فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره اول، زمستان ۱۴۰۰، صفحات ۶۶-۲۹

جنگ سایبری: چالش‌ها و راهکارها در حقوق بین‌الملل

علی‌اکبر سورانی[۱]

تاریخ دریافت: ۱۴۰۰/۰۳/۲۶ **تاریخ پذیرش: ۱۴۰۰/۰۹/۲۵**

چکیده

فضای سایبر عرصه جدیدی در برابر زندگی انسان امروزی گشوده و فرصت‌ها و تهدیدهای فراوانی را فراروی بشر قرار داده است. ظهور این فضا، اغلب حوزه‌ها را دستخوش تغییر و تحول نموده است. ازجمله موضوعات مهمی که با پدیدار شدن فضای سایبر با تحول مواجه شده، جنگ است. فضای سایبر به‌عنوان عرصه پنجم نبرد، منجر به شکل‌گیری نسل جدیدی از جنگ‌ها گردیده که از آن با عنوان جنگ سایبری یاد می‌شود.

با گسترش فضای سایبری در تمامی شئون زندگی، بشر بیش‌ازپیش به این فضا وابسته شده است. به همین دلیل بروز جنگ سایبری و تعرض به دارایی‌های وابسته به این فضا می‌تواند خسارت‌ها و پیامدهای ناگواری داشته باشد. وابستگی شدید زیرساخت‌های حیاتی کشورها به فضای سایبری و امکان حمله به این زیرساخت‌ها، نگرانی‌های جدی‌ای برای دولت‌ها به وجود آورده و از طرفی نبود قوانین بین‌المللی پذیرفته‌شده در حوزه جنگ سایبری، موجب تشدید این نگرانی‌ها شده است. با این اوصاف در مقاله حاضر در پی آنیم که چالش‌ها و مشکلات جنگ سایبری در حوزه حقوق بین‌الملل را با رویکرد توصیفی- تحلیلی و گردآوری ترکیبی داده‌ها با استفاده از ابزار فیش و مصاحبه، مورد واکاوی قرار داده و راهکارهای مربوطه را ارائه نماییم.

کلید واژه‌ها: فضای سایبر، حمله سایبری، جنگ سایبری، حقوق بین‌الملل

۱. دانشجوی دکتری مدیریت راهبردی فضای سایبر/ امنیت سایبر دانشگاه و پژوهشگاه عالی دفاع ملی(نویسنده مسئول) A.a.soorani@sndu.ac.ir

مقدمه

فضای سایبر با ویژگی های خاصی که دارد منجر به شکل گیری حوزه جدیدی از نبرد گردیده که می‌توان آن را نوعی نبرد و جنگ نامتقارن نامید. بازیگران عرصه سایبر در پایین‌ترین سطح آن، شامل یک یا چند نفر یا یک تیم هکری است که می‌توانند یک کشور یا حکومت را با چالش جدی مواجه نمایند و در بالاترین سطح، حکومت‌ها، دولت‌ها و حتی شرکت‌ها و نهادهای چندملیتی به ایفای نقش در این عرصه می‌پردازند و جالب توجه، اینکه در این عرصه نبرد نامتقارن، امکان تأثیرگذاری برای کشورهای کوچک و حتی گروه‌های محلی و نیز تیم‌های چندنفره وجود دارد که شاید در سایر عرصه‌های نبرد حرفی برای عرضه نداشته یا در موضع ضعف قرار داشته باشند.

زیرساخت‌های حیاتی کشورها، وابستگی زیادی به فضای سایبر پیدا کرده‌اند و اعتماد و اتکای جهانی به فناوری اطلاعات در تمام کشورها و سازمان‌های اطلاعاتی آن‌ها، به‌صورت چشمگیری نه‌تنها فرایند اطلاعاتی، بلکه جنگ نظامی را نیز تغییر داده است و فضای سایبر به میدان جنگ اطلاعات تبدیل شده است.

در قرن ۲۱، جنگ، ناگزیر، شامل جنگ سایبری[1] خواهد بود. جنگ همراه با پیشرفت سلاح‌های ویژه، نرم‌افزارها، تجهیزات الکترونیکی، تاکتیک‌ها و دفاع‌های ویژه، به سمت فضای سایبری خواهد رفت؛ بنابراین با در نظر گرفتن توسعه سریع فناوری ها و محیط دیجیتال، لازم است کشورها، برنامه‌ای برای جنگ سایبری داشته باشند.

یکی از دلایل اصلی بروز نابسامانی و مناقشات در فضای سایبر، بی‌قانونی در این فضا است که از آن با عنوان خلأ قانون بین المللی جنگ سایبری یاد می شود؛ بنابراین، اولین گام در عرصه جنگ سایبری در سطح بین الملل، تدوین و تنظیم قوانین مرتبط با جنگ سایبری است که باید مورد توافق و تأیید جامعه بین الملل و بازیگران فعال در عرصه سایبری قرار گیرد تا ضمن پذیرش از سوی ذینفعان، از ضمانت اجرای لازم نیز برخوردار گردد.

1 .Cyber warfare.

۱. بیان مسئله

فضای سایبر به‌عنوان فضایی تعریف می‌شود که در آن، اطلاعات از یک محیط بـه محـیط دیگر، گردش دارند و در آن پردازش، کپی و ذخیره می‌شوند. ایـن فضـا شـامل سیسـتم‌هـای ارتباطات، رایانه‌ها، شبکه‌ها، ماهواره‌ها و زیرساخت ارتباطات است و توانسته نقش بی‌بـدیلی در زندگی بشر ایفا نموده و عرصه و محیط جدیدی و نوینی را فراروی بشر بگشاید.

فضای سایبر، دنیای جدید و گسترده‌ای است که در آن همه چیز مبهم و نامشخص اسـت. در این فضا ارتباطات، جنگ سـایبری و الکترونیکـی بـه شـدت گسـترش پیـدا کـرده اسـت. موضوعات مختلف دولت ها از امور نظامی تا امور فرهنگی و اجتماعی همگـی رایانـه محـور شده است. این امر سبب شده که رقبا برای افزایش توانمندی خود و نیز ضـربه بـه دشـمن در این فضا سرمایه گذاری کنند. فضایی که در آن معاهده حقوقی مشـخص و جـامعی کـه تمـام جنبه های مختلف را در برگیرد، بـه وجـود نیامـده اسـت و حـق و تکلیـف دولـت هـا مـبهم است(عباسی و مرادی، ۱۳۹٤: ٦٦).

فضای سایبر عرصه جدیدی برای زندگی بشـر فـراهم کـرده و فرصـت هـا و تهدیـدهای فراوانی را با خود به همراه داشته است. ظهور این فضـا، اغلـب حـوزه‌هـا و مفـاهیم آن‌هـا را دستخوش تغییر و تحول نموده است. ازجمله موضوعات مهمی که بـا پدیـدار شـدن فضـای سایبر با تحول مواجه شده، جنگ است. هم‌اکنون عرصه جدیدی از جنگ و نبرد شکل گرفتـه که از آن با نام عرصه پنجم نبرد یا همان فضای سایبری یاد می‌شود.

ورود مناقشات و جنگ‌ها به فضای سایبری، جنگ سایبری را شکل داده و در عـین حـال، سایبر در سایر عرصه های جنگ و نبرد (زمینی، دریایی، هوایی و فضایی) نیز ورود پیدا کـرده و مفهومی با عنوان سایبر در رزم یا نبرد را به وجود آورده و دیگر عرصه های نبرد، بـه شـدت به فضای سایبر وابسته شده است؛ بنابراین بهره‌گیری از قابلیت‌های سایبری می‌تواند منجر بـه موفقیت در سایر عرصه‌های نبرد نیز گردد.

تاکنون تعریف پذیرفته‌شده‌ای از جنگ سایبری ارائه نشده است، اما به‌طور کلی مـی‌تـوان گفت جنگ سایبری به جنگی اطلاق می‌شود که در فضای سـایبر و بـا اسـتفاده از روش‌هـا و ابزارهای سایبری انجام می‌شود. جنگ سایبری به‌عنوان وسیله‌ای برای اجـرای عملیـات‌هـای

نظامی، طبق اصول مرتبط با اطلاعات است. فضای جنگ سایبری فضای اطلاعات است که هنگام جنگ مورد توجه قرار می گیرد. فضای جنگ سایبری شامل هر چیزی است که در محیط فیزیکی و نیز محیط فضای سایبری روی می‌دهد.

برخی صاحب‌نظران، حملات سایبری[1] در قرن بیست‌ویکم را معادل با سلاح‌های هسته‌ای در قرن بیستم دانسته اند که این موضوع حاکی از اهمیت و حساسیت بالای فضای سایبر و لزوم نقش آفرینی حاکمیت ها در آن است. به همین دلیل تعداد کشورهایی که در عملیات های سایبری نقش دارند، هر روز در حال افزایش است. از طرفی حقوق بین الملل در عرصه جنگ سایبری تقریباً سکوت کرده و قاعده و قانون مورد توافق جامعه بین الملل در حوزه جنگ سایبری وجود ندارد که این موضوع، فرصت‌ها و تهدیدهای بی‌شماری را برای جوامع و دولت‌ها داشته است.

با اوصاف فوق، پژوهش حاضر در پی آن است که با تبیین و تشریح مفهوم جنگ سایبری و موضوعات مرتبط، به خلأهای قانونی و حقوقی این عرصه پرداخته و چالش‌ها و مشکلات حقوق بین الملل در حوزه جنگ سایبری را مورد بررسی و واکاوی قرار داده و راهکارهای برخورد با آن‌ها را ارائه نماید.

۲. اهمیت و ضرورت

نبردهای سایبری به‌عنوان جدیدترین و پیچیده‌ترین نبردها در جنگ پست‌مدرن به شمار می آید. حملات سایبری به دلیل بکر بودن، درصد هزینه و فایده بالا، عدم توانایی کشور هدف در مشخص و اثبات نمودن منشأ تهدید و عدم توانایی در تعیین میزان و دامنه خسارات واردشده در مراحل اولیه شروع حمله، مورد توجه کشورهای متخاصم به‌ویژه در جنگ های پنهان قرار گرفته است (حسینی، ۱۳۹۲).

جنگ سایبری با توجه به تبعات و دامنه تأثیر بالای آن از اهمیت بالایی برخوردار است؛ به نحوی که توجه بسیاری از دولت ها به این موضوع معطوف شده و نگرانی هایی در این زمینه احساس می شود از طرفی با توجه به نبود قانون جهانی در خصوص جنگ ها و مخاصمات سایبری که از سوی جامعه بین الملل مورد قبول واقع شده باشد موضوع جنگ سایبر را به

1 .Cyber Attacks.

موضوع و چالش جهانی برای دولت ها مبدل کـرده اسـت. بـا ایـن اوصـاف موضـوع جنـگ سایبری و حقوق بین الملل در این حوزه از اهمیت بالایی برخوردار بوده و عدم توجه به ایـن حوزه می تواند ضررها و تبعات سنگینی را در پی داشته باشد که ضرورت و لزوم پرداختن بـه این موضوع را، به‌خوبی توجیه می‌نماید.

به دلایل زیر پرداختن به موضوع جنگ سایبری و حقوق بـین‌الملـل در ایـن عرصـه، از اهمیت بالایی برخوردار بوده و بیش‌ازپیش در این خصوص، احساس نیاز می‌شود:

۱. آشنایی با مفهوم جنگ سایبری و ویژگی‌های آن

۲. شناخت فرصت‌ها و تهدیدهای جنگ سایبری

۳. اطلاع از خلأهای حقوقی و قانونی حـوزه جنـگ سـایبری در عرصـه بـین‌المللـی و بهره‌گیری از فرصت‌های مثبت و بر حذر ماندن از چالش‌ها و تهدیدهای آن

٤. اتخاذ تمهیدات و سازوکار مناسب برای پیگیری اقدامات سـایبری خصـمانه دشـمنان در عرصه بین‌الملل

۵. ایجاد بازدارندگی حقـوقی لازم در برابـر اقـدامات خصـمانه دشـمنان، بـروز جنـگ سایبری و ایجاد خسارت به زیرساخت‌های کشور

٦. کسب آمادگی برای مواجهه حقوقی لازم با جنگ سایبری و جلـوگیری از غـافلگیری در این مواجهه

ضررها یا پیامدهای سلبی (منفی) ناشی از عدم انجـام ایـن پـژوهش کـه ضـرورت آن را توجیه می‌کند، در موارد زیر می‌توان خلاصه نمود:

۱. ضعف در شناخت و اطلاق جنگ سایبری.

۲. عدم اطلاع از پیامدها و نتایج عملیات سایبری بر ضد دشمنان در جامعه بین‌الملل.

۳. عدم نقش‌آفرینی مناسب در عرصه حقوق فضای سایبر در سطح بین‌الملل.

٤. ضعف در پیگیری حقوقی مخاصمات و حملات سایبری و نیز تهدید جنگ سایبری از سوی دشمنان در سطح بین‌الملل.

۵. ضعف در بهره گیری از فرصت های موجود در عرصه جنگ سایبری و عـدم توجـه بـه این عرصه مهم و مؤثر در سطح جهانی.

٦. ضعف در ایجاد بازدارندگی حقوقی لازم در مقابل اقدامات خصمانه دشمنان در عرصه جنگ سایبری.

۷. نداشتن تمهید مناسب برای مواجهه با جنگ سایبری در عرصه حقوق بین‌الملل.

۸. در معرض تهدید قرار گرفتن زیرساخت‌های کشور در مقابل حمله و جنگ سایبری.

۳. پیشینه تحقیق

اسمعیل‌زاده ملاباشی و دیگران (۱۳۹٦) در مقاله‌ای با عنوان «حملات سایبری و اصول حقوق بین الملل بشردوستانه (مطالعه موردی: حملات سایبری به گرجستان)»، صرفاً به بررسی حملات سایبری صورت گرفته در سال ۲۰۰۸ میلادی به گرجستان پرداخته و امکان تسری قواعد حاکم بر مخاصمات مسلحانه سنتی بر این حملات را مورد تحلیل قرار می دهند و در این خصوص نتیجه گیری می کنند که در حملات سایبری به گرجستان، اصول حقوق بشردوستانه نقض شده است.

برادران و حبیبی (۱۳۹۸) در مقاله خود چگونگی اعمال قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری را تبیین نموده و نتیجه‌گیری می‌کنند تا زمانی که قواعد خاص حقوق بشردوستانه بین المللی در مخاصمات سایبری تدوین نشده است، همچنان می توان با توسل به اصول و قواعد موجود، روش های نبرد سایبری را در چارچوب حقوق بین‌الملل بشردوستانه به نظم درآورد.

جعفری و اسدی (۱۳۹۷) در مقاله ای با عنوان «بررسی ابعاد حقوقی جنگ سایبری با نگاهی به قواعد حاکم بر مخاصمات مسلحانه بین‌المللی» در خصوص اعمال قواعد حقوق بین‌الملل بشردوستانه بر حوزه جنگ سایبر به بحث و بررسی پرداخته‌اند و نتیجه گیری می‌کنند که در مخاصمات مسلحانه، اصول حقوق بین‌الملل بشردوستانه می‌تواند حاکم بر فضای عمومی جنگ سایبر باشد، اما این روند نیازمند تدوین قوانینی است تا بتواند در صحنه‌های جنگ نیز کارایی داشته باشد.

جعفری و توتونچیان (۱۳۹۸) در مقاله‌ای با عنوان «بررسی راهکارهای تحدید حملات سایبری از منظر حقوق بین‌الملل بشردوستانه» به نحوه کاربست حقوق بین‌الملل بشردوستانه

در حملات سایبری پرداخته و عنوان می‌کنند حملات سایبری به دلیل صدمه زدن به غیرنظامیان می‌تواند مورد توجه حقوق بین‌الملل بشردوستانه قرار گیرد.

خلف رضایی (۱۳۹۲) به مطالعه موردی حمله استاکس نت پرداخته و آن را از دیدگاه حقوق بین الملل مورد بررسی و واکاوی قرار داده و بیان می دارد در فضای سایبر مسئله انتساب از مشکلات اصلی طرح مسئولیت دولت هایی است که حملات سایبری انجام می‌دهند، یا از آن حمایت می‌کنند.

صلاحی و کشفی (۱۳۹۵)، جنگ سایبری را از نظر حقوق بین الملل و با توجه به مفاد دستورالعمل تالین مورد تحلیل قرار داده و از دستورالعمل مذکور به عنوان تنها منبع بین المللی فعلی با موضوع حقوق بین‌الملل قابل اعمال در نبردهای سایبری یاد می‌کنند.

با اوصاف فوق، بررسی‌های نگارنده حاکی از آن بود که در اغلب پژوهش‌های صورت گرفته در حوزه مباحث حقوقی جنگ سایبری، به صورت بخشی، به این مبحث پرداخته شده و توجه چندانی به حوزه کلان موضوع نشده و از طرفی راهکارهای ارائه‌شده در آن ها نیز صرفاً به همان موضوع بخشی اشاره داشته است؛ بنابراین در این پژوهش بیشتر به تبیین بحث کلان موضوع پرداخته شده و راهکارهای ارائه‌شده هم با همین دیدگاه و در راستای آن بوده است.

٤. روش‌شناسی تحقیق

این تحقیق با توجه به هدف آن، از نوع تحقیقات کاربردی است؛ چراکه می خواهد چالش ها و مشکلات جنگ سایبری را در حوزه حقوق بین‌الملل مورد بررسی و تحلیل قرار داده و راهکارهای مربوطه را ارائه کند.

تحقیق حاضر، از طریق گردآوری داده های کیفی و با مطالعه جدی و عمقی داده ها و تحلیل آن‌ها، در پی واکاوی موضوع است؛ بنابراین از نظر مفروضات معرفت‌شناختی، این تحقیق در زمره تحقیقات کیفی به شمار می رود. از آنجا که این تحقیق در پی توصیف و تحلیل چالش های جنگ سایبری در حقوق بین الملل است؛ بنابراین از منظر ماهیت و روش نیز یک تحقیق توصیفی-تحلیلی است.

برای گردآوری داده‌ها از هر دو روش کتابخانه‌ای و میدانی استفاده شده است بدین نحو که ابتدا به مطالعه و بررسی اسناد و مقالات علمی موجود در حوزه تحقیق اقدام شده و پس از جمع‌بندی و تحلیل و بررسی آن‌ها، موارد در مصاحبه با تعدادی از نخبگان، مورد نقد و بررسی قرار گرفته است.

با توضیحات فوق، ابزار مورد بهره‌برداری برای گردآوری داده‌ها در این تحقیق، فیش و مصاحبه است.

۵. مفهوم جنگ سایبری

هنوز تعریف مشخصی برای فضای سایبر و نیز جنگ وجود ندارد؛ بنابراین تعریف جنگ سایبری آسان نخواهد بود.

باید گفت که از لحاظ تئوری، تعریف جنگ سایبری بسیار آسان‌تر از تعریف آن به‌صورت عملی است؛ زیرا تاکنون هیچ جنگ سایبری علنی و آشکاری روی نداده و هیچ کشوری اعلام جنگ سایبری نکرده است.

اگرچه جنگ سایبری می‌تواند تأثیرات مخربی داشته باشد؛ اما در آن از ویرانی و خونریزی های مرسوم در جنگ واقعی خبری نیست. اگرچه اطلاعات موجود در جنگ سایبری، مستقیماً عامل مرگ انسانی نمی‌شود، اما این اطلاعات ممکن است سیستم‌ها و برنامه‌هایی را از بین ببرد که جان انسان‌ها را به خطر بیندازد (جعفری و اسدی، ۱۳۹۷: ٦٠).

جنگ سایبر در ساده‌ترین تعریف به‌عنوان «استفاده از رایانه و اینترنت برای جنگیدن در فضای سایبر تعریف شده است» (عبدالله‌خانی، ۱۳۸٦: ۱۳٦-۱۳۵)؛ اما به‌صورت جزئی‌تر اصطلاح جنگ سایبر به جنگ انجام گرفته در فضای سایبر از طریق ابزارها و روش‌های سایبری اشاره دارد.

در سند راهبردی پدافند سایبری کشور، جنگ سایبری به این صورت تعریف شده است:

بالاترین سطح و پیچیده‌ترین نوع از تهاجم سایبری که توسط ارتش سایبری کشورهای مهاجم یا گروه‌های سازماندهی‌شده تحت حمایت دولت‌های متخاصم بر ضد منافع ملی کشورها انجام می‌شود جنگ سایبری است.

در بخش دیگری از سند راهبردی پدافند سایبری در تعریف جنگ سایبری آمده است:

جنگ سایبری به نوعی از نبرد اطلاق می شود که طرفین جنگ در آن از رایانه و شبکه‌های رایانه‌ای (به‌خصوص شبکه اینترنت) به‌عنوان ابزار تهاجم استفاده کرده و نبرد را در فضای سایبری به راه می‌اندازند (سازمان پدافند غیرعامل کشور، ۱۳۹٤).

طبق واژه‌نامه مشترک روسیه و آمریکا، جنگ سایبری، حالت تشدید برخورد سایبری بین دو کشور است که در آن حملات سایبری به وسیله عوامل یک کشور به‌عنوان بخشی از عملیات جنگی بر ضد زیرساخت سایبری کشور دیگر انجام می‌شود که ممکن است به‌صورت رسمی، به‌وسیله مسئولین یک طرف مخاصمه اعلان شود، یا آنکه به‌طور رسمی اعلام نشود.

در ادامه، واژه‌نامه مذکور تعریفی از نبرد سایبری ارائه می‌دهد که بسیار نزدیک به جنگ سایبری است و آن تعریف چنین است: نبرد سایبری عبارت است از حملات سایبری که به‌وسیله عوامل یک کشور بر ضد زیرساخت‌های سایبری کشور دیگر، در رابطه با یک سلسله عملیات جنگی انجام می‌شود (RAUSCHER & YASCHENKO, 2014:43).

نبرد سایبری در اصل به معنای روش جنگ است، ولی با تسامح به عنوان جنگ نیز به کار گرفته شده است. (قاسمی و اسماعیلی فرزین، ۱۳۹٦: ۵۳). آنچه در خصوص تفاوت جنگ و نبرد سایبری می توان گفت اینکه، نبرد سایبری بیشتر معطوف و ناظر به شیوه، فنون و روش جنگ سایبری است در حالی که جنگ سایبری بیشتر به یک درگیری مسلحانه خاص اشاره دارد.

جنگ سایبری، توسعه سیاست‌ها در فضای مجازی توسط عوامل دولتی و غیردولتی است که به منزله یا در پاسخ به تهدید جدی بر ضد امنیت ملی انجام می‌گیرد (SHAAKARIAN, 2013).

کلارک و کناک[1] جنگ سایبر را به‌عنوان «نفوذ غیرمجاز به‌وسیله، از طرف، یا در حمایت از یک دولت به شبکه‌ها یا رایانه‌های ملی دیگری، یا هر فعالیت متأثرکننده سیستم‌های رایانه‌ای که هدف در آن جمع کردن، تغییر دادن یا دست‌کاری اطلاعات، یا باعث مختل شدن یا صدمه زدن به رایانه، طرح شبکه، یا اهداف کنترل سیستم رایانه است» تعریف کرده‌اند(MAURER, 2011: 15).

1 .Clarke and Knake.

صلاحی و کشفی در مقاله‌ای، جنگ سایبری را از منظر حقوق بین‌الملل مورد واکاوی قرار داده و معتقدند که جنگ سایبری، به کارگیری هدفمند قوای سایبری یک کشور، شامل مجموعه اقدامات پیوسته رایانه‌ای، در جهت تخریب، ضربه یا تصرف کشور هدف است که می‌تواند از طریق کنترل و تخریب زیرساخت‌های اطلاعاتی و امنیتی یک کشور انجام گیرد. آنچه در این تعریف، جنگ سایبری را از کنش و واکنش‌های آنی و کوتاه‌مدت دیگر اقدامات سایبری مجزا می‌کند دو موضوع «هدفمندی» و «پیوستگی» است (صلاحی و کشفی، ۱۳۹۵).

به‌زعم جعفری و اسدی، جنگ سایبری شامل حملات دیجیتالی به شبکه‌ها، سامانه‌ها اطلاعات کشور دیگری با هدف صدمه زدن به آن ها است. این حملات ممکن است حاوی تخریب، تغییر یا به سرقت بردن اطلاعات یا از دسترس خارج کردن خدمات برخط باشد که جامعه نظامی یا جامعه‌های بزرگ‌تر از آن‌ها استفاده می‌کنند (جعفری و اسدی، ۱۳۹۷: ٦٠)

نکته مهمی که در تعریف جنگ سایبری باید مورد توجه قرار گیرد این است که برخی افراد، در تعریف «حمله سایبری»[1]، به اشتباه آن را، جنگ سایبری یا مخاصمه مسلحانه می دانند. این در حالی است 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 می گیرند؛ به بیانی دیگر اگر در یک حمله سایبری، آسیب ها به حدی شدید بوده باشند که قابل مقایسه با آسیب های معمول در جنگ ها باشند، در این صورت، حمله سایبری در حکم جنگ سایبری خواهد بود (جعفری و توتونچیان، ۱۳۹۸: ۳۳٦).

برخی صاحب‌نظران، جنگ سایبر را به‌عنوان نفوذ غیرمجاز به‌وسیله، از طرف، یا در حمایت از یک دولت به شبکه‌ها یا رایانه‌های ملی دیگری، یا هر فعالیت متأثرکننده سیستم‌های رایانه‌ای که هدف در آن جمع کردن، تغییر دادن یا دست‌کاری اطلاعات، یا باعث مختل شدن یا صدمه زدن به رایانه، طرح شبکه، یا اهداف کنترل سیستم رایانه است تعریف کرده‌اند.

سازمان همکاری منطقه‌ای شانگهای تعریف نسبتاً جامعی از جنگ سایبری ارائه کرده است. تعریف این سازمان از جنگ سایبری عبارت است از: مقابله میان دولت ها، در عرصه

1 .Cyber Attack.

اطلاعاتی با هدف صدمه زدن به سیستم های اطلاعاتی، روندها و منابع، ساختارهای حیاتی و مهم، تضعیف سیستم‌های سیاسی، اقتصادی و اجتماعی، عملیات‌های روانی گسترده برای بی ثبات سازی جامعه و دولت، همچنین مجبور کردن دولت برای اتخاذ تصمیماتی در راستای منافع مخالفین تعریف کرده است (عباسی و مرادی، ۱۳۹٤: ٤٨).

در مجموع می توان گفت که هنوز تعریف مورد توافقی از جنگ سایبری در عرصه بین‌الملل ارائه نشده و تعاریف موجود، هر یک از دیدگاهی به تعریف و تبیین مفهوم جنگ سایبری پرداخته‌اند. ولی آنچه که از تعاریف ارائه‌شده قابل استنتاج است اینکه اگر حمله سایبری واجد شرایط زیر باشد می‌توان گفت که جنگ سایبری روی داده است:

ـ منبع و منشأ حمله از جانب یک یا چند کشور باشد.

ـ عواقب و نتایج حملات، مخرب و جبران‌ناپذیر باشد.

ـ برخوردار از انگیزه و اهداف سیاسی باشد.

ـ نیاز به طرح‌ریزی پیچیده و روش‌های سفارشی برای اجرا داشته باشد.

٦. ویژگی‌های جنگ سایبری

همان‌طور که اشاره شد، با وجود تعاریف متعدد ارائه‌شده، هنوز تعریف پذیرفته‌شده و دقیقی از جنگ سایبری در سطح بین الملل وجود ندارد ولی ویژگی هایی برای جنگ سایبری می‌توان برشمرد که بر اساس آن می‌توان مفهوم جنگ سایبری را دریافت و تبیین نمود.

در کل ویژگی‌های زیر را می‌توان برای جنگ سایبری برشمرد:

ـ حمله از راه دور: قابلیت طراحی، اجرا و نتیجه گیری از راه دور یکی از خصایص اصلی و کلیدی جنگ سایبری است به نحوی که برای حمله سایبری نیازی به حرکت فیزیکی نیست و سربازهای سایبری می‌توانند در تمام دنیا پخش شوند.

ـ دشواری در شناسایی و ردیابی: به سبب خصائصی که در ذات پروتکل های ارتباطی در فضای سایبری وجود دارد، عملاً شناسایی و ردیابی منبع اصلی حمله و انتساب[1] حمله به وی بسیار دشوار و گاهی غیرممکن می‌شود.

1 .Attribution.

ـ **محدودیت در انتقال:** به دلیل وابستگی فضای سایبری به پروتکل های ارتباطی موجود، انتقال و عوامل وابسته به آن (نظیر سرعت، حجم، کیفیت، اعتبار و ...) با چالش محدودیت در این فرایند روبه‌رو هستند. هم اکنون پروتکل انتقال در اینترنت[1] کـه تمـام اینترنـت را بـه هـم متصل نموده دارای نواقص و محدودیت‌هایی است.

ـ **تهدید متوجه هر سه جنبه امنیـت:** در جنـگ فیزیکـی، حملـه کننـده سـعی در تهدیـد جنبه‌های فیزیکی زندگی انسان دارد در حالی که در جنگ سایبری، تهدید یکـی از سـه جنبـه امنیت اطلاعات (محرمانگی، جامعیت و دسترسی پذیری) موجـب تهدیـد عنصـر سـایبری و اشیاء مرتبط با آن می‌گردد.

ـ **اندازه هدف:** بزرگی و کوچکی هدف در جنگ‌های فیزیکی فوق‌العاده بااهمیـت اسـت ولی در جنگ های سایبری، بزرگی اهداف با بزرگی فیزیکی آن ها قابل فهم و مقایسه نیست و باید اندازه سایبری آن ها را در نظر گرفت. در جنگ سایبری، اهـداف مهـم و اساسـی از نظـر سایبری و نقش آن‌ها در این فضا باید هدف قرار گیرد نه اهداف فیزیکی بزرگ.

ـ **انتشار حمله:** حمله سایبری می تواند به سادگی از چندین منبع یـا کانـال صـورت پـذیرد در حالی که هدایت و راهبری حملات فیزیکی که از چندین محل آغاز می‌گردند بسیار دشوار است.

ـ **هزینه پایین:** بدون شک هزینه جنگ فیزیکی از جنگ سایبری بیشتر است.

ـ **مسئولیت پذیری:** قوانین مدون، مشخص و مورد توافق بین‌المللی برای مبـارزه و ایجـاد دعاوی سایبری وجود ندارد؛ بنابراین کشورها به‌سادگی از زیر بار مسئولیت حملات سـایبری خود، شانه خالی می‌کنند.

ـ **راهبری ساده:** راهبردی و هدایت جنگ سایبری به‌مراتب ساده‌تر از جنگ‌های فیزیکی است.

ـ **شروع و پایان:** شروع و پایان مشخصی برای جنگ‌های سایبری وجود ندارد.

ـ **از بین رفتن مرزهای شناخته شده فیزیکی:** در جنگ های فیزیکـی، دو طـرف درگیـر در یـک منطقه جغرافیایی مشخص وارد عمل شده و جبهه و منطقه نبرد و همین طور مرزهای فیزیکی روشـن و مشخص است در حالی که در فضای سایبری مرزهای فیزیکی سنتی از بین رفته و ناپدید می‌شود.

1 .TCP/IP.

۷. منشأ جنگ سایبری، اهداف، سناریوها و پیامدهای آن

به‌طور کلی منشأ جنگ سایبری را می‌توان در نیروی سایبری کشور مهاجم یا گروه‌های سازمان‌دهی‌شده تحت دولت‌های متخاصم، سلاح‌های سایبری تحت کنترل یا رهاشده توسط این نیروها دانست.

قاسمی و بارین چهاربخش، منابع حملات سایبری و مرتکبین این حملات را با پنج فرض دسته‌بندی می‌کنند (قاسمی و بارین چهاربخش، ۱۳۹۱: ۱۲۳-۱۲۰):

۱. نفوذگران سایبری نظامی: نخستین و ساده‌ترین فرض، «نفوذگران سایبری نظامی»[1] است. ارتش های سایبری رسمی کشورها در این دسته قرار می گیرند. در این فرض، اقدام نفوذگران سایبری نظامی باید به دولتی که ارگان‌های قانونی آن می‌باشند، نسبت داده شود.

۲. نفوذگران سایبری عضو تشکیلات حکومتی یا اشخاص شبه حکومتی: شرکت های خصوصی شده یا پیمانکاران مستقل که قانوناً حدودی از اقتدار دولت را اعمال می نمایند از این دسته‌اند.

۳. نفوذگران سایبری اجیرشده توسط دولت ها: این امکان وجود دارد که نفوذگران سایبری، عضو یا مستخدم یک دولت نباشند، بلکه اشخاص یا شرکت های باشند که توسط دولت‌ها و به‌منظور اقدام به حملات سایبری اجیر شده‌اند.

٤. نفوذگران سایبری تحت تحریک عوامل دولتی: نفوذگران سایبری ای که ارگان قانونی یا عملی دولت نباشند، اما اقدامات آن‌ها با تحریک عوامل دولت در وب‌سایت‌ها، اتاق‌های گفتگو، ایمیل و شبکه های اجتماعی صورت پذیرد. گاهی اوقات این امکان وجود دارد که پس از اقدام به تحریک، مقامات دولتی به نحو علنی از اقدامات صورت‌گرفته حمایت نمایند.

۵. حملات سایبری که از رایانه های موجود در کشوری خاص بدون دخالت هیچ دولتی، سرچشمه گرفته اند: در چنین موردی، اقدام نفوذگران سایبری را نمی توان به کشوری نسبت داد، اما این امکان وجود دارد که کشور محل استقرار رایانه های نفوذگران سایبری را مسئول دانست؛ چنین مسؤولیتی به دلیل عدم اتخاذ اقدامات ضروری و عقلایی جهت

1 .Uniformed Hackers.

جلوگیری یا متوقف کردن حمله مانند غیرممکن کـردن دسترسـی اینترنتـی مرتکبـان، ایجـاد می شود. در چنین حالتی عمل خلاف دولت، حمله سایبری نیست، بلکه نقـض تعهـد اجـازه ندادن به استفاده از قلمرو دولت برای اعمال خلاف حقوق دیگران است.

جنگ های سایبری بیشتر با هدف کلی سلطه طلبی و براندازی در سطح حاکمیت و دولـت (متوجه یک حکومت) صورت می گیرد.

سند راهبردی پدافند سایبری کشور، سناریوهای جنگ سایبری و هـدف هـر سـناریو را به شرح زیر برشمرده است (سازمان پدافند غیرعامل کشور، ۱۳۹٤):

ـ سناریو ۱): جاسوسی سایبری با حمایـت دولـت‌هـا بـا هـدف جمـع‌آوری اطلاعـات برای برنامه‌ریزی تهاجم‌های سایبری بعدی.

ـ سناریو ۲): یورش سایبری با هدف بسترسازی برای هرج‌ومرج و شورش مردمی.

ـ سناریو ۳): یورش (تهاجم) سـایبری بـا هـــدف از کـارانـــدازی تجهیـزات و تسـهیل تهاجم فیزیکی.

ـ سناریو ٤): یورش (تهاجم) سایبری به‌عنوان مکمل تهـاجم فیزیکی.

ـ سناریو ٥): یورش (تهـاجم) سـایبری بـا هـدف تخریـب یـا اختلال گسترده به‌عنوان هدف نهایی جنگ سایبری.

در سند مذکور به موارد زیر به‌عنوان پیامدهای جنگ سایبری اشاره شده است:

ـ براندازی نظام حاکمیتی یا تهدید فاجعه‌بار امنیت ملی.

ـ آغاز هم‌زمان جنگ فیزیکی یـا زمینـه‌سـازی و تسـهیل شـروع.

ـ جنگ فیزیکی در آینده نزدیک.

ـ تخریب یا صدمه فاجعه‌بار به وجهه کشور در سطح بین‌المللی.

ـ تخریب یا صدمه فاجعه‌بار به روابط سیاسی و اقتصادی کشور.

ـ تلفات انسانی یا مخاطره گسترده بـرای سـلامت و ایمنـی عمـــومی (از طریـق ایجـاد آلودگی هسته‌ای، شیمیایی یا بیولوژیک).

ـ هرج‌ومرج و شورش داخلی.

ـ اختلال گسترده در اداره امور کشور.

ـ تخریب (یا صدمه گسترده بـه) اطمینـان عمـومی یـا باورهـای دینی، ملی و قومی.
ـ خسارت شدید به (یا اختلال گسترده در) اقتصاد ملی.
ـ تخریب یا اختلال گسترده در عملکرد سرمایه‌های ملی سایبری.

۸. وضعیت فعلی جنگ سایبری در حقوق بین‌الملل

به‌طور کلی می‌توان گفت که هیچ اصل و قاعده بین‌المللـی پذیرفتـه‌شـده مختـص جنـگ سایبری وجود ندارد، اما این دلیل نمی‌شود که نتیجه‌گیری کنیم حوزه جنگ سایبری، بـه کـل، فاقد قاعده و قانون است، بلکه باید گفت که هم‌اکنون قـوانینی در سـایر حـوزه‌هـای حقـوق بین‌الملل وجود دارد که فارغ از خلأهای قانونی موجود و نبود قوانین بین‌المللـی اختصاصـی حوزه جنگ سایبری، بر این حوزه قابل اعمال و تعمیم است.

ازجمله قوانین بین‌المللی موجود، قواعد حقوق بین‌الملل بشردوستانه است کـه بـه‌عنـوان بخشی از قواعد حقوق منازعات مسلحانه، قابلیت اعمال در حوزه جنگ سـایبر را دارا اسـت. حقوق بین‌الملل بشردوستانه شاخه‌ای از حقوق بین‌الملل عمومی است که تلاش مـی‌کنـد تـا رفتار منازعه مسلحانه را تعدیل کرده و رنج ناشی از آن را تسکین دهد.

در حال حاضر هیچ اجماعی در خصـوص اعمـال حقـوق بشردوسـتانه در خصـوص جنـگ سایبری وجود ندارد. این مطلب از قطعی نبـودن تعریـف واحـدی از جنـگ سـایبری سرچشـمه می‌گیرد. همچنین هیچ‌گونه عرف و رویه‌ای نیز در این خصوص حاکم نیست و حقوق بـین‌الملـل کنونی به‌طور صریح مقرراتی در خصوص جنگ سایبری پیش‌بینی نکـرده اسـت؛ بنـابراین اعمـال قواعد حقوق بشردوستانه در خصوص چنین حملاتی در هاله‌ای از ابهام است؛ بـه عبـارت دیگـر، در حال حاضر هیچ مقرره‌ای در حقوق بشردوستانه یا حقوق بین‌الملل عرفی وجود نـدارد کـه بـه صراحت در زمان جنگ یا صلح، جنگ سایبری را ممنوع اعلام کند(جعفری و اسدی، ۱۳۹۷: ٦١).

بعضی معتقدند که حقوق بین‌الملل بشردوستانه نمی‌تواند به حملات سـایبر حـاکم باشـد چون هیچ عمل حاکی از تحرک یا جنبشی و فیزیکـی در چنـین عملیـاتی وجـود نـدارد. بـه عبارت دیگر، حملات شبکه رایانه‌ای، منازعه مسلحانه نیسـت و بنـابراین خـارج از محـدوده حقوق بین‌الملل بشردوستانه قرار می‌گیرد (ناتان شاو، ۱۳۹۵: ۹۱).

با اوصاف فوق باید گفت که اعمال قواعد حقوق بین الملل فعلی در حوزه جنگ سایبری با ابهاماتی مواجه بوده و اجماع جهانی بر نحوه اعمال این قوانین در حوزه جنگ سایبری به وجود نیامده است؛ بنابراین برداشت های متفاوتی از سوی کشورها در این زمینه صورت می گیرد. علاوه بر آن با توجه به نبود تعریف یکسان از جنگ سایبری، اتفاق نظری بر وقوع جنگ سایبری در بسیاری از موارد وجود ندارد که بتوان قوانین موجود در حوزه های جنگی را در عرصه سایبری نیز لحاظ نمود. از طرفی ویژگی های خاص جنگ سایبری امکان تعیین متجاوز را بسیار مشکل و در مواردی غیرممکن می‌نماید که این موضوع نیز بر ابهامات قبلی افزوده است و اعمال قوانین موجود را در حوزه جنگ سایبری با مشکل مواجه نموده است؛ بنابراین به‌طور خلاصه و کلی می توان گفت که در شرایط فعلی، حقوق بین‌الملل در حوزه جنگ سایبری با خلأهای اساسی مواجه است.

۹. قوانین بین‌المللی قابل اعمال به حوزه جنگ سایبری

همان طور که پیش تر نیز اشاره گردید، هنوز قانون یا معاهده بین المللی مورد پذیرش جامعه بین الملل در حوزه جنگ سایبری وجود ندارد ولی می توان قواعد حقوقی موجود را به موضوعات حوزه جنگ سایبری بار کرد.

امروزه مهم ترین منبع حقوق حاکم بر روابط بین الملل، منشور سازمان ملل متحد است. طبق بند ۲ ماده ٤ منشور ملل متحد «همه اعضای سازمان ملل متحد در روابطشان از تهدید یا استفاده از زور علیه تمامیت ارضی یا استقلال سیاسی هر دولتی، یا در هر روشی مغایر با اهداف سازمان ملل متحد خودداری خواهند کرد».

عرف بین الملل و هنجارهای کلی حقوق بین الملل، اتخاذ هرگونه رفتار مداخله جویانه و تخاصم‌آمیز در عرصه مجازی و تمسک به جنگ سایبری را به شدت تقبیح نموده است. با وجود چنین اصل خدشه‌ناپذیری در تقبیح مخاصمات سایبری، به دلیل ماهیت نامتمرکز و نامشخص بودن منشأ حملات سایبری، ظرفیت‌های حقوق بین‌الملل شاهد تکوین رویه منسجم، کارآمد و جامعی در این حوزه نیست. این امر برخی از محققان را به این باور سوق داده است که حقوق بین الملل کنونی جهت کارایی و تحقق نظم حقوقی بایسته، نیازمند

شکل گیری قواعد افتراقی حول مباحث مربوط به حقوق جنگ سایبری است. با وجود چنین دیدگاه قابل تأملی با ژرف نگری در مبانی حقوق بین الملل و معاهدات موجود می توان سلسله قواعد حاکم بر منازعات سایبری را استخراج نموده و مورد کنکاش قرار داد. با بررسی عرف حاکم بر روابط بین الملل و معاهدات بین المللی می توان اذعان داشت جنگ سایبری مصداقی از توسل به زور و مداخله در امور داخلی دولت ها به شمار می آید که می تواند به مسئولیت مباشران و دولت های حامی آن منتهی شود. نخستین معاهده ای که در پرتو اصول و قواعد عام آن، جنگ سایبری را می توان مورد بررسی قرار داد، «کنوانسیون های ژنو ۱۹۴۹ و پروتکل های الحاقی آن» است. به زعم بسیاری از مفسران و حقوقدانان، جنگ سایبری هم ردیف حملات مسلحانه بوده و تابع قواعد حاکم بر جنگ سنتی و مخاصمات مسلحانه است. همچنین طبق ماده ۳۰ «کنوانسیون بین المللی ارتباطات از راه دور»[1] هرگونه مداخله زیان بار با استفاده از فناوری های مخابرات و ارتباطات از راه دور ممنوع است. علاوه بر این، بند ٤ ماده ۲ منشور ملل متحد تمامی کشورها را از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی کشورهای دیگر و نیز اتخاذ هر نوع روشی که با مقاصد ملل متحد مباینت داشته باشد؛ منع نموده است. بنابراین حقوق بین الملل عام و معاهدات مزبور چارچوب قانونی و رویه حقوقی قابل استنادی در مورد اصول و قواعد حاکم بر جنگ سایبری را ارائه می دهد(نعمتی، ۱۳۹۷).

در صورتی که حمله سایبری به آستانه یک درگیری مسلحانه برسد، حقوق بین الملل بشردوستانه به اندازه کافی انعطاف دارد تا حملات سایبری نیز تحت پوشش آن قرار گیرند. حتی برخی علمای حقوق کیفری بر این اعتقاد هستند که بعضی از حملات سایبری اگر به آستانه‌ای از حمله مسلحانه برسند؛ مطابق با ماده ۵۱ منشور ملل متحد، دولت مورد حمله می تواند به دفاع مشروع متوسل شود (SHAKARIAN ET AL., 2013: 7).

با توجه به ویژگی های حملات سایبری، در صورتی که حملات سایبری در آستانه یک حمله مسلحانه قرار گیرد، می توان این حمله را نوعی از جنگ نامتقارن دانست که در این صورت حقوق بین الملل بشردوستانه قابلیت اعمال پیدا می کند. ممکن است حملات سایبری

1 .International Telecommunication Convention (ITC) .

در پاره‌ای از مواقع، به‌مثابه یک سلاح جنگی عمل کنند و به‌تبع 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 (جعفری و توتونچیان، ۱۳۹۸: ۳۳۳).

با اوصاف فوق می توان استنباط کرد که قواعد حقوق بین‌الملل بشردوستانه به‌عنوان بخشی از قواعد حقوق منازعات مسلحانه، قابلیت اعمال در حوزه جنگ سایبر را دارا است و به نظر می‌رسد توسل به آموزه‌ها و قواعد حقوق بین‌الملل بشردوستانه تا حدود زیادی می تواند آسیب ها و تهدیدهای ناشی از حملات سایبری را به حداقل برساند و برای جنگ‌ها و حملات جدید، قواعدی را معین کند.

اصل عدم توسل به زور به عنوان یکی از اصول مهم سازمان ملل متحد موضوع بند ٤ ماده ۲ منشور است و ممنوعیت طرح شده در آن هم فقط شامل کاربرد آن نیست، بلکه تهدید به کاربرد آن را نیز در برمی گیرد. همچنین منظور از زور، توسل به زور نظامی است و بنابراین فشارهای سیاسی یا اقتصادی از حوزه آن خارج می گردد (برادران و دیگران، ۱۳۹٦: ٢٤٤).

با این توجیه که امروز یکی از روش های نوین توسل به زور، حمله سایبری است که می تواند آثار مخربی به بار آورده و منجر به تخریب زیرساخت‌ها و حتی تلفات انسانی گردد می توان گفت که حملات سایبری با آثار مخرب فیزیکی جدی با نقض بند ٤ ماده ۲ منشور، توسل به زور غیرقانونی محسوب می شوند و در صورتی که به آستانه لازم برای ایجاد یک حمله مسلحانه برسند، در مقابل برای دولت قربانی حق دفاع مشروع از خود، طبق چارچوب مقرر در ماده ۵۱ منشور به وجود می‌آید.

در صورتی که خسارات وارده حمله سایبری باعث تخریب و ورود آسیب های جدی به زیرساخت های حیاتی کشور قربانی نشود، به گونه‌ای که نتوان آن را حمله مسلحانه به مفهوم کلاسیک تلقی کردد، می توان حمله سایبری صورت گرفته را مصداق مداخله در امور داخلی دولت‌ها از نوع خصمانه قلمداد نمود که طبیعتاً موجبات طرح مسئولیت بین‌المللی مرتکب یا مرتکبین آن حملات را فراهم خواهد نمود (برادران و دیگران، ۱۳۹٦: ۲۵۰).

قانون ۱۰ دستورالعمل تالین[1] نیز تأکید می‌کند: «این واقعیت که حملات سایبری فاقد شدت لازم ولی مختل کننده یا حملات شدید سایبری که زیرساخت های غیرحساس را مختل می‌کنند، نقض بند ٤ ماده ۲ تلقی نمی‌شود، به معنای مشروعیت آن‌ها نیست. حملات مذکور را زمانی که قابلیت انتساب به یک دولت را داشته باشند، می‌توان به‌مثابه نقض اصل عدم مداخله در امور داخلی دولت دیگر تلقی کرد» (Schmitt, 2013: 45).

مداخله غیرقانونی در موضوعاتی قابل طرح است که در رابطه با آن موضوعات، هر دولتی مجاز است طبق اصل حاکمیت ملی خود آزادانه راجع به آن‌ها تصمیم‌گیری نماید. ازجمله این موضوعات انتخاب یک سیستم سیاسی، اقتصادی، اجتماعی، فرهنگی خاص و نیز تدوین سیاست خارجی کشور است. مداخله زمانی غیرقانونی است که از این روش‌ها برای اعمال اجبار در جهت این انتخاب‌ها استفاده شود، انتخاب‌هایی که باید آزادانه صورت بگیرند، عنصر اجبار، شرط ایجاد یک مداخله غیرقانونی است. به این ترتیب مداخله زمانی صورت می‌گیرد که واجد شرایط اجبار شود و معمولاً به‌منظور ایجاد تغییر در سیاست‌های دولت هدف، اعمال گردد. درضمن اجبار به تنهایی برای ایجاد یک مداخله غیرقانونی کافی نیست و این اجبار باید در رابطه با موضوعی صورت گرفته باشد که دولت قربانی به طور آزادانه حق دارد، خود راجع به آن موضوع تصمیم‌گیری نماید (برادران و دیگران، ۱۳۹٦: ۲٤۸).

حملات سایبری صورت‌گرفته با هدف اجبار دولت قربانی به تغییر رفتار، در باب موضوعی که محق است خود به طور آزادانه راجع به آن تصمیم بگیرد، به دلیل مغایرت با اصل عدم مداخله در امور داخلی دولت دیگر، غیرقانونی محسوب شده و به دولت قربانی حق اعمال اقدام متقابل متناسب، مطابق با شروط و محدودیت های بیان شده در موارد ۵۰، ۵۱ و ۵۲ طرح مسئولیت دولت‌ها مورخ ۱۲ دسامبر ۲۰۰۱ را می‌دهد (ROSCINI, MARCO, OP.CIT: 114).

---

1. Tallinn Manual.

در خصوص موازین و هنجارهای حاکم بر جنگ سایبری، نخستین سند تخصصی و منبع بین‌المللی مدوّن تحت عنوان «دستورالعمل تالین در خصوص حقوق بین‌الملل قابل اجرا در جنگ سایبری» در سال ۲۰۱۳ میلادی توسط سازمان پیمان آتلانتیک شمالی (ناتو) تدوین یافت. با وجود آنکه دستورالعمل تالین از ماهیت الزام‌آوری برخوردار نبوده و یک سند ارشادی تلقی می‌شود؛ به عنوان راهنما و بارزترین الگو در جهت تدوین حقوق حاکم بر درگیری‌های اینترنتی و جنگ سایبری ارزیابی می‌شود.

نکته قابل تأملی که در خصوص شرایط حملات سایبری با آثار کمتر از حمله مسلحانه و تطبیق مصداق نقض اصل عدم مداخله بر این حملات وجود دارد این است که اگر بررسی حقوق بین‌الملل عرفی و رویه دولت‌ها نشان دهد که اجرای اجبار مجاز است، در این صورت نمی‌توان گفت که مداخله صورت‌گرفته غیرقانونی بوده است. با این اوصاف رویه دولت‌ها می‌تواند حوزه اصل عدم مداخله را تعیین کند.

از آنجایی که غالب حملات سایبری صورت‌گرفته با در نظر گرفتن معیار مضیق مندرج در منشور، به آستانه یک حمله مسلحانه نمی رسند، بنابراین می توان تحقق چنین حملاتی در فضای سایبر بر ضد سایر کشورها را نوعی اقدام متخلفانه غیر از توسل به زور و حمله مسلحانه تلقی نمود و در نتیجه با در نظر گرفتن حملات مذکور به عنوان اقدامی خلاف قواعد حقوق بین الملل، دولت قربانی قادر خواهد بود که بر ضد دولت خطاکار، تحت عنوان خودحمایتی به اقدامات متقابل متوسل گردد.

به طور خلاصه باید گفت حملات سایبری ای که منجر به آسیب فیزیکی می شوند مشمول اصل عدم توسل به زور که موضوع بند ٤ ماده ۲ منشور سازمان ملل متحد است می گردند و در صورتی که به آستانه لازم برای ایجاد یک حمله مسلحانه برسند، در مقابل برای دولت قربانی حق دفاع مشروع از خود، طبق چارچوب مقرر در ماده ۵۱ منشور به وجود می‌آید. در خصوص حملات سایبری‌ای که منجر به ایجاد صدمات فیزیکی نشوند، اما آثاری به بار می آورند که باعث می شود یک دولت مجبور به اتخاذ تصمیم در ارتباط با موضوعاتی شود که در چارچوب اعمال حاکمیت خود، حق دارد آزادانه در ارتباط با آن‌ها تصمیم بگیرد، ناقض اصل عدم مداخله بوده و بر اساس حقوق بین‌الملل عرفی، مداخله غیرقانونی محسوب می‌شوند و در مقابل برای دولت قربانی، حق توسل به اقدامات متقابل ایجاد می گردد.

۱۰. اصول اخلاقی حقوقی لازم‌الرعایه در جنگ سایبری

در ذیل قوانین و قواعد حقوقی بین المللی قابل اعمال بر حوزه جنگ سایبر که در بخش قبل به آن ها اشاره گردید، اصول اخلاقی ای وجود دارد که لازم است از سوی طرفین درگیر

در جنگ رعایت شود تا از ایراد خسارت غیرمتعارف به جامعه بشری و حتی صدمه و آسیب به غیرنظامیان ممانعت گردد یا این موارد را به حداقل رساند.

تئوری جنگ عادلانه[1] درباره اصول اخلاقی در جنگ، به‌طور کلی و به‌طور خاص در جنگ سایبری بحث می کند. در این تئوری به رفتارها در طول سه فاز مختلف جنگ شامل آغاز یک جنگ، حین و پایان جنگ نگریسته شده است. در هر یک از فازها لازم است اصول اخلاقی ای رعایت شود که در ادامه، به طور مختصر به اصول اخلاقی در هر فاز اشاره می‌شود(برگرفته از معاونت پژوهش و تولید علم، ۱۳۹۶: ۷۶۷-۷۵۷).

فاز آغاز جنگ شامل پنج اصل زیر است:

ـ **اصل حق قانونی**: در جنگ سایبری تنها مقامات قانونی یک دولت دارای اختیارات حقوقی برای به راه انداختن جنگ می باشند. این به آن معنی است که یک دولت که به طور کلی معادل یک کشور است تنها نهادی است که از نظر قانونی می‌تواند اعلان جنگ کند.

ـ **اصل حق اراده**: حق اراده در جنگ مشخص می کند که ما باید تنها در مواردی از زور استفاده یا تهدید به استفاده از آن کنیم که یک دلیل واقعاً درست داشته باشیم.

ـ **اصل احتمال موفقیت**: این اصل حکم می کند که زور نباید در تلاش برای یک جنگ بیهوده استفاده شود.

ـ **اصل گزینه آخر**: این اصل تصریح می کند که تنها زمانی باید از زور استفاده شود که دیپلماسی به شکست انجامیده یا عملی به نظر نمی‌رسد.

ـ **اصل تناسب**: این اصل در فاز آغاز جنگ بیان می کند که مزایای جنگ باید بیشتر از مضراتی باشد که توسط آن ایجاد می‌شود.

اصول اخلاقی در فاز حین جنگ شامل دو اصل زیر است:

ـ **اصل تمایز**: این اصل روش انجام جنگ را مشخص می کند؛ به این معنا که کدام اهداف قانونی هستند. به عبارت دیگر اصل تمایز مشخص می کند که جنگ نباید به سمت غیرنظامیان و احزاب بی‌طرف هدایت شود.

1 .Bellum Iustum.

ـ **اصل تناسب:** اصل تناسب در فاز حین جنگ به این معنا است که نمی توان به یک هدف مشروع حمله کرد و بدون علت، مقدار زیادی خسارت ناخواسته در مناطق اطراف آن ایجاد نمود.

اصول اخلاقی در فاز پس از جنگ را در سه اصل زیر می‌توان بیان نمود:

ـ **اصل پیگیری صلح پایدار:** این اصل اظهار می دارد که همانند شروع جنگ، صلح نیز باید توسط یک مقام مشروع، پیشنهاد و پذیرفته شود.

ـ **اصل پاسخگویی برای رعایت نکردن اصول اخلاقی:** این اصل برای پاسخگویی افراد در مورد رعایت نکردن اصول اخلاقی در جنگ سایبری است. یافتن فردی که مسئولیت پاسخگویی را بر عهده بگیرد مشکل خواهد بود.

ـ **اصل گرفتن غرامت:** این اصل، لزوم پرداخت غرامت از سوی مهاجم به قربانی را مورد تأکید قرار می‌دهد.

۱۱. چالش‌های حقوقی در حوزه جنگ سایبری

نظر به بررسی‌های صورت‌گرفته و نیز توضیحات ارائه‌شده در بخش‌های قبلی، چالش‌های حقوقی‌ای که در حال حاضر با آن مواجهیم را در موارد زیر می‌توان جمع‌بندی و خلاصه نمود:

ـ یک قانون جهانی مورد قبول همه کشورها در حوزه جنگ سایبری: به دلیل اختلاف‌نظر دولت‌ها، ترجیح منافع از سوی هر یک از دولت‌های عرصه بین‌الملل و نیز اعمال فشار و نفوذ از سوی قدرت‌های بزرگ، هنوز یک قانون یا معاهده جهانی در حوزه جنگ سایبری که مورد قبول همه کشورهای دنیا باشد شکل نگرفته است.

ـ نبود درک مشترک در خصوص قواعد حقوق بین‌الملل قابل اعمال بر رفتار دولت‌ها در حوزه فضای سایبر: به این دلیل که زبان استفاده‌شده برای نوشتن قوانین حقوق بین‌الملل، به‌سادگی قابل برگردان به فضای سایبری نیست، عمدتاً درک بین‌المللی پذیرفته‌شده‌ای از این مسئله وجود ندارد که چگونه قوانین مرتبط با جنگ در حوزه‌های فیزیکی (زمین، دریا، هوا و فضا) به حوزه جنگ سایبری اعمال می‌شوند.

ـ عدم تمایل دولت‌ها به ایجاد معاهدات و اسناد حقوقی الزام‌آور در حوزه جنگ‌ها و مناقشات سایبری: تلاش‌هایی با هدف ایجاد معاهدات و حقوق بین‌الملل در ارتباط با جرائم سایبری و جنگ سایبری صورت گرفته است، اما این تلاش‌ها بسیار کند پیش می‌روند. یک مانع بسیار مهم برای ایجاد اجماع در معاهدات سایبری، بی‌نام بودن ذاتی اینترنت است که هویت خلاف‌کاران را مخفی می‌کند و موجب می‌شود انتساب حملات به یک فرد یا گروه یا کشور مشخص سخت شود. به‌علاوه برخی مواقع بازیگرانی که خارج از کنترل یک دولت هستند حملاتی صورت می‌دهند که می‌تواند ضد حمله نامتناسب یک کشور را برانگیزد. این را جهت‌گیری غلط[1] می‌نامند. مشکل دیگر مربوط به جهت‌گیری غلط این است که مهاجمان می‌توانند به‌عمد، ردی از خود بر جای گذارند تا پای طرف‌های دیگر را به ورطه بکشانند. به همین دلیل کشورها مایل نیستند هیچ‌گونه سند حقوقی الزام‌آوری را امضا کنند که آن‌ها را مسئول فعالیت‌هایی می‌شناسد که چه‌بسا توسط کشورهای دیگر با فریب و نیرنگ به آن‌ها منتسب شود (معاونت پژوهش و تولید علم، ۱۳۹۶ الف: ۳۷).

ـ مشکل در انتساب حملات سایبری به دولت متخاصم و نبود قطعیت در این حوزه: یک مسئله مهم در جنگ سایبری، تعیین این است که چه کسی مسئول یک عملیات سایبری خاص است خواه می‌خواهد یک حمله، شناسایی یا سرقت اطلاعات باشد، این به‌عنوان مشکل انتساب شناخته می‌شود (SHAKARIAN ET AL., 2013).

طبق حقوق بین‌الملل اقدام به دفاع مشروع در هر حوزه‌ای ازجمله فضای سایبر، منوط به احراز حمله مسلحانه است و پیش‌شرط اصلی برای اینکه حملات سایبری را حملات مسلحانه تلقی نمود و طبق قوانین بین‌المللی با آن‌ها برخورد نمود این است که بتوان حمله سایبری را به یک دولت منتسب کرد.

در فضای سایبر، مسئله انتساب از مشکلات اصلی طرح مسئولیت دولت‌هایی است که حملات سایبری انجام می‌دهند، یا از آن حمایت می‌کنند (خلف رضایی، ۱۳۹۲: ۱۴۹).

چالش اصلی مسئله انتساب است. درواقع هر چند تشخیص مبدأ یا محل انجام حملات سایبری برای متخصصان چندان دشوار نیست، اما این واقعیت نمی‌تواند موجب انتساب

1 .Misdirection.

حمله به دولت مبدأ حمله شود؛ زیرا اعمال اشخاص خصوصی به دولت متبوع آن‌ها منتسب نخواهد شد مگر آنکه این موضوع اثبات شود (همان: ١٤٤).

فراتر از پنهان کردن منبع حمله به‌عمد، مهاجمان اقداماتی را می‌توانند انجام دهند تا حمله به منبع دیگری نسبت داده شود. استفاده از کشور یا سازمانی دیگر برای مخفی کردن منبع یک حمله می‌تواند به تنش یا حملات آشکار به سیستم‌هایی که مهاجم در پشت آن مخفی شده است منجر شود و به‌طور بالقوه به معنی درگیر کردن سپر بی‌خبر در جنگ است.

ـ تردید در چگونگی و سطح برخورد حقوقی با حملات سایبری در حقوق بین‌الملل به علت ویژگی‌های خاص حملات در عرصه سایبر: برخلاف حملات و جنگ‌ها در عرصه‌های نبرد زمینی، دریایی و هوایی، کنترل ارتش‌های سایبری، مشکل و غیرعملی خواهد بود و همین ضعف در کنترل نتایج ناخواسته حملات سایبری باعث ایجاد تردیدهایی در خصوص نحوه برخورد حقوقی با حملات سایبری شده است. از سوی دیگر مشکل عدم انتساب قطعی حملات به مهاجم و خودداری مهاجمان از پذیرش مسئولیت حمله در فضای سایبری، تردیدها در خصوص نحوه برخورد حقوقی در عرصه سایبری را افزایش داده است.

ـ نبود اشتراک نظر بین‌المللی در خصوص نحوه پاسخگویی به حملات سایبری: در فضای سایبری هیچ درک مشترکی از آنچه یک استفاده از زور یا اقدام جنگی در اینترنت شکل می‌دهد وجود ندارد، از این رو هیچ دکترین مورد توافق قرار گرفته‌ای برای نحوه مبارزه با یک جنگ سایبری وجود ندارد و اگر حمله‌ای وجود داشته باشد، پاسخ به مهاجم (در صورت تحقق انتساب) یکدست نخواهد بود.

ـ مشکل در انطباق اصل عدم مداخله در مورد حملات سایبری‌ای که به آستانه لازم برای ایجاد حمله مسلحانه نرسیده‌اند: تعیین معیار و ضابطه در برشمردن مصادیقی از حملات سایبری به‌عنوان نقض اصل عدم مداخله در حال حاضر، امری مورد اختلاف است هر چند که این موضوع نباید مانع اعمال اصل عدم مداخله در این‌گونه حملات باشد ولی اختلاف‌نظرهایی را به وجود می‌آورد که به کار بردن این اصل را با مشکل مواجه می‌کند.

ـ عدم بازدارندگی قوانین فعلی در حوزه جنگ سایبری و عدم مواجهه مهاجم با هزینه‌های بالا و پیامدهای سنگین در این عرصه از جنگ: جنگ‌های سایبری به علت ویژگی‌های خاص نظیر پایین بودن هزینه، بالا بودن سطح گمنامی، خطر پایین و پیامدهای ناچیز، از جذابیت کافی برای مهاجمان برخوردار بوده و خلأهای قانونی نیز بر این جذابیت افزوده است؛ بنابراین در شرایط حاضر، عوامل بازدارنده کافی در برابر جنگ سایبری وجود ندارد.

ـ نبود تدابیر اعتمادساز و به‌تبع آن عدم اعتماد کشورها به قواعد حقوق بین‌الملل فعلی در حوزه جنگ سایبری: با وجود امکان اعمال معاهدات و نظام حقوقی بین‌الملل فعلی به حوزه جنگ سایبری، معضل عدم پایبندی برخی کشورها به تعهدات و اصول و قواعد فعلی، بروز کرده و به‌تبع آن عدم اعتماد بقیه کشورها به ضوابط فعلی را در پی داشته است.

ـ عدم امکان تعمیم حقوق مخاصمات مسلحانه به حملات از سوی عوامل غیردولتی: حقوق مخاصمات مسلحانه، به‌عنوان بخشی از حقوق بین‌الملل، تنها محدود به دولت‌ها است. با این حال تخلف ممکن است همچنین پیگیری افراد برای جنایات جنگی را در برگیرد.

لزوماً دولت‌ها طرف درگیری نیستند، بلکه گروه‌ها و سازمان‌های غیردولتی و حتی افراد می‌توانند در این فضا به امنیت ملی قدرتمندترین دولت‌ها صدمه وارد کنند و امنیت اقتصادی و انسانی آن‌ها را با خطر مواجه کنند. برخی حملات سایبری می‌توانند به تلفات انسانی به غیرنظامیان منجر بشوند و جان عده زیادی را با خطر مواجه کنند (عباسی و مرادی، ۱۳۹٤: ٦٦).

چنانچه حملات سایبری صرفاً از سوی اشخاص خصوصی ارتکاب یابد و امکان انتساب آن به دولتی وجود نداشته باشد با مفهوم جرم سایبری مواجه خواهیم بود که به احتمال زیاد مصداقی از جرم سابوتاژ یا خرابکاری خواهد بود و در این خصوص باید به قوانین داخلی کشورها رجوع کرد.

ـ مشکل در اثبات کنترل یک دولت بر بازیگران غیردولتی درگیر در مخاصمات بر ضد دولت دیگر: یک مخاصمه زمانی که بازیگران غیردولتی درگیر در مخاصمات بر ضد دولت تحت کنترل کلی یک دولت دیگر باشند نیز بین‌المللی تلقی می‌شود. ولی در چنین مواردی

اثبات اینکه آیا یک دولت فعالیت‌های سایبری یک بازیگر غیردولتی را کنترل می‌کند امری مشکل خواهد بود (Schmitt, 2013: 79).

ـ نبود اجماع بین‌المللی در خصوص تعریف جنگ سایبری: فقدان تعریفی مشخص و جامع‌الاطراف، نه‌تنها مسیر حقوقی پیش رو را مبهم می‌نماید، بلکه منجر به نوعی تشتت آرا و تنوع و چندگانگی در تفسیر و رویه عملی و سرانجام نیل به نتایج حقوقی بعضاً متناقض خواهد گردید (اصلانی و رنجبریان، ۱۳۹٤: ۲۵۹).

این موضوع که از نبود تعریف مشخص از فضای سایبری و جنگ نشأت می‌گیرد تعیین مصادیق جنگ سایبری را مشکل نموده و منجر به بروز ابهام در تعیین معیارها و شاخص‌های به رسمیت شناختن یک حمله یا مناقشه سایبری به‌عنوان جنگ سایبری شده است. به‌تبع این موضوعات، اعمال قوانین جنگی بر اغلب حملات و مناقشات سایبری با چالش‌ها و ابهاماتی مواجه است.

ـ همگام نبودن رشد نظام‌های حقوقی با رشد سریع فناوری‌های حوزه فضای سایبر و بروز مشکلات و چالش‌های جدید حقوقی در خصوص فناوری‌های جدید فضای سایبر: یکی از چالش‌های مهم در برخورد با عرصه‌های فناورانه نوظهور، عقب ماندن نظام‌های حقوقی است. این موضوع علل متعددی می‌تواند داشته باشد که ازجمله آن‌ها به عدم آشنایی متخصصان این فناوری‌ها با علم حقوق، بیگانه بودن اغلب متخصصان علم حقوق با فناوری‌های نوظهور، نگرانی‌ها در خصوص مانایی فناوری‌ها و نحوه تقابل و برخورد جامعه با آن‌ها و درنهایت تردید در لزوم تدوین نظام‌های حقوقی خاص برای این‌گونه فناوری‌ها می‌توان اشاره کرد.

۱۲. راهکارهای رفع چالش‌های حقوقی بین‌المللی جنگ سایبری

متناظر با چالش‌های مطروحه در بخش قبل، می‌توان راهکارهای زیر را برای رفع چالش‌های حقوق بین‌الملل در حوزه جنگ سایبری ارائه نمود:

ـ شکل‌گیری یک رژیم حقوقی مشترک جهانی مورد توافق اکثر کشورهای جهان زیر سازمان ملل: اصول حقوق بین‌الملل بشردوستانه می‌تواند حاکم بر فضای عمومی جنگ

سایبر باشد، اما حوزه جنگ سایبری نیازمند تدوین قوانین تخصصی‌تر و کارآمدتری است تا بتواند در صحنه‌های جنگ نیز کارایی داشته باشد.

با توجه به ویژگی‌های خاص و متفاوت فضای سایبر و از آنجا که عوامل متعددی، کنترل فضای سایبر را با مشکل مواجه می‌کنند و نیز نبود درک مشترک در خصوص قواعد حقوق بین‌الملل قابل اعمال بر رفتار دولت‌ها در این حوزه، بهتر است که اعضای جامعه بین‌المللی هر چه سریع‌تر معاهده‌ای جامع در خصوص قواعد حاکم بر جنگ‌های سایبری منعقد کنند (برادران و حبیبی، ۱۳۹۸: ۱۵۵).

ـ بازبینی نحوه اجرا و یا تفسیر قوانین فعلی موجود در حوزه منازعات و مناقشات و تطبیق آن‌ها با وضعیت منازعه و جنگ در فضای سایبر یا به عبارتی تعمیم قوانین موجود در حوزه حقوق بین‌الملل نظیر حقوق بشردوستانه به جنگ سایبری: این مهم با مشارکت جامعه بین‌الملل ممکن و میسر خواهد شد البته زیاده‌خواهی ابرقدرت‌ها و دیدگاه قیم‌مآبانه آن‌ها نیز در این خصوص باید تعدیل شود تا اجماع جهانی حاصل شود و الا همچنان این موضوع بلاتکلیف خواهد ماند.

فضای سایبر امروزه بخشی انکارناپذیر از زندگی بشر را تشکیل می‌دهد و دولت‌ها که مدت‌ها خود را محصور در مرزهای ملی و حاکم بر فضای بین این مرزها تلقی می‌کردند، ناگزیر از پذیرش واقعیت این فضای بدون مرز هستند و بی‌تردید روابط بین آن‌ها در این فضا نیز بر اساس حقوق بین‌الملل فعلی قابل تنظیم بوده و حقوق بین‌الملل بر رفتار دولت‌ها در فضای سایبر نیز قابل اعمال است.

برخی معتقدند اولین قدم در رویارویی و مقابله با حملات سایبری، شباهت‌سازی قواعد موجود با ساختار و ویژگی‌های حملات سایبری است. اصل شباهت‌سازی به لحاظ فنی و پاسخگویی دولت‌ها و نظام‌های سیاسی در عرصه بین‌الملل، به شکل قابل توجهی می‌تواند به تدوین قوانینی در زمینه حملات سایبری منجر شود (جعفری و توتونچیان، ۱۳۹۸: ۳٤۱).

با توجه به نوپا بودن 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 مراجعه نمود (همان: ۳۳۹).

از آنجا که به‌واسطه جدید بودن پدیده، هنوز مقررات‌گذاری ویژه‌ای در خصوص استفاده از فضای سایبر به‌عنوان محمل اقدامات خصمانه صورت نگرفته و تلاش‌های ابتدایی در رویه‌سازی (مانند تدوین دستورالعمل تالین از سوی ناتو) واجد اثر حقوقی لازم نیستند، لاجرم باید از اصول و قواعد کلی حقوق بین‌الملل بشردوستانه برای تنظیم روابط خصمانه در فضای سایبر استفاده کرد (برادران و حبیبی، ۱۳۹۸: ۱۵۵).

با وجود جدید بودن عملیات سایبری نسبت به معاهدات حقوق بین‌الملل بشردوستانه و نبود قواعد معین و مشخص در حقوق جنگ که به‌طور واضح و مشخص در خصوص حملات سایبری وضع شده باشند، قواعد حقوق مخاصمات مسلحانه در چنین مواردی چه در مخاصمات بین‌المللی و چه داخلی قابل به کار بردن هستند (همان: ۱٤٤-۱٤۳).

با توجه به توضیحات فوق، تا زمانی که قواعد خاص حقوق بشردوستانه بین‌المللی در مخاصمات سایبری تدوین نشده باشد، همچنان می‌توان با توسل به اصول و قواعد موجود، روش‌های نبرد سایبری را در چارچوب حقوق موجود بین‌المللی نظیر حقوق بین‌الملل بشردوستانه به نظم درآورد.

ـ همکاری نزدیک و مساعدت دولت‌ها و سازمان‌ها و نهادهای بین‌المللی برای مقابله با حملات سایبری و شکل‌گیری پیمان‌ها و معاهدات حقوق الزام‌آور در عرصه جنگ سایبری: همکاری‌های بین‌المللی در سطوح منطقه‌ای و جهانی می‌تواند در مقابله با حملات سایبری که پدیده‌ای بدون مرز است، نقش مؤثری ایفا نماید. این مهم با محور قرار گرفتن سازمان‌های بین‌المللی ازجمله سازمان ملل متحد و نیز ایفای نقش از سوی تمامی بازیگران عرصه سایبری جهان اعم از دولت‌ها و سازمان‌ها و شرکت‌های فعال در حوزه فضای سایبر، میسر خواهد بود.

ـ تدوین ساختار، سازوکار و امکانات لازم برای شناسایی و انتساب حملات سایبری: این موضوع علاوه بر فراهم نمودن زیرساخت‌های فنی و سامانه‌های لازم، نیازمند همکاری و تشریک‌مساعی همه دولت‌ها در سطح بین‌الملل است.

در سطح بین‌الملل نیاز است توافقنامه‌ها و فرایندهایی برای چاره‌جویی درباره انتساب، زنجیره تأمین و مسائل حقوقی شکل بگیرد.

ـ تعیین نوع و شکل مناسب و سطح بازدارنده واکنش و پاسخگویی به حملات سایبری در نظام حقوق بین‌الملل، با در نظر گرفتن ضمانت اجرای لازم: ضرورت دارد این موضوع در رژیم حقوقی مشترک جهانی که در این عرصه تنظیم می‌گردد دیده شود. در این خصوص لازم است قواعد مشخصی درباره آنچه یک حادثه یا حمله را شکل می‌دهد و نوعی از پاسخ (فنی، حقوقی یا سیاسی) که باید به اجرا دربیاید به صراحت بیان شود.

ـ داشتن یک راهبرد یا خط‌مشی حقوقی باثبات و به‌هم‌پیوسته کشوری برای پاسخگویی به حملات سایبری و اعلام رسمی آن از سوی حاکمیت: در شرایط فعلی لازم است برای ایجاد بازدارندگی از حملات سایبری، راهبرد کشورها در خصوص نحوه پاسخگویی به حملات سایبری، به‌صورت شفاف اعلام شود. این مهم هم‌اکنون با بیانیه اخیر ستاد کل نیروهای مسلح جمهوری اسلامی ایران در قبال حقوق بین‌الملل فضای سایبری، در کشورمان محقق شده است.

داشتن راهبرد یا خط‌مشی مناسب، نحوه پاسخگویی در برابر حملات سایبر را برای متولیان داخلی شفاف و روشن نموده و اعلام رسمی آن نیز منجر به ایجاد بازدارندگی در برابر اقدامات مهاجمان برای حمله سایبری به کشور خواهد شد.

ـ بررسی موردی حملات سایبری ناقض اصل عدم مداخله در دادگاه صالحه بین‌المللی: تا زمان تعیین ضوابط و معیارهای انطباق نقض اصل عدم مداخله در حملات سایبری از سوی جامعه بین‌الملل، نمی‌توان وضعیت حقوقی چنین حملاتی را در هاله‌ای از ابهام قرار داد. به نظر می‌رسد که در حال حاضر چاره‌ای جز توسل به رویکرد بررسی موردی آثار و تبعات ثانویه حملات سایبری وجود ندارد و حداقل نتیجه این اقدام، آن است که جامعه بین‌المللی، موضعی منفعل و خنثی در قبال حملات سایبری ناقض اصل عدم مداخله نداشته و همین موضع می‌تواند منجر به بازدارندگی از بروز بسیاری از حملات سایبری گردد.

ـ بالا بردن هزینه‌های جنگ و مناقشه سایبری در جامعه بین‌الملل: اگر بتوان حملات سایبری را گران و پرهزینه یا پیامدهای آن را بسیار دردناک نمود، کسی از آن استفاده

نخواهد کرد. این ایده در حوزه هسته‌ای جواب داد؛ زیرا هزینه ورود بـه باشـگاه توانمنـدی هسته‌ای گران بود و اعضای باشگاه همه متعهد بودند اجازه ورود به دیگران را ندهند.

ـ اتخاذ تدابیر اعتمادساز در معاهدات، توافقنامه‌ها یا بیانیه‌های مرتبط با جنگ سـایبر: در کنار ضابطه‌مند کردن اسـتفاده از فضـای سـایبر در حـوزه حقـوق بـین‌الملـل، بایـد تـدابیر اعتمادساز نیز در هر معاهده یا بیانیه‌ای پیش‌بینی گردد. اتخاذ تـدابیر اعتمادسـاز در جامعـه بین‌الملل، علاوه بر جلب اعتماد کشورها می‌تواند زمینه و مقدمه‌ای بـرای عقـد پیمـان‌هـای بین‌المللی نهایی در حوزه فضای سایبر گردد.

جان براوسکی[1] تدابیر اعتمادساز را به سه دسته تقسیم می‌کند (Brewski, 1986):

۱- محدودیت‌ها؛ ۲- تبادل اطلاعات و ۳- نظارت و تحقیق.

محدودیت‌ها، فعالیت‌های مربوط را از طریق تنظیم مقرراتـی کـه کجـا، کـی و چگونـه صورت پذیرند، محدود می‌نمایند. هدف از تبادل اطلاعات، افزایش آگـاهی‌هـای دو طـرف در مورد راهبردها و اقدامات مربوط است و درنهایت تحقیق و نظارت باعث مـی‌شـود کـه ارزیابی مستقل و قابل اعتمادی از نوع و ماهیت اقـدامات طـرفین صـورت پـذیرد. بـا ایـن اوصاف، هر کشوری برای فعالیت در فضـای سـایبر بایـد محـدودیت‌هـایی را طبـق نظـام پایبندی در تعهدات بپذیرد و در هنگام تبادل اطلاعات شـفافیت داشـته باشـد و در مراحـل تحقیق و نظارت با سازمان‌ها و نهادهـای مربوطـه همکـاری لازم را داشـته باشـد (جعفـری و توتونچیان، ۱۳۹۸: ۳٤۱-۳٤۰).

ـ مسئولیت‌پذیر و متعهد نمودن کشورها بـه کنتـرل عوامـل غیردولتـی در حمـلات سایبری و لزوم پاسخگویی آن‌ها بـه حمـلات ایـن عوامـل بـه زیرسـاخت‌هـا و منـافع کشورهای دیگر: در حقوق عرفی، دولت‌هـا در کشورشـان مکلـف‌انـد جلـو حمـلات مسلحانه غیردولتی‌ها را بر ضد دولت دیگر بگیرند؛ بنابراین دولتی که بـه پیشـگیری از چنین حملاتی قادر باشد، در صورت کوتاهی از انجام تعهـد، طبـق حقـوق بـین‌الملـل مسئولیت خواهد داشت (خلف رضایی، ۱۳۹۲: ۱٤٦).

1 .Joan Brewski.

برای تحقق این مهم نیز ضرورت دارد تدابیر و سازوکارهای لازم در رژیم حقوقی مشترک جهانی حوزه سایبر یا در بازنگری قوانین فعلی و تعمیم آن‌ها به حوزه جنگ سایبری اتخاذ گردد.

ـ تعریف روشن و دقیق جنگ سایبری در یک اجماع یا از سوی یک نهاد صالحه بین‌المللی و تعیین مصادیق و شاخص‌های آن: در این خصوص لازم است حدود و آستانه هر شاخص برای رسمیت شناختن یک حمله یا مناقشه سایبری به‌عنوان جنگ سایبری مشخص شود.

ـ همکاری و تعامل نزدیک متخصصان حقوق و فضای سایبری در عرصه بین‌الملل به‌منظور تسریع در تنظیم قواعد حقوقی حوزه فضای سایبر.

۱۳. نتیجه‌گیری

با ظهور فضای سایبر، یک مرحله تمدنی جدید در زندگی بشر آغاز گردید و زیست‌بوم جدیدی شکل گرفت که به تعبیر برخی صاحب‌نظران، امتداد زندگی بشر را به این فضا برد، فضایی که هر صاحب قدرتی در پی دست‌اندازی و تصاحب سهم بیشتری از آن برای خود است.

ویژگی‌های خاص و کارکردهای ویژه فضای سایبر، آن را در کنار مؤلفه‌های اصلی قدرت قرار داده و حاکمیت‌ها و دولت‌ها و حتی سازمان‌ها و گروه‌های غیردولتی را به دستیابی به قدرت سایبری ترغیب نموده است. شکی نیست که هم‌اکنون فضای سایبر به‌عنوان عرصه پنجم نبرد و جنگ، جایگاه خود را پیدا کرده است و غفلت از این عرصه خسارت‌ها و پیامدهای ناگواری را در پی خواهد داشت.

هنوز تعریف مشخصی برای فضای سایبر و نیز جنگ وجود ندارد؛ بنابراین تعریف جنگ سایبری آسان نخواهد بود. جنگ سایبر در ساده‌ترین تعریف به‌عنوان «استفاده از رایانه و اینترنت برای جنگیدن در فضای سایبر تعریف شده است»؛ اما به صورت جزئی تر اصطلاح جنگ سایبر به جنگ انجام گرفته در فضای سایبر از طریق ابزارها و روش های سایبری اشاره دارد.

ویژگی‌ها و مزایای جنگ سایبری را در مواردی نظیر هزینه کم، دسترسی آسان از راه دور و به‌صورت غیرفیزیکی، انتساب دشوار، قوانین کم حاکم بر آن و خطرات کمتر در برابر مزایای آن برای مهاجم می‌توان خلاصه نمود. این ویژگی‌ها، جنگ‌های سایبری را برای دولت‌ها و حتی گروه‌های غیردولتی جذاب نموده و اقبال به این نوع جنگ را افزایش داده است.

در حوزه مباحث حقوق بین‌الملل، به‌طور کلی می‌توان گفت که هیچ اصل و قاعده بین‌المللی پذیرفته شده مختص جنگ سایبری وجود ندارد؛ اما این دلیل نمی‌شود که نتیجه گیری کنیم حوزه جنگ سایبری، به کل، فاقد قاعده و قانون است، بلکه باید گفت که هم‌اکنون قوانینی در سایر حوزه‌های حقوق بین‌الملل وجود دارد که فارغ از خلأهای قانونی موجود و نبود قوانین بین المللی اختصاصی حوزه جنگ سایبری، بر این حوزه قابل اعمال و تعمیم است.

ازجمله قوانین بین‌المللی موجود، قواعد حقوق بین‌الملل بشردوستانه است که به‌عنوان بخشی از قواعد حقوق منازعات مسلحانه، قابلیت اعمال در حوزه جنگ سایبر را دارا است. حملات سایبری ای که منجر به آسیب فیزیکی می شوند مشمول اصل عدم توسل به زور که موضوع بند ٤ ماده ٢ منشور سازمان ملل متحد است می گردند و در صورتی که به آستانه لازم برای ایجاد یک حمله مسلحانه برسند، در مقابل برای دولت قربانی حق دفاع مشروع از خود، طبق چارچوب مقرر در ماده ۵۱ منشور به وجود می آید. در خصوص حملات سایبری‌ای که منجر به ایجاد صدمات فیزیکی نشوند، اما آثاری به بار می آورند که باعث می‌شود یک دولت مجبور به اتخاذ تصمیم در ارتباط با موضوعاتی شود که در چارچوب اعمال حاکمیت خود، حق دارد آزادانه در ارتباط با آن ها تصمیم بگیرد، ناقض اصل عدم مداخله بوده و بر اساس حقوق بین الملل عرفی، مداخله غیرقانونی محسوب می شوند و در مقابل برای دولت قربانی، حق توسل به اقدامات متقابل ایجاد می‌گردد.

در کنار قوانین بین‌المللی قابل اعمال بر حوزه جنگ سایبری، دستورالعمل تالین به‌عنوان یک سند تخصصی در خصوص موازین و هنجارهای حاکم بر جنگ سایبری است که هر چند از ماهیت الزام‌آوری برخوردار نیست و یک سند ارشادی تلقی می‌شود ولی می‌تواند

به‌عنوان یک راهنما و بارزترین الگو در جهت تدوین حقوق حاکم بر درگیری‌های اینترنتی و جنگ سایبری مورد بهره‌برداری قرار گیرد.

در ذیل قوانین و قواعد حقوق بین‌الملل قابل اعمال بر حوزه جنگ سایبر، اصول اخلاقی‌ای وجود دارد که لازم است از سوی طرفین درگیر در مناقشات سایبری رعایت شود تا از ایراد خسارت غیرمتعارف به جامعه بشری و صدمه و آسیب به غیرنظامیان ممانعت گردد این اصول اخلاقی که در تئوری جنگ عادلانه مورد بحث قرار می‌گیرند عبارت‌اند از: حق قانونی، حق اراده، احتمال موفقیت، گزینه آخر، تناسب، تمایز، پیگیری صلح پایدار، پاسخگویی برای رعایت نکردن اصول اخلاقی و گرفتن غرامت.

با وجود موارد پیش‌گفته، چالش‌های حقوقی اساسی در حوزه جنگ سایبری وجود دارد که مهم‌ترین آن‌ها را در نبود قانون جهانی پذیرفته‌شده جهانی، ابهام در اعمال قوانین فعلی بر حوزه جنگ سایبری، عدم تمایل دولت‌ها به ایجاد معاهدات حقوقی، مشکل بودن انتساب در حملات سایبری، ابهام در نحوه برخورد حقوقی و واکنش در برابر جنگ سایبری، عدم امکان تعمیم حقوق بین‌الملل به حملات از سوی عوامل غیردولتی، نبود اجماع در خصوص تعریف جنگ سایبری و همگام نبودن رشد نظام‌های حقوقی با رشد فناوری‌های حوزه سایبر می‌توان خلاصه نمود.

فراخور هر یک از چالش‌های حقوق بین‌الملل در حوزه جنگ سایبری، راهکارهایی را می‌توان ارائه نمود که به‌طور خلاصه عبارت‌اند از: شکل‌گیری یک رژیم حقوق مشترک جهانی، بازبینی نحوه اجرا یا تفسیر قوانین فعلی، همکاری نزدیک و مساعدت دولت‌ها و سازمان‌ها و نهادهای بین‌المللی، تدوین ساختار، سازوکار و امکانات لازم برای شناسایی و انتساب حملات سایبری، داشتن یک راهبرد یا خط‌مشی حقوقی باثبات و به‌هم‌پیوسته کشوری و اعلام آن، بالا بردن هزینه‌های جنگ و مناقشه سایبری، مسئولیت‌پذیر و متعهد نمودن کشورها به کنترل عوامل غیردولتی، تعریف روشن و دقیق جنگ سایبری، همکاری و تعامل نزدیک متخصصان حقوق و فضای سایبری در عرصه بین‌الملل.

در پایان باید خاطرنشان ساخت که جمهوری اسلامی ایران ازجمله کشورهایی است که آماج حملات سایبری و به تعبیری جنگ سایبری قرار گرفته است. ارسال انواع بدافزارهای

جاسوسی به تأسیسات هسته‌ای و صنعتی ایران با هدف از کار انداختن زیرساخت‌های کشور، لطمه به منافع ملّی و تزلزل امنیت سایبری تنها یکی از ابعاد جنگ سایبری بر ضد کشور است. در ۲۰ مارس ۲۰۱۳ میلادی مرکز جنگ سایبری ناتو حملات سایبری آمریکا و رژیم صهیونیستی بر ضد جمهوری اسلامی ایران در سال ۲۰۰۹ میلادی را مصداق استفاده از زور ارزیابی نمود؛ بنابراین کشور ایران به‌عنوان قربانی جنگ سایبری می‌تواند در پیگیری حقوقی حملات مزبور ضمن اثبات انتساب حملات سایبری و احراز منبع جنگ سایبری اقداماتی از قبیل رجوع به دیوان بین‌المللی دادگستری و مطالبه غرامت را اتخاذ نماید. پرواضح است که در کنار چنین سازوکارهای حقوقی با تقویت سرمایه ملّی سایبری و غنای سامانه‌های پدافند سایبری می‌توان همانند مقابله با تهدیدات گذشته، بر هجمه و تهدیدات سایبری نیز فائق آمد.

۱٤. پیشنهادها

به‌عنوان ادامه پژوهش می‌توان هر یک از چالش‌های حقوقی جنگ سایبری و نیز راهکارهای ارائه‌شده برای رفع چالش‌های حقوقی بین‌المللی جنگ سایبری را به‌عنوان یک موضوع پژوهشی، مورد مداقه قرار داد و در خصوص چگونگی پیاده‌سازی هر یک از راهکارهای مطروحه، به ارائه طرح یا الگو پرداخت.

به‌طور مثال مواردی نظیر: ارائه طرح راهبردی برای شکل‌گیری رژیم حقوقی مشترک جهانی برای جنگ سایبری، ارائه الگوی انتساب حملات سایبری، امکان‌سنجی تدوین میثاق بین‌المللی حقوق فضای سایبر و ارائه الگوی ارزیابی جنگ سایبری از منظر حقوق بین‌الملل را می‌توان به‌عنوان موضوعات پیشنهادی آتی مطرح نمود.

فهرست منابع و مآخذ

الف. منابع فارسی

- اندیشگاه شریف و اندیشکده کاوشگران آینده (۱۳۸٤)، **جنگ و دفاع سایبر**: پروژه الزامات جنگ‌های نوین در فضای سایبر، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.
- عبدالله‌خانی، علی (۱۳۸٦)، **جنگ نرم ۳؛ نبرد در عصر اطلاعات**، تهران: مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی معاصر.
- معاونت پژوهش و تولید علم (۱۳۹٦)، **رهیافت‌هایی نو در جنگ سایبری**، جلد اول، چاپ اول، تهران: انتشارات دانشگاه اطلاعات و امنیت ملی.
- معاونت پژوهش و تولید علم (۱۳۹٦)، **رهیافت‌هایی نو در جنگ سایبری**، جلد دوم، چاپ اول، تهران: انتشارات دانشگاه اطلاعات و امنیت ملی.
- ناتان‌شاو، مالکوم (۱۳۹۵)، **حقوق مخاصمات مسلحانه** (مترجمان سیده لطیفه حسینی و نرگس‌سادات حسینی)، تهران: نشر خرسندی.
- اسمعیل‌زاده ملاباشی، پرستو؛ عبداللهی، محسن و زمانی، سید قاسم (۱۳۹٦)، **حملات سایبری و اصول حقوق بین‌الملل بشردوستانه (مطالعه موردی: حملات سایبری به گرجستان)**، فصلنامه مطالعات حقوق عمومی، دوره ٤۷، شماره ۲، (تابستان ۱۳۹٦)، صص ۵۵۹-۵۳۷.
- اصلانی، جبار و رنجبریان، امیرحسین (۱۳۹٤)، **بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه- کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل**، فصلنامه تحقیقات حقوقی، ۱۸(۷۱)، ۲۷۸-۲۵۷.
- امیرلی، حسین و ثقفی، کامیار (۱۳۹۸)، **ارائه مدل مفهومی ارزیابی تهدیدات تروریسم سایبری**، فصلنامه علمی امنیت ملی، ۹(۳۳)، ٤۲٤-۳۸۹.
- برادران، نازنین و حبیبی، همایون (۱۳۹۸)، **قابلیت اعمال قواعد حقوق بین‌الملل بشردوستانه در جنگ‌های سایبری**، فصلنامه مطالعات حقوق عمومی، دوره ٤۹، شماره ۱، (بهار ۱۳۹۸)، صص ۱۵۸ - ۱۳۹.
- برادران، نازنین؛ حبیبی، همایون؛ زمانی، سید قاسم و هنجی، سید علی (۱۳۹٦)، **کاربرد اصل عدم مداخله در امور داخلی دولت‌ها در حملات سایبری**، فصلنامه پژوهش‌های سیاسی و بین‌المللی، سال هشتم، شماره ۳۳، (زمستان ۱۳۹٦)، صص ۲٦۷ - ۲٤۱.
- حسینی، پرویز و ظریف‌منش، حسین (۱۳۹۲)، **مطالعه تطبیقی ساختار دفاع سایبری کشورها**، فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین (ع)، سال دوم، شماره ۵، (بهار ۱۳۹۲)، صص ٦۸ - ٤۱.

- جعفری، افشین و توتونچیان، مهری (۱۳۹۸)، **بررسی راهکارهای تحدید حملات سایبری از منظر حقوق بین‌الملل بشردوستانه**، مجله اخلاق زیستی، ویژه‌نامه حقوق بشر و حقوق شهروندی، (۱۳۹۸)، صص ۳٤۲ - ۳۳۱.
- جعفری، محسن و اسدی، فاطمه (۱۳۹۷)، **بررسی ابعاد حقوقی جنگ سایبری با نگاهی به قواعد حاکم بر مخاصمات مسلحانه بین‌المللی**، فصلنامه مطالعات علوم سیاسی، حقوق و فقه، دوره ٤، شماره ۲، (تابستان ۱۳۹۷)، صص ٦۳-۵۷.
- خلف رضایی، حسین (۱۳۹۲)، **حملات سایبری از منظر حقوق بین‌الملل (مطالعه موردی: استاکس‌نت)**، فصلنامه مجلس و راهبرد، سال بیستم، شماره ۷۳، (بهار ۱۳۹۲)، صص ۱۵۳ - ۱۲۵.
- صلاحی، سهراب و کشفی، سید مهدی (۱۳۹۵)، **جنگ سایبری از نظر حقوق بین‌الملل با نگاه به دستورالعمل تالین**، دو فصلنامه علمی-پژوهشی مطالعات قدرت نرم، سال ششم، شماره ۱٤، (بهار و تابستان ۱۳۹۵)، صص ٤۷ - ۲۸.
- عباسی، مجید و مرادی، حسین (۱۳۹٤)، جنگ سایبر از منظر حقوق بین‌الملل بشردوستانه، فصلنامه مجلس و راهبرد، سال بیست‌ودوم، شماره ۸۱، (بهار ۱۳۹٤)، صص ٦۸-۳۷.
- فرحبخت، احمدرضا و دهقانی، مهدی (۱۳۹۸)، **همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی**، فصلنامه امنیت ملی، سال نهم، شماره ۳۱، (بهار ۱۳۹۸)، صص ۲۱۹ - ۱۹۹.
- قاسمی، علی و بارین چهاربخش، ویکتور، (۱۳۹۱)، **حملات سایبری و حقوق بین‌الملل**، مجله حقوقی دادگستری، شماره ۷۸، (تابستان ۱۳۹۱)، صص ۱٤۵-۱۱۵.
- قاسمی، فرهاد و اسماعیلی فرزین، ایرج (۱۳۹٦)، **جنگ هیبریدی در سیستم بین‌المللی پیچیده-آشوبی**، فصلنامه مدیریت نظامی، سال هفدهم، شماره ۲، (تابستان ۱۳۹٦)، صص ۹۲-۵۲.
- محمدی، علی (۱۳۹٦)، **فضای سایبر: مفاهیم، امنیت، دفاع و استانداردها**، کتاب منتشرنشده دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی.
- نعمتی، لیلا (۱۳۹۷)، **واکاوی جنگ سایبری در پرتو معاهدات بین‌المللی**، برگرفته از https://www.papsa.ir.
- سازمان پدافند غیرعامل کشور (۱۳۹٤)، **سند راهبردی پدافند سایبری کشور**.
- مرکز فضای مجازی نیروهای مسلح (۱۳۹۹)، **بیانیه ستاد کل نیروهای مسلح جمهوری اسلامی ایران در قبال حقوق بین‌الملل فضای سایبری**.

ب. منابع انگلیسی

- Betz, David, (2012), **Cyberpower and international security**, Foreign policy research institute.
- Brewski J, (1986), **Avoiding War in the Nuclear age**, Boulder: Westview Press.
- James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko, (2014), **Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations ۲**, available at www.ewi.inf۰
- Johnson, Thomas A, (2015), **CyberSecurity: Protecting Critical Infrastuctures from Cyber Attack and Cyber Warefare**, CRC Press.
- Kulesza, Joanna, (2009), **State Responsibility for Cyber-attacks on International Peace and Security,** Polish Yearbook of International Law, Vol. XXIX, Electronic Copy Available at: http://ssrn.com/abstract=1668020
- Maurer, Tim, (2011), **Cyber Norm Emergence at the United Nations- An Analysis of the UN's Activities Regarding Cyber-security**, Belfer Center for Science and International Affairs.
- Ralph, Langner, (2013), **To Kill a centrifuge: a technical analysis of what Stuxnet's creators tried to achieve,** Langner anistitude.
- Rid, T, (2013), **Cyber War Will Not Take Place**, New York: Oxford University Press.
- Roscini, Marco, (2010), **World Wide Warfare- Jus ad Bellum and Use of Cyber Force**, Max Plank Yearbook of United Nations Law, Vol.14.
- Schmitt, M. N, (2013), **Tallinn manual on the international law applicable to cyber warfare**, Cambridge Univercity press.
- Shakarian, Paulo, (2011), "**Stuxnet: Cyberwar Revolution in Military Affairs**," Small Wars Journal.
- Shakarian, Paulo, Shakarian, Jana & Ruef, Andrew, (2013), **Introduction to Cyber warfare: A Multidisciplinary Approach**, USA, Elsevier.
- United States, (2011), **International strategy for cyberspace**.
- DOD**,** (2015),**The Departmet of Defence Cyber Strategy**.
- United States, (2018), **National Cyber Strategy of the United States of America**.