Criminal Law and Criminology Studies Online ISSN: 2588-5901
Journal of the Faculty of Law and Political Science Volume: 55, Issue:3
Homepage: https://clcs.ut.ac.ir Autumn 2025

Cyber Aggression and the Right of Self-Defense Against It

Shadi Tazesh[1]✉ | Seyyed Ghasem Zamani[2] | Mehdi Abdolmaleki[3]

1. PhD. in International Law, Allameh Tabataba'i University, Tehran, Iran.
Email: shaditazesh1402@gmail.com
2. Professor, Department of International Law, Allameh Tabataba'i University, Tehran, Iran.
Email: zamani@atu.ac.ir
3. Assistant Professor, Department of International Law, Karaj Branch, Islamic Azad University, Karaj, Iran.
Email: mabdulmaleki@gmail.com

Article Info

Article type:
Research Article

Article history:
Manuscript Received:
1 May 2025
Accepted:
21 November 2025
Published online:
21 December 2025

Keywords:
Cyber Aggression,
Self-Defense,
Kampala Agreement,
Tallinn Manual,
Use of Force.

ABSTRACT

Technological advancement has undergone a huge transformation in old forms of attack in such a way that various news is heard about the attacks by governmental and non-governmental actors towards the fundamental foundations of another country's life and not necessarily the tangible borders of that land. Given that many types of modern attacks meet the criteria of aggression and on the other hand in 2010 after years of doubt and speculation states have agreed on the definition of aggression in Kampala and have drawn up an agreement and it is unlikely over the next few decades we can hope for the formation of a document to legalize these attacks one can optimistically believe that the Kampala document has such a capacity to solve the problem of legal vacuum in these years although it is not the final solution. By validating the hypothesis of the realization of aggression in cyber space, self-defense is raised against it by the violated country which can be resolved by resorting to existing rules such as Article 51 of the Charter of the United Nations and the Tallinn Guidelines in such a way that cyber-attacks must necessarily fulfill the criteria of the threshold i.e. character, gravity and scale, be consider as an armed attack and be placed within the scope of the concept of force included in the article 2(4) Charter of the United Nations. Legal requirements of self-defense such as 'necessity' and 'proportionality' should be observed towards off a 'present' or 'imminent' danger of armed cyber aggression; however, things like the variety of attackers in the cyber space and collision of non-territorial borders can make the issue of self-defense subject to new bumps.

Cite this article: Tazesh, Shadi; Zamani, Seyyed Ghasem; Abdolmaleki, Mehdi (2025). "Cyber Aggression and the Right of Self-Defense Against It". *Criminal Law and Criminology Studies,* 55(3): 3-21.
DOI: https://doi.org/10.22059/JQCLCS.2026.392754.1990

© The Author(s). Publisher: University of Tehran Press.
https://doi.org/10.22059/JQCLCS.2026.392754.1990

مطالعات حقوق کیفری و جرم شناسی

مجله دانشکده حقوق و علوم سیاسی

https://clcs.ut.ac.ir

شاپا الکترونیکی: ۵۹۰۱-۲۵۸۸

دوره ۵۵، شماره ۳

پاییز ۱۴۰۴

تجاوز سایبری و حق دفاع مشروع در برابر آن

شادی تازش[۱]✉ | سید قاسم زمانی[۲] | مهدی عبدالمالکی[۳]

۱. دانش‌آموخته دکترای حقوق بین‌الملل، دانشگاه علامه طباطبایی، تهران، ایران.

رایانامه: shaditazesh1402@gmail.com

۲. استاد، گروه حقوق عمومی و بین‌الملل، دانشگاه علامه طباطبایی، تهران، ایران.

رایانامه: zamani@atu.ac.ir

۳. استادیار، گروه حقوق بین‌الملل، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران.

رایانامه: mabdulmaleki@gmail.com

اطلاعات مقاله

نوع مقاله:

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۴/۰۲/۱۱

تاریخ پذیرش:
۱۴۰۴/۰۸/۳۰

تاریخ انتشار:
۱۴۰۴/۰۹/۳۰

کلیدواژه‌ها:

تجاوز سایبری،
دفاع مشروع،
توافق کامپالا،
راهنمای تالین،
توسل‌به‌زور.

چکیده

فناوری‌های جدید، اشکال قدیمی حمله را دستخوش دگرگونی نموده‌اند، به‌نحوی‌که اخبار متعددی از حملات کنشگران غیردولتی و دولتی به بنیادهای حیاتی یک کشور و نه الزاماً مرزهای ملموس آن سرزمین، به گوش می‌رسد. ازآنجاکه در سال ۲۰۱۰، دولت‌های عضو اساسنامه دیوان کیفری بین‌المللی در کامپالا جنایت تجاوز را تعریف نمودند، می‌توان خوش‌بینانه باور داشت که سند کامپالا از این ظرفیت برخوردار است که راهگشای مسئله خلأ قانونی در حملات سایبری باشد، هر چند که راه‌حل نهایی نیست. با صحه نهادن بر امکان تحقق تجاوز در فضای سایبری و به‌تبع، دفاع مشروع در مقابل آن، با توسل به قواعد موجود، چون ماده ۵۱ منشور ملل متحد و دستورالعمل تالین می‌توان به چاره‌جویی پرداخت. بااین‌حال حملات سایبری باید الزاماً به آستانه مورد نیاز یعنی ماهیت، شدت و گستره برسد تا حمله مسلحانه تلقی شده و در محدوده مفهوم «زور» مندرج در ماده ۲(۴) منشور ملل متحد جای گیرد. الزامات حقوقی دفاع مشروع نظیر «ضرورت»، «تناسب» و «فوریت» باید در مقابله با تجاوز سایبری رعایت شوند، هرچند مواردی چون تنوع عاملان حمله در فضای سایبر و درهم نوردیدن مرزهای غیرسرزمینی می‌تواند موضوع دفاع مشروع را دستخوش دست‌اندازهای نوینی نماید.

استناد: تازش، شادی؛ زمانی، سید قاسم؛ عبدالمالکی، مهدی (۱۴۰۴). تجاوز سایبری و حق دفاع مشروع در برابر آن. *مطالعات حقوق کیفری و جرم‌شناسی*، ۵۵(۳)، ۲۱-۳.

DOI: https://doi.org/10.22059/JQCLCS.2026.392754.1990

ناشر: مؤسسه انتشارات دانشگاه تهران.

© نویسندگان.

https://doi.org/10.22059/JQCLCS.2026.392754.1990

۱. مقدمه

به‌موازات تکامل فضای سایبری، نظام بین‌المللی با موانع و چالش‌های نوین برای مقابله با زور سایبری مواجه شده است. کنشگران غیردولتی با کسب مهارت و تخصص لازم و با استفاده از سلاح‌های غیرسنتی، مبادرت به برپایی جنگ‌های نامتقارن کرده‌اند که به‌مراتب آثار و نتایج مخرب‌تری را به همراه دارند. وضع قواعد بین‌المللی از سوی دولت‌ها متناسب با پدیده‌های نوظهور اصولاً زمان‌بر است، به همین دلیل نظام حقوق بین‌الملل لاجرم باید خود را با این واقعیت همسو کرده و با کاربست قواعد موجود به دنبال راهبردهای عملی برای نظام‌مند ساختن آنها برآید.

اقدام به گنجاندن جنایت تجاوز در زمره جرائم موضوع ماده ۵ اساسنامه رم و سپس اجماع بر تعریفی مشخص از آن در کنفرانس بازنگری کامپالا، نشان‌دهنده آن است که اراده جامعه بین‌المللی می‌تواند بر موانع فائق آید. با این وصف، عوامل ناپیدایی در سیر قانونمندسازی می‌توانند امکان وضع قواعدی جامع‌ومانع را با محدودیت مواجه نمایند. بر این اساس تعریف مندرج در موافقت‌نامه کامپالا، که فراز و نشیب‌های فراوانی را تا تصویب پشت سر نهاد، به دلیل چشم‌پوشی از گونه‌های مدرن تجاوز، از تحقق هدف بنیادین جرم‌انگاری این مفهوم بازماند. ازاین‌رو زمان آن فرا رسیده که مشخص شود اقدامات تجاوزکارانه، اعم از کلاسیک یا مدرن، چه زمانی به آستانه ضروری برای تحقق تجاوز می‌رسند. به نظر می‌رسد در این مسیر حقوق‌دانان در ارائه دکترین و تفسیر باید از خود انعطاف‌پذیری نشان دهند و تابع محض دولت‌ها برای چاره‌اندیشی نباشند. درست است که حملات سایبری کاملاً با چهارچوب بین‌المللی سنتی توسل‌به‌زور مطابقت ندارد بااین‌حال با تلاش‌های صورت‌گرفته در زمینه جرم‌انگاری جنایات بین‌المللی، می‌توان قائل به این بود که «مشکل واقعی در مورد حقوق و فضای سایبری، فقدان «حقوق» به‌خودی‌خود نیست، بلکه در پیچیدگی واقعیاتی است که حقوق باید در مورد آنها اعمال گردد» (Richardson, 2011).

این مقاله، در پی پاسخ به این پرسش بنیادین است که با توجه به تحولات نوین در اشکال توسل‌به‌زور، آیا می‌توان حملات سایبریِ واجد شدت و گستره کافی را در زمره جنایت تجاوز موضوع موافقت‌نامه کامپالا جای داد؟ در صورت پاسخ مثبت، دولت قربانی تا چه حد می‌تواند با تکیه بر ماده ۵۱ منشور ملل متحد، به دفاع مشروع متوسل شود؟ پاسخ به این پرسش‌ها مستلزم پیمایشی منطقی و گام‌به‌گام است؛ ازاین‌رو مقاله بر اساس سه مؤلفه اساسیِ هر تحلیل حقوقیِ کیفری ـ بین‌المللی ساختار یافته است؛ «تعریف و عناصر جرم» (بخش نخست)، «شرایط احراز و اعمال دفاع مشروع» (بخش دوم) و «موانع و چالش‌های فرارو» (بخش سوم)؛ که هر سه درنهایت به پاسخ نهایی در بخش نتیجه‌گیری منتهی می‌شوند. برای نیل به این هدف، نخست با واکاوی عناصر سه‌گانه جنایت تجاوز (قانونی، مادی و روانی) در پرتو اساسنامه رم و موافقت‌نامه کامپالا، ظرفیت‌ها و تنگناهای تعریف موجود در انطباق با حملات سایبری بررسی می‌شود و با تکیه بر اختیارات تفسیری قضات دیوان کیفری بین‌المللی و غیرحصری بودن فهرست اقدامات تجاوزکارانه، امکان قیاس و تسری تعریف به مصادیق نوین تبیین می‌گردد. سپس با استناد به ماده ۴(۲) منشور و معیارهای هشت‌گانه دستورالعمل تالین، آستانه تحقق «توسل‌به‌زور» و «حمله مسلحانه» در فضای سایبری ترسیم شده و در گام بعد، الزامات سه‌گانه «ضرورت»، «فوریت» و «تناسب» در مقام دفاع مشروع سایبری، همراه با چالش‌های ناشی از ناشناس بودن عاملان و دشواری انتساب، مورد ارزیابی نقادانه قرار می‌گیرد. این سه بخش، به ترتیب منطقی از «ثبوت جرم» تا «قابلیت دفاع» و درنهایت «موانع عملی» را پوشش می‌دهند و با توجه به اینکه وزن اصلی بحث بر دو رکن «تعریف جرم» و «دفاع مشروع» استوار است، بخش سوم به‌عنوان حلقه تکمیلی و تبیین‌کننده دشواری‌های اجرایی، به‌اختصار اما به‌اندازه کفایت مورد بررسی قرار گرفته است. در پایان، ضمن تأکید بر ضرورت تفسیر موسع و پویا از قواعد موجود و نیز توجه به

رویه دولت‌ها، این نتیجه حاصل می‌شود که هرچند تعریف کامپالا به‌صراحت متضمن حملات سایبری نیست، اما با بهره‌گیری از ظرفیت‌های تفسیری و استناد به دستورالعمل تالین، می‌توان قائل به تحقق تجاوز سایبری و اعمال دفاع مشروع شد، مشروط بر آنکه معیارهای آستانه‌ای و الزامات حقوقی مربوطه با انعطاف‌پذیری لازم و متناسب با ماهیت خاص این فضا احراز گردند.

۲. جنایت تجاوز در پرتو توافق‌نامه کامپالا

اختلاف‌نظر دولت‌ها در کنفرانس رم درخصوص جنایت تجاوز (شایگان‌فرد، ۱۳۸۷: ۲۵۷)، عمدتاً مربوط به حدود و گستره آن بود. برخی دولت‌ها، شمول تعریف عمل تجاوزکارانه مندرج در قطعنامه ۳۳۱۴ مجمع عمومی را خیلی موسع دانسته و خواستار تعریفی مضیق‌تر بودند، ولی شمار بیشتری تعریف مزبور را جامع‌ومانع دانسته و خواستار انعکاس همان تعریف به‌عنوان جنایت تجاوز بودند (موسی‌زاده و فروغی‌نیا، ۱۳۹۱: ۱۳۱). سال ۲۰۱۰، دولت‌ها به‌جای پافشاری بر مواضع سیاسی خود، رسیدن به نتیجه قطعی را هدف قرار دادند (Barriga & Kress, 2012: 3)؛ با وجود این به علت ملاحظاتی از پذیرش تعریفی موسع از تجاوز اجتناب نمودند (Glennon, 2010: 112) و مواضع میانه‌ای را برگزیدند. دولت‌ها «برای دستیابی به توافق میان کشورهای مخالف، شماری از روش‌های پیش‌نویس[1] ازجمله «ابهام سازنده»[2] را به کار گرفتند... نتیجه عملی، چه خوب چه بد، محول کردن وظیفه تفسیر تعریف جنایت تجاوز و شرایط صلاحیتی آن به قضات دیوان بین‌المللی کیفری بود» (Weisbord, 2011: 86). با وجود اینکه تعریف حاصل اجماع بود، اما واکنش‌ها به تعریف جدید گیج‌کننده بود و بسیاری اظهار نگرانی کردند که این تعریف، قابلیت اعمال اندکی بر اشکال جدید جنگ خواهد داشت (Bassiouni, 2013). حملات سایبری، هواپیماهای بدون سرنشین[3] و حملات شیمیایی و بیولوژیکی که توسط کنشگران غیردولتی هدایت می‌شوند، به‌سختی در مفهوم کلاسیک جنگ، که از جنگ جهانی دوم و جنگ سرد ترسیم شده است، جای می‌گیرند (اسمعیل‌زاده ملاباشی، ۱۳۹۶: ۴۳).

۲. ۱. عناصر جنایت تجاوز

تدوین‌کنندگان اساسنامه دیوان بین‌المللی کیفری، عناصر جرائم بین‌المللی مشتمل بر عناصر قانونی، مادی و معنوی را در سند عناصر پیوست اساسنامه آورده‌اند که در ادامه مورد بررسی قرار می‌گیرند.

۲. ۱. ۱. عنصر قانونی

جرم‌انگاری جنایت تجاوز در ماده ۸ مکرر اساسنامه دیوان بین‌المللی کیفری، گام بلندی در جهت رفع خلأ قانونی و مبارزه با بی‌کیفری مرتکبان تجاوز است.[4] مطابق ماده ۲۱ اساسنامه رم، دیوان باید اساسنامه‌اش را در کل، که متشکل از قواعد رسیدگی و ادله، معاهدات و اصول و قواعد حقوق بین‌الملل قابل اجرا است، اعمال کند (Rome Statute, art. 21(1)(a)(b)). چنانچه این منابع برای رسیدگی به پرونده مطروحه کافی نباشد، از قضات انتظار می‌رود «اصول کلی حقوقی منبعث از ... قوانین ملی نظام‌های حقوقی جهان» (Ibid, art. 21(1)(c)) و «رویه قبلی‌اش» (Ibid, art. 21(2)) را در نظر گیرند.

در مواجهه با خلأ قانونی و ابهامات نیز قضات دیوان باید قواعد تفسیر را به کار بسته تا خلأ را پر

1. Drafting
2. Constructive ambiguity
3. Drone attacks
4. Resolution RC/Res.6

نموده یا ابهام را برطرف و حکمی مستدل صادر کنند، نه آنکه از اعتبار و قدرت قانون بکاهند و آن را زیر سؤال برند. بدین ترتیب با اختیار تفسیری که به قضات دیوان اعطا شده، تعریف موجود، قابلیت انعطاف و تطابق با اشکال جدید تجاوز، ازجمله تجاوز سایبری را خواهد داشت و عذر عنصر قانونی در مورد تجاوز سایبری مرتفع می‌گردد. با وجود این نکته اساسی در پاسخ به شبهه نقض اصل قانونی بودن، آن است که در حقوق کیفری بین‌المللی، برخلاف برخی نظام‌های حقوقی داخلی با رویکرد کاملاً مضیق، تفسیر قضایی همواره نقشی پویا در انطباق قواعد با پدیده‌های نوظهور ایفا کرده است. ماده ۲۲(۲) اساسنامه رم به‌صراحت مقرر می‌دارد که «تعریف یک جرم باید به‌طور مضیق تفسیر شده و به قیاس تسری داده نشود. در صورت ابهام، تفسیر به نفع متهم انجام می‌شود» (اصل تفسیر مضیق). بااین‌حال این اصل مانع از آن نیست که قاضی با استفاده از روش‌های معتبر تفسیر (ازجمله تفسیر لفظی، سیستمی و غایی) دامنه شمول یک قاعده را که به‌وضوح ظرفیت انطباق با مصادیق جدید را دارد، توسعه دهد. آنچه ماده ۲۲(۲) ممنوع می‌کند، «قیاس» به معنای توسل به قیاس محض برای ایجاد جرم جدیدی است که در نص نیامده، اما در جایی که عناصر مادی و معنوی جرم با تفسیر از متن قابل استنباط باشد و قاضی صرفاً با بهره‌گیری از مفاهیم کلی موجود (همچون «ماهیت، شدت و گستره» در ماده ۸(۱) مکرر) به تطبیق مصداق جدید با قاعده موجود می‌پردازد، این اقدام در چهارچوب تفسیر قضایی قرار می‌گیرد و «قیاس ممنوع» محسوب نمی‌شود.

گذشته از این، نکته بنیادین درخصوص جنایت تجاوز این است که ماده ۸(۲) مکرر اساسنامه، جرم تجاوز را به‌صورت یک «تعریف کلی» همراه با «فهرستی تمثیلی» از مصادیق وضع کرده است و نه یک فهرست حصری و انحصاری. عبارت آغازین این ماده («اعمال ذیل») در کنار عنصر آستانه‌ایِ مندرج در ماده ۸(۱) مکرر (نقض آشکار و فاحش منشور بر اساس ماهیت، شدت و گستره) نشان می‌دهد که قانونگذار بین‌المللی به‌عمد از ارائه فهرست حصری خودداری کرده است؛ چراکه نخست، آگاهی از تحولات آینده در شیوه‌های توسل‌به‌زور داشته و دوم، قصد نداشته با شمارش محدود اقدامات، راه را بر توسعه قضایی بر اساس معیارهای عینی و ماهوی ببندد؛ بنابراین آنچه در مورد حملات سایبری رخ می‌دهد، خلق جرم جدید از طریق قیاس نیست؛ بلکه تطبیق عنوان مجرمانه موجود (تجاوز) بر مصداقی نوین (حمله سایبریِ واجد شرایط شدت، گستره و ماهیت) است که با معیارهای تعیین‌شده در تعریف قانونی مطابقت دارد. این رویکرد نه نقض اصل قانونی بودن، بلکه به‌کارگیری تفسیر پویا در چهارچوب اصول پذیرفته‌شده حقوق کیفری بین‌المللی است؛ به‌ویژه آنکه ماده ۲۱ اساسنامه به قضات اجازه می‌دهد از اصول کلی حقوقی و رویه قبلی خویش بهره گیرند و در مواجهه با خلأها و ابهامات، از اعتبار و قدرت قانون نکاهند.

۲. ۱. ۲. عنصر مادی: رفتار[1]

در تعریف جنایت تجاوز در ماده ۸(۱) مکرر اساسنامه رم، به چهار نوع مشارکت: طراحی، تدارک، آغاز و ارتکاب عمل تجاوزکارانه اشاره شده که تنها توسط رهبران سیاسی یا نظامی می‌تواند ارتکاب یابد؛ بدین ترتیب این جنایت در زمره «جنایت رهبران» جای می‌گیرد و سایر بازیگرانی که امروزه نقش‌آفرینی پررنگی در حوادث و وقایع اسف‌بار دارند، نادیده گرفته می‌شوند. ازاین‌جهت جنایت تجاوز متفاوت از سایر جنایات تحت صلاحیت اساسنامه رم است؛ زیرا جنایات جنگی، جنایت علیه بشریت و نسل‌کشی چنین شرطی را قید نکرده‌اند. اساساً هدف گروه کاری از گنجاندن شرط فرماندهی در این ماده، این بود که قابلیت ارتکاب جنایت تجاوز محدود به افرادی باشد که در سمت بوده و اعمال کنترل مؤثر می‌کنند یا اقدامات سیاسی یا نظامی دولت را هدایت می‌نمایند (International Criminal

1. Conduct Verbs

Court [ICC], 2009). بدین ترتیب درحالی‌که اشکال مشارکت، اقسام گسترده‌ای از فعالیت‌های مسئولیت‌زا را دربرمی‌گیرد، احراز آن به‌طور اجتناب‌ناپذیری به شرط فرماندهی گره خورده است.

ازآنجاکه حملات سایبری بدون فرماندهی نیز قابل تحقق هستند، لذا شرط فرماندهی می‌تواند مانع قابل ملاحظه‌ای برای قابلیت اعمال این تعریف بر حملات سایبری باشد. به‌ویژه آنکه تعداد معتنابهی از حملات سایبری عمدتاً با هدف تأمین منفعت مالی توسط گروه‌های غیر وابسته به دولتی معین انجام می‌شوند (Solce, 2008: 301). حتی در برخی موارد که حملات سایبری شرط فرماندهی را دارد، ازآنجایی‌که از سوی دولت نیست، امکان اعمال صلاحیت دیوان بر آن وجود ندارد، زیرا عبارات «توسط یک دولت» و «از یک دولت» مندرج در قطعنامه ۱۹۷۴، در ماده (۲)۸ مکرر به‌منظور تأکید بر ارتکاب اقدامات تجاوزکارانه توسط بازیگران دولتی تکرار شده و پیوندی که میان اشکال مشارکت و شرط فرماندهی وجود دارد، نمایانگر آن است که شمار زیادی از حملات سایبری که توسط کنشگران غیردولتی ارتکاب می‌یابند، از حیطه مقررات بین‌المللی خارج می‌گردند. در تأیید این امر، به نظر دادگاه بین‌المللی یوگسلاوی سابق، «عاملی که می‌توان بر اساس آن مقامات مافوق را مسئول شناخت، داشتن یا نداشتن قدرت کنترل واقعی نسبت به اعمال زیردستان است» (ICTY, Celebici, Judgment, para.378). بدین ترتیب چنانچه حملات سایبری از سوی سرباز عادی که در سلسله‌مراتب دولت متجاوز خدمت می‌کند هدایت شود، مطابق اساسنامه رم (ماده (۳)۲۵ مکرر) نمی‌توان او را به‌عنوان شریک یا معاون جنایت مجازات نمود. درست است که متناسب با ویژگی خاص فضای سایبر، امکان مطابقت رفتار و حملات سایبری وجود دارد، اما همچنان تنگناهایی پیش روی احراز تجاوز سایبری قرار دارد. به‌عنوان مثال تاکتیک سایبری ایجاد «در پنهان»[1] در مجموعه‌ای از شبکه‌ها به‌منظور دسترسی آسان، می‌تواند به‌عنوان گامی ابتدایی برای تجاوز تلقی گردد (Ophardt, 2010: 15)؛ اما این استفاده متقلبانه، دشواری‌هایی را در انتساب مسئولیت ایجاد می‌کند و ضرورت طرح دکترین مسئولیت را در جرم تجاوز پیش می‌کشد.

۲. ۱. ۳. عنصر روانی:[2] دشواری احراز

بر اساس ماده ۳۰ اساسنامه رم، به‌جز موارد استثنایی، قصد و علم همراه با عنصر مادی جنایت ضروری است. با لحاظ این ماده، بند ۶ ماده ۸ مکرر سند عناصر جنایات مقرر می‌دارد: «مرتکب نیز از شرایط و اوضاع‌واحوال واقعی که چنین نقض آشکاری[3] منشور سازمان ملل متحد را مسلم می‌دارد، آگاهی داشته باشد». این مقرره احراز جنایت تجاوز و قابلیت انتساب مسئولیت را با محدودیت‌هایی مواجه می‌کند. به‌عنوان مثال زمانی که حمله سایبری خفیفی به بانکی صورت می‌گیرد و هم‌زمان حملاتی توسط دولت علیه اهداف نظامی آن کشور آغاز شده، چنانچه ارتباطی میان آن دو حمله نتوان برقرار کرد، حمله سایبری به بانک قسمتی از تجاوز نخواهد بود (Barriga & Kress, op. cit: 58, 75-76).

علاوه بر موارد مذکور، آنچه احراز عنصر روانی را در حملات سایبری دشوارتر می‌سازد، پیش‌بینی پیامدهای ناشی از حمله است؛ بدین معنی که در مواردی مرتکب قصد برجای گذاشتن نتایجی را دارد، اما در جریان عادی امور، وقایع دیگری نیز به وقوع می‌پیوندند. برای مثال هدف نهایی کرم استاکس‌نت، سانتریفیوژهای ایران بود، اما درنهایت در سطح وسیع‌تری انتشار یافته و بسیاری از سیستم‌هایی را که دارای نرم‌افزار PLC بودند، متأثر ساخت. به‌علاوه به طرز غیرقابل پیش‌بینی، به

---

1. Trapdoor

معنای استعاری و رایانه‌ای (Trapdoor): این عبارت در حوزه امنیت رایانه و رمزنگاری به کار می‌رود و به یک «در پشتی» (Backdoor) یا نقص عمدی در یک سیستم کامپیوتری گفته می‌شود که امکان دسترسی غیرمجاز به اطلاعات را فراهم می‌کند.

2. Mens Rea

3. Manifest Violation

نرم‌افزار کنترل لوله‌های نفت، جریان برق و... نیز خساراتی وارد نمود. حال چنانچه نتایج پیش‌بینی‌نشده، معیار آستانه نقض فاحش را محقق سازد، آیا می‌توان برچسب عمل تجاوز سایبری بر آن نهاد؟ به نظر می‌رسد پاسخ به این پرسش مثبت است. بدین معنی که ورود خسارت معیار، ارزیابی اینکه یک حمله به آستانه تجاوز رسیده است یا خیر، نیست. با وجود این ورود خسارت می‌تواند قرینه‌ای آشکار بر تحقق تجاوز باشد. ضمن آنکه قصد ورود خسارت نیز ضابطه تحقق تجاوز تلقی نمی‌شود. کما اینکه در سند عناصر جرم اساسنامه دیوان کیفری بین‌المللی نیز نه ورود خسارت و نه قصد ایراد خسارت، عنصر جنایت محسوب نشده‌اند. در این صورت چنانچه وضعیتی با این ویژگی به دیوان بین‌المللی کیفری ارجاع شود، دیوان اگر دریابد که اقدام تجاوز معیار آستانه را برآورده ساخته، امکان رسیدگی درخصوص جنایت تجاوز وجود داشته و قصد یا عدم قصد مرتکبان، تأثیری در مسئولیت آنان نخواهد داشت.

۲. ۲. عمل تجاوز

قضات دیوان در فرایند رسیدگی دو وظیفه را ایفا می‌نمایند: ۱- تعیین اقدام تجاوزکارانه؛ ۲- رسیدن عمل ارتکابی به آستانه‌ای که سبب طرح مسئولیت کیفری بر اساس اساسنامه دیوان گردد. مورد اول مربوط به مرحله صلاحیت رسیدگی است که شعبه مقدماتی در مورد قابلیت پذیرش پرونده تصمیم‌گیری می‌کند. مورد دوم مربوط به مرحله محاکمه است. در بخش بعد، دو مسئله بررسی می‌شود که قاضی باید درباره آنها تصمیم‌گیری کند: نخست، آیا نقض فاحش منشور ملل متحد رخ داده است و دوم، کدام اقدامات را می‌توان تجاوزکارانه تلقی کرد؟

۲. ۲. ۱. اقدامات تجاوزکارانه

ماده (۲)۸ مکرر، «عمل تجاوز» را «به‌کارگیری زور نظامی توسط یک دولت بر ضد حاکمیت، تمامیت ارضی یا استقلال سیاسی دولت دیگر» تعریف می‌کند. این ماده عیناً هفت مورد مذکور در ماده ۳ قطعنامه ۳۳۱۴ را به‌عنوان مصادیق اعمال تجاوزکارانه بیان نموده که عمدتاً مربوط به شیوه‌های کلاسیک نبرد هستند و این سؤالات را در ذهن برمی‌انگیزاند که با توجه به ظهور اشکال نوین جنگ، ازجمله تجاوز سایبری، آیا این تعریف منسوخ شده است؟ آیا فهرست اقدامات ذکرشده محصور است؟

در کنفرانس کامپالا، کارگروه ویژه جنایت تجاوز با دشواری‌هایی مواجه شد. از جمله اینکه بسیاری از کشورها بر این عقیده بودند که واگذاری تعریف تجاوز به صلاحدید شورای امنیت، اصل قانونی بودن را نقض می‌کند (International Criminal Court, Assembly of States Parties, 2007, p. 87) و بنابراین تصمیم گرفتند ماده ۴ قطعنامه را کنار بگذارند. با وجود این، سؤال مطروحه این است که آیا ماده ۴ قطعنامه، تفسیر تعریف کارگروه را تحت تأثیر قرار می‌دهد؟ به‌عبارت‌دیگر کارگروه مقرر نموده که اقدامات ویژه‌ای «مطابق با» قطعنامه ۳۳۱۴، به‌عنوان اقدامات تجاوزکارانه توصیف شوند. بر این اساس آیا می‌توان مقررات قطعنامه ۳۳۱۴ را که در تعریف کارگروه نیامده، در تفسیر لحاظ نمود؟ آیا قطعنامه ۳۳۱۴ به‌طور تلویحی در تعریف کارگروه گنجانده شده است؟ پاسخ به این ابهامات، مستلزم توسل به قواعد تفسیر است. بااین‌حال نمی‌توان منکر این نکته شد که دادرس نیز باید در انجام وظیفه خود نقشی سازنده و خلاق داشته باشد. بدون تردید دادرس سعی نمی‌کند خالق قاعده باشد؛ اما به‌هرحال حریمی نیز برای شخص او قائل شده‌اند که به کشف و گاهی انشای اراده دولت‌ها بپردازد (اراده مفروض) یا برای شفاف کردن نظام‌مند اصولی اقدام کند که راهبر اقدامات دولت‌ها باشد (سالمون، ۱۳۸۲: ۲۳۷). بدین ترتیب پاسخ به پرسش بالا بستگی به میزان اختیاری دارد که به‌منظور تفسیر برای قضات دیوان قائل هستیم؛ چنانچه قضات، آن را به معنای «مطابقت با» تمام

قطعنامه ۳۳۱۴ تفسیر کنند، در این صورت شامل ماده ۴ محذوف نیز شده و درنتیجه احراز اقدامات تجاوزکارانه توسط شورای امنیت ورای فهرست احصاشده را هم دربرمی‌گیرد. در مقابل اعتقاد بر این است که ضرورتی ندارد دیوان با عبارت «مطابق با»، خود را این‌گونه محدود کند. دلایلی که برای تقویت این موضع‌گیری بیان شده، این است که نخست، عنایت به پیشینه مذاکرات و کارهای مقدماتی به‌خوبی گویای آن است که به دنبال عدم درج ماده ۴ قطعنامه ۳۳۱۴ در ماده (۲)۸ مکرر، مذاکره‌کنندگان تمایل نداشته‌اند خود را مقید و ملتزم به تصمیم شورای امنیت بدانند (December 2007 SWGCA Report: op.cit, paras. 20-21). دوم، توجه به محل قرار گرفتن عبارت «مطابق با» نشان می‌دهد مذاکره‌کنندگان درصدد اجرای دقیق قطعنامه ۳۳۱۴ نبوده‌اند، بلکه علت تمایل رجوع به این قطعنامه این بوده که فهرست اقدامات کلمه‌به‌کلمه از آن گرفته شده است (Barriga & Kress, op.cit: 27). سوم، چنین قرائتی با هدف قید «بدون پیش‌داوری»[1] در ماده (۹)۱۵ مکرر و ماده (۴)۱۵ مکرر مغایر است، زیرا موارد مزبور تضمین‌کننده این موضوع است که دیوان تحت تأثیر تصمیمات سیاسی شورای امنیت در تعیین اقدامات تجاوزکارانه قرار نخواهد گرفت. با وجود این با توجه به نقش و اختیارات قاضی در رسیدگی قضایی و با ملاحظه عبارت‌پردازی ماده پیش رو، این‌گونه می‌نماید که حتی در صورت موافق بودن با عقیده مخالفان، فهرست اقدامات مندرج در ماده (۲)۸ مکرر، محصور نیست که برای توجیه این ادعا می‌توان دلایلی را برشمرد. اول اینکه، توجه به واژگان و معنای معمولی ماده، گویای آن است که اگر پیش‌نویسان در پی احصای موارد مذکور بودند، ساده‌ترین راه استفاده از عبارت «صرفاً اعمال ذیل» به‌جای واژه «هر» بود؛ دوم، تاریخچه مذاکرات نشان می‌دهد که یکی از دلایل برشمردن مواردی از اقدامات تجاوزکارانه توجه به اصل قانونی بودن بوده است (Miller, 2014: 232)؛ به‌علاوه گروه کاری در گزارش ۲۰۰۸ ژانویه خود اظهار داشت که «ارائه تعریف کلی در صدر پاراگراف دوم، همراه با فهرست احصانشده اقدامات تجاوزکارانه ... به‌منظور تعادل حق[2] صورت گرفته است (International Criminal Court [ICC], 2008, para. 34). درحقیقت درج این عبارت برای برقراری موازنه میان آرای متضاد در گروه کاری بود که آیا فهرست اعمال تجاوزکارانه محصور باشد یا غیرمحصور (Weisbord, Ibid: 182-183). هدف نهایی تأمین اصل قانونی بودن بود، اما از دیگر سو مانعی بر تفسیر موسع این فهرست وجود ندارد (SWGCA 2009 Report, op.cit). بدین ترتیب عبارت‌پردازی نهایی، حاصل مذاکرات سیاسی بوده که تفسیر نهایی را بر عهده قضات گذاشته است؛ بنابراین می‌توان نتیجه گرفت که تعریف ارائه‌شده صرفاً نمونه‌های بارز از اقداماتی هستند که به‌تازگی به‌عنوان تجاوز در حقوق بین‌الملل عرفی پذیرفته شده‌اند (Military and Paramilitary Activities (Nicar. V. U.S), 1986 I.C.J. 14 (June 27); Weisbord: op.cit).

نکته محوری در انطباق حملات سایبری با تعریف تجاوز، تبیین دقیق قرابت میان دو مفهوم «استفاده از زور مسلحانه توسط دولت» در ماده (۲)۸ مکرر اساسنامه رم و «عملیات سایبری» است. ماده مذکور، «عمل تجاوز» را «استفاده از زور مسلحانه توسط یک دولت علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی دولت دیگر» تعریف کرده و فهرستی از مصادیق کلاسیک را ارائه می‌دهد که همگی ناظر به عملیات جنبشی و متکی بر نیروهای مسلح متعارف هستند. بااین‌حال تفسیر قضایی و دکترین حقوقی بر این نکته تأکید دارند که معیار تعیین‌کننده در تشخیص «اقدام تجاوزکارانه»، صرفاً وسیله ارتکاب نیست، بلکه پیامد و شدت اثر آن است. در دستورالعمل تالین، کارشناسان به‌اتفاق بر این نظرند که یک عملیات سایبری در صورتی می‌تواند به‌عنوان «استفاده از زور» یا «حمله مسلحانه» تلقی شود که پیامدهای آن (مانند تلفات انسانی، تخریب فیزیکی اموال، یا اختلال گسترده و پایدار در

1. Without Prejudice
2. Right Balance

زیرساخت‌های حیاتی) با پیامدهای یک حمله کلاسیک مسلحانه قابل قیاس باشد و این رویکرد مبتنی بر «مقیاس و پیامدها» در رأی دیوان در قضیه نیکاراگوئه نیز پشتیبانی می‌شود؛ بنابراین آنچه یک اقدام را به «استفاده از زور مسلحانه» بدل می‌سازد، در درجه نخست شدت، گستره و ماهیت اثرات تخریبی آن است، نه صرفاً نوع ابزار به‌کاررفته؛ به‌گونه‌ای که ویروسی که خطوط لوله نفت را منهدم می‌کند یا سیستم کنترل ترافیک هوایی را مختل می‌سازد، به دلیل تحقق عینی خسارت فیزیکی، از حیث حقوقی قابل قیاس با بمباران یا حمله نظامی خواهد بود.

با این وصف، تطابق حملات سایبری با بندهای هفت‌گانه فهرست اقدامات تجاوزکارانه (مستخرج از قطعنامه ۳۳۱۴ مجمع عمومی) از طریق تفسیر موسع و استفاده از قیاس امکان‌پذیر است، چراکه فهرست مزبور صرفاً جنبه تمثیلی داشته و حصری نیست. بدین معنا که تخریب داده‌ها و سخت‌افزارهای نظامیِ مستقر در قلمرو دولت دیگر می‌تواند منطبق با مفهوم «حمله به سرزمین» (بند الف)، اختلال فراگیر در سامانه‌های تأمین مالی که موجب فلج شدن اقتصاد کشور هدف و ایجاد پیامدهای انسانی گسترده گردد، قابل قیاس با «محاصره» (بند ج) و ارسال بدافزار از سوی یک دولت و به‌کارگیری شبکه‌های کامپیوتری کشور ثالث برای حمله به دولت دیگر، مصداقی از «استفاده از سرزمین برای تجاوز علیه کشور ثالث» (بند و) محسوب شود. در همه این موارد، عنصر مشترک تحقق «زور مسلحانه»، احراز آستانه «نقض فاحش منشور» با ملاحظه سه معیار ماهیت، شدت و گستره است؛ بنابراین راهکار اصلی برای پوشش خلأ قانونی موجود، توسل به تفسیری پویا از تعریف تجاوز بر اساس معیار «پیامدگرا» و «اثرمحور» است که به قضات دیوان اجازه می‌دهد با احراز شدت اثرات مخرب یک عملیات سایبری، آن را در چهارچوب تعریف موجود جای دهند، بدون آنکه نیازی به تعدیل لفظی متن اساسنامه باشد.

با توجه به اختیار وسیع قضات در تفسیر، پرسش دیگر این است که آیا امکان مطابقت اقدامات تجاوزکارانه در ماده (۲)۸ مکرر با اشکال تجاوز سایبری از طریق قیاس وجود دارد؟ عمده دلایل مخالفان قیاس، ماده (۲)۲۲ اساسنامه است. بدین معنی که نخست، قیاس ناقض اصل قانونی بودن خواهد بود؛ دوم، هرگونه اختلال سیستم به‌طور مشخص در محدوده اقدامات برشمرده‌شده در ماده ۸ مکرر قرار نمی‌گیرد. سوم، مقایسه موارد اختلال سیستم با اقدامات برشمرده‌شده، شرط «حمله مسلحانه» را که در تعریف آمده، برآورده نمی‌سازد؛ اما این انتقاد دارای یک ایراد اساسی است؛ همان‌طور که اشاره شد، در تعریف جرم تجاوز سه عنصر مادی، روانی و قانونی باید وجود داشته باشد. به‌علاوه برای احراز اقدام تجاوز باید همه اجزای ماده (۲)۸ با هم قرائت شوند؛ بدین معنا که اقدامات فهرست‌شده در ماده (ب)(۲)۸ باید شرایط آستانه مندرج در ماده (۱)۸ مکرر را که شامل ماهیت، شدت و گستره می‌شود، برآورده سازد. بدین ترتیب با در نظر گرفتن ارتباط میان صدر ماده (۱)۸ مکرر و فهرست اقدامات تجاوزکارانه مندرج در ماده (ب)(۲)۸ مکرر، می‌توان به این نتیجه رسید که استفاده از قیاس برای مطابقت با اشکال تجاوز سایبری نقض اصل قانونی بودن نخواهد بود، زیرا فهرست اقدامات (ب)(۲)۸ مکرر، عناصر جرم نبوده بلکه تنها ذکر مصادیق هستند (Miller, op. cit: 233). به‌عنوان مثال ماده (الف)(۲)۸ مکرر، به «حمله به سرزمین کشور دیگر یا هرگونه اشغال نظامی به‌عنوان نتایج آن حمله و تهاجم مزبور هرچند که موقتی باشد» اشاره دارد. در مقام مقایسه، چنانچه دولتی، ویروس کامپیوتری را به شبکه‌های نظامی دولت دیگری بفرستد، به‌گونه‌ای که سخت‌افزارهای کامپیوتری و حافظه اطلاعاتی موجود در سرزمین دولت دیگر به‌طور موقت اشغال شود، می‌توان تمثیلی از تجاوز سایبری قلمداد نمود. به‌علاوه دولتی می‌تواند با الحاق شبکه‌های کامپیوتری یک کشور، یک بات‌نت[1] به وجود آورده و حمله

1. Botnet

بات‌نت به شبکه‌ای از رایانه‌های هک‌شده گفته می‌شود که به‌منظور حمله و کلاهبرداری سایبری در اختیار گرفته شده‌اند. عبارت

کامپیوتری به کشور دیگر انجام دهد که با این کار ماده (ب)(۲)۸ مکرر را نقض کرده است. نمونه دیگر، حملات سایبری نظیر آنچه در گرجستان روی داد، است که مانع دسترسی به خدمات شده بود. بدین ترتیب چنانچه حمله هواپیماهای بدون سرنشین سبب بروز اختلال در ارتباطات حیاتی و زیربنایی برای تأمین خدمات و مایحتاج مردم گردد، پیامدهایی مشابه با محاصره خواهد داشت که می‌توان نقض ماده (ج)(۲)۸ مکرر قلمداد نمود. بر اساس ماده (ی)(۲)۸ مکرر، امکان استفاده از سرزمین کشور دیگر برای تجاوز علیه کشور ثالث وجود ندارد؛ حال می‌توان چنین تصور کرد که اگر چین به کره شمالی اجازه دهد از شبکه‌های کامپیوتری‌اش برای حملات سایبری علیه کره جنوبی استفاده نماید، نقض این بند صورت گرفته است (Ibid). اگر این توجیه پذیرفته شود، تنگنای دیگری ایجاد می‌شود و آن اینکه برخی از اشکال حملات سایبری مانند دست‌کاری در بازارهای مالی یک کشور با اسب تروا یا هک کردن حساب توییتر، که نه حمله‌ای علیه «نیروهای مسلح» صورت گرفته و نه از نیروی مسلح استفاده شده، در فهرست اعمال تجاوزکارانه قطعنامه ۱۹۷۴ نمی‌گنجند. حل این مشکل از طریق برداشت موسع از مفهوم «نیروی مسلح» میسر می‌نماید، به‌گونه‌ای که دیوان در تفسیر مفهوم «مسلحانه»، آن را به همه اشکال توسل‌به‌زور تسری داده و با احراز قصد تجاوزکارانه و قید آستانه مندرج در صدر ماده، اهمیت کمتری برای ویژگی‌های ظاهری تسلیحات قائل باشد (Nuclear Weapons Advisory Opinion, para. 39). بر این مبنا، کامپیوتری که حمله را آغاز کرده، به‌عنوان اسلحه قلمداد می‌گردد.

۳. دفاع مشروع در مقابل تجاوز سایبری

مهم‌ترین شاخص بین‌المللی پیرامون دفاع مشروع، ماده ۵۱ منشور است. با وجود این دستورالعمل تالین[۱] نیز به‌عنوان استاندارد و میزانی برجسته در ارزیابی تجاوز سایبری و دفاع مشروع باید مورد مداقه قرار گیرد. درحقیقت تمرکز عمده دستورالعمل تالین، ارزیابی جنبه‌های گوناگون عملیات سایبری در پرتو منشور ملل متحد، به‌ویژه مواد (۴)۲ و ۵۱ است. بدین ترتیب دیوان بین‌المللی کیفری باید احراز جنایت تجاوز، «توسل‌به‌زور»، «زور مسلحانه» و «حمله مسلحانه» را از مجرای این مواد ارزیابی کند؛ چراکه در ماده (۲)۸ مکرر تأکید شده که توسل‌به‌زور باید «مغایر با منشور ملل متحد باشد».

۳. ۱. حمله سایبری به‌مثابه نقض ممنوعیت توسل‌به‌زور

بررسی سیاق ماده (۴)۲ منشور، ممکن است عده‌ای را به این باور برساند که انتخاب واژه زور در این

بات‌نت از دو قسمت بات به معنی ربات و نت که همان مخفف network یا شبکه است، تشکیل شده است. بات‌نت معمولاً در مرحله نفوذ به سیستم‌های دیگر، در یک طرح چندلایه، وارد می‌شود. بات ها به‌عنوان ابزاری برای حملات انبوه مثل سرقت اطلاعات، خرابی سرور و پخش بدافزار استفاده می‌شوند. این تعریف برگفته از پایگاه زیر است:
https://mihanwebhost.com/blog/articles/460/%D8%A8%D8%A7%D8%AA-%D9%86%D8%AA-%DA%86%DB%8C%D8%B3%D8%AA

۱. برگرفته از پایگاه مرکز ملی فضای مجازی: «دستورالعمل تالین» (تالیت پایتخت کشور استونی است) به‌عنوان یکی از مهم‌ترین اسناد تخصصی، توضیح می‌دهد که اصول شناخته‌شده حقوق بین‌الملل همچنان در فضای دیجیتال نیز قابل اجرا هستند. این سند با پرداختن به موضوعاتی مانند حملات سایبری، آستانه توسل به‌زور، دفاع مشروع، اصل عدم مداخله، مسئولیت دولت‌ها و تعهدات آنها در پیشگیری از حملات، نشان می‌دهد که فضای سایبر برخلاف تصور رایج، یک قلمرو بی‌قانون و رهاشده نیست، بلکه بخشی از همان نظم حقوقی بین‌المللی محسوب می‌شود. دستورالعمل تالین ۱ (Tallinn Manual 1.0) تدوین‌شده توسط گروه متخصصان بین‌المللی به دعوت مرکز عالی دفاع سایبری ناتو (CCDCOE) در سال ۲۰۱۳ (تمرکز بر حقوق در زمان مخاصمات مسلحانه/جنگ سایبری). دستورالعمل تالین ۲ (Tallinn Manual 2.0)تدوین‌شده در سال ۲۰۱۷ (گسترش‌یافته به حقوق بین‌الملل زمان صلح، شامل اصل عدم مداخله، مراقبت بایسته و حقوق دریاها.)
https://www.majazi.ir/s/mfaLhF
برای اطلاعات بیشتر نک: موسی کرمی. (۱۴۰۲). نیم نگاهی به دستورالعمل های تالین در باب حقوق بین الملل حاکم بر فضای سایبر. پایگاه انجمن ایرانی مطالعات سازمان ملل متحد. قابل دسترسی در:
https://unstudies.ir/iauns-forum

ماده بدون هرگونه صفتی، به‌طور عامدانه و به‌منظور مطابقت با اشکال جدید و غیرقابل پیش‌بینی زور و متناسب با عملکرد دولت‌ها در روابط بین‌المللی بوده تا مسیر تحول مقررات دراین‌باره مسدود نگردد؛ زیرا نخست، تدوین‌کنندگان منشور از اشکال مختلف زور آگاهی داشته‌اند. دوم، توجه به سایر مواد منشور ما را در این نتیجه‌گیری مصمم‌تر می‌نماید که در مواردی که شکل خاصی از زور مقصود اصلی بوده، به‌صراحت بدان اشاره شده است (Benatar, 2009: 382).

در جریان تدوین پیش‌نویس ماده ۲(۴)، شمار انبوهی از پیشنهادها درخصوص تفسیر موسع ممنوعیت توسل‌به‌زور ارائه شد تا تمام اشکال قابل تصور زور را دربرگیرد. برای نمونه اکوادور زور غیرقانونی اخلاقی و فیزیکی را پیشنهاد کرد (3 U.N.C.I.O. Docs. 399, U.N.C.I.O. Docs. 561 (1945); 432 (۱۹۴۵))، درحالی‌که ایران خواهان ممنوعیت زور سیاسی مستقیم و غیرمستقیم بود (U.N.C.I.O. Docs. 563, 588 (1945)). در این میان، خواسته برزیل جایگاه ممتازی یافت؛ بدین مضمون که «همه اعضای سازمان ملل باید در روابط بین‌المللی‌شان از تهدید یا توسل‌به‌زور و از تهدید یا توسل به اقدامات اقتصادی، به‌گونه‌ای که مغایر با مقاصد سازمان است، بپرهیزند» (U.N.C.I.O. Docs. 559 (1945))؛ اما مخالفت‌های گسترده با تفسیر موسع زور در ماده ۲(۴)، مهر تأییدی بر پذیرش تفسیر مضیق پیرامون مفهوم زور بود. نتیجه آنکه منشور ملل متحد بین سه دسته از اشکال زور مسلحانه، اقتصادی و سیاسی قائل به تمایز می‌شود که همه آن‌ها می‌توانند منتهی به نقض حقوق بین‌الملل، یعنی اصل عدم مداخله، شوند، اما تنها زور مسلحانه ناقض قاعده مندرج در ماده ۲(۴) است.

چنانچه عملیات سایبری را نتوان توسل‌به‌زور تلقی نمود، بدین معنا نیست که عملی قانونی است؛ بلکه ممکن است نقض قاعده عدم مداخله باشد (Schmitt, 2013: 44, para. 7). به‌عنوان مثال عملیات سایبری روانی را که آثار تخریبی نداشته و صرفاً برای تضعیف روحیه همبستگی هدایت می‌شود، نمی‌توان توسل‌به‌زور قلمداد کرد. دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه اظهار داشت که صرف تأمین مالی شورشیان دولتی توسط دولت دیگر، استفاده از زور محسوب نمی‌شود (Nicaragua Judgement, para, 228)؛ بنابراین برای نمونه، صرف تأمین مالی گروهی که در لوای شورش، عملیات سایبری را هدایت می‌کنند، توسل‌به‌زور نیست (Schmitt, op. cit.:46. para. 3).

از سوی دیگر توسل‌به‌زور لزوماً به معنای به‌کارگیری زور نظامی یا دیگر اشکال زور مسلحانه توسط دولت نیست. در همان رأی، دیوان به این نتیجه رسید که رساندن اسلحه و آموزش شورشیانی که درگیر مخاصمه با دولت دیگری هستند، استفاده از زور است (Nicaragua Judgement, para, 228)؛ بنابراین تدارک گروه سازمان‌یافته با بدافزار و آموزش لازم برای استفاده از آن به‌منظور هدایت حملات سایبری علیه دولت دیگر، عنوان توسل‌به‌زور می‌یابد (Ibid.: 46. para. 4).

۳. ۲. حمله سایبری به‌مثابه حمله مسلحانه

برای آنکه دولتی به حق دفاع مشروع استناد کند، باید در اجرای ماده ۵۱ منشور، حمله سایبری را به‌مثابه حمله‌ای مسلحانه تلقی کند. صحت این مدعا به دنبال رأی دیوان در قضیه نیکاراگوئه آشکار گشت؛ زیرا دیوان میان صرف توسل‌به‌زور و «شدیدترین اشکال توسل‌به‌زور» قائل به تمایز شد، بدین معنا که توسل‌به‌زور با سنجش «گستره و پیامدها»[1] ممکن است به آستانه‌ای برسد که به‌عنوان حمله مسلحانه قلمداد شود (Nicaragua Judgement, para, 191). بدین ترتیب برای ارزیابی گستره و تأثیرات توسل‌به‌زور در عملیات سایبری می‌توان به معیارهای هشت‌گانه سند تالین متوسل شد تا تحقق یا عدم تحقق آستانه «حمله سایبری» احراز شود.[2] معیارهای هشت‌گانه که جامع و کامل

1. Scale and Effects

۲. نک: (مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، ۱۳۹۱ب: ۳۰۰).

نیستند، عبارت‌اند از: ۱- شدت؛ ۲- قریب‌الوقوع بودن؛ ۳- بلاواسطه بودن؛ ۴- تهاجمی بودن؛ [1]۵- قابلیت اندازه‌گیری پیامدها؛ ۶- ماهیت نظامی؛ ۷- مشارکت دولت؛ و ۸- قانونی بودن احتمالی (Schmitt, op. cit.: 48-51, para. 9).

به نظر می‌رسد در میان عناصر فوق بتوان ارزش و سنگینی بیشتری را برای عامل شدت قائل بود؛ چون خسارت فیزیکی به اموال یا آسیب به اشخاص همیشه توسل‌به‌زور محسوب می‌شود (Miller, op. cit.: 244). مدل مبتنی بر نتیجه در مورد حملات سایبری حاصل ابتکار مایکل اشمیت است. بر این اساس حملات سایبری را که منتهی به تخریب فیزیکی و آسیب به حیات انسانی می‌شوند، می‌توان معادل توسل‌به‌زور مسلحانه تلقی نمود. برای مثال کنترل سیستم‌های کنترل ترافیک هوایی توسط هکرها که سبب سقوط هواپیما گردد (Benatar, op. cit.: 390)؛ اما به نظر می‌رسد بیشترین محل کاربرد این الگو در عملیات سایبری است که فاقد هرگونه خسارت فیزیکی نسبت به سایر حملات هستند و به پیامدهای اقتصادی احتمالی منتج می‌شوند و گستردگی آنها، سبب تلقی آنها به‌عنوان تهدیدی جدی علیه امنیت کشوری می‌گردد. برای نمونه حمله ویروس شامون به شرکت آرامکو در عربستان، بخش سخت‌افزار هزاران کامپیوتر را در آن شرکت از بین برد، به‌گونه‌ای که اطلاعات مهم را نابود کرد. بر اساس معیار بلاواسطه بودن حمله و قابلیت اندازه‌گیری پیامدها می‌توان ادعا کرد با توجه به خسارات گسترده و قابل اندازه‌گیری و به‌علاوه امکان پیوند زدن میان قصد عملیات سایبری و اثرات برجای‌مانده از حمله ویروس شامون، نمره بالایی را در توسل‌به‌زور به خود اختصاص داده است (Schmitt, op. cit.: 50, Para. 9). به‌علاوه برای احراز معیار تهاجمی بودن حمله می‌توان نفوذ به سیستم‌های کامپیوتری با امنیت بالا و سیستم‌های نظامی را ملاک قرار داد (Ibid, 49, Para. 9). نمونه عملی آن، حمله ویروس استاکس‌نت به تأسیسات هسته‌ای ایران است که نسبت به هک شدن وب‌سایت عمومی وزارت دادگستری ایالات متحده رتبه بالاتری را در تهاجمی بودن حمله کسب می‌کند. نکته دیگر آنکه اقداماتی که به‌طور مستقیم از سوی واحدهای نظامی هدایت یافته یا مورد حمایت دولت هستند، نسبت به اعمالی که توسط افرادی ناشناس یا گروه‌های ملی‌گرا ارتکاب می‌یابند، به توسل‌به‌زور نزدیک‌تر هستند (Ibid, 50-51, para. 9). درنهایت بر اساس فاکتور هشتم، اقداماتی که مطابق با معاهده یا عرف بین‌المللی منع نشده‌اند، مانند جاسوسی دولت، تبلیغات، یا فشار اقتصادی، در موارد معدودی به‌عنوان توسل‌به‌زور تلقی می‌گردند (Ibid, 51, para. 9).

با وجود اینکه الگوی ارائه‌شده در مواردی راهگشاست، اما به‌طور کامل از انتقاد مصون نمانده است؛ زیرا مدل اشمیت، همانند دیدگاه ابزارمحور، این نقیصه را دارد که مواردی را «احصا کرده است».[2] حقیقت آن است که زور سایبری ویژگی‌های منحصربه‌فردی دارد که آن را از سلاح‌های کلاسیک متمایز کرده و آثار سهمگینی بر جای می‌گذارد. درنتیجه برخی اشکال زور مطابق با معیارهای تعریف‌شده اشمیت نیستند. برای مثال تخریب اطلاعات سیستم‌های بانکی یک کشور معین می‌تواند باعث به زانو درآمدن تمامی بخش‌های مالی گردد. ازآنجایی‌که هیچ‌کدام از اقسام زور مسلحانه، سیاسی یا اقتصادی چنین نتیجه‌ای را در پی نخواهند داشت، امکان مقایسه آنها به‌راحتی وجود ندارد. حال آیا منحصربه‌فرد بودن حملات سایبری، از به نظم کشیدن آن بر اساس ماده (۴)۲ و ۵۱ ممانعت می‌کند؟ (Benatar, op. cit.: 391) واقعیت این است که مباحثات در حوزه حقوق بین‌الملل کیفری راجع به ویژگی و کیفیت حملات سایبری به‌عنوان جرائم خطیر همچنان در جریان‌اند و پاسخی قطعی به آن داده نشده است (Greco, 2020: 45). بااین‌حال شاید بهترین راهکار، تفسیر موسع اصطلاح «مسلحانه» به‌منظور شمول مقرره بر تسلیحات غیرکلاسیک باشد تا بدون آنکه

1. Invasiveness
2. Under-inclusiveness

نیازی به اعمال تغییر و تجدیدنظر باشد، دامنه تعریف توسعه یابد؛ اما باید توجه داشت که شرط حداقل ممکن است در این زمینه موانعی را ایجاد کند و مشکل بزرگ‌تر مسئله انعطاف‌پذیری تاکتیک‌های سایبری است، زیرا حمله سایبری می‌تواند به‌سرعت به اقدام تجاوزکارانه‌ای تبدیل شود که امکان تدارک پاسخ متناسب در مقابل آن وجود نداشته باشد.

در این میان توجه به رویه معمول دولت‌ها در ارزیابی موضوعات مطرح‌شده اهمیت دارد، به‌گونه‌ای که حتی کارشناسان تالین بر این عقیده‌اند که «با توجه به استمرار تهدیدات سایبری، رویه دولت‌ها می‌تواند تفاسیر و اعمال حقوق بر جنگ را در مورد عملیات سایبری تغییر دهد» (Schmitt, op. cit.: 42, para. 2) و بدین ترتیب رویه مستقیم دولت‌ها می‌تواند پیامدها و تأثیرات عمده‌ای بر درک و فهم بین‌المللی از توسل به «زور مسلحانه» داشته باشد.

۴. الزامات حقوقی دفاع مشروع در تجاوز سایبری

در دفاع مشروع در مقابل تجاوز سایبری باید الزامات «ضرورت»، «تناسب» و «فوریت» رعایت شود. دیوان در رأی نیکاراگوئه به دو معیار ضرورت و تناسب در دفاع مشروع اشاره و در رأی سکوهای نفتی آن دو را تأیید کرد. ضرورت بدین معنی است که توسل‌به‌زور آخرین گزینه و راهکار است؛ لذا باید سایر راهکارها ناکارآمد و بی‌فایده باشند. به‌عنوان یک الزام و شرط حداقلی، ضرورت بر این دلالت دارد که کشوری که درصدد دفاع مشروع است، باید دریابد که حمله سایبری یک تصادف نبوده و موضوع را نمی‌توان با توسل به روش‌های کم‌تر قهرآمیز حل‌وفصل نمود (Ibid, 62, Paras. 2,3)؛ روش‌هایی چون جلوگیری از دسترسی نفوذگران سایبری به شبکه‌ها و وب‌سایت‌های هدف حمله از طریق توسل به دفاع سایبری. معیار ضرورت توسط دولت قربانی سنجیده می‌شود و تشخیص آن با توجه به اوضاع‌واحوال مربوطه صورت می‌گیرد (Ibid, 62, para. 4).

تناسب به این معناست که جایی که توسل‌به‌زور ضروری به نظر می‌رسد، چه مقدار زور، ازجمله زور سایبری مورد نیاز است. این معیار گستره، مدت و شدت پاسخ تدافعی به حمله مسلحانه را که برای پایان دادن به وضعیت لازم است، در چهارچوب حق دفاع مشروع تعیین می‌کند. تناسب، میزان زوری را که به کار می‌رود، محدود نمی‌کند، چراکه مقدار زور مورد نیاز برای دفاع مشروع بستگی به شرایط دارد (Ibid, para. 5).

ازآنجاکه ماده ۵۱ منشور، حق برخورداری از دفاع مشروع را فقط منحصر به دفاع در برابر حملات مسلحانه نموده است؛ لذا اگر حمله محقق‌شده، از حیث دسته‌بندی ابزارهای اعمال زور، از نوع زور غیرمسلحانه باشد، ازآنجاکه یکی از معیارهای اصلی دفاع مشروع بر اساس ماده ۵۱ منشور، وقوع حمله مسلحانه است که در این وضعیت محقق نشده است، دولت قربانی نمی‌تواند برای دفاع از خود، متوسل به اعمال زور بر اساس ماده ۵۱ منشور گردد. عده‌ای بر این باورند اگر حمله محقق‌شده از حیث دسته‌بندی ابزارهای اعمال زور از نوع حمله مسلحانه باشد، یعنی حمله مذکور باعث تخریب فیزیکی و یا صدمه به حیات انسانی گردد، باز هم دولت قربانی نمی‌تواند برای دفاع از خود، متوسل به اعمال زور طبق ماده ۵۱ منشور گردد؛ زیرا یکی از معیارهای اساسی در دفاع مشروع، رعایت قاعده تناسب از نظر ابزارهای به‌کاررفته در حمله و دفاع است، ازآنجاکه در این حمله، مجموعه کدهای عملیاتی به‌عنوان ابزارهای تهاجمی مورد استفاده واقع شده‌اند، لذا اعطای حق دفاع با توسل به اقدامات نظامی متعارف و مبتنی بر زور فیزیکی (جنبشی) به کشور قربانی، در شرایطی که حمله صرفاً در بستر فضای سایبری رخ داده و با ابزارهای غیرجنبشی (کُدهای عملیاتی و بدافزارها) صورت پذیرفته است، نوعی نقض قاعده تناسب در «ابزار و وسایل جنگ» محسوب می‌گردد؛ چراکه تناسب ایجاب می‌کند واکنش دفاعی از حیث نوع، شدت و گستره با حمله اولیه قابل قیاس بوده و از کیفیت و کمیت فراتر از آنچه برای دفع

حمله ضروری است، برخوردار نباشد. درنتیجه در هر حالتی از حملات سایبری، چه مسلحانه و چه غیرمسلحانه، کشور قربانی نمی‌تواند برای دفاع از خود، متوسل به اعمال زور بر اساس ماده ۵۱ منشور شود. راهکار مقابله فردی که برای چنین حملاتی پیشنهاد شده، این است که در هر دو وضعیت، صرف‌نظر از مسلحانه و یا غیرمسلحانه بودن حملات سایبری، دولت قربانی می‌تواند ضمن استناد به ماده (۲)(۱)۳۵ منشور، به شورای امنیت مراجعه کند و مدعی شود که اقدامات صورت‌گرفته در قالب حمله به شبکه‌های رایانه‌ای، صلح و امنیت جهانی را تهدید می‌کند؛ چراکه در صلاحدید و اختیار شورای امنیت است که تصمیم بگیرد عملیات سایبری علیه سیستم بانکداری یا زیرساخت‌های اساسی ملی از چنان کیفیتی برخوردار است که بتواند بر اساس ماده ۳۹ منشور به‌عنوان تهدید صلح و امنیت بین‌المللی توصیف شده و به دنبال آن بر اساس ماده ۴۱ و ۴۲ به اتخاذ اقدامات متناسب اقدام نماید یا خیر. علاوه بر این دولت قربانی می‌تواند تا محقق شدن اقدامات لازم توسط شورای امنیت، بر اساس ضرورت و فوریت و بر اساس قاعده تناسب به دفاع از خود بپردازد. به‌عبارت‌دیگر با ارسال و انتشار کدهای عملیاتی در شبکه‌های رایانه‌ای کشور مهاجم از خود دفاع کند.

علت اصلی اعمال محدودیت فردی برای مقابله با حملات سایبری بر اساس ماده ۵۱ منشور و احاله آن به شورای امنیت، قابلیت ردیابی آسان و دقیق منبع و محل وقوع این‌گونه حملات است. حال اگر در چنین وضعیتی به او اجازه حمله داده می‌شد تا برای دفاع از خود، متوسل به اعمال زور بر اساس ماده ۵۱ منشور گردد، ممکن است این امر منجر به تشدید اصطکاک و اختلاف بین‌المللی شود که این موضوع در تعارض با ماده ۳۴ منشور قرار می‌گیرد. لذا به نظر می‌رسد که واکنش به چنین حملاتی از طریق شورای امنیت در قیاس با اقدامات فردی امری پسندیده‌تر باشد (رجبی حنفیه، ۱۳۸۷: ۷۵). این نظریه دارای ایرادات اساسی است؛ کسانی که بر اساس معیار تناسب، توسل به روش‌های قهرآمیز در دفاع مشروع مندرج در ماده ۵۱ منشور را مجاز نمی‌دانند، معتقدند که دفاع مشروع در فضای مجازی هم به‌طور کامل نتیجه مورد نظر آنها را که رعایت معیار تناسب است، محقق نمی‌کند؛ مواقعی که در پاسخ به حملات سایبری، حمله سایبری صورت می‌گیرد، به‌ویژه در جایی که میان ابرقدرت‌ها و صاحبان فناوری نبردی صورت می‌گیرد، دامنه خسارات می‌تواند بسیار فاجعه‌آمیزتر از حملاتی باشد که در قالب‌های سنتی صورت می‌گیرد. از طرف دیگر چنانچه توازنی میان سطح فناوری طرفین وجود نداشته باشد، خدشه‌دار شدن اصل تناسب به نحو بارزتری به چشم می‌خورد. حالتی را در نظر بگیرید که حملات سایبری از سوی کشور صاحب فناوری علیه کشوری که پیشرفت چندانی در این زمینه نداشته، صورت گیرد؛ اگر برای کشور مورد حمله حق دفاع مشروع در قالب ماده ۵۱ و با توسل به ادوات نظامی را قائل نباشیم، به‌طورکلی آن کشور را از حق دفاع از موجودیت خود محروم ساخته‌ایم؛ چراکه این کشور به جهت سطح پایین فناوری توان مقابله با کشور قدرتمندتر را در فضای مجازی ندارد. نکته دیگر اینکه اگر بخواهد منتظر اقدام شورای امنیت بماند، گذشته از نادیده گرفتن اصل فوریت در دفاع مشروع، شرایط بحرانی‌تر می‌شود و حالات مختلفی را می‌توان متصور بود. یک حالت این است که معمولاً چنین حملاتی از سوی اعضای دائم شورای امنیت صورت می‌گیرد که این خود روند تصمیم‌گیری شورا را طولانی‌تر کرده، مضاف بر اینکه اصلاً معلوم نیست شورای امنیت این وضعیت را تهدید صلح و امنیت بین‌المللی تلقی نماید. باید به کسانی که بر روی معیار تناسب پافشاری می‌کنند، متذکر شد که اصل فوریت در دفاع مشروع هم ارزشی برابر با اصل تناسب دارد و این سه معیار باید در کنار هم دیده شوند. الزام فوریت بیانگر آن است که هدف غایی دفاع مشروع، تنبیه مهاجم نیست، بلکه هدف، دفع حمله مسلحانه است. چنین الزامی به‌ویژه درخصوص حملات سایبری باید به نحو انعطاف‌پذیری به کار رود؛ نتیجه آنکه در مواردی ممکن است امکان رعایت اصل تناسب در ابزار مورد استفاده در حمله وجود نداشته باشد و از سویی

اصل فوریت اقتضا کند دولت مورد حمله برای دفاع از زیرساخت‌ها و موجودیت خود، اقدامات لازم را به عمل آورد که در این مرحله مبادرت به حمله نظامی در قالب دفاع مشروع علیه حملات سایبری موجه می‌نماید. نکته قابل تأمل این است که دشواری‌های شناسایی محل وقوع حمله و اثبات انتساب و طرح مسئولیت، با اصل فوریت در دفاع مشروع در تعارض قرار می‌گیرد. شاید بهترین راه برون‌رفت از این تنگنا، مستثنا نمودن اصل فوریت باشد که بعید است دلیلی برای این امر وجود داشته باشد.

ایراد عمده دیگری که به این نظریه وارد است، تصور اشتباهی است که در مورد شناسایی محل وقوع حملات سایبری و انتساب و طرح مسئولیت وجود دارد. نمونه‌های عینی حملات سایبری به‌خوبی تأییدکننده این حقیقت است که یکی از چالش‌ها و مشکلات اساسی در این حملات تشخیص محل شروع عملیات است که از آن جمله می‌توان به مورد استونی[۱] اشاره کرد. چه‌بسا ممکن است این حملات توسط شخصی هدایت شود که با کامپیوتر شخصی خود مایل‌ها دورتر از محل وقوع حادثه قرار دارد، بدون اینکه بتوان رابطه‌ای را میان شخص مورد نظر و دولتی متصور بود.

آنچه گفته شد، در توضیح مواردی است که کشوری هدف حملات سایبری قرار می‌گیرد و اختلاف بر سر این است که دفاع مشروع باید به‌صورت واقعی یا در فضای مجازی صورت گیرد؛ اما شکل دیگر، در جایی قابل تصور است که کشوری مورد حمله نظامی واقع شده و کشور مورد تهاجم در مقام دفاع مشروع، متوسل به حملات سایبری می‌شود. در این حالت آیا می‌توان قائل به مشروعیت چنین دفاعی در چهارچوب ماده ۵۱ بود؟ به نظر می‌رسد برای پاسخ دادن به این سؤال باید ابتدا برای فرض پیشین پاسخی یافت. بدین معنا که اگر مجوز دفاع مشروع با سلاح‌های متعارف در مقابل حمله سایبری وجود داشته باشد، چه دلیلی وجود دارد که نتوانیم در مقابل حمله مسلحانه کلاسیک امکان استفاده از فضای سایبر برای دفاع مشروع را به رسمیت بشناسیم؟

در دستورالعمل تالین با ذکر دو فرض، امکان مبادرت به عملیات سایبری را در جایی که ابتدا حمله سایبری وقوع نیافته، منوط به فرمان و اجازه شورای امنیت دانسته و در غیر این دو صورت ساکت است.

فرض اول؛ مطابق ماده ۴۲، زمانی که شورای امنیت تشخیص دهد تهدید علیه صلح، نقض صلح، یا عمل تجاوز رخ داده است و اقدامات غیرقهرآمیز برای حفظ یا احیای صلح و امنیت بین‌المللی کافی نباشد، شورای امنیت می‌تواند تصمیم به استفاده از زور گیرد. برای مثال کشور «الف» قابلیت استفاده از سلاح‌های هسته‌ای را دارد؛ آن دولت نسبت به خواست شورای امنیت مبنی بر توقف فعالیت‌هایش بی‌توجه است و به‌موجب ماده ۴۱ تحریم اقتصادی شده است. در اینجا شورای امنیت به‌منظور پایان دادن به برنامه‌های هسته‌ای آن کشور می‌تواند به دولت‌ها اجازه دهد علیه آن کشور عملیات سایبری انجام دهند. البته در اینجا حمله مسلحانه‌ای روی نداده است (Schmitt, op. cit.: 55, Para. 6).

فرض دوم؛ شورای امنیت معمولاً «همه اقدامات ضروری» را که برای اجرای قطعنامه نیاز است، در نظر می‌گیرد. این عبارت به‌طور تلویحی اشاره به این مطلب دارد که امکان هدایت عملیات سایبری علیه دولت یا نهادی که موضوع قطعنامه است، وجود دارد. همچنین امکان عملیات جنبشی علیه توانمندی‌های سایبری آن دولت یا نهاد نیز وجود دارد. البته اقدامات اتخاذشده باید در چهارچوب قطعنامه و مجوز شورای امنیت قرار گیرد (Ibid, Para. 7).

این دو فرض خارج از بحث دفاع مشروع‌اند، اما زمینه مناسبی برای اندیشیدن دراین‌باره هستند که آیا شورای امنیت می‌تواند مطابق ماده ۴۲ منشور استفاده از فضای سایبر را به‌عنوان قوه قهریه به کار گیرد؟ که اگر این فرض پذیرفته شود، آنگاه تحولی در مفهوم سلاح و قوه قهریه ایجاد خواهد شد.

---

۱. برای اطلاعات بیشتر، نک: (مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، ۱۳۹۱ب).

۵. عاملان حمله

به دلیل مجازی بودن فضا و ابهام در نوع و ماهیت حمله، شناسایی کشور یا نیروی مهاجم دشوار است. ماهیت حملات سایبری به‌گونه‌ای است که در آن کمترین نشانه‌ای از عامل حمله وجود دارد؛ ضمن اینکه مکان حمله سایبری نیز چندان مشخص نیست و بدافزار ارسال‌شده نیز کمترین نشانه‌ای از عامل حمله ندارد. همچنین به دلیل تعدد بازیگران در حوزه و فضای سایبر که شامل کشورها، سازمان‌ها و نهادهای دولتی و غیردولتی، تروریست‌ها، هکرها و حتی افراد می‌شود، شناخت عامل حمله سخت‌تر و پیچیده‌تر است. در حملات سایبری که تاکنون صورت گرفته، کشور یا عامل حمله، نه بر اساس حملات سایبری و شواهد روشن، بلکه بر اساس اوضاع‌واحوال سیاسی و نیات و اهداف کشورها شناسایی شده‌اند (ترابی، پیشین: ۱۳۹). درحقیقت تأخیر در شناسایی عامل بحث دفاع مشروع را با چالش‌هایی مواجه می‌سازد؛ چراکه یکی از الزامات مطروحه در دفاع فوریت است که به دلیل ناشناس ماندن عامل و مکان حمله، امکان دفاع را از کشور مورد حمله می‌گیرد (همان: ۱۴۰).[۱]

۶. نتیجه

روشن است که با تحولات جدید در اشکال نبرد نمی‌توان به تفسیری مضیق از موافقت‌نامه کامپالا بسنده نمود و به هنگام رسیدگی موضوع در دیوان بین‌المللی کیفری لازم است که نخست اینکه قضات دیوان در تفسیر اینکه چه اقداماتی، توسل‌به‌زور مسلحانه قلمداد شده، آزادی عمل داشته باشند؛ چراکه فهرست اقدامات در ماده (ب)(۲)۸ مکرر، غیرحصری است؛ دوم، عبارت «زور مسلحانه» باید در پرتو حقوق بر جنگ و درنتیجه مواد ۲(۴) و ۵۱ منشور تفسیر گردد؛ نکته توجه قضات به تحولات روی‌داده در حوزه حقوق بر جنگ، دستورالعمل تالین است که در رسیدگی و تعقیب جنایت تجاوز سایبری مؤثر است. سوم، دیوان در ارزیابی اقدامات تجاوزکارانه‌ای که از زور مسلحانه استفاده شده، با ملاحظه سه معیار ماهیت، شدت و گستره، فاحش بودن آن را احراز نماید؛ چهارم، صرف‌نظر از عقیده مرتکب، وصف «آشکار»[۲] معیاری عینی است. بر این اساس به نظر می‌رسد که امکان ارائه تفسیر موسع از تعاریف و عناصر جرم تجاوز وجود دارد، به‌گونه‌ای که اشکال جدید تجاوز نظیر تجاوز سایبری و حتی انواع در حال ظهور آن را دربرگیرد.

با وجود این با توجه به‌تازگی ارائه تعریف مورد اجماع از تجاوز در عرصه بین‌المللی، بعید می‌نماید که امکان اعمال صلاحیت بر تجاوز سایبری با تکیه بر شرایط تعیین‌شده برای تجاوز در آینده‌ای نزدیک متصور باشد و نیاز است راهکارهای دیگری به‌طور هم‌زمان برای ارتقای صلح در فضای سایبری در پیش گرفته شود. ضمن آنکه نمی‌توان از این واقعیت چشم‌پوشی کرد که برای مطابقت تجاوز سایبری با حقوق بین‌الملل، تحول در هنجارها به‌طور تدریجی نیز ضروری است؛ زیرا عدم توجه به این تحولات، سبب می‌شود قواعد موجود، بسیاری از اشکال نوظهور حملات را دربرنگیرد.

با وقوع تجاوز سایبری می‌توان در برابر آن به دفاع مشروع متوسل شد. بر اساس قاعده عمومی دفاع مشروع، حمله سایبری باید مسلحانه و به‌مثابه نقض ممنوعیت توسل‌به‌زور، ماده ۲(۴) منشور ملل متحد، تلقی شود؛ در این زمینه، راهنمای تالین نیز می‌تواند به‌عنوان معیاری تکمیلی برای ارزیابی تحقق یا عدم تحقق حمله سایبری و به‌تبع آن، امکان توسل به دفاع مشروع مورد توجه قضات قرار گیرد. با احراز شرایط توسل به دفاع مشروع به‌قطع باید الزامات حقوقی چون «ضرورت»، «فوریت» و «تناسب» از سوی دولت مورد تجاوز رعایت گردد، هرچند به دلیل خصیصه‌های ویژه‌ای که حملات در فضای سایبری دارند، پیاده‌سازی تمام و کمال آنها همیشه امکان‌پذیر نیست؛ نکته مهم‌تر به

---

۱. همچنین نک: (مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، ۱۳۹۱ب: ۳۵۰).

۲. Manifest

ویژگی کنشگران دولتی و عامل سرزمینی بودن در موارد مصرح در ماده ۵۱ منشور ملل متحد برمی‌گردد که بی‌گمان با توجه به ویژگی‌های فضای سایبری باید به تفاسیر موسعی از این ماده از سوی قضات دل بست.

منابع

الف) فارسی

کتاب‌ها

۱. مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران. (۱۳۹۱الف). *امنیت و جنگ سایبری ۱؛ ویژه مفاهیم و مبانی*. تهران: نشر مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.

۲. مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران. (۱۳۹۱ب). *امنیت و جنگ سایبری ۲؛ ویژه سلاح‌ها، جنگجویان و حملات سایبری*. تهران: نشر مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.

مقالات

۳. اسمعیل‌زاده ملاباشی، پرستو. (۱۳۹۶). حمله سایبری به‌مثابه جنایت تجاوز و بررسی صلاحیت دیوان کیفری بین‌المللی در رسیدگی به آن. *پژوهشهای حقوق جزا و جرم‌شناسی*، ۵(۱۰): ۶۵-۴۳.

۴. سالمون، ژان.ژ.ا. (۱۳۸۲). استدلال از طریق قیاس در حقوق بین‌الملل عمومی. ترجمه سید علی هنجنی و رحیم نوبهار. *مجله تحقیقات حقوقی*، (۳۷).

۵. شایگان‌فرد، مجید. (۱۳۸۷). دیوان بین‌المللی کیفری و صلاحیت دیوان در رسیدگی به جنایت تجاوز. *فصلنامه حقوق*، ۴.

۷. موسی‌زاده، رضا و حسین فروغی‌نیا. (۱۳۹۱). تعریف جنایت تجاوز در پرتوی قطعنامه کنفرانس بازنگری اساسنامه دیوان کیفری بین‌المللی در کامپالا. *راهبرد*، ۲۱(۶۳).

پایان‌نامه تحصیلی

۸. رجبی حنفیه، محمد. (۱۳۸۷). حمله به شبکه‌های رایانه‌ای در حقوق بین‌الملل. پایان‌نامه کارشناسی ارشد. تهران: دانشگاه علامه طباطبایی.

ب) انگلیسی

Books

1. Barriga, S., & Kreß, C. (Eds.). (2012). *Negotiating the amendments on the crime of aggression: The travaux préparatoires of the crime of aggression*. Cambridge University Press.

2. Bassiouni, M. C. (2013). *Introduction to international criminal law* (2nd rev. ed.). Martinus Nijhoff Publishers.

3. Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare: Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge University Press.

Articles

4. Benatar, M. (2009). The use of force: Need for legal justification? *Goettingen Journal of International Law*, 1(3).

5. Glennon, M. (2010). The blank-prose crime of aggression. *Yale Journal of International Law*, 35, 71.

6. Greco, G. (2020). Cyber-attacks as aggression crimes in cyberspace in the context of international criminal law. *European Journal of Political Science Studies*, 4(1).

7. Kessler, O., & Werner, W. (2013). Expertise, uncertainty and international law: A study of the Tallinn Manual on cyberwarfare. *Leiden Journal of International Law*, 26.

8. Miller, K. L. (2014). The Kampala compromise and cyberattacks: Can there be an international crime of cyber-aggression? *Southern California Interdisciplinary Law Journal*, 23, 217.

9. Ophardt, J. A. (2010). Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. *Duke Law & Technology Review*, 3.

10. Schmitt, M. N. (1999). Computer network attack and the use of force in international law: Thoughts on a normative framework. *Columbia Journal of Transnational Law*, 37, 885.
11. Solce, N. (2008). The battlefield of cyberspace: The inevitable new military branch - The Cyber Force. *Albany Law Journal of Science & Technology*, 18, 293.
12. Weisbord, N. (2011). Judging aggression. *Columbia Journal of Transnational Law*, 50, 82.
13. Weisbord, N. (2008). Prosecuting aggression. *Harvard International Law Journal*, 49, 161.
14. International Criminal Court, Assembly of States Parties, Special Working Group on the Crime of Aggression. (2009, February 9–13). Report of the Special Working Group on the Crime of Aggression (ICC-ASP/7/20/Add.1, Annex II, Appendix I).
15. International Criminal Court, Assembly of States Parties. (2007). Report of the Special Working Group on the Crime of Aggression (ICC-ASP/6/SWGCA/1). In Official Records of the Assembly of States Parties to the Rome Statute of the International Criminal Court (ICC-ASP/6/20, Annex II, p. 87, para. 21).