چکیده نوشتارها

حملات سایبری از منظر حقوق بین‌الملل بشردوستانه با نگاهی به قضیه استاکس‌نت و ایران

جبار اصلانی

بررسی ابعاد و جوانب حقوقی مختلف پدیده نوین و پیچیده حملات سایبری در دنیای امروز و در چهارچوب قواعد حقوق بین‌الملل معاصر نه تنها ضروری و مهم بلکه اجتناب ناپذیر نیز می‌نماید. جستار حاضر به تبیین مفاهیم فنی و کلیدی فضای سایبر و حملات سایبری پرداخته و جوانب حقوقی این موضوع را مورد سوال، بررسی و تحلیل قرار داده است و زوایای ناگفته و پنهان این پدیده در عرصه ادبیات حقوقی حقوق بشردوستانه بین‌المللی را تا حدی روشن و تبیین نموده و به این رهیافت نایل گردیده است که قواعد و مقررات موجود در حقوق بشردوستانه ناظر بر مخاصمات مسلحانه به علت جنس و بستر شکل‌گیری متفاوت این نوع از حملات، قادر به پوشش کامل این پدیده نیست و احتمالاً نیاز به وضع و تدوین قواعد و سازوکارهای جدید در این حوزه وجود دارد.

کلید واژگان: فضای سایبر، حمله سایبری، حقوق بشردوستانه، حقوق بین‌الملل، اصول بشردوستانه.

حملات سایبری از منظر حقوق بین‌الملل بشردوستانه با نگاهی به قضیه استاکس‌نت و ایران

جبار اصلانی*

دیباچه

بشر از دوران اولیه شکل‌گیری تمدن و متعاقب مفهوم یافتن منافع جمعی و مشترک در قالب و اشکال مختلف تا به دوره حاضر به مبارزه ادامه داده و خواهد داد. یکی از نمادهای بارز و برجسته این مبارزات همواره جنگ و مخاصمه (دوجانبه و چندجانبه) بوده که به اشکال و با تمسک به ابزارهای مختلفی همچون سرنیزه، شمشیر، سلاح‌های گرم، توپ و تانک، هواپیما، بمب‌های خوشه‌ای، میکروبی، هسته‌ای و اخیراً نیز سایبری و کامپیوتری نمود و ظهور پیدا کرده است.

آنچه که در این میان عیان و البته حائز اهمیت است، این مهم است که از دیرباز قواعد و اصولی کلی بر این مخاصمات حاکم بوده که ابتداء به ساکن به صورت رسوم و سنت‌های

* جبار اصلانی دانشجوی دکتری حقوق بین‌الملل دانشگاه تهران است (jabbar968@yahoo.com).

تاریخ دریافت: ۱۳۹۲/۶/۴ تاریخ پذیرش: ۱۳۹۲/۱۰/۲۰
فصلنامه مطالعات بین‌المللی (ISJ)، سال دهم، شماره ۴، بهار ۱۳۹۳، صص ۲۹-۱.

جنگی و با گذر زمان و رشد نهادهای حقوقی در جوامع بشری با سیمای قواعد عرفی و نظامات مدون و موضوعه (نظیر معاهدات و قراردادهای دو و چندجانبه) ظهور یافته است؛ به طوری که نقطه عطف چنین تکاملی همانا تصویب کنوانسیون‌های چهارگانه ژنو ۱۹۴۹ و پروتکل‌های الحاقی مصوب ۱۹۷۷ می‌باشد که بدون تردید از اقبال و اجماعی جهانی در عرصه حقوق حاکم بر مخاصمات مسلحانه بین‌المللی و داخلی برخوردار است. آنچه که در این خصوص واضح و روشن است این مسأله است که مجموعه این قواعد و مقررات (حقوق بین‌الملل بشردوستانه) و سایر اصول و مقررات حاکم بر فضای مخاصمات مسلحانه بین‌المللی و داخلی اساساً و اصولاً جهت تنظیم رژیم حقوقی حاکم بر مخاصمات سنتی و کلاسیک وضع شده‌اند و به طور کلی روند مخاصماتی از این نوع را مدیریت و کنترل می‌کنند.

اخیراً با روند رو به رشد چشمگیر و بعضاً اعجاب‌انگیز تکنولوژی در همه عرصه‌ها و به ویژه در قلمرو ابزار و ادوات نظامی و تسلیحاتی و پیوند این رشد تکنولوژیکی با شبکه گسترده و پیچیده اینترنت و سایبری در سطح جهانی، پدیده نوظهور دیگری را موجب و وارد معادلات حیات جمعی بشر نموده است که از آن به عنوان جنگ‌های الکترونیک، عملیات‌های اطلاعاتی و به عبارت دیگر و بهتر حملات و جنگ‌های سایبری که در فضای مجازی به عنوان تهدیدی واقعی رخ می‌دهند، یاد می‌شود. پرواضح است که بروز و ظهور چنین پدیده نوظهوری در روابط خصمانه میان کشورها به طور قطع مستلزم کنکاش، تفحص، تأمل و یافتن راهکارهای حقوقی مناسب جهت نظام‌مند کردن این پدیده در آینده نزدیک خواهد بود. بدیهی است که هدف اصلی و غایت حقوق بین‌الملل بشردوستانه حمایت از تمامیت فیزیکی و روانی انسان در هر وضعیتی از مخاصمه است و دغدغه و کارویژه اصلی این حوزه مهم از حقوق بین‌الملل همانا وضع قاعده بر موقعیت‌ها و وضعیت‌های مستحدثه در حوزه حقوق مخاصمات است. مضاعف شدن اهمیت این موضوع شاید محصول پیشرفت تکنولوژی در فضای مجازی و سایبر در یک دهه اخیر باشد چرا که مواردی عینی از نبردهای سایبری میان دولت‌ها طی مخاصمات مسلحانه رخ داده است[1] تا حدی که توجه جهانیان به ویژه مقامات سیاسی-نظامی کشورها و حقوقدانان بین‌المللی را به خود معطوف ساخته است.

بنابراین، بررسی ابعاد و جوانب حقوقی مختلف این پدیده در دنیای امروز و در چهارچوب قواعد حقوق بین‌الملل معاصر نه تنها ضروری و مهم، بلکه اجتناب ناپذیر نیز می‌نماید. با توجه به آنچه گفته شد، جستار حاضر سعی بر آن دارد تا جوانب حقوقی این

موضوع را مورد سوأل، بررسی و تحلیل قرار بدهد تا زوایـای ناگفتـه و پنهـان ایـن پدیـده در عرصه ادبیات حقوقی حقوق بین‌الملل بشردوستانه روشن و شفاف گردد.

۱. تعریف فضای سایبر

در رابطه با فضای سایبر، واقعیت این است که تعریف جامع و مانعی که مورد اتفاق نظر عموم باشد وجود ندارد و تعاریف مختلفی از این اصطلاح عرضه گردیده است. در مجموع، می‌توان بر آن بود که تعاریف ارائه شده یا دربردارنده این هستند کـه فضـای سـایبر در عـرض دنیـای واقعی مطرح شده است یا آن را همچون منبعی برای تبـادل اطلاعـات دانسـته‌انـد و یـا اینکـه فضای سایبر را با دیدی سخت‌افزارانه نگریسته و آن را تشکیل یافته از اتصـال بـی‌شـماری از کامپیوترها و سامانه‌ها می‌دانند که بررسی این معیارها بـا عنایـت بـه ابعـاد فنـی آن بـه عهـده خواننده گذاشته می‌شود.

۲. مفهوم جنگ سایبری[۲]

همان گونه که اجماعی در خصوص تعریف فضای سایبری وجود نـدارد، راجـع بـه مفهـوم و تعریف جنگ سایبری هم اتفاق‌نظر وجود ندارد. با این حال، جهت تنویر ابعاد فنی و تکنیکـی بحث، به ارائه برخی از تعاریف موجود در این راستا پرداخته می‌شود تـا حـوزه مفهـومی ایـن اصطلاح فنی درهاله‌ای از ابهام قرار نگیرد. بـرای نمونـه، وزارت دفـاع امریکـا «عملیـات‌هـای سایبری»[۳] را بکارگیری توانمندی‌های سایبر در جایی می‌داند که هدف اصلی آنها کسب نتـایج نظامی در فضـای سـایبر یـا از طریـق آن باشـد و در عـین حـال، عنـوان مـی‌دارد کـه چنـین عملیات‌هایی شامل فعالیت‌های شبکه‌محور کامپیوتری برای انجـام عملیـات و دفـاع از شـبکه اطلاعاتی جهانی می‌باشد.[۴] این وزارت، عبارت «حمله شبکه‌محور کامپیوتری»[۵] را «اقداماتی بـا استفاده از شبکه‌های کامپیوتری جهت ایجاد اختلال، قطـع سـرویس، پـایین آوردن کیفیـت یـا نابودی اطلاعات در کامپیوترها و شبکه‌های کامپیوتری یا خود کامپیوترها و شبکه‌هـا» تعریـف می‌کند.[۶] علاوه بر این، مرکز پژوهش‌های کنگره امریکا نیز در سال ۲۰۰۱ ابراز داشت که جنگ سایبر را می‌توان برای توصیف جنبـه‌هـای گونـاگون دفـاع در برابـر شـبکه‌هـای اطلاعـاتی و کامپیوتری و حمله به آنها در فضای سایبر و نیز جلوگیری از دست‌زدن دشمن به چنین کـاری مورد استفاده قرار داد.[۷] مرکز مزبور در سال ۲۰۰۶ عبارت حمله شبکه‌محـور کـامپیوتری را بـه

عنوان «عملیات‌هایی برای اختلال یا نابودی اطلاعات موجود در کامپیوترها و شبکه‌های کامپیوتری» تعریف می‌کند. گزارش یاد شده اشعار می‌دارد که یکی از خصائص برجسته و بارز این نوع از حملات آن است که بر جریان داده‌هایی اتکا دارد که به عنوان سلاحی برای اجرای یک حمله مورد استفاده قرار می‌گیرد، برای نمونه، ارسال سیگنال دیجیتال از طریق شبکه برای کنترل کننده جهت از کار انداختن جریان برق.[۸] در تعریفی دیگر، «کوین کولمن»[۹]–مشاور و کارشناس مدیریت استراتژیک مؤسسه «تکنولتیکس»[۱۰]– جنگ سایبری را اینگونه تعریف می‌کند: «نبردی که از حملات یا اقدامات خصمانه و غیرقانونی علیه کامپیوترها و شبکه‌ها در راستای ایجاد اختلال در ارتباطات و دیگر بخش‌های زیرساختی به عنوان مکانیزمی برای وارد ساختن ضربات اقتصادی یا از کار انداختن تمهیدات دفاعی استفاده می‌کند».[۱۱]

لازم به ذکر است که عملیات‌های جنگ سایبری نیز بسان جنگ‌های سنتی و معمول، دارای سلاح‌ها و ابزارهای مخصوص به خود می‌باشند که به اختصار عبارتند از: ۱. حمله قطع سرویس؛ ۲. برنامه‌های مخرب؛ ۳. بمب منطقی؛ ۴. جعل‌ای پی؛ [۱۲] ۵. دستکاری دیجیتالی؛ ۶. عملیات‌های جاسوسی سایبری. گروه متخصصین و کارشناسان بین‌المللی نیز در گزارش راهنمای «تالین»، [۱۳] حمله سایبری را به عنوان بخشی از عملیات سایبری در قالب تهاجمی و تدافعی در نظر گرفته‌اند که نتیجه منطقی و مورد نظر آنها ورود خسارات جانی و مالی به اشخاص و اموال می‌باشد و با ابتناء بر این تعریف، به قابلیت اعمال قواعد حقوق بین‌الملل بر حملات سایبری پرداخته‌اند.[۱۴]

در نهایت، باید متذکر شد که وجود تعاریف مختلف از اصطلاح جنگ سایبری، نشان از دشواری تعریف دقیق این مفهوم و تعیین حدود و ثغور آن دارد. با این حال، آنچه که در دنیای امروز در فضای لایتاهی و مبهم سایبر به صورت خزنده اثرات منفی و مخرب خود را در عرصه عمل به منصه ظهور رسانده است، توسل به این فضا جهت ورود خسارت مالی و گاهی جانی به انسان‌های مقیم در قلمرو ملی کشورهاست که بدون تردید، حوزه‌های مختلف حقوق بین‌الملل و به طور خاص حقوق بشردوستانه بین‌المللی را تحت تأثیر قرار داده و فعّالان این حوزه‌ها را ناگزیر به واکنش کرده تا این پدیده را هنجارمند کرده و آن را با قواعد موجود و یا احتمالاً قواعد جدید نظام‌مند کنند.

۳. قابلیت اعمال حقوق بشردوستانه بر حملات سایبری (CNA) [۱۵]

پرسشی که در اینجا مطرح می‌شود اینست که آیا حملات مبتنی بر شبکه کامپیوتر (که از این به بعد حملات سایبری خوانده می‌شود) می‌توانند موضوع حقوق بشردوستانه بوده و تحت لـوای قواعد حقوقی این حوزه از حقوق بین‌الملل قرار بگیرند یا خیر؟ واقعیت امر اینست که که هیچ یک از قواعد و مقررات موجود حقوق بشردوستانه –اعم از موضـوعه و عرفـی– بـه صـورت مستقیم مسأله حملات سایبری را مورد توجه قرار نداده‌اند. از این رو، در نگاه نخست، به نظـر می‌رسد که این نوع حملات در جریـان مخاصـمات مسـلحانه هنـوز هنجارمنـد و قاعـده‌منـد نشده‌اند. علاوه بر این، می‌توان قایل به این شد که گسترش و توسل به حملات سایبری به بعد از حقوق معاهداتی موجود برمی‌گردد و از این رو مستثنی از پوشش موضوعی قواعـد موجـود است. البته، ممکن است استدلال سومی نیز در این حوزه وجود داشته باشد دال بر اینکه قواعد حقوق بشردوستانه صرفاً برای روش‌ها و ابزارهای مربوط به مخاصمات فیزیکی و سنتی وضع و تدوین شده‌اند و بنابراین، قواعد یاد شده نسبت به حمـلات سـایبری قابـل اعمـال نیسـتند، چراکه حملات سایبری شکل فیزیکی و سنتی مرسوم را نداشـته و بـه همـین دلیـل خـارج از قلمرو موضوعی حقوق بشردوستانه قرار می‌گیرند.[۱۶] این استدلال که کنوانسـیون‌هـای موجـود درباره خصوص حملات سایبری سکوت اختیار کرده‌اند، خیلی حائز اهمیت نیست.

نخست، شرط مارتنس به عنوان یکی از اصول کلی پذیرفته شده حقوق بشردوستانه مقرر می‌دارد که؛ هرگاه موقعیت یا وضعیتی توسط موافقت‌نامه‌های بین‌المللـی تحـت پوشـش قـرار نگرفته باشند، غیرنظامیان و رزمندگان تحت حمایت و حاکمیت قواعد و اصـول کلـی حقـوق بین‌الملل –که منتج از عرف تثبیت شده، اصول انسانیت و مناسبات مربوط به وجـدان عمـومی می‌باشند– قرار می‌گیرند.[۱۷] به واسطه وجود چنین هنجاری، تمـامی رویـدادهایی کـه در حـین مخاصمات مسلحانه رخ می‌دهند، خارج از دایره و اصول حقوق بشردوستانه نخواهنـد بـود و این قواعد بر همه حالات و وضعیت‌های مستحدثه در طول مخاصمات حاکم خواهد بود.

با پذیرش و قبول عرف بین‌المللی به عنوان یکی از منابع حقـوق بـین‌الملـل در مـاده ۳۸ اساسنامه دیوان دادگستری بین‌المللی، نادرست بودن ادعـای یـاد شـده در رابطـه بـا حمـلات سایبری آشکار می‌گردد و مؤید قابلیت اعمال حقوق بشردوستانه در این باره اسـت. همچنـین، وجود چنین منبعی (عرف) لزوم وجود منابع مکتوب و معاهداتی را برای حاکمیت این قواعـد بر وضعیت‌های از قبل پیش‌بینی نشده همانند حملات سایبری را نفـی مـی‌کنـد. تجلـی مبـانی

استدلالی این گفته به وضوح در رویه قضایی بین‌المللی به چشم می‌خورد که از جمله می‌توان به قضایایی همچون فلات *قاره دریای شمال*،[18] *قضیه لوتوس*[19] و همچنین *قضیه پناهندگی*[20] اشاره کرد.

این نحوه استدلال در رأی مشورتی دیوان در *قضیه مشروعیت تهدید یا استفاده از سلاح‌های هسته‌ای* نیز مورد توجه قرار گرفته است. در این رأی، دیوان این استدلال را که قواعد و اصول بشردوستانه مقدم بر ساخت و ابداع سلاح‌های هسته‌ای رشد کرده است و از این رو، قواعد حقوق بشردوستانه قابلیت اعمال خود را بر این وضعیت از دست می‌دهند، رد نمود. همانگونه که دیوان مقرر داشت، از دیدگاه بیشتر کشورها و همچنین، از نقطه‌نظر علما و دکترین، هیچ‌گونه تردیدی در رابطه با قابلیت اعمال حقوق بشردوستانه در خصوص سلاح‌های هسته‌ای وجود ندارد.[21] با این استدلال دیوان، هیچ دلیلی برای تمایز قائل شدن میان سلاح‌های هسته‌ای و حملات سایبری یا سلاح‌های کامپیوتری وجود ندارد.

افزون بر این، بازنگری سلاح‌های نوین و سیستم این تسلیحات جهت مطابقت و تطبیق با حقوق بشردوستانه، بدون تردید، یک نیاز قانونی و هنجاری است که مستلزم اتخاذ یک سیاست حقوقی کلی و جامع است.[22] تحلیل بالا در صورتی درست است که بتوان حملات سایبری را به عنوان مخاصمه در مفهوم سنتی آن در نظر گرفت، در غیر این صورت، اساساً موضوعیت خود را از دست می‌دهد و نمی‌توان قواعد حقوق بشردوستانه را اعمال نمود. در حقیقت، وجود مخاصمه در مفهوم سنتی و فیزیکی آن از جمله شروط لازمی است که قواعد حقوق مخاصمات مسلحانه را فعال ساخته و حاکم می‌گرداند. ماده ۲ مشترک کنوانسیون‌های چهارگانه ژنو ۱۹۴۹ مقرر می‌دارد که مقررات این کنوانسیون‌ها –جدای از مقررات خاصی که مربوط به زمان صلح است– نسبت به تمامی مواردی که در آن اعلام جنگ شده یا هر مخاصمه مسلحانه دیگری که ممکن است میان دو یا چند طرف متعاهد رخ بدهد، حتی اگر وضعیت جنگی توسط آنها تأیید نشده باشد، قابل اعمال خواهد بود. پروتکل الحاقی اول ۱۹۷۷ نیز همین استاندارد (وجود و وقوع مخاصمه مسلحانه) را جهت قابلیت اعمال قواعد خود پذیرفته است. لازم به ذکر است که برخی از مواد پروتکل مزبور تقریباً جنبه عرفی یافته و مورد اقبال عمومی قرار گرفته است. همان‌گونه که گفته شد، با آغاز مخاصمه مسلحانه، قواعد حقوق بشردوستانه و اعمال آنها موضوعیت پیدا می‌کنند. افزون بر این، *گروه بین‌المللی متخصصین و کارشناسان* در گزارش راهنمای تالین (درباره حقوق بین‌الملل قابل اعمال بر جنگ سایبری)

همگی بر این باور هستند که حقوق مخاصمات مسلحانه بر حملات سایبری قابل اعمال است، البته، منوط به این که مفهوم حمله مسلحانه در این نوع از حملات متجلی و محقق شود.[۲۳]

پرسشی که در اینجا مطرح می‌شود این است که مفهوم مخاصمه مسلحانه چیست؟ نظریات تفسیری کمیته بین‌المللی صلیب سرخ درباره کنوانسیون‌های ژنو ۱۹۴۹ و پروتکل‌های الحاقی ۱۹۷۷ رویکرد بسیار موسعی را در قبال مفهوم مخاصمه مسلحانه اتخاذ کرده است. رویکرد یاد شده، مخاصمه مسلحانه را به عنوان «هرگونه اختلاف رخ داده میان دو کشور که منجر به مداخله نیروهای مسلح شده است، حتی اگر یکی از طرفین وجود وضعیت جنگی را انکار نماید» تعریف می‌کند.[۲۴] به همین ترتیب، نظریه تفسیری درباره پروتکل الحاقی اول به طور خاص مقرر می‌دارد که: «حقوق بشردوستانه هرگونه اختلافی را میان دو کشور از جمله استفاده از نیروهای مسلح آنها را در بر می‌گیرد. در این باره، نه مدت مخاصمه و نه میزان شدت آن نقشی در تحقق مخاصمه ندارد.»[۲۵] در همه موارد یاد شده، تحقق حمله مسلحانه توسط نیروهای مسلح طرفین درگیر از جمله شروط لازم تلقی می‌شود. با این حال، منازعه یا اختلافی که ناشی از درگیری‌های نیروهای مسلح است، نمی‌تواند یک معیار صرف برای تحقق حمله مسلحانه باشد. افزون بر این، در حال حاضر به طور کلی پذیرفته شده است که رویدادهایی نظیر تنش‌های مرزی یا حملاتی با مقیاس کوچک که به سطح مخاصمه مسلحانه نرسیده‌اند، در حقوق بشردوستانه مخاصمه مسلحانه تلقی نمی‌شوند.[۲۶] بدین ترتیب، رویه دولت‌ها که توسط دکترین نیز مورد حمایت قرار گرفته است، نشان می‌دهد که به تدریج از اهمیت فقدان شدت و استمرار قید شده در پروتکل الحاقی اول کاسته شده و تا حدی تعدیل شده است.

در رابطه با موضوع اصلی مورد بحث باید گفت که جدای از موضوعات مربوط به حقوق توسل به زور، قواعد و اصول حقوق بشردوستانه در صورتی نسبت به حملات سایبری قابل اعمال خواهد بود که بتوان حملات سایبری صورت گرفته را به کشوری معین منتسب کرد و گستره این حملات نیز بایستی فراتر از حملات پراکنده و حوادث موردی باشد. افزون بر این، چنین حملاتی باید عامدانه و همراه با قصد ورود خسارت یا تخریب، مرگ یا ایجاد جراحت بوده و یا اینکه چنین عواقبی از این حملات قابل پیش‌بینی باشد. با اتخاذ و پذیرش معیار یاد شده، حمله سایبری علیه سیستم کنترل تردد هوایی توسط عوامل رسمی یک کشور می‌تواند فتح‌البابی برای اعمال قواعد حقوق بشردوستانه باشد. همین وضعیت، در صورتی که حملات

سایبری صورت گرفته با قصد تخریب لوله‌های نفتی از طریق ایجاد اختلال در سیستم کنترل شریان‌های نفتی باشد[۲۷] یا اینکه حمله سایبری منجر به ذوب شدن راکتورهای هسته‌ای از طریق دستکاری در سایت‌های مرکزی پایگاه‌های هسته‌ای بشود، صادق خواهد بود. از سوی دیگر، حقوق بشردوستانه اقدامات ذیل را به این دلیل که منجر به ایجاد صدمه، مرگ، خسارت یا تخریب نمی‌شوند، تحت پوشش قرار نمی‌دهد: قطع کردن و ایجاد اختلال در شبکه اینترنت دانشگاه‌ها؛ دانلود کردن و دستیابی به اسناد و اطلاعات مالی؛ قطع اینترنت و ایجاد اختلال در دسترسی موقت به آن یا کنترل و مدیریت جاسوسی سایبری. افزون بر موارد یاد شده، در گزارش تالین این نکته مورد اشاره و بررسی قرار گرفته است که برای مثال، حملات سایبری انجام شده علیه کشور استونی در سال ۲۰۰۷، علیرغم این که زیرساخت‌ها و شبکه کامپیوتری این کشور مورد هجوم و دچار اختلال گسترده گردید، ولی چون منجر به تحقق حمله مسلحانه نگردید، از این رو، حقوق مخاصمات مسلحانه در مورد آن قابل اعمال نمی‌باشد. بر عکس، در مخاصمه میان روسیه و گرجستان، حملات سایبری صورت گرفته در حین مخاصمه، مشمول مفهوم حمله مسلحانه شده و در نهایت، حقوق مخاصمات در این رابطه قابل اعمال می‌باشد.[۲۸]

با رشد تکنولوژی و تأثیر شگرف آن در گسترش و خلق ابزارها و شیوه‌های جنگی نوین، بدیهی است که معیار بازیگر–محوری جهت اعمال حقوق بشردوستانه در حملات سایبری کافی نیست و باید معیار نتیجه–محوری را بیشتر مدنظر قرار داد و به نظر می‌رسد که پذیرش معیار اخیر مناسب‌تر و معقول‌تر باشد. واقعیت این است که ظهور این نوع از مخاصمه (حملات سایبری) از نظر قانونی و رویه‌ای بسیار دشوار و سخت به نظر می‌رسد. برای مثال، هیچ‌کس نمی‌تواند منکر این باشد که سلاح‌های شیمیایی یا بیولوژیکی در حوزه حقوق بشردوستانه قرار دارد. اعمال معیار نتیجه–محوری به واسطه وجود این واقعیت مطلوب می‌نماید که به محض وقوع حمله مسلحانه و فارغ از ممنوعیت‌های مربوط به سلاح‌های خاص، روش‌هایی که منجر به مرگ، جراحت و ایجاد خسارت می‌شوند، هیچ‌گونه محملی برای توجیه مشروعیت اعمال ارتکابی نخواهند داشت. هدف قرار دادن غیرنظامیان یا سایر افراد و اموال مورد حمایت به صورت عمدی –فارغ از روش‌ها یا ابزار بکار گرفته شده– غیرقانونی تلقی می‌شوند. ایجاد شرایط قحطی و گرسنگی، تیراندازی به سوی غیرنظامیان، بمب‌گذاری و حتی حملات سایبری اگر منجر به نتایج و عواقب پیش‌گفته بشوند (مرگ، جراحت و خسارت یا تخریب)، همگی در قلمرو حقوق بشردوستانه قرار می‌گیرند. در

گزارش تالین نیز، به روشنی، به قابلیت اعمال حقوق مخاصمات در این باره اشاره شده است.[۲۹] ممکن است مخالفین در مقابل این گونه استدلال کنند که در حملات سایبری نیروهای مسلح و نظامی به مفهوم واقعی و فیزیکی وجود ندارند و بنابراین در قلمرو حقوق بشردوستانه قرار نمی‌گیرند. در پاسخ باید گفت که شرط اصلی اعمال حقوق بشردوستانه در این موارد تنها ایجاد عواقب و تبعات ناشی از این حملات است که قابلیت اعمال و یا عدم اعمال حقوق بشردوستانه را روشن می‌کند.

۴. قربانیان حملات سایبری

همان‌گونه که گفته شد، حملات سایبری اگر بخشی از یک حمله مسلحانه کلاسیک یا یک جنگ سایبری باشند که منجر به ورود صدمه، خسارت یا تخریب و مرگ افراد بشوند یا بروز چنین عواقب و تبعاتی از این حملات قابل پیش‌بینی باشد، تابع حقوق بشردوستانه خواهند بود. در اینجا، ضروری است که مخاطبین و به عبارتی قربانیان حملات سایبری مشخص بشوند. از آنجایی که مفاد پروتکل الحاقی اول استانداردهای قابل اعمال بر کشورهای عضو و غیرعضو را به صورت همسان و برابر برمی‌شمرد، از این رو، این سند می‌تواند نقطه شروع مطلوب و موجهی در این باره باشد. ماده ۴۸ این پروتکل، به عنوان قاعده بنیادین مربوط به حمایت از جمعیت غیرنظامی مقرر می‌دارد: «طرفین مخاصمه عملیات‌های خود را فقط علیه اهداف و و مقاصد نظامی انجام خواهند داد». از نظر ظاهری، ماده یاد شده هرگونه عملیات نظامی، از جمله حملات سایبری، که مستقیماً علیه سایر مقاصد و اهدافی که نظامی نیستند را ممنوع کرده است. مواد بعدی نیز به خوبی ممنوعیت حمله علیه افراد و اموال غیرنظامی را اعلام کرده‌اند.[۳۰]

با این حال، با فرض اینکه عملیات سایبری حمله تلقی بشود، هدف یا اهداف چنین عملیات یا حملاتی چه چیزها یا چه کسانی خواهند بود؟ از نظر تحلیلی، اهداف بالقوه حملات سایبری را می‌توان در سه دسته تقسیم‌بندی کرد که عبارتند از: ۱. رزمندگان و اهداف نظامی؛ ۲. غیرنظامیان و اهداف غیرنظامی؛ ۳. اهداف و اموالی که می‌توانند هم کارکرد نظامی و در عین حال غیرنظامی داشته باشند.[۳۱] افزون بر این، انواع خاصی از این اهداف بالقوه از حمایت‌های ویژه و خاص برخوردار هستند که در ذیل به تفصیل مورد بررسی قرار می‌گیرند.

۱-۴. رزمندگان و اهداف نظامی

رزمندگان و اهداف نظامی به واسطه اهمیتی که دارند اهداف طبیعی در طول مخاصمات مسلحانه تلقی شده و روشن است که می‌توانند به صورت مستقیم مورد حمله و هدف قرار بگیرند. البته، باید یادآور شد که حمله به رزمندگان و اهداف نظامی باید تابع محدودیت‌های حاکم بر بکارگیری شیوه‌ها و ابزارهای نظامی باشد. کسانی که به اهداف نظامی و رزمندگان حمله می‌کنند، باید همواره به این تعهد پای‌بند باشند که تمامی تلاش خود را بکار گیرند تا فقط اهداف مشروع و مجاز را هدف قرار دهند. اهداف مشروع در حقوق مخاصمات به اهدافی گفته می‌شوند که بر اساس حقوق بشردوستانه بین‌المللی از مصونیت بهره‌مند نیستند.[۳۲]

رزمنده به عضوی از اعضای نیروهای مسلح (به استثنای کارکنان بهداری و کارکنان مذهبی) اطلاق می‌شود. نیروهای مسلح عبارتند از: تمامی نیروهای مسلح سازمان یافته، گروه‌ها و واحدهایی که تحت نظر فرماندهی قرار دارند که در قبال اعمال زیردستان خود در برابر طرف مقابل مسوول هستند و متعهد به اجرای قواعد حقوق بشردوستانه بین‌المللی در طول مخاصمات هستند.[۳۳] برای نمونه، حملات سایبری در مواردی می‌تواند به صورت مستقیم علیه رزمندگان صورت بگیرد که چنین حمله‌ای علیه سیستم کنترل ترافیک هوایی نظامی طرف متخاصم بوده و هدف از انجام آن، انتقال نادرست اطلاعات هوانوردی برای ایجاد مشکل و اختلال در پرواز هواپیماهای نظامی طرف مقابل باشد.

پروتکل الحاقی اول ۱۹۷۷ اهداف نظامی را در ماده ۵۲ به شرح ذیل تعریف می‌کند: «اهداف نظامی به اموالی محدود می‌شود که به لحاظ ماهیت، محل، هدف یا کاربرد آنها سهم مؤثری در عملیات نظامی داشته و تخریب کلی یا جزئی، یا از کار انداختن آنها در شرایط زمانی موجود یک مزیت نظامی معین به شمار رود. تجهیزات و ادوات نظامی –به استثنای تجهیزات پزشکی یا آیتم‌های مذهبی–اهداف نظامی تلقی می‌شوند و بنابراین می‌توانند به صورت مستقیم هدف حملات سایبری قرار بگیرند. با این توصیف، تعیین و تشخیص این که کدام یک از تجهیزات و ادوات اهداف نظامی قلمداد می‌شوند، صرف نظر از نمونه‌های روشن و بدیهی آن، اغلب کار مشکلی به نظر می‌رسد.[۳۴]

مشکل اصلی در اینجا احراز و تأیید ارتباط لازم میان هدف مورد حمله و عملیات نظامی است. پیچیدگی و بغرنج بودن این معما در حقیقت به مسأله تفسیر واژگان «مؤثر» و « قطعی» برمی‌گردد. برخی همچون کمیته بین‌المللی صلیب سرخ این عبارات را بسیار مضیق تفسیر

می‌کنند. بر اساس نظریه تفسیری کمیته بین‌المللی صلیب سرخ در خصوص پروتکل الحاقی اول، بخش مؤثر شامل اهدافی است که به صورت مستقیم توسط نیروهای مسلح مورد استفاده قرار می‌گیرند، مانند سلاح و ادوات نظامی، پل‌ها و اهدافی که برای مقاصد نظامی بکار گرفته می‌شوند.[۳۵] اما در رابطه با مزیت‌های قطعی نظامی، نظریه تفسیری بالا حملاتی را که فقط منجر به مزایای نظامی بالقوه یا نامعین و مبهم می‌شوند، استثناء کرده است.[۳۶] در مقابل، ایالات متحده امریکا قائل به یک نوع تفسیر موسع و گسترده است. به طوری که این کشور اهداف اقتصادی را –که به صورت غیرمستقیم ولی مؤثر مقاصد نظامی و ظرفیت‌های جنگی دشمن را حمایت و تقویت می‌کند– جزو مزایای نظامی می‌داند.[۳۷] چنین تمایزی در تفسیر، نتایج جالب توجهی را در قبال حملات سایبری به همراه دارد. آیا یک سیستم بانکداری به این دلیل که متولی انجام حمایت‌های مادی از برنامه‌های نظامی است، می‌تواند به عنوان یک هدف نظامی مؤثر مورد حمله سایبری قرار بگیرد؟ در رابطه با بازار بورس به چه صورت خواهد بود؟ اگر کشوری به یک صنعت خاص –همانند نفت– برای تأمین درآمدهای صادراتی تکیه کرده باشد، آیا حملات سایبری می‌تواند برای ایجاد اختلال در شبکه تولید و توزیع محصول مورد استفاده قرار بگیرد و آیا اصولاً می‌توان در چنین مواردی به حملات سایبری متوسل شد؟ مسأله هدف قرار دادن اهداف اقتصادی از حساسیت بسیار بالایی برای کشورها برخوردار است زیرا این نوع از عملیات اغلب با ابزارهایی همچون کامپیوتر و بهره‌گیری از فضای سایبر انجام می‌شوند و از این رو، اهداف مزبور برای حملات سایبری از جذابیت بسیار بالایی برخوردار هستند. موضوع اصلی در اینجا این است که آیا حمله سایبری انجام شده الزاماً باید منجر به ورود خسارات و صدمات مالی و جانی شده باشد یا خیر. اگر این معیار را در نظر بگیریم، تفاسیر متفاوتی از اهداف نظامی ظهور پیدا می‌کنند که در تمامی احتمالات منجر به تحقق نتایج نابرابر و مختلفی در رابطه با مشروعیت حملات انجام گرفته نسبت به هدف خواهند شد. از سوی دیگر، اگر عملیات انجام شده، برای مثال، تنها منجر به عدم دسترسی موقت به خدمات عمومی بشود، در نتیجه، می‌توان گفت که چنین حملاتی هنوز به سطح حمله نرسیده‌اند و بدین ترتیب، فارغ از ارتباط اهداف با عملیات‌های نظامی، مجاز تلقی خواهند شد. برای نمونه، ایستگاه تلویزیونی صربستان در طول حملات ناتو علیه این کشور در سال ۱۹۹۹ طی یک حمله سایبری مورد هدف قرار گرفت که هیچ‌گونه تلفات جانی و مالی را به همراه نداشت. در چنین شرایطی، به انتقادهای وارده مبنی بر اینکه یک هدف غیرنظامی (تلویزیون ملی یک

کشور) مورد هدف قرار گرفته است، وقعی نهاده نشد و رسانه‌ها نیز از پوشش و تحلیل چنین حمله‌ای خودداری کردند و حتی دعوی مطروحه در دیوان اروپایی حقوق بشر در این باره غیرقابل استماع تشخیص داده شد.[۳۸]

۲-۴. افراد و اموال غیرنظامی

افراد غیرنظامی به اشخاصی گفته می‌شود که رزمنده نیستند[۳۹] و منظور از هدف و اموال غیرنظامی هدفی است که نظامی نباشد.[۴۰] ممنوعیت حمله علیه افراد و اموال غیرنظامی تقریباً مطلق است. به طور خاص، پروتکل الحاقی اول در این باره اعلام می‌دارد که سکنه غیر نظامی و افراد غیر نظامی نباید مورد حمله قرار بگیرند و همچنین، اعمال تهدیدهای خشونت‌آمیز که هدف اصلی آن ایجاد ترس و وحشت در میان سکنه غیر نظامی باشد، ممنوع است (بند ۲ ماده ۵۱). اموال غیرنظامی نباید هدف حمله یا اقدامات تلافی‌جویانه قرار بگیرند.[۴۱] در صورت وجود تردید در خصوص ماهیت یک فرد یا یک هدف (اینکه نظامی است یا غیرنظامی) همواره مسأله به نفع وضعیت غیرنظامی بودن حل و فصل می‌شود و به عبارتی تردیدها به نفع غیرنظامی بودن است.[۴۲]

به همین صورت، در مورد حملات سایبری نیز موضوع اصلی و اساسی این است که آیا حمله صورت گرفته منجر به ورود صدمات و یا خسارات جانی و مالی شده و یا احتمال ورود چنین خسارات و صدماتی می‌رود یا خیر؛ اگر چنین باشد، ممنوعیت‌های پیش‌گفته که بدون تردید ریشه در حقوق عرفی موجود دارند، قابل اعمال خواهند بود. علیرغم روشن بودن این قواعد و هنجارها، متأسفانه قواعد مزبور در چنگال مشکلات تفسیری گرفتار می‌شوند. استانداردها و معیارهای تمایز و تشخیص اموال غیرنظامی از اهداف نظامی پیشتر به خوبی تشریح و روشن شده‌اند. تفاوت‌های مشابهی هنگامی که یک غیرنظامی مورد حمله قرار می‌گیرد، وجود دارد. پروتکل الحاقی اول در صورتی حمله به فرد غیر نظامی را مجاز دانسته است که آن فرد به صورت مستقیم در مخاصمات مشارکت کند. در عرصه عملیات‌های سایبری، موضوع غیرنظامیان از اهمیت ویژه‌ای برخوردار است. بعضی از کشورها ساختار و عملکرد جنگ‌های سایبری را خارج از قواعد و اصول حاکم بر حقوق مخاصمات مسلحانه دانسته‌اند، اعم از اینکه این کارکردها متضمن حمایت از دارایی یا هدایت عملیات‌ها باشد. علاوه بر این، حملات سایبری ممکن است بیشتر سازمان‌ها و ارگان‌های دولتی و وابسته به دولت را مورد توجه قرار بدهند تا نیروها و ادوات نظامی. از این رو، این حملات به عنوان

تالی منطقی بحث، مسئولیت دولت و سازمان‌های وابسته به آن را مطرح می‌کنند تا مسوولیت نظامیان و فرماندهان نظامی.

هنگامی که پیمانکاران غیرنظامی یا پرسنل غیرنظامی نقش حامی را در هدایت عملیات به عهده دارند و انجام چنین نقشی از سوی آنها ضروری باشد -برای نمونه، حمایت و صیانت از تجهیزات مربوط به حملات سایبری- آنها می‌توانند به صورت مستقیم مورد هدف قرار بگیرند. افزون بر این، چون آنها اهداف مشروع تلقی می‌شوند، بنابراین، هرگونه صدمه‌ای که به آنها وارد شود، به هنگام ارزیابی این که آیا حمله صورت گرفته متناسب بوده است یا خیر، محاسبه و مورد توجه قرار نخواهند گرفت. از سوی دیگر، با اعمال مضیق معیار مشارکت مستقیم در مخاصمات، این افراد از حمایت‌های لازم (به عنوان افراد غیرنظامی) بهره‌مند خواهند شد و در واقع، اعمال این استاندارد به صورت مضیق، منجر به صیانت و تضمین حمایت‌های موجود از آنها خواهد شد، حتی اگر این افراد دستگیر هم بشوند مستحق برخورداری از وضعیت اسیر جنگی خواهند بود و همانند اسرای جنگی با آنها رفتار خواهد شد زیرا به عنوان افرادی عمل کرده‌اند که نیروهای مسلح را در طول مخاصمه همراهی کرده‌اند.[۴۳]

افراد غیرنظامی اگر بنا به اراده و تصمیم شخصی خود و فارغ از جریان مخاصمه نیروهای مسلح در یک حمله سایبری مشارکت کنند، مشکل به مراتب پیچیده‌تر می‌شود. اگر حمله سایبری منجر به ورود خسارات و صدمات جانی و مالی گردد و یا تحقق چنین تبعاتی محتمل باشد، در نتیجه، مرتکبین آن رزمندگان غیرقانونی خواهند بود. در واقع، چنین وصفی (رزمنده غیرقانونی) اضافی خواهد بود چراکه افراد مزبور فارغ از رعایت معیار و ویژگی‌های یک رزمنده، به صورت مستقیم در مخاصمات شرکت کرده‌اند. افراد بالا به عنوان رزمندگان غیرقانونی می‌توانند به صورت مستقیم مورد حمله قرار بگیرند و ورود هرگونه صدمه یا خسارتی به آنان در محاسبات مربوط به رعایت اصل تناسب محلی از اعراب نداشته و به هنگام دستگیری نیز از وضعیت و مزایای اسرای جنگی متمتع نخواهند شد. بر عکس، اگر افراد غیرنظامی که در مخاصمه شرکت داشته و هدایت حملات سایبری را نیز که هنوز به سطح حمله مسلحانه نرسیده است، به عهده داشته‌اند، رزمندگان غیرقانونی تلقی نمی‌شوند زیرا اساساً هیچ‌گونه جرم جنگی مرتکب نشده‌اند و در نتیجه، وضعیت غیرنظامی بودن آنها و حمایت‌های موجود و پیش‌بینی شده برای آنان برقرار بوده و غیر قابل خدشه خواهد بود. با این حال، اگر

افراد یاد شده به نیروهای نظامی ملحق شده و این واحدها را همراهی کنند، در صورت دستگیری، به عنوان اسیر جنگی با آنها برخورد خواهد شد.[44] البته، تجهیزات و امکانات مورد استفاده برای انجام عملیات بایستی به صورت مشخص اهداف نظامی تلقی شوند که در نتیجه، می‌توانند مورد حمله قرار بگیرند. همان‌گونه که پیداست، استفاده از غیرنظامیان و بکارگیری آنها، اعم از اینکه به عنوان پیمانکاران یا مستخدمین دولتی باشند یا خیر، نوعی ملازمت و همراهی با خلاءها و خطرات قانونی تلقی می‌شود. پیداست که برای بکارگیری پرسنل نظامی جهت مدیریت و هدایت حملات سایبری باید یک رویکرد کاملاً محتاطانه اتخاذ شود.

۵. محدودیت‌های حاکم بر حمله به اهداف مشروع

مبانی اصلی مربوط به حمله به اهداف مشروع، بر اساس اصل تفکیک بنیاد نهاده شده است.[45] اصل یادشده، در واقع، تبلور توازن ایجاد شده توسط حقوق بشردوستانه میان دیدگاه حاکمیت‌محور کشورها در توسل به زور و منافع گسترده بشری برای حفاظت از جان و مال افرادی است که در مخاصمات شرکت ندارند و خواهان مصون ماندن از اثرات ناگوار مخاصمات هستند. تفکیک در اصل دارای دو بعد است: نخست، نسبت به سلاح‌ها قابل اعمال است –اصل مزبور استفاده از سلاح‌هایی را که قادر به تمایز میان رزمندگان و اهداف نظامی از یک سو و غیرنظامیان و اهداف غیرنظامی از سوی دیگر نیست– ممنوع می‌نماید و دوم، نسبت به تاکتیک‌های جنگی قابل اعمال است –اصل یاد شده در این حوزه مقرر می‌دارد که تمامی تلاش‌ها باید مبتنی بر این باشد که در هنگام کنترل و هدایت عملیات نظامی، میان دو دسته از افراد نظامی و غیرنظامی تمایز و تفکیک قائل شود.[46]

۵-۱. سلاح‌های غیرمتعارف

حملات سایبری توسط یک سیستم عامل کامپیوتری، یک کد کامپیوتری و ابزاری که به واسطه آن کد یاد شده منتقل می‌شود، صورت می‌گیرد. بدیهی است که خود کامپیوتر فی‌نفسه یک وسیله و ابزار غیرمتعارف تلقی نمی‌شود چراکه این وسیله می‌تواند یک کد خاص را به درستی برای کامپیوترها و سایر شبکه‌های مرتبط ارسال نماید. ارسال ایمیل نمونه بارز چنین انتقالی تلقی می‌شود. در مقابل، کد نوشته شده می‌تواند غیرمتعارف و نامناسب باشد. نمونه بارز و کلاسیک چنین موردی، ویروسی است که فارغ از هرگونه کنترل از سوی صادرکننده آن، از یک کامپیوتر به کامپیوتر دیگر رسوخ می‌کند. از آنجا که کد مزبور –حتی اگر ویروسی غیرقابل

کنترل باشد- می‌تواند اهداف نظامی خاصی را مورد هدف قرار بدهد. ویروس یاد شده به این علت که نمی‌تواند مستقیم باشد، غیرمتعارف تلقی نمی‌شود. با این توصیف، چنین کدی در صورتی که اثرات آن محدود نباشد، می‌تواند غیرمتعارف تلقی بشود. در بسیاری از موارد، هنگامی که یک کد ویروسی به یک شبکه یا یک کامپیوتر حمله می‌کند، حمله‌کننده هیچ راهی برای محدود ساختن تبعات ناشی از ارسال مجدد آن ندارد. همین حالت حتی در شبکه بسته برای ویروسی که می‌تواند از یک دیسکت وارد شبکه شود نیز صدق می‌کند. از این رو، یک کد آلوده و مخرب که به صورت غیر قابل کنترل در سراسر سیستم‌های غیرنظامی انتشار پیدا می‌کند، به عنوان یک سلاح غیرمتعارف ممنوع می‌باشد. باید یادآور شد که بند (۴) ماده ۵۱ پروتکل الحاقی اول ۱۹۷۷ از شیوه‌ها و ابزار مبارزه سخن رانده است. ابزار مخاصمه در نظریات تفسیری پروتکل الحاقی اول به عنوان «سلاح» تعریف و تفسیر شده است، در حالی که شیوه مخاصمه راهی است که از طریق آن سلاحی بکار گرفته می‌شود.[۴۷] مفهوم واضح و شفاف سلاح، چیزی است که می‌تواند برای حمله به طرف مقابل بکار گرفته شود. از تحلیل بالا در رابطه با اصطلاح حمله در حقوق بشردوستانه می‌توان این نتیجه منطقی را گرفت که کدهای کامپیوتری در صورتی که منجر به ورود صدمات و خسارات جانی و مالی گردند، بخشی از یک سیستم تسلیحاتی تلقی می‌شوند. در حال حاضر، اگر این نوع کدهای ویروسی بخشی از سیستم تسلیحاتی نباشند، نمی‌توانند ممنوع باشند چراکه در این صورت جزو سلاح‌های غیرمتعارف تلقی نمی‌شوند.

۲-۵. اصل تفکیک

بدون تردید، اصل تفکیک یکی از قواعد عرفی حقوق بشردوستانه بین‌المللی است که در ماده ۴۸ پروتکل الحاقی اول به صراحت مورد تأکید قرار گرفته است. چتر حمایتی اصل تفکیک در مواردی که به موجب آن حمله مستقیماً علیه افراد و اموال غیرنظامی اتفاق نمی‌افتد اما در خلال وقوع حمله احتمال قربانی شدن آنها وجود دارد، قابل اعمال است. ممنوعیت مشابهی نیز به همین ترتیب در چهارچوب حملات سایبری وجود دارد که در گزارش تالین نیز مورد تصریح قرار گرفته است.[۴۸] چنین حالتی شامل وضعیت‌هایی است که به موجب آن احتمال هدف قرار دادن یک هدف نظامی از طریق انجام حملات سایبری با دقت تمام وجود دارد، اما در عوض یک حمله گسترده با هدف تحت تأثیر قرار دادن سیستم‌های غیرنظامی صورت می‌گیرد. چنین حمله‌ای قابل مقایسه با حمله موشک‌های اسکات عراق به مراکز و سایت‌های

غیرنظامی عربستان و اسرائیل در طول جنگ خلیج در سال‌های ۹۱-۱۹۹۰ می‌باشد.[۴۹] موشک‌های نامبرده به طور ذاتی از نوع سلاح‌های غیرمتعارف تلقی نمی‌شوند ولی استفاده آنها علیه مراکز غیرنظامی نادرست و غیرمتعارف بوده است، حتی اگر قصد نیروهای عراقی حمله به اهداف نظامی مستقر در این مراکز بوده باشد. زیرا احتمال اصابت موشک‌ها به افراد و اموال تحت حمایت به مراتب بیشتر از اصابت به اهداف نظامی بوده است که چنین استفاده‌ای غیرقابل قبول است. امروزه، ارتباط میان سیستم‌های کامپیوتری امری بدیهی است، از این رو، حملات سایبری به آسانی می‌توانند در اشکال مشابه یاد شده رخ بدهند.

۳-۵. اصل تناسب

اصل تناسب ناظر بر وضعیت‌هایی است که به موجب آن ایراد صدمه به اشخاص و اموال تحت حمایت از عواقب محتمل و قابل پیش‌بینی حمله تلقی می‌شود، اما در واقع، ورود این صدمات هدف اصلی حمله نبوده است. اصل یاد شده بیشتر اوقات (گاهاً بدون هیچ‌گونه قصد قبلی ولی به دلیل سهل‌انگاری و عدم دقت کافی در هدف‌گیری) به دلایل ذیل نقض شده است: ۱. فقدان آگاهی و درک کافی از آنچه که مورد حمله و هدف قرار می‌گیرد؛ ۲. ناتوانی در برآورد و تخمین میزان زور بکار گرفته شده توسط تجهیزات نظامی علیه اهداف؛ ۳. ناتوانی و ضعف در تضمین هدف‌گیری دقیق و کامل.[۵۰] هر سه عنصر فوق می‌توانند در قالب حملات سایبری مبتلابه باشند و به این حوزه ورود پیدا کنند.

همانطور که پروتکل الحاقی اول مقرر داشته است، اگر حمله ناقض اصل تناسب باشد و انتظار برود که منجر به سلب حیات غیرنظامیان و آسیب به آنها و اموال آنان می‌شود، در نتیجه، چنین حمله‌ای نیز غیرمتعارف تلقی می‌شود چراکه فراتر از مزایای نظامی مقرر برای حمله بوده و موجب ورود رنج و آسیب اضافی و غیرضروری به غیرنظامیان و اموال آنها شده است.[۵۱] برای نمونه، زندگی مسافران غیرنظامی در برابر حمله سایبری به سیستم کنترل ترافیک هوایی یک هواپیمای نظامی چگونه مورد ارزیابی قرار می‌گیرد و چگونه می‌توان میان این دو مقصود متعارض تعادل و توازن ایجاد کرد؟ یا اینکه چگونه می‌توان میان رنج تحمیل شده به افراد در هنگام حمله سایبری به یک مرکز توزیع برق که هم به غیرنظامیان خدمت‌رسانی می‌کند و هم به نیروهای نظامی، توازن ایجاد کرد؟ تمام مثال‌های بالا حاکی از سخت و پیچیده بودن ارزیابی و سنجش مزایای نظامی حملات سایبری و در عین حال حفظ حقوق اساسی غیرنظامیان است که کماکان به عنوان چالشی فراروی اصل تناسب در حقوق بشردوستانه تلقی می‌شود و تلاقی

این دو وضعیت -مزیت نظامی و حقوق غیرنظامیان- بر پیچیدگی هرچه بیشتر موضوع افـزوده است.

از جمله پیچیدگی‌های دیگری که حاکم بر این قضایاست، موضوع تأثیرات زنجیره‌ای یـا ثانویه[۵۲] است؛ بدین معنی که این اثرات بلافاصله و مستقیماً پس از حمله صورت گرفته ظهـور پیدا نمی‌کنند ولی به هر تقدیر محصول و زاییده حمله انجام شده هستند. شـاهد مثـال در ایـن باره حمله به شبکه سراسری توزیع برق عراق در طول جنـگ خلـیج در سـال‌هـای ۹۱-۱۹۹۰ بود. اگرچه این حمله به صورت مؤثر فرماندهی و کنترل نیروهای عراقی را مختل و فلج نمود، ولی در عوض، باعث شد تا افراد غیرنظامی از دسترسی به نیروی برق به عنوان اثر اولیه حملـه محروم شوند و در نتیجه، قطع جریان برق بر فعالیت بیمارستان‌ها، سیستم‌هـای پاسـخ‌گـویی و خدمات ارتباطاتی و حتی مواصلاتی تأثیر منفی گذاشت (اثرات ثانویه). چنین حملاتی منجر به ایجاد اثرات ثانویه که همان تحمیل رنج اضافی بر جمعیت غیرنظامی بود، گردید. بدیهی اسـت که چنین اثراتی می‌توانـد از تبعـات یـک حملـه سـایبری نیـز باشـد و موجبـات رنـج و آزار غیرنظامیان را فراهم آورد. این واقعیت بر هیچ‌کس پوشیده نیسـت کـه اثـرات ثانویـه ناشـی از تحقق حملات سایبری به مراتب بیشتر از حملات کلاسیک و سنتی است و دلیل منطقی و فنی آن نیز به ارتباط ناگسستنی میان شبکه‌های کامپیوتری در فضای سایبر برمی‌گردد که عمـلاً و از نظر تکنیکی تفاوتی میان آنها (شبکه‌های با کاربرد نظامی و مدنی) وجـود نـدارد. شـاید بتـوان چنین وضعیتی را بسان مال مشاعی تصور کرد که افراز آن عملاً ناممکن می‌نمایـد. گسـتردگی اثرات ثانویه در حملات سایبری به دلیل ارتباط وسـیعی کـه در شـبکه و فضـای سـایبر میـان سیستم‌ها وجود دارد، بسیار گسترده‌تر و پیچیده‌تر از حالت سنتی و کلاسیک آن است. علیرغم مشکل بـودن تشـخیص نحـوه عملکـرد و مبـداء و منشـاء حمـلات سـایبری، بـه هـر تقـدیر برنامه‌ریزان و تصمیم‌گیران این عرصـه متعهـد هسـتند تـا تمـامی تـلاش خـود را در راسـتای جلوگیری از ورود خسـارات و صـدمات غیرضـروری و ثانویـه ناشـی از حمـلات بـه عمـل بیاورند.[۵۳]

۶. استاکس‌نت:[۵۴] چالش‌ها و راهکارهای حقوقی پیش‌رو

در این گفتار، تلاش بر آن است تا مواضع ایران و راه‌کارهای حقـوقی پـیش‌رو بـرای مقابلـه و احتمال بکارگیری آنها در عرضه مخاصمات سایبری مورد بررسی قرار بگیرد.

۱-۶. تلقی حقوقی از عملکرد استاکس‌نت: توسل به زور یا مداخله در امور داخلی؟

پرسشی که مطرح می‌شود اینست که آیا حمله استاکس‌نت نقض اصل ممنوعیت توسل به زور است یا اینکه مشمول وصف حمله مسلحانه نشده و تنها در قالب ممنوعیت مداخله در امور داخلی کشورها (بند ۷ ماده منشور ملل متحد) می‌گنجد؟ به نقل از نشریه ستاد مشترک ارتش امریکا، واقعه استاکس‌نت در حقیقت، یک حمله سایبری بود که تا بدین لحظه نیز وقوع آن به طور رسمی اعلام نشده است. این بدافزار که با نیت قبلی طراحی شد، هدفش تخریب فیزیکی تجهیزات دولتی بوده است. کرم رایانه‌ای استاکس‌نت که جمهوری اسلامی ایران را هدف گرفت، فقط یک تهدید سایبری نبود. به نظر می‌رسد، این حمله خارجی علاوه بر رایانه‌های ویژه، کنترل خودکار مثلاً نیروگاه‌های آبی و نیز شبکه‌های برق، به طور ویژه تأسیسات غنی‌سازی اورانیوم در نطنز را هدف گرفته بود. این نشریه، همچنین، با تأکید بر غیر قانونی بودن این حمله سایبری مقرر داشت که بیانیه رسمی کشور قربانی می‌توانست تأییدی بر وقوع این حمله سایبری باشد و اینکه به جامعه بین‌المللی اجازه دهد تا این مصداق عینی را به‌مثابه یک حمله سایبری بررسی کند. با وضعی که پیش آمد، این حادثه در زمره یکی دیگر از حوادث سایبری غیرمحرمانه قرار گرفت و بدین ترتیب، فرصت تعیین مرزهای قابل تشخیص برای رفتار غیرقانونی در فضای مجازی از دست رفت. جهت تشریح هر چه بهتر این مسأله و نیل به پاسخی درخور نیاز است تا توضیحاتی فنی–حقوقی در این باب داده شود.

ویروس استاکس‌نت در حقیقت برای ایجاد تغییر در سرعت گردش سانتریفیوژهای تأسیسات هسته‌ای نطنز طراحی شده بود، که در نتیجه چنین تغییری، سرعت گردش سانتریفیوژها به شدت افزایش و کاهش می‌یافت. لازم به ذکر است که ویروس استاکس‌نت به صورت مخفیانه فعالیت کرده و با ورود به شبکه اینگونه وانمود کرده بود که سانتریفیوژها به صورت طبیعی کار می‌کنند.[۵۵] در ۲۳ نوامبر ۲۰۱۰ آقای علی‌اکبر صالحی –رئیس وقت سازمان انرژی اتمی ایران– اعلام داشت که: «*ما ویروس را دقیقاً در نقطه‌ای که قصد نفوذ داشته با دقت و هوشیاری کامل شناسایی کردیم و از ورود هرگونه آسیبی به تأسیسات هسته‌ای خود جلوگیری نمودیم*».[۵۶] این اظهارات بدان معناست که ویروس یاد شده تأثیر چندانی بر پروسه غنی‌سازی اورانیوم در تأسیسات هسته‌ای نطنز نداشته است. البته، در نقطه مقابل اظهارات آقای صالحی، رئیس‌جمهور وقت ایران ورود خسارت و وجود مشکلات محدودی را در تأسیسات نطنز به واسطه نفوذ ویروس استاکس‌نت مورد تأیید قرار داده بودند[۵۷] البته، گزارش‌هایی نیز

وجود دارند که میزان آسیب‌های وارده توسط استاکس‌نت را فراتر از گزارش و ادعای مقامات رسمی ایران پیش‌بینی و تخمین زده‌اند. در این باره، مؤسسه مطالعات علوم و امنیت بین‌المللی اعلام داشته است که با افزایش و کاهش شدید سرعت چرخش سانتریفیوژها، ویروس استاکس‌نت توانسته است تأثیر مخربی بر سانتریفیوژهای پایگاه نظنز داشته باشد.[۵۸] مؤسسه مزبور مقرر می‌دارد که این لرزش‌های شدید برای ایجاد اختلال و حتی تخریب سانتریفیوژها کافی به نظر می‌رسد.

با این تفاسیر و پذیرش این موضوع که ممنوعیت مندرج در بند ۴ ماده ۲ منشور ملل متحد ممنوعیتی بر پایه نتیجه‌محور بودن حملات سایبری می‌باشد،[۵۹] مشخص کردن این که حمله صورت گرفته علیه تأسیسات اتمی ایران نوعی توسل به زور غیر قانونی است یا خیر، تا حد زیادی مشکل و پیچیده می‌باشد چراکه تأثیر واقعی ویروس استاکس‌نت هرگز به صورت عینی شناسایی نگردیده است. با این وجود، با استناد به اظهارات رییس جمهور ایران دال بر ایجاد مشکلاتی چند توسط ویروس یاد شده، می‌توان مدعی شد که استاکس‌نت مانع چرخش سانتریفیوژها در سرعت استاندارد و معمول خود شده و در نتیجه مانع غنی‌سازی اورانیوم شده است؛ از این رو، چون استاکس‌نت خسارات مالی به دنبال نداشته است، نمی‌توان گفت که ممنوعیت توسل به زور را نقض کرده است.[۶۰] اگر گزارش‌های مؤسسه مطالعات علوم و امنیت بین‌المللی درست باشند و استاکس‌نت موجب ورود خسارت و تخریب فیزیکی سانتریفیوژها در تأسیسات نطنز شده باشد، می‌توان گفت که شرط لازم برای تحقق ممنوعیت توسل به زور بر اساس موازین حقوق بین‌الملل حاصل شده است و حمله استاکس‌نت مصداق بارز ممنوعیت مندرج در منشور تلقی می‌شود. با این حال، حتی اگر در میان شک و تردید درست یا نادرست بودن این گزارش‌ها باقی بمانیم، این واقعیت را به هیچ‌وجه نمی‌توان انکار کرد که حمله یاد شده در هر صورت و در پایین‌ترین سطح خود از دیدگاه حقوق بین‌الملل نقض قاعده عرفی ممنوعیت مداخله در امور داخلی کشورها (بند ۷ ماده ۲ منشور ملل متحد) تلقی می‌شود. به هر حال، چه حمله استاکس‌نت را مصداق نقض قاعده ممنوعیت توسل به زور تلقی کنیم و یا نقض قاعده عرفی ممنوعیت مداخله در امور داخلی کشورها، ایران گزینه‌های حقوقی مختلفی را پیش‌رو دارد که می‌تواند برای دفاع از خود در برابر چنین حملاتی، در آینده به این تدابیر متوسل بشود که در مبحث آتی بدان پرداخته می‌شود.

۲-۶. اتخاذ سیاست‌ها و اقدامات ایجابی حقوقی توسط ایران

با رسوخ ویروس استاکس‌نت به سایت تأسیسات اتمی پایگاه بوشهر و ورود خساراتی چند، از عملکرد مخرب هر چه بیشتر این کرم خطرناک جلوگیری شد و نیروهای امنیت سایبری کشور توانستند با کنترل به موقع آن از ورود خسارات جبران‌ناپذیر و احتمالاً ایجاد انفجار جلوگیری کنند. در واقع، حمله استاکس‌نت زنگ خطری بود که مقامات ایران را بر آن داشت تا در این باره تدابیر لازم را اتخاذ و تا حد توان در جهت حفظ امنیت سایبری تأسیات زیربنایی کشور و به ویژه تأسیسات اتمی کشور برآیند. مهمترین اقدام در این باره راه‌اندازی ارتش سایبری ایران به فرماندهی سپاه پاسدران انقلاب اسلامی است که به صورت جدی در این رابطه ابراز موجودیت کرده و در تلاش برای دفع و کنترل حملات سایبری پیش‌رو است. آنچه که ارتش سایبری در تلاش برای تحقق آن است در واقع اقدامی ملی-امنیتی و فنی است که به فراخور نیازهای روز اجتناب‌ناپذیر است و سایر کشورها نیز چنین اقداماتی را به صورت کاملاً جدی در برنامه کاری خود قرار داده و از این راه سعی در مدیریت و کنترل چنین وقایعی در فضای سایبر را دارند. البته، بنا به استراتژی متفاوت کشورها، این اقدامات می‌توانند جنبه تهاجمی و یا تدافعی داشته باشند که در مواضع رسمی و اخیر بعضی از کشورها مورد اشاره قرار گرفته است. برای نمونه، ایالات متحده امریکا اعلام داشته است که در صورت وقوع حملات سایبری علیه این کشور، امریکا حق دفاع مشروع مندرج در ماده ۵۱ منشور ملل متحد را برای خود محفوظ دانسته و حتی مقرر داشته که در پاسخ به چنین حملاتی خود را محق به دادن انواع پاسخ‌های نظامی می‌داند.[۶۱]

مواضع سیاسی در این خصوص، قاعدتاً بر تدابیر و راهکارهای حقوقی نیز تأثیرگذار هستند. واکنش‌های مختلفی نسبت به حمله استاکس‌نت به پایگاه اتمی بوشهر نشان داده شد که همگی در راستای محکومیت آن و انجام اقدامات متقابل بوده است. واقعیت امر این است که اقدامات حقوقی ایران، به عنوان قربانی این نوع از حملات، می‌تواند صور مختلفی داشته باشد چراکه در صورت ورود خسارت جانی و مالی و در صورتی که مصدر و منشاء حمله انجام شده مشخص و معین باشد و به عبارتی بتوان آن را منتسب به کشور یا کشورهایی معین دانست، در این صورت، طبق قواعد حاکم بر دفاع مشروع مندرج ماده ۵۱ ایران نیز قادر به پاسخ‌گویی خواهد بود اما به هر تقدیر دادن چنین پاسخی مستلزم رعایت اصول حاکم بر مخاصمات مسلحانه بین‌المللی و به طور عام تعهد به رعایت قواعد حقوق بشردوستانه

بن‌المللی می‌باشد. اینکه پاسخ یاد شده بایستی حتماً از نوع سایبری بدوه یا نه منوط به سیاستگذاری رسمی و مواضع رسمی مقامات ایرانی است که ظاهراً در این حوزه (حملات سایبری) جنبه تدافعی دارد. نکته مهم و البته بسیار پیچیده در بحث مخاصمات سایبری که اتخاذ اقدامات حقوقی را نیز به شدت تحت تأثیر قرار می‌دهد همانا اثبات معیار انتساب حملات است که بحثی کاملاً فنی بوده و مستلزم همکاری و اظهارنظرهای کارشناسانه دانشمندان عرصه فناوری اطلاعات و دنیای مجازی می‌باشد.

آنچه در حال حاضر واضح و مبرهن است این واقعیت است که دنیای امروز جنگ در فضای مجازی و سایبری را واقعیتی انکارناپذیر تلقی کرده است و در حقیقت، به وقوع پیوستن آن را در دنیای واقع بسان جنگ‌های سنتی و کلاسیک تا حدی تجربه کرده است که تجربه جنگ روسیه-گرجستان نمونه بارز آن می‌باشد. واقعیت موجود به حدی فراگیر شده است که حتی مقامات نظامی کشور ایران نیز آن را تهدیدی جدی قلمداد کرده‌اند به طوری که رئیس سازمان بسیج مستعفین فضای مجازی را صحنه جنگ واقعی تلقی کرده است.[۶۲] اهمیت واقعی بودن تهدیدات یاد شده تا بدان حد بوده است که منجر به صدور فتوای کمیته فتوا در دانشگاه الأزهر شده است. کمیته مزبور طی فتوای صادره اعلام کرده است که هک‌کردن سایت‌های اسرائیلی و امریکایی حلال است و جهاد به شمار می‌رود.[۶۳]

فرجام

روی‌هم‌رفته باید اذعان داشت که قواعد فعلی حقوق بشردوستانه بین‌المللی برای حمایت از افراد و اموال غیرنظامی و سایر اشیاء تحت حمایت تا حد زیادی کافی و وافی به نظر می‌رسد. با این وجود، جنبه‌های بدیع و نوینی نظیر حملات مبتنی بر شبکه کامپیوتری یا به عبارت مرسوم‌تر، حملات سایبری پیچیدگی‌ها و معماهای جدید و به نسبت بغرنجی را مطرح کرده‌اند که برای نمونه توسل ناتو به حملات سایبری علیه یوگسلاوی سابق در سال ۱۹۹۹ نمونه عملی و بارز چنین پدیده‌ای است که مواجهه حقوق بشردوستانه با این پدیده را وارد ادبیات حقوق بین‌الملل به طور عام و حقوق بشردوستانه بین‌المللی به طور خاص نموده است و واقعیت امر اینست که حقوق بشردوستانه تاکنون نتوانسته است تمامی ابعاد و جوانب پیچیده این پدیده را حل و فصل کند.[۶۴]

برای اعمال قواعد موجود حقوق بشردوستانه بر حملات سایبری لازم است که یک سری

مقدمات و مفروضات اولیه را مورد پذیرش قرار بدهیم که مهمترین آن پذیرش تفسیر نتیجه‌محور بودن مخاصمات و حملات مسلحانه است. در صورت عدم پذیرش چنین دیدگاهی، قابلیت اعمال قواعد حقوق بشردوستانه بر حملات سایبری بدون تردید مشکل و غیرممکن خواهد بود.

نکته جالب توجهی که باید یادآور شد این است که ارزیابی حملات سایبری در حوزه حقوق توسل به زور[۶۵] نیز در نهایت، منجر به اتخاذ رویکرد نتیجه‌محوری خواهد شد.[۶۶] دوم اینکه، حتی اگر معیارهای ملهم از تفاسیر بالا را مورد پذیرش قرار دهیم، یک خلاء هنجاری کماکان باقی می‌ماند که با قواعد فعلی حقوق بشردوستانه قابل پر کردن نیست. نمونه بارز این خلاء در جایی است که حمله سایبری صورت گرفته علیه غیرنظامیان و اموال آنها که الزاماً منجر به ورود خسارت، صدمه، مرگ و یا تخریب نشده است، می‌تواند مجاز باشد چراکه شرط ورود خسارت را احراز نکرده است.

در پایان، باید گفت که قواعد حقوق بشردوستانه به طور عمومی برای حمایت از افراد و اموالی که درصدد جلب حمایت‌های حقوقی ناشی از اثرات و تبعات حملات سایبری هستند کافی به نظر می‌رسد، ولی کماکان خلاءهای هنجاری مهمی وجود دارند که قواعد حاضر قادر به پر کردن این خلاءها نیستند که نمونه بارز و بسیار مهم و جدی آن در بحث قابلیت اعمال اصل تفکیک و تناسب در مخاصمات سایبری است چراکه جنس و ماهیت این نوع از حملات کاملاً متفاوت از نوع سنتی و کلاسیک آن در دنیای واقعی است. البته اشاره به مساله انتساب در حملات سایبری کماکان بسان کلاف سردرگمی است که به عنوان پاشنه آشیل این پدیده تلقی می‌گردد که امری فنی و در عین حال بسیار پیچیده و دارای تبعات حقوقی متعدد است. افزون بر این، با عنایت به ظرفیت‌هایی که در کنترل حملات سایبری از نظر فنی وجود دارد، وضع و تدوین هنجارهای لازم برای قاعده‌مند کردن این ظرفیت‌ها لازم و ضروری به نظر می‌رسد که باید به صورت جدی مورد توجه قرار بگیرند چراکه آینده مخاصمات مسلحانه را حملات سایبری و عملیات‌های سایبری تشکیل خواهند داد و این مسأله واقعیتی اجتناب‌ناپذیر است که جامعه بین‌المللی با آن مواجه بوده و ناگزیر باید پذیرا و البته حلال اثرات و تبعات آن از هر نظر به ویژه از منظر حقوقی باشد که ایران نیز بدون تردید بخشی از جامعه بین‌المللی محسوب شده و با تهدیداتی که اخیراً با آنها مواجه شده است تافته‌ای جدا بافته نخواهد بود و باید در این باره علاوه بر ارتقای توانمندی‌های سایبری خود از نظر حقوقی نیز به صورت جدی به این قضیه رویکردی کاملاً فعال و ایجابی داشته باشد تا بتواند بر تهدیدات موجود و احتمالی آتی غلبه نماید.❖

یادداشت‌ها:

۱. از جمله این موارد می‌توان به عملیات ناتو در کوزوو، واقعه استونی، حمله سایبری به وزارت دفاع امریکا، حملات نظامی اسراییل به نوار غزه، حملات سایبری به امارات متحده عربی، حملات سایبری به پنتاگون و مخاصمات سایبری در ایران اشاره کرد.

2. Cyber Warfare.

3. Cyber Operations

4. Joint Chiefs of Staff (2001) Joint publication 1-02, DEPT OF DHF, *Dictionary of Military and Associated terms*, (12 April 2001) , http://www.dtic.mil/dictrine/new_pubs/jp1_02.pdf

5. Computer Network Attack

6. Joint Chiefs of Staff (2001) Joint publication 1-02, DEPT OF DHF, *Ibid.*

7. Hildreth, S.A. (2001) , *Cyberwarfare, Congressional Research Service Report for Congress on Cyberwarfare,* No. RL30735, http://wwwfas.org/irp/crs/RL30735.pdf

8. Wilson, C. W. (2006) , *Information Operations, Electronic Warfare and Cyberwar: Cababilities and Related Policy Issues*, Congressional Research Service Report for Congress. No. RL31787, http://www.fas.org/irp/crs/RL31787.pdf

9. Kevin Coleman

10. Technolytics Institute

11. Coleman, K. (2008) , *Russia's Cyber Forces, Defense Tech*, http://www.defensetech.org/archives/cat_cyberwarfare.html

12. IP Spoofing

13. *Tallin Manual on the International Law Applicable to Cyber Warfare*, prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence, Cambridge University Press, p. 68 , 2013.

14. *Ibid*, Rule 30, Definition of Cyber Attack.

15. Computer Network Attack

16. On this Point See: Emily Haslam, *"Information Warfare: Technological Changes and International Law*", Journal of Conflict and Security Law, Vol. 5, 2000, p.157; see also: Aldrich, Richard, "*The International Legal Implications of Information Warfare*", Airpower Journal, Fall 1996, p.99; and also: Mark, Schulman, "*Discrimination in the Laws of Information Warfare*", Columbia Journal of Transnational Law, Vol.37, 1999, p.939.

۱۷. بند (۲) ماده ۱ پروتکل الحاقی اول ۱۹۷۷ به کنوانسیون‌های چهارگانه ژنو ۱۹۴۹. شرط مارتنس در حقیقت، ریشه معاهداتی داشته به طوری که در مقدمه کنوانسیون پنجم لاهه در رابطه با حقوق و عرف‌های جنگ‌های زمینی مورخ ۱۸ اکتبر ۱۹۰۷ آمده است.

18. North Sea Continental Shelf Cases, 3 ICJ Reports, 1969, p.44.

19. S.S. Lotus (France v. Turkey) , PCIJ (ser. A) , No. 10, 1927.

20. Asylum Case (Columbia v. Peru) , 5 ICJ Reports, 1950, p.266.

21. Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) , 1996, p. 226.

۲۲. ر.ک.: ماده ۳۶ پروتکل الحاقی اول ۱۹۷۷.

23. *op.cit*.., For a State's position on this issue , See: U.S. Department of Defense, *Cyberspace Policy Report*, a report to congress pursuant to the national defense authorization act for fiscal year 2011, section 934, at 7,9 (Nov. 2011).

24. ICRC, *Commentary on the Geneva Conventions for the Amelioration of the condition of the Wounded and Sick in Armed Forces in the Field*,-Geneva, 1952, p. 32-33.

25. Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds*) , Commentary on the additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC, Geneva, 1987, para. 62.

26. For Instance see: Detter De Lupis, "*The Law of War*", 2nd ed., Cambridge University press, Cambridge, 2000, pp. 20-21. Also see: Christopher Greenwood, "*Historical Development and Legal Basis*", in: Dieter Fleck (ed) , *The Handbook of humanitarian Law in Armed Conflict*, Oxford University Press, Oxford, 1995, p.42.

27. This possibility was described in: *president's commission on critical Infrastructure protection, Critical Foundations: Protecting America's Infrastructure*, October 1997, at 1-46.

28. *Tallin Manual*, Rule 20 (3).

29. *Ibid*, Rule 30 & 32, pp. 92-98.

۳۰. ر.ک.: بندهای (۱)، (۲) و (۳) ماده ۵۲ پروتکل الحاقی اول ۱۹۷۷.

31. Dual-Based Objects

۳۲. ر.ک.: شق (۱) قسمت (a) بند (۲) ماده ۵۷ پروتکل الحاقی اول ۱۹۷۷.

۳۳. ر.ک.: بند (۱) ماده ۴۳ پروتکل الحاقی اول ۱۹۷۷.

34. Yves Sandoz, Christophe Swinarski and Bruno Zimmerman*, op.cit.*

35. *Ibid*, Paras, 2020-23.

36. *Ibid*, para. 2024.

37. Us Navy/marine/Coastal Guard, *The Commander's Handbook on the Law of Naval Operations*, para.8.1.1 (1995) , reprinted in US Naval War College's International Law Studies Series, Vol. 73.

38. Bankovic and Others v. Belgium, the Czech Republic, Denmark, France, Germany, Greece, Hungary, Iceland, Italy, Luxemburg, the Netherlands, Norway, Poland, Portugal, Spain, Turkey and UK, ECHR, App. No.52207/99 (2001).

۳۹. ر.ک.: بند (۱) ماده ۵۰ پروتکل الحاقی اول ۱۹۷۷.

٤٠. *همان*، بند (۱) ماده ۵۲.

41. See: M. Cherif, Bassiouni, "*The Statute of the International Criminal Court: a Documentary History*", Transnational Publishers, New York, 1999, p. 39.

٤٢. ر.ک.: بند (۱) ماده ۵۰ پروتکل الحاقی اول برای افراد غیرنظامی و بند (۳) ماده ۵۲ همان پروتکل برای اموال غیرنظامی.

٤٣. ر.ک.: بند (۴) ماده ۴ کنوانسیون سوم ژنو ۱۹۴۹ در خصوص اسیران جنگی.

٤٤. *همان*.

45. For more information in this regard see: Esbjorn Rosenblad, *International Humanitarian Law on Armed Conflict: Some Aspects of the Principle of Distinction and Related Problems*, Henry Dunant Institute, Geneva, 1979.

٤٦. پروتکل الحاقی اول در بند (۴) ماده ۵۱ خود این تفاوت را مورد توجه قرار داده است.

47. Additional Protocols: A Commentary, *op.cit.*

48. *Tallin Manual*, Rule 30, pp.95-97.

49. See: US Department of Defense, "*Conflict of the Persian Gulf War*", Title v Report to congress, 1992, p. 63, reprinted in 31 International Legal Matyerials, 1992, p. 612.

50. Michael Schmitt, *"Bellum Americanum: The US View of 21th Century War and its possible Implications for the Law of Armed Conflict*", Michigan Journal of International Law, Vol. 19, 1998, p.1051, pp.1080-81.

۵۱. ر.ک.: قسمت (a) از بند (۵) ماده ۵۱ پروتکل الحاقی اول و (iii) (a) بند (۲) ماده ۵۷ همان پروتکل.

52. Knock-on Effects

۵۳. ر.ک.: ماده ۵۷ پروتکل الحاقی اول ۱۹۷۷.

٥٤. استاکس‌نت نوعی کرم ویندوز است که توسط USB پخش می‌شود. این کرم می‌تواند در داخل یک سازمان خودش را در منابع به اشتراک گذاشته شده شبکه (در صورت انتخاب کلمات عبور ضعیف) پخش کند. کرم مزبور می‌تواند موتورها، حمل‌کننده‌های تسمه‌ای و پمپ‌ها را تعدیل کند. استاکس‌نت می‌تواند یک کارخانه را از کار بیاندازد. با یک تغییرات اساسی، حتی قدرت انفجار اجزاء را نیز دارد. استاکس‌نت، نخستین کرم صنعتی جهان است که با هدف حمله سایبری به زیرساخت‌های حیاتی صنعت ایران، آسیب به تأسیسات هسته‌ای نطنز و در نهایت، تأخیر در راه‌اندازی نیروگاه اتمی بوشهر طراحی و منتشر شده است. این کرم قادر به ایجاد اخلال در تجهیزات حساس مانند تخریب سرعت چرخش روند بالا از آرایه‌های سانتریفیوژ و کاهش تعداد سانتریفیوژهای غنی عملیاتی، کنترل فعالیت‌های صنعتی محدودیت دور توربین، روغن‌کاری و یا بستن سیستم‌های خنک کننده، تخریب لوله‌های گاز و حتی انفجار دیگ‌های بخار کارخانجات مختلف است. سیستم‌های آسیب‌پذیر در برابر این کرم عبارتند از:

Microsoft Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows Vista, Windows XP on 32-bit Platforms.

55. For a discussion of the Stuxnet virus, see: P. Shakarian, "*Stuxnet: Cyber war Revolution in Military Affairs*" (2011) 7 Small Wars J 1.

56. Quoted in: '*Iran 'Briefly Halted Enrichment*'' Aljazeera (23 November 2010).

57. Quoted in: '*Iran says Cyber Foes Caused Centrifuge Problems*' Reuters (29 November 2010).

58. The Institute produced its Preliminary Report on 22 December 2010: D. Albright, P. Brannan and C. Walrond, "*Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?"* Institute for Science and International Security, 22 December 2010. This report was updated on 15 February 2011: D. Albright, P. Brannan and C. Walrond, "*Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*", Institute for Science and International Security, 15 February 2011.

۵۹. تفسیر غالب حقوق‌دانان بین‌المللی از ممنوعیت مندرج در بند ۴ ماده ۲ منشور ملل متحد این است که این ممنوعیت صرفاً دربرگیرنده حملات مسلحانه می‌شود و سایر مصادیق نظیر مداخلات و فشارهای سیاسی و اقتصادی را شامل نمی‌شود. برای اطلاعات بیشتر در این باره ر.ک.:

Committee on Offensive Information Warfare and others, *Technology, Policy Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities Report,* (National Research Council 2009) 253; Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2 (4) of the United Nations Charter*, *in: COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW*, 73, 80–82 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002).

60. J.C. Woltag, "*Computer Network Operations below the Level of Armed Force*" (European Society of International Law Conference Paper Series 1, Tartu, Estonia, 26 May 2011).

61. USCYBERCOM, Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012.

٦٢. رئیس سازمان بسیج مستضعفین فضای مجازی را صحنه واقعی یک میدان جنگ دانست و گفت: این روزها باید بیشتر از هر زمان دیگری در این فضا هوشیار بود و ابتکار عمل را داشت. سردار "محمد رضا نقدی" در مراسم آغاز دوره آموزش تکمیلی فضای مجازی که در دانشگاه علوم حدیث آغاز شده بود، گفت: «این روزها اقتضای زمان و مکان برای جنگ با دشمنان اسلام تغییر کرده و فضای مجازی در حقیقت صحنه یک جنگ و رویارویی واقعی است». http://cir.ir/news/46018

٦٣. در ادامه فتوای الأزهر چنین آمده: این نوع جهاد هیچ تفاوتی با جهاد مسلحانه ندارد

بلکه حتی از آن نیز اهمیت بیشتری دارد زیرا امروز جهان به شـبکه مخـابراتی وسـیعی تبـدیل شده است و هرکس قدرتمندتر باشد در آن پیروز خواهد شد. *همان*، به تاریخ: ۱۳۹۱/۰۵/۲۳.

64. Michael N. Scmitt, "*Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*", Colombia Journal of Transnational Law, Vol. 37, 1999.

65. Jus ad Bellum

66. Bradley Graham, "*Military Grappling with Rules for Cyber Warfare: Questions prevented Use on Yugoslavia*", Washington Post, 8 Nov. 1999, p. A. 1.