جستارهای سیاسی معاصر، پژوهشگاه علوم انسانی و مطالعات فرهنگی
سال هفتم، شمارهٔ اول، بهار ۱۳۹۵، ۱۱۵ – ۱٤٤

جنگ مدرن و تخاصمات سایبری
در چارچوب فضای بین‌الملل

علی فقیه حبیبی*

چکیده

مخاصمات در دنیای کنونی در دوقالب سایبری و نظامی به وقوع می پیوندد. حملات سایبری مانند مخاصمات مسلحانه باید متناسب و در چهارچوب حقوق بشردوستانه تجلی باید. اصلی بی طرفی در حملات سایبری و حفظ معیارهای حقوق بشردوستانه در حملات سایبری به مراکز اصلی کشورها باید در رعایت حقوق غیرنظامیان و منطبق بر تمایز بین نظامیان ، افراد غیر نظامی که به طور مستقیم در جنگ شرکت کرده اند باشد. تناسب در رفتار یا عکس العمل در مخاصمه سایبری نیز ازاصولی است که باید رعایت گردد. هنگامی که که حمله ای باعث جان باختن زندگی غیر نظامیان ، ایراد صدمه و آسیب به آنها، ایراد خسارت به اشیاء و اموال غیر نظامی، و یا ایراد تمام خسارت های ذکر شده برخلاف نوع تجاوز گردد و به طور کلی منافع غیرنظامیان مورد تجاوز جدی قرار گیرد تناسب در حمله رعایت نگردیده و ممنوع می باشد.

کلیدواژه‌ها: فضای سایبر، تجاوز، حمله سایبری، ضرورت،تناسب ، تمایزو بی طرفی در حملات سایبری

۱.مقدمه

در این مقاله به بررسی تاثیرات پیشرفت تکنولوژی بر حقوق بین الملل یا به عبارت دیگر تاثیر فضای سایبری –به طور خاص حمله ی سا یبری–، مصداق سلاح جدیدی که می تواند روش هدایت جنگ مدرن توسط بازیگران دولتی و غیردولتی را دگرگون سازد، برمفاد حقوق بین الملل پرداخته می شود . به نظر می رسد سرشت بی مانند این تهدید و توانمندی مرتکبان جنگهای سایبری در آسیب رساندن، کشتار و تخریب

*استادیار دانشکده حقوق دانشگاه آزاد اسلامی– واحد تهران جنوب faghih.habibi@gmail.com
تاریخ دریافت: ۱۳۹۵/۲/۱۲، تاریخ پذیرش: ۱۳۹۵/٤/۱٤

فیزیکی از طریق فضای سایبر، تعاریف سنتی توسل بـه زور را متحـول سـاخته اسـت . البته این موضوع باید لحاظ گردد که هرچه کشورها به سطح پیشرفت بیشترو وابسـتگی بیشتر به تجهیزات الکترونیکی رسیده باشـند امکـان صـدمه دیـدن آنهـا از قبـل چنـین حملاتی بیشتر است به همین دلیل در این زمینه بیشتر مباحث مطرح شده نیز بـا تبیـین دیدگاه غالب از سوی کشور های توسعه یافته صورت می پذیرد و دیگر اینکه اگـر چـه تلاش های متعددی از جانب هر کشور جهت تعریف و توجیه حملات سایبری وجـود دارد ولی به دلیل توانمندی های متفاوت و سطح آسیب وارده به کشـورها اجمـاعی در این زمینه در نحوه برخورد به لحاظ قطعنامه تجاوز و یا نحوه تفسیر ماده ۲ بند ٤ دیـده نمی شود تا در نبود قاعده کنوانسیونی بتوان به عملکرد یکسـان دولتهـا در طـول زمـان جهت بدست آوردن قاعده ای عرفی اشاره کرد .

۲.فضای سایبر[۱]

۲-۱.تعریف و مفهوم فضای سایبر

فضای سایبر(Cyberspace) عبارتی است کـه در دنیـای اینترنـت، رسـانه و ارتباطـات بسیار شنیده می‌شود. به نظر می‌رسد به‌کارگیری این اصطلاح برای ارجاع به امـور فنـی، به آن رنگ و بویی صرفاً فنی و مکانیکی داده باشد. ملاحظه دقیق‌تر این اصطلاح نشـان می‌دهد که این واقعیت، وجـوه و جنبـه‌هـای متنـوعی، از جملـه خصـلت‌هـای جامعـه شناختی قابل توجهی دارد.در منابع موجود آمده است که: واژه سـایبر از لغـت یونـانی (Kybernetes)به معنی سکاندار یا راهنما مشتق شده است .نخستین بـار ایـن اصـطلاح "سایبرنتیک"[۲] توسط ریاضیدانی به نام "نوربرت وینر (Norbert Wiener) "در کتـابی با عنوان "سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین " در سال ۱۹٤۸ به‌کار برده شده است. سایبر پیشوندی است برای توصیف یک شخص، یک شـی، یـک ایـده و یـا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است. در طی توسعه اینترنت واژه‌های ترکیبی بسیاری از کلمه سایبر به‌وجود آمده است که به تعدادی از آنها اشاره می کنیم: فضـــای ســـایبر[۲] Cyberspace شـــهروند ســـایبر Cybercitizen،تجـــارت سایبرCyberbussiness، و در نهایت جنگ سایبر(Cyberwarfare) که بحث مد نظر مـا را در بر می گیرد.

۲-۲.ارکان فعالیت‌های تخریبی سایبر از منظر نحوه عملکرد

با توجه به اهمیت روزافزون اطلاعات و IT ، خیلی تعجب آور نیست که طرفهای یـک درگیری به دنبال به دست آوردن مزیت بیشتر نسبت به دشمنان خود با استفاده از ابـزار

های مختلف از جمله تکنولوژی فناوری اطلاعـات و تکنیـک هـای متعـدد بـرای بهـره برداری از جنبه های خاصی از فضای مجازی باشند. بـه عبـارت دیگـر هـدف و نحـوه عملکرد فضا را برای تخریب فـراهم مـی آورد و منظـور محوریـت ابـزار هـای مـورد استفاده و انسانها در فضای مجازی، به شرح ذیل است؛

" **۱**.دسترسیAccess،می تواند به صورت خاموش از طریق اینترنت، مودم دایـل آپ یـا نفوذ از طریق شبکه وایر لس به دستگاهی که به آن وصل می شوند، صورت پذیرد.البته در نهایت برای دسترسی نیاز به نزدیکـی فیزیکـی اسـت ماننـد عملیـات جاسوسـی یـا تعمیرات تکنیکی یا فروشنده بودن و می تواند در هر جایی از این چرخه اتفـاق بیفتـد، از زمان ساخت تراشه ، مونتاژ، بارگیری نرم افزار، حمل و نقل به مشتری، و یا در زمـان استفاده مشتری؛

۲. قابلیت آسیب پذیریVulnerability ، خواستگاه IT می تواند آسـیب رسـانی باشـد. این آسیب می تواند در هنگام ساخت، غیرعامدانه ایجاد شده باشـد و یـا عامدانـه و در حالتی که غیر عامدانه باشد راه را برای ورود خرابکاران باز می گذارد.

۳.ظرفیت ترابری Payload ، این اصطلاح برای توضیح مکانیزم اثر گـذاری بـر روی IT بعد از اینکه دسترسی جهت تخریب مورد استفاده قرار گرفت استفاه می شود. بـه طـور مثال وقتی نرم افزار مد نظر وارد سیستم کامپیوتری شد می تواند دوبـاره برنامـه ریـزی شود. بدین معنا که شبیه خودش را بازتولید کنـد یـا خـودش را انتقـال دهـد، فایلهـای سیستم را تخریب یا تغییر دهد . این عملیات می توانـد بیشـتر از یـک فعالیـت بـوده و بارها تکرار شود و یا حتی در زمانهای مختلف تکـرار پـذیرد و اگـر کانالهـای ارتبـاطی موجود باشد ، به صورت خاموش می تواند بارها به روزرسانی گردد.

٤.تکنیک ها بر اساس نحوه عملکرد افراد تعریف می شود، افرادی که بـا IT سـر وکـار دارند، می توانند از طریق رشوه یا black mail یا بـاج خـواهی از یـک کارمنـد داخلـی عملیات خود را انجام دهند، مثلا یک فرد از متخاصمین را وارد یـک مناقصـه کننـد تـا بتوانند ابزار های تکنیکی را به طور خاص بدست آورده یا می توانند با رشـوه دادن بـه یک سرایدار یک فلش جاسوسی را به کامپیوترورد کنند یا حتـی یـک بـاج خـواهی از طرف یک برنامه نویس با نوشتن کدهای معیوب باشد، که در این حالـت تکنیـک هـای انسانی و تکنولوژیکی با هم مورد استفاده است."[٤]

اما در خصوص هدفهای این نوع عملیات فعالیت های مهاجمانه[٥] در فضای سایبری می تواند به عنوان حمله سایبری یا بهره برداری های اینترنتی تفکیک شود:

۱.حمله سایبری Cyber attack، اشاره به استفاده از فعالیت های عمدی برای تغییر ، مختل ، فریب ،کاهش و یا از بین بردن سیستم های کامپیوتری و یا شبکه ها و یااطلاعات و برنامه ها یا انتقال از طریق این سیستم هاو یا شبکه می باشد.این فعالیت ها ممکن است سازمان های متصل به این سیستم ها را نیز به شدت تحت تاثیر قرار دهد. حمله سایبری ممکن است حتی مانع از دسترسی کاربران مجاز به دسترسی به خدمات کامپیوتری و یا اطلاعات ، از بین بردن ماشین آلاتی که توسط کامپیوتر کنترل می شوند(هدف ادعا شده از استاکس نت ، و یا برای از بین بردن یا تغییر داده های حساس (مانند جدول زمانی برای استقرار تدارکات نظامی) منجرشود.نکته حیاتی در این زمینه اثرات به بار آمده است که اثرات غیر مستقیم آسیب به یک سیستمهای متصل به کامپیوتر در یک حمله سایبری از آسیب به خودکامپیوتر می تواند به مراتب قابل توجه تر باشد.

۲. بهره برداری سایبریCyber exploitation : اشاره به فعالیت های آگاهانه طراحی شده برای نفوذ به سیستم های کامپیوتری و یا شبکه های استفاده شده از سوی دشمن ، به منظور اخذ اطلاعات و یا انتقال از طریق این سیستم و یاشبکه های دیگر است. بهره برداری های سایبری به دنبال برهم زدن عملکرد طبیعی سیستم کامپیوتری یا شبکه از نقطه نظر کاربر می باشد. در اینجا هدف افشا شدن اطلاعات دشمن،از طریق جمع آوری اطلاعات با ارزش به وسیله جاسوسی انسانی ، یا افشا کردن برنامه های تحقیقاتی دشمن برای جلوگیری یا اختلال در برنامه های جنگی به منظور تخریب عملیات نظامی یا در سطح کوچکتر بهره مندی از اطلاعات شبکه ای یک شرکت در یک کشور در کشور دیگر به منظور بهره مندی رقیب داخلی آن شرکت است.

در کل باید دقت شود که آنچه در جامعه به صورت عمومی و اغلب استفاده می گردد لفظ " حملات سایبری " است در حالی که فعالیت انجام شده در واقع شامل هر دو قسم بهره برداری و حملات سایبری می باشد.[۶]

آنچه در این مرحله لازم است تبیین گردد، تاثیر هر دوشق از عملیات است که اگر چه در هر دو حالت چه به شکل حمله و چه به شکل بهربردای-تخریب سیستم های زیر بنایی یا جاسوسی- اجماعی در نحوه برخورد از منظر بین المللی وجود ندارد و هر کشوری به فراخور سیستم امنیتی و توان دفاعی با موضوع برخورد می کند اما این مقاله از منظر قابلیت تطبیق اصطلاح حملات سایبری در دو حوزه حقوق بر جنگ « ***jus ad bellum***»و حقوق بشردوستانه بین المللی «***jus in bello*** » به بازنگری مجدد قطعنامه

تجاوز در خصوص عمل تجاوز و ماده ۲ بند ٤ منشور در خصوص تهدید و توسل به زور از یک طرف و از سوی دیگر بند۱ ماده ٤۹ پروتکل اول الحاقی کنواسیون ژنو ۱۹٤۹ در مواقع حمله به اهداف مد نظر می پردازد

بدین معنا به ترتیب به بررسی تعریف تجاوز و ارکان آن ، توسل به زور و آستانه اش و بررسی هدف در پروتکل الحاقی کنوانسیون ژنو با مقایسه شرایط موجود در جنگ سایبری و آستانه آن پرداخته می شود.

۲-۳.تعریف و ارکان تجاوز

در جامعه ای بین المللی سنتی با وجه مشخصه نبودن یک قدرت فوق ملی و رشد نیافتگی نظام حقوقی، دولتها برای دستیابی به هدفهایشان به راههای گوناگون، از جمله بکار گرفتن زور متوسل می شدند. این کاربرد زور شکلهای گوناگون به خود می گرفت. با توجه به موقعیت طرفهای اختلاف و اوضاع و احوال، زور از راههای متفاوت و به درجات مختلف بکار می رفت مانند؛ استفاده از نیروهای مسلح علیه سرزمین دولت دیگر و بیشترین درجه استفاده از زور، جنگ است-در جنگ، اعمال فشارهای پراکنده، نامنظم و در بسیاری موارد یکجانبه و گاه بگاه با ویژگی مسلحانه اتفاق می افتد-.

اگرچه جنگ طی سده ها به مثابه ابزاری در اختیار دولتها برای رسیدن به هدفهایشان قرار داشته است، اما به سبب مصائب ناشی از آن انسانها همواره در تلاش برای جلوگیری از آن بوده اند. از این رو ورود مفهوم جنگ ناعادلانه یا نامشروع بعد ازوقوع جنگ های جهانی اول و دوم ، جامعه بین المللی را به سمت ممنوعیت جنگ و استفاده از راههایی برای حل مسالمت آمیز اختلافات، یعنی داوری و رسیدگی قضایی در پیمان بریان کلوگ حرکت داد، «اما به رغم این منع، از پیمان و شرایط همراه آن می توان دریافت که جنگ در مواردی قانونی شناخته شده بود، نظیر:دفاع از خود، -اقدام جمعی برای اجرای تعهدات بین المللی پذیرفته شده در اسناد موجود-،اختلاف میان دولتهای عضور و غیر عضو پیمان،و سرانجام اقدام علیه عضوی که با نقض پیمان به جنگ متوسل می شد. به این ترتیب،پیمان در عمل، جنگ را لغو نکرد، بلکه فقط توسل به آن را با استثنائاتی منع نمود»[۷]. این پیمان گرچه به اقدامات تجاوزکارانه اشاره نمی کند، اما «می توان استدلال کرد که غیر قانونی شناختن جنگ به مثابه ابزار سیاست ملی بطور ضمنی به معنی منع جنگ تجاوزکارانه است» از زمان پیمان بریان-کلوگ تا به حال

گرچه به طور ضمنی سعی در تعریف وممنوعیت دقیق جنگ و تجاوز بود اما نتیجه عملی خاصی جهت رسیدن به تعریف در خصوص بحث تجاوز به دلایل متعدد حاصل نگردید، و البته مجمع عمومی سازمان ملل متّحد در سال ۱۹۷٤ قطعنامه شماره۳۳۱٤ را، تحت عنوان «قطعنامه تعریف تجاوز» به اتفاق آراء(اجماع) تصویب کرد.

۳.قطعنامه تجاوز، ارکان و اجزای آن

قطعنامه تجاوز دارای یک سند تصویب و یک ضمیمه است که ضمیمه نیز دارای یک مقدمه در ده بند و هشت ماده است . ماده ۸ این قطعنامه تکیه زیادی بر یکپارچگی مقدمه و مواد دارد و بندهای پنجم و نهم و دهم بر ضرورت تعریف تکیه کرده است .
در این قطعنامه، تجاوز عبارت است از به کارگیری زور به صورت مسلّحانه توسط یک دولت علیه حاکمیت یا تمامیت ارضی یا استقلال سیاسی دولت دیگر یا به هر نحو دیگر که با اهداف سازمان ملل متّحد ناسازگار باشد. [۸]
نکات تعریف: منظور از به کارگیری زور که مورد بحث تجاوز است فقط به کارگیری نیروی‌مسلّحانه است و مسایلی نظیر تهاجم فرهنگی، ایدیولوژیک و یا اقتصادی را شامل نمی‌شود. چراکه این اقدامات از سوی نیروی مسلح صورت نمی گیرد، ولی به هر حال، طبق تعریف حاضر چنین تجاوزی اگر از راه کاربرد نیروی مسلح صورت پذیرد در چهارچوب تعریف توافق شده قرار خواهد گرفت.

۳-۱.اقدامات دارای کیفیت تجاوز

علاوه بر تعریف کلی تجاوز، ماده ۳ قطعنامه اقداماتی را بر می شمارد و آنها را دارای کیفیت تجاوز می داند[۹] که در هفت بند توضیح داده شده است[۱۰]، در اغلب بندها حضور فیزیکی دولتی علیه دولت دیگر به نوعی از انحا به چشم می خورد اما بند ((ب)) ماده ۳ موردی را در برمی گیرد که لزوما تهاجم فیزیکی یا حمله واقعی به سرزمین دولت دیگر را شامل نمی شود. این بند حاکی است:
« بمباران سرزمین یک دولت توسط نیروهای مسلح دولتی دیگر، یا کاربرد هر نوع سلاح توسط یک دولت علیه سرزمین دولتی دیگر...» شوروی و پاره ای از دولتهای دیگر اعتقاد داشتند ((کاربرد سلاحهای هسته ای، میکربی، شیمیایی و دیگر سلاحهای دارای قدرت انهدام گسترده)) مورد اشاره قرار گیرد، و استدلال می کردند که گنجاندن این عبارت نشان دهنده تنفر ویژه جامعه بین المللی نسبت به اینگونه سلاحها است.

مخالفان استدلال می کردند که عدم مشروعیت حمله ناشی از نوع سلاح نیست، و ذکر ((هر نوع سلاح)) چنان فراگیر است که برشماری انواع سلاحها را زائد می گرداند و این استدلال با توجه به بند پنجم مقدمه که از ((سلاحهای دارای قدرت انهدام گسترده)) نام می برد، پذیرفته می شود .

همچنین از این بند چند مساله را دیگر را نیز می توان به طور ضمنی دریافت:

نخست: حضور فیزیکی برای تجاوز به کشور دیگر لازم دانسته نشده و صرف بمباران از راه موشک های دور برد هسته ای یا شیمیایی یا.... یا حتی موشکهایی که صرفا جنبه تخریب دارند اما هسته ای و شیمیایی نیستند نیز به عنوان عمل تجاوز شناخته می شود و؛

دوم: دغدغه بسیاری از کشور ها –مخصوصا شوروری با کفه قدرت بالای تسلیحات نظامی – گنجاندن موضوع نوع تسلیحات در تعریف بوده است. اگر چه بکاربردن نام سلاحهای شیمیایی ، هسته ای و یا میکروبی قسمتی از دغدغه ها را پوشش می داد لیکن قسمتی از موضوع که قدرت تخریب با تسلیحات نظامی جدید و پیشرفته تر است با آوردن نام تعدادی مورد تغافل می ماند.

سوم: بحث اصلی قدرت تخریب این تسلیحات است ، بدین معنا که تسلیحات از هر نوع که باشد اهمیت خود را با توجه به بند پنجم مقدمه قطعنامه با صفت «قدرت انهدام گسترده» باز می یابد ؛ به عبارت بهتر نتیجه و اثر کاربرد اسلحه ای که انهدام وسیع و گسترده را بر جای می گذارد عمل تجاوز نامیده می شود .[۱۱]

۴.حملات سایبری و مقایسه آن با تعریف تجاوز در قطعنامه

با توجه به آنچه که به عنوان نکته در تعریف تجاوز مطابق با بند ۲ قطعنامه ذکر شد که قابلیت حمله بدون در نظرگرفتن نوع اسلحه و در نظر گرفتن اثرات تخریب و اینکه امکان حملات خارج از مرز نیز وجود دارد و با توجه به خصوصیات حملات سایبری که مرزی برای حمله در آن مشخص نیست و بسیاری از موارد تخریب به سیستم هاو سازمانهای مرتبط به کامپیوتر از قوه تصور خارج می گردد، به راحتی می توان این سلاح کشنده و این نوع حملات را در زمره تجاوز بدون مرز تعریف کرد.

ماده ۲ بند ٤ منشور ملل متحد: حال به بیانی دیگر در خصوص بررسی موضوع ممنوعیت جنگ سایبری با بازنگری ماده ۲ بند ٤ منشور ملل متحد می پردازیم؛ لازم

بذکر است که در بعضی موارد برای توضیح مطلب به مواد دیگر منشور نیز اشاره گذرایی می شود.

در این جا دو موضوع مطرح می شود یک مساله این است که آیا منشور توانایی پاسخ به جنگ های کنونی را دارد؟ و در مرحله بعد آیا صرفا اتکا به متن مواد برای استناد در شرایط کنونی مفید و موثر است؟

درپاسخ به پرسش اول باید گفت که پروفسور توماس فرانک در سال ۱۹۷۰ مرگ ماده ۲ بند٤ را اعلام کرد ، او همچنین اعلام نمود که با توجه به سرعت تغییر مناقشات، ممنوعیت زور اصطلاحی منسوخ شده است . چراکه از دیدگاه او بزرگترین جنگهای گذشته تا زمان کنفرانس سانفرانسیسکو ،با تهاجم سازمان یافته تشکل های نظامی بزرگ یک کشور بر روی خاک دیگری آغاز می شده است و این حملات معمولا با بسیج قبلی نیروهای نظامی و حرکت آنها و از طریق اعلامیه رسمی جنگ اتفاق می افتاد . درحالیکه فضای جنگ کنونی این مقدمات را در عمل پشت سر گذاشته است و در حال حاضر ابرقدرتها به صوزت معمول، از شورش ،جنبش های شورشی و کودتا بر علیه دولتهای دیگر با اشکال مختلفی مانند کمکهای نظامی حمایت می کنند و جنگ هایی در مقیاس کوچک ، مانند خرابکاری و خرابکاری متقابل از طریق گروه های محلی به نسبت عملیات های جنگی قانونی مطابق کنوانسیون و مستقیم رایج شده است و رژیم منشور به سختی برای هدایت کردن مناقشاتی از این دست مجهز می باشد. نگرانی پروفسور فرانک از این بود که اشکال مناقشه های کنونی خارج از توانایی رژیم منشور برای تحمیل هزینه های لازم به گونه ای است که مانع جنگ شود. به عبارت بهتر نظر پروفسور فرانک بر عدم کفایت ماده به لحاظ تغییر موقعیت ابزاری در طول تاریخ جنگ هاست. هرچند این دیدگاه غالب نیست اما قابل تأمل است، چرا که در هر بحثی از فضای حاکم تاریخی نمی توان غافل بود. علاوه بر آن دیوان بین المللی دادگستری در رای نیکاراگوئه۱۹۸٦ بر عرفی بودن ماهیت این مقرره تاکید می کند، بدین معنا جامعه بین المللی ملزم به رعایت این مقرره است و این خود دلیلی دیگر بر موجودیت این ماده و اهمیت آن است.

۵.بررسی متن ماده و تفاسیر مربوط به آن

این ماده بیان می کند که؛ «کلیه اعضاء در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر روش دیگری

که با مقاصد ملل متحد مباینت داشته باشد خودداری خواهند نمود.»[۱۲] لازم به ذکر است حمله مسلحانه در هیچ کنوانسیونی تعریف نشده است و به عبارت دیگر نحوه برخورد با لفظ توسل به زور در مقام حمله مسلحانه به دیدگاه هر کشور بستگی دارد و اگرچه به نظر مساله ساز می باشد اما چهارچوبی قانونی برای معنی دادن اصولی به آن وجود دارد. کمیته بین المللی دیدگاه آقای Jean S. Pictet را مبنای حرکت و نقطه آغاز قرار می دهد ؛ این معیار مدت زمان و شدت عمل است که در هر حمله مسلحانه اهمیت می یابد. و اگر چه این معیار یک معیار قانونی است اما بازیکنان دولتی و غیر دولتی آن را به شکل های مختلف فراخور موقعیت خود تفسیر می کنند. آقای Harkening به نسخه فرانسوی منشور سازمان ملل متحد ، که اشاره به " تجاوز مسلحانه " به جای" حمله مسلحانه " دارد، می کند که مجمع عمومی سازمان ملل در تعریف قطعنامه تجاوز در سال ۱۹۷٤ به تصویب رساند . و در این قطعنامه اعلام می دارد که یک حمله باید به اندازه کافی سنگین باشد تا به عنوان یک حمله مسلحانه در نظر گرفته شود.[۱۳]

همچنین نکته دیگر در این ماده منع تهدید و منع توسل به زور با توجه مفاد ماده است، بر اساس ماده ۲بند ٤ پاسخ به این پرسش که تهدید به حمله ، تهدیدی غیرقانونی است یا خیر؟ دیوان بین المللی دادگستری در رای تسلیحات هسته ای ، قانونی بودن تهدید را با قانونی بودن توسل به زور در شرایط یکسان مرتبط دانسته است.

در مورد توسل به زور بر اساس مفاد ماده تا مدتهای طولانی، آمریکا و دیگر متحدانش این ماده و ماده ۵۱ را برای مقابله با حملات مسلحانه و زور کافی می دانستند چرا که بیان ساده این ماده به همراه مواد ٤۱ و ٤۲ که به شورای امنیت برای مقابله غیر نظامی و عملیاتی معادل با حملات مسلحانه مجوز می دهد، موضوع را به سرانجام می رساند. اما آیا صرفا متن ماده ۲ بند٤ بدون در نظر گرفتن دیگر موارد برای استناد در مورد حملات سایبری در شرایط کنونی مفید و موثر است؟

بدین ترتیب به واکاوی اصطلاح استفاده از زور در ماده مذکور با توجه به متن ، سیاق و تفاسیر می پردازیم؛

رویکردی با حمایت از تفسیر مضیق و ماده مذکور ، آن را صرفاً به حمله ی مسلحانه محدود میداند . اما با نگاهی دقیق تر، در واقع هدف اساسی منشور آن گونه که در مقدمه آن ذکر شده، محفوظ داشتن نسل های آینده از مصایب جنگ است و نه صرفا منع نمودن تمامی اشکال زور.به بیان دیگر این ماده بیانگر آن نیست که در « کارهای

مقدماتی» طراحان منشور بر این مقصود بوده اند که ممنوعیت توسل به زور را به فشارهای اقتصادی و سیاسی تسری دهند. بدین علت اصلاحیه ارائه شده توسط برزیل که تمامی اشکال تهدید یا توسل به اقدامات اقتصادی مغایر با اهداف ملل متحد را ممنوع می دانست ، در کنفرانس سال ۱۹٤٥ سانفرانسیسکو رد شد .اسناد بعدی سازمان ملل متحد نیز موید این موضوع دانسته شد[۱٤]

حال این پرسش مطرح می شود که لفظ مسلحانه به چه معنی است؟ در مقام پاسخ می توان گفت لفظ مسلحانه یا مسلح به معنی تجهیز به یک سلاح یا درگیری با سلاح برای استفاده جهت صدمه زدن به دیگری یا قتل وی است. تقریباً تمامی اشیاء می توانند به عنوان سلاح به کار روند؛ در صورتی که قصد دارنده ی آن خصمانه باشد .دیوان بین المللی دادگستری در نظریه مشورتی خود در خصوص مشروعیت توسل به سلاح های هسته ای[۱٥] تصریح نمود که مواد ۲بند ٤ و ٤۲ و ٥۱ منشور ملل متحد، به تسلیحات خاصی اشاره ندارد .این مواد، صرف نظر از تسلیحات مورد استفاده، تمامی مصادیق توسل به زور را در جنگ در برمی گیرد، بنابراین، ضرورتی نیست تسلیحات مذکور ؛ دارای آثار انفجاری بوده و یا برای اهداف تهاجمی ساخته شده باشند. بی تردید، استفاده از برخی مواد بیولوژیک یا شیمیایی ،یا سلاحهای غیرجنبشی با کاربرد دو گانه علیه یک کشور، باید از سوی کشور قربانی به عنوان توسل به زور در معنای ماده ۲ بند ٤ منشور ملل متحد تلقی می گردد. دیوان بین المللی دادگستری به نحو ضمنی پذیرفته است که استفاده از تسلیحات غیرجنبشی می تواند موجب نقض ماده ٤ بند ۲ منشور ملل متحد گردد؛ زیرا دیوان در قضیه نیکاراگوئه، تسلیح و آموزش کنتراها توسط ایالات متحده آمریکا را به عنوان تهدید یا توسل به زور علیه نیکاراگوئه توصیف نمود. ،

اما از دیدگاهی دیگر می توان با توجه به قواعد تفسیر در ماده ۳۱ و ۳۲ معاهدات ، که عبارتند از تفسیر بر اساس حسن نیت مطابق با معنای معمولی کلمات در سیاق آن و در پرتو هدف و موضوع به تفسیر ماده ۲ بند ٤ پرداخت .

بدین منظور به جای صرفا در تظر گرفتن لفظ زور ، به هدف ماده که حفظ و حمایت جان انسانها از بلایای جنگ بوده است دقت می شود و هر زوری اعم از عملیات مسلحانه یا غیرآن که موجب مرگ یا خسارت جسمی به اشخاص یا صدمه و تخریب به اشیا باشد با تفسیری موسع ممنوع می گردد .

دیدگاه بعدی حتی با نگاهی وسیع تر فارغ از نگاه ابزار به کار برده شده در جنگ محور ماده را به تاثیرات عمومی تمامی ابزار های استفاده شده منتقل می کند و با نگاه به

نتیجه و آثار حاصل شده از زور ماده ۲ بند ٤ را تفسیر می کند. در این حالت نیز حمله شبیه حمله دینامیکی است لیکن تمرکز اصلی بر تاثیر حمله صورت پذیرفته به کشور دیگر است. به طوری که در این حالت نیز همانند تفسیر موسع در بالا، مبنای حقوقی ماده که اجتناب از نتایج زیانبار خاص است، مد نظر قرار می گیرد.
با توجه به رویکردهای ارائه شده به نظر می رسد که اگر با هرکدام از تفاسیر بالا به سراغ ماده برویم در جایی که دولت ها با آثار شدید خاص که به اندازه کافی موجب آسیب شده باشد می‌توانند به کنارگذاشتن ممنوعیت استفاده از زور استناد نمایند.

۶.منشور ملل متحد و حملات سایبری

همان گونه که در بالا ذکر شد حملات سایبری با توجه به نوع شدت و تاثیری که می توانند بر سیستم های کامپیوتری و سازمان های مرتبط با آن بگذارند و با توجه به دیدگاه های متعدد در خصوص حملات مسلحانه و استفاده از زور همچنین برای بهتر دسته بندی کردن موضوع بعضی از پژوهشگران چندین مدل تحلیلی پیشرفته پیشنهادی برای مقابله با حملات مسلحانه غیر متعارف ، همانند حملات سایبری، در نظر گرفته اند تا با در نظر گرفتن دامنه حمله ، مدت زمان و شدت سنگینی حمله بتوانند به زور اعمال شده استناد کنند و از عملیات دفاعی لازم جهت مقابله استفاده نمایند. به این معنی به بعضی از آن موارد در ذیل اشاره می گردد:
اولین مدل پیشنهادی مدل روش ابزار است، با در نظرگرفتن این موضوع که آیا آسیب های ناشی از روش حمله جدید ، در گذشته نیز می توانست تنها با یک حمله جنبشی به دست آید. به عنوان مثال، در این رویکرد یک حمله سایبری مورد استفاده برای قطع کردن یک شبکه برق حمله مسلحانه است ، به این دلیل که برای انهدام شبکه برق به طور معمول نیاز به پرتاب یک بمب در یک نیروگاه برق و یا استفاده از دیگر ابزار های مکانیکی جهت ازکار افتادن آن شبکه است . از آنجا که مهمات معمولی که قبلا لازم بود برای رسیدن به این نتیجه ، تحت رویکرد ابزار محور است ، پس حمله سایبری نیز ابزار محور می باشد چون همان نتیجه را به بار آورده است.
دومین مدل اثر محور است ، که گاهی به نام رویکرد مبتنی بر نتیجه نیز استفاده می شود، که در اینجا نیز شباهتی میان این حمله و حمله مکانیکی جنبشی وجود ندارد و تمرکز بر تاثیر کلی این حمله است بر روی یک قربانی . به عنوان مثال، در رویکرد مبتنی بر اثر ، یک حمله سایبری سراسری به اطلاعات بانکی و موسسات مالی یک

کشور که به طور جدی مخل تجارت می گردد، حمله مسلحانه است . چراکه اگر چه دستکاری اطلاعات یک حمله مکانیکی نیست ، لیکن باتوجه به اثرات مخرب این حمله بر اقتصاد دولت به اندازه کافی نتیجه شدیدی دارد که آن را همانند یک حمله مسلحانه قرار می دهد.
بدین ترتیب می توان حملات سایبری را فارغ از ابزار مورد استفاده با توجه به شدت اثری که بر سیستم یک کشور دارد با توجه به ماده ۲ بند ٤ زیر مجموعه ای از زور و به طور خاص حمله مسلحانه قرار داد.

۷. تاثیر حملات سایبری بر حقوق بشردوستانه بین‌المللی (jus in bello)

حال به بررسی تاثیرات این نوع حملات بر "حقوق در جنگ"- حقوق بشر دوستانه – می پردازیم، در حقوق بشر دوستانه از آنجایی که فضای حمایتی بیشتری نسبت به افراد و اشیاء غیر نظامی وجود دارد و تلاش بیشتری برای حمایت نسل بشر از بلایای جنگ در حیطه محدودیت ابزار ها و تکنیک های جنگی و یا نوع وسایل کشنده صورت پذیرفته، پیچیدگی مسائل،خود را در مقایسه جنگهای سایبری با فضای موجود به نمایش می گذارد و همانند حقوق جنگ در این جا نیز با نقص تعریف حملات سایبری در کنوانسونهای ژنو و به طور خاص پروتکل الحاقی اول ۱۹۷۷روبرو هستیم . اگر چه که حمله سایبری خودش به تنهایی یک مناقشه مسلحانه نیست اما برای مقابله در نبرد از آن به عنوان ابزار جنگی استفاده می شود. در این بخش به بررسی اصطلاح حمله در حقوق بشر دوستانه و رابطه بین حیطه های سنتی الزامات jus in bello و حملات سایبری که در درگیری های مسلحانه به کار گرفته شده اند، پرداخته می شود. مباحث مربوطه به حوزه خقوق بشر دوستانه در حیطه مفاد کنوانسیون ژنو و هم وزن آن در قواعد عرفی جای دارد.

۷-۱.مفهوم حمله

مفهوم حمله مسلحانه در ‘‘حقوق بر جنگ’’ نبایستی با کاربرد این اصطلاح در حقوق بشردوستانه اشتباه گرفته شود، چرا که در طرف دیگر لفظ حمله در‘‘حقوق در جنگ’’ صف طویلی از حمایتهای حقوقی دیده می شود که به نوعی این ممنوعیت ها و محدودیت ها ناشی از اصل تمایز –از اصول حقوق بشر دوستانه و البته اصول اولیه هستند که جهت راهنمایی در حملات باید مد نظر باشند–است. اصل تمایز در حقوق

بشردوستانه در عملیات نظامی به چشم می خورد، اما واضح است که همه عملیات های نظامی به شکل مکانیکی آن انجام نمی شود، به طور مثال رویه طولانی مدت دولتها اعلام می دارد که عملیات روانی بدون تخریب با هدف غیر نظامیان ، همانند پخش بروشور یا گستردن جمعیت دشمن یا پراکندن عمومی دشمن، مشروع بوده در حالیکه هیچ آثار جسمی را باقی نمی گذارد. اگرچه این اصل در عمل مبحث عملیات نظامی را به حمله بر می گرداند اما بهتر است این اصطلاح در سیاق حقوقی آن نیز دیده شود. واقعیت های مختلفی در سیاق مباحث مطرح شده در پروتکل از بحث مزبور حمایت می کند، اگر خوب دقت شود اصل تمایز ناشی از ماده ٤٨ پروتکل اول الحاقی ، در بخش " قواعد اساسی و نحوه اجرا "بخش راهبردی مخاصمات معاهده ظاهر می شود. در حالیکه ماده دیگر که ماده ٤٩ است حمله را تعریف می کند، در نتیجه این جایگاه به طور ضمنی منظور از عملیات نظامی ماده ٤٨ را به حمله بر می گرداند.

علاوه بر آن مواد بعدی نیز به نحوی دیگر از بحث تفکیک حمله به غیر نظامیان و نظامیان صحبت می کند.[١٦] به نحوی که دلالت ضمنی بر مفهوم ممنوعیت حمله علیه غیرنظامیان با عنوان هدایت عملیات نظامی در مفهوم ، عمومی ، حقوقی است.

نتیجه ای که از این سوال ایجاد می شود این است که حمله چیست ؛ کلید حل مساله در خود ماده ٤٩ است. در بخش تفسیر پروتکل الحاقی اول عبارت "عمل تجاوز"به معنای زور فیزیکی است. در نتیجه ، مفهوم حمله شامل انتشار تبلیغات ، تحریم ، یا دیگر ابزار های غیر مادی یا روانی یا اقتصادی جنگی نیست.

در کنفرانس دیپلماتیک برای تدوین پروتکل کمیته بین المللی صلیب سرخ به طور مشابه عبارت "حمله به معنی عملیات رزمی"آورده می شود. مساله اصلی بعد از تعریف حمله شناخت عملیات سایبری است که به طور واضح و آشکار نیروی تهاجمی نیستند. در این خصوص باید دید در چه زمان و چه حالتی عملیات سایبری از نظر کیفی در زمره حملات حقوق بین المللی بشردوستانه است تا ممنوعیت ها و محدودیت های این حقوق در مورد آن بکار برده شود.

همانگونه که در مباحث منشور نیز دیده می شود، استفاده از اجبار بدون نمایش ظاهری از آن ، فرای تفکر نویسندگان پروتکل الحاقی ۱۹۷۷ بوده است. لیکن نزدیک به نیم قرن قبل، باغیر قانونی اعلام کردن استفاده از تسلیحات شیمیایی و بیولوژیکی برای طرفین مخاصمه ، در پروتکل گاز ۱۹۲۵و تصدیق این اعمال به عنوان حمله به واسطه

آثار تخریبی که موجب می شد ،گامی به سمت جلو گذاشته می شود. در نتیجه با همین منطق می توان اعمال تهاجمی دیگر را نیز که آثاری مخرب را موجب می شود ممنوع اعلام کرد.

بعلاوه ، همانطور که بیان شد معاهدات باید در سیاق و در پرتو موضوع و هدف تفسیرشود.یک معنای دقیق ممنوعیت و محدودیت موجود در حملات پروتکل الحاقی اول نشان می دهد که در خصوص اعمالی که تهاجمند نگرانی زیادی وجود تدارد ، بلکه موضوع نتایج زیانباری است که از تهاجمات ناشی می شود، یا به عبارت دیگر آثار تهاجم نگران کننده تر است و تا حد ممکن در پرتو ضرورت نظامی در بخش عظیمی از معاهدات ، موضوع و هدف آنها اجتناب کردن از رفتارهایی هست که آثار مخرب دارند . برای مثال غیرنظامیان از حمایت علیه خطرهای ناشی شده از عملیات نظامی بهره می برند و اعمالی که قصد ترساندن جمعیت غیر نظامی را دارند ، ممنوع هستند.یا در قاعده تناسب، هر عملی را در پرتو زیان وارده به زندگی غیر نظامیان، صدمه یا خسارت به آشیای آنها و یا ترکیبی از آنها ارزیابی می کند. هم چنین احتیاط هایی که لازم است در زمان هدایت حمله انجام شوند، شامل انتخاب اسلحه و تاکتیکها با بررسی ورود کمترین خسارت به جمعیت نظامی است ، برگرداندن پرتابها، معلق کردن و منحل کردن حملات که می توند خسارات وسیعی را موجب شود ، منتج به اخطار می شوند.این رویکرد نتیجه محور /آثار محور در حمایت از اشیا نیز به طور خاص کاربرد دارد به نحوی که محدودیت در هدایت حملات علیه سدها،آب بندها و جایگاههای ژنراتورهای هسته ای که خسارات شدیدی را در میان جمعیت نظامی موجب می شود و ممنوعیت در استفاده از متدها و وسایل جنگ افروزی بطوری که به طور گسترده و طولانی مدت و شدید خساراتی را به محیط طبیعی و در نتیجه سلامت جانداران و مردم و مردم ایجاد کند، ممنوع است.

حقوق بشردوستانه بین المللی علیرغم انتخاب یک مبنای ابزارمحور در تعریف حمله ، واضح است که در برخورد عملیاتی با موضوع ، رویکردی با مبنای نتیجه گرا دارد. بیانیه های مربوط به ماده ٤٩ این نتیجه را موید ارجاع به این رویکرد عملیات نظامی می دانند که بیشترین هدف، جلوگیری از تاثیرات مستقیم جهت امنیت بیشتر جمعیت غیرنظامیان و تمامیت اشیای مرتبط به آنها است و بدین ترتیب درطول این فرایند استقرایی، می توان نتیجه گرفت اصول کلی در ارتباط با مفهوم حمله وجود دارد که در سیاق سایبری قابل باز تعریف است.

در نتیجه ، تجزیه حقوقی حملات در فضای حقوق بین المللی بشردوستانه نتایج یکسانی را در حقوق در جنگ به وجود می آورد .اگرچه پارامترهای دقیقی برای استفاده در عمل در هر مورد وجود دارد.

بدین معنا عملیات سایبری می تواند مستقیما بر سیستم های غیر نظامی، مادامی که نوع ضروری از خسارت هدف گیری نشده و هیچ ممنوعیت کاربردی خاص دیگری وجود ندارد، هدف گیری شود.

بعد از بررسی لفظ حملات سایبری در سیاق حقوق بین المللی بشردوستانه به بررسی تاثیرات این حملات بر دیگر اصول اساسی در این قسم از حقوق پرداخته می شود.

۷-۲.ضرورت، تناسب ، تمایز و بی‌طرفی

شرایط جدید جنگ سایبری چالش های جدیدی را برای استفاده از قواعد عرفی حقوق بشر دوستانه مانند ضرورت ، تناسب ، تمایز و بی طرفی در بردارد. به عبارت دیگر در اصول اساسی حقوق بشر دوستانه بین المللی در برخورد با حملات سایبری با مشکل مواجه هستیم. از آنجا که حملات سایبری اغلب بلافاصله کشنده و یا مخرب نیستند و ممکن است تنها نقص موقتی در سیستم های شبکه ایجاد کنند، ارزیابی این که آیاحمله سایبری متناسب است یا نه به سختی ممکن می گردد. از طرف دیگر تمایز بین نظامیان ، افراد غیر نظامی که به طور مستقیم در جنگ شرکت کرده اند ، افراد غیر نظامی درگیر در یک مبارزه مداوم اساسی، و افراد غیر نظامی حفاظت شده در زمینه حملات سایبری غیر ممکن بوده و در نهایت، پوشیده بودن منبع حملای سایبری اجرای وظایف بی طرفی را پیچیده تر می کند.

مباحث راجع به **ضرورت** مختص حملات سایبری نیست و درکل در هر حمله ای، اگر ضرورت آن حمله در بتن حملات برای رسیدن به اهداف نظامی لازم باشد، این حمله مشروع است و در غیر این صورت هر قسمت از حمله که به صورت جزئی برای رسیدن با اهداف نظامی ضروری نباشد، غیر مشروع است.

در خصوص ممنوعیت های مطرح در **تناسب** در حمله نیز در جایی که حمله ای باعث از دست رفتن زندگی غیر نظامیان ، صدمه به آنها، آسیب به اشیاء غیر نظامی، و یا ترکیبی از آن بیش از منافع و مزیت های جنگی پیش بینی شده باشد، حمله مزبور را ممنوع می دانند. در تجزیه و تحلیل تناسب باید این موضوع را در نظر گرفت که یک تصمیم گیرنده نظامی در سنجیدن تلفات بالقوه غیر نظامی، تخریب اموال غیر نظامی، و

از دست دادن موارد غیر نظامی ضروری جهت رسیدن به اهداف نظـامی افـراط نکـرده باشد. در اینجا در مباحث مربوط به حمـلات سـایبری در سـنجش تناسـب بـا چالشـی منحصر به فرد روبرو هستیم . ارزیابی اینکه آیا یک حمله را می توان با توجه بـه دسـته بندی های مربوط به افرادو اشیاء به عنوان اثر مستقیم نمونه ای از حملات سایبری غیـر کشنده موقت یا شدید در نظرگرفت بسیار سخت است . علاوه بـر ایـن ، چگونـه مـی توان عدم توانایی موقت سیستم های حیاتی را ارزیابی کرد؟ به عنوان مثـال، تناسـب در حملات سایبری که به طور موثر انتقال اطلاعات از طریق اینترنت را متوقف و منجر بـه نارضایتی عمومی می شود را نمی توان با تاثیری که در بیمارستان جهت توقف برقراری ارتباط اطلاعات حیاتی منجر به از دست دادن زندگی افـراد مـی شـود مقایسـه نمـود . درکل تجزیه و تحلیل تناسب نیازمنـد پـیش بینـی عواقـب احتمـالی حمـلات صـورت پذیرفته است ، که در حملات سایبری این موضوع یا به سختی ممکـن مـی شـود و یـا حتی غیر ممکن است بـه طوریکـه تـاثیر ایـن حمـلات را هـم وزن تـاثیرات حمـلات مکانیکی که در آن از مواد شیمیایی و بیولـوژیکی اسـتفاده شـده و اثـرات موقـت غیـر کشنده دارد، در نظر می گیرند.

قاعده **تمایز**، یکی دیگر از چالش های بزرگ در ارزیابی قانونی بودن حملات سـایبری را به نمایش می گذارد این اصل مدعی تمایز بین افراد و اشیاءنظامی و غیر آنها و هدف قرار دادن نظامیان در فضای جنگ اسـت، همچنـین فرمانـدهان نظـامی بایـد از ابـزاری استفاده کنند تا در حملات به طور صـحیح میـان افـراد و اشـیاء نظـامی و غیـر نظـامی تفکیک کند و به عبارت بهتر حقوق بشر دوستانه حملات سایبری را که بـدون کنتـرل ، بدون پیش بینی یا بدون تمایز میان افراد و اشیاء نظامی و غیر نظامیان اتفـاق بیفتـد منـع کرده است. در بعضی از مصادیق شرایطی وجود دارد که حملات سایبری مشروع است چرا که هدف درآن مشخصا افراد نظامی هستند و اصل تمـایز قابـل اجـرا اسـت ماننـد زمانی که یک سیستم کنترل ترافیک هوایی نظامی هدف حمله سایبری قرار بگیرد و این حمله مانع حمل ونقل نیروهای نظامی گردد. به طور مشابه اعمالی نیـز وجـود دارد کـه در آن به آسانی حملات سایبری غیر قانونی است، مانند حمله به برخی از اهداف ماننـد بیمارستان ها، موزه ها، و مکان های عبادت، این مکانها حتـی اگـر جزئـی از اهـداف و منافع حملات نظامی نیز به حسـاب آینـد بـاز هـم از حمایـت لازم برخوردارنـد. البتـه همیشه مسائل به این سادگی نیست گذشته از این حمایت سـنتی از اشـیای ذکـر شـده، تجزیه و تحلیل پیچیده ای در زمینه حملات سایبری به وقوع مـی پیونـدد چـرا کـه در آنجا که حملات در فضای مجازی به وقوع می پیوندد و به طور قطع حملـه بـه شـبکه

های هدایت کننده مکانهای ذکر شده نیز باید غیر قانونی باشد اما به دلیل کثـرت تعـدد بازیگران نظامی و غیر نظامی ، احتمال استفاده از این اهداف به ظاهر غیرنظـامی توسـط نظامیان افزایش می یابد و به دلیل کاربرد دوگانه موضوع، حمایت مورد نیـاز در بحـث تمایز اتفاق نمی افتد.

قاعده **بی طرفی** وضعیتی است که دولت می تواند به صورت دائمی ، همانند سـوئیس، و یا موقت ، در یک زمان خاص از مخاصمه ، نسبت به شرایط جنگ اعلام بـی طرفـی نماید و به تبع آن دارای حقوق و مسئولیت هایی می گردد.

چالش ها در ارزیابی قانونی بودن حملات سایبری در جایی به چشم می خـورد کـه از سرزمین کشور بی طرف جهت حملات سایبری استفاده گردد، بـدین ترتیـب برخـی از محققان استدلال می کنند که کشورهای بی طرف موظف بـه توقـف طـرفین درگیـر در استفاده از امکانات ارتباطی جهت حمـلات سـایبری نیسـتند لـیکن در ایـن خصـوص کمکی نیز جهت استفاده از امکانـات نبایـد صـورت پـذیرد، در مقابـل گروهـی دیگـر استدلال می کنند که کشورهای بی طرف باید، برای متوقف کردن حمله نشأت گرفته از خاک خود ، اقدام نمایند و در غیر این صورت مسئول استفاده غیـر قـانونی از زور مـی باشند.

ویژگی های خاص حملات سایبری ارزیابی اصل بی طرفی را به طـور غیـر منتظـره ای پیچیده می نماید. حملات سایبری ممکن است کامپیوترهای واقع در یک کشـور دیگـر را برای آسیب رساندن به شبکه در کشور ثالث بدون آگاهی کشـور منشـاء مـدعی بـی طرفی استفاده نمایند. در چنین حملاتی به سختی می توان اصل بی طرفـی را تجزیـه و تحلیل کرد، چرا که نخست کشورمنشاء مدعی بی طرفی نمی داند ممکن است رایانه ها و سرورهایش برای یک حمله سایبری استفاده شود، و بنابراین ممکن است بـی طرفـی اش در معرض تهدید قرار گیرد و دوم، به عنـوان اصـل بـی طرفـی، پاسـخ قـانونی بـه حملات بر اساس هویت،کشور مبدا باید مشخص باشد که این امکان پـذیر نیسـت. بـه هر حال وضوح بیشترقواعد در اطراف چارچوب حـاکم بـر حمـلات سـایبری، ممکـن است موانع را به نسبت کاهش دهد.

۸.نتیجه گیری

فضای سایبری فضایی اینترنتی که در ان کشورها بسیاری از داده های اطلاعاتی خـود را جهت انجام امور کشوری ونظامی خود به صورت نهان و حتی در برخیم وارد غیر قابل دسترس قرار می دهند. جنگ نرم اصصطلاحی است کـه در دنیـای امـروز در حمـلات کشورها بر علیه یکدیگر در این فضا رخ می دهد. حملات سایبری چالشـهای جدیـدی

در حیطه اصول حقوق بشر دوستانه ایجاد می کنـد . بیشـتر حمـلات سـایبری موجـب ایجاد ناتوانی موقت در برآورد کردن نتایج حمله می گردد و ارزیـابی اینکـه آیـا حملـه سایبری متناسب بوده یا نه را سخت می کند، استفاده دوگانه از زیرساخت های اینترنتی و مشارکت بالقوه غیر نظامیان به همراه نظامیان تمایز بین آنهـا را در حمـلات سـایبری پیچیده کرده و در نهایت، استفاده از کامپیوترهای زامبـی و سـرورهای میزبـان سـوالات بسیاری را در مورد حقوق و تعهدات کشورهای بی طرف ایجاد مـی نمایـد. چـارچوب قوانین موجود جنگی شامل هر دو حیطه jus in bello -jus ad bellum ،بعضی راهنمایی های کوچک را برای دولت ها جهت پاسخ به حملات سایبری فراهم مـی کنـد . امـا از آنجا که اکثریت قریب به اتفاق حملات سایبر دسته بندی نشده اند، نیروی مسلح اغلب یک واکنش غیر قانونی و یا در بسیاری موارد نامناسب به حمـلات سـایبری نشـان مـی دهند. بسیاری از حملات سایبری مخرب به دلیل نامعلوم بودن شخص حمله کننـده در کل جنگ سایبری تلقی نمی شوند. با همـه ایـن احـوال محـدودیت در قـوانین جنگـی حاضر لزوما به معنی عدم امکان تنظیم حملات سایبری نمـی باشـد و چـارچوب هـای دیگر قانونی برای پرکردن این شکاف تا تدوین یا اصلاح قوانین جنگی وجـود دارد. دم تدوین قوانین متناسب در مورد تخاصم سایبری موجب تفسیر نوعه حملـه و تحلیـل ان برکنوانسیون های چهارگانه و الحاقات ان می باشد در حالی که بسـیاری از ایـن قواعـد در مورد خملات مسلحانه می باشد که متاسفانه هـر چنـد مقصـود از تخاصـم سـایبری ورود آسیب به اماکن ودستگاه های حساس و استراتژی کشور مورد حمله می باشد امـا اغلب منافع و اموال غیر نظامیان مورد آسیب قرار می گیرد.

۱. سایبر واژه ای یونانی‌تبار است به معنای سکاندار و راهنما. امروزه این کلمه به معنـی مجـــــازی بکـــــار میـــــرود دانشـــــنامه ویکـــــی پـــــدیا http://fa.wikipedia.org/wiki/%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1

۲. سایبرنتیک، علم مطالعه و کنتـرل مکـانیزم‌هـا در سیسـتم‌هـای انسـانی ، ماشـینی (و کامپیوتر ها) است. واژه "فضای سایبر" را نخسـتین بـار "ویلیـام گیبسـون William) " (Gibsonنویسنده‌ی داستان علمی تخیلی در کتاب "نورومونسـر (Neuromoncer) "در سال ۱۹۸٤ به‌کار برده است.فضای سایبر (Cyberspace) در معنـا بـه مجموعـه‌هـایی از ارتباطات درونی انسانها از طریق کـامپیوتر و مسـائل مخـابراتی بـدون در نظـر گـرفتن جغرافیای فیزیکی گفته می‌شود. یک سیستم آن لاین نمونه ای از فضای سایبر است کـه کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط بـر قرارکننـد. بـر خـلاف فضـای

واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه‌ی اعمال فقط از طریق فشردن کلیدها یا حرکات "ماوس" صورت می‌گیرد . این عدم جابجایی فیزیکی ، محققان را واداشت که به مطالعه برخی شباهت‌های فضای سایبر با حالت‌های ناهوشیاری، به‌خصوص حالت‌های ذهنی‌ای که در رویاها ظاهر می‌شوند، بپردازند. آنان با الهام از گفته‌های یکی از رهبران بزرگ" ذن" به نام "چانگ تزو (Chuang Tzu) " برای تحقیقات خود در زمینه کشف شباهت‌هایی بین فضای سایبر و رویا بهره جسته اند. گفته می‌شود که":چانگ تزو شبی در خواب می بیند که پروانه شده است . وقتی بیدار می‌شود با خود می‌اندیشد: آیا من مردی هستم که خواب می‌بیند "پروانه" شده است؛ یا اینکه پروانه‌ای هستم که اکنون خواب می‌بیند یک" مرد" شده است".روند کاری یک کاربر کامپیوتر در فضای سایبر دقیقاً نوعی یکی شدن یا محو شدن در درون واقعیتی متفاوت یعنی واقعیتی مجازی است که ورای قوانین و واقعیت‌های واقعی است. مانند یک رهبر ذن در هنگام مدیتیشن که با محیط اطراف خود به وحدت می‌رسد، کاربر کامپیوتر هم در هنگام کار در فضای مجازی با آن یکی می‌شود.شما تقریباً بی حرکت و آرام می‌نشینید، چشمانتان روی پرده‌ای درخشان خیره می‌شود، اتاق کاملاً تاریک است، تنها منبع نور در درون شما است در حالیکه همه توجه و ذهنتان بر کلمات و تصاویر این پرده درخشان متمرکز است. انگشتانتان کلیدهای کی بورد را می‌نوازد. در این لحظه دوست دارید با ذهنیات و تصورات خود یگانه شوید. مرز بین دنیای درون و بیرون تقریباً ناپدید می‌شود و دیگر گذر زمان معنایی ندارد.البته این سناریوی هر روز کاربران کامپیوتر نیست. زیرا اغلب اوقات ما صرفاً به جهت انجام کاری مشخص و بدون آنکه به درون جهان مجازی فرو رویم به صفحه کلید ضربه می‌زنیم اما اگر از استفاده‌های دم دستی کامپیوتر صرف نظر کنیم و از کاربران حرفه‌ایی و پروپاقرص کامپیوتر پرس و جو کنیم، درخواهیم یافت که بسیاری از آن ها به راحتی لحظاتی را به یاد می‌آورند که گویی هیچ حائل و فاصله‌ای بین خود و کامپیوترشان احساس نمی کردند.در واقع می‌توان گفت که فضای سایبر گستره‌ایی از ذهن است که می‌تواند تمامی اشکال زندگی منطقی را بسط و معنا دهد. شما می‌توانید حالت‌های متنوع و متفاوت ذهنی را از قبیل تخیلات، خیال‌پردازی‌ها، خیال‌پروری‌ها، توهمات، حالات هیپنوتیستیک و سطوح گوناگونی از هوشیاری را در فضای مجازی تجربه کنید. تحت این چنین شرایط است که فضای سایبر همانند دنیای "رویا" می‌شود. دنیایی که وقتی ما به خواب فرو می‌رویم، پدیدار می‌شود. در واقع همانگونه که علم روانشناسی

خواب شبانه را برای حفظ سلامتی، توسعه‌ی عاطفی و رشد شخصیت یک فرد ضروری می‌داند، این فضای مجازی هم بیش از هر چیز دیگری در خدمت روان انسان است. زیرا مرزهای بین واقعیت‌های آگاهانه و ناآگاهانه را به هم نزدیک کرده است و می‌تواند درباره‌ی معنای "واقعیت "چیزهایی به ما بگوید.محیط" پلس Palace "یک محیط چت گرافیکی است که ما برای این تحقیق آن را انتخاب کرده‌ایم. کاربران در این محیط می‌توانند برای برقراری ارتباط با دیگران از بین صورتک‌های گرافیکی موجود در آن محیط، یک یا چند صورتک را برای بازنمایی شخص خود انتخاب کنند. این صورتک‌ها هر یک موقعیت یا حالت روانی خاصی را بیان می‌کند. بعضی از این حالت‌های "رویاگونه" در محیط "پلس" را می‌توان در دیگر فضاهای مجازی هم پیدا کرد. ولی تعدادی از این حالت‌های تنها در محیط " پلس" وجود دارند و کاملاً بی نظیر و خاص هستند.مهم‌تر از همه این است که محیط ، در فضای اینترنت مانند رویا بسیار مجذوب کننده است. این بدان خاطر است که این محیط یک " تجربه بصری" جدی است. یک مثل قدیمی می گوید : «یک "تصویر" با ارزش‌تر از هزاران "کلمه" است .» علم روانشناسی هم تجربه بصری را تجربه‌ای بسیار غنی، و تصاویر و نمادها را زبان ناآگاهانه می‌نامد.برای درک و آشنایی بیشتر با این "تجربه‌ی بصری" باید از دیدگاه روان‌شناسی خواب، رویا و رویا بینی را مورد توجه قرار داد.

http://www.ehsanionline.com/fa/index.php?option=com_content&view=article&id=164:1389-11-19-18-24-05&catid=62:farhng-va-honar&Itemid=102

۳. فضای سایبر ، فضایی غیر مادی و ناملموس است که توسط رایانه ها و شبکه های رایانه ای به وجود آمده و دنیایی مجازی را در کنار دنیای واقعی ایجاد نموده است .این فضا، فراتر از اینترنت توسعه یافته است و تمامی فعالیت های دیجیتال شبکه ای را در بر می گیرد: فضای مذکورد ارای گستره ای جهانی و بدون مرز ، پوشیده و پنها ن، ناهنجارمند و کنترل ناپذیر است .فضای سایبر ماهیتاً برای آزادی گردش اطلاعات شکل گرفته و محدودیت در این فضا معنا ندارد.

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, THE LAW OF CYBER-ATTACK, Forthcoming in the California Law Review, 2012,p7

٤.حملات سایبری در چارچوب عملیات اطلاعاتی، قرار میگیرند عملیات اطلاعاتی که« جنگ اطلاعاتی نیز زیر مجموعه ای از آن است و هنگام مخاصمه ی مسلحانه به

آن متوسل میشود،عبارت است از به کارگیری منسجم توانمند یهای جنگ الکترونیکی، عملیات شبکه ای رایانه ای ، عملیات روانی، حیله های نظامی و عملیات هماهنگ با قابلیت های پشتیبانی است که به منظور تأثیرگذاری، متوقف نمودن،تخریب یا سرقت اطلاعات دشمن و در عین حال پشتیبانی از فرایندهای تصمیم گیری نهادهای ملی صورت میگیرد.

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, THE LAW OF CYBER-ATTACK, Forthcoming in the California Law Review, 2012,p10

۵. برگرفته از مقاله

Herbert Lin, Cyber conflict and international humanitarian law, international review of red cross, Volume 94 Number 886 Summer 2012,p517-518

٦. رایاجنگ، نبرد مجازی، یا جنگ سایبری Cyberwarfare یا cyber War، به نوعی از نبرد اطلاق می‌گردد که طرفین جنگ در آن از رایانه و شبکه‌های رایانه‌ای به خصوص شبکه اینترنت به عنوان ابزار استفاده کرده و نبرد را در فضای مجازی جاری می‌سازند.جنگ اطلاعاتی با انقلاب اطلاعات ظهور پیدا کرده‌است. این انقلاب به دلیل دامنه وسیع و تاثیرات گسترده آن می‌تواند سبک نوینی از جنگ را ارائه بدهد.مارتین لیبیکی، از محققان برجسته موسسه مطالعات استراتژیک در دانشگاه دفاع ملی، در کتاب «جنگ اطلاعاتی چیست؟» می‌نویسد «تلاش برای درک مفهوم جنگ اطلاعاتی مانند این است که چند نفر نابینا بخواهند با لمس کردن بخش‌های مختلف یک فیل بگویند که این موجود چیست. جنگ اطلاعاتی نیز شامل بخش‌های مختلف و متعددی میشود.» تلاش برایداشن نگرش جامعه نگرانه در تعریف جنگ اطلاعات نکته ایست که باید حتماً به آن توجه شود.مگان برنز در سال ۱۹۹۹ با نگرشی کلی تریف زیر را ارئه می‌دهد «جنگ اطلاعاتی طبقه یا مجموع‌های از تکنیک‌ها شامل جمع آوری، انتقال، حفاظت، ممانعت از دسترسی، ایجاد اغتشاش و افت کیفیت در اطلاعات است که از طریق آن یکی از طرفین درگیر بر دشمنان خود به مزیتی چشمگیر دست یافته و آن را حفظ می‌کند.»مارتین لیبیکی ضمن وفادارماندن به تعریف کاملاً نظامی از جنگ اطلاعاتی هفت شکل مختلف جنگ اطلاعاتی را به شرح زیر نام می‌برد:

جنگ فرماندهی و کنترل که هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن، است؛جنگ برپایه اطلاعات که متشکل از طراحی، حفاظت و ممانعت از

دسترسی به سیستم هائی است که برای برتری بر فضای نبرد در جستجوی دانش کـافی هستند،جنگ الکترونیک تکنیک‌های رادیوئی، الکترونیک، یا رمزنگاری؛جنگ روانی کـه در آن از اطلاعات برای تغییر ذهنیت و طرزفکر دوستان، بی طرف‌ها، و دشمنان استفاده می‌شود؛جنگ هکرها که در آن به سیستم‌های رایانه‌ای حمله می‌شود؛
جنگ اطلاعاتی اقتصادی ایجاد مانع در برابر اطلاعات یـا تسـهیل جریـان اطلاعـات بـا هدف کسب برتری اقتصادی؛جنگ سایبر ترکیبی از همه موارد شش گانه بالا.
انواع نفوذ گران در جنگ سایبر:
White hat hackers؛گروه نفوذگران کلاه سفید هر کس که بتواند ازسد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه‌ای انجام ندهد را یـک هکـر کـلاه سـفید مـی‌خواننـد. هکرهای کلاه سفید متخصصین شبکه‌ای هستند که چاله‌های امنیتی شبکه را پیدا میکنند و به مسوولان گزارش می‌دهند.
Black hat hackers؛گروه نفوذگران کلاه سیاه اشخاصی هستند که وارد کامپیوتر قربـانی خود شده و به دستبرد اطلاعات و یا جاسوسی کردن و یا پخش کردن ویروس و غیـره می‌پردازند.
Gray hat hackers؛گروه نفوذگران کلاه خاکستری اشخاصی هستند کـه حـد وسـط دو تعریف بالا می‌شوند.
Pink hat hackers؛گروه نفوذگران کلاه صورتی این افراد آدم‌های کم سوادی هستند کـه با چند نرم‌افزار خرابکارانه به آزار و اذیت بقیه اقدام می‌کننـد. گـروه نفـوذ گـران کـلاه قرمزعده ای متخصص که اطلاعاتی نادرست را به شبکه های اینترنت وارد می کنند
انواع حملات نفوذگران؛شنود یاinterception ،در این روش نفوذ گر می‌تواند بـه شـکل مخفیانه از اطلاعات نسخه برداری کند.
تغییر اطلاعات یاmodification ؛در این روش نفوذگر بـه دسـتکاری و تغییـر اطلاعـات می‌پردازد.
افزودن اطلاعات یاfabrication ؛در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می‌کند.
وقفهinterruption ؛در این روش نوع نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود؛
http://fa.wikipedia.org/wiki/%D8%AC%D9%86%DA%AF_%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C

همچنین مقالات....

۷. حملات سایبری عبارت است از تغییر یا نابودی اطلاعات موجود در رایانه های هدف یا شبکه ی رایانه ای و به منظور ازکار انداختن سیستم کنترل و ارتباطات فرماندهی دشمن و وارد کردن خسارات خارج از شبکه ی رایانه ای با هدف سیاسی و امنیت ملی انجام میگیرد

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, THE LAW OF CYBER-ATTACK, Forthcoming in the California Law Review, 2012,p10-12

۸. از مقاله Herbert Lin, Cyber conflict and international humanitarian law و Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)

*مفهوم تجاوز در حقوق بین الملل http://www.ghavanin.ir/PaperDetail.asp?id=938

،

۹. البته این تعریف کلمه تهدید را ذکر نکرده ولی از آنجایی که این قطعنامه برای شورای امنیت به عنوان تنها مرجع صالح برای تشخیص تجاوز الزام آور نمی‌باشد و تنها جنبه راهنمایی دارد شورا می‌تواند بند ٤ ماده ۲ منشور سازمان ملل متّحد را نیز مستند قرارداده و تهدید را نیز جزو تجاوز به حساب آورد.

۱۰. البته این تعریف کلمه تهدید را ذکر نکرده ولی از آنجایی که این قطعنامه برای شورای امنیت به عنوان تنها مرجع صالح برای تشخیص تجاوز الزام آور نمی‌باشد و تنها جنبه راهنمایی دارد شورا می‌تواند بند ٤ ماده ۲ منشور سازمان ملل متّحد را نیز مستند قرارداده و تهدید را نیز جزو تجاوز به حساب آورد.

۱۱. در مورد بند آغازین ماده ۳ این نکته حائز اهمیت است که کیفیت تجاوزکارانه یک اقدام را به ((اعلان جنگ)) وابسته نمی گرداند؛ زیرا جنگهای امروزین بدون اعلان رسمی آغاز می شوند.

۱۲. بندهای هفتگانه ماده ۳ قطعنامه تعریف تجاوز: الف – تهاجم یا حمله نیروهای مسلح یک دولت به سرزمین دولتی دیگر، یا هرگونه اشغال نظامی، هرچند موقت، ناشی از چنان تهاجم یا حمله ای، یا هرگونه ضمیمه سازی سرزمین یک دولت یا قسمتی از آن با استفاده از زور...))

ب- بمباران سرزمین یک دولت توسط نیروهای مسلح دولتی دیگر، یا کاربرد هر نوع سلاح توسط یک دولت علیه سرزمین دولتی دیگر...))
پ-محاصره بنادر یا سواحل یک دولت توسط نیروهای مسلح دولتی دیگر...
ت-((حمله نیروهای مسلح یک دولت به نیروهای زمینی، دریائی یا هوائی، یا ناوگانهای هوائی و دریائی دولتی دیگر...))
ث-ستفادهٔ یک دولت از نیروهای مسلّح، مغایر با شرایط مورد توافق با دولتی دیگر که در سرزمین آن مستقّر شدهاند، یا ادامهٔ حضور آن نیروها در این سرزمین پس از پایان مورد توافق...»
ج-«اجاره یک دولت برای استفاده از سرزمینش که در اختیار دولتی دیگر قرار داده است بمنظور انجام اقدامی تجاوزکارانه علیه دولیتی ثالث...»
چ-«اعزام دسته ها، گروهها، نیروعای نامنظّم یا مزدوران مسلح توسط یا از جانب یک دولت بمنظور انجام عملیات مسلّحانه علیه دولتی دیگر با آنچنان شدتی که در زمرهٔ اقدامات فهرست شدهٔ بالا قرار گیرند، یا درگیر شدن قابل ملاحظهٔ دولت مزبور در آن عملیات ...»

۱۳. پس از ارائه تعریفی کلی از تجاوز و تعیین اقدامات دارای کیفیت تجاوز، موضوع تشخیص و آثار حقوقی تجاوز مطرح میگردد.معیارهای تشخیص تجاوز و رکن مسئول تشخیص آن در مادّهٔ ۲ تعریف تجاوز آمده است که مقرر میدارد:«پیشدستی یک دولت در کاربرد نیروی مسلح مغایر با منشور، نشانهٔ اولیهٔ اقدامی تجاوزکارانه به شمار خواهد آمد، گرچه شورای امنیّت طبق منشور می تواند نتیجه بگیرد که احراز وقوع تجاوز با توجّه به دیگر شرایط مربوط از جمله کافی نبودن شدّت اقدامات بعمل آمده یا نتایج آنها، قابل توجیه نیست»عبارت سازی مادّهٔ ۲ آشکار می سازد که تدوین کنندگان آن با مشکلات فراوانی روبرو بوده اند. از همان آغاز کوشش برای تعریف تجاوز، دو طرز تلقّی عمده در تشخیص تجاوز وجود داشت: در یکسو برخی از دولتها مانند شوروی برای قبولاندن اصل پیشدستی تلاش میکردند. از نظر آنها متجاوز دولتی بود که ابتدا به یکی از اقدامات منع شده متوسل میشد. در سوی دیگر، دولتهایی بودند که اصل پیشدستی را نمی پذیرفتند و بر اهمیّت نیّت تجاوزکارانه تأکید داشتند. از این گروه میتوان به فرانسه، ایالات متّحده و بریتانیا اشاره کرد. بسیاری از دولتها نیز خواهان سازش میان این دو طرز تلقی بودند.دولتهای طرفدار اصل پیشدستی، تقدم در کاربرد نیروی مسلح توسط یک دولت علیه دولت دیگر را برای تجاوزکارانه دانستن یک اقدام

کافی میدانستند. طرفداران نیت تجاوزکارانه نیز در مقابل، استدلال میکردند که غالباً تشخیص پیشدستی در مبادرت به اقدامی تجاوزکارانه ناممکن است و پیشدستی در کاربرد نیروی مسلح در حد ناچیز، امکان دارد بهانهٔ اقدام تلافی جویانه در حد وسیع قرار گیرد. منطقی نیست که در عصر اتم دولتی در معرض نابودی قرار گیرد به صرف اینکه دولتی که نیت تجاوزکارانه دارد هنوز دست به اقدام نزده است .طرفداران اصل پیشدستی در پاسخ به جانبداران نیت تجاوزکارانه استدلال میکردند که اثبات نیت ممکن نیست و معیار قراردادن آن، فشاری غیر منطقی بر قربانی تجاوز تحمیل میکند.در پی این استدلالهای دور از هم، کوشش برای سازش دو طرز تلقی آغاز شد .بنابر این پیشنهاد گردید که پیشدستی در کاربرد نیروی مسلح «مغایر با منشور»، نشانهٔ اولیهٔ تجاوز به شمار رود و به شورای امنیت اختیار داده شود تا «دیگر شرایط مربوط» را در نظر گیرد. عبارت «دیگر شرایط مربوط» چنان گسترده و مبهم بود که اجازهٔ تفسیر مقاصد و نیات طرفها را میداد. بعلاوه، شایان ذکر است که وجود «نشانهٔ اولیه» به معنای دلیل تجاوز نیست، بلکه فقط یک نشانه است و شورای امنیت باید با درنظر گرفتن این نشانه تجاوز را تشخیص دهد. شورای امنیت در این تشخیص علاوه بر «توجه به دیگر شرایط مربوط» باید «شدت اقدامات به عمل آمده یا نتایج آنها» را نیز در نظر گیرد .به دیگر سخن، باید حداقلی برای شدت و اقدامات به عمل آمده وجود داشته باشد.ماده ۲ در واقع مادّهٔ اساسی تعریف تجاوز به شمار میرود . به شورای امنیت اختیار کامل میدهد که رغم تفسیرهای مختلف طرفهای یک مورد تجاوز، تصمیم بگیرد که آیا تجاوزی رخ داده است یا خیر و در این تصمیم گیری، همهٔ جنبه هایی را که از تفسیر این مادّه ناشی میشود مورد توجه قرار دهدالبته با توجه به عدم احصای موارد تجاوز باید این موضوع را مد نظر داشته باشیم که شورا در تعیین و تشخیص موارد تجاوز کاملاً مختار است و از آنجایی که این قطعنامه وظیفه‌ای را بر عهده شورای امنیت نمی‌گذارد و شورای امنیت در رعایت و یا عدم رعایت آن مختار است. به عبارت دیگر حتّی می‌تواند مواردی نظیر تروریسم ، هواپیما ربایی و حتّی کودتا را نیز از مصادیق تجاوز محسوب نماید.مشکلی که در عمل وجود دارد این است که شورای امنیت گاهی از توصیف قضیه به عنوان تجاوز خودداری کرده و به صورت درستی آن را توصیف نکرده است، به خصوص در مورد تجاوز، به جهت مسؤولیت‌های‌مدنی و بین‌المللی که ممکن است برای دولت متجاوز وجود داشته باشد. اما در نهایت همان طور که گفته شد مواد یک تا هشت قطعنامه تجاوز، بسیار مهم و حائز اهمیت است،

Lectures at The Hague Academy of International Law; first published in Receuil des Cours -197211(1973), 136. Leiden, A. W. Sijthoff.
mefacts.org/cached.asp?x_id=10943

۱٤. ماده ۲ بند ٤ منشور ملل متحد

*http://my.safaribooksonline.com/book/networking/security/9781449377229/responding-to-international-cyber-attacks-as-acts-of-war/analyzing_cyber_attacks_under_jus_ad_bel

هر چند که آقای پروفسوراشمیت در مقاله خود با عنوان؛
AND THE USE OF FORCE IN COMPUTER NETWORK ATTACK INTERNATIONAL LAW:THOUGHTS ON A NORMATIVE FRAMEWORK
به نقل از پروفسور Michael Reismanمعتقد است که حتی با در نظر گرفتن معیارهای متعدد همچنان لفظ استفاده از زور تعریف نشده است و با توجه به اتفاقات دهه گذشته که خارج از منشور اتفاق افتاده است و بعد ها به دلایل متعدد وجهه قانونی به خود گرفته اند جز ماده ۲ بند ٤ به حساب آمدند.

۱۵. مانند اعلامیه ی سال 1970 میلادی در خصوص روابط دوستانه ، A/RES/2625 (xxv) of 24 October1970و اعلامیه ی سال ۱۹۸۷در مورد عدم توسل به زور A/RES/42/22of18November1987

Weapons case, 1996, Para: 39 * Nuclear

۱٦. ماده ۵۱ کاملا واضح است.ماده این گونه شروع میکند،"جمعیت غیر نظامی و اشخاص غیرنظامی عموما از حمایت نسبت به خطرات ناشی از عملیات نظامی بهره می برند" پس برای عملی کردن مقررات با توجه به "اثربخشی به حمایت"حمله به اشخاص و جمعیت غیر نظامی ممنوع می باشد.هدایت یک حمله که به سمت اشیای نظامی هدفمند نشده،بکارگیری حملات مقابل به مثل علیه غیر نظامیان ،شروع کردن حملات به نحوی که خسارات تضمینی پیش بینی شده نسبت به منافع نظامی پیش بینی شده افراطی باشد،با اشیای نظامی جداگانه در طول یک حمله مانند اشیای واحد رفتار شود هنگامی که آنها به طور واضح جدا هستند و در متمرکز کردن غیر نظامیان تفکیک می شوند،و استفاده کردن از یک روش یا وسیله نظامی در طول یک حمله که ناتوان در تفکیک اهداف قانونی از غیر قانونی است یا اثرات آن نمی تواند کنترل شود."گرچه ماده های بعدی درخصوص چاچوب بندی شرایط ممنوعیت و محدودیت است.لیکن

مهمترین این ممنوعیت حمله هابر اشیای غیر نظامی و فرمان دادن پیشروی های متنـوع است که بایستی در طول حمله صورت پذیرد برای اجتناب از صدمه بـه جمعیـت غیـر نظامی و اشیا غیر نظامیان.ممنوعیت به عملیات نظامی مستقیم علیـه غیرنظامیـان، اشـیای غیر نظامی و دیگر اشخاص و اشیای حمایت شده بایستی بـه طـور اساسـی بـه عنـوان ممنوعیت حمله به آنها فهمیده شود .

منابع

AP I, arts. 51(2). art. 51(3)., arts. 51(5)(b) & 57(2)(a)(iii)., art. 57(1)., art. 57., art. 58., art. 56(1). art. 55(1). arts. 51(2) & 54

Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, 1880 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann, eds., 1987

Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases,and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, T.I.A.S. No. 8061

Geoffrey S. Corn, Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions, 2 J. NAT'L SECURITY L. & POL'Y 257, 261 (2008)

Herbert Lin, Cyber conflict and international humanitarian law, international review of red cross, Volume 94 Number 886 Summer 2012,p517-518

Herbert Lin, Cyber conflict and international humanitarian law, international review of red cross, Volume 94 Number 886 Summer 2012,p525

http://my.safaribooksonline.com/book/networking/security/9781449377229/responding-to-international-cyber-attacks-as-acts-of-war/analyzing_cyber_attacks_under_jus_ad_bel

International Law Department United States Naval War College,Newport, U.S.A. 2012 4th International Conference on Cyber Confl ict,C. Czosseck, R. Ottis, K. Ziolkowski (Eds.),2012 © NATO CCD COE,publications, Tallinn

International Law Department United States Naval War College,Newport, U.S.A. 2012 4th International Conference on Cyber Confl ict,C. Czosseck, R. Ottis, K. Ziolkowski (Eds.),2012 © NATO CCD COE,publications, Tallinn,p284

James D. Fry, Gas Smells Awful: U.N. Forces, Riot-Control Agents, and the Chemical Weapons Convention, 31 MICH. J. INT'L L. 475 (2010);

Jeffrey Carr,Inside Cyber Warfare, Publisher: O'Reilly Media, Inc.Pub. Date: December15,2009 p:65-66
http://my.safaribooksonline.com/book/networking/security/9781449377229/responding-to-international-cyber-attacks-as-acts-of-war/analyzing_cyber_attacks_under_jus_ad_bel

Jeffrey T.G. Kelsey, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, 106 MICH. L. REV. 1431 (2008).

Jeffrey T.G. Kelsey, Hacking into International Humanitarian Law:The Principles of Distinction and Neutrality in the Age of Cyber Warfare, Michigan Law Review ,Vol. 106,p1446-8

Lectures at The Hague Academy of International Law; first published in Receuil des Cours -197211(1973), 136. Leiden, A. W. Sijthoff. mefacts.org/cached.asp?x_id=10943

Lectures at The Hague Academy of International Law; first published in Receuil des Cours -197211(1973), 136. Leiden, A. W. Sijthoff. mefacts.org/cached.asp?x_id=10943

Matthew C. Waxman (Associate Professor of Law, Columbia Law School) .Cyber Attacks as "Force" under UN Charter Article 2(4), International Law Studies - Volume 87.p45

Matthew C. Waxman (Associate Professor of Law, Columbia Law School). Cyber Attacks as "Force" under UN Charter Article 2(4), International Law Studies - Volume 87.p 48

Matthew C. Waxman (Associate Professor of Law, Columbia Law School). Cyber Attacks as "Force" under UN Charter Article 2(4), International Law Studies - Volume 87.p 49

Matthew C. Waxman (Associate Professor of Law, Columbia Law School). Cyber Attacks as “Force” under UN Charter Article 2(4), International Law Studies - Volume 87.p 45

Matthew C. Waxman (Associate Professor of Law, Columbia Law School). Cyber Attacks as “Force” under UN Charter Article 2(4), International Law Studies - Volume 87.p46

Matthew C. Waxman (Associate Professor of Law, Columbia Law School). Cyber Attacks as “Force” under UN Charter Article 2(4), International Law Studies - Volume 87.p46

Matthew C. Waxman (Associate Professor of Law, Columbia Law School). Cyber Attacks as “Force” under UN Charter Article 2(4), International Law Studies - Volume 87.p 48

Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), THE YALE JOURNAL OF INTERNATIONAL LAW,Vol. 36: 421

Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), YALE JOURNAL OF INTERNATIONAL LAW ,Vol. 36,p428,.

Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), YALE JOURNAL OF INTERNATIONAL LAW ,Vol. 36,p429

Michael N. Schmitt ,“Attack” as a Term of Art in International Law: The Cyber Operations Context”,

Michael N. Schmitt ،“Attack” as a Term of Art in International Law: The Cyber Operations Context,

MICHAEL N. SCHMITT. 1999. “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework.” Columbia Journal of Transnational Law 37,p6-7

Michael N. Schmitt. 1999. “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework.” Columbia Journal of Transnational Law 37: 885, 913–15. This article also appears in The Columbia Journal of Transnational Law, Volume 37, 1999,pages 885-937 و https://cyber.law.harvard.edu/cybersecurity/Computer_Network_Attack_and_the_Use_of_Force_in_International_Law#Full_Title_of_Reference

Military objectives are targets that meet two criteria: they serve a military purpose and their incapacitation conveys a definite advantage. Protocol Additional I, supra note 120, art. 52(2).

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, THE LAW OF CYBER-ATTACK, Forthcoming in the California Law Review, 2012,p7

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, THE LAW OF CYBER-ATTACK, Forthcoming in the California Law Review, 2012,p10

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, THE LAW OF CYBER-ATTACK, Forthcoming in the California Law Review, 2012,p10-12

Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel , THE LAW OF CYBER-ATTACK, Forthcoming in the California Law Review, 2012,p43

Protection of Victims of International Armed Conflicts (Protocol 1),art. 51(5)(b), 57(2)(a)(iii)

Protocol Additional I, art. 54(2).

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1),art. 48, art. 51(5)(b),art. 85(3)(b).,art. 85(3)(a). arts. 51(5)(b), 54, 57(2)(a)(iii), 52(2)

Yoram Dinstein, Computer Network Attacks and Self-Defense, 76 INT'L L. STUD. 99,114-15 (2002)