهد کرد. اعضاء باید اقداماتی را که در اعمال این حق دفاع از خود، به عمل می‌آورند؛ فوراً به شورای امنیت گزارش دهند. این اقدامات به‌هیچ‌وجه در اختیار و مسئولیتی که شورای امنیت طبق این منشور دارد و به‌موجب آن برای حفظ و اعاده صلح و امنیت بین‌المللی در هر موقع که ضروری تشخیص دهد، اقدام لازم را به عمل خواهد آورد، تأثیری نخواهد داشت». هدف از گنجاندن عبارتی مانند حمله مسلحانه، در منشور، کاهش آزادی عمل دولت‌ها به‌منظور جلوگیری از سوءاستفاده احتمالی آن‌ها است.

ماده ۲۱ طرح مسئولیت کمیسیون حقوق بین‌الملل ۲۰۰۱، نیز، به موضوع دفاع از خود به‌عنوان یکی از معاذیر رافع مسئولیت بین‌المللی دولت پرداخته است و مقرر می‌دارد «درصورتی‌که فعل دولت، اقدام قانونی دفاع از خود بر طبق منشور ملل متحد باشد وصف متخلفانه بین‌المللی آن زایل می‌گردد». در این راستا، قاعده ۷۱ دستورالعمل تالین ۲، مقرر داشته است «دولتی که هدف عملیات سایبری‌ای قرار دارد که به سطح حمله مسلحانه رسیده است، می‌تواند حق ذاتی خود مبنی بر دفاع از خود را اعمال نماید. شکل‌گیری یا عدم شکل‌گیری حمله مسلحانه توسط عملیاتی سایبری به مقیاس و آثار آن وابسته است». بدین ترتیب، توسل هر یک از دولت‌های عضو ملل متحد به دفاع مشروع تنها در صورتی امکان‌پذیر است که حمله‌ای مسلحانه علیه آن‌ها صورت پذیرد (Tallinn Manual 2.0, 2017: Rule71, Para1). حمله مسلحانه، به‌عنوان شرط ابتدایی، باید واجد عنصری فرامرزی باشد؛ این معیار، همواره زمانی که یک دولت، مبادرت به عملیاتی سایبری می‌نماید که در حالتی دیگر حمله مسلحانه علیه دولتی دیگر به شمار می‌آید یا بازیگران غیردولتی را، فارغ از اینکه کجا مستقر باشند، برای انجام این کار به نیابت از خویش هدایت می‌کند، محقق می‌گردد.

حق توسل به زور در قالب دفاع از خود، به فراتر از حملات مسلحانه فیزیکی و حملاتی که انحصاراً از رهگذر عملیات‌های سایبری ارتکاب یافته‌اند، تسری می‌یابد. پاره‌ای از عملیات‌های سایبری می‌توانند به‌اندازه کافی برای قرار گرفتن ذیل مفهوم مخاصمه مسلحانه در معنای موردنظر منشور، شدید باشند. این نتیجه‌گیری با پافشاری دیوان بین‌المللی دادگستری در رأی مشورتی خود در قضیه‌ی تسلیحات هسته‌ای بر این‌که انتخاب شیوه حمله در مسئله مربوط به حمله مسلحانه قلمداد شدن یا نشدن یک عملیات اهمیتی ندارد سازگار است (Nuclear Weapons advisory opinion, Para. 39). به‌علاوه، این موضع با رویه دولتی، نیز هم‌خوانی دارد[۱۳]؛ به‌صورت جهان‌شمول پذیرفته شده است که حملات شیمیایی، بیولوژیکی و رادیولوژیکی واجد مقیاس و آثار لازم برای شکل‌گیری حمله مسلحانه، حق دفاع از خود را ایجاد می‌کنند. تحقق این امر به‌رغم ماهیت غیر فیزیکی آن‌هاست، زیرا پیامدهای متعاقب می‌توانند شامل رنج شدید یا مرگ باشند. استدلال مشابهی در رابطه با عملیات‌های سایبری مطرح می‌گردد.

یک حمله مسلحانه دست‌کم متضمن توسل به زور در معنای بند ۴ ماده ۲ است. بااین‌حال، همان‌گونه که توسط دیوان بین‌المللی دادگستری بیان گردید، هر توسل به زوری، به سطح یک حمله مسلحانه نمی‌رسد (Nicaragua Judgment, 1986: 191). هدف عملیاتی سایبری که ویژگی‌های فرامرزی بودن و مقیاس و آثار را محقق می‌سازد، می‌تواند حمله مسلحانه به شمار آمدن یا نیامدن آن را نیز تعیین نماید؛ اگر هدف مربوطه متضمن اموال یا اشخاص دولتی یا خصوصی موجود و حاضر در قلمرو دولت متأثر از عملیات است، اقدام مربوطه، حمله‌ای مسلحانه علیه آن کشور قلمداد می‌شود. مقیاس و آثار لازم برای یک عمل جهت توصیف آن به‌عنوان حمله‌ای مسلحانه ضرورتاً از مقیاس و آثاری که اقدامی را واجد وصف توسل به زور می‌نماید، فراتر می‌رود. تنها درصورتی‌که توسل به زور به آستانه یک حمله مسلحانه برسد، دولت حق دارد با توسل به زور در قالب دفاع از خود به پاسخ دست بزند (Tallinn Manual 2.0, 2017: Rule 71, Para6). از

۱۳ See, e.g. NATO Wales Summit Declaration, Para. 72; Government Response to the AIV/ CAVV Report, Para. 4; The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (2011), at 10, 13; DoD Manual, Para. 16.3.3.

دانشگاه آزاد اسلامی واحد مراغه

طرفی، ممکن است آثار حمله مسلحانه دولت (الف) علیه دولت (ب)، به دولت ثالث (ج) تسری پیدا کند. اگر آن آثار معیارهای مقیاس و آثار مربوط به حمله‌ای مسلحانه را محقق سازند، دولت (ج) حق دارد، مادامی‌که اقدام دفاعی مربوطه با ویژگی ضرورت و تناسب هم‌خوانی داشته باشد، در قالب دفاع از خود به زور متوسل شود. افزون بر این، حتی اگر عملیات‌های سایبری انجام شده علیه دولت (ب) حمله‌ای مسلحانه به شمار نرود، این امر مانع از حمله مسلحانه قلمداد شدن تسری آثار آن‌ها به دولت (ج) نمی‌گردد (Tallinn Manual 2.0 Rule 71, 2017: 15). دیوان بین‌المللی دادگستری در رأی قضیه نیکاراگوئه ابراز داشت: «حمله مسلحانه باید به‌گونه‌ای فهم شود که صرفاً اقدام نیروهای منظم در طول مرزهای بین‌المللی را در برنگیرد، بلکه گسیل دسته‌ها، گروه‌ها، نیروهای نامنظم یا مزدوران مسلح که به اقدامات معطوف به زور مسلحانه علیه دولت دیگر با چنان شدتی دست می‌زنند که گویی حمله مسلحانه واقعی صورت گرفته توسط نیروهای منظم یا مشارکت اساسی آن‌ها در آن به شمار می‌آید را نیز شامل گردد» (Nicaragua Judgment, 1986: 195). رویه دولتی، حق دفاع از خود در برابر عملیات‌های سایبری در سطح حمله مسلحانه توسط بازیگرانی غیردولتی همچون گروه‌های تروریستی یا شورشی که بدون مشارکت یک دولت دست به اقدام می‌زنند را به رسمیت شناخته است[۱۴]، به‌عنوان‌مثال، عملیات سایبری ویرانگر گروهی از تروریست‌ها از قلمرو یک دولت، علیه زیرساخت حیاتی مستقر در دولتی دیگر را، حمله مسلحانه تروریست‌های سایبری علیه دولت دوم به شمار آورده‌اند.

آنچه موجب ایجاد حق دفاع از خود می‌گردد، صرفاً حمله مسلحانه محسوب شدن عمل نیست، بلکه اعمال حق دفاع از خود مشمول ویژگی‌های ضرورت، تناسب، قریب‌الوقوع بودن و فوریت است. بی‌گمان، حق توسل به دفاع از خود نیز مشروط به تعیین منطقی در شرف وقوع بودن یا وقوع یافتن حمله مسلحانه و نیز هویت مهاجم است. تعیین این امور باید به‌صورت پیشینی باشد نه پسینی. منطقی بودن این تشخیص‌ها بر مبنای اطلاعات موجود در زمان تعیین آن‌ها و نه اطلاعاتی که متعاقباً به دست می‌آیند مورد ارزیابی قرار خواهد گرفت (Tallinn Manual 2.0, 2017: Rule 72, Para1).

اگرچه متن ماده ۵۱ منشور ملل متحد در رابطه باوجود حالت ضرورت، به‌عنوان شرط استفاده از حق دفاع مشروع، صراحت ندارد، اما قاعده ۷۲ دستورالعمل تالین ۲، مقرر می‌دارد «توسل به زوری که شامل عملیات‌های سایبری انجام شده توسط یک دولت در اعمال حق دفاع از خود است، باید ضروری و متناسب باشد»؛ هم‌چنین، قاعده ۷۳ دستورالعمل تالین ۲، مقرر می‌دارد، «حق به‌کارگیری زور در دفاع از خود، درصورتی‌که حمله مسلحانه سایبری رخ دهد یا قریب‌الوقوع باشد، بروز می‌کند؛ این حق، سپس تحت بایسته فوریت قرار دارد». ماده ۵۱ منشور ملل متحد، به وضعیتی اشاره دارد که در آن حمله‌ای مسلحانه رخ‌داده است. بدیهی است که این ماده وقایعی که در آن آثار حمله مسلحانه پیش‌تر پدیدار شده‌اند، یعنی زمانی که حمله مسلحانه سایبری موجب ایراد خسارت یا جراحت شده یا در حال ایراد خسارت است را در برمی‌گیرد؛ هم‌چنین ماده مزبور وضعیت‌هایی که در آن‌ها عملیات سایبری گام آغازین انجام یک حمله مسلحانه فیزیکی است را نیز شامل می‌شود. مصداق چنین وضعیتی عملیات‌های سایبری هدایت شده علیه پدافند هوایی دولت دیگر به‌منظور آماده‌سازی میدان جنگ برای نبردی هوایی است؛ حتی اگر ماده ۵۱ صراحتاً اقدام پدافندی در پیش‌دستی مقابل حمله‌ای مسلحانه را مقرر نکند، نیازی نیست دولت زمانی که دشمن در حال تدارک حمله است بیکار بماند؛ در عوض، دولت مربوطه می‌تواند به‌مجرد «قریب الوقوع» بودن حمله از خود دفاع کند. چنین اقدامی در حقوق بین‌الملل «دفاع پیش‌دستانه»[۱۵] نام دارد (Bowett, 1958: 188–189).

اقدامات معطوف به دفاع از خود تنها زمانی مجاز هستند که در عمل، حمله‌ای صورت گرفته باشد؛ دفاع از خود پیش‌دستانه ممنوع است (Brownlie, 1963; 275–278). اقدام در قالب دفاع از خود در مقابله با حمله ابتدایی که به مقصد خود نرسیده مجاز است (Dinstein, 2001: 203–204)؛ سرعت عملیات‌های سایبری معمولاً آن‌ها را از قرار گرفتن ذیل این دسته بازمی‌دارد. رویکردهای متفاوتی در رابطه با

---

۱۴ در رابطه با مواضع دولت‌ها در عرصه سایبر ازجمله بنگرید به:

DoD Manual, Para. 16.3.3.4; Government Response to AIV/CAVV Report, at 5.

۱۵ Anticipatory self-defence

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

دفاع از خود پیش‌دستانه وجود دارد (Gill, 2007: 113). یکی از رویکردها خواهان آن است که حمله مسلحانه، در شرف انجام باشد و از این رهگذر بر اقدامات پیش‌دستانه، محدودیتی موقتی بار می‌کند (Bowett, 1958: 187–192). وفق ضابطه «آخرین مجال ممکن»[۱۶]، زمانی که مهاجم، آشکارا درصدد انجام حمله‌ای مسلحانه است و دولت قربانی در صورت عدم اقدام فرصت دفاع مؤثر از خویش را از کف خواهد داد، آن دولت می‌تواند در قالب دفاع از خود پیش‌دستانه، چه سایبری و چه فیزیکی، برای مقابله با حمله مسلحانه عمل کند. به دیگر سخن، دولت مربوطه تنها در خلال آخرین مجال برای دفاع از خویش در مقابل حمله مسلحانه‌ای که در شرف وقوع است می‌تواند به‌صورت پیش‌دستانه اقدام نماید. این مجال ممکن است خود را بی‌درنگ پیش از حمله موردنظر یا در پاره‌ای مواقع خیلی قبل‌تر از وقوع آن نمایان سازد، مسئله اصلی نه نزدیکی موقتی اقدام پدافندی پیش‌دستانه به حمله مسلحانه آتی، بلکه قصور در اقدام درزمانی است که منطقاً انتظار می‌رود به ناتوانی دولت مربوطه در دفاع مؤثر از خویش به هنگام آغاز عملی آن حمله بیانجامد.

در ارزیابی چنین مواردی، باید میان اقداماتی که موجب شکل‌گیری مرحله آغازین حمله مسلحانه می‌شوند و اعمالی که صرفاً برای آماده سازی هستند قائل به تفکیک شد. مورد نصب یک بمب منطقی را در نظر بگیرید. عمل نصب درصورتی‌که احتمال وقوع شرایط مقرر برای فعال‌سازی وجود داشته باشد، یک حمله مسلحانه قریب‌الوقوع قلمداد خواهد شد؛ عمل مربوطه همانند کار گذاشتن مین‌های دریایی در مسیرهای مربوط به کشتی‌رانی است که از دریای سرزمینی دولت هدف عبور می‌کنند. چنین وضعیت‌هایی را باید از جایگذاری بدافزاری که از راه دور فعال می‌شود متمایز ساخت. اگر طرف آغازکننده تنها در حال دستیابی به توانمندی آغاز حمله‌ای مسلحانه در آینده است، معیار قریب‌الوقوع بودن محقق نمی‌شود. در رابطه با مورد دوم باید خاطرنشان ساخت که اگر آغازکننده عملاً تصمیم گرفته باشد با استفاده از بدافزار به حمله مسلحانه دست بزند، حمله مربوطه در نقطه‌ای که دولت قربانی در صورت اقدام نکردن فرصت دفاع مؤثر از خویش را از دست خواهد داد، قریب‌الوقوع می‌شود. ازآنجایی‌که اغلب در عمل ایجاد این تفکیک دشوار خواهد بود، قانونی بودن هر واکنش دفاعی با منطقی بودن ارزیابی دولت قربانی از وضعیت مربوطه و نیز سایر بایسته‌های دفاع از خود و به‌طور خاص ضرورت و تناسب، تعیین خواهد گردید (Tallinn Manual 2.0, 2017: Rule 73)[۱۷].

اقدامات صورت گرفته مشتمل بر عملیات‌های سایبری توسط دولت‌ها در اعمال حق دفاع از خود وفق ماده ۵۱ منشور ملل متحد، باید بی‌درنگ به شورای امنیت ملل متحد گزارش شوند. قصور عضوی از ملل متحد در گزارش اقداماتِ اتخاذی در دفاع از خود، مقابل یک حمله مسلحانه سایبری به شورای امنیت، نقض تعهدات او به‌موجب ماده ۵۱ است (Nicaragua Judgment, 1986: 235). باوجوداین، ضرورت ارائه گزارش را نباید به‌عنوان امری واجد ماهیت حقوق بین‌الملل عرفی تفسیر کرد. دیوان بین‌المللی دادگستری، در قضیه نیکاراگوئه به‌طور خاص این مسئله را مدنظر قرارداد. دیوان ابراز داشت «بدیهی است که در حقوق بین‌الملل عرفی، لزوم پیروی از آیینی که کاملاً به محتوای یک التزام معاهداتی وابسته است و نهادهای ایجاد شده به‌وسیله آن، شرط قانونی بودن به‌کارگیری زور در دفاع از خود نیست» (Nicaragua Judgment, 1986: 200)؛ بنابراین، قصور مربوطه دولت موردنظر را از حق خود مبنی بر اقدام در قالب دفاع از خود محروم نمی‌سازد.

طبق ماده ۵۱، حق اقدام در قالب دفاع از خود تا زمانی که شورای امنیت «اقدامات ضروری برای حفظ صلح و امنیت بین‌المللی را اتخاذ نماید» ادامه می‌یابد؛ در چنین مواردی شورا باید صراحتاً دولت را از حق دفاع از خود به‌موجب ماده ۵۱ محروم سازد؛ تنها شورای امنیت از چنین اقتداری برخوردار است و در صورت صدور دستور توقف از جانب شورای امنیت در عمل، اقدامات اتخاذ شده توسط شورا یا اقداماتی که قرار است اتخاذ شوند، باید موجب محروم شدن دولت قربانی از حق دفاع از خودگردند. اینکه یک دولت به‌صورت قانونی و در اعمال حق خویش بر دفاع از خود در مقابل حمله‌ای سایبری به انجام پاره‌ای اقدامات دست‌زده یا انتخاب کرده چنین نکند، شورای

۱۶ See, e.g. US Justice Dept. White Paper, Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who Is a Senior Operational Leader of Al–Qa'da or an Associated Force (n.d), at 7.

۱۷ See also UK Government Response to House of Commons Defence Committee's Sixth Report of Session 2012–13, Para. 10 (22 March 2013).

دانشگاه آزاد اسلامی واحد مرند

امنیت را از اقتدار خویش راجع به حفظ صلح و امنیت بین‌المللی به‌موجب فصل هفتم منشور ملل متحد محروم نمی‌سازد (Tallinn Manual 2.0, 2017: Rule 72, Para 5-6).

نتیجه‌گیری

به نظر می‌رسد در این برهه از زمان، دولت‌ها ترجیح می‌دهند در عملیات سایبری با آستانه پایین و عملیات جاسوسی شرکت کنند و با توسعه مسیرهای موازی محدود، انتقام‌جویی پنهانی و مقابله‌به‌مثل آشکار و منوط به شرایط خاصی از تناسب، فعلاً درجه‌ای از ثبات را در فضای مجازی حفظ کنند؛ دولت‌ها، هرچند که به دلیل حفظ منافع خود، تاکنون، از سیاست سکوت و ابهام در برخورد و تعقیب حملات سایبری بهره برده و اما اخیراً بعضاً دیده شده است که کشورها نسبت به تعقیب مسئول حملات تمایل نشان داده و نسبت به حفظ سیاست ابهام سکوت پیشین خود حساسیت کمتری نشان می‌دهند؛ در این شرایط، باید دانست که دولت‌ها بر اساس منابع موجود در حقوق بین‌الملل از قبیل قواعد سخت و نرم موجود، در مقابل حملات سایبری، با گزینه‌هایی از قبیل حل‌وفصل اختلافات به‌صورت مسالمت‌آمیز، ارجاع به شورای امنیت، مراجعه به دادگاه‌های بین‌المللی، اقدام متقابل و دفاع مشروع، جهت پاسخگویی، مواجه هستند. آنچه می‌تواند در استفاده محدود از نیروی سایبرنتیک موردتوجه باشد، نگرانی در مورد محدود بودن پاسخ‌هایی است که برای کشورهای قربانی، در دسترس است، ازجمله دفاع از خود و اقدامات متقابل به‌عنوان پاسخ اولیه به یک حمله سایبری. طبق قاعده ۷۱ دستورالعمل تالین ۲، «کشوری که هدف یک عملیات سایبری است که به سطح یک حمله مسلحانه افزایش می‌یابد، ممکن است از حق ذاتی خود در دفاع از خود استفاده کند». بااین‌حال، دفاع از خود فقط در عملیات واجد شرایط توسل به زور که به دلیل مقیاس و اثر قابل‌توجه، یک حمله مسلحانه را تشکیل می‌دهد قابل انجام است؛ آنچه توسل به زور را تشکیل می‌دهد لزوماً به یک حق حتی محدودتر برای اعمال دفاع از خود در برابر حمله مسلحانه اشاره دارد. درست است که حق گسترده‌تری برای اقدام متقابل در قاعده ۲۰ یافت می‌شود که چنین شرایطی را فراهم می‌کند «ممکن است دولت در پاسخ به نقض تعهدات قانونی بین‌المللی ناشی از کشور دیگری، مجاز به اقدامات متقابل باشد، خواه ماهیت سایبری داشته باشد یا نه»؛ بااین‌وجود چنین اقداماتی تحت شرایط مختلفی ازجمله اطلاع‌رسانی و تناسب است و نمی‌تواند شامل اقداماتی در حد توسل به زور باشد. هم‌چنین، مجاز بودن حملات سایبری پیش‌دستانه (به‌عنوان شکلی از دفاع از خود پیش‌بینی شده) را پذیرفتند، اما سودمندی این روش نیز با توجه به مشکلات عملی شناسایی آماده‌سازی قریب‌الوقوع حملات سایبری زیر سؤال رفته است.

چنانکه ملاحظه شد، هریک از پاسخ‌های ممکن نسبت به حمله سایبری، دارای شرایط و محدودیت‌هایی هستند که دولت‌ها را وادار می کند در انتخاب پاسخ متناسب، دقت بیشتری داشته باشند. هم‌چنین، به نظر می‌رسد، باوجود منابع غیر الزام‌آوری که تاکنون در عرصه سایبر ایجادشده‌اند و بیشتر جنبه توصیه‌ای، منطقه‌ای یا صرفاً آکادمیک دارند، دولت‌ها قاعده‌مند سازی حملات سایبری و نحوه مقابله با آن‌ها را تحت عنوان یک کنوانسیون خاص الزام‌آور، مدنظر قرارداد و نسبت به سیاست سکوت خود در برابر قاعده‌مند سازی فضای سایبر، به‌عنوان فضایی برای فعالیت‌های غیرملموس، تجدیدنظر کنند.

منابع

- ابراهیم گل، علیرضا. (۱۳۹۳). مسئولیت بین‌المللی دولت متن و شرح مواد کمیسیون حقوق بین‌الملل، تهران: گنج دانش.

- گیوکی، آذر. (۱۴۰۰). ارزیابی مؤلفه‌های تأثیرگذار بر حقوق سایبری در تحول مفهوم مسئولیت بین‌المللی دولت‌ها. رساله دکتری، دانشگاه آزاد اسلامی واحد قم.

- Aerial Incident Judgment (Israel v. Bulgaria), 26 May 1959

- American Treaty on Pacific Settlement (Pact of Bogotá), 30 April 1948

- Bowett, Derek. (1958). Self Defence in International Law. Praeger: New York.

- Brownlie, Ian. (1963). International Law and the Use of force by States. Oxford: Scholarship Online.

- Case Concerning Certain Property (Liech. v. Ger.) Judgment on preliminary objections, 10 February 2005

- Corfu Channel Case (UK and Northern Ireland v. Albania) (Merits) (1949) ICJ Reports 4, International Court of Justice.

- European Convention for the Peaceful Settlement of Disputes, 29 April 1957

- Fisheries Jurisdiction (Spain v. Can.) Judgment, 1998 ICJ 432

- Gabčíkovo-Nagymaros Judgment

- Gill, Terry D. (2007). The Temporal Dimension of Self- Defence: Anticipation, Pre-emption, Prevention and Immediacy, in International Law and Armed Conflict: Exploring the Faultlines (Michael N. Schmitt and Jelena Pejic eds).

- Government Response to the AIV/ CAVV Report

- Mavrommatis Palestine Concessions (Greece v. UK) 30 August 1924

- Monitoring Mechanism on Sanctions against UNITA Report, appended to Letter from the Chairman of the Security Council Committee established pursuant to Resolution 864 to the President of the Security Council, UN Doc. S/2001/966,12 October 2001

- NATO Wales Summit Declaration

- Nicaragua v. United States of America - Military and Paramilitary Activities in and against Nicaragua - Judgment of 27 June 1986.

- Roscini, Marco. (2010).World Wide Warfare-Jus ad bellum and the use of cyber force, Max Plank Yearbook of United Nation Law, Vol 14 No 1.

- SC Res. 1373, UN Doc. S/RES/2001, 28 September 2001

- SC Res. 1540, UN Doc. S/RES/1540, 28 April 2004

- Tallinn Manual 2.0 (2107). On The International Law Applicable to Cyber Operations, Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence (CCODCE).Cambridge University Press.

- Tehran Hostages Judgment, Paras83, 86; Vienna Convention on Consular Relations.

- The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World 2011

- UK Government Response to House of Commons Defence Committee's Sixth Report of Session 2012–13, 22 March 2013

- UN GGE 2015 Report Report, Paras26, 28(b).

- US Justice Dept. White Paper, Lawfulness of a Lethal Operation Directed against a U.S. Citizen Who Is a Senior Operational Leader of Al–Qa'da or an Associated Force (n.d).

- Van Der Meer, Sico. (2018). State-Level Responses to Massive Cyber Attacks: a policy tool box, Clingdael: Netherland Institute of International Relations.

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