شناسایی تروریست در شبکه‌های اجتماعی به‌وسیله اطلاعات منبع‌باز

مهدي كوره‌پز[۱]، رضا شیبانی[۲]

[۱] گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد مشهد، ایران
korehpaz65@gmail.com
[۲] استادیار انفورماتیک پزشکی، مدیر گروه مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد مشهد، ایران
reza.shni@gmail.com

چکیده

در فعالیت‌های اطلاعاتی، امنیتی و انتظامی، برای شناسایی اهداف، از نظارت بر شبکه اجتماعی استفاده می‌شود. این رویکرد به تحلیل‌گران کمک می‌کند تا گروه‌های مخفی مانند یک شبکه ضد امنیتی، یک خانواده جنایتکار سازمان‌یافته یا یک باند تبهکار را با تحلیل داده‌ها شناسایی و از رشد افراط‌گرایی به هر شکل ممکن جلوگیری شود. فعالیت‌های تروریستی در سراسر جهان منجر به توسعه روش‌های پیچیده برای تجزیه و تحلیل گروه‌ها و شبکه‌های تروریستی شده است. تحقیقات فعلی و گذشته نشان داده است تجزیه و تحلیل شبکه‌های اجتماعی (SNA) رویکردی برای تجزیه و تحلیل شبکه‌های تروریستی و درک بهتر ساختار زیربنایی یک گروهک و شناسایی بازیگران کلیدی در گروه و پیوندهای آنها در سراسر سازمان است. در این رابطه مهم‌ترین چالش، حفظ حریم خصوصی برای دسترسی به اطلاعات است. این مقاله جنبه‌های مختلف تحلیل شبکه‌های اجتماعی را در مورد تروریسم، با در نظر گرفتن داده‌های تجربی و مطالعات مبتنی بر داده‌های منبع‌باز بررسی می‌کند. جمع‌آوری داده‌های باز بدون نیاز به داشتن مجوز از مراجع قضایی و با در نظر گرفتن اطلاعات منتشر شده توسط خود فرد در سطح وب صورت می‌گیرد. کار ما در درجه اول مطالعه‌ای بر روی انواع مختلف شبکه‌ها و گره‌های تروریستی غیرمتمرکز قابل دسترس بوسیله جمع‌آوری داده‌های باز است.

کلمات کلیدی: تحلیل شبکه‌های اجتماعی، اسینت، جرم کاوی، داده کاوی، هوش مصنوعی.

۱ مقدمه

سازمان‌های تروریستی از رسانه‌های اجتماعی برای گسترش تبلیغات و جذب اعضای جدید استفاده می‌کنند [۲]. در جنگ داعش بر علیه حاکمیت سوریه و عراق، رسانه‌های اجتماعی به ایجاد تحولات جدید کمک کردند. اتفاقاتی که از لیبی تا افغانستان و نیجریه تا بنگلادش را تحت تاثیر قرار داد [۳]. در شناسایی اهداف تروریستی با استفاده از داده‌کاوی، مرکزیت درجه و تعداد پیوندهای مستقیم متصل به هر گره اهمیت آن گره

را نمایان می‌کند و سایر اطلاعات مانند گره اصلی با رهبر قابل درک است [۴].

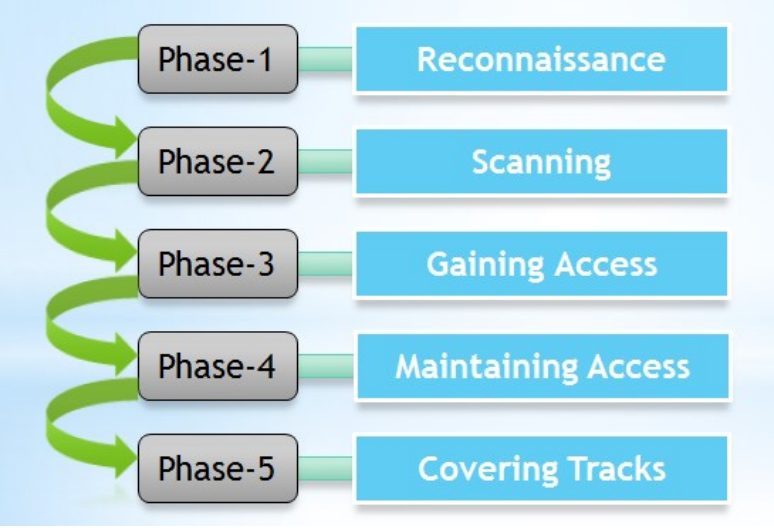
با افزایش شدید استفاده از شبکه‌های اجتماعی، بانک اطلاعاتی برخط در قالب نظرات، احساسات، عواطف و نیات تولید شد که نشان‌دهنده وابستگی‌ها و تمایل اعضا به یک نهاد، رویداد و سیاست است [۵]. شناسایی محتوای افراطی برای تجزیه و تحلیل احساسات کاربران نسبت به برخی از گروه‌های افراطی و جلوگیری از چنین اعمال غیرقانونی مرتبط و مهم است [۶].

تحلیل شبکه‌های اجتماعی Social networks analysis (SNA) می‌تواند به شناسایی رهبران یا افراد مهم تاثیرگذار در عملیات تروریستی کمک کند و باید به منظور ایجاد اختلال در فعالیت های سازمانی مورد هدف قرار گیرند [۱].

فرآیند استخراج OSINT در سه مرحله مشاهده می شود (الف) اکتساب داده، (ب) غنی‌سازی داده، و (ج) استنتاج دانش. در زمینه تروریسم، محققان کارهای قابل توجهی در انطباق با این سه مرحله انجام داده‌اند [۸].

OSINT یا اوسینت مخفف Open Source Intelligence به‌معنای جستجوی هوشمندانه در منابع اطلاعات آزاد است [۹].

OSINT به‌صورت آن‌لاین جهت شناسایی هدف توسط سازمان‌های جنایی، هکرها و آزمایش‌کنندگان نفوذ به‌طور بسیار گسترده مورد استفاده قرار می‌گیرد [۱۲] همان‌طور که در شکل ۱ آورده شده است، اولین مرحله اول نفوذ، شناسایی است.



شکل ۱: مراحل تست نفوذ

انواع ابزارهای هوش که می توان از آن برای جمع آوری اطلاعات منبع‌باز استفاده کرد.

- هوش منابع انسانی (HUMINT)

- هوش منابع تصویری (IMINT)
- هوش منابع جغرافیایی (GEOINT)
- هوش منابع سیگنالی (SIGINT)
- هوش رسانه‌های اجتماعی (SOCMINT)
- هوش منابع اقتصادی (FININT)
- هوش منابع باز (OSINT)

در سال ۲۰۱۲ برای اولین بار از عبارت SOCMINT یا هوش رسانه‌های اجتماعی استفاده شد؛ یعنی بررسی رسانه‌های اجتماعی برای به‌دست آوردن اطلاعات از منابع باز (OSINT) [۱۳]. از طرفی منابع اوسینت بدون نگرانی در رابطه با هر گونه مجوز حق انتشار، می‌توانند بین افراد مختلف به اشتراک گذاشته شوند، زیرا این اطلاعات قبلاً توسط صاحب اطلاعات، منتشر شده‌اند [۱۴]. برای به‌دست آوردن اطلاعات از رسانه‌های اجتماعی، از تکنیک‌های شرح داده شده زیر استفاده می شود [۱۵]:

۱. جستجوی مستقیم در رسانه‌های اجتماعی با موتور جستجوی داخلی و گزینه‌های جستجو پیشرفته.

۲. جستجوی ابزارهای خارجی که از طریق اتصال API به رسانه‌های اجتماعی به شما امکان دانلود می‌دهد.

۳. داده‌ها و ساختار آنها یا ابزارهایی که وظیفه آنهاست.

۴. ایجاد جستجوی پیشرفته در موتور جستجو گوگل با استفاده از عملگرهای پیشرفته و تکنیک‌های رشته بولی.

ابزارهای OSINT به‌سرعت در حال تکامل هستند [۱۶]، روش‌های رایج را می‌توان در چهار قالب اصلی دسته‌بندی کرد: روش‌های مبتنی بر متن، سیستم‌های اطلاعات جغرافیایی (GIS)، علوم شبکه و پزشکی قانونی بصری [۱۹].

روش مبتنی بر متن و Natural Language Processing: بررسی متن، از طریق موجودیت‌ها، کلمات کلیدی، روابط کلمه/ عبارت و نقش‌های معنایی/ نحوی. NLP روش‌های مبتنی بر متن معاصر مانند خلاصه‌سازی خودکار متن، تجزیه و تحلیل احساسات مبتنی بر ماشین، استخراج موضوع، پایه ابزارهای مدرن متن‌کاوی را تشکیل می‌دهد [۱۷].

پروفایل کاربر: شامل زبان استفاده شده و لحن کلمات، حساب‌های پیونده شده، دوستان مشترک با گره‌های تروریستی، رسانه‌ها و ویدئوهای بارگذاری شده، علاقه‌مندی‌ها، اخبار دنبال شده، هشتگ‌های استفاده شده، موقعیت‌های انتشار پست، متادیتا، استفاده از کلمات خاص ویژه گروه‌های تروریستی و ... [۱۷].

ابزارهای تسهیل کننده کسب و تجزیه و تحلیل اطلاعات در رسانه‌های اجتماعی: در زیر چند مورد منتخب از ابزارهایی برای تسهیل کسب اطلاعات از رسانه‌های اجتماعی را معرفی می‌کنیم. ابزارهایی که برای همه در دسترس هستند و استفاده از آنها آسان است و به‌راحتی در وب یافت می‌شود [۱۸].

روش‌های اوسینت: روش‌های داده‌کاوی و تجزیه و تحلیل داده‌های نوآورانه، روش جستجوی زبانی هوشمند، موتورهای جستجوی هوشمند، سیستم مرتب‌سازی موضوعی (مانند نظارت خودکار RSS)، نظارت بر سایت‌های جامعه (مانند ارزیابی فوری خطر فلش موب)، ارزیابی کد منبع وب‌سایت‌ها، نمایش محتوای پنهان، جستجوی دامنه، ابزار whois (بازیابی داده های مرتبط با مشترکین دامنه سایت)، نظارت بر مطبوعات و ...

حوزه‌های کلیدی اوسینت: اخبار اینترنتی، ادبیات خاکستری، شبکه‌های اجتماعی، رسانه‌های سنتی، مخازن باز داده‌ها، سوابق.

۲ مرور پیشینه

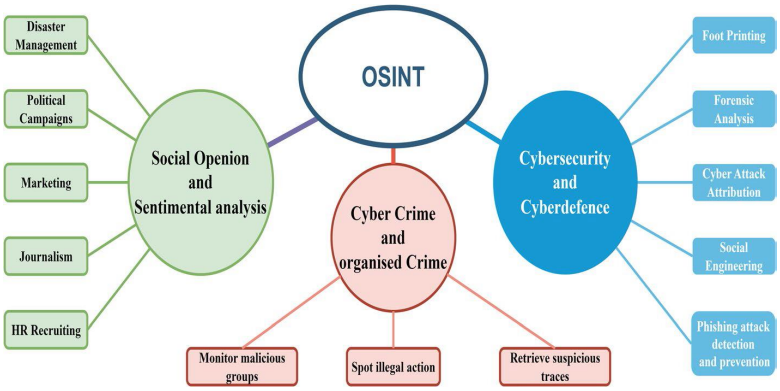
پزشکی قانونی دیجیتال و اطلاعات منبع‌باز دو نوع گسترده از تحقیقات جرایم سایبری هستند. قاچاق انسان، هرزه‌نگاری، پورنوگرافی کودکان، ترور، فروش مواد مخدر، فعالیت‌های تروریستی، بازارهای جرایم سایبری و مبادلات ارزهای دیجیتال از جمله هشت جنایت سایبری اصلی هستند که توسط Nazah و همکاران (۲۰۲۰) برجسته شده‌اند. آنها دریافتند که هیچ ابزار یا روش واحدی نمی‌تواند تمام شواهدی را که بازرسان نیاز دارند جمع‌آوری کند و به این دلیل از ترکیب‌های مختلف ابزارها و تکنیک‌ها برای انجام تحقیقات جرایم سایبری استفاده می‌کنند.

کوئیک و چو (۲۰۱۸) چارچوبی مبتنی بر OSINT پیشنهاد کردند که دقت دستگیری مجرم را افزایش می دهد و OSINT را در پزشکی قانونی دیجیتال برای بهبود تجزیه و تحلیل اطلاعات جنایی اعمال می‌کند.

توسط جونجینگ، یان، و جین چیانگ (۲۰۲۰) در راستای پزشکی قانونی شبکه اجتماعی، رابطه مبتنی بر داده‌های بزرگ با استفاده از ارتباط شبکه و فرآیند پزشکی قانونی تلفن‌های همراه را مطرح کردند.

در کار دیگری (Giudice, Paratore, Moltisanti, Battiato, 2017) بر روی پلت فرم Wechat به‌طور ویژه روش ارتباط شبکه‌های اجتماعی بر اساس مجموعه داده‌های نمونه را تجزیه و تحلیل می‌کند.

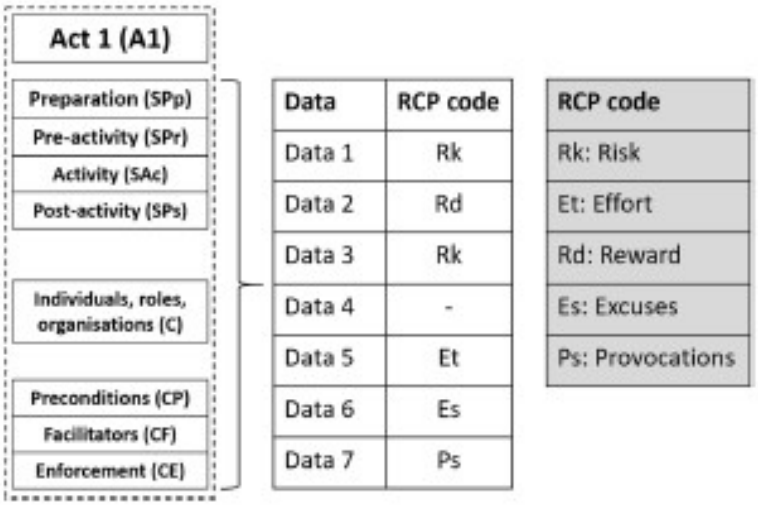
بر اساس مقاله (La Stampa, 2018)، هر فردی که در سایت‌های شبکه‌های اجتماعی حساب کاربری دارد، به‌طور متوسط هفت نوع اطلاعات از وی در آن سایت‌ها ثبت شده است (شکل ۲: نمایه اطلاعات و کاربردهای اوسینت).



شکل ۲: کاربردهای اوسینت

۱.۲ یک فرآیند روشمند ساختاریافته برای جمع‌آوری سناریوی جرائم سازمان‌یافته با استفاده از OSINT

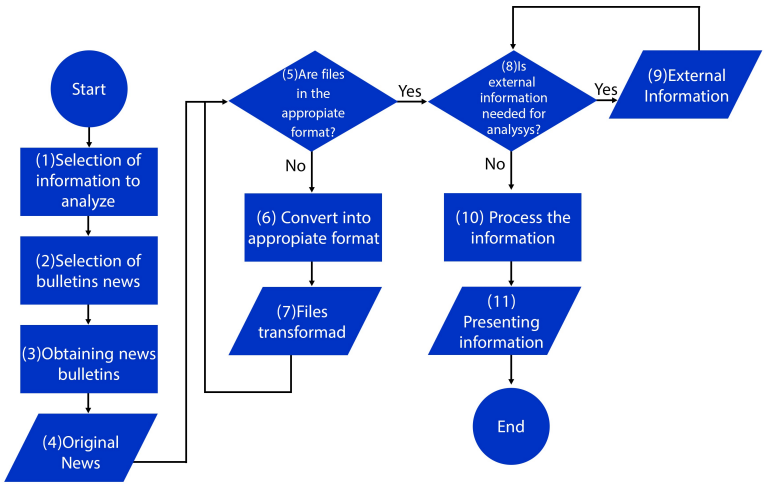
مقاله [۱۸] به‌دنبال اقدام‌شناسی مجرمان است. تحلیل‌گران منابع آشکار با کمک هوش مصنوعی اقدام به تولید فیلم‌نامه‌های جنایی کردند تا رویه وقوع جرم را بررسی و در مواردی منجر به تولید فیلم‌های جنایی با کیفیت و با موضوعات جدید و منحصر به فرد بشوند. این ایده به طور مؤثر باعث شده، اقدامات سازمان‌یافته جنایی پیش‌بینی شود. SCP شامل تعدادی تکنیک است که ارتکاب جرم را پر خطرتر، پاداش کمتر و تلاش را بیشتر می‌کند. تکنیک‌های SCP نیز می‌توانند کمک به حذف بهانه‌هایی که بر تصمیم‌گیری مجرم تأثیر می‌گذارند (مانند تنظیم قوانین واضح‌تر) و کاهش تحریکات به سمت مشارکت مجرمانه (مانند دلسرد کردن) را ایجاد کنند. در شکل ۳ پیش‌بینی نقش‌ها با استفاده از اوسینت رسم شده است.



شکل ۳: پیش‌بینی نقش‌ها با استفاده از اوسینت

۲.۲ تشخیص اخبار جعلی کرونا از طریق بررسی MedOSINT در بولتن‌های رسمی مراقبت‌های بهداشتی با توضیح CBR

بر مبنای الگوی مرجع [۸] گام دوم، روش‌های دسترسی به منابع اطلاعاتی سالم و قابل اعتماد بررسی شد. در بولتن‌های رسمی پزشکی حجم بسیار زیاد اطلاعات در مورد درمان‌های مختلف و درمان‌های خودساخته همراه با شایعات و اطلاعات نادرست منتشر می‌شود و باعث سردرگمی و بی‌اعتمادی مردم گردیده و سایت‌های خبری قانونی هم در دام پخش اطلاعات نادرست قرار می گیرند. MedOSINT با ارائه شیوه پیشنهادی کمک می‌کند مطمئن شوید آیا اخبار پزشکی مورد نظر، درست است یا غلط. با ادغام MedOSINT و سیستم استدلال مبتنی بر مورد ،(CBR) راهکارهای مورد اعتماد مهیا خواهد شد [۲۰]. در تصویر ۴ نمودار پیشنهادی MedOSINT آورده شده است. در این پژوهش ویژگی‌های تحلیل شده به دو دسته کلی تقسیم می‌شوند: ۱) منبع ۲) محتوا.



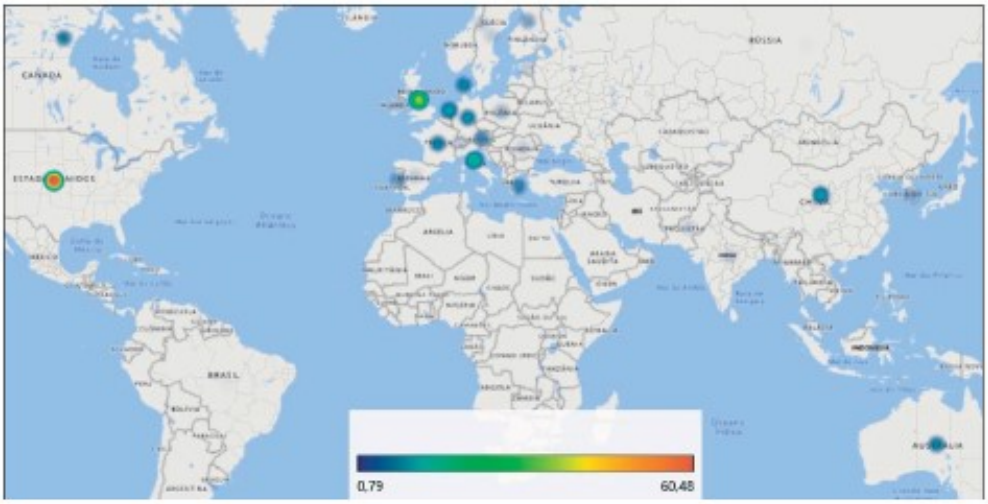
شکل ۴: نمودار جریان پیشنهادی MedOSINT

۳.۲ بررسی رسانه های اجتماعی مبتنی بر پیش‌بینی ناآرامی‌های مدنی

با در نظر گرفتن ناآرامی‌های اخیر ۲۰۲۳ که در ایران اتفاق افتاد بررسی ارتباط ناآرامی‌های مدنی و ارتباط با تروریست‌ها ضروری به‌نظر می‌رسد. در این کار، ابتدا پیش‌بینی ناآرامی مدنی مفهوم‌سازی شده و به‌نوبه خود، فناوری‌های پیش‌بینی ناآرامی‌های مدنی نیز به عنوان ابزار ارزیابی ریسک ارائه شده است که ناآرامی‌های آینده خطرناک را پیش بینی و قابل محاسبه می‌کند. در نهایت، روش‌های ارائه شده توسط محققان ارزیابی می‌شود [۲۱].

۴.۲ مروری بر ادبیات سیستماتیک برای بررسی کاربرد هوش منبع‌باز (OSINT) با هوش مصنوعی: تلفیق هوش منبع‌باز با هوش مصنوعی

در راستای انگیزه‌یابی تروریست در شبکه های اجتماعی با استفاده از اوسینت، با تجزیه و تحلیل نتایج، اطلاعات مرتبطی در مورد انتشاراتی که OSINT را با هوش مصنوعی یا سایر زمینه‌ها تلفیق می‌کنند، پیدا می‌کنیم [۲۲]. برای نمایش حوزه انتشارات OSINT از تجزیه و تحلیل اطلاعات به اشتراک گذاشته شده هوشمند در رسانه‌های اجتماعی برای تولید دانش جدید استفاده می‌شود. بنابراین، تنها در این ۴ سال، یعنی از ۲۰۱۶ تا ۲۰۱۹، انتشارات OSINT با هوش مصنوعی برای حوزه امنیت سایبری، بررسی و نقشه‌ای با بیشترین تمرکز برنامه‌ها در تصویر ۵ نشان داده شده است.



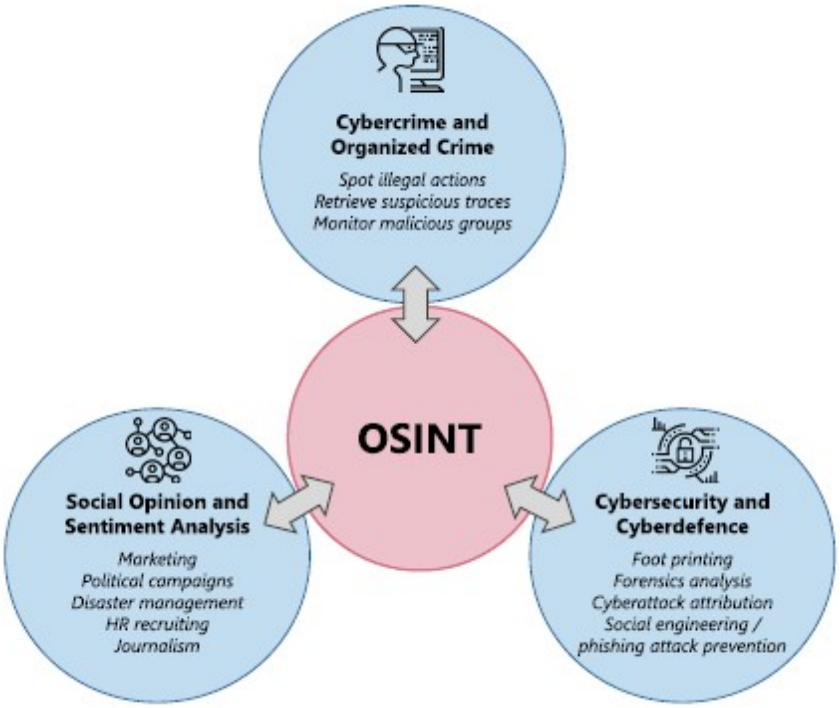
شکل ۵: کشورهای منتشر کننده بولتن‌های اوسینت

با تجزیه و تحلیل این نتایج، به این نتیجه رسیدیم که استفاده از یک مرور متون سیستماتیک می‌تواند کاربرد OSINT با هوش مصنوعی را نشان دهد.

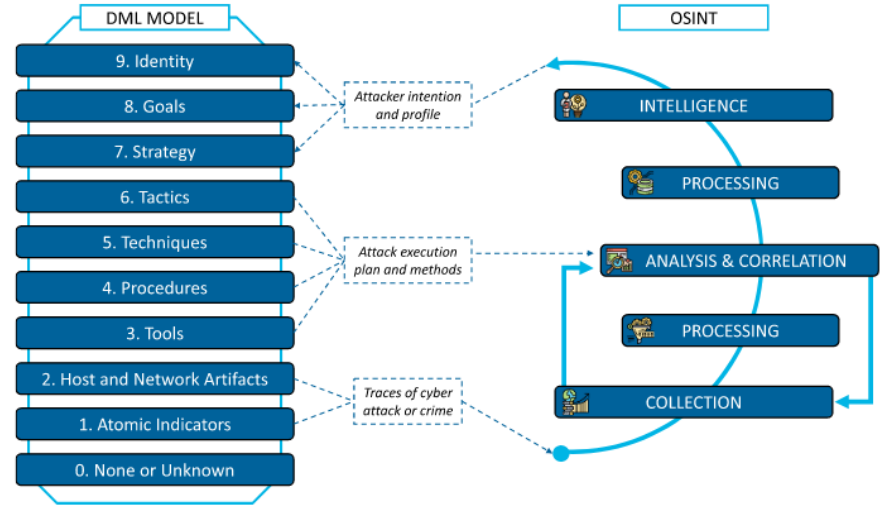
۵.۲ فرصت‌ها، چالش‌های منابع باز و روندهای آینده

در حقیقت اطلاعات منبع‌باز مانند معدن طلا هستند که در دسترس همه هست ولی فقط عده کمی قادر به استخراج آن هستند. در این مقاله سه مورد استفاده اصلی OSINT ذکر شده است. برای هر کاربر، در هر زمان و از هر نقطه از اینترنت، قابل دسترسی است. موارد استفاده اصلی اوسینت در تصویر ۶ آورده شده است.

در حالت ایده‌آل، OSINT در آینده باید بتواند اطلاعات خاصی را که در جستجوی کاربر بیشترین صحت و دقت را دارد برگرداند. چرخه و مدل جمع‌آوری و تحلیل داده‌ها پیشنهادی در تصویر شماره ۷ آورده شده است.



شکل ۶: موارد استفاده اصلی اوسینت



شکل ۷: مدل جمع‌آوری و تحلیل داده‌ها

۳ یافته‌ها

به همان اندازه که هوش منبع‌باز ارزشمند است، اضافه بار اطلاعات یک مشکل واقعی است. اکثر ابزارها و تکنیک‌های مورد استفاده برای انجام ابتکارات اطلاعاتی منبع‌باز برای کمک به متخصصان امنیتی تلاش‌های خود را بر روی حوزه‌های خاص مورد علاقه متمرکز می‌کنند.

مرجع [۱۹] (اسپنسر چنی و همکاران ۲۰۲۱) ایده‌ی اولیه بسیار عالی است و راهگشا در پیش‌بینی اقدامات تروریستی و لیکن حریم خصوصی مغفول مانده است و به‌نوعی ما از همه روش‌ها برای به‌دست آوردن اطلاعات استفاده می‌کنیم ولیکن در قواعد بین‌المللی قانون به ما اجازه دسترسی به اطلاعات خصوصی محرمانه در پرونده‌های قضائی را حتی به‌شرط انتشار توسط نفوذگران نمی‌دهد و برخی از صاحب‌نظران این موضوع را غیر اخلاقی و متضاد با روح اوسینت می‌دانند.

مرجع [۲۰] (سرجیو مائوریسیو و همکاران ۲۰۲۱) ایده پیشنهادی در راستای کشف اطلاعات منتشر شده غیر مستند در فضای مجازی است همان چیزی که در ادبیات ما به نوعی فیک‌نیوزها نام دارند. از جمله نگاه نویسنده به کار پیشنهادی نگاه عملیات روانی هر موضوع بوده و قصدش را کاهش بار روانی بر روی افکار مردم دانسته که در نوع خود کم نظیر است. نکته حائز اهمیت روش پیشنهادی این است که یک الگوریتم تحت نظارت CBR برای شناسایی اخبار مشابه تلفیق کرده است و باعث بالارفتن صحت دسته بندی شده است.

مرجع [۲۱] (گابریل گریل، دانشگاه میشیگان ۲۰۲۱) نویسنده با بهره‌گیری از روش‌های خزش در اطلاعات آشکار موجود، کاربرهای مختلف شبکه‌های اجتماعی را دسته‌بندی کرده و برای هر فرد یک الگوی سیاسی، اجتماعی، فرهنگی، اعتقادی و ... تهیه می‌کند که برای کارهای کارآگاهی بعدی از جمله جرم‌شناسی و پیش‌بینی مخالفت‌های مردم بسیار مؤثر است.

مرجع [۲۲] (ژائو رافائل گونسالوس اوانجلیستا و همکاران ۲۰۲۰) حاوی روش‌های مرسوم جمع‌آوری اطلاعات ازجمله هوش انسانی، هوش ماشین، هوش ارتباطی و هوش جمع‌آوری اطلاعات آشکار که در نهایت دانش ارتباطی انواع هوشمندی است.

مرجع [۲۳] (خاویر پاستور و همکاران ۲۰۲۰) علاوه بر کارهای قبلی، روش‌های جمع‌آوری اطلاعات در وب عمیق و وب تاریک را مورد بررسی قرار داده است. این مقاله با معرفی وب‌سایت‌های مرتبط با هر موضوع جمع‌آوری اطلاعات، اهمیت استفاده و درصد بهره‌وری هر روش را مشخص کرده است.

۴ نتیجه‌گیری

در کارهای پژوهشی بررسی شده به‌دلیل استفاده از دایرکتوری برخط ذخیره اطلاعات می‌توان یک آزمایشگاه جامع کارآگاهی در اینترنت راه‌اندازی کرد، به شکلی که با گسترش پرونده‌های کارآگاهی در وب هر روز به دایرکتوری تجمیعی اطلاعات برای پیش‌بینی‌های بعدی افزوده شود. علاوه بر داده‌های استخراج شده از اینترنت، باید به اهمیت اطلاعات دارک‌وب و دیپ‌وب توجه داشت.

با توجه به سرعت رشد اطلاعات و پیچیدگی تحلیل‌های اوسینت، در کارهای آینده بر روی جمع‌آوری

جدول ۱: مقایسه فنی بین روش‌های بررسی شده دسترسی به اطلاعات

مراجع بررسی شده	چالش‌ها	مزایا
[۸، ۹، ۱۷]	دسترسی به دیتاست برخط در دسترس آشنایی مجرمان سایبری به روش‌های دسترسی به داده‌های آشکار عدم ساختار واحد نمایه‌سازی اطلاعات	تولید سناریوهایی که تاکنون کمتر یا هرگز اتفاق نیافتاده و در آینده ممکن است با آن درگیر شویم دلایل ارتکاب به جرم قبل از وقوع افزایش هزینه اقدام مجرمانه
[۱۷، ۲۰]	هیجان باعث باورپذیری خبر جعلی می‌شود. ضعف سازوکار برچسب‌زنی به اخبار جعلی. تولید تنش‌های اجتماعی با پخش شایعه.	تحلیل اخبار با هوش مصنوعی. ایجاد بستر برخط و پرسرعت واکنش گسترش دسترسی به داده باز تولید ابزارهای صحت‌سنجی فردی تولید اخبار امن توسط هوش مصنوعی سازوکار برچسب‌زنی خبر
[۱۸، ۲۲]	دسترسی به اخبار محلی در حوادث ضعف NLP در زبان‌های بومی ضعف اطلاعاتی در دسترسی به منابع باز	گسترش روش‌های ثبت وقایع تولید مجلات هوشمند تحلیل وقایع تولید ابزار پرقدرت کشف ناهنجاری توسط منابع باز و هوش مصنوعی

اطلاعات با استفاده از کامپیوترهای کوانتومی متمرکز خواهیم شد.

مراجع

[۱] نهادا. حسن، رامی حجازی (۱۴۰۰). جمع‌آوری اطلاعات منبع‌باز: ابزار و روش‌های جمع‌آوری اطلاعات منابع آزاد از اینترنت، مترجم مهدی کوره‌پز، نشر شاملو.

[2] Mishra, Ranjit (2033). “Terror Attack Prediction Based on Time Series”. Journal of Defense Studies, 17(1).

[3] Berger J.M., Jonathon Morgan (2015). “Defining and Describing the Population of ISIS Supporters on Twitter”. The Brookings Institution.

[4] Koerner, Brendan I. (2017). “Why ISIS is Winning the Social Media War”. Wired (1 May 2017), available at https://www.wired.com/2016/03/isis-winningsocial-media-war-heres-beat.

[5] Hao F., Park D.S., Pei Z. (2018). “When social computing meets soft opportunities and insights”. Human-centric Comput Inform Sci, 8(8):1–18.

[6] Azizan, S. A., Aziz, I. A. (2017). “Terrorism detection based on sentiment analysis using machine learning”. Journal of Engineering and Applied Sciences, 12(3), 691-698.

[7] Dhillon, H. (2021). Building effective network security frameworks using deep transfer learning techniques (Doctoral dissertation, The University of Western Ontario (Canada)).

[8] Chaudhary, M., Bansal, D. (2022). "Open source intelligence extraction for terrorism-related information: A review". Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 12(5), e1473.

[9] Kumari, S., Yadav, R. J., Namasudra, S., Hsu, C. H. (2021). "Intelligent deception techniques against adversarial attack on the industrial system". International Journal of Intelligent Systems, 36(5), 2412-2437.

[10] Singer, G., Golan, M. (2019). "Identification of subgroups of terror attacks with shared characteristics for the purpose of preventing mass-casualty attacks: A data-mining approach". Crime Science, 8(1), 14.

[11] Rehman, A. U., Jiang, A., Rehman, A., Paul, A., Din, S., Sadiq, M. T. (2020). "Identification and role of opinion leaders in information diffusion for online discussion network". Journal of Ambient Intelligence and Humanized Computing, 1-13.

[12] Yadav, A., Kumar, A., Singh, V. (2023). "Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security". Artificial Intelligence Review, 56(11), 12407-12438.

[13] Omand, D. (2017). "Social media intelligence (SOCMINT)". The Palgrave handbook of security, risk and intelligence, 355-371.

[14] Kuehn, P., Bäumler, J., Kaufhold, M. A., Wendelborn, M., Reuter, C. (2022). "The Notion of Relevance in Cybersecurity: A Categorization of Security Tools and Deduction of Relevance Notions".

[15] Thapa, B. (2022). "Applying socmint to extract cyber threat intelligence from the Russia-Ukraine conflict". IADIS International Journal on WWW/Internet, 20(2).

[16] Nastasi, C., Battiato, S. (2021). "Defamation 2.0: New Threats in Digital Media Era-An Overview on Forensics Approaches in the Social Network Ecosystem". IMPROVE, 121-127.

[17] Böhm, I., Lolagar, S. (2021). "Open source intelligence: Introduction, legal, and ethical considerations". International Cybersecurity Law Review, 2(2), 317-337.

[18] Camacho, D., Panizo-LLedot, A., Bello-Orgaz, G., Gonzalez-Pardo, A., Cambria, E. (2020). "The four dimensions of social network analysis: An overview of research methods, applications, and software tools". Information Fusion, 63, 88-120.

[19] Chainey, S. P., Alonso Berbotto, A. (2022). "A structured methodical process for populating a crime script of organized crime activity using OSINT". Trends in Organized Crime, 25(3), 272-300.

[20] Monterrubio, S. M. M., Noain-Sánchez, A., Pérez, E. V., Crespo, R. G. (2021). "Coronavirus fake news detection via MedOSINT check in health care official bulletins with CBR explanation: The way to find the real information source through OSINT, the verifier tool for official journals". Information Sciences, 574, 210-237.

[21] Grill, G. (2021). “Future protest made risky: Examining social media based civil unrest prediction research and products”. Computer Supported Cooperative Work (CSCW), 30(5), 811-839.

[22] Evangelista, J. R. G., Sassi, R. J., Romero, M., Napolitano, D. (2021). “Systematic literature review to investigate the application of open source intelligence (osint) with artificial intelligence”. Journal of Applied Security Research, 16(3), 345-369.

[23] Pastor-Galindo, J., Nespoli, P., Mármol, F. G., Pérez, G. M. (2020). “The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends”. IEEE Access, 8, 10282-10304.