شاپا چاپی: ۱۸۴۱-۲۷۸۳
شاپای الکترونیکی: ۱۹۲۲-۲۷۸۳

تمدن حقوقی

دوره ۷ - شماره ۲۰ - تابستان ۱۴۰۳

Legal Civilization
Vol.7, No.20, Summer 2024
Pages: 177-194
Article Type: Promotional Article
https: //www.pzhfars.ir/article_198042.html
doi: 10.22034/LC.2024.460797.1499

تمدن حقوقی
دوره ۷، شماره ۲۰، تابستان ۱۴۰۳
صفحات:۱۹۴-۱۷۷
نوع مقاله: ترویجی

Feasibility of Legitimate Self-defense through Cyber Attacks

Saleh Gholam Heidari
Master's student in Human Rights, Faculty of Law and Political Sciences, University of Tehran, Tehran, Iran

Abstract

International law has generally been unable to precisely regulate the rules of cyber operations thus far. This is due to the complexity of cyberspace, the nature of the technology, and the need to adapt existing laws to technological developments. Many previous international rules, such as those related to armed attacks, war, or human rights, do not directly apply to cyber operations. Instead, some general principles and concepts may apply cyber operations. Therefore, there are no precise rules regarding cyber operations, and many existing international concepts and rules may not be readily applicable to cyber operations. This is a significant challenge in the field of international law, which has led to the need to develop new rules and standards for this domain as technology progresses and cyber operations continue to grow. One of these concepts is the conduct of cyber operations and cyber-attacks by one state against another under the principle of legitimate self-defense. This research, while identifying cyber-attacks, examined the question of whether, from the perspective of international law, cyber-attacks against a country in a state of acute self-defense, where the very existence of the state is at risk, are permissible or prohibited. The research conducted is descriptive-analytical, the author hypothesized that states may use this type of attack in self-defense due to the specific characteristics of cyber operations, including high and irreparable destructive power.

Keywords: Cyber-attacks, Self-defense Right, International Humanitarian Law, Conditions for Self-defense.

Received: 2024/04/15 - Review: 2024/06/27 - Accepted: 2024/08/07

امکان‌سنجی دفاع مشروع از طریق حملات سایبری

صالح غلام‌حیدری
دانشجوی کارشناسی‌ارشد حقوق بشر، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران
salehheidarii77@ut.ac.ir

چکیده

تا به امروز حقوق بین‌الملل عموماً قادر به تنظیم دقیق قوائد عملیات سایبری نیست. این موضوع به علت پیچیدگی فضای سایبر، ماهیت فناوری و نیاز به تطبیق قوانین موجود با تحولات تکنولوژی است. بسیاری از قوائد بین‌المللی قبلی، مانند قوائد مربوط به حمله مسلحانه، جنگ یا حقوق بشر به‌صورت مستقیم برای عملیات سایبری اعمال نمی‌شوند. در عوض، برخی از اصول و مفاهیم کلی قابل اعمال بر روی عملیات سایبری می‌باشند. بنابراین قوائد دقیق در ارتباط با عملیات سایبری وجود ندارد و بسیاری از مفاهیم و قوائد بین‌المللی موجود ممکن است قابل تطبیق با عملیات سایبری نباشند. این یکی از چالش‌های قابل توجه در حوزه حقوق بین‌المللی است که با پیشرفت فناوری و رو به رشد بودن عملیات سایبری، نیاز به توسعه قوائد و استانداردهای جدید را برای این حوزه به وجود آورده است. یکی از این مفاهیم انجام عملیات و حملات سایبری از طرف یک دولت به دولت دیگر تحت قاعده دفاع مشروع است. در این پژوهش ضمن شناسایی حملات سایبری، به بررسی این سؤال پرداخته شد که از منظر حقوق بین‌الملل، حملات سایبری به یک کشور در وضعیت حاد دفاع مشروع که هستی دولتی در خطر است مجاز یا ممنوع می‌باشد؟ بررسی‌های صورت گرفته به‌صورت توصیفی ـ تحلیلی می‌باشد و فرضیه نگارنده این بود که دولت‌ها ممکن است در مقام دفاع مشروع به علت ویژگی‌های خاص عملیات‌های سایبری، از جمله قدرت تخریب بالا و جبران‌ناپذیر از این نوع حملات بهره برند.

واژگان کلیدی: حملات سایبری، حق دفاع مشروع، حقوق بین‌الملل بشردوستانه، شروط دفاع مشروع.

دریافت مقاله: ۱۴۰۳/۰۱/۲۷ -بازنگری مقاله: ۱۴۰۳/۰۴/۰۷ -پذیرش مقاله: ۱۴۰۳/۰۵/۱۷

ارجاع:
غلام‌حیدری، صالح؛ (۱۴۰۳)، امکان‌سنجی دفاع مشروع از طریق حملات سایبری، تمدن حقوقی، شماره ۲۰.

مقدمه

در دهه‌های اخیر، با پیشرفت فزاینده فناوری اطلاعات و ارتباطات، حملات سایبری به یکی از چالش‌های امنیتی بزرگ در سراسر جهان تبدیل شده‌اند. حملات سایبری، عمدتاً به وسیله افراد یا گروه‌هایی که دسترسی غیرمجاز به سیستم‌ها و شبکه‌های رایانه‌ای دارند، انجام می‌شوند و به منظور بهره‌برداری از ضعف‌ها و آسیب‌پذیری‌های موجود در سیستم‌ها، اطلاعات حساس را نقض می‌کنند، سرویس‌های مهم را مختل می‌کنند و در برخی موارد، می‌توانند ضررهای مالی و عملیاتی قابل توجهی به همراه داشته باشند.

در سال ۲۰۱۹ میلادی، دو حمله سایبری رخ دادند. یکی از آن‌ها حمله ای[1] بود که شهر بالتیمور در ایالت مریلند امریکا را هدف قرار داد. در این حمله، سیستم‌های شهری تحت حمله قرار گرفتند و فایل‌ها رمزگذاری شدند. این حمله باعث اختلال شدید در عملکرد سرویس‌های شهری مانند سامانه ترافیک و پرداخت مالی شد.[2] حمله دیگری که در سال ۲۰۱۹ میلادی رخ داد، حمله ای[3] بود که در ایرلند رخ داد. در این حمله، سیستم‌های شبکه حمل‌ونقل عمومی راه‌آهن شهری[4] تحت حمله قرار گرفت و تا حدودی تأثیرات منفی بر روی خدمات ارائه شده داشت.[5] یکی از حملات سایبری مهم در سال ۲۰۱۷ میلادی، حمله

1. Baltimore ransomware
2. https: //statescoop.com/baltimore-ransomware-crowdstrike-extortion/
3. Luas cyberattack
4. Luas
5. https: //www.irishexaminer.com/news/arid-30895306.html

رنسومر[۶] بود. این حمله، با استفاده از نرم‌افزار رنسومر[۷]، که به سیستم‌های ویندوز وارسی شده نفوذ می‌کرد، میلیون‌ها سیستم را در سراسر جهان تحت تأثیر قرار داد و نشان داد که حملات سایبری می‌توانند آسیب‌های عمده‌ای به زیرساخت‌های حیاتی ایجاد کنند.[۸] این حملات به هکرهایی از کره شمالی منتسب شده است.[۹]

می‌توان به چند حمله سایبری بزرگ دیگر اشاره کرد که در جهان رخ داده‌اند و نشان می‌دهند که حملات سایبری به‌صورت جنگ‌های سایبری نیز می‌توانند تأثیرات عمده‌ای داشته باشند: در سال‌های ۲۰۱۵ میلادی و ۲۰۱۶ میلادی، اوکراین شاهد یک سری حملات سایبری گسترده بود. در یک حمله مشهور، شبکه برق اوکراین تحت حمله قرار گرفت و برق در برخی مناطق این کشور قطع شد.[۱۰] این حمله نشان داد که حملات سایبری می‌توانند به زیرساخت‌های بحرانی یک کشور وابسته باشند و زندگی روزمره مردم را تحت تأثیر قرار دهند. این مثال‌ها نشان می‌دهند که حملات سایبری به‌صورت جنگ‌های سایبری می‌توانند به امنیت ملی و بین‌المللی تأثیر به سزایی بگذارند. این نمونه‌ها فقط بخشی از حملات سایبری واقعی هستند که در سال‌های اخیر رخ داده‌اند. آن‌ها نشان می‌دهند که حملات سایبری می‌توانند به کلیه نقاط جهان تأثیر بگذارند و به مردم، سازمان‌ها و زیرساخت‌های حیاتی آسیب برسانند.

از طرفی دیگر مطابق بند چهارم ماده ۲ منشور سازمان ملل متحد که در آن ذکر شده است «کلیه اعضاء در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر روش دیگری که با مقاصد ملل متحد مباینت داشته باشد خودداری خواهند نمود.» توسل به زور در روابط میان دولت‌ها ممنوع اعلام شده است. ممنوع کردن توسل به زور به‌صورت مطلق و بدون هیچ استثنائی، در واقعیت موجود در روابط میان دولت‌ها امکان‌پذیر نخواهد بود. همواره احتمال وقوع وضعیت‌هایی خواهد بود که جامعه جهانی در کل و یا دولت‌ها به‌صورت فردی یا جمعی ناچار به انجام اقدامات واکنشی شوند. ازاین‌رو منشور سازمان ملل متحد در حمایت از اعضاء سازمان ملل متحد و افزایش کارآمدی، دو استثناء در جهت استفاده از زور پیش‌بینی کرده است. این دو استثناء عبارتند از: اقدامات قهری شورای امنیت سازمان ملل متحد مطابق ماده ۴۲ منشور و دفاع مشروع فردی یا جمعی مطابق ماده ۵۱ منشور.

6. WannaCry ransomware
7. WannaCry
8. https: //www.kaspersky.com/resource-center/threats/ransomware-wannacry
9. Hern, Alex, "WannaCry, Petya, NotPetya: How Ransom Ware Hit the Big Time in 2017", The Guardian, https: //www.Theguar dian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware
10. https: //en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack

در این پژوهش به استثناء دوم که دفاع مشروع است، از این جهت خواهیم پرداخت که بررسی کنیم، با توجه به قواعد معاهداتی یا عرفی موجود و آرای قضایی آیا حملات سایبری به‌عنوان بخشی از دفاع مشروع در مقابل حمله نظامی‌مندرج در ماده ۵۱ منشور که شرط اصلی توسل به دفاع مشروع ذکر شده است امکان‌پذیر است؟ آیا یک دولت که از زمین یا هوا یا دریا مورد حمله نظامی قرار گرفته است، می‌تواند به کشور متجاوز حمله سایبری انجام دهد؟ پاسخ به این سؤال‌ها از جهات مختلفی می‌تواند حائز اهمیت باشد. اول فراگیر شدن استفاده از حملات سایبری در مخاصمات به‌عنوان بخشی از ابزار پیشبرد اهداف سیاسی و نظامی است چراکه به علت شرایط خاص این حملات از جمله پیچیده بودن قابلیت انتساب و همچنین آثار بسیار گسترده‌ای که روی کشور مورد حمله قرار گرفته می‌گذارد، کشورها امروزه تمایل بیشتری به استفاده از این حملات دارند. دوم آثار بسیار زیادی است که حملات سایبری می‌تواند بر روی کشور قربانی حملات بگذارد که باید در این خصوص بررسی شود تا چه آستانه‌ای این حملات احتمالا بلااشکال و چه آستانه‌ای ممکن است سبب نقض قوائد حقوق بشر و حقوق بشردوستانه شود. در اینجا لازم است ابتدا به ارائه تعریفی از حملات سایبری، انواع آن، تفکیک آن با جرائم سایبری و تروریسم سایبری بپردازیم.

۱- مفهوم حملات سایبری، عملیات سایبری و جنگ سایبری

در طول تاریخ، بشر به دنبال پیشبرد برنامه‌های ملی در یک بازی بین‌المللی قدرت بوده است. از نبردهای شمشیر در گذشته تا حملات پهپادهای بدون سرنشین امروزی، این بازی قدرت به‌طور مداوم توسط فناوری به سمت تغییر و تحول سوق داده می‌شود. وابستگی روزافزون جهان به سیستم‌های به هم‌پیوسته و زیرساخت‌های دیجیتالی شده، حملات سایبری را به‌عنوان یک نگرانی مهم ظاهر کرده‌اند و زیرساخت‌های حیاتی، دولت‌ها، مشاغل و افراد را به‌طور یکسان هدف قرار می‌دهند. در جنگ‌های امروزی، حملات سایبری ممکن است به‌عنوان یک ابزار قدرتمند در دسترس دولت‌ها، به‌عنوان دفاع مشروع در یک مخاصمه مسلحانه مورد استفاده قرار می‌گیرند. بنابراین، فهم نحوه مرسوم شدن حملات سایبری در جنگ‌ها اهمیت بسیاری دارد.

برای بیش از دهه‌ها، تحلیلگران درباره پیامدهای حملات سایبری پیش‌بینی‌هایی داشته‌اند. پیش‌بینی‌هایی نظیر غیرفعال کردن بازار سهام (Hollis; 2007) تا یک پیام نادرست که باعث خاموش

شدن یک راکتور هسته‌ای (Antolin-Jenkins, 2005) یا باز شدن یک سد می‌شود و یا قطع برق سیستم کنترل ترافیک هوایی که منجر به سقوط هواپیماها شود.[11] اگر چه هیچ‌یک از این سناریوها با وسعت بالا تاکنون رخ نداده است، اما حوادث سایبری بسیاری با مقیاس کوچک سالانه در جای جای جهان رخ می‌دهند (Kelsey, 2009). با این حال هیچ تعریف قطعی از حملات سایبری تاکنون وجود ندارد.

ابتدا باید این نکته را مطرح کرد که حملات سایبری، متفاوت از جرایم سایبری هستند. جرائم سایبری جرایمی هستند که در قوانین جزایی داخلی مورد بررسی قرار گرفته و مواردی مانند سرقت هویت و یا کلاه‌برداری اینترنتی را شامل می‌شود (Ayalew, 2014). به عبارت دیگر جرائم سایبری شامل یک طیف گسترده‌ای از فعالیت‌های غیرقانونی است. برخلاف حملات سایبری، جرم‌های سایبری نیازی به تضعیف شبکه رایانه‌ای هدف ندارند (اگرچه در برخی موارد ممکن است این اتفاق بیفتد) و همچنین بیشتر آن‌ها هدف سیاسی یا امنیت ملی ندارند و در نهایت جرم‌های سایبری به طور کلی به‌عنوان اقدامات انفرادی و نه توسط دولت‌ها تعریف می‌شود.

تعاریف موجود برای جنگ سایبری نیز بسیار متفاوت هستند. یکی از تعاریفی که بیشتر از سایرین نقل می‌شود، از جانب متخصص امنیتی دولتی «ریچارد آ. کلارک»[12] آورده شده است که به‌عنوان «اقدامات یک کشور در نفوذ به کامپیوترها یا شبکه‌های دیگر کشوری به منظور ایجاد آسیب یا اختلال» تعریف جنگ سایبری را می‌دهد (Clarke & Knake, 2011). به طور مشابه، «مایکل هیدن»، مدیر سابق سازمان امنیت ملی ایالات متحده امریکا[13] و سازمان سیا[14] درباره جنگ سایبری به‌عنوان «تلاش آگاهانه برای غیرفعال کردن یا نابود کردن شبکه‌های کامپیوتری یک کشور دیگر» صحبت کرده است (Gjelten, 2009). با این حال، این تعاریف تمایزی میان حمله سایبری و جنگ سایبری قائل نمی‌شوند. به همین دلیل، آن‌ها در معرض استفاده بیش از حد گسترده از چهارچوب جنگ در زمینه سایبر قرار می‌گیرند.

علاوه بر این، تعریف کلارک به نظر خیلی محدود است. تعریف کلارک تا حدی محدود می‌شود به حملاتی که توسط دولت‌ها انجام می‌شود و در نتیجه، به طور کامل سناریوهای معقولی را که حملات توسط عوامل غیردولتی انجام می‌شوند را از بین می‌برد. کارشناسان فنی تعاریف محدودتری را پیشنهاد

11. U.S. Gen. Accounting Office, 2010
12. Richard A. Clarke
13. NSA
14. CIA

داده‌اند. به‌عنوان مثال، مارتین لیبیکی، جنگ سایبری را این گونه تعریف می‌کند: «حملات دیجیتالی که باعث می‌شوند سیستم‌ها به نظر عادی عمل کنند، درحالی‌که در واقع پاسخ‌های مغایر با واقعیت را تولید می‌کنند» (Libicki, 1995). اما همین تعریف نیز در بر دارنده طیف گسترده‌ای از تهدیدهای ممکن به امنیت ملی یک کشور که به زیرساخت‌های سایبری هدف می‌شوند نیست، چراکه تنها شامل یک نوع از جنگ‌ها است. هر تعریفی از حمله سایبری که آن‌ها را مستثنی کند، به طور ضروری ناقص است.

تعریفی مطابق نسخه دوم تالین[۱۵] نیز وجود دارد که در آن مقرر می‌دارد: «حمله سایبری[۱۶]، عملیات سایبری تهاجمی یا تدافعی است که از آن به‌طور معقول انتظار ایراد صدمه یا مرگ به اشخاص و یا وارد کردن خسارات به اشیاء می‌رود.» در مجموع، می‌توان این تعریف را از حملات سایبری ارائه نمود: اقداماتی که از سوی یک دولت برای هدف قرار دادن زیرساخت‌های اساسی یک دولت دیگر از جمله سیستم بانکی، انرژی و حمل‌ونقل عمومی که به شبکه رایانه‌ای متصل هستند صورت می‌پذیرد (خلیل‌زاده، ۱۳۹۳، ۳۳). در نهایت همان‌طور که در بالا گفته شد حملات سایبری درصورتی‌که در مقیاس و مختصات و آستانه بالایی صورت گیرد، می‌توانیم از آن به‌عنوان جنگ سایبری نام ببریم.

بعد از آشنایی با مفاهیم سایبری و برخی از مدل‌های حملات، برای پاسخ به سؤال اصلی این پژوهش، که همان امکان سنجی انجام عملیات سایبری و حملات سایبری در قالب دفاع مشروع هست از دو مبحث استفاده خواهیم کرد. مورد اول مفهوم دفاع مشروع و شروط آن است که در بخش بعدی به آن خواهیم پرداخت تا از آن مستمسک برای پاسخ به سؤال خود پیدا کنیم و دوم بهره‌گیری از قوائد راهنمای تالین که در بخش سوم ضمن آشنایی با تالین، به مطالعه قوائد مربوطه به سؤال خواهیم پرداخت.

15. Tallinn Manual 2.0

۱۶. الف: حملات Dos با پر کردن درخواست‌های جعلی و وادار کردن وب‌سایت‌ها به رسیدگی به این درخواست‌ها، از دسترسی کاربران قانونی به وب‌سایت‌ها جلوگیری می‌کند. این نوع حمله می‌تواند برای ایجاد اختلال در عملیات‌ها و سیستم‌های حیاتی و مسدود کردن دسترسی غیرنظامیان، پرسنل نظامی و امنیتی یا نهادهای تحقیقاتی به وب‌سایت‌های حساس استفاده شود. ب: حملات آپلود بالا: در این نوع حملات، حمله‌کننده سعی می‌کند منابع یک سرویس را با ترافیک بالا و غیرمعمول سرازیر کند. این باعث اشباع شدن پهنای باند، منابع سخت‌افزاری و نرم‌افزاری سرویس می‌شود و در نتیجه، کاربران عادی قادر به دسترسی به سرویس نمی‌باشند. حملات انکار سرویس توزیع شده زیرمجموعه حملات انکار سرویس هستند. ج: نفوذ به سیستم‌های مهم: حمله‌کنندگان می‌توانند به سیستم‌های مهم یک سرویس یا شبکه نفوذ کرده و کنترل آن‌ها را به دست بگیرند. این کار به آن‌ها امکان می‌دهد تا داده‌ها را تخریب، تغییر دهند یا سرویس را به‌صورت کامل قطع کنند.

۲- مفهوم دفاع مشروع

حق دفاع مشروع در قرارداد عمومی برای مردود شمردن جنگ[17] در ۱۹۲۸ میلادی محترم شمرده شد و اعلام گردید که این حق در ذات حاکمیت کشور هر دولت و در هر پیمان به طور ضمنی وجود دارد. بعدها بر اساس منشور سازمان ملل، دو استثناء در ممنوعیت استفاده از نیرو وجود دارد: اقدام شورای امنیت سازمان ملل بر اساس ماده ۴۲ و دفاع فردی یا جمعی بر اساس ماده ۵۱ منشور. شروط حق دفاع مشروع، اولین بار در قضیه کارولین توسط دانیل وبستر[18] عنوان شد. در سال ۱۸۳۷ میلادی، حکومت کانادا به کشتی امریکایی کارولین که در اجاره شورشیان بود حمله کرد و پس از تصرف تسلیحات آن، کشتی را به آتش کشید که منجر به کشته شدن دو امریکایی و زخمی شدن چند تن دیگر شد. ایالات متحده امریکا، توسل حکومت کانادا به دفاع مشروع را تحت شرایطی که وزیر خارجه این کشور، وبستر اعلام داشت قابل پذیرش دانست و بعدها این شرایط تحت عنوان فرمول وبستر به یک مرجع عرفی دفاع مشروع مبدل شد (Shaw, 1977).

شروط حق دفاع مشروع را می‌توان به شروط قبل و بعد از دفاع تقسیم کرد. شروطی برای قبل از دفاع مانند تقدم تجاوز بر دفاع یا ماهیت تجاوز وجود دارد اما در این پژوهش ما قصد بررسی آن‌ها را نداریم و فرضی را مطرح می‌کنیم که تمامی شروط قبل از دفاع محقق شده است. اما برای شروط بعد از دفاع بر اساس شروط وبستر، پاسخ یک دولت به یک حمله مسلحانه باید سه ویژگی داشته باشد که به‌عنوان حق دفاع از خود معتبر محسوب شود: ضرورت[19]، تناسب[20] و فوریت.[21]

۲-۱- شرط‌های ضرورت و تناسب

استفاده از نیرو توسط یک کشور به منظور اجرای حق دفاع مشروع که نیز شامل عملیات سایبری نیز می‌تواند باشد، باید ضروری و تناسب‌پذیر باشد. به عبارت دیگر، تدابیر اتخاذ شده در حق دفاع باید دو معیار ضرورت و تناسب را برآورده کنند. دیوان بین‌المللی دادگستری در ابتدا این دو معیار را در پرونده نیکاراگوئه و سپس در پرونده سکوهای نفتی پذیرفت.[22] دادگاه نورمبرگ نیز این معیار را تأیید کرده

17. General Treaty for the Renunciation of war
18. Daniel Webster
19. Necessity
20. Proportionality
21. Immediacy

۲۲. رجوع شود به پرونده فعالیت‌های نظامی و شبه نظامی در و علیه نیکاراگوئه، بندهای ۱۹۴ و ۲۳۷ و پرونده سکوهای نفتی، بندهای ۴۳، ۷۳ و ۷۴.

است. همان‌طور که در این تصمیم‌ها ذکر شده است، این دو معیار نمایانگر حقوق بین‌الملل عرفی در این زمینه هستند (باید توجه داشت که مفهوم ضرورت و تناسب با مفهوم ضرورت نظامی و قاعده تناسب در حقوق بشردوستانه و حقوق در جنگ[۲۳] متفاوت است).

ضرورت، استفاده از نیرو به منظور دفع یک حمله فوری یا شکست دادن یک حمله در حال وقوع است. این بدان معنا نیست که ضروری است استفاده از نیرو تنها پاسخ ممکن به حمله مسلح باشد، بلکه تنها ضروری است که اقدامات غیرخشونت‌آمیز در برابر وضعیت به وجود آمده کافی نباشد. البته اقدامات نظامی ممکن است همراه با اقدامات غیرنظامی مانند دیپلماسی، تحریم‌های اقتصادی و غیره صورت گیرد. شرایط ضرورت و تناسب عوامل اصلی هستند که در تعیین قانونی بودن یا اصالت درخواست یک کشور برای استفاده از حق دفاع از خود در نظر گرفته می‌شوند. الزامات ضرورت و تناسب از قوانین بین‌المللی عرفی ناشی می‌شوند که قبل از سال ۱۹۴۵ میلادی وجود داشته‌اند و اغلب به حادثه کارولین از سال ۱۸۳۷ میلادی باز می‌گردند. با این حال، این اصول پس از تصویب منشور سازمان ملل متحد نیز باقی مانده‌اند.[۲۴]

این اصول بیان می‌کنند، کشوری که قربانی یک حمله مسلحانه است، مجاز به استفاده از زور علیه حمله‌کننده است، اما این استفاده از زور تنها به اندازه‌ای باید باشد که برای دفاع از خود و دفع حمله لازم باشد. ضرورت فرض می‌کند حمله مسلحانه ادامه دارد و نیاز به متوقف کردن حمله است. اصل ضرورت مقتضی می‌کند که برای توجیه یک اقدام در دفاع از خود، یک کشور باید نشان دهد که اقدامی که انجام داده تنها گزینه موجود در شرایط حمله مسلحانه بوده است و راه دیگری برای دفع حمله وجود نداشته است. در مورد عواقب قانونی ساخت دیوار در سرزمین فلسطین اشغالی، گزارش‌های دیوان بین‌المللی دادگستری در سال ۲۰۰۴ میلادی دیوان بین‌المللی دادگستری در قضیه سد گابچیکوناگیماروس بر آن است که حالت ضرورت زمانی قابل طرح است که وجود یک منفعت اساسی[۲۵] در میان باشد. آن گاه دیوان بین‌المللی دادگستری اعلام می‌دارد که منفعت اساسی باید به با یک خطر شدید و فوری مورد تهدید قرار گرفته باشد (بیگ زاده، ۱۴۰۱، ۸۰۹).

تناسب نیز، به مجموعه ابزارهای استفاده شده برای دفع حمله مسلحانه و رابطه آن با حمله می‌پردازد.

23. Jus In Bellum

۲۴. در قضیه نیکاراگوئه، قانونی بودن تهدید یا استفاده از سلاح‌های هسته‌ای و گزارش‌های دیوان بین‌المللی دادگستری در سال ۱۹۹۴ میلادی.

25. Essential Interest

بنابراین، یک نوع مقایسه بین شدت حمله مسلحانه و میزان نیروی استفاده شده برای دفاع از آن انجام می‌شود. برای استفاده قانونی از حق دفاع مشروع، یک کشور نباید از میزان نیروی مورد نیاز برای دفع حمله مسلحانه علیه خود فراتر رود. الزامات ضرورت و تناسب بر این اصل تأسیس شده‌اند که هدف دفاع مشروع پایان دادن به وضعیت غیرقانونی ناشی از حمله مسلحانه است و چیز دیگری نیست. بنابراین، دفاع از خود نباید انتقامی یا تنبیهی باشد.

این نکته قابل توجه است که ضرورت و تناسب به‌عنوان شرایطی برای استفاده از حق دفاع مشروع، الزاماً تعیین نمی‌کنند که یک کشور که قربانی یک حمله مسلحانه است، صرفاً باید از درجه و نوع نیرو و حتی از همان سلاح‌های کشور حمله‌کننده استفاده کند، بلکه کشور برای به درستی عمل کردن در دفاع از خود، باید از نیرویی استفاده کند که نسبت به آنچه برای دستیابی به اهداف مشروع دفاع از خود نیاز است، تناسب داشته باشد. با این حال، یک عامل مهم مورد استفاده در بررسی ضرورت دفاع از خود، طبیعت سلاح استفاده شده است. در تعیین قانونی بودن استفاده از حق دفاع مشروع از نظر ضرورت و تناسب، پس از این که شرط اول برآورده شود، دادگاه و یا دیوان بین‌المللی دادگستری به شرط دوم می‌پردازد و اگر این شرط نیز برآورده شود، در این صورت ادعای دفاع مشروع توجیه می‌شود.

به این ترتیب، یک اقدام ممکن است شرط ضرورت را برآورده کند، اما تطابق با شرط تناسب را برآورده نکند. در این حالت، ادعای دفاع مشروع توجیه نمی‌شود. اما درصورتی‌که شرط ضرورت برآورده نشود، دیگر نیازی نیست تا به شرط تناسب بپردازیم.[۲۶] البته لازم به ذکر است که معیار مشخصی برای تعیین ضرورت یا تناسب در دفاع از خود وجود ندارند. همه چیز به واقعیت‌های یک پرونده خاص وابسته است. در مورد نیکاراگوئه، دیوان رأی داد که حملات ایالات متحده امریکا علیه نیکاراگوئه، در به اندازه‌ای که این اعمال بر اساس حق دفاع مشروع بنا شده باشد، لازم نبود و نیز نسبت به کمک‌های ادعا شده دولت نیکاراگوئه به السالوادور تناسب نداشته است.[۲۷] الزامات ضرورت و تناسب همچنان به‌عنوان راهنمای اصلی در تعیین مشروع بودن ادعای حق دفاع مشروع باقی می‌مانند. هر کشوری که یک طرف اختلاف است و حق دفاع مشروع مطرح می‌شود، دلیلی را از سمت خود مطرح می‌کند که به منافع خودش بیشتر همراه باشد. اما

---

۲۶. در مورد پرونده سکوهای نفتی (ایران در برابر ایالات متحده امریکا) و گزارش‌های دیوان بین‌المللی دادگستری در سال ۲۰۰۳ میلادی.

۲۷. نیکاراگوئه پاراگراف ۲۳۷

دیوان بین‌المللی دادگستری، پس از بررسی واقعیت‌های پرونده تصمیم می‌گیرد.

همان‌طور که بیان شد شروط دفاع مشروع به شروط قبل از دفاع و در زمان دفاع تقسیم شد. توجه به شروط در زمان اجرای حق دفاع مشروع و به‌خصوص شرط تناسب مهم و قابل تأمل است. شرط تناسب به‌طور ویژه در خلال بحث‌های مربوط به مشروعیت تهدید یا کاربرد تسلیحات اتمی در مقابل دیوان بین‌المللی دادگستری مورد توجه قرار گرفت. عده‌ای بر آن نظر بودند که با توجه به آثار مخرب بسیار شدید تسلیحات اتمی، این گونه تسلیحات نمی‌توانند در قالب دفاع مشروع مورد استفاده قرار گیرند.

در مقابل ارزیابی دیوان بین‌المللی دادگستری بر آن است که اصل تناسب به خودی خود نمی‌تواند توسل به تسلیحات هسته‌ای را در دفاع مشروع و در کلیه وضعیت‌ها ممنوع کند و آن چیزی که باید مورد توجه و ملاحظه قرار گیرد ماهیت این‌گونه تسلیحات و خطرات شدیدی که توسل به آن‌ها ایجاد می‌کند است. دیوان بین‌المللی دادگستری با اشاره به رای نیکاراگوئه که در آن اعلام نموده بود اقدامات صورت گرفته در چهارچوب دفاع مشروع باید متناسب با حمله مسلحانه و ضروری باشد اظهار داشت «اصل تناسب به‌تنهایی نمی‌تواند مانع از استفاده از سلاح‌های هسته‌ای در دفاع مشروع در تمامی شرایط شود، ولی درعین‌حال استفاده از نیرو مسلحانه به گونه‌ای که بر اساس قواعد دفاع مشروع متناسب می‌باشد، باید همچنین به منظور مشروع بودن، شرایط پیش‌بینی شده در قواعد حاکم بر مخاصمات مسلحانه را که به‌ویژه شامل اصول و قواعد حقوق بشردوستانه می‌شود رعایت نمایند.» از این عبارات مشخصا می‌توان نتیجه گرفت که دربارهٔ سلاح‌هایی که تاکنون در حقوق بین‌الملل موضوعه یا عرفی، قائده قطعی دربارهٔ جواز یا عدم جواز نداریم، شرط استفاده از آن‌ها در قالب دفاع مشروع در نظر گرفتن و لحاظ کردن قوائد حقوق بشردوستانه است.

می‌توان با کسب وحدت ملاک از این رای مشورتی دیوان بین‌المللی دادگستری که در ارتباط با به‌کارگیری سلاح‌های هسته‌ای است، دربارهٔ حملات سایبری نیز به نتیجه در مورد جواز یا عدم جواز از منظر حقوق بین‌الملل برسیم. با ظهور تکنولوژی سایبری در قرن بیست و یکم، مشکلاتی در چگونگی اعمال استانداردهای اخلاقی حقوق بشر دوستانه[۲۸] در فضای سایبری به وجود آمده است. حقوق بشردوستانه، مجموعه مقررات و قواعد حقوق بین‌الملل است که ضمن تعیین حقوق حمایت از افراد انسانی اعم از رزمنده یا غیررزمنده و اموال غیرنظامی و حقوق طرف‌های متخاصم در مخاصمات مسلحانه اعم از بین‌المللی یا غیربین‌المللی تکالیف افراد انسانی و طرف‌های متخاصم را نیز در آن مخاصمات مشخص می‌کند

28. Internatiomal humanitarian law– IHL

(ضیایی‌بیگدلی، ۱۴۰۱). هدف حقوق بشردوستانه، محدود کردن صدمات و لطمات ناشی از درگیری‌های مسلحانه و ممنوع کردن استفاده از برخی وسایل و شیوه‌های نبرد علیه رزمندگان (تحت شرایط خاصی) افراد غیرنظامی و نیز اهداف غیرنظامی در مخاصمات مسلحانه است (ضیایی‌بیگدلی، ۱۴۰۱).

در قسمت اخیر همین تعریف که ارائه گردید حقوق بشردوستانه قوائد لازم الاجرا در زمان مخاصمات مسلحانه است و با احتساب این تعریف باید دنبال رهیافتی برای شناسایی حملات سایبری به مثابه نقض حقوق بشردوستانه باشیم. عبارت مخاصمه مسلحانه[۲۹] در اثنای تدوین قوائد حقوق جنگ در کنفرانس‌های سال ۱۹۴۹ میلادی به کار رفت و از مطالعه ماده ۲ مشترک کنوانسیون‌های ژنو این گونه برداشت می‌شود که نوع سلاح و ادوات به کار رفته اثری در اعمال قوائد حقوق بشردوستانه ندارد و این قوائد در عملیات سایبری در جریان سایر مخاصمات مسلحانه نیز قابلیت اعمال دارد. قانون مخاصمات مسلحانه به همان اندازه که برای هر عملیات دیگری در زمینه یک مخاصمه مسلحانه مربوط است، بر عملیات سایبری نیز اعمال می‌شود. با وجود نوآوری عملیات سایبری و عدم وجود موارد خاص در قوائد مخاصمات مسلحانه که به طور صریح به آن‌ها بپردازد، گروه بین‌المللی کارشناسان که وظیفه تنظیم راهنمای تالین را داشتند، در یافتن این که قوائد مخاصمات مسلحانه برای چنین فعالیت‌هایی در مخاصمات مسلحانه بین‌المللی و غیربین‌المللی اعمال می‌شود، هم نظرند (Schmitt, 2013).

شرط اولیه برای اعمال این قوائد، وجود یک مخاصمه مسلحانه است. اصطلاح «مخاصمه مسلحانه» برای اولین بار در مجموعه قوانین جنگ در کنوانسیون ژنو ۱۹۴۹ میلادی استفاده شد، اما تاکنون به‌طور رسمی تعریف نشده است. امروزه این اصطلاح به جای عبارت «جنگ» استفاده می‌شود. بر اساس راهنمای تالین که در قسمت بعدی پژوهش به آن پرداخته خواهد شد، می‌توان گفت پیش شرط قابلیت اجرای قواعد حقوق بین‌الملل بشردوستانه وجود یک مخاصمه مسلحانه است. این اصطلاح برای توصیف مخاصمات مسلحانه بین‌المللی و غیربین‌المللی به معنای متفاوتی در نظر گرفته می‌شود. قواعد ۲۲ و ۲۳ نسخه اول تالین میزان آستانه‌ای که برای رسیدن به حدود مخاصمه مسلحانه لازم است را بررسی می‌کنند. برای توضیح، در سال ۲۰۰۷ میلادی استونی هدف عملیات سایبری مداوم قرار گرفت. با این حال، قانون مخاصمات مسلحانه برای آن عملیات سایبری اعمال نمی‌شد زیرا وضعیت به حد منازعه مسلح نرسیده بود. در مقابل، قوائد منازعات مسلحانه بر عملیات سایبری که در منازعه مسلحانه بین گرجستان و روسیه در

29. Armed Conflict

سال ۲۰۰۸ میلادی صورت گرفت، اعمال شد زیرا که این عملیات به منظور پیشرفت آن مخاصمه انجام شده بود (Schmitt, 2013). از نظر کمیته بین‌المللی صلیب سرخ نیز، موارد زیر جنگ سایبری موضوع حقوق بشردوستانه قرار می‌گیرد: اگر در وسایل و شیوه‌های جنگی از فضای سایبری استفاده شود و اگر در یک درگیری مسلحانه، عملیات سایبری علیه دشمن به کار رود و منجر به ورود خسارت به او گردد.[۳۰]

با این استدلال بر عملیات‌های سایبری با این شروط می‌توان قوائد حقوق بشردوستانه را اعمال کرد و این عملیات‌ها باید مطابق با اصول حقوق بشردوستانه باشد. پاره‌ای دیگر از حقوقدانان نیز معتقدند که اعمال رژیم حقوقی کنونی حقوق بین‌الملل بشردوستانه در حوزه سایبری امری دشوار است. چراکه پیچیدگی فنی موضوع مورد بحث، باعث بروز مشکلاتی در انطباق قواعد حقوق بین‌الملل بشردوستانه در این حوزه خواهد شد. استدلال این افراد بر این مبنا است که فضای سایبری مکان عینی نیست و یک فضای انتزاعی است (برادران و حبیبی، ۱۳۹۸). در پاسخ اما می‌گویند که فضای سایبری یک فضای تخیلی نیست که هیچ ارتباطی با دنیای بیرون نداشته باشد سخت افزارها و شبکه‌ها (حتی شبکه‌های بیسیم و مجازی) به یک ساختار فیزیکی نیازمندند. ایراد دیگری که می‌گیرند این است که در هیچ‌یک از اسناد حقوق بشردوستانه اسم و نامی از سلاح‌های سایبری نیامده است. باید توجه داشت که اگر چه تا به‌حال هیچ قانون یا توافقنامه‌ای در قواعد حقوق بین‌الملل بشردوستانه وجود ندارد که به شکلی صریح به حملات رایانه‌ای اشاره‌ای شده باشد اما با توجه به شرط مارتنز که به اصول پذیرفته شده حقوق بین‌الملل مربوط است، هر زمان که موقعیتی تحت پوشش توافقات جهانی قرار نگرفته باشد، غیرنظامیان و مبارزان، تحت حمایت صلاحیت‌ها و اصول حقوق بین‌الملل که از عرف استقرار یافته است، اصول انسانی و درخواست وجدان عمومی سرچشمه می‌گیرد، قرار می‌گیرند (برادران و حبیبی، ۱۳۹۸).

دیوان بین‌المللی دادگستری در قسمتی دیگر اذعان می‌دارد کاربرد هر سلاحی را در صورتی در حکم کشتار دسته جمعی و نقض کنوانسیون‌های مربوطه می‌داند که چنین کاربردی با قصد نابودی[۳۱] همراه باشد. به نوعی این شرط را می‌توان عنصر روانی در نظر گرفت. عنصر روانی که به قصد و نیت طرفین درگیر می‌پردازد. در راستای ابزار نظامی تلقی‌شدن آنچه بیشتر مورد توجه هست هدف استفاده از ابزار می‌باشد که می‌تواند آن را داخل در ابزار تسلیحاتی قرار دهد و با این نگاه غایت محور ملزومات استفاده

---

۳۰. کمیته صلیب سرخ ۲۰۱۷ میلادی

31. Intent to destroy

شده در عملیات‌های سایبری از قبیل رایانه، اینترنت، کاربر و... می‌توانند به‌عنوان تسلیحات مورد توجه قرار گیرند (توحیدی و سیجانی، ۱۳۹۸). در مجموع با توضیحات ارائه شده می‌توان حملات سایبری را با شروطی که گفته شد «در خلال یک مخاصمه مسلحانه باشد، یا آستانه حملات به حدی باشد که مستقلا آن را یک حمله مسلحانه در نظر گرفت» اجرای آن‌ها را تحت قوائد حقوق بشردوستانه لازم دانست.

۲-۲- دیدگاه راهنمای تالین در ارتباط با دفاع مشروع

دستورالعمل تالین[۳۲] یک مجموعه قواعد و رهنمودهای حقوق بین‌المللی در حوزه عملیات سایبری است که توسط گروه کاری حقوق بین‌المللی در حوزه عملیات سایبری تهیه شده است. در سال ۲۰۰۹ میلادی، سازمان بین‌المللی نظامی واقع در تالین استونی با نام مرکز عالی همکاری دفاع سایبری که در سال ۲۰۰۸ میلادی از طرف ناتو به‌عنوان قطب علمی شناخته شده بود، از گروه بین‌المللی کارشناسان مستقل جهت نگارش دستورالعملی دربارهٔ قانون حاکم بر جنگ سایبری دعوت به عمل آورد. این پروژه که توسط متخصصین و محققان حقوق بین‌الملل طرح‌ریزی شد به دنبال تسری هنجارهای حقوقی و قانونی در این گونه جنگ‌های نوین است. این دستورالعمل اصول و قواعد حقوقی مرتبط با نحوه برخورد با حملات سایبری و جنگ سایبری را در قالب گزارشی جامع شرح می‌دهد. دستورالعمل تالین در دو نسخه منتشر شده است. هر دو نسخه به جزئیات حقوق بین‌المللی در حوزه سایبری پرداخته‌اند. اما تمرکز نسخه اول[۳۳] بر روی نحوه تعامل کشورها در جنگ سایبری بوده و نسخه دوم[۳۴] تمرکز خود را بر روی عملیات غیرجنگی سایبری، مانند حملات سایبری متقابل و مقابله با تهدیدهای سایبری، قرار داده است.

دستورالعمل تالین گزارشی جامع است که به بررسی مفاهیم و اصول حقوقی در حوزه عملیات سایبری می‌پردازد. این گزارش شامل تعریف حملات سایبری، استفاده از نیرو در فضای سایبری، حقوق و تعهدات کشورها در مورد حملات سایبری، استفاده از اسلحه سایبری و بسیاری از مسائل دیگر است. اهمیت دستورالعمل تالین در این است که تلاش می‌کند قوانین و اصول حقوقی را در حوزه سایبری تأمین کند و به کشورها راهنمایی می‌کند که با تهدیدات سایبری و حملات سایبری مواجه شده، چگونه عمل کنند و چه تدابیری را اتخاذ کنند. هر دو دستورالعمل تالین توسط گروه‌هایی از کارشناسان حقوق

32. Tallinn Manual
33. Tallinn Manual 1
34. Tallinn Manual 2

بین‌المللی توسط «مایکل ان. شمیت»[۳۵]، متخصص سایبری جهانی مشهور، جمع‌آوری شده‌اند. گروه اول شامل کارشناسان حقوق جنگی مسلح[۳۶] عمدتاً از کشورهای غربی بود. در پاسخ به انتقادات از نسخه اول تالین، گروه بین‌المللی کارشناسان برای نسخه دوم تالین گسترده‌تر بود، هم از نظر منشأ[۳۷] و هم از نظر تخصص موضوعی.[۳۸] کمیته بین‌المللی صلیب سرخ[۳۹] دعوت شد تا مشاهده‌گران خود را به هر دو گروه ارسال کند، همچنین دیگر کشورها و سازمان‌ها نیز دعوت شدند.

هدف اصلی این پروژه هرگز تبدیل شدن به قانون یا تولید کردن یک دستورالعمل با قوت قانونی نبود. همان‌طور که مقدمه واضح می‌کند: در نهایت، نسخه دوم تالین باید فقط به‌عنوان بیانی از نظرات دو گروه بین‌المللی کارشناسان درباره وضعیت قانون در نظر گرفته شود. این راهنما باید به‌عنوان بازنمای قانون در زمان تصویب آن توسط دو گروه بین‌المللی کارشناسان در ژوئن ۲۰۱۶ میلادی توصیف شود. به عبارت دیگر، نسخه دوم تالین به‌عنوان یک بیانیه بی‌طرف از قوائد موجود[۴۰] در نظر گرفته شده است.

نسخه دوم تالین با بحث درباره حاکمیت آغاز می‌شود و نکته‌ای که در قائده اول آن آمده است این است که «اصل حاکمیت بر فضای سایبری اعمال می‌شود». دو قائده بعدی بین حاکمیت داخلی و حاکمیت خارجی تفاوت قائل می‌شوند و قانون چهارم می‌گوید که «یک کشور نباید عملیات سایبری انجام دهد که حاکمیت یک کشور دیگر را نقض کند» (Schmitt, 2013). فرضیه زیربنایی که در نتیجه آن به نتیجه قائده چهارم می‌رسند، این است که حاکمیت یک قاعده از قوانین حقوق بین‌الملل است و نقض آن یک عمل غیرقانونی بین‌المللی است. توضیحات قائده چهارم بیان می‌کند: «در زمینه سایبری نقض حاکمیت، توسط اتباع یک کشور یا دیگران که رفتار آن‌ها می‌تواند به کشوری منتسب شود، به وسیله انجام عملیات سایبری، رخ می‌دهد. به‌عنوان مثال، اگر عاملی از یک کشور از طریق یک فلش مموری[۴۱]، نرم‌افزار مخربی را به زیرساخت سایبری موجود در کشور دیگری وارد کند، نقض حاکمیت اتفاق افتاده است» (Schmitt, 2013).

35. Michael N. Schmitt
36. LOAC

۳۷. شامل تایلند، ژاپن، چین و بلاروس.

۳۸. شامل کارشناسان حقوق بشر، حقوق فضایی و حقوق بین‌المللی مخابرات.

39. ICRC
40. lex lata
41. USB

با احتساب این قوائد، نسخه دوم تالین حمله سایبری را نقض حاکمیت دانسته است. با این وجود در چند مورد قوائدی را در ارتباط با دفاع مشروع به وسیله حملات سایبری بیان داشته است. در قائده ۱۹ شرایطی را که از نادرستی عملیات سایبری جلوگیری می‌کنند را بیان می‌دارد: رضایت[۴۲]، دفاع مشروع یا دفاع از خود[۴۳]، اقدامات متقابل[۴۴]، ضرورت[۴۵]، فورس ماژور[۴۶] و اضطرار.[۴۷] در ادامه به بیان برخی قوائد در ارتباط با هر کدام می‌پردازد که در اینجا قسمت حائز اهمیت درباره دفاع مشروع خواهد بود. قسمت یازدهم از همین قائده مقرر می‌دارد: طبق بند «ب»، عملیات سایبری که به‌عنوان دفاع مشروع در برابر یک حمله مسلحانه صورت گیرد، در زمینه حقوق بر جنگ[۴۸] به‌عنوان اعمال غیرقانونی بین‌المللی محسوب نمی‌شوند.[۴۹] به‌عنوان مثال، تشخیص یک عمل به‌عنوان دفاع مشروع همچنین باعث می‌شود که این عمل به‌عنوان نقض حاکمیت دولتی که حمله مسلحانه را انجام داده است، شناخته نشود.[۵۰] قائده در قسمت دوازدهم ادامه می‌دهد درصورتی‌که یک حمله مسلحانه منجر به شروع یک مخاصمه مسلحانه شود[۵۱]، این که پاسخ به‌عنوان دفاع مشروع قانونی شناخته شود، نمی‌تواند از غیرقانونی بودن هر نقضی از قوائد مخاصمه مسلحانه که ممکن است رخ دهد، جلوگیری کند. به‌عنوان مثال، تدابیر دفاعی نباید شامل حملات سایبری علیه غیرنظامیان[۵۲] یا اشیاء غیرنظامی[۵۳] باشد. به طور مشابه، این که عملیات در حالت دفاع مشروع انجام می‌شود، از نادرستی رفتار در مورد تعهدات حقوق بشر قابل اعمال[۵۴] که دولت از آن‌ها مستثنی نشده است[۵۵]، جلوگیری نمی‌کند (Schmitt, 2013).

42. Consent
43. Self-defense
44. Countermeasures
45. Necessity
46. Force majeure
47. Distress
48. Jus ad bellum

۴۹. قاعده ۷۱

۵۰. قاعده ۴

۵۱. قواعد ۸۲ و ۸۳

۵۲. قاعده ۹۴

۵۳. قاعده ۹۸

۵۴. قاعده ۳۵

۵۵. قاعده ۳۸

از این قوائد نیز در می‌یابیم که شرط استفاده از حملات سایبری به‌عنوان دفاع مشروع اعمال اصول حقوق بشردوستانه است. این اصول عبارتند از اصل تفکیک، مستخرج از قائده نودوسوم که اشعار دارد: در تفسیر معاهده سنت پترزبورگ سال ۱۸۶۸ میلادی، آمده است که «تنها هدف مشروع که دولت‌ها در طول جنگ باید سعی کنند به دست آورند، ضعیف کردن نیروهای نظامی دشمن است». این اصل عمومی، پایه‌ای است که بر اساس آن اصل تفکیک استخراج شده است. اصل تفکیک یکی از دو اصل «ابتدایی» حقوق مخاصمات مسلحانه است که توسط دیوان بین‌المللی دادگستری در نظریه مشورتی خود درباره قانونی بودن تهدید یا استفاده از سلاح‌های هسته‌ای به‌عنوان اصول حقوق عرفی بین‌المللی تأیید کرده است. دیگر اصل، ممنوعیت کشیدن درد غیرضروری است[۵۶] به گفته دیوان بین‌المللی دادگستری، این اصول حقوق عرفی بین‌المللی قابل نقض نیستند (Schmitt, 2013).

نتیجه

حق دفاع مشروع مطابق حقوق بین‌الملل عرفی و معاهداتی یک حق قطعی برای دولت‌ها است در مقابل حملاتی که موجودیت دولت‌ها را نشانه گرفته است. آن چنان که در ماده ۵۱ منشور سازمان ملل متحد مشخصا برای دولت‌ها این حق را در مقابل حملات مسلحانه در نظر گرفته است و حتی تا جایی این حق پیشرفته است که برخی دکترین این را استثنایی بر اصل منع توسل به زور می‌دانند. از طرفی حملات و عملیات‌های سایبری به سبب ویژگی‌های خاصی که دارد ممکن است به‌عنوان ابزاری برای دفاع مشروع استفاده شود.

سؤالی که درصدد پاسخ به آن در این پژوهش بودیم این سؤال بود که از منظر حقوق بین‌الملل آیا جواز یا عدم جوازی در این خصوص وجود دارد یا خیر؟ که پس از بررسی در قوائد موجود حقوق بین‌الملل و همچنین آراء قضایی، به طور مشخص دیوان بین‌المللی دادگستری و در نهایت با عنایت به راهنمای تالین که یک راهنمای غیرالزام‌آور ولی مهم در حوزه جنگ و عملیات‌های سایبری است می‌توان به این نتیجه دست یافت که قائده قطعی در این زمینه وجود ندارد و در این خصوص باید با کسب وحدت ملاک از رأی مشورتی دیوان بین‌المللی دادگستری در قضیه سلاح‌های هسته‌ای سال ۱۹۹۶ میلادی، در زمینه ابزاری و سلاح‌هایی که می‌تواند وسیله‌ای برای دفاع مشروع دولت‌ها قرار بگیرد که قائده مشخصی دربارهٔ ممنوعیت آن وجود ندارد، نقش تعیین‌کننده در حرمت یا جواز آن‌ها رعایت اصول حقوق بشردوستانه است.

---

۵۶. قاعده ۱۰۴

اگر استفاده از این ابزار و سلاح‌ها ناقض اصول حقوق بشردوستانه از قبیل اصل تفکیک، اصل منع تحمل رنج اضافی و... باشد قطعا ممنوع بوده و اگر این حملات ناقض این اصول نباشد ممنوعیتی در این خصوص نخواهد بود. آن چنان که در سال ۱۹۹۶ میلادی زمانی که دیوان بین‌المللی دادگستری در مقام پاسخ به سؤال مشورتی مجمع عمومی سازمان ملل متحد در ارتباط با حرمت یا جواز کاربرد سلاح‌های هسته‌ای بر می‌آید چنین استدلال می‌نماید که حرمت یا جوازی در استفاده از این حملات از منظر حقوق بین‌الملل کشف نشده است و در این خصوص ملاک رعایت اصول حقوق بشردوستانه است. همچنین در قائده نوزدهم نسخه دوم تالین یکی از عواملی که سبب عدم ممنوعیت حملات سایبری میان دولت‌ها می‌شود حملاتی است که در قالب دفاع مشروع صورت می‌گیرد و در ادامه این راهنما در قسمت دوازدهم همان قائده تأیید می‌کند که پاسخ به‌عنوان دفاع مشروع قانونی شناخته شود، نمی‌تواند از غیرقانونی بودن هر نقضی از قوائد مخاصمه مسلحانه که ممکن است رخ دهد، جلوگیری کند. در همین خصوص قاعده نودوسوم راهنما نیز مقرر داشته است که اصل تفکیک بر حملات سایبری اعمال می‌شود و همچنین در نسخه اول تالین نیز مقرراتی در این مورد تأیید شده است که از جمله آن در قاعده سی و دوم مقرر می‌دارد جمعیت غیرنظامی همانند افراد نظامی نباید هدف حمله سایبری قرار گیرند. قاعده سی و سوم نسخه اول تالین نیز فرضی را مطرح کرده است که در نتیجه آن اعلام می‌دارد که فرض بر غیرنظامی بودن افراد است.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و ارجاعات مقاله تماماً رعایت گردیده است.

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

منابع

فارسی

ـ بیگ‌زاده، ابراهیم، ۱۴۰۱، **حقوق بین‌الملل**، جلد دوم، تهران، انتشارات میزان.

ـ توحیدی، احمدرضا و سیجانی، محسن، ۱۳۹۸، ارزیابی ماهیت حقوقی حملات سایبری با نگاهی به منشور سازمان ملل متحد، **فصلنامه پدافند غیرعامل**، شماره ۴۰.

ـ خلیل‌زاده، مونا، ۱۳۹۳، **مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری**، چاپ اول، تهران، انتشارات مجد.

ـ ضیایی‌بیگدلی، محمدرضا، ۱۴۰۱، **حقوق بین‌الملل بشردوستانه**، چاپ ششم، تهران، انتشارات گنج‌دانش.

ـ برادران، نازنین و حبیبی، همایون، ۱۳۹۸، قابلیت اعمال قواعد حقوق بین‌الملل بشر دوستانه بر حملات سایبری، **فصلنامه مطالعات حقوق عمومی**، شماره ۱.

لاتین

- Schmitt, Michael. N, 2013, Tallinn Manual on the International Law Applicable to Cyber Warfare. New York, United States of America: Cambridge University Press.
- Malcom Shaw, 1977, International Law, Teach Your self Book, Hodder and Stoughton.
- Vida M. Antolin-Jenkins, 2005, Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?.
- U.S. Gen. Accounting Office, Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety

-Kelsey, Jeffrey T.G., 2009. Hacking in to International Humanitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare.

-CLARKE & KNAKE; see, e.g., 2011, More Than Firewalls: Three Challenges to American Cyber Security, asymmetric THREAT.

- Ayalew, Y.E., 2014, the impact of cyber warfare under international humanitarian law: critical legal analysis Dessie, Ethipia School of law, Wollo University.
- Martin C. Libicki, 1995, What Is Information Warfare?

Tom Gjelten, 2009, Extending the Law of War to Cyberspace.

Legal Civilization

ISSN: 2873-1841
ISSN: 2873-1922

No.20- Summer 2024