DOI: 10.22034/ISJ.2022.305392.1603

International Studies Journal (ISJ)
Vol. 19, No. 2 (74), Fall 2022
Reseived Date: 2022/4/13
Accept Date: 2022/9/17
Article Type: Original Research
PP: 163-178

فصلنامه مطالعات بین‌المللی
سال ۱۹، شماره ۲ (۷٤)، پاییز ۱٤۰۱
تاریخ دریافت: ۱٤۰۱/۱/۲٤
تاریخ پذیرش: ۱٤۰۱/٦/۲٦
نوع مقاله: علمی- پژوهشی
صفحات: ۱۷۸-۱٦۳

ضرورت همکاری دولت‌ها در تقویت امنیت سایبری*

پرویز فرشاسعید**- دکتر محمود جلالی***- دکتر مهناز گودرزی****

چکیده

حملات سایبری معضلی جهانی است که امنیت جهان را با تهدیدات زیادی مواجه نموده است. همه روزه شاهد حملات سایبری در سطح جهان هستیم به نحوی که فعلا هیچ نقطه ای از جهان در برابر این حملات مصون نمی‌باشد. ظرفیت‌ها و پتانسیل‌هایی که فضای سایبری برای جامعه بشری به ارمغان آورده باعث گردیده تعدادی از کشورها از این ظرفیت‌ها برای مقاصد سیاسی و اقتصادی خود سوءاستفاده نمایندکه این باعث بر هم خوردن امنیت سایبری جهانی گردیده است.آنچه می‌تواند به حل این معضل در جهان کمک نماید همکاری دولت‌ها در سطح بین‌المللی برای تقویت امنیت سایبری خویش می‌باشد. سؤالی که در این تحقیق مطرح می‌گردد این است که چه ضرورتی برای دولت‌ها وجود دارد تا جهت تقویت امنیت سایبری با یکدیگر همکاری نمایند؟با روش توصیفی- تحلیلی به این سؤال پاسخ داده شده که به دلیل اینکه تمام جنبه های زندگی بشری به فناوری‌های حوزه سایبری وابسته شده و چنین سطح از وابستگی موجب سوءاستفاده بعضی از دولت‌ها در ارتکاب حملات سایبری به زیرساخت‌های حیاتی دولت‌ها می‌گردد نیاز است تا جهت تقویت امنیت سایبری همکاری‌هایی در سطح بین‌المللی توسط دولت‌ها صورت گیرد.

کلیدواژگان

امنیت سایبری، حملات سایبری، سطح بین‌المللی، فضای سایبری، همکاری دولت‌ها

* این مقاله برگرفته از رساله دکتری پرویز فرشاسعید با عنوان «قلمرو انطباق اصول حاکم بر دفاع مشروع سنتی با دفاع مشروع در فضای سایبر از دیدگاه حقوق بین‌الملل» با راهنمایی دکتر محمود جلالی است.

** دانشجوی دکتری حقوق بین‌الملل عمومی، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان (خوراسگان)، ایران.

*** دانشیار گروه حقوق دانشگاه اصفهان، اصفهان، ایران. (نویسنده مسئول)/ایمیل: m.jalali@ase.ui.ac.ir

**** دانشیار گروه روابط بین‌الملل، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان (خوراسگان)، ایران.

Article Link: https://www.isjq.ir/article_158974.html

مقدمه

اختراع کامپیوتر و اینترنت مهم‌ترین تحولی بوده که در طول تاریخ تمدن بشری حادث گردیده است. تمام زیرساخت‌های حیاتی کشورها مانند ارتباطات، دفاع، انرژی، حمل و نقل، کشاورزی، بهداشت و امور اقتصادی توسط فضایی به نام فضای سایبری به هم متصل و مرتبط شده است. این فضا از یک طرف باعث سهولت انجام کارها شده و از طرف دیگر خطرات زیادی را برای جامعه بشری به ارمغان آورده است. در گذشته رقابت اصلی دولت‌ها در عرصه‌های نظامی و فناوری‌های مرتبط با این حوزه بود ولی در حال حاضر رقابت دولت‌ها به فضای سایبری نیز تسری یافته است و هر از گاهی اخباری در رسانه‌ها درج می‌گردد که علیه کشوری حمله سایبری صورت گرفته است. اگر چه در بحث ارتکاب حملات سایبری انگیزه‌های فراوانی برای دولت‌ها و اشخاص وجود دارد ولی مهم‌ترین انگیزه‌ها سیاسی و اقتصادی می‌باشند. ایالات متحده آمریکا به دلیل سیاست‌های هژمونیک و قلدرمآبانه اش باعث قطب بندی هایی در سطح جهانی و منطقه‌ای گردیده است. در سطح جهانی کشورهایی مانند روسیه، ایران، چین و کره شمالی مقابل دولت ایالات متحده آمریکا قرار گرفته و رقابت‌های خودشان را به فضای سایبری کشانده‌اند. در سطح منطقه‌ای نیز وضع به همین گونه است به عنوان مثال در خاورمیانه که متشنج‌ترین جای دنیا می‌باشد فارغ از منازعات و درگیری‌های نظامی که در سوریه، عراق و یمن وجود دارد کشورهای اسرائیل و عربستان در مقابل کشور جمهوری اسلامی ایران قرار گرفته‌اندکه به‌طور متقابل حملات سایبری را علیه یکدیگر هدایت می‌نمایند. در شبه‌جزیره کره نیز رقابت و دشمنی شدیدی بین دوکشور کره شمالی و جنوبی وجود دارد که احتمال ارتکاب حملات سایبری از طرف این کشورها علیه یکدیگر را شدت می بخشد. شبه قاره هند نیز متشنج است، زیرا رقابت سنگینی بین دوکشور هند و پاکستان وجود دارد و هر از گاهی این کشورها حملات سایبری را علیه یکدیگر هدایت می‌نمایند. در قاره آمریکا هم دولت ایالات متحده آمریکا و تعدادی از کشورهای آمریکای لاتین حملات سایبری را علیه دولت ونزوئلا هدایت می‌نمایند. چنین وضعیت پیچیده و بغرنجی در جهان باعث شده آینده خطرناکی را برای صلح و امنیت بین‌المللی پیش بینی کنیم. در تحقیق پیش‌رو این سؤال مطرح گردیده که ضرورت همکاری دولت‌ها جهت تقویت امنیت سایبری چه می‌باشد؟ با روش توصیفی- تحلیلی به این سؤال پاسخ داده ایم که به دلیل اینکه تمام جنبه های حیات بشری به فناوری‌های حوزه سایبری وابسته شده و چنین سطح از وابستگی موجب سوءاستفاده بعضی از دولت‌ها در ارتکاب حملات سایبری به زیرساخت‌های حیاتی کشورها در سطح جهان می‌گردد، نیاز است تا جهت تقویت امنیت سایبری در سطح بین‌المللی همکاری‌هایی بین دولت‌ها صورت گیرد.

۱-پیشینه

در رابطه با موضوع مورد بحث مقاله حاضر یعنی «ضرورت همکاری دولت‌ها در تقویت امنیت

سایبری » در زبان فارسی مقاله ای مشاهده نگردید، اما در رابطه با امنیت سایبری از جوانب متعددی تحقیقاتی انجام گرفته که در این قسمت به چند مورد از این مقالات اشاره می‌نمائیم. مقاله ای با عنوان چالش‌های امنیت سایبری درکشورهای آسه‌آن[۱](کتانچی و قهرمان‌پور، ۱۴۰۰: ۱۵۶-۱۳۹)؛ (Katanchi & Poorghahremani, 2021:139-156) منتشر شده که یافته‌های این پژوهش نشان می‌دهد که در مورد شاخص های مطالعاتی امنیت سایبری به خصوص در زمینه سیاست‌های دولت و محافظت در برابر حریم خصوصی در برخی ازکشورهای آسه آن تحقیقات محدود صورت گرفته است که این موضوع ارتباط مستقیم با افزایش جرایم سایبری دارد. این مقاله نتیجه گرفته است که برای غلبه بر موانع در امنیت سایبری، همه کشورهای آسه آن باید همکاری نمایند. به دلیل اینکه این مقاله تنها به بررسی امنیت سایبری در کشورهای آسه آن از سال ۲۰۱۴ تا سال ۲۰۱۹ می‌پردازد و این کشورها جزء کشورهای پیشرفته در حوزه سایبری نیستند تنها دارای اعتبار تحقیقاتی می‌باشد.

در مقاله دیگری با عنوان مروری بر امنیت سایبری؛ درس‌هایی برای جمهوری اسلامی (برقعی، ۱۳۹۳: ۱۰۴-۸۵)؛(Borqe'I,2014:85-104) نویسنده ابتدا انواع حملات سایبری را ذکرکرده و ویژگی های آنها را بیان نموده است. سپس به بیان راهبرد دولت آمریکا و دولت‌های اروپایی در قبال حملات سایبری پرداخته و در نهایت نتیجه گرفته است که جمهوری اسلامی ایران باید به تدوین «استراتژی امنیت ملی سایبری» خودش بپردازد. اگر چه نقطه قوت این مقاله ارائه راهبرد دولت آمریکا و دولت‌های اروپایی به عنوان دول پیشرو در فناوری‌های حوزه سایبری است اما نقطه ضعف آن عدم اشاره به راهبرد دولت‌های چین و روسیه در قبال حملات سایبری به عنوان دو کشور بسیار مهم در حوزه سایبر می‌باشد.

در اثر دیگری با عنوان امنیت سایبری در انرژی نگرشی جامع (Vasileiou, 2019: 1-61) نویسنده بیان می کند که دولت‌ها باید به یک تعریف مشترک از مفهوم امنیت سایبری و حمله سایبری برسند، زیرا چنین اقدامی می‌تواند مسئله انتساب یک حمله و مجازات عامل آن را آسانتر نماید. این مقاله اگر چه به دلیل اینکه به بحث امنیت سایبری در حوزه انرژی به عنوان مهم‌ترین حوزه تمدنی بشری پرداخته است دارای ارزش و اعتبار وافریست اما چون به صورت تک بعدی به مسئله امنیت سایبری نگریسته نمی‌تواند به‌طور جامع انتظارات امنیت سایبری را برآورده نماید.

در مقاله دیگری با عنوان نقش امنیت سایبری در جهان سیاست (Taskanian, 2017: 339-348)، این سئوال مطرح گردیده که چگونه امنیت سایبری روابط بین دولت‌ها را تحت تاثیر قرار می‌دهد و فضای سایبری در این رابطه چه نقشی بازی می‌نماید؟ نویسنده ابتدا مطالبی را درباره وابستگی مردم و کشورها به فضای سایبری و فناوری‌های این حوزه بیان نموده و سپس اقدامات سه کشور ایالات متحده آمریکا، فدراسیون روسیه و چین را در بحث امنیت سایبری مطرح نموده است و

---

۱. ASEAN

نتیجه‌گیری کرده که امنیت سایبری نقش مهم و ویژه‌ای در جهان سیاست دارد. این مقاله چون اقدامات سه کشور مهم و پیشرفته در حوزه فناوری سایبری را در بحث امنیت سایبری مطرح نموده است دارای ارزش فراوانی است.

آنچه که مقاله پیش‌رو را از مقالات منتشر شده قبلی متمایز می‌نماید ارائه راهبردهایی برای تقویت امنیت سایبری در سطح جهان می‌باشد. نویسنده در ابتدا دلایل و ضرورت‌های همکاری دولت‌ها جهت تقویت امنیت سایبری را مطرح نموده و سپس راهبردهایی را که دولت‌ها برای تقویت امنیت سایبری خودشان نیاز دارند ارائه نموده است.

۲- چارچوب مفهومی

امنیت موضوعی است که بشر از گذشته‌های دور به دنبال آن بوده است. اکثر دولت‌ها به مسئله امنیت نگرش داخلی دارند و در سطح داخلی برنامه‌هایی را برای تامین امنیت خود تدوین و طراحی می‌نمایند. حتی در بحث حوزه سایبری نیز که حوزه فرامرزی است دولت‌هایی مانند چین تمایل کمتری به مشارکت در سطح بین‌المللی نشان می‌دهند و برنامه‌هایی داخلی برای تامین امنیت سایبری خود دارند. پایه و اساس هر کشوری بر اساس مجموعه‌ای از زیرساخت‌های حیاتی آن کشور در بخش های ارتباطات، دفاع، انرژی، حمل و نقل،کشاورزی، بهداشت و امور اقتصادی است که فضای سایبر مانند یک سیستم عصبی، آنها را به هم مرتبط می‌نماید. «امروزه این نگرانی برای دولت‌ها ایجاد شده که حملات مبتنی بر فضای مجازی می‌توانند سرویس‌های ارتباطی، اقتصادی و حیاتی کشورها را مختل نموده و موجب خسارات شدید گردند»(برقعی، ۱۳۹۳: ۸۵)؛(Borqe'I, 2014: 85). افزایش فعالیت‌های دورکاری و خدمات غیر حضوری به دلیل همه‌گیری ویروس کرونا در سراسر جهان باعث افزایش تهدیدات سایبری و مخرب شده است. به دلیل اینکه افزایش حملات سایبری تهدیدی جهانی به شمار می رود نیاز است تا دولت‌ها خطر این تهدید را جدی بشمارند و با همکاری هم و تقسیم کار، امنیت سایبری‌شان را افزایش دهند. بنابراین امنیت سایبری نمی‌تواند بدون همکاری بین‌المللی به نتیجه‌ای برسد. در ۳۰ آوریل سال ۲۰۲۰ جوزپ بورل[1] نماینده عالی اتحادیه اروپا در امور خارجی و سیاست امنیتی بیانیه‌ای را در خصوص فعالیت‌های سایبری مخرب در شرایط همه‌گیری بیماری کرونا[2] منتشر کرد. در این بیانیه بیان شده است که « از زمان گسترش همه‌گیری ویروس کرونا در سراسر جهان،اتحادیه اروپا و دولت‌های عضو این اتحادیه با تهدیدها و فعالیت‌های سایبری مخربی روبه‌رو بوده و هستند. فعالیت‌هایی که اپراتورهای کلیدی به‌ویژه در

[1]. Josep Borrell

[2]. Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic,30 April 2020, https://eucyberdirect.eu

بخش سلامت در این دولت‌ها و شرکای بین‌المللی را مورد هدف قرار داده‌اند»(Borrell, 2020: para 4). در این بیانیه «به تقویت همکاری های تکنیکی،عملیاتی، قضایی و دیپلماتیک با شرکای بین‌المللی تاکید شده است»(Borrell, 2020: para 4). همچنین « اتحادیه اروپا و دولت‌های عضو این اتحادیه در کنار یکدیگر و در کنار آنهایی که (در سراسر جهان) از این همه‌گیری آسیب دیده‌اند،ایستاده و خواهند ایستاد»(Borrell, 2020: para 6). چنانکه مشاهده می‌شود در این بیانیه نیز به تقویت همکاری‌های بین‌المللی تاکید گردیده است. با توجه به این مباحث و خطر حملات سایبری نیاز است تا نگرش دولت‌ها از سطح تامین امنیت داخلی به سطح تامین امنیت بین‌المللی تغییر یابد، زیرا با پیشرفت فناوری‌های حوزه سایبری و ظرفیت‌های این حوزه صلح و امنیت بین‌المللی با چالش‌های جدی مواجه گردیده است.

۳-تاریخچه

فضای سایبری به دلیل ظرفیت‌ها و پتانسیل‌هایی که دارد محیط بسیار امن و کم هزینه ای را برای ارتکاب حملات سایبری برای دولت‌ها فراهم آورده است. « ترکیب فناوری ارتباطات راه دور با فناوری کامپیوتر در اواخر دهه ۱۹۷۰ و اوایل دهه ۱۹۸۰ (بنیان انقلاب اطلاعاتی حاضر) به عنوان نقطه شروع بحث تهدیدات سایبری به حساب می‌آید»(Cavelty, 2012: 105). «بحث امنیت سایبری در ایالات متحده آمریکا در دهه ۱۹۷۰ آغاز گردید در دهه ۱۹۸۰ شتاب گرفت و در اواخر دهه ۱۹۹۰ به سایر کشورها گسترش یافت»(Cavelty, 2012: 104). حملات سایبری با اهداف سیاسی یا اقتصادی انجام می‌گیرند چنانکه در سال ۲۰۰۷ دولت روسیه حملاتی را علیه کشور استونی انجام داد[1]و همچنین حملات استاکس‌نت علیه تاسیسات هسته‌ای ایران در سال ۲۰۱۰[2] با اهداف سیاسی انجام گرفت. پس از شیوع بیماری منحوس کرونا، حملات سایبری علیه کشورهایی مانند بریتانیا، آمریکا و کانادا که جهت تولید واکسن این بیماری در حال تحقیق بودند افزایش یافت. هدف از انجام این حملات سرقت نتیجه تحقیقات در مورد واکسن این بیماری بود. چنین حملاتی بیشتر برای اهداف اقتصادی انجام می‌گرفت، زیرا رقابتی بین‌المللی برای ساخت واکسن کرونا شکل گرفته بود که نتیجه اقتصادی چنین واکسنی می‌توانست میلیاردها دلار را عاید کشور یا کشورهای

[1]. در سال ۲۰۰۷ کشور استونی هدف حملات سایبری قرار گرفت که کل زیرساخت‌های اینترنتی این کشور را تحت تاثیر خود قرار دادند و البته هدف اصلی وب‌سایت‌های دولتی و سازمانی، بانکها و روزنامه‌ها بودند. با توجه به زمان‌بندی حملات که در زمان مجادله این کشور و روسیه بر سر برداشتن یادبود شوروی از پایتخت استونی بود، مقامات استونی روسها را عامل اصلی این حملات می‌دانستند.

[2]. یک ویروس رایانه ای قدرتمند به نام استاکس‌نت، در سال ۲۰۱۰ میلادی برای متوقف کردن برنامه هسته‌ای ایران به تاسیسات هسته‌ای کشورمان حمله کرد. این ویروس به مراکز هسته‌ای کشور، آسیب‌های فراوانی وارد کرد و با آلوده کردن هزاران رایانه به متوقف شدن فعالیت سانتریفیوژهای غنی‌سازی منجر شد.

سازنده آن نماید. « تاریخ تحولات روابط بین‌الملل نشان داده است که مقتضیات زمان، به پیچیدگی های مفهوم امنیت افزوده است به‌ویژه‌اینکه امروزه کشورها نمی‌توانند در معادلات امنیتی و راهبردی خود، از نقش فناوری سایبری و تاثیر آن بر امنیت غافل شوند » (داوند و سلطانی‌نژاد، ۱۳۹۷ :۹۳)؛ (Davand & Soltani Nejad, 2018: 93).

٤- دلایل همکاری دولت‌ها و راهکارهای آنها جهت تقویت امنیت سایبری

در این قسمت به بررسی دلایل همکاری دولت‌ها جهت تقویت امنیت سایبری می‌پردازیم.

٤-۱- افزایش استفاده از رایانه و فناوری‌های اطلاعات

در حال حاضر به دلیل فواید و مزایایی که رایانه ها و فناورهای اطلاعات دارند، استفاده‌کنندگان از این پدیده نوین روزبه‌روز در حال افزایش می‌باشند. اختراع گوشی‌های هوشمند و قابلیت اتصال به اینترنت این گوشی‌ها باعث افزوده شدن تعداد بسیار زیادی از کاربران اینترنت گردید و به دنبال آن با اختراع نرم‌افزارهایی مانند واتساپ و تلگرام و سایر نرم‌افزارهای موبایلی، اینترنت به عنوان بخشی از حیات روزمره انسانها تبدیل شد تا حدی که می‌توان گفت اکثر افراد جامعه در حال حاضر دچار اعتیاد به اینترنت گردیده و شدیدا به آن وابسته شده‌اند. همچنین با توجه به ظرفیت‌ها و پتانسیل‌های رایانه و اینترنت تمام ارکان زندگی بشری به این پدیده نوظهور وابسته گردیده و تمام سازمان‌های دولتی و غیر دولتی به این شبکه متصل شده به نحوی که بدون وجود اینترنت تمدن بشر حاضر، قادر به ادامه حیات نمی‌باشد. چنین حجم گسترده استفاده از اینترنت خطراتی را نیز برای تمدن بشری به همراه آورده است که هر روزه شاهد ارتکاب حملات سایبری متعددی در سر تا سر جهان هستیم که جدید ترین و مهم‌ترین این حملات،حملات سایبری به کشورهایی مانند ایالات متحده آمریکا،کانادا و انگلستان جهت سرقت نتیجه تحقیقات واکسن کرونا بوده است. «شیوع جهانی بیماری کووید ۱۹ یک واقعه بی سابقه برجسته ای بود که زندگی چندین میلیارد نفر در جهان را تغییر داد. اضطراب شدیدی که توسط این بیماری ایجاد شد احتمال حملات سایبری را افزایش داد که باعث افزایش در تعداد و گستره حملات سایبری گردید»(Lallie et.al., 2020: 1). «گسترش بیماری کرونا که از سال ۲۰۱۹ شروع شد تبدیل به یک بحران جهانی گردید که در نتیجه باعث قرنطینه جمعی ۱۰۰ میلیون نفر در کشورهای متعددی در جهان گردید. این خانه نشینی افراد هم تهدید مهمی برای جامعه وابسته به فناوری سایبری گردید یعنی مجموعه‌ای از حملات بی‌هدف و نیز مجموعه‌ای از حملات سایبری و جرائم سایبری هدفمند گردید»(Lallie et.al., 2020: 1).

٤-۲- افزایش قدرت‌های سایبری در جهان

درسطح بین‌المللی سه کشورروسیه، چین و ایالات متحده آمریکا از مهم‌ترین کشورهایی هستند که بیشترین رقابت تسلیحاتی و سرمایه‌گذاری را در حوزه نظامی انجام می‌دهند. از نظر نظامی کشور

چین بزرگترین ارتش جهان را دارد و کشور روسیه دارای بیشترین تعداد تانک‌های جنگی می‌باشد و کشور ایالات متحده آمریکا پیشرفته ترین ماهواره ها را در اختیار دارد. اگر چه کشور ایالات متحده آمریکا در حال حاضر بزرگترین قدرت سایبری جهان است اما به دلیل ظهور قدرت‌های جدید سایبری مانند چین، روسیه و ایران، توان سایبری این دولت با چالش‌های جدیدی مواجه گردیده است. در جریان انتخابات سال ۲۰۲۰ آمریکا، مدیر اطلاعات ملی این کشور جان راتکلیف[1] ایران و روسیه را به تلاش برای مداخله در انتخابات ایالات متحده آمریکا متهم کرد. در سال های اخیر، فضای سایبری به عرصه تقابل بین دولت‌ها تبدیل گردیده است به نحوی که هر روزه شاهد حملات سایبری در سراسر جهان هستیم. رقابت‌های سیاسی دولت‌ها در حال حاضر وارد فضای سایبری گردیده که این باعث شده میلیاردها دلار صرف تقویت توان سایبری آنها در سطح جهان گردد. بنابراین« فضای سایبری و فناوری‌های مرتبط با آن یکی از مهم‌ترین منابع قدرت در هزاره سوم می‌باشند»(Li & Liu, 2021: 8184). بر اساس گزارش جدید دانشگاه هاروارد[2]«کشورهای ایالات متحده آمریکا، چین، بریتانیا، روسیه، هلند، فرانسه، آلمان، کانادا، ژاپن و استرالیا به ترتیب به عنوان ده قدرت برتر سایبری جهان رتبه بندی شده‌اند. دولت اسرائیل در رتبه یازدهم و کشور جمهوری اسلامی ایران نیز در رتبه ۲۳ این رتبه بندی قرار دارد و عربستان سعودی نیز پس از ایران در رتبه ۲۶ می‌باشد»(Voo et.al. , 2020: 8).

۳-٤- افزایش رو به رشد حملات سایبری درجهان

داده‌ها و اطلاعات افراد منابعی هستند که معمولا در معرض خطر حملات سایبری قرار دارند و در پاره ای مواقع لطمات سنگینی را به بدنه یک کشور وارد می‌نمایند. با رشد فعالیت‌های اینترنتی و آنلاین شدن کارها و ذخیره اطلاعات در فضای سایبری در دنیا، شاهد افزایش روزافزون این سوءاستفاده‌های اینترنتی و دزدیده شدن اطلاعات هستیم که گاه فضای ناامنی را برای رد و بدل کردن اطلاعات فراهم می‌نماید. هزینه پایین حملات سایبری نسبت به سلاح‌های سنتی و کلاسیک باعث شده که کشورها تمایل بیشتری به استفاده از این نوع حملات داشته باشند.

٤-٤- نبود قوانین روشن و شفاف برای حوزه سایبر

نبود قوانین روشن و شفاف برای حوزه سایبر معضلی است که باید برای آن چاره ای اندیشیده شود. «سرعت پیشرفت فناوری و ویژگی های منحصر به فرد فضای سایبر سبب تغییر بسیاری از مفاهیم سنتی حقوق بین‌الملل شده و در مواردی شکل نگرفتن رژیم های هنجاری منسجم تنها زمینه تفسیر جدید از مفاهیم سنتی را فراهم کرده است»(شهبازی، آقاجانی رونقی، ۱۳۹۹: ۱۴۸۷)؛ (Shahbazi & Aghajani Ronaghi, 2021: 1487). «حملات سایبری یک پدیده نوظهور است که هنوز قاعده حقوقی معتبری در قالب معاهدات یا عرف بین‌المللی در خصوص آن شکل نگرفته

[1]. John Ratcliffe

[2]. Harvard University

است»(قاسمی و نامدار، ۱۳۹۷: ۲۲۸)؛(Ghasemi & Namdar, 2018: 228). در حال حاضر اصلی‌ترین معاهدات بین‌المللی در حوزه سایبر «کنوانسیون ۲۰۰۱ جرایم سایبری »[1]و پروتکل الحاقی ۲۰۰۶ آن و « توافقنامه امنیت اطلاعاتی بین‌المللی سازمان همکاری شانگهای ۲۰۰۹»[2]می‌باشند.

این دو معاهده نقاط ضعف مهمی‌دارند که یکی تعداد دولت‌های عضو و دیگری قلمرو محدود آنها می‌باشد. تا کنون اقدام مهمی که در حوزه سایبر مطرح شده این بوده است که چطور حقوق بین‌الملل موجود را در حوزه فضای سایبر بکار گیرند. دستورالعمل تالین[3] قابل اعمال در جنگ های سایبری که دارای مجموعه‌ای از قوانین است که چطور حقوق بین‌الملل موجود مانند حق بر جنگ، حقوق بین‌الملل بشر دوستانه و حقوق مسئولیت دولت در فضای سایبر بکار می رود. «متاسفانه اینکه راهنمای تالین نتوانست خارج از گروه محدود اعضای ناتو که از آن حمایت می نمودند مورد توجه قرار گیرد»(Lucas, 2017: 40). علت این است که دستورالعمل تالین قوانین جدید بین‌المللی برای حوزه سایبر ارائه نداده بلکه قوانین حقوق بین‌الملل موجود را تفسیر نموده است. «اینترنت مانند هر امر اجتماعی دیگری نیازمند نظام دهی است و بخشی از این نظام دهی در قالب تدوین قوانین و مقررات انجام می‌شود استفاده از اینترنت و فناوری‌های مرتبط با آن امری حیاتی برای کل جامعه بشری می‌باشد.کنار گذاشتن این فناوری از ترس آسیب‌ها و مضرات آن اقدامی نسنجیده بوده و دولت‌هایی موفق هستند که بتوانند با تدابیر و اقدامات مناسب ضمن استفاده کامل از تمام فواید و امکانات اینترنت آسیب‌های آن را از بین برده یا به حداقل برسانند»(رضایی و بابازاده مقدم، ۱۳۹۳: ۸۰-۷۹)؛(Rezai & Babazade Moghadam, 2014: 79-80).

٥-٤- راهبرد دولت‌ها در تقویت امنیت سایبری

برای اینکه بتوان امنیت سایبری جهانی را تقویت نمود باید زمینه همکاری دولت‌ها در تقویت امنیت سایبری فراهم آید. چنین کاری صورت نخواهد گرفت مگر اینکه دولت‌ها با همکاری یکدیگر و تدوین معاهده بین‌المللی در این زمینه شرایط همکاری بین‌المللی خود را فراهم آورند. به دلیل اینکه هنوز مسئله استفاده از فناوری سایبری موضوعی تازه می‌باشد و مضرات و فوائد آن به‌طور کامل مشخص نگردیده است، یکی از مهم‌ترین مشکلات موجود بر سر راه یک معاهده

[1]. کنوانسیون جرایم سایبری معروف به «کنوانسیون جرایم سایبری بوداپست» یا به اختصار «کنوانسیون بوداپست» نخستین معاهده بین‌المللی است که به جرائم رایانه‌ای و اینترنتی می‌پردازد و می‌کوشد قوانین ملی را سازگار کرده، روش‌های تحقیقات را ارتقا دهد و همکاری بین کشورها را بهبود بخشد. این کنوانسیون توسط شورای اروپا در سال ۲۰۰۱ ارائه شد و از ۲۳ نوامبر ۲۰۰۱ کشورها می‌توانستند آن را امضا کنند. از ابتدای ژوئیه ۲۰۰۴ کنوانسیون به اجرا درآمد.

[2]. The agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security.

[3]. Tallin Manual

بین‌المللی درباره فناوری‌های حوزه سایبر این است که هنوز برای مذاکره درباره آن زود است. « از نظر تاریخی معاهدات حاکم بر فناوری‌های سلاح‌های جدید تنها پس از اینکه این فناوری‌ها برای مدتی مورد استفاده قرار گرفته‌اند تدوین شده‌اند»(Eilstrup Sangiovanni, 2017: 401). مهم‌ترین مشکل و مانع بر سر همکاری بین‌المللی دولت‌ها در حوزه سایبر عدم تمایل قدرت‌های بزرگ سایبری می‌باشد، زیرا با این وضعیت آشفته و پر از هرج‌ومرج بین‌المللی قدرت‌های بزرگ سایبری مانند روسیه، چین و آمریکا در حال حاضر استفاده‌های فراوانی از این حوزه می برند که مشکل است چنین دولت‌هایی را به راحتی بتوان وادار به همکاری بین‌المللی در حوزه سایبری نمود.اگر چه «قرار گرفتن در معرض انواع مختلف حملات سایبری درک تهدیدات سایبری را افزایش می‌دهد و نگرش های سیاسی را در حمایت از سیاست‌های سختگیرانه سایبری تغییر می‌دهد» (Snider, 2021: 7).

۱-۵-٤- افزایش همکاری بین‌المللی

به دلیل اینکه حملات سایبری پدیده ای بین‌المللی است نیاز است تا جهت مواجهه با این پدیده همکاری‌هایی در سطح بین‌المللی انجام گیرد. «دنیای سایبر بستر مشترک منافع و تهدیدهای جامعه ملل امروز است و دولت‌ها را وادار کرده تا علی رغم افتراق ها و اختلاف های دنیای فیزیکی به یکپارچگی روی آورند و از این نگاه معاهده های فراملی سایبری نقش تعیین کننده ای را ایفا می‌کنند»(فقیهی و جلالی‌فراهانی، ۱۳۹۷: ۱)؛(Faghihi & Jalali Farahani, 2018: 1). اگر چه به دلیل جبهه بندیهای بین‌المللی و رقابت دولت‌ها مشکل است به راحتی بتوان همکاری قطعی و صد درصدی آنها را در سطح بین‌المللی انتظار داشت ولی ضرورت حفظ صلح و امنیت بین‌المللی باعث می‌گردد دولت‌ها تا حدی تشویق به همکاری بین‌المللی گردند. این همکاری بین‌المللی تنها می‌تواند در قالب تدوین یک معاهده جامع و کامل درباره ممنوعیت کامل انجام حملات سایبری نمود پیدا کند.

۲-۵-٤- تقسیم کار جهانی

برای اینکه امنیت سایبری بین‌المللی تقویت گردد باید در سطح جهانی تقسیم کار صورت گیرد. حملات سایبری تهدیداتی جهانی هستند که تنها با راه‌حلی جهانی می‌توان چنین تهدیداتی را کنترل و برطرف نمود. ابتدا باید حوزه فعالیت شرکت های فعال در حوزه اینترنت و فعالیت‌های مرتبط با آن مشخص گردد و با تدوین قوانین روشن و شفاف جلو سوءاستفاده این شرکتها گرفته شود. سپس کشورهای دنیا را ملزم به تصویب قوانین داخلی جهت مقابله و برخورد با افراد، شرکت ها و سازمان‌هایی نمود که اقدام به ارتکاب حملات سایبری علیه دولت‌های دیگر می‌نمایند. البته انجام چنین اقداماتی بسیار سخت و مشکل می‌باشد زیرا درپاره‌ای از کشورها نهادهایی وجود دارند که اقدامات کاملا خودسرانه انجام می‌دهند و به هیچ نهاد یا ارگان داخلی پاسخگو نیستند. چنین سازمان‌هایی آنقدر قدرت و اختیار دارند که به نهادهای انتخابی و مردمی پاسخگو نمی‌باشند و البته

بیشتر چنین نهادها و سازمان‌هایی نظامی می‌باشند که علاوه بر انحصار کنترل زیرساخت‌های سایبری، نهاد های قوی و قدرتمند غیر انتخابی را نیز در اختیار دارند و این باعث می گردد در سطح داخلی به هیچ وجه امکان پاسخگو نمودن چنین نهادهایی وجود نداشته باشد. «تهدیدهای سایبری به علت برخورداری از ویژگی هایی چون قیمت پایین ورود، گمنامی و تاثیرگذاری شگرف، پدیده ای به نام انتشار قدرت را بوجود آورده است که نه تنها باعث شده دولت‌های کوچک از ظرفیت بیشتری برای اعمال قدرت در این فضا برخوردار شوند، بلکه منجر به ورود بازیگران جدیدی همچون شرکت ها، گروههای سازمان یافته و افراد به معادلات قدرت جهانی شده است. بنابراین، این پدیده امنیت ملی را از ابعاد مفهوم امنیت،دولت محوری در امنیت، بعد جغرافیایی تهدید، گستردگی آسیب پذیری ها، شیوه مقابله با تهدیدها و تعدد بازیگران در این عرصه تحت تاثیر قرار داده است»(خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۶۷)؛(Khalilipoor Rokn Abadi & Noor alivand, 2012: 167).

۳-۵-٤- تغییرات راهبردی در مفهوم امنیت

امنیت در گذشته دارای مفهومی ملی بود و دولت‌ها داخل مرزهای خود به این مساله توجه می کردند و به آن می پرداختند. در داخل کشورها سازمان‌های مختلفی جهت حفظ و برقراری امنیت داخلی کشورها تاسیس گردیده است. سازمان‌های نظامی و اطلاعاتی وظیفه حفظ امنیت داخلی کشورها را برعهده دارند. با گسترش و توسعه سلاح‌های کشتارجمعی و سلاح‌های دوربرد مانند انواع موشکها و سایر تسلیحات پیشرفته، امنیت مفهومی جهانی یافت تا حدی که دولت‌ها اقدام به تاسیس سازمان‌های جهانی و منطقه‌ای جهت برقراری صلح و امنیت بین‌المللی و منطقه‌ای نمودند که چنین سازمان‌هایی اگر چه به صورت صد درصد جهت حفظ صلح و امنیت بین‌المللی موفق نبوده‌اند ولی تا حدی می‌توان گفت که سازمان‌هایی مانند سازمان ملل متحد[1]و پیمان آتلانتیک شمالی ناتو[2] تا حدی توانسته‌اند در حفظ صلح و امنیت بین‌المللی موفق شوند. اما ظهور اینترنت و فناوری‌های مرتبط با آن عصر جدیدی را در تمدن بشری آغاز نمود. فناوری‌های حوزه سایبری مفهوم امنیت ملی را به مفهوم امنیت جهانی و بین‌المللی تغییر داد زیرا فناوری سایبری با حذف نمودن مرزها تهدیدات جدید و خطرناکی را برای تمدن بشری به ارمغان آورد. در حال حاضر وجود یک سیستم و یک ارتباط اینترنتی تنها سلاحی است که هر فردی می‌تواند با کمترین هزینه خسارات بسیار زیاد و گسترده ای را به یک شرکت یا دولتی وارد نماید. به دلیل نیاز شدید دولت‌ها به فضای سایبری مفهوم دهکده جهانی در حال حاضر شکل گرفته و تمام دولت‌ها و کشورها در مسیر ارتباطات اینترنتی قرار دارند. «فناوری اطلاعات و ارتباطات به عنوان متغیری جدید مطرح

[1]. United Nations

[2]. North Atlantic Treaty

است که در قالب نظریات سایبر پلتیک و مبتنی بر مفهوم ارتباطات فراتر از آنچه پیش از این مطرح می شد ابعاد و تعابیر مختلف امنیت نظامی، اقتصادی، سیاسی، اجتماعی و فرهنگی و زیست محیطی را تحت تاثیر قرار داده است»(سلطانی‌نژاد و همکاران، ۸:۱۳۹۵)؛(Soltani Nejad et.al., 2016 :8). «مفهوم امنیت با مفهوم تهدید رابطه ای تنگاتنگ دارد به این معنی که تامین یا عدم تامین امنیت در جایی مطرح می‌شود که تهدیدی وجود داشته باشد. بر این اساس باید گفت در فرایند تاریخ با تغییر مفهوم تهدیدات، مفهوم امنیت نیز تغییر پیدا کرده است؛ اما در این مسیر وجود یک متغیرمیانجی به نام فناوری اطلاعات و ارتباطات توانسته است منجر به باز تعریف این مفاهیم و به صورت خاص مفهوم امنیت گردد. بنابراین همزمان با فرایند جهانی شدن فناوری‌های اطلاعات و ارتباطات تسهیلات و تهدیدات جدید نیز ظهور یافته است»(سلطانی‌نژاد و همکاران، ۱۳۹۵: ۱۳۸)؛(Soltani Nejad et.al., 2016 :38). قبل از اختراع اینترنت برهم زدن امنیت کشورها تنها با استفاده از سلاح‌های کلاسیک انجام می‌گرفت که دسترسی مردم به چنین سلاح‌هایی آسان نبود ولی در حال حاضر فناوری‌های حوزه سایبر هیچ جای امنی را در جهان باقی نگذاشته است.

٤-٥-٤- تقویت قوانین مسئولیت بین‌المللی

در بحث مسئولیت بین‌المللی دولت‌ها در حوزه سایبر باید گفت برای اینکه بتوان امنیت بین‌المللی در این حوزه را تقویت نمود باید توجه بیشتری به مسئولیت بین‌المللی کشورهای مبدا حملات سایبری صورت گیرد. در حال حاضر کشورهایی که حملاتی از داخل آنها علیه دولت‌های دیگر انجام می‌گیرد به راحتی نقش خودشان را در ارتکاب حملات سایبری انکار می‌نمایند. نمونه های متعددی از حملات سایبری از داخل کشورهایی مانند روسیه و چین انجام می‌گیرد اما این دولت‌ها از ارتکاب چنین حملاتی از داخل کشورهایشان اظهار بی اطلاعی می‌نمایند و گاها ارتکاب این حملات را به عناصری مانند هکر ها و سازمان‌های غیر دولتی منتسب می‌نمایند. «از بدو ورود فضای سایبر به زندگی بشر موضوع قانونگذاری و شناخت قانونگذار صالح در این فضا از اهمیت زیادی برخوردار بوده است. با جهان شمولی اینترنت و نگرانی دولت‌ها از تاثیر پذیری حاکمیت آنها قانونگذاری در این فضا از اهمیت زیادی در مناسبات بین‌المللی بر خوردار شد» (ضیایی و شکیب‌نژاد، ۱۳۹۶: ۲۲۸)؛(Ziaei &Shakib Nejad, 2017: 228). «جهانی شدن پدیده ای فراگیر است که هر روز بیش از گذشته مرزها را در می نوردد و به تمامی عرصه‌های زندگی جهانیان ارتباط می یابد. حقوق نیز یکی از عرصه‌هایی است که هم از این فرایند تاثیر پذیرفته و هم بر آن تاثیر گذاشته است»(جلالی و توسلی‌اردکانی، ۱۳۹۸: ۱۳۶۷)؛(Jalali and Tavasoli, 2019: 1367). اگر قرار است در آینده دارای جهانی با ثبات امنیتی بالا در حوزه سایبری باشیم، برای فرار از مسئولیت دولت‌ها باید جلوی چنین بهانه هایی گرفته شود و تاکید بر مسئولیت دولت‌هایی شود که حملات سایبری از داخل قلمرو هدایت می‌گردد. با توجه به پیشرفت های دانش بشری در حوزه

کامپیوتر و فناوری‌های مرتبط با اینترنت ردیابی حملات سایبری تا حدی ممکن است اما اگر دولت‌ها به نحوی متعهد گردند که در صورت ارتکاب حملات سایبری از قلمرو آنها مسئولیت صد درصدی برای آنها وجود داشته باشد چنین دولت‌هایی با تصویب قوانین سختگیرانه باعث می‌شوند که اشخاص و عناصر غیر دولتی این ترس را داشته باشند که در صورت ارتکاب حملات سایبری امکان پیگیری و مجازات آنها وجود دارد چنین اشخاص و عناصری دیگر تا حد امکان از انجام حملات سایبری امتناع می‌نمایند. بنابراین لازم است دولت‌ها معیار مراقبت بایسته[1] در قبال حملات سایبری را در یک معاهده بین‌المللی بگنجانند. این معیار به معنای هوشیاری لازم در انجام تعهد حقوقی می‌باشد و بر اساس این معیار هیچ کشوری حق ندارد از سرزمین خود به گونه ای استفاده کند یا اجازه استفاده دهد که آثار ناشی از آن موجب ایراد آسیب به سرزمین، اموال یا اشخاص دولت دیگر گردد. اگر چنین اتفاقی بیفتد و مبنای مسئولیت بر مبنای معیار مراقبت بایسته دولت‌های مبدا حملات سایبری لحاظ گردد در این حالت هم ازحجم و تعداد حملات سایبری در سطح جهانی کاسته می‌شود و هم امنیت سایبری بین‌المللی تقویت می گردد.

نتیجه‌گیری

اختراع کامپیوتر و اینترنت باعث به هم تنیدگی جامعه بین‌المللی گردیده وموجب سرعت انتقال اطلاعات در سطح جهان شده ولی به دلیل اینکه تمام سطوح تمدن و حیات بشری را به خود وابسته نموده، مضرات و خطراتی را نیز برای صلح و امنیت بین‌المللی به همراه داشته است. فضای سایبری محیط امن و کم هزینه ای را برای مجرمان سایبری فراهم نموده به نحوی که همه روزه شاهد حملات سایبری و سایر سوءاستفاده‌ها از ظرفیت‌های این فضا در جهان می‌باشیم. حملاتی مانند ویروس استاکس‌نت و سایر حملات سایبری برجسته نشان می‌دهد که اگر در سطح بین‌المللی اقداماتی برای کنترل فضای سایبری انجام نگیرد این فضا چقدر می‌تواند خطراتی را برای کشورهای جهان در پی داشته باشد. تنها چاره ای که برای جلوگیری از مضرات و خطرات فضای سایبری وجود دارد همکاری کشورها در سطح بین‌المللی است. تا کنون همکاری‌های دولت‌ها برای مواجهه با حملات سایبری دارای بعد منطقه‌ای بوده و بنابراین نتوانسته برای کل جامعه بین‌المللی مؤثر باشد. حملات سایبری معضلی جهانیست بنابراین نیاز است تا برای مواجهه با آن راه حلی جهانی اندیشیده شود. راهبردی که دولت‌ها می‌توانند برای معضل حملات سایبری داشته باشند این است که در سطح بین‌المللی همکاری های خودشان را در این حوزه افزایش دهند و با تدوین یک معاهده جامع و کامل بین‌المللی در باره حملات سایبری کنترل این حوزه خطرناک را بدست بگیرند. همچنین در بحث مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری باید « معیار مراقبت بایسته » در چنین

[1]. Due Diligence Standard

معاهده ای گنجانده شود زیرا در غیر اینصورت راههای زیادی برای فرار از مسئولیت دولت‌ها وجود خواهد داشت.

منابع فارسی

۱. برقعی، س. (۱۳۹۳). مروری بر امنیت سایبری درسهایی برای جمهوری اسلامی ایران. *فصلنامه مطالعات انقلاب اسلامی*، ۱۱ (۳۸)، ۱۰۴-۸۵

۲. جلالی، م، توسلی اردکانی، س. (۱۳۹۸). ضرورت ایجاد نظام هماهنگ حقوقی بین‌المللی در مقابله با جرائم در فضای مجازی. *فصلنامه مطالعات حقوق عمومی*، ۴۹(۴)، ۱۳۷۲-۱۳۵۱.

۳. خلیلی پور رکن‌آبادی، ع.، نورعلی‌وند، ی. (۱۳۹۱). تهدیدات سایبری و تاثیر آن بر امنیت ملی. *فصلنامه مطالعات راهبردی*، ۱۵(۵۶)، ۱۹۶-۱۶۷.

۴. داوند، م.، سلطانی نژاد، ا. (۱۳۹۷). *امنیتی‌سازی تنش سایبری جمهوری اسلامی ایران و عربستان سعودی تهدیدها و الزامات راهبردی*. *فصلنامه راهبرد*، ۲۷(۱)، ۷۱-۹۸.

۵. رضایی، م.، بابازاده مقدم، ح. (۱۳۹۳). اصول تدوین قوانین و مقررات برای اینترنت با تاکید بر مصوبات یونسکو و شورای اروپا. *فصلنامه پژوهش حقوق عمومی‌دانشگاه علامه طباطبایی*، ۱۵(۴۲)، ۸۲-۴۳.

۶. سلطانی‌نژاد، ا.، جمشیدی،م.، محسنی، س. (۱۳۹۵). تحول مفهوم امنیت در پرتو جهانی شدن و فناوری اطلاعات و ارتباطات نوین. *فصلنامه سیاست جهانی*، ۵(۲)، ۴۲-۷.

۷. شهبازی، آ.، آقاجانی‌رونقی، آ. (۱۳۹۹). جاسوسی سایبری در حقوق بین‌الملل: مسئلهٔ انتساب مسئولیت بین‌المللی به دولت در هاله‌ای از ابهام. *فصلنامه مطالعات حقوق عمومی‌دانشگاه تهران*، ۵۰ (۴)، ۱۴۸۷-۱۵۰۳. DOI:10.22059/jplsq.2020.274302.1912

۸. ضیایی، س، شکیب نژاد،ا. (۱۳۹۶). قانونگذاری در فضای سایبر:رویکرد حقوق بین‌الملل و حقوق ایران. *مجله حقوقی بین‌المللی*، ۳۴(۵۷)، ۲۴۹-۲۲۷.

۹. فقیهی، م.، جلالی‌فراهانی، ا .(۱۳۹۷). مروری بر معاهده های فراملی سایبری.معاونت پژوهش‌های زیر بنایی و امور تولیدی، تهران: دفتر مطالعات ارتباطات و فناوری‌های نوین.

۱۰. قاسمی، غ، نامدار،س.(۱۳۹۷). بررسی مفهوم دفاع مشروع در پرتو حملات سایبری (با تأکید بر حمله استاکس‌نت به تأسیسات هسته‌ای ایران). *فصلنامه مطالعات حقوقی دانشگاه شیراز*، ۱۰(۱)، ۱۹۹-۲۳۵. DOI: 10.22099/jls.2018.23191.2178

۱۱. کتانچی، ا.، پورقهرمانی، ب. (۱۴۰۰). چالش‌های امنیت سایبری در کشورهای آ.سه.آن. *فصلنامه مطالعات بین‌المللی*، ۱۸(۱)، ۱۳۹-۱۵۶. DOI: 10.22034/isj.2021.252695.1237

English References

1. Borrell, J. (2020). Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic,30 April 2020, https://eucyberdirect.eu
2. Dunn Cavelty, M. (2012). The Militarisation of Cyber Security as a Source of Global Tension ,.*Center for Security Studies*, 103-124
3. Harjinder, L., Lynsay, S, Jason, N., Arnau, E., Gregory, E., Carsten, M., Xavier B. (2020). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic, Department of Electronic and Electrical Engineering, University of Strathclyd, 1-20
4. Li, Y., Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *EnergyReports*, 7, 8176–8186, DOI: https://doi.org/10.1016/j.egyr.2021.08.126
5. Lucas, G. (2017). Ethics of cyber warfare. The quest for responsible security in the age of digital warfare, Oxford,Oxford University Press.
6. Mukherjee, S. (2019). Implementing Cybersecurity in the Energy Sector , University of the Cumberlands (formerly Cumberland College), 1-18
7. Eilstrup-Sangiovanni, M. Why the World Needs an International Cyberwar Convention. Philos. Technol. 31, 379–407 (2018). https://doi.org/10.1007/s13347-017-0271-5
8. Snider, K., Ryan, S., Shay, Z., Daphna, C. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, 7 (1), 1-11
9. Tsakanyan, V. T. (2017). The role of Cybersecurity in World Politics. *Vestnik RUDN. International Relations*, 17(2), 339-348. Doi:10.22363/2313-0660-2017-17-2-339-348
10. Vasileiou, K. G. (2019). Cyber Security in the Energy Sector a Holistic Approach, University of Piraeus, Department of International & European Studies.
11. Voo , J., Hemani, I., Jones, S., Desombre, W., Cassidy, D., Schwarzenbach, A (2020).National Power Cyber Index 2020 Methodology and Analytical Consideration, Harvard Kennedi School Belfer center for Science and International Affairs.

Translated References to English

1. Borqe'I, S. (2014). A Review on Cyberspace Security: Lessons for Islamic Republic of

Iran. *Journal of Islamic Revolution Studies*, 11 (38), 85-104 **(In Persian)**

2. Borrell, J. (2020). Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic,30 April 2020, https://eucyberdirect.eu
3. Davand, M., Soltani Nejad, A. (2018). Securitization of the Islamic Republic of Iran and Saudi Arabia Cyber-Tensions; Threats and Strategic Requirements , *Strategy Quarterly*,27 (1), 71-98, DOI: 20.1001.1.1.0283102.1397.27.1.4.8 **(In Persian)**
4. Dunn Cavelty, M. (2012). The Militarisation of Cyber Security as a Source of Global Tension ,.*Center for Security Studies*, 103-124
5. Eilstrup-Sangiovanni, M. Why the World Needs an International Cyberwar Convention. Philos. Technol. 31, 379–407 (2018). https://doi.org/10.1007/s13347-017-0271-5
6. Faghihi, M., Jalali Farahani, A.H. (2018). Review of Transnational Cyber Agreements, Deputy Minister of Infrastructure Research and Production, Office of Communication Studies and New Technologies, 1-23 **(In Persian)**
7. Ghasemi, G.A., Namdar, S. (2018). Analyzing of the Concept of Self-defense in Light of Cyber Aattack (With an emphasis on Stuxnet attack on Iran's nuclear facilities) , *Journal of Legal Studies*, 10 (1), 199-235, DOI: 10.22099/jls.2018.23191.2178 **(In Persian)**
8. Harjinder, L., Lynsay, S, Jason, N., Arnau, E., Gregory, E., Carsten, M., Xavier B. (2020). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic, Department of Electronic and Electrical Engineering, University of Strathclyd, 1-20
9. Jalali, M ,Tavassoli Ardakani, S. (2019). Necessity of Establishment of an International Harmonized Legal System against Crimes in Cyberspace, Public Law Studies Quarterly, 49(4), 1351-1372, DOI: 10.22059/jplsq.2019.208109.1271 **(In Persian)**
10. Katanchi, E., Pour-Qahramani, B. (2021). Cyber Security Challenges in ASEAN Countries, *International Studies Journal* ,18(1) , 139-156, DOI: 10.22034/isj.2021.252695.1237 **(In Persian)**
11. Khalilipour Rokanabadi, A. ,Nooralivand, Y. (2012). Cyber Threats and Its Impact on National Security, *Strategic Studies Quarterly*,15(56), 167- 196 **(In Persian)**
12. Li, Y., Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *EnergyReports*, 7, 8176–8186,

DOI: https://doi.org/10.1016/j.egyr.2021.08.126

13. Lucas, G. (2017). Ethics of cyber warfare. The quest for responsible security in the age of digital warfare, Oxford,Oxford University Press.
14. Mukherjee, S. (2019). Implementing Cybersecurity in the Energy Sector , University of the Cumberlands (formerly Cumberland College), 1-18
15. Rezaei, M., Babazadeh Moghadam, H. (2014). Principles of Codification for the Laws and Regulations of the Internet with the Emphasis on UNESCO and European Council Documents , *The Quarterly Journal of Public Law Research*, 15(42) , 43-82 **(In Persian)**
16. Shahbazi, A., Aghajani Ronaghi, A. (2021). Cyber Espionage in International Law: Attribution of International Responsibility to States in a State of Uncertainty, *Quarterly Journal of Public Law Studies*, 50 (4) , 1487-1503, DOI: 10.22059/jplsq.2020.274302.1912 **(In Persian)**
17. Snider, K., Ryan, S., Shay, Z., Daphna, C. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, 7 (1), 1-11
18. Soltaninejad, A., Jamshidi, M., Mohseni, S. (2016). The Evolution of Security Concept in the Light of Globalization and New Information and Communication Technologies, *World Politics*, 5(2), 7-42 **(In Persian)**
19. Tsakanyan, V. T. (2017). The role of Cybersecurity in World Politics. *Vestnik RUDN. International Relations*, 17(2), 339-348. Doi:10.22363/2313-0660-2017-17-2-339-348
20. Vasileiou, K. G. (2019). Cyber Security in the Energy Sector a Holistic Approach, University of Piraeus, Department of International & European Studies.
21. Voo , J., Hemani, I., Jones, S., Desombre, W., Cassidy, D., Schwarzenbach, A (2020).National Power Cyber Index 2020 Methodology and Analytical Consideration, Harvard Kennedi School Belfer Center for Science and International Affairs.
22. Ziaei, S.Y., Shakibnejad, E. (2018). Legislation in Cyberspace from the Prospect of International Law and the Iranian Law, *International Law Journal*, 34(57), 227-249, DOI:10.22066/cilamag.2017.27971 **(In Persian)**