Vol. 1, No. 1, Serial No. 1, Autumn & Winter 2024

JAROS

Journal of Asian Regional Orders Studies

Journal Homepage: https://ijas.shirazu.ac.ir

Research Article

Exploring Trojan Horses in Asia: An Analysis of Israeli-Iranian Confrontations Post the Stuxnet Attack

Masih Mirzaei[1], Seyed Yousof Qorashi[2*]

1. MA in Political Sciences, Political Sciences Department, Shiraz University, Shiraz, Iran
2. Assistant Professor of International Relations, Department of Political Science, Shiraz University, Shiraz, Iran

Article history: Received: 23/05/2024 Accepted: 19/08/2024

Abstract

The competition among major powers to acquire nuclear capabilities has shifted from Europe to Asia over time. The addition of India, Pakistan, North Korea, and Israel has resulted in two-thirds of the world's nuclear countries being located in Asia. Although the NPT regime was established to ensure the peaceful management of atomic threats, some political entities, such as Israel, managed these threats independently. It is important to examine how Israel has managed nuclear threats because it signifies a transformation in the realm of security. Israel has influenced this development by utilizing cyber Trojan horses, particularly the Stuxnet worm, against Iran's nuclear program. In this article, the authors examine the impact of the Stuxnet attack on Iran's nuclear program and its influence on the realm of security and the Iran-Israel conflicts. The findings indicate that cyber issues have become part of security discussions in Asia after the Stuxnet attack. Iran, in response, aimed to deal with threats by bolstering its cybersecurity infrastructure, establishing a cyber army, and investing in its cyber capabilities. This has led to the occurrence of the Iran-Israel cyber war and the normalization of the use of Trojan horses in Asia as a consequence of these policies. This article relies on a descriptive-analytical method using library data.

Keywords: Asia, Cybersecurity, Iran, Israel, Stuxnet, Trojan Horse

Please cite this article as:
Mirzaei, M., Qorashi, S.Y. (2024). Exploring Trojan Horses in Asia: An Analysis of Israeli-Iranian Confrontations Post the Stuxnet Attack. *Journal of Asian Regional Order Studies*, *1*(1) 309-336.

* Corresponding author:
E-mail address: qorashi@shirazu.ac.ir

سال اول، شماره ۱، پاییز و زمستان ۱۴۰۳

JAROS

پژوهشنامه نظم‌های منطقه‌ای آسیا

Journal Homepage: https://ijas.shirazu.ac.ir

doi: https://doi.org/10.22099/IJAS.2024.50410.1004

مقاله پژوهشی

اسب‌های تروای سایبری در آسیا: تحلیلی از رویارویی اسرائیل و ایران پس از حمله استاکس نت

مسیح میرزائی[۱]، سید یوسف قرشی[۲*]

۱. دانش آموخته کارشناسی ارشد علوم سیاسی، گروه علوم سیاسی، دانشگاه شیراز، شیراز ، ایران

۲. استادیار روابط بین الملل، گروه علوم سیاسی، دانشگاه شیراز، شیراز، ایران

اطلاعات مقاله تاریخ دریافت: ۱۴۰۳/۰۳/۰۳ تاریخ پذیرش: ۱۴۰۳/۰۵/۲۹

چکیده

رقابت اروپامحور قدرت‌های بزرگ برای دستیابی به قابلیت‌های هسته‌ای با گذر زمان به آسیا منتقل شد. اضافه شدن هند، پاکستان، کره شمالی و اسرائیل سبب شده که در حال حاضر دوسوم کشورهای هسته‌ای جهان، آسیایی باشند. هرچند رژیم ان‌پی‌تی جهت تضمین مدیریت صلح‌آمیز تهدیدات هسته‌ای تأسیس شد، برخی موجودیت‌های سیاسی همچون اسرائیل به‌صورت خودبنیاد، تهدیدهای هسته‌ای را مدیریت کردند. بررسی شیوه مدیریت تهدیدهای هسته‌ای توسط اسرائیل اهمیت دارد، زیرا یک دگرگونی در قلمرو تأمین امنیت را رقم زد. اسرائیل به کمک اسب‌های تروای سایبری، به‌ویژه به‌کارگیری کرم استاکس‌نت علیه برنامه هسته‌ای ایران، این تحول را شکل داد. در این مقاله، چنین تحولی در پرتو سؤال «حمله استاکس‌نت به برنامه هسته‌ای ایران چه تحولی را در قلمرو امنیت و منازعات ایران-اسرائیل رقم زد» بررسی شده است. یافته‌ها نشان می‌دهد که پس از حمله استاکس‌نت، آسیا شاهد ورود موضوعات سایبری به قلمرو امنیت شد و ایران به‌عنوان کشور آماج این تهدیدها، به مدد تقویت زیرساخت‌های امنیت سایبری، تأسیس ارتش سایبری، بازنگری و سرمایه‌گذاری در توانمندی‌های سایبری به مدیریت این تهدیدها پرداخت. وقوع جنگ سایبری ایران- اسرائیل و عادی‌سازی کاربرد تروا‌ها در آسیا پیامد اتخاذ این سیاست‌ها بوده است. روش مقاله حاضر توصیفی-تحلیلی است و از داده‌های کتابخانه‌ای بهره گرفته شده است.

واژگان کلیدی: آسیا، اسب تروا، استاکس‌نت، اسرائیل، امنیت سایبری، ایران

استناد به این مقاله:

میرزائی، مسیح و قرشی، سید یوسف (۱۴۰۳). اسب‌های تروای سایبری در آسیا: تحلیلی از رویارویی اسرائیل و ایران پس از حمله استاکس نت. *پژوهشنامه نظم‌های منطقه‌ای آسیا*. ۱. (۱). ۳۳۶-۳۰۹.

* نویسنده مسئول:

E-mail address: qorashi@shirazu.ac.ir

سرآغاز

اسب تروا یادآور افسانه یا واقعیتی از جنگ تروا با یونانی‌هاست که به‌وسیله پیکره‌ای از اسب که سربازان یونانی در آن مخفی شده بودند، پیروزی به دست آمد. به‌کارگیری چنین ترفندهایی برای پیروزی در جنگ همواره از سوی استراتژیست‌ها به رهبران سیاسی توصیه شده است؛ به‌ویژه زمانی که ناکامی در جنگ و عدم دستیابی به اهداف قریب‌الوقوع باشد. افسانه یا رویداد جنگ تروا و پیروزی یونانی‌ها به مدد اسب تروا یکی از مثال‌های کلاسیک دوست‌پنداری دشمن به‌واسطه ظاهر فریبنده است. اگر ترواییها (تروجان‌ها) اسب پیشکشی یونانی‌ها را به قلعه خود راه نمی‌دادند، ایده اودیسیوس، استراتژیست یونانی برای پیروزی در جنگ با شکست مواجه می‌شد. امروزه مستند به این افسانه یا رویداد تاریخی، اسب تروا یا تروجان را به ترفندی نسبت می‌دهند که هکرها برای ورود به کامپیوتر افراد از آن بهره می‌برند. رایانه‌ها، تروجان را به‌مثابه یک برنامه بی‌خطر تشخیص می‌دهند، لذا اجازه ورود و جای‌گیری در کنار فایل‌های دیگر می‌یابند.

این اقتباس تاریخی و سپس فنی کامپیوتری در حال حاضر تبدیل به ابزاری در دست دولت‌هایی شده که از پیروزی در جنگ‌ها به‌طور سنتی ناامید شده‌اند، اما همچنان سودای پیروزی در سر دارند. آسیای ژئوپلیتیک به‌عنوان بخشی منازعه‌خیز از جهان که قرن‌هاست عرصه رویارویی قدرت‌ها و موجودیت‌های جهانی و منطقه‌ای بوده نیز از این قاعده مستثنا نیست. رهبران کشورهای این منطقه با ملاحظه پیگیری اهداف خود در جنگ و شکست دشمنان به اسب‌های تروا متوسل شده‌اند و نهادهایی را برای تحقیق و توسعه این امر اختصاص داده‌اند. این نهادها ذیل بخش «امنیت سایبری» تعریف شده‌اند که وظیفه آن‌ها شناسایی فرصت‌ها و تهدیدهایی ناظر به فضای سایبر است. عربستان سعودی، امارات متحده عربی، مصر، عراق و ترکیه در زمره کشورهایی محسوب می‌شوند که در این قلمرو فعال‌اند.

اما دو قدرت منطقه‌ای، اسرائیل و ایران نیز که منازعات پر قدمتی را تجربه کرده‌اند، به این حوزه وارد شده‌اند. به تعبیر دیگر، این دو کشور علاوه بر منازعات سنتی و فیزیکی، دارای تقابلات متعدد سایبری بوده‌اند. اسرائیل در تمامی استراتژی‌های ملی منتشرشده از راهبردهای سالیانه خود و بنا به نظر اندیشمندان این کشور که برآمده از کنفرانس‌های علمی و اندیشکده‌های

آن است، جمهوری اسلامی ایران را به‌عنوان تهدید اول و در رده تهدید وجودی قرار می‌دهد (قرشی و پورحسن، ۱۴۰۰: ۱۵۲). به سخن دیگر و به اذعان این منابع، ایران موجودیت اسرائیل را تهدید می‌کند و تقابل با مؤلفه‌های قدرت ایران یک الزام استراتژیک محسوب می‌شود. برنامه هسته‌ای ایران یک مؤلفه مهم قدرت از نوع نامتعارف به‌حساب می‌آید که نابودی آن فوری و شدید تلقی می‌شود. ازاین‌رو بیش از دو دهه است که با اتکا به ابزارهای سخت همچون ترور افراد درگیر با این برنامه، سازوکارهای نهادی همچون ائتلاف‌سازی‌های جهانی و اقلام سایبری اعم از ویروس و بدافزار به رویارویی با ایران دست زده است. حمله استاکس نت در سال ۲۰۱۰ به سیستم‌های تأسیسات هسته‌ای ایران که منجر به خسارت به کامپیوترها و تخریب سانتریفیوژهای در حال کار شد، در زمره اقلام سایبری قرار می‌گیرد.

فارغ از بررسی خسارات وارد بر برنامه هسته‌ای ایران، موضوع مهم این است که حمله سایبری استاکس نت اولین حمله سایبری تاریخ با تأثیرات بر دنیای فیزیکی برشمرده شده و از این حیث نیازمند بررسی است. این اولین بار است که فضای سایبری باعث برهم‌خوردن منازعات در فضای فیزیکی و حقیقی در سطح بین بازیگران دولتی شده است و بررسی این تأثیر و صحت‌سنجی آن ضرورت دارد. ازنظر پیامدهای سیاسی، حمله استاکس نت نشان داد جنگ سایبری در حال تبدیل‌شدن به شاخصه مهم جنگ‌های مدرن و اثرگذار بر جایگاه قدرت کشورهاست. این حمله پتانسیل تسلیحات سایبری را به‌منظور ایراد آسیب فیزیکی به زیرساخت‌های حیاتی نشان داد و نیاز کشورها به توسعه دفاع مؤثر در برابر حملات سایبری را برجسته کرد.

در قلمرو پژوهشی مرتبط با موضوع این مقاله آثاری به چشم می‌آید. آرون برنتلی (Brantly, 2018) به بررسی روند تغییرات در نگرش به بازدارندگی سایبری پرداخته و مشکلات عملکردی این موضوع در عصر حاضر و برداشت‌های ناصحیح از آن را موردبررسی قرار داده است. همچنین بندیک و متزگر (Bendiek and Metzger, 2015) به ابعاد دیگر موضوع بازدارندگی سایبری در قرن حاضر پرداخته‌اند. در موضوع جنگ سایبری و بخصوص بررسی آن در آسیا آثار متعدی منتشر شده است. ولنتینا فون کنشتاین (Mellor,2022) در مقاله خود به موضوع امنیت سایبری در آسیا پرداخته است. همچنین آنتونی ماتازارو (Mattazaro,2020) در نوشتار خود به بررسی ماهیت جنگ سایبری و سطوح عملیاتی آن

پرداخته است. بخش عمده‌ای از آثاری که در ایران نگاشته شده‌اند به ابعاد حقوقی حمله استاکس‌نت پرداخته‌اند. به‌عنوان نمونه سعید نامدار و غلامعلی قاسمی (۱۳۹۷) در مقاله خود به ابعاد حقوقی حمله استاکس اشاره می‌کنند و نتیجه می‌گیرند که اگر حملات سایبری با تلفات جانی و مادی همراه باشد، قربانی حمله می‌تواند با استناد به ماده ۵۱ منشور ملل متحد، حق دفاع مشروع را در برابر مهاجم بکار گیرد. مقاله خلف رضایی (۱۳۹۲) نیز در این حوزه نگاشته شده است. در نوشتار دیگری جورج لوکاس (Lucas,2014) اظهار می‌دارد که هدف‌شناسی و اختصاصی بودن کرم استاکس‌نت از جهت ضربه زدن به سانتریفیوژ، پیش‌ازاین هرگز در قالب یک سلاح امکان‌پذیر نبود. همچنین او به این موضوع اشاره می‌کند که در شرایط حمله استاکس نظریات خردگرا و بازدارندگی کاربرد خود را از دست می‌دهند.

در اثر دیگری، پاول کر و همکاران (Kerr, Rollins and Theohary,2010) به ابعاد امنیت بین‌الملل موضوع اشاره می‌کند و اذعان می‌کنند که پیدایش و استفاده از کرم موسوم به استاکس نت یک مخاطره بزرگ برای ساختارهای حیاتی یک کشور محسوب می‌شود. ایشان نتیجه می‌گیرند که حمله مشابه استاکس نت در صورت اتفاق در ایالات‌متحده، توانایی از کاراندازی طولانی‌مدت زیرساخت‌های دولتی و به دنبال آن کاهش قدرت عمومی را به دنبال خواهد داشت. الکساندر ون دائن (Van Dine,2011) نیز ظهور استاکس‌نت به‌عنوان سلاحی با تاثیرات فیزیکی مخرب بر روی تأسیسات هسته‌ای را به‌عنوان زنگ هشداری برای دولت‌های دیگر در خصوص ریسک و تلفات حملات سایبری به زیرساخت‌های حساس متصور می‌شود. بروس شنیر (Creators,2013) از بعد فنی به بررسی داده‌های حاصل از مهندسی معکوس کدهای مخرب استاکس‌نت می‌پردازد و با اشاره به برنامه هسته‌ای ایران در بین سال‌های ۲۰۰۸ و ۲۰۰۹، استدلال می‌کند که موضوع از امنیت دولتی فراتر بوده و امنیت بین‌المللی را تحت‌الشعاع قرار می‌دهد.

در مقاله حاضر، با نگاهی به آثار فوق و با بهره‌گیری از چهارچوب نظری امنیت سایبری، تقابلات سایبری میان ایران و اسرائیل در پسِ حمله استاکس‌نت بررسی شده است.

۱. چهارچوب نظری: امنیت سایبری

به‌طورکلی مطالعات امنیتی پساجنگ سرد دربرگیرنده دو رویکرد متمایز است: سنت‌گرایان و بازاندیشان. سنت‌گرایان تحت تأثیر فضای جنگ سرد، موضوع‌هایی همچون حاکمیت دولت، قدرت نظامی و ژئوپلیتیک را در اولویت قرار می‌دهند. این دیدگاه بر دولت به‌عنوان بازیگر اصلی در یک نظام بین‌الملل آنارشیک تأکید می‌کند، جایی که امنیت عمدتاً از طریق قدرت نظامی و اتحادهای استراتژیک به دست می‌آید. در مقابل، بازاندیشان یا رویکرد موسع و تعمیق‌گرا به امنیت، بر مفاهیم تکامل‌یافته‌تر از امنیت سنتی یعنی ثبات اقتصادی، پایداری زیست‌محیطی، رفاه اجتماعی و حقوق بشر تأکید می‌کند. به سخن دیگر، درحالی‌که سنت‌گرایان، امنیت را از دریچه سیاست قدرت و منافع ملی می‌بینند، رهیافت موسع و تعمیق‌گرا، وابستگی متقابل جهانی و پیوند ذاتی بین رفاه فردی و صلح بین‌المللی را در اولویت قرار می‌دهد. تفاوت بین این رویکردها نه‌تنها در تعریف آن‌ها از تهدیدها بلکه در راه‌حل‌های تجویزشده آن‌ها نهفته است؛ جایی که سنت‌گرایان از بازدارندگی و دفاع نظامی حمایت می‌کنند، طرفداران دیدگاه موسع و تعمیق گرا خواستار شکل‌دهی به چارچوب‌های همکاری و یکپارچگی سیاست‌ها در بخش‌های مختلف هستند (Buzan and Hansen,2009:4-7).

فضای سایبر به‌عنوان بستر فعالیت انسان‌ها نیز در دهه‌های اخیر در دایره شمولیت امنیت بین‌الملل قرار گرفته است. بر این اساس، دو دیدگاه فوق به مشخص کردن جایگاه و وزن آن پرداخته‌اند. از دیدگاه سنت‌گرایان، امنیت سایبری اغلب در چارچوب جنگ سایبری قرار می‌گیرد که بر اساس آن، نقش دولت در دفاع در برابر تهدیدات سایبری نشأت‌گرفته از سوی سایر دولت‌ها یا بازیگران تحت حمایت دولت دیگر برجسته می‌شود. این رویکرد قابلیت‌های دفاع سایبری ملی، توسعه استراتژی‌های جنگ سایبری تهاجمی و حفاظت از زیرساخت‌های حیاتی را در اولویت قرار می‌دهد. در این قلمرو، فضای سایبری به‌عنوان حوزه دیگری از جنگ در نظر گرفته می‌شود که در آن کشورها برای تسلط رقابت می‌کنند و امنیت از طریق بازدارندگی و اقدامات متقابل در برابر متجاوزان بالقوه حاصل می‌شود.

در مقابل، رهیافت موسع و تعمیق‌گرا به امنیت حامی رویکردی جامع‌تر به موضوع امنیت سایبری است. با اذعان به اینکه تهدیدات سایبری به مرزهای ملی احترام نمی‌گذارند و

می‌توانند از بازیگران غیردولتی، ازجمله تروریست‌ها، هکرها و سازمان‌های جنایی فراملی سرچشمه بگیرند، این دیدگاه بر پیوستگی شبکه‌های جهانی و نیاز به همکاری بین‌المللی، مشارکت عمومی- خصوصی و مدل‌های حکمرانی چندجانبه برای پرداختن به ماهیت چندوجهی تهدیدات سایبری پای می‌فشارد. این مفهوم‌سازی، امنیت را گسترش می‌دهد تا حفاظت از حریم خصوصی افراد، ثبات اقتصادی و اعتماد اجتماعی در سیستم‌های دیجیتال را هم شامل شود. از این منظر، امنیت سایبری صرفاً به‌منظور جلوگیری از جنگ سایبری نیست، بلکه به‌منظور تضمین انعطاف‌پذیری جوامع در برابر تهدیدات سایبری است که می‌تواند حقوق بشر، توسعه اقتصادی و صلح جهانی را تضعیف کند (Kivimaa, Paula,et al.,2022:2-3).

به‌طور خلاصه، درحالی‌که رویکرد سنت‌گرا به امنیت سایبری بر اقدام‌های دولت‌محور و نظامی‌سازی فضای سایبری برای مقابله با جنگ سایبری متمرکز است، در مقابل چشم‌انداز موسع و تعمیق‌گرا به امنیت خواستار چارچوبی جامع و مشارکتی است که فراتر از مرزهای ملی و شامل طیف گسترده‌تری از بازیگران است. این واگرایی منعکس‌کننده بحث گسترده‌تری در مطالعات امنیتی بین حفظ اولویت دولت - ملت و تصدیق ماهیت فراملی فزاینده چالش‌های امنیتی معاصر است.

به‌منظور انضمامی کردن امنیت سایبری ضروری است مفاهیم و تعاریف موجود در این قلمرو بررسی شوند. با کاوش در این مفاهیم،

ماهیت چندوجهی مخاطرات سایبری آشکار می‌شود. جاسوسی، جنگ و تروریسم سایبری سه مفهوم مهم در قلمرو امنیت سایبری هستند که شایسته توجه بسیارند.

جاسوسی سایبری ناظر به استفاده از تاکتیک‌های سایبری برای نفوذ به سیستم‌های دیجیتال به‌منظور جمع‌آوری اطلاعات حساس، طبقه‌بندی‌شده یا اختصاصی است. برخلاف جرائم سایبری که غالباً انگیزه مالی دارد یا جنگ سایبری که به دنبال واردکردن آسیب است، اهداف جاسوسی سایبری چندوجهی است و می‌تواند از دستیابی به برنامه‌های نظامی، ارتباطات دولتی و جزئیات زیرساخت‌های حیاتی گرفته تا سرقت اسرار تجاری و مالکیت معنوی از شرکت‌ها را در برگیرد. هدف نهایی جاسوسی سایبری، ارتقای موقعیت استراتژیک و توانایی‌های تصمیم‌گیری مهاجم است که اغلب به بهای از دست دادن امنیت ملی، ثبات اقتصادی یا موقعیت رقابتی آماج انجام می‌شود. کارشناسان این حوزه، پیامدهای جاسوسی سایبری را

بسیار عمیق می‌دانند، زیرا این دست حملات می‌تواند تنش بین دولت‌ها را به‌شدت افزایش دهد و اقدامات تلافی‌جویانه را در فضای مجازی و فراتر از آن تشدید کند.

اما تروریسم سایبری از گستره وسیع و به‌هم‌پیوسته فضای سایبری برای انجام فعالیت‌های تروریستی سوءاستفاده می‌کند. این شکل مدرن تروریسم از فناوری دیجیتال برای نقض، مختل کردن یا دست‌کاری سیستم‌های الکترونیک با هدف آسیب رساندن، ایجاد رعب و ترس یا دستیابی به اهداف ایدئولوژیک، مذهبی یا سیاسی استفاده می‌کند. تروریسم سایبری چالش‌های منحصربه‌فردی را برای سازمان‌های امنیتی که وظیفه حفاظت از امنیت عمومی و ملی بر عهده‌دارند، ایجاد می‌کند. تروریسم سایبری از هک کردن و تخریب وب‌سایت‌ها تا راه‌اندازی حملات سایبری پیچیده علیه زیرساخت‌های حیاتی مانند شبکه‌های برق، سیستم‌های مالی یا شبکه‌های دولتی را شامل می‌شود. هدف این اقدام‌ها نه‌تنها اعمال آسیب مستقیم، بلکه تضعیف اعتماد عمومی به توانایی دولت برای محافظت از شهروندان است. سازمان‌های امنیتی در مبارزه با تروریسم سایبری با چالش‌های مهمی ازجمله نیاز به قابلیت‌های فنی پیشرفته برای شناسایی و کاهش تهدیدات، دشواری انتساب و نیاز به سازوکارهای واکنش سریع مواجه هستند (Weimann,2006).

در مقایسه با جاسوسی و تروریسم سایبری، جنگ سایبری از اهمیت بیشتری برخوردار است، زیرا جنگ سایبری نمایانگر یک مرز مدرن در عملیات استراتژیک کشورهاست؛ جایی که قلمرو دیجیتال به میدان نبرد برای دستیابی به اهداف نظامی، سیاسی و استراتژیک تبدیل شده است. این تحول در جنگ، منعکس‌کننده ماهیت در حال تغییر در قرن بیست و یکم است، جایی که نیروی فیزیکی با حملات دیجیتالی باهدف مختل کردن، تخریب یا نابود کردن قابلیت‌های دشمن بدون شلیک حتی یک گلوله انجام می‌شود.

جنگ سایبری شامل اقدام‌هایی است که توسط دولت‌ها از طریق فضای سایبری انجام می‌شود و هدف آن آسیب رساندن یا وادار کردن سایر کشورها یا گروه‌ها برای دستیابی به اهداف استراتژیک ملی است. این موضوع می‌تواند شامل حمله به زیرساخت‌های حیاتی، عملیات جاسوسی برای سرقت اطلاعات حساس نظامی یا تلاش‌های خرابکارانه‌ای باشد که به‌منظور برهم زدن قابلیت‌ها و توانایی‌های نظامی دشمن طراحی‌شده‌اند (خلیلی‌پور رکن‌آبادی و نورعلی وند، ۱۳۹۱: ۱۷۲-۱۷۱).

استراتژی نظامی مدرن، به‌طور فزاینده‌ای جنگ سایبری را به‌عنوان یک جزء مهم دفاع ملی و عملیات تهاجمی تلقی می‌کند. ادغام عملیات سایبری در استراتژی نظامی امکان ایجاد بعد جدیدی از جنگ را فراهم می‌کند که کمتر قابل مشاهده است اما می‌تواند عمیقاً بر ابعاد مختلفی از ثبات یک کشور تأثیر بگذارد. حمله کرم استاکس نت در سال ۲۰۱۰ به برنامه هسته‌ای ایران را می‌توان به‌عنوان یک جنگ سایبری تلقی کرد. استقرار استاکس نت پیامدهای عمیقی بر هنجارهای جنگ سایبری داشت. این موضوع پتانسیل عملیات سایبری برای دستیابی به اهداف نظامی استراتژیک را نشان داد و به‌طور مؤثر مانند زرادخانه‌ای در دست اسرائیل برای اعمال قدرت عمل کرد.

۲. جنگ سایبری به‌مثابه یک استراتژی و ابزار بازدارنده برای اسرائیل

موانع موجود بر سر همکاری در آسیای غربی که از دیرباز درگیری‌های قومی، قبیله‌ای، دینی و ایدئولوژیک را به همراه داشته است در کنار فقدان عمق استراتژیک و آسیب‌پذیری‌های ناشی از عدم تقارن عناصر قدرت ملی اسرائیل در برابر همسایگان عرب و دشمنانش باعث شده که دکترین دفاعی این کشور به سمت دوری از جنگ به شیوه کلاسیک به سمت بهره‌برداری از ابزارهای نامتعارف بازدارندگی حرکت کند. بر اساس اسناد رسمی منتشرشده توسط این کشور به نظر می‌رسد در دهه اخیر و بعد از تجربه جنگ‌های کلاسیک، راهبرد دفاعی آن با بازتعریف ابزارهای بازدارندگی امنیتی و دفاعی همراه بوده و سرمایه‌گذاری هدفمندی در توسعه توانمندی‌های بازدارندگی سایبری دنبال شده است.

بر اساس اسناد رسمی موجود، کشورهای ایران، لبنان، سوریه و بازیگران غیردولتی نظیر حزب‌الله، حماس، جهاد اسلامی و نظایر آن، در زمره تهدیدات پیش روی اسرائیل قرار می‌گیرند. افزون بر این موارد، احتمال درگیری شامل گسترش تسلیحات کشتارجمعی و تسلیحات تهاجمی راهبردی مانند موشک‌های بالستیک و تهدیدات فضای سایبر رو به افزایش و قابل‌توجه است. موارد یادشده در دکترین راهبردی نوین آیزنکوت، ژنرال اسرائیلی، نشان از تغییر در رویکرد نظامی و دفاعی این کشور و گذار از اسرائیل تهاجمی به اسرائیل دفاعی با قابلیت‌های تهاجمی پنهان هدایت کرده است (حبیبی، یوسفی و رودباری، ۱۴۰۰: ۳۰). در فصل پنجم سند راهبردی

نظامی اسرائیل تأکید بر حفظ نیروی نظامی کارآمد به چشم می‌خورد، بااین‌حال افزایش توانمندی سایبری به‌عنوان ابزاری مهم در حوزه دفاعی اسرائیل مورد تأکید است (INSS,2016:2). مقام‌های اسرائیلی مترصد تبدیل کشور خود به ابرقدرت سایبری در منطقه و جهان هستند، زیرا ایشان همواره خود را قربانی حملات سایبری با منشأ نامشخص دولتی تصور می‌کنند و انگشت اتهام خود را به سمت ایران گرفته‌اند (ToI Staff,2020).

با توجه به بینش بنیان‌گذاران و سران اسرائیل، این رژیم همواره خود را در بن‌بست استراتژیک بین کشورهای عربی دیده و تمرکز خود را بر اتکا به خود و توانمندی‌های داخلی گذاشته است تا در محیط آنارشیک خاورمیانه به موجودیت خود ادامه دهد. بر همین اساس با تشویق ایده‌های نو در زمینه‌های سایبری یک اکوسیستم کامل در خصوص فناوری سایبری را در خود شکل داده است. مهاجران یهودی از کشورهای پیشرو در فناوری سایبری به این سرزمین اشغالی مهاجرت کردند و به دیاسپورای متخصص این حوزه شکل دادند. این امر سبب پیشرفت چشمگیر اسرائیل در فضای سایبر شد. بااین‌حال با توجه به این موضوع که تقریباً تمام ساکنان سرزمین‌های اشغالی عضو ارتش یا نیروی دفاعی اسرائیل هستند، با انتقال این مهارت‌ها به فضای نظامی و استراتژیک به پیشبرد هر چه بیشتر دکترین دفاعی نوین کشور اسرائیل کمک کرده‌اند. یگان‌هایی نظیر تالپیوت و ۸۲۰۰ در ارتش، در موضوع‌های سایبری پیش‌رو محسوب می‌شوند (Times of Israel,2017). با توجه به این امر که عمده تمرکز اسرائیل در دکترین نظامی دفاعی خود بر بازدارندگی است می‌بایست از این نظر به موضوع سایبری نیز نگاه شود، زیرا نظریه امنیت سنتی قابلیت کاربرد در عرصه سایبری را نیز دارد. برخی از اندیشمندان با به کار بستن مفروضات بازدارندگی سنتی، چارچوبی جدید از بازدارندگی سایبری مطرح کرده‌اند (Bendiek and Metzger,2015:553-567).

مبتنی بر چارچوب سنتی، دو رویکرد اساسی در بازدارندگی سایبری تعریف می‌شود که شامل انکار و مجازات مهاجم است که حمله استاکس نت در راستای شیوه دوم قابل گنجاندن است. روش انکار با توجه به این نگاه که تلافی در سطح فنی بالاتر از حمله اولیه بسیار دشوار و چالش‌برانگیز است، همواره مطلوب قلمداد شده و بر این اصل استوار است که اگر حملات سایبری با معافیت از مجازات و پیگرد باشد، مهاجم بهانه ناچیزی برای متوقف کردن دارد. درواقع باید مهاجم را متقاعد کرد که حمله و نفوذ هیچ‌گونه دستاوردی متناسب با هزینه کرد

خود نداشته است. در روش دیگر که مبتنی بر مجازات است می‌بایست این‌گونه تحلیل کرد که اگر تهدید به‌تلافی در ذهن دشمن مؤثر تلقی شود؛ به‌گونه‌ای که تغییر در رویکرد آن حاصل شود، بازدارندگی مؤثر بوده است، زیرا اگر قربانی مهارت کافی برای پاسخ به قابلیت‌های فنی به‌کاربرده‌شده را نداشته باشد احتمالاً گرفتار خواهد شد (Bendiek and Metzger, 2015:553-567). نتیجه اینکه با توجه به این موضوع که اسرائیل تنها کشوری است که همسایگان عرب آن موجودیت کشور را تهدید کرده‌اند باوجود برتری نظامی از گذشته تابه‌حال بر اساس دکترین دفاعی خود جنگ را گزینه‌ای ناگزیر از انتخاب می‌داند و همواره به دنبال بازدارندگی چه از نوع هسته‌ای و چه از نوع سایبری رفته است. با نگاهی به سیر تحول رویدادهای محرک داخلی اسرائیل تأثیر حمله استاکس‌نت بر روند تغییر دکترین دفاعی کشور از تهاجم به دفاع و راهبردهای غیرمتعارف مشخص است.

دفاع سایبری و عملیات دفاعی دو بال استراتژی امنیت ملی اسرائیل هستند که متشکل از واحد ۸۲۰۰ ارتش که نام آن ذکر شد، برای عملیات آفندی و اداره سی‌فورآی[1] مخصوص عملیات پدافندی و زیرساختی است. البته نباید فراموش کرد که موساد، شاباک و شین‌بت نیز توانایی‌های بسیاری در این زمینه دارند که به‌واسطه محرمانگی اطلاعات قابل کنکاش نیستند. بنا بر اطلاعات منتشر شده، واحد موسوم به ۸۲۰۰ ارتش اسرائیل شامل نخبگان حوزه تکنولوژیک است و تاکنون به تعداد بسیاری عملیات موفق دست یافته است. ساخت استاکس نت به این واحد نسبت داده می‌شود. ویروس شعله به‌عنوان نسخه تکامل‌یافته استاکس نت نیز با هدف جمع‌آوری اطلاعات سایبری از کشورهای ایران، سوریه و فلسطین محصول دیگر این نهاد است. بدافزارهای دی‌یوکیویو[2] و جی‌ای‌یواس‌اس[3] که مؤثر بر سیستم بانکی هستند نیز به‌طور غیررسمی به واحد ۸۲۰۰ نسبت داده می‌شود.

در نوامبر ۲۰۱۰، بنیامین نتانیاهو، نخست‌وزیر اسرائیل، رسماً از یک کارگروه ویژه برای ارائه توصیه‌هایی برای استراتژی ملی سایبری که به‌عنوان ابتکار سایبری نیز شناخته می‌شد، نام برد. این گروه متشکل از ده‌ها کارشناس به سرپرستی اسحاق بن اسرائیل، استاد دانشگاه

---

1. C4I
2. DUQU
3. GAUSS

تل‌آویو، بود که برای چندین ماه در هشت کمیته فرعی فعالیت کرد. گروه مزبور تمام مؤلفه‌های حیاتی برای نیاز دولت اسرائیل برای مقابله موفقیت‌آمیز در فضای سایبری، ازجمله تجزیه‌وتحلیل منافع ملی در رابطه با جنبه‌های اقتصادی، آکادمی و امنیت ملی را بررسی کرد. تحقیقات کارگروه ابتکار سایبری در می ۲۰۱۱ به پایان رسید و نتیجه بررسی‌ها در گزارش ویژه‌ای به نخست‌وزیر ارسال شد.

کارگروه ویژه توصیه کرد که دو نهاد اعم از دفتر ملی سایبری و سازمان اجرایی برای امنیت ایجاد شود. همچنین مقرر شد بنا بر نظر این گروه یک سامانه دفاع سایبری ملی و یک مرکز واکنش اضطراری رایانه‌ای ملی[1] تأسیس شود. پس‌ازآن، در اوت ۲۰۱۱، دولت اسرائیل قطعنامه‌ای برای تأسیس دفتر ملی سایبری اسرائیل[2] تصویب کرد که برای کمک به نخست‌وزیر، دولت و کمیته‌های آن در ایجاد یک سیاست ملی سایبری و تقویت کاربرد جنبه‌های ملی آن تعیین شده بود. دفتر ملی سایبری به‌طور ویژه مأموریت یافت تا یک استراتژی امنیت سایبری ملی را توسعه دهد. درنهایت با تصمیم دولت مبنی بر ایجاد یک نهاد غیرنظامی در دفتر نخست‌وزیری به نام سازمان ملی امنیت سایبری[3] این امر محقق شد.

در فوریه ۲۰۱۵، سی و سومین دولت اسرائیل دو قطعنامه دولتی در مورد دفاع سایبری با محوریت قطعنامه ۲۴۴۴ دولت، در راستای ارتقای آمادگی ملی برای دفاع سایبری تصویب کرد. در این قطعنامه، دفاع از عملکرد صحیح در فضای مجازی یک هدف حیاتی، ملی و یکی از منافع ملی حیاتی کشور اسرائیل تلقی شد. همچنین مقرر شد که هدف سازمان ملی امنیت سایبری حفاظت از کل فضای سایبری غیرنظامی اسرائیل باشد. در این راستا، سازمان ملی امنیت سایبری فعالیت خود را از اوایل سال ۲۰۱۶ با معرفی بوکی کارملی[4] به‌عنوان مدیر آغاز کرد. کارملی پس از ۲۰ سال خدمت در واحد سایبری ۸۲۰۰ ارتش به این سمت رسیده بود. مطابق با آمارهای ارائه‌شده، سازمان ملی امنیت سایبری رهبری ملی مقابله با ده‌ها تهدید

1. computer emergency response team
2. Israel National Cyber Directorate
3. National Cyber Security Authority
4. Buky Carmeli

سایبری ازجمله باج افزارهای واناکرای[1]، ناتپتیا[2]، سی‌سی‌کلینر[3] و بدربیت[4] را بر عهده داشته است. از مارس ۲۰۱۷، سازمان ملی امنیت سایبری مسئولیت هدایت سازمان‌های ملی الکترونیک، مانند شرکت الکتریک اسرائیل و راه‌آهن اسرائیل، برای مقابله با خطرات سایبری را بر عهده گرفت. علاوه بر این، سازمان ملی امنیت سایبری در اوایل سال ۲۰۱۷ دستورالعمل دفاع سایبری سازمانی را منتشر کرد که بر اساس آن به هر سازمانی در اسرائیل، چه بزرگ و چه کوچک، ابزارهایی برای مدیریت و بهینه‌سازی جهت دفاع از خود در برابر تهدیدات سایبری ارائه می‌داد و به آن‌ها در طراحی یک برنامه کاری منظم کمک می‌کرد.

۳. جنگ سایبری اسرائیل علیه ایران: مورد برنامه هسته‌ای

جهش ایران به سمت توانمندی هسته‌ای در دهه ۱۹۵۰ تحت برنامه اتم برای صلح آغاز شد و شاه ایران انرژی هسته‌ای را به‌عنوان سنگ بنای مدرن‌سازی و قدرت ارزیابی می‌کرد. بااین‌حال، پس از انقلاب اسلامی، این برنامه با اتکا به اصل بومی‌سازی و خوداتکایی چرخشی پنهانی پیدا کرد و ابهام‌هایی درباره نیات ایران در مورد سلاح هسته‌ای پدید آورد (Waltz,2003). افشای پیشرفت هسته‌ای ایران در اوایل سال ۲۰۰۲ ناظر به تأسیسات نطنز و اراک و نیز کشف سایت اعلام‌نشده فوردو در سال ۲۰۰۹ نگرانی‌های بین‌المللی در باب برنامه هسته‌ای ایران را تشدید کرد؛ به‌نحوی‌که شدیدترین تحریم‌های ملل متحد در ۲۰۱۰ علیه ایران را رقم زد.

اما این تحریم‌ها که دامنه وسیعی را در برمی‌گرفت و با هدف توقف برنامه هسته‌ای ایران انجام شده بود، بر عزم ایران در توسعه برنامه هسته‌ای چندان اثرگذار نبود و ایران در همین سال اعلام کرد که به اورانیوم ۱۹.۸ درصد دست یافته است. این امر سبب واکنش‌های تدریجی تقابلی با ایران به‌ویژه از سوی بازیگران منطقه‌ای ازجمله اسرائیل شد. در مرحله اولیه، اسرائیل بر افزایش آگاهی بین‌المللی در مورد تهدید بالقوه ناشی از برنامه هسته‌ای ایران تمرکز کرد. برخی بر این باورند عمومی‌سازی برنامه هسته‌ای ایران در ۲۰۰۲ نیز به‌واسطه اطلاعات اسرائیل

1. WannaCry
2. NotPetya
3. CCleaner
4. Bad Rabbit

انجام شده بود (Ansari,2006:198). عناصر اثرگذار شامل رهبران اسرائیل، به‌ویژه بنیامین نتانیاهو مکرراً در مجامع بین‌المللی نظیر مجمع عمومی سازمان ملل سخنرانی کردند تا خطرات ایران مجهز به سلاح هسته‌ای را برجسته کنند. همچنین اسرائیل روابط خود را با متحدان راهبردی به‌ویژه ایالات‌متحده تقویت کرد تا از رویکردی هماهنگ در خصوص ایران اطمینان حاصل کند. این همکاری‌ها شامل به اشتراک‌گذاری اطلاعات و لابی برای یک موضع واحد در برابر برنامه هسته‌ای ایران بود.

در خلال سال‌های ۲۰۰۶ الی ۲۰۱۵ و با پیشرفت برنامه هسته‌ای ایران، استراتژی اسرائیل به سمت حمایت از تحریم‌های شدید بین‌المللی تغییر کرد. اسرائیل نقش مهمی در لابی کردن جهت صدور قطعنامه‌های شورای امنیت سازمان ملل متحد برای اعمال تحریم‌های اقتصادی علیه ایران، هدف قرار دادن صادرات نفت و بخش مالی آن داشت (Kaye,2016). همکاری نزدیک با کشورهای اروپایی منجر به تحریم‌های بیشتر و فشار اقتصادی و دیپلماتیک بر ایران شد. مقام‌های اسرائیلی بر استفاده از ظرفیت تریبون‌های عمومی برای تأکید بر عدم پایبندی ایران به توافق‌های هسته‌ای بین‌المللی و تهدیدات بالقوه امنیتی منطقه‌ای و جهانی پافشاری داشتند و از ظرفیت دیپلماسی عمومی در این موضوع بهره گرفتند (Arad,2023).

علاوه بر اقدام‌های فوق و البته حذف فیزیکی افراد مرتبط با برنامه هسته‌ای ایران، اسرائیل در راستای اسناد استراتژیک خود به حوزه سایبری نیز وارد شد. گزارش‌ها حاکی از آن است که قبل از حمله سایبری، چند عملیات مخفی برای تسهیل ورود کرم به تأسیسات هسته‌ای ایران انجام شده بود. این امر نشان از ادغام استراتژیک قابلیت‌های سایبری با روش‌های جاسوسی سنتی برای دستیابی به اهداف امنیت ملی اسرائیل دارد (Lindsay,2013). درنهایت، در ژوئن ۲۰۱۰ کرم کامپیوتری استاکس‌نت، در رایانه‌های نیروگاه اتمی شناسایی شد (Nakashima and Warrick,2012). این ویروس سپس به سایر تأسیسات سرایت کرد. طبق گزارش‌ها تا سپتامبر ۲۰۱۰، سی هزار رایانه در حداقل ۱۴ تأسیسات (Kushner,2013) ازجمله تأسیسات نطنز، آلوده شده بودند (Sanger,2010). عملکرد ویروس بدین‌صورت بود که ابتدا موتورهای سانتریفیوژهای IR-1 سرعت خود را افزایش دادند و درنهایت منفجر شدند. موسسه علوم و امنیت بین‌الملل در آن زمان تخمین زد که حداقل هزار سانتریفیوژ از نه هزار سانتریفیوژ نصب‌شده در نطنز منهدم شده است. ایران پس از انجام تحقیقات، اسرائیل و آمریکا

را مقصر این حمله اعلام کرد (CBS,2011). علی‌اکبر صالحی، رئیس وقت سازمان انرژی اتمی ایران نیز اعلام کرد که ازآنجایی‌که سیستم‌های کنترل نطنز به اینترنت متصل نیستند، استاکس نت باید با یک درایو قابل جابجایی از یک کامپیوتر آلوده به سیستم کنترل نطنز وارد شده باشد. آژانس بین‌المللی انرژی اتمی نیز در گزارش خود در ۲۲ دسامبر ۲۰۱۰ داده‌هایی منتشر کرد مبنی بر اینکه استاکس نت حدود هزار سانتریفیوژ IR-1 را در کارخانه غنی‌سازی سوخت نطنز منهدم کرده است. آژانس این نتیجه‌گیری را بر اساس گزارش ایران مبنی بر از رده خارج کردن هزار سانتریفیوژ از تأسیسات نطنز ارائه داده بود.

بار دیگر در آوریل ۲۰۱۱ سازمان دفاع سایبری ایران از ویروسی با نام مستعار ستاره‌ها[1] نام برد و اعلام کرد که برای نفوذ و آسیب رساندن به تأسیسات هسته‌ای کشور طراحی شده است (Yong,2011). به گفته غلامرضا جلالی، رئیس سازمان پدافند غیرعامل ایران، این ویروس از فایل‌های رسمی دولتی تقلید کرده و به سیستم‌های رایانه‌ای آسیب جزئی وارد کرده است (CBS,2011). ایران، این بار هم آمریکا و اسرائیل را مقصر دانست (Rashid,2011). همچنین در ۱۳ نوامبر ۲۰۱۱ ایران اعلام کرد که بدافزار دوکو[2]، سومین ویروسی که هدف آن مختل کردن برنامه هسته‌ای ایران بوده مورد شناسایی قرار گرفته است (Hounshell,2011). این ویروس از کد برنامه‌نویسی استفاده کرده بود که مشابه آن، در حمله استاکس نت در سال ۲۰۱۰ نیز تجربه شده بود (Fox News,2011).

در آوریل ۲۰۱۲ ایران بدافزار وایپر[3] را کشف کرد که دیسک‌های سخت رایانه‌های متعلق به وزارت نفت و شرکت ملی نفت ایران را پاک می‌کرد (Zetter,2012). وایپر نیز ازنظر طراحی شبیه به دوکو و استاکس نت بود که تصور می‌شود توسط اسرائیل و ایالات‌متحده ساخته شده است. (Mills,2012). همچنین در ۹ می ۲۰۱۲ ایران اعلام کرد که ویروسی به نام شعله[4] کامپیوترهای دولتی را آلوده کرده و سعی کرده است اطلاعات دولتی را به سرقت ببرد (Nakashima,2012). واشنگتن‌پست گزارش داد که اسرائیل و ایالات‌متحده ویروس شعله را

---

1. stars
2. duqu
3. Wiper
4. Flame

برای جمع‌آوری اطلاعات و آماده شدن برای یک کارزار جنگ سایبری گسترده‌تر به کار گرفته‌اند (Nakashima, Miller and Tate,2012). در اسرائیل، موشه یعلون، معاون نخست‌وزیر، دخالت این کشور را تأیید نکرد اما اذعان کرد که اسرائیل از همه ابزارها برای آسیب رساندن به برنامه هسته‌ای ایران استفاده خواهد کرد (Nakashima,2012). وقوع این رخدادها همگی پیش از توافق هسته‌ای ایران با کشورهای ۵+۱ بود؛ اما این حوادث پس از انعقاد این توافق متوقف شد تا این‌که چند ماه پس از خروج آمریکا از برجام، این اقدام‌ها از سر گرفته شد.

در ۲۸ اکتبر ۲۰۱۸ رئیس سازمان پدافند غیرعامل ایران مدعی شد که نسل جدید ویروس استاکس نت را که تلاش می‌کرد به زیرساخت‌های ارتباطی آسیب برساند، خنثی کرده است (Reuters,2018). در ۹ می ۲۰۲۰ نیز رایانه‌هایی که ترافیک دریایی را در بندر شهید رجایی در سواحل جنوبی ایران در خلیج‌فارس تنظیم می‌کنند، موردحمله قرار گرفت. این اختلال باعث ایجاد ترافیک کشتی‌هایی شد که روزها منتظر بودند تا پهلو بگیرند. ایران اذعان کرد که موردحمله سایبری قرار گرفته است. بنا به گزارش واشنگتن‌پست، اسرائیل در پشت این حمله سایبری قرار داشت، اگرچه این کشور مسئولیت آن را بر عهده نگرفت (Warrick and Nakashima,2020 a). در ۲ جولای ۲۰۲۰ انفجاری به سایت اصلی غنی‌سازی هسته‌ای ایران در نطنز آسیب زیادی وارد کرد و این برنامه را ماه‌ها به عقب انداخت. این انفجار به کارخانه تولید سانتریفیوژهای پیشرفته IR-4 و IR-6 آسیب زد. نیویورک‌تایمز و واشنگتن‌پست گزارش دادند که اسرائیل بمبی در این تأسیسات کار گذاشته است (Warrick, Mekhennet and Hendrix,2020 a).

لازم به ذکر است که اقدام‌های سایبری اسرائیل علیه ایران به برنامه هسته‌ای محدود نشده است. در روزهای ۹ و ۱۰ ژوئن ۲۰۲۱ هکرها با ارسال پیام‌های جعلی در روی تابلوهای نمایش ایستگاه‌های قطار در سراسر کشور هرج‌ومرج ایجاد کردند (The Guardian, 2021). در این پیام‌ها از مسافران خواسته شده است که با شماره تلفن دفتر مقام معظم رهبری تماس بگیرند. همچنین وب‌سایت‌های مرتبط با وزارت راه و شهرسازی از کار افتادند (Reuters,2021). علاوه بر این، در ۲۶ اکتبر ۲۰۲۱ طی حمله سایبری دیگری، سیستم

سوخت‌رسان و کارت سوخت موردحمله قرار گرفت. این قطعی تمام ۴۳۰۰ پمپ‌بنزین در ایران را تحت تأثیر قرار داد (AP, 2021).

نبرد سایبری بین ایران و اسرائیل در آوریل ۲۰۲۱ شدت گرفت، زیرا گمان می‌رفت اسرائیل در پشت یک حمله سایبری قرار داشته باشد که باعث خاموشی گسترده در مجتمع غنی‌سازی نطنز شد (Fassihi, Pérez-Peña and Bergman,2020). بنا بر گزارش‌ها، این حمله، سیستم برقی را که سانتریفیوژهای تأسیسات را راه‌اندازی می‌کرد، از بین برد و گفته می‌شد غنی‌سازی ایران در نطنز را نه ماه عقب انداخته است. این حادثه اندکی پس از اعلام ایران از نصب سانتریفیوژهای پیشرفته جدید در نطنز و پس از آغاز غنی‌سازی اورانیوم تا ۶۰ درصد توسط ایران رخ داد (O'Grady,2021). در زمان حمله، ایران و ایالات‌متحده به‌تازگی وارد مذاکره شده بودند تا پایبندی خود به برجام را بازگردانند. این حمله از تمایل اسرائیل برای در دست گرفتن امور در صورت نارضایتی از جهت‌گیری تلاش‌های دیپلماتیک برای حل‌وفصل برنامه هسته‌ای ایران حکایت داشت.

۴. تقابلات سایبری ایران با اسرائیل پس از حمله استاکس‌نت

برای اولین بار در سال ۲۰۰۷ پس از تأسیس مرکز مطالعات جرائم سازمان‌یافته توسط سپاه پاسداران انقلاب اسلامی، ایران ظهور عملیات با منشأ دولتی علیه دشمن خارجی تجربه کرد. تا سال ۲۰۰۹، سپاه پاسداران شروع به استخدام گسترده متخصصین سایبری در یک واحد نظامی موسوم به ارتش سایبری ایران کرد. سردار حسین همدانی در سال ۲۰۱۰ اعلام کرد که شورای سایبری بسیج به‌عنوان یک نهاد سایبری تحت مجموعه سپاه پاسداران با ظرفیت ۱۵۰۰ متخصص امنیت سایبری برای به‌کارگیری در بخشی از حملات تهاجمی و جمع‌آوری اطلاعات فضای مجازی به‌کارگیری شده‌اند.

ایران در پاسخ به حمله استاکس‌نت به تقویت زیرساخت‌های امنیت سایبری، تأسیس ارتش سایبری و بازنگری و سرمایه‌گذاری در قابلیت‌های سایبری دفاعی و تهاجمی خود پرداخت. رویکرد ایران برای کاهش پیامدهای استاکس‌نت دارای ابعاد دیپلماتیک نیز بود، زیرا تلاش کرد تا مخالفت‌های بین‌المللی را نسبت به آنچه به‌عنوان یک اقدام تروریستی سایبری معرفی

می‌کرد، متمرکز کند. تلاش‌های ایران برای برجسته کردن خطرات جنگ سایبری هم با هدف تأمین همدلی بین‌المللی و هم توجیه ابتکارات سایبری خود بود (Lindsay,2013). ارزیابی جامع ایران از حمله استاکس‌نت، راه را برای توسعه یک استراتژی ملی سایبری هموار کرد. کانون اصلی این استراتژی، به رسمیت شناختن فضای سایبری به‌عنوان یک حوزه جنگ بود که ادغام عملیات سایبری در دکترین کلی نظامی ایران را ضروری می‌ساخت. این استراتژی شامل مؤلفه‌های مختلفی ازجمله حفاظت از زیرساخت، جمع‌آوری اطلاعات سایبری و توسعه فناوری‌های امنیت سایبری بومی با هدف کاهش وابستگی به فناوری‌های خارجی بود که ممکن بود آسیب‌پذیری‌هایی را در خود جای دهد (Farwell and Rohozinski,2011). در پاسخ به چشم‌انداز تهدیدات سایبری در حال تحول، ایران تشکیل سازمان‌های سایبری اختصاصی به‌ویژه ارتش سایبری ایران را آغاز کرد که وظیفه حفاظت از زیرساخت‌های سایبری کشور را بر عهده داشتند. این نهادها برای عملیاتی کردن استراتژی ملی سایبری ایران، اجرای پروتکل‌های دفاعی در بخش‌های حیاتی و توسعه قابلیت‌های سایبری تهاجمی تأسیس شدند (Sembiring, 2020).

پس از حمله استاکس‌نت، ایران فرماندهی دفاع سایبری و یک بخش امنیت سایبری جدید را تحت عنوان سازمان پدافند غیرعامل برای محافظت از سیستم‌های اطلاعاتی داخلی از نفوذ دشمنان خارجی به شبکه‌های کلیدی تأسیس کرد. لازم به ذکر است که این توانایی‌های آفندی سایبری صرفاً اسرائیل را هدف قرار نداد و کشورهای متخاصم را نیز شامل می‌شد. بااین‌حال با بررسی آمار حملات صورت گرفته، روشن است که گروه‌های هکر ایرانی، اسرائیل را به‌عنوان هدف اصلی اولویت‌بندی کرده‌اند. به‌عنوان‌مثال، کمپین سی‌ان‌ای ۲۰۱۴[1] به نام عملیات نیوزکستر[2] و کمپین سی‌ان‌ای ۲۰۱۴[3] به نام تمر رزرووار[4] هر دو عملیاتی ایرانی بودند که تاکتیک‌ها، تکنیک‌ها و رویه‌های منحصربه‌فرد حمله بر پایه تی‌تی‌پی‌اس[5] را با هدف دولت و مقام‌های نظامی اسرائیل انجام دادند. تلاش‌های آفندی ایران بعد از حمله استاکس‌نت علیه

1. CNE 2014
2. Newscaster
3. CNA 2014
4. Thamar Reservoir
5. ttps

کشور اسرائیل معطوف به همکاری با گروه‌های هکری حماس و حزب‌الله به‌منظور انجام عملیات علیه آژانس امنیتی اسرائیل[1]، فرماندهی جبهه داخلی، دفتر نخست‌وزیری، وزارت دفاع، بانک اورشلیم، خطوط هواپیمایی ملی اسرائیل، احزاب سیاسی لیکود و کادیما و اجزای عملیاتی ارتش اسرائیل بود. بر اساس گزارش روزنامه جروزالم پست، در بازه زمانی ۲۰۱۲ تا ۲۰۱۵ یکی از هکرهای برجسته حماس، بنام جواد اودح، با موفقیت به شبکه‌های ارتباطی داده‌های ارتش اسرائیل نفوذ کرده و لینک‌های داده را از هواپیماهای بدون سرنشین ارتش اسرائیل که از غزه به سمت فرماندهان حماس پرواز می‌کردند، به دست آورده بود. این نفوذ برای فرماندهان نظامی غزه فرصتی را فراهم کرده بود که بتوانند تصویری پایدار از پهپادهای نظارت هوایی اسرائیل به دست آورند و خود را از نظارت آن‌ها خلاص کنند.

نکته جالب‌توجه این‌که در پی آغاز مذاکرات هسته‌ای ایران که درنهایت به برجام ختم شد (۲۰۱۳ تا ۲۰۱۵)، کاهش چشمگیری در عملیات سایبری ایران ایجاد شد تا به‌عنوان حسن‌نیت تلقی شود و درروند مذاکرات تسهیل شود. این امر نشان‌دهنده ارتباط مستقیم بین مانورهای ژئوپلیتیک ایران و عملیات سایبری ملی بود که ارزش‌گذاری راهبردی ایران را بر توانایی‌های سایبری خود در خدمت دیپلماسی بین‌المللی به نمایش گذاشت؛ اما خروج آمریکا از برجام در ماه می ۲۰۱۸ منجر به احیای فوری فعالیت‌های سایبری ایران و افزایش قابل‌توجهی در عملیات فیشینگ تهاجمی علیه مقام‌های تجاری و نظامی ایالات‌متحده و اسرائیل شد. این تجدیدقوا، ماهیت واکنشی استراتژی سایبری ایران را نشان می‌داد که به‌سرعت با تغییرات محیط ژئوپلیتیک سازگار می‌شد و از عملیات سایبری برای پاسخگویی به تهدیدات درک‌شده یا تغییرات در جهت‌دهی روابط دیپلماتیک استفاده می‌کرد.

ایران علاوه بر شرکای خارجی، از گروه‌های هکری خصوصی داخلی نیمه‌وقت نیز برای عملیات سایبری استفاده کرده است. به‌عنوان‌مثال در سال ۲۰۱۸ یک گروه هکری به نام چارمینگ کیتن[2] مسئول انجام حملاتی علیه چندین رسانه یهودی در داخل ایالات‌متحده بود که از اسرائیل حمایت می‌کردند. حمله مشابهی نیز علیه اپیک (کمیته امور عمومی آمریکا و

1. Shin bet
2. Charming Kitten

اسرائیل)[1]، رهبران سیاسی و دانشگاهی یهودی در سراسر جهان به همراه سازمان‌هایی که از اقدام‌های اسرائیل در غزه یا لبنان حمایت می‌کردند، رخ داد و انگشت اتهام به سمت ایران نشانه رفت.

در اوت ۲۰۱۸، فیس‌بوک و توییتر صدها گروه و حساب‌های کاربری مستقر در ایران را که به نظر می‌رسید بخشی از یک تلاش هماهنگ و مرتبط با رسانه‌های دولتی ایران برای انتشار محتوای غیرواقعی در چهار قاره مختلف ازجمله در ایالات‌متحده بودند، پاک‌سازی کردند (Ingram, 2018; UNAI, 2023). گفته می‌شد که هدف از این عملیات، ترویج روایت‌های سیاسی در راستای منافع ایران است (FireEye Intelligence, 2018). صفحات غیرمعتبر به دنبال حمایت از الزام‌های سیاست خارجی ایران بودند و محتوایی را به نمایش می‌گذاشتند که طرفدار ایران و فلسطین یا ضد اسرائیلی بودند و جهت شرکت در روز قدس تبلیغ می‌کردند. در آوریل ۲۰۲۰، عاملان مظنون ایرانی دست به کارزار بی‌سابقه‌ای از عملیات سایبری زدند و به سیستم‌های کنترل صنعتی با هدف صدمه به مواضع اسرائیلی حمله کردند (Warrick and Nakashima, 2020 b). رسانه‌های اسرائیلی گزارش دادند که شش مورد از تأسیسات آبی اسرائیلی مورد هدف هکرهای ایرانی قرارگرفته‌اند (ToI Staff, 2020) که باعث بی‌نظمی در عملکرد زیرساخت‌ها و سیستم‌های کنترل در تصفیه‌خانه‌های فاضلاب، ایستگاه‌های پمپاژ و تأسیسات فاضلاب شد که قصد افزایش سطح کلر آب تصفیه‌شده در این تأسیسات را داشته است (Srivastava, 2020).

رئیس اداره ملی سایبری اسرائیل پس از حملات آوریل هشدار داد که زمستان سایبری حتی سریع‌تر ازآنچه من گمان می‌کردم شروع شده و ابراز نگرانی کرد که حملات سایبری با هدف قرار دادن مواضع اسرائیلی به‌طور فزاینده‌ای افزایش خواهد یافت (ToI Staff and Agencies, 2020). دولت ایران مسئولیت حملات به سیستم آبی اسرائیل را رد کرد و مدعی شد که موضع سایبری ایران کاملاً دفاعی است و ایران نمی‌تواند ضربه‌ای را که از تلاش برای مسموم کردن غیرنظامیان اسرائیلی ناشی می‌شود، تحمل کند (Srivastava, 2020). رد ادعاها توسط مقام‌های رسمی ایران نشان داد که استفاده از درجه انکار قابل‌قبول ارائه‌شده توسط

1. American Israel Public Affairs Committee

قلمرو سایبری تا چه حد نسبت به حمله نظامی مستقیم بهتر و مؤثرتر و دارای ریسک پایین‌تری است.

حملات سایبری ایران به زیرساخت‌های آبی اسرائیل نیز صدمه وارد کرده است. در ژوئن ۲۰۲۰، هکرها تأسیسات مدیریت آب اسرائیل را هدف قرار دادند و به پمپ‌های آب کشاورزی در جلیل علیا و مرکز اسرائیل حمله کردند. این حملات حاکی از این موضوع است که موضوع بازدارندگی درصحنه سایبر با صحنه متعارف به دلیل قابلیت شدید انکار حملات بسیار متفاوت و در مرحله اجرا بسیار سخت است، زیرا تنبیه متجاوز و پاسخ متقابل تعارف متفاوتی در فضای سایبر یافته است.

در اکتبر ۲۰۲۰، شرکت‌های امنیت سایبری اسرائیلی ازجمله کلیر اسکای[1] و پروفرو[2] گزارش دادند که کمپین حملات باج افزاری را شناسایی کرده‌اند که شرکت‌ها و سازمان‌های برجسته اسرائیلی را در توسط یک گروه هکری به نام مادی واتر کیتن[3] نامیده می‌شود، هدف قرار داده‌اند (Clear Sky, 2020). محققان امنیت سایبری در دسامبر ۲۰۲۰ فاش کردند که هکرهای ایرانی حملات سایبری شامل باج افزار را انجام داده‌اند و ۸۰ شرکت اسرائیلی را موردحمله قرار داده‌اند. به نظر می‌رسد عملیات ایرانی که به نام پی‌توکی[4] شناخته می‌شود (Ziv, 2020)، دست‌ساخته یک گروه هکری تحت حمایت دولت ایران بوده است که به‌عنوان فاکس کیتن[5] شناخته می‌شود و ده‌ها شرکت را در بخش‌های بیمه، لجستیک و صنعتی اسرائیل به‌ویژه صنعت هوافضا هدف قرار داده است (Arghire, 2020). در ماه مه ۲۰۲۲، شین بت از عملیات ایران برای فریب دادن و احتمالاً آسیب رساندن به بازرگانان و دانشگاهیان اسرائیلی در خارج از اسرائیل و جمع‌آوری اطلاعات از طریق عملیات سایبری خبر داد (Joffre, 2022).

در ۱۸ دسامبر ۲۰۲۳، گزارشی ارائه شد (i24NEWS, 2023) مبنی بر این‌که که اداره ملی سایبری اسرائیل در پی تلاش برای حمله سایبری به یکی از تأسیسات اسرائیل واقع در شمال این کشور را انجام داد. این حمله به هکرهای وابسته به ایران و حزب‌الله نسبت داده شد. به

---

1. Clear Sky
2. Profero
3. MuddyWater Kitten
4. Pay2Key
5. Fox Kitten

گفته اداره ملی سایبری اسرائیل، گروه حمله سایبری آگریوس، مرتبط با وزارت اطلاعات جمهوری اسلامی، این حمله را در اواخر نوامبر ۲۰۲۳ در میان تنش‌های مربوط به درگیری شمشیرهای آهنین سازمان‌دهی کرده است. تحقیقات نشان داد که در این عملیات سایبری، واحد سایبری حزب‌الله به نام سدر لبنان به رهبری محمدعلی مرعی با همکاری سرویس‌های اطلاعاتی ایران مشارکت داشته است. لازم به توضیح است که اگرچه بخش عمده‌ای از این حملات به ایران نسبت داده شده است، اما ایران به آن واکنش نشان نداده است.

فرجام سخن

در این مقاله با محوریت بررسی امنیت سایبری در آسیا به دگرگونی منازعات با تمرکز بر منازعات ایران و اسرائیل پس از حمله استاکس‌نت به برنامه هسته‌ای ایران پرداختیم. مراجعه به تاریخ تقابلات این دو کشور حکایت از منازعات شدید استراتژیک مبتنی بر قابلیت‌های مادی و تسلیحاتی آن‌ها دارد. این منازعات بیش از چهار دهه بر پایه تهدیدهای سنتی رقم خورده و مدیریت شده است. برنامه هسته‌ای ایران به‌طور مشخص با آغاز هزاره سوم برای اسرائیل به‌مثابه تهدید جسمانی وجودی تلقی شده و مدیریت آن با اتکا به اجماع سازی جهانی علیه ایران جهت تقابل نظامی، تحریم در قالب قطع‌نامه‌های نهادهای بین‌المللی و حذف و ترور افراد مرتبط با این برنامه از سوی اسرائیل دنبال شد؛ اما حمله استاکس‌نت که از آن می‌توان تعبیر اسب تروای سایبری داشت، یک تغییردهنده بازی در منازعات آسیا بود. اسرائیل با اتکا به این حمله سایبری به‌صورت ناشناس، در ورای مرزهای جغرافیایی ایران و به دور از خسارت جانی به توقف کوتاه‌مدت برنامه هسته‌ای دست زد. مقام‌های اسرائیلی این موضوع را یک پیروزی برای خود تلقی می‌کردند و آن را به‌عنوان تحقق اهداف استراتژیک خود در راستای اسناد امنیت ملی به‌حساب آوردند.

ورود اسرائیل به حوزه سایبری و ضربه استاکس‌نت سبب شد جمهوری اسلامی ایران، به‌عنوان یک کشور آماج، تلاش کند تا به تقویت زیرساخت‌های سایبری، تأسیس ارتش در حوزه سایبری، بازاندیشی و سرمایه‌گذاری در قابلیت‌های سایبری تدافعی و تهاجمی خود بپردازد. این امر موجب آغاز حملات سایبری ایران علیه اسرائیل و شکل‌گیری جنگ سایبری

میان این دو موجودیت شد. حملات ایران علیه اسرائیل ابعاد گسترده‌ای اعم از زیرساختی، سازمانی و نهادی داشت. ساختارهای حکومتی اعم از اداری، سیاسی و حتی نظامی تحت تأثیر حملات سایبری ایران قرار گرفتند. در نقطه مقابل نیز اسرائیل دست به استفاده گسترده از بدافزارها، کرم‌ها و تروجان‌ها زد. حملات اسرائیل هم علیه ساختارهای گوناگون نظامی، سیاسی و شهری بکار گرفته شد.

نکته حائز اهمیت در توسیع و تعمیق تهدیدهای متقابل ایران و اسرائیل آن است که به‌واسطه این دگرگونی، خاورمیانه و به‌صورت عام‌تر، آسیا بیش‌ازپیش خصلت منازعه‌آمیز به خود گرفته است؛ مسئله‌ای که در تعارض با تلاش‌های اغلب موجودیت‌های منطقه‌ای و فرامنطقه‌ای در قبال آسیا و خاورمیانه است. این موجودیت‌ها به‌واسطه نگاه منحصربه‌فردی که دارند، درصددند ثبات یا صلح حداقلی را در بخش از جهان برقرار کنند اما قدر مسلم پدیدار شدن تهدیدهای جدید، مدیریت و تقابل با تهدید به شیوه‌ای جدید را طلب می‌کند. حاصل این امر، چیزی جز افزایش نگرانی افراد و گروه‌های مردمی از استمرار زیست در این قسمت از جهان و تلاش برای ترک این منطقه نیست.

منابع

حبیبی، رحمان، مجید یوسفی و علی رودباری (۱۴۰۰). تحلیل اسناد راهبردی رژیم صهیونیستی (استراتژی امنیت ملی، استراتژی آیزنکوت و استراتژی نظامی)، *مطالعات بنیادین و کاربردی جهان اسلام*، ۳(۸)، ۹-۳۸.

خلف‌رضایی، حسین (۱۳۹۲). حملات سایبری از منظر حقوق بین الملل (مطالعه موردی: استاکس نت). *مجلس و راهبرد* ۷۳(۲۰): ۱۲۵-۱۵۴.

خلیلی پور رکن‌آبادی، علی و یاسر نورعلی وند (۱۳۹۱) تهدیدات سایبری و تأثیر آن بر امنیت ملی، *فصلنامه مطالعات راهبردی* ۱۵, (۵۶)، ۱۹۶-۱۶۷.

نامدار، سعید و غلامعلی قاسمی (۱۳۹۷). بررسی مفهوم دفاع مشروع در پرتو حملات سایبری (با تأکید بر حمله استاکس‌نت به تأسیسات هسته‌ای ایران)، *مطالعات حقوقی* ۱۰(۱): ۱۹۹-۲۳۵.

قرشی، سید یوسف و ناصر پورحسن (۱۴۰۰). واکاوی رفتارهای اسرائیل در سوریه در چهارچوب فرهنگ راهبردی (۲۰۲۰-۲۰۱۳)، *پژوهش های روابط بین الملل*، ۱۱(۴)، ۱۴۱-۱۴۸.

Ansari, A. M. (2006). *Confronting Iran*, London: Hurst & Company.
AP (2021) A cyberattack paralyzed every gas station in Iran, (October 18, 2023), at: https://www.npr.org/2021/10/27/1049566231/irans-president-says-cyberattack-was-meant-to-create-disorder-at-gas-pumps
Arad, U. (2023). Israel's Policy Toward Iran's Nuclear Program—Some Counterfactual Remarks, (15 March, 2024), at: https://jstribune.com/arad-israels-policy-toward-irans-nuclear-program/
Arghire, I. (2020). Iranian Hackers Target Israeli Companies with Pay2Key Ransomware, (December 21, 2023) at: https://www.securityweek.com/iranian-hackers-target-israeli-companies-pay2key-ransomware
Bendiek, A., and Tobias M. (2015). Deterrence theory in the cyber-century.
Buzan, B., and Hansen, L. (2009) *The evolution of international security studies*, Cambridge University Press.
CBS (2011) Iran blames U.S., Israel for Stuxnet malware, (December 16, 2023), at: https://www.cbsnews.com/news/iran-blames-us-israel-for-stuxnet-malware/
CBS (2011) Iran claims the second major cyber attack, (December 12, 2023), at: https://www.cbsnews.com/news/iran-claims-second-major-cyber-attack/
Clear Sky (2020) Operation Quicksand, (October 15, 2023) at: https://www.clearskysec.com/operation-quicksand/
Creators, W. S. S. (2013). To Kill a Centrifuge, A Technical Analysis of What Stuxnet's Creators Tried to Achieve, Munich: The Langner Group
Fassihi, F., Pérez-Peña, R., and Bergman, R. (2020) Iran Admits Serious Damage to Natanz Nuclear Site, Setting Back Program, (February 15, 2024) at: https://www.nytimes.com/2020/07/05/world/middleeast/iran-Natanz-nuclear-damage.html
FireEye Intelligence (2018). Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East, (August 21, 2023), at: https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html
Fox News (2011). Iran Admits Nuclear Sites Hit by 'Duqu' Cyberweapon, (November 14, 2023), at: https://www.foxnews.com/tech/iran-admits-nuclear-sites-hit-by-duqu-cyberweapon
Hounshell, B. (2011). Son of Stuxnet?, (December 19, 2023), at: https://foreignpolicy.com/2011/10/19/son-of-stuxnet/
i24NEWS (2023). Iran, Hezbollah behind cyber attack on Israeli hospital – investigation, (January 18, 2024), at: https://www.i24news.tv/en/news/israel-at-war/1702886863-iran-

hezbollah-behind-cyber-attack-on-israeli-hospital-according-to-investigation

Ingram, D. (2018). Facebook and Twitter say they found an Iran-based propaganda effort, (January 20, 2024), at: https://www.nbcnews.com/news/amp/ncna902716

INNS (2016). The IDF Strategy, (December 25, 2023), at: https://www.inss.org.il/he/wp-content/uploads/sites/2/2017/04/IDF-Strategy.pdf

Kerr, P. K., Rollins, J., and Theohary, C. A. (2010). The Stuxnet computer worm: Harbinger of an emerging warfare capability, Congressional Research Service Washington, DC

Kim, Z. (2012). Wiper Malware That Hit Iran Left Possible Clues of Its Origins, (Aug 29, 2023) at: https://www.wired.com/2012/08/wiper-possible-origins/

Kivimaa, P., et al (2022). A socio-technical lens on security in sustainability transitions: Future expectations for positive and negative security., *Futures*, 141

Kushner, D. (2013). The Real Story of Stuxnet, (Feb 26, 2024), at: https://spectrum.ieee.org/the-real-story-of-stuxnet

Lindsay, Jon R. (2013). Stuxnet and the limits of cyber warfare. *Security studies,* 22(3): 365-404.

Lucas, G. R. (2014). Permissible preventive cyberwar: Restricting cyber conflict to justified military targets. The Ethics of Information Warfare, Springer**:** 73-83

Mattazaro, A. J. (2020). The future fight: Cyberwar at the operational level of war. Army Command And General Staff College Fort Leavenworth Ks, Tech. Rep.

Mellor, N. (2022). Arab Digital Journalism. Cybersecurity in the Middle East and North Africa by Valentina von Finckenstein.

Mills, E. (2012). Behind the 'Flame' malware spying on Mideast computers, (June 18, 2023) at: https://www.cnet.com/tech/services-and-software/behind-the-flame-malware-spying-on-mideast-computers-faq/

Nakashima, Ellen (2012) Iran acknowledges that Flame virus has infected computers nationwide, (June 29, 2023), at: https://www.washingtonpost.com/world/national-security/iran-acknowledges-that-flame-virus-has-infected-computers-nationwide/2012/05/29/gJQAzlEF0U_story.html

Nakashima, E. and Warrick, J. (2012) Stuxnet was work of U.S. and Israeli experts, officials say, (June 02, 2023), at:

https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Nakashima, E., Miller, G. and Tate, J. (2012). U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say, (June 19, 2023), at: https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

Rashid, F. Y. (2011). Iran Claims Stars Virus a Second Cyber-Attack, (April 25, 2023), at: https://www.eweek.com/security/iran-claims-stars-virus-a-second-cyber-attack/

Reuters (2018). Iran's Khamenei calls for fight against enemy 'infiltration', (December 28, 2023), at: https://www.reuters.com/article/us-iran-khamenei/irans-khamenei-calls-for-fight-against-enemy-infiltration-idUSKCN1N20CN/

Reuters (2021). Iran says Israel, U.S. likely behind cyberattack on gas stations, (November 28, 2023), at: https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/

Sanger, D. E. Iran Fights Malware Attacking Computers, (September 25, 2023), at: https://www.nytimes.com/2010/09/26/world/middleeast/26iran.html

Siobhán, O. (2021). What we know about the Natanz nuclear site attack, (April 14, 2023) at: https://www.washingtonpost.com/world/2021/04/12/faq-natanz-nuclear-site-attack-israel/

Srivastava, M. (2020). Israel-Iran attacks: ‘Cyber winter is coming’, (November 31, 2023) at: https://www.ft.com/content/3ea57426-40e2-42da-9e2c-97b0e39dd967

Brantly, A. F. (2018). The cyber deterrence problem. In 2018 *10th International Conference on Cyber Conflict* (CyCon), pp. 31-54. IEEE, 2018.

The Guardian (2021). ‘Cyber-attack’ hits Iran’s transport ministry and railways, (July 15, 2023) at: https://www.theguardian.com/world/2021/jul/11/cyber-attack-hits-irans-transport-ministry-and-railways

Time of Israel (2017). Unit 8200, (April 6, 2023), at: https://www.timesofisrael.com/topic/unit-8200/

ToI Staff (2020). 6 facilities said hit in Iran’s cyberattack on Israel’s water system in (April, 27 June, 2023) at: https://www.timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april/#:~:text=The%20Water%20Authority%20and%20Israel,incidents%

20on%20April%2024%2D25.&text=Israel%20reportedly%20responded%20to%20the,chaos%20in%20the%20Islamic%20Republic.

ToI Staff and Agencies (2020). Iran cyberattack on Israel's water supply could have sickened hundreds – report, 12 Kuly, 2023, at: https://www.timesofisrael.com/iran-cyberattack-on-israels-water-supply-could-have-sickened-hundreds-report/

Tzvi, J. (2022). Shin Bet uncovers Iranian attempts to lure Israeli businessmen, academics, (January 19, 2024, https://www.jpost.com/breaking-news/article-707147

UNAI (2023). How Iran Exports its Ideology, (June 26, 2024), https://www.unitedagainstnucleariran.com/sites/default/files/expansion/Iran%27s%20Ideological%20Expansion%20Final%20Report_11.28.23_JC_JMB_JC.pdf

Van Dine, A. (2017). After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities. In *Project on Nuclear Issues: A Collection of Papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series*. Center for Strategic and International Studies (CSIS) (pp. 101-114).

Warrick, J. and Nakashima, E. (2020 a) Foreign intelligence officials say attempted cyberattack on Israeli water utilities linked to Iran, (August 8, 2023), at: https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html

Warrick, J. and Nakashima, E. (2020 b) Officials: Israel linked to a disruptive cyberattack on Iranian port facility, (August 8, 2023), at: https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

Warrick, J., Mekhennet, S. and Hendrix, S. (2020). Signs increasingly point to sabotage in fiery explosion at Iranian nuclear complex, (August 8, 2023), at: https://www.washingtonpost.com/national-security/signs-increasingly-point-to-sabotage-in-fiery-explosion-at-iranian-nuclear-complex/2020/07/06/d1035e84-bfce-11ea-b178-bb7b05b94af1_story.html

Weimann, G. (2006). *Terror on the Internet: The new arena, the new challenges*, US Institute of Peace Press.

Yong, W. (2011). Iran Discovers New Cyberattack, (June 18, 2023), at: https://www.nytimes.com/2011/04/26/world/middleeast/26iran.html

Ziv, A. (2020). Iranian Hackers Hit 80 Israeli Firms as Massive Cyberattack Continues, (Dec 16, 2023), at: https://www.haaretz.com/israel-news/tech-news/.premium-iranian-hackers-hit-over-80-israeli-firms-as-massive-cyberattack-continues-1.9375486