Original Article

Study of Strategies to Limit of Cybercrime Attacks from the Perspective of International Humanitarian Law

Afshin Jafari[1*], Mehri Toutounchian[2]

1. Assistant of Professor, Payame-Noor University, P.O.BOX: 19395-3697, Tehran, Iran. (Corresponding Author) Email: jafariafshin@yahoo.com

2. Ph.D. in Department of Jurisprudence and Principles of Islamic Law, Central Tehran Branch, Islamic Azad University, Tehran, Iran.

Received: 20 Feb 2019 Accepted: 25 Jul 2019

Abstract

Human progress in various political and social arenas creates new opportunities and challenges. This subject has led that international laws, including international humanitarian law, to seek for create appropriate laws for new developments. One of these new challenges is Cybercrime attacks, which is due to the increasing spread of technology and the development of cybercaps in various parts of the world, this Attacks are considered as a threat to human life. The main question of the current research is that what are the most important strategies for reducing cyberattacks from the perspective of international humanitarian law? The findings of this study are that Cybercrime attacks, Because of hurting to civilians, are considerable for international humanitarian law. In addition, Due to the increasing number of cybercrime attacks, need to apply the principles of international humanitarian law or to formulate new rules in the face of these attacks, is essential. Meanwhile, In the area of confronting with the effects and consequences of Anti-human rights Cybercrime attacks, Unilateral decisions are not very effective and in this regard, one of the main weaknesses have been the lack of collective agreement on how to manage cyber space. The present research approach is a descriptive-analytical approach which has taken a library Method to collecting information.

Keywords: Cybercrime Attacks; International Humanitarian Law; Human Rights; Cyberspace

Please cite this article as: Jafari A, Toutounchian M. Study of Strategies to Limit of Cybercrime Attacks from the Perspective of International Humanitarian Law. *Bioethics Journal*, Special Issue on Human Rights and Citizenship Rights 2019; 331-342.

مقاله پژوهشی

بررسی راه‌کارهای تحدید حملات سایبری از منظر حقوق بین‌الملل بشردوستانه

افشین جعفری[1*]، مهری توتونچیان[2]

۱. استادیار دانشگاه پیام نور، صندوق پستی: ۳۶۹۷-۱۹۳۹۵، تهران، ایران. (نویسنده مسؤول) Email: jafariafshin@yahoo.com

۲. دکتری فقه و مبانی حقوق اسلامی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران.

دریافت: ۱۳۹۷/۱۲/۱ پذیرش: ۱۳۹۸/۵/۳

چکیده

پیشرفت‌های بشری در عرصه‌های مختلف سیاسی و اجتماعی باعث ایجاد فرصت‌ها و چالش‌های جدیدی می‌شود. همین موضوع باعث شده تا قوانین بین‌المللی از جمله حقوق بین‌الملل بشردوستانه به دنبال ایجاد قوانینی متناسب برای تحولات جدید باشند. یکی از این چالش‌های جدید، حملات سایبری است که به دلیل گسترش فزاینده فناوری و توسعه فضای مجازی در نقاط مختلف جهان تهدیدی برای حیات بشری قلمداد می‌شوند. سؤال اصلی پژوهش حاضر این است که مهم‌ترین راه‌کارهای تقلیل و تحدید حملات سایبری از منظر حقوق بین‌الملل بشردوستانه کدام هستند؟ از یافته‌های پژوهش حاضر این است که حملات سایبری به دلیل صدمه‌زدن به غیر نظامیان مورد توجه حقوق بین‌الملل بشردوستانه است. به علاوه با توجه به افزایش روزافزون حملات سایبری، ضرورت اعمال اصول و قواعد حقوق بین‌الملل بشردوستانه و یا تدوین قواعد جدید در مواجهه با این حملات امری ضروری است، ضمن این‌که در زمینه مقابله با آثار و پیامدهای ضد حقوق بشری حملات سایبری، تصمیم‌گیری‌های یک‌جانبه کارآیی زیادی ندارد و یکی از نقاط ضعف اساسی در این زمینه نبود توافق جمعی بر نحوه مدیریت فضای سایبر بوده است. رویکرد پژوهش حاضر، توصیفی ـ تحلیلی است که با روش کتابخانه‌ای نسبت به جمع‌آوری اطلاعات اقدام کرده است.

واژگان کلیدی: حملات سایبری؛ حقوق بین‌الملل بشردوستانه؛ حقوق بشر؛ فضای مجازی

مقدمه

امروزه همگام با تحول در ارتباطات و تعاملات بشری، جنگ‌ها و تهدیدات نیز دچار تغییر شده‌اند. بدین معنا که تکیه بر روش‌های سنتی به تنهایی نمی‌تواند باعث قدرتمندشدن یک کشور تلقی شود. از طرفی دیگر، انقلاب اطلاعات باعث حساسیت نظام‌های سیاسی و اجتماعی در مقابل آسیب پذیری‌های متعدد شده است. بنابراین در تحولات جدید ارتباطی و اطلاعاتی، نظام‌های سیاسی ضعیف و قوی در معرض آسیب‌پذیری قرار دارند. در تهدیدات و جنگ‌های جدید دیگر نیازی به ارتش قوی و نیروی نظامی گسترده نیست، بلکه ممکن است فردی با مهارت‌های بالا بتواند امنیت یک جامعه را در معرض خطر قرار دهد. به علاوه، خسارت‌های ناشی از تحولات جدید می‌تواند ابعاد سیاسی، اجتماعی، فرهنگی، اقتصادی و دفاعی یک کشور را در معرض خطر قرار دهد. این رویکرد امروزه در قالب تهدیدات و حملات سایبری دنبال می‌شود. تهدیدات و حملات سایبری امروزه این امکان را فراهم آورده است تا علاوه بر دولت‌ها به عنوان بازیگران اصلی صحنه نظام بین‌الملل، بازیگران غیر دولتی نیز به تجهیز و افزایش توانایی‌های خود بیندیشند و باعث ایجاد ترس و تهدید در طرف مقابل خود شوند.

در شیوه جدید تهدیدات، حمله به نقاط ضعف دشمن و در عین حال پرهیز از رویارویی با توانمندی‌های دشمن مورد توجه است، حتی در مخاصمات و درگیری‌های چند سال اخیر استفاده از این فناوری‌ها باعث تضعیف اراده برخی کشورها در رویارویی با کشورهای با فناوری بالا شده است، هرچند که در مواردی اندک، این رویکرد نتیجه عکس داشته است. به این نوع رویارویی، جنگ ناهمگون یا نامتقارن می‌گویند که با توسعه فناوری اطلاعات و حملات سایبری جنگ‌های نامتقارن در حملات سایبری نیاز به بازتعریف مجدد و بررسی مفاهیم و ویژگی‌های آن دارد. با توجه به این‌که اطلاعات نقش اول را در هر نوع جنگی بازی می‌کند، لذا فضای سایبر یکی از مساعدترین مکان‌ها برای دسترسی به اطلاعات طرف مقابل می‌باشد. بنابراین کشورها با استفاده از نوعی از حملات سایبری همچون بهره‌برداری سایبری (Cyber Exploitation) می‌توانند به اطلاعات مهم و حیاتی کشور هدف دست یابند و از طرفی دیگر با اطلاعات به دست‌آمده می‌توانند به زیرساخت‌های حیاتی کشور مقابل حمله نمایند که این نوع حمله می‌تواند مصداقی از جنگ نامتقارن باشد، البته اگر به آستانه موردنظر در تعریف حملات سایبری رسیده باشد.

بنابراین در جنگ‌های نامتقارن، اطلاعات دو کارکرد دارد. یکی این‌که بتوان با کمک آن، اهداف و برنامه‌های طرف مقابل را کشف و در مقابل آن‌ها پدافند کرد یا اهدافی که قرار است مورد حمله قرار بگیرد، شناسایی شده و در زمان معینی به آن‌ها حمله کرد؛ کارکرد دوم، ارائه اطلاعات غلط به طرف مقابل است. اطلاعات همواره در جنگ‌های کلاسیک و نامتقارن نقش بسیار بالایی دارد، ولیکن در جنگ‌های نامتقارن اطلاعات به موقع و دقیق اهمیت بالاتری نسبت به جنگ‌های دیگر دارد، چراکه در جنگ نامتقارن فرض بر این است که می‌توان با قدرت سلاح و آتش کم‌تر، تخریب بیشتری انجام داد (۱).

با توجه به ویژگی‌های حملات سایبری، در صورتی که حملات سایبری در آستانه یک حمله مسلحانه قرار گیرد، می‌توان این حمله را نوعی از جنگ نامتقارن دانست که در این صورت، حقوق بین‌الملل بشردوستانه قابلیت اعمال پیدا می‌کند. حقوق بین‌الملل بشردوستانه که با تکیه بر مجموعه قواعد و قوانینی درصدد حمایت از آسیب‌دیدگان و مجروحان جنگی است، قواعد جنگ‌ها و آثار و خسارت‌های آنان را مورد بررسی قرار می‌دهد. با توجه به این‌که ممکن است حملات سایبری در پاره‌ای از مواقع به مثابه یک سلاح جنگی عمل کنند و به تبع آن خسارت‌ها و آسیب‌های جانی و مالی فراوانی به بار آورند، در این صورت حقوق بین‌الملل بشردوستانه می‌تواند با بررسی نقض اصل عدم توسل به زور توسط حمله کنندگان سایبری، اصول و قواعد خود را به کار گیرد. در همین راستا پژوهش حاضر درصدد بررسی این موضوع است که آیا حملات سایبری ناقض اصل عدم توسل به زور است؟ و در صورتی که چنین موضوعی رخ دهد، راه‌کارهایی رسیدگی و برطرف‌کردن آن کدام هستند؟ به نظر می‌رسد توسل به آموزه‌ها و قواعد حقوق بین‌الملل بشردوستانه تا حدود زیادی

می‌تواند آسیب‌ها و تهدیدات ناشی از حملات سایبری را به حداقل برساند و برای جنگ‌ها و حملات جدید، قواعدی را معین کند.

مفاهیم و گزاره‌ها

۱ـ سایبر و حملات سایبری

۱-۱- سایبر در لغت: واژه سایبر از ریشه یونانی لغت «Kybeenetes» به معنی سکاندار یا راهنما مشتق شده (۲) و به طور ترکیبی در واژه سایبرنتیک به کار رفته است (۳). با این حال حملات سایبر ترکیبی از دو مفهوم مجزا است که در کنار هم مفهوم واحدی را خلق کرده‌اند. حملات، اشاره به رویکرد تهاجمی در مبارزات دارد که می‌تواند طیفی از حملات آشکار و نامحسوس را دربر گیرد. مفهوم سایبرنتیک دلالت بر سیستم‌های کنترلی ابرتکنولوژی‌های رایانه‌های به هم پیوسته، تکنولوژی جدید و واقعیات مصنوعی با راهبردهای دستیابی و کنترل سیستمی دارد. مفهوم دوم به کاررفته در واژه فضای سایبر که این مفهوم مورد نظر ما می‌باشد، مفهوم «فضا» است. وجود کلمه فضا در این واژه حاکی از آن است که «فضای سایبر» باید بُعد داشته باشد (۴). مکان دارای محتوا است، ولی فضا نوعی خلأ است، مکان دارای دو بعد است، در حالی که فضا مفهومی سه بعدی است. مکان مفهومی مرزپذیر و قابل محدود شدن، اما فضا مفهومی مرکز و تا حدودی نامتناهی است.

۱-۲- حملات سایبری در اصطلاح: واژه سایبر هنگامی که در عمل با اصطلاحات دیگری نظیر جنگ سایبری و حملات سایبری گره می‌خورد، حالتی عملیاتی به خود می‌گیرد. بنابراین چالش اولیه در ارزیابی و تعریف حملات سایبری، ماهیت و قلمروی این‌گونه عملیات می‌باشد. به عنوان مثال، شورای پژوهش ملی ایالات متحده آمریکا، حمله سایبری را به مثابه اقدامی آگاهانه برای جایگزینی، اختلال، فریب، تغییر یا تخریب سیستم‌های رایانه‌ای و اطلاعات آن‌ها تعریف کرده است. از سوی دیگر سازمان همکاری‌های شانگهای از زاویه‌ای دیگر حمله سایبری را به مثابه «شستشوی مغزی گسترده جهت ناامن و بی‌ثبات‌کردن جامعه داخلی و وادارکردن دولت به اتخاذ تصمیم به نفع طرف مخالف» تعریف کرده است (۵).

برخی نیز حملات سایبری را این‌گونه تعریف کرده‌اند: «هر اقدامی که به منظور تضعیف کارکرد شبکه‌های رایانه‌ای یک کشور با هدفی سیاسی و یا بر ضد امنیت ملی کشور مورد هدف واقع شود، یک حمله سایبری است» (۵). لازم به ذکر است به دلیل عدم اجماع جهانی در خصوص مفهوم حمله سایبری، برخی از دولت‌ها از این خلأ استفاده کرده و هرگونه تعریفی که به صلاح نظام امنیتی خودشان باشد را مبنای تصمیم‌گیری قرار می‌دهند.

ضمن این‌که تداخل و تلاقی حملات سایبری با جنگ سایبری مشکلاتی را پدید آورده است، به طوری که در زمینه تعریف حمله سایبری، به اشتباه، این‌گونه حملات را همان جنگ سایبری یا مخاصمه مسلحانه می‌دانند که در بیشتر موارد این‌گونه برداشت اشتباه بوده است، چنانچه جنگ سایبری، با هدف ازهم‌گسیختن سیستم‌های اطلاعاتی و مخابراتی، سیستم‌های کنترل و فرماندهی، ارتباطات و جاسوسی نیروی نظامی دشمن در هنگام یک مخاصمه مسلحانه و در فضای سایبر صورت می‌گیرد. در واقع جنگ سایبری اشاره به علمیات نظامی براساس اصول اطلاعاتی و شبکه‌های الکترونیکی دارد (۴)، ضمن این‌که جنگ سایبری می‌تواند دربردارنده حمله سایبری باشد، اما حمله سایبری اختلال در صحت یا درستی داده‌ها است که معمولاً از طریق کدهای مخرب، تغییر در برنامه‌های رایانه‌ای و کنترل داده‌ها که منجر به خروجی اشتباه می‌شود، صورت می‌گیرد (۴). با این حال، حملات سایبری بر حسب این‌که تا چه اندازه توانایی تخریب و آسیب‌رسانی دارند، می‌توانند به مثابه یک حمله مسلحانه تلقی شوند و یا این‌که در زمره تهدیدات سایبری جای بگیرند.

۲ـ حقوق بین‌الملل بشردوستانه

حقوق بین‌الملل بشردوستانه (IHL: International Humanitarian Law) به عنوان شاخه‌ای از حقوق بین‌الملل، شامل مجموعه قوانینی در حمایت از قربانیان در موقع جنگ و همچنین مقرراتی برای انواع جنگ و تلفات ناشی از آن است.

نقض قواعد این شاخه از حقوق، هم باعث ایجاد مسؤولیت کیفری و هم مسؤولیت غیر کیفری می‌شود. مسؤولیت کیفری برای افرادی که قواعد مربوط به این شاخه از حقوق را نقض می‌کنند و مسؤولیت غیر کیفری برای دولتی که اقدامات ناقضان قواعد حقوق بشردوستانه به آن‌ها قابل انتساب است. مسؤولیت فردی جنبه کیفری دارد و در شاخه حقوق بین‌الملل از آن بحث می‌شود، ولی مسؤولیت دولت (به رغم تلاش‌های کمیسیون حقوق بین‌الملل در تهیه ماده ۱۹ طرح پیش‌نویس سابق در سال ۱۹۷۶ م.)، جنبه غیر کیفری دارد و در شاخه حقوق مسؤولیت بین‌المللی دولت‌ها بررسی می‌شود (۶). امروزه حقوق بین‌الملل بشردوستانه بسیار گسترده شده و رفتارهای بازیگران دولتی و غیر دولتی را مورد توجه قرار می‌دهد، ضمن این‌که با پیشرفت وسایل و تجهیزات ارتباطی و اطلاعاتی، ملاک‌ها و معیارهای حقوق بین‌الملل بشردوستانه درباره مخاصمات، انواع آن‌ها و شیوه کمک به آسیب‌دیدگان و بازماندگان جنگی تغییر کرده است. حقوق بین‌الملل بشردوستانه موازین سازمان‌های بین‌المللی از جمله سازمان ملل متحد را در دستور کار قرار می‌دهد.

۳ـ جنگ نامتقارن

جنگ نامتقارن در اصطلاح به نبردهایی گفته می‌شود که طرف‌های درگیر در آن از توانایی نظامی یکسانی برخوردار نیستند و برخلاف جنگ‌های کلاسیک فرمول مشخصی برای موقعیت‌های خاص نظامی ندارند، بلکه از عملیات گوناگون، معمولاً با استفاده از عامل غافلگیری برای ضربه‌زدن به دشمن استفاده می‌شود (۷). در واقع در جنگ نامتقارن، سطح بالای امکانات یک طرف مخاصمه باعث اجتناب از رویارویی، درگیری مستقیم و رو در رو با دیگری می‌شود.

حملات سایبری؛ اهداف و جایگاه آنان در قواعد حقوق بین‌الملل

حملات سایبری گونه‌ای از جنگ نامتقارن نیز به شمار می‌روند که در آن، تعداد و نحوه مشارکت بازیگران درگیر در آن مشخص نیست، حتی بازیگران غیر دولتی و حتی افراد دارای مهارت نیز در آن نقش تعیین‌کننده‌ای بر عهده دارند. از طرفی دیگر، حملات سایبری ممکن است در نهایت به جنگ سایبری منجر شود که برخلاف جنگ‌های سنتی، به استفاده از تجهیزات و وسایل رایانه‌ای و ارتباطی برای جنگیدن متکی است. با این حال حملات سایبری دارای گونه‌ها، آثار و پیامدهای متفاوتی هستند که بدان‌ها پرداخته می‌شود.

۱ـ حملات سایبری و آثار آن

حملات سایبری در قوانین و مقررات بین‌المللی چندان شفاف بیان نشده است، حتی مورد توجه نیز قرار نگرفته است، اما به طور کلی، حملات سایبری، شامل رفتار بازیگران دولتی و غیر دولتی در عرصه‌های ارتباطی و اطلاعاتی است که می‌تواند ساختارها و روندهای طرف مقابل را با نابسامانی‌های جدی رو به رو سازد. حملات سایبری اغلب توسط هکرهایی صورت می‌گیرد که شهروندان یک دولت می‌باشند. از آنجایی که برخی از این حملات توسط دولت‌ها و علیه دولتی دیگر صورت می‌پذیرد، غالباً می‌تواند به اختلال و آسیب‌رسانی جدی بر علیه طرف مقابل منجر شود.

برخی شواهد در زمینه حملات سایبری نشانگر آن است که برخی از این حملات می‌توانند نوعی جنگ مسلحانه نیز تلقی شوند، به این دلیل که سلاح، تنها به سلاح‌های سرد و گرم ختم نمی‌شود و در تعریفی موسع می‌تواند شامل وسایلی شود که به دیگران آسیب می‌رساند. به عنوان مثال، در سال ۲۰۰۷ میان روسیه و استونی تنش‌هایی درگرفت که در اثر آن، بسیاری از وزارتخانه‌ها، روزنامه‌ها، احزاب سیاسی، بانک‌ها و نهادهای دولتی استونی توسط حملات سایبری روس‌ها هدف قرار گرفته‌اند. علاوه بر این، اسراییل در ۶ سپتامبر ۲۰۰۷، «عملیات اورکارد (The Operation Orchard)» را علیه مراکز هسته‌ای «دیروزور (Deir ez-Zor.)» در سوریه انجام داد که مورد توجه محققین حملات سایبری واقع شده است (۸). در این حمله اسراییل نشان داد که می‌تواند از تکنولوژی مشابه با سیستم حملات شبکه هوایی «سوتر» آمریکا استفاده کرده و اجازه دهد تا هواپیماهایش به صورت غیر قابل شناسایی از مقابل رادارها عبور کرده و به سوریه وارد گردد. سوتر، یک برنامه رایانه‌ای نظامی است که می‌تواند به شبکه‌های رایانه‌ای و همچنین ساختارهای ارتباطی سایبری از

طریق تکنولوژی و سیستم حمله «Back Door» مجهز شود و حمله کند. آخرین نسخه این نرم‌افزار، تحت عنوان سوتر ۳ در تابستان ۲۰۰۶ آزمایش شده است و تهاجم به لینک‌ها و اهداف بحرانی زمانی مانند موشک‌های بالستیک جنگی و یا موشک‌اندازهای زمین به هوای قابل جابجایی را امکان‌پذیر ساخته است (۹).

در اینجا باید باید تأکید نمود که فقط آن دسته از حملات سایبری که پیامدهایی برابر با پیامدهای حملات مسلحانه دارند یا در بستر مناقشه‌ای مسلحانه رخ می‌دهند، در سطح جنگ سایبری قرار می‌گیرند. به بیانی دیگر، اگر در یک حمله سایبری، آسیب‌ها به حدی شدید بوده باشند که قابل مقایسه با آسیب‌های معمول در جنگ‌ها باشند، در این صورت، حمله سایبری در حکم جنگ سایبری خواهد بود. بنابراین حملاتی که اصل «عدم توسل به زور» را نقض کنند و خسارات قابل توجهی همانند حملات مسلحانه پدید آورند، می‌توانند در زمره حملات مسلحانه نیز قرار گیرند. با این حال به دلیل نبود معیار و ملاک جهانی و حقوقی در این زمینه به چند روش برای بررسی مسلحانه‌بودن یا نبودن حملات سایبری اشاره می‌شود.

۲ـ معیارهای ارزیابی ابزارهای حملات سایبری به عنوان توسل به زور مسلحانه

از آنجایی‌که یکی از مشکلات فراروی حقوقدانان در ارزیابی حقوقی حملات سایبری، فقدان یک معیار مشخص برای تشخیص نوع حملات سایبری از نظر نقض قاعده منع توسل به زور می‌باشد، لذا برای حل این مشکل، راه حل‌هایی پیشنهاد گردیده که به سه مورد اصلی آن اشاره می‌شود.

۲-۱- تحدید حمله سایبری به ابزارهای نظامی کلاسیک: یک رویکرد، که در محافل آکادمیک و دانشگاهی مد نظر و مورد توجه قرار گرفته، این است که از منطق موجود در منشور برای دستیابی به نتایج مطلوب کمک بگیریم. از آنجایی که در منشور «کاربرد زور مسلحانه» ممنوع اعلام گردیده، پس هر چیزی «غیر از کاربرد زور مسلحانه» مجاز است. به عبارت دیگر «کمیت زور» اهمیت کم‌تری نسبت به «کیفیت» آن دارد. استفاده از قوه قهریه نظامی را هنگامی می‌توان کاهش داد که استفاده از روش‌های دیپلماتیک، اقتصادی و سیاسی را بتوان به عنوان جایگزین‌های صلح‌آمیز برای یک جنگ کامل در نظر گرفته و مطرح نمود. بدین‌ترتیب حملات سایبری که در چارچوب حقوق مخاصمات مسلحانه انجام گرفته باشد، می‌تواند قانونی باشد. در نتیجه این رویکرد، با وجود بهره‌مندی از مزایای گفته‌شده، نمی‌تواند به خوبی ظرفیت‌های مخرب حملات سایبری را تعیین کرده و مشخص نماید، لذا معیار دیگری برای سنگ محک حملات سایبری لازم است و آن، رویکرد نتیجه محور به حملات سایبری است.

۲-۲- معیار نتیجه‌محور: روش دیگری که در حل مسأله به ما کمک می‌کند، این است که به جای پرداختن به روش‌ها و ابزارهای جنگی، بر مقدار آسیب وارده تمرکز نماییم. در این حالت، دیگر این مسأله مطرح نیست که آیا یک کارخانه، توسط یک بمب و یا روش‌های مخرب دیگر تخریب گردیده است، بلکه آنچه که در واقع حائز اهمیت است، مقیاس تخریبی است که پس از چنین حمله‌ای بر جای می‌ماند.

در این زمینه، شارپ یک قاعده ساده را مطرح کرده و پیشنهاد داده است: «هر حمله سایبری که به صورت عمدی سبب تأثیرات نامطلوب در قلمروی حاکمیت یک کشور یا دولت خاص گردد، به عنوان استفاده غیر قانونی از زور بر مبنای مفاهیم بند ۴ ماده ۲ قابل احراز بوده و حق دفاع مشروع را به دنبال خواهد داشت. همچنین در مواجهه با این مسأله که آیا عبارت مخرب تنها به معنای تخریب فیزیکی می‌باشد و یا آسیب اقتصادی را شامل می‌گردد، شارپ پیشنهاد می‌دهد که در برخی از شرایط، می‌تواند مورد دوم را نیز شامل شود» (۱۰).

به نظر می‌رسد ایده شارپ تمامی تحریم‌های سیاسی و اقتصادی را پوشش نمی‌دهد و فقط تحریم‌های سیاسی و اقتصادی اجباری تعدیل‌کننده پیوستگی و اتحاد قلمرو و یا استقلال کشورها را شامل می‌شود. بدین‌ترتیب و بر اساس این ایده، یک تأثیر مخرب غیر فیزیکی (مانند اختلال در بازارهای مالی) را در صورتی می‌توان به عنوان «کاربرد زور» تحت بند ۴ ماده ۲ به حساب آورد که برای استقلال و تمامیت ارضی دولت هدف به قدر کافی جدی باشد. این نتیجه سبب تضعیف

این ایده گردیده و به نظر می‌رسد که با فحوای قوانین موجود و دیگر اصول حقوقی بین‌المللی هماهنگ و سازگار نیست، لذا لازم است که به دنبال معیار دیگری برای احراز حملات سایبری به عنوان زور مسلحانه باشیم و این معیار در ویژگی‌های توسل به زور در کاربرد زور مسلحانه نهفته است.

۳-۲- ویژگی‌های «زور مسلحانه» به عنوان سنگ محک: یکی از راه حل‌های نسبتاً مناسب در خصوص احراز کاربرد زور در حملات سایبری، اثبات شباهت حمله سایبری با توسل به زور می‌باشد. این کار با تجزیه و تحلیل حملات سایبری و مشابهت‌سازی آن در چارچوب روش‌های سنتی، قابل انجام و آزمایش بوده و می‌تواند معیاری برای تشخیص و تمایز بین کاربرد زور مسلحانه و فشار اقتصادی یا سیاسی باشد.

این راه حل را مایکل اشمیت نیز مطرح کرده است. در دیدگاه سنتی، زور بر مبنای ابزار شناسایی می‌شود، چراکه در ماده ۲ بند ۴ منشور سازمان ملل متحد نیز ممنوعیت استفاده از زور مربوط به استفاده از زوری است که تحت عنوان و با ابزار مخصوص «نیروی مسلح» در مقابل دولت‌های دیگر استفاده می‌شود و همراه با مقادیر بالای ارتباط بین استفاده و نتایج حاصل از آن شکل گرفته و سازماندهی می‌شود و بیشتر، تخریب و آسیب فیزیکی را شامل می‌گردد. این معیار نشان می‌دهد که چرا زوری که تقریباً همیشه می‌تواند به تخریب یا آسیب فیزیکی بیانجامد، منع شده است، در حالی که اجبار اقتصادی یا سیاسی که با تخریب یا آسیب فیزیکی مورد انتظار همراه است، ضعیف می‌باشد (۱۱).

مایکل اشمیت چارچوب و برخی از معیارها را بر پایه هفت عامل کلیدی تعیین نموده تا ارزیابی نماید که آیا حملات سایبری کم و بیش نزدیک به زور مسلحانه انجام شده و صورت می‌پذیرند یا خیر؟ این عوامل عبارتند از: شدت، نزدیکی، سرعت، تهاجمی‌بودن حمله، قابلیت اندازه‌گیری و تعیین مقیاس، مشروعیت حقوقی و مسؤولیت (۱۲). به نظر می‌رسد که این روش بتواند اصول کیفی منشور را در زمینه شناسایی زور مسلحانه به روشی کمی تغییر دهد و در ضابطه‌مندکردن حملات سایبری کاربرد خواهد داشت.

ضمن این‌که دیوان بین‌المللی دادگستری در نظریه مشورتی خود در خصوص مشروعیت توسل به سلاح‌های هسته‌ای تصریح نمود که مواد ۲ بند ۴ و ۴۲ و ۵۱ منشور ملل متحد، به تسلیحات خاصی اشاره ندارد. این مواد، صرف نظر از تسلیحات مورد استفاده، تمامی مصادیق توسل به زور را دربر می‌گیرد. بنابراین ضرورتی نیست تسلیحات مذکور، دارای آثار انفجاری بوده و یا برای اهداف تهاجمی ساخته شده باشند (۱۳). بدین‌ترتیب از آنجا که ابزار سایبری، برخی از ویژگی‌های جنگ افزارهای کلاسیک را دارد، دقت در این شباهت‌ها می‌تواند در احراز برخی از این حملات سایبری به عنوان یک حمله مسلحانه، به ما کمک کند. بنابراین با استناد به بند ۴ ماده ۲ منشور ملل متحد، ممنوعیت توسل به زور به عنوان یک قاعده آمره و عرفی، برای تمامی دولت‌ها، اعم از عضو و غیر عضو، قابل استناد می‌باشد.

هدف غایی در تدوین این ممنوعیت را می‌توان از طریق دیدگاه‌های موجود مد نظر قرار داد. در مذاکرات تدوین منشور، نماینده برزیل ممنوعیت استفاده از زور مسلحانه و اقتصادی را پیشنهاد داده بود، اما این پیشنهاد در ادامه رد شد (۱۴). امروزه می‌توان این مورد را به عنوان یک توافق عمومی در حوزه اصولی مطرح کرد که در آن استفاده از زور، زور مسلحانه و نه فشارهای روانی یا اقتصادی را پوشش می‌دهد. بر مبنای توضیحات فوق می‌توانیم اولین ویژگی‌های حقوقی جنگ افزارهای سایبری را مشخص نموده و مد نظر قرار دهیم. بر این اساس در صورتی که ابزارهای سایبری در حکم کاربرد زور مسلحانه باشند، در واقع این ابزارها ممنوعیت توسل به زور موضوع ماده ۲ بند چهارم منشور را نقض نموده‌اند. مثال‌های ذکرشده در زمینه حملات سایبری اسرائیل به مراکز هسته‌ای دیرالزور و همچنین حملات سایبری روسیه به استونی از مهم‌ترین مصادیق توسل به زور و نقض اصل عدم توسل به زور مطابق ماده ۲ بند چهارم است.

۳ـ جایگاه حقوق بین‌الملل بشردوستانه در حملات سایبری

برای مقابله با این فعالیت‌ها در سطح ملی، ساز و کارهای حقوق مدنی و حقوق جزا کارآیی کافی دارند و در صورتی که برخی از این حملات ابعاد و آثار فراملی داشته باشند، راه‌های

رفع این مشکل را بایستی در سطح قواعد بین‌المللی جستجو کرد. در این زمینه، «معاهده جرائم سایبری» (۱۵) اولین معاهده بین‌المللی می‌باشد که هدف آن، توجه به جرائم اینترنتی و رایانه‌ای و هماهنگ‌سازی با قوانین ملی بوده است و سبب بهبود روش‌های تحقیقاتی و یا افزایش مشارکت میان کشورها و ملت‌ها در این زمینه شده است. با این حال به دلیل نبود معیار و میزان مشخصی در این زمینه می‌توان به همان اصل گفته‌شده توسط اشمیت یعنی «اثبات شباهت حمله سایبری با توسل به زور» رجوع کرد و با بررسی شواهد و اثرگذاری حملات سایبری بر حوزه‌های مختلف سیاسی، اقتصادی، اجتماعی، نظامی و امنیتی، این نوع حملات را به عنوان ناقض اصل عدم توسل به زور قلمداد کرد و به مقابله با آنان پرداخت.

علاوه بر این، هنگامی که نقض اصل عدم توسل به زور اثبات شود، حقوق بین‌الملل بشردوستانه می‌تواند با ساز و کارهای خود به منازعات سایبری به عنوان یکی از وجوه حملات مسلحانه ورود پیدا کند، به این دلیل که حقوق بین‌الملل بشردوستانه بر مبنای ایده قربانیان منازعات مسلحانه بنیان نهاده شده و از مصدومان این منازعات حمایت می‌کند. این حمایت معمولاً بر حسب صدمه، مرگ، مالکیت، آسیب یا تخریب چارچوب‌بندی شده است. بنابراین اصول اساسی، حقوق بین‌الملل بشردوستانه تصریح می‌کند که منازعات مسلحانه وقتی اتفاق می‌افتد که یک گروه اقداماتی انجام دهد که سبب صدمه کشتار، آسیب یا تخریب شود (۲). بدین‌ترتیب حقوق بین‌الملل بشردوستانه در مواردی که توسل به زور در دستور کار طرفین قرار گیرد و باعث ایجاد خسارات و تلفات گردد، می‌تواند اثرگذاری خود را نشان دهد، ضمن این‌که در منشور ملل متحد، مفاهیم کاربرد زور و حمله مسلحانه تدوین و مشخص شده‌اند. با این وجود تحقیقات زیادی پیرامون تفسیر کاربرد زور و حمله مسلحانه انجام شده که می‌توان آن‌ها را به عنوان راهنمایی برای تفسیر به حساب آورده و نشان‌دهنده ایده‌ها و هنجارهای گوناگون مرتبط با زمان تدوین منشور می‌باشند. حقوق بین‌الملل عرفی نیز بر مبنای کاربردها و رویه‌های دولتی و دکترین مطرح شده است.

برخی از پژوهشگران، در نحوه ارتباط حملات سایبری با حقوق بین‌الملل بحث کرده و اصول مندرج در منشور سازمان ملل و حقوق بین‌الملل عرفی را با بیان مباحث مرتبط با این قوانین و مفهوم حمله مسلحانه مورد توجه قرار داده‌اند. به عنوان مثال، ملزر معتقد است: «منشور سازمان ملل، به عنوان یکی از مهم‌ترین منابع حقوق بین‌الملل در حقوق مخاصمات مسلحانه مطرح می‌باشد. مطالعه در این زمینه نشان داده که محاکم قضایی بین‌المللی نیز در تصمیماتشان از همین منابع استفاده زیادی داشته‌اند» (۱۶). همانند نظر مشورتی دیوان در زمینه سلاح‌های هسته‌ای. بنابراین نبود قوانین و قواعد مشخص در زمینه حملات سایبری به معنای رهاکردن این مسأله مهم در عرصه بین‌المللی نیست. از همین منظر، حقوق بین‌الملل بشردوستانه می‌تواند با توسل به آموزه‌های مندرج در منشور، حملات سایبری را شناسایی نماید و آثار و پیامدهای مخرب آن را برملا سازد.

در واقع دلیل اصلی استفاده این‌گونه محاکم از اصول مندرج در منشور این است که، سنگ بنای اصلی این‌گونه محاکم همچون دیوان بین‌المللی دادگستری، منشور بوده است (۱۷)، هرچند که در کنار منشور، اصول و قواعد حقوق بین‌الملل عرفی و دیگر منابع حقوق بین‌الملل نیز کارایی خود را داشته و دارند، اما حقوق بین‌الملل بشردوستانه به طور خاص می‌تواند با توسل به اصل عدم توسل به زور در نزد منشور سازمان ملل متحد، راهی برای کاهش آثار و خسارت‌های ناشی از حملات سایبری بیابد. بدین‌ترتیب یکی از نظریاتی که در خصوص حملات سایبری امروزه قوت گرفته، قراردادن حملات سایبری در چارچوب نقض اصل منع مداخله در امور داخلی و بین‌المللی، طبق منشور ملل متحد می‌باشد (۱۸).

اگرچه در مقابله با نقض این اصل، حق دفاع مشروع مسلحانه جایز دانسته نشده و فقط دولت قربانی می‌تواند به محاکم قضایی مراجعه نماید، اما در هنگام نقض اصل منع توسل به زور، حق دفاع مشروع برای کشور قربانی در شرایطی قابل اعمال است که حمله مسلحانه انجام یافته باشد و بایستی بر مبنای شرایط مندرج در ماده ۵۱ منشور عمل گردد (۱۹). این مورد در زمره استدلال دولت‌هایی است که حملات

سایبری را در زمره حملات مسلحانه ارزیابی می‌کنند و خواستار اِعمال قوانین حملات مسلحانه و توسل به زور بر حملات سایبری هستند. بر اساس این راه‌کارها می‌توان حملات سایبری را در زمره «توسل به زور» قلمداد نمود.

نکته حائز اهمیت ذکر این مورد است که کارشناسان راهنمای تالین مقیاس و تأثیرات را به عنوان معیارهایی طبقه‌بندی نموده‌اند که برای تعیین این مسأله مطلوب است که آیا حملات سایبری می‌تواند در استفاده از زور تأثیرگذار باشد. همچنین این مورد در راهنمای تالین مطرح شده است که به حملات سایبری به عنوان موارد محتمل توجه شده است که در حملات مسلحانه مدنظر قرار می‌گیرد و استفاده از زور را بر مبنای مقیاس و تأثیرات نشان می‌دهد که در تطابق با حقوق بین‌الملل عرفی و منشور قرار دارد (۱۸). همچنین به نظر می‌رسد که نوع سلاح مورد استفاده در یک حمله اهمیت زیادی هنگام تصمیم‌گیری پیرامون تشخیص حمله مسلحانه نداشته باشد و در صورتی که حمله از یک کشور به کشور دیگر انجام شده باشد، می‌توان مشخص نمود که در چه زمانی و چگونه، فعالیت به سطح حمله مسلحانه می‌رسد (۱۷). بدین‌ترتیب از آنجا که به ظاهر هیچ سند بین‌المللی صراحتاً حملات سایبری را پوشش نداده است، بنابراین اولین قدم در رویارویی و مقابله با حملات سایبری، شباهت‌سازی قواعد موجود با ساختار و ویژگی‌های حملات سایبری می‌باشد.

۱-۳- راه حل؛ تعامل حقوق بین‌الملل بشردوستانه و حقوق حاکم بر حملات سایبری: شاید بتوان گفت یکی از دلایلی که مذاکرات مربوط به کنترل تسلیحات درطول دوره جنگ سرد را به اضمحلال کشانده بود، همانا نگاه امنیتی به تسلیحات به عنوان گزینه اصلی برای حفظ توازن قوا و حفاظت از امنیت ملی بوده است، اما بی‌نتیجه ماندن معاهداتی همچون معاهده کنترل تسلیحات عملاً نشان داد که پارامتر «امنیت ملی» به تنهایی نمی‌تواند بر جامعه بین‌المللی معاصر و عصر تکنولوژی و اطلاعات مؤثر باشد. بنابراین تنها راه حل برون رفت از این چالش، ایجاد یک مفهوم جدید از امنیت بود که بتواند با تهدیدات جدیدی همچون شورش‌های داخلی، تروریسم، جنگ و حملات سایبری و... مقابله نماید. در همین راستا، مفهوم جدیدی به نام «امنیت انسانی» پا به عرصه وجود نهاد. معنا و مفهوم این امنیت در «انسان‌محور» بودن روابط بین‌المللی به جای «دولت‌محور» بودن سیاستگزاری‌های مربوط به امنیت ملی کشورها خواهد بود (۲۰). به نظر می‌رسد همین موضوع برای کنترل و قاعده‌مندکردن حملات سایبری در عرصه حقوق بین‌الملل قابل استفاده باشد. بنابراین همان‌گونه که جامعه جهانی به تسلیحات هسته‌ای و مسائل مربوط به منع توسط زور، رویکردی انسان‌محور داشته است، دولت‌ها و سازمان‌های بین‌المللی نیز در مواجهه با حملات سایبری و تسلیحات نوین، رویکردی انسان‌محور را دنبال کنند. بدین‌معنا هرگاه که اصول مخاصمات مسلحانه و درگیری‌ها به میان بیاید، اصول حقوق بین‌الملل بشردوستانه و امنیت انسانی نیز جلوه‌گر شوند و با توجه به ویژگی‌هایی که حملات سایبری دارد، لزوم رعایت اصول و قواعد حقوق بین‌الملل بشردوستانه نیز بر آنان اِعمال شود.

همچنین از آنجایی‌که فلسفه وجودی حقوق بین‌الملل بشردوستانه، ایجاد قواعد محدودیت‌زا در زمینه استفاده از تسلیحات و حمایت از ابنای بشری می‌باشد و هدف از تدوین قواعد حاکم برحملات سایبری نیز ایجاد امنیت انسانی در عصر فناوری اطلاعات می‌باشد، از این جهت این دو حقوق از نظر موضوعی اشتراک داشته و در بسیاری از جهات با هم در تعامل خواهند بود (۲۱). بدین‌ترتیب با توجه به نوپابودن رویکرد حقوقی به حملات سایبری، تا زمان برقراری و تدوین یک حقوق جامع و حاکم بر حملات سایبری، می‌توان از اصول و قواعد حقوق بین‌الملل بشردوستانه استفاده نمود و هر جا که کمبودی احساس گردد، می‌توان به حقوق بین‌الملل عرفی یا اصولی همچون شرط مارتنز روی آورد. از طرفی دیگر هر دوی این حقوق (حقوق بین‌الملل بشردوستانه و حقوق حاکم بر حملات سایبری) بر مسأله امنیت متمرکز بوده و اشتراک غایی آن‌ها نیز همین مسأله امنیت و به خصوص امنیت انسانی در کنار امنیت ملی می‌باشد. بنابراین در هر دوی آن‌ها، توجه و تأکید ویژه‌ای بر مفهوم امنیت انسانی گردیده است (۲۱).

حقوق بین‌الملل بشردوستانه از آنجا که بر کمک به انسان‌ها در شرایط جنگی معطوف است، توانایی پیوندزدن قوانین خود

با امنیت انسانی را در شرایط نقض اصل عدم توسل به زور دارا می‌باشد. بدین‌معنا که هرگونه اقدام مسلحانه را که به نقض اصل مزبور منجر شود، تحت پوشش خود قرار دهد و رویکردهای بین‌المللی را برای متوقف‌کردن آن به کار گیرد، ضمن این‌که حقوق بین‌الملل بشردوستانه، می‌تواند آموزه‌های حقوق بشری را برای همه جهانیان به طور مساوی برقرار سازد و توسعه انسانی مساوات‌طلبانه را برای همه رقم بزند. بنابراین با به کارگیری روش‌های انسان‌مدارانه و امنیت انسان‌محور، همه کشورهای جهان، می‌توان شاهد رویکرد واحدی در قابل تهدیدات ناشی از حملات سایبری بود، چنانچه در منشور حقوق بشر بر توسعه همکاری دولت‌های ملی برای تحقق حقوق بشر تأکید شده است. بنابراین لازمه این همکاری آن است که کشورهای توسعه‌یافته به کشورهای در حال توسعه کمک کنند (۲۲).

۲-۳- آثار اعمال حقوق بین‌الملل بشردوستانه بر حملات سایبری: با ضابطه‌مندکردن فضای سایبر در چارچوب حقوق بین‌الملل بشردوستانه هم فضای سایبر، فضایی امن برای مراودات بین مردم و تعاملات بین‌المللی می‌شود که درآن فضا، امنیت انسانی به حداکثر می‌رسد و هم لزوم رعایت ضوابط حقوق بین‌الملل بشردوستانه در فضای سایبر، باعث نمایان‌شدن کارکرد واقعی حقوق بین‌الملل بشردوستانه که همانا حمایت از کرامت انسانی بوده است، می‌شود.

در اینجا لازم به ذکر است با تمام تمهیداتی که حقوق بین‌الملل برای ضابطه‌مندکردن روابط بین‌المللی در قالب معاهدات و در رأس آن‌ها، منشور ملل متحد انجام داده است، اما هنوز نقطه ضعفی به نام «عدم پایبندی به تعهدات» در نظام حقوقی بین‌المللی از گذشته به جا مانده است، هرچند که با ایجاد حوزه‌های جدیدی همچون مسؤولیت بین‌المللی دولت، مسؤولیت کیفری بین‌المللی و... تا اندازه‌ای از «عدم پایبندی» کاسته شده است، اما با توسعه حقوق بین‌الملل درچند دهه اخیر، حقوقدانان بین‌المللی در اکثر معاهدات از «تدابیر اعتمادساز» در قالب مفاد معاهدات و ایجاد ضمانت اجرا در خصوص «عدم پایبندی به تعهدات» این معضل را حل نموده‌اند.

در این راستا یکی از مشکلات عمده در ضابطه‌مندکردن فضای سایبر و سوق دادن این فضا به سمت «انسانی‌شدن»، همانا عدم پایبندی برخی کشورها به اصول و قواعد فعلی و عدم اعتماد بقیه کشورها به ضوابط فعلی بوده است، هم‌چنانکه برخی کشورهای قدرتمند با ایجاد قواعد و مقرراتی دست و پاگیر نه‌تنها ضوابط بین‌المللی را در این زمینه رعایت نمی‌کنند، بلکه برخی اصول جهانی از جمله حقوق بشر را در راستای منافع خود تفسیر می‌کنند. از این منظر، مقوله حقوق بشر، نمونه دیگری از سلطه کم و بیش آگاهانه‌ای است که ملت‌های قدرتمند به کار می‌گیرند تا برتری خود را حفظ کنند و از وضع موجود دفاع کنند، این حقوق، سلاحی سیاسی باقی می‌ماند (۲۳). از این جهت، اتخاذ چنین رویه‌ای در عرصه حملات سایبری باعث ایجاد چالش‌های متعددی شده است که به نوبه خود می‌تواند موانعی برای اِعمال قوانین حقوق بین‌الملل بشردوستانه گردد.

به نظر می‌رسد در کنار ضابطه‌مندکردن استفاده از فضای سایبر در حوزه حقوق بین‌الملل، می‌بایست تدابیر اعتمادساز نیز در هر معاهده یا بیانیه‌ای پیش‌بینی گردد تا مشکلاتی که در دهه‌های قبل در اجرای معاهدات بین‌المللی وجود داشته است، در معاهدات مرتبط با فضای سایبر پدید نیاید. در همین زمینه، یکی از پیشنهاداتی که برای تدوین تدابیر اعتماد ساز در معاهدات و موافقت‌نامه‌های بین‌المللی ارائه گردیده مربوط به پیشنهاد «جان براوسکی» (۲۴) می‌باشد که به زعم ایشان تدابیر اعتماد ساز به سه دسته تقسیم می‌شوند: ۱ـ محدودیت‌ها؛ ۲ـ تبادل اطلاعات؛ ۳ـ نظارت و تحقیق.

محدودیت‌ها در واقع فعالیت‌های مربوط را از طریق تنظیم مقرراتی که کجا، کی و چگونه صورت بپذیرد، محدود می‌نماید.

هدف از تبادل اطلاعات، افزایش آگاهی‌های دوطرف در مورد استراتژی‌ها و اقدامات مربوط می‌باشد.

و نهایتاً این‌که تحقیق و نظارت باعث می‌گردد که ارزیابی مستقل و قابل اعتمادی از نوع و ماهیت اقدامات طرفین صورت پذیرد (۲۴).

بنابراین در ضابطه‌مندکردن فضای سایبر و برای جلوگیری از حملات سایبری و نقض حقوق بین‌الملل بشردوستانه لازم

است که هر سه مرحله تدابیر اعتمادساز را در هر معاهده یا موافقتنامه بین‌المللی در خصوص استفاده از فضای سایبر لحاظ نمود، یعنی هر کشوری برای فعالیت در فضای سایبر بایستی محدودیت‌هایی را طبق نظام پایبندی در تعهدات بپذیرد و در هنگام تبادل اطلاعات شفافیت داشته باشد و در مراحل تحقیق و نظارت با سازمان‌ها و نهادهای مربوطه همکاری لازم را داشته باشد.

نتیجه‌گیری

حملات سایبری پدیده‌ای نوظهور در میان جنگ‌افزارهای مدرن محسوب می‌شود. این حملات صلح و امنیت جهانی را به خطر می‌اندازد و نیاز به تعریف قواعد جدید و منطبق با اصول حقوق بین‌الملل و منشور سازمان ملل متحد را گوشزد می‌کند. تسلیحات سایبری قادرند در کوتاه‌ترین زمان اثرات ویرانگر و خارج از کنترلی از خود نشان دهند. از این رو امروزه قواعد بین‌المللی در مورد سربازی که اقدام به پرتاب نارنجک به آن سوی مرز می‌کند، وجود دارد، ولی در مورد سربازان سایبری که نهادهای مالی و اقتصادی یک دولت را هدف حملات خود قرار می‌دهند، قوانین بسیار ضعیفی وجود دارد. این حملات از دیدگاه قواعد شناخته‌شده بین‌المللی و از جمله اصول و اهداف منشور ملل متحد غیر قانونی محسوب می‌شوند. همچنین در کنوانسیون‌های ژنو که درباره قواعد حقوق بین‌الملل بشردوستانه می‌باشند، بیان شده است که دولت‌ها در استفاده از هر نوع سلاحی مجاز نمی‌باشند، به این دلیل که در این کنوانسیون تفکیک و جداسازی میان سلاح‌های مورد استفاده صورت نگرفته است. بنابراین می‌توان با تعریفی جدید و مشخص‌نمودن انواع حملات جدید از جمله حملات سایبری، راه‌کارهای تحدید آنان را نیز فراهم آورد.

بر اساس تحقیق حاضر، رویکردی که اشمیت مطرح نموده است و خواستار شبیه‌سازی میزان اثرگذاری حملات سایبری همانند سایر حملات از جمله حملات نظامی و آشکار شده است، به شکل بهتری می‌تواند قواعد و قوانین را در زمینه تحدید حملات سایبری به کار گیرد. مطابق ایده وی، شدت، نزدیکی، سرعت، تهاجمی‌بودن حمله، قابلیت اندازه‌گیری و تعیین مقیاس، مشروعیت حقوقی و مسؤولیت حملات سایبری می‌توانند به عنوان ملاک‌هایی در این زمینه در نظر گرفته شوند، ضمن این‌که به کارگیری این روش می‌تواند باعث ورود هرچه بیشتر قواعد حقوق بین‌الملل بشردوستانه در زمینه حملات سایبری گردد و حملات سایبری‌ای که منجر به آسیب پذیری گسترده و تضییع حقوق شهروندان در دولت‌های مختلف می‌شود را تحت کنترل قرار دهد. به علاوه ایجاد شفافیت در میان دولت‌ها، از جمله قدرت‌های بزرگ در زمینه استفاده از حملات سایبری به شکل مطلوب‌تری می‌تواند قواعد حقوق بین‌الملل بشردوستانه را در این زمینه اجرایی نماید. بنابراین اصل مشابهت‌سازی به لحاظ تکنیکی و پاسخگویی دولت‌ها و نظام‌های سیاسی در عرصه بین‌الملل به شکل قابل توجهی می‌تواند به تدوین قوانینی در زمینه حملات سایبری منجر شود. همچنین گذر نهادهای حقوقی بین‌المللی از جمله سازمان ملل متحد از منظر سنتی و تأکید بر مؤلفه‌های نظامی جدید از جمله حملات سایبری و قرارگرفتن «امنیت انسانی» به عنوان مؤلفه‌ای کیفی در کنار امنیت نظامی به شکل قابل توجهی می‌تواند آثار و پیامدهای حملات سایبری را مدنظر قرار دهد. بدین‌ترتیب با ضابطه‌مندکردن فضای سایبر در چارچوب حقوق بین‌الملل بشردوستانه هم فضای سایبر، فضایی امن برای مراودات بین مردم و تعاملات بین‌المللی می‌شود که درآن فضا، امنیت انسانی به حداکثر می‌رسد.

References

1. Ahmadi M. Smart Wars. *Magazin Mehrnameh* 2009: 2(3): 1-18.

2. Abbasi M, Moradi H. Cyber war from the perspective of international humanitarian law. *Journal Parliament and Strategy* 2015; 22(81): 37-81.

3. Dost Mohammadian H. Crims, Law, Regulation and Elaectronic evidence. *Magazin Analysts of the Information Age* 2010; 4(35): 1-21.

4. Yeganeh Azad S. The rights of cyberatttacks. Master of Thesis. Shiraz: University of Shiraz; 2014.

5. Hathaway O, Crootof R, Levitz P. The Law of Cyber Attack. California: Law Review; 2012.

6. Shamsaie M, Soleimani Torkmani H. Thinking about the International responsibility of goverments, cause by violations of international humanitarian law. *Journal of Jurisprudence and Law* 2008: 5(17); 179-206.

7. Aghdar H. The Nature of the asymmetric warfar. Tehran: Publications an Inrernational Relations Think Tank; 2012.

8. Leyden J. Israel suspected of 'hacking' Syrian air defenses. *Posted in Enterprise Security* 2007; 1(2): 1-19. Available at: http://www.theregister.co.uk.10/04/ radar_hack_raid/.

9. Remus T. Cyber-attacks and International law of armed conflicts; a "jus ad bellum" perspective. *Journal of International Commercial Law and Technology* 2013; 8(3): 402-571.

10. Sharp W. Cyberspace and the use of force. New York: Publications Aegis Research Corporation; 1999.

11. Schmitt M. Computer network attack and the use of force in international law: Thoughts on a normative framework. *Columbia Journal of Transnational Law* 1999; 13(37): 885-936.

12. Starr S. Towards an Evolving Theory of Cyberpower. New York: A Center for Technology and National Security Policy (CTNSP); 2009. p.1-38.

13. Faghih Habibi A. Modern warfar and Cyberattack in the context of international space. *Journal Contemporary Political Quotes* 2016; 7(1): 115-144.

14. Simma B. The Charter of the United Nations: A commentary. London: Oxford; 2002.

15. The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe on 8 November 2001. It was opened for signature in Budapest, on 23 November 2001 and it has entered into force on 1 July 2004. Significantly, Russia and China never sign it.

16. Melzer N. Cyberwarfare and International Law. UNIDIR Resources, Ideas for peace and security. Liverpool: Liverpool John Moores University; 2011.

17. Josefson E. Cyber Warfare and the Concept of Armed Attack. Victoria: Publications Department of Law at the Gothenburg University; 2012.

18. Tallinn M. Cyber Attacks and the Use of Force in International Law. Helsinki: University of Finland; 2014.

19. Wingfield T. The Law of Information Conflict. London: Publications Hardcover; 2000.

20. Abdollahkhani A. International Security: Opportunities Treats and Challenges. Tehran: Publications Abrare Moaser; 2004.

21. Saed N. International Humintarian Law and Nuclear Weapons. Tehran: Institude for Legal Reasers and Studies Share Danesh; 2009.

22. Alston S, Philip H. International Human Rights in Context: Law, Politics, Morals. London: Axford University Press; 1996.

23. Panikkar R. Is the Nation of Human Rights a Western concept?. In Book Fathers Language. Translate by Nikoo Bandari A. Tehran: Publications Tarjoman; 2002.

24. Brewski J. Avoiding War in the Nuclear age. Boulder: Westview Press; 1986.