فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره سوم | پاییز ۱۴۰۱
وبگاه مجله: https://cyberlaw.maragheh.iau.ir
ISSN:2821-126X

Investigation of the Ways to Reduce Cyberattacks from the Perspective of the International Humanitarian Law

Alireza Ansari Mahyari
Assistant Professor, Department of Law, Faculty of Law, Theology and Islamic Studies, Najafabad Branch, Islamic Azad University, Najafabad, Iran
Hadi Mahmoudi*
PhD Student in International Law, Faculty of Law, Theology and Islamic Studies, Najafabad Branch, Islamic Azad University, Najafabad, Iran
mahmoodihadi55@gmail.com

DOI: 10.30495/CYBERLAW.2022.696600

Keywords:
Armed Warfare, Cyber Warfare, Cyber-attacks, Cyberspace, International Humanitarian Law

Abstract

Human progress in various political and social fields creates new opportunities and challenges. One of such challenges is cyber-attacks which are considered as a threat to human life due to the increasing development of technology and the development of virtual space in different parts of the world. The purpose of the present article is to examine the ways to reduce cyber-attacks from the perspective of the International Humanitarian Law. This article is conducted employing descriptive-analytical method. The results of the investigations led the authors to reach the conclusion that the rules and regulations of International Humanitarian law do not cover the entire framework of cyber war and cyber-attack but, due to the existential philosophy of humanitarian law, it covers civilian protection as well as other principles such as the Principles of Proportionality and Distinction and, therefore, these principles and regulations still remain applicable and, wherever there are no regulations, it is necessary to refer to the Customary International Humanitarian Law, and in particular situations, the International Humanitarian Law itself must be implemented and applied. On the other hand, due to the lack of consensus of the international community and ambiguity in implementation of some of these principles and rules, with the gradual development in the field of current contractual and customary rules, even the existing ambiguities can also be resolved.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره سوم | پاییز ۱۴۰۱

بررسی راه کارهای تقلیل حملات سایبری از منظر حقوق بین‌الملل بشردوستانه

علیرضا انصاری مهیاری
استادیار گروه حقوق، دانشکده حقوق، الهیات و معارف اسلامی، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران
هادی محمودی *
دانشجوی دکتری حقوق بین‌الملل، دانشکده حقوق، الهیات و معارف اسلامی، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران
mahmoodihadi55@gmail.com

تاریخ دریافت: ۲۲ خرداد ۱۴۰۱ تاریخ پذیرش: ۰۵ مهر ۱۴۰۱

چکیده

پیشرفت انسان در عرصه‌های مختلف سیاسی و اجتماعی فرصت‌ها و چالش‌های جدیدی را ایجاد می‌کند و یکی از این چالش‌ها، حملات سایبری است که باتوجه‌به گسترش روزافزون فناوری و توسعه فضای مجازی در نقاط مختلف جهان، تهدیدی برای زندگی انسان‌ها محسوب می‌شود. هدف از این مقاله، بررسی راه کارهای تقلیل حملات سایبری از منظر حقوق بین‌المللی بشردوستانه است. این مقاله با روش توصیفی – تحلیلی، انجام شده است و باتوجه‌به بررسی‌های انجام شده، نگارندگان به این نتیجه می‌رسند که قواعد و مقررات حقوق بین‌الملل بشردوستانه تمام چارچوب جنگ سایبری و حمله سایبری را پوشش نمی‌دهد اما به دلیل فلسفه وجودی حقوق بشردوستانه، حمایت از جمعیت غیرنظامی و اصول دیگری همچون اصل تناسب و تمایز را مدنظر دارد، لذا این اصول و مقررات همچنان کاربرد داشته و هرجا که مقرراتی وجود نداشته باشد لازم است که به حقوق بین‌الملل بشردوستانه عرفی و اصولی استناد کرده و در آن وضعیت خاص، حقوق بین‌الملل بشردوستانه را اجرا و اعمال نمود. از سوی دیگر به دلیل عدم اجماع جامعه جهانی و ابهام در نحوه ی اجرای برخی از این اصول و قواعد، با توسعه تدریجی در حوزه قواعد قراردادی و عرفیِ فعلی، ابهامات موجود نیز قابل‌حل هستند.

کلید واژگان: جنگ سایبر، جنگ مسلحانه، حملات سایبری، حقوق بین‌الملل بشردوستانه، فضای سایبر

مقدمه

هم‌زمان با ظهور بشر، جنگ نیز به وجود آمده و باگذشت تاریخ، همراه با پیشرفت بشر در عرصه‌های مختلف، شیوه‌های جنگ نیز همواره تغییر کرده است. با پیشرفت علم و فناوری، جنگ انفرادی که با چوب و چماق انجام می‌شد نیز به جنگ با ابزار آهنی مانند شمشیر تبدیل شد. در این جنگ‌ها هیچ حقی وجود نداشت و تنها اصل، شجاعت و افزایش قدرت بدنی برای پیروزی بود. این روند تا زمان کشف باروت ادامه یافت. با کشف باروت و به دنبال آن سلاح گرم، روش‌های جنگ نیز تغییر کرد و تنها در آن زمان بود که بشر به فکر اعمال حداقل استانداردها برای جنگ افتاد. بنیان‌گذاران حقوق بین‌الملل به‌تدریج با پیشرفت علم و افزایش قدرت آتش به دنبال مشروعیت بخشیدن به این نوع جنگ‌ها بودند. این تلاش‌ها در هر دوره‌ای برای سلاح‌های نوین انجام شد و قوانینی نوشته می‌شد. اما گسترش فناوری و توسعه آن در دنیای مجازی فرصت نوشتن قوانین این نوع جنگ را به متخصصان نداد و با اختراع کامپیوتر و به دنبال آن اینترنت فضای جدیدی به نام دنیای مجازی در مقابل انسان ایجاد کرد. بر همین اساس، جنگ‌ها به جنگ‌های فضای مجازی تبدیل شد، جنگی که مشخص نیست طرف مقابل چه کسی است. این جنگ تن‌به‌تن نیست، بلکه جنگ فکری از فاصله بسیار دور است. در این نوع نبرد از فناوری‌های خود ملت هدف علیه آن استفاده می‌شود و زیرساخت‌های حیاتی آن متوقف می‌شود. با پیشرفت اینترنت و فناوری‌های ارتباطی، روش‌های جنگ نیز تغییر کرده است. علاوه بر این، حملات سایبری به دلیل هزینه کم و دسترسی گسترده به رایانه و همچنین توانایی آنها برای عملیات ناشناس، روشی جذاب برای جنگ است. در سال‌های اخیر، تعداد حملات سایبری توسط بازیگران ملی و غیر ملی و همچنین حملات رایانه‌ای مخرب به طور چشمگیری افزایش‌یافته است. علاوه بر این، این حملات نه تنها در درگیری‌های سیاسی، بلکه در برنامه‌هایی باهدف آسیب رساندن به تأسیسات حیاتی نیز مورداستفاده قرار گرفته است. سؤال: این مقاله در صدد پاسخ به این سؤال است که آیا قوانین حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری قابل‌استفاده است؟

آیا قوانین حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری قابل‌استفاده است؟

فرضیه: می‌توان گفت که هیچ ماده یا قانونی در حقوق بین‌الملل بشردوستانه وجود ندارد که صراحتاً جنگ سایبری یا حمله به شبکه‌های رایانه‌ای را چه در زمان جنگ و چه در زمان جنگ و به طور مستقل ممنوع کرده باشد. این به این دلیل است که قانون جنگ به قرن نوزدهم باز می‌گردد و برای قابلیت استفاده در عصر اطلاعات به‌روز نشده است. اما با تفسیر برخی از قوانین موجود در حوزه جنگ مسلحانه می‌توان این قوانین را در حوزه جنگ سایبری نیز اعمال کرد.

مفهوم شناسی فضای سایبر

برای تعریف و شناخت جنگ سایبری باید کلمه جنگ و سپس مفهوم فضای سایبری را موردبحث قرارداد تا در نهایت به درک مناسبی از پدیده جنگ سایبری دست‌یافت.

مفهوم جنگ

اپنهایم، حقوق‌دان مشهور، جنگ را این‌گونه تعریف می‌کند: «درگیری نیروی نظامی دو دولت، باهدف برتری بر یکدیگر و اعمال شرایط دلخواه». امروزه این تعریف حداقل در آخرین بخش آن یعنی اعمال شرایط موردنظر طرف پیروز کنار گذاشته شده است. علاوه بر این، در این تعریف مشخص نیست که یک جنگ خاص چه زمانی رخ می‌دهد (مسائلی و ارفعی، ۴:۱۳۷۱)

وردوس[1] جنگ را «درگیری مسلحانه بین دولت‌ها» می‌دانند که در آن‌همه روابط مسالمت‌آمیز به حالت تعلیق درآمده است. در اینجا نیز باید توجه داشت که امروزه تنها دولت‌ها نیستند که به جنگ متوسل می‌شوند. کوینسی رایت می‌نویسد: "جنگ یک

[1] Verdos

شرط قانونی است که به دو یا چند گروه متخاصم فرصت سازماندهی درگیری با نیروهای مسلح، احساسات عمومی، تعصبات قانونی و فرهنگ‌های ملی را می‌دهد" (دانشگاه امام حسین، ۲:۱۳۷۵).

همچنین به نظر او «جنگ زمانی آغاز می‌شود که دولت قصد خود را برای متوسل شدن به آن از طریق اعلان‌جنگ یا ضرب‌الاجل اعلام کند». وی علاوه بر اعتقاد به جنگ در ابعاد مختلف، دو شرط اساسی را برای وجود دولت و اعلام جنگ می‌داند. همچنین وجود قصد و نیت را می‌توان در گزارش «وضعیت حقوقی ناشی از اعمال فشارهای اقتصادی در ایام صلح» نیز مشاهده کرد. دبیرکل سازمان ملل متحد در این گزارش تصریح می‌کند که وجود وضعیت جنگی بین دو دولت از نظر قانونی به نیت آنها بستگی دارد نه به ماهیت اقدام آنها. در نتیجه، اتخاذ این معیارها، هرچند با خشم و نفرت همراه باشد، ازنظر قانونی رابطه جنگی بین دولت‌های مربوطه ایجاد نمی‌کند، مگر اینکه با قصد جنگ همراه باشد و از سوی کشورهایی که معیارها برای آنها اتخاذ شده جنگ تلقی نشود (مسائلی و ارفعی، ۱۳۷۱ : ۵).

کلازوویتس می‌گوید: «جنگ یک عمل خشونت‌آمیز است که به معنای وادار کردن شخص به پذیرش و اجرای نظرات و اراده ماست. جنگ ادامه سیاست است. جنگ فقط نظامی نیست، بلکه دیپلماتیک، روانی و اقتصادی نیز هست». وی همچنین معتقد است که جنگ ادامه سیاست است و باید از همه ابزارها برای رسیدن به اهداف سیاسی استفاده کرد. فون بوگوسلافسکی[۲] جنگ را مبارزه گروه خاصی از مردم، قبایل، ملت‌ها، مردمان یا دولت‌ها علیه گروه همگن دیگری می‌داند. به گفته گاستول بوتول[۳]، «جنگ یک مبارزه مسلحانه و خونین بین گروه‌های سازمان‌یافته است». او استفاده از سلاح در درگیری، خونریزی آن و سازماندهی گروه‌های متخاصم را عامل جنگ می‌داند (دانشگاه امام حسین، ۲:۱۳۷۵). ماده دوم قطعنامه ۳۳۱۴ مجمع‌عمومی سازمان ملل متحد که در اصلاح اساسنامه دیوان کیفری به‌عنوان اساس و پایه تعریف تجاوز بود، «زمانی که یک دولت علیه قلمرو دولت دیگر از هر نوع سلاح استفاده نماید» نمونه‌ای از اقدام تجاوزکارانه تلقی می‌شود (موسی زاده و امینیان، ۱۳۹۰ : ۵۶).

تعریف ابعاد جنگ، امروزه بسیار مشکل‌تر از گذشته است؛ زیرا جنگ‌ها لزوماً بین دولت‌ها نیستند. ویژگی‌های سنتی جنگ که مستلزم وجود حداقل دو دولت بود، جای خود را به جنگ‌هایی داده که عناصر غیردولتی نیز در آن دخالت دارند. برای اطلاق جنگ به عملی که صورت‌گرفته است، حتماً باید در روابط بین‌دولتی نوعی برخورد مسلحانه صورت گیرد تا عملی جنگی فرض شود. بااین‌حال، امروزه بازیگران غیردولتی هستند که توانایی آنها برای تأثیرگذاری در عرصه بین‌المللی به‌مراتب بهتر از برخی کشورها است و جبران خسارت آنها بسیار دشوارتر از آسیب‌های موشکی و بمب است.

انقلاب اطلاعاتی، با گسترش قدرت در میان بازیگران دولتی ضعیف‌تر و بازیگران غیردولتی، بازتعریف افرادی را که پتانسیل تهدید دارند، درعین‌حال تغییر انتظارات از تعارض بین جوامع را تغییر داده است (عبدالله خانی، ۱۳۸۶ : ۲۷).

مفهوم سایبر و فضای سایبری

کلمه سایبر به‌عنوان پیشوند از کلمه یونانی به معنای سکان‌دار یا راهنما[۴] گرفته شده است (Melzer . 2011:4). اصطلاح سایبرنتیک اولین‌بار توسط ریاضی‌دان نوربرت وینر[۵] در کتابی در سال ۱۹۴۸ در مورد سایبرنتیک و کنترل حیوانات استفاده شد. بااین‌حال، حملات سایبری ترکیبی از دو مفهوم مجزا هستند که با هم یک مفهوم واحد را ایجاد می‌کنند. حملات به یک رویکرد تهاجمی در نبرد اشاره دارد که می‌تواند شامل طیف وسیعی از حملات آشکار و نامحسوس باشد. سایبرنتیک از لحاظ مفهومی، به

[2] Fonbogoslafsky
[3] Gastalbotag
[4] Kybernetes
[5] Norbert Wiener

مطالعه و کنترل مکانیسم‌های سیستم انسانی و رایانه‌ای گفته می‌شود. دومین مفهومی که در اصطلاح فضای مجازی به کار می‌رود، مفهوم «فضا» است. وجود کلمه فضا در این کلمه بیانگر این است که فضای مجازی باید بعد داشته باشد .

واژه «فضای سایبری»[6] یا فضای مجازی را نخستین‌بار ویلیام گیبسون[7] نویسنده داستان علمی تخیلی در کتاب نورومنسر[8] در سال ۱۹۸۴ به کار برد. این رمان جمعیت کثیری از دانشمندان علم کامپیوتر فعال در زمینه طراحی و ساخت وب سایت ها که سازندگان بعدی دنیای آنلاین بودند را تحت تأثیر قرار داد. نظر گیبسون در مورد فضای دیجیتالی ارتباط و کنترل به بحث هایی در خصوص امنیت سایبر انجامید (Reverson. 2012:15). فضای مجازی در واقع با اختراع اینترنت ایجاد شد. تا سال ۱۹۵۰، رایانه‌ها، رادیوها و تلویزیون‌ها اختراع شده بودند اما در دست تعداد کمی بودند و هیچ یک از آنها نمی‌توانستند وصل شوند یا حتی از راه دور به هم متصل شوند. رایانه‌ها در دهه ۱۹۶۰ به هم متصل شدند. این اولین‌بار در سازمان‌ها به‌عنوان شبکه‌های محلی انجام شد. تا سال ۱۹۶۹، اولین شبکه بزرگ در داخل ایالات متحده فعالیت می‌کرد. فضای مجازی «مجموعه‌ای از ارتباطات داخلی انسان از طریق رایانه و دستگاه‌های مخابراتی بدون توجه به جغرافیای فیزیکی» است. به عبارتی دیگر، فضای مجازی، «محیط الکترونیکی، واقعی است که در آن ارتباطات انسانی، فراتر از مرزهای جغرافیایی و با ابزارهای خاص خود به‌سرعت و واقع‌بینانه انجام می‌شود». محیطی که در حقیقت ارتباطات در آن شکل می‌گیرد فضای مجازی است. اگرچه ممکن است این ارتباطات، در همه شرایط آنلاین نباشند، اما واقعی و مستقیم هستند. ازاین‌جهت، تأثیر زیادی در این روابط رخ می‌دهد (Ottis and Lorents . 2010:1-2).

وزارت دفاع، فضای سایبری را به‌عنوان «حوزه جهانی یک محیط اطلاعاتی که متشکل از شبکه‌ای به‌هم‌پیوسته‌ای از زیرساخت‌های فناوری اطلاعات، است» تعریف می‌کند. این تعریف تنها عامل سخت‌افزاری را در نظر می‌گیرد و نقش انسان را نادیده می‌گیرد. مرکز عالی همکاری دفاع سایبری ناتو، مستقر در استونی، نیز فضای سایبری را این‌گونه تعریف می‌کند: "فضای سایبری طبقه‌ای از سیستم‌های اطلاعاتی وابسته به زمان و درهم‌تنیده با انسان است که با این سیستم‌ها تعامل دارند." این تعریف نقش عامل انسانی را نیز در نظر می‌گیرد و سیستم‌های اطلاعاتی درهم‌تنیده شامل سخت‌افزار، نرم‌افزار و ابزارهایی است که آنها را به هم متصل می‌کند (Ottis and Lorents . 2010: 2).

فضای سایبر در اصل فضایی شبیه به سایر عرصه‌های رقابتی مانند دریا، زمین و هوا است، اما با این تفاوت که این محیط بر خلاف سایر محیط‌ها ساخته دست بشر و ناملموس است (Libicki . 2009: 11).

اصطلاح سایبر به فناوری رایانه و الکترونیک اشاره دارد. فضای مجازی همچنین یک حوزه عملیاتی است که با استفاده از علم الکترونیک برای بهره‌برداری از اطلاعات از طریق سیستم‌های به‌هم‌پیوسته و زیرساخت‌های مرتبط تنظیم می‌شود؛ بنابراین، فضای مجازی یک رژیم به‌هم‌پیوسته منحصربه‌فرد از دارایی‌ها، سخت‌افزار و نرم‌افزار فیزیکی و مجازی است که تمامی شبکه‌های رایانه‌ای در جهان از جمله اینترنت و همچنین سایر شبکه‌هایی که به اینترنت متصل نیستند را در بر می‌گیرد (Maurer. 2011: 8).

هرچند دستورالعمل تالین فاقد تعریفی جامع است اما، اقدامات سایبری را در صورتی مخرب می‌داند که کشوری به زیر ساخت‌های سایبری کشور دیگر آسیب برساند. همچنین در جای دیگر این دستورالعمل ذکر شده که زیرساخت سایبری عبارت است از منابع ارتباطات، ذخیره‌سازی و محاسباتی که براساس آن سامانه‌های اطلاعاتی عمل می‌کنند. ظاهرا این آسیب باید فیزیکی باشد چون اقداماتی از قبیل نظارت، خارج از تعریف گروه کارشناسی تنظیم کنندگان می‌نماید(Schmitt. 2013:24-25).

[6] Cyber Space
[7] William Gibson
[8] Neuromancer

مفهوم جنگ سایبر

جنگ سایبری توسعه سیاست‌ها در فضای مجازی توسط عوامل دولتی و غیر دولتی است که به منزله و یا در پاسخ به تهدید جدی علیه امنیت ملی انجام می‌گیرد(Shakarian et al. 2013:2). در سند راهبردی پدافند سایبری کشور ایران، جنگ سایبری، به نوعی از نبرد اطلاق می‌شود که طرفین جنگ در آن از رایانه و شبکه‌های رایانه‌ای (به خصوص شبکه اینترنت) به عنوان ابزار تهاجم استفاده کرده و نبرد را در فضای سایبری به راه می‌اندازند. برای درک موضوع جنگ سایبری[9] به‌عنوان یک پدیده جدید در عرصه روابط بین بازیگران (دولتی و غیردولتی)، تعاریف متعددی ارائه شده است. جنگ سایبری در ساده‌ترین تعریف خود به‌عنوان «استفاده از رایانه و اینترنت برای نبرد در فضای سایبری» تعریف می‌شود (عبدالله خانی، ۱۳۸۶: ۱۳۶-۱۳۵). اما با جزئیات بیشتر، اصطلاح جنگ سایبری به جنگی اطلاق می‌شود که در فضای مجازی از طریق ابزارها و روش‌های سایبری انجام می‌شود. درحالی‌که اصطلاح جنگ به‌طورکلی به خصومت نظامی در موقعیت‌های درگیری مسلحانه اشاره دارد، فضای سایبری را می‌توان به‌عنوان شبکه جهانی درهم‌تنیده ارتباطات دیجیتال و زیرساخت‌های اطلاعاتی، از جمله اینترنت، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای و اطلاعات توصیف کرد؛ بنابراین، آلودگی شبکه رایانه‌ای دشمن در حال مبارزه با ویروس را می‌توان یک جنگ سایبری در نظر گرفت، درحالی‌که بمباران سایبری هوایی یک فرماندهی سایبری نظامی نمی‌تواند (Melzer . 2011:4).

کلارک و کنارک[10] جنگ سایبری را به‌عنوان "تداخل غیرمجاز در حمایت از یک دولت، با سایر شبکه‌ها یا هر فعالیتی که بر سیستم‌های رایانه‌ای باهدف جمع‌آوری، تغییر یا دست‌کاری اطلاعات، یا ایجاد اختلال یا آسیب تأثیر می‌گذارد، توصیف می‌کند." " ضربه‌زدن به کامپیوتر یک طرح شبکه یا هدف کنترل یک سیستم کامپیوتری است" (Maurer. 2011: 15).

مرکز عملیات سایبری آمریکا و کتاب راهنمای تروریسم سایبری، حملات سایبری را چنین تعریف می‌کنند: «استفاده عمدی از فعالیت‌های مخرب یا تهدید علیه آنها، علیه رایانه‌ها و شبکه‌ها به‌منظور آسیب رساندن و بیان بیشتر از نظر اجتماعی، ایدئولوژیکی، مذهبی، «سیاسی». یا اهداف مشابه یا وادار کردن هر شخصی به دنبال چنین اهدافی ...» چنین آسیب‌هایی می‌تواند علاوه بر امکانات فیزیکی و افراد به شبکه رایانه‌ای آسیب برساند. حملات سایبری با جرایم سایبری که توسط قوانین کیفری ملی تنظیم می‌شود متفاوت است و شامل اعمالی مانند سرقت هویت و کلاهبرداری سایبری می‌شود. حملات سایبری، بر خلاف جرایم سایبری، "شامل تهاجم علیه یک دشمن یا حریف است که ممکن است یک فرد، سازمان یا دولت رقیب باشد، به‌عنوان تلاشی مستمر برای به‌دست‌آوردن هژمونی در حوزه‌های سیاسی و تجاری". در واقع از منظر دولت محوری، جنگ سایبری باهدف برچیدن سامانه‌های اطلاعاتی و مخابراتی، سامانه‌های کنترل و فرماندهی، ارتباطات و جاسوسی نیروهای نظامی دشمن و عدم عملیات آنها در میدان نبرد انجام می‌شود. به‌عبارت‌دیگر، به عملیات نظامی بر اساس اصول اطلاعاتی و شبکه‌های الکترونیکی اطلاق می‌شود (Arquilla and Rohfeldt . 1993:27).

به‌طورکلی، اصطلاحات «جنگ سایبری»، «درگیری سایبری» و «خصومت‌های سایبری»، از نظر حقوق بین‌الملل به طور کامل تعریف نشده‌اند. این اصطلاحات توسط سازمان همکاری شانگهای تعریف شده است که ضمن ابراز نگرانی نسبت به «جنگ اطلاعاتی»، جنگ سایبری را به معنای «مقابله دولت‌ها در حوزه اطلاعاتی باهدف آسیب رساندن به سیستم‌ها، فرایندها و منابع اطلاعاتی» می‌داند. ساختارهای حیاتی و مهم، تضعیف نظام‌های سیاسی، اقتصادی و اجتماعی، عملیات روانی گسترده برای بی‌ثباتی جامعه و دولت و نیز اجبار دولت به تصمیم‌گیری در راستای منافع مخالفان. بنابراین عبارات «جنگ سایبری»، «درگیری

[9] Cyber Warfare
[10] Clarke and Knake

سایبری» و «خصومت سایبری» باید در چارچوب حقوق بین‌الملل بشردوستانه به درگیری‌های مسلحانه و در واقع تهدیدات امنیتی ناشی از فضای سایبری و نرسیدن به مرز محدود شود. حمله مسلحانه به آن «جنایت سایبری»، «عملیات سایبری»، «انضباط سایبری»، «تروریسم سایبری» و «سرقت سایبری» می‌گویند (Melzer . 2011:22).

دستورالعمل تالین ۲ ناتو در مورد جنگ سایبری

در سال ۲۰۰۹، سازمان بین‌المللی نظامی واقع در تالین استونی با نام مرکز عالی همکاری دفاع سایبری که در سال ۲۰۰۸ از طرف ناتو به عنوان قطب علمی شناخته شده بود، از گروه بین المللی کارشناسان مستقل جهت نگارش دستورالعملی در مورد قانون حاکم بر جنگ سایبری دعوت به عمل آورد. این پروژه که توسط متخصصین و محققان حقوق بین الملل طرح ریزی شد به دنبال تسری هنجارهای حقوقی و قانونی در اینگونه جنگ های نوین است. دستورالعمل حقوق بین الملل در مورد جنگ سایبری یا دستورالعمل تالین، که از روندی کارشناس محور نشأت گرفته در پی سندی غیر الزام‌آور جهت بسط قانون موجود به جنگ سایبری و همچنین تلاش جهت شفاف سازی بیشتر اسناد منتشره پیرامون اقدامات سایبری از سوی دولت ها و با توجه خاص به قوانین حقوق بر جنگ و حقوق در جنگ است. بنابراین دستورالعمل تالین به بررسی حقوق حاکم بر جنگ سایبری پرداخته و به طور کلی در برگیرنده حقوق برجنگ، حقوق بین الملل حاکم بر توسل به زور از سوی کشورها به عنوان ابزار سیاست ملی و حقوق در جنگ، حقوق بین الملل تنظیم کننده رفتار درگیری های مسلحانه است.عناصر مرتبط حقوق بین الملل، مانند مسئولیت دولت ها و حقوق دریاها نیز در این دستورالعمل گنجانده شده است. به طور خلاصه، این دستورالعمل، برخلاف آنچه در کاربرد رایج از آن استنباط می شود، در مورد امنیت سایبری نگارش شده است. جاسوسی سایبری، سرقت مالکیت معنوی و طیف گسترده ای از اقدامات کیفری در فضای مجازی تهدیداتی جدی و واقعی علیه کشورها، سازمان ها و افراد خصوصی تلقی می شوند. واکنش کافی به چنین اقداماتی، مناسبات ملی و بین المللی را طلب می کند که دستورالعمل تالین به دلیل عدم ایفای نقش لازم توسط حقوق بین المللی در خصوص توسل به زور و مخاصمات مسلحانه، این مناسبات را مدنظر قرار نمی دهد. حقوق بین الملل فاقد کارایی لازم جهت مقابله باتهدیدات حادث در حوزه سایبری است. تأکید دستورالعمل تالین، در معنای دقیق، بر اقدامات سایبری علیه تجهیزات سایبری، به عنوان مثال به کارگیری اقدامات سایبری علیه زیرساخت های حیاتی یک دولت یا حمله سایبری با هدف سامانه هاای کنترلی و فرماندهی دشمن، است. بنابراین هدف این دستورالعمل حول محور اقدامات سایبری علیه تجهیزات مادی، همچون حمله هوایی و بمباران مرکز کنترل سایبری، نمی چرخد. همچنین حملات نظامی الکترونیک سنتی، مانند انداختن پارازیت، را نیز در بر نمی‌گیرد. چنین اقداماتی قبلا تحت حقوق مخاصمات مسلحانه تعریف شده اند (Schmitt. 2013:16-19).

۱-۱- انواع حملات سایبری

در یک سطح عمیق‌تر، جنگ سایبری در واقع یک جنگ دانش است، جنگی مبتنی بر رایانه و اطلاعات (Arquilla and Rohfeldt . 1993:27). مارتین لیبسکی از دانشکده دفاع ملی آمریکا در سال ۱۹۹۵ جنگ اطلاعاتی را به هفت دسته تقسیم کرد: فرماندهی و کنترل[11]، جنگ جاسوس محور[12]، جنگ الکترونیک، جنگ روانی، جنگ هکری[13]، جنگ اطلاعات اقتصادی و جنگ سایبری (Hughes. 2010:5).

[11] Command-and-Control
[12] Intelligence-Based Warfare
[13] Hacker Warfare

جنگ سایبری جدیدترین شکل جنگ اطلاعاتی است و می‌تواند شامل موارد زیر باشد:

۱- خرابکاری اینترنتی[14]: حملاتی برای تغییر محتوا و شکل صفحات وب یا ایجاد اختلال در خدماتی که آسیب چندانی ایجاد نمی‌کند.

۲- اخلال در سرویس‌دهی[15]: تعداد زیادی رایانه در یک کشور تلاش می‌کنند تا سرویس سیستم کشورهای دیگر را مختل کنند.

۳- اخلال در تجهیزات[16]: استفاده‌های نظامی از رایانه‌ها در محیط کار؛ زیرا دستورات و ارتباطات توسط افراد مهاجم قابل ردیابی یا تغییر هستند.

حمله به زیرساخت‌های حیاتی: نیروگاه‌ها، تأسیسات تأمین آب و سوخت‌گیری، ارتباطات و حمل‌ونقل در برابر این نوع حمله بسیار آسیب‌پذیر هستند (عبدالله خانی، ۱۳۸۶: ۱۳۶).

عملیات سایبری به سه دسته «حمله شبکه رایانه‌ای»، «استثمار شبکه رایانه‌ای» و «دفاع شبکه رایانه‌ای» تقسیم می‌شوند. درحالی‌که تمام عملیات سایبری باهدف ایجاد اختلال، جلوگیری، تخریب یا ازبین‌بردن اطلاعات موجود در رایانه‌ها و شبکه‌های رایانه‌ای انجام می‌شود، بهره‌برداری از شبکه‌های رایانه‌ای به «ناتوانی در جمع‌آوری اطلاعات برای به‌دست‌آوردن داده‌ها از شبکه هدف دشمن یا سیستم‌های اطلاعات خودکار» اشاره دارد. در عوض، دفاع شبکه کامپیوتری به «فعالیت‌هایی برای پشتیبانی، کنترل، تجزیه‌وتحلیل، شناسایی و پاسخ به فعالیت‌های غیرمجاز در سیستم‌های اطلاعاتی و شبکه‌های رایانه‌ای» اشاره دارد (عباسی و مرادی، ۱۳۹۴: ۳۷-۶۸). به طور خلاصه، جلوگیری از حملات شبکه‌های رایانه‌ای و بهره‌برداری از شبکه رایانه‌ای از طریق جاسوسی، ضدجاسوسی، تقویت قانون و توانایی‌های نظامی است. این عبارات که مختص عملیات سایبری است باید با اصطلاحات فنی حقوق بین‌الملل مانند «زور»، «حمله مسلحانه» و «حمله» به‌دقت شناسایی شوند. استثمار شبکه رایانه یک حمله نیست و باید از حملات سایبری متمایز شود. این اقدام دارای برخی ویژگی‌های متمایز است که آن را از حملات سایبری متمایز می‌کند. ۱. بهره‌برداری از شبکه رایانه‌ای کاربر را از استفاده کامل از سیستم یا دستگاه محروم نمی‌کند، بلکه تنها ضرر کاربر این است که اسرار خصوصی و محرمانه وی به سرقت رفته است. ۲. ازآنجایی‌که تشخیص بهره‌برداری از شبکه‌های رایانه‌ای تقریباً غیرممکن است، سیاست بازدارندگی تنها در موارد استثنایی می‌تواند کارساز باشد (Libicki . 2009: 23).

۲- قدرت در فضای سایبر

فضای سایبر، مانند هر فضای دیگری، زمینه‌ای برای تضاد است که منجر به اجتناب‌ناپذیری درگیری می‌شود؛ بنابراین، در این منطقه از درگیری، مانند هر میدان نبرد دیگری، برخورداری از توان و توانمندی‌های لازم مربوط به آن نبرد می‌تواند در کسب موفقیت در تأمین امنیت شهروندان و قلمرو داخلی مؤثر باشد. همان‌طور که جوزف نای اشاره می‌کند، قدرت معنا پیدا می‌کند و رشد سریع فضای مجازی، زمینه جدید و مهمی در سیاست جهانی است. هزینه‌های پایین ورود و عدم تقارن در آسیب‌پذیری‌ها به این معنی است که بازیگران کوچک‌تر در فضای سایبری ظرفیت بیشتری برای اعمال قدرت سخت و نرم نسبت به مناطق سنتی‌تر سیاست جهانی دارند (Nye . 2010:1)؛ بنابراین از این نظر جنگ در فضای مجازی جزء همیشگی سیاست خواهد بود. کسب قدرت در فضای مجازی به دلیل انقلاب اطلاعاتی کنونی موسوم به «انقلاب صنعتی سوم» است که نوع تضاد بین بازیگران را نیز متحول کرده

[14] Web Vandalism
[15] Denial-of-ServiceAttacks
[16] Equipment Disruption

است. قدرت سایبری از دیدگاه رفتاری به معنای «توانایی دستیابی به نتایج مطلوب با استفاده از منابع اطلاعات الکترونیکی در حوزه سایبری» است. این تعریف جامع به نظر نمی‌رسد.

تعریف دیگری که شاید جامع‌تر باشد «توانایی استفاده از فضای مجازی برای ایجاد مزایا و تأثیرگذاری بر رویدادها در سایر محیط‌های عملیاتی و بیان و استفاده از ابزارهای قدرت» است. می‌توان از قدرت سایبری برای دستیابی به نتایج مطلوب در فضای مجازی استفاده کرد و یا از ابزارهای سایبری برای دستیابی به نتایج مطلوب در سایر حوزه‌های خارج از فضای مجازی استفاده کرد. در همین راستا، باراک اوباما در سال ۲۰۰۹ باتوجه‌به اهمیت موضوع، خواستار تمرکز بر قدرت سایبری شد (Nye 2010:2-5 .) و دستور تشکیل فرماندهی سایبری آمریکا که جزئی از آژانس امنیت ملی آمریکا[17] است را صادر کرد. ین دستور در ۲۳ ژوئن ۲۰۰۹ به فرماندهی استراتژیک آمریکا ابلاغ شد و در سپتامبر همان سال راه‌اندازی شد و در ۱۲ ژوئن ۲۰۱۱ مجوز جنگ سایبری و خرابکاری رایانه‌ای در کشورهای دیگر را صادر کرد (www.khabaronline.ir).

۲-۱- امنیت و تبعات امنیتی حملات سایبری

امنیت سایبری توسط اتحادیه جهانی مخابرات به‌عنوان مجموعه‌ای از ابزارها، سیاست‌ها، مفاهیم امنیتی[18]، خط‌مشی‌های حفاظتی، دیدگاه‌های مدیریت بحران فعالیت‌ها آموزش، بهترین رویه‌ها، اطمینان یا اعتماد و فناوری‌هایی است که می‌تواند برای حمایت محیط سایبر و دارایی‌های کاربر و سازمان استفاده شود. به گفته جوزف نای، امنیت سایبری را می‌توان به چهار تهدید اصلی تقسیم کرد: جاسوسی، بزهکاری، جنگ سایبری و تروریسم سایبری.

احتمال تهدید در مرحله اول به سه منبع برمی‌گردد: ۱.نقص در طراحی اینترنت ۲. نقص در سخت‌افزار و نرم‌افزار ۳. حرکت به سمت بارگذاری سیستم‌های آنلاین بحرانی و حساس‌تر (Maurer. 2011: 8-9).

حملات سایبری که در کمتر از یک دهه رخ‌داده است نشان می‌دهد که چگونه دولت‌ها از فناوری‌های مدرن استفاده می‌کنند و به‌شدت درگیر جنگ اطلاعاتی برای تضعیف زیرساخت‌های حیاتی رقبا هستند. یک نگرانی جدی بین‌المللی وجود دارد که درگیری‌های خارجی دولت‌ها می‌تواند حملات پیشگیرانه مبتنی بر رایانه به سیستم‌های ملی یا منطقه‌ای، مانند زیرساخت‌های توزیع انرژی، مخابرات و خدمات مالی را سرعت بخشد. حملات سایبری معروف اخیر شامل حمله به وب‌سایت‌های دولتی و تجاری لیتوانی در ژوئن ۲۰۰۸، حملات به وب‌سایت‌های دولتی استونی در ۲۰۰۷، شکستن ایمیل در پنتاگون در ۲۰۰۷ و هک کردن وب‌سایت‌های شرکت تلفن پاکستان در ژانویه ۲۰۰۳ است. در آگوست ۲۰۰۸، حملات به وب‌سایت‌های رسمی گرجستان به طور موقت آنها را غیرفعال کرد، از جمله دفتر رئیس‌جمهور، وزارت امور خارجه و وزارت دفاع که منجر به مشکلات ارتباطی در سراسر کشور شد. حتی اخیراً، اخیراً کشف شده است که هکرهای چینی بارها شبکه‌های رایانه‌ای کاخ سفید را هک کرده‌اند و ایمیل‌های ارتباطی ردوبدل شده بین مقامات دولتی را به دست آورده‌اند. گاهی اوقات حتی آسیب ناشی از بسیاری از این حملات منجر به صدمات شخصی، مرگ و تلفات می‌شود. شاید در افراطی‌ترین مثال، حملات سال ۲۰۰۷ به وب‌سایت‌های استونیایی، اکثر مردم را سردرگم کرد. در زمان حملات، استونی اساساً یک ایمیل دولتی ارسال می‌کرد که بسیاری از جنبه‌های دولت را آفلاین می‌کرد. علاوه بر غیرفعال‌کردن بسیاری از وب‌سایت‌های تجاری و دولتی عمده استونی، حملات سایبری باعث شده است که شماره‌تلفن‌های اضطراری بیش از یک ساعت در دسترس نباشد. در نتیجه شورش‌ها و ناآرامی‌های گسترده ۱۵۰ نفر مجروح و یک تبعه روسیه کشته شد. در مقایسه، حملات لیتوانیایی چهره وب‌سایت‌های دولتی و تجاری با نمادهای

[17] National Security Agency(NSA)
[18] Security Concepts

کمونیستی و بی‌معنی را مخدوش کرد. اما دولت توانست دفاع لازم را برای این حملات فراهم کند. این دو مثال نشان دادند که حملات سایبری می‌توانند غیرقابل‌پیش‌بینی باشند (Swanson . 2010:308-310).

نوع منحصربه‌فرد حمله سایبری که توجه جهان را به خود جلب کرد حمله اینترنتی به تأسیسات هسته‌ای ایران در نطنز بود. در سال ۲۰۱۰ ویروسی کشف شد که بسیاری از سیستم‌های رایانه‌ای در جهان را مختل کرد. پس از خرابکاری بسیاری که در رایانه‌های در سراسر جهان به وجود آمد مشخص شد که ویروس معروف به «استاکس نت» برای نفوذ و ازکارانداختن مخصوص تأسیسات هسته‌ای ایران ساخته شده است. در نهایت مشخص شد که این ویروس به‌عنوان سلاحی برای مختل کردن یا غیرفعال‌کردن سانتریفیوژها در چرخه غنی‌سازی اورانیوم طراحی شده است. این ویروس ابتدا در بلاروس کشف شد و در نهایت سیستم‌های کامپیوتری ایران، اندونزی، هند، ایالات متحده، استرالیا، بریتانیا، مالزی و پاکستان را تحت‌تأثیر قرار داد (Richardson . 2011:10-11).

۲-۲- بازدارندگی سایبری

ژنرال کارت وی[19] از ارتش آمریکا، بازدارندگی سایبری را این‌گونه تعریف می‌کند: «ما باید در فضای سایبری قابلیت‌هایی را توسعه دهیم تا در مقابل آنچه دیگران می‌خواهند علیه ما انجام دهند، اقدام کنیم». این مستلزم نوعی تلافی و اقدام متقابل علیه دولت متجاوز است. هدف از بازدارندگی کاهش انگیزه برای شروع یا انجام اعمال خصمانه بیشتر است و در واقع این نوعی مجازات علیه متجاوز است (Libicki . 2009: 27-28).

توازن هسته‌ای میان آمریکا و شوروی در طول جنگ سرد، مبنای تاریخی این ایده را فراهم کرد که باید بازدارندگی هسته‌ای وجود داشته باشد. البته بازدارندگی سایبری با بازدارندگی هسته‌ای یا به‌طورکلی بازدارندگی نظامی متفاوت است. در بازدارندگی هسته‌ای یا نظامی، هدف مشخص و در خطر است و تا زمانی که سلاح در دسترس باشد، ادامه خواهد داشت. در مناقشه هسته‌ای نیز، دخالت شخص ثالث یا غیردولتی تقریباً غیرممکن است. در بازدارندگی سایبری، اشتباه با ضربه‌زدن به شخص ثالث نمی‌تواند منطق بازدارندگی را توجیه کند، بلکه فقط جبهه درگیری را به‌جای یک نفر به دو نفر تبدیل می‌کند. بنابراین مدارک مورداستفاده باید کاملاً قانع‌کننده و معتبر باشد. بر اساس اطلاعات موثق، بیش از صد کشور درحال‌توسعه توانایی‌های حمله سایبری هستند. هر کشوری می‌تواند مورد حمله قرار گیرد، زیرا مانند جنگ هسته‌ای، هدف در اینجا به‌صراحت بیان نشده است و هدف برای دیگران مشخص نیست در اینجا فقط به مهاجم اطلاع داده می‌شود که حمله انجام شده است حتی اگر حمله موفقیت‌آمیز نباشد. حملات تلافی‌جویانه فقط برای بازدارندگی مفید است. بر خلاف حملات تلافی‌جویانه یا هسته‌ای سنتی، آنها قادر به خلع سلاح نیستند. پیش‌نیازهای حمله سایبری بسیار اندک است و شامل موارد زیر است: یک هکر توانا، اطلاعات هدف، برآورد آسیب‌پذیری بالقوه، رایانه‌های شخصی و هر نوع اتصال شبکه (Libicki . 2009: 39-59).

۳- جنگ سایبری و سازمان ملل متحد

مهم‌ترین منبع حقوقی حاکم بر روابط بین‌الملل امروزه منشور سازمان ملل متحد است. سازمان ملل متحد به‌عنوان مرکز تصمیم‌گیری جهانی در مورد موضوعات مهم و تأثیرگذار روابط بین‌الملل، برای اولین‌بار در سال ۱۹۹۸ توجه خود را به امنیت سایبری معطوف کرد. در این سال روسیه پیش‌نویس قطعنامه‌ای در زمینه مخابرات و فناوری اطلاعات به سازمان ملل ارائه کرد که با مخالفت آمریکا مواجه شد. تا اینکه در سال ۲۰۱۰ پدیده‌های استاکس نت و ویکی‌لیکس خبرساز شد و رویدادهای مهمی در یک اتاق جلسه کوچک در سازمان ملل رخ داد. ایالات متحده موضع سیاسی دیرینه خود را تغییر داد و برای اولین‌بار به طور

[19] Cartwright

مشترک پیش‌نویس قطعنامه‌ای را در زمینه ارتباطات و فناوری اطلاعات در حوزه امنیت بین‌المللی تهیه کرد که امروزه به‌اختصار امنیت سایبری نامیده می‌شود (Henderson, 2021: 582-614).

در اوایل سال ۲۰۱۰، گروه از کارشناسان دولتی [20] در سازمان ملل متحد، از جمله دیپلمات‌هایی از ایالات متحده، روسیه و چین، به به طور مشترک در گزارشی که در ژوئیه همان سال منتشر شد، به طور مشترک اعلام کردند: «تهدیدات بالقوه و موجود در حوزه امنیت اطلاعات از جمله مهم‌ترین چالش‌های قرن بیست و یکم هستند». البته قبل از سال ۱۹۹۸ قطعنامه‌هایی دررابطه‌با جرایم سایبری همانند قطعنامه شماره ۵۵/۳۳ که در هشتمین نشست مجمع درباره جلوگیری از جرایم و تهدید مهاجمان در سال ۱۹۹۰ تصویب شد، صادر شده بود. اما آنچه آن را در سال ۱۹۹۸ در صدر قرارداد توجه قدرت‌های بزرگ به آن و همچنین افزایش میزان دسترسی جهانی به پدیده اینترنت بود. در آخرین اقدام در این زمینه نیز کشورهای روسیه و چین (همراه با ازبکستان و تاجیکستان) کردارنامه بین‌المللی نظارت بر امنیت بین‌المللی را در ۱۴ سپتامبر ۲۰۱۱ پیشنهاد کردند تا در مجمع‌عمومی سازمان ملل متحد بررسی شود. علاوه بر این، روسیه ایده برگزاری نشستی در مورد امنیت اطلاعات بین‌المللی را تنها یک هفته بعد اعلام کرد. در سازمان ملل متحد دو جریان اصلی را در ارتباط با امنیت در فضای سایبری می‌توان از یکدیگر جدا کرد: جریان نظامی – سیاسی که بر جنگ سایبری متمرکز است و جریان اقتصادی که بر بزهکاری سایبری متمرکز است. هر دوی این روند نشان می‌دهد که استانداردها در فضای مجازی در حال ظهور هستند. در زمینه سیاسی – نظامی سه دوره مهم تاریخی است: از سال ۱۹۹۸ تا سال ۲۰۰۴ به‌عنوان اولین قدم در تثبیت هنجارهای فضای مجازی بود. ارائه پیش‌نویس قطعنامه‌ای در مورد امنیت سایبری توسط روسیه، در این دوره بود که بدون رأی مخالف در مجمع‌عمومی تصویب شد. درنهایت با مخالفت کشورهای اروپایی و ایالات متحده مواجه شدند و استدلال آنها هم این بود که این قطعنامه با آزادی اطلاعات مغایر است. از سال ۲۰۰۵ تا سال ۲۰۰۸ را دوره دوم گویند و این دوره را دوره بازگشت به عقب نیز می‌نامند. [21] در سال ۲۰۰۵ این پیش‌نویس در مجمع‌عمومی، رأی‌گیری شد که با مخالفت آمریکا قطعنامه مورد تأیید قرار نگرفت. این تصمیم مانع از شکل‌گیری اجماع جهانی در حوزه فضای سایبر شد. از سال ۲۰۰۹ تا ۲۰۱۲ دوره سوم است که این دوره را حرکت دوباره به سمت جلو [22] گویند. باراک اوباما با شروع دوره ریاست‌جمهوری، تلاش کرد خط‌مشی‌های دوره ریاست‌جمهوری بوش دررابطه‌با روسیه و سازمان ملل متحد را بازبینی نماید. این موضوع باعث حمایت آمریکا از روسیه در تصویب قطعنامه‌ای در مورد امنیت سایبری شد (Maurer. 2011: 1-23). در سال ۲۰۰۰ جریان اقتصادی در سازمان ملل متحد با عنوان "مبارزه با سوءاستفاده از فناوری اطلاعات" توسط آمریکا و ۳۸ کشور دیگر از جمله روسیه، فرانسه و انگلیس مطرح شد. کشور چین به این قطعنامه نپیوست. هدف اصلی قطعنامه ۵۵/۶۳ ایجاد "مبنایی حقوقی برای مبارزه با استفاده‌های تبهکارانه از فناوری‌های اطلاعاتی" بود (Maurer. 2011: 35).

۳-۱- حملات سایبری: حمله مسلحانه یا توسل به‌زور

برای شناسایی عملی به‌عنوان یک حمله خصمانه چهار معیار را می‌توان شناسایی کرد: اول، مطابق ماده ۲ (۴) منشور سازمان ملل "همه اعضای سازمان ملل در روابط خود با تهدیدها یا استفاده از زور در برابر صداقت ارضی یا استقلال سیاسی از هر "دولت یا به هر طریقی بر خلاف اهداف سازمان ملل". در پاسخ به این سؤال که چه طیف وسیعی از عملیات سایبری می‌تواند "زور" در ممنوعیت باشد؟ می‌توان گفت؛ در صورت عدم وجود پیمان، مفهوم نیرو "باید مطابق با اهداف منشور تعریف شود. اگرچه معنی «زور» آن‌قدر گسترده است که شامل درگیری‌های مسلح و غیرمسلح است، اکثر مفسران امروز کلمه "زور" در ماده ۲ (۴) منشور سازمان ملل متحد مترادف با "عمل مسلحانه" یا "استفاده نیروی نظامی "در نظر آنها. اما این بدان معنا نیست که

[20] Group of government experts (GGE)
[21] Stepping Backward
[22] Forward Again

مهار زور محدود به جلوگیری از استفاده از سلاح‌های شیمیایی، بیولوژیکی یا هسته‌ای است. مطابق نظر مشورتی دیوان بین‌المللی دادگستری در مورد قانونی‌بودن تهدید یا استفاده از سلاح‌های هسته‌ای، دادگاه توضیح داد که ممنوعیت "هرگونه استفاده از نیرو بدون درنظرگرفتن سلاح" استفاده می‌شود. در حقیقت، شکی نیست که عملیات سایبری نیز می‌تواند با سایر سلاح‌ها سازگار باشد. این ممکن است شامل استفاده از عملیات سایبری به‌عنوان ابزاری دفاعی یا توهین‌آمیز باشد که افراد را می‌کشد یا به مردم آسیب می‌رساند یا اهداف یا زیرساخت‌ها را نابود می‌کند، صرف‌نظر از چنین تخریب یا هر دو ترکیب، یا هر دو ترکیب. درحالی‌که حملات سایبری به توانایی دسترسی به سلاح‌های فیزیکی سنتی، بیولوژیکی، شیمیایی یا هسته‌ای بستگی ندارد، اما بدون زیرساخت‌های لازم برای فضای مجازی نمی‌توان آنها را انجام داد و آیا این "سلاح‌های نظامی" هستند؟ از این منظر، می‌توان گفت که انتخاب ابزار یک کاربرد منظم نیست که دستگاهی را به سلاح تبدیل کند بلکه هدفی است که از آن دستگاه استفاده می‌شود و تحت‌تأثیر آن قرار می‌گیرد؛ بنابراین، استفاده از هر برنامه ترفند یا تعدادی از ترفندهایی که منجر به ازبین‌رفتن تعداد قابل‌توجهی از افراد یا ازبین‌بردن دارایی‌ها می‌شود، باید واجد شرایط حمله مسلحانه باشد که عملیات سایبری ظرفیت کیفی برای نامیدن به‌عنوان حمله مسلحانه در چارچوب ماده ۵۱ منشور ملل متحد را دارد. طبق ماده ۵۱ منشور سازمان ملل متحد، "در صورت حمله مسلحانه علیه یک عضو سازمان ملل، هیچ‌چیز در منشور فعلی حق خود را تضعیف نمی‌کند." باتوجه‌به این موضوع شکافی بین بند «۲» ماده (۴) که استفاده از زور است و ماده ۵۱ به وجود می‌آید. در واقع دامنه بند «۲» ماده (۴) گسترده‌تر از ماده ۵۱ است، زیرا نه‌تنها از کشورهای مسلح جلوگیری می‌کند بلکه شامل حالات غیرمستقیم و غیرمسلح زور نیز می‌شود و نه‌تنها استفاده واقعی بلکه تهدیدات صرف.

واژه جنگ سایبر بیشتر مفهوم بین‌دولتی دارد. بند «۲» ماده (۴) منشور ملل متحد فقط به دولت‌ها خطاب می‌کند و از آنها برای تفریح خودداری می‌کند. این بدان معنی است که استفاده یا تهدید باید به دولت‌ها نسبت داده شود. در حقوق بین‌الملل، این اعمال هنگامی که شخص یا هویت نماینده دولت‌ها یا با اجازه یا تصویب دولت به شکلی که مسئولیت حقوقی بین‌المللی را برای رفتار وی می‌پذیرد، به دولت‌ها نسبت داده می‌شود. چنین فردی به‌عنوان «نماینده دولت» توصیف شده است. این نماینده دولت در شمول قانون ۲۰۰۱ مسئولیت بین‌المللی دولت خواهد بود. استفاده از زور توسط بازیگران و هکرها غیردولتی ممکن است مربوط به حقوق بین‌الملل بشردوستانه یا حقوق جرایم بین‌المللی باشد. مفهوم حملات سایبری در واقع شامل عملیات مربوط به بازیگران دولت و غیردولتی است. معیار دوم برای تعیین اینکه آیا حملات سایبری یک حمله مسلحانه هستند توجه به دیدگاه مختل‌کنندگی به‌جای تخریب‌کنندگی است که بخش وسیعی از حملات سایبری همانند آنچه در گرجستان یا استونی رخ داد، آن را ناخوشایند نموده و همین امر آن را هم سنگ تخریب فیزیکی کرده است. معیار سوم که می‌تواند مفید باشد "میزان و اثرات" برای تخمین آسیب به زیرساخت‌های حیاتی است؛ بنابراین زیرساخت‌های حیاتی چیست؟ مجمع‌عمومی سازمان ملل زیرساخت‌های حیاتی را تعریف می‌کند: "زیرساخت‌های حیاتی شامل تولید، حمل‌ونقل و توزیع انرژی، حمل‌ونقل هوایی و دریایی، خدمات بانکی و مالی، تجارت الکترونیکی، آبرسانی، توزیع مواد غذایی و بهداشت عمومی و زیرساخت‌ها است." این به طور فزاینده‌ای تحت‌تأثیر فعالیت‌های آنها قرار می‌گیرد. "سازمان همکاری شانگهای همچنین شامل زیرساخت‌های حیاتی، از جمله تأسیسات عمومی، سیستم‌ها و نهادهایی است که این حمله ممکن است مستقیماً امنیت ملی را به خطر اندازد، چه به‌صورت جداگانه، اجتماعی و چه ایالتی (Melzer . 2011:10-14). پروفسور مایکل اشمیت[23] برای بررسی اینکه آیا حملات سایبری از نظر حقوق بشردوستانه بین‌المللی یک حمله مسلحانه محسوب می‌شوند، وجود خصوصیاتی را برای تطابق اثرات حمله سایبری با حمله مسلحانه لازم می‌داند (Schmitt . 1999:892-915).

[23] Michael Schmitt

۱. شدت: حملات مسلحانه تهدید به آسیب، مرگ، خسارت یا تخریب بیشتر نسبت به‌اجبار سیاسی یا اقتصادی است.
۲. فوریت: نتایج منفی حملات مسلحانه نسبت به‌اجبار سیاسی یا اقتصادی سریع‌تر هستند.
۳. مستقیم یا صراحت: نتایج حمله مسلحانه نسبت به‌اجبار اقتصادی یا سیاسی بیشتر وابسته به حمله است.
۴. مداخله کردن: در حمله مسلحانه، خسارات معمولاً در داخل مرزهای کشور هدف است اما در جنگ اقتصادی عموماً خارج از مرزهای هدف است.
۵. قابلیت اندازه‌گیری: نتایج حمله مسلحانه نسبت به اقتصادی یا سیاسی، راحت‌تر قابل‌اندازه‌گیری است.
۶. مشروعیت احتمالی: کاربرد خشونت عموماً غیرقانونی فرض می‌شود درحالی‌که اجبار اقتصادی یا سیاسی به‌صورت قانونی تصور می‌شود (Richardson . 2011:18-19).

حملات سایبری که باعث آسیب جسمی یا مرگ می‌شوند، به‌ویژه در تعریف قوانین بین‌المللی بشردوستانه است. بااین‌حال، هنوز مشخص نیست که آیا حمله سایبری که به مردم آسیب نمی‌رساند یا خسارت به اشیا در حوزه حقوق بین‌الملل بشردوستانه قرار می‌گیرد یا نه؟ (Richardson . 2011:18-19).

برای درک نقش حملات سایبری در جنگ، ما همچنین باید همان سؤالاتی را که از سلاح‌های دیگر داریم، یعنی دامنه، تخریب، هزینه، تأثیر و کاربردهای سیاسی داشته باشیم. حملات سایبری دارای قابلیت‌های استراتژیک و تاکتیکی است و می‌تواند در برابر نیروهای ایجاد شده یا علیه اهداف استراتژیک در اعماق دشمن مورداستفاده قرار گیرد. دامنه آن نامحدود است و تا آنجا که شبکه جهانی گسترش می‌یابد قابل‌استفاده است. اگرچه پیش‌زمینه‌های آماده‌سازی برای حمله سایبری زمان بر است اما سرعت حمله بدون توجه به مسافت می‌تواند در ثانیه اتفاق بیفتد (کوتاه‌ترین زمان ممکن) که هزینه‌های آن نیز بسیار پایین است. بااین‌حال، جنگ سایبری نقص دارد. ما هنوز قادر به تخمین خسارات ناشی از حملات سایبری نیستیم. به‌ویژه زمانی که اهداف تاکتیکی (مثل نیروهای نظامی) تبدیل به اهداف استراتژیک (مثل زیرساخت‌های غیرنظامی یا شهری می‌شود برای اینکه حملات برای غیرفعال‌کردن شبکه‌ها، آسیب‌های غیرضروری به‌طرف‌های غیر حل شده، خنثی یا حتی حمله‌کننده ممکن است مورد حمله قرار گیرد. این موضوع می‌تواند خطرات سیاسی ناخواسته‌ای به بار آورد (برای مثال حمله به صربستان فعالیت‌های تجاری متحدان ناتو را نیز متحمل خسارت کند) یا حمله به کره شمالی خدمات در چین را نیز آسیب رساند. ضربه اول سایبری ممکن است قابل‌درک باشد. البته، به‌عنوان بخشی از یک نبرد بزرگ‌تر، اما به‌تنهایی سایبری فقط می‌تواند به‌عنوان یک هشداردهنده یا برانگیختگی دشمن عمل کند و بنابراین نمی‌تواند در سلاح‌های هسته‌ای یا سنتی مؤثر باشد. عملکرد حملات سایبری بیشتر به‌سرعت عمل و غافلگیری بستگی دارد (Lewis . 2010:1-3). بنابراین در خصوص اینکه آیا حمله سایبری به حد حمله مسلحانه می رسد یا خیر، باید بر نتایج حوادث تکیه نمود و در نتیجه باید تحلیلی تأثیرگرایانه از یک حمله سایبری را در شناخت یک وضعیت به عنوان مخاصمه مسلحانه، که دستور العمل تالین۲ آن را وضعیتی معرفی می کند که مشتمل بر عملیات های خصمانه بوده و به عملیات های انجام شده با به کارگیری ابزارهای سایبری اشاره دارد را مد نظر قرار داد. دستورالعمل تالین، توسل و تهدید به توسل به زور را در اقدامات سایبری تعریف نموده و هردو آنان را ممنوع دانسته است. چنین اقداماتی مغایر اصل تمامیت ارضی و استقلال سیاسی کشورها و همچنین اهداف سازمان ملل تلقی شده اند. تاثیرات و اندازه اقدامات سایبری به جهت اطلاق به توسل به زور و غیر قانونی خواندن آنان را باید با اقدامات غیر سایبری در سطح توسل به زور مقایسه نمود(Schmitt . 2013:45-53).

۴- جنگ سایبر و حقوق بین‌الملل بشردوستانه

جنگ سایبری را می‌توان به‌عنوان یک جنگ مسلح ارزیابی کرد، بنابراین باید سازگاری آن با حقوق درگیری مسلحانه ارزیابی شود. به دلیل عدم تعریف رسمی از جنگ سایبری و فقدان تاریخچه‌ای که قوانین جنگ را در حال حاضر و در آینده راهنمایی

کند، تاکنون توافق بین‌المللی در مورداستفاده از قانون درگیری‌های مسلحانه برای جنگ سایبری در قرن بیست و یکم وجود ندارد. حقوق بین‌الملل بشردوستانه که گاهی اوقات به‌عنوان حقوق درگیری مسلحانه توصیف می‌شود، در هنگام افزایش خشونت بین طرفین مورداستفاده قرار می‌گیرد، اگرچه هیچ پیمان یا دستورالعمل به طور رسمی و قانونی استفاده از حقوق درگیری مسلحانه برای جنگ سایبری اعلام نشده است و بدون هیچ پیمانی پیش‌بینی‌نشده است. قوانین بشردوستانه باید در مورد همه ابزارهای جنگی کاربرد داشته باشد. از طرفی چون اصول و قوانین آشکار حقوق بشردوستانه برای سلاح‌های هسته‌ای اعمال نمی‌شود. این نتیجه‌گیری مغایر با توصیف حقوق بشردوستانه از اصول حقوقی است که کل حقوق درگیری مسلحانه را پوشش می‌دهد و برای همه اشکال جنگ و انواع سلاح‌ها از جمله سلاح‌های گذشته، حال و آینده اعمال می‌شود (ساعد، ۱۳۷۸: ۹۰-۹۱)؛ بنابراین، می‌توان آن را از این دیدگاه قوانین حقوق بشردوستانه به‌عنوان بخشی از قوانین حقوق درگیری مسلحانه در زمینه جنگ سایبری استنباط کرد.

۴-۱- مفهوم «حمله» تحت حقوق بین‌الملل بشردوستانه و عملیات سایبری

زیرساخت‌های غیرنظامی حیاتی که امکان ارائه خدمات ضروری را فراهم می‌کند، به طور فزاینده‌ای بر سیستم‌های دیجیتالی شده متکی است. حفاظت از چنین زیرساخت‌ها و خدماتی در برابر حملات سایبری یا آسیب‌های اتفاقی برای حفاظت از جمعیت غیرنظامی ضروری است. حقوق بین‌الملل بشردوستانه بدون توجه به نوع عملیات مضر، حفاظت خاصی را برای زیرساخت‌های خاص، مانند خدمات پزشکی و اشیای ضروری برای بقای جمعیت فراهم می‌کند. بیشتر قوانین ناشی از اصول تمایز، تناسب و اقدامات احتیاطی که حفاظت کلی از غیرنظامیان و اشیای غیرنظامی را فراهم می‌کند، فقط در مورد عملیات نظامی اعمال می‌شود که به‌عنوان "حمله" مطابق با تعریف حقوق بین‌الملل بشردوستانه اعمال می‌شود.[۲۴]

ماده ۴۹ پروتکل الحاقی، حملات را به‌عنوان «اعمال خشونت علیه دشمن، چه در حمله و چه در دفاع» تعریف می‌کند.[۲۵] بنابراین، این سؤال که مفهوم «حمله» باتوجه‌به عملیات سایبری چقدر گسترده یا محدود تفسیر می‌شود، برای کاربرد این قوانین و حفاظتی که از غیرنظامیان و زیرساخت‌های غیرنظامی انجام می‌دهند ضروری است. به طور گسترده پذیرفته شده است که عملیات سایبری که انتظار می‌رود منجر به مرگ، جراحت یا آسیب فیزیکی شود، حملات تحت حقوق بین‌الملل بشردوستانه است. از نظر کمیته بین‌المللی صلیب سرخ، این شامل آسیب‌های ناشی از تأثیرات قابل‌پیش‌بینی مستقیم و غیرمستقیم یک حمله می‌شود، برای مثال، مرگ بیماران در بخش‌های مراقبت‌های ویژه ناشی از عملیات سایبری در شبکه برق که منجر به قطع برق بیمارستان می‌شود. حملاتی که به طور قابل‌توجهی خدمات ضروری را بدون ایجاد آسیب فیزیکی مختل می‌کنند، یکی از مهم‌ترین خطرات برای غیرنظامیان است. بااین‌حال، دیدگاه‌های متفاوتی در مورد اینکه آیا عملیات سایبری که منجر به ازدست‌دادن عملکرد بدون ایجاد آسیب فیزیکی می‌شود، به‌عنوان یک حمله مطابق تعریف حقوق بین‌الملل بشردوستانه وجود دارد یا خیر. از نظر کمیته بین‌المللی صلیب سرخ، در طی یک درگیری مسلحانه، عملیاتی که برای غیرفعال‌کردن یک رایانه یا یک شبکه رایانه‌ای طراحی شده است، یک حمله تحت حقوق بین‌الملل بشردوستانه است، خواه این شیء از طریق جنبشی یا سایبری غیرفعال شود.[۲۶]

---

[۲۴] مفهوم حمله تحت حقوق بین الملل و حقوق بشر، که در هنر تعریف شده است از اولین پروتکل الحاقی ۱۹۷۷، با مفهوم «حمله مسلحانه» طبق ماده متفاوت است و نباید با آن اشتباه گرفته شود. ۵۱ منشور ملل متحد که به قلمرو jus ad bellum تعلق دارد. تأیید اینکه یک عملیات سایبری خاص، یا نوعی از عملیات سایبری، به منزله حمله تحت حقوق بین‌الملل حقوق بشر است، لزوماً به این معنا نیست که بر اساس منشور سازمان ملل متحد به عنوان یک حمله مسلحانه واجد شرایط است.

[۲۵] برای قوانینی که به طور خاص برای حملات اعمال می شود، به متن مربوط به پاورقی ۱۰ تا ۱۴ در بالا مراجعه کنید.

[۲۶] به صلیب سرخ، حقوق بشردوستانه بین‌المللی و چالش‌های درگیری‌های مسلحانه معاصر، ۲۰۱۱، ص. ۳۷; ICRC، حقوق بشردوستانه بین المللی و چالش های درگیری‌های مسلحانه معاصر، ۲۰۱۵، ص ۴۱-۴۲.

اگر مفهوم حمله تنها به‌عنوان اشاره به عملیاتی باشد که منجر به مرگ، جراحت یا آسیب فیزیکی شود، یک عملیات سایبری که هدف آن ناکارآمد کردن یک شبکه غیرنظامی (مانند برق، بانک، یا ارتباطات) است، یا انتظار می‌رود باعث ایجاد چنین مواردی شود. اتفاقاً، ممکن است تحت پوشش قوانین اساسی حقوق بین‌الملل بشردوستانه که از جمعیت غیرنظامی و اشیای غیرنظامی محافظت می‌کند، نباشد. تطبیق چنین درک بیش از حد محدودکننده‌ای از مفهوم حمله باهدف قواعد حقوق بین‌الملل بشردوستانه در مورد انجام خصومت‌ها دشوار خواهد بود؛ بنابراین ضروری است که کشورها برای محافظت کافی از جمعیت غیرنظامی در برابر تأثیرات عملیات سایبری، تفاهم مشترکی پیدا کنند.

۴-۲- قواعد حقوق بشردوستانه و کاربرد آن در جنگ سایبری

حقوق درگیری مسلحانه، به‌عنوان بخشی از قوانین بین‌المللی، فقط به دولت‌ها محدود می‌شود. بااین‌حال، این تخلف همچنین ممکن است شامل پیگیری مردم برای جنایات جنگی باشد. قوانین بشردوستانه بین‌المللی به اعتقاد برخی از افراد، قادر به کنترل حملات سایبری نیستند. به‌عبارت‌دیگر، حملات شبکه‌های رایانه‌ای درگیری مسلحانه محسوب نمی‌شوند و خارج از محدوده حقوق بین‌الملل بشردوستانه هستند؛ بنابراین، چنین حملاتی باید در واقع یک درگیری مسلحانه ایجاد کند تا بر حقوق بین‌الملل بشردوستانه در فضای مجازی مسلط شود. بااین‌حال، مفاد کنوانسیون ژنو و پروتکل‌های الحاقی متعاقب آن اظهار داشته‌اند که درگیری مسلحانه به روشی عادلانه قابل‌مشاهده است. درگیری مسلحانه به‌عنوان "هرگونه اختلاف بین کشورها و منجر به مداخله نیروهای مسلح" تعریف شده است. بااین‌حال، درگیری که منجر به دخالت ارتش می‌شود، تنها معیار نیست؛ بنابراین، هنگامی که اصول حقوق بین‌الملل بشردوستانه مطرح می‌شود، باید درجه‌ای از شدت و تداوم نیز در نظر گرفته شود. حقوق بین‌الملل بشردوستانه مبتنی بر ایده قربانیان درگیری مسلحانه است و از مجروحان حمایت می‌کند. اصول اساسی حقوق بین‌الملل بشردوستانه بیان می‌کند که درگیری‌های مسلحانه زمانی اتفاق می‌افتد که یک گروه برای آسیب، کشتن یا نابودی اقدام می‌کنند؛ بنابراین، حملات سایبری، درگیری مسلحانه تلقی می‌شود، حتی اگر استفاده از رایانه‌ها یک سلاح فیزیکی یا سنتی جنگی نباشد. ماده ۳۶ کنوانسیون نشان می‌دهد که نویسندگان قوانینی را برای پیشرفت‌های جدید در شیوه‌های جنگ پیش‌بینی کرده‌اند. به‌عبارت‌دیگر، حملات باید اساساً با تأثیرات آنها اندازه‌گیری شود، نه نحوه عملکرد آنها (Swanson . 2010:313-314).

اصول چهارگانه‌ای وجود دارد که در درگیری‌های مسلحانه باید در نظر گرفته شوند. علاوه بر اصل تمایز و تناسب، می‌بایست ضرورت نظامی و جلوگیری از رنج‌های غیرضروری نیز مدنظر قرار گیرد. هر یک از این اصول چارچوبی برای ارزیابی پیروی از قوانین بین‌المللی بشردوستانه ایجاد می‌کند (Richardson . 2011:22). اولین پروتکل الحاقی ۱۹۹۷ به کنوانسیون ژنو، اصول تمایز را تعیین می‌کند. "اصطلاح فنی در حقوق درگیری مسلحانه باهدف حمایت از غیرنظامیان و اهداف است." بر اساس این اصول، احزاب درگیر در جنگ باید ازیک‌طرف و اهداف نظامی و جنگ از طرف دیگر بین اهداف نظامی و غیرنظامی تمایز قائل شوند. دولت‌ها هرگز نباید از سلاح‌هایی استفاده کنند که قادر به شناسایی بین اهداف نظامی و غیرنظامی نیستند. برخی از اهداف هم استفاده نظامی و غیرنظامی دارند. این اهداف می‌تواند شامل ایستگاه‌های تولید برق، ارتباطات از راه دور، پل‌ها و سایر زیرساخت‌های غیرنظامی مورداستفاده گروه‌های نظامی در طول جنگ باشد. اگر هدف برای استفاده نظامی مؤثر و مفید باشد، این "استفاده ثانویه" ممکن است آن را به یک هدف نظامی مشروع تبدیل کند (Kelsey . 2008:1436).

تجزیه‌وتحلیل تطبیق حملات سایبری با اصل تمایز بسیار شبیه به تجزیه‌وتحلیل حمله سنتی خواهد بود و در بسیاری از عملیات حمله سایبری به‌وضوح مطابق با این اصل خواهد بود. مانند برنامه‌های توسعه نظامی برای حملات سایبری توسط اتحادیه‌های نظامی و حقوقی، باید آن را برای استفاده مؤثر در فضای مجازی دوباره تفسیر کند. برخی معتقدند که هر چیزی که برای حملات سنتی قانونی باشد، یک هدف نظامی قانونی برای حملات سایبری است. همچنین، موانع نسبی قوانین بین‌المللی بشردوستانه به

انواع سلاح‌ها یا جنگ مورداستفاده بستگی ندارد و بدون شک باید برای جنگ سایبری مورداستفاده قرار گیرد. همچنین، برخی از کاربردهای سلاح‌های سایبری به‌وضوح تحت اصل تمایز دوباره به دست می‌آیند، درحالی‌که این اصل به‌وضوح مانع استفاده‌های دیگر می‌شود. طبق این اصل، در برخی حملات، سلاح‌های سایبری می‌توانند برای اهداف کاملاً نظامی استفاده شوند. به نظر می‌رسد چنین کاربردی نقض اصل تمایز در حقوق بین‌الملل بشردوستانه است. به‌عنوان‌مثال، حمله به یک ایستگاه دفاعی هوایی و آن را به‌عنوان بخشی از صحنه نبرد عمومی خنثی می‌کند و ایستگاه دفاع هوایی نیز به‌عنوان یک مزیت نظامی خاص تلقی می‌شود. عملیاتی که تلفات غیرنظامی بیشتری دارند، مانند حمله به سیستم رایانه‌ای از هواپیمای مسافربری یا شبکه دفاع هوایی، اصل تمایز احتمالاً نقش مهمی در تعریف عملیات نظامی بازی خواهد داشت. حقوق بین‌الملل بشردوستانه تهاجم حقوق بین‌الملل بشردوستانه به فرماندهانی نیاز دارد که "می‌دانند که آنها نه‌تنها مورد اصابت قرار می‌گیرند، بلکه قادر به پیش‌بینی همه واکنش‌های یک حمله هستند."

۴-۳- اصول حقوق بین الملل بشر دوستانه در جنگ های سایبری

در شرایطی که هنوز مقررات صریحی در مورد درگیری‌های سایبری یا عملیات سایبری وضع نشده است، می‌توان از مقررات عمومی و اصول کلی حقوق بشردوستانه برای روشن‌کردن حقوق و وظایف طرفین استفاده کرد.

۴-۳-۱- اصل اساسی تفکیک

این اصل که تفکیک میان هدف‌های نظامی و غیرنظامی است، نقش بسیار مهمی در هدایت درگیری‌های مسلحانه بین‌المللی ایفا می‌کند. در سال ۱۹۹۶، دیوان بین‌المللی دادگستری دررابطه‌با سلاح‌های هسته‌ای اعلام کرد که هدف از اعمال این اصل در حقوق بشردوستانه، حفاظت از جمعیت و اموال غیرنظامیان است و این اصل، تمایز بین رزمندگان و غیر رزمندگان را مشخص می‌کند. دولت‌ها هرگز نباید جمعیت غیرنظامی را هدف قرار دهند و از سلاح‌هایی استفاده کنند که نمی‌تواند بین اهداف نظامی و غیرنظامی تمایز قائل شود. این قاعده فراگیر حقوق مخاصمات مسلحانه که حملات مستقیم علیه اشخاص و اموال غیرنظامی را ممنوع می‌کند در مورد حملات شبکه‌های رایانه‌ای نیز اعمال می‌شود (Dinstein . 2012:17).

۴-۳-۲- اصل تناسب و ممنوعیت ایراد خسارات جانبی بیش از حد

حفاظت از افراد و اموال غیرنظامیان، بر اساس اصل تفکیک، تنها محدود به حملات بدون تبعیض و ممنوعیت حملات مستقیم علیه آنها نیست، بلکه موضوع اساسی دیگر، کنترل و محدودکردن میزان خسارات جانبی به غیرنظامیان است. حقوق مخاصمات مسلحانه از این فرض شروع می‌شود که در حین اجرای عملیات نظامی ممکن است خساراتی به مردم غیرنظامی وارد شود و این قواعد تلاش می‌کند تاحدامکان این خسارات را محدود کند (Kalshoven . 2007).

۴-۳-۳- احتیاط های ممکن

احتیاط‌های ممکن، مواردی هستند که یا به‌صورت عملی بوده و یا به لحاظ عملی ممکن هستند و شامل درنظرگرفتن تمام شرایط حاکم در آن زمان (زمان حمله) هستند و از جمله ملاحظات نظامی و انسانی‌اند؛ بنابراین، احتیاط‌های ممکن می‌تواند بر مواردی مانند زمان حمله، مهماتی که قرار است استفاده شود و نیز ترجیح برخی تاکتیک‌های خاص بر سایر موارد تأثیرگذار باشند (Roscini . 2010:14).

بحث و نتیجه‌گیری

استفاده از عملیات سایبری به‌عنوان ابزار یا روش جنگ در یک درگیری مسلحانه خطر واقعی آسیب برای غیرنظامیان را به همراه دارد. برای حفاظت از جمعیت غیرنظامی و زیرساخت‌های غیرنظامی، مهم است که بدانیم چنین عملیاتی در خلأ قانونی رخ نمی‌دهند. کمیته بین‌المللی صلیب سرخ از همه کشورها می‌خواهد تأیید کنند که حقوق بین‌المللی بشردوستانه در عملیات سایبری در طول درگیری‌های مسلحانه اعمال می‌شود، با این درک که چنین تأییدی نه نظامی‌سازی فضای سایبری را تشویق می‌کند و نه جنگ سایبری را مشروعیت می‌بخشد. درعین‌حال، کمیته بین‌المللی صلیب سرخ معتقد است که بحث‌های بیشتری به‌ویژه در میان کشورها در مورد چگونگی تفسیر و اعمال حقوق بین‌الملل بشردوستانه در فضای سایبری موردنیاز است. زیرا کشورهایی تصمیم به توسعه یا دستیابی به قابلیت‌های سایبری دارند که به‌عنوان سلاح، ابزار و روش‌های جنگ واجد شرایط هستند، چه برای اهداف تهاجمی یا دفاعی باید اطمینان حاصل کنند که این قابلیت‌ها می‌تواند مطابق با تعهداتشان استفاده شود.

ازآنجایی‌که، حمله سایبری شکل جدیدی از کاربرد فضای سایبری در روابط بین‌الملل است که تغییرات اساسی در عرصه جنگ مدرن ایجاد کرده و ازاین‌رو جامعه بین‌المللی را با چالش جدیدی مواجه کرده است. با وجود پتانسیل حملات سایبری برای واردکردن خسارت شدید، موضوع کاربرد قواعد حقوق بشردوستانه بین‌المللی در حملات سایبری به چالشی مهم در حقوق بین‌الملل تبدیل شده است. این مقررات اگرچه تمام چارچوب جنگ سایبری و حمله سایبری را در برنمی‌گیرد، اما به دلیل فلسفه حقوق بشردوستانه، حمایت از غیرنظامیان و اصول دیگری مانند اصل تناسب و تمایز را مدنظر قرار داده است؛ بنابراین، این اصول و مقررات کماکان اجرا می‌شود و در مواردی که مقرراتی وجود ندارد، لازم است به حقوق بین‌الملل بشردوستانه عرفی و اصولی رجوع شود و در آن شرایط خاص، حقوق بین‌الملل بشردوستانه اجرا و اعمال شود. از سوی دیگر به دلیل عدم اجماع مجامع بین‌المللی و ابهام در اجرای برخی از این اصول و قواعد، با توسعه تدریجی قواعد قراردادی و عرفی فعلی می‌توان ابهامات موجود را برطرف کرد.

مراجع

- مسائلی، محمود و ارفعی، عالیه. (۱۳۷۱) جنگ صلح از منظر حقوق و روابط بین‌الملل، مؤسسه انتشارات وزارت امور خارجه، تهران.
- موسی‌زاده، رضا و امینیان. اکبر. (۱۳۹۰)، جمهوری اسلامی ایران و دیوان کیفری بین‌المللی، پژوهشکده تحقیقات استراتژیک، تهران.
- ساعد، نادر. (۱۳۷۸)، حقوق بشردوستانه و مسائل نوظهور (جنگ‌های پس از جنگ)، تهران، خرسندی.
- عباسی، مجید و مرادی، حسین، (۱۳۹۴) ، جنگ سایبری از دیدگاه حقوق بشردوستانه بین‌المللی، مجله مجلس و راهبرد، دوره ۲۲، شماره ۸۱، صفحات ۳۷ تا ۶۸ .
- دوست محمدیان، حمید، (۱۳۸۹) ، قانون جرایم و مقررات. "شواهد الکترونیکی." مجله تحلیلگران عصر اطلاعات، صفحات ۱-۲۱.
- یگانه آزاد. سعید. (۱۳۹۳). قانون حمله سایبری پایان‌نامه کارشناسی ارشد. شیراز: دانشگاه شیراز.
- دانشگاه امام حسین (ع) . (۱۳۷۸). هنر جنگ. تهران.
- نگاهی به فرماندهی سایبری آمریکا، ۱۳۹۱/۴/۲۰
- Arquilla, J. And David. R. (1993). "Cyberwar is coming!". Com parative Strategy, Vol. 12, No. 2.
- Sharp. W. (1999). "Cyberspace and the use of force". New York: Publications Aegis Research Corporation.
- T.G. Kelsey, Jeffrey (2008). "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", Michigan Law Review, Vol. 106.

- Lewis, James .A. (2010). "Thresholds for Cyberwar", Center for Strategic and International Studies, Available at: http://www.csis.org
- Maurer, T. (2011). "Cyber Norm Emergence at the United Nations- An Analysis of the UN"s Activities Regarding Cyber-security", Belfer Center for Science and International Affairs.
- Melzer, N. (2011). "Cyber warfare and International Law", The United Nations Institute for Disarmament Research, Availabale: www.unidir.org.
- Nye. Jr, J. S. (2010). "Cyber power". Harvard Univ Cambridge MA Belfer Center for Science and International Affairs.
- Ottis, R. (2011). "A systematic approach to offensive volunteer cyber militia". TUT Press.
- Shakarian, Paulo; Shakarian, Jana & Ruef, Andrew (2013), Introduction to Cyber warfare: A Multidisciplinary Approach, USA, Elsevier.

- Schmitt .M.(1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia: Journal of Transnational Law; Vol. 37. p. 892, 914, 915.
- Schmitt, M. N. (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.
- Reverson, Derek S. (2012), Cyberspace and national security: threats, opportunities, and power in a virtual world, USA, Georgetown University Press.

- Richardson, J. (2011). "Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield. J. Marshall J. Computer & Info. L., 29, 1. [10] Richardson, J. (2011). Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield. J. Marshall J. Computer & Info. L., 29, 1.
- Swanson, L. (2010). "The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict. Loy. LA Int'l & Comp. L. Rev., 32, 303.
- Dinstein, Y. (2012). The principle of distinction and cyber war in International Armed Conflicts. Journal of Conflict and Security Law, 17(2), 261-277.
- Khani, A. A. (2007). Soft War 3 (Battle in the Information Age). Tehran: Iran's Cultural Institute of Contemporary Abrar International Studies.
- Henderson, C. (2021). The United Nations and the regulation of cyber-security. Research Handbook on International Law and Cyberspace, 582-614.
- Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND corporation.
- Kalshoven, F. (2007). Reflections on the law of war: Collected essays. Brill.
- Roscini, M. (2010). World Wide Warfare-'Jus Ad Bellum'and the Use of Cyber Force. Max Planck Yearbook of United Nations Law, 14, 85-130.
- See text in relation to footnotes 16 and 15 above. With regard to the latter, they must not be attacked, destroyed, removed or rendered useless.
- The notion of attack under IHL, defined in Art. 49 of the 1977 First Additional Protocol, is different from and should not be confused with the notion of 'armed attack' under Art. 51 of the UN Charter, which belongs to the realm of jus ad bellum. To affirm that a specific cyber operation, or a type of cyber operations, amounts to an attack under IHL does not necessarily mean that it would qualify as an armed attack under the UN Charter.
- For rules that apply specifically to attacks, see text in relation to footnotes 10 to 14 above.
- See ICRC, International humanitarian law and the challenges of contemporary armed conflicts, 2011, p. 37; ICRC, International humanitarian law and the challenges of contemporary armed conflicts, 2015, pp. 41-42.
- http://www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf
- http://www.khabaronline.ir