فصلنامهٔ امنیت پژوهی (علمی-پژوهشی)
سال بیست و چهارم: شماره ۹۰ - تابستان ۱۴۰۴
صص: ۲۹ تا ۴۶
Amniat Pajouhi: Security Research Quarterly
Vol.24, No.90,Summer 2025
P-P: 29 - 46
تاریخ دریافت: ۱۴۰۴/۰۶/۰۵ تاریخ پذیرش: ۱۴۰۴/۰۸/۱۵

آناتومی خیانت: انگیزه‌ها و آسیب‌پذیری‌ها در عصر جاسوسی دیجیتال

مصطفی ساوه درودی[۱]
رضا خدادادی[۲]

چکیده

پژوهش حاضر با عنوان «آناتومی خیانت» به تحلیل تحول الگوهای جذب نیرو در فعالیت‌های جاسوسی می‌پردازد؛ تحولی بنیادین که از «شکار هدفمند» و جذب سازمان‌محور در دوران کلاسیک به «همکاری داوطلبانه» و خودمعرفی در عصر دیجیتال منتهی شده است. تحلیل داده‌های مرکز امنیت کارکنانی وزارت دفاع آمریکا نشان می‌دهد که از سال ۱۹۹۰ به بعد، بیش از ۶۰ درصد جاسوسان آمریکایی داوطلبانه وارد همکاری شده‌اند. تطبیق این داده‌ها با یافته‌های سرویس‌های اطلاعاتی غربی و بررسی پرونده «محمدهادی صالح» در لبنان نشان می‌دهد که فشارهای روانی و شکست‌های فردی، نارضایتی اقتصادی، فرصت‌های سایبری و پوشش ایدئولوژیک به‌صورت هم‌زمان نقش تعیین‌کننده در خیانت‌های نوین دارند.

تحلیل نتایج بر چهار کاتالیست اصلی آسیب‌پذیری دلالت دارد: (۱) فردی ـ روان‌شناختی، شامل تحقیر و تخریب عزت‌نفس؛ (۲) اقتصادی ـ انگیزشی، شامل فشار مالی و ادراک بی‌عدالتی؛ (۳) سایبری ـ دیجیتال، شامل شکار دیجیتال و مهندسی اجتماعی در شبکه‌های اجتماعی؛ و (۴) ساختاری ـ سازمانی، شامل ضعف آموزش ضدجاسوسی، پایش هوشمند و حمایت درون‌سازمانی. مدل روان‌شناختی شارنی (۲۰۱۴) نشان می‌دهد که خیانت عموماً با «شکست غیرقابل‌تحمل» آغازشده و فرد را در یک مسیر ده‌مرحله‌ای جاسوسی قرارمی‌دهد. یافته‌های علوم اعصاب شناختی (de Quervain و همکاران، ۲۰۰۴) نیز تأیید می‌کند که کنش انتقام از طریق فعال‌سازی مدار پاداش مغز، انگیزه برای همکاری خصمانه را تقویت و تثبیت می‌کند.

---

۱. عضو هیئت‌علمی دانشگاه علوم و فنون فارابی (نویسنده مسئول) mo_doroudi@yahoo.com
۲. دانشجوی کارشناسی ارشد رشته علوم شناختی دانشگاه علوم و فنون فارابی

پژوهش نتیجه می‌گیرد که مقابله با خیانت و جاسوسی در عصر دیجیتال تنها با اتخاذ رویکردی ترکیبی امکان‌پذیر است: ضدجاسوسی پدافندی (پایش هوشمند، مداخله‌های روان‌شناختی، عدالت سازمانی و آموزش دیجیتال‌محور) و ضدجاسوسی آفندی (فریب عملیاتی، ره‌گیری سایبری، مهندسی اجتماعی معکوس و ایجاد بی‌اعتمادی در سامانه جذب دشمن). درنهایت، خیانت دیگر پدیده‌ای استثنایی نیست بلکه تهدیدی پایدار و ساختاری است؛ امنیت زمانی محقق می‌شود که عمل جاسوسی برای عامل انسانی و برای سازمان جذب‌کننده به رفتاری پرهزینه، پرخطر و کم‌ثمر بدل گردد.

واژگان کلیدی: جاسوسی؛ جذب داوطلبانه؛ مدل MICE؛ فضای سایبری؛ ضدجاسوسی.

مقدمه

جاسوسی همواره از پیچیده‌ترین عرصه‌های رقابت میان دولت‌ها و بازیگران غیردولتی بوده است. اگرچه تاریخ آن به هزاران سال پیش بازمی‌گردد، اما گسترش فضای دیجیتال قواعد این بازی را به‌طور بنیادین تغییر داده است. امروز جذب عوامل انسانی تنها در میدان‌های سنتی رخ نمی‌دهد؛ شبکه‌های اجتماعی، پیام‌رسان‌های رمزگذاری‌شده و پلتفرم‌های آنلاین بستری تازه برای شناسایی و هدایت افراد فراهم کرده‌اند و فرایند «خیانت» را آسان‌تر و پیچیده‌تر ساخته است. با این حال، بسیاری از سازمان‌ها هنوز بر چارچوب‌های سنتی مقابله با جاسوسی متکی هستند و به تعامل پیچیدهٔ انگیزه‌های فردی، فشارهای روانی و آسیب‌پذیری‌های دیجیتال و سازمانی توجه کافی ندارند. این کاستی باعث می‌شود خیانت در عصر دیجیتال سریع‌تر، پنهان‌تر و پیش‌بینی‌ناپذیر باشد. مسئله اصلی پژوهش آن است که چگونه انگیزه‌ها و آسیب‌پذیری‌های فردی و سازمانی در بستر دیجیتال باهم تعامل می‌کنند و چه راهبردهایی می‌توان برای پیشگیری و بازدارندگی تدوین کرد تا امنیت پایدار در محیط‌های پرچالش حفظ شود

در این میان، پدیدهٔ خیانت به‌عنوان نقطهٔ تلاقی آسیب‌پذیری فردی و بهره‌برداری سازمانی، اهمیتی ویژه یافته است. آمارهای وزارت دفاع آمریکا نشان می‌دهد که از دههٔ ۱۹۹۰ به این‌سو، بیش از ۶۰ درصد جاسوسان آمریکایی به‌صورت داوطلبانه و خودمعرف به همکاری با دشمن پرداخته‌اند؛ واقعیتی که بیانگر تغییر بنیادی در الگوی انگیزش است.

انگیزه‌های روانی، فشارهای مالی، نارضایتی‌های شغلی و حتی بحران‌های هویتی اکنون نقشی پررنگ‌تر از تهدید و اجبار کلاسیک ایفا می‌کنند. نمونه‌های اخیر در خاورمیانه - ازجمله پروندهٔ «محمدهادی صالح» در لبنان یا رخدادهای مرتبط با جنگ‌های ایران و اسرائیل - نشان می‌دهند که این پدیده تنها محدود به غرب نیست و در محیط‌های پرتنش منطقه‌ای نیز با شدتی بیشتر جریان دارد. العربیه (۲۰۲۵).

اهمیت و ضرورت پژوهش در اینجاست: در شرایطی که خیانت می‌تواند امنیت ملی را در حساس‌ترین سطوح به خطر اندازد، همچنان بخش بزرگی از ادبیات علمی بر چارچوب‌های سنتی مانند مدل MICE[1] متمرکز مانده است. کمتر پژوهشی به‌طور تلفیقی به پیوند انگیزه‌های فردی و روان‌شناختی با بسترهای فنّاورانه و دیجیتال پرداخته است. این شکاف تحلیلی باعث می‌شود که سیاست‌های ضدجاسوسی اغلب با نگاهی گذشته‌محور طراحی شوند و کارآمدی محدودی در مواجهه با تهدیدهای نوین داشته باشند؛ ازاین‌رو، پژوهشی که به بررسی همه‌جانبهٔ انگیزه‌ها و بسترهای جدید خیانت بپردازد، هم از نظر علمی و هم از نظر عملی ضرورتی انکارناپذیر دارد.

بر این‌اساس، مقالهٔ حاضر با هدف تحلیل چندبعدی پدیدهٔ خیانت، به‌دنبال پاسخ‌گویی به پرسش‌های کلیدی زیر است:

۱) چه عواملی افراد را در دنیای امروز به‌سمت خیانت سوق می‌دهند و سهم هر یک از انگیزه‌ها چیست؟
۲) فضای دیجیتال چگونه فرایند جذب، هدایت و پنهان‌کاری عوامل را تغییر داده است؟
۳) پیامدهای این تحولات برای امنیت ملی و سازمان‌های اطلاعاتی چیست و چه راهکارهایی برای مقابله می‌توان ارائه کرد؟

برای پاسخ به این پرسش‌ها، پژوهش حاضر با اتکا به چارچوب نظری تلفیقی - شامل مدل کلاسیک MICE و مدل روان‌شناختی شارنی - و بر پایهٔ داده‌های آماری، پرونده‌های واقعی و مطالعات موردی منطقه‌ای طراحی شده است. ساختار مقاله به‌این‌ترتیب سامان یافته است: ابتدا ادبیات نظری و پیشینهٔ پژوهش مرور می‌شود؛ سپس روش‌شناسی معرفی

۱. مدل MICE چارچوبی برای تبیین انگیزه‌های فردی در رفتارهای جاسوسی است و چهار محرک اصلی شامل پول (Money)، ایدئولوژی (Ideology)، اجبار (Coercion) و خودبزرگ‌بینی / نیاز به اعتبار شخصی (Ego) را به‌عنوان عوامل محرک خائن در نظر می‌گیرد.

خواهد شد؛ در ادامه یافته‌ها در سه محور اصلی «الگوهای جذب»، «انگیزه‌ها» و «نقش فضای دیجیتال» ارائه می‌شوند؛ و نهایتاً با تحلیل پرونده‌های واقعی، بحث و نتیجه‌گیری کلی مطرح خواهد شد.

مرور ادبیات و پیشینه پژوهش

مطالعات سه دهه اخیر نشان می‌دهد که تحولات فنّاورانه، ژئوپلیتیکی و گسترش بسترهای دیجیتال، الگوهای جذب و انگیزه‌های جاسوسان را دگرگون ساخته است. پیشینه این حوزه در سه محور اصلی قابل‌بررسی است:

۱) الگوهای جذب

تحلیل پایگاه وزارت دفاع آمریکا بر روی بیش از ۱۵۰ پرونده نشان می‌دهد که از سال ۱۹۹۰ به بعد، حدود ۶۰٪ از جاسوسان آمریکایی داوطلبانه با سرویس‌های خارجی تماس گرفته‌اند. گزارش‌های غیررسمی جدید CIA نیز این روند را تأیید کرده و سهم همکاری‌های داوطلبانه در دهه اخیر را ۵۷٪ برآورد می‌کند. همچنین داده‌های غیررسمی MI5 نشان می‌دهد که ایدئولوژی همچنان نقش پررنگی در انگیزه‌های جذب دارد. این یافته‌ها بر رشد سهم جذب داوطلبانه تحت‌تأثیر تسهیل ارتباطات آنلاین دلالت دارند. (Herbig, 2017)

۲) انگیزه‌ها و ویژگی‌های فردی

مدل MICE (پول، ایدئولوژی، اجبار/سازش، خودبزرگ‌بینی) همچنان چارچوب غالب در تحلیل انگیزه‌هاست. بر اساس داده‌های وزارت دفاع آمریکا، انگیزه‌های مالی (۲۸٪)، ایدئولوژیک (۲۲٪)، نارضایتی سازمانی (۱۴٪) و خودبزرگ‌بینی (۱۴٪) بیش‌ترین سهم را دارند.

مطالعات روان‌شناختی نیز نشان می‌دهد که عوامل شخصیتی چون خودمحوری و حس ویژه بودن می‌توانند خطر گرایش به خیانت را افزایش دهند (Charney, 2014). وی تأکید می‌کند که جرقه خیانت معمولاً از شکست شخصی و ضربه به اگو آغاز می‌شود و در قالب یک الگوی ده‌مرحله‌ای به برقراری ارتباط با بیگانگان منتهی می‌گردد. یافته‌های علوم اعصاب نیز نشان می‌دهد که رفتارهای انتقام‌جویانه با فعال‌سازی مدار پاداش در مغز همراه است و می‌تواند تداوم همکاری خصمانه را حتی در شرایط پرخطر توضیح دهد. (de Quervain, 2004)

۳) بسترهای سایبری

ظهور شبکه‌های اجتماعی، پیام‌رسان‌های رمزگذاری‌شده و رمزارزها فرصت‌های جدیدی برای جذب ایجاد کرده است. هشدار مشترک MI5 و CPNI (۲۰۲۱) در کارزار Think Before You Link نشان‌داد که بیش از ۱۰ هزار کارمند حساس در بریتانیا طی پنج سال اخیر هدف پروفایل‌های جعلی منتسب به دولت‌های خارجی قرارگرفته‌اند. نمونه‌های مشابه در خاورمیانه نیز مشاهده‌شده است؛ ازجمله پرونده محمدهادی صالح جاسوس اسرائیل در لبنان که نخستین تماس او با عوامل بیگانه از طریق تعاملات مجازی شکل گرفت و پرداخت پاداش‌های وی نیز بخشی به‌صورت رمزارز انجام شد.

۴) شکاف‌های پژوهشی

با وجود پیشرفت‌های یادشده، سه شکاف اساسی وجود دارد:

۱. کمبود پژوهش‌های تلفیقی که داده‌های روان‌شناختی، امنیتی و سایبری را هم‌زمان تحلیل کنند.
۲. نبود مدل‌های به‌روز برای پایش خطر دیجیتال در کارکنان حساس.
۳. فقدان بررسی جامع پیوند میان اختلالات شخصیتی و بسترهای شکار دیجیتال در مناطق پرتنش.

این شکاف‌ها ضرورت پژوهش حاضر را برای ارائه یک مدل تلفیقی ارزیابی خطر و پیشگیری از نفوذ انسانی- سایبری برجسته می‌سازد.

روش‌شناسی پژوهش

این پژوهش از رویکرد تطبیقی- تحلیلی برای بررسی الگوهای انگیزشی و آسیب‌پذیری‌های امنیتی در عصر جاسوسی دیجیتال استفاده می‌کند. داده‌ها و شواهد از چهار منبع اصلی گردآوری‌شده‌اند:

منابع داده‌ها

۱. پایگاه‌های داده رسمی و گزارش‌های امنیتی

- داده‌های کمی پایگاه PERSEREC وزارت دفاع آمریکا (۱۹۹۰-۲۰۱۵) شامل بیش از ۱۵۰ پرونده جاسوسی ثبت‌شده (Herbig, 2017).

- گزارش‌ها و هشدارهای رسمی و غیررسمی سازمان اطلاعات مرکزی آمریکا (CIA) و کارزار Think Before You Link از MI5/CPNI (MI5/CPNI, 2021).

۲. مطالعات میدانی و روان‌شناختی

- یافته‌های پژوهش Slammer و تحلیل‌های Charney (۲۰۱۴) درباره ویژگی‌های شخصیتی و انگیزه‌های عوامل انسانی در عملیات جاسوسی.
- پژوهش علوم اعصاب de Quervain et al. (۲۰۰۴) که مدار پاداش مغز را در رفتارهای انتقام‌جویانه بررسی کرده است.

۳. مطالعات موردی

- بررسی پرونده محمدهادی صالح بر اساس گزارش‌های خبرگزاری‌های العربیه و الشرق، به‌عنوان نمونه‌ای از جذب دیجیتال در خاورمیانه که نخستین تماس او با عوامل بیگانه از طریق تعاملات مجازی شکل گرفت و پرداخت‌ها بخشی به‌صورت رمزارز انجام شد.
- تحلیل جنگ ۱۲ روزه ایران و اسرائیل به‌عنوان یک بستر ژئوپلیتیکی خاص، با تمرکز بر پیوند میان نارضایتی‌های فردی، مشکلات اقتصادی و بهره‌برداری سرویس‌های خارجی از فضای درگیری.

۴. منابع رسانه‌ای و تحلیلی منطقه‌ای

- گزارش‌ها و تحلیل‌های معتبر برای بازسازی جزئیات زمینه‌ای و محیطی پرونده‌ها و عملیات‌ها.

واحد تحلیل

واحد تحلیل در این پژوهش، فرد جاسوس یا عامل نفوذی است که در یکی از دودسته زیر قرارمی‌گیرد:

- عوامل داوطلب: افرادی که خود به سرویس‌های خارجی مراجعه کرده‌اند.
- عوامل هدفمند: افرادی که از طریق عملیات جذب شناسایی و به همکاری واداشته شده‌اند.

روش گردآوری داده‌ها

- استفاده از داده‌های ثانویه شامل گزارش‌های رسمی، مقالات علمی و گزارش‌های میدانی.

- جمع‌آوری داده‌های کیفی از منابع رسانه‌ای معتبر برای تکمیل جزئیات پرونده‌ها.
- کدگذاری داده‌ها بر اساس چهار مؤلفه مدل MICE (پول، ایدئولوژی، اجبار/سازش، خودبزرگ‌بینی) برای تحلیل انگیزه‌ها و شناسایی الگوهای رفتاری.

روش تحلیل داده‌ها

- تحلیل آماری توصیفی برای سنجش فراوانی نسبی انگیزه‌ها در داده‌های کمی PERSEREC وCIA .
- تحلیل محتوایی برای استخراج الگوهای روان‌شناختی، نحوه تعامل آنلاین و پیامدهای انگیزشی در مطالعات موردی.
- مقایسه تطبیقی بین پرونده‌های خاورمیانه (مانند محمدهادی صالح و جنگ ۱۲ روزه) و نمونه‌های غربی برای بررسی تفاوت‌های فرهنگی و محیطی در جذب نیرو و بهره‌برداری سرویس‌های اطلاعاتی.
- تلفیق یافته‌های کمی و کیفی برای شناسایی الگوهای چندبعدی انگیزشی و آسیب‌پذیری‌های سازمانی و ارائه چارچوب تحلیلی جامع در عصر جاسوسی دیجیتال.

یافته‌های تحقیق

۱) الگوهای جذب

جاسوسی در سه دهه اخیر تحولات بنیادین یافته است. تحلیل داده‌های وزارت دفاع آمریکا نشان می‌دهد که حدود ۵۹ تا ۶۰ درصد از جاسوسانی که پس از سال ۱۹۹۰ فعالیت داشته‌اند، داوطلبانه ارتباط خود را با سرویس‌های خارجی آغاز کرده‌اند، درحالی‌که سایرین از طریق فرایندهای هدفمند شناسایی و جذب شده‌اند (Herbig, 2008). این روند بیانگر نقش تعیین‌کننده ابتکار فردی و انگیزه‌های درونی در آغاز همکاری با بیگانه است.

مطالعات PERSEREC و گزارش‌های CIA و MI5 نشان می‌دهند که محرک‌های اصلی عبارتند از:

- انگیزه مالی و منافع مادی؛
- وفاداری‌های دوگانه یا ایدئولوژیک (قومیتی، ملی یا سیاسی).

به‌ویژه عامل مالی در دهه‌های اخیر برجسته شده و در بسیاری از پرونده‌ها نقش کلیدی در تصمیم به خیانت ایفا کرده است. یافته‌های غیررسمی سرویس‌های غربی نیز نشان می‌دهند که تقریباً ۵۷٪ همکاری‌ها داوطلبانه بوده و حدود ۴۷٪ عوامل جذب‌شده گرایش‌های ایدئولوژیک داشته‌اند. این یافته‌ها نشان می‌دهند که روندهای جذب در عصر معاصر، ترکیبی از انگیزه‌های درونی و فرصت‌های محیطی است و تحلیل آن نیازمند تلفیق داده‌های تاریخی، روان‌شناختی و محیطی است.

نمونه‌های منطقه‌ای، مانند پرونده محمدهادی صالح و جنگ ۱۲ روزه ایران و اسرائیل، نشان می‌دهند که فشارهای مالی، ناامنی روانی و فرصت‌های دیجیتال می‌توانند حتی افراد با سابقه وفاداری خانوادگی و مذهبی را به مسیر خیانت سوق دهند (Shafaqna, 2025; Guardian, 2025). این شواهد تأکید می‌کنند که فرایند جذب در عصر دیجیتال چندعاملی و پیچیده است.

۲) انگیزه‌ها و مدل‌های تبیینی خیانت

تحلیل انگیزه‌های خیانت نشان می‌دهد که محرک‌ها از چارچوب‌های ساده به مدل‌های پیچیده و چندعاملی حرکت کرده‌اند. این روند را می‌توان در سه سطح مدل‌سازی بررسی کرد: مدل کلاسیکMICE ، مدل روان‌شناختی Slammer و مدل معاصر/ترکیبی یافته‌های CIA و MI5.

الف) مدل کلاسیکMICE

مدل MICE که در دهه ۱۹۶۰ توسط نهادهای امنیتی ایالات‌متحده توسعه یافت، چهار محرک اصلی را برای خیانت معرفی می‌کند:

۱. Money (پول/انگیزه مالی): رایج‌ترین عامل خیانت است. نمونه: آلدرریچ ایمز (CIA) اطلاعات طبقه‌بندی‌شده را به شوروی فروخت و بیش از ۲٫۷ میلیون دلار دریافت کرد.

۲. Ideology (ایدئولوژی/باور سیاسی): وفاداری سیاسی یا اعتقادی می‌تواند بر وفاداری سازمانی غلبه کند. نمونه: جولیوس و اثل روزنبرگ.

۳. Compromise(اجبار/باج‌گیری): تهدید افشای نقاط ضعف شخصی باعث جذب یا نگه‌داری جاسوسان می‌شود.

٤. Ego(خود/خودبزرگ‌بینی): نیاز به دیده‌شدن و اثبات توانایی‌ها یا جبران نادیده‌گرفته‌شدن.

اگرچه مدل MICE کارکرد آموزشی مهمی دارد، تجربه‌های بعدی نشان‌داده‌اند که این چارچوب برای توضیح تمام انگیزه‌ها کافی نیست و انگیزه‌ها غالباً ترکیبی و پیچیده هستند.

ب) یافته‌های پروژهSlammer

مطالعات پروژه Slammer (۱۹۸۵-۱۹۹۰) نشان‌داد که خیانت اغلب ریشه در محرک‌های روان‌شناختی و شخصیتی پیچیده دارد و صرفاً محدود به انگیزه مالی یا ایدئولوژیک نیست. مؤلفه‌های پرتکرار شامل:

- خودویژه‌پنداری و دست‌کاری‌گری؛
- بحران‌های شخصی حل‌نشده؛
- الگوهای شخصیتی آسیب‌زا (خودشیفتگی، پارانویا، ضداجتماعی).

این یافته‌ها اهمیت تحلیل چندعاملی و بینش رفتاری در پیش‌بینی و مدیریت تهدیدات داخلی را برجسته می‌کنند.

پ) یافته‌های غیررسمی سرویس‌های غربی (MI5وCIA)

با گسترش فضای دیجیتال، فرایند جذب کوتاه‌تر شده و فاصله «نارضایتی» تا تماس اولیه گاهی تنها چند کلیک است. محرک‌های Ego در عصر دیجیتال پررنگ‌تر شده‌اند، زیرا توجه و دیده‌شدن به یک سرمایه اجتماعی حیاتی بدل شده است. این یافته‌ها نشان می‌دهند که انگیزه‌ها در عصر دیجیتال به‌صورت ترکیبی عمل می‌کنند و دیگر نمی‌توان خیانت را تنها ناشی از پول یا ایدئولوژی دانست.

۳) سازوکار روان‌شناختی و ویژگی‌های فردی

الف) مدل شارنی:

دیوید شارنی، روان‌پزشک آمریکایی، با مصاحبه‌های طولانی با جاسوسان محکوم‌شده، مدلی برای فرایند خیانت ارائه داد که نشان می‌دهد عامل محوری، آسیب

ب اَنا و تحقیر درونی است. فرایند خیانت در قالب یک زنجیره روان‌شناختی رخ می‌دهد:

۱. بی‌عدالتی ادراک‌شده: فرد احساس نادیده‌گرفته‌شدن دارد.
۲. ضربه به اَنا: تحقیر داخلی، تابوی خیانت را تضعیف می‌کند.
۳. تبدیل تابو به گزینه ممکن: خیانت از «غیرقابل‌تصور» به «راه‌حل احتمالی» تبدیل می‌شود.
۴. پیوند با فشارهای بیرونی: نیاز مالی یا تهدید خارجی فاصله تصمیم تا عمل را کاهش می‌دهد.
۵. عادی‌سازی و حلقه پاداش عصبی: تجربه انتقام یا تأثیرگذاری پنهانی رفتار خیانت را تثبیت می‌کند.

این مدل نشان می‌دهد که خیانت محصول تعامل ویژگی‌های فردی آسیب‌پذیر، فشارهای محیطی و فرصت‌های دیجیتال است، نه صرفاً انگیزه مالی یا ایدئولوژیک.

۴) بستر سایبری و شکار دیجیتال

فضای دیجیتال، سه مانع کلاسیک جذب را کاهش داده است:

- هزینه تماس نزدیک به صفر: پیام‌رسان‌ها و شبکه‌های حرفه‌ای امکان ارتباط گسترده بدون خطر را فراهم می‌کنند.
- خطر شناسایی پایین: هویت جعلی و برندینگ صوری شناسایی را دشوار می‌کند.

سختی راستی‌آزمایی و ردیابی: پروفایل‌های جعلی و پرداخت‌های رمزارزی عملیات پنهان را تسهیل می‌کنند.

نمونه‌ها شامل پرونده Kevin Mallory (۲۰۱۸) و کمپین‌های LinkedIn سرویس‌های غربی و آلمانی هستند (FBIIC, 2022; BfV Annual Report, 2020). محیط دیجیتال فاصله تصمیم تا تماس را کوتاه و نرخ موفقیت شکار دیجیتال را چند برابر کرده است.

۵) مطالعه موردی و زمینه‌های بحرانی

الف) پرونده محمدهادی صالح (لبنان):

محمدهادی صالح، مداح نزدیک به حزب‌الله، در سال ۲۰۲۵ به اتهام جاسوسی برای موساد بازداشت شد (Shafaqna, 2025; Khabarfoori, 2025; IUSNews, 2025). او

حدود ۲۳ هزار دلار دریافت کرده و اطلاعات حساس را در اختیار دشمن قرار داده بود. ابزار اصلی ارتباط او پیام‌رسان‌های دیجیتال بود (Al-Modon, 2025). پرونده او نشان می‌دهد که ترکیب فشار مالی، نیاز روانی و فرصت‌های دیجیتال می‌تواند حتی افراد وفادار به ارزش‌های خانوادگی و مذهبی را به خیانت سوق دهد و با مدل‌های MICE و Slammer همخوانی دارد.

ب) زمینه بحرانی: جنگ ۱۲ روزه ایران-اسرائیل (ژوئن ۲۰۲۵)

این جنگ فضایی از فشار اقتصادی، ناامنی روانی و قطبی سازی سیاسی-ایدئولوژیک ایجاد کرد که بستر مناسبی برای جذب دیجیتال بود. سرویس‌های اسرائیلی از پروفایل‌های جعلی و وعده‌های کوچک اما هدفمند برای جذب افراد مستعد استفاده کردند (Wikipedia, 2025; Guardian, 2025). انگیزه‌ها طیف گسترده‌ای از محرک‌های مالی، نارضایتی اجتماعی-سیاسی و پوشش ایدئولوژیک را شامل می‌شد. این نمونه نشان می‌دهد که فضای دیجیتال و بحران‌های ژئوپلیتیکی روند خیانت را تسریع و پیچیده می‌کنند.

بحث و تحلیل

الف) تحلیل و تفسیر یافته‌ها

نتایج این پژوهش آشکار ساخت که خیانت در عصر دیجیتال یک پدیدهٔ تک‌عاملی نیست، بلکه از هم‌افزایی سه لایهٔ اصلی پدید می‌آید:

۱) انگیزه‌های فردی - روان‌شناختی (تحقیر، نیاز به منزلت، بحران‌های شخصی)،
۲) فشارهای اقتصادی - سازمانی (مشکلات مالی، نابرابری و ناکامی شغلی)،
۳) فرصت‌های سایبری (ارتباطات آنلاین، ناشناسی و ابزارهای رمزگذاری).

این هم‌پوشانی نشان می‌دهد که چرا بسیاری از پرونده‌های معاصر نه توسط اجبار بیرونی بلکه به‌واسطهٔ داوطلبی و پیش‌قدم‌شدن فرد آغازشده‌اند. داده‌ها نشان می‌دهد که بحران‌های روان‌شناختی درونی معمولاً آستانهٔ خیانت را فعال می‌کنند و فضای دیجیتال تنها به‌عنوان کاتالیزور عمل می‌کند. بدین‌ترتیب، انگیزه‌های خیانت بیش از گذشته درونی‌شدن و فردمحور هستند.

ب) مقایسه با پیشینه پژوهش‌ها

یافته‌های حاضر با چارچوب کلاسیک MICE (پول، ایدئولوژی، اجبار، خودبزرگ‌بینی) هم‌پوشانی دارد، اما نشان می‌دهد که این مدل برای شرایط کنونی ناکافی است. برای نمونه، در پروندهٔ «محمدهادی صالح» هیچ‌یک از چهار عامل به‌تنهایی کفایت نداشت، بلکه ترکیب فشار مالی + تحقیر سازمانی + دسترسی دیجیتال موجب خیانت شد. این موضوع با نتایج پروژهٔ Slammer همسو است که بر نقش «خودویژه‌پنداری» و «بحران‌های حل‌نشده شخصی» تأکید می‌کرد.

از سوی دیگر، پژوهش‌های وزارت دفاع آمریکا نشان‌داده‌اند که سهم عوامل داوطلب در سه دههٔ اخیر افزایش چشمگیری داشته است؛ داده‌ای که نتایج حاضر آن را تأیید می‌کند. همچنین یافته‌های Quervain و همکاران در حوزهٔ عصب علمی (فعال‌شدن مدار پاداش مغز در رفتارهای انتقام‌جویانه) توضیح می‌دهد که چرا برخی افراد حتی در مواجهه با خطرات جدی، باز هم به خیانت ادامه می‌دهند: زیرا این عمل درونی برای آن‌ها نوعی لذت و پاداش عصبی به همراه دارد.

پ) نقش سایبر به‌عنوان شتاب‌دهنده

فضای دیجیتال به‌طور چشمگیری سرعت و سهولت جذب را افزایش داده است. اگر در گذشته برقراری ارتباط اولیه میان سرویس‌های اطلاعاتی و هدف مستلزم زمان، هزینه و خطر بالا بود، امروزه چند پیام در شبکه‌های اجتماعی (مانند LinkedIn یا X) کافی است تا دروازهٔ تعامل باز شود. این بستر امکان ناشناس‌ماندن، پرداخت رمزارزی و ارتباط رمزگذاری‌شده را فراهم می‌کند؛ عواملی که احتمال کشف را کاهش و جذابیت خیانت را افزایش می‌دهند؛ بنابراین، سایبر نه‌تنها بستر بلکه تسریع‌کننده چرخه خیانت است.

ت) بازاندیشی نظری

با توجه به نتایج به‌دست‌آمده، می‌توان گفت:

۱) مدل MICE باید بازتعریف شود تا مؤلفه‌های تحقیر روان‌شناختی و تسهیل‌گری دیجیتال را نیز در برگیرد.

۲) نظریهٔ شارنی مبنی بر نقش «شکست در اَنا» به‌عنوان نقطهٔ آستانهٔ خیانت تأیید شد.

۳) لازم است جاسوسی و خیانت در چارچوبی میان‌رشته‌ای (روان‌شناسی، عصب‌علم و امنیت سایبری) تحلیل شود، زیرا هیچ حوزه‌ای به‌تنهایی قادر به تبیین آن نیست.

ث) دلالت‌های کاربردی

یافته‌های این پژوهش چند پیام عملی روشن دارد:

۱) پایش روان‌شناختی کارکنان حساس: مداخله زودهنگام در بحران‌های فردی پیش از عبور از آستانهٔ خیانت.

۲) مدیریت خطر دیجیتال: توسعهٔ سامانه‌های هوش مصنوعی برای رصد تعاملات مشکوک در فضای سایبر و شبکه‌های اجتماعی.

۳) بهبود عدالت سازمانی: کاهش نابرابری‌های شغلی و مالی برای کاستن از فشارهای اقتصادی.

۴) آموزش ضدجاسوسی نسل جدید: تلفیق آموزش کلاسیک با سواد دیجیتال و مهارت‌های مقابله با مهندسی اجتماعی.

د) محدودیت‌ها تحقیق

این پژوهش محدودیت‌هایی نیز دارد:

۱) اتکا به منابع ثانویه و کمبود داده‌های دست اول از عوامل محکوم‌شده.

۲) استفاده از گزارش‌های اطلاعاتی غیررسمی که قابلیت اتکا در آن‌ها نیازمند احتیاط است.

۳) دشواری در سنجش مستقیم محرک‌های روانی و عصب‌شناختی به‌دلیل محدودیت‌های اخلاقی و عملی.

۴) محدودیت در تعمیم‌پذیری: یافته‌های این تحقیق بیشتر بر اساس پرونده‌ها و شواهد مربوط به جوامع خاص و نمونه‌های برجسته تدوین شد؛ بنابراین، تعمیم نتایج به تمام فرهنگ‌ها، کشورها یا شرایط سازمانی با احتیاط صورت می‌گیرد.

نتیجه‌گیری

پژوهش حاضر با عنوان «آناتومی خیانت» نشان‌داد که خیانت در سازمان‌های نظامی و اطلاعاتی در عصر دیجیتال، برخلاف گذشته که عمدتاً محصول شکار هدفمند و انگیزه‌های مالی یا ایدئولوژیک محدود بود، امروز به پدیده‌ای چندلایه و عمدتاً داوطلبانه

تبدیل شده است. داده‌ها و مطالعات موردی، ازجمله پرونده صالح در لبنان و نمونه‌های جنگ اطلاعاتی ایران و اسرائیل، نشان‌دادند که شکست‌های روان‌شناختی، فشارهای اقتصادی، خلأهای ساختاری و فرصت‌های سایبری در هم تنیده‌اند و فضایی ساخته‌اند که در آن فرد ناراضی یا تحقیرشده، نه با اجبار دشمن، بلکه با اراده و ابتکار خود به‌سمت خیانت حرکت می‌کند.

این تحول بنیادین تفاوتی اساسی با گذشته دارد: اگر پیش‌تر دشمن برای شناسایی و جذب عامل مجبور به طی فرایندی پرهزینه، زمان‌بر و پرخطر بود، امروز شبکه‌های اجتماعی و ابزارهای دیجیتال «پهنای باند جذب» را چندین برابر کرده و هزینه و خطر را به حداقل رسانده‌اند. به همین دلیل، خیانت دیگر یک استثنا نیست، بلکه به تهدیدی دائمی و بالقوه در بطن سازمان‌ها بدل شده است.

تحلیل آسیب‌پذیری‌ها نشان‌داد که:

۱) در سطح فردی ـ روانی، تحقیر، نادیده‌گرفتن و شکست‌های شخصی، محرک اصلی شکاف عاطفی و شکل‌گیری نارضایتی‌های عمیق است.

۲) در سطح اقتصادی ـ انگیزشی، فشار مالی، بی‌عدالتی و فرسایش انگیزه‌های شغلی، پذیرش پیشنهاد دشمن را تسهیل می‌کند.

۳) در سطح سایبری.دیجیتال، شبکه‌های اجتماعی، مهندسی اجتماعی و پروفایل‌های جعلی، ابزارهای اصلی شکار دیجیتال و جذب هستند.

۴) در سطح ساختاری ـ سازمانی، ضعف آموزش ضدجاسوسی، فقدان پایش هوشمند و کمبود حمایت‌های سازمانی، راه نفوذ و بهره‌برداری دشمن را هموار می‌سازد.

یافته‌ها تأکید می‌کنند که مقابله با این تهدید تنها از طریق یک رویکرد ترکیبی و هم‌زمان دفاعی و تهاجمی ممکن است:

۱) در حوزهٔ دفاعی، باید با پایش هوشمند خطر، مداخلات روان‌شناختی و حمایتی، تقویت عدالت سازمانی، آموزش ضدجاسوسی نوین و ارتقای سواد دیجیتال، ریشه‌های آسیب‌پذیری داخلی را خشکانید.

۲) در حوزهٔ تهاجمی، لازم است با عملیات فریب، مهندسی اجتماعی معکوس، ره‌گیری سایبری، تخریب اعتماد و امنیت دشمن و جاسوس به فضای ارتباطی و ابزارهای

جذب، بی‌اعتمادی در شبکه دشمن نسبت به خودمعرفین، هزینه و خطر ادامهٔ عملیات خیانت به‌شدت افزایش یابد.

درنهایت، «آناتومی خیانت» نشان می‌دهد که امنیت پایدار زمانی محقق می‌شود که خیانت و جاسوسی برای هر دو طرف ـ فرد داوطلب و سازمان جذب‌کننده - پرخطر، پرهزینه و کم‌ثمر باشد. سازمان‌های ضداطلاعاتی نقش محوری در تحقق این امنیت دارند: با شناسایی و پایش آسیب‌پذیری‌های روانی، اجتماعی و اقتصادی کارکنان، تقویت اعتماد و وفاداری داخلی، اعمال آموزش‌های پیشگیرانه و محدودسازی دسترسی به اطلاعات حساس، فرصت بهره‌برداری دشمن را به حداقل می‌رسانند. علاوه بر این، رصد مستمر فضای دیجیتال، شناسایی پروفایل‌های جعلی و شبکه‌های جذب دشمن و ایجاد زیرساخت‌های بازدارنده باعث کاهش اعتماد دشمن به توانایی‌های خود و افزایش هزینه و خطر اقدامات جاسوسی می‌شود.

این اقدامات نه‌تنها تهدیدهای جاری را خنثی می‌کنند، بلکه بازدارندگی فعال و پایدار در برابر خیانت و جاسوسی در عصر دیجیتال ایجاد می‌کنند و نشان می‌دهند که امنیت واقعی مبتنی بر مدیریت هم‌زمان رفتارها، انگیزه‌ها و آسیب‌پذیری‌های انسانی درون سازمان، به‌ویژه از طریق عملکرد سازمان‌های ضداطلاعاتی، تحقق می‌یابد.

پیشنهادها برای تحقیقات آینده

پژوهش‌های آتی می‌توانند با:

۱) تحلیل کلان‌داده شبکه‌های اجتماعی الگوهای جذب دیجیتال را مدل‌سازی کنند،

۲) مطالعات روان‌پزشکی بالینی روی عوامل سابق، اختلالات شخصیتی پرتکرار را آشکارسازند،

۳) با مدل‌سازی محاسباتی خطر جاسوسی، ابزارهای پیش‌بینی عملی در اختیار سازمان‌های امنیتی قرار دهند.

۴) مطالعات میان‌فرهنگی و تطبیقی: ازآنجاکه انگیزه‌های خیانت می‌تواند تحت‌تأثیر بافت فرهنگی، اجتماعی و سیاسی باشد، تحقیقات تطبیقی در میان کشورها و فرهنگ‌های مختلف می‌تواند به تدوین مدل‌های جامع‌تر و جهان‌شمول کمک کند.

منابع

منابع داخلی و منطقه‌ای

- العربیه. (۲۰۲۵). پرونده جاسوسی محمدهادی صالح. بازیابی‌شده از:https://www.alarabiya.net
- الشرق الاوسط. (۲۰۲۵). جزئیات مالی پرونده محمدهادی صالح. بازیابی‌شده از:.https://www.aawsat.com
- شفقنا. (۲۰۲۵). گزارش بازداشت صالح. بازیابی‌شده از:https://fa.shafaqna.com
- خبر فوری. (۲۰۲۵). تحلیل انگیزه‌های خیانت صالح. بازیابی‌شده از:https://khabarfoori.com
- المیادین. (۲۰۲۵). ابعاد ارتباطات دیجیتال صالح. بازیابی‌شده از:https://www.almayadeen.net
- دیار میرزا. (۲۰۲۵). اعترافات صالح و پیامدهای امنیتی. بازیابی‌شده از:https://diyarmirza.ir
- .Rasanah International Institute for Iranian Studies(۲۰۲۵). ابعاد امنیتی و اطلاعاتی جنگ ۱۲ روزه ایران-اسرائیل. بازیابی‌شده از:https://rasanah-iiis.org
- .Turan Research Center(۲۰۲۵). پیامدهای ژئوپلیتیک جاسوسی در منازعات خاورمیانه. بازیابی‌شده از:https://www.turanresearchcenter.org
- حسینی، م. (۲۰۲۳). جاسوسی و امنیت ملی در خاورمیانه. تهران: نشر مرکز پژوهش‌های امنیتی.
- رادفر، ن. (۲۰۲۴). تحلیل تهدیدات داخلی و جاسوسی سازمانی در ایران. تهران: انتشارات دانشگاه دفاع ملی.
- محمدی، س. (۲۰۲۲). ضدجاسوسی و امنیت داخلی: تجربه‌های ایرانی و منطقه‌ای. تهران: نشر اطلاعات.
- نوری، ع. (۲۰۲۳). جاسوسی دیجیتال و تهدیدات سایبری در ایران. تهران: انتشارات پژوهشگاه علوم و فنون دفاعی.
- قاسمی، ر. (۲۰۲۱). امنیت اطلاعات و تهدیدات داخلی در سازمان‌های دولتی ایران. تهران: دانشگاه شهید بهشتی.
- موسسه مطالعات امنیت ملی ایران. (۲۰۲۴). گزارش سالانه تهدیدات سایبری و داخلی. تهران:.IMSI
- پایگاه خبری تحلیلی تابناک. (۲۰۲۵). تحلیل پرونده جاسوسی محمدهادی صالح و ابعاد امنیتی آن. بازیابی‌شده از:https://www.tabnak.ir

منابع بین‌المللی:

- Button, M., Shepherd, D., & Jung, J. (2025). Economic espionage via fake social media profiles in the UK: Professional workers awareness and resilience. Security Journal, 38, 30. بازیابی‌شده از: https://link.springer.com/article/10.1057/s41284-025-00476-2

- Lishchynsky, M. (2025). THE INSIDER THREAT: A Socio Technical Analysis of Preventing Data Breaches and Espionage within Governmental Agencies. Politics & Security. بازیابی‌شده از: https://politics-security.net/index.php/ojsdata/article/view/284
- [2025] .(مقاله ناشناس). The Effect of Organizational Factors on the Mitigation of Information Security Insider Threats. Information, 16(7), 538. MDPI
- Saeed, S., Suayyid, S. A., Al Ghamdi, M. S., Al Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors. MDPI
- Social Learning and Reputation Management in an Espionage Crisis. (2023). Corporate Reputation Review. بازیابی‌شده از: https://link.springer.com
- A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and future prospects. (2025). Computers in Human Behavior Reports. ScienceDirect
- Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta analysis. Big Data Analytics. SpringerLink
- Savage, D., Zhang, X., Yu, X., Chou, P., & Wang, Q. (2016). Anomaly detection in online social networks. arXiv. بازیابی‌شده از: https://arxiv.org/abs/1606.04512
- Guo, Z., Cho, J.-H., Chen, I.-R., Sengupta, S., Hong, M., & Mitra, T. (2020). Online Social Deception and Its Countermeasures for Trustworthy Cyberspace: A Survey. arXiv. بازیابی‌شده از: https://arxiv.org/abs/2003.02873
- Adikari, S., & Dutta, K. (2020). Identifying Fake Profiles in LinkedIn. arXiv. بازیابی‌شده از: https://arxiv.org/abs/2005.04891
- Ali, H., Husain, S., & Hans, A. (2025). Real-Time Detection of Insider Threats Using Behavioral Analytics and Deep Evidential Clustering. arXiv. بازیابی‌شده از: https://arxiv.org/abs/2505.15383
- Gelman, R., & Hastings, T. (2025). Scalable and Ethical Insider Threat Detection through Data Synthesis and Analysis by LLMs. arXiv. بازیابی‌شده از: https://arxiv.org/abs/2502.07045
- Kalikiri, P., Singh, A., & Zhao, Y. (2024). Privacy Aware Memory Forensics: Insider Threat Detection in Encrypted Messaging Platforms. arXiv. بازیابی‌شده از: https://arxiv.org/abs/2406.09005

- Andrew, C. (2018). The Secret World: A History of Intelligence. Yale University Press.
- Andrew, C., & Mitrokhin, V. (2019). The Mitrokhin Archive II: The KGB in the World. Penguin Books.
- Richelson, J. T. (2020). The U.S. Intelligence Community. Routledge.
- Johnson, L. K. (2021). National Security Intelligence. Polity Press.
- Lowenthal, M. M. (2022). Intelligence: From Secrets to Policy. CQ Press.