Quarterly journal of strategic management attitude
Vol 3, No 3(11), autumn 2025
https://pmr.sndu.ac.ir

Type of Article: Reseach

An Analysis of Cyber OSINT: Dimensions, Consequences, and Countermeasures Against Ambiguous and Unknown Threats

Asghar Bayat[1] , Ebrahim Soltaninasab[2*] , Abdolah Dolatabadi[3]

Received: 2024/07/09 **PP: 133-168** **Accepted:** 2025/09/25

Abstract

In the contemporary era, publicly available data is generated and disseminated at an accelerating rate, making Open-Source Intelligence (OSINT) one of the most critical resources for security-related information collection and analysis. Although a substantial body of research has explored the applications of OSINT, its analysis within the framework of unknown threats has received comparatively less attention. This study aims to investigate the dimensions and implications of OSINT as an unknown threat, employing a descriptive-analytical research method and relying on library research and documentary analysis. The findings indicate that OSINT encompasses three key dimensions—operational, technological, and strategic—whose interplay can facilitate the emergence of unknown threats. At the operational level, challenges related to data collection, filtering, and validation may lead to the dissemination of inaccurate information. At the technological level, while the adoption of artificial intelligence and big data has enhanced analytical capabilities, it has also enabled large-scale misuse. At the strategic level, the absence of legal frameworks and analytical expertise can distort security decision-making processes. This study concludes that OSINT represents a security paradox, functioning both as an opportunity and a threat. The primary contribution of this research lies in proposing an integrated analytical framework that demonstrates how the inherent characteristics of OSINT—including its openness, velocity, and accessibility—can transform it into a breeding ground for unknown threats. Finally, practical strategies are suggested, including the development of legal frameworks, the enhancement of validation technologies, the training of specialized human resources, and the strengthening of inter-organizational cooperation.

KeyWords: Open-Source Intelligence (OSINT), Security, Unknown Threats.

Reference: Bayat, A., Soltaninasab, E. & Dolatabadi, A. (2025). An Analysis of Cyber OSINT: Dimensions, Consequences, and Countermeasures Against Ambiguous and Unknown Threats. *Strategic management attitude*, *3*(3), 133-168.
https://dor.isc.ac/dor/20.1001.1.30605865.1404.3.3.5.4

[1]. Ph.D, Department of Political sciences, Islamic Azad University, Shahreza, Isfahan, Iran. a.dolatabadi89@gmail.com

[2]. Corresponding author, Ph.D., Department of Future Studies Managment, Faculty of Strategic Management, University of Superme National Defence University, Tehran, Iran. E-mail: saeedsoltaninasab@gmail.com

[3]. Ph.D, Department of Social sciences and Sociology, Faculty of Literature, Humanities and Social Sciences, Science and Research Branch, Islamic Azad University, Tehran, Iran. E-mail: abdolah.dolatabadi@gmail.com

فصلنامه نگرش مدیریت راهبردی
سال ۳/ شماره ۳(۱۱)/ پاییز ۱۴۰۴
https://pmr.sndu.ac.ir/

نوع مقاله: پژوهشی

بررسی تحلیلی اطلاعات منبع باز با تأکید بر ابعاد و پیامدهای آن در چارچوب تهدیدات ناشناخته

اصغر بیات[۱]، ابراهیم سلطانی‌نسب[۲*] و عبداله دولت‌آبادی[۳]

دریافت: ۱۴۰۴/۰۴/۱۸ صص: ۱۳۲-۱۶۸ پذیرش: ۱۴۰۴/۰۷/۰۳

چکیده

در عصر کنونی که داده‌ها به‌سرعت تولید و منتشر می‌شوند، اطلاعات حاصل از منابع علنی به‌عنوان یکی از مهم‌ترین منابع جمع‌آوری و تحلیل اطلاعات امنیتی شناخته می‌شود. اهمیت اطلاعات حاصل از منابع علنی، نه‌تنها در شناسایی تهدیدات آشکار، بلکه در کشف الگوهای پنهان و ناشناخته‌ای است که می‌توانند ساختارهای امنیتی را تحت‌تأثیر قرار دهند. با وجود حجم گسترده مطالعات در زمینه کاربردهای اطلاعات حاصل از منابع علنی، بررسی تحلیلی آن در قالب یک تهدید ناشناخته کمتر مورد توجه قرار گرفته است و این امر شکاف مهمی در ادبیات علمی این حوزه ایجاد کرده است. این پژوهش با رویکرد مطالعات کتابخانه‌ای و تحلیل اسنادی به واکاوی مفهومی و نظری اطلاعات منبع باز پرداخته است و تلاش کرده ابعاد و پیامدهای آن را در چارچوب تهدیدات ناشناخته تحلیل کند. یافته های پژوهش نشان می دهد که اطلاعات منبع باز دارای سه بُعد عملیاتی، فناورانه و راهبردی است که در تعامل با یکدیگر می توانند به ایجاد تهدیدات ناشناخته منجر شوند. در بُعد عملیاتی، چالش‌های گردآوری، پالایش و صحت‌سنجی داده‌ها می‌تواند به انتشار اطلاعات نادرست منجر شود. در بُعد فناورانه، بهره گیری از هوش مصنوعی و کلان داده ها اگرچه توان تحلیل را افزایش داده، اما امکان سوءاستفاده در مقیاس بزرگ را نیز فراهم کرده است. در بُعد راهبردی، فقدان چارچوب های قانونی و تخصص تحلیلی می تواند تصمیم‌سازی امنیتی را مخدوش کند. مهم‌ترین نوآوری پژوهش، ارائه چارچوب تحلیلی یکپارچه‌ای است که نشان می‌دهد چگونه ویژگی‌های ذاتی اطلاعات منبع باز (باز بودن، سرعت و دسترسی آزاد) می تواند آن را به بستری برای تهدیدات ناشناخته تبدیل کند. در پایان، راه‌کارهای عملیاتی شامل تدوین چارچوب‌های قانونی، ارتقای فناوری‌های صحت‌سنجی، آموزش نیروی انسانی متخصص و تقویت همکاری‌های بین‌سازمانی پیشنهاد شده است. بنابراین، نتایج این مطالعه ضرورت بازنگری در سیاست‌ها و چارچوب‌های امنیتی موجود را آشکار می‌سازد و پیشنهاد می‌کند که نهادهای امنیتی و پژوهشی، دستورالعمل‌های دقیق‌تری برای بهره‌برداری ایمن از اطلاعات منبع باز تدوین کنند.

کلیدواژه‌ها: اطلاعات حاصل از منابع علنی، امنیت، تهدیدات ناشناخته.

استناددهی(APA): بیات، اصغر، سلطانی نسب، ابراهیم و دولت آبادی، عبدالله (۱۴۰۴). بررسی تحلیلی اطلاعات منبع باز با تأکید بر ابعاد و پیامدهای آن در چارچوب تهدیدات ناشناخته. *فصلنامه نگرش مدیریت راهبردی*،۳(۳)،۱۳۲-۱۶۸.
https://dor.isc.ac/dor/20.1001.1.30605865.1404.3.3.5.4

[۱]. دکتری، گروه علوم سیاسی، دانشگاه آزاد اسلامی، واحد شهرضا، اصفهان، ایران. رایانامه fn2020ke@gmail.com

[۲]. دکتری، گروه آینده پژوهی، دانشکده مدیریت راهبردی، دانشگاه عالی دفاع ملی، تهران، ایران(نویسنده مسئول). رایانامه: saeedsoltaninasab@gmail.com

[۳]. دکتری، گروه جامعه شناسی، دانشکده ادبیات و علوم انسانی و علوم اجتماعی، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران، ایران. رایانامه: abdolah.dolatabadi@gmail.com

مقدمه

در عصر اطلاعات، داده‌ها به‌عنوان سرمایه‌ای راهبردی شناخته می‌شوند که نه‌تنها بنیان تصمیم‌سازی‌های کلان را شکل می‌دهند، بلکه نقش تعیین‌کننده‌ای در معادلات امنیتی، سیاسی و حتی اقتصادی ایفا می‌کنند. در این میان، اطلاعات منبع باز[1] به‌عنوان یکی از مهم‌ترین و چالش‌برانگیزترین منابع اطلاعاتی، جایگاه ویژه‌ای در نظام‌های امنیتی و تحلیلی یافته است.

اطلاعات منبع باز با بهره‌گیری از داده‌هایی که از منابع عمومی، قانونی و قابل‌دسترس استخراج می‌شود، امکان شناسایی الگوهای رفتاری، تحلیل محیطی و پیش‌بینی تهدیدات را برای سازمان‌های امنیتی، اطلاعاتی و پژوهشی فراهم می‌آورد (هولنیک، ۲۰۲۳ و ناتو، ۲۰۰۶). با وجود این، ماهیت پیچیده، چندبُعدی و همواره در حال تحول اطلاعات منبع باز، آن را از یک ابزار صرفاً اطلاعاتی فراتر برده و به پدیده‌ای راهبردی بدل کرده است (هابز و موران، ۲۰۲۱ و شیرر و بِرد، ۲۰۲۳)؛ پدیده‌ای که همزمان می‌تواند عامل قدرت‌آفرینی برای سیستم‌های هوشمند تصمیم‌ساز باشد و بستری برای شکل‌گیری تهدیدات پیچیده و ناشناخته تلقی شود. درواقع، گستره فزاینده منابع متن‌باز، از شبکه‌های اجتماعی و رسانه‌های برخط گرفته تا پایگاه‌های داده عمومی، اگرچه مزیت‌هایی چون سرعت، دسترسی گسترده و هزینه پایین دارند، اما به همان میزان، خطرات پنهانی همچون نشر اطلاعات نادرست، سوءاستفاده بازیگران مخرب و گمراه‌سازی شناختی را نیز در خود نهفته دارند (واردل و درخشان، ۲۰۱۷ و آرنا، ۲۰۲۲). این پژوهش با رویکردی تحلیلی و بین‌رشته‌ای، در پی تبیین و بازشناسی نقش اطلاعات منبع باز در بستر تهدیدات ناشناخته[2] است. هدف اصلی پژوهش، آن است که با ترسیم ابعاد گوناگون اطلاعات منبع باز در سطوح عملیاتی، فناورانه و راهبردی، نحوه تأثیرگذاری آن بر فرایندهای شناخت تهدیدات و نیز امکان‌آفرینی آن در تولید تهدیدات پیش‌بینی‌ناپذیر را بررسی و تبیین کند. این تحقیق با بهره‌گیری از روش تحلیل اسنادی و مرور نقادانه ادبیات، به دنبال آن است که با فراتر رفتن از رویکردهای ابزاری رایج، نگاهی ساختاری و آینده‌نگر به مقوله اطلاعات منبع باز ارائه دهد. بدین‌ترتیب، مسئله‌محوری این پژوهش را می‌توان چنین صورت‌بندی کرد:

1. Open Source Intelligence - OSINT
2. Unknown Threats

«چگونه اطلاعات منبع باز، فراتر از یک ابزار گردآوری داده، به پدیده‌ای با ظرفیت دوگانه در مدیریت یا تشدید تهدیدات ناشناخته بدل می‌شود؟». این پرسش، نقطه آغاز این مطالعه برای تحلیل دقیق و علمی پیوند بین ظرفیت‌های اطلاعاتی متن‌باز و مخاطرات پنهان در بستر تحولات شتابان امنیتی است. درمجموع، مقاله کنونی با ترسیم پیوندی نظام‌مند میان ادبیات اطلاعات منبع باز و تهدیدات ناشناخته، تلاش دارد ضمن شناسایی شکاف‌های مفهومی موجود در مطالعات پیشین، چارچوبی نظری برای تحلیل آینده‌محور و راهبردی این پدیده در اختیار پژوهشگران، سیاست‌گذاران و تحلیلگران امنیتی قرار دهد. این چارچوب نه‌تنها می‌تواند در سیاست‌گذاری‌های اطلاعاتی و امنیتی مؤثر واقع شود، بلکه مسیرهای تازه‌ای برای تحقیقات بین‌رشته‌ای در حوزه‌های مطالعات امنیتی، داده‌کاوی و آینده‌پژوهی فراهم خواهد ساخت.

پیشینه و مبانی نظری

مفهوم اطلاعات منبع باز در متون علمی و امنیتی

از منظر مفهومی، اطلاعات منبع باز نه صرفاً «اطلاعات خام»، بلکه محصول یک چرخه اطلاعاتی است که شامل استخراج، پالایش، اعتبارسنجی، تحلیل و ارائه داده‌ها در قالب اطلاعات قابل‌اعتماد و تصمیم‌پذیر می‌شود. (کلارک، ۲۰۲۰ و ناتو، ۲۰۲۳). این چرخه، بر پایه الگوهای اطلاعاتی کلاسیک، ازجمله چرخه اطلاعاتی پنج‌مرحله‌ای (هدایت و تعیین نیازهای اطلاعاتی، گردآوری داده‌ها و اطلاعات، پردازش و ساماندهی، تحلیل و تفسیر اطلاعات و انتشار و اشاعه اطلاعات) که توسط جامعه اطلاعاتی ایالات متحده توسعه یافته است، صورت می‌گیرد (لونتال، ۲۰۱۶ و وزارت دفاع ایالات متحده آمریکا، ۲۰۲۰).

مقاله کنونی به بررسی تحلیلی اطلاعات منبع باز با تأکید بر ابعاد و پیامدهای آن در بستر تهدیدات ناشناخته می‌پردازد. اطلاعات منبع باز نه‌تنها یک ابزار گردآوری داده تلقی می‌شود، بلکه به‌مثابه یک پدیده راهبردی و چندوجهی نگریسته می‌شود که می‌تواند نقش دوجانبه‌ای ایفا کند: از یک‌سو، نقش تسهیل‌گر در افزایش آگاهی موقعیتی، پیش‌بینی تهدیدات، تحلیل محیط امنیتی و مقابله با بحران‌ها دارد و از سوی دیگر، در صورت عدم‌مدیریت صحیح یا بهره‌برداری خصمانه، می‌تواند بسترساز تهدیدات غیرمنتظره، حملات شناختی، عملیات فریب و گمراه‌سازی اطلاعاتی باشد. درواقع، پیشرفت‌های علم و فناوری، جمع‌آوری، تحلیل و توزیع سریع اطلاعات را امکان‌پذیر کرده است که تغییرات بی‌سابقه‌ای را در تمام جنبه‌های زندگی

بشر به همراه داشته است. با وجود این، سهولت دسترسی به اطلاعات عمومی به افزایش تصاعدی جرائم سایبری منجر شده است. به‌طور خاص، بازیگران تهدید مختلف از آسیب‌پذیری‌های سیستم‌های رایانه‌ای، شبکه‌ها و رفتار انسان برای انجام حملات سایبری در مقیاس بزرگ با استفاده از اطلاعات عمومی استفاده می‌کنند. در این زمینه، اطلاعات منبع باز (اطلاعات منبع باز) به‌عنوان ابزاری ضروری برای مبارزه با این تهدیدات سایبری ظهور کرده است (رحمان، ۲۰۲۵). در طول دهه گذشته، ظهور رسانه‌های اجتماعی و تلفن‌های هوشمند مجهز به دوربین، این روند را تسریع کرده است (فورد، ۲۰۲۳).

بنابراین، در این مطالعه، اطلاعات منبع باز به‌عنوان یک اکوسیستم اطلاعاتی با پیامدهای گسترده و چندلایه تعریف می‌شود که در تقاطع «فناوری– اطلاعات– امنیت– تهدید» قرار دارد. اطلاعات منبع باز در این معنا، صرفاً ابزار جمع‌آوری اطلاعات نیست، بلکه عاملی تأثیرگذار در بازتعریف مرزهای امنیت، شکل‌دهی به تهدیدات نوظهور و دگرگونی در فرایندهای تصمیم‌سازی امنیتی است. از همین منظر، بازشناسی علمی و نظام‌مند ابعاد آن در نسبت با تهدیدات ناشناخته، ضرورتی پژوهشی و راهبردی تلقی می‌شود.

سیر تاریخی:

تاریخچه اطلاعات منبع باز را می‌توان در قالب چهار دوره کلیدی تحلیل کرد: دوره‌هایی که نشان‌دهنده تحول تدریجی این مفهوم از ابزار اطلاعاتی ساده به یکی از مؤلفه‌های راهبردی امنیت ملی، اطلاعات رقابتی و تهدیدات نوظهور است (هابز، ۲۰۲۱، شیرر، ۲۰۲۳ و مؤسسه رند، ۲۰۲۰).

۱. دوره ابتدایی: استفاده سنتی از اطلاعات باز (پیش از قرن بیستم)؛ در دوران پیشامدرن، دولت‌ها، ارتش‌ها و بازرگانان، از منابع عمومی مانند خبرنامه‌ها، شایعات بازار، سفرنامه‌ها، مکاتبات دیپلماتیک و مشاهدات مسافران برای جمع‌آوری اطلاعات استفاده می‌کردند. این اطلاعات غالباً در قالب گزارش‌های شخصی یا تحلیل‌های کیفی و تجربی مورد بهره‌برداری قرار می‌گرفتند. در این دوره، هیچ مرز مفهومی دقیقی میان «اطلاعات عمومی» و «اطلاعات اطلاعاتی» وجود نداشت، اما اطلاعات باز به‌عنوان مکمل منابع سری مورد استفاده قرار می‌گرفت.

۲. دوره نظامی- اطلاعاتی: شکل‌گیری اطلاعات منبع باز به‌مثابه یک حوزه رسمی (قرن بیستم)؛ در طول جنگ جهانی دوم، به‌ویژه از دهه ۱۹۴۰، سازمان‌های اطلاعاتی کشورهای

بزرگ مانند دفتر خدمات راهبردی در ایالات متحده (سلف سازمان سیا) به تحلیل روزنامه‌ها، برنامه‌های رادیویی و گزارش‌های مطبوعاتی دشمن اقدام کردند. در همین راستا، نهادهایی مانند خدمات اطلاعاتی بخش‌های خارجی اداره تحقیقات فدرال آمریکا ایجاد شد که هدف آن رصد، ترجمه و تحلیل اطلاعات رسانه‌ای دشمنان بود. این فعالیت‌ها، نخستین گام در نهادینه‌سازی اطلاعات منبع باز به‌عنوان رشته‌ای نظام‌مند و کاربردی به‌شُمار می‌آید.

۳. دوره اطلاعات رقابتی و انقلاب دیجیتال (۲۰۰۰-۱۹۸۰): با پیشرفت فناوری اطلاعات، گسترش پایگاه‌های داده عمومی، ظهور اینترنت و توسعه رسانه‌های الکترونیکی، ظرفیت اطلاعات منبع باز به شکل چشمگیری افزایش یافت. در دهه ۱۹۹۰، با افول جنگ سرد، تمرکز اطلاعات منبع باز از میدان‌های نظامی به سمت اطلاعات رقابتی، نظارت ژئوپلیتیکی، تحلیل بازار و مقابله با تروریسم بین‌الملل تغییر یافت. سازمان‌هایی مانند سیا به‌طور رسمی اهمیت اطلاعات حاصل از منابع علنی را به‌عنوان منبعی معادل منابع محرمانه مطرح کردند. در همین دوران، مفهوم «اطلاعات قابل‌استفاده از منابع باز» به صورت پُررنگ‌تری وارد ادبیات امنیتی شد.

۴. دوره نوین: عصر داده‌های کلان و تهدیدات ناشناخته (۲۰۰۰ تاکنون)؛ در دهه‌های اخیر، با رشد شبکه‌های اجتماعی، سکوهای مشارکتی، فضای وب[۲] و سپس وب[۳]، ظرفیت اطلاعات حاصل از منابع علنی نه‌تنها افزایش کمی و کیفی یافت، بلکه به یک منبع تهدید بالقوه نیز بدل شد.

اطلاعات منبع باز اکنون نه‌تنها برای جمع‌آوری اطلاعات توسط دولت‌ها، بلکه از سوی بازیگران غیردولتی، هکرها، گروه‌های تروریستی و فعالان سایبری مورد استفاده قرار می‌گیرد. در این دوره، استفاده از هوش مصنوعی، یادگیری ماشین، ربات‌های خزنده، تحلیل احساسات و گراف‌های ارتباطی باعث شده است تا پردازش اطلاعات حاصل از منابع علنی به سطوح پیشرفته‌تری از تحلیل شناختی و پیش‌بینی امنیتی برسد. همچنین، با ظهور پدیده‌هایی نظیر جنگ‌های شناختی، عملیات اطلاعات نادرست، دستکاری افکار عمومی و تهدیدات ناشناخته، مرز میان «اطلاعات» و «تهدید» در حوزه اطلاعات منبع باز به‌شدت تیره و مبهم شده است.

تحول اطلاعات منبع باز از یک ابزار کمک‌اطلاعاتی به یک عامل دوگانه (فرصت– تهدید)، بازتاب‌دهنده گذار مفهومی آن از سطح عملیاتی به سطح راهبردی است (شیرر، ۲۰۲۳ و مؤسسه رند، ۲۰۲۰). عصر کنونی، اطلاعات حاصل از منابع علنی نه فقط داده‌ای بی‌ضرر، بلکه

یک میدان نبرد اطلاعاتی پنهان است که در صورت سوءاستفاده یا بهره‌برداری هدفمند، می‌تواند زیرساخت‌های امنیت ملی، افکار عمومی و حتی ادراکات راهبردی جوامع را دگرگون کند (واردل و درخشان، ۲۰۱۷ و آرنا، ۲۰۲۲). ازهمین‌رو، تحلیل ابعاد و پیامدهای اطلاعات منبع باز در پیوند با تهدیدات ناشناخته، ضرورتی گریزناپذیر برای پژوهش‌های امنیتی پیشرفته به‌شُمار می‌رود (هابز، ۲۰۲۱ و وزارت دفاع ایالات متحده آمریکا، ۲۰۲۰).

ظهور اطلاعات منبع باز نشان‌دهنده تکامل شیوه‌های سنتی اطلاعات است: جمع‌آوری، پردازش، تحلیل و انتشار حجم زیادی از اطلاعات. در حالی که رشد نمایی داده‌های متن‌باز در حال تغییر شکل چشم‌انداز اطلاعات است، نه انقلابی در اطلاعات ایجاد می‌کند و نه آن را دموکراتیک می‌کند. در عوض، این امر بازیگران دولتی و غیردولتی را بر آن می‌دارد تا بررسی کنند که چگونه می‌توانند به بهترین نحو شیوه‌های اطلاعات منبع باز را ادغام کرده و سواد دیجیتالی را در جوامع خود افزایش دهند. چالش‌های اصلی اطلاعات منبع باز- اضافه بار اطلاعات، قابلیت اطمینان و نگرانی‌های قانونی و اخلاقی- همچنان با مسائل اطلاعاتی گسترده‌تر سازگار هستند (پوی ولده و رینزی، ۲۰۲۵).

۱. نقش اطلاعات منبع باز در جمع‌آوری اطلاعات: اطلاعات متن‌باز، به‌عنوان یکی از ارکان اصلی در ساختار نوین اطلاعاتی، جایگاهی راهبردی و کلیدی در فرایند جمع‌آوری داده‌ها ایفا می‌کند. این نوع از اطلاعات بر پایه منابع عمومی، قابل‌دسترس و قانونی استوار است که بدون نیاز به نفوذ یا عملیات‌های محرمانه، از محیط‌های باز استخراج می‌شود. این ویژگی، اطلاعات منبع باز را به ابزاری توانمند، سریع و مقرون‌به‌صرفه در محیط‌های اطلاعاتی تبدیل کرده است؛ به‌ویژه در شرایطی که دسترسی به اطلاعات طبقه‌بندی‌شده با محدودیت یا هزینه‌های بالا همراه است.

۲. جایگاه اطلاعات منبع باز در چرخه اطلاعات[1]: در چارچوب چرخه اطلاعاتی متداول که شامل مراحل «نیازسنجی»، «جمع‌آوری»، «پردازش»، «تحلیل» و «توزیع» است، نقش اطلاعات منبع باز به‌ویژه در مرحله جمع‌آوری اطلاعات برجسته و تعیین‌کننده است. بهره‌برداری از اطلاعات متن‌باز، امکان واکنش سریع‌تر، درک محیطی بهتر و دسترسی گسترده‌تری را نسبت به دیگر روش‌های اطلاعاتی فراهم می‌آورد. به‌عبارت دیگر، اطلاعات

1. Intelligence Cycle

منبع باز نه‌تنها مکمل سایر روش‌های اطلاعاتی، بلکه در برخی حوزه‌ها به‌عنوان منبع اصلی و کافی عمل می‌کند.

۳. مهم‌ترین منابع اطلاعات منبع باز در جمع‌آوری اطلاعات: منابع اطلاعاتی متن‌باز، گستره‌ای وسیع دارند و به صورت پیوسته در حال توسعه‌اند. مهم‌ترین آنها عبارت‌اند از:

- رسانه‌های خبری بین‌المللی و محلی[1]؛
- شبکه‌های اجتماعی و پیام‌رسان‌ها؛
- پایگاه‌های داده عمومی دولتی و غیردولتی؛
- وب‌گاه‌های داده‌باز و شفاف‌سازی اطلاعات[2]؛
- مقالات علمی، پایان‌نامه‌ها و منابع آکادمیک؛
- تصاویر ماهواره‌ای و نقشه‌های برخط؛
- وب‌گاه‌ها، ویکی‌ها و فروم‌های تخصصی.

این منابع نه‌تنها حجم عظیمی از داده را ارائه می‌دهند، بلکه اطلاعات متنوعی در سطوح مختلف (سیاسی، اقتصادی، اجتماعی، فرهنگی و ...) تولید می‌کنند که می‌تواند مبنای تحلیل‌های چندلایه و موقعیت‌محور باشد.

۴. مزیت‌های اطلاعات منبع باز در فرایند جمع‌آوری اطلاعات: استفاده از اطلاعات منبع باز نسبت به روش‌های سنتی و بسته اطلاعاتی دارای چند مزیت مهم است:

جدول ۱. مزیت‌های اطلاعات منبع باز در فرایند جمع‌آوری اطلاعات

مزیت	توضیح
دسترسی آزاد و گسترده	اطلاعات بدون نیاز به مجوزهای ویژه قابل‌استفاده هستند.
سرعت بالا در گردآوری	امکان پایش بلادرنگ اطلاعات و واکنش سریع به تحولات
هزینه پایین	برخلاف عملیات میدانی یا سایبری، بهره‌گیری از اطلاعات منبع باز غالباً کم‌هزینه است.
پوشش جغرافیایی و موضوعی وسیع	اطلاعات از مناطق و موضوعات متنوع و گسترده جمع‌آوری می‌شود.
قابلیت صحت‌سنجی متقابل	به‌علت منابع متعدد، امکان مقایسه و راستی‌آزمایی وجود دارد.
پتانسیل پیش‌بینی و هشدار زودهنگام	در تحلیل روندها و رفتارها نقش حیاتی دارد.

1. News Agencies
2. Open Data Platforms

این مزیت‌ها باعث شده‌اند تا نهادهای امنیتی، رسانه‌ها، تحلیل‌گران راهبردی و حتی شرکت‌های خصوصی به‌طور فزاینده‌ای به اطلاعات منبع باز به‌عنوان منبع اطلاعاتی مستقل و قدرتمند اتکا کنند.

۵. ابزارها و فناوری‌های پشتیبان اطلاعات منبع باز: با توسعه فناوری‌های هوش مصنوعی، یادگیری ماشین، کلان‌داده و جغرافیای مکانی، قدرت پردازشی و تحلیلی اطلاعات منبع باز به شکل قابل‌توجهی افزایش یافته است. امروزه ابزارهای تحلیل داده، پایش زنده شبکه‌های اجتماعی، استخراج خودکار کلیدواژه‌ها، تحلیل احساسات و سیستم‌های هشدار سریع در بستر اطلاعات منبع باز توسعه یافته‌اند. این ابزارها موجب تسهیل در مراحل جمع‌آوری، دسته‌بندی، پالایش و تفسیر اطلاعات شده‌اند و نقش انسان را در این فرایندها از حالت دستی به سطح راهبردی و تصمیم‌ساز ارتقا داده‌اند.

۶. ملاحظات بهره‌برداری از اطلاعات منبع باز: گرچه اطلاعات منبع باز مزایای زیادی دارد، اما استفاده مؤثر از آن نیازمند رعایت ملاحظاتی است:

نیاز به تحلیل زمینه‌ای و فرهنگی داده‌ها: تفسیر دقیق داده‌ها نیازمند شناخت زمینه‌های زبانی، اجتماعی و فرهنگی هر منطقه است.

چالش راستی‌آزمایی[1]: به‌علت آزاد بودن منابع، بررسی صحت و اصالت داده‌ها ضروری است.

کنترل حجم داده‌ها[2]: نیاز به فیلترگذاری و استخراج اطلاعات مهم از بین انبوه داده‌ها وجود دارد.

سوگیری الگوریتمی یا انسانی: تحلیل ناصحیح ممکن است به دلیل انتخاب سوگیرانه داده‌ها یا ابزارهای پردازشی رُخ دهد.

اطلاعات منبع باز امروزه یکی از مهم‌ترین و کاربردی‌ترین منابع جمع‌آوری اطلاعات به‌شُمار می‌رود. انعطاف‌پذیری، گستره پوشش، دسترسی سریع و هزینه پایین، این نوع اطلاعات را به ستون فقرات نظام‌های اطلاعاتی نوین تبدیل کرده است. با ارتقای ابزارهای فناورانه و بهره‌گیری هوشمندانه از منابع متن‌باز، اطلاعات منبع باز توانسته است نقش تعیین‌کننده‌ای در تحلیل محیط، پیش‌بینی روندها و پشتیبانی از تصمیم‌گیری ایفا کند. ازاین‌رو، در بسیاری از حوزه‌ها از تحلیل‌های بازار گرفته تا امنیت ملی، اطلاعات منبع باز دیگر یک گزینه نیست، بلکه یک ضرورت راهبردی است.

1. Verification
2. Data Overload

تهدیدات ناشناخته

تعریف تهدیدات ناشناخته: تهدیدات ناشناخته، گونه‌ای از تهدیدهای امنیتی هستند که ماهیت، منشأ، انگیزه، زمان و شیوه تحقق آنها مبهم یا نامشخص است. این تهدیدات اغلب در قالب رُخدادهایی ظاهر می‌شوند که: سابقه مشابهی در داده‌های امنیتی ندارند؛
یا از ابزارها و فناوری‌هایی استفاده می‌کنند که هنوز در مرحله ظهور[1] قرار دارند؛
یا از تلفیق چند عامل غیرمرتبط (مانند اطلاعات، هوش مصنوعی و روانشناسی اجتماعی) شکل می‌گیرند.

بنابراین، تهدیدات ناشناخته نه‌تنها در افق تهدیدهای آینده‌نگرانه مطرح‌اند، بلکه در حال حاضر نیز بخشی از واقعیت امنیتی جهان پیچیده امروز را تشکیل می‌دهند.

بنابر تعریفی دیگر، تهدید ناشناخته تهدیدی است که توانسته از کنترل‌های امنیتی موجود در سیستم مورد آماج، عبور کند، بدون اینکه هیچ یک از کنترلگرها، نشانه‌ای از وجود آن را شناسایی، دریافت و اعلام نمایند (سلطانی‌نسب، ۱۴۰۲).

ویژگی‌های اصلی تهدیدات ناشناخته

ویژگی‌های ذاتی این تهدیدات باعث می‌شود شناسایی، پیش‌بینی و مقابله با آنها بسیار دشوارتر از تهدیدات کلاسیک باشد. مهم‌ترین ویژگی‌های آنها عبارت‌اند از:

نامرئی‌بودن اولیه: در مراحل ابتدایی، این تهدیدات به دلیل ضعف سیگنال یا الگوگریزی، توسط سیستم‌های سنتی کشف نمی‌شوند.

عدم‌انطباق با الگوهای موجود: الگوهای تحلیل خطر، هشدار زودهنگام یا سیستم‌های پایش (مانیتورینگ)، اغلب از پیش‌فرض‌های تهدیدات شناخته‌شده بهره می‌گیرند. اما تهدیدات ناشناخته از این قالب‌ها تبعیت نمی‌کنند.

پیش‌بینی‌ناپذیر بودن پیامدها: گاهی منشأ تهدید قابل‌ردیابی است، اما اثرگذاری آن به دلیل طبیعت زنجیره‌ای، ترکیبی یا روانی، به‌شدت متغیر است.

پویایی بالا: تهدیدات ناشناخته معمولاً در محیط‌های ناپایدار، تغییرپذیر و چندسطحی[2] شکل می‌گیرند و ممکن است در مدت‌زمان کوتاه تغییر ماهیت دهند.

واکنش‌های امنیتی به تهدیدات ناشناخته

در برابر این نوع تهدیدات، رویکردهای سنتی کفایت ندارند. واکنش‌های مناسب شامل:

1. Emerging
2. Multi-domain

ایجاد سامانه‌های هشدار بر مبنای داده‌های ضعیف: سامانه‌هایی که می‌توانند ناهنجاری‌های کوچک و نامعمول را ردیابی کنند.

استفاده از اطلاعات منبع باز و تحلیل‌های بین‌رشته‌ای: داده‌های باز و تحلیل‌های ترکیبی از جامعه‌شناسی، روان‌شناسی، علوم داده و سیاست، می‌توانند سرنخ‌های پنهان تهدیدات ناشناخته را کشف کنند.

توانمندسازی سیستم‌های انعطاف‌پذیر و تاب‌آور: سازمان‌ها باید توانایی بازیابی سریع، سازگاری مداوم و اصلاح ساختار در مواجهه با بحران‌های پیش‌بینی‌نشده را داشته باشند.

تهدیدات ناشناخته، بیش از آنکه صرفاً یک نوع تهدید باشند، نشانگر محدودیت‌های درک و پیش‌بینی در عصر داده‌محور و پیچیده امروز هستند. این تهدیدات:

نیازمند بازاندیشی در الگوواره‌های امنیتی؛

توسعه ابزارهای تحلیلی نوین (مانند هوش مصنوعی تطبیقی و تحلیل بلادرنگ اطلاعات باز)؛

و پذیرش رویکردهای منعطف، تطبیقی و چندلایه در سیاست‌گذاری امنیتی هستند.

مواجهه موفق با تهدیدات ناشناخته، نه در حذف آن‌ها، بلکه در افزایش ظرفیت‌های تاب‌آوری و آگاهی موقعیتی پیوسته خلاصه می‌شود؛ جایی که اطلاعات منبع باز، آینده‌پژوهی و تحلیل‌های ترکیبی، به‌مثابه اجزای اصلی پاسخ امنیتی نوین ایفای نقش می‌کنند.

رابطه اطلاعات منبع باز با امنیت و تهدیدات

نسبت مفهومی اطلاعات منبع باز با امنیت و تهدیدات

اطلاعات منبع باز یا اطلاعات متن‌باز، به داده‌هایی گفته می‌شود که به صورت قانونی، آزاد و دردسترس عموم قرار دارد و با روش‌های تحلیلی و استخراجی، به اطلاعات دارای ارزش امنیتی و راهبردی تبدیل می‌شود. این نوع اطلاعات:

منشأشان منابع باز مانند اینترنت، رسانه‌ها، مطبوعات، شبکه‌های اجتماعی، پایگاه‌های داده علمی و غیره هستند؛

اما ارزش آنها در تحلیل، ترکیب، تفسیر و به‌کارگیری در زمینه‌های امنیتی، نظامی، سیاسی، اقتصادی و اجتماعی نهفته است.

از این منظر، اطلاعات منبع باز در تعامل مستقیم با ساحت‌های گوناگون امنیت قرار دارد؛ زیرا هم ابزار پایش و پیش‌بینی تهدیدات است و هم در صورت بهره‌برداری مخرب، می‌تواند منشأ تهدیدات جدیدی ازجمله تهدیدات ناشناخته باشد.

نقش اطلاعات منبع باز در ارتقای امنیت

افزایش آگاهی موقعیتی[1]: اطلاعات منبع باز با ارائه تصویری چندلایه و روزآمد از محیط، به نهادهای امنیتی این امکان را می‌دهد که تهدیدات در حال ظهور را زودتر شناسایی کرده و اقدامات پیش‌دستانه انجام دهند.

پشتیبانی از تصمیم‌گیری راهبردی: اطلاعات حاصل از منابع علنی می‌تواند در تحلیل محیط عملیاتی، فضای رسانه‌ای، رفتار جمعی، تحولات منطقه‌ای و تحلیل بازیگران غیردولتی، برای تصمیم‌گیران سطح ملی و سازمانی بسیار مؤثر باشد.

ارزیابی تهدیدات هیبریدی و پنهان: در دنیای امروز که تهدیدات امنیتی به‌شدت ترکیبی شده‌اند، اطلاعات منبع باز ابزار مؤثری برای ردیابی سیگنال‌های اولیه، تحلیل نیت دشمن، شناسایی عملیات شناختی یا ارزیابی مخاطرات سایبری به‌شُمار می‌رود.

پایش شبکه‌های اجتماعی برای تحلیل رفتار اجتماعی: اطلاعات منبع باز به سازمان‌های امنیتی این توان را می‌دهد تا از طریق تحلیل روندهای اجتماعی، پویش‌های اطلاعاتی و حرکت‌های جمعی، نشانه‌های بحران یا نارضایتی‌های اجتماعی را در مراحل اولیه شناسایی کنند.

نسبت اطلاعات منبع باز با تهدیدات ناشناخته

تهدیدات ناشناخته از ویژگی‌هایی چون غیرخطی‌بودن، ضعف سیگنال، الگوگریزی و چندلایه‌بودن برخوردارند. در این‌جا اطلاعات منبع باز همزمان می‌تواند ابزار کشف و تحلیل اولیه نشانه‌های این تهدیدات باشد و نیز بستر ظهور خود این تهدیدات از طریق سوءاستفاده بازیگران غیردولتی، هکرها، تروریست‌ها یا حتی دولت‌های متخاصم باشد.

رادار تهدیدات ناشناخته

با رصد گسترده داده‌های باز و بهره‌گیری از ابزارهای نوین مانند هوش مصنوعی، تحلیل کلان‌داده و شبیه‌سازی‌های آینده‌نگر، اطلاعات منبع باز می‌تواند هم رفتارهای غیرمعمول در فضای سایبری را کشف کند و زنجیره‌های پیچیده ارتباطی را در شبکه‌های پنهان ردیابی کند و درنهایت الگوهای پنهان در تحولات امنیتی را آشکار سازد.

1. Situational Awareness

بستر تهدیدسازی

از سوی دیگر، اطلاعات منبع باز به‌دلیل ذات شفاف و عمومی خود، می‌تواند خود منشأ انتشار اطلاعات غلط[1] باشد و به دلیل ماهیت و گستردگی خویش، افزون‌بر اینکه به‌عنوان ابزار جنگ‌های شناختی و عملیات روانی مورد استفاده قرار گیرد، در تکنیک‌های مهندسی اجتماعی به‌کار رفته و به سبب سیالیتش موجب نشت اطلاعات حساس شود.

ظرفیت دوگانه اطلاعات منبع باز در امنیت نوین

اطلاعات منبع باز یک ابزار دوجنبه‌ای (Dual-Use) به‌شُمار می‌رود. همان‌گونه که می‌تواند به پیشگیری از تهدیدات کمک کند، می‌تواند در صورت عدم‌مدیریت یا رگولاتوری مناسب، به تهدید جدی تبدیل شود. این ظرفیت دوگانه را می‌توان چنین جمع‌بندی کرد:

جدول ۲. ظرفیت دوگانه اطلاعات منبع باز در امنیت نوین

نقش مثبت	نقش منفی
رصد و پیش‌بینی تهدیدات جدید	تسهیل جاسوسی باز و هدفمند
تقویت پاسخ سریع امنیتی	ترویج اطلاعات جعلی و نادرست
هشدار زودهنگام	نشت تدریجی اطلاعات حیاتی
تحلیل افکار عمومی	ابزار جنگ شناختی علیه دولت‌ها

رابطه اطلاعات منبع باز با امنیت و تهدیدات، رابطه‌ای چندلایه، ترکیبی و متناقض است. از یک‌سو، اطلاعات منبع باز ابزار قدرت‌مندی برای هوشمندسازی امنیت ملی، افزایش ظرفیت‌های پیش‌بینی و ارتقای آگاهی موقعیتی در عصر داده‌محور به‌شُمار می‌رود. از سوی دیگر، اگر در معرض دستکاری، جعل داده، عملیات فریب یا سوءمدیریت قرار گیرد، می‌تواند بستر زایش تهدیدات پیچیده و ناشناخته شود. درواقع، اطلاعات منبع باز نه‌تنها یک ابزار فنی، بلکه یک «فضای نبرد جدید» در امنیت آینده است.

در این پژوهش، تلاش شده است تا با تمرکز بر دو مفهوم کلیدی یعنی اطلاعات منبع باز و تهدیدات ناشناخته، یک الگوی مفهومی طراحی شود که روابط متقابل این دو را روشن کند. در چارچوب‌های سنتی، اطلاعات منبع باز صرفاً به‌عنوان ابزار جمع‌آوری و تحلیل اطلاعات در نظر گرفته می‌شود، اما در این پژوهش، اطلاعات منبع باز به‌مثابه پدیده‌ای دووجهی در نظر گرفته شده است که می‌تواند همزمان هم به‌عنوان ابزار شناسایی تهدیدات و هم به‌عنوان بستر بالقوه تهدیدات ناشناخته ایفای نقش کند.

[1] Disinformation

بر مبنای مرور ادبیات، چهار مؤلفه اصلی در تعامل اطلاعات منبع باز و تهدیدات ناشناخته شناسایی شده است:

سطح جمع‌آوری اطلاعات: میزان و کیفیت داده‌های متن‌باز گردآوری‌شده از منابع مختلف؛

سطح تحلیل و صحت‌سنجی: فرایندهای تحلیلی که اطلاعات خام را به دانش قابل‌استفاده امنیتی تبدیل می‌کند؛

سطح فرصت‌ها و مزایا: قابلیت‌های اطلاعات منبع باز در پیش‌بینی، پیشگیری و مقابله با تهدیدات نوظهور؛

سطح تهدیدات بالقوه: امکان سوءاستفاده از داده‌های متن‌باز برای ایجاد، گسترش یا پنهان‌سازی تهدیدات ناشناخته.

در این الگوی مفهومی، اطلاعات منبع باز در مرکز قرار می‌گیرد و دو مسیر اصلی از آن منشعب می‌شود: مسیر اول، به سوی افزایش امنیت و آگاهی موقعیتی حرکت می‌کند و مسیر دوم، به سوی افزایش خطر و شکل‌گیری تهدیدات ناشناخته هدایت می‌شود. نقش اصلی تحلیلگر یا سازمان امنیتی در این الگو، مدیریت و کنترل تعادل میان این دو مسیر است.

شکل ۱. نمودار مفهومی اطلاعات منبع باز

این نمودار نشان می‌دهد که اطلاعات منبع باز از یک سو می‌تواند به تقویت امنیت و شناسایی تهدیدات کمک کند و از سوی دیگر، در صورت سوءمدیریت یا بهره‌برداری خصمانه، به بستر ظهور تهدیدات ناشناخته تبدیل شود.

نوآوری این مطالعه در چند محور اصلی به شرح ذیل متجلی می‌شود:

۱. ارائه چارچوب تحلیلی یکپارچه برای تهدیدات ناشناخته

این پژوهش، سه بُعد عملیاتی، فناورانه و راهبردی اطلاعات منبع باز را در تعامل پویا با یکدیگر و در چارچوب مفهوم «ناشناختگی» مورد تحلیل قرار می‌دهد. چارچوب پیشنهادی، نشان می‌دهد که چگونه ضعف در یک بُعد (مانند خطای تحلیلی در بُعد فناورانه) می‌تواند به صورت آبشاری، ابعاد دیگر را تحت‌تأثیر قرار داده و به خلق تهدیدی پیش‌بینی‌ناپذیر بینجامد.

۲. تغییر الگوواره از اطلاعات منبع باز به عنوان «ابزار» به «بستر تهدید»

نوآوری بنیادین این مقاله، در تغییر نگرش از اطلاعات منبع باز به‌عنوان یک ابزار جمع‌آوری اطلاعات، به دیدگاهی جامع‌نگر است که آن را به یک بستر اکوسیستمی برای ظهور و رشد تهدیدات ناشناخته تبدیل می‌کند. این تحلیل نشان می‌دهد که ماهیت باز، غیرمتمرکز و دردسترس بودن داده‌های علنی، خود به‌عنوان یک «آسیب‌پذیری ساختاری» عمل می‌کند که می‌تواند توسط بازیگران دولتی و غیردولتی با اهداف خرابکارانه به‌کار گرفته شود.

۳. معرفی و تبیین شاخص‌های «ناشناختگی» در حوزه اطلاعات منبع باز

این مطالعه به صورت پیشگامانه، شاخص‌هایی را برای سنجش و شناسایی ظرفیت تهدیدزایی ناشناخته در اطلاعات منبع باز ارائه می‌دهد. این شاخص‌ها شامل پیش‌بینی‌ناپذیری (برآمده از حجم و سرعت داده‌ها)، عدم‌قطعیت تحلیلی (ناشی از مشکل صحت‌سنجی) و تعدد و ناشناسی بازیگران است که در کنار هم، اطلاعات منبع باز را از یک محیط اطلاعاتی کنترل‌پذیر، به یک محیط پیچیده و خطرخیز تبدیل می‌کنند.

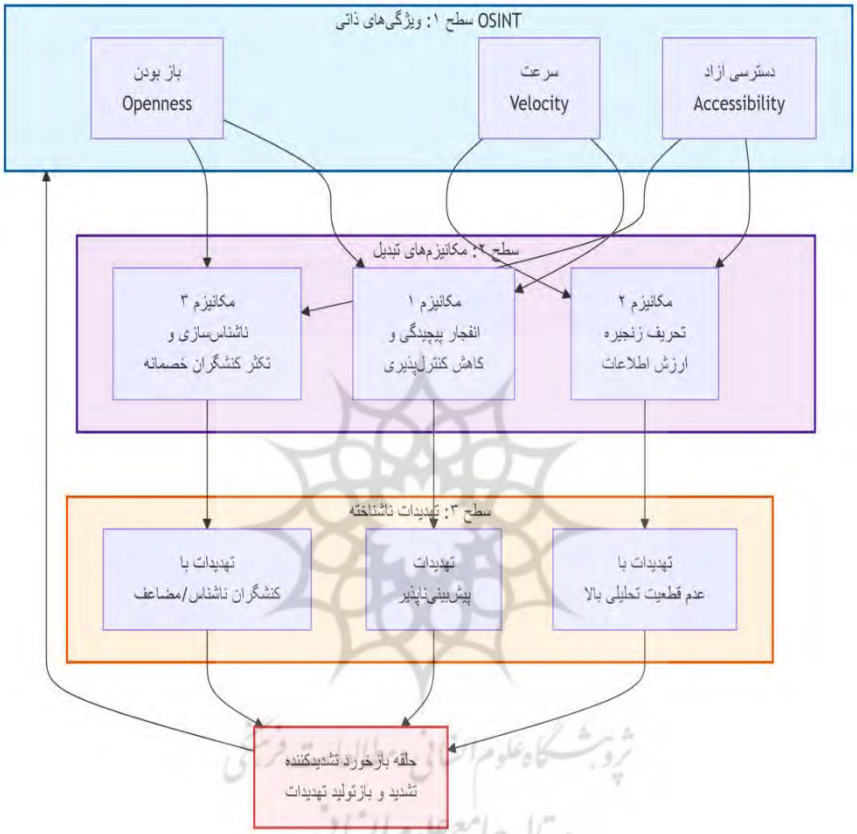
۴. تدوین الگوی مفهومی «چرخه تبدیل تهدید بالقوه به بالفعل»

این پژوهش یک الگوی مفهومی جدید ارائه می‌کند که مراحل تبدیل اطلاعات منبع باز از یک فرصت اطلاعاتی به یک تهدید امنیتی را ترسیم می‌کند. این چرخه با سوءاستفاده بازیگران خصمانه از داده‌های علنی آغاز شده و از طریق تولید اطلاعات نادرست، تحریف تحلیلی و درنهایت تأثیرگذاری بر تصمیم‌سازی راهبردی، تکمیل می‌شود. این الگو، درک نظام‌مندی از سازوکار شکل‌گیری تهدید ارائه می‌دهد.

۵. پیوند دادن چالش‌های فنی اطلاعات منبع باز به پیامدهای راهبردی کلان

برخلاف مطالعاتی که چالش‌های اطلاعات منبع باز را عمدتاً در سطح فنی می‌نگرند، این مقاله به صورت نوآورانه، این چالش‌ها را به صورت مستقیم به امنیت ملی و سازمانی پیوند می‌زند و نشان می‌دهد که چگونه یک خطای تحلیلی ساده در پردازش داده‌های علنی می‌تواند به یک بحران راهبردی با ابعاد گسترده منجر شود.

این نوآوری‌ها، مجموعاً این پژوهش را از حالت توصیفی صرف خارج کرده و آن را به یک مطالعه راهبردی و پیشرو تبدیل می‌کند که می‌تواند مبنای مناسبی برای تدوین سیاست‌های امنیتی، طراحی شیوه‌نامه‌های عملیاتی ایمن و انجام تحقیقات آتی در این حوزه حساس باشد.



شکل ۲. چارچوب تحلیلی ویژگی‌های ذاتی اطلاعات منبع باز به‌مثابه بستری برای تهدیدات ناشناخته

روش تحقیق

این پژوهش از نظر ماهیت، توصیفی- تحلیلی و از نظر روش گردآوری اطلاعات، مبتنی‌بر مطالعات کتابخانه‌ای و بررسی اسنادی است. داده‌ها و اطلاعات موردنیاز از طریق مطالعه منابع معتبر داخلی و خارجی، ازجمله کتاب‌های علمی، مقالات پژوهشی منتشرشده در مجلات معتبر (به‌ویژه مجلات کیو ۱ و مؤسسه اطلاعات علمی ISI)، گزارش‌های سازمان‌های بین‌المللی و نهادهای امنیتی و اسناد سیاستی گردآوری شده است. تمرکز اصلی بر آثار

منتشرشده در پنج تا ده سال اخیر بوده است تا ضمن بهره‌گیری از یافته‌های روزآمد، مبانی نظری کلاسیک نیز در نظر گرفته شود. اطلاعات گردآوری‌شده با روش تحلیل محتوای کیفی و استنتاج نظری مورد بررسی قرار گرفته است. در این فرایند، ابتدا مفاهیم و چارچوب‌های ارائه‌شده درباره اطلاعات منبع باز و تهدیدات ناشناخته استخراج و دسته‌بندی شده‌اند. سپس از طریق مقایسه تحلیلی[1]، نقاط هم‌پوشانی و تفاوت‌های این مفاهیم شناسایی و الگوی مفهومی پیشنهادی تدوین شده است.

فرایند اجرای تحقیق شامل مراحل زیر است:

۱. مرحله گردآوری داده‌ها

داده‌ها و اطلاعات موردنیاز از طریق بررسی نظام‌مند منابع معتبر داخلی و خارجی گردآوری شد. ابزارهای اصلی گردآوری در این مرحله شامل:

فهرست‌های پیشرفته کتابخانه‌ای: جست‌وجو در پایگاه‌های علمی مانند ScienceDirect، IEEE Xplore، Springer Link و SAGE Journals؛

پایگاه‌های اطلاعاتی مقالات: استفاده از پایگاه‌های ISI/Web of Science، Scopus، Google Scholar و PubMed برای دستیابی به مقالات ژورنالی؛

پایگاه‌های اطلاعاتی داخلی: جست‌وجو در پایگاه‌های پرتال جامع علوم انسانی، SID، Magiran، Civilica و Noormags؛

موتورهای جست‌وجوی تخصصی: استفاده از Google Scholar و Microsoft Academicبرای ردیابی استنادات و آثار مرتبط.

معیارهای انتخاب منابع

تمرکز بر مقالات پژوهشی منتشرشده در مجلات معتبر کیو ۱ و کیو ۲ و دارای رتبه ISI و Scopus؛

در نظرگیری کتاب‌های مرجع و تألیفی استادان برجسته در حوزه امنیت ملی، اطلاعات باز و جنگ سایبری؛

مطالعه گزارش‌های تحلیلی منتشرشده توسط نهادهای امنیتی و اندیشکده‌های معتبر بین‌المللی (مانند مؤسسه رند).

1. Comparative Analysis

محدودیت زمانی: اولویت با آثار منتشرشده در ده سال اخیر (۲۰۱۵ تا ۲۰۲۴) بوده است تا از روزآمدی تحلیل اطمینان حاصل شود. با وجود این، از مبانی نظری کلاسیک و مقالات شاخص قدیمی‌تر که به تعریف بنیادین مفاهیم پرداخته‌اند، نیز استفاده شده است.

در این مطالعه حدود ۴۵ مقاله مطالعه شد که پس از بررسی آنها، ۱۳ مورد از مقالات مرتبط با موضوع این پژوهش مورد استفاده قرار گرفت و در بخش‌های مختلف مطالعه به‌ویژه ادبیات پژوهش به‌کار گرفته شد.

۲. مرحله سازمان‌دهی و پالایش داده‌ها

پس از گردآوری اولیه، منابع سازمان‌دهی شدند. در این مرحله، منابع بر اساس معیارهای دارای ارتباط مستقیم با پرسش تحقیق، اعتبار منبع و تازگی پالایش و اولویت‌بندی نهایی شدند.

۳. مرحله تحلیل داده‌ها

در این مرحله از روش تحلیل محتوای کیفی با رویکرد استقرایی استفاده شد. فرایند تحلیل به شرح زیر بود:

این روش‌شناسی نظام‌مند، امکان درک عمیق از پدیده مورد مطالعه و ارائه تحلیلی نوآورانه از پیوند بین اطلاعات منبع باز و تهدیدات ناشناخته را فراهم کرده است.

یافته‌های تحقیق

یافته‌های این مطالعه در سه محور اصلی سامان یافته‌اند: ابعاد اطلاعات منبع باز در محیط‌های امنیتی، پیامدهای اطلاعات منبع باز در شکل‌گیری تهدیدات ناشناخته و تقاطع و تعامل اطلاعات منبع باز با تهدیدات ناشناخته. تحلیل‌ها به صورت توصیفی– تحلیلی و بر پایه منابع علمی و گزارش‌های معتبر امنیتی انجام شده‌اند.

۱. ابعاد اطلاعات منبع باز در محیط‌های امنیتی

در محیط‌های امنیتی، اطلاعات منبع باز به‌عنوان ابزاری حیاتی برای شناسایی تهدیدات، ارزیابی خطرها و پشتیبانی از فرایند تصمیم‌گیری عمل می‌کند. ابعاد مختلف اطلاعات منبع باز نه‌تنها ماهیت آن را مشخص می‌سازند، بلکه تعیین می‌کنند چگونه می‌توان این ظرفیت را به صورت مؤثر در معماری امنیت ملی، نظامی و سایبری به‌کار گرفت. این ابعاد شامل بُعد

عملیاتی، بُعد فناورانه و بُعد راهبردی هستند که هر کدام نقش منحصربه‌فردی در چرخه اطلاعاتی دارند.

۱. بُعد عملیاتی

بُعد عملیاتی اطلاعات منبع باز ناظر بر چرخه اصلی کار اطلاعاتی است که از مرحله جمع‌آوری تا ارزیابی و صحت‌سنجی داده‌ها ادامه می‌یابد. این چرخه شامل سه مرحله کلیدی است:

۱-۱. گردآوری داده‌ها

در این مرحله، داده‌ها از منابع آشکار و عمومی نظیر رسانه‌ها، شبکه‌های اجتماعی، پایگاه‌های داده باز، گزارش‌های علمی، وب‌گاه‌های دولتی و حتی داده‌های جغرافیایی و تصویری استخراج می‌شود. نکته اساسی در این فرایند، گستره و تنوع منابع است که به تحلیل‌گر اجازه می‌دهد تصویر کامل‌تر و دقیق‌تری از موضوع هدف به‌دست آورد.

۱-۲. پردازش و پالایش داده‌ها

پس از جمع‌آوری، داده‌ها خام و پراکنده هستند و ممکن است حاوی اختلال اطلاعاتی یا داده‌های زائد باشند. در این مرحله، داده‌ها از نظر قالب، ساختار و محتوای غیرمرتبط پالایش می‌شوند. استفاده از فیلترهای معنایی، روش‌های طبقه‌بندی و استانداردسازی داده‌ها ازجمله اقدامات کلیدی این گام است.

۱-۳. صحت‌سنجی و ارزیابی اعتبار

اعتبارسنجی داده‌ها در محیط‌های امنیتی حیاتی است؛ چراکه اطلاعات نادرست یا جعلی می‌تواند تصمیمات امنیتی را منحرف کند. این مرحله شامل تطبیق داده‌ها با منابع معتبر، تحلیل همگرایی یا تضاد اطلاعات و بهره‌گیری از شاخص‌های اعتمادپذیری است.

۲. بُعد فناورانه

بُعد فناورانه اطلاعات منبع باز بر ابزارها، فناوری‌ها و زیرساخت‌هایی متمرکز است که امکان بهره‌برداری مؤثر از داده‌ها را فراهم می‌کنند. این بُعد نقش حیاتی در سرعت، دقت و مقیاس‌پذیری تحلیل‌های اطلاعاتی دارد.

۲-۱. سکوهای تخصصی

این سکوها مجموعه‌ای از نرم‌افزارها و سیستم‌ها هستند که عملیات گردآوری، پردازش و تحلیل داده‌ها را تسهیل می‌کنند. نمونه‌ها شامل ابزارهای جست‌وجوی پیشرفته، سامانه‌های

پایش شبکه‌های اجتماعی و موتورهای کاوش تخصصی در وب است. در صوروت عدم رعایت، مقاله برای اصلاح به شما برگردانده می‌شود. نمونه:

۲-۲. هوش مصنوعی و یادگیری ماشین

تکنیک‌های هوش مصنوعی و یادگیری ماشین، نقش فزاینده‌ای در شناسایی الگوها، تشخیص ناهنجاری‌ها و پیش‌بینی رفتارهای احتمالی دارند. این فناوری‌ها می‌توانند حجم عظیمی از داده‌ها را در زمان بسیار کوتاه تحلیل و طبقه‌بندی کنند که برای مدیریت تهدیدات نوظهور مهم است.

۲-۳. زیرساخت‌های پردازش کلان‌داده

حجم و تنوع داده‌های اطلاعات منبع باز ایجاب می‌کند که از زیرساخت‌های کلان‌داده بهره گرفته شود. این زیرساخت‌ها، امکان ذخیره‌سازی گسترده، پردازش موازی و تحلیل بلادرنگ را فراهم می‌آورند.

۳. بُعد راهبردی

بُعد راهبردی اطلاعات منبع باز بر نقش آن در هدایت تصمیمات کلان امنیتی و برنامه‌ریزی بلندمدت تمرکز دارد. این بُعد باعث می‌شود اطلاعات جمع‌آوری‌شده، نه تنها در سطح راه‌کنشی (تاکتیکی)، بلکه در چارچوب کلان امنیت ملی و بین‌المللی به‌کار گرفته شود.

۳-۱. پشتیبانی از تصمیم‌سازی

اطلاعات اطلاعات منبع باز به تصمیم‌گیران این امکان را می‌دهد که گزینه‌های راهبردی خود را بر اساس داده‌های واقعی، روزآمد و جامع ارزیابی کنند. این پشتیبانی می‌تواند در حوزه‌های سیاست خارجی، امنیت سایبری و مدیریت بحران حیاتی باشد.

۳-۲. افق‌نگری و آینده‌پژوهی

با تحلیل روندها و الگوهای موجود در داده‌های اطلاعات منبع باز، می‌توان پیش‌بینی‌هایی درباره تحولات آتی انجام داد. این رویکرد آینده‌نگر به نهادهای امنیتی کمک می‌کند تا در برابر تهدیدات بالقوه آماده باشند و راه‌کارهای پیشگیرانه تدوین کنند.

۳-۳. سیاستگذاری امنیتی

اطلاعات به‌دست‌آمده از اطلاعات منبع باز می‌تواند مبنای تدوین و اصلاح سیاست‌های امنیتی در سطح ملی و بین‌المللی باشد. این سیاستگذاری شامل تعیین اولویت‌های امنیتی، تخصیص منابع و ایجاد چارچوب‌های همکاری بین‌سازمانی است.

۲. پیامدهای اطلاعات منبع باز در شکل‌گیری تهدیدات ناشناخته

اطلاعات منبع باز یا «اطلاعات متن‌باز» به‌دلیل ماهیت گسترده، پویا و روزآمد خود، می‌تواند نقشی دوگانه در محیط‌های امنیتی ایفا کند. از یک سو، این قابلیت را دارد که با گردآوری و پردازش داده‌های عمومی، آگاهی موقعیتی را برای نهادهای امنیتی ارتقا دهد و از بروز بسیاری از تهدیدات جلوگیری کند. اما از سوی دیگر، همین دسترسی گسترده به داده‌های باز، اگر در اختیار بازیگران مخرب قرار گیرد، می‌تواند زمینه‌ساز ایجاد و تشدید تهدیدات ناشناخته شود. درواقع، ماهیت تهدیدات ناشناخته به گونه‌ای است که منبع، الگو و حتی زمان وقوع آنها به سادگی قابل پیش‌بینی نیست و همین امر باعث می‌شود که کارکرد دوگانه اطلاعات منبع باز در این حوزه، اهمیت دوچندان پیدا کند.

۱. فرصت‌ها

فرصت‌های ناشی از به‌کارگیری اطلاعات منبع باز در حوزه تهدیدات ناشناخته شامل موارد زیر است:

افزایش آگاهی موقعیتی: با تجمیع داده‌های متن‌باز از منابع متنوع (رسانه‌های اجتماعی، پایگاه‌های خبری، تصاویر ماهواره‌ای، گزارش‌های فنی و غیره)، سازمان‌های امنیتی می‌توانند دیدی جامع‌تر نسبت به محیط عملیاتی خود پیدا کنند. این وضعیت به شناسایی نقاط ضعف، الگوهای رفتاری و تغییرات محیطی کمک می‌کند.

شناسایی تهدیدات نوظهور: یکی از مهم‌ترین مزایای اطلاعات منبع باز، توانایی کشف زودهنگام نشانه‌های تهدیدات پیش از شکل‌گیری کامل آنهاست. برای نمونه، افزایش ناگهانی فعالیت‌های سایبری در یک منطقه خاص یا تغییر در الگوهای خرید تجهیزات خاص، می‌تواند نشانگر شکل‌گیری یک تهدید جدید باشد. این قابلیت، به‌ویژه در مقابله با تهدیدات ناشناخته، ارزش راهبردی بالایی دارد.

۲. چالش‌ها

با وجود فرصت‌های یادشده، استفاده از اطلاعات منبع باز در محیط تهدیدات ناشناخته با چالش‌های جدی همراه است:

سوءاستفاده از داده‌های باز: همان اطلاعاتی که برای تحلیل‌گران امنیتی ارزشمند است، می‌تواند توسط گروه‌های تروریستی، مجرمان سایبری یا دولت‌های متخاصم مورد بهره‌برداری

قرار گیرد. برای نمونه، داده‌های عمومی درباره زیرساخت‌های حیاتی ممکن است برای برنامه‌ریزی حملات هدفمند استفاده شوند.

ایجاد حملات پیش‌بینی‌ناپذیر: ترکیب داده‌های متن‌باز با تحلیل‌های پیشرفته می‌تواند به طراحی سناریوهای حملاتی منجر شود که پیش از وقوع، شناسایی آنها تقریباً غیرممکن باشد. این ویژگی، تهدیدات ناشناخته را خطرناک‌تر می‌کند، زیرا مهاجمان می‌توانند از مسیرهای غیرمعمول یا داده‌های کمتر رصدشده بهره ببرند.

۳. پیامدهای کوتاه‌مدت و بلندمدت

پیامدهای کوتاه‌مدت: شامل تأثیرات سریع و مستقیم بر محیط امنیتی است؛ مانند اختلال موقت در سیستم‌های حیاتی، ایجاد بی‌ثباتی در مناطق حساس یا شکل‌گیری موج‌های اطلاعاتی گمراه‌کننده. در این بازه، واکنش سریع و تحلیل لحظه‌ای داده‌ها، نقش کلیدی در کاهش خسارات دارد.

پیامدهای بلندمدت: به تغییرات ساختاری و پایدار در الگوهای امنیتی و تهدیدی اشاره دارد. استفاده مستمر و گسترده از اطلاعات منبع باز، اگر بدون کنترل‌های مناسب باشد، می‌تواند به شکل‌گیری الگوهای جدید تهدید و افزایش پیچیدگی محیط امنیتی منجر شود. همچنین در صورت سوءاستفاده مهاجمان از ظرفیت‌های اطلاعات منبع باز، نهادهای امنیتی در بلندمدت با چالش اعتماد به داده‌های عمومی و افزایش حجم حملات هدفمند مواجه خواهند شد.

درمجموع، اطلاعات منبع باز در شکل‌گیری تهدیدات ناشناخته هم نقش تسهیل‌گر و هم نقش بازدارنده دارد. بهره‌گیری هوشمندانه و متوازن از آن، همراه با سیاست‌های حفاظتی و شیوه‌های امنیتی دقیق، می‌تواند فرصت‌های این حوزه را به حداکثر و تهدیدات آن را به حداقل برساند.

۴. تقاطع اطلاعات منبع باز و تهدیدات ناشناخته؛ تحلیل انتقادی تبدیل اطلاعات منبع باز از «ابزار» به «تهدید»

در پژوهش کنونی، پس از تبیین ابعاد عملیاتی، فناورانه و راهبردی اطلاعات منبع باز و بررسی پیامدهای آن، لازم است رابطه عمیق و دوسویه میان اطلاعات منبع باز و «تهدیدات ناشناخته» به‌طور مجزا و نقّادانه مورد کنکاش قرار گیرد. این بخش تلاش می‌کند پیوندهای مفهومی و سازوکارهای عملی که اطلاعات منبع باز را هم‌زمان به ابزاری برای شناسایی تهدیدات و به بستری بالقوه برای تولید تهدیدات ناشناخته تبدیل می‌کنند، به صورت منظم،

مستدل و قابل‌اتکا تبیین کند. افزون‌بر این، شاخص‌ها و شرایطی که فرایند تبدیل اطلاعات منبع باز از «منبع اطلاعاتی» به «منشأ خطر» را تسهیل می‌کند، شناسایی و تحلیل می‌شوند.

۱. نقطه تلاقی: چگونه اطلاعات منبع باز با تهدیدات ناشناخته برخورد می‌کند؟

اطلاعات منبع باز و تهدیدات ناشناخته در یک میدان مفهومی و عملی به‌هم می‌رسند؛ جایی که داده‌های علنی حاملِ هر دو معنا هستند: هم سیگنال‌های ضعیف پیش‌میدان تهدید و هم مواد خامی که می‌توانند توسط کنش‌گران خصمانه به‌منزله ابزار حمله مورد استفاده قرار گیرند. این تقاطع را می‌توان در سه سطح مشاهده کرد:

کشف و آشکارسازی اطلاعات منبع باز: با رصد گسترده منابع باز امکان شناسایی نشانه‌های ضعیف، تغییرات ساختاری در رفتار بازیگران و ظهور الگوهای جدید را فراهم می‌کند؛ این توانایی به‌طور مستقیم به کاهش عدم‌قطعیت و ارتقای آگاهی موقعیتی کمک می‌کند.

تزریق و سوءاستفاده: همان داده‌های باز که برای مدافعان ارزشمند است، برای مهاجمان نیز ابزار طراحی و اجرا به‌شُمار می‌رود؛ از تحلیل ساختار شبکه تا استخراج داده‌های حساسِ پراکنده.

تغییر ماهیت تهدید: استفاده همزمان از اطلاعات منبع باز و فناوری‌های تحلیلی پیشرفته هوش مصنوعی، شبکه‌های گرافی و تجمیع کلان‌داده) می‌تواند به ظهور تهدیداتی منجر شود که الگوهای سنتی را دور می‌زنند- تهدیداتی که در ادبیات به‌عنوان «ناشناخته» توصیف می‌شوند.

این سه سطح نشان می‌دهد که اطلاعات منبع باز نه‌تنها در کشف، بلکه در پیدایش ساختاری و ماهیتی تهدیدات نقش دارد؛ بنابراین تقاطعِ یادشده ماهیتی پویاتر و پیچیده‌تر از رابطه یک‌طرفه «ابزار ← شناسایی» را متبادر می‌سازد.

۲. تحلیل انتقادی: شاخص‌های تبدیل اطلاعات منبع باز از ابزار به تهدید

بر اساس بررسی‌های نظری و مصادیق عملی (مطالعات موردی و گزارش‌های تحلیلی)، چهار شاخصِ کلیدی فرایند تبدیل را تسریع یا تسهیل می‌کنند.

۲.۱. فقدان چارچوب‌های قانونی و اخلاقی مشخص

در غیاب قوانین روشن درباره جمع‌آوری، ذخیره‌سازی، اشتراک‌گذاری و نشر داده‌های متن‌باز، مرز میان استفاده مشروع و سوءاستفاده خصمانه تار می‌شود. نبود ضوابط حقوقی و

سازوکارهای پاسخ‌گویی، امکانِ بهره‌برداری سازمان‌یافته از داده‌ها را برای بازیگران غیرمسئول تسهیل می‌کند.

نبود خطوط قرمز قانونی می‌تواند به ایجاد بازارهای خاکستری اطلاعات، تراکم داده‌های آسیب‌پذیر دردسترس عمومی و درنهایت طراحی عملیات پیچیده‌ای شود که از منظر پیشین قابل‌تشخیص نیست.

۲.۲. ضعف در صحت‌سنجی و اعتبارسنجی داده‌ها

اطلاعات منبع باز به‌واسطه تنوع و سرعت تولید، مستعد ورود داده‌های ناصحیح، دستکاری‌شده یا ازپیش‌طراحی‌شده برای فریب است. در صورت نبود شیوه‌نامه‌های صحت‌سنجی چندمنبعه و تکنیک‌های اعتبارسنجی نظام‌مند، تحلیلگران ممکن است بر پایه اطلاعات اشتباه، الگوهای غلط استخراج کنند. تحلیل نادرست می‌تواند به تصمیم‌سازی خطا و ایجاد نقاط آسیب‌پذیرِ نوین در ساختارهای دفاعی بینجامد؛ افزون‌بر این، مهاجمان می‌توانند با تزریق اطلاعات ساختگی، واکنش‌های مدافعان را هدایت و سازمان‌دهی کنند، رویدادی که خود مصداق تهدیدات ناشناخته است.

۲.۳. دسترسی گسترده بازیگران متخاصم

ماهیت باز منابع اطلاعات منبع باز به‌معنای دسترسی برابر یا تقریباً برابر همه کنش‌گران است. بازیگران بدخواه با بهره‌گیری از ابزارهای اتوماسیون، داده‌کاوی و تحلیل‌گر، می‌توانند اطلاعات پراکنده را تجمیع و به «نقشه آسیب‌پذیری[1]» تبدیل کنند. این دسترسی گسترده، امکان طراحی حملات هدفمند و چندلایه را فراهم می‌آورد که پیشتر نیازمند عملیات‌های پیچیده جمع‌آوری اطلاعات محرمانه بود؛ درنتیجه تهدیداتی پدید می‌آیند که برای سازوکارهای دفاعی مرسوم ناشناخته و غافلگیرکننده‌اند.

۲.۴. کمبود تخصص تحلیلی

تحلیل متون بزرگ، استخراج سیگنال‌های ضعیف و تفسیر زمینه‌ای نیازمند تخصص میان‌رشته‌ای (فنی، زبان‌شناسی، جامعه‌شناسی و حوزه‌محوری) است. فقدان نیروی انسانی آموزش‌دیده موجب می‌شود که سازمان‌ها به ابزارهای نیمه‌خودکار متکی شوند یا تحلیل‌های سطحی ارائه کنند.

[1]. vulnerability map

کمبود تخصص به خطاهای تفسیر، افراط در اعتماد به الگوهای جانبدار الگوریتمی و ناتوانی در تشخیص الگوهای نوظهور منجر می‌شود؛ این آسیب‌پذیری تحلیلی به مهاجمان امکان می‌دهد تا با راه‌کنش‌های نامتقارن، تهدیدات ناشناخته‌ای را توسعه دهند.

۳. شرایط و سازوکارهای تبدیل: از شاخص‌ها تا فرایند تهدیدزایی

ترکیب چهار شاخص یادشده می‌تواند فرایند تبدیل را تسریع کند. در سطح کلان، این فرایند را می‌توان در سه مرحله تشریح کرد:

تراکم داده و تجمیع: منابع متعدد باز بدون چارچوبِ محافظت یا هدایت، در قالب مخازن یا پایگاه‌های ترکیبی گرد می‌آیند.

تحلیل معکوس و نقشه‌برداری: بازیگران خصمانه با ابزارهای تحلیلی، داده‌ها را غربال و نقاط حساس را به‌دست می‌آورند.

عملیاتی‌سازی و فریب: با بهره‌گیری از نتایج تحلیل، سناریوهای حمله نوین (سایبری، شناختی و ترکیبی) طراحی می‌شود که به‌دلیل پنهانی و چندلایه بودن، در ابتدا «ناشناخته» باقی می‌مانند.

این چرخه نشان می‌دهد که کنترل ناقص بر هر یک از مراحل می‌تواند به خلق تهدیداتی منجر شود که نه‌تنها سیستم‌های دفاعی را دچار خطا می‌کند، بلکه اعتماد عمومی و انسجام راهبردی را نیز تضعیف می‌کند. بنابر تحلیل یادشده، پیامدهای راهبردی عبارت‌اند از افزایش پیچیدگی فضای تهدید، نیاز به بازتعریف معیارهای اعتماد اطلاعاتی و ضرورت ساختارهای میان‌بخشی برای مدیریت اکوسیستم داده‌های باز.

تجربه‌های جهانی

درک تجربیات سایر کشورها می‌تواند به طراحی راه‌کارهای عملی و آزمون‌شده در بستر ملی کمک کند. در ادامه، راه‌کارهای کلیدی کشورهای پیشرو و میزان موفقیت آنها بررسی می‌شود:

جدول ۳. تجربه سایر کشورها

نام کشور	راه‌کار محوری	نتیجه‌گیری و درس کلیدی
ایالات متحده	مراکز ادغام اطلاعات	یکپارچگی و استانداردسازی بین نهادهای امنیتی برای شکستن حفره‌های اطلاعاتی ضروری است (رولینز، ۲۰۱۰).
اتحادیه اروپا	چارچوب قانونی سخت‌گیرانه	قانون‌مندی و شفافیت، پیش‌نیاز جلب اعتماد عمومی استفاده مشروع از اطلاعات

نام کشور	راه‌کار محوری	نتیجه‌گیری و درس کلیدی
		منبع باز است (فویگت و فون دم بوشه، ۲۰۱۷).
رژیم صهیونیستی	نهادهای تخصصی و چابک در بدنه امنیتی	تخصصی‌سازی، نیروی انسانی نخبه و فرهنگ نوآوری، مزیت رقابتی اصلی در حوزه اطلاعات منبع باز است (کار، ۲۰۲۱ و برنتلی، ۲۰۱۸).
سنگاپور	راهبرد ملی هوشمند یکپارچه	اتخاذ یک نگرش کل‌نگر و برنامه‌ریزی بلندمدت برای هماهنگی بین ابعاد قانونی، فناوری و انسانی اطلاعات منبع باز حیاتی است (وزارت امور داخلی سنگاپور، ۲۰۲۰).

علل کم‌توجهی به ابعاد تهدیدزای اطلاعات منبع باز در ایران

۱. عوامل ساختاری و بوروکراتیک

تمرکز بر تهدیدات سنتی و سخت‌افزارمحور: ساختار امنیتی و دفاعی ایران به دلیل سابقه تاریخی (مانند جنگ تحمیلی) و تهدیدات منطقه‌ای، عمدتاً بر تهدیدات فیزیکی، نظامی و سخت‌افزاری متمرکز است. بودجه، منابع و تمرکز سیاست‌گذاران عمدتاً به این حوزه‌ها معطوف است و تهدیدات ناملموس و اطلاعاتی مانند اطلاعات منبع باز در اولویت پایین‌تری قرار می‌گیرند.

موازی کاری و فقدان نهاد متولی واحد: هیچ نهاد یا فرماندهی واحدی مسئولیت یکپارچه «مدیریت تهدیدات» اطلاعات منبع باز را بر عهده ندارد. فعالیت‌های پراکنده بین نهادهای مختلف امنیتی، اطلاعاتی و نظامی بدون هماهنگی مرکزی انجام می‌شود که به شکاف‌های امنیتی و نادیده‌گرفته‌شدن ابعاد کلان مسئله منجر می‌شود.

۲. عوامل فرهنگی- سازمانی

فرهنگ محرمانگی بالا و بی‌اعتمادی به داده‌های علنی: در فرهنگ امنیتی ایران، ارزش و اعتبار اصلی به اطلاعات «محرمانه» و «طبقه‌بندی‌شده» داده می‌شود. داده‌های علنی اغلب به‌عنوان اطلاعاتی «درجه دو»، «غیرقابل اعتماد» و کم‌ارزش تلقی می‌شوند. این نگرش، سرمایه‌گذاری جدی بر روی آن را توجیه‌ناپذیر می‌کند.

مقاومت در برابر تغییر و نوآوری: ساختارهای سلسله‌مراتبی و سنتی در برابر پذیرش روش‌های جدید اطلاعاتی که مبتنی‌بر چابکی، اشتراک‌گذاری داده و استفاده از فناوری‌های نوین هستند، مقاومت می‌کنند. «اینجا روال خودش را دارد»، یک مانع فرهنگی بزرگ است.

کمبود شدید نیروی انسانی متخصص و آموزش‌دیده: تربیت تحلیلگر اطلاعات منبع باز نیازمند ترکیبی از مهارت‌های زبان خارجی، تحلیل رسانه‌ای، علوم داده، هوش مصنوعی و درک راهبردی است. سیستم‌های آموزشی و جذب نیرو در ایران، عمدتاً برای پُرکردن این پروفایل شغلی پیچیده طراحی نشده‌اند.

۳. عوامل راهبردی و ادراکی

عدم درک «اکوسیستم تهدیدات» جدید: گذاران اغلب اطلاعات منبع باز را صرفاً به‌عنوان یک «ابزار» می‌بینند که می‌توان از آن برای جمع‌آوری اطلاعات استفاده کرد، اما درک نمی‌کنند که چگونه خود این محیط به یک «بستر تهدید» تبدیل شده است. آنها هنوز به‌طور کامل درنیافته‌اند که چگونه یک پویش اطلاعات نادرست طراحی‌شده در فضای مجازی می‌تواند امنیت ملی را به اندازه یک عملیات نظامی سنتی به‌خطر بیندازد.

تأخر راهبردی: ایران در حال تجربه «تأخر راهبردی» است؛ به این معنا که سرعت تحول در محیط تهدید (فضای سایبر)، اطلاعات منبع باز بسیار بیشتر از سرعت تطبیق راهبردها، رهنامه‌ها و ساختارهای امنیتی کشور است.

۴. عوامل فنی- عملیاتی

چالش زبان و بستر: حجم عظیم داده‌های اطلاعات منبع باز به زبان انگلیسی و در سکوهای غربی تولید می‌شود. فقدان ابزارهای پیشرفته «پردازش زبان فارسی» برای تحلیل مؤثر محتوای داخلی و همچنین محدودیت دسترسی به برخی سکوها، توانایی رصد جامع را کاهش می‌دهد.

تحلیل یافته‌ها

یافته‌های این پژوهش به‌طور جامع نشان می‌دهد که اطلاعات منبع باز به‌عنوان یک ابزار چندبُعدی در حوزه امنیت، دارای ابعاد عملیاتی، فناورانه و راهبردی است که هر یک نقش تعیین‌کننده‌ای در فرایندهای جمع‌آوری، پردازش و تحلیل داده‌های متن‌باز ایفا می‌کنند. بُعد عملیاتی، متشکل از مراحل گردآوری داده‌ها از منابع متنوع، پالایش و صحت‌سنجی اطلاعات، تضمین‌کننده کیفیت و اعتبار داده‌هاست؛ درحالی‌که بُعد فناورانه با بهره‌گیری از سکوهای

تخصصی، فناوری‌های هوش مصنوعی، یادگیری ماشین و زیرساخت‌های پردازش کلان‌داده، ظرفیت تحلیل داده‌های عظیم را به صورت دقیق و کارآمد فراهم می‌آورد. افزون‌بر این، بُعد راهبردی، نقش محوری در پشتیبانی از تصمیم‌سازی‌های امنیتی، افق‌نگری و سیاست‌گذاری امنیتی ایفا می‌کند و امکان توسعه راهبردهای انعطاف‌پذیر در مواجهه با پیچیدگی‌های فضای امنیتی را فراهم می‌کند.

با وجود این ظرفیت‌ها، پژوهش کنونی تأکید دارد که همزمان با فرصت‌های قابل‌توجه اطلاعات منبع باز در افزایش آگاهی موقعیتی و شناسایی تهدیدات نوظهور، چالش‌های مهمی نیز در این حوزه وجود دارد. ازجمله این چالش‌ها می‌توان به امکان سوءاستفاده بازیگران خصمانه از داده‌های باز برای طراحی حملات پیش‌بینی‌ناپذیر و پیچیده، نارسایی در فرایندهای صحت‌سنجی و اعتبارسنجی داده‌ها که می‌تواند به تحلیل‌های نادرست و تصمیم‌گیری‌های اشتباه منجر شود و همچنین پیچیدگی فزاینده فضای تهدیدات اشاره کرد که در بلندمدت می‌تواند به تضعیف اعتماد به داده‌های عمومی منجر شود. این موارد نشان می‌دهد که بهره‌برداری نامناسب از اطلاعات منبع باز می‌تواند خود عامل ایجاد تهدیدات ناشناخته شود.

در این پژوهش، اطلاعات منبع باز به‌عنوان مفهومی پیچیده و چندوجهی مورد تحلیل قرار گرفته است که در سه بُعد اصلی عملیاتی، فناورانه و راهبردی فعالیت می‌کند. بُعد عملیاتی شامل فرایندهای گردآوری، پالایش، صحت‌سنجی و اعتبارسنجی داده‌هاست که با هدف تضمین دقت و صحت اطلاعات به‌کار گرفته می‌شود. این موضوع با مطالعات اسمیت (۲۰۱۸) و جانسون و میلر (۲۰۲۰) هماهنگ است که صحت‌سنجی داده‌ها را به‌عنوان ستون فقرات هر سیستم اطلاعاتی برجسته کرده‌اند. بُعد فناورانه اطلاعات منبع باز، با استفاده از سکوهای تخصصی، هوش مصنوعی و یادگیری ماشین، امکان تحلیل داده‌های کلان با سرعت و دقت بالا را فراهم می‌آورد که این امر در مطالعات پیشرفته مانند گارسیا و همکاران (۲۰۲۲) مورد تأکید قرار گرفته است. درنهایت، بُعد راهبردی اطلاعات منبع باز در قالب پشتیبانی از تصمیم‌سازی، آینده‌پژوهی و سیاستگذاری امنیتی نقش کلیدی دارد که در مطالعات کلارک و لوییس (۲۰۲۱) و براون (۲۰۱۹) به آن اشاره شده است. یافته‌های پژوهش کنونی ضمن تأکید بر این ابعاد، به‌طور ویژه به خطرها و تهدیدات ناشناخته مرتبط با اطلاعات منبع باز پرداخته‌اند که در ادبیات موجود کمتر مورد توجه قرار گرفته است و ضرورت پرداختن به آن در عصر پیچیده امنیتی کنونی را روشن می‌سازد.

درنهایت، یافته‌های این پژوهش بر ضرورت اتخاذ رویکردی هوشمندانه، چندجانبه و آینده‌نگر در مدیریت اطلاعات منبع باز تأکید دارد تا ضمن حفظ مزایا و قابلیت‌های این ابزار حیاتی، مخاطرات بالقوه آن به حداقل برسد و جایگاه اطلاعات منبع باز در ساختارهای امنیتی به صورت پایدار تقویت شود.

تحقیقات پیشین عمدتاً بر کاربردهای مثبت و فرصت‌های توسعه اطلاعات منبع باز متمرکز بوده‌اند، مانند توانمندسازی تحلیلگران در افزایش آگاهی موقعیتی و بهبود تصمیم‌گیری (کلارک و لوییس، ۲۰۲۱ و میلر، ۲۰۱۷). اما با رشد روزافزون داده‌های متن‌باز و ابزارهای فناوری، برخی مطالعات جدید به چالش‌ها و خطرهای احتمالی اطلاعات منبع باز اشاره کرده‌اند (گارسیا و همکاران، ۲۰۲۲). این پژوهش، ضمن حفظ دیدگاه‌های مثبت، شکاف مهمی را پُر می‌کند و به تأثیر منفی احتمالی ضعف در صحت‌سنجی داده‌ها، نبود چارچوب‌های قانونی و دسترسی بی‌ضابطه بازیگران خصمانه می‌پردازد. این رویکرد ترکیبی، مقیاس پیچیدگی اطلاعات منبع باز و تأثیرات آن بر تهدیدات ناشناخته را به گونه‌ای بازتاب می‌دهد که در مطالعات پیشین کمتر دیده شده است. نوآوری اصلی این مقاله در ارائه یک چارچوب جامع است که ابعاد عملیاتی، فناورانه و راهبردی اطلاعات منبع باز را در بستر تهدیدات ناشناخته به صورت یکپارچه و نظام‌مند تحلیل می‌کند. برخلاف مطالعات گذشته که غالباً تمرکز محدود به فناوری یا کاربردهای خاص داشتند، این پژوهش به صورت تلفیقی به ابعاد قانونی، اخلاقی و آموزشی نیز توجه کرده است. این رویکرد چندجانبه، بر اهمیت توسعه چارچوب‌های قانونی، استانداردهای اخلاقی و آموزش تخصصی برای مقابله با تهدیدات ناشناخته ناشی از اطلاعات منبع باز تأکید می‌کند. افزون‌بر این، مطالعه کنونی ضمن شناسایی عوامل زمینه‌ساز تبدیل اطلاعات منبع باز از یک ابزار مفید به یک منبع بالقوه تهدید، به راه‌کارهای پیشگیری و مدیریت آن نیز اشاره می‌کند که این مسئله نوآوری عملی پژوهش را نشان می‌دهد.

ابعاد اخلاقی و قانونی در استفاده از اطلاعات منبع باز

در ادبیات امنیتی، فقدان چارچوب‌های قانونی و اخلاقی مناسب در جمع‌آوری و استفاده از داده‌های متن‌باز، یکی از موانع بزرگ مدیریت مؤثر اطلاعات منبع باز شناخته شده است (براون، ۲۰۱۹). این پژوهش بر لزوم تدوین قوانین ملی و بین‌المللی برای حفاظت از حریم خصوصی و جلوگیری از سوءاستفاده تأکید دارد. همچنین، رعایت اصول اخلاقی در تحلیل و

انتشار داده‌ها به‌منظور حفظ اعتماد عمومی و جلوگیری از تشدید تهدیدات ناشناخته، یکی از محورهای مهم مقاله است.

اهمیت آموزش و تخصص تحلیلی در مدیریت اطلاعات منبع باز

نیروی انسانی ماهر و دارای تخصص تحلیلی قوی، اساس بهره‌برداری موفق از اطلاعات منبع باز است (گارسیا و همکاران، ۲۰۲۲). این مطالعه بر ضرورت آموزش‌های تخصصی و مداوم برای تحلیل دقیق داده‌ها و شناسایی تهدیدات ناشناخته تأکید دارد. توانمندسازی تحلیلگران به ابزارهای تحلیلی پیشرفته و افزایش مهارت‌های تشخیص سیگنال‌های ضعیف، نقش مهمی در کاهش خطاهای انسانی و ارتقای کیفیت تصمیم‌گیری‌های امنیتی ایفا می‌کند. به‌علاوه، پرورش فرهنگ سازمانی مبتنی‌بر اخلاق و مسئولیت‌پذیری در مدیریت داده‌ها، از دیگر الزامات مهم این حوزه به‌شُمار می‌رود.

چالش‌ها و فرصت‌های اطلاعات منبع باز در فضای تهدیدات ناشناخته

پژوهش کنونی به‌طور جامع فرصت‌های اطلاعات منبع باز در افزایش آگاهی موقعیتی، شناسایی تهدیدات نوظهور و تسهیل تصمیم‌سازی را تأیید می‌کند، اما همزمان بر چالش‌های مهمی مانند سوءاستفاده‌های احتمالی از داده‌های باز توسط بازیگران خصمانه، پیچیدگی‌های تحلیل و فقدان چارچوب‌های قانونی و تخصصی تأکید دارد (میلر، ۲۰۱۷، گارسیا و همکاران۲۰۲۲). این شرایط ضرورت اتخاذ رویکردهای چندجانبه و هوشمندانه در مدیریت اطلاعات منبع باز را نمایان می‌سازد. تلفیق فناوری‌های پیشرفته، چارچوب‌های قانونی و آموزشی کارآمد، کلید کاهش خطرها و بهره‌برداری پایدار از مزایای اطلاعات منبع باز است.

در بستر تهدیدات ناشناخته، اطلاعات منبع باز نقشی دوگانه ایفا می‌کند که هم فرصت‌های بی‌سابقه‌ای در شناخت و مقابله با تهدیدات نوظهور ایجاد می‌کند و هم در صورت مدیریت نادرست می‌تواند خود منشأ بروز تهدیدات پیچیده و پیش‌بینی‌ناپذیر باشد. درمجموع، اطلاعات منبع باز در فضای تهدیدات ناشناخته، نه‌تنها به‌عنوان ابزاری برای پیش‌بینی و مقابله با تهدیدات عمل می‌کند، بلکه بستر بالقوه‌ای برای ظهور تهدیدات جدید است که شناخت دقیق و مدیریت هوشمندانه آن، محور اصلی تحقیقات آینده و سیاست‌گذاری‌های امنیتی خواهد بود.

شکل ۳. الگوی تحلیلی اطلاعات منبع باز و پیامدهای آن در چارچوب تهدیدات ناشناخته

بحث و نتیجه‌گیری

بررسی تحلیلی اطلاعات منبع باز با تأکید بر ابعاد و پیامدهای آن در چارچوب تهدیدات ناشناخته، نشان داد که اطلاعات منبع باز فراتر از یک ابزار صرف جمع‌آوری اطلاعات است و دارای ابعاد عملیاتی، فناورانه و راهبردی پیچیده‌ای است که هر یک به شکل مستقیم و غیرمستقیم بر امنیت ملی و سازمانی تأثیرگذار هستند. ابعاد عملیاتی اطلاعات منبع باز، شامل گردآوری، پالایش، صحت‌سنجی و ارزیابی اعتبار داده‌هاست که بدون دقت و صحت کافی، می‌تواند به انتشار اطلاعات نادرست و گمراه‌کننده منجر شود. بُعد فناورانه، با بهره‌گیری از هوش مصنوعی، یادگیری ماشین و زیرساخت‌های پردازش کلان داده، ظرفیت تحلیل اطلاعات حاصل از منابع علنی را به‌طرز چشمگیری افزایش داده است، اما این پیشرفت‌ها نیز با چالش‌هایی مانند خطاهای تحلیلی و سوءاستفاده‌های فناوری همراه است. بعد راهبردی اطلاعات منبع باز نیز با پشتیبانی از تصمیم‌سازی، آینده‌پژوهی و سیاست‌گذاری امنیتی، اهمیتی بسزا دارد که در فقدان چارچوب‌های قانونی و تخصص تحلیلی، زمینه‌ساز بروز تهدیدات ناشناخته می‌شود. این مطالعه نشان داد که تهدیدات ناشناخته به‌عنوان تهدیداتی با ماهیتی پیچیده، نوظهور و پیش‌بینی‌ناپذیر، در پرتو استفاده نادرست و مدیریت ضعیف اطلاعات منبع باز، می‌توانند ابعادی گسترده‌تر و عمیق‌تر یابند. فقدان قوانین و مقررات شفاف، ضعف در صحت‌سنجی و تحلیل داده‌ها، دسترسی بی‌ضابطه بازیگران خصمانه و کمبود نیروی انسانی متخصص از مهم‌ترین عوامل تسهیل‌کننده این روند است. درنتیجه، اطلاعات منبع باز هم به‌عنوان یک فرصت راهبردی برای ارتقای آگاهی موقعیتی و شناسایی تهدیدات نوظهور

عمل می‌کند و هم به‌عنوان بستر بالقوه تهدیدات ناشناخته که نیازمند مدیریت هوشمندانه و جامع است.

این پژوهش با واکاوی اطلاعات منبع باز در چارچوب تهدیدات ناشناخته، به این نتیجه‌گیری کلان و راهبردی دست یافت که اطلاعات منبع باز در عصر کنونی، یک تناقض امنیتی بزرگ است. از یک سو، به‌عنوان یک فرصت بی‌بدیل برای ارتقای آگاهی موقعیتی، شناسایی زودهنگام تهدیدات و پشتیبانی از تصمیم‌سازی راهبردی عمل می‌کند. از سوی دیگر، به دلیل ماهیت باز، غیرمتمرکز و فناوری‌محورش، به یک بستر گسترده و پیچیده برای شکل‌گیری تهدیدات ناشناخته تبدیل شده است. مهم‌ترین یافته این پژوهش آن است که خودِ ویژگی‌هایی که اطلاعات منبع باز را قدرتمند می‌سازند– سرعت، دسترسی آزاد و حجم انبوه داده– همان عواملی هستند که آن را به یک محیط آسیب‌پذیر در برابر تهدیدات پیش‌بینی‌ناپذیر بدل می‌کنند. این تحقیق سه بُعد اصلی این تناقض را تشریح کرد:

۱. بُعد عملیاتی: فرایند گردآوری و تحلیل داده‌های علنی، در صورت فقدان دقت و استانداردهای صحت‌سنجی دقیق، نه‌تنها خنثی نیست، بلکه می‌تواند به خطای سیستمی و تولید اطلاعات گمراه‌کننده بینجامد.

۲. بُعد فناورانه: هوش مصنوعی و کلان‌داده‌ها اگرچه توان تحلیل اطلاعات منبع باز را افزایش می‌دهند، اما توانایی تولید و گسترش سریع اطلاعات نادرست را نیز به سطحی بی‌سابقه رسانده‌اند و امکان سوءاستفاده در مقیاس بزرگ را فراهم می‌کنند.

۳. بُعد راهبردی: در غیاب چارچوب‌های قانونی شفاف و تخصص تحلیلی کافی، اطلاعات منبع باز می‌تواند تصمیم‌سازی در سطوح عالی ملی را مخدوش کند و با ایجاد درک نادرست از واقعیت‌ها، زمینه‌ساز بحران‌های امنیتی غیرمنتظره شود.

درنتیجه، رویکرد سنتی که اطلاعات منبع باز را صرفاً یک «ابزار اطلاعاتی» می‌دانست، دیگر کافی نیست. ما نیازمند یک تغییر نگرش راهبردی هستیم که در آن اطلاعات منبع باز به‌عنوان یک عامل مؤثر در معادلات امنیتی شناخته شود که هم ظرفیت فرصت‌آفرینی و هم توان تهدیدزایی دارد. این نگرش جدید، تدوین ره‌نامه‌های جامع، سرمایه‌گذاری بر نیروی انسانی متخصص و ایجاد چارچوب‌های قانونی و اخلاقی محکم را برای مدیریت هوشمندانه این تناقض، به یک ضرورت اجتناب‌ناپذیر تبدیل می‌کند. آینده امنیت ملی در گرو توانایی ما در درک و مدیریت این دوگانگی ذاتی اطلاعات منبع باز خواهد بود.

پیشنهاد

تدوین و تقویت چارچوب‌های قانونی متناسب با تحولات سریع فناوری‌های اطلاعات منبع باز: چالش اصلی «دسترسی بی‌ضابطه بازیگران متخاصم» و «فقدان قوانین شفاف» را هدف می‌گیرد. یک چارچوب قانونی روزآمد، با تعریف واضح مرزهای مجاز برای جمع‌آوری و استفاده از داده‌های علنی، به بازیگران خصمانه (مانند جاسوسان یا تروریست‌ها) مشروعیت قانونی نمی‌دهد و اقدامات آنان را به‌وضوح جرم‌مند می‌کند. این کار، «پیش‌بینی‌ناپذیری» ناشی از سوءاستفاده‌های قانونی را کاهش داده و فضای امن‌تری برای فعالیت نهادهای مشروع ایجاد می‌کند.

۱. ارتقای فناوری‌های صحت‌سنجی و اعتبارسنجی داده‌ها برای مقابله با چالش‌های مربوط به داده‌های ناقص، نادرست یا جهت‌دار: این پیشنهاد به صورت مستقیم به مقابله با چالش «ضعف در صحت‌سنجی و تحلیل داده‌ها» و «خطاهای تحلیلی» می‌پردازد. با توسعه و به‌کارگیری فناوری‌هایی مانند هوش مصنوعی برای ردیابی منبع اولیه داده، شناسایی دیپ‌فیک‌ها و تحلیل احساسات جهت‌دار، «عدم‌قطعیت تحلیلی» که یکی از شاخص‌های اصلی ناشناختگی است، کاهش چشمگیری می‌یابد. درنتیجه، احتمال تبدیل داده‌های نادرست به یک «تهدید ناشناخته» گمراه‌کننده کمتر می‌شود.

۲. آموزش و توانمندسازی وجود قوانین جامع و هماهنگ ملی و بین‌المللی برای جمع‌آوری، پردازش و استفاده از داده‌های متن‌باز: این مورد، دو چالش «کمبود نیروی انسانی متخصص» و «فقدان قوانین» را همزمان مورد توجه قرار می‌دهد. آموزش متخصصان، «کمبود تخصص تحلیلی» را که به تفسیرهای نادرست و تشدید تهدیدات منجر می‌شود، برطرف می‌کند. از سوی دیگر، قوانین جامع ملی و بین‌المللی، «پیچیدگی و پیش‌بینی‌ناپذیری» محیط اطلاعات منبع باز را با ایجاد یکدستی در استانداردهای عمل، کاهش می‌دهند و به نهادهای امنیتی امکان می‌دهند در یک چارچوب مشخص و پیش‌بینی‌پذیر عمل کنند.

۳. تقویت همکاری‌های ملی و بین‌المللی و ایجاد شبکه‌های همکاری میان سازمان‌های امنیتی، مراکز پژوهشی و دانشگاه‌ها: پیشنهاد یادشده، ماهیت فرامرزی و غیرمتمرکز تهدیدات ناشناخته اطلاعات منبع باز را هدف می‌گیرد. ایجاد شبکه‌های همکاری، «تعدد و ناشناسی بازیگران خصمانه» را خنثی می‌کند؛ چرا که سامانه‌های اشتراک اطلاعات، امکان ردیابی و شناسایی الگوهای تهدید را در سطحی وسیع‌تر فراهم می‌کنند. این همکاری، «آگاهی

موقعیتی» جمعی را افزایش داده و «پیش‌بینی‌پذیری» تهدیدات نوظهور را بالا می‌برد.

۴. تدوین نظام‌های نظارتی و شناسه‌های اخلاقی برای حفظ اعتماد عمومی: این مورد، چالش «سوءاستفاده بازیگران» و «از دست دادن اعتماد عمومی» را در کانون توجه قرار می‌دهد. شناسه‌های اخلاقی، استفاده مسئولانه از اطلاعات منبع باز توسط نهادهای مجاز را تضمین کرده و از تبدیل این نهادها به یک تهدید بالقوه جلوگیری می‌کنند. نظارت مستقل نیز با شفاف‌سازی فرایندها، اعتماد عمومی را جلب می‌کند.

سپاسگزاری

از تمامی کسانی که در انجام این پژوهش مشارکت داشتند کمال تشکر و قدردانی به عمل می‌آید.

تعارض منافع

هیچ گونه تعارض منافعی در این مقاله وجود ندارد.

فهرست منابع

سلطانی‌نسب، ابراهیم(۱۴۰۳). تهدیدات ناشناخته و مدل مفهومی استراتژی‌های مقابله با آنها. تهران: فصلنامه مدیریت نگرش راهبردی، دوره ۱، ش ۴، ۱۵۱-۱۲۹.

ARENA(2022). A Beginner’s Guide to Cognitive Warfare. The Australian National University. https://arena.gov.au/assets/2022/03/A-Beginners-Guide-to-Cognitive-Warfare

Brantly, A. F(2016). The decision to attack: military and intelligence cyber decision-making (Vol. 5). University of Georgia Press.

Brown, T(2019). Strategic Decision-Making in the Digital Age: The Role of OSINT. Journal of Strategic Security, 12(4), 78-95.

Carr, J(2012). Inside cyber warfare: Mapping the cyber underworld. " O'Reilly Media, Inc.".

Clark, R. M(2020). Intelligence Analysis: A Target-Centric Approach (6th ed.). CQ Press.

Clark, R., & Lewis, M(2021). Foresight and Policy Support through Open-Source Intelligence. International Journal of Intelligence and CounterIntelligence, 34(2), 210-230.

Ford, M(2023). Ukraine, participation and the smartphone at war. Political Anthropological Research on International Social Sciences (PARISS), 4(2), 219-247.

Garcia, L., Chen, H., & Patel, K(2022). Leveraging Artificial Intelligence for Big Data Analysis in Open-Source Intelligence. Journal of Advanced Security Research, 15(3), 45-62.

Hobbs, C., & Moran, M(2021). Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities. Palgrave Macmillan.

Hulnick, A. S(2006). Keeping Us Safe: Secret Intelligence and Homeland Security. Praeger Security International.

Johnson, A., & Miller, B(2020). Validation Frameworks in Modern Intelligence Systems. International Security Review, 8(1), 112-130.

Lowenthal, M. M(2016). Intelligence: From Secrets to Policy (7th ed.). CQ Press.

NATO(2023). NATO Open Source Intelligence Handbook (Ed. 2.0). NATO Open Source Intelligence Working Group.

Rahman, M. D(2025). The Art of Open Source Intelligence (OSINT): Addressing Cybercrime, Opportunities, and Challenges. The Art of Open Source Intelligence (OSINT): Addressing Cybercrime, Opportunities, and Challenges (May 01, 2025).

RAND Corporation(2020). The Role of Open Source Intelligence in Modern Security Environments. Research Report. https://www.rand.org/pubs/research_reports/RR2700.html

Rollins, J(2008). Fusion centers: Issues and options for Congress (No. CRSRL34070).

Shearer, E., & Bird, C(2023). How Open-Source Intelligence is Changing the News Landscape. Pew Research Center. https://www.pewresearch.org/journalism/2023/09/21/how-open-source-intelligence-is-changing-the-news-landscape/

Singapore Ministry of Home Affairs(2020). *Singapore's National Security Priorities*.: https://www.mha.gov.sg/

Smith, J(2018). The Principles of Data Verification in Intelligence Cycles. Security and Intelligence Journal, 4(2), 22-39.

US Department of Defense. (2020). Joint Publication 2-0: Joint Intelligence.

Van Puyvelde, D., & Rienzi, F. T(2025). The rise of open-source intelligence. European Journal of International Security, 1-15.

Voigt, P., & Von dem Bussche, A(2017). The eu general data protection regulation (gdpr). A practical guide, 1st ed., Cham: Springer International Publishing, 10(3152676), 10-5555.

Wardle, C., & Derakhshan, H(2017). Information Disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c