چالش‌ها و فرصت‌های پیش روی جرم شناسی سایبری

محمود گلستانی[1]، محمد تقی پهلوانی[2]، مهدی عبدالله پور[3]

تاریخ دریافت: ۱۳۹۱/۰۶/۰۲

تاریخ پذیرش: ۱۳۹۱/۰۸/۲۳

چکیده

این مقاله ترجمه شده از اثر پژوهشی دکتر کِی. (Dr K. Jaishankar) استادیار ارشد دپارتمان جرم شناسی و عدالت کیفری دانشگاه Manonmaniam Sundaranar هندوستان و رئیس انجمن جرم شناسی و قربانی شناسی آسیای جنوبی است. در این مقاله، پدیده ای با عنوان جرایم سایبری و چالش ها و فرصت‌های پیش رو را مورد بررسی قرار می‌دهیم. امکان ناشناس باقی ماندن در اینترنت به مجرمین کمک می کند تا با پنهان کردن هویت خود به سوء استفاده از کاربران دیگر و انجام فعالیت های مجرمانه بپردازند.

واژگان کلیدی: *جرم شناسی، جرایم سایبری، امنیت سایبری.*

[1] دانشجوی دکترای حقوق بین الملل دانشگاه آزاد اسلامی واحد اصفهان، مدرس دانشگاه جامع علمی کاربردی استان سمنان و دانشگاه پیام نور واحد مهدیشهر. ایمیل: *golestani.m22@gmail.com*

[2] دانشجوی دکترای حقوق بین الملل دانشگاه آزاد اسلامی واحد کیش، وکیل پایه یک دادگستری، مدرس دانشگاه پیام نور واحد علی آباد کتول. ایمیل: *pahlevani_mohamad_t@yahoo.com*

[3] کارشناس ارشد حقوق خصوصی، وکیل پایه یک دادگستری، مدرس دانشگاه جامع علمی کاربردی استان سمنان و دانشگاه آزاد اسلامی واحد سمنان. ایمیل: *lawyer-mma@yahoo.com*

مقدمه

پا به پای پیشرفت های بشر در زمینه تکنولوژی، سهمیه خلاقیت های کامپیوتری و سایبری از همه افزون تر است. شاهد این ادعا ورود کامپیوتر در تمام فعالیت های اجتماعی، اقتصادی و حقوقی است که هر روزه می توان به راحتی آن را مشاهده نمود. این پیشرفت آنقدر در عرصه های مختلف زندگی رسوخ یافته که می توان ادعا نمود کامپیوتر از اجزای جدا نشدنی زندگی افراد در عصر حاضر شده است به گونه ای که کم کم زندگی بدون آن دشوار یا شاید ناممکن است. سرعت و گسترش ارتباطات اجتماعی در حوزه های علمی، هنری و غیره و امکان دسترسی آسان به انبوه اطلاعات فقط گوشه ای از این تکنولوژی است. از میان چهار وظیفه و قابلیت اصلی اینترنت یعنی ایجاد ارتباط، اطلاع رسانی، سرگرمی، خرید و فروش، جنبه اطلاعاتی آن مفیدترین آنها می باشد. در گذشته ای نه چندان دور نیروهای انتظامی بطور فیزیکی از افراد و اماکن محافظت و مراقبت می کردند اما ورود این تکنولوژی به زندگی انسان مخصوصاً در حوزه های اقتصادی و مالی نحوه محافظت از اموال و حتی حیثیت افراد در این فضا و تامین امنیت آنها هم به نوبه خود تغییر شکل داده است. امروز به علت ظهور جرایم سایبری و رشد روزافزون آنها همزمان با رشد و گسترش فناوری‌های نوین، دغدغه نظام‌های مختلف جوامع بشری نیز گسترش پیدا کرده است. در یک فرایند کلی از تعاریف ارائه شده در خصوص جرم شناسی سایبری و مطابقت آنها با مقاله پیش روی می‌توان گفت: جرم‌شناسی سایبری مطالعه عوامل ایجاد جرم در فضای مجازی و تاثیرات آن بر دنیای حقیقی و راهکارهای پیشگیری از حدوث اینگونه جرائم است. ویژگی اساسی جرایم سایبری این است که این گونه جرایم بر خلاف روال سنتی پیشین، در فضای فیزیکی اتفاق نمی افتند؛ انتقال جرم و جنایت از فضای فیزیکی جامعه به فضای سایبر در عصر حاضر، بسیاری از معادلات شناسایی و برخورد با مجرمان را تغییر داده است. ویژگی اصلی جرایم سایبری که فهم این واژه را هم در درون خود تداعی می کند، نامرئی و پنهان بودن این گونه جرایم در اذهان کاربران می باشد به طوری که بسیاری از مردم هنوز شناختی درست از مسئله جرم و جنایت در فضای مجازی پیدا نکرده‌اند و همین امر

باعث می‌شود در برابر جرایم سایبری آسیب پذیرتر جلوه کنند و زمینه برای سارقان و جنایتکاران سایبری فراهم‌تر شود. ویژگی دیگر جرایم سایبری این است که جرایم بر خلاف روال سنتی پیشین در فضای فیزیکی اتفاق نمی افتند، این مفاهیم همگی باعث شده اند تا نیاز رو به افزایشی در زمینه آموزش های دانشگاهی در این رشته احساس گردد و این مهم جز با ایجاد شاخه جدید جرم شناسی سایبری و به تبع آن ایجاد مشاغل و حرفه های مرتبط با این رشته ممکن و میسر نیست. به لحاظ تاریخی به قول پروفسور «سوزان برنر» در کتابش با نام «جرایم سایبری» این جرایم ریشه در دو دوره دارند؛ اولین دوره مربوط به زمانی بین ساخت رایانه‌های غول‌پیکر تا سال ۱۹۹۰؛ و دوره دوم نیز از زمان پیدایش اینترنت و رایانه‌های شخصی می باشد. نویسنده سعی دارد به این مهم اشاره کند که چون گسترش دامنه نفوذ فضای سایبری در زندگی انسان باعث ایجاد اَشکال مختلف جرایم سایبری گردیده لذا لازم است جهت مقابله با آن جرم شناسی سایبری نیز اولاً برای شناسایی و تلاش برای پیشگیری و دوماً برای تعقیب و مجازات مرتکبین آن صورت پذیرد. به نظر نویسنده برای اینکه به درستی با جرایم سایبری برخورد گردد شایسته است که رشته جدیدی تحت همین عنوان ایجاد و در مراکز دانشگاهی تدریس گردد. در نهایت نتیجه گیری می کند که با توجه به نوپا بودن این رشته با محدودیت ها و چالش هایی از قبیل مشکلات آموزشی مانند نبود اساتید مجرب و کافی و نبود منابع تحقیق در زمینه جرم شناسی سایبری و تلاش برای حرفه ای سازی این رشته وجود، دارند. نویسنده با برشماری مصادیقی از جرایم سایبری ما را به این حقیقت می رساند که سرعت در شکل گیری این نوع از جرایم باید مراکز علمی و حقوقدانان را به آن وادارد که راه های شناسایی برای مقابله با آن نیز سرعت گیرد.

جرم شناسی سایبری

فناوری اینترنت و توسعه فضای سایبری (فضای مجازی) جامعه را وارد مرحله جدیدی از تکامل کرده است. فضای سایبری مرزها را از میان برداشته و جغرافیا (یا مکان) را بی معنا کرده

است. این فضا در هزاره جدید فرصت های بیشماری را در اختیار جوامع قرار می دهد. در دهه ۹۰ میلادی عصر جدیدی آغاز شد که در آن فناوری اینترنت بر سایر فناوری ها برتری داشت. با وجود این، افزایش شمار شهروندان سبب شده است تا این فناوری به یک رسانه انحصاری تبدیل شود. افزون بر آن، مجرمینی که در گذشته از طریق ماشین ها به ماشین های دیگر حمله می کردند از زمان ظهور اینترنت به حمله به انسان های واقعی از طریق ماشین ها روی آورده اند. این پیشرفت بنیادین منجر شده تا جرم شناسان در جهت رفع نیاز به وجود رشته ای برای مطالعه و بررسی رفتار مجرمانه در فضای سایبری اقدام کنند. رفتارهای مجرمانه و قربانی کردن افراد در فضای سایبری باید از منظر علوم اجتماعی و تکنولوژیکی مطالعه شود. در این راستا بنده رشته جرم شناسی سایبری (یا اینترنتی) را به عنوان یکی از زیرشاخه های جرم شناسی در سال ۲۰۰۷ و با آغاز انتشار یک مجله اینترنتی رایگان به نام «مجله بین المللی جرم شناسی سایبری»، به آدرس *http://www.cybercrimejournal.com*، به وجود آورده ام. در سال ۲۰۰۸ نظریه ای برای گسترش رشته جرم شناسی سایبری مطرح کرده ام. این نظریه به نام «نظریه تبدیل فضایی» شناخته شده و علت ارتکاب جرم در فضای مجازی را توضیح می دهد (جایشانکار، ۲۰۰۷ و ۲۰۰۸).

جرم شناسی سایبری یک رشته چند شاخه ای است که محققان حوزه های مختلف نظیر رشته جرم شناسی، قربانی شناسی، علم اینترنت، و علوم کامپیوتر را در بر می گیرد. تعریفی که بنده برای جرم شناسی سایبری ارائه می دهم از این قرار است: «جرم شناسی سایبری به مطالعه علت جرایمی که در فضای سایبری رخ می دهند و تاثیر آن ها بر فضای فیزیکی اختصاص دارد» (جایشانکار، ۲۰۰۷، بند ۱). من به طور آکادمیک اصطلاح جرم شناسی سایبری را به دو دلیل ابداع کرده ام. نخست آنکه پیکره دانشی که به جرایم سایبری اختصاص دارد نباید با تحقیق و پزشکی قانونی سایبری اشتباه گرفته شود؛ دوم، یک شاخه مستقل باید برای مطالعه و کاوش جرایم سایبری از منظر علوم اجتماعی وجود داشته باشد. از زمان آغاز به کار «مجله بین المللی جرم شناسی سایبری» اصطلاح «جرم شناسی سایبری» جایگاهی در محافل اینترنتی (آنلاین) و

غیر اینترنتی (آفلاین) کسب کرده است (جایشانکار، ۲۰۰۷؛ نان و باخمَن، ۲۰۱۰). بر اساس اثر «نان» و «باخمَن» (۲۰۱۰)، جرم شناسی سایبری یک شاخه تثبیت شده در حال ظهور است و اغلب توسط جرم شناسی مرسوم به حاشیه رانده می شود و جای خود را به موضوعات با اهمیت تر می دهد (صفحه ۱۷۵). اگرچه جرم شناسی سایبری در حال یافتن جایگاه خود در جریان اصلی جرم شناسی می باشد، اما پرسش مهمی که در این رابطه وجود دارد آنست که: «آیا جرم شناسی سایبری به یک شاخه مجزا تبدیل خواهد شد یا خیر؟» حوزه های جرم شناسی متعددی وجود دارند که نتوانسته اند به شاخه های مجزا تبدیل شوند. از جمله این حوزه ها می توان به جرم شناسی سبز، جرم شناسی زیستی و جرم شناسی زیست محیطی اشاره کرد. یکی از دلایل این مسئله می تواند فقدان محتوای لازم برای آموزش افراد علی رغم وجود حوزه های تحقیقاتی مورد نیاز باشد. با این حال، جرم شناسی سایبری از پتانسیل لازم برای تبدیل شدن به یک شاخه مجزا برخوردار است زیرا می تواند از طریق آموزش و تحقیق و به صورت پویا محتوای میان شاخه ای منحصر بفردی را به وجود آورد.

چالش‌های جرم شناسی سایبری :

اگر قرار باشد جرم شناسی سایبری به عنوان یک شاخه مجزا معرفی شود، چالش های متعددی پیش روی جرم شناسان سایبری امروزی قرار خواهد گرفت. این چالش ها عبارت اند از: ۱- مشکلات آموزشی، ۲- تحقیق در زمینه جرم شناسی سایبری، ۳- حرفه ای سازی این رشته.

۱- مشکلات آموزشی:

بسیاری از دانشگاه های ایالات متحده و انگلستان برنامه های درسی مربوط به جرم شناسی را همراه با دروس مربوط به جرایم سایبری ارائه می کنند. اخیراً برخی از دانشگاه های انگلستان نظیر «دانشگاه کلیسای مسیح کانتربوری»، «دانشگاه دوبلین» و «دانشگاه بِدفورد شایر»

برگزاری کلاس های کارشناسی ارشد پزشکی قانونی سایبری و محاسبه پزشکی قانونی را آغاز کرده اند. برگزاری کلاس های بیشتر در مورد پزشکی قانونی سایبری حاکی از آن است که دانشگاه ها بیشتر به بخش تحقیق در خصوص جرایم سایبری علاقمند هستند تا علل آن ها. اگرچه جنبه عملی تحقیقات نیز حائز اهمیت است، اما چشم پوشی از مسائل نظری تولید کننده جرایم سایبری نمی تواند مکمل درکی کل نگرانه از جرایم سایبری باشد. در مقطع کارشناسی ارشد باید کلاس هایی در خصوص جرم شناسی سایبری و پزشکی قانونی سایبری برگزار شود. بدین ترتیب، امکان ترکیب جنبه های نظری و عملی جرایم سایبری فراهم می شود. استفاده از مدرسان متخصص برای تدریس جرایم سایبری و نیز انجام تحقیقات یکی از چالش های مرتبط با ایجاد برنامه های درسی مربوط به جرم شناسی سایبری است. رشد علم اینترنت، علوم کامپیوتر و فناوری اطلاعات تاثیر بسزایی بر توسعه رشته جرم شناسی سایبری دارد. به نظر نمی رسد که جرم شناسان سنتی در حال منطبق ساختن خود با نیازهای روبه رشد شاخه (درحال توسعه) جرم شناسی باشند. آن ها به یادگیری رشته های دیگر نظیر فناوری اطلاعات و علم اینترنت (که هر دو آن ها حوزه جرم شناسی سایبری را در بر می گیرند) تمایلی ندارند. جرم شناسان سنتی بدون برخورداری از دانش فنی نمی توانند از آموزش جنبه های نظری جرایم سایبری فراتر روند. از طرفی، اگر قرار باشد تکنوکرات ها (حامیان تکنوکراسی) نیز در آموزش جرم شناسی سایبری سهیم شوند از تمرکز آن ها بر اصول جرم شناسی سایبری کاسته خواهد شد و احتمالاً این افراد بیشتر به سخن گفتن در مورد فناوری و نه مسائلی که منجر به ارتکاب جرایم سایبری می شوند تمایل خواهند داشت. از سوی دیگر، چنانچه قرار باشد وکلا به تدریس دروس جرم شناسی سایبری بپردازند تمرکز آنها باید تنها بر قوانین سایبری باشد و سایر مولفه-های مهم جرایم سایبری را نادیده بگیرند. این قبیل آموزش های ذره گرایانه که توسط جرم شناسان، تکنوکرات ها و یا وکلا ارائه می شوند در به ثمر نشاندن تلاش های انجام شده در جهت توسعه شاخه رسمی جرم شناسی سایبری موثر نخواهند بود. نیاز شدیدی به متخصصین کل نگر و برخوردار از دانش جامع در مورد جرم شناسی سایبری، حقوق و پزشکی قانونی وجود

دارد. متخصصینی که می توانند جرم شناسی سایبری را وارد مرحله دیگری از تکامل کنند. واحدهای جرم شناسی سنتی می توانند یک برنامه چندرشته ای مرکب از جرم شناسی سایبری و پزشکی قانونی سایبری را با کمک گرفتن از سایر واحدها مانند دانشکده علوم کامپیوتر، حقوق و فناوری اطلاعات ارائه دهند. آن دسته از متخصصینی که موفق به کسب مدرک جرم شناسی سایبری می شوند می توانند به عنوان دستیار برای انجام تحقیقات و اقدامات آموزشی و توسعه این شاخه، بکار گرفته شوند. بدین ترتیب مجموعه ای متشکل از متخصصینی که به نوعی گنجینه ای را در اختیار می گذارند تشکیل می شود و ترکیبی از دانش نظری و عملی در خصوص جرایم سایبری، تحقیقات و قوانین به وجود می آید. این افراد متخصص برای پیشبرد این حرفه و یاری رساندن به اداره دادگستری کیفری در انجام تحقیقات در مورد جرایم سایبری ارزشمند خواهند بود.

۲- تحقیق در زمینه جرم شناسی سایبری:

نتایج تحقیقات حاضر در زمینه جرم شناسی سایبری بسیار امیدبخش است. جرم شناسان جدید و قدیم به سرعت از وجود شکاف تحقیقاتی در حوزه های تحقیقاتی جرایم سایبری آگاه شدند (نان و باخمن، ۲۰۱۰). اگرچه مرحله تحقیقات در این حوزه به کندی پیش می رود اما توان آن رو به افزایش است (جوکِز، ۲۰۰۶؛ مان و سوتون، ۱۹۹۸). همچنین در حال حاضر مجموعه های ویراستاری شده و کتب تالیف شده متعددی در مورد جرایم سایبری وجود دارند که به دست جرم شناسان و صرفاً از منظر جرم شناسی نگاشته شده اند (جوکِز، ۲۰۰۷؛ مَک کوئید، ۲۰۰۵؛ اشمالگر و پیتارو، ۲۰۰۸؛ اسمیت، گرابوسکی و اورباس، ۲۰۰۴؛ وال، ۲۰۰۱، ۲۰۰۳، ۲۰۰۷، ۲۰۰۹؛ یار، ۲۰۰۶؛ یار و جوکِز، ۲۰۱۰). مقالات تحقیقاتی منتشر شده در مجله بین المللی جرم شناسی سایبری مقالاتی کیفی و کمّی بوده و دارای کیفیت بالایی هستند. از آنجایی که تحقیقات در زمینه جرم شناسی سایبری به تازگی آغاز شده نمی توان عاری از نقیصه‌های روش شناختی دانست. «نان» و «باخمن» در اثر اخیر خود (۲۰۱۰) به معرفی برخی

از اشتباهات روش شناختی ویژه در زمینه تحقیقات جرم شناسی سایبری پرداخته اند. این محققین بر این باورند که «مشکل نبود یک تعریف عمومی، مسائل مربوط به اندازه گیری، و مشکلات تحقیقاتی مانند تعصب ها و خطاها» (صفحات ۱۷۹ تا ۱۸۲) باید به دست جرم شناسان سایبری آینده برطرف شوند. صرف نظر از مسائل تحقیقاتی مذکور، مسئله کمبود محقق در حوزه جرم شناسی سایبری یکی دیگر از مشکلات موجود است. به جز تعداد محدودی از محققین که در کشورهایی مانند ایالات متحده، انگلستان، هندوستان و کانادا فعالیت دارند، هیچ محقق برجسته ای در حوزه جرم شناسی سایبری مشغول فعالیت نیست. همانطور که پیش از این در بخش «مشکلات آموزشی» اشاره شد، این کمبودها را می توان با آموزش جرم شناسان سایبری بیشتر برطرف کرد. همکاری تحقیقاتی میان دانشگاه های متعدد که تحقیقاتی را در زمینه جرم‌شناسی سایبری انجام می‌دهند، می‌تواند برطرف کننده این شکاف باشد. افزون بر آن، بازدید مداوم از مراکز تحقیقاتی توسط متخصصین بخش صنعت نیز در پیشرفت همکاری‌های تحقیقاتی و تبادل تخصص موثر خواهد بود.

۳- حرفه‌ای سازی در رشته جرم شناسی سایبری:

چالش اصلی پیش روی شاخه های جدید مانند شاخه جرم شناسی سایبری ایجاد مشاغل و حرفه ای سازی رشته مورد نظر است. چنانچه جرم شناسی سایبری جایگاه خود را به عنوان یک رشته نظری حفظ کند، ایجاد مشاغل در این حوزه تنها به مشاغل مربوط به انجام تحقیقات نظری محدود خواهد شد. همانطور که پیش از این تاکید شد، نیاز به توسعه شاخه جرم شناسی سایبری نه صرفاً به عنوان یک رشته نظری بلکه به عنوان یک رشته عملی وجود دارد. ترکیب جرم شناسی سایبری، حقوق و پزشکی قانونی کامپیوتری می تواند زمینه ساز ایجاد مشاغل جدید در حوزه جرم شناسی سایبری باشد. دانشگاه ها و سایر نهادها می توانند برنامه ای برای اعطای گواهینامه به جرم شناسان سایبری طراحی کنند. به این ترتیب جرم شناسان سایبری دارای گواهینامه می توانند در ادارات پلیس در انجام تحقیقات موثر یاری برسانند و کمپانی های

مستقلی را راه اندازی کنند. همچنین جرم شناسان سایبری می توانند به متخصصین حقوق سایبری تبدیل شوند. خدمت رسانی به قربانیان نیز یکی دیگر از حوزه های فعالیت برای جرم شناسان سایبری است. جرم شناسان سایبری می توانند به عنوان مشاورین قربانیان سایبری به افرادی که طعمه جرایم سایبری شده اند خدمات مشاوره ای ارائه دهند و اشخاص حقوقی را در جلوگیری از قربانی شدن در فضای سایبری یاری کنند. این متخصصین همچنین می توانند به عنوان منبع تحقیقاتی در زمینه قربانی کردن افراد برای جرایم سایبری و در نتیجه ایجاد آگاهی در میان پژوهشگران و عموم مردم مورد استفاده قرار گیرند.

فرصت‌های جرم شناسی سایبری

تاسیس یک «مرکز تحقیقاتی بین المللی جرایم سایبری» در مرکز دانشگاه «سیمون فریزر» برای تحقیق در زمینه جرایم سایبری و نیز در موسسه فناوری دانشگاه «اونتاریو» (در کانادا) زمینه‌ی مناسبی را برای پیشرفت اقدامات تحقیقاتی در زمینه جرم شناسی سایبری فراهم کرده است. برخی مراکز تحقیقاتی مانند «مرکز اینترنت و جامعه بِرکمان» و «مرکز مطالعات جرم شناسی سایبری» در «دانشکده دادگستری کیفری جان جِی» به همکاری با هدف توسعه جرم شناسی سایبری اختصاص یافته اند. انجام یک جستجوی سریع در اینترنت اطلاعاتی را در مورد سایر مراکز در دست ساخت و در حال راه اندازی برای این منظور بدست می دهد. این اطلاعات نوید بخش تداوم تحقیق در زمینه جرم شناسی سایبری با هدفی کاملاً جدید و محرک می باشند. به علاوه، بنده به واقع معتقد هستم که چالش های بررسی شده در این نوشتار را می توان به کمک جرم شناسان سایبری کنونی و آینده بر طرف کرد. همچنین آینده روشنی را برای رشد جرم شناسی سایبری به عنوان یک شاخه مستقل پیش بینی می کنم.

«هو» و همکارانش که در حوزه های مالی و ارتباطات فعالیت دارند تاثیر بسزایی در پیشرفت جرم شناسی سایبری داشته اند. آن ها تجزیه و تحلیل های جامعی را بر روی هرزنامه ها و با اهداف جدید انجام داده اند. این محققین تا کنون به بررسی رفتار تجاری افراد در مقابل

هرزنامه‌های ارسال شده توسط کمپانی های بازاریابی سهام پرداخته اند. آن ها با بررسی بیش از ۴۰۰۰ هرزنامه متوجه شدند که میزان بازده غیرمعمول، حجم تجارت و بی ثباتی قیمت روزانه در هرزنامه های حاوی قیمت نهایی، بسیار بالاتر است. همچنین آن ها به این یافته رسیده اند شرکت هایی که اداره مرکزی آن ها در خارج از مرزهای ایالات متحده قرار دارد از ارزش هدف کمتری در مقایسه با شرکت هایی که ادارات مرکزی آن ها در ایالات متحده واقع است برخوردارند. این مسئله ممکن است با سطح اعتماد کاربران فعال در بورس سهام در رابطه باشد. «ماریون دیون» مسئله هزینه نامه های تقلبی را از نگاه ماکیاولی یا از منظر خودشیفتگی مورد بررسی قرار داده است. وی به مطالعه بیشتر در مورد اختلافات جزئی میان این نامه ها پرداخته است و چگونگی بهره گیری از مهارت های بازاریابی برای کلاه برداری از قربانیان را از طریق تاکید بر پیش زمینه درخشان آن ها و امکان برقراری این نوع تماس ها برای قربانیان مورد بررسی قرار می دهد. این مقاله یک گام کیفی کلیدی در این راستا محسوب می شود چراکه توانسته است به امر تجزیه و تحلیل هزینه نامه های تقلبی رونق ببخشد. این مقاله از زاویه دیگری به بررسی روان مجرمینی که این قیبل نامه ها را جعل می کنند می پردازد و تاثیر بسزایی در این زمینه برجای می گذارد.

با توجه به فریبنده بودن فضای سایبری انجام مطالعه بر روی مجرمین سایبری امری دشوار است. «باخمن» در مقاله ای تلاش کرده است تا به تجزیه و تحلیل میزان ریسک پذیری هَکِرها بپردازد. برقراری تماس با هَکرها کار آسانی نیست و باید برای انجام چنین مطالعه پرمشقتی به وی تبریک گفت. وی در این مطالعه روان هَکرها را مورد تجزیه و تحلیل قرار می دهد و متوجه می شود که هَکرها ریسک پذیری بالاتری نسبت به سایر افراد دارند و این ویژگی آن ها را از عموم مردم متمایز می سازد. وی تلاش کرد تا این قبیل رفتارها را به کمک برخی از نظریه های مربوط به جرم شناسی بررسی کند. از آنجایی که این پژوهش یک مطالعه اکتشافی بود امکان اثبات گسترده این نظریه ها وجود نداشت. این مقاله کمبود موجود در زمینه ادبیات جرم شناسی سایبری را به ویژه در مورد مجرمین سایبری برطرف می سازد.

دزدی موسیقی مسئله بسیار جنجال برانگیزی است. بسیاری از کشورهای جهان قوانین متفاوتی را در رابطه با مالکیت موسیقی وضع کرده اند. در حالیکه برخی کشورها اهمیت بسیاری برای مسائل مربوط به حق الامتیاز (کُپی رایت) و مالکیت موسیقی قائل می شوند، اما بعضی کشورها امکان دانلود (پایین گذاری) آزادانه موسیقی را از طریق وب سایت های «تورِنت» (*torrent*) و سایر وب سایت ها فراهم می کنند. «گانتر» و همکارانش به بررسی این مسئله در بطن ایالات متحده با یک جامعه آماری متفاوت پرداخته اند. از آنجایی که مطالعات انجام شده در این زمینه بر روی دانشجویان انجام شده است، این پژوهش رویه دیگری را پی می گیرد. به عبارت بهتر، این پژوهش بر روی مسئله دزدی موسیقی در میان دانش آموزان تمرکز می کند، این محققین تلاش کرده اند تا به پیش بینی میزان دخالت دانش آموزان در دزدی موسیقی بر حسب ویژگی های آماری (جنسیت، نژاد و طبقه)، دستاوردهای آموزشی، تمایلات فردی، و قوه خودداری آن ها بپردازند. آن ها متوجه شده اند که عوامل مذکور در دزدی موسیقی توسط دانش آموزان تاثیرگذار بوده اند. قلدری سایبری (اینترنتی) یکی از عمده ترین جرایم اینترنتی بررسی شده است. با وجود این، تحقیق در زمینه قلدری سایبری تنها بر روی جمعیت تعداد محدودی از کشورها انجام می شود. با وجود این، «سو» و «هولت» در اقدامی بی سابقه به انجام مطالعه بر روی مجموعه ای از جوامع پرداخته اند که پیش از این مطالعه ای بر روی آن ها صورت نگرفته بود. آن ها رفتار قربانیان و قلدرهای چینی را مورد بررسی قرار دادند. تا آن زمان مانعی به نام زبان امکان انجام این تحقیقات و ارائه نتایج آن ها به مخاطبین بین المللی را به وجود نیاورده بود، در حال حاضر با همکاری مترجمین و تحلیلگران کارآمد امکان انجام این مطالعات به وجود آمده است. این پژوهش نیز به عنوان گام موثری در این راستا محسوب می شود چراکه بُعد جدیدی را به تحقیقات مربوط به قلدری سایبری اضافه می کند. با انجام این پژوهش مشخص شد که دخالت های جنسی و حمایت ناظرین از قربانیان در قلدری تاثیر گذار می باشد. نتایج مربوط به حمایت ناظرین کاملاً بی‌سابقه هستند، زیرا غالب مطالعات ناظرین را

یا به عنوان شرکای فعال و یا غیرفعال معرفی می کنند و آن ها را به عنوان واسطه هایی که می توانند از وقوع چنین جرایمی جلوگیری کنند معرفی نمی کنند.

رفتار گزارشگری یکی از زمینه های مهم تحقیقاتی در زمینه قربانی شناسی است. «مور» و همکارانش تلاش کرده اند تا رفتار گزارشگری را در قبال تهدیدهای اینترنتی مورد ارزیابی قرار دهند. با وجود آنکه قربانیان زن در مورد تهدیدهای فیزیکی گزارشی ارائه نمی کنند اما اکثر زن ها تهدیدهای اینترنتی مربوط به خود را گزارش می‌کنند. این محققین همچنین به این یافته رسیده اند که قوانین تعیین شده توسط والدین تاثیری بر رفتار گزارشگری قربانیان نداشته اند. این محققین تاکید می کنند جوانانی که بیشتر از فضای سایبری استفاده می کنند در مقایسه با افرادی که گاهی از فضای سایبری استفاده می کنند بیشتر موارد قربانی شدن خود را گزارش می کنند. تحقیق حاضر که در زمینه قربانی شدن سایبری (اینترنتی) انجام شده است علاوه بر رفع کمبود موجود در ادبیات مربوطه به توسعه جرم شناسی سایبری و قربانی شناسی نیز کمک می کند. «ماریون» نیز پژوهشی را در مورد اثربخشی «کنوانسیون جرایم سایبری» که در سال ۲۰۰۱ توسط شورای اروپا به وجود آمد انجام داده است. وی این کنوانسیون را به روش رمزگرایی که توسط «اِدِل مَن» به وجود آمده است مورد آزمایش قرار می دهد. خانم «ماریون» نقد فوق العاده ای را بر روی کنوانسیون جرایم سایبری انجام داده و تاکید کرده است که موضع کنونی کنوانسیون جرایم سایبری در تخفیف جرایم کشورهای عضو موثر نخواهد بود چراکه این موضع گیری یک اقدام نمادین است. وی همچنین توصیه هایی را برای ارتقاء کارایی این کنوانسیون و خلق سیاستی بهتر برای برخورد با جرایم سایبری ارائه کرده است.

تشکر و قدردانی

انتشار این مقاله تنها با اعتقاد نویسندگان آن به کیفیت «مجله بین المللی جرم شناسی سایبری» و منتقدین برجسته آن میسر شده است. منتقدین این شماره طی اطلاعیه مختصری، نظر خود را در مورد مطالب مندرج در آن مطرح کردند و بنده تاکنون به میزان بسیاری از

حمایت های آن ها در مطرح کردن این موضوع بهره برده ام. از صمیم قلب و خالصانه از تمام منتقدین این مجله برای حمایت مداوم و یاری آن ها در تبدیل این مجله به یک مجله رایگان اینترنتی عالی سپاسگزاری می کنم. مسئولین این مجله بر این باورند که دانش موجود درباره جرایم سایبری باید بدون اغماض در اختیار تمام افرادی که به اینترنت دسترسی دارند قرار داده شود.

فهرست منابع

- *Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, 1, 1–6.*
- *Jaishankar, K. (2007). Editorial: Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology, 1(2), 7–9.*
- *Jewkes, Y. (2006). Comment on the book Cyber Crime and Society by Majid Yar, Sage. Publications.*
- *Jewkes, Y. (2007). Crime online. Cullompton: Willan.*
- *Mann, D., & Sutton, M. (1999). NetCrime. More change in the organisation of thieving. British Journal of Criminology, 38(2), 201-229.*
- *McQuade, S. C. (2005). Understanding and managing cyber crime. Upper Saddle River, NJ: Allyn & Bacon.*
- *Nhan, J., & Bachmann, M. (2010). Developments in cyber criminology. In M. Maguire & D. Okada (Eds.), Critical issues in crime and justice: Thought, policy, and practice (pp. 164–183). Thousand Oaks, CA: Sage.*
- *Pittaro (Eds.), Crimes of the Internet (pp. 283• 301). Upper Saddle River, NJ: Prentice Hall.*
- *Schmalleger, F., & Pittaro, M. (Eds.) (2008). Crimes of the Internet. Upper Saddle River, NJ: Prentice Hall.*
- *Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. Cambridge, UK: Cambridge University Press.*
- *Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Cambridge, UK: Polity.*
- *Wall, D. S. (Ed.). (2001). Crime and the Internet. London: Routledge.*
- *Wall, D. S. (Ed.). (2003). Cyberspace crime. Aldershot, UK: Dartmouth/Ashgate (Dartmouth International Library of Criminology and Penology).*
- *Wall, D. S. (Ed.). (2009). Crime and deviance in cyberspace. Aldershot, UK: Dartmouth/ Ashgate (Dartmouth International Library of Criminology and Penology).*

- Yar, M. (2006). Cybercrime and society. London: Sage Publications.
-J ewkes, Y., & Yar, M. (2010). Handbook of Internet crime. Cullompton: Willan.
-Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger, & M.