فصلنامهٔ علمی راهبرد دفاعی، سال ، شمارهٔ ، ۱۴۰۱

فرمانده معظم کل قوا: «فضای مجازی پدیده‌ی تازه‌ای است و قبلاً وجود نداشته، بنابراین، برای پیشگیری از مشکلات ناشی از آن و برای اینکه کشور و جامعه از مشکلاتش و ضررهایش و آسیب‌هایش مصون بماند، امروز به فکرهای جدید و راه‌های ابتکاری و در واقع دانش و فکر نو نیاز هست».

مقالهٔ پژوهشی: بررسی و تبیین نقش دیپلماسی جمهوری اسلامی ایران در کنترل تهدیدات سایبری

20.1001.1.17351723.1401.20.77.2.8

رهبر طالعی حور[۱] جمشید نصرت آبادی[۲] محمد حاجی حسینی[۳]

تاریخ دریافت: ۱۴۰۱/۰۲/ تاریخ پذیرش: / /۱۴۰۱

چکیده

دیپلماسي در تاریخ سیاسي جهان پیشینه ای دیرینه دارد. گرایش به قدرت و حفاظت از منافع و وحشت از جنگ و پیامدهای ناگوار آن در ایجاد و توسعه روابط دیپلماسي تأثیرگذار بوده است. از سویی دیگر قابلیت‌ها و امکانات فضای سایبر سبب شده است تا در قرن بیست و یکم بسیاری از کشورها برای تسهیل اداره امور جوامع خود استقبال زیادی به منظور بهره گیری از این فضا از خود نشان دهند و این فضا ضمن ایجاد فرصت، می‌تواند خطرات جبران ناپذیری را برای دولت‌ها به وجود آورد که فضای سایبری جمهوری اسلامی ایران نیز از این قاعده مستثنی نیست. این پژوهش با هدف بررسی نقش دیپلماسی جمهوری اسلامی ایران در کنترل تهدیدات سایبری انجام شده است از نظر هدف، کاربردی و از نظر روش، توصیفی - تحلیلی است. جامعه آماری این پژوهش ۲۵۸ نفر و تعداد نمونه آماری با استفاده از فرمول کوکران ۱۰۰ نفر تعیین‌شده است. با استناد به منابع کتابخانه اي و پژوهش‌میداني و بر اساس‌تجزیه وتحلیل پرسشنامه ها، یافته های تحقیق بیانگر این است که دیپلماسی رسمی جمهوری اسلامی ایران با استفاده از معاهدات دو یا چند جانبه سایبری می‌تواند موجب کاهش اثر تهدیدات سایبری بر علیه منافع ملی شود و دیپلماسی عمومی جمهوری اسلامی ایران موجب تنویر افکار عمومی در سطح بین الملل گردیده و با توجه به گستردگی فضای سایبر در تمامی نقاط جهان، دولتمردان

۱. استادیار روابط بین الملل دانشگاه محقق اردبیلی،اردبیل، ایران (نویسنده مسئول) taleihur10@gmail.com

۲ .استادیار و عضو هیئت علمی دانشگاه فارابی، تهران، ایران Dr.Nosratabadi110@gmail.com

۳ . دانش آموخته کارشناسی ارشد علوم سیاسی

کشورهای معاند جمهوری اسلامی ایران را برای اقدام علیه منافع کشور، درتنگنا قرار دهد.

واژگان کلیدی: دیپلماسی، جمهوری اسلامی ایران، دیپلماسی رسمی، دیپلماسی عمومی،تهدیدات سایبری.

مقدمه

امروزه دیپلما سی در انواع مختلف آن مهم‌ترین ابزار برای تضمین کسب منافع و امنیت ملی می‌باشد. به این معنی که برای بالا بردن سطح تعامل و همکاری بین کشورها در سطوح مختلف و جایگزین کردن ثبات به جای تنش، این مفهوم کاربرد اساسی دارد. از سویی دیگر قابلیت‌ها و امکانات فضای سایبر سبب شده است تا در قرن بیست و یکم بسیاری از کشورها برای تسهیل اداره امور جوامع خود استقبال زیادی به منظور بهره گیری از این فضا از خود نشان دهند. با این وجود وابستگی کشورهای دنیا به این فضا همواره نمی‌تواند به عنوان یک فرصت در نظر گرفته شود و تهدیداتی که علیه فضای سایبری یک کشور صورت می گیرد، می تواند خطرات جبران ناپذیری را برای دولت‌ها بوجود آورد. فضای سایبری جمهوری اسلامی ایران نیز از این قاعده مستثنی نیست.(شیرنگی، ۱۳۹۱ : ۷)

ماهیت و ویژگی‌های فضای سایبر از جمله فراگیربودن این فضا، ناشناس بودن بازیگران این عرصه و ... موجب می‌شود روش‌های معمول در کنترل تهدیدات، پاسخگو نبوده و روز به روز بر وسعت و عمق این تهدیدات افزوده شود. به نظر می‌رسد یکی از محورهای اساسی در مدیریت تهدیدات این فضا، با توجه به جهانی بودن آن و نداشتن مرزهای مشخص، به کارگیری فن دیپلماسی در مهار تهدیدات موجود در این فضا می‌باشد. بنابراین، مطالب مذکور محققین را بر آن داشت تا در مقاله حاضر نقش و چگونگی استفاده از دیپلماسی در تامین امنیت جمهوری اسلامی ایران در مواجهه با تهدیدات سایبری را بررسی نمایند. این تحقیق با توجه به ماهیت پژوهش انجام شده و اینکه به تاثیر دیپلماسی در مقابله با تهدیدات سایبری می پردازد و می توان از نتایج و یافته های آن در بهبود امنیت سایبری استفاده نمود، کاربردی است و با توجه به ارائه عوامل جدید در حوزه دیپلماسی و فضای سایبری و توسعه دانش در این زمینه، توسعه‌ای می باشد. رویکرد تحقیق آمیخته است، در

بخش کیفی ابتدا با مراجعه به پیشینه تحقیق، مبانی نظری و خبرگی، سازوکارهای دیپلماسی در مقابله با تهدیدات سایبری استخراج و سپس پرسشنامه‌ای طراحی گردید و در بخش کمی پس از انجام مراحل روایی و پایایی با مراجعه به جامعه آماری، اقدام به نمونه‌گیری گردید و با به‌کارگیری فنون آمارهای توصیفی و استنباطی تجزیه و تحلیل لازم صورت پذیرفت.

۱. کلیات

۱-۱. بیان مسئله

طی دو دهه اخیر استفاده از اینترنت و فضای سایبری اهمیت ویژه‌ای در تعاملات جهانی و زندگی روزمره انسان‌ها پیدا کرده است به نحوی که بسیاری از فعالیت‌های اقتصادی، سیاسی، فرهنگی و اجتماعی تحت تاثیر مستقیم این فضا قرار دارد. این فضا به‌طور اساسی موجب تغییر در اطلاعات و ارتباطات–دو اصل اساسی دیپلماسی– شده است.در واقع اینترنت یکی از عمیق‌ترین تغییرات را در دیپلماسی به همراه داشته است(عاملی و همکاران، ۱۳۹۵). شاخه‌ها و گرایش‌های مختلفی که در فضای سایبری وجود دارد مانند فناوری اطلاعات[1]، فناوری ارتباطات[2]، جنگ اطلاعات[3] جنگ الکترونیک[4]، شبکه های اجتماعی[5]ویژگی‌های منحصر به فردی از قبیل هزینه کم استفاده از آن، ناشناس بودن در فضای سایبر و اینترنت، عدم وابستگی به فضای جغرافیایی، در دسترس عموم قرار داشتن و ... موجب شده بسیاری از تقابلات و قدرت‌نمایی‌ها بین دولت‌ها به این فضا منتقل شود به گونه‌ای که در ادبیات جدید سیاسی ناتو و وزارت دفاع آمریکا، فضای سایبر به عنوان قلمرو پنجم نیروهای نظامی در کنار قلمروهای زمینی، هوایی، دریایی و فضایی تعریف شده است.

---

۱. Information Technology
۲. Communication Technology
۳. Information War
۴. Electronic War
۵. Social War

جایگاه خاص جمهوری اسلامی ایران در منطقه از نظر جغرافیای سیاسی و اقتصادی، پیروزی‌های جبهه مقاومت با مساعدت‌های ایران و توفیق ایران در تولید مستقل تجهیزات نظامی به ویژه موشکی از یکسو و عدم مدیریت مستقل ایران بر فضای مجازی و اینترنت، وابستگی مراکز حیاتی و مهم ایران به فضای سایبر و بالا بودن هزینه حمله نظامی به ایران باتوجه به توانمندی‌های نظامی موجود در جمهوری اسلامی، از سوی دیگر، انگیزه کافی به دشمنان این مرز و بوم می‌دهد که جنگ با ایران را به فضای سایبر منتقل کنند. نمونه این فعالیت‌ها را می‌توان به استفاده از شبکه توییتر در جریان فتنه سال ۱۳۸۸ و یا ویروس استاکس نت[۱] برای تاسیسات هسته‌ای نطنز اشاره کرد. از آنجایی که تهدیدات سایبری به ویژه از جانب نهادهای غیردولتی جزو تهدیدات نرم محسوب می‌شوند بنابراین برای مقابله با آن می‌بایستی از قدرت نرم استفاده کرد. به همین دلیل بهره‌برداری درست و به موقع از دیپلماسی در مواجهه با تهدیدات غیرسخت نظامی، راه کسب امنیت ملی و منافع ملی را هموار می‌کند. در مطالعات مختلف تاثیر فضای سایبر بر سیاست‌های دولتمردان و منافع ملی کشورهای مختلف بررسی شده است. اما دقت و مطالعه چندانی در خصوص نقش دیپلماسی در کنترل تهدیدات سایبری اعم از جنگ و حملات سایبری، جرایم سایبری، تروریسم سایبری و ... صورت نگرفته است. بنابراین به نظر می‌رسد یکی از محورهای اساسی در مدیریت تهدیدات این فضا با توجه به جهانی بودن آن و نداشتن مرزهای مشخص، به کارگیری دیپلماسی در مهار تهدیدات موجود در این فضا می‌باشد و بر همین اساس مسئله اصلی در این پژوهش این است که دیپلماسی جمهوری اسلامی ایران در کنترل تهدیدات سایبری نقش روشن و مشخصی ندارد و در این پژوهش نقش آن بررسی و تبیین می گردد.

۱-۲. اهمیت و ضرورت تحقیق

---

۱. Stuxnet

در مورد اهمیت و بعد ایجابی تحقیق می توان گفت، پرداختن به این موضـــوع اهمیت دیپلماسی را به عنوان یک ابزار مناسب برای مقابله با تهدیدات سایبری نشان داده و می‌تواند پیامدهای مثبت زیر را داشته باشد:

-همگرایی و وابستگی متقابل در حوزه سایبری با دیگر کشورها.

-مدیریت ظرفیت‌های دو یا چند جانبه در کاهش و کنترل تهدیدات سایبری.

-تقویت اراده بین‌المللی در کنترل و مقابله با تهدید تروریسم سایبری.

-اعتماد سازی و ارتقاء امنیت در فضای سایبری بین‌الملل.

– کاهش هزینه‌های دفاعی در مقابله با تهدیدات سایبری.

از نظر ضرورت و بعد سلبی نیز می توان گفت، با توجه به رویکرد جدید د شمنان در جایگزینی تهدیدات سایبری به جای تهدیدات کلا سیک و نظامی ، بدیهی ا ست که عر صه فضای سایبر برای مقابله با ایران منا سب‌ترین و در د سترس ترین راه ا ست، بنابراین غفلت از ابزارهای منا سب برای مقابله با تهدیدات سایبری می تواند تبعات زیر را به دنبال دا شته باشد:

-گسترش تهدیدات سایبری در بخش‌های مختلف و افزایش هزینه‌های دفاعی.

-کمک به سیاست منزوی سازی ایران و ایجاد ذهنیت‌های منفی در افکار عمومی جهان و عدم جلب حمایت‌های بین‌المللی در حوزه سایبری.

-اجرای سخت سیاست‌های دفاع سایبری در عرصه بین‌الملل.

- شکل‌گیری ائتلاف‌های سایبری ضد ایرانی.

–بی توجهی به تقویت و توسعه تجهیزات و سامانه‌های دفاع سایبری.

۱-۳. پیشینهٔ تحقیق

(۱) مقاله ای تحت عنوان " دیپلماســی دفاعی و نقش آن در کنترل تهدیدات ســایبری " توسـط محمدصـادق رسـتمی، در پاییز ۱۳۹۷ارائه شـده اسـت در این پژوهش، می‌توان دیپلماسـی دفاعی سـایبری را وجه ضـروری و تکمیلی فعالیت های دفاعی و راهبردی

دانست. شناسایی عوامل غیر ایمن و شکاف‌های امنیتی در زیرساخت های اصلی کشور، مطالعه تطبیقی استقرار فضای سایبر در کشورهای توسعه یافته، تعیین اولویت ها در استقرار فضای سایبر، ایجاد یک بستر ارتباطی ایمن، بومی سازی تجهیزات مورداستفاده در بخش های اصلی این فضا، توجه به تعاملات بین المللی در این زمینه، دادن آموزش های لازم به کلیه افرادی که به گونه‌ای در این فضای مجازی قرار می گیرند، همگی از نکاتی هستند که باید مورد توجه مسئولین استقرار فضای سایبر واقع شود، در غیر این صورت، افزون بر اینکه هزینه های بسیاری را بر سازمان مربوطه تحمیل می کند، موجب آسیب‌پذیری بخش‌های اصلی سازمان مربوطه به ویژه در ارتباط با زیرساخت های اصلی آن می گردد.

(۲) تحقیقی با موضوع " نقش فضای سایبری درپیشبرد دیپلماسی عمومی مدرن" توسط سید فضل اله قاضوی و همکاران در سال ۱۳۹۵ ارائه و بیان گردید در کل اینترنت و فضای سایبر با توجه به گستردگی، جذابیت، سرعت بالای انتقال پیام، امکان برقراری ارتباط با سایر شهروندان را فراهم نموده و از این ابزار می‌توان در جهت ارتقای وجهه مثبت کشور استفاده نمود. ضمن این که این فضا با استفاده از سازوکارهایی مانند گسترش ابراز نظرات سیاسی، آگاهی بخشی به جریان های سیاسی، غنی گردن رقابت‌های سیاسی و حزبی آثار مهمی بر دیپلماسی عمومی مدرن خواهد داشت.

(۳) تحقیقی با عنوان " نقش حملات سایبری بر امنیت ملی از منظر حقوق بین الملل" توسط علیرضا جهانشاهی در سال ۱۳۹۸ انجام گردید. در این تحقیق تاکید شده که جامعه بین‌الملل با توجه به وضعیت موجود به معیارهای مطرح شده درباره توسل به زور در فضای سایبر باید توجه خاصی نماید و با در نظر داشتن این معیارها، قواعد سنتی درباره توسل به زور در فضای نوین را اجرا کند. تا از این طریق از تحول خطرناک مفهوم توسل به زور در فضای سایبری جلوگیری نماید. چرا که چنین تحولی صلح جهانی را به مخاطره خواهد انداخت. ازآنجایی که مفهوم توسل به زور در فضای سایبر نسبت به فضای واقعی متفاوت

اســـت بنابراین قواعد خاص خود را دارد، پس به جا می‌باشـــد که کشـــورها با تشـــکیل کنفرانس‌های بین‌المللی قواعدی وضـــع نمایند که جلوی این نوع از تحولات را بگیرد، از طرفی سازمان ملل با ارجاع این امر به کمیسیون حقوق بین الملل به وظیفه خود در راستای حفظ صلح اقدام نماید.

در خصـــوص نوآوری مقاله می‌توان گفت در پژوهش های انجام شـــده هر کدام بخشـــی از موضـــوع پژوهش را مورد بررســـی قرار داده‌اند. اما هیچ کدام به نقش دیپلماســـی در کاهش تهدیدات سایبری اعم از جنگ و حملات سایبری، جرایم سایبری، تروریسم سایبری و ... نپرداخته اند. از این رو نوآوری پژوهش حاضـــر در این اســـت که نقش دیپلماســـی از نوع رسمی و عمومی را در کاهش تهدیدات سایبری با استفاده از نظرات متخصصان این حوزه مورد بررســـی قرار می دهد امید اســـت که بتواند خلاء پژوهشـــی موجود در این زمینه را پوشش دهد.

۱-۴. سؤال‌های تحقیق

۱-۴-۱. سوال اصلی

دیپلماسی جمهوری اسلامی ایران در کنترل تهدیدات سایبری چه نقشی دارد؟

۱-۴-۲. سوال‌های فرعی

(۱)دیپلماسی رسمی جمهوری اسلامی ایران در کنترل تهدیدات سایبری چه نقشی دارد؟

(۲)دیپلماسی عمومی جمهوری اسلامی ایران در کنترل تهدیدات سایبری چه نقشی دارد؟

۱-۵. هدف‌های تحقیق

۱-۵-۱. هدف اصلی

بررسی نقش دیپلماسی جمهوری اسلامی ایران در کنترل تهدیدات سایبری.

۱-۵-۲. هدف‌های فرعی

(۱) بررسی نقش دیپلماسی رسمی جمهوری اسلامی ایران در کنترل تهدیدات سایبری.

(۲) بررسی نقش دیپلماسی عمومی جمهوری اسلامی ایران کنترل تهدیدات سایبری.

۱-۶. روش شناسی تحقیق

پژوهش حاضر از نوع کاربردی – توسعه ای و به روش توصیفی – تحلیلی انجام گرفته ا ست. این پژوهش برای ا ستدلال و تحلیل یافته های خود رویکرد ترکیبی(کمی و کیفی) دارد. در بخش نخست این تحقیق با مراجعه به مراکز مختلف علمی و پژوهشی و استفاده از فیش برداری و مصاحبه با خبرگان به گردآوری اطلاعات لازم در رابطه با موضوع اقدام گردید.در بخش دوم یافته ها و مفروضه های بخش نخست به صورت میدانی و با ا ستفاده از پر سشنامه مورد برر سی قرار گرفت. بر این ا ساس به منظور استخراج ابعاد مسئله از دیگاه نخبگان در زمینه هدف های تحقیق تعداد ۲۳ گویه در قالب طیف ۵ گزینه ای لیکرت طراحی شد. قلمرو تحقیق از نظر زمانی سال ۱۴۰۰ و از نظر مکانی و جغرافیایی جمهوری اسلامی ایران و از نظر موضوعی شامل حوزه دیپلماسی و تهدیدات سایبری می باشد.

۱-۶-۱.جامعه آماری و حجم نمونه

جامعه آماری تحقیق شامل ا ستادان روابط بین الملل، علوم سیا سی و فضای سایبر دان شگاه های تهران و مدیران و کار شنا سان وزارت امورخارجه بوده که تعداد آن ۲۵۸ نفر تعیین گردید. برای انتخاب حجم نمونه از فرمول کوکران استفاده شد که در نتیجه آن تعداد حجم نمونه ۱۰۰ نفر به دست آمد.

۲-۶-۱.روایی و پایایی

روایی منطقی پر سشنامه‌ها از دو جنبه روایی ظاهری و محتوایی به جهت رو شن و بدون ابهام بودن گویه ها و همچنین کفایت کمیت و کیفیت آن‌ها توسط خبرگان و صاحب‌نظران و استادان دانشگاه تأیید گردید. به‌منظور بررسی روایی شاخص‌های پرسشنامه ابتدا یک نمونه ۱۵ تایی بین جامعه هدف توزیع و گردآوری گردید، پس از

دسته‌بندی داده‌ها، میزان روایی تک‌تک شاخص‌ها موردبررسی قرار گرفت همچنین برای محاسبه پایایی، از روش آلفای کرونباخ استفاده گردید

مقدار آلفای کرونباخ برای سئوال‌های حوزه دیپلماسی رسمی جمهوری اسلامی ایران در کنترل تهدیدات سایبری (۰/۷۲۵)، سئوال‌های حوزه دیپلماسی عمومی جمهوری اسلامی ایران در کنترل تهدیدات سایبری (۰/۸۸۰) و برای کل سئوال‌های (۰/۸۳۸) به دست آمده است که در همه موارد بیشتر از (۰/۷) بوده است. بنابراین پرسشنامه در حوزه‌های مختلف و در کل از ضریب اعتماد یا پایایی مطلوبی برخوردار است.

۲. ادبیات و مبانی نظری تحقیق

۱-۲.دیپلماسی

دیپلماسی را مفهومی با پیشینه‌ای به‌اندازه تاریخ ملت‌ها می‌دانند؛ اما به تایید بیشتر اندیشمندان حوزه علوم سیاسی و سیاست خارجی، تعریف دیپلماسی کار مشکلی است. نه‌تنها تعریف واحدی از «دیپلماسی» وجود ندارد بلکه وجود تعاریف متنوع و زیاد، این مفهوم را مبهم‌تر نیز نموده است. تعاریف گوناگونی با نگاه به ابعاد، اهداف و آثار مختلف دیپلماسی ارائه‌شده است، برخی دیپلماسی را به مانند مدیریت کل سیاست خارجی تبیین می‌کنند، چنانچه «هالستی»[1] می‌گوید: «هدف اصلی دیپلماسی فن مدیریت و هنر حل‌وفصل صلح‌آمیز مشکلات و اختلافات کشورها به طریق مسالمت‌آمیز است. دیپلماسی، مدیریت روابط کشورها با یکدیگر و میان کشورها با دیگر بازیگران بین‌المللی است؛ این بازیگران شامل گروه‌ها، سازمان‌ها و افرادی هستند که در کنار دولت‌ها دیپلماسی را به‌عنوان نظامی اطلاعاتی برای بیان و دفاع از منافع و اعلان تهدیدها و اولتیماتوم‌ها به کار می‌برند. درواقع دیپلماسی مجرای تماسی است برای اعلام مواضع، گردآوری اطلاعات و راضی یا قانع کردن یک کشور برای حمایت از مواضع کشوری دیگر. سیاستمداران کسانی هستند که به نمایندگی از تمامیت یک

---

[1]. Holsti

جامعه تصـمیم می‌گیرند و این عمل را با ادعای حفظ ثبات یا ایجاد تغییر در محیط (داخلی یا خارجی) و یا ساختارهای خاص روابط بین‌المللی انجام می‌دهند.» (هالستی، ۱۳۷۳: ۲۱۲). اما شـاید بتوان بهترین تعریف از دیپلماسـی را از جان بیلیس[۱] و اسـتیو اسـمیت[۲] که در کتاب «جهانی‌شـدن سـیاسـت: روابط بین‌الملل در عصـر نوین» بیان کرده‌اند دانسـت: «دیپلماسـی در سـیاسـت جهانی عبارت اسـت از فرایند ارتباط بین بازیگران بین‌المللی که قصد دارند از طریق مذاکره، تعارض را بدون جنگ حل‌وفصل نمایند. این فرآیند در طول قرن‌ها پالایش و نهادینه شده و به صورت حرفه‌ای در آمده است.» (بیلیس و اسمیت، ۱۳۸۳: ۷۱۵).

۲-۲.اهمیت دیپلماسی

دیپلماسـی با مدیریت مناسـبات میان دولت‌ها و روابط دولت‌ها با سـایر بازیگران سروکار دارد. از دیدگاه دولت، دیپلماسی با رایزنی، طراحی و اجرای سیاست خارجی ارتباط دارد. بدین لحاظ دیپلماسی وسیله‌ای است که دولت‌ها به کمک آن و از طریق نمایندگان رسـمی و غیررسـمی خود و نیز سـایر بازیگران، با اسـتفاده از مکاتبات، مذاکرات خصوصی، تبادل دیدگاه‌ها، اعمال‌نفوذ، ملاقات، تهدیدها و دیگر فعالیت‌های مربوط به بیان، هماهنگ سازی و تأمین منافع ویژه و گسترده‌تر می‌پردازد. هرچند اغلب متصور می‌شد دیپلماسی با فعالیت صلح‌آمیز سروکار دارد، ممکن است برای نمونه در بسـتر جنگ یا تعارض مسـلحانه نیز تحقق یابد و یا برای هماهنگ‌سـازی برخی فعالیت‌های خشونت‌آمیز موردا ستفاده قرار گیرد. در حقیقت مشخص شدن مرز میان فعالیت دیپلماتیک و خشـونت ازجمله تحولات برجسـته‌ای اسـت که وجه مشـخصـه دیپلماسـی نوین به شـمار می‌رود. این نکته به شـکل کلی‌تر در مورد محتوای در حال گسترش دیپلماسی نیز صادق است. از یک جنبه تغییراتی که در شکل اساسی دیپلماسی حاصـل به وجود آمده در قالب اصـطلاحاتی چون دیپلماسـی دلار، دیپلماسـی نفت،

---

۱. John Bayliss
۲. Steve Smith

دیپلماسی منابع و دیپلماسی اتمی منعکس گردیده است. با اطمینان می توان گفت امروزه دیپلماسی از مفهوم سیاسی راهبردی محدودی که زمانی برای آن حمل می شد، فراتر می‌رود. از طرف دیگر مناسب نیست که با قایل شدن معنایی محدود یا رسمی برای دیپلماسی، آن را تنها متعلق به وزرای خارجه و کارکنان ادارات دیپلماتیک بدانیم. چه‌بسا طیف وسیعی از کارکنان دیگر وزارتخانه‌ها یا مؤسسات یا همتایان خارجی خود به اجرای دیپلماسی در معنای فنی کلمه بپردازند. همچنین ممکن است مقامات سازمان‌های مختلف همچون صندوق بین‌المللی پول (IMF) و دبیرخانه سازمان ملل متحد باهم یا شرکت‌های خارجی و یک حکومت میزبان، در حال اجرای دیپلماسی باشند.(بارستون، ۱۳۷۹: ۲۶-۲۱).

۳-۲.انواع دیپلماسی

۱-۳-۲.دیپلماسی رسمی:

ویژگی دیپلماسی رسمی حاکمیت دیدگاه دولت محور و تاکید بر فرآیندهای بین دولتی دیپلماتیک بوده است. براین اساس دیپلماسی رسمی در دیدگاه نخبگان این حوزه، تعاریف مختلفی پیدا کرده است مانند :

الف) نیکلسون:[۱] مدیریت روابط بین دولت‌های مستقل از طریق فرایندهای مذاکره.

ب) ارنست ساتو:[۲] کاربرد هوش و مهارت برای هدایت روابط رسمی بین دولت‌هایی با حاکمیت مستقل.

ج) المرپلیشکه:[۳] فرآیند سیاسی که از طریق آن نهادهای سیاسی(به ویژه دولت‌ها) به برقراری و حفظ روابط رسمی جهت تعقیب هدف‌ها، منافع و سیاست‌های واقعی خود در محیط بین المللی اقدام می‌کنند. (عباسی و طالعی، ۱۳۹۷ : ۱۲)

---

۱. Nicholson
۲. Ernest Satow
۳. Elmer Plischke

در عصـــر اطلاعات دیپلماســـی رســـمی میان دولت ها همچنان از اهمیت و جایگاه ویژه‌ای در نظام بین الملل برخوردار اســـت. امروزه در نظام بین الملل دولت محوری، برقراری روابط سیاسی میان دولت ها و تاسیس سفارتخانه ها و اعزام سفرا و کارداران، زمینه ساز برقراری روابط متقابل در عر صه های اقتصادی، فرهنگی و نظامی محسوب می شود. همچنین سطح روابط سیا سی میان دو کشور و میزان ملاقات ها و مراودات سیا سی میان نمایندگان آنها، می تواند نشان دهنده میزان علاقه و نوع روابط دو جانبه باشـــد. هدف دیپلماســـی رســـمی، نزدیکی ملل به یکدیگر و برقراری صـــلح و آرامش بین‌المللی است. دیپلماسی درصدد است تا ضمن ایجاد ارتباط دوستانه میان کشورها، تمام امکانات مادی و معنوی آن ها را در تداوم و غنی تر ســـاختن این روابط فراهم آورد. تلاش دیپلماســـی رســـمی همواره حفظ منافع ملی از طریق روش های مســـالمت آمیز بوده است که این هدف در طول ادوار مختلف تاریخی، شیوه‌های گوناگونی را در مقابل دیپلماسی قرار داده است.(ستوده آرانی و علویان، ۱۳۹۱: ۱۵۸-۱۵۶)

برخی از ویژگی‌های دیپلما سی ر سمی عبارتند از: حاکمیت فرهنگ سلسله مراتبی، سری بودن، شفاف بودن، انحصار طلبی، فقدان پا سخگویی، محافظت از اطلاعات و دانش. (عباسی و طالعی، ۱۳۹۷ : ۱۲)

۲-۳-۲.دیپلماسی عمومی:

عبارت دیپلماسی عمومی در حوزه مطالعات روابط بین الملل، اصطلاحی است که در دهه ۱۹۶۰ برای توصـیف جنبه های جدید دیپلماســی بین المللی رایج شـد. اصـطلاح دیپلما سی عمومی نخستین بار در سال ۱۹۶۵ در آمریکا تو سط ادموند گولیون[۱] رئیس مدرسه حقوق و دیپلما سی فلچر[۲] در دانشگاه تافنز[۳] به کار گرفته شد و عبارت است از: « ارتباطات معطوف به منافع ملی یک کشـــور از طریق ارتباط با مردم خارج از مرزهای

۱. Edmund Gullion
۲. Fletcher School of Law and Diplomacy
۳. Tufts University.

جغرافیایی». با این تعریف مسائلی از قبیل اعزام دانشجو به خارج، پذیرش بورس های تحصیلی، خبرنگاران اعزامی، فرایند ارتباط میان فرهنگی، برگزاری انواع جشنواره های هنری، همایش ها و سمینارهای فرهنگی و پخش برنامه های صوتی و تصویری و حتی ایجاد سایت های اینترنتی، همه و همه در حوزه دیپلماسی عمومی قابل بحث است.(Wolf, 2004: 3)

۱-۲-۳-۲.انواع دیپلماسی عمومی:

۱-دیپلماسی فرهنگی : منظور از دیپلماسی فرهنگی، فرایندی است که از طریق آن دولت‌ها می‌توانند با توسل به ظرفیت‌ها، امکانات، توانمندی‌ها و ویژگی‌های فرهنگی خود بر افکار عمومی و رفتار سایر کشورها اثر بگذارند. در واقع، دیپلماسی فرهنگی ابزاری است که یک دولت با به معرض گذاشتن نمادهای فرهنگی، جذابیت‌هایی را در افکار عمومی مردم سایر کشورها ایجاد می‌کند تا از طریق نفوذ ناشی از آن، بر رفتار و سیاست‌های دولت بیگانه اثر گذارد(اژدری و همکاران، ۱۳۹۶ : ۲۸).

۲-دیپلماسی رسانه ای: دولت‌ها از دیپلماسی رسانه ای نیز به عنوان ابزاری مؤثر در شکل دهی افکار و نظرات مردم سایر کشورها نسبت به وقایع و تحولات استفاده می‌کنند؛ علاوه بر این، رسانه‌ها چنین امکانی را به وجود می آورند تا دولت‌ها نظرات و دیدگاه‌های خود را در صحنه ی بین‌الملل بیان کنند. فعالیت‌های رسانه ای در قالب دیپلماسی رسانه ای به دنبال جهت دهی افکار عمومی و توجیه تصمیم گیری‌ها در حوزه سیاست خارجی است. در واقع هدف دیپلماسی رسانه ای ایجاد تصویر مثبت و مطلوب از اهداف و سیاست‌های دولت‌ها در افکار عمومی است(اژدری و همکاران، ۱۳۹۶ : ۲۸).

۳-دیپلما سی مبادله ای: در کنار دیپلما سی فرهنگی و ر سانه ای، دیپلما سی مبادله ای به دنبال دستیابی اهداف دراز مدت است و منظور از آن، مجموعه ای از فعالیت‌ها و اقدامات فراملی که به دنبال انتقال فرهنگ ارزش‌ها و باورها به سایر سرزمین‌ها است.

هر چند گستره دیپلماسی مبادله ای، وسیع به نظر می‌رسد، ولی بیشتر شامل فعالیت‌های دانشگاهی می‌گردد. مبادله ی استاد، اعطای بورس‌های دانشجویی، ارائه فرصت‌های مطالعاتی و تحقیقاتی، برگزاری تور های علمی و کار گاه های آموزشی از جمله فعالیت‌هایی هستند که در قالب دیپلما سی مبادله ای، مطرح می شوند. در واقع این نوع دیپلماسی یکی از شیوه‌های مهم برقراری ارتباط با نخبگان سایر کشورها است(اژدری و همکاران، ۱۳۹۶ : ۲۸).

۴-دیپلماسی سایبری: دیپلماسی سایبری را شاید بتوان نوعی از دیپلماسی عمومی تفسیر کرد که شاکله و موجودیت آن از طریق اینترنت و فضای مجازی به وجود آمده است. در واقع با رشد سریع فناوری های ارتباطی کابلی(تلویزیون ها)، ارتباطات بی سیم(رادیو) و در نهایت ظهور فضای مجازی و توسعه ارتباطات و امکان برقراری ارتباط و تبادل اطلاعات بین مردم جای جای جهان در مدت زمان چند ثانیه ای، انفجاری در فضای دیپلماسی عمومی پدیدار شد و دیپلماسی سایبری به وجود آمد. به عبارت دیگر این دیپلما سی را می‌توان اعمال امور دیپلماتیک از طریق کانال سایبری در نظر گرفت، که زمینه تعامل با میلیون‌ها شهروند خارجی از کشورهای دیگر را فراهم می سازد. از آنجا که دیپلما سی سایبری زیر شاخه‌ای از دیپلما سی عمومی ا ست، در این دیپلماسی نیز بر خلاف دیپلماسی رسمی که طرفین ارتباط دو دولت و یا هیأت دیپلماتیک هستند، در یکسو یک دولت و در طرف دیگر مردم کشور یا کشورهای دیگر قرار دارند. این ارتباط به جای اینکه از طریق ارسال نماینده و نامه نگاری رسمی صورت گیرد از طریق کانال‌های مجازی و فضای سایبر صورت می‌پذیرد.

همین شیوه ارتباط گیری و تأثیرپذیری باعث شده است که در سال‌های اخیر در سیاست بین المللی، دیپلماسی سایبری تبدیل به یک کانال دیپلماتیک برای تعامل با توده های مردمی جوامع مختلف گردد. هدف از این دیپلماسی می‌تواند تغییر در فرهنگ جوامع دیگر، همسو کردن آنها با سیاست‌ها و فعالیت‌های یک دولت خاص، بر پا کردن

جنبش اعترا ضی از طریق شبکه‌های اجتماعی، بسیج گروه‌های برانداز از طریق فضای سایبر، جمع آوری اطلاعات در مورد صف آرایی نیروهای اجتماعی- سیاسی طرف مقابل و ... باشد(کولایی و همکاران، ۱۳۹۲: ۵۱).

۴-۲. فضای سایبری

در سند راهبردی امنیت فضای تبادل اطلاعات(افتا)، به فضای سایبری، فضای تبادل اطلاعات گفته شده و به صورت زیر تعریف می شود:

« در عصر اطلاعات شاهد شکل گیری فضایی هستیم که در آن فعالیت های گوناگونی از قبیل اطلاع رسانی، داده ورزی، ارائه خدمات، مدیریت و کنترل و ارتباطات، از طریق سازوکارهای الکترونیکی و مجازی انجام می پذیرد. از این فضا با نام فضای تبادل اطلاعات (فتا) یاد می شود»(حقی، ۱۳۹۸: ۲۸۱).

کمیسیون اروپایی فضای سایبر را یک فضای مجازی دانسته که در آن داده‌های الکترونیکی رایانه های شخصی در سرتاسر جهان منتشر می شوند. فضای سایبری از مولفه های زیر تشکیل شده است (Shaw,2010:5):

۱-مؤلفه سیستمی: شامل جنبه‌های فنی، زیرساختی و معماری فضای سایبری است. این مؤلفه شامل سخت‌افزار و کاربردهای نرم‌افزاری است که کاربران برای ذخیره‌سازی، انتقال و پردازش اطلاعات در فضای سایبری به آن‌ها اتکا دارند.

۲- مؤلفه محتوا و کاربرد: به محتوا و اطلاعات ارجاع دارد که در فضای سایبری وجود داشته و ابزارهایی که برای دستیابی و پردازش این اطلاعات مورداستفاده قرار می‌گیرد. مؤلفه محتوا و کاربرد به مؤلفه سیستمی اتکا دارد و کاربردها را در راستای مدیریت و اشتراک اطلاعات برای کاربران فراهم می‌کند.

۳-مؤلفه انسانی و اجتماعی: به ارتباطات و تعامل‌ها بین انسان‌ها در فضای سایبری و به اطلاعاتی که به اشتراک می‌گذارند ارجاع دارد. دو مؤلفه قبلی فضای سایبری،

امکان رشد مؤلفه انسانی و اجتماعی را با تسهیل ایجاد انجمن‌ها در فضای سایبری برای دسترسی و اشتراک اطلاعات مابین کاربران را فراهم می‌نمایند.

۴- مؤلفه حاکمیتی: همه مؤلفه‌های قبلی فضای سایبری را تحت تأثیر قرار می‌دهند. این مؤلفه مشخصات فناوری (مؤلفه سیستمی)، استانداردسازی برای قالب‌بندی و تبادل داده‌ها (مؤلفه محتوایی و کاربردی) و چارچوب‌های قانونی کشورها برای کاربران فضای سایبری (مؤلفه انسانی و اجتماعی) را تحت تأثیر قرار می‌دهد. سازوکارهای مدیریتی اینترنت به شدت پیچیده بوده و نیازمند هزینه نمودن منابع قابل‌توجه در محاکم مختلف برای نیل به اهداف می باشند. جدول زیر این مؤلفه‌ها را باهم نشان می‌دهد:

جدول شماره ۱: مؤلفه‌های کلیدی فضای سایبر(Shaw,2010:۵)

مؤلفه حاکمیتی دربردارنده همه جنبه‌های فضای سایبر		
مؤلفه انسانی و اجتماعی مخابرات و تعامل‌های بین افراد و اطلاعات	مؤلفه محتوا و کاربرد پایگاه اطلاعاتی و سازوکارهای های دسترسی و پردازش اطلاعات	مؤلفه سیستمی شالوده فنی، زیرساخت و معماری

امروزه فعالیت مقامات و سیاسیون در فضای سایبری موجب پیشبرد اهداف سیاست خارجی کشورها شده است. وب سایت‌ها از محبوب ترین ابزارهای الکترونیکی مورد استفاده در فضای سایبری می‌باشند، امروزه اغلب وزارتخانه امورخارجه دارای وب سایت رسمی برای ارتباطات عمومی می‌باشد، پس از وب سایت ها، توئیتر و فیس بوک در حال حاضر از محبوب ترین ابزارهای الکترونیکی هستند که توسط وزارتخانه های امورخارجه در سرتاسر جهان استفاده می‌شوند. از دیگر رسانه های اجتماعی مورد

اســـتفاده در وزارتخانه های امور خارجه می‌توان از یوتیوب[۱] فلیکر[۲] لینکدین[۳] پینترست[۴] و اینستاگرام[۵] نام برد.(کولایی و همکاران، ۱۳۹۲: ۲۵)

۵-۲. تهدید سایبری

تهدید سایبری پدیده‌ای جدید است که در دهه‌های اخیر، همزمان با تحول فن‌آوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسر جهان ظهور پیدا کرده است، به گونه ای که امروزه چالش تهدیدهای سایبری، هم مهم و هم پیچیده به نظر می رســـد. این اهمیت و پیچیدگی ناشـــی از ماهیت جدید تهدیدهای سایبری و ویژگی‌ها و نمودهای منحصر به فردی است که شناخت از آن را بسیار مهم و ضروری می نماید.

در همایشی که در دوم مارس ۲۰۱۰ از سوی موسسه بین المللی CACI و موسسه مطالعاتی نیروی دریایی ایالات متحده با عنوان "تهدیدهای سایبری امنیت ملی و مقابله با چالش های پیش روی زنجیره عرضـــه جهانی" برگزار شـــد، تهدیدهای ســـایبری به صورت "وقایعی که به صورت طبیعی و یا توسط انسان بصورت عمدی یا غیرعمدی برفضـای مجازی تاثیرگذار باشـد یا حوادثی که از طریق فضـای مجازی عمل کند یا به نحوی به آن مرتبط باشد" تعریف شد (خلیلی پور، نورعلیوند، ۱۳۹۱ : ۱۶۹).

۶-۲. ویژگی‌های تهدید سایبری

تهدیدهای ســایبری ویژگی‌های منحصـر به فردی دارند .از یک ســو، این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می شوند و از سوی دیگر، هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبر

---

۱. YouTube
۲. Flickr
۳. LinkedIn
۴. pinterest
۵. Instagram

موجب شده بازیگران زیادی به این عرصه وارد شوند. مهم‌ترین ویژگی‌های تهدیدهای سایبری در مؤلفه های زیر خلاصه می‌شود:

۱- تعدد بازیگران در فضای سایبری:

هزینه کم فن آوری رایانه ای، اتصال گسترده به اینترنت و سهولت ایجاد یا به دست آوردن نرم افزارهای مخرب به این معنا ست که تقریباً هر کسی می تواند به این فضا وارد شود .این بازیگران شامل افراد، گروه های سازمان یافته جنایی ، گروه های تروریستی، شرکت های خصوصی و دولت- ملت هستند.

۲- هزینه کم ورود، صرف زمان کم و سرعت بالای اقدام:

هر فرد برای انجام حمله سایبری تنها به یک رایانه، یک ارتباط اینترنتی و دانش فنی محدود در زمینه فضای سایبری نیاز دارد .در نتیجه، فضای سایبری شرایطی را فراهم کرده است که با هزینه پایین می‌توان اقدامات خطرناکی را در مدت زمان کم و با سرعت بالایی انجام داد .البته انجام حملات پیچیده تر سایبری نیازمند صرف وقت بیشتر و هزینه‌های بالاتری است.

۳- ناشناس ماندن بازیگران و عدم قابلیت ردیابی:

اینترنت به عنوان سیستم نامتمرکز طراحی شده و کاربران آن، اغلب شناخته شده نیستند .همین ناشناختگی موجب می شود هیچ اثری از برخی از حمله های سایبری باقی نماند .افراد فعال در عرصه اینترنت می توانند از اقصی نقاط دنیا، بدون هشدار و در عرض چند ثانیه و بدون آنکه اثر یا نامی از خود بر جای بگذارند، اهداف دیجیتالی را مورد هدف قرار دهند .

۴- تأثیرگذاری شگرف:

ماهیت خاص فضای سایبری شرایطی را به وجود آورده است که بروز هر اختلال یا وقفه می تواند تأثیرات و پیامدهای به مراتب بیشتری از حادثه اولیه در پی داشته باشد. وقوع حمله های سایبری و در نتیجه آن، بروز اختلال در شبکه‌ها می تواند موجب ایجاد خسارت به اموال، زمان، محصولات و تولیدات، اعتبار، اطلاعات حساس و حتی

از دست دادن جان انسان ها شود، زیرا در این گونه مواقع، زیرساخت ها و سامانه های مهم دچار آسیب می شوند .

۵- کمرنگ شدن نقش جغرافیا:

فضای سایبری سرعت انتقال به سراسر جهان را در لحظه کوتاهی فراهم کرده است. بنابراین، تهدیدکنندگان قادر به فراتررفتن از محدوده جغرافیایی خود و رسیدن به اهداف کلیدی شان هستند.

۶- ساختار فضای اینترنت:

اینترنت، دامنه مشترک و یکپارچه است. استفاده از این فضا توسط شهروندان، شرکت ها و دولت ها به شیوه ای است که جداسازی آنها بسیار دشوار است. توانایی محدود برای جداکردن بازیگران و فعالیت های آنها، پاسخ مناسب به آنها از سوی دیگر، ساختار تهدید را بسیار دشوارتر کرده است. اینترنت، دولت ها و شرکت های خصوصی را با عدم اطمینان در قبال خطرات فضای اینترنتی مواجه کرده است. این عدم قطعیت ناشی از پیچیدگی‌ها و فن آوری در حال تکامل برای پشتیبانی از سیستم‌های حیاتی است. بازیگران دولتی و غیردولتی از قدرت سایبری استفاده می‌کنند تا به اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مالی خود در فضای سایبری و دنیای واقعی دست یابند. این اهداف در فضای سایبری از شیوه های متفاوتی حاصل می‌شوند که مهم‌ترین آنها عبارتند از:جنگ سایبری، تروریسم سایبری، جرایم سایبری، جاسوسی سایبری و اختلال سایبری. (خلیلی پور، نورعلیوند، ۱۳۹۱: ۴۸)

۷-۲.انواع تهدید سایبری:

۱-جنگ سایبری

جنگ سایبری عبارت است از "اقدامات آفندی غیر متحرکی که به منظور کسب برتری اطلاعاتی از طریق تحت تاثیر قراردادن سامانه اطلاعاتی و شبکه های رایانه ای دشمن اتخاذ می گردند." بر اساس این تعریف به نظر می رسد که جنگ سایبری زیر

شاخه ای از جنگ اطلاعاتی بوده و شامل اقداماتی است که در فضای سایبری در تقابل با فضا یا دنیای واقعی صورت می پذیرد. بستر جنگ سایبری عبارت است از هر سامانه واقعیت مجازی که دربرگیرنده مجموعه ای از رایانه ها و شـــبکه ها باشـــد. یکی از شـاخص ترین محیط های جنگ سـایبری اینترنت و شـبکه های (نظامی یا غیر نظامی) مرتبط می باشـد که به نحوی اطلاعات را به اشـتراک می گذارند. با درنظر گرفتن جنبه نظامی جنگ سایبری می توان آنرا جنگی در حوزه اینترنت قلمداد نمود.(توکل، ۱۳۸۵ : ۱۷)

۲-تروریسم سایبری:

تروریسم سایبر، حمله یا تهدید به حمله به شبکه های رایانه‌ای و اطلاعات ذخیره شده در آنها به قصد ایجاد رعب و وحشت یا وادار کردن دشمن به انجام یک کار است. سه نوع از این تروریسم نرم افزاری عبارتند از :

-حمله به نتایج حاصـل از اکتشـافات نظامی، ارتباطات، فرماندهی و کنترل و جنبه های مختلف اطلاعات محرمانه.

-حمله به حلقه های مهم برقراری ارتباط در جامعه از جمله صدا، تصویر، انتقال داده ها و سامانه های تلفنی.

-بکارگیری رادیو، تلویزیون و سایر ابزارهای مشابه برای حمله یا تحت تاثیر قراردادن دیدگاه های افراد نظامی یا جامعه، سیاست‌مداران و رهبران اقتصادی. (اسکندری، ۱۳۹۱ : ۳۵)

۳-جرایم سایبری

در تعریف محدود، اگر رایانه صرفاً ابزار و وسیله ارتکاب جرم باشد، نمی توان آنرا جرم در زمره جرایم رایانه ای قلمداد کرد. اما در تعریف گسـترده هر فعل یا ترک فعلی که از طریق یا به کمک سـیسـتم های رایانه ای رخ می‌دهند جرم رایانه ای قلمداد می شـود، که از این دیدگاه به سـه دسـته تقسـیم می‌شـوند: دسـته اول از جرایم رایانه و

تجهیزات رایانه ای، موضوع جرایم سنتی مثل سرقت، تخریب تجهیزات و ... هستند. در دسته دوم رایانه و سیله و ابزار ارتکاب جرم است و از آن برای جعل مدرک، گواهینامه و ... استفاده می شود. در دسته سوم جرایم محض، جرایمی مانند هک یا ویروسی کردن که صرفاً در فضای سایبر (مجازی) اتفاق می‌افتد. (رستمی ، ۱۳۹۷: ۳۸)

درقوانین جمهوری اسلامی ایران، مصادیق جرائم سایبری به شرح زیر گنجانده شده است:

-جرم‌هایی که علیه محرمانگی انجام داده می‌شود. مثل: دسترسی غیرمجاز (هکرها، کراکرها و..) ،شنود غیر مجاز، جاسوسی در فضای مجازی.

-جرم‌هایی که علیه صحت و درستی داده‌ها می‌باشد. مثل: جعل رایانه، ایجاد اخلال در داده ها و اطلاعات و یا تخریب داده‌ها.

-کلاهبرداری و یا انجام سرقت در فضای مجازی با رایانه.

-اعمال منافی عفت و اخلاق مثل ایجاد محتویات مستهجن و انتشار آنها.

-نشر اکاذیب.

۴-جاسوسی سایبری

جاسوسی سایبری از رایانه ها و سیستم های مربوط به آن استفاده می کند تا اطلاعات محرمانه را جمع آوری کند. برخلاف جرایم سایبری که مسائل مالی و اقتصادی محرک اصلی مجرمان است، جاسوسی سایبری بیشتر تأثیرات سیاسی داشته و جامعه را تهدید می کند. محرک های اصلی جاسوسی سایبری متفاوت است، اما شامل کسب منافع نظامی، صنعتی، سیاسی و فنی است. جاسوسان سایبری اطلاعات دزدیده شده را با اهداف مختلف مورد استفاده قرار می‌دهند که برخی از آنها عبارتند از تهدید، اخاذی و مختل کردن اقدامات رقبای سیاسی. (خلیلی پور، نورعلی وند : ۱۳۹۱: ۶۹)

جاسوسی سایبری یکی از طرق جاسوسی، دستکاری یا بهره برداری غیرقانونی از اطلاعات محسوب می شود. این قسم از جاسوسی به دسترسی غیرقانونی یا دزدی

اطلاعات محرمانه ذخیره شده در فرمت‌های دیجیتال یا رایانه ها و شبکه‌های اینترنت گفته می‌شود. دولت‌ها، قوای نظامی، شرکتها و مؤسسات دولتی و خصوصی و حتی در مواردی اشخاص خصوصی نیز میتوانند هدف جاسوسی سایبری واقع شوند. جاسوس از شبکه‌های رایانه برای دسترسی غیرقانونی یا دزدی اطلاعات محرمانه و حساس یا به عبارت دیگر، حفاظت شده استفاده می‌کند. این اطلاعات حساس می‌تواند مشتمل بر مالکیت معنوی، تحقیقات و داده‌های مربوط به توسعه پروژه ها یا هر اطلاعات دیگری شود که برای دارنده اطلاعات مهم و حیاتی است. بنابراین از طریق جاسوسی می‌توان به مهم و طبقه بندی شده‌ای از یا مکان دور به صورت پنهانی، کاملا ارزان و احتمالا در مقیاس وسیع نفوذ کرد. (شهبازی و آقاجانی، ۱۳۹۹ : ۱۴۹۰)

۵-آشفتگی سایبری

آشفتگی سایبری از رایانه ها و سیستم های مربوط به آن استفاده می کند تا هدف مورد نظر خود را ناقص کرده، تحت تأثیر قرار داده و یا آن را آزار دهد. اهداف سیاسی و ایدئولوژیکی در پشت این اقدامات وجود دارد و افراد از ابزاری استفاده می کنند که غیرقانونی هستند.

برخلاف جرایم سایبری و جاسوسی سایبری که هدف شان دزدی یا تغییر اطلاعات است، آشفتگی سایبری سعی در مجازات یا تأثیرگذاری بر عقاید و رفتار هدف های خود دارد. ممکن است طی این مرحله، اطلاعات زیادی دزدیده شده و یا تغییر یابد و یا هزینه های مادی فراوانی به شبکه های هدف وارد شود. اما قصد و نیت اصلی آشفتگی سایبری، آسیب رساندن است. بازیگران دولتی و غیردولتی می توانند از این ابزار استفاده کنند، ولی تا کنون آشفتگی سایبری توسط افرادی انجام شده که با نام فعالان عرصه هک شناخته شده اند. (خلیلی پور، نورعلی وند : ۱۳۹۱: ۷۱)

۳. یافته های تحقیق و تجزیه وتحلیل آن ها

سئوال فرعی اول تحقیق عبارت بود از: « دیپلماسی رسمی جمهوری اسلامی ایران در کنترل تهدیدات سایبری چه نقشی دارد؟ » برای پاسخ به این سئوال ۱۱ گویه از مصاحبه با خبرگان احصا شد که نتایج آن به شرح جدول شماره ۳ است.

جدول شماره۳ : نقش دیپلماسی رسمی جمهوری اسلامی ایران در کنترل تهدیدات سایبری

ردیف	گویه های پرسشنامه	فراوانی و درصد	دیدگاه نمونه آماری					میانگین (درصد)
			درجه های ارزیابی					
	نقش دیپلماسی رسمی جمهوری اسلامی ایران در کنترل تهدیدات سایبری		خیلی زیاد	زیاد	متوسط	کم	خیلی کم	
۱	روابط سیاسی متقابل و رضایت بخش جمهوری اسلامی ایران با کشورهای منطقه و جهان چه میزان در کنترل تهدیدات سایبری نقش دارد؟	فراوانی	۲	٦	۲۲	٤۳	۲۷	٦,۲۷
		درصد	۲	٦	۲۲	٤۳	۲۷	
۲	انعقاد قراردادها و معاهدات سایبری دو جانبه و چند جانبه جمهوری اسلامی ایران با کشورها چه میزان درکنترل تهدیدات سایبری نقش دارد؟	فراوانی	۲۸	٦۱	۱۱	۰	۰	۷,۲۲
		درصد	۲۸	٦۱	۱۱	۰	۰	
۳	بهره گیری جمهوری اسلامی ایران از قوانین و حقوق بین الملل چه میزان در کنترل تهدیدات سایبری نقش دارد؟	فراوانی	۲	۷	۳۳	٤۷	۱۱	٥,۲۳
		درصد	۲	۷	۳۳	٤۷	۱۱	
٤	سفارتخانه ها و کنسولگری های جمهوری اسلامی ایران در کشورها چه میزان در کنترل تهدیدات سایبری نقش دارد؟	فراوانی	٤	٥۹	۲٦	۸	۳	٤,۹۷
		درصد	٤	٥۹	۲٦	۸	۳	
٥	حضور فعال جمهوری اسلامی ایران در نهادهای بین المللی از جمله	فراوانی	٦	٥٤	۳۲	۷	۱	٥,۰۷
		درصد	٦	٥٤	۳۲	۷	۱	

	سازمان ملل متحد چه میزان در کنترل تهدیدات سایبری نقش دارد؟							
٦	بهره گیری جمهوری اسلامی ایران از ظرفیت سازمان های منطقه ای چه میزان در کنترل تهدیدات سایبری نقش دارد؟	فراوانی	٥	٥٦	٢٨	٦	٥	٤,٩٥
		درصد	٥	٥٦	٢٨	٦	٥	
٧	همکاری سایبری جمهوری اسلامی ایران با کشورها چه میزان در کنترل تهدیدات سایبری نقش دارد؟	فراوانی	٣٨	٤٢	١٩	١	٠	٧,١٤
		درصد	٣٨	٤٢	١٩	١	٠	
٨	همکاری های اطلاعاتی و امنیتی جمهوری اسلامی ایران با کشورها چه میزان در کنترل تهدیدات سایبری نقش دارد؟	فراوانی	٤٩	٣٤	١٢	٣	٢	٧,٦٥
		درصد	٤٩	٣٤	١٢	٣	٢	
٩	رویکرد تعاملی و تنش زدایی با کشورهای منطقه و جهان چه میزان در کنترل تهدیدات سایبری نقش دارد؟	فراوانی	٥٥	٢٣	١٣	٥	٤	٧,٦١
		درصد	٥٥	٢٣	١٣	٥	٤	
١٠	همگرایی جمهوری اسلامی ایران با کشورهای منطقه چه میزان در کنترل تهدیدات سایبری نقش دارد؟	فراوانی	٥	٥٧	٢٦	٩	٣	٥,٠١
		درصد	٥	٥٧	٢٦	٩	٣	
١١	استفاده از قدرت نظامی و دفاعی جمهوری اسلامی ایران به عنوان یک ابزار دیپماسی (دیپلماسی دفاعی) در کنترل تهدیدات سایبری چه نقشی دارد؟	فراوانی	٤	٥٦	٢٧	٩	٤	٤,٨٩
		درصد	٤	٥٦	٢٧	٩	٤	

در تحلیل گویه های مربوط به سئوال فرعی اول یافته ها نشان می دهد؛ « همکاری‌های اطلاعاتی و امنیتی جمهوری اسلامی ایران با کشورها » با میانگین ۷/۶۵ و « استفاده از قدرت نظامی و دفاعی جمهوری اسلامی ایران به عنوان یک ابزار دیپماسی(دیپلماسی دفاعی)» با میانگین ۴/۸۹ به ترتیب بیشترین و کمترین میانگین

رتبه‌ای را به خود اختصاص داده‌اند. سایر ارزش‌های مربوط به میانگین رتبه‌ای متغیرها در جدول شماره ۳ درج شده است.

با توجه به این که در آزمون متغیرهای دیپلما سی ر سمی جمهوری ا سلامی ایران در کنترل تهدیدات سایبری، ارزش خی‌دوی م شاهده شده (۱۳۵/۸۴۰) در درجه آزادی ۳ معنی‌دار است، در نتیجه استنباط می‌شود که بین فراوانی‌های مشاهده شده تفاوت معنی‌داری وجود دارد. یعنی فر ضیه H1 پذیرفته می شود و فر ضیه مقابل آن یعنی H0 رد می‌گردد.

سئوال فرعی دوم تحقیق عبارت بود از: « دیپلما سی عمومی جمهوری اسلامی ایران در کنترل تهدیدات سایبری چه نقشی دارد؟ » برای پاسخ به این سئوال ۱۲ گویه از مصاحبه با خبرگان احصا شد که نتایج آن به شرح جدول شماره ۵ است.

جدول شماره ۴ : نقش دیپلماسی عمومی جمهوری اسلامی ایران در کنترل تهدیدات سایبری

ردیف	گویه های پرسشنامه	فراوانی و درصد	دیدگاه نمونه آماری					میانگین (درصد)
			درجه های ارزیابی					
	نقش دیپلماسی عمومی جمهوری اسلامی ایران در کنترل تهدیدات سایبری		خیلی زیاد	زیاد	متوسط	کم	خیلی کم	
۱	همکاری های علمی جمهوری اسلامی ایران در حوزه سایبری با خارج از کشور چه میزان در کنترل تهدیدات سایبری نقش دارد؟	فراوانی	۷	۵۰	۲۶	۱۵	۲	۵,۶۷
		درصد	۷	۵۰	۲۶	۱۵	۲	
۲	رسانه های شنیداری برون مرزی جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟	فراوانی	۷	۵۶	۲۰	۱۵	۲	۶,۰۲
		درصد	۷	۵۶	۲۰	۱۵	۲	
۳	رسانه های دیداری برون مرزی جمهوری اسلامی ایران چه میزان در کنترل	فراوانی	۵	۵۲	۳۲	۹	۲	۵,۷۳
		درصد	۵	۵۲	۳۲	۹	۲	

							تهدیدات سایبری نقش دارد؟
٦,٠١	۳	۱۳	۲۲	٥۲	۱۰	فراوانی	٤ تبادلات علمی مانند بورس کردن دانشجویان دیگر کشورها توسط جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟
	۳	۱۳	۲۲	٥۲	۱۰	درصد	
۷,۹۰	٤	٥	۱۱	٤۷	۳۳	فراوانی	٥ استفاده از ظرفیت شبکه های اجتماعی توسط جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟
	٤	٥	۱۱	٤۷	۳۳	درصد	
۹,۲۱	۰	۰	۲	٥۸	٤۰	فراوانی	٦ استفاده از ظرفیت پیام رسان ها توسط جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟
	۰	۰	۲	٥۸	٤۰	درصد	
٥,۷۹	۳	۱۰	۲٤	٦۰	۳	فراوانی	۷ گسترش توریسم و گردشگری در جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟
	۳	۱۰	۲٤	٦۰	۳	درصد	
٥,۷۲	٤	۱٤	۲٦	٤۷	۹	فراوانی	۸ برگزاری همایش های علمی بین المللی در حوزه سایبر توسط جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟
	٤	۱٤	۲٦	٤۷	۹	درصد	
٥,۸۲	۲	۱۷	۲۲	٤۸	۱۱	فراوانی	۹ اشتراکات دینی، فرهنگی و تاریخی جمهوری اسلامی ایران با کشورهای منطقه چه میزان در کنترل تهدیدات سایبری نقش دارد؟
	۲	۱۷	۲۲	٤۸	۱۱	درصد	
٦,۱۲	۲	۱۳	۱۹	٦۱	٥	فراوانی	۱۰ بهره گیری از سازمان هاو نهادهای غیر دولتی و مردم نهاد توسط جمهوری اسلامی
	۲	۱۳	۱۹	٦۱	٥	درصد	

	ایران چه نقشی در کنترل تهدیدات سایبری دارد؟							
۱۱	ارتباط سیاسیون و دیپلمات‌های جمهوری اسلامی ایران با افراد مشهور و نخبگان حوزه‌های مختلف در عرصه بین الملل در کنترل تهدیدات سایبری چه نقشی دارد.	فراوانی	۱۷	٥٤	۲۲	٤	۳	٦,۸۳
		درصد	۱۷	٥٤	۲۲	٤	۳	
۱۲	بهره گیری از مهاجرین ایرانی در سایر کشورها، برای معرفی ایران و انقلاب اسلامی، جهت آشنایی بیشتر ملت‌های جهان با فرهنگ، تمدن وعقاید مردم ایران، چه نقشی در کنترل تهدیدات سایبری دارد؟	فراوانی	۲٥	٤۸	۱٤	۱۱	۲	۷,۲۱
		درصد	۲٥	٤۸	۱٤	۱۱	۲	

در تحلیل گویه های مربوط به سئوال فرعی اول ورتبه بندی آنها با استفاده از آزمون فرید من نشان می دهد؛ «استفاده از ظرفیت پیام‌رسان‌ها توسط جمهوری اسلامی ایران » با میانگین ۹/۲۱ و « همکاری های علمی جمهوری اسلامی ایران در حوزه سایبری با خارج از کشور » با میانگین ۵/۶۷ به ترتیب بیشترین و کمترین میانگین رتبه‌ای را به خود اختصاص داده‌اند. سایر ارزش‌های مربوط به میانگین رتبه‌ای متغیرها در جدول شماره ۵ درج شده است.

با توجه به این که در آزمون متغیرهای دیپلما سی عمومی جمهوری ا سلامی ایران در کنترل تهدیدات سایبری، ارزش خی‌دوی م شاهده شده (۱۰۹/۳۶۰) در درجه آزادی ۳ معنی‌دار است، در نتیجه استنباط می‌شود که بین فراوانی‌های مشاهده شده تفاوت معنی‌داری وجود دارد. یعنی فر ضیه H1 پذیرفته می شود و فر ضیه مقابل آن یعنی H0 رد می‌گردد.

۴. نتیجه‌گیری

۱-۴. جمع‌بندی

رهبران سیاسی، سیاست گذاران خارجی و راهبردشناسان فرایندهای دیپلماتیک در سراسر جهان، به طور روزافزون به این نتیجه رسیده‌اند و بر این باورند که دیپلماسی را به عنوان یک راهبرد ضروری، محوری، مقتضی، شایسته، قابل دستیابی و فوق العاده برای قرن بیست و یکم انتخاب کنند. در دوره و زمانی که تهدیدات سایبری بخش عمده‌ای از تهدیدات را شامل می‌شود، استفاده از قدرت دیپلماسی می‌تواند تهدیدات سایبری را مدیریت کرده و چه بسا آن ها را به فرصت‌های بدیع تبدیل کند. بنابراین جمهوری اسلامی ایران که به دلیل ویژگی منحصر به فرد نظام حاکم در آن در معرض تهدیدات سایبری است باید بیش از سایر دولتها برای مقابله با این تهدیدات اهتمام جدی داشته و از همه ابزارهای موجود استفاده نماید که دیپلماسی از نوع رسمی و عمومی می تواند یکی از مهمترین ابزارها باشد. بررسی نقش هر یک از دیپلماسی‌های اشاره شده در کاهش تهدیدات سایبری در این مقاله مهم‌ترین هدف بود.

در ارتباط با سئوال فرعی اول پژوهش مبنی بر نقش دیپلماسی رسمی در کنترل تهدیدات سایبری علیه جمهوری اسلامی ایران، مولفه‌های زیر به ترتیب درصد اهمیت از نظر خبرگان به‌دست آمده است:

(۱) همکاری های اطلاعاتی و امنیتی جمهوری اسلامی ایران با سایر کشورها.

(۲) رویکرد تعاملی و تنش زدایی با کشورهای مختلف به ویژه در منطقه غرب آسیا.

(۳) همکاری سایبری جمهوری اسلامی ایران با سایر کشورها.

(۴) انعقاد قراردادها و معاهدات دوجانبه و چند جانبه میان جمهوری اسلامی ایران و سایر کشورها.

(۵) روابط سیاسی متقابل و رضایت بخش جمهوری اسلامی ایران با کشورهای منطقه و جهان.

نتایج حاصله در ارتباط با سئوال فرعی اول نشان می‌دهد که دیپلماسی سنتی در کنترل تنش‌ها و تهدیدات سایبری تاثیر گذار بوده و نیاز است جمهوری اسلامی ایران بیش از پیش از دیپلماسی سنتی دو جانبه و چند جانبه برای کاهش تهدیدات سایبری استفاده نماید.

در ارتباط با سئوال فرعی دوم پژوهش مبنی بر نقش دیپلماسی عمومی در کنترل تهدیدات سایبری علیه جمهوری اسلامی ایران، مولفه‌های زیر به ترتیب اولویت بیشترین نقش را دارند:

(۱) استفاده از ظرفیت پیام رسان های مختلف در جمهوری اسلامی ایران.

(۲) استفاده از شبکه های اجتماعی مختلف در جمهوری اسلامی ایران.

(۳) بهره گیری از مهاجران ایرانی در سایر کشورها برای معرفی ایران و انقلاب اسلامی.

(۴) ارتباط سیاسیون و دیپلمات‌های جمهوری اسلامی ایران با افراد مشهور و نخبگان حوزه‌های مختلف در عرصه بین الملل.

(۵) بهره گیری از سازمان‌ها و نهادهای غیر دولتی و مردم نهاد.

نتایج حاصله در ارتباط با سئوال فرعی دوم نشان می دهد که بهره‌گیری از دیپلماسی عمومی می‌تواند افکار عموم مردم جهان را تحت تاثیر قرار داده و با تحت فشار قراردادن دولت‌مردان کشورهای مختلف، انواع تهدیدات از جمله تهدیدات سایبری علیه جمهوری اسلامی ایران را کاهش دهد.

۴-۲. پیشنهادها

برای تاثیر گذاری بیشتر دیپلماسی جمهوری اسلامی ایران در کنترل تهدیدات سایبری موارد زیر پیشنهاد می گردد:

(۱) همکاری اطلاعاتی و امنیتی جمهوری اسلامی ایران با کشورهای همسایه با هدف کنترل تهدیدات سایبری، در دستور کار سازمان‌های امنیتی و اطلاعاتی کشور قرار گیرد.

(۲) جمهوری اسلامی ایران به تعامل سازنده با کشورهای منطقه تاکید زیادی داشته که نیاز است به منظور کاهش تهدیدات حوزه سایبری بیش از پیش به این موضوع اهمیت داده شود.

(۳) همکاری سایبری با کشورهایی که رویکرد تعاملی با جمهوری اسلامی ایران دارند مورد توجه جدی قرار گیرد.

(۴) با توجه به گستردگی حملات سایبری علیه جمهوری اسلامی ایران، وزارت امور خارجه دیپلماسی فعال دوجانبه و چندجانبه‌ای را برای مقابله با این گونه حملات اتخاذ نماید.

(۵) با توجه به استفاده قشر عظیم جامعه از شبکه های اجتماعی و پیام رسان‌های خارجی و تهدیداتی که آن شبکه‌ها و پیام رسان‌ها می‌توانند داشته باشند، مسئولین امر بر ایجاد یک پیام رسان بومی واحد و یکپارچه تمرکز نموده تا از تعدد پیام رسان‌های ضعیف که با اقبال کمی مواجه هستند اجتناب گردد.

(۶) نهادهای دولتی و غیر دولتی متولی دیپلماسی فرهنگی کشور، از ظرفیت ایرانی‌های مقیم در سایر کشورها برای معرفی فرهنگ و تمدن جمهوری اسلامی ایران با هدف مقابله با تبلیغات سوء علیه کشور استفاده نمایند.

منابع

الف. منابع فارسی

۱. اسکندری، حمید(۱۳۹۱) ، ***فرهنگ واژگان موضوعی پدافند غیر عامل***، انتشارات بوستان حمید، تهران

۲. اژدری ، لیلا ، فرهنگی ، علی اکبر ، صالحی امیری ، سید ر ضا ، سلطانی فر ، محمد ،(۱۳۹۶) ، مدل دیپلما سی فرهنگی جمهوری ا سلامی ایران ، ***مطالعات فرهنگ – ارتباطات***، سال هجدهم ،شماره ۳۸.

۳. بارستون، آر. پی، (۱۳۷۹)، ***دیپلماسی نوین***، ترجمه محمد جعفر جواد، تهران: دادگستر.

۴. بیلیس، جان و اسمیت، استیو، (۱۳۸۳)، ***جهانی شدن سیاست: روابط بین الملل در عصر نوین***، تهران: مؤسسه ابرار معاصر.

۵. توکل، اکبر(۱۳۸۵) مفهوم جنگ ســایبری و کاربرد آن در جنگ آینده، ***فصــلنامه علوم و فنون نظامی***، شماره ۷.

۶. جهانشاهی، علیرضا(۱۳۹۸)، نقش حملات سایبری بر امنیت ملی از منظر حقوق بین الملل، پایان نامه کارشناسی ارشد، دانشگاه فارابی.

۷. حقی، مجید(۱۳۹۸)، ارائه مدل مدیریت راهبردی امنیت فضــای ســایبر بر اســاس کلان داده های فضای سایبر، فصلنامه امنیت ملی، سال نهم، شماره ۳۴.

۸. خلیلی پور، علی، نورعلی وند، یاسر،(۱۳۹۱) تهدیدات سایبری وتاثیر آن بر امنیت ملی ، ***فصلنامه مطالعات راهبردی***، شماره ۵۶.

۹. رستمی، محمد صادق(۱۳۹۷) دیپلماسی دفاعی و نقش آن در کنترل تهدیدات سایبری، ***فصلنامه دانش انتظامی*** ، شماره ۲۸.

۱۰. ستوده آرانی، محمد؛ علویان، مرتضی(۱۳۹۱)، راهکارهای دیپلما سی عمومی و ر سمی ایران در مواجهه با اسلام هراسی غرب، ***فصلنامه علوم سیاسی***، سال پانزدهم، شماره ۵۸.

۱۱. شیرنگی، سید سعید،(۱۳۹۱) ***رویارویی امنیتی ایران و آمریکا در فضای سایبر با تاکید بر نقش آژانس امنیت ملی آمریکا***، دانشگاه امام صادق (ع).

۱۲. شهبازی، آرامش، آقاجانی، آیدا، (۱۳۹۹)، جاسوسی سایبری در حقوق بین الملل: مسئلۀ انتساب مسئولیت بین المللی به دولت در هاله ای از ابهام، ***فصلنامه مطالعات حقوقی عمومی***، زمستان ۱۳۹۹ شماره ۴

۱۳. عاملی، سید حامد، خرازی آذر، رها، مظفری، افسانه،(۱۳۹۶) نقش تکنولوژی های نوین رسانه در دیپلماسی رسانه ای جمهوری اسلامی ایران، ***فصلنامه راهبرد اجتماعی فرهنگی*** ، شماره ۲۲.

۱۴. عباسی، محمد، طالعی حور، رهبر(۱۳۹۷) ***دیپلماسی و حقوق دیپلماتیک و کنسولی در اسلام و غرب***، انتشارات دانشگاه فارابی.

۱۵. قاضوی، سید فضل اله، زیبا کلام، صادق، عقیلی، سید وحید(۱۳۹۵) نقش فضای سایبر در پیشبرد دیپلماسی عمومی مدرن، ***فصلنامه رسانه و فرهنگ*** ، شمار ۱۲.

۱۶. کولایی، الهه، شکاری، حسن، احمدی نیا، مسعود،(۱۳۹۲)، دیپلماسی سایبری آمریکا–مطالعه موردی جمهوری آذربایجان، ***فصلنامه آسیای مرکزی و قفقاز***، شماره ۸۲.

۱۷. هالستی کی .جی، (۱۳۷۳) ***مبانی تحلیل سیاست بین‌الملل***، ترجمه بهرام مستقیمی و مسعود طارم سری، تهران: وزارت امورخارجه.

ب. منابع انگلیسی

- Shaw(2010) , Cybersoace: What Senior Military Leaders Need to Know,http://handle.dtic.mil/100.2/ADA520146

- Wolf, Charles and Brian Rosen, 2004, ìPublic diplomacy: How to think about and improve itî, Available at: www.rand.org/pubs/occasional_papers/2004/RAND_OP134.pdf, Accessed 15 April 2012.

❊❊❊❊❊