نشریه علمی سیاست دفاعی

قواعد و مقررات حقوقی در فضای سایبر و دعاوی حقوقی جمهوری اسلامی ایران

افشین جعفری[1] | علی غلامعلی[2] | هدایت‌الله درخشان[3]

۱۲۲
سال سی و دوم
بهار ۱۴۰۲
مقاله پژوهشی
تاریخ دریافت:
۱۴۰۰/۰۸/۲۹
تاریخ پذیرش:
۱۴۰۲/۰۴/۱۱
صص: ۱۳۶-۱۱۹
شاپا چاپی: ۵۰۸۷-۱۰۲۵
الکترونیکی: ۴۹۷۱-۲۶۵۴

چکیده

محیط زندگی همواره با تهدیدات متعددی روبرو بوده است که امروزه نیز شکل دیگری از این تهدیدات مشاهده می‌شود. آنچه دولت‌ها و نظام‌های سیاسی در گذشته‌های دور و نزدیک به کار می‌بردند، توسل به ابزار زور و یا جنگ علیه کشوری بود که با آنان وارد جنگ و یا مجادله می‌شدند. اما امروزه شکل تهدیدات دچار تغییر شده است و از فضای سایبر به عنوان محملی برای تهدید دیگران و رسیدن به منافع ملی بهره برده می‌شود. استفاده تهدیدآمیز از فضای سایبر، مشمول قوانین و مقررات داخلی و بین‌المللی می‌گردد. پژوهش حاضر نیز به بررسی قوانین حقوقی در فضای سایبر و دعاوی حقوقی جمهوری اسلامی ایران پرداخته است. سؤالی که مطرح است اینکه قوانین حقوقی برای مقابله با تهدیدات و حملات در فضای سایبری از سوی ایران شامل چه مواردی است؟ پاسخی که ارائه می‌شود این است که هرچند در داخل نیز رویکردهای حقوقی متعددی برای بررسی تهدیدات سایبری وجود دارد، اما با توجه به محدود بودن به فضای داخلی از اثرگذاری چندانی برخوردار نیستند. اما از جهت توسل به آموزه‌های حقوق بین‌الملل، استناد به تهدید صلح و امنیت نظیر آنچه شورای امنیت و منشور ملل متحد می‌گویند؛ توسل به اعلامیه‌ها و منشورهای منطقه‌ای و بین‌المللی، توسل به دیوان بین‌المللی دادگستری برای شناسایی و مجازات متجاوز و در نهایت استناد به اصل دفاع مشروع بخش‌های مختلفی از قوانین حقوقی مقابله با تهدیدات فضای سایبری شناخته می‌شوند. در پژوهش حاضر از روش توصیفی- تحلیلی بهره‌برده شد.

کلیدواژه‌ها: قوانین؛ فضای سایبر؛ دعاوی حقوقی؛ جمهوری اسلامی ایران

DOR: 20.1001.1.10255087.1402.32.122.5.1

۱. نویسنده مسئول: دانشیار گروه حقوق، دانشکده حقوق و علوم اجتماعی، دانشگاه پیام نور، تهران، ایران
jafariafshin@pnu.ac.ir
۲. استادیار گروه معارف اسلامی.دانشکده الهیات دانشگاه پیام نور تهران، ایران
۳. دانش آموخته کارشناسی ارشد حقوق بین‌الملل

مقدمه و بیان مسئله

یکی از مهمترین چالش‌های فن‌آوری‌های نوین، استفاده از این فن‌آوری‌ها جهت اختلال در امنیت بین‌المللی است، چرا که این فن‌آوری‌ها توانایی اثرگذاری بر افکار عمومی را داشته و می‌توانند با تبلیغات، مردم را بر ضد حکومت تحریک کرده و سبب ایجاد اختلاف میان کشورها شود. از آنجایی که در دو دهه‌ی اخیر حملات سایبری، مهمترین هدف سازمان ملل متحد ؛که همانا صلح و امنیت بین‌المللی بوده؛ را به مخاطره انداخته است، لذا ارکان سازمان ملل نیز ساکت نبوده و از طریق مجمع عمومی و شورای امنیت و دیگر سازمان‌های وابسته به تحقیق و پژوهش و اقدام در مقابل ناامنی سایبری در سطح جهانی پرداخته‌اند. در همین راستا مجمع عمومی تاکنون چندین قطعنامه[1] در این خصوص صادر نموده که البته دارای ابهاماتی نیز بوده‌اند. در ماه اوت سال ۱۹۹۹، سازمان ملل متحد یک نشست بین‌المللی تحت عنوان " درک مفاهیم امنیت اطلاعاتی در حال ظهور" در ژنو با حضور کارشناسان خبره برگزار نمود و به دنبال آن در سال ۲۰۰۲ قطعنامه مجمع عمومی در خصوص " تحولات در زمینه اطلاعات و ارتباطات از راه دور در حوزه امنیت بین‌المللی" را صادر نمود که البته مقدار کار انجام شده بر روی آن بسیار کم بود و در پی آن اجلاس جهانی جامعه اطلاعاتی برگزار گردید. این سازمان در سال ۲۰۱۰ یک گام بزرگ به جلو برداشت و دبیر کل سازمان ملل متحد از متخصصان امنیت سایبری پانزده کشور برتر سایبری دعوت نمود تا همایشی با عنوان " ارائه مجموعه‌ای از توصیه‌های ابتدایی در جهت ساخت چارچوب بین‌المللی برای امنیت و ثبات" بر گزار نمایند.(باقری، ۱۳۹۷: ۵)

با توجه به اینکه در راستای مقابله با تهدیدات ناشی از فضای سایبری، قواعد حقوقی متعددی در عرصه داخلی و بین‌المللی مطرح شده است، برخی دعاوی حقوقی کشورهای مختلف در این زمینه از طریق همین قوانین حل شده است. اما به طور مشخص در دهه اخیر، تهدیداتی از طریق فضای سایبری امنیت داخلی جامعه ایرانی را مورد تعرض قرار داده است. با توجه به اینکه جمهوری اسلامی ایران، رقبا و دشمنان منطقه‌ای و بین‌المللی متعددی دارد، تلاش قانونی و حقوقی برای مبارزه با این تهدیدات یکی از دغدغه‌های اساسی به شمار می‌رود. تصمیم گیران و

۱- از جمله قطعنامه‌های مرتبط با این موضوع،قطعنامه‌های: ۳۲/۵۸، ۶۱/۵۹، ۴۵/۶۰، ۵۴/۶۱، ۱۷/۶۲، ۳۷/۶۳، ۲۵/۶۴، ۲۵۲/۶۰ می‌باشد.

تصمیم‌سازان کشور نیز از جهت رسیدگی به این تعرضات هم از قوانین داخلی و هم از قوانین حقوقی بین‌المللی بهره برده اند. اما به طور مشخص برخی دعاوی حقوقی ناشی تهدیدات سایبری به دلیل ماهیت پیچیده و نامشخص بودن عاملان آن و نبود سازوکار حقوقی مدون داخلی و عدم توجه به قوانین حقوقی بین‌المللی، مسکوت مانده است. با توجه به اهمیت رسیدگی به تهدیدات ناشی از فضای سایبری، پژوهش حاضر درصدد است تا از منظر حقوق داخلی و بین‌المللی نسبت به این مسأله توجه نشان دهد.

اهمیت پژوهش حاضر بر کسی پوشیده نیست. زیرا امروزه تهدیدات ناشی از فضای سایبر از سوی کشورهای معاند به اوج خود رسیده است و مکان‌های متعددی از جمله تأسیسات هسته‌ای را نشانه گرفته است. بنابراین رسیدگی به این موضوع از حیث بررسی سازوکارهای حقوقی داخلی و بین‌المللی دارای اهمیت خاصی است. سؤالی که مطرح است اینکه قوانین حقوقی داخلی و بین-المللی برای رسیدگی به تهدیدات ناشی از فضای سایبری شامل چه مواردی است؟

مبانی نظری

فضای سایبر

وقتی صحبت از فضای سایبر به میان می‌آید مردم اغلب به رایانه یا رایانه‌هایی فکر می‌کنند که به اینترنت متصل است. در حالی که این فقط بخش بسیار کوچکی از فضای سایبر را تشکیل می‌دهد. فضای سایبر فقط مجموعه‌ای از سخت‌افزار و نرم‌افزار نیست بلکه مجموعه‌ای از تعاریف نمادین است که شبکه‌ای از اطلاعات، برنامه‌ها، سیستم‌های کنترل پرواز، سیستم‌های کنترل تأسیسات آب، برق، گاز، پتروشیمی و.. را در قالب "صفر و یک" رد و بدل می‌کنند. فضای سایبر را می‌توان برای توصیف تمام انواع منابع اطلاعاتی موجود در شبکه‌های رایانه‌ای به کار برد. در حقیقت فضای سایبر نوع متفاوتی از واقعیت مجازی و دیجیتالی است که توسط شبکه‌های رایانه‌ای هم پیوند تامین می‌شود. اندرسون فضای مجازی را "واقعیت خلق شده توسط رایانه" می‌داند (جی پست، ۱۳۸۵: ۲۷). واقعیتی که از آن رو مجازی یا مصنوعی است که در دنیای واقعی محیط مادی، مکانی را اشغال نکرده و در اذهان کاربران در نتیجه تعامل با واسط الکترونیکی وجود دارد. واقعیت مجازی واقعیتی است که وجود فیزیکی نداشته توسط نرم‌افزار تولید می‌شود. به عقیده

برخی از سیاست‌مداران و حقوق‌دانان، "فضای سایبر یک حوزه عملیاتی است که به منظور بهره‌برداری از اطلاعات از طریق سیستم‌های به هم پیوسته و زیرساخت یکپارچه آن‌ها، با استفاده از علم الکترونیک شکل گرفته است." قدرت به زمینه بستگی دارد، و قدرت سایبری به منابعی که قلمرو فضای سایبر را شکل می‌دهند (Saleh, et. al, 2019: 15)

فضای سایبر علیرغم مباحث متعددی که درباره مزایا و معایب آنان مطرح می‌شود، نوعی دستاورد و پدیده جدیدی است که توان دولت‌ها برای سلطه بر آن را به حداقل رسانیده است. به عبارت دیگر، دولت‌ها نمی‌توانند بر فضای سایبر حاکمیت تام داشته باشند زیرا فراگیری گسترده فضای سایبر و نقش‌آفرینی بازیگران غیردولتی این امکان را از دولت‌ها گرفته است(Everard,2000: 44). فضای سایبر دربرگیرنده مجموعه‌ای وسیع از داده‌ها و اطلاعات است که امروزه فضای فعالیت را برای دسته‌های مختلف بازیگران در این عرصه فراهم ساخته است. همان‌گونه که در دنیای واقعی، تهدیدها، فرصت‌ها و چالش‌هایی برای گروه‌های مختلف انسانی وجود دارد، در فضای سایبر نیز این دسته از تهدیدها برای حاکمیت وجود دارد (Jiaxuan, et. al, 2019: 15). در این چارچوب، تهدیدات وجودی ناشی از کاربست الگوی قدرت نرم که قبلاً به ظاهر کم اهمیت جلوه می‌کردند توسط کشورهای مختلف مورد توجه قرار گرفته است. بنابراین یکی از مؤلفه‌های حکمرانی در عرصه بین‌الملل، توان مضاعف دولت‌ها برای استفاده از فضای سایبری در جهت رسیدن به منافع خود است. برخی از کشورها برای رسیدن به مقاصد خود از فضای سایبر به عنوان محفلی برای تضعیف رقبا و دشمنان و رسیدن به اهداف موردنظر استفاده می‌کنند.

۲-۱- حملات سایبری

پرداختن به علل و دلایل وقوع جرایم و حملات سایبری نیازمند مباحث گسترده و عمیق‌تری است. اما آنچه امروزه به عنوان جرایم و تخلفات در فضای سایبری مطرح می‌شود، به دلایل متعددی از جمله رقابت‌های اقتصادی و ایدئولوژیکی میان دولت‌های مختلف پدید آمده است. بنابراین فضای سایبر هرچند در نگاه آغازین، امری مشترک برای همه کشورها در نظر آورده می‌شود، اما عوامل مختلفی از جمله برتری دانش و ثروت، حاکمیت برابر در فضای سایبر را تحت تأثیر خود قرار می‌دهند (Chander and Sander, 2004: 1331). به عنوان مثال، کشور X به

دلیل توانایی‌های نظامی، اقتصادی و اطلاعاتی، تأثیرگذاری بیشتری بر کشور Y دارد. یا اینکه برخی دولت‌ها با توجه به نقش مؤثری که در امور سایر کشورها و مناطق دارند، از توان اثرگذاری بیشتری در این زمینه برخوردار هستند.

علاوه بر این، حملات سایبری که حتی در شرایط خاصی تحت عنوان جنگ سایبری از آن نام برده می‌شود، یکی از تهدیدات مهم در عرصه بین‌المللی به شمار می‌روند. ابزارها و نظام‌های تسلیحاتی جنگ سایبری اگر چه ارزان‌تر و سریع‌تر از موشک‌های جنگی هستند، اما دارای آثار تخریبی بیشتری نسبت به موشک هستند (Lewis, 2020: 310). با این حال، حملات سایبری علاوه بر آثار و پیامدهای آشکار دارای آثار و پیامدهای پنهانی هستند که به دلیل ماهیت پنهان آنان حتی توسط دولت‌ها نیز به صورت شفاف بیان نمی‌شوند. به عنوان مثال، حمله سایبری به سامانه دفاعی و نظامی، افشای اسناد و مدارک سری و همچنین دستکاری در تأسیسات هسته‌ای از جمله مواردی است که گرچه ممکن است واکنش دولت‌ها را در پی داشته باشد، اما همواره در خفا باقی می‌مانند.

ایالات‌متحده آمریکا و روسیه و چین در سازمان همکاری شانگهای تعاریف متفاوتی را از حمله سایبری ارائه کرده‌اند که خود جای تأمل و بحث دارد (Gellman, 2002:15) به‌عنوان مثال، ستاد مشترک ارتش آمریکا حملات سایبری را نزدیک به جنگ سایبری دانسته (Gellman, 2002:16) و آن را به عنوان اقدامات کلی برای تغییر، مختل کردن، فریب و یا از بین بردن سیستم‌های رایانه‌ای و شبکه‌های اطلاعاتی دانسته‌اند. (General Accounting Office, 1998:45) البته ناگفته نماند که جنگ سایبری نیز به نوبه خود بر نحوه تصمیم‌گیری در مخاصمات و طرز به‌کارگیری تسلیحات و همچنین در جنگهای نیابتی، کاربرد خود را به طرز شگفت‌انگیزی نشان داده است (قنبری‌جهرمی، ۱۳۹۹: ۴۴). به همین دلیل، امروزه جنگ‌های سایبری یکی از موضوعات امنیتی و حقوقی کشورهای مختلف برشمرده می‌شود. علاوه بر این، کشورهای قدرتمند تلاش می‌کنند تا با بهره گیری از ابزارهای پیشرفته، آسیب هایی را بر رقبای خود و یا کشورهای دارای سیستم امنیتی ضعیف به کار گرفته و از رقبا پیشی بگیرند. در همین راستا، سازمان همکاری شانگ‌های حملات سایبری را تهدید علیه امنیت داخلی و بین‌المللی و

همچنین بی ثبات کردن جامعه داخلی از طریق شستشوی مغزی و یا وادار کردن دولت جهت تصمیم گیری به نفع یک حزب مخالف تعریف نموده‌اند. (U.S Dep't of Def., 2006:4-6)

بنابراین می‌توان این‌گونه برداشت نمود که دولت‌های مختلف یک چشم انداز گسترده‌ای از حملات سایبری که شامل مسائل سیاسی نیز می‌گردد، در نظر داشته‌اند. و تفاوت میان این تعاریف نشان دهنده اهمیت ارائه یک تعریف واضح از مشکلاتی است که کشورها با آن‌ها مواجه هستند. با توجه به رویکرد متفاوت برخی از دولت‌ها به مصادیق حمله سایبری، تعریف پیشنهادی برای حمله سایبری به شرح ذیل می‌باشد: هر عملیاتی که موجب مختل شدن عملکرد یک شبکه رایانه‌ای و یا تجهیزات الکترونیکی، مخابراتی، و... با اهداف سیاسی و یا بر هم زدن امنیت ملی و صدمه زدن به زیرساخت‌های حیاتی یک کشور انجام پذیرد، حمله سایبری می‌باشد. روزانه حجم بسیار زیادی از حملات سایبری اتفاق می‌افتد که این‌ها می‌توانند سطوح دیگری از تهدیدات را در برگیرند و طبعاً هر حمله سایبری یا هر نفوذ سایبری را نمی‌توان مساوی با جنگ سایبری تشخیص داد و به همین دلیل دولت‌ها به دنبال راه حلی به غیر از دفاع مسلحانه هستند. اما در پاره‌ای از مواقع چنان چه حجم تخریب و خسارت وارده زیاد باشد و یا دولت مورد حمله قرار گرفته تلقی تهدید امنیت ملی را از حملات سایبری داشته باشد، احتمال تلقی جنگ سایبری نیز بالا می‌گیرند.

افزایش به‌کارگیری حملات سایبری به عنوان یک ابزار سیاسی بازتاب یک رویه خطرناک در روابط بین‌المللی است. سیستم‌های اطلاعاتی آسیب‌پذیر و نبود مبانی حقوقی مناسب در جهت مقابله با این‌گونه حملات باعث می‌شوند بازیگران دولتی و غیردولتی نسبت به حمله علیه کشورها و منافع این کشورها وسوسه شوند. (Albakri, M., Sturm, L., Williams, C. B., & Tarazaga, 2017). همین موضوع، آسیب پذیری صنایع را به شدت بالا برده و تهدیدات سایبری می‌تواند بروز یک فاجعه را رقم بزند. رویکرد جهانی به این موضوع را می‌توان در هشدار اخیر سازمان ملل نیز دریافت. پیرو آسیب دیدن کشورهای خاورمیانه از حمله بدافزارها، یکی از مسئولین "هماهنگ کننده امنیت سایبری در اتحادیه بین‌المللی ارتباطات و مخابرات وابسته به سازمان ملل متحد" مستقر در ژنو گفت: این هشدار محرمانه برای کشورهای عضو روشن خواهد کرد که بدافزارها یک ابزار خراب‌کاری خطرناک است که بالقوه می‌تواند برای حمله به زیربنای حیاتی کشورها مورد استفاده قرار گیرد و کشورهای عضو باید در این‌باره هوشیار

باشند. (Economictimes, 2012:38) به همین دلیل برخی از کشورها جهت مقابله با حملات و تهدیدات سایبری به جای انتظار، به سازوکارهای دیگری به غیر از دفاع مسلحانه روی آورده‌اند که در ذیل به برخی از آنها اشاره گردیده است.

با توجه به روند رو به رشد حملات سایبری و نقض اصول و قواعد حقوق بین‌الملل در خلال این حملات و از آنجایی‌که احتمال گسترده شدن این‌گونه حملات سایبری وجود دارد. لذا اصول و قواعد حقوق مخاصمات مسلحانه اعم از Jus ad bellum و Jus in bello نیز تحت الشعاع قرار میگیرند اما از آنجائیکه در شناسایی اینگونه حملات تحت عنوان "حملات مسلحانه" اختلاف نظرهای حقوقی وجود دارد، بنابراین سازمان‌هایی همچون اتحادیه اروپا به‌جای دفاع مسلحانه به دنبال راه‌های پیش‌گیری از اینگونه حملات بوده‌اند و به همین دلیل با توجه به تعداد اعضاء اتحادیه اروپا و حساسیت اعضاء آن در مواجهه با حملات سایبری، اخیراً پیرامون این موضوع تلاش‌هایی گردیده که در چارچوب اساسنامه این اتحادیه در حال پیگیری می‌باشد. هرچند در اساسنامه این سازمان مبحثی در خصوص رویارویی با حملات سایبری ذکر نگردیده اما بند ۷ ماده ۴۲ این معاهده در خصوص دفاع متقابل در مواقع اضطراری، از دولت‌های عضو می‌خواهد که در هنگام حمله مسلحانه به خاک یکی از اعضاء، به یکدیگر کمک کنند. البته دوباره این چالش پیش می‌آید که حملات سایبری در چه هنگامی مصداق یک حمله مسلحانه می‌گردد که خوشبختانه (و شاید متاسفانه) هنوز رویه عملی مهمی در این خصوص شکل نگرفته است. (Elhabashy, 2019: 2489–2504)

یکی از تصمیمات اخیر اتحادیه اروپا، تلاش در جهت تشکیل یک گروه واکنش فوق العاده، به منظور حفاظت از امنیت شبکه‌های اطلاعات بوده است البته طبق اساسنامه این اتحادیه، به نوعی ماده ۲۲ نیز می تواند در مواجهه با حملات سایبری مورد استناد قرار گیرد، زیرا در این ماده این‌گونه عنوان گردیده که:" اگر یکی از اعضای اتحادیه هدف حمله تروریستی یا فاجعه طبیعی یا انسانی قرار بگیرد اتحادیه و اعضایش باید با روحیه همبستگی عمل کنند و باید همه ابزارها را برای کمک به آن عضو بسیج نمایند(Michele L., 2019:183) به هر صورت، شرایط موجود نشان می‌دهد که فضای سایبر، فضای رقابت، خصومت، انتقام، تهدید و ضربه زدن به دیگری است. بنابراین تلقی جنگ سایبری، حمله سایبری، خرابکاری سایبری و مفاهیمی از این قبیل از جمله

محورهای مرتبط با امنیت ملی کشورها در سطوح داخلی، منطقه‌ای و بین‌المللی است. با توجه به جدی بودن موضوع حملات سایبری، به سازوکارهای حقوقی و قوانین مرتبط با پیگیری حملات سایبری از منظر حقوق داخلی و حقوق بین‌الملل، به رویکردهای مهم در این زمینه پرداخته می‌شود و به مصادیق حملات سایبری در جمهوری اسلامی ایران نیز بیان می‌شود.

حاکمیت و قانون‌گذاری بر فضای سایبر در نظام حقوقی جمهوری اسلامی ایران

لازمه وجود امنیت سیاسی در یک کشور، ثبات ساختاری مجموعه‌ی نهادهای دولتی و نهادینه شدن ایدئولوژی‌های مشروع می‌باشد که نتیجه آن، انسجام و هم‌زیستی مسالمت‌آمیز هویت‌های فرهنگی سنتی در بین ملت‌هاست و ضمانت پایداری اینگونه امنیت، استمرار حاکمیت قانون و حمایت از این ویژگی‌های سیاسی-فرهنگی است. یکی از مواردی که امنیت سیاسی را می‌تواند تهدید کند، فضای سایبر است. استدلالی که درباره شرایط و موقعیت جمهوری اسلامی ایران مطرح می‌شود این است که کشورهایی مخالف جمهوری اسلامی ایران، با استفاده از فضای سایبر از طریق بی‌ثبات‌سازی ساختاری-نهادی و بی‌ثبات‌سازی ایده و معنا، هویت مشروع حکومت‌هایی همچون جمهوری اسلامی ایران را هدف گرفته‌اند(سلیمانی‌پورلک، ۱۳۹۲: ۲۶۹). به عبارتی دیگر، با توجه به هزینه‌بر بودن تقابل نظامی با کشورهای مختلف دنیا از جمله جمهوری اسلامی ایران، رقبا و دشمنان منطقه‌ای و بین‌المللی ایران سعی می‌کنند با توسل به روشهای کم هزینه و اثرگذار در حوزه‌های مختلف، توان نظامی و امنیتی جمهوری اسلامی ایران را زیر سؤال ببرند.

در خصوص مقابله با تهدیدات فضای سایبر و ارائه رویکردی پیش‌گیرانه، دو راه‌حل کلی جهت حاکمیت بر این فضا وجود دارد، قانونگذاری ملی و قانونگذاری بین‌المللی. جمهوری اسلامی ایران در خصوص مدیریت بر اینترنت و فضای سایبر رویکردی مبتنی بر حاکمیت سنتی و قانونگذاری ملی داشته و دارد و به همین دلیل بر اساس دستور مقام معظم رهبری و در راستای «سیاست‌های کلی شبکه‌های اطلاع رسانی رایانه‌ای»، شورای عالی انقلاب فرهنگی، مقررات مربوطه و لازم را تحت عنوان « مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه‌ای» در سال ۱۳۸۰ به تصویب رسانید. بر اساس این قانون رعایت، حمایت و اجرای حقوق اجتماعی وفرهنگی در چارچوب حقوق و قوانین داخلی الزامی است هرچند که حق دسترسی آزاد به اطلاعات نیز در جای خود بایستی رعایت گردد. البته ناگفته نماند که مقررات و قواعد دیگری همچون آیین‌نامه

نحوه اخذ مجوز و ضوابط فنی نقطه تماس بین‌المللی، آیین‌نامه واحدهای ارائه کننده خدمات اطلاع رسانی و اینترنت "رسا" (ISP)، مصوبات کمیسیون تنظیم مقررات ارتباطات درسال ۱۳۸۴، قوانین پنج ساله توسعه و قانون تجارت الکترونیک نیز وجود دارد، لیکن نخستین قانون جامع و متمرکز در جمهوری اسلامی ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸و قوانین اصلاحی آن، مندرج در قانون آیین دادرسی کیفری ۱۳۹۲ است. (ضیایی‌وهمکار،۱۳۹۶ :۲۴۱)

با توجه به نکات فوق و با عنایت به اینکه رویکرد حقوق داخلی جمهوری اسلامی ایران به مدیریت بر فضای سایبر، روش حاکمیت و قانون‌گذاری ملی بوده است، اما نحوه نگرش انتقادی جمهوری اسلامی ایران به نحوه مدیریت بر زیرساخت‌های فضای سایبر در "سازمان اینترنتی، انتصاب اسامی و کدهای رقمی (آیکان)" نشان دهنده‌ی پذیرش تلویحی روش قانون‌گذاری بین‌المللی در این خصوص بوده است. گواه بر این ادعا، رأی مثبت جمهوری اسلامی ایران به سند اصلاحی اتحادیه بین‌المللی مخابرات در سال ۲۰۱۲ است. البته امروزه طرح شبکه ملی اطلاعات و مجموعه قوانین حاکم بر فضای سایبر در جمهوری اسلامی ایران، نشان دهنده رویکرد ملی جمهوری اسلامی ایران به قانونگذاری بر فضای سایبر است. با این حال، اعمال روش قانونگذاری ملی در قوانین داخلی و پذیرش روش بین‌المللی در مدیریت آینده این فضا حاکی از تمایل جمهوری اسلامی ایران به اعمال روش مختلط در قانونگذاری در این فضا است (ضیایی‌وهمکار، ۱۳۹۶: ۲۴۶). هرچند قوانین داخلی از مطلوبیت قابل توجهی برای مقابله با تهدیدات سایبری به شمار می‌روند، اما هنگامی که تهدیدات مزبور از سوی دولت‌ها و گروه‌های خارج از مرز ایران شکل می‌گیرند، امکان کمتری برای پیگیری این موارد از منظر حقوق داخلی وجود دارد. بنابراین در صورت شکل گیری و یا وقوع تهدیدات خارجی علیه جمهوری اسلامی ایران، می‌توان با اتخاذ سازوکارهای متعددی نسبت به شناسایی و تنبیه متجاوز و عامل و همچنین دریافت غرامت و خسارت از وی اقدام نمود. رویکردهایی که با توسل به حقوق بین‌الملل می‌توانند قابلیت کاربرد داشته باشند، طیف متعددی را در بر می‌گیرند که در اینجا به برخی از مهمترین آنان پرداخته می‌شود.

قواعد و مقررات حقوقی بین‌المللی برای مقابله با حملات سایبری

از جمله مهم‌ترین چالش‌های حقوق بین‌الملل درباره فضای سایبری و مخصوصاً تهدیدات ناشی از آن، «بین‌المللی بودن» این جرایم است. با توجه به گستردگی جرایم و نامشخص بودن

قوانین عام و فراگیر برای همه کشورها، تهدیدات ناشی از حملات سایبری بیش از پیش محل توجه است. با توجه به تهدیدات و فرصت‌های ناشی از فضای سایبر که به فراتر از مرزهای سرزمینی تسری یافته است، صلاحیت قانونگذاری در این زمینه نیز به مراجعی بالاتر از دولت‌ها واگذار شده است. از همین رو، این رویکرد در مناطقی مانند دریای آزاد، اعماق دریاها، قطب جنوب و فضای ماورای جو دنبال شده است (Anthony, 2010: 40). بدین معنا که برخی از مسائل که دغدغه‌ای جهانی و فراتر از محدوده و اختیارات دولت‌ها محسوب می‌شوند، نیازمند قوانین حقوقی بین‌المللی هستند که عام و فراگیر باشند و برای برخی میراث‌های مشترک بشریت، قوانین همه‌گیری در نظر بگیرند.

در این میان، سازمان همکاری و توسعه اقتصادی[1] رویه‌های حقوقی خود را با تأکید بر حمایت از حریم خصوصی، حقوق فردی و همچنین مراقبت از اطلاعات شخصی مطرح نمود (جلالی‌وتوسلی‌اردکانی، ۱۳۹۸: ۱۳۵۸). سازمان مزبور، رهنمودهای خود را در زمینه جرایم رایانه‌ای منتشر نمود و فهرستی از جرایم رایانه‌ای را منتشر نمود که براساس آنها، سازمان مزبور، رویکردهای خود را در سال ۱۹۸۹م، در خصوص امنیت سیستم‌های رایانه‌ای ادامه داد (گرکی، ۱۳۸۹: ۲۲۰). بخش مهم دیگری از قوانین حقوقی بین‌المللی به رویکردهای حقوقی سازمان ملل متحد در قبال جرایم و تخلفات سایبری است. قوانین حقوقی متعددی در این زمینه مطرح شده است که از جمله در سال ۲۰۱۳م، سازمان ملل متحد، سند مهمی درباره جرایم در فضای سایبری تحت عنوان «مطالعه جامع در خصوص جرایم سایبری» انتشار داد که در آن به انقلاب جهانی ارتباطات، رشد سریع جرایم سایبری به عنوان چالشی برای دنیای معاصر، مرتکبان جرایم سایبری، نقش قانون در مبارزه با این تخلفات و ضرورت هماهنگ سازی این قوانین تأکید می‌کرد (جلالی‌وتوسلی‌اردکانی، ۱۳۹۸: ۱۳۶۰).

راهکارهای پیش روی ایران برای مقابله با تهدیدات سایبری

تهدیدات و حملات سایبری علیه ایران یکی از چالش‌های تهدیدآمیز به شمار می‌روند. مصادیق حملات و تهدیدات سایبری علیه ایران متعدد هستند. از جمله می‌توان به گزارش روزنامه نیویورک تایمز اشاره کرد که در سال ۲۰۱۰ م، با انتشار یک گزارش مدعی شد که حملات

1. Organization for Economic Cooperation and Development(OECD)

سایبری به تأسیسات هسته‌ای ایران از طریق نرم افزاری به نام استاکس نت[1] صورت گرفته است. این حملات با هدف متوقف کردن و یا کند کردن روند برنامه هسته‌ای جمهوری اسلامی ایران دنبال شده است و براساس این حملات، قرار بود تا سرعت سانتریفیوژهای ایران را کند نماید (New York Times, May 2010). در این حمله سایبری، علاوه بر اطلاعات سیستم‌های کنترل صنعتی و نیروگاهی و رایانه ای تأسیسات هسته‌ای، اطلاعات سیستم‌های خانگی را نیز به سرقت برد و حدود ۶۰ درصد رایانه‌ها ی ایرانی را آلوده ساخت. تحقیقات نشان داد که این کرم برای این منظور طراحی شده که سانتریفیوژهای ویژه غنی‌سازی اورانیوم را مختل کند. پیچیدگی کرم نرمافزاری «استاکس نت» به حدی بود که برخی از متخصصان از آن به عنوان «تروریسم سایبری» یاد کردند. بدین ترتیب، گروه یا کشوری با هدف تخریب ساختارهای حیاتی یک کشور این نرم افزار مخرب را نوشته و فعال کردند که هدف‌گیری این ویروس در راستای جنگ الکترونیکی علیه ایران اعلام شد تا اطلاعات مربوط به خطوط تولید را به خارج از کشور منتقل کند (عظیمی و خشنودی، ۱۳۹۵: ۱۶۶). پس از این عملیات خرابکارانه سایبری که حتی گفته می‌شد دستور آن در زمان ریاست جمهوری اوباما نیز صادر شده بود، در سالهای بعدی نیز تأسیسات هسته‌ای ایران مورد حمله سایبری قرار گرفت و خسارات‌های قابل توجهی نیز به تأسیسات هسته‌ای ایران وارد شده است. مصادیق دیگری نظیر حمله به نیروگاه برق کشور و همچنین سامانه توزیع بنزین در سال ۱۴۰۰ رخ داده است که تا یک هفته مراکز پمپ بنزین قادر به ارائه خدمات سوخت نبودند. هرچند در اینجا گروه خاصی مسؤولیت آن را بر عهده نگرفت، اما آنچه روشن است اینکه لزوم اتخاذ تدابیری هم از منظر حقوق بین‌الملل و هم از نظر حقوق داخلی برای مقابله با این تهدیدات امری ضروری و بایسته است. بر این موارد باید هک شدن اطلاعات مربوط به زندان‌های ایران در سال ۱۴۰۰ را نیز افزود که تداوم این تهدیدات سایبری می‌تواند منافع ملی را نیز به خطر بیندازد.

به نظر می‌رسد در صورت وقوع تهدیدات سایبری اعم از جنگ سایبری یا تهدیدات مشابه در سطوح پایین‌تر، راهکارهای حقوقی بین‌المللی پیشروی جمهوری اسلامی ایران نیز وجود دارد. از جمله توسل به مواد حقوقی شورای امنیت سازمان ملل متحد می‌تواند راهکاری حقوقی برای مقابله

1 .Stax net

با تهدیدات سایبری، شناسایی متخلفان و برخورد با آنان تلقی گردد. از جمله در زمینه پیگیری حقوقی تهدیدات سایبری علیه جمهوری اسلامی ایران، شورای امنیت می‌تواند با تلقی تهدیدات مزبور تحت عنوان «علیه صلح»، براساس ماده ۳۹ منشور سازمان ملل متحد توصیه‌هایی را ارائه کند و برای پیش‌گیری از وخیم‌تر شدن اوضاع و بحرانی شدن آن، به موجب ماده ۴۰ منشور ملل متحد اقدامات عملی را توصیه نماید. علاوه بر این می‌توان با استناد به مواد ۴۱ و ۴۲ منشور ملل متحد در خصوص اقدامات مبتنی بر عدم توسل به زور و یا با توسل به زور اتخاذ تصمیم نماید (قاسمی‌وچهاربخش، ۱۳۹۱: ۱۲۸).

ابزار حقوقی دیگری که در حقوق بین‌الملل می‌تواند مورد استناد جمهوری اسلامی ایران واقع شود، استفاده از رویکردهای تفسیری از مواد منشور سازمان ملل است. از جمله اینکه ماده ۲ منشور سازمان ملل متحد استفاده از زور را منع کرده است. حسب این رویکرد تفسیری می‌توان گفت که سلاح نیز دارای موسع است و دربرگیرنده ابزاری طراحی شده برای استفاده و یا صدمه زدن به دیگری از جمله قتل وی است (Garner, 2009: 124). با ارائه چنین تفسیری و طرح آن در مجامع بین‌المللی می‌توان این نظریه را مطرح کرد که سلاح در صورتی که با نیت خصمانه و نشان دادن این خصومت در عمل همراه باشد، می‌تواند تهدیدی علیه صلح نیز در نظر گرفته شود. بنابراین هنگامی که اقدامات سایبری به صورت عملی و واقعی، تأسیسات هسته‌ای را با آسیب روبرو می‌سازد و یا اینکه باعث اختلال در سیستم خدمات ارائه بنزین می‌گردد، می‌توان با استناد به ماده ۲ منشور سازمان ملل، شکایت حقوقی را به مجامع بین‌المللی ارجاع داد.

علاوه بر این، منشور در بند ۱ ماده ۱ مقاصد و اهداف ملل متحد را به شرح زیر ذکر می‌کند. حفظ صلح و امنیت بین‌المللی و برطرف کردن تهدیدات علیه صلح و متوقف ساختن هرگونه عمل تجاوز و یا سایر اعمال ناقض صلح و فراهم آوردن موجبات حل و فصل اختلافات بین‌المللی یا وضعیت‌هایی که ممکن است منجر به نقض صلح گردد با شیوه‌های مسالمت‌آمیز و بر طبق اصول عدالت و حقوق بین‌الملل. همچنین در بند ۳ ماده ۲ بیان می‌دارد: کلیه اعضاء اختلافات بین‌المللی خود را با شیوه‌های مسالمت‌آمیز به صورتی که صلح و امنیت بین‌المللی به خطر نیفتد، حل و فصل خواهند کرد. اما فصل‌الخطاب عدم توسل به زور و ممنوعیت اقدام به جنگ بند ۴ ماده ۲ منشور می‌باشد که با صراحت تصریح نموده است: کلیه اعضاء در روابط بین‌المللی خود از تهدید به زور

یا استعمال آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر روش دیگر که با اهداف ملل متحد مغایر باشد خودداری خواهند نمود.

مطابق ماده ۵۳ کنوانسیون وین حقوق معاهدات عدم توسل به زور و اقدام به جنگ بعنوان یک قاعده آمره حقوق بین‌الملل عام پذیرفته شده است، زیرا از نظر آن عهدنامه قاعده آمره حقوق بین-الملل عام، قاعده‌ای است که از سوی جامعه بین‌المللی کشورها، به طور کلی بعنوان قاعده‌ای که تخلف از آن مجاز شمرده نشده است؛ یعنی تخلف‌ناپذیر است و فقط از طریق قاعده بعدی حقوق بین‌الملل عام با همان ویژگی قابل تغییر می‌باشد.

در هر صورت جمهوری اسلامی ایران می‌توان با استناد به مواد بیان شده، پیگیر مطالبات خود و خسارات وارده بر تأسیسات داخلی از حیث و معنوی باشد که ناشی از حملات سایبری بوده است. در این صورت می‌توان گفت قاعده آمره بین‌المللی، قاعده‌ای است که اکثریت کشورهای جامعه بین‌المللی آن قاعده را از رهگذر مشارکت در یک معاهده بین‌المللی (منشور ملل متحد) که آن قاعده را در بر دارد پذیرفته باشند، بنابراین قاعده آمره قاعده‌ای است که هیچ گونه تخطی از آن مجاز نمی‌باشد، دیوان بین‌المللی دادگستری نیز در دعوای نیکاراگوئه علیه ایالات متحده آمریکا چنین بیان می‌دارد: «...آنچه که مسلم می‌نماید این است که هم منشور و هم حقوق بین-الملل عرفی از اصول بنیادین مشترکی در غیر قانونی شمردن استفاده از زور در روابط بین‌المللی تبعیت می‌کنند ...» (زمانی، ۱۳۷۷: ۳۰۶).

برداشت دیگری که از قواعد آمره بین‌المللی می‌شود، تلقی تجاوزگونه از حملات سایبری است که جمهوری اسلامی ایران می‌تواند مهاجمان را شناسایی و آنان را به عنوان متجاوز به دادگاه‌های بین‌المللی معرفی نموده و اقامه دعوی نماید. توضیح اینکه مجمع عمومی سازمان ملل متحد نیز در سال ۱۹۷۴ طی قطعنامه ۳۳۱۴ معروف به قطعنامه تعریف تجاوز که از طریق کنسانسوس تصویب شد به تعریف تجاوز، اعمال تجاوزکارانه و مسئولیت متجاوز پرداخت. حال که بدین نتیجه رسیدیم استفاده از زور و توسل به جنگ در حقوق بین‌الملل معاصر غیر قانونی بوده و تخطی از آن به هیچ وجه جایز نیست که همین رویکرد قابل تعمیم به حملات سایبری نیز می-باشد. بر همین اساس، توسل به راهکارهای قانونی در زمینه حملات سایبری علیه جمهوری اسلامی ایران به دلیل آنکه حملات مزبور تهدید صلح و امنیت جامعه تلقی شده و حتی دارای آثار تخریبی

و خسارت‌آوری می‌باشند، رویکردی قابل دفاع است. استدلال این است که تهدید صلح و امنیت داخلی کشورها می‌تواند با هر ابزاری صورت گیرد و از این جهت رویکرد سازمان ملل فراگیر است (Chestman, 2008: 71).

ابزار حقوقی دیگری که می‌تواند مورد استفاده قرار گیرد، طرح شکایت در دیوان دادگستری بین‌المللی است. زیرا براساس منشور سازمان ملل کشورهایی که امنیت کشور دیگری را تهدید می‌کنند، مشمول پرداخت خسارت و یا شناسایی به عنوان متجاوز هستند. به هر صورت، حملات سایبری از مصادیق تهدید نظام و امنیت کشورها در نظر گرفته شده و نوعی تجاوز محسوب می‌شوند. علاوه بر مسؤولیت دولت در این زمینه، مسؤولیت کیفری بین‌المللی افراد متخلف نیز قابل توجه است (Weisbord, 2009: 39).

ابزار دیگری که می‌تواند به عنوان بخشی از راهکارهای مقابله با تهدیدات سایبری تلقی شود، استفاده از توان دفاعی و نظامی کشور مورد تجاوز است. در صورتی که توسل به نهادهای و ابزارهای حقوقی بین‌المللی کارساز نباشد و یا حتی حمله سایبری، امنیت ملی جامعه ایرانی را تهدید نماید، توسل به «دفاع مشروع» در مقابل کشور و یا گروه متجاوز سازوکاری مقبول است. بدین معنا که هر سیستم قانونی به اعضای خود اجازه می‌دهد در صورتیکه مورد حمله مسلحانه قرار گرفته و به حقوق آنها تجاوز شود از خود دفاع نمایند مگر اینکه آن سیستم یک ارگان اجرای قدرتمند و فعال جهت دفاع از اعضای خود داشته باشد (Ignarski and Barrister1982:212). به نظر می‌رسد با توجه به دشواری حملات نظامی و روی آوردن دشمنان جمهوری اسلامی ایران به راه‌های کم هزینه تر و پرخطر از جمله حملات سایبری، افزایش توان دفاعی کشور برای مقابله با این تهدیدات می‌تواند پذیرفتنی باشد. همان طور که هر اصلی استثنائاتی دارد، ماده ۴ بند ۲ منشور ملل متحد نیز دارای استثناء می‌باشد و آن ماده ۵۱ منشور بوده که مقرر می‌دارد:

در صورت وقوع حمله مسلحانه علیه یک عضو ملل متحد تا زمانیکه شورای امنیت اقدامات لازم برای حفظ صلح و امنیت بین‌المللی را به عمل آورد، هیچ یک از مقررات این منشور به حق ذاتی دفاع از خود، خواه فردی یا دسته جمعی لطمه‌ای وارد نخواهد کرد، اعضاء باید اقداماتی را که در اعمال حق دفاع از خود بعمل می‌آورند فوراً به شورای امنیت گزارش دهند. این اقدامات به هیچ وجه در اختیار و مسئولیتی که شورای امنیت بر طبق این منشور دارد و به موجب آن برای

حفظ و اعاده صلح و امنیت بین‌المللی و در هر موقع که ضروری تشخیص دهد اقدام لازم بعمل خواهد آورد تأثیری نخواهد داشت.

ماده ۵۱ منشور ملل متحد مبنای قانونی پیمان‌های نظامی از جمله ناتو، ورشو و پیمان‌های مشابه دیگر است که حق دفاع جمعی علیه متجاوز را به رسمیت شناخته است، اما آنچه مورد پذیرش اکثریت حقوقدانان بین‌المللی است عدم جواز اقدام به حمله پیش‌گیرانه در مقابل یک خطر قریب الوقوع می‌باشد و اگر کشوری در چنین حالتی ابتدا اقدام به جنگ نماید به احتمال زیاد خود متجاوز شناخته خواهد شد، هرچند که در خصوص حمله پیش‌گیرانه و پیش دستی در حمله نظریات دیگری نیز وجود دارد، اما آنچه که اصل مسلم و مورد قبول اکثریت حقوقدانان است عدم مشروعیت و قانونی نبودن حمله پیش‌گیرانه در حقوق بین‌الملل معاصر است (Akherst, 1984: 262). اما در زمینه مقابله با تهدیدات سایبری نیازمند تفکیک نظری و عملی میان حملات پیش گیرانه و دفاع مشروع هستیم. چه اینکه دفاع مشروع در برابر این حملات پذیرفتی و حمله پیشدستانه قبل از آنکه اقدام آشکاری صورت گیرد، پذیرفتنی نیست. اما سیاسیون و دانشمندان روابط بین‌الملل نظر دیگری دارند، آنها معتقدند که عدم مشروعیت و محرومیت از پیش دستی در حمله بعنوان حق دفاع در برابر خطر یک حمله قریب‌الوقوع، کشورها را از مزیت نظامی وارد آوردن ضربه اول محروم می‌نماید. هرچند که مزیت وارد آوردن ضربه اول در مخاصمه و جنگ بین کشورها به همان اندازه منازعه بین دو فرد تعیین کننده و سرنوشت‌ساز نیست و حتی مورد تردید است که یک قدرت هسته‌ای بتواند در ضربه اول با بمب اتمی تمام زیرساخت-های یک کشور را تخریب نماید (Ibid: 263).

نتیجه‌گیری

فضای سایبر به عنوان بارزترین جلوه عصر ارتباطات و اطلاعات همانند همه دستاوردهای بشری، تهدیدها و فرصت‌های بسیاری را فراروی جوامع بشری قرار داده است. این حوزه هم با اقبال جهانی مردم و کاربران خصوصی روبرو شده و هم مورد توجه فزاینده دولت‌ها در جهت خدمات عمومی مانند دولت الکترونیک و حتی مسائل نظامی قرار گرفته است. با توجه به ویژگی‌هایی که فضای سایبر دارد، تهدیدات جدیدی از سوی دولت‌ها و بازیگران غیردولتی

دیگر، این فضا را احاطه کرده است و هر یک از بازیگران سیاسی درصدد هستند تا با اتخاذ رویکردهای حقوقی و یا نظامی، تهدیدات ناشی از حملات سایبری را به حداقل رسانیده و یا اینکه مانع بروز حملات دیگری علیه خود شوند و از مهاجمان در شرایط مختلف اقامه دعوی نماید. با این اوصاف، راهکارهای متعددی در عرصه داخلی و بین‌المللی دیده می‌شوند که هر کدام با توجه به شدت حملات سایبری، تلقی تهدیدآمیز بودن و یا نبودن آن، هویت کشور و یا گروه مهاجم و همچنین وقوع آن در زمان و مکان دارای تفسیر و معنای خاص خود هستند. با در نظر گرفتن اینکه تهدیدات سایبری می‌تواند طیفی از حمله ساده تا حملات سایبری و حتی جنگ سایبری و تروریسم سایبری نامیده شوند، ابزارهای حقوقی و حتی نظامی متعددی برای مقابله با این تهدیدات وجود دارند. با توجه به اینکه محور پژوهش حاضر، توجه به راهکارهای حقوقی برای مقابله با تهدیدات سایبری است، رویکردهای حقوقی داخلی از توان اثرگذاری و پذیرش بالای کمتری نسبت به قوانین حقوقی بین‌المللی برخوردار هستند. به همین جهت به چند روش حقوقی کارآمد در عرصه حقوق بین‌المللی می‌توان اشاره نمود که شامل: توسل به مفاد و مواد متعددی منشور ملل متحد است که با توجه به قابل تفسیر بودن تهدید در آن، قابل تفسیر بودن تهدید صلح و امنیت کشورها، رویکرد حقوقی قابل توجهی است. علاوه بر این نهادهای دیگری از جمله دیوان بین‌المللی دادگستری نیز نقش مهمی در رسیدگی به پرونده‌های حقوقی مرتبط با تهدیدات سایبری بر عهده می‌گیرند. با توجه به اینکه در رسیدگی به پرونده‌های مرتبط با فضای سایبری بر رسیدگی دقیق به مهاجم، اهداف و ابزارهای آن و همچنین بازگرداندن خسارت نیز تأکید می‌شود، بهره‌گیری از آن نیز می‌تواند قوانین حقوقی در فضای سایبری را غنای بیشتری ببخشد. توسل به اعلامیه‌های اختصاصی در زمینه امنیت سایبری نیز رویه حقوقی و قانونی دیگری در این زمینه است. در نهایت اینکه در صورت ناکارآمدی روش‌های مزبور و در شرایطی که حجم و دامنه تهدیدات سایبری گسترده باشد، توسل به دفاع مشروع ابزار نظامی مؤثری برای جمهوری اسلامی ایران در نظر گرفته می‌شود.

فهرست منابع

باقری، رضا (۱۳۹۷)، پدیده‌های ناامنی نرم‌افزاری و امنیت هستی‌شناختی در جمهوری اسلامی ایران(تـأثیر فضـای سایبر بر هویت فردی و ملی)، پایان‌نامه دکتری، گروه علوم سیاسی، دانشگاه شهید باهنر.

جلالی، محمود، توسلی اردکانی، سعیده (۱۳۹۸)، ضرورت ایجاد نظام هماهنگ حقـوقی بـین‌المللـی در مقابلـه بـا جرایم در فضای مجازی، فصلنامه مطالعات حقوق عمومی، دوره ۴۹، شماره ۴، صص ۱۳۷۲-۱۳۵۱.

جی پست، دیوید (۱۳۸۵)، هرج ومرج، دولت واینترنت، جسـتاری در بـاب قـانون‌گـذاری در فضـای شـبکه ای، ترجمه پرویزعلوی، فصلنامه علمی ـ پژوهشی دانشگاه آزاد اسلامی واحد آشتیان، پیش شماره ۱، پاییز ۱۳۸۵.

زمانی، سید قاسم (۱۳۷۷)، جایگاه قاعده آمره در میان منابع حقوق بین‌الملـل، مجلـه حقـوقی شـماره ۲۲، صـص ۳۰۵-۳۳۴.

سلیمانی‌پورلک، فاطمه (۱۳۹۲)، قدرت نـرم در اسـتراتژی خاورمیانـه‌ای آمریکـا، چـاپ سـوم، تهـران، انتشـارات پژوهشکده مطالعات راهبردی.

ضیایی، سیدیاسر؛ شکیب‌نژاد، احسان (۱۳۹۶)، "قانونگذاری در فضای سایبر"، مجله حقوقی بین‌المللی، دوره ۳۴، شماره۵۷.

عظیمی، فاطمه، خشنودی، هـادی (۱۳۹۵)، "نقـش تروریسـم سـایبری در تهدیـد علیـه امنیـت ایـران و راه‌هـای پیش‌گیری از آن"، فصلنامه مطالعات سیاسی، سال نهم، شماره ۳۴، صص ۱۷۲-۱۵۹.

قاسمی، علی، چهاربخش، ویکتوربارین (۱۳۹۱)، "حملات سایبری و حقوق بین‌الملل"، مجله حقوقی دادگستری، شماره ۷۸، صص ۱۴۶-۱۱۵.

قنبری جهرمی، محمدحسین (۱۳۹۹)، "فلسفه جنگ‌های نیابتی در عصر جدید"، مجله سیاست دفاعی، (۱۱۳)۲۹.

Akeherst, Micheal (1984), A Modern Introduction to International Law, op.cit.pp.259 - 262

Albakri, M., Sturm, L., Williams, C. B., & Tarazaga, P. (2017). Impedance-based non-destructive evaluation of additively manufactured parts. Rapid Prototyping Journal, 23(3), 589–601. https://doi.org/10.1108/RPJ-03-2016-0046.

Anthony Aust, Handbook of International Law, Cambridge University Press, New York, 2010, p. 40.

Chander, Anupam & Madhavi Sunder, "The Romance of the Public Domain", California Law Review, vol. 92, 2004.

Chesterman,S. T.M.Franck and D.M.Mallone,(2008) Law and Practice of the United Nations, Oxford.

Elhabashy, Ahmad E., Lee J. Wells, Jaime A. Camelio & William H. Woodall (2014), A cyber-physical attack taxonomy for production systems: a quality control perspective, Journal of Intelligent Manufacturing volume 30, pages2489–2504 .

Everard, Jerry (2000) Virtual StatesThe Internet and the boundaries of the nation-state, Rutledge publication.

Garner, B.A. (2009), Black's Law Dictionary, Eagan: West Group, 9th ed.

Gellman, Barton(2002), Cyber Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say, WASH. POST, June 27, 2002, at A01.

Hathaway, Oona and Crootof, Rebecca(2012), Levitz Philip, "The Law of Cyber Attack", California Law Review.

Ignarski, Jonathan , Barrister Alfred M. de Zayas (1982), Encyclopedia of Public International Law, Use of force, War and Neutrality Peae Treaties (vol 3), Amsterdam: Published under the Auspices of the Max Planck institute, North Holand Publishing company.

Jiaxuan Fei ; Congcong Shi ; Xuechong Yuan ; Rui Zhang (2019), Wei Chen Reserch on Cyber Attack of key Measurement and Control Equipment in Power Grid, IEEE Digital Library, https://ieeexplore.ieee.org/abstract/document/87913016.

Lewis, James Andrew(2020), "Cyber Stability, Conflict Prevention, and Capacity Building", Center for Strategic and International Studies in Washington, D.C.

Michele L., Frank, Jonathan H. Grenier, and Jonathan S. Pyzoha (2019), How Disclosing a Prior Cyberattack Influences the Efficacy of Cybersecurity Risk Management Reporting and Independent Assurance. Journal of Information Systems: Vol. 33, No. 3, pp. 183-200.

Weisbord, N.(2009), "Conceptualizing Aggression", Duke J.Comp. & Int'l L., No. 20.