

## پلیس آینده و شبکه‌های اجتماعی مجازی: فرصت‌ها و چالش‌ها

نادر رازقی<sup>۱</sup>

کاظم عباس نژاد عربی<sup>۲</sup>

تاریخ پذیرش نهایی: ۹۶/۳/۱۸

تاریخ دریافت: ۹۵/۱۱/۱۳

فصلنامه‌ی مطالعات راهبردی ناجا / سال دوم / شماره سوم - بهار ۱۳۹۶

### چکیده

رشد شتابان شبکه‌های اجتماعی مجازی تغییراتی در فعالیت‌های پلیس ایجاد کرده است. گزارش‌های راهبردی شرکت‌های بزرگ مخابراتی و اینترنتی جهان نشان می‌دهد تا سال ۲۰۲۰ میلادی، ۵۰ میلیارد دستگاه متصل به اینترنت وجود خواهد داشت که از این تعداد ۱۵ میلیارد دستگاه‌های تلفن همراه و تبلت‌ها هستند که کاربران را قادر می‌سازند به صورت آن‌لاین به فیلم‌ها و کلیپ‌های ویدئویی دسترسی یابند. بخشی دیگر از این آمارها حاکی از آن است که تا پایان این دهه پهنای باند شبکه‌های تلفن همراه ۹۰ درصد از جمعیت کل جهان را تحت پوشش قرار خواهد داد.

این مقاله تلاش دارد به این پرسش پاسخ دهد که شبکه اجتماعی مجازی چه فرصت‌ها و چالش‌هایی برای پلیس ایجاد می‌کند؟ فرصت‌های شبکه‌های اجتماعی مجازی برای پلیس را در سه بخش فرصت‌های ایجاد، ارتباط و کشف می‌توان بیان کرد. در مقاله حاضر شبکه‌های اجتماعی مجازی به عنوان فرصتی برای ایجاد و به‌روزرسانی هشدارهای پلیس، کشف جرم، خوانش رفتاری، ارتقای همکاری و تحلیل آنها مورد کنکاش و بررسی قرار گرفته است. پلیس علاوه بر فرصت، با چالش‌ها و خطرهای بالقوه‌ای در شبکه‌های اجتماعی در حال و آینده روبه‌روست. چالش‌های سطح خرد در شبکه‌های اجتماعی مجازی عبارت‌اند از: هرزه‌نگاری جنسی، سوءاستفاده از کودکان، پورنوگرافی، آسیب‌های امنیتی، تجاوز به حریم خصوصی و جرایم مالی. در سطح کلان، چالش‌های هویتی و انزوای اجتماعی، اعتیاد اینترنتی و تروریسم اینترنتی مورد بحث قرار گرفته است. بدون شک، یکی از مباحث مورد توجه برای سازمان‌های امنیتی و انتظامی در این سیر دگردیسی، جهت‌دهی و تغییر شکل محتوایی جرایم سنتی به تکامل‌یافته (ترکیب مجازی و سنتی) و جرایم نوظهور (صرفاً سایبری) و ظهور پدیده جرایم

۱. استادیار جامعه‌شناسی گروه علوم اجتماعی دانشگاه مازندران

۲. کارشناسی ارشد پژوهشگری علوم اجتماعی

سایبری است که در حال حاضر با رویکردهای اجتماعی، سیاسی، مالی، امنیتی و شبه‌امنیتی در حال گسترش است.

## واژگان کلیدی

پلیس آینده، شبکه اجتماعی مجازی، جرایم اینترنتی، فرصت‌ها، چالش‌ها

### مقدمه

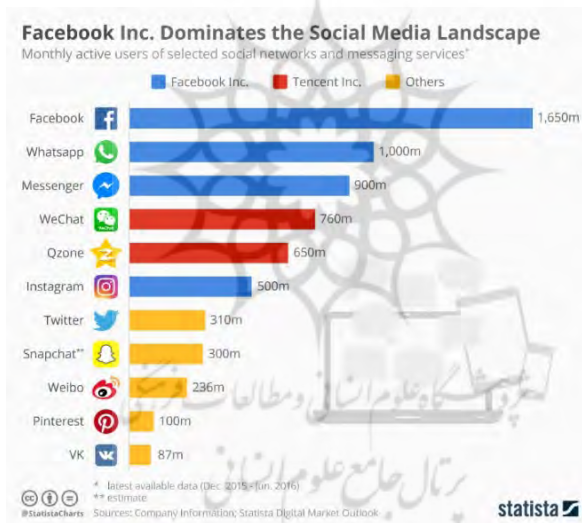
میل و اشتیاق پیوستن به جامعه مجازی و بهره‌مندی از مزایای آن، تمایلی جهانی است که بین آحاد مردم و دولت‌ها با سرعت درخور توجهی در حال افزایش است. در سند ششم توسعه جمهوری اسلامی ایران که در سال ۱۳۹۴ مقام معظم رهبری ابلاغ کردند، بر حرکت سریع‌تر در فضای مجازی تأکید شده است. برای مثال یکی از مباحث مورد توجه در سند ششم توسعه کشور موضوع صدور فرهنگ از طریق ظرفیت فضای مجازی است. در بند ۳۳ سند ششم، توسعه محتوا در فضای مجازی بر اساس نقشه مهندسی فرهنگی کشور تا حداقل پنج برابر وضعیت کنونی و بومی‌سازی شبکه‌های اجتماعی و در بند ۷۲ حضور مؤثر نهادهای فرهنگی، دولتی و مردمی در فضای مجازی به منظور توسعه و ترویج فرهنگ، مفاهیم و هویت اسلامی- ایرانی و مقابله با تهدیدها مورد تأکید قرار گرفته است. برابر گزارش پلیس فتا، در حال حاضر جرایم ارتكابی در فضای سایبر بیشتر با محوریت برداشت‌های غیرمجاز و سرقت‌های اینترنتی و برابر گزارش سازمان‌های امنیتی، جرایم ارتكابی در فضای سایبر بیشتر با محوریت باندهای قاچاق و تبه‌کار مثل مواد مخدر و...، جاسوسی و سرقت اطلاعات مطرح است که البته جامعه هدف آن نیز با جرایم عمومی که پلیس فتا رسیدگی می‌کند، متفاوت است. برای مثال سیاسیون، افراد نظامی، دانشمندان علوم نوین و سایر افراد نظامی، دانشمندان علوم نوین و سایر افراد تأثیرگذار که به اطلاعات مهم و طبقه‌بندی‌دار دسترسی دارند، همواره به عنوان جامعه هدف باندهای تبه‌کار و سرویس‌های جاسوسی و امنیتی مورد توجه هستند و به صورت پنهان یا آشکار در مسیر ارتكاب جرم از طریق فضای سایبر قرار می‌گیرند (یادگاری و همکاران، ۱۳۹۴: ۴۲-۴۳).

## طرح مسئله

ما در جهانی متحول و دست‌خوش دگرگونی‌های چشم‌گیر و مستمر زندگی می‌کنیم (گیدنز، ۱۳۷۳: ۵۰). یکی از شگفت‌انگیزترین رویدادهای دنیای معاصر را می‌توان سرعت بی‌سابقه تغییرات اجتماعی دانست (لنسکی و دیگران، ۱۳۶۹: ۱۱۲). زمینه بسیاری از چنین تغییر و تحولات سریع و شگرفی بی‌شک دستاوردهای تکنولوژیکی جدید مربوط به اینترنت است. اینترنت با ایجاد فضایی بدون محدودیت زمان، مرزهای جغرافیایی و سیاسی به وجود آورده است. رشد روزافزون شبکه جهانی وب باعث شده است که این شبکه در سراسر جهان به عنوان رسانه‌ای کارآمد به منظور تبادل اطلاعات اقتصادی، سیاسی، فرهنگی و علمی و اشاعه آن در حدی گسترده مورد توجه قرار گیرد. ارتباطات اینترنتی، افراد سراسر جهان را نسبت به وضع خود حساس و تأثیرپذیر کرده است. اکنون همه مردم آگاهی بیشتری برای تغییرپذیری دارند. افراد از طریق این رسانه، به شیوه‌ای تعاملی از نحوه زندگی سایر ملل آگاه می‌شوند و می‌کوشند ارزش‌ها و سنت‌هایی را که مانع ارتقای سطح زندگی‌شان می‌شود، کنار بگذارند یا تغییر دهند (رازقی، ۱۳۸۹ و ۱۳۹۰). باید اذعان کرد تکنولوژی‌های جدید نه تنها قواعد و قوانین حاکم بر ارتباط و تعامل میان انسان‌ها، بلکه نگرش‌های ما را نسبت به خود، دیگران و جهان تغییر داده‌اند (اولسون، ۱۳۷۷: ۵۷).

شبکه اجتماعی مجازی با همه تسهیلاتی که برای جوامع فراهم کرده، سبب ایجاد یا تسهیل بسیاری از آسیب‌ها، انحراف‌ها و خشونت‌های نوین شده یا اینکه انحراف‌ها و جرم‌هایی را که در گذشته وجود داشته، تسهیل و حمایت کرده است. خشونت، آزار و اذیت‌های دنیای جدید و حتی جرایم با رشد فزاینده شبکه‌های ارتباطی مجازی، شکل جدیدی به خود گرفته‌اند. امروز خشونت‌ها دیگر به محیط فیزیکی‌مان محدود نمی‌شود. ما هر روز با ایمیل‌ها، پیام‌های ناخواسته و به عبارت دیگر، با اشکال نوینی از خشونت روبه‌رو هستیم. دسترسی بدون محدودیت به انواع اطلاعات، دسترسی به محتوای متنوع و بولتن بوردهای مختلف، دانلود برنامه‌ها، عضویت در گروه‌های مختلف شبکه اجتماعی مجازی که ممکن است بسیاری از آنها منفی باشند و کاربران را در مسیر مخاطره‌آمیزی هدایت کنند. به خصوص افراد کم سن و سال که تجربه و مهارت زندگی اجتماعی کمتری دارند به راحتی تحت تأثیر قرار می‌گیرند و ممکن است قربانی خشونت‌های متفاوتی شوند. توسعه انواع خشونت‌ها، انحراف‌ها و جرایم جدید در فضای مجازی بسیار گسترده، به پهنای فضای بی‌انتهای اینترنت است.

از سال ۲۰۱۰ تا کنون با رشد فزاینده کاربران شبکه‌های اجتماعی مجازی روبه‌رو هستیم. پیش‌بینی می‌شود تعداد کاربران رسانه‌های اجتماعی در سراسر جهان تا سال ۲۰۲۰ به سه میلیارد نفر برسد. هر دو سال اندازه اطلاعات در فضای مجازی دو برابر می‌شود و تا سال ۲۰۲۰ به ۴۴ زتا بایت (ZB) یا ۴۴ تریلیون گیگا بایت می‌رسد. در فیس بوک با ۱,۴۴ میلیارد کاربر فعال ماهانه در هر دقیقه ۳۱/۲۵ میلیون پیام و ۲/۷۷ میلیون ویدئو در هر دقیقه دیده می‌شود. توییتر با ۲۸۸ میلیون کاربر فعال در ماه به طور متوسط ۳۴۷,۲۲۲ در هر دقیقه توییت می‌شود. در اینستاگرام هر دقیقه ۴۸,۶۱۱ تصویر پست می‌شود. در یوتیوب<sup>۱</sup> با یک میلیارد کاربر در هر دقیقه ۳۰۰ ساعت ویدئو آپلود<sup>۲</sup> می‌شود. تا پایان سال ۲۰۱۶ شاهد ظهور شبکه‌های اجتماعی جدیدی مانند تلگرام، اینستاگرام، واتس آپ، تانگو و مانند آن بودیم. برخی از آنها در کشور ما بسیار مورد استقبال قرار گرفته‌اند.



علاوه بر تنوع شبکه‌های اجتماعی مجازی، ما با بخش متنوعی از انواع محتوای مجازی هم روبه‌رو هستیم. این تحولات عظیم در فضای مجازی تغییراتی را در مفهوم سنتی پلیس ایجاد کرده است. برای همین پلیس امروز و آینده بیشتر و بیشتر به فضای مجازی می‌پردازند، پلیس

- 1 . YouTube
- 2 . uploads

و ارائه‌دهندگان امنیت جامعه نیاز به تثبیت حضور خود در شبکه اجتماعی مجازی دارند تا قادر به محافظت از افراد، اشخاص حقوقی و منافع ملی باشند (سدربرگ، ۲۰۱۵). در کشور ما به طور کلی سیاست‌های متفاوتی در قبال شبکه‌های اجتماعی مجازی اتخاذ شده است. برخی از آنها فیلتر شدند و برخی دیگر همچنان مجاز به استفاده هستند. سؤالی که این مقاله تلاش دارد به آن پاسخ دهد این است که شبکه اجتماعی مجازی چه فرصت‌ها و چالش‌هایی را برای پلیس ایجاد می‌کند؟

### شبکه‌های اجتماعی مجازی به عنوان فرصت برای پلیس

تجربه‌های جهانی پلیس بسیاری از کشورها، از جمله مطالعه روی ۲۲ افسر ارشد پلیس از ۱۶ کشور در سراسر جهان و مصاحبه با ۱۷ مرکز خدمات پلیس از استرالیا، کانادا، دانمارک، انگلستان، ولز، فنلاند، آلمان، هند، ایرلند، ایتالیا، نروژ، پرتغال، اسکاتلند، اسلواکی، اسپانیا و ایالات متحده آمریکا نشان داده است که پلیس می‌تواند از شبکه‌های مجازی به عنوان فرصت استفاده کند (اکسنچر، ۲۰۱۳). این فرصت‌ها عبارت‌اند از:

#### ۱. تعامل و درگیر شدن پلیس در شبکه‌های مجازی

شبکه‌های اجتماعی مجازی توسط پلیس مورد شناسایی قرار می‌گیرند. برای تعامل و همچنین مشارکت پلیس در اجتماع و یافتن راه‌حل برای کاهش جرم نیز شبکه‌های اجتماعی ضروری تلقی می‌شوند (برلت، ۲۰۱۲: ۳۰-۴۰). رئیس اداره امور عمومی آف‌بی‌آی ضمن تقویت قوانین برای حضور پلیس در شبکه‌های اجتماعی مجازی، آن را گامی مهم برای ارتباط پلیس با اجتماع می‌داند (بی‌شرر، ۲۰۱۶: ۱-۱۳). یکی از مفروضات تئوری شبکه اجتماعی این است که دانش و اطلاعات در یک فرایند رابطه‌ای و شبکه‌ای ساخته می‌شوند (دان، ۱۹۸۳: ۴۵۱-۴۶۳). در حقیقت نوع اطلاعاتی که به وسیله شبکه تولید می‌شود به نوع شبکه وابسته است. برای مثال دانش فنی مالی از حضور و یادگیری در شبکه اجتماعی مالی به دست می‌آید. بر اساس این مفروضات، حضور پلیس در شبکه‌های اجتماعی مجازی موجب اشکال جدیدی از دانش علمی پلیس خواهد شد که بدون ارتباط با آن میسر نیست. مقولات و الگوهای ارتباطی

با نوع شبکه‌های مجازی نوع جدیدی از دانش را برای پلیس تولید خواهد کرد. علاوه بر این، چنین ارتباطی به تبادل معنادار اطلاعات بین پلیس و اجتماع در شبکه‌های مجازی خواهد انجامید. حضور پلیس در شبکه‌های اجتماعی مجازی بر دانش آنها درباره علایق و نگرانی‌های اجتماع می‌افزاید (ولمن، ۱۹۹۷: ۲۰۵-۱۷۹). تنها در این صورت پلیس می‌تواند انواع تخلفات و جرایم و آسیب‌های متفاوت در شبکه‌های مجازی را شناسایی کند و این مهم‌ترین گام پلیس در حال و آینده باید باشد.

خدمات پلیس در فضای مجازی از طریق طیف وسیعی از تماس و تعامل با شهروندان در اجتماع جدید، امکان می‌یابد. البته باید توجه کرد اعتماد اعضای اجتماع به پلیس، اصلی اساسی در این وضعیت است. در خصوص نحوه تعامل (ناشناس بودن و حضور با مشخصات واقعی) بحث‌های زیادی وجود دارد که خارج از این مقاله است. باید در اجتماع سنجش انجام گیرد که کدام‌یک از شیوه‌ها کارایی بیشتری دارد و اعتماد اعضای اجتماع را به خود جلب می‌کند.

## ۲. افزایش اعتماد عمومی از طریق شبکه‌های مجازی

استفاده بالقوه دیگر، بهبود تصور شهروندان از پلیس است. افزایش تعامل با مردم به خصوص مردمی که در آینده بیشتر امورات خود را در فضای مجازی انجام می‌دهند، ممکن است اعتماد عمومی نسبت به پلیس را افزایش دهد. فضای مجازی کمک خواهد کرد تا پلیس خود را به یک پلیس شهروند یا مردم‌محور تبدیل کند (ادلین، ۲۰۱۶: ۱۷۳). مطالعات نشان داده است ارتباط پلیس و مردم همان‌گونه که در فضای واقعی احساس آرامش را به ساکنان منتقل می‌کند، در شبکه‌های اجتماعی مجازی نیز موجب افزایش اعتماد خواهد شد. همان‌گونه که لوری<sup>۱</sup> مشاور شبکه اجتماعی پلیس آمریکا، تأکید می‌کند: اعتماد با حضور پلیس در مردم، به اشتراک‌گذاری اطلاعات، نه فقط نگه داشتن اطلاعات و داشتن یک مکالمه و درگیر شدن مردم ساخته می‌شود.

### ۳. ایجاد و به‌روزرسانی هشدارهای پلیسی

پلیس‌های دنیا از طریق شبکه‌های مجازی در پی اطلاع‌رسانی عمومی هستند و در آینده به عنوان یک الگوی ارتباطی و نیز یکی از کانال‌های اطلاع‌رسانی مهم پلیس به مردم خواهند بود (ولد و دیگران، ۲۰۱۵: ۱۶-۴). به اشتراک‌گذاری اطلاعات و هشدارهای پلیسی از جمله فرصت‌های مهم شبکه‌های مجازی برای پلیس است.

برای مثال پلیس فتا در خصوص امنیت در شبکه تلگرام پیام می‌دهد: «هیچ‌گاه کدهای تأییدی را که از طرف تلگرام یا هر برنامه دیگری برایتان ارسال می‌شود در اختیار کسی حتی نزدیکانتان قرار ندهید، چون این کدهای تأیید، کلید راهیابی به حریم خصوصی شما هستند.»<sup>۱</sup>

### ۴. شبکه‌های اجتماعی مجازی برای کشف جرم

رسانه‌های اجتماعی ممکن است در مبارزه با جرم مهم تلقی شوند. بسیاری از مجرمان و کسانی که ایجاد رعب و وحشت می‌کنند، از رسانه‌های اجتماعی برای لاف زدن و به رخ کشیدن جنایاتی که مرتکب شده‌اند، استفاده می‌کنند. در این صورت پلیس هوشمندانه از افسران کارآگاه با استفاده از رسانه‌های اجتماعی برای تشخیص جرم و جنایت با مجرمین و برخورد با آنها استفاده خواهد کرد.

### ۵. جمع‌آوری گزارش

تجربه‌های استفاده از شبکه‌های اجتماعی مجازی نشان داده است که مردم از این طریق وضعیت امنیتی محل خود و آنچه را در حال اتفاق است، به پلیس گزارش می‌کنند (فوغ، ۲۰۱۵: ۲).

### ۶. نظارت بر رفتارهای پلیس

با انتشار ویدئوی ضبط شده مردم از پلیس در شبکه‌های اجتماعی مجازی امروزه چنین ویدئوهایی می‌تواند منبع مهمی برای نظارت عملکرد پلیس از سوی شهروندان باشد.

۷. خوانش رفتاری و درک چالش‌های آتی اجتماع و اقدام پیشگیرانه و مقابله با آن استفاده پلیس از اشکال متفاوت شبکه‌های اجتماعی مجازی فرصتی فراهم می‌کند تا اداره پلیس سنجشی از درک، نگرش و رفتار مردم داشته باشد و چالش پیش رو و زمینه بحران‌های آشکار و پنهان را بیابد و به سرعت عمل خود برای ایجاد نظم اجتماعی عمومی بیفزاید (پروکتر و همکاران، ۲۰۱۳: ۴۱۳).

#### ۸. بهینه‌سازی راهکارها<sup>۱</sup>

دیجیتالی شدن پاسگاه‌ها و کلانتری‌های پلیس و ایجاد یا بهینه‌سازی زیرساختارهای مربوط ضرورتی اجتناب‌ناپذیر در حال و آینده خواهد بود. این مسئله در کشورهای توسعه‌یافته موجب کاهش هزینه‌های خدمات پلیس و افزایش سرعت و کارایی سازمان پلیس شده است. حتی برخی کشورها به کمک شبکه‌های مجازی خدمات جدیدی به خصوص در حوزه مدیریت تقاضا ارائه داده‌اند. این مسئله نه تنها موجب صرفه‌جویی در هزینه‌های پلیس می‌شود، بلکه کمک می‌کند مأمور پلیس قابل مشاهده و قابل دسترس در قلب جامعه باشد.

#### ۹. پیش‌بینی و بهبود خدمات<sup>۲</sup>

در آینده نزدیک از طریق شبکه‌های اجتماعی موبایلی، ترافیک شهری مورد تجزیه و تحلیل قرار خواهد گرفت و شهروندان و پلیس می‌توانند از آن به عنوان مدیریت ترافیک استفاده کنند.

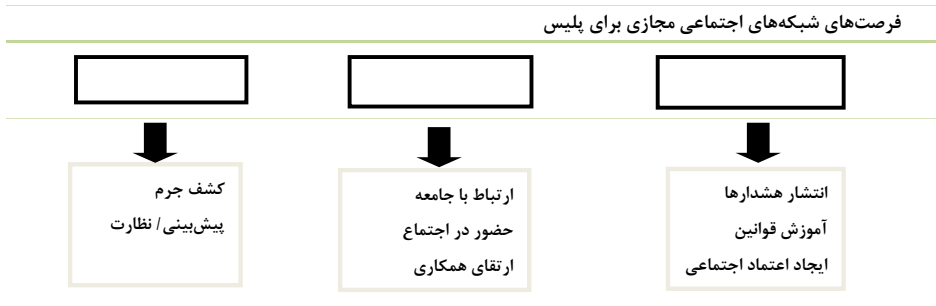
#### ۱۰. ارتقای همکاری<sup>۳</sup>

پلیس برای ارائه بهتر خدمات خود نیاز به همکاری در سطح ملی و بین‌المللی با سایر نیروهای پلیس، قوه قضاییه و سازمان‌های بخش دولتی، بخش خصوصی، سازمان‌های داوطلبانه و شهروندان خود دارد. پلیس می‌تواند برای ارائه خدمات سریع‌تر و پاسخگو، به اشتراک‌گذاری اطلاعات و منابع دیگر برای مقابله با جرم و جنایت با دادن هزینه کمتر به طور مؤثرتری عمل کند.

- 1 . Optimize Ways of Working
- 2 . Predict and Improve Services Through Analytics
- 3 . Enhance Collaboration



با توجه به مطالب یادشده می‌توانیم فرصت‌های شبکه‌های اجتماعی مجازی برای پلیس را به سه بخش زیر تقسیم کنیم و خلاصه آن را در مدل زیر ببینیم.

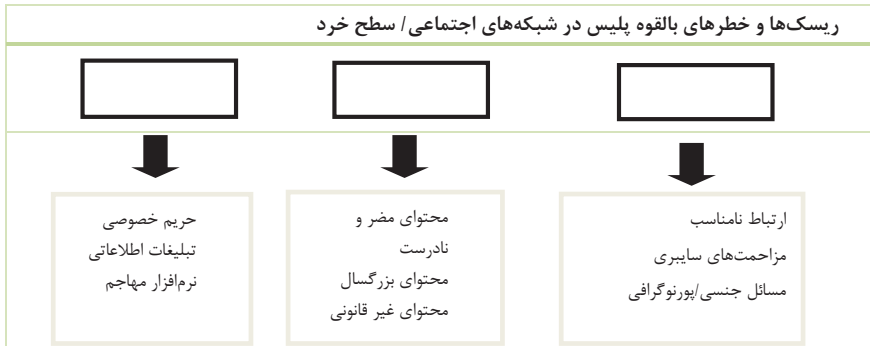


### چالش‌های پیش روی پلیس در ارتباط با شبکه‌های اجتماعی مجازی

پلیس با شکل‌ها و سطوح مختلفی از چالش‌ها روبه‌روست. برخی از انحرافات و جرایم سنتی که در گذشته وجود داشته‌اند در فضای مجازی تسهیل شده‌اند و برخی از انحرافات جدید با شکل‌گیری فضای مجازی پدید آمده‌اند (نات و تیلور، ۲۰۰۵: ۹۳). برای مثال اینترنت ممکن است ابزار مناسبی برای ارتباط میان قاچاقچیان کالا باشد. علاوه بر این اینترنت و فضای مجازی جدید فرصتی نوین برای رفتارهای انحرافی و مخاطره‌آمیز فراهم می‌آورد (وال، ۲۰۰۱: ۳). در کنار آن مطالعات آینده‌پژوهی شبکه‌های اجتماعی مجازی قرار دارند که پلیس باید به خطرهای ناشی از آن توجه جدی کند. حمله‌های سایبری، نفوذ در زیرساخت‌های اطلاعاتی حساس، تقلب یا سرقت اطلاعات از جمله تهدیدهای مهم آینده به شمار می‌روند. ریسک‌ها و خطرهای بالقوه‌ای که پلیس در شبکه‌های اجتماعی با آنها روبه‌روست، به دو سطح خرد و کلان تقسیم می‌شوند.

#### ۱. چالش‌های بالقوه پلیس در شبکه‌های اجتماعی مجازی در سطح خرد

ریسک‌ها و خطرهای بالقوه‌ای را که پلیس در شبکه‌های اجتماعی / سطح خرد با آنها روبه‌روست می‌توان به سه دسته ارتباطی، محتوایی و مالی تقسیم کرد:



### الف) پورنوگرافی<sup>۱</sup>

انحرافات جنسی و پورنوگرافی صنعتی سه بیلیون دلاری با چهار و نیم میلیون وب سایت شامل محتوای پورنوگرافی است که ۲۵ درصد از کل جست‌وجوهای اینترنتی جهان را به خود اختصاص داده است (کوپین، ۲۰۰۵: ۱۹۲). به همین علت قربانی شدن بچه‌ها و محافظت از آنها از خطرهای استفاده از شبکه‌های اجتماعی مجازی، بسیار جدی مورد توجه والدین، جامعه‌شناسان، جرم‌شناسان و پلیس بوده است (مک کیب، ۲۰۰۸: ۲۴۷). به نظر می‌رسد این نوع از انحرافات، تهدیدی عظیم برای همه جهانیان به خصوص برای کشورهایی است که ساخت جمعیتی جوان (مثل کشور ما) دارند.

در میان انواع انحرافات جنسی در اینترنت سوءاستفاده جنسی از کودکان در اینترنت یکی از تهدیدهای مهم اخلاقی در جهان محسوب می‌شود. بین جامعه‌شناسان این توافق وجود دارد که فضای مجازی اینترنت باعث شده است که سوءاستفاده کنندگان در ارتباطی وسیع‌تر و در شبکه سریع‌تری عمل کنند (Beech, Elliott, Birgden, & Findlater, 2008; Durkin, (Durkin and Colleagues, 2006: 599; Forsyth Quinn, 2006

طبق یک بررسی در کشور، ۶۲ درصد کاربران اینترنت اظهار داشته‌اند که به طور مرتب به سایت‌های پورنوگرافی سر می‌زنند و اضافه کرده‌اند که برخی اوقات دچار برانگیختگی جنسی نیز می‌شوند. طبق این تحقیق، این افراد به طور متوسط در طول یک هفته ۴ ساعت را به گشت و گذار در سایت‌های غیراخلاقی بزرگسالان می‌گذرانند (یوسفی، ۱۳۸۶: ۱۴).

1 . Pnography

2 . McCabe

بسیاری از خانواده‌ها برای اینکه فرزندان‌شان از آسیب‌های موجود در جامعه در امان بمانند آنها را با کامپیوتر و اینترنت در خانه و اتاق‌هایشان تنها می‌گذارند، غافل از اینکه ممکن است فرزندان‌شان با آسیب‌های به مراتب خطرناک‌تری در فضای مجازی روبه‌رو یا قربانی دام‌های به مراتب بزرگ‌تر و پلیدتری شوند.

### ب) آسیب‌های امنیتی

اینترنت و فضای مجازی محیط امنی برای جاسوسان و کسانی که امنیت فردی و جمعی را تهدید می‌کنند، شناخته شده است. در حال حاضر روزی نیست که خبری از سرقت اطلاعات محرمانه اشخاص حقیقی و حقوقی یا خالی شدن حساب‌های بانکی مشتریان بانک‌ها منتشر نشود. مسلماً اینترنت بهترین منبع برای جاسوسی از شرکت‌های عظیم تجاری به شمار می‌رود. به همین علت متخصصان مسائل امنیتی به شرکت‌های بزرگ اقتصادی و چند ملیتی در جهان هشدار داده‌اند تا بر امکانات دفاعی شبکه‌های خود برای مقابله با اقدامات خرابکارانه و سازمان‌یافته بیفزایند.

### ج) هک<sup>۱</sup>

به هرگونه نفوذ در یک سیستم امنیتی شبکه کامپیوتری هک گفته می‌شود که این نفوذ می‌تواند تنها ورود به سیستم اطلاعاتی بدون تغییر دادن آن باشد یا بخشی از اطلاعات را تغییر دهد و حتی آنها را نابود سازد. هکرها می‌توانند با توجه به انگیزه‌ها و دامنه نفوذ، کل مدیریت وب سایت یا سیستم شبکه کامپیوتری و به طور کلی اطلاعات قربانی را در دست گیرند و او را با مشکل اساسی روبه‌رو کنند. هک کردن یکی از انحرافات و جرایم کامپیوتری است. افرادی که دارای دانش و اطلاعات کامپیوتری و شبکه‌های اینترنتی هستند و سیستم‌ها و زبان‌های برنامه‌نویسی را می‌دانند، ممکن است درصدد آزار و اذیت دیگران برآیند. هولینگر<sup>۲</sup> چندین نوع انحراف را با عنوان هک تبیین کرده است: به دست آوردن پسورد دیگران، استفاده بدون مجوز از اکانت کامپیوتر دیگران، دریافت بدون مجوز فایل از کامپیوتر دیگران، کپی کردن بدون مجوز فایل‌های دیگران، تغییر بدون مجوز فایل دیگران، آسیب رساندن به

1 . Hacking

2 . Hollinger

برنامه‌ها و نرم‌افزارهای دیگران، طراحی در آسیب رساندن نرم‌افزاری و سخت‌افزاری سیستم دیگران، دریافت کد و مجوز و نرم‌افزار دیگران برای استفاده غیرقانونی برای کاربران دیگر (هولینگر، ۱۹۸۸: ۱۹۹).

ویروس ملیسا اولین ویروس رایانه‌ای است که دیوید اسمیت ایجاد کرد و از طریق اینترنت انتقال پیدا کرده و خسارات فراوانی در سراسر جهان به بار آورده است. اسمیت مدت کوتاهی پس از گسترش این ویروس دستگیر و به دلیل به بار آوردن خسارتی حدود ۸۰ میلیون دلار محکوم به زندان شد.

تایلور و جردن اجتماع هکرها را با شش ویژگی یا ابعاد توصیف کرده‌اند: جنبه تکنولوژیکی، نهانکاری<sup>۱</sup>، گمنامی<sup>۲</sup>، سیال بودن<sup>۳</sup> و عضویت. اغلب هکرها مرد هستند و انگیزه‌های هکرها نیز متفاوت است (تایلور و جردن، ۱۹۹۸: ۷۵۷). هکرها معمولاً هویت واقعی خود را پنهان می‌کنند و از اسامی مستعار بهره می‌گیرند. بعضی از آنها دارای انگیزه‌های ماجراجویی هستند و از این کار لذت می‌برند و گاهی نیز بدان افتخار می‌کنند. آنها معمولاً آدم‌های باهوشی هستند که با داشتن اطلاعات وسیع در خصوص شبکه‌های اینترنتی به خصوص سیستم‌های امنیتی آن دست به چنین کاری می‌زنند.

#### د) انحرافات و جرایم مالی

از انحرافات و جرایمی دیگر که در شبکه‌های اجتماعی مجازی در دنیا شایع است به مسائل مالی مربوط می‌شود. دیو توماس<sup>۴</sup>، رئیس کامپیوتر بخش سایبر افبی‌آی، بزرگ‌ترین حوزه نگرانی خود را حمله و نفوذ به بخش مالی و تجارت الکترونیک می‌داند، زیرا این کار بیشترین تأثیر را هم از حیث مالی و هم از حیث اعتباری بر اجتماع می‌گذارد.

#### ه) پخش ویروس

یکی دیگر از انحرافات مهم در فضای مجازی پخش ویروس‌های اینترنتی است. افراد منحرف یا مجرم با فرستادن ویروس‌ها می‌توانند وارد حریم خصوصی افراد شوند.

- 
- 1 . Secrecy
  - 2 . Anonymity
  - 3 . Fluidity
  - 4 . Dave Thomas
-

## و) جاسوسی

امروزه بسیاری از کشورها از شبکه‌های اجتماعی مجازی به عنوان ابزاری مهم برای جاسوسی استفاده می‌کنند. برای نمونه آمریکایی‌ها پیش از اینکه به عراق حمله کنند، از طریق شبکه‌های مجازی اطلاعات بسیار زیادی درباره مردم عراق کسب کرده بودند. امروزه سازمان‌های جاسوسی دنیا بسیاری از افراد کشورهای مختلف به خصوص جوانان بیکار را برای جمع‌آوری اطلاعات از کشورشان رسماً استخدام می‌کنند. آنها معمولاً با ترغیب و تشکیل اجتماع‌های متعدد سیاسی مجازی، وبلاگ‌نویسی، فروم، چت‌روم و یوزنت سعی در جهت‌دهی افکار و انتشار شایعه دارند و خبرهای تحریف‌شده و نافرمانی‌های مدنی را هدایت می‌کنند و در نهایت تلاش برای براندازی و چالش‌های سیاسی دارند.

## ۲. چالش‌های بالقوه پلیس در شبکه‌های اجتماعی مجازی در سطح کلان

ریسک‌ها و خطرهای بالقوه‌ای را که پلیس در شبکه‌های اجتماعی در سطح کلان با آنها روبه‌روست، می‌توان به سه دسته اجتماع/ فرهنگ، اقتصاد و سیاست به طور کلی تقسیم کرد. شاید گفته شود برخی از موارد یادشده جزو مأموریت‌های مستقیم پلیس نیستند، اما تأثیر آنها به گونه‌ای است که در نهایت حال و آینده به پلیس مرتبط می‌شود.



## الف) آسیب‌های هویتی و انزوای اجتماعی

دو دهه پیش (۱۹۸۴) که شری تارکل مفهوم «خود دوم» را برای کامپیوتر ابداع کرد، کنش متقابل بین فرد و کامپیوتر اتفاق افتاد؛ اما امروز با گسترش روزافزون شبکه‌های اینترنتی و خلق فضای مجازی میلیون‌ها نفر در ارتباط قرار گرفتند (تارکل، ۱۹۹۹). دنیای مجازی،

عناصر زندگی آن‌لاین و تأثیرات آن بر هویت، امروزه در حوزه مطالعات جامعه‌شناسی نوین قرار گرفته است. اینترنت این فرصت را به افراد می‌دهد که با هویت‌های جدید در اجتماعات متعدد حضور یابند. ویژگی‌های منحصر به فرد اینترنت از جمله آزادی آن حتی بسیاری از جنبه‌های واقعی و تغییرناپذیر هویت افراد از جمله سن، نژاد، قومیت و جنسیت را به چالش کشیده است. هویت ابعاد متعددی یافت. انسان‌های متفاوت در فضاهای متعدد با هویت‌های متعدد از ویژگی‌های دنیای جدید است. طبیعی است بی‌هویتی با ظهور شبکه‌های وسیع‌تر و هویت متنوع و نامشخص‌تر فرصت بی‌نظیری برای انحرافات و آسیب‌های اجتماعی در فضای مجازی و فضای واقعی فراهم می‌آورد (روگرز و همکاران، ۲۰۰۶: ۲۴۶).

این مسئله خود باعث انزوای اجتماعی می‌شود و فرد از حضور فعال در عرصه‌های اجتماعی جهان واقعی باز می‌ماند. مطالعات جامعه‌شناسی متعددی نشان داده است که تعامل در دنیای مجازی به دلیل ویژگی‌های خاص آن باعث کاهش اندازه دایره اجتماعی افراد و افزایش افسردگی و تنهایی آنها می‌شود. برای جامعه ما که حضور در عرصه‌ها و فعالیت‌های اجتماعی یک ضرورت است، انحراف بسیار ظریف و پنهان از دیده‌ها معمول می‌گردد. بسیاری از تحقیقات تجربی نشان داده‌اند که اینترنت تأثیر منفی روی اجتماع داشته است. مطالعات طولی کروت<sup>۱</sup> و همکارانش روی ۱۶۹ نفر در ۷۳ خانواده در پیتزبورگ<sup>۲</sup> و پنسیلوانیا<sup>۳</sup> در سال ۱۹۹۸ بر نتایج منفی اینترنت بر شبکه اجتماعی تأکید می‌کند. آنها در مطالعات خود نشان داده‌اند که استفاده از اینترنت باعث کاهش ارتباط بین اعضای خانواده و همچنین باعث کاهش سایز دایره شبکه اجتماعی افراد در جامعه می‌شود که سرانجام به افزایش افسردگی و تنهایی افراد می‌انجامد (کروت و دیگران، ۱۹۹۸: ۱۰۱۷). کروت و همکارانش مجدداً در تحقیقات خود در سال ۲۰۰۱ به نتایج مشابهی دست یافتند (کروت و دیگران، ۲۰۰۲: ۴۹). گروه مرکز مطالعات کمی جامعه در دانشگاه استنفورد<sup>۴</sup> به سرپرستی نای<sup>۵</sup> در نمونه‌ای روی ۴۱۱۳ نفر از ۲۶۸۹ خانوار در بررسی‌های خود نشان داده‌اند که اینترنت باعث کاهش شبکه روابط اجتماعی افراد و کاهش تماس افراد با دوستان و خانواده می‌شود (نای، ۲۰۰۱: ۴۲۳).

- 1 . Kraut
- 2 . Pittsburgh
- 3 . Pennsylvania
- 4 . Stanford Institute for the Quantitative Study of Society (SIQSS)
- 5 . Nie

در تحقیق دیگری که فرزن در سال‌های ۱۹۹۸ و ۲۰۰۱ روی ۸۴۳ خانواده در سوئیس انجام داد، مشخص شد تماس بیشتر افراد با اینترنت باعث کاهش ارتباط با خانواده و دوستان می‌شود (فرزن، ۲۰۰۳: ۴۲۳).

#### ب) اعتیاد اینترنتی

نوع دیگری از آسیب و انحراف اجتماعی ناشی از حضور در شبکه‌های مجازی به ماهیت خود این تکنولوژی و استفاده از آن مربوط می‌شود. به عبارت دیگر خود شبکه‌های مجازی به دلیل ویژگی خاص خود سبب آسیب‌های جدیدی در این حوزه می‌شوند که آسیب‌های مدرن به شمار می‌آیند. استفاده غیرضرور و دائمی، نوعی عادت کاذب و اعتیاد اینترنتی را به وجود می‌آورد که فرد همواره دوست دارد خود را با اینترنت سرگرم کند. اعتیاد به اینترنت یک اختلال فیزیولوژیک- روانی نیز به حساب می‌آید که دارای نشانه‌هایی از قبیل جدایی، اختلالات عاطفی و ازهم‌گسستگی در ارتباطات اجتماعی است.

همانند تمامی انواع دیگر اعتیاد، اعتیاد به اینترنت نیز با علایمی همچون اضطراب، افسردگی، کج خلقی، بیقراری، تفکرهای وسواسی، کناره‌گیری، اختلالات عاطفی و ازهم‌گسستگی روابط اجتماعی همراه است. روابط اجتماعی افراد مبتلا به اعتیاد اینترنتی در جهان مجازی افزایش پیدا می‌کند. مطالعه آقای درگاهی و همکاران او درباره مشکل اعتیاد به اینترنت و ویژگی‌های رفتاری، شخصیتی و جمعیتی کاربران به روش مقطعی روی ۷۳۲ نفر از کاربران اینترنت در سنین ۳۹-۱۵ سال در منطقه ۲ غرب تهران نشان داده است که ۳۰ درصد کاربران، به اینترنت اعتیاد داشتند و درجات مختلفی از اختلالات اجتماعی و رفتاری نظیر احساس بیگانگی با خود، احساس ضعف و ناتوانی در انجام امور، رفتار ناهنجار اجتماعی، اجتماع‌گریزی، درون‌گرایی و رفتار احساسی میان کاربران اینترنت مشاهده شده است. این مطالعه نشان داده است که اعتیاد به اینترنت در گروه سنی ۱۹-۱۵ سال در مقایسه با سایر گروه‌های سنی بیشتر و چندین برابر است. بین اعتیاد به اینترنت در کاربران، با احساس بیگانگی از خود و ابعاد آن و همچنین با ویژگی‌های شخصیتی رابطه معنی‌داری وجود داشته است. در کاربرانی که اعتیاد شدید داشته‌اند، استفاده از گفت‌وگوی اینترنتی سه برابر کاربران معمولی بوده است (درگاهی، ۱۳۸۶: ۲۶۵).

### جرایم شایع اینترنتی

همان گونه که گفته شد، برابر گزارش سازمان‌های امنیتی، کارکنان نیروی انتظامی جمهوری اسلامی ایران علاوه بر اینکه همانند عموم مردم در معرض جرایم اینترنتی هستند، به دلیل جایگاه و اهمیت آن در ارکان و ساختار نظام، همواره به عنوان گروه هدف سرویس‌های جاسوسی و باندهای تبهکار در فضای مجازی بوده و افراد شاغل در آن به علت جایگاه شغلی و تأثیرگذاری در جامعه و دسترسی به اطلاعات مهم و طبقه‌بندی‌دار، مورد توجه هستند که در نتیجه به صورت پنهان یا آشکار در مسیر ارتکاب جرم از طریق فضای سایبر قرار می‌گیرند. البته روش‌های این موضوع با توجه به دگرذیسی مستمر فناوری‌های فضای سایبر، متناسب با زمان در حال تغییر است (یادگاری و همکاران، ۱۳۹۴: ۵۶).

### تروریسم اینترنتی

یکی از انحرافات و آسیب‌های نوین در فضای اینترنت، تروریسم است. در جهان امروز بمب‌های مجازی و الکترونیکی بسیار مخرب‌کننده‌تر و ویران‌کننده‌تر از بمب‌های واقعی به نظر می‌رسند. آنها بردهای نامحدودی دارند و می‌توانند یکباره سیستم‌های دولتی و سازمانی را با تهدیدی جدی روبه‌رو کنند. به نظر می‌رسد جدیدترین چالش و رویارویی کشورها در مقابل هم جنگ‌های اینترنتی یا سایبری<sup>۱</sup> یا جنگ شبکه‌ای<sup>۲</sup> باشد. امروزه اینترنت صحنه‌های درگیری جدیدتری را برای کشورهای درگیر گشوده است. این شکل از جنگ ممکن است تاکتیک‌ها و فناوری‌های متنوعی را برای فرماندهی و کنترل (شامل جمع‌آوری اطلاعات، پردازش و توزیع، تثبیت موقعیت، شناسایی دوست یا دشمن یا فریب دادن و انحراف افراد) دربرگیرد. ایجاد مناقشه و درگیری در سطح بزرگ میان ملت‌ها و جوامع، تلاش برای مختل کردن یا صدمه زدن، تلاش برای تغییر افکار عمومی، نخبگان یا دیپلماسی، تبلیغات و کمپین‌های روانی، سیاسی و فرهنگی خرابکاری، فریب یا تداخل با رسانه‌های محلی، نفوذ در شبکه‌های کامپیوتری و پایگاه‌های داده و همچنین حمایت از جنبش‌های مخالف در سراسر شبکه‌های کامپیوتری از جمله این مسائل محسوب می‌شوند.

---

1 . Cyberwar  
2 . Netwar



## آینده‌نگاری شبکه‌های مجازی

با توجه به سیر دگرذیسی اینترنت و وضعیت آن در آینده، روش‌های شایع پنهان و آشکار جرایم جاسوسی و سازمان‌یافته از طریق اینترنت و از طرفی کیس پژوهی جرایم شایع اینترنتی، می‌توان آینده‌نگاری جرایم سایبری را برابر شکل زیر ارائه کرد:

### آینده‌نگاری شبکه‌های مجازی

نسل	سال	نگاری آینده
نسل ۱	سال‌های ۱۹۹۳-۲۰۰۰	جاسوسی و برقراری ارتباط با بیگانگان و مخالفان نظام از طریق ایمیل ایجاد وب سایت و بروشور و کاتالوگ الکترونیکی برای عملیات روانی، موضوعات اخلاقی و...
نسل ۲	سال‌های ۲۰۰۰-۲۰۰۸	افشای اطلاعات طبقه‌بندی‌شده مثل فیلم، صوت و متن از طریق ایجاد وبلاگ و صفحات اجتماعی و اشتراک‌گذاری اطلاعات ایجاد صفحات اجتماعی، وبلاگ و... به منظور بهره‌برداری‌های غیراخلاقی، سیاسی، مذهبی و... ایجاد صفحات جعلی، اقدامات نفوذ، هک و... به منظور جرایم مالی عضویت، بسط و گسترش شبکه‌های تجارت الکترونیکی غیرمجاز (شبکه‌های هرمی)، کلاهبرداری سایبری و... افشای اطلاعات طبقه‌بندی‌شده از طریق ویکی‌ها (دانشنامه‌های آزاد اینترنتی) ایجاد اجتماعات مجازی در قالب مباحث سیاسی، اعتقادی، اخلاقی و...
نسل ۳	سال‌های ۲۰۰۸-۲۰۱۲	افشای اطلاعات و جاسوسی ناخواسته به واسطه جست‌وجو از طریق موتورهای جست‌وجو مثل گوگل کنونی، به کاربران برای یافتن اطلاعات کمک می‌کند، در خرید و کار آنها را یاری می‌دهد و چیزی را که در حاشیه‌ها وجود دارد ظاهر می‌کند و البته از این طریق هویت، شغل، وابستگی‌ها، علایق و اطلاعات و... را به دست می‌آورد. افشای اطلاعات و جاسوسی ناخواسته به واسطه حضور در وب، وبلاگ، شبکه‌های اجتماعی و... با توجه به تغییر نسل Web2.0 به Web3.0 یا وب معناگرا و تحلیلی و هوشمند افشای اطلاعات و جاسوسی ناخواسته به واسطه حضور در جهان‌های مجازی مثل زندگی دوم (Second Life) و...

<p>افشای اطلاعات سازمانی و جاسوسی ناخواسته از طریق شرکت در بازی‌های سینمایی آن‌لاین و تغییر هویت</p> <p>افشای اطلاعات و جاسوسی از طریق اینترنت اشیا (اینترنت کلیه تجهیزات الکترونیکی به اینترنت و ...)</p> <p>افشای اطلاعات مکانی، زمانی، بیولوژیکی و... به صورت ناخواسته از طریق هوش مکان‌محور به واسطه استفاده از سیستم‌های الکترونیکی، تکنولوژی قابل پوشیدن و...</p> <p>استفاده گسترده از ربات‌های هوش مصنوعی، پردازش صوت، تکنولوژی‌های اشاره و حرکت و... برای جاسوسی و افشای اطلاعات و...</p>	<p>سال‌های ۲۰۲۰-۲۰۱۲</p>	<p>نسل ۴</p>
<p>ظهور جو دیجیتال و ایجاد هوش مصنوعی برای جاسوسی و افشای اطلاعات به صورت ناخواسته</p> <p>جاسوسی و افشای اطلاعات به صورت ناخواسته در تعامل و همگرایی انسان و تکنولوژی</p> <p>روباتیک، مغز مصنوعی و...</p> <p>جاسوسی و افشای اطلاعات ناخواسته از طریق کنترل امواج مغز انسان</p> <p>ناهنجاری رفتاری به واسطه ترکیب انسان و آواتارهای مجازی مثل خالکوبی یک فیلم روی پوست انسان و به واقعیت پیوستن انسان‌های رؤیایی در شخصیت‌سازی و...</p>	<p>سال‌های ۲۰۲۰ تا ...</p>	<p>نسل ۵</p>

هرچند موارد یادشده برای تمامی افراد جامعه قابل تصور است، اما به واسطه حساسیت و دسترسی پلیس به اطلاعات مهم و طبقه‌بندی‌شده سازمانی، گسترش راهکارهای پنهان و آشکار سایبری برای افشا، سرقت و جاسوسی اطلاعات و... علیه پلیس بسیار برجسته است و می‌تواند تبعات فراوانی در حوزه‌های امنیتی داشته باشد. برای مثال عضویت کارکنان در شبکه‌های اجتماعی و تشکیل گروه‌های مختلف و تبادل افکار، نظریات و اطلاعات، بسیار متفاوت با مردم عادی است و حتی می‌تواند در امنیت ملی چالش‌هایی ایجاد کند که البته مبسوق به سابقه نیز هست (یادگاری و همکاران، ۱۳۹۴: ۶۳-۶۲).

### نتیجه‌گیری

این بررسی نشان داده است که به گسترش شبکه‌های مجازی باید نگاهی واقع‌بینانه داشت؛ پلیس هم می‌تواند از فرصت‌های آن استفاده کند و هم باید از چالش‌های آن آگاهی یابد تا بتواند امنیت شهروندان را تأمین کند. فیلتر کردن و جلوگیری از دسترسی و عدم استفاده از

تکنولوژی شبکه‌های مجازی به امنیت اجتماع ما کمکی نمی‌کند؛ بنابراین، اقدامات پیشگیرانه و مصونیت‌ساز بهترین گزینه برای محافظت، نظارت و کنترل در فضای مجازی است. برای این کار توانمندسازی<sup>۱</sup> افسران پلیس به خصوص کسانی که در حوزه شبکه‌های اجتماعی فعال هستند از یک سو و آموزش همگانی و توانمندسازی کاربران شبکه‌های اجتماعی مجازی از سوی دیگر، امری مهم برای کاهش ناامنی‌ها و افزایش امنیت در جامعه است.

ماهیت در حال تغییر جهان جنایی و امنیت در شبکه‌های اجتماعی مجازی امری پیچیده است. امروز پلیس ما با مجرمانی روبه‌روست که به آخرین فناوری مجهز و با آن آشنا هستند. با توجه به اهمیت این مسئله، برای درک بهتر چگونگی مقابله با چالش‌ها، ایجاد مرکز مطالعه شبکه‌های اجتماعی مجازی و به کارگیری متخصصین، جامعه‌شناسان و مهندسان شبکه برای شناسایی و پیش‌بینی تهدیدها و ارائه هشدارهای مرتبط با آن برای سازمان پلیس امری ضروری است.

### منابع فارسی

- اولسون، دیوید (۱۳۷۷)، رسانه‌ها و نمادها: صورت‌های بیان ارتباط و آموزش، ترجمه تجربه مهاجر، تهران: سروش.
- درگاهی حسین و سیدمنصور رضوی (۱۳۸۶)، «اعتیاد به اینترنت و عوامل مؤثر بر آن در ساکنان منطقه ۲ غرب تهران»، پایش، تابستان، ۶ (۳): ۲۶۵-۲۷۲.
- رزاقی، نادر (۱۳۸۹)، «شناخت آسیب‌ها و جرایم اجتماعی در فضای مجازی»، مجموعه مقالات همایش بررسی آسیب‌های اجتماعی، بابلسر: انتشارات دانشگاه مازندران.
- رزاقی، نادر (۱۳۹۰)، «اعتیاد اینترنتی»، مجموعه مقالات همایش بررسی آسیب‌های نوپدید، انتشارات دانشگاه آزاد اسلامی بابل.
- صادقی فسائی، سهیلا و شهریار محمدی (۱۳۸۷)، «نگاهی جرم‌شناسانه بر جرایم، امنیت و کنترل در اینترنت»، در اینترنت و آسیب‌های اجتماعی، ویراسته مسعود کوثری، تهران، نشر سلمان.
- عبداللهیان حمید (۱۳۸۴)، «نوع‌شناسی و بازتعریف آسیب‌های اینترنتی و تغییرات هویتی در ایران»، فصلنامه ایرانی مطالعات فرهنگی و ارتباطات، ش ۳، بهار و تابستان.

- کاستلز، مانوئل (۱۳۸۰)، عصر اطلاعات: اقتصاد، جامعه و فرهنگ، (جلد اول)، ظهور جامعه شبکه‌ای، ترجمه علی پایا، تهران: طرح نو.
- گیدنز، آنتونی (۱۳۷۳)، جامعه‌شناسی، ترجمه منوچهر صبوری، تهران: نشر نی.
- لنسکی گرهارد و جین لنسکی (۱۳۶۹)، سیر جوامع بشری، ترجمه ناصر موفقیان، تهران: سازمان انتشارات و آموزش انقلاب اسلامی.
- یادگاری، وحید و همکاران (۱۳۹۴)، «آینده‌پژوهشی جرایم سایبری علیه کارکنان ناجا»، فصلنامه مطالعات حفاظت و امنیت انتظامی، س ۱۰، ش ۳۵، تابستان.
- یوسفی، علی و حسین اکبری (۱۳۹۰)، «تأملی جامعه‌شناختی در تشخیص و تعیین اولویت مسائل اجتماعی ایران»، مسائل اجتماعی ایران، ۱: ۲۲۳-۱۹۵.

#### منابع لاتین

- Accenture (2013), "Preparing Police Services for the Future [internet]", Dublin: Accenture, Available from <https://www.accenture.com/us-en/insight-preparing-police-service-future-six-steps-toward-transformation> [Accessed 1 January 2017]
- Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012), "The Impact of Polices on Government Social Media Usage: Issues, Challenges, and Recommendations", *Government Information Quarterly*, 29(1), 30-40.
- Beshears, M. L. (2016), "Effectiveness of Police Social Media Use", *American Journal of Criminal Justice*, 1-13.
- Cederberg, Aapo (2015), "Future Challenges in Cyberspace, Geneva Center for Security Policy", GCSP Policy Paper.
- Dunn, W. N. (1983), "Social Network Theory", *Science Communication*, 4(3), 453-461.
- Edlins, M. (2016), "Pursuing the Promises of Social Media? Changes in Adoption and Usage of Social Media by the top 10 US Police Departments", *Information Polity*, (Preprint), 1-18.
- Franzen, Axel (2003), "Social Capital and the Internet: Evidence from Swiss Panel Data", *Kyklos* 56.
- Hollinger, Richard C. (1988), "Computer Hackers Follow a Guttman-like

Progression”, *Sociology and Social Research*, Vol. 72 No. 3, April.

- Janice, Denegri -Knott and Jacqui Taylor (2005), “The Labeling Game: A Conceptual Exploration of Deviance on the Internet”, *Social Science Computer Review*, 23; 93.

- Joinson, A. N. (2005), “Deviance and the Internet: New Challenges for Social Science”, *Social Science Computer Review*, 23(1), 5–7.

- Kraut R, Kiesler S, Boneva B, Cummings J, Helgeson V, Crawford A. (2002), “Internet Paradox Revisited”, *Journal of Social Issues*, Vol.58.

- Kraut, Robert, Patterson Michael, Lundmark Vicki, Kiesler Sara, Mukopadhyay Tridas, Scherlis William (1998), “Internet Paradox: A Social Technology that Reduces Social Involvement and Psychological Well-Being?”, *American Psychological Association*, Vol. 53(9).

- McCabe, Kimberly A. (2008), “The Role of Internet Service Providers in Cases of Child Pornography and Child Prostitution”, *Social Science Computer Review*, Vol. 26, No. 2.

- Mesch, G. S. (2009), “Social Bonds and Internet Pornographic Exposure among Adolescents”, *Journal of Adolescence*, 32, 601-618.

- Nie NH. (2001), “Sociability, Interpersonal Relations, and the Internet Reconciling Conflicting Findings”, *American Behavioural Scientist* 45.

- Philippsohn, S. (2001), “Trends in Cybercrime: An Overview of Current Financial Crime on the Internet”, *Computers & Security*, 20.

- Procter, R., Crump, J., Karstedt, S., Voss, A., & Cantijoch, M. (2013), “Reading the Riots: What Were the Police Doing on Twitter?”, *Policing and Society*, 23(4).

- Quinn, J. F. & Forsyth, C. J. (2005), “Describing Sexual Behavior in the Era of the Internet: A Typology for Empirical Research”, *Deviant Behavior*, 26.

- Rogers, M., Smoak, N., & Liu, J. (2006), “Self-reported Deviant Computer Behavior”, *Deviant Behavior*, 27(3).

- Scholes-Fogg, Tom (2015), “Police and Social Media”, Written Evidence to the Independent Police Commission.

Taylor, Paul and Jordan Time (1998), “A Sociology of Hackers”, *The Sociological Review*, Vol. 46, No. 4.

- Turkle, S. (1999), "Cyberspace and Identity", *Contemporary Sociology*.
- Van De Velde, B., Meijer, A., & Homburg, V. (2015), "Police Message Diffusion on Twitter: Analysing the Reach of Social Media Communications", *Behaviour & Information Technology*, 34(1).
- Wall, David S. (2001), *Cybercrimes and the Internet in Edited Book: Crime and The Internet*, Routledge: London and New York.
- Warren, Peter and Michael Streeter (2005), *Cyber Alert, How the World is Under Attack from a New form of Crime*, Publisher: Sheena Dewan, London, UK.
- Wellman, B. (1997), "An Electronic Group is Virtually a Social Network", In S. Kiesler (Ed.), *Culture of the Internet*, Mahwah, NJ: Lawrence Erlbaum.
- Yaman, Akdeniz (2001), "Controlling Illegal and Harmful Content on the Internet", In Edited Book: *Crime and The Internet*, Routledge: London and New York.

