حملات سایبری از منظر قواعد و مقررات حقوق بین‌الملل و حقوق بشردوستانه

محمدرضا حسینی[۱]، علی حسینی [۲]

[۱] دانشجوی دکتری حقوق بین‌الملل و پژوهشگر دانشگاه عالی دفاع ملی

تهران، ایران

m.hosseini@sndu.ac.ir

[۲] دانشجوی دکتری حقوق خصوصی دانشگاه شهید مطهری

تهران، ایران

ali-hosseini.13@yahoo.com

چکیده

فضای سایبر پدیدهٔ شگفت‌انگیز قرن بیست و یکم است. ظهور عصر سایبر مفاهیم و مبانی متعددی از زندگی صنعتی را دستخوش تغییر و تحول نموده است و امروزه بعنوان «ابزار جنگی» مورد استفاده قرار می‌گیرد. تهاجم سایبر توانسته مفهوم نبرد کلاسیک را تغییر داده و به نوعی جایگزین ابزار و ادوات نظامی‌شود. لذا عرصه فناوری اطلاعات را باید به میدان جنگ تشبیه کرد که اعمال قواعد منع توسل به زور از یک سو و مشروعیت حملات سایبری در چارچوب حقوق بین‌المللی و حقوق مخاصمات مسلحانه از سوی دیگر باید مورد ارزیابی قرار گیرد. یکی از اهداف این تحقیق، پاسخگویی به سوالات زیر است که ممکن است در ذهن شکل می‌گیرد: بازیگران این میدان جنگ چه کسانی هستند و آیا اعمال آنها می‌تواند موجبات مسئولیت بین‌المللی دولت متبوعشان شود؟ آیا حملات سایبر به عنوان «حملات مسلحانه» تلقی می‌شوند؟ آیا می‌توان در مقابل یک حمله سایبری به اصل «دفاع از خود» توسل جست؟ دراین مقاله اولاً تلاش خواهد شد تهدیدات سایبری درچارچوب قوانین بین‌المللی موجود در دو شاخه «حقوق حاکم بر جنگ» و «حقوق حاکم در جنگ» مورد تجزیه و تحلیل قرار گیرد، و ثانیاً آثار آن را بر نقض سه اصل بنیادین مخاصمات مسلحانه بین‌المللی (تمایز، ضرورت و تناسب) را بررسی می‌نمائیم. نتایج این مقاله نشان می‌دهد فضای سایبر نیازمند هنجارسازی و چارچوب حقوقی مطلوب در قالب یک معاهده بین‌المللی می‌باشد.

کلمات کلیدی:

سایبری، حقوق بین‌الملل، حقوق بشردوستانه، اصول مخاصمات مسلحانه، معاهدات بین‌المللی.

۱- مقدمه

جنگ سایبری باعث برهم خوردن نقش سنتی قدرت درمحیط بین‌الملل گردیده است. دلیل این امر معکوس شدن ارتباط تناسب بین سطح پیشرفت تکنولوژیک یک کشور و درجه آسیب‌پذیری آن است. امروزه پیشرفت فناوریهای یک کشور بیشتر بر شبکه اینترنت متکی است، درنتیجه، بیشتر در معرض نفوذ و رسوخ به این شبکه‌ها است.

از زمان آغاز جوامع انسانی، بشر همیشه علاقه خاصی به ایجاد قواعدی داشته که بتواند روابط آنان را با یکدیگر تنظیم نماید. درقلمرو جهانی نیز حقوق بین‌الملل به آرامی درحال تحول است. یکی از چالش‌هایی که نظام حقوق بین‌الملل با آن دست به گریبان است، پیدایش پدیده‌های نوظهور در حوزه‌های فناوری بویژه فناوریهای با کاربردهای دوگانه مانند فضای مجازی و شبکه‌های ارتباطی است. دستیابی به هرگونه فناوری که احتمال می‌رود از آن بعنوان ابزار جنگی استفاده شود، بحث مشروعیت کاربرد آن تحت قوانین بین‌المللی مطرح می‌گردد؛ از جمله این ابزار، انجام عملیات‌های سایبری از سوی اشخاص حقیقی یا از طرف دولتها است که این خود مسائل حقوقی پیچیده‌ای را بدنبال دارد.

دراین مقاله ابتداء به قواعد منع توسل به زور در حقوق بین‌الملل پرداخته می‌شود و تلاش می‌گردد یک چارچوب قانونی معتبر برای بررسی مشروعیت جنگ سایبری ارائه گردد. و سپس تلاش خواهد شد عملیات تهاجم سایبری را تحت موجود ممنوعیت حقوق بین‌الملل طبقه‌بندی کرده و آن را با دو اصل مهم حقوقی محک بزنیم: (الف) توسل به زور؛ (ب) عمل تجاوز. در ادامه، ارتباط بین عملیات جنگ سایبر و مفهوم «دفاع از خود» بررسی خواهد شد که درقالب دو سوال به آن خواهیم پرداخت: (الف) آیا یک حمله اینترنتی حق قانونی «دفاع از خود» را مسلم می‌کند؟ (ب) می‌تواند یک حمله اینترنتی به عنوان ابزاری برای «دفاع از خود» صورت گیرد؟ در نهایت، عناصر لازم برای «قابلیت انتساب» بودن یک حمله اینترنتی به منظور احراز مسئولیت بین‌المللی دولت‌ها برای اعمال غیر قانونی در چارچوب قوانین بین‌المللی موجود کدامند؟

۲- مفاهیم و تعاریف

بررسی‌ها نشان می‌دهد هنوز یک تعریف جهانی پذیرفته شده برای اصطلاح جنگ سایبری و شبکه مبتنی بر حملات سایبری وجود ندارد، مجله اکونومیست «فضای مجازی» را به عنوان حوزه پنجم از قدرت، پس از زمین، دریا، هوا و فضا معرفی می‌کند.[۱] واژه «فضای مجازی» درسال ۱۹۸۱ توسط نویسنده داستانهای علمی تخیلی ویلیام گیبسون ارائه شد.[۲] وزارت دفاع ایالات متحده نیز «فضای مجازی» را بعنوان "یک دامنه جهانی در درون محیط اطلاعاتی متشکل از شبکه‌های وابسته از اطلاعات و زیرساخت های فن آوری، از جمله اینترنت، شبکه‌های ارتباطات راه دور، سیستم‌های کامپیوتری، و جاسازی شده پردازنده ها و کنترل کننده" تعریف می‌کند.[۳] در فرهنگ اصطلاحات نظامی، جنگ سایبری عبارت است از: "هرگونه عملیاتی که حریف را به انجام وادار فعل یا ترک فعلی نماید، در برابر ابزار کنترل فرآیندها و نفوذ در درون سیستم حریف".[۴]

در تعریف «جنگ»، کوینسی رایت (Quincy wright)[۵] به نقل از وردوس (Verdoss) «جنگ» را "جدلی مسلحانه بین دولتها می داند که درآن کلیه روابط صلح آمیز معلق شده باشد". مفهوم «حقوق جنگ» را می توان "مجموعه عملیات و اقدامات قهرآمیز مسلحانه" بر شمرد، همچنین جنگ به عنوان یکی از جلوه‌های بارز «توسل به زور» است.[۶] در نهایت، می‌توان گفت؛ حقوق جنگ شامل مجموعه اصول و قواعدی است که بر روابط میان کشورهای متخاصم با یکدیگر و یا میان کشورهای متخاصم با کشورهای بیطرف حاکم می‌باشد.

۳- سوالات تحقیق

۱) آیا تهدیدات سایبری یک حمله مسلحانه است و می‌توان از یک عملیات سایبری بعنوان ابزاری برای «حق دفاع از خود» توسل جست؟

۲) آیا قوانین انسان دوستانه بین المللی می تواند به عملیات سایبری اعمال می‌شود؟

۳) آیا حملات سایبری مسئولیت بین‌المللی دولتها را بدنبال دارد؟

۴) آیا قوانین و مقررات معاهدات بین‌المللی موجود پاسخگوی ابعاد مختلف تهاجم سایبری است؟

۴- انواع حملات سایبری

حملات سایبری می‌تواند دامنه گسترده‌ای داشته باشد. از تهاجم «نرم» گرفته مانند اختلال در شبکه‌های تلویزیونی و رادیوئی، پخش تبلیغات جهت آشفتگی بازارهای سهام و نظام بانکداری، سیستم مصرف و درنتیجه وحشت مردم. با این حال، حملات سایبری در مقیاس گسترده می‌تواند به تخریب جدی اموال و تلفات انسانی، تهدید امنیت ملی، هدف قرار دادن زیرساخت‌های 'حیاتی' منجر شود.

در اینجا نمونه‌هایی از حملات سایبری در سه بخش عمده طبقه‌بندی شده‌اند:

۱) هدف قرار دادن زیرساخت‌های ارتباطی، به عنوان مثال مسدود کردن و اختلال در خطوط شبکه تلفن، بستن و یا متوقف کردن سیگنال شبکه تلفن همراه، و یا حتی بستن تمام پهنای باند اینترنت کل کشور، در نتیجه محروم کردن مردم از دسترسی به اینترنت.

۲) هدف قرار دادن حمل و نقل؛ به عنوان مثال اخلال در ترافیک فرودگاه، سقوط هواپیماها بدلیل اختلال در هدایت برج‌های کنترل ترافیک هوایی، سیگنال‌های مختل کننده (GPS)، دسترسی به سیستم‌های کامپیوتری راه آهن و ایجاد انحراف در مسیر قطارها، و یا برهم زدن نظم چراغ‌های ترافیکی و ایجاد تصادفات جدی.

۳) هدف قرار دادن زیرساخت‌های حیاتی؛ مانند تامین آب، سدهای آبی، غذا، سیستم‌های توزیع، شبکه برق، نیروگاه‌های برق، سوخت و حتی با استفاده از انرژی هسته‌ای، سیستم‌های ایمنی گیاهان.

۵- طبقه‌بندی جنگ سایبری

بررسی ادبیات موجود در رابطه با طبقه‌بندی و قانونی بودن عملیات سایبری نشان می‌دهد که میزان مخالفت حقوقدانان بین‌المللی از دو موضوع اساسی ناشی می‌گردد: ۱) توسل به زور، ۲) عمل تجاوز. برای رفع این اختلاف نظر، در ابتدا به بررسی و تجزیه و تحلیل دکترین "منع توسل به زور" می‌پردازیم و مشخص می‌کنیم آیا حملات سایبری می‌تواند تابعی از اصل عدم توسل به زور باشد. پس از آن، با ارائه تعریفی از جرم بین‌المللی 'تجاوز'، از آن بعنوان مدلی برای یافتن زمینه‌های ممنوعیت توسل به حملات سایبری استفاده خواهیم کرد.

۵-۱- حملات سایبر به عنوان "توسل به زور"

سنگ بنای ممنوعیت از استفاده از زور در ماده (۲) (۴) از منشور سازمان ملل نهفته است که اعلام می‌دارد؛"کلیه اعضاء در بین‌المللی خود را روابط از تهدید یا توسل به زور علیه تمامیت ارضی و یا سیاسی استقلال هر کشور، و یا هر شیوه‌ای دیگر مغایر با اهداف سازمان ملل متحد خودداری کنند".[۷] ممنوعیت تهدید یا توسل به زور نه تنها در قواعد قراردادی بعنوان قاعده الزام آور شناخته می‌شود، بلکه طبق قوانین عرفی توسط دیوان بین‌المللی دادگستری (ICJ) جزو قواعد آمرانه بشمار می‌رود.[۸] تنها استثناء وارده بر آن اجازه صریح شورای امنیت سازمان ملل متحد است که در مفهوم «دفاع از خود» تجلی می‌یابد.

بحث‌های حقوقی میان تدوین کنندگان در هنگام تهیه پیش‌نویس منشور بر این موضوع متمرکز شد که عبارت "توسل به زور" فقط در مفهوم خاص آن، بعنوان منع "تهدید به زور"،' حمله مسلحانه 'یا "عمل تجاوز" است. اما این اصطلاح موجب بروز تفاسیر گوناگون گردید. برای مثال آیا تحریم اقتصادی تشکیل دهنده عنصر "توسل به زور' است؟ آیا "توسل به زور» تنها توسط قوای مسلح می‌تواند اعمال گردد؟ و آیا حملات سایبری در داخل این آستانه قرار می‌گیرد؟

به منظورپیدا کردن پاسخ به سوالات فوق، مراجعه به اسناد بین‌المللی مانند اعلامیه سال ۱۹۷۰ در مورد «اصول روابط دوستانه حقوق بین‌الملل»[۹] و اعلامیه سال ۱۹۸۷ درباره ارتقای «اثربخشی اصل خودداری از تهدید یا توسل به زور در روابط بین‌المللی»[۱۰] می‌تواند مفید باشد.

«بناتار» استدلال می‌کند که براساس کنوانسیون ۱۹۶۹ حقوق معاهدات می‌توان ماده ۲ (۴) را طوری تفسیرکرد که شامل نیروی سایبری گردد.[۱۱] وی با انجام تفسیر مضیق ماده۲ (۴)، نتیجه‌گیری کرد که توسل به زور بمنزله کاربرد زور درماهیت مسلح بودن آن است. اما از سوی دیگر، تفسیر موسعی توسط برانلی انجام شد، که به (رویکرد نتیجه‌گرا) معروف است. رویکرد نتیجه‌گرا، توسط اکثریت از دانشمندان حقوق سایبری مورد پذیرش قرار گرفته است.

طرفداران این رویکرد معتقدند بایستی یک مبنای حقوقی جدیدی برای یکسان‌سازی توسل به زور ایجاد کرد.

با این حال، نقص ذاتی رویکرد نتیجه‌گرا این است که مبتنی بر خسارات فیزیکی (بدنی) است لیکن اغلب حملات سایبری مستقیماً باعث تلفات انسانی نمی‌شود. حتی محدود کردن پهنای باند در سطح یک کشور و یا بستن ارتباط آن با جهان خارج، بلافاصله سبب مرگ و میر انسان نمی‌شود.

«مایکل اشمیت» با استفاده از هفت معیار زیر را بعنوان شاخصی که جامعه بین‌المللی باید آن را به مثابه یک تهاجمی که مقارن با توسل به زور است در نظر بگیرد: **فوریت، مستقیم بودن، تهاجمی بودن، اضرار، قابلیت اندازه‌گیری، مشروعیت و مسئولیت**. [۱۲] اما، مشکل با این رویکرد این است که همه عوامل فوق‌الذکر، عناصری که ذهنی هستند و بصورت عینی قابل اندازه‌گیری نیست.

۵-۲- حملات سایبر به عنوان «عمل تجاوز»:

تعاریف مندرج در چارچوب ماده۲ (۴) را نمی‌توان برای طبقه‌بندی حملات سایبری استفاده کرد. حملات سایبر دولت به دولت، در قالب «عمل تجاوز» تجزیه و تحلیل خواهد شد. از یکسو، می‌توان حمله سایبری را بعنوان چهارمین جرم بین‌المللی درنظر گرفت و دیوان کیفری بین‌المللی (ICC) را برای رسیدگی به آن صالح دانست، و جرایم فردی را به سران دولتها تعمیم داد، به شرطی که پیوندی میان حمله کننده با دولت متبوع بتوان برقرار کرد.[۱۳]

تاکنون، ادبیات حقوق بشردوستانه تعریف قابل قبولی را از «تجاوز» ارائه نکرده است اما در قطعنامه ۳۳۱۴ درسال ۱۹۷۴مجمع عمومی سازمان ملل متحد ابعاد آن روشن نماید. ماده ۸ مکرر، قطعنامه، جرم تجاوز را اینگونه تعریف می‌کند: «"جرم تجاوز" به معنای برنامه‌ریزی، آماده‌سازی، شروع به جرم و یا اجرای آن، توسط یک فرد در یک موقعیت به طور موثر به اعمال کنترل بر و یا مستقیم اقدام سیاسی یا نظامی یک دولت است». در این راستا، دیوان کیفری بین‌المللی (ICC) اخیراً در کنفرانس بررسی اساسنامه رم درکامپالا، موضوع تعریف تجاوز که تقریبا بازتعریف قطعنامه فوق‌الذکر بود را به تصویب رساند[۱۴].

در ماده ۴۳ پروتکل الحاقی به کنوانسیون ژنو۱۹۴۹ مقرر می‌کند که :"نیروهای مسلح طرفین یک درگیری که دارای سلاح، سازمان یافته، گروه‌های تشکیل شده و واحد که تحت یک فرمان آن طرف رفتار و یا آن عوامل تحت فرمان مسئولین عمل کنند".[۱۵]

قرار دادن حملات سایبری تحت جرم تجاوز، عبارت "قوای مسلح" را دچار ابهام می‌نماید، چراکه درجنگ سایبری استفاده از 'سلاح' در معنای سنتی آن موضوعیتی ندارد. از طرف دیگر، حقوق بین‌الملل تعریف دقیقی از سلاح ارائه نمی‌دهد. فرهنگ آکسفورد لغت تعریف سلاح به عنوان 'ابزار یا ابزاری که طراحی شده و یا استفاده می‌شود برای تحمیل آسیب به دشمن" تعریف نموده است. بر این اساس، جنگ سایبری قطعا در داخل محدوده این تعریف می‌افتد.

با این حال، از رویه دولتها درسطح جهان نشان می‌دهد اغلب آنها شروع به تشکیل نیروهای سایبری بعنوان شاخه جداگانه از این فناوری پیشرفته درسطح نیروهای مسلح کرده‌اند.[۱۶] بعنوان مثال، اخیراً در ایالات متحده قرارگاه فرماندهی سایبری ایالات متحده (USCYBERCOM) تحت تابعیت وزارت دفاع ایجاد گردید، همچنین در بریتانیا مرکز عملیات امنیت سایبر تحت کنترل دفتر هیات دولت راه‌اندازی شد[۱۷]. بنابراین، اگر محرز و مسلم شود که قرارگاه سایبری بخشی از نیروهای مسلح یک کشور است، قرار دادن حملات سایبر در داخل چارچوب قانونی «عمل تجاوز» مطروحه در بندهای (الف)، (ب)، (ج)، (د) و (ه) قطعنامه تعریف تجاوز بسیار آسان است. در نتیجه، عملیات جنگ سایبری به طور بالقوه می‌تواند در تعریف جرم تجاوز عنوان شده در ماده (۸) مکرر قرار گیرد.

۶- مفهوم «دفاع از خود» در مقابل حملات سایبری

تلاش برای ممنوعیت اعمال حملات سایبری به ثمر نشست و ذیل قاعده «منع توسل به زور» قرار گرفت، اما یکی از استثنائات قاعده عرفی عدم توسل به زور، «دفاع از خود» است که در این چارچوب انجام حملات سایبری مجاز شمرده می‌شود. تقابل میان عملیات‌های سایبری و توسل به اصل«دفاع از خود» مندرج در ماده ۵۱ منشور سازمان ملل، دو پرسش اساسی را مطرح می‌سازد. اول، آیا سطح حمله سایبری با سطح حمله مسلحانه مقارنت دارد؟، آیا می‌توان به موجب ماده ۵۱ منشور، حق «دفاع از خود» را می‌توان اعمال کرد؟

ماده ۵۱ از منشور مقرر می‌کند: "هیچ چیز در این منشور نمی‌تواند به حق فردی یا جمعی «دفاع از خود» درصورت حمله مسلحانه علیه یک عضو ملل متحد رخ دهد، تا زمانی که شورای امنیت اقدامات

لازم برای حفظ بین‌المللی صلح و امنیت انجام ندهد وارد سازد». لذا حمله مسلحانه شرط لازم برای اعمال حق «دفاع ازخود» است. با این وجود، ماده ۵۱ منشور، هیچ تعریف خاصی از مفهوم "حمله مسلحانه" تحت شرایط "حقوق حاکم بر جنگ" ارائه نمی‌کند. اما دیوان بین المللی دادگستری (ICJ) درقضیه نیکاراگوئه درسال ۱۹۸۶ اظهار داشت که اگر 'حمله مسلحانه' صورت گیرد، اعمال حق ذاتی «دفاع از خود»ـ حتی اگر در منشور ارائه نشده بود ـ مجاز و مشروع تلقی می‌شود.

با این توضیح، اگر پاراگراف (G) از ضمیمه ماده ۳ قطعنامه تعریف تجاوز ۳۳۱۴، منعکس کننده قوانین عرفی بین‌المللی باشد، به راحتی می‌توان نتیجه گرفت که حملات سایبری به عنوان یکی از اعمال جرم تجاوز محسوب می‌گردد. بنابراین، با توجه به این که عملیات جنگ سایبری می‌تواند ذیل جرم و جنایت بین‌المللی تجاوز تعریف شود، حملات سایبر می‌تواند عنوان حمله مسلحانه را بخود بگیرد، و در نتیجه حق قانونی «دفاع از خود» محرز است. لذا انجام حمله سایبری درچارچوب اصل دفاع از خود مجاز است، چراکه اصولی همچون«ضرورت خود از دفاع» معنای «فوریت، قریب‌الوقوع بودن، ناچار و ناگزیر بودن» را می‌دهد، و هیچ راهی برای استمداد از شورای امنیت وجود ندارد.

در نهایت، مسئله بسیار انگیز «دفاع از خود احتمالی» است. اگر رفتار یک دولت حاکی از این باشد که آن دولت قصد انجام یک حمله سایبری به دولت دیگری دارد یا گروه‌های متخصص هکرها را سازماندهی کرده و حمله قریب‌الوقوعی علیه دولت دیگری در شرف انجام است، براساس«دفاع پیش دستانه» دکترین بوش حمله متقابل مشروع است.

۷- مسئولیت دولتها

انتساب حملات سایبری به دولتها یکی از چالش‌های فراروی حقوق بین‌الملل است. وقتی یک حمله اینترنتی رخ می‌دهد شناسایی مجرم آن به منظور احراز پیوند بین هکرها و دولت مربوطه به منظور انتساب اعمال به دولت خاص بسیار مشکل است. در واقع، اگر یک هکرهای «کلاه سیاه» با سوء نیتی که دارد همواره بدنبال پنهان سازی آثاری است که از آن طریق می‌توان او را شناسایی کرد، یکی دیگر از هکرها بنام «کلاه سفید» وجود دارند که به همان اندازه در ردیابی او تجربه دارد.

[۱۸] با این وجود، حتی اگر این حمله را ازنظر جغرافیایی بتوان رصد کرد، مشکل بعدی قلمرو سرزمینی است که دامنه انتساب دولتها در برابر اعمال گروهی از هکرها را دچار اشکال می‌سازد.

مسئولیت دولتها درقلب حقوق بین‌الملل جای دارد که در پیش‌نویس کمیسیون حقوق بین‌الملل سال ۲۰۰۱ مربوط به مسئولیت دولتها برای اعمال غیر قانونی بین‌المللی تدوین شد.[۱۹] براین اساس، موضوع انتساب رفتارها به یک دولت را می‌توان از چند راه اثبات کرد: ازجمله، از طریق رفتار بالفعل و یا قانونی ارگان دولتی (حتی در مواردی که آنها فراتر از صلاحیت خود و یا نقض دستور کرده‌اند)، از طریق رفتار افراد و یا نهادهایی دولتی، و یا ازطریق رفتار یک شخص و یا گروهی از افراد با اقدام براساس دستورالعمل و یا زیر نظر و یا کنترل آن دولت اقدام نموده باشند.[۲۰]

"قابلیت استناد به دولت" یکی از بحث برانگیزترین موضوعات است که به معنای «درجه کنترلی است که توسط دولت نسبت به عوامل مربوطه اعمال می‌شود» و این یک موضوع کلیدی است که در سه رویه قضایی بین‌المللی تکرار شده است. دیوان بین‌المللی دادگستری در مورد نیکاراگوئه نقطه عطفی ۲۰۰۷ حکم داد که "کنترل موثر" معیار مناسبی است که اسناد دولتی مورد نیاز را می‌توان به دست آورد، درحالی که دادگاه بین‌المللی کیفری برای یوگسلاوی سابق درقضیه معروف مورد تادیچ تصمیم گرفت که کنترل برخی از کشورها ضعیف، معیار "کلی" به اندازه کافی رضایت‌بخش است. این معیار به شدت توسط دیوان بین‌المللی دادگستری در آن مورد نقطه عطفی ۲۰۰۷ نسل‌کشی بعنوان غیرقانع کننده انتقاد و نامناسب، چنانکه بعنوان اشکال عمده‌ای از گسترش دامنه مسئولیت دولتها و فراتر از اصل اساسی حاکم بر حقوق بین‌الملل است.[۲۱]

بنابراین، در صورتیکه یک حمله سایبری مورد مناقشه به دیوان بین‌المللی دادگستری ارجاع شود، بایستی بررسی شود که آیا معیارهای مورد استفاده به اندازه کافی دقیق هستند که بتوان مسئولیت بین‌المللی دولت مقصر را اثبات کرد.

۸- حقوق مخاصمات مسلحانه

«حقوق حاکم درجنگ»، که به عنوان حقوق مخاصمات مسلحانه و یا قوانین انسان دوستانه بین‌المللی شناخته شده، بخشی ازحقوق بین‌الملل است که به موضوع حفاظت از افرادی که نه در مخاصمات

شرکت داشته و نه نظامی هستند می‌پردازد. همچنین ابزارها و روش‌های جنگی را محدود می‌کند. این شامل مقررات قراردادی و قواعد عرفی می‌شود.[۲۲] مقررات قراردادی عمدتا شامل دو دسته از معاهدات ژنو و قوانین لاهه است:

اولین معیار، قانون ژنو است که به موضوع حمایت از غیر نظامیان، زندانیان جنگی می‌پردازد و حمایت از افراد مجروح و بیمار در روی زمین و در دریا در کنوانسیونهای ژنو۱۹۴۹ که متشکل از چهار کنوانسیون است درج گردیده است. این کنوانسیونها توسط دو پروتکل‌های اضافی درسال ۱۹۷۷ تکمیل شد که مربوط به حفاظت از قربانیان درگیری‌های مسلحانه بین‌المللی و غیر بین‌المللی می‌پردازد.

دومین معیار، قوانین لاهه است که جنبه‌های عملیات نظامی در رفتار متخاصمین می‌پردازد که شامل مقررات لاهه ۱۸۹۹ و ۱۹۰۷ بهمراه کنوانسیونها و توافقنامه مختلف منع استفاده از سلاح‌های خاص و تاکتیک‌های نظامی است.

در این بخش به کاربرد احتمالی قوانین جنگ در درگیری‌های بین‌المللی سایبری می‌پردازیم، از آنجا که قوانین جنگی باید نسبت به تمامی عملیاتهای نظامی اعمال گردد، لذا عملیات سایبری را نمی‌توان از آن استثنا نمود. با این حال، سوال این است که آیا قوانین انسان دوستانه بین‌المللی می‌تواند به عملیات سایبری اعمال می‌شود؟

نویسندگان مختلف تائید می‌کنند که موضوع درگیریهای سایبری می‌تواند بدون هیچ ابهامی تابع قانون بشردوستانه باشد. شایان ذکر است که قوانین حقوق بین‌الملل نسبت به هر درگیری مسلحانه قابلیت اعمال دارد و کنوانسیون ژنو که نسبت به تمام موارد اعلام جنگ و یا هر درگیری مسلحانه دیگر که ممکن است بین دو یا بیشتر از دولتها بوجود آید اعمال می‌شود. بنابراین می‌تواند برای حملات سایبری نیز معتبر باشد.

جدای از اطلاق 'حمله مسلحانه' به عملیات سایبری، پرداختن به تعریف 'حمله' درقوانین انسان دوستانه بین‌المللی مفید خواهد بود. در ماده۴۹ پرتکل الحاقی اول آمده است: 'حمله' بعنوان «اعمال خشونت آمیز علیه دشمن، اعم حمله یا دفاع» تعریف می‌شود. در نتیجه، حملات سایبری قطعا در درون حوزه این تعریف قرار می‌گیرد. بنابراین، بعنوان قانون عرفی پذیرفته شده است. ماده ۳۶ پرتکل الحاقی اول اعلام می‌کند: «مطالعه، تحقیق، کسب و یا دستیابی به یک سلاح جدید، و یا ابزار و یا شیوه‌های جنگی، طرفین متعاهد ملزم هستند تعیین کنند آیا کاربرد آن در برخی موارد یا تحت هر شرایطی، قابل انطباق با این پروتکل و یا هر قواعد ممنوعه بین‌المللی است یا خیر؟»

۸-۱- اصول اساسی حقوق مخاصمات مسلحانه

به نظر می‌رسد استفاده از قوانین بین‌المللی بشردوستانه در عملیات سایبری، موضوعی است که مورد علاقه محققان 'حقوق سایبری' باشد. با این حال، همانطور که انتظار می‌رود، هیچ اجماع در میان علمای حقوق بین‌الملل راجع به محدودیتهای اصول قوانین انساندوستانه بین المللی وجود ندارد، و بررسی نمونه‌هایی از اصول اساسی حقوق حاکم بر جنگ نشان می‌دهد که برخی از آنها با هم تداخل دارند.[۲۳]

تمرکز ما در این مقاله بر سه اصل زیربنایی حقوق مخاصمات مسلحانه بین‌المللی قرار دارد: تمایز، ضرورت و تناسب.

۸-۱-۱- اصل تمایز

اصل تمایز یکی از اساسی‌ترین اصول جنگ است که در ماده۴۸ پرتکل الحاقی اول درج گردیده است. بر اساس آن،"برای تضمین رعایت و حفاظت از جمعیت غیرنظامی و اشیاء غیرنظامی، طرفین درگیری باید درهمه حال بین جمعیت غیرنظامی و نظامیان و بین اشیاء غیرنظامی و اهداف نظامی تمایز قائل شوند و باید عملیات خود را تنها علیه اهداف نظامی مستقیم بکار برند". اصل تمایز، بیشتر در فصول دوم و سوم پرتکل اول اشاره شده، که به موضوعات محافظت از غیر نظامیان و مردم غیر نظامی (مواد ۵۰ و ۵۱)، و حفاظت از اشیاء غیر نظامی (مواد ۵۲ به ۵۶)، می‌پردازد.

سنگ زیربنای قوانین انسان دوستانه بین المللی اصل تمایز است به خصوص امروزه که ارتباط تنگاتنگ شبکه‌های رایانه‌ای موجب شده ارائه خط افتراق بین اهداف غیرنظامی و نظامی سخت باشد. دلیل این امر اینست که تنها اهداف نظامی است که می تواند مورد حمله و اشیاء غیرنظامی باید محترم شمرده شود. با توجه به ماده ۵۲ (۲)، حملات باید محدود به اهداف نظامی باشد، که بیشتر براساس ماهیت اشیاء، موقعیت، هدف و یا استفاده از ارائه توضیح داده قطعی مزیت نظامی به وسیله خود را نابودی کل یا قسمتی، دستگیری و یا خنثی‌سازی تفکیک می‌گردند.

به طور ساده، هدف باید دارای ارزش نظامی باشد و زور به اندازه کافی باشد تا از تخریب آن اطمینان حاصل گردد. هر فرمانده نظامی از هدف قرار دادن، دیگر اهداف که موجبات ارتکاب جنایات جنگی را فراهم می‌سازد خودداری کند. بنابراین بازار سهام، نظام بانکداری، دانشگاه‌ها، و زیرساخت‌های غیرنظامی مشابه آن؛ نمی‌تواند مورد حمله قرار گیرد حتی اگر متخاصمین توانایی انجام این کار را داشته باشند.[۲۴]

درخصوص مشروع بودن حملات سایبری، با توجه به ویژگی غیرکشندگی (nonlethal) آن می‌توان استدلال کرد که جنگ سایبری ممکن است منجر به نقض مکرر اصل تمایز در جنگهای متعارف گردد. زیرا این فناوری مدرن آمیختگی میان غیر نظامی و نظامی را افزایش می‌دهد. فلذا تفکیک میان اهداف غیرنظامی از نظامی امکان پذیر نیست.

۸-۱-۲- هدف قرار دادن مردم

اصل تمایز بین نظامیان و غیرنظامیان توسط ماده ۴۳ پرتکل‌های الحاقی اول در تعریف «نیروهای مسلح» روشن شده است. با توجه به ماده ۴۳ (۲) "اعضای نیروهای مسلح طرف مناقشه رزمندگان هستند که بطور مستقیم در خصومت ها مشارکت دارند". ماده ۵۰ با استفاده از تعریف منفی برای توصیف غیرنظامیان به سادگی تمام اشخاصی که در دسته تعلق ندارند رزمندگان و زندانیان جنگ (اسرای جنگی) را شامل می‌گردد.

آقای «وات» با انجام یک ارزیابی حقوقی در زمینه وضعیت مبارزه سایبری، این نتیجه رسید که به منظور بررسی مشارکت در حمله سایبری، توسل به معیارهای کنوانسیون ژنو که درحال حاضر بعنوان استانداردهای قانونی برای وضعیت رزمندگان پذیرفته شده است به دور از واقعیت بوده و کارآیی ندارد'.[۲۵]

با توجه به ماده (۴) (۶) کنوانسیون سوم ژنو به افراد دستگیر شده زیر می‌توان «وضعیت اسرای جنگی» اعطا کرد : «ساکنان یک قلمرو غیراشغال شده، درصورت نزدیک بودن دشمن حق بدست گرفتن سلاح برای مقاومت در برابر نیروهای مهاجم، بدون نیاز به سازماندهی درقالب واحدهای مسلح منظم، و حمل سلاح آشکارا، مشروط به احترام به قوانین و آداب و رسوم جنگ». با این حال، برخی مسائل عملی در زمانی که این تعریف را بخواهیم به یک منازعه اینترنتی تعمیم دهیم آشکار خواهد شد. چگونه می‌توان حمل آشکار اسلحه که یکی از معیارهای شناسایی نظامیان است را در یک حمله به شبکه کامپیوتری یافت؟

۸-۱-۳- اصول انسانیت و ضرورت های نظامی

تعادل بین ضرورت‌های نظامی و انسانیت در ذات حقوق مخاصمات مسلحانه نهفته است، به این صورت که معمولا ضرورت نظامی در یک جهت حرکت می‌کند و ملاحظات بشردوستانه درجهت دیگر. اصل ضرورت نظامی، در مقابل اصل انسانیت قرار می‌گیرد. در رسیدگی‌های نورنبرگ، یک دادگاه نظامی آمریکا در سال ۱۹۴۸ اینگونه تعریف کرده است: "ضرورت نظامی به متخاصمین اجازه می‌دهد، مشروط به رعایت حقوق جنگ، هر میزان زور مورد نیاز برای وادار کردن دشمن به تسلیم کامل با کمترین هزینه و زمان ممکن و حداقل تلفات نیروی انسانی».[۲۶]

از سوی دیگر، «اصل انسانیت» مستلزم آن است که این حمله نباید منجر به درد و رنج غیر ضروری و یا آسیب بی جا برای یک هدف نظامی گردد.

هرچند امروزه اصل ضرورت‌های نظامی و اصل انسانیت درهم تنیده شده است، نشان از این است که قوانین جنگ موجود برای هدایت فرماندهان در استفاده از شبکه‌های مجازی به عنوان یک روش جنگی و یا به معنای واقعی جنگ، کافی است.

۸-۱-۴- اصل تناسب

اصل تناسب، تعیین 'ارزش' جان غیرنظامیان درمقابل مزیت نظامی است که به صراحت در معاهدات حقوق بشردوستانه بین‌المللی پیش‌بینی شده است. پیوند میان نتایج منطقی، ابزار و اثرات آن را می‌توان در ماده ۵۱ (۵) (ب) یافت که اشعار می‌دارد: حمله کور؛ 'حمله‌ای که ممکن است باعث از دست دادن اتفاقی جان غیرنظامیان، آسیب به غیرنظامیان، آسیب به اشیاء غیر نظامی، یا ترکیبی از آن گردد. لذا آثار آن بیش از حد معمول مزیت نظامی مستقیم پیش‌بینی شده است". در ماده ۵۷ (۲) (ب) پرتکل الحاقی اول اعلام می‌کند: "اگر معلوم شود که یک هدف نظامی نیست و یا هدف تحت حمایت ویژه‌ای است که حمله نباید به آن انجام شود، حمله باید لغو شود یا در حالت تعلیق قرار گیرد".

اکثریت حقوقدانان بین المللی معتقدند که با توجه به وجود ارتباطات شبکه‌ای درسراسر دنیا، هم اکنون موضوع عدم تناسب و آثار جمعی

آن تقریبا درحملات سایبر حل شده است[۲۷]. اما برخی دیگر که دیدگاه مثبت‌تری به آن دارند، ادعا می‌کنند که سلاح‌های سایبری تا حد زیادی آسیب‌های جمعی کمتری نسبت به سلاح‌های انرژی جنبشی دارد، در نتیجه دستیابی به اصل تناسب، تفکیک حملات (اهداف نظامی) از مکان‌ها، اموال، و شهروندان محافظت شده، سبب به حداقل رساندن درد و رنج غیر ضروری خواهد بود. با این وجود، حقیقت این است که در جایی همه شبکه‌های غیرنظامی و نظامی به هم متصل هستند، دیگر نمی‌توان تمام خسارت‌های ناخواسته را حذف کرد.

۹- حقوق معاهداتی

در دو بخش قبلی این مقاله، کاربرد رژیم حقوقی بین‌المللی موجود در این شیوه جدیدی از جنگ تحلیل شد. سنجش حملات سایبری با قواعد عرفی در دو حوزه «حقوق حاکم برجنگ» و «حقوق حاکم درجنگ»، همراه با ابهام است. همانطور که قبلا نیز تاکید شد، چارچوب حقوقی فعلی تنها نمی‌تواند بعنوان روش پذیرفته شده جهانی محسوب گردد. بنابراین، به منظور غلبه بر مشکلاتی که ممکن است دراعمال رژیم حقوقی موجود درحملات سایبری بوجود آید، چارچوب حقوقی جدیدی از معاهدات بین‌المللی مورد نیاز است.

به طور خلاصه، قابلیت اعمال پذیری معاهدات موجود بین‌المللی در جنگ سایبری ما را به اینجا رساند که پیشنهاد تهیه پیش‌نویس یک معاهده بین‌المللی برای جنگ سایبری را ارائه کنیم. اما به روی، اشاره به معاهدات موجود که ممکن است در تنظیم عملیات جنگ سایبری مورد استفاده قرار گیرد (شامل معاهدات فضایی، هوایی، دریایی، مخابراتی و معاهدات خلع سلاح) خالی از لطف نخواهد بود.

تا آنجا که به قوانین بین‌المللی فضایی مربوط است، ممنوعیت توسل به زور در سه معاهده حقوق فضا شامل: معاهده فضا (۱۹۶۷)، موافقتنامه ماه (۱۹۷۹) و کنوانسیون مسئولیت (۱۹۷۲) درج گردیده است.[۲۸] درحوزه هوایی، ممنوعیت حمله و تهدید درکنوانسیون مونترال سال ۱۹۷۱ درخصوص جلوگیری از اعمال غیرقانونی علیه هواپیمایی غیرنظامی و در کنوانسیون شیکاگو سال ۱۹۴۴ در رابطه با حمل و نقل هوایی بین‌المللی قید گردیده است. علاوه بر این، نویسندگان مختلف پیشنهاد می‌کنند، مواد ۱۹ و ۱۰۹ کنوانسیون حقوق دریاها سال ۱۹۸۲سازمان ملل متحد نیز می‌تواند بعنوان یک چارچوب مناسب برای حملات سایبری بکار رود. در نهایت، از نظر اتحادیه بین‌المللی مخابرات، می‌توان به مواد ۳۵، ۳۶، و ۳۷ کنوانسیون بین‌المللی مخابرات (ITU) مراجعه کرد.[۲۹]

درخصوص اعمال‌پذیری معاهدات خلع سلاح، ممکن است بتوان قیاسی بین جنگ سایبر و هسته‌ای برقرار کرد."این ارگما"(Ene Ergma)، عضو پارلمان استونی، اظهار داشت: "همانند هنگامی که به یک انفجار هسته‌ای و انفجار رخ دهد، جنگ سایبری بدون خونریزی، می‌تواند همه چیز را نابود کند [۳۰]. اسکات شاکلفورد این مقارنه را تائید می‌کند و اعلام می‌دارد "کنوانسیون‌ها و رویه قضایی قابل اجرا درمورد جنگ هسته‌ای قابلیت اعمال در جنگ سایبری را دارند و برخی از اثرات سلاح‌های هسته‌ای می‌تواند شبیه به حملات سایبری سنگین به یک دولت باشد". وی اضافه کرد که "این نظام تا زمان انعقاد پیمان جامع امنیت سایبر مفید است".[۳۱] با این حال، خط فکری وی نشان دهنده برخی از چالش‌ها است که باید تحت بررسی دقیق حقوقی قرار گیرد. سلاح‌های سایبری، در صورتی که در حد متعادل استفاده می‌شود نمی‌تواند در مقایسه با یک بمب هسته‌ای همان کشنده گی و فجایع را ایجاد کنند.

۱۰- اقدامات سازمان ملل

سازمان ملل متحد، به عنوان یک سازمان جهانی گام‌های بسیار کوتاهی برای تنظیمات استاندارد بین المللی درخصوص تنظیم حملات رایانه‌ای برداشته است. پس از تصویب قطعنامه توسط مجمع عمومی در۲۰۰۴ درمورد ایجاد «فرهنگ جهانی امنیت سایبر و حفاظت از زیرساخت اطلاعات حیاتی»[۳۲] که تنها با استقبال چند دولت محدود روبرو شد، قطعنامه جدیدی در سال ۲۰۱۰ تحت عنوان «ایجاد یک فرهنگ جهانی امنیت سایبر و انجام تلاش ملی برای حفاظت از زیرساخت اطلاعاتی حیاتی' را تنظیم کرد.[1] علاوه براین، پیشنهاد شد که شورای امنیت صلاحیت داشته باشد تا عاملان حمله سایبری را به منزله یک تهدید یا نقض صلح بین‌المللی تلقی نموده و بر اساس اقدامات مندرج در ماده ۴۲ منشور با آن برخورد کند.

[1] UNGA Res/64/211, Sixty-fourth session, 'Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures'

۱۱- نتیجه‌گیری

از یکسو ماهیت فضای سایبر به گونه‌ای است که با در اختیار گزاردن ابزار لازم ارتکاب جرم را تسهیل می‌کند و از سوی دیگر به دلیل فرامرزی بودن این جرائم و نیز عدم نیاز حضور فیزیکی مجرم در ارتکاب جرم، تعقیب، دستگیری و مجازات او بسیار مشکل است. این امکانات منحصر به فرد در کنار دیگر ویژگی‌های فضای سایبر موجب شده تا ضرورت پرداختن به ابعاد حقوقی آن بویژه در سطح بین‌المللی بیشتر آشکار شود.

به نظر می‌رسد تجزیه و تحلیل بالا گویای این است که پاسخ روشنی برای این سوالات وجود ندارد. دلیل آن این می‌تواند باشد قواعد عرفی قدیمی و تعاریف سنتی توسل به زور، تهاجم یا حمله مسلحانه، نسبت به سلاحهای جدید ناقص و غیرکاربردی هستند.

مجموعه وسیعی از مسائل پیچیده و پیامدهای آن باید در چارچوب قوانین بین‌المللی فعلی به منظور پوشش عملیات سایبری پیش‌بینی شوند. تلاش برای قراردادن این مدرن سلاح در چارچوب قوانین بین‌المللی بشردوستانه ناموفق بوده است. از سوی دیگر، باتوجه به وجه غالب سیاسی حاکم بر شورای امنیت سازمان ملل، نمی‌تواند درمقام یک مرجع تصمیم‌گیر برای احراز"وقوع یک تهدید یا توسل به زور و یا برای اعمال تجاوز احتمالی" در این حوزه اعمال صلاحیت کند.

تهیه پیش‌نویس یک سند بین‌المللی که موجد چارچوب حقوقی بین‌المللی برای عملیات جنگ سایبری باشد می‌تواند مجموعه‌ای از منافع مثبت را برای جامعه بین‌المللی بدنبال داشته باشد که اولین و مهمترین اثر آن، ایجاد احساس امنیت کشورهای آسیب‌پذیر است. از سوی دیگر، ایجاد مجموعه‌ای از قوانین لازم‌الاتباع درخصوص حملات سایبری می‌تواند ابهامات فعلی در مورد رفتار و مسئولیت‌های کشورهای درگیر را روشن ساخته و اختلافات احتمالی را حل و فصل نماید.

این مقاله میدان آزمایش میزان کارایی حقوق بین‌المللی فعلی برای اعمال آن دریک حوزه جدید از مخاصمات بود. نتایج آن نشان می‌دهد خیلی رضایت بخش نیست و حملات سایبری را نمی‌توان با قوانین بین‌المللی تنظیم و منع کرد. حملات سایبری را نمی‌توان بعنوان "توسل به زور" یا "اعمال تجاوز" طبقه‌بندی کرد. حملات رایانه ای نمی‌تواند تا سطح 'حمله مسلحانه افزایش یابد تا با قطعیت بتوان گفت که حق قانونی «دفاع از خود» محرز شود. به ترتیب، حق «دفاع از خود» نمی‌تواند درشکل یک حمله سایبری محقق شود، یا را نمی‌توان به راحتی اعمال نهاد غیردولتی یا گروه‌های هکری را به دولتها منتسب کرد.

با توجه به ارتباط متقابل و درهم تنیده شبکه‌های نظامی و غیرنظامی، اصول بنیادین حقوق بشردوستانه همچون اصل تمایز، انسانیت و تناسب را به سختی می‌توان بطور موثر درمورد تهدیدات سایبری استفاده کرد، در نتیجه درحفاظت از جمعیت غیرنظامی و زیرساخت‌ها ناکارآمد است.

به رغم اشتراک در بسیاری از اصول تعریف، نمی‌توان جنگ سایبر را در قالب منابع فعلی حقوق بین‌الملل تحلیل کرد و لذا ظهور منابع جدید مورد نیاز است. جای دادن حملات سایبری در مفاهیم فعلی حقوق مخاصمات مسلحانه ممکن نیست. بنابراین، در بررسی منابع حقوق مخاصمات مسلحانه چنین استنباط می‌گردد که عرف (به عنوان مهمترین منبع حقوق مخاصمات مسلحانه) نسبت به جنگ در محیط سایبر ساکت است، چرا که اساساً این حوزه دارای قدمت و ظهور کاملی نبوده است که انتظار تحقق عرف برای آن را داشته باشیم. همچنین معاهدات بین‌المللی زیرساخت‌های لازم جهت پرداختن به حقوق سایبر را ندارند.

۱۲- پیشنهادات

از آنجا که قوانین بین‌المللی موجود نمی‌تواند برای تنظیم این سلاح چند وجهی مناسب باشد، ارائه پیشنهاد می‌گردد یک معاهده چندجانبه زیر نظر سازمان ملل تنظیم تا به طور خاص به بررسی این موضوع بپردازد. باید چنین معاهده‌ای توسط یک نهاد بین‌المللی هدایت شود.

پیشنهاد می‌شود «یک رکن سازمان ملل متحد برای بررسی ادعاهای مربوط به حملات سایبری تاسیس شود». برای این منظور الگویی مانند آژانس بین‌المللی انرژی اتمی مناسب خواهد بود.

شورای امنیت صلاحیت و مشروعیت پرداختن به این موضوع را ندارد، از طرف دیگر، آن قطعا می‌تواند منجر به این شود که سازمان ملل متحد به عنوان مجموعه‌ای متمرکز برای کنترل و تنظیم کننده هرگونه رابطه بین دولتی درسطح جهانی تبدیل شود.

از آنجا که در حملات سایبری کشف محل دقیق و هویت مرتکب و تفکیک هکرهای خصوصی از هکرهای دولتی بسیار دشوار است و انتساب اعمال بازیگران غیردولتی به دولتها مشکل خواهد بود.

پیشنهاد می گردد 'قابلیت انتساب' حملات سایبری به دولت باید به عنوان حقوق عرفی به رسمیت شناخته شود. و دیوان بین‌المللی دادگستری (ICJ) به عنوان یک مرجع صالح برای حل و فصل اختلاف معرفی شود.

پیشنهاد می‌شود تیم واکنش سریع به حملات سایبری دول مسلمان ایجاد شود تا اولاً؛ بررسی کند کدام دولت عامل حمله سایبری بوده است، و ثانیا؛ تخصص لازم دفاعی برای پاسخ سریع و بهنگام در مقابل حملات را داشته باشد.

یک مکانیسم بین‌المللی برای تعیین موارد نقض و نحوه مجازات و تحریم را برای دولت‌هایی که جرم آنها محرز شده پیش‌بینی گردد.

مراجع

[1] http://www.economist.com/node/16478792.

[۲] جنگ و دفاع سایبر، پروژه" الزامات جنگ های نوین در فضای مجازی سایبر"، اندیشگاه شریف و اندیشکده کاوشگران آینده، ۱۳۸۴، ص ۱۴.

[۳] همان منبع، ص ۲۶

[4] Dictionary of Military and Associated Terms.

[۵] جلد ۱۸ مجله آمریکایی حقوق بین‌الملل (AJIL) صفحات ۷۵۹ ـ ۷۵۶.

[۶] ضیایی بیگدلی، محمدرضا(۱۳۸۶)، حقوق جنگ، کتابخانه گنج دانش، ص ۴۵.

[۷] حسینی، سید ابراهیم(۱۳۸۲)، اصل منع توسل به زور و موارد استثنای آن در اسلام و حقوق بین‌الملل ، پژوهشکده فرهنگ و معارف اسلامی، ص ۱۴۰.

[۸] این موضوع در قضیه فعالیتهای نظامی و شبه نظامی آمریکا علیه نیکاراگوئه توسط دیوان بین‌المللی دادگستری در ۱۹۸۶ به رسمیت شناخته شد. (پاراگراف ۱۷۴ و ۱۸۸ رای دیوان)

[9] UN General Assembly, A/RES/26/2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, Twenty-fifth session, 24 October 1970.

[10] United Nations General Assembly A/RES/42/22, 73rd plenary meeting, 18 November 1987.

[11] M Benatar, 'The Use of Cyber Force: Need for Legal Justification?' (2009) 3 Goettingen Journal of International Law, 375-396

[12] MN Schmitt, Computer Network Attack and the Use of Force in International Law :Thoughts on Normative Framework - [s.l.] : US Air Force Academy, 1999, at 18.

[۱۳] ساک کیتی شیایزری، کریانگ(۱۳۸۳)، حقوق بین‌الملل کیفری، ترجمه بهنام یوسفیان و محمد اسماعیلی، انتشارات سمت، تهران.

[۱۴] بیگ زاده، ابراهیم (۱۳۷۸)، دیوان کیفری بین‌المللی، مجله تحقیقات حقوقی، ش. ۲۶-۲۵ ، ص ۳۰۳.

[15] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

[۱۶] حسن‌بیگی، ابراهیم، «آسیب‌شناسی شبکهٔ جهانی اطلاع‌رسانی اینترنت و ارائهٔ راهبردهای مناسب جهت مقابله با تهدیدها از دیدگاه امنیت ملی با تأکید بر جنبه‌های حقوقی و فنی»، پایان‌نامهٔ دکتری، دانشگاه عالی دفاع ملی، ۱۳۸۲.

[17] http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf.

[۱۸] جنگ و دفاع سایبر(۱۳۸۴)، پروژه" الزامات جنگ‌های نوین در فضای مجازی سایبر"، اندیشگاه شریف و اندیشکده کاوشگران آینده.

[19] Annex to General Assembly Resolution 56/83 of 12 December 2001, and corrected by document A/56/49 (Vol. I)/Corr.4.

[۲۰] ضیایی بیگدلی، محمدرضا(۱۳۸۷)، حقوق بین‌الملل عمومی، ویرایش جدید، چاپ سی و دوم، کتابخانه گنج دانش، صص ۸۴-۴۸۲.

[۲۱] این موضوع درقضیه فعالیتهای نظامی و شبه نظامی آمریکا علیه نیکاراگوئه توسط دیوان بین‌المللی دادگستری در ۱۹۸۶ و قضیه تادیچ در ۱۴ ژولای ۲۰۰۷ و در قضیه نسل زدایی در بوسنی در ۲۶ فوریه ۲۰۰۷ به رسمیت شناخته شد.

[22] ICRC has contributed with a recent customary IHL database published with the results of research on customary humanitarian law conducted in 2005,

[23] JM Henckaerts, Study on Customary International Humanitarian Law, (2005)37 International Review of the Red Cross,

[24] DO Banks, 'Information war crimes: Mitnick meets Milosevic'. (2001). Maxwell AFB, AL: Air Command and Staff College.

[25] S Watts, Combatant Status and Computer Network Attack (August 3, 2009). Virginia Journal of International Law, Vol. 50, No. 2, p. 392, 2010

[26] Y Dinstein, War, aggression and self-defence, Cambridge: Cambridge University Press, 2001, 3rd ed.

[27] MN Schmitt, Wired Warfare: Computer Network Attack and the Jus in Bello, International Law Studies Series. US Naval War College, Vol. 76, pp. 187-218

[۲۸] نواده توپچی، حسین(۱۳۷۸)، حقوق بین‌الملل فضا، تهران، نشر سازمان عقیدتی سیاسی ارتش ج.ا.ا، ص ۲۶.

[29] International Telecommunications Convention, Oct. 25, 1972, arts. 4, 35, 28 U.S.T. 2495,

[30] SJ Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law (April 28, 2009).

[31] UNGA Res/58/199, Fifty-eighth session, 'Creation of a global culture of cybersecurity and the protection of critical informational infrastructures'

[32] UNGA Res/64/211, Sixty-fourth session, 'Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures'