فصلنامهٔ مطالعات بنیادین و کاربردی جهان اسلام،
سال ششم، شمارهٔ بیست‌ودوم، زمستان ۱۴۰۳
https://doi.org/10.22034/fasiw.2025.481812.1390

انجمن ژئوپلیتیک ایران
Iranian Association of Geopolitics (I.A.G)

نوع مقاله: علمی ـ پژوهشی

فضای سایبری در راهبرد آفندی و پدافندی اسرائیل از منظر اسناد بالادستی

* سید امین حبیبی[۱]، عارفه عباسی کرافشانی[۲]

۱. دکتری روابط بین‌الملل، استاد میهمان دانشکده حقوق، الهیات و علوم سیاسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی
۲. دانش‌آموخته علوم سیاسی، پژوهشگر حوزه بین‌الملل

اطلاعات مقاله

تاریخ دریافت: ۱۳ مهر ۱۴۰۳
تاریخ پذیرش: ۵ آذر ۱۴۰۳
تاریخ انتشار: ۲۰ اسفند ۱۴۰۳

کلیدواژه‌ها:
فضای سایبری، اسرائیل، راهبردهای نظامی، امنیت ملی، اسناد بالادستی اسرائیل، امنیت موسع.

* نویسندهٔ مسئول:
دکتر سید امین حبیبی
نشانی: دکتری روابط بین‌الملل، استاد میهمان دانشکده حقوق، الهیات و علوم سیاسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی.
پست الکترونیک:
se.aminhabibi@gmail.com

چکیده

تهدیدات امنیتی نوین همچنین مفهوم امنیت موسع، امروزه چالش‌های فراوانی را پیش روی بازیگران منطقه‌ای قرار داده است. در این بین، فضای سایبری طی دهه گذشته تبدیل به یکی از مهم‌ترین میدان‌های نبرد شده است. فضای سایبری در کنار فرصت‌های بی‌شماری که برای بشر ایجاد می‌کند، درعین‌حال خالق تهدیدات نوین و چالش‌های جدی برای امنیت جوامع انسانی نیز است. اسرائیل با درک اهمیت فضای مذکور، هم در نقش محافظ امنیت و جبران‌کننده ضعف‌های ژئوپلیتیکی و هم در نقش عامل بازدارنده و تهاجمی، علاوه‌بر سرمایه‌گذاری‌های شگرف مادی و انسانی، راهبردهای منظم و دقیقی در رابطه با آن تدوین کرده است. این پژوهش درصدد است که با مطالعه اسناد راهبردی اسرائیل در حوزه سایبر، به سؤال «فضای سایبر چه نقشی در راهبردهای نظامی اسرائیل بازی می‌کند؟» پاسخ دهد. باتوجه‌به یافته‌های پژوهش، اسرائیل با ایجاد همکاری‌های نزدیک میان نهادهای نظامی- امنیتی و شرکت‌های فعال خصوصی در حوزه امنیت سایبری و با تعریف کردن آن‌ها زیر یک چتر واحد توانسته حوزه آفندی و پدافندی خود را توأمان پوشش دهد و همچنین تا حد زیادی تهدیدات این حوزه‌ها را کنترل و اقدام به خلق بازدارندگی سایبری کند. اسرائیل در چهار بعد اقتصادی، نظامی- اطلاعاتی، اجتماعی و سیاسی به‌صورت تفکیک‌شده راهبردهای سایبری خود را طرح‌ریزی کرده است. همچنین اسرائیل توانسته با توانایی‌های خود در حوزه سایبر، اشراف اطلاعاتی، جاسوسی و خرابکاری خود را در منطقه و جهان بسط و گسترش دهد.

استناد به این مقاله:
حبیبی، سید امین و عباسی کرافشانی، عارفه . (۱۴۰۳). فضای سایبری در راهبرد آفندی و پدافندی اسرائیل از منظر اسناد بالادستی. مطالعات بنیادین و کاربردی جهان اسلام، ۶(۴)، ۱۶۴-۱۳۹.

۱. مقدمه

با ورود به عصر جهانی شدن و پیشرفت فناوری، حکمرانی دولت‌ها دستخوش تغییر شده و فضای سایبری بیشترین نقش را در این تحول داشته است؛ به‌طوری‌که در مواردی موجب بهینه‌سازی حکمرانی شده و از سوی دیگر، تهدیدات جدیدی را نیز موجب شده و تهدیدات سایبری را جزئی جدایی‌ناپذیر از مطالعات امنیتی قرار داده است. اسرائیل با استفاده از فناوری‌های غربی، از فضای سایبری در امور نظامی، دفاعی و جاسوسی بهره می‌برد و به‌دلیل تهدیدات ژئوپلیتیکی و محدودیت عمق استراتژیک، به فضای سایبری به‌عنوان یک حوزه حیاتی در ابعاد آفندی و پدافندی می‌نگرد. محیط سایبری، برخلاف محیط جغرافیایی سنتی، دارای ویژگی‌های منحصربه‌فردی مانند گستردگی زیرساخت‌های شبکه‌ای و سرعت بالای انتقال داده‌هاست. این ویژگی‌ها به اسرائیل امکان داده‌اند تا توانمندی‌های نظامی خود را در این فضا توسعه دهد و با بهره‌گیری از روش‌های جدید جنگی، موازنه قدرت را تغییر دهد. اسرائیل که همواره با تهدیدات وجودی مواجه بوده، فضای سایبری را در اولویت قرار داده و در این حوزه سرمایه‌گذاری گسترده‌ای انجام داده است. این کشور با در اختیار داشتن ۱۲ درصد از ۵۰۰ شرکت بزرگ امنیت سایبری جهان و ۴۷۰ استارتاپ فعال در این زمینه، دومین مرکز بزرگ امنیت سایبری در جهان محسوب می‌شود. در سال ۲۰۲۱، صادرات محصولات امنیت سایبری این رژیم سه برابر بیشتر از بریتانیا بود. (Eisenstadt, 2021:1)

فضای سایبری از سه لایه انسانی، نرم‌افزاری و فیزیکی تشکیل شده است که هر سه می‌توانند اهداف آفندی و پدافندی باشند. حملات در این فضا می‌توانند شامل تغییر رفتار کاربران، نفوذ نرم‌افزاری برای جاسوسی و حمله به زیرساخت‌های فیزیکی باشند. ازجمله تهدیدات می‌توان به ایجاد اختلال در نیروگاه‌ها یا سیستم‌های ناوبری هواپیما اشاره کرد. این مقاله جایگاه فضای سایبر در اسناد بالادستی اسرائیل و استراتژی‌های آفندی و پدافندی این رژیم را بررسی می‌کند. فرضیه تحقیق این است که اسرائیل با ایجاد هماهنگی بین نهادهای نظامی- امنیتی و شرکت‌های سایبری، راهبردهای جامعی در این حوزه اجرا کرده و تا حد زیادی تهدیدات سایبری را کنترل می‌کند. اسرائیل راهبردهای سایبری خود را در چهار بعد اقتصادی، نظامی- اطلاعاتی، اجتماعی و سیاسی طرح‌ریزی کرده و با توانایی‌های خود در این حوزه، نفوذ اطلاعاتی، جاسوسی و خرابکاری خود را در سراسر جهان گسترش داده است. روش تحقیق این مقاله مبتنی بر گردآوری داده‌ها به‌صورت اسنادی و تحلیل توصیفی است و یافته‌های آن در پنج بخش بررسی می‌شود: نقش فضای سایبری در اسناد بالادستی اسرائیل، رویکردهای پدافندی

و آفندی در راهبردهای سایبری این رژیم، پرورش نیروی ماهر در این حوزه و جایگاه فضای سایبری در استراتژی‌های کلان نظامی اسرائیل.

۲. پیشینه پژوهش

پژوهش‌های متعددی در رابطه با اهمیت فضای سایبری و امنیت سایبری انجام شده است. استفاده از فضای سایبری در اتخاذ راهبردهای نظامی به‌صورت اخص نیز مورد توجه پژوهشگران بوده و پژوهش‌های مرتبطی در این زمینه وجود دارد. کار ویژه و هدف این پژوهش اما بررسی جایگاه فضای سایبری از منظر اسناد بالادستی در اتخاذ راهبردهای آفندی و پدافندی مختص به اسرائیل است. با کلیدواژه‌های اسرائیل و امنیت سایبری پژوهش‌هایی به فارسی و انگلیسی وجود دارند که بررسی آن‌ها برای نیل به هدف پژوهش حاضر ضروری است. ابتدا مقاله محمد سهرابی و احسان جنتی با عنوان «اولویت‌های سیاست خارجی و امنیتی اسرائیل در فضای نوین منطقه‌ای» در ۱۳۹۴ بررسی شد که در آن پژوهشگران با بررسی عوامل نوین امنیتی ازجمله فضای سایبری، استراتژی‌های نظامی اسرائیل در منطقه را تبیین کرده‌اند، اما کار ویژه پژوهش موارد مضیق امنیتی بوده و امنیت موسع به‌صورت اجمالی بررسی شده و موضوع امنیت سایبری و بازدارندگی سایبری مغفول مانده است. مقاله ولی‌گل محمدی و طاهره جمشیدی با عنوان «بازدارندگی سایبری و تحول در دکترین دفاعی اسرائیل» در ۱۴۰۱ نیز بررسی شد. این پژوهش با تبیین مفهوم بازدارندگی سایبری، دکترین دفاعی اسرائیل را بررسی کرده که هدف آن بررسی صرف منطق دفاعی و تبیین دکترین دفاعی و نه آفندی این رژیم است. همچنین مقاله امیررضا مقومی و روح‌الله قادری با عنوان «تغییر و تداوم اصول امنیت ملی رژیم صهیونیستی» در ۱۴۰۱ نیز بررسی شد. این پژوهش اولویت‌های اصول امنیتی اسرائیل در طول زمان را بررسی کرده و اشاره می‌کند که با روی کار آمدن فضای مجازی دکترین‌های امنیتی و نظامی سایبری در اسرائیل مورد توجه قرار گرفته و به کار برده شده است. در زبان انگلیسی نیز مقاله متیو کهن با عنوان «اسرائیل و فضای سایبری» در سال ۲۰۱۷ بررسی شد که نویسنده با بیان اهمیت جایگاه فضای سایبر در اسرائیل، توجه تصمیم‌گیران این رژیم به فضای سایبری را تبیین کرده است. همچنین در مقاله بن عطار با عنوان «امنیت سایبری در اسرائیل» در سال ۲۰۲۱، جایگاه امنیت سایبری در دکترین امنیتی اسرائیل را تبیین کرده است. درنهایت، اما بررسی اسنادی قوانین و اسناد سیاستی و بالادستی اسرائیل به‌دلیل تبیین جایگاه امنیت سایبری و همچنین چگونگی اتخاذ دکترین‌های آفندی و پدافندی نظامی این رژیم (به‌طورتوامان) در مقالات فوق مغفول مانده است که اهمیت و ضرورت پژوهش حاضر را نمایان می‌کند.

۳. چهارچوب نظری

الف) فضای سایبر

محیط یا فضای سایبر به‌صورت کلی دارای تعاریف متعدد است که بسیاری از آن‌ها دارای جنبه‌های مشترک و هم‌پوشان هستند، اما در این میان تعریفی جامع در مورد محیط سایبر وجود دارد که مختص به اتحادیه بین‌المللی ارتباطات از راه دور سازمان ملل متحد[1] است. در این تعریف فضای سایبر عبارت است از حوزه فیزیکی و غیرفیزیکی متشکل از عناصری مانند اقسام کاربران، رایانه‌ها، سیستم‌های رایانه‌ای، شبکه‌ها و برنامه‌های نرم‌افزاری و درنهایت داده‌های رایانه‌ای و محتوایی. (ITU,2018) این تعریف حاکی از آن است که فضای سایبری شامل سه لایه وابسته به هم است: الف) لایه انسانی: اقسام مختلف کاربران رایانه‌ها که می‌توانند حقوقی، حقیقی، دولتی و غیره باشند. ب) لایه برنامه‌ای: نرم‌افزار و بیت‌ها[2]، اجزای این لایه با سرعت نور حرکت می‌کنند و دستورالعمل‌ها و اطلاعات مهم فضای سایبر (مانند اطلاعات نرم‌افزارها و صندوق‌های الکترونیکی)، بدافزار و موارد دیگر را در برمی‌گیرد. ج) لایه فیزیکی: اجزای فیزیکی فضای سایبر ازجمله وسایل سخت‌افزاری و زیرساخت‌های آن موجود در زمین، دریا، هوا و فضا. باتوجه‌به دسته‌بندی لایه‌های فوق‌الذکر، فضای سایبر یک فضای مجازی و غیر فیزیکی است که با کمک حوزه الکترومغناطیس با حوزه‌های فیزیکی نیز ارتباط برقرار می‌کند. (Foulan, 2024) به‌این‌ترتیب، فضای سایبری در امور نظامی برای تقویت عملکرد سیستم‌های نظامی و غیرنظامی فعال در همه حوزه‌ها نقش حیاتی ایفا می‌کند، اما درعین‌حال آن‌ها را در معرض حملات فضای سایبری نیز قرار می‌دهد.

ب) مکتب کپنهاگ و امنیت موسع

مکتب کپنهاگ تلاش می‌کند تا مطالعات امنیتی را از حوزه روابط نظامی و قدرت سخت فراتر ببرد و موضوعات اقتصادی، سیاسی، اجتماعی، محیط‌زیستی و تکنولوژیکی را به امنیت بیفزاید. این مکتب امنیت را مفهومی چندبعدی می‌داند که از سطوح متنوع و مرتبط با یکدیگر تشکیل شده است. نخستین پایه‌های این مکتب در دهه ۱۹۸۰ با آثار بری بوزان، ازجمله کتاب «مردم، دولت و هراس» شکل گرفت و سپس با اندیشه‌های ویور توسعه یافت. (Habibi & Ghorbani, 2017)

1. International Telecommunication Union
2. bits

یکی از مفاهیم کلیدی این مکتب، امنیتی‌سازی است که بیان می‌کند همه ابعاد زندگی انسانی می‌توانند جنبه‌های امنیتی داشته باشند. این رویکرد درحالی‌که برخی مفاهیم نظریه‌های سنتی امنیت را حفظ کرده، اما حوزه‌هایی مانند امنیت موسع را نیز دربر می‌گیرد. طی دو دهه گذشته، این مکتب به یکی از مهم‌ترین رویکردهای مطالعات امنیتی تبدیل شده است. امنیتی‌سازی فرایندی است که طی آن، موضوعاتی که قبلاً در حوزه امنیت تعریف نمی‌شدند، امنیتی تلقی می‌شوند. (Dehghani, 2018) مکتب کپنهاگ امنیت را پدیده‌ای نسبی و موسع می‌داند و بر ارتباط متقابل امنیت ملی با الگوهای منطقه‌ای و بین‌المللی تأکید دارد. این پیوستگی امنیتی منجر به ظهور بازیگران جدیدی در حوزه امنیت شده است که نه‌تنها به مسائل نظامی، بلکه به حوزه‌های غیرنظامی مانند اقتصاد، بهداشت، محیط‌زیست و فناوری نیز می‌پردازند. (Habibi et al., 2024) این تحول باعث شده ماهیت فعالیت‌های نظامی- امنیتی تغییر کند و امنیت بین بازیگران منطقه‌ای و جهانی به شکل پیچیده‌تری درهم‌تنیده شود. درنتیجه کشورها در حوزه‌هایی فعالیت می‌کنند که پیشتر خارج از قلمرو مسائل امنیتی تلقی می‌شدند.

ج) امنیت سایبری و بازدارندگی سایبری

با گسترش جهانی شدن، انقلاب تکنولوژیکی و نفوذ اینترنت در تمامی جنبه‌های حکمرانی، اقتصاد و فرهنگ امنیت سایبری به یکی از محورهای مطالعات امنیتی تبدیل شده است. ظهور تهدیدات و فرصت‌های جدید در این فضا، دولت‌ها را وادار به ایجاد چهارچوب‌های نظارتی و سیاست‌گذاری برای حفظ ثبات و کنترل بحران‌ها کرده است. (Kello, 2013) در روابط بین‌الملل، امنیت سایبری شامل مجموعه‌ای از سیاست‌ها، تصمیم‌گیری‌ها و راهبردهایی است که به شناسایی، نظارت و رفع تهدیدات سایبری کمک می‌کند. در دنیای امروز، امنیت سایبری برای دولت‌ها به یک ضرورت تبدیل شده و حکمرانی کارآمد بدون در نظر گرفتن این فضا غیرممکن است. بازدارندگی یکی از راهبردهای کلیدی امنیتی است که در حوزه‌های نظامی، موشکی، فضایی و سایبری کاربرد دارد. این نظریه ابتدا در دوران جنگ سرد برای توصیف تأثیر سلاح‌های هسته‌ای در جلوگیری از درگیری مستقیم شکل گرفت. (Bendiek & Metzger, 2015:55) امروزه مفهوم بازدارندگی فراتر رفته و شامل ابزارهای اقتصادی، اطلاعاتی، جاسوسی، تکنولوژیکی و رسانه‌ای شده است که به آن بازدارندگی مدرن گفته می‌شود. (Burak Tolga, 2018:7) ویژگی‌های بازدارندگی سایبری شامل ماهیت مجازات و تنبیهی است، به‌طوری‌که قدرت سایبری یک کشور می‌تواند موجب ترس دشمن و مانع از اقدام خصمانه شود. همچنین فراتر از حوزه سایبری عمل کند و بازدارندگی سایبری

می‌توانـد دشـمن را از حمـلات فیزیکـی، موشـکی و جاسوسـی نیـز بـازدارد. از سـویی دیگـر، بـا کمـک ایـن راهبـرد، واکنـش بـه تهدیـدات امنیتـی- نظامـی می‌توانـد هـم به‌صـورت سـنتی (نظامـی) و هـم به‌صـورت سـایبری انجـام شـود. (Bendiek & Metzger, 2015:54) درنتیجـه فضـای سـایبری نه‌تنهـا بـه یـک عرصـه نویـن بـرای رقابت‌هـای امنیتـی- نظامـی تبدیـل شـده اسـت، بلکـه ابزارهـای جدیـدی را بـرای ایجـاد بازدارندگـی در سـطح بین‌المللـی فراهـم کـرده اسـت.

۳. مؤلفه‌های نظامی فضای سایبری در اسناد بالادستی اسرائیل

اسـرائیل همـواره بـه دنبـال افزایـش برتـری سـایبری خـود در حـوزه نظامـی و امنیتـی بـوده اسـت. بـرای نیـل بـه ایـن هـدف، ایـن رژیـم راهبردهـای کلان و اسـناد بالادسـتی را تدویـن کـرده اسـت. کمیتـه «حفاظـت از زیرسـاخت‌های حیاتـی» مسـئول تدویـن «سـند ملـی فضـای سـایبر» اسـت کـه اسـتراتژی‌های نظامـی- سـایبری اسـرائیل را تعییـن می‌کنـد. سـاخت اسـتاکس‌نت به‌عنـوان بخشـی از راهبـرد ایـن کمیتـه، نشـان‌دهنده تمرکـز اسـرائیل بـر عملیات‌هـای تهاجمـی و دفاعـی سـایبری اسـت. سـند امنیـت سـایبری رژیـم بـا هـدف تبدیـل اسـرائیل بـه مرکـز جهانـی توسـعه فنـاوری اطلاعـات و افزایـش امنیـت زیرسـاخت‌ها تدویـن شـد. در بنـد ۳۶۱۱ سـند «امنیـت فضـای سـایبر اسـرائیل» (۲۰۱۱)، پیشـبرد قابلیت‌هـای سـایبری به‌عنـوان اسـتراتژی اصلـی رژیـم تصویـب شـد. (Stancu & Pavel, 2023: 2-3) راهبـرد امنیـت سـایبری اسـرائیل علاوه‌بـر حفاظـت از زیرسـاخت‌ها بـه دنبـال رشـد اقتصـادی، رفـاه اجتماعـی و حفـظ موقعیـت بین‌المللـی ایـن رژیـم به‌عنـوان رهبـر فناوری‌هـای نویـن اسـت. اولیـن گام مهـم در توسـعه امنیـت سـایبری اسـرائیل در سـال ۲۰۰۲، بـا اجـازه سـازمان امنیـت اطلاعـات ملـی، بـرای محافظـت از سیسـتم‌های رایانـه‌ای حیاتـی برداشـته شـد. تأسـیس دفتـر ملـی سـایبری در سـال ۲۰۱۲ و تصویـب دو قطعنامـه کلیـدی در سـال ۲۰۱۵ باعـث ایجـاد «سـازمان امنیـت سـایبری ملـی» شـد کـه اکنـون مسـئول هدایـت امنیـت سـایبری در اسـرائیل اسـت. ایـن سـازمان سیاسـت‌ها و راهبردهـای سـایبری را طراحـی و توسـعه قابلیت‌هـای دفاعـی و تهاجمـی را مدیریـت می‌کنـد. (Baezner & Cordey, 2019: 6-9) راهبـرد امنیـت سـایبری اسـرائیل بـر سـه لایـه عملیاتـی اسـتوار اسـت: لایـه اول: استحکام‌بخشـی سـایبری جمعـی کـه بـر افزایـش مقاومـت سـازمان‌ها دربرابـر حمـلات سـایبری تمرکـز دارد. لایـه دوم: انعطاف‌پذیـری سیسـتمی کـه بـر مقابلـه بـا حمـلات قبـل، حیـن و بعـد از وقـوع تأکیـد دارد و از طریـق اشـتراک‌گذاری اطلاعـات و کمـک بـه سـازمان‌ها اجـرا می‌شـود. لایـه سـوم: دفـاع سـایبری کلان کـه تهدیـدات پیشـرفته و خطـرات جـدی را بررسـی می‌کنـد و راه‌حل‌هایـی بـرای مقابلـه بـا آن‌هـا ارائـه می‌دهـد. (Baezner & Cordey, 2019:

6-12) این رویکرد سه‌لایه‌ای راه‌حلی جامع را برای مقابله با تهدیدات سایبری ارائه می‌دهد و باتوجه‌به سطح تهدید و ماهیت حمله، واکنش مناسب را مشخص می‌کند. نمودار مرتبط نحوه عملکرد اسرائیل را باتوجه‌به بزرگی تهدیدات و مداخله دولت نشان می‌دهد، به‌گونه‌ای‌که اقدامات دفاعی می‌توانند براساس شدت تهدیدات تشدید شوند.

۴. قانون‌گذاری و سیاست‌گذاری سایبری در اسرائیل

قانون‌گذاری سایبری در اسرائیل در دو سطح مرکزی و پیرامونی انجام می‌شود. دستگاه‌های اجرایی برای رفع نیازهای تخصصی خود، مقررات خاصی را تدوین می‌کنند، درحالی‌که نهادهای مرکزی چهارچوب کلی قانون‌گذاری را مشخص می‌کنند. برای مثال، مقررات دفاع سایبری در حوزه سلامت توسط وزارت بهداشت تعیین می‌شود و شرکت‌های آب تحت نظارت وزارت امور زیربنایی قرار دارند. در سطح مرکزی، یک مرجع اصلی مانند دفتر سایبری و سازمان دفاع دسته‌جمعی چهارچوبی واحد برای امنیت سایبری در بخش‌های نظامی و غیرنظامی تعیین می‌کند. این ساختار به‌ویژه باتوجه‌به پیچیدگی‌های فناوری و نیاز به یکپارچگی امنیتی، در سال ۲۰۱۱ با ایجاد «ستاد سایبری» تقویت شد. این ستاد مسئول توسعه فضای سایبری، هماهنگی سازمان‌های مختلف، افزایش امنیت زیرساخت‌ها و تبدیل اسرائیل به مرکز دانش سایبری در سطح جهانی است. (Ta-bansky, 2020: 50-53) بررسی قوانین و اسناد بالادستی اسرائیل نشان می‌دهد که بازدارندگی سایبری و ارتقای قدرت سایبری این رژیم بر چند مؤلفه کلیدی استوار است: ابتدا مشاوره با نخست‌وزیر و کابینه در حوزه امنیت سایبری از طریق ستاد امنیت و هماهنگی فعالیت‌های دولت و پیگیری اجرای تصمیمات امنیت سایبری. از طرفی ارائه سیاست‌های کلان سایبری و اجرای آن‌ها تحت نظارت دولت (Finkel, 2020: 12)، تدوین و ابلاغ بخشنامه‌های امنیتی به نهادهای مرتبط و ارزیابی سالانه تهدیدات سایبری (Sayyad et al., 2020: 300-310)، ترویج تحقیق و توسعه در فضای سایبری و حمایت از صنعت امنیت سایبری در سرزمین‌های اشغالی و تدوین سند ملی مقابله با حملات سایبری نیز از دیگر مولفه‌های کلیدی است. برگزاری رزمایش‌های داخلی و بین‌المللی برای افزایش آمادگی سایبری (Mielko, 2023: 3-8)، جمع‌آوری اطلاعات امنیت سایبری از نهادهای اطلاعاتی، ارزیابی وضعیت امنیت سایبری در سطح داخلی، افزایش آگاهی عمومی درباره تهدیدات سایبری، اطلاع‌رسانی و آموزش درباره تهدیدات و روش‌های پیشگیری، توسعه برنامه‌های آموزشی برای استفاده ایمن از فضای سایبری (Reed, 2015)، همکاری بین‌المللی با نهادهای امنیت سایبری، هماهنگی میان کابینه، دانشگاه‌ها، صنعت و سایر نهادها در حوزه سایبری، تقویت

چهارچوب‌های قانونی مرتبط با امنیت سایبری، از دیگر این مولفه‌ها هستند. درنهایت تعیین یک نهاد مرکزی به‌عنوان تنظیم‌کننده قوانین در حوزه امنیت سایبری (Elran, 2015: 3-20) تکمیل کننده این راهبردهاست.

این راهبردها نشان می‌دهند که اسرائیل با رویکردی جامع، بر افزایش قدرت سایبری خود و هماهنگی در سیاست‌گذاری‌های امنیتی تمرکز دارد. جدول زیر به‌صورت کلی، وظایف و نقش ستاد سایبری اسرائیل نشان داده شده است.

جدول ۱. وظایف و نقش ستاد سایبری اسرائیل

ردیف	وظایف و نقش ستاد سایبری در قانون‌گذاری اسرائیل
۱	مشورت با کابینه اسرائیل
۲	برگزاری جلسات و هماهنگی میان بخش‌های مختلف متولی در حوزه سایبر و امنیت
۳	ارائه توصیه‌های سیاست‌گذاری به نخست‌وزیر و مدیران ارشد امنیتی
۴	صدور بخش‌نامه‌های حاصل از تصمیمات کابینه و کمیته‌های مربوطه سایبری و ابلاغ آن‌ها به سایر بخش‌ها
۵	تعیین و اعتبارسنجی سالانه تهدیدات امنیت فضای سایبری
۶	راهبری معاونت تحقیق و توسعه وظایف محوله
۷	ارائه تسهیلات تشویقی به صنعت فضای سایبری در سرزمین‌های اشغالی
۸	تدوین سند بالادستی مقابله با حوادث غیرمترقبه فضای سایبری
۹	برگزاری رزمایش داخلی و بین‌المللی برای ارتقای آمادگی سایبری اسرائیل
۱۰	اخذ نظرات دستگاه‌های اطلاعاتی و امنیتی و تدوین تصویر جامع حوزه سایبری مشتق از آن
۱۱	ارزیابی وضعیت داخلی امنیت سایبری از تمامی ارکان فعال در این زمینه
۱۲	ارتقای آگاهی عمومی از تهدیدات و راه‌های مقابله با آن در فضای سایبر
۱۳	اطلاع‌رسانی عمومی در مورد تهدیدات بالقوه سایبری
۱۴	ترویج برنامه‌های آموزشی برای استفاده هوشمندانه از فضای سایبری
۱۵	ارتقای همکاری بین نهادهای امنیت سایبری اسرائیل و همتایان آن‌ها در خارج
۱۶	ارتقای هماهنگی و همکاری بین نهادها و سازمان‌های دولتی و غیردولتی مرتبط با فضای سایبر
۱۷	ترویج قوانین و مقررات سایبری
۱۸	مرجعیت تصمیم‌گیر نهایی حوزه سایبر

۵. جایگاه فضای سایبری در راهبردهای نظامی اسرائیل

فضـای سـایبری به‌دلیـل ویژگی‌هـای منحصربه‌فـرد خـود، بـه یـک میـدان جنـگ مـدرن تبدیـل شـده اسـت و دولت‌هـا همـواره در حـال آمادگـی بـرای مقابلـه در ایـن فضـا هسـتند. ایـن آمادگـی مسـتلزم قابلیت‌هـا و زیرسـاخت‌های دفاعـی و تهاجمـی اسـت. در بسـیاری از مـوارد، زیرسـاخت‌های نظامـی و غیرنظامـی در فضـای سـایبری بـه هـم مرتبط‌انـد بنابرایـن حفاظـت از زیرسـاخت‌های غیرنظامـی بـرای اهـداف نظامـی نیـز حیاتـی اسـت. بخش‌هایـی ماننـد حمل‌ونقـل، حکمرانـی اجتماعـی، بهداشـت و صنعـت بـه فضـای سـایبری وابسـته‌اند. اسـرائیل به‌شـدت بـه ایـن فضـا متکـی اسـت، به‌طوری‌کـه هرگونـه لطمـه بـه آن، علاوه‌بـر آسـیب‌های نظامـی و اطلاعاتـی، می‌توانـد پیامدهـای اجتماعـی و اقتصـادی گسـترده‌ای داشـته باشـد. بـه همیـن دلیـل، حفـظ ثبـات و امنیـت سـایبری یکـی از اولویت‌هـای کلیـدی در اسـناد راهبـردی نظامـی اسـرائیل اسـت. (Behrami & Araghchi, 2017: 3-6) مؤسسـات امنیـت سـایبری، کـه صهیونیسـت‌ها تأسـیس کرده‌انـد، نقطـه عطفـی در سـامان یافتـن فضـای سـایبری و نظـارت و ارتبـاط نهادهـای نظامـی و اطلاعاتـی اسـرائیل در مواجهـه بـا محیـط چالش‌برانگیـز تهدیـدات نظامـی و غیرنظامـی بـوده اسـت. از اواخـر سـال ۲۰۱۶، دفتـر سـایبری سـند یکپارچـه‌ای را منتشـر کـرد کـه خط‌مشـی کلـی سـایبری رژیـم را تعییـن می‌کنـد کـه پیشـتر بیـان شـد. قطعنامـه ۳۶۱۱[۳] رژیـم، چهـار اولویـت اصلـی اسـرائیل را در حـوزه فضـای سـایبر نشـان می‌دهـد: ۱- ارتقـای توانمندی‌هـای رژیـم و بهبـود مدیریـت چالش‌هـای فعلـی و آتـی فضـای سـایبری ۲- بهبـود دفـاع از زیرسـاخت‌های داخلـی کـه بـرای حفـظ یـک زندگـی باثبـات و سـازنده در سـرزمین‌های اشـغالی ضـروری اسـت ۳- ارتقـای جایـگاه رژیـم به‌عنـوان «مرکـز جهانـی توسـعه فنـاوری اطلاعـات» و ۴- تشـویق همکاری‌هـای بین‌رشـته‌ای بیـن دانشـگاه‌ها، صنعـت، بخـش خصوصـی و وزارتخانه‌هـای حکومتـی و نهادهـای نظامـی و اطلاعاتـی. (Stancu,Pavel,2023: 2-3) ارتـش اسـرائیل بـرای دو دهـه نگـران مسـائل امنیـت و تهدیـدات سـایبری بـوده اسـت. بااین‌حـال، مطابـق بـا رویکـرد آن‌هـا در سـایر حوزه‌هـای سیاسـت دفاعـی، جزئیـات کمـی در مـورد ملاحظـات امنیـت سـایبری و سیاسـت در حـوزه نظامـی اسـرائیل بـا عمـوم بـه اشـتراک گذاشـته شـده اسـت، امـا در آگوسـت ۲۰۱۵، ایـن رژیـم بـا انتشـار «سـند راهبـردی ارتـش صهیونیسـتی»، کـه گادی آیزنکـوت[۴]، رئیـس سـتاد ارتـش تنظیـم کـرده و خلاصـه‌ای طبقه‌بندی‌نشـده از رویکـرد کلـی نظامـی ارتـش در حـوزه سـایبر اسـت، رویکـرد خـود

۳. در این لایحه و قطعنامه که در ۹ صفحه تدوین شده، ابتدا کنست فضای سایبر و قسمت‌های مختلف آن را تعریف عملیاتی کرده سپس وظایف و اهداف تاسیس دفتر سایبری اسرائیل ذکر شده است.

4. Gadi Eisenkot

را در زمینه نظامی مشخص کرد. این سند شامل مواضع ارتش اسرائیل در مورد امنیت سایبری است که ازجمله می‌توان به درک اینکه فضای سایبری یک قلمرو نظامی است، اشاره کرد؛ اولویت‌بندی تداوم ایجاد ظرفیت دفاع سایبری و حمله در سطوح راهبردی، عملیاتی و تاکتیکی، آگاهی از تهدیدات در فضای سایبری و آغاز فرایندی برای تأسیس ساختار فرماندهی سایبری در داخل ارتش رژیم از دیگر موارد مذکور است. سند راهبرد ارتش اسرائیل خاطرنشان می‌کند که «دفاع سایبری در شرایط جنگ و شرایط اضطراری برای تضمین تداوم فعالیت نهادهای رژیم و همچنین عملکرد کافی ارتش آن ضروری است». (Housen-Couriel,2017: 9) همان‌طورکه بیان شد، حفظ وضعیت دفاعی یکی از مهم‌ترین اهداف سند بالادستی اسرائیل در حوزه سایبری است که در دکترین نظامی چند ساله گذشته ارتش اسرائیل قابل‌مشاهده است. در سند سال ۲۰۱۵ گنجانده شده است که دشمنان را نمی‌توان با وضعیت دفاعی صرف شکست داد، درنتیجه «استفاده از راهبرد حمله با روش‌های متنوع جهت شکست دادن رقبا و کسب نتایج نظامی ضروری است». (Adamsky,2017: 120) اجرای راهبرد مذکور با استفاده از فناوری‌های پیچیده و به‌روز رژیم در مقایسه با گذشته تسهیل شده است، اما همچنان بارها در مقابل مهاجمان آسیب‌های جدی دیده است.

ازآنجاکه استفاده از فضای سایبری برای مقاصد نظامی ملموس شده است، اسرائیل برای ایجاد قدرت و تسلیحات سایبری خود به‌طورمنسجم با اولویت از بین بردن سیستم‌های دفاعی پیشرفته دشمن از نظر سایبری، برنامه‌های مدونی را تدوین و اجرا کرده است. در کنار ج.ا.ا و کشورهای منطقه، بازیگران غیردولتی بسیاری نیز هستند که از ظرفیت‌های سایبری بالایی برخوردارند. استفاده فزاینده حماس و حزب‌الله از سلاح‌های سایبری، استراتژی امنیتی اسرائیل را از نظر سیستم‌های دفاعی و عملیات تهاجمی تغییر داده است. رژیم در سال‌های اخیر دچار درگیری‌های متعدد با حماس و حزب‌الله شده است که در آن استفاده از ابزارهای سایبری در کانون توجه قرار گرفته‌اند. (Eizenkot,2016)

توسل به ابزارهای غیرمتعارف مانند تهاجم در فضای سایبر در چهارچوب درگیری‌های کم‌شدت منجر به دگرگونی اساسی در ساختار ارتش اسرائیل شده است. در دکترین امنیتی رژیم در حوزه مذکور، حفظ برتری از نظر توانمندی‌های تکنولوژیکی و اطلاعاتی یکی از اهداف اساسی است. درواقع حوزه سایبری به همراه حوزه‌های زمین، هوا و دریا در پدافند و آفند

چندبعدی گنجانده شده است و ارتش رژیم حوزه سایبر را بیشتر ذیل موضوعات و چالش‌های نظامی می‌پندارد. درواقع، از زمان استاکس‌نت و شواهدی مبنی بر احتمال هدف تسلیحات سایبری تحت حمایت حکومت‌ها و دولت‌ها قرار گرفتن، فعالیت نظامی خود را -دفاعی یا تهاجمی- در حوزه فضای سایبری گسترش داده‌اند. در مورد اسرائیل، سناریو یک حمله سایبری مخرب، شدیداً آسیب‌زاست، زیرا سیستم‌های ارتش صهیونیستی مبتنی بر شبکه هستند و یک حمله سایبری می‌تواند از عملکرد مؤثر آن‌ها جلوگیری کند. (Housen-Couriel,2017: 13)

اهداف راهبردی اسرائیل را دو سازمان اصلی در ساختار ارتش رژیم عملیاتی می‌کنند: الف) واحد ۸۲۰۰ برای حملات سایبری و ب) اداره خدمات رایانه‌ای، فرماندهی، کنترل، ارتباطات و اطلاعات[5] برای دفاع سایبری. دو اداره مذکور، نهادهای اصلی مسئول در حوزه قلمرو سایبری نظامی هستند و مثالی عینی در اولویت داشتن بخش نظامی در مباحث سایبری اسرائیل به‌حساب می‌آیند. ایده تقویت گسترده‌تر فضای سایبری رژیم در حالت تدافعی یا تهاجمی را نخست‌وزیر نفتالی بنت[6] در اجلاس سایبری ۲۰۲۱ در تل‌آویو ارائه کرد که در آن او هدف ایجاد «یک سپر شبکه جهانی» با سایر کشورها برای همکاری را پیشنهاد کرد که درراستای آن یک نیروی دفاعی برخط[7] و واکنش سریع دربرابر تهدیدات سایبری ایجاد شود که در مرحله اول هشدار دهد سپس بررسی کند و با هم یک نسخه مقابله با آن را به‌صورت واحد ارائه دهند. (Tel Aviv University,2021) ازجمله وظایف اصلی و شناخته‌شده واحد ۸۲۰۰ زیرمجموعه اداره اطلاعات نظامی (امان)[8]، دریافت سیگنال‌های اطلاعاتی، عملیات رمزگشایی و جنگ الکترونیکی است. باتوجه‌به آسیب‌زا بودن حیطه‌های فعالیت آن، یگان تقویت شد و با ۵۰۰۰ سرباز فعال در حال انجام‌وظیفه، تبدیل به یکی از بزرگ‌ترین واحدهای ارتش اسرائیل تبدیل شد. به گفته برخی از پژوهشگران، واحد ۸۲۰۰ ارگانی است که بسیاری از حملات سایبری را راه‌اندازی کرده است و همچنین اعتقاد بر این است که ۸۲۰۰ و آژانس امنیت ملی ایالات‌متحده به‌طورمشترک استاکس‌نت را ساخته‌اند. درنتیجه موضوع مذکور اهمیت حوزه سایبر در فعالیت‌های نظامی در سند راهبرد امنیت رژیم را نشان می‌دهد. (Gori,2022: 13)

5. C4I
6. Naftali Bennett
7. online
8. Aman

واحد ۸۲۰۰ که از بسیاری جهات معادل آژانس امنیت ملی ایالات‌متحده است، در سال ۲۰۰۹ به قابلیت‌های سایبری تهاجمی ارتش اسرائیل افزود و طبق گزارش‌ها، در سال ۲۰۱۱ یک ستاد سایبری ویژه جدید برای توسعه و استقرار سلاح‌های سایبری تهاجمی ایجاد کرد. بودجه و کارکنان برای برنامه‌های سایبری در ارتش نیز افزایش یافته است که ازجمله آن دفتر جدید قابلیت‌ها و عملیات در واحد ۸۲۰۰ را می‌توان نام برد. در ژوئن ۲۰۱۵، ارتش صهیونیستی برنامه‌های خود را برای ایجاد یک فرماندهی سایبری یکپارچه تا سال ۲۰۱۷ اعلام کرد؛ وظایف فرماندهی، کنترل، ارتباطات، کامپیوتر و شاخه اطلاعاتی واحد ۸۲۰۰ و اطلاعات نظامی ادغام شدند و تمامی عملیات تهاجمی و دفاعی ارتش رژیم تحت فرماندهی سایبری واحد ۸۲۰۰ به‌صورت یکپارچه قرار خواهد گرفت. ایجاد فرماندهی سایبری، رژیم را قادر می‌سازد تا اطمینان حاصل کند که قابلیت‌های دفاعی و تهاجمی خود کاملاً یکپارچه شده است و اختلاف در تصمیمات وجود ندارد. در همین راستا، اسرائیل بودجه قابل‌توجهی به یگان ۸۲۰۰ اختصاص می‌دهد که نشان از اهمیت بعد نظامی فضای سایبر برای رژیم دارد. (Cohen,et.al.,2016: 9)

۶. تبیین رویکردهای پدافندی اسرائیل در اسناد راهبردی سایبری

اسرائیل باتوجه‌به انواع تهدیدات امنیتی که با آن‌ها مواجه است، همچنین اهمیت استراتژیک فضای سایبری و درعین‌حال وابستگی زیاد رژیم به حضور و مدیریت این فضا، دو رویکرد کلی را در اسناد امنیت سایبری خود مورد توجه قرار داده است که یکی پدافند و دیگری آفند در فضای سایبری است. در بررسی اسناد راهبردی اسرائیل، فضای سایبری دارای چند مؤلفه متنوع است، شامل محلی برای نفوذ و حمله بیگانه، عاملی برای مدیریت و حکمرانی بهینه، عاملی برای توسعه و رشد اقتصادی، عنصر رفاه‌بخش و ثبات‌ساز امور اجتماعی و ...، اما مهم‌ترین و پررنگ‌ترین مؤلفه در بین مؤلفه‌های متنوع فضای سایبری، توجه ویژه به امور دفاعی و نظامی است. انواع متعددی از نهادهای حکومتی و خصوصی در اسرائیل در حوزه دفاعی در فضای مجازی فعالیت دارند. نهادهای مسئول امنیت سایبری در رژیم، درصدد هستند تا مؤسساتی را نظارت و کنترل کنند که خدمات ضروری در سرزمین‌های اشغالی ارائه می‌کنند و مسئول رویه‌های اداری و زندگی روزمره ساکنین این سرزمین‌ها هستند لذا حمله به این نهادها روحیه و احساس عمومی، نظم، شیوه حکمرانی و مقبولیت رژیم را تحت تأثیر قرار می‌دهد. منابع تهدید سایبری از منظر اسرائیل، که در اسناد راهبردی و بالادستی به‌صورت اجمالی در بخش قبل بررسی شدند، چندگانه تلقی می‌شوند که شامل کشورهای ناهمسو، دولت‌های دشمن، سازمان‌های تروریستی، هکرها و حتی افراد خصوصی می‌شود.

در طراحی استراتژی دفاعی در سند امنیت سایبری رژیم، بین سه نوع حمله و تهدید تمایز وجود دارد: ۱) تهدید پایدار پیشرفته یعنی نفوذ به عمق سیستم کامپیوتری یک سازمان ۲) حمله سریع و سطحی که فوراً نتایج قابل‌تشخیصی دارد و هدف آن تغییر سایت یا جلوگیری از دسترسی به آن و خدماتی است که در فضای سایبری ارائه داده می‌شود و ۳) حمله به زیرساخت‌ها با هدف آسیب رساندن به قطعات سخت‌افزاری. باتوجه‌به سه نوع حمله‌ای که در امنیت سایبری رژیم مطرح‌شده است، با بررسی و واکاوی اسناد امنیت سایبری رژیم می‌توان راهکارها و رویکردهای متنوعی را در حوزه دفاع و پدافند سایبری مورد توجه و تبیین قرار داد که به شرح زیر هستند:

۱- در ساخت دستگاه‌هایی که به اینترنت متصل هستند، عمدتاً از ابزارها و قابلیت‌هایی باید استفاده کرد که نقاط ضعف موجود در سری‌های تولیدی قبلی را رفع کرده‌اند و با داده‌های به‌روز توانسته‌اند توانایی خود را در دفاع برابر حملات پیشرفته سایبری ارتقا دهند. درواقع هدف از این طرح، مقابله حداکثری با روش‌های به‌روز شده است، چون اگر سیستم صرفاً براساس اطلاعات و روش‌های مسبوق طرح‌ریزی شده باشد در مقابله با تهدیدات جدید آسیب‌پذیر خواهد بود. ۲- به‌اشتراک‌گذاری اطلاعات و ارتباطات میان‌سازمانی برای اشراف بر تهدیدات سایبری از اهمیت ویژه‌ای برخوردار است که در صورت اجرا می‌تواند توانایی دفاع سایبری در مواقع حمله را ارتقا بخشد. ۳- تدوین و تهیه گزارش‌ها و ارزیابی‌های مستمر و گسترده در ارتباط با وضعیت سایبری توسط سازمان‌های متولی ۴- ایجاد گروه‌های واکنش سریع سایبری با استفاده از اندیشکده‌هایی که به‌صورت تخصصی در حوزه موضوعی مذکور مطالعه می‌کنند.(Baram,2017: 5) ۵- همکاری با سازمان‌های دفاعی و اطلاعاتی و نیز نهادهای بین‌المللی از اهمیت فزاینده‌ای برخوردار است. ۶- رصد و مراقبت و جمع‌آوری اطلاعات مستمر در مورد دشمنان و مخالفان برای اعلام هشدار ۷- تدوین طرح‌های مستمر برای واکنش سایبری به‌عنوان بخشی از ابزار احتمالی بازدارندگی ۸- توسعه توانایی‌های بازیابی و بازپس‌گیری پس از حمله سایبری با درک اینکه خط دفاع سایبری ممکن است شکسته شود بنابراین سیستم باید برای بازیابی سریع اطلاعات و داده‌ها پس از حملات موفقیت‌آمیز دشمن سازمان‌دهی شود. ۹- ایجاد پل ارتباطی مستمر و همکاری نزدیک با بخش خصوص برای مدیریت بحران پس از حملات سایبری و توانایی بازیابی سریع داده‌ها، افزایش پهنای باند با کمک تأمین‌کنندگان سرور در بخش غیرنظامی که باید از قبل هماهنگی‌ها و آمادگی‌های

لازم انجـام شـود.(Shafqat, Masood,2016: 2-131) ۱۰- افزایـش توانایـی انتقـال سـریع از سـایت‌های مـورد حملـه بـه سـایت‌های موقـت جایگزیـن ۱۱- سـازمان‌های امنیتـی بایـد ملـزم شـوند کـه ابزارهـای دفـاع سـایبری را در برنامه‌هـای عملیاتـی خـود هـم در شـرایط اضطـراری و هـم عـادی ادغـام کننـد. ۱۲- یـک حملـه مؤثـر لزومـاً یـک حملـه غافلگیرانـه پیچیـده نیسـت؛ قـدرت دفاعـی سـایبری بایـد توانایـی مقابلـه بـا یـک حملـه سـایبری مؤثـر بـه یـک هـدف خـاص از طریـق حمـلات سـطحی، سـریع و گسـترده بـه نه‌تنهـا اهـداف حیاتـی (اهـداف نظامـی، زیرسـاخت‌های داخلـی) بلکـه اهـداف سـاده‌تر را نیـز داشـته باشـد. ۱۳- مهاجمـان بایـد در سیسـتمی تحـت عنـوان «سیسـتم ثبـت سـوابق» طراحی‌شـده به‌عنـوان بخشـی از راهبردهـای دفـاع سـایبری ثبـت شـوند؛ بدیـن معنـا کـه بایـد یـک دیتابیـس[9] بـرای نگهـداری از سـوابق مهاجمـان تهیـه شـود. (Zureik,2020: 225)

جدول ۲. رویکرد پدافند سایبری در اسناد بالادستی

انواع تهدید	راه کارها و رویکردهای پدافندی
تهدید پایدار پیشرفته حمله سریع و سطحی حمله به زیرساخت ها	- اشتراک گذاری و تبادل ارتباطات میان دستگاه های نظارتی - تدوین و تهیه گزارشات نو به نو توسط دستگاه های ذیربط - ایجاد گروه های واکنش سریع - همکاری با سازمان های اطلاعات سایبری بین المللی - رصد و پایش سایبری و اطلاعاتی دشمنان - تدوین نقشه ها و طرح های عملیاتی پدافندی مستمر و ملی - توسعه و ارتقا توانایی های بازپس گیری سیستم ها بعد از سقوط - ایجاد پل ارتباطی امن و مستمر با بخش خصوصی سایبری - افزایش چالاکی در انتقال و جایگزین سازی موقت سامانه های مورد حمله - اجرای مانورهای سایبری متناوب توسط دستگاه های ذیربط - پوشش آفندی خط دفاع سایبری توسط سازمان های اطلاعاتی در زمان حمله - شناسایی و ایمن سازی اهداف احتمالی حمله سایبری از اهداف طلایی تا اهداف عادی - ایجاد مرکز داده حملات گذشته و ثبت سوابق - به روز رسانی امنیتی شبکه ها و سامانه ها به صورت مداوم

۷. تبیین رویکردهای آفندی اسرائیل در اسناد راهبردی سایبری

نفـوذ بـه خطـوط دفاعـی سـایبری دشـوار اسـت، درحالی‌کـه موفقیـت در عملیات‌هـای پدافنـدی آسـان‌تر

9. Data base

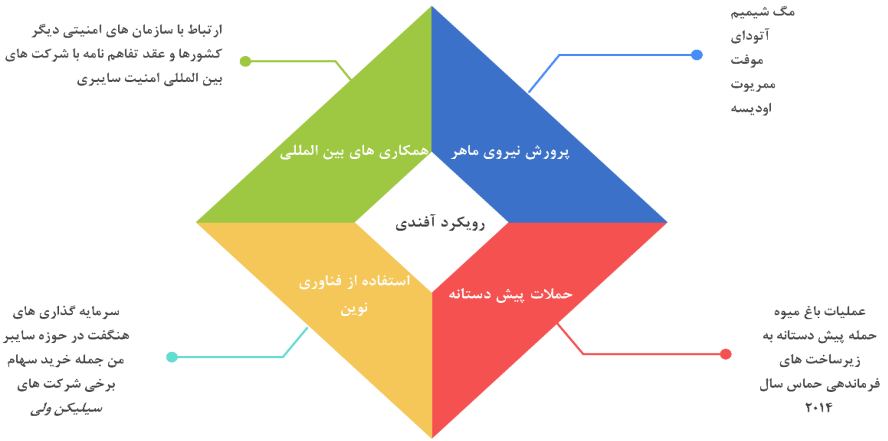
است، اما به‌دلیل ملاحظات محرمانگی کمتر دیده می‌شود. درمقابل، عملیات‌های تهاجمی سایبری موفقیت کمتری دارند، اما روشی کم‌هزینه برای دفاع پیش‌دستانه محسوب می‌شوند. ارتش اسرائیل با اجرای عملیات‌های سایبری تهاجمی دستاوردهای مهمی در این زمینه داشته است. نمونه‌هایی از عملیات‌های سایبری اسرائیل عبارت‌اند از: **عملیات «باغ میوه» (۲۰۰۷):** پیش از حمله به رآکتور اتمی سوریه، ارتش اسرائیل با یک حمله سایبری، سیستم دفاع هوایی سوریه را مختل کرد. (Lawfare Media, 2024) **جنگ ۲۰۱۴ با حماس:** اسرائیل شبکه‌های ارتباطی و فرماندهی حماس را هدف گرفت تا توانایی‌های عملیاتی آن‌ها را کاهش دهد. (Gill, 2023: 4-8) ازجمله عوامل موفقیت اسرائیل در جنگ سایبری را می‌توان توسعه فناوری پیشرفته و همکاری بین ارتش، دانشگاه و صنعت دانست که منجر به تولید راهکارهای امنیت سایبری پیشرفته شده است (Oruj, 2023: 102-105) و همچنین سرمایه‌گذاری در نیروی انسانی متخصص ازجمله پرورش استعدادها در واحد ۸۲۰۰ (Baram, 2017: 7) و رویکرد فعالانه در امنیت سایبری شامل استراتژی‌های تهاجمی، به‌اشتراک‌گذاری اطلاعات و همکاری‌های بین‌المللی که به حفظ برتری اسرائیل کمک کرده است (Gill, 2023: 4-8). اسرائیل با ایجاد زیرساخت‌های سایبری و پرورش نیروی انسانی متخصص، بازدارندگی سایبری را از طریق افزایش شدت و گستردگی حملات سایبری تقویت کرده است. این کشور از طریق واحدهای واکنش سریع و آموزش نیروهای نخبه، استانداردهای تهاجمی خود را ارتقا داده است. مهم‌ترین عملیات‌های تهاجمی سایبری اسرائیل عبارت‌اند از: **ویروس استاکس‌نت (۲۰۱۰):** طراحی‌شده برای مختل کردن سانتریفیوژهای نطنز در ایران (DW, 2019)، **عملیات «افشای کامل» (۲۰۱۴):** متوقف کردن کشتی ایرانی حامل اسلحه برای حماس با کمک ابزارهای سایبری (BBC News, 2014)، **خنثی‌سازی حمله داعش (۲۰۱۸):** اسرائیل با ابزارهای رهگیری سایبری، حمله داعش به یک هواپیمای استرالیایی را کشف و متوقف کرد (IDF, 2018)، **ویروس شعله (Flame):** بدافزاری پیچیده برای جاسوسی در ایران، فلسطین و لبنان (Cordey, 2019: 9)، **ویروس Duqu و Gauss** : بدافزارهای سایبری طراحی‌شده برای نفوذ به سیستم‌های صنعتی، جمع‌آوری اطلاعات بانکی و جاسوسی در منطقه (Bencsith et al., 2015)، **ویروس Duqu 2.0:** برای حملات سایبری پیچیده علیه مذاکرات هسته‌ای ایران و ۵+۱ طراحی شد .(Cordey, 2019: 9) این عملیات‌ها نشان‌دهنده قدرت سایبری اسرائیل و رویکرد تهاجمی آن در جنگ سایبری است که این کشور را به یکی از رهبران جهانی در این حوزه تبدیل کرده است.

۷-۱. پرورش نیروی‌های ماهر در راهبرد آفندی سایبری اسرائیل

اسرائیل به‌دلیل توانایی‌های پیشرفته در جنگ سایبری، خود را به‌عنوان یک قدرت سایبری جهانی معرفی کرده است. بخش مهمی از این موفقیت ناشی از برنامه‌های توسعه استعداد است که با هدف شناسایی، پرورش و آموزش نیروی انسانی متخصص در امنیت سایبری اجرا می‌شوند. برنامه‌های کلیدی توسعه استعداد در امنیت سایبری اسرائیل عبارت‌اند از: **مگ‌شیمیم:** یک برنامه دبیرستانی متمرکز بر آموزش امنیت سایبری که دانش‌آموزان بااستعداد را شناسایی می‌کند و آن‌ها را در زمینه‌های علوم کامپیوتر، رمزنگاری و امنیت شبکه آموزش می‌دهد و فارغ‌التحصیلان آن اغلب به واحدهای سایبری ارتش اسرائیل ملحق می‌شوند. (Jensen, 2018) **آتودای:** یک برنامه بورسیه تحصیلی است که از دانشجویان استثنایی در حوزه امنیت سایبری حمایت مالی می‌کند و به آن‌ها اجازه می‌دهد بدون دغدغه مالی تحصیلات خود را ادامه دهند. (Jerusalem College of Technology) **موفت (دختران سایبری):** یک برنامه ویژه برای زنان که آموزش‌های تخصصی و فرصت‌های شغلی در امنیت سایبری را برای آن‌ها فراهم کرده و مشارکت زنان را در این حوزه افزایش می‌دهد. (Luxner, 2018) **ممریوت:** یک برنامه نظامی برای آموزش متخصصان سایبری درجهت حفاظت از زیرساخت‌های حیاتی ازجمله سیستم‌های صنعتی، درمانی و ارتباطی. این برنامه شرکت‌کنندگان را برای مقابله با تهدیدات سایبری آماده می‌کند. (Siboni & Assaf, 2016: 12-13) **اودیسه:** برنامه‌ای که همکاری بین ارتش اسرائیل و دانشگاه‌ها را در زمینه امنیت سایبری تقویت می‌کند. دانشجویان منتخب در پروژه‌های تحقیقاتی مشارکت و در کنار واحدهای سایبری ارتش کار می‌کنند که به توسعه راه‌حل‌های نوآورانه برای تهدیدات سایبری کمک می‌کند. (Bharti Jain, 2022) این برنامه‌ها نقش کلیدی در تربیت نیروهای متخصص سایبری، افزایش حمایت دولتی از تحقیقات سایبری و تقویت توانمندی‌های سایبری اسرائیل ایفا می‌کنند.

رژیم صهیونیستی همواره اقداماتی دامنه‌دار و پرمعنا را در منطقه دنبال می‌کند و به‌زعم بسیاری، یکی از کشورهای کلیدی در معماری سیاست جهانی محسوب می‌شود. بسیاری از کشورهای منطقه و جهان با بیم زیاد و حفظ ملاحظات ویژه، روابط آشکار و گاه پنهانی با

این رژیم برقرار می‌کنند. با اینکه ردپای این رژیم در بسیاری از تحولات ناخوشایند منطقه دیده می‌شود، صهیونیست‌ها با انکارهای مکرر، جوسازی و سکوت برخوردهای متناقض، چندوجهی و پیچیده‌ای از خود نشان می‌دهند. نقش این رژیم در کنترل و هدایت رسانه‌های بین‌المللی، حمایت‌های مادی و معنوی از اندیشکده‌ها، بنگاه‌ها و خبرگزاری‌های رسانه‌ای همچنین ارتباط با لابی‌های قدرتمند جهانی و منطقه‌ای بر کسی پوشیده نیست. بااین‌حال، رژیم صهیونیستی در انزوای ژئوپلیتیکی شدیدی، حداقل در منطقه، به سر می‌برد و ماهیت تحمیلی و مصنوعی آن در نقشه جغرافیای سیاسی منطقه نتوانسته این رژیم را به جغرافیای فرهنگی تحمیل کند. (Elhami et al., 2024) در چهارچوب مطالعات امنیتی، طرح مسئله ناظر بر شرایط نااطمینانی و بلاتکلیفی به این معناست که حکومت‌ها، تصمیم‌گیران، برنامه‌ریزان نظامی و تحلیلگران سیاست خارجی هرگز نمی‌توانند قطعی از انگیزه‌ها و اهداف کنونی و آینده افرادی که توانایی وارد کردن آسیب نظامی به آن‌ها را دارند، مطمئن باشند. این وضعیت را بلاتکلیفی برطرف‌ناشدنی می‌نامند و آن را هسته اصلی چالش‌هایی می‌دانند که معمای امنیت را شکل می‌دهد. بلاتکلیفی برطرف‌ناشدنی ناشی از عوامل متعددی است، اما می‌توان آن‌ها را به دو دسته پدیده‌های مادی و روان‌شناختی و نمادگرایی ابهام‌آمیز جنگ‌افزارها فروکاست. این همان پویش روان‌شناختی‌ای است که مشکل درک انگیزه‌های دیگران را ایجاد می‌کند و به «خواندن ذهن دیگران» تعبیر می‌شود. درک سیاست‌های امنیتی اسرائیل از نگاه واقع‌گرایی تقریباً به اصلی اساسی تبدیل شده است. به نظر می‌رسد این بازیگر منطقه‌ای تمامی روابط خود را با کشورهای منطقه براساس سیاست حاصل‌جمع جبری صفر تنظیم کرده است. ازاین‌رو، نگرانی‌های امنیتی بر سایر ابعاد سیاست‌گذاری این بازیگر سایه افکنده است. براین‌اساس، سیاست خارجی اسرائیل تقریباً معادل سیاست امنیت ملی این کشور است و بدون درک ماهیت تهدیدها و چالش‌های امنیتی، نمی‌توان فرایند سیاست‌گذاری خارجی آن را تحلیل و ارزیابی کرد. در نگاه کلان و بلندمدت به نظر می‌رسد که چالش‌های امنیتی اسرائیل تغییر چندانی نکرده است و این بازیگر کوچک همچنان با تهدیدهای متعدد در سطح پیرامونی و منطقه‌ای مواجه است. (Borhani & Hosseini, 2021) در شکل زیر رویکرد آفندی اسرائیل نمایش داده شده است.



نمودار ۱. رویکرد آفندی اسرائیل

۸. نتیجه‌گیری

اهمیت فضای سایبری امروزه بر کسی پوشیده نیست و دولت‌ها با کمک آن حکمرانی خود را گسترده‌تر و عمیق‌تر کرده‌اند. اهمیت فضای سایبر چه در بعد نظامی و چه در ابعاد غیرنظامی نیز برای اسرائیل پراهمیت و حیاتی است. این رژیم به علت نداشتن عمق راهبردی و درگیری پیوسته با بازیگران منطقه‌ای، دچار بن‌بست ژئوپلیتیک شده که آن را ملزم به اتخاذ تدابیر متنوع نظامی می‌کند. در این بین، استفاده از قابلیت‌های فضای سایبری برای اسرائیل می‌تواند مانند روزنه‌ای برای تنفس باشد. ازاین‌رو، اسرائیل در دو دهه گذشته تلاش کرده است با کمک تربیت نیرو انسانی کارآمد، قانون‌گذاری و تدوین اسناد بالادستی، ایجاد نهادهای متنوع و ... به تقویت بنیه سایبری خود بپردازد. همچنین نتایج این پژوهش نشان می‌دهد همکاری نزدیک با شرکای غربی همچون ایالات‌متحده، که خود از قدرت سایبری بالایی برخوردار است، توانسته اسرائیل را تبدیل به بازیگر سایبری تأثیرگذار در منطقه کند. درواقع اسرائیل توانسته قدرت سایبری خود را هم در آفند و هم پدافند ارتقا دهد و از فضای سایبر در استراتژی‌های نظامی- اطلاعاتی در درگیری‌های پیرامونی خود استفاده کند. نمونه‌هایی ازجمله عملیات باغ میوه و درگیری با حماس در سال ۲۰۱۴ در این مقاله بررسی شدند. نتایج این پژوهش نشان می‌دهد که اهمیت و جایگاه فضای سایبر در راهبردهای نظامی اسرائیل، در نحوه کارکرد و وجود نهادها و سازمان‌های نظارتی متعدد و مرتبط با حوزه سایبر مشهود بوده که جدیدترین آن‌ها ستاد سایبری است. در

یک نگاه جامع به نهادها و ساختار تصمیم‌گیری اسرائیل ذکر این نکته حائز اهمیت است که یک تقسیم مسئولیت بین قوا برای دفاع سایبری وجود دارد.

نتایج این پژوهش نشان می‌دهد که اسرائیل با کمک قابلیت‌های فضای سایبری، همچنین توانایی‌های تکنولوژیکی سایبری خود به دنبال ایجاد بازدارندگی سایبری دربرابر تهدیدات پیرامونی خود است. حملات سایبری متعدد، همچنین فعالیت‌های موفق جاسوسی از کشورهای منطقه، به خلق فضای بازدارنده سایبری اسرائیل کمک کرده‌اند. متنوع شدن تهدیدات در عصر حاضر و روی کار آمدن مفهوم امنیت موسع باعث شده اسرائیل فعالیت‌های امنیتی خود را در آفند و پدافند نظامی گسترده‌تر و جبهه‌های جدیدی با رقبای خود باز کند.

شیوه قانون‌گذاری و تدوین اسناد بالادستی سایبری در اسرائیل، در نوع خود حائز اهمیت است و مراحل و پیچیدگی‌های مخصوص به خود را دارد که به این شرح زیر است: اولین اقدام در حوزه فضای مجازی در سرزمین‌های اشغالی مربوط به «قانون و مقررات امنیت در مؤسسات حکومتی» مصوب ۱۹۹۸ است که اختیارات و مسئولیت‌های مربوط به امنیت اطلاعات و امنیت سیستم‌های کامپیوتری واحدهای عمومی را تعیین می‌کند و مسئول امنیت اطلاعات دفتر نخست‌وزیری، وزارت دفاع، کارخانه‌های سیستم‌های دفاعی، دفتر رئیس‌جمهور و وزارت خارجه است. همچنین آخرین اقدام مربوط به سال ۲۰۱۵ است که رژیم تصمیم به ایجاد یک دفتر «ملی سایبری»[10] ذیل دفتر نخست‌وزیر، دولت و کمیته‌های آن گرفت که سیاست‌های کلان این حوزه را تعیین و توصیه‌هایی ارائه کند و اجرای آن را در حوزه فضای سایبری با رعایت کلیه قوانین و تصمیمات دولت بر عهده بگیرد. علاوه‌بر وظایف مذکور، دفتر سایبری وظیفه اجرای توصیه‌های رئیس شورای تحقیق و توسعه یعنی پیشرفت و توسعه زیرساخت‌های دانش سایبری را بر عهده دارد. مشارکت در تحقیق و توسعه مرتبط با فناوری سایبری، توسعه ابزارهایی برای شرایط اضطراری در زمینه سایبری، ایجاد چهارچوب امنیت سایبری و راه‌حل‌هایی برای دفاع محلی از دیگر وظایف دفتر سایبری است. دفتر مذکور باید بدون دخالت در نهاد دیگری مسئولیت خود را اجرا کند.

در سال ۲۰۱۵، رئیس ستاد کل ارتش اسرائیل مسئولیت عملیات فضای سایبری را به دو نهاد اعطا کرد: واحد ۸۲۰۰ اطلاعات نظامی در زمینه آفند و «یگان تله پردازش»[11] که یگان دفاعی

10. national cyber bureau
11. Teleprocessing Corps

بخش کامپیوتری ارتش برای حوزه دفاعی است. سایر نهادها در اسرائیل مسئولیت خاصی برای دفاع دربرابر حملات سایبری ندارند، اما فعالیت آن‌ها در برخی زمینه‌ها تأثیرگذارد که تعدادی از آن‌ها بدین‌صورت هستند: بخش رایانه وزارت دارایی که مسئول ارائه خدمات اینترنتی امن به اداره‌ها و دفاع از شبکه‌های دولتی در اتصال به اینترنت در آن‌هاست. واحد پلیس رژیم برای پیشگیری از جرائم سایبری که به‌عنوان بخشی از واحد لاهاو[12] ۴۳۳ عمل می‌کند و جرائم سایبری و تهدیدات رخ‌داده را بررسی می‌کند و نهایتاً مرجع قانون در حوزه فناوری و اطلاعات، وزارت دادگستری است که نقش آن افزایش آگاهی افراد از مسائل حریم خصوصی و حفاظت از اطلاعات شخصی در اینترنت است.

اسرائیل با افزایش توانایی خود در حوزه سایبری و داشتن برنامه‌های راهبردی منظم در بخش مذکور توانسته خود را به‌عنوان یک قطب سایبری در جهان معرفی کند که علاوه‌بر توان صادراتی بالا به کشورهای جهان و کسب عایدی اقتصادی قابل‌توجه برای شرکت‌های خصوصی صهیونیستی، با فروش نرم‌افزار و سخت‌افزارهای مربوطه توان جاسوسی سایبری و قدرت خرابکاری خود را بهبود بخشیده است. در بخش نظامی- اطلاعاتی با تأسیس یگان ۸۲۰۰ و استخدام نخبگان و خبرگان جوان دانشگاهی در واحد مذکور، عملیات‌های سایبری زیادی را علیه کشورهای مختلف ازجمله ج.ا.ا. سازمان‌دهی کرده است. هرچند طی سالیان گذشته حزب‌الله لبنان و سایر گروه‌های مقاومت با افزایش توان سایبری خود توانسته‌اند بازدارندگی رژیم را از بین ببرند و آنان را در مقابل تهدیدات سایبری آسیب‌پذیر کنند. رژیم با متوسل شدن به خرابکاری‌های سایبری و به‌صورت کلی افزایش توان خود در حوزه مذکور، قصد دارد ضعف‌های وجودی خود مانند نداشتن مشروعیت سیاسی و عمق استراتژیک را پوشش دهد. همچنین اقتصاد رژیم وابستگی زیادی به فضای سایبر دارد. در همین راستا، رژیم با رویکردی تهاجمی در ابعاد مختلف، سعی در ضربه زدن به کشورهای مختلف با اهداف گوناگون دارد. باتوجه‌به آنچه در تاریخچه شکل‌گیری و حوزه اختیارات برخی از اصلی‌ترین نهادهای نظارتی در حوزه سایبر در اسرائیل بیان شد، پنج گروه اصلی هستند که سازمان‌ها و نهادهای حوزه مذکور ذیل آن‌ها تعریف می‌شوند:

۱. سازمان‌های دفاعی- ارتش اسرائیل، سازمان‌های جامعه اطلاعاتی، پلیس و نهادهای مشابه: این سازمان‌ها در مورد مفهوم دفاعی خود تصمیم می‌گیرند و آن را مطابق با نیازها و اختیارات عملیاتی خود اجرا می‌کنند.

12. Lahav

۲. صنایع دفاعی- شرکت‌ها و سازمان‌ها با ماهیت دفاعی: مدیر امنیت تشکیلات دفاعی، الزامات حوزه دفاع سایبری را تعیین و تأیید می‌کند.

۳. زیرساخت‌های حیاتی- بخش‌هایی که فعالیت آن‌ها برای عملکرد رژیم ضروری است، برای مثال تأمین برق، آب و غیره. این‌ها تحت هدایت و کنترل آژانس امنیت رژیم عمل می‌کنند.

۴. دفاتر دولتی- دفاع از اکثر اداره‌های دولتی و مقامات رژیم زیر نظر بخش رایانه انجام می‌شود که دارای واحدی است که در زمینه امنیت سایبری فعالیت می‌کند. رئیس امنیت تشکیلات دفاعی، وزارت دفاع را هدایت می‌کند.

۵. بخش مدنی- کلیه کاربران غیرنظامی اینترنت ازجمله سازمان‌ها، مشاغل و افراد خصوصی: این قشر آسیب‌پذیرترین گروه است، درنتیجه مهاجمان ممکن است ترجیح دهند علیه این بخش که دفاع در آن ناقص صورت می‌گیرد، اقدام کنند. این گروه تحت مقرراتی که «دفتر دفاع سایبری» اخیراً تأسیس کرده است، تعریف می‌شوند. باتوجه‌به آنچه در پژوهش حاضر بیان شد، مهم‌ترین قوانین، اسناد و ارگان‌های متولی در حوزه سایبری اسرائیل در جدول زیر خلاصه شده است.

جدول ۳. مهم‌ترین قوانین، اسناد و ارگان‌های متولی در حوزه سایبری اسرائیل

ارگان‌های متولی	قوانین و اسناد بالادستی
سازمان امنیت سایبری اسرائیل[۱۳]	ذیل قانون ۲۴۴۴: استراتژی امنیت سایبری اسرائیل در درجه اول، ابزاری برای تحقق چشم‌انداز سایبری این رژیم از طریق ایمن نگه داشتن فضای سایبری و مقابله با تهدیدات سایبری مختلف مطابق با «منافع ملی» این رژیم است.
سازمان امنیت ملی اطلاعات[۱۴]	مصوبه۸۴/B کمیته وزیران در مورد «مسئولیت حفاظت از سیستم‌های رایانه‌ای در اسرائیل- ۲۰۰۲» بیان می‌کند که سازمان امنیت اطلاعات ملی که در داخل سرویس امنیت عمومی فعالیت می‌کند، برای آموزش و حفاظت از سیستم‌های رایانه‌ای حیاتی تشکیل می‌شود و توسعه می‌یابد. مخاطب این نهاد، سازمان‌های مدنی دولتی و خصوصی با اولویت زیرساخت‌های حیاتی رژیم است.

13. Israel National Cyber Security Authority
14. National Information Security Authority

ارگان‌های متولی	قوانین و اسناد بالادستی
دفتر ملی سایبری اسرائیل[15]	مصوبه ۳۶۱۱ هیئت‌وزیران اسرائیل در ۲۷ اوت ۲۰۱۱، دفتر «ملی» سایبری زیر نظر دفتر نخست‌وزیر به‌عنوان اولین نهاد مشاور و تثبیت امنیت سایبری تأسیس شد. این قطعنامه به سیاست‌گذاری کلی در حوزه سایبر انسجام داد و ذیل یک دفتر تعریف کرد.
اداره ملی سایبری اسرائیل[16]	ذیل دفتر نخست‌وزیر تعریف می‌شود و مسئول حفاظت از فضای سایبری غیرنظامی است.
کمیسیون سایبری کنست[17]	بررسی لوایح و الزامات متناسب با دنیای کنونی در مجلس اسرائیل
اداره امنیت اطلاعات و سایبری، دفتر دادستانی اسرائیل[18]	دفتر حوزه جرائم سایبری ذیل وزارت دادگستری مسئول کیفرخواست و تعقیب مجرمانی است که مرتکب جرائم سایبری شده‌اند.
گروه آمادگی رویدادهای سایبری اسرائیل[19]	نظارت بر تمام سرزمین‌های اشغالی به غیر از زیرساخت‌های نظامی و حیاتی رژیم را برعهده دارد.

15. Israel National Cyber Bureau
16. Israel National Cyber Directorate
17. Knesset Subcommittee for Cyber Defense
18. Department of Emergency, Information Security and Cyber, State Attorney's Office
19. Israel National Cyber Event Readiness Team

References

Adamsky, D. (2017). The israeli odyssey toward its national cyber security strategy. The Washington Quarterly, 40(2), PP. 113-127.

Army, U. S. (2010). Cyberspace operations concept capability plan 2016-2028. US Army Capabilities Integration Center, 22.

Baezner, M.; Cordey, S. (2019). National Cybersecurity Strategies in Comparison–Challenges for Switzerland. ETH Zurich.

Baram, G. (2017). Israeli defense in the age of cyber war. Middle East Quarterly.

Behrami, Zahra; Araghchi, Seyyed Abbas (2017). New Security Threats of Israel. Defensive Policy Journal, 25(98), PP. 127-162. **[In persian]**

Bencsith, B.; Kurucz, G.; Molnar, G. (2015). Duqu, a comparisent to Duqu. Budapest university.

Bendiek, A.; Metzger, T. (2015). Deterrence theory in the cyber-century Researcher.Lecture Notes in Informatics (LNI). Bonn: Gesellschaft für Informatik.

Borhani, S. H.; Hosseini, S. H. (2021). Israel's National Security Strategy in Facing Regional Environmental Threats. Fundamental and Applied Studies of the Islamic World, 3(7), PP. 40-64. **[In persian]**

Burak Tolga, I. (2018). Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture. Estonia, Tallinn: CCDCOE.

Cordey, Smith (2019). The Israel unit 8200 – OSINT / based study. Trend analysis. Centre for security studies.

Cohen, M. S.; Freilich, C. D.; Siboni, G. (2016). Israel and cyberspace: Unique threat and response. International Studies Perspectives, 17(3), PP. 307-321.

Dehghani, Ali Asghar (2018). Cyber Deterrence in Modern Global Security. International Political Approaches, 8(50), PP. 121-147. **[In persian]**

Elhami, A.; Kavandi Kateb, A.; Jalali Rad, M. S. (2024). Examining the Cultural and Social Components of the Zionist Regime for Influence in the Region. Fundamental and Applied Studies of the Islamic World, 6(3), PP. 25-60. **[In persian]** https://doi.org/10.22034/fasiw.2024.420586.1290.

Eizenkot, G. (2016). Deterring Terror: How Israel Confronts the Next Generation of Threats. translated by Susan Rosenberg, Belfer Center for Science and International Affairs, Harvard Kennedy School.

Eisenstadt, M. I. C. H. A. E. L.; Pollock, D. A. V. I. D. (2021). Asset Test 2021: How the US Can Keep Benefiting from Its Alliance with Israel. The Washington Institute for Near East Policy, 2021-02.

Elran, M. (2015). Establishing an IDF Cyber Command.

Even, S.; Ṭov, D. S. (2012). Cyber Warfare: Concepts and Strategic Trends. Institute for National Security Studies.

Finkel, M. (2020). IDF strategy documents, 2002-2018: On processes, chiefs of staff, and the IDF. A Multidisciplinary Journal on National Security, 23(4), PP. 4-17.

Foulan, Michiel (2024). How Cyber Space Affects International Relation, Contemporary Security Policy, NO.45, Issue 3

Gill, G. S. (2023). Israel's Approach to Building Cyber Capabilities: Lessons for the Indian Armed Forces.

Habibi, Seyyed Amin; Ghorbani, Zahra (2017). Islamic Radicalism Movements in Baluchistan and Their Security Threats to the Islamic Republic of Iran. Nations Research Journal, 22(2), PP 69-87. **[In persian]**

Habibi, Seyed Amin; Sadeghi Haghighi, Didokht; Barzegar, Keyhan. (2023). The Position of the Concept of Environmental Security in International and Global Security. Quarterly Journal of International Relations Studies, 16(2), PP. 57-85. **[In persian]**

Housen-Couriel, D. (2017). National Cyber Security Organisation, Israel. Washington, DC: NATO Cooperative Cyber Defence Centre of Excellence.

Jensen, B. (2018). A Minnow Among Sharks: Cyber Conflict and the Implications for Singapore N/A.

Kello, Lucas. (2013). The Meaning of theCyber Revolution: perils to theory and statecraft, International Security, vol. 38.

Lemieux, F. (Ed.). (2015). Current and emerging trends in cyber operations: Policy, strategy and practice.

Mielko, T. (2023). Could Pegasus Gate have been prevented? The evolution of the export control regime for cyber-surveillance tools in Israel. Cybersecurity and Law, 9(1), PP. 155-166.

Oruj, Z. (2023). Cyber Security: contemporary cyber threats and National Strategies. Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspects, (2), PP. 100-116.

Reed, J. (2015). Unit 8200: Israel's cyber spy agency. The Financial Times, 16-16.

Seyyad, Mohammad Kazem; Amini, Armin; Taheri, Abolghasem (2020). Cyber Threats and Security Measures in Cyberspace: A Comparative Study of the Approaches of the United States and the Islamic Republic of Iran. National Security Quarterly, 10(38), PP. 293-330 **[In persian]**.

Shafqat, N.; Masood, A. (2016). Comparative analysis of various national cyber security strategies. International Journal of Computer Science and Information Security, 14(1), PP. 129-136. **[In persian]**

Siboni, G.; Assaf, O. (2016). Guidelines for a national cyber strategy. Tel Aviv: Institute for National Security Studies.

Stancu, A. I.; Pavel, T. (2023). Unveiling Israel's Cyber Legal Landscape: A Comprehensive Analysis of Cybersecurity Regulations and Policies. Perspectives of Law and Public Administration, 12(4), PP. 643-650.

Tabansky, L. (2020). Israel defense forces and national cyber defense. Connections, 19(1), PP. 45-62

Zureik, E. (2020). Settler colonialism, neoliberalism and cyber surveillance: the case of Israel. Middle East Critique, 29(2), 219-235.

https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/how-israel-became-top-cyber-power

https://www.ITU.org/ Cyber Space (2018), last visited 2024.

https://timesofindia.indiatimes.com/world/middle-east/israel-focuses-on-training-next-gen-to-drive-its-cyber-systems/articleshow/92610619.cms

https://www.cssii.unifi.it/ls-6-cyber-security.html

https://www.lawfaremedia.org/article/lessons-from-israel-s-rise-as-a-cyber-power

https://www.DW.com/how did stuxnet virus enter the Natanz nuclear facility?

https://www.BBC.com/Israel halts weapons shipment from iran 2014

https://www.IDF.il/en/articles/terror/8200unit thwarts an ISIS attack

https://english.tau.ac.il/news/cyber-week-21

https://www.jct.ac.il/en/special-programs/atudai-program/