بررسی جامعه‌شناختی بزه‌دیدگی ناشی ازآزاررسانی سایبری در میان دانشجویان دانشگاه مازندران

اکبر علیوردی‌نیا،* فائزه قربان زاده سیاهکلرودی**

چکیده

بررسی تحقیقات در نقاط مختلف دنیا نشان می‌دهدکه بزه‌دیدگی (قربانی‌شدن) ناشی از فعالیت درفضای سایبر یکی از مشکلاتی است که در بسیاری از جوامع رواج دارد. در کشور ایران نیز این پدیده با گسترش استفاده از اینترنت و شبکه‌های ارتباطی مجازی، در حال گسترش است. پژوهش حاضر می‌کوشد در پرتو نظریهٔ فعالیت‌های روزمره و سنجش رفتارهای آنلاین، بزه‌دیدگی ناشی از فعالیت درفضای سایبر را در میان دانشجویان بررسی و تبیین کند. این تحقیق با روش پیمایش و با نمونهٔ آماری ۳۷۴ نفری (۲۲۶ دختر و ۱۴۸ پسر) از دانشجویان دانشگاه مازندران در سال تحصیلی ۹۷- ۱۳۹۶ به اجرا در آمده است. طبق نتایج تحقیق، سه متغیر سبک زندگی منحرفان آنلاین، محافظت آنلاین (به‌طور مستقیم) و مجاورت آنلاین با متخلفان (به‌طور معکوس) تأثیر معناداری بر بزه‌دیدگی ناشی از آزاررسانی سایبری داشته‌اند. همچنین، احتمال بیشتری وجود دارد که دانشجویان پسر قربانی این نوع بزه‌دیدگی شوند. به‌لحاظ ابعاد بزه‌دیدگی ناشی از آزاررسانی سایبری دختران بیش از پسرها قربانی بزه‌دیدگی مالی و جنسی می‌شوند. در مجموع متغیرهای مبتنی بر فعالیت‌های روزمره، بعد آبرویی این بزه‌دیدگی بیشتر از ابعاد مالی و جنسی آن تبیین می‌کند. این تحقیق نشان داد که نظریهٔ فعالیت‌های روزمره، قابلیت به‌کار گرفته‌شدن در تبیین بزه‌دیدگی ناشی از مزاحمت‌های سایبری در میان دانشجویان را دارد.

کلیدواژه‌ها: نظریهٔ فعالیت‌های روزمره، سایبرآزاری، قربانی‌شدن، جذابیت هدف آنلاین، محافظت آنلاین.

* استاد جامعه‌شناسی دانشگاه مازندران (نویسندهٔ مسئول) aliverdinia@umz.ac.ir

** کارشناس ارشد جامعه‌شناسی دانشگاه مازندران f.ghorbanzadee@gmail.com

تاریخ دریافت: ۱۳۹۷/۰۶/۱۰ تاریخ پذیرش:۱۳۹۸/۰۳/۰۸

مسائل اجتماعی ایران، سال دهم، شمارهٔ ۱، بهار و تابستان ۱۳۹۸، صص ۱۴۵- ۱۶۹

۱. مقدمه

افزایش استفاده از اینترنت بر تعداد موارد آزاررسانی مجازی یا بزه دیدگی ناشی از آزاررسانی سایبری[1] و تهدید و اذیت‌های آنلاین تأثیر داشته است (پالت و همکاران، ۲۰۰۹:۶۴۰). در جامعهٔ شبکه‌ای امروز، سوءاستفاده از رفتار آنلاین می‌تواند موجب آسیب جدی از جمله ناراحتی‌های عاطفی شدید، محروم‌شدن از اشتغال، و حتی خشونت فیزیکی یا مرگ گردد (لیپتون، ۲۰۱۱: ۱۱۰۵). همچنین شبکه‌های اینترنتی با وجود تعداد زیاد کاربران و منبع تقریباً بی‌پایان از بزه‌دیدگان[2] بالقوه محل جدیدی را برای فعالیت‌های مجرمانه مانند سایبرآزاری ایجاد می‌کند (رینز و همکاران، ۲۰۱۱: ۱۱۴۹). با توجه به تعداد زیاد کاربران و تهدید بیش از حد بزه دیدگی آنلاین، حریم خصوصی به یک موضوع امنیتی عمده برای سایت های شبکه های اجتماعی و کاربران آنلاین تبدیل شده است. (هنسون و همکاران، ۲۰۱۱: ۲۵۴). به استناد گزارش پلیس فتا، ۶۹ هزار و ۷۲۹ حملهٔ سایبری در طول سال ۹۴ اتفاق افتاده است که ۹۸۹ مورد به سایت‌های دولتی و ۶۸ هزار و ۷۴۰ مورد به سایت‌های غیردولتی مربوط است، همچنین متوسط سنی مجرمان اینترنتی در کشور ۱۸ تا ۲۵سال است. رئیس پلیس فتا از افزایش ۲۴ درصدی جرایم در مقایسه با سال گذشته در همین حوزه خبر داد و گفت در حوزهٔ مزاحمت‌های اینترنتی ۱۹ درصد افزایش و در انتشار فیلم‌های خصوصی ۹۰ درصد افزایش را داشته‌ایم. در بحث هتک حیثیت و نشر اکاذیب ۷۹ درصد افزایش و انتشار فیلم‌های خصوصی ۹۰ درصد افزایش نسبت به مدت مشابه سال ۹۳ داشته‌ایم (خبرگزاری مهر، ۱۸ اسفند ۱۳۹۴).

رایانه می‌تواند به عنوان ابزاری برای انواع فعالیت‌ها از جمله جرایم مالی، فروش غیرقانونی مقالات، هرزه‌نگاری، قماربازی، کلاهبرداری از طریق ایمیل[3]، جعل اسناد[4]، هتک حرمت سایبری[5]و سایبر آزاری استفاده شود (داشورا، ۲۴۳:۲۰۱۱). در واقع، آزارسایبری یا آزار به کمک تکنولوژی، استفاده از ارتباطات الکترونیک یا فناوری‌های ردیابی برای تعقیب متوالی اشخاص دیگر جهت القای ترس به آنهاست (هنسلر، ۲۰۰۸:۱). به عبارت دیگر، سایبرآزاری عبارت است از آزار مکرر یک فرد با استفاده از ابزارهای الکترونیکی یا اینترنتی. رایا آزاران می‌توانند از ابزارهای الکترونیکی نظیر دوربین‌ها، دستگاه‌های شنود، برنامه‌های کامپیوتری سیستم موقعیت‌یابی جهانی برای کنترل بزه‌دیدگان خود استفاده کنند (رینز و همکاران، ۲۰۱۱: ۱۱۵۳). مزاحمت‌های سایبری، استفاده از ایمیل، اتاق‌های گفت‌وگو، یا ارسال تصاویر و پیام‌هایی از طریق تلفن همراه

1. Cyber Stalking
2. Victims
3. E-Mail Spoofing
4. Forgery
5. Cyber Defamation

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

و ابزارهای آنلاین برای تحقیرکردن و ترساندن دیگران و همین‌طور برای ایجاد احساس درماندگی در افراد است (دیلماک و آیدوگان،۲۰۱۰:۱۶۶۷). آزاررسانی سایبری نیز به همان شیوه‌ای که قلدری برای بزه‌دیدگان در دنیای واقعی ناراحتی به وجود می‌آورد، باعث پریشانی و یا ترس می‌شود (بوسل و همکاران، ۲۰۱۲:۵۰۲). این نوع آسیب رسانی می‌تواند شامل پیام‌های تهدیدآمیز و یا ارسال تصاویر جنسی از طریق ایمیل و سرویس پیام‌های فوری باشد. نتایج این آزار و اذیت برای بزه‌دیدگان به‌لحاظ شدت می‌تواند از یک آزار و اذیت کوچک تا استرس شدید احساسی و عاطفی تجربه‌شده توسط بزه‌دیدگان متفاوت باشد (آدینگتون، ۲۰۱۳، بوسلر و همکاران، ۲۰۱۱).

تشریح فرصت‌های ایجادشده برای سایبرآزاری و همچنین کاربرد و آزمون نظریهٔ فعالیت‌های روزمرهٔ زندگی[1]، از کانون‌های متمرکز در زمینهٔ شناخت بزه‌دیدگان است. در سال‌های اخیر، دیدگاه‌های نظری به تعدادی از جرایم همانند تجاوز جنسی[2]، جرایم مالی و شکل‌های دیگر آزاررسانی سایبری اشاره کرده‌اند (رینز و همکاران، ۲۰۱۱:۱۱۴۹). دانشجویان به دلیل آنکه برای انجام کارهای تحقیقاتی خود بیشتر از اینترنت و کامپیوتر استفاده می‌کنند و بیشتر در فضای سایبری سر می‌کنند، ممکن است بیشتر در معرض آسیب‌های اینترنتی و آزار واذیت‌های سایبری قرار گیرند (ریچاو و سکنیک، ۲۰۱۵:۷۸). این تحقیق در پی پاسخگویی به این سؤال است که «چگونه می‌توان در پرتو نظریهٔ فعالیت‌های روزمره، آزاررسانی سایبری را در میان دانشجویان دختر و پسر دانشگاه مازندران تبیین کرد؟»

پیشینهٔ تجربی

در خارج از کشور، تحقیقات و مطالعات نسبتاً زیادی در زمینهٔ سایبر آزاری در میان دانشجویان صورت گرفته است. در این قبیل مطالعات نظریهٔ فعالیت روزمره به عنوان چارچوب نظری پژوهش کمتر مورد توجه قرارگرفته است. به‌لحاظ چارچوب نظری، تحقیقات چوی (۲۰۰۸)، ویلسم (۲۰۰۹)، باسلر و هالت (۲۰۰۹)، کندی و تیلور (۲۰۱۰)، مارکوم و همکاران (۲۰۱۰)، نگو و پترنوستر (۲۰۱۱)، جرالدز (۲۰۱۱)، دربینگ و همکاران (۲۰۱۴)، لوکفلد و یار (۲۰۱۶) و رینز و همکاران (۲۰۱۱) از نظریهٔ فعالیت‌های روزمره برای تبیین مسئله استفاده کرده‌اند. بر اساس یافته های این پژوهش ها، احتمال بزه‌دیدگی برای کسانی که به غریبه‌ها اجازهٔ دسترسی به اطلاعات آنلاین خود را می‌دهند، دو برابر بیشتر از کسانی است که این اجازه را به غریبه‌ها نمی‌دهند. به‌طور کلی نتایج این مطالعات از نظریهٔ فعالیت‌های روزمره برای تبیین بزه‌دیدگی ناشی از آزاررسانی سایبری حمایت می‌کند. استفاده از داده‌های طولی در تحقیقات خارجی از ویژگی‌های

1. Routine Activities Theory
2. Sexual Assault

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

مهم تحقیقات اخیر است که یافته‌های قابل‌توجهی در مورد پیش بینی بزه‌دیدگی به دست می‌دهد و نتایج پژوهش را قابل استناد می‌کند. مرور نتایج تحقیقات پیشین در مورد بزه‌دیدگی در ایران واقعیت‌های تلخی را درخصوص گسترش روزافزون آن بازگو می‌کند. در میان تحقیقات داخلی در زمینهٔ بزه‌دیدگی ناشی از آزاررسانی سایبری، برای نمونه، پژوهش‌های مالمیر و زررخ(۱۳۸۹)، میر (۱۳۹۴) و اسلامی (۱۳۹۵) قابل توجه است. بررسی‌های انجام‌گرفته حاکی از آن است که با توجه به رشد و افزایش شیوع و استفاده از اینترنت، جرایم سایبری و به تبع آن بزه‌دیدگی ناشی از آزاررسانی سایبری که حاصل مزاحمت‌های سایبری است افزایش یافته است و مطالعهٔ آن موضوع جدیدی است. علی‌رغم پژوهش‌های گسترده در خارج از کشور در خصوص بزه‌دیدگی ناشی از آزاررسانی سایبری، تنها زررخ (۱۳۹۰) در داخل کشور با توجه به نظریهٔ به‌کاررفته در تحقیق حاضر به تبیین آزاررسانی سایبری پرداخته است. به نظر می‌رسد که در ایران تحقیقی به بررسی جامعه‌شناختی بزه‌دیدگی ناشی از آزاررسانی سایبری با استفاده از نظریهٔ فعالیت‌های روزمره نپرداخته است. تحقیقات موجود اغلب از منظر حقوقی و قانونی‌اند و به بررسی جرایم رایانه‌ای و انواع و اقسام آن پرداخته‌اند و به مطالعه نقش و جایگاه بزه‌دیده از دیدگاه جامعه‌شناختی پرداخته نشده‌است.

۲. چارچوب نظری

چارچوب نظری تحقیق حاضر براساس نظریهٔ فعالیت‌های روزمره که توسط کوهن و فلسون در سال ۱۹۷۹ توسعه یافت، شکل گرفته است. کوهن و فلسون نظریهٔ فعالیت‌های روزمرهٔ بزه‌دیدگان را با الهام‌گرفتن از دیدگاه‌های طرح‌شده در نظریهٔ انتخاب عقلانی که با نام نظریهٔ کنش عقلانی[1] مشهور است و چارچوبی برای فهم و مدل‌سازی رفتارهای اجتماعی و اقتصادی به شمار می‌آید مطرح کردند (میلر و همکاران، ۲۰۰۶: ۸۱). برخلاف اکثر نظریه‌های جریان اصلی جرم‌شناسی، نظریهٔ فعالیت‌های روزمره سعی در تبیین آن دارد که چرا احتمال بیشتری دارد جرم بر برخی از افراد تأثیر بگذارد و در موقعیت‌های خاص رخ دهد (جرالدز، ۲۰۱۱: ۸). به‌طور عمده، نظریهٔ فعالیت‌های روزمره یک رویکرد اکولوژیکی به علیت جرم و جنایت است، و به همین ترتیب تمرکز مکانی (و زمانی) افراد، اهداف و فعالیت‌ها پیش‌فرض اصلی از طرح تبیینی آن است (یار، ۲۰۰۵: ۴۱۴). ارتباط میان جرم و مکان از دیرباز تاکنون مورد علاقهٔ جرم‌شناسان بوده است. زمانی که دو نظریهٔ سبک زندگی و نظریهٔ فعالیت‌های روزمره ارائه شدند، فضای مجازی که امروزه ما آن را به خوبی می‌شناسیم وجود نداشت و تنها برخورد فیزیکی بین مجرمان و بزه‌دیدگان از شروط لازم در ایجاد فرصتی مناسب برای ارتکاب جرم در نظر گرفته می‌شد؛ اگرچه، در فضای سایبری

1. Rational Action Theory

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

این‌گونه نیست؛ بزه‌دیدگان بالقوه و مجرمان بدون هیچ ارتباطی در مکان فیزیکی مشترک کنار هم می‌آیند (رینز، ۱۱۵۲:۲۰۱۱). تأکید اصلی این نظریه روی تلاقی بین متخلفان باانگیزه و اهداف مناسب (بزه‌دیدگان) در نبود یک نگهبان تواناست که به ایجاد فرصت برای بزه‌دیدگی می‌انجامد.

متغیرهای اصلی نظریهٔ فعالیت‌های روزمره عبارت است از: ۱- جذابیت هدف آنلاین[1] (هدف مناسب) ۲- محافظت آنلاین[2] ۳- متخلفان انگیزه‌دار[3] که در ادامه به اختصار به توضیح آنها پرداخته‌ایم.

۱- جذابیت هدف آنلاین (هدف مناسب)، خود دارای چهار جزء است:

ارزش[4]: بیشتر اهداف جرایم سایبری از نوع اطلاعاتی هستند. مسلم است که تمام اشخاصی که در فضای مجازی وجود دارند و اقداماتی که انجام می‌دهند اشکالی از نوع برنامه‌های دیجیتالی هستند. اهداف اولیه از این نوع عبارت‌اند از: «خصوصیات ذهنی» مانند موسیقی، عکس‌های متحرک، تصاویر، نرم افزارهای رایانه‌ای، اسرار تجاری و دولتی و غیره (وبستر، ۲۰۰۲: ۱۴- ۱۲). هدف ممکن است فردی باشد که مورد سوءاستفاده قرار گرفته و یا اعضای یک گروه ممکن است در معرض بزه‌دیدگی مشابهی به دلیل ویژگی‌های مشترک اجتماعی، قومی، مذهبی، جنسی و غیره قرار گیرند. هدف ممکن است یک محصول غیرقانونی باشد که برای لذت یا سود معامله شده‌است (مانند پورنوگرافی کودکان). به‌طور کلی ما می‌توانیم نتیجه‌گیری کنیم که اهداف جرایم سایبری، مانند جرایم زمینی بسیار گسترده هستند و ارزیابی‌های متفاوتی را جذب می‌کنند و این ارزیابی‌ها احتمالاً بر روی مناسب بودن هدف زمانی که از دیدگاه مجرم بالقوه نگریسته می‌شود، تأثیر می‌گذارد (یار، ۲۰۰۵: ۴۱۹).

اینرسی[5] (سکون): این اصطلاح در مورد خواص فیزیکی اشیا یا افراد به کار می‌رود که در مقابل تعرض، درجات مختلفی از مقاومت را از خود نشان می‌دهند. به‌طور مثال، یک شیء بزرگ و سنگین را تقریباً به‌سختی می‌توان جابه‌جا کرد و به یک شخص دارای هیکلی تنومند و سنگین وزن تقریباً به‌سختی می‌توان تعرض کرد (فلسون،۵۷:۱۹۹۸). با این حال، تأمل بیشتر نشان می‌دهد که حتی محصولات اطلاعاتی خصوصیات جبری را تا حدی حفظ می‌کنند. نخست آنکه، حجم اطلاعات (نظیر اندازهٔ فایل) بر روی توان انتقال هدف تأثیر می‌گذارد و هر کسی که به دشواری اسناد پرحجم را با استفاده از تماس تلفنی استخراج کرده باشد با این امر آشنایی دارد.

1. Online Target Attractiveness
2. Online Guardianship
3. Motivated Offenders
4. Value
5. Inertia

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

دوم، ویژگی فنی ابزارها (سیستم رایانه‌ای) که توسط سارق اطلاعات استفاده می‌شود، محدودیت‌هایی را برای مناسب‌بودن اهداف اطلاعاتی اعمال می‌کند، به‌عنوان مثال سرقت موفق مستلزم این است که رایانه‌ای که به کار می‌رود، ظرفیت ذخیرهٔ کارآمد (نظیر فضای هارد درایو یا ابزارهای دیگر) داشته باشد که بتوان هدف را در آن ذخیره کرد. بنابراین، اگرچه اهداف اطلاعاتی مقاومت جبری تقریباً کمی ایجاد می‌کنند، اما بی‌وزن بودن[1] آنها مسئلهٔ مطلقی نیست (یار، ۲۰۱۱: ۴۲۰).

قابل‌رؤیت بودن[2]: نظریهٔ فعالیت‌های روزمره رابطهٔ مثبت میان قابل‌رؤیت بودن و مناسب‌بودن هدف را بدیهی فرض می‌کند: «متخلف احتمالی باید از وجود هدف خبر داشته باشد» (بنت، ۱۹۹۱: ۱۴۸). اموال و افرادی که بیشتر قابل دید هستند، احتمال هدف قرارگرفتن آنها بیشتر است.

قابلیت دسترسی[3]: این اصطلاح در مورد توانایی یک متخلف در دستیابی به هدف و سپس گریختن از صحنهٔ جرم به کار می‌رود (فلسون، ۱۹۹۸: ۵۸). در اینجا نیز هرچه هدف بیشتر در دسترس باشد، مناسب‌بودن آن افزایش می‌یابد و برعکس.

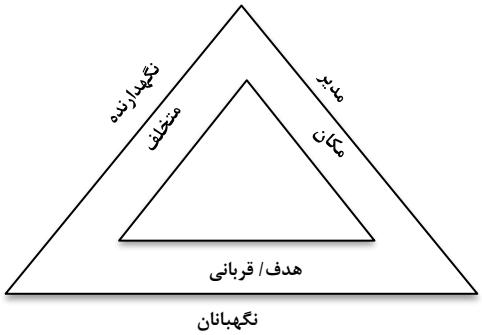
۲- محافظت توانمند آنلاین:

محافظت به «توانایی اشخاص برای جلوگیری از وقوع جرم» اشاره دارد (تسلونی و همکاران، ۲۰۰۴: ۷۴). محافظت به‌طور کلی به سه نوع، محافظت شخصی، محافظت اجتماعی و محافظت فیزیکی تقسیم می‌شود. محافظت شخصی، دانش فنی و آگاهی از مخاطرات آنلاین بزه‌دیدگان بالقوه ممکن است تعیین‌کنندهٔ دسترسی پیداکردن به آنها باشد. کاربران با درجات بالای دانش فنی و یا کسانی که از خطراتی که به‌صورت آنلاین با آنها مواجه هستند آگاهی دارند، بیشتر قادر به پیش‌بینی‌کردن حملات هستند و بنابراین برای تبدیل‌شدن به یک قربانی در خطر کمتری قرار دارند (لوکفلد و یار، ۲۰۱۶: ۲۷۰). علاوه بر چنین «محافظان اجتماعی»، این نظریه همچنین اقدامات امنیتی فیزیکی، مواردی همچون موانع، قفل‌ها، هشدارها و روشنایی خیابان‌ها و داخل خانه را نگهبانی تأثیرگذار تلقی می‌کند (تسلونی و همکاران، ۲۰۰۴: ۷۴). علاوه بر اینچنین محافظان اجتماعی، فضای مجازی با محافظت «فیزیکی» یا تکنولوژیکی، یعنی عوامل خودکاری که به‌صورت مداوم محافظت می‌کنند، تکمیل شده‌است. این گستره «دیوارهای آتش[4]»، سیستم‌های ردیابی و نرم‌افزارهای اسکن ویروس را شامل می‌شود (دنینگ، ۱۹۹۹: ۳۵۲) این سه

1. Weightless
2. Visibility
3. Accessibility
4. Firewall

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

فرضیه یعنی وجود اهداف مناسب، نبود محافظان توانا و حضور متخلف انگیزه‌دار اغلب با عنوان"مثلث جرم" شناخته می‌شود (میلر، ۲۰۰۹:۲۸۰) شکل این مثلث در زیر آمده است.



مثلث درونی بیانگر عناصر لازم برای جرم است: متخلف با انگیزه و هدف مناسب باید در زمان و مکان واحدی قرار بگیرند. مثلث بیرونی بیانگرکنترل‌کننده‌های بالقوه یعنی نگهبانان، نگهدارندگان و مدیران است. برای آنکه جرم صورت گیرد، این عوامل باید غایب و یا بی‌تأثیر باشند. حضور یک کنترل‌کنندۀ کارآمد، از وقوع جرم می‌تواند جلوگیری کند. کنترل‌کنندگان، کسانی که نزدیک‌ترین ارتباط را با متخلفان بالقوه، اهداف، مکان‌ها دارند، به احتمال بیشتری موفق به کنترل و جلوگیری از جرم می‌شوند (میلر، ۲۰۰۹:۲۸۰).

نگهدارنده[1]: منظور از نگهدارندگان، افرادی هستند که در مقابل مجرمان بالقوه، کنترل اجتماعی غیررسمی را اعمال می‌کنند تا از وقوع جرم پیشگیری کنند. در واقع، نگهدارندگان اشخاصی هستند که رابطۀ احساسی با متخلف دارند که ممکن است خانواده، دوستان، مذهب و ... باشد (میلر، ۲۰۰۹: ۲۸۰).

مدیر[2]: در نهایت مدیران، مکان‌های خاصی را مشاهده و نظارت می‌کنند، مانند صاحب مغازه‌ای که دوربین‌های نظارتی نصب می‌کند (میلر، ۲۰۰۹:۲۸۰).

۳- متخلفان انگیزه‌دار:

افراد و گروه‌هایی هستند که هم تمایل و هم توانایی ارتکاب جرم را به دلایل مختلف دارند . این انگیزه ممکن است به دلایل مختلفی در فرد به وجود آمده باشد. برای مثال ممکن است در شخص بیکار، معتاد به مواد مخدر یا کسی که برای زنده‌ماندن و گذران زندگی به پول نیاز دارد، دلایل اقتصادی موجب تخلف شود. در یک نوجوان و یا مصرف‌کنندۀ مواد ممکن است دلایل فیزیکی (مادی) منجر به تخلف شود (علیوردی‌نیا و علیمردانی، ۱۳۹۵).

1. Handler
2. Manager

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

تأمل نظری سیستماتیک دربارهٔ توانایی نظریهٔ فعالیت‌های روزمره برای تبیین الگوهای جرایم سایبری توسط یار(۲۰۰۵) ارائه شده‌است. او ابتدا، با در نظر گرفتن هریک از عناصر اصلی مدل نظریهٔ فعالیت‌های روزمره از وضعیت‌های جرم‌زا (متخلفان باانگیزه، اهداف مناسب و فقدان محافظان توانا) آغاز می‌کند و آنها را به‌لحاظ کارایی در محیط‌های آنلاین بررسی می‌کند؛ باتوجه به آنکه به نظر می‌رسد کلاهبرداران مختلف، هکرها، سرقت‌های ادبی و غیره در محیط‌های آنلاین کم نباشند. به همین‌سان، اهداف مناسب متعددی همچون داده‌های اختصاصی، اطلاعات شخصی، پرداخت آنلاین و خدمات خرید و همچنین سیستم‌های رایانه‌ای که ممکن است با نفوذ غیرمجاز به خطر افتاده باشند برای شکار وجود دارند. بدین ترتیب، محافظان توانا ممکن است انواع مختلفی داشته باشند، از جمله مسئولان شبکه، مدیران، کاربران، همآلان و همچنین طیفی از حفاظت‌های خودکار مانند دیوارهای آتش، شبکه‌های خصوصی مجازی، نرم‌افزارهای آنتی‌ویروس و ضدنفوذ شناسایی هویت و دسترسی به سیستم‌های مدیریت (یار، ۲۰۰۵). برخی از محققان از نظریه‌های فعالیت‌های روزمره و سبک زندگی برای تبیین جرایم اینترنتی استفاده کرده‌اند (اسمیت، ۲۰۱۰؛ یار، ۲۰۰۵).

یار دو روش متمایز که فضای سایبر را به دنیای واقعی متصل می‌کند، پیشنهاد می‌کند. او به استناد کاستلز[1] (۲۰۰۲)، ادعا می‌کند که فضای سایبر خود در اجتماع جهان فیزیکی، اقتصاد و روابط سیاسی ریشه دارد و محیط‌های مجازی، از قبیل وب‌سایت‌ها یا سیستم‌های ایمیل، که اکثراً در کشورهای توسعه‌یافتهٔ جهان زمینی[2] تولید شده‌اند، فضای مجازی را بازتابی از روابط اقتصادی موجود و سلسله‌مراتب آن می‌سازد. به عنوان مثال بسیاری از وب‌سایت‌هایی که توسط ۸۳ درصد از کاربران اینترنت مشاهده شده‌اند از ایالات متحده آغاز شده‌اند (یوسدال، ۲۰۱۰: ۴۰). بنابراین، فضای سایبری می‌تواند به عنوان یک محلهٔ گسترده در مقیاس جهانی در نظر گرفته شود. ما می‌توانیم استدلال کنیم که هربار که یک فرد (مرد یا زن) به اینترنت متصل می‌شود، اوقاتش را در منطقه‌ای که نرخ جرمش بالاتر است، درست همانند جهان زمینی می‌گذراند و این او را تبدیل به هدف بالقوه می‌سازد. به هنگام تماس با متخلف با انگیزه یا اقدامات مجرم در غیاب محافظان توانمند، جرایم اینترنتی رخ می‌دهد. آنچه را که احتمال بزه‌دیدگی افرادی را که در محلهٔ مشابهی زندگی می‌کنند متفاوت می‌سازد، می‌توان با تفاوت‌های سبک زندگی افراد و فعالیت‌های روزمره‌شان تبیین کرد (یوسدال، ۲۰۱۰: ۴۳-۴۴).

1. Castells
2. Terrestrial World

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

فرضیه‌ها

- جذابیت هدف آنلاین با بزه‌دیدگی ناشی از آزاررسانی سایبری در میان دانشجویان رابطهٔ مثبت دارد.
- محافظت آنلاین با بزه‌دیدگی ناشی از آزاررسانی سایبری در میان دانشجویان رابطهٔ منفی دارد.
- در معرض دید متخلفان انگیزه‌دار قرارگرفتن با بزه‌دیدگی ناشی از آزاررسانی سایبری در میان دانشجویان رابطهٔ مثبت دارد.
- در مجاورت آنلاین با متخلفان انگیزه‌دار قرارگرفتن با بزه‌دیدگی ناشی از آزاررسانی سایبری در میان دانشجویان رابطهٔ مثبت دارد.
- سبک زندگی منحرفان آنلاین با بزه‌دیدگی ناشی از آزاررسانی سایبری در میان دانشجویان رابطهٔ مثبت دارد.
- مشارکت در فعالیت‌های مخاطره‌آمیز آفلاین با بزه‌دیدگی ناشی از آزاررسانی سایبری در میان دانشجویان رابطهٔ مثبت دارد.

۳. روش‌شناسی

جمعیت تحقیق این پژوهش، همهٔ دانشجویان دانشگاه مازندران که در سال ۱۳۹۶-۱۳۹۷ مشغول تحصیل بوده‌اند، است که تعداد آنها بر اساس آمار به‌دست‌آمده از معاونت آموزشی این دانشگاه ۱۵۰۲۲ دانشجو (۹۲۰۹ دختر و ۵۸۱۳ پسر) است. حجم نمونهٔ تحقیق با خطای نمونه‌گیری ۵ درصد، ۴۰۰ نفر برآورد گردید (دواس، ۱۳۹۰: ۷۸). با توجه به احتمال مخدوش‌شدن پرسشنامه‌ها در اثر پاسخ‌ندادن، الگوی یکنواختی در پاسخ‌دهی، پاسخ‌های نامربوط، مفقودشدن پرسشنامه‌ها و غیره و برای جلوگیری از کاهش حجم نمونه، در مجموع ۴۲۰ پرسشنامه تکثیر و توزیع گردید. پس از کنار گذاشتن پرسشنامه‌های مخدوش، در نهایت ۳۷۴ پرسشنامه تجزیه و تحلیل شد. روش نمونه‌گیری در این تحقیق، روش نمونه‌گیری تصادفی طبقه‌ای متناسب با حجم بود که مطابق با آن، دانشگاه بر اساس دو مقولهٔ جنسیت و دانشکده طبقه‌بندی شد. در این تحقیق برای بررسی اعتبار ابزار سنجش، از روش اعتبار محتوا برای تمامی مقیاس‌های تحقیق و اعتبار سازهٔ نظری برای متغیر وابسته استفاده شد. در این شیوهٔ ارزیابی، سنجه برحسب مطابقت آن با انتظارات نظری صورت می‌گیرد (همان: ۶۴). نتایج این تحقیق حاکی از آن بود که میانگین بزه‌دیدگی ناشی از آزاررسانی سایبری در پسران و دختران متفاوت است. به این معنا که میانگین این نوع بزه‌دیدگی در پسران در مقایسه با میانگین آن در دختران به طرز معناداری بیشتر است. این یافته با نتایج تحقیقات متعدد پیشین خارجی باومن و همکاران (۲۰۱۳) مطابقت دارد.

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

بنابراین مقیاس متغیر وابستهٔ این پژوهش از اعتبار سازهٔ نظری برخوردار است. همچنین برای سنجش پایایی ابزار سنجش از ضریب آلفای کرونباخ استفاده شده‌است (جدول ۱).

جدول ۱. نتایج آلفای کرونباخ مقیاس‌های تحقیق

مقیاس‌ها	تعداد گویه	α
بزه‌دیدگی ناشی از آزاررسانی سایبری	۱۶	۰/۷۰
جذابیت هدف	۹	۰/۷۷
محافظت توانمند	۱۲	۰/۷۰
فعالیت‌های مخاطره‌آمیز آفلاین	۶	۰/۷۱
مجاورت آنلاین با متخلفان انگیزه‌دار	۵	۰/۶۶
فعالیت‌های منحرفان آنلاین	۷	۰/۵۷
در معرض دید متخلفان انگیزه‌دار قرارگرفتن	۴	۰/۳۳

مهم‌ترین سنجه‌های تحقیق نیز بدین شرح بودند:[۱]

- بزه‌دیدگی حاصل از آزاررسانی سایبری[۲]: این نوع بزه دیدگی زمانی اتفاق می‌افتد که افراد از طریق تکنولوژی رایانه و استفاده از شبکه‌های متصل به اینترنت مورد آزار و اذیت قرار می‌گیرند (رینز و همکاران، ۲۰۱۱: ۱۱۵۳). سایبر آزاری تعقیب مکرر افراد با استفاده از دستگاه‌های الکترونیکی یا وابسته به اینترنت است (رینز و همکاران، ۲۰۱۱: ۱۱۵۶). متغیر بزه‌دیدگی ناشی از آزاررسانی سایبری، در قالب شانزده گویه و سه بعد « مالی»، « جنسی» و « آبرویی» سنجش شده‌است. برای پاسخ‌های هر گویه از طیف دفعات تکرار پنج‌تایی «اصلاً، یک تا دو بار، سه تا پنج بار، شش تا هشت بار، نُه بار و بیشتر» استفاده گردید. نحوهٔ سنجش متغیر آزاررسانی سایبری بر مبنای سنجه پژوهش‌های پیشین بوده است (رینز و همکاران، ۲۰۱۱؛ لوکفلد و یار، ۲۰۱۶).

۱. نحوهٔ سنجش متغیرهای مستقل این تحقیق در قالب جداول گویه، در انتهای این مقاله به‌صورت پیوست گزارش شده‌است.

2. Cyber Stalking Victimization

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

جدول ۲. مقیاس سنجش بزه‌دیدگی ناشی از آزاررسانی سایبری

مقیاس	ابعاد (خُرده‌مقیاس‌ها)	گویه (تمام گویه‌ها دارای قید زمانی در دوازده ماه گذشته است)
بزه‌دیدگی ناشی از آزاررسانی سایبری	مالی	۱. پیام‌هایی مبنی بر مورد تهدید قرارگرفتن اموالم در فضای مجازی دریافت کرده‌ام. ۲. افراد دیگر برای خرید کالاها از نامم بدون اجازهٔ من استفاده کرده‌اند. ۳. بدون اطلاع من از حساب بانکی‌ام پول برداشت شده‌است. ۴. اشخاصی از نام کاربری و رمز عبورم برای ضرر مالی رساندن به من استفاده کرده‌اند.
	جنسی	۱. از طریق شبکه‌های اجتماعی پیشنهادات جنسی ناخواسته‌ای داشته‌ام. ۲. عکس‌ها و فیلم‌هایم بدون آگاهی من در وب‌سایت‌های پورنو منتشر شده‌است. ۳. شایعات و اطلاعات شرم‌آوری دربارهٔ من از طریق ایمیل، پیام‌های متنی، وبلاگ‌ها و غیره منتشر شده‌است. ۴. از طریق فضای مجازی برای برقراری رابطهٔ جنسی تهدید به خشونت فیزیکی شده‌ام. ۵. از طریق فضای مجازی جهت مجبورکردنم برای برقراری رابطهٔ جنسی از من اخاذی مالی شده‌است.
	آبرویی	۱. آبرو و حیثیتم توسط سخنان کذب و نادرست از بین رفته‌است. ۲. افرادی برای بدنام کردنم به جمع‌آوری اطلاعات نادرست در مورد من پرداخته‌اند. ۳. اطلاعات خصوصی من جمع‌آوری شده و بدون رضایت من افشا شده‌است. ۴. عکس‌ها و فیلم‌هایم بدون اطلاع خودم برای کسانی ارسال یا منتشر شده‌است. ۵. تصاویر و فیلم‌های واقعی خصوصی و خودمانی من در شبکه‌های اجتماعی بدون رضایت من منتشر شده‌است. ۶. تصاویر جعلی شرم‌آور از من ساخته شده و سپس در فضای مجازی منتشر شده‌است. ۷. دیگران از طریق ویرایش عکسم مرا مورد تمسخر قرار داده‌اند.

- جذابیت هدف آنلاین[1]: جذابیت هدف به‌عنوان «شرایط مطلوب مادی یا نمادین اشخاص یا اهداف مالی مجرمان بالقوه، همچنین فهمیدن ناکارآمدی یک هدف در برابر اقدام غیرقانونی» تعریف شده‌است (کوهن و همکاران،۱۹۸۱: ۵۰۸). در مورد بزه‌دیدگی آنلاین، اطلاعات خاص ممکن است تعقیب نمودن قربانی از سوی مجرمان را آسان‌تر سازد (به‌عنوان مثال، آدرس‌های

1. Online Target Attractiveness

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

پست الکترونیکی، پیام‌رسان‌های فوری) یا فرد را هدفی مطلوب‌تر بسازد (به‌عنوان مثال، ارسال کردن وضعیت رابطه، عکس‌ها، گرایش جنسی)، در نتیجه جذابیت فرد را به عنوان یک هدف افزایش می‌دهد (رینز و همکاران، ۲۰۱۱: ۱۱۵۹). برای سنجش و اندازه‌گیری مقیاس جذابیت هدف آنلاین از نُه گویه در قالب طیف لیکرت پنج‌تایی استفاده شده‌است. تدوین گویه‌های مربوط به جذابیت هدف آنلاین بر مبنای پژوهش‌های پیشین بوده است (رینز و همکاران، ۲۰۱۱).

- محافظت آنلاین[1]: محافظت به توانایی افراد یا اشیایی که از صدمه‌زدن یا حملهٔ مجرم باانگیزه به هدف جلوگیری می‌کنند، اشاره دارد (بوسلر و هالت، ۲۰۰۹: ۴۰۲). محافظت به اقدامات امنیتی اتخاذشده برای جلوگیری از بزه‌دیدگی اشاره دارد، افراد یا اشیایی که به‌واسطهٔ حضورشان یا از طریق اقدامی خاص از وقوع جرم جلوگیری می‌کنند (مک نیلی، ۲۰۱۵: ۳۴). مقیاس محافظت آنلاین، در قالب دوازده گویه، که مبتنی بر پژوهش‌های پیشین (رینز و همکاران، ۲۰۱۱؛ لوکفلد و یار، ۲۰۱۶) بود، مورد سنجش قرار گرفته‌است.

- متخلفان انگیزه‌دار[2]: متخلف انگیزه‌دار شخصی است که در صورت فراهم‌بودن فرصت به واسطهٔ نبود نگهبان و وجود هدف مناسب، تمایل به ارتکاب جرم دارد (مارکوم و همکاران، ۲۰۱۰: ۴۱۵). متخلفان انگیزه‌دار، دارای دو بعدِ در معرض دید متخلفان انگیزه‌دار بودن و در مجاورت متخلفان انگیزه‌دار بودن است که برای سنجش آنها از نُه گویه استفاده شده‌است.

- سبک زندگی منحرفان الکترونیکی/ آنلاین[3]: تعداد زیادی از تحقیقات جرم‌شناختی مشارکت در شیوهٔ زندگی منحرفانه را به عنوان یک عامل خطر برای انواع مختلفی از بزه‌دیدگی از جمله بزه‌دیدگی ناشی از آزاررسانی سایبری (به عنوان مثال، چوی، ۲۰۰۸) شناسایی کرده‌اند. مشارکت در سبک زندگی و یا فعالیت‌های روزمرهٔ منحرفانه، فرضیه‌ای برای افزایش در معرض دید قرار گرفتن و در مجاورت با متخلفان انگیزه‌دار بودن (به عنوان مثال، سایر متخلفان) و موقعیت هایی که موجب قربانی شدن می گردد (به‌عنوان مثال فقدان محافظ توانمند) می باشد (رینز و همکاران، ۲۰۱۱: ۱۱۵۹).

- فعالیت‌های مخاطره‌آمیز آفلاین[4]: مشارکت در فعالیت‌هایی که خطرناک تلقی می‌شوند (مثل نوشیدن الکل و حضور در پارتی) همبستگی روشنی با بزه‌دیدگی دانشجویان دارد. با این حال، ارتباط بین این نوع از فعالیت‌ها و بزه‌دیدگی آنلاین تا کنون به‌طور تجربی توسط محققان بررسی نشده‌است. بنابراین، مقیاس فعالیت‌های مخاطره‌آمیز آفلاین به‌عنوان یک متغیر کنترل به کار

1. Online Guardianship
2. Motivated Offenders
3. Online/Electronic Deviant Lifestyle
4. Offline Risky Activities

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

می‌رود. فعالیت‌های مخاطره‌آمیز آفلاین با هفت گویه سنجش شده و برای پاسخ‌های هر گویه از طیف لیکرت پنج‌تایی استفاده شده‌است.

٤. یافته‌ها

جنسیت ۶۳/۷ درصد (۲۴۲ نفر) پاسخگویان دختر و ۳۶/۳ درصد (۱۳۸ نفر) آنها پسر بوده است. میانگین سنی پاسخگویان ۲۲/۵ سال بود و گروه سنی ۲۳-۲۱ سال با ۴۶/۶ درصد (۱۷۷ نفر) بیشترین نسبت و گروه سنی بالاتر از ۲۹ سال با ۲/۶ درصد (۱۰ نفر) کمترین نسبت از پاسخگویان را تشکیل می‌دادند. تعداد دانشجویان ساکن در خوابگاه با ۶۳/۲ درصد (۲۴۰ نفر) و تعداد دانشجویان ساکن در نزد اقوام با ۰/۵ درصد (۲ نفر) به ترتیب بیشترین و کمترین نسبت را تشکیل می‌دادند.

جدول ۳. توزیع فراوانی متغیر بزه‌دیدگی ناشی از آزاررسانی سایبری

بزه‌دیدگی سایبری	جنسیت	پسر		دختر		جمع کل	
		f	٪	f	٪	f	٪
اصلاً		۶۵	۴۳/۹	۱۱۲	۴۹/۵	۱۷۷	۴۷/۴
متوسط		۷۵	۵۰/۷	۱۰۸	۴۷/۸	۱۸۳	۴۸/۹
زیاد		۸	۵/۴	۶	۲/۷	۱۴	۳/۷
جمع		۱۴۸	۱۰۰	۲۲۶	۱۰۰	۳۷۴	۱۰۰

داده‌های جدول ۳ نشان می‌دهد که ۴۷/۴ درصد از پاسخگویان اصلاً در معرض بزه‌دیدگی ناشی از آزاررسانی سایبری قرار نگرفته‌اند. در مقایسهٔ پاسخگویان دختر و پسر، داده‌های جدول نشان می‌دهد که پسران بیش از دختران در معرض این نوع بزه‌دیدگی قرار گرفته‌اند. در این جا به برخی از مهم‌ترین یافته‌های توصیفی مستخرج از سنجش متغیرهای مستقل اشاره می‌شود:

ـ مقایسهٔ پسران و دختران نشان داد که در تمامی موارد، پسران بیش از دختران اطلاعات خصوصی یا عکس‌ها و فیلم‌هایشان را در شبکه‌های اجتماعی ارسال کرده یا به اشتراک گذاشته‌اند. به عنوان نمونه، ۷۵ درصد از پسران در طول دوازده ماه گذشته حداقل یک بار و بیشتر شمارهٔ تلفن همراه خود را در شبکه‌های اجتماعی مجازی ارسال کرده‌اند. این در حالی است که ۴۲/۹ درصد از دختران در طول دوازده ماه گذشته حداقل یک بار و بیشتر شمارهٔ تلفن همراه خود را برای کسی ارسال کرده‌اند.

ـ بیشترین ساعتی که پاسخگویان به‌صورت آنلاین سپری می‌کنند، یک تا پنج ساعت است که ۵۹/۴ درصد از پاسخگویان (۶۸/۲ درصد از پسران و ۵۹/۴ درصد از دختران) گزینهٔ مذکور را انتخاب کرده‌اند.

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

ـ از حیث مجاورت آنلاین با متخلفان باانگیزه برحسب جنسیت، یافته‌های مربوط به گویهٔ «درحال‌حاضر، با چند نفر که آشنایی با آنها از طریق شبکه‌های اجتماعی بوده، دوست هستید» نشان داد که ۶۱ درصد از پاسخگویان (۶۸/۹ درصد از پسران و ۵۵/۸ درصد از دختران) در طول دوازده ماه گذشته با کسانی که به‌صورت مجازی آشنا شده‌اند، وارد رابطهٔ دوستانه شده‌اند.

ـ حدود ۳۶ درصد از پاسخگویان در طول دوازده ماه گذشته حداقل یک بار و بیشتر به دیگر کاربران اینترنتی که آنها را نمی‌شناخته‌اند (غریبه‌ها) اجازه داده‌اند به شبکه‌های اجتماعی‌شان، که ممکن است شامل اطلاعات شخصی (به‌عنوان مثال، عکس‌ها و علایق) باشد، دسترسی پیدا کنند که نشان‌دهندهٔ آن استکه پسران حدود ۱۸ درصد بیشتر از دختران به افرادی که نمی‌شناسند اجازه داده‌اند به شبکه‌های اجتماعی مجازی‌شان دسترسی پیدا کنند.

ـ همچنین حدود ۳۲/۴ درصد از پاسخگویان (۴۱/۹ درصد از پسران و ۲۶/۱ درصد از دختران) در طول دوازده ماه گذشته حداقل یک بار و بیشتر با کسانی که برای نخستین‌بار در شبکه‌های اجتماعی با آنها آشنا شده‌اند، ملاقات حضوری داشته‌اند. پسران حدود ۱۵/۸ درصد بیشتر از دختران، با کسانی که برای نخستین‌بار در شبکه‌های اجتماعی با آنها آشنا شده‌اند ملاقات حضوری داشته‌اند.

ـ در بعد ناکارآمدی محافظت اجتماعی این گویه با بیشترین انتخاب از سوی پاسخگویان همراه بوده است: «در طول دوازده ماه گذشته، دوستانم از اطلاعاتی که به‌صورت آنلاین ارسال کرده‌ام برای آزار و اذیت و تهدیدکردن من استفاده کرده‌اند». به طور کلی ۳۲/۵ درصد از پاسخگویان (۳۳/۹ درصد از پسران و ۳۱/۸ درصد از دختران) در طول یک سال گذشته حداقل یک‌بار و بیشتر این تجربه را داشته‌اند که دوستانشان از اطلاعاتی که به‌صورت آنلاین ارسال کرده‌اند جهت آزار و اذیت و تهدیدکردن آنها استفاده کنند.

ـ مقایسهٔ بین دختران و پسران نشان داد که در تمامی موارد، پسران بیش از دختران مرتکب رفتارهای متخلفانهٔ آنلاین شده‌اند. به‌عنوان نمونه، ۲۵ درصد از پسران در طول دوازده ماه گذشته حداقل یک بار و بیشتر به افرادی از طریق فضای مجازی پیشنهاد جنسی داده‌اند. این در حالی است که ۵/۷ درصد از دختران در طول دوازده ماه گذشته از طریق فضای مجازی به افرادی پیشنهاد جنسی داده‌اند.

ـ وضعیت توزیع فراوانی و درصدی پاسخگویان در متغیر فعالیت‌های مخاطره‌آمیز آفلاین نشان داد این گویه با بیشترین میزان ارتکاب از سوی پاسخگویان همراه بوده است: «در طول دوازده ماه گذشته، در قرارهای عاشقانه حضور یافته‌ام». به‌طور کلی، ۳۶ درصد از پاسخگویان (۴۶/۶ درصد از پسران و ۲۷ درصد از دختران) در طول دوازده ماه گذشته حداقل یک بار و بیشتر در قرارهای عاشقانه حضور پیدا کرده‌اند.

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

ـ گویهٔ «در طول دوازده ماه گذشته، در پارتی‌ها و مهمانی‌های دوستانهٔ مختلط حضور داشته‌ام» با بیشترین میزان ارتکاب از سوی پاسخگویان همراه بوده است. حدود ۲۴/۴ درصد از پاسخگویان (۴۱/۹ درصد از پسران و ۱۲/۸ درصد از دختران) در طول دوازده ماه گذشته حداقل یک بار و بیشتر در پارتی‌ها و مهمانی‌های مختلط شبانه شرکت کرده‌اند.

ـ ۳۱/۸ درصد از پسران در طول دوازده ماه گذشته حداقل یک بار و بیشتر از مشروبات الکلی استفاده کرده‌اند. این در حالی است که ۱۱ درصد از دختران در طول دوازده ماه گذشته حداقل یک بار و بیشتر مشروبات الکلی استفاده کرده‌اند.

ـ به‌طور کلی می‌توان گفت هم در سبک زندگی متخلفان آنلاین و هم در فعالیت‌های مخاطره‌آمیز آفلاین، تعداد پسران بیش از دختران است. در فضای مجازی پسران بیشتر از دختران کسی را مورد آزار و تهدید قرار داده‌اند یا عکس‌های مستهجن را برای دیگران ارسال کرده‌اند که تعداد دختران به‌مراتب کمتر است. همچنین در فعالیت‌های مخاطره‌آمیز آفلاین پسران بیش از دختران از مشروبات الکلی استفاده کرده یا رابطهٔ جنسی قبل از ازدواج را تجربه کرده‌اند. ارتکاب رفتارهای انحرافی، چه به شکل مجازی و چه غیرمجازی، در پسران بیش از دختران است.

جدول ۴. تحلیل رگرسیونی چندگانهٔ بزه‌دیدگی ناشی از آزاررسانی سایبری

متغیر	β	T	P	همبستگی			شاخص‌های چندهم‌خطی	
				مرتبه صفر	تفکیکی	نیمه‌تفکیکی	ضریب حداقل تحمل	عامل تورم واریانس
سبک زندگی منحرفان آنلاین	۰/۳۷۶	۶/۳۶۹	۰/۰۰۰	۰/۴۴۶	۰/۳۱۶	۰/۲۸۶	۰/۵۸۰	۱/۷۲۴
مشارکت در فعالیت‌های مخاطره‌آمیز آفلاین	۰/۱۰۱	۱/۸۶۷	۰/۰۶۳	۰/۲۹۲	۰/۰۹۷	۰/۰۸۴	۰/۶۹۰	۱/۴۴۹
مجاورت آنلاین با متخلفان انگیزه‌دار	۰/۱۲۶	۲/۱۳۹	۰/۰۳۳	۰/۳۱۷	۰/۱۱۱	۰/۰۹۶	۰/۵۸۶	۱/۷۰۸
در معرض دید متخلفان بودن	۰/۰۰۵	-۰/۸۹	۰/۹۲۹	۰/۱۵۳	-۰/۰۰۵	-۰/۰۰۴	۰/۷۶۰	۱/۳۱۶
جذابیت هدف آنلاین	۰/۰۰۷	۰/۱۱۳	۰/۹۱۰	۰/۲۳۸	۰/۰۰۶	۰/۰۰۵	۰/۵۴۷	۱/۸۲۷
محافظت آنلاین	-۰/۲۲۸	-۴/۷۵۲	۰/۰۰۰	-۰/۱۰۱	-۰/۲۴۱	-۰/۲۱۴	۰/۸۷۶	۱/۱۴۲
$R = ۰/۵۱$ $R^2 = ۰/۲۶$ $R^2_{Adj.} = ۰/۲۵$ $F = ۲۱/۵۱۹$ $p < ۰/۰۰۰$								

جدول ۴ نشان می‌دهد که همبستگی چندگانهٔ متغیرهای مستقل با بزه‌دیدگی ناشی از آزاررسانی سایبری معادل ۰/۵۱ است. ضریب تعیین نشان‌دهندهٔ آن است که ۲۶ درصد از تغییرات بزه‌دیدگی ناشی از آزاررسانی سایبری در میان دانشجویان دانشگاه مازندران توسط متغیرهای مستقل تبیین

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

می‌شود. برای تشخیص سهم هریک از متغیرهای مستقل در تبیین و پیش‌بینی این نوع بزه‌دیدگی، ضرایب تأثیر استانداردشدهٔ متغیرهای مستقل با یکدیگر مقایسه شده‌اند که طبق نتایج، متغیر سبک زندگی منحرفان آنلاین (β = ۰/۳۷۶) بیشترین سهم را در پیش‌بینی بزه‌دیدگی ناشی از آزاررسانی سایبری دارد و پس از آن، متغیر محافظت آنلاین (β = -۰/۲۲۸) بیشترین سهم را داراست.

جدول ۵. تحلیل رگرسیونی چندمتغیرهٔ بزه‌دیدگی ناشی از آزاررسانی سایبری

متغیر	β	t	P
سبک زندگی منحرفان آنلاین	۰/۳۹۴	۵/۴۰۷	۰/۰۰۰
مشارکت در فعالیت‌های مخاطره‌آمیز آفلاین	۰/۰۰۳	۰/۰۴۲	۰/۹۶۷
مجاورت آنلاین با متخلفان انگیزه‌دار	۰/۱۳۸	۱/۸۲۸	۰/۰۶۹
در معرض دید متخلفان بودن	-۰/۰۷۶	-۱/۱۱۳	۰/۲۶۷
جذابیت هدف آنلاین	۰/۰۵۳	۰/۶۸۱	۰/۴۹۷
محافظت آنلاین	۰/۲۹۰	-۴/۸۰۶	۰۰۰-۰
$R = ۰/۵۱۸$ $R^2 = ۰/۲۶۸$ $R^2_{Adj.} = ۰/۲۴۸$ $F = ۱۳/۳۵۵$ $p < ۰/۰۰۰$			

مطابق با داده‌های جدول ۵ می‌توان بیان کرد که متغیرهای مستقل با بزه‌دیدگی ناشی از آزاررسانی سایبری در پسران همبستگی متوسطی دارند. ضریب تعیین نشان‌دهندهٔ آن است که تنها ۲۶ درصد تغییرات این نوع دختران توسط متغیرهای مستقل تبیین می‌شود. نتایج مقایسه نشان می‌دهد که متغیر سبک زندگی منحرفان آنلاین (β=۰/۳۹۴) سهم قابل‌توجهی در پیش‌بینی بزه‌دیدگی ناشی از آزاررسانی سایبری در دختران داشته است.

جدول ۶. تحلیل رگرسیونی چندمتغیرهٔ بزه‌دیدگی ناشی از آزاررسانی سایبری

متغیر	β	t	p
سبک زندگی منحرفان آنلاین	۰/۳۵۴	۳/۸۷۳	۰/۰۰۰
مشارکت در فعالیت‌های مخاطره‌آمیز آفلاین	۰/۲۱۲	۲/۴۹۸	۰/۰۱۴
مجاورت آنلاین با متخلفان انگیزه‌دار	۰/۰۸۹	۱/۰۰۴	۰/۳۱۷
در معرض دید متخلفان بودن	۰/۰۸۷	۱/۱۲۱	۰/۲۶۴
جذابیت هدف آنلاین	۰/۰۲۹	-۰/۳۱۳	۰/۷۵۵
محافظت آنلاین	-۰/۱۳۳	-۱/۷۲۲	۰/۰۸۷
$R = ۰/۵۴۴$ $R^2 = ۰/۲۹۶$ $R^2_{Adj.} = ۰/۲۶۶$ $F = ۹/۱۲۵$ $p < ۰/۰۰۰$			

مطابق با داده‌های جدول ۶، تنها ۲۹ درصد تغییرات بزه‌دیدگی ناشی از آزاررسانی سایبری توسط متغیرهای مستقل تبیین می‌شود. ضمن اینکه متغیر سبک زندگی منحرفان آنلاین (β=۰/۳۵۴) و متغیر مشارکت در فعالیت‌های مخاطره‌آمیز آفلاین (β= ۰/۲۱۲) سهم قابل‌توجهی در پیش‌بینی این نوع بزه‌دیدگی در پسران را داشته‌اند.

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

جدول۷. آماره‌های تحلیل رگرسیون چندمتغیره برای تبیین ابعاد بزه‌دیدگی ناشی از آزاررسانی سایبری

ابعاد متغیر وابسته	متغیرهای مستقل	R	R^2	F	β	T	p
بعد آبرویی بزه‌دیدگی ناشی از آزاررسانی سایبری	سبک زندگی منحرفان آنلاین	۰/۴۹۷	۰/۲۴۷	۱۹/۹۹۷	۰/۳۶۰	۶/۰۴۵	۰/۰۰۰
	مشارکت در فعالیت‌های مخاطره‌آمیز آفلاین				۰/۱۱۲	۲/۰۴۸	۰/۰۴۱
	مجاورت آنلاین با متخلفان انگیزه‌دار				۰/۱۵۷	۲/۶۴۴	۰/۰۰۹
	در معرض دید متخلفان بودن				۰/۰۰۷	۰/۱۳۸	۰/۸۹۱
	جذابیت هدف آنلاین				-۰/۰۳۵	-۰/۵۶۳	۰/۵۷۳
	محافظت آنلاین				-۰/۱۱۹	-۲/۴۶۶	۰/۰۱۵
بعد جنسی بزه‌دیدگی ناشی از آزاررسانی سایبری	سبک زندگی منحرفان آنلاین	۰/۴۰۱	۰/۱۶۱	۱۱/۶۷۳	۰/۳۳۷	۵/۳۵۷	۰/۰۰۰
	مشارکت در فعالیت‌های مخاطره‌آمیز آفلاین				۰/۰۲۴	۰/۴۱۶	۰/۶۷۸
	مجاورت آنلاین با متخلفان انگیزه‌دار				۰/۰۵۸	۰/۹۳۵	۰/۳۵۱
	در معرض دید متخلفان بودن				۰/۰۵۷	۰/۹۹۰	۰/۳۲۳
	جذابیت هدف آنلاین				۰/۰۱۱	۰/۱۶۸	۰/۸۶۷
	محافظت آنلاین				۰/۱۰۲	-۱/۹۸۶	۰/۰۴۸
بعد مالی بزه‌دیدگی ناشی از آزاررسانی سایبری	سبک زندگی منحرفان آنلاین	۰/۲۸۹	۰/۰۸۴	۵/۵۷۶	۰/۱۱۶	۱/۷۶۰	۰/۰۴۹
	مشارکت در فعالیت‌های مخاطره‌آمیز آفلاین				۰/۰۵۶	۰/۹۲۶	۰/۳۵۵
	مجاورت آنلاین با متخلفان انگیزه‌دار				۰/۰۲۷	۰/۴۱۰	۰/۶۸۲
	در معرض دید متخلفان بودن				۰/۰۵۶	۰/۹۷۵	۰/۳۳۰
	جذابیت هدف آنلاین				۰/۰۵۳	۰/۷۸۹	۰/۴۳۰
	محافظت آنلاین				-۰/۲۷۲	-۵/۰۸۳	۰/۰۰۰

داده‌های جدول ۷ و مقایسهٔ ابعاد بزه‌دیدگی ناشی از آزاررسانی سایبری نشان می‌دهند که متغیرهای مستقل با بعد آبرویی بزه‌دیدگی، بیشتر و متغیرهای مستقل با بعد مالی بزه‌دیدگی، کمتر از سایر ابعاد همبستگی دارند.

۵. بحث و نتیجه‌گیری

با وجود گسترش رفتارهای انحرافی وابسته به فعالیت در فضای سایبر و استفاده از اینترنت و این که جرایم جدیدی متوجه افراد و به‌خصوص نسل جوان است، به نظر می‌رسد تحقیقی در ایران به بررسی سایبر آزاری و بزه‌دیدگی حاصل از آن (بزه‌دیدگان سایبری دانشجویان از دیدگاه نظریهٔ فعالیت‌های روزمره) نپرداخته است. یکی از سه عنصر کلیدی نظریهٔ فعالیت‌های روزمره که در کاهش وقوع بزه‌دیدگی نقش بسزایی دارد، محافظت آنلاین است، که یکی از مصادیق آن دانش و اطلاعات شخص از خطرات آنلاین در فضاهای مجازی است. در واقع، هرچه اطلاعات و دانش شخصی بیشتر باشد، احتمال بزه‌دیدگی او کاهش می‌یابد. ازاین‌رو، افزایش دانش افراد از

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

خطرات شبکه‌های مجازی و افزایش اطلاعات کاربران از برنامه‌های امنیتی رایانه‌شان، می‌تواند تا حدی از بروز بزه‌دیدگی ناشی از آزاررسانی سایبری جلوگیری کند. این تحقیق نشان داد که نظریهٔ فعالیت‌های روزمره، قابلیت به‌کار گرفته‌شدن در بزه‌دیدگی ناشی از مزاحمت‌های سایبری در میان دانشجویان را دارد.

فرضیه‌ای که دلالت بر این دارد که بین جذابیت هدف آنلاین و بزه‌دیدگی ناشی از آزاررسانی سایبری دانشجویان، رابطهٔ مستقیم و معناداری وجود دارد، تأیید نشد. بر اساس نظریهٔ فعالیت‌های روزمره تصور می‌شود که هرچه هدف دارای ارزش، سکون، دید و دسترسی باشد، آن هدف از مطلوبیت بیشتری برخوردارخواهد بود. بنابراین احتمال بزه‌دیدگی ناشی از آزاررسانی سایبری بیشتر می شود. در پژوهش‌های پیشین نتایج متناقضی از وجود رابطه بین جذابیت هدف و بزه‌دیدگی ناشی از آزاررسانی سایبری به دست آمده است. نتایج این تحقیق منطبق با نتایج تحقیقات رینز و همکاران (۲۰۱۱) و در تناقض با نتایج تحقیق لوکفلد و یار (۲۰۱۶) است. این فرضیه در حالت کلی تأیید نشد، اما هنگامی که متغیرهای مستقل پژوهش جداگانه بررسی شدند، متغیر جذابیت هدف در دو بعد (بزه‌دیدگی جنسی و بزه‌دیدگی آبرویی) معنادار بود و تأیید شد. برخلاف تصور، پسران بیش از دختران به عنوان اهداف جذاب محسوب شدند. این نکته به این علت است که پسران در مقایسه با دختران، در شبکه‌های اجتماعی مجازی بی‌پرواتر عمل می‌کنند و اطلاعات خود را بیشتر در دسترس عموم قرار می‌دهند و کمتر از دختران از اینکه مورد آزار و اذیت‌های مجازی قرار گیرند بیم دارند. در مجموع، خرده متغیرهای حاوی مناسب‌بودن هدف درجات مختلفی از قابلیت جابه‌جایی را در محیط‌های مجازی نشان می‌دهند. به نظر می‌آید که بیشترین همگرایی در مورد ارزش هدف احتمالاً به‌طور عمده به این دلیل وجود داشته باشد که ارزیابی از محیط اکولوژیکی (واقعی یا مجازی) سرچشمه نمی‌گیرد بلکه از جای دیگری یعنی از حوزه‌های روابط اقتصادی و نمادین به آن محیط آورده می‌شود.

فرضیهٔ دوم مبنی بر اینکه بین محافظت آنلاین و بزه‌دیدگی ناشی از آزاررسانی سایبری، رابطهٔ معکوسی وجود دارد، تأیید شد. به عقیدهٔ کوهن، فقدان محافظان توانا، که از تحقق جرم در زمان فعالیت‌های روزمرهٔ مردم که هر روز نیز تکرار می‌شود، جلوگیری کنند، موجب تحقق جرم می‌شود. این فرضیه به‌لحاظ تجربی تأیید شده است. در مجموع، فقدان یا عدم‌حضور نگهبانان در نقطه‌ای که در آن مجرمان بالقوه و اهداف مناسب در زمان و مکان وجود دارند، به‌عنوان بحران در تعیین احتمال وقوع جرم در نظر گرفته می‌شود. نتایج این تحقیق نشان داد که هرچه محافظت در سطح بالاتری باشد، خطر بزه‌دیدگی ناشی از آزاررسانی سایبری کاهش می‌یابد. این دو متغیر به‌صورت معکوس با یکدیگر ارتباط دارند. آن دسته از دانشجویانی که دانش بیشتری در مورد مرورگر اینترنت و یا اسکن‌کردن ویروس داشته‌اند و یا شبکه‌های اجتماعی مجازی‌شان را به

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

دسترسی افراد محدود تنظیم کرده‌اند، کمتر مورد بزه‌دیدگی قرار گرفته‌اند. این تحقیق نشان داد که دانش دانشجویان پسر دربارهٔ شبکه‌های اجتماعی مجازی و در مورد سیستم‌های عاملشان در مقایسه با دختران در سطح بالاتری قرار دارد.

فرضیه‌ای که دلالت بر این دارد که بین در معرض دید متخلفان انگیزه‌دار بودن و بزه‌دیدگی ناشی از آزاررسانی سایبری، رابطهٔ مستقیم و معنادار وجود دارد، در حالت کلی تأیید نشد، اما هنگامی که متغیرهای مستقل پژوهش، جداگانه در هریک از ابعاد بزه‌دیدگی ناشی از آزاررسانی سایبری بررسی شدند، این متغیر در دو بعد بزه‌دیدگی آبرویی و بزه‌دیدگی جنسی معنادار بود و تأیید شد. در بعد بزه‌دیدگی آبرویی، تعداد پسران بیش از دختران است و علت آن می‌تواند این باشد که پسران عکس‌ها و یا اطلاعات شخصی خود را آسان‌تر از دختران با دیگران به اشتراک می‌گذارند، و به این علت اطلاعات خصوصی‌شان، چه واقعی و چه ساختگی (اطلاعات کذب) بیشتر در شبکه‌های اجتماعی مجازی پخش می‌شود. اما در بعد بزه‌دیدگی جنسی، تعداد دختران بیش از پسران است.

فرضیه‌ای که دلالت بر این دارد که بین دو متغیر در مجاورت متخلفان انگیزه‌دار قرارگرفتن و بزه‌دیدگی ناشی از آزاررسانی سایبری رابطهٔ مستقیم و معناداری وجود دارد، تأیید شد. طبق نتایج تحقیق حاضر، هرچه مجاورت آنلاین به متخلفان انگیزه‌دار آنلاین بیشتر باشد، میزان خطر بزه‌دیدگی بیشتر خواهد بود. به عبارتی می‌توان گفت آن دسته از افرادی که به کسانی که به‌صورت مجازی با آنها آشنا شده‌اند اجازهٔ آشنایی بیشتر را داده‌اند و یا کسانی که با افرادی که ابتدا به‌صورت مجازی با آنها آشنا شده‌اند، ملاقات حضوری داشته‌اند، بیشتر در مجاورت آنلاین با متخلفان انگیزه‌دار قرار گرفته‌اند. تفاوت در معرض دید بودن و مجاورت آنلاین با متخلفان این است که آنهایی که در معرض دید متخلفان قرار گرفته‌اند هنوز، به‌صورت مجازی، مجاورت و نزدیکی با متخلفان انگیزه‌دار ندارند، اما در مجاورت آنلاین با متخلفان انگیزه‌دار یک گام جلوترند و افراد به‌صورت مجازی در زمان و مکان همگرا هستند و نزدیکی میان اهداف مناسب و متخلفان انگیزه‌دار به وجود آمده است.

فرضیه‌ای که دلالت بر این دارد که بین سبک زندگی منحرفان آنلاین و بزه‌دیدگی ناشی از آزاررسانی سایبری، رابطهٔ مستقیم و معناداری وجود دارد نیز تأیید شد. بسیاری از تحقیقات جرم‌شناختی مشارکت در فعالیت‌های آنلاین منحرفانه یا سبک زندگی منحرفان آنلاین را به‌عنوان عامل خطر برای انواع متنوعی از بزه‌دیدگی، از جمله بزه‌دیدگی ناشی از آزاررسانی سایبری، معرفی کرده‌اند (به‌عنوان مثال، چوی، ۲۰۰۸). به‌عبارتی، می‌توان گفت مشارکت در چنین فعالیت‌هایی، باعث آشنایی و هم‌نشینی با همالان آنلاین منحرف می‌شود که خود این همالان می‌توانند در مواقعی یکدیگر را به‌صورت آنلاین مورد آزار و اذیت قرار داده و به عبارتی خود منبع تهدیدی

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

برای یکدیگرند. مقایسهٔ بین دختران و پسران نشان داد که پسران بیشتر از دختران سبک زندگی منحرفانهٔ آنلاین دارند. به عبارت دیگر آنها بیش از دختران پیشنهادات جنسی مجازی و یا تصاویر مستهجن را در شبکه‌های اجتماعی مجازی برای کسی ارسال کرده‌اند.

فرضیه‌ای که دلالت بر این دارد که بین مشارکت در فعالیت‌های مخاطره‌آمیز آفلاین و بزه‌دیدگی ناشی از آزار رسانی سایبری رابطهٔ مستقیم و معناداری وجود دارد، تأیید نشد. بخش کوچکی از تحقیقاتی که تأثیرات رفتارهای خطرناک یا منحرفانه را بر روی بزه‌دیدگی ناشی از آزاررسانی سایبری بررسی کرده‌اند، نشان دادند که درگیرشدن در این گونه فعالیت‌ها خطر بزه‌دیدگی آنلاین را افزایش می‌دهد؛ اگرچه تاکنون رابطهٔ میان این نوع از فعالیت‌ها و بزه‌دیدگی آنلاین به‌طور تجربی توسط محققان بررسی نشده است (رینز و همکاران، ۲۰۱۱). این فرضیه در حالت کلی تأیید نشد، اما هنگامی که متغیرهای مستقل پژوهش در هریک از ابعاد بزه‌دیدگی ناشی از آزاررسانی سایبری جداگانه بررسی شدند، این متغیر در دو بعد بزه‌دیدگی جنسی و بزه‌دیدگی آبرویی معنادار بود و تأیید شد.

دانشجویانی که در فعالیت‌های خطرناک آنلاین یا بازدید مکرر از وب‌سایت‌های جدید مشغول هستند، احتمال بیشتری دارد که بزه‌دیدهٔ جرایم سایبری شوند. علاوه بر این، دانشجویانی که از نگهبان‌های دیجیتال (آنتی‌ویروس‌ها، برنامه‌های ضدجاسوسی و دیوارهای آتش) استفاده می‌کنند، به احتمال کمتری بزه‌دیدگان جرایم سایبری هستند. تعداد معدودی از تحقیقات داخلی همچون مقالهٔ مالمیر و زررخ (۱۳۸۹) تحت عنوان «پیشگیری از بزه‌دیدگی ناشی از آزاررسانی سایبری» و همچنین مقالهٔ زررخ (۱۳۹۰) تحت عنوان «بزه‌دیده‌شناسی سایبری» به بررسی بزه‌دیدگی ناشی از آزاررسانی سایبری با استفاده از نظریهٔ فعالیت‌های روزمره پرداخته‌اند که روش تحقیق هر دو مقاله به‌صورت توصیفی و تحلیلی در تبیین فرصت‌های بزه‌دیدگی آنلاین است. با این حال، تاکنون موضوع تلاقی در زمان و مکان بین بزه‌دیده و مجرم و چگونگی اثر این تباین فرصت‌های ساختاری برای بزه‌دیده و مجرم و نیز چگونگی اثر این تلاقی فرصت‌های ساختاری برای بزه‌دیده‌شدن به‌لحاظ نظری بررسی نشده‌است.

منابع

اسلامی، ابراهیم (۱۳۹۵) «جایگاه حمایت از بزه‌دیدگان جرایم سایبری در مقررات کیفری حقوق داخلی و حقوق بین الملل»، *پژوهشنامهٔ حقوق اسلامی*، سال هفدهم، شمارهٔ ۱ (پیاپی ۴۳): ۱۸۲-۱۵۷.

خبرگزاری مهر، (۱۳۹۴)، «تهران در صدر جرایم اینترنتی»، برگرفته از *https://www.mehrnews.com/news/3575583*، ۱۳۹۷/۵/۵.

دواس، دی.ای (۱۳۹۰) *پیمایش در تحقیقات اجتماعی*، ترجمهٔ هوشنگ نایبی، تهران: نی.

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

زررخ، احسان (۱۳۹۰) «بزه‌دیده‌شناسی سایبری»، *مجلهٔ پژوهش*، سال هفدهم، شمارهٔ ۶۴: ۱۲۷-۱۵۷.

علیوردی‌نیا، اکبر؛ منا علیمردانی (۱۳۹۵) «کاربست تجربی نظریهٔ فعالیت‌های روزمره در بررسی رفتارهای انحرافی دانشجویان»، *جامعه‌شناسی کاربردی*، سال بیست و هشتم، شمارهٔ پیاپی (۶۷)، شمارهٔ ۳: ۱-۲۴.

مالمیر، محمود؛ زررخ، احسان (۱۳۸۹) «پیشگیری از بزه‌دیدگی سایبری»، *مطالعات پیشگیری از جرم*، سال پنجم، شمارهٔ ۱۷: ۵۹-۸۶.

میر، فاطمه (۱۳۹۴) نقش بزه‌دیدگی در تحقق جرایم سایبری، پایان‌نامهٔ دورهٔ کارشناسی ارشد علوم اقتصادی دانشگاه فردوسی مشهد.

Addington, Lynn A (2013) "Reporting and Clearance of Cyberbullying Incidents: Applying 'Offline' Theories to Online Victims." *Journal of Contemporary Criminal Justice*,20(10):1-21.

Bennett, R. (1991) Routine activities: A Cross-National Assessment of a Criminological Perspective, *Social Forces 70*, 147–63.

Bauman, S., Toomey, R. B., & Walker, J. L. (2013) Associations Among Bullying, Cyberbullying, And Suicide In High School Students, Journal of Adolescence, 36(2), 341-350.

Bossler, A. M., & Holt, T. J. (2009) On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory, International Journal of Cyber Criminology, 3(1), 400- 420.

Bossler, A. M., Holt, T. J., & May, D. C. (2012) Predicting online harassment victimization among a Juvenile population. Youth & Society, 44(4), 500-523.

Choi, K. S. (2008) Computer Crime Victimization and Integrated Theory: An Empirical Assessment, International Journal of Cyber Criminology, 2(1), 308-333.

Cohen, L. E., & Felson, M. (1979) Social Change and Crime Rate Trends: A Routine Activity Approach, American Sociological Review,44: 588-608.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981) Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory. *American Sociological Review, 46*, 505-524.

Dashora, K. (2011) "Cybercrime in the Society: Problems and Preventions" , Journal of Alternative Perspectives in the Social Sciences, 3 (1), 240-259.

Denning, D. (1999) Information Warfare and Security. New York: Addison Wesley.

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

Dilmac, Bulent & Aydogan, D. (2010) Parental Attitude as Predictor of Cyber Bullying among Primary School Children, International Journal of Social, Behavioral, Educational, Economic and Management Engineering, 4 (7), 1667-1671.

Drebing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014) Cyber stalking In a Large Sample of Social Network Users: Prevalence, Characteristics, And Impact Upon Victims, Cyber psychology, Behavior, and Social Networking, 17(2), 61-67.

Felson, M. (1998) Crime and Everyday Life, 2nd ed. Thousand Oaks, CA: Pine Forge Press.

Hensler-McGinnis, N. F. (2008) Cyberstalking Victimization: Impact and Coping Responses in a National University Sample. Dissertation submitted to the Faculty of the Graduate School of the University of Maryland, College Park.

Henson, B., Reyns, B. W., & Fisher, B. S. (2011) Security in The 21st Century: Examining the Link Between Online Social Network Activity, Privacy, And Interpersonal Victimization. Criminal Justice Review, 36(3), 253-268.

Jeralds, L. M. (2011) Bullying Victimization, Target Suitability, and Guardianship: A Routine Activities Approach (Doctoral Dissertation, University of North Carolina Wilmington).

Kennedy, M. A., & Taylor, M. A. (2010) Online Harassment and Victimization of College Students, Justice Policy Journal, 7(1), 1-21.

Leukfeldt, E. R., & Yar, M. (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis, Deviant Behavior, 37(3), 263-280.

Lipton, J. D. (2011) Combating cyber-victimization. Berkeley Technology Law Journal, 26(2), 1103-1155.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010) Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory, Deviant Behavior, 31(5), 381-410

McNeeley, S. (2015). Lifestyle-Routine Activities and Crime Events, Journal of Contemporary Criminal Justice, 31(1), 30-52.

Miller, J, Mitchell Christopher, J, Schreck, T. (2006) Criminological Theory: a Brief Introduction Boston, Pearson/ Allyn and Bacon.

Miller, J. Mitchell (Ed). (2009) *21st Century Criminology A Reference Handbook*, USA: SAGE Publications.

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

Ngo, F. T., & Paternoster, R (2011) Cybercrime Victimization: An Examination of Individual and Situational Level Factors. *International Journal of Cyber Criminology*, *5*(1), 773.

Paullet, Karen & Rota, & Swan, T. (2009) Cyber stalking: An Exploratory Study Of Students at a Mid-Atlantic University, Issues in Information Systems, 10(2): 640-649.

Reychay, Iris, Sukenik, S. (2015) Cyberbullying: Keeping Our Children Safe in 21 st century, Handbook of Research on Digital Crime, Cyberspace Security and Information Assurance, 77-79.

Reyns, B., B. Henson & S. F. (2011) Being Pursued Online. Applying Cyber lifestyle-Routine Activities Theory to Cyber stalking Victimization, Criminal Justice and Behavior 38(11):1149–1169.

Shinder, D. L., & Tittel, E. (2002) Scene of the Cybercrime: Computer Forensics Handbook, Syngress Publishing.

Smith, A., Rainie, L., & Zickuhr, K. (2010) College Students and Technology, Pew Research Center's Internet & American Life Project, Washington, DC.

Tseloni, A., Wittebrood, K., Farrell, G. and Pease, K. (2004) Burglary Victimization In England and Wales, The Unites States and The Netherlands: A Cross-national Comparative Test of Routine Activities and Lifestyle Theories. British Journal of Criminology 44, 66–91.

Webster, F. (2002) Theories of The Information Society, 2nd edn. London: Routledge.

Wilsem, Johan V. (2009) World Tied Together? Online and Non – Domestic Routine Activities and Their Impact on Digital and Traditional Threat Victimization, European Journal of Criminology, 8 (12), 115 – 127.

Yar, M. (2005) The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), 407-427.

Yucedal, B. (2010) Victimization in cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories (Doctoral Dissertation, Kent State University).

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

پیوست ۱. مقیاس جذابیت هدف آنلاین (رینز و همکاران، ۲۰۱۱)

متغیر	گویه ها
جذابیت هدف آنلاین	۱. در طول دوازده ماه گذشته، نام واقعی‌ام را به‌طور کامل در شبکه‌های اجتماعی منتشر ارسال کرده‌ام. ۲. در طول دوازده ماه گذشته، اطلاعاتی در مورد چگونگی وضعیت تأهل (مجرد، متأهل) خود در شبکه‌های اجتماعی ارسال کرده‌ام. ۳. در طول دوازده ماه گذشته، اطلاعاتی در مورد گرایش جنسی‌ام(دگرجنس‌گرایی، همجنس‌گرایی، هردوجنس‌گرایی، هیچ جنس‌گرایی) در شبکه‌های اجتماعی ارسال کرده‌ام. ۴. در طول دوازده ماه گذشته، شمارهٔ تلفن همراه خود را در شبکه‌های اجتماعی ارسال کرده‌ام. ۵. در طول دوازده ماه گذشته، آدرس ایمیل خود را در شبکه‌های اجتماعی ارسال کرده‌ام. ۶. در طول دوازده ماه گذشته، آدرس دیگر سایت‌های شبکه‌های اجتماعی خود را که در آنها عضو هستم، یا وبلاگ‌هایی که دارم را به اشتراک گذاشته‌ام. ۷.در طول دوازده ماه گذشته، اطلاعاتی در مورد علایق و فعالیت‌های خود در شبکه‌های اجتماعی ارسال کرده‌ام. ۸. در طول دوازده ماه گذشته، عکس‌های نامناسبم را در شبکه‌های اجتماعی ارسال کرده‌ام. ۹. در طول دوازده ماه گذشته، فیلم‌های نامناسبم را در شبکه‌های اجتماعی ارسال کرده‌ام.

پیوست ۲. مقیاس محافظت آنلاین(رینز و همکاران، ۲۰۱۱؛ لوکفلد و یار، ۲۰۱۶)

متغیر مستقل	ابعاد	گویه ها
محافظت آنلاین	محافظت فیزیکی	۱. در طول دوازده ماه گذشته، شبکهٔ اجتماعی یا وبلاگم را برای دسترسی محدود تنظیم کرده‌ام. ۲.در طول دوازده ماه گذشته، از ردیاب پروفایل برای مشاهدهٔ کسانی که از عکس پروفایلم بازدید کرده‌اند، استفاده کرده‌ام. ۳.در طول دوازده ماه گذشته، رایانه‌ام را به نرم‌افزارهای آنتی‌ویروس مجهز ساخته‌ام.
	محافظت شخصی	۱. در طول دوازده ماه گذشته، ایمیل‌های فرستندگان ناشناس را باز کرده‌ام. ۲. در طول دوازده ماه گذشته، پیوست‌ها یا فایل‌های فرستندگان ناشناس را باز کرده‌ام. ۳. در طول دوازده ماه گذشته، از رمز عبورهای مختلف برای حساب‌های مختلف استفاده کرده‌ام. ۴. در طول دوازده ماه گذشته، قبل از آنکه چیزی را به‌صورت اینترنتی خریداری کرده باشم، مطمئن شده‌ام که فروشنده قابل اعتماد است. ۵. اطلاعات در مورد سیستم عامل رایانهٔ شخصی. ۶. اطلاعات در مورد مرورگر اینترنت. ۷. اطلاعات در مورد اسکن کردن ویروس.
	(ناکارآمدی) محافظت اجتماعی	۱.در طول دوازده ماه گذشته، دوستانم از اطلاعاتی که به‌صورت آنلاین ارسال کرده‌ام برای آزار و اذیت و تهدید کردن من استفاده کرده‌اند. ۲. در طول دوازده ماه گذشته، افراد غریبه‌ای از اطلاعاتی که به‌صورت آنلاین ارسال کرده ام برای آزار و اذیت و تهدید کردنم استفاده کرده‌اند.

پیوست ۳. مقیاس مجاورت آنلاین با متخلفان انگیزه‌دار (رینز و همکاران، ۲۰۱۱)

متغیر	گویه ها
مجاورت آنلاین با متخلفان انگیزه‌دار	اجازهٔ دسترسی پیدا کردن دیگر کاربران به شبکه‌های اجتماعی مجازی.
	استفاده از سرویس آنلاین (برنامه‌های دوست یاب) جهت پیدا کردن دوستان در شبکه‌های اجتماعی مجازی.
	اجازهٔ آشنایی بیشتر با کسانی که به‌صورت مجازی رابطهٔ دوستی با آنها شکل گرفته است.
	ملاقات حضوری داشتن با کسانی که برای نخستین بار در شبکه‌های اجتماعی آشنایی صورت گرفته است.
	تعداد دوستان در شبکه‌های اجتماعی مجازی

[DOR: 20.1001.1.24766933.1398.10.1.7.9]

پیوست ۴. مقیاس در معرض دید متخلفان انگیزه‌دار بودن (رینز و همکاران، ۲۰۱۱)

متغیر	گویه ها
در معرض دید متخلفان انگیزه‌دار بودن	میزان زمانی که به‌صورت آنلاین صرف شده‌است.
	تعداد شبکه‌های اجتماعی متعلق به پاسخگو.
	تعداد دفعات بازدید از شبکه‌های اجتماعی مجازی.
	تعداد عکس‌های ارسال شدهٔ آنلاین.

پیوست ۵. مقیاس سبک زندگی منحرف آنلاین (رینز و همکاران، ۲۰۱۱)

نام متغیر	گویه ها
سبک زندگی منحرف آنلاین	تماس یا تلاش برای تماس آنلاین با افرادی حتی پس از آنکه آنها تقاضای متوقف‌ساختن آن را داشته‌اند.
	دیگران را به‌صورت آنلاین مورد آزار و اذیت قرار دادن حتی پس از آنکه آنها تقاضای متوقف‌ساختن آن را داشته‌اند.
	به‌صورت مجازی پیشنهاد جنسی به کسی دادن.
	با افرادی به شیوهٔ خشونت‌آمیز صحبت کردن علی‌رغم تقاضای آنها برای متوقف کردن.
	تلاش برای هک کردن حساب شبکه‌های اجتماعی آنلاین افراد.
	موسیقی یا فیلمی را به‌صورت غیرقانونی دانلود کردن.
	تصاویر شرم‌آور جنسی را به‌صورت آنلاین یا از طریق پیام‌های متنی برای کسی ارسال کردن.

پیوست ۶. مقیاس فعالیت‌های مخاطره‌آمیز آفلاین (رینز و همکاران، ۲۰۱۱)

متغیر	گویه‌ها
فعالیت‌های مخاطره‌آمیز آفلاین	از مشروبات الکلی (آبجو، ویسکی، شراب، ودکا) استفاده کردن.
	از مواد مخدر (تریاک، حشیش، هروئین) استفاده کردن.
	تجربهٔ استفاده از مواد روان‌گردان (شیشه، کراک، اکس) داشتن.
	در پارتی‌ها و مهمانی‌های دوستانهٔ مختلط حضور داشتن.
	تجربهٔ رابطهٔ جنسی (آمیزش جنسی) بدون ازدواج داشتن.
	در قرارهای عاشقانه حضور یافتن.

[DOR: 20.1001.1.24766933.1398.10.1.7.9]