*فصلنامه علمی امنیت ملی*
*سال یازدهم، شماره چهل‌ویکم، پاییز ۱۴۰۰*
*مقاله پنجم از صفحات ۱۵۸-۱۳۱*

**مقاله پژوهشی:** # تفاوت‌های امنیت سایبری اجتماعی با امنیت سایبری

محسن محمدی خانقاهی[۱]، محمدحسین آزادی[۲]

**تاریخ دریافت: ۹۹/۰۱/۲۸** **تاریخ پذیرش: ۹۹/۱۱/۲۰**

## چکیده

برخلاف اشکال سنتی حملات سایبری، امروزه عملیات‌های سایبری اعضای یک جامعه را هدف قرار می‌دهند و بر اعتقادات و باورهای آنان اثر می‌گذارند و میزان اعتماد به دولت‌ها را کاهش می‌دهند. مخالفان جمهوری اسلامی ایران اکنون به دنبال کنترل و بهره‌برداری از ظرفیت‌های رسانه‌های اجتماعی برای آسیب رساندن به منافع ملّی، بی‌اعتبار کردن نهادهای دولتی و خصوصی و ایجاد اختلافات داخلی هستند. این عملیات‌های نامحسوس نشان‌دهنده‌ی یک رویکرد نسبتاً جدید و به‌طور فزاینده‌ای خطرناک برای متقاعدسازی کاربران در رسانه‌های اجتماعی است؛ بنابراین، فعالان دولتی و غیردولتی خارج از ایران می‌توانند به‌جای حمله به تأسیسات نظامی یا اقتصادی، به جریان اطلاعات آنلاین از طریق رسانه-های اجتماعی دسترسی داشته باشند و از این طریق حوزه نوظهور امنیت سایبری اجتماعی کشور را به‌طور جدی تهدید کنند. پژوهش حاضر به بررسی این عرصه نوظهور پرداخته و تمایزات آن با امنیت سایبری را بررسی کرده است. براساس یافته‌ها می‌توان گفت امنیت سایبری اجتماعی از حیث ماهیت، ابزار و اهداف متفاوت از امنیت سایبری است. رسانه‌های اجتماعی به‌واسطه دو عامل مهم «غیرمتمرکزسازی» و «عدم نیاز به حضور فیزیکی» فضا را برای تولید و گسترش مطالب زیان‌بار نظیر اخبار جعلی و تهدید امنیت سایبری اجتماعی فراهم ساخته‌اند.

**کلیدواژه‌ها:** **رسانه‌های اجتماعی، امنیت سایبری، امنیت سایبری اجتماعی، اخبار جعلی، عملیات اطلاعاتی**

۱. دانشجو دکتری علوم سیاسی و پژوهشگر دانشگاه عالی دفاع ملی.
۲. کارشناس ارشد علوم ارتباطات، دانشگاه صداوسیما (نویسنده مسئول) mh.azadi73@gmail.com

## مقدمه و بیان مسئله

پیشرفت روزافزون فناوری نظیر پیدایش اینترنت، فرایند تولید و دسترسی به اخبار و اطلاعات را دگرگون ساخت. هیچ‌گاه انسان با این حجم از اطلاعات مواجه نشده بود. اگر روزی رسانه‌های جمعی نظیر رادیو، تلویزیون و روزنامه‌ها انحصار عرضه اخبار و اطلاعات را بر عهده داشتند، امروز رسانه‌های اجتماعی با انحصارزدایی از آن‌ها، امکان تولید اخبار و اطلاعات را در اختیار کاربران خود قرار داده‌اند. این کاربران اغلب شهروندان عادی یا همان شنوندگان، خوانندگان و بینندگان رسانه‌های جمعی هستند که به سبب ظهور نسل دوم اینترنت امکان تعامل با سایرین و عرضه اخبار و اطلاعات را بدون هیچ‌گونه سانسور و حتی نظارتی به دست آورده‌اند.

رسانه‌های جمعی اغلب تحت نظارت قوانین و مقررات دولتی و جهانی وظیفه خویش را ارتقای آگاهی و نشر حقیقت می‌دانند و تخطی از این مهم منجر به سلب اعتماد از آن‌ها و برخوردهای قانونی می‌شود؛ اما تکثر مبادی تولید اخبار و اطلاعات در رسانه‌های اجتماعی امکان نظارت قانونی از این فضای عظیم اطلاعاتی را تا حدود زیادی غیرممکن ساخته است.

رسانه‌های اجتماعی به همان اندازه که در تسهیل فرایند تعاملات جهانی، چرخش اطلاعات و ارتقای آگاهی مؤثر بوده‌اند، آسیب‌ها و خطراتی را نیز به دنبال داشته‌اند؛ به‌طوری‌که تولید و توزیع اطلاعات غلط و مغرضانه نظیر خبرهای جعلی، فرایند آگاه‌سازی و اعتماد عمومی را به‌شدت تحت شعاع قرار داده و آسیب‌های فراوانی را به اصولی نظیر دموکراسی وارد کرده است.

دولت‌های رقیب و عناصر مخالف با حکومت‌ها با اطلاع از ظرفیت بالای رسانه‌های اجتماعی و محصولاتی نظیر خبرهای جعلی با تشکیل گروه‌هایی حرفه‌ای اقدام به تولید و توزیع اطلاعات غلط و خبرهای جعلی در فضای سایبری کشورهای هدف کرده و افکار عمومی را در جهت اهداف خویش و تقابل با دولت‌هایشان بسیج می‌کنند. درواقع در «دوره پساحقیقت»[1] با ظهور کانال‌های ارتباطی جدید نظیر رسانه‌های اجتماعی مسیر

---

1. Post Truth Era.

ارتباط‌گیری با افکار عمومی نسبت به گذشته دگرگون شده و توییت‌ها می‌توانند توده‌ها را بسیج کنند و نتایجی را به دست آورند که چند سال پیش از آن غیرقابل تصور بود(ساعی، آزادی و البرزی، ۱۳۹۸: ۶۰).

شکل‌گیری این وضعیت منجر به ظهور زیرشاخه‌ای در امنیت ملّی با نام «امنیت سایبری اجتماعی»[۱]شده است. پیش از طرح مفهوم «امنیت سایبری اجتماعی» با مفهومی به نام «امنیت سایبری»[۲]مواجه بودیم، امنیت سایبری شامل عوامل انسانی است که از فناوری برای «هک کردن»[۳]فناوری استفاده می‌کنند و هدف آن سیستم‌های اطلاعاتی است ولی امنیت سایبری اجتماعی به بررسی نقش «واسطه‌های سایبری»[۴]می‌پردازد که از فناوری برای «هک کردن» انسان‌ها یا همان شهروندان و کاربران رسانه‌های اجتماعی استفاده می‌کنند. درواقع هدف امنیت سایبری اجتماعی، انسان‌ها و نظام‌های سیاسی و دست‌کاری در اطلاعات برای اثرگذاری بر افکار عمومی است (بسکو[۵]و همکاران، ۲۰۱۹).

اینک، پژوهش حاضر در تلاش است تا با مرور ظرفیت‌های رسانه‌های اجتماعی برای دست‌کاری اطلاعاتی در فضای جوامع، ماهیت و چیستی «امنیت سایبری اجتماعی» را بررسی کرده و تمایزات آن با حوزه «امنیت سایبری» را مورد واکاوی قرار دهد.

## ۱. مبانی نظری

### ۱-۱. پیشینه‌شناسی پژوهش

در منابع علمی داخلی مقاله یا پژوهشی که به بررسی مفهوم نوظهور «امنیت سایبری اجتماعی» پرداخته باشد یافت نشد ولی در منابع لاتین، مجموعه‌ای از مقالات را که از حیث معنا و مفهوم می‌توانست در پیشبرد مقاله حاضر یاری رساند بررسی و مختصری از آن را در ادامه مرور می‌کنیم.

---

۱. Social Cybersecurity.
۲. Cybersecurity.
۳. Hacking.
۴. Cyber Mediated.
۵. Beskow.

«جارد پریر»[۱](۲۰۱۷) در مقاله‌ای با عنوان «سلطه‌ی ترند: رسانه‌های اجتماعی به‌مثابه جنگ اطلاعاتی»[۲]که در فصلنامه مطالعات استراتژیک منتشر شده نشان می‌دهد چگونه رسانه‌های اجتماعی به ابزاری برای جنگ‌های اطلاعاتی جدید تبدیل شده‌اند. نویسنده بر این باور است که انتشار یک پیام تبلیغات سیاسی (پروپاگاندا) با ایجاد اختلال در روایت-های موجود همراه است. این پژوهش مدعی است این پیام‌ها به کمک ربات‌ها گسترش می‌یابند تا الگوریتم‌های رسانه‌های اجتماعی آن‌ها را به‌عنوان ترند تشخیص دهند. این سازوکار که با هدف متقاعدسازی کاربران یا همان شهروندان جامعه مدنی صورت می‌گیرد از ابزارهای مهم جنگ‌های اطلاعاتی است که بیشتر کشورها برای عملیات‌های اطلاعاتی بر ضد رقبا در رسانه‌های اجتماعی از آن بهره می‌جویند.

«کارلی، سروون، آگاروال و لیو»[۳](۲۰۱۹)، در مقاله‌ای با عنوان «امنیت سایبری اجتماعی»[۴]این حوزه را یک رشته علمی نوظهور می‌دانند که ماهیتی چند رشته‌ای دارد و تأکید آن بر راهبردهای اطلاعاتی پویا است. آن‌ها در این مقاله کوتاه از منظر خود به بررسی مختصر این رشته نوظهور علمی پرداخته‌اند.

«آلکات و گنزکو»[۵](۲۰۱۷) در مقاله «رسانه‌های اجتماعی و اخبار جعلی در انتخابات ۲۰۱۶ آمریکا»[۶]نشان داده‌اند کم‌وبیش تمام آمریکایی‌ها، دست‌کم یک یا چند خبر جعلی را در ماه منتهی به انتخابات دریافت کرده بودند و حدود بیش از نیمی از آن‌ها اخباری را باور کرده بودند که دیده بودند. نتایج همچنین نشان داد مردم اخباری را که از کاندیدای منتخب آن‌ها طرفداری می‌کند بیشتر باور می‌کنند.

«یوینگ، ماگلینسکی، ویلا کاکس، سووا و کارلی»[۷](۲۰۱۸) در مقاله «خطوط ارتباطی همکنش‌پذیر برای امنیت سایبری اجتماعی: ارزیابی عملیات اطلاعاتی توییتری در خصوص

---

۱. Jarred Prier.
۲. Commanding the Trend: Social Media as Information Warfare.
۳. Kathleen M. Carley, Guido Cervone, Nitin Agarwal, Huan Liu.
۴. Social Cyber Security.
۵. Allcott, Gentzkow.
۶. Social media and fake news in the 2016 Election.
۷. Uyheng, Magelinski, Villa-Cox, Sowa, M. Carley.

ناتو در سال ۲۰۱۸»[۱] با استفاده از ابزارهای یادگیری ماشین و پردازش اطلاعات شبکه به بررسی توییت‌های منتشرشده درباره ناتو در فضای توییتر پرداخته‌اند. آن‌ها مدعی هستند که فعالیت‌های قابل توجهی را که هدفشان بی‌اعتبار کردن ناتو بوده شناسایی کرده‌اند.

### ۱-۲. نظریه حباب فیلتر

اینترنت و رسانه‌های اجتماعی آن‌قدر اطلاعات در اختیار فرد قرار می‌دهند که تصمیم‌گیری در مورد اینکه کدام محتوا برای آن‌ها اهمیت دارد دشوار است. یک امکان فنی که می‌تواند و باید به کاربران اینترنت کمک کند تا اطلاعات مربوطه را انتخاب کنند، «سیستم‌های توصیه‌گر»[۲] هستند (رسنیک[۳] و همکاران، ۲۰۱۳). در این سیستم‌ها، یک الگوریتم، اطلاعات قابل مشاهده برای کاربر را فیلتر می‌کند و تلاش دارد محتواهایی را مطابق با علاقه و سلیقه کاربر فراهم سازد.

یک نتیجه ممکن از الگوریتم‌های توصیه‌گر، حباب‌های فیلتر و اتاق‌های پژواک هستند(پاریزر[۴] ۲۰۱۱). در چنین حباب‌ها یا اتاق‌هایی، کاربران تنها محتوایی که دوست دارند را می‌بینند، مانند نظرات و مواضع سیاسی که ناخواسته با باورهایشان مطابقت دارد(فلکسمن، گوئل و رائو[۵] ۲۰۱۶). چنانچه گفته شد، هدف اصلی سیستم‌های توصیه‌گر کاهش بار اضافی اطلاعات است، اما این سیستم‌ها خواسته یا ناخواسته یک هزینه مهم به همراه دارند؛ اگر سیستم‌های توصیه‌گر برای محتوای خبری اعمال شوند، ممکن است تنوع محتوایی که به یک کاربر نشان داده می‌شود را محدود کنند و در نتیجه او در حباب فیلتری از اخبار گیر بیفتد (زوییدروین[۶] و همکاران، ۲۰۱۶).

---

۱. Interoperable pipelines for social cyber‐security: assessing Twitter information operations during NATO Trident Juncture 2018.
۲. Recommender Systems.
۳. Resnick.
۴. Pariser.
۵. Flaxman, Goel & Rao.
۶. Zuiderveen.

پیام‌رسان اجتماعی «توییتر»[۱] قابلیت‌های جدیدی را به عرصه ارتباطات آنلاین معرفی کرد. یکی از این قابلیت‌های مهم «ترند»[۲] است که با سازوکار مبتنی بر «هشتگ»[۳] مفهوم‌سازی شده است. هشتگ می‌تواند یک کلیدواژه یا گویه باشد، سازوکار امکان شمارش دفعات استفاده از هشتگ‌ها بیانگر میزان مورد توجه قرار گرفتن آن نزد کاربران است (ناطقی، ۱۳۹۷: ۲۰). کاربرانی که الزاماً نظرات موافق یا مخالفی با آن هشتگ ندارند و ممکن است با هم اختلاف‌نظر هم داشته باشند. اگر دفعات انتشار یک هشتگ گسترده شود به‌اصطلاح «ترند» می‌شود و برای سایر کاربرانی که الزاماً هشتگ مشابهی منتشر نکرده‌اند نیز نمایش داده می‌شود به عبارتی کاربران را تحریک می‌کند تا توییت‌های مرتبط با آن هشتگ را بخوانند یا حتی منتشر کنند. هنگامی که یک هشتگ که براساس یک رویداد شکل می‌گیرد در فضای رسانه‌های اجتماعی ترند می‌شود سایر موضوعات و هشتگ‌ها را به حاشیه می‌راند و به تعبیری سایر صداها را خاموش می‌کند و باعث شنیده شدن تک‌صدای ترندشده می‌شود. طبق یک مطالعه در سال ۲۰۱۱ میلادی روی رسانه‌های اجتماعی، یک موضوع ترندشده «توجه مخاطبان زیادی را برای مدت کوتاهی جلب خواهد کرد» و در نتیجه «به سازوکار برجسته‌سازی آن موضوع در سطح جامعه کمک می‌کند»(آسور[۴] و همکاران، ۲۰۱۱). با استفاده از شبکه‌های آنلاین و ربات‌های موجود در آن‌ها، عناصر خارجی می‌توانند تبلیغات سیاسی را به یک پلتفرم رسانه اجتماعی وارد کنند، یک ترند بسازند و سریع‌تر و ارزان‌تر از هر رسانه دیگر پیام‌های مدنظرشان را پخش کنند. درواقع رسانه‌های اجتماعی با ایجاد ترندها ترویج یک روایت خارجی در گروه‌های اجتماعی داخلی را تسهیل می‌کنند (پریر[۵] ۲۰۱۷: ۵۲).

رونق ترندها منجر به ظهور شکل جدیدی از برجسته‌سازی شده است؛ به‌طوری که ترندها می‌توانند فضای فکری و رسانه‌ای جوامع را برای چندساعتی یا حتی چند روزی

---

۱. Twitter.
۲. Trend.
۳. Hashtag.
۴. Asur.
۵. Prier.

تحت تأثیر قرار دهند و به کاربران و حتی سایر شهروندان بگویند درباره چه موضوعی بیندیشند. این سطح از اثرگذاری ترندها باعث دخالت کاربران مخربی چون «ربات‌ها»[۱]، «ترول‌ها»[۲]و «سایبرگ‌ها»[۳]در ترندسازی برخی از هشتگ‌های خاص شده است. سازوکار ترند نوعی شخصی‌سازی اطلاعات است که توسط پلتفرم‌ها تعبیه شده و باعث شکل‌گیری پیله‌های اطلاعاتی در جامعه می‌شود.

## ۲. مبانی مفهومی

### ۲-۱. تبلیغات سیاسی (پروپاگاندا)

سازگاری رسانه‌های اجتماعی به‌عنوان ابزاری برای جنگ‌های مدرن نباید تعجب‌آور باشد. فناوری اینترنت برای پاسخگویی به نیازهای اطلاعاتی در حدود سال ۲۰۰۶ میلادی با ظهور وب ۲ متحول شد. وب ۲ به کاربران اینترنت اجازه می‌داد به‌جای مصرف صرف محتوای آنلاین، خود تولیدکننده محتوا باشند. علاوه بر این، فرد می‌توانست تصمیم بگیرد که چه چیزی برایش اهمیت دارد و فقط آنچه را که اهمیت دارد بخواند (جرمی[۴] ۲۰۰۵). پس ماهیت اجتماعی انسان درنهایت به شبکه‌های مجازی منجر شد. بر این اساس رقبای سیاسی به‌سرعت راه‌هایی برای بهره‌برداری از باز بودن اینترنت پیدا کردند و درنهایت در حال توسعه روش‌هایی برای استفاده از رسانه‌های اجتماعی به‌عنوان ابزاری برای انتشار تبلیغات سیاسی یا همان پروپاگاندا هستند. درواقع رسانه‌های اجتماعی نقطه‌ی تزریق تبلیغات سیاسی را فراهم می‌کنند و تبدیل به زنجیره عملیات‌های اطلاعاتی و جنگ‌های سایبری شده‌اند (پریر، ۲۰۱۷: ۵۱). برای درک این موضوع، باید مفهوم مهم پروپاگاندا را بررسی کنیم و مختصراً به اصول تبلیغات سیاسی بپردازیم.

---

۱. Bot.
۲. Trolls.
۳. Cybergs.
۴. Jeremy.

ریشه کلمه «پروپاگاندا»[۱] از واژه لاتین «پروپاگاره»[۲] مشتق شده است. کلمه پروپاگاره به معنای «پخش کردن»، «نشا کردن» و «چیزی را شناساندن» است که درواقع سه مرحله کاشت، داشت و برداشت را نشان می‌دهد (محسنیان راد، ۱۳۸۴: ۳۲۴)؛ اما معنای اصطلاحی پروپاگاندا عبارت است از «منتشر ساختن»[۳] یا «ترویج کردن»[۴] پاره‌ای از افکار و دیدگاه‌ها. براساس این نظر هدف از این اقدام، تقویت، جایگزین کردن یا تعدیل گرایش‌ها و رفتارهای گروهی از مخاطبان است (جووت و اودونل[۵]؛ ۲۰۱۸).

در تعریف لغت‌نامه آکسفورد این‌چنین آمده است: «اطلاعات جانب‌دارانه یا گمراه‌کننده‌ای است که برای ترویج علل و دیدگاه‌های سیاسی مورد استفاده قرار می‌گیرد» (لغت‌نامه آکسفورد[۶]؛ ۲۰۱۹).

«ژاکوس الول»[۷] (۱۹۷۳: ۶۱) در کتاب خود یعنی «پروپاگاندا: شکل‌گیری نگرش مردم»[۸] نظریه خود درباره پروپاگاندا را این‌چنین توضیح می‌دهد که طی آن «یک گروه سازمان‌یافته، از پلتفرم‌های رسانه‌ای برای به‌کارگیری مشارکت فعالانه یا منفعلانه توده‌های مردمی بهره می‌گیرد». در این زمینه اغلب اوقات، واقعیت‌ها به‌صورت گزینشی بیان و بازنمایی می‌شوند تا شاهد واکنش و رفتاری احساسی و نه آگاهانه و خردمندانه از سوی مخاطب باشیم. نتیجه این امر، تغییر گرایش دلخواه به‌سوی هدفی است که برای مخاطب و به‌منظور پیشبرد یک برنامه سیاسی، در نظر گرفته شده است (ریخته‌گری برنجی و کدخدایی، ۱۳۹۷).

---

۱. Propaganda.
۲. Propagare.
۳. Disseminate.
۴. Promote.
۵. Jowett & O'donnell.
۶. Oxford Dictionary.
۷. Jacques Ellul.
۸. The Formation of Men's Attitudes.

### ۲-۲. جنگ سایبری و اطلاعاتی

جنگ سایبری یا اطلاعاتی[۱] محصول عصر اطلاعات است که در آن تأکید بسیاری بر فناوری‌های اطلاعاتی و اطلاعات به‌عنوان تسلیحات شده است (مالونون[۲] ۱۹۹۹: ۱۸۰). اطلاعات در این نوع نبرد در حکم قلمرو، سلاح و هدف به شمار می‌رود (ویلسون[۳] ۲۰۰۴: ۲). جنگ اطلاعاتی توسط جوامع و ارتش‌های پیشرفته توسعه می‌یابد. تسلیحات این نوع نبرد تنها می‌تواند در برابر دشمنی مورد استفاده قرار گیرد که دارای قابلیت‌های پیشرفته مشابهی باشد (هائین[۴] ۱۹۹۷: ۳).

این نوع نبرد نسبتاً جدید بوده و اصطلاح جنگ اطلاعاتی دارای معانی مختلفی نیز بوده است (هائین، ۱۹۹۷: ۴). بنابراین می‌توان شاهد فقدان وجود تعریف رسمی برای تبیین مفهوم جنگ اطلاعاتی بود. این امر در حالی است که جنگ اطلاعاتی به‌طور معمول به‌عنوان به‌کارگیری و مدیریت اطلاعات برای پیگیری مزیت‌های رقابتی، ازجمله تلاش‌های تدافعی و تهاجمی مفهوم‌سازی می‌شود؛ بنابراین این نبرد نه‌تنها دارای بُعد نظامی بوده، بلکه برای توصیف «جنگ» در اینترنت مورد استفاده قرار می‌گیرد (همان: ۴). در ابتدا اصطلاح جنگ اطلاعاتی تنها براساس استفاده از فناوری‌های اطلاعاتی و ارتباطی برای شکست زیرساخت‌های اطلاعاتی به‌منظور اخلال در آن‌ها یا دست‌یابی به اطلاعات و اطلاعات مرتبط به منابع حریف، راهبرد نظامی و... تعریف می‌شده است (تادئو[۵] ۲۰۱۲۱: ۱۰۹).

یکی از مراکز مهمی که احتمال می‌رود نقش مهمی در به‌کارگیری و هدایت کاربران مخرب داشته باشد و اقدام به رصد مستمر و دست‌کاری در حوزه اطلاعاتی کشورهای همسایه جهت برهم زدن امنیت سایبری اجتماعی آن‌ها کند، مرکز اعتدال[۶] (مرکز جهانی مبارزه با افراط‌گرایی) عربستان سعودی است. این مرکز پیشرفته در ۲۱ مه ۲۰۱۷ میلادی با

---

۱. Information or Cyberwarfare.
۲. Mulvenon.
۳. Wilson.
۴. Haein.
۵. Taddeo.
۶. Etidal – Global center for combating extremist ideology.

حضور ملک سلمان پادشاه عربستان، دونالد ترامپ رئیس‌جمهور آمریکا و تعدادی از رهبران کشورهای عربی افتتاح شد (مشرق، ۱۳۹۸).

**تصویر ۱. مرکز اعتدال عربستان سعودی**

یکی دیگر از مراکز مهم عملیات‌های اطلاعاتی با هدف دست‌کاری در حوزه مجازی که به‌طور خاص بر ایران متمرکز است، مرکز سایبری گروهک منافقین در آلبانی است. این مرکز نیز همچون مرکز اعتدال با به‌کارگیری کاربران مخرب به‌طور سازمان‌دهی شده و مستمر بر فضای مجازی ایران اثرگذاری می‌کنند. رضا حیرانی از اعضای جداشده این گروه در مصاحبه با نشریه اینترسپیت گفته: «در پایگاه اشرف عراق، کامپیوترهایی برای انجام عملیات آنلاین بر ضد ایران راه‌اندازی شد. در طول سال‌ها، این فعالیت با معرفی پلتفرم-های اجتماعی مثل فیس‌بوک و توییتر شدیدتر شد». او با اشاره به تولید خبرهای جعلی بر ضد ایران ادامه می‌دهد: «ما به‌طور مستمر خبرهایی جعلی برای اثرگذاری بر فضای خبری داخل و خارج از ایران تولید و منتشر می‌کردیم» (حسین[۱]، ۲۰۱۹).

**تصویر ۲. مقر سایبری گروهک منافقین**

۱. Hussain.

### ۲-۳. رسانه‌های اجتماعی

رسانه‌های اجتماعی، گونه‌ای از رسانه‌ها هستند که بعد از رسانه‌های جمعی بر بستر وب ۲ ظهور پیدا کرده و امکان تعامل میان تولیدکننده پیام و دریافت‌کننده آن را فراهم می‌آورند. به این معنا که در این رسانه‌ها، مخاطب یا گیرنده پیام منفعل نبوده و ضمن تبدیل شدن به کاربر، به تعامل پویا و فعالانه با پیام، فرستنده، فرایند ارسال و دریافت و بستر ارائه پیام می‌پردازد و امکان ایجاد تغییرات در پیام ارسالی و بازنشر آن را دارد که به افراد دیگر پیامی ترکیب‌شده با اندیشه‌ها و آموزه‌های فکری خود را بازنشر می‌دهد. وجه اشتراک گونه‌های متعدد رسانه‌های اجتماعی، کاربر محور بودن آن‌ها و تولید محتوا توسط افراد استفاده‌کننده است (اکبری‌تبار و اسکندری‌پور، ۱۳۹۱). رسانه‌های اجتماعی بستر قدرتمندی را برای شهروندان در سراسر جهان فراهم کرده است تا از این طریق در مباحث سیاسی مشارکت کنند و در مقیاس بی‌سابقه‌ای تبادل‌نظر کنند (کانه و بویر[۱] ۲۰۱۸: ۴۹۳-۴۷۰).

در حوزه سیاسی، رسانه‌های اجتماعی یک فضای بسیار دموکراتیک را برای گفتمان عمومی معرفی کرده‌اند. خطوط ارتباطی ارائه‌شده توسط پلتفرم‌های رسانه‌های اجتماعی به فعالان مختلف سراسر جوامع اجازه می‌دهد تا ایده‌ها و اطلاعات را به شیوه‌ای نسبتاً بدون محدودیت تبادل کنند. با این حال به همین دلایل رسانه‌های اجتماعی نیز مستعد دست‌کاری هستند (مک گاتی[۲] و همکاران، ۲۰۱۴). «ریچارد دیاکون»[۳] (۱۹۸۷: ۹۵) در کتاب خود[۴] رایانه‌ها را تهدیدی برای تفکر مستقل انسان‌ها دانسته و بر این باور بود که انسان‌ها تحت کنترل رایانه‌ها قرار می‌گیرند؛ به‌گونه‌ای که هر چیزی رایانه به آن‌ها می‌گوید می‌پذیرند. او معتقد بود پروپاگاندا ابزار قدرتمندی است که برای دست‌کاری عموم به‌طور گسترده مورد استفاده قرار می‌گیرد. رسانه‌های اجتماعی گسترش تبلیغات سیاسی را برای هر دو بازیگر دولتی و غیردولتی آسان‌تر می‌سازد (پریر، ۲۰۱۷: ۷۹).

---

۱. Kahne & Bowyer.
۲. McGarty.
۳. Richard Deacon.
۴. Truth Twisters.

عملیات‌های اطلاعاتی هدفمند در این پلتفرم‌ها از طریق معرفی تأثیرات مصنوعی به مکالمات آنلاین، چنین ظرفیت دموکراتیزه‌ای را محدود می‌کنند (آگاروال و بندلی[۱] ۲۰۱۸). با استفاده از عوامل مصنوعی نظیر ربات‌ها، عملیات‌های اطلاعاتی در ساختار شبکه‌ای پلتفرم‌های رسانه‌های اجتماعی اختلال ایجاد می‌کنند (کارلی[۲] و همکاران، ۲۰۱۸: ۳۹۰). به عبارتی پیام‌های طراحی‌شده برای اثرگذاری بر افکار و رفتار جوامع رقیب از قرن‌ها پیش وجود داشته، اما ظهور رسانه‌های اجتماعی به دلیل ویژگی‌هایی چون سرعت بالای چرخش اطلاعات انتشار گسترده‌ی تبلیغات سیاسی را سریع‌تر و آسان‌تر از همیشه کرده است (پریر، ۲۰۱۷: ۵۶). به عبارتی به‌واسطه رسانه‌های اجتماعی، موازی با جامعه مدنی یک جامعه شبکه‌ای شکل گرفته و کاربران در این جامعه تمایل دارند اطلاعات منتشرشده در رسانه‌های اجتماعی را باور کنند؛ زیرا آن‌ها به‌طور معمول افرادی را دنبال می‌کنند که مطالبی متناسب با عقایدشان را به اشتراک می‌گذارند. به همین ترتیب کاربران مطالب را با افراد همفکر خود و کاربرانی که مستعد دریافت آن محتوا هستند به اشتراک می‌گذارند و در عرض چند دقیقه یک روایت بیگانه و محتوای هدفمند مضر در این شبکه گسترش می‌یابد و بر اذهان عمومی اثر می‌گذارد.

### ۲-۴. امنیت سایبری

تهدیدهای سایبری پدیده‌ای جدید است که در دهه‌های اخیر، هم‌زمان با تحول فناوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسر جهان ظهور پیدا کرده است، به‌گونه‌ای که امروز چالش تهدیدهای سایبری، هم مهم و هم پیچیده به نظر می‌رسد. تهدیدهای سایبری ویژگی‌های منحصربه‌فردی دارند. از یک‌سو، این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند و از سوی دیگر، هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران زیادی به این عرصه وارد شوند (خلیلی‌پور و نورعلی‌وند، ۱۳۹۱: ۱۶۹-۱۶۸).

---

۱. Agarwal & Bandeli.
۲. Carley.

در طول دهه گذشته، شماری از ویژگی‌های عمومی که به‌وسیله کامپیوتر شکل گرفته و به تهدیدهای سایبری معروف شده‌اند، به‌عنوان یکی از بدترین تهدیدهای منافع ملی امروز شناسایی شده است (کاوتلی[۱] ۲۰۱۰: ۱۸۰). بر این اساس، می‌توان امنیت سایبری را به‌طور کلی به‌عنوان «حفاظت از زیرساخت‌های اطلاعاتی مهم و فرایندها و محتوای آن تعریف کرد»(تئواری و رولینس[۲] ۲۰۰۹)

**۲-۵. امنیت سایبری اجتماعی:**

قرن بیستم شاهد جنگ‌های متقارن و پویایی بود، در حالی که قرن ۲۱ پس از جنگ‌های سرد، با درگیری نامتقارن متعدد و غیرپویایی آغاز شد. در طول جنگ جهانی اول هزاران نفر تنها برای متری زمین قربانی شدند. امروزه بسیاری از بازیگران عرصه بین‌الملل، طراحی‌های پیچیده‌ای برای رسیدن به حوزه‌های انسانی برنامه‌ریزی می‌کنند تا به پیشرفت در حوزه‌های فیزیکی دست یابند.

«دیمیتری کیسلیو»[۳]هماهنگ‌کننده آژانس دولتی روسیه معتقد است «اصلی‌ترین نوع جنگ، جنگ اطلاعاتی است. از اطلاعات برای تقویت روایت شما هنگام حمله، از هم گسیختن، تحریف و چندپاره کردن جامعه، فرهنگ و ارزش‌های کشورها و سازمان‌های رقیب استفاده می‌شود» (جوشوا[۴] ۲۰۱۴).

«بارتلز»[۵](۲۰۱۶: ۳۸-۳۰) با مطالعاتی که در خصوص انقلاب‌های کشورهای عربی داشته، معتقد است بهار عربی و ائتلاف شکل گرفته در این مقطع به رهبری ایالات متحده آمریکا به‌شدت بر منابعی به غیر از نیروهای نظامی متعارف متکی بودند. به عقیده وی نیروهای نظامی فقط در آخرین لحظه به‌عنوان نیرویی که تیر خلاص را شلیک می‌کند وارد عمل می‌شدند. این پژوهشگر شکل‌گیری رویدادهای یادشده در کشورهایی نظیر مصر، لیبی،

۱. Cavetly.
۲. Theohary & Rollins.
۳. Dmitry Kiselev.
۴. Joshua.
۵. Bartles.

الجزایر و... را نتیجه «عملیات‌های اطلاعاتی»[۱] می‌داند و اظهار می‌دارد: «جنگ اطلاعاتی، امکانات نامتقارن وسیعی برای کاهش ظرفیت جنگی دشمن ایجاد می‌کند».

درواقع عملیات اطلاعاتی برای اختلاف‌افکنی بین احزاب سیاسی، نژادها، مذاهب، بین یک ملت و دولت آن و همچنین بین یک ملت و هم‌پیمانانش است، چراکه یک ملت شکست‌خورده از نظر توانایی دفاعی (ملت چندپاره) در برابر حملات، ذاتاً ملتی ضعیف‌تر است.

به‌طور کلی دو تغییر عمده در ارتباطات انسانی و جریان‌های اطلاعاتی، تهدید سایبری اجتماعی را فعال ساخته است. نخست آنکه، فناوری، نیاز به نزدیکی و مجاورت فیزیکی برای اثرگذاری بر جامعه را نادیده گرفته و دوم تمرکززدایی از جریان‌های اطلاعاتی، هزینه ورود را کاهش داده است. در همین راستا «فابیو روگی»[۲](۲۰۱۸) از «مؤسسه مطالعات سیاسی بین‌الملل ایتالیا»[۳]این موضوع را این‌چنین توضیح می‌دهد: «فضای سایبری، یک عامل قدرتمند برای تأثیرات بی‌ثبات‌کننده از طریق دست‌کاری اطلاعات است؛ چراکه با عبور از مرزهای مرسوم جغرافیایی، ارتباطی سریع، ارزان، بدون واسطه و فراملی را رقم می‌زند و از همه مهم‌تر ناشناسی کاربران متعدد، فضای مجازی را به فضایی مبهم تبدیل کرده است». به عبارتی در این رسانه‌ها، هزینه ورود، تولید و توزیع اطلاعات ارزان است و هویت‌ها در بسیاری از موارد ناشناخته باقی می‌ماند؛ بنابراین فضا برای ورود بازیگران خارجی و تمرکززدایی از جریان اطلاعات به‌راحتی فراهم آمده است (شئارر و گاتفید[۴] ۲۰۱۷). از طرفی اینترنت به بازیگرانی از گوشه‌های دنیا این اجازه را می‌دهد تا در مباحث سیاسی کشورهای دیگر مشارکت کنند. به‌طور واضح کشورهایی که آزادی بیان و عرصه‌ای آزاد برای عقاید و ایده‌ها را ارج می‌نهند در برابر این تهدیدات آسیب‌پذیرتر هستند (بایومن[۵] ۲۰۱: ۶۳-۵۰). از آن رو که اکثر اقدامات اطلاعاتی بر روی پلتفرم‌های رسانه‌های اجتماعی بین‌المللی انجام می‌گیرد و این پلتفرم‌ها تحت مالکیت خصوصی و خارج از نظارت مستقیم دولت‌ها (هرچند تحت

---

۱. Information Operation.
۲. Fabio Rugge.
۳. The Italian Institute for International Political Studies.
۴. Shearer & Gottfried.
۵. Baumann.

تأثیر مقررات) قرار دارند، تخریب جوامع آزاد از طریق دست‌کاری اطلاعات تشدید یافته است. مدیریت محتوا در محیط رسانه‌های اجتماعی به‌جای نگرانی‌های امنیت ملی برای هر کشور، به‌طور کلی بر بهبود تجربه کاربران تمرکز دارد.

امنیت سایبری اجتماعی زیرشاخه‌ای در حال ظهور از امنیت ملی است که بر تمام سطوح جنگ‌های متعارف و غیرمتعارف آینده که دارای عواقب راهبردی هستند تأثیرگذار است. امنیت سایبری اجتماعی ذاتاً علم اجتماعی محاسباتی و چند رشته‌ای شامل علوم سیاسی، جامعه‌شناسی، ارتباطات، رایانه و هوش مصنوعی است. بسیاری از محققان در این زمینه از ابزارهای علوم اجتماعی محاسباتی، مانند آنالیز شبکه، آنالیز فضایی، آنالیز معنایی و یادگیری ماشینی استفاده می‌کنند (بسکوف و کارلی، ۲۰۱۹: ۱۱۸).

از نظر ماهیت، امنیت سایبری اجتماعی از امنیت سایبری سنتی متفاوت است. امنیت سایبری سنتی شامل استفاده انسان از فناوری برای «هک»[1] فناوری است و هدف آن سیستم‌های اطلاعاتی است. امنیت سایبری اجتماعی دربرگیرنده انسان استفاده‌کننده از فناوری برای «هک» انسان‌های دیگر است. اهداف، انسان‌ها و جامعه‌ای است که آن‌ها را به هم پیوند می‌دهد که این امر در پارادایم سنتی سایبری گاهی اوقات به‌عنوان «هک شناختی»[2] معرفی می‌شود (بسکوف و کارلی، ۲۰۱۹: ۱۱۸).

به‌منظور دفاع از امنیت کشور، رهبران سیاسی و نظامی باید این نظم در حال ظهور امنیت سایبری اجتماعی و چگونگی تأثیر آن بر اعضا و ارزش‌های جامعه را درک کنند. اصلی‌ترین هدف عملیات‌های اطلاعاتی تضعیف اعتماد بین دولت–ملت است (بسکوف و کارلی، ۲۰۱۹: ۱۲۶).

**۲-۵-۱. انواع مانور سایبری اجتماعی**

همانند حوزه فیزیکی، حوزه اینترنتی سایبری نیز از شگردهای خاصی برای دست‌یابی به اهدافش بهره می‌برد. در این حوزه، رقیب می‌تواند علاوه بر اطلاعات، شبکه‌های ارتباطی را نیز دست‌کاری کند. این شبکه‌ها می‌توانند شبکه‌های اجتماعی (صابر و سلمان دوست

---

۱. Hack.
۲. Cognitive hacking.

هم هستند) شبکه‌های مکالمه (پاسخ صابر به سلمان) یا شبکه‌های اطلاعاتی (صابر و سلمان هر دو یک هشتگ را به اشتراک می‌گذارند) باشند.

حالت پایان مطلوب برای عملیات‌های اطلاعاتی، متفاوت است. عملیات‌های اطلاعاتی سنتی حمایت از روایت مطلوب را افزایش داده و حمایت از روایت مقابل را کاهش می‌دهند. سایر عملیات علاوه بر پایان مطلوب در پی افزایش تحریک و کاهش اعتماد در جامعه هستند. هدف مانور اطلاعات، دست‌کاری اطلاعات و جریان ارتباطی در فضای مجازی است. از آن جمله می‌توان به موارد زیر اشاره کرد (بسکوف و کارلی، ۲۰۱۹):

«**راهنمایی غلط**»[۱] وارد کردن موضوعات تفرقه‌ساز و بی‌ربط به یک بحث آنلاین به‌منظور تغییر در فرایند گفتگو.

«**ایجاد روایت از طریق ترندسازی**»[۲] سازوکار ترند یک روش قدرتمند برای انتشار اطلاعات است، ترند می‌تواند به سبب درگیر ساختن افکار عمومی پیامش را به خارج از رسانه‌های اجتماعی منتقل کند. ترندسازی نیازمند تلاش زیادی ازجمله صرف هزینه و به‌کارگیری ربات‌های زیادی است (پریر، ۲۰۱۷: ۵۴).

«**چفت کردن هشتگ‌ها**»[۳] پیوند محتوا و روایت به هشتگ‌ها و موضوعات غیرمرتبط ترند شده.

«**استتار دود**»[۴] پخش محتوا (هم از لحاظ معنا و هم از لحاظ جغرافیایی) برای پنهان سازی سایر مباحث آنلاین. درواقع هدف از این نوع مانور تغییر توجه افراد از یک موضوع به موضوعات دیگر است.

«**محتواربایی**»[۵] به معنای گرفتن بخشی از یک پیام اصلی و تغییر آن به سمت محتوایی است که عاملان در نظر دارند.

---

۱. Misdirection.
۲. Narrative creation by Trend.
۳. Hashtag latching.
۴. Smoke screening.
۵. Thread jacking.

در مانور شبکه نیز رقیب یک شبکه اجتماعی را ترسیم می‌کند. نمونه‌هایی از مانور شبکه عبارت‌اند از:

«**به دام انداختن رهبران افکار**»[۱] تهییج رهبران افکار برای اظهارنظر در خصوص روایت طراحی شده و استفاده از نفوذ وی برای انتشار آن در سطح جامعه.

«**انجمن‌سازی**»[۲] ایجاد انجمن حول یک موضوع، ایده یا سرگرمی سپس تزریق یک روایت در انجمن.

«**اتصال جوامع آنلاین**»[۳] تزریق عقاید از یک گروه به گروه دیگر. در این حالت، عوامل مانور، دو جامعه «الف» و «ب» را شناسایی می‌کنند. هدف آن‌ها تزریق ایده‌های گروه «ب» به گروه «الف» است. این هدف ابتدا با نفوذ در گروه «الف» انجام می‌شود، سپس به‌آرامی ایده‌ها از گروه «ب» به گروه «الف» منتقل می‌شوند.

«**تعمیم روایت‌های کاذب**»[۴] ترویج یک تصور اشتباه مبنی بر اینکه یک روایت خاص مورد اجماع توده‌ها است؛ بنابراین باید آن روایت توسط همه مورد پذیرش قرار گیرد.

## ۳. روش‌شناسی تحقیق

پژوهش حاضر از نقطه‌نظر روش‌شناسی، یک تحقیق توصیفی- تحلیلی و از لحاظ هدف یک پژوهش «توسعه‌ای کاربردی»[۵]است. از ویژگی‌های تحقیق توصیفی این است که محقق دخالتی در موقعیت، وضعیت و نقش متغیرها ندارد و آن‌ها را دست‌کاری و کنترل نمی‌کند(حافظ‌نیا، ۱۳۸۷). از طرف دیگر این پژوهش یک تحقیق کاربردی است و براساس نیاز به استفاده انجام گرفته است. ابزار مورد استفاده در این

---

۱. Opinion leader co-opting.
۲. Community building.
۳. Community bridging.
۴. False generalized other.
۵. Applied Research.

پژوهش کیفی از حیث گردآوری اطلاعات «مطالعه اسنادی و کتابخانه‌ای» است. سپس داده‌های به‌دست‌آمده را با استفاده از روش تحلیل محتوای کیفی بررسی کرده و مقولات و زیرمقولات را در قالب جدولی ارائه دادیم. پژوهشگر با بررسی منابع موجود و مرتبط دست اول، ضمن مطالعه دقیق، اقدام به کدگذاری مطالب نمود و از این طریق مجموعه‌ای از مقولات را کشف و به مقایسه گذارد. در طول پژوهش برای افزایش اعتبارپذیری، مقولات توسط دو کارشناس دیگر کدگذاری و نتایج مشابهی به دست آمد.

## ۴. تجزیه‌وتحلیل یافته‌ها

اگر در دهه‌های گذشته، ظهور فناوری‌هایی نظیر اینترنت و شکل‌گیری خدمات ناشی از آن، فرصت را برای تهدید سایبری ملت‌ها و دست‌کاری در سیستم‌ها و سرویس‌های مبتنی بر نت فراهم ساخته بود، امروزه توسعه همان فناوری‌ها، بازیگران دولتی و غیردولتی را قادر می‌سازد تا بازار جهانی عقاید و باورها را با بذر الگوریتم‌ها دست‌کاری کنند. این اقدام در پوشش «عملیات اطلاعاتی» و با هدف «دست‌کاری اطلاعاتی» در جوامع هدف انجام می‌گیرد. در حال حاضر هر دو تهدید، یعنی «دست‌کاری سیستم» و «دست‌کاری اطلاعات» موجودند و «امنیت سایبری» و «امنیت سایبری اجتماعی» نقاط مورد نظر را به شکلی تهدید می‌کنند. از آن رو که مفهوم «امنیت سایبری اجتماعی» به‌تازگی وارد ادبیات حوزه امنیت شده، بسیاری از مراکز درگیر و چهره‌ها و محافل آکادمیک درک جامعی از آن ندارند و مرزبندی آن با مقوله «امنیت سایبری» روشن نیست؛ بنابراین در این بخش، مهم‌ترین تفاوت‌های این دو حوزه مهم امنیتی را بررسی می‌کنیم.

**جدول ۱. تفاوت‌های امنیت سایبری و امنیت سایبری اجتماعی**

| مقوله‌ها | | زیرمقوله‌ها |
|---|---|---|
| ماهیت | امنیت سایبری | علمی مبتنی بر علوم رایانه و فناوری اطلاعات است |
| | | استفاده انسان از فناوری برای «هک» فناوری |
| | | تمرکز اصلی بر فناوری |
| | | تأکید بر حملات و زیرساخت‌های سایبری است |
| | | عملیات براساس «فیشینگ» به معنای سرقت رمزها و اطلاعات شخصی |
| | | تمرکز بر حفظ حریم خصوصی افراد |
| | امنیت سایبری اجتماعی | علمی اجتماعی محاسباتی و چند رشته‌ای شامل علوم سیاسی، جامعه‌شناسی، روان‌شناسی، علوم ارتباطات، انسان‌شناسی و... است |
| | | استفاده انسان از فناوری برای «هک» انسان‌های دیگر |
| | | تمرکز بر حوزه انسانی برای پیشرفت نهایی در حوزه فیزیکی |
| | | تأکید بر دست‌کاری افراد، گروه‌ها و جوامع است |
| | | عملیات فیشینگ به معنای قلاب کردن و هدایت ذهن |
| | | تمرکز اصلی بر زمینه‌های اجتماعی و سیاسی |
| | | تمرکز بر نحوه دست‌کاری گروه‌ها و شکل‌دهی عقاید آن‌ها |
| | | مبارزه برای کنترل ذهن انسان و هدایت آن به نقطه مطلوب |
| | | به‌طور عمده این عملیات جنبه‌ی تهاجمی دارند |
| | | تمرکز بر نحوه دست‌کاری گروه‌ها و شکل‌دهی عقاید آن‌ها |
| | | به بار آوردن پیامدهای اجتماعی و سیاسی از طریق اثرگذاری بر رفتار انسان‌ها |
| ابزار | امنیت سایبری | اینترنت |
| | | تروجان |
| | | ویروس |
| | امنیت سایبری اجتماعی | اینترنت |
| | | رسانه‌های اجتماعی |
| | | اطلاعات دروغ، گمراه‌کننده و مضر |
| | | شایعه |
| | | خبر جعلی |
| اهداف | امنیت سایبری | هدف امنیت سایبری، سیستم‌های اطلاعاتی است |
| | | هدف اثرگذاری بر فناوری، سرقت یا نابود کردن اطلاعات و سرقت پول یا هویت است |

| مقوله‌ها | | زیرمقوله‌ها |
|---|---|---|
| | | اختلال در صحت و درستی داده‌ها از طریق کدهای مخرب و تغییر در منطق برنامه |
| | | ایجاد اختلال در خدمات مبتنی بر اطلاعات و ارتباطات نظیر سیستم‌های آب‌رسانی، برق-رسانی، مخابرات، بانکداری، حمل‌ونقل هوایی و... |
| | | برنامه‌ریزی عملیات‌های تروریستی و فرماندهی و کنترل عملیات از طریق ابزارهایی چون نقشه‌های اینترنتی و سرویس موقعیت‌یاب |
| | | نقض حق مالکیت معنوی، نقض حق اختراع و ربودن اسرار تجاری و کپی‌برداری از اطلاعات دیجیتال |
| | | سرقت اطلاعات نظامی، صنعتی، سیاسی و فنی از طریق حمله به رایانه‌های هدف |
| | امنیت سایبری اجتماعی | هدف عمده، انسان‌ها و جامعه‌ای است که آن‌ها را به هم پیوند می‌دهد |
| | | اختلاف‌افکنی و ایجاد شکاف سیاسی، مذهبی و نژادی در میان یک جامعه و بین یک جامعه و هم‌پیمانانش |
| | | از هم گسیختن، تحریف، تقسیم و چندپاره کردن جامعه، فرهنگ و ارزش‌های کشورها و سازمان‌های رقیب |
| | | تضعیف تعهد به ارزش‌های ملی و تعهد به آن ارزش‌ها در سطوح بین‌المللی |
| | | تضعیف اعتماد به چهره‌ها و مؤسسات ملّی |
| | | تقویت یک روایت مشخص در جنگ گفتمان‌ها و روایت‌ها حول یک رویداد یا مجموعه-ای از رویدادها |
| | | تقویت و سازمان‌دهی جنبش‌های غیرمتمرکز از طریق فناوری‌هایی نظیر رسانه‌های اجتماعی |
| | | اختلال در فضای اطلاعاتی از طریق حاشیه‌سازی، تغییر اولویت‌ها، طرح موضوعات تفرقه-ساز و به حاشیه راندن موضوعات اصلی به سمت موضوعات فرعی |
| | | کاهش ظرفیت و توان نظامی جامعه هدف |

تهدیدات موجود در هر دو حوزه امنیت سایبری و امنیت سایبری اجتماعی توسط عواملی صورت می‌گیرد. این عوامل در حوزه امنیت سایبری اغلب با نام «هکر»[1] و در حوزه امنیت سایبری اجتماعی تحت اصطلاح «واسطه‌گران اجتماعی»[2] شناخته می‌شوند. در این بخش به بررسی این عوامل و نقش آن‌ها در تهدیدآفرینی‌های موجود می‌پردازیم.

۱. Hacker.
۲. Social Mediates.

**جدول .Error! No text of specified style in document۲. واسطه‌گران اجتماعی و ویژگی-های آن‌ها**

| مقوله‌ها | | زیرمقوله‌ها |
|---|---|---|
| واسطه‌گران سایبری | امنیت سایبری | هکر |
| | امنیت سایبری اجتماعی | ترول |
| | | ربات |
| | | سایبرگ |

## ۵. نتیجه‌گیری

### ۵-۱. تفاوت‌های امنیت سایبری اجتماعی با امنیت سایبری از حیث «ماهیت»

امنیت سایبری اجتماعی را می‌توان در سه مقوله کلی «ماهیت»، «ابزار» و «اهداف» با امنیت سایبری مقایسه کرد. از حیث ماهیت، امنیت سایبری علمی مبتنی بر علوم رایانه و فناوری اطلاعات است. در این حوزه انسان‌ها از فناوری برای هک کردن فناوری استفاده می‌کنند. تمرکز اصلی در حوزه امنیت سایبری بر فناوری و حمله به زیرساخت‌های سایبری است. عملیات‌ها در امنیت سایبری براساس فیشینگ صورت می‌گیرد. در فیشینگ رمزها و اطلاعات شخصی همچنین اطلاعات سیاسی، نظامی و... با حمله به رایانه‌ها و سرورهای هدف سرقت می‌شوند؛ بنابراین در امنیت سایبری تمرکز به حفظ حریم خصوصی و ارتقای سطح امنیت سایبری کاربران، شرکت‌ها و سازمان‌ها است.

در مقابل امنیت سایبری اجتماعی، علمی اجتماعی محاسباتی و چند رشته‌ای شامل علوم سیاسی، جامعه‌شناسی، روان‌شناسی، علوم ارتباطات، انسان‌شناسی و... است. اگر پیش‌تر از طریق عملیات‌های نظامی اقدام به پیشرفت در حوزه فیزیکی و جغرافیایی؛ برای مثال فروپاشی حکومت‌ها، استعمار، اشغال اراضی و... می‌شد، امروزه از طریق اینترنت و رسانه‌های اجتماعی نخست بر حوزه انسانی تمرکز می‌شوند و درنهایت عملیات به پیشرفت در حوزه فیزیکی ختم می‌شود. در حوزه امنیت سایبری اجتماعی انسان‌ها از فناوری برای هک کردن انسان‌های دیگر استفاده می‌کنند. تأکید آن‌ها بر زمینه‌های اجتماعی

و سیاسی و دست‌کاری افراد، گروه‌ها و جوامع و شکل‌دهی عقاید آن‌ها است. به عبارتی عملیات‌های صورت گرفته به‌طور عمده جنبه‌ی تهاجمی دارند و نوعی تلاش برای کنترل ذهن و اثرگذاری بر رفتار انسان‌ها و هدایت آن‌ها به نقطه مطلوب برای به باور آوردن پیامدهای اجتماعی و سیاسی است. عملیات‌ها در حوزه امنیت سایبری اجتماعی به‌صورت فیشینگ به معنای طعمه‌سازی که می‌تواند تولید اطلاعات غلط و گمراه‌کننده، اخبار جعلی و شایعات باشد و سپس قلاب کردن کاربران رسانه‌ها و هدایت ذهن‌ها آن‌ها انجام می‌شود. به‌طور قطع حضور کاربران در حباب فیلتر و پیله‌های اطلاعاتی امکان اثرپذیری از این عملیات‌ها را به‌مراتب افزایش می‌دهد.

### ۵-۲. تفاوت‌های امنیت سایبری اجتماعی با امنیت سایبری از حیث «ابزار»

از حیث ابزار، امنیت سایبری به‌وسیله ابزارهایی چون اینترنت، تروجان و ویروس و امنیت سایبری اجتماعی به‌وسیله ابزارهایی چون اینترنت، رسانه‌های اجتماعی، اطلاعات دروغ و گمراه‌کننده، شایعات و خبرهای جعلی انجام می‌شود.

چنانچه اشاره شد، تهدیدات موجود در هر دو حوزه امنیت سایبری و امنیت سایبری اجتماعی توسط عواملی صورت می‌گیرد. این عوامل در حوزه امنیت سایبری اغلب با نام «هکر» و در حوزه امنیت سایبری اجتماعی تحت اصطلاح «واسطه‌گران اجتماعی» شناخته می‌شوند. یکی از بخش‌های مهم و اصلی در ارتکاب جرائم سایبری مربوط به بخش سرقت اطلاعات «هک و نفوذ» است. به‌طور کلی هک و نفوذ را هکرها انجام می‌دهند. هکر به معنای نفوذگر است و به شخصی که هدف اصلی او نشان دادن قدرت خود به رایانه و سایر ماشین‌ها است گفته می‌شود. هکرها به چهار دسته کلی هکر کلاه سفید، هکر کلاه سیاه، هکر کلاه صورتی و هکر کلاه خاکستری تقسیم می‌شوند. در حوزه امنیت سایبری اجتماعی، عوامل را که از آن‌ها به «واسطه‌گر اجتماعی» یاد می‌شود به سه دسته عمده ترول، ربات و سایبرگ تقسیم می‌شوند. ربات‌ها نوعی از حساب‌های رسانه‌های اجتماعی هستند که توسط یک الگوریتم رایانه‌ای کنترل می‌شوند و می‌توانند نهادهای

مخربی باشند که به‌خصوص برای دست‌کاری اطلاعات، سرکوب و ارعاب مخالفان و انتشار خبرهای جعلی در رسانه‌های اجتماعی طراحی شده‌اند. ربات‌ها با بازنشر خبر جعلی در گروه‌ها و صفحات مجازی این توهم را به مخاطب القا می‌کنند که آن مطالب به‌طور گسترده‌ای توسط کاربران دیگر دیده شده است. درواقع، این ربات‌ها به‌طور هماهنگ و خودکار مجموعه‌ای از خبرهای جعلی را در فضای مجازی پمپاژ می‌کنند و احتمال تصدیق کاربران بر محتواهای آنلاین مضر را به‌شدت افزایش می‌دهند.

ربات‌ها برای واقع‌نمایی، گفتگوهای جزئی‌تر را به اپراتورهای انسانی واگذار می‌کنند. این بازیگران انسانی اغلب به‌عنوان «ترول» یاد می‌شوند. ترول در گفتمان اینترنتی به افرادی گفته می‌شود که با رفتار مخرب در فضای وب به دنبال جلب نظر کاربران، ایجاد تشنج و بیان مطالب محرک و توهین‌آمیز هستند. اگرچه ما اغلب برای طبقه‌بندی یک حساب به ربات یا انسان (ترول) تلاش می‌کنیم، اما اغلب یک طیف متفاوتی از مشارکت خودکار با یک حساب وجود دارد. بسیاری از حساب‌ها تنها خودکار نیستند؛ به این معنا که تمام کنش‌ها توسط رایانه انجام شود. این حساب‌ها به مداخله انسان نیاز دارند تا به دیالوگ‌های جزئی‌تر کمک کنند. این گروه‌ها که درواقع ترکیبی از ورودی انسانی و ماشینی‌اند را سایبرگ می‌نامند. نتیجه این ترکیب، وقوع عملیات‌های پیچیده است.

به‌طور خلاصه می‌توان گفت، دولت‌های رقیب و حتی افراد حقیقی تلاش می‌کنند از طریق به‌کارگیری ابزارهای مختلف ازجمله استخدام ربات‌ها و ترول‌ها و دست‌کاری در محتوای رسانه‌های اجتماعی توان اثرگذاری و حتی بازدارندگی خود را افزایش دهند. دولت-ها طیف مختلفی از اقدامات ازجمله جلوگیری از دسترسی به رسانه‌های اجتماعی، شایعه-پراکنی در رسانه‌های اجتماعی و نیز تحمیل برداشت خود را برای اعمال قدرت در فضای مجازی به کار می‌گیرند. در این میان، عملیات‌های اطلاعاتی به گزینه قدرتمندی در رقابت‌ها تبدیل شده و رقابت در فضای مجازی همانند فضای واقعی بین دولت‌ها در جریان است. به‌طوری که رقبا از فضای مجازی جهت اثرگذاری بر رویدادها و تحولات داخلی یکدیگر و دست‌یابی به نتایج دلخواه استفاده می‌کنند. در این میان، تولید و نشر اخبار جعلی، ترندسازی

در رسانه‌های اجتماعی و استفاده از ترول‌ها و ربات‌ها از اهمیت ویژه‌ای برخوردارند.

**۵-۳. تفاوت‌های امنیت سایبری اجتماعی با امنیت سایبری از حیث «اهداف»**

اهداف تهاجمات در حوزه امنیت سایبری عبارت‌اند از: سیستم‌های اطلاعاتی، اثرگذاری بر فناوری، سرقت یا نابود کردن اطلاعات و سرقت پول یا هویت، اختلال در صحت و درستی داده‌ها از طریق کدهای مخرب و تغییر در منطق برنامه، ایجاد اختلال در خدمات مبتنی بر اطلاعات و ارتباطات نظیر سیستم‌های آب‌رسانی، برق‌رسانی، مخابرات، بانکداری، حمل‌ونقل هوایی و...، برنامه‌ریزی عملیات‌های تروریستی و فرماندهی و کنترل عملیات از طریق ابزارهایی چون نقشه‌های اینترنتی و سرویس موقعیت‌یاب، نقض حق مالکیت معنوی، نقض حق اختراع و ربودن اسرار تجاری و کپی‌برداری از اطلاعات دیجیتال و سرقت اطلاعات نظامی، صنعتی، سیاسی و فنی از طریق حمله به رایانه‌های هدف. اهداف تهاجمات در حوزه امنیت سایبری اجتماعی را می‌توان در راستای جنگ روانی تعریف کرد، عمده این اهداف عبارت‌اند از: انسان‌ها و جامعه‌ای که آن‌ها را به هم پیوند می‌دهد (این انسان‌ها اینک به‌واسطه رسانه‌های اجتماعی، یک جامعه شبکه‌ای تشکیل داده‌اند. جامعه‌ای که حوزه امنیتی آن «امنیت سایبری اجتماعی» نام دارد و توسط عوامل بیگانه مورد تهدید جدی قرار گرفته است)، اختلاف‌افکنی و ایجاد شکاف سیاسی، مذهبی و نژادی در میان یک جامعه و بین یک جامعه و هم‌پیمانانش، از هم گسیختن، تحریف، تقسیم و چندپاره کردن جامعه، فرهنگ و ارزش‌های کشورها و سازمان‌های رقیب، تضعیف تعهد به ارزش‌های ملّی و تعهد به آن ارزش‌ها در سطوح بین‌المللی، تضعیف اعتماد به چهره‌ها و مؤسسات ملّی، تقویت یک روایت مشخص در جنگ گفتمان‌ها و روایت‌ها حول یک رویداد یا مجموعه‌ای از رویدادها، تقویت و سازمان‌دهی جنبش‌های غیرمتمرکز از طریق فناوری‌هایی نظیر رسانه‌های اجتماعی، اختلال در فضای اطلاعاتی از طریق حاشیه‌سازی، تغییر اولویت‌ها، طرح موضوعات تفرقه‌ساز و به حاشیه راندن موضوعات اصلی به سمت موضوعات فرعی و کاهش ظرفیت و توان نظامی جامعه هدف.

## فهرست منابع ومآخذ

### الف. منابع فارسی


- اکبری‌تبار، علی‌اکبر و اسکندری‌پور، ابراهیم (۱۳۹۱)، روش مطالعه علمی در باب صفحه‌های مرتبط با شبکه‌های رادیو و تلویزیونی در شبکه‌های اجتماعی مجازی (با رویکرد ترکیبی کمّی و کیفی)، ***پژوهش‌های ارتباطی***، ۲۰(۷۶)، ۱۴۱-۱۱۳.
- حافظ‌نیا، محمدرضا (۱۳۸۷)، ***مقدمه‌ای بر روش تحقیق در علوم انسانی***، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).
- خلیلی‌پور رکن‌آبادی، علی و نورعلی‌وند، یاسر (۱۳۹۱)، تهدیدات سایبری و تأثیر آن بر امنیت ملی، ***فصلنامه مطالعات راهبردی***، ۲(۵۶)، ۱۶۷-۱۹۶.
- ریخته‌گر برنجی، ریحانه و کدخدایی عباس (۱۳۹۷)، رویکرد حقوق بین‌الملل در خصوص تبلیغات خصمانه برای جنگ (پروپاگاندا)، ***فصلنامه مطالعات حقوق عمومی***، ۴۸(۳)، ۵۲۵-۵۴۵.
- ساعی، محمدحسین؛ آزادی، محمدحسین و البرزی دعوتی، هادی (۱۳۹۸)، ظهور «خبر جعلی» در «عصر پساحقیقت»؛ اهداف و پیامدها، ***فصلنامه رسانه‌های دیداری و شنیداری***، ۱۳(۳۱)، ۵۹-۸۵.
- محسنیان راد، مهدی (۱۳۸۴)، ایران در چهار کهکشان ارتباطی، تهران: انتشارات سروش.
- مشرق (۱۳۹۸)، مرکز اعتدال چه نقشی در تحولات اخیر عراق داشته است؟ منتشرشده در ۱۳۹۸/۷/۱۲. mshrgh.ir/998349. مطالعه‌شده در ۱۳۹۸/۱۲/۲۵.
- ناطقی، امیرحسین (۱۳۹۷)، ***دگردیسی نظریه‌های ارتباطی از رسانه‌های سنتی به رسانه‌های نوین: مطالعه تطبیقی برجسته‌سازی تلویزیونی و ترند توییتری در رخدادهای دی‌ماه ۱۳۹۶***، پایان‌نامه کارشناسی ارشد علوم ارتباطات اجتماعی، تهران: دانشگاه صداوسیما.


### ب. منابع انگلیسی


- Agarwal, N., & Bandeli, K. K. (2018). Examining strategic integration of social media platforms in disinformation campaign coordination. ***Defence Strategic Communications***, *4*(1), 173.
- Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 Election. ***Journal of Economic Perspectives,*** 31(2), 211-36.

- Asur, S., Huberman, B. A., Szabo, G., & Wang, C. (2011, July). Trends in social media: Persistence and decay. In ***Fifth international AAAI conference on weblogs and social media***.
- Bartles, C. K. (2016). Getting Gerasimov Right. ***Military Review***, *96*(1), 30-38.
- Baumann, R. F. (2018). A Central Asian Perspective on Russian Soft Power: The View from Tashkent. ***Military Review***, *98*(4), 48.
- Beskow, D. M., & Carley, K. M. (2019). Social cybersecurity: an emerging national security requirement. ***Military Review***, 99(2), 117.
- Beskow, D. M., & Carley, K. M. (2019). Social cybersecurity: an emerging national security requirement. ***Military Review***, 99(2), 117.
- Carley, K. M., Cervone, G., Agarwal, N., & Liu, H. (2018, July). Social cyber-security. In ***International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation*** (pp. 389-394). Springer, Cham.
- , R. (1987). ***The truth twisters***. Macdonald.
- Ellul, J. (1973). ***Propaganda: The formation of men's attitudes*** (pp. 116-120). New York: Vintage Books.
- Flaxman, S., Goel, S., & Rao, J. M. (2016). Filter bubbles, echo chambers, and online news consumption. ***Public opinion quarterly***, *80*(S1), 298-320.
- Hussain, Murtaza. (2019). ***An Iranian activist wrote dozens of articles for right-wing outlets. But is he real person?***. Published June 9 2019, https://theintercept.com/2019/06/09/heshmat-alavi-fake-iran-mek/.
- Jeremy, Scott-Joynt. (2005). ***What Myspace Means to Murdoch. BBC News Analysis***, 19 July 2005, http://news.bbc.co.uk/2/hi/business/4697671.stml.
- Joshua, Yaffa (2014). Dmitry Kiselev Is Redefining the Art of Russian Propaganda. ***The New Republic*** (website), 1 July 2014, accessed 14 November 2018, https://newrepublic.com/article/118438/dmitrykiselev-putins-favorite-tv-host-russias-top-propogandist.
- Jowett, G. S., & O'donnell, V. (2018). ***Propaganda & persuasion***. Sage Publications.
- Kahne, J., & Bowyer, B. (2018). The political significance of social media activity and social networks. ***Political Communication***, *35*(3), 470-493.
- McGarty, C., Thomas, E. F., Lala, G., Smith, L. G., & Bliuc, A. M. (2014). New Technologies, New Identities, and the Growth of Mass Opposition in the A rab S pring. ***Political Psychology***, *35*(6), 725-740.
- Mulvenon, J. (1999). "The PLA and information warfare". The People's Liberation Army in the Information Age, 297, pp.175-186.
- , E. (2011). ***The filter bubble: What the Internet is hiding from you***. Penguin UK.
- Prier, J. (2017). Commanding the trend: Social media as information warfare. ***Strategic Studies Quarterly***, *11*(4), 50-85.
- Resnick, P., Garrett, R. K., Kriplean, T., Munson, S. A., & Stroud, N. J. (2013, February). Bursting your (filter) bubble: strategies for promoting diverse exposure. In ***Proceedings of the 2013 conference on Computer supported cooperative work companion*** (pp. 95-100). ACM.

- Rugge, Fabio. (2018). "'Mind Hacking': Information Warfare in the Cyber Age," Analysis No. 319, ***Italian Institute for International Political Studies***, 11 January 2018, accessed 14 November 2018, https://www.ispionline.it/en/pubblicazione/mind-hacking-information-warfare-cyber-age-19414.
- Shearer, Elisa & Gottfried ,Jeffrey .(2017). News Use Across Social Media Platforms 2017," ***Pew Research Center***, 7 September 2017, accessed 14 November 2018, http:// www.journalism.org/2017/09/07/news-use-across-socialmedia-platforms-2017/.
- Taddeo, M. (2012). "Information warfare: A philosophical perspective". ***Philosophy & Technology***, 25(1), pp.105-120.
- Theohary, C. A. (2018). "Information Warfare: Issues for Congress". ***Congressional Research Service***.
- Uyheng, J., Magelinski, T., Villa-Cox, R., Sowa, C., & Carley, K. M. (2019). Interoperable pipelines for social cyber-security: assessing Twitter information operations during NATO Trident Juncture 2018. ***Computational and Mathematical Organization Theory***, 1-19.
- Wilson, C. (2004). Information Warfare and Cyberwar: Capabilities and Related Policy Issues. ***CRS Report for Congress***. pp.1-21.
- Zuiderveen, Borgesius, F., Trilling, D., Möller, J., Bodó, B., De Vreese, C. H., & Helberger, N. (2016). Should we worry about filter bubbles?. ***Internet Policy Review. Journal on Internet Regulation***, *5*(1).