

فرمانده معظم کل قوا: «فضای مجازی پدیده 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 درواقع دانش و فکر نو نیاز هست».

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

رهبر طالعی حور،^۱ جمشید نصرت‌آبادی،^۲ محمد حاجی حسینی^۳

تاریخ پذیرش: ۱۴۰۱/۰۵/۱۲

تاریخ دریافت: ۱۴۰۱/۰۲/۰۲

چکیده

دیپلماسی در تاریخ سیاسی جهان پیشینه‌ای دیرینه دارد. گرایش به قدرت و حفاظت از منافع و وحشت از جنگ و پیامدهای ناگوار آن در ایجاد و توسعه روابط دیپلماسی تأثیرگذار بوده است؛ از سوی 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 به‌منظور بهره‌گیری از این فضا از خود نشان دهند و این فضا ضمن ایجاد فرصت، می‌تواند خطرات جبران‌ناپذیری را برای دولت‌ها به وجود آورد که فضای سایبری جمهوری اسلامی ایران نیز از این قاعده مستثنا 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 تعیین شده است. با استناد به منابع کتابخانه‌ای و پژوهش میدانی و بر اساس تجزیه و تحلیل پرسشنامه‌ها، یافته‌های تحقیق بیانگر این است که دیپلماسی رسمی جمهوری اسلامی ایران با استفاده از معاهدات دو یا چندجانبه سایبری می‌تواند موجب کاهش اثر تهدیدات سایبری علیه منافع ملی شود و دیپلماسی عمومی جمهوری اسلامی ایران موجب تنویر افکار عمومی در سطح بین‌الملل شده و با توجه به گستردگی فضای سایبر در تمامی نقاط جهان، دولتمردان کشورهای معاند جمهوری اسلامی ایران را برای اقدام علیه منافع کشور در تنگنا قرار دهد.

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

۱. استادیار روابط بین‌الملل 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. دانش‌آموخته کارشناسی ارشد علوم سیاسی.

مقدمه

امروزه دیپلماسی در انواع مختلف آن مهم‌ترین ابزار برای تضمین کسب منافع و امنیت ملی است؛ 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 بهره‌گیری از این فضا از خود نشان دهند؛ با این وجود وابستگی کشورهای دنیا به این فضا همواره نمی‌تواند به‌عنوان یک فرصت در نظر گرفته شود و تهدیداتی که علیه فضای سایبری یک کشور صورت می‌گیرد، می‌تواند خطرات جبران‌ناپذیری را برای دولت‌ها به وجود آورد. فضای سایبری جمهوری اسلامی ایران نیز از این قاعده مستثنا نیست (شیرنگی، ۱۳۹۱: ۷).

ماهیت و ویژگی‌های فضای سایبر از جمله فراگیر بودن این فضا، ناشناس بودن بازیگران این عرصه و... موجب می‌شود روش‌های معمول در کنترل تهدیدات، پاسخگو نبوده و روزه‌روز 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، به‌کارگیری فن دیپلماسی در مهار تهدیدات موجود در این فضا است؛ بنابراین مطالب مذکور محققان را بر آن داشت تا در مقاله حاضر نقش و چگونگی استفاده از دیپلماسی در تأمین امنیت جمهوری اسلامی ایران در مواجهه با تهدیدات سایبری را بررسی کنند. این تحقیق با توجه به ماهیت پژوهش انجام شده و اینکه به تأثیر دیپلماسی در مقابله با تهدیدات سایبری می‌پردازد و می‌توان از نتایج و یافته‌های آن در بهبود امنیت سایبری استفاده کرد، کاربردی است و با توجه به ارائه عوامل جدید در حوزه دیپلماسی و فضای سایبری و توسعه دانش در این زمینه، توسعه‌ای است. 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 و در بخش کمی پس از انجام مراحل روایی و پایایی با مراجعه به جامعه آماری، به نمونه‌گیری اقدام

شد 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 تأثیر 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: ۱۵). شاخه‌ها و گرایش‌های مختلفی که در فضای سایبری وجود دارد مانند فناوری اطلاعات،^۱ فناوری ارتباطات،^۲ جنگ اطلاعات،^۳ جنگ الکترونیک،^۴ شبکه‌های اجتماعی^۵ 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 به‌عنوان قلمرو پنجم نیروهای نظامی در کنار قلمروهای زمینی، هوایی، دریایی و فضایی تعریف شده است.

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

1. Information Technology
2. Communication Technology
3. Information War
4. Electronic War
5. Social War

نظامی به‌ویژه 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 با توجه به توانمندی‌های نظامی موجود در جمهوری اسلامی؛ از سوی دیگر انگیزه کافی به دشمنان این مرزوبوم می‌دهد که جنگ با ایران را به فضای سایبر منتقل کنند؛ نمونه این فعالیت‌ها را می‌توان به استفاده از شبکه توئیتر در جریان فتنه سال ۱۳۸۸ و یا ویروس استاکس نت^۱ برای تأسیسات هسته‌ای نظیر اشاره کرد. از آنجایی که تهدیدات سایبری به‌ویژه از جانب نهادهای غیردولتی جزء تهدیدات نرم محسوب می‌شوند؛ بنابراین برای مقابله با آن باید از قدرت نرم استفاده کرد؛ به همین دلیل بهره‌برداری درست و به‌موقع از دیپلماسی در مواجهه با تهدیدات غیرسخت نظامی، راه کسب امنیت ملی و منافع ملی را هموار می‌کند. در مطالعات مختلف تأثیر 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، به‌کارگیری دیپلماسی در مهار تهدیدات موجود در این فضا است 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 می‌شود.

۲-۱. اهمیت و ضرورت تحقیق

در مورد اهمیت و بعد ایجابی تحقیق می‌توان گفت پرداختن به این موضوع اهمیت دیپلماسی را به‌عنوان 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 چندجانبه در کاهش و کنترل تهدیدات سایبری؛
 - تقویت اراده بین‌المللی در کنترل و مقابله با تهدید تروریسم سایبری؛
 - اعتمادسازی و ارتقای امنیت در فضای سایبری بین‌الملل؛
 - کاهش هزینه‌های دفاعی در مقابله با تهدیدات سایبری.
- از نظر ضرورت و بعد سلبی نیز می‌توان گفت با توجه به رویکرد جدید دشمنان در جایگزینی تهدیدات سایبری به جای تهدیدات کلاسیک و نظامی، بدیهی است که عرصه فضای سایبر برای مقابله با ایران مناسب‌ترین و در دسترس‌ترین راه است؛ بنابراین غفلت از ابزارهای مناسب برای مقابله با تهدیدات سایبری می‌تواند تبعات زیر را به دنبال داشته باشد:
- گسترش تهدیدات سایبری در بخش‌های مختلف و افزایش هزینه‌های دفاعی؛
 - کمک به سیاست منزوی‌سازی 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؛
 - بی‌توجهی به تقویت و توسعه تجهیزات و سامانه‌های دفاع سایبری.

۱-۳. پیشینه تحقیق

(۱) مقاله‌ای تحت عنوان «دیپلماسی دفاعی و نقش آن در کنترل تهدیدات سایبری» توسط محمداصادق رستمی در پاییز ۱۳۹۷ ارائه شده است. در این پژوهش، می‌توان دیپلماسی دفاعی سایبری را وجه ضروری و تکمیلی فعالیت‌های دفاعی و راهبردی دانست. شناسایی عوامل غیر ایمن و شکاف‌های امنیتی در زیرساخت‌های اصلی کشور، مطالعه تطبیقی استقرار فضای سایبر در کشورهای توسعه‌یافته، تعیین اولویت‌ها در استقرار فضای سایبر، ایجاد یک بستر ارتباطی ایمن، بومی‌سازی تجهیزات مورداستفاده در بخش‌های

اصلی این فضا، توجه به تعاملات بین‌المللی در این زمینه، دادن آموزش‌های لازم به کلیه افرادی که به گونه‌ای در این فضای مجازی قرار می‌گیرند، همگی از نکاتی هستند که باید مورد توجه مسئولان استقرار فضای سایبر واقع شود؛ در غیر این صورت افزون بر اینکه هزینه‌های بسیاری را بر سازمان مربوط تحمیل می‌کند موجب آسیب‌پذیری بخش‌های اصلی سازمان مربوط به‌ویژه در ارتباط با زیرساخت‌های اصلی آن می‌شود.

(۲) تحقیقی با موضوع «نقش فضای سایبری در پیشبرد دیپلماسی عمومی مدرن» توسط سید فضل‌الله قاضوی و همکاران در سال ۱۳۹۵ ارائه و بیان شد در کل اینترنت و فضای سایبر با توجه به گستردگی، جذابیت، سرعت بالای انتقال پیام، امکان برقراری ارتباط با سایر شهروندان را فراهم کرده و از این ابزار می‌توان به‌منظور ارتقای وجهه مثبت کشور استفاده کرد؛ ضمن اینکه این فضا با استفاده از سازوکارهایی مانند گسترش ابزار نظرات سیاسی، آگاهی بخشی به جریان‌های سیاسی، غنی کردن 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 بین‌الملل» توسط علیرضا جهانشاهی در سال ۱۳۹۸ انجام شد؛ در این تحقیق تأکید شده که جامعه بین‌الملل با توجه به وضعیت موجود به معیارهای مطرح‌شده دربارهٔ توسل به زور در فضای سایبر باید توجه خاصی کند و با در نظر داشتن این معیارها، قواعد سنتی دربارهٔ 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؛ چراکه چنین تحولی صلح جهانی را به مخاطره خواهد انداخت. از آنجایی که مفهوم توسل به زور در فضای سایبر نسبت به فضای واقعی متفاوت است؛ بنابراین قواعد خاص خود را دارد؛ پس به‌جا است که کشورها با تشکیل کنفرانس‌های بین‌المللی قواعدی وضع کنند که جلوی این نوع از تحولات را بگیرد، از طرفی سازمان ملل با ارجاع این امر به کمیسیون حقوق بین‌الملل به وظیفه خود در راستای حفظ صلح اقدام کند.

در خصوص نوآوری مقاله می‌توان گفت در پژوهش‌های انجام‌شده هرکدام بخشی از موضوع پژوهش را مورد بررسی قرار داده‌اند؛ اما هیچ‌کدام به نقش دیپلماسی در کاهش تهدیدات سایبری اعم از جنگ و حملات سایبری، جرایم سایبری، تروریسم سایبری و... پرداخته‌اند؛ از این رو نوآوری پژوهش حاضر در این است که نقش دیپلماسی از نوع رسمی و عمومی را در کاهش تهدیدات سایبری با استفاده از نظرات متخصصان این حوزه مورد بررسی قرار می‌دهد امید است که بتواند خلأ پژوهشی موجود در این زمینه را پوشش دهد.

۱-۴. سؤال‌های تحقیق

۱-۴-۱. سؤال اصلی

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

۱-۴-۲. سؤال‌های 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 در کنترل تهدیدات سایبری.

۱-۶. روش‌شناسی تحقیق

پژوهش حاضر از نوع کاربردی - توسعه‌ای و به روش توصیفی - تحلیلی انجام گرفته است؛ این پژوهش برای استدلال و تحلیل یافته‌های خود رویکرد ترکیبی (کمی و کیفی) دارد. در بخش نخست این تحقیق با مراجعه به مراکز مختلف علمی و پژوهشی و استفاده از فیش‌برداری و مصاحبه با خبرگان به گردآوری اطلاعات لازم در رابطه با موضوع اقدام شد. در بخش دوم یافته‌ها و مفروضه‌های بخش نخست به صورت میدانی و با استفاده از پرسشنامه مورد بررسی قرار گرفت. بر این اساس به منظور استخراج ابعاد مسئله از دیدگاه نخبگان در زمینه هدف‌های تحقیق تعداد ۲۳ گویه در قالب طیف ۵ گزینه‌ای 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 است.

۱-۶-۱. جامعه آماری و حجم نمونه

جامعه آماری تحقیق شامل استادان روابط بین‌الملل، علوم سیاسی و فضای سایبر دانشگاه‌های تهران و مدیران و کارشناسان وزارت امور خارجه بوده که تعداد آن ۲۵۸ نفر تعیین شد. برای انتخاب حجم نمونه از فرمول کوکران استفاده شد که در نتیجه آن تعداد حجم نمونه ۱۰۰ نفر به دست آمد.

۱-۶-۲. روایی و پایایی

روایی منطقی پرسشنامه‌ها از دو جنبه روایی ظاهری و محتوایی برای روشن و بدون ابهام بودن گویه‌ها و همچنین کفایت کمیت و کیفیت آن‌ها توسط خبرگان و صاحب‌نظران و استادان دانشگاه تأیید شد. به منظور بررسی روایی شاخص‌های پرسشنامه ابتدا یک نمونه ۱۵ تایی بین جامعه هدف توزیع و گردآوری شد؛ پس از دسته‌بندی داده‌ها، میزان روایی تک تک شاخص‌ها مورد بررسی قرار گرفت؛ همچنین برای محاسبه پایایی از روش آلفای کرونباخ استفاده شد.

مقدار آلفای کرونباخ برای سؤال‌های حوزه دیپلماسی رسمی جمهوری اسلامی ایران در کنترل تهدیدات سایبری (۰/۷۲۵)، سؤال‌های حوزه دیپلماسی عمومی جمهوری اسلامی ایران در کنترل تهدیدات سایبری (۰/۸۸۰) و برای کل سؤال‌های (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

۲-۱. دیپلماسی

دیپلماسی را مفهومی با پیشینه‌ای به اندازه تاریخ ملت‌ها می‌دانند؛ اما به تأیید بیشتر اندیشمندان حوزه علوم سیاسی و سیاست خارجی، تعریف دیپلماسی کار مشکلی است. نه تنها تعریف واحدی از «دیپلماسی» وجود ندارد بلکه وجود تعاریف متنوع و زیاد، این مفهوم را مبهم‌تر نیز کرده است. تعاریف گوناگونی با نگاه به ابعاد، اهداف و آثار مختلف دیپلماسی ارائه شده است، برخی دیپلماسی را به مانند مدیریت کل سیاست خارجی تبیین می‌کنند، چنانچه «هالستی»^۱ می‌گوید: «هدف اصلی دیپلماسی فن مدیریت و هنر حل و فصل 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 به عنوان نظامی اطلاعاتی برای بیان و دفاع از منافع و اعلان تهدیدها و اولتیماتوم‌ها به کار می‌برند؛ در واقع 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 جامعه تصمیم می‌گیرند و این عمل را با ادعای حفظ ثبات یا ایجاد تغییر در محیط (داخلی یا خارجی) و یا ساختارهای خاص روابط بین‌المللی انجام

می دهند» (هالستی، ۱۳۷۳: ۲۱۲)؛ اما شاید بتوان بهترین تعریف از دیپلماسی را از جان بیلینس^۱ و استیو اسمیت^۲ که در کتاب «جهانی شدن سیاست: روابط بین‌الملل در عصر نوین» بیان کرده‌اند دانست: «دیپلماسی در سیاست جهانی عبارت است از فرایند ارتباط بین بازیگران بین‌المللی که قصد دارند از طریق مذاکره، تعارض را بدون جنگ حل و فصل نمایند. این فرآیند در طول قرن‌ها پالایش و نهادینه شده و به صورت حرفه‌ای در آمده است» (بیلینس و دیگران، ۱۳۸۳: ۷۱۵).

۲-۲. اهمیت دیپلماسی

دیپلماسی با مدیریت مناسبات میان دولت‌ها و روابط دولت‌ها با سایر 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 رسمی و غیررسمی خود و نیز سایر بازیگران با استفاده از مکاتبات، مذاکرات خصوصی، تبادل دیدگاه‌ها، اعمال نفوذ، ملاقات، تهدیدها و دیگر فعالیت‌های مربوط به بیان، هماهنگ‌سازی و تأمین منافع ویژه و گسترده‌تر می‌پردازد؛ هرچند اغلب متصور می‌شد دیپلماسی با فعالیت صلح‌آمیز سروکار دارد ممکن است برای نمونه در بستر جنگ یا تعارض مسلحانه نیز تحقق یابد و یا برای هماهنگ‌سازی برخی فعالیت‌های خشونت‌آمیز مورد استفاده قرار گیرد. در حقیقت مشخص شدن مرز میان فعالیت دیپلماتیک و خشونت از جمله تحولات برجسته‌ای است که وجه مشخصه دیپلماسی نوین به شمار می‌رود. این نکته به شکل کلی‌تر در مورد محتوای در حال گسترش دیپلماسی نیز صادق است. از یک جنبه تغییراتی که در شکل اساسی دیپلماسی حاصل به وجود آمده در قالب اصطلاحاتی چون دیپلماسی دلار، دیپلماسی نفت، دیپلماسی منابع و دیپلماسی اتمی منعکس شده است. با اطمینان می‌توان گفت امروزه دیپلماسی از مفهوم سیاسی راهبردی محدودی که زمانی برای آن

1. John Bayliss
2. Steve Smith

حمل می‌شد فراتر می‌رود. از طرف دیگر مناسب نیست که با قائل شدن معنایی محدود یا رسمی برای دیپلماسی، آن را تنها متعلق به وزرای خارجه و کارکنان ادارات دیپلماتیک بدانیم؛ چه بسا 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).

۲-۳. انواع دیپلماسی

۲-۳-۱. دیپلماسی رسمی

ویژگی دیپلماسی رسمی حاکمیت دیدگاه دولت‌محور و تأکید بر فرآیندهای بین‌دولتی 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 (به‌ویژه دولت‌ها) به برقراری و حفظ روابط رسمی جهت تعقیب هدف‌ها، منافع و سیاست‌های واقعی خود در محیط بین‌المللی اقدام می‌کنند (عباسی و دیگران، ۱۳۹۷: ۱۲).

در عصر اطلاعات دیپلماسی رسمی میان دولت‌ها همچنان از اهمیت و جایگاه ویژه‌ای در نظام بین‌الملل برخوردار است. امروزه در نظام بین‌الملل دولت‌محوری، برقراری روابط سیاسی میان دولت‌ها و تأسیس سفارتخانه‌ها و اعزام سفرا و کارداران، زمینه‌ساز برقراری

-
1. Nicholson
 2. Ernest Satow
 3. Elmer Plischke

روابط متقابل در عرصه‌های اقتصادی، فرهنگی و نظامی محسوب می‌شود؛ همچنین سطح روابط سیاسی میان دو کشور و میزان ملاقات و مراودات سیاسی میان نمایندگان آنها می‌تواند نشان‌دهنده میزان علاقه و نوع روابط دوجانبه باشد. هدف دیپلماسی رسمی، نزدیکی ملل به یکدیگر و برقراری صلح و آرامش بین‌المللی است. دیپلماسی درصدد است تا ضمن ایجاد ارتباط دوستانه میان کشورها، تمام امکانات مادی و معنوی آنها را در تداوم و غنی‌تر ساختن این روابط فراهم آورد. تلاش دیپلماسی رسمی همواره حفظ منافع ملی از طریق روش‌های مسالمت‌آمیز بوده است که این هدف در طول ادوار مختلف تاریخی، شیوه‌های گوناگونی را در مقابل دیپلماسی قرار داده است (ستوده آرائی و دیگران، ۱۳۹۱: ۱۵۸-۱۵۶).

برخی از ویژگی‌های دیپلماسی رسمی عبارتند از: حاکمیت فرهنگ سلسله‌مراتبی، سری بودن، شفاف بودن، انحصارطلبی، فقدان پاسخگویی، محافظت از اطلاعات و دانش (عباسی و دیگران، ۱۳۹۷: ۱۲).

۲-۳-۲. دیپلماسی عمومی

عبارت دیپلماسی عمومی در حوزه مطالعات روابط بین‌الملل اصطلاحی است که در دهه ۱۹۶۰ برای توصیف جنبه‌های جدید دیپلماسی بین‌المللی رایج شد. اصطلاح دیپلماسی عمومی نخستین بار در سال ۱۹۶۵ در آمریکا توسط ادموند گولون،^۱ رئیس مدرسه حقوق و دیپلماسی فلچر^۲ در دانشگاه تافنز^۳ به کار گرفته شد و عبارت است از: «ارتباطات معطوف به منافع ملی یک کشور از طریق ارتباط با مردم خارج از مرزهای جغرافیایی». با این تعریف مسایلی از قبیل اعزام دانشجویان به خارج، پذیرش بورس‌های تحصیلی، خبرنگاران اعزامی، فرایند ارتباط میان فرهنگی، برگزاری انواع جشنواره‌های هنری، همایش‌ها و سمینارهای فرهنگی و پخش برنامه‌های صوتی و تصویری و حتی ایجاد سایت‌های اینترنتی، همه و همه در حوزه دیپلماسی عمومی قابل بحث است (Wolf, 2004: 3).

1. Edmund Gullion
2. Fletcher School of Law and Diplomacy
3. Tufts University.

۲-۳-۱. 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 رسانه‌ای**؛ دولت‌ها از دیپلماسی رسانه‌ای نیز به‌عنوان ابزاری مؤثر در شکل‌دهی افکار و نظرات مردم سایر کشورها نسبت به وقایع و تحولات استفاده می‌کنند؛ علاوه بر این رسانه‌ها چنین امکانی را به وجود می‌آورند تا دولت‌ها نظرات و دیدگاه‌های خود را در صحنه بین‌الملل بیان کنند. فعالیت‌های رسانه‌ای در قالب دیپلماسی رسانه‌ای به دنبال جهت‌دهی افکار عمومی و توجیه تصمیم‌گیری‌ها در حوزه سیاست خارجی است؛ در واقع هدف دیپلماسی رسانه‌ای ایجاد تصویر مثبت و مطلوب از اهداف و سیاست‌های دولت‌ها در افکار عمومی است (اژدری و همکاران، ۱۳۹۶: ۲۸).

۳. **دیپلماسی مبادله‌ای**؛ در کنار دیپلماسی فرهنگی و رسانه‌ای، دیپلماسی مبادله‌ای به دنبال دستیابی اهداف درازمدت است و منظور از آن، مجموعه‌ای از فعالیت‌ها و اقدامات فراملی که به دنبال انتقال فرهنگ ارزش‌ها و باورها به سایر سرزمین‌ها است. هرچند گستره دیپلماسی مبادله‌ای، وسیع به نظر می‌رسد ولی بیشتر شامل فعالیت‌های دانشگاهی می‌گردد. مبادله استاد، اعطای بورس‌های دانشجویی، ارائه فرصت‌های مطالعاتی و تحقیقاتی، برگزاری تورهای علمی و کارگاه‌های آموزشی از جمله فعالیت‌هایی هستند که در قالب دیپلماسی مبادله‌ای مطرح می‌شوند؛ 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؛

درواقع با رشد سریع فناوری‌های ارتباطی کابلی (تلویزیون‌ها)، ارتباطات بی‌سیم (راديو) و درنهایت ظهور فضای مجازی و توسعه ارتباطات و امکان برقراری ارتباط و تبادل اطلاعات بین مردم جای‌جای جهان در مدت‌زمان چندثانیه‌ای، انفجاری در فضای دیپلماسی عمومی پدیدار شد و دیپلماسی سایبری به وجود آمد؛ به‌عبارت‌دیگر این دیپلماسی را می‌توان اعمال امور دیپلماتیک از طریق کانال سایبری در نظر گرفت که زمینه تعامل با میلیون‌ها شهروند خارجی از کشورهای دیگر را فراهم می‌سازد. از آنجاکه دیپلماسی سایبری زیرشاخه‌ای از دیپلماسی عمومی است، در این دیپلماسی نیز برخلاف دیپلماسی رسمی که طرفین ارتباط دو دولت و یا هیئت دیپلماتیک هستند در یک سو یک دولت و در طرف دیگر مردم کشور یا کشورهای دیگر قرار دارند. این ارتباط به جای اینکه از طریق ارسال نماینده و نامه‌نگاری رسمی صورت گیرد از طریق کانال‌های مجازی و فضای سایبر صورت می‌پذیرد. همین شیوه ارتباط‌گیری و تأثیرپذیری باعث شده است که در سال‌های اخیر در سیاست بین‌المللی، دیپلماسی سایبری تبدیل به یک کانال دیپلماتیک برای تعامل با توده‌های مردمی جوامع مختلف شود. هدف از این دیپلماسی می‌تواند تغییر در فرهنگ جوامع دیگر، همسو کردن آن‌ها با سیاست‌ها و فعالیت‌های یک دولت خاص، بر پا کردن جنبش اعتراضی از طریق شبکه‌های اجتماعی، بسیج گروه‌های برانداز از طریق فضای سایبر، جمع‌آوری اطلاعات در مورد صف‌آرایی نیروهای اجتماعی - سیاسی طرف مقابل و... باشد (کولایی و همکاران، ۱۳۹۲: ۵۱).

۲-۴. فضای سایبری

در سند راهبردی امنیت فضای تبادل اطلاعات (افتا) به فضای سایبری، فضای تبادل اطلاعات گفته شده و به‌صورت زیر تعریف می‌شود: «در عصر اطلاعات شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی از قبیل اطلاع‌رسانی، داده‌ورزی، ارائه خدمات، مدیریت و کنترل و ارتباطات از طریق سازوکارهای الکترونیکی و مجازی انجام می‌پذیرد. از این فضا با نام فضای تبادل اطلاعات (فتا) یاد می‌شود» (حقی، ۱۳۹۸: ۲۸۱).

کمسیون اروپایی فضای سایبر را یک فضای مجازی دانسته که در آن داده‌های الکترونیکی رایانه‌های شخصی در سرتاسر جهان منتشر می‌شوند. فضای سایبری از مؤلفه‌های 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 مورد استفاده 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 فراهم می‌کنند.

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 کردن منابع قابل توجه در محاکم مختلف برای نیل به اهداف هستند. جدول زیر این مؤلفه‌ها را باهم نشان می‌دهد:

جدول شماره ۱: مؤلفه‌های کلیدی فضای سایبر (Shaw,2010:5)

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

امروزه فعالیت مقامات و سیاسیون در فضای سایبری موجب پیشبرد اهداف سیاست خارجی کشورها شده است. وبسایت‌ها از محبوب‌ترین ابزارهای الکترونیکی مورداستفاده در فضای سایبری هستند، امروزه اغلب وزارتخانه امور خارجه دارای وبسایت رسمی برای ارتباطات عمومی است؛ پس از وبسایت‌ها، توئیتر و فیس‌بوک در حال حاضر از محبوب‌ترین ابزارهای الکترونیکی هستند که توسط وزارتخانه‌های امور خارجه در سرتاسر جهان استفاده می‌شوند؛ از دیگر رسانه‌های اجتماعی مورداستفاده در وزارتخانه‌های امور خارجه می‌توان از یوتیوب^۱، فلیکر^۲، لینکدین^۳، پینترست^۴ و اینستاگرام^۵ نام برد (کولابی و همکاران، ۱۳۹۲: ۲۵).

۲-۵. 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 گونه‌ای که امروزه چالش تهدیدهای سایبری، هم مهم و هم پیچیده به نظر می‌رسد. این اهمیت و پیچیدگی ناشی از ماهیت جدید تهدیدهای سایبری و ویژگی‌ها و نمودهای منحصربه‌فردی است که شناخت از آن را بسیار مهم و ضروری می‌نماید.

در همایشی که در دوم مارس ۲۰۱۰ از سوی مؤسسه بین‌المللی CACI و مؤسسه مطالعاتی نیروی دریایی ایالات متحده با عنوان «تهدیدهای سایبری امنیت ملی و مقابله با چالش‌های پیش روی زنجیره عرضه جهانی» برگزار شد، تهدیدهای سایبری به صورت «وقایعی که به صورت طبیعی و یا توسط انسان به صورت عمدی یا غیرعمدی بر فضای مجازی تأثیرگذار باشد یا حوادثی که از طریق فضای مجازی عمل کند یا به نحوی به آن مرتبط باشد» تعریف شد (خلیلی‌پور و دیگران، ۱۳۹۱: ۱۶۹).

1. YouTube
2. Flickr
3. LinkedIn
4. pinterest
5. Instagram

۲-۶. ویژگی‌های تهدید سایبری

تهدیدهای سایبری ویژگی‌های منحصر به فردی دارند؛ از یک سو این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند و از سوی دیگر، هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبر موجب شده بازیگران زیادی به این عرصه وارد شوند. مهم‌ترین ویژگی‌های تهدیدهای سایبری در مؤلفه‌های زیر خلاصه می‌شود:

۱. **تعدد بازیگران در فضای سایبری:** هزینه کم فن‌آوری رایانه‌ای، اتصال گسترده به اینترنت و سهولت ایجاد یا به دست آوردن نرم‌افزارهای مخرب به این معناست که تقریباً هرکسی می‌تواند به این فضا وارد شود؛ این بازیگران شامل افراد، گروه‌های سازمان‌یافته جنایی، گروه‌های تروریستی، شرکت‌های 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 پیچیده‌تر سایبری نیازمند صرف وقت بیشتر و هزینه‌های بالاتری است.

۳. **ناشناس ماندن بازیگران و عدم قابلیت ردیابی:** اینترنت به‌عنوان سیستم نامتمرکز طراحی شده و کاربران آن، اغلب شناخته‌شده نیستند؛ همین ناشناختگی موجب می‌شود هیچ اثری از برخی از حمله‌های سایبری باقی نماند. افراد فعال در عرصه اینترنت می‌توانند 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 می‌تواند تأثیرات و پیامدهای به‌مراتب بیشتری از حادثه اولیه در پی داشته باشد. وقوع حمله‌های سایبری و در نتیجه آن، بروز اختلال در شبکه‌ها می‌تواند موجب ایجاد خسارت به اموال، زمان، محصولات و تولیدات، اعتبار، اطلاعات حساس و

حتی از دست دادن جان انسان‌ها شود؛ زیرا در این گونه مواقع، زیرساخت‌ها و سامانه‌های مهم دچار آسیب می‌شوند.

۵. **کمرنگ شدن نقش جغرافیا:** فضای سایبری سرعت انتقال به سراسر جهان را در لحظه کوتاهی فراهم کرده است؛ بنابراین، تهدیدکنندگان قادر به فراتر رفتن از محدوده جغرافیایی خود و رسیدن به اهداف کلیدی‌شان هستند.

۶. **ساختار فضای اینترنت:** اینترنت، دامنه مشترک و یکپارچه است. استفاده از این فضا توسط شهروندان، شرکت‌ها و دولت‌ها به شیوه‌ای است که جداسازی آن‌ها بسیار دشوار است. توانایی محدود برای جدا کردن بازیگران و فعالیت‌های آن‌ها، پاسخ مناسب به آن‌ها از سوی دیگر، ساختار تهدید را بسیار دشوارتر کرده است. اینترنت، دولت‌ها و شرکت‌های خصوصی را با عدم اطمینان در قبال خطرات فضای اینترنتی مواجه کرده است؛ این عدم قطعیت ناشی از پیچیدگی‌ها و فن‌آوری 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 شیوه‌های متفاوتی حاصل می‌شوند که مهم‌ترین آن‌ها عبارتند از: جنگ سایبری، تروریسم سایبری، جرایم سایبری، جاسوسی سایبری و اختلال سایبری (خلیلی پور و دیگران، ۱۳۹۱: ۴۸).

۲-۷. انواع تهدید سایبری

۱. **جنگ سایبری:** جنگ سایبری عبارت است از «اقدامات آفندی غیر متحرکی که به منظور کسب برتری اطلاعاتی از طریق تحت تأثیر قرار دادن سامانه اطلاعاتی و شبکه‌های رایانه‌ای دشمن اتخاذ می‌شوند». بر اساس این تعریف به نظر می‌رسد که جنگ سایبری زیرشاخه‌ای از جنگ اطلاعاتی بوده و شامل اقداماتی است که در فضای سایبری در تقابل با فضا یا دنیای واقعی صورت می‌پذیرد. بستر جنگ سایبری عبارت است از هر سامانه واقعی مجازی که دربرگیرنده مجموعه‌ای از رایانه‌ها و شبکه‌ها باشد. یکی از شاخص‌ترین

محیط‌های جنگ سایبری اینترنت و شبکه‌های (نظامی یا غیرنظامی) مرتبط است که به نحوی اطلاعات را به اشتراک می‌گذارند. با در نظر گرفتن جنبه نظامی جنگ سایبری می‌توان آن‌ها جنگی در حوزه اینترنت قلمداد نمود (توکل، ۱۳۸۵: ۱۷).

۲. **تروریسم سایبری:** تروریسم سایبر، حمله یا تهدید به حمله به شبکه‌های رایانه‌ای و اطلاعات ذخیره‌شده در آن‌ها به قصد ایجاد رعب و وحشت یا وادار کردن دشمن به انجام یک کار است. سه نوع از این تروریسم نرم‌افزاری عبارتند از:

- حمله به نتایج حاصل از اکتشافات نظامی، ارتباطات، فرماندهی و کنترل و جنبه‌های مختلف اطلاعات محرمانه؛

- حمله به حلقه‌های مهم برقراری ارتباط در جامعه از جمله صدا، تصویر، انتقال داده‌ها و سامانه‌های تلفنی؛

- به‌کارگیری رادیو، تلویزیون و سایر ابزارهای مشابه برای حمله یا تحت تأثیر قرار دادن دیدگاه‌های 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 نمی‌توان آن را جرم در زمره جرایم رایانه‌ای قلمداد کرد؛ اما در تعریف گسترده هر فعل یا ترک فعلی که از طریق یا به کمک سیستم‌های رایانه‌ای رخ می‌دهند جرم رایانه‌ای قلمداد می‌شود که از این دیدگاه به سه دسته تقسیم می‌شوند؛ دسته اول از جرایم رایانه و تجهیزات رایانه‌ای، موضوع جرایم سنتی مثل سرقت، تخریب تجهیزات و... هستند. در دسته دوم رایانه وسیله و ابزار ارتکاب جرم است و از آن برای جعل مدرک، گواهینامه و... استفاده می‌شود. در دسته سوم جرایم محض، جرایمی مانند هک یا ویروسی کردن که صرفاً در فضای سایبر (مجازی) اتفاق می‌افتد (رستمی، ۱۳۹۷: ۳۸). در قوانین جمهوری اسلامی ایران مصادیق جرایم سایبری به شرح زیر گنجانده شده است:

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

- جرم‌هایی که علیه صحت و درستی داده‌ها است؛ مثل جعل رایانه، ایجاد اختلال در داده‌ها 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 رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا اطلاعات محرمانه را جمع‌آوری کند. برخلاف جرایم سایبری که مسایل مالی و اقتصادی محرک اصلی مجرمان است، جاسوسی سایبری بیشتر تأثیرات سیاسی داشته و جامعه را تهدید می‌کند. محرک‌های اصلی جاسوسی سایبری متفاوت است؛ اما شامل کسب منافع نظامی، صنعتی، سیاسی و فنی است. جاسوسان سایبری اطلاعات دزدیده‌شده را با اهداف مختلف مورد استفاده قرار می‌دهند که برخی از آن‌ها عبارتند از تهدید، اخاذی و مختل کردن اقدامات رقبای سیاسی (خلیلی‌پور، نورعلی‌وند: ۱۳۹۱: ۶۹). جاسوسی سایبری یکی از طرق جاسوسی، دستکاری یا بهره‌برداری غیرقانونی از اطلاعات محسوب می‌شود. این قسم از جاسوسی به دسترسی غیرقانونی یا دزدی اطلاعات محرمانه ذخیره شده در فرمت‌های دیجیتال یا رایانه‌ها 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 حفاظت‌شده استفاده می‌کند. این اطلاعات حساس می‌تواند مشتمل بر مالکیت معنوی، تحقیقات و داده‌های مربوط به توسعه پروژه‌ها یا هر اطلاعات دیگری شود که برای دارنده اطلاعات مهم و حیاتی است؛ بنابراین از طریق جاسوسی می‌توان به اطلاعات مهم و طبقه‌بندی‌شده‌ای از یا مکان دور به صورت پنهانی (جمله اصلاح شود)، کاملاً ارزان و احتمالاً در مقیاس وسیع نفوذ کرد (شهبازی و دیگران، ۱۳۹۹: ۱۴۹۰).

۵. **آشفتگی سایبری:** آشفتگی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا هدف موردنظر 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 می‌کنند که غیرقانونی هستند. برخلاف جرایم سایبری و جاسوسی سایبری که هدفشان دزدی یا تغییر اطلاعات است، آشفتگی سایبری سعی در مجازات یا تأثیرگذاری بر عقاید و رفتار هدف‌های خود دارد. ممکن است طی این مرحله، اطلاعات زیادی دزدیده شده و یا تغییر یابد و یا هزینه‌های مادی فراوانی به شبکه‌های هدف وارد شود؛ اما قصد و نیت اصلی آشفتگی سایبری آسیب رساندن است. بازیگران دولتی و غیردولتی می‌توانند از این ابزار استفاده کنند ولی تاکنون آشفتگی سایبری توسط افرادی انجام شده که با نام فعالان عرصهٔ هک شناخته شده‌اند (خلیلی‌پور و دیگران: ۱۳۹۱: ۷۱).

۳. یافته‌های تحقیق و تجزیه و تحلیل آن‌ها

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

جدول شماره ۳: نقش دیپلماسی رسمی جمهوری اسلامی ایران در کنترل تهدیدات سایبری

میانگین (درصد)	دیدگاه نمونه آماری					فراوانی و درصد	نقش دیپلماسی رسمی جمهوری اسلامی ایران در کنترل تهدیدات سایبری	ردیف
	درجه‌های ارزیابی							
	بسیار زیاد	زیاد	متوسط	کم	بسیار کم			
۶۲٫۲۷	۲۷	۴۳	۲۲	۶	۲	فراوانی	روابط سیاسی متقابل و رضایت‌بخش جمهوری اسلامی ایران با کشورهای منطقه و جهان چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۱
	۲۷	۴۳	۲۲	۶	۲	درصد		
۷۲٫۲۲	۰	۰	۱۱	۶۱	۲۸	فراوانی	انعقاد قراردادهای و معاهدات سایبری دوجانبه و چندجانبه جمهوری اسلامی ایران با کشورها چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۲
	۰	۰	۱۱	۶۱	۲۸	درصد		
۵۲٫۲۳	۱۱	۴۷	۳۳	۷	۲	فراوانی	بهره‌گیری جمهوری اسلامی ایران از قوانین و حقوق بین‌الملل چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۳
	۱۱	۴۷	۳۳	۷	۲	درصد		
۴۹٫۷	۳	۸	۲۶	۵۹	۴	فراوانی	سفارتخانه‌ها و کنسولگری‌های جمهوری اسلامی ایران در کشورها چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۴
	۳	۸	۲۶	۵۹	۴	درصد		
۵۰٫۷	۱	۷	۳۲	۵۴	۶	فراوانی	حضور فعال جمهوری اسلامی ایران در نهادهای بین‌المللی از جمله سازمان ملل متحد چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۵
	۱	۷	۳۲	۵۴	۶	درصد		
۴۹٫۹۵	۵	۶	۲۸	۵۶	۵	فراوانی	بهره‌گیری جمهوری اسلامی ایران از ظرفیت سازمان‌های منطقه‌ای چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۶
	۵	۶	۲۸	۵۶	۵	درصد		
۷۱٫۱۴	۰	۱	۱۹	۴۲	۳۸	فراوانی	همکاری سایبری جمهوری اسلامی ایران با کشورها چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۷
	۰	۱	۱۹	۴۲	۳۸	درصد		
۷۶٫۵	۲	۳	۱۲	۳۴	۴۹	فراوانی	همکاری‌های اطلاعاتی و امنیتی جمهوری اسلامی ایران با کشورها چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۸
	۲	۳	۱۲	۳۴	۴۹	درصد		
۷۶٫۱	۴	۵	۱۳	۲۳	۵۵	فراوانی	رویکرد تعاملی و تنش‌زدایی با کشورهای منطقه و جهان چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۹
	۴	۵	۱۳	۲۳	۵۵	درصد		
۵۰٫۱	۳	۹	۲۶	۵۷	۵	فراوانی	همگرایی جمهوری اسلامی ایران با کشورهای منطقه چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۱۰
	۳	۹	۲۶	۵۷	۵	درصد		
۴۸٫۹	۴	۹	۲۷	۵۶	۴	فراوانی	استفاده از قدرت نظامی و دفاعی جمهوری اسلامی ایران به‌عنوان یک ابزار دیپلماسی (دیپلماسی دفاعی) در کنترل تهدیدات سایبری چه نقشی دارد؟	۱۱
	۴	۹	۲۷	۵۶	۴	درصد		

در تحلیل گویه‌های مربوط به سؤال فرعی اول یافته‌ها نشان می‌دهد «همکاری‌های اطلاعاتی و امنیتی جمهوری اسلامی ایران با کشورها» با میانگین $7/65$ و «استفاده از قدرت نظامی و دفاعی جمهوری اسلامی ایران به عنوان یک ابزار دیپلماسی (دیپلماسی دفاعی)» با میانگین $4/89$ 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 اینکه در آزمون متغیرهای دیپلماسی رسمی جمهوری اسلامی ایران در کنترل تهدیدات سایبری، ارزش خی دوی مشاهده شده ($135/840$) در درجه آزادی ۳ معنی‌دار است؛ در نتیجه استنباط می‌شود که بین فراوانی‌های مشاهده‌شده تفاوت معنی‌داری وجود دارد. یعنی فرضیه $H1$ پذیرفته می‌شود و فرضیه مقابل آن یعنی $H0$ رد می‌شود. سؤال فرعی دوم تحقیق عبارت بود از «دیپلماسی عمومی جمهوری اسلامی ایران در کنترل تهدیدات سایبری چه نقشی دارد؟» برای پاسخ به این سؤال ۱۲ گویه از مصاحبه با خبرگان احصا شد که نتایج آن به شرح جدول شماره ۵ است.

جدول شماره ۵: نقش دیپلماسی عمومی جمهوری اسلامی ایران در کنترل تهدیدات سایبری

میانگین (درصد)	دیدگاه نمونه آماری					فراوانی و درصد	گویه‌های پرسشنامه نقش دیپلماسی عمومی جمهوری اسلامی ایران در کنترل تهدیدات سایبری	ردیف
	درجه‌های ارزیابی							
	۱	۲	میانگین	۳	۴			
۵۶۷	۲	۱۵	۲۶	۵۰	۷	فراوانی	همکاری‌های علمی جمهوری اسلامی ایران در حوزه سایبری با خارج از کشور چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۱
	۲	۱۵	۲۶	۵۰	۷	درصد		
۶۰۲	۲	۱۵	۲۰	۵۶	۷	فراوانی	رسانه‌های شنیداری برون‌مرزی جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۲
	۲	۱۵	۲۰	۵۶	۷	درصد		
۵۷۳	۲	۹	۳۲	۵۲	۵	فراوانی	رسانه‌های دیداری برون‌مرزی جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۳
	۲	۹	۳۲	۵۲	۵	درصد		
۶۰۱	۳	۱۳	۲۲	۵۲	۱۰	فراوانی	تبادلات علمی مانند بورس کردن دانشجویان دیگر کشورها توسط جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۴
	۳	۱۳	۲۲	۵۲	۱۰	درصد		

میانگین (درصد)	دیدگاه نمونه آماری					فراوانی و درصد	گویه‌های پرسشنامه	رتبه
	درجه‌های ارزیابی							
	بسیار زیاد	زیاد	متوسط	کم	بسیار کم		نقش دیپلماسی عمومی جمهوری اسلامی ایران در کنترل تهدیدات سایبری	
۷۹۰	۴	۵	۱۱	۴۷	۳۳	فراوانی	استفاده از ظرفیت شبکه‌های اجتماعی توسط جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۵
	۴	۵	۱۱	۴۷	۳۳	درصد		
۹۲۱	۰	۰	۲	۵۸	۴۰	فراوانی	استفاده از ظرفیت پیام‌رسان‌ها توسط جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۶
	۰	۰	۲	۵۸	۴۰	درصد		
۵۷۹	۳	۱۰	۲۴	۶۰	۳	فراوانی	گسترش توریسم و گردشگری در جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۷
	۳	۱۰	۲۴	۶۰	۳	درصد		
۵۷۲	۴	۱۴	۲۶	۴۷	۹	فراوانی	برگزاری همایش‌های علمی بین‌المللی در حوزه سایر توسط جمهوری اسلامی ایران چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۸
	۴	۱۴	۲۶	۴۷	۹	درصد		
۵۸۲	۲	۱۷	۲۲	۴۸	۱۱	فراوانی	اشتراکات دینی، فرهنگی و تاریخی جمهوری اسلامی ایران با کشورهای منطقه چه میزان در کنترل تهدیدات سایبری نقش دارد؟	۹
	۲	۱۷	۲۲	۴۸	۱۱	درصد		
۶۱۲	۲	۱۳	۱۹	۶۱	۵	فراوانی	بهره‌گیری از سازمان‌ها و نهادهای غیردولتی و مردم‌نهاد توسط جمهوری اسلامی ایران چه نقشی در کنترل تهدیدات سایبری دارد؟	۱۰
	۲	۱۳	۱۹	۶۱	۵	درصد		
۶۸۳	۳	۴	۲۲	۵۴	۱۷	فراوانی	ارتباط سیاست‌یون و دیپلمات‌های جمهوری اسلامی ایران با افراد مشهور و نخبگان حوزه‌های مختلف در عرصه بین‌الملل در کنترل تهدیدات سایبری چه نقشی دارد؟	۱۱
	۳	۴	۲۲	۵۴	۱۷	درصد		
۷۲۱	۲	۱۱	۱۴	۴۸	۲۵	فراوانی	بهره‌گیری از مهاجران ایرانی در سایر کشورها برای معرفی ایران و انقلاب اسلامی برای آشنایی بیشتر ملت‌های جهان با فرهنگ، تمدن و عقاید مردم ایران چه نقشی در کنترل تهدیدات سایبری دارد؟	۱۲
	۲	۱۱	۱۴	۴۸	۲۵	درصد		

در تحلیل گویه‌های مربوط به سؤال فرعی اول و رتبه‌بندی آن‌ها با استفاده از آزمون فریدمن نشان می‌دهد «استفاده از ظرفیت پیام‌رسان‌ها توسط جمهوری اسلامی ایران» با میانگین ۹/۲۱ و «همکاری‌های 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 اینکه در آزمون متغیرهای دیپلماسی عمومی جمهوری اسلامی ایران در کنترل تهدیدات سایبری ارزش خی‌دوی مشاهده شده (۱۰۹/۳۶۰) در درجه آزادی ۳ معنی‌دار است؛ در نتیجه استنباط می‌شود که بین فراوانی‌های مشاهده‌شده تفاوت معنی‌داری وجود دارد؛ یعنی فرضیه H_1 پذیرفته می‌شود و فرضیه مقابل آن یعنی H_0 رد می‌شود.

۴. نتیجه‌گیری

۴-۱. جمع‌بندی

رهبران سیاسی، سیاست‌گذاران خارجی و راهبردشناسان فرایندهای دیپلماتیک در سراسر جهان به‌طور روزافزون به این نتیجه رسیده‌اند و بر این باورند که دیپلماسی را به‌عنوان یک راهبرد ضروری، محوری، مقتضی، شایسته، قابل دستیابی و فوق‌العاده 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 چه‌بسا آن‌ها را به فرصت‌های بدیع تبدیل کند؛ بنابراین جمهوری اسلامی ایران که به دلیل ویژگی منحصربه‌فرد 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 کند که دیپلماسی از نوع رسمی و عمومی می‌تواند یکی از مهم‌ترین ابزارها باشد. بررسی نقش هر یک از دیپلماسی‌های اشاره‌شده در کاهش تهدیدات سایبری در این مقاله مهم‌ترین هدف بود.

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

(۱) همکاری‌های اطلاعاتی و امنیتی جمهوری اسلامی ایران با سایر کشورها؛

- (۲) رویکرد تعاملی و تنش‌زدایی با کشورهای مختلف به‌ویژه در منطقه غرب آسیا؛
- (۳) همکاری سایبری جمهوری اسلامی ایران با سایر کشورها؛
- (۴) انعقاد قراردادهای و معاهدات دوجانبه و چندجانبه میان جمهوری اسلامی ایران و سایر کشورها؛
- (۵) روابط سیاسی متقابل و رضایت‌بخش جمهوری اسلامی ایران با کشورهای منطقه و جهان.

نتایج حاصل در ارتباط با سؤال فرعی اول نشان می‌دهد که دیپلماسی سنتی در کنترل تنش‌ها و تهدیدات سایبری تأثیرگذار بوده و نیاز است جمهوری اسلامی ایران بیش‌ازپیش از دیپلماسی سنتی دوجانبه و چندجانبه برای کاهش تهدیدات سایبری استفاده کند. در ارتباط با سؤال فرعی دوم پژوهش مبنی بر نقش دیپلماسی عمومی در کنترل تهدیدات سایبری علیه جمهوری اسلامی ایران، مؤلفه‌های زیر به ترتیب اولویت بیشترین نقش را دارند:

- (۱) استفاده از ظرفیت پیام‌رسان‌های مختلف در جمهوری اسلامی ایران؛
- (۲) استفاده از شبکه‌های اجتماعی مختلف در جمهوری اسلامی ایران؛
- (۳) بهره‌گیری 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 بین‌الملل؛
- (۵) بهره‌گیری از سازمان‌ها و نهادهای غیردولتی و مردم‌نهاد.

نتایج حاصل در ارتباط با سؤال فرعی دوم نشان می‌دهد که بهره‌گیری از دیپلماسی عمومی می‌تواند افکار عموم مردم جهان را تحت تأثیر قرار داده و با تحت فشار قرار دادن دولت‌مردان کشورهای مختلف، انواع تهدیدات از جمله تهدیدات سایبری علیه جمهوری اسلامی ایران را کاهش دهد.

۴-۲. پیشنهادها

برای تأثیرگذاری بیشتر دیپلماسی جمهوری اسلامی ایران در کنترل تهدیدات سایبری موارد زیر پیشنهاد می‌شود:

- (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 تأکید زیادی داشته که نیاز است به منظور کاهش تهدیدات حوزه سایبری بیش‌ازپیش 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 این‌گونه حملات اتخاذ کند؛
- (۵) با توجه به استفاده قشر عظیم جامعه از شبکه‌های اجتماعی و پیام‌رسان‌های خارجی و تهدیداتی که آن شبکه‌ها و پیام‌رسان‌ها می‌توانند داشته باشند مسئولان امر بر ایجاد یک پیام‌رسان بومی واحد و یکپارچه تمرکز کنند تا از تعدد پیام‌رسان‌های ضعیف که با اقبال کمی مواجه هستند اجتناب شود؛
- (۶) نهادهای دولتی و غیردولتی 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 کنند.



فهرست منابع

الف. منابع فارسی

۱. اژدری، لیلا؛ فرهنگ، علی اکبر؛ صالحی امیری، سید رضا؛ سلطانی فر، محمد (۱۳۹۶)، مدل دیپلماسی فرهنگی جمهوری اسلامی ایران، *مطالعات فرهنگ - ارتباطات*، س ۱۸، ش ۳۸.
۲. اسکندری، حمید (۱۳۹۱)، *فرهنگ واژگان موضوعی پدافند غیرعامل*، تهران: بوستان حمید.
۳. بارستون، آر. پی (۱۳۷۹)، *دیپلماسی نوین*، ترجمه محمدجعفر جواد، تهران: دادگستر.
۴. بلیس، جان؛ اسمیت، استیو (۱۳۸۳)، *جهانی شدن سیاست: روابط بین الملل در عصر نوین*، تهران: مؤسسه ابرار معاصر.
۵. توکل، اکبر (۱۳۸۵)، مفهوم جنگ سایبری و کاربرد آن در جنگ آینده، *فصلنامه علوم و فنون نظامی*، ش 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 فضای سایبر بر اساس کلان داده های فضای سایبر، *فصلنامه امنیت ملی*، س ۹، ش ۳۴.
۸. خلیلی پور، علی؛ نورعلی وند، یاسر (۱۳۹۱)، تهدیدات سایبری و تاثیر آن بر امنیت ملی، *فصلنامه مطالعات راهبردی*، ش ۵۶.
۹. رستمی، محمداصداق (۱۳۹۷)، دیپلماسی دفاعی و نقش آن در کنترل تهدیدات سایبری، *فصلنامه دانش انتظامی*، ش ۲۸.
۱۰. ستوده آرانی، محمد؛ علویان، مرتضی (۱۳۹۱)، راهکارهای دیپلماسی عمومی و رسمی ایران در مواجهه با اسلام هراسی غرب، *فصلنامه علوم سیاسی*، س ۱۵، ش ۵۸.
۱۱. شهبازی، آرامش؛ آقاجانی، آیدا (۱۳۹۹)، جاسوسی سایبری در حقوق بین الملل: مسئله انتساب مسئولیت بین المللی به دولت در هاله ای از ابهام، *فصلنامه مطالعات حقوقی عمومی*، زمستان ۱۳۹۹، ش ۴.
۱۲. شیرنگی، سید سعید (۱۳۹۱)، *رویارویی امنیتی ایران و آمریکا در فضای سایبر با تأکید بر نقش آژانس امنیت ملی آمریکا*، دانشگاه امام صادق (ع).
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*، ش ۲۲.

۱۴. عباسی، محمد؛ طالعی حور، رهبر (۱۳۹۷)، *دیپلماسی و حقوق دیپلماتیک و کنسولی در اسلام و غرب*، انتشارات دانشگاه فارابی.
۱۵. قاضوی، سید فضل‌الله؛ زیباکلام، صادق؛ عقیلی، سید وحید (۱۳۹۵)، نقش فضای سایبر در پیشبرد دیپلماسی عمومی مدرن، *فصلنامه رسانه و فرهنگ*، ش ۱۲.
۱۶. کولابی، الهه؛ شکاری، حسن؛ احمدی نیا، مسعود (۱۳۹۲)؛ *دیپلماسی سایبری آمریکا-مطالعه موردی جمهوری آذربایجان، فصلنامه آسیای مرکزی و قفقاز*، ش ۸۲.
۱۷. هالستی کی. جی (۱۳۷۳)، *مبانی تحلیل سیاست بین‌الملل*، ترجمه بهرام مستقیمی و مسعود طارم‌سری، تهران: وزارت امور خارجه.

ب. منابع انگلیسی

1. Shaw(2010), Cybersoace: What Senior Military Leaders Need to Know,<http://handle.dtic.mil/100.2/ADA520146>
2. Wolf, Charles and Brian Rosen, 2004, iPublic diplomacy: How to think about and improve it, Available at: www.rand.org/pubs/occasional_papers/2004/RAND_OP134.pdf, Accessed 15 April 2012.

