فصلنامه سیاست خارجی
سال سی و دوم، شماره ۳، پاییز ۱۳۹۷، صص ۱۸۲- ۱۵۳

۶

جنگ‌های سایبری: چالشها و راهکارهای تعامل در پرتو مقررات توسل به زور

دکتر علی امیری[۱]
مهدی حیدری فرد[۲]

[۱] . استادیار حقوق بین‌الملل، دانشگاه آزاد اسلامی، واحد دامغان aliamiri20@yahoo.com
[۲] . دانشجوی دکترای حقوق بین الملل عمومی mahdiheydarifard@yahoo.com
(تاریخ دریافت: ۱۳۹۷/۸/۱۵ تاریخ تصویب: ۱۳۹۷/۹/۱۵)

چکیده

منشور سازمان ملل متحد تمامی اعضای جامعه بین‌المللی را از تهدید یا توسل به زور علیه تمامیت ارضی یا استقلال اقتصادی سایر کشورها، یا هر اقدامی که در تعارض با اهداف ملل متحد باشد، نهی نموده است. البته، اصولی مثل اصل توسل به دفاع مشروع و یا توسل کشورها به مکانیزم تامین امنیت دسته جمعی در مقابل کشور خاطی، به عنوان استثنای این اصل، در قالب ماده حقوقی دیگری در منشور مورد تاکید قرار گرفته است. در عین حال، واقعیت این است که اصول سنتی مذکور در مواجهه و تطبیق با تحولات معاصر جامعه بین الملل از جمله پیدایش پدیده نوظهور فضای سایبری ناتوان است.فضای سایبری شبکه‌ای به هم پیوسته از زیرساختهای فن آوری اطلاعات، اینترنت، شبکه های مخابراتی، سیستم های رایانه‌ای، کنترل‌کننده ها، پردازشگرها، کابل های فیبر نوری، مسیریابها[1] است که عملکرد اکثر سازوکارهای اقتصادی جوامع امروزی را به خود متکی ساخته و از طرف دیگر، امکان مورد هدف قرار گرفتن آنها در قالب حملات و عملیات سایبری هشداربرانگیز است. اینگونه عملیات می تواند تاثیرات بسیار جدی، نه‌تنها بر داده‌های سیستم کامپیوتری، بلکه اختلال و ازکار افتادگی زیرساخت های متکی بر سیستم‌های رایانه‌ای را به‌دنبال داشته باشد. البته دامنه یک جنگ سایبری می‌تواند از خشونت‌های شبکه‌ای ظاهرا بی‌ضرر تا حملات شدید به زیرساختهای زیربنایی در نوسان باشد. متاسفانه در حالی که بیشتر نگرانی کشورها در برخورد با این پدیده بعد حفاظتی امنیتی داشته و تاکید آنها حفاظت از زیرساخت‌های رایانه‌ای در برابر فیلترینگ، ایجاد اختلال و آسیب به آنها بوده، چالش‌های حقوقی این حوزه و نحوه اعمال و تفسیر قواعد حقوق جنگ به ویژه مقررات توسل به زور با توجه به ویژگی های ذاتی فضای سایبری کمتر بدان پرداخته شده و قابلیت اعمال مقررات مذکور در فضای مجازی در هاله ای از ابهام قراردارد.

واژگان کلیدی

حقوق مخاصمات مسلحانه، توسل به زور، عملیات سایبری، حمله سایبری، حمله نظامی در فضای سایبری، دفاع مشروع.

---

[1]. Routers

مقدمه

با وجود بالا گرفتن هشدارها نزد کشورها جهت تقویت امنیت سایبری، هنوز عموم مردم اطلاعات اندکی در خصوص برنامه ریزی و سیاست‌گذاری کشورها در اختیار دارند. سیاست‌گذاری دولت ها در این حوزه ترکیبی از راهبردهای تهاجمی و تدافعی بوده است، بدین معنی که آنها سعی دارند به موازات تلاش های خود جهت حفاظت از زیرساختهای حیاتی خود، بدنبال ارتقای ظرفیت های فناورانه با هدف بکارگیری عملیات سایبری علیه دشمنان خود باشند. اصلی‌ترین سوال نظام حقوقی بین‌الملل در برخورد با چالش های فضای سایبری این بوده که آیا کشورها در راستای اعتمادسازی در این حوزه، باید به سمت وسوی خلع سلاح و اجتناب از تکثیر سلاح در فضای سایبری بروند یا می توان با وضع یک رشته مقررات در صدد ایجاد نظم حقوقی این حوزه برآمد[1].البته دهه هاست که بحث هایی در خصوص لزوم تدوین معاهده جدید با هدف به نظم کشیدن حوزه سایبری مورد بحث بوده و در این حوزه نیز صف بندی کشورهای توسعه یافته از جمله آمریکا و کشورهای غربی به عنوان مخالفان نظم بخشی حقوقی حوزه سایبر، کشور روسیه به عنوان موافق آن و کشور چین به عنوان مخالف اصلی نظامی سازی حوزه سایبری و اینترنت مشهود بوده است.مهمترین این تلاش‌ها تدوین «کنوانسیون جرایم سایبری بوداپست» در سال ۲۰۰۱، به عنوان نخستین معاهده بین المللی جرایم رایانه ای و اینترنتی در سال ۲۰۰۱ ، به پیشنهاد شورای اروپا و با هدف سازگاری قوانین ملی با مقررات بین المللی، ارتقای روش‌های تحقیق و توسعه همکاری‌های بین‌المللی در این حوزه است. البته در سطح منطقه ای نیز سازوکارهایی توسط کشورها در پیش گرفته شده که مهمترین آن تهیه و تدوین دستورالعمل تالین توسط گروه کارشناسان مرکز عالی دفاع سایبری ناتو است.در نتیجه حمله به استونی دولت های عضو ناتو هم به فکر هماهنگ ساختن و اعلام عمومی اقدامات خود در مقابل

---

[1] . James Andrew Lewis, confidence- Building agreement in cybersecurity, Avalable at http//www.unidir.org/Pdf-art3168pdf (Jr, Spring 2011)

حملات سایبری بر آمدند که منجر به تدوین نظامنامه تالین شد . در مورد ارزش حقوقی نظامنامه تالین بحث زیادی وجود دارد. در درجه اول بحث معدود بودن دول حامی این سند است ، نه تنها منحصرا دولت های اروپایی و امریکای شمالی در تدوین آن نقش داشتند بلکه در بین آنها هم هیچ کشوری که دارای نظام حقوقی مکتوب (سیویل لا) باشد وجود نداشت ، بنابر این عام شمولی قواعد آن به شدت مردود است. در درجه بعد علمای شرکت کننده هستند که جایگاه و شان یک سند مورد اتفاق برجسته ترین علمای حقوق بین الملل را (مانند ارزشی که مصوبات کمیسیون حقوق بین الملل یا موسسه سن رمو دارد) به آن نمی دهند زیرا بجز اشمیت سایر شرکت کنندگان درجه علمی بالایی نداشتند. البته اگر سند از نظر علمی جامعیت وکیفیت بالاتری داشت طوری که بتواند هماهنگی و سازگاری با سایر قواعد مرتبط پیدا کند آنگاه می توانست بین خود تدوین کنندگان یک نظام حقوق خاص (یا در صورت عدم رعایت تشریفات معاهداتی یک عرف خاص) را بنیان گذارد. البته تدوین کنندگان برای رفع برخی نواقص آن دست به کار شده و ورژن جدیدی از آن را ارائه کرده اند.

جنگ سایبری و حقوق توسل به زور

اساسا استفاده از فناوری سایبری در درگیری های نظامی، موضوع نسبتا جدید بوده و به همین دلیل است که در اسناد قراردادی حقوق مخاصمات مسلحانه و حقوق بشردوستانه بین المللی نیز هیچ اشاره خاصی به امکان بکارگیری این شیوه تهاجمی نوین و مسائل حقوقی آن نشده است. این ملاحظه به این معنی نیست که چنین عرصه‌ای، موضوع حقوق مخاصمات مسلحانه، مقررات توسل به زور و اصول و مقررات حقوق بشردوستانه نیست. با توجه به رشد روزافزون کاربرد تسلیحات سایبری در درگیری‌های نظامی و یا خارج از آن و ناکامی تلاش‌های صورت گرفته در راستای ارائه تعریف از نبرد سایبری در چارچوب حقوق بین الملل، اهتمام جامعه حقوقی، باید ابهام زدایی، تفسیر بهینه و منطبق با نیاز روز در رابطه با نحوه اعمال مقررات حقوق بین الملل به ویژه حقوق توسل به زور بر نبردهای سایبری باشد (Jr, Spring 2011) .حقوق بین الملل مدرن در زمینه توسل به زور بر اساس بخش ۴ ماده ۲ منشور سازمان ملل

متحد شکل گرفته است. ممنوعیت ناشی از ماده مذکور، ماده ۵۱ منشور ملل متحد در رابطه با حق دفاع مشروع، ساز وکار امنیت دسته جمعی مندرج در فصل هفت منشور و مکمل همه اینها یعنی حقوق بین الملل عرفی که زائیده رفتار متحدالشکل و مداوم دولتها در قبال رویداد جامعه بین المللی است، همگی ابزارهای بین المللی جهت مهار افسارگسیختگی و توسل به قوه قاهره برخی کشورها علیه سایر کشورها است. بند ۴ ماده ۲ منشور سازمان ملل متحد حاوی قواعد کلیدی حقوق بین الملل در زمینه توسل به زور است. این ماده اشعار می دارد:"تمام اعضای منشور در روابط بین‌المللی خود از تهدید یا توسل به زور علیه تمامیت ارضی یا استقلال اقتصادی سایر کشورها، یا هر اقدامی که در تعارض با اهداف ملل متحد باشد، اجتناب خواهند ورزید".بر اساس منشور ملل متحد دو استثنا بر اصل کلی ممنوعیت توسل به زور وجود دارد. مورد اول ساز و کار امنیت دسته جمعی شورای امنیت است و مورد دوم که موضوع اصلی مقاله حاضر است، حق ذاتی "دفاع مشروع" است که در ماده ۵۱ منشور درباره آن چنین آمده است:"هیچ چیز در منشور حاضر ناقض حق ذاتی اعضای ملل متحد مبنی بر دفاع مشروع از خود (بصورت فردی یا جمعی) در صورت مورد حمله قرار گرفتن نیست، تا زمانی که شورای امنیت اقدامات لازم برای برقراری صلح و امنیت بین المللی را اتخاذ کند. البته، این دفاع مشروع باید ضرورت، تناسب و فوریت داشته باشد".پس از پرداختن به خاستگاه حقوقی اصول سنتی توسل به زور و دفاع مشروع، جای آنست که با پرداختن به ویژگی‌های ذاتی فضای سایبری بدنبال پاسخ به این سوال باشیم که آیا مفروضات سنتی حقوق جنگ با ویژگی های ذاتی یک جنگ سایبری قابل تطبیق هستند؟ به نظر می‌رسد پاسخ منفی باشد. بطور کلی ویژگی‌های ذاتی جنگ سایبری برخی از اساسی‌ترین مفروضات مقررات توسل به زور را به چالش می کشد:

۱) بنا به مفروضات حقوق مخاصمات مسلحانه، یک جنگ کلاسیک در دنیای واقعی روی داده و طرفین آن، حتی مخاصمات غیر بین المللی، شناخته‌شده هستند، نتیجه این وضعیت محدود بودن موقعیت جغرافیایی و صحنه نبرد است. این در حالی است که عملیات سایبری محدود به هیچ مرزی نیست و از طرف دیگر "ناشناس بودن" عامل یک حمله سایبری یک اصل است و بقیه موارد استثنا هستند. این عامل شناخت

عامل اصلی حمله و انتساب عمل متخلفانه به وی را حتی در زمانی که طرفین درگیری شناخته شده باشند، با مشکلاتی مواجه خواهد نمود.

۲) دیگر مفروض حقوق جنگ این است که یک درگیری نظامی کلاسیک تاثیرات مخرب و شدیدی، به شکل فیزیکی و ملموس، بدنبال خواهد داشت، در حالی که جنگ سایبری در فضای مجازی درگرفته، تحرکات نظامی جنگ‌های نظامی را نداشته و تاثیرات بسیاری از این جنگ ها گرچه مخرب، عموما بصورت فیزیکی و قابل لمس نمی باشند.

۳) از طرف دیگر، تدوین حقوق مخاصمات مسلحانه و حقوق بشردوستانه بین المللی بر مبنای تمایز اهداف نظامی و غیرنظامی شکل گرفته است. ساختار قواعد هدایت مخاصمات در حقوق بشردوستانه، به ویژه اصل تفکیک بر این پیش فرض بنا شده که اصولا اهداف نظامی و غیرنظامی متمایز و مهم‌تر از همه قابل تشخیص باشند. در صورتی که در عرصه یک جنگ سایبری این وضعیت جدای از اینکه یک مفروض اصلی باشد، بیشتر یک استثناست. چرا که بیشتر تاسیسات سایبری بعنوان مثال (کابل های زیردریایی، سرورهای رایانه، ماهواره ها، مسیریاب‌ها) کاربرد دوگانه داشته و برای مقاصد نظامی و غیر نظامی تعبیه شده اند.

۴) ارتباطات درونی و بهم پیوستگی فضای سایبر، تسری تاثیرات سوء حمله سایبری به سایر سیستم‌های رایانه‌ای را بدنبال خواهد داشت. این امر تهدیدی بر رعایت الزامات تفکیک و تناسب محسوب و توسعه میدان نبرد سایبری به یک آوردگاه جهانی را بدنبال خواهد داشت (schmitt, 2013).

سیر تحول مفهوم توسل به زور

اساسا منشور ملل متحد که در شرایط بین‌المللی حاکمیت محور شکل گرفته، در خصوص تبیین مفهوم توسط به زور و حمله مسلحانه مسکوت بوده است. در چنین فضایی، منابع مکمل حقوق بین الملل از جمله دکترین علمای حقوق و رویه قضایی هر کدام به نوعی به این موضوع پرداخته اند. برخی حقوقدانان اولین معیار حمله و تجاوز یک کشور علیه کشور ثالث (بند ۲ ماده ۴) را استفاده از زور از بیرون مرزهای تحت

حاکمیت کشور می دانند. در مقابل، بعضی یک اقدام نظامی را عمل یا اعمال نظامی دولتی علیه کشور ثالث می دانستند که هم دارای شدت لازم و هم دارای نتایج تخریبی نسبت به زیرساخت ها و ع ناصر حیاتی آن کشور باشد (Constantinau,2007.63-64). در این تعریف، معیار اصلی آستانه شدت و سطح گستردگی معین است؛ حال ممکن است این حمله از طرف گروههای نامنظم و غیردولتی صورت گرفته باشد. گرچه دیوان بین المللی دادگستری در قضیه دعوی حقوقی آمریکا و نیکاراگوئه بیان می دارد که اعمال نیروهای نامنظم می تواند در حد یک حمله باشد، در صورتی که از شدت یک حمله مسلحانه بالفعل با نیروهای منظم دولتی برخوردار باشد. طی سالهای پس از تدوین منشور تفاسیر مختلفی از مفهوم "توسل به زور" صورت گرفته است که بدان اشاره خواهد شد:

برداشت مضیق از مفهوم توسل به زور

طی سال های پس از تدوین منشور، تفاسیر مختلفی نسبت به مفهوم توسل به زور و دفاع مشروع صورت گرفت. برخی اقدام به تفسیر مضیق مفهوم توسل به زور و ماده ۵۱ نموده و توسل به ساز وکار دفاع مشروع را محدود به وقوع یک حمله مسلحانه فیزیکی می دانستند. به عقیده ایشان ساز وکار دفاع مشروع یک کشور تنها در مقابل یک حمله مسلحانه سنگین علیه تمامیت ارضی و استقلال سیاسی و حیات یک دولت فعال خواهد شد. در خصوص میزان و نحوه حمله نیز معتقد بودند که زمانی اعمال زور به سطح حمله مسلحانه می رسد که دارای شدت، استمرار و گستردگی کافی باشد. چنین رویکردی در تصویب قطعنامه ۳۲۱۴ مجمع عمومی سازمان ملل متحد سال ۱۹۷۴ بعنوان ابزار اختیاری شورای امنیت برای احراز اقدامات تجاوزکارانه، مطمح نظر قرار گرفت. تعریف این قطعنامه از واژه تجاوز چنین است:"تجاوز به معنی طراحی ، تدارک، آغاز یا اجرای اقدامی که با توجه به ماهیت، شدت و گستردگی آن نقض آشکار منشور ملل متحد محسوب گردد".

این تعریف بعدها مبنای رویه کشورها و آرای قضایی قرار گرفت. همچنین، با توجه به اینکه تعریف جنایت تجاوز در اساسنامه دیوان بین المللی کیفری همچنان معلق

مانده بود، کشورهای عضو اساسنامه در ماده ۸ مکرر کنفرانس بازنگری اساسنامه دیوان مذکور که در سال ۲۰۱۰ در شهر کامپالا برگزار گردید، موافقت نمودند در تعریف جنایت تجاوز قطعنامه ۳۲۱۴ مجمع عمومی مبنا قرار گیرد (موسی زاده، فروغی نیا.۱۳۹۱). در راستای پاراگراف اول این قطعنامه، عمل تجاوزکارانه به معنی استفاده از نیروهای مسلح به وسیله یک دولت در مقابل حاکمیت، تمامیت سرزمینی یا استقلال سیاسی سایر دولت ها است. اینجا اولین مشکل در عدم سازگاری تعریف مذکور با تحولات کنونی نظام بین الملل و تحولات جدید از جمله موضوع پدیده نوظهور تروریسم سایبری[1] خود را نمایان می سازد. چرا که تعریف فوق، نقش بازیگران غیردولتی مثل سازمانهای تروریستی، گروههای جدایی طلب و یا حتی افراد را نادیده می گیرد. این در حالی است که امروزه ایشان نقش غیرقابل انکاری در حملات از جمله حملات سایبری، چه بصورت مستقل و یا با هدایت برخی دولت ها دارند.

برداشت موسع از مفهوم توسل به زور[2]

در مقابل، طرفداران برداشت موسع از موضوع دفاع مشروع و حمله نظامی، در رابطه با اقدام به دفاع مشروع یک کشور، فقط در صورت مواجهه با حمله مسلحانه فیزیکی صرف، ابراز تردید کرده و معتقدند در فقدان یک حمله فیزیکی، یک کشور می تواند با تاکید بر اعمال منطقی اصول ضرورت و تناسب به دفاع پیشگیرانه، حمایت از اتباع و یا مداخله دمکراتیک دست بزند (Shaw. 2008). با چنین تعریفی دفاع مشروع می تواند در پاسخ به یک حمله تروریستی، که حتی توسط دولتی محقق نشده، صورت پذیرد. این مفهوم پس از حملات ۱۱ سپتامبر ۲۰۰۱ از طریق قطعنامه ۱۳۶۸ شورای امنیت سازمان ملل متحد صراحتا به رسمیت شناخته و مستمسک حقوقی برای حمله به افغانستان گردید، گرچه بطور کلی نتوانسته تاکنون اجماع جهانی را کسب کند.

---

[1] . Cyber Terrorism
[2] . Resort to Armed Force

آیا حمله سایبری "حمله مسلحانه[1]" محسوب می شود؟در اینجا به دنبال پاسخ این سوال هستیم که در پرتو تعاریفی که در رابطه با مفهوم توسل به زور و حملات نظامی ارائه گردیده، آیا عملیات سایبری، با توجه به ویژگی های ذاتی خود، ظرفیت آن را خواهند داشت که مصادیق ماهیت، شدت و گستردگی خاص حملات نظامی را برآورده کند؟ به عنوان اولین پیش شرط برای بررسی موضوع باید گفت بطور کلی حملات سایبری می بایست در قالب یک حمله مسلحانه جای گیرد، بدین معنی که باید بخشی از یک درگیری نظامی همه جانبه بین المللی یا غیربین المللی بوده و به عنوان مقدمه ای برای یک مخاصمه مسلحانه سنتی و یا تسهیل کننده آن صورت گیرد (Gill&Duchein.2013). این در حالیست که برخی عملیات سایبری معاصر صرفا جرایم شکل گرفته در فضای سایبر در موقعیت های روزمره، بدون ارتباط با شرایط جنگی بوده و لزوما به عنوان بخشی از یک مخاصمه نظامی صورت نپذیرفته است، گرچه می توانند باعث تحریک دشمن و اتخاذ اقدام تلافی جویانه گردد.موضوع دوم به گستره عملیات سایبری مربوط می شود. حملات سایبری، از لحاظ شدت و گستردگی، می تواند در مقیاس های متنوعی صورت گیرد. در این راستا، باید حملات سایبری را از تهدیدات امنیتی سایبری و یا عملیات پراکنده مجرمانه سایبری تفکیک نمود. بخش اعظمی از عملیات سایبری شامل هک های رایانه ای، جاسوسی و یا خرابکاری های معمول، پایین تر از حد حمله مسلحانه بوده و نمی تواند موجبات دفاع مشروع کشوری را فراهم سازد (Rid.2013). گاهی یک حمله سایبری می تواند صرفا یک "عملیات خصمانه" باشد. به عنوان مثال، بسیاری از تحلیل گران حملات به تاسیسات نفتی آرامکو توسط بدافزار شاموم را حائز چنین ویژگی می دانند. زیرا بدون خطر خاصی برای کل کشور صرفا صادرات نفت را مختل کرد حال آنکه همین حملات به یک تاسیسات اتمی که می تواند کل یک کشور یا منطقه را درگیر نماید ممکن است یک حمله مسلحانه در نظر گرفته شود. تحلیلگران حمله ویروس استاکسنت به سایت غنی سازی اورانیوم نطنز را که با هدف ایجاد اختلال در سیستم رایانه ای آن صورت گرفته بود را

[1]. Armed Conflict

صرفا یک اقدام خصمانه علیه جمهوری اسلامی ایران دانسته و خارج از یک درگیری نظامی می دانند (۱۳۹۳، اصلانی). البته در صورتی که این اقدام قابلیت انتساب به کشوری خاص داشته باشد، می توان آن را یک درگیری نظامی بین المللی قلمداد کرد.گاهی اوقات نیز عملیات سایبری در مقیاس بزرگ می تواند توسط یک گروه نظامی سازمان یافته غیردولتی علیه زیرساخت‌های سایبری کشور دیگری صورت پذیرد. این که آیا این عملیات در قالب یک مخاصمه نظامی غیردولتی تفسیر شود، جای بررسی داشته، در عین حال موضوع بحث کنونی نمی باشد. سوالی که در خصوص جنگ سایبری مطرح می شود این است که در فقدان هر گونه تحرکات نظامی[1] معمول جنگ‌های کلاسیک و توسل به قوه قاهره، آیا یک مخاصمه مسلحانه بین‌المللی می تواند از طریق حمله به یک شبکه رایانه‌ای آغاز شود؟ توسل به زور در نبرد سایبری به چه معناست؟ آیا نبرد سایبری، چه در مقام حمله یا یک اقدام تلافی جویانه، نوعی توسل به زور غیرقانونی و یا تهدید و در نتیجه نقض اصل آمره حقوق بین الملل محسوب می شود؟ منظور از حمله در فضای سایبری چیست؟پاسخ به سوالات مذکور مستلزم ارائه تفسیری شفاف نسبت به دو وضعیت است: اول اینکه آن حمله "قابلیت انتساب به یک دولت" را داشته باشد و دوم اینکه آیا از نظر حقوق بین‌الملل آن اقدام "توسل به زور" محسوب گرددیا نه؟ (Dinniss, 2012).

قابلیت انتساب یک حمله سایبری به دولت مشخص: اصل گمنامی و ناشناخته بودن عامل یک حمله سایبری به عنوان مفروض اصلی در این نوع حملات، ابهامات و سوالات در خصوص انتساب حمله را بصورت روزافزونی افزایش داده است. در شرایطی که معلوم نیست یک حمله سایبری از طرف دولت یا گروه غیردولتی خاصی صورت گرفته، طبعا قابلیت انتساب آن به دولتی یا نهاد غیردولتی و یا حتی فردی خاص غیر ممکن خواهد بود. در چنین فضای ابهامی می‌توان نتیجه گرفت اگر یک حمله سایبری از شبکه رایانه‌ای کشوری خاص نشات گرفته باشد، به آن دولت منتسب است. یا بر اساس فرضیه دیگر، با استناد به این اصل حقوقی در طرح مسئولیت بین المللی دولت‌ها

[1]. Kinetic

که"کشورها نباید اجازه استفاده از قلمروشان جهت انجام اعمال متخلفانه بین‌المللی را بدهند"، می توان حمله سایبری را به کشوری خاص نسبت داد. آیا مقررات موجود حقوق بین‌الملل از این فرضیات حمایت می کند؟ پاسخ منفی است.طرح کمیسیون حقوق بین‌الملل درباره مسئولیت دولت‌ها در قبال اعمال متخلفانه بین‌المللی، فرض انتساب یک عمل به یک دولت را مورد پذیرش قرار نداده و آنرا صرفا مبتنی بر واقعیات حقوقی، نه "فرضیه" می داند (International Law Commission, ۲۰۰۱).از طرف دیگر، دیوان بین‌المللی دادگستری، هرگاه بحث انتساب یک جرم بین المللی مانند نسل زدایی یا جرم تجاوز به یک دولت باشد ، آستانه نسبتا بالایی برای انتساب اقدام یک دولت در ارتباط با حق دفاع مشروع در نظر گرفته است. در قضیه سکوهای نفتی، دولت آمریکا مدعی گردید که قربانی حمله مسلحانه دولت ایران قرار گرفته و برای توجیه کاربرد نیروی نظامی علیه ایران به اصل دفاع مشروع استناد نمود. در این قضیه، دیوان بین المللی دادگستری، بطور موثر مسئولیت اثبات حق دفاع مشروع را به دوش کشوری گذارده که ادعا نموده است[1]. در حالی که این موضوع در قالب حق دفاع مشروع[2] در حقوق توسل به زور آمده، همین نتیجه‌گیری را می توان به تمام شرایط عینی در رابطه با قابلیت انتساب یک حمله سایبری به کشوری خاص تعمیم داد. با وجود این، سیستم‌های رایانه‌ای زیرساخت‌های یک کشور که به سختی قابل دستکاری بوده و از طرف دیگر به آسانی بوسیله رایانه قابل کنترل از راه دور است، بار اثبات این ادعا که یک حمله سایبری ممکن است از یک کشور خاص صورت گرفته باشد را سخت نموده و به این دلیل هر گونه ادعایی از طرف هر کشور باید به اثبات برسد. پس وجود این فرضیه در خصوص فضای سایبری تا حدودی بعید به نظر می‌رسد (Melzer, 2011).موضوع بعدی، قابلیت انتساب یک حمله سایبری به طرف‌های غیردولتی مثل گروه‌های هکر اطلاعات رایانه‌ای است. جدای از ابهامات مربوط به اصل ناشناس بودن عملیات سایبری، قواعد حقوقی در خصوص انتساب عمل متخلفانه به شخص یا

[1] . ICJ, Oil platform Case (Islamic Republic of Iran&United States of America).Judgment of 6th Nowamber 2003,Para 57

[2] . Right to Self-Defence

گروه‌های غیردولتی، در پیش‌نویس طرح مسئولیت کشورها در قبال اعمال متخلفانه بین‌المللی آمده است:"طبق این مقررات یک کشور مسئول عمل متخلفانه است در صورتی که شخص یا گروه غیردولتی تحت هدایت و یا کنترل موثر آن دولت اقدام به عمل متخلفانه نموده باشد". در اینجا عبارت "هدایت" یا "کنترل" نیاز به شفاف سازی دارد. دیوان بین‌المللی دادگستری عقیده دارد که اقدامات کلی عمل یک طرف غیردولتی (فرد یا عضوی از یک گروه سازمان یافته) اگر تحت هدایت و کنترل موثر کشور دولتی خاص باشد، قابل انتساب به آن دولت است. طبیعی است که در نبود چنین کنترلی بر یک عملیات مشخص ، حتی اگر گروه دولتی مورد نظر، تا حد زیادی به دولتی وابسته باشد، آن عملیات به دولت خاصی قابل انتساب نخواهد بود. در رابطه با معنی عبارت "کنترل موثر" پیش نویس طرح مسئولیت بین‌المللی معتقد است در صورتی هدایت حمله موثر قلمداد خواهد شد که روند هدایت‌گری و کنترل، به عنوان بخش اساسی عملیات متخلفانه صورت گرفته باشد، بطوری‌که در صورت فقدان کنترل، اجرای عملیات غیرممکن باشد. دیوان بین المللی کیفری یوگسلاوی حتی از این هم فراتر رفته و عقیده دارد:"وقتی که یک گروه، مثلا یک گروه مخالف نظامی سازمان‌یافته دست به یک عمل متخلفانه بین المللی زد، در صورتی اقدام قابلیت انتساب به دولتی خاص را دارد که مقامات دولت مذکور کنترل کلی بر این گروه داشته و رابطه ساختاری و سلسله مراتبی بین دو طرف برقرار باشد". با توجه به موارد مذکور، به نظر می‌رسد با عنایت به ویژگی‌های ذاتی فضای سایبر، برای اثبات انتساب یک حمله سایبری که توسط شخص یا گروه غیردولتی صورت گرفته، به شواهد و الزامات گسترده‌تری، در مقایسه یک حمله نظامی در دنیای واقع، نیاز داریم. با این‌حال، ارزیابی موردی واقعیات و شرایط حملات ضروری و مفید خواهد بود.

عملیات سایبری و انطباق آن با معیارهای سنتی اصل توسل به نیروی نظامی

در این بخش، به انطباق شرایط و ویژگی‌های منحصر بفرد عملیات سایبری با الزامات و معیارهای حقوق توسل به زور می‌پردازیم. از منظر حقوق توسل به زور سوال این است که آیا و چه زمانی عملیات سایبری معیارهای توسل به زور، مطابق ماده ۴ بند

۲ منشور ملل متحد را خواهد داشت؟ در چه شرایطی یک حمله سایبری می‌تواند موجبات شکل‌گیری یک مخاصمه نظامی را فراهم آورد؟ سوال بعدی این که تحت چه شرایطی یک جنگ سایبری می‌تواند توسط کشور قربانی، برای عملیات دفاع مشروع و متقابل مطابق ماده ۵۱ منشور ملل متحد، مورد استناد حقوقی قرار گیرد؟در یک مخاصمه مسلحانه بین‌المللی، یک اقدام، بدون پیشداوری در مورد اینکه این اقدام با کاربرد نیروهای مسلح در مفهوم ماده ۴ بند ۲ منشور ملل متحد همراه بوده است یا نه، می تواند توسل به زور قلمداد شود. انجام یک بررسی تطبیقی بین ماهیت"کاربرد نیروی نظامی" در جنگ‌های سنتی و عملیات سایبری شاید بتواند به فهم بیشتر موضوع کمک کند.بطور سنتی هدف یک جنگ کلاسیک غلبه بر دشمن می باشد. برای پیشبرد همین هدف است که طرفین جنگ آرایش نظامی گرفته و اقدام به استفاده از ابزار نظامی مثل تسلیحات، توپخانه همچنین نیروی انسانی می نمایند. در یک جنگ کلاسیک، رویارویی طرفین، مستلزم حضور نیروهای مسلح ایشان در صحنه نبرد و تبادل آتش است. اما آیا در جنگ سایبری هم همین شرایط حکمفرماست؟ به عبارت دیگر، در شرایط عدم حضور سلاح‌های نظامی و همچنین تحرکات نظامی و فیزیکی معمول جنگ‌های کلاسیک، منظور از نیروهای نظامی در یک جنگ سایبری چیست؟ در رابطه با چگونگی احراز معیارهای یک حمله نظامی توسط حمله سایبری دیدگاه‌های مختلفی وجود دارد:

دیدگاه ابزار محور[1]: این دیدگاه سنتی معتقد است که حملات سایبر باید مشخصه‌های فیزیکی متداول با حملات نظامی در دنیای واقع را داشته باشد. طبق نظر طرفداران این رویکرد، یک حمله سایبری هیچ گاه مصادیق یک حمله مسلحانه مد نظر ماده ۵۱ منشور ملل متحد را برآورده نخواهد کرد. ایشان تعریف قطعنامه ۳۲۱۴ مجمع عمومی سازمان ملل متحد[2] از واژه "تجاوز" را مبنای تفاسیر خود قرار می دهند. ماده ۳ اعلامیه مذکوردر بیان مصادیق تجاوز، اعمالی را تجاوز می داند که به شکل توسل به قوه قاهره با ابزار فیزیکی و نظامی باشد. چنین تفسیری، دربرگیرنده عملیات حملات

[1] . Means-Oriented
[2] . UN.DOC.A/RES29/2314

سایبری نیست (Hathaway.2012). البته که اکثریت علمای حقوق بین‌الملل این نظریه را رد کرده اند.

دیدگاه هدف محور[1]:این رویکرد به هدف حمله تمرکز داشته و ارزش حیاتی آن را مد نظر دارد. بر مبنای این نظریه، تنها وقتی یک حمله سایبری، معادل یک حمله مسلحانه تلقی می شود که سیستم رایانه‌ای یا زیرساخت مورد هدف قرار گرفته، اهمیت حیاتی نزد کشور قربانی داشته باشد. لذا چنانچه زیرساخت‌های حیاتی کشوری مانند سایت‌های هسته‌ای، شیمیایی، سیستم حمل و نقل هوایی و ریلی هدف یک حمله سایبری قرار گیرد، صرفا بدلیل حیاتی بودن اهداف، فارغ از اینکه آن حمله تلفات یا خرابی‌هایی داشته یا نه، حمله مذکور مسلحانه تلقی می شود. در این دیدگاه، واکنش کشورها در مقابل حملات سایبری صورت گرفته به تاسیسات زیرساختی خود تا حدود زیادی به میزان اتکا و وابستگی تاسیسات مورد نظر به سیستم رایانه‌ای و دنیای سایبر و در نتیجه میزان حساسیت کشورها بستگی دارد، بدین‌معنی که چنانچه زیرساخت‌های یک کشور تا حدود زیادی مبتنی بر سیستم‌های رایانه‌ای و فضای سایبر باشد، در این صورت کشور مورد نظر هر گونه حمله به تاسیسات مورد اشاره را یک اقدام خصمانه تلقی کرده و آنرا مکانیزمی برای توسل به زور و استناد بر اصل دفاع مشروع می داند. گرچه ممکن است واکنش کشورها در رابطه با هدف قرار گرفتن زیرساخت‌های نظامی یا شهروندی متفاوت باشد که این تمایز قائل شدن منطقی به نظر نمی رسد، چرا که توسل به زور، توسل به زور است خواه علیه اهداف نظامی یا غیرنظامی صورت گرفته باشد.

دیدگاه تاثیر محور[2]: قدم اول این بررسی تطبیقی، مقایسه تاثیرات مشابه یک حمله سایبری بر معادله نظامی و نتیجه نهایی جنگ است. این دیدگاه معتقد است که حملات سایبری باید با توجه به نتایج و تاثیراتشان قضاوت شوند. بیشتر تحلیلگران بر این عقیده‌اند که اگر یک حمله سایبری قابل انتساب به یک کشور بوده و تاثیرات مخرب آن بر معادله جنگ، قابل مقایسه با تاثیرات یک حمله نظامی فیزیکی باشد به‌طوری که

[1] . Target-oriented
[2] . Effect-Oriented

معیارهای توسل به زور را احراز کرده باشد، این حمله می‌تواند موجب شکل‌گیری یک مخاصمه نظامی گردد. به عبارت بهتر، اگر مثلا یک حمله سایبری به سیستم حمل و نقل کشوری، سبب بروز تصادفات هواپیما یا قطار و در نتیجه کشتار و مجروحیت افراد گردد، در این شرایط دیگر دلیلی برای تمایز قائل شدن بین یک حمله سایبری در فضای مجازی و حمله کلاسیک در دنیای واقعی وجود نخواهد داشت.

این شرایط در موقعیت‌هایی است که یک حمله سایبری به کشته و مجروح شدن جمعیت غیرنظامی و یا صدمه جدی به زیرساخت‌های یک کشور منجر می شود، اما گاهی اوقات یک حمله سایبری منجر به تلفات جانی غیرنظامیان و تخریب زیرساخت‌های کشور، آن گونه که در جنگ‌های کلاسیک و فیزیکی معمول است، نمی شود و فقط بر عملکرد زیرساخت‌های مذکور اثر گذاشته و سبب از کارافتادن و ایجاد اختلال در کارکرد آن می گردد. به طور مثال، تاثیرات بالقوه یک حمله سایبری به سیستم بانکداری یا شبکه تولید و توزیع برق یک کشور، هر چند در نگاه اول می تواند بدون کشته و زخمی شدن جمعیت غیرنظامی یا صدمه فیزیکی به تاسیسات یک کشور باشد، اما اثرات بالقوه اینگونه حملات بر افراد غیرنظامی می تواند بسیار گسترده‌تر از یک حمله نظامی در جهان واقع بوده و مستمسکی برای کشور قربانی برای توسل به زور با استناد به اصل دفاع مشروع باشد. با چنین رویکردی، کشورها هر گونه عملیات سایبری که باعث اختلال در عملکرد تاسیسات زیرساختی رایانه‌ای شود را یک حمله نظامی خصمانه قلمداد و آنرا بهانه‌ای برای توسل به اقدام متقابل نظامی می دانند. این کشورها برای توجیه حقوقی نظر خود به ماموریت ذاتی حقوق بشردوستانه بین‌المللی مبنی بر حفاظت از افراد و اهداف غیرنظامی در مقابل تاثیرات حمله نظامی اشاره و معتقدند با توجه به تاثیرات چنین حمله سایبری بر جمعیت غیرنظامی، حملات مورد نظر می توانند یک حمله نظامی تلقی شده و شروع یک درگیری نظامی از طریق توسل کشور قربانی به نیروی نظامی باشد. پاسخ به این سوال که تحت چه شرایطی حملات سایبری می‌تواند به عنوان یک درگیری نظامی شناخته شود؟ را با در نظر گرفتن ماموریت اصلی حقوق بشردوستانه بین‌المللی که همانا حفاظت از جان جمعیت غیرنظامی در برابر اثرات یک حمله نظامی است، می توان داد. یک حمله سایبری به

سیستم بانکداری یک کشور و یا شبکه آب و برق آن، اگر چه می تواند زیان‌های سهمگین اقتصادی بدنبال داشته باشد، اما با تاثیرات مخرب حاصل از یک حمله نظامی در دنیای واقع، قابل مقایسه نیست. با این وجود، در شرایطی که چنین حمله‌ای باعث قطعی سیستم برق‌رسانی یا آب‌رسانی یک کشور شده و سختی شدیدی را به جمعیت غیرنظامی تحمیل کند، می تواند به عنوان یک حمله نظامی تفسیر گردد. حتی اگر این حمله به تلفات جانی جمعیت و تخریب اهداف غیرنظامی نیز منجر نشده و تاثیرات آن با تاثیرات مخرب یک حمله نظامی فیزیکی قابل مقایسه نباشد.در این حوزه واکنش کشورها به آستانه آسیبی وابسته است که کشورها آن را تحمل می کنند و تاثیراتی است که حمله مورد نظر بر تغییر معادله جنگ خواهد داشت. اگر حمله به یک شبکه رایانه‌ای کوتاه مدت (موقت) باشد، تنها در صورتی می تواند توسل به زور تلقی شود که به آستانه شدت خاصی برسد. به عنوان مثال، می توان به حمله ویروس استاکس‌نت به سایت اتمی نطنز اشاره نمود که بیشتر نشریات آن زمان، آن را یک اقدام خصمانه موردی علیه جمهوری اسلامی ایران دانستند، بدون اینکه فعل و انفعالات جنگی در میان باشد. در این وضعیت، حمله کننده جدای از ناشناس ماندن به دلایل سیاسی مایل است حمله در همین سطح انجام شده و مخاصمه افزایش نیابد. ویروس استاکس‌نت باعث تخریب و جایگزینی حدود یک هزار دستگاه سانتریفیوژ IR-1 گردید. در صحنه واقعی جنگ، اگر سانتریفیوژها از طریق بمباران هوایی تخریب می شد ، همین سطح تخریب و ایراد صدمه می توانست توسل به زور تعبیر و شروع یک مخاصمه مسلحانه را باعث شود. اما در نبود یک تحرکات نظامی معمول جنگ های سنتی و اینکه تاثیرات حمله فقط متوجه سانتریفیوژها بوده و تاثیرات مخرب جانبی نداشته است، در این حالت تعبیر یک حمله سایبری به عنوان توسل به زور محل بحث و مجادله است. اقدام خصومت‌آمیز پراکنده یک کشور علیه کشور دیگری نمی‌تواند توجیهی برای دفاع مشروع بوده و آغازگر پروسه یک جنگ بین‌المللی باشد. چنین اقدامی فقط اقدامات پلیسی موردی و پراکنده را می طلبد. به هر حال در دنیای واقع، رویه کشورها در این رابطه ناهمگون بوده و کشورها –حتی کشورهای قربانی- با توجیه لزوم اجتناب از افزایش رویارویی‌های بین‌المللی، در مواجهه با حملات سایبری ساکت مانده اند.

ارائه راه حل متوازن در ارزیابی حملات سایبری به عنوان یک حمله مسلحانه

با وجود اینکه به نظر می رسد رویکرد اثر محور در تفسیر یک حمله سایبری به عنوان حمله مسلحانه، نسبت به دو رویکرد دیگر معتدل‌تر عمل کرده و در نتیجه مورد اقبال بیشتر علمای حقوق بین‌الملل باشد، در عین حال، رویکرد متوازن در این حوزه نگاه چند وجهی به یک حمله سایبری و بررسی مجموعه عوامل دخیل در یک حمله به جای رویکرد انحصاری به ابزار، هدف و اثر یک حمله خواهد بود. این دیدگاه منحصرا دست به مقایسه تاثیرات عملیات سایبری با یک حمله فیزیکی در قالب یک جنگ کلاسیک نمی زند بلکه به ترکیب عواملی مثل شدت پیامدهای یک حمله سایبری، ابزارهای بکار رفته، درگیر بودن ارتش یا طرف‌های دیگر درگیر در عملیات خصمانه، ماهیت نظامی یا غیرنظامی هدف و طول مدت عملیات توجه دارند. به عنوان مثال، میشل اشمیت برای ارزیابی یک حمله سایبری معیارهایی مثل نوع و میزان صدمه، فاصله زمانی میان خسارت و حمله، مستقیم و بی واسطه بودن حمله، خاصیت تهاجمی، قابلیت اندازه‌گیری خسارت و غیرقانونی بودن حمله را مد نظر قرار می دهد (Schmitt M. N., 2014). توجیه یک حمله سایبری به عنوان توسل به زور به ارزیابی دقیق موردی آن، نه توسط کشورهای طرف درگیری، بلکه به Opinion Juris بستگی داشته و این رویه یکسان و واحد آتی کشورهاست که مبنای حقوقی به این نظریه خواهد بخشید.در مسیر بررسی ترکیب عوامل و معیارهای موثر در تلقی یک حمله سایبری به عنوان حمله مسلحانه و مقایسه تطبیقی آن با حمله نظامی فیزیکی و انطباق آن با مقررات حقوق بین‌الملل سوالات متعددی مطرح می شود. اینکه مفهوم حمله در حقوق بین‌الملل چیست؟ و چگونه می توان آنرا در قالب جنگ سایبری تفسیر کرد؟ آیا مثلا اگر بخش‌هایی از تاسیسات هسته ای با نفوذ عوامل خارجی دچار اختلال شود، این حمله می تواند مستمسکی برای توسل به زور از طرف کشور قربانی تلقی شود؟ اگر هدف نظامی یا غیرنظامی باشد، آیا پاسخ متفاوت خواهد بود؟

حمله چیست؟با توجه به تفاوت ذات و ماهیت فضای سایبری با جنگ‌های کلاسیک در دنیای واقع، طبیعتا ابزار و شیوه‌های جنگی مورد کاربرد در این دو عرصه با هم یکسان نیستند. لذا مفهوم حمله در یک جنگ کلاسیک، مستلزم کاربرد یک رشته

ابزار جنگی و نیروی فیزیکی بوده و آنچه در این حوزه به عنوان خشونت تعریف می شود با تعریف آن درحوزه جنگ سایبری متفاوت خواهد بود. ماده ۴۹ بند یک پرتکل الحاقی اول حمله را اینگونه تعریف می کند:"اقدامات خشونت‌بار علیه دشمن (چه تدافعی و چه تهاجمی)"از نظر طراحان پیش‌نویس پرتکل مذکور، یک حمله لزوما نمی تواند فیزیکی باشد. طبق تعریف مذکور یک حمله در درجه اول باید یک اقدام خشونت‌بار باشد. اکثر صاحب‌نظران بر این نکته توافق دارند که در تعیین مصادیق "خشونت" به هیچ وجه به ابزار حمله توجه نمی شود، بدین‌معنی که ناصواب خواهد بود اگر تصور شود که تنها اقدام خشونت‌بار با ابزار فیزیکی و نیروی حرکتی حمله محسوب می گردد (Dinstein, 2004). پایه اطلاق "حملات" در مخاصمات مسلحانه" عواقب خشونت‌بار حاصله از یک اقدام است. پس طبق این تعریف بی‌تردید عملیات شیمیایی، بیولوژیک و رادیولوژیک حمله محسوب می شود، حتی اگر در این حمله هیچ نیروی فیزیکی بکار نرفته باشد (Haslam, 2000). لذا، این اصل پذیرفته شده که فاکتور اصلی تعیین‌کننده، نه "خشونت ابزاری" بلکه عواقب خشونت‌بار یک حمله است (Schmitt M. N., 2002) . حتی یک جریان داده ها که از طریق کابل‌ها یا ماهواره عبور می کند، نیز می‌تواند تحت شمول تعریف "حمله" باشد.در فضای سایبری شاخص مهم تاثیرات یک حمله است. در این عرصه یک حمله لزوما منجر به کشته و یا مجروح شدن افراد و یا ایراد صدمه به زیرساخت‌های نظامی و غیرنظامی، مانند عواقب فیزیکی، محسوس و فاجعه‌بار حملات نظامی معمول در جنگ‌های سنتی نمی شود. یک حمله سایبری ممکن است سبب ازکار افتادن و یا ایجاد اختلال در عملکرد زیرساخت‌های نظامی و غیرنظامی یک کشور شده و زندگی شهروندان را بصورت غیرمستقیم مورد تهدید قرار دهد. تصور کنید شبکه برق‌رسانی یک کشور مورد حمله سایبری قرار گیرد، در چنین شرایطی عملکرد مراکز خدماتی ضروری مثل بیمارستان‌ها تحت تاثیرات منفی این حمله خواهد بود. نکته قابل ملاحظه اینکه همیشه عواقب یک حمله سایبری یکسان نخواهد بود. هر گونه عملیات سایبری علیه سیستم ارتباطی مراکز تجاری، بانک‌های و مراکز مالی پولی یک کشور، اختلال در فعالیت‌های روزمره تجاری و بانکی را بدنبال خواهد داشت که طبیعتا تاثیرات آن قابل مقایسه با وضعیت توصیف شده در مثال قبل نخواهد بود.حال سوال این است

که آیا چنین عملیاتی، دربردارنده مصادیق"حملات"، آنطور که در ماده ۴۹ پرتکل الحاقی اول آمده هست؟قبل از پرداختن به پاسخ سوال مذکور باید گفت که یک عملیات سایبری ممکن است به دو طریق انجام شود: گاهی عملیات سایبری با هدف از کارانداختن عملکرد زیرساخت‌های متکی بر سیستم رایانه‌ای صورت می پذیرد و گاهی عملیات سایبری انسداد ظرفیت‌های ارتباطی مثلا انسداد سیستم دفاع هوایی دشمن، سیستم بانکداری و یا ایجاد اختلال در سیگنال‌های رادیو تلویزیونی را هدف‌گذاری کرده است. با در نظر گرفتن تقسیم‌بندی فوق ممکن است پاسخ‌های ارائه شده نیز در دو حوزه و در قالب دو نظریه کاملا جداگانه مطرح گردند. هر کدام از این نظریات تفسیرهای موسع و مضیقی از عبارت حمله در فضای سایبری داشته و طبیعتا از طرف علمای معروف حقوق بین الملل پشتیبانی می گردد.

تفسیر مضیق "حمله" در فضای سایبری

نظریه اول تفسیر مضیق و محدودی از مفهوم یک حمله سایبری داشته و منحصرا به عواقب و تاثیرات یک حمله توجه دارد. طبق نوشته های میشل اسمیت، عملیات سایبری مثل هر عملیات دیگری حمله محسوب می شود، وقتی که به کشته و مجروح شدن افراد و صدمه و تخریب اهداف (چه نظامی و چه غیرنظامی) منجر گردد. در این تفسیر منظور ایراد صدمه فیزیکی[1] است. طبق این تعریف حملات سایبری، در صورتی که فقط سبب بروز مشکلات و دردسرهایی شده و یا بصورت موقتی سبب اختلال در عملکرد یک هدف گردد، حمله محسوب نمی شود، مگر اینکه سبب رنج افراد گردد.در مقام نقد این نظریه ابتدا باید به تفاوت ماهوی "صدمه" و "تخریب[2]" اشاره نمود. در حالی که واژه "تخریب" بیشتر به ویرانی‌های فیزیکی یک هدف اشاره دارد، در متون حقوقی "صدمه" به معنای آسیب در عملکرد یک هدف که به کاهش ارزش و از دست رفتن سودمندی آن منجر گردد، تعبیر شده است. گاهی ممکن است یک عملیات سایبری به "صدمه" منجر شود بدون آنکه تخریب فیزیکی بدنبال داشته باشد. بر مبنای

[1] . Physical Damage
[2] . Destruction

این تعبیر، اختلال در عملکرد و از کار انداختن زیرساخت‌های متکی بر سیستم‌های رایانه‌ای "صدمه" محسوب می شود. پس واژه" صدمه فیزیکی" نمی‌تواند معیار مناسبی برای اطلاق "حمله" به یک عملیات سایبری باشد. بر مبنای این تعریف اگر یک هدف غیرنظامی مثل شبکه توزیع برق شهری، هدف یک عملیات سایبری قرار گرفته و در نتیجه از کار بیافتد، جدای از آنکه از چه طریقی از کار افتاده است، چون این حمله صدمه و تخریبی را بدنبال نداشته، پس این اقدام حمله محسوب نمی شود. در صورتی‌که صرف انجام یک حمله سایبری به تاسیسات زیرساختی متکی بر سیستم‌های رایانه‌ای، خواه تخریب و صدمه فیزیکی در پی داشته باشد یا نه، همچنین چه بطورکوتاه مدت سبب اختلال در عملکرد زیرساخت‌های یک کشور گردد و چه بصورت دائمی، سبب رنج افراد و اختلال در زندگی شهروندی خواهد شد. علاوه بر آن، هیچ آستانه‌ای از رنج افراد در این نظریه تعیین نشده است. پذیرش این نظریه منجر به این خواهد شد که به عنوان مثال ما تخریب یک منزل مسکونی در نتیجه بمباران دشمن را یک حمله قلمداد کنیم و در مقابل عملیات سایبری علیه شبکه توزیع برق شهری که تامین کننده برق میلیون‌ها شهروند است را حمله محسوب نکنیم. با تعابیر فوق، قابل انتقاد خواهد بود اگر صرف اختلال در عملکرد یک هدف که بصورت کوتاه و موقت رنج افراد انسانی را در پی داشته باشد، یا ایراد صدمه کوتاه مدت فیزیکی به اهداف، یا ازعملکرد ساقط شدن یک هدف بصورت کامل یا موقتی در نتیجه یک عملیات سایبری را "حمله" در مفهوم حقوق بشردوستانه ندانیم.

تفسیر موسع از عبارت "حمله" در فضای سایبری

در نقطه مقابل، صاحبنظرانی مثل "نات دورمان" هستند که تفسیر موسعی داشته و معتقدند عملیات سایبری، حتی اگر به صدمه هم منجر نشود، حمله محسوب می شود. در برخی از موارد، تنها عملکرد ارتباطی در فضای مجازی و گاهی عملکرد یک هدف متکی بر سیستم رایانه‌ای (نظامی و غیرنظامی) در دنیای فیزیکی مورد هدف یک عملیات سایبری است. این تفسیر عملیات سایبری در اشکال مختلف اعم از مداخلات در سیستم رایانه‌ای غیرنظامی مثل ایمیل‌های شخصی، شبکه‌های ارتباطی، سیستم‌های

خرید آنلاین، سیستم‌های ثبت نام تا عملیات سایبری مهمتر مثل اختلال در شبکه تولید و توزیع برق، سیستم رایانه‌ای حمل و نقل ریلی و هوایی، سایت‌های هسته‌ای را معادل یک "حمله" فرض می‌کند(Schmitt M. N., 2014) .تمرکز اصلی این نظریه بر روی "هدف نظامی" است. این دیدگاه در تدوین ماده ۵۲ بند دوم پرتکل الحاقی مورد توجه قرار گرفته است. این ماده بیان می دارد:یک "هدف نظامی" هدفی است که تخریب کلی یا جزئی آن ، محاصره یا تسخیر آن و یا حتی خنثی سازی و از عملکرد ساقط کردن آن مزیت نظامی مشخصی را بدنبال داشته باشد.آوردن عبارت "حتی خنثی‌سازی یک هدف" بدین‌معنی است که هدف اصلی یک حمله از عملکرد انداختن یک هدف است که نیل به این هدف لزوما با تخریب و ایراد صدمه همراه نخواهد بود. در اینجا مهم این است که هدف مذکور مورد استفاده دشمن برای بدست آوردن مزیتی در رویارویی نظامی قرار نگیرد.طراحان پیش‌نویس پروتکل الحاقی اول نه تنها حملاتی را در نظر داشته اند که قصد آنها تخریب و ایراد صدمه به اهداف است، بلکه به حملاتی اشاره دارند که با قصد "عدم کاربرد هدف توسط دشمن" صورت گرفته و تخریبی بدنبال ندارد. به عنوان مثال، سیستم دفاع هوایی دشمن را می توان از طریق یک عملیات سایبری برای یک دوره زمانی، از طریق مداخله در سیستم رایانه‌ای، اما بدون تخریب یا صدمه ای به زیرساخت‌های فیزیکی از کار انداخت. در اینجا تمرکز یک حمله بر خنثی‌سازی و از عملکرد ساقط کردن یک هدف است. یک عملیات سایبری در صورتی می تواند یک "حمله" طبق تعاریف حقوق بین الملل قلمداد گردد که دردرجه اول در قالب یا به عنوان بخشی از یک مخاصمه مسلحانه صورت گرفته باشد. در ثانی، عملیات فوق منجر به کشته شدن یا مجروحیت افراد، ایراد صدمه فیزیکی به اهداف از طریق ایجاد اختلال و یا از بین رفتن عملکرد یک زیرساخت متکی بر سیستم رایانه‌ای گردد. اختلال و از کار افتادن سیستم دفاع هوایی، شبکه برق و بانکداری می تواند یک حمله باشد. با این وجود همه نوع عملیات سایبری حمله محسوب نمی شود. امروزه در رابطه با حمله محسوب شدن عملیات سایبری به زیرساخت‌های متکی بر سایبر، که به اختلال در عملکرد و از کارافتادگی (در دنیای فیزیکی) منجر خواهد شد، تردیدی وجود ندارد. در حالی که ابهامات در خصوص اطلاق حمله در مواقعی که عملکرد ارتباطی فضای

سایبری هدف یک عملیات سایبری است، به عنوان مثال مداخلات در سیستم‌های ارتباطی مثل ایمیل، شبکه های اجتماعی یا رسانه‌ای وجود داشته و سوالات بی‌پاسخ مانده است. جدای از آن، با توجه به هدف و ماموریت ذاتی حقوق بشردوستانه که همانا حفاظت افراد و اهداف غیرنظامی در مقابل تاثیرات سوء حملات نظامی است، از منظر مقررات هدایت مخاصمات، اهمیتی ندارد که یک عملیات حمله محسوب شود و یا نشود. آنچه مهم است ایجاد رنج و دردسری است که برای افراد و اهداف غیرنظامی بدنبال دارد. بدین‌معنی که با توجه به میزان رنج و زحمتی که یک عملیات سایبری بر افراد و اهداف غیر نظامی بار می کند، می توان در خصوص "حمله" محسوب شدن یا نشدن آن تصمیم گرفت. با این روش به نظر می‌رسد در خصوص عواقب فاجعه‌بار حمله سایبری به یک سایت هسته‌ای و یا شیمیایی یک کشور اتفاق نظر بیشتری نسبت به عواقب عملیات نظامی علیه سیستم بانکی و یا سیستم بلیط فروشی آن‌لاین، در حمله فرض کردن عملیات مورد نظر وجود داشته باشد. تاکنون رویه کشورها در برخورد با موضوع فوق یکسان نبوده و ایجاد رویه واحد در آینده باید مورد اهتمام محافل حقوق بین الملل قرار گیرد.

اصل دفاع مشروع: قلمرو ماده ۵۱ منشور ملل متحد همواره یکی از بحث برانگیزترین حوزه‌های مطالعاتی حقوق بین‌الملل به ویژه حقوق مخاصمات مسلحانه بوده است. در تفسیر این ماده تحلیلگران حوزه حقوق بین‌الملل معتقدند که در روند اتخاذ تصمیم دفاع مشروع، دولت قربانی باید ملاحظات مربوط به اصول تناسب، ضرورت و فوریت را رعایت کند. حال به امکان سنجی کاربرد اصول مذکور در اتخاذ اقدام دفاعی مشروع در قبال یک حمله سایبری می پردازیم:

اصل ضرورت[1]: اصل ضرورت به کشور قربانی این تعهد را بار می کند که در روند اتخاذ اقدام دفاعی در قبال یک اقدام تجاوزکارانه، باید حمله را به یک منبع خاص ارتباط داده و قصد متخاصمانه دولت مهاجم را احراز و اثبات کند. فناوری ذاتی موجود در نبرد سایبری که در آن ناشناس بودن عامل یک حمله سایبری اصل می باشد، امکان

[1]. Necessity

ایجاد ارتباط میان حمله و یک منبع خاص و شناسایی قصد و انگیزه مهاجم را تقریبا غیرممکن می سازد. الزامات اصل مذکور با خصوصیات ذاتی دنیای دیجیتال همگون نبوده و در شرایطی که به سبب محدودیت فوق، امکان عکس العمل دولت قربانی کاهش پیدا می کند، به همان میزان باعث تقویت و تشویق دول متخاصم و گروه‌های تروریستی سایبری خواهد شد.

اصل تناسب[1]:اصل فوق بدین‌معنی است که زور استفاده شده در پاسخ به یک حمله حمله باید با هجوم اولیه تناسب داشته باشد. در فضای سایبری ضرورت رعایت اصل تناسب، به عنوان پیش نیاز اتخاذ اقدام دفاعی منطبق با اصل ۵۱ منشور ملل متحد با نوعی ابهام و همراه است. با توجه به این مهم که بیشتر سیستم‌های سایبری و زیرساخت‌های متکی بر سیستم‌های رایانه‌ای دارای کاربرد دوگانه هستند، ارتباطات درون سیستمی فضای سایبری، به ویژه در بعد تهاجمی عملیات سایبری امکان سرایت حملات به سایر شبکه‌های رایانه‌ای و همچنین سیستم‌های غیرنظامی و در نتیجه توسعه میدان نبرد سایبری زیاد خواهد بود که نتیجه طبیعی آن تضعیف اصل تناسب می باشد. در مواقعی که عملیات سایبری در مقام دفاع از پیش برنامه ریزی شده در مقابل نفوذ سیستم رایانه خارج و بطور اتوماتیک طراحی شده است (هک متقابل)، تعهد مورد نظر پیشاپیش برآورده شده است. چنین عملیاتی به سادگی کامپیوترهایی را مورد هدف قرار خواهد داد که حمله سایبری، مزاحمت ها و نفوذها از آن نشات گرفته است.

اصل فوریت[2]:طبق این اصل اقدام دفاعی باید فوری باشد نه پس از گذشت مدت طولانی. به نظر می رسد در فضای سایبری تعبیه مکانیزم "هک متقابل" الزام فوریت داشتن یک اقدام دفاعی تلافی‌جویانه مشروع را بر طرف خواهد کرد.

نتیجه‌گیری

تحولات کنونی در نظام بین‌الملل به طرفی پیش رفته که دیگر نمی‌توان صرفا به تعریف‌های سنتی حاکم بر روابط بین دولت‌ها تکیه داشت. واقعیت این است که منشور

[1]. Proportionality
[2]. Immediacy

ملل متحد در شرایط دولت محور و بروز جنگ‌های کلاسیک تدوین گردیده و پس از آن دنیا شاهد پیشرفت سرسام‌آور فناوری به ویژه در دنیای فناوری اطلاعات بوده است. به موازات پیشرفتهای مذکور که به توسعه ابزار و شیوه های جنگی منجر شد، موضوع عملیات سایبری، به عنوان گونه ای از نبردهای نامتقارن و تهدید حاکمیت های رو به تضعیف کشورها مطرح و در راس نگرانی محافل حقوقی و فنی آنان قرار گرفت. پیدایش این فضای جدید چالشی نو برای تعاریف سنتی منشور ملل متحد در بحث توسل به زور و دفاع مشروع محسوب می شود. در واقع، محدودیت‌هایی که تفاسیر تاریخ گذشته حاکم بر توسل به زور بر کشورها تحمیل نموده تهدیدات زیادی را بدنبال داشته و عملا دست کشورها را در برخورد با حملات جدید به ویژه عملیات سایبری بسته است.این موضوع که میدان عمل جنگ سایبری، فضای مجازی بوده و برخلاف جنگ های کلاسیک تحرکات نظامی معمول را دارا نمی باشد، دلیلی نیست که این حوزه را به عنوان استثنایی در حقوق مخاصمات مسلحانه در نظر بگیریم. ویژگی های ذاتی حملات رایانه‌ای مثل ناشناس بودن عامل حمله و مشکلات انتساب حمله، پیوندهای درونی دنیای سایبر و از طرف دیگر دانستن این موضوع که بیشتر اهداف حملات سایبری دارای کاربردهای دو گانه نظامی و غیرنظامی هستند، چالش های حقوقی زیادی در حوزه حقوق بشردوستانه و حقوق مخاصمات بین‌المللی ایجاد می کند. به علاوه دانستن این مطلب که دامنه حملات سایبری از عملیات دارای اهمیت کمتر هک اطلاعات تا حملات مهم‌تر به زیرساخت های حیاتی شهروندی در نوسان است و در بیشتر حملات سایبری تاثیرات حاصله قابل مقایسه با حملات نظامی فیزیکی نیست (جنگ بدون خونریزی) تردیدها در خصوص تفسیر یک حمله سایبری به عنوان "توسل به زور" را افزایش می دهد. شرایط مذکور بررسی موردی حملات مذکور با امعان نظر به شرایط مکانی، زمانی و بررسی تاثیرات حمله را طلب کرده و پراکندگی رویه دولت‌ها در قبال حملات سایبری معاصر را باعث می شود. با این وجود، احتمال افزایش میزان حملات مذکور در آینده نزدیک به ایجاد رویه واحد کمک خواهد کرد، گرچه به هیچ وجه مشخص نیست که عملکرد دولت‌ها به کدام جهت گرایش خواهد داشت.در چنین شرایطی، اصول سنتی حقوق بین‌الملل (مثل بند ۴ ماده ۲ منشور) که اساسا در فضای

حاکمیت محور تدوین و طرف اصلی آن نیز کشورها می باشد، به هیچ وجه با تحولات کنونی جامعه بین الملل سازگاری ندارد. در شرایطی که بیشتر عملیات سایبری بطور بالقوه می تواند توسط افراد و برخی سازمان های تروریستی صورت پذیرد، این ماده، نقش بازیگران غیردولتی را نادیده گرفته است. حقوق بین الملل در شرایط جدید نباید کشورها را وادار کند که در راستای حفاظت از زیرساختهای سایبری خود مجبور باشند یک رشته ملزومات انعطاف ناپذیر برخاسته از تعاریف سنتی اصول توسل به زور و دفاع مشروع را احراز نمایند. شاید یکی از راه حل‌ها در فضای سایبری استثنا قائل شدن برای قوانین سنتی توسل به زور از طریق تهیه فهرستی از تاسیسات زیربنایی یک کشور باشد. با تهیه چنین لیستی، کشورها می توانند برای دفاع از زیرساخت های مذکور، به اقدام دفاعی فعال، بدون اثبات ضرورت، دست زنند. با توجه به فراگیر شدن تهدید حملات سایبری لزوم تعریف مورد اجماع کشورها در خصوص نبرد سایبری در چارچوب الگوی فعلی حقوق مخاصمات مسلحانه و ارائه گزینه های در دسترس به دولتهایی که هدف چنین حملاتی قرار می گیرند احساس می شود.

منابع و مآخذ

۱. اصلانی ,جابر .(1393) .حملات سایبری از منظر حقوق بین الملل، با نگاهی به قضیه استاکسنت و ایران .(*فصلنامه مطالعات بین المللیشماره . 10*)

۲. نواده توپچی ,حسین(1393) .*حقوق جنگ و مخاصمات مسلحانه* .تهران : انتشارات خرسندی

۳. خلف رضایی، حسین خلف (1392) .,حملات سایبری از منظر حقوق بین الملل، *فصلنامه مجلس و راهبرد، سال بیستم، شماره 73ص*.154-125

۴. رضائیان ,مهرداد .(1383) .*حقوق بین الملل ناظر بر هدایت مخاصمات(مجموعه کنوانسیونهای لاهه و برخی اسناد بین المللی دیگر)*. تهران :انتشارات سرسم

۵. شریفی طرازکوهی ,حسین .(1375) .*حقوق جنگ(مجموعه مقالات)*. تهران : انتشارات جدیت پژوهشگاه علوم استراتژیک دانشگاه امام حسین

۶. مالر ,آ .ر .(1382) .*قواعد کاربردی حقوق مخاصمات مسلحانه* .تهران :انتشارات امیرکبیر
۷. نامدار ,غلامرضا .(1397) .بررسی مفهوم دفاع مشروع در پرتو حملات سایبری با تاکید بر حمله استاکس نت به تاسیسات هسته ای ایران .*مجله مطالعات حقوقی دانشگاه شیراز*،صص ۱۲-۲۵
۸. موسی زاده، رضا، فروغی نیا، حسین (1391) .تعریف جنایت تجاوز در پرتو قطعنامه کنفرانس بازنگری اساسنامه دیوان کیفری بین المللی در کامپالا، تهران، *فصلنامه راهبرد*، صص ۱۴۱-۱۷
۹. نیاورانی ,ص .(1386) .*تحول قاعده دفاع مشروع در حقوق بین الملل* .تهران : دانشگاه شهید بهشتی، دانشکده حقوق
10. 31th International Conference of the Red Cross and Red Crescent. (2011). *Report on international Humanitarian Law and the Challenges of contemporary Armed Conflicts. pp 21-22.* Geneva: ICRC.
11. Al, H. e. (2012). The Law of Cyber Attack. *California Law Review* , Vol 100.
12. Annual Review ICRC. (2017). *Weapons contamination.* Geneva: International Comittee Of Red Cross .
13. beck, J.-m. H. (2005). Customery international Humanitarian Law. *ICRC and Cambridge University Press* , Vol,I ,Rules.
14. Brown, D. (2006). Aperposal For an international Convension to Regulate the use of information System in Arned conflicts. *Harvard international law Journal* , Vol.47. No 1. P179.
15. C.Csosseck. (2012). "Attack"as a term of Art in international Low: the Syber Operation Context. *4th international conference on cyber conflict* (p. 291). NATO CCD COE Publication,Tallinn.
16. Camlus, M. (Last Revised, May 2016). cyber attacks and internatinal law of Armad conflicts: a Jus Ad Bellum Prespective. *Journal of internatinal Commercial Law and Technology* , pp 179-189.
17. Campos, M. (2016). Cyber-Attacks and International Law of Armed Conflicts: A 'Jus Ad Bellum' Perspective. *Jornal of Commecial Law and Technology* , 265.
18. Clark.A.Richard. (2010). *Cyber War.* New York: Harper Callins.

19. Departmentof the Navy,Department of Homeland security,USA. (July 2007). *The commanders Handbook on the Law of Naval operations* , ,Para 8.3.
20. Dinniss, H. H. (2012). Syber Warefare and the Law of War. *Cambridge Univercity Press* , 131.
21. Dinstein, Y. (2004). *cambridge university press* , 48.
22. Dinstein, Y. (2004). the conduct os Hostilities under the low of internatinal Armed conflict. *cambridge university press* , 48.
23. Dinstein, Y. (2017). *War aggression and Self- defense 6th Edition.* Geneva.
24. Haslam, E. (2000). Information warfare,Technologocal Changes and international law. *Conflict and Security law* , Vol 5. No 2,P 170.
25. Hathaway, O. (2012,). *the Law of Syber attack.* Vol.100 No 4,p 817: california Law Review.
26. ICJ Reports. (1986). *Case concerning the Military and paramilitary actinities in and against Nicaragua.*
27. ICRC annual Review 2017. (2017). *Humanity in Action, Protecting the Valenerable and Promoting the Law.* Geneva: internatinal comittee of Red cross.
28. International Law Commission. (2001). draft articles on the Responsibilityof States for international Wrongful Acts. *Yearbook of International Law Commission* , Vol. 2.
29. Jesen, E. T. (2010). Cyber Warfare And Precautions against the Effect of attacks. *Texas Law Review* , Vol 88 P 1534.
30. Jr, C. J. (Spring 2011). . Prespectives for Cyber strategies on law forcyberwar. *Strategic Studies Quarterly* , 81.
31. Kelsey, J. T. (2007-2008). Hacking in to international Humanitarian Law:the principles of Distinction,and Neutrality in the age of Syber Warfare. *Michigan Law Review* , Vol 106 p 1439.
32. Mark. R. Shulman. (1999). Discrimination in the law of information Warfare. *Columbia Journal of Transnatinal Law* , Vol 37. p 964.
33. Melzer, N. (2011). Syber Warefar and international Law. *UNIDIR Resourses Paper* , 24.
34. Michael.N.Schmitt. (2011). Syber operations and"Jus in Bello": Key Issues. *Naval War College international low Studies* , Vol.87 p 91.
35. N.Malcom, S. (2008). *International Law.* New York: Cambridge University Press.

36. Oconell, M. E. (29, May 2012). Cyber mania,in Syber Security and international Low. *Meeting Summery in chatham House* .
37. *The ICRC Annual Reports – International Comitee of Red CCross*
38. *International Review of The Red Cross. International Comitee of Red CCross*
39. Pejic, e. i. (Vol 15 206). *International Law and Armed Conflict: Exploring the Faultlines.* Geneva: ICRC.
40. Queguiner, G. F. (.DEC 2006). Precautions Under the Low governing the conduct of Hostilities. *international Rewie qo the Red Cross* , Vol 88.No 864.P 801.
41. R.Laurie, B. (2013). International Law and Syber Treats From Non-state Actors. *International Law StudiesT US Naval War College* , Vol 89.
42. Rid, T. (2013). *Cyber War Will not take Place.* New York: Oxford University Press.
43. Schmitt, M. N. (2014). *1) Tallinn Manual on the International Law Applicable to Cyber Warfare by: Michael N. Schmitt Cambridge University Press 978-1-107-02443-4 - Tallinn Manual on the International Law Applicable to Cyber Warfare.* Geneva: Cambridge University Press 978-1-107-02443-4 - T.
44. schmitt, M. N. (2013). Tallinn manual on the international law applicable to syber warfare. *Cambridge Univercity press* , 249.
45. The ICRC Customery International Humanitarian Law Study. International Law studies. Volume 82. The low of War in 21 Century. Weaponary and use of Force. Yoran Dinstein
46. Schmitt, M. N. (Vol 2. 1999.P 170). the Principle of Discrimination in 21th century Warfare. *Yale Human rights and Development* .
47. Schmitt, M. N. (2002). Wired Warfare, Computer Network Attacks and Jus in Bello. *international Review of the Red Cross Vol 84 No 846* , 377.
48. Schmitt, M. (2017). *Tallin Mannual 2.0 on the international law applicable to cyber operations* . Geneva: the Group of Experts in Nato.
49. Schmitt, w. H. (2015). *the conduct of Hostilities in international Humanitarian Law.*
50. The geneva conventions under aasault. Sarah periggo and jim Whitman.2010. Chicago university

51. Principles of International Humanitarian Law. By (author) Jonathan Crowe , By (author) Kylie Weston-Scheuber
52. Segal, A. (2011). Cyber Space Governance:the next step. *Council of foreghn Relations, Policy innovation Memorandom* , 3.
The Handbook of International Humanitarian Law. Edited by Dieter Fleck. 21 septambre 2009 and 1 Novamber 2014
International Humanitarian Law : Theory, Practice, Context. Pocket Books of the Hague Academy of International Law By (author) Daniel Thürer
53. Shane, S. (2012, Septamber 26). Cyber warfare emerges from Shadows of public discussion by Us officials. *the New York times* , p. A10.
54. thurer, D. (2014). *Internatinal Humanitarian Law,Theory,practice,context.* Hague: Hague Academi of international law.
Paperback. Prepared for publication by Harvard School of Public Health. Program on Humanitarian Policy and Conflict Research , General editor Claude Bruderlein
Judges, Law and War : The Judicial Development of International Humanitarian Law. Cambridge Studies in International and Comparative Law. By (author) Shane Darcy
The New Humanitarians in International Practice : Emerging Actors and Contested Principles. Routledge Humanitarian Studies. Edited by Zeynep Sezgin , Edited by Dennis Dijkzeul
Scope and Applicability of International Humanitarian Law. By (author) Prof. Dr. Wolff Heintschel von Heinegg , Edited by Prof. Michael N. Schmitt
The Changing Face of Conflict and the Efficacy of International Humanitarian Law. Edited by Helen Durham , Edited by Timothy L. H. McCormack , Foreword by A Gilbert
Yearbook of International Humanitarian Law . Other adaptation by Timothy McCormack , Edited by A. McDonald
International Humanitarian Law : Challenges. Edited by John Carey , Edited by William Dunlap , Edited by John R. Pritchard
The Changing Nature of War and Its Impacts on International Humanitarian Law. By (author) Philipp Schweers

International Humanitarian Law Facing New Challenges : Symposium in Honour of Knut Ipsen .Edited by Prof. Dr. Wolff Heintschel von Heinegg , Edited by Volker Epping
The Continued Relevance of International Humanitarian Law in the 21st Century .By (author) P. J. S. Sandhu , By (author) William Bowie
The Changing Nature of War and Its Impacts on International Humanitarian Law .By (author) Philipp Schweers
Unprivileged Belligerents' in International Humanitarian Law : with a Special Focus on the United States' 'War on Terror' .By (author) Gerrit Zach
The New Challenges of Humanitarian Law in Armed Conflicts : In Honour of Professor Juan Antonio Carrillo-Salced .Edited by Pablo Antonio Fernandez-Sanchez
L'application De Droit Humanitaire / The Application of Humanitarian Law 1986 .By (author) Centre for Studies and Research in International Law and International Relations
International Law and Armed Conflict : International Law and Armed Conflict: Exploring the Faultlines .dbaEdited by Michael Schmitt , Edited by Jelena Pejic

55. US Department of Defense. (Nov 2010 Amended on Jun 2011, Washington,Dc). Dictionary of Military and Associated Terms.
56. Walker, B. b. (2011). Confidence- building and international agreement in sybersecurity. *Transparency and confidence- building in syber space,towared norms of behaviour* (p. issue 4). UNIDIR Disarmamant forum.