مدیریت پیش‌گیری از تحقق و تداوم چرخهٔ باطل جرایم سایبری

امین پژوهش جهرمی*[1] و افسانه زمانی جبّاری[2]

[1]استادیار، دانشکده مدیریت و مهندسی صنایع، دانشگاه صنعتی مالک‌اشتر، تهران، ایران
Amin.pazhouhesh@gmail.com

[2] جانشین معاون دادستان و دادیار اظهارنظر دادسرای عمومی و انقلاب شیراز
Afsaneh.s.zamani@gmail.com

چکیده

هدف مقالهٔ حاضر، مطالعهٔ تداوم چرخهٔ جرایم سایبری و ارائهٔ راه‌کارهایی برای مدیریت پیش‌گیری از تحقق آن است. جرایم سایبری طیفی را شامل می‌شود که یک سمت آن متّکی بر فناوری است و سوی دیگر، بر روابط بین‌فردی تکیه دارد. پژوهش حاضر از نظر هدف، کاربردی و از نظر نوع، کیفی و با توجه به نحوهٔ گردآوری داده‌ها، کتابخانه‌ای و مبتنی بر مطالعه منابع برخط داخلی و خارجی است. مقاله با بررسی ادبیات موضوعی، نتیجه می‌گیرد فاصلهٔ زمانی میان عرضهٔ فناوری و بروز جرم مرتبط و وضع قوانین کیفری، متناسب نیست و اغلب امکان انتقال تجربه جرایم سنّتی به حوزهٔ سایبری وجود ندارد؛ لذا با توجه به گسترده‌بودن این پدیده، چارچوب قانونی مناسب، پویا و چابک، نیاز ضروری برای پژوهش و تعقیب آن است. این پژوهش به برخی راه‌بردهای پیش‌گیرانه همچون ارزیابی تهدید و تحلیل راه‌بردی، توسعهٔ همکاری‌های ملّی، منطقه‌ای و بین‌المللی، و افزایش آگاهی و آموزش اشاره می‌کند.

واژگان کلیدی: مدیریت پیش‌گیری، جرایم سایبری، راه‌بردهای پیش‌گیرانه.

۱- مقدّمه

جرایم سایبری همانند جرایم متعارف و سنّتی، جنبه‌های مختلف دارد و در انواع گسترده‌ای از حالات و محیط رخ می‌دهد. تعریف جهانی و به‌رسمیت شناخته‌شده‌ای از این مفهوم وجود ندارد و تعاریف کنونی موجود، به‌طور تجربی و با تکامل این نوع جرایم ارائه شده و در حال تکاملند؛ لذا تا حدی تابع تکامل فاوا[1] در حوزهٔ جغرافیایی هستند[2] [۱]. این دسته جرایم به‌طورمعمول به‌عنوان یک فرایند درک می‌شوند تا یک کنش لحظه‌ای [۲]. اگرچه اینترنت، بستر اصلی این گونه جنایات است، با این حال تنها به شبکهٔ جهانی اینترنت محدود نشده و تمام شبکه‌های رایانه‌ای محلی و سامانه‌ها فاوا، حتی خطوط تلفن ثابت و همراه را نیز در برمی‌گیرد [۱]. بنابراین جرایم سایبری طیف گسترده‌ای از کنش‌های مجرمانه را شامل می‌شود. این پژوهش جرایم سایبری را بدین صورت تعریف می‌کند:

> *هر جرم و جنایتی که توسط رایانه، شبکه، و یا دستگاه سخت‌افزاری به‌عنوان عامل، تسهیل‌کننده و یا هدف انجام شده و فعالیت‌هایی بر علیه اطلاعات (کلاه‌برداری[3]، جعل، تقلب[4]، دسترسی غیرمجاز)، فعالیت‌های جنایی در حوزه محتوا (مانند، هرزه‌نگاری کودکان، و زورگیری مجازی[5] و نقض قوانین حق تکثیر را شامل شود.*

از این تعریف مشخص می‌شود رایانه و فناوری اطلاعات و ارتباطات، سه نقش مختلف در جرایم کیفری[6] بازی می‌کنند:

---

[1] فناوری اطلاعات و ارتباطات

[2] شورای پیمان جرایم اینترنتی در اروپا از اصطلاح "جرم سایبری" برای اشاره به جرایم اعم از فعالیت‌های جنایی علیه اطلاعات تا محتوا و نقض قوانین حق تکثیر استفاده می‌کند. بنابراین جرایم اینترنتی طیف گسترده‌ای از کنش‌های مجرمانه را شامل می‌شود.

[3] Fraud
[4] Forgery
[5] Cyberstalking
[6] Punishable crimes

* نویسندهٔ مسؤول

- **عامل:** سامانه‌های رایانه‌ای و فاوا، وسیلهٔ ارتکاب جرم و جنایت هستند؛
- **تسهیل‌کننده:** سامانه‌های رایانه‌ای و فاوا، واسطهٔ انجام و یا ابزار بهبود کنش مجرمانه می‌شوند؛ برای مثال به‌عنوان ابزاری برای ذخیره داده‌های کاربردی یا داده‌های هدف اقدام مجرمانه؛
- **هدف:** سامانه‌ها و فناوری‌ها هدف انجام این جرایم هستند (نمونه‌های شناخته‌شدهٔ این دسته، مواردی همچون بدافزارهای رایانه‌ای، هک‌کردن، و امثال آنهاست).

هر سه کارکرد یادشده زیرمجموعه عبارت جرایم سایبری قرار می‌گیرند، و با توجه به گسترده‌بودن این مفهوم و پدیده، چارچوب قانونی مناسب، پویا و چابک، نیاز ضروری برای پژوهش و تعقیب جرایم سایبری است. به بیان دیگر در نتیجهٔ تکامل و توسعهٔ پیوستهٔ اینترنت، که به تبع آن انواع جدید و با پیچیدگی بیش‌تر این نوع جنایات کیفری را موجب شده است، قانون‌گذاران افزون بر این که مجبور به پاسخ‌گویی مداوم به این تحولات هستند، لازم است بر اثربخشی رویکردهای قانونی موجود نظارت داشته باشند. اما به دو دلیل، وضع قوانین و به‌روزنگهداشتن آن با مشکلاتی مواجه است:

- نخست با نگاهی کوتاه به گذشته درمی‌یابیم فاصلهٔ زمانی میان عرضهٔ فناوری و بروز جرم مرتبط، و فاصلهٔ زمانی میان عرضهٔ فناوری وضع قوانین کیفری متناسب نیست. به‌عنوان مثال، هنگامی که شبکه‌های رایانه‌ای در دههٔ هفتاد میلادی معرفی شدند، نخستین دسترسی غیرمجاز به این شبکه‌ها مدت کوتاهی پس از معرفی رخ داد، به‌طور مشابه، جرایم نرم‌افزاری بلافاصله پس از معرفی رایانه‌های شخصی در دههٔ هشتاد میلادی انجام شد، یعنی هنگامی که از محصولات نرم‌افزاری، رونوشت تهیه شد؛ درحالی‌که در هر دو مورد، در همان آغاز، شرایط وضع قانون برای این مسأله فراهم نبود و مدت زمان به‌نسبه طولانی طول کشید که زمینهٔ وضع قوانین متناسب فراهم شد [۳]. طولانی‌شدن این فرایندها، یعنی شناخت سوءاستفاده‌های احتمالی از فناوری‌های جدید و سپس اصلاحات لازم در قوانین کیفری ملی، فرصت‌های طلایی بر مجرمان فراهم می‌آورد.
- دوم آن‌که قانون‌گذاران به‌طورکلی نیازمند مجال و فرصت برای به‌روزرسانی قوانین کیفری برای امکان‌پذیرکردن تعقیب اشکال جدید جرایم سایبری هستند. حتی جرایمی که جدید نبوده و توسط قانون مجازات تعریف شده‌اند، نیازمند بررسی و به‌روزرسانی هستند، برای مثال، امضاهای دیجیتال نیازمند آن بودند که به وضعیت حقوقی همسان با امضاهای سنتی و چاپی دست یابند [۳].

به دو مورد یادشده در بالا باید افزود که در بیش‌تر موارد، امکان انتقال تجربه جرایم سنتی به حوزهٔ سایبری وجود ندارد. این موضوع به سه علت رخ می‌دهد: صحنه جرم، بزه‌دیده، و بزه‌کار.

- **محل (صحنهٔ جرم):** صحنهٔ جرم در جرایم سایبری، از ویژگی‌هایی است که موجب تمایز جرایم سایبری از سایر جرایم می‌شود. در جرایم سنتی، مجرم به‌طور فیزیکی در صحنهٔ جرم حاضر می‌شود. بنابراین، مقامات مجری قانون می‌توانند مجرم را دستگیر و تسلیم عدالت کنند. این شرایط، مشابهتی با جرایم سایبری ندارد، از آن‌رو که جنایت‌کار سایبری به‌طورمعمول در صحنه جرم نبوده و بازداشت وی مشکل است. نه‌تنها مجرم در صحنهٔ جرم حاضر نیست، بلکه ممکن است، حتی در حوزهٔ قضایی مربوطه نیز نبوده و در کشور و یا قاره دیگر باشد.
- **قربانی (بزه‌دیده):** فراتر از مشکلات قضایی فراروی سازمان‌های مجری قانون، مسأله دیگر، برخورد با طیف گسترده‌ای از قربانیان با شخصیت‌های حقوقی و حقیقی مختلف است که اغلب دارایی نامشهودشان مورد آسیب قرار می‌گیرد که ارزش‌گذاری میزان خسارت برای این نوع دارایی‌ها بسیار دشوار است. البته ارزیابی خسارت در شرایطی امکان‌پذیر است که قربانی محدودیتی برای اطلاع‌رسانی خسارت نداشته باشد. از آن‌رو که، اطلاع‌رسانی شرکت قربانی درباره مورد تهاجم قرارگرفتن داده‌های مربوط به فناوری‌اش، افزون بر خسارت ناشی از بزه‌دیده‌گی سایبری، شرکت را با تهدید رقبا برای دست‌یابی به آن اطلاعات و کاهش ارزش سهام نیز مواجه می‌سازد.
- **مجرم (بزه‌کار):** بخش دیگر معادلهٔ تهدید، مجرم، انگیزه‌ها و نیاتش است که یکی از منحصربه‌فردترین حوزه‌های جرایم سایبری است. در برخی موارد، مجرم یک نوجوان خاطی است که برای تفریح و یا برای اثبات خودش به همسالانش دست به اقدامات مجرمانه می‌زند. در موارد دیگر، مجرم فردی بزرگسال است که به دنبال خراب‌کاری در رایانه و یا سرقت اطلاعات حساس و فروش آن‌ها است. در سطح بالاتر، مجرمان می‌توانند گروه‌های سازمان‌یافته‌ای باشند که گاه از حمایت‌های پنهان دولتی نیز برخوردارند. افزون بر این موارد، مجرم یا مجرمان در هر سطحی، ممکن است از پیامدها و عواقب احتمالی اقدامات مجرمانه خود آگاه باشند؛ لذا حوزه‌های خاکستری نیز وجود دارد که

قضاوت صریحی درباره آن نمی‌توان داشت؛ مثل بارگذاری غیرقانونی نرم‌افزار از اینترنت. این حوزه، هم‌پوشانی بسیار قطعی با حقوق مالکیت معنوی و قوانین حاکم بر آن دارد که از کشوری به کشور دیگر متفاوت است و یا حوزهٔ خاکستری نگارش نرم‌افزارهایی که کاربرد دوگانه دارند.

در تمام موارد، طولانی‌شدن فرایندهای وضع و بروزرسانی قوانین، یعنی شناخت سوءاستفاده‌های احتمالی از فناوری‌های جدید و اصلاحات لازم در قانون کیفری ملی، فرصت‌های طلایی برای مجرمان فراهم می‌آورد. بنابراین، به‌روزماندن قوانین که لازم است هم‌سنگ سرعت نوآوری در فناوری‌های اطلاعاتی و شبکه‌ها باشد، بدل به چالش کلیدی قانون‌گذاران شده است. ازهمین‌رو، در بسیاری از کشورها شاهد تلاش سخت برای به‌روزنگه‌داشتن قوانین متناسب با تحولات فناورانه هستیم. به همین خاطر بی‌اغراق است اگر گفته شود، جرایم سایبری چالش ویژه‌ای فراروی قوانین کیفری کشورها می‌گذارد.

مقاله ابتدا به بررسی پیشینهٔ نظری و ادبیات موضوعی می‌پردازد و سپس مبتنی بر روش پژوهش اتخاذی، به مطالعهٔ جرایم سایبری از انسان‌محور تا فناوری‌محور پرداخته و توانمندسازهای جرایم سایبری را معرفی می‌کند؛ سپس چرخهٔ باطل شکل‌گیری و تداوم جرایم سایبری را توضیح داده و اقدامات پیش‌گیرانه از تحقق چرخهٔ باطل را معرفی می‌کند.

۲- پیشینهٔ نظری

جرایم سایبری توجه بسیاری از پژوهش‌گران و کارشناسان را به خود جلب کرده و به یکی از موضوع مورد بحث در ادبیات علمی تبدیل شده است و درنتیجه مجموعهٔ بزرگی از ادبیات موضوعی را ایجاد کرده است؛ اما با توجه به گستردگی این حوزه، و علاقه خاص پژوهش‌گران، مطالعات، گسسته و نامتوازن هستند. با توجه به علائق حرفه‌ای‌شان، پژوهش‌گران بر یک و در بهترین حالت بر چند وجه این مشکل بسیار پیچیده و غامض متمرکز می‌شوند.

راشکوفسکی و همکاران [۴] به حوزهٔ جرایم سایبری از منظر رویکرد بین‌المللی پرداخته و قوانین کیفری و جزایی مقدونیه در حوزهٔ جرایم سایبری را با توجه به شیوه‌نامه‌های بین‌المللی مبارزه با جرایم سایبری مورد بحث و تحلیل قرار می‌دهند. مقاله با ارائهٔ چند پروندهٔ برجستهٔ جرایم سایبری که در همین اواخر در مقدونیه مطرح شده، جرایم سایبری را از منظر بین‌المللی در هفت طبقه با عناوین دزدی و تقلب؛ جاسوسی رایانه‌ای؛ هک و نفوذ غیرقانونی در سامانه‌های رایانه؛ توزیع بدافزار و دیگر اشکال نرم‌افزاری مخرب هم‌چون تروجان‌ها؛ زورگیری سایبری؛ تولید و توزیع هرزه‌نگاری؛ تروریسم سایبری و نقض حقوق مالکیت معنوی دسته‌بندی می‌کند.

بونو [۵] به حوزه جرایم سایبری از منظر رویکرد سیاسی پرداخته و نتیجه گرفته مبارزه با جرایم سایبری به رویکرد سیاسی جامع نیاز دارد. چنین رویکردی باید بر روند جرایم سایبری اشراف داشته و توانایی پیش‌بینی تحولات آینده را به‌منظور جلوگیری از تهدیدات جدید و کمک به اطمینان از آمادگی‌های موردنیاز پیش رو داشته باشد. اقدامات پیش‌گیرانه باید مبتنی بر این رویکرد باشد. مرکز ثقل این اقدامات، هم‌گرایی در سطح عمودی (با دادستان‌ها و قضات) و در سطح افقی (با صنعت اینترنت، سایر ذی‌نفعان و جامعه مدنی به‌عنوان یک کل) و درنهایت، افزایش آگاهی و آموزش مداوم در تمام سطوح اجتماع است. بالابردن سطح آگاهی کلی دربارهٔ تهدیدات ناشی از جرایم سایبری، و البته پرهیز از تضعیف اعتماد کاربران اینترنت، یک چالش کلیدی برای سال‌های پیش رو است.

شتری [۶] به حوزهٔ جرایم سایبری از منظر اقتصادی پرداخته و نتیجه می‌گیرد ویژگی‌های مجرمان سایبری، قربانیان جرایم سایبری، و سازمان‌های اجرای قانون، متأسفانه اثر تقویت‌کننده بر یکدیگر داشته که منجر به شکل‌گیری دور باطلی از جرایم سایبری می‌شود. پژوهش‌گر بر اساس عناصر کلیدی این حلقه، الگوی اقتصادی هزینه-فایده برای عملکرد هکر ارائه می‌دهد که تحلیل این الگو، می‌تواند به سازوکارهای احتمالی برای مبارزه با جرایم سایبری منتهی شود.

۳- روش پژوهش

این پژوهش از نظر هدف، کاربردی، از نظر نوع، کیفی و با توجه نحوهٔ گردآوری داده‌ها، کتابخانه‌ای (مطالعات ثانویه از نوع فراتحلیل) و مبتنی بر مطالعه منابع اطلاعاتی برخط داخلی هم‌چون بانک جامع مقالات کنفرانس و همایش‌های سیویلیکا[1]، مرکز اطلاعات علمی برخط جهاد دانشگاهی[2]، پایگاه مجلات تخصصی نور[3]، سامانه نشر مجلات علمی *دانشگاه تهران*[4]، پایگاه مطبوعات ایران[5]، پژوهشگاه علوم و فناوری اطلاعات *ایران*[6] و بانک‌های اطلاعاتی برخط خارجی

[1] www.civilica.com
[2] www.SID.ir
[3] www.noormags.com
[4] journal.ut.ac.ir
[5] www.magiran.com
[6] www.irandoc.ac.ir

همچون ساینس‌دایرکت[1]، اسپرینگر[2]، جان‌وایلی[3]، آی‌تریپل‌ایی[4]، و تیلور و فرانسیس[5] بدون درنظرگرفتن قید زمانی تهیه شده است. تجزیه و تحلیل اطلاعات در این پژوهش در سه مرحله رخ داد: با بررسی کامل ادبیات پژوهش، فهرستی از مقالات مرتبط با این حوزه و حتی مقالاتی که به‌طور فرعی به این موضوع پرداخته‌اند، تهیه شد؛ چکیدهٔ کلام این مقالات استخراج و دسته‌بندی شد؛ و درنهایت، با استخراج عناصر کلیدی، ترکیب نهایی این موارد انجام شد و جمع‌بندی صورت گرفت.

۴- جرایم سایبری از انسان‌محور تا فناوری‌محور

درنظرگرفتن تمایزها و ارائهٔ طبقه‌بندی انواع جرایم سایبری به چند دلیل بسیار مهم است:

- نخست آن‌که هدف اصلی در ایجاد طبقه‌بندی، ایجاد ارتباط و تسهیل آن است. از آن جا که دانش مربوط به جرایم سایبری به‌سرعت در حال رشد بوده و البته هنوز جوان است، همانند اغلب حوزه‌ها و رشته‌های در حال ظهور و نورس، نظریه‌های توصیفی و اصولی و هرگونه اطلاعات در دسترس در این حوزه نیز در بهترین حالت تکه‌تکه و پراکنده هستند.
- هم‌چنین از آن‌جایی که حوزه جرایم سایبری مورد توجه بسیاری از رشته‌های علوم اجتماعی مانند حقوق، جامعه‌شناسی، و همچنین مهندسی، و مدیریت و نیز مرکز توجه سیاست‌گذاران بخش عمومی، خصوصی، و غیرانتفاعی، و تصمیم گیرندگان در سطح جامعه، منطقه و در سطح ملی بوده و به حوزهٔ جامعه اقتصادی چندملیّتی (به‌عنوان مثال، جامعه اقتصادی اروپا) نیز وارد شده است، در نظر گرفتن تمایزها و ارائهٔ طبقه‌بندی در توسعهٔ تعریف دقیق موضوعات مبهم کمک کرده و موجب شکل‌گیری ادبیات مشترک بین حوزه‌های مختلف علمی شده و به پژوهش‌گران کمک می‌کند حوزه‌های مبهمی را که نیازمند پژوهش و شفاف‌سازی هستند، شناسایی کرده و مورد مطالعه قرار دهند.
- و به‌طور مشخص از منظر حقوقی، این طبقه‌بندی هم‌چنین می‌تواند چارچوبی مفهومی ایجاد کند که قانون‌گذاران از آن برای ایجاد تعاریف حقوقی (که از نظر فنّی و اجتماعی معنادار باشند) استفاده کنند. این مسأله ازآن‌رو اهمیت دارد که تعاریف حقوقی از جرایم سایبری، به‌شدت بین حوزه‌های قضایی، متفاوت است [۱]. از نگاه فنّی نیز، کارشناسان فاوا می‌توانند تفاوت‌های ظریف جرایم الکترونیکی را درک کنند. درنهایت با ایجاد زبان مشترک میان حقوق‌دانان و کارشناسان فنی، امکان برداشت‌های یکسان از بحث‌ها ممکن شده و تعاریف حقوقی منسجم‌تری نتیجه می‌شود.

این پژوهش، جرایم سایبری را بر اساس گوردون و فورد [۱] به دو نوع متمایز و طیف فازی میان این دو طبقه‌بندی می‌کند: جرایم سایبری نوع نخست و جرایم سایبری نوع دوم.

جرایم سایبری نوع نخست: این طبقه جرایم مبتنی بر این ویژگی‌ها و صفات است: نخست آن‌که از منظر قربانی یک رویداد فردی و مجزا به‌شمار می‌روند؛ دوم آن‌که اغلب توسط ورود بدافزارها، همانند ویروس‌ها، و تروجان‌ها به سامانه رایانه‌ای کاربر (قربانی) تسهیل می‌شود؛ و سوم آن‌که زمینه این رخداد ممکن است (البته نه لزوما) توسط خود قربانی فراهم شود. یک رویداد واحد و یا گسسته، از دیدگاه کاربر، ممکن است، چیزی شبیه به این موارد باشد:

- کاربر برای انجام کاری برخط می‌شود؛ به‌عنوان مثال به جستجوی صفحات وب مشغول می‌شود، و یا به خواندن / پاسخ‌دادن رایانامه‌اش می‌پردازد.
- کاربر اقداماتی انجام می‌دهد که امکان دسترسی مجرم به اطلاعاتش را فراهم می‌سازد](همانند وارد کردن اطلاعات شخصی در یک شبه‌سایت، (یا) فشردن روی برخی پیوندها (لینک‌ها) و در نتیجه بارگیری(دانلود) یک تروجان)].
- اطلاعات توسط مهاجم/مجرم استفاده می‌شود.
- کاربر از جرم آگاه می‌شود؛

این رویداد یک رویداد منفرد از دیدگاه کاربر است.

جرایم سایبری نوع دوم: نوع دوم جرایم سایبری، که در انتهای دیگر این طیف قرار دارد، فعالیت‌هایی همانند زورگیری مجازی و آزار و اذیت سایبری، کودک‌آزاری جنسی[6]، اخاذی[7]، باج‌خواهی[8]، دستکاری بازار سهام، جاسوسی پیچیدهٔ اطلاعاتی از شرکت‌های بزرگ، و برنامه‌ریزی یا انجام فعالیت‌های تروریستی برخط است. این طبقه مبتنی بر این ویژگی‌ها و صفات است: این جرایم به‌طور کلی با برنامه‌هایی

[1] www.sciencedirect.com
[2] Link.springer.com
[3] Onlinelibrary.wiley.com
[4] Ieeexplore.ieee.org
[5] www.tandfonline.com

[6] Child predation
[7] Extortion
[8] Blackmail

که زیرمجموعه بدافزارها قرار نمی‌گیرند، تسهیل می‌شوند (به‌عنوان مثال، ممکن است با استفاده از سامانه‌های پیام فوری رخ داده و یا فایل‌ها با استفاده از پروتکل FTP [1] منتقل شوند)؛ و دوم آن‌که از نگاه کاربر، این تماس‌ها یا حوادث تکراری هستند.

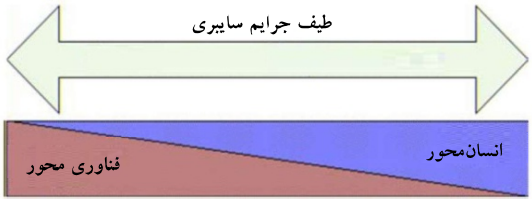
زنجیرهٔ حوادث در شکل‌گیری یک جرم از نوع دوم، از دیدگاه کاربر، ممکن است، چیزی شبیه به این موارد باشد:

- کاربر (قربانی) در جستجوی برخی اطلاعاتی در مورد یک موضوع خاص است. بنابراین تصمیم به عضویت در یک گروه تبادل نظر (فوروم) دربارهٔ حوزهٔ مورد علاقه‌اش می‌گیرد.
- کاربر دیگری (مجرم) در این گروه تبادل نظر، فعالیت‌های کاربر نخست را در طی چند روز زیر نظر گرفته و در پی ایجاد آشنایی اولیه بر می‌آید. پس از مدتی کاربر دوم، درخواستی برای بحث خصوصی با استفاده از سامانهٔ پیام فوری برای کاربر نخست (سامانهٔ پیام فوری درون فوروم) می‌فرستد. کاربر نخست که از طریق گروه تبادل نظر با کاربر دوم آشنا شده است، پاسخ مثبت به این درخواست داده و شروع به چت می‌کنند. این دوره، به‌عنوان القا یا نصب اعتماد [2] (شبیه مفهوم نصب نرم‌افزار) شناخته می‌شود. پس از مدتی تعامل، کاربر نخست دربارهٔ ویژگی‌های فردی و اجتماعی و یا توان مالی‌اش، اطلاعاتی در اختیار کاربر دوم قرار می‌دهد.
- کاربر دوم، با استفاده از اطلاعات به‌دست‌آورده (شماره تماس، عکس‌های خصوصی، اطلاعات محل کار کاربر نخست و سایر اطلاعاتی که می‌تواند انتشار آن برای کاربر نخست ناخوشایند باشد)، کاربر نخست را تهدید به افشای اطلاعات در گروه تبادل نظر کرده و در پی آزار و یا باج‌خواهی برمی‌آید.

همان‌گونه که مشخص است، این رویداد، مجزا و ایزوله نبوده و متأثر از روابط فرد با محیط اطرافش است و هم‌چنین تک‌مورد نبوده و به‌کرّار انجام می‌شود. یک‌چنین کنش‌های مجرمانه‌ای که زیرعنوان زورگیری مجازی قرار می‌گیرند، هم‌اکنون به مشکل بسیار جدی در جامعهٔ برخط امروزی بدل شده‌اند [۷]. به این ترتیب، این نوع جرایم از جرایم نوع یک (که ماهیتا فنی‌تر هستند) متفاوت هستند. درک نقش زورگیری مجازی در طبقه‌بندی جرایم سایبری مهم است. با این حال، اگرچه عنصر سایبری جرم در این دسته ضعیف‌تر است، اما هنوز زیرمجموعهٔ جرایم سایبری قرار می‌گیرد.

[1] File Transfer Protocol
[2] Instilling trust

بنابراین، جرایم سایبری طیفی را شامل می‌شود که یک سمت آن به‌طور کامل متکی بر فناوری و سوی دیگر این طیف، متکی بر روابط بین‌فردی است (شکل ۱). برای مثال، کلاه‌برداری از طریق رایانامه را در نظر بگیرید که از کاربری به‌طور مستقیم و به‌سادگی خواسته می‌شود مبلغی پول نقد را به نشانی فیزیکی خاصی در ازای خدماتی که هرگز انجام نشده است، پست کند. این کلاه‌برداری از طریق پست معمولی یا حتی تلفن نیز امکان‌پذیر است. به این ترتیب، این موضوع یک مسئله فناوری‌محور نیست، هر چند مرتکب می‌تواند از ویژگی‌های خاصی از فناوری به نفع خود استفاده کند (که اغلب نیز انجام می‌دهد). در انتهای دیگر این طیف، کاربری را می‌توان مثال زد که دستگاهش مورد نفوذ قرار گرفته، و اگرچه ممکن است، خسارت مالی ندیده باشد، اما صرف نفوذ به دستگاه، ماهیت به‌طورکامل فناورانه دارد.



(شکل-۱): طیف جرایم سایبری از انسان‌محور تا فناوری‌محور

(جدول-۱): نمونه‌ای از جرایم سایبری بر حسب نوع [۱]

نمونه	نوع	نرم‌افزار	بدافزار
فیشینگ	۱	Mail client	خیر
هویت‌دزدی	۱	Keylogger, Trojan	آری
زورگیری مجازی	۲	Email Client, Messenger Clients	خیر
حمله منع سرویس توزیع‌شده [3]	۱	Bots	آری
تروریسم سایبری	۲	Steganography, Encryption, Chat Software	خیر

به‌احتمال زیاد جرایمی که تنها فناورانه و یا به‌طورکامل متکی بر روابط انسانی باشند، کمینه بوده و عمده جرایم، در میانه این طیف قرار داشته و ترکیبی از هر دو است. شناخت این طیف ازآن‌رو اهمیت دارد که پژوهش‌گران سنتی بیش‌تر تمایل به مطالعه و رسیدگی به جرایمی دارند که بیش‌تر انسان‌محور هستند تا فناوری‌محور و کارشناسان امنیت رایانه، به‌احتمال زیاد، تمرکزشان در مورد مسائلی است که اغلب فناوری‌محور هستند تا انسان‌محور. جدول زیر نمونه‌ای از جرایم سایبری را بر حسب نوع نشان می‌دهد (جدول ۱).

[3] Distributed Denial of Service (DDoS)

۵- توانمندسازهای جرایم سایبری

توانمندسازها، ویژگی‌هایی هستند که امکان تحقق جرم را افزایش داده و تداوم آن را تسهیل می‌کنند. توانمندسازهای[1] جرایم سایبری را می‌توان بدین شرح برشمرد:

- نخست: ناشناس‌بودن، کنش مجازی و عدم محدودیت‌های ارتکاب جرایم در دنیای واقعی (همچون وابستگی به مکان).
- دوم: دسترسی است که توسط زیرساخت‌ها و پلت‌فرم‌های اینترنت، از جمله ظهور شبکه‌های اجتماعی برخط محقق می‌شود. منابع به‌راحتی در دسترس میلیون‌ها کلاه‌بردار و در معرض حملات فیشینگ بالقوه است. به‌عنوان مثال، کاربران، تمایل به به‌روزنگه‌داشتن پروفایل‌های شبکه‌های اجتماعی‌شان با توجه به زمان و مکان کنونی و نیز بیان علاقهٔشان دارند، که همین انتشار اطلاعات، مجرمان را قادر به هدف‌قراردادن قربانیان در پرتو الگوها و پس‌زمینهٔ رفتاری‌شان می‌سازد.
- سوم: پراکندگی بین‌المللی و تنوع چارچوب‌ها و قوانین جرایم سایبری ملی که درعمل در میان شکاف این قوانین، مجرمان لانه گزیده و فعالیت می‌کنند.
- و درنهایت، عامل کلیدی دیگر، بی‌اهمیتی عمومی به خطر جرایم سایبری است. نسبت جرایم سایبری شناسایی‌شده به نسبت سایر جرایم، بسیار پایین است. با توجه به مطالعهٔ انجام‌شده توسط دفتر مطالعات مواد مخدر و جرایم سازمان ملل متحد[2] در سال ۲۰۱۳، گزارش قربانیان جرایم سایبری به پلیس در مجموع کمی بیش از یک درصد بوده است. بی‌شک اقدامات قانونی نقش حیاتی در مبارزه با جرایم سایبری بازی کرده و لذا بازنگری حوزه‌های مختلف، اعم از قانون اساسی تا قانون آیین دادرسی کیفری، و همچنین مسائل قضایی را شامل شود.

در هر حال، راه‌برد جامع سیاسی نیز (مشتمل بر زیرراه‌بردهای پیش‌گیری از طریق ارزیابی تهدید، توسعه و افزایش آگاهی) باید برای مبارزه با جرایم سایبری اتخاذ شود.

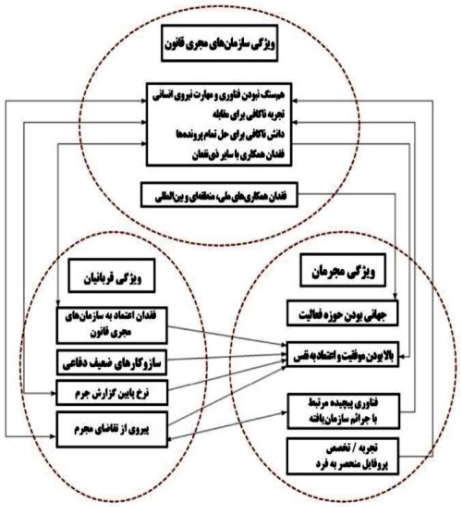
۶- چرخه باطل شکل‌گیری و تداوم جرایم سایبری

همان‌طور که پیش‌تر بیان شد، ویژگی‌های بستر وقوع جرم، مجرمان و قربانیان، شرایطی را فراروی سازمان‌های اجرای قانون قرار داده که یک دور باطل از وقوع جرایم سایبری را موجب شده است. نخست آن‌که سازمان‌های اجرای قانون با این نوع جدید جرایم، بیگانه و نامانوس هستند. درواقع، در بسیاری از کشورها این سازمان‌ها به ابزارها و دانش مقابله با ماهیت جهانی این جرایم (جرایم سایبری) مجهز نشده‌اند. افزون‌براین، با کمبود نیروی انسانی برای مقابله با جرایم مجازی نیز مواجه‌اند. این کمبود ممکن است از ضعف در جذب و نگه‌داشت استعدادهای در دسترس در این حوزه ناشی شود. به بیان دیگر جرایم سایبری به‌طور فزاینده‌ای پیچیده شده، و اَشکال و روش‌های این گونه جنایات جدید به‌سرعت در حال بهبود هستند. سازمان‌های اجرای قانون، فاقد منابع کافی بوده و به‌طورمعمول در به‌دست‌آوردن سریع نیروی انسانی و هم‌چنین فناوری‌های مقابله ناکام می‌مانند. هم‌چنین پژوهش‌های جرایم سایبری، بسیار پیچیده و نیز به‌شدّت متکی به منابع و تخصص بوده، و درنتیجه بسیاری از کشورها توانایی بررسی همهٔ جرایم گزارش‌شده را ندارند.

بر این اساس، سازمان‌های اجرای قانون، اعتمادبه‌نفس لازم را ندارند و افزون‌براین با عدم تمایل قربانیان به گزارش این گونه جنایات نیز مواجه‌اند. نیم‌رخ منحصربه‌فرد مجرمان سایبری، به‌طور قابل توجهی متفاوت از پروفایل مجرمان معمولی است. به‌عنوان مثال در روسیه، بسیاری از هکرها جوان و تحصیل‌کرده بوده، و به‌طور مستقل فعالیت می‌کنند، و درنتیجه شباهت چندانی با پروفایل جانیان معمولی ندارند [۶]. در جهان فیزیکی، بسیاری از جرایم نزدیک به خانه مجرمان رخ می‌دهد و مجرمان تنها در موارد خاص و وجود انگیزه کافی، قلمرو خود را به سمت مکان‌های ناشناخته ترک می‌کنند. برخی جرایم از جمله آدم‌ربایی و یا سرقت از بانک، مسافرت به مناطق ناشناخته را پرهزینه کرده و نیاز به برنامه‌ریزی دقیق‌تری دارند. جنایات در دنیای مجازی در این بُعد نیز به‌طور قابل توجهی متفاوت هستند. فناوری اطلاعات و ارتباطات به‌راحتی مرزهای ملی را پشت سر می‌گذارد. علاوه‌براین، ناشناس‌ماندن در اینترنت، تعاملات پیچیده‌ای را موجب می‌شود که گروه‌های جنایی سایبری، سازمان‌های تروریستی فراملی، و شرکت‌های درگیر در جاسوسی را قادر به گسترش عملیات‌شان در سطح جهانی بدون ترک خانه می‌کند. درنتیجه نسبت بالایی از پژوهش‌های جرایم سایبری با مسائل قضایی روبه‌رو هستند. در بسیاری از موارد، انجام جرایم سایبری فراتر از مرزها، اهمیت کمتری برای مراجع قضایی پیدا می‌کند. درنتیجه مرزهای ملی موانع جدی برای سازمان‌های اجرای قانون ایجاد کرده‌اند. همکاری و هماهنگی میان سازمان‌های قضایی مختلف، می‌تواند به این مسأله کمک کند، اما راه حل کمی دست‌نیافتنی می‌کند. برای مثال، اگر چه روسیه با آمریکا برای کمک به بررسی جنایات متعدد توافق امضا کرده‌اند، اما جرایم مجازی در زمره این توافق‌نامه نیست [۶]. قوانین جرایم سایبری درجهٔ بالایی از ناهمگنی و

[1] Enabler
[2] United Nations Office on Drugs and Crime

عدم‌تجانس بین‌المللی دارند. در شرایطی که کشورهای صنعتی در تلاش برای همکاری‌های بین‌المللی برای مبارزه با جرایم سایبری هستند، کشورهای فقیر هنوز درگیر اقدامات اولیه نیز نیستند و در بسیاری از این کشورها هیچ یک از قوانین جرایم سایبری هنوز تصویب نشده است. بسیاری از قربانیان نیز تمایلی به گزارش جرم ندارند؛ زیرا فکر می‌کنند رفتن به سراغ قانون حمله را متوقف نمی‌کند. عوامل دیگر می‌تواند خجالت، ترس ازدست‌دادن اعتماد مشتری، آسیب در اعتبار شرکت، و احتمال کاهش قیمت سهام شرکت باشد. بانک‌ها، مؤسسات مالی و کسب و کارهای دیگر که با داده‌های حساس سروکار دارند، در این دسته قرار می‌گیرند. هوش بالا نیز در کنار مهارت و تجربهٔ مناسب از ویژگی‌هایی است که مانع گیرافتادن مجرمان سایبری می‌شود. ضعف سازوکارهای دفاعی قربانی نیز مزید بر علت است (شکل ۲).



(شکل-۲): چرخه باطل شکل‌گیری و تداوم جرایم سایبری [۶]

۷- اقدامات پیش‌گیرانه از تحقق چرخهٔ باطل

پیش‌گیری از جرایم سایبری، کنشی چندبعدی، پیوسته و طولانی است. این پژوهش با استفاده از ادبیات موضوعی به برخی راه‌بردهای پیش‌گیرانه هم‌چون ارزیابی تهدید و تحلیل راه‌بردی، توسعه و همکاری‌های ملی، منطقه‌ای و بین‌المللی، و افزایش آگاهی و آموزش به‌اختصار اشاره می‌کند.

- **ارزیابی تهدید و تحلیل راه‌بردی:** هوش و تحلیل راه‌بردی در مبارزه با جرایم سایبری نقش مهمی بازی می‌کند. از نگاه روش‌شناختی، این موضوع اغلب شامل گردآوری داده‌ها، تفسیر آن و تحلیل‌های نظری و پیش‌بینانه دربارهٔ آیندهٔ تحولات، الگوها، روندها، تهدیدات و فرصت‌های به‌روز و پیش‌گیری از بروز جرایم سایبری است. درواقع کاربرد هوش راه‌بردی در حوزهٔ جرایم سایبری تلاش برای پاسخ به این سوال است: « در مورد تهدیدات فعلی و آینده، در سطح عملی چه کاری می‌توانیم انجام دهیم؟». مرکز ثقل این راه‌برد، بررسی ویژگی‌های تهدید، ویژگی‌های مجری تهدید (همچون اندازه گروه مجرم سایبری، منابع مالی دردسترس، سطح تخصص، ابعاد بین‌المللی فعالیت، انعطاف‌پذیری، ساختار داخلی گروه، و غیره)، محدودهٔ تهدید (ابعاد تهدید، حوزهٔ تهدید و حتی محدودهٔ جغرافیایی تهدید) و درنهایت پیش‌بینی تهدیدهای آینده است.
- **توسعهٔ همکاری‌ها:** اینترنت به ملاحظات جغرافیایی وابستگی خیلی کمی دارد (این وابستگی اگرچه ناچیز است اما صفر نیست)؛ اما با قطعیت پایین‌ترین میزان را در مقایسه با فعالیت‌های جنایی متعارف بین‌المللی دارد که متأثر از فرودگاه‌ها، مسیرهای حمل و نقل زمینی، دریایی یا هوایی و زیرساخت فیزیکی است. درواقع جرایم سایبری مرز نمی‌شناسد و تنها یک کلیک، با اقدام مجرمانه فاصله دارد!. همین موضوع مقامات اجرای قانون را ملزم به اتخاذ رویکردی جامع در سطح ملی، منطقه‌ای و بین‌المللی با درگیرساختن تمام ذی‌نفعان دولتی و خصوصی می‌سازد. نیروهای متعددی را که می‌توانند به مبارزه مؤثرتر در برابر جرایم سایبری کمک کنند، بدین شرح می‌توان برشمرد: دولت‌های ملی، سازمان‌های بین‌المللی، مجموعه حاکمیت اینترنت و ارائه‌دهندگان خدمات سایبری، شرکت‌های درگیر در امنیت اینترنت و بخش مالی، کارشناسان دانشگاهی و سازمان‌های جامعهٔ مدنی. با این حال، یک نقطهٔ کانونی که نقش یک هماهنگ‌کننده و کاتالیزور را ایفا کند در هر کشوری الزامی است. به عنوان مثال در اتحادیه اروپا این نقش به مرکز جرایم سایبری اروپا[1] واگذار شده است. حوزهٔ عملیات این مرکز، پشتیبانی، پژوهش، آموزش، پیش‌گیری و برقراری ارتباطات گسترده با ذی‌نفعان فعال است. امروز مبارزه با جرایم سایبری بدون اطمینان از گفت‌وگوی منظم با ارائه‌دهندگان خدمات سایبری، مسئولان شبکه‌های اجتماعی که در آن میلیاردها عکس و پیام هرروزه رد و بدل می‌شود، شرکت‌های فناوری امنیتی که ارائه‌دهندهٔ خدمات امنیتی هم‌چون ضدبدافزارها

[1] European Cybercrime Centre (EC3)

هستند، غیر قابل تصور است. اعتمادسازی و اطمینان بین صنایع اینترنت و مقامات بخش دولتی اهمیت زیادی در مبارزه با جرایم سایبری دارد. شبکه‌ها و پلت‌فرم‌های قابل اعتماد تبادل داده باید با همکاری بخش خصوصی و سایر فعالان، همانند حوزهٔ دانشگاهی و جامعه مدنی ایجاد شوند.

- **افزایش آگاهی و آموزش:** آموزش کاربران اینترنت، هیچ‌گاه دیر نیست. مبارزه با جرایم سایبری، حق ویژه‌ای نیست که تنها به مقامات مجری قانون اختصاص داشته باشد. برنامه‌های آگاهی‌بخش مناسب و سازمان‌یافته برای کاربران اینترنت باید به‌طور مداوم اجرا شده و دراین‌باره اطلاع‌رسانی شود. به‌یقین با توجه به سطح بالای مهارت، تخصص، و نوآوری کلاه‌برداران و هکران، کاربران معمول اینترنت همیشه از کمبود مهارت‌های حوزهٔ فاوا و کسر سواد دیجیتالی رنج می‌برند؛ لذا نمی‌توان انتظار داشت که کاربران معمولی در سطح سواد و مهارت مجرمان سایبری قرار بگیرند؛ اما افزایش آگاهی و دستِ‌کمی از آموزش (که البته این سطح کمینه‌ای، همیشه ثابت نبوده و رو به صعود است) می‌تواند مانع عمده‌ای در موفقیت مجرمان سایبری باشد. هم‌چنین افزایش آگاهی عمومی، نه‌تنها می‌تواند مصونیت را تا حدّ زیادی افزایش دهد، بلکه از تبدیل‌شدن افراد اجتماع به یک قربانی فیزیکی مستقیم جرایم سایبری (همانند موارد سوءاستفاده جنسی از کودکان) جلوگیری کند.

۸- نتیجه‌گیری

اگر پلیس امکان استفاده از سلاح را در شرایط متعارف، در برخورد با مجرم مسلح، دارد، این امکان در جرایم سایبری فراهم نیست؛ به بیان دیگر درصورت استفاده مجرم از ابزارهایی هم‌چون ویروس‌ها، کرم‌ها، و سایر بدافزارهای مخرب علیه جامعه، این امکان برای پلیس فراهم نیست که از همین ابزارها برای مقابله با مجرم استفاده کند. به‌طوراساسی بهبود توانایی سازمان مجری قانون در واکنش برابر به جرایم سایبری راه‌برد صحیحی نیست؛ ازآن‌رو که سازمان را در سطحی قرار می‌دهد که موجب شکل‌گیری چرخهٔ رو به افزایش جرم می‌شود و از همه مهم‌تر این کار به منزلهٔ مهر تأییدی است که دولت به واسطه آن و به‌وضوح اعمال خلاف قانون را به‌رسمیت می‌شناسد.

طبیعت به‌هم‌پیوستهٔ فناوری فاوا بدان معنا است که جرایم سایبری، مشکلی جهانی است. به بیان دیگر شبکه‌های رایانه‌ای مدرن، دیدگاه سنتی را که قوانین کیفری، ماهیتی منطقه‌ای دارند، به چالش کشیده‌اند. همان‌گونه که فردی با دیگری در هزاران کیلومتر دورتر، همانند همسایه مجاورش ارتباط برقرار می‌کند، به همان اندازه جرایم و مجرم آن سوی دنیا به قربانی در این سوی دنیا نزدیک بوده و در معرض تهدید است. حتی در جایی که مجرم و قربانی در صلاحیت یک دادگاه هستند، ماهیت ارتباطات شبکه‌ای بدان معنا است که حوزه‌های قضایی متعدد ممکن است در این زمینه درگیر باشند. به‌عنوان مثالی ساده، ارسال و دریافت رایانامه‌ای در ایران از طریق جی‌میل را می‌توان برشمرد، که با واسطه سرور مستقر در آمریکا رخ می‌دهد. همین ویژگی جهانی و مستقل از مکان‌بودن است که از یک سو دنیایی از فرصت‌های مجرمانه برای مجرمان ایجاد کرده، و از دیگر سو چالش‌های عظیمی فراروی قانون و اجرای آن می‌گذارد؛ لذا بدیهی است وجود هماهنگی در وضع قوانین و اجرا بین کشورها امری حیاتی است که البته ساده نبوده و با موانع سختی روبه رو است.

از دو گزارهٔ بالا می‌توان دریافت ابزار اصلی پیش‌گیری از تحقق و تداوم جرایم سایبری، بیش‌تر متّکی بر ابزارهای نرم هم‌چون ارزیابی تهدید و تحلیل راه‌بردی، توسعهٔ همکاری‌های میان‌سازمانی در سطح ملّی و منطقه‌ای و افزایش آگاهی و آموزش کاربران اینترنت است.

۹- مراجع

[1] Gordon, S., & Ford, R., On the definition and classification of cybercrime. Journal in Computer Virology, 2006, 2(1), 13 –20.

[2] Akopyan, D. A., & Yelyakov, A. D., Cybercrimes in the information structure of society: a survey. Scientific and Technical Information Processing, 2009, 36(6), 338-350.

[3] Gercke, M., Understanding cybercrime: Phenomena, challenges and legal response. International Telecommunication Union. 2012, Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

[4] Rashkovski, D., Naumovski, V., & Naumovski, G. (2016). Cybercrime Tendencies and Legislation in the Republic of Macedonia. European Journal on Criminal Policy and Research, 22(1), 127-151.

[5] Buono, L. (2014). Fighting cybercrime through prevention, outreach and awareness raising. In ERA Forum (Vol. 15, No. 1, pp. 1-8). Springer Berlin Heidelberg.

[6] Kshetri, Nir. "The simple economics of cybercrimes." IEEE Security & Privacy 4.1 (2006): 33-39.

[7] Bocij, P. (2005). Reactive stalking: a new perspective on victimisation. The British Journal of Forensic Practice, 7(1), 23-34.

امین پژوهش جهرمی تحصیلات مقطع کارشناسی و کارشناسی ارشد خود را در رشته مکانیک در دانشگاه صنعتی شریف گذرانده و دکترای خود را در رشتهٔ مدیریت از دانشگاه تهران دریافت کرده و هم‌اکنون به‌عنوان استادیار و عضو هیأت علمی رسمی دانشگاه صنعتی مالک‌اشتر مشغول به فعالیت است. علایق پژوهشی ایشان شامل مدیریت دانش، نوآوری باز، مدیریت کسب‌وکار و شرکت‌های کوچک و دانش‌بنیان است.

افسانه زمانی جباری تحصیلات مقطع کارشناسی و کارشناسی ارشد را در رشته حقوق دانشگاه تهران گذرانده و دانشجوی دکترای حقوق در رشته حقوق کیفری و جرم‌شناسی دانشگاه تربیت مدرس و هم‌اکنون به‌عنوان جانشین معاون دادستان و دادیار اظهارنظر دادسرای عمومی و انقلاب شیراز مشغول به فعالیت است. علایق پژوهشی ایشان شامل حقوق کیفری، جرم‌شناسی، پیش‌گیری از جرم و آیین دادرسی کیفری است.