مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

عصر فضای مجازی
نود و پنجم

استخراج داده‌های بیولوژیک از طریق اوسینت

Extraction of biological data through Osint

بسم الله الرحمن الرحیم

عصر فضای مجازی

گزارش شماره ۹۵

بهمن ۱۴۰۰

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

استخراج داده‌های بیولوژیک از طریق اوسینت

محتوای انتشار یافته در این اثر
الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست

تهیه شده در پژوهشگاه فضای مجازی
(گروه مطالعات بنیادین فضای مجازی)

تهیه‌کننده: محمد اسماعیل حسنی جبل کندی
(دانشجوی دکتری ریاضی دانشگاه تربیت‌مدرس)

ناظر علمی: دکتر علیرضا کاظمی، دکتر سیدجمال قریشی خوراسگانی، دکتر حسین مطلبی کربکندی

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶ غربی، پلاک ۲۰
تلفن: ۸۶۱۵۱۰۶۱-۰۲۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست ۵
چکیده ۹
مقدمه ۱۳

بخش اول

روش‌شناسی و ابزارهای اوسینت ۱۹

بخش دوم

اوسینت و داده‌های بیولوژیک ۲۷
۲-۱- جمع‌آوری داده‌های بیولوژیک ایرانیان در فضای مجازی ۳۰
۲-۱-۱- تشویق به انتشار داده‌های زیستی ۳۱
۲-۲- تحلیل ساعات فعالیت روزانه (استراحت، فعالیت کاری و تغذیه) ۴۰
۲-۲-۱- تحلیل ۱، پیام‌رسان تلگرام ۴۱
۲-۲-۲- تحلیل ۲، تحلیل توییتر ۴۳
۲-۲-۳- تحلیل ۳، ماه رمضان ۴۴
۲-۳- طول دوره عادت ماهانه زنان ۴۷
۲-٤- زبان مادری و نژاد ۴۹
۲-٤-۱- روش ۱، نام کاربری ۴۹
۲-٤-۲- روش ۲، نگارش به زبان غیررسمی ۵۰
۲-٤-۳- روش ۳، برانگیختن احساسات نژادی ۵۰
۲-٤-٤- روش ٤، محل زندگی ۵۱
۲-٤-۵- روش ۵، ادبیات نگارش ۵۱
۲-۵- کشف عادات غذایی بر اساس تحلیل تصویر ۵۳

جمع بندی ۵۵
منابع ۶۳

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

چکیده

چکیده

مفهوم اوسینت[1] ناظر به جستجو، جمع‌آوری، تحلیل و استفاده از داده‌های منابع باز و ابزارها و روش‌های مختلف در این باره است. از مهم‌ترین منابع یک فعالیت اوسینتی می‌توان به داده‌های قانونی و فراداده‌های منتشر شده توسط کاربران اشاره داشت. فراداده‌ها، در واقع توصیفات داده‌های اصلی - مانند حجم داده، تاریخ ایجاد آن و...- هستند که همراه داده منتشر می‌شوند و آن‌ها را تشریح می‌کنند. آنها گاه حامل اطلاعاتی هستند که از دید کاربران پنهان است یا بی‌اهمیت فرض می‌شود. متخصصین اوسینت و هوش مصنوعی می‌توانند با استخراج فراداده‌ها به اطلاعاتی دسترسی پیدا کنند که نتیجه پردازش آن‌ها به نتایج باارزشی جامعه‌شناختی، سیاسی، بیولوژیک و... منجر می‌شود. در این گزارش داده‌های باز و در دسترس (اعم از داده‌های قانونی و لو رفته) از منظر استخراج داده‌هایی از قبیل پزشکی، روانپزشکی و ... مطالعه شده است و تلاش شده است جایگاه داده‌های منبع باز در تهدیدات زیستی احتمالی مشخص شود.

در **مقدمه**، بحثی کلی در مورد چیستی اوسینت و تاریخچه و ویژگی‌های آن بیان شده است.

1. Open Source Intelligence (OSINT)

در **روش‌شناسی و ابزارهای اوسینت**، روش‌شناسی اوسینت توضیح داده شده است و اهم ابزارها و روش‌های مورداستفاده در عملیات‌های اوسینتی مورد تحلیل قرار گرفته است.

در **اوسینت و داده‌های بیولوژیک**، با استفاده از مباحث مطرح‌شده در دو فصل قبل، مثال‌هایی از جمع‌آوری، پردازش و سوءاستفاده احتمالی از داده‌های بیولوژیک ایرانیان مطرح شده است تا اهمیت و حساسیت این حوزه هرچه بیشتر مشخص شود.

در نهایت در **جمع‌بندی و پیشنهادهای راهبردی**، نتیجه‌گیری گزارش انجام گرفته است و تعدادی پیشنهاد راهبردی برای کمینه کردن تهدیدات و مواجهه هرچه بهتر با عملیات‌های اوسینتی ارائه شده است.

واژگان کلیدی: اوسینت، بیولوژی، جنگ بیولوژیک، فراداده

مقدمه

مقدمه

اطلاعـات منبـع بـاز یـا به‌اختصـار اوسـینت[1] بـه مجموعـه‌ای از روش‌هـا و ابزارهـا بـرای جمـع‌آوری و تحلیـل داده‌هـای منبـع بـاز بـرای اسـتحصال داده‌هـای ارزشـمند و حتـی حیاتـی اطلاق می‌شـود. بـه بیان دیگر، اوسـینت علـم جسـتجوی بسـیار هوشـمند در بیـن داده‌هایـی اسـت کـه در دسـترس عمـوم قـرار دارد (اسـتیل ۲۰۰۷، ص. ۱۲۹). یـک متخصـص اوسـینت، نیازی بـه هـک و نفـوذ نـدارد و پیگیـر ایـن مسـئله هـم نیسـت، بلکـه تنهـا چیزی کـه نیـاز دارد، داده‌هـای عمومـی اسـت کـه در دسـترس همـگان اسـت و هـر روز بـا آنهـا مواجـه می‌شـوید. ازایـن‌رو هـدف اوسـینت کشـف اطلاعـات مهـم و گاهـی بسـیار محرمانـه بـدون نیـاز بـه سـرقت آن‌هاسـت و بـه ایـن خاطـر اسـت کـه در بـدو امـر اوسـینت یـک مفهـوم پارادکسـیکال بـه نظـر می‌رسـد (میلـر ۲۰۱۸، صـص. ۷۰۴-۷۰۵). اوسـینت یـک مفهـوم نویـن نیسـت و نسـل اول اوسـینت بـه جنـگ جهانـی دوم بـاز می‌گـردد (ویلیامـز و بلـوم ۲۰۱۸، ص. ۴). نسـل اول اوسـینت متکـی بـر دسترسـی به انتشـارات چاپـی بـه زبان‌هـای دیگـر و ترجمـه و تحلیـل آن‌هـا بـرای دسـتیابی بـه اطلاعـات مهـم بوده‌اسـت. از ایـن رو مهـارت ترجمـه مهم‌تریـن مهارتـی بوده‌اسـت کـه یـک فعـال اوسـینت نسـل اول بایسـتی بـه آن مجهـز

1. Open-Source Intelligence (OSINT)

می‌بوده‌است. با گسترش فضای مجازی و انفجار اطلاعات منتشرشده در آن اوسینت نیز دچار یک تحول جدی شد و متخصصان امروزه از اوسینت نسل دوم یاد می‌کنند. در اوسینت نسل دوم، مهارت‌های فنی برای استخراج و تحلیل داده‌های منتشرشده در فضای مجازی حرف اول را می‌زنند. به جای دسترسی کند و هزینه‌بر فیزیکی، دسترسی مجازی جایگزین شده‌است و امکان اکتساب مستمر و آن‌به‌آن اطلاعات منبع‌باز در سرتاسر دنیا فراهم آمده‌است. همچنین محتوای تولیدشده در فضای مجازی امروزه حیرت‌انگیز است تا جایی که در سال ۲۰۲۰ در هرروز ۵۰۰ میلیون توییت انجام شده‌است. روش‌شناسی اوسینت در تلاش است تا با جمع‌آوری، پردازش و تحلیل این حجم شگفت‌انگیز از داده، به اطلاعات ارزشمندی متناسب با نیازهای مدنظر دست یابد. یک متخصص اوسینت گاه ممکن است یک موضوع جزئی و خاص را مطالعه کند، مثلاً تصویر شخصی را در اختیار دارد و به دنبال نشانی منزل وی است؛ گاه نیز نیازمند تحلیل‌های عمیق و تجهیز فعالیت‌هایش با هوش مصنوعی و تحلیل کلان داده است (الدریج و دیگران ۲۰۱۷؛ اواجلیستا و دیگران ۲۰۲۰)، برای مثال زمانی که در پی تحلیل نظرات مردم یک کشور درباره سیاست‌های دولتی است.

پیش از هر چیز بایستی کاربردهای مختلف اوسینت را مدنظر داشت. اوسینت کاربردهای متنوع تجاری دارد. کشف سلایق و ترجیحات مشتریان بر اساس جمع‌آوری و تحلیل اطلاعات منبع باز نقشی محوری برای توسعه بسیاری از کسب‌وکارها دارد. بنابراین تعجبی ندارد که بسیاری از ابزارهای موجود اوسینت با اهداف تجاری

توسعه داده شده‌اند (همان، ص. ۲۱). اوسینت همچنین توسط نهادهای امنیتی برای کشف جرایم سایبری و سازمان‌یافته مانند خرید و فروش مواد مخدر و داروهای غیرقانونی (فرانک و میخایلوف ۲۰۲۰)، و کودک‌آزاری (چارالامبوث و دیگران ۲۰۱۷) استفاده شده‌است و نتایج ارزشمندی به بار آورده‌است. افکار سنجی مدرک در زمینه‌های مختلف چون انتخابات نیز از طریق روش‌شناسی اوسینت به خوبی قابل انجام است (پستور-گالیندو ۲۰۲۰، ص. ۱۰۲۸۳).

بااین‌وجود نمی‌توان از تهدیدهای عملیات‌های اوسینتی نیز غافل شد. به اذعان متخصصین امر بسیاری از کاربردها و نتایج به‌دست‌آمده از اوسینت محرمانه باقی می‌مانند و هیچ‌گاه منتشر نمی‌شوند (ویلیامز و بلوم ۲۰۱۸، صص. ۲-۳)؛ بنابراین بررسی دقیق روش‌شناسی اوسینت و ابزارهای مورداستفاده آن و بررسی سناریوهای مختلف و احتمالی استفاده از آن تنها راه برای آمادگی در برابر استفاده‌های سوء از اوسینت توسط بیگانگان و کشورهای متخاصم است. این کار می‌تواند آمادگی مقابله احتمالی با چنین عملیات‌هایی را بالا برد و همچنین منجر به انجام اقداماتی شود که امکان بروز چنین تهدیدهایی را به حداقل برساند. نکته شایان توجه دیگر در این زمینه این است که اعتبار اطلاعات به‌دست‌آمده از اوسینت را نباید به‌صورت صفر و یکی (صادق و کاذب) ارزیابی کرد. بلکه در روش‌شناسی اوسینت مانند بسیاری از روش‌های کسب اطلاعات حیاتی، ما شاهد یک طیف از اعتبار اطلاعات هستیم (ویلیامز و بلوم ۲۰۱۸، ص. ۱۰). ازاین‌رو حتی اگر اعتبار اطلاعات به‌دست‌آمده نتواند به‌صورت ایدئال احراز شود، بااین‌وجود می‌تواند کمک شایان توجهی به جهت‌دهی عملیاتی‌های

مختلف داشته باشد.

محور اصلی این گزارش تهدیدهای احتمالی مبتنی بر اوسینت در حوزهٔ داده‌های زیستی است. این داده‌ها می‌توانند اثر انگشت، نمونه خون، چهره، گروه خونی، نژاد و دیگر داده‌های زیستی گروهی از مردم (مانند ایرانیان) را شامل شود. همان‌طور که در این گزارش خواهیم داد، اوسینت شیوه‌های جدیدی را برای به‌دست‌آوردن این داده‌ها به دست می‌دهد که چنانچه سوء نیتی وجود داشته باشد، این داده‌ها برای واردکردن آسیب‌های جدی مورداستفاده قرار گیرند. همان‌طور که ذکر شد، در حوزه تهدیدهای اوسینت اطلاعات غیرمحرمانه اندکی در دست است و محققان تنها با بررسی روش‌ها و ابزارهای اوسینت، عملیات‌های تهدیدآمیز احتمالی را به‌صورت مهندسی معکوس و باتکیه‌بر فرضیات موجه کشف می‌کنند. همچنین دیدیم که در اوسینت اعتبار اطلاعات به‌صورت طیفی (تشکیکی - فازی) ارزیابی می‌شود و لازم نیست اعتبار اطلاعات به‌صورت ۱۰۰٪ احراز شده باشد تا ارزشمند تلقی گردد. بسته به حساسیت موضوع، اطلاعات احتمالی نیز می‌توانند ارزشی حیاتی داشته باشند.

پیش از ورود به این بحث لازم است، بحثی کوتاه حول روش‌شناسی اوسینت و ابزارهای آن داشته باشیم.

بخش اول

روش شناسی و ابزارهای اوسینت

بخش اول

روش‌شناسی و ابزارهای اوسینت

ویلیامز و بلوم (۲۰۱۸)، اوسینت را متکی بر یک چرخه ۴ مرحله‌ای می‌دانند: ۱) جمع‌آوری، ۲) پردازش، ۳) به‌کارگیری[1] و ۴) تولید که به طور خلاصه به معنای کسب اطلاعات، صحت‌سنجی آن‌ها، تشخیص ارزش آن‌ها و عرضه آن به متقاضیان است (ص. ۱۳). در مرحله نخست، به‌روش‌های مختلف اطلاعات جمع‌آوری و نگه‌داری می‌شوند. اطلاعات موجود در فضای مجازی و شبکه‌های اجتماعی منبعی عالی برای جمع‌آوری اطلاعات هستند که به لطف نسل دوم وب فراهم آمده‌است. امروزه به راحتی می‌توان اطلاعات میلیاردهای توییت موجود را ذخیره کرد. اگر دشواری را که فعالان اوسینت نسل اول در جمع‌آوری روزنامه‌ها، مجلات و کتب چاپی کشورهای دیگر و انتقال آن‌ها به کشور مبدأشان را داشتند مدنظر بیاوریم به تحول انقلابی‌ای که در این زمینه رخ داده‌است اذعان خواهیم کرد. با این وجود شاید مهم‌ترین مرحله در روش‌شناسی اوسینت، مرحله پردازش و قابل‌استفاده‌کردن آن‌ها باشد. در اوسینت نسل اول، این ترجمه انسانی اطلاعات بود که مهم‌ترین مرحله پردازش اطلاعات محسوب می‌شد. ولی امروزه با ظهور فناوری‌های گسترده چون پردازش

1. Exploitation

زبان طبیعی، ترجمه ماشینی، یادگیری ماشین و هوش مصنوعی، روش‌های پردازش اطلاعات به طرز حیرت‌انگیزی کارامدتر شده‌اند. در مرحله سوم (به‌کارگیری) که گاهی تحلیل نیز نامیده می‌شود، صحت‌سنجی اطلاعات و ارزش آن‌ها مورد بررسی قرار می‌گیرد. با حجم حیرت‌انگیز از داده‌های موجود، صرف جمع‌آوری و پردازش داده‌ها کفایت نمی‌کند و لازم است داده‌های خوب و بد از هم جدا شوند. منظور از داده بد صرفاً داده‌ها کاذب نیستند بلکه داده‌های صادق ولی بی‌کاربرد (بی‌ربط) را نیز در بر می‌گیرد. هم‌گام با گسترش سریع اطلاعات در فضای مجازی، حجم داده‌های کاذب و بی‌فایده نیز نسبت به گذشته رشد نمایی داشته‌است و این اهمین مرحله به‌کارگیری را دوچندان می‌کند. در مرحله آخر نیز نتیجه سه مرحله قبل به صورت قابل استفاده و قابل‌فهم به متقاضیان مدنظر ارائه می‌شود. شکل (۱) روش‌شناسی چهارمرحله‌ای اوسینت را نشان می‌دهد.

شکل (۱) روش‌شناسی چهارمرحله اوسینت

در هرکدام از مراحل فوق روش‌های مختلفی قابل استفاده هستند که جالب‌ترین آن‌ها مربوط به مرحله به‌کارگیری و تحلیل داده‌هاست. در واقع وقتی از نسل دوم اوسینت صحبت می‌کنیم جمع‌آوری و پردازش اطلاعات در فضای مجازی کار سختی محسوب نمی‌شود و امروزه منابع و روش‌های آسانی برای جمع‌آوری و ترجمه/تجمیع اطلاعات در فضای مجازی وجود دارد. این صحت‌سنجی و زمینه‌مندکردن اطلاعات (یعنی یافتن الگوهای مهم در آن‌ها و تمییز داده‌های مرتبط و غیرمرتبط) است که محوری‌ترین بخش یک عملیات اوسینتی محسوب می‌شود. با عنایت به این موضوع امروزه روش‌های مختلفی

برای تحلیل اطلاعات منبع‌باز ارائه شده‌است که در ادامه به معرفی آن‌ها می‌پردازیم (ویلیامز و بلوم ۲۰۱۸، صص. ۳۸-۵۰).

تحلیل واژگانی[1]: بررسی داده‌های خام متنی برای کشف روابط و ویژگی‌های آن‌ها. در ساده‌ترین مدل، تحلیل واژگانی می‌تواند واژگانی را که بیشترین میزان جستجو را به خود اختصاص داده‌اند عیان کند و در شیوه‌های پیشرفته‌تر می‌تواند با تحلیل متن، اطلاعاتی نظیر اطلاعات قومیتی، سنی و اقتصادی صاحبان متن را استخراج کند.

تحلیل کلیدی بودن[2]: این تحلیل به دنبال یافتن میزان تکرار واژگان در یک متن مشخص است. این امر می‌تواند به کشف سریع موضوع و جهت‌گیری یک متن کمک کند و همچنین می‌تواند اطلاعات بیشتری را نیز در مورد متن نشان دهد. برای مثال به‌کاربردن واژگانی مشخص در کنار هم و یا به‌کاربردن/نبردن واژگانی خاص می‌تواند اطلاعات ارزشمندی را در مورد متن و نویسنده آن به دست دهد (مرجع؟)

تحلیل احساسات[3] **و تحلیل موضع**[4]: تحلیل احساسات به شناسایی واژگان و ساختارهایی می‌پردازد که می‌توانند احساسات شخص صاحب متن را عیان کنند. برای مثال کشف خوشحالی، ناراحتی، رضایت یا میزان قاطعیت یک نوشتار از طریق تحلیل احساسات ممکن می‌شود. تحلیل موضع نیز می‌تواند ارزش‌های بنیادینی را که صاحب متن دارد (مثلاً نژادپرستی، مذهبی بودن و ...) به دست دهد.

تحلیل شبکه اجتماعی: تحلیل شبکه‌های اجتماعی ارتباط

1. Lexical Analysis
2. Keyness Analysis
3. Sentiment Analysis
4. Stance Analysis

میان افراد و نقش آن‌ها را در میان تعاملات افراد بررسی می‌کند. این تحلیل موجب به‌دست‌آمدن حجم عظیمی از داده‌ها در مورد افراد و ارتباطاتشان با یکدیگر شده است. در واقع با بررسی گراف روابط و تعاملات اشخاص با یکدیگر در شبکه‌های اجتماعی می‌توان اطلاعات ارزشمندی مانند نسبت‌های خانوادگی، دوستی‌ها و میزان تأثیروتأثر افراد از یکدیگر را به دست آورد. همان‌طور که خواهیم دید، کشف نسبت‌های خانوادگی می‌تواند به معنای افشای اطلاعات مهمی بیولوژیک نیز باشد.

تحلیل فضایی[1]: در تحلیل فضایی با بررسی فراداده‌های مرتبط با تصاویر و پست‌های موجود در فضای مجازی در مورد موقعیت مکانی افراد و مکان‌ها اطلاعات ارزشمندی به دست می‌آید. متأسفانه بسیاری از برنامه‌ها به‌صورت پیش‌فرض اطلاعات مکانی را به همراه تصاویر ثبت می‌کنند و کاربران نمی‌دانند که می‌توانند در تنظیمات گوشی‌شان این مورد را غیرفعال نمایند.

تحلیل صوت و تصویر: مانند تحلیل واژگان، تحلیل صوت و تصویر نیز می‌تواند اطلاعات بسیاری زیادی را برملا کند. تشخیص چهره و کشف قومیت ازروی گویش و صدای افراد تنها بخشی از کاربردهای تحلیل صوت و تصویر است. فناوری‌های پیشرفته تحلیل صوت و تصویر عمر کمتری نسبت به فناوری‌های تحلیل متن دارند، بااین‌وجود به نظر می‌رسد باتوجه‌به حجم بسیار بالای محتوای چندرسانه‌ای تولیدشده در بستر اینترنت، این فناوری‌ها نقش بیشتر و بیشتری را در آینده نزدیک ایفا کنند.

بایستی توجه کرد که در تمامی روش‌های فوق فناوری‌های

1. Geospatial Analysis

چون هوش مصنوعی، یادگیری ماشین و تحلیل کلان داده‌ها نقش محوری ایفا می‌کنند. شکل (۲) اهم روش‌ها و ابزارهای مورداستفاده در عملیات‌های اوسینتی در فضای مجازی را به نمایش می‌گذارد.

شکل (۲) اهم روش‌ها و ابزارهای مورد استفاده در اوسینت

حال با داشتن مقدمه و چهارچوب فوق، حال تلاش می‌کنیم تا سناریوهای محتمل تهدیدات ناشی از اوسینت را با تمرکز بر سوءاستفاده از داده‌های بیولوژیک ایرانیان به تصویر کشیم.

بخش دوم

اوسینت و داده‌های بیولوژیک

بخش دوم

اوسینت و داده‌های بیولوژیک

سال‌هاست ایرانیان فعالیت پویا و گسترده‌ای در فضای سایبری دارند. در ۲۰ سال گذشته، ابزارهای یاهومسنجر[1]، ایران کلابز[2]، کلوب دات‌کام[3]، فیسبوک و در نهایت پیام‌رسان‌ها، میزبان ایرانیان بوده‌اند و داده‌های ایرانیان را در سرورهایشان ضبط و ثبت کرده‌اند. از طرف دیگر، در این مدت هکرها نیز داده‌های زیادی را منتشر کرده‌اند. این داده‌ها به همراه فراداده‌هایشان مهم‌ترین اطلاعاتی است که متخصصین اوسینت[4] آن‌ها را می‌کاوند. هدف این بخش، بررسی توان متخصصین اوسینت در استخراج داده‌های بیولوژیکی است که می‌تواند نیروهای متخاصم را علیه جمهوری اسلامی ایران یاری کند. به‌خصوص که پس از ظهور و گسترش بیماری کرونا در اواخر سال ۱۳۹۸ زمین وارد فاز جدیدی از ارزش‌گذاری‌های بیولوژیک شده است و قدرت‌های بزرگ جهان توسط این ویروس به چالش کشیده شده‌اند. در هر قسمت سعی شده است به یکی از انواع داده‌های بیولوژیک دسترس‌پذیر در فضای مجازی اشاره کنیم و نحوه استخراج، هوشمندسازی و احتمال این بحران توسط آن داده‌ها را به تصویر بکشیم. همان‌طور که پیش‌تر تأکید شد، به‌خاطر ماهیت محرمانه آن‌ها،

1. Yahoo Mesenger
2. http://forums.iranclubs.org/
3. www.cloob.com
4. OSINT (Open Source Intelligence)

مستندات زیادی از تهدیدات ناشی از اوسینت در دسترس نیست. بااین‌وجود، با شناخت روش‌شناسی و ابزارهای اوسینت و استفاده از مهندسی معکوس و مقداری قوه تخیل می‌توان سناریوهای محتملی را مطرح کرد.

منظور از داده‌های بیولوژیک داده‌هایی چون گروه خونی، اثر انگشت، نژاد، DNA و دیگر ویژگی‌های زیستی انسان‌هاست. قبل از این که ببینیم دسترسی به این داده‌ها چگونه از طریق اوسینت ممکن است بایستی به اهمیت احتمالی داده‌های بیولوژیک اشاره کنیم. فرض کنید به طریقی بتوان عکسی با کیفیت از اثر انگشت یک نفر پیدا کرد. امروزه با فناوری پرینت سه‌بعدی می‌توان به‌راحتی نمونه‌ای مصنوعی از انگشت این شخص را ایجاد کرد و از آن برای مقاصد مختلف (جعل سند یا ایجاد اتهام کاذب) استفاده کرد یا از شخص مدنظر اخاذی کرد. به طریق مشابه فرض کنید که امکان به‌دست آوردن نمونه‌های خونی متعددی از یک قومیت برای یک دولت متخاصم فراهم شود. از این طریق امکان استخراج نقشه ژنتیکی این ملت و استفاده از آن در ترورهای بیولوژیک ممکن می‌شود.

همان‌طور که دیدیم اولین قدم در روش‌شناسی اوسینت، جمع‌آوری داده‌هاست. چگونه می‌توان داده‌های بیولوژیک ایرانیان را از منابع منبع باز استخراج کرد؟

۲-۱- جمع‌آوری داده‌های بیولوژیک ایرانیان در فضای مجازی

همان‌طور که در ادامه خواهیم داد، بخشی از اطلاعات موردنیاز

برای استخراج داده‌های بیولوژیکی در اینترنت موجود است. ساعات فعالیت و خواب افراد و غذاهای مصرف‌شده از جمله این داده‌ها هستند. بااین‌وجود برخی دیگر از این داده‌ها در حالت عادی قابل‌دسترسی نیستند. ولی می‌توان به روش‌های مختلف افراد را بدون ایجاد حساسیت، تشویق به انتشار این اطلاعات کرد. در ادامه چند مثال در این مورد را بررسی می‌کنیم.

۲-۱-۱- تشویق به انتشار داده‌های زیستی

۲-۱-۱-۱- جمع‌آوری داده‌ها در پوشش پویش‌های درخواست کمک

این فعالیت که شاید خطرناک‌ترین و صریح‌ترین فعالیت در راستای جنگ بیولوژیک در فضای وب باشد بدین صورت است که با ادعای کمک و اعانه به بیماران سرطانی، مغز استخوان و ... از افراد اطلاعات دقیق خانوادگی، بزاق و حتی خونی دریافت می‌کنند و در انبارهای بیولوژیک خارج از کشور ذخیره می‌شوند. در تعدادی از این تلاش‌ها از بازیگران و سلبریتی‌های ملی نیز جهت افزایش اقبال عمومی به این پویش‌ها استفاده شده است و متأسفانه علی‌رغم روشنگری‌های رسانه ملی و شبکه‌های اجتماعی این درخواست‌ها گاهی با اجابت بخشی از مردم روبرو شده است. عکس (۱) نمونه‌ای از این پویش‌ها را در فضای مجازی نشان می‌دهد.

تصویر (۱) نمونه‌ای از پویش‌های جمع‌آوری نمونه‌های خونی برای مقاصد نوع‌دوستانه

۲-۱-۱-۲- جمع‌آوری اطلاعات از طریق چالش‌های مختلف

چالش، اصطلاحی است در شبکه‌های اجتماعی که به سرگرمی‌های غیرعادی اجتماعی گفته می‌شود که از افراد دعوت می‌کنند تا دستورالعملی غیرمعمول را اجرا کنند. هدف بنیادین این چالش‌ها تفریح و سرگرمی است و عمدتاً در حالت عادی افراد نسبت به اجرای دستورالعمل‌های چالش اکراه دارند. اصطلاح چالش نیز دقیقاً از همین منشأ به وجود آمده است؛ بنیان‌گذاران نخستین چالش‌ها، جرئت دوستان خود را به چالش می‌کشند و از آنها دعوت می‌کنند این کار غیرعادی را انجام دهند. یکی از معروف‌ترین و نخستین چالش‌ها،

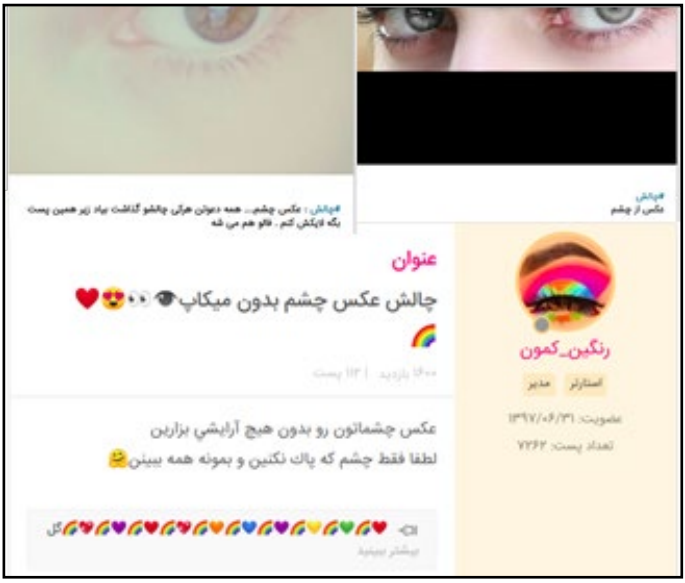
چالش آب یخ بود که پشتیبانی رسانه‌ای گسترده‌ای نیز از آن شد. طبق این چالش فرد بین خالی‌کردن یک سطل آب یخ روی بدن نیمه برهنه (و ضبط و پخش ویدئوی آن) یا ۱۰۰ دلار کمک به جامعه بیماران ALS مخیر می‌شد. افراد در پایان چالش انتخابی‌شان، می‌توانستند دیگران را نیز به چالش دعوت کنند. دعوت‌شدگان تا ۲۴ ساعت فرصت داشتند تصمیم بگیرند و یکی از دو گزینه را انتخاب کنند. البته این چالش موفق شد میلیون‌ها دلار به جامعه بیماران مختلف از جمله جامعه ALS کمک کند.[1] پس از چالش آب یخ، چالش‌های مجازی متعددی شکل گرفت که به‌مرور اهداف خیریه از آنها حذف و تنها هدف‌گذاری تفریحی در آنها لحاظ شده بود. به‌هرحال امروزه با چالش‌هایی مواجه هستیم که داده‌های مهمی (از جمله داده‌های بیولوژیک) را خواسته یا ناخواسته منتشر می‌کنند. نهادهای امنیتی متخاصم نیز می‌توانند با طراحی چالش‌های بیولوژیک و مهندسی اجتماعی یا با رصد چالش‌های موجود به جمع‌آوری داده بپردازند. هرچند امروزه چالش‌ها به حدی از گستردگی رسیده‌اند که نیروهای اطلاعاتی ممکن است از پشتیبانی اطلاعات لو رفته در چالش‌ها ناتوان باشند.

۲-۱-۱-۲-۱- عکس چشم:

این چالش در شبکه‌های اجتماعی فارسی‌زبان رواج محدودی دارد و تصاویر چشم ایرانیان و افغان‌ها با کیفیت بالایی در اختیار نیروهای اطلاعاتی دشمن قرار می‌گیرد. گستره این چالش منحصر به کاربران فارسی‌زبان شبکه‌های اجتماعی خارجی نیست و در شبکه‌های داخلی

1. https://www.iribnews.ir/fa/news/2592322/فوت-مبتکر-چالش-سطل-آب-یخ

و حتی علمی نیز دیده می‌شود. سایت تخصصی نینی‌بان (راهنمای بارداری و کودک‌یاری)، شبکه اجتماعی ویسگون، توییتر و ... بسترهایی بودند که این چالش در آنها رصد شده‌اند (استقبال از این چالش همواره محدود بوده است) (عکس ۲).



تصویر (۲) تصاویری از چالش عکس چشم

۲-۱-۱-۲-۲- انگشت ممهور انتخاباتی:

نمایش دادن انگشت جوهری در انتخابات‌های از امور متداولی است که در هر انتخابات به‌رسم نشان‌دادن وفاداری به آرمان‌های اسلام و انقلاب اتفاق می‌افتد. این از معدود چالش‌هایی است که (بدون

استفاده از کلمه چالش) و با هدفی غیر تفریحی به طور مستمر وجود داشته و دارد. در کنفرانس Chaos Computer، سخنرانی به نام جان کریسلر[1] با استفاده از عکس با کیفیتی که از انگشت وزیر دفاع آلمان گرفته شده بود، موفق شد اثر انگشت وی را بازسازی کند (هرن ۲۰۱۴). قابل‌توجه اینکه با داشتن اثر انگشت یک فرد، بازسازی اثر انگشت و جعل آن در محل دلخواه، به‌راحتی ممکن است و آموزش‌های دقیق و مختلفی نیز جهت ایجاد اثر انگشت جعلی در فضای وب وجود دارد.[2] البته درصورتی‌که به یک چاپگر سه‌بعدی دسترسی داشته باشید کار بسیار ساده‌تر خواهد بود و هر نوجوانی با استعداد متوسط نیز قادر به ایجاد اثر انگشت جعلی خواهد بود. اثر انگشت جعلی، خطری است که بسیاری از مقامات کشوری و لشگری را تهدید می‌کند. دقت کنید در محیط انتخابات وجود تعداد زیادی دوربین با کیفیت عالی کاملاً عادی است و باتوجه‌به نمایش انگشت جوهری، تهیه تصویری دقیق و با جزئیات از اثر انگشت مسئولین، امری سهل‌الوصول خواهد بود. همین‌طور جمع‌آوری تصاویر متعددی که از انگشتان

تصویر (۴) دسترسی آسان به عکس‌های انگشت مهرزده افراد مختلف

1. Jan Krissler
2. https://www.aparat.com/v/673q0/اثر_انگشت_تقلبی_چگونه_درست_می_شود؟

مسئولین منتشر شده نیز می‌تواند در این امر کمک کند. متأسفانه اکثریت قریب به‌اتفاق رای‌دهندگان اجازه تصویربرداری از انگشتشان را به خبرنگاران و اطرافیانشان می‌دهند (عکس ۴). همان‌طور که پیش‌تر ذکر شد، وجود تصاویر با کیفیت از اثر انگشت اشخاص وقتی با فناوری‌هایی چون پرینت سه‌بعدی ترکیب شود امکان ساختن انگشت مصنوعی افراد را می‌دهد. این امر می‌تواند منجر به جعل سند، زدن اتهام کاذب به افراد (با گذاشتن اثر انگشت آن‌ها در صحنه جرم) و یا اخاذی از ایشان گردد.

۲-۱-۱-۲-۳- چالش ۴، عکس ده سال قبل:

در این چالش معروف و همه‌گیر افراد باید تصاویر ۱۰ سال پیش خود و امروز خود را کنار هم منتشر کنند و روند پیر شدنشان را به رخ دیگران بکشند. این چالش داده‌هایی فراهم می‌کند تا نیروهای اطلاعاتی، به‌سرعت، پایگاه داده‌ای بزرگ و کم‌هزینه تهیه کنند که روند پیر شدن را نمایان می‌سازد. این پایگاه داده شامل میلیون‌ها زوج تصویر است که یکی برچسب قدیمی و دیگری برچسب جدید دارد. با داشتن این پایگاه داده و تحلیل آن دشمن قادر خواهد بود:

۱. با دریافت دو تصویر، آن‌ها را با یکدیگر انطباق دهد و با دقت بهتری یکتایی هویت دو تصویر را تشخیص دهد (مشکلات ناشی از عامل پیر شدن را بهبود ورزد).

۲. تصویر فرد در ۱۰ سال آینده را پیش‌بینی کند.

به‌عنوان یک ابزارسازی قوی مبتنی بر چالش ۱۰ سال قبل، می‌توان اپلیکیشن FaceApp را مثال زد، این اپلیکیشن در آزمون‌های

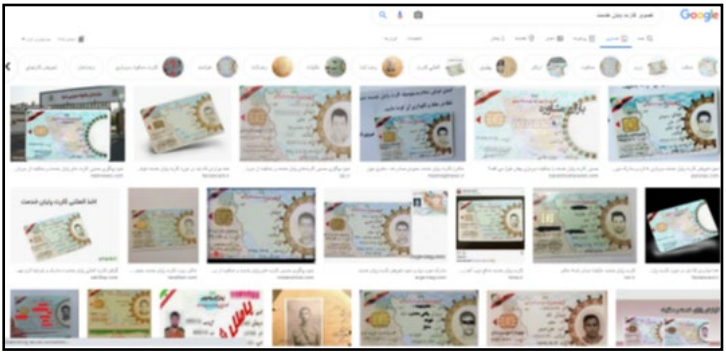
آزمایشگاهی با دقت قابل قبولی چهره‌ها را پیش‌بینی کرد. باتوجه‌به این ابزار عمومی، به نظر می‌رسد مراکز نظامی با دقتی بسیار نزدیک به واقعیت قادر به پیش‌بینی چهره مخالفین خود باشند. برای مثال فرض کنید که یک سرویس متخاصم در پی ترور شخصی است که آخرین نسخه عکس موجود از وی مربوط به ۱۰ سال پیش است؛ ابزارهای فوق می‌توانند با دقت بسیار بالایی چهره کنونی این فرد را برای نیروهای متخاصم آشکار نمایند.

۲-۱-۱-۲-۴- روش ۴، چالش‌های عکس کارت ملی

در این چالش کاربر با انتشار تصویر کارت ملی خود، نشان می‌دهد که از انتشار عکس بدون آرایش، فاقد روتوش و پرسنلی‌اش هراسی ندارد. عکس کارت ملی نسبت به بسیاری از عکس‌ها و تصاویری که در فضای وب منتشر می‌شود اهمیت بیشتری دارد، زیرا تمامی این تصاویر از یک زاویه، بدون آرایش و کاملاً استاندارد تهیه می‌شوند. چنین پایگاه داده‌ای اگر برچسب‌گذاری مناسبی شود نسبت به همه پایگاه داده‌های دیگری که در این گزارش معرفی شده‌اند، اهمیت بیشتری دارد و می‌تواند موضع نیروهای متخاصم را علیه منافع ملی ایران تقویت کند. برای مثال، عکس کارت ملی برای تعیین نژاد به‌مراتب گویاتر از تصاویر خوشگذرانی در کنار رودخانه خواهد بود. هرچند این چالش به‌اندازه چالش‌های پرطرفدار دیگر مانند چالش آب یخ یا چالش ده سال پیش، پرطرفدار نشد ولی اطلاعات قدرتمندی را از کشور خارج کرد.

متأسفانه حجم قابل‌توجهی کارت شناسایی در دسترس عموم قرار

دارد که شامل کد ملی (شناسنده محل تولد) و برخی اطلاعات حیاتی دیگر است. حتی خبرگزاری‌های رسمی و قانونی نیز بعضاً به انتشار سانسور نشده اطلاعات خصوصی مردم مبادرت می‌ورزند. اطلاعات لو رفته به حدی زیاد و قابل‌توجه است که حتی جستجوی عبارت‌های «کارت پایان خدمت»، «کارت دانشجویی» و ... در موتور جستجوها می‌تواند کمک شایانی به نیروهای متخاصم در تقویت پایگاه داده‌های بیولوژیک و غیر بیولوژیک داشته باشد. همان‌طور که در عکس (۵) می‌بینید یک کاربر متبحر می‌تواند با صرف چند دقیقه زمان و هوشمندی در استفاده از موتورهای جستجو، حجم قابل‌توجهی از کارت‌های شناسایی با عکس‌های پرسنلی جمع‌آوری کند.



تصویر (۵) نتیجه جستجوی کلمه تصویر کارت پایان خدمت در موتور جستجوی گوگل

۲-۱-۲- استفاده از داده‌های لو رفته

در جهان، سالانه تلاش‌های متعددی برای هک و نفوذ انجام می‌شود که ایران نیز در این میان استثناء محسوب نمی‌شود. ایران به‌عنوان یکی از قربانیان حملات سایبری چندین بار متحمل

شکست‌های سنگینی شده است و پایگاه داده‌هایی که حتی شامل داده‌های بیولوژیک بودند لو رفته است. برای مثال پایگاه داده لو رفته یکی از اپراتورهای همراه اول شامل نام، نام خانوادگی، کد ملی، شماره شناسنامه، آدرس دقیق، تلفن ثابت و کد پستی است. آدرس‌های یکسان در این پایگاه داده به همراه نام خانوادگی یکسان به معنای پیوند خونی یا به معنای پدر و فرزندی است یا به معنای هم والد بودن است که می‌تواند در توسعه و تکمیل گراف روابط اجتماعی به‌خوبی کارساز باشد. البته داده‌های لو رفته به‌روزتری نیز موجود است. در نوروز ۱۳۹۹ خبری مبنی‌بر لورفتن داده‌های بیش از ۷۰ میلیون ایرانی از طریق نفوذ به وزارت بهداشت لو رفت که شامل نام پدر نیز می‌شد و کار را برای تشکیل گراف بسیار ساده‌تر می‌کرد.[1] چنین اتفاقاتی منحصر به ایران نیست و داده‌های اتباع ترکیه با دقت کامل که حتی شامل بیمارستان محل تولد نیز می‌شد، سال‌هاست که در ویکی‌پدیای تاریک وب در دسترس عموم قرار دارد.[2] توجه نمایید که هرچند در یک فعالیت اوسینتی عملیات هک و نفوذ جایگاهی ندارد ولی داده‌های لو رفته که در دسترس عموم قرار می‌گیرد یکی از منابع مهم در علم اوسینت محسوب می‌شود.

حال اجازه دهید تعدادی سناریوی پردازش و تحلیل اطلاعات باز بیولوژیک ایرانیان را که به طرق مختلف جمع‌آوری شده‌اند، بررسی کنیم .

1.http://www.baharnews.ir/news/208279/افشای-اطلاعات-هویتی-۷۰-میلیون-ایرانی-اینترنت

2. http://torc5bhzq6xorhb4.onion/ (برای استفاده از این سایت باید وارد بخش تاریک وب شوید، همچنین این لینک چند ماه پس از انتشار به صورت خودکار غیرفعال می‌شود.)

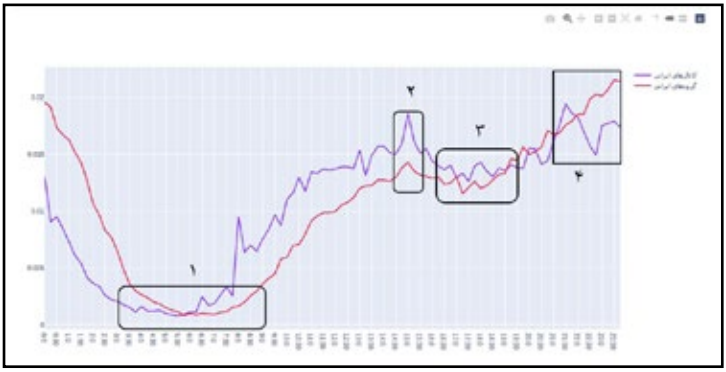
۲-۲- تحلیل ساعات فعالیت روزانه (استراحت، فعالیت کاری و تغذیه)

۲-۲-۱- تحلیل ۱، پیام‌رسان تلگرام

با تحلیل ساعات ارسال پیام کاربران در پیام‌رسان‌ها و شبکه‌های اجتماعی ساعات فعالیت روزانه کاربران (و مردم) قابل استخراج است. نمودار (۶) زیر حاصل برهم‌نهی چند کانال تلگرامی است که در موضوعات خبر، تفریح، رایانه و ... فعال هستند. طبق نمودار زیر (که از ۱۰ کانال و نزدیک به ۱۰۰ هزار پیام استخراج شده است) می‌توان ساعت خواب، بیداری، غذا خوردن و استراحت‌های روزانه جامعه ایرانی به‌راحتی قابل استخراج است.

تصویر (۶) نمودار توزیع تجمعی ساعت ارسال پیام در کانال‌های ایرانی

اما داده‌های فوق یک ایراد دارد. داده‌های فوق حاصل تجربه مدیران بنگاه‌های سخن‌پراکنی است و لزوماً این تجربه بیانگر واقعیت جامعه ایرانی نیست؛ لذا به تحلیل گروه‌های عمومی ایران می‌پردازیم و آن را با کانال‌ها مقایسه می‌کنیم.



تصویر (۷) نمودار توزیع تجمعی ساعت ارسال پیام در کانال‌ها و گروه‌های عمومی[۱] ایرانی

در عکس (۷)، محدوده ۱، ساعات خواب اکثریت جمعیت ایران را بیان می‌کند. البته در این ساعت‌ها نیز فعالیت مجازی به صفر نرسیده، همچنین روند نزولی و صعودی تعداد پیام‌ها پیش‌وپس از محدوده ۱ بیانگر بخشی از مردم است که در آن ساعت‌ها خوابیده‌اند. ناحیه شماره ۲، جهش پس از صرف نهار را نشان می‌دهد. ناحیه ۳ نیز استراحت بعدازظهر است. واضح است که با افزایش تعداد پیام‌ها دقت نمودار و درعین‌حال اطلاعات آن افزایش پیدا می‌کند. در این نمودار تفاوت منحنی آبی و قرمز در ناحیه ۴ به دلیل مشتری‌مداری در کانال‌های عمومی رخ می‌دهد. همچنین همین بی‌نیازی از مشتری‌مداری باعث شده که از ساعت ۲۲ تا ۶ صبح در گروه‌ها آزادانه‌تر پیام ردوبدل شود تا کانال‌ها.

حال تلاش می‌کنیم با یک مستند قوی‌تر ادعاهایی را که نمودار فوق در باب عادات روزانه کاربران ایرانی بیان می‌کند، بررسی کنیم. به این منظور، گروه‌ها و پیام‌های نیمه‌خصوصی (بیش از ۶۰ هزار

۱. نمودار با تحلیل نزدیک به ۷۰۰هزار پیام در گروه‌های عمومی استخراج شده است.

پیام) و خصوصی (بیش از ۱۷ هزار پیام) را کنکاش می‌کنیم. عکس (۸) نتیجه این تحلیل است:

تصویر (۸) نمودارهای توزیع تجمعی ساعت ارسال پیام ایرانیان در گروه‌های عمومی و فضاهای خصوصی تلگرام[۱]

تنها دو تفاوت عمده در داده‌های عمومی و غیرعمومی مشاهده می‌شود:

۱. به دلیل تفاوت در برخورد با آشنایان و مراعات بیشتر در گروه‌های نیمه‌خصوصی، سرعت خاموش شدن گروه‌های نیمه‌خصوصی بیشتر از گروه‌های عمومی (و حتی کانال‌ها) است. گفتگوهای خصوصی‌تر نیز بدون دغدغه تا نیمه‌های شب می‌تواند تداوم داشته باشد.

۲. واضح است که داده‌های غیرعمومی بیانگر مسائل ریزتری نسبت به داده‌های عمومی است. باتوجه‌به اینکه نمونه‌گیری داده‌های غیرعمومی از خانواده‌های عادی ایرانی انتخاب شده‌اند، ساعت نماز صبح به‌وضوح خود را نشان می‌دهد. درحالی‌که همچنان به دلیل جلوگیری از مزاحمت برای دیگران، در گروه‌های عمومی پیامی ارسال نمی‌شود.

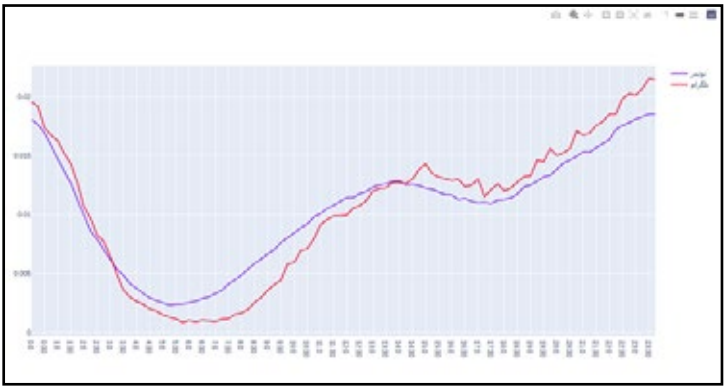
۱. روش جمع‌آوری داده خصوصی مبتنی بر نمونه‌گیری و جمع‌آوری داده‌های داوطلبانه بوده و دسترسی غیرقانونی یا استفاده از داده‌های لو رفته رخ نداده است.

۳. نوسان زیاد در داده‌ها خصوصی می‌تواند به دلیل کم بودن داده خصوصی اتفاق افتاده باشد.

به‌هرحال به دلیل ذات تلگرام که برخلاف شبکه‌های اجتماعی مبنی‌بر تعامل است، شبکه اجتماعی توییتر می‌تواند با دقت بیشتری عادات روزانه ایرانیان را آشکار کند.

۲-۲-۲- تحلیل ۲، تحلیل توییتر

شبکه اجتماعی توییتر برخلاف تلگرام که روح تعاملی (پیام‌رسانی و انتظار برای پاسخ) در آن مشهود است، محلی برای مونولوگ و تعامل با مخاطبین عام در بازه زمانی نسبتاً بلندمدت‌تر است. به بیان دقیق‌تر فرد توییت خود را در صفحه شخصی‌اش منتشر می‌کند و نه‌تنها پیام‌های صفحات هر شخص مخاطب خاص ندارد، بلکه مخاطبین وی خود را ملزم به پاسخگویی یا حداقل سرعت عمل در پاسخگویی نمی‌بینند. عکس (۹) بیانگر مقایسه داده‌های تلگرام و توییتر با یکدیگر است. برای استخراج داده‌های توییتر، ۱۲۰۰ تولیت ۴۸۶۲ کاربر تصادفی را استخراج کردیم (اگر کل توییت‌های ارسالی یک کاربر کمتر از ۱۲۰۰ عدد بود، همه توییت‌های وی استخراج شد) و در نهایت با استخراج بیش از ۳/۵ میلیون تولیت به نمودارهای زیر رسیدیم.



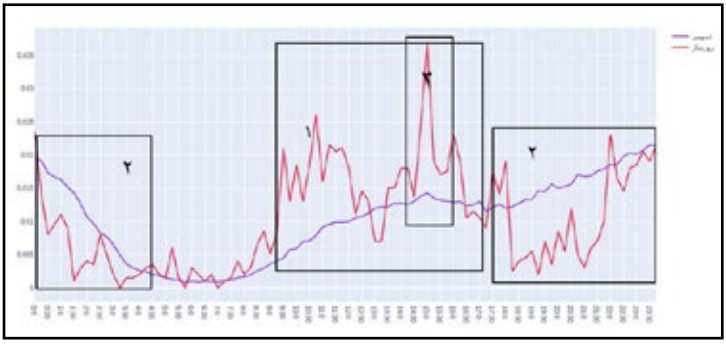
تصویر (۹) نمودارهای توزیع تجمعی ساعت ارسال پیام ایرانیان در تلگرام و توییتر[۱]

دلیل بزرگ‌تر بودن سرانه توییت‌های شبانه را می‌توان در عدم تعاملی بودن توییتر دانست که مراعات کردن ساعت خواب مخاطب را بی‌معنا می‌کند و نظم خواب و بیداری و استراحت را با دقت بیشتری نمایش می‌دهد. در نمودار تلگرام، تشخیص ساعت نهار باتوجه‌به جهشی که ساعت ۱۵:۰۰ اتفاق می‌افتد قابل تشخیص است. کاربران در این ساعت به پیام‌هایی دریافتی یک ساعت گذشته، پاسخ می‌دهند.

۲-۲-۳- تحلیل ۳، ماه رمضان

واضح است که ساعات فعالیت روزه‌داران در ماه مبارک رمضان نسبت به ماه‌های دیگر متفاوت خواهد بود. شب‌بیداری، فعالیت کمتر در ساعات غروب و افطار، آزاد بودن زمان نهار، بیدار ماندن پس از سحری و ... همگی تأثیرات خود را در نمودار فعالیت‌های کاربران در ماه رمضان بر جای می‌گذارند. در نمودارهای زیر، تفاوت رفتار

کاربـران در مـاه رمضـان را نسـبت بـه کل سـال در دو سـرویس تلگـرام و توییتـر می‌بینیـد. همچنیـن نمودارهـای مـاه رمضـان تلگـرام و توییتـر را مشـاهده می‌کنیـد. شـایان ذکـر اسـت کـه در نمـودار پیام‌رسـان تلگـرام، حـدود ۲۰۰۰ پیـام افـراد مذهبـی بررسـی شـده اسـت ولـی در مـورد توییتر فیلتـری روی کاربـران اعمـال نشـد و ۸۶ هـزار پیـام کاربـران عمومـی تحلیـل شـد. اگـر نمـودار سـاعات فعالیـت یـک کاربـر مذهبـی در ایـام مـاه رمضـان تغییـر خاصـی نکنـد یـا منطبـق بـر فعالیت‌هـای کاربـران مذهبـی در ایـام مـاه رمضـان نباشـد، می‌توانـد بیانگـر عـدم روزه‌داری وی (یعنـی ابتـلا بـه یـک بیمـاری جـدی) باشـد. البتـه درارتباط‌بـا کاربـران مذهبـی خانـم، می‌توانـد عـادت ماهانـه وی را فـاش کنـد.



تصویر (۱۰) مقایسه نمودار توزیع تجمعی ساعت ارسال پیام کاربران تلگرام در کل سال و مذهبی‌ها در ماه رمضان

تحلیل نمودار:

۱. تغییـر نمـودار از فعالیـت شـبانه بـه روزانـه؛ بـه دلیـل اینکـه در روزهـای رمضـان وقت‌گذرانـی در فضـای مجـازی افزایـش می‌یابـد.

۲. ناحیه ۳ محلی را نشان می‌دهد که در روزهای عادی، پس از تناول نهار است و در ایام ماه مبارک رمضان صرف ارتباط با اطرافیان می‌شود.

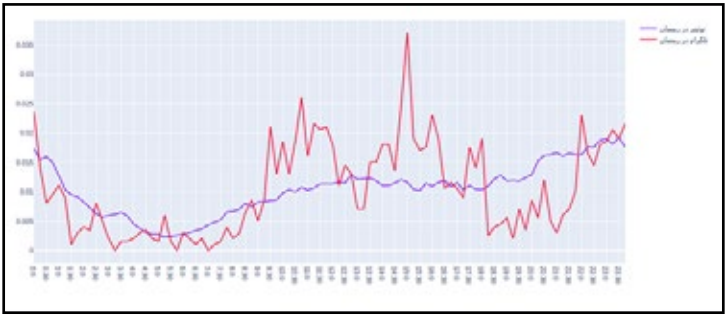
تصویر (۱۱) مقایسه نمودار توزیع تجمعی ساعت ارسال پیام کاربران توییتر در کل سال و ماه رمضان

تحلیل نمودار:

۱. بیدارشدن برای سحری

۲. افزایش ارتباطات پس از نماز صبح در ماه رمضان

۳. کاهش ارتباطات پیش از افطار و افزایش حجم پیام‌ها پس از افطار



تصویر (۱۲) مقایسه نمودار توزیع تجمعی ساعت ارسال پیام کاربران تلگرام و توییتر در ماه رمضان

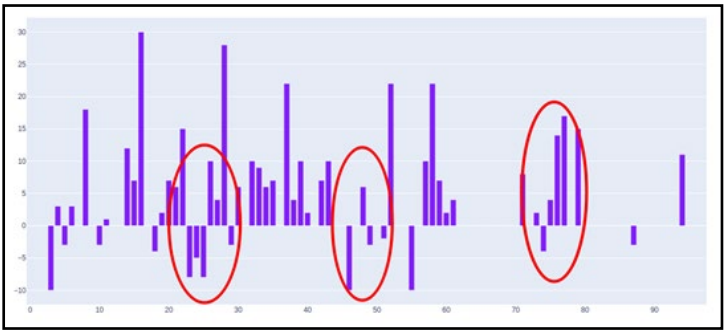
۲-۳- طول دوره عادت ماهانه زنان

تحلیل احساسات به‌عنوان یکی از زیرشاخه‌های متن‌کاوی وظیفه درک و تشخیص احساسات نهفته در متن را برعهده دارد. به‌عنوان‌مثال سایت نیوزویت به گزاره‌های زیر اشاره می‌کند:

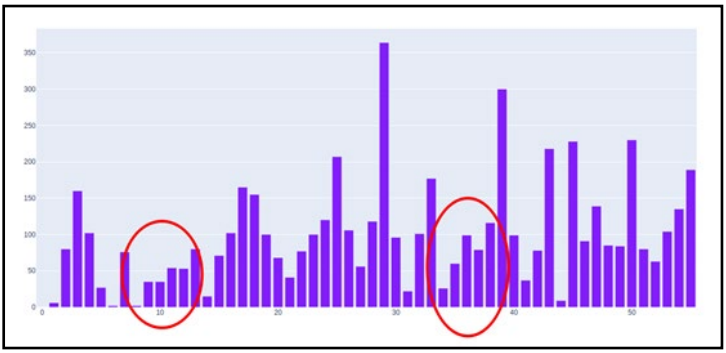
> برای مثال یک الگوریتم تحلیل احساسات باید تشخیص دهد که جمله «تحریم‌های آمریکا ظالمانه است» جمله‌ای با احساس منفی و جمله «مردم ایران در تمامی این سال‌ها به‌خوبی روحیه استکبارستیز خویش را حفظ نموده‌اند» دارای **جهت‌گیری و رویکردی مثبت** است.

از سوی دیگر باتوجه‌به روان‌شناسی عمومی زنان در طول عادت ماهانه،[1] این انتظار وجود دارد که در طول دوره قاعدگی خلق خوی زنان شکل خاصی به خود گیرد. زنان در طول دوره قاعدگی اضطراب، تندخویی، زودرنجی، کاهش فعالیت‌های فیزیکی و ... را شاهد هستند و این تغییر در فضای مجازی تأثیر خود را بر جای می‌گذارد. با ایجاد یک سازوکار امتیازدهی به پیام‌ها متناسب با احساس مثبت یا منفی آنها، موفق به امتیازدهی به روحیه روزانه کاربران شدیم (مجموع امتیاز پیام‌های روزانه). نمودارهای زیر بیانگر احساسات روزانه چند نفر از کاربران خانم توییتر است (به‌منظور حفظ اسرار شخصی، اطلاعات هویتی کاربران بیان نمی‌شود). در هر نمودار بخش تشخیص‌داده‌شده به‌عنوان دوره عادت ماهانه را محصور در دایره قرمز مشاهده می‌کنید.

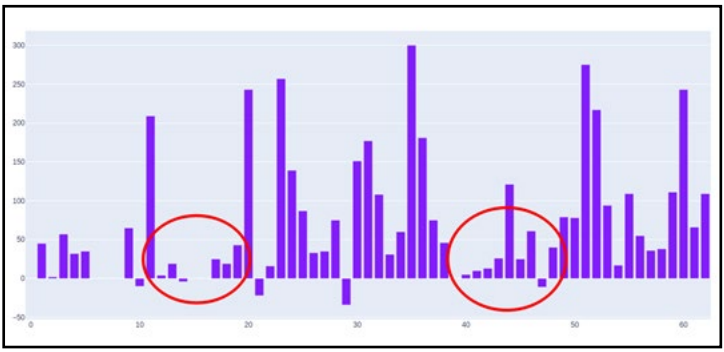
1. https://rastineh.com/حالات-روحی-زنان-دوران-قائدگی-۱/



تصویر (۱۳) نمودار احساسات روزانه یک کاربر خانم



تصویر (۱۴) نمودار احساسات روزانه یک کاربر خانم



تصویر (۱۵) نمودار احساسات روزانه یک کاربر خانم

رونـد فـوق به‌صـورت تجربـی و مبتنـی بـر مشـاهدات بـود کـه سـرعت و دقـت مدنظـر متخصصیـن هـوش مصنوعـی را تأمیـن نمی‌کنـد. ولـی آزمون‌هـای آمـاری مبتنـی بـر آنالیـز فوریـه وجـود دارد کـه در رشـته‌های طولانـی از اعـداد، می‌توانـد نظـم پریودیـک دیتـا را کشـف و نمایـان کنـد. آزمـون تبدیـل گسسـته فوریـه (طیف‌نـگاری) از معروف‌تریـن ایـن آزمون‌هاسـت و در ابـزار متن‌بـاز NIST Randomness tools [1] پیاده‌سـازی شـده اسـت.[2]

۲-۴- زبان مادری و نژاد

۲-۴-۱- روش ۱، نام کاربری

نام‌هـای کاربـری بـه طـور معمـول باتوجه‌بـه نـام حقیقـی، فرهنـگ و جامعـه کاربـر انتخـاب می‌شـود. بـرای مثـال در یـک جسـتجوی سـاده پیام‌رسـان تلگـرام متوجـه خواهیـد شـد کـه نـام بیشـتر کاربـران ایرانـی، کلمـات فارسـی، شـامل کاراکترهـای فارسـی،[3] یـا عبارتـی فارسـی ولـی بـا کاراکترهـای غیرفارسـی اسـت. لـذا نیـروی اطلاعاتـی کـه در پـی اسـتخراج اطلاعـات بیولوژیـک یـک کاربـر باشـد در همـان ابتـدای مسـیر بـا دیـدن نام‌کاربـری می‌توانـد ملیـت و تاحـدودی نـژاد وی را حـدس بزنـد. دقـت داشـته باشـید کـه همـواره سـوژه، مشـخص و از پیـش تعییـن شـده نیسـت، بلکـه ممکـن اسـت هـوش مصنوعـی در حـال پایـش مجموعـه‌ای از کاربران باشـد و ایـن روش می‌توانـد بـا دقـت مناسـبی نسـبت جمعیتـی را تخمیـن بزنـد و خطاهـای آن قابـل چشم‌پوشـی خواهـد بـود.

۱. این ابزار شامل آزمون‌هایی است که با هدف تشخیص تصادفی یا غیرتصادفی بودن یک رشته عدد طراحی شده‌اند؛ در یکی از آزمون‌ها به وجود نظم پریودیک پنهان در رشته عدد دردست بررسی، پرداخته می‌شود.

2. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication22-800r1a.pdf

۳. دقت کنید که برخی کاراکترهای فارسی و عربی متفاوت هستند، مانند «ک» و «ک»

۲-۴-۲- روش ۲، نگارش به زبان غیررسمی

عمده کسانی که در فضای سایبری به زبانی غیررسمی (در ایران غیرفارسی) تکلم می‌کنند یا می‌نویسند، به زبان مادری خود می‌نویسند؛ لذا تحلیل‌گران به‌راحتی می‌توانند نژاد شخص را تشخیص دهند. باتوجه‌به اینکه در ایران غیر از زبان فارسی، دیگر زبان‌ها، فرهنگستانِ مقبول عموم ندارند، با کمی دقت در نوشته‌ها علاوه بر نژاد حتی می‌توان متوجه لهجه محلی فرد نیز شد.

تصویر (۱۶) تکلم به زبان غیررسمی (ترکی آذربایجانی) به لهجه ارومیه‌ای

۲-۴-۳- روش ۳، برانگیختن احساسات نژادی

کمتر کسی است که با توهین به نژاد و قومیتش بتواند آرامش خود را حفظ کند، به‌خصوص اگر زبان وی، زبان رسمی کشور نباشد،

۱. لهجه‌های ارومیه‌ای و تبریزی لهجه معیار زبان ترکی آذربایجانی نیستند.

نـژاد او نـژاد حاکـم محسـوب نشـود یـا در موضـع ضعـف قـرار گرفتـه باشـد. نیروهـای اطلاعاتـی می‌تواننـد بـا تحریـک کاربـران آنهـا را وادار بـه عکس‌العمـل کـرده و اطلاعـات آنهـا را ثبـت کننـد. از معروف‌تریـن ایـن اقدامـات (تحریـک احساسـات قومـی) نظرسـنجی‌های غیرواقعـی نـام خلیج‌فـارس بـود کـه مدت‌هـا در آدرس http://www. persianorarabiangulf.com/ فعـال بـود[1] و هـدف ظاهـری آن سـایت تحریـک ایرانیـان بـرای ورود بـه ایـن سـایت و درآمدزایـی از راه تبلیغـات بـود. البتـه ممکـن اسـت شناسـه mac دسـتگاه‌هایی کـه از ایـن سـایت دیـدن کرده‌انـد نیـز به‌عنـوان دسـتگاه‌های ایرانـی ثبـت شـده باشـند.

۲-۴-۴- روش ۴، محل زندگی

باتوجه‌بـه آمـار رسـمی می‌تـوان از محـل زندگـی در مـورد نـژاد فـرد اطلاعاتـی کسـب کـرد. بـرای مثـال با کشـف اینکـه شـخصی اهل کرمانشـاه اسـت بـا مطالعـه بافـت جمعیتـی اسـتان کرمانشـاه می‌تـوان یـک توزیـع احتمالـی دربـاره نـژاد ایشـان در نظـر گرفـت. در مثالـی دیگـر یـک فـرد سـکنه جمهـوری آذربایجـان، تنهـا ۹/۵٪ ممکـن اسـت روس‌تبـار باشـد. در بخش‌هـای بعـدی نوشـتار بـه روش‌هایـی خواهیـم پرداخـت کـه تشـخیص محـل زندگـی را میسـر می‌کنـد.

۲-۴-۵- روش ۵، ادبیات نگارش

طبـق تحقیقـات و تجربیـات فنـی نگارنـده در حـوزه متـن‌کاوی، زبـان مـادری در نـگارش و کتابـت افـراد تأثیـر مسـتقیمی دارد. ایـن تأثیـر در هیسـتوگرام واج‌هـا، هجاهـا و کلمـات نمایـان می‌شـود. حتـی شـواهدی

۱. پس از غیرفعال شدن این سایت به مدت چند سال و منقضی شدن اعتبار آدرس، ایرانیان این آدرس را در دست گرفتند و در آن به معرفی خلیج فارس و تاریخچه آن پرداختند.

مبنی‌بر تأثیر آن بر طول کلمات و جملات نیز دیده شده است. مثال‌هایی از این مشخصه در ادامه می‌آید:

- بین افرادی که زبان مادری و دوران کودکی آنان ترکی آذربایجانی است ولی به زبان فارسی معیار تکلم و کتابت می‌کنند، کلمه «دیگه» بسامد بیشتری نسبت به فارس زبان‌های اصیل دارد، همین امر در لغت‌هایی مانند «بعدشم» و «تازه‌شم» نیز صدق می‌کند.
- در شرق ایران به قابلمه معمولی نیز دیگ گفته می‌شود (در گویش معیار فارسی، دیگ بزرگ‌تر از قابلمه است)، کلمه فضول به معنای شلوغ استفاده می‌شود و ....

با یک تحقیق گسترده در بین گویشوران فارسی مناطق مختلف می‌توان به‌دقت آماره‌هایی را کشف کرد که تفکیک قابل‌توجهی در زبان مادری ایجاد کند.

با استفاده از داده‌های فوق می‌توان یک پایگاه داده قدرتمند ایجاد کرد که در آن تصاویر چهره، طرز نگارش و ساعات فعالیت در شبانه‌روز هر کاربر با برچسب نژاد وی ثبت شده باشد. با یادگیری این پایگاه داده توسط هوش مصنوعی، قادر خواهیم بود که با داشتن تنها یک تصویر یا متن، نژاد کاربر را شناسایی کنیم. چنین پایگاه داده‌ای امکان استخراج تفاوت ساعت بدن در نژادهای مختلف را نیز مهیا می‌کند.

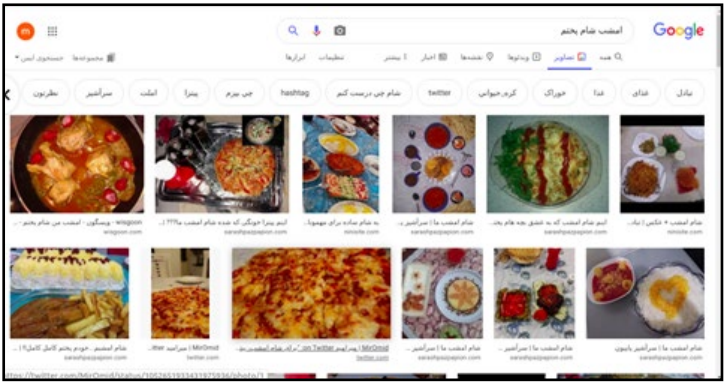
۲-۵- کشف عادات غذایی بر اساس تحلیل تصویر

اشتراک‌گذاری غذاهای روزانه یکی از علائق کاربران دنیای مجازی است. عمده محتواهای تصویری تولید شده با هدف فوق، همراه با کلیدواژه‌هایی مانند خودم‌پز، شام امشب، دستپختم و ... است[۱] که به اپراتور در جمع‌آوری داده‌ها کمک شایانی می‌کند. شبکه اجتماعی اینستاگرام یکی از بهترین بسترها برای رصد این فعالیت است ولی شبکه‌های دیگر و حتی موتورهای جستجو نیز کمک مناسبی برای جست‌وجوی این فعالیت هستند. در شبکه اجتماعی توییتر باتوجه‌به ماهیت خاص آن، آموزش‌های آشپزی و مشابه آن طرف‌دار چندانی ندارد و جستجو در این سرویس‌دهنده به نتایج قابل‌تعمیمی نمی‌رسد. دقت داشته باشید اینستاگرام و تلگرام نیازمند تحلیل بیشتری هستند و باید پیش از هر تحلیلی داده‌های آموزشی، غیرواقعی و هدفمند (مانند چشم‌وهم‌چشمی) از تحلیل‌ها کنار گذاشته شوند.

در موضوع این بخش، نتایج جستجوهای مختلف سرویس‌دهنده‌های مختلف، به نتایج محدودی منجر می‌شود و اپراتور هوشمند با چالش تشخیص دایره کلیدواژگان مواجه خواهد بود. همچنین تخصص‌های وب‌گردی در جمع‌آوری چنین پایگاه داده‌ای (به‌خصوص در تمایز دادن بین آموزش آشپزی و آشپزی در خانه) اهمیت قابل‌توجهی خواهد داشت. به هر حال، اطلاعات گسترده موجود از وعده‌های غذایی مورد مصرف ایرانیان می‌تواند اطلاعات زیادی را در مورد وضعیت سلامت، کمبود ویتامین‌ها و مواد معدنی ایرانیان به دست دهد. عکس‌های (۱۷) و (۱۸) نمایی از اطلاعات موجود و دسترس‌پذیر از غذاهای مورد مصرف ایرانیان را نشان می‌دهد.

۱. شناخت کلیدواژه‌های عمومی یک موضوع، نیازمند شناخت از کنش‌های اجتماعی در فضای سایبری است و در فعالیت اوسینتی این کلیدواژه‌ها نقش مهمی را بازی می‌کنند.

تصویر (۱۷) تصویر غذا به همراه توضیحاتی از آن در شبکه اجتماعی توییتر



تصویر (۱۸) جستجوی کلیدواژه‌های مرتبط با اشتراک‌گذاری غذا

جمع بندی

جمع بندی

علـم اوسـینت، علـم جمـع‌آوری اطلاعـات اسـت، ازایـن‌رو پروژه‌هـا و عملیـات اوسـینتی از جنـس عملیات‌هـای اطلاعاتـی و ضداطلاعاتـی طبقه‌بنـدی می‌شـود و وقـوع ایـن عملیات‌هـا در پـس پـرده و خامـوش اسـت. ایـن سـکوت، عملیات‌هـای اوسـینتی را به‌خوبـی توجیـه می‌کنـد، بـدون آنکـه نیـاز بـه سرشـماری یـا فراخـوان باشـد اطلاعـات قابل‌توجهـی از جامعـه اسـتخراج می‌شـود کـه در زمـان و هزینه‌هـای صرفه‌جویـی بـه ارمغـان مـی‌آورد و هـم اینکـه تبعاتـی از جنـس حساسـیت اجتماعـی در آن دیـده نمی‌شـود. البتـه ایـن عـدم حساسـیت تـا زمانـی اسـت کـه عملیات‌هـای اوسـینتی محرمانـه و سـری باقـی بماننـد.

ویژگی‌هـای فـوق نهادهـای مدیریتـی و امنیتـی را بـه اسـتفاده از اوسـینت ترغیـب می‌کنـد، پزشـکان، جامعه‌شناسـان، نهادهـا و.. بـا کاهـش هزینه‌هـا می‌تواننـد خدمـات بهتـری ارائـه کننـد یـا محبوبیـت خـود را بسـنجند؛ امنیتی‌هـا نیـز می‌تواننـد اتبـاع خـود یـا دشـمن را زیـر نظـر بگیرنـد، اینجاسـت کـه حساسـیت‌ها بیشـتر می‌شـود. تعارضـات بـا حقـوق بین‌الملـل، تجـاوز در حریـم کشـورها، دخالـت در کشـورها و تهدیدهـا علیـه امنیـت ملت‌هـا بـه معنـای عـام (پزشـکی، فرهنگـی، پلیسـی و...) شـکل

می‌گیرد. به‌این‌ترتیب عملیات‌های اوسینتی در بالاترین سطوح امنیتی و حفاظتی محافظت می‌شوند و اطلاعات آشکار چندانی از آنها نیست و هر چه هست حدس و گمان‌هایی است که جامعه علمی بیان می‌کنند.

باتوجه‌به موارد فوق پیشنهادهای راهبردی زیر در زمینه اوسینت قابل طرح هستند.

۱) روشن است که اوسینت منبعی مهم و کارآمد برای کسب اطلاعات حیاتی و ارزشمند است که می‌توانند برای مقاصد مفید یا مضر مورداستفاده قرار گیرند. هم‌اکنون چهارچوب حقوقی روشنی برای بررسی امکان و محدودیت‌های استفاده از اوسینت وجود ندارد و این امر می‌تواند در میان‌مدت موجب آشفتگی و سوءاستفاده شود. برای مثال این موضوع که تا چه اندازه می‌توان به اطلاعات استخراج‌شده از اوسینت در دادگاه‌ها اتکا کرد، مسئله‌ای باز است که متفکران هم‌اکنون در حال پرداختن به آن هستند (سمپسون ۲۰۱۷، صص. ۲۹۵-۳۰۴؛ بازل ۲۰۲۱، صص. ۶۳۹-۶۴۶). همچنین این سؤال که آیا اطلاعات به‌دست‌آمده از روش‌شناسی اوسینت نیز عمومی هستند یا می‌بایست محرمانه باشند نیازمند بررسی‌های دقیق حقوقی است (ویلیامز و بلوم ۲۰۱۸، ص. ۴۱). به این موارد می‌توان لزوم بررسی ابعاد حقوقی و سیاست‌گذاری مناسب برای جنبه‌های تجاری اوسینت را نیز اضافه کرد. ازاین‌رو انجام پژوهش‌های دقیق متناظر با اقتضائات جمهوری اسلامی ایران در این حوزه ضروری به نظر می‌رسد.

۲) اوسینت حریم خصوصی را دچار چالش جدی می‌کند. چراکه

اگرچه منابع اطلاعاتی اوسینت، باز هستند، بااین‌وجود تحلیل‌های پیشرفته مبتنی بر کلان‌داده و هوش مصنوعی نتایجی را برملا می‌کند که شاید افراد به‌هیچ‌وجه راضی به استفاده از آن‌ها نباشند. ازاین‌رو سؤالات اخلاقی منحصربه‌فردی در مورد حریم خصوصی و خدشه‌های احتمالی اوسینت به آن به وجود می‌آید (بازل ۲۰۲۱، صص ۶۴۷-۶۵۳؛ حسن و حجازی ۲۰۱۸، صص. ۱۷-۱۸) که لازم است توسط پژوهشگران فقه و اخلاق اسلامی مورد مداقه قرار گیرد. در ضمن هم‌اکنون روش‌هایی برای ارتقاء حریم خصوصی در فضای اوسینت پیشنهاد شده است (لیتون و واترز ۲۰۱۶، صص. ۶۱-۷۸) که بررسی و بومی‌سازی آن‌ها لازم است.

۳) اگرچه در این گزارش تمرکز بر آسیب‌ها و تهدیدهای احتمالی ناشی از اوسینت بود، بایستی خاطرنشان کرد که فرصت‌های زیادی نیز در استفاده صحیح از اوسینت وجود دارد. به بیان دقیق‌تر اوسینت می‌تواند به کشف فعالیت‌های غیرقانونی در بستر اینترنت کمک شایانی کند (واداز و دیگران ۲۰۱۷؛ چارالامبوس و دیگران ۲۰۱۷). برای مثال از اوسینت برای کشف فروش داروهای غیرقانونی (فرانک و میخایلوف ۲۰۲۰)، آزار و اذیت کودکان (چارالامبوث و دیگران ۲۰۱۷) و کارتل‌های غیرقانونی (واداز و دیگران ۲۰۱۷) استفاده شده است. شکی نیست که استفاده صحیح از اوسینت نیازمند آشنایی کامل با روش‌شناسی و کاربست‌های احتمالی آن است و ازاین‌رو پژوهش روی ابعاد مختلف این فناوری می‌تواند کمک شایانی به مقابله با تهدیدهای احتمالی و استفاده از فرصت‌های ممکن کند. درهرحال همان‌طور که متفکران زیادی خاطرنشان کرده‌اند (استانیفورث

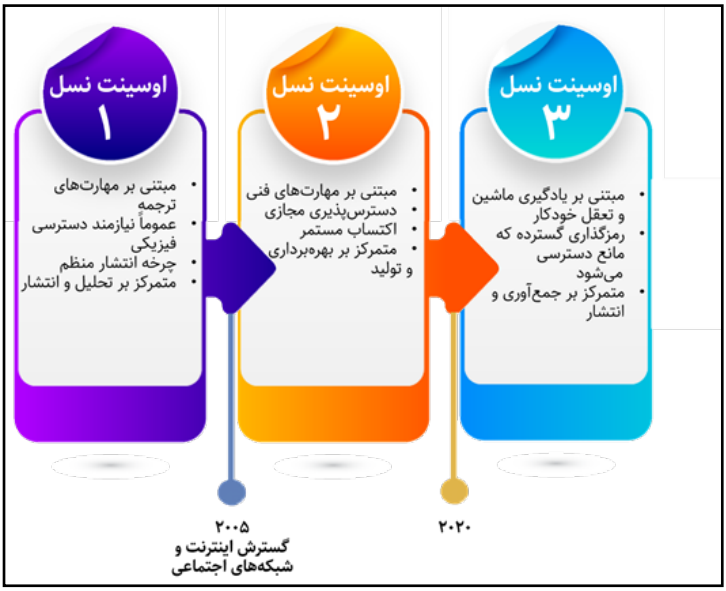
۲۰۱۷: مارزل ۲۰۱۷)، اوسینت از هر دو جنبه تهدید و فرصت ارتباط تنگاتنگی با امنیت ملی برقرار می‌کند و ازاین‌رو شایسته توجه مضاعف است.

۴) مثال‌های مورداستفاده در این گزارش منحصر به مواردی بود که اطلاعات به‌صورت عمومی قابل‌دسترس بودند. بااین‌وجود، مهم‌ترین کاربردهای اوسینت مربوط به مواردی است که اطلاعات محرمانه و طبقه‌بندی شده در کنار اطلاعات به‌دست‌آمده از روش اوسینت قرار می‌گیرند. در این جاست که ممکن است خطرناک‌ترین نتایج به دست آید. ازاین‌رو در بررسی تهدیدهای اوسینت، بایستی امکان ترکیب روش‌های مختلف و همچنین اطلاعات اوسینتی و غیراوسینتی را در نظر داشته باشیم (دی و همکاران ۲۰۱۷).

۵) هم‌اکنون محققان از نسل سوم اوسینت صحبت به عمل می‌آورند. اوسینت نسل دوم که این گزارش حول آن می‌چرخید، مبتنی بر فناوری وب ۲ بود که در صفحات وب پویا و محتوای تولیدشده توسط کاربران ظهور پیدا کردند. بااین‌وجود محققین هم‌اکنون از وب ۳ یا وب معناشناختی[1] صحبت به عمل می‌آورند که در آن پردازش اطلاعات ماشینی و یادگیری ماشین و تعقل خودکار[2] محوریت پیدا می‌کند. آیا با ظهور وب ۳، روش‌شناسی اوسینت نیز دچار یک تحول بنیادین خواهد شد؟ برای مثال در سال ۲۰۱۹ هر دقیقه ۵۰۰ ساعت ویدئو توسط افراد در سایت یوتیوب دانلود شده است. این‌که چه حجمی از اطلاعات در این ویدئوها مستتر است و روش‌شناسی اوسینت می‌تواند چه تحلیل‌های حیرت‌انگیزی از آن‌ها داشته باشد، نیاز به تخیل زیادی ندارد. بااین‌وجود این امر

1. Semantic Web
2. Automated Reasoning

نیازمند استفاده‌های پیشرفته‌تر از هوش مصنوعی و یادگیری عمیق ماشین است که از ویژگی‌های وب ۳ هستند. جهت جلوگیری از عقب ماندن و غافل‌گیری احتمالی لازم است که با رویکرد آینده‌پژوهی، پژوهش‌هایی در مورد اوسینت ۳ و اقتضائات آن انجام پذیرد.



شکل (۳) سه نسل اوسینت

منابع

[1] Akhgar, B. (2017). OSINT as an Integral Part of the National Security Apparatus. In B. Akhgar, P. S. Bayerl, & F, Sampson, (eds.). Open Source Intelligence Investigation: From Strategy to Implementation (pp. 3-10). Springer.

[2] Arzipe, J., et al. (2016). Differences in Looking at Own- and Other-Race Faces Are Subtle and Analysis-Dependent: An Account of Discrepant Reports. PLOS ONE. https://doi.org/10.1371/journal.pone.0148253s

[3] Bazzell, M. (2021). Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information: Eighth Edition. CreateSpace Independent Publishing Platform.

[4] Charalambous, E., et al. (2017). Combatting Cybercrime and Sexual Exploitation of Children: An Open Source Toolkit. In B. Akhgar, P. S. Bayerl, & F, Sampson, (eds.). Open Source Intelligence Investigation: From Strategy to Implementation (pp. 233-250). Springer.

[5] Day, T., Gibson, H., & Ramwell, S. (2017). Fusion of OSINT and Non-OSINT Data. In B. Akhgar, P. S. Bayerl, & F, Sampson, (eds.). Open Source Intelligence Investigation: From Strategy to Implementation (pp. 133-152). Springer.

[6] Eldridge, C., Hobbs, C. & Moran, M. (2017). Fusing algorithms and analysts: open-source intelligence in the age of 'Big Data'. Intelligence and National Security, https://doi.org/10.1080/02684527.2017.1406677

[7] Evagelista, J. R. G., et al. (2020). Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence. Journal of Applied Security Research. https://doi.org/10.1080/19361610.2020.1761737

[8] Fleming, N. (2007). Fingerprints can reveal race and sex. The Telegraph.

https://www.telegraph.co.uk/news/uknews/1559302/Finger prints-can-reveal-race-and-sex.html

[9] Frank, R. & Mikhaylov, A. (2020). Beyond the 'Silk Road': Assessing Illicit Drug Marketplaces on the Public Web. In M. A. Tayebi, U. Glaesser, & D. B. Skillicorn (eds.) Open Source Intelligence and Cyber Crime (pp. 89-112). Springer.

[10] Hassan, N. H., & Hijazi, R. (2018). Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence. Apress.

[11] Hern, A. (2014). Hacker fakes German minister's fingerprints using photos of her hands. The Guardian. https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

[12] Hudson, J., Ryan, M., & Dawsey, J. (2020). On the day U.S. forces killed Soleimani, they targeted a senior Iranian official in Yemen. The Washington Post. https://www.washingtonpost.com/world/national-security/on-the-day-us-forces-killed-soleimani-they-launched-another-secret-operation-targeting-a-senior-iranian-official-in-yeen/2020/01/10/60f86d-bc-3245-11ea-898f-eb846b7e9feb_story.html

[13] Lyle, A. (2017). Legal Considerations for Using Open Sourc Intelligence in the Context of Cybercrime and Cyberterrorism. In B. Akhgar, P. S. Bayerl, & F, Sampson, (eds.). Open Source Intelligence Investigation: From Strategy to Implementation (pp. 277-294). Springer.

[14] Marzell, L. (2017). OSINT as Part of the Strategic National Security Landscape. In B. Akhgar, P. S. Bayerl, & F, Sampson, (eds.). Open Source Intelligence Investigation: From Strategy to Implementation (pp. 33-56). Springer.

[15] Pastor-Galindo, J. et al. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. IEEE Access, 8: 10282-10304.

[16] Sampson, F. (2017). Following the Breadcumbs: Using Open Source Intelligence as Evidence in Criminal Proceedings. In B. Akhgar, P. S. Bayerl, & F, Sampson, (eds.). Open Source Intelligence Investigation: From Strategy to Implementation (pp. 295-304). Springer.

[17] Staniforth, A. (2017). Open Source Intelligence and the Protection of National Security. In B. Akhgar, P. S. Bayerl, & F, Sampson, (eds.). Open Source Intelligence Investigation: From Strategy to Implementation (pp. 11-20). Springer.

[18] Steele, R. D. (2007). Open Source Intelligence. In L. K. Johnson (ed.). Handbook of Intelligence Studies (pp. 129-147). London: Routledge.

[19] Miller, B. H. (2018). Open Source Intelligence (OSINT): An Oxymoron? International Journal of Intelligence and Counterintelligence, 31(4): 702-719

[20] Williams, H. J., & Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. RAND Corporation.

[21] Layton, R., & Walters, P. A., (2015). Automating Open Source Intelligence: Algorithms for OSINT. Elsevier Science.

[22] Vadász, P. et al. (2017). Identifying Illegal Cartel Activities from Open Sources. In B. Akhgar, P. S. Bayerl, & F, Sampson, (eds.). Open Source Intelligence Investigation: From Strategy to Implementation (pp. 251-273). Springer.

csri.majazi.ir

حوزه فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانه پر از آب و خروشان است که می آید و دائماً هم بر آب آن افزوده و خروشان تر می شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه‌کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می‌شود فرصت. اگر رهایش کنیم و برنامه‌ای برای آن نداشته باشیم می‌شود یک تهدید.

csri.majazi.ir