# الگوی راهبردی مقابله با جرایم سایبری در ایران

رضا صبح‌خیز[1]
بابک پورقهرمانی[2]
علی صفاری[3]

تاریخ دریافت: ۹۹/۹/۸ تاریخ پذیرش نهایی: ۹۹/۱۱/۲۹
فصلنامه مطالعات راهبردی ناجا/ سال پنجم / شماره هجدهم -زمستان۱۳۹۹*۱۱۲-۷۷

## چکیده

یکی از مهم‌ترین مسائل و دغدغه‌های جوامع بشری، ایجاد و توسعه امنیت، برقراری نظم و تأمین آسایش عمومی جامعه می‌باشد؛ از این حیث، جوامع سایبری امروزی نیز از این امر مستثنی نبوده و نهادهای مربوط به‌دنبال ارائه راهبردهایی برای رسیدن به این هدف مهم هستند. بر این اساس، پژوهش حاضر با هدف کلی ارائه الگوی راهبردی مبارزه با جرایم سایبری در ایران و همچنین، شناسایی، تبیین و تدوین مفاهیم، ابعاد، مولفه‌ها و شاخص‌های مطلوب مبارزه با جرایم سایبری در ایران انجام گردیده‌است. تحقیق حاضر، از نظر هدف، از نوع بنیادی بوده و روش تولید و تحلیل داده‌ها، ترکیبی از روش‌های کیفی و کمی است؛ به‌طوری که در مرحله کیفی، با مطالعه اسناد و منابع کتابخانه‌ای پیرامون سیاست جنایی، فضای سایبری، جرایم سایبری و جرم‌انگاری و پاسخ‌ها به این نوع جرایم در سطح داخلی و بین‌المللی، چارچوب مفهومی تحقیق شکل گرفته و در ادامه این مرحله، با نمونه‌گیری هدفمند از طریق به‌کارگیری فن گلوله برفی، خبرگانی از جامعه علمی و تجربی فضای سایبری به تعداد ۳۰ نفر شناسایی و انتخاب شدند. برای مصاحبه با این افراد، از ابزار مصاحبه نیمه ساختاریافته و برای تولید داده‌های نهایی، از کدگذاری باز و محوری استفاده گردید. به‌منظور سنجش یافته‌ها، اولویت‌بندی و اعتبارسنجی، از نظرات تعداد ۶۰ نفر از نخبگان و متخصصان جرایم سایبری به‌عنوان حجم نمونه با به‌کارگیری ابزار پرسش‌نامه در بخش کمی استفاده شده‌است. نتایج حاصل از این تحقیق نشان می‌دهد که الگوی راهبردی مبارزه با جرایم سایبری در ایران چه می‌تواند باشد و نیز ابعاد، مولفه‌ها و معرف‌های آن کدامند.

**واژگان کلیدی:** فضای سایبری، فضای مجازی، جرایم سایبری، مبارزه با جرایم سایبر

---

۱. دانشجوی دکترای حقوق کیفری و جرم شناسی واحد علوم و تحقیقات دانشگاه آزاد اسلامی
reza123onlymorning@gmail.com
۲. دانشیار گروه حقوق جزا و جرم‌شناسی دانشگاه آزاد اسلامی واحد مراغه (نویسنده مسئول)، b.pourghahramani@yahoo.com
۳. دانشیار دانشکده حقوق دانشگاه شهید بهشتی(ره) a-Saffary@ sbu.ac.ir

**مقدمه**

فناوری اطلاعات و ارتباطات روز به روز در حال تکامل و پیشرفت بوده و تا لایه‌های پایین و جزئی جوامع بشری نفوذ پیدا کرده‌است. فضای مجازی زائیده فناوری اطلاعات و ارتباطات است؛ فضای کاملا رویایی که انسان‌ها با آن انس گرفته‌اند و به آن علاقه‌مندند؛ فضایی که با دارا بودن قابلیت‌های منحصربه‌فردی چون دقت، سرعت، ذخیره‌سازی حجم بالای اطلاعات، خستگی‌ناپذیری، تبادل سریع اطلاعات، دسترسی آسان و محاسن بی‌شمار دیگر شده‌است تا ارتباطات نزدیک و نزدیک‌تر و به‌تبع آن، کارها سهل‌تر انجام پذیرد؛ اما در هر ارتباط و جامعه‌ای، طبعی است که تهدیدها، آسیب‌ها و ناهنجاری‌هایی پدیدار می‌گردد که شکل صحیح این ارتباطات را دستخوش تغییر منفی می‌سازد. فضای مجازی با تمام قابلیت‌ها و پیچیدگی‌ها به‌شدت در مقابل این عوامل آسیب‌پذیر است؛ بر این اساس و با توجه به ویژگی‌های منحصربه‌فرد فضای مجازی، مجرمان و تبهکاران رغبت وافری در جهت استفاده از این فضا به‌ویژه از بستر شبکه‌های اجتماعی آن برای ارتکاب اعمال نابهنجار خود نشان می‌دهند که از این اعمال با عنوان "جرایم سایبری" یاد می‌شود.

از سوی دیگر، جرم سایبری اغلب دارای بعد بین‌المللی است و ابعاد بین‌المللی این نوع جرایم موجب شده‌است تا افراد مختلف، از جمله جرم‌شناسان، حقوق‌دانان و پلیس به مطالعه و بررسی همه‌جانبه این پدیده روی آوردند؛ به‌طوری که تدوین قوانین و اجرای مجازات با توجه به فراملی بودن ماهیت جرایم سایبری به مسئله‌ای پیچیده به‌ویژه در حقوق بین‌الملل تبدیل شده‌است؛ چراکه وقوع این نوع جرایم موجب تشدید خلأهای قانونی و قضایی حاکم در حقوق بین‌الملل همانند تشخیص صلاحیت دادگاه‌های کشورها نسبت‌به رسیدگی و نیز تعارض قوانین این کشورها در برخورد با جرایم سایبری شده‌است؛ بنابراین، با توجه به خلأهای حقوقی و قضایی و حتی همکاری‌های انتظامی در سطح داخلی و بین‌المللی و به‌تبع آن، سردرگمی و هزینه‌های کشف جرم نیز در مواجهه مقامات مسئول با این نوع جرایم بسیار مشهود می‌باشد.

باتوجه به موارد کلی یادشده، باید اذعان نمود که جامعه جهانی امروزه، با جلوه خاص و نوینی از جرم مواجه گردیده‌است که به موجب آن، حوزه کنترل این نوع جرایم در زمینه‌های حاکمیتی و جامعوی، به‌شدت دچار چالش شده و به نظر می‌رسد که با معیارها و الگوهای مطلق معرفی‌شده پیشین، نمی‌توان کنترل مناسبی را بر روی این جرایم اعمال نمود و از طرفی، با توجه به سطح گستردگی معضلات و چالش‌های حوزه‌های مختلف فضای عمومی سایبری

همانند مبتنی‌بودن بر فناوری اطلاعات و ارتباطات، افزایش تعداد کاربران فضای سایبری، دسترسی به اطلاعات معیوب یا غلط، از دست دادن کارکردهای کنترل، ابعاد بین‌المللی، سرعت فرآیندهای مبادله اطلاعات، توسعه فضای سایبری، ارتباطات بی‌نام، دسترسی آسان به ابزارها و هزینه پایین و دسترسی آسان به اینترنت و نیز چالش‌های حقوق کیفری و بین‌الملل در طیف شکلی و ماهوی و چالش‌های پلیسی در حوزه پی‌جویی و مبارزه؛ بنابراین، تنها راهی که باقی می‌ماند ارائه الگو است؛ چراکه با اقدامات مقطعی نمی‌توان این چالش‌های فراگیر را مرتفع نمود.

بر این اساس، پژوهش حاضر با هدف کلی ارائه الگوی راهبردی مبارزه با جرایم سایبری در ایران و نیز هدف فرعی شناسایی، تبیین و تدوین مفاهیم، ابعاد، مولفه‌ها و شاخص‌های مطلوب مبارزه با جرایم سایبری در ایران به‌دنبال پاسخ به این سوال اصلی است که «الگوی راهبردی مبارزه جرایم سایبری در ایران چیست؟» از این حیث، باید به سوالات فرعی‌ای همچون «ابعاد، مولفه‌ها و شاخص‌های الگوی راهبردی مبارزه با جرایم سایبری در ایران کدامند؟» نیز پاسخ داده شود.

این تحقیق به‌دلیل اکتشافی بودن، فاقد فرضیه است؛ بنابراین، به نظر می‌رسد که بهترین روش انجام تحقیق روش آمیخته(کیفی ـ کمی) باشد؛ به‌طوری که در مرحله کیفی، با مطالعه اسناد و منابع کتابخانه‌ای پیرامون سیاست جنایی، فضای سایبری، جرایم سایبری و جرم‌انگاری و پاسخ‌ها به این نوع جرایم در سطح داخلی و بین‌المللی چارچوب مفهومی تحقیق شکل گرفته و در ادامه این مرحله، با نمونه‌گیری هدفمند از طریق به‌کارگیری فن گلوله‌برفی، خبرگانی از جامعه علمی و تجربی فضای سایبری به تعداد ۳۰ نفر شناسایی و انتخاب شده‌اند. برای مصاحبه با این افراد، از ابزار مصاحبه نیمه ساختاریافته و برای تولید داده‌های نهایی از کدگذاری باز و محوری استفاده گردید. به‌منظور سنجش یافته‌ها، اولویت‌بندی و اعتبارسنجی، از نظرات تعداد ٦٠ نفر از نخبگان و متخصصان جرایم سایبری به‌عنوان حجم نمونه با به‌کارگیری ابزار پرسش‌نامه در بخش کمی استفاده شده‌است.

اعتبارسنجی نهایی این پژوهش، از طریق آزمون‌های آماری و تحلیلی از طریق نرم‌افزار spss صورت پذیرفت. در این نوع اعتبارسنجی، روابط بین متغیرهای هم‌عرض با یکدیگر و نیز در طول ابعاد، مولفه‌ها و شاخص‌ها بر اساس چرخه عاملی و آزمون‌های مرتبط مورد ارزیابی و راستی‌آزمایی قرار می‌گیرد.

## ادبیات و مفاهیم تحقیق

**فضای سایبری:** از نظر شکلی، فضای سایبری پدیده‌ای است کل از جزء که می‌تواند ابعاد مختلفی را همانند اینترنت، مخابرات، رادیو، تلویزیون و کلیه مواردی که از ویژگی‌های کلی ـ یعنی شبکه، تهیه داده و انتقال داده ـ برخوردار است را شامل گردد. بر این اساس، فضای سایبری را می‌توان چنین تعریف نمود: «فضایی است در امتداد فضای فیزیکی که غیرقابل لمس بوده و توسط ابزارهای رایانه‌ای و الکترونیکی در جهت ارتباطات درونی انسان‌ها بر بستر تهیه، ساخت و انتقال داده‌های الکترونیکی ایجاد گردیده‌است»؛ بنابراین، از این تعریف، در مرتبه نخست، غیرقابل لمس بودن و فیزیکی نبودن این فضا ـ که نقطه متمایز از فضای فیزیکی می باشد ـ و در مرتبه دوم، ارتباطات درونی انسان‌ها توسط تهیه و انتقال داده ـ که باز هم متمایز از فضای فیزیکی می‌باشد ـ و در مرتبه سوم، استفاده از ابزار الکترونیکی ـ که به صورت مشترک، در هر دو فضا می‌باشد ـ را می‌توان نتیجه گرفت. این تعریف می‌تواند به‌نوعی تلفیقی از ماهیت و پوسته فضای سایبری را شامل گردد(حافظ نیا، ۱۸: ۱۳۹۱).

از نظر ماهوی، به نظر می‌رسد همچنان‌که ماهیت فضای فیزیکی را تنها می‌توان از لحاظ علم فیزیک تعریف کرد، می‌توان ماهیت فضای سایبری را نیز از نوع علم فیزیک تعریف نمود. در تشریح گذر از فضای فیزیکی به فضای مجازی، می‌توان گفت که در فضای فیزیکی، انسان در یک بعد خاصی از مکان و زمان زندگی می‌کند؛ به‌طوری که شنوایی و بینایی او فقط یک محدوده فرکانسی خاص را درک می‌کند. این فرکانس در شنوایی، محدود ۲۰ هرتز تا ۲۰ کیلو هرتز و در بینایی، طیف مادون قرمز تا ماورا بنفش(۱۸۴ ترا هرتز تا ۷۸۹ ترا هرتز) را شامل می‌گردد؛ چراکه موجودیت فیزیکی و قدرت سمعی ـ بصری انسان، فرکانس‌های بالاتر و پایین‌تر از این طیف را درک نمی‌کند؛ به‌عنوان مثال، یک مورچه در طیف فرکانسی متفاوتی از فرکانس‌های طیف بالا، در فضا صدا پخش می‌کند اما باتوجه به اینکه آن فرکانس در محدوده شنوایی انسان نیست، گوش انسان قادر به شنیدن این فرکانس‌ها نمی‌باشد. با توجه به اینکه محدوده فرکانسی فیزیکی یا واقعی(بینایی و شنوایی) دارای قدرت پایینی بوده و به‌سرعت زمین‌گیر می‌شود(جاذبه زمین) و قدرت خود را از دست می‌دهد، بنابراین، این نقطه‌ضعف موجب می‌گردد که ما برای انتقال صدا و تصویر واقعی به جاهای دوردست، از فرکانس‌های قوی‌تر(بالاتر) یا طول موج پایین‌تر استفاده نماییم؛ چراکه هرقدر فرکانس قوی‌تر باشد، شدت مقاومت آن بر زمین بالاتر خواهد بود. به این فرکانس‌های قوی‌تر که دامنه گسترده‌ای را شامل

می‌شود، فرکانس یا امواج الکترومغناطیس(رادیویی) گفته می‌شود که طیف ۲۰ کیلو هرتز تا ۳۰ گیگا هرتز را شامل می‌گردد و اسامی آنها عبارتند از: فرکانس‌های خیلی پایین، فرکانس‌های پایین، فرکانس‌های متوسط، فرکانس‌های بالا، فرکانس‌های خیلی بالا، فرکانس‌های مافوق بالا[1].

از هرکدام از این طیف‌ها برای عملکرد پخش و انتشار[2] خاصی استفاده می‌گردد؛ به‌عنوان مثال، امواج فرکانس‌های بالا[3] برای پخش و انتشار دور بُرد استفاده می‌شود؛ به‌طوری‌که این طیف به لایه یونسفر زمین تابیده شده و بازتابش آن در نقطه دیگری از زمین به‌دست می‌آید. امواج خیلی بالا[4] در انتشار آنتن به آنتن و مستقیم استفاده می‌گردد و امواج مافوق بالا[5] در انتشار ماهواره‌ای استفاده می‌گردد. شکل زیر، وضعیت طیف‌های فرکانسی واقعی، الکترومغناطیسی و نوری را نشان می‌دهد:


شکل ۱. شکل‌گیری فضای سایبری

با این وجود، برای اینکه فرکانس واقعی برای نقاط دوردست فرستاده شودف مولفه این فرکانس(فرکانس واقعی) بر روی فرکانس‌های بالاتر(امواج الکترومغناطیس یا نوری) ادغام شده(مدولاسیون)[6] و در فضا پخش می‌گردد و در نقطه‌ای که باید فرکانس فضای واقعی دریافت شود، امواج الکترومغناطیس از امواج قابل‌دسترس تفکیک می‌گردد که به آن، دمدولاسیون[7]

1. Very Low Frequencies(VLF). Low Frequencies(LF). High Frequencies(HF). Very High Frequencies(VHF). Super High Frequencies(SHF)
2. Broadcasting
3. hf
4. VHF,UHF
5. SHF
6. modulation
7. de modulation

گفته می‌شود؛ به‌عنوان مثال، تصویری که توسط دوربین فیلم برداری صدا و سیما گرفته می‌شود، دارای فرکانس قابل لمس(۲۰ هرتز تا ۲۰ کیلو هرتز) است که توسط امواج فرکانسی خیلی بالا مدوله شده(ادغام شده) و در فضا پخش می‌شود و در مکان دیگری توسط ابزاری مانند تلویزیون، این فرکانس دمدوله(تفکیک کردن فرکانس‌ها از همدیگر) شده و در نهایت، فرکانس‌های واقعی توسط تلویزیون پخش می‌گردد. با این اوصاف، از زمان مدولاسیون تا دمدولاسیون، ما در فضای سایبری قرار می‌گیریم؛ فضایی که دیگر فرکانس‌های قابل‌لمس(۲۰ هرتز تا ۲۰ کیلو هرتز) در دسترس ما قرار ندارد و توسط امواج دیگری حمل می‌شود. پس زمانی که سخن از فضای سایبری می‌شود، باید توجه کنیم که این فضا شامل فرکانسی است که فرکانس‌های قابل‌لمس ما را به‌صورت آنالوگ یا دیجیتال حمل می‌کند. این فرایند می‌تواند نگاه کاملی از ماهیت فضای مجازی را به ما بدهد(صبح خیز، ۱۳۹۸: ۳۶).

**جرم سایبری**: تعاریف گوناگونی از جرم سایبری از سوی سازمان‌ها، متخصصان و در برخی از قوانین کشورها ارائه شده‌است که وجود تفاوت در آنها بیانگر ابهامات موجود در ماهیت و تعریف این نوع از جرایم است و از آنجا که این نسل از جرایم هنوز سیر مراحل تکاملی خود را طی می‌کند، بنابراین، از تعریف قطعی برخوردار نیست؛ ولی تاکنون در تعریف جرم سایبری، وسیله بودن، هدف بودن و موضوع بودن رایانه و وسایل مخابراتی و الکترونیکی تثبیت شده‌است(زیبر، ۱۳۷۶: ۴۵). با توجه به این رویکرد، جرم سایبری عمدتاً به دو شکل زیر توصیف می‌شود:

۱. جرم سایبری انتقال‌یافته(توسعه‌یافته): جرایم سایبری انتقالی، جرایمی هستند که قبلاً در فضای واقعی به‌عنوان جرم تعریف شده‌اند و در حال حاضر، این جرایم به فضای سایبر انتقال یافته‌اند؛ همانند سرقت و کلاهبرداری که در فضای واقعی، جرم است و در حال حاضر، این جرایم در فضای سایبر نیز اتفاق می‌افتد. امروزه، اغلب جرایم سایبری که در دنیا اتفاق می‌افتد، در این بخش از جرایم سایبری تعریف می‌شود؛ چراکه بسترهای فنی، حقوقی و اجتماعی تعریف‌شده در فضای سایبری، منطبق‌با معیارهای عینی در فضای فیزیکی است و مجرمان بدین‌سان، به‌دنبال تسرّی معیارهای کسب‌شده از تجربیات خود در فضای فیزیکی به فضای سایبری هستند. عمده جرایم این بخش، مرتبط با حوزه‌های مالی ـ اعم از سرقت و کلاهبرداری ـ است. مجرمان این حوزه، اغلب مجرمان سنتی هستند که در حال حاضر، اقدامات مجرمانه خود را به فضای سایبر انتقال داده‌اند.

۲. جرم سایبری محض: جرمی است که فقط مختص فضای سایبر بوده و تا پیش از این، از جرایم سنتی به شمار نمی‌رفته‌است و تنها با شکل‌گیری فضای سایبر می‌تواند اتفاق بیفتد؛

همانند هک یا ساپوتاژ(تخریب داده)؛ به این معنی که باید داده وجود داشته باشد تا تخریب انجام شود). به نظر می‌رسد که این بخش از جرایم نیز با توسعه بسترهای فنی توسعه پیدا کرده‌است. در برخی از موارد، مشاهده می‌کنیم که مجرمان جهت انجام فعل مجرمانه خود در ردیف اول(انتقال‌یافته) به‌ناچار مرتکب این نوع از جرایم شده‌اند تا بتوانند فعل ردیف اول را صورت دهند. به‌عنوان مثال، مرتکب جهت برداشت غیرمجاز و یا سرقت از حساب‌های بانکی(جرم سایبری انتقال‌یافته) در گام اول، ساختار امنیتی بانک را مورد هک و نفوذ قرار می‌دهد(جرم سایبری محض)(صبح خیز، ۱۳۹۸: ۷۲).

به‌هرحال، جهت تبیین ماهیت جرایم سایبری، باید از ساختارهای تبیین‌شده در جرم‌شناسی استفاده کرد و لازم است که ماهیت جرم سایبری را از نقطه‌نظر حقوقی تبیین نمود؛ چراکه جرم، خود، یک پدیده اجتماعی و حقوقی است؛ بنابراین، باید مؤلفه جرم در جرم‌شناسی را در بستر جرایم سایبری مورد بررسی و تحقیق و توسعه قرار داد. بر این اساس، جرم سایبری را برابر قوانین و مقررات کشورمان چنین می‌توان تعریف کرد: «جرم سایبری هر فعل یا ترک فعلی است که به‌وسیله انسان با ابزارهای الکترونیکی در فضای سایبری صورت گیرد و برابر قوانین کشور جرم محسوب گردد».

## الگوی راهبردی مبارزه با جرایم سایبری

زمانی‌که صحبت از الگو می‌شود، باید به‌دنبال روش‌های ذهنی و انتزاعی کلی بر اساس تئوری‌های پیشین گشت. این در حالی است که در مدل، همین روش‌های ذهنی کسب‌شده توسط الگو را در دامنه واقعیت پیاده سازی می‌نماییم؛ بنابراین، الگو و مدل شاید از ریشه یکنواختی برخوردار باشند اما در مرحله اجرا با همدیگر متفاوت هستند و به نوعی مدل، رنگ و بوی عملیاتی‌تری را به خود می‌گیرد. به عبارتی، الگوها را باید شفاف نمود تا به مدل برسیم. با توجه به نوپایی موضوعات مرتبط با فضای سایبری، محقق بر آن است که به‌دنبال الگو بر اساس سه زمینه ساختار، برنامه‌ریزی و اجرا باشد؛ چراکه تا زمانی که الگو احصا نگردد، ارائه مدل کار عبث و بیهوده‌ای است. بنابراین، در ارائه الگوی راهبردی در این مقوله، ضمن اینکه به‌دنبال بررسی وضعیت موجود هستیم، باید با نگاه به وضعیت مطلوب، الگوی خود را ارائه دهیم تا جنبه راهبردی داشته‌باشد.

از سوی دیگر، "مبارزه" در لغت، به‌معنی رویارویی و مواجهه است و در اصطلاح، به وضعیتی اطلاق می‌گردد که در مقابل و متضاد با یک پدیده، شی، حیوان و یا انسان اتخاذ می‌گردد. با

وجود اینکه در بسیاری از موارد، واژه مقابله و مبارزه در یک مفهوم به‌کار گرفته می‌شود اما به نظر می‌رسد که معنای "مقابله" فراگیرتر از "مبارزه" است که بیشتر وضعیت قبل از مبارزه را در بر دارد. به عبارت دیگر، می‌توان گفت که وضعیت مبارزه در دل وضعیت مقابله قرار دارد و مبارزه زیرمجموعه‌ای از مقابله است. "مبارزه" رزمیدن و جنگیدن نیز معنی شده‌است؛ پس نمایان است که در این وضعیت، اقدامات عملیاتی تر و تهاجمی‌تر مورد نظر می‌باشد. مبارزه دارای ابعاد عملیاتی و کارکردی بوده و بیشتر میل به تهاجم برای سرکوب پدیده مجرمانه را دارد. اغلب، این رفتارهای تهاجمی در جوامع مختلف، از طریق نیروهای انتظامی و پلیس صورت می‌گیرد اما مجموعه مولفه‌هایی که مبارزه را شامل می‌گردد را در سه سطح قضایی، اداری و انتظامی می‌توان تعریف و تشریح نمود.

وضعیت "مقابله" با وجود دارا بودن وضعیت عملیاتی، دارای وضعیت قبل‌از عملیات ـ اعم از پیش‌بینی و پیشگیری ـ نیز می‌باشد. مقابله به هرگونه واکنش و اقدام عملی(نوعاً سلبی) در برابر خطرات و تهدیدات افراد و جامعه اطلاق می‌شود؛ به عبارتی، مقابله عبارت است از تلاش‌های فکری، هیجانی و رفتاری فرد که هنگام روبه‌رو شدن با فشارهای روانی به‌منظور غلبه، تحمل یا به حداقل رساندن عوارض استرس به‌کار گرفته می‌شود(نادری، ۱۳۹۸: ۱۱۷). با این اوصاف و برای نیل به یک ادبیات مشترک در این حوزه، در حوزه جرایم، به‌ویژه درخصوص جرایم سایبری، می‌توان واژه "مبارزه" یا "مقابله" را در یک مفهوم به‌کار برد و چنین تعریف کرد: «مقابله و یا مبارزه با جرم سایبری، مجموعه رفتارها و اقدامات و یا وضعیتی را شامل می‌گردد که در مواجهه با پدیده مجرمانه، از طرف شخص، جامعه و یا حاکمیت، در ابعاد داخلی و بین‌المللی اتخاذ می‌گردد و هدف از آن، تحت‌کنترل درآوردن پدیده مجرمانه است که شامل اقدامات قبل از وقوع، حین وقوع و بعد از وقوع جرم می‌گردد». بنابراین، تمامی واژه‌های مبارزه و مقابله در این تحقیق، در یک طیف، سطح و معنی استفاده می‌شوند و شامل اقدامات کنشی و واکنشی هستند.

باتوجه به موارد پیش‌گفته، الگوی مبارزه با جرایم سایبری را می‌توان چنین تبیین کرد: این الگو شامل متغیرهای کلان و راهبردی می‌باشد که حاوی چیستی‌های مبارزه فراگیر با جرایم سایبری است؛ به عبارت دیگر، منظور از این الگو آن است که برای مقابله با جرایم سایبری، به چه چیزهایی نیازمند هستیم تا با به‌کارگیری آنها بتوانیم جرم سایبری را در قبل، حین و بعد از وقوع جرم، تحت‌کنترل قرار داده و مدیریت نماییم.

## یافته‌های تحقیق

در مرحله کیفی تا مرحله اقناع و رسیدن به اهداف تحقیق، از ابزار مصاحبه استفاده شده‌است و به همین منظور، نتایج چارچوب مفهومی جهت بومی‌سازی و تطبیق با شرایط موجود، از طریق مصاحبه‌های کیفی با نخبگان و کارشناسان مرتبط با موضوع پژوهش به بحث گذاشته شده و با کدگذاری باز و محوری صورت گرفته‌است. برخی از گزاره‌های نامرتبط که با شرایط مورد مطالعه هم‌خوانی نداشتند، حذف و گزاره‌های جدیدی متناسب با شرایط مورد مطالعه اضافه گردید. نتیجه این مرحله، تقطیر و خلاصه‌سازی انبوه اطلاعات کسب‌شده از مصاحبه‌ها به درون مفاهیم و دسته‌بندی‌های آنها(کدگذاری باز) و ایجاد رابطه بین مقوله‌های تولیدشده در کدگذاری باز است(کدگذاری محوری). نتایج مرحله کیفی به شرح جدول‌های ۱ الی ٤ می‌باشد که پایه و اساس مرحله کمی را شکل می‌دهد.

**۱- بعد بزه‌انگاری:** بر اساس اصول سیاست جنایی و کدگذاری باز و محوری صورت‌گرفته بر روی مقولات احصاشده، بزه انگاری یکی از ابعاد تشکیل‌دهنده الگوی راهبردی ترسیم گردید. این بعد به‌عنوان یکی از ارکان مهم الگو مطرح بوده و معرف‌های شناسایی‌شده در ٤ مولفه جامعوی، دولتی در سطح داخلی، دولتی در سطح بین‌المللی و غیردولتی در سطح بین‌المللی به شرح جدول شماره ۱ تبیین شده‌است و حاوی معرف‌های مرتبط با وضع، همکاری، مشارکت و الحاق به قوانین و مقررات داخلی و بین‌الملل می‌باشد.

جدول شماره ۱. جدول احصای ابعاد، مولفه‌ها و معرف‌ها در حوزه بزه‌انگاری

| مفهوم | بُعد | مولفه‌ها | معرف‌ها |
|---|---|---|---|
| | | جامعوی | مشارکت موثر در تدوین مقررات داخلی شرکت‌های ارائه‌دهنده خدمات اینترنتی و سایبری برای کاربران |
| | | | نقش موثر در فرهنگ‌سازی در مدرسه(تبیین قواعد سبک زندگی در مدرسه) |
| | | | مشارکت موثر در تدوین مقررات داخلی اصناف و اتحادیه‌ها |

| | | | |
|---|---|---|---|
| مبارزه با جرایم سایبری در ایران | بزه انگاری سایبری | | نقش موثر در فرهنگ‌سازی در خانواده(تبیین قواعد سبک زندگی در خانواده) |
| | | | نقش موثر در فرهنگ‌سازی در جامعه(تبیین قواعد سبک زندگی در جامعه) |
| | | دولتی در سطح داخلی | مشارکت موثر در تدوین قوانین شکلی کیفری(آئین دادرسی) |
| | | | مشارکت موثر در تدوین قوانین ماهوی کیفری |
| | | | مشارکت موثر در تدوین قوانین(غیرکیفری) |
| | | | مشارکت موثر درتدوین مقررات، آئین‌نامه‌ها و دستورکارهای دولتی(غیرکیفری) |
| | | | تدوین مقررات(آئین‌نامه‌ها و دستورکارهای) انتظامی مرتبط |
| | | دولتی در سطح بین‌المللی | مشارکت موثر در الحاق به کنوانسیون‌های مربوطه |
| | | | تدوین دکترین راهبردی بین‌المللی پلیسی |
| | | | ایجاد رویه‌های قضایی پلیسی بین‌المللی |
| | | | مشارکت موثر در انعقاد معاهدات دو یا چند جانبه |
| | | | تدوین موافقت‌نامه‌های غیر الزام‌آور انتظامی بین‌المللی(اعلامیه‌ها، تفاهم‌نامه‌ها، توصیه‌نامه‌ها) |

| | | | |
|---|---|---|---|
| | | غیردولتی در سطح بین المللی | مشارکت در تدوین مقررات الزام‌آور ناظر بر کاربران توسط شرکت‌های ارائه‌دهنده سرویس و خدمات اینترنتی و سایبری بین‌المللی |
| | | | مشارکت در تدوین مقررات غیر الزام‌آور (اعلامیه‌ها، توصیه‌نامه‌ها) سازمان‌های مردم‌نهاد غیردولتی بین‌المللی فعال در حوزه سایبری |

**بعد پاسخ‌ها:** بر اساس اصول سیاست جنایی و کدگذاری باز و محوری صورت‌گرفته بر روی مقولات احصاشده، بعد پاسخ‌ها به‌عنوان یکی دیگر از ابعاد تشکیل‌دهنده الگوی راهبردی ترسیم گردید؛ به‌طوری که در این بعد، مجموعه اقدامات عملیاتی که از طریق نهادهای پاسخ‌گو باید بر ضدّ جرم سایبری صورت پذیرد، تدوین شده‌است. این اقدامات شامل اقدامات کنشی و واکنشی سخت و نرم به پدیده جرم سایبری بوده و معرف‌های(شاخص‌های) شناسایی‌شده در این سه مولفه، به شرح جدول شماره ۲ تبیین شده‌است.

جدول شماره ۲. جدول احصای ابعاد، مولفه‌ها و معرف‌ها در حوزه نوع پاسخ‌ها

| مفهوم | بُعد | مولفه‌ها | معرف‌ها |
|---|---|---|---|
| | | کنشی | اشراف اطلاعاتی درخصوص جرایم و مجرمان سایبری |
| | | | تشخیص وقوع جرم سایبری |
| | | | پیشگیری وضعی و اجتماعی از وقوع جرم سایبری |
| | | | پیش‌بینی وقوع جرم سایبری |

| | | | |
|---|---|---|---|
| مبارزه با جرایم سایبری در ایران | پاسخ‌ها | | خنثی‌سازی بر خط جرم سایبری |
| | | واکنشی سخت | نقش موثر و سازنده در اجرای احکام جرم سایبری |
| | | | نقش موثر و سازنده در رسیدگی به جرم سایبری(دادگاه) |
| | | | مرجعیت پیگیری انتظامی جرایم و حملات سایبری در سطح بین‌الملل |
| | | | مرجعیت تحقیقات مقدماتی جرم سایبری |
| | | واکنشی نرم | مشارکت موثر دراقدامات درمانی نسبت‌به بزه‌کاران از طریق جامعه |
| | | | مشارکت موثر دراقدامات درمانی نسبت‌به بزه‌کاران از طریق حاکمیت |
| | | | کمک به مداخلات تربیتی خانواده نسبت‌به بزه‌کاری اعضا |
| | | | کمک به مداخلات تربیتی مدرسه نسبت‌به بزه‌کاری دانش‌آموزان |
| | | | مشارکت موثر در واکنش‌های آگاهی‌بخش و محدودکننده صنفی(اتحادیه‌ها) نسبت به بزه‌کاران سایبری ذی‌نفع خود |
| | | | مشارکت موثر در واکنش‌های آگاهی‌بخش و محدودکننده از طرف شرکت‌های ارائه‌دهنده خدمات رایانه‌ای و سایبری بر کاربران بزه‌کار |

| | | | |
|---|---|---|---|
| | | | مشارکت موثر در مداخلات تربیتی مدنی(امر به معروف و نهی از منکر) نسبت‌به بزه‌کاران سایبری |

**بعد اقدامات مبتنی‌بر فناوری:** از آنجا که فضای سایبری کاملا مبتنی‌بر فناوری اطلاعات بوده و حیات خود را مرهون این فرایند است؛ بنابراین، بر اساس کدگذاری باز و محوری صورت‌گرفته بر روی مقولات احصاشده، بعد اقدامات مبتنی‌بر فناوری به‌عنوان یک بعد جداگانه و به‌عنوان یکی دیگر از ابعاد تشکیل‌دهنده الگوی راهبردی شناسایی گردید. در این بعد، مجموعه اقدامات عملیاتی مبتنی‌بر فناوری که از طریق نهادهای پاسخ گو باید بر ضدّ جرم سایبری صورت پذیرد، تدوین شده‌است. این اقدامات شامل اقدامات قبل، حین و بعد از وقوع جرم بوده و معرف‌های(شاخص‌های) شناسایی‌شده در این سه مولفه به شرح جدول شماره ۳ تبیین شده‌است.

جدول شماره ۳. جدول احصای ابعاد، مولفه‌ها و معرف‌ها در حوزه اقدامات مبتنی‌بر فناوری

| مفهوم | بعد | مولفه‌ها | معرف‌ها |
|---|---|---|---|
| | | | مشارکت موثر درامنیت زیرساخت ارتباطی درون‌سازمانی نهادها |
| | | | مشارکت موثر در احراز هویت کاربران |
| | | | مشارکت موثر در کنترل دسترسی کاربران اینترنت |
| | | | مشارکت موثر در امنیت زیرساخت ارتباطی برون‌سازمانی نهادها |

| | | |
|---|---|---|
| مبارزه با جرایم سایبری در ایران | اقدامات مبتنی‌بر فناوری | اقدامات قبل از وقوع جرم |
| | | مشارکت در امنیت داده‌های ارسالی(برخط) |
| | | پیش‌بینی جرایم و حملات سایبری |
| | | مشارکت موثر در امنیت پایگاه داده |
| | | کنترل دسترسی کارکنان ناجا |
| | | مرجعیت اشراف اطلاعاتی مبتنی‌بر فناوری |
| | | مرجعیت حیطه‌بندی جرایم و حملات سایبری |
| | | همکاری با نهادهای ذی‌نفع در اقدامات پیش دستانه |
| | | ارتقای سطح آگاهی کارکنان ذی‌نفع ناجا |
| | | اقدامات حین وقوع جرم |
| | | مشارکت موثر در خنثی‌سازی برخط حمله سایبری |
| | | همکاری موثر در تشخیص نوع حملات سایبری |
| | | مشارکت موثر در اطلاع‌رسانی برخط نسبت‌به حمله سایبری |
| | | مشارکت موثر درتعیین سطح حملات سایبری |
| | | بررسی و احصای ادله موجود در آثار الکترونیکی |

| | | | |
|---|---|---|---|
| | | اقدامات بعد وقوع جرم | بررسی صحنه جرم الکترونیکی(فارنزیک) |
| | | | حفظ، ضبط و جمع‌آوری آثار و ادله الکترونیکی |
| | | | شناسایی صحنه جرم الکترونیکی |
| | | | همکاری در اقدامات متقابل |

**بعد مدیریتی:** بی‌شک، مدیریت، مهم‌ترین رکن هر راهبرد می‌باشد؛ بنابراین، بر اساس کدگذاری باز و محوری صورت‌گرفته بر روی مقولات احصاشده، بعد مدیریتی نیز به‌عنوان یکی دیگر از ابعاد تشکیل‌دهنده الگوی راهبردی مبارزه با جرایم سایبری شناسایی گردید. در این بعد، مجموعه مدیریت راهبردی، عملیاتی، منابع، ارتباطات و تحقیق و توسعه به‌عنوان مولفه‌های مرتبط شناسایی شده‌است. معرف‌ها(شاخص‌های) شناسایی‌شده در این پنج مولفه، به شرح جدول شماره ۴ تبیین شده‌است.

جدول شماره ۴. جدول احصای ابعاد، مولفه‌ها و معرف‌ها در حوزه مدیریتی

| مفهوم | بُعد | مؤلفه‌ها | معرف‌ها |
|---|---|---|---|
| | | | سهم‌بندی و مسئول‌سازی حوزه امنیتی انتظامی نهادها |
| | | | تدوین راهبردهای امنیتی انتظامی |
| | | | تدوین سیاست‌های امنیتی انتظامی |
| | | | مشارکت موثر درتدوین و تبیین روابط کاری بین نهادهای ذی‌نفع |

| | | | |
|---|---|---|---|
| مبارزه با جرایم سایبری در ایران | مدیریتی | مدیریت راهبردی | مرجعیت هدایت و راهبری مبارزه با جرایم سایبری در کشور |
| | | | آینده‌پژوهی در روندها |
| | | | ارزیابی و نظارت بر کارکرد مطلوب منابع |
| | | مدیریت عملیاتی | برنامه‌ریزی و تدوین راهکارها نقشه راه فرایندها |
| | | | اجرای موثر برنامه‌ها و راهکارها |
| | | | انگیزش کارکنان |
| | | | کنترل و بازرسی |
| | | | قابلیت ایجاد و تغییر در ساختار سازمان |
| | | | تصمیم‌گیری موثر در به‌کارگیری روش‌های مبارزه |
| | | منابع و امکانات | اختصاص منابع مالی مستقل به ناجا مختص مبارزه با جرایم سایبری |
| | | | به‌کارگیری فناوری(سخت‌افزار و نرم‌افزار) به‌روز |
| | | | به‌کارگیری ابزارهای لجستیکی به‌روز |
| | | | به‌کارگیری نیروی انسانی متخصص و متعهد |
| | | | ارتباط موثر ناجا با نهادهای بین‌المللی ذی‌نفع |
| | | | ارتباط موثر ناجا با نهادهای برون‌سازمانی ذی‌نفع |
| | | | نقش موثردر ارتباط بین نهادهای برون‌سازمانی ذی‌نفع |

| | | | |
|---|---|---|---|
| | | ارتباطات | ارتباط موثر بین نهادهای بین‌المللی ذی‌نفع |
| | | | ارتباط موثر بین پلیس‌های تخصصی و یگان‌های درون‌سازمانی ذی‌نفع |
| | | تحقیق و توسعه | ارائه راه‌حل‌های موثر بر چالش‌ها |
| | | | احصای چالش‌های مبارزه با جرایم سایبری |
| | | | نیازسنجی در منابع و الزامات |
| | | | آموزش و یادگیری کارکنان حرفه‌ای |
| | | | خلاقیت و نوآوری در روش‌های مبارزه با جرایم سایبری |

**تحلیل یافته‌های تحقیق:** در مرحله اول از تحلیل کمی، پرسش‌نامه مناسب طراحی شد و در گام نخست، روایی و پایایی پرسش‌نامه طراحی‌شده مورد بررسی قرار گرفت و جهت بررسی روایی نظری، از نظرات تعدادی از کارشناسان خبره بهره‌گیری گردید؛ همچنین، پایایی ابزار سنجش از طریق محاسبه ضریب آلفای کرونباخ مورد بررسی قرار گرفت که نتایج آن در جدول شماره ۵ گزارش شده‌است.

جدول ۵. نتایج پایایی پرسش‌نامه

| ردیف | مولفه‌ها | ضریب آلفا | نتیجه |
|---|---|---|---|
| ۱ | مدیریت راهبردی(مدیریتی) | /۷۴ | میزان پایایی در حد مطلوب |
| ۲ | ارتباطات(مدیریتی) | /۷۱ | میزان پایایی در حد مطلوب |
| ۳ | واکنشی نرم(پاسخ‌ها) | /۷۷ | میزان پایایی در حد مطلوب |

| | | | |
|---|---|---|---|
| ۴ | اقدامات حین وقوع جرم(مبتنی‌بر فناوری) | /۸۱ | میزان پایایی در حد مطلوب |
| ۵ | اقدامات قبل از وقوع جرم(مبتنی‌بر فناوری) | /۸۸ | میزان پایایی در حد مطلوب |
| ۶ | منابع و امکانات(مدیریتی) | /۷۲ | میزان پایایی در حد مطلوب |
| ۷ | دولتی در سطح بین‌المللی(بزه‌انگاری) | /۷۷ | میزان پایایی در حد مطلوب |
| ۸ | تحقیق و توسعه(مدیریتی) | /۷۳ | میزان پایایی در حد مطلوب |
| ۹ | کنشی(پاسخ‌ها) | /۷۵ | میزان پایایی در حد مطلوب |
| ۱۰ | مدیریت عملیاتی(مدیریتی) | /۷۷ | میزان پایایی در حد مطلوب |
| ۱۱ | بعد از وقوع جرم(مبتنی‌بر فناوری) | /۷۶ | میزان پایایی در حد مطلوب |
| ۱۲ | واکنشی سخت(پاسخ‌ها) | /۷۹ | میزان پایایی در حد مطلوب |
| ۱۳ | دولتی در سطح داخلی(بزه‌انگاری) | /۷۸ | میزان پایایی در حد مطلوب |
| ۱۴ | جامعوی(بزه‌انگاری) | /۷۲ | میزان پایایی در حد مطلوب |
| ۱۵ | غیردولتی در سطح بین‌المللی(بزه‌انگاری) | /۷۲ | میزان پایایی در حد مطلوب |
| ۱۶ | کل پرسش‌نامه | /۸۳ | میزان پایایی در حد مطلوب |

با توجه به اینکه مقدار آزمون آلفا در تمامی مولفه‌ها و آلفای کل، بیش از ۷/. می‌باشد، می‌توان با اطمینان ۹۵ درصدی بیان کرد که پرسش‌نامه دارای پایایی مطلوب است.

در بررسی توصیفی معرف‌ها(شاخص‌ها) مشخص گردید که معرف "اشراف اطلاعاتی بر جرایم و مجرمان سایبری" با میانگین ۶/۷۲ در رتبه اول، معرف "پیش‌بینی وقوع جرم سایبری" با میانگین ۶/۷۰ در رتبه دوم و معرف "پیشگیری از وقوع جرم سایبری" با میانگین ۶/۶ در رتبه سوم قرار دارد. همچنین، معرف "تدوین مقررات غیر الزام‌آور(اعلامیه‌ها، توصیه‌نامه‌ها) سازمان‌های مردم‌نهاد غیردولتی بین‌المللی فعال در حوزه سایبری" و "اقدامات درمانی نسبت به بزه‌کاران از طریق جامعه" با میانگین ۵/۶۰ و "مداخلات تربیتی مدنی(امر به معروف و نهی از منکر) نسبت‌به بزه‌کاران سایبری" با میانگین ۴/۹۸ در رتبه‌های آخر قرار دارند. آمار جامع برابر جدول شماره ۶ ارائه شده‌است.

جدول شماره ۶. بررسی توصیفی معرف‌های پرسش‌نامه

| معرف | کمینه | بیشینه | میانگین | انحراف معیار | واریانس |
|---|---|---|---|---|---|
| اشراف اطلاعاتی بر جرایم و مجرمان سایبری | ۵ | ۷ | ۶/۷۲ | ۰/۵۶ | ۰/۳۱ |
| پیش‌بینی وقوع جرم سایبری | ۵ | ۷ | ۶/۷۰ | ۰/۵۳ | ۰/۲۸ |
| پیشگیری وضعی و اجتماعی از وقوع جرم سایبری | ۵ | ۷ | ۶/۶۵ | ۰/۶۳ | ۰/۴۰ |
| مشارکت موثر در امنیت پایگاه داده | ۴ | ۷ | ۶/۶۵ | ۰/۶۸ | ۰/۴۷ |
| مشارکت موثر در احراز هویت کاربران | ۴ | ۷ | ۶/۶۲ | ۰/۶۷ | ۰/۴۴ |
| به‌کارگیری فناوری(سخت‌افزار و نرم‌افزار) به‌روز | ۵ | ۷ | ۶/۶۰ | ۰/۶۲ | ۰/۳۸ |
| تشخیص وقوع جرم سایبری | ۵ | ۷ | ۶/۶۰ | ۰/۵۶ | ۰/۳۱ |
| مشارکت موثر در امنیت زیرساخت ارتباطی درون‌سازمانی نهادها | ۴ | ۷ | ۶/۶۰ | ۰/۶۷ | ۰/۴۵ |

| | | | | | |
|---|---|---|---|---|---|
| اختصاص منابع مالی مستقل به ناجا مختص مبارزه با جرایم سایبری | ۵ | ۷ | ۶/۵۸ | ۰/۶۵ | ۰/۴۲ |
| مشارکت موثر در امنیت زیرساخت ارتباطی برون‌سازمانی نهادها | ۴ | ۷ | ۶/۵۷ | ۰/۷۲ | ۰/۵۲ |
| آموزش و یادگیری کارکنان حرفه‌ای | ۴ | ۷ | ۶/۵۳ | ۰/۶۵ | ۰/۴۲ |
| مشارکت در امنیت داده‌های ارسالی(برخط) | ۴ | ۷ | ۶/۵۰ | ۰/۷۲ | ۰/۵۳ |
| به‌کارگیری ابزارهای لجستیکی به‌روز | ۵ | ۷ | ۶/۵۰ | ۰/۷۰ | ۰/۴۹ |
| نقش موثر در فرهنگ‌سازی در مدرسه(تبیین قواعد سبک زندگی در مدرسه) | ۳ | ۷ | ۶/۴۸ | ۰/۸۵ | ۰/۷۳ |
| حفظ، ضبط و جمع‌آوری آثار و ادله الکترونیکی | ۵ | ۷ | ۶/۴۸ | ۰/۷۰ | ۰/۴۹ |
| نقش موثر در فرهنگ‌سازی در جامعه(تبیین قواعد سبک زندگی در جامعه) | ۳ | ۷ | ۶/۴۷ | ۰/۸۱ | ۰/۶۶ |
| خنثی‌سازی برخط جرم سایبری | ۵ | ۷ | ۶/۴۷ | ۰/۷۲ | ۰/۵۲ |
| ارتقای سطح آگاهی کارکنان دی‌نفع ناجا | ۴ | ۷ | ۶/۴۷ | ۰/۷۲ | ۰/۵۲ |
| شناسایی صحنه جرم الکترونیکی | ۴ | ۷ | ۶/۴۷ | ۰/۷۲ | ۰/۵۲ |

| | | | | | |
|---|---|---|---|---|---|
| خلاقیت و نوآوری در روش‌های مبارزه با جرایم سایبری | ۴ | ۷ | ۶/۴۷ | ۰/۷۲ | ۰/۵۲ |
| نقش موثر در فرهنگ‌سازی در خانواده(تبیین قواعد سبک زندگی در خانواده) | ۳ | ۷ | ۶/۴۵ | ۰/۸۵ | ۰/۷۳ |
| نقش موثر و سازنده در رسیدگی به جرم سایبری(دادگاه) | ۴ | ۷ | ۶/۴۳ | ۰/۷۲ | ۰/۵۲ |
| مشارکت موثر در اطلاع‌رسانی برخط نسبت به حمله سایبری | ۵ | ۷ | ۶/۴۳ | ۰/۷۰ | ۰/۴۹ |
| ارزیابی و نظارت کارکرد مطلوب منابع | ۴ | ۷ | ۶/۴۲ | ۰/۷۹ | ۰/۶۲ |
| مشارکت موثر در خنثی‌سازی بر خط حمله سایبری | ۵ | ۷ | ۶/۴۲ | ۰/۷۷ | ۰/۵۹ |
| انگیزش کارکنان | ۳ | ۷ | ۶/۴۰ | ۰/۸۷ | ۰/۷۵ |
| بررسی صحنه جرم الکترونیکی(فارنزیک) | ۴ | ۷ | ۶/۳۸ | ۰/۹۰ | ۰/۸۲ |
| تصمیم‌گیری موثر در به‌کارگیری روش‌های مبارزه | ۴ | ۷ | ۶/۳۸ | ۰/۷۴ | ۰/۵۵ |
| بررسی و احصای ادله موجود در آثار الکترونیکی | ۴ | ۷ | ۶/۳۸ | ۰/۸۸ | ۰/۷۸ |
| بندی و مسئول‌سازی حوزه سه امنیتی انتظامی نهادها | ۳ | ۷ | ۶/۳۸ | ۰/۹۰ | ۰/۸۲ |
| مرجعیت اشراف‌اطلاعاتی مبتنی‌بر فناوری | ۴ | ۷ | ۶/۳۸ | ۰/۹۰ | ۰/۸۲ |

| | | | | | |
|---|---|---|---|---|---|
| برنامه‌ریزی و تدوین نقشه‌راه فرایندها | ۳ | ۷ | ۶/۳۳ | ۰/۷۳ | ۰/۵۳ |
| ارتباط موثر ناجا با نهادهای برون‌سازمانی ذی‌نفع | ۵ | ۷ | ۶/۳۳ | ۰/۷۱ | ۰/۵۰ |
| ارائه راه‌حل‌های موثر بر چالش‌ها | ۴ | ۷ | ۶/۳۳ | ۰/۷۵ | ۰/۵۶ |
| پیش‌بینی جرایم و حملات سایبری | ۳ | ۷ | ۶/۳۲ | ۰/۹۱ | ۰/۸۳ |
| مشارکت موثر در تدوین و تبیین روابط کاری بین نهادهای ذی‌نفع | ۴ | ۷ | ۶/۳۲ | ۰/۸۹ | ۰/۸۰ |
| همکاری موثر در تشخیص نوع حملات سایبری | ۴ | ۷ | ۶/۳۰ | ۰/۷۷ | ۰/۵۹ |
| نقش موثر در ارتباط بین نهادهای برون‌سازمانی ذی‌نفع | ۵ | ۷ | ۶/۳۰ | ۰/۷۲ | ۰/۵۲ |
| احصای چالش‌های مبارزه با جرایم سایبری | ۵ | ۷ | ۶/۲۸ | ۰/۶۹ | ۰/۴۸ |
| همکاری با نهادهای ذی‌نفع در اقدامات پیش‌دستانه | ۴ | ۷ | ۶/۲۸ | ۰/۷۸ | ۰/۶۱ |
| مرجعیت هدایت و راهبری مبارزه با جرایم سایبری در کشور | ۳ | ۷ | ۶/۲۸ | ۰/۸۵ | ۰/۷۱ |
| نیازسنجی در منابع و الزامات | ۵ | ۷ | ۶/۲۷ | ۰/۶۹ | ۰/۴۷ |
| تدوین راهبردهای امنیتی انتظامی | ۳ | ۷ | ۶/۲۷ | ۰/۸۴ | ۰/۷۱ |
| ارتباط موثر ناجا با نهادهای بین‌المللی ذی‌نفع | ۵ | ۷ | ۶/۲۵ | ۰/۷۳ | ۰/۵۳ |
| مرجعیت تحقیقات مقدماتی جرم سایبری | ۴ | ۷ | ۶/۲۵ | ۰/۸۲ | ۰/۶۷ |

| | | | | | |
|---|---|---|---|---|---|
| نقش موثر و سازنده در اجرای احکام جرم سایبری | ۴ | ۷ | ۶/۲۵ | ۰/۷۷ | ۰/۶۰ |
| کنترل دسترسی کارکنان ناجا | ۳ | ۷ | ۶/۲۵ | ۰/۹۱ | ۰/۸۳ |
| نقش موثر در ارتباط بین نهادهای برون‌سازمانی ذی‌نفع | ۴ | ۷ | ۶/۲۳ | ۰/۷۴ | ۰/۵۵ |
| مشارکت موثر در تدوین قوانین شکلی کیفری(آئین دادرسی) | ۲ | ۷ | ۶/۲۳ | ۱/۰۸ | ۱/۱۶ |
| آینده‌پژوهی در روندها | ۴ | ۷ | ۶/۲۳ | ۰/۸۵ | ۰/۷۲ |
| مشارکت موثر در تدوین مقررات داخلی شرکت‌های ارائه‌دهنده خدمات اینترنتی و سایبری برای کاربران | ۳ | ۷ | ۶/۲۳ | ۰/۹۱ | ۰/۸۳ |
| مشارکت در تدوین مقررات الزام‌آور ناظر بر کاربران توسط شرکت‌های ارائه‌دهنده سرویس و خدمات اینترنتی و سایبری بین‌المللی | ۴ | ۷ | ۶/۲۰ | ۰/۷۸ | ۰/۶۰ |
| مشارکت موثر در تدوین قوانین ماهوی کیفری | ۲ | ۷ | ۶/۲۰ | ۱/۰۲ | ۱/۰۴ |
| مشارکت موثر در تعیین سطح حملات سایبری | ۴ | ۷ | ۶/۲۰ | ۰/۸۲ | ۰/۶۷ |
| تدوین سیاست‌های امنیتی انتظامی | ۳ | ۷ | ۶/۲۰ | ۰/۸۴ | ۰/۷۱ |
| ایجاد رویه‌های قضایی پلیسی بین‌المللی | ۳ | ۷ | ۶/۲۰ | ۰/۹۰ | ۰/۸۱ |

| | | | | | |
|---|---|---|---|---|---|
| نقش موثردر ارتباط بین نهادهای برون‌سازمانی ذی‌نفع | ۴ | ۷ | ۶/۲۰ | ۰/۸۰ | ۰/۶۴ |
| کنترل و بازرسی | ۴ | ۷ | ۶/۱۸ | ۰/۸۵ | ۰/۷۳ |
| مشارکت موثر در کنترل دسترسی کاربران اینترنت | ۳ | ۷ | ۶/۱۷ | ۰/۹۸ | ۰/۹۵ |
| اجرای موثر برنامه‌ها و راهکارها | ۴ | ۷ | ۶/۱۷ | ۰/۷۸ | ۰/۶۲ |
| تدوین دکترین راهبردی بین‌المللی پلیسی | ۴ | ۷ | ۶/۱۵ | ۰/۹۰ | ۰/۸۱ |
| مشارکت موثر در تدوین مقررات داخلی اصناف و اتحادیه‌ها | ۳ | ۷ | ۶/۰۸ | ۱/۰۱ | ۱/۰۳ |
| مرجعیت پیگیری انتظامی جرایم و حملات سایبری در سطح بین‌الملل | ۳ | ۷ | ۶/۰۷ | ۰/۹۷ | ۰/۹۴ |
| قابلیت ایجاد و تغییر در ساختار سازمان | ۳ | ۷ | ۶/۰۵ | ۰/۹۵ | ۰/۹۰ |
| مرجعیت حیطه‌بندی جرایم و حملات سایبری | ۳ | ۷ | ۶/۰۳ | ۱/۰۹ | ۱/۱۹ |
| مشارکت موثر در الحاق به کنوانسیون‌های مربوطه | ۳ | ۷ | ۶/۰۲ | ۰/۹۳ | ۰/۸۶ |
| همکاری در اقدامات متقابل | ۴ | ۷ | ۵/۹۸ | ۰/۸۷ | ۰/۷۶ |
| کمک به مداخلات تربیتی خانواده نسبت به بزه‌کاری اعضا | ۳ | ۷ | ۵/۹۷ | ۱/۰۹ | ۱/۱۹ |
| تدوین مقررات(آئین‌نامه‌ها و دستورکارهای) انتظامی مرتبط | ۳ | ۷ | ۵/۹۰ | ۱/۰۸ | ۱/۱۸ |

| | | | | | |
|---|---|---|---|---|---|
| مشارکت موثر در واکنش‌های آگاهی‌بخش و محدودکننده از طرف شرکت‌های ارائه‌دهنده خدمات رایانه‌ای و سایبری بر کاربران بزه‌کار | ۳ | ۷ | ۵/۸۸ | ۱/۰۶ | ۱/۱۲ |
| مشارکت موثر در تدوین مقررات و آئین‌نامه‌ها و دستورکارهای دولتی(غیرکیفری) | ۳ | ۷ | ۵/۸۳ | ۱/۰۶ | ۱/۱۲ |
| مشارکت موثردر انعقاد معاهدات دو یا چند جانبه | ۳ | ۷ | ۵/۸۰ | ۰/۹۴ | ۰/۸۷ |
| اقدامات انتظامی آگاهی‌بخش و محدودکننده نسبت‌به بزه‌کاران سایبری | ۴ | ۷ | ۵/۷۸ | ۰/۹۰ | ۰/۸۲ |
| مشارکت موثر در تدوین قوانین(غیرکیفری) | ۲ | ۷ | ۵/۷۸ | ۱/۲۴ | ۱/۵۳ |
| کمک در مداخلات تربیتی مدرسه نسبت‌به بزه‌کاری دانش‌آموزان | ۳ | ۷ | ۵/۷۵ | ۱/۱۴ | ۱/۳۱ |
| مشارکت موثر در واکنش‌های آگاهی‌بخش و محدودکننده صنفی(اتحادیه‌ها) نسبت‌به بزه‌کاران سایبری ذی‌نفع خود | ۳ | ۷ | ۵/۷۵ | ۱/۰۵ | ۱/۱۱ |
| مشارکت موثر در اقدامات درمانی نسبت‌به بزه‌کاران از طریق حاکمیت | ۲ | ۷ | ۵/۷۲ | ۱/۱۱ | ۱/۲۲ |
| تدوین موافقت‌نامه‌های غیر الزام‌آور انتظامی بین‌المللی | ۲ | ۷ | ۵/۷۰ | ۱/۱۷ | ۱/۳۷ |

| | | | | | |
|---|---|---|---|---|---|
| مشارکت موثر دراقدامات درمانی نسبت‌به بزه‌کاران از طریق جامعه | ۴ | ۷ | ۵/۶۰ | ۰/۹۸ | ۰/۹۶ |

در تحلیل مولفه‌ها، آزمون‌ها نشان می‌دهند که مقدار عدد به‌دست‌آمده از آزمون‌های چرخه عاملی در رابطه با روابط متغیرهای مربوط به مولفه‌ها در سطح مطلوبی قرار دارند که نتایج آن به شرح جدول ۷ تشریح گردیده‌است.

جدول شماره ۷. جدول مقدار آزمون‌های مولفه

| ردیف | مقدار آزمون KMO | مقدار آزمون بارتلت | سطح معناداری | مقدار واریمکس |
|---|---|---|---|---|
| ۱ | ./۷۷۷ | ۶۶۲/۸۷ | ./۰۰۰ | ۷۱/۲۱ |

مقدار آزمون kmo که ۷۷۷/. و بارتلت که ٦٦٢/٨٧ و سطح معناداری ۰۰۰/. بدان معناست که ۱۹ مولفه موردنظر، به‌درستی ابعاد را می‌سنجند. از طرفی، با توجه به مقدار واریمکس، می‌توان گفت که این ۱۹ مولفه ۷۱/۲۱ درصد از تغییرات ابعاد موردنظر را تبیین می‌کنند. جدول میزان اهمیت معرف‌ها به شرح جدول شماره ۸ می‌باشد.

جدول شماره ۸. جدول میزان اهمیت مولفه‌ها

| ردیف | مولفه‌ها | میزان اهمیت |
|---|---|---|
| ۱ | مدیریت راهبردی | .۷۸۸ |
| ۲ | ارتباطات | .۷۸۶ |
| ۳ | پاسخ‌های واکنشی نرم | .۷۸۰ |
| ۴ | اقدامات حین وقوع جرم مبتنی‌بر فناوری | .۷۸۰ |
| ۵ | اقدامات قبل از وقوع جرم مبتنی‌بر فناوری | .۷۷۳ |
| ۶ | منابع و امکانات | .۷۶۹ |

| | | |
|---|---|---|
| ۷ | بزه‌انگاری دولتی در سطح بین‌المللی | .۷۶۸ |
| ۸ | تحقیق و توسعه | .۷۳۷ |
| ۹ | پاسخ‌های کنشی | .۷۳۳ |
| ۱۰ | مدیریت عملیاتی | .۷۳۰ |
| ۱۱ | اقدامات بعد از وقوع جرم مبتنی‌بر فناوری | .۷۲۱ |
| ۱۲ | پاسخ‌های واکنشی سخت | .۷۰۹ |
| ۱۳ | بزه‌انگاری دولتی در سطح داخلی | .۵۸۳ |
| ۱۴ | بزه‌انگاری جامعوی | .۵۳۶ |
| ۱۵ | بزه‌انگاری غیردولتی در سطح بین‌المللی | .۵۱۹ |

بر این اساس، در بررسی میزان اهمیت معرف‌ها، مشخص می‌شود که مولفه "مدیریت راهبردی" با ضریب ۷۸۸/. در رتبه اول و مولفه "ارتباطات" با ضریب ۷۸۶/. در رتبه دوم و مولفه "واکنشی نرم" با ضریب ۷۸۰/. در رتبه سوم قرار دارد. تحلیل ابعاد نیز حاکی از روابط مطلوب بین متغیرهای مرتبط با ابعاد است که به شرح جدول ۹ ارائه شده‌است.

جدول شماره ۹. جدول مقدار آزمون‌های ابعاد

| ردیف | مقدار آزمون KMO | مقدار آزمون بارتلت | سطح معناداری | مقدار واریمکس |
|---|---|---|---|---|
| **۱** | **./۷۸۵** | **۱۵۶/۴۹** | **./۰۰۰** | **۶۶/۶۳** |

مقدار آزمون kmo که ۷۸۵/. و بارتلت که ۱۵۶/۴۹ و سطح معناداری ۰۰۰/. بدان معناست که ۵ بعد موردنظر، به‌درستی متغیر اصلی "مبارزه با جرایم سایبری در ایران" را می‌سنجند. از طرفی، با توجه به مقدار واریمکس می‌توان گفت که این ۵ بعد ۶۶/۶۳ درصد از تغییرات ابعاد موردنظر را تبیین می‌کنند. جدول میزان اهمیت معرف‌ها به شرح زیر است.

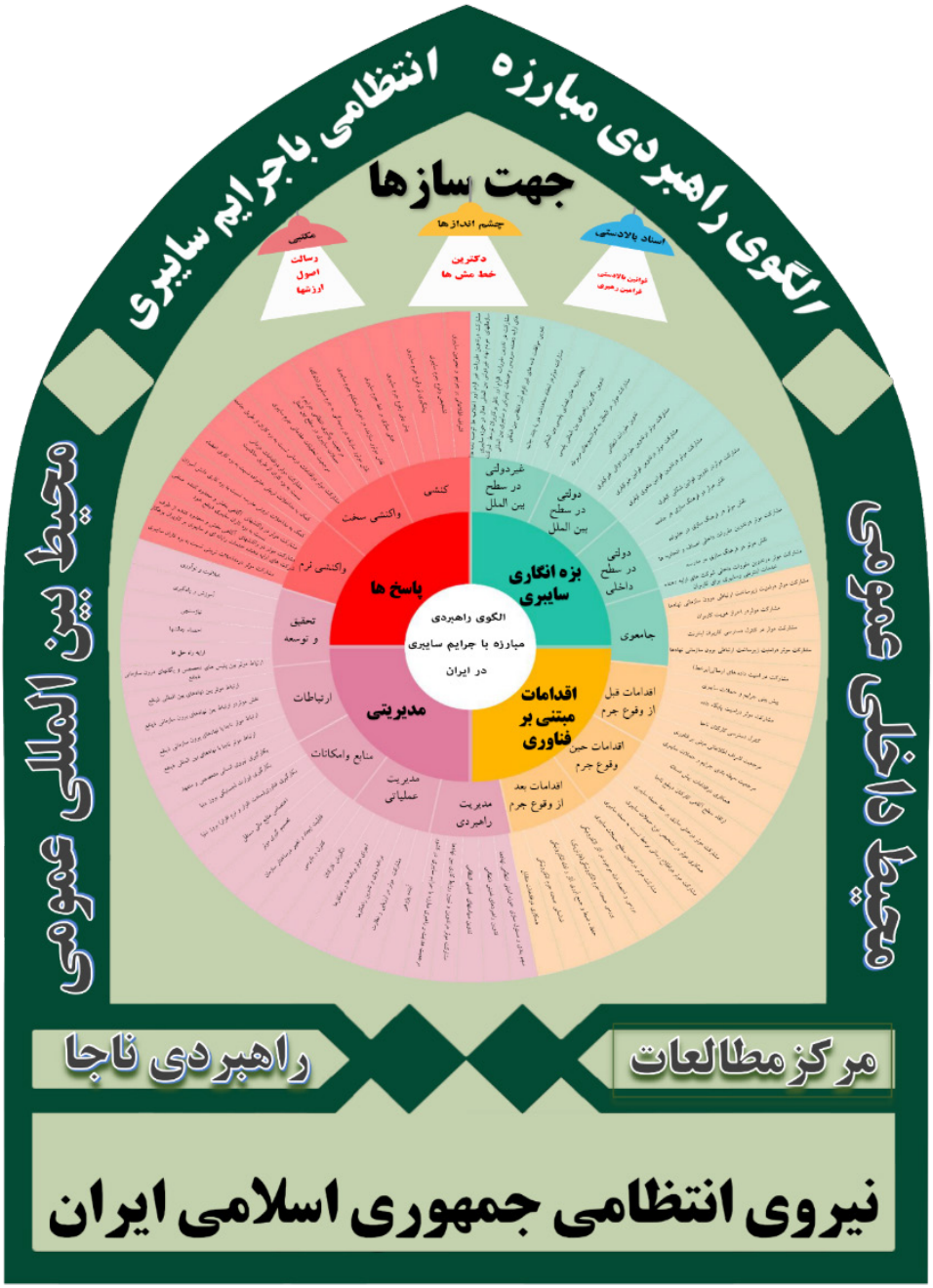
در بررسی میزان اهمیت معرف‌ها مشخص می‌شود که بعد "پاسخ‌ها" با ضریب ۸۱۸/. در رتبه اول و بعد "مدیریتی" با ضریب ٦٩٢/. در رتبه دوم و بعد "اقدامات مبتنی‌بر فناوری" با ضریب ٦٣٩/. در رتبه سوم قرار دارد که شرح آن در جدول شماره ۱۰ ارائه شده‌است.

جدول شماره ۱۰. جدول میزان اهمیت ابعاد

| ردیف | ابعاد | میزان اهمیت |
|---|---|---|
| ۱ | پاسخ‌ها | .۸۱۸ |
| ۲ | مدیریتی | .۶۹۲ |
| ۳ | اقدامات مبتنی‌بر فناوری | .۶۳۹ |
| ۴ | بزه‌انگاری سایبری | .۵۷۹ |

با وجود احصای ابعاد، مؤلفه‌ها و معرف‌های الگوی راهبردی در جهت مبارزه با جرایم سایبری، به نظر می‌رسد که در فضای پیچیده از متغیرهای چند جانبه و ویژگی‌های ناپایدار و تحولات محیطی امروزی، باید به‌دنبال لحاظ نمودن عوامل محیطی(عمومی) و جهت‌سازها در الگوی موصوف بود. این دو بعد خارج از هسته اصلی الگو، به‌مراتب سمت‌وسوی حرکت الگو را شکل می‌دهند. هسته اصلی احصاشده باید به‌گونه‌ای باشد که انعطاف لازم را درخصوص ابعاد بیرونی خود نشان دهد؛ بنابراین، لازم است که در ترسیم نهایی الگوی ارائه‌شده، دو بعد پایدار جهت‌سازها و ناپایدار عوامل محیط عمومی نیز ترسیم گردد.

با توجه به داده‌ها و تحلیل صورت‌گرفته بر روابط بین متغیرها، «الگوی راهبردی مبارزه با جرایم سایبری» به‌صورت شکل شماره ۱ تبیین و ترسیم گردیده‌است.




شکل ۱. الگوی راهبردی مبارزه با جرایم سایبری در ایران

## جمع‌بندی

در پاسخ به سؤال اصلی پژوهش، ضمن شناسایی و بررسی ابعاد، مولفه‌ها و شاخص‌ها، در انتهای این مقوله نیز مدل تحلیلی اولیه الگوی راهبردی مبارزه با جرایم سایبری در ایران طراحی و ارائه گردیده‌است که هر کدام از اجزای آن در طول و عرض، توسط نرم‌افزارهای آماری مورد آزمون قرار گرفته‌است و ارتباط بین آنها نیز تجزیه و تحلیل و در نهایت، تأیید شده‌است.

در پاسخ به اولین سوال فرعی تحقیق، نتایج پژوهش حاضر نشان می‌دهد که اساس الگوی راهبردی مبارزه با جرایم سایبری در ایران با ابعاد "پاسخ‌ها، مدیریتی، اقدامات مبتنی‌بر فناوری و بزه‌انگاری سایبری" طراحی و تدوین می‌شود؛ به‌طوری که عوامل مداخله‌گری همانند جهت‌سازها و عوامل محیطی در سطح داخلی و بین‌المللی برآن تأثیر می‌گذارند.

۱.بُعد "پاسخ‌ها" با سه مؤلفه کنشی، واکنشی سخت و واکنشی نرم، دارای رابطه معنی‌دار با یکدیگر هستند. مؤلفه پاسخ های کنشی شامل اشراف اطلاعاتی بر جرایم و مجرمان سایبری، تشخیص وقوع جرم سایبری، پیشگیری وضعی و اجتماعی از وقوع جرم سایبری، پیش‌بینی وقوع جرم سایبری و خنثی‌سازی برخط جرم سایبری است که در یک زیرمجموعه با هم، دارای رابطه معنی‌دار هستند.

مؤلفه "واکنشی سخت" دارای معرف‌های نقش موثر و سازنده در اجرای احکام جرم سایبری، نقش موثر و سازنده در رسیدگی به جرم سایبری(دادگاه)، مرجعیت پیگیری انتظامی جرایم و حملات سایبری در سطح بین‌الملل و مرجعیت تحقیقات مقدماتی بر جرم سایبری است.

مؤلفه "واکنشی نرم" نیز دارای معرف‌های مشارکت موثر در اقدامات درمانی نسبت‌به بزه‌کاران از طریق جامعه، مشارکت موثر در اقدامات درمانی نسبت‌به بزه‌کاران از طریق حاکمیت، کمک به مداخلات تربیتی خانواده نسبت‌به بزه‌کاری اعضا، کمک به مداخلات تربیتی مدرسه نسبت‌به بزه‌کاری دانش‌آموزان، مشارکت موثر در واکنش‌های آگاهی‌بخش و محدودکننده صنفی(اتحادیه‌ها) نسبت‌به بزه‌کاران سایبری ذی‌نفع خود، مشارکت موثر در واکنش‌های آگاهی‌بخش و محدودکننده صنفی(اتحادیه‌ها) نسبت‌به بزه‌کاران سایبری ذی‌نفع خود، مشارکت موثر در واکنش‌های آگاهی‌بخش و محدودکننده از طرف شرکت‌های ارائه‌دهنده خدمات رایانه‌ای و سایبری بر کاربران بزه‌کار، مشارکت در مداخلات تربیتی مدنی(امر به معروف و نهی از منکر) نسبت‌به بزه‌کاران سایبری و اقدامات انتظامی آگاهی‌بخش و محدودکننده نسبت‌به بزه‌کاران سایبری می‌باشد.

۲." بُعد مدیریتی" دارای پنج مؤلفه مدیریت عملیاتی، منابع و امکانات، ارتباطات، تحقیق و توسعه است.

مؤلفه "مدیریتی راهبردی" دارای معرف‌های سهم‌بندی و مسئول‌سازی حوزه امنیتی انتظامی نهادها، تدوین راهبردهای امنیتی انتظامی، تدوین سیاست‌های امنیتی انتظامی، مشارکت موثر در تدوین و تبیین روابط کاری بین نهادها، مرجعیت هدایت و راهبری مبارزه با جرایم سایبری در کشور، آینده‌پژوهی در روندها و مشارکت موثر در ارزیابی و نظارت کارکرد مطلوب منابع می‌باشد.

مؤلفه "مدیریت عملیاتی" دارای معرف‌های برنامه‌ریزی و تدوین راهکارها، اجرای موثر برنامه‌ها و راهکارها، انگیزش کارکنان، کنترل و بازرسی، قابلیت ایجاد و تغییر در ساختار سازمان و به‌کارگیری روش‌های مبارزه می‌باشد.

مؤلفه "منابع و امکانات" دارای معرف‌های اختصاص منابع مالی مستقل به ناجا مختص مبارزه با جرایم سایبری، به‌کارگیری فناوری(سخت‌افزار و نرم‌افزار) به‌روز، به‌کارگیری ابزارهای لجستیکی به‌روز و به‌کارگیری نیروی انسانی متخصص و متعهد می‌باشد.

مؤلفه "ارتباطات" شامل معرف های ارتباط موثر ناجا با نهادهای بین‌المللی ذی‌نفع، ارتباط موثر ناجا با نهادهای برون‌سازمانی ذی‌نفع، نقش موثر در ارتباط بین نهادهای برون‌سازمانی ذی‌نفع، ارتباط موثر بین نهادهای بین‌المللی ذی‌نفع و ارتباط موثر بین پلیس‌های تخصصی و یگان‌های درون‌سازمانی ذی‌نفع است.

مؤلفه "تحقیق و توسعه" دارای معرف‌های ارائه راه‌حل‌های موثر بر چالش‌ها، احصای چالش‌ها، نیازسنجی، آموزش و یادگیری کارکنان حرفه‌ای و خلاقیت و نوآوری در روش‌های مبارزه با جرایم سایبری می‌باشد.

۳."بُعد اقدامات مبتنی‌بر فناوری" با سه مؤلفه شامل اقدامات قبل از وقوع جرم، اقدامات حین وقوع جرم و اقدامات بعد از وقوع جرم در نظر گرفته شده‌است که معرف‌های هرکدام از مؤلفه‌های این بُعد در ادامه آورده شده‌است:

مؤلفه "اقدامات قبل از وقوع جرم" دارای معرف‌های مشارکت موثر در امنیت زیرساخت ارتباطی درون‌سازمانی نهادها، مشارکت موثر در احراز هویت کاربران، مشارکت موثر در کنترل دسترسی کاربران اینترنت، مشارکت موثر در امنیت زیرساخت ارتباطی برون‌سازمانی نهادها، مشارکت در امنیت داده‌های ارسالی(برخط)، پیش‌بینی جرایم و حملات سایبری، مشارکت

موثر در امنیت پایگاه داده، کنترل دسترسی کارکنان ناجا، مرجعیت اشراف اطلاعاتی مبتنی‌بر فناوری، مرجعیت حیطه‌بندی جرایم و حملات سایبری، همکاری با نهادهای ذی‌نفع در اقدامات پیش‌دستانه و ارتقای سطح آگاهی کارکنان دی‌نفع ناجا است.

مؤلفه "اقدامات حین وقوع جرم سایبری" شامل معرف‌های مشارکت موثر در خنثی‌سازی برخط حمله سایبری، همکاری موثر در تشخیص نوع حملات سایبری، مشارکت موثر در اطلاع‌رسانی برخط نسبت‌به حمله سایبری و مشارکت موثر در تعیین سطح حملات سایبری می‌باشد.

مؤلفه "اقدامات بعد از وقوع جرم سایبری" شامل معرف‌های بررسی و احصای ادله موجود در آثار الکترونیکی، بررسی صحنه جرم الکترونیکی(فارنزیک)، حفظ، ضبط و جمع‌آوری آثار و ادله الکترونیکی، شناسایی صحنه جرم الکترونیکی و همکاری در اقدامات متقابل است.

٤.بُعد "بزه‌انگاری" با چهار مؤلفه اصلی جامعوی، دولتی در سطح بین‌المللی و غیردولتی در سطح بین‌المللی مطرح شده‌است که دارای معرف‌های گسترده‌ای به شرح زیر هستند:

مؤلفه "دولتی در سطح داخلی" شامل معرف‌های مشارکت موثر در تدوین قوانین شکلی کیفری(آئین دادرسی)، مشارکت موثر در تدوین قوانین ماهوی کیفری، مشارکت موثر در تدوین قوانین(غیرکیفری)، مشارکت موثر در تدوین مقررات(آئین‌نامه‌ها و دستورکارهای)، دولتی(غیرکیفری) و مشارکت موثر در تدوین مقررات(آئین‌نامه‌ها و دستورکارهای) انتظامی می‌باشد.

مؤلفه "جامعوی" شامل معرف‌های مشارکت موثر در تدوین مقررات داخلی شرکت‌های ارائه‌دهنده خدمات اینترنتی و سایبری برای کاربران، نقش موثر در فرهنگ‌سازی در مدرسه(تبیین قواعد سبک زندگی در مدرسه)، مشارکت موثر در تدوین مقررات داخلی اصناف و اتحادیه‌ها، نقش موثر در فرهنگ‌سازی در خانواده(تبیین قواعد سبک زندگی در خانواده) و نقش موثر فرهنگ‌سازی در جامعه(تبیین قواعد سبک زندگی در جامعه) می‌باشد.

مؤلفه "دولتی در سطح بین‌المللی" شامل معرف‌های مشارکت موثر در الحاق به کنوانسیون‌های مربوطه، تدوین دکترین راهبردی بین‌المللی پلیسی، ایجاد رویه‌های قضایی پلیسی بین‌المللی، مشارکت موثر در انعقاد معاهدات دو یا چند جانبه و تدوین موافقت‌نامه‌های غیر الزام‌آور انتظامی بین‌المللی(اعلامیه‌ها، تفاهم‌نامه‌ها، توصیه‌نامه‌ها) می‌باشد.

و در نهایت، مؤلفه "غیردولتی در سطح بین‌المللی" شامل معرف‌های مشارکت در تدوین مقررات الزام‌آور ناظر بر کاربران توسط شرکت‌های ارائه‌دهنده سرویس و خدمات اینترنتی و سایبری بین‌المللی و نیز مشارکت در تدوین مقررات غیر الزام‌آور(اعلامیه‌ها، توصیه‌نامه‌ها) سازمان‌های مردم‌نهاد غیردولتی بین‌المللی فعال در حوزه سایبری می‌باشد.

دو کلان عامل مداخله‌گر ـ یعنی "جهت‌سازها" و "عوامل محیطی داخلی و بین‌المللی" ـ نیز به‌صورت مستمر بر هسته اصلی الگوی طراحی‌شده تأثیر می‌گذارند. مفهوم جهت‌ساز دارای سه بعد مکتبی، چشم‌اندازها و اسناد بالادستی است و مفهوم عوامل محیط در سطح داخلی و بین‌المللی دارای مولفه‌هایی اعم از سیاسی، اقتصادی، فرهنگی، اجتماعی، حقوقی، فناورانه، زیست محیط و نظامی است.

## نتیجه‌گیری و پیشنهادها

امروزه، فضای سایبری در تمامی ابعاد زندگی بشری سایه افکنده است. روابط انسان‌ها در این بستر، روز به روز رشد و نمو دارد. حجم و وسعت این روابط در سطح جهانی تعریف می‌گردد، به‌طوری که در حال حاضر، کشورها از طریق فضای سایبری در یک قالب مشترک پدیدار شده و در یک جامعه مشترک جهانی شکل یافته‌اند. امنیت مهم‌ترین رکن پایداری یک جامعه است و مبارزه با جرایم حوزه سایبری نیز یکی از ارکان مهم امنیت سایبری محسوب می‌گردد. از آنجا که فضای سایبری از بستر علمی و فنی شکل یافته‌است، بنابراین، نیازمند اقدامات علمی و فنی در امنیت‌سازی این فضا است. تحقیق حاضر، گامی کوتاه اما مهم، اثر گذار و لازم در جهت برداشتن گام دوم ـ یعنی همان ترسیم اقدامات عملیاتی در راستای مبارزه با جرایم سایبری ـ می‌باشد که نیاز است از طریق روش‌ها و مدل‌های اجرایی و از طریق تدوین و تبیین مدل‌ها و برنامه‌های اجرایی در جهت عملیاتی نمودن آن گام برداشت. در این راستا، سیاست جنایی انتظامی جرایم سایبری برای اولین‌بار در سطح دنیا ترسیم شده‌است. این الگو نشان می‌دهد که نیروهای انتظامی جمهوری اسلامی ایران باید دارای چه سیاست‌های راهبردی در جهت مبارزه با جرایم سایبری باشند اما چگونگی اجرای این سیاست‌ها باید در قالب موضوعات راهبردی از طریق مدل‌سازی اجرایی در بدنه ساختار انتظامی کشور تبیین و اجرا گردد.

باتوجه به نتایج به‌دست‌آمده و یافته‌های پژوهش حاضر بر اساس ابعاد الگوی راهبردی مبارزه با جرایم سایبری در ایران، پیشنهادهای راهبردی و کاربردی زیر حائز اهمیت بوده و به این شرح پیشنهاد می‌گردد:

۱-تقویت حوزه فضای سایبری ناجا و ترسیم ساختارهای غنی و قوی به‌منظور مدیریت یکپارچه فرایندهای الگو در حوزه امنیتی و انتظامی؛

۲-بازنگری ساختار، سازمان مبارزه با جرایم سایبری در کشور و بازمهندسی آن؛

۳- مدل‌سازی اجرایی هر معرف در قالب برنامه پنج‌ساله ششم؛

۴- تدوین دکترین، راهبردها، سیاست‌ها، تنظیم و تصویب قوانین، مقررات، دستورکارهای کارآمد در راستای چابکی و افزایش توان پیش‌دستانه.

## منابع فارسی

- آجرلویی، محمود(۱۳۹۱)، "نقش رسانه‌های گروهی در پیشگیری از جرایم و مطالعات پیشگیری از جرم"، شماره ۲۲
- آذرخش، سمیه؛ آذرخش، سپیده(۱۳۹۲)، شبکه‌های اجتماعی در محیط وب۲، تهران، نشر آتی
- اخوان، پیمان؛ باقری، پیمان(۱۳۸۹)، فناوری اطلاعات در مدیریت دانش، تهران، نشر کیان رایانه سبز
- الوانی، سید مهدی(۱۳۸۵)، مدیریت عمومی، تهران، نشر نی
- انصاری، محمد مهدی(۱۳۹۰)، جنگ واقعی در فضای مجازی، تهران، دفتر مطالعات و برنامه‌ریزی رسانه‌ها
- اولریش زیبر(۱۳۸۲)، جرایم رایانه‌ای، ترجمه محمد علی نوری، تهران، انتشارات گنج دانش
- باستانی و برومند(۱۳۸۸)، جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، تهران، بهنامی
- بای، حسینعلی؛ پورقهرمانی، بابک(۱۳۸۸)، بررسی فقهی حقوقی جرایم رایانه‌ای، تهران، پژوهشگاه علوم و فرهنگ اسلامی
- بای، وحیدرضا(۱۳۹۶)، ظرفیت‌های موجود در شبکه‌های اجتماعی مجازی، تهران، انتشارات موجک
- پاکزاد، بتول(۱۳۸۸)، "تروریسم سایبری"، رساله برای دریافت درجه دکتری، تهران، دانشکده حقوق دانشگاه شهید بهشتی
- پلومان، ادوارد(۱۳۸۰)، حقوق بین‌الملل ارتباطات و اطلاعات، ترجمه بهمن آقایی، تهران، کتابخانه گنج و دانش
- پورقهرمانی، بابک(۱۳۹۵)، سیاست جنایی ایران در قبال جرایم رایانه‌ای، تهران، شهر دانش
- جلالی فراهانی، امیر حسین(۱۳۹۵)، کنوانسیون جرایم سایبر و پروتکل الحاقی آن، تهران، انتشارات خرسندی
- حافظ نیا، محمدرضا(۱۳۹۱)، جغرافیای سیاسی فضای مجازی،تهران، انتشارات سمت
- حسینی، سید محمد(۱۳۹۴)، سیاست جنایی در اسلام و در جمهوری اسلامی ایران، تهران، انتشارات سمت
- خرم آبادی، عبدالصمد(۱۳۸٤)، "جرایم فناوری اطلاعات"، رساله برای دریافت درجه دکتری، دانشکده حقوق و علوم سیاسی دانشگاه تهران
- دباراتی هاردی، کی جشینکار(۱۳۹۳)، جرم رایانه‌ای و بزه‌دیدگی زنان، ترجمه مهرداد رایجیان اصلی و دیگران، تهران، انتشارات مجد

- دستور، علی؛ جمشیدی نسب، عین اله(۱۳۹۳)، پیشگیری از جرایم سایبری با رویکرد انتظامی، اراک، نشر نویسنده
- زرگر، علیرضا؛ میرزا محمدی، زیبا(۱۳۸۵)، امنیت و تهدید در جامعه اطلاعاتی، تهران، انتشارات قدیم
- زندی، محمدرضا(۱۳۹٤)، تحقیقات مقدماتی در جرایم سایبری، تهران، انتشارات جنگل
- سهلانی، حسین(۱۳۹۷)، آشنایی با تهدیدات فضای سایبری، تهران، انتشارات دانشگاه علوم انتظامی
- شیرزاد، کامران(۱۳۸۸)، جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل، تهران، شرکت نشر بهینه فراگیر
- صادقی، میرمحمد(۱۳۸۹)، جرایم علیه اموال و مالکیت، تهران، نشر میزان
- صبح خیز، رضا(۱۳۹۸)، جرایم سایبری در نظام حقوقی ایران و جهان، تهران، انتشارات دانشگاه علوم انتظامی
- کامر، داگلاس، ای.(۱۳۸۸)، مهندس فناوری اطلاعات، ترجمه سید حجت‌اله جلیلی، تهران، انتشارات ناقوس
- کلاه چیان، محمود(۱۳۹۱)، اثرات فناوری‌های نوین اطلاعاتی و ارتباطی بر افکار عمومی، مجموعه کتاب مجموعه نشست‌های همایش افکار عمومی و امنیت اجتماعی، تهران، ناجا
- کلاه‌چیان، محمود(۱۳۹۰)، تأثیر شبکه‌های مجازی بر افکار عمومی و امنیت اجتماعی، مجموعه مقالات نخستین همایش افکار عمومی و امنیت اجتماعی، تهران، ناجا
- گرکی، مارکو(۱۳۹۰)، جرایم سایبری راهنمایی برای کشورهای درحال‌توسعه، ترجمه مرتضی اکبری، تهران، انتشارات پلیس فتا
- نیری، هومن(۱۳۸۹)، "نقش شبکه‌های اجتماعی اینترنتی و مشارکت سیاسی"، پایان نامه برای دریافت درجه کارشناسی‌ارشد، تهران، دانشکده حقوق و علوم سیاسی دانشگاه تهران
- _____ (۱۳۸۳)، بررسی ابعاد حقوقی فناوری اطلاعات، تهران، مرکز مطالعات راهبردی و توسعه قضایی