

توسعه و ارزیابی مقیاس سنجش بزه‌دیدگی سایبری در ایران

مطالعه موردی: کاربران اینترنت در استان قم

تاریخ پذیرش: ۹۸/۰۳/۲۵

تاریخ دریافت: ۹۷/۱۱/۲۱

(صص ۱ - ۲۳)

مونا جامی‌پور^۱

چکیده

علیرغم اهمیت توسعه جامعه دیجیتال، چالش‌های بی‌شماری در رابطه با پیشگیری از جرایم رو به رشد سایبری و کاهش میزان بزه‌دیدگی سایبری وجود دارد. علیرغم نوظهور بودن تحقیقات حوزه بزه‌دیدگی سایبری، مطالعات محدودی در رابطه با سنجش بزه‌دیدگی سایبری صورت گرفته است. با توجه به اینکه جرایم سایبری با توجه به قوانین حاکم بر کشورها و بسترهای اجتماعی و فرهنگی آنها متفاوت می‌باشد لذا نیاز به توسعه مقیاس سنجش بزه‌دیدگی سایبری در ایران با توجه به قانون سایبری کشور کاملاً آشکار است که تاکنون پژوهشی در این رابطه صورت نگرفته است.

به منظور دستیابی به هدف اصلی پژوهش در مرحله اول با استخراج مصادیق بزه‌دیدگی‌های سایبری از قانون جرایم سایبری کشور و برگزاری جلسات متوالی با خبرگان حوزه تحقیق ابزار اولیه سنجش بزه‌دیدگی سایبری توسعه یافته است. در مرحله دوم پژوهش به منظور اعتبارسنجی ابزار توسعه یافته از روش پیمایش بهره گرفته شده است. در این مرحله مشارکت کنندگان در پژوهش کاربران اینترنت در استان قم بوده‌اند. داده‌های حاصل با استفاده از روش تحلیل عاملی تایید و بکارگیری نرم افزار آموس مورد تحلیل قرار گرفت. نتایج نشان دهنده چهار بعد بزه‌دیدگی اجتماعی، بزه‌دیدگی اقتصادی، بزه‌دیدگی اخلاقی و بزه‌دیدگی سیاسی می‌باشد.

واژگان کلیدی: فضای سایبری، جرایم سایبری، بزه‌دیدگی، بزه‌دیدگی سایبری

۱. استادیار مدیریت سیستم‌ها دانشگاه حضرت معصومه(س) (m.jami@hmu.ac.ir)

۱. مقدمه

پیدایش و رشد بی‌سابقه فناوری‌های رایانه‌ای شبکه محور، تحولات شگرف و دستاوردهای ستרגی را در جهت جامعه انسانی به سوی قله‌های پیشرفت اجتماعی همراه داشته است. بی‌تردید عمده‌ترین شکل‌گیری این دنیای جدید، رهایی از قالب خاکی بوده است که محدودیت‌ها و موانع، بشر را برآن داشت تا به آرمان خود که دستیابی به دنیای بی‌حد و مرز است دست یابد (گلن، ۲۰۱۴).

نقش ابزارها و سرویس‌های فناوری اطلاعات روز به روز پر رنگتر می‌شود، طبق پیش بینی سازمان *ITU* تا سال ۲۰۲۰ بیش از ۱۲ میلیارد وسیله دیجیتال از طریق اینترنت به هم متصل می‌شوند. با این وجود علیرغم اهمیت استفاده از چنین فضایی هنوز تهدیدهای متنوع امنیتی خسارات فراوانی را برای جوامع به همراه دارد (*ITU*, 2018).

رایانه‌ها با توجه به قابلیت‌های بسیار زیاد مانند: دقت بالا، سرعت زیاد، قابلیت ذخیره‌سازی حجم زیاد اطلاعات، دسترسی آسان و محاسن بی‌شمار دیگر امکانات بسیاری را در اختیار بشر قرار داده است (جباری، ۱۳۹۵). به دنبال گسترش و بسط فضای مجازی و افزایش دسترسی به آن میل و اشتیاق و تنوع استفاده از آن نیز افزایش یافته است. این تمایل که با سرعت قابل توجهی در حال افزایش است؛ اگرچه زمینه مشارکت جوامع را در فرایند اقتصاد داده‌پردازی فراهم می‌سازد؛ اما در عین حال شرایط و بستر مساعدی نیز برای ظهور پدیده‌های نوین بزهکاری به وجود آورده است (مرعشیان و کشفی، ۱۳۹۵).

طی مطالعه‌ای که در سطح مدارس توسط راسکوداس و استولتز (۲۰۰۷) انجام شده حدود ۴۹٪ از دانش آموزان رده سنی ۱۳ تا ۱۸ سال بزه‌دیده سایبری و ۲۱٪ از آن‌ها مجرمین سایبری بوده‌اند. محققین معتقدند که زنان بیشتر در مزاحمت‌های

سایبری نقش دارند تا مردان چراکه مزاحمت سایبری نوع ارتباطی مزاحمت است که بیشتر توسط دختران صورت می‌گیرد.

طبق گزارش سال ۱۳۹۷ مرکز مبارزه با جرایم سایبری، تنها در سال ۱۳۹۷ میزان یک تریلیارد و ۱۰ میلیارد تومان خسارت ناشی از برداشت‌های غیرمجاز می‌باشد که پرونده‌های آن مختومه شده است. جرایم بزهکاری در فضای سایبری یکی از این پدیده‌های نوین تلقی می‌شود. در حال حاضر جرایم و تهدیدهای سایبری به عنوان یکی از دغدغه‌های بزرگ هزاره سوم میلادی امنیت کاربران فضای مجازی در سراسر دنیا را به مخاطره انداخته است (لاندول و همکاران، ۲۰۱۵). هرگونه رفتار غیرقانونی که به وسیله سیستم‌ها و شبکه‌های کامپیوتری انجام می‌شود جرایم سایبری گفته می‌شود (رجب پور و همکاران، ۱۳۹۲).

به هر رفتار غیرقانونی که با استفاده از وسایل الکترونیکی ایجاد می‌شود و امنیت سیستم‌های کامپیوتری و اطلاعات پردازش شده آن‌ها را مورد هدف قرار می‌دهد جرایم سایبری گفته می‌شود (کمال، ۲۰۰۵). با افزایش استفاده از فناوری‌های اطلاعاتی تهدیدهای امنیتی آن‌ها نیز متنوع تر و جدی تر می‌گردند به همین منظور، امنیت سایبری اهمیت دوچندانی برای تصمیم‌گیران در سطح ملی پیدا کرده است (ITU، ۲۰۱۸).

مزاحمت سایبری ارسال پیام‌های تهدیدآمیز برای قربانیانیا استفاده از فناوری‌های دیجیتال به شیوه‌ای که مشکلات روانی و اجتماعی برای افراد ایجاد کند. مزاحمت‌های سایبری توسعه یافته مزاحمت‌های سنتی در جامعه می‌باشند که با ابزارهای الکترونیکی چون دستگاه‌های موبایل، بلاگ‌ها، وب سایت‌ها و اتاق‌های گفتگو صورت می‌گیرد. علیرغم اینکه در مزاحمت‌های سنتی مجرم و قربانی یکدیگر را می‌شناختند در مزاحمت‌های سایبری، معمولاً مجرم، قربانی را می‌شناسد ولی قربانی شناختی از مجرم

ندارد. پرواضح است که کنترل و مدیریت جرایم سایبری با چنین ویژگی هایی بسیار دشوار می باشد.

یکی از عوامل اصلی بروز جرایم سایبری و در نتیجه بزه‌دیدگی عدم اطلاع و آموزش کافی بزه دیدگان می باشد. به منظور توسعه برنامه‌های آموزشی می‌بایست حوزه‌های آسیب پذیری و بزه‌دیدگی افراد در فضای سایبر شناسایی شود و سپس اقدامات لازم جهت ارتقای آگاهی آن‌ها صورت گیرد. از طرف دیگر، ایجاد مراکزی جهت گزارش دهی افرادی که بزه‌دیدگان سایبری بوده اند، تسهیل کننده توسعه استراتژی‌های مناسب برای ایجاد امنیت سایبری می باشد. لذا شناسایی حوزه‌های اولویت دار بزه‌دیدگی سایبری می‌تواند به کشورها در جهت اثربخشی سرمایه گذاری‌های حوزه امنیت سایبری و ارتقای ایمن سازی این فضا کمک کند. به عبارت دیگر، راهکارهای ارتقای امنیت سایبری مستلزم شناخت کافی از مصادیق بزه‌دیدگی‌های سایبری می باشد که با وجود اهمیت آن، هنوز شکاف تحقیقاتی در کشور از نظر آگاهی، درک، سنجش بزه‌دیدگی سایبری وجود دارد. باید بیان کرد که جرایم سایبری در کشورهای مختلف با توجه بسترهای فرهنگی و اجتماعی متفاوت نیاز به ابزارهای بومی شده ای برای سنجش بزه‌دیدگی سایبری می‌باشند، لذا مسئله اصلی پژوهش حاضر توسعه مقیاس و ابزار سنجش بزه‌دیدگی سایبری در کشور ایران با توجه به بستر فرهنگی، اجتماعی و قانونی متفاوت از سایر کشورهای می باشد.

۲. روش تحقیق

هدف اصلی پژوهش حاضر توسعه مقیاس سنجش بزه‌دیدگی سایبری در ایران می باشد. این پژوهش به لحاظ هدف کاربردی و از نظر نحوه گردآوری اطلاعات از نوع توصیفی-پیمایشی می باشد. دستیابی به هدف پژوهش در دو مرحله صورت گرفته است:

در این پژوهش، به منظور طراحی مقیاس سنجش بزه‌دیدگی سایبری، در مرحله‌ی اول، قانون جرایم سایبری و نیز ادبیات حوزه بزه‌دیدگی سایبری مورد بررسی جامع قرار گرفت و ابعاد و مصادیق بزه‌دیدگی سایبری شناسایی و استخراج شدند. در این مرحله یک گروه کانونی متشکل از ۵ متخصص و صاحب‌نظر حوزه حقوقی، فناوری اطلاعات، و همچنین علوم انتظامی که دارای تجربه کاری و یا آکادمیک در حوزه مورد بررسی بوده و دارای کتاب، مقاله، پایان‌نامه مرتبط با حوزه پژوهش بودند و همچنین حاضر به مشارکت در جلسه مباحثه در رابطه با ابزار توسعه بزه‌دیدگی سایبری بودند برای اصلاح و اغنای بیشتر ابزار اولیه تشکیل شد تا در صورت لزوم مصادیقی حذف یا اضافه شوند و در نهایت این مصادیق بزه‌دیدگی طبقه‌بندی شوند. بدین طریق مصادیق‌بازار پیشنهادی اولیه در قالب ۴ بعد، شاخص ارائه گردید.

در مرحله دوم تلاش شد تا با استفاده از روش میدانی به ارائه پرسشنامه محقق ساخته به کاربران اینترنتی در استان قم جهت اعتبارسنجی ابعاد و مصادیق بزه‌دیدگی مطرح شده در ابزار توسعه یافته پرداخته شود. معیار انتخاب افراد برای مشارکت در پژوهش در این مرحله عبارت بودند از: بازه سنی بین ۱۹ تا ۴۰ سال که بیشترین احتمال را برای بزه‌دیدگی سایبری دارا می‌باشند، کاربر اینترنت بودن و در محدوده استان قم بودن. این مرحله برای اعتبارسنجی چارچوب طراحی شده صورت گرفت. برای سنجش سؤالات پرسشنامه در رابطه با وجود ابعاد و شاخص‌ها در این چارچوب از طیف لیکرت (خیلی کم تا خیلی زیاد) استفاده شده‌است.

به منظور سنجش روایی ابزار پژوهش، پرسشنامه در اختیار تنی چند از اساتید دانشگاه قرار گرفت و برخی اصلاحات نوشتاری و مفهومی در آن ایجاد شد. علاوه بر روایی محتوا از روایی سازه با استفاده از تحلیل عاملی تایید نیز برای ارزیابی روایی ابزار مورد استفاده بهره گرفته شده که نتایج آن در یافته‌ها بیان شده است. برای سنجش

پایایی نیز از آلفای کرونباخ استفاده شده است که نتایج محاسبه ی آلفای کرونباخ برای ابعاد و شاخص های پرسشنامه در جدول ۲ ارائه گردیده است.

جدول ۲: ضریب آلفای کرونباخ برای ابعاد بزه‌دیدگی سایبری

آلفا کرونباخ	تعداد شاخص	بعد بزه‌دیدگی سایبری
۰.۷۵۳	۱۰	اجتماعی
۰.۸۵۸	۷	اقتصادی
۰.۷۳۷	۶	اخلاقی
۰.۷۹۳	۳	سیاسی

همانطور که در جدول بالا آمده است، تمامی ابعاد پرسش نامه دارای پایایی بیش از مقدار قابل قبول ۰.۷ (نیوکِرک و لدرر^۱، ۲۰۰۶) بوده‌اند. برای مجموعه سؤالات پرسشنامه نیز مقدار آن ۰.۹ بوده است که نشان دهنده پایایی بالای آن می‌باشد. سؤالات پرسشنامه در پیوست مقاله آورده شده است.

۳. پیشینه پژوهش

۳-۱. فضای سایبری و آمار و ارقامی در رابطه با اهمیت آن

فضای سایبری محیطی است که در مقابل فضای واقعی و فیزیکی قرار دارد و دارای ماهیتی خاص و پیچیده بوده، که در آن، سیستم‌های فیزیکی و ملموس، اطلاعات، محتوا و داده‌هایی وجود دارند که کاملاً ناملموس و غیر واقعی هستند. فضای مجازی علاوه بر اینکه موجب رشد و توسعه هر چه بیشتر پیشرفت‌های بشر در زمینه‌های

گوناگون علمی، اقتصادی، اجتماعی و... شده است؛ مخاطرات و تهدیداتی نیز به همراه داشته است (گلن، ۲۰۱۴).

فضای مجازی با تمام ویژگی‌های خود هر روزه تعداد بیشتری از افراد را جذب می‌نماید که در ادامه تعداد کاربران کل فضای مجازی در دنیا در شکل ۱ نشان داده شده است.



شکل ۱. وضعیت دیجیتال در جهان (یوروپول، ۲۰۱۸)

در ایران نیز میزان نفوذ اینترنت بیش از ۶۹٪ شده است که از این میان بیش از ۴۰ میلیون (۴۹٪) کاربر فعال شبکه‌های اجتماعی هستند (یوروپول، ۲۰۱۸).

فضای سایبری قابلیت‌ها و امکانات شگفت‌انگیزی ایجاد نموده است که باعث جذب میلیون‌ها کاربر در سراسر دنیا شده است و تعداد کاربران آن روزانه در حال افزایش است که محیط مناسبی برای افراد سودجو جهت ارتکاب جرایم سایبری شده است. با توجه به نرخ نفوذ اینترنت و نیز رشد تنوع بزهکاری‌های اینترنتی، توجه به بزهکاری‌ها و بزه‌دیدگی‌ها در محیط سایبری در اولویت‌های تصمیم‌گیرندگان در سطح بین‌المللی قرار گرفته است.

۲-۳. مفهوم بزه‌دیده و بزه‌دیدگان سایبری

واژه بزه‌دیده معادل واژه انگلیسی "*Victim*" به شخصی گفته می‌شود که به‌دنبال رویداد یک جرم، آسیب و زیان می‌بیند. این واژه در نوشتگان فارسی به معنای "قربانی" به کار رفته است. درنوشتگان علوم جنایی هرگاه این آسیب از رفتار مجرمانه انسان برخاسته باشد به فرد زیان‌دیده "قربانی جرم" یا "بزه‌دیده" می‌گویند (مالمیر و زرخ، ۱۳۸۹).

مطابق ماده ده آیین دادرسی کیفری بزه‌دیده کسی است که از وقوع جرم متحمل ضرر و زیان می‌گردد (اسلامی، ۱۳۹۵). بزه‌دیدگی در مقابل جرم نیست. مجرم بودن به سادگی قابل تشخیص است: ارتکاب عملی که توسط قانونگذار جرم شناخته شده است؛ لکن بزه‌دیدگی یک واقعیت اجتماعی، زیستی و روانی است که توسط آسیب‌پذیری یک فرد و به وسیله آنچه که متحمل شده می‌تواند مشخص گردد هرچند که این امر به یک جرم مربوط نباشد. بزه‌دیدگی مستلزم یک رنج است، گاهی اوقات بزه‌دیدگی به سبب یک رفتار اجتماعی محرک روی می‌دهد. به عنوان مثال می‌توان از میل به سریع راندن اتومبیل، حوادث کار، استعمال دارو ها، الکل و غیره نام برد. مسئله بزه‌دیدگی همانند بیماری‌ها و اپیدمی‌ها پیچیده و خطرناک است (کتاب بزه‌دیدگی).

تعریف علمی بزه‌دیده به طور دقیق تر در سال ۱۹۷۶ صورت گرفت. لفظ "بیمار" و "بزه‌دیده" هر دو معنای رنج را القا می‌کنند. مندلسون با تبیین محتاطانه تفاوت این دو بزه‌دیده را اینگونه تعریف می‌کند: "شخصی مستقل یا متعلق به یک مجموعه که متحمل آثار دردناک برخی عوامل شده که این عوامل دارای ریشه‌های مختلف فیزیکی، روانی، اقتصادی، سیاسی، اجتماعی و طبیعی می‌باشد.

با توسعه روبه رشد فضای سایبری، این فضا مورد تهاجم مجرمان سایبری و به تبع آن بزه‌دیدگان سایبری واقع شده است. روزانه هزاران نفر در جهان به دلیل اینکه

آگاهی چندانی از جرائم سایبری و نحوه وقوع آن‌ها ندارند؛ قربانی جرائم در فضای مجازی می‌گردند (گرنٹ، ۲۰۱۵).

مزاحمت سایبری به عنوان استفاده تکراری فناوری اطلاعات با هدف بدخواهی توسط فرد یا گروهی برای تهدید دیگران می‌باشد. در فضای سایبری امکان گمنامی مجرم برای قربانی و مشاهده کنندگان وجود دارد (ستین و همکاران، ۲۰۱۱). افرادی که هدف مزاحمت‌های سایبری می‌باشند به عنوان بزه دیدگان سایبری شناخته می‌شوند (بروان و همکاران، ۲۰۱۴). به افرادی که با استفاده وسایل الکترونیکی از قبیل: ایمیل، پیام‌های فوری و... مورد حمله قرار می‌گیرند بزه‌دیده سایبری گفته می‌شود (فنیستین و همکاران، ۲۰۱۴). بزه‌دیده سایبری فردی است که در فضای مجازی توسط رفتار منفی دیگران مورد هدف قرار گرفته و خساراتی بر او تحمیل می‌گردد (رایت، ۲۰۱۵).

بروان و همکاران (۲۰۱۴) بیان می‌کنند که تعریف استاندارد از بزه‌دیدگی سایبری وجود ندارد ولی تمامی آن‌ها حاوی عناصری در رابطه با آسیب‌هایی هدفمند و تکرارشونده از طریق استفاده از فناوری می‌باشند. مزاحمت سایبری آسیب‌های هدفمند برای تهدید افراد یا گروه‌هایی از طریق فناوری اطلاعات تعریف شده است.

۳-۳. انواع بزه‌دیدگان سایبری

برای تقسیم‌بندی بزه‌دیدگان معیارهای متفاوتی اراده شده است. در برخی مواقع تقسیم‌بندی بر مبنای معیارهای جنسیت، وضعیت ظاهری، ویژگی‌های فردی و... انجام شده است. آنچه بیشتر از همه توجه جرم‌شناسان را به خود جلب کرده است؛ تقسیم‌بندی بر مبنای نقش و مسئولیت بزه‌دیدگان است. ما نیز در این متن برآنیم تا انواع بزه‌دیدگان سایبری را بر اساس نقش و مسولیتشان طبقه‌بندی کنیم. بزه‌دیدگان را

با توجه به میزان تقصیرشان به دو دسته کلی تقسیم می‌شوند که در ادامه به بررسی هریک از آن‌ها می‌پردازیم.

۱-۳-۳. بزه‌دیدگان با کمینه تقصیر

میزان آگاهی کاربران در بزه‌دیدگی آنان نقش تعیین‌کننده‌ای دارد. آگاهی یا ناآگاهی قربانیان می‌تواند عامل مؤثری در وقوع جرم و تحقق بزه‌دیدگی افراد باشد.

- **بزه‌دیدگان آگاه:** این دسته از بزه‌دیدگان با آنکه می‌دانند رفتارشان پرخطر است و در اثر آن چه عواقب خطرناکی محقق خواهد شد؛ باز هم مرتکب آن رفتار می‌شوند که در نتیجه منجر به تحقق جرم و بزه‌دیدگی خود می‌شوند (مالمیر و زرخ، ۱۳۸۹).

- **بزه‌دیدگان ناآگاه:** فضای سایبر یک فضای مدرن است و کار با این فضا نیاز به آگاهی و دانش رایانه‌ای دارد. اما متأسفانه بسیاری از کاربران فضای سایبر فاقد دانش کافی برای ورود به این دنیای مجازی هستند. در نتیجه به علت فقدان آگاهی، ناخواسته موجبات تحقق جرم و بزه‌دیدگی خویش را فراهم می‌کنند (حسینی، ۱۳۹۵).

۲-۳-۳. بزه‌دیدگان با بیشینه تقصیر

در این نوع تقسیم‌بندی بی‌احتیاطی و سهل‌انگاری عاملی برای در نظر گرفتن بیشترین میزان تقصیر تلقی می‌شود که در ادامه به بررسی آن‌ها پرداخته خواهد شد.

- **بزه‌دیده بی‌احتیاط:** بزه‌دیده بی‌احتیاط فردی است که مراتب احتیاط را رعایت نکرده و توجه و دقت کافی هنگام کار با رایانه در فضای سایبر را مدنظر

قرار نمی‌دهد. در واقع این دسته از افراد بی‌احتیاطی و حتی سهل‌انگاری‌شان منجر به بزه‌دیدگی آن‌ها می‌شود (میر، ۱۳۹۴).

- **بزه‌دیده طماع:** منظور از بزه‌دیدگان طماع افراد حریص و طمع‌کاری است که به خیال دستیابی به پول بیشتر، شارژ بیشتر و یا دستیابی به تسهیلات فوق‌العاده فریب تبلیغات دروغین و آگهی‌های وسوسه‌انگیز را خورده و به راحتی مدارک و یا اطلاعات حساس و محرمان خود از قبیل شماره ملی، شماره کارت، رمز عبور و... را به راحتی در اختیار بیگانگان قرار می‌دهند، در این دسته از بزه‌دیدگان حرص و طمع زمینه بزه‌دیدگی آنان را فراهم کرده است (مالمیر و زرخ، ۱۳۸۹).

۳-۴. تحقیقات حوزه بزه‌دیدگی سایبری

آریکاک و همکاران (۲۰۰۸) رفتارهایی چون شایع پراکنی، توهین کردن، تهدید کردن، انتشار عکس کسی بدون اجازه او و تمسخر فرد را از جمله انواع رفتارهای مزاحمت سایبری بیان می‌کند. لی (۲۰۰۵) نیز ابزاری را برای سنجش مزاحمت سایبری با ۱۵ آیتم توسعه داده است معمولاً این ابزارها از سؤالات بله و خیر استفاده می‌کنند. در تحقیق لی (۲۰۰۵) بیشترین آسیب دیدگی سایبری از طریق ایمیل و پیام فوری صورت گرفته بوده است و اینترنت و اتاق‌های گفتگو در رتبه‌های بعدی آسیب‌رسانی به بزه‌دیدگان بوده‌اند. اسمیت و همکاران (۲۰۰۶) به دسته بندی هفتگانه از مزاحمت‌های سایبری پرداخته است که عبارتند از: مزاحمت پیام متنی، مزاحمت تصویری و ویدئویی، مزاحمت تماس تلفنی، مزاحمت ایمیلی، مزاحمت چت روم، مزاحمت پیام فوری و مزاحمت از طریق سایت. کوالمسکی و لیمبر (۲۰۰۷) بزه‌دیدگی سایبری با شاخص‌هایی چون آسیب دیدگی از طریق پیام فوری، آسیب دیدگی از طریق اتاق گفتگو، آسیب دیدگی از طریق وب سایت، آسیب دیدگی از طریق ایمیل، آسیب دیدگی از طریق پیام

متنی مورد سنجش واقع شده است. اردور بیکر و کاوسوت (۲۰۰۷) برای اولین باز پرسشنامه مزاحمت سایبری را توسعه داده است که این پرسشنامه حاوی دویخش موازی می‌باشد: یک بخش برای مزاحمت سایبری حاوی ۱۶ سؤال و یک بخش دیگر برای بزه‌دیدگی سایبری شامل ۱۸ سؤال می‌باشد.

بروان و همکاران (۲۰۱۴) برای سنجش بزه‌دیدگی سایبری از ابزار محقق شامل ۲۰ آیتم استفاده کرده است که از پژوهش‌های کوالمسکی و لیمبر (۲۰۰۷) و هیندوجا و پتچین (۲۰۰۹) بهره گرفته است. در پژوهش آن‌ها هدف بررسی تأثیر جنسیت، تحصیلات و نژاد بر میزان بزه‌دیدگی سایبری بوده است که با نتایج بزه‌دیدگی ستنی مقایسه شده است.

آیاس و هورزوم (۲۰۱۰) ابزاری را برای مزاحمت سایبری توسعه داده است که میزان اقدامات یا در معرض اقدامات مزاحمت‌های سایبری را اندازه‌گیری می‌کند. شاخص‌های ابزار توسعه یافته آن‌ها در رابطه با سه حوزه، موضوعات مزاحمت/بزه‌دیدگی جنسی، مزاحمت/بزه‌دیدگی آزار و اذیت، مزاحمت/بزه‌دیدگی انتشار شایعه و توهین در فضای سایبری بوده است.

ستین و همکاران (۲۰۱۱) در پژوهشی به توسعه ابزار تعیین میزان بزه‌دیدگی سایبری و رفتارهای مزاحمتی سایبری پرداخته‌اند. در مطالعه آن‌ها ۴۰۴ دانشجو مشارکت داشته اند که ۲۵۰ مرد و ۱۵۴ زن نمونه آماری آن‌ها را تشکیل داده است. میانگین سنی آن‌ها ۱۶.۶۸ سال بوده و دانش آموزان دوره دبیرستان بوده‌اند. ابزار آن‌ها شامل ۳ عامل اصلی و ۲۲ شاخص بوده است که برای سنجش میزان بزه‌دیدگی سایبری و مزاحمت سایبری مورد استفاده قرار می‌گیرد. جدول ۱ ابزار سنجش بزه‌دیدگی سایبری ستین و همکاران (۲۰۱۱) را نشان می‌دهند.

جدول. ابزار سنجش بزه‌دیدگی سایبری (ستین و همکاران، ۲۰۱۱)

ابعاد	شاخص
مزاحمت زبانی سایبری ^۱	شایعه پراکنی در اینترنت استفاده از نام مستعار در اینترنت با هدف مزاحمت استفاده از نمادهای توهین‌آمیز در اینترنت تمسخر افراد در اینترنت شوخی و استهزای اطلاعات به اشتراک گذاشته شده در اینترنت ارائه نظرات توهین‌آمیز در اخبار منتشر شده در وب سایت استفاده از عبارات تحقیرآمیز در اینترنت
پنهان کردن هویت ^۲	استفاده از هویت فرد دیگری بدون اجازه او در اینترنت مخفی‌سازی هویت در اینترنت ورود به صفحه شخصی فرد دیگری بدون اجازه او در اینترنت هک کردن صفحه شخصی فرد دیگری بدون اجازه او ارسال فایل/برنامه ویروسی از طریق ایمیل
جعل سایبری ^۳	اشتراک ویدئو بدون اجازه در اینترنت اشتراک عکس‌های فرد بدون اجازه در اینترنت ویرایش عکس‌ها به شیوه اهانت‌آمیز در اینترنت مجبور کردن به صحبت در رابطه با مسائل جنسی در اینترنت استفاده از سمبل‌های جنسی حین گفتگو در اینترنت اشتراک تصاویری با محتوای جنسی در اینترنت استفاده از زبان توهین‌آمیز و سواستفاده در ایمیل استفاده از اینترنت به عنوان ابزاری برای تهمت زدن استفاده از اینترنت به عنوان یک ابزار تبلیغاتیبه نفع خود استفاده از اینترنت برای اقدامات کلاهبردانه

1. Cyber verbal bullying

2. Hiding identity

3. Cyber forgery

پرسشنامه‌ها و پیمایش‌های صورت گرفته در حوزه سنجش مزاحمت سایبری یا بزه‌دیدگی سایبری حاوی معیارهای قابل اطمینان و اثربخشی برای پدیده مورد نظر نمی‌باشند و نیاز برای توسعه ابزار سنجش مزاحمت و بزه‌دیدگی سایبری با مرور ادبیات در این حوزه آشکار است. غالب ابزارهای سنجش تنها یک یا ابعاد محدودی از بزه‌دیدگی سایبری را در نظر گرفته است؛ درحالی‌که مزاحمت سایبری دربرگیرنده طیف وسیعی از اقدامات شامل قصد مزاحمت و آسیب رساندن به روابط اجتماعی چون انتشار شایعه، توهین به افراد تا اقداماتی چون کلاهبرداری، استفاده از اینترنت برای ترویج مسائل جنسی بین افراد می‌باشد.

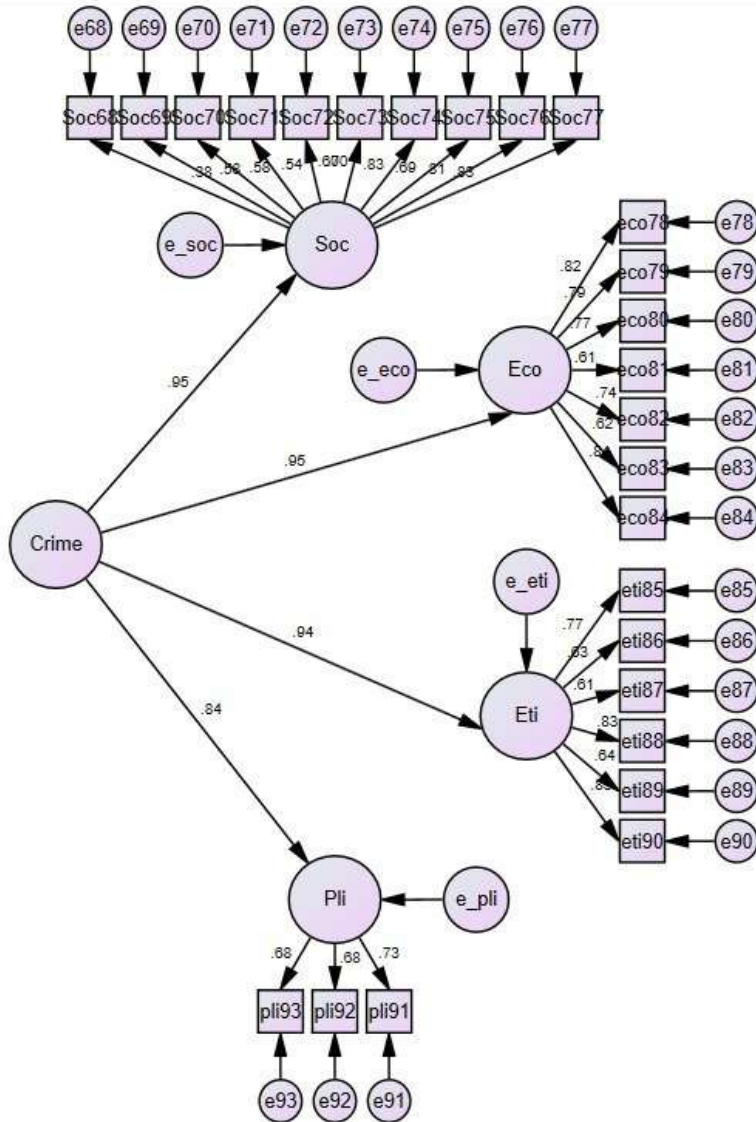
۴. یافته‌ها

آمار توصیفی متغیرهای جمعیت شناختی نشان می‌دهد از بین پاسخ دهندگان به این سؤال ۶۸.۵٪ درصد زن و ۳۱.۵٪ درصد مرد هستند، بیشتر از ۸۲.۲۸٪ دارای مدرک کارشناسی و بالاتر بوده‌اند. حدود ۱۷.۷٪ درصد دارای تحصیلات کاردانی و پایین تر، ۳۸٪ درصد دارای تحصیلات لیسانس، ۳۸.۵٪ درصد دارای تحصیلات فوق لیسانس و ۵.۸۳٪ درصد دارای تحصیلات دکتری بوده‌اند. از بین پاسخ دهندگان ۲۴.۴۸ درصد پاسخ دهندگان بین ۱۹ تا ۲۵ سال، ۳۹.۸۶ درصد دارای سن بین ۲۵ تا ۳۰ سال و ۳۵.۶۶ درصد دارای سن بین ۳۱ تا ۴۰ سال بوده‌اند.

قبل از بررسی برازش مدل‌های اندازه‌گیری و معناداری بارهای عاملی، باید شاخص‌های کفایت نمونه‌گیری مورد بررسی قرار می‌گیرد. جهت بررسی شاخص‌های کفایت نمونه‌گیری از دو شاخص *KMO* و آزمون بارتلت استفاده می‌شود. شاخص *KMO* برای داده‌های گردآوری شده ۰.۹۳ بدست آمده است که نشان دهنده اینست که داده‌های مورد نظر برای تحلیل عاملی مناسب هستند. معنی‌داری در آزمون بارتلت (*sig*)

شکل ۲. نتایج حاصل از تحلیل عاملی تایید برای سازه بزه‌دیدگی سایبری را نشان می‌دهد. به منظور اعتبارسنجی ابزار توسعه یافته از تحلیل عاملی و نرم‌افزار آموس بهره گرفته شده است. (= 0.000) نیز کوچکتر از ۵٪ باشد تحلیل عاملی برای شناسایی ساختار مناسب است.

شکل ۲. نتایج حاصل از تحلیل عاملی تایید برای سازه بزه‌دیدگی سایبری را نشان می‌دهد.



در نهایت برای تست برازش مدل که به بررسی پذیرش یا رد مدل می‌پردازد از شاخص‌های NFI ، JFI ، RFI و CFI بهره گرفته شده است که به ترتیب ۰.۹۹۱، ۰.۹۹۳، ۰.۹۷۲ و ۰.۹۹۳ می‌باشند و تمامی شاخص‌های برازش مدل اندازه‌گیری بزه‌دیدگی از مقدار قابل قبول بالاتر بوده است. برای ارزیابی روایی همگرا از دو شاخص پایایی ترکیبی و میانگین (CR) واریانس استخراجی (AVE) بهره گرفته شد که نتایج برای هر یک از ابعاد بزه‌دیدگی سایبری به تفکیک جدول زیر آورده شده است. جدول ۳ نتایج مربوط به بارعاملی و متغیرهای توصیفی متغیرها را نشان می‌دهد.

جدول ۳: بارعاملی و متغیرهای توصیفی

میزان بزه‌دیدگی	ضریب پایایی ترکیبی (CR)	میانگین واریانس استخراجی (AVE)	واریانس	میانگین	بارهای عاملی استاندارد شده	کدها	بعد
۶۲.۵٪	۰.۸۸۵	۰.۴۴۶	۰.۸۷۳	۱.۶۶	۰.۴	Soc68	اجتماعی
			۰.۵۹۸	۱.۲۵	۰.۵۸۴	Soc69	
			۰.۶۶۴	۱.۳	۰.۵۷۷	Soc70	
			۰.۷۵۵	۱.۴۱	۰.۵۴۴	Soc71	
			۰.۶۷	۱.۳۱	۰.۶۰۱	Soc72	
			۰.۵۲	۱.۱۵	۰.۶۹۹	Soc73	
			۰.۳۷۴	۱.۰۷	۰.۸۳۵	Soc74	
			۰.۵۱	۱.۱۷	۰.۶۸۶	Soc75	
			۰.۵۶۲	۱.۱۷	۰.۸۰۵	Soc76	
			۰.۴۶۴	۱.۱۲	۰.۸۲۷	Soc77	
۳۲.۶٪	۰.۸۹۷	۰.۵۵۸	۰.۵۰۵	۱.۱۳	۰.۸۲	Eco78	اقتصادی
			۰.۳۸	۱.۰۷	۰.۷۹۳	Eco79	
			۰.۳۸۴	۱.۰۷	۰.۷۷۵	Eco80	
			۰.۶۶۱	۱.۲۹	۰.۶۱۵	Eco81	
			۰.۴۶۲	۱.۱۳	۰.۷۳۸	Eco82	
			۰.۷۴	۱.۳۱	۰.۶۲	Eco83	
			۰.۵۲	۱.۱۱	۰.۸۳۵	Eco84	

۰.۴۴.۵	۰.۸۶۷	۰.۵۲۴	۰.۴۶۳	۱.۱	۰.۶۰۶	<i>Eti85</i>	اجتماعی
			۰.۸۴۵	۱.۴۴	۰.۸۲۷	<i>Eti86</i>	
			۰.۷۳۳	۱.۳۱	۰.۶۴۲	<i>Eti87</i>	
			۰.۵۰۵	۱.۱۲	۰.۸۲۷	<i>Eti88</i>	
			۰.۷۳	۱.۳۵	۰.۶۴۲	<i>Eti89</i>	
			۰.۵۱۹	۱.۱۵	۰.۸۲۷	<i>Eti90</i>	
۰.۲۸.۴	۰.۷۴۱	۰.۵	۰.۵۳۴	۱.۱۷	۰.۷۳	<i>Pli91</i>	سیاسی
			۰.۸	۱.۳۹	۰.۶۸۳	<i>Pli92</i>	
			۰.۵۴۳	۱.۱۴	۰.۶۸	<i>Pli93</i>	

همانطور که در جدول آمده است تمامی بارهای عاملی بالاتر از حد قابل قبول ۰.۴ می‌باشند و مورد تایید قرار گرفتند. علاوه بر معناداری بارهای عاملی مربوط به شاخص‌های بزه‌دیدگی، از ضریب پایایی ترکیبی (*CR*) و شاخص میانگین واریانس استخراجی (*AVE*) برای ارزیابی روایی همگرا بهره گرفته شده است.

این معیار نشان دهنده میانگین واریانس به اشتراک گذاشته شده بین هر سازه با شاخص‌های خود می‌باشد. به بیان ساده، این معیار میزان همبستگی یک سازه با شاخص‌های خود را نشان می‌دهد و هرچه بیشتر باشد برازش بیشتر است.

مقدار بحرانی *AVE* ۰.۵ می‌باشد که در پژوهش هوانگ و همکاران (۲۰۱۳) بالای ۰.۴ نیز قابل قبول است و نشان دهنده روایی همگرایی قابل قبولی می‌باشد. برای ارزیابی پایایی سازه علاوه بر آلفای کرونباخ از *CR* که معیار مدرن تری می‌باشد نیز بهره گرفته شده است.

همانطور که در جدول آمده، برای تمامی ابعاد بیشتر از حد قابل قبول ۰.۷ می‌باشد. بیشترین میزان بزه‌دیدگی مربوط به بزه‌دیدگی اجتماعی و کمترین میزان بزه‌دیدگی سایبری مربوط به بزه‌دیدگی سیاسی می‌باشد.

۵. نتیجه‌گیری

به دلیل پنهان بودن هویت فرد توسط ابزارهای فناوری اطلاعات، استفاده از فضای سایبری برای مجرمین جذابیت زیادی پیدا کرده است و میزان بزه‌دیدگی‌های سایبری روز به روز در حال افزایش می‌باشد (ستین و همکاران، ۲۰۱۱). از آنجا که تحقیقات در حوزه بزه‌دیدگی سایبری در مراحل اولیه می‌باشند (بروان و همکاران، ۲۰۱۴)، درک روشنی از ابعاد بزه‌دیدگی سایبری وجود ندارد و یکی از الزامات توسعه امنیت سایبری وجود ابزاری برای سنجش بزه‌دیدگی سایبری می‌باشند تا با استفاده از آن حوزه‌های اولویت دار شناسایی شده و تدابیر امنیتی لازم و آموزش مهارت‌های سایبری مورد نیاز صورت گیرد. از آنجا که جرایم سایبری با توجه به قوانین حاکم بر کشورها با یکدیگر متفاوت است مصادیق بزه‌دیدگی و ابزار سنجش آن نیز متفاوت خواهد بود که در ایران تاکنون پژوهشی به توسعه مقیاس سنجش بزه‌دیدگی سایبری نپرداخته است که هدف اصلی پژوهش حاضر بوده است.

به همین منظور در مرحله اول، همراه با بررسی جامع قانون جرایم سایبری و ادبیات حوزه مربوطه با استفاده از نظرات گروه کانونی به استخراج ابزار سنجش بزه‌دیدگی سایبری مبادرت ورزیده شد و در مرحله دوم، با استفاده از روش پیمایش به اعتبارسنجی ابزار توسعه یافته پرداخته شده است.

ابزار توسعه سنجش بزه‌دیدگی سایبری پیشنهادی دارای چهاربعد اجتماعی، اقتصادی، اخلاقی و سیاسی می‌باشد.

- با توجه به یافته‌های پژوهش به کشورها جهت کاهش میزان بزه‌دیدگی سایبری پیشنهادات زیر ارائه می‌شود:

- ایجاد مراکز پایش بزه‌دیدگی سایبری و بکارگیری ابزار توسعه یافته جهت توسعه نقشه بزه‌دیدگی کشور
- بکارگیری ابزارسنجش جامع جهت درک و شناخت حوزه هایی با بزه‌دیدگی بالاتر برای توسعه دوره‌های مهارت‌های سایبری
- بهره‌گیری از ابزار توسعه یافته برای شناخت شکاف‌های امنیتی و اتخاذ تصمیمات اثربخش در حوزه امنیت سایبری

در ادامه نیز باید بیان کرد، یافته‌های هر پژوهشی باید بتواند راه‌پایا برای مطالعات کمیوکیفی پس از خود باز کند، از این رو با توجه به بر خیزان نتایج هم‌موجدید پژوهش حاضر، به محققان آتی پیشنهاد می‌شود به مقایسه تطبیقی ابزارهای سنجش بزه‌دیدگی سایبری در کشورهای مختلف بر اساس قانون جرایم سایبری آن‌ها پردازند تا تفاوت‌های فرهنگی، اجتماعی و قانونی تأثیرگذار بر آن آشکار گردد. همچنین پیشنهاد می‌شود به بررسی با توجه به ظهور فناوری‌های نوین ابزار توسعه یافته را مورد بازبینی قرار دهند و مصادیق فناوری‌های نوظهور را در بزه‌دیدگی سایبری بررسی نمایند.

۶. منابع

۱. جباری، فهیمه. (۱۳۹۵). شناسایی و رتبه‌بندی عوامل تأثیرگذار بر قربانی شدن سایبری (مورد مطالعه: دانشجویان کارشناسی ارشد دانشگاه‌های غیرانتفاعی استان مازندران). پایان نامه کارشناسی ارشد، موسسه آموزش عالی نیما.
۲. حسینی، سیده سیما. (۱۳۹۵). پیشگیری پلیسی از جرایم سایبری. پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی.
۳. رجب پورکاشف، مهدی؛ سالمی، نیلوفر (۱۳۹۲). نگاهی به جرایم سایبری با تأکید بر ضرورت تدوین قوانین مناسب به عنوان راهکاری برای مقابله با آن، همایش ملی مهندسی کامپیوتر و توسعه پایدار با محوریت شبکه‌های کامپیوتری، مدل سازی و امنیت سیستم ها.

۴. مالمیر، محمود؛ زرخ، احسان. (۱۳۸۹). پیشگیری از بزه‌دیدگی سایبری. فصلنامه مطالعات پیشگیری از جرم، ۵(۱۷)، ص ۵۹-۸۶.
۵. مرعشیان، زینب سادات؛ کشفی‌سیدسعید. (۱۳۹۵). عوامل مرتبط با بزهکاری زنان در فضای سایبری با تأکید بر اعتیاد به اینترنت. فصلنامه زن و فرهنگ، ۸(۳۰)، ص ۹۱-۱۰۲.
۶. میر، فاطمه. (۱۳۹۴). نقش بزه‌دیده در تحقق جرایم سایبری. پایان نامه کارشناسی ارشد، دانشگاه فردوسی مشهد.

7. Ahmad Kamal, (2005): "The Law of Cyber-Space. An Invitation to the Table of Negotiations". Published by United Nations Institute for Training and Research.
8. Aricak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Ciplak, S., Yilmaz, N., & Memmedov, C. (2008). Cyberbullying among Turkish adolescents. *Cyberpsychology & behavior*, 11(3), 253-261.
9. Ayas, T., & Horzum, M. B. (2010). Cyber bully/victim scale development study. *Akademik Bakis*, 19, 1-17.
10. Brown, C. F., Demaray, M. K., & Secord, S. M. (2014). Cyber victimization in middle school and relations to social emotional outcomes. *Computers in human behavior*, 35, 12-21.
11. Çetin, B., Yaman, E., & Peker, A. (2011). Cyber victim and bullying scale: A study of validity and reliability. *Computers & Education*, 57(4), 2261-2271.
12. Erdur-Baker, O., & Kavut, F. (2007). Cyber bullying: a new face of peer bullying. *Eurasian Journal of Educational Research*, 7(27), 31-42.
13. Europol, (2018), *Internet Organised Crime Threat Assessment (IOCTA) 2018*, available at: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018>, (accessed December 5, 2018).
14. Grant, H. (2015). *Social crime prevention in the developing world: exploring the role of police in crime prevention*. Switzerland: Springer.

15. Huang, C. C., Wang, Y. M., Wu, T. W., & Wang, P. A. (2013). An empirical analysis of the antecedents and performance consequences of using the moodle platform. *International Journal of Information and Education Technology*, 3(2), 217.
16. Feinstein, B. A., Bhatia, V., & Davila, J. (2014). Rumination mediates the association between cyber-victimization and depressive symptoms. *Journal of Interpersonal Violence*, 29(9), 1732-1746.
17. Glen, C. M. (2014). Internet governance: territorializing cyberspace?. *Politics & Policy*, 42(5), 635-657.
18. ITU (2018), Digital Skills Toolkit, Available at: <https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/ITU%20Digital%20Skills%20Toolkit.pdf>, (accessed December 5, 2018).
19. Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *Journal of adolescent health*, 41(6), S22-S30.
20. Landoll, R. R., La Greca, A. M., Lai, B. S., Chan, S. F., & Herge, W. M. (2015). Cyber victimization by peers: Prospective associations with adolescent social anxiety and depressive symptoms. *Journal of adolescence*, 42, 77-86.
21. Li, Q. (2005). Cyber harassment: a study of new method for an old behavior. *Journal of Educational Computing Research*, 32(3), 265–277.
22. Newkirk, H. E., & Lederer, A. L. (2006). The effectiveness of strategic information systems planning under environmental uncertainty. *Information & Management*, 43(4), 481-501.
23. Smith, P. K., Mahdavi, J., Carvalho, M., & Tippett, N. (2006). An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying. *Research Brief No. RBX03-06*. London: DfES.
24. Wright, M. F. (2015). Cyber victimization and perceived stress: Linkages to late adolescents' cyber aggression and psychological functioning. *Youth & Society*, 47(6), 789-810.

پیوست

این بخش حاوی سؤالاتی برای ارزیابی میزان بزه‌دیدگی در فضای سایبری می‌باشد. لطفاً گزینه مناسب را براساس طیف هرگز (۱)، به ندرت (۲)، گاهی اوقات (۳)، اغلب اوقات (۴)، بیشتر اوقات (۵) انتخاب نمایید.

• بزه‌دیدگی سایبری اجتماعی

۱. تاکنون بدون اجازه من داده‌های سیستم‌ام مورد دستکاری (ایجاد، حذف و یا تغییر) قرار گرفته است.
۲. تاکنون سیستم یا سامانه مورد استفاده‌ام توسط فرد دیگر یا برنامه‌های مخرب از کار افتاده است.
۳. تاکنون سیستم یا سامانه مورد استفاده‌ام توسط فرد دیگر یا برنامه‌های مخرب قفل شده یا از دسترس خارج شده است.
۴. تاکنون محتوای منتشر شده در فضای سایبری (ویدئوها، بازی‌های اینترنتی، عکس‌ها و ...) من را ترغیب به استعمال دخانیات یا مواد روان گردان کرده‌اند.
۵. تاکنون محتوای منتشر شده در فضای سایبری (ویدئوها، عکس‌ها، بازی‌های اینترنتی چون نهنگ آبی و ...) من را ترغیب به خودکشی کرده‌اند.
۶. تاکنون محتوای منتشر شده در فضای سایبری (ویدئوهای خشونت‌آمیز، بازی‌های اینترنتی خشن، عکس‌ها و ...) من را ترغیب به انجام اعمال خشونت‌آمیز کرده‌اند.
۷. تاکنون در معرض تهدیدهای سایبری (تهدیدهایی در رابطه با جان، مال و آبرو) قرار گرفته‌ام.
۸. تاکنون در معرض اخاذی سایبری قرار گرفته‌ام.

• بزه‌دیدگی سایبری اقتصادی

۱. تاکنون از حساب بانکی من برداشت اینترنتی غیرمجاز شده است.
۲. تاکنون با کارت اعتباری من در اثر اعتماد به غیر معامله باطل انجام شده است.
۳. تاکنون از طریق کارت اعتباری من پول سرقتی بدون اطلاع من جابجا شده است.
۴. تاکنون تجربه خرید از فروشگاه اینترنتی غیرمعتبر داشته‌ام.
۵. تاکنون در معرض کلاهبرداری از طریق سامانه‌های جعلی پرداخت قرار گرفته‌ام.

۶. تاکنون از طریق فضای سایبری کالای تقلبی خرید کرده‌ام.
۷. تاکنون به دلیل استفاده از سایت‌های شرط بندی و قماربازی خسارت دیده‌ام.

• بزه دیدگی سایبری اخلاقی

۱. تاکنون به دلیل استفاده از محتویات مستهجن (مصادیقی چون ربات‌های جنسی، چت سکسی، سایت‌های صیغه یابی و غیره) مورد کلاهبرداری قرار گرفته‌ام.
۲. تاکنون به استفاده از محتوای مستهجن و مبتذل منتشر شده در فضای سایبری ترغیب شده‌ام.
۳. تاکنون استفاده از محتوای منتشر شده در فضای سایبری موجب انحرافات جنسی (بچه‌بازی، میدل پوشی جنسی، خودارضایی و...) در من شده است.
۴. تاکنون فیلم خصوصی و خانوادگی من در فضای مجازی بدون اجازه‌ام منتشر شده است.
۵. تاکنون در معرض مزاحمت‌های سایبری (ارسال پیام‌های ناخواسته، درخواست دیدار با دیگری، توهین و غیره) قرار گرفته‌ام.
۶. تاکنون اعمال و گفتارهایی در فضای سایبری برخلاف واقع به من منتسب شده است.

• بزه دیدگی سایبری سیاسی

۱. تاکنون محتوای منتشر شده در فضای سایبری موجب گرایش، ترغیب و تشویق من به بی‌خدایی، فرقه‌گرایی، شیطان‌پرستی و فعالیت‌های هنجارشکن دینی شده‌اند.
۲. تاکنون اقدامات صورت گرفته توسط سلطنت طلب ها، منافقین و کانال‌های رسانه‌های ماهواره ای در فضای سایبری موجب تغییر نگرش من علیه نظام جمهوری اسلامی شده‌اند.
۳. تاکنون محتوای منتشر شده در فضای سایبری موجب ترغیب من به اعمالی علیه امنیت ملی کشور شده است.