فصلنامهٔ پدافند غیرعامل و امنیت (پژوهشی)
سال سیزدهم: شمارهٔ ۵۱ - تابستان ۱۴۰۴
صص: ۹۳ - ۱۱۸

Quarterly of Passive Defense & Security
Vol.13, No.51,Summer 2025
P-P: 93 - 118

تهدیدات امنیتی اینترنت ماهواره‌ای استارلینک برای ج.ا.ایران

مهدی اسمعیلی[۱]
حسین ابراهیمی[۲]
محمدحسین براتی[۳]

چکیده

در دهه‌های اخیر، ورود فنّاوری‌های نوظهور به جمهوری اسلامی ایران همواره کشور را با چالش‌های متعددی مواجه کرده است. با وجود فرصت‌های این فنّاوری‌ها، همواره آسیب‌هایی را نیز به همراه داشته‌اند. این فنّاوری‌ها می‌توانند به‌عنوان ابزاری در دست کنشگران تهدید علیه ج.ا.ایران عمل کنند. یکی از این فنّاوری‌های نوظهور، منظومه ماهواره‌ای استارلینک است که با توجه به ویژگی‌های این فنّاوری و کشور مبدأ آن، می‌توان انتظار داشت که همانند سایر فنّاوری‌های نوظهور، این فنّاوری نیز برای جمهوری اسلامی ایران تهدیداتی را در ابعاد مختلف به همراه داشته باشد. ازآنجاکه شناخت تهدیدات ناشی از فنّاوری‌های نوظهور، گام اول در مواجه با آن تهدید است؛ در این پژوهش سعی شد پس از تدوین ادبیات جامع، مؤلفه‌ها و متغیرهای پژوهش از طریق مبانی نظری احصاء و مصاحبه‌ای ساختاریافته با ۲۰ نفر از صاحب‌نظران حوزه فنی و امنیتی در مورد تهدیدات اینترنت ماهواره‌ای به عمل آید سپس با بهره‌گیری از رویکرد کیفی و روش توصیفی-تحلیلی و ابزار تحلیل محتوا، تهدیدات اینترنت ماهواره‌ای استارلینک برای ج.ا.ایران در ابعاد نظامی، سیاسی، اجتماعی-فرهنگی و اقتصادی به شیوه علمی و نظام‌مند احصاء گردد. نتایج پژوهش در قالب ۲۱ مقوله در چهار بعد اصلی نظامی، سیاسی، اجتماعی-فرهنگی و اقتصادی دسته‌بندی و موردبررسی قرار گرفته است که در بعد نظامی «بهره‌برداری در انواع عملیات نظامی» و «جمع‌آوری اطلاعات

۱. استادیار جغرافیای سیاسی دانشکده علوم و فنون فارابی smaeilim1358@gmail.com
۲. دکتری علوم سیاسی و مدرس دانشکده علوم و فنون فارابی h.ebrahimy91@yahoo.com
۳. نویسنده مسؤل: کارشناس ارشد علوم سیاسی گرایش امنیت ملی

نظامی» به‌عنوان مهم‌ترین مقوله‌های تهدیدآمیز علیه ج.ا.ایران شناسایی شده‌اند. در حوزه سیاسی، «تهدید حاکمیت سایبری و کنترل ارتباطات» و «نفوذ اطلاعاتی و تبلیغاتی» از اصلی‌ترین چالش‌های پیش‌رو به شمار می‌آیند. در بعد اجتماعی-فرهنگی نیز، مقوله‌هایی نظیر «تضعیف هویت ملی» و «تضعیف رسانه ملی و تسهیل در انتشار اخبار جعلی» از مهم‌ترین تهدیدها محسوب می‌شوند. درنهایت، در حوزه اقتصادی، «رقابت نابرابر با کاربران داخلی و کاهش اشتغال» و «فشار بر زیرساخت‌های اقتصادی» به‌عنوان تأثیرگذارترین عوامل بر اقتصاد کشور مطرح شده‌اند.

کلیدواژه‌ها: اینترنت ماهواره‌ای استارلینک، تهدید نظامی، تهدید سیاسی، تهدید اجتماعی-فرهنگی و تهدید اقتصادی

مقدمه

امروزه فنّاوری اطلاعات و ارتباطات روزبه‌روز در حال گسترش است و اینترنت به‌عنوان یکی از اجزای اصلی آن، به عضو جدایی‌ناپذیر زندگی بشری تبدیل شده که پیوسته در حال تکامل است. یکی از اصلی‌ترین تحولات در این حوزه، استفاده از ماهواره برای برقراری ارتباط اینترنتی در سراسر دنیا است. حدود سه دهه است که استفاده از ماهواره به‌عنوان ابزار ارتباط ماهواره‌ای مطرح شده است و شرکت‌های مختلفی نظیر آمازون، طرح‌هایی را در این حوزه مطرح کرده‌اند که یکی از مهم‌ترین آن‌ها پروژه اینترنت ماهواره‌ای استارلینک است. استارلینک یک فنّاوری ارائه خدمات اینترنت ماهواره‌ای است که در آن یک سامانه ماهواره‌ای به‌جای استفاده از فنّاوری کابل، مانند فیبر نوری برای انتقال داده‌های اینترنتی، از سیگنال‌های رادیویی از طریق خلأ فضا استفاده می‌کند. هدف استارلینک ایجاد یک شبکه با تأخیر کم در فضا است که محاسبات لبه[1] را در زمین تسهیل می‌کند.

---

۱. عبارت "محاسبات لبه(Edge Computing) " به مفهوم پردازش داده‌ها در نزدیکی منبع تولید داده‌ها اشاره دارد، به‌جای اینکه داده‌ها به یک سرور مرکزی یا ابر (Cloud) ارسال شوند تا پردازش شوند. به‌عبارت‌دیگر، در محاسبات لبه، پردازش اطلاعات به نزدیک‌ترین نقطه به محل تولید داده‌ها انجام می‌شود که معمولاً در دستگاه‌ها یا گره‌های شبکه‌ای قرار دارند. در مورد استارلینک یا هر سامانه ماهواره‌ای مشابه، ممکن است منظور از محاسبات لبه، پردازش داده‌ها بر روی خود ماهواره‌ها یا گره‌های زمینی باشد که به کاهش تأخیر در پردازش داده‌ها و افزایش سرعت پاسخ‌دهی کمک می‌کند. به‌این‌ترتیب، برای کاربردهای حیاتی مثل ارتباطات نظامی یا خدمات اضطراری، پردازش داده‌ها سریع‌تر و مؤثرتر انجام می‌شود.

چالش ایجاد یک شبکه جهانی در فضای بیرونی چالش کوچکی نیست، به‌خصوص به این دلیل که تأخیر کم یک تقاضای مهم است. اسپیس ایکس یک مجموعه متشکل از تقریباً ۴۲۰۰۰ ماهواره به‌اندازه تبلت را پیشنهاد کرده است که در مدار پایین دور کره زمین می‌چرخند تا این تقاضا را برآورده کند.[1] CubeSats به‌عنوان ماهواره‌های مینیاتوری که معمولاً در مدار LEO[2] استفاده می‌شوند، پوشش شبکه درهم‌تنیده‌ای ایجاد می‌کنند و قرارگرفتنشان در مدار پایین زمین، امکان کاهش تأخیر را فراهم می‌کند. با این حال، استارلینک تنها گزینه در حوزه اینترنت ماهواره‌ای نیست و چند رقیب دیگر ازجمله OneWeb، HughesNet، Viasat و Amazon در این زمینه فعالیت می‌کنند. اما استارلینک رویکرد متفاوتی را دنبال می‌کند، به‌عنوان‌مثال از هزاران ماهواره کوچک به‌جای تعداد محدودی ماهواره بزرگ بهره می‌گیرد، ماهواره‌های آن تنها در فاصله ۴۸۰ کیلومتری از سطح زمین دور سیاره می‌چرخند که این مدار کوتاه شده زمین ایستا، سرعت اینترنت را بهبود می‌بخشد و تأخیر را کاهش می‌دهد همچنین جدیدترین ماهواره‌های استارلینک دارای عناصر ارتباطی لیزری برای انتقال سیگنال‌ها بین ماهواره‌ها هستند و وابستگی به ایستگاه‌های متعدد زمینی را کاهش می‌دهند. همه این‌ها مواردی است که استارلینک را از سایر رقبای خود متمایز می‌کند و همین مقدورات موجب شده استارلینک فارغ از عموم مردم، مورد استقبال حاکمیت و نهادهای دولتی و نظامی نیز قرار گرفته و چالش‌های زیادی را در حوزه قانونی و امنیتی به‌دنبال داشته باشد؛ که این امر موجب نگرانی بسیاری از کشورهای دنیا شده است. استارلینک فعالیت خود را به کاربردهای تجاری محدود ننموده و فعالیت در حوزه‌های پژوهشی و نظامی را نیز در دستورکار خود

---

۱. "Cubesats" (کوب‌ست‌ها) به ماهواره‌های کوچک و مکعبی شکلی گفته می‌شود که معمولاً از بلوک‌های ۱۰×۱۰×۱۰ سانتی‌متر (که به آن واحد «U» گفته می‌شود) ساخته می‌شوند. این ماهواره‌ها می‌توانند به‌صورت یک یا چند واحد (1U، 2U، 3U و ...) ترکیب شوند تا اندازه و وزن بیشتری داشته باشند Cubesats.به‌دلیل اندازه کوچک، وزن کم و هزینه‌های پایین، برای پروژه‌های پژوهشی، تجاری و حتی نظامی استفاده می‌شوند. این ماهواره‌ها معمولاً برای اهداف مختلفی مانند بررسی زمین، سنجش محیط فضایی، آزمایش‌های علمی یا برقراری ارتباطات استفاده می‌شوند.

۲. مدار پایینی زمین(Low Earth Orbit) که به‌اختصار لئو نیز نامیده می‌شود، مداری است که مرکز آن زمین است که معمولاً دوره گردشی (دوره گردشی) آن به دور زمین کمتر از ۱۲۸ دقیقه است (حدود ۱۱٫۲۵ چرخش در هرروز) و مرکز گریزی شکل آن خیلی نزدیک به دایره یعنی ۰/۲۵ است (۰٫۲۵ یعنی دایره کامل و ۱ یعنی بیضوی).

قرارداده است که این امر سبب شده تا بتوان از دیدگاه یک کنشگر تهدید در حوزه‌های امنیتی نیز به آن نگریست.

بیان مسئله

با توجه به توانمندی‌های منحصربه‌فرد منظومهٔ ماهواره‌ای استارلینک و گسترش روزافزون کاربردهای آن، این شبکه اینترنتی به یکی از بازیگران اصلی در عرصه فنّاوری و ارتباطات جهانی تبدیل شده است. استارلینک که ابتدا با هدف فراهم‌سازی اینترنت پرسرعت برای مناطق دورافتاده و نیازمند به زیرساخت‌های ارتباطی آغاز به کار کرد، به‌تدریج در حوزه‌های دیگر نیز وارد شده است. هدف اولیه این پروژه، بهبود دسترسی به اینترنت در مناطقی بوده که فاقد زیرساخت‌های مناسب هستند تا این نواحی را به یک شبکه ارتباطی جهانی متصل کند. در این راستا، استارلینک توانسته است برای بسیاری از نقاط دورافتاده دسترسی اینترنت فراهم کند و این امر موجب شده تا به یکی از راهکارهای اساسی برای رفع شکاف دیجیتال در سطح جهانی تبدیل شود (ماسک، ۲۰۲۲)[1].

با این حال، گسترش کاربردهای این سامانه فراتر از بخش تجاری رفته و به‌ویژه در بحران‌های جهانی مانند جنگ‌ها، استارلینک توانسته است نقش اساسی در حفظ ارتباطات اینترنتی ایفا کند. نمونه برجسته این عملکرد، واکنش سریع استارلینک به بحران جنگ در اوکراین است. پس از حمله نظامی روسیه به اوکراین در فوریه ۲۰۲۲، استارلینک به‌سرعت درخواست دولت اوکراین را پاسخ داد و با ارسال بیش از ۵۰۰۰ دستگاه پایانه اینترنتی، ارتباطات اینترنتی کشور را حفظ کرد. این اقدام نه‌تنها نشان‌دهنده توانمندی‌های استارلینک در مقابله با بحران‌های جهانی است، بلکه تأثیرات گسترده‌ای نیز در زمینه‌های امنیتی دارد. زیرا این شبکه اینترنتی توانسته در شرایط بحرانی به حفظ ارتباطات راهبردی کمک کند و این امر زمانی حائز اهمیت می‌شود؛ که ارتباطات ماهواره‌ای به‌عنوان یک عنصر حیاتی در عملیات‌های نظامی محسوب شود (پیالی[2]، ۲۰۲۲).

---

1. Musk: صاحب شرکت اسپیس ایکس؛ مطالب درج‌شده در این بخش برگرفته از مصاحبه‌ها، توئیت‌ها، پیام‌های شبکه‌های اجتماعی است که در پایان به روش APA رفرنس‌دهی گردیده است.
2. Pillay

علاوه بر این، استارلینک در سال‌های اخیر در قراردادهایی با نیروی هوایی ایالات‌متحده و سایر نهادهای نظامی، ازجمله آژانس توسعه فضایی آمریکا (SDA)[1]، در راستای تأمین نیازهای ارتباطی نظامی و شناسایی تهدیدات به‌ویژه در حوزه ردیابی موشک‌های بالستیک مافوق صوت، وارد عرصه‌های نظامی شده است. این همکاری‌ها که در زمینه‌های مختلف ازجمله تأمین ارتباطات امنیتی برای عملیات‌های نظامی و همچنین شناسایی تهدیدات موشکی انجام می‌شود، بر اهمیت استارلینک به‌عنوان یک ابزار استراتژیک در جنگ‌های مدرن تأکید دارند. در این راستا، استارلینک علاوه بر اینکه به‌عنوان یک ابزار ارتباطی سریع و پایدار در بحران‌ها شناخته می‌شود، به یکی از ارکان مهم در عملیات‌های نظامی مدرن تبدیل شده است (زنگ[2]، لئو[3]، ۲۰۲۳).

با این حال، این گسترش کاربردهای نظامی استارلینک و بهره‌برداری آن توسط رژیم صهیونیستی در طول جنگ ۱۲ روزه برای برقراری ارتباط، ردیابی و هدف‌گیری اهداف، نگرانی‌هایی را در خصوص تهدیدات آن برای امنیت ملی جمهوری اسلامی ایران، به وجود آورده است؛ بنابراین ضروری است، تمامی تهدیدات نظامی، سیاسی، اجتماعی-فرهنگی و اقتصادی ناشی از فعالیت‌های اینترنت ماهواره‌ای استارلینک را شناسایی نمود. در همین راستا هدف از این پژوهش شناسایی تهدیدات اینترنت ماهواره‌ای استارلینک برای جمهوری اسلامی ایران است.

اهمیت و ضرورت پژوهش

اهمیت پژوهش

انجام این پژوهش می‌تواند به شناسایی تهدیدات امنیتی اینترنت ماهواره‌ای استارلینک کمک کند و این امکان را فراهم آورد که راهکارهای مناسب برای مقابله با آن تدوین شود. همچنین، این پژوهش می‌تواند به تقویت امنیت کشور کمک نماید و آگاهی از چالش‌های مرتبط با اینترنت ماهواره‌ای استارلینک را افزایش دهد. انجام این پژوهش ضمن حرکت در مسیر تدابیر فرماندهی معظم کل قوا (مدظله‌العالی) مبنی بر شناخت تهدیدات نوین امنیتی امکان برنامه‌ریزی دقیق و مبتنی بر ادبیات علمی و

1. SDA: SPACE DEVELOPMENT AGENCY
2. Zeng
3. Liu

پژوهشی را برای پیشگیری از تهدیدات اینترنت ماهواره‌ای استارلینک و مقابله با آن را برای تصمیم‌گیران فراهم می‌آورد.

ضرورت پژوهش

انجام نشدن این پژوهش ضمن مغفول‌ماندن تدابیر فرمانده معظم کل قوا (مدظله‌العالی)، می‌تواند منجر به تأخیر در اجرای برنامه‌های مقابله‌ای در حوزه امنیتی گردد و کشور را دچار عقب‌ماندگی و غافلگیری در زمان بالفعل شدن تهدیدات نماید و آسیب‌پذیری‌های جدی برای امنیت جمهوری اسلامی ایران را به‌دنبال داشته باشد. گسترش استفاده از این فنّاوری بدون شناسایی و مقابله با خطرات آن می‌تواند به تهدیداتی همچون حملات سایبری، نفوذ اطلاعاتی و اختلال در سامانه‌های دفاعی در بخش نظامی و همچنین کمک به اغتشاشات خیابانی و تحت‌الشعاع قراردادن حاکمیت سیاسی در بخش ارتباطات گردد؛ ازاین‌رو، ضروری است که تهدیدات مرتبط با این فنّاوری به‌طور دقیق مورد ارزیابی قرار گیرد تا از وقوع چنین آسیب‌هایی جلوگیری شود.

پیشینه پژوهش

لک (۱۴۰۱) در پایان‌نامه خود با عنوان «تأثیر تهدیدات سایبری بر امنیت ملی جمهوری اسلامی ایران» به این نتایج دست یافته که درنتیجه گسترش و نفوذ روزافزون فنّاوری‌های نوین الکترونیکی در تمامی ساختار کشور و پایین‌بودن ضریب امنیتی؛ این فنّاوری‌ها موجب افزایش سطح تهدیدات اقتصادی ایران شده است.

ترابی (۱۴۰۰) در مقاله خود با عنوان «ابعاد امنیتی سرویس اینترنت ماهواره‌ای» به این نتایج دست یافته که هرچند پروژه‌های اینترنت ماهواره‌ای متعلق به شرکت‌های خصوصی است اما از هم‌اکنون دولت‌ها و به‌خصوص دولت آمریکا دارای راهبرد و سیاست نسبتاً روشنی برای بهره‌برداری از آن در جهت تأمین منافع و ارزش‌های خود است .هرچند شرکت‌های فعال در حوزه ماهواره‌های اینترنتی خصوصی هستند اما بر اساس شواهد و مدارک ازجمله افشاگری‌های ادوارد اسنودن و سایت ویکی‌لیکس این شرکت‌ها ارتباط نزدیکی با بخش‌های مختلف دولت آمریکا دارند؛ بنابراین، اینترنت ماهواره‌ای این شرکت‌ها را عملاً باید بخشی از راهبرد تهاجمی آمریکا در عرصه سایبری و اطلاعاتی و در

قالب جنگ‌های جدیدی چون جنگ اطلاعاتی، جنگ ترکیبی، جنگ نرم، جنگ معرفتی، جنگ ادراکی و جنگ شناختی ارزیابی کرد.

حکمی‌زاده و فرازمند (۱۴۰۲) در مقاله خود با عنوان «بررسی راهبردهای منظومه ماهواره‌ای استارلینک از منظر عوامل راهبردی چهارگانه قوت، ضعف، فرصت و تهدید» به این نتایج دست‌یافته‌اند که اینترنت ماهواره‌ای دیر یا زود تمام مناطق جهان را تحت پوشش کامل خود درمی‌آورد و دسترسی کاربران در ایران نیز از این امر مستثنا نیست. تجربه‌های قبلی نشان‌داده‌اند استقبال از فنّاوری‌های جدید و سیاست‌گذاری صحیح برای آن‌ها بهترین راه‌حل برای برخورد با چنین موضوعاتی است. در مواجه با این فنّاوری می‌توان به دودسته راهکارهای سلبی و ایجابی اشاره داشت. راهکار سلبی پیشنهادی که جنبه حقوقی نیز دارد به این شرح است: بهره‌گیری و استناد به مصوبه مقررات حاکم بر حقوق سرزمینی ارائه خدمات ماهواره‌ای در جمهوری اسلامی ایران که با هدف ایجاد ضمانت اجرایی برای ساماندهی ارائه خدمات ماهواره‌ای توسط دارندگان مجوز تأسیس و بهره‌برداری از شبکه ماهواره‌ای توسط یک کشور خارجی عضو ITU[1] در سال ۱۳۹۹ تصویب شده است؛ اما برخی از راهکارهای ایجابی که می‌تواند در چارچوب رقابت با این شبکه پیشنهاد گردد عبارتند از:

۱ - ایجاد مزیت رقابتی چشمگیر برای شبکه یکپارچه ملی از منظر کیفیت و تعرفه خدمات

۲ - راه‌اندازی منظومه‌های ماهواره‌ای با مشارکت کشورهای منطقه و همسو به منظور ارائه خدمات ارتباطی با کیفیت به اقصی نقاط کشور و پشتیبانی از فنّاوری‌های نوین نوظهور نظیر اینترنت اشیا و نسل‌های جدید ارتباطات سیار با عنایت به نرخ رشد پرشتاب کاربران و متقاضیان این شبکه ماهواره‌ای در اقصی نقاط کشور ضروری است تا تمهیدات و اقدامات عاجلی نیز در مقاطع زمانی کوتاه‌مدت و میان‌مدت به عمل آورده شود.

احترام و احمدی (۱۴۰۰) در مقاله خود با عنوان «فنّاوری اینترنت ماهواره‌ای به‌عنوان پیشران و یا تهدید فراروی انقلاب اسلامی در گام دوم مطالعه موردی: پروژه استارلینک» به این نتایج دست‌یافته‌اند که تاکنون بازار هدف اینترنت ماهواره‌ای دولت‌ها و کسب و

---

۱. اتحادیه بین‌المللی مخابرات (International Telecommunication Union)؛ یک سازمان بین‌المللی وابسته به سازمان ملل متحد است. این اتحادیه وظیفه قانون‌گذاری و مدیریت فضای فرکانسی، تدوین استانداردهای تبادل داده و اطلاعات و همچنین کمک به رشد و توسعه ارتباطات در سراسر جهان را بر عهده دارد.

کارهـای بزرگی بودند که توانایی مالی پرداخت هزینه‌های زیاد آن را داشـتند. شـرکت‌های بزرگـی با سـرمایه‌های زیـادی از دهه ۹۰ میلادی تاکنون به‌دنبال تحقق دسترسـی اینترنت ماهواره‌ای برای کاربران نهایی عمومی با پوشش جهانی بودند. باکاهش هزینه‌های ساخت و ارسـال ماهـواره و پیشـرفت فنّـاوری دوبـاره شـرکت‌های بزرگـی در ارائه خدمـات اینترنت ماهواره‌ای برای عموم مردم گام برمی‌دارند. ازآنجایی‌که مهم‌ترین دغدغه حاکمیت ارتقاء رفـاه و تضمیـن حقـوق آحـاد مردم جامعه اسـت، ارائـه خدمات نبایـد به‌گونه‌ای باشـد که منافـع مـردم و کشـور نادیـده گرفته شـده و صرفاً شـرکت‌های خارجی از مزایـای آن منتفع شـوند، به‌عبارت‌دیگـر ارائـه خدمـات بایـد توسـط تأمین‌کنندگانی کـه به ارزش‌هـا و اصول حاکمیتی کشـور پایبند هسـتند، صورت پذیرد. حذف برنامک‌های موبایلی از روی گوشی کاربران بدون اجازه، عدم ارائه خدمات به کسـب و کارها و کاربران ایرانی و عدم پشـتیبانی برنامک‌های ایرانی برای ارائه خدمات به کاربران خود ازجمله موارد نقض حریم خصوصی و حقوق عامه مردم کشـور در چند سـال اخیر بوده اسـت که همه این‌ها تهدیدی فراروی انقلاب اسـلامی محسـوب می‌گردد. از طرف دیگر ورود کشورهای منطقه از قبیل عربستان که رقیب دیرینه ایران اسـت به این حوزه نشـان‌دهنده اهمیت موضوع بوده و ایران نباید از این عرصه عقب بماند.

وکیلـی و اعتمادی‌فـر (۱۴۰۰) در مقالـه خـود بـا عنوان «تحلیل و بررسـی پیرامـون پروژه اسـتارلینک» به این نتایج دسـت‌یافته‌اند که اسـتارلینک یک پروژه ماهواره‌ای اسـت که از سـوی شـرکت اسپیس ایکس برای توسعه دسترسـی ماهواره‌ای کم‌هزینه و باکارایی بالا در پیاده‌سـازی اینترنت ماهواره‌ای اسـت. اسـتارلینک قرار است سـرویس ارتباطی «پهن‌باند بی‌سـیم» با «دسترسـی اینترنت بی‌سـیم پرسرعت» باشد که سـرویس‌های دیگر نیز به آن افزوده می‌شـود. در سـال ۲۰۱۷، اسـپیس ایکس، بـرای راه‌اندازی نزدیک بـه ۱۲,۰۰۰ ماهواره تـا اواسـط دهـه ۲۰۲۰ درخواسـت قانونـی کرده اسـت. اسـپیس ایکـس همچنین بنـا دارد تا ماهواره‌هایی را برای اهداف، نظامی، علمی یا اکتشافی استفاده کند.

دکامئـی و ناصـری (۱۴۰۱) در مقالـه خـود بـا عنـوان «تحلیـل و بررسـی معمـاری پـروژه استارلینک» به این نتایج دست‌یافته‌اند که استارلینک یک صورت فلکی ماهواره‌ای است که از سـوی شـرکت اسـپیس اییکـس بـرای فراهم‌کـردن اینترنت ماهواره‌ای سـاخته شـده

است. به‌زودی بسیاری از کشورها آگاه خواهند شد که باید خواه یا ناخواه در این نسل جدید اینترنت ماهواره‌ای نقشی داشته باشند؛ بنابراین زودتر آگاه‌شدن با استارلینک اینترنت (ماهواره‌ای) می‌تواند ما را برای بهره‌وری از مزایای آن و یا مقابله با خطرات احتمالی آن ایمن کند .استارلینک یک پروژه بسیار کاربردی و هیجان‌انگیز درزمینهٔ اینترنت ماهواره‌ای است که توسط ایلان ماسک ایده‌پردازی شده و توسط شرکت اسپیس ایکس ایالات‌متحده در حال اجرا است این فنّاوری درواقع یک سامانه ماهواره‌ای است که هدف اصلی از ایجاد و راه‌اندازی آن فراهم‌آوردن اینترنت با سرعت و سطح دسترسی بالا برای تمام نقاط زمین است. سامانه استارلینک از اجزای مهمی همچون چندین هزار ماهواره که در مدار پایینی زمین قابل‌استقرار و حرکت هستند و پایانه‌ها یا گیرنده‌های زمینی تشکیل شده است. این سامانه هم‌اکنون در مراحل اجرایی قرار دارد و هنوز به اتمام نرسیده؛ اما پیش‌بینی می‌شود و انتظار می‌رود که تا سال ۲۰۲۷ عملاً در تمام نقاط جهان در دسترس باشد.

مبانی نظری

- تهدیدات

- مفهوم‌شناسی تهدید:

در فرهنگ معین، تهدید؛ به ترسانیدن، بیم‌دادن، بیم‌کردن از کسی یا چیزی گفته می‌شود (معین، ۱۳۷۸، ج۱: ۸۵۶)، در فرهنگ عمید، کلمه تهدید؛ ترساندن و بیم‌دادن معنا شده است (عمید،۱۳۶۲: ۹۳۷)، لغتنامه لانگمن؛ سه تعریف از تهدید ارائه کرده است. نخست تهدید را بیان آشکار آسیب‌رساندن به کسی یا ناراحت‌کردن و به دردسر انداختن او می‌داند. در تعریف دوم، آن را احتمال وقوع حادثه‌ای بسیار بد معنا کرده و در تعریف سوم، تهدید را شخص یا چیزی که به‌عنوان خطر شناخته می‌شود معرفی نموده است. لغتنامه آکسفورد نیز دو تعریف ارائه نموده: نخست، قصد ابرازشده برای صدمه یا آسیب‌رسانی یا دیگر اقدامات خصمانه علیه کسی معرفی می‌شود و در تعریف دوم به شخص یا چیزی گفته می‌شود که بتواند خطر یا صدمه‌ای ایجاد کند.

- تهدید در نظر صاحب‌نظران:

بری بوزان: فقدان امنیت و ناامنی را بازتاب ترکیبی از تهدیدها و آسیب‌پذیری‌ها دانسته که جدا ساختن معنادار آن‌ها از یکدیگر غیرممکن است (بوزان، ۱۳۷۹: ۱۳۵)؛ باری بوزان موضوع آسیب‌پذیری‌ها را وجهۀ داخلی ناامنی و تهدیدها را وجهۀ خارجی آن می‌داند.

افتخاری: در تعریف واژه تهدید باید دو مفهوم مخاطره و منافع را در نظر داشت. تهدید از جنس مخاطره بوده و می‌توان مخاطره نسبت به منافع یک بازیگر را تهدید دانست. به‌عبارت‌دیگر از منظر یک بازیگر، تهدید زمانی شکل می‌گیرد که منافع یک بازیگر، از منظر خود آن بازیگر، مورد مخاطره واقع شود (افتخاری، ۱۳۹۱: ۲۴).

ریچارد اولمان: تهدیدات امنیت ملی اقدام یا سلسله رویدادهایی است که به شکل مؤثر و در دوره زمانی نسبتاً کوتاهی خطر افت کیفیت زندگی برای ساکنان یک کشور را پیش آورد و نیز با خطر جدی کاهش طیف خط‌مشی‌هایی که حکومت یک کشور یا واحدهای غیرحکومتی خصوصی موجود در یک کشور (اشخاص، گروه‌ها و شرکت‌ها) می‌توانند میان آن‌ها دست به انتخاب زنند همراه باشد (عبدالله‌خانی، ۱۳۸۶: ۲۳).

کارل روپر: تهدید عبارت است از هرگونه نشانه، حادثه، یا شرایطی که توان ایجاد خسارت و ضرر علیه یک دارایی را داشته باشد. وی همچنین در جای دیگر تهدید را مقصد و توان دشمن برای انجام حملاتی که منافع کشور را به خطر اندازد تعریف نموده است (همان: ۲۳).

مرادیان تمایز تهدید و آسیب را این‌گونه تعریف می‌کند: آسیب‌ها زمینه‌های ایجاد تهدید را فراهم می‌آورند و به‌نوعی تهدیدات بالقوه محسوب می‌شوند. هدف سیاست‌گذاران حوزه امنیت ملی باید معطوف به کاهش و مقابله با تهدیدات و آسیب‌ها از یکسو و استفاده از فرصت‌ها از سوی دیگر باشد.

از نظر وی، عوامل قابل‌توجه در تعریف تهدید شامل: منافع ملی– توانمندی موضوع یا واحد مورد تهدید– شرایط محیطی–قدرت و توانایی تهدید – زمان – تصور از اقدامات یا پدیده‌ها می‌گردند.

همچنین عوامل مؤثر در جدی‌بودن تهدید این موارد هستند: مشخص‌بودن هویت تهدید– نزدیکی از نظر زمان – شدت احتمال وقوع – اوضاع و شرایط تاریخی که باعث تقویت آن می‌شوند.

متغیرهای مؤثر در فرایند درک تهدیدات نیز این موارد هستند: بعد روان‌شناختی در درک تهدید – بعد تاریخی – بعد ژئوپلیتیکی و ژئواستراتژیکی کشور و موقعیت جغرافیایی و راهبردی کشور– موازنه قوا و قدرت نسبی کشورها – آسیب-پذیری داخلی کشورها – نظام اعتقادی و ارزش‌های حاکم بر کشور – بعد ساختار نظام سیاسی کشور (مرادیان، ۱۳۹۳).

-انواع تهدیدات:

باری بوزان در کتاب «مردم دولت‌ها و هراس» از پنج گونه اصلی تهدیدات سیاسی، اقتصادی، اجتماعی، نظامی و زیست‌محیطی سخن گفته است (بوزان، ۱۳۷۹: ۱۵۴-۱۴۱). افتخاری تهدید فنّاورانه را به‌عنوان ششمین تهدید به این تهدیدات اضافه نموده است.

-نظریه‌های تهدید:

نظریه توازن تهدید:

این نظریه توسط «استفن ام. والت» در مقاله‌ای با نام «شکل‌گیری اتحاد و توازن قدرت» در سال ۱۹۸۵ در نشریه «امنیت بین‌المللی» مطرح گردید. نظریه توازن تهدید به اصلاح و تغییر نظریه معروف نئورئالیستی- «توازن قدرت» پرداخته و عامل تعیین‌کننده رفتار کشورها برای ایجاد اتحاد را، درک تهدید از سوی دیگران عنوان کرده است. به اعتقاد والت کشورها اغلب با تشکیل اتحاد علیه تهدید (درک شده) به ایجاد توازن می‌پردازند حال‌آنکه کشورهای بسیار ضعیف برای دفاع از امنیت خود پیوستن به تهدید یا «هم‌رنگ شدن» با آن را ترجیح می‌دهند. وی به‌عنوان‌مثال از «الگوهای اتحاد» کشورهای اروپایی قبل و حین جنگ جهانی اول و دوم نام می‌برد و ایجاد اتحادی از کشورهای دارای قدرت ترکیبی بسیار بیشتر علیه (تهدید) توسعه‌طلبی آلمان را نمونه‌ای از توازن تهدید ذکر می‌کند (عبدالله‌خانی، ۱۳۸۶: ۹۷).

نظریه مکتب کپنهاک:

شناسایی امنیت ملی صرفاً پس از درک معقول از ماهیت تهدیدات و آسیب‌پذیری‌ها امکان‌پذیر است. همچنین فقدان امنیت و یا وجود ناامنی، بازتاب، ترکیبی از تهدیدها و آسیب‌پذیری‌هاست که جدا ساختن معنادار آن‌ها از یکدیگر ناممکن است. بر این اساس سیاست امنیت ملی می‌تواند روی مسائل داخلی تمرکز نموده و در پی کاهش آسیب‌پذیری‌های دولت باشد یا بر مسائل خارجی تمرکز داشته و از طریق منابع ذی‌ربط درصدد کاهش تهدیدات خارجی برآید (بوزان، ۱۳۸۶: ۱۳۵-۱۳۶).

نظریه مطالعات امنیتی جهان سوم:

مبنای تجزیه‌وتحلیل امنیت ملی در «مطالعات امنیتی جهان سوم» بر پایه سه مؤلفه اساسی قرار دارد که عبارتند از؛ «محیط امنیتی»، «ابعاد سخت‌افزاری امنیت» و «ابعاد نرم‌افزاری امنیت» در این چارچوب محیط امنیتی محل رویش و پیدایش تهدیدات و فرصت‌ها، ابعاد سخت‌افزاری شامل توانمندی‌های فیزیکی و مادی و ابعاد نرم‌افزاری شامل «ظرفیت سیاسی» و زیرمجموعه‌های مربوطه می‌گردد.

مدل ارائه شده از امنیت ملی توسط مطالعات امنیتی جهان سوم خصوصاً شخص «ادوارد ای. آزر» و «چونگ این مون» تلاش دارد تا یک تبیین بومی‌تر و با قابلیت انطباق افزون‌تر از امنیت ملی کشورهای جهان سوم ارائه دهد. بر همین اساس موضوع تهدیدات نرم در قالب مطالعات امنیتی جهان سوم بیش از مطالعات رئالیستی امنیت قابل تبیین است (ادوارد ای. آزر و چونگ این مون، ۱۳۷۹: ۲۹۹-۳۱۷).

- اینترنت ماهواره‌ای استارلینک

آشنایی با منظومه ماهواره‌ای استارلینک:

با گسترش بی‌سابقه فنّاوری‌های ارتباطی، اینترنت ماهواره‌ای به‌عنوان روشی نوین برای فراهم‌آوردن دسترسی به اینترنت در مناطق دورافتاده و حتی در شرایط بحرانی مطرح شده است. پروژه استارلینک شرکت SpaceX که تحت رهبری ایلان ماسک راه‌اندازی شده، با بهره‌گیری از هزاران ماهواره در مدار پایین زمین (LEO) نقش بسزایی در تغییر چشم‌انداز ارتباطات جهانی ایفا می‌کند (ماسک، ۲۰۲۲).

پـروژه اسـتارلینک (Starlink) یکـی از بلندپروازانه‌تریـن طرح‌هـای قـرن بیسـت‌ویکم در حـوزه فنّاوری‌های ارتباطی و فضایی اسـت که توسـط شـرکت آمریکایی اسـپیس‌ایکس (SpaceX) و تحـت رهبـری ایلان ماسـک آغاز شـد. هدف اصلی این پروژه، ایجاد شـبکه‌ای جهانی از ماهواره‌های مخابراتی در مدار پایین زمین (LEO–Low Earth Orbit) برای ارائه خدمات اینترنت پرسـرعت به سراسـر جهان، به‌ویژه مناطق محروم و فاقد زیرساخت‌های مخابراتی، عنوان شده است (اسپیس ایکس[1]، ۲۰۲۳).

- تاریخچه استارلینک

- تولید ایده و مراحل اولیه

اسـتارلینک به‌عنـوان بخشـی از چشـم‌انداز وسـیع‌تر شـرکت SpaceX جهـت کاهـش هزینه‌های فضایی و ایجاد شبکه‌ای جهانی از اینترنت ماهواره‌ای مطرح شد. از سال ۲۰۱۵ به بعد، با شـروع پروژه‌های آزمایشـی و آزمون‌های اولیه، اولین ماهواره‌های اسـتارلینک به فضـا پرتـاب شـدند (ماسـک، ۲۰۲۲). ایـن پروژه با هـدف ارائه اینترنت پرسـرعت در سراسـر جهان و فراهم‌آوردن پوشش ارتباطی در مناطق روستایی و دورافتاده، به‌سرعت رشد کرد.

- توسعه و گسترش

تاکنون، تعداد ماهواره‌های استارلینک به چندین هزار واحد رسیده است و با استفاده از فنّاوری‌هـای نویـن ماننـد لینک‌های لیـزری بین ماهـواره‌ای و آنتن‌های فـازدار، به یکی از پرسـرعت‌ترین و کم‌تأخیرترین شـبکه‌های ارتباطی تبدیل شـده اسـت (اسپیس ایکس، ۲۰۲۳). به‌روزرسـانی‌های دوره‌ای سـامانه، اصـلاح مدارهـا و افزایـش دقـت در مانیتورینگ وضعیت ماهواره‌ها از ویژگی‌های کلیدی روند توسعه این پروژه به شمار می‌روند.

- معماری و ساختار استارلینک

- ساختار فیزیکی و تعداد ماهواره‌ها

اسـتارلینک از هـزاران ماهواره کوچک بهره می‌برد که در مـدار پایین زمین (ارتفاع ۵۵۰ کیلومتری) قرار دارند. طراحی مدولار و قابلیت‌های خودکارسازی بالا، از ویژگی‌های کلیدی این سامانه محسوب می‌شوند (اسپیس ایکس، ۲۰۲۳).

1. SpaceX

- ویژگی‌های ماهواره‌های استارلینک

جرم کمتر، فشرده‌تر: هر ماهواره دارای طراحی جمع و جور و تخت است که حجم را به حداقل می‌رساند و به پرتابگر اجازه پرتاب متراکم می‌دهد تا از قابلیت‌های پرتاب موشک فالکون ۹ اسپیس ایکس استفاده کامل کند.

ردیاب ستاره: حسگرهای ناوبری سفارشی استارلینک ستاره‌ها را بررسی می‌کنند تا مکان، ارتفاع و جهت هر ماهواره را تعیین کنند و امکان قرارگیری دقیق پهنای باند را فراهم کنند.

لیزرهای فضای نوری: هر ماهواره استارلینک شامل ۳ لیزر فضایی (پیوندهای بین ماهواره‌ای نوری یاISL) است که با سرعت ۲۰۰ گیگابایت بر ثانیه کار می‌کنند که باهم در سراسر صورت فلکی یک شبکه اینترنتی جهانی را تشکیل می‌دهد.

آنتن‌ها: هر ماهواره استارلینک از ۵ آنتن آرایه فازی باند (Ku) پیشرفته و ۳ آنتن دو باندِ (E-bandوKa-band) استفاده می‌کند تا اتصال پهنای باند بالا را به مشتریان استارلینک ارائه دهد.

سامانه‌های محرکه یونی: رانشگرهای کارآمد آرگون، ماهواره‌های استارلینک را قادر می‌سازد تا در پایان عمر مفید خود در مدار بالا بروند، در فضا مانور دهند و از مدار خارج شوند. استارلینک اولین فضاپیمای پیشرانه آرگون است که تاکنون در فضا پرواز کرده است.

سامانه برق: ماهواره‌های استارلینک دارای یک آرایه خورشیدی دوگانه و باتری با ظرفیت بالا برای تأمین انرژی محموله‌ها هستند. این دو آرایه خورشیدی نیز از نظر آئرودینامیکی لدون بار الکتریکی هستند که مانورهای سریع‌تری در مدار را ممکن می‌کنند.

واکنش چرخ‌ها: چهار چرخ واکنش، کنترل رفتار چابک‌تری را برای وسیله نقلیه فراهم می‌کنند. پیکربندی یدکی hot-spare[1] از قابلیت اطمینان بالایی برخوردار است و flywheel[2] آلومینیومی آن در پایان عمر به‌طور کامل از بین می‌رود (اسپیس ایکس، ۲۰۲۵).

---

۱. hot-spare: یک قابلیت بکاپ محسوب می‌شود که در آن یک هارد می‌تواند جایگزین هارد اصلی دستگاه گردد و اختلالی در کارکرد سامانه به وجود نیاید.

۲. چرخ لنگر (به انگلیسی: flywheel) یک وسیله، مکانیکی گردان سنگین است که برای ذخیره‌سازی انرژی دورانی به کار می‌رود. چرخ لنگرها دارای گشتاور و لختی بالایی هستند؛ بنابراین در برابر تغییر سرعت دورانی مقاومت می‌کنند.

- فنّاوری‌های مورداستفاده

آنتن‌های فازدار: جهت ارسال و دریافت سیگنال‌های رادیویی با دقت بالا (وایس[1]، ۲۰۲۰).

لینک‌های لیزری بین ماهواره‌ای: انتقال داده‌ها بین ماهواره‌ها بدون وابستگی به ایستگاه‌های زمینی (وایس، ۲۰۲۰).

سامانه‌های رمزنگاری پیشرفته: برای حفاظت از داده‌های انتقالی و جلوگیری از حملات نفوذ (وایس، ۲۰۲۰).

پروتکل‌های ارتباطی سفارشی: بهینه‌سازی‌شده برای کاهش تأخیر و افزایش پهنای باند (وایس، ۲۰۲۰).

روش‌شناسی پژوهش و جامعه آماری

پژوهشگر درصدد شناسایی تهدیدات اینترنت ماهواره‌ای استارلینک برای ج.ا.ایران است. بر این اساس در ادبیات پژوهشی اعم از کتاب‌ها، مقالات، پایان‌نامه‌ها، مجلات، پروژه‌ها و نیز پویش‌های اینترنتی به جستجو پرداخته و پس از تدوین ادبیات جامع، مؤلفه‌ها و متغیرهای پژوهش از طریق مبانی نظری احصاء و مصاحبه‌ای ساختاریافته از ۲۰ نفر از صاحب‌نظران حوزه فنی و امنیتی در مورد تهدیدات اینترنت ماهواره‌ای استارلینک برای ج.ا.ایران به عمل آمد؛ سپس با استفاده از روش توصیفی-تحلیلی و ابزار تحلیل محتوا و تجزیه‌وتحلیل با استفاده از نرم‌افزار Maxqda2020 تهدیدات اینترنت ماهواره‌ای استارلینک برای ج.ا.ا استخراج گردید. ابزار جمع‌آوری اطلاعات و داده‌ها، مطالعات کتابخانه‌ای و مصاحبه است. جامعه آماری این پژوهش متخصصان حوزه فنی و امنیتی هستند. به‌منظور وارسی روایی و اعتبار تحلیل‌ها به ترتیب از روش‌های بررسی اعتبارپذیری، انتقال‌پذیری و تأییدپذیری و روش بررسی اعتبار هالستی با استفاده از دو کدگذار استفاده شد که ضریب به‌دست‌آمده (۰/۸) توافق بالا بین کدگذارها را نشان داد.

تجزیه‌وتحلیل و یافته‌ها

در این پژوهش نظر به ادبیات و اهداف پژوهش به چهار بعد تهدید (نظامی، سیاسی، اجتماعی-فرهنگی و اقتصادی) پرداخته شد. بر همین اساس این چهار بعد به‌عنوان مقوله‌های اصلی تلقی و در ذیل آن بر اساس مصاحبه‌های انجام شده، زیر مقولاتی

1. Weiss

شناسایی گردید. در گام نخست ۲۰ مصاحبه انجام گرفته کدگذاری بازشده و ۳۷۳ کد باز احصاء گردید. در گام بعدی پس از تعیین کدهای باز، محوری و کدگذاری انتخابی برای شناسایی زیرمقوله‌ها انجام که صورت‌بندی آن به شرح جدول شماره ۲ است. نمونه‌ای از خروجی مصاحبه‌های انجام شده به شرح زیر است:

ردیف	کد مصاحبه‌شونده	مقوله اصلی	زیرمقوله	واحد معنی
۱	کد۱	تهدیدات اجتماعی و فرهنگی	ایجاد شکاف دیجیتالی و تشدید نابرابری اجتماعی	شکاف دیجیتالی و تشدید نابرابری اجتماعی - استارلینک در ابتدا برای قشر مرفه و شهرنشینان قابل دسترسی است و این موضوع شکاف دیجیتال بین شهرها و روستاها را افزایش می‌دهد. - اگر دولت‌ها نتوانند اینترنت مقرون به صرفه ارائه دهند، طبقات کم درآمد از دسترسی به اطلاعات محروم می‌مانند. - این نابرابری می‌تواند به اعتراضات اجتماعی و افزایش تنش‌های طبقاتی منجر شود.
۲	کد۲	تهدیدات سیاسی	نفوذ اطلاعاتی و تبلیغاتی	- کمک به القای ناکارآمدی مسئولین در رسیدگی به مشکلات مردم - القای ناکارآمدی نظام در رفع مشکلات معیشتی مردم
۳	کد۳	تهدیدات اقتصادی	خروج ارز و قاچاق کالا	خروج ارز و رشد بازار سیاه تجهیزات برای استفاده از استارلینک، کاربران نیاز به تجهیزات خاصی مانند دیش، پایانه و اشتراک ماهانه دلاری دارند. در ایران که تحت تحریم‌های مالی و تجاری قرار دارد، تهیه این تجهیزات عمدتاً از طریق بازار سیاه، قاچاق یا ارزهای دیجیتال صورت می‌گیرد. این فرایند باعث خروج گسترده ارز از کشور و رشد اقتصاد زیرزمینی می‌شود که خود تهدیدی جدی برای ثبات اقتصادی کشور به شمار می‌رود.
۴	کد۴	تهدیدات نظامی	بهره‌برداری در انواع عملیات نظامی	ناوبری و کنترل آنلاین سامانه سلاح، موشک و پهپاد نیز به سهولت توسط این منظومه قابل انجام است. این منظومه به سهولت و با به‌کارگیری یک رمزگذار می‌تواند به یک سامانه فرماندهی و کنترل بسیار خطرناک و جهانی تبدیل شود که در مواقع حساس می‌تواند بسیار تأثیرگذار و تعیین‌کنندهٔ طرف برندهٔ جنگ باشد.

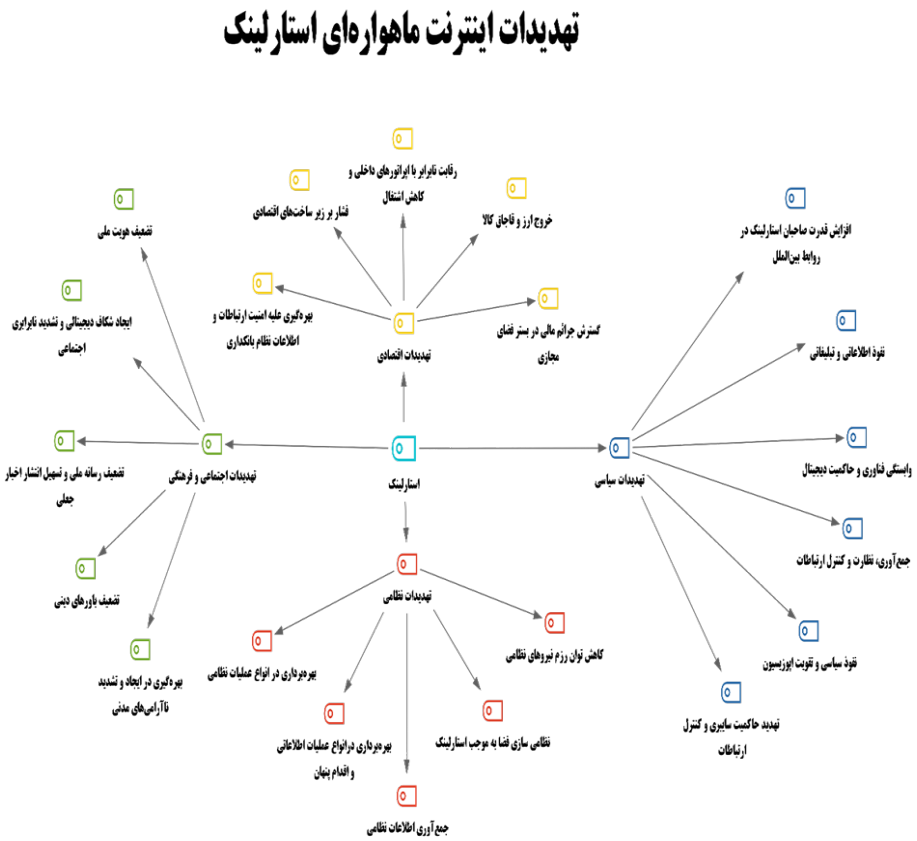
جدول شماره اگزیده‌ای از مصاحبه‌های انجام شده با خبرگان

ردیف	مقوله اصلی	زیرمقوله‌ها
۱	تهدیدات نظامی	کاهش توان رزم نیروهای نظامی
		بهره‌برداری در انواع عملیات نظامی
		نظامی‌سازی فضا به موجب استارلینک
		جمع‌آوری اطلاعات نظامی
		بهره‌برداری در انواع عملیات اطلاعاتی و اقدام پنهان
۲	تهدیدات سیاسی	جمع‌آوری، نظارت و کنترل بر ارتباطات
		وابستگی فنّاوری و حاکمیت دیجیتال
		نفوذ اطلاعاتی و تبلیغاتی
		نفوذ سیاسی و تقویت گروه مخالف
		افزایش قدرت صاحبان استارلینک در روابط بین‌الملل
		تهدید حاکمیت سایبری و کنترل ارتباطات
۳	تهدیدات اجتماعی و فرهنگی	تضعیف رسانه ملی و تسهیل انتشار اخبار جعلی
		ایجاد شکاف دیجیتالی و تشدید نابرابری اجتماعی
		بهره‌گیری در ایجاد و تشدید ناآرامی‌های مدنی
		تضعیف هویت ملی
		تضعیف باورهای دینی
۴	تهدیدات اقتصادی	گسترش جرائم مالی در بستر فضای مجازی
		بهره‌گیری علیه امنیت ارتباطات و اطلاعات نظام بانکداری
		فشار بر زیرساخت‌های اقتصادی
		رقابت نابرابر با کاربران داخلی و کاهش اشتغال
		خروج ارز و قاچاق کالا

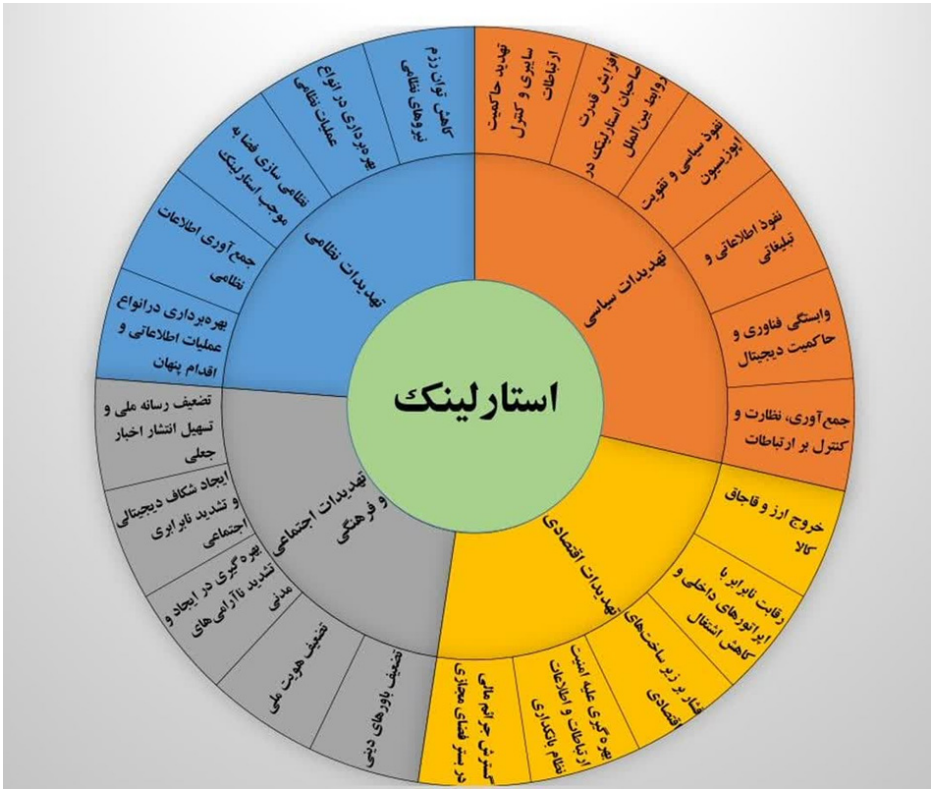
جدول شماره ۲ تجزیه‌وتحلیل داده‌ها

ابعاد و مؤلفه‌های تهدیدات اینترنت ماهواره‌ای استارلینک برای ج.ا.ایران از منظر صاحب‌نظران

پس از اخذ خروجی نقشه نرم‌افزار مکس‌کیودا، ابعاد و مؤلفه‌های پیشگیری امنیتی به شرح شکل زیر احصا گردید.



شکل ۱- الگوی نموداری استخراج‌شده تهدیدات اینترنت ماهواره استارلینک



شکل شماره ۲- الگوی مفهومی استخراج‌شده تهدیدات اینترنت ماهواره‌ای استارلینک

نتیجه پژوهش و پیشنهادها

الف-نتیجه تحقیق

این پژوهش به‌دنبال پاسخگویی به این سؤال بود که «تهدیدات اینترنت ماهواره‌ای استارلینک برای ج.ا.ایران کدامند؟» در این پژوهش تهدیدات در ابعاد نظامی، سیاسی، اجتماعی-فرهنگی و اقتصادی آن موردپژوهش قرارگرفته است.

در بعد تهدیدات نظامی، توزیع فراوانی پاسخ تعداد ۲۰ نفر مصاحبه‌شونده (جامعه خبرگان) مؤید این مطلب است که به تأیید تعداد ۱۲ نفر از مصاحبه‌شوندگان، بیش‌ترین فراوانی، با ۳۴ کد باز احصاشده، مربوط به مقوله «بهره‌برداری در انواع عملیات نظامی» بوده است و پس‌ازآن، به تأیید تعداد ۱۲ نفر از ۲۰ نفر مصاحبه‌شونده، مقوله «جمع‌آوری

اطلاعات نظامی» با فراوانی ۲۷ کد باز احصا شده، در مرتبه دوم قرار دارد سپس به تأیید تعداد ۱۰ نفر از مصاحبه‌شوندگان، مقوله» بهره‌برداری در انواع عملیات اطلاعاتی و اقدام پنهان» با فراوانی ۲۲ کد باز احصا شده، در مرتبه سوم قرار گرفته است.

در رتبه‌های چهارم و پنجم، به ترتیب، با تأیید تعداد ۶ و ۵ نفر از ۲۰ نفر مصاحبه‌شونده، مقوله‌های «کاهش توان رزم نیروهای نظامی» و «نظامی‌سازی فضا به موجب استارلینک» با فراوانی‌های ۹ و ۹، می‌تواند تهدیدی در بعد نظامی برای ج.ا.ایران به شمار آید.

در بعد نظامی، بهره‌برداری از اینترنت ماهواره‌ای در حوزه نظامی تنها به معنای افزایش دسترسی‌های فنی نیست، بلکه نشان‌دهنده گذار از جنگ‌های متعارف به بسترهای «نامتقارنِ مبتنی بر داده» است. ماهیت غیرقابل‌کنترل و توزیع‌یافتگیِ شبکه استارلینک، راهبردهای سنتی دفاع سایبری و جنگ الکترونیک (Jamming) را که بر پایه تمرکز زیرساختی بنا شده‌اند، با چالش جدی مواجه می‌سازد. استارلینک به دلیل ساختار غیرمتکی به زیرساخت‌های زمینی، قابلیت ایجاد ارتباطات پایدار و نسبتاً امن را برای کنشگران متخاصم فراهم خواهد کرد و امکان پشتیبانی از انواع عملیات نظامی و اطلاعاتی را افزایش خواهد داد. همچنین این فناوری می‌تواند زمینه جمع‌آوری اطلاعات نظامی، ارسال داده‌های میدانی و هدایت شبکه‌های عملیاتی را در شرایط اختلال یا قطع شبکه‌های داخلی تسهیل کند. در مجموع، بُعد نظامی تهدیدات استارلینک نشان خواهد داد که تقویت پدافند ارتباطی و ارتقای توان رصد و پایش فنی، ضرورتی راهبردی برای مواجهه با تحولات آینده خواهد بود.

در بعد تهدیدات سیاسی، توزیع فراوانی پاسخ تعداد ۲۰ نفر مصاحبه‌شونده (جامعه خبرگان) مؤید این مطلب است که به تأیید تعداد ۱۹ نفر از مصاحبه‌شوندگان، بیش‌ترین فراوانی، با ۳۵ کد باز احصا شده، مربوط به مقوله «تهدید حاکمیت سایبری و کنترل ارتباطات» بوده است و پس‌ازآن، به تأیید تعداد ۱۰ نفر از ۲۰ نفر مصاحبه‌شونده، مقوله «نفوذ اطلاعاتی و تبلیغاتی» با فراوانی ۲۱ کد باز احصا شده، در مرتبه دوم قرار دارد سپس به تأیید تعداد ۸ نفر از مصاحبه‌شوندگان، مقوله‌های «نفوذ سیاسی و تقویت گروه مخالف» و «افزایش قدرت صاحبان استارلینک در روابط بین‌الملل» با فراوانی ۱۴ کد باز احصا شده، در مرتبه سوم به‌طور مشترک قرارگرفته‌اند.

در رتبه‌های پنجم و ششم، به ترتیب، با تأیید تعداد ۷ و ۸ نفر از ۲۰ نفر مصاحبه‌شونده، مقوله‌های «وابستگی فنّاوری و حاکمیت دیجیتال» و «جمع‌آوری، نظارت و کنترل ارتباطات» با فراوانی‌های ۱۳ و ۱۱، می‌تواند تهدیدی در بعد سیاسی برای ج.ا.ایران به شمار آید.

در بُعد سیاسی، ظهور استارلینک مفهوم سنتی «حاکمیت سایبری» و کنترل دروازه‌ای (Gatekeeping) دولت بر جریان اطلاعات را با فرسایش ساختاری مواجه می‌کند. این فناوری با دور زدن زیرساخت‌های ملی و شبکه ملی اطلاعات، ابزارهای نظارتی و مدیریت فضای مجازی حاکمیت را عملاً به حاشیه می‌راند. این وضعیت نشان می‌دهد که نفوذ اطلاعاتی و تبلیغاتی از طریق این بستر، نه یک تهدید گذرا، بلکه عاملی در جهت تضعیف «مرجعیت خبری دولت» است؛ چراکه با گسستن زنجیره نظارت رسمی بر جریان داده‌ها، بستری امن برای نفوذ فکری و ایجاد اختلال در ثبات سیاسی از طریق دستکاری ادراکات عمومی در شرایط بحرانی فراهم می‌شود.

در بعد تهدیدات اجتماعی و فرهنگی، توزیع فراوانی پاسخ تعداد ۲۰ نفر مصاحبه‌شونده (جامعه خبرگان) مؤید این مطلب است که به تأیید تعداد ۱۷ نفر از مصاحبه‌شوندگان، بیش‌ترین فراوانی، با ۴۶ کد باز احصا شده، مربوط به مقوله «تضعیف هویت ملی» بوده است و پس‌ازآن، به تأیید تعداد ۱۶ نفر از ۲۰ نفر مصاحبه‌شونده، مقوله «تضعیف باورهای دینی» با فراوانی ۲۳ کد باز احصا شده، در مرتبه دوم قرار دارد سپس به تأیید تعداد ۱۲ نفر از مصاحبه‌شوندگان، مقوله» تضعیف رسانه ملی و تسهیل انتشار اخبار جعلی» با فراوانی ۲۳ کد باز احصا شده، در مرتبه سوم قرار گرفته است.

در رتبه‌های چهارم و پنجم، به ترتیب، با تأیید تعداد ۵ و ۷ نفر از ۲۰ نفر مصاحبه‌شونده، مقوله‌های «ایجاد شکاف دیجیتالی و تشدید نابرابری اجتماعی» و «بهره‌گیری در ایجاد و تشدید ناآرامی‌های مدنی» با فراوانی‌های ۹ و ۷، می‌تواند تهدیدی در بعد اجتماعی و فرهنگی برای ج.ا.ایران به شمار آید.

در حوزه اجتماعی-فرهنگی، چالش بنیادین فراتر از صرفِ دسترسی به محتوای ممنوعه است؛ موضوع بر سر تغییر «قابِ مرجع» (Frame of Reference) هویتی جامعه است. با گسترش اینترنت ماهواره‌ای، کنترل نهادهای فرهنگی بر فرآیند جامعه‌پذیری

دیجیتال به شدت کاهش می‌یابد. این فناوری با تسریع ادغامِ کاربران در اکوسیستم فرهنگی غرب، زمینه‌ساز شکاف‌های هویتی و تضعیف هویت ملی در برابر «هویت بیگانه» می‌شود. انتشار اخبار جعلی در این بستر با سرعتی غیرقابل‌مهار، به‌گونه‌ای است که حتی اقدامات اصلاحی رسانه ملی نیز به دلیل تأخیر در بازتولید روایت، در فضای شناختیِ تحت سیطره الگوریتم‌های بیگانه، ناتوان از اقناع‌سازی مخاطب عمل می‌کند.

در بعد تهدیدات اقتصادی، توزیع فراوانی پاسخ تعداد ۲۰ نفر مصاحبه‌شونده (جامعه خبرگان) مؤید این مطلب است که به تأیید تعداد ۱۱ نفر از مصاحبه‌شوندگان، بیش‌ترین فراوانی، با ۱۸ کد باز احصا شده، مربوط به مقوله «رقابت نابرابر با کاربرهای داخلی و کاهش اشتغال» بوده است و پس‌ازآن، به تأیید تعداد ۱۰ نفر از ۲۰ نفر مصاحبه‌شونده، مقوله «خروج ارز و قاچاق کالا» با فراوانی ۱۵ کد باز احصا شده، در مرتبه دوم قرار دارد سپس به تأیید تعداد ۹ نفر از مصاحبه‌شوندگان، مقوله «فشار بر زیرساخت‌های اقتصادی» با فراوانی ۱۵ کد باز احصا شده، در مرتبه سوم قرار گرفته است.

در رتبه‌های چهارم و پنجم، به ترتیب، با تأیید تعداد ۴ و ۳ نفر از ۲۰ نفر مصاحبه‌شونده، مقوله‌های «بهره‌گیری علیه امنیت ارتباطات و اطلاعات نظام بانکداری» و «گسترش جرائم مالی در بستر فضای مجازی» با فراوانی‌های ۴ و ۴، می‌تواند تهدیدی در بعد اقتصادی برای ج.ا.ایران به شمار آید.

در بعد اقتصادی، تهدیدات استارلینک در سطح استراتژیک به معنای ایجاد یک «اقتصاد دیجیتال موازی» است که خارج از نظارت و مقررات‌گذاری ملی عمل می‌کند. این وضعیت نه تنها رقابت نابرابر با سرویس‌دهندگان داخلی را تشدید بلکه باعث خروج سرمایه و کاهش اشتغال در حوزه آی‌تی می‌شود و استقلال زیرساختی کشور را به چالش می‌کشد. این وضعیت نشان می‌دهد که وابستگی به چنین شبکه‌ای برای خدمات پایه، کشور را در بلندمدت از مسیر توسعه بومی و خودکفایی دیجیتال منحرف و زیرساخت‌های اقتصادی را در برابر اهرم‌های فشار خارجی در شرایط تحریم یا منازعات بین‌المللی، به شدت نفوذپذیر و آسیب‌پذیر می‌سازد.

نتایج حاصله مبین این مطلب است که در صورت فراگیری و عملیاتی‌شدن کاملِ اینترنت ماهواره‌ای استارلینک، تهدیدات برآمده از آن نه یک پدیده تک‌بعدی، بلکه

به یک «تهدید ترکیبی و چندلایه» بدل خواهد شد که بنیان‌های حاکمیت ملی را در ساحت‌های نظامی، سیاسی، اجتماعی و اقتصادی به چالش خواهد کشید. شواهد نشان می‌دهد که این فناوری در آینده به مثابه یک «محرک گسستِ ساختاری» عمل خواهد کرد که با عبور از حصارهای سنتیِ نظارتی و زیرساختی، ابزارهای کلاسیکِ حکمرانی را با ناکارآمدیِ بنیادین مواجه خواهد ساخت. همگراییِ این تهدیدات در ابعاد چهارگانه، کشور را در معرضِ وضعیتِ نوینِ «آسیب‌پذیریِ شبکه‌ای» قرار خواهد داد؛ وضعیتی که در آن، استراتژی‌های واکنشیِ مبتنی بر انسدادِ فیزیکی یا پارازیت، کاراییِ گذشته را از دست خواهند داد. بنابراین، گذار از رویکردِ «تهدیدمحورِ منفعل» به سمت «حکمرانیِ فعالِ سایبری» و بازتعریفِ الگوی مواجهه با این فناوریِ نوظهور از طریق تقویت زیرساخت‌های بومی، به ضرورتی استراتژیک و حیاتی برای حفظ امنیت ملی و بازیابی اقتدار در فضای دیجیتال در افق پیش رو تبدیل خواهد شد.

ب- پیشنهادها

با توجه به ماهیت پویا و پیش‌رونده فناوری‌های ماهواره‌ای و با هدف مواجهه فعال با سناریوهای محتمل در آینده، پیشنهادهای زیر برای بهره‌برداری ارائه می‌شود:

الف) پیشنهادهای راهبردی

۱- شکل‌گیری «پدافند سایبری چندلایه»: با توجه به ابعاد ترکیبی تهدیدات استارلینک، بازتعریف ساختار پدافند غیرعامل کشور با محوریت هم‌افزایی میان بخش‌های نظامی، ارتباطی و امنیتی جهت رصد مستمر، کشف سیگنال و مدیریت مخاطرات امنیتی اینترنت ماهواره‌ای در افق آینده، به یک ضرورت راهبردی تبدیل خواهد شد.

۲- سرمایه‌گذاری روی فناوری‌های جایگزین و بومی: تسریع در توسعه شبکه ملی اطلاعات و حمایت ساختاری از پروژه‌های بومی ارتباطات پهن‌باند (نظیر توسعه فیبر نوری و منظومه‌های ماهواره‌ای بومی/منطقه‌ای) به منظور کاهش جذابیت و نیاز عمومی به شبکه‌های خارجی، باید به عنوان اولویت اول توسعه زیرساختی کشور تعریف گردد.

ب) پیشنهادهای کاربردی و عملیاتی

۱- توسعه ابزارهای فنی پایش و آشکارسازی: سرمایه‌گذاری و حمایت از شرکت‌های دانش‌بنیان داخلی جهت طراحی و تولید تجهیزات فنی آشکارسازی فرکانسی و پایش ترمینال‌های زمینی فعال استارلینک (گیرنده‌ها) به منظور پیشگیری از نشت اطلاعات حساس نظامی و اداری.

۲- تاب‌آوری و امن‌سازی زیرساخت‌های بانکی و حیاتی: تدوین پروتکل‌های امنیتی نوین برای شبکه بانکی و پایگاه‌های داده حیاتی کشور جهت جلوگیری از دور زدن کانال‌های امن ارتباطی و کاهش ریسک جاسوسی اطلاعات مالی در بستر شبکه‌های ماهواره‌ای غیرمجاز.

۳- بازمهندسی الگوهای رسانه‌ای و اقناع عمومی: تغییر رویکرد رسانه ملی و رسانه‌های رسمی از مدل یک‌سویه به سمت رویکردهای مشارکتی و تولید محتوای جذاب، غنی و متناسب با نیاز جامعه، تا از این طریق میزان تمایل شهروندان به استفاده از شبکه‌های خارجی کاهش یافته و اثرات نفوذ فرهنگی-اجتماعی استارلینک در آینده به حداقل برسد.

منابع و مراجع

الف: منابع فارسی

کتب

- ادوارد ای. آزر و چونگ این مون. (۱۳۷۹). امنیت ملی در جهان سوم، ترجمه پژوهشکده مطالعات راهبردی، تهران: پژوهشکده مطالعات راهبردی.
- افتخاری،۱. (۱۳۸۵). کالبدشکافی تهدید، تهران: دانشگاه امام حسین (علیه‌السلام) مرکز چاپ و انتشارات سپاه.
- افتخاری،۱. (۱۳۹۱) تهدیدی نرم (رویکردی اسلامی)، تهران: پژوهشکده مطالعات فرهنگی و اجتماعی.
- بوزان، ب (۱۳۷۹) مردم دولت‌ها و هراس، تهران: پژوهشکده مطالعات راهبردی.
- بوزان، باری؛ الی، ویور و دو ویلد، پاپ. (۱۳۸۶). «چارچوبی تازه برای تحلیل امنیت»، ترجمه علیرضا طیب، تهران: پژوهشکده مطالعات راهبردی.
- عبدالله‌خانی، ع. (۱۳۸۶). تهدیدات امنیت ملی (شناخت و روش)، تهران: ابرار معاصر.
- عبدالله‌خانی، ع. (۱۳۸۹) نظریه‌های امنیت، تهران: ابرار معاصر.
- عمید، حسن. (۱۳۶۲). فرهنگ عمید، تهران: امیرکبیر.
- مرادیان،.م. (۱۳۹۳). مبانی نظری امنیت، تهران: دانشگاه علوم و فنون فارابی.
- معین، م. (۱۳۷۸). فرهنگ معین، تهران: زرین.

مقالات و پایان‌نامه‌ها

- احترام، محسن و احمدی، مریم. (۱۴۰۰). فنّاوری اینترنت ماهواره‌ای به‌عنوان پیشران و یا تهدید فراروی انقلاب اسلامی در گام دوم (مطالعه موردی: پروژه استارلینک)، دومین همایش سراسری پیشران‌ها و تهدیدهای فراروی انقلاب اسلامی در گام دوم، تهران.
- ترابی، قاسم. (۱۴۰۰). ابعاد امنیتی سرویس اینترنت ماهواره‌ای، نشریه دیدبان امنیت ملی، ۱۷۱ - ۱۷۶.
- حکمی زاده، فرشاد و فرازمند، عاطفه. (۱۴۰۲). بررسی راهبردهای منظومه ماهواره‌ای استارلینک از منظر عوامل راهبردی چهارگانه قوت، ضعف، تهدید و فرصت، سومین کنفرانس بین‌المللی پژوهش‌ها و دستاوردهای نو در علوم مهندسی و فنّاوری‌های نوین، تهران.
- لک، حامد. (۱۴۰۰). تأثیر تهدیدات سایبری بر امنیت ملی جمهوری اسلامی ایران، پایان‌نامه کارشناسی ارشد، دانشکده علوم سیاسی دانشگاه اصفهان.
- وکیلی، سهیل؛ اعتضادی‌فر، پوریا و طلعتی، سعید. (۱۴۰۰). تحلیل و بررسی پیرامون سامانه استارلینک. پنجمین همایش بین‌المللی دانش و فنّاوری مهندسی برق، کامپیوتر و مکانیک ایران. تهران.

ب: منابع انگلیسی

- Elon Musk says SpaceX's Starlink satellites active over Ukraine after request from embattled country's leaders. ,2022) February 22.(independent.

- **Musk, E. .(2022) SpaceX and the role of satellite internet in global crises: The Starlink response to the Ukraine conflict. Global Communications Review, 45(3.210-223 ,(** https://doi.org/10.1002/gcr.3125
- Musk, E. .(2022) Starlink and its Role in Global Connectivity and Security. SpaceX Press.
- Pillay, S. .(2022) Starlink and the future of internet infrastructure in wartime. International Journal of Communications, 56(4.99-115 ,(https://doi.org/10.1177/1234567890
- Zeng, J., & Liu, F. .(2023) Satellite internet systems and national security: The dual-use challenge of Starlink. Journal of Military and Security Studies, 19(1.23-41 ,(https://doi.org/10.1016/j.jmss.2023.01.007
- Zeng, L., & Liu, Y. .(2023) Impact of Satellite Communications in Modern Warfare and Security. International Journal of Defense Studies, 11(2.92-107 ,(
- SpaceX. .(2021) Petition of Starlink Services, LLC for Designation as an Eligible Telecommunications Carrier. SpaceX .
- SpaceX. .(2023) Technical Updates on Starlink. Retrieved from SpaceX official website.
- SpaceX. .(2024) Starlink Mission Updates. Retrieved from]https://www.spacex.com)[https://www.spacex.com(
- Weiss, J. .(2020) Cybersecurity for Critical Infrastructure Protection: A Comprehensive Approach. Springer.