فصلنامهٔ پدافند غیرعامل و امنیت (پژوهشی)
سال دهم: شمارهٔ ٤٠- پاییز ١٤٠١
صص: ٢٧ - ٥٨

Quarterly of Passive Defense & Security
Vol.10, No.40,Autumn 2022
P-P: 27 - 58

تاریخ دریافت: ١٤٠٢/٠٥/١٥
تاریخ پذیرش:١٤٠٢/٠٩/١٤

طرح راهبردی دفاع حقوقی در مقابله با تهدیدهای سایبری

اردشیر رئیسی دهکردی[١]

چکیده

امروز عرصه فضای سایبری پنجمین عرصه نبرد، پس از زمین، دریا، هوا و فضا بین‌کشورهاست؛ به‌گونه‌ای که فراوانی حملات صورت‌گرفته علیه‌کشورها در این فضا در سطح جهان در مقام مقایسه با سایر عرصه‌ها به‌شدت رو به افزایش است؛ به‌ویژه علیه‌کشورهای مستقل و سلطه ستیز، مانند جمهوری اسلامی ایران‌که در طی سال‌های اخیر شاهد مواجه با حملات مکرر در این فضا بوده است. گستردگی حملات سایبری منجر به اقدامات ٣٢ کشور جهان در خصوص طراحی برنامه دفاع سایبری در مقابله با تهدیدهای فضای سایبر شده است و ١٤٠ کشور نیز در حال مطالعه در حوزه دفاع ملی (سایبری) هستند که قطعاً این امر برای جمهوری اسلامی ایران‌که همواره مورد دشمنی نظام سلطه واقع گردیده است از اهمیت بیشتری برخوردار است؛ ازاین‌رو در این مقاله با توجه به‌گسترهٔ ابعاد دفاع در حوزه سایبر با پرداختن به بعد دفاع حقوقی با مبنا قراردادن این سؤال‌که طرح راهبردی دفاع حقوقی در مقابله با تهدیدهای سایبری‌کشور چیست؟ از روش تحلیلی -توصیفی و با استفاده از روش‌های‌کمی و کیفی برای جمع‌آوری اطلاعات از نخبگان در حوزه سایبری و روش اکتشافی در مراجعه به اسناد و مدارک بهره‌برداری گردید و سپس به تجزیه‌وتحلیل اطلاعات‌کسب‌شده پرداخته شد‌که نتایج حاصل از این تحقیق طرح راهبردی دفاع حقوقی با عنایت به اصول و ارزش‌ها، چالش‌ها، قوت‌ها، فرصت‌ها، ضعف‌ها، تهدیدها و راهبردها مشخص‌گردید و تدوین قوانین، حداکثر استفاده از قوانین، نهادینه‌سازی فرهنگی، طراحی و ساماندهی، سازمان‌دهی و تقسیم‌کار، طراحی و پیاده‌سازی، برشمردن جرائم، راه‌اندازی سامانه جمع‌آوری ادله، طراحی پیمان دفاعی به‌عنوان راهبردهای دفاع حقوقی معین‌گردید.

واژگان کلیدی: دفاع، دفاع حقوقی، تهدید، تهدیدهای سایبری

---

١. عضو هیئت‌علمی دانشگاه haniye.1282@gmail.com

جستارگشایی

در روند جابجای قدرت در قرن بیست‌ویکم، رسانه‌ها را می‌توان سرچشمه جدید قدرت دانست. در این میان، اینترنت و فضای سایبری به سبب سرعت، دقت، قابلیت حجم عظیم انتقال پیام و گستردگی وسیع مخاطبان جز ابزار ارتباطی پرجاذبه و تعیین‌کننده در جنگ نرم راهبردی به شمار می‌رود (قدیمی و دیگران، ۱۳۹۳: ۶۸). فضای مجازی روزبه‌روز ابعاد جدیدتری می‌یابد، به‌نحوی‌که می‌توان گفت زندگی افراد در این فضا نیز استمرار دارد و علاوه بر اینکه به نیازی مهم برای فرد و جامعه بدل شده امکان کنشگری را نیز به کاربران این فضا داده است پس زندگی علاوه بر اینکه در دنیای واقعی جریان دارد، در فضای مجازی نیز استمرار دارد وهم قواعد و رفتارهای که در دنیای واقعی انتظار می‌رود، در فضای مجازی نیز امکان ظهور و بروز دارد پس می‌توان گفت امروز با گسترش فنّاوری‌ها و فراگیرشدن شبکه‌های اجتماعی جدید که باعث ارتباطات زیادی بین افراد می‌شود ضرورت تدوین قواعد حاکم بر زیست در این فضا بیشتر محسوس است (نعناکار، خلخالی، ۱۳۹۷: ۴). ازآنجاکه لزوم حیات هر پدیده‌ای، چه اجتماعی و چه ارتباطی، نتیجتاً تدوین مقرراتی را ایجاب می‌کند تا چگونگی استفاده منطقی و حقوقی از آن مشخص گردد، فضای سایبری نیز از این قاعده کلی مستثنا نبوده است؛ بخصوص اینکه فضای سایبری بعد از هوا، دریا، زمین و فضا به‌عنوان پنجمین قلمرو کشورها محسوب می‌گردد. همان‌طوری که چهار قلمرو دیگر تابع مقررات و قوانین بین‌المللی هستند، این قلمرو نیز نباید از این امر مستثنا گردد؛ فضای سایبری به‌طور نمادین، دنیای جدیدی است که باید از طریق قانون‌گذاری مستقل، مانند دنیای واقعی آن را به نظم مطلوب درآورد، نظمی که در پرتو سازکارهای قانونی و حقوقی فراگیر در عرصه ملی و بین‌المللی زمینه تهدیدات و حملات را در فضای مجازی کاهش داده و امکان دفاع و مقابله با تهدیدات داخلی و خارجی را فراهم نماید. پیچیدگی و توسعه روزافزون فنّاوری‌های سایبری باعث به وجود آمدن فضای حمله آسان و دفاع سخت شده است (عصاریان نژاد،۱۳۹۴)؛ اما علی‌رغم این نیاز تاکنون در عرصه بین‌الملل نظام حقوقی همانند سایر نظام‌های حقوقی، نظیر معاهدات تجارت، دریاها و ... در قالب کنوانسیون‌های بین‌المللی که ناظر بر کنترل فضای سایبری از حیث جلوگیری از تهاجمات سایبری کشورها علیه یکدیگر باشد، تدوین نشده است؛ اگرچه در راستای مقابله با جرائم رایانه‌ای کوشش‌هایی صورت گرفته است که منتج به شکل‌گیری کنوانسیون‌ها و معاهدات منطقه‌ای و بین‌المللی شده است؛ ولی معطوف و محصور به جرائم سایبری گردیده است؛ ولی با توجه به اینکه تهدیدها در فضای سایبری از یک ظرفیت جهانی بودن، شبکه‌ای بودن، دسترسی مبتنی بر زمان و کار مجازی برخوردار است قانون‌گذاری و طراحی و اجرای یک نظام دفاع حقوقی جامع و هماهنگ که متضمن کنترل و تأمین امنیت و صلح در فضای سایبری باشد؛ به‌ویژه در قبال تهدیدات و حملات خارجی (دشمن و گروه‌های وابسته به دشمن). به منافع حساس، مهم و حیاتی از اهمیت خاصی برخوردار است.

امروزه بهره‌گیری از ابزار حقوقی برای دفاع در مقابله با تهدیدهای سایبری از موضوعاتی است که در صحنه بین‌الملل که سایبر در آن گسترده شده، موردتوجه کشورها قرار گرفته است. گسترش جرائم رایانه‌ای و تهدیدها در فضای سایبری در دنیا، خصوصاً در کشورهایی که بیشترین استفاده‌کنندگان رایانه و اینترنت در دنیا محسوب می‌شوند، باعث شد تا حکومت‌ها به فکر ایجاد سازوکار قانونی و حقوقی رسیدگی و مبارزه با این‌گونه جرائم و تهدیدها بیافتند. کنوانسیون‌های بین‌المللی نیز برای تشریک‌مساعی در روند شناسایی جرم و مجرمان، همکاری در پی‌جویی و تعقیب قضایی و پلیسی مجرمان و تبادل دانش و اطلاعات پلیسی در شناخت و کشف علمی جرائم سایبری نیز در این راستا شکل گرفته‌اند که از مهم‌ترین آن‌ها می‌توان به کنوانسیون بوداپست در سال ۲۰۰۱ اشاره کرد. پیشگیری از تجاوز و تجاوز مجدد در فضای سایبری از طریق احقاق حقوق قانونی یا استفاده از قوانین، ظرفیت‌ها و قابلیت‌های حقوق بین‌المللی برای دفاع از منافع ملی در برابر تهدیدات و حملات خارجی ازجمله ظرفیت‌های مطلوبی است که می‌باید در طراحی دفاعی به آن توجه بایسته صورت گیرد. دفاع مبتنی بر به‌کارگیری ظرفیت‌های حقوقی موجود (قوانین، مقررات، معاهدات، موافقت‌نامه‌ها، پیمان‌ها و پروتکل‌ها). در عرصه ملی و بین‌المللی در برای کاهش آسیب‌پذیری‌های بالقوه در مقابل حملات سایبری و کمک به بازدارندگی مهاجمان بالقوه و همچنین فراهم کردن شرایط بهره‌گیری امن و متعادل از فضای سایبری برای کشور است. بر همین اساس در این تحقیق با مبنا قراردادن این سؤال که طرح راهبردی دفاع حقوقی کشور در برابر تهدیدهای سایبری چیست؟ و اصول و ارزش‌های حاکم، چالش‌های اساسی، ضعف‌ها، قوت‌ها، فرصت‌ها، تهدیدها و راهبردها در حوزه دفاع حقوقی در فضای سایبری چیست؟ درصدد رسیدن به سطحی از دفاع حقوقی در مقابله با تهدیدها سایبری با ارائه راهبردهای مطلوب در جهت تأمین منافع و امنیت ملی است.

در بحث اهمیت و ضرورت پژوهش با توجه به توسعهٔ روزافزون زیرساخت‌های فنّاوری اطلاعات و ارتباطات در کشور و افزایش کاربران و استفاده‌کنندگان از اینترنت و سایر فنّاوری‌های اطلاعاتی، ارتباطی و مخابراتی نظیر خطوط تلفن‌های ثابت و همراه، شبکه‌های دیتای کشوری و محلی، ارتباطات ماهواره‌ای و توسعهٔ خدمات الکترونیک نظیر دولت الکترونیک، بانکداری الکترونیک، تجارت الکترونیک، آموزش الکترونیک و سایر خدمات ازاین‌دست، اهمیت پرداختن به راهکارهای افزایش ضریب امنیت و مقابله با تهدیدهای رخداده در این فضا و ارتقا توانمندی در پیگیری رخدادها و تهاجم سایبری علیه کشور در مجامع بین‌المللی را آشکار می‌کند. از سوی دیگر، عدم توجه به این مهم باعث افول توانمندی در پیگیری رخدادهای تهاجم‌گونه سایبری علیه کشور در مجامع بین‌المللی و غافلگیری در قبال مسائل حقوقی مرتبط با پیامدهای حملات سایبری می‌گردد رشد قارچ‌گونهٔ جرائم و تهدیدها در حوزهٔ فضای تولید و تبادل اطلاعات کشور (فتا). مثل تروریسم شبکه‌ای، کلاه‌برداری‌های اینترنتی، جعل داده‌ها و عناوین، سرقت اطلاعات، تجاوز به

حریم خصوصی اشخاص و گروه‌ها، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، هرزه‌نگاری و جرائم اخلاقی و برخی جرائم سازمان‌یافتهٔ اقتصادی، اجتماعی و فرهنگی و حمله‌های سایبری توسط دولت‌ها که این عرصه را به میدان نبردی بین کشورها تبدیل کرده است نبردهای که 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 دامنهٔ خسارات وارده در مراحل اولیه شروع حمله، موردتوجه کشورهای متخاصم؛ به‌ویژه در جنگ‌های پنهان قرار گرفته است

این پژوهش با الهام‌گیری از نظریه دفاع همه‌جانبه امام خامنه‌ای (مدظله‌العالی) به‌عنوان چارچوب نظری پژوهش دنبال شده است و برای تبیین موضوع موردمطالعه به دلیل ماهیتی که دارد نوع تحقیق از نوع کاربردی –توسعه‌ای است و روش تحقیق مورداستفاده روش توصیفی – تحلیلی است.

داده‌های مربوطه در این پژوهش از دو روش گرداوری اطلاعات، کتابخانه‌ای و بررسی اسنادی و روش میدانی (مصاحبه با نخبگان) جمع‌آوری شده است و در تحلیل داده‌ها از شاخص‌های مرکزی که مهم‌ترین آن میانگین است و همچنین با بهره‌گیری از نرم‌افزار Excel و SPSS مورد تجزیه‌وتحلیل قرار گرفته است.

مروری اجمالی بر پیشینه ادبیات موضوع

با توجه به پیشینه و جست‌وجوی صورت‌گرفته در سایت‌ها و بانک‌های معتبر تاکنون پژوهشی با این عنوان انجام نشده است؛ ولی درخصوص فضای سایبر از جنبه‌های گوناگون دیگری؛ به‌ویژه تهدیدها و فرصت‌های فرارو، رساله، پایان‌نامه، مقاله و کتب متعددی منتشر شده است که به یک نمونه از آنان اشاره می‌گردد.

طرح تحقیقی با عنوان نظام جامع فنّاوری اطلاعات کشور توسط جمعی از محققان انجام که نتیجه این تحقیق منجر به ارائه و تصویب سند «نظام جامع فنّاوری اطلاعات کشور» شده و طی آن ۷ حوزه راهبردی تدوین و به بررسی قلمروهای اساسی پرداخته است. این حوزه‌ها عبارتند از: «جامعه و شهروندان»،«توسعه منابع انسانی باکیفیت»،«دولت و شیوهٔ مدیریت عمومی و ارائه خدمات و سرویس‌های موردنیاز و به‌روز در جامعه»، «تحقیق و پژوهش و نوآوری فنّاوری»، «توسعه صنعت فنّاوری اطلاعات»، «کسب‌وکارهای مبتنی بر فنّاوری اطلاعات» و «چگونگی تعامل محیط ملی و فراملی با شبکه‌های جهانی اینترنت، کشورها، بنگاه‌ها و بازارها.»

۱- مبانی نظری و مفاهیم

۱-۱- مفاهیم:

۱-۱-۱-فضای سایبر

فضای سایبر درواقع نامی است که تعداد زیادی از کاربردهای امروز فنّاوری‌های جدید ارتباطی را

دربرمی‌گیرد این نام را نخستین بار ویلیام گیبسون در رمان نورومانسر (۱۹۸٤) ابداع کرد او تعبیر فضای سایبر را برای توصیف یک دنیای جدید مجازی به‌کاربرد (هاشمی زاده، انصاری نسب، ۱۳۹۶: ۱۵). دنیل کوئل فضای سایبر را به‌عنوان دامنه عملیاتی تعریف می‌کند که با مجموعه‌ای از کاربری‌های الکترونیک و طیف الکترومغناطیسی برای ایجاد، ذخیره‌سازی، اصلاح، تبادل و کاربرد اطلاعات از طریق سامانه‌های مرتبط به هم و سامانه‌های اطلاعاتی درهم‌تنیده و تأسیسات زیربنایی مرتبط با آن‌ها شکل گرفته است (کرامر و دیگران،۲۰۱۵: ۲۳). فضای سایبری برای توصیف تمام انواع منابع اطلاعاتی ایجادشده از طریق شبکه‌های رایانه‌ای به‌کاربرده می‌شود. تعاریف متعددی برای فضای سایبر وجود دارد اما عموماً «سایبر» پیشوندی است که معنای فعالیت‌های مرتبط با کامپیوتر و الکترونیک را می‌رساند. بر اساس یکی از تعاریف، «فضای سایبر یک حوزهٔ عملیاتی است که به‌منظور بهره‌برداری از اطلاعات از طریق سامانه‌های به‌هم‌پیوسته و زیرساخت یکپارچهٔ آن‌ها، با استفاده از علم الکترونیک شکل گرفته است (*WWW.hccmr.com/news*).

۱-۱-۲-جامعهٔ شبکه‌ای

جامعهٔ شبکه‌ای را می‌توان شکلی از جامعه تعریف کرد که به‌گونه‌ای فزاینده روابط خود را در شبکه‌های رسانه‌ای سامان می‌دهد، شبکه‌هایی که به‌تدریج جایگزین شبکه‌های اجتماعی رودررو می‌شوند یا آن‌ها را تکمیل می‌کنند. مانوئل کاستلز شبکه را مجموعه‌ای از نقاط اتصال یا گره‌های به‌هم‌پیوسته تعریف می‌کند به عبارتی شبکه مجموعه‌ای از اتصالات میان اجزاء یک واحد است (هاشمی زاده، انصاری نسب، ۱۳۹۶: ۴۵).

۱-۱-۳-دفاع حقوقی در فضای سایبری

هنر به‌کارگیری ظرفیت‌های حقوقی موجود (قوانین، مقررات، معاهدات، موافقت‌نامه‌ها، پیمان‌ها و پروتکل‌ها) در عرصه ملی و بین‌المللی در جهت مقابله با تهدیدات خارجی سایبری و جرائم سایبری و همچنین ساماندهی پیمان‌های منطقه‌ای وجهانی جدید ناظر بر فراهم‌کردن شرایط بهره‌گیری امن و متعادل از فضای سایبری برای همه کشورها است، دفاع جزئی از هویت یک ملت زنده است ملتی از آسیب محفوظ می‌ماند که ثابت کند آماده دفاع است (بیانات امام خامنه‌ای،۱۳۸۹/۳/۱۴).

۱-۲-چارچوب نظری

در این تحقیق برای ارائه طرح راهبردی دفاع حقوقی در مقابله با تهدیدهای سایبری بر اساس نظریه دفاع همه‌جانبه حضرت امام خامنه‌ای (مدظله‌العالی) سامان یافته است که می‌فرمایند: ازآنجاکه فعالیت نظام سلطه تنها در بعد سیاسی نیست؛ بلکه توانسته است منطق فرهنگی خاص خود و شبکه اقتصادی و تبلیغاتی وابسته به خود را نیز به وجود آورد، دفاع در مقابل آن نیز باید همه‌جانبه باشد (بیانات،۱۳۹۱/۳/۱۴). دفاع همه‌جانبه را می‌توان کاربست تمامی ظرفیت‌ها و مقدورات موجود برای مواجهه با تهدیدهای فراوان علیه جمهوری اسلامی ایران دانست. چنین ظرفیتی اجازه می‌دهد از زوایای گوناگون به این مفهوم نگاه و اندیشه شود. یکی از ابعاد آن دفاع حقوقی در مقابله با تهدیدهای سایبری است که در این

خصوص جمهوری اسلامی ایران در طول حیات خود با طیف کاملی از تهدیدها روبه‌رو شده است

۱-۲-۱-تهدید در حوزه فضای سایبری

با توجه به ابعاد مختلف و کاربرد فضای سایبر در حوزه‌های عمومی و نظامی، تهدیدها در این فضا نیز متنوع و گوناگون است (ابوالحسنی،۱۳۹۲: ۱۰۳). تهدیدهای امنیتی در فضای سایبری به دودسته کلی تقسیم می‌شوند: تهدیدات عادی که با انگیزه معمولی انجام می‌پذیرد و می‌توان آن‌ها را در زمره جرائم عادی در فضای سایبری و شبکه اینترنت قرارداد، مانند سرقت، جعل، کلاه‌برداری و قاچاق که این‌گونه تهدیدات و ناامنی‌ها به‌عنوان چالش‌های حاکمیتی در فضای سایبری محسوب می‌گردند. دسته دوم تهدیدهای امنیتی است که با انگیزه‌های غیرمعمولی انجام می‌شود و ممکن است تمامی عرصه‌های سیاسی، اقتصادی، اجتماعی، فرهنگی، علمی، نظامی و غیره را در برگیرد و شامل مواردی نظیر جاسوسی، تخریب اطلاعات و تروریسم و تهاجم است (حافظنیا،۱۳۹۰: ۲۵۵). این دودسته تهدید را می‌توان از زاویهٔ دیگر بر اساس منشأ تهدید به چهار نوع تهدید دسته‌بندی نمود. اولین تهدید، تهدیدهای خارجی هستند. این تهدید از ناحیه کسانی است که به یک کشور خارجی وابسته‌اند، از قبیل بخش‌های نظامی و آژانس‌های امنیتی و حتی شرکت‌هایی که وابستگی زیادی به آن دولت دارند طراحی و اجرا می‌شود. تهدید دوم، تروریست‌ها و گروه‌های افراطی هستند. این افراد ممکن است به دولت خاصی وابستگی نداشته باشند؛ ولی در راستای اهداف خود به خرابکاری مبادرت ورزند. تهدید سوم شامل جنایتکاران و سازمان‌های جنایی است. این گروه نه‌تنها جرائم سازمان‌یافته بزرگ را در فضای سایبری مرتکب می‌شوند؛ بلکه به‌صورت انفرادی نیز اقدام می‌کنند. ویژگی خاص فضای سایبر باعث شده که یک فرد به‌تنهایی بتواند جرائم بزرگی را مرتکب شود و تهدید چهارم نیز کاربران داخل سازمان‌ها و نیروهای خودی هستند (حسن‌بیگی، ۱۳۸۸: ۱۰۲). تهدید نوع اول و دوم عمدتاً ماهیت نظامی و دفاعی دارند؛ زیرا امنیت ملی و زیرساخت‌های کشور رقیب و دشمن را مورد هدف قرار می‌دهند و تهاجم به آن‌ها از هر طریقی ازجمله هکرها یا ویروس‌ها و غیره می‌تواند نقطه آغاز یک کشمکش، منازعه و جنگ در فضای سایبری باشد به‌طوری‌که طرفین با حداکثر قوا و با استفاده از سازکارها، سربازان و رزمندگان مجازی سعی می‌کنند تأسیسات، سرمایه‌ها و نهادهای کشور دشمن در فضای سایبری و شبکه اینترنت را مورد هدف قرار دهند و تخریب کنند. تهدیدات نوع سوم عمدتاً اجتماعی و جزو جرائم رایانه‌ای و اینترنتی محسوب می‌شود که در حوزه کار پلیس مجازی قرارمی‌گیرد. تهدیدات نوع چهارم نیز ماهیت امنیتی و جاسوسی دارد که در حوزه کار دستگاه‌های اطلاعاتی و پلیس قرارمی‌گیرد (حافظنیا، ۱۳۹۰: ۲۸۷). با توجه به تقسیم‌بندی صورت‌گرفته تهدید خارجی در فضای سایبری مستقیماً متوجه امنیت ملی کشورها هستند و در حوزه دفاعی -امنیتی قراردارند.

۱-۲-۲-تهدید خارجی در فضای سایبری

اگرچه هر چهار دسته تهدید مطرح‌شده، به‌واسطه ناامن‌سازی فضای سایبری دارای اهمیت است؛ ولی با

توجه به اینکه حوزه تهدید خارجی سایبری معطوف به زیرساخت‌ها و ارزش‌های حیاتی مرتبط با امنیت ملی و منافع ملی کشورهاست از اهمیت ویژهٔ برخوردار است و در حوزه دفاعی تعریف می‌شود. به‌طور سنتی تهدید خارجی اصلی‌ترین تهدید برای امنیت ملی محسوب می‌گردند. به علت آن‌که پایداری فیزیکی کشور و استقلال آن در مقابله با تهدید خارجی نسبت به تهدید داخلی آسیب‌پذیرتر است، تهدید خارجی همچنان به‌عنوان منبع اصلی تهدید امنیت ملی، اهمیت خود را حفظ کرده‌اند. تهدید خارجی طیف گسترده سیاسی، نظامی، اقتصادی، فرهنگی و سایبری را در خود جای می‌دهد (مرادیان،۱۳۸۸: ۱۹۳). تهدید خارجی به تهدیداتی با عامل خارجی که قابلیت وارد نمودن ضربات فاجعه‌بار به امنیت ملی، اقتصاد ملی، وجهه کشور در سطح بین‌المللی، روابط سیاسی و اقتصادی کشور، سلامت. ایمنی عمومی، اطمینان عمومی، باورهای دینی یا ملی یا اداره امور کشور از طریق تخریب یا ایجاد اخلال گسترده در عملکرد زیرساخت‌های حیاتی و حساس نیز تعریف شده است (حافظنیا، ۱۳۹۰: ۲۸۶).

۱-۲-۳-انواع تهدید خارجی در فضای سایبری

فضای سایبری در امتداد فضای واقعی، علی‌رغم ماهیتی فرصت‌ساز، ماهیتی تهدیدزا نیز دارد. تهدیداتی که عمدتاً از ناحیه رقبا و دشمنان یک کشور (گروه‌ها، سازمان‌ها و کشورها) ایجاد می‌گردند. هر سطحی از فضای سایبر، تأسیسات فیزیکی، نرم‌افزار عملیاتی، اطلاعات و مردم- مستعد شکست امنیتی است، خواه از طریق حمله، نفوذ یا تصادم که توسط دشمنان طراحی و اجرا می‌گردد که در سه دسته می‌توان آنان را قرارداد:

۱-۲-۳-۱ تهدیدهای نظامی، امنیتی :تهدیداتی که متوجه زیرساخت‌های اساسی و حیاتی یک کشور ازجمله تأسیسات مخابرات، انرژی، شبکه بانکی و پولی، آب و خدمات فوریتی نهادهای حکومتی و دولتی و نهادهای حیاتی اقتصادی و سرمایه‌ها و نهاده‌های یک کشور می‌گردد.

۱-۲-۳-۲-تهدیدات سیاسی: تهدیداتی که موجودیت، ایدئولوژی، ارکان و کارکردهای حکومت را به‌منظور سرنگونی و یا کنترل قدرت سیاسی موردتوجه قرارمی‌دهد.

۱-۲-۳-۳-تهدیدات اجتماعی و فرهنگی: تبلیغ گسترده فرهنگ مغایر با یک کشور در سطح بین‌الملل، زیر سؤال بردن ارزش‌های و فرهنگ یک کشور در سطح بین‌المللی، رسوخ و انتقال فرهنگ بیگانه در جامعه هدف (کشور موردتهاجم).

۱-۲-۴-ویژگی تهدیدات خارجی در فضای سایبری

خودکارسازی زیرساخت‌های ملی (هوشمندسازی) از طریق فنّاوری اطلاعات و اتصال روزافزون شبکه‌های رایانه‌ای به شبکه جهانی، تهدیدات ناشی از سوی کشورها و سازمان‌های خارجی به فضای سایبری را افزایش داده و توسعه این تهدیدات، خود بخشی از تلاش‌های گسترده برای اثرگذاری بر امنیت ملی کشورها در عصر اطلاعات است (حسن‌بیگی، ۱۳۸۸: ۱۰۲). تهدیداتی که تمایزات اساسی با تهدیدات سنتی که تا

به امروز جوامع با آن روبه‌رو بوده‌اند دارد که به بخشی از این ویژگی‌ها پرداخته می‌شود:

الف) غیر سرزمینی بودن: برخی تهدیدات نظیر تروریسم، بیماری‌های مسری، حملات سایبری در دنیای پس از جنگ سرد فراسرزمینی‌اند و در کوتاه‌ترین زمان ممکن می‌تواند از کشوری به کشور دیگر منتقل شوند و وجود مرزهای دولتی مانعی در برابر انتقال تهدیدات نیست.

ب) غیرقابل مدیریت: این تهدیدها را نمی‌توان تنها با اتکا به سیاست‌های دفاعی سنتی مدیریت کرد. سازمان‌های نظامی، دفاعی امکان دارد به‌ویژه در کشمکش‌های خشونت‌آمیز نقش داشته باشند؛ ولی باید در نظر داشت که مدیریت مؤثر، مستلزم طیفی از رهیافت‌های غیرنظامی است (همان: ۹۸).

ج) نامشخص بودن: در شرایط حاضر دولت‌ها و ملت‌ها با زنجیره‌ای از تهدیدهای نامشخص در محیط‌های مجازی مواجهند که امنیت آن‌ها را به چالش کشیده و ابزارهای سنتی تأمین امنیت ملی نیز توان مقابله با آن‌ها را ندارد. اکنون مرزهای بین حوزه‌های داخلی و خارجی، عمومی و خصوصی و نیروهای نظامی و انتظامی و اطلاعاتی در هم ادغام‌شده و ماهیت و ملزومات امنیت ملی نیز به‌سرعت در حال تغییر هستند (همان: ۲۸۸).

د) عدم انتساب: یکی از ویژگی‌های حملات و تهدیدات سایبری عدم امکان انتساب حمله به حمله‌کنندگان است، به‌واسطه نامشخص بودن منشأ تهدید یا حمله فرایند انتساب دچار چالش می‌گردد.

۱-۲-۵-تهدیدات خارجی و جنگ سایبری

کارشناسان فنّاوری اطلاعات عقیده دارند در جنگ‌های آینده، گروه‌های کوچک نظامی که با استفاده از آخرین تجهیزات اطلاعاتی و ارتباطی در جنگ‌ها شرکت می‌کنند، می‌توانند ارتش‌های تادندان‌مسلح به سلاح‌های جنگی را از پای درآورند. عرصه و میدان جنگ در آینده نزدیک دیگر محصور در زمین و هوا و دریا نخواهد بود؛ بلکه عرصه اصلی کارزار و درگیری، فضای سایبر و جنگ سایبری خواهد شد. همان‌طوری که در تعریف جنگ سایبری بیان‌شده است، جنگ سایبری یعنی ایجاد اختلال، در سامانه‌های اطلاعاتی و ارتباطی که دشمن برای دانستن خود به آن‌ها تکیه می‌کند (خوش عمل، ۱۳۹۱: ۳۸). درنتیجه برخورد مستقیم و فیزیکی میان دوسوی یک مبارزه خشونت‌آمیز را به برخورد غیرمستقیم تبدیل کرده‌اند با توسعه فزاینده فنّاوری اطلاعات و ارتباطات در عصر جهانی‌شدن و پیدایش و توسعه فضای سایبر، مرزهای سیاسی و بین‌المللی کارکرد گذشته خود را تااندازه‌ای ازدست‌داده‌اند. از این پدیده جغرافیایی سیاسی، دیگر نمی‌توان انتظار کنترل کالا، انسان، اندیشه و حفظ استقلال کامل دولت – ملت‌ها را داشت (خوش عمل، ۱۳۹۱: ۴۶). هدف جنگ سایبری نه تخریب انبوه؛ بلکه ازهم‌گسیختگی و غیرعملیاتی کردن قوای دشمن است و اگرچه در واقعیت مجازی روی‌می‌دهد؛ اما آثار خود را روی جهان واقع می‌گذارد.

۱-۲-۶-ظرفیت‌های دفاع حقوقی در فضای سایبری

تنها راه ممکن برای داشتن یک ساختار مؤثر دفاع سایبری بازگشت به تفکر رایج، یعنی همیشه در حال دفاع بودن است که به‌وسیله یک ساختار سازمانی همراهی شود تا بتواند واکنش سریع و اثربخشی لازم را برای دفاع علیه تهاجماتی که بدون اعلام قبلی رخ می‌دهند فراهم کند، چون دفاع سایبری چیزی نیست جز بهره‌گیری از کلیه امکانات سایبری و غیر سایبری کشور به‌منظور ایجاد بازدارندگی، پیشگیری، پیش‌دستی، ممانعت از انجام، تشخیص به‌موقع، کنترل ابعاد، مقابله مؤثر و بازدارنده با هرگونه تجاوز سایبری به زیرساخت‌های حیاتی، حساس یا مهم کشور، توسط متخاصمین سایبری، اعم از نیروی نظامی (ارتش سایبری) کشورهای متخاصم و گروه‌های تحت حمایت پنهان دولت‌های متخاصم و مدیریت صحنه نبرد از طریق رسیدگی فوری و مؤثر با منشأ و پیامدهای ناشی از تجاوز سایبری، انجام اقدامات قانونی، تلافی‌جویانه و تنبیهی علیه متجاوز و منشأ تجاوز سایبری است که با مبنا قراردادن این تعریف می‌توان سه رویکرد اصلی در دفاع سایبری را برشمرد که عبارتند از:

مقابله دفاعی: دفع تهدید از طریق انجام اقدامات صرفاً دفاعی یا بازدارندگی از طریق قدرت دفاعی

مقابله تهاجمی: پیش‌گیری از تجاوز از طریق منع و ترساندن، ایجاد ترس از طریق انتشار دکترین تهاجمی، نمایش قدرت سایبری یا عملیات سایبری غیرجنگی

مقابله قانونی: پیشگیری از تجاوز و تجاوز مجدد از طریق احقاق حقوق قانونی یا استفاده از قوانین، ظرفیت‌ها و قابلیت‌های حقوق بین‌المللی برای دفاع از منافع ملی در برابر تهدیدات و حملات خارجی سایبری است؛ که در بعد مقابله قانونی یا دفاع حقوقی با توجه به طبیعت خاص فضای سایبری و شباهت آن با فضای واقعی و امکان گسترش تهدید در این فضا حکومت‌ها و نهادهای بین‌المللی را وادار کرده است تا برای مقابله و دفاع در برابر حملات و منازعات سایبری به سمت بهره‌گیری از ظرفیت‌های حقوقی داخلی و بین‌المللی حرکت نمایند. درواقع در مقام تمثیل می‌توان فضای سایبری را به فضای خارج از جو و اتمسفر تشبیه کرد که ملک همگان است و ملک هیچ‌کس نیست، فضای سایبری به‌طور نمادین، دنیای جدیدی است که باید از طریق قانون‌گذاری مستقل، مانند دنیای واقعی آن را به نظم مطلوب درآورد، نظمی که در پرتو سازکارهای قانونی و حقوقی فراگیر در عرصه ملی و بین‌المللی زمینه تهدیدات و حملات را در فضای مجازی کاهش داده و امکان دفاع و مقابله با تهدیدات داخلی و خارجی را فراهم نماید، درنتیجه می‌توان گفت که فضای سایبری تنها محدود به خود نیست؛ بلکه در فضای واقعی با نام جامعه جهانی قرار دارد که در آن علاوه بر پیروی از قواعد خاص خود می‌بایست از قواعد مربوط به جامعه بین‌المللی، یعنی از قواعد حقوق بین‌الملل عام نیز پیروی کند. حقوق بین‌الملل عام، واجد اصول متعددی است که دسته‌ای از آن‌ها مربوط به وضعیت کشورها به‌صورت منفرد و دسته دیگر نیز بر وضعیت جامعه بین‌المللی (حداقل

گروهی از کشورها) اشراف دارد و دارای ظرفیت حقوقی در راستای بهره‌گیری در دفاع حقوقی هستند اگرچه در حقوق بین‌الملل، طبقه‌بندی خاصی که مورد شناسایی و توافق عمومی باشد تحت عناوین حقوق سایبر و یا حقوق اطلاعات به چشم نمی‌خورد (آرایی، ۳۰: ۱۳۹۰). علت نبود یک بنیان خاص در حقوق سایبری شناسایی نشدن اصول مربوط به این حوزه است؛ که در ذیل به بخشی از اصول و قوانین حقوق بین‌الملل با ظرفیت بهره‌گیری در راستای به نظم آوردن فضای سایبر اشاره می‌گردد.

۱-۲-۶-۱-اصل استقلال کشورها

استقلال کشورها، یکی از اولین اصول حقوق بین‌الملل است که در جامعه بین‌المللی بر آن تأکید فراوانی می‌شود. این اصل یکی از مهم‌ترین اصول حقوق بین‌الملل عام است که بنیان حاکمیت کشورها بر آن استوار است. قبل از دهه‌های اخیر، اگر صحبت از تعرض به حاکمیت و استقلال کشورها به میان می‌آمد، اولین چیزی که به ذهن خطور می‌کرد تجاوزهای نظامی و اقداماتی ازاین‌دست بود، اما از دهه‌های اخیر، بعد از ظهور فنّاوری ارتباطات و شکل‌گیری فضای سایبری دیگر نمی‌توان تعرض را محدود به مورد فیزیکی نمود؛ چراکه این امر مصادیق متعددی در فضای سایبر یافته است و اتفاقاً تنش‌های بسیاری را در سطح بین‌المللی، میان قدرت‌های جوامع پدید آورده است. از همین روی توضیح این اصل و بررسی نسبت آن با حقوق و تکالیف در فضای سایبری ضروری به نظر می‌رسد (آرایی، ۱۳۹۰: ۱۶۳). استقلال کشورها، به معنای مختار بودن دولت‌ها در اداره امور خود، بدون مداخله (اعم از داخلی و خارجی) دیگران است، به عبارت ساده‌تر می‌توان گفت معنای استقلال کشورها در حقوق بین‌الملل، مستقل بودن نظام سیاسی یک کشور از سایر حاکمیت‌ها و کشورها است و رعایت این امر در جامعه بین‌المللی هم، به معنای عدم‌مداخله کشورها در امور داخلی یکدیگر و احترام به اراده حاکمیت برآمده از سازواره‌های موجود در هر کشور، از سوی سایر کشورهاست؛ حال ممکن است احترام به حاکمیت دولت‌ها، به نسبت موضوعات مختلف، صور گوناگونی بیابد که البته در عرصه فضای سایبری مصادیق خاص خود را دارا است (آرایی، ۱۳۹۰: ۱۶۳). شکی نیست که بر اساس منطق حقوقی، استقلال کشورها در فضای سایبر، در مقایسه با ابعاد این اصل در جهان فیزیکی، صورتی متفاوت به خود می‌گیرد از همین رو تنها به ذکر مصادیقی می‌پردازیم که در فضای سایبر ناقض اصل استقلال کشورها است.

۱-۲-۶-۲-اصل حاکمیت دولت بر قلمرو خود:

یکی از اصول مهم حقوق بین‌الملل که توجه زیادی را؛ به‌ویژه پس از جنگ جهانی اول، به خود معطوف داشته و مباحث فراوانی پیرامون آن صورت گرفته است، اصل حاکمیت دولت‌ها است.

دراین‌ارتباط، عده‌ای ریشه اصل حاکمیت دولت‌ها را ناشی از اصولی چون استقلال، عدم‌مداخله کشورها در امور یکدیگر ونیز اصل تساوی مطلق دولت‌ها می‌دانند. در معنای این اصل اظهارشده که حاکمیت یعنی قدرت اداره کشور در داخل که متضمن اصل استقلال بوده و استقلال نیز خود به معنی عدم نفوذ

قدرت خارجی و دخالت در امور داخلی یک کشور است.

اصل حاکمیت در منشور سازمان ملل متحد به دو صورت بیان گردیده است. بند ۲ از ماده اول منشور، ازجمله اهداف سازمان ملل را توسعه روابط دوستانه در میان ملت‌ها بر اساس احترام به اصل حقوق مساوی و خودمختاری مردم می‌داند. همچنین در بند ۱ از ماده ۲ ازجمله اصولی که سازمان و اعضای آن باید بر آن اساس منظورهای مطروحه در ماده یک را پیگیری کنند، اصل تساوی حاکمیت تمام اعضای آن است. درهرصورت مفهوم حاکمیت اصل دیگری را نیز در بردارد که عبارت از عدم‌مداخله کشورها در امور یکدیگر است. گرچه این اصل به لحاظ نظری پذیرفته‌شده؛ لیکن در عمل کمتر به آن توجه گردیده است و دولت‌های قوی به‌انحاءمختلف در امور دیگر کشورها دخالت کرده و حاکمیت آنان را نقض کرده‌اند که این امر با توجه به بستر جهانی ایجادشده در قالب اینترنت و فضای سایبری امروزه ابعاد گستردهٔ به خود گرفته است و زمینه مداخلات سیاسی، فرهنگی و اجتماعی و نظامی را فراهم کرده است. این در حالی است که ماده ۲ از بند ٤ منشور سازمان ملل متحد به‌صراحت دولت‌ها را از هرگونه تهدید و به‌کارگیری زور علیه قلمرو دیگر کشورها بر حذر داشته است (کدخدایی،۱۳۷۹: ۳۸)

۱-۲-۶-۳-اصل عدم‌مداخله:

یکی از اصول حقوق بین‌الملل که در ادبیات سیاسی کاربرد زیادی دارد، اصل عدم‌مداخله در امور داخلی دولت‌ها است. اصل عدم‌مداخله که یکی از اصول بنیادین ملل متحد و ازجمله حقوق و تکالیف بنیادین دولت‌ها است، یکی از اصول اساسی جامعه بین‌المللی بوده که ریشه در اصل تساوی حاکمیت دولت‌ها دارد. این اصل که مبنای آن را باید در حقوق بین‌الملل عرفی جست‌وجو کرد، در برخی از اسناد بین‌المللی نیز انعکاس یافته است. ازجمله در بند هفت ماده دو منشور ملل متحد عدم‌مداخله سازمان ملل متحد در امور داخلی دولت‌ها پیش‌بینی‌شده و در اعلامیه‌های ۲۱۳۱ سال ۱۹٦٥ و ۲٦۲٥ سال ۱۹۷۰ مصوب مجمع عمومی سازمان ملل، عدم‌مداخله دولت‌ها در امور داخلی دولت‌های دیگر مقررشده است. علاوه بر این، اصل عدم‌مداخله در ماده ۱٥ منشور بوگوتا، ماده ۸ پیمان ورشو، اصل ششم سند نهایی هلسینکی و ماده ۲۷ کنوانسیون اروپایی راجع به حل مسالمت‌آمیز اختلافات قید شده است؛ بنابراین، اصل مذکور در سطوح جهانی و منطقه‌ای مورد تأیید و تأکید دولت‌ها و سازمان‌های بین‌المللی است. عموم حقوق‌دانان عقیده دارند که مداخله به معنای عملی است که دولت یا سازمانی نسبت به دولتی به عمل می‌آورد تا آن دولت در امور داخلی یا خارجی خود رفتار معینی را پیشه کند. این عمل ممکن است با زور همراه باشد (موثق، ۱۳۹۰: ۱). باوجود جایگاه اصل عدم‌مداخله در حقوق بین‌الملل، امروزه شاهد آن هستیم که فضای سایبری در کنار فرصت‌هایی که برای بشریت فراهم کرده است سطح مداخله در دیگر کشورها را در حوزه سیاسی، فرهنگی، اجتماعی و اقتصادی افزایش داده است. کشورها در روابط بین‌المللی خود، خواستار عدم‌مداخله در امور داخلی خود بوده و ازاین‌جهت، فعالیتی که می‌تواند منجر به

جنگ، شورش و یا هر اقدام دیگری شود و در تضاد با منافع ملی آن‌ها قرار دارد محکوم می‌کنند (آرایی، ۱۶۸: ۱۳۹۰). عموم حقوق‌دانان مداخله را به‌طورکلی ناقض حقوق بین‌الملل واصل حاکمیت دولت‌ها می‌دانند. در همین حال عده‌ای که قائل به تنوع در مداخله هستند، آن را به مداخلات نظامی، سیاسی و تبلیغاتی تقسیم کرده‌اند، ولی تماماً آن را ناقض اصل حاکمیت دانسته‌اند. مداخلات بر اساس نوع ابزار اعمال آن‌ها، تقسیم‌بندی‌های گوناگونی را به خود گرفته است؛ لیکن تقسیم‌بندی آن به نظامی، سیاسی، اقتصادی و تبلیغی می‌تواند سایر موارد را نیز تحت پوشش قرار دهد (کدخدایی،۱۳۷۹: ۳۸)در مقررات بین‌المللی، مانند منشور سازمان ملل و قطعنامه‌های آن ونیز در پرونده‌های مطروحه در مراجع قضائی بین‌المللی، هرگونه مداخله در امور کشورها ممنوع شده که می‌توان موارد بسیاری را در این رابطه عنوان کرد. ماده ۲ از بند ٤ منشور سازمان ملل متحد دولت‌ها را از هرگونه تهدید و به‌کارگیری زور علیه قلمرو دیگر کشورها بر حذر داشته است و همچنین در اعلامیه ۱۹٦٥ در مورد غیرقابل‌قبول بودن دخالت در امور داخلی دولت‌ها اشاره‌شده است: «هیچ دولتی حق مداخله مستقیم و غیرمستقیم را به هر دلیل که باشد در امور داخلی یا خارجی دیگر دولت‌ها ندارد لذا هرگونه دخالت اعم از نظامی یا سایر اشکال آن و یا تهدید علیه شخصیت دولت و یا عناصر سیاسی، اقتصادی و فرهنگی آن محکوم است.» اکنون این سؤال مطرح می‌گردد که با توجه به شمول امور فرهنگی سیاسی در دامنه ممنوعیت‌ها؛ آیا تهدیدات خارجی در فضای سایبری که از ماهیت نظامی، امنیتی، فرهنگی، اجتماعی و اقتصادی توسط یک کشور علیه کشور دیگر صورت می‌گیرد، طبق مقررات بین‌المللی و حقوق بین‌المللی عرفی آیا مصداق نقض اصل مداخله نیست؟ به‌طور خلاصه می‌توان گفت انواع تهدیدات خارجی در فضای سایبری می‌تواند در اعمال حاکمیت دولت‌ها مؤثر واقع گردد و سبب اخلال و یا نقض حاکمیت دولت‌ها شده و ازلحاظ عرف و حقوق بین‌الملل محکوم است.

۱-۲-۶-۴-اصل تساوی کشورها:

یکی دیگر از اصول مهم حقوق بین‌الملل عام که در منشور ملل متحد نیز به‌کرات مورداستفاده قرار گرفته است، اصل تساوی حاکمیت‌ها در عرصه بین‌المللی است. جامعه بین‌المللی، فضایی است که بازیگران اصلی آن کشورها هستند. بر اساس رویه جاری در جامعه بین‌المللی، می‌توان ادعا کرد که منظور از اصل تساوی حاکمیت کشورها، تساوی در همه‌چیز، به‌جز در آن چیزهایی مطرح است که قواعد بین‌المللی مستثنا نموده است (آرایی،۱۳۹۰: ۱۷۶). اصل تساوی کشورها در نسبت با فضای سایبری وجوه خاصی می‌یابد که یکی از وجوه آن توسعه ارتباطات است. در جامعه جهانی، کشورها ممکن است به صورت‌های متفاوتی باهم در ارتباط باشند. یکی از مهم‌ترین صور ارتباط میان ملت‌ها و کشورها، ارتباطی است که در آن اطلاعات موضوعیت دارد. ازآنجایی که اصل تساوی کشورها جز در عرصه ارتباطات بروز پیدا

نمی‌کند، در ارتباطی که در آن اطلاعات موضوعیت دارد نیز بحث تساوی کشورها مطرح می‌شود بر همین اساس از عمده‌ترین وظایف دولت‌ها در فضایی که اصول حقوق بین‌الملل عام حاکم است، احترام به‌تساوی حاکمیت‌ها بوده تا با بهره‌گیری از فضای سایبر به این مهم دست یابند (آرایی، ۱۳۹۰: ۱۷۸). بر اساس آموزه‌های حقوق بین‌الملل عمومی در خصوص اصل تساوی حاکمیت کشورها، رفتارهایی که به هر صورت متضمن قسمی از تبعیض است محکوم بوده نباید صورت پذیرد. این رفتارها ممکن است در صور متفاوتی از برقراری ارتباط متجلی گردد که نمونه‌هایی از آن عبارتند از: استفاده از وسایل ارتباطات ماهواره‌ای، دسترسی به شبکه‌های رایانه‌ای و فضای سایبری، دسترسی به ابزارهای ارتباطات زمینی نظیر تلفن، تلویزیون، رادیو و... به‌طورکلی می‌توان گفت کشورها در فضای سایبر نباید به صورتی فعالیت کنند که اصل برابری حاکمیت را زیر پا بگذارند.

۱-۲-۶-۵-طرح میثاق جرائم علیه صلح و امنیت بشری

چارلز راین در کتاب حقوق بین‌الملل خود درباره مفهوم تهاجم چنین می‌نویسد: توضیح مفهوم تهاجم برای آنکه دفاع معنی داشته باشد لازم است، چون دفاع یکی از موارد اعمال قدرت است؛ ولی کوشش‌هایی که برای تعریف تهاجم بکار رفته، به نظر واحدی دست نیافته است. پاره‌ای از کشورها ازجمله شوروی سابق پیشنهادی دراین‌باره برای تصویب به سازمان ملل متحد داده است. در این پیشنهاد، تهاجم، پاره‌ای از اعمال عاری از زور راگرفته تا اعمال مستقیم زور را شامل می‌شود. پاره‌ای دیگر بر این عقیده‌اند که تهاجم نباید فقط تهاجم مسلح را در برگیرد؛ بلکه باید مفهوم آن به‌اندازه‌ای موسع باشد که پاره‌ای از اعمال تهاجمی که آن‌ها را اعمالی مضر به استقلال و آزادی کشور تعریف کرده‌اند شامل شود. طرح میثاق جرائم علیه صلح و امنیت بشری، اعمال تهاجمی غیرمسلحانه را چنین برمی‌شمارد: دخالت در امور سیاسی کشور دیگر، اقدام به اعمالی به‌منظور ایجاد جنگ داخلی در کشور دیگر و توطئه برای ارتکاب این اعمال که آن توطئه هم مخالف حقوق بین‌المللی و قابل مجازات است که با توجه به اثرات تهاجمات سایبری در امور سیاسی و داخلی کشورها می‌توان آنان را نمونه از تهاجم‌هایی که نقض میثاق جرائم علیه صلح و امنیت بشری قلمداد کرد (حسینی نژاد،۱۳۸۳: ۱۱۰)

۱-۲-۶-۶-مسئولیت بین‌المللی

مسئولیت بین‌المللی یکی از مهم‌ترین و اساسی‌ترین نهادهای حقوقی بین‌المللی است؛ زیرا اصولاً هرگونه تعهد حقوقی بین‌المللی که از سوی تابعان حقوق بین‌الملل نادیده انگاشته و نقض شود، بلافاصله موضوع مسئولیت بین‌المللی آن‌ها پیش می‌آید. اهمیت و جایگاه مسئولیت در جامعه بین‌الملل به‌مراتب بیش از جامعه داخلی است؛ چراکه جامعه بین‌الملل محیطی است که کشورها بر اساس حاکمیتشان آزادانه تصمیم می‌گیرند و این امر به‌طریق‌اولی به آزادی برابر با سایر کشورها برخورد پیدا می‌کند. مسئولیت بین‌المللی

به‌عنوان سازوکار قانونمند، اساسی و ضروری روابط متقابل کشورهاست. حقوق مسئولیت بین‌المللی در اساس شکل عرفی دارد (ضیایی بیگدلی،۱۳۸۲: ۴۰۷)؛ به‌بیان‌دیگر، تنها کافی است که عمل ارتکابی برخلاف مقررات و تعهدات بین‌المللی باشد تا مسئولیت محرز گردد و دیگر لزومی به تحقیق در مورد تقصیر یا عدم تقصیر مرتکب نیست؛ یعنی به‌محض اینکه بین فعالیت‌ها و اعمال یک کشور یا یک سازمان بین‌المللی و عمل خلاف حقوق بین‌الملل رابطه سببیت برقرار گردید، مسئولیت بین‌المللی ایجاد شده است حقوق‌دانان برای تحقق مسئولیت دولت‌ها در قبال عمل یا ترک عمل درصحنه‌های بین‌المللی وجود سه شرط را ضروری می‌دانند: اول آنکه یک تعهد حقوقی بین‌المللی و قابل‌اجرا میان طرفین وجود داشته باشد و دوم وقوع عمل یا ترک آن که موجب نقض آن تعهد می‌گردد، قابل استناد به دولت مربوطه باشد و سوم خسارات یا ضررهایی به دولت طرف مقابل وارد شده باشد (ضیائی بیگدلی، ۱۳۸۲: ۴۱۱). صرف‌نظر از تفاسیر متفاوتی که در تبیین مسئولیت دولت‌ها و اقسام مختلف آن به‌عمل‌آمده، معمولاً اختلاف‌نظر پیرامون نوع خسارت، مادی و غیرمادی بودن، الزامی بودن ایراد خسارت برای تحقق مسئولیت، عدم دخالت دولت زیان‌دیده در خسارت وارده و غیره ازجمله مواردی است که هنوز در عرصه‌های حقوق بین‌الملل قابل‌بحث و بررسی است. بر همین اساس تهدیدات و حملات سایبری یک کشور علیه کشوری دیگر را به‌واسطه ایراد ضرر اعم از مادی و غیرمادی که متوجه زیرساخت‌های آن کشور می‌نماید مشمول این اصل دانست و با استناد به قطعنامه‌هایی که از سوی مجمع عمومی سازمان ملل به تصویب رسیده؛ می‌توان آنان را مسئول دانست و ملزم نمود تا خسارت وارده را به نحو مقتضی جبران نمایند.

۱-۲-۶-۷-اعمال حقوقی یک‌جانبه

حقوق‌دان فرانسوی پی یر ولا، اعمال یک‌جانبه را به‌قرار زیر تعریف می کند، عمل یک‌جانبه به یک عمل حقوقی که وضعیت حقوقی جدیدی را ایجاد کرده و به سایر تابعین حقوق بین‌الملل قابل‌اعمال است اطلاق می‌شود. عمل یک‌جانبه یک منبع حقوق بین‌الملل به شمار می‌آید. اعمال یک‌جانبه سندیت دارند و در داوری‌ها و محاکم قضایی می‌توان به آن استناد کرد (موسی زاده، ۱۳۹۱: ۲۱۹). شارول روسو حقوق‌دان فرانسوی اعمال حقوقی یک‌جانبه را به پنج دسته زیر طبقه‌بندی می کند: اعمال در حکم شرط، اعمال موجد تکالیف، اعمال مؤید حقوق، اعمال مبتنی بر طرد حقوق، اعمال یک‌جانبه ضمنی که یکی از مواردی که در زمره اعمال در حکم شرط است اعلان است. اعلان که در ابتدا و به‌موجب رویه قضایی بین‌المللی صرفاً برای تصرف و اشغال سرزمین به کار می‌رفت، امروزه توسعه‌یافته و شامل موارد متعددی می‌شود. درواقع اعلان عملی است که به‌موجب آن رسماً یک رویداد، یک وضعیت و یا سندی به اطلاع کشور ثالث می‌رسد. این عمل دارای آثار حقوقی برای کشور دریافت کننده اعلان است. البته، اعلان می‌تواند قانونی و یا غیرقانونی باشد که در صورت اخیر کشور طرف اعلان می‌تواند نسبت به آن اعتراض کند (همان: ۲۱۹)

۱-۲-۶-۸-عدم توسل به‌زور

یکی دیگر از اصولی که در حقوق بین‌الملل عام از اهمیت بسیاری برخوردار بوده و از جنگ جهانی دوم به بعد بسیار مورد تأکید قرار گرفته اصل عدم توسل به‌زور در روابط بین‌الملل است این اصل برخلاف آنچه در ظاهر به نظر می‌رسد، تنها در عالم فیزیکی مصداقی نداشته و مصادیقی در فضای مجازی دارد. در روابط بین‌المللی مابین کشورها، منطق حکم می‌کند که حسن رفتار و حسن نیت رعایت شود و از توسل به روش‌های نامشروع و خشونت‌آمیز خودداری گردد. به‌طورکلی در عرصه حقوق بین‌الملل عام دو واژه وجود دارد که به اقدامات قهرآمیز مربوط می‌شوند که عبارتند از زور و اجبار، واژه زور در معنی خاص خود عبارت است از توسل به نیروی نظامی و واژه اجبار نیز واژه‌ای است که به معنی هر نوع اقدام متکی بر اعمال فشار است که منجر به تغییر تصمیم اشخاص شود که البته در یک تفسیر موسع، شامل زور نیز می‌شود (آرایی، ۱۳۹۰: ۱۸۸). طبیعی است که اعمال زور، به آن معنی که مشمول اقدامات نظامی شود در فضای مجازی سالبه به انتفاع موضوع است؛ ولی می‌توان صوری از اجبار و زور را تصور نمود (موج‌های تبلیغاتی با بهره‌گیری از بستر فضای مجازی علیه یک کشور) که نه شبیه به اعمال زور هستند و نه کاملاً بی‌شباهت با آن اصطلاحاً به چنین رفتاری در جامعه بین‌المللی، عنوان اعمال زور کمتر از جنگ اطلاق می‌شود.

اگر رفتاری از نوع منتسب به اعمال زور کمتر از جنگ به‌عنوان کنشی از سوی یکی از تابعان حقوق بین‌الملل موردنظر باشد، قطعاً می‌توان ضوابط مربوط به مخاصمات مصلحانه را بر آن تسری داد. چنانچه فشار به کشوری باعث شود حاکمیت آن تحت‌تأثیر قرار گیرد، قطعاً آن عمل ازلحاظ حقوق بین‌الملل، غیر مشروع تلقی می‌شود.

۱-۲-٦-۹-دفاع مشروع

دفاع مشروع اصلی پذیرفته در تمامی نظام‌های حقوقی است. هرچند در مورد منشأ پیدایش این حق اختلافات زیادی وجود دارد؛ ولی شرایط آن با اختلاف جزئی در تمامی نظام‌های حقوقی یکسان است. امروزه یکی از مباحثی که در بین حقوق‌دانان جایگاهی پیدا نموده است امکان استناد کشورها به این اصل در مواجه با تهدیدات و حملات در فضای مجازی است.

امروزه گستره فضای سایبری و فنّاوری رایانه تا جایی پیش رفته است که در آن کشورها توانایی واردکردن جراحت، کشتن و ایجاد خسارت‌های فیزیکی از طریق فضای مجازی را علیه دیگر کشورها دارند. دامنه نبرد سایبری می‌تواند از خشونت‌های شبکه‌ای بی‌ضرر تا حملات شدید به ساختارهای زیربنایی ملی در نوسان باشد. درحالی که از کار انداختن موقت سایت‌های اینترنتی یک دولت شاید آسیب چندانی به آن دولت وارد نکند، تهدید ارائهٔ اطلاعات نادرست به فرماندهان نظامی در صحنهٔ جنگ‌های فیزیکی، یا یک هجمه سنگین به شبکه‌های الکتریکی، آب‌رسانی، ارتباطی و ترافیکی یک دولت می‌تواند خطراتی جدی برای

سربازان و شهروندان دولت یادشده به بار آورد. نفوذ به شبکه‌های اطلاعاتی دولت‌ها و دست‌اندازی به اطلاعات طبقه‌بندی شدهٔ آن‌ها که در اصطلاح با عنوان «جاسوسی کامپیوتری خوانده می‌شود نیز بخشی از گسترهٔ نبرد سایبری به شمار می‌رود. این اعمال امروزه به دلیل وابستگی روزافزون آژانس‌های دولتی به ارتباطات الکترونیکی به‌مراتب ساده‌تر گردیده است.

علیرغم مرگ‌آوری بالقوه نبرد سایبری، این شکل از جنگ در حال حاضر در محیطی قانونی (فضای مجازی) در حال رخ‌دادن است. سناریوهای بسیار مخرب، مانند امکان استفاده از تکنیک‌های نبرد سایبری در جنگ‌های نامتقارن. باعث افزایش احساس نیاز به یک استاندارد واضح و قابل‌درک برای رفتار در جنگ‌های سایبری گردیده است که از جانب همه شناسایی و مورداحترام واقع شود. این موضوع که آیا استفاده از جنگ‌های سایبری می‌تواند نوعی توسل به‌زور به‌حساب آید تا باعث ایجاد حق دفاع از خود گردد یا خیر، تبدیل به یک سؤال مهم در حقوق بین‌الملل گردیده است.

حقوق مدرن در زمینهٔ توسل به‌زور بر اساس بند ٤ ماده ٢ منشور ملل متحد شکل گرفته است. البته در منشور ملل متحد تعریف دقیقی ازآنچه توسل به‌زور به شمار می‌آید، ارائه نشده است. نه منشور و نه هیچ‌یک از دیگر ارکان بین‌المللی این اصطلاح را به‌طور دقیق تعریف ننموده‌اند. تلاش‌ها برای تعریف کردن نبرد سایبری بر اساس مفهوم بند ٤ ماده ٢ منشور بیشتر باعث دست‌وپاگیر شدن برداشت‌های سنتی از توسل به‌زور گردیده است. آنالیز این موضوع که آیا نبرد سایبری در حقوق جنگ. بخشی از حقوق بین‌الملل که بر توسل به‌زور به‌عنوان ابزار سیاست داخلی حاکم است. قابل‌پذیرش و بررسی هست یا خیر در منابعی مانند ممنوعیت مطروحه در منشور ملل متحد (بند ۴ ماده ۲) در مورد استعمال زور، شمای کلی امنیتی فصل هفتم این منشور، حق ذاتی دفاع از خود که در ماده ۵۱ به آن اشاره‌شده و حقوق بین‌الملل عرفی که توسط رفتار مستمر دولت‌ها ایجادشده است قابل‌جست‌وجو است.

اگرچه بخش قابل‌توجهی از حقوق بین‌الملل به توسل به‌زور توسط دولت‌ها اختصاص دارد، قابلیت اعمال این بخش به فضای مجازی در هاله‌ای ابهام قرار دارد و سؤالات بسیاری حول این مسئله قرار دارد که حقوق بین‌الملل دقیقاً چگونه با نبرد سایبری ارتباط پیدا می‌کند.

۱-۲-۶-۱۰-جنایت بین‌المللی:

جرم بین‌الملل دولت موضوع تازه‌ای است که در طرح مواد راجع به مسئولیت بین‌المللی کشورها مصوب ۱۹۹۶ کمیسیون حقوق بین‌الملل تحت عنوان جنایت بین‌المللی پیش‌بینی‌شده است. در طرح مذکور، نقض شدید و فاحش برخی از تعهدات بین‌المللی جنایت بین‌المللی تلقی شده‌اند. معذلک ازآنجاکه طرح یادشده تاکنون به‌صورت معاهده درنیامده است؛ بنابراین مسئولیت بین‌المللی جدید دولت‌ها ناشی از ارتکاب جنایت بین‌المللی از نوع کیفری نیست، زیرا مسئولیت کیفری بین‌المللی در حقوق بین‌الملل جزای

موجود هنوز محدود به افراد است، لیکن محاکمه و مجازات کارگزار یا نماینده یک دولت در رابطه با جنایت بین‌المللی ارتکابی که درنهایت قابل انتساب به دولت باشد، چنین دولتی را از پرداخت یا ترمیم خسارات یا اعاده وضع به حالت عادی مبری نمی‌کند و مسئولیت مدنی بین‌المللی دولت متخلف نه‌فقط در قبال دولت متضرر یا منجی علیه، در مقابل کلیه دولت‌های عضو جامعه بین‌المللی به قوت خود باقی است. طبق رویه عمومی کشورها و مقررات عرفی و معاهدات بین‌المللی، جرائم بین‌المللی را می‌توان با توجه به نوع آن‌ها در سه‌طبقه قرارداد: جنایات علیه صلح، جنایات جنگی و جنایات علیه بشریت. جنایت علیه صلح، عبارت است از نقض عمده و فاحش هر تعهد بین‌المللی که برای حفظ صلح و امنیت بین‌المللی اهمیت اساسی دارد؛ مانند ممنوعیت تجاوز درمجموع، علی‌رغم اینکه طرح مواد راجع به مسئولیت بین‌المللی کشورها فاقد قدرت اجرایی است و دیوان کیفری بین‌المللی هنوز تشکیل نگردیده است؛ اما مسلم است که عمل تجاوز و به‌طورکلی توسل به‌زور، چنانچه منطبق با مقررات منشور ملل متحد و قطعنامه تعریف تجاوز (مصوب ۱۹۷٤ مجمع عمومی ملل متحد) صورت‌گرفته باشد، جنایات بین‌المللی است. به‌علاوه این‌که اصل عدم تجاوز، اصل تحریم جنگ واصل عدم توسل به‌زور در زمره قواعد آمره بین‌المللی هستند (ضیائی بیگدلی،۱۳۸۲: ۲۶۰)

۱-۲-۷-آسیب‌پذیری حوزه دفاع حقوقی

پایه‌گذاری یک نظام دفاع حقوقی بین‌المللی برای فضای سایبری با آسیب‌هایی به این شرح روبه‌روست.

عدم متابعت از اصول حقوقی: ازجمله چالش‌های اساسی موجود در فضای سایبری با زبان حقوقی عدم تدوین نظام حقوقی حاکم بر فضای سایبری، همانند سایر نظام‌های حقوقی، نظیر معاهدات مربوط به سایر قلمروها (آب‌وخاک، هوا و فضا) است

چالش در مفاهیم سنتی قضایی :چالشی که اینترنت برای مفاهیم سنتی صلاحیت قضایی و حکمرانی ایجاد کرده است، چندوجهی است؛ اما به دو عامل وابسته است. اول وقتی که بر خط هستید، درآن‌واحد هم همه‌جا هستید و هم هیچ‌کجا نیستید. همه‌جایی بودن شاید ویژگی فضای سایبر بدون مرز است در این حالت جغرافیا تقریباً بی‌معنا است. دوم هیچ شرکت یا کشور واحدی کنترل اینترنت را در دست ندارد. بخش‌های مختلف این به‌اصطلاح (شبکه، شبکه‌ها) در مالکیت شرکت‌های خصوصی، سازمان‌ها یا حتی دولت‌ها است؛ اما اشاره به هر یک از مالکان خاص اینترنت امکان‌پذیر نیست. علت بحث‌برانگیز بودن صلاحیت قضایی در فضای سایبری این است که ما در این مورد با سیستم حقوقی ملی و اینترنت فراملی مواجه هستیم که ذاتاً باهم ناسازگارند (عاملی،۱۳۹۰: ۳۸۰).

وابستگی به قدرت‌های سیاسی: وضعیت فعلی فضای سایبری در سطح کره خاکی حاکی از آن است که فضای سایبری نه‌تنها از قواعد و اصول حقوقی متابعت نمی‌کند؛ بلکه کاملاً وابسته به قدرت‌های

سیاسی و تکنیکی کشورها و یا اشخاصی است که از امکانات پیشرفته‌تر و گسترده‌تر ارتباطی برخوردارند و هرگاه سازمان ملل متحد و یا سازمان‌های تخصصی آن خواسته‌اند قواعدی را بر این حوزه وضع و یا قواعد پراکنده آن را در چارچوبی بخصوص گردآوری کنند با مقاومت شدید کشورهای مختلف روبرو شده‌اند (آرابی، ۱۳۹۰: ۸).

تفاوت در سنت‌های حقوقی: وجود تفاوت در سنت‌های حقوقی کشورهای مختلف و مبادی مربوط نظیر عقاید دینی، حقوق عرفی، حقوق مدنی، حقوق شهروندی، حقوق بشر و نظایر آن.

تعارض منافع: تعارض منافع و نگرش‌های متفاوت اعتقادی به فضای سایبری و کارکردها و مقتضیات آن، مانند نگرش نسبت به حاکمیت و کنترل یا جریان آزاد اطلاعات و نیز تعارض نسبت به‌حق حاکمیت دولت‌ها و حقوق شهروندی در فضای سایبری (حافظنیا، ۱۳۹۰: ۳۰۸)

درهم تنیدگی: در هم تنیدگی مباحث پیچیده فنی که خاستگاه آن ابزارهای فنی اعم از رایانه، شبکه‌های رایانه‌ای و سوی دیگر جنبهٔ اجتماعی این فضا زمینه بروز و ظهور مسائلی را فراهم کرده است که در حقوق سنتی به آن پرداخته نشده است

عدم شناخت :عدم شناخت در زمینه‌های مختلف حقوقی و قراردادی، ظرفیت تصمیم‌گیری مسئولان را در مسائل مختلف کاهش می‌دهد. وقتی ما از تمامی حقوق مشروع خود در قلمروهای گوناگون اطلاع نداشته باشیم، به‌تبع قادر نخواهیم بود در مواقع مقتضی منافع و مصالح کشور خود را با تصمیمات و مواضع مقتضی در مجامع بین‌المللی و به هنگام عقد قراردادهای دو یا چندجانبه حفظ و ملحوظ کنیم.

۱-۲-۸-کارکردهای دفاع حقوقی در قبال تهدیدات خارجی در فضای سایبری

گام نخست و اساسی در جهت طراحی یک سازوکار مناسب در فضای سایبری برای هنجارمند کردن، قاعده سازی و قانونمند کردن فضای سایبری بهره‌گیری از چهارچوب حقوق داخلی و بین‌المللی است. کشورها و دولت‌ها در چهارچوب تلقی از منافع و مقتضیات و ارزش‌های خود اقدام به تدوین، تصویب و اجرای قوانین در فضای سایبری می‌نمایند و از این طریق حاکمیت خود بر فضای سایبری را منطبق بر قلمرو فضای ملی اعمال می‌کنند، ازاین‌رو در نظام حقوقی جمهوری اسلامی ایران نیز به علت اهمیت و جایگاه این عرصه مراکز مهمی در راستای مدیریت این فضا که موسوم به فضای مجازی ایجاد گردیده است، شورای عالی فضای مجازی یکی از مراکز مهمی است که در خصوص سامان‌دادن به این فضا ایجادشده است. در بند ده حکم انتصاب اعضای شورای عالی فضای مجازی که توسط مقام معظم رهبری صادر شده است آمده، این شورا موظف است در خصوص تدوین و تصویب نظام‌های امنیتی، حقوقی قضایی و انتظامی موردنیاز در فضای مجازی اهتمام ورزد (نعناکار، خلخالی، ۱۳۹۷: ۷). بدیهی است تدوین قواعد و هنجارهای حقوقی در حوزه حقوق داخلی برای اعمال حاکمیت بر فضای سایبری شرط لازم است،

اما کافی نیست. کنترل‌پذیری و قانون‌مند نمودن فضای سایبری مستلزم اجماع کشورهای جهان و همکاری آن‌ها در چهارچوب حقوق بین‌الملل است

در خصوص نظام حقوقی بین‌المللی که ناظر بر مقابله با تهدیدات خارجی در فضای سایبری باشد می‌توان گفت تاکنون غیر از موضوع نام دامنه و ارتباط آن با علامت تجاری که به سبب ضوابط جهانی آیکن و تصمیمات مراکز حل‌وفصل شبه قضایی بین‌المللی اختلاف مربوط به آن‌که از این رهگذر تقریباً مقررات و ضوابط یکنواختی تحقق یافته است، در سایر موارد مقررات لازم‌الاجرای متحد شکلی در سطح بین‌المللی به وجود نیامده و کشورها اساساً برحسب ساختار و مبانی حقوقی خود با مسائل مطروحه در این فضا برخورد می‌کنند (صادقی نشاط،۱۳۸۹: ۲۷۹)

۱-۲-۹-حقوق ارتباطات بین‌الملل و رابطه آن با دفاع سایبری

در حقوق بین‌الملل، طبقه‌بندی خاصی که مورد شناسایی و توافق عمومی باشد تحت عناوین حقوق ارتباطات و یا حقوق اطلاعات به چشم نمی‌خورد. این عناوین صرفاً به‌صورت پوششی برای یک سلسله موضوعات مختلف که با ارتباطات و اطلاعات مرتبط هستند به‌کاررفته است و علت آن نیز در دو امر خلاصه می‌شود: اولاً ارتباط در قالب مدنی آن پدیده‌ای نوظهور است و ثانیاً علم حقوق برای این زمینه، همچون دیگر امور اجتماعی اصولی وضع نکرده است (آرایی،۳۰: ۱۳۹۰). در متون حقوقی و کتب برتر حقوق بین‌الملل نیز به‌ندرت می‌توان مباحثی را راجع به حقوق ارتباطات یافت و در حال حاضر، تمامی نام‌گذاری‌های این حوزه بر محور یکی از موضوعات ارتباط (عناصر یا وسایل و یا خود اطلاعات) صورت گرفته است که اکثر آن‌ها نیز مبتنی بر وسایل ارتباطی است. به‌عنوان‌مثال: حقوق ارتباط دور، حقوق رسانه‌های جمعی، حقوق پخش، حقوق سایبر، حقوق اطلاعات، حقوق ارتباطات الکترونیکی و مواردی ازاین‌دست، شاخه‌هایی از حقوق ارتباطات هستند. همان‌طوری که در بالا ذکر شد، حقوق سایبر به واسط بهره‌گیری فضای سایبری از وسایل و عناصر ارتباط می‌توان آن را در ذیل حقوق ارتباطات قرارداد. ما در عرصه بین‌المللی، شاهد زمینه خاصی که به‌گونه‌ای منسجم، فضای سایبر را بررسی کند نبوده‌ایم و هریک از موضوع‌های حقوق سایبری به‌عنوان یک زمینه حقوقی مستقل، در یک چهارچوب قانونی و مقرراتی مخصوص به خود قرار دارد (حافظ‌نیا،۱۳۹۰: ۲۸۶). علت نبود یک بنیان خاص در حقوق سایبری شناسایی نشدن اصول مربوط به این حوزه است.

۳-روش‌شناسی تحقیق

۳-۱-نوع تحقیق در این پژوهش کاربردی -توسعه‌ای است و روش تحقیق مورداستفاده ترکیبی (روش توصیفی - تحلیلی و ترکیب با روش دلفی است.

۳-۲-جامعه آماری:

جامعه آماری در این پژوهش خبرگان، صاحب‌نظران و کارشناسان ارشد که در موضوع فضای سایبری و ارتباطات فعال هستند و دارای تحصیلات دکتری و یا حداقل دارای ۱۰ سال سابقه مدیریت در مشاغل مرتبط هستند، در نظر گرفته‌شده و حجم نمونه با توجه به اینکه جامعه آماری در این تحقیق در سطوح مشخصی قرارگرفته‌اند، از روش نمونه‌گیری غیر تصادفی هدفمند (گلوله برفی تا نیل به اشباع) بهره گرفته‌شده است؛ که این فرایند تا ۴۰ نفر دنبال شد.

۳-۳- روش جمع‌آوری داده‌ها:

در این پژوهش از دو روش گرداوری اطلاعات استفاده شده است.

الف)کتابخانهٔ علمی و تخصصی: در این پژوهش به‌منظور تدوین ادبیات و مباحث نظری تحقیق، از روش جمع‌آوری اطلاعات به‌صورت کتابخانه‌ای و بررسی اسنادی استفاده شد بدین‌صورت که با مطالعه متون، کتب، مقالات، منابع اینترنتی، تحقیقات پیشین مرتبط با عنوان تحقیق اطلاعات لازم با استفاده از فیش‌برداری جمع‌آوری گردید.

ب) روش میدانی: در این پژوهش به‌منظور دست یافتن به داده‌های موردنیاز و کسب دیدگاه خبرگان و صاحب‌نظران و کارشناسان ارشد در امور فضای سایبری، از روش جمع‌آوری میدانی اطلاعات با بهره‌گیری از روش دلفی و ابزار پرسش‌نامه استفاده شد.

۳-۴-روش تجزیه‌وتحلیل

در تحلیل داده‌ها از شاخص‌های مرکزی که مهم‌ترین آن میانگین است و همچنین با بهره‌گیری از نرم‌افزار Excel و SPSS مورد تجزیه‌وتحلیل قرار گرفت

۳-۵-روایی و پایایی پرسش‌نامه

با توجه به مؤلفه‌ها و متغیرهای برشمردن شده برای دفاع حقوقی پرسش‌نامه تهیه گردید و برای بررسی اعتبار آن در اختیار ۱۲ نفر از استادان و خبرگان قرار گرفت و پس از اخذ نظر صاحب‌نظران اصلاحات در دو مرحله انجام و پس از اعتبارسنجی و رفع اشکالات، پرسش‌نامه نهایی تهیه گردید. برای تعیین پایایی پرسش‌نامه از ضریب آلفای کرونباخ[1] استفاده شده است.

۳-یافته‌های تحقیق و تجزیه‌وتحلیل آن‌ها

ابتدا فرایند استخراج و احصای اصول و ارزش‌های حاکم، چالش‌های اساسی، ضعف‌ها، قوت‌ها، فرصت‌ها و تهدیدات مربوط به حوزه دفاع حقوقی در فضای سایبری از طریق بررسی یادداشت‌های نظری و برگزاری جلسات خبرگی و هم‌اندیشی تهیه و تنظیم گردید و سپس برای هر یک از موضوعات ۷ گانه (اصول و ارزش‌های حاکم، چالش‌های اساسی، ضعف‌ها، قوت‌ها، فرصت‌ها و تهدیدات، راهبردها) ۷ نوع

1. Cronbach Alpha

پرسش‌نامه تهیه شد در این پرسش‌نامه‌ها از سؤال‌های بسته استفاده گردید. در سؤال‌های بسته در مقابل هر یک از گویه‌ها ارزش‌گذاری از ۱ تا ۹ قرار داده شد تا پاسخ‌دهنده موضع (باورها، عقاید و نگرش) خود را در مورد آن سؤال بر روی یک طیف و مقیاس چند درجه‌ای با انتخابی که درواقع بهترین انتخاب او است ابراز نماید. پس از تنظیم پرسش‌نامه‌ها مقرر شد به تعداد ۴۰ نسخه از هر یک از آن‌ها، برای حجم نمونه مشخص‌شده ارسال و توسط آن‌ها تکمیل شود که در ادامه نتایج به‌دست‌آمده ارائه می‌گردد.

۱. به نظر شما که از اعضای جامعه نخبگی هستید، آیا متغیرهای زیر می‌تواند به‌عنوان اصول و ارزش‌های حاکم بر دفاع حقوقی سایبر قرار گیرد. اهمیت آن را چگونه ارزیابی می‌کنید؟

جدول شماره ۱: اهمیت اصول و ارزش‌های دفاع حقوقی سایبر

ردیف	اصول و ارزش‌های دفاع حقوقی سایبر	درجه اهمیت هر سؤال از صددرصد									
		۹	۸	۷	۶	۵	٤	۳	۲	۱	میانگین
۱	احترام به حاکمیت ملی	۹۷,۵	۲,۵	*	*	*	*	*	*	*	۹۹,۲
۲	رعایت حقوق بین‌الملل	۹۵	۲,۵	*	۲,۵	*	*	*	*	*	۹۸,۸
۳	دفاع مشروع	۱۲,۵	۷,۵	۸۰	*	*	*	*	*	*	۸۱,۳
٤	دفاع از منافع ملی	۲۲,۵	*	۷۷,۵	*	*	*	*	*	*	۸۲,۷
۵	قانون‌مداری	۷۵	۱۰	*	۵	*	۱۰	*	*	*	۲۰,۸
۶	ابتکار عمل در دفاع حقوقی	۱۲,۵	*	۸۷,۵	*	*	*	*	*	*	۸۰,۵
۷	چندوجهی بودن	۱۲,۵	۱۲,۵	*	*	۷۲,۵	۲,۵	*	*	*	۶۵
۸	هماهنگی عناصر	۱۲,۵	۷,۵	۵	*	۷۵	*	*	*	*	۶٤,۷
۹	در نظر داشتن منافع عموم	۵	۱۰	۷,۵	*	۷۵	*	*	*	*	۶۱,۳
۱۰	بصیرت سیاسی و دینی	۱۰	۱۵	۷۵	*	*	*	*	*	*	۲۳,۳
۱۱	عدم پذیرش حرف زور	۲۰	۵	۵۰	۲۵	*	*	*	*	*	۲٤,٤
	میانگین کل										۶۳,۹

از مجموعِ میانگین (۶۳/۹۱%)، حداقل تعداد پاسخگویان (۲۳/۳۳%)، شاخصِ بصیرت سیاسی و دینی را به‌عنوان اصول و ارزش‌های اساسی در حوزهٔ زیرساخت‌های دفاع حقوقی سایبر کشور دانسته و در نقطهٔ مقابل، بیشترین پاسخ‌گویان (۹۹/۷۲%)، خواهانِ احترام به حاکمیت ملی بوده و این شاخص را نسبت به سایر شاخص‌ها بالاتر دانسته و به‌عنوان اصول و ارزش‌های اساسی در حوزهٔ موردنظر معرفی نموده‌اند.

۲. به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان چالش‌های

اساسی در حوزه دفاع حقوقی سایبر قرار گیرد. اهمیت آن را چگونه ارزیابی می‌کنید؟

جدول شماره ۲: اهمیت چالش‌های اساسی دفاع حقوقی سایبر

ردیف	چالش‌های اساسی دفاع حقوقی سایبر	درجه اهمیت هر سؤال از صددرصد									
		۹	۸	۷	۶	۵	٤	۳	۲	۱	میانگین
۱	نبود قوانین	۹۹.۵	*	*	۲.۵	*	*	*	*	*	۹۹.۱
۲	عدم انطباق ویژگی‌ها	۹۲.۵	۵	۲.۵	*	*	*	*	*	*	۹۸.۸
۳	مشکل اثبات حقوقی	۹۲.۵	۷.۵	*	*	*	*	*	*	*	۹۹.۱
٤	عدم تبیین مفاهیم	۷.۵	۸۷.۵	۵	*	*	*	*	*	*	۸۹.۱
۵	نداشتن فرهنگ نهادینه	۱۰	۵	۸۵	*	*	*	*	*	*	۸۰.۵
۶	نبود ساختار	۲۰	۸۰	*	*	*	*	*	*	*	۹۱.۱
۷	عدم تبیین جرائم	۲.۵	۹۲.۵	۵	*	*	*	*	*	*	۸۸.۶
	میانگین کل										۹۲.۳

از مجموعِ میانگین (۹۲/۳۸%)، حداقل تعداد نخبگان (۸۰/۵٦%)، شاخصِ نداشتن فرهنگ نهادینه درخصوص چالش‌های دفاع حقوقی سایبر و ضعف در مسیر ارتقای توان مقاومت ملی در برابر هجمه‌های فرهنگی و دفاع حقوقی سایبر دشمن را مهم‌ترین عنوان چالش‌های اساسی در حوزه دفاع حقوقی سایبر تشخیص داده و در نقطهٔ مقابل، بیشترین نخبگان (۹۹/۱۷%)، در تشخیص خود، نبود قوانین در زیرساخت‌های دفاع حقوقی سایبر را مهم‌ترین چالش‌های اساسی در حوزهٔ یادشده اعلام کرده‌اند (جدول ۴/۴۴).

۳. به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان تهدید در زیرساخت‌های دفاع حقوقی سایبر قرار گیرد. اهمیت آن را چگونه ارزیابی می‌کنید؟

جدول شماره ۳: اهمیت تهدیدات دفاع حقوقی سایبر

ردیف	تهدیدات دفاع حقوقی سایبر	درجه اهمیت هر سؤال از صددرصد									
		۹	۸	۷	۶	۵	٤	۳	۲	۱	میانگین
۱	اشراف اطلاعاتی	۹۷.۵	۲.۵	*	*	*	*	*	*	*	۹۹.۷
۲	سابقه انجام حمله	۱۲.۵	۸۵	۲.۵	*	*	*	*	*	*	۹۰

ردیف	تهدیدات دفاع حقوقی سایبر	درجه اهمیت هر سؤال از صددرصد									
		۹	۸	۷	۶	۵	٤	۳	۲	۱	میانگین
۳	وجود حمله	۲۰	۵	۷۵	*	*	*	*	*	*	۸۲,۷
٤	توان و ظرفیت آفندی دشمن	۲۰	۸۰	*	*	*	*	*	*	*	۹۱,۱
۵	داشتن فرماندهی سایبری	۱۰	۸۲,۵	۵	۲,۵	*	*	*	*	*	۸۸,۹
	میانگین کل										۹۰,۵

از مجموعِ میانگین (۹۰/۵%)، حداقل تعداد نخبگان (۸۲/۷۸%)، شاخصِ وجود راهبرد حمله را مهم‌ترین تهدید در زیرساخت‌های دفاع حقوقی سایبر تشخیص داده و در نقطهٔ مقابل، بیشترین نخبگان (۹۹/۷۲%)، در تشخیص خود، اشراف اطلاعاتی در حوزهٔ زیرساخت‌های دفاع حقوقی سایبر کشور را مهم‌ترین تهدید در حوزهٔ یادشده اعلام کرده‌اند (جدول ۴/۴۵).

٤. به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان فرصت در زیرساخت‌های دفاع حقوقی سایبر کشور قرار گیرد. اهمیت آن را چگونه ارزیابی می‌کنید؟

جدول شماره ٤: اهمیت فرصت‌ها دفاع حقوقی سایبر

ردیف	فرصت‌های دفاع حقوقی سایبر	درجه اهمیت هر سؤال از صددرصد									
		۹	۸	۷	۶	۵	٤	۳	۲	۱	میانگین
۱	استفاده از قوانین مرجع	۱۲,۵	۷,۵	۸۰	*	*	*	*	*	*	۸۱,۳
۲	استقلال نسبی	۵	۱۲,۵	۵	۷۵	۲,۵	*	*	*	*	۷۱,۳
۳	استفاده از قوانین اعلام یک‌طرفه	۱۲,۵	۷,۵	۲,۵	۷۷,۵	*	*	*	*	*	۷۲,۷
٤	مظلوم‌نمایی	۱۰	۸۵	۵	*	*	*	*	*	*	۸۹,٤
۵	استفاده از تجارب حقوقی	۵	۸۵	۵	*	۲,۵	*	*	*	*	۸۵,۸
۶	استفاده از قوانین مرجع بین‌الملل	۲۵	۵۰	۲۵	*	*	*	*	*	*	۲۱,۳
۷	استقلال نسبی بعضی از مراکز جهانی	٤۰	۵۰	۱۰	*	*	*	*	*	*	۱۷,۲
۸	استفاده از قوانین اعلام یک‌طرفه	۱۰	۵۰	٤۰	*	*	*	*	*	*	۱۸,۳
	میانگین کل										۵۷,۲

از مجموعِ میانگین (۵۷/۲۲%)، کمترین تعداد پاسخگویان (۱۸/۳۳%)، شاخص استفاده از قوانین اعلام یک‌طرفه را به‌عنوان فرصت در زیرساخت‌های دفاع حقوقی سایبر کشور اعلام کرده‌اند و از سوی دیگر، بیشترین تعداد پاسخگویان (۸۹/٤٤%)، در اعلام نظر خود شاخصِ مظلوم‌نمایی را به‌عنوان یک

فرصت در زیرساخت‌های دفاع حقوقی سایبر کشور ارزیابی کرده‌اند (جدول ۴/۴۶).

۵. به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان ضعف در زیرساخت‌های دفاع حقوقی سایبر کشور محسوب شود. اهمیت آن را چگونه ارزیابی می کنید؟

. جدول شماره ۵: اهمیت ضعف‌های دفاع حقوقی سایبر

ردیف	ضعف‌های اساسی دفاع حقوقی سایبر	درجه اهمیت هر سؤال از صددرصد									
		۹	۸	۷	۶	۵	٤	۳	۲	۱	میانگین
۱	نبود قوانین بین‌المللی	۱۵	۸۰	۵	*	*	*	*	*	*	۸۸
۲	عدم تطابق عناصر دفاع سایبری	۱۰	۱۲.۵	۷۵	*	*	*	*	*	*	۷۹.٤
۳	نبود نظام دفاع حقوقی سایبر	۹۰	۱۰	*	*	*	*	*	*	*	۸۸.۹
٤	نبود انسجام بین دستگاه‌های عضو چرخه	۱۵	۷۷.۵	۷.۵	*	*	*	*	*	*	۸۹.۷
۵	نبود درک واحد در مسئولین حوزه امنیت ملی کشور	۱۰	۱۲.۵	۷۵	۲.۵	*	*	*	*	*	۸۱.۱
۶	نبود متولی اقامه دعوی حقوقی بین‌المللی سایبری	۱۰	۱۲.۵	۷۷.۵	*	*	*	*	*	*	۸۱.۳
۷	ضعف اساسی در اثبات و ثبت	۱۷.۵	۲.۵	۸۰	*	*	*	*	*	*	۸۱.۹
۸	ضعف عمده دستگاه‌های موردتهاجم	۱۷.۵	۵	۷۷.۵	*	*	*	*	*	*	۸۲.۲
	میانگین کل										۸٤

از مجموعِ میانگین (۸٤/۰۹%)، حداقل تعداد نخبگان (۷۹/٤٤%)، در تشخیص خود شاخصِ عدم تطابق عناصر دفاع سایبری را به‌عنوان ضعف در حوزهٔ موردنظر اعلام کرده‌اند لیکن در نقطهٔ مقابل، بیشترین نخبگان (۸۸/۸۹%)، در ارزیابی خویش نبود نظام دفاع حقوقی سایبر را به‌عنوان ضعف در زیرساخت‌های دفاع حقوقی سایبر کشور دانسته‌اند

٦. به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان قوت در زیرساخت‌های دفاع حقوقی سایبر کشور محسوب گردد. اهمیت آن را چگونه ارزیابی می کنید؟

جدول شماره ٦: اهمیت قوت‌های دفاع حقوقی سایبر

ردیف	قوت‌های دفاع حقوقی سایبر	درجه اهمیت هر سؤال از صددرصد									
		۹	۸	۷	٦	۵	٤	۳	۲	۱	میانگین
۱	استفاده از شخصیت‌ها	۱۵	۸۵	*	*	*	*	*	*	*	۹۰.۵
	میانگین کل										۹۰.۵

از مجموعِ میانگین (۹۰/٥٦%)، استفاده از شخصیت‌ها را به‌عنوان قوت در این حوزه اعلام کرده‌اند.

۷. به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان راهبردهای زیرساخت‌های دفاع حقوقی سایبر قرار گیرد. اهمیت آن را چگونه ارزیابی می کنید؟

جدول شماره ۷: اهمیت راهبردهای دفاع حقوقی سایبر

ردیف	راهبردهای دفاع حقوقی سایبر	درجه اهمیت هر سؤال از صددرصد									
		۹	۸	۷	۶	۵	٤	۳	۲	۱	میانگین
۱	تدوین قوانین	۱۵	۸۵	*	*	*	*	*	*	*	۹۰،۵
۲	حداکثر استفاده از قوانین	۸۷،۵	۱۲،۵	*	*	*	*	*	*	*	۸۸،۶
۳	نهادینه‌سازی فرهنگی	۱۲،۵	۸۷،۵	*	*	*	*	*	*	*	۹۰،۲
٤	طراحی و ساماندهی	۹۵	۵	*	*	*	*	*	*	*	۸۹،٤
۵	سازمان‌دهی و تقسیم کار	۷،۵	۹۲،۵	*	*	*	*	*	*	*	۸۹،۷
۶	طراحی و پیاده‌سازی	۱۲،۵	۱۰	۷۷،۵	*	*	*	*	*	*	۸۱،۶
۷	برشمردن جرائم	۹۲،۵	۵	۲،۵	*	*	*	*	*	*	۸۸،۹
۸	راه‌اندازی سامانه جمع‌آوری ادله	۱۰	۹۰	*	*	*	*	*	*	*	۹۰
۹	طراحی پیمان دفاعی	۸۰	۲۰	*	*	*	*	*	*	*	۸۷،۵
	میانگین کل										۸۸،۵
	میانگین‌مجموع										۸۵،۱

از مجموعِ میانگین (۸۸/۵۵%)، حداقل تعداد نخبگان (۸۱/٦۷%)، در تشخیص خود شاخصِ طراحی و پیاده‌سازی را به‌عنوان راهبردهای زیرساخت‌های دفاع حقوقی سایبر کشور دانسته‌اند و در نقطهٔ مقابل نیز بیشترین تعداد نخبگان (۹۰/۵٦%)، در نظرات خویش تدوین قوانین را به‌عنوان راهبردهای زیرساخت‌های دفاع حقوقی سایبر کشور ارزیابی کرده‌اند

ماتریس ارزیابی اصول و ارزش‌های حاکم، چالش‌های اساسی، تهدید، فرصت، ضعف، قوت و راهبردها در هر یک از حوزه‌های دفاع سایبری و میانگین این حوزه‌ها

جدول شماره ۸: ماتریس حوزه‌ها و متغیرهای دفاع سایبری

متغیرها حوزه‌های دفاع سایبری	اصول و ارزش‌های حاکم	چالش‌های اساسی	تهدید	فرصت	ضعف	قوت	راهبردها
دفاع حقوقی	۶۳،۹	۹۳،۲	۹۰،۵	۵۷،۲	۸٤،۱	۹۰،۵	۸۸،۵

در این بخش، اصول و ارزش‌های حاکم، چالش‌های اساسی، تهدید، فرصت، ضعف، قوت و راهبردها در حوزه‌های دفاع سایبری به‌صورت یکجا بررسی شده است که بیشترین امتیاز (۹۳/۲) مربوط به چالش‌های

اساسی و کمترین امتیاز (۵۷/۲) مربوط به فرصت‌ها در حوزه‌های دفاع سایبری بوده است

طرح راهبردی دفاع حقوقی

در این بخش از پژوهش پس از سنجش متغیرهای مؤلفه‌های ۷ گانه زیرساخت‌های دفاع حقوقی (اصول و ارزش‌ها، چالش‌ها فرصت‌ها، تهدیدها، ضعف‌ها، قوت‌ها، راهبردها)، متغیرهایی که بالاترین امتیاز را کسب کرده بودند، یافته و مجدد در قالب پرسش‌نامه از نخبگان خواسته شد اولویت اهمیت هر متغیر را در طرح راهبردی دفاع حقوقی مشخص کنند.

۱. به نظر شما که از اعضای جامعه نخبگی هستید، آیا متغیرهای زیر می‌تواند به‌عنوان اصول و ارزش‌های حاکم بر طرح راهبردی دفاع حقوقی قرار گیرد. اهمیت آن را چگونه ارزیابی می کنید؟

ردیف	اصول و ارزش‌های اساسی طرح راهبردی دفاع حقوقی	درجه اهمیت هر سؤال از صددرصد									
		۱	۲	۳	٤	۵	۶	۷	۸	۹	میانگین
۱	احترام به حاکمیت ملی	*	*	۵	۱۵	۶۷,۵	۷,۵	۵	*	*	۵٤,۷
۲	رعایت حقوق بین‌الملل	*	*	۷,۵	۱۲,۵	۶۰	۲۰	*	*	*	۵۵,۸
۳	بصیرت سیاسی و دینی	*	*	*	*	*	*	*	۱۵	۸۵	۹۸,٤
	میانگین کل										۶۹,۶

از مجموعِ میانگین (٦۹/٦)، حداقل تعداد پاسخگویان (٥٤/۷)، شاخصِ احترام به حاکمیت ملی را به‌عنوان اصول و ارزش‌های حاکم بر طرح راهبردی دفاع حقوقی دانسته و در نقطهٔ مقابل، بیشترین مخاطبان (۹۸/٤%)، بصیرت سیاسی و دینی را نسبت به آن بالاتر دانسته و به‌عنوان اصول و ارزش‌های اساسی دفاع حقوقی معرفی نموده‌اند.

۲. به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان چالش‌های اساسی در طرح راهبردی دفاع حقوقی قرار گیرد. اهمیت آن را چگونه ارزیابی می کنید؟

ردیف	چالش‌های اساسی طرح راهبردی دفاع حقوقی	درجه اهمیت هر سؤال از صددرصد									
		۱	۲	۳	٤	۵	۶	۷	۸	۹	میانگین
۱	نبود قوانین	*	*	*	*	*	*	*	۷۵	۹۲,۵	۹۹,۱
۲	مشکل اثبات حقوقی	*	*	*	*	۱۰	۸۰	۱۰	*	*	۶۶,۷
	میانگین کل										۸۲/۹

از مجموعِ میانگین (۸۲/۹)، حداقل تعداد نخبگان (۶۶/۷%)، شاخصِ مشکل اثبات حقوقی را به‌عنوان چالش در دفاع سایبری تشخیص داده و در نقطهٔ مقابل، بیشترین نخبگان (۹۹/۱%)، در تشخیص خود، نبود قوانین در زیست‌بوم سایبری را مهم‌ترین چالش اساسی در حوزهٔ یادشده اعلام کرده‌اند.

۳-به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان تهدید در طرح راهبردی دفاع حقوقی قرار گیرد. اهمیت آن را چگونه ارزیابی می کنید؟

ردیف	گویه‌های تهدید دفاع حقوقی	درجه اهمیت هر سؤال از صددرصد									
		۱	۲	۳	٤	۵	۶	۷	۸	۹	میانگین
۱	اشراف اطلاعاتی	*	*	*	۵	۲۰	۶۰	۱۵	*	*	۶۵
۲	توان و ظرفیت آفندی دشمن	*	*	*	*	۲٫۵	۱۲٫۵	۶۵	۲۰	*	۷۸
	میانگین کل										۷۱/۵

از مجموعِ میانگین (۷۱/۵%)، حداقل تعداد نخبگان (٦۵%) شاخصِ اشراف اطلاعاتی را مهم‌ترین تهدید در طرح راهبردی دفاع حقوقی تشخیص داده و در نقطهٔ مقابل، بیشترین نخبگان (۷۸%) در تشخیص خود توان و ظرفیت آفندی دشمن را مهم‌ترین تهدید در حوزهٔ یادشده اعلام کرده‌اند.

٤-به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان فرصت در طرح راهبردی دفاع حقوقی قرار گیرد. اهمیت آن را چگونه ارزیابی می کنید؟

ردیف	گویه‌های فرصت دفاع سایبری	درجه اهمیت هر سؤال از صددرصد									
		۱	۲	۳	٤	۵	۶	۷	۸	۹	میانگین
۱	مظلوم‌نمایی	*	*	۲٫۵	۷٫۵	۲۰	٤۷٫۵	۲۰	۲٫۵	*	۶٤٫۷
۲	استفاده از تجارب حقوقی	*	*	۷٫۵	۲۲٫۵	۳۵	۲۷٫۵	۷٫۵	*	*	۵۶٫۱
	میانگین کل										۶۰/٤

از مجموعِ میانگین (٦۰/٤%) کمترین تعداد پاسخگویان (۱/ ۵٦%)، شاخص استفاده از تجارب حقوقی را به‌عنوان فرصت در دفاع حقوقی کشور اعلام کرده‌اند و از سوی دیگر، بیشترین تعداد پاسخگویان (٦٤/۷%)، در اعلام نظر خود شاخصِ استفاده از تجارب حقوقی را به‌عنوان یک فرصت در دفاع سایبری کشور ارزیابی کرده‌اند

۵-به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان ضعف در طرح

راهبردی دفاع حقوقی قرار گیرد. اهمیت آن را چگونه ارزیابی می کنید؟

ردیف	گویه‌های ضعف دفاع حقوقی	درجه اهمیت هر سؤال از صددرصد									
		۱	۲	۳	٤	٥	٦	۷	۸	۹	میانگین
۱	نبود انسجام بین دستگاه‌های عضو چرخه در حوزه سایبر	*	*	*	۲٫۵	۲٫۵	۲۰	۵۷٫۵	۱۷٫۵	*	۷۶٫۱
۲	نبود نظام دفاع حقوقی سایبر	*	*	*	*	۵	۱۰	۷۰	۱۵	*	۷۷٫۲
۳	ضعف عمده دستگاه‌های موردتهاجم	*	*	*	۲٫۵	۵	۲٫۵	۷٫۵	۷۰	۱۲٫۵	۸۶٫۱
	میانگین کل										۷۹/۸

از مجموعِ میانگین (۷۹/۸%) کمترین تعداد پاسخگویان (۷٦/۱%)، شاخص **نبود انسجام بین دستگاه‌های عضو چرخه در حوزه سایبر** را به‌عنوان ضعف در دفاع حقوقی کشور اعلام کرده‌اند و از سوی دیگر، بیشترین تعداد پاسخگویان (۸٦/۱%)، در اعلام نظر خود شاخصِ ضعف عمده دستگاه‌های موردتهاجم را به‌عنوان یک ضعف در دفاع حقوقی کشور ارزیابی کرده‌اند.

٦-به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان قوت در طرح راهبردی دفاع حقوقی قرار گیرد. اهمیت آن را چگونه ارزیابی می کنید؟

ردیف	گویه‌های قوت دفاع سایبری	درجه اهمیت هر سؤال از صددرصد									
		۱	۲	۳	٤	٥	٦	۷	۸	۹	میانگین
۵	استفاده از شخصیت‌ها	*	*	۲٫۵	۱۵	۶۷٫۵	۱۵	*	*	*	۵۵
	میانگین کل										۵۵

۷-به نظر شما که از اعضای جامعه نخبگی هستید، آیا گویه‌های زیر می‌تواند به‌عنوان راهبرد در طرح راهبردی دفاع حقوقی قرار گیرد. اهمیت آن را چگونه ارزیابی می کنید؟

ردیف	گویه‌های راهبردی دفاع حقوقی	درجه اهمیت هر سؤال از صددرصد									
		۱	۲	۳	٤	٥	٦	۷	۸	۹	میانگین
۱	تدوین قوانین	*	*	*	۲٫۵	۲٫۵	۵	۷۵	۱۰	۵	۶۸/۵
۲	نهادینه‌سازی فرهنگی	*	*	*	*	۷٫۵	۵	۷۵	۱۰	۲٫۵	۶۸
۳	راه‌اندازی سامانه جمع‌آوری ادله	*	*	*	*	*	۱۲٫۵	۷۲٫۵	۱۵	*	۶۷/۷
٤	سازمان‌دهی و تقسیم کار	*	*	*	*	*	۱۰	۷۷٫۵	۱۲٫۵	*	۶۶/۳
	میانگین کلی										۶۷/۶

از مجموعِ میانگین (۶۷/۶%) کمترین تعداد پاسخگویان (۶۶/۳%)، شاخص سازماندهی و تقسیم‌کار در حوزه حقوقی را به‌عنوان راهبرد در دفاع حقوقی کشور اعلام کرده‌اند و از سوی دیگر، بیشترین تعداد پاسخگویان (۶۸/۵%)، در اعلام نظر خود شاخصِ تدوین قوانین را به‌عنوان راهبرد در دفاع حقوقی کشور ارزیابی کرده‌اند

نتیجه‌گیری

هدف اصلی این تحقیق شناخت وضعیت زیرساخت‌های دفاع حقوقی در حوزه‌های سایبری و تهدیدهایی که متوجه این حوزه‌ها بوده و سپس ارائه طرح راهبردی دفاع حقوقی کشور در برابر تهدیدات سایبری بوده است؛ که در اجرای این تحقیق و در درجه نخست با انجام مطالعات اکتشافی و انجام مطالعات نظری و با استفاده از اسناد و مدارک معتبر مبادرت به شناخت کلیاتی از وضعیت سایبری کارکردها و تهدیدهایی که از این ناحیه در کشور وجود دارد پرداخته شد و سپس با مراجعه به جامعه خبرگی و جامعه آماری درصدد پاسخگویی به سؤالات پژوهشی به شرح زیر برآمده است:

. در پاسخ به سؤال اصلی پژوهش برای دستیابی به طرح راهبردی دفاع حقوقی در مقابله با تهدیدهای سایبری، منابع دینی، اسناد بالادستی، مبانی نظری، مطالعات تطبیقی و سایر مطالعات انجام و اصول و ارزش‌های حاکم بر طرح، عوامل خارجی و داخلی مؤثر بر آن و راهبردهای دفاع سایبری برشمردن و با استفاده از نرم‌افزار EXCEL و نرم‌افزار SPSS تجزیه‌وتحلیل داده‌ها انجام گرفت.

که مشخص شد اصول و ارزش‌های اولویت‌دار حاکم بر طرح راهبردی دفاع حقوقی عبارتند از (بصیرت سیاسی و دینی، رعایت حقوق بین‌الملل، احترام به حاکمیت ملی) چالش‌های اساسی در طرح راهبردی دفاع حقوقی عبارتند از (مشکل اثبات حقوقی، نبود قوانین) تهدید در طرح راهبردی دفاع حقوقی عبارتند از (اشراف اطلاعاتی دشمن، توان و ظرفیت آفندی دشمن) فرصت در طرح راهبردی دفاع حقوقی عبارتند از (استفاده از تجارب حقوقی، مظلوم‌نمایی) ضعف در طرح راهبردی دفاع حقوقی عبارتند از (نبود انسجام بین دستگاه‌های عضو چرخه در حوزه سایبر، نبود نظام دفاع حقوقی سایبر، ضعف عمده دستگاه‌های موردتهاجم) قوت در طرح راهبردی دفاع حقوقی عبارتند از (استفاده از شخصیت‌ها) و راهبرد در طرح راهبردی دفاع حقوقی عبارتند از تدوین قوانین، نهادینه‌سازی فرهنگی، راه‌اندازی سامانه جمع‌آوری ادله، سازماندهی و تقسیم‌کار)

و در پاسخ به سؤال دیگر پژوهش مبنی بر این‌که اصول و ارزش‌های حاکم، چالش‌های اساسی، ضعف‌ها، قوت‌ها، فرصت‌ها و تهدیدها، حوزه دفاع حقوقی در فضای سایبری چیست مشخص شد. در بحث اصول (احترام به حاکمیت ملی، رعایت حقوق بین‌الملل، دفاع مشروع، دفاع از منافع ملی، قانون مداری، ابتکار عمل در دفاع حقوقی، چندوجهی بودن، هماهنگی عناصر، در نظر داشتن منافع عمومی،

بصیرت سیاسی و دینی، عدم پذیرش حرف زور) را می‌توان به‌عنوان اصول و ارزش‌های حاکم قلمداد کرد و در بحث چالش‌ها (نبود قوانین، عدم انطباق ویژگی‌ها، مشکل اثبات حقوقی، عدم تبیین مفاهیم، نداشتن فرهنگ نهادینه، نبود ساختار، عدم تبیین جرائم) را می‌توان به‌عنوان چالش‌های این حوزه دانست و در بحث ضعف‌ها (نبود قوانین بین‌المللی، عدم تطابق عناصر دفاع سایبری، نبود نظام دفاع حقوقی سایبر، نبود انسجام بین دستگاه‌های عضو چرخه، نبود درک واحد در مسئولین حوزه امنیت ملی کشور، نبود متولی اقامه دعوی حقوقی بین‌المللی سایبری، ضعف اساسی در اثبات و ثبت، ضعف عمده دستگاه‌های موردتهاجم) را به‌عنوان ضعف‌های این حوزه منظور نمود و در بحث قوت‌ها (استفاده از شخصیت‌ها) را نام برد و در رابطه با تهدیدها (اشراف اطلاعاتی، سابقه انجام حمله، وجود راهبرد حمله، توان و ظرفیت آفندی دشمن، داشتن فرماندهی سایبری) را به‌عنوان تهدید در این حوزه در نظر گرفت و از تدوین قوانین، حداکثر استفاده از قوانین، نهادینه‌سازی فرهنگی، طراحی و ساماندهی، سازماندهی و تقسیم‌کار، طراحی و پیاده‌سازی، برشمردن جرائم، راه‌اندازی سامانه جمع‌آوری ادله، طراحی پیمان دفاعی را به‌عنوان راهبردهای دفاع حقوقی سایبر نام برد.

پیشنهادها:

– ساماندهی ساختار سازمانی جامع برای تقویت هماهنگی و انسجام در نهادهای کشور در حوزه سایبر

– بهره‌گیری از دیپلماسی منطقه‌ای در جهت شکل‌دهی ائتلاف و اتحاد برای مطالبه از مجامع جهانی در جهت وضع قوانین الزام‌آور برای فضای سایبر.

– انجام تحقیقات تکمیلی توسط پژوهشگران آشنا به حوزه سایبر در جهت جاری‌سازی راهبردهای به‌دست‌آمده

–افزایش دانش سایبری نمایندگان مجلس شورای اسلامی در جهت بهره‌گیری بیشتر از ظرفیت قوه مقننه در جهت تقویت حکمرانی در فضای سایبر

منابع:

- آرایی، میثم (۱۳۹۰) **حقوق بین‌الملل ارتباطات**، تهران: انتشارات سروش
- ابوالحسینی، علیرضا (۱۳۹۲) **معرفی و برآورد تهدیدات سایبری**، تهران: انتشارات دیده‌بان
- اسلوین، جمیز، **اینترنت و جامعه**، ترجمه عباس گیلوردی و علی رادباوه، نشر کتابدار، تهران، ۱۳۸۰
- اینترنت و فنّاوری اطلاعات (۱۳۹۲) سایت ساز اطلاعات: (WWW.hccmr.com/news)
- بی‌نا (۱۳۹۰) **راهبردهای امنیت فضای سایبری در سه کشور**، تهران: انتشارات موسسه آموزشی و تحقیقاتی صنایع دفاعی
- جاویدنیا، جواد (۱۳۸۷) جرائم **تجارت الکترونیکی**، تهران: انتشارات خرسندی

حافظ‌نیا، محمدرضا (۱۳۹۰)، **جغرافیای سیاسی فضای مجازی**، تهران: سازمان مطالعه و تدوین کتب علوم انسانی

- حسن‌بیگی، ابراهیم (۱۳۸۸)، **حقوق و امنیت در فضای سایبر**، تهران: انتشارات دانشگاه عالی دفاع ملی
- حسینی نژاد، حسینقلی، (۱۳۸۳) **حقوق کیفری بین‌الملل**، تهران: انتشارات میزان
- خوش عمل، حسین (۱۳۹۱) پدافند **غیرعامل در حوزه سایبر**، تهران: مرکز آموزشی و پژوهشی شهید صیاد شیرازی
- ستوده، محمد (۱۳۸۵) **تحولات نظام بین‌الملل** قم: دانشگاه امام محمدباقر علیه‌السلام
- صادقی نشاط، امیر (۱۳۸۹) حقوق **پدیدآورندگان نرم‌افزارهای کامپیوتری**، تهران، انتشارات میزان
- ضیایی بیگدلی، محمدرضا (۱۳۸۲)، **حقوق بین‌الملل عمومی**، تهران: کتابخانه گنج دانش
- قدیمی و دیگران (۱۳۹۳) مدیریت بحران در فضای سایبری، تهران: انتشارات مرکز آموزشی پژوهشی شهید صیاد شیرازی
- عاملی، سعیدرضا (۱۳۹۲) **محتوای ملی در فضای مجازی**، انتشارات سازمان اسناد
- عصاریان نژاد، حسین (۱۳۹٤) نشست تخصصی (کتاب مجموعه مقالات سایبر و فنّاوری)
- کدخدایی، عباس (۱۳۷۹) **برنامه‌های ماهواره‌ای از دیدگاه حقوقی**، تهران: موسسه مطالعات و پژوهش‌های حقوقی
- کرامر، فرانکلین و دیگران (۱۳۹٤) **قدرت سایبری و امنیت ملی**، ترجمه معاونت پژوهش و تولید علم، تهران موسسه چاپ انتشارات دانشگاه امام محمدباقر علیه‌السلام
- کیانی، داود (۱۳۸٦) **منافع ملی جمهوری اسلامی ایران**، تهران: پژوهشکده مطالعات راهبردی
- کلاهچیان، محمود، (۱۳۸٤) **الگوی طراحی راهبرد امنیت ملی در جمهوری اسلامی ایران**، مجموعه مقالات اولین همایش ملی مطالعات استراتژیک در جمهوری اسلامی ایران، تهران.
- مایک، کلاو، (۱۳۸۸)، **تهاجم و حفاظت سایبری**، مترجم: عبدالحسین طائفی، تهران: انتشارات دانشگاه عالی دفاع ملی
- مرادیان، محسن (۱۳۸۸) تهدید **و امنیت، تهران**، انتشارات مرکز آموزشی پژوهشی شهید صیاد شیرازی
- مطالعات گروهی (۱۳۸۷)، **نظریه امنیت در جمهوری اسلامی ایران**، تهران: انتشارات دانشگاه عالی دفاع

- میر محمدصادقی، حسین (۱۳۸۳) **حقوق کیفری اختصاصی جرائم علیه امنیت**، تهران: انتشارات میزان
- موسی زاده، رضا (۱۳۹۱)، **بایسته‌های حقوق بین‌الملل عمومی**، تهران: بنیاد حقوقی میزان
- نعناکار، محمدجعفر خلخالی، محمدحسن (۱۳۹۷) مجموعه قوانین و مقررات مبتنی بر فضای مجازی، تهران: انتشارات راه پرداخت
- هاشمی‌زاده، انصاری نسب (۱۳۹۶) **عصر مجازی تأملی بر کارکردها و رویکردهای جامعه مجازی**، تهران: انتشارات تیسا