




Creative Commons Attribution 4.0 International License (CC BY 4.0)

 <http://dx.doi.org/10.22067/PG.2022.71588.1068>

مقاله پژوهشی

بازدارندگی سایبری و تحول در دکترین امنیتی-دفاعی اسرائیل

ولی گل محمدی (عضو هیأت علمی گروه روابط بین‌الملل دانشگاه تربیت مدرس، تهران، ایران، نویسنده مسئول)

vali.golmohammadi@modares.ac.ir

تاهره جمشیدی (کارشناسی ارشد روابط بین‌الملل دانشگاه تربیت مدرس، تهران، ایران)

tahereh.jamshidi@modares.ac.ir

صص ۲۳-۱

چکیده

محدودیت‌های ناظر بر موقعیت جغرافیایی در محیط آشوبناک خاورمیانه، فقدان عمق استراتژیک، و آسیب‌پذیری‌های ناشی از عدم تقارن عناصر قدرت ملی در مقابل دشمنان و همسایگان، دکترین دفاعی نوین اسرائیل را به سمت پرهیز از جنگ‌های کلاسیک و بهره‌برداری از ابزارهای نامتعارف بازدارندگی سوق داده است. این مقاله با مطالعه تحولات دکترین امنیتی-دفاعی اسرائیل به دنبال فهم چارچوب‌مند ظرفیت‌های سایبری در شکل‌دهی به راهبرد بازدارندگی نوین آن در مقابله با تهدیدات داخلی و خارجی است. در چارچوب مفروضه‌های بازدارندگی سایبری، مقاله‌این ایده اصلی را مطرح می‌کند که؛ اسرائیل با بازتعریف ابزارهای بازدارندگی امنیتی-دفاعی خود، سرمایه‌گذاری هدفمندی در توسعه توانمندی‌های بازدارندگی سایبری انجام داده است. راهبرد بازدارندگی سایبری قلمرو مقابله با تهدیدات امنیت ملی اسرائیل را به خارج از مرزها گسترش داده و آسیب‌پذیری محیطی تهدیدات داخلی را به‌طور قابل توجهی کاهش داده است. براین اساس، گذار از ابزارهای متعارف نظامی به ابزارهای غیرمتعارف، اسرائیل را به تنظیم راهبردهای امنیتی ملی با محوریت توانمندی سایبری در مقابله با کانون‌های جدید تهدید ترغیب می‌کند. آسیب‌پذیری نظامی در مقابل گروه‌های مقاومت فلسطینی در جنگ اخیر نشان داد که در برخورد با چالش جدی‌تر مثل ایران، جنگ نظامی گزینه‌ای مطلوب برای اسرائیل نیست و پیش‌بینی می‌شود که در آینده بازدارندگی سایبری جایگاه ویژه‌ای در دکترین امنیتی-دفاعی اسرائیل داشته باشد.

واژگان کلیدی: بازدارندگی سایبری، دکترین امنیتی-دفاعی، جنگ نامتعارف، اسرائیل

مقدمه

تحولات نوظهور در محیط جهانی و منطقه‌ای و همچنین تغییر در محیط راهبردی خاورمیانه منجر به تحول در دکترین امنیتی- دفاعی اسرائیل و ارائه راهبرد جدید در حوزه نظامی شده است. با توجه به کم‌رنگ شدن نقش ارتش نسبت به تحولات ویژه محیط استراتژیک در تأمین منافع ملی و انتقال از رویکرد کنش به واکنش، اسرائیل وادار به تغییر راهبرد خود و تبدیل آن به ماهیت دفاعی شده که در چنین شرایطی دستاوردهای اسرائیل در زمینه جنگ‌های غیرنظامی ابزاری مطلوب در مقابل کانون‌های جدید تهدید این کشور به حساب می‌آید. بر طبق سند راهبرد نظامی اسرائیل، تهدیدهای پیش روی دولت اسرائیل در محیط راهبردی جدید به شرح زیر است: کشورهای دور (ایران) و مجاور (لبنان)، دولت‌های ورشکسته و کشورهایی که در روند تجزیه (سوریه) هستند. بازیگران غیردولتی (حزب الله، حماس)؛ سازمان‌های تروریستی مستقل از دولت یا جامعه خاص (جهاد اسلامی، جهاد اسلامی فلسطین، داعش و سایرین). علاوه بر این کنشگران، کانون تهدیدات دیگری از قبیل: احتمال گسترش تسلیحات کشتار جمعی و تسلیحات آفندی راهبردی مثل موشک‌های بالستیک و تهدیدات سایبری رو به افزایش، قابل توجه است (Eizenkot, 2016:4).

در این راستا، در فصل پنجم سند راهبرد نظامی اسرائیل،^۱ با تأکید بر ایجاد نیروی نظامی کارآمد، افزایش قابلیت فضای سایبری به عنوان یک ابزار کارآمد در حوزه دکترین دفاعی- امنیتی این کشور در نظر گرفته شده است. در واقع، فضای سایبری یکی از مناطق نبرد نوین در نظر گرفته شده که فعالیت‌های دفاعی، اطلاعاتی و تهاجمی در این فضا انجام خواهد شد. مقامات اسرائیل خود را یکی از اصلی‌ترین قربانیان تهدیدات نرم و جنگ سایبری معرفی می‌کنند. به همین دلیل اسرائیل با سرمایه‌گذاری هدفمند در توسعه توانمندی‌های سایبری خود به دنبال تبدیل نمودن این رژیم به «ابرقدرت سایبری جهان» است. هدف مقامات اسرائیلی در این زمینه ایجاد یک اسرائیل امن سایبری است. ضمن اینکه اسرائیل در صدد است که به قابلیت‌هایی دست یابد که دیگران را در سطح عالی رصد کرده و در صورت لزوم با تهدیدات جدی سایبری مواجه سازد (Torabi, 2016:41-42).

بدین ترتیب، یکی از بخش‌هایی که علم و فناوری در آن نمود بیشتری یافته، صنایع نظامی اسرائیل است؛ صنایع نظامی اسرائیل دارای بیشترین پیشرفت در بین کشورهای صنعتی بوده است. امروزه می‌توان ادعا کرد که پیشرفت قابل توجه در حوزه «امنیت سایبری»^۲ مهم‌ترین دستاورد این صنعت در سال‌های اخیر است. در واقع بر اساس اصل ضرورت نوآوری، تغییر و سازگاری و به دلیل محیط آشوبناک همسایگی، اسرائیل یک اکوسیستم ایجاد کرده است که ایده‌های جدید و راه‌حل‌های ابتکاری را پرورش داده و پشتیبانی می‌کند. عامل اصلی موفقیت اسرائیل به عنوان یک کشور نوآور را می‌توان این‌گونه برشمرد: تمرکز استراتژیک بر اتکا به خود، زیرا از زمان تأسیس تاکنون اسرائیل با محیطی خصمانه و آناشیک روبرو بوده و این بدان معنی است که این رژیم از ابتدا می‌بایست بسیار خلاقانه عمل کند. رژیم صهیونیستی به عنوان یک

1. Israel Defense Forces Strategy

2. Cybersecurity

موجودیت نوپا، دارای سابقه مهاجرت گسترده است و استعدادهای مختلفی را از سراسر جهان به این کشور وارد می‌کند. عامل دیگر نقش و تأثیر شدید ارتش این کشور است. نیروی دفاعی اسرائیل^۱ (IDF) مهارت بالایی در حوزه‌های نوین نظامی و دفاعی دارد. از آنجاکه بیشتر شهروندان اسرائیلی مجبور به خدمت در ارتش هستند، ارتش به‌عنوان حلقه اتصال زنجیره نوآوری، به‌ویژه در حوزه امنیت سایبری عمل می‌کند. برخی از واحدهای ویژه دفاع ملی، مانند برنامه‌های تالیپوت^۲ و یگان ۳۸۲۰۰ در اینجا نقش اصلی را دارند. هم دولت و هم ارتش در ساخت و تقویت قدرت ابتکاری و فناوریانه کشور نقش اساسی داشته‌اند (Hols, 2020:30).

در مجموع، ارتش این رژیم در زمینه دفاع سایبری در شرایطی که بسیاری از قدرت‌های بزرگ جهانی هنوز اقدامات مهمی در تأمین امنیت شبکه‌های ملی خود انجام نداده بودند، مهارت و پاسخگویی منحصر به فردی را ایجاد کرده‌اند. عملیات سایبری ارتش اسرائیل - چه دفاعی و چه تهاجمی - در حقیقت به دلیل پیچیدگی و نوآوری در سطح بین‌المللی شناخته شده است. از یک طرف، این سطح از مهارت نظامی را می‌توان به‌عنوان یک نتیجه طبیعی مناقشات سیاسی، نگرانی‌های امنیتی و نیازهای دفاعی دانست. از سوی دیگر، با نگاهی به توسعه آن به مرور زمان، این تخصص بیشتر نتیجه یک استراتژی متمرکز حاکمیت سایبری است که با ترکیب کارآمد رویکردهای نظامی و غیرنظامی، مزایای راهبردی در زمینه امنیت سایبری ایجاد می‌کند (Cristiano, 2020:1-6).

مقاله حاضر با نگاهی به سیر تحول دکترین امنیتی - دفاعی اسرائیل، به دنبال فهم چارچوب‌مند جایگاه و کارکرد بازدارندگی سایبری اسرائیل در مقابله با تهدیدات نوظهور داخلی و محیطی است. در راهبرد جدید اسرائیل، توجه به گسترش بی‌سابقه عملکرد این کشور در عرصه‌های جنگ‌های غیرنظامی است. راهبرد جدید ارتش اسرائیل بر اهمیت آگاهی این کشور به قابلیت‌های کنونی در عرصه سایبری و فضای مجازی تأکید می‌کند. این موضوع را می‌توان اولین نشانه‌ی در دستور کار قرار دادن عرصه‌های دیگر تقابل، غیر از موازنه‌های نظامی در راهبرد نظامی اسرائیل دانست. عرصه‌هایی که از اهمیت استراتژیک برخوردار بوده و این بدان معنی است که تحول بی‌سابقه و قابل توجهی از سوی دشمنان اسرائیل در بخش‌های مختلف جنگ روانی و جنگ نرم و جنگ هوشمند به وجود خواهد آمد. در پاسخ به سؤال اصلی پژوهش؛ چگونگی جایگاه و کارکرد توانمندی‌های سایبری در تحول دکترین امنیتی - دفاعی اسرائیل؟ مقاله تلاش می‌کند تا سازوکار و کارکرد ظرفیت‌های نوظهور سایبری اسرائیل را در چارچوب بازدارندگی غیرمتعارف تبیین کند. برای پاسخگویی به این پرسش؛ روش گردآوری داده‌ها کتابخانه‌ای و اینترنتی است. داده‌های کتابخانه‌ای از طریق کتاب، نشریه، مقاله گردآوری شده است. از نظر هدف این پژوهش کاربردی بوده و از نظر نوع داده‌ها و تحلیل و بررسی آن‌ها از تحقیقات کیفی بوده و ماهیت فرضی - استنتاجی دارد و سطح و رویکرد تحقیق توصیفی - تحلیلی است

-
1. Israeli Defense Forces
 2. Talpiot
 3. Unit 8200

بازدارندگی سایبری

رویکرد «بازدارندگی»^۱ یکی از نظریه‌های امنیت سستی محسوب می‌شود که از قابلیت کاربرد در عرصه سایبری نیز برخوردار است. در طول جنگ سرد، نظریه بازدارندگی چارچوب محوری تجزیه و تحلیل سیاست دفاعی دولت‌ها بوده که در تبیین تأثیر سلاح‌های غیرمتعارف چنین استدلالی پیشروی ما می‌گذاشت که قدرت‌های هسته‌ای از ترس عواقب مخرب استفاده از سلاح‌های هسته‌ای وارد جنگ با یکدیگر نمی‌شوند. برخی پژوهشگران با بهره‌گیری از مفروضه‌های بازدارندگی چارچوب «بازدارندگی سایبری»^۲ در فضای مجازی را مطرح کرده‌اند (Bendiek & Metzger, 2015: 554). بازدارندگی سایبری به لحاظ ماهیت بازیگران و کارکرد ابزارها، متفاوت از بازدارندگی هسته‌ای کلاسیک و بازدارندگی متعارف است. بازدارندگی سایبری در هسته اصلی خود نتیجه‌ی تمایل دولت‌ها برای مقابله با تهاجمات در فضای مجازی یا از طریق آن است (Burak Tolga, 2018: 7). براساس چارچوب بازدارندگی سایبری، دو روش اصلی در اعمال بازدارندگی سایبری وجود دارد؛ بازدارندگی از طریق انکار^۳ و بازدارندگی از طریق مجازات^۴. در مطالعاتی دیگر، جوزف نای دو روش دیگر برای بازدارندگی مطرح می‌کند که شامل گرفتارسازی^۵ و تابوهای هنجاری^۶ است (Nye, 2017 as cited in Bendiek & Metzger, 2015: 554).

بازدارندگی از طریق مجازات به‌عنوان یک روش بازدارندگی سایبری است که این وضعیت را به خود می‌گیرد: اگر شما اقدام X را بر علیه من انجام دهید، سپس من اقدام Y را در پاسخ انجام می‌دهم. نکته این است که مقیاس مجازات Y بزرگ‌تر از مقدار درک شده X است. بنابراین باعث می‌شود که دشمن در مرحله اول از انجام X جلوگیری کند. اگر تهدید به تلافی در ذهن دشمن امری جدی تلقی شود، به گونه‌ای که منجر به اصلاح رفتار آن‌ها شود، گفته می‌شود بازدارندگی مؤثر است (Ryan, 2017: 323). بازدارندگی از طریق مجازات در فضای سایبری می‌تواند مؤثر باشد، به‌ویژه اگر بین نهادهای مجری کشورها همکاری و انسجام وجود داشته باشد. وقتی یک توافق‌نامه همکاری قوی بین نهادهای اجرای قانون فضای مجازی و سایبری وجود داشته باشد، درک اینکه چرا تهدید به مجازات بازدارنده مؤثر هستند، راحت‌تر است. زیرا قربانی اگر مهارت کافی نداشته باشد و از قابلیت فنی بالایی برخوردار نباشد، احتمالاً گرفتار می‌شود (Ryan, 2017: 333).

-
1. Deterrence
 2. Cyber Deterrence
 3. Deterrence by Denial
 4. Deterrent by Punishment
 5. Entanglement
 6. Normative taboo

روش انکار^۱ از مدت‌ها پیش یک استراتژی مطلوب در بازدارندگی سایبری بوده است به‌ویژه با توجه به این تصور که تلافی^۲ و انتساب^۳ در سطح فنی و بالاتر در سطح استراتژیک بسیار چالش‌برانگیز است. بازدارندگی از طریق انکار بر این اصل متکی است که: اگر حملات سایبری با معافیت از مجازات انجام شود، مهاجم دلیل کمی برای متوقف کردن دارد (Libicki, 2009 as cited Bendiek & Metzger, 2015:554). در این موارد جدا از ظرفیت تهاجمی یک کشور، مهاجم از حمله باز نمی‌ایستد. برای اینکه روش بازدارندگی از طریق مجازات موفق عمل کند باید شدت هزینه را نسبت به سود برای مهاجم بالا برد. در واقع متقاعد کردن فرد مهاجم به اینکه حمله هیچ‌گونه دستاوردی متناسب با هزینه آن نخواهد داشت، به‌عنوان یک ابزار قدرتمند دفاعی مانع حمله می‌شود (Philbin, 2013:15).

این ایده که هنجارها و تابوها در فضای مجازی می‌توانند به‌عنوان یک عامل بازدارنده عمل کنند، صریحاً توسط جوزف نای مطرح شده است. هنجارها به‌عنوان قراردادهای غیر الزام‌آور یا استانداردی از رفتار منطقی در مورد چگونگی عملکرد یک گروه از بازیگران در نظر گرفته می‌شود. از طرف دیگر، تابوها به شیوه‌های نامناسب عملکرد یا اخلاق فرهنگی ممنوعه اشاره دارند و با وجود بار معنایی معکوس و منفی، شبیه به هنجارها هستند. هنجارها باگذشت زمان پدیدار می‌شوند و هنگامی که نظم، ثبات و امنیت را فراهم می‌کنند، اغلب به صورت قانون تدوین می‌شوند (Ryan, 2017:335). در صورتی که بتوان با تصویب قوانین بین‌المللی، عملیات سایبری را به صورت تابو درآورد، آنگاه شکستن تابو برای کشورها هزینه خواهد داشت. بازدارندگی از این طریق، قدرت نرم کشورها را هدف قرار می‌دهد. هنجارهای سایبری باگذشت زمان شکل می‌گیرند. البته هنجارسازی مراحل پیچیده‌ای دارد که در زمینه سایبر، در مراحل اولیه آن قرار داریم.

بهره‌گیری از سازوکار بازدارندگی، فهم مشترکی مبنی بر سودمندی استفاده از اینترنت و فضای مجازی می‌طلبد. در صورت رسیدن به چنین فهمی، مطمئناً دولت‌ها در پی استفاده غیر صلح‌آمیز از این بستر نخواهند بود. آشکارترین نمونه استفاده از این سازوکار در بازدارندگی، موضوع اختلافات سایبری آمریکا و چین است. می‌دانیم که ادامه قدرت چین به طور مطلق وابسته به اینترنت است (Nye, 2017:60-61). در واقع این سازوکار بر اساس وابستگی متقابل عمل می‌کند. برخی از وابستگی‌ها دو یا چند طرفه هستند، ولی برخی دیگر سیستمی بوده و در اثر اختلال در سیستم، منافع حیاتی مورد هدف قرار خواهند گرفت. در این حالت کشورها به دنبال ثبات سیستمی خواهند رفت (Dehghani, 2018:137).

بازدارندگی سایبری مانند سایر شیوه‌های بازدارندگی، هنگامی موفق می‌شود که یک دشمن تصمیم بگیرد که تهاجمی عمل نکند. این تصمیم مستلزم دو ارزیابی جداگانه است: آیا هزینه‌های تجاوزگری سایبری از مزایای آن بیشتر است یا اینکه مزایای محدودیت در فضای مجازی از هزینه‌های آن بیشتر است؟ (Goodman, 2010: 107). چارچوب بازدارندگی سایبری این مفروضه کلی را پیشروی ما می‌گذارد که در عصر فناوری و فضای سایبری، دولت‌ها به‌ویژه آن‌هایی که

1. Denial
2. retaliation
3. Attribution

آسیب‌پذیری محیطی بالایی در امنیت ملی دارند، چاره‌ای جز تقویت و تحکیم قابلیت‌های امنیت سایبری ندارند تا بتوانند در مقابل اهداف خصمانه نیروهای متخاصم بازدارندگی موثر ایجاد کنند.

تحول در دکترین امنیتی ملی و نظامی اسرائیل

دکترین امنیتی - دفاعی اسرائیل از آغاز پیدایش تاکنون بر پایه‌ی دیدگاهی متمرکز و گسترده نسبت به مسئله تهدید قرار گرفته است. در چارچوب دکترین دفاعی اسرائیل، اکثر کشورهای عربی بالفعل یا بالقوه بخشی از یک ائتلاف به منظور نابودی اسرائیل هستند. با توجه به موقعیت ژئوپلیتیک و حساس خود، این کشور همواره در طراحی دکترین امنیتی - دفاعی خود نگاهی ویژه به محدودیت‌های جغرافیایی، عدم عمق استراتژیک، جمعیت اندک با بافتی ناهمگن و کاستی‌های منابع داشته است (Ben-Horin & Posen, 1981:6). هر چند در آغاز شکل‌گیری، این رژیم در مسیر استقلال و تصرف سرزمین ناگزیر بود رویکردی تهاجمی را در پیش گیرد که منجر به چندین جنگ تمام عیار و گسترده با اعراب شد، ولی به تدریج به سمت رویکردی تدافعی، بازدارندگی و کاهش تنش با اعراب پیش رفت و همواره به جنگ کوتاه مدت، برق‌آسا، پیروزی مطلق، حداقل تلفات و حداکثر دستاورد معتقد بود. اسرائیل تنها رژیمی است که همسایگان آن را تهدید به ریشه‌کنی کامل کرده اند. با وجود برتری نظامی اسرائیل، دکترین دفاعی این کشور جنگ را «گزینه‌ای بدون انتخاب» می‌داند که مستلزم تحمل هزینه‌های اجتماعی و اقتصادی سنگینی است (Bar, 2020:1).

در این راستا یکی از عناصر مهم سیاسی - نظامی اسرائیل، مسئله بازدارندگی بوده است. اینکه چطور از توانمندی‌های نظامی خود به‌عنوان ابزاری بازدارنده در مقابل تهدیدات بهره‌مند شود که ضمن آسیب استراتژیک به پیکره دشمن، هزینه‌های میدان نبرد را به حداقل برساند. علاوه بر اعمال کاستی‌های وجودی در نوع رفتار، اسرائیل دائماً درصدد جبران این کاستی‌ها جهت شناسایی و تثبیت بیشتر جایگاه خود در سطح منطقه خاورمیانه و نظام بین‌الملل به طرق مختلف برآمده است. یکی از مسیرهایی که این کشور جهت بهبود جایگاه و افزایش نفوذ و مشروعیت خود در سطح منطقه‌ای در آن گام نهاده، مسیر پیشرفت روز افزون در تکنولوژی است. جداول پایین به ترتیب وقایع داخلی و بین‌المللی که بر درک اسرائیل از مفهوم تهدید تأثیر گذاشته و امنیت سایبری و سیاست‌های دفاع سایبری آن را شکل داده و تحول در امنیت سایبری اسرائیل از دهه ۹۰ را موجب شده، به تصویر می‌کشد (Frei, 2020: 5-6).

جدول ۱. جدول زمانی رویدادهای محرک (داخلی)

۱۹۴۸	بعد از پیروزی در جنگ ۱۹۴۸ اعراب - اسرائیل دیوید بن گوریون با تشریح اصول سازمان نظامی اسرائیل اظهار داشت که حتی اگر صلح برقرار باشد، اسرائیل باید آمادگی کافی و مداوم خود را برای دفاع در هر زمان حفظ کند.
۱۹۶۷	در جریان جنگ شش روزه که تحریم تسلیحاتی بر منطقه اعمال و همکاری نظامی با فرانسه متوقف شد. اسرائیل به‌نوبه خود شروع به سرمایه‌گذاری در دفاع داخلی کرد. این به بخش هایتک کنونی اسرائیل کمک کرد.
۱۹۷۳	شکست اطلاعاتی در رهگیری سیگنال در آغاز جنگ یوم کیپور (۱۹۷۳) منجر به تلفات بیش از ۲۰۰۰۰ نیروی نظامی اسرائیل شد.
۱۹۹۵	ترور نخست‌وزیر اسحاق رابین اشتباهات اساسی توسط سرویس‌های اطلاعاتی را نشان داد.

انتفاضة دوم جامعه اطلاعاتی اسرائیل با استفاده از فناوری برتر و روشهای نظارتی برای کسب اطلاعاتی در زمان واقعی جهت مقابله با تروریسم، از برتری کیفی خود بهره برد.	۲۰۰۰ ۲۰۰۵
ادعا می شود سلاح سایبری اسرائیلی / آمریکایی استاکس نت موجب اختلال در فعالیت های تحقیقاتی ایران شده است.	۲۰۱۰
حملات DNS-DDoS که اسرائیل را هدف قرار دادند به عنوان پاسخی به موفقیت هایش علیه حماس در عملیات تیغه حفاظتی بود.	۲۰۱۴
حماس جهت دستیابی به تلفن های هوشمند سربازان اسرائیلی بد افزارهایی طراحی کرد و موفق به نظارت و جمع آوری اطلاعات محدود اما پیچیده ای شد.	۲۰۱۸
ایران با هک کردن تلفن همراه یکی نامزدان پست نخست وزیری و احتمالاً با تهدید وی، سعی در مداخله در انتخابات اسرائیل داشت.	۲۰۱۹

منبع: Jasper Frie (2020)

جدول ۲. جدول زمانی رویدادهای محرک (بین المللی)

ایالات متحده و شرکای آن با موفقیت از تاکتیک های جنگ الکترونیکی بهره برده اند. اسرائیل انتظار دارد که این به عنوان تاکتیک اصلی درگیری های آینده عمل کند	۱۹۹۱ / ۱۹۹۸
ایران مظنون به توسعه برنامه هسته ای با اهداف نظامی جهت افزایش قدرت منطقه ای خود و / یا حمله به اسرائیل است.	۲۰۰۰
حملات ۱۱ سپتامبر سرویس امنیتی اسرائیل را از خطر شکست های اطلاعاتی آگاه کرد.	۲۰۰۱
اسرائیل اقدام به حمله هوایی به تأسیسات سوریه که احتمال تولید سلاح هسته ای وجود داشت، کرد. در این جریان آن ها از قابلیت های سایبری برای از کار انداختن ضد هوایی سوریه بهره بردند.	۲۰۰۷
بدافزار رایانه ای «شعله» ویروس «شمون» کشف شدند. شمون توانایی های مخرب و در عین حال پیشرفته ایران را در زمینه فضای مجازی آشکار کرد.	۲۰۱۲
پس از اعلام خروج ایالات متحده از برجام، فعالیت های سایبری تهاجمی ایران علیه ایالات متحده به میزان قابل توجهی افزایش یافت.	۲۰۱۷
به تلافی حمله سایبری حماس علیه اهداف اسرائیل، ارتش اسرائیل یکی از مراکز سایبری حماس را بمباران کرد.	۲۰۱۹

منبع: Jasper Frie (2020)

جدول ۳. جدول زمانی تغییر و تحولات سیاسی

فاز نخست: تمرکز بر حفاظت از زیرساخت های حیاتی	
مسئول هماهنگی زیرساخت های ICT دولت و افزایش بهره وری، کارایی و امنیت در سراسر دولت است	۱۹۹۷ ایجاد واحد تهیلا
تعریف کلیه زیرساخت های مهم	۱۹۹۸ قانون تنظیم امنیت در ارگانهای عمومی
تنظیم بالفعل چارچوب سیاست امنیت سایبری ملی غیرنظامی و ایجاد سیاست های سیستم های رایانه ای ملی حیاتی از طریق سازمان امنیت ملی اطلاعات.	۲۰۰۲ قطعه نامه ۸۴ / B کمیته وزیران امنیت ملی
سایر به عنوان هدف ملی، تلاش در جهت ارتقا جایگاه اسرائیل و قرار گرفتن در بین پنج کشور پیشرو در زمینه فضای سایبری.	۲۰۱۰ ابتکار سایبری ملی
فاز دوم: تمرکز بر مشارکت بخش خصوصی	
پیشبرد توانمندی های سایبری ملی، ایجاد معماری ملی، اولویت های ملی و تأسیس دفتر سایبری ملی	۲۰۱۱

قطعنامه ۳۶۱۱/۲۰۱۱	
۲۰۱۵ قطعنامه ۲۴۴۳	پیشبرد مقررات ملی و رهبری دولتی " و قطعنامه ۲۴۴ " پیشرفت آمادگی ملی: تقویت معماری سایبری کشور با ایجاد اداره دفاع سایبری ملی، مرجع امنیت سایبری ملی و مرکز هماهنگی تیم پاسخ اضطراری رایانه ملی
۲۰۱۵ استراتژی نیروهای دفاعی اسرائیل	آخرین دکترین امنیت ملی عمومی، که فضای مجازی را به‌عنوان پنجمین حوزه جنگ در نظر می‌گرفته است
۲۰۱۷ راهبرد امنیت سایبری ملی اسرائیل	چشم‌انداز، اهداف، مفهوم عملیات اسرائیل را مشخص می‌کند
۲۰۱۷ قطعنامه ۳۲۷۰	ادغام دفتر ملی سایبر اسرائیل و مرجع امنیت ملی سایبر سابق در اداره ملی سایبر اسرائیل تازه تأسیس

منبع: Jasper Frie (2020)

علی‌رغم سیاست دفاع ملی قوی، اسرائیل استراتژی رسمی امنیت ملی ندارد. در گذشته، به دلیل موانع سیاسی و دیوان‌سالاری قابل توجه، تلاش برای تدوین استراتژی امنیت ملی به نتیجه نرسیده است. تلاش‌های امنیتی اسرائیل به‌جای اتکا به فرایندهای برنامه‌ریزی رسمی، تلاش می‌کند تا به صورت موقت پیگیری شود. در ادامه به مهم‌ترین استراتژی‌ها و اسناد سیاست‌گذاری اسرائیل اشاره می‌شود.

علیرغم عدم انتشار رسمی، اصول اصلی اعتقادی سیاست امنیتی اسرائیل کاملاً مشخص است. نخست‌وزیر اسبق، دیوید بن گوریون، اصول اساسی را در گزارش ۱۸ اکتبر ۱۹۵۳ خود به هیئت دولت ارائه داد. این اصول و درخواست بن گوریون در سال ۱۹۴۸ از اسرائیل جهت حفظ «آمادگی مداوم و کارآمد برای دفاع در هر زمان» حتی پس از پایان جنگ، هنوز هم برای امنیت سایبری امروز و استراتژی‌های دفاع سایبری مهم تلقی می‌شود. با جمع‌بندی این اصول، بن گوریون به ارتش اسرائیل دستور داد که تلاش خود را در این زمینه‌ها به کارگیرد:

- دفاع از دولت، ساکنان، زیرساخت‌ها و منافع آن
- بازدارندگی از حملات احتمالی
- تشکیل اتحاد با قدرت‌های بزرگ
- توسعه قابلیت‌های پیشرفته هشدار سریع برای جبران عدم عمق استراتژیک اسرائیل
- دستیابی به برتری فناوری و برتری کیفی برای جبران کمبود منابع حیاتی اسرائیل
- اطمینان از پیروزی سریع و قاطع در صورت رویارویی (Frei, 2020:9).

مسئله تهدید با وجود تغییر کانون تهدید، همواره اساسی‌ترین چالش پیش رو اسرائیل بوده و در دکترین امنیتی بن گوریون به آن پرداخته شده است. در واقع تهدیدات چهار حوزه را در برمی‌گیرند:

- حوزه داخلی: خطر سقوط اقتصادی و اجتماعی کشور؛

- حوزه منطقه‌ای: خطر جنگی دیگر با کشورهای عربی و مشکل نفوذ متخصص؛
- حوزه بین‌الملل: عدم شناسایی مرزهای آتش‌بس اسرائیل در سال ۱۹۴۹، مسئله آوارگان فلسطینی، مسئله وضعیت قدس و جایگاه اسرائیل در درگیری‌ها و اتحادهای بین بلوکی؛
- حوزه یهودیان: خاطره هولوکاست و اراده‌ای برای جلوگیری از تکرار چنین اتفاقی برای مردم یهود (Fried, 2020:130).

راهبرد نظامی اسرائیل ۲۰۱۵

سند راهبرد نظامی اسرائیل در اوت ۲۰۱۵ توسط ستاد مشترک اسرائیل به ریاست گادی آیزنکوت به زبان عبری منتشر شد و در اوت ۲۰۱۶ برگردان انگلیسی این سند به همت گراهام ایسون و مرکز بلفر انتشار یافت. این راهبرد که نخستین سند رسمی منتشرشده رژیم صهیونیستی در حوزه نظامی محسوب می‌شود، اصول راهنما، ساختار فرماندهی، اهداف و برنامه‌های نظامی اسرائیل در شرایط جدید امنیتی و محیط راهبردی متغیر خاورمیانه را آشکار می‌کند. به طور خاص، این استراتژی توسعه دشمنان در زمینه توانایی سایبری و همچنین دامنه سایبری را به‌عنوان یکی از چهار حوزه مرتبط به دفاع اسرائیل (زمین، دریا و هوا) تأیید می‌کند. این راهبرد همچنین توانمندی‌های سایبری را به‌عنوان پشتیبانی یکپارچه برای دفاع و حمله متعارف در تمام سطوح نبرد (به‌عنوان مثال استراتژیک، عملیاتی و تاکتیکی) در نظر گرفته است. ارتش اسرائیل برای اطمینان از این موارد، دفاع و تهاجم نظامی را حیاتی می‌داند: عملکرد دولت و نهادهای اسرائیلی، استفاده از اطلاعات، دفاع جمعی، اعمال نفوذ و دستیابی به مشروعیت و همچنین پاسخ‌های قانونی. سرانجام، این استراتژی بر بازدارندگی استراتژیک و تاکتیکی از طریق جنگ سایبری تأکید دارد (Eizenkot, 2016: 44).

استراتژی امنیت سایبری ملی اسرائیل ۲۰۱۷

قبل از سال ۲۰۱۷، اسرائیل هیچ‌گاه یک استراتژی جامع و رسمی امنیت ملی سایبری تدوین نکرده بود. این استراتژی توسط اداره ملی سایبری اسرائیل، اولین گزارش هیئت دولت در ارتباط با امنیت ملی اسرائیل از زمان اعلام اصول استراتژیک بن گوریون در سال ۱۹۵۳ محسوب می‌شود. این سند کوتاه اولویت‌های اداره ملی سایبر اسرائیل را توصیف می‌کند. جدا از اهداف مشترک عمومی، ارتباط چندانی با راهبرد نظامی اسرائیل ۲۰۱۵ ایزنکوت ندارد (Frei, 2020: 9). به طور خاص، این سند به چگونگی برنامه‌ریزی اسرائیل برای بهبود قدرت سایبری، انعطاف‌پذیری سیستمی، دفاع غیرنظامی ملی سایبری و تشریح و ایجاد وظایف مرجع امنیت ملی سایبری سابق می‌پردازد. سرانجام، این سند همچنین به ظرفیت-سازی و همکاری بین‌المللی اشاره دارد (INCD, 2017).

قطعه‌نامه‌های دولتی

پیش از استراتژی امنیت سایبری سال ۲۰۱۷، در قطعه‌نامه‌های مختلف دولتی تلاش شده است که فضای امنیت سایبری اسرائیل در دستور کار قرار گیرد. جدول زیر (جدول ۱) جزئیات بیشتری از این قطعه‌نامه‌ها شرح می‌دهد.

جدول ۴. لیست قطعه‌نامه‌های دولتی تنظیم‌کننده چشم‌انداز امنیت سایبری اسرائیل

اهداف	قطعه‌نامه‌ها
تنظیم با بالفعل چارچوب سیاست امنیت سایبری ملی غیرنظامی و ایجاد سیاست‌های سیستم‌های رایانه‌ای ملی حیاتی از طریق سازمان امنیت ملی اطلاعات.	B / ۸۴ (۲۰۰۲)
پیشبرد توانمندی‌های سایبری ملی، ایجاد معماری ملی، اولویت‌های ملی و تأسیس دفتر سایبری ملی	۳۶۱۱ (۲۰۱۱)
«پیشبرد مقررات ملی و رهبری دولتی» و «پیشرفت آمادگی ملی»: تقویت معماری سایبری کشور با ایجاد اداره دفاع سایبری ملی، مرجع امنیت سایبری ملی و مرکز هماهنگی تیم پاسخ اضطراری رایانه ملی	۴۲۴۴ و ۲۴۴۳ (۲۰۱۵)
ایجاد اداره سایبری ملی اسرائیل که دفتر ملی سایبری اسرائیل و مرجع امنیت سایبری ملی سابق را در خود ادغام می‌کند.	۲۳۷۰ (۲۰۱۷)

منبع: Jasper Frie (2020)

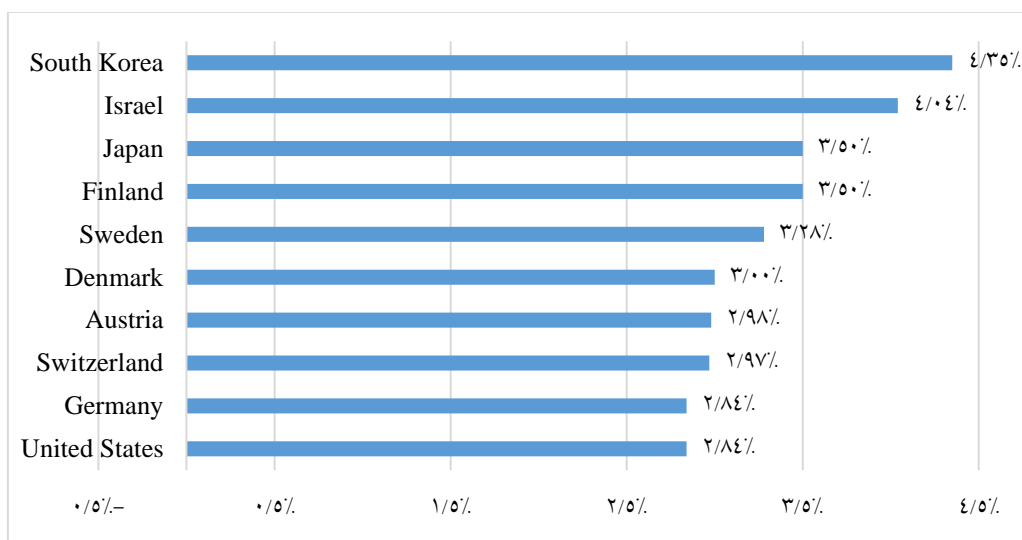
یک ارزیابی از توانمندی‌های سایبری اسرائیل

اسرائیل با حدود نه میلیون نفر جمعیت به‌سختی از لحاظ جمعیت در بین ۱۰۰ کشور قرار می‌گیرد اما در چندین رتبه‌بندی عمده‌ی کشورها، که ارزیابی بر اساس رقابت نوآوری، آمادگی برای تغییر و مهارت و استعداد نیروی کار صورت می‌گیرد، این رژیم جز بیست کشور اول جهان است. سیاست دولت و نیروهای دفاعی اسرائیل عامل اصلی نوآوری هستند. در واقع اکوسیستم فناوری اسرائیل متشکل از شرکت‌های چندملیتی و فناوری باز هست که عمدتاً در سلیکون وادی واقع در تلاویو متمرکز شده‌اند؛ تل آویو و نواحی اطراف آن غالباً به‌عنوان سلیکون وادی (عربی به معنای دره) شناخته می‌شود. زیرا صنعت فناوری برتر و نوآوری به‌طور گسترده در این مناطق متمرکز است. این بزرگترین و مرتبط‌ترین خوشه فناوری اسرائیل است و در میان خوشه‌های برتر فناوری و نوآوری در سراسر جهان قرار دارد. تل آویو از نظر تعداد استارت‌آپ‌ها در بین ۲۰ شهر برتر جهان قرار دارد و تقریباً نیمی از استارت‌آپ‌های اسرائیل در این شهر واقع شده‌اند. این شهر همچنین از نظر سرانه شرکت‌های نوپا پس از سلیکون ولی دوم است. براساس گزارش سازمان جهانی مالکیت معنوی، تل آویو جایگاه مطلوبی در رتبه‌بندی جهانی اکوسیستم فناوری دارد. تل آویو در سال ۲۰۲۰ در حوزه‌ی اکوسیستم فناوری نوپا جایگاه ششم در سطح جهان به خود اختصاص داده است (WIPO, 2020).

صدها شرکت چندملیتی^۱ امروزه در اکوسیستم تکنولوژی برتر اسرائیل نقش دارند. از اوایل سال ۲۰۲۰، با افزایش چشمگیر سرمایه‌گذاری‌ها در کشور، این تعداد رشد چشمگیری داشته است به‌ویژه در چند سال اخیر. بیش از نیمی از شرکت‌های چند ملیتی فعال در اسرائیل، از جمله غول‌های فناوری گوگل، IBM، آمازون، مایکروسافت، ایتل، فیس بوک و اپل، دارای دفتر مرکزی در ایالات متحده هستند. اروپا با پیشگامی آلمان، فرانسه و انگلیس با حدود یک‌چهارم شرکت‌های چندملیتی فعال، در منطقه دوم است. در مجموع، ۳۵ کشور حداقل از طریق یک شرکت چندملیتی در اسرائیل

1. Multinational corporations

حضور دارند. اکثر شرکت‌های آمریکایی در زمینه نوآوری باز فعالیت دارند؛ از هر ده شرکت آمریکایی که در حوزه نوآوری فعال و پیشرو هستند، شش شرکت در اسرائیل فعالیت می‌کنند. نوآوری در این چارچوب به معنای پیگیری رویکردی توزیع پذیرتر، مشارکت پذیرتر و غیرمتمرکزتر نسبت به خلاقیت‌های راهبردی نوآورانه است. تمرکز اصلی بر این موضوع است که شرکت‌ها باید از ایده‌های خارجی و داخلی استفاده کنند (Holst, 2020: 19). اسرائیل از لحاظ صرف هزینه‌های تحقیق و توسعه، بعد از کره جنوبی در رده دوم جهان در قرار دارد (M. Szmigiera, 2021) و از نظر سرانه‌ی سرمایه‌گذاری‌های ریسک‌پذیر در جهان جایگاه نخست دارد و همچنین دارای سابقه طولانی در نوآوری است. در واقع اسرائیل درست از زمان تاسیس، تحت فشار یک محیط خصمانه قرار داشت و باید از منابع کمیاب نهایت استفاده را می‌کرد. هم دولت و هم ارتش در ساخت و تقویت قدرت ابتکاری کشور نقش اساسی داشته‌اند (Holst, 2020: 11).



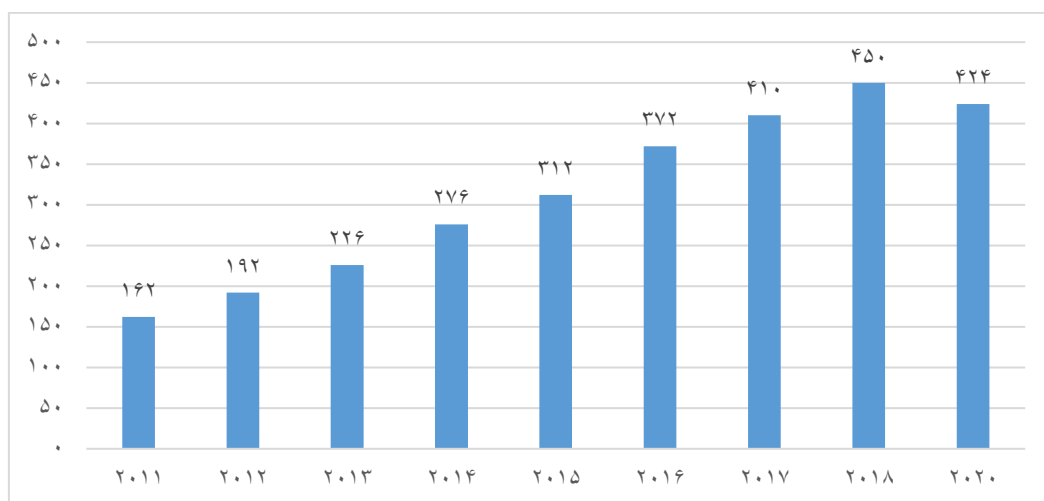
نمودار ۱. کشورهای پیشرو در صرف هزینه تحقیق و توسعه منبع: (Statista 2021)

درواقع اسرائیل به‌عنوان یک موجودیت سیاسی کوچک با تمرکز بر نقاط قوت خود توانسته است در مصاف با قدرت‌های بزرگی همچون ایالات متحده و چین، در زمینه هوش مصنوعی به یک ابرقدرت جهانی تبدیل شود. اسرائیل با استفاده از قابلیت‌های خود در زمینه هوش مصنوعی، در حوزه امنیت سایبری، سلامت دیجیتال و فین-تک به‌چنین دستاوردی رسیده است.

صنعت امنیت سایبری اسرائیل در دهه ۱۹۸۰ با تأسیس چندین شرکت توسعه نرم افزارهای ضد ویروس و امنیت اطلاعات تاسیس شد. این ورود زود هنگام به بازار فناوری سایبر و امنیت اطلاعات زمینه را برای تبدیل شدن اسرائیل به یکی از کشورهای پیشرو در این صنعت فراهم کرده است. بودجه کلی در این بخش در سال ۲۰۱۹ به بیش از ۱.۸ میلیارد

دلار آمریکا رسید که سهم دو رقمی از بازار جهانی بودجه امنیت سایبری است که در آن سال بالغ بر ۶.۲۴ میلیارد دلار آمریکا بود.

پیش از ۴۰۰ شرکت امنیت سایبری امروز در اسرائیل فعال و بیش از ۱۰ هزار کارمند در این بخش مشغول به کار هستند. سایبر آرک^۱، رادویر^۲، چک پوینت^۳ و Imperva از معروف‌ترین شرکت‌های امنیت سایبری اسرائیلی به شمار می‌آیند. صنعت امنیت سایبری اسرائیل داوطلبانی را از استعداد‌های نیروی مسلح خود جذب می‌کند. برخی از واحدهای ویژه نیروهای دفاعی اسرائیل مانند برنامه تالیپوت و یگان ۸۲۰۰ در مقابله مداوم با تهدیدات سایبری پیشتاز هستند. این سطح بالایی از دانش و تخصص به دست آمده توسط اعضای آن واحدها، به استعدادی با مهارت ویژه در صنعت امنیت سایبری اسرائیل تبدیل شده است (Hols, 202:31).



نمودار ۲. شرکت‌های فعال در حوزه امنیت سایبری در اسرائیل ۲۰۱۱-۲۰۲۰ منبع: (Statista 2021)

علی‌رغم اینکه تعداد شرکت‌ها در حال حاضر در حدود ۴۰۰ شرکت است (Liu, 2021)، این صنعت در سال ۲۰۱۹ افزایش قابل توجهی در جذب سرمایه داشته است. بودجه سال ۲۰۲۱ نسبت به سال قبل ۸۰ درصد رشد داشت. این پیشرفت نشانه رشد بازار است زیرا تقریباً همین تعداد شرکت به طور متوسط بودجه بسیار بالاتری دریافت می‌کنند (Holst, 202:30).

1. CyberArk
2. Radware
3. Check Point

جایگاه توانمندی سایبری در دکترین امنیت ملی اسرائیل

اسرائیل با برخورداری از فناوری‌های رقابتی، بودجه بالای فنی و تجهیزات نظامی-اطلاعاتی فعال، یکی از پیشرفته‌ترین بازیگران امنیت و دفاع سایبری در جهان است. موقعیت ژئوپلیتیکی آن باعث شده است تا از پیشرفته‌ترین قابلیت‌های اطلاعاتی و تهاجمی برای پشتیبانی از عملیات نظامی متداول، برق‌آسا و نمایش قدرت در منطقه بهره‌گیرد. تلاش برای امنیت همچنین باعث شده است تا مشارکت استراتژیک خود را با ایالات متحده تقویت کرده و تا حدودی در فرایندهای ایجاد هنجارهای بین‌المللی فضای مجازی شرکت کند. سیاست استراتژیک امنیت سایبری اسرائیل در راس امور، توسط اداره ملی سایبر اسرائیل¹ (INCD) که مستقیماً تحت حمایت نخست‌وزیر و دفتر وی قرار دارد، هدایت و هماهنگی می‌شود. اداره ملی سایبر اسرائیل، وظایف مرجع امنیت ملی سایبری² سابق (NCSA) را که دارای گرایش عملیاتی و دفتر ملی سایبر اسرائیل³ (INCB) که سیاست محورتر است را در خود ادغام می‌کند.

در سطح عملیاتی، تلاش‌ها با توجه به زمینه‌های حوزه موضوعی بین موساد⁴، شین‌بت⁵، پلیس اسرائیل⁶ و اداره ملی سایبر اسرائیل تقسیم می‌شود. در عمل، این آژانس‌ها ارزش‌های اصلی و رویکردهای عملیاتی مختلفی را ایجاد کرده‌اند که با اداره ملی سایبر اسرائیل اصطکاک ایجاد کرده‌اند. دفاع فعال سایبری و عملیات دفاعی دو ستون اصلی استراتژی امنیت سایبری اسرائیل محسوب می‌شود. رویکرد ارتش اسرائیل نیز توسط چهار اصل اعتقادی بن‌گوریون هدایت می‌شود: بازدارندگی، پیروزی قاطع، هشدار سریع و اتحاد. توانایی‌های آن در پاسخ به دشمنانی که صریحاً ذکر شده‌اند، مانند سوریه، ایران، لبنان، حزب‌الله، حماس و داعش توسعه‌یافته است (Frei, 2020). ارگان‌های اصلی دفاع سایبری نیروهای دفاعی اسرائیل (IDF) متشکل از واحد ۸۲۰۰ (برای عملیات سایبری تهاجمی) و اداره C-41⁷ (عملیات دفاعی و امنیت زیرساخت‌ها) است. شین‌بت، موساد، پلیس اسرائیل و وزارت دادگستری نیز در این ماجرا دخیل هستند. آن‌ها با اداره ملی سایبر اسرائیل (INCD) همکاری و هماهنگی دارند.

واحد ۸۲۰۰

ریشه واحد ۸۲۰۰ را می‌توان در فعالیت‌ها و میراث تعدادی از گروه‌های اطلاعاتی قبل از استقلال جستجو کرد که اکثر آن‌ها در دوران اقتدار انگلیس فعالیت می‌کردند و در طی شورش اعراب از ۱۹۳۹ تا ۱۹۳۵ و تا زمان استقلال اسرائیل در سال ۱۹۴۸ بسیار فعال بودند. بنابراین در پی جنگ یوم کیپور بود که واحد ۸۲۰۰ شکل مدرن به خود گرفت. در حالی که به طور متوسط هر چهار سال یکبار فرماندهان خود را تغییر داده و در بسیاری از جبهه‌ها فعال بوده و سازمان و ساختار

1. Israeli National Cyber Directorate
2. National Cyber Security Authority
3. National Cyber Bureau
4. Mossad
5. Shin Bet
6. Israel Police
7. C4I Directorate

کلی آن تا به امروز کاملاً ثابت مانده است (Cordey, 2019:5). واحد ۸۲۰۰ واحد اطلاعاتی یک ارتش نخبه است که بهترین استعدادها را در جهان تولید می‌کند. می‌توان آن را جهان کوچک متمرکز نامید که پیشران مهم داستان موفقیت اسرائیل بزرگ‌تر است. در واقع واحد ۸۲۰۰ اجتماع منحصربه‌فردی از افراد باهوش، مبتنی بر فناوری و با انگیزه، در محیطی برخوردار از آموزش‌های فنی پیشرفته، تجربه عملی نظامی و یک شبکه حرفه‌ای قدرتمند است (Rousseau, 2017:51). در ادامه به عمده وقایع مرتبط با فضای مجازی اشاره می‌شود، که حداقل تا حدی به واحد ۸۲۰۰ نسبت داده شده‌اند (Cyber Fusion Team, 2018):

- **ویروس استاکسنت^۱ (۲۰۱۰-۲۰۰۵):** این ویروس با موفقیت ساترفیوژهای نیروگاه هسته‌ای در نطنز ایران را از کار انداخت. طبق برخی ادعاها، این ویروس بخشی از بازی‌های مشترک عملیاتی بین آژانس امنیت ملی ایالات متحده^۲ و واحد ۸۲۰۰ اسرائیل بود (DW, 2019).
- **عملیات باغ میوه^۳ (سپتامبر ۲۰۰۷):** که در آن واحد ۸۲۰۰ به احتمال زیاد بدون هشدار به اپراتورهای پدافند هوایی، سیستم‌های راداری سوریه را مسدود کرده تا شرایط حمله هوایی دقیق به تأسیسات هسته‌ای سوریه در دیرالزور را فراهم کند. واحد ۸۲۰۰ با استفاده از رهگیری سیگنال^۴ جهت مکان‌یابی تأسیسات، باعث نقص عملکرد دفاع ضد هوایی در هنگام حمله شد (Cordey, 2019:9).
- **عملیات افشای کامل^۵ (مارس ۲۰۱۴):** که در آن یک کماندوی اسرائیلی یک کشتی ایرانی را در دریای سرخ، که اسلحه و تجهیزات نظامی به مقصد حماس حمل می‌کرد، رهگیری کرد. این عملیات توسط اطلاعات واحد به واسطه «قابلیت‌های پیشرفته سایبری و ارتباطی» امکان‌پذیر شده است (BBC News, 2014; Dombe, 2014).
- **خشی‌سازی توطئه تروریستی داعش^۶ (فوریه ۲۰۱۸):** واحد ۸۲۰۰ حمله احتمالی تروریستی داعش علیه هواپیمای مسافربری غیرنظامی را که از استرالیا به مقصد امارات متحده عربی در حرکت بود، کشف و از آن جلوگیری کرد. به طور قابل توجهی ارتباطات رهگیری خود را برای جلوگیری از حمله با مقامات استرالیایی به اشتراک گذاشت (IDF, 2018).

علاوه بر این فعالیت‌ها، این واحد در راستای اقدام برای پیشگیری از توطئه‌های پیچیده اقداماتی انجام می‌دهد. این حملات شامل حملات سایبری ایران علیه سازمان‌های خصوصی و عمومی در اسرائیل، اقدامات احتمالی ترکیه، قطر، کویت، امارات متحده عربی، عربستان سعودی و لبنان و همچنین حملات مختلف علیه اسرائیل توسط فلسطینی‌های

1. Stuxnet Virus
 2. National Security Agency (NSA)
 3. Operation Orchard
 4. SIGINT
 5. Operation Full Disclosure
 6. ISIS terrorist plot thwarted

مستقل از حماس^۱ در کرانه باختری است (Zitun, 2018). سایر بد افزارها و عملیات‌های غیر مستند اما مشکوک و منسوب به اسرائیل و واحد ۸۲۰۰ شامل موارد زیر است ((Cyber Fusion Team, 2018):

- **بدافزار شعله^۲** (۲۰۱۲-۲۰۰۷)، یک بدافزار ماژولار چند منظوره پیچیده‌ای است که ظاهراً توسط یک تیم حرفه‌ای برای اهداف جاسوسی سایبری تولید شده است. این اهداف در سراسر ایران، اسرائیل و سرزمین‌های فلسطین گسترش یافته است. بر طبق گزارشات این دارای اشتراکاتی با نسخه قبلی ویروس استاکسنت است. مقاله‌ای در واشنگتن پست عنوان کرده که هدف از رشته عملیات جاسوسی سایبری ویروس شعله ارائه اطلاعات برای حمله سایبری استاکسنت بوده است (Cordey, 2019:9).
- **ویروس Duqu** (۲۰۱۱-۲۰۰۹) بدافزار پیچیده و چند مرحله‌ای است که تولیدکنندگان سیستم‌های صنعتی را در بیش از دوازده کشور از جمله ایران، سودان و مجارستان هدف قرار می‌دهد. این ارتباط نزدیک با حمله استاکسنت دارد (Bencsáth et al., 2015:2).
- **بد افزار گاوس^۳** (۲۰۱۱-۲۰۱۲) این بدافزار به طور فعال در خاورمیانه منتشر شده است. بر خلاف شعله که در ایران گسترش می‌یابد، این بد افزار بیشترین تعداد آلودگی را در لبنان ایجاد می‌کند. در واقع، گاوس برای جمع‌آوری هر چه بیشتر اطلاعات در مورد سیستم‌های آلوده طراحی شده است. با این حال، یک ویژگی بارز گاوس این است که با تزریق ماژول‌های خاص خود به مرورگرهای مختلف، اعتبار سیستم‌های بانکی مختلف و شبکه‌های اجتماعی و همچنین حساب‌های ایمیل و پیام فوری را می‌دزد (Bencsáth et al; 2012:986).
- **ویروس Duqu 2.0** (۲۰۱۵-۲۰۱۴) یک نوع Duqu، یک عملیات سایبری مخرب و پیچیده که سازمان‌ها و اماکن مرتبط با مذاکرات توافق هسته‌ای ایران و ۱ + ۵ در وین و سوئیس را هدف قرار داد. طبق مقاله‌ای از گاردین، پیچیدگی و زمینه این بدافزار قویاً آن را به اسرائیل مرتبط می‌کند (Cordey, 2019:9).

شین بت و موساد

شین بت و موساد در کنار سازمان‌های اجرای قانون اسرائیل و امنیت سایبری غیرنظامیان فعالیت می‌کنند. آن‌ها تخصص و اطلاعات را به اشتراک می‌گذارند اما به اقتضای وظیفه خود به‌عنوان سرویس‌های اطلاعاتی، از اداره ملی سایبر اسرائیل جدا عمل می‌کنند. به همین دلیل است که هیچ اطلاعات عمومی در مورد وظایف، اقدامات، قابلیت‌های عملیاتی مرتبط با امنیت سایبری آن‌ها و همکاری‌شان با دیگر سازمان‌ها در دسترس نیست (Frei, 2020:5).

1. Lone - wolf Palestinians
2. Flame
3. Gauss

شین بت همچنین در دفاع از فضای مجازی نقش مهمی ایفا می‌کند اما مسئولیت‌های متفاوتی نسبت به ارتش اسرائیل بر عهده دارد. وظیفه آن در زمینه دفاع سایبری نسبتاً جامع است که نمونه آن هک تلفن همراه نخست‌وزیر علی‌البدل بنی گانتز در سال ۲۰۱۸ توسط ایران است. جامعه امنیتی نگران بود ایران با نوشتن محتوای در انتخابات ۲۰۱۹ دخالت کند. این مسئولیت کاهش خطر را به عهده شین بت می‌گذارد (Haaretz, 2019 & Harkov, 2019).

سامانه C4I

وظیفه سامانه C4I حفاظت از زیرساخت‌های ارتباطی نیروی دفاعی اسرائیل و سیستم‌های پردازش از راه دور است. علاوه بر این، از توسعه فناوری مربوطه پشتیبانی می‌کند. اخیراً، رویکرد C4I از دفاع سایبری به سمت «دفاع فعال» تغییر یافته است که شامل حملات بازدارنده و پیشگیرانه است. این پیشرفت مطابق با اصول اعتقادی بن گوریون در سال ۱۹۵۳ برای دفاع از دولت است به‌ویژه پیروزی سریع، قاطع، بازدارندگی، برتری کیفی و عالی‌ترین توانایی‌های هشدار سریع را می‌طلبد. سامانه C4I مرکزی را تأسیس کرده که بخش کامپیوتر و نیروهای اطلاعاتی ارتش را با هم ادغام می‌کند (Frei, 2020:5).

مواردی از بازدارندگی سایبری اسرائیل

دست برتر اسرائیل در جذب و گسترش گول‌های تکنولوژی، این کشور را در زمره پیشگامان صنعت امنیت سایبری در جهان قرار داده است. اقدامات سازمانی که توسط این رژیم برای حفاظت از فضای مجازی صورت می‌گیرد حاکی از اهمیت و ضرورت این بستر برای اسرائیل است. ارتش اسرائیل با تقسیم وظایف در بین بخش‌های مختلف از قبیل یگان ۸۲۰۰، شین بت، سامانه C4I و پلیس اسرائیل، نقش برجسته در تأثیرگذاری توانمندی سایبری در دکترین امنیت ملی این کشور ایفا می‌کند. در واقع، قلمرو سایبری مدت‌هاست که جایگاه قابل توجهی در تفکرات امنیتی اسرائیل به خود اختصاص داده است. طوری که امروزه توانمندی سایبری به‌عنوان اهرم بازدارندگی غیرمتعارف در دکترین امنیت ملی اسرائیل بیش از گذشته نمود یافته است.

گنجانده شدن فضای مجازی در استراتژی امنیت ملی اسرائیل، در خلال جنگ علیه اهداف استراتژیک در ایران، لبنان، سوریه و فلسطین (حماس) که بر طبق سند راهبرد نظامی اسرائیل تهدیدهای پیش روی این کشور در محیط راهبردی جدید خاورمیانه به‌حساب می‌آیند، به مرحله عملیاتی رسیده است. به زعم سران اسرائیل، جمهوری اسلامی ایران، به‌ویژه ایران هسته‌ای اصلی‌ترین تهدید وجودی اسرائیل به‌شمار می‌رود که به علت ضعف ساختاری دولت اسرائیل امکان اقدام نظامی متعارف علیه آن وجود ندارد و تنها در بستر مجازی است که می‌توان در روند فعالیت هسته‌ای ایران اختلال ایجاد کرد.

حمله به راکتور هسته‌ای ایران در سال ۲۰۰۹ اولین نمونه جنگ سایبری به حساب می‌آید و آغازگر دوران جدیدی در تحول استفاده از فضای مجازی در جنگ محسوب می‌شود. کیم ستر^۱، در مقاله‌ای به نقل از کانال دویچه وله فارسی، مدعی است که این ویروس نخستین ویروسی بوده که در عرصه جاسوسی و خرابکاری در تأسیسات اتمی طراحی و تولید شده است. این ویروس برای نخستین بار در سال ۲۰۰۷ وارد سامانه نرم‌افزاری تأسیسات اتمی نظنز شد؛ فرض محتمل این است که واحد ۸۲۰۰ ارتش اسرائیل، دارنده برترین روش‌های سایبری تهاجمی، با همکاری آژانس امنیت ملی ایالات متحده از ویروس استاکسنت برای حمله به نیروگاه هسته‌ای ایران در نظنز استفاده کرد (DW, 2019). از آن زمان به بعد هر از چندگاهی تحرکات سایبری علیه مراکز مربوط به فعالیت هسته‌ای ایران رخ داده که بی شک انگشت اتهام علیه اسرائیل نشانه می‌رود. از موارد دیگر می‌توان از عملیات سایبری مخرب و پیچیده بوسیله ویروسی موسوم به Duqu نام برد که سازمان‌ها و اماکن مرتبط با مذاکرات توافق هسته‌ای ایران و ۱ + ۵ در وین و سوئیس هدف قرار داد. و اما تازه ترین تحرک سایبری در ارتباط با تأسیسات هسته‌ای ایران، وقوع حادثه در تأسیسات هسته‌ای نظنز در تاریخ ۲۲ فروردین ۱۴۰۰ بود که منجر به اختلال در سیستم برق این مرکز شد. رسانه‌های اسرائیل به حمله سایبری بودن این حادثه و نقش موساد در آن اذعان کردند. مقامات ایران این حمله را مصداق «تروریسم هسته‌ای» خوانده و هدف اصلی اسرائیل از این اقدام را جلوگیری از توسعه صنعت هسته‌ای ایران و مذاکرات موفق برای رفع تحریم‌ها می‌دانند.

اسرائیل همچنین عملیات‌های سایبری مشابهی علیه لبنان و سوریه و جنبش حماس، به‌عنوان کانون‌های تهدید این کشور صورت داده است؛ سپتامبر ۲۰۰۷ عملیاتی موسوم به باغ میوه، جهت فراهم کردن شرایط حمله هوایی دقیق به تأسیسات هسته‌ای سوریه در دیرالزور، توسط واحد ۸۲۰۰ طراحی شد. گاووس، بدافزار دیگری است که به طور فعال در خاورمیانه منتشر شده و بیشترین میزان آلودگی را در لبنان ایجاد می‌کند. در واقع، گاووس برای جمع‌آوری هر چه بیشتر اطلاعات در مورد سیستم‌های آلوده طراحی شده است. با این حال، یک ویژگی بارز گاووس این است که با تزریق ماژول‌های خاص خود به مرورگرهای مختلف، اعتبار سیستم‌های بانکی مختلف و شبکه‌های اجتماعی و همچنین حساب‌های ایمیل و پیام فوری را می‌دزدد.

از بین بردن مغز متفکر و شخصیت‌های برجسته دشمن در عرصه‌های مختلف سیاسی و علمی یکی از اشکال تهاجم سایبری به حساب می‌آید که استفاده از این ابزار توسط اسرائیل نمود بیشتری یافته است. در واقع، اسرائیل تنها دولتی است که بخش مجزایی را در حلقه‌ی امنیتی و جاسوسی خود برای ترور افراد مختلف تاسیس کرده و آن را به‌عنوان یکی از برجسته ترین مبانی فکری و استراتژیک خود مطرح می‌کند. در اوایل دهه ۱۹۵۰ مأموران سازمان جاسوسی اسرائیل موسوم به موساد یک سری عملیات ترور علیه دانشمندان برجسته عرب انجام دادند. از همه مهم‌تر، اسرائیل مسئول مرگ فیزیکدان مصری دکتر علی مصطفی مشرفه فرض شد. اخیراً، از سال ۲۰۰۷، پنج دانشمند هسته‌ای ایران در شرایط اسرارآمیز

۱. نویسنده کتاب "شمارش معکوس تا روز صفر: استاکسنت و راه‌اندازی نخستین جنگ‌افزار دیجیتال جهان"

کشته شده‌اند، بیشتر آن‌ها با حمله مهاجمان موتورسوار و چسباندن بمب‌های مغناطیسی کوچک را به بدنه اتومبیل قربانیان به وقوع پیوست که سازمان جاسوسی اسرائیل به طور ضمنی و آشکار به طراحی این عملیات‌ها اقرار کردند (Meisels, 2013:207).

ترور رهبران سیاسی و فرماندهان نظامی لبنان و فلسطین، به‌ویژه اعضای گروه حماس و حزب‌الله، همواره در دستور کار دولت اسرائیل بوده است. تاکنون اشخاص بسیاری به واسطه سازمان‌های جاسوسی اسرائیل حذف فیزیکی شده‌اند. دو ماه پس از وقوع انتفاضه دوم در سپتامبر ۲۰۰۰، اسرائیل آشکارا سیاست خود را برای ترور شورشیان تحت نظر فلسطینی تصدیق کرد. تنها ۱۱ تن از رهبر سیاسی فلسطین بین سالهای ۲۰۰۰ و ۲۰۰۵ ترور شدند (Gazit & Bry, 2011: 862-3). جدول زیر اطلاعاتی در ارتباط با ترور رهبران فلسطینی که در جریان انتفاضه دوم قربانی ترور شدند ارائه می‌دهد.

جدول ۵. رهبران سیاسی فلسطینی قربانی ترور در جریان انتفاضه دوم

نام	مکان	زمان
ثابت ثابت	فتح	دسامبر ۲۰۰۰
جمال سلیم	حماس	ژوئیه ۲۰۰۱
جمال منصور	حماس	ژوئیه ۲۰۰۱
ابوعلی مصطفی	PFLP	آگوست ۲۰۰۱
جهاد احمد جبرئیل	PFLP	مه ۲۰۰۲
صلاح شهاده	حماس	ژوئیه ۲۰۰۲
ابراهیم المقدمه	حماس	مارس ۲۰۰۳
اسماعیل ابوشناب حمزه	حماس	آگوست ۲۰۰۳
احمد یاسین	حماس	مارس ۲۰۰۴
عبدالعزیز الرتیسی	حماس	آوریل ۲۰۰۴
عزالدین خلیل	حماس	سپتامبر ۲۰۰۴

باوجود رویکرد تهاجمی در فضای سایبری، دولت اسرائیل مدعی است که هدف اصلی حملات سایبری قرار گرفته است. در دکترین امنیت دفاعی اسرائیل، حملات سایبری یکی از چهار تهدید اصلی اسرائیل است. در ادامه به برخی از این حملات که بخش‌های مختلفی از اسرائیل را متأثر ساخته اشاره کوتاهی می‌شود. در سالهای ۱۲-۲۰۰۹، گروهی وابسته به ارتش آزادیبخش چین، ظاهراً به منظور سرقت نقشه سیستم‌های ضد راکتی و ضد موشکی، سه شرکت اسرائیلی را هک کردند. در سال ۲۰۱۱ گزارش شده است که ایران با ایجاد یک سری هویت‌های جعلی مجازی در نقش مجری خبری جهت ارتباط با مقامات دولتی و خبرنگاران اقدام به جمع‌آوری اطلاعات علیه اسرائیل، ایالات متحده و دیگر کشورهای غربی نموده است. اسرائیل، ایران، حماس و حزب‌الله را به یک سری حملات گسترده علیه «سیستم‌های حیاتی ملی» از

جمله آب، برق و سایت‌های بانکی متهم کرد. در طول مبارزات ۲۰۱۴ غزه، حملات ایران هم از نظر دامنه و هم از نظر اهداف انتخاب‌شده بیش از گذشته بود؛ حملات ایران عمدتاً زیرساخت‌های غیرنظامی، از جمله شبکه‌های مالی و همچنین سیستم‌های امنیتی دولت را هدف قرار داده است. اسرائیل با حملاتی از طرف ترکیه، شمال آفریقا و فلسطینیان روبرو شده است. علاوه بر این موارد، خطر بازیگران غیردولتی و فعالیت‌های سایبری توسط افراد و گروه‌ها نیز در حال افزایش است (Cohen & Charles, 2016:4). بنا به این دلایل ارتش اسرائیل در زمینه دفاع سایبری مهارت و پاسخگویی منحصر به فردی را ایجاد کرده است.

در سال ۱۹۹۷ اسرائیل تهیلا (زیرساخت‌های دولتی برای اینترنت)، یکی از اولین آژانس‌های امنیتی سایبری دولتی در جهان، را به منظور اطمینان از ارتباطات امن برای دفاتر دولتی و میزبانی امن برای وب سایت‌های دولتی تأسیس کرد. در سال ۲۰۰۲ دولت اسرائیل تصمیم گرفت برای حفاظت از زیرساخت‌های مهم ملی خود، سازمان امنیت ملی اطلاعات (NISA) را ایجاد کند. در سال ۲۰۱۱، اداره ملی سایبر تأسیس شد و اسرائیل اخیراً فرماندهی سایبر متمرکز جدیدی را ایجاد کرده است. در این راستا راهبرد نظامی اسرائیل که در آگوست ۲۰۱۵ توسط ستاد مشترک منتشر شد، توسعه دشمنان در زمینه توانایی سایبری و همچنین دامنه سایبری را به‌عنوان یکی از چهار حوزه مرتبط به دفاع اسرائیل (زمین، دریا و هوا) تأیید می‌کند. این راهبرد همچنین توانمندی‌های سایبری را به‌عنوان پشتیبانی یکپارچه برای دفاع و حمله متعارف در تمام سطوح نبرد (به‌عنوان مثال استراتژیک، عملیاتی و تاکتیکی) در نظر گرفته است. استراتژی امنیت سایبری ملی اسرائیل (۲۰۱۷) که سند ی کوتاه به منظور ارائه اولویت‌های اداره ملی سایبر اسرائیل است را می‌توان تلاشی دیگر در این مسیر دانست.

نتیجه‌گیری

امروز تهدیدات سایبری پیامد مستقیم جایگاه حیاتی سیستم‌های رایانه‌ای در زیرساخت‌های ملی و زندگی مدرن است. سیستم‌ها و بخش‌های مختلف به‌طور جداگانه توسعه یافتند و در نهایت برای تشکیل یک شبکه سایبری که معمولاً امنیت محور نبود، همگرا شدند. بر اساس یافته‌های ارائه‌شده پرداختن به جنبه‌های امنیتی حیات سایبری ضروری است، رهبران اسرائیل نیز ملزم به پیش‌بینی چگونگی میدان نبرد سایبری آینده و الزامات موردنیاز برای پیروزی در آن شده‌اند. توسعه راهبردهایی برای مشارکت در جنگ سایبری و دفاع در برابر آن با دیگر جنبه‌های وضعیت اسرائیل همخوانی دارد. تجارب گذشته گویای این است که درگیری‌های نظامی به دلیل عدم عمق استراتژیک، جمعیت اندک و ناهمگن و موقعیت ژئوپلیتیک حساس اسرائیل، دستاورد چندانی برای این کشور در پی نخواهد داشت. در واقع با بررسی جنگ‌های نظامی اخیر، به‌ویژه پس از سال ۲۰۰۶ میلادی، می‌توان دریافت که ارتش اسرائیل در میدان از دستیابی به هدف ناتوان بوده و از کنترل و ابتکار عمل عاجز است. در طول دو دهه اخیر اسرائیل حتی با ایجاد «گنبد آهنین»، در افزایش ضریب ایمنی و

آمدگی این جبهه و تاب‌آوری آن برای یک جنگ حداقل دوماهه ناکام بوده و گسست جبهه داخلی اسرائیل و عدم توانایی آن در همزیستی با یک جنگ طولانی مدت را بیش پیش آشکار کرده است.

برای نمونه می‌توان به جنگ سی سه روزه اشاره کرد. این جنگ در واقع ششمین جنگ و می‌توان از آن به‌عنوان آخرین جنگ تمام عیار اسرائیل با یک کشور عربی یاد کرد که با وجود سال‌ها پیشرفت تکنولوژیک و نظامی نسبت به جنگ‌های قبل، وادار به تسلیم در مقابل توان مبارزاتی و مدیریت جنگی جنبش مقاومت حزب‌الله لبنان شده و سرانجام با میانجیگری سازمان ملل و با صدور قطعنامه‌ای توانست از باتلاقی که در آن گیر کرده بود خارج شود. از آن زمان تاکنون درگیری‌های کوتاه مدت با نوار غزه در سال‌های ۲۰۰۸-۹، ۲۰۱۲، ۲۰۱۴ و به‌ویژه جنگ یازده روزه می‌۲۰۲۱ هر بار ضعف اسرائیل در عرصه نبرد نظامی متعارف آشکارتر ساخت. نبرد یازده روزه می‌۲۰۲۱ که آخرین آزمون اسرائیل در عرصه نظامی است، ضعف و ناکارآمدی سرویس اطلاعاتی این کشور در پیش‌بینی چنین حملات موشکی آن هم در این سطح از سوی جنبش حماس و ناتوانی سیستم گنبد آهنین در مقابله با موشک‌ها را آشکار ساخت. در واقع اسرائیل قادر به پیش‌بینی چنین حملاتی را در این سطح از سوی حماس نبوده و می‌توان گفت که حمله موشکی فراگیر حماس به‌ویژه در تل‌آویو رخدادی غیرقابل تصور و شوک بزرگی برای سران اسرائیل بوده است. عدم موفقیت اسرائیل در حفاظت از عمق مناطق تحت کنترل، این کشور را وادار به بازبینی تئوری‌های گذشته و ارزیابی درست و واقع‌بینانه از مؤلفه امنیت با نقش-آفرینی ویژه توانمندی سایبری خواهد کرد.

جنگ سایبری به اسرائیل این امکان را می‌دهد که بدون به خطر انداختن جان شهروندان و سربازان خود، عملیات علیه اهداف دوردست را آغاز کند، که هدف اصلی چنین کشور کوچکی با منابع انسانی محدود است. عملیات‌هایی از این دست همچنین اعتبار جهانی را برای اسرائیل به ارمغان می‌آورد، که می‌تواند هم از نظر اقتصادی به نتیجه این کشور کمک کند - همانطور که سایر کشورها به دنبال تخصص و فناوری‌ها و کاربردهای پیشرفته به دولت یهود هستند - و هم بازدارندگی را تقویت می‌کند.

در حالی که به نظر می‌رسد اسرائیل با تهدید سایبری به روش‌های پیشرفته‌ای مطابق با مفهوم کلی امنیت ملی خود برخورد می‌کند، احتمالاً باگذشت زمان اقدامات بیشتری باید انجام شود. یکی از این اقدامات ممکن است ایجاد همکاری بین نهادهای مختلف امنیتی متولی دفاع سایبری به منظور ایجاد سیاست بهینه برای دفاع سایبری و تعیین تمهیدات ملی برای این منظور باشد.

هدف این مقاله ایجاد یک ارتباط معنادار بین توانمندی سایبری اسرائیل و بازتعریف بازدارندگی در دکترین امنیتی دفاعی این کشور بود. مقاله این ایده اصلی را به آزمون گذاشت که اسرائیل با تقویت توانمندی‌ها و قابلیت‌های سایبری، قلمرو بازدارندگی را به خارج از مرزها گسترش داده و با بازتعریف بازدارندگی در دکترین امنیتی دفاعی خود به سمت ابزارهای بازدارندگی غیرمتعارف در حرکت است؛ تغییرات در محیط جهانی و منطقه‌ای و همچنین تغییر در محیط راهبردی

خاورمیانه، ضعف ساختاری و شکست در میدان نبرد نظامی، انتقال از رویکرد کنش به واکنش و قابلیت‌های سایبری بالا موجب ارزیابی واقع‌بینانه اسرائیل از مؤلفه امنیت با نقش‌آفرینی فزاینده توانمندی‌های سایبری شده است. در واقع، گذر از ابزارهای متعارف نظامی به ابزارهای غیرمتعارف، اسرائیل را به رصد راهبردهای امنیتی ملی با محوریت توانمندی سایبری در مقابله با کانون‌های جدید تهدید ترغیب می‌کند. هدف راهبردی دولت اسرائیل از آغاز شکل‌گیری تاکنون مبارزه با تهدیدات وجودی و ارتقاء و تثبیت جایگاه خود در نظام بین‌الملل بوده است. علیرغم ضعف‌های ساختاری که اقتضای نحوی به وجود آمدن آن به‌عنوان یک موجودیت بین‌المللی است، اسرائیل با تمرکز بر نقاط قوت خود توانسته است در مصاف با قدرت‌های بزرگی همچون ایالات متحده و چین، در زمینه هوش مصنوعی و متعاقباً در حوزه توانمندی سایبری به یک ابرقدرت جهانی تبدیل شود. در حال حاضر اسرائیل در تلاش است تا از دریچه توانمندی سایبری پرتویی به نقاط تاریک امنیتی خود افکند. شکست نظامی - اطلاعاتی در مقابل موجودیتی مثل حماس در نبرد اخیر نشان داد که در برخورد با چالش جدی‌تر مثل ایران، جنگ نظامی گزینه‌ای مطلوب برای اسرائیل نخواهد بود و پیش‌بینی می‌شود که در آینده بازدارندگی سایبری جایگاه استراتژیک‌تری در دکترین امنیتی - دفاعی اسرائیل به خود اختصاص دهد.

کتابنامه

1. Bar, S., (2020). Israeli strategic deterrence doctrine and practice. *Tandfonline*, 3(1), 321-353. *Published online*: <https://www.tandfonline.com/doi/abs/10.1080/01495933.2020.1772624>
2. BBC News. (2014). Israel halts weapons shipment from Iran [WWW Document]. BBC News. URL <https://www.bbc.com/news/world-middleeast-26451421>
3. Bencsáth, B., Ács-Kurucz, G., Molnár, G., Vaspöri, G., Buttyán, L., & Kamarás, R., (2015). *Duqu 2.0: A comparison to Duqu*. Budapest: Budapest University of Technology and Economics. <https://www.crysys.hu/publications/files/duqu2.pdf>
4. Bencsath, B., Felegyházi, M., Buttyan, L., & Gabor, P., (2012). *The Cousins of Stuxnet: Duqu, Flame, and Gauss*. Budapest: Budapest University of Technology and Economics. www.mdpi.com/journal/futureinternet
5. Bendiek, A., & Metzger, T., (2015). *Deterrence theory in the cyber-century Researcher. Lecture Notes in Informatics (LNI)*. Bonn: Gesellschaft für Informatik
6. Ben-Horin, Y., & Posen, B., (1981). *Israel's Strategic Doctrine*. Rand.
7. Burak Tolga, I., (2018). *Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture*. Estonia, Tallinn: CCDCOE.
8. Cohen, M., & Freilich, C., (2016). Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives*, 1-15. <https://www.researchgate.net/publication/288823312>
9. Cordey, S., (2019). The Israeli Unit 8200 – An OSINT-based study Trend Analysis. *Center for Security Studies (CSS), ETH Zürich*, <https://doi.org/10.3929/ethz-b-000389135>.
10. Cristiano, F., (2020). *Cyber defense and security as national trademarks of international legitimacy (Israel)* in Romaniuk S. N. and Manjikian M. (2020, eds.) *Routledge Companion to Global Cyber-Security Strategy*. New York: Routledge.
11. Cyber Fusion Team. (2018). Spies in the Middle East: Israeli Cyber Operations [WWW Document]. Secur. Alliance. URL <https://www.secalliance.com/blog/spies-in-the-middle-east/>

12. Dehghani, A.A., (2018). Cyber Deterrence in the New Global Security: The Cyber Threat of Russia and China against Vital US Infrastructure. *Political and International Approaches*, 4(4), 121- 147.[in persion]
13. DW. (2019). How did the Stuxent virus enter the Natanz nuclear facility? <https://www.dw.com/fa-ir> [in persion]
14. Eizenkot, G., (2016). *Deterring Terror. How Israel Confronts the Next Generation of Threats*. (Rosenberg, S., Trans.). Cambridge: Belfer Center.
15. Frei, J., (2020). Israel's National Cybersecurity and Cyberdefense Posture. *Center for Security Studies (CSS), ETH Zürich*.
16. Fried, Y., (2020). Military, Civilian or Both: David Ben-Gurion's Perception of National Security after the War of Independence. *Contemporary Review of the Middle East*, 7(2) 125–142.
17. Gazit, N., Brym, R.J., (2011). State-directed political assassination in Israel: A political hypothesis. *International Sociology* .26(6) 862–877.
18. Goodman, W., (2017). Cyber Deterrence: Tougher in Theory than in Practice? *Strategic Studies Quarterly*, 4(3), 102-135.
19. Haaretz. (2019). Israel Says Iran Hacked Ex-general Gantz's Phone Ahead of Election. *Haartzet*, 14.03.2019. <https://www.haaretz.com/israel-news/elections/benny-gantz-s-cellphone-hacked-by-iranian-intelligence-1.7022269>
20. Harkov, L., (2019). Politics: The cybersecurity election. *The Jerusalem Post*. 04.04.2019. <https://www.jpost.com/Israel-Elections/Politics-They-cybersecurity-election-585802>
21. Holst, A., (2020). Israel: the Tech Innovation Nation, Released: October 2020 at: <https://www.statista.com/study/82392/israel-the-tech-innovation-nation/> .
22. IDF. (2018). 8200 Unit thwarts an ISIS attack [WWW Document]. IDF. URL <https://www.idf.il/en/articles/terror-and-threats/8200-unit-thwarts-an-isis-attack/>
23. INCD. (2017). Israel National Cyber Security Strategy in Brief. Prime Minister Office. https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf
24. Libicki, M.C., (2009). Cyber deterrence and Cyberwar. In Cyber deterrence and Cyberwar, CA: RAND, 27-37.
25. Liu, Sh., (2021). Active cybersecurity companies in Israel 2011-2020. Jan 18. <https://www.statista.com/statistics/1003442/israel-cyber-security-companies/>.
26. Meisels, T., (2013). Assassination: Targeting Nuclear Scientists, *Law and Philosophy* (2014) 33: 207- 234.
27. Muttahid Askari, E., (2000). Science and Technology in Israel. *Regional Studies in Israeli Studies and American Studies* No. 4. [in persion]
28. Nye, J.S., (2017). Deterrence and Dissuasion in Cyberspace. *International Security*. *International Security*, 41(3), 44–71.
29. Philbin, M.J., (2013). Cyber Deterrence: An Old Concept in a New Domain Carlisle. Available at: <https://www.semanticscholar.org/paper/Cyber-Deterrence%3A-An-Old-Concept-in-a-New-Domain-Philbin/356d310b914e32596ea46f2beaf26048a5de1b2>
30. Rousseau, J.P., (2017). The history and impact of unit 8200 on Israeli HI-TECH entrepreneurship. A Thesis Presented to The Honors Tutorial College. *Ohio University*.
31. Ryan, N.J., (2018). Five Kinds of Cyber Deterrence. *Philos. Technol.* 31:331–338.
32. Szmigiera, M., (2021). Research and development worldwide - Statistics & Facts. <https://www.statista.com/topics/6737/research-and-development-worldwide/?topicHeaderWrapper>
33. Torabi, Q., (2016). An analysis of the military strategy document of the Zionist regime. *National Watch*, 54(3), 39-44. [in persion]

34. World Intellectual Property Organization. (2020). Ranking the Tel Aviv startup ecosystem. <https://www.savills.com/search/sitesearch.aspx?page=1&searchKeyRanking%20the%20Tel%20Aviv%20startup%20ecosystem&filter>
35. Zitun, Y., (2018). IDF's Unit 8200 helped Australia thwart attempt to bomb plane. [WWW Document]. Ynet. URL <https://www.ynetnews.com/articles/0,7340,L5124744,00.html>