جنگ سایبر از منظر حقوق بین‌الملل بشردوستانه

مجید عباسی،* حسین مرادی**

تاریخ دریافت ۱۳۹۲/۴/۲۳	تاریخ پذیرش ۱۳۹۳/۱۲/۲۵

در طول تاریخ همراه با پیشرفت‌های بشری در زمینه‌های گوناگون، شیوه‌های جنگ نیز دستخوش تغییر و تحول شده و به مرور تلاش شده تا این جنگ‌ها قانونمند شود. این تلاش‌ها در هر دوره‌ای برای سلاح‌های نوین انجام شد و قوانین مکتوب شدند. اما به یکباره گسترش فزاینده فناوری و توسعه آن به دنیای مجازی این مجال را به متخصصان نداد تا قوانین این نوع جنگ را نیز مکتوب نمایند و به ناگاه در مقابل اسلحه جدیدی قرار گرفتند که دارای خصوصیات مرموز و ناشناخته‌ای می‌باشد. اختراع رایانه و متعاقب آن اینترنت فضای جدیدی را به نام دنیای مجازی مقابل بشر قرار داد. این بار جنگ‌ها در فضای مجازی و سایبری پیش رفتند. حملات رایانه‌ای در حال افزایش شتاب است و این حملات نه تنها در منازعات سیاسی، بلکه در برنامه‌های باج‌گیرانه و با هدف صدمه زدن به تأسیسات حیاتی نیز استفاده شده‌اند. لذا از آنجا که این نوع حملات قابلیت صدمه زدن به غیرنظامیان را دارا می‌باشد کاربرد حقوق بین‌الملل بشردوستانه در این حوزه لازم و ضروری می‌باشد.

کلیدواژه‌ها: جنگ؛ جنگ سایبر؛ حملات سایبری؛ حقوق بین‌الملل بشردوستانه؛ فضای سایبر؛ جنگ مسلحانه

---

* استادیار دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبایی (نویسنده مسئول)؛
Email: majid_abbasi@yahoo.com

** دانشجوی دکتری روابط بین‌الملل دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبایی؛
Email: m.hossein1361@gmail.com

مقدمه

از زمانی که بشر پا به عرصه وجود نهاد، جنگ نیز همگام با او زاده شد و در روند سپری شدن تاریخ همراه با پیشرفت‌های بشری در زمینه‌های گوناگون، شیوه‌های جنگ نیز دستخوش تغییر و تحول قرار گرفت. همراه با پیشرفت علم و فناوری جنگ‌های تن به تن همراه با گرز و چوب تبدیل به جنگ‌های رو در رو با ابزار و آلات آهنی همچون شمشیر شد. در این جنگ‌ها هیچ حقوقی وجود نداشت. تنها اصل، شجاعت و جسارت و بالا بردن قدرت بدنی برای پیروزی بود. این روند ادامه یافت تا اینکه باروت اختراع شد. با کشف باروت و متعاقب آن اسلحه‌های آتشین شیوه‌های جنگ نیز متحول گردیده و دیگر، فقط آنکه در مقابلت مشغول جنگ بود متأثر نمی‌شد بلکه ممکن بود تیر شلیک شده به هرکسی اصابت کند. از آن زمان بود که بشر به این فکر فرو رفت تا حداقل معیارهایی را برای جنگیدن اعمال کردند. بانیان حقوق بین‌الملل کم‌کم تلاش کردند تا همگام با پیشرفت علم و افزوده شدن قدرت آتش و توان آسیب زدن، این نوع جنگ‌ها را قانونمند کنند. این تلاش‌ها در هر دوره‌ای برای سلاح‌های نوین انجام شد و قوانین مکتوب شدند. اما به یکباره گسترش فزاینده فناوری و توسعه آن به دنیای مجازی این مجال را به متخصصان نداد تا قوانین این نوع جنگ را نیز مکتوب کنند و به ناگاه در مقابل اسلحه جدیدی قرار گرفتند که دارای خصوصیات مرموز و ناشناخته‌ای است. اختراع رایانه و متعاقب آن اینترنت فضای جدیدی را به نام دنیای مجازی مقابل بشر قرار داد. این بار جنگ‌ها به سمت جنگ‌هایی در فضای مجازی و سایبری پیش رفتند، جنگی که معلوم نیست در آن سوی خط نبرد چه کسی صف‌آرایی کرده است. در دنیای مجازی دیگر دوست و دشمن مشخص نیست. این جنگ تن به تن نیست بلکه جنگ تفکر و اندیشه از مسافت بسیار طولانی است.

حال اعم از اینکه جهان آماده است یا نه، تسلیحات سایبری به بخش مهمی از جنگ نوین تبدیل شده‌اند. این نوع نبرد، فناوری‌های خود ملت هدف را بر علیه آن استفاده می‌کند تا زیرساخت‌های حیاتی آن را متوقف کند. به موازات پیشرفت اینترنت و فناوری‌های ارتباطی، شیوه‌های جنگ نیز متغیر و گوناگون شده است. علاوه‌براین، به خاطر هزینه پایین و قابلیت دسترسی گسترده به رایانه، همچنین توانایی فعالیت در آن به‌صورت گمنام، حملات سایبری

یک روش جذابی برای جنگ محسوب می‌شوند. در سال‌های اخیر، شمار حملات سایبری هم توسط بازیگران ملی و هم بازیگران غیرملی به‌طور چشمگیری افزایش یافته است.

همان‌طور که جوامع مدرن به‌طور فزاینده‌ای به ساختارهای اطلاعاتی داخلی و جهانی متکی هستند، این ساختارها بیشتر به‌عنوان اهدافی برای حمله در طی جنگ و انواع دیگر منازعات مدنظر قرار می‌گیرند. حملات رایانه‌ای بدخواهانه[1] درحال افزایش شتابمند است. به‌علاوه، این حملات نه تنها در منازعات سیاسی، بلکه همچنین در برنامه‌های باجگیرانه و با هدف صدمه زدن به تأسیسات حیاتی نیز استفاده شده‌اند. درحالی که حملات آنلاین هماهنگ برای سال‌های زیادی به‌عنوان تهدید مطرح بوده است، منازعه سایبری روسیه گرجستان در سال ۲۰۰۸ نشان داد که چگونه دولت‌ها به‌طور مؤثرتری در حال ورود به استفاده از حملات سایبری به‌عنوان راهی برای تضعیف زیرساخت‌های حیاتی حریفان و رقبا و سیستم‌ها و ابعاد حیاتی برای امنیت ملی، امنیت اقتصادی، ایمنی و بهداشت عمومی هستند. کارشناسان نظامی و استراتژیست‌ها اعتقاد دارند، اگر تاکنون نبردهای نظامی در زمین، دریا، هوا و فضا رقم می‌خورد؛ با ورود به قرن بیست و یکم باید منتظر نبرد در فضای سایبر به‌عنوان پنجمین بستر نبردهای نظامی باشیم.

با توجه به این مقدمه و اینکه جمهوری اسلامی ایران از جمله کشورهایی است که در سال‌های اخیر با معضل جنگ مجازی و سایبری مواجه بوده است، این مقاله می‌خواهد به این سؤال پاسخ دهد که آیا قوانین حقوق بین‌الملل بشردوستانه را می‌توان در زمینه جنگ‌های سایبری نیز به‌کار برد؟ و آیا می‌توان جنگ سایبر را به‌عنوان یک شیوه نوین جنگی خطاب کرد؟ در پاسخ به این پرسش، فرضیه پژوهش عبارت از این است که در حقوق بین‌الملل بشردوستانه یا حقوق بین‌الملل عرفی هیچ ماده یا قانونی وجود ندارد که به‌طورصریح جنگ سایبری یا حملات به شبکه‌های رایانه‌ای چه در زمان جنگ یا در زمان‌های خارج از جنگ و به‌صورت مستقل را غیرقانونی و ممنوع اعلام کند. این موضوع به این دلیل است که حقوق جنگ مربوط به قرن نوزدهم بوده و برای قابلیت کاربرد در عصر اطلاعات به روز نشده است. اما با تفسیر برخی قواعد موجود در زمینه جنگ‌های مسلحانه می‌توان این قوانین را به حوزه جنگ سایبر نیز مطابقت داد.

---

1. Malicious

۱. چارچوب مفهومی و ویژگی‌های فضای سایبر

۱-۱. تعریف جنگ

در ابتدای امر برای تعریف و شناخت جنگ سایبر می‌بایست واژه جنگ و سپس مفهوم فضای سایبر مورد کنکاش قرار گیرد تا در نهایت درک درستی از پدیده جنگ سایبر کسب شود. اپنهایم، حقوقدان معروف، جنگ را «جدل بین دو دولت از طریق قوای نظامی، با هدف تفوق و غلبه بر دیگری و اعمال شرایط دلخواه طرف پیروز» تعریف می‌کند. به نظر می‌رسد این تعریف امروزه حداقل در قسمت آخرین خود یعنی اعمال شرایط دلخواه طرف پیروز، مهجور شده باشد. به‌علاوه، در این تعریف روشن نیست که در چه زمان معینی جنگ واقع می‌شود (مسائلی و ارفعی، ۱۳۷۱: ۴).

برخی مثل وردوس[1] نیز جنگ را «جدلی مسلحانه بین دولت‌ها که در آن کلیه روابط صلح آمیز معلق شده باشد» می‌دانند. در اینجا نیز باید خاطرنشان کرد که امروزه فقط دولت‌ها نیستند که به جنگ توسل می‌جویند. کوینسی رایت نیز می‌نویسد: «جنگ شرط قانونی است که به دو یا چند گروه متخاصم فرصت می‌دهد تا نزاعی را با نیروهای مسلح، احساسات مردمی، تعصبات حقوقی و فرهنگ‌های ملی سازمان دهند» (دانشگاه امام حسین، ۱۳۷۵: ۲). او اضافه می‌کند که «جنگ هنگامی آغاز می‌شود که دولتی نیت خود را برای توسل به آن از طریق اعلان جنگ یا ضرب‌الاجل اعلام می‌دارد». او علاوه‌بر اعتقاد به جنگ در ابعاد مختلف، به دو شرط اساسی وجود دولت و اعلان جنگ توجه می‌کند. همچنین وجود قصد و نیت را می‌توان در گزارش «وضعیت حقوقی ناشی از اعمال فشارهای اقتصادی در ایام صلح» یافت. در این گزارش دبیر کل جامعه ملل اظهار می‌کند که از نظر حقوقی وجود حالت جنگ بین دو دولت به قصد آنها و نه طبیعت عملشان بستگی دارد. بدین ترتیب اتخاذ معیارهایی هرچند خشونت‌آمیز اگر با قصد جنگ همراه نباشد و از دید کشورهایی که آن معیارها در مورد آنان اتخاذ می‌گردد، جنگ تلقی نشود، از نظر حقوقی موجب ایجاد رابطه جنگ بین دول مربوطه نخواهد بود (مسائلی و ارفعی، ۱۳۷۱: ۵).

کلازوویتس می‌گوید: «جنگ عمل خشونت‌باری است که هدفش وادار کردن حریف

1. Verdos

به اجرای خواسته ماست. جنگ ادامه سیاست است. جنگ نه تنها خصیصه نظامی بلکه دیپلماتیک، روانشناسی و اقتصادی را نیز دارد.» او معتقد است جنگ ادامه سیاست است و برای نیل به اهداف سیاسی باید از همه ابزار کمک گرفت.

فون بوگوسلافسکی[1] جنگ را عبارت از «منازعه گروهی مشخص از انسان‌ها، قبایل، ملتها، مردم یا دولت علیه یک گروه متجانس دیگر می‌داند. از نظر گاستول بوتول[2] نیز «جنگ مبارزه مسلحانه و خونین بین گروه‌های سازمان یافته است». او به‌کارگیری اسلحه در نزاع، خونین بودن آن و سازمان داشتن گروه‌های متخاصم را دلیل بر وجود جنگ می‌داند (دانشگاه امام حسین، ۱۳۷۵: ۳-۲). در قطعنامه ۳۳۱۴ مجمع عمومی سازمان ملل متحد مورخ ۱۴ دسامبر ۱۹۷۴ که مبنای تعریف تجاوز در اصلاح اساسنامه دیوان کیفری بین‌المللی قرار گرفت، در ضمیمه ۱ این قطعنامه در بند «ب» ماده (۲) نیز «استفاده از هرگونه سلاح توسط یک دولت بر علیه قلمرو دولت دیگر» مصداق یک عمل تجاوزکارانه در نظر گرفته شده است (موسی‌زاده و امینیان، ۵۶:۱۳۹۰).

با توجه به تعاریف منتخب ذکر شده، جنگ در موارد زیر وجود خواهد داشت:

۱. حداقل دو گروه متخاصم وجود داشته باشد.

۲. حداقل یکی از آنها از قوای مسلح استفاده نماید.

۳. برخورد هرچند ساده، برای مدت طولانی بین آنها جریان داشته باشد.

۴. هردو طرف به اندازه معمول سازمان داده شده باشند (مسائلی و ارفعی، ۱۳۷۱: ۶).

باید پذیرفت که امروزه تعریف ابعاد جنگ، بسیار مشکل‌تر از گذشته است؛ چرا که لزوماً جنگ‌ها بین دولت‌ها نیست. مشخصات سنتی جنگ که وجود حداقل دو دولت را لازم می‌دانست جای خود را به جنگ‌هایی داده است که در آن عناصر غیردولتی هم مشارکت دارند. برای اطلاق جنگ به یک عمل رخ داده، به‌طور حتم می‌بایست یک نوع برخورد مسلحانه در روابط بین‌دولتی شکل گیرد تا به‌عنوان یک عمل جنگی فرض شود. واضح است که این نوع نگرش، یک تحلیل وستفالیایی از روابط بین‌المللی است که دولت‌ها را مبنای

1. Fonbogoslafsky
2. Gastalbotag

روابط قرار می‌دهد حال آنکه امروزه بازیگران غیردولتی وجود دارند که توانایی تأثیرگذاری آنها در عرصه بین‌المللی به مراتب در مواردی برتر از برخی کشورهاست.

امروزه همگام با تحول و انقلاب در فناوری، جنگ‌ها دچار تغییر و تحول شده‌اند و دیگر صرف اعتماد بر روش‌های سنتی جنگی نمی‌تواند پیروزی در جنگ را تضمین نماید. لذا نسل جدید نبردها، جنگ‌های فناوری محور با هدف کاهش خسارات غیرضروری و افزایش دقت و سرعت عملیات‌ها می‌باشد. در کنار این موارد، افراد، اشخاص و یا بازیگران غیردولتی دیگر در برخی مواقع با استفاده از امکاناتی که اینترنت و یا محیط سایبر در اختیار آنها قرار داده، بدون اینکه گلوله‌ای شلیک شود اعمالی را مرتکب می‌شوند که خسارات ناشی از آن بسی بالاتر از خسارات برخی جنگ‌های مسلحانه است. در جنگ سایبر به ساز و برگ‌های نظامی و ارتش‌های بزرگ نیاز نیست. در این جنگ چه بسا افراد اندکی با برخورداری از مهارت‌های بالا بتوانند به زیرساخت‌های حیاتی یک کشور خسارات زیادی وارد کنند. خساراتی که جبران آنها از خسارت‌های ناشی از موشک و بمب به مراتب مشکل‌تر باشد.

انقلاب اطلاعاتی آسیب‌پذیری را بازتعریف کرده است؛ زیرا هم اکنون پیشرفته‌ترین جوامع به‌دلیل وابستگی بسیار به اطلاعات دارای بیشترین آسیب‌پذیری در مقابل حملات هستند. انقلاب اطلاعاتی با پخش و توزیع قدرت در میان بازیگران دولتی ضعیف‌تر و بازیگران غیردولتی، دوباره به تعریف اینکه چه کسی توانایی تهدید را دارد، پرداخته و در عین حال انتظارات راجع به درگیری میان جوامع را نیز تغییر داده است (عبدالله‌خانی، ۱۳۸۶: ۲۷).

۲-۱. فضای سایبر

واژه سایبر به‌عنوان پیشوند از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضیدانی به نام نوربرت وینر[1] در کتابی با عنوان *سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین* در سال ۱۹۴۸ به‌کار برده شده است. سایبرنتیک علم مطالعه و کنترل سازوکارها در نظام‌های انسانی و رایانه‌ای است.

1. Norbert Wiener

سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای رایانه و اطلاعات است.

واژه «فضای سایبر»[1] یا فضای مجازی را نخستین بار ویلیام گیبسون[2] نویسنده داستان علمی تخیلی در کتاب نورومنسر[3] در سال ۱۹۸۴ به‌کار برده است. فضای سایبر در واقع با اختراع اینترنت به‌وجود آمد. تا سال ۱۹۵۰ رایانه، رادیو و تلویزیون اختراع شده بود اما در اختیار کمتر کسی قرار داشت و هیچ کدام از اینها نیز به هم متصل یا حتی از راه دور هم قابل اتصال نبودند. در دهه ۱۹۶۰ رایانه‌ها به هم متصل شدند. این کار ابتدا در داخل سازمان‌ها به‌صورت شبکه‌های محلی انجام گرفت. تا سال ۱۹۶۹ اولین شبکه وسیع در داخل آمریکا عمل می‌کرد. این شبکه که به نام حامی آن، یعنی آژانس پروژه پژوهش پیشرفته وزارت دفاع، آرپانت نامیده شد، مؤسسه پژوهشی استنفورد دانشگاه کالیفرنیا واقع در لس‌آنجلس، دانشگاه کالیفرنیا واقع در سانتاباربارا و دانشگاه یوتا را به هم متصل کرد. این شبکه تکامل یافت و تبدیل به اینترنت شد. در سال ۱۹۹۰ که مأموریت آرپانت به پایان رسید، اینترنت بیش از سیصد هزار میزبان داشت. این میزان در سال ۱۹۹۲ به یک میلیون، سال ۱۹۹۶ به ده میلیون و تا سال ۱۹۹۸ به ۳۰ میلیون نفر رسید و بعد از این سال بود که ضریب نفوذ اینترنت در جهان روبه گسترش نهاد (عبدالله‌خانی، ۱۳۸۶: ۱۵).

فضای سایبر یا فضای مجازی در تعریف برخی نویسندگان عبارت از: «مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی است». البته شاید بهتر باشد آن را چنین تعریف کنیم: «محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع و واقعی، فراتر از مرزهای جغرافیایی و با ابزار خاص خود، در آن زنده و مستقیم روی می‌دهد». قید «واقعی»، مانع از این است که تصور شود مجازی بودن این فضا به معنای غیرواقعی بودن آن است؛ چرا که در این فضا نیز همان ویژگی‌های تعاملات انسانی در دنیای خارج همچون مسئولیت وجود دارد. ضمن این که فضای سایبر در واقع یک «محیط» است که ارتباطات در آن انجام می‌شود؛ نه صرف

1. Cyber Space
2. William Gibson
3. Neuromancer

مجموعه‌ای از ارتباطات. از سوی دیگر، این ارتباطات اگرچه ممکن است در همه شرایط آنلاین نباشد، ولی زنده و واقعی و مستقیم است. از این‌رو، تأثیر و تأثر بالایی در این روابط رخ می‌دهد (Ottis and Lorents, 2010: 1-2).

تعاریف بسیاری از فضای سایبر انجام شده است. برای مثال وزارت دفاع آمریکا، فضای سایبر را به‌عنوان «قلمرو جهانی در محیط اطلاعاتی مشتمل بر شبکه به هم پیوسته‌ای از زیرساخت‌های فناوری اطلاعات شامل اینترنت، شبکه‌های ارتباطات راه دور، سیستم‌های رایانه و پردازشگرها و کنترل‌کننده‌های تعبیه شده»[1] تعریف کرده است. این تعریف فقط عامل سخت‌افزار را در نظر گرفته و به نقش انسان بی‌توجه است. مرکز عالی همکاری دفاع سایبری ناتو که در استونی واقع شده نیز فضای سایبر را این‌گونه تعریف کرده: «فضای سایبر دسته‌ای از سیستم‌های اطلاعات درهم تنیده وابسته به زمان[2] و کاربران انسانی که با این سیستم‌ها در حال درهم کنش[3] می‌باشد.» این تعریف نقش عامل انسانی را نیز در نظر می‌گیرد و سیستم‌های اطلاعاتی درهم تنیده نیز عوامل سخت‌افزار، نرم‌افزار و ابزارهایی که آنها را به هم متصل می‌کند را شامل می‌شود (Ottis and Lorents, 2010:2).

فضای سایبر در اصل یک فضا و محیطی است مشابه سایر حوزه‌های رقابتی همچون دریا، زمین و هوا اما با یک تفاوت و آن هم اینکه این محیط برخلاف بقیه محیط‌ها ساخته دست بشر بوده و غیرملموس است (Libicki, 2009:11). واژه سایبر به فناوری رایانه و الکترونیک‌محور اشاره دارد. فضای سایبر نیز یک قلمرو عملیاتی تنظیم شده به‌وسیله استفاده از علم الکترونیک است تا اطلاعات را از طریق سیستم‌های به هم پیوسته و زیرساخت‌های مرتبط با آن مورد بهره‌برداری قرار دهد. بنابراین فضای سایبر یک رژیم پیوندی منحصر به فرد از دارایی‌های فیزیکی و مجازی، سخت‌افزار و نرم‌افزار، که همه شبکه‌های رایانه‌ای در جهان از جمله اینترنت به‌علاوه شبکه‌های دیگر که به اینترنت وصل نیستند را دربرمی‌گیرد، می‌باشد (Maurer, 2011:8).

---

1. Embedded Processors and Controllers
2. Time-Dependent
3. Interact

۳-۱. قدرت در فضای سایبر[1]

فضای سایبر همانند هر فضایی، زمین منازعه است که منتهی به اجتناب‌ناپذیری منازعه در آن می‌شود. لذا در این حوزه منازعه همانند هر میدان جنگ دیگری، داشتن قدرت لازم و توانمندی‌های مرتبط با آن نبرد می‌تواند در راه کسب موفقیت در تأمین امنیت برای شهروندان و قلمرو داخلی مثمرثمر باشد. همان‌طور که جوزف نای مطرح می‌نماید قدرت در زمینه معنا می‌یابد و رشد سریع فضای سایبر زمینه‌ای جدید و مهم در سیاست‌های جهانی است. هزینه پایین ورود، گمنامی و نامتقارن بودن در آسیب‌پذیری، بدین معناست که بازیگران کوچکتر در فضای سایبر نسبت به حوزه‌های سنتی‌تر سیاست جهانی ظرفیت بیشتری برای اعمال قدرت سخت و نرم دارند (Nye, 2010: 1). لذا در این معنا جنگ در فضای سایبر امری همیشگی و جزئی از سیاست خواهد بود.

به دست آمدن قدرت در فضای سایبر مدیون انقلاب اطلاعاتی کنونی موسوم به «انقلاب صنعتی سوم[2]» می‌باشد که این نوع از قدرت، نوع درگیری میان بازیگران را نیز متحول کرده است. قدرت سایبری از نگاه رفتاری به معنای «توانایی کسب نتایج مطلوب با استفاده از منابع اطلاعاتی الکترونیکی در حوزه سایبری می‌باشد». این تعریف جامع به نظر نمی‌رسد. تعریف دیگری که شاید جامع‌تر باشد عبارت است از: «توانایی استفاده از فضای سایبر برای خلق مزیت‌ها و تأثیر بر حوادث محیط‌های عملیاتی دیگر و بیان و کاربرد ابزارهای قدرت». قدرت سایبری می‌تواند برای کسب نتایج دلخواه در فضای سایبر استفاده شده و یا می‌تواند از ابزارهای سایبری برای کسب نتایج مطلوب در حوزه‌های دیگر خارج از فضای سایبر استفاده کند. در همین راستاست که باراک اوباما در سال ۲۰۰۹ با توجه به اهمیت موضوع، خواستار تمرکز در زمینه قدرت سایبری شده (Nye, 2010: 2-5) و دستور تشکیل فرماندهی سایبری آمریکا که جزئی از آژانس امنیت ملی آمریکا مشهور به NSA می‌باشد را صادر کرد. در تاریخ ۲۳ ژوئن ۲۰۰۹ این

1. Cyber Power
2. Third Industrial Revolution

دستور به فرماندهی استراتژیک ایالات متحده ابلاغ شد و در سپتامبر همان سال این نهاد شروع به فعالیت نمود (www.mashreghnews.org, 1391) و در ۱۲ ژوئن ۲۰۱۱ نیز مجوز جنگ سایبری و خرابکاری رایانه‌ای را در سایر کشورها صادر کرد (www.khabaronline.ir).

٤-١. امنیت سایبری

امنیت سایبری توسط اتحادیه جهانی مخابرات به‌عنوان «مجموعه‌ای از ابزارها، سیاست‌ها، مفاهیم امنیتی[1]، خط‌مشی‌های حفاظتی[2]، دیدگاه‌های مدیریت بحران[3]، فعالیت‌ها[4]، آموزش، بهترین رویه‌ها[5]، اطمینان یا اعتماد[6] و فناوری‌هایی است که می‌تواند برای حمایت محیط سایبر و دارایی‌های کاربر و سازمان استفاده شود. طبق نظر جوزف نای امنیت سایبری می‌تواند به چهار تهدید اصلی تقسیم شود: جاسوسی، بزهکاری، جنگ سایبری و تروریسم سایبری. امکان وجود تهدید در مرحله نخست به سه منبع برمی‌گردد: ۱. نقص‌هایی که در طراحی اینترنت وجود دارد، ۲. نقص‌هایی که در سخت‌افزار و نرم‌افزار می‌باشند، ۳. حرکت به سمت بارگذاری سیستم‌های آنلاین بحرانی و حساس‌تر (Maurer, 2011: 8-9).

٥-١. جنگ سایبر

اعم از اینکه فضای سایبر را به‌عنوان یک فضای مجازی یا فقط مجموعه‌ای از منابع[7] در نظر گیریم، بازیگران (اعم از دولت‌ها، شرکت‌ها، سازمان‌ها، گروه‌ها و اشخاص) برای کنترل آن با هم رقابت خواهند کرد و با در نظر گرفتن ویژگی‌های قدرت در فضای سایبر، منازعه و برخورد امری همیشگی و جزئی از سیاست روزمره خواهد بود (Ottis and Lorents, 2010: 4).حال برای فهم موضوع جنگ سایبری به‌عنوان یک پدیده جدید در عرصه روابط

1. Security Concepts
2. Security Sefeaguard
3. Risk Management Approaches
4. Actions
5. Best Practices
6. Assurance
7. Collection of Resources

میان بازیگران (دولتی و غیردولتی) تعاریف متعددی که از آن بعمل آمده، ارائه می‌شود.

جنگ سایبر در ساده‌ترین تعریف به‌عنوان «استفاده از رایانه و اینترنت برای جنگیدن در فضای سایبر تعریف شده است» (عبدالله‌خانی، ۱۳۸۶: ۱۳۶-۱۳۵). اما به‌صورت جزئی‌تر اصطلاح جنگ سایبر به جنگ انجام گرفته در فضای سایبر از طریق ابزارها و روش‌های سایبری اشاره دارد. در حالی که واژه جنگ عموماً به خصومت ارتش در وضعیت‌های منازعه مسلحانه اشاره دارد، فضای سایبر می‌تواند به‌عنوان شبکه درهم تنیده جهانی زیرساخت‌های ارتباطاتی و اطلاعاتی دیجیتال شامل اینترنت، شبکه‌های ارتباطات راه دور، سیستم‌های رایانه‌ای و اطلاعات موجود در آن توصیف شود. بنابراین، آلودگی شبکه رایانه دشمن درحال مبارزه با ویروس می‌تواند یک جنگ سایبری تلقی شود، درحالی که بمباران هوایی فرماندهی سایبری نظامی نمی‌تواند (Melzer, 2011: 4).

کلارک و کناک[1] جنگ سایبر را به‌عنوان «نفوذ غیرمجاز به‌وسیله، از طرف، یا در حمایت از، یک دولت به شبکه‌ها یا رایانه‌های ملی دیگری، یا هر فعالیت متأثرکننده سیستم‌های رایانه‌ای، که هدف در آن جمع کردن، تغییر دادن یا دستکاری اطلاعات[2]، یا باعث مختل شدن یا صدمه زدن به رایانه، طرح شبکه[3]، یا اهداف کنترل سیستم رایانه است» تعریف کرده‌اند (Maurer, 2011: 15).

مرکز عملیات سایبری آمریکا و کتاب راهنمای تروریسم سایبری حملات سایبری را به‌صورت زیر تعریف می‌کنند: «استفاده عمدی از فعالیت‌های مختل کننده، یا تهدید مربوط به آن، علیه رایانه‌ها وشبکه‌ها، با هدف ضرر و زیان به بار آوردن یا بیشتر با هدف اجتماعی، ایدئولوژیکی، مذهبی، سیاسی یا اهداف مشابه. یا برای وادار کردن هر شخصی برای پیشبرد چنین اهدافی ...» چنین ضرر و زیانی می‌تواند به شبکه رایانه‌ای علاوه‌بر تسهیلات فیزیکی و اشخاص نیز ضرر بزند. حملات سایبری متفاوت از جرم‌های سایبری[4] هستند، که توسط قوانین جنایی ملی کنترل شده و شامل اعمالی همچون دزدی هویت[5] و کلاهبرداری اینترنتی هستند. حملات سایبری برخلاف جرم‌های سایبری، «عملی تهاجمی

1. Clarke and Knake
2. Falsify Data
3. Network Device
4. Cyber Crimes
5. Identity Theft

برعلیه حریف یا دشمن، که ممکن است فرد، سازمان و یا دولت رقیب باشد، را به‌صورت یک تلاش مداوم برای کسب هژمونی در حوزه‌های سیاسی و تجاری شامل می‌شود» (Swanson, 2010: 307).

در واقع از نگاه دولت‌محورانه جنگ سایبر، با هدف از هم گسیختن سیستم‌های اطلاعاتی و مخابراتی، سیستم‌های کنترل و فرماندهی، ارتباطات، خبرگیری و جاسوسی نیروهای نظامی دشمن و غیرعملیاتی‌سازی آنها در صحنه نبرد صورت می‌گیرد. به عبارت بهتر به انجام عملیات نظامی براساس اصول اطلاعاتی و شبکه‌های الکترونیکی اشاره دارد (Arquilla and Rohfeldt, 1993: 27).

به‌طور کلی واژه‌های «جنگ سایبر»، «مبارزه سایبری»، «خصومت‌های سایبری[1]»، «منازعه سایبری» به‌صورت کاملاً موثق با هدف حقوق بین‌المللی تعریف نشده است. تنها معاهده‌ای که آن را تعریف کرده به‌وسیله سازمان همکاری منطقه‌ای شانگهای[2] است که نگرانی‌هایی را نسبت به «جنگ اطلاعات» ابراز داشته و اشاره کرده است که جنگ سایبری به معنای: مقابله میان دولت‌ها در عرصه اطلاعاتی با هدف صدمه زدن به سیستم‌های اطلاعاتی، روندها و منابع، ساختارهای حیاتی و مهم، تضعیف سیستم‌های سیاسی، اقتصادی و اجتماعی، عملیات‌های روانی گسترده برای بی‌ثبات‌سازی جامعه و دولت، همچنین مجبور کردن دولت برای اتخاذ تصمیماتی در راستای منافع مخالفین.

با توجه به مطالب فوق‌الذکر واژه‌های «جنگ سایبر» «منازعات سایبری» و «خصومت سایبری» باید به منازعه مسلحانه در چارچوب حقوق بین‌الملل بشردوستانه محدود شود و در واقع تهدیدات امنیتی که از فضای سایبری نشئت گرفته و به آستانه حمله مسلحانه نرسیده باشد تحت عناوین «جرم سایبری»، «عملیات‌های سایبری[3]»، «نظم و کنترل سایبری[4]»، «تروریسم سایبری» و«دزدی سایبری[5]» نامیده می‌شود (Melzer, 2011: 22).

---

1. Cyber Hostilities
2. Shanghai Regional Cooperation Organization
3. Cyber Operations
4. Cyber Policing
5. Cyber Piracy

۱-۵-۱. ویژگی خاص جنگ سایبری

فضای سایبر تنها حوزه‌ای است که به‌طور کامل ساخته دست بشر است. آن مجموعه‌ای است که توسط بخش خصوصی ساخته شده، حفظ شده و در سرتاسر جهان عمل کرده و به آرامی در واکنش به نوآوری‌های فناوری نیز تغییر می‌کند. در حالی که فضای سایبر به راحتی برای دولت‌ها، سازمان‌های غیردولتی، بازیگران خصوصی و اشخاص قابل دسترس است، IPهای نامشخص و استفاده از بات‌نتها، شناسایی منشأ عملیات را مختل می‌کند بنابراین ارائه هویت معتبر و نسبت دادن حملات سایبری مشکل است (Melzer, 2011:5).

۲-۵-۱. انواع حملات سایبری

جنگ سایبر در سطحی عمیق‌تر، در واقع جنگ دانش است (Arquilla and Ronfeldt, 1993: 27) جنگی که برمبنای رایانه و اطلاعات می‌باشد. مارتین لیبسکی از دانشکده دفاع ملی آمریکا در سال ۱۹۹۵ جنگ اطلاعات را بر هفت دسته طبقه‌بندی کرده است: فرماندهی و کنترل[1]، جنگ جاسوس‌محور[2]، جنگ الکترونیک، جنگ روانی، جنگ هکری[3]، جنگ اطلاعات اقتصادی و جنگ سایبری (Hughes, 2010: 5).

جنگ سایبری آخرین شکل جنگ اطلاعات است و می‌تواند شامل موارد زیر باشد:

۱. **خرابکاری اینترنتی[4]:** حملاتی جهت تغییر محتوا و شکل صفحات وب یا اخلال در سرویس‌دهی[5] که آسیب چندانی را وارد نمی‌سازد.

۲. **گردآوری داده‌ها:** دسترسی به اطلاعات طبقه‌بندی شده که امکان جاسوسی از نقاط مختلف جهان را فراهم می‌کند.

۳. **حملات گسترده اخلال در سرویس‌دهی:** در این نوع حمله شمار زیادی از رایانه در یک کشور مبادرت به ایجاد اخلال در سرویس‌دهی سیستم‌های کشورهای دیگر می‌کنند.

---

1. Command-and-Control
2. Intelligence-Based Warfare
3. Hacker Warfare
4. Web Vandalism
5. Denial-of-ServiceAttacks

٤. اخلال در تجهیزات[1]: فعالیت‌های نظامی که در آنها از رایانه و ماهواره برای هماهنگی استفاده می‌شود در خطر این نوع حمله قرار دارند، زیرا مهاجمان می‌توانند فرمانها و ارتباطات را رهگیری کرده یا تغییر دهند.

۵. حمله به زیرساخت‌های حیاتی: نیروگاه‌های برق، تأسیسات آبرسانی و سوخت‌رسانی، ارتباطات و حمل‌ونقل در برابر این نوع حمله با آسیب‌پذیری زیادی مواجه هستند (عبدالله‌خانی، ۱۳۸۶: ۱۳۶).

۳-۵-۱. استثمار شبکه رایانه‌ای

اصطلاح «عملیات سایبری[2]» یا «عملیات شبکه رایانه‌ای[3]» اشاره به تقلیل اطلاعات به‌صورت فرمت الکترونیکی و حرکت واقعی آن اطلاعات میان عناصر فیزیکی زیرساخت‌های سایبری دارد. عملیات‌های سایبری به سه دسته «حمله شبکه رایانه‌ای[4]»، «استثمار شبکه رایانه‌ای[5]» و «دفاع شبکه رایانه‌ای[6]» تقسیم می‌شوند. در حالی که همه عملیات‌های سایبری با هدف «اختلال، ممانعت[7]، تنزل دادن یا تخریب اطلاعات موجود در رایانه‌ها و شبکه‌های رایانه‌ای را شامل می‌شود، استثمار شبکه رایانه‌ای اشاره به «عملیات توانمندکننده و جمع‌آوری اطلاعات برای به دست آوردن داده‌ها از هدف یا سیستم‌های اطلاعاتی خودکار دشمن یا شبکه‌ها دارد». در عوض دفاع شبکه رایانه‌ای اشاره به «فعالیت‌هایی برای حمایت، کنترل، تحلیل، کشف و پاسخ به فعالیت غیرمجاز داخل سیستم‌های اطلاعاتی و شبکه‌های رایانه‌ای می‌نماید». یا به‌طور خلاصه جلوگیری از حملات شبکه رایانه و استثمار شبکه رایانه از طریق جاسوسی، ضدجاسوسی تقویت قانون و قابلیت‌های نظامی است. این اصطلاحات که مخصوص عملیات در فضای سایبر است باید به دقت از اصطلاحات فنی موجود در حقوق

1. Equipment Disruption
2. Cyber Operation
3. Computer Network Operation
4. Computer Network Attack
5. Computer Network Exploitation
6. Computer Network Defence
7. Denial

بین‌الملل همچون «زور[1]» «حمله مسلحانه» و «حمله» شناسایی شود (Melzer, 2011: 5).

استثمار شبکه رایانه یک حمله محسوب نمی‌شود و باید بین آن و حملات سایبری تمایز قائل شد. این عمل دارای برخی مشخصه‌های بارز است که آن را از حملات سایبری متمایز می‌کند. ۱. استثمار شبکه رایانه کاربر را از استفاده کامل از سیستم یا دستگاه محروم نمی‌کند بلکه تنها ضرری که به کاربر می‌رسد این است که اسرار خصوصی و محرمانه او دزدیده می‌شود. ۲. چون تقریباً کشف استثمار شبکه رایانه غیرممکن است سیاست بازدارندگی تنها در موارد استثنا می‌تواند کارساز باشد (Libicki, 2009: 23).

٤-٥-١. بازدارندگی سایبری[2]

ژنرال کارت وی[3] از ارتش آمریکا، بازدارندگی سایبری را این‌گونه تعریف می‌کند:«نیاز به توسعه قابلیت‌ها و تواناییهایی در فضای سایبر برای انجام اعمالی علیه آنچه دیگران می‌خواهند بر علیه ما انجام دهند.» این عمل متضمن نوعی تلافی و عمل متقابل بر علیه دولت مهاجم می‌باشد. هدف بازدارندگی کاهش انگیزه‌ها برای شروع یا انجام اعمال متضمن دشمنی بیشتر می‌باشد و در واقع این یک نوع تنبیه در مقابل طرف نقض‌کننده و متجاوز است (Libicki, 2009: 27-28).

توازن هسته‌ای میان آمریکا و شوروی در طی جنگ سرد، قاعده‌ای تاریخی برای این عقیده به‌وجود آورد که بازدارندگی هسته‌ای نیز باید وجود داشته باشد. البته بازدارندگی سایبری متفاوت از بازدارندگی هسته‌ای یا به‌طورکلی بازدارندگی نظامی است. در بازدارندگی هسته‌ای یا نظامی هدف واضح و مشخص بوده و در معرض خطر قرار دارد و تازمانی که تسلیحات وجود دارند ادامه خواهد یافت. در درگیری هسته‌ای همچنین، دخالت و درگیری طرف ثالث یا طرف غیردولتی تقریباً غیرممکن است. در بازدارندگی سایبری ضربه زدن اشتباهی به طرف ثالث نمی‌تواند توجیه‌کننده منطق بازدارندگی باشد بلکه فقط جبهه درگیری را به جای یک نفر تبدیل به دو نفر می‌کند. بنابراین اسناد مورد استفاده باید

1. Force
2. Cyberdeterrence
3. Cartwright

کاملاً مجاب‌کننده و موثق باشد. براساس اطلاعات موثق بیش از یکصد کشور در حال توسعه آنچه قابلیت‌های حملات سایبری[1] نامیده می‌شود، هستند. هر کشوری می‌تواند هدف حمله قرار گیرد چراکه همانند جنگ هسته‌ای در اینجا هدف به‌صورت آشکار بیان نمی‌شود و برای دیگران نیز هدف آشکار و مشهود نیست. در اینجا فقط حمله‌کننده و مورد حمله واقع شده باخبر می‌شوند که حمله صورت گرفته است حتی اگر این حمله موفق نباشد. حملات تلافی‌جویانه تنها برای بازدارندگی مفید هستند. برخلاف حملات تلافی‌جویانه سنتی یا هسته‌ای، آنها قادر به خلع سلاح نیستند. پیش‌نیازهای حمله سایبری بسیار اندک بوده و شامل موارد زیر است: یک هکر توانمند، اطلاعات درباره هدف، برآورد آسیب‌پذیری‌های احتمالی، رایانه شخصی و هر نوع ارتباط شبکه‌ای[2](Libicki, 2009: 39-59).

۲. تبعات امنیتی حملات سایبری

حملات سایبری که در کمتر از یک دهه گذشته اتفاق افتاده مشخص می‌کند که چگونه دولت‌ها در حال استفاده از فناوری‌های مدرن هستند و به شدت خود را درگیر جنگ اطلاعاتی کرده‌اند تا زیرساخت‌های حیاتی رقبا را تضعیف کنند. یک نگرانی جدی بین‌المللی وجود دارد مبنی‌بر اینکه منازعات خارجی دولت‌ها می‌تواند به‌طور پیش‌دستانه‌ای حملات رایانه‌محور[3] به سیستم‌های ملی یا منطقه‌ای، همچون زیرساخت‌های توزیع انرژی، ارتباطات راه دور 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 به‌طور موقت آنها را از کار انداخت که این سایت‌ها شامل دفتر رئیس‌جمهور، وزارت امور خارجه و وزارت دفاع بود که منتهی به

1. Cyberattack Capability
2. Network Connection
3. Computer-Based

بروز مشکلات ارتباطاتی در سراسر این کشور شد. حتی جدیدتر از آن، به تازگی کشف شده که هکرهای چینی به دفعات زیاد شبکه‌های رایانه‌ای کاخ سفید را شکسته‌اند و ایمیل ارتباطی مبادله شده در میان مقامات دولتی را به دست آورده‌اند.

گاهی اوقات حتی خسارت به‌وجود آمده به‌وسیله بسیاری از این حملات منجر به آسیب، مرگ و ضرر شخصی شده است. شاید در شدیدترین مثال، حملات ۲۰۰۷ به وب‌سایت‌های استونی، بیشتر مردم را دچار سردرگمی و گیجی کرد. در زمان این حملات، استونی اساساً یک ایمیل دولتی بنیان نهاد که بسیاری از ابعاد دولتی خارج از حالت آنلاین شدند. علاوه‌بر از کار انداختن بسیاری از وب‌سایت‌های تجاری و دولتی مهم استونی، حملات سایبری همچنین باعث شد شماره تلفن‌های ضروری برای تماس با آمبولانس و آتش‌نشانی به مدت بیش از یک ساعت غیرقابل دسترس باشد. در نتیجه، آشوب و ناراحتی گسترده ۱۵۰ زخمی به جای گذاشت و یک تبعه روسی نیز کشته شد. در مقایسه، حملات لیتوانی منجر به مخدوش شدن چهره وب‌سایت‌های دولتی و تجاری با نمادهای کمونیستی و بی‌محتوا شد. به هرحال، دولت قادر بود تا امور دفاعی لازم برای این حملات را تدارک بیند. این دو مثال اثبات کردند که حملات سایبری می‌تواند غیرقابل پیش‌بینی باشد (Swanson, 2010: 308-310).

نوع منحصربه فرد 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 به‌وجود آمد مشخص شد که ویروس معروف به «استاکس نت» برای نفوذ و از کار انداختن مخصوص تأسیسات هسته‌ای ایران ساخته شده است. در نهایت مشخص شد که این ویروس به‌عنوان یک سلاح طراحی شده تا سانتریفیوژهای حاضر در چرخه غنی‌سازی اورانیوم را مختل کند یا از کار بیندازد. این ویروس ابتدا در بلاروس کشف شد و در نهایت سیستم‌های رایانه‌ای در ایران، اندونزی، هند، آمریکا، استرالیا، انگلیس، مالزی و پاکستان را تحت تأثیر قرار داد (Richardson, 2011: 10-11).

۳. عملیات‌های سایبری و حقوق حاکم بر روابط بین‌الملل

۳-۱. سازمان ملل متحد و جنگ سایبری

امروزه مهمترین منبع حقوق حاکم بر روابط بین‌الملل منشور سازمان ملل متحد می‌باشد. سازمان ملل متحد به‌عنوان مرکز تصمیم‌گیری جهانی در امور مهم و تأثیرگذار بر روابط بین‌الملل برای نخستین بار در سال ۱۹۹۸ توجه خود را معطوف به امنیت در فضای سایبر کرد. در این سال روسیه پیش‌نویس قطعنامه‌ای را درباره فناوری ارتباطات تلفنی و اطلاعاتی[1] به سازمان ملل متحد ارائه داد که مورد مخالفت آمریکا واقع شد. تا اینکه در سال ۲۰۱۰ پدیده‌های استاکس‌نت و ویکی لیکس در صدر اخبار جهانی قرار گرفت و وقایع مهمی در اتاق جلسه کوچکی در سازمان ملل رخ داد؛ آمریکا موضع سیاسی طولانی مدتش را تغییر داد و برای نخستین بار به‌طور مشترک پیش‌نویس قطعنامه‌ای را درباره فناوری ارتباطات تلفنی و اطلاعاتی در زمینه امنیت بین‌الملل (که امروزه به‌صورت کوتاه امنیت سایبری خوانده می‌شود) به عهده گرفت. و در همین راستا در اوایل سال ۲۰۱۰، در سازمان ملل متحد گروهی از متخصصان دولتی از جمله دیپلمات‌هایی از آمریکا، روسیه و چین در گزارشی که در ماه جولای آن سال منتشر شد به‌طور 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 در رابطه با جرایم سایبری همانند قطعنامه شماره ۵۵/۳۳ که در هشتمین نشست مجمع درباره جلوگیری از جرایم و تهدید مهاجمان[2] در سال ۱۹۹۰ تصویب شد، صادر شده بود. اما آنچه آن را در سال ۱۹۹۸ در صدر قرار داد 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) نظامنامه بین‌المللی نظارت بر امنیت بین‌المللی[3] را در ۱۴ سپتامبر ۲۰۱۱ پیشنهاد کردند تا در مجمع عمومی سازمان ملل

1. Information and Telecommunication Technology
2. Prevention of Crime and the Treatment of Offenders
3. International Code of Conduct for Information Security

متحد بررسی شود. علاوه‌بر این، روسیه ایده‌ای برای گردهمایی درباره امنیت بین‌المللی اطلاعات را تنها یک هفته بعد از آن منتشر ساخت.

در سازمان ملل متحد دو جریان اصلی را در ارتباط با امنیت در فضای سایبری می‌توان از یکدیگر تمییز داد: جریان نظامی ـ سیاسی[1] که بر جنگ سایبری متمرکز است و جریان اقتصادی[2] که بر بزهکاری سایبری[3] متمرکز است. هر دو این روندها نشان‌دهنده این موضوع است که معیارهایی در حوزه سایبر در حال ظهور هستند.

در جریان سیاسی ـ نظامی می‌توان سه دوره تاریخی مهم را مورد شناسایی قرار داد:

دوره اول از سال ۱۹۹۸ تا ۲۰۰۴ که دوره اقدامات اولیه در جهت ایجاد هنجارهایی برای فضای سایبر است. در این دوره همان‌طورکه پیش از این بیان شد روسیه پیش‌نویس قطعنامه‌ای را در حوزه امنیت در فضای سایبر پیشنهاد کرد که در ابتدا بدون رأی‌گیری در مجمع عمومی پذیرفته شد اما کشورهای اروپایی و آمریکا در نهایت با آن با این استدلال که مغایر با آزادی اطلاعات است مخالفت نمودند.

دوره دوم از سال ۲۰۰۵ تا ۲۰۰۸که دوره بازگشت به عقب است[4]. در سال ۲۰۰۵ پیش‌نویس ارائه شده برای رأی‌گیری به مجمع عمومی آورده شد که در جلسه رأی‌گیری در ۲۸ اکتبر مورد مخالفت آمریکا واقع شد و این قطعنامه تصویب نشد. این تصمیم مانع از آن شد که یک اجماع جهانی در حوزه فضای سایبر شکل گیرد.

دوره سوم از سال ۲۰۰۹ تا ۲۰۱۲ که دوره حرکت دوباره به سمت جلو[5] است و از اکتبر ۲۰۰۹ یعنی سالی که دوره ریاست جمهوری جورج دبلیو بوش تمام و دوره باراک اوباما آغاز شد، سعی کرد در سیاست‌های دوره بوش در ارتباط با روسیه و سازمان ملل متحد تجدیدنظر کند. همین موضوع باعث همراهی آمریکا با روسیه در تصویب قطعنامه‌ای درباره امنیت در فضای سایبر شد (Maurer, 2011: 1-23).

---

1. Politico- military Stream
2. Economic Stream
3. Cyber - crime
4. Stepping Backward
5. Forward Again

جریان اقتصادی نیز سال ۲۰۰۰ در سازمان ملل متحد شکل گرفت که این موضوع تحت عنوان «مبارزه با سوءاستفاده از فناوری‌های اطلاعاتی» توسط آمریکا و ۳۸ کشور دیگر همچون روسیه، فرانسه، رژیم صهیونیستی و انگلیس مطرح شد که بعداً نیز ۱۹ کشور دیگر به آن ملحق شدند. 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).

۲-۳. حملات سایبری: حمله مسلحانه یا توسل به زور

جهت شناسایی عملی به‌عنوان یک تهاجم خصمانه چهار معیار را می‌توان مورد شناسایی قرار داد: اول اینکه طبق بند «۲» ماده (۴) منشور ملل متحد «همه اعضای سازمان ملل متحد در روابطشان از تهدید یا استفاده از زور علیه تمامیت ارضی یا استقلال سیاسی هر دولتی، یا در هر روشی مغایر با اهداف سازمان ملل متحد خودداری خواهد کرد». سؤال این است که چه محدوده عملیات‌های سایبری می‌تواند به‌عنوان «زور» در داخل این ممنوعیت قرار گیرد. در غیاب یک تعریف معاهده‌ای «مفهوم زور» باید در تطابق با اهداف منشور تعریف شود. اگرچه معنی «زور» به قدری گسترده است که منازعات مسلحانه و غیرمسلحانه را شامل شود، اما اکثریت قاطع مفسران امروزه واژه «زور» در بند «۲» ماده (۴) منشور ملل متحد را مترادف با «اقدام مسلحانه» یا «به‌کارگیری نیروی نظامی» در نظر می‌گیرند. اما این امر به این مفهوم نیست که ممانعت از به‌کارگیری زور بین دولتی محدود به جلوگیری از کاربرد تسلیحات شیمیایی، بیولوژیکی یا هسته‌ای شده است. مطابق با نظر مشورتی دیوان بین‌المللی دادگستری درباره قانونی بودن تهدید یا استفاده از تسلیحات هسته‌ای، دیوان توضیح داده است که ممانعت «به هرنوع استفاده از زور بدون توجه به تسلیحات به‌کار گرفته شده» می‌باشد. در واقع جای تردید نیست که عملیات‌های سایبری نیز قابل تطبیق با سلاح‌های دیگر هستند. این موضوع به‌طورحتم شامل استفاده از عملیات‌های سایبری به‌عنوان یک ابزار دفاعی یا تهاجمی طراحی شده که باعث کشته شدن یا صدمه به افراد یا تخریب اهداف و زیرساخت‌ها، بدون توجه به اینکه چنین تخریبی شامل خسارات فیزیکی، صدمات کارکردی، یا ترکیب هر دو باشد، می‌شود.

در حالی که حملات سایبری بستگی به قابلیت دسترسی به جنگ افزارهای فیزیکی سنتی[1]، بیولوژیکی، شیمیایی یا هسته‌ای ندارند، اما در عین حال آنها نمی‌توانند بدون زیرساخت‌های لازم برای فضای سایبر انجام شوند، اینجاست که این سؤال پیش می‌آید که آیا اینها «جنگ‌افزار نظامی» محسوب می‌شوند؟ از این منظر این نکته قابل ذکر است که گزینش ابزار یا استفاده معمولی نیست که یک وسیله را تبدیل به تسلیحات می‌کند بلکه هدفی که آن وسیله برای آن به‌کار رفته و تأثیر آن است که این کار را انجام می‌دهد. بنابراین استفاده از هر طرح ترفندی، یا تعدادی ترفند که منجر به از دست رفتن زندگی تعداد قابل ملاحظه‌ای افراد شده یا باعث تخریب دارایی شود باید واجد شرایط حمله مسلحانه در نظر گرفت که عملیات‌های سایبری ظرفیت کیفی برای نامیدن به‌عنوان حمله مسلحانه در چارچوب ماده (۵۱) منشور ملل متحد را دارد.

طبق ماده (۵۱) منشور ملل متحد، «هیچ چیزی در منشور حاضر حق ذاتی خودیاری جمعی یا فردی را درصورتی که حمله مسلحانه‌ای علیه یکی از اعضای سازمان ملل اتفاق بیفتد را تضعیف نخواهد کرد». با توجه به این موضوع شکافی میان بند «۲» ماده (۴) که استفاده از زور است و ماده (۵۱) به‌وجود می‌آید. در واقع محدوده بند «۲» ماده (۴) گسترده‌تر از ماده (۵۱) است چراکه نه تنها حالت‌های مسلحانه بلکه همچنین حالت‌های غیرمستقیم و غیرمسلحانه زور را نیز مانع می‌شود و نه تنها استفاده واقعی بلکه صرف تهدید به زور را نیز شامل می‌شود.

واژه جنگ سایبر بیشتر مفهوم بین دولتی دارد. بند «۲» ماده (۴) منشور ملل متحد تنها دولت‌ها را خطاب قرار داده و آنها را از توسل به زور باز می‌دارد. این امر به این معنی است که استفاده یا تهدید به زور باید منتسب به دولت‌ها باشد. در حقوق بین‌الملل اعمال زمانی قابل انتساب به دولت‌ها هستند که توسط یک شخص یا هویت‌هایی به نمایندگی از دولت‌ها، یا با اجازه یا تأیید دولت به‌گونه‌ای که مسئولیت قانونی بین‌المللی برای رفتارهای او را بپذیرد. 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 غیردولتی و هکرها ممکن است مربوط به حقوق بین‌الملل بشردوستانه یا حقوق جرایم بین‌المللی باشد. مفهوم حملات سایبری در واقع عملیات‌های مربوط به بازیگران دولتی و غیردولتی را شامل می‌شود.

1. Traditional KineticWeaponry

معیار دوم برای تعیین اینکه آیا حملات سایبری یک حمله مسلحانه می‌باشند توجه به دیدگاه مختل‌کنندگی به جای تخریب‌کنندگی[1] است که از این نظر نتایج بخش وسیعی از حملات سایبری همانند آنچه در گرجستان یا استونی رخ داد، آن را ناخوشایند نموده و همین امر آن را همسنگ تخریب فیزیکی کرده است.

معیار سوم که می‌تواند مفید باشد «میزان و تأثیرات[2]» برای برآورد خسارات به زیرساخت‌های حیاتی است. حال باید دید زیرساخت‌های حیاتی چیست. مجمع عمومی سازمان ملل متحد آن را این‌گونه تعریف می‌کند: «زیرساخت‌های حیاتی شامل آنهایی است که برای تولید، حمل‌ونقل و توزیع انرژی، حمل‌ونقل هوایی و دریایی، خدمات بانکی و مالی، تجارت الکترونیک، تهیه آب، توزیع غذا و بهداشت عمومی و زیرساخت‌های اطلاعاتی مهم که به‌طور فزاینده‌ای فعالیت‌های آنها را متأثر و به هم مرتبط کرده است، می‌باشد». سازمان همکاری شانگهای نیز زیرساخت‌های حیاتی را شامل تسهیلات عمومی، سیستم‌ها و مؤسساتی که حمله به آنها ممکن است به‌طور مستقیم امنیت ملی را به خطر بیندازد حال چه به لحاظ فردی، اجتماعی یا دولتی تعریف می‌کند (Melzer, 2011: 10-14).

چهارمین و آخرین معیار نیز آزمایش شش مرحله‌ای پروفسور میشائیل اشمیت[3] برای بررسی اینکه آیا حملات سایبری از نظر حقوق بشردوستانه بین‌المللی یک حمله مسلحانه محسوب می‌شوند عبارت است از:

۱. شدت:[4] حملات مسلحانه تهدید به آسیب، مرگ، خسارت یا تخریب بیشتر نسبت به اجبار سیاسی یا اقتصادی است.

۲. فوریت یا بی‌واسطگی:[5] نتایج منفی حملات مسلحانه نسبت به اجبار سیاسی یا اقتصادی سریع‌تر هستند.

۳. مستقیم یا صراحت:[6] نتایج حمله مسلحانه نسبت به اجبار اقتصادی یا سیاسی بیشتر وابسته به حمله است.

---

1. Disruptive, Rather Than Destructive
2. Scale and Effects
3. Michael Schmitt
4. Severity
5. Immediacy
6. Directness

٤. مداخله‌آمیز بودن:[1] در حمله مسلحانه، ضرر و زیان معمولاً در داخل مرزهای کشور هدف می‌باشد اما در جنگ اقتصادی عموماً خارج از مرزهای هدف می‌باشد.

۵. قابلیت اندازه‌گیری:[2] نتایج حمله مسلحانه نسبت به اقتصادی یا سیاسی، راحت‌تر قابل اندازه‌گیری است.

٦. مشروعیت احتمالی:[3] کاربرد خشونت عموماً غیرقانونی فرض می‌شود در حالی که اجبار اقتصادی یا سیاسی به‌صورت قانونی تصور می‌شود (Richardson, 2011: 18-19).

حملات سایبری که باعث خسارات فیزیکی[4] یا صدمه یا مرگ افراد شوند مخصوصاً در داخل دایره تعریف حقوق بین‌الملل بشردوستانه قرار می‌گیرند. به هرحال، هنوز کاملاً مشخص نیست که آیا حمله سایبری که منجر به وارد آمدن آسیب به مردم یا خسارت به اجسام نشود در داخل محدوده حقوق بین‌الملل بشردوستانه قرار می‌گیرد یا نه (Richardson, 2011: 26).

برای درک نقش حملات سایبری در جنگ، باید همان سؤال‌هایی را که از تسلیحات دیگر داریم یعنی دامنه، نابودکنندگی، هزینه، تأثیر و کاربردهای سیاسی را نیز از آنها داشته باشیم. حملات سایبری قابلیت‌های استراتژیکی و تاکتیکی دارند. می‌توانند علیه نیروهای استقراریافته یا علیه اهداف استراتژیک در عمق سرزمین دشمن استفاده شوند. دامنه آن نامحدود است و می‌تواند تا هرجا که شبکه جهانی گسترده شده استفاده شود. اگرچه پیش‌زمینه‌های آماده‌سازی برای حمله سایبری زمان‌بر است اما سرعت حمله بدون توجه به مسافت می‌تواند در ثانیه اتفاق بیفتد (کوتاه‌ترین زمان ممکن) که هزینه‌های آن نیز بسیار پایین است.

به هرحال جنگ سایبری نقص‌هایی دارد. ما هنوز توانایی نداریم تا آسیب‌های ناشی از حملات سایبری را برآورد کنیم. به‌خصوص زمانی که اهداف تاکتیکی (مثل نیروهای نظامی) تبدیل به اهداف استراتژیک (مثل زیرساخت‌های غیرنظامی یا شهری) می‌شود. برای حملاتی به‌منظور ناتوان‌سازی شبکه‌ها ممکن است خسارات غیرقابل پیش‌بینی بر طرف‌های غیردرگیر، بی‌طرف یا حتی خود حمله‌کننده وارد آید. این موضوع می‌تواند خطرات سیاسی

1. Intrusiveness
2. Measurability
3. Presumptive Legitimacy
4. Kinetic Damage

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 قابل درک باشد البته به‌عنوان بخشی از نبرد بزرگ‌تر، اما ضربه سایبری به تنهایی فقط می‌تواند به‌عنوان هشدار یا برانگیختن دشمن عمل کند و در نتیجه نمی‌تواند به مانند سلاح‌های هسته‌ای یا سنتی کارایی داشته باشد. کارایی حملات سایبری بیشتر بستگی به سرعت عمل و غافلگیری دارد (Lewis, 2010: 1-3).

جمع‌آوری اطلاعات و ایجاد اختلال همیشه مهمترین ابزارهای جنگ بوده‌اند. اختلال در شبکه‌های ارتباطی حریف ممکن است حتی ارزش استراتژیک بیشتری نسبت به تخریب انبار مهمات یا خطوط پشتیبانی داشته باشد. در واقع، برخی روش‌های جنگ اطلاعاتی به قدری ناخوشایند هستند که با حقوق جنگ جلوگیری نمی‌شوند. هرچند حمله سایبری همچون حملات فیزیکی یا جنبشی شبیه شکل‌های سنتی جنگ نمی‌باشد، اما حمله سایبری نیز ممکن است حتی منجر به تخریب فیزیکی یا حتی مرگ شود. برای مثال حمله سایبری به یک توربین سد در در روسیه در سال ۲۰۰۷ آن را دچار خودانفجاری نمود، تولید برق را مختل کرد، سیل در منطقه به‌وجود آورد و ۲۰ نفر نیز کشته شدند. بنابراین، به‌خاطر این نتایج احتمالی، حمله سایبری می‌تواند یک منازعه مسلحانه را بنیان نهد.

۳-۳. جنگ سایبر و حقوق بین‌الملل بشردوستانه

جنگ سایبری باتوجه به تأثیرات و خساراتی که به جا می‌گذارد شایسته بررسی به‌عنوان یک جنگ مسلحانه است، لذا باید تطبیق‌پذیری آن با حقوق منازعات مسلحانه مورد ارزیابی قرار گیرد. تا اینجا هیچ اجماع بین‌المللی درباره کاربرد حقوق منازعات مسلحانه برای جنگ سایبری در قرن ۲۱ وجود ندارد، این مشکل ناشی از عدم تعریف جنگ سایبر به‌صورت رسمی و نیز فقدان سابقه‌ای است که راهنمای حقوق جنگ در حال حاضر و زمان آینده باشد. چالش دیگر این است که برخلاف دیگر ابزارهای جنگ در قرن ۲۱، جنگ سایبر در دوره‌ای ظهور یافته که نظم دولتی وستفالیایی در حال تغییر شکل و تحول به نوعی دیگر می‌باشد.

حقوق بین‌الملل بشردوستانه که گاهی اوقات به‌عنوان حقوق منازعات مسلحانه نیز توصیف می‌شود، زمانی کاربرد دارد که خشونت میان طرفین افزایش یابد اگرچه هیچ معاهده

و یا دستورالعملی کاربرد حقوق منازعات مسلحانه برای جنگ سایبر را به‌طور رسمی و قانونی اعلام نکرده و در هیچ معاهده‌ای نیز پیش‌بینی نشده اما این امر دلیل نمی‌شود که ما نتوانیم حقوق جنگ سایبر را در چارچوب حقوق منازعات مسلحانه قرار دهیم. هرچند در زمان تدوین اصول حقوقی منازعات مسلحانه استفاده از فضای سایبر مطرح نبوده و جنگ سایبری به‌عنوان یک ابزار جنگی شناسایی نشده است اما قواعد حقوق بین‌الملل بشردوستانه بسیار فراتر از آن هستند که محدود به زمان و مکان تلقی شوند، دیدگاهی که در سال ۱۹۶۳ نیز دیوان آن را تأیید کرد. حقوق بشردوستانه باید بر تمامی ابزارهای جنگی و به‌ویژه بر سلاح‌های دارای آثار غیرقابل کنترل قابل اعمال باشد. در سال ۱۹۶۳، دادگاه شهر توکیو اصول و قواعد حقوق جنگی لازم‌الاجرا در زمان جنگ جهانی دوم را بر کاربردهای بمب اتمی در هیروشیما و ناکازاکی که بعدها به‌عنوان یک وسیله جدید جنگی مورد پذیرش قرار گرفت، اعمال کرد. دیوان این دیدگاه را تأیید کرد که در واقع سلاح‌های هسته‌ای متعاقب آنکه بسیاری از اصول و قواعد حقوق بشردوستانه قابل اعمال در درگیری‌های مسلحانه که قبلاً موجودیت یافته بودند اختراع شد (بند «۸۶» رأی مشورتی ۱۹۹۶ دیوان) اما از این نمی‌توان نتیجه گرفت که اصول و قواعد مسلم حقوق بشردوستانه قابل اعمال در درگیری‌های مسلحانه بر سلاح‌های هسته‌ای اعمال نمی‌شوند. این نتیجه‌گیری با وصف بشردوستانه نهفته در اصول حقوقی مورد بحث که کل حقوق درگیری‌های مسلحانه را تحت پوشش قرار می‌دهد و نسبت به تمامی اشکال جنگی و تمام انواع سلاح‌های اعم از سلاح‌های گذشته، حال و آینده اعمال می‌شود، مغایرت دارد (ساعد، ۱۳۷۸: ۹۱-۹۰). بنابراین، از این نظر می‌توان استنباط کرد قواعد حقوق بین‌الملل بشردوستانه به‌عنوان بخشی از قواعد حقوق منازعات مسلحانه قابلیت اعمال در حوزه جنگ سایبر را دارا می‌باشد.

٤-٣. پیشینه حقوق بین‌الملل بشردوستانه

حقوق بین‌الملل بشردوستانه شاخه‌ای از حقوق بین‌الملل عمومی است که «تلاش می‌کند تا رفتار منازعه مسلحانه را تعدیل کرده و رنج ناشی از آن را تسکین دهد. آن، یکی از دو تقسیم اصلی حقوق جنگ است و تحت عنوان «حقوق در جنگ» و دیگری «حقوق برای جنگ[1]»

1. Law to War

معروف شده است، که منطق به‌کارگیری نیروی نظامی را جاری می‌کند. اصطلاحات «حقوق جنگ» و «حقوق منازعه مسلحانه» مترادف‌های آنها هستند (Swanson, 2010: 312).

حقوق منازعات مسلحانه آن‌گونه که امروزه وجود دارد در اواسط قرن نوزدهم پدیدار شده است، زمانی که حقوق بشردوستانه جنگ و خشونت تدوین شده است. اصول، معیارها و هنجارهایی که امروزه راهنمای حقوق منازعات مسلحانه هستند می‌توانند در منابع مختلفی همچون حقوق عرفی، معاهدات بین‌المللی، تصمیمات قضایی، نظریه‌های حقوقی و مقررات جنگی یافت شوند. اگرچه عرف‌های مربوط به حقوق منازعات مسلحانه را می‌توان در اروپای قرون وسطی در قرن پانزدهم ردیابی کرد اما ریشه‌های مدرن‌تر آن به جنگ‌های شهری ۱۸۶۱ تا ۱۸۶۵ آمریکا می‌رسد. قانونمند کردن جنگ و خشونت تحت اصول بشردوستانه در سال ۱۸۶۳ با ایجاد کمیته بین‌المللی صلیب سرخ به‌وجود آمد. طی جنگ ۱۸۷۶ تا ۱۸۷۸ عثمانی - روسیه امپراطوری عثمانی هلال احمر را ایجاد کرد. کمیته بین‌المللی صلیب سرخ به‌عنوان حافظ و ارتقادهنده حقوق بین‌الملل بشردوستانه عمل نمود. کنوانسیون اول ژنو در سال ۱۸۶۳ نیز اهداف و اصول صلیب سرخ را دنبال کرد (Hughes, 2010: 2).

اما حقوق بشردوستانه به‌عنوان بخشی از حقوق قابل اعمال بر درگیری‌های مسلحانه، مجموعه‌ای متشکل از حقوق لاهه، ژنو و نیویورک است. با اینکه ابتدا حقوق مربوط به انجام مخاصمات (موسوم به حقوق لاهه) در یک سلسله از معاهدات در سال‌های ۱۸۹۹ و ۱۹۰۷ پیش‌بینی شد، حقوق حمایت از قربانیان (موسوم به حقوق ژنو) به‌صورت مستقل و مجزا در کنوانسیون‌های متعدد ژنو تکوین یافت و اینکه این دو شاخه بعدها در چارچوب پروتکل‌های الحاقی ۱۹۷۷ به همدیگر پیوند یافته تا یک مجموعه حقوقی واحد را تشکیل دهند. حقوق ژنو مبتنی‌بر چهار کنوانسیون ۱۹۴۹ ژنو و دو پروتکل الحاقی ۱۹۷۷ است. در کنار این دو مجموعه حقوقی، حقوق نیویورک یعنی قواعد حمایتی برگرفته از تصمیمات ملل متحد را نیز باید در نظر داشت. در هرحال این سه مجموعه به ظاهر مجزا، مجموعه همگونی به نام حقوق بشردوستانه را تشکیل می‌دهند که اساسی‌ترین هدف آن پیگیری انسانی کردن درگیری‌های مسلحانه است. به‌گونه‌ای که اولویت بشردوستی در عنوان این حقوق نیز به خوبی متجلی است. در واقع اساس شکل‌گیری حقوق بشردوستانه، محدود کردن آزادی عمل دولت‌های حاکم و درگیر در جهت انسانی کردن مخاصمات است (ساعد، ۱۳۷۸: ۷۹-۷۸).

٤. کاربرد قواعد حقوق بشردوستانه در جنگ سایبری

حقوق مخاصمات مسلحانه، به‌عنوان بخشی از حقوق بین‌الملل، تنها محدود به دولت‌هاست. با این حال تخلف ممکن است همچنین پیگیری افراد برای جنایات جنگی را در برگیرد. بعضی معتقدند که حقوق بین‌الملل بشردوستانه نمی‌تواند به حملات سایبر حاکم باشد چون هیچ عمل حاکی از تحرک یا جنبشی و فیزیکی در چنین عملیاتی وجود ندارد. به عبارت دیگر، حملات شبکه‌ای رایانه منازعه مسلحانه نیست و بنابراین خارج از محدوده حقوق بین‌الملل بشردوستانه قرار می‌گیرد. ماده (۲)، که برای هر چهار کنوانسیون ژنو عمومی است، تصریح می‌کند که علاوه‌بر ملزوماتی که در زمان صلح به‌کار می‌رود کنوانسیون فعلی، باید برای همه انواع جنگ اعلام شده یا هر نوع منازعه مسلحانه دیگری که ممکن است بین دو طرف یا تعداد بیشتری طرف قراردادهای، حتی اگر اعلام جنگ توسط یکی از آنها تشخیص داده نشده باشد، به‌کار رود. پروتکل الحاقی یکم همچنین به همان واژه «منازعه مسلحانه» تأکید می‌کند. بند «۱» ماده (۳) پروتکل الحاقی یکم بیان می‌کند که «این پروتکل که کنوانسیون ۱۹۴۹ ژنو برای حمایت از قربانیان جنگی را تکمیل می‌کند در شرایطی که به ماده (۲) آن کنوانسیون ارجاع دهد کاربرد دارد». بنابراین، برای حاکم شدن حقوق بین‌الملل بشردوستانه به فضای سایبر، چنین حمله‌ای در حقیقت باید یک منازعه مسلحانه ایجاد کند. با این وجود، مفاد مطروحه در کنوانسیون ژنو و پروتکل‌های الحاقی بعدی اعلام کرده‌اند که منازعه مسلحانه می‌تواند در شیوه عادلانه گسترده‌ای نگریسته شود. منازعه مسلحانه به‌عنوان «هر اختلاف به‌وجود آمده بین کشورها و منتهی به مداخله نیروهای مسلح» تعریف شده است. به هرحال، منازعه‌ای که منتهی به درگیری نیروهای نظامی شود نمی‌تواند تنها ملاک باشد برای مثال، جایگزینی پلیس مرزی با سربازان یا حمله ناگهانی مرزی به‌وسیله افراد به نیروهای نظامی منازعه مسلحانه نمی‌باشد. بنابراین، زمانی که اصول حقوق بین‌الملل بشردوستانه مطرح می‌شود. درجه‌ای از شدت و تداوم نیز باید مدنظر باشد. حقوق بین‌الملل بشردوستانه برمبنای ایده قربانیان منازعات مسلحانه بنیان نهاده شده و از مصدومان این منازعات حمایت می‌کند. این حمایت معمولاً برحسب صدمه، مرگ، مالکیت، آسیب یا تخریب چارچوب‌بندی شده است. بنابراین اصول اساسی حقوق بین‌الملل بشردوستانه تصریح می‌کند که منازعات مسلحانه وقتی اتفاق می‌افتد که یک گروه اقداماتی انجام دهد که سبب صدمه کشتار، آسیب یا تخریب شود.

با توجه به مباحث فوق، منطقی است که حملات سایبری ممکن است منازعه مسلحانه

تلقی شود حتی اگرچه استفاده از رایانه به‌عنوان اسلحه فیزیکی یا سنتی جنگ نیست. درحالی که حملات سایبری، فناوری جدیدی را به‌کار گرفته که طی پیش‌نویس کنوانسیون ژنو به ذهن خطور نکرده اما ماده (۳۶) این کنوانسیون نشان می‌دهد که نویسندگان قواعدی برای پیشرفت‌های جدید در شیوه‌های جنگ پیش‌بینی کرده‌اند. در حقیقت، حقوق بین‌الملل بشردوستانه تغییر فناوریکی را پیش‌بینی می‌کند. برای مثال، مارتینز کلاوس[1]، ادعا می‌کند که حتی اگر موردی به‌طور صریح به‌وسیله توافقنامه‌ای پوشش داده نشده، شهروندان و رزمندگان تحت حمایت و صلاحیت اصول حقوق بین‌الملل ناشی از حقوق عرفی، اصول حقوق بشری و تحمیل‌های وجدان عمومی قرار می‌گیرند. به عبارت دیگر، حملات باید اساساً تا اندازه زیادی به‌وسیله تأثیرات آنها نه چگونگی اعمال آنها سنجیده شوند (Swanson, 2010: 313-314).

چهار اصل وجود دارد که باید در منازعات مسلحانه مدنظر قرار گیرند. علاوه‌بر اصل تمایز و تناسب، ضرورت نظامی[2] و جلوگیری از رنج غیرضروری[3] نیز می‌بایست مدنظر قرار گیرد.هر کدام از این اصول با دیگری مرتبط بوده و چارچوبی برای ارزیابی مطابقت با حقوق بین‌الملل بشردوستانه ایجاد می‌کند. تبعیض قائل شدن باعث می‌شود تا میان کسی که در حال نبرد بوده و کسیکه نمی‌باشد تمییز قائل شویم (Richardson, 2011: 22).

پروتکل اول الحاقی ۱۹۷۷ به کنوانسیون ژنو اصول تمایز را مشخص می‌کند؛ «اصطلاح فنی در حقوق منازعات مسلحانه با هدف حمایت اشخاص و اهداف غیرنظامی». تحت این اصول، طرفین درگیر در جنگ باید میان اهداف نظامی و غیرنظامی از یک طرف و اهداف نظامی و جنگی از طرف دیگر تمایز قائل شوند. دولت‌ها نباید هرگز تسلیحاتی را که قادر به تشخیص میان اهداف نظامی و غیرنظامی نیستند به‌کار برند.

برخی اهداف هم کاربرد نظامی و هم کاربرد غیرنظامی دارند. این اهداف به اصطلاح دارای کاربرد دوگانه، به‌کارگیری این اصول را پیچیده کرده است. این اهداف می‌تواند شامل ایستگاه‌های تولید برق، ارتباطات راه دور، پل‌ها و زیرساخت‌های غیرنظامی دیگر باشد که در زمان جنگ به‌وسیله گروه‌های نظامی استفاده شود. اگر هدف برای استفاده نظامی کارایی داشته و مفید باشد، این

1. Martens Clause
2. Military Necessity
3. Prevention of Unnecessary Suffering

«استفاده ثانویه» ممکن است آن را به هدف نظامی مشروع تبدیل نماید (Kelsey, 2008: 1436).

تحلیل مطابقت حملات سایبری با اصل تمایز بسیار شبیه به تحلیل برای حمله سنتی خواهد بود و در بسیاری از عملیات‌ها حمله سایبری به وضوح با این اصل همخوانی خواهد داشت. همانند طرح‌های توسعه نظامی برای حملات سایبری اتحادیه‌های نظامی و قانونی نیاز به تفسیر دوباره برای کاربرد مؤثر آن با فضای سایبر خواهد داشت. برخی نظامیان معتقدند، هرچیزی که برای حملات سنتی هدف مشروع بود، یک هدف نظامی مشروع برای حملات سایبری نیز محسوب می‌شود. همچنین، ممانعت‌های نسبی در حقوق بین‌الملل بشردوستانه بستگی به انواع تسلیحات یا جنگ استفاده شده نخواهد داشت و باید بدون شک برای جنگ سایبر نیز به‌کار رود. همچنین، برخی کاربردهای تسلیحات سایبری به وضوح تحت اصل تمایز قابل پذیرش می‌باشد، درحالی که این اصل به‌وضوح استفاده‌های دیگر را ممانعت می‌نماید.

براساس این اصل در برخی حملات می‌توان تسلیحات سایبری را برای اهداف صرفاً نظامی استفاده کرد. به نظر می‌رسد چنین کاربردی نقض اصل تمایز در حقوق بین‌الملل بشردوستانه نخواهد بود. برای مثال، حمله‌ای که به یک ایستگاه دفاع هوایی صورت می‌گیرد و آن را به‌عنوان بخشی از صحنه نبرد عمومی خنثی می‌کند و به این ایستگاه دفاع هوایی نیز به‌عنوان یک مزیت نظامی مشخصی نگریسته می‌شود.

در عملیات‌هایی که تهدیدات تلفات غیرنظامی بیشتری دارد، مثل حمله به سیستم رایانه‌ای یک هواپیمای مسافربری یا به شبکه دفاع هوایی، اصل تمایز احتمالاً نقش بزرگی در تعریف عملیات نظامی بازی خواهد کرد. حداقل، حقوق بین‌الملل بشردوستانه نیازمند فرماندهانی است که «بدانند نه فقط به کجا ضربه بزنند بلکه قادر باشند تا همه واکنش‌های یک حمله را پیش‌بینی نمایند». اگر اهداف و پیام‌های غلط به شبکه دفاع هوایی ارسال شده بتواند هواپیماهای امدادی یا تجاری را با خطر مواجه کند اصل تمایز، فرمانده را مجبور خواهد کرد تا ارزیابی کند که آیا چنین طرحی بهترین شیوه برای کسب مزیت نظامی مورد انتظار بوده است.

۵. جمع‌بندی و نتیجه‌گیری

حقوق بین‌الملل بشردوستانه حملات سایبری را که باعث کشتار و تخریب عمدی تأسیسات غیرنظامی‌شود را ممنوع می‌نماید. مثال‌هایی از آن شامل تخریب سیستم کنترل رفت و آمد هوایی

که باعث شود تا هواپیماهای مسافربری سقوط کنند، یا دستکاری بانک اطلاعات پزشکی که باعث شود غیرنظامیان و سربازان زخمی گروه خونی ناهمخوانی دریافت کنند. به عبارت بهتر اصول حقوق بین‌الملل بشردوستانه می‌تواند حاکم بر فضای عمومی جنگ سایبر باشد اما این روند نیازمند تدوین قوانین تخصصی‌تر و کارآمدتری می‌باشد تا بتواند در صحنه‌های جنگ نیز کارایی داشته باشد.

امروزه امنیت به شدت پیچیده و چندلایه شده است، در کنار فضای واقعی با دنیای جدید و گسترده به نام فضای مجازی مواجه هستیم. فضایی که در آن همه چیز مبهم و نامشخص است. ارتباطات، جنگ سایبری و الکترونیکی به شدت گسترش پیدا کرده است. موضوعات مختلف دولت‌ها از امور نظامی تا امور فرهنگی و اجتماعی همگی رایانه‌محور شده است. این امر سبب شده که رقبا برای افزایش توانمندی خود و نیز ضربه به دشمن در این فضا سرمایه‌گذاری کنند. فضایی که در آن معاهده حقوقی مشخص و جامعی که تمام جنبه‌های مختلف را دربرگیرد، به‌وجود نیامده است. حق و تکلیف دولت‌ها مبهم است. لزوماً دولت‌ها طرف درگیری نیستند بلکه گروه‌ها و سازمان‌های غیردولتی و حتی افراد می‌توانند در این فضا به امنیت ملی قدرتمندترین دولت‌ها صدمه وارد کنند و امنیت اقتصادی و انسانی آنها را با خطر مواجه کنند. برخی حملات سایبری می‌توانند به تلفات انسانی به غیرنظامیان منجر بشوند و جان عده زیادی را با خطر مواجه کنند و در اینجاست که می‌توان پیوند حقوق بین‌الملل بشردوستانه و جنگ سایبری را مشاهده کرد. امروزه بر هیچ کس پوشیده نیست که رقبا در سطح بین‌الملل در یک جنگ سایبری به سر می‌برند و به‌صورت دائم درصدد ضربه زدن به دیگری در این فضا هستند. تشکیل ارتش‌های سایبری گواه بر این امر است. در این شرایط اگر چنانچه حملات به‌گونه‌ای باشد که جان غیرنظامیان را در خطر قرار دهد، آنگاه دیگر نمی‌توان به این دلیل که هنوز معاهده‌ای برای نظم‌دهی به حقوق بشردوستانه مجازی شکل نگرفته است از بار مسئولیت شانه خالی کرد.

منابع و مآخذ

۱. دانشگاه امام حسین (ع) (۱۳۷۵). *هنرجنگ*، تهران.

۲. عبدالله‌خانی، علی (۱۳۸۶). *جنگ نرم ۳؛ نبرد در عصر اطلاعات*، تهران، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی معاصر.

۳. مسائلی، محمود و عالیه ارفعی (۱۳۷۱). *جنگ و صلح از دیدگاه حقوق و روابط بین‌الملل*، تهران، مؤسسه چاپ و انتشارات وزارت امورخارجه.

۴. موسی‌زاده، رضا و اکبر امینیان (۱۳۹۰). *جمهوری اسلامی ایران و دیوان کیفری بین‌المللی*، تهران، پژوهشکده تحقیقات راهبردی.

۵. نادر، ساعد (۱۳۷۸). *حقوق بشردوستانه و مسائل نوظهور* (جنگ‌های پسانوین)، تهران، خرسندی.

۶. نگاهی به فرماندهی سایبری آمریکا (۱۳۹۱/۴/۲۰)، www.grshreghnews.oam

7. Arquilla, John and David Ronfeldt (1993). "Cyberwar is Coming!", *Comparative Strategy*, Vol. 12, No. 2.

8. http://www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf

9. http://www.khabaronline.ir

10. Hughes, Rex (2010). "Towards a Global Regime for Cyber Warfare", Cyber Security Project, Chatham House, London.

11. Kelsey, Jeffrey T.G. (2008). "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", *Michigan Law Review*,Vol. 106.

12. Lewis, James A. (2010). "Thresholds for Cyberwar", Center for Strategic and International Studies, Available at: http://www.csis.org

13. Libicki, Martin C. (2009). *Cyberdeterrence and cyberwar*, RAND Corporation, Available: http://www.rand.org

14. Maurer, Tim (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.*

15. Melzer, Nils (2011). "Cyber warfare and International Law",The United Nations Institute for Disarmament Research, Availabale: www.unidir.org

16. Nye, Joseph S. Jr. (2010). "Cyber Power", Belfer Center for Science and International Affairs.

17. Ottis, Rain and Peeter Lorents (2010). "Cyberspace: Definition and Implications",

Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, available:

18. Richardson, John (2011). "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield". Available at SSRN: http://www.ssrn.com

19. Swanson, Lesley (2010). "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict",Loyola of Los Angeles International and Comparative Law Review,Vol. 32, Available at: http://digitalcommons.lmu.edu/ilr/vol32/iss2/5

20. www.mashreghnews.org, 1391