Quarterly Journal of Virtual Space and Social Media
Vol. 2, Series. 7, No. 3, Autumn 2025/ 55 - 80
DOI: https://doi.org/10.22083/cssms.2025.499627.1032

Challenges of Cyber Diplomacy in Iran

Seyed Reza Naghibolsadat, *Full Professor, Faculty of Communication Sciences, Allameh Tabataba'i University, Tehran, Iran. Email: naghibsadat@atu.ac.ir*

Extended Abstract

Cyber diplomacy in Iran's political literature is regarded as a key instrument in international relations and in strengthening the country's position at both regional and global levels. This form of diplomacy encompasses a set of activities and strategies that enable the Iranian government to engage with other states in the digital domain and manage cyber threats effectively. Given Iran's geopolitical position and the numerous challenges it faces in the cyber arena-including sanctions and cyberattacks-the necessity of adopting a comprehensive and coordinated approach to cyber diplomacy has become increasingly evident.

This research aims to examine the conceptualization of cyber diplomacy and to analyze the main challenges as well as practical strategies for leveraging it to enhance and expand the country's diplomatic capacity. Employing secondary analysis and a systematic review of prior research, the study adopts a descriptive-analytical approach through library-based methods. In analyzing the challenges and obstacles to Iran's cyber diplomacy, the first major factor identified is sanctions and technological restrictions. These sanctions not only limit access to advanced technologies but also constrain Iran's ability to employ such technologies to strengthen its cyber diplomacy.

The second major obstacle concerns security issues and global cyber threats. Iran has experienced extensive cyberattacks from hacker groups and foreign states in recent years, which has intensified the need to strengthen defensive systems and develop effective strategies to counter such threats. The third challenge relates to the governance of cyberspace. Domestic policies-such as extensive filtering and restrictions on internet accessibility-reduce the country's capacity to engage digitally with other nations and hinder the effective utilization of cyber diplomacy opportunities.

Moreover, one of the most critical challenges is the lack of coordination and internal planning in the implementation of cyber diplomacy. This form of diplomacy should be pursued comprehensively and in coordination among various state institutions, including the Ministry of Foreign Affairs, the Ministry of Communications, security agencies, and private-sector entities. In essence, cyber diplomacy represents not only a necessity for Iran but also a major challenge in the digital era. Countries capable of effectively employing this tool to enhance international relations and counter cyber threats will be able to play more prominent roles in the global system.

In light of these challenges, the cyber diplomacy of the Islamic Republic of Iran requires strategies that integrate defensive measures with international cooperation to strengthen its position at both regional and global levels. Regionally, Iran can enhance its capacity to address cyber threats by forming cyber alliances with neighboring countries and utilizing indigenous capabilities. Establishing common defensive frameworks and supporting technological startups within the region can reduce dependency on foreign technologies. Furthermore, leveraging regional social media platforms to disseminate cultural and political messages will reinforce Iran's soft power among Islamic countries.

At the global level, Iran should seek a more active role in international organizations related to cyberspace, such as the International Telecommunication Union, to increase its influence in shaping global cyber governance regulations. Collaboration with neighboring states and global powers such as Russia and China to promote a multipolar order in cyberspace will further enhance Iran's deterrent capacity. Additionally, academic and technological exchanges with advanced countries, combined with public diplomacy initiatives aimed at improving Iran's international image, can contribute to strengthening the country's global standing. Overall, the integration of defensive strategies and international cooperation, along with the effective use of soft power and local capacities, plays a vital role in advancing Iran's cyber diplomacy. This approach can pave the way for sustainable security and greater influence within the global cyber landscape. Iran thus requires a strategic and coordinated cyber diplomacy framework to seize emerging opportunities and overcome existing challenges.

Keywords: Cyberspace, challenges, cyber diplomacy, Iran, cyber threats.

فصلنامه مطالعات فضای مجازی و رسانه‌های اجتماعی
سال ۲ / شماره ۳/ شماره مسلسل ۷ / پاییز ۱۴۰۴/ ۸۰ - ۵۵
Quarterly Journal of Virtual Space and Social Media
Vol. 2, Series. 7, No. 3, Autumn 2025/ 55 - 80
DOI: https://doi.org/10.22083/cssms.2025.499627.1032

چالش‌های دیپلماسی سایبری در ایران

سیدرضا نقیب‌السادات[1]

چکیده

شناخت دیپلماسی سایبری در ادبیات سیاسی ایران و تحلیل چالش‌های اصلی و راهکارهایی عملی برای بهره‌برداری از دیپلماسی سایبری در جهت توسعه و تقویت دیپلماسی کشور. در این تحقیق با تکنیک تحلیل ثانویه و مرور نظام‌مند دستاوردهای پژوهش‌های پیشین و باتوجه‌به نوع انتظارات مطرح، با شیوه تحلیلی ــ توصیفی و از روش کتابخانه‌ای استفاده می‌شود. در تحلیل چالش‌ها و موانع دیپلماسی سایبری ایران، نخستین عامل مهمی که مطرح می‌شود، تحریم‌ها و محدودیت‌های فناوری است. دومین مانع بزرگ، مسائل امنیتی و تهدیدات سایبری است که کشورها در سطح جهانی با آن مواجه‌اند. ایران در سال‌های اخیر تجربه حملات سایبری گسترده‌ای را از سوی گروه‌های هکری و دولت‌های خارجی داشته است. چالش سوم مربوط به حکمرانی فضای مجازی است. سیاست‌های داخلی مانند فیلترینگ گسترده و محدودیت‌های دردسترس‌بودن اینترنت در ایران، توانایی تعامل با دیگر کشورها در فضای دیجیتال را کاهش داده است. از سوی دیگر، سوم ویکی از مهم‌ترین چالش‌ها، ضعف هماهنگی و برنامه‌ریزی داخلی در اجرای دیپلماسی سایبری است. درحالی‌که دیپلماسی سایبری باید به طور جامع و هماهنگ میان نهادهای مختلف کشور ازجمله وزارت امور خارجه، وزارت ارتباطات، سازمان‌های امنیتی و نهادهای خصوصی صورت گیرد. دیپلماسی سایبری برای ایران نه‌تنها یک ضرورت، بلکه یک چالش بزرگ در دنیای دیجیتال است. کشورهایی که بتوانند به طور مؤثر از این ابزار برای تقویت روابط بین‌المللی و مقابله با تهدیدات سایبری استفاده کنند، قادر خواهند بود نقش مهم‌تری در نظام جهانی ایفا کنند. ایران باتوجه‌به موقعیت ژئوپلیتیکی خود و تهدیدات متعددی که با آن مواجه است، نیازمند یک دیپلماسی سایبری استراتژیک و هماهنگ است تا بتواند از این فرصت‌ها بهره‌برداری کند و موانع موجود را برطرف سازد.

واژگان کلیدی

فضای مجازی، چالش‌ها، دیپلماسی سایبری، ایران، تهدیدات سایبری.

تاریخ دریافت: ۱۴۰۳/۱۰/۲۴ تاریخ پذیرش:۱۴۰۴/۰۵/۱۲

۱. استاد تمام دانشکده علوم ارتباطات دانشگاه علامه طباطبائی، تهران، ایران. naghibsadat@atu.ac.ir

مقدمه

دیپلماسی سایبری به‌عنوان پدیده‌ای نوین و ابزار کلیدی حکمرانی در عصر دیجیتال، جایگاهی برجسته در سیاست‌گذاری و روابط بین‌الملل به خود اختصاص داده است. این مفهوم که در تقاطع فناوری‌های پیشرفته و تعاملات بین‌المللی قرار دارد، نقشی چندوجهی در مدیریت فضای مجازی ایفا می‌کند. دیپلماسی سایبری نه‌تنها برای پیشبرد منافع ملی و ایجاد همکاری‌های جهانی، بلکه برای حفظ امنیت و تقویت حاکمیت دیجیتال کشورها نیز حیاتی است.

ویژگی‌های دیپلماسی سایبری آن را به ابزاری مؤثر و منحصربه‌فرد تبدیل کرده است. انعطاف‌پذیری در مواجهه با مسائل پیچیده، سرعت بالا در واکنش به تهدیدات سایبری، و توانایی تأثیرگذاری بر تصمیم‌گیری‌های بین‌المللی، از جمله نقاط قوت این حوزه محسوب می‌شوند. باوجود این، چالش‌هایی نظیر وابستگی شدید به فناوری‌های نوظهور، تغییرات سریع در ماهیت تهدیدات سایبری و نابرابری دیجیتال میان کشورها، ضرورت پرداختن دقیق و استراتژیک به دیپلماسی سایبری را دوچندان می‌کند.

دیپلماسی سایبری فرصت‌هایی کم‌نظیر برای کشورها فراهم می‌آورد. از ایجاد چارچوب‌های قانونی بین‌المللی برای مدیریت فضای مجازی گرفته تا ارتقای امنیت سایبری و تسریع در پیشرفت فناوری، همه‌وهمه بر اهمیت این حوزه تأکید دارند. بااین‌حال، تهدیداتی نظیر گسترش جنگ‌های سایبری، انتشار اطلاعات نادرست، و سوءاستفاده از فناوری‌ها نیز مخاطراتی جدی به شمار می‌آیند که می‌توانند امنیت جهانی را تهدید کنند.

ضرورت پرداختن به دیپلماسی سایبری از این واقعیت سرچشمه می‌گیرد که فضای مجازی به یکی از عرصه‌های اصلی تعاملات جهانی تبدیل شده است. باتوجه‌به وابستگی روزافزون جوامع و دولت‌ها به فضای مجازی، نبود برنامه‌های راهبردی در این زمینه می‌تواند پیامدهای منفی جدی به همراه داشته باشد. در شرایطی که کشورها با تهدیداتی مانند حملات سایبری به زیرساخت‌های حیاتی، افشای اطلاعات محرمانه، و تأثیرات مخرب اطلاعات جعلی مواجه‌اند، دیپلماسی سایبری می‌تواند ابزاری مؤثر برای مدیریت بحران‌ها و کاهش آسیب‌پذیری‌ها باشد.

درعین‌حال، این حوزه، فرصتی برای شکل‌دهی به نظم جهانی در عصر دیجیتال فراهم می‌کند. دیپلماسی سایبری نه‌تنها ابزاری برای حل مناقشات سایبری و تقویت حاکمیت دیجیتال است، بلکه امکان تعامل سازنده میان کشورها و تأثیرگذاری بر

سیاست‌های جهانی را فراهم می‌سازد. در این میان، بهره‌گیری مناسب از ظرفیت‌های دیپلماسی سایبری می‌تواند گامی اساسی برای توسعه حکمرانی فضای مجازی در کشورها باشد.

این مقاله باهدف شناخت چالش‌های دیپلماسی سایبری در ایران انجام شده است و تلاش می‌کند بامطالعهٔ منابع موجود و با روش کتابخانه‌ای چالش‌های این حوزه را شناسایی و راهکارهایی عملی برای بهره‌برداری مسئولان صاحب‌نظران در جهت توسعه و تقویت سیاسی کشور ارائه دهد. پرداختن به این موضوع نه‌تنها از منظر دیپلماسی عمومی در عرصهٔ حفظ منافع سیاسی کشور و ایجاد امنیت ملی، بلکه به‌عنوان ضرورتی برای توسعهٔ پایدار و مشارکت فعال در نظام بین‌المللی حائز اهمیت است.

سؤال اصلی:

دیپلماسی سایبری درایران دارای چه وضعیتی است؟

سؤال‌های فرعی:

- دیپلماسی سایبری چیست؟ چه مؤلفه‌هایی دارد؟
- قوت‌ها و ضعف‌های دیپلماسی سایبری چیست؟
- فرصت‌ها و تهدیدات دیپلماسی سایبری چیست؟
- امنیت سایبری در کشورهای قدرتمند دنیا دارای چه رویکردهایی است؟
- چالش‌ها و موانع بهره‌گیری از دیپلماسی سایبری در مناسبات کشورها چیست؟
- رویکردهای دیپلماسی سایبری در کشورهای قدرتمند و جایگاه ایران در بین این کشورها چیست؟
- راهکارها و شیوه‌های تقویت دیپلماسی سایبری ایران کدام‌اند؟

پیشینه پژوهش

درمقاله‌ای با عنوان مفهوم‌شناسی و مطالعه تطبیقی دیپلماسی سایبر، دیجیتال و همگرا (با تأکید بر بند هفتم سیاست‌های کلی اطلاع‌رسانی)، نصراللهی و باغبادرانی (۱۴۰۳) به مطالعهٔ تطبیقی دیپلماسی سایبری و دیپلماسی دیجیتال پرداخته‌اند. در این مقاله آمده است: یکی از مهم‌ترین حوزه‌های میان‌رشته‌ای فضای مجازی، ارتباط میان دو حوزه حکمرانی فضای مجازی و دیپلماسی است. نو بودن این حوزه میان‌رشته‌ای و ماهیت پویای هر دو ساحت، سبب بروز نوعی سیالیت، پویایی، عدم استقرار و حتی تشتت در چارچوب مفهومی آن شده است. در این میان دو مفهوم «دیپلماسی دیجیتال» و

«دیپلماسی سایبر» دارای بیشترین بسامد در کاربرد هستند که از عارضه تشتت و خلط مفهومی رنج می‌برند. مسئله این پژوهش ناظر به دو سؤال است:

۱. باتوجه‌به سپهر حکمرانی فضای مجازی مربوط، مرز مفهومی میان دیپلماسی دیجیتال و دیپلماسی چیست؟

۲. در جهت پیوند و همگرایی دیپلماسی دیجیتال و سایبر، مفهوم «دیپلماسی همگرا» در سپهر معرفتی «حکمرانی عصر فضای مجازی» از چه چهارچوبی برخوردار است؟ این پژوهش با روش جمع‌آوری کتابخانه‌ای و روش تحلیل توصیفی ـ تحلیلی انجام شده است. یافته‌ها و نتایج حاصل از پژوهش نشان می‌دهد که دیپلماسی دیجیتال و دیپلماسی سایبر ذیل دو سپهر اندیشه‌ای حکمرانی متفاوت تعریف می‌شوند (حکمرانی «با» فضای مجازی و حکمرانی «بر» فضای مجازی) و براین‌اساس در شاخص‌هایی همچون چیستی، کنشگر، مورد کنش، هدف و نوع حکمرانی تفاوت معنادار دارند. از همین رهگذر، جنبه نوآورانه این پژوهش، پیشنهاد مفهوم «دیپلماسی همگرا» در سپهر حکمرانی «عصر» فضای مجازی است. در دیپلماسی همگرای عصر فضای مجازی، شاهد پیوند و تقارب دیپلماسی سایبر و دیپلماسی دیجیتال هستیم؛ به‌طوری‌که تأثیر و تأثرهای متراکم آن‌ها را شاهد هستیم. بر اساس این چهارچوب مفهومی می‌توان دلالت‌های نظری و سیاستی جدی برای حکمرانی عصر فضای مجازی جمهوری اسلامی پیشنهاد داد (نصراللهی و باغبادرانی، ۱۴۰۳).

همچنین در پژوهشی باعنوان دیپلماسی سایبری آمریکا (مطالعه موردی جمهوری آذربایجان)

نویسندگان کولایی، شکاری، احمدی‌نیا (۱۳۹۲) بر نقش رسانه های جدید بر ظهور کنشگری‌های سیاسی جدید اشاره کرده‌اند. نویسنگان معتقدند، رسانه‌های جدید به سمت سرشت غیرتمرکز خود، زمینهٔ قدرت‌گیری نیروهای حاشیه‌نشین زندگی اجتماعی را افزایش بخشیده‌اند؛ بازیگران کم‌قدرت و بی‌صدای جهانی به عرصهٔ گفتگوهای سیاسی راه یافته‌اند، و زمینهٔ شکل‌گیری سپهرسیاسی در عرصهٔ مجازی و فضای سایبری فراهم شده است. در این مقاله همچنین آمده است:

بروز انقلاب فناوری در اواخر دههٔ ۸۰ میلادی زمینه‌ساز تحولاتی شگرف در حوزهٔارتباطات و رسانه گردید. رسانه‌های دیجیتال که حاصل این انقلاب فناوری بودند، زمینه‌های جدیدی را برای نقش آفرینی بازیگران غیردولتی و مردمی در عرصهٔ

روابـط سیاسـی و دیپلماتیک‌فراهـم کردنـد. بـا شـکل‌گیری شـبکه‌های اجتماعـی، وبـلاگ نویسـی و امـکان اشـتراک‌گذاری ویدئوهـا ازطریـق فضـای مجـازی، سیاسـتگذاران آمریکایـی بـه ایـن نتیجـه رسـیدند کـه از ایـن فناوری‌هـا در راسـتای‌تأمین اهـداف سیاسـت خارجـی و دیپلماسـی خـود اسـتفاده کننـد. انتخـاب بـاراک اوبامـا و تأکیـد او برقـدرت نـرم آمریـکا، توجـه آمریکایی‌هـا را بـه اسـتفاده از ظرفیـت ایـن ابـزار در ترمیـم چهـره بین‌المللـی آمریـکا و همچنیـن حمایـت از نیروهـای همسـو بـا آمریـکا در سراسـر جهـان پیـش رانـد. جمهـوری آذربایجـان از یـک سـو بـه دلیـل داشـتن منابـع انـرژی فسـیلی از اهمیـت اسـتراتژیک‌بالایی در سیاسـت اوراسـیایی آمریـکا برخـوردار اسـت. از سـوی دیگـر، جمعیـت جـوان و علاقه‌منـد به‌شـبکه‌های اجتماعـی دارد کـه نقـش مهمـی در دیپلماسـی سـایبری آمریـکا ایفـا می‌کنند.بـا توجـه بـه آنچـه گفتـه شـد، سـعی نویسـندگان بـر آن اسـت کـه بـه ایـن سـؤال اساسـی پاسـخ دهنـد کـه جنبه‌هـا و جهت‌گیری‌هـای کلـی دیپلماسـی سـایبری آمریـکا چـه هسـتند و چگونـه درجمهـوری آذربایجـان بـه اجـرا گذاشـته می‌شـوند؟(کولایی، شـکاری واحمدی‌نیـا، ۱۳۹۲).

در مقالـه سـایبر دیپلماسـی: ایجـاد یـک جامعـه بین‌المللـی در عصـر دیجیتـال» کـه توسـط آنـدره بارینیـا و تومـاس رنـارد (۲۰۱۷) از دانشـگاه Vrije بروکسـل کـه در دسـامبر ۲۰۱۷ منتشـر شـده اسـت بـه موضـوع دیپلماسـی سـایبری و سـازوکارهای ایجـاد یـک جامعـه واحـد بین‌المللی پرداختـه شـده اسـت. در ایـن مقالـه آمـده اسـت:

فضـای سـایبری به‌کانـون و نقطـه تمرکـز اصلـی روابـط بین‌الملـل تبدیل شـده اسـت. اکثر قدرت‌هـای جهانـی اکنـون مسـائل سـایبری را در سیاسـت‌های خارجـی خـود گنجانده‌انـد، اسـتراتژی‌های سـایبری اتخـاذ کرده‌انـد و دیپلمات‌هـای تعیین‌شـده‌ای را بـرای پیگیـری ایـن اهداف اسـتراتژیک منصوب کرده‌اند. این مقاله با تجزیه‌وتحلیل تکامل دیپلماسـی سـایبری و پیونـد آن بـا مباحـث گسـترده‌تر دیپلماسـی به‌عنوان یک نهاد اساسـی جامعه بین‌المللی، آن‌طور که توسـط دانشـکده روابط بین‌الملل انگلیس تعریف شـده اسـت، مفهوم دیپلماسـی سـایبری را بررسـی کنـد. ایـن مقاله اسـتدلال می‌کند که دیپلماسـی سـایبری یک‌رویـه بین‌المللی نوظهور اسـت کـه در تـلاش بـرای ایجاد یک جامعه سـایبری ــ بین‌المللی اسـت و منافـع ملی دولت‌ها را بـا پویایـی جامعـه جهانـی ــ قلمـرو غالبـی کـه فضـای سـایبری در چهـار دهـه گذشـته در آن تکامـل یافتـه اسـت ــ پیونـد می‌دهـد (Barrinha, Renard, 2017).

در مقالـه‌ای دیگـر باعنـوان «امنیـت سـایبری و دیپلماسـی: هدایـت کشـورداری در عصـر دیجیتـال» عایشـه طریـق (۲۰۲۵) نویسـنده مقالـه بـه تهدیـدات سـایبری بـرای امنیـت بین‌المللـی اشـاره مـی‌کنـد.

و به بررسی تلاقی امنیت سایبری و دیپلماسی، دو حوزه‌ای که در عصر دیجیتال به طور فزاینده‌ای درهم‌تنیده شده‌اند، می‌پردازد. ازآنجایی‌که تهدیدات سایبری خطرات قابل‌توجهی را برای امنیت بین‌المللی ایجاد می‌کنند، چارچوب‌های دیپلماتیک در حال تکامل هستند تا منازعات را مدیریت کنند، هنجارها را برقرار کنند و همکاری را تشویق کنند. این مقاله باتکیه‌بر نظریه‌های واقع‌گرایانه، لیبرال و سازنده‌گرایانه روابط بین‌الملل، تحولات کلیدی در دیپلماسی سایبری، چالش‌هایی مانند انتساب و هوش مصنوعی و عدم حضور کشورهای جنوب جهان را بررسی می‌کند. این مقاله استدلال می‌کند که دیپلماسی سایبری یک ضرورت استراتژیک برای صلح و امنیت جهانی است (Tariq, 2025).

مبانی نظری پژوهش

اگر «دیپلماسی سایبری» را مجموعه سیاست، فناوری اطلاعات و ارتباطات، امنیت سایبری بین‌المللی، گفت و شنودهای دوجانبه سایبری، سیاست توسعه، مسائل اینترنتی، حقوق بشر در عصر سایبری، موضوعات تجارت و مالکیت معنوی تعریف کنیم، می‌توان گفت که این عرصه، حوزه‌ای نوظهور در سطح جهان و به طبع آن بسیار نوپدید در ایران است که ابعاد و عناصر و مؤلفه‌های آن در حال تشکیل و به‌سرعت درحال‌توسعه است. این موضوع در حوزه‌های روابط و دیپلماسی بین‌الملل و سیاست داخلی، فناوری اطلاعات، علوم ارتباطات و حقوق است که بنا بر زاویه‌ای که به این موضوع نگریسته شود، حوزه‌های دانشی دیگر را نیز درگیر مسئله می‌کند.

تاریخچه دیپلماسی سایبری در جهان

شاید نخستین دیپلمات‌های جهان را مبلغین مسیحی در دوران پاپ گرگوری بدانیم که اخبار و اطلاعات هر منطقه از محیط تبلیغی خود را از بریتانیا به واتیکان می‌رساندند. هیئت تبلیغاتی گریگوری یا میسیون آگوستین[1]، یک میسیون مسیحی بود که توسط پاپ گریگوری یکم در سال ۵۹۶ فرستاده شد تا آنگلوساکسون‌های بریتانیا را به دین مسیحیت دربیاورند. این مأموریت توسط آگوستین کانتربری اداره می‌شد. درزمان پاپ کلمنت چهارم که فرستادگان پاپ در سراسر امپراطوری‌ها ضمن تبلیغ مسیحیت، اخبار و اطلاعات آن جا را برای دربار پاپ می‌فرستادند. نمایندگانی هم از کشورهای مختلف به‌عنوان نماینده (دیپلمات) در واتیکان اخبار را برای دولت‌های خودشان می‌فرستادند.

1. Gregorian mission

پیدایـش خبرگزاری‌هـا در طـول تاریـخ بـا عملکـردی فرهنگـی و سیاسـی همـراه بـوده اسـت. ایـن فعالیت‌هـای اطلاع‌رسـانی از زمـان داریـوش شـاه، تـا دیپلمات‌هـای سـال ۶۴۷ خورشـیدی در دربـار پـاپ پـاپ کلمنـت[1] وشـکل گیـری خبرگـزاری هـاواس بـه عنـوان اولیـن خیرگـزاری درجهـان، تاکنـون بـه خوبـی قابـل تبییـن اسـت. تأسـیس نخسـتین شـبکهٔ اطـلاع رسـانی جهـان بـه وسـعت ایـران تـا یونـان، بخشـی از هویـت ملـی ایرانیـان و فرهنـگ آگاهـی بخـش آنـان در دیپلماسـی اسـت. فعالیـت هـای خبرگـزاری هـا در دوران حکومت‌های سـلاطینی ماننـد داریـوش شـاه،پیدایش حاکمیـت ملـی وتعییـن مرزهـای کشـورها پـس از «پیمـان وسـتفالی» و در نظـام روابـط بیـن الملـل پـس از دوران تأسـیس سـازمان ملـل متحـد، نشـان دهنـدهٔ امتـزاج سیاسـت ورسـانه در جهـت سـلطه بـر افـکار عمومـی و پیشـبُرد سیاسـت هـای صاحبـان شـرکت‌های چندملیتـی بـرای ادامـهٔ حیـات سـرمایه در کشـورهای تحت سـلطه اسـت.با پیدایـش خبرگزاری‌هـای اینترنتـی و راه‌انـدازی پایـگاه هـای خبـری اینترنتـی و ظهـور حـدود۵۶۰ شـبکهٔ ماهـواره ای تلویزیونـی، انحصـار خبـری خبرگـزاری هـای بـزرگ غربـی بـه ویـژه خبرگـزاری هـای امریکایـی دچـار شـکنندگی و آسـیب پذیـری شـده اسـت. در ایـن میـان، تـلاش جهـان سـوم و کشـورهای سوسیالیسـتی بـرای مقابلـه بـا سـلطهٔ ارتباطـی غـرب بـه ویـژه در دوران جنـگ سـردو درون سـازمان‌ها و کنفرانس‌هـای بین‌المللـی ماننـد سـازمان ملـل متحـد، سـازمان یونسـکو وکنفرانـس کشـورهای غیرمتعهـد قابـل ارزیابـی و تحسـین اسـت. (مسـعودی، ۱۴۰۳: ۱۱۲). بدین‌ترتیـب بیشـتر مـی تـوان بـه نقـش رسـانه‌های سـایبری در دیپلماسـی جدیـد پـی بـرد.

دیپلماسـی سـایبری به‌عنـوان شـاخه‌ای نوظهـور از دیپلماسـی، در دهه‌هـای اخیـر و بـا گسـترش فنـاوری اطلاعـات و ارتباطـات (ICT[2]) و اهمیـت روزافـزون فضـای مجـازی در تعامـلات بین‌المللـی شـکل گرفتـه اسـت. ریشـه‌های ایـن مفهـوم را می‌تـوان در زمینه‌هـای زیـر جسـتجو کـرد:

۱. شروع توجه به امنیت سایبری (دهه ۱۹۹۰)

بـا رشـد اینترنـت و دیجیتالی‌شـدن جوامـع در دهـه ۱۹۹۰، کشـورها به اهمیت امنیت سـایبری پـی بردنـد. ایـن دوره بـا حمـلات سـایبری اولیـه ماننـد ویـروس موریـس (۱۹۸۸) آغـاز شـد و باعـث شـد دولتمـردان بـرای مقابلـه بـا ایـن تهدیـدات، به‌خصـوص در زیرسـاخت‌های حیاتـی، برنامه‌ریـزی کننـد.

۱. پاپ کلمنت چهارم (به انگلیسی: Clement IV) (تولد:۲۳ نوامبر بین ۱۱۹۰ تا ۱۲۰۰ ــ درگذشت :۲۹ نوامبر۱۲۶۸) یکی ازپاپ‌های کلیسای کاتولیک رم‌بود که درفرانسه‌به دنیا آمد و از۱۲۶۵ تا ۱۲۶۸ میلادی (۶۴۷خورشیدی)پاپ بود.

2. Information Communication Technology

۲. اهمیت فضای مجازی در تعاملات بین‌المللی (دهه ۲۰۰۰)

پس از حمله سایبری به استونی در سال ۲۰۰۷ که به زیرساخت‌های دیجیتال این کشور آسیب زد، توجه جهانی به دیپلماسی سایبری افزایش یافت. این حمله که به روسیه نسبت داده شد، یکی از نخستین مواردی بود که نشان داد تهدیدات سایبری می‌توانند باعث تنش‌های بین‌المللی شوند (Rid, 2013).

۳. تدوین سیاست‌ها و چارچوب‌های بین‌المللی

کشورهایی مانند ایالات متحده و اتحادیه اروپا از اوایل دهه ۲۰۱۰، راهبردهای جامعی برای امنیت و دیپلماسی سایبری تدوین کردند. برای مثال، ایالات متحده در سال ۲۰۱۱، اولین راهبرد بین‌المللی خود در زمینه فضای سایبری را منتشر کرد که بر همکاری بین‌المللی و مدیریت تهدیدات سایبری تمرکز داشت (U.S. Department of State, 2011).

۴. ایجاد نهادهای تخصصی در سازمان‌های بین‌المللی

در این دوره، سازمان ملل متحد و اتحادیه بین‌المللی مخابرات (ITU) به طور رسمی به مسائل فضای سایبری پرداختند و چارچوب‌هایی برای همکاری بین‌المللی در زمینه امنیت سایبری ارائه دادند. تشکیل گروه کاری بین‌المللی در زمینه قوانین استفاده از فضای مجازی در سال ۲۰۱۳ از گام‌های کلیدی بود (UN GGE, 2013).

۵. گسترش دیپلماسی سایبری با ظهور تهدیدات جدید

حملات گسترده‌ای مانند WannaCry (2017) و NotPetya (2017) که به کشورهای مختلف خسارت‌های فراوانی وارد کرد، نشان داد که همکاری سایبری بین‌المللی برای مقابله با جرائم سایبری، جنگ‌های اطلاعاتی و تهدیدات زیرساختی ضرورت دارد. این موضوع نقش دیپلماسی سایبری را در مدیریت بحران‌های سایبری تقویت کرد.

تاریخچه دیپلماسی سایبری در ایران

ایران به دلیل موقعیت استراتژیک و تنش‌های منطقه‌ای و بین‌المللی، به‌طورجدی درگیر مسائل فضای مجازی بوده و در دهه‌های اخیر گام‌هایی در زمینه دیپلماسی سایبری برداشته است:

۱. آغاز توجه به فضای مجازی (دهه ۱۳۸۰)

در دهه ۱۳۸۰ (۲۰۰۰ میلادی)، ایران با گسترش اینترنت و دیجیتالی‌شدن زیرساخت‌ها، به اهمیت فضای مجازی پی برد. حملات سایبری علیه ایران، از جمله ویروس

استاکس‌نت (Stuxnet) در سال ۱۳۸۸ (۲۰۱۰ میلادی)، نشان داد که کشور نیازمند توسعه سیاست‌های امنیت سایبری و استفاده از دیپلماسی سایبری برای مدیریت تهدیدات است (Zetter, 2014).

۲. تدوین سیاست‌ها و اسناد راهبردی

در سال ۱۳۹۰ (۲۰۱۱)، ایران با تشکیل شورای عالی فضای مجازی، تلاش کرد تا سیاست‌گذاری‌های جامعی در زمینهٔ فضای مجازی انجام دهد. این شورا به‌عنوان مرجع اصلی در تصمیم‌گیری‌های کلان فضای مجازی، نقش کلیدی در پیشبرد سیاست‌های سایبری و دیپلماسی سایبری ایفا می‌کند (Supreme Council of Cyberspace, 2011).

۳. گسترش تعاملات بین‌المللی سایبری

ایران در سال‌های اخیر تلاش کرده است تا از طریق مشارکت در نهادهای بین‌المللی، جایگاه خود را در دیپلماسی سایبری تقویت کند. تعاملات ایران درزمینهٔ مسائل حقوقی مرتبط با فضای مجازی در سازمان ملل و اتحادیه بین‌المللی مخابرات نمونه‌هایی از این تلاش‌هاست (ITU, 2016).

۴. استفاده از دیپلماسی سایبری در مذاکرات هسته‌ای

در مذاکرات برجام، دیپلماسی سایبری نقشی غیرمستقیم در مدیریت اطلاعات و دفاع در برابر تهدیدات اطلاعاتی ایفا کرد. همچنین، ایران تلاش کرد تا توانایی خود را در برابر جنگ‌های اطلاعاتی و عملیات روانی تقویت کند (Fathollah-Nejad, 2018).

۵. چالش‌ها و فرصت‌های کنونی

در سال‌های اخیر، ایران با چالش‌های ناشی از تحریم‌ها، جنگ‌های سایبری و تحریم‌های فناوری مواجه بوده است. این چالش‌ها باعث شده تا دیپلماسی سایبری به ابزاری برای مقابله با فشارهای بین‌المللی و تقویت همکاری‌های سایبری با کشورهای دوست تبدیل شود.

دیپلماسی سایبری به‌عنوان یکی از شاخه‌های نوین دیپلماسی، در جهان و ایران باتوجه‌به گسترش تهدیدات سایبری و اهمیت روزافزون فضای مجازی شکل گرفته است. در سطح جهانی، این حوزه با تأکید بر همکاری بین‌المللی، امنیت سایبری و مدیریت بحران‌ها توسعه‌یافته و در ایران نیز با تمرکز بر دفاع از زیرساخت‌های حیاتی و تقویت تعاملات بین‌المللی موردتوجه قرار گرفته است.

مفهوم دیپلماسی

دیپلماسی یکی از مفاهیم کلیدی در روابط بین‌الملل است که به مدیریت صلح‌آمیز روابط میان دولت‌ها و بازیگران بین‌المللی اشاره دارد. این مفهوم در طول تاریخ تعاریف مختلفی یافته است. ساتو (۲۰۱۷) دیپلماسی را به‌عنوان «رهبری و مدیریت روابط رسمی میان دولت‌های مستقل» تعریف کرده است که بیشتر به جنبه‌های سنتی این مفهوم تمرکز دارد. در مقابل، کول (۲۰۰۸) آن را «ارتباط استراتژیک میان بازیگران مختلف در عرصهٔ بین‌المللی» می‌داند که شامل دولت‌ها، سازمان‌های غیردولتی، شرکت‌های چندملیتی و حتی افراد است. این تعریف مدرن‌تر، گستردگی نقش بازیگران در عرصه دیپلماسی را نشان می‌دهد.

دیپلماسی می‌تواند در بسترهای گوناگونی مانند فرهنگی، اقتصادی، عمومی و اخیراً سایبری مطرح شود. نای (۲۰۰۴) بر این باور است که دیپلماسی از جمله ابزارهای نرم‌افزار در سیاست خارجی است که به‌جای اعمال قدرت سخت، از طریق تعاملات سازنده و اقناع منافع ملی را دنبال می‌کند.

ابعاد دیپلماسی نیز گسترده‌اند و شامل دیپلماسی رسمی (بین دولت‌ها)، دیپلماسی غیررسمی (بین سازمان‌ها و افراد) و دیپلماسی چندجانبه (تعامل میان چندین کشور یا سازمان) می‌شوند. کیسنجر (۱۹۹۴) بر این نکته تأکید دارد که دیپلماسی هنری است برای ایجاد تعادل میان منافع متضاد و تأمین صلح و امنیت جهانی.

یکی از اشکال نوین دیپلماسی، دیپلماسی سایبری است که بر تعاملات و مدیریت تهدیدات در فضای مجازی تمرکز دارد. این نوع دیپلماسی به‌عنوان پاسخی به تغییرات فناوری و نیازهای جدید حکمرانی در عصر دیجیتال پدید آمده است (Cull, 2008).

بنابراین، دیپلماسی نه‌تنها ابزاری ارتباطی برای تعاملات بین‌المللی است، بلکه به‌عنوان یک هنر و مهارت برای حفظ منافع ملی و ارتقای صلح جهانی شناخته می‌شود. تحول در تعریف و ابعاد دیپلماسی، نشان‌دهنده اهمیت آن در سیاست جهانی معاصر است.

اشکال دیپلماسی:

دیپلماسی به‌عنوان یکی از ابزارهای کلیدی در روابط بین‌الملل، به اشکال و انواع مختلفی تقسیم می‌شود که هر یک متناسب با اهداف، شرایط و بازیگران مرتبط، نقش خاصی را ایفا می‌کند.

دیپلماسی به‌عنوان یکی از ابزارهای کلیدی در روابط بین‌الملل، به اشکال و انواع

مختلفی تقسیم می‌شود که هر یک متناسب با اهداف، شرایط و بازیگران مرتبط، نقش خاصی را ایفا می‌کند. در ادامه، به عناوین انواع دیپلماسی پرداخته می‌شود:

۱. دیپلماسی سنتی[1] (Satow, 2017)؛
۲. دیپلماسی عمومی[2] (Nye, 2004)؛
۳. دیپلماسی فرهنگی[3] (Cull, 2008)؛
۴. دیپلماسی اقتصادی[4] (Baldwin, 1985)؛
۵. دیپلماسی چندجانبه[5] (Kissinger, 1994)؛
۶ .دیپلماسی دیجیتال[6] (Hanson, 2012)؛
۷. دیپلماسی سایبری[7] (Cull, 2008)؛
۸. دیپلماسی دفاعی[8] (Buzan, 1991)؛
۹. دیپلماسی محیط‌زیستی[9] (Falkner, 2016)؛
۱۰. دیپلماسی انسانی[10] (Barnett & Weiss, 2008)؛
۱۱. دیپلماسی نوآورانه[11] (Hocking, 2016).

۱. مقصود از دیپلماسی سایبری چیست؟

ضمن تأکید بر تعریف بالا و تفاوت‌های بین انواع دیپلماسی که مرزهای بین دیپلماسی سایبری با سایر انواع آن را مشخص می‌کند؛ به ابعاد این دیپلماسی در قالب تعریف زیر می‌پردازیم:

دیپلماسی سایبری به استفاده از فناوری‌های دیجیتال و اینترنت در روابط بین‌المللی و حل‌وفصل مسائل جهانی اشاره دارد. این مفهوم به مجموعه‌ای از تلاش‌های دولت‌ها، سازمان‌های بین‌المللی، و نهادهای غیردولتی برای مدیریت مسائل امنیتی، اقتصادی و اجتماعی در فضای سایبری اختصاص دارد.

1. -Traditional Diplomacy
2. Public Diplomacy
3. Cultural Diplomacy
4. Economic Diplomacy
5. Multilateral Diplomacy
6. Digital Diplomacy
7. Cyber Diplomacy
8. Defense Diplomacy
9. Environmental Diplomacy
10. Humanitarian Diplomacy
11. Innovation Diplomacy

دیپلماسی سایبری شامل جنبه‌های مختلفی است:

- مدیریت اختلافات سایبری: شامل پیشگیری و حل مناقشات ناشی از حملات سایبری؛
- تدوین قوانین بین‌المللی: تنظیم قوانین و پروتکل‌های بین‌المللی برای تعاملات در فضای سایبری؛
- تقویت امنیت سایبری: از طریق همکاری‌های بین‌المللی برای کاهش آسیب‌پذیری‌ها؛
- ترویج ارزش‌ها و منافع ملی در فضای مجازی: از جمله نفوذ فرهنگی و اقتصادی از طریق فضای دیجیتال.

تعاریف دیپلماسی سایبری در منابع معتبر:

۱. تعریف دیپلماسی سایبری به‌عنوان ابزاری برای ارتباطات بین‌المللی دیجیتال: بر اساس کَری و سایمون (۲۰۲۰)، دیپلماسی سایبری استفاده از اینترنت و ابزارهای دیجیتال برای تسهیل روابط بین‌المللی، افزایش شفافیت و کاهش تنش‌ها میان دولت‌ها است (Carr & Simon, 2020)؛

۲. تعریف دیپلماسی سایبری در چارچوب امنیت بین‌المللی: به گفته کانسولو و همکاران (۲۰۱۸)، دیپلماسی سایبری فرایندی است که از طریق آن دولت‌ها و سازمان‌ها برای ایجاد یک چارچوب قانونی بین‌المللی همکاری می‌کنند تا امنیت سایبری جهانی تضمین شود (Consuelo et al., 2018)؛

۳. دیپلماسی سایبری به‌عنوان سازوکار حل‌وفصل بحران‌های سایبری: بر اساس لیندسی (۲۰۱۳)، دیپلماسی سایبری می‌تواند ابزاری برای مذاکره و کاهش بحران‌های ناشی از حملات سایبری میان دولت‌ها باشد (Lindsay, 2013)؛

۴. دیپلماسی سایبری در چارچوب دیپلماسی عمومی: آسوی و همکاران (۲۰۱۹) دیپلماسی سایبری را ابزاری برای دیپلماسی عمومی تعریف می‌کنند که به طور مستقیم با افکار عمومی بین‌المللی در فضای دیجیتال تعامل می‌کند (Asi et al., 2019).

ویژگی‌های دیپلماسی سایبری به شرح زیر است:

۱. وابستگی به فناوری اطلاعات و ارتباطات (ICT)

دیپلماسی سایبری به‌شدت وابسته به زیرساخت‌های فناوری اطلاعات است. اینترنت، شبکه‌های اجتماعی، و ابزارهای ارتباطی دیجیتال ابزارهای کلیدی این نوع دیپلماسی هستند .

چندبعدی بودن

دیپلماسی سایبری از یک سو در برگیرندهٔ تعاملات میان دولت‌ها (G2G) و از سوی دیگر شامل تعاملات میان دولت‌ها و بازیگران غیردولتی مانند سازمان‌های مردم‌نهاد، شرکت‌های فناوری، و کاربران عادی اینترنت می‌شود.

۲. سرعت بالا در انتقال پیام‌ها و تعاملات

به دلیل ماهیت دیجیتال، تعاملات در دیپلماسی سایبری با سرعت بالایی انجام می‌شود. این ویژگی باعث می‌شود تصمیم‌گیری‌ها نیز باید سریع و هم‌زمان با تغییرات در فضای سایبری باشد.

غیرمتمرکز بودن

برخلاف دیپلماسی سنتی که معمولاً توسط دولت‌ها و سفارتخانه‌ها کنترل می‌شود، دیپلماسی سایبری بازیگران متنوعی از جمله افراد، شرکت‌های فناوری و سازمان‌های غیردولتی را درگیر می‌کند.

تعامل در محیطی با قوانین ناپایدار و درحال‌توسعه

در دیپلماسی سایبری، تعاملات در فضایی رخ می‌دهد که قوانین و مقررات بین‌المللی سایبری هنوز به طور کامل شکل نگرفته و درحال‌توسعه هستند. این موضوع باعث می‌شود این نوع دیپلماسی بسیار پیچیده باشد.

تمرکز بر امنیت و حاکمیت سایبری

حفاظت از زیرساخت‌های حیاتی سایبری و تأمین امنیت داده‌ها از محورهای اصلی دیپلماسی سایبری است. این ویژگی شامل تلاش برای جلوگیری از حملات سایبری و تضمین حاکمیت ملی در فضای مجازی است.

۷. ماهیت جهانی و فراملی

دیپلماسی سایبری اغلب از مرزهای جغرافیایی فراتر می‌رود و به مسائل جهانی می‌پردازد. این ویژگی باعث می‌شود که همکاری‌های بین‌المللی در آن نقش مهمی ایفا کند.

۸. شفافیت و تعامل عمومی

این نوع دیپلماسی در بسیاری از موارد از شفافیت و تعامل عمومی برای جلب‌اعتماد عمومی استفاده می‌کند. پلتفرم‌های دیجیتال امکان برقراری ارتباط مستقیم با مردم را فراهم می‌کنند.

۹. چالش‌پذیری بالا در برابر تهدیدات سایبری

ازآنجاکه تعاملات در فضای سایبری مستعد حملات سایبری و نفوذ است، دیپلماسی سایبری نیاز به تدابیر امنیتی خاصی دارد.

روش پژوهش

باتوجه‌به نوع انتظارات مطرح در این پژوهش که فرا تحلیل از نوع با تکنیک تحلیل ثانویه است. از روش تحلیلی ـ توصیفی استفاده می‌شود:

یافته‌های پژوهش

در این بخش برای ارائه پاسخ به سؤالات تحقیق به بررسی یافته‌های پژوهش می‌پردازیم.

ـ دیپلماسی سایبری چیست؟ چه مؤلفه‌هایی دارد؟

دیپلماسی سایبری به معنای استفاده از فضای دیجیتال و فناوری‌های نوین ارتباطی به‌منظور مدیریت روابط بین‌المللی و سیاست خارجی است. این نوع دیپلماسی به کشورها این امکان را می‌دهد که از ابزارهای فناوری اطلاعات و ارتباطات (ICT) برای تعامل، تبادل اطلاعات، مذاکره و حل اختلافات استفاده کنند، به‌ویژه در زمینه‌هایی مانند امنیت سایبری، حقوق بشر دیجیتال، و حکمرانی فضای مجازی. دیپلماسی سایبری به‌طورکلی در چهار حوزهٔ اصلی یعنی سیاسی، اقتصادی، اجتماعی و امنیتی تأثیرگذار است.

مؤلفه‌های دیپلماسی سایبری

۱. امنیت سایبری: یکی از مهم‌ترین مؤلفه‌های دیپلماسی سایبری، مدیریت تهدیدات و بحران‌های سایبری است. کشورها از طریق دیپلماسی سایبری می‌توانند به هماهنگی‌های بین‌المللی دست یابند تا تهدیدات سایبری همچون حملات هکری، جاسوسی دیجیتال، و خرابکاری‌های سایبری را کاهش دهند.

۲. حقوق بشر دیجیتال: در سطح جهانی، دیپلماسی سایبری به حفظ و توسعه حقوق بشر در فضای مجازی کمک می‌کند. این حقوق شامل آزادی بیان، حریم خصوصی آنلاین، و دسترسی به اطلاعات است.

۳. حکمرانی فضای مجازی: دیپلماسی سایبری در این مؤلفه به کشورها کمک می‌کند تا نقش خود را در حکمرانی فضای مجازی تقویت کرده و در فرایندهایی

چـون تدویـن اسـتانداردهای بین‌المللـی، نظـارت و مدیریـت فضـای دیجیتـال مشـارکت کننـد.

۴. دیپلماسـی عمومـی دیجیتـال: ایـن بخـش از دیپلماسـی سـایبری بـه اسـتفاده از رسـانه‌های دیجیتـال و فضـای مجـازی بـرای ارتقـای تصویـر و منافـع ملی کشـورها در عرصـه جهانـی اختصـاص دارد. ابزارهایـی ماننـد شـبکه‌های اجتماعـی و وب‌سـایت‌های دولتی بـه کشـورها ایـن امکان را می‌دهنـد کـه مواضـع سیاسـی خـود را در سـطح جهانـی اعـلام کننـد.

۵. همکاری‌هـای بین‌المللـی: در دیپلماسـی سـایبری، کشـورهای مختلـف به‌صـورت همکاری‌هـای دوجانبـه و چندجانبـه بـه تبـادل اطلاعـات، تجـارب و فناوری‌هـای سـایبری پرداختـه و در برابـر تهدیـدات سـایبری یکدیگـر را حمایـت می‌کننـد. ایـن همکاری‌هـا می‌توانـد شـامل توافقـات امنیـت سـایبری، آموزش‌هـای مشـترک و اقدامـات هماهنـگ در مواقـع بحـران باشـد.

۶. اقتصـاد دیجیتـال: دیپلماسـی سـایبری بـه تقویـت همکاری‌هـای اقتصـادی از طریـق فضـای مجـازی نیـز پرداختـه و بـه کشـورهای مختلـف کمـک می‌کنـد تـا تجـارت آنلایـن و فعالیت‌هـای دیجیتـال را تسـهیل کننـد. ایـن مؤلفـه شـامل مبـارزه بـا جرائـم اقتصـادی دیجیتـال، قاچـاق داده‌هـا و توسـعه خدمـات مالـی آنلایـن می‌شـود.

جدول ۱. قوت‌ها و ضعف‌ها؛ فرصت‌ها و تهدیدهای دیپلماسی سایبری

بخش	قوت‌ها	ضعف‌ها	فرصت‌ها	تهدیدات
۱. دیپلماسی سایبری و حکمرانی جهانی	ـ افزایش تعاملات جهانی و استفاده از فضای سایبری برای گفت‌وگو و تعاملات دیپلماتیک. ـ ایجاد همکاری‌های بین‌المللی در راستای امنیت و بحران‌های سایبری.	ـ کمبود استانداردهای بین‌المللی در زمینه دیپلماسی سایبری. ـ چالش‌های نظارتی بر فضای سایبری و اطلاعات.	ـ تقویت حکمرانی جهانی فضای مجازی از طریق توافقات بین‌المللی. ـ ایجاد چارچوب‌های مشترک برای نظارت و امنیت سایبری در سطح جهانی.	ـ تهدیدات سایبری از جمله حملات اطلاعاتی و سایبری در سطح جهانی. ـ دستکاری اطلاعات و انتشار اخبار جعلی توسط کشورهای مختلف.

بخش	قوت‌ها	ضعف‌ها	فرصت‌ها	تهدیدات
۲. دیپلماسی سایبری و امنیت سایبری	ـ بهبود کارایی در مقابله با تهدیدات سایبری و بحران‌های امنیتی. ـ توانایی دولت‌ها در استفاده از فناوری برای مدیریت بحران‌های سایبری.	ـ اختلافات در رویکردهای امنیت سایبری کشورهای مختلف و نبود هماهنگی کافی. ـ ضعف در تامین زیرساخت‌های امنیتی مناسب در برخی کشورها.	ـ افزایش امنیت سایبری در سطح بین‌المللی از طریق همکاری‌های مشترک. ـ استفاده از فضای سایبری برای آموزش و آگاهی‌رسانی در حوزه امنیت.	ـ حملات سایبری علیه زیرساخت‌های دولتی و غیر دولتی. ـ استفاده از فضای سایبری برای عملیات‌های خرابکارانه.
۳. دیپلماسی سایبری و دیپلماسی عمومی	ـ تقویت دیپلماسی عمومی از طریق فضای مجازی و رسانه‌های اجتماعی. ـ بهبود تصویر جهانی کشورهای مختلف از طریق دیپلماسی سایبری.	ـ بحران‌های اطلاعاتی و چالش‌های فنی در استفاده از ابزارهای دیجیتال در دیپلماسی عمومی.	ـ ارتقاء دیپلماسی عمومی و معرفی سیاست‌های خارجی از طریق پلتفرم‌های آنلاین. ـ استفاده از فضای مجازی برای گسترش همکاری‌های فرهنگی و علمی.	ـ تهدیدات مرتبط با جاسوسی اطلاعاتی و سوءاستفاده از داده‌های شخصی در فضای مجازی. ـ دستکاری افکار عمومی از طریق اطلاعات نادرست و تبلیغات.
۴. دیپلماسی سایبری و امنیت اطلاعات	ـ توانمندسازی کشورها در مقابله با تهدیدات امنیتی سایبری از طریق دیپلماسی سایبری.	ـ چالش‌های مدیریتی و نظارتی در حفظ امنیت داده‌ها در فضای سایبری.	ـ ارتقاء ظرفیت‌های فناوری اطلاعات و ارتباطات برای مقابله با تهدیدات امنیتی.	ـ تهدیدات ناشی از حملات سایبری سازمان‌یافته علیه زیرساخت‌های حساس اطلاعاتی.

(منبع:محقق)

در جدول شماره ۱ چهار موضوع مهم حکمرانی،امنیت، دیپلماسی سایبر وعمومی وامنیت اطلاعات، بیانگر قوت‌ها، تهدیدها، ضعف ها وفرصت ها است.

جدول ۲. رویکردهای امنیت سایبری در کشورهای قدرتمند دنیا

کشور	رویکردها	اهداف
آمریکا	استفاده از قدرت سایبری برای مداخله و تأثیرگذاری در دیگر کشورها؛ ایجاد چارچوب‌های بین‌المللی.	گسترش نفوذ جهانی و تأمین امنیت سایبری ملی.
چین	توسعه حکمرانی سایبری داخلی و تأثیرگذاری اقتصادی از طریق دیپلماسی سایبری.	تقویت نفوذ اقتصادی و سیاسی جهانی.
روسیه	ایجاد چارچوب‌های بی‌طرفی در فضای سایبری و مقابله با هژمونی آمریکا.	مدیریت حکمرانی جهانی فضای مجازی.

در جدول شماره ۲ بیانگر این مطلب است که دیپلماسی سایبری به‌عنوان ابزار نوین سیاست خارجی، نقش کلیدی در مدیریت مسائل بین‌المللی فضای مجازی دارد. این حوزه نیازمند هماهنگی بین‌المللی و تعامل میان دولت‌ها برای دستیابی به امنیت و نظم در اینترنت جهانی است. برای کشورهای در حال توسعه، تمرکز بر سیاست‌های دفاعی و توسعه چارچوب‌های حقوقی ملی ضروری است.

رویکردهای دیپلماسی سایبری در کشورهای قدرتمند و جایگاه ایران در بین این کشورها چیست؟

جدول ۳. مقایسه‌ای رویکرد دیپلماسی سایبری در کشورهای منتخب (با اضافه‌شدن ایران و انگلستان)

کشور	رویکردها	اهداف
آمریکا	استفاده از قدرت سایبری برای مداخله و تأثیرگذاری در دیگر کشورها؛ ایجاد چارچوب‌های بین‌المللی.	گسترش نفوذ جهانی و تأمین امنیت سایبری ملی.
چین	توسعه حکمرانی سایبری داخلی و تأثیرگذاری اقتصادی از طریق دیپلماسی سایبری.	تقویت نفوذ اقتصادی و سیاسی جهانی.
روسیه	ایجاد چارچوب‌های بی‌طرفی در فضای سایبری و مقابله با هژمونی آمریکا.	مدیریت حکمرانی جهانی فضای مجازی.
انگلستان	استفاده از دیپلماسی سایبری برای هماهنگی بین‌المللی و تقویت همکاری‌های اروپایی در امنیت سایبری.	افزایش همکاری‌های بین‌المللی و تأمین امنیت ملی و بین‌المللی.
ایران	تمرکز بر دفاع سایبری؛ مقابله با مداخلات سایبری خارجی؛ بهره‌گیری از دیپلماسی سایبری برای دفاع از حاکمیت ملی.	تأمین امنیت ملی؛ جلوگیری از تهاجم سایبری.

بر اساس منابع ارزیابی شده در جدول ۳ رویکردکشورمان به شرح زیر است:

کشور ما رویکردی دفاعی در دیپلماسی سایبری اتخاذ کرده است که شامل توسعه زیرساخت‌های امنیت سایبری و مقابله با حملات سایبری خارجی می‌شود. از دیپلماسی سایبری برای تقویت حاکمیت ملی در فضای مجازی و مقابله با جنگ نرم دشمنان استفاده می شود.

چالش‌های اصلی در این عرصه به شرح زیر است:

تحریم‌های اقتصادی و فناوری، عدم دسترسی به برخی ابزارهای بین‌المللی همکاری در حوزهٔ سایبری و تهدیدات مستمر از سوی کشورهایی مانند آمریکا.

چالش‌ها و موانع بهره‌گیری از دیپلماسی سایبری کشورمان در مناسبات بین‌المللی در قالب جدول آورده شده است:

جدول ۴. چالش‌ها و موانع بهره‌گیری از دیپلماسی سایبری درایران

چالش/مانع	توضیحات
تحریم‌های بین‌المللی و محدودیت‌های فناوری	ـ محدودیت‌های دسترسی به فناوری‌های نوین. ـ محدودیت‌های دسترسی به پلتفرم‌های دیجیتال جهانی مانند گوگل، توییتر، فیس‌بوک به دلیل تحریم‌ها یا سیاست‌های فیلترینگ.
سختی در دستیابی به اعتماد بین‌المللی	ـ شکاف‌های سیاسی و ایدئولوژیک بین ایران و برخی کشورهای غربی. ـ رکود در ایجاد مکانیزم‌های مشترک برای همکاری‌های سایبری با دیگر کشورها.
امنیت سایبری و تهدیدات	ـ تهدیدات سایبری متقابل از سوی دیگر کشورها مانند حملات هکری و جاسوسی سایبری. ـ ضعف در زیرساخت‌های امنیتی و فقدان نیروی انسانی ماهر در حوزه سایبری.
چالش‌های حکمرانی فضای مجازی	ـ محدودیت‌های داخلی در حکمرانی فضای مجازی مانند سیاست‌های فیلترینگ. ـ نیاز به تنظیم قوانین دیجیتال با توجه به تحولات جهانی.
فیلترینگ و محدودیت‌های داخلی	ـ سیاست‌های فیلترینگ در داخل کشور که مانع از تعاملات بین‌المللی در فضای سایبری می‌شود. ـ کاهش مشارکت ایران در ابتکارات جهانی حکمرانی سایبری.
موانع اقتصادی و منابع محدود	ـ کمبود منابع مالی برای توسعه دیپلماسی سایبری و زیرساخت‌های مرتبط. ـ وابستگی به منابع خارجی برای تأمین نرم‌افزارها و خدمات کلیدی.
ضعف در رویکردهای هماهنگ داخلی	ـ عدم هماهنگی بین نهادهای دولتی، امنیتی و خصوصی در سیاست‌گذاری و اجرای دیپلماسی سایبری.
چالش‌های فرهنگی و اجتماعی	ـ تفاوت‌های فرهنگی در تعاملات دیجیتال، به‌ویژه در زمینه حریم خصوصی، آزادی بیان و حقوق بشر.

در جدول ۴ نمای کلی از چالش‌ها و موانع استفاده از دیپلماسی سایبری در کشور است که بر اساس ویژگی‌های فضای سایبری، سیاست‌های داخلی و خارجی و محدودیت‌های موجود در این حوزه بر اساس منابع واسناد ومدارک مورد ارزیابی تنظیم شده است.

راهکارها و شیوه‌های تقویت دیپلماسی سایبری ایران کدام‌اند؟

جدول ۵. راهکارها و شیوه‌های تقویت دیپلماسی سایبری ایران

شیوه‌ها و راهکارها	سطح منطقه‌ای	سطح جهانی
۱. ایجاد اتحادهای سایبری	ـ تشکیل اتحادیه‌های سایبری با کشورهای همسایه (عراق، پاکستان، ترکیه)	ـ همکاری با قدرت‌های جهانی (چین و روسیه) برای ایجاد نظم چندقطبی در حکمرانی فضای مجازی.
۲. تقویت قدرت نرم سایبری	ـ استفاده از شبکه‌های اجتماعی برای تقویت پیام‌های فرهنگی و سیاسی در منطقه.	ـ توسعه محتوا و برنامه‌های سایبری برای افزایش تصویر ایران در مجامع جهانی.
۳. حمایت از توانمندی‌های بومی	ـ حمایت از استارتاپ‌های فناوری منطقه‌ای برای تولید نرم‌افزارها و ابزارهای بومی.	ـ ایجاد روابط علمی و فناوری با کشورهای پیشرفته در زمینه سایبری (چین، اتحادیه اروپا)
۴. حضور در نهادهای بین‌المللی	ـ مشارکت در سازمان‌های منطقه‌ای مرتبط با فناوری و سایبری (مانند سازمان همکاری اقتصادی)	ـ تقویت نقش ایران در نهادهای بین‌المللی مانند ITU و مشارکت در تدوین استانداردهای جهانی.
۵. بازدارندگی سایبری	ـ ایجاد چارچوب‌های دفاعی مشترک با کشورهای منطقه برای مقابله با تهدیدات سایبری.	ـ تقویت توانمندی‌های بازدارنده و تدوین سیاست‌های واکنش سریع برای پاسخ به تهدیدات جهانی.
۶. توسعه حکمرانی فضای مجازی	ـ همکاری برای تدوین قوانین مشترک در حکمرانی فضای مجازی منطقه‌ای.	ـ مشارکت در مذاکرات جهانی برای تدوین چارچوب‌های حقوقی حکمرانی فضای مجازی.
۷. آموزش و ظرفیت‌سازی	ـ آموزش نیروهای متخصص سایبری در کشورهای همسایه با مشارکت ایران.	ـ تبادل علمی و فناوری با کشورهای پیشرفته و شرکت در کنفرانس‌های بین‌المللی سایبری.
۸. استفاده از دیپلماسی عمومی	ـ بهره‌گیری از رسانه‌های منطقه‌ای برای انتقال پیام‌های سیاسی و فرهنگی.	ـ استفاده از ابزارهای دیپلماسی عمومی برای ارتباط با جوامع جهانی و تقویت تصویر ایران.

برای تقویت دیپلماسی سایبری کشورمان بر اساس جدول ۵ باید در دوسطح عمل کنیم: در سطح منطقه‌ای: جمهوری اسلامی ایران باید بر توسعهٔ همکاری‌های سایبری با کشورهای همسایه و تقویت توانمندی‌های بومی تمرکز کند.

در سطح جهانی: تعامل با قدرت‌های بزرگ، حضور فعال در نهادهای بین‌المللی و توسعه توان بازدارندگی از اولویت‌های جمهوری اسلامی ایران می‌تواند باشد.

نتیجه‌گیری

در این پژوهش، به بررسی چالش‌های دیپلماسی سایبری؛ ابعاد، ویژگی‌ها، ضعف‌ها، قوت‌ها، فرصت‌ها و تهدیدات و چالش‌ها و موانع بهره‌گیری از آن در روابط بین‌الملل کشورمان پرداخته شد. دیپلماسی سایبری به‌عنوان یک مفهوم نوظهور، توانسته است تأثیرات چشمگیری در نحوه تعاملات بین‌المللی کشورها ایجاد کند. این نوع دیپلماسی نه‌تنها به دلیل اهمیت روزافزون فضای مجازی و فناوری اطلاعات در سیاست‌های جهانی به‌ویژه در دوران معاصر مطرح شده است، بلکه به دلیل تهدیدات جدید و پیچیده‌ای که در سطح جهانی در حال گسترش هستند، توجه ویژه‌ای را به خود جلب کرده است. دیپلماسی سایبری به دولت‌ها این امکان را می‌دهد که با بهره‌گیری از ابزارهای دیجیتال، منافع ملی خود را در فضای مجازی تقویت کنند و با کشورها و نهادهای بین‌المللی در سطح سایبری تعامل داشته باشند.

در تحلیل چالش‌ها و موانع دیپلماسی سایبری ایران، نخستین عامل مهمی که مطرح می‌شود، تحریم‌ها و محدودیت‌های فناوری است. تحریم‌های اقتصادی و سیاسی که به‌ویژه ایران را هدف قرار داده‌اند، نه‌تنها بر دسترسی به تکنولوژی‌های پیشرفته و زیرساخت‌های دیجیتال تأثیر گذاشته‌اند، بلکه سبب شده‌اند که کشورمان در برقراری روابط سایبری با دیگر کشورها با مشکلات فراوانی مواجه شود. این تحریم‌ها محدودیت‌های شدیدی را در زمینه استفاده از خدمات آنلاین و پلتفرم‌های دیجیتال به وجود آورده و مانع از دسترسی به اطلاعات جهانی می‌شود.

دومین مانع بزرگ، مسائل امنیتی و تهدیدات سایبری است که کشورها در سطح جهانی با آن مواجه‌اند. ایران در سال‌های اخیر تجربه حملات سایبری گسترده‌ای را از سوی گروه‌های هکری و دولت‌های خارجی داشته است. این تهدیدات نه‌تنها منجر به آسیب‌های مالی و اطلاعاتی به کشور می‌شود، بلکه بر اعتبار دیپلماسی سایبری ایران در سطح جهانی تأثیر منفی می‌گذارد.

چالش دیگر مربوط به حکمرانی فضای مجازی است. سیاست‌های داخلی مانند فیلترینگ گسترده و محدودیت‌های دردسترس‌بودن اینترنت در ایران، توانایی تعامل با دیگر کشورها در فضای دیجیتال را کاهش داده است. این موانع باعث می‌شود که

ایـران نتوانـد بـه طـور مؤثـر در پروژه‌هـای جهانـی حکمرانـی سـایبری شـرکت کـرده و از مزایـای همکاری‌هـای بین‌المللـی بهره‌منـد شـود.

از سـوی دیگـر، یکـی از مهم‌تریـن چالش‌هـا، ضعـف هماهنگـی و برنامه‌ریـزی داخلـی در اجـرای دیپلماسـی سـایبری اسـت. درحالی‌کـه دیپلماسـی سـایبری بایـد بـه طـور جامـع و هماهنـگ میـان نهادهـای مختلـف کشـور از جملـه وزارت امـور خارجـه، وزارت ارتباطـات، سـازمان‌های امنیتـی و نهادهـای خصوصـی صـورت گیـرد، نبـود اسـتراتژی‌های منسـجم و برنامه‌ریزی‌هـای کلان باعـث کاهـش اثربخشـی ایـن دیپلماسـی می‌شـود. بـدون هم‌افزایـی و هماهنگـی بیـن ایـن نهادهـا، امـکان بهره‌بـرداری از فرصت‌هـای سـایبری و مقابلـه بـا تهدیـدات در سـطح جهانـی بـه طـور مؤثـر وجـود نخواهـد داشـت.

در نتیجه‌گیـری، دیپلماسـی سـایبری بـرای ایـران نه‌تنهـا یـک ضـرورت، بلکـه یـک چالـش بـزرگ در دنیـای دیجیتـال اسـت. کشـورهایی کـه بتواننـد به طـور مؤثر از این ابـزار برای تقویت روابـط بین‌المللی و مقابله با تهدیدات سـایبری اسـتفاده کنند، قـادر خواهند بود نقش مهم‌تری در نظـام جهانـی ایفـا کننـد. ایـران باتوجه‌به موقعیـت ژئوپلیتیکی خـود و تهدیـدات متعددی که با آن مواجه اسـت، نیازمند یک دیپلماسـی سـایبری اسـتراتژیک و هماهنگ اسـت تا بتواند از ایـن فرصت‌هـا بهره‌بـرداری کنـد و موانـع موجود را برطرف سـازد.

پیشنهادها

دیپلماسـی سـایبری جمهـوری اسـلامی ایـران در تقویـت جایـگاه خـود در سـطح منطقـه‌ای و جهانـی نیازمنـد راهکارهایـی اسـت کـه هم‌زمـان بُعـد دفاعـی و همکاری‌هـای بین‌المللـی را پوشـش دهـد. در سـطح منطقـه‌ای، ایـران می‌توانـد بـا تشـکیل اتحادهـای سـایبری بـا کشـورهای همسـایه و بهره‌گیـری از ظرفیت‌هـای بومـی، توانمندی‌هـای خـود را بـرای مقابلـه بـا تهدیـدات سـایبری ارتقـا دهـد. ایجـاد چارچوب‌هـای دفاعـی مشـترک و حمایـت از اسـتارتاپ‌های فنـاوری در منطقـه، زمینـه را بـرای کاهـش وابسـتگی بـه فناوری‌هـای خارجـی فراهـم می‌کنـد. همچنیـن، اسـتفاده از شـبکه‌های اجتماعـی منطقـه‌ای بـرای گسـترش پیام‌هـای فرهنگـی و سیاسـی، قـدرت نـرم ایـران را در میـان کشـورهای اسـلامی تقویـت می‌کنـد.

در سـطح جهانـی، ایـران بایـد حضـور فعال‌تـری در نهادهـای بین‌المللـی مرتبـط بـا فضـای مجـازی ماننـد اتحادیـه بین‌المللـی ارتباطـات دور[1] داشـته باشـد و نقـش خـود را در تدویـن قوانیـن جهانـی حکمرانـی فضـای سـایبری افزایـش دهـد. همـکاری بـا همسـایگان،

1. ITU

قدرت‌های جهانی؛ مانند روسیه و چین در ایجاد نظم چندقطبی در فضای سایبری، توانمندی‌های بازدارنده ایران را تقویت می‌کند. همچنین، تبادل علمی و فناوری با کشورهای پیشرفته و استفاده از دیپلماسی عمومی برای بهبود تصویر بین‌المللی ایران می‌تواند به تقویت جایگاه جهانی کشور کمک کند.

به‌طورکلی، راهبردهای ترکیبی دفاعی و همکاری بین‌المللی، به همراه بهره‌گیری از قدرت نرم و ظرفیت‌های بومی، نقشی کلیدی در تقویت دیپلماسی سایبری ایران ایفا می‌کنند. این رویکرد می‌تواند زمینه‌ساز امنیت پایدار و تأثیرگذاری بیشتر در فضای سایبری جهانی باشد.

تعارض منافع

تعارض منافع ندارم.

منابع و مأخذ

زینلی، سجاد و مجید پارسا (۲۰۲۰). تحلیل سیاست‌های دیپلماسی سایبری جمهوری اسلامی ایران. *فصلنامه سیاست خارجی*، ۳۱(۲)، ۴۵ـ۵۹.

شیری، محسن و محمد نیکوئی (۲۰۱۹). *دیپلماسی سایبری و امنیت ملی در ایران: چالش‌ها و فرصت‌ها*. نشریه مطالعات امنیت ملی، ۲۲(۴)، ۶۵ـ۸۰.

مسعودی، امیدعلی (۱۴۰۳). واکاوی نقش فرهنگی و سیاسی ایران در روند تکاملی اطلاع‌رسانی اروپاییان. *پژوهشنامه دیپلماسی فرهنگی*، ۱(۳)، ۹۵ـ۱۱۴. https://doi.org/10.22034/cdrj.2024.473343.1013

کولایی، الهه؛ حسن‌شکاری، حسن و مسعود احمدی‌نیا (۱۳۹۲). دیپلماسی سایبری آمریکا (مطالعه موردی جمهوری آذربایجان). *فصلنامه علمی مطالعات آسیای مرکزی و قفقاز*، ۱۹(۸۲)، ۸۱ـ۱۰۱.

نصراللهی، محمدصادق و احسان امینی باغبادرانی (۱۴۰۳). مفهوم‌شناسی و مطالعه تطبیقی دیپلماسی سایبر، دیجیتال و همگرا (با تأکید بر بند هفتم سیاست‌های کلی اطلاع‌رسانی). *راهبرد اجتماعی فرهنگی*، ۱۳(۲)، ۵۱۱ـ۵۵۰. doi: 10.22034/scs.2023.411493.1479

Abertay University Research Archive. (2020). *Cyber diplomacy: A systematic literature review*. Retrieved from https://www.abertay.ac.uk/research

Asi, N., & Coauthors. (2019). Cyber diplomacy in the digital age: Public diplomacy in cyberspace. *Journal of International Affairs, 35*(2), 45-67.

Baldwin, D. A. (1985). *Economic statecraft*. Princeton University Press.

Barrinha, André, & Renard, Thomas. (2017). Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs, 3*(4-5), 1-12. https://doi.org/10.1080/23340460.2017.1414924

Buzan, B. (1991). *People, states and fear: An agenda for international security studies in the post-Cold War era*. Harvester Wheatsheaf.

Carr, M., & Simon, C. (2020). The role of cyber diplomacy in international relations. *Cyber Security Review, 28*(1), 12-20.

Consuelo, M., & Coauthors. (2018). International cybersecurity frameworks and diplomacy. *International Relations Quarterly, 40*(4), 89-105.

Cull, N. J. (2008). *Public diplomacy: Lessons from the past*. USC Center on Public Diplomacy.

CyberTech Accord. (2021). *Towards effective cyber diplomacy*. Retrieved from https://www.cybertechaccord.org

Diplo Resource. (2019). *Cyber-diplomacy: Managing foreign policy in the twenty-first century*. Retrieved from https://www.diplomacy.edu

Fathollah-Nejad, A. (2018). *Iran in the age of cyber politics*. Springer.

Hanson, F. (2012). Digital diplomacy. *Foreign Policy*.

Hocking, B. (2016). *Innovative diplomacy in a changing world*. Oxford University Press.

ITU. (2016). *International Telecommunication Union reports on cybersecurity*.

Kissinger, H. (1994). *Diplomacy*. Simon & Schuster.

Kolahi, E., Hassanshekari, H., & Ahmadi-Nia, M. (2013). American cyber diplomacy (Case study: Republic of Azerbaijan). *Central Asia and Caucasus Studies Quarterly*, 19(82), 81–101. **[In Persian]**

Masoudi, O. A. (2024). An analysis of Iran's cultural and political role in the evolutionary process of European information dissemination. *Cultural Diplomacy Research Journal*, 1(3), 95–114. https://doi.org/10.22034/cdrj.2024.473343.1013. **[In Persian]**

Nasrollahi, M. S., & Amini Baghbadorani, E. (2024). Conceptualization and comparative study of cyber, digital, and convergent diplomacy (with emphasis on Clause 7 of the General Information Policies). *Socio-Cultural Strategy*, 13(2), 511–550. **[In Persian]**

Nye, J. S. (2004). *Soft power: The means to success in world politics*. Public Affairs.

Lindsay, J. R. (2013). Cyber conflict and diplomatic solutions. *Cyber Policy Journal, 10*(3), 23-41.

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

Satow, E. M. (2017). *Guide to diplomatic practice*. Oxford University Press.

Shiri, M., & Nikooei, M. (2019). *Cyber diplomacy and national security in Iran: Challenges and opportunities*. National Security Studies Journal, 22(4), 65–80. **[In Persian]**

SSRN. (2019). Cyber diplomacy: Defining the opportunities for cybersecurity. Retrieved from https://www.ssrn.com

Supreme Council of Cyberspace. (2011). *Policies and strategies of cyberspace in Iran*.

Tariq, A. (2025). Cybersecurity and diplomacy: Navigating statecraft in the digital age. Available at SSRN: https://ssrn.com/abstract=5266901 or http://dx.doi.org/10.2139/ssrn.5266901

U.S. Department of State. (2011). *International strategy for cyberspace*.

UN GGE. (2013). Group of governmental experts on developments in the field of information and telecommunications in the context of international security.

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown.

Zinelli, S., & Parsa, M. (2020). Analysis of cyber diplomacy policies of the Islamic Republic of Iran. *Foreign Policy Quarterly, 31*(2), 45-59. **[In Persian]**