مقاله پژوهشی:
بررسی جرائم سایبری حوزه اجتماعی و راهبردهای پیشگیری و مقابله با آن در جمهوری اسلامی ایران

رضا صبوری[1] و کامیار ثقفی[2]

تاریخ دریافت: ۱۳۹۷/۰۸/۱۵ تاریخ پذیرش:۱۳۹۷/۱۱/۱۸

چکیده

جرائم سایبری حوزه اجتماعی در جمهوری اسلامی ایران روند رو بـه رشـدی دارد و سـالانه خسـارت‌هـای مادی و معنوی کلانی را به کشور و مردم تحمیل می‌کند. با توجه بـه گسـتره وقـوع ایـن جـرائم در ابعـاد ملـی و تأثیرپذیری فضای سایبر از عوامل داخلی و عوامل محیطی، مبارزه با آن نیـز مسـتلزم اجـرای راهبردهـای کـلان و فراگیر در سطح ملی است. به همین منظور پژوهش حاضر با هدف دستیابی به راهبردهای پیشـگیری و مقابلـه بـا جرائم سایبری حوزه اجتماعی در جمهوری اسلامی ایران انجام گردید. روش این پژوهش «توصـیفی-تحلیلـی» از نوع «پیمایشی و اسنادی» است. حجم جامعه آماری تعداد ٦٨ نفر و روش نمونه‌گیری به‌صورت تمـام‌شـمار بـود. برای گردآوری داده‌ها از پرسشنامه محقق‌ساخته با تعداد ٤٦ گویه و بر اساس مقیاس درجه‌بنـدی لیکـرت اسـتفاده شد. روایی پرسشنامه از طریق روایی محتوایی و پایایی آن از طریق آلفای کرونباخ به دست آمد. بـه‌منظـور تحلیـل محیطـی و دسـتیابی بـه راهبردهـا از تکنیـک SWOT، بـرای ارزیـابی موقعیـت و اقـدام راهبـردی از مـاتریس SPACE، برای اولویت‌بندی راهبردها از ماتریس QSPM و برای انتخاب راهبردهـای برتـر، از معیـار ارزیـابی بحرانی استفاده گردید. یافته‌ها حاکی از این است که حوزه اجتماعی فضای سایبر جمهوری اسـلامی ایـران دارای موقعیت راهبردی رقابتی بوده و برای پیشگیری و مقابله با جرائم سایبری این حوزه لازم اسـت تعـداد ۱۲ راهبـرد برتر احصاشده مورد استفاده قرار گیرد.

کلیدواژه‌ها: جرم، فضای سایبر، راهبرد، پیشگیری از جرائم، مقابله با جرائم

۱- عضو هیئت علمی داخلی دانشگاه علوم انتظامی امین rezasabouri123@chmail.ir(نویسنده مسئول)

۲- دانشیار برق – الکترونیک دانشکده فنی و مهندسی و عضو هیئت‌علمی دانشگاه شاهد

مقدمه

فضای سایبری دارای ویژگی‌های خاص و بعضاً منحصربه‌فردی است که تا حد زیادی آن را از فضای ملموس متمایز کرده است. این فضا نیز مانند سایر محیط‌ها دارای نقاط ضعف و تهدیدهایی است که بخش اعظم آن متأثر از همین ویژگی‌ها است. بعضاً درهم‌تنیدگی این عوامل با حضور و فعالیت افراد متخلف و قانون‌شکن موجب وقوع جرائمی شده که معضلات و مشکلات زیادی را برای مردم و مسئولین به‌ویژه در حوزه اجتماعی ایجاد کرده است. این در حالی است که برخی از جرائم سنتی نیز به این فضا منتقل شده و مشکلات را تشدید نموده است. این موضوع باعث شد تا پژوهش حاضر با عنوان «بررسی جرائم سایبری حوزه اجتماعی و راهبردهای پیشگیری و مقابله با آن در جمهوری اسلامی ایران» انجام گیرد.

امروزه در بسیاری از موارد مردم ناگزیر به استفاده از فضای سایبر هستند. امکانات و فناوری‌های این فضا و یا قواعد و مقررات الزام‌آور اداری مردم را به‌طور جدی درگیر فضای سایبر نموده، به نحوی که این فضا بخشی از زندگی واقعی مردم شده است؛ به عبارت دیگر فضای سایبر امتداد زندگی مردم در مراودات اجتماعی شده است. این موضوع مسئله جدی‌تری برای کشور ایران است، چراکه ایرانی‌ها اجتماعی‌تر از جوامع دیگر بوده و تمایل بیشتری برای استفاده از شبکه‌های اجتماعی فضای سایبر دارند.

حضرت امام خامنه‌ای(مدظله العالی) در مورد فضای مجازی می‌فرمایند: «این فضای مجازی امروز از فضای حقیقیِ زندگی ما چندبرابر بزرگ‌تر شده؛ بعضی‌ها اصلاً در فضای مجازی تنفس می‌کنند؛ زندگی‌شان در فضای مجازی است. جوانان هم با فضای مجازی سروکار دارند، با انواع و اقسام چیزها و کارها، با برنامه‌های علمی‌اش، با اینترنتش، با شبکه‌های اجتماعی‌اش، با مبادلات و امثال این‌ها سروکار دارند؛ خب، اینجا لغزشگاه است. هیچ‌کس نمی‌گوید آقا جاده نکش. اگر شما در یک منطقه‌ای جاده‌ای لازم دارید، خیلی خب، جاده بکش، جاده اتوبان هم بکش، امّا مواظب باش! آنجایی که ریزش کوه محتمل است، آنجا محاسبه لازم را بکنید. ما به دستگاه‌های

ارتباطی خودمان، به مجموعه وزارت ارتباطات و شورای عالی مجازی -که بنده از آن هم گله دارم- سفارشمان این است. ما نمی‌گوییم این راه را ببندید؛ نه اینکه بی‌عقلی است. یک کسانی نشسته‌اند، فکر کرده‌اند، یک راهی باز کرده‌اند. به‌عنوان این فضای مجازی و به قول خودشان سایبری؛ خیلی خب، از این استفاده کنید، منتها استفاده درست بکنید؛ دیگران دارند استفاده درست می‌کنند؛ بعضی از کشورها طبق فرهنگ خودشان این دستگاه‌ها را قبضه کرده‌اند. ما چرا نمی‌کنیم؟ چرا حواسمان نیست؟ چرا رها می‌کنیم این فضای غیر قابل کنترل و غیر منضبط را؟ مسئولند، یکی از مسئولین هم همین‌ها هستند، دستگاه وزارت ارتباطات است»(امام خامنه‌ای،۱۳۹۵/۲/۱۳).

در فضای سایبر نیز مانند دنیای واقعی جرم و جنایت، امنیت مردم را با خطر مواجه کرده است، در این فضا برخلاف دنیای واقعی، مجرمین به‌راحتی مرزهای جغرافیایی را درنوردیده و به‌آسانی در هر جای این دهکده جهانی می‌توانند مرتکب جرم شوند. اگرچه در فضای سایبر ارتکاب جرم تخصصی‌تر شده، اما نسبتاً آسان‌تر و سهل‌الوصول‌تر از دنیای واقعی گردیده است. یکی از ویژگی‌های بارز فضای سایبر، غیر متمرکز بودن آن است، به نحوی که نمی‌توان آن را به مرزهای جغرافیایی محدود نمود، این موضوع قدرت زیادی را به مجرمین، جنایتکاران، تروریست‌ها، جاسوسان، خرابکاران، معارضین سیاسی، کشور حریف و دولت‌های متخاصم داده تا بتوانند از این طریق درصدد تحقق اهداف شوم خود باشند؛ بنابراین در راستای پیشگیری و مقابله با جرائم حوزه اجتماعی فضای سایبر این پژوهش با هدف «دستیابی به راهبردهای پیشگیری و مقابله با جرائم سایبری حوزه اجتماعی در جمهوری اسلامی ایران» شکل گرفت. در راستای رسیدن به این هدف و متناظر با آن، سؤال پژوهش به این شرح طرح گردید: راهبردهای پیشگیری و مقابله با جرائم سایبری حوزه اجتماعی در جمهوری اسلامی ایران کدامند؟

مبانی نظری

الف) پیشینه و سابقه پژوهش

نجفی علمی (۱۳۹۱ هـ.ش) در پژوهشی تحت عنوان روند تحولات فضای سایبر و نقش آن در تهدیدات ناشی از جرم در محیط سایبر (مورد: مدیریت تهدیدات) به این نتیجه رسید که قابلیت و ظرفیت سازگاری روند تحولی جرم، همگام و همسو با روند تحولات فضای سایبر (در سه عرصه کلی و با هفت تغییر ماهوی)؛ الگوی تهدید جرم (اهداف و راهبردها، نوع، ماهیت، فرآیند، گستره، محیط، آثار و پیامدها) را در کشور از قابلیت و ظرفیت های پیچیده و نوینی برخوردار کرده است. این اتفاق پیچیده و نرم، به معنی آن است که «تهدیدات جرم با استفاده از قدرت فنّاوری به فنّاوری قدرت نرم تبدیل شده است» که این موضوع ضمن بی‌سابقه بودن در تاریخ تهدیدات جرم، می‌تواند سبب چالشی جدی در شناخت تهدیدات و مدیریت آن در محیط سایبر و تحول در نگاه به مفهوم نظم و امنیت در وضعیت کنونی کشور گردد.

رامک (۱۳۹۷ هـ.ش) در پژوهشی تحت عنوان ارائه الگوی راهبردی همکاری‌های بین المللی برای ارتقای امنیت فضای مجازی بر اساس منافع ملّی ج.ا.ایران، با رویکرد مبارزه با جرائم سایبری به این نتیجه رسید که شاخص‌های پنج‌گانه همکاری بین‌المللی برای ارتقای امنیت سایبری (توافق‌های دوجانبه، توافق‌های چندجانبه، مشارکت‌های سازمانی، مشارکت‌های دولتی و خصوصی، مشارکت‌های بین‌المللی)، ابزارهای کارآمدی به‌منظور تحقق اهداف تک‌تک اجزای الگو خواهد بود و باید به‌صورت فراگیر جهت ارتقای امنیت فضای مجازی در همکاری‌های بین‌المللی، مورد استفاده قرار گیرد.

درزی و همکاران (۱۳۹۲ هـ.ش) در پژوهشی تحت عنوان مطالعه تحلیلی رویکرد مدیریت فضای سایبری در ایالات متحده آمریکا به این نتیجه رسیدند که با مطالعه انجام‌شده، تهیه و تدوین یک مدل برای مدیریت فضای سایبر در داخل کشور امکان‌پذیر است. از آنجا که در کشور ایران برای این پدیده نهادهای مختلفی وجود دارد و برخی از وظایف آن‌ها با یکدیگر همپوشانی یا تداخل دارد، در آینده نزدیک، کنترل این فضا

دشواری‌های خاصی پیدا می‌کند. با در نظر گرفتن الگوی ایالات متحده و با بومی‌سازی آن متناسب با نهادهای موجود در کشور و یا نهادهایی که ممکن است لازم باشد به این مجموعه اضافه شوند، می‌توان این الگوی جامع را تدوین نمود. خروجی این مطالعه می‌تواند در تدوین استراتژی‌های امنیتی کشور در حوزه فضای مجازی یاری‌رسان باشد.

ستارزاده (۱۳۸۸ هـ.ش) در پژوهشی تحت عنوان شناساییِ تهدیدها و فرصت‌های مجازی در سطح استان مازندران (با تأکید بر اینترنت) به این نتیجه رسید که میانگین استفاده از اینترنت در میان پاسخگویان دو ساعت در روز بوده و مواردی چون چت، سایت‌های جنسی، سایت‌های دانلود موسیقی و فیلم بیشترین استفاده را در میان جوانان دارد. نتایج دیگر نشان داد میان اعتماد به دوستان، عدم روابط خانوادگی، ارتباطات دوستانه و اعتیاد به اینترنت رابطه معناداری وجود دارد.

صادق محمدی (۱۳۷۸ هـ.ش) در پژوهشی تحت عنوان شناخت کلی جرائم رایانهای و روش‌های مبارزه با آن به این نتیجه رسید که لازم است برای کلیه کارکنان کشف جرم در رابطه با جرائم رایانه‌ای برنامه آموزش مقدماتی تدوین گردیده و آن‌ها مورد آموزش قرار گیرند. همچنین برای پیشگیری از جرائم رایانه‌ای کلیه اقشاری که در حوزه فضای سایبر و رایانه فعال هستند مورد آموزش‌های کلی و همگانی قرار گیرند.

لاورگنا (۲۰۱۱ م) در پژوهشی تحت عنوان «رفتار مجرمانه در عصر اینترنت»: سازمان اجتماعی جرائم سازمان‌یافته فراملی و با بررسی رابطه بین استفاده از اینترنت و قاچاق فراملی، راهبردهای مبارزه با جرائم سازمان‌یافته را ارائه نمود. نتایج دیگر نشان‌دهنده شواهد تجربی برای تفسیر تأثیر اینترنت بر رفتار سازمان یافته مجرمانه بوده و درک بهتری از جرم سازمان‌یافته فراملی در جامعه الکترونیک ارائه کرده است.

سلطان الکعبی (۲۰۱۰ م) در پژوهشی تحت عنوان مبارزه با جرائم رایانه‌ای: چشم‌اندازی بین‌المللی، به این نتیجه رسید که ماهیت جهانی اینترنت منجر به افزایش فوق‌العاده فرصت‌ها برای مجرمان اینترنتی شده است. جرائم رایانه‌ای یا سایبری به‌طور فزاینده‌ای به یکی از تهدیدهای اصلی برای رفاه ملت‌های جهان تبدیل شده است؛ بنابراین،

بدیهی است که یک نیاز حیاتی برای درک مشترک چنین فعالیت‌های مجرمانه در سطح بین‌المللی برای برخورد مؤثر با آن وجود دارد. به‌علاوه کشف و درک مشکل به‌طور جزئی و شناسایی موانع همکاری‌های بین‌المللی در مبارزه با جرائم کامپیوتری بسیار مهم است. همین‌طور شناسایی و اتخاذ بهترین روش‌ها برای مبارزه با جرائم کامپیوتری مهم است. این امور، به تحقیقات مداوم در حوزه‌های قانون‌گذاری، ابتکارات بین‌المللی، سیاست و روش کار و فناوری برای مبارزه و بررسی جرائم رایانه‌ای در سطح جهان به‌صورت هماهنگ نیاز دارد و می‌تواند به بهبود آن کمک کند.

در بررسی و جمع‌بندی پیشینه‌ها مشخص گردید که پیشینه‌های مذکور خیلی منطبق با ماهیت و اهداف این پژوهش نیست؛ اما این موضوع دلیلی بر نادیده گرفتن آن‌ها نمی‌باشد، چراکه در راستای دانش‌افزایی در حوزه سایبر و جرائم آن و همچنین افزودن به غنای ادبیات پژوهش تا حدودی کفایت و قابلیت لازم را داشته و می‌تواند در تکمیل برخی از بخش‌های این پژوهش مفید واقع شود.

ب) مفهوم‌شناسی

جرم: جرم عبارت است از هر فعل یا ترک فعلی که در قانون برای آن مجازات تعیین‌شده باشد (مادهٔ ۲ قانون مجازات اسلامی).

فضای سایبر: فضایی است نسبتاً نامحدود، فرازمانی و فرامکانی مبتنی بر فناوری اطلاعات و ارتباطات؛ شامل سخت‌افزارها، نرم‌افزارها و زیرساخت‌های شبکه که در آن تعاملات و فعالیت‌های گوناگون انسانی و ماشینی از قبیل اطلاع‌رسانی، داده‌ورزی، ارائه خدمات، مدیریت، کنترل و ارتباطات، از طریق سازوکارهای الکترونیکی و رایانه‌ای انجام می‌پذیرد.

جرائم سایبری: جرائم سایبری عبارت است از هر فعل یا ترک فعلی که با بهره‌گیری از فناوری اطلاعات و ارتباطات و با استفاده از سامانه‌های رایانه‌ای و شبکه‌های ارتباطی و انتقال داده‌ها از طریق سازوکارهای الکترونیک انجام‌شده و قانون برای آن مجازات تعیین کرده باشد.

جرائم سایبری حوزه اجتماعی: عبارت‌اند از مصادیق جرائمی که به استناد مفاد قانون جرائم رایانه‌ای، علیه اشخاص، اموال، عفت و اخلاق عمومی و امنیت اطلاعات و ارتباطات در فضای سایبر به وقوع می‌پیوندند.

راهبرد: راهبرد برآمده از یک طرح واحد همه‌جانبه است که پس از تلفیق و ایجاد پیوند و ارتباط میان چهار عامل نقاط قوت و ضعف، فرصت‌ها و تهدیدهای محیطی به‌دست‌آمده و رهنمودهایی است برای دستیابی به اهداف کلان و بلندمدت. راهبرد باید حاوی سه عنصر اصلی هدف[1]، ابزار[2] و روش[3] باشد. به عبارت کامل‌تر راهبرد باید محقق‌کننده اهداف بلندمدت و حیاتی سازمان بوده، ابزار (منابع، امکانات و تسهیلات) مورد استفاده را معرفی و شیوه، راه و روش و مسیر دستیابی به اهداف را نیز مشخص کند. راهبردها، راه و روش‌هایی هستند که اهداف بلندمدت یک طرح از طریق آن‌ها محقق می‌شود.

پیشگیری و مقابله با جرم: پیشگیری و مقابله با جرم عبارت است از مجموعه اقدام‌ها و تدابیر گوناگون به‌منظور جلوگیری از وقوع جرم و بزهکاری و حذف فرصت‌های وقوع آن و به کار بردن فنون و روش‌های مختلف برای کاهش اثرات جرم و تبعات آن از طریق واکنش نشان دادن به بزهکاران و مهار مجرمین به‌منظور جلوگیری از تکرار جرم.

ج) چارچوب نظری پژوهش

داده‌های ورودی برای دستیابی به راهبردهای پیشگیری و مقابله با جرائم سایبری حوزه اجتماعی در جمهوری اسلامی ایران که چارچوب نظری این پژوهش را تشکیل می‌دهند و در واقع پژوهشگر از دریچه یا لنز آن‌ها به پدیده جرائم سایبری می‌نگرد که عبارت‌اند از:

1. End, Aim, Goal, Objective
2. Means
3. Way

۱- نظریه‌های مربوط به جرائم سایبری

- نظریه رسانه‌های جدید دنیس مک کوئیل: اینترنت، نمونه بارز رسانه جدید است که علاوه بر تولید و توزیع پیام، به پردازش، مبادله و ذخیره اطلاعات می‌پردازد که مؤید یک نهاد خصوصی اما به‌مثابه ارتباطات عمومی است و صرفاً دارای فعالیت حرفه‌ای و به لحاظ بوروکراتیک، سازمان‌دهی‌شده نیست (مک کوئیل،۲۰۱۰:۱۳۵).

- **انتقال فضایی کی جایشانکار:** وقتی افراد از یک فضا خارج شده و به فضای دیگری وارد می‌شوند، رفتارشان تفاوت خواهد کرد. به‌عنوان نمونه افرادی که رفتار مجرمانه آنان در فضای فیزیکی سرکوب‌شده و با توجه به وضعیت و موقعیتی که دارند فرصت و امکان ارتکاب جرم برای آنان وجود ندارد، میل به ارتکاب جرم در فضای مجازی دارند (جایشانکار،۲۰۰۸:۳۰۱-۲۸۳).

- **جامعه شبکه‌ای مانوئل کاستلز**: اینترنت از راه قدرت مجتمع‌های رسانه‌ای که در سرتاسر جهان و در تمامی کشورها استقرار یافته اند، ظرفیت تکنولوژیک خود و جریان اطلاعات و نمادهایی که ساخته است به‌طور عمده نمی‌تواند تحت کنترل خاص و مقررات وضع‌شده‌ای قرار بگیرد و تنها راه کنترل آن پیدا کردن راهی برای وارد کردن خود و کنترل بیشتر اطلاعات تولیدی در این محیط است (کاستلز، جلد اول،۱۳۸۰:۱۹-۱۶).

- **هویت گمنام شری ترکل:** فضای مجازی به علت ویژگی‌های خاص آن، ازجمله امکان گمنامی و حذف آثار فیزیکی به کاربر این امکان را می‌دهد که به‌راحتی نقش‌های متعدد و متفاوتی را در زمان های مختلف و با تنظیمات متفاوت مورد دلخواه و پسند خود بازی کند (ترکل،۱۹۹۵:۱۷۸).

- **انقلاب اطلاعات الوین تافلر:** تافلر بر این باور است که درگیری عمیق و همه‌جانبه‌ای بین تمدن موج اول زندگی بشر، یعنی انقلاب کشاورزی و موج دوم، یعنی تمدن صنعتی و همچنین موج سوم، یعنی اطلاعات و ارتباطات که چند دهه است جریان دارد به وجود خواهد آمد (تافلر،۱۹۹۵:۱۲۰).

- **دهکده جهانی هربرت مارشال مک لوهان:** وی بر این باور بود که اکنون دیگر کره زمین، به‌وسیله‌ی رسانه‌های جدید، آن‌قدر کوچک شده که ابعاد یک دهکده را یافته

است(لوهان،۱۳۷۷:۱۷۲). از دیدگاه مک لوهان دنیای امروز یک دنیای الکترونیکی است و رسانه‌های الکترونیکی با گسترش خود فاصله‌های زمانی و مکانی موجود میان انسان‌ها را از بین برده‌اند.

۲- نظریه‌های مربوط به پیشگیری از جرائم

- **نظریه کنترل اجتماعی هیرشی:** هیرشی بر این باور است که وقوع فعالیت‌های انحرافی نتیجه شکست پیوندهایی است که فرد را به جامعه پیوند می دهد (هیرشی،۱۹٦۹:۳٤). وی مدعی است که پیوند میان فرد و جامعه علت هم‌نوایی و عامل اصلی کنترل رفتارهای فرد است و ضعف این پیوند یا نبود آن، دلیل اصلی کج رفتاری است و در این میان نهادهایی مثل خانواده، دوستان، همسایه‌ها و مدرسه نقش زیادی دارند (معظمی،۱۳۸۸:۷۸).

- **نظریه سبک زندگی هیندلانگ و گاروفالو:** برخی سبک‌های زندگی فرصت‌های جرم را ایجاد می‌کنند و احتمال قربانی شدن را نیز افزایش می‌دهند؛ بنابراین کنش‌ها و فعالیت‌هایی که فرصت تولید خصوصیات سبک زندگی خاصی را ایجاد کند، منجر به کاهش خطر جرم می‌شود (بنت،۱۹۹۸:۳۷۳).

- **نظریه فعالیت‌های روزمره کوهن و فلسون:** نظریه فعالیت‌های معمول یا روزمره ناظر به تبیین کیفیت تأثیر فعالیت‌های روزمره و سبک زندگی بر وقوع جرائم است (کلدی،۱۳۸۱:٦٤). این نظریه بر اساس پژوهشی که توسط لورنس کوهن و مارکوس فلسون (۱۹۷۹ م) انجام شده، بنیان گرفته است و بر همگرایی زمانی و محیطی سه رکن اصلی لازم برای وقوع جرم (یعنی وجود یک بزهکار بالقوه، یک هدف جذاب و فقدان مراقب توانمند) متمرکز است. نظریه فعالیت روزمره از بوم‌شناسی اجتماعی پدید آمده و از نظر وجود متغیر اساسی با نظریه سبک زندگی دارای وجه اشتراک است. همچنین هر دو نظریه مزبور با رویکرد کاهش فرصت های جرم که با مفهوم پیشگیری از جرم سازگار است، مطابقت دارند (پرویزی،۱۳۷۹:۳۰)

- **نظریه انتخاب عقلانی یا منطقی بزهکار کلارک و کورنیش:** بر اساس این رویکرد مجرمان بالقوه تصمیم گیرندگان عاقلی هستند که به دنبال تأمین منافع اقتصادی خود، پس از

ارزیابی میزان خطر و منافع حاصله از طریق ارتکاب جرم، می باشند. این رهیافت تأکید می کند که روند تصمیم‌گیری در جرائم مختلف، متفاوت است. مدل انتخاب عقلانی به پژوهشگران اجازه می‌دهد در چهارچوبی مشخص به بررسی تجربی این تصمیم‌گیری بپردازند (پرویزی،۱۳۷۹:۲۸).

– **نظریه فرصت رنجر:** فرض اصلی آن این است که هرچه فرصت های احتمالی وقوع جرم بیشتر باشد، تعداد جرائم نیز بیشتر خواهد شد؛ بنابراین برای پیشگیری از وقوع جرم لازم است فرصت‌ها یا زمینه های وقوع آن از میان برداشته شود. رنجر بر این باور است که هر فرصت نه‌تنها به عینیت خاص آن در حالت‌های خاص، بلکه به افرادی که از این ویژگی‌ها و حالت‌ها بهره می‌برند نیز وابسته است (مالمیر،۱۳۸۸:۱۵۳).

– **نظریه** جابه‌جایی: فردی که از جرم و بزهکاری منع شده باشد، به دنبال یافتن فرصت‌های جدید جرم، تلاش خواهد کرد. بنابراین جرائمی که منع می‌شوند، ممکن است به‌سادگی در زمان‌ها و مکان‌های دیگر جایگزین شوند. انواع جابه‌جایی عبارت‌اند از: جابه‌جایی موقتی، جابه‌جایی هدف، جابه‌جایی جغرافیایی، جابه‌جایی تاکتیکی، جابه‌جایی کارکردی (بنت،۱۹۹۸:۳۷٤).

– **نظریه توزیع اشاعه منافع:** مفهوم اشاعه منافع مبنی بر این ایده است که جرائمی که در یک مکان و یا زمان خاص پیشگیری می‌شوند، ممکن است اثر کاهنده بر روی جرائم در مکان‌ها و زمان‌های دیگر داشته باشند. در ادبیات مربوطه، پدیده اشاعه منافع گاهی اوقات با عنوان اثر سواری رایگان یا اثر هاله نیز یاد می‌شود. کلارک پیشنهاد می‌کند پژوهش‌های بیشتر این زمینه، می‌توانند سازوکارهای بالقوه‌ای را بررسی کنند که اشاعه از طریق آن می‌تواند کارایی و اثربخشی برنامه‌های پیشگیری از جرم را تقویت کنند (بنت،۱۹۹۸:۳۷۵).

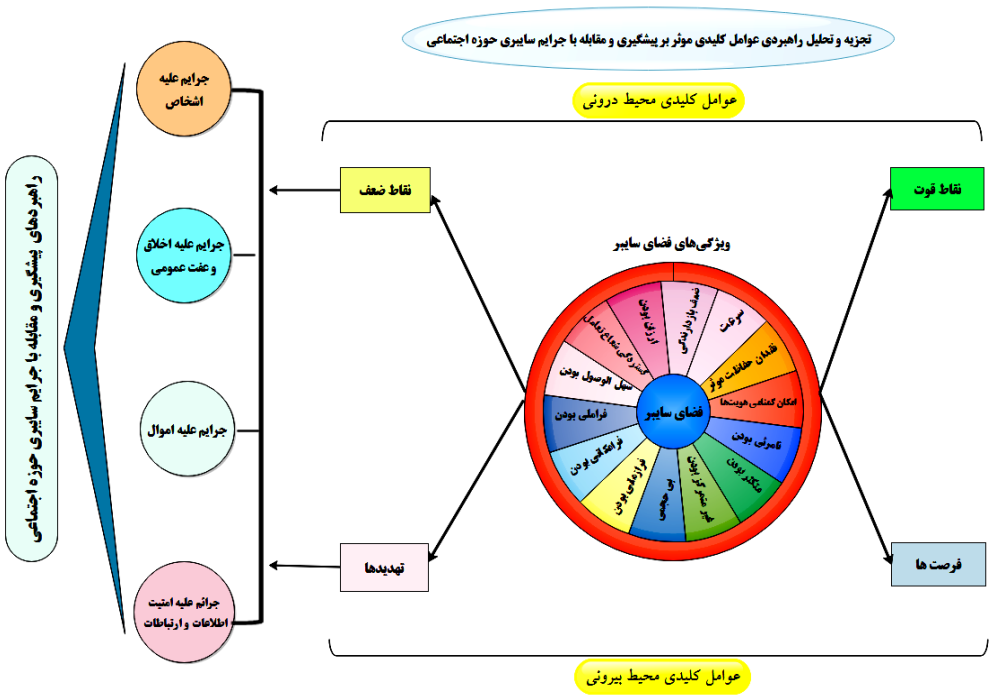
۳– اسناد بالادستی: اسناد بالادستی شامل تدابیر، فرمان‌ها و احکام صادره توسط مقام معظم رهبری (مدظله‌العالی)، قانون اساسی، قوانین موضوعه، سیاست‌های کلی، اسناد راهبردی، مصوبات قانونی، آراء و تصمیمات الزام‌آور، قطعنامه‌ها و کنوانسیون‌های بین‌المللی پذیرفته‌شده به‌عنوان شاخص‌های اصلی و خط‌مشی‌های تعیین‌کننده در دستیابی به راهبردها مورد توجه قرار گرفته‌اند.

٤- ارکان جهت‌ساز: «ارکان جهت‌ساز» شامل «بیانیه ارزش‌ها»، «بیانیه چشم‌انداز»، «بیانیه مأموریت»، «اهداف بنیادین» و «خط‌مشی‌های ملی» نیز مانند یک قطب‌نما جهت این پژوهش را برای رسیدن به مطلوبیت‌های اساسی، یعنی دستیابی به راهبردهای برتر (کارآمد و اثربخش) مشخص می‌کند.

۵- مدل راهبردپردازی: از آنجایی که تکنیک SWOT دیوید برای تدوین راهبرد در ابعاد سازمان‌های بزرگ و یا یک کشور پاسخگو بوده و به راهبردپرداز فرصت شناسایی، ارزیابی و انتخاب راهبردهای برتر را می‌دهد در این پژوهش از آن استفاده شده است.

- مکتب تدوین راهبرد: مکتب مورد توجه برای تدوین راهبردهای این پژوهش «مکتب تلفیقی یا ترکیب‌بندی» است. چراکه در فرآیند تدوین راهبردها به اصول، ارکان، بنیان‌ها و اهداف رویکرد تجویزی داشته و در روش‌ها و ابزار دارای رویکرد توصیفی است.

د) مدل مفهومی پژوهش



شکل ۱) مدل مفهومی پژوهش

در این شکل، فضای سایبر به‌عنوان یک پدیده جدید و تأثیرگذار در نقطه عزیمت مدل برای فهم مسئله قرار گرفته است. فضای سایبر یا فضای غیرملموس که محصول آخرین دستاوردهای علمی بشر به‌ویژه فناوری اطلاعات و ارتباطات است دارای ویژگی‌های خاص و بعضاً منحصربه‌فردی است که تا حد زیادی آن را از فضای ملموس متمایز کرده است. این فضا نیز مانند سایر محیط‌ها دارای نقاط قوت و ضعف، فرصت‌ها و تهدیدهایی است که بخش اعظم آن متأثر از همین ویژگی‌ها است. درهم‌تنیدگی عوامل آسیب‌زا با حضور افراد جامعه‌ستیز، متخلف و مجرم و سوء فعالیت آنان، موجب وقوع جرائمی است که معضلات و مشکلات زیادی را برای مردم و مسئولین ایجاد کرده است. به تبعیت از سنت پذیرفته‌شده و رایج تقسیم جرائم در حقوق جزای اختصاصی و منطق حاکم بر آن؛ یعنی توجه به آثار زیان‌بار و جهات مشترک جرائم، می‌توان آن‌ها را به چهار دسته به شرح زیر تقسیم کرد:

الف) جرائم علیه اشخاص؛

ب) جرائم علیه اموال؛

ج) جرائم علیه عفت و اخلاق عمومی؛

د) جرائم علیه امنیت اطلاعات و ارتباطات.

از آنجایی که این مدل به فهم مسئله پژوهش کمک کرده و تا حدودی وضعیت را شبیه‌سازی کرده است، پژوهشگر سعی می‌کند با استفاده از خروجی‌های آن در قدم بعدی با بهره‌گیری از تکنیک SWOT اقدام به راهبردپردازی کند.

روش‌شناسی پژوهش

پژوهش حاضر از حیث طرح تحقیق، در زمره تحقیقات «آینده‌نگر» با رویکرد نتیجه‌گرا دسته‌بندی می‌گردد؛ چراکه درصدد تبیین و ارائه راهبردهای پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران است.

تحقیق را می‌توان با توجه به هدف به سه دسته بنیادی، کاربردی و تحقیق و توسعه تقسیم کرد (سرمد، بازرگان و حجازی،۱۳۸٤:۸۲). بر همین اساس این پژوهش به لحاظ هدف، «کاربردی-توسعه‌ای» است.

رویکرد این پژوهش با توجه به ماهیت، ویژگی‌های اهداف و سؤال‌ها و بر اساس نوع داده‌ها، کمی است. همچنین بر اساس نحوه گردآوری داده‌ها (مطالعه اسناد بالادستی، مبانی نظری، پیشینه ها و پرسشنامه)، روش آن «توصیفی-تحلیلی» از نوع «پیمایشی و اسنادی» است. تحقیقات پیمایشی به‌منظور کشف واقعیت‌های موجود یا آنچه هست انجام می‌شود(دلاور،۱۳۸٤:۱۰۲).

قلمروی زمانی این پژوهش «افق پنج‌ساله آینده» و قلمروی مکانی آن «فضای سایبر کشور جمهوری اسلامی ایران» است. از آنجایی که هدف اصلی این پژوهش، دستیابی به راهبردهای پیشگیری و مقابله با جرائم سایبری حوزه اجتماعی است؛ بنابراین قلمروی موضوعی آن نیز «جرائم سایبری حوزه اجتماعی» است. مکان انجام این پژوهش نیز کشور جمهوری اسلامی ایران است.

جامعه آماری این پژوهش شامل خبرگان و صاحب‌نظران عرصه‌های مختلف فناوری اطلاعات و ارتباطات به‌ویژه فضای سایبر و خبرگان دانش راهبردی، آشنا با جرائم سایبری حوزه اجتماعی است که دارای مدرک تحصیلی کارشناسی ارشد یا بالاتر بوده و در دانشگاه عالی دفاع ملی، دانشگاه علوم انتظامی امین، پلیس فضای تبادل اطلاعات و ارتباطات (فتا)، سپاه پاسداران انقلاب اسلامی و وزارت اطلاعات مشغول به تحصیل و یا فعالیت هستند. با توجه به ویژگی‌های پیش‌گفته، حجم جامعه آماری تعداد ٦٨ نفر است. با توجه به اینکه حجم جامعه آماری این پژوهش کمتر از ۱۰۰ نفر است، بنابراین روش نمونه‌گیری به‌صورت تمام‌شمار و حجم نمونه آماری مساوی جامعه آماری، یعنی تعداد ٦٨ نفر در نظر گرفته شده است.

برای گردآوری داده‌ها از روش مطالعه اکتشافی به‌منظور تدوین مبانی نظری و ادبیات موضوع و روش مطالعه میدانی و جمع‌آوری اطلاعات مورد نظر از جامعه آماری استفاده

شد. ابزار گردآوری داده‌ها پرسشنامه محقق‌ساخته به تعداد ٤٦ گویه و بر اساس مقیاس درجه‌بندی لیکرت بود. روایی پرسشنامه از طریق روایی محتوایی و پایایی آن از طریق آلفای کرونباخ به دست آمد.

برای تجزیه‌وتحلیل داده‌های گردآوری‌شده از شاخص‌های آمار توصیفی و آمار استنباطی استفاده گردید. در بخش آمار توصیفی از جداول فراوانی مطلق، فراوانی نسبی، میانگین و انحراف معیار و در بخش آمار استنباطی برای رتبه‌بندی پاسخ‌های ارائه‌شده توسط پاسخگویان از آزمون فریدمن استفاده شد. برای دستیابی به راهبردهای اجرایی و پاسخ به سؤال‌های تحقیق با استفاده از تکنیک SWOT هر یک از عوامل نقاط قوت، نقاط ضعف، فرصت‌ها و تهدیدها با توجه به محیط داخلی و خارجی حوزه اجتماعی فضای سایبر کشور شناسایی شد. در ادامه با استفاده از ماتریس ارزیابی موقعیت و اقدام راهبردی[1] موقعیت راهبردی حوزه اجتماعی فضای سایبر کشور تعیین و راهبردهای مناسب آن تدوین و با استفاده از ماتریس کمی برنامه‌ریزی راهبردی[2] اولویت آن‌ها نیز تعیین و برای انتخاب راهبردهای برتر نیز از معیار ارزیابی بحرانی استفاده گردید.

تجزیه‌وتحلیل داده‌ها و یافته‌های پژوهش

جرائم سایبری حوزه اجتماعی در جمهوری اسلامی ایران کدامند؟

الف) جرائم علیه اشخاص: این جرائم شامل توهین، افترا و هتک حیثیت، نشر اکاذیب به قصد تشویش اذهان عمومی، منتسب نمودن اعمالی برخلاف حقیقت به دیگران، نقض حریم خصوصی، اهانت به مقامات رسمی و مأمورین دولتی، مزاحمت اینترنتی، تهدید و اخاذی، تحریک، ترغیب، تهدید، دعوت یا فریب افراد به استعمال مواد مخدر یا روان‌گردان، آموزش یا تسهیل شیوه استعمال مواد مخدر یا روان‌گردان، تحریک، ترغیب، تهدید، دعوت یا فریب افراد به خودکشی، آموزش یا تسهیل شیوه خودکشی، تحریک،

1. SPACE
2. QSPM

ترغیب، تهدید، دعوت یا فریب افراد به ارتکاب اعمال خشونت‌آمیز و آموزش یا تسهیل شیوه ارتکاب اعمال خشونت‌آمیز است.

ب) جرائم علیه اموال: این جرائم شامل سرقت، کلاه‌برداری، برداشت اینترنتی غیر مجاز از حساب‌های بانکی، نقض حقوق و مالکیت معنوی، قماربازی، پول‌شویی و انجام معاملات غیرقانونی است.

ج) جرائم علیه عفت و اخلاق عمومی: این جرائم شامل انتشار، توزیع، معامله، تولید، ذخیره و نگهداری محتواهای مستهجن و مبتذل، تحریک، ترغیب، تطمیع و یا فریب افراد برای دستیابی آنان به محتویات مستهجن و مبتذل، آموزش یا تسهیل شیوه دستیابی افراد به محتویات مستهجن و مبتذل، تحریک، ترغیب، تهدید، دعوت یا فریب افراد به ارتکاب جرائم منافی عفت یا انحرافات جنسی، آموزش یا تسهیل شیوه ارتکاب جرائم منافی عفت یا انحرافات جنسی است.

د) جرائم علیه امنیت اطلاعات و ارتباطات: این جرائم شامل دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی، شنود غیرمجاز سامانه‌های رایانه‌ای، مخابراتی، امواج الکترومغناطیسی و نوری، جعل داده‌های رایانه‌ای، جعل کارت‌های حاوی داده، استفاده از ابزار و داده مجعول، تخریب، غیر قابل پردازش نمودن، مختل نمودن و حذف نمودن داده‌ها، از کار انداختن سامانه‌ها، ممانعت غیر مجاز از دسترسی اشخاص به سامانه‌های خود، سرقت داده‌های رایانه‌ای، استفاده غیر مجاز از پهنای باند بین‌المللی، نقض قوانین و مقررات فیلترینگ (پالایش)، تولید، انتشار، توزیع، در دسترس قرار دادن یا معامله داده‌ها، نرم‌افزارها یا ابزار الکترونیکی ارتکاب جرائم رایانه‌ای، فروش، انتشار یا در دسترس قرار دادن گذرواژه برای دسترسی غیرمجاز به داده‌ها، سامانه‌های رایانه‌ای و مخابراتی، انتشار یا در دسترس قرار دادن محتویات آموزش دسترسی و شنود غیرمجاز، جاسوسی رایانه ای و تخریب و اخلال در داده ها یا سامانه‌های رایانه‌ای و مخابراتی است.

نقاط قوت حوزه اجتماعی فضای سایبری جمهوری اسلامی ایران کدامند؟

جدول ۱) نقاط قوت حوزه اجتماعی فضای سایبر به ترتیب اولویت

	گویه	برآیند
S1	امکان تمرکز بر مهم‌ترین و پرتکرارترین جرائم	٤.۰٤
S2	امکان حضور، مشارکت و فعالیت همه افراد و گروه‌ها در فضای سایبر	۳.۹۵
S3	امکان تمرکز روی بزهکاران و مجرمین پرخطر	۳.۸٤
S4	وجود متخصصان پیشگیری و مقابله با جرائم سایبری	۳.۷۹
S5	سرعت عمل در کشف جرائم فضای سایبر	۳.٦۳
S6	حمایت پلیس از کاربران	۳.۵۷
S7	پایبندی کاربران به ارزش‌های دینی و اصول اخلاقی	۳.٤۱
S8	حمایت سیستم قضایی از کاربران	۳.۳۹
S9	تلاش برای تغییر انگیزه‌های مجرمانه افراد	۳.۱۵

نقاط ضعف حوزه اجتماعی فضای سایبری جمهوری اسلامی ایران کدامند؟

جدول ۲) نقاط ضعف حوزه اجتماعی فضای سایبر به ترتیب اولویت

	گویه	برآیند
W1	عدم دسترسی کامل برای جمع‌آوری ادله الکترونیکی غیر قابل انکار ... ادامه اثبات جرم	۳.۸۲
W2	بی‌دفاع بودن گروه‌های آسیب‌پذیر	۳.۷۹
W3	ضعف در تجمیع بانک‌های اطلاعاتی مورد نیاز برای پیشگیری و مقابله	۳.۷۷
W4	عدم رعایت اصول و قواعد امنیتی حضور در فضای سایبر (پیکره‌بندی صحیح سامانه‌ها و استفاده از رمزهای قوی، آنتی‌ویروس و فایروال)	۳.۷٦
W5	پایین بودن سطح سواد استفاده از فضای سایبر (سواد دیجیتال، سواد اینترنت، سواد رسانه‌ای)	۳.۷٤
W6	ضعف سامانه‌های محافظ الکترونیکی (رمزکننده‌ها و توکن‌ها)	۳.۷۱
W7	ضعف در فرهنگ‌سازی، آگاهی‌بخشی و آموزش همگانی جامعه	۳.٦٦
W8	کندی رفع خلأهای تقنینی به موازات سرعت رشد و توسعه فضای سایبر	۳.٦۵
W9	ضعف شبکه ملی اطلاعات	۳.۵۷
W10	ضعف نظارت والدین بر کودکان و نوجوانان	۳.۵۳
W11	ضعف سرویس‌دهنده‌های پست الکترونیکی بومی	۳.٤۸
W12	ضعف شبکه‌های اجتماعی و پیام‌رسان‌های بومی	۳.٤٦
W13	ضعف در نظارت و کنترل دسترسی کاربران به فضای سایبر	۳.٤٦
W14	ناکافی بودن میزان دسترسی پلیس فتا به زیرساخت‌های فنی، ارتباطی و سامانه‌های اطلاعاتی برای تشخیص و مقابله با جرائم برخط	۳.٤۵
W15	نبود سامانه‌های عامل بومی	۳.٤۱
W16	کمبود تجهیزات نوظهور و امکانات مرتبط با مأموریت پلیس فتا	۳.۳۵
W17	ضعف موتورهای جستجوی بومی	۳.۲۷

فرصت‌های حوزه اجتماعی فضای سایبری جمهوری اسلامی ایران کدامند؟

جدول ۳) فرصت‌های حوزه اجتماعی فضای سایبر به ترتیب اولویت

	گویه	برآیند
O1	نظارت الکترونیکی و گشت‌زنی پلیس در فضای سایبری	۳.۸۸
O2	همکاری و تعامل بین پلیس و ارائه‌دهندگان خدمات اینترنت (ISP)	۳.۷۸
O3	امکان استفاده از ظرفیت‌های علمی دانشگاهی، متخصصین شرکت‌ها و نخبگان بخش خصوصی	۳.٦۷
O4	وجود ظرفیت‌های رسانه‌ای مناسب برای آموزش و جلب مشارکت مردم	۳.٦۰
O5	همکاری بین‌المللی برای تعقیب و کشف جرائم سایبری	۳.۵۵
O6	استفاده از رمزهای یک‌بارمصرف (OTP)	۳.۵٤
O7	اقبال مردم به استفاده از تجهیزات و فناوری‌های مراقبتی و کنترلی و امکان بهره‌برداری از آن‌ها توسط پلیس	۳.٤۸
O8	اعمال نظارت دقیق‌تر بر رایانه‌های عمومی متصل به اینترنت	۳.۳۲
O9	کاهش فرصت‌های وقوع جرم با اعمال فیلترینگ (پالایش) هوشمند	۳.۲٦
O10	محرومیت موقت کاربران متخلف و مجرم برای دسترسی به فضای سایبر	۳.۰۸

تهدیدهای حوزه اجتماعی فضای سایبری جمهوری اسلامی ایران کدامند؟

جدول ٤) تهدیدهای حوزه اجتماعی فضای سایبر به ترتیب اولویت

	گویه	برآیند
T1	توسعه روزافزون جرائم در فضای مجازی	٤.۱۰
T2	روند رو به رشد سازمان‌یافتگی و پیچیده‌تر شدن جرائم در فضای سایبر	٤.۰٦
T3	پنهان بودن هویت کاربران	۳.۹۷
T4	توسعه روزافزون سایت‌های اینترنتی و شبکه‌های اجتماعی مغایر با ارزش‌های دینی و شئونات فرهنگی	۳.۹٤
T5	وجود سرورها و زیرساخت‌های اصلی در خارج از کشور	۳.۸٦
T6	انحصاری بودن اینترنت	۳.٦۸
T7	استفاده از سامانه‌های عامل غیر بومی	۳.٦۲
T8	استفاده از موتورهای جستجوی غیر بومی	۳.٦۰
T9	استفاده از شبکه‌های اجتماعی و پیام‌رسان‌های غیر بومی	۳.۵۷
T10	استفاده از سرویس‌دهنده‌های پست الکترونیکی غیر بومی	۳.٤۸

به‌منظور ترسیم «ماتریس ارزیابی موقعیت و اقدام راهبردی[1]»، میانگین برآیندها به شرح جدول زیر به دست آمد:

جدول ۵) میانگین برآیندها

ر	گویه‌ها	میانگین برآیندها
الف	نقاط قوت	۳/٦٤
ب	نقاط ضعف	۳/۵۸
ج	فرصت‌ها	۳/۵۲
د	تهدیدها	۳/۷۹

با استفاده از مختصات به‌دست‌آمده در جدول بالا و مشخص نمودن نقاط آن روی محورهای نمودار و متصل نمودن این نقاط به یکدیگر، ماتریس ارزیابی موقعیت و اقدام راهبردی ترسیم می‌گردد.

جدول ٦) راهبردهای برتر

اولویت	راهبردها
۱	احراز هویت کاربران برای انجام فعالیت‌های خاص، با استفاده از سازوکارهای فنی یا بیومتریک با کمک متخصصان پیشگیری و مقابله با جرائم سایبری و بهره‌گیری از ظرفیت‌های علمی دانشگاهی، متخصصین شرکت‌ها و نخبگان بخش خصوصی به‌منظور مقابله با توسعه روزافزون جرائم در فضای سایبر
۲	راه‌اندازی، توسعه و استفاده از شبکه ملی اطلاعات به‌منظور کاهش تهدیدات ناشی از انحصاری بودن اینترنت با استفاده از متخصصان داخلی، انتقال فناوری به داخل کشور و استفاده از تجربیات کشورهای موفق.
۳	شناسایی، دستگیری و تعقیب قضایی مرتکبان جرم در فضای سایبر به‌منظور دفاع از گروه‌های آسیب‌پذیر، با تمرکز بر مهم‌ترین و پرتکرارترین جرائم.
٤	افزایش سطح سواد کاربران فضای سایبر (سواد دیجیتال، سواد اینترنت، سواد رسانه‌ای) به‌منظور کاهش تهدیدها و آسیب‌های ناشی از حضور و فعالیت آنان در فضای سایبر از طریق متولیان آموزش رسمی در کشور مانند وزارت آموزش‌وپرورش و وزارت علوم، تحقیقات و فناوری و همچنین رسانه‌های گروهی، مانند رادیو، تلویزیون و مطبوعات با استفاده از متخصصان پیشگیری و مقابله با جرائم سایبری

1. Strategic Position and Action Evaluation (SPACE) Matrix

اولویت	راهبردها
۵	تجمیع بانک‌های اطلاعاتی مورد نیاز برای پیشگیری و مقابله با جرائم سایبری در کشور و افزایش دسترسی پلیس فتا به زیرساخت‌های فنی، ارتباطی و سامانه‌های اطلاعاتی به‌منظور مقابله با توسعه روزافزون جرائم در فضای سایبر
٦	استفاده حداکثری از ظرفیت رسانه‌ها برای فرهنگ‌سازی، آگاهی‌بخشی و آموزش همگانی جامعه در خصوص قابلیت خطرپذیری سامانه‌های متصل به فضای سایبر به‌ویژه رایانه‌ها و تشویق آنان به استفاده از تدابیر امنیتی به‌منظور کاهش وقوع جرائم سایبری.
۷	توسعه و تقویت سامانه‌های محافظ الکترونیکی مانند استفاده از رمزکننده‌ها، توکن‌ها و رمزهای یک‌بارمصرف (OTP) برای تراکنش‌های مالی در فضای سایبر به‌منظور جلوگیری از جرائم مالی ازجمله برداشت‌های غیرمجاز از حساب‌های بانکی.
۸	سرعت عمل در کشف جرائم، شناسایی، دستگیری و تعقیب قضایی مرتکبان جرم در فضای سایبر به‌منظور جلوگیری از توسعه روزافزون جرائم با تمرکز روی مهم‌ترین و پرتکرارترین جرائم
۹	از دسترس خارج کردن شبکه‌های اجتماعی و پیام‌رسان‌های زمینه‌ساز وقوع جرائم اجتماعی و ترغیب و تشویق کاربران به استفاده از نمونه‌های بومی و تحت کنترل از طریق اعتمادسازی و افزایش مزیت‌های رقابتی آن‌ها
۱۰	محدودسازی سایت‌های اینترنتی و شبکه‌های اجتماعی مغایر با ارزش‌های دینی و شئونات فرهنگی از طریق اعمال فیلترینگ هوشمند و تقویت پایبندی کاربران به ارزش‌های دینی و اصول اخلاقی
۱۱	تسریع در رفع خلأهای تقنینی به‌منظور کارآمدی و اثربخشی بیشتر قوانین در کاهش وقوع جرائم سایبری از طریق تصویب قوانین جدید، اصلاح قوانین قبلی و نسخ قوانین متناقض، ناکارآمد و مزاحم به موازات سرعت رشد و توسعه فضای سایبر
۱۲	جلوگیری از روند رو به رشد سازمان‌یافتگی و پیچیده‌تر شدن جرائم در فضای سایبر از طریق تمرکز روی بزهکاران و مجرمین پرخطر با استفاده از متخصصان پیشگیری و مقابله با جرائم سایبری

نتیجه‌گیری

جرائم سایبری حوزه اجتماعی در جمهوری اسلامی ایران کدامند؟

مرجع پاسخ به این سؤال، قانون جرائم رایانه‌ای مصوب ۱۳۸۸/۳/۵ مجلس شورای اسلامی بوده و ملاک اصلی تقسیم‌بندی پنج‌گانه آن نیز رویکرد حقوقی، به‌ویژه سنت پذیرفته‌شده و رایج در حقوق جزای اختصاصی و منطق حاکم بر آن؛ یعنی توجه به آثار زیان‌بار و جهات مشترک جرائم است. با این توصیف جرائم سایبری حوزه اجتماعی در

ج.ا.ا عبارت‌اند از: الف) جرائم علیه اشخاص؛ ب) جرائم علیه اموال؛ ج) جرائم علیه عفت و اخلاق عمومی؛ د) جرائم علیه امنیت اطلاعات و ارتباطات. گفتنی است مصادیق هر یک در بخش تجزیه‌وتحلیل داده‌ها و یافته‌های پژوهش مشروحاً بیان شده است.

نقاط قوت حوزه اجتماعی فضای سایبری جمهوری اسلامی ایران کدامند؟

۱) امکان تمرکز بر مهم‌ترین و پرتکرارترین جرائم؛
۲) امکان حضور، مشارکت و فعالیت همه افراد و گروه‌ها در فضای سایبر؛
۳) امکان تمرکز روی بزهکاران و مجرمین پرخطر؛
٤) وجود متخصصان پیشگیری و مقابله با جرائم سایبری؛
۵) سرعت عمل در کشف جرائم فضای سایبر؛
٦) حمایت پلیس از کاربران؛
۷) پایبندی کاربران به ارزش‌های دینی و اصول اخلاقی؛
۸) حمایت سیستم قضایی از کاربران؛
۹) تلاش برای تغییر انگیزه‌های مجرمانه افراد.

نقاط ضعف حوزه اجتماعی فضای سایبری جمهوری اسلامی ایران کدامند؟

۱) عدم دسترسی کامل برای جمع‌آوری ادله الکترونیکی غیر قابل انکار برای اثبات جرم؛
۲) بی‌دفاع بودن گروه‌های آسیب‌پذیر؛
۳) ضعف در تجمیع بانک‌های اطلاعاتی مورد نیاز برای پیشگیری و مقابله؛
٤) عدم رعایت اصول و قواعد امنیتی حضور در فضای سایبر (پیکره‌بندی صحیح سامانه‌ها و استفاده از رمزهای قوی، آنتی‌ویروس و فایروال)؛
۵) پایین بودن سطح سواد استفاده از فضای سایبر (سواد دیجیتال، سواد اینترنت، سواد رسانه‌ای)؛
٦) ضعف سامانه‌های محافظ الکترونیکی (رمزکننده‌ها و توکن‌ها)؛
۷) ضعف در فرهنگ‌سازی، آگاهی‌بخشی و آموزش همگانی جامعه؛

۸) کندی رفع خلأهای تقنینی به موازات سرعت رشد و توسعه فضای سایبر؛
۹) ضعف شبکه ملی اطلاعات؛
۱۰) ضعف نظارت والدین بر کودکان و نوجوانان؛
۱۱) ضعف سرویس‌دهنده‌های پست الکترونیکی بومی؛
۱۲) ضعف شبکه‌های اجتماعی و پیام‌رسان‌های بومی؛
۱۳) ضعف در نظارت و کنترل دسترسی کاربران به فضای سایبر؛
۱٤) ناکافی بودن میزان دسترسی پلیس فتا به زیرساخت‌های فنی، ارتباطی و سامانه‌های اطلاعاتی برای تشخیص و مقابله با جرائم برخط؛
۱۵) نبود سامانه‌های عامل بومی؛
۱٦) کمبود تجهیزات نوظهور و امکانات مرتبط با مأموریت پلیس فتا؛
۱۷) ضعف موتورهای جستجوی بومی.

فرصت‌های حوزه اجتماعی فضای سایبری جمهوری اسلامی ایران کدامند؟

۱) نظارت الکترونیکی و گشت‌زنی پلیس در فضای سایبری؛
۲) همکاری و تعامل بین پلیس و ارائه‌دهندگان خدمات اینترنت[1]؛
۳) امکان استفاده از ظرفیت های علمی دانشگاهی، متخصصین شرکت ها و نخبگان بخش خصوصی؛
٤) وجود ظرفیت‌های رسانه‌ای مناسب برای آموزش و جلب مشارکت مردم؛
۵) همکاری بین‌المللی برای تعقیب و کشف جرائم سایبری؛
٦) استفاده از رمزهای یک‌بارمصرف[2]
۷) اقبال مردم به استفاده از تجهیزات و فناوری‌های مراقبتی و کنترلی و امکان بهره‌برداری از آن‌ها توسط پلیس
۸) اعمال نظارت دقیق‌تر بر رایانه‌های عمومی متصل به اینترنت

1. ISP
2. OTP

٩) کاهش فرصت‌های وقوع جرم با اعمال فیلترینگ (پالایش) هوشمند
١٠) محرومیت موقت کاربران متخلف و مجرم برای دسترسی به فضای سایبر

تهدیدهای حوزه اجتماعی فضای سایبری جمهوری اسلامی ایران کدامند؟

١) توسعه روزافزون جرائم در فضای مجازی؛
٢) روند رو به رشد سازمان‌یافتگی و پیچیده‌تر شدن جرائم در فضای سایبر؛
٣) پنهان بودن هویت کاربران؛
٤) توسعه روزافزون سایت‌های اینترنتی و شبکه‌های اجتماعی مغایر با ارزش‌های دینی و شئونات فرهنگی؛
٥) وجود سرورها و زیرساخت‌های اصلی در خارج از کشور؛
٦) انحصاری بودن اینترنت؛
٧) استفاده از سامانه‌های عامل غیر بومی؛
٨) استفاده از موتورهای جستجوی غیر بومی؛
٩) استفاده از شبکه‌های اجتماعی و پیام‌رسان‌های غیر بومی؛
١٠) استفاده از سرویس‌دهنده‌های پست الکترونیکی غیر بومی.

راهبردهای پیشگیری و مقابله با جرائم سایبری حوزه اجتماعی در جمهوری اسلامی ایران کدامند؟

١) احراز هویت کاربران برای انجام فعالیت های خاص، با استفاده از سازوکارهای فنی یا بیومتریک با کمک متخصصان پیشگیری و مقابله با جرائم سایبری و بهره‌گیری از ظرفیت‌های علمی دانشگاهی، متخصصین شرکت‌ها و نخبگان بخش خصوصی به‌منظور مقابله با توسعه روزافزون جرائم در فضای سایبر؛
٢) راه‌اندازی، توسعه و استفاده از شبکه ملی اطلاعات به‌منظور کاهش تهدیدات ناشی از انحصاری بودن اینترنت با استفاده از متخصصان داخلی، انتقال فناوری به داخل کشور و استفاده از تجربیات کشورهای موفق؛

۳) شناسایی، دستگیری و تعقیب قضایی مرتکبان جرم در فضای سایبر به‌منظور دفاع از گروه‌های آسیب‌پذیر، با تمرکز بر مهم‌ترین و پرتکرارترین جرائم.

٤) افزایش سطح سواد کاربران فضای سایبر (سواد دیجیتال، سواد اینترنت، سواد رسانه‌ای) به‌منظور کاهش تهدیدها و آسیب‌های ناشی از حضور و فعالیت آنان در فضای سایبر از طریق متولیان آموزش رسمی در کشور، مانند وزارت آموزش‌وپرورش و وزارت علوم، تحقیقات و فناوری و همچنین رسانه های گروهی مانند رادیو، تلویزیون و مطبوعات با استفاده از متخصصان پیشگیری و مقابله با جرائم سایبری؛

۵) تجمیع بانک‌های اطلاعاتی مورد نیاز برای پیشگیری و مقابله با جرائم سایبری در کشور و افزایش دسترسی پلیس فتا به زیرساخت‌های فنی، ارتباطی و سامانه‌های اطلاعاتی به‌منظور مقابله با توسعه روزافزون جرائم در فضای سایبر؛

٦) استفاده حداکثری از ظرفیت رسانه ها برای فرهنگ‌سازی، آگاهی‌بخشی و آموزش همگانی جامعه در خصوص قابلیت خطرپذیری سامانه های متصل به فضای سایبر به‌ویژه رایانه‌ها و تشویق آنان به استفاده از تدابیر امنیتی به‌منظور کاهش وقوع جرائم سایبری؛

۷) توسعه و تقویت سامانه‌های محافظ الکترونیکی مانند استفاده از رمزکننده‌ها، توکن‌ها و رمزهای یک‌بارمصرف[1] برای تراکنش‌های مالی در فضای سایبر به‌منظور جلوگیری از جرائم مالی ازجمله برداشت‌های غیرمجاز از حساب‌های بانکی؛

۸) سرعت عمل در کشف جرائم، شناسایی، دستگیری و تعقیب قضایی مرتکبان جرم در فضای سایبر به‌منظور جلوگیری از توسعه روزافزون جرائم با تمرکز روی مهم‌ترین و پرتکرارترین جرائم؛

۹) از دسترس خارج کردن شبکه‌های اجتماعی و پیام‌رسان‌های زمینه‌ساز وقوع جرائم اجتماعی و ترغیب و تشویق کاربران به استفاده از نمونه های بومی و تحت کنترل از طریق اعتمادسازی و افزایش مزیت‌های رقابتی آن‌ها؛

1. OTP

۱۰) محدودسازی سایت‌های اینترنتی و شبکه‌های اجتماعی مغایر با ارزش‌های دینی و شئونات فرهنگی از طریق اعمال فیلترینگ هوشمند و تقویت پایبندی کاربران به ارزش‌های دینی و اصول اخلاقی؛

۱۱) تسریع در رفع خلأهای تقنینی به‌منظور کارآمدی و اثربخشی بیشتر قوانین در کاهش وقوع جرائم سایبری از طریق تصویب قوانین جدید، اصلاح قوانین قبلی و نسخ قوانین متناقض، ناکارآمد و مزاحم به موازات سرعت رشد و توسعه فضای سایبر؛

۱۲) جلوگیری از روند رو به رشد سازمان‌یافتگی و پیچیده‌تر شدن جرائم در فضای سایبر از طریق تمرکز روی بزهکاران و مجرمین پرخطر با استفاده از متخصصان پیشگیری و مقابله با جرائم سایبری.

پیشنهادها

الف) پیشنهادهای کاربردی

۱- بازنگری، اصلاح و تکمیل قانون جرائم رایانه‌ای جمهوری اسلامی ایران؛

۲- تشکیل قرارگاه ارتقای امنیت در فضای سایبر و تلاش مستمر و مضاعف همه متولیان مربوط، برای مهار جرم در این فضا؛

۳- تشکیل رده پلیس فتا در شهرهای با جمعیت بیش از ۱۰۰ هزار نفر (توسعه ساختاری)؛

٤- تأمین منابع انسانی متخصص و واگذاری امکانات به‌روز و تجهیزات مورد نیاز پلیس فتا؛

۵- برگزاری دوره‌های علمی و کارگاه‌های آموزشی مستمر برای کارکنان پلیس فتا در سراسر کشور در خصوص مبارزه با جرائم سایبری؛

٦- تلاش مستمر برای افزایش سطح سواد استفاده از فضای سایبر (سواد دیجیتال، سواد اینترنت، سواد رسانه‌ای) در میان همه اقشار و گروه‌های جامعه؛

۷- انعقاد تفاهم‌نامه همکاری با سایر کشورها برای تعقیب و کشف جرائم سایبری؛

۸- فراهم نمودن سازوکارهای احراز هویت بیومتریک برای دسترسی کاربران به فضای سایبر؛

۹- تشکیل انباره داده‌های ملی[1] با محوریت سازمان ثبت احوال و فراهم نمودن دسترسی برای پلیس فتا و مقامات قضایی کشور؛

۱۰-تجمیع بانک‌های اطلاعاتی کشور به‌منظور تغذیه انباره داده ملی؛

۱۱-رایزنی‌های بین‌المللی برای شکستن انحصار حاکمیت اینترنت؛

۱۲-توسعه استفاده از رمزهای یک‌بارمصرف؛[2]

۱۳-اجبار شرکت‌ها، مؤسسه‌ها و نهادهای خارجی مایل به فعالیت در حوزه اجتماعی فضای سایبری ج.ا.ا برای انتقال سرورها، زیرساخت‌ها و سایر ذخیره‌سازها به داخل کشور و اخذ تضمین‌های معتبر و محکمه‌پسند برای همکاری با پلیس و سیستم قضایی در هنگام وقوع جرائم؛

۱۴-تولید سامانه‌های عامل بومی با استفاده از ظرفیت‌های علمی دانشگاهی، متخصصین داخلی و نخبگان بخش خصوصی و ترغیب و تشویق کاربران به بهره‌برداری از آن‌ها؛

۱۵-توسعه و تقویت موتورهای جستجوی بومی و بهره‌گیری از ظرفیت‌های رسانه‌ای برای ترغیب و تشویق کاربران به استفاده از آن‌ها؛

۱۶-توسعه و تقویت سرویس‌دهنده‌های پست الکترونیکی بومی و بهره‌گیری از ظرفیت‌های رسانه‌ای برای ترغیب و تشویق کاربران به استفاده از آن‌ها؛

۱۷-راه‌اندازی، توسعه و استفاده از شبکه ملی اطلاعات؛

۱۸-جذب و بهره‌گیری از توانمندی هکرهای نخبه تواب برای پیشگیری و مقابله با جرائم سایبری.

ب) پیشنهادهای علمی– پژوهشی

۱- بررسی جرائم سایبری حوزه امنیتی و راهبردهای پیشگیری و مقابله با آن در جمهوری اسلامی ایران؛

1. National Data Warehouse(NDWH)
2. OTP

۲- بررسی و ریشه‌یابی مستمر علل وقوع جرائم اجتماعی فضای سایبر و ارائه راهکارهای پیشگیری و مقابله با آن در قالب طرح‌های تحقیقاتی زودبازده؛
۳- انجام تحقیقات علمی برای ساخت و تولید سخت‌افزارها و نرم‌افزارهای بومی؛
٤- انجام مطالعات تطبیقی مستمر برای شناخت راهبرهای پیشگیری و مقابله با جرم در سایر کشورها؛
۵- آینده‌پژوهی جرائم در فضای سایبر به‌صورت مستمر؛
٦- مشارکت نخبگان کشور در طرح‌های تحقیقاتی بین‌المللی مربوط به مبارزه با جرائم سایبری؛
۷- مطالعه تطبیقی قوانین بازدارنده جرائم فضای سایبر در کشورهای مطرح جهان؛
۸- بررسی نقش همکاری‌های بین‌المللی در مبارزه با جرائم سایبر.

فهرست منابع ومآخذ

الف) منابع فارسی

۱. امام خامنه‌ای (مدظله‌العالی)، مجموعه بیانات، قابل دسترسی در: WWW.Khamenei.ir

۲. پرویزی، رضا، (۱۳۷۹)، پیشگیری وضعی و نقش آن در پیشگیری از قتل، تهران، انتشارات معاونت آموزش ناجا.

۳. درزی، محمد و همکاران (۱۳۹۲)، مطالعه تحلیلی رویکرد مدیریت فضای سایبری در ایالات متحده آمریکا (پروژه تحقیقاتی)، پژوهشکده فناوری اطلاعات و ارتباطات.

٤. دلاور، علی، (۱۳۸٤)، روش تحقیق در روان‌شناسی و علوم تربیتی، تهران، نشر ویرایش.

۵. رامک، مهراب (۱۳۹۷)، ارائه الگوی راهبردی همکاری‌های بین‌المللی برای ارتقای امنیت فضای مجازی بر اساس منافع ملّی ج.ا.ایران، با رویکرد مبارزه با جرائم سایبری (رساله دکتری) دانشگاه عالی دفاع ملی.

٦. ستارزاده، داوود (۱۳۸۸)، شناسایی تهدیدها و فرصت‌های مجازی در سطح استان مازندران- با تأکید بر اینترنت (پروژه تحقیقاتی)، سپاه کربلای استان مازندران.

۷. سرمد، زهره؛ بازرگان، عباس؛ حجازی، الهه، (۱۳۸٤)، روش‌های تحقیق در علوم رفتاری، تهران، آگاه.

۸. صادق محمدی، حمیدرضا (۱۳۷۸)، شناخت کلی جرائم رایانه‌ای و روش‌های مبارزه با آن، (پروژه تحقیقاتی)، نیروی انتظامی جمهوری اسلامی ایران.

۹. کاستلز، مانوئل، (۱۳۸۰)، عصر اطلاعات: اقتصاد، جامعه و فرهنگ ظهور جامعه شبکه‌ای، جلد اول، مترجم احد علیقلیان و همکاران، تهران، انتشارات طرح نو.

۱۰. کلدی، علیرضا، (بهار ۱۳۸۱)، انحراف، جرم و پیشگیری، فصلنامه علمی-پژوهشی رفاه اجتماعی، سال ۱، شماره ۳.

۱۱. مالمیر، مهدی (تابستان ۱۳۸۸)، مروری بر نظریه‌های جرم‌شناختی و جامعه‌شناختی پیشگیری از جرم بر اساس تقسیم‌بندی «ون ویک» و «دوارد»، فصلنامه مطالعات پیشگیری از جرم، سال چهارم، شماره ۱۱.

۱۲. معظمی، شهلا (۱۳۸۸)، بزهکاری کودکان و نوجوانان، چاپ اول، تهران، انتشارات دادگستر.

۱۳. مک‌لوهان، مارشال (۱۳۷۷)، برای درک رسانه‌ها، ترجمه سعید آذری، چاپ اول، تهران، انتشارات مرکز تحقیقات، مطالعات و سنجش برنامه‌ای صداوسیما.

۱٤. نجفی علمی، مرتضی (۱۳۹۱)، روند تحولات فضای سایبر و نقش آن در تهدیدات ناشی از جرم در محیط سایبر، مورد: مدیریت تهدیدات (رساله دکتری) دانشکده علوم اجتماعی دانشگاه علامه طباطبایی.

ب) منابع انگلیسی

1. Bennet, Trever, (1998), **Crime and Prevention,** The Handbook of Crime and Punishment, Edited by Michael Tonry, New York, Oxford University Press.
2. Jaishankar, K, (2008), **Space Transition Theory of Cyber Crimes**. In Schmallager, F, & Pittaro, M, (Eds.), Crimes of the Internet, Upper Saddle River, NJ: Prentice Hall.
3. Lavorgna, Anita, (2011), **Criminal Behavior in the Internet Age: The Social Organization of Transnational Organized Crime,** (Doctoral thesis), Italy: University of Trento.
4. McQuail, Denis, (2010), **McQuail`s Mass Communication Theory,** 6th edition, California, Sage Publication Ltd.
5. Sultan Alkaabi, Ali Obaid, (2010), **Combating Computer Crime: An International Perspective,** (Doctoral thesis), Australia, Queensland University.
6. Toffler, Alvin & Heidi Toffler, (1995) **Creating a New Civilization: The Politics of the Third Wave,** USA, Turner.
7. Turkle, Sherry, (1995), **Life on the Screen: Identity in the Age of the Internet,** New York, Simon and Schuster.