نشریه علمی پدافند غیرعامل

سال دهم، شماره ٤، زمستان ۱۳۹۸، (پیاپی ٤٠): صص ۵۵-۴۷

ارزیابی ماهیت حقوقی حملات سایبری با نگاهی به منشور سازمان ملل متحد

احمدرضا توحیدی[۱*]، محسن سیجانی[۲]

تاریخ دریافت: ۱۳۹۷/۱۱/۱۳
تاریخ پذیرش: ۱۳۹۸/۰۲/۱۵

چکیده

حملات سایبری به‌عنوان شیوه نوین جنگی در حال بروز و ورود به عرصه مخاصمات می‌باشد. این شیوه جنگی به علت ملموس نبـودن فضـای ایجاد شده در آن باعث بروز ابهاماتی در عرصه اعمال قواعد حقوق بین‌الملل بر آن گردیده است. مرز در این فضای غیر ملموس کاربرد فضاهای دیگر حقوق بین‌الملل (خشکی، دریا، هوا، فضا) را ندارد. مسئله‌ای که در این نوشتار مطرح است بررسی این نکته می‌باشد که حملات سایبری با توجه به اصول منشور ملل متحد در کدام اصل می‌گنجد. آیا حملات سایبری شامل اصل منع عـدم توسـل بـه زور مـی‌شـود؟ آیـا حمـلات سایبری در زمره اصل عدم مداخله در امور داخلی دولت‌ها قرار می‌گیرد؟ معیار و ضابطه در قاعده‌مندی حملات سایبری بر اساس اصول منشور ملل متحد چه می‌باشد؟ و این‌که دولت قربانی این حملات حق توسل به دفاع مشروع و اقدامات متقابل را در مقابله با این حملات دارد؟ معیار تشخیص حملات سایبری در مفهوم زور توجه به شدت و گستردگی است که در نظریات دیوان بین‌المللی دادگستری هم بدان پرداختـه شـده است.

کلیدواژه‌ها: حملات سایبری، فضای سایبری، توسل به زور، عدم مداخله ، دفاع مشروع، اقدامات متقابل

۱- استادیار، عضو هیات علمی گروه حقوق بین‌الملل دانشگاه قم، (ar.tohidi@qom.ac.ir)- نویسنده مسئول

۲- دانشجوی دکترای حقوق بین‌الملل دانشگاه قم

۱. مقدمه

قلمرو جامعه بین‌المللی شامل قلمرو خشکی، دریایی، هوایی و فضای ماورای جو می‌باشد، با گسترش دانش بشری فضای جدیدی در پیش روی بشریت گشوده شده است و ارتباطات بین انسان‌ها را تا حد زیادی متحول ساخته است که از آن به‌عنوان فضای پنجم در حقوق بین‌الملل و یا همان فضای سایبری یاد می‌شود. هر کدام از فضای چهارگانه ذکر شده دارای نظام حقوقی خاص خود می‌باشد. اما فضای سایبری از بعد قاعده‌سازی حقوقی با خلا مواجه است، که حملات سایبری از این امر استثنا نیست. جنگ در گذشته با ابزارهای سنتی و سرد و به‌صورت تن به تن بود تا این‌که سلاح گرم به‌عنوان ابزار جنگی مورد استفاده دولت‌های غربی قرار گرفت، به مقتضای پیشرفت سلاح‌های جنگی مقررات آن هم به فراخور این پیشرفت توسط دولت‌ها وضع گردید، که می‌توان به کنفرانس‌های صلح لاهه، کنوانسیون‌های چهارگانه ژنو و پروتکل‌های آن اشاره کرد. در جنگ جهانی دوم با ظهور سلاح مخرب و پیشرفته اتمی و استفاده از آن توسط ایالات متحده، جامعه بین‌المللی متوجه خطر بزرگی شد که این سلاح می‌تواند برای آینده بشریت داشته باشد. بعد از جنگ جهانی دوم در کنوانسیون‌های بین‌المللی به ممنوعیت استفاده از این سلاح‌ها اشاره شده و به عدم گسترش سلاح های هسته‌ای و ممنوعیت تولید و انباشت آن پرداخته شده است و نحوه استفاده صلح‌آمیز از انرژی هسته‌ای به‌طور عمده تحت نظر آژانس بین‌المللی انرژی اتمی قرار گرفت. بنا به آلام انسانی که جنگ برای بشریت ایجاد کرده بود، ممنوعیت جنگ در حقوق بین‌الملل، مطرح گردید که در میثاق جامعه ملل به‌طور مطلق منع نشده بود تا این‌که در میثاق بریان- کلوگ به‌طور مطلق ممنوع اعلام گردید. با این وجود منع اصلی و عمده جنگ در منشور ملل متحد در اصول منشور ملل متحد گنجانده شده است. در ادامه ضمن تعریف حملات سایبری و بیان معیار تشخیص این نوع حملات به تطبیق آن با اصول منشور ملل متحد، اصل منع توسل به زور و اصل عدم مداخله، پرداخته شده است.

۱-۱. تعاریف

حملات سایبری که در فضای سایبری رخ می‌دهد، نیازمند تعریف و شناخت این فضا است. واژه سایبر از لغت یونانی (Kybernetes) به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضیدانی به نام نوربرت وینر در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به کار برده شده است [۱].

تعاریف گوناگونی از سوی اندیشمندان درباره فضای سایبری وجود دارد. در یک تعریف فضای سایبر «قلمرویی جهانی در محیط اطلاعات مشتمل بر شبکه‌های وابسته به یکدیگر زیرساخت‌های فناوری اطلاعات، شامل اینترنت، شبکه‌های مخابرات دور، سامانه‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های نصب شده است» [۲]. فضای سایبری در اصل یک فضا و محیطی است مشابه سایر حوزه‌های رقابتی همچون دریا، زمین و هوا با یک تفاوت و آن هم این‌که این محیط برخلاف بقیه محیط‌ها ساخته دست بشر بوده و غیرملموس است [۳].

حملات سایبری که در فضای سایبر رخ می‌دهد. بدین‌گونه تعریف شده است: حملات سایبری در چارچوب طیف گسترده‌تری از آن چه عملیات اطلاعاتی نامیده می‌شود، قرار می‌گیرند. عملیات اطلاعاتی که جنگ اطلاعاتی نیز زیر مجموعه‌ای از آن است و هنگام مخاصمه مسلحانه به آن توسل می شود. در دستورالعمل تالین [۴]، حملات سایبری بدین‌گونه تعریف شده است: حمله سایبری عملیات سایبری تهاجمی یا تدافعی است که از آن به‌طور معقول انتظار ایراد صدمه، یا مرگ به اشخاص و یا وارد کردن خسارت به اشیا می‌رود [۵]. حملات سایبری بر خلاف جرم‌های سایبری، «عملی تهاجمی بر علیه 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 [۶].

به‌طور کلی حمله سایبری به‌صورت کاملا موثق با هدف حقوق بین‌الملل تعریف نشده است. تنها معاهده‌ای که آن را تعریف کرده به وسیله سازمان همکاری منطقه‌ای شانگهای است که نگرانی‌هایی را نسبت به جنگ اطلاعات ابراز داشته و اشاره کرده است که حمله سایبری به معنای مقابله میان دولت‌ها در عرصه اطلاعاتی با هدف صدمه زدن به سامانه‌های اطلاعاتی، روندها و منابع، ساختارهای حیاتی و مهم، تضعیف سامانه‌های سیاسی، اقتصادی و اجتماعی، عملیات‌های روانی گسترده برای بی‌ثبات‌سازی جامعه و دولت، همچنین مجبور کردن دولت برای اتخاذ تصمیماتی در راستای منافع مخالفین است [۷].

۲-۱. ویژگی‌های حملات سایبری

برای حملات سایبری با توجه به فضای شکل‌گیری آن می‌توان ویژگی‌های زیر را برشمرد: کم هزینه بودن، خدشه وارد کردن در مرزهای سنتی، گسترش فریب و مدیریت افکار عمومی، چالش جدید راهبرد اطلاعاتی، دشواری مشکلات هشداردهنده تاکتیکی

و ارزیابی حمله، دشواری ایجاد و نگهداری ائتلاف، آسیب‌پذیری کشورهای توسعه‌یافته، قرار گرفتن یک فرد در برابر جمع، غافلگیرانه، نامشخص و مبهم بودن، آسیب‌رسانی غیرقطعی و نامعلوم، ماهیت تروریستی، پیشتازی صاحبان فناوری ... [۸].

درباره گسترش فناوری و ایجاد عملیات سایبری و حقوق بین‌الملل که در طول زمان از طریق منابع خود توسعه و تدوین یافته است. نکته‌ای که باید مورد توجه قرار گیرد کارایی این قوانین در بستر جدید فضای سایبری می‌باشد. ریموند کو در این باره بیان داشته است که «با هر بحثی که به فضای اینترنت مربوط می‌شود، حقوق ناگزیر است در دو سطح با فضای سایبری برخورد کند. اولین سطح، ملاحظه این امر است که قواعد فضای واقعی و رژیم‌های حقوقی چگونه باید در فضای سایبری اعمال شود. در این سطح در پی آن هستیم که دریابیم چه زمانی می‌توان ارزش های موجود و اصول حقوقی را به ارزش‌ها و اصولی تبدیل کرد که قابل اعمال در فضای سایبری باشند. در سطح دوم ایجاد موازین جدید برای فضای سایبری، ما را بر آن می‌دارد تا به بررسی قواعد و همچنین تعهداتمان نسبت به ارزش‌هایی که قبل از ایجاد فضای سایبری مبنای آن قواعد را تشکیل می‌دادند بپردازیم» به بیانی دیگر در حوزه سایبری مشکل اصلی نبود قانون نیست، بلکه پیچیدگی‌هایی است که در احراز و تشخیص واقعیت‌ها و امور موضوعی وجود دارد که تعیین آنها پیش شرط اعمال قانون و صدور احکام قانونی است [۹].

۱-۳. انواع جرایم سایبری

اینک با گسترش فناوری و ایجاد فناوری‌های جدید، ورود به سامانه‌های کشورهای دیگر تحت عنوان عملیات سایبری به‌طور عمده در شش بخش تقسیم می‌شود [۱۰].

تجاوز سایبری: تجاوز به اموال دیگران و یا ایجاد خسارت مانند هک، خرابکاری و ویروس‌ها

تقلب و دزدی سایبری: سرقت (پول و اموال)، برای مثال جعل کارت‌های اعتباری و نقض مالکیت معنوی

هرزه نگاری سایبری: فعالیت‌های ناقض قوانین مربوط به هرزگی و نجابت

خشونت سایبری: ایراد یا تحریک به وارد ساختن خسارت بدنی نسبت به دیگران و درنتیجه نقض قوانین مربوط به حمایت از اشخاص، همچون سخنان کینه توزانه و تعقیب و مزاحمت

تروریسم سایبری: حمله به سامانه‌های اطلاعاتی، کامپیوترها و داده‌ها یا به‌طور عام اختلال در زیرساخت‌های حیاتی سامانه‌های اطلاعاتی، به تعبیر پلیت "تروریسم سایبری" حمله‌ای با انگیزه سیاسی و قصد قبلی علیه سامانه‌های کامپیوتری، اطلاعاتی، برنامه‌های کامپیوتری و داده‌هاست که منتج به خشونت علیه اهداف غیر مبارز از سوی گروه‌های ملی یا عوامل مخفی می‌شوند.

جنگ سایبری: جنگ سایبری توسعه سیاست‌ها در فضای سایبری توسط عوامل دولتی و غیردولتی است که به منزله و یا در پاسخ به تهدید جدی علیه امنیت ملی انجام می‌گیرد [۱۱].

۲. اصل منع تهدید و عدم توسل به زور و حملات سایبری

با توجه به اصل منع عدم توسل به زور در بند ۴ ماده ۲ منشور ملل متحد که بیان می‌دارد «کلیه اعضاء در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری و یا از هر روش دیگری که با اهداف ملل متحد مباینت داشته باشد خودداری خواهند کرد» آیا حملات سایبری در این تعریف می‌گنجد؟ آوردن قید تمامیت ارضی و این‌که آیا تهدید در فضای سایبری که محیطی غیرملموس هست در این باره کاربرد دارد؟ هرچند که فضای سایبری فضایی غیر ملموس هست ولی نتیجه فعالیت‌های انجام شده در آن در محیط ملموس خشکی، دریا، هوا و فضا به بار می‌نشیند و عملیات آغازین این فعالیت‌ها در محیط ملموس توسط بشر انجام می‌شود و یا حداقل کنترل می‌شود. آیا اقدامات انجام شده در فضای سایبری در راستای حمله سایبری به‌عنوان زور که در منشور قید شده است می‌تواند باشد؟ منظور از زور در این ماده چیست؟ با توجه به ویژگی‌هایی که حملات سایبری دارد می‌توان بیان داشت که دو اصل مهم منشور ملل متحد اصل منع تهدید و توسل به زور و اصل عدم مداخله در امور داخلی کشورها به شدت در معرض تهدید این حملات نوین قرار دارد. و جامعه بین‌المللی جهت تطبیق و تفسیر بروز قواعد حقوق بین‌الملل با این تغییرات هر چه سریعتر باید این خلا حقوقی را پر کرده و نسبت به شناسائی و مقابله با آن تمهیدی بیاندیشد.

آیا ابزارهای به‌کار رفته در حملات سایبری را می‌توان به‌عنوان سلاح جنگی در نظر گرفت؟ توسل به زور که در منشور سازمان ملل متحد به‌کار رفته است، به دو صورت موسع و مضیق تفسیر شده است. توسل به زور در مفهوم نخست، عبارت است از هرگونه عمل قهرآمیزی که نمی‌توان آن را اقدامی نظامی قلمداد نمود. اما در مفهوم دوم، کلیه تدابیر و عملیات نظامی، از جمله جنگ را شامل می‌شود [۱۲].

اصل منع تهدید یا توسل به زور به‌عنوان سنگ بنای منشور ملل متحد، به دلیل وقوع جنگ جهانی دوم و خسارات گسترده و

کشتار فراوان مردم بی گناه، طی نشست‌های مختلف (نشست مسکو، تهران، یالتا، اعلامیه بین‌المتحدین و...) مورد توجه دولت‌ها قرار گرفت. واژه زور در اصل مذکور همواره محل مناقشه بوده است آیا منظور از زور در این اصل فقط زور نظامی است و یا زور اقتصادی و سیاسی هم مد نظر بوده است. حتی می‌توان با توجه به ماهیت عملیات سایبری از زور فناوری و دانش به‌طور خاص یاد کرد که آیا می‌تواند تحت عنوان زور در این اصل قرار گیرد؟ واژه زور در پیش‌نویس‌های منشور و توسط دیوان بین‌المللی دادگستری و مجمع عمومی تعریف نشده است. براونلی تهدید توسل به زور را این‌گونه تعریف می‌کند «وعده صریح یا ضمنی یک حکومت مبنی بر توسل به زور در صورت عدم قبول درخواست‌های خاص آن حکومت» به عقیده سادورسکا، یک تهدید به زور پیامی است صریح یا ضمنی که توسط یک تصمیم ساز تنظیم و به مخاطب ابلاغ شده و حاکی از آن است که چنانچه قاعده‌ای رعایت نشود یا درخواستی اجابت نگردد پای زور به میان خواهد آمد [۱۳].

بحث تفسیر از زور در منشور ملل متحد، از زمان کنفرانس سانفرانسیسکو، به‌صورت مکرر به ویژه از جانب کشورهای در حال توسعه و کشورهای بلوک شرق مطرح شده است. هرچند نتیجه قطعی دراین باره حاصل نشده است اما رویکرد غالب و عمدتا پذیرفته شده این است که زور در بند ۴ ماده ۲ محدود به زور نظامی می‌شود. با توجه به این‌که در تفسیر باید تا حد امکان واژگان به‌صورت هماهنگ تفسیر شوند. با عنایت به منشور ملل متحد واژه زور در مواد ۲ و ۴۴ منشور بیان شده است، در ماده ۴۴ در فصل هفتم منشور که مختص اقدامات شورای امنیت در جهت حفظ صلح و امنیت بین‌المللی می‌باشد، در این ماده استفاده از زور را به ماده ۴۳، که مربوط به مشارکت جامعه بین‌الملل در حفظ صلح و امنیت بین‌المللی است، ارجاع داده است. در ماده ۴۱ از اقدامات غیرنظامی و در ماده ۴۲ از اقدامات نظامی در صورت موثر نبودن اقدامات ذیل ماده ۴۱ سخن به میان آورده است. در مواد ۴۵ و ۴۶ نیز که به صراحت از اقدامات نظامی یاد کرده است، در مجموع بیانگر این است که ماهیت این فصل به اقدامات قهری اشاره داشته و واژه زور در ماده ۴۴ صرفا مفهوم زور نظامی را دارد. در ماده ۲ منشور که قرابت خاصی بین بند ۴ این ماده با فصل هفتم منشور وجود دارد و به نوعی یکی از موارد اصلی نقض صلح و امنیت بین‌المللی نقض اصل مذکور در بند ۴ ماده ۲ می‌باشد، منظور از زور در ماده ۲ هم صرفا زور نظامی می‌باشد و زور اقتصادی سیاسی و فناوری را شامل نمی‌شود. با توجه به مذاکرات تدوین منشور یکی از پیشنهادهایی که درباره این بند مطرح شد گنجاندن واژه تجاوز به‌جای واژه زور بود که به دلیل عدم صراحت در واژه تجاوز و صریح بودن واژه زور با آن مخالفت شد. در قضیه نیکاراگوئه هم دیوان با تفسیر ضمنی زور نظامی را مد نظر قرار داد. که این تفسیر با مد نظر قرار دادن معیار کنترل موثر که دیوان در انتساب مسئولیت به ایالات متحده آمریکا به کار برد تقویت می‌شود.

در قطعنامه تعریف تجاوز (۳۳۱۴، ۱۴ دسامبر ۱۹۷۴ تصویب مجمع عمومی سازمان ملل متحد) هم تجاوز بدین صورت تعریف شده است: طبق ماده ۱۰ قطعنامه «تجاوز عبارت است از کاربرد نیروی مسلح به وسیله یک کشور علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی کشور دیگر یا کاربرد آن از دیگر راه‌های مغایر با منشور ملل متحد، به‌گونه‌ای که در این تعریف آمده است. در ماده ۳ این قطعنامه مواردی را که به‌عنوان عمل تجاوزکارانه محسوب می‌شود را برشمرده است و لیکن در ماده ۴ قید شده است که موارد ذکر شده در ماده ۳ احصائی نیست و شورای امنیت می‌تواند موارد دیگری را احراز کند که طبق مفاد منشور تجاوز محسوب می‌شود. پس می‌توان طبق این قطعنامه و فصل هفتم منشور ملل متحد برای شورای امنیت در شناسائی حملات سایبری به‌عنوان تجاوز و نقض اصل منع توسل به زور نقش قائل شد کما این‌که مهمترین وظیفه شورای امنیت حفظ صلح و امنیت بین‌المللی می‌باشد که امروزه مفهوم صلح و امنیت بین‌المللی به معنای نبود تهدید و جنگ نیست، مفهوم صلح و امنیت بین‌المللی، در طول زمان با توجه به تغییرات متعدد حادث شده در روابط بین‌المللی تغییر یافته و معنا و مصادیق آن گسترش یافته است [۱۴].

با توجه به این مقرره باید به سمت تعریف زور نظامی بپردازیم و این‌که حملات سایبری در آن چه جایگاهی دارد. منظور از زور نظامی به عملیات مسلحانه اطلاق می‌شود که از طرف دولتی بر دولت دیگر تحمیل می شود در این باره نیاز به تعریف نیروهای مسلح و این‌که منظور از مسلحانه چیست و مصادیق سلاح چه می‌باشد.

در جنگ میان دولت‌ها عوامل و عناصر دخیل را می‌توان این‌گونه بر شمرد:

عنصر تشکیلاتی که به‌طور عمده، کشورها می‌باشند. عنصر تشکیلاتی که در حملات سایبری وجود دارد. البته در مواردی انتساب عنصر دخیل در حمله و شناسایی محل اغاز حمله به سادگی جنگ‌های سنتی امکان‌پذیر نیست.

عنصر مادی که به توان تسلیحاتی اشاره دارد. عنصر مادی یا همان توان تسلیحاتی که به نیروهای مسلح و تسلیحات نظامی اشاره دارد می‌پردازد. در اشاره به تسلیحات به‌کار رفته در جنگ، این طراحی یا کاربرد متداول یک وسیله نیست که آن را سلاح می‌کند بلکه (ملاک) قصد و اثر به‌کارگیری آن است. استفاده از

هر وسیله یا تعدادی از وسایل که باعث تلفات معتنابه جانی و یا تخریب گسترده مالی می‌شود می بایست حائز شرایط یک حمله مسلحانه در نظر گرفته شود [۱۵].

ماده ۲۲ مقررات لاهه، بیانگر این اصل اساسی است که حق طرف‌های مخاصمه مسلحانه در انتخاب ابزارهای جنگ، نامحدود نیست. این مفهوم از جنگ محدود که تقریبا کلمه به کلمه در بند ۱ ماده ۳۵ پروتکل الحاقی اول و مقدمه کنوانسیون مربوط به برخی سلاح‌های متعارف نیز تکرار شده است، روی هم رفته پایه و اساس قواعد حقوقی راجع به کاربرد روش‌ها و ابزارهای جنگی را تشکیل می‌دهد. شرط مارتنز ابتدا در کنوانسیون لاهه و سپس در بند ۲ ماده ۱ پروتکل الحاقی آمده است بدین مضمون اشاره دارد مواردی که به وسیله این کنوانسیون یا دیگر موافقت‌نامه‌های بین‌المللی پوشش داده نمی‌شوند، غیرنظامیان و رزمندگان تحت حمایت و پشتیبانی اصولی از حقوق بین‌الملل هستند که از عرف، اصول بشردوستانه و وجدان عمومی نشات گرفته‌اند. همان‌طور که دیوان در قضیه سلاح‌های هسته‌ای اشاره کرده است، این شرط نشانه و بیانگر قابلیت پوشش‌دهی حقوق بشردوستانه بین‌المللی نسبت به تحول فناوری‌های سریع نظامی است. در جایی که یک نوع خاص از حملات سایبری فی‌نفسه نتایجی دارد که اصول بشری را نقض یا وجدان عمومی را جریحه‌دار می‌کند، آن حملات مطابق با شرط مارتنز ناقض اصول کلی حقوق بشردوستانه هستند [۱۶].

در هر مخاصمه‌ای اصول بنیادین حقوق بشر دوستانه نظیر اصول تفکیک، تناسب، ضرورت نظامی و پرهیز از ایراد رنج غیر ضرور باید مد نظر قرار گیرد. براساس اصل تفکیک فقط اهداف نظامی می‌توانند مورد حمله قرار گیرند. اهداف نظامی، اهدافی هستند که به دلیل ماهیت، موقعیت، هدف یا کاربری آنها از نظر نظامی موثر بوده و تخریب کلی یا جزئی و توقیف یا بی اثر ساختن آنها در زمان حمله مزیتی نظامی به‌شمار می‌آید. مواد (۵۱ و ۵۷) پروتکل اول الحاقی برای حمایت از غیرنظامیان، طرف‌های مخاصمه را به اتخاذ برخی تدابیر احتیاطی موظف دانسته و مقرر کرده که غیرنظامیان نباید مورد هدف مستقیم قرار گیرند و از حملاتی که خسارت جانبی انها زیاد باشد نیز مصون بمانند [۱۷].

موضع‌گیری صلیب‌سرخ نیز اعمال حقوق بشردوستانه در خصوص حملات سایبری است که حمله مسلحانه تلقی می‌شوند، بدین شرح که ابزارها و روش‌های جنگ طی زمان تغییر می کنند و این ابزارها و روش‌ها همان ابزارها و روش‌های زمان تهیه پیش نویس کنوانسیون‌های چهارگانه ژنو نیستند [۱۸].

دیوان بین‌المللی دادگستری نیز در نظریه مشورتی خود در خصوص مشروعیت توسل به سلاح‌های هسته‌ای تصریح نمود که مواد ۲، ۴۲ و ۵۱ منشور ملل متحد، به تسلیحات خاصی اشاره ندارند. این مواد صرف نظر از تسلیحات مورد استفاده، تمامی مصادیق توسل به زور را در برمی‌گیرد. بنابراین، ضرورتی نیست تسلیحات مذکور دارای آثار انفجاری بوده و یا برای اهداف تهاجمی ساخته شده باشند. بی‌تردید استفاده از برخی سلاح‌های غیرجنبشی با کاربرد دوگانه از قبیل مواد زیستی یا شیمیایی علیه یک کشور باید از سوی کشور قربانی به‌عنوان توسل به زور در معنی ماده ۲ منشور ملل متحد تلقی گردد. دیوان بین‌المللی دادگستری به‌طور ضمنی پذیرفته است که استفاده از تسلیحات غیرجنبشی می‌تواند موجب نقض ماده ۲ منشور ملل متحد گردد.[۱۹]

عنصر معنوی که به قصد و نیت طرفین درگیر می پردازد. در راستای ابزار نظامی تلقی شدن آنچه بیشتر مورد توجه هست هدف استفاده از ابزار می باشد که می‌تواند آن را داخل در ابزار تسلیحاتی قرار دهد و با این نگاه غایت محور ملزومات استفاده شده در عملیات‌های سایبری از قبیل رایانه، اینترنت، کاربر و... می‌توانند به‌عنوان تسلیحات مورد توجه قرار گیرند.

با توجه به اثراتی که حملات سایبری برجای می گذارند بهتر هست که آن را به‌عنوان جنگ مسلحانه در نظر گرفته و مشمول حقوق مخاصمات مسلحانه باشد. هرچند که ابزارهای به کار رفته در حملات سایبری جدید بوده و این نوع ابزارها و حملات سایبری در هیچ معاهده‌ای مدون نشده است ولی می‌توان آنها را در چارچوب کنوانسیون‌های چهارگانه ژنو گنجاند همچنانی که درباره تسلیحات هسته‌ای این‌گونه بوده مقرراتی که قبل از وجود سلاح‌های هسته‌ای وجود داشتند بر سلاح‌های هسته‌ای قابلیت اعمال دارند. که این دیدگاه از جانب دیوان بین‌المللی دادگستری در رای مشورتی ۱۹۹۶ مورد تایید قرار گرفته است.

عنصر چهارم هدف دار بودن جنگ است. یعنی کشور آغاز گر جنگ هدفی معین و نهائی دارد که همواره درصدد پیگیری و رسیدن به آن هدف است. این هدف معمولا تحمیل یا قبولاندن یک نقطه نظر سیاسی و یا به عبارت روشن تر یک منظور و هدف ملی است.[۲۰]

۲-۱. توسل به دفاع مشروع در موارد نقض اصل منع تهدید یا استفاده از زور

اقدامات کشور قربانی حملات سایبری چه می‌تواند باشد؟ توسل به دفاع مشروع، رجوع به شورای امنیت، آیا حملات سایبری

نقض صلح تلقی می‌شود؟ اقداماتی که شورای امنیت در این باره می‌تواند انجام دهد.

مبانی حقوقی دفاع مشروع به‌عنوان یک قاعده در حقوق بین‌الملل که خود استثنایی بر قاعده اصل منع تهدید و یا استفاده از زور می باشد، در ماده ۵۱ منشور ملل متحد آمده است. دفاع مشروع در طرح مسئولیت بین‌المللی دولت‌ها ۲۰۰۱ به‌عنوان یکی از معاذیر رافع وصف متخلفانه بین‌المللی ذکر شده است و از شرایط اساسی آن احراز تجاوز مسلحانه و رعایت شرط تناسب و ضرورت در اعمال حق دفاع مشروع است. از موارد دیگر در رعایت آن محدود و تحت کنترل بودن آن می‌باشد که باید به شورای امنیت در این باره گزارش داد و به محض ورود شورای امنیت به قضیه دفاع مشروع منتفی می‌شود.

در استناد به دفاع مشروع در مقابل حملات سایبری سه رویکرد وجود دارد:

رویکرد ابزار محور: در این رویکرد استفاده از تسلیحات نظامی متعارف برای استناد به دفاع نشروع اهنیت دارد.در این رویکرد در صورتی یک حمله سایبری واجد شرایط استناد به ماده ۵۱ منشور است که از تسلیحان نظامی استفاده شود مثلا بمباران سرورهای رایانه ای یا کابل های اینترنتی،

رویکرد هدف محور: براساس این رویکرد در صورت وقوع یک حمله سایبری واحد به یک سامانه حیاتی کشور، می‌توان پاسخ نظامی متعارف به این حمله داد.

رویکرد تاثیر محور: رویکرد تاثیر محور به واسطه شدت تاثیرات یک حمله سایبری، آن را یک حمله مسلحانه تلقی می‌کند رویکرد تاثیر محور به دلیل مواضع میانه خود از مقبولیت بیشتری برخوردار است [۲۱].

باید توجه داشت حتی هنگامی که توسل به زور در فضای سایبر، به آستانه ی دفاع «حمله مسلحانه نرسیده باشد، کشور قربانی هم چنان می‌تواند در وضعیتی علیه حمله سایبری مذکور متوسل شود؛ حمله‌ای که هدف آن» مشروع بازدارنده تدارک یک حمله مسلحانه متعارف فوری است [۲۲].

حتی برخی از کشورها از جمله روسیه و آمریکا برای خود حق دفاع مشروع در مواجهه با حملات سایبری قائل شده‌اند. مقامات روس اعلام کرده‌اند که حتی حق توسل به سلاح اتمی در مواجهه با حملات سایبری را دارند [۲۳]. این قبیل موضع‌گیری از جانب کشورهای قدرتمند و عضو دائم شورای امنیت و موضع‌گیری‌های مشابه از سوی کشورهای دیگر به نوعی بیانگر آینده خطرناک حملات سایبری و لزوم شناسائی آن توسط جامعه بین‌المللی را برای جهانیان گوشزد می‌کند.

۳. اصل عدم مداخله در امور داخلی کشورها و حملات سایبری

اصل عدم مداخله در امور داخلی کشورها به‌عنوان اصلی که به نوعی حقوق بین‌الملل در آن خلاصه شده است در بند ۷ ماده۲ منشور ملل متحد به این اصل اشاره دارد: «هیچ یک از مقررات مندرج در منشور، ملل متحد را مجاز نمی‌دارد در اموری که ذاتا جزء صلاحیت داخلی هر کشوری است دخالت نماید و اعضا را نیز ملزم نمی‌کند که چنین موضوعاتی را تابع مقررات این منشور قرار دهند لیکن این اصل به اعمال اقدامات قهری پیش‌بینی شده در فصل هفتم منشور لطمه نخواهد آورد»

اصل عدم مداخله در امور داخلی کشورها در واقع تکمیل‌کننده اصل منع تهدید و استفاده از زور می‌باشد. دیوان بین‌المللی دادگستری در دعوای نیکاراگوئه علیه آمریکا مقرر می‌دارد: در جایی که مداخله در قالب و شکل تهدید یا توسل به زور نمود پیدا می‌کند، اصل ممنوعیت مداخله در امور داخلی کشورها در کنار ممنوعیت مندرج در بند ۴ ماده ۲ قرار می گیرد [۲۴].

اصل عدم مداخله ریشه در حاکمیت دولت‌ها دارد، همواره دولت‌ها در حفظ و حراست آن حساسیت زیادی داشته و حتی در پذیرش مقررات حقوق بین‌الملل همواره در رعایت این اصل جانب احتیاط را داشته‌اند. عدم مداخله در فرهنگ حقوق بین‌الملل به‌صورت زیر تعریف شده است: «مداخله را عبارت از نفوذ همراه با فشار یک کشور در امور داخلی و یا خارجی کشور دیگر به گونه ای که اراده حاکم کشور مورد مداخله نقض شده و آن کشور را به اتخاذ رفتار خاصی وادار نماید. در این تعریف عمل مداخله با زور همراه است به این معنی که کشوری با توسل به نیروی نظامی یا ابزارهای سیاسی و اقتصادی کشور دیگر را تحت فشار و کنترل قرار دهد.

حمله سایبری را می‌توان ناقض حقوق بین‌الملل دانست هر چند که در برخی موارد به علت شدت عمل آن و اثرات آن می‌توان به دفاع مشروع استناد کرد. در سایر موارد که دارای آثار مذکور نباشد و در تعاریف و مفاهیم اصل عدم توسل به زور نگنجد می‌توان به اصل عدم مداخله در امور داخلی دولت‌ها اشاره داشت که برای دولت آسیب دیده می‌تواند حق اقدامات متقابل ایجاد شود البته در این راستا باید این اعمال با توجه به اصول حقوق بین‌الملل انجام پذیرد که مواد ۲۲ و ۴۹ تا ۵۴ طرح مسئولیت بین‌المللی دولت‌ها ۲۰۰۱ به این شرایط اشاره دارد.

۳-۱. توسل به اقدامات متقابل در اصل عدم مداخله

اقدامات متقابل بر علیه فعل خلاف دولت متخلف در حقوق بین‌الملل پیش‌بینی شده است. ماده ۲۲ طرح مسئولیت

بین‌المللی دولت‌ها به این مطلب اشاره دارد و در مواد ۴۹ تا ۵۴ این طرح به شرایط و حدود و ثغور اعمال آن پرداخته شده است. از این‌که اقدامات متقابل باید واداشتن دولت متخلف و توقف اعمال خلاف وی باشد و مقررات مربوط به حقوق بین‌الملل بشردوستانه و قواعد آمره حقوق بین‌الملل از اعمال اقدامات متقابل مستثنی گردیده‌اند، اقدامات متقابل باید دارای شرط تناسب با فعل متخلفانه باشد. بر اساس ماده ۵۲ طرح مسئولیت دولت زیان‌دیده پیش از مبادرت به اقدامات متقابل باید به دولت مقابل اعلان کرده و پیشنهاد مذاکره دهد و اگر فعل متخلفانه بین‌المللی متوقف شده باشد نمی‌توان به اقدامات متقابل استناد کرد.

با توجه به ماهیت مبهم و تقریبی اثرات در حملات سایبری می شود تحت شرایط مقرر به اقدامات متقابل بر علیه دولتی که از جانب وی حملات سایبری صورت گرفته اقدام نمود.

۴. معیار در تعیین حملات سایبری

حال با توجه به این‌که حملات سایبری در دو اصل فوق‌الذکر می‌تواند گنجانده شود. معیار این‌که حملات سایبری منجر به تجاوز گردیده و اصل عدم توسل به زور نقض گردیده است و یا این‌که به این حد از اثر نبوده وصرفا دارای اثر مداخله بوده است، چیست؟

دیوان در رای نیکاراگوئه به هنگام بررسی یک عملیات خاص به‌عنوان یک حمله نظامی، بیان داشت که بایستی دو عنصر مقیاس و تاثیرات را مورد توجه قرار داد. به‌عنوان مثال عملیات روانی سایبری غیر مخرب که صرفا در صدد تضعیف اعتماد موجود نسبت به یک اقتصاد یا دولت است واجد شرایط کاربرد زور نیست [۲۵].

جهت شناسایی عملی به‌عنوان یک تهاجم خصمانه چهار معیار را می‌توان مورد بررسی قرار داد: اول این‌که آیا این عملیات قابلیت گنجاندن در مفهوم زور را دارد. که طبق بررسی که انجام گرفت و نگاه غایت محور حملات سایبری می‌تواند تحت عنوان زور نظامی هم تلقی شود.

معیار دوم برای تعیین حملات سایبری به‌عنوان حمله مسلحانه توجه به دیدگاه مختل کنندگی به جای تخریب کنندگی 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 همچون تخریب فیزیکی دانسته است. جمع‌آوری اطلاعات و ایجاد اختلال همیشه مهمترین ابزارهای جنگ بوده‌اند. اختلال در شبکه‌های ارتباطی حریف ممکن است حتی ارزش راهبردی بیشتری نسبت به تخریب انبار مهمات یا خطوط پشتیبانی داشته باشد. در واقع، برخی روش های جنگ اطلاعاتی به‌قدری ناخوشایند هستند که با حقوق جنگ جلوگیری نمی‌شوند. هر چند 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 روسیه در سال ۲۰۰۷ آن را دچار خود انفجاری نمود و تولید برق را مختل کرد سیل در منطقه به‌وجود آورد و ۲۰ نفر نیز کشته شدند. بنابراین، به خاطر این نتایج احتمالی، حمله سایبری می‌تواند یک منازعه مسلحانه را بنیان نهد.

معیار سوم که می‌تواند مفید باشد میزان و تاثیرات برای برآورد خسارات به زیر ساخت‌های حیاتی است. مجمع عمومی سازمان ملل متحد زیرساخت‌های حیاتی را این‌گونه تعریف می‌کند «زیرساخت‌های حیاتی شامل آنهایی است که برای تولید، حمل ونقل و توزیع انرژی، حمل ونقل هوایی و دریایی، خدمات بانکی و مالی، تجارت الکترونیک، تهیه آب، توزیع غذا و بهداشت عمومی و زیرساخت‌های اطلاعاتی مهم که به‌طور فزاینده فعالیت‌های آنها را متاثر و به هم مرتبط کرده است می‌باشد» [۲۶]. سازمان همکاری شانگهای زیر ساخت‌های حیاتی را شامل تسهیلات عمومی، سامانه‌ها و موسساتی که حمله به آنها ممکن است به‌طور مستقیم امنیت ملی را به خطر بیندازد حال چه به لحاظ فردی، اجتماعی یا دولتی تعریف می‌کند [۲۷].

معیار چهارم آزمایش شش مرحله‌ای پروفسور میشائیل اشمیت برای بررسی این‌که ایا حملات سایبری از نظر حقوق بشردوستانه بین‌المللی یک حمله مسلحانه محسوب می‌شوند عبارت است از: ۱. شدت، ۲. فوریت یا بی‌واسطگی، ۳. مستقیم یا صراحت، ۴. مداخله امیز بودن، ۵. قابلیت اندازه‌گیری، ۶. مشروعیت احتمالی [۲۸].

وقتی حملات سایبری به ایجاد صدمات فیزیکی یا خسارات منجر و زمانی که آن حملات به آثار مورد نظر منتهی شوند، این‌گونه حملات به درگیری مسلحانه یا جنگ سایبری منجر خواهند شد از طرف دیگر نیز مطابق قاعده ۲۰ راهنمای تالین، هرگونه عملیات سایبری که در چارچوب حمله مسلحانه به وقوع بپیوندد موضوع حقوق مربوط به مخاصمات مسلحانه خواهد بود. به‌عبارت دیگر در صورتی که مخاصمات مسلحانه بین‌المللی به وقوع بپیوندد حقوق درگیری‌های مسلحانه بر تمامی عملیات سایبری که در قالب آن مخاصمه به وقوع می‌پیوندد نیز اعمال می‌شود. عملکرد دولت‌ها، نظریات قضایی و دیدگاه اکثر مفسران حقوق بین‌الملل حاکی از این است که برای رسیدن به سطح

درگیری مسلحانه، حمله سایبری می بایست به سطح معینی از شدت و وخامت رسیده باشد [۲۹].

علاوه بر موارد ذکرشده، معیارهای ششگانه زیر هم توسط اسمیت مطرح شده است که شامل:

۱. شدت: شامل نوع و حجم آسیب‌های وارده؛
۲. فوریت: تعیین سرعت ایراد آسیب پس از انجام حمله؛
۳. صراحت: طول زنجیره علیت یا رابطه میان انجام حمله و وقوع آسیب؛
۴. شاکله حمله داشتن: میزان تاثیر حمله بر سرزمین دولت قربانی؛
۵. قابلیت اندازه‌گیری: میزانی که می‌توان آسیب را اندازه‌گیری کرد.
۶. مشروعیت فرضی: توجه به این واقعیت که در کل فعالیت‌های سایبری وقوع حملات سایبری که منجر به حمله مسلحانه شود، یک استثناست [۳۰].

۵. نتیجه‌گیری

با پیشرفت فناوری، فضای سایبری به‌عنوان فضای پنجم در حقوق بین‌الملل دیر زمانی نیست پا به عرصه ظهور گذاشته است. مثل اکثر پیشرفت‌هایی که فناوری به همراه داشته است در این باره هم از این فضا برای اعمال خرابکارانه استفاده شده است. ماهیت غیرملموس فضای سایبری و تهدیداتی که این فضا برای امنیت و حاکمیت دولت‌ها دارد و ویژگی‌هایی که حملات سایبری دارد، تدوین و تطبیق قوانین بین‌المللی بر این نوع فعالیت‌های سایبری را ایجاب می‌کند. با توجه به عناصری که برای یک جنگ می‌توان برشمرد، با نگاهی به مقررات بین‌المللی، از جمله منشور ملل متحد، نظریات تفسیری دیوان بین‌المللی دادگستری در قضایای ترافعی یا مشورتی، کنوانسیون‌های چهارگانه ژنو۱۹۴۹، پروتکل‌های الحاقی ۱۹۷۷آن و رویه دولت‌ها، می‌توان ابزارهای به‌کار رفته در حملات سایبری را با نگاه غایت محور به‌عنوان ابزار جنگی شناسائی کرد. و این نوع حملات را تحت عنوان «زور» که در منشور ملل متحد آمده است، قلمداد نمود. علاوه‌بر این، با به کار بردن معیارهای شناخت حملات سایبری می‌توان این نوع حملات را به‌عنوان ناقض اصول منع تهدید و عدم توسل به زور و اصل عدم مداخله در امور داخلی کشوها بر شمرد. با در نظر گرفتن ملاحظات ذکرشده، کشورها در هنگام مواجهه با حملات سایبری با رعایت مقررات و موازین بین‌المللی حق توسل به دفاع مشروع و اقدامات متقابل را دارا می‌باشند. با توجه به اهمیت این اصول برای جامعه بین‌المللی که به‌عنوان قواعد آمره بین‌المللی نیز شناسایی شده‌اند، ماهیت حقوقی حملات سایبری باید توسط نهادهای ذیربط همچون دیوان بین‌المللی دادگستری با ارجاع دعوای ترافعی به دیوان یا درخواست نظریه مشورتی، همچنین توسط شورای امنیت سازمان ملل متحد که طبق فصل هفتم منشور ملل متحد مسئولیت اصلی حفظ صلح و امنیت بین‌المللی را به دوش می‌کشد و به‌عنوان مرجع اصلی احراز وقوع تجاوز طبق قطعنامه تعریف تجاوز باید به این عرصه ورود پیدا کنند.

۶. مراجع

۱. فقیه حبیبی، علی، جنگ مدرن و تخاصمات سایبری در چارچوب فضای بین‌الملل، جستارهای سیاسی معاصر، پژوهشگاه علوم انسانی و مطالعات فرهنگی، سال هفتم، شماره اول، صفحه ۱۱۶، بهار ۱۳۹۵.

۲. شایگان، فریده، اعمال حقوق بی طرفی در فضای سایبر، فصلنامه مطالعات حقوق عمومی، دوره۴۶، شماره۲، صفحه ۳۳۹، تابستان ۱۳۹۵.

3. M. C. Libicki, "Cyberdeterrence and cyberwar," RAND Corporation, p. 11, 2009. Available:http://www.rand.org

۴. دستورالعمل تالین، مرکز عالی همکاری دفاع سایبری، تالین استونی، ۲۰۰۹.

۵. اسماعیل‌زاده ملاشی، پرستو، عبداللهی، محسن، زمانی، سید قاسم، حملات سایبری و اصول حقوق بین‌الملل بشردوستانه (مطالعه موردی: حملات سایبری به گرجستان)، فصلنامه مطالعات حقوق عمومی، دوره ۴۷، شماره ۲، صفحه ۵۴۲، تابستان ۱۳۹۶.

6. S. Lesley, "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, p. 307, 2010. Available at: http://digitalcommons.lmu.edu/ilr/vol32/iss2/5.

۷. عباسی مجید، مرادی، حسین، جنگ سایبر از منظر حقوق بین‌الملل بشردوستانه، فصلنامه مجلس و راهبرد، سال بیست و دوم، شماره ۸۱، صفحه ۴۸، بهار ۱۳۹۴.

۸. حسن بیگی، ابراهیم، حقوق و امنیت در فضای سایبر، انتشارات دانشگاه عالی دفاع ملی، صفحات ۱۱۵-۱۱۱، ۱۳۸۸.

9. C. J. Dunlap, "Perspectives for Cyber Strategists on Law for Cyberwar," Strategic Studies Quarterly, p. 81, 2011. http://www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf.

۱۰. صلاحی، سهراب، کشفی، سید مهدی، جنگ سایبری از منظر حقوق بین‌الملل با نگاه به دستورالعمل تالین، فصلنامه علمی و پژوهشی مطالعات قدرت نرم، سال ششم، شماره چهاردهم، صفحات ۷-۶ ، بهار و تابستان ۱۳۹۵.

۱۱. صلاحی، سهراب، کشفی، سید مهدی، جنگ سایبری از منظر حقوق بین‌الملل با نگاه به دستورالعمل تالین، فصلنامه علمی و پژوهشی مطالعات قدرت نرم، سال ششم، شماره چهاردهم، صفحه ۳۴، بهار و تابستان ۱۳۹۵.

۱۲. ضیائی بیگدلی، محمدرضا، نگرشی به حقوق جنگ، فصلنامه مجله حقوقی بین‌المللی، دوره ۶، شماره ۶، صفحه ۴۷، بهار و تابستان ۱۳۶۵.

۱۳. قاسمی، علی، چهاربخش ویکتور بارین، حملات سایبری و حقوق بین‌الملل، مجله حقوقی دادگستری، شماره ۷۸، صفحه ۱۳۶، تابستان ۱۳۹۱.

۱۴. اشرافی، داریوش، تفسیر جدید از صلح و امنیت بین‌المللی و تاثیر آن بر مفهوم حاکمیت ملی، فصلنامه پژوهش حقوق عمومی، سال پانزدهم، شماره ۴۲، صفحه ۸۵، بهار ۱۳۹۳.

۱۵. خلف رضایی، حسین، حملات سایبری از منظر حقوق بین‌الملل مطالعه موردی استاکس نت، فصلنامه مجلس و راهبرد، سال بیستم، شماره ۷۳، صفحه ۱۳۴، بهار ۱۳۹۲.

۱۶. هیتر هریس داسنیس، ترجمه سعید حکیمی‌ها و هومان شاهرخ، میزان، صفحه۲۵۲، ۱۳۹۵.

۱۷. خلف رضایی، حسین، حملات سایبری از منظر حقوق بین‌الملل مطالعه موردی استاکس نت، فصلنامه مجلس و راهبرد ، سال بیستم، شماره ۷۳، صفحه ۱۴۲، بهار ۱۳۹۲

۱۸. اسماعیل‌زاده ملاشی، پرستو، عبداللهی، محسن، زمانی، سید قاسم، حملات سایبری و اصول حقوق بین‌الملل بشردوستانه (مطالعه موردی: حملات سایبری به گرجستان)، فصلنامه مطالعات حقوق عمومی، دوره ۴۷، شماره ۲، صفحه ۵۴۴، تابستان ۱۳۹۶.

۱۹. قاسمی، علی، چهاربخش ویکتور بارین، حملات سایبری و حقوق بین‌الملل، مجله حقوقی دادگستری، شماره ۷۸، صفحه۱۲۶، تابستان ۱۳۹۱.

۲۰. ضیائی بیگدلی، محمدرضا، حقوق جنگ، انتشارات دانشگاه علامه طباطبائی، صفحه ۴۶ و۴۷، ۱۳۷۳.

۲۱. آهنی امینه، محمد، حقوق بین‌الملل مدرن و جنگ سایبری در فضای مجازی، موسسه انتشاراتی جهان جام جم، صفحات ۱۱۰-۱۰۶، ۱۳۹۷.

22. H. B. Robertson Jr, “Self-Defense Against Computer Network Attack Under International Law,” in: Schmitt/O’Donnell (eds), Computer Network Attack and International Law, p. 139, 2001.

23. K. Joanna , “State Responsibility for Cyber attacks on International Peace and Security,” Polish Yearbook of International Law, vol. XXIX, P. 142, 2009. Available at: http://ssrn.com/abstract=1668020

۲۴. اصلانی‌جبار، ایران، استاکس نت و چالش های حقوقی پیش رو در مواجهه با حملات سایبری، مقاله مندرج در مجموعه مقالات ایران و چالش های حقوقی بین المللی معاصر(عابدینی عبدالله)، شهر دانش، صفحه ۲۷۳، ۱۳۹۳.

25. Case Concerning Military and Paramilitary Activities in and Against Nicaragua b(Nicaragua v. United States of America), I. C. J. Reports, para 195, 1986.

۲۶. عباسی، مجید، مرادی، حسین، جنگ سایبر از منظر حقوق بین الملل بشردوستانه، فصلنامه مجلس و راهبرد، سال بیست و دوم، شماره ۸۱، صفحات ۶۰-۵۸، بهار ۱۳۹۴.

27. M. Nils, “Cyber warfare and International Law,” The United Nations Institute for Disarmament Research, pp. 10-14, 2011. Availabale: www.unidir.org

28. J. Richardson, “Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield,” pp. 18-19, 2011. Available at SSRN: http://www.ssrn.com.

۲۹. اسماعیل‌زاده ملاشی، پرستو، عبداللهی، محسن، زمانی، سید قاسم، حملات سایبری و اصول حقوق بین‌الملل بشردوستانه (مطالعه موردی: حملات سایبری به گرجستان)، فصلنامه مطالعات حقوق عمومی، دوره ۴۷، شماره ۲، صفحه ۵۵۳، تابستان ۱۳۹۶.

30. M. Schmitt, “Computer Network attack and the use of force in international law: thoughts on a normative framework,” Columbia journal of Transnational Law, vol. 37, p. 904, 1999.

Legal Nature of Cyberattacks with Regard to the United Nations Organization Charter

A. Tohidi[*]**, M. Seyjani**

Abstract

Cyberattacks are emerging as a new method of war, and entering hostility grounds. This war method has made some ambiguities over the application of international laws because of its intangible atmosphere. The borderline in this intangible atmosphere does not have its usability in other contexts of international laws (land, sea, air, space). The main issue of this paper is to look at the principles of the United Nations Charter and determine which one contains cyberattacks. Are cyberattacks included in the principles which prevent the use of force? Are cyberattacks involved in the principle of non-interference in the internal affairs of governments? What are the criteria for rules and regulations of cyberattacks according to the principles of the United Nations Charter? Do the governments under attack have the right to resort to legitimate defense and countermeasures to confront these attacks? The criterion for identifying cyberattacks as a concept of assault is their intensity and extent, which has also been addressed in the jurisprudence of the International Court of Justice.

Key Words: *Cyberattacks, Cyber Atmosphere, Non-use of Force, Non-Intervention in the Internal Affairs of Countries, Legitimate Defense, Countermeasure*

[*] Qom University - (ar.tohidi@qom.ac.ir) - Writer-in-Charge