مجله حقوقی بین‌المللی/ شماره ۶۲/ بهار ـ تابستان ۱۳۹۹/ صفحات ۱۴۴ ـ ۱۱۹

چالش‌های حقوقی قابلیت‌های فضای سایبری در پرتو ماده ۳۶ پروتکل یکم الحاقی ۱۹۷۷

حسین شریفی طرازکوهی

جعفر برمکی **

شناسه دیجیتال اسناد (DOI) : 10.22066/CILAMAG.2019.84640.1491

تاریخ دریافت: ۱۳۹۷/۰۲/۰۲ تاریخ پذیرش: ۱۳۹۷/۰۸/۰۱

چکیده

بیش از چهار دهه از تصویب ماده ۳۶ پروتکل اول الحاقی به کنوانسیون‌های چهارگانه ژنو به‌عنوان هنجار ارزیابی حقوقی سلاح‌ها، ابزار و روش‌های جدید جنگی می‌گذرد. معیارهای مندرج در این ماده بر اساس سلاح‌هایی تدوین شده که در زمان تصویب آن وجود داشت. توسعه فناوری‌های جدید، سلاح‌هایی را پدید آورده که برای هنجارهای نظارتی احراز قانونی‌بودن آن‌ها دشواری‌هایی ایجاد کرده است. فضای سایبری به‌عنوان یکی از این فناوری‌ها، قابلیت‌هایی دارد که ممکن است به‌عنوان سلاح برای ورود خسارت و جراحت در مخاصمات مسلحانه به کار گرفته شود. آیا ماده ۳۶ پروتکل یکم الحاقی می‌تواند چنین قابلیت‌هایی را بر اساس حقوق بین‌الملل بشردوستانه قانونمند کند؟ به‌دلیل جدیدبودن این قابلیت‌ها و دشواری در اطلاق آن‌ها به‌عنوان سلاح، بررسی حقوقی آن‌ها در پرتو ماده ۳۶ پروتکل یکم الحاقی چالش‌هایی دارد. بررسی ارکان ماده ۳۶ به همراه ماهیت قابلیت‌های فضای سایبری نشان داد که ارزیابی حقوقی آن‌ها با دشواری‌هایی روبه‌روست، مانند فقدان قواعد و مقرراتی که صریحاً استفاده از فضای سایبری را منع یا مجاز کرده باشد، سپردن تعریف سلاح به دول عضو پروتکل، تعریف سلاح جدید، عدم اطلاق شئ به داده‌های رایانه‌ای برای تلقی قابلیت سایبری به‌عنوان سلاح، فقدان اجماع بین‌المللی در خصوص آثار به‌کارگیری قابلیت‌های سایبری، فقدان مقرره‌ای در خصوص الزام افراد و گروه‌های تولیدکننده سلاح‌های سایبری برای ارزیابی حقوقی و مهم‌تر از همه، درهم‌تنیدگی شبکه‌های نظامی و غیرنظامی که احتمال دارد با کاربرد قابلیت‌های سایبری، شبکه‌های غیرنظامی حیاتی آلوده شده و رعایت اصول بنیادین

دانشیار دانشکده حقوق‌وعلوم‌سیاسی دانشگاه آزاد اسلامی، واحد علوم‌وتحقیقات تهران hsharifit@yahoo.com

نویسنده مسئول، دانشجوی دکتری حقوق بین‌الملل دانشگاه پیام نور jbarmaki@yahoo.com

حقوق بین‌الملل بشردوستانه اعم از تفکیک، تناسب، ضرورت نظامی و اتخاذ اقدامات احتیاطی را با فناوری امروز غیرممکن کند.

واژگان کلیدی

حقوق بین‌الملل بشردوستانه، حقوق مخاصمات مسلحانه، پروتکل یکم الحاقی، فضای سایبری، بررسی حقوقی، سلاح‌های جدید، فناوری‌های نوین، دستورالعمل تالین

مقدمه

بشر برای ساخت تسلیحات قوی جهت ازپادرآوردن هم‌نوعان خود، استعداد بسیار شگرفی دارد و تاریخ به‌خوبی بیانگر این امر است. زمانی که حقوق بین‌الملل با انگیزه حمایت مستقیم از دولت‌ها یا با انگیزه حمایت از انسان‌ها پا به عرصه وجود گذاشت، برای محدودکردن اختیار دولت‌ها در استفاده از جنگ‌افزارها تلاش بسیاری کرد. دقیقاً در زمانی که در سال ۱۸۶۴ مذاکرات مربوط به نخستین کنوانسیون ژنو در حال انجام بود، سلاحی جدید و بسیار مخرب، (البته در زمان خود) در حال شکل‌گیری و توسعه بود. در سال ۱۸۶۳ گلوله‌ای که قدرت انفجاری بسیار بالایی داشت از سوی امپراتوری روسیه به جهان معرفی شد. قدرت انفجاری این گلوله در سال ۱۸۶۷ به‌گونه‌ای اصلاح شد که بتواند جراحات شدیدی در بدن انسان ایجاد کند.[۱] در همین زمان بود که با ابتکار دولت روسیه تزاری، یک کمیسیون بین‌المللی نظامی[۲] با هدف منع کاربرد این گلوله تشکیل شد که نتیجه آن، بیانیه ۱۸۶۸ *سن پترزبورگ* بود. این بیانیه با ممنوعیت استفاده از یک سلاح خاص بر مبنای انسان‌دوستی و حقوق انسانیت، به اولین سند بین‌المللی تبدیل شد که به قانونمندکردن سلاح‌های حاصل از پیشرفت‌های فناوری پرداخت.[۳] بر اساس این بیانیه، تضعیف نیروهای نظامی

1. Daoust, Isabelle, Coupland, Robin and Ishoey, Rikke, "New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare", *International Review of Red Cross*, vol. 84, no. 846, 2002, p. 346.

۲. تزار روسیه، *الکساندر سوم* که نگران به‌کارگیری گلوله‌های انفجاری علیه نیروهای خود بود، یک کمیسیون بین‌المللی نظامی متشکل از ۱۶ کشور (اتریش ـ مجارستان، باواریا، بلژیک، دانمارک، فرانسه، انگلیس، یونان، ایتالیا، هلند، پرتغال، پروس، کنفدراسیون آلمان شرقی، روسیه، سوئد ـ نروژ، سوئیس، امپراطور عثمانی و ورتمبرگ، ایالتی از آلمان امروزی در سال‌های ۱۹۱۸–۱۸۰۵) تشکیل داد که هدف آن، بحث درباره ممنوعیت استفاده از مرمی‌های جدید بود. این کمیسیون در یازدهم دسامبر ۱۸۶۸ بیانیه‌ای امضا کرد که بر اساس آن، استفاده از هر مرمی انفجاری یا آتش‌زای زیر ۴۰۰ گرم ممنوع شناخته شد. برای اطلاعات بیشتر، ن.ک:

Frits Kalshoven, "The History of International Humanitarian Law Treaty-Making", in: Rain Liivoja and Tim McCormack (eds.), *Routledge Handbook of the Law of Armed Conflict*, 1st ed., London, Routledge, 2016.

See also: http://hhr-atlas.ieg-mainz.de/articles/jevglevskaja-st_petersburg.

۳. قربان‌نیا، ناصر؛ *حقوق بشر و حقوق بشردوستانه*، پژوهشگاه فرهنگ و اندیشه اسلامی، ۱۳۷۸، ص ۱۷۸.

دشمن تا جایی باید ادامه پیدا کند که دشمن را به تسلیم وادارد. در نتیجه هیچ ضرورتی ندارد که اقدامات یک طرف درگیری سبب تشدید رنج یا ناتوانی نیروهای نظامی طرف مقابل شود.[۴] لذا هر سلاحی که به این امر منتهی شود، مغایر حقوق انسانیت است.[۵]

حدود ۸۰ سال بعد، اعضای متعاهد پروتکل یکم (۱۹۷۷) الحاقی به کنوانسیون‌های چهارگانه ۱۹۴۹ ژنو، ماده‌ای تحت عنوان «سلاح‌های جدید» (ماده ۳۶) در پروتکل گنجاندند. این ماده دولت‌ها را موظف می‌کند قبل از به‌کارگیری هر سلاح، ابزار یا روش نوین جنگی، از قانونی‌بودن آن اطمینان حاصل کنند. به‌علاوه از دولت‌ها می‌خواهد در هر مرحله‌ای از مطالعه، توسعه، کسب یا پذیرش سلاح، ابزار یا روش‌های جدید جنگی، آن‌ها را با قواعد موجود در پروتکل یکم الحاقی و قواعد حقوق بین‌الملل قابل اعمال مطابقت داده تا بتوانند قانونی یا غیرقانونی‌بودن آن را معین کنند. یک سلاح، ابزار یا روش جنگی، بسته به شرایط به‌کارگیری آن می‌تواند قانونی یا غیرقانونی تلقی شود. به همین دلیل است که ماده ۳۶، ضرورت تعیین قانونی‌بودن کاربرد سلاح‌ها، ابزار و روش‌های جدید جنگی را بیان می‌دارد. این ماده، سلاح‌ها، ابزار و روش‌های نوین جنگی که در تمام شرایط به‌کارگیری، حقوق بین‌الملل را نقض می‌کنند ممنوع کرده و در صورتی که در برخی شرایط، سبب نقض حقوق بین‌الملل شوند، کاربرد آن‌ها را صرفاً در همان شرایط محدود می‌کند.[۶] این دو اقدام از طریق تعیین قانونی‌بودن سلاح‌های نوین، قبل از توسعه، کسب یا پذیرش در زرادخانه یک دولت انجام می‌گیرد.

اگرچه هنجارهای عرفی و معاهداتی در زمینه قانونمندکردن (ممنوعیت یا محدودیت) سلاح‌های مغایر با اصول و قواعد حقوق بین‌الملل بشردوستانه وجود دارد، پیشرفت‌های خیره‌کننده علمی و فنی دهه‌های اخیر به حدی سریع است که حقوق بین‌الملل نمی‌تواند همه تغییرات سریع ناشی از فناوری‌های تسلیحات را پوشش دهد. دامنه و شتاب روند تکاملی به‌کارگیری این فناوری‌ها در میدان جنگ طی قرن اخیر، به‌ویژه چند دهه گذشته، به‌سرعت در حال پیشرفت است. مهم‌ترین عامل در اجرای حقوق بین‌الملل بشردوستانه در قرن حاضر، به‌طور مشخص مربوط به تغییرات شگرف در فناوری جنگ است. تغییرات ناگهانی و عمده در شیوه‌های جنگیدن ناشی از فناوری‌های نوین، تغییرات گسترده در حقوق بین‌الملل بشردوستانه را ضروری می‌نماید.[۷] برخی از این فناوری‌ها مانند فضای سایبری در حال حاضر به کار می‌روند و برخی دیگر (مانند نانوفناوری، روبات‌های سرباز و فناوری فضایی) در حال توسعه هستند. قابلیت‌های سایبری، گاهی به شکل برنامه‌های

4. Green, Leslie C., *The Contemporary Law of Armed Conflict*, 3rd ed., UK, Juris Publishing, 2008, p. 155.

5. Daoust, Isabelle et al., *op.cit.*, p. 346.

6. Boulanin, Vincent, "Implementing Article 36, Weapon Reviews in the Light of Increasing Autonomy in Weapons Systems", *SIPRI Insight on Peace and Security*, no.201/1, November 2015.

۷. شریفی طرازکوهی، حسین؛ *حقوق بشردوستانه بین‌المللی*، چاپ دوم، میزان، ۱۳۹۵، ص ۱۹۲.

نرم‌افزاری و آن‌هم با اهداف تخریبی استفاده می‌شوند که به‌کارگیری‌شان می‌تواند آثار مخربی هم‌پایه آثار سلاح‌ها در شکل فیزیکی داشته باشد. حال باید دید که آیا در حقوق بشردوستانه مقرراتی وجود دارد که به‌طور صریح و مستقیم، استفاده از وسایل و شیوه‌های نبرد در فضای سایبری را منع کرده یا مجاز دانسته باشد.

در این راستا، از یک سو هنجارهای عرفی و معاهداتی در حوزه بررسی حقوقی سلاح‌ها، ابزار و روش‌های جدید جنگی مطرح است که مربوط به دهه‌های گذشته است و از سوی دیگر، قابلیت‌های عرصه فضای سایبری که نتیجه فناوری‌های امروز است. هنجارهای موجود باید بتواند کلیه فناوری‌های تسلیحاتی جدید ازجمله قابلیت‌های فضای سایبری را از لحاظ حقوقی بررسی و قانونی‌بودن یا غیرقانونی‌بودن آن‌ها را تعیین کند. اما توسعه بسیاری از فناوری‌های جدید نظامی به‌ویژه مواردی که در فضای سایبری به کار برده می‌شود، سبب تغییر در کیفیت عناصر مخاصمات مسلحانه (مانند میدان نبرد، بازیگران و ابزار و روش‌های جنگی) شده و کاربرد قطعی چنین فرضیه‌هایی را با مشکل مواجه کرده است. مضاف بر آن، قابلیت‌های فضای سایبری بر روی زیرساخت‌های غیرنظامی قرار داشته و برای ورود خسارت یا جراحت طراحی نشده یا مورد استفاده قرار نمی‌گیرد. به همین دلیل، اطلاق جنگ‌افزار به این قابلیت‌ها و انجام بررسی حقوقی برای آن‌ها با دشواری‌هایی روبه‌روست. سپردن تعریف جنگ‌افزار به دولت‌ها و فقدان اجماع بین‌المللی در مورد تعریف آن‌ها، پیچیدگی بررسی حقوقی قابلیت‌های سایبری را دوچندان کرده است.

در نتیجه این پرسش مطرح می‌شود که آیا می‌توان بررسی حقوقی قابلیت‌های فضای سایبری را با استفاده از ماده ۳۶ پروتکل یکم الحاقی انجام داد؟ برای پاسخ به این پرسش، مقاله حاضر در چهار مبحث به استخراج چالش‌های بررسی حقوقی خواهد پرداخت، شامل: ۱ـ بررسی حقوقی ذیل ماده ۳۶ پروتکل یکم الحاقی ۲ـ قابلیت‌های سایبری: ماهیت و ویژگی ۳ـ امکان اطلاق سلاح به قابلیت‌های سایبری و ۴ـ بررسی حقوقی قابلیت‌های فضای سایبری ذیل ماده ۳۶.

۱. ماده ۳۶ پروتکل یکم الحاقی

در زمانی که ماهیت مخاصمات مسلحانه در حال تغییر است و دسترسی به سلاح‌ها، ابزار و روش‌های نوین جنگی پیچیده سهل‌تر شده است، ضرورت دارد تا این سلاح‌ها دقیق‌تر ارزیابی شوند. استعداد فوق‌العاده بشر در توسعه سلاح‌های جدید، اغلب با تلاش‌هایی برای محدود یا قانونمندکردن استفاده از آن‌ها نیز همراه بوده است. اولین نمونه این محدودیت، بیانیه *سن‌پترزبورگ* بود که با دعوت تزار روسیه برای تشکیل کمیسیون بین‌المللی نظامی و در پی معرفی سلاح مرگبار جدیدی در سال ۱۸۶۸ حاصل شد. بیانیه *سن‌پترزبورگ*، اولین توافق چندجانبه کنترل تسلیحات

برای قانونمندکردن ابزار و روش‌های مورد استفاده در جنگ است. در پاراگراف‌های مقدماتی این بیانیه، اصلی مبنی بر تضعیف نیروی نظامی دشمن به‌عنوان هدف قانونی جنگ آمده و به‌کارگیری سلاح‌هایی را که رنج انسان‌های ناتوان را به‌صورت غیرضرور افزایش داده یا مرگ آن‌ها را اجتناب‌ناپذیر می‌کند، فراتر از هدف مزبور می‌داند.[۸]

پس از بیانیه *سن پترزبورگ* که اولین سند ممنوعیت کاربرد سلاح جدید است، تنها اشاره به قانونمندکردن سلاح‌های جدید را می‌توان در ماده ۳۶ پروتکل یکم (۱۹۷۷) الحاقی به کنوانسیون‌های چهارگانه ۱۹۴۹ ژنو یافت. ماده ۳۶ دولت‌ها را موظف می‌کند از قانونی‌بودن جنگ‌افزار، ابزار یا روش نوین جنگی که تصمیم دارند در ارتش‌های خود به کار گیرند اطمینان حاصل کنند. این ماده از دولت‌ها می‌خواهد تا در مرحله مطالعه، توسعه، کسب یا پذیرش هر سلاح، ابزار یا روش نوین جنگی، آن را با قواعد موجود در پروتکل یکم الحاقی و قواعد حقوق بین‌الملل قابل اعمال، مطابقت داده تا بتوانند قانونی یا غیرقانونی‌بودن آن را معین کنند. هدف ماده ۳۶، ممنوعیت کاربرد سلاح‌ها، ابزار و روش‌های نوین جنگی است که حقوق بین‌الملل را در تمامی شرایط نقض کرده و محدودکردن کاربرد آن‌هایی است که حقوق بین‌الملل را در برخی شرایط نقض می‌کنند. این دو اقدام از طریق تعیین قانونی‌بودن جنگ‌افزارهای جدید، قبل از توسعه، کسب یا پذیرش در زرادخانه یک دولت انجام می‌گیرد.[۹] این امر بدین معنی است که به‌عنوان اولین قدم در بررسی حقوقی باید تعیین کرد آیا ممنوعیتی خاص ذیل معاهداتی که دولت بررسی‌کننده متعاهد آن است وجود دارد و اینکه آیا آن معاهده، استفاده از یک سلاح یا روش جنگی را ممنوع یا محدود کرده است یا خیر. در این بررسی، علاوه بر معاهدات ممنوعیت تسلیحات خاص، دو دسته تعهدات حقوقی بین‌المللی دیگر، دولت‌ها را موظف می‌کند تا سلاح را طبق حقوق بین‌الملل عرفی و ماده ۳۶ پروتکل یکم الحاقی به کنوانسیون‌های ۱۹۴۹ ژنو بررسی کنند.[۱۰]

۱ـ۱. ارکان ماده ۳۶ پروتکل یکم الحاقی

قبل از ورود به ارکان ماده ۳۶ لازم است ماده ۳۵ پروتکل یکم الحاقی مرور شود تا زمینه لازم برای درک بهتر ماده ۳۶ فراهم آید. ماده ۳۵ حاوی سه بند است که هریک از آن‌ها به اصول بنیادین در خصوص کاربرد سلاح‌ها اشاره دارد. بند ۱ به محدودبودن اختیار طرف‌های درگیری

---

۸. برای مطالعه متن بیانیه مزبور، ن.ک:
http://www.weaponslaw.org/assets/downloads/1868_St_Petersburg_Declaration.pdf.

9. "A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977", *International Review of the Red Cross*, Geneva, vol. 88, No. 864, December 2006, p. 933.

10. Blake, Dunkan & Imburgia, Joseph S., "Bloodless Weapons? The Need to Conduct Legal Review of Certain Capabilities and the Implications of Defining Them as Weapons", *The Air Force Law Review*, vol. 66, 2010, p. 163.

مسلحانه در انتخاب روش‌ها و ابزار جنگی می‌پردازد و بند دوم به‌کارگیری سلاح‌ها، پرتابه‌ها و مواد و روش‌های جنگی را که دارای ماهیتی غیرانسانی بوده و سبب ورود جراحت غیرضرور یا رنج بیهوده می‌شود ممنوع کرده است. بند سوم، روش‌ها یا ابزار جنگی را ممنوع می‌کند که به‌کارگیری عمدی آن‌ها سبب ورود خسارت گسترده، درازمدت و شدید به محیط‌زیست شده یا انتظار می‌رود که چنین آثاری داشته باشد. این اصول در بررسی حقوقی بر اساس ماده ۳۶ به کار گرفته می‌شود.

بررسی تفاسیر موجود از ماده ۳۶ پروتکل یکم الحاقی، چهار رکن مهم ماده مزبور را روشن می‌کند که شامل کشورهای مشمول بررسی، سلاح‌های مشمول بررسی، مقررات حاکم بر بررسی و اقدامات پس از بررسی حقوقی است. آگاهی از این ارکان، به بررسی حقوقی برای قابلیت‌های فضای سایبری ذیل ماده ۳۶ کمک می‌کند.

الف. کشورهای مشمول بررسی

در خصوص کشورهای مشمول بررسی دو نظریه متفاوت وجود دارد. برخی معتقدند پروتکل یکم الحاقی، حاکم بر مخاصمات مسلحانه بین‌المللی است و چنین مخاصماتی صرفاً میان دولت‌ها رخ می‌دهد و تنها متعاهدین پروتکل ملزم به تعیین قانونی‌بودن یا غیرقانونی‌بودن کاربرد سلاح‌هایی هستند که تصمیم دارند در نیروهای مسلح خود به کار گیرند.[۱۱] ادبیات این ماده نشان می‌دهد که الزام انجام بررسی فقط شامل متعاهدین این پروتکل است، چه به توسعه و ساخت سلاح‌ها بپردازند یا اینکه آن را خریداری کنند؛ در حالی که برخی دیگر معتقدند دولت‌ها بر اساس حقوق بین‌الملل عرفی ملزم به بررسی حقوقی هستند.[۱۲] آن‌ها استدلال می‌کنند که قبل از تدوین این ماده، برخی دولت‌ها در سطح ملی چنین سازوکاری را ایجاد کرده و قانونی‌بودن به‌کارگیری سلاح‌ها را بر اساس آن بررسی می‌کردند. لذا تعهد ذیل این ماده را در حوزه حقوق بین‌الملل عرفی برشمرده و همه کشورها را ملزم به رعایت آن می‌دانند. اما تفسیر ماده ۳۶ نشان می‌دهدکه این ماده، مشکل را به همان‌جایی که به آن تعلق دارد (یعنی دولت‌ها) سپرده است.[۱۳] چالشی که در اینجا به وجود می‌آید، سپردن تعیین شرایط لازم برای اطلاق یک وسیله به‌عنوان جنگ‌افزار به دولت‌هاست و این دولت‌ها هستند که تعیین می‌کنند جنگ‌افزار باید دارای چه شرایطی باشد. در نتیجه ممکن است از دید یک کشور، سلاح قانونی و از دید دیگری غیرقانونی ارزیابی شود.

---

11. Hans-Peter Gasser, Sylvie-So Junod, Claude Pilloudt, …, Bruno Zimmermann, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, International Committee of the Red Cross, Geneva, 1987, p. 428.

12. Blake, Dunkan & Imburgia, Joseph S., *op.cit.*, p. 159.

13. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949.

ب. سلاح‌های مشمول بررسی

مفاد ماده ۳۶ بیان می‌دارد که سلاح‌ها، ابزار و روش‌های «نوین» جنگی باید بررسی شوند. اینکه چه سلاحی جدید است، توسط دو عامل تعیین می‌شود. ابتدا با رجوع به دولتی که قصد استفاده از آن را دارد. این واقعیت که یک سلاح قبل از اینکه به کشور دیگری فروخته شود برای مدتی در یک کشور مورد استفاده بوده سبب نمی‌شود که کشور دریافت‌کننده آن را جدید به حساب نیاورد و بررسی لازم را بر اساس ماده ۳۶ انجام ندهد. دوم اینکه جدیدبودن سلاح با رجوع به تاریخی که به خدمت گرفته شده تعیین می‌شود. سلاح‌هایی که قبل از تاریخ تصویب پروتکل یکم الحاقی از سوی کشوری به خدمت گرفته شده‌اند، بر اساس ضوابط ماده ۳۶، جدید به حساب نمی‌آیند.[۱۴] به عبارتی، بررسی حقوقی مربوط به آینده است و نه گذشته. سلاح‌های موجود که تغییراتی در آن‌ها داده شده نیز مشمول بررسی حقوقی می‌شوند. البته این تغییر باید بر قدرت و توانایی سلاح تأثیر داشته باشد تا جدید به حساب بیاید و نه بر کاهش وزن آن.[۱۵] در نتیجه بر اساس عامل دوم، واژه «جدید» نباید مشخصاً در مفهوم فنی آن استنباط شود زیرا هر سلاحی می‌تواند برای دولتی که قرار است آن را بخرد، جدید به‌شمار آید.[۱۶] بدیهی است که توسعه هر نوع سلاح جدید مانند سلاح‌های خودگردان،[۱۷] روبات‌های سرباز، فناوری‌های فضایی و فضای سایبری که دارای کاربرد نظامی هستند، به طریق اولی به چنین بررسی حقوقی نیاز دارند.[۱۸] البته باید توجه داشت که هر بررسی حقوقی باید تنها به‌کارگیری سلاح، ابزار یا روش جنگی نوین در مخاصمات مسلحانه را پوشش دهد؛ صرف مالکیت آن‌ها، الزامات ماده ۳۶ را برنمی‌انگیزد.[۱۹]

علاوه بر آن، ماده ۳۶ به‌عنوان سازوکار بررسی حقوقی تسلیحات نوین، در پروتکل یکم الحاقی درج شده است و این پروتکل ناظر بر موقعیت‌های مخاصمات مسلحانه بین‌المللی است، در حالی که پروتکل دوم الحاقی که ناظر بر مخاصمات مسلحانه غیربین‌المللی است، حاوی الزامات مشابهی در مورد انجام بررسی حقوقی برای سلاح‌های جدید جهت استفاده در این نوع مخاصمات نیست. لذا ادبیات به‌کاررفته در ماده ۳۶ از لحاظ فنی نباید به‌گونه‌ای تفسیر شود که یک دولت می‌تواند از بررسی حقوقی سلاح، ابزار یا روش جنگی نوینی که تصمیم دارد در مخاصمات مسلحانه غیربین‌المللی استفاده کند، صرف‌نظر نماید زیرا بر اساس ماده ۳۵ پروتکل یکم الحاقی، به‌کارگیری

14. McClelland, Justin, "The Review of Weapons in Accordance with Article 36 of Additional Protocol I", *International Review of the Red Cross*, vol. 85, no. 850, 2003, p. 404.

15. *Ibid.*

16. Daoust, Isabelle et al., *op.cit.*, p. 352.

17. Autonomous Weapons

18. Biontino, Michael, *Lethal Autonomous Weapon Systems Expert Meeting*, Geneva, 13-16 May, 2014, p. 2.

19. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, *op.cit.*, p. 426.

سلاح‌ها صرف‌نظر از اینکه در مخاصمات مسلحانه بین‌المللی یا غیربین‌المللی به کار می‌روند، باید بتوانند اصول بنیادین مندرج در ماده مزبور را رعایت کنند.

ج. مقررات حاکم بر بررسی حقوقی

ماده ۳۶ دولت‌ها را ملزم می‌کند تا ماهیت قانونی یا غیرقانونی سلاح‌ها، ابزار یا روش‌های نوین جنگی را با توجه به مقررات پروتکل یکم الحاقی و دیگر قواعد قابل کاربرد حقوق بین‌الملل تعیین کنند. عبارت «هر قاعده دیگر بین‌المللی قابل اعمال نسبت به اعضای متعاهد»، اشاره به هر موافقت‌نامه خلع سلاحی دارد که دولت‌های موردنظر منعقد کرده باشند یا هر موافقت‌نامه دیگری که مرتبط با ممنوعیت یا محدودیت کاربرد یک سلاح یا نوع خاصی از سلاح باشد. طبیعی است که این عبارت شامل قواعد حقوق بین‌الملل عرفی نیز می‌شود.[۲۰] بدیهی است که برای جلوگیری از ابهامات یا ملاحظات بعدی مربوط به پایبندی باید به الزامات قانونی حقوق بین‌الملل بشردوستانه ازجمله ماده ۳۵ در مرحله توسعه فنی سلاح‌ها و ابزار جنگی نیز توجه شود.[۲۱] گرچه ماده ۳۶ چگونگی انجام این تعیین را مشخص نکرده، به‌صورت تلویحی پذیرش تدابیر ملی منسجم برای ارزیابی قانونی‌بودن سلاح‌های جدید را در بر دارد. در اصل، ماده ۳۶ دو وظیفه بر عهده دولت‌های عضو گذاشته است: ایجاد رویه‌های ملی برای تعیین قانونیت سلاح‌های جدید و استفاده از این رویه‌ها برای بررسی حقوقی هر سلاح جدید بر اساس حقوق بین‌الملل.[۲۲]

د. اقدامات پس از بررسی حقوقی

اگر سلاحی توسط یک دولت و پس از بررسی حقوقی، غیرقانونی شناخته شود، هیچ الزامی ذیل حقوق بین‌الملل وجود ندارد که دولت مورد نظر را ملزم به فاش‌کردن یافته‌هایش کند.[۲۳] بنا بر تعریف گزارشگر کمیته سوم از ماده ۳۶ پروتکل یکم الحاقی، تعیین قانونی‌بودن یک سلاح توسط هر دولتی که آن سلاح را به‌کار می‌گیرد، از لحاظ بین‌المللی الزام‌آور نیست.[۲۴] نتیجه بررسی باید با توجه به شرایط و مقتضیات، منجر به صدور مجوز، قانونمندکردن یا ممنوعیت به‌کارگیری یک سلاح، ابزار یا روش نوین جنگی از سوی دولت بررسی‌کننده شود.[۲۵]

20. *Ibid.*, p. 425.

21. Herbach, Jonathan David, "Into tae Caves of Steel: Precaution Cognition and Robotic Weapon Systems under the International; Law of Armed Conflict", *Amsterdam Law Forum*, VU University Amsterdam, Summer Issue, 2012, p. 19.

22. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, *op.cit.*, p 428.

23. *Ibid.*

24. *Ibid.*, p. 424.

25. *Ibid.*, p. 426.

بررسی معاهدات بین‌المللی مرتبط نشان می‌دهد مقرراتی در دیگر معاهدات بین‌المللی مربوط به تسلیحات وجود دارد که می‌تواند نقش مکمل را برای ماده ۳۶ بازی کند. این معاهدات ضمن الزام‌آورکردن بررسی حقوقی در فحوای مواد مندرج، تعهد اعضای معاهده را در انجام بررسی حقوقی به‌کارگیری سلاح‌های جدید برمی‌شمرند. ماده ۸ کنوانسیون ممنوعیت یا محدودیت استفاده از سلاح‌های متعارف خاص (تحت عنوان بررسی و اصلاحات)، یک سازوکار بازبینی پیش‌بینی کرده که هدف آن درج دسته‌بندی‌های جدید از سلاح‌های متعارف است که ذیل پروتکل‌های ضمیمه کنوانسیون قرار نگرفته‌اند. بر اساس ماده ۸، برای دولت‌های عضو کنوانسیون مزبور این امکان فراهم شده تا با پیشنهاد اصلاح در کنوانسیون یا پروتکل‌های آن یا پیشنهاد پروتکلی جدید، سلاح‌های دیگری را در زمره جنگ‌افزارهایی قرار دهند که باید ممنوعیت یا محدودیت در خصوص آن‌ها اعمال شود. در عمل، نتیجه بررسی حقوقی ذیل ماده ۳۶ پروتکل یکم الحاقی می‌تواند از سوی دولت‌ها به‌عنوان اصلاحیه و جهت اعمال ممنوعیت یا محدودیت بر سلاح موردنظر به این کنوانسیون پیشنهاد شود.[۲۶]

معاهده تجارت تسلیحات[۲۷] نیز موادی دارد که ضمانت اجرای ماده ۳۶ پروتکل یکم الحاقی محسوب می‌شود. این معاهده اعضا را ملزم می‌کند تا بر اساس اصولی معاهده را اجرا کنند. ازجمله این اصول، اصل پنجم است که به رعایت و تضمین رعایت حقوق بین‌الملل بشردوستانه، ازجمله کنوانسیون‌های ۱۹۴۹ ژنو اشاره دارد.[۲۸] علاوه بر آن در بند ۳ ماده ۶ (ممنوعیت‌ها) معاهده مزبور آمده است: « دولت متعاهد نباید اجازه انتقال تسلیحات متعارفی را که در ماده ۲ معاهده آمده بدهد، در صورتی که در زمان صدور مجوز مطلع شود که این تسلیحات ..... نقض فاحش کنوانسیون‌های ۱۹۴۹ ژنو .... یا دیگر جنایات جنگی مندرج در موافقت‌نامه‌های بین‌المللی را به‌دنبال خواهد داشت.[۲۹] ماده ۷ (۱)(b)(i) همین معاهده در خصوص صادرات و ارزیابی صادرات بیان می‌دارد: هر دولت صادرکننده، قبل از صدور مجوز صادرات ..... باید عوامل مرتبط را مدنظر قرار دهد..... ازجمله ارزیابی عوامل بالقوه‌ای که ممکن است سبب شود استفاده از سلاح موردنظر، نقض جدی حقوق بین‌الملل بشردوستانه را به‌دنبال داشته باشد.[۳۰]

26. "Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects", *International Committee of Red Cross*, Article 8, https://www.icrc.org/eng/assets/files/other/ icrc_002_0811.pdf. (last visited 11/2/2018).

27. Arms Trade Treaty

28. "United Nations Arms Trade Treaty", Principles, http://legal.un.org/avl/pdf/ha/att/att_e.pdf. p.2, (last visited 11/2/2018).

29. *Ibid*., p. 5.

30. *Ibid*.

۲. قابلیت‌های فضای سایبری: ماهیت و ویژگی

فضای سایبری، فضایی مجازی ازجمله اینترنت است که اطلاعات به‌وسیله فناوری ارتباطات در آن مبادله می‌شود. استفاده از این فضا به‌سرعت در حال گسترش است به‌گونه‌ای که فعالیت جوامع امروزه به‌شدت وابسته به آن است.[۳۱] این فضا محیطی منحصربه‌فرد با ماهیتی دوگانه است که حاوی اجزای سخت‌افزاری و نرم‌افزاری است. جنبه فیزیکی شامل انشعابات و اتصالات است که شبکه‌ها را می‌سازد و فضای مجازی شامل داده‌ها (با استفاده از سامانه رقمی و سیگنال‌های الکتریکی)، ایده‌ها و اطلاعات غیرقابل لمسی است که داده‌ها را تشکیل می‌دهند.[۳۲] در چنین فضایی است که قابلیت‌های سایبری به‌کار گرفته می‌شوند.

قابلیت‌های سایبری گاهی به شکل برنامه‌های نرم‌افزاری و آن‌هم با اهداف تخریبی به کار می‌رود که می‌تواند آثار مخربی هم‌پایه آثار سلاح‌ها در شکل فیزیکی به دنبال داشته باشد. برنامه‌های مخرب[۳۳] یا بدافزارها عموماً با قطع کارکرد معمولی رایانه یا با بازکردن یک در پشتی،[۳۴] امکاناتی را برای مهاجم فراهم می‌آورند تا بتواند رایانه مزبور را از راه دور کنترل کند[۳۵] و در مرحله بعدی از آن به‌عنوان سکویی برای عملیات‌های آتی استفاده کند.

یکی از معروف‌ترین بدافزارهای رایانه‌ای، ویروس *استاکس‌نت* است که سبب مختل‌شدن فعالیت رآکتور هسته‌ای ایران در سال ۱۳۸۹ شد. در ۲۷ خرداد سال ۱۳۸۹، شرکت تولیدکننده برنامه‌های آنتی‌ویروس در بلاروس، ایمیلی از یک مشتری ایرانی خود دریافت کرد مبنی بر اینکه رایانه وی دائم در حال خاموش و روشن‌شدن است. پیگیری این موضوع منجر به کشف یک بدافزار مرموز شد که بازرسان آن را بر اساس نام فایلی که در مجموعه کدهای ویروس مزبور یافتند، *استاکس‌نت* نامیدند. کارشناسان، *استاکس‌نت* را پیچیده‌ترین برنامه مخرب رایانه‌ای از لحاظ فناوری توصیف کردند که برای حمله هدفمند تهیه شده است. این حمله که کار عملیات مشترک امریکایی ـ اسرائیلی بود به بیش از هزار سانتریفیوژ در سایت غنی‌سازی هسته‌ای نطنز خسارت وارد و رایانه‌های بسیاری را در کشورهای متعدد آلوده کرد. سفیر روسیه در ناتو این عملیات را به مین‌هایی تشبیه کرد که می‌توانند به فاجعه‌ای جدید همانند *چرنوبیل* منجر شود.[۳۶] *استاکس‌نت*، اولین نمونه حمله شبکه رایانه‌ای بود که سبب ورود خسارت فیزیکی شد و توانست به‌عنوان سلاح سایبری

31. "Toward Stable and Effective Use of Cyberspace", *Ministry of Defence*, Japan, September 2012, p. 2.

32. Madison, David, "Geography, Territory and Sovereignty in Cyber Warfare" in Nasu, Hitoshi & McLaughlin, Robert (eds.), *New Technologies and the Law of Armed Conflict*, The Hague, Asser Press, 2014, p. 77.

33. Malicious Program

34. Back-door

35. Robin, Bradley, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", *Journal of the National Association of Administrative Law Judiciary*, vol. 31, issue 2, 2011, p. 613.

36. Lindsay, Jon R., "Stuxnet and the Limits of Cyber Warfare", *Security Studies*, vol. 22, 2013, p. 365.

عمل کند. این ویروس بیش از ۱۰۰ هزار سامانه هدف را آلوده کرد[۳۷] که بیش از نیمی از آن‌ها در قلمرو ایران بودند.[۳۸]

دیمیتری آلپروویچ،[۳۹] یکی از بنیانگذاران شرکت امنیت اطلاعاتی که رخنه به کمیته ملی حزب دموکراتیک امریکا در سال ۲۰۱۶ را بررسی کرده بود گفت: بزرگ‌ترین نگرانی من در سال ۲۰۱۸ درباره کره شمالی است. وی اظهار داشت که این کشور ممکن است حمله ویرانگری علیه بخش مالی ایالات متحده امریکا انجام دهد تا بدین طریق، اقدامی بازدارنده در قبال حمله احتمالی امریکا علیه تأسیسات هسته‌ای یا دولت این کشور انجام داده باشد. کره شمالی حملات متعدد سایبری در چند سال گذشته علیه کره جنوبی داشته است. در سال ۲۰۱۷ گروهی متشکل از هکرهای نخبه کره شمالی، باج‌افزاری[۴۰] به نام *واناکرای*[۴۱] را توسعه دادند. این بدافزار به‌سرعت شیوع پیدا کرد و سامانه‌های فناوری اطلاعات جهانی را از کار انداخت و سامانه‌های خدمات بهداشت ملی انگلستان را به‌صورت موقت مختل کرد. برخی گزارش‌ها در سال ۲۰۱۸ نشان می‌دهد که هکرهای کره شمالی، فعالیت‌های سایبری علیه برخی نهادها در کره جنوبی، ژاپن و امریکا انجام داده‌اند. آن‌ها با دسترسی به شبکه جهانی و از طریق ابزار دسترسی از راه دور، بدافزارهایی را برای پاک‌کردن داده‌ها در رایانه‌هایی نگهداری کردند تا به موقع لزوم از آن‌ها علیه اهداف خود استفاده کنند.[۴۲]

شیوع باج‌افزار *واناکرای* سبب خاموشی رایانه‌ها در بیش از ۸۰ سازمان ارائه‌دهنده خدمات بهداشتی در انگلستان شد که منجر به لغو ۲۰ هزار وقت ملاقات با پزشکان، بازگشت به شیوه قدیمی کاغذ و قلم در ۶۰۰ واحد جراحی برای انجام کارهای خود و انحراف مسیر آمبولانس‌های ۵ بیمارستان شد و در نتیجه آن‌ها نمی‌توانستند موارد اورژانسی را مدیریت کنند. این باج‌افزار به دارنده رایانه و سامانه‌های آلوده که داده‌های آن‌ها به سرقت رفته بود اطلاع می‌داد که در ازای پرداخت پول می‌توانند اطلاعات خود را پس بگیرند. آن‌ها برای جلوگیری از ردیابی انتقال پول درخواست‌شده از طریق سامانه بانکی، از پول مجازی[۴۳] برای این منظور استفاده می‌کردند. گسترش

۳۷. در خصوص آثار بدافزار *استاکس‌نت*، گزارش‌های متعددی منتشر شده که سه مورد از آن‌ها برای نمونه ذکر شد. ن.ک:
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
https://ccdcoe.org/sites/default/files/multimedia/pdf/Falco2012_StuxnetFactsReport.pdf.
https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf.

38. Mele, Stefano, "Cyber Weapons: Legal and Strategic Aspects", *Italian Institute of Strategic Studies*, Rome, 2013, p. 4.

39. Dimitri Alperovitch

۴۰. Ransomware: بدافزاری که در ازای برگرداندن اطلاعات به‌سرقت‌رفته از روی رایانه، درخواست پول می‌کند.

41. WannaCry

42. Hern, Alex, "WannaCry, Petya, NotPetya: How Ransom Ware Hit the Big Time in 2017", *The Guardian*, https://www.Theguar dian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware, (last visited 5/3/2018).

43. Virtual currency

استفاده از این نوع باج‌افزارها به چند دلیل قابل توجه بود: میزان خسارتی که وارد می‌کردند، شیوه غیرمعمول برای پایان‌دادن به فعالیت خود تحت عنوان «کلید مرگ»[۴۴] و رشد این نظریه که معماران این بدافزارها مجرمان سایبری نبوده بلکه بازیگران حمایت‌شده از سوی دولت‌ها هستند. این ویروس قادر به تکثیر خود بود و همانند بیماری‌های مسری، از یک رایانه به رایانه دیگر منتقل می‌شد و به‌محض ورود به رایانه، آن را آلوده می‌کرد. یک نوع از همین بدافزارها به نام *کانفیکر*[۴۵] تنها طی ژانویه ۲۰۰۸ حدود ۲۰ میلیون رایانه، اعم از رایانه‌های نیروی دریایی فرانسه، وزارت دفاع انگلیس و اداره پلیس منچستر را آلوده کرده بود. نوع دیگر باج‌افزار *نات‌پتیا*[۴۶] بود که حتی اگر صاحب رایانه آلوده، پولی برای آزادسازی داده‌هایش می‌پرداخت، داده‌هایش بازیافت نمی‌شد.[۴۷]

گاهی از نقاط ضعف سامانه‌ها به‌عنوان وسیله‌ای برای جاسوسی یا خرابکاری استفاده می‌شود. در آوریل سال ۲۰۱۷، یک گروه هکر به‌نام *شَدو بروکر*،[۴۸] نقطه‌ضعفی از سامانه عامل میکروسافت ویندوز منتشر کرد که از طریق آن، امکان اجرای برنامه‌هایی بر روی رایانه‌ای دیگر متصل به همان شبکه به‌صورت خودکار فراهم می‌آمد. گفته می‌شود این ضعف سامانه‌ای از آژانس امنیت ملی[۴۹] امریکا به‌سرقت رفته بود. این نقطه‌ضعف که به نام *اِترنال‌بلو*[۵۰] معروف بود، بخشی از جعبه ابزار فنون هک‌کردن آژانس مزبور بود که برای حمله به رایانه‌های مخالفان امریکا به‌کار می‌رفت. هنوز هویت گروه مزبور ناشناخته مانده اما احتمال می‌رود که به دولت روسیه وابسته باشد. همین گروه در اوت سال ۲۰۱۶ مجموعه‌ای از سلاح‌های سایبری را به حراج گذاشت که گفته می‌شود از آژانس امنیت ملی امریکا سرقت کرده بودند.[۵۱] بررسی پانزده ماهه نشان داد که *کرملین* اولین مظنون لورفتن سلاح‌های سایبری با کمک یک نفوذی در داخل آژانس امنیت ملی امریکاست. بنابر همین گزارش، سلاح‌های سایبری به‌سرقت‌رفته از امریکا، توسط هکرهایی از کره شمالی و روسیه، علیه امریکا به‌کار گرفته شد.[۵۲]

کاربرد دیگر قابلیت‌های فضای سایبری، تلاش برای ازکارانداختن توانایی‌های هسته‌ای کشور مقابل است. برای مثال، ایالات متحده امریکا این موضوع را مدنظر دارد که در زمان جنگ با کره شمالی بتواند از ابزار سایبری برای کنترل موشک‌های هسته‌ای کره شمالی استفاده کند. مطمئناً

44. Kill switch
45. Conficker
46. NotPetya
47. Hern, Alex, *op.cit*.
48. Shadow Broker
49. National Security Agency
50. Eternalblue
51. Hern, Alex, *op.cit*.
52. Ballesteros, Carlos, "Russians Stole NSA Cyber Weapons and Are Using Them against US", *Newsweek*, http://www.newsweek.com/russia-nsa-cyber-weap ons-hacking-710053, 2017, (last visited 5/3/2018).

دیگر دولت‌ها نیز همین محاسبات را درباره امریکا مدنظر دارند.[۵۳] بنابر مطالعه *چاتم هاوس*،[۵۴] مؤسسه سلطنتی امور بین‌الملل، تسلیحات هسته‌ای در قبال سلاح‌های سایبری آسیب‌پذیرتر بوده و ممکن است منجر به پرتاب تصادفی موشک هسته‌ای شود. این مطالعه می‌گوید: سامانه‌های هسته‌ای امروزه در دوره قبل از عصر دیجیتال توسعه یافته‌اند؛ لذا به آسیب‌پذیری آن‌ها در مقابل سلاح‌های سایبری توجه اندکی شده است. طی دهه‌های اخیر، معرفی فناوری پیچیده سایبری در سامانه‌های تسلیحات هسته‌ای مانند فرماندهی، کنترل و تسهیلات ارتباطی، آن‌ها را در مقابل آسیب‌پذیری‌های بی‌شماری قرار داده است. ازکارانداختن سانتریفیوژهای تأسیسات هسته‌ای نطنز از طریق ویروس *استاکس‌نت*، ازکارانداختن آزمایش‌های موشکی کره شمالی به‌وسیله نفوذ در سامانه‌ها توسط امریکا و دسترسی اسرائیل به داده‌های یک رایانه مستقل و بدون ارتباط با شبکه اینترنت و از طریق صدای پنکه خنک‌کننده، نمونه‌هایی از کاربرد قابلیت‌های سایبری است.[۵۵]

بدافزار *شامون*،[۵۶] نمونه دیگری از سلاح‌های سایبری است که در سال ۲۰۱۲ موفق شد به حدود ۳۰ هزار رایانه شرکت نفتی آرامکو عربستان سعودی حمله و فایل‌های آن‌ها را تخریب کند. این بدافزار با حذف بخشی از حافظه اصلی[۵۷] رایانه‌ها که برای آغاز به کار سامانه لازم بود، امکان روشن‌شدن مجدد آن‌ها را با مشکل مواجه کرده بود.[۵۸] نمونه‌های فراوانی از این نوع قابلیت‌های سایبری وجود دارد که می‌توان به بمب‌های منطقی،[۵۹] اسب‌های *تروژان*،[۶۰] *رئوس تروژان*[۶۱] و *رت*[۶۲] اشاره کرد.

علاوه بر نمونه‌های یادشده که تحت عنوان تسلیحات سایبری از آن‌ها یاد می‌شود، امروزه

53. Rachman, Gideon, "Nuclear Weapons Are A Risky Defence against Cyber Attacks", *Financial Times*, accessed on 5 March 2018, https://www.ft.com/ content/d2241b68-fc31-11e7-9b32-d7d59aace167, (last visited 5/3/2018).

54. Chatam House

55. Szondy, David, "Cyber Attacks Could Lead to Use of Nuclear Weapons", https://newatlas.com/cyberattack-launch-nuclear-weapons/52924/, (last visited 5/3/2018).

56. Shamoon

57. Master Boot Record

58. Mele, Stefano, *op.cit.*, p. 12.

۵۹. Logic bomb: بمب‌های منطقی برنامه‌های بسیار پیشرفته‌ای هستند که آثار مخرب آن‌ها با حوادث خاص در یک زمان ازقبل‌تعیین‌شده آغاز می‌شود. زمانی که این بمب شروع به کار کند، با ورود خسارات شدید به رایانه آلوده، آن را غیرقابل استفاده کرده و اطلاعات خاصی را از روی آن حذف می‌کند.

۶۰. Trojan Horses: نوعی نرم‌افزار مخرب، با فریب‌دادن رایانه‌های هدف به آن‌ها می‌قبولاند که برنامه‌های مخرب دارای کارکرد سودمند هستند. اسب‌های *تروآ* در مقابل به کاربر خود اجازه می‌دهد به رایانه آلوده دست پیدا کرده و از آن به‌عنوان منبعی برای حملات قطع ارائه خدمات استفاده کند.

۶۱. ZeuS Trojan: این برنامه نرم‌افزاری در عقبه سامانه رایانه‌ای عمل کرده و از تراکنش‌های بانکی جلوگیری می‌کند.

۶۲. Poison Ivy RAT: نرم‌افزاری است که به کاربر خود اجازه می‌دهد به یک سامانه رایانه‌ای همانند کاربر اصلی آن دسترسی داشته باشد. این بدافزار همانند تروآ عمل می‌کند اما دسترسی وسیع‌تری به رایانه هدف از راه دور دارد.

سامانه‌های تسلیحاتی تا اندازه زیادی به نرم‌افزارهای پیچیده و متصل به هم برای عملیات خود وابسته‌اند. قابلیت‌های سایبری، بسیاری از امکانات پیشرفته مانند حملات الکترونیکی، ترکیب حس‌گرها و ارتباطات از راه دور را فراهم می‌آورند که به نیروهای نظامی یک کشور علیه طرف دیگر برتری می‌دهند. برای مثال، ستون فقرات ارتباطات جهانی ارتش امریکا متشکل از ۷ میلیون وسیله رایانه‌ای بر روی هزاران شبکه در کشورهای مختلف است. در یک مطالعه برآورد شده است که ۹۵ درصد ارتباطات راه دور وزارت دفاع امریکا از طریق شبکه عمومی سایبری انجام می‌گیرد.[۶۳] در همین راستا و برای به‌دست‌آوردن برتری در این حوزه، ناتو تصمیم دارد قابلیت‌های جنگ سایبری کشورهای عضو را در زمره گزینه‌های نظامی قرار داده و اعضا معتقدند به همان اندازه که در عرصه جنگ‌های زمینی، هوایی و دریایی کارآمد هستند، به دلیل تهدیداتی که با آن روبه‌رو هستند باید توانایی‌های خود را برای مقابله با این تهدیدات افزایش دهند..[۶۴] در نتیجه، چنین رویکردهایی، به‌کارگیری این قبیل قابلیت‌ها به‌عنوان سلاح را افزایش داده و ضرورت بررسی امکان اطلاق سلاح به آن‌ها را دوچندان می‌نماید.

۳. امکان اطلاق سلاح به قابلیت‌های سایبری

وقتی فناوری‌های حوزه فضای سایبری ارتقا می‌یابد، ارتش‌های مدرن به کسب کاربردهای نوآورانه این فناوری‌ها روی می‌آورند. دولت‌ها برای پرهیز از برانگیخته‌شدن مسئولیت‌شان در قبال استفاده از جنگ‌افزارهای غیرقانونی باید نسبت به قانونی‌بودن تسلیحات اطمینان حاصل کنند.[۶۵] بدیهی است که قبل از هر بررسی حقوقی، ابتدا باید اثبات شود که شئ تحت بررسی سلاح است. این رویکرد در قبال قابلیت‌های سایبری که امکان دارد کاربرد آن‌ها سبب ورود خسارت یا جراحت شود نیز باید به کار گرفته شود.

تعریف سلاح سایبری در توانایی نیروهای نظامی برای انجام عملیات سایبری بسیار مهم است زیرا آثار حقوقی و سیاسی فراوانی برای دولت‌ها دارد. تعریف اشتباه یا مضیق از سلاح سایبری می‌تواند منجر به عدم پایبندی به معیارهای حقوق بین‌الملل شود. اگر تعریف موسع باشد می‌تواند ابزار و فنون جاسوسی را در برگرفته و در عملیات حیاتی برای امنیت ملی اختلال ایجاد کند. از سوی دیگر، حقوق بین‌الملل، استفاده از نیروی نظامی علیه غیرنظامیان و اموال آن‌ها را ممنوع کرده است. اگر هر قابلیت سایبری به‌عنوان سلاح تعریف شود، استفاده از هریک از آن‌ها می‌تواند

63. Gervais, Michael, "Cyber Attacks and the Laws of War", *Berkley Journal of International Law*, vol. 30, issue 2, 2012, p. 568.

64. Ranger, Steve, "NATO Just Added Cyber Weapons to Its Armoury", http://www.zdnet.com/article/nato-just-added-cyber-weapons-to-its-armoury/, 2017 (last visited 5/3/2018).

65. Blake, Dunkan & Imburgia, Joseph S., *op.cit.*, p. 163.

حمله محسوب شود. در آن صورت، ماهیت غیرنظامی اکثر قابلیت‌های فضای سایبری با محدودیت و ممنوعیت روبه‌رو خواهد شد.[۶۶]

تا به امروز، اجماعی در خصوص اینکه سلاح سایبری چیست حاصل نشده است. فقدان توافق در مورد تعریف سلاح سایبری، ناشی از دو عامل است. عامل اول، فقدان تعریف عام از سلاح‌های جنبشی[۶۷] در راهبردهای نظامی و مجموعه قواعد حقوقی است. دومین عامل، کاربرد واژگان و مفاهیم برگرفته از سلاح‌های متعارف یا سلاح‌های کشتار جمعی برای سلاح سایبری است. وقتی از این مفاهیم در فضای سایبری استفاده می‌شود، در بسیاری موارد کارآیی خود را از دست داده و واژه‌های به‌کاررفته در پارادایم‌های حقوقی مانند جنگ، سلاح و تخریب، حمله یا بازدارندگی در فضای سایبری، مفاهیم متفاوتی ارائه می‌دهند. به‌عنوان مثال، عبارت جنگ سایبری برای توصیف استفاده از فضای مجازی جهت هدایت عملیات سایبری، اعم از اقدامات پشتیبانی تا حملات نظامی خشونت‌آمیز را در بر می‌گیرد.[۶۸]

برخی کارشناسان فعال در تهیه پیش‌نویس ماده ۳۶ معتقد بودند که تعریف واژه سلاح باید صریح باشد؛ واژه سلاح باید به هر قابلیتی اعم از تهاجمی یا تدافعی که می‌تواند به‌عنوان سلاح علیه هدف نظامی دشمن به‌کار گرفته شود، اشاره ضمنی داشته باشد. باید توجه داشت که در حوزه سایبری و در این مقاله، «قابلیت»، واژه‌ای کلیدی است که قابلیت‌های غیرمهلک و غیرخشونت‌آمیز فضای سایبری را در بر می‌گیرد. اگر به‌کارگیری چنین قابلیت‌هایی آثار مستقیمی بر توانایی نیروی نظامی یک طرف درگیر در عملیات داشته باشد (مانند ورود خسارت به اهداف نظامی یا جراحت نیروهای نظامی)، می‌تواند در زمره سلاح قرار گرفته و باید آن را قبل از به‌کارگیری، از لحاظ حقوقی بررسی کرد.[۶۹]

نمی‌توان بررسی حقوقی سلاح یا ابزار جنگی را در خلأ انجام داد. تعیین قانونیت سلاح صرفاً به قصد کاربرد آن بستگی ندارد، بلکه به شرایط کاربرد آن نیز بستگی دارد. علاوه بر آن ممکن است کاربرد سلاح در شرایطی معین، از ارزیابی حقوقی ماده ۳۶ سربلند بیرون بیاید، اما در شرایط دیگر خیر. به همین دلیل است که در ماده مزبور از عبارت «در برخی یا تمامی شرایط»[۷۰] برای همین منظور استفاده شده است.

در این راستا از یک منظر برای داشتن تعریفی مناسب از سلاح سایبری می‌توان بر سه عنصر

66. Brown, Gary D. and Metcalf, Andrew O., "Easier Said Than Done: Legal Review of Cyber Weapons", *Journal of National Security Law and Po*licy, vol. 7, no. 1, 2014, p. 129.

67. Kinetic

68. Devai, Dora, "Proliferation of Offensive Cyber Weapons, Strategic Implications and Non-Proliferation Assumptions", *AARMS*, vol. 15, no. 1, 2016, p. 62.

69. Blake, Dunkan & Imburgia, Joseph S., *op.cit.*, p.172.

70. In some or all circumstances

مهم متمرکز شد: ۱ـ بستر: سلاح سایبری باید در چارچوب فعلی از جنگ سایبری به‌کار گرفته شود. می‌توان این مفهوم را درگیری میان بازیگران ملی یا غیرملی توصیف کرد که مشخصه آن، استفاده از سامانه‌های اطلاعاتی فناورانه با هدف به‌دست‌آوردن، حفظ یا دفاع از شرایط راهبردی، عملیاتی یا مزیت تاکتیکی است؛ ۲ـ قصد: ورود خسارت فیزیکی (حتی غیرمستقیم) به تجهیزات یا افراد یا خرابکاری یا ورود خسارت مستقیم به سامانه‌های اطلاعاتی هدف با استفاده از سلاح سایبری است و ۳ـ وسیله یا ابزار: حمله از طریق کاربرد سامانه‌های اطلاعاتی فناورانه ازجمله اینترنت انجام می‌شود. به نظر می‌آید، اینها تنها عناصر مورد استفاده برای تعیین مجموعه‌ای از دستورهای رایانه‌ای به‌عنوان سلاح است.[۷۱] با استفاده از عناصر فوق، در زیر به برخی تعاریف اشاره می‌شود.

یکی از محققین، سلاح سایبری این طور توصیف می‌کند: «بخشی از تجهیزات، یک وسیله یا هر مجموعه‌ای از دستورهای رایانه‌ای مورد استفاده در درگیری میان بازیگران ملی یا غیرملی، با هدف ورود خسارت فیزیکی حتی به‌صورت غیرمستقیم، خسارت فیزیکی به تجهیزات یا افراد یا خرابکاری یا خسارت مستقیم به سامانه‌های اطلاعاتی هدف حساس».[۷۲] در مطالعات سازمان همکاری اقتصادی و توسعه، سلاح سایبری شامل دسترسی غیرمجاز به سامانه‌ها (هک‌کردن)، ویروس‌ها، تروژان‌ها، قطع ارائه خدمات، قطع خدمات توزیعی با استفاده از شبکه تعریف شده است. روسیه در این خصوص از عبارت سلاح اطلاعاتی استفاده کرده و آن را این طور توصیف می‌کند: فناوری اطلاعات، ابزار یا روش‌های مورد استفاده برای جنگ اطلاعاتی.[۷۳]

دستورالعمل *تالین* به‌عنوان تنها مجموعه مقررات موجود درباره جنگ سایبری در سطح بین‌المللی، در قاعده ۴۱ (حاوی تعریف ابزار و روش‌های جنگ سایبری)، ابزار جنگ سایبری را شامل سلاح‌های سایبری و سامانه‌های همراه آن‌ها می‌داند. دستورالعمل مزبور، تسلیحات سایبری را ابزار جنگی می‌داند که با هدف ورود صدمه یا مرگ افراد یا ورود خسارت یا تخریب اموال طراحی یا استفاده می‌شوند. وجود چنین ویژگی برای قابلیت‌های سایبری لازم است تا بتوان با استناد به آثار آن، حمله سایبری را عملیات نظامی به حساب آورد. در نتیجه، جنگ‌افزار سایبری شامل هر وسیله، مواد، ابزار، سازوکار، تجهیزات یا نرم‌افزار سایبری می‌شود که برای هدایت حمله سایبری طراحی شده یا به‌کار می‌رود.[۷۴] البته باید میان رایانه‌ای که ابزار جنگی محسوب می‌شود و زیرساخت سایبری (اینترنت) که رایانه‌ها از طریق آن به یکدیگر متصل می‌شوند، تفاوت قائل شد. زیرساخت

71. Mele, Stefano, *op.cit.*, p. 10.

72. *Ibid*.

73. Ebner, Nike, "Cyber Space, Cyber Attack and Cyber Weapons", *Institute for Peace Research and Security Policy*, University of Hamburg, 2015, p. 6.

74. *Tallin Manual on the International Law Applicable to Cyber Warfare*, NATO Cooperative Defense Centre of Excellence, Cambridge University Press, Cambridge, 2013, p. 118.

سایبری ابزار جنگی نیست زیرا برای اینکه یک شئ، سلاح محسوب شود باید در کنترل یکی از طرف‌های درگیری باشد تا ابزار جنگیدن به حساب بیاید. ضمناً باید توجه داشت همان گونه که از جنگ سایبری با عبارت‌های متفاوتی مانند انقلاب در امور نظامی، نسل چهارم جنگیدن، جنگ الکترونیکی، جنگ اطلاعاتی، جنگ شبکه‌محور، جنگ سایبری و جنگ شبکه‌ای[۷۵] یاد می‌شود، برای ابزار قابل کاربرد در این حوزه نیز الفاظ مختلفی مانند سلاح سایبری، سلاح رایانه‌ای یا سلاح دیجیتال استفاده می‌شود.

در خلال مباحث کارشناسان تدوین‌کننده دستورالعمل *تالین*، موضوعی که بالا گرفت، مربوط به رفتار با داده‌ها و به‌ویژه در خصوص این موضوع بود که آیا داده‌ها واجد شرایط یک شئ[۷۶] در حقوق بین‌الملل هستند. اگر چنین باشد، ابزار سایبری که سبب تخریب یا تغییر داده‌ها شود، سلاح محسوب شده و سلاحی که علیه داده‌های غیرنظامی و دیگر داده‌های مورد حمایت به‌کار گرفته شود، غیرقانونی است. البته اگر یک ابزار سایبری در حمله به داده‌ها به‌طور مستقیم منجر به جراحت افراد (مانند تغییر داده‌ها در تصفیه‌خانه آب که منجر به بیماری شود) یا خسارت به اشیاء (مانند دستکاری در داده‌های ترافیک هوایی منجر به سقوط هواپیماها) شود، سلاح به حساب می‌آید. اما آیا ابزاری که داده‌ها را هدف قرار می‌دهد، صرف‌نظر از پیامدهای فیزیکی یا عملکردی، سلاح محسوب می‌شود؟ اکثریت کارشناسان گروه بین‌المللی، مایل به تسری مفهوم شئ به داده‌ها نبودند. آن‌ها تفسیر کمیته بین‌المللی صلیب سرخ درباره ماده ۵۲ (ممنوعیت حمله به اشیاء غیرنظامی) را متقاعدکننده یافتند. طبق این تفسیر، در زبان انگلیسی و فرانسه، واژه شئ به معنی چیزی است که قابل رؤیت و لمس باشد. آن‌ها نتیجه گرفتند که داده‌ها نه قابل لمس هستند و نه قابل رؤیت؛ لذا شئ نبوده و نمی‌توانند از حمایت‌های اشیاء خاص ذیل حقوق بین‌الملل بشردوستانه بهره‌مند شوند.[۷۷] البته باید توجه داشت که گاهی تخریب اطلاعات می‌تواند آثاری را به وجود آورد که زیان‌آورتر از حمله جنبشی است. برای مثال، تغییر در داده‌های سامانه مالی که منجر به بی‌اعتمادی به نظام اقتصادی کشور شود، زیان‌آورتر از حمله جنبشی به بانک است. این امر، دشواری در تمایز هنجاری میان ضرر وارده به اشیاء فیزیکی و وارده به داده‌ها در جوامع متکی به فضای سایبری را ثابت می‌کند.

باید خاطرنشان کرد که گرچه فضای سایبری محیط فیزیکی نیست، اقدامات در این فضا می‌تواند آثار فیزیکی به دنبال داشته باشد و بر افراد، اماکن و اموال در دنیای فیزیکی اثرگذار باشد.[۷۸]

75. Brose, Robert, "Cyber War, Net War and the Future of Cyber Defence", *Office of the Director of National Intelligence*, United States, 2015, p. 4.

76. Object

77. Schmitt, Michael N., "Rewired Warfare: Rethinking the Law of Cyber Attack", *International Review of the Red Cross*, vol. 96, no. 893, 2014, p. 200.

78. Madison, David, *op.cit.*, p. 76.

برای اینکه یک ابزار در مفهوم کنونی در دسته‌بندی جنگ‌افزارها قرار گیرد باید با هدف ورود خسارت به اموال یا ورود جراحت به افراد، در بستر مخاصمه مسلحانه طراحی شده یا به کار گرفته شود.[۷۹] برخی محققین، پیامدهای خشونت‌آمیز در زمینه به‌کارگیری سلاح سایبری را مهم دانسته و چنین پیامدهایی را مرگ، جراحت، خسارت یا تخریب توصیف می‌کنند.[۸۰]

در اسناد بین‌المللی نیز به آثار فیزیکی این نوع تسلیحات نیز اشاره شده است. برای مثال، قطعنامه‌های ۱۳۶۸ شورای امنیت سازمان ملل متحد مورخ ۱۲ سپتامبر ۲۰۰۱ و ۱۳۷۳ مورخ ۲۸ سپتامبر ۲۰۰۱ که متعاقب حمله ۱۱ سپتامبر به برج‌های دوقلوی *نیویورک* تصویب شدند، مفهوم مبهم سلاح نامحسوس[۸۱] را به جامعه بین‌المللی معرفی کردند. سلاح نامحسوس به هر وسیله یا سازوکاری اطلاق می‌شود که به‌عنوان سلاح تعریف نشده است، اما با سوءاستفاده از آن می‌توان سبب تلفات انسانی و تخریب تجهیزات و فناوری (ازجمله استفاده مخرب از فناوری اطلاعاتی و ارتباطاتی) شد.[۸۲] به نظر می‌آید گسترش دامنه این تعریف با استناد به پیامدهای خشونت‌آمیز به‌عنوان مشخصه‌ای برای سلاح‌های سایبری، منطقی و اجتناب‌ناپذیر باشد. می‌توان سلاح سایبری را با سلاح معمولی مقایسه کرد. در سلاح معمولی، فرد با کشیدن ماشه، گلوله را رها می‌کند و در ابزار سایبری، فرد با زدن کلید، به‌طور مثال بدافزار را در شبکه رها می‌کند. از لحاظ کیفی، این دو مفهوم با یکدیگر متفاوت نیستند. در نتیجه، جنگ‌افزار سایبری می‌تواند هر تجهیزات رایانه‌ای یا ابزار رایانه‌ای باشد که طراحی شده تا سبب مرگ، جراحت، خسارت یا تخریب در مخاصمه مسلحانه شود. اما اگر ابزار سایبری تنها برای رنجش و ایذا طراحی شده باشد، جنگ‌افزار سایبری به‌حساب نمی‌آید. حال اگر چنین ابزاری جنگ‌افزار به حساب آید، حقوق تسلیحات در مورد آن به کار می‌رود.[۸۳]

چنانچه مشاهده می‌شود، اکثر محققین بر آثار فیزیکی یک قابلیت برای تلقی آن به‌عنوان سلاح، متمرکزند، حال آنکه آثار به‌کارگیری بسیاری از قابلیت‌های سایبری در حوزه مجازی رخ می‌دهد، مانند حذف داده‌های مهم از روی رایانه یا ازکارانداختن سامانه عامل رایانه که کارکرد رایانه به آن بستگی دارد. در نتیجه شاید بتوان یکی از چالش‌های بررسی حقوقی قابلیت‌های

79. Boothby, William H., "Where Do Cyber Hostilities Fit in the International Law Maze?" in Nasu, Hitoshi & McLaughlin, Robert (eds.), *New Technologies and the Law of Armed Conflict*, The Hague, ASSER Press, 2014, p. 67.

80. Schmitt Michael, N., "Cyber Operations and the Jus in Bello: Key Issues", in Pedrozo R.A., Wollschlaeger D.P. (eds.) *International Law and the Changing Character of War*, Newport, US Naval War College International Law Studies, vol. 87, Naval War College, 2011, p. 95.

81. Intangible Weapon

82. Streltsov, Anatoly, "Key Trends of International Law Relating to the Conflicts in Cyber Space", in Greppi, Edoardo (ed.) *Conduct of Hostilities: The Practice, The Law and The Future*, International Institute of Humanitarian Law, 2015, pp. 191 & 192.

83. Boothby, William H., *op.cit.*, p. 67.

سایبری به‌عنوان سلاح را فقدان اجماع بین‌المللی در خصوص آثار مجازی به‌کارگیری این نوع سلاح‌ها دانست.

۴. بررسی حقوقی تسلیحات سایبری

در مبحث قبلی این نتیجه به دست آمد که کاربرد برخی قابلیت‌های سایبریِ دارای آثار مخرب فیزیکی را می‌توان ذیل تسلیحات، ابزار یا روش‌های جنگی قرار داد و اگر قابلیت‌های فضای سایبری دارای همان آثاری محسوب شود که سلاح‌های متعارف در جهان واقعی دارند (ازجمله انهدام، آسیب، ضرر و زیان، جراحت و مرگ)، همان قواعد حاکم بر سلاح‌های متعارف بر فضای سایبری نیز حاکم خواهد بود. از سوی دیگر می‌توان قانونیت یا ممنوعیت یا حداقل محدودیت کاربرد وسایل و شیوه‌های نبرد در فضای سایبری را بر اساس اصول بنیادین حقوق بشردوستانه ارزیابی کرد و در نتیجه اگر استفاده از آن‌ها با اصول مزبور منطبق باشد می‌توان به مشروعیت یا محدودیت آن‌ها رسید و اگر مغایر باشد، عدم قانونیت یا ممنوعیت آن‌ها را محرز دانست.[۸۴]

در تعیین قانونیت سلاح جدید، دولت بررسی‌کننده باید اصول حقوق بین‌الملل بشردوستانه و قواعد موجود حقوق بین‌الملل (قراردادی و عرفی) را که به آن متعاهد است به‌کار گیرد. علاوه بر آن، ماده ۳۶ پروتکل یکم الحاقی، به همان پروتکل و دیگر قواعد قابل کاربرد حقوق بین‌الملل در مورد دولت بررسی‌کننده نیز رجوع می‌کند. قواعد مرتبط شامل این موارد است: «قواعد عام حقوق بین‌الملل بشردوستانه» حاکم بر تمامی سلاح‌ها، ابزار و روش‌های جنگی، «قواعد خاص حقوق بین‌الملل بشردوستانه» و حقوق بین‌الملل منع‌کننده کاربرد سلاح‌ها و ابزار خاص جنگی، یا محدودکننده روش‌های جنگی که از طریق آن‌ها سلاح تحت بررسی به کار می‌رود.[۸۵]

اولین قدم در بررسی حقوقی، پاسخ به این پرسش است که آیا به‌کارگیری سلاح یا ابزار خاص جنگی تحت بررسی، توسط معاهده یا حقوق بین‌الملل عرفی که دولت بررسی‌کننده به آن متعاهد است،[۸۶] ممنوع یا محدود شده است (مانند ممنوعیت گلوله‌های انفجاری یا آتش‌زای زیر ۴۰۰ گرم توسط بیانیه *سنت‌پترزبورگ* یا ممنوعیت سلاح‌های شیمیایی و لیزری توسط کنوانسیون‌های ذی‌ربط)؟ همان گونه که قبلاً نیز ذکر شد، هیچ‌گونه معاهده یا قاعده حقوق بین‌الملل عرفی وجود ندارد که به‌طور مستقیم، استفاده از قابلیت‌های سایبری را محدود یا ممنوع کرده باشد. اما در بسیاری موارد می‌توان با استفاده از اصول بنیادین حقوق بین‌الملل بشردوستانه و قواعد و مقررات موجود در این زمینه و با تفسیر آن‌ها، به نتایج موردنظر در بررسی حقوقی سلاح‌های سایبری رسید.

---

۸۴. ضیایی بیگدلی، محمدرضا؛ *حقوق بین‌الملل بشردوستانه*، چاپ سوم، گنج دانش، ۱۳۹۲، ص ۲۶۶.

85. A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977, *op.cit.*, p. 10.

۸۶. برای اطلاع از فهرست چنین معاهداتی، ن.ک: منبع شماره ۷۴، صص ۱۲ و ۱۳.

در صورت فقدان چنین ممنوعیتی، مرحله بعد، پاسخ به این پرسش است که آیا سلاح تحت بررسی، با قواعد عام موجود در پروتکل یکم الحاقی و همچنین معاهدات دیگر و حقوق بین‌الملل عرفی که دولت بررسی‌کننده به آن‌ها متعهد است سازگاری دارد؟ در این خصوص باید شماری از ممنوعیت‌ها یا محدودیت‌های عام قراردادی و عرفی درباره سلاح‌ها، ابزار یا روش‌های جنگی بررسی شود. بنابر ماده ۳۶ پروتکل یکم الحاقی، دولت متعاهد به این پروتکل باید به قواعد زیر در زمان بررسی توجه داشته باشد: ممنوعیت به‌کارگیری سلاح‌هایی که سبب ورود جراحت غیرضرور یا رنج بیهوده می‌شوند (ماده (۲)۳۵)؛ ممنوعیت به‌کارگیری سلاح‌هایی که سبب ورود خسارت گسترده، درازمدت و شدید به محیط‌زیست طبیعی می‌شوند (ماده (۳)۳۵ و ۵۵)؛ ممنوعیت به‌کارگیری سلاح‌هایی که به‌صورت غیرتفکیکی عمل می‌کنند (ماده (c) و (b)(۴)۵۱) و ممنوعیت به‌کارگیری روش‌های جنگی که چندین هدف متفاوت نظامی در مناطق غیرنظامی را هدف قرار می‌دهند ((a)(۵)۵۱).[۸۷]

علی‌رغم جدیدبودن این فناوری، محدودیت‌های حقوقی حاکم بر ابزار و روش‌های جنگی (در پروتکل یکم الحاقی، معاهدات خلع سلاح و حقوق بین‌الملل عرفی) نسبت به قابلیت‌های فضای سایبری نیز قابل اعمال است،[۸۸] اما بی‌شک اعمال چنین قواعدی در خصوص تسلیحات سایبری با چالش‌هایی روبه‌روست که قبلاً برخی از آن‌ها ذکر شد و در زیر به دیگر موارد اشاره می‌شود.

ممکن است قابلیت سایبری به داده‌های موجود در رایانه هدف حمله، خسارت وارد کند. در اینجا تعیین شئ‌بودن داده‌ها بسیار مهم است زیرا در صورت شئ بودن داده‌ها، قابلیتی که به آن‌ها خسارت وارد کرده، سلاح محسوب می‌شود. از نظر اکثریت کارشناسانی که در فرآیند تدوین دستورالعمل *تالین* مشارکت داشته‌اند، همه داده‌ها با یکدیگر برابر نیستند. عملیات سایبری که مقدار معینی از داده‌ها را در رایانه هدف تغییر می‌دهد، ممکن است کمتر از حمله بر اساس ماده ۴۹ پروتکل یکم الحاقی محسوب شود زیرا داده‌هایی که از بین رفته‌اند، تأثیری بر کارکرد مناسب سامانه عامل رایانه مورد نظر نداشته‌اند. برخلاف آن، ممکن است عملیات سایبری مشابه که حجم کمتری از داده‌های حساس برای کارکرد مناسب سامانه عامل رایانه را تخریب کند، حمله به‌حساب بیاید. طبق این تحلیل، زمانی داده‌های رایانه هدف، شئ تلقی می‌شود که سامانه کنترل یا بخش‌هایی از آن در نتیجه این عملیات، نیاز به تعویض داشته باشد. شاید بهترین راه این باشد که

87. *Ibid.*, pp. 15 & 16.

88. Turns, David, "Cyber War and the Concept of Attack in International Humanitarian Law", in Saxon, Dan (ed.) *International Humanitarian Law and the Changing Technology of War*, Boston, Martinus Nijhoff Publishers, 2013, p. 220.

کارکرد سامانه عامل رایانه هدف،[۸۹] شئ تلقی شود.[۹۰] چالشی که در اینجا بروز می‌کند این است که ممکن است تخریب برخی داده‌ها بر سامانه عامل رایانه تأثیری نداشته باشد، اما ارزش آن داده‌ها می‌تواند بیش از سامانه عامل رایانه باشد، مانند آنکه داده‌های تخریب‌شده حاوی اطلاعات مربوط به مختصات جغرافیایی استقرار موشک‌های بالستیک کشور دشمن است که در زمان حمله، رصدکردن آن سایت‌ها از لحاظ نظامی بسیار ضروری می‌نماید. *اشمیت* در خصوص اهمیت داده‌های موجود بر روی رایانه‌ها (به‌جز سامانه عامل) در یکی از کلاس‌های درس خود می‌گوید: برای من مهم نیست اگر رایانه‌ام از کار بیفتد یا از بین برود اما اگر مقاله‌ام که با زحمت زیاد تهیه کرده‌ام و در رایانه نگهداری می‌کنم آسیب ببیند، (به شوخی) خودکشی می‌کنم.[۹۱]

ماهیت اینترنت چالش‌برانگیز است زیرا کاربردی دوگانه دارد. عرضه‌کنندگان خدمات اینترنتی غیرنظامی به شبکه‌های بر خط خدمات‌رسانی می‌کنند که در عین حال، اهداف ارتباطاتی نیروهای نظامی دشمن را نیز تأمین می‌کنند. در نتیجه، فرمانده باید برای حمله محدود به بخشی از شبکه که مورد استفاده ارتش دشمن است، اقداماتی معقول اتخاذ کند. اگر این فرمانده به‌صورت تصادفی یک ویروس رایانه‌ای را از طریق شبکه‌ها پخش کند که در نتیجه آن کارکردهای غیرنظامی حیاتی مانند بانکداری، مراقبت‌های پزشکی یا انرژی برق تحت تأثیر قرار گیرند، اصل تفکیک نقض شده است.[۹۲] علاوه بر آن، به دلیل وجود اجماع ضعیف در خصوص چیستی سلاح سایبری، به‌کاربردن این اصل دشوار است.[۹۳] برای مثال، *استاکس‌نت* ازجمله بدافزارهایی است که به‌صورت غیرتفکیکی عمل نموده و رایانه‌های نظامی و غیرنظامی را آلوده کرده بود.[۹۴]

همان گونه که در مبحث قابلیت‌های فضای سایبری اشاره شد، بسیاری از سلاح‌های سایبری توسط گروه‌ها، افراد (هکر) و شرکت‌ها تولید می‌شوند یا به سرقت می‌روند. هر کسی می‌تواند چنین سلاح‌هایی را توسعه و انتقال داده، یا توزیع و کسب کند و مالک شود.[۹۵] آیا این بازیگران همانند دولت‌ها موظف به بررسی حقوقی سلاح‌های سایبری قبل از به‌کارگیری آن هستند؟ آیا سرقت این

۸۹. با نصب مجدد سامانه عامل می‌توان کارکرد آن را به حالت اولیه برگرداند. با این ترتیب، آیا ملزومات ورود خسارت و اطلاق حمله به آن حاصل شده است؟ کارشناسان در این خصوص به دو دسته تقسیم شده بودند.

90. Boothby, William H., *op.cit.*, p. 61.

91. Schmitt, Michael N., "Cyber Operations and International Humanitarian Law: Faultiness and Vectors", *HLS Program on International Law and Armed Conflict*, http://www.youtube.com/ watch?v=zwwrvamsot4, 2015, (last visited 6/3/2018).

92. West, Dondi S., "A Survey and Examination of the Adequacy of the Laws Related to Cyber Warfare", *Defence Conference*, July 30th -August 1st 2010, Las Vegas, p. 14.

93. Hughes, Rex, "A Treaty for Cyberspace", *The Royal Institute of International Affairs*, vol. 86, no. 2, 2010, pp. 538 & 539.

94. Brown, Gary D. and Metcalf, Andrew O., *op.cit.*, p. 131.

95. Denning, Dorothy, "Reflections on Cyber Weapons Controls", *Computer Security Journal*, vol. 16, no. 4, 2000, p. 43.

نوع تسلیحات، در زمره کسب[۹۶] آن‌ها به‌حساب می‌آید؟ زیرا تنها واژه نزدیک به سرقت در ماده ۳۶، واژه کسب است.

این مبحث، شش چالش را احصا کرد که به‌طور خلاصه عبارت‌اند از: فقدان قواعد منع‌کننده یا محدودکننده کاربرد قابلیت‌های سایبری، سپردن تعریف سلاح به دولت‌های عضو پروتکل، تعریف جدیدبودن سلاح‌ها، اطلاق شئ‌بودن داده‌های مورد حمله قابلیت‌های سایبری، دوگانگی اینترنت و الزام افراد یا گروه‌ها و شرکت‌های تولیدکننده سلاح‌ها به بررسی حقوقی قبل از به‌کارگیری آن‌ها.

نتیجه

فضای سایبری یکی از فناوری‌هایی است که به‌سرعت در حال پیشرفت است و قابلیت‌های آن در حوزه نظامی کاربردهای فراوانی دارد. می‌توان بسیاری از قابلیت‌های فضای سایبری را سلاح تلقی کرد. بر اساس حقوق بین‌الملل بشردوستانه، هر سلاح نوینی باید از لحاظ حقوقی ارزیابی شود تا سازگاری آن با قواعد و مقررات موجود در حقوق مخاصمات مسلحانه اثبات شود. هدف این مقاله، بررسی ماهیت و ویژگی‌های چنین قابلیت‌هایی برای یافتن پاسخ به این پرسش بود: «آیا می‌توان بررسی حقوقی قابلیت‌های فضای سایبری را با استفاده از ماده ۳۶ پروتکل یکم الحاقی انجام داد؟ گرچه پاسخ به این پرسش مثبت است، دشواری‌های در این خصوص وجود دارد.

بررسی ماهیت و ویژگی قابلیت‌های فضای سایبری، بیانگر بروز چالش‌هایی در روند بررسی حقوقی آن‌هاست. اولین چالش، فقدان قواعد و مقرراتی است که صریحاً و مستقیماً استفاده از وسایل و شیوه‌های نبرد در فضای سایبری را منع کرده یا مجاز دانسته باشد زیرا عملیات سایبری و بهره‌برداری از فناوری سایبری نسبتاً جدید است. چالش بعدی، فقدان تعریف مورد اجماع بین‌المللی از سلاح است زیرا تفسیر ماده ۳۶، تعریف سلاح و ابزار جنگی برای بررسی حقوقی را به دولت‌ها سپرده است. در نتیجه ممکن است هر کشوری تفسیری متفاوت از موضوع داشته باشد.

تعریف سلاح جدید، چالش دیگری است که بررسی حقوقی قابلیت‌های فضای سایبری را با دشواری مواجه می‌کند. ویرایش‌های جدید نرم‌افزار یا بدافزار (سلاح سایبری) که به‌صورت دوره‌ای و برای بالابردن توانایی‌های آن‌ها انجام می‌گیرد، آن‌ها را مشمول بررسی مجدد می‌کند، در حالی که بسیاری از این ویرایش‌ها در دوره‌های زمانی کوتاه‌مدت انجام شده و در نتیجه، بررسی مجدد آن‌ها عملاً غیرممکن و بسیار زمان‌بر و هزینه‌بر خواهد بود. لذا پیشنهاد می‌شود یک آستانه عینی به‌عنوان مقیاسی برای تغییر در ویرایش‌های بعدی درنظر گرفته شود تا بر اساس آن بررسی حقوقی تکرار شود. ماهیت کیفی اثرگذار باید ملاک تغییر باشد و نه ماهیت کمّی، اما همین روش جایگزین نیز با چالش روبه‌رو خواهد شد زیرا چگونگی اندازه‌گیری ماهیت کیفی تغییر موردنظر، سبب

96. Acquisition

پیچیده‌ترشدن موضوع می‌شود.

چالش تعریف شئ (به‌عنوان هدف حمله) که در مباحث کارشناسان تدوین‌کننده دستورالعمل *تالین* بروز کرد، همچنان باقی است. در صورت عدم اطلاق شئ به داده‌های رایانه هدف حمله، قابلیتی که برای ورود خسارت به داده‌ها از آن استفاده شده، سلاح به حساب نخواهد آمد، حال آنکه تخریب بسیاری از داده‌ها نه‌تنها ممکن است خسارات فیزیکی به دنبال داشته باشد، بلکه خسارت‌های مجازی نیز رخ خواهد داد که می‌تواند از لحاظ نظامی دارای اهمیت فراوانی باشد.

دوگانگی کاربرد اینترنت به‌عنوان زیرساخت فضای سایبری، چالش دیگری است. عرضه‌کنندگان خدمات اینترنتی، هم به شبکه‌های غیرنظامی و هم نظامی خدمات‌رسانی می‌کنند. استفاده فرمانده از قابلیت سایبری برای حمله به رایانه‌های نظامی دشمن می‌تواند سبب آلودگی رایانه‌های غیرنظامی مهم مانند بانکداری، مراقبت‌های پزشکی یا انرژی برق شود.

بخش اعظمی از سلاح‌های سایبری در نتیجه فعالیت افراد و گروه‌ها تولید و کشف می‌شود یا به سرقت می‌رود، در حالی که در ماده ۳۶ هیچ الزامی بر چنین بازیگرانی برای بررسی حقوقی سلاح‌های جدید تحمیل نشده است. حال آنکه به‌کارگیری تسلیحات بدون ارزیابی حقوقی نیز غیرقانونی است.

چالش‌های یادشده بیانگر پیچیدگی بررسی حقوقی قابلیت‌های فضای سایبری است. علاوه بر آن، سرعت توسعه این فناوری و فقدان اطلاعات جامع در زمینه پیشرفت‌های آن، ممکن است نتایج هر تحقیقی را ضعیف نشان داده و دشواری‌هایی در روند تحقیقات به وجود آورد. لذا پرسش‌های متعددی برای روشن‌شدن دیگر زوایای قابلیت‌های فضای سایبری مطرح می‌شود. برای مثال، آیا نوع هدف سایبری (تحت عنوان شئ در قاعده ۸ حقوق بین‌الملل عرفی) بر تلقی قابلیت‌های سایبری به‌عنوان سلاح تأثیر دارد؟ یا چه آثار مجازی ناشی از کاربرد قابلیت‌های سایبری، آن‌ها را در زمره تسلیحات قرار می‌دهد؟ آیا بدافزارها یا سلاح‌های سایبری مشمول معاهده کنترل تسلیحات می‌شوند؟

با عنایت به اینکه اسناد مربوط به حقوق بین‌الملل بشردوستانه در زمانی تدوین شده‌اند که چنین فناوری‌هایی وجود نداشته، بدیهی است که اِعمال آن‌ها بر سلاح‌های جدید در حوزه سایبری با چالش‌هایی که ذکر شد روبه‌رو خواهد بود. برای فایق‌آمدن بر این چالش‌ها و تضمین ایفای تعهدات کشورهای عضو جامعه جهانی در قبال حقوق بین‌الملل بشردوستانه، تفاسیری جدید از برخی قواعد، مقررات و تعاریف موجود در حقوق بین‌الملل بشردوستانه (مانند بازتفسیر میدان نبرد و سلاح) ضروری می‌نماید.

منابع:

الف. فارسی

شریفی طرازکوهی، حسین؛ *حقوق بشردوستانه بین‌المللی*، چاپ دوم، میزان، ۱۳۹۵.

ضیایی بیگدلی، محمدرضا؛ *حقوق بین‌الملل بشردوستانه*، چاپ سوم، گنج دانش، ۱۳۹۲.

قربان‌نیا، ناصر؛ *حقوق بشر و حقوق بشردوستانه*، پژوهشگاه فرهنگ و اندیشه اسلامی، ۱۳۸۷.

ب. انگلیسی

- Books

Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, International Committee of the Red Cross, Geneva. 1987.

Green, Leslie C., *The Contemporary Law of Armed Conflict*, 3rd ed., UK, Juris Publishing, 2008.

- Articles

"A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977", (December 2006), International Committee of the Red Cross, Geneva, *International Review of the Red Cross*, vol. 88, no. 864.

Blake, Dunkan & Imburgia, Joseph S., "Bloodless Weapons? The Need to Conduct Legal Review of Certain Capabilities and the Implications of Defining them as Weapons", *The Air Force Law Review*, vol. 66. 2010.

Boothby, William H., "Where Do Cyber Hostilities Fit in the International Law Maze?" in Nasu, Hitoshi & McLaughlin, Robert (eds.), *New Technologies and the Law of Armed Conflict*, The Hague, ASSER Press. 2014.

Boulanin, Vincent, "Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapons Systems", *SIPRI Insight on Peace and Security*, No.201/1. 2015.

Brown, Gary D. and Metcalf, Andrew O., "Easier Said Than Done: Legal Review of Cyber Weapons", *Journal of National Security Law and P*olicy, vol. 7, no. 1. 2014.

Daoust, Isabelle, Coupland, Robin and Ishoey, Rikke, "New Wars, New Weapons? The Obligation of States to Assess the Legality of Means and Methods of Warfare", *International Review of Red Cross*, vol. 84, no. 846. 2002.

Denning, Dorothy, "Reflections on Cyber Weapons Controls", *Computer Security Journal*, vol. 16, no. 4. 2002.

Devai, Dora, "Proliferation of Offensive Cyber Weapons. Strategic Implications and Non-Proliferation Assumptions", *AARMS*, vol. 15, no. 1. 2016.

Ebner, Nike, "Cyber Space, Cyber Attack and Cyber Weapons", *Institute for Peace Research and Security Policy*, University of Hamburg. 2015.

Gervais, Michael, "Cyber Attacks and the Laws of War", *Berkley Journal of International Law*, vol. 30, issue 2, 2012.

Herbach, Jonathan David, "Into the Caves of Steel: Precaution Cognition and Robotic Weapon Systems under the International; Law of Armed Conflict", *Amsterdam Law Forum*, VU University Amsterdam, Summer Issue, 2012.

Hughes, Rex, "A Treaty for Cyberspace", *The Royal Institute of International Affairs*, vol. 86, no. 2. 2010.

Lindsay, Jon R., "Stuxnet and the Limits of Cyber Warfare", *Security Studies*, vol. 22. 2013.

Madison, David, "Geography, Territory and Sovereignty in Cyber Warfare", in Nasu, Hitoshi & McLaughlin, Robert (eds.), *New Technologies and the Law of Armed Conflict*, The Hague, ASSER Press. 2014.

McClelland, Justin, "The Review of Weapons in Accordance with Article 36 of Additional Protocol I", *International Review of the Red Cross*, vol. 85, no. 850. 2003.

Mele, Stefano, "Cyber Weapons: Legal and Strategic Aspects", *Italian Institute of Strategic Studies*, Rome, 2013.

Robin, Bradley, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", *Journal of the National Association of Administrative Law Judiciary*, vol. 31, issue 2. 2011.

Schmitt Michael, N., "Cyber Operations and the *Jus in Bello*: Key Issues", in Pedrozo R.A., Wollschlaeger D.P. (eds.) *International Law and the Changing Character of War*, Newport, US Naval War College International Law Studies, vol. 87, Naval War College, 2011.

Schmitt, Michael N., "Rewired Warfare: Rethinking the Law of Cyber Attack", *International Review of the Red Cross*, vol. 96, no. 893. 2014.

Streltsov, Anatoly, "Key Trends of International Law Relating to the Conflicts in Cyber Space", in Greppi, Edoardo (ed.) *Conduct of Hostilities: The Practice, The Law and The Future*, International Institute of Humanitarian Law, 2015.

Turns, David, "Cyber War and the Concept of Attack in International Humanitarian Law", in Saxon, Dan (ed.) *International Humanitarian Law and the Changing Technology of War*, Boston, Martinus Nijhoff Publishers. 2013

- Documents

Biontino, Michael, "Lethal Autonomous Weapon Systems Expert Meeting", Geneva, 13-16 May 2014.

Brose, Robert, "Cyber War, Net War and the Future of Cyber Defence", *Office of the Director of National Intelligence*, United States. 2015.

Tallin Manual on the International Law Applicable to Cyber Warfare, NATO Cooperative Defense Centre of Excellence, Cambridge University Press, Cambridge, 2013.

West, Dondi S., "A Survey and Examination of the Adequacy of the Laws Related to Cyber Warfare", *Defence Conference*, July 30th -August 1st, Las Vegas. 2010.

"Toward Stable and Effective Use of Cyberspace", *Ministry of Defence*, Japan, September 2012.

- Websites

Ballesteros, Carlos, "Russians Stole NSA Cyber Weapons and Are Using Them against US, *Newsweek*, http://www.newsweek.com/russia-nsa-cyber-weap ons-hacking-710053, (last visited 5/3/2018).

Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, International Committee of Red Cross, Article 8, https://www.icrc.org/eng/assets/files/other/icrc_002_0811.pdf, (last visited 11/2/2018).

Hern, Alex, "WannaCry, Petya, NotPetya: How Ransom Ware Hit the Big Time in 2017", *The Guardian*, https://www.Theguar dian.com/technology/ 2017/dec/30/wannacry-petya-notpetya-ransomware, (last visited 5/3/2018).

Hern, Alex, "North Korea Is a Bigger Cyber-Attack Threat than Russia, *The Guardian*, https://www.theguardian.com/technology/2018/feb/26/ north-korea-cyber-attack-threat-russia, (last visited 5/3/2018).

Schmitt, Michael N., "Cyber Operations and International Humanitarian Law: Faultiness and Vectors", HLS Program on International Law and Armed Conflict, http://www.youtube.com/watch?v=zwwrvamsot4, (last visited 6/3/2018).

Rachman, Gideon, "Nuclear Weapons Are a Risky Defence against Cyber Attacks", *Financial Times*, accessed on 5 March 2018, https://www.ft.com/ content/d2241b68-fc31-11e7-9b32-d7d59aace167.

Ranger, Steve, NATO Just Added Cyber Weapons to Its Armoury", accessed on 5 March 2018, http://www.zdnet.com/article/nato-just-added-cyber-weapons-to-its-armoury/.

Szondy, David, "Cyber Attacks Could Lead to Use of Nuclear Weapons, accessed on 5 March 2018, https://newatlas.com/cyberattack-launch-nuclear-weapons/52924/.

United Nations Arms Trade Treaty, Principles, p. 2, accessed on 11 February 2018 on: http://legal.un.org/avl/pdf/ha/att/att_e.pdf.