Defense Policy

130

Vol. 34
Spring 2025
P.P: 113-134

Research Paper

Received:
2024-03-11
Revised:
2024-05-30
Accepted:
2025-06-16
Published:
2025-08-17

ISSN: 1025-5087
E-ISSN: 2654-4971

Ways to deal with cyber espionage of the Zionist regime

Reza Hamzeh Shalamzari [1*] | Zahra Esmaeili Vardanjani [2]

Abstract

In the age of information and communication technology, the increasing development of emerging technologies has undergone fundamental changes in all areas of human life, including the fields of espionage, defense, and military. Recognizing the challenges and threats of these new technologies and being prepared to deal intelligently with the macro-technological trends is one of the constant concerns of policymakers and beneficiaries of the cyber space, hence future research, deep exploratory study, review and analysis of reliable global documents and reports in this Scope is essential. In this research, looking for answers to the questions "What is the impact of disruptive technologies in cyber espionage of the Zionist regime?" and "What are the ways to deal with the cyber espionage of the Zionist regime?" This is a descriptive-case study and in order to collect data, library sources, reliable scientific sites, internal and external documents and reports are used. The results of this research show that the Zionist regime is one of the most prominent parties in the world that increasingly uses basic cyber technology, especially artificial intelligence, for its military and civilian purposes. These technologies give the Zionist regime more facilities for analysis, prediction and espionage operations, the most impact can be counted in the field of cyber espionage.

Keywords: cyber espionage, Zionist regime, espionage threats.

1. PhD student, Department of Information Technology Management, Science and Research Unit, Islamic Azad University, Tehran, Iran. Email: rezahamzeh.sh@gmail.com
2. Master's student, Department of Law, South Tehran Branch, Islamic Azad University, Tehran, Iran. Email: zesmaeili748@gmail.com

Publisher: Imam Hussein University

«سیاست دفاعی»

راه کارهای مقابله با عملیات سایبری رژیم صهیونیستی

رضا حمزه شلمزاری[1]* | زهرا اسماعیلی وردنجانی[2]

۱۳۰

سال سی وچهارم
بهار ۱٤۰٤
صص: ۱۳٤-۱۱۳

مقاله پژوهشی

تاریخ دریافت: ۱٤۰۲/۱۲/۲۱
تاریخ بازنگری: ۱٤۰۳/۰۳/۱۰
تاریخ پذیرش: ۱٤۰٤/۰۳/۲٦
تاریخ انتشار: ۱٤۰٤/۰۵/۲٦

شاپا چاپی: ۵۰۸۷-۱۰۲۵
الکترونیکی: ٤۹۷۱-۲٦۵٤

چکیده

در عصر فناوری اطلاعات و ارتباطات توسعه روزافزون فناوری‌های نوظهور تمامی عرصه‌های زندگی بشر ازجمله حوزه‌های جاسوسی، دفاعی و نظامی را دستخوش تغییرات اساسی نموده است. شناخت چالش‌ها و تهدیدات این فناوری‌های نوین و آمادگی برای مواجهه هوشمندانه باکلان روندهای فناورانه از دغدغه‌های همیشگی سیاست‌گذاران و ذینفعان فضای سایبر است ازاین‌رو آینده‌پژوهی، مطالعه اکتشافی عمیق، بررسی و تحلیل اسناد و گزارش‌های معتبر جهانی در این حوزه امری ضروری است. در این پژوهش به دنبال پاسخ به سؤالات " تأثیر فناوری‌های شالوده شکن در جاسوسی سایبری رژیم صهیونیستی چیست؟" و " راه‌های مقابله با جاسوسی سایبری رژیم صهیونیستی چیست؟ " هستیم. این پژوهش توصیفی _ موردی است و به‌منظور گردآوری داده‌ها از منابع کتابخانه‌ای، سایت‌های معتبر علمی، اسناد و گزارش‌های داخلی و خارجی استفاده است. نتایج حاصل از این پژوهش نشان می‌دهد که رژیم صهیونیستی یکی از بارزترین طرف‌ها در جهان است که به شکل فزاینده‌ای از فناوری سایبر پایه به‌خصوص هوش مصنوعی برای اهداف نظامی و غیرنظامی خود استفاده می‌کند. این فناوری‌ها به رژیم صهیونیستی امکانات بیشتری برای تحلیل، پیش‌بینی و عملیات جاسوسی می‌دهد، می‌توان بیشترین تأثیر را در حوزه جاسوسی سایبری برشمرد.

کلیدواژه‌ها: جاسوسی سایبری، رژیم صهیونیستی، تهدیدات جاسوسی.

۱. دانشجوی دکتری، گروه مدیریت فناوری اطلاعات، واحد علوم و تحقیقات دانشگاه آزاد اسلامی، تهران، ایران.
Email: rezahamzeh.sh@gmail.com
۲. دانشجوی کارشناسی ارشد، گروه حقوق، واحد تهران جنوب دانشگاه آزاد اسلامی، تهران، ایران.
Email: zesmaeili748@gmail.com

مقدمه

روند شکل‌گیری و توسعه فناوری‌های پیشرفته برهم زن و بعضاً غیرقابل‌پیش‌بینی مرتبط با فضای سایبر نشان می‌دهد؛ این فناوری‌ها زمینه‌ساز یک انقلاب صنعتی نوین و جهش تاریخی خواهد بود که پیامدهای آن‌همه ارکان زندگی بشر را تحت تأثیر قرار خواهد داد. وابستگی به فضای سایبر در جهان آینده یک تصویر خیالی نیست بلکه واقعیتی انکارناپذیر و اجتناب‌ناپذیر است. در کشورهای پیشرفته درزمینه فناوری اطلاعات و ارتباطات بخش عمده‌ای از فعالیت‌های اقتصادی اجتماعی و زیست‌محیطی مبتنی بر فضای سایبر است. در این کشورها سازمان‌های اطلاعاتی، نظامی و دفاعی نیز به تجهیزات نوین سایبری مجهز شده‌اند. یکی از حوزه‌هایی که تأثیر قابل‌توجهی از این فناوری‌ها را می‌توان در آن مشاهده کرد، حوزه جاسوسی است. رژیم صهیونیستی، یکی از کشورهایی است که در حوزه جاسوسی فعالیت گسترده‌ای دارد و از فناوری‌های نوظهور برای دستیابی به اهداف خود استفاده می‌کند(Perenc, 2022).

جاسوسی به کسب اطلاعات محرمانه یا طبقه‌بندی‌شده از افراد، سازمان‌ها یا دولت‌ها بدون رضایت یا اطلاع آن‌ها اشاره دارد. جاسوسی را می‌توان از طریق ابزارهای مختلفی ازجمله اطلاعات انسانی، اطلاعات سیگنال و اطلاعات سایبری انجام داد. امنیت ملی، حفاظت از حاکمیت، تمامیت ارضی و منافع یک ملت در برابر تهدیدات خارجی است. جاسوسی نقش مهمی در امنیت ملی ایفا می‌کند زیرابه یک کشور کمک می‌کند تا اطلاعاتی در مورد تهدیدات و آسیب‌پذیری‌های احتمالی جمع‌آوری کند و تصمیمات آگاهانه‌ای برای حفاظت از منافع خود بگیرد. اهمیت جاسوسی در امنیت ملی را می‌توان از جهات زیر دانست: (Gl et al., 2019)

۱- ارزیابی تهدید: جاسوسی به یک حکومت کمک می‌کند تا تهدیدات بالقوه امنیت ملی خود را شناسایی کند، مانند سازمان‌های تروریستی، دولت‌های سرکش یا قدرت‌های رقیب. با جمع‌آوری اطلاعات در مورد توانمندی‌ها، نیات و برنامه‌های این تهدیدها، یک حکومت می‌تواند سطح خطر را ارزیابی کرده و اقدامات مناسب را برای مقابله با آن‌ها انجام دهد.

۲- تصمیم‌گیری استراتژیک: جاسوسی اطلاعات دقیق و به موقعی را در اختیار سیاست‌گذاران قرار می‌دهد که آن‌ها را قادر می‌سازد تا در مورد مسائل مربوط به امنیت ملی تصمیمات آگاهانه بگیرند.

۳- مبارزه با تروریسم: جاسوسی نقش مهمی در شناسایی و برهم زدن سازمان‌های تروریستی دارد. آژانس‌های جاسوسی بانفوذ به این سازمان‌ها می‌توانند اطلاعاتی در مورد برنامه‌ها، تاکتیک‌ها و استراتژی‌های خود جمع‌آوری کنند که می‌تواند برای جلوگیری یا پاسخ به حملات تروریستی مورداستفاده قرار گیرد.

۴- امنیت اقتصادی: جاسوسی می‌تواند با جمع‌آوری اطلاعات در مورد اسرار تجاری، پیشرفت‌های فنّاورانه و استراتژی‌های تجاری کشورها یا شرکت‌های رقیب، به یک کشور کمک کند تا از منافع اقتصادی خود محافظت کند. از این اطلاعات می‌توان برای کسب مزیت رقابتی و حفاظت از امنیت اقتصادی یک کشور استفاده کرد.

۵- روابط دیپلماتیک: جاسوسی می‌تواند بینش‌هایی را در مورد اهداف و نیات سیاست خارجی سایر کشورها ارائه دهد که می‌تواند به یک ملت در جهت‌یابی روابط و مذاکرات دیپلماتیک کمک کند. همچنین می‌توان از این اطلاعات برای تأثیرگذاری بر رفتار ملت‌های دیگر و پیشبرد منافع یک ملت استفاده کرد.

با توجه به اهمیت امنیت ملی و نیاز به جمع‌آوری اطلاعات استراتژیک، بررسی فناوری‌های نوظهور در جاسوسی رژیم صهیونیستی ضروری به نظر می‌رسد. فهم دقیق‌تر از نحوه استفاده از این فناوری‌ها و تأثیر آن‌ها بر فعالیت‌های جاسوسی رژیم صهیونیستی، می‌تواند به سازمان‌ها و کشورها جهت مقابله با این فعالیت‌ها کمک و راهکارهایی برای مقابله با آن‌ها ارائه دهد.

در این پژوهش به دنبال پاسخ به سؤالات " تأثیر فناوری‌های شالوده شکن در جاسوسی سایبری رژیم صهیونیستی چیست؟" و " راه‌های مقابله با جاسوسی سایبری رژیم صهیونیستی چیست؟ " هستیم.

مبانی نظری

هوش انسانی: به اطلاعاتی اشاره دارد که از طریق تماس و روابط انسانی به دست می‌آید، یا به عبارتی مجموعه‌ای از اطلاعات کسب‌شده از منابع انسانی است. منابع می‌توانند از افراد معمولی گرفته تا جاسوسان حرفه‌ای باشند که در یک سازمان خاص کار می‌کنند. این اطلاعات می‌تواند از مصاحبه‌ها، ملاقات، مذاکرات یا هر نوع ارتباط انسانی به دست آید. این نوع از جمع‌آوری اطلاعات می‌تواند در هر دو حوزه نظامی و غیرنظامی کاربرد داشته باشد. (Vie et al., 2015)

اطلاعات سیگنال : جاسوسی سیگنال، اطلاعات سیگنال یا رهگیری سیگنال به عملیات بررسی اطلاعاتی گفته می‌شود که توسط سیگنال‌های الکترونیکی جابجا می‌شوند، به عبارتی می‌توان گفت به رهگیری ارتباطات بین دو یا چند طرف اشاره دارد. (Zou et al., 2023)

اطلاعات سایبری : اطلاعات سایبری که گاهی اوقات "هوش شبکه دیجیتال " نیز نامیده می‌شود، به جمع‌آوری اطلاعات از فضای سایبر گفته که به‌صورت هک و نفوذ یا روش‌های دیگری انجام می‌شود. (Perenc, 2022)

هوش مصنوعی : درواقع هوش مصنوعی شاخه‌ای از علوم رایانه است که هدف اصلی آن تولید ماشین‌های هوشمندی است که توانایی انجام وظایفی که نیازمند به اطلاعات انسانی است را داشته باشد. هوش مصنوعی در حقیقت نوعی شبیه‌سازی اطلاعات انسانی برای کامپیوتر است و منظور از هوش مصنوعی درواقع ماشینی است که به‌گونه‌ای برنامه‌نویسی شده که همانند انسان فکر کند و توانایی تقلید از رفتار انسان را داشته باشد. این تعریف می‌تواند به‌تمامی ماشین‌هایی اطلاق شود که به‌گونه‌ای همانند ذهن انسان عمل می‌کنند و می‌توانند کارهایی مانند حل مسئله و یادگیری داشته باشند. (Mese et al., 2023)

بدافزارها : یک نرم‌افزار ناخواسته و مخرب است که بر روی دستگاه‌ها شخصی، صنعتی، اداری و ... نصب می‌شود و به‌صورت پنهانی اطلاعات سازمانی ،شخصی و... را جمع‌آوری نموده و به سرقت می‌برد یا می‌تواند به دستگاه‌ها آسیب برساند. بدافزار می‌تواند شامل ویروس، کرم، تروجان، جاسوس‌افزار، باج افزار، بات نت، روت کیت، و دیگر انواع نرم‌افزارهای مخرب باشد. (Mat et al., 2021)

تهدیدات سایبری : توسعه فضای سایبر در کنار فرصت‌ها و مزایای بی‌بدیل خود، تهدیدات فزاینده‌ای را نیز به همراه داشته است. به خاطر وابستگی مستقیم یا غیرمستقیم زیرساخت‌های حیاتی کشورها به فضای سایبر این تهدیدات امکان ایجاد خسارات زیان‌بار و خدشه به امنیت و منافع ملی را فراهم نموده است. ازاین‌رو تهدیدات سایبری در راهبردهای اکثر کشورها موردتوجه قرارگرفته است. در این بخش ویژگی‌های مهم تهدیدات سایبری بررسی‌شده است. واژه تهدید ازنظر لغوی به معنای ترساندن، بیم دادن است. در لغت‌نامه آکسفورد تهدید به معنای شخص یا چیزی است که بتواند صدمه، خطر یا اقدام خصمانه علیه کسی یا چیزی انجام دهد. در فرهنگ لغت لانگمن، نیز، تهدید به معنای احتمال وقوع فاجعه و حادثه و ایجاد خطر است ازنظر مفهومی تهدید به معنای هرگونه، نیت، حادثه، قابلیت و اقدام بالفعل و بالقوه برای مداخله یا جلوگیری از نیل به منافع و اهداف است. بنابراین تهدید سایبری را می‌توان به‌صورت زیر تعریف نمود:

هرگونه عامل بالقوه، رویداد یا واقعه باقابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، سرمایه‌های ملی سایبری یا کارکنان سازمان به‌واسطه یک سامانه اطلاعاتی و از طریق دسترسی غیرمجاز، انهدام (تخریب)، افشاء، تغییر اطلاعات و یا ممانعت از ارائه خدمت. ماهیت فراگیر و گستره جهانی فضای سایبر، زمینه‌ای برای ایجاد تهدیدات سایبری در ابعاد سیاسی، اقتصادی، اجتماعی، فرهنگی زیست‌محیطی و دفاعی نظامی فراهم نموده است. تهدیدات سایبری در حوزه نظامی و دفاعی برخلاف سایر ابعاد آن، رویکردی سخت و چهره‌ای خشن دارد. بسیاری، از این تهدیدات به خاطر محدودیت‌های بین‌المللی(Herr, 2014) به‌صورت بالقوه وجود دارد و تنها جنبه بازدارندگی دارد در صورت افزایش تنش و تخاصم میان کشورها این تهدیدات به مرحله عملیاتی و جنگ منجر می‌شود در یک دسته‌بندی کلی انواع تهدیدات سایبری در حوزه امنیتی عبارت‌اند از:

- **جاسوسی سایبری** : در این نوع از تهدید امکان سرقت اطلاعات، برنامه‌ها و عملیات نظامی و فناوری‌های مرتبط با صنایع دفاعی وجود دارد به‌عنوان‌مثال وزارت دفاع ایالات‌متحده اعلام نموده که جاسوسان سایبری اطلاعات شرکت سازنده جنگنده اف ۳۵ را که شامل میلیون‌ها کد نرم‌افزاری و گران‌قیمت‌ترین برنامه تسلیحاتی در تاریخ آمریکاست سرقت کرده‌اند (Cook, ۲۰۱۸).

- **تروریسم سایبری** : تهدیدات تروریسم سایبری، باهدف ترساندن و مجبور نمودن دولت‌ها برای پیشبرد اهداف سیاسی یا اجتماعی گروه‌های مخالف صورت می‌گیرد. این کار با استفاده از ابزارهای سایبری و ایجاد رعب و وحشت در جامعه انجام می‌شود از کار انداختن سامانه‌های اضطراری، انفجار، سقوط هواپیما و .... از طریق حملات سایبری توسط تروریست‌ها قابل انجام است(Herr, ۲۰۱۴).
- **تسلیحات سایبری** : سلاح سایبری به حملات پیچیده کامپیوتر به کامپیوتر گفته می‌شود که از طریق شناسایی و بهره‌برداری آسیب‌پذیری در یک بخش از نرم‌افزار مورداستفاده توسط طرف مقابل موجب ایجاد اختلال و نابودی یک سامانه فناوری اطلاعات یا یک شبکه می‌شود. سلاح سایبری یک سلاح ناشناس و دقیق، بدون نیاز به حضور سرباز (هکر) است. این سلاح وابسته به شناسایی و بهره‌برداری از آسیب‌پذیری‌های فناوری اطلاعات است اما تنها زمانی می‌تواند کارآمد و مؤثر باشد که مخفی و محرمانه باشد و در صورت افشا شدن، کارایی خود را از دست می‌دهد. جذابیت این سلاح‌ها، عمدتاً به خاطر توانایی آن‌ها در ایجاد عدم اطمینان نسبت به اعتبار و کارایی سامانه‌های مبتنی بر اطلاعات ازجمله سامانه فرماندهی و کنترل نظامی است که در آن محرمانگی و امنیت اطلاعات امری حیاتی است.
- **حمله سایبری** : عبارت است از هجوم با استفاده از سلاح سایبری به‌منظور صدمه زدن به اهداف مشخص. حمله سایبری با توجه به نوع سلاح سایبری مورداستفاده تعریف می‌شود نه طبیعت هدف. بنابراین یک حمله سایبری می‌تواند از یک جنگ‌افزار سایبری علیه یک دارایی غیر سایبری یا علیه یک دارایی سایبری استفاده کند اما حمله سایبری به استفاده از یک جنگ‌افزار غیر سایبری علیه یک دارایی سایبری یا غیر سایبری اطلاق نمی‌شود(Cook, ۲۰۱۸).
- **جنگ سایبری** : در این نوع از جنگ، زیرساخت‌های حیاتی و حساس مانند اهداف نظامی، خدمات اجتماعی، سامانه‌های حمل‌ونقل، انرژی، مخابرات و... هدف قرار می‌گیرد. این نوع از جنگ به خاطر حمله از راه دور، دشواری در شناسایی و ردیابی منبع حمله از جنگ‌های سنتی

متفاوت است. در جنگ سایبری به شبکه‌های رایانه‌ای امنیتی دشمن نفوذ کرده و موجب تخریب آن‌ها می‌شود.

پیشینهٔ پژوهش

از مهم‌ترین آثار منتشرشده پیرامون جاسوسی سایبری رژیم صهیونیستی و استفاده از فناوری‌های نوظهور که شامل دو گزارش و یک پژوهش هست در ادامه موردبررسی قرارگرفته‌اند.

- گل محمدی و همکاران در پژوهش خود با عنوان " بازدارندگی سایبری و تحول در دکترین امنیتی- دفاعی اسرائیل"، بیان کردند که رژیم صهیونیستی از طریق تقویت توانمندی‌ها و قابلیت‌های سایبری، به گسترش بازدارندگی خود تا خارج از مرزها پرداخته است و با تغییر در دیدگاه مبنایی دفاعی خود به سمت بازدارندگی‌های غیرمتعارف در حوزه سایبری حرکت کرده است. (گل محمدی، جمشیدی،۱۴۰۱)
- گزارش "تحلیل روند: مطالعه‌ای بر واحد ۸۲۰۰ اسرائیل" تهیه‌شده توسط مرکز مطالعات امنیتی زوریخ سوئیس، در این گزارش سعی بر آن شده است که یک نمای کلی از تاریخچه اقدامات جاسوسی رژیم صهیونیستی، استفاده از فناوری‌های پیشرفته و یگان‌های فعال در این حوزه رژیم نمایش داده شود. (Cordey, ۲۰۱۹)
- گزارش "کشف قابلیت‌های سایبری تهاجمی اعلام‌شده و درک شده دولت‌ها" تهیه‌شده توسط مرکز مطالعات استراتژیک لاهه - دیده بان تسلیحات سایبری، در این گزارش به‌صورت مشروح به اقدامات سایبری کشورها ازجمله عملیات سایبر پایه منتسب و ادعاشده رژیم صهیونیستی اشاره‌شده است، تمامی این عملیات با استفاده از فناوری‌های نوظهور طراحی و اجراشده‌اند. (The Cyber Arms, ۲۰۲۲)

در پژوهش‌های گذشته پژوهشگران تلاش کرده‌اند تجزیه‌وتحلیل دقیقی از موفقیت فناورانه رژیم صهیونیستی ارائه دهند که بر اساس فرهنگ، اقتصاد و خدمت اجباری نظامی رژیم

صهیونیستی و همچنین تهدید وجودی کـه رژیـم صهیونیسـتی احسـاس مـی‌کننـد مبتنـی اسـت. در بررسی‌ها مشخص است که این فناوری‌ها در حوزه‌های جاسوسی و نظامی به‌کـارگیری شـده‌انـد و موجب بازتعریف بازدارندگی در دکترین امنیتی دفاعی این کشور گردیده است.

در پـژوهش حاضـر هـدف اصـلی بررسـی و تحلیـل فنـاوری‌هـای نوظهـوری اسـت کـه رژیـم صهیونیستی در جاسوسی خود به کار می‌برد. این پژوهش به‌منظور شناخت بهتر راهبردها و فن‌های جاسوسی رژیم صهیونیستی، ارائه راهکارهای مقابله و توصیه‌هایی بـرای سـازمان‌هـا و کشـورها در حفاظت از امنیت ملی آن‌ها مفید است. با توجه به اهمیت موضوع و نیـاز بـه بررسـی دقیـق‌تـر، ایـن تحقیق سعی می‌کند تا با بررسی و تحلیـل فنـاوری‌هـای نوظهـور در جاسوسـی رژیـم صهیونیسـتی، مفاهیم و روش‌های مورداستفاده را بررسی و تأثیر آن‌ها را بر فعالیت‌های جاسوسـی مـورد ارزیـابی قرار دهد و ضمن بررسی نقاط قوت و ضعف سـعی در بیـان نکـاتی جهـت الگـوبرداری صـحیح و روش‌های مقابله با رژیم صهیونیستی در این حوزه را دارد.

روش‌شناسی پژوهش

در این تحقیق به مفهوم‌سازی و توصیف جنبه‌های مختلـف فنـاوری‌هـای نوظهـور و تهدیـدات سایبری پرداخته‌شده است، بنابراین این تحقیق ازنظر هدف با توجه به این‌که صرفاً توسعه دانش در مورد جنبه‌های مختلف فناوری‌های نوظهـور و تهدیـدات سـایبری نیسـت بلکـه ارائـه راه‌حـل‌هـا و کاربردهای عملی برای مقابله با این تهدیدات نیز هست، از نوع کاربردی توسـعه‌ای اسـت و ازنظـر ماهیت و روش گردآوری داده‌ها از نوع توصـیفی مـوردی اسـت. در تحقیقـات توصـیفی مـوردی محقـق بـه دنبـال مطالعـه عمیـق در چیسـتی و چگـونگی یـک موضـوع و توصـیف ویژگـی‌هـا و تجزیه‌وتحلیل یک پدیده است. به‌منظور گردآوری داده‌ها از منابع کتابخانـه‌ای، سـایت‌هـای معتبـر علمی، اسـناد و گـزارش‌هـای داخلـی و خـارجی اسـتفاده‌شـده اسـت. ایـن تحقیـق ازنظـر رویکـرد مورداستفاده برای تجزیه‌وتحلیل داده‌ها از نوع کیفی است. در این تحقیق، روایی و پایایی بر مبنـای معیارهای کرسول محقق شده است (Creswell,2014)، در این روش معیارهـای روایـی و پایـایی شامل تماس طولانی با فضای پژوهش، مشاهده مستمر، بررسـی از زوایـای مختلـف، گـردآوری از منابع اطلاعاتی متنوع، تبادل‌نظر با همتایان است.

یافته‌های پژوهش

مشخصه تلاش‌های جاسوسی رژیم صهیونیستی ترکیبی از روش‌های سنتی و رویکردهای فناوری نوآورانه است. در سال‌های اولیه، اطلاعات انسانی نقش برجسته‌ای داشت و رژیم از شبکه‌ای از جاسوسان و مأموران برای جمع‌آوری اطلاعات استفاده می‌کرد. بااین‌حال، با پیشرفت فنّاوری، رژیم صهیونیستی شروع به استفاده از ابزارهای فنّاورانه مانند نظارت الکترونیکی، اطلاعات سیگنال و... در عملیات جاسوسی خود کرد. در ادامه ابعاد جاسوسی رژیم صهیونیستی، نقش هوش مصنوعی و نقاط قوت و ضعف ایجادشده به‌واسطه فناوری‌های نوظهور را بررسی می‌نماییم :

رژیم صهیونیستی از ترکیبی از روش‌های سنتی و نوآورانه برای جمع‌آوری اطلاعات جاسوسی استفاده می‌کند. هوش انسانی، اطلاعات سیگنال و اطلاعات سایبری سه بعد اصلی این فعالیت‌ها را تشکیل می‌دهند.

هوش انسانی:

- درگذشته، از شبکه‌ای از جاسوسان و عوامل برای جمع‌آوری اطلاعات استفاده می‌شد.
- باوجود پیشرفت‌های فنّاوری، اطلاعات انسانی همچنان نقش مهمی ایفا می‌کند.

اطلاعات سیگنال :

- شامل رهگیری، رمزگشایی و تجزیه‌وتحلیل پیام‌های ارتباطی است.
- از هواپیماهای بدون سرنشین و تصاویر ماهواره‌ای برای افزایش قابلیت‌های خود استفاده می‌کنند.

اطلاعات سایبری :

- شامل هک و نفوذ، جمع‌آوری اطلاعات از طریق ابزارهای سایبری و استفاده از هوش مصنوعی برای حملات و دفاع سایبری است.

- رژیم صهیونیستی به‌طور فزاینده‌ای از هوش مصنوعی برای نفوذ و مداخله در امور داخلی سایر کشورها استفاده می‌کند. (فارس ، ۱۴۰۲/۰۱/۲۳)

نقش هوش مصنوعی:

- هوش مصنوعی به‌طور فزاینده‌ای در ابعاد اطلاعات سیگنال و اطلاعات سایبری رژیم صهیونیستی نقش دارد.
- از هوش مصنوعی برای هک و نفوذ به سیستم‌ها، تجزیه‌وتحلیل داده‌ها، شناسایی افراد و فعالیت‌ها و توسعه سیستم‌های دفاع سایبری استفاده می‌شود.
- شرکت‌های هوش مصنوعی رژیم صهیونیستی اغلب با وزارت جنگ و موساد این رژیم ارتباط دارند. (گرداب ،۱۳۹۹/۰۹/۱۱).
- از هوش مصنوعی برای مداخله در انتخابات، انتشار اطلاعات نادرست و هک اطلاعات شخصی استفاده می‌شود. (گرداب ، ۱۴۰۲/۰۶/۰۸)

استفاده از هوش مصنوعی این قابلیت‌ها را به‌طور قابل‌توجهی ارتقا داده است. بااین‌حال، استفاده از این ابزارها خطرات و چالش‌هایی را نیز به همراه دارد که باید موردتوجه قرار گیرد.
به‌طورکلی استفاده از فناوری هوش مصنوعی توسط رژیم صهیونیستی را می‌توان به‌صورت زیر بیان نمود:

استفاده‌های نظامی:

- شناسایی و گشت زنی در امتداد مرزهای فلسطین، لبنان، سوریه و ... (دویچه وله ، ۱۴۰۲/۰۵/۰۷)
- افزایش سرعت در تشخیص و هدف قرار دادن اهداف در حملات هوایی (فارس ، ۱۴۰۲/۰۱/۲۳)
- پیش‌بینی حملات (ایسنا ، ۱۴۰۲/۰۴/۲۵)
- استفاده از مدل هوش مصنوعی "فایر فکتوری" در حملات نظامی (ایسنا ، ۱۴۰۲/۰۴/۲۵)
- شناسایی سکوهای پرتاب موشک و پهپادها توسط هوش مصنوعی (جوان انلاین ،۱۴۰۲/۰۴/۲۶)
- استفاده از نرم‌افزار "آنی ویژن" برای ایجاد القای ترس و ناامیدی (گرداب ، ۱۴۰۲/۰۶/۰۸)

استفاده‌های امنیتی – اطلاعاتی :

- مداخله در امور داخلی کشورها ازجمله انتخابات به‌وسیله هوش مصنوعی (فارس ،۱۴۰۲/۰۱/۲۳)
- هک اطلاعات شخصی کاربران شبکه‌های اجتماعی و پیام‌رسان‌ها (فارس ، ۱۴۰۲/۰۱/۲۳)
- استفاده از هوش مصنوعی برای مداخله در انتخابات آمریکا (فارس ، ۱۴۰۲/۰۱/۲۳)
- دخالت شرکت صهیونیستی "گروه ارشمیدس" در انتخابات کشورهای آفریقایی ، آمریکای لاتین و آسیای شرقی (فارس ، ۱۴۰۲/۰۱/۲۳)
- استفاده از هوش مصنوعی در ترور شهید محسن فخری زاده با استفاده از سلاح کشنده خودمختار ، سلاح‌های کشنده خودمختار به سلاح‌هایی که بتوانند بدون دخالت، نظارت یا فرمان انسان جراحات کشنده را وارد کنند گفته می‌شود. این سلاح‌ها می‌توانند بر روی زمین، در هوا، دریا یا حتی فضا به کار گرفته شوند. (گرداب ،۱۳۹۹/۰۹/۱۱)

فرصت‌ها و نقاط قوت، چالش‌ها و محدودیت‌ها

با توجه به مباحث مطرح‌شده می‌توان تأثیرات فناوری‌های نوظهور در اقدامات جاسوسی رژیم را با تمرکز بر فرصت‌ها و نقاط قوت ایجادشده، چالش‌ها و محدودیت‌های پیش رو برشمرد که در ادامه به آن‌ها پرداخته‌شده است :

فرصت‌ها و نقاط قوت:

- **افزایش کارایی و اثربخشی**
  - اتوماسیون وظایف معمول: فناوری‌های پیشرفته مانند هوش مصنوعی و یادگیری ماشینی، اتوماسیون وظایف معمول در جاسوسی رژیم صهیونیستی را فعال کرده است و منابع انسانی را برای کارهای پیچیده‌تر و پرمخاطره آزاد می‌کند. به‌عنوان‌مثال، الگوریتم‌های هوش مصنوعی می‌توانند برای غربال کردن مقادیر زیادی از داده‌ها برای شناسایی الگوها و ناهنجاری‌ها مورداستفاده قرار گیرند و نیاز تحلیل‌گران انسانی به بررسی و تحلیل دستی حجم وسیعی از داده‌ها را کاهش دهند.

- بهبود دقت، سرعت جمع‌آوری، تجزیه‌وتحلیل اطلاعات: فناوری‌های پیشرفته مانند هواپیماهای بدون سرنشین، تصاویر ماهواره‌ای و حسگرهای پیشرفته، جاسوسی رژیم صهیونیستی را قادر ساخته است تا اطلاعات را با دقت و سرعت بیشتری جمع‌آوری و تجزیه‌وتحلیل کند. به‌عنوان‌مثال، پهپادهای مجهز به حسگرهای پیشرفته می‌توانند تصاویر و داده‌های نظارتی را در زمان واقعی ارائه دهند و الگوریتم‌های هوش مصنوعی می‌توانند به‌سرعت این داده‌ها را پردازش و تجزیه‌وتحلیل کنند تا اطلاعات عملی ارائه کنند.
- افزایش دسترسی به اطلاعات: فناوری‌های پیشرفته مانند اینترنت، رسانه‌های اجتماعی و دیگر پلتفرم‌های دیجیتالی، جاسوسی رژیم صهیونیستی را قادر به دسترسی و جمع‌آوری اطلاعات از طیف وسیع‌تری از منابع کرده است. به‌عنوان‌مثال، ابزارهای نظارت بر رسانه‌های اجتماعی را می‌توان برای ردیابی، تجزیه‌وتحلیل فعالیت‌های آنلاین مورداستفاده قرارداد، درحالی‌که الگوریتم‌های هوش مصنوعی می‌توانند برای شناسایی و استخراج اطلاعات مرتبط از حجم وسیعی از داده‌ها استفاده شوند.

- **افزایش قابلیت‌ها در زمینه‌هایی مانند سایبر و اطلاعات سیگنال**
  - استفاده از هوش مصنوعی و یادگیری ماشینی برای حملات سایبری و دفاع: فناوری‌های پیشرفته مانند هوش مصنوعی و یادگیری ماشینی، جاسوسی رژیم صهیونیستی را قادر ساخته تا قابلیت‌های سایبری خود را هم برای اهداف تهاجمی و هم برای اهداف دفاعی افزایش دهد. به‌عنوان‌مثال، الگوریتم‌های هوش مصنوعی می‌توانند برای شناسایی و خنثی کردن تهدیدات سایبری در زمان واقعی استفاده شوند و یادگیری ماشینی می‌تواند برای شناسایی و بهره‌برداری از آسیب‌پذیری‌ها در سیستم‌های دشمن استفاده شود.
  - تهدیدهای پایدار پیشرفته و سایر حملات سایبری پیچیده.
  - استفاده از یادگیری ماشین برای تشخیص ناهنجاری، تجزیه‌وتحلیل و پیش‌بینی.
  - توسعه الگوریتم‌های پیشرفته برای پردازش و تجزیه‌وتحلیل سیگنال‌ها: فناوری‌های پیشرفته مانند یادگیری ماشین و الگوریتم‌های پردازش سیگنال، جاسوسی رژیم

صهیونیستی را قادر ساخته است تا قابلیت‌های اطلاعات سیگنال خود را بهبود بخشد و به آن اجازه می‌دهد سیگنال‌های ارتباطی را با دقت و سرعت بیشتری رهگیری و تجزیه‌وتحلیل کند. به‌عنوان‌مثال، الگوریتم‌های یادگیری ماشینی را می‌توان برای شناسایی و استخراج اطلاعات مرتبط از مقادیر وسیعی از داده‌های ارتباطی استفاده کرد و الگوریتم‌های پردازش سیگنال را می‌توان برای بهبود و شفاف‌سازی کیفیت سیگنال استفاده نمود.

- **بهبود آگاهی موقعیتی و تصمیم‌گیری**
  - استفاده از داده‌ها و تجزیه‌وتحلیل‌های بلادرنگ: فناوری‌های پیشرفته جاسوسی رژیم صهیونیستی را قادر ساخته است تا آگاهی موقعیتی و توانایی‌های تصمیم‌گیری خود را بهبود بخشد. به‌عنوان‌مثال، داده‌های بلادرنگ را می‌توان برای ارائه اطلاعات لحظه‌به‌لحظه در مورد تحرکات و فعالیت‌های دشمن استفاده کرد.
  - تجسم پیشرفته و فناوری‌های نقشه‌برداری: فناوری‌های پیشرفته مانند مدل‌سازی سه‌بعدی و واقعیت مجازی، جاسوسی رژیم صهیونیستی را قادر ساخته تا قابلیت‌های تجسم و نقشه‌برداری خود را بهبود بخشد و درک دقیق و دقیق‌تری از مناطق و عملیات دشمن ارائه دهد. برای مثال می‌توان از مدل‌های سه‌بعدی برای ایجاد نقشه‌های دقیق از امکانات و زیرساخت‌ها استفاده کرد، درحالی‌که از واقعیت مجازی می‌توان برای شبیه‌سازی و تمرین مأموریت‌ها بهره جست. (Cordey, ۲۰۱۹)
- **منابع انسانی:**
  - تعداد کارکنان یگان ۸۲۰۰ بیش از ۱۰,۰۰۰ نیرو تخمین زده می‌شود که از این تعداد ۵۰۰۰ نفر در هرلحظه در حال انجام‌وظیفه هستند. درحالی‌که نسبت به همتای آمریکایی خود، آژانس امنیت ملی که در سال ۲۰۱۳ بین ۳۵,۰۰۰ تا ۵۵,۰۰۰ تخمین زده می‌شود پایین‌تر است، و در مقایسه با ستاد ارتباطات بریتانیا در سال ۲۰۱۲/۱۱/۲ هم‌تراز است. علاوه بر این، وقتی اندازه یگان را نسبت به جمعیت رژیم صهیونیستی تقریباً بیش از ۹ میلیون نفر در نظر بگیریم، اهمیت آن بلافاصله آشکار

می‌شود. ازنظر مزیت رقابتی، چنین نیروی قابل‌توجهی به واحد اجازه می‌دهد تا در حوزه‌های مختلف تخصص و توسعه یابند و طیف وسیعی از فعالیت‌ها و مأموریت‌ها (مانند عملیات سایبری تهاجمی، رمزگشایی، و غیره) را پوشش دهند. (Cordey, ۲۰۱۹)

- **منابع مالی و زیرساخت:**
  - با در نظر گرفتن اندازه و پیچیدگی برخی از عملیات آن‌ها - به‌عنوان‌مثال استاکس نت، که از چهار آسیب‌پذیری روز صفر استفاده می‌کرد، می‌توان فرض کرد که منابع مالی قابل‌توجهی دارند. همراه با منابع انسانی غنی ذکرشده در بالا، این بودجه سخاوتمندانه به واحد اجازه می‌دهد تا از طریق کانال‌های مختلف، ازجمله امکان و توانایی انجام عملیات متعدد، گاهی با بودجه بسیار محدود و گاهی در سطوح بسیار پیچیده در صورت نیاز، مزیت رقابتی خود را توسعه داده و حفظ کند. (Cordey, ۲۰۱۹)

- **قابلیت‌ها و دانش:**
  - علاوه بر فناوری، این واحد طی دهه‌های گذشته، قابلیت‌های اطلاعاتی و سایبری قابل‌توجهی را توسعه داده است. به‌این‌ترتیب، اکنون دارای دانش و حافظه نهان است که تعداد کمی از کشورها می‌توانند با آن رقابت کنند و سال‌به‌سال در طی آموزش، دانش به نیروهای جدید منتقل می‌شود (با ۲۵ درصد کاهش). این دانش، که با تکمیل مأموریت‌ها و دنبال کردن نوآوری‌های بیشتر توسط واحد، دائماً بر روی آن ساخته می‌شود، یکی از نقاط قوت اصلی آن در حفظ برتری رقابتی نسبت به دیگران است. (Cordey, ۲۰۱۹)

- **برند و فرآیند غربالگری :**
  - نقطه قوت دیگر توانایی واحد برای شناسایی، جذب و حفظ نیروی کار کارآمد و باهوش است. دسترسی مستمر آن به افراد ماهر عمدتاً به دلیل دو عنصر است، تصویر و شهرت برند و فرآیندهای گزینشی غربالگری و انتخاب. برند واحد در

طول سال‌ها از طریق ابتکارات فارغ‌التحصیلان و همچنین افشای فعالیت‌های برجسته، گفتمان/تبلیغات دولتی و مصاحبه با فارغ‌التحصیلان برای ترویج استارت‌آپ‌هایشان، با دقت ساخته و تقویت‌شده است. این شهرت به‌نوبه خود باعث ایجاد آگاهی گسترده در مورد واحد شده و تصویری را ترویج می‌کند که برای نیروهای جوان و ماهر بسیار جذاب است. در همین حال، فرآیندهای غربالگری و گزینش واحد به آن‌ها اجازه می‌دهد تا استعدادهای جوان را شناسایی و دنبال کنند و توانایی‌ها و مهارت‌های آن‌ها را حتی قبل از پیوستن به واحد پرورش دهد. آن‌ها همچنین اطمینان حاصل می‌کنند که استخدام‌کنندگان قادر به انتخاب نامزدهایی (همسر) هستند که با نیازهای واحد مطابقت دارند. (Cordey, ۲۰۱۹)

چالش‌ها و محدودیت‌ها:

- **وابستگی به فناوری :**
  - آسیب‌پذیری در برابر حملات سایبری و جنگ الکترونیک: اتکای فزاینده به فناوری‌های پیشرفته در جاسوسی رژیم صهیونیستی نیز این کشور را در برابر حملات سایبری و جنگ الکترونیک آسیب‌پذیرتر کرده است. حملات سایبری می‌تواند برای به خطر انداختن امنیت سیستم‌های اطلاعاتی رژیم صهیونیستی، سرقت اطلاعات حساس یا مختل کردن عملیات استفاده شود. همچنین می‌توان از جنگ الکترونیک برای پارازیت یا رهگیری سیگنال‌های ارتباطی استفاده کرد و تلاش‌های جاسوسی رژیم صهیونیستی را کم اثر کرد. به‌عنوان‌مثال، در سال ۲۰۱۰، سیستم‌های رایانه‌ای ارتش رژیم صهیونیستی هدف یک حمله سایبری پیچیده موسوم به "عملیات موش سایه‌دار" قرار گرفت. این حمله که به هکرهای چینی نسبت داده شد، منجر به سرقت اطلاعات حساس و به خطر افتادن امنیت سیستم‌های نظامی رژیم صهیونیستی شد. (The Cyber Arms, ۲۰۲۲)
  - خطر خرابی یا نقص فناوری: استفاده از فناوری‌های پیشرفته در جاسوسی رژیم صهیونیستی نیز خطر شکست یا نقص فناوری را به همراه دارد. اشکالات فنی،

اشکالات نرم‌افزاری، یا نقص سخت‌افزاری می‌تواند اثربخشی عملیات جاسوسی را به خطر بیندازد یا حتی منجر به از دست رفتن اطلاعات حساس شود. به‌عنوان‌مثال، در سال ۲۰۱۸، ناوگان هواپیماهای بدون سرنشین ارتش رژیم صهیونیستی به دلیل نقص فنی که باعث سقوط هواپیماهای بدون سرنشین یا گم‌شدن مسیر خود شد، زمین‌گیر شد. این حادثه خطرات مرتبط با تکیه‌بر فناوری‌های پیشرفته و نیاز به طرح‌های پشتیبان و اقدامات اضطراری را برجسته کرد.

- مشکل در حفظ رازداری و پنهان‌کاری: استفاده از فناوری‌های پیشرفته در جاسوسی رژیم صهیونیستی نیز می‌تواند حفظ رازداری و پنهان‌کاری را دشوارتر کند. فناوری‌های پیشرفته قابل‌شناسایی هستند و استفاده از آن‌ها می‌تواند شبهاتی را ایجاد کند و انجام عملیات مخفی را چالش‌برانگیزتر کند. به‌عنوان‌مثال، استفاده از پهپادها برای نظارت می‌تواند توسط سیستم‌های راداری قابل‌شناسایی باشد و شناسایی و رهگیری پهپادها را برای کشورهای دیگر آسان‌تر می‌کند.

- **اهمیت شهود و قضاوت انسان :**
  - درحالی‌که فناوری‌های پیشرفته به‌طور قابل‌توجهی قابلیت‌های جاسوسی رژیم صهیونیستی را افزایش داده‌اند، شهود و قضاوت انسان در شرایط خاص بسیار حیاتی است. افسران اطلاعاتی قادر به تجزیه‌وتحلیل موقعیت‌های پیچیده، شناسایی الگوها و تصمیم‌گیری بر اساس تجربه و تخصص خود هستند. شهود انسان می‌تواند ناهنجاری‌ها و بی‌نظمی‌هایی را که ممکن است توسط فناوری تشخیص داده نشود، مانند تغییرات ظریف در رفتار یا تناقضات در اطلاعات را تشخیص دهند. قضاوت انسانی در ارزیابی قابلیت اطمینان و اعتبار منابع و همچنین در تصمیم‌گیری استراتژیک بر اساس اطلاعات جمع‌آوری‌شده ضروری است.

- **محدودیت‌های فناوری در شرایط خاص :**
  - علیرغم پیشرفت‌های فنّاوری، هنوز شرایط خاصی وجود دارد که هوش انسان مؤثرتر یا ضروری است. به‌عنوان‌مثال، در برخی موارد، منابع انسانی ممکن است تنها

راه جمع‌آوری اطلاعات در زمان واقعی باشد، مانند محیط‌های متخاصم یا هنگام برخورد با اهداف غیرقابل‌پیش‌بینی، افسران اطلاعاتی همچنین می‌توانند در مناطقی که فناوری محدود یا غیرقابل‌اعتماد است، مانند مناطق دورافتاده یا توسعه‌نیافته، فعالیت کنند. علاوه بر این، اطلاعات انسانی می‌تواند درک عمیق‌تری از انگیزه‌ها و مقاصد اهداف ارائه دهد که تشخیص آن‌ها تنها از طریق فناوری دشوار است.

- **نیاز به تعادل بین فناوری و اطلاعات انسانی:**
  - درحالی‌که فناوری توانایی‌های جاسوسی رژیم صهیونیستی را بسیار افزایش داده است، ایجاد تعادل بین فناوری و اطلاعات انسانی مهم است. اتکای بیش‌ازحد به فناوری می‌تواند منجر به از دست دادن مهارت‌ها و تخصص‌های انسانی شود. تعادل بین فناوری و اطلاعات انسانی تضمین می‌کند که از نقاط قوت هر دو استفاده می‌شود و درعین‌حال نقاط ضعف آن‌ها به حداقل می‌رسد. این تعادل همچنین تضمین می‌کند که استفاده از فناوری با قضاوت و نظارت انسان، جلوگیری از سوءاستفاده‌های احتمالی و تضمین مسئولیت‌پذیری انجام می‌شود.
- **جنجال‌های سیاسی :**
  - در چند سال گذشته، یگان ۸۲۰۰ به دلیل برخی از فعالیت‌هایش تا حدودی بدنام و به‌شدت بحث‌برانگیز شده است. این به‌طور قابل‌توجهی در سال ۲۰۱۴ نشان داده شد، زمانی که ۴۳ نیروی ذخیره، در نامه‌ای سرگشاده و امضاشده نظارت "غیراخلاقی" از فلسطینیانی که در خشونت دخالت ندارند را محکوم کردند. چنین افشاگری‌ها و تبلیغاتی می‌تواند پیامدهای مضری برای یگان و رژیم صهیونیستی را داشته باشد. حوادثی با این ماهیت خطر ایجاد اختلاف در میان صفوف یگان را تشدید می‌کند. همچنین آن‌ها می‌توانند به اعتبار رژیم صهیونیستی آسیب بیشتری وارد کنند و فشار بین‌المللی را افزایش دهند.

- **تجاوز بوروکراتیک :**
  - یگان ۸۲۰۰ به یکی از بزرگ‌ترین واحدهای ارتش رژیم صهیونیستی تبدیل‌شده است. به‌این‌ترتیب، و علیرغم معماری غیرمتمرکز فعلی آن، مستعد سطح معینی از تجاوزات بوروکراتیک است، همان‌طور که در مورد هر سازمانی به‌اندازه آن وجود دارد. اگرچه بدیهی است که به‌خودی‌خود یک ضعف نیست، اما نظام‌مندی بیش‌ازحد فرآیندهای داخلی می‌تواند سطح نوآوری آن را خفه کند. این عنصری است که واحد از آن آگاه است و با "قانون حفظ جنون" و فعالیت‌های مختلف سعی در کنترل آن دارد. (Cordey, ۲۰۱۹)

نتیجه‌گیری و پیشنهادها

گسترش فناوری و وسایل ارتباطی جدید یک سلاح دو لبه است. از سویی می‌توان از آن برای تسهیل امور، کوتاه‌تر کردن فاصله‌های میان کشورها و تمدن‌های مختلف استفاده کرد، از سوی دیگر ممکن است از آن برای واردکردن خسارت‌های سنگین به افراد یا نهادها یا کشورها به‌منظور تحقق اهداف مشخص استفاده شود و بدین ترتیب ما در یک فضای به سر می‌بریم که کنترل و اعمال قانون بر آن کار سختی است.

در این پژوهش پس از مروری بر مهم‌ترین فناوری‌های نوآورانه به بررسی عملیات و اقدامات اخلالگرایانه رژیم منحوس صهیونیستی و بررسی ابعاد جاسوسی این رژیم پرداختیم و سعی در تشریح اهداف پشت پرده این تلاش‌ها مانند تحقق دستاوردهای امنیتی، سیاسی و ... در عرصه بین‌المللی از طریق استفاده از این فناوری‌ها یا فروش آن‌ها به شرکت‌ها، دولت‌ها و کشورهای موردنظر دارد؛ همان‌طوری که بنیامین نتانیاهو نخست‌وزیر رژیم صهیونیستی در جریان اجلاس "سایبرتک" در تاریخ ۲۰۱۹/۱/۲۹ اعلام کرد، این فناوری‌ها به‌طرف صهیونیستی اجازه می‌دهد که به‌راحتی به اطلاعات موردنظر درباره ملت‌ها دست یابد یا مستقیماً از شرکت‌های تجاری مانند گوگل، یاهو، فیس‌بوک و مایکروسافت و غیره بخواهد که این اطلاعات را در اختیار آن‌ها قرار دهند. در صورتی هم که این شرکت‌ها از ارائه اطلاعات موردنیاز رژیم صهیونیستی خودداری

کنند، مراجع صهیونیستی امکانات و راهکارهای موردنیاز برای دستیابی به بسیاری از این اطلاعات رادارند. (مرکز اطلاع‌رسانی فلسطین ، ۱۳۹۸/۰۷/۰۶)

در انتهای پژوهش در مورد نقاط قوت، فرصت‌ها و محدودیت‌های به‌کارگیری فناوری‌های نوظهور بحث گردید. این نقاط قوت شامل منابع انسانی غنی، منابع مالی و زیرساخت‌های پیشرفته، قابلیت‌ها و دانش، فرهنگ داخلی و برند و فرآیند غربالگری هستند. چالش‌ها و محدودیت‌ها شامل وابستگی زیاد به فناوری با آسیب‌پذیری در برابر حملات سایبری و جنگ الکترونیک، خطر خرابی یا نقص فناوری، مشکل در حفظ رازداری و پنهان‌کاری، اهمیت شهود و قضاوت انسان در مقابل محدودیت‌های فناوری در شرایط خاص، نیاز به تعادل بین فناوری و هوش انسانی، جنجال‌های سیاسی ناشی ازاین‌گونه فعالیت‌ها و تجاوز بوروکراتیک که ممکن است تأثیرات منفی بر عملکرد رژیم داشته باشد می‌باشند.

بررسی‌ها نشان می‌دهد در استفاده از این فناوری‌ها، باید میان نگرانی‌های امنیتی ناشی از دستیابی به اطلاعات حساس و کارایی جذاب و وسوسه‌انگیز آن‌ها، مصالحه برقرار نمود. استفاده از فناوری‌های نوظهور مستلزم غلبه بر چالش‌های امنیت اطلاعات است.

با توجه به بررسی یافته‌های پژوهش می‌توان مواردی را برای ضربه به رژیم منحوس و جعلی و همچنین پیشنهادهایی برای الگوبرداری جهت استفاده از فناوری‌های سایبر پایه در حوزه جاسوسی و اطلاعاتی برشمرد، که می‌توان آن‌ها را به‌صورت زیر بیان نمود :

- تشویق نهادهای رسانه‌ای به‌منظور آگاه‌سازی جامعه درزمینه خطر برنامه‌های جاسوسی و انگیزه‌های رژیم صهیونیستی.
- همکاری با نهادهای رسمی عربی و غیرعربی و مراکز حقوقی و بشردوستانه برای وضع قوانین بین‌المللی کارآمد به‌منظور حمایت از شهروندان در برابر فعالیت‌های جاسوسی و نقض حریم شخصی آن‌ها؛ هرچند که اجرای این قوانین در عرصه عمل سخت است؛ چراکه دستیابی به راهکارهای کشف موارد جاسوسی به‌ندرت محقق می‌شود.
- استفاده از چارچوب‌های موجود برای تحریم‌ها یا کیفرخواست‌های هدفمند.
- بهبود اشتراک‌گذاری اطلاعات در مورد تهدیدات در میان جوامع.

پیشنهادهای استفاده از فناوری‌های نوظهور برای سازمان‌های اطلاعاتی و امنیتی سایر کشورها

- اهمیت ایجاد تعادل بین فناوری و اطلاعات انسانی: درحالی‌که فناوری‌های پیشرفته توانایی‌های جاسوسی را بسیار افزایش داده است اما مهم است که بدانیم فناوری به‌تنهایی نمی‌تواند همه چالش‌های پیش روی سازمان‌های اطلاعاتی را حل کند. هوش و قضاوت انسان هنوز برای تجزیه‌وتحلیل و تفسیر حجم عظیمی از داده‌های جمع‌آوری‌شده توسط فناوری‌های پیشرفته و برای تصمیم‌گیری استراتژیک بر اساس آن داده‌ها ضروری است. بنابراین، ایجاد تعادل بین فناوری و اطلاعات انسانی بسیار مهم است و اطمینان حاصل شود که هر دو در هماهنگی برای دستیابی به بهترین نتایج ممکن مورداستفاده قرار می‌گیرند.
- آموزش و آگاهی عمومی : برای حفاظت از حریم خصوصی و امنیت شخصی، آموزش و آگاهی عمومی درباره راهکارها و تهدیدات جدید در حوزه جاسوسی ضروری است. ارائه راهنماها و آموزش‌هایی درباره استفاده امن از فناوری‌ها و محافظت از اطلاعات شخصی می‌تواند مفید باشد.
- حصول اطمینان از تخصیص منابع انسانی و مالی کافی و همچنین زیرساخت‌های با فناوری پیشرفته.
- ترویج انتقال منظم و مستمر دانش و تجربه.
- پرورش فرهنگ داخلی کارآفرینی و نوآوری.
- توسعه و تقویت روابط با بخش خصوصی.
- افزایش جذابیت عمومی و حرفه‌ای فعالیت‌ها برای استخدام‌شدگان و کارفرمایان، برای مثال بورسیه برای تحصیلات دانشگاهی و ...
- توسعه آگاهی عمومی از فعالیت‌ها و موفقیت‌های آن به‌منظور جذب بهترین افراد ممکن.
- تلاش برای توسعه نیروی انسانی فعال در عرصه فنّاوری و به‌ویژه عرصه امنیت اطلاعات.
- تشویق دانشگاه‌ها به هدایت دانشجویان به سمت تحصیلات مرتبط و راه‌اندازی مراکز تولیدات عملی.

- تشویق مراکز پژوهشی به‌منظور پژوهش و نگارش مطالعات علمی تخصصی در زمینه‌های فناوری و حقوقی مرتبط با جرائم اینترنتی به‌منظور آگاهی بخشی به جامعه.

فهرست منابع

ایسنا. (۲۵/۰۴/۱۴۰۲). بلومبرگ: رژیم صهیونیستی در عملیات نظامی خود از هوش مصنوعی استفاده می‌کند. قابل دسترس در https://www.isna.ir.

جوان آنلاین. (۲۶/۰۴/۱۴۰۲). استفاده ارتش صهیونیستی از هوش مصنوعی. قابل دسترس در https://www.javanonline.ir.

دویچه وله. (۰۵/۰۷/۱۴۰۲). رژیم صهیونیستی پیشگام در ساخت ربات‌های جنگی مبتنی بر هوش مصنوعی. قابل دسترس در https://www.dw.com/fa-ir.

فارس. (۲۳/۰۱/۱۴۰۲). هوش مصنوعی در خدمت اهداف جاسوسی رژیم صهیونیستی. قابل دسترس در https://www.farsnews.ir.

گرداب. (۰۸/۰۶/۱۴۰۲). رژیم صهیونیستی، هوش مصنوعی و کشتار مردم بی‌گناه فلسطین. قابل دسترس در https://gerdab.ir.

گرداب. (۱۱/۰۹/۱۳۹۹). ردپای جاسوسی سایبری در ترور شهید فخری‌زاده. قابل دسترس در https://gerdab.ir.

گل محمدی، و. و جمشیدی، ط. (۱۴۰۱). بازدارندگی سایبری و تحول در دکترین امنیتی-دفاعی اسرائیل. فصلنامه جغرافیای سیاسی، ۷.(4)

مرکز اطلاع رسانی فلسطین. (۰۶/۰۷/۱۳۹۸). یگان ۸۲۰۰ رژیم صهیونیستی و نقش آن در فناوری‌های جاسوسی این رژیم. قابل دسترس در.https://farsi.palinfo.com

هلیلی خداداد، و. و ولوی محمدرضا، و. و موحدی صفت، م. (۱۳۹۶). مدلسازی فرایندهای C4I توسط سامانه‌های فیزیکی-سایبری-اجتماعی (CPSS). دهمین کنفرانس ملی فرماندهی و کنترل ایران، دانشگاه خاتم الانبیاء (ص).

Attatfa, A., Renaud, K., & De Paoli, S. (2020). Cyber Diplomacy: A Systematic Literature Review. *Procedia Computer Science, 176*, 60–69. https://doi.org/10.1016/j.procs.2020.08.00

Cook, P. J. (2018). Gun theft and crime. *Journal of Urban Health, 95*(3), 305–312. https://doi.org/10.1007/s11524-018-0253-

Cordey, S. (2019). Trend Analysis: The Israeli Unit 8200 – An OSINT-based study. *Center for Security Studies (CSS), ETH Zürich*. Available at https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-12-Unit-8200.pdf

Creswell, J. W. (2014). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Thousand Oaks, CA: Sage.

Gl, S., Jh, A., Roberts, K., Gordon, J., Smith, E. R., Afman, J., & Sm, S. (2019). The Joint Counterterrorism Awareness Workshop Series (JCTAWS): Integrating disciplines for enhanced capabilities during a complex coordinated attack. *Journal of Emergency Management, 17*(3), 210–212. https://doi.org/10.5055/jem.2019.0419

Herr, T. Prep. (2014). A framework for malware & cyber weapons. *The Journal of Information Warfare, 13*(1), 87-106.

Mat, S. R. T., Ab Razak, M. F., Kahar, M. N. M., Arif, J. M., Mohamad, S., & Firdaus, A. (2021). Towards a systematic description of the field using bibliometric analysis: malware evolution. *Scientometrics, 126*(3), 2013–2055. https://doi.org/10.1007/s11192-020-03834-6

Mese, I., Taslicay, C. A., & Sivrioglu, A. K. (2023). Improving radiology workflow using ChatGPT and artificial intelligence. *Clinical Imaging, 103*(109993), 109993. https://doi.org/10.1016/j.clinimag.2023.109993

Perenc, L. (2022). Psychopathic personality disorder and cybercriminality: an outline of the issue. *Current Issues in Personality Psychology*. https://doi.org/10.5114/cipp.2022.114205

Senor, D., & Singer, S. (2009). *Start-up nation: the story of Israel's economic miracle*. United States.

The Hague Centre for Strategic Studies. (2022). *The Cyber Arms*. Available at https://hcss.nl/wp-content/uploads/2022/05/Cyber-Arms-Watch-HCSS-2022-1.pdf

Vie, L. L., Scheier, L. M., Lester, P. B., Ho, T., Labarthe, D. R., & Seligman, M. E. P. (2015). The U.S. Army Person-Event Data Environment: a Military–Civilian big data enterprise. *Big Data, 3*(2), 67–79. https://doi.org/10.1089/big.2014.0055

Zou, L., Wang, Z., Han, Q., & Yue, D. (2023). Tracking control under Round-Robin scheduling: Handling impulsive transmission outliers. *IEEE Transactions on Cybernetics, 53*(4), 2288–2300. https://doi.org/10.1109/tcyb.2021.3115459