تدوین راهبردهای مقابله با جرائم علیه امنیت ملی در فضای مجازی

نویسندگان: مهدی محسنی[1]،نجمه سادات عزتی[2]

چکیده:

پژوهش حاضر به تدوین راهبرد های جنایی جمهوری اسلامی ایران در عرصه مقابله با جرایم علیه امنیت ملی در فضای مجازی می‌پردازد. تامین امنیت ملی همواره جز اولویت حاکمیت‌ها در سراسر جهان بوده است. همچنین فضای سایبری به عنوان یک فناوری نوظهور و رو به پیشرفت با سرعت بالا چالش‌های زیادی را در راستای حفظ امنیت ملی ایجاد کرده است. در حال حاضر جرایم و تهدیدهای سایبری در هزاره سوم میلادی، آینده اجرای قوانین را در بسیاری از کشورهای جهان به مخاطره انداخته است. تدوین راهبرد یکی از اساسی‌ترین مؤلفه‌های مدیریت اصولی مجموعه هدف است. از جمله الگوهای مطرح جهت تدوین راهبرد، استفاده از نقاط قوت، ضعف، تهدیدها و فرصت‌ها برای مجموعه مورد مطالعه است که در نتیجه چهار مجموعه از تحلیل با عناوین تهاجمی، رقابتی، محافظه کارانه، تدافعی را به دنبال دارد. با تدوین مجموعه راهبرد در حوزه جرایم علیه امنیت ملی در بستر فضای مجازی، امکان پیشگیری از ارتکاب جرایم مذکور فراهم می‌شود؛ و به تبع آن آمار ارتکاب این جرایم به طور مشهود کاهش می‌یابد. همچنین با استفاده از سند راهبردی امکان رصد آینده و پیش بینی وقایع احتمالی و تحرکات برنامه‌ریزی شده عوامل محرک خارجی نیز مهیا هست؛ تا بتوان با این آینده نگری مدیریت بحران‌های محتمل را بهتر به سرانجام رساند. از جمله راهبرد های حاصل شده از تحلیل تهاجمی می توان به طراحی سیستم سه‌ضلعی نظارت، فرهنگ‌سازی و بازدارندگی اشاره نمود.

واژگان کلیدی: جرم، فضای مجازی، جرائم امنیتی، جرائم سایبری، امنیت ملی.

[1] دانشجوی دکتری دانشگاه علوم اسلامی رضوی
[2] دانشجوی کارشناسی ارشد دانشگاه علوم اسلامی رضوی

مقدمه:

امروزه بستر فضای مجازی به بخش تفکیک‌ناپذیر زندگی انسان‌ها تبدیل‌شده است و با توجه به‌سرعت رشد بالای آن در تمامی عرصه‌های زیست انسان تأثیرگذار شده است. فضای مجازی امکان آسیب‌رسانی به دیگران و آسیب دیدن را توأمان دارد و با توجه به گستره تأثیر آن‌که تمامی اقشار جامعه را در برمی‌گیرند، وجود امنیت فضای مجازی به شکل قابل‌توجهی به موضوع حیاتی برای تمامی کشورهای جهان تبدیل‌شده است. چراکه شرط لازم در ایجاد تهدید امنیتی در فضای مجازی دسترسی گسترده و استفاده از شبکه‌های اطلاعاتی موجود در این فضاست و همچنین شرط کافی نیز اینترنتی شدن تمامی زیرساخت‌ها و مجموعه دستگاه‌های اقتصادی و اجتماعی و سیاسی جوامع است. با همین لحاظ ماهیت شناسی فضای مجازی و تشخیص و شناخت بسترهای تأثیر آن در موارد امنیت ملی بی‌تردید مورد اهمیت قرار دارد که تبدیل‌شدن به کارگردانان توانمند در این فضا برای صیانت از جامعه جزء مهم‌ترین مسائل به شمار می‌رود. در سال ۱۳۹۱ مقام معظم رهبری فرمان تشکیل شورای عالی فضای مجازی کشور را صادر فرمودند که نشان‌دهنده توجه وافر معظم الله به تأثیر شگرف این فضاست. کشورهای توسعه‌یافته برای مبارزه با این جرائم پیش‌قدم شده قوانین تدوین کرده‌اند؛ که بسیاری از آن‌ها از اسناد بین‌المللی سرچشمه می‌گیرند. این اسناد راهکارهای مناسبی پیشروی قانون‌گذاران کشورها قرار داده‌اند.(هلیلی، ۱٤۰۰، ص۱۰۲) تهدیدات موجود متنوعی در بخش‌های مختلفی است تهدیدات امنیتی و اطلاعاتی و یا فرهنگی و اجتماعی و یا روانی و روان‌شناختی و یا اقتصادی که قابلیت پرداختن به آن وجود دارد اما آنچه در این مسئله مهم در راستای اهداف کمک‌کننده خواهد بود تدوین مجموعه راهبرد در جهت خنثی نمودن تهدیدهای متوجه برای امنیت ملی در فضای مجازی است و ایجاد فرصت‌هایی در راستای رشد و تعالی هر چه بیشتر مردم و جامعه است همچنین شناسایی نقاط ضعف و یا نقاط نیازمند به تقویت بیشتر در خصوص ایجاد امنیت در حوزه جرائم در بستر فضای مجازی است و همچنین شناخت و استفاده درست از نقاط قوت موجود در جامعه و نهادهای مربوط به آن درزمینهٔ رفع تهدیدهای احتمالی و کم کردن نقاط ضعف است. لذا تدوین راهبردهای جهت پیشگیری از تهدیدات مختلف موجود در این فضا را امری ضروری و غیرقابل‌اجتناب کرده است و بی‌توجهی به آن هزینه‌های جبران‌ناپذیری را به جامعه تحمیل خواهد کرد. قانون‌گذار در ماده ۱۱ قانون جرائم رایانه‌ای مصوب ۱۳۸۸ به جرم انگاری تهدیدات سایبری علیه سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی بکار می‌رود مانند خدمات درمانی، آب، برق، گاز، مخابرات، حمل‌ونقل و بانکداری درصورتی‌که تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی به‌قصد به خطر انداختن آسایش و امنیت عمومی باشد، پرداخته است. نکته‌ای که در اینجا وجود دارد آن است که قانون‌گذار فقط در یک ماده به بیان تهدیدات سایبری علیه زیرساخت‌های حساس پرداخته اما جوانب امر به‌طور دقیق و مفصل در قانون مشخص نشده و اینکه چه راهبردهای پیشگیرانه‌ای باید اتخاذ شود تا این‌گونه زیرساخت‌ها از تهدیدات ایمن بمانند تعیین نشده است. جرائم بر ضد امنیت ملی در فضای سایبر را می‌توان به دودسته جرائم سایبری ناب (محض) بر ضد امنیت ملی و جرائم بر ضد امنیت ملی در بستر فضای سایبر (ارتکاب جرائم امنیتی سنتی در بستر فضای مجازی) تقسیم کرد. در مورد جرائم سایبری ناب بر ضد امنیت ملی می‌توان از دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تروریسم سایبری، ممانعت از دستیابی، تخریب و اخلال داده‌ها و سامانه‌های رایانه‌ای و مخابراتی نام برد. همچنین جرائم بر ضد امنیت ملی در بستر فضای سایبر شامل تشکیل

گروه مجازی بیش از دو نفر که هدف آن برهم زدن امنیت کشور باشد (موضوع ماده ٤٩٨ قانون مجازات اسلامی ١٣٧٥) و سایر جرائم امنیتی سنتی یادشده در قوانین در بستر فضای مجازی است. آنچه باعث ایجاد تفاوت عمده بین پژوهش‌های موجود در این زمینه و پژوهش حاضر است اهتمام ویژه در به‌کارگیری و استفاده از راهکارهای مدیریتی در کنار مباحث حقوقی خواهد بود که نتیجه آن می‌شود ترکیب هدفمند الگوی ماتریس سوات در جهت تدوین راهبرد در علم مدیریت و مباحث حقوق جزا و جرم شناسی است.

١.جرائم فضای مجازی

با توجه به توصیه‌نامه اروپا همان تعریف اصلی OECD است که عبارت از سوءاستفاده از رایانه است و ناظر به هر رفتار غیرقانونی، غیراخلاقی و یا غیرمجاز مربوط به پردازش فنّاوری رایانه‌ای و انتقال داده‌ها است. سوءاستفاده از رایانه یعنی هر واقعه‌ای که توأم با فنّاوری رایانه انجام می‌شود و به‌واسطه آن بزه دیده متحمل خساراتی شود و مرتکب به‌عمد، مالی یا منفعتی را کسب کند، یا بتواند کسب کند(زندی،١٣٩٨، ص١٨) این جرائم به دلیل ماهیت تکنولوژیک، مختصات و آثار ویژه‌ای دارد که در تدوین راهبردها دارای اهمیت بسزایی بوده و قابلیت بهره‌برداری و تدوین خواهد داشت.

کلمه سایبر ازنظر ریشه به مطالعه مکانیسم‌های استفاده‌شده جهت کنترل اعم از انسان یا ماشین گفته می‌شود، اصطلاح سایبر یا دنیای مجازی آنلاین نخستین بار توسط ویلیام گیبسون مورداستفاده قرار گرفت، در تفاوت محیط سایبر در مقایسه با سایر محیط‌ها چند ویژگی مهم و منحصربه‌فرد نهفته است که می‌توان از آن‌ها یادکرده:الف)نامحدود بودن فضای سایبر. ب)ناملموس بودن محیط سایبر که این ویژگی فضای سایبر را خطرسازتر از محیط حقیقی می‌نمایاند. پ)توسعه و تغییرپذیری. ت)پیچیدگی و تخصصی بودن. ث)دسترسی آسان و سریع. ج)استفاده گسترده از فضای سایبر. که این ویژگی‌ها فضای مجازی را در دنیای کنونی بیشتر حساس و پراهمیت می‌نماید.(وروانی و مدنی پور، ١٣٩٩، ص٣) از محیط سایبر به محیط فن‌آوری اطلاعات (IT) یا محیط اطلاعات و ارتباطات نیز یادشده است ازاین‌رو مشاهده می‌شود که برای نمونه به جرم‌های محیط سایبر، جرم‌های علیه فن‌آوری اطلاعات نیز گفته می‌شود. (زندی، ١٣٩٣، ص ٢٠)

١-١.ویژگی‌های فضای مجازی ازنظر تسهیل در ارتکاب جرم: الف)قابلیت گزینشی بودن اطلاعات: فضای مجازی یک فضای خاموش است، با این توضیح که در این فضا در ابتدا اطلاعات غالباً توسط خود مشترکین که ارائه‌کننده اطلاعات هستند ایجاد می‌شود و تا کاربران در ایجاد اطلاعات فعال نباشند اطلاعات قابل‌دسترس نخواهند بود. ثانیاً خود اطلاعات در صورتی به دست مخاطب می‌رسد که توسط کاربر درخواست گردد. درواقع با جستجو و کنکاش در صفحات هزارتو و درهم‌تنیده اینترنتی است که کاربر به درخواست خود اطلاعات را در دالان‌های اینترنتی می‌یابد. ب)عدم توازن بین قابلیت کنترل فضای مجازی به نسبت رشد زیرساختی و فنی آن (فضلی، ١٣٩١، ص٦٨) به اعتقاد برخی اندیشمندان این حوزه، محیط فضای مجازی از همان پیدایش آن علیرغم نظم فنی اعجاب‌آورش، از منظر رفتار کاربران محیطی مبتنی بر آنارشیسم و هرج‌ومرج بوده است. پ)امکان ردیابی و شناسایی کاربران خاص‌و نفوذ غیرمجاز به حریم اشخاص. ت) تخصصی و علمی بودن.

۲.جرائم علیه امنیت ملی

با توجه به اولویت حاکمیت ها برای حفظ قدرت و حاکمیت خود و مصونیت از خطراتی که جرائم علیه امنیت می‌توانند برای حاکمیت و استقلال آن‌ها ایجاد نمایند، از قدیم‌الایام مقررات سختی راجع به جرائم علیه امنیت وجود داشته است. در حال حاضر ازجمله جرائم علیه امنیت که در قوانین آمده است، جرم محاربه به‌عنوان مصداق بارز جرائم علیه امنیت در حقوق ایران و فقه اسلامی فصل هشتم از قانون مجازات اسلامی مصوب ۱۳۹۲، بغی و افساد فی‌الارض فصل نهم از قانون مجازات اسلامی مصوب ۱۳۹۲، جرائم علیه امنیت مذکور در فصل اول از قانون تعزیرات مصوب ۱۳۷۵ و موارد مشابه آن در قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲، اهانت به مقدسات مذهبی و سوءقصد به جان مقامات سیاسی مذکور در فصل دوم و سوم از قانون تعزیرات مصوب ۱۳۷۵، تخریب به‌قصد مقابله با نظام، تبانی برای ارتکاب جرائم علیه امنیت، اشاعه اکاذیب، تظاهر قدرت‌نمایی هیاهو و جنجال، اقدام برای جدا کردن قسمتی از قلمرو حاکمیت ایران (ماده ۲۰ قانون مجازات جرائم نیروهای مسلح) است.

در بیان تفاوت بین جرایم علیه امنیت و جرایم علیه آسایش می توان گفت جرائمی مانند جاسوسی، شورش یا تحریک مردم به شورش، جمع‌آوری اطلاعات محرمانه و نظایر آن‌ها که به‌طور مستقیم با حاکمیت ملی و اساس و پایه‌های یک نظام و حکومت برخورد دارند، جرائم علیه امنیت محسوب می‌شوند و جرائمی مانند جعل و قلب سکه، از باب این‌که اعتماد عمومی را نسبت به صحت اسناد، نوشته‌های، اوراق بهادار، اسکناس، سکه و نظایر آن‌ها سلب کرده، جرائم علیه آسایش عمومی محسوب می‌شوند.(میرمحمدصادقی، ۱۳۹۳، ص۱۶)

۲-۱. اقسام جرائم علیه امنیت در فضای مجازی: دسته‌بندی‌های مختلفی پیشنهادشده که مشهورترین آن، بر اساس نقش رایانه صورت گرفته چون این رایانه است که مفهوم و مصادیق جرم را در فضای مجازی دگرگون ساخته، دسته‌بندی نیز با محوریت نقش آن‌ها ارائه‌شده است. در بیشتر نوشته‌ها، بزه‌های رایانه‌ای را بزه‌هایی دانسته‌اند که رایانه در تحقق آن‌ها نقش منفعل و پذیرا دارد و موضوع رفتار مجرمانه قرار می‌گیرد، و یا وسیله ارتکاب جرایم را فراهم می آورد و در وسیله جرم نقشی فعال دارد و جرم با کمک آن ارتکاب می‌یابد.(عالی پور، ۱۳۸۷، ص۱۴۵)

۲-۱-۱.جرائمی که فضای مجازی در آن مورد هدف قرار می‌گیرد و موضوع رفتار مجرمانه است: اغلب این جرائم ماهیت سنتی نداشته و فقط از طریق فضای مجازی تحقق پیدا می‌کنند ازاین‌رو به این قسم از جرائم مجازی محض نیز گفته می‌شود چراکه با تشکیل فضای مجازی ایجادشده‌اند؛ که مواردی به‌عنوان مصادیق اصلی آن گفته می‌شود.

الف) تروریسم بزرگ‌ترین خطر برای صلح و امنیت ملی و بین‌المللی شمرده می‌شود. این پدیده به سبب پیوند با فناوری‌های نوین به یک گرفتاری راهبردی تبدیل‌شده و توانسته است گروه‌هایی کوچک اما با ساختارهای پیچیده را به بازیگران برجسته در پهنه بین‌المللی تبدیل کنند. تروریسم سایبری که درواقع نقطه تلاقی تروریسم با فضای رایانه‌ای است، عبارت است از فعالیت‌های اخلالگرانه از پیش برنامه‌ریزی‌شده در فضای مجازی به‌منظور پیشبرد اهداف اجتماعی، ایدئولوژیک، مذهبی، سیاسی و غیره یا ارعاب افراد در پیشبرد این اهداف.(محسنی، ۱۳۹۰، ص۲۰۰) معمولاً یک حمله سایبری به‌گونه‌ای اجرا می‌شود که خسارات حاصله به حداکثر رسیده و موج رسانه‌ای گسترده‌ای در جامعه تولید کند، مانند حمله به تأسیسات دولتی یا به زیرساخت‌های حساس و آسیب‌پذیر جامعه.

ب) جاسوسی سایبری از غالب‌ترین اقسام جرم رایانه‌ای است. اهمیت این جرم به‌ویژه از حیث مرتکب و خطرها برای دولت متضرر ازآن‌جهت است که در مراکز رایانه‌ای بیشتر سازمان‌ها و حتی شرکت‌ها اطلاعات ارزشمند ذخیره می‌شود.(حسن بیگی، ۱۳۸۹، ص۲۱۱) در این جرم داده‌های رایانه‌ای به‌منزله موضوع جرم جز رکن مادی است. به عبارتی، در جاسوسی رایانه‌ای داده‌ها و اطلاعات یا به عبارتی موضوع جرم در مرحله مقدماتی انجام جرم دارای پایه و قالب مادی نیست که قابل‌لمس باشد و دارای وجود خارجی نیست و صرفاً در فضای سایبر وجود دارند؛ بدون اینکه به‌صورت خارجی مثل سی دی درآمده باشد.(رهامی و پرویزی، ۱۳۹۲، ص۱۸۰) برای جمع‌آوری اطلاعات محرمانه در ارتکاب جرم جاسوسی سایبری از رایانه‌ها و سامانه‌های مربوط به آن استفاده می‌کنند.

۲-۱-۲.جرائم علیه امنیت ملی با استفاده از فضای مجازی: معیار وسیله محور در تقسیم جرائم سایبری آن چیزی را موردبررسی قرار می‌دهد که در یارانه و فضای سایبر به‌عنوان ابزاری برای ارتکاب جرم در نظر گرفته می‌شود و نه اینکه خود هدف باشد درواقع در این دسته اغلب جرائم ماهیت آن‌ها سنتی بود و فقط ابزار ارتکاب آن مدرنیته شده ازاین‌رو به این قسم جرائم علیه امنیت ملی در بستر فضای سایبر گفته می‌شود.

۳.سیاست‌های جمهوری اسلامی ایران در عرصه پیشگیری و مقابله با جرائم فضای مجازی

تقریباً از اواخر دهه ۷۰ و اوایل ده ۸۰ تدابیر مختلفی در رده‌های حاکمیتی جمهوری اسلامی ایران در تبیین ضرورت مقابله با ناهنجاری‌های سایبری اتخاذشده. ازجمله موارد مهم آن ابلاغیه ۷ ماده‌ای مقام معظم رهبری در خصوص شبکه‌های اطلاع‌رسانی در بستر فضای مجازی در سال ۱۳۸۰ است که می‌توان از آن به‌عنوان منشور سیاست جنایی ملی جرائم رایانه‌ای یادکرد. این ابلاغیه، علاوه بر جنبه‌های کیفری شامل مفاهیم پیشگیرانه بااهمیتی است که توجه و پایبندی به آن می‌تواند مشکلات این حوزه را تا حدود قابل‌توجهی برطرف سازد. پیش‌نویس جرائم رایانه‌ای در شورای عالی توسعه قضائی بعد از گذشت ۱۵ سال از زمان تصویب آن در هیئت‌وزیران در خردادماه ۱۳۸۸ به تصویب مجلس شورای اسلامی و مورد تائید شورای نگهبان قرار گرفت (زیوری، ۱۳۹۱، ص۷۹)

۳-۱.رویکرد تقنینی در جرائم فضای مجازی: روند تصویب و تدوین قانون جرائم رایانه‌ای مصوب سال ۱۳۸۸ را می‌توان به عنوان اساسی ترین قدم قانون‌گذار در جهت سیاست‌های تقنینی پیشگیرانه از جرائم فضای مجازی برشمرد.(وطنی، ۱۳۹۵، ص۱۲)از جمله سازمان‌ها، مجموعه ها و نهادهایی که رویکرد های تقنینی جهت ایجاد سازوکار پیشگیری از جرائم فضای مجازی را دارند می شود به موارد ذیل اشاره کرد.

۳-۱-۱.شورای عالی فضای مجازی که به فرمان مقام معظم رهبری در ۷ اسفند ماه سال ۱۳۹۰ شکل گرفت و موظف است تا به‌نحو جامع و روزآمد بر محیط درونی و بیرونی اینترنت نظارت و اشراف پیدا کند و امنیت را در این فضا تأمین نماید.

۳-۱-۲.قرارگاه پدافند سایبری کشور که در حقیقت از لحاظ ساختاری زیر نظر مجموعه سازمان پدافند غیرعامل است که خود این سازمان یکی از زیرشاخه‌های مربوط به نیروهای مسلح جمهوری اسلامی ایران است این قرارگاه از آبان ماه سال ۱۳۸۹ آغاز به کار کرده است. این پدافند از چند مجموعه و زیرشاخه‌های استانی و مناطق ویژه تشکل می شود. با این حساب که اکثر وظایف و مسولیت این قرارگاه در خصوص با پیش‌بینی، آسیب‌شناسی، تحلیل و بررسی سامانه های زیرساختی و اطلاع‌رسانی عمومی است، اما با این حال بعضی از وظایف آن را می‌شود زیرمجموعه ای از موارد پیشگیری در حوزه فضای مجازی برشمرد.

۳-۱-۳.سند تبیین الزامات شبکه ملی اطلاعات مورخه ۱۳۹۵/۰۹/۲۰، در این سند تعریف و الزامات مصوب شبکه در شش محور:زیرساخت ارتباطی فضای مجازی کشور، استقلال، مدیریت، سالم‌سازی و امنیت، خدمات و تعرفه و مدل اقتصادی شبکه ملی اطلاعات تبیین و در چهارچوب قواعد کلی در جهت حاکمیت بر طراحی شبکه آورده شده است.

۳-۲. رویکرد قضائی در جرائم فضای مجازی: از جمله نهادهایی‌که با رویکرد قضایی در عرصه پیشگیری و مقابله با جرائم در حوزه فضای مجازی در حال فعالیت هستند.

۳-۲-۱.مرکز مدیریت امداد و هماهنگی عملیات رخداد با عنوان اختصاری ماهر است اکثر فعالیت این مرکز برای پیشگیری جهت حفاظت از اطلاعات مربوط به اشخاص است فعالیت میکند که در واقع یک فعالیت به نحو محدود است.

۳-۲-۲.نهاد آپا از سال ۱۳۸٦ در این حوزه فعالیت خود را شروع کرده است. و در تلاش بوده است که با ساخت سیستم جهت مقابله با حملات سایبری گام بردارد تا بتواند با استفاده از زیرساخت های فناورانه متناسب امنیت اطلاعات را تامین کند.(وطنی، ۱۳۹۵، ص۲۰).

۳-۲-۳.در سال ۱۳٦۳ شورای عالی قضایی وقت بر اساس آیین‌نامه خاصی مرکز مطالعات حقوقی و قضایی دادگستری را تأسیس کرد. بر اساس بند ۷ این آیین‌نامه «پژوهش درباره اقدامات مناسب برای پیشگیری از وقوع جرم» به‌منزله یکی از وظایف آن بیان شد.(توکلی، ۱۳۹۲، ص٦۲)

۳-۲-٤.معاونت اجتماعی و پیشگیری از وقوع جرم قوه قضاییه در راستای به فعلیت رساندن بند پنجم از اصل ۱٥٦ قانون اساسی معاونت در قوه قضائیه تشکیل شد و در سال ۱۳۸۳ با تغییر توسط رئیس قوه قضائیه وقت که در چارت سازمانی صورت گرفت این معاونت حذف گردید. (بیات و همکاران، ۱۳۸۷، ص۱۲٤) ث-اساسنامه شورای عالی توسعه قضائی که طراحی مدل های جهت پیشگیری از وقوع جرم بر اساس آموزه های شرع مقدس اسلام و همچنین انجام مطالعات تطبیقی و در نهایت ارائه راه حل های اجرائی بر اساس بند ز در ماده ۱۱۲ اساسنامه مذکور از رسالت های این شورا است. (منصورآبادی، ۱۳۸۷، ص۲٥)

۳-۳.رویکرد عملیاتی کردن پیشگیری از جرائم فضای مجازی: در سیاست های جنایی دولت ها در سطوح گستره هم خودشان سیاست گذاری میکنند و هم اجرا کننده این سیاست گذاری هستند و هم وظیفه ضمانت اجرای آن را بر دوش می کشد.(نوید کیا، ۱۳۹۹، ص۳٤) در فضای بین الملل تقریبا هیچ مجموعه ای زمام دار حاکمیت و کنترل جرایم در فضای مجازی را بر عهده

ندارد. چون شبکه اینترنت یک محیط در عرض است و دارای سلسه مراتب طولی نیست و این ساختار این گونه است که هر کاربر سهم مشخصی در کنار سایر کاربران دارد. پس نظارت هم از لحاظ فناورانه و هم از لحاظ بروکراسی دچار مشکل است. اما دولت، وظیفه دارد که زمینه را فراهم آورند تا همه ی نهادهای دولتی و مدنی، ازجمله بخش خصوصی، نقش خود را در پیشگیری از جرم به درستی ایفا کنند.(جوان جعفری و سیدزاده ثانی، ۱۳۹۱، ص۸۱)

۳-٤. پیشگیری در فرآیند ارتکاب جرم: ابتدا از شناخت قصد وانگیزه مجرمانه، تشکیل می شود. این مسئله به ما کمک میکند تا یک مرحله قبل از ارتکاب، یعنی قصد مجرم را مخدوش نماییم. در حوزه فضای مجازی بستر های حفاظتی و امنیتی پیشگیرانه موجود به نحوی قرار دارند که جهت جلوگیری از شروع اقدامات جرم و ارتکاب آن تدابیری اندیشیده است. قدم بعدی در فرایند ارتکاب جرم توسط مجرم تهیه مقدمات ارتکاب جرم است که مجرم احتمالی مقدماتی که مورد نظر دارد یا سخت‌افزاری است و یا نرم‌افزاری پس در این حالت بهره‌گیری از تصمیمات حفاظتی مانند دیواره آتش، پالایش، ردیابی، ذخیره اطلاعات و کنترل دامنه و اقداماتی از این قبیل در خصوص دستیابی مجرم به ابزار ارتکاب جرم پیشگیری فنی خوبی را می تواند به عمل آورد. با این حساب یکی از سیاست‌های پیشگیری وضعی همین اقدامات برشمرده می شوند.

مرحله اصلی در این فرایند عملیات اجرایی جرم و رفتار مادی است که بزه دیدگان در فضای مجازی اکثراً از روی علم یا بعضاً از روی جهل به دست به اقداماتی میزنند که بزه دیده واقع‌شدن آن‌ها محتمل می شود و اگر سواستفاده گران از حضور دیگران اگاه باشند، تعرض به آنان از جانب افراد مختلف به‌سوی آنان بسیار زیاد است. این در حالی است که اگر شخصی به نحوی رفتار کند که برای مجرمین جلت توجه نکند، درصد مصونیت او از خطرات احتمالی بیشتر می شود. به همین خاطر یکی از ساده‌ترین ویژگی‌های تامین فضا، کم بودن اطلاعات از افراد در دسترس دیگران است.(عباسی کلیمانی و اکبری، ۱۳۹٤، ص۱۵۷)

۳-۵.ویژگی‌های تدوین راهبرد در عرصه پیشگیری از جرایم علیه امنیت در فضای مجازی: الف)قهری نبودن، بدین معنا که در حوزه پیشگیری از جرائم از تصمیم هایی اتخاذ شوند که سرکوبگر نیستند. ب)قابلیت پیشبینی و کنشگری، گام های پیشگیرانه از جرائم متوجه به زمانی است که هنوز جرم اتفاق نیافته است؛ بدین معنا که اتخاذ تصمیمات جهت پیشگیری پیش از اینکه اشخاص به سمت رفتار های مجرمانه بروند، مورد نظر گرفته می‌شود که هدف از آن جلوگیری از ورود مردم به رفتارهای مجرمانه است. این در حالی است که تصمیمات نظام عدالت کیفری برخورد با جرائم است و بنابر اصول پس از واقع شدن جرم به اجرا در می‌آیند.(شاکری، ۱۳۸۳، ص۱۰) پ)کلی وجامع بودن، تصمیمات متخذه در جهت پیشگیری از جرائم

مربوط به کاهش سطح تهدیدات جرم زا مربوط به گروه خاصی از مردم جامعه نیست؛ و همه مردم جامعه و یا بخش قابل توجهی از شهروندان را شامل می شود. ت)متاثر سازی بستر های جرم، پیشگیری از جرائم با توجه به عامل فرد با محیط و عامل وضعی تاثیر پذیرفته از گام های جهت پیشگیری تشکیل می شود.(نیازپور، ۱۳۹٤، ص٤۳) سازمان ملل نیز اصول راهبردی برای پیشگیری از جرم دارد که می‌تواند مورد استفاده قرار گیرد. (قناد، ۱۳۸۷، ص۲۱۹)

۳-٦.مراحل پیشگیری از جرم علیه امنیت ملی در فضای مجازی:

مرحله اول شناخت چهره جرم: برای دستیابی به این مقوله که با عنوان سیمای بزهکاری نیز از آن یاد می شود باید با استفاده از داده های آماری و اطلاعات مناسب و همچنین با لحاظ آگاهی‌هایی که در نتیجه عمل مجرمانه حاصل می شود، باید چهره‌ی عمل مجرمانه، چهره مجرمان این حوزه، ویژگی‌های مشترک بین بزه دیدگان مورد مطالعه و شناخت قرار گیرند.

مرحله‌ی دوم شناسایی اهداف مجرمانه: در این قدم باید برای شناخت اهداف و سبیل جرم اقدام کرد. در جرایم فضای مجازی به دلیل گستردگی موجود این امکان نیست که برای جرائم به‌صورت جداگانه اتخاذ تصمیم و تدبیر نمود تا در حوزه پیشگیری از جرم رشد ایجاد شود. در نتیجه باید به اولویت‌بندی التفات کرد.

مرحله سوم مطالعه و انتخاب نظریه: برای دستیابی به این مسئله ابتدا جرم علل یابی می شود و سپس عوامل مؤثر بر ارتکاب آن مورد مطالعه قرار میگیرد و در نهایت یک نظریه جرم شناسانه و علت شناسانه ارائه می شود.

مرحله چهارم تعیین روش: این مرحله مخصوص آن گروه از روش‌هایی است که با توجه به خصوصیات مشترک بین بزهکاران و انتخاب اهداف مجرمانه است و می‌توانند ما را به انتخاب روش نزدیک‌تر کنند.

مرحله پنجم انتخاب مجریان: پس از انتخاب و اتخاذ و برنامه های پیشگیرانه در این قدم مراجع مجری و متولی که باید روش‌های پیشگیرانه را عملی سازند، مشخص می‌شوند.

مرحله‌ی ششم برنامه اجرایی: تصمیمات اتخاذ شده پیشگیرانه برای عملیاتی شدن باید طبقه بندی شود. تدابیر و طراحی پیشگیرانه باید یک بازه زمانی معین و بررسی شده و زمان دقیق‌عملیاتی هر یک از طبقات و گام های پیشگیرانه در آن گنجانده شود به نحوی که حتما به سر انجام برسد.

مرحله هفتم آزمودن و ارزیابی: در مرحله آخر و پس از عملیاتی شدن باید ارزیابی تمام مراحل انجام شود به‌موجب این ارزیابی

در طراحی سیستم پیشگیری، می توانیم نقاط قوت و ضعف موجود در سیستم مورد مطالعه پیشگیرانه بشناسیم. (نیازپور، ۱۳۹٤، ص۱۲۲)

٤. روش تحقیق

روش جمع آوری داده ها با استفاده از مدل کتابخانه ای و داده های اسنادی و همچنین روش گروه کانونی است که به‌عنوان روش پژوهش مکمل در پژوهش‌های کمّی و کیفی بکار می‌رود. روش گروه کانونی به‌نوعی بحث گروهی [3]اطلاق می‌شود که درصدد کاوش دسته‌ای از جریان‌های معین است. مصاحبه گروه کانونی (در معنای عام) سبکی از مصاحبه است که برای گروه‌های کوچک طراحی‌شده است. جامعه هدف مورد مصاحبه در این پژوهش خبرگان در حوزه‌های فناوری اطلاعات و ارتباطات و حقوق جزا و جرم‌شناسی تعداد ده نفر هستند. طبقه‌بندی بیان‌شده مورد اتفاق اکثریت افراد مورد مصاحبه بوده و بدون استفاده از تقدیم‌وتأخیر و اولویت فقط احصاء و نگارش شده است.

روش تجزیه‌وتحلیل داده‌ها در این پژوهش با استفاده از ماتریس سوات[4]است؛ که یک روش موفق برای برنامه‌ریزی راهبردی به شمار می‌رود. جهت دستیابی به راهبردهای اجرایی و پاسخ به سوال‌های تحقیق در مرحلع ابتدائی با استفاده از تکنیک مذکور هر یک از عوامل نقاط قوت، نقاط ضعف، فرصت‌ها و تهدیدها با توجه به محیط داخلی و خارجی حوزه جرائم علیه امنیت ملی در فضای مجازی جمهوری اسلامی ایران شناسایی شد؛ و در ادامه با استفاده از تحلیل چهارگانه اقدام به تدوین و توضیح راهبرد می‌شود.

٥. تشکیل سوات[5]

جمع‌آوری ویژگی‌ها و عوامل مخصوص به جرائم علیه امنیت ملی در فضای مجازی با استفاده از مصاحبه عمیق و گروه کانونی و همچنین جمع‌آوری داده‌های کتابخانه‌ای صورت گرفته است. این مصاحبه‌ها در چندین مرحله صورت گرفته که در هر مرحله پس از جمع‌آوری ویژگی‌ها بر اساس محیط داخلی و خارجی و ویژگی مثبت و منفی طبقه‌بندی‌شده است.. برخی از این ویژگی‌ها از یک بعد می‌تواند دارای نکات مثبت و از بعد دیگر دارای نکات منفی باشد، همچنین برخی از این ویژگی‌ها از یک بعد مؤثر بر محیط داخل و از بعد دیگر جز عوامل محیط خارجی هستند. در این مبحث صرفاً به شخص کردن تعدادی از

[3] group discussion
[4] SWOT
[5] SWOT

عوامل و ویژگی‌های جرائم علیه امنیت ملی پرداخته‌شده و این به این معنا نیست که تمامی موارد احساس شده، اما آنچه مقصود نگارنده و جامعه خبرگانی بوده، جمع‌آوری موارد کلی بااهمیت برای تعیین و تدوین راهبرد مؤثر است.یافته‌ها نشان می‌دهد که ضعف سواد دیجیتالی کاربران، نیازهای احساسی، مالی و اطلاعاتی افراد، ضعف فرهنگی، کمبود قوانین و مقررات مناسب و بازدارنده، ناکارآمدی سیستم‌های ایمنی، تورم و نقایص اقتصادی، افزایش بیکاری و خطر پایین دستگیری مهمترین عوامل موثر در بروز رفتارهای مجرمانه در فضای مجازی هستند.(محمدی مقدم وهمکاران ۱۴۰۱، ص۸۷)

۵-۱.شناسایی نقاط قوت[6]: الف)وجود متخصصان برای پیشگیری و مقابله با جرائم امنیتی در فضای مجازی. ب)عدم محدودیت جغرافیایی در عرصه مقابله با جرم، از این قابلیت به‌عنوان یک نقطه قوت از دو جهت پیشگیری و اقدام متقابل می‌توان یادکرد. پ)وجود سرعت بالا در فناوری‌ها جهت مقابله با جرائم، معمولاً برای شناخت و تعقیب مجرمان و حفظ آثار و ادله جرم و جلوگیری از فرار مرتکب یا رفع آثار زیان‌بار جرم هرچه مأمورین زودتر بتوانند درصحنه جرم حاضر شوند موفق‌تر خواهند بود. فضای مجازی باوجود سرعت‌بالای آن می‌تواند این امکان را برای ضابطین فراهم آورد. ت)وجود کار تیمی، تیم مجموعه کوچکی از افراد است که مهارت‌های مکمل دارند، همگی نسبت به یک مقصد مشترک شیوه عملکرد مشترک و اهداف مشترک متعهد هستند و خود را نسبت به یکدیگر مسئول می‌دانند. ث)امکان قابلیت پیشگیرانه کنترل و رصد. ج)توجه و اهتمام در سطح حاکمیت. چ)وجود قابلیت ردیابی و تعقیب جرایم. ح)طبقه‌بندی متمرکز بر جرائم از نظر اهمیت جرم و مجرمین با توجه به شخصیت آنها. خ)امکان مقابله چندبعدی ازجمله افزایش پیشگیری‌های شناختی، مقابله نرم و هدفمند، اعمال مؤلفه‌های جامعه‌شناسی جرم و کاهش بسترهای اجتماعی جرم‌زا است.

۵-۲. شناسایی نقاط ضعف[7]: الف)نبود زیرساخت‌های کافی جهت پیشگیری و مقابله حداکثری. ب)وجود دسترسی بالا و بدون محدودیت کاربران. پ)نبود منابع انسانی متخصص، آنچه به‌عنوان نقطه‌ضعف می‌توان نام برد: اول نبود منابع انسانی متخصص به مقدار کافی است و دوم نداشتن تخصص لازم منابع انسانی حاضر است. ت)گستردگی چندبعدی فضای ارتکاب جرم، بزهکاران در این بستر از حیث تعداد دفعات ارتکاب جرم در جرائم آنی شرایط مساعدتری دارند. همچنین در جرائم مستمر به خاطر وجود محدودیت کمتر می‌توانند استمرار را در پهنه زمانی بالاتری ارتکاب یابند. ث)ضعف آگاهی و فرهنگ استفاده صحیح و نبود آموزش کافی، با توجه به رشد صنعت و فنّاوری، ازجمله مسائل تمدنی در سده اخیر، عقب‌ماندگی فرهنگ‌سازی مناسب جهت استفاده صحیح از این پیشرفت‌ها است. این موضوع کلی در خصوص فضای مجازی و تحقق جرائم علیه امنیت ملی در این فضا نیز صادق است. بخش زیادی از بزه دیدگان در این موضوع و یا مجرمان اتفاقی کسانی هستند که عدم آموزش کافی، آگاهی لازم، فرهنگ استفاده صحیح و توان مدیریت اصولی در آن‌ها نهادینه نشده است. ج)غیر فیزیکی بودن، که باعث سهل‌انگاری و ساده‌انگاری کاربران در خصوص ارتکاب جرم یا پیامدهای مجرمانه رفتار آنان است. چ)عدم هماهنگی کافی بین افراد و سازمان‌ها و سامانه‌های اطلاعاتی و امنیتی، جهت ایجاد امنیت پایدار. ح)عدم تناسب بین بزهکار و بزه دیده، بزهکاران جرائم علیه امنیت ملی در فضای مجازی به‌طورمعمول از افراد نخبه جامعه با تخصص بالا هستند که با برنامه‌ریزی و نقشه قبلی و معمولاً به‌طور سازمان‌یافته مرتکب جرم می‌شوند. بزه دیدگان مورد سوءاستفاده در این جرائم به‌طورمعمول افراد دارای جهل

[6] Strengths
[7] Weaknesses

و غفلت نسبت به جرم هستند که به‌صورت ناگهانی با رفتار مجرمانه مواجه و هنگام تصمیم‌گیری در عمل انجام‌شده قرار می‌گیرند. خ) وجود بستر آماده جهت ارتکاب جرم، ازجمله آن ساماندهی آسان گروه‌های مجرمانه، ارتباطات راحت با اعضا، استفاده از پلتفرم‌های بدون محدودیت و عدم نیاز به پاسخگویی به دولت باعث ایجاد فضایی مناسب جهت ارتکاب جرم شده است.

۵-۳.شناسایی فرصت ها[8]: الف) مدیریت هدفمند امکانات و ایجاد بهره‌وری بالا، درواقع وجود منابع و امکانات قدم اول برای رسیدن به هدف است اما چگونه برنامه‌ریزی کردن و مدیریت مهم‌ترین مسئله خواهد بود. ب) گسترش دانش بومی. پ) امکان همکاری بین‌المللی، امروز جامعه جهانی در گذار تاریخی خروج از دوقطبی بودن و افزایش دیپلماسی بین‌المللی بر پایه روابط برابر است. ت) نظارت الکترونیک جهت هویت بخشی و پالایش اصولی. ث) استقبال مردم به فضای مجازی، فرصت خوبی برای مدیران این حوزه است تا بتوانند اقدام مناسب جهت تخصیص منابع، افزایش امکانات و... برای پیشگیری و کاهش وقوع جرائم علیه امنیت ملی انجام دهند. ج) فرهنگ‌سازی و آموزش عمومی. چ) امکان استفاده از قوانین و مقررات، در همه کشورها و در همه عرصه‌ها معمولاً، انتقادات منتقدین حقوقدان به قوانین مصوب وجود اجمال، اهمال، نقص، ناکارآمدی و عدم تناسب قوانین و اهداف قانون‌گذار است که باید به آن پرداخته شود؛ اما آنچه ما می‌خواهیم به آن بپردازیم وجود فرصت‌های خوبی است که قوانین برای دستگاه قضایی ایجاد کرده تا بتواند با استفاده از آن کیفردهی متناسب و مجازات‌های بازدارنده را برای مرتکبین جرائم علیه امنیت ملی در فضای مجازی به عمل آورد. ازجمله این موارد وجود دادرسی افتراقی و یا مجازات‌های تکمیلی برای این دسته از جرائم و مجرمین است. ح) استفاده از بخش خصوصی، این همکاری‌ها می‌تواند به‌صورت دائم و یا موقت پروژه محور باشد.

۵-٤. شناسایی تهدیدات[9]: الف)افزایش روزافزون جرائم فضای مجازی. ب) جاماندگی در تقنین به نسبت رشد فضای مجازی. پ) پویایی و تغییرات. ت)عدم محدودیت‌های جغرافیایی در ارتکاب جرم. ث) نبود شرایط ایجاد زیرساخت‌های بومی به مقدار کافی. ج) وجود برخی سرورها و زیرساخت‌ها سایبری در خارج از کشور. چ) سو استفاده از عدم وجود شرایط کافی جهت حفاظت از فضای مجازی. ح) گسترده بودن حجم و ابعاد تأثیرگذاری.

٦. تحلیل سوات

در مدل ماتریس سوات پس از تشخیص و تشکیل نقاط قوت، نقاط ضعف، فرصت‌ها و تهدیدها چهار الگو از تحلیل ذیل انجام می‌شود. الف)راهبرد تهاجمی[10] در این راهبرد با استفاده از نقاط قوت تأثیر فرصت‌ها محیطی را برای افزایش بازدهی، بهره‌وری و رشد انجام می‌دهیم. ب)راهبرد رقابتی[11] به این شکل که از نقاط قوت برای کم کردن و یا از بین بردن تهدیدها

[8] Opportunities

[9] Threats

[10] SO
[11] ST

استفاده می‌شود. ج)راهبرد محافظه‌کارانه [12]بدین معنا که با استفاده از فرصت‌های شناسایی‌شده بتوان نقاط ضعف را کاهش داد یا از بین برد. د)راهبرد تدافعی[13] زمانی است که با دوری کردن از تهدیدهای محیطی به دنبال کاهش نقاط ضعف است.

جدول ماتریس ارزیابی عوامل

محیط داخلی	نقاط قوتS	نقاط ضعفW

[12] WO
[13] WT

فرصت‌هاO	الف) تخصیص امکانات و بودجه برای گسترش دانش‌بنیان آینده‌نگر ب) طراحی سیستم سه‌ضلعی نظارت، فرهنگ‌سازی و بازدارندگی پ) کنترل و رصد فضای مجازی در سطح جهانی با افزایش روابط دیپلماتیک بین‌المللی ت) افزایش سطح کارآمدی و بهره‌وری بهینه با استفاده از مدیران	الف) ایجاد سیستم اطلاعاتی ارتباطی منسجم و هدفمند بین اشخاص و نهادها برای کاهش هزینه و صرفه‌جویی ب) شناخت و حل نیازهای پیش روی آینده فضای مجازی برای پیشگیری و مقابله با جرائم علیه امنیت ملی پ) ایجاد سیستم آموزشی جهت افزایش آگاهی و فرهنگ‌سازی مردم جامعه ت) کنترل و هدایت فضای مجازی با فعال‌سازی بخش خصوصی در همکاری و انتقال دانش بین‌المللی
تهدیداتT	الف) ایمن‌سازی فضای مجازی با طبقه‌بندی در کنترل و رصد ب) ردیابی و تشخیص تیمی با استفاده از وسعت زمانی و مکانی جهت کاهش حجم و ابعاد جرائم پ) گسترش زیرساخت‌های دانش‌بنیان با بهره‌مندی از متخصصین	الف) ایجاد تدابیر حفاظت از فضای مجازی ب) ایجاد محدودیت تأثیرات جرائم علیه امنیت ملی پ) برنامه‌ریزی برای آینده جهت آمادگی مواجه با تغییرات ت) فراهم کردن شرایط لازم جهت ساخت و گسترش زیرساخت‌ها

نتیجه

جهان امروز به‌گونه‌ای تکامل می‌یابد که بشر در زندگی روزمره وابستگی بیشتری به فضای مجازی پیدا می‌کند. این تکامل در کنار جهات مثبت خود در عرصه ارتباطات و اطلاعات فرصت سوءاستفاده مجرمین را فراهم آورده تا بتوانند به مقصد سو خود جهت ایجاد خسارت و آسیب در امنیت کشورها وارد آورند. همان‌طور که بیان شد جمهوری اسلامی ایران در ایجاد مجموعه‌های

مختلف، زیرساخت‌ها و قوانین و مقررات تا حدود زیادی در این مسیر حرکت روبه‌پیشرفت داشته. لکن فاصله وضعیت موجود و مطلوب را می‌توان بامطالعه، برنامه‌ریزی و مدیریت کمتر کرد. در این پژوهش الگوی مشخص جهت استخراج داده‌های جمع‌آوری‌شده پس از شناسایی عوامل مؤثر بر محیط داخلی و بیرونی وجود داشته که چهار مؤلفه اصلی راهبردی است.

پس با توجه به انجام فرایند تحلیل و بررسی از چهار سرفصل می‌توان به‌عنوان نتایج به‌دست‌آمده یادکرد. در ابتدا اشاره به راهبردهای به‌دست‌آمده از تحلیل تهاجمی می‌شود که حاصل جمع عوامل فرصت زا در محیط خارجی و نقاط قوت در محیط داخلی ارتکاب جرائم علیه امنیت ملی در فضای مجازی است. راهبرد تخصیص امکانات و بودجه برای گسترش دانش‌بنیان با لحاظ آینده‌نگری یکی از اهمیت‌های آن مواجهه با پدیده‌های نوظهور ازجمله هوش مصنوعی و یا ارزهای دیجیتالی است که با سرعت خیلی بالایی در حال گسترش هستند. درواقع یکی از راه‌های مقابله با جرائم ضد امنیت ملی در فضای مجازی در این پدیده‌های مختلف پیش‌بینی آینده و تدارک و ایجاد امکانات لازم است. راهبرد طراحی سیستم سه‌ضلعی نظارت، فرهنگ‌سازی و بازدارندگی، با توجه به حجم و ابعاد وسیع بستر فضای مجازی و تنوع جرائم ضد امنیت ملی باید دستگاه‌های باقابلیت مقابله چندبعدی طراحی کرد تا بتوان در این زمینه حرکت مطلوبی انجام داد. راهبرد کنترل و رصد فضای مجازی در سطح جهانی با افزایش روابط دیپلماتیک بین‌المللی، راهبرد مذکور حتماً باید به‌صورت مشخص در وزارت امور خارجه در دستور کار قرار بگیرد و جز اولویت‌های توافق‌نامه‌های همکاری بین کشورهای دوست و پلیس اینترپل باشد، این راهبرد ازجمله مؤلفه‌هایی است که ارتباط بسیار زیادی به قدرت دیپلماسی و توانایی گفتمان کشور دارد. راهبرد افزایش سطح کارآمدی و بهره‌وری بهینه با استفاده از مدیران، وجود مدیران متخصص و مجرب در سطح کلان، میانی و صفی جهت مقابله با جرائم ضد امنیت ملی ازجمله ضرورت‌هایی است که به‌واسطه آن افزایش سطح کارآمدی و بهروه وری را به دنبال دارد.

راهبردهای به‌دست‌آمده از تحلیل رقابتی یعنی استفاده از نقاط قوت موجود برای کاهش تهدیدها در محیط خارجی ارتکاب جرائم ضد امنیت فضای مجازی که می‌توان به آن‌ها اشاره کرد، راهبرد اول ایمن‌سازی فضای مجازی با طبقه‌بندی در کنترل و رصد. وجود قابلیت کنترل و رصد در فضای مجازی یک نقطه قوت است که با طبقه‌بندی نوع جرم و شخصیت مجرم به فعلیت می‌رسد. طبقه‌بندی نوع جرم ازلحاظ سطح اهمیت و قدرت تأثیر مخرب و همچنین طبقه‌بندی مجرمی به لحاظ سابقه و سطح تخصص در کنترل و رصد فضای مجازی جهت پیشگیری و ارتکاب جرم علیه امنیت ملی نقش بسزایی دارد. راهبرد دوم ردیابی و تشخیص تیمی با استفاده از وسعت زمانی و مکانی جهت کاهش حجم و ابعاد جرائم. کار تیمی یک مؤلفه جدید تدوین‌شده در سرفصل‌های دروس مدیریتی است که بسیار مثمر ثمر بوده و در این زمینه مطالعات دقیق انجام‌شده، وجود کار تیمی می‌تواند در این زمینه همانند هر زمینه‌ی دیگر می‌توان یکی از بازوان تنظیم این راهبرد در کنار استفاده از وسعت زمانی و مکانی جهت مقابله با جرائم ضد امنیت ملی در فضای مجازی باشد. راهبرد سوم گسترش زیرساخت‌های دانش‌بنیان با بهره‌مندی از متخصصین. وجود متخصصین مستعد و توانمند ایرانی در حوزه اطلاعات و فنّاوری به‌عنوان سرمایه‌های واقعی کشور به‌عنوان نقطه قوت است. این مهم وقتی توأم با توجه و اهتمام حاکمیت به جرائم امنیتی سایبری قرار بگیرد می‌تواند زمینه گسترش و پیشرفت در حوزه افزایش هدفمند زیرساخت‌های بومی باشد. پس در عرصه پیشگیری و مقابله با جرائم ضد امنیت ملی در فضای مجازی این راهبرد باید توسط مدیران به مرحله‌ی عملیات برسد.

راهبردهای به‌دست‌آمده با عنوان راهبردهای محافظه‌کارانه درواقع استفاده از وجود فرصت‌ها احتمالی موجود در فضای خارجی جرائم ضد امنیت ملی در فضای مجازی و همچنین شناسایی نقاط ضعف موجود در فضای داخل سازمان و کاهش سطح نقاط ضعف احتمالی است. راهبرد اول ایجاد سیستم اطلاعاتی ارتباطی منسجم و هدفمند بین اشخاص و نهادها برای کاهش هزینه و صرفه‌جویی. استفاده از این راهبرد کاهش هزینه‌ها و افزایش دقت در عمل را در پی خواهد داشت. راهبرد دوم شناخت و حل نیازهای پیش روی آینده فضای مجازی برای پیشگیری و مقابله با جرائم علیه امنیت ملی. این مسئله نیازمند تدوین برنامه جهت استفاده هدفمند از منابع هستیم تا بتوانیم با فنّاوری دانش‌بنیان متخصصین و با پیش‌بینی و آینده‌نگری نیاز سخت‌افزاری کشور، راه‌حل مناسب برای پیشگیری و مقابله حداکثری با جرائم داشته باشیم. راهبرد سوم ایجاد سیستم آموزشی جهت افزایش آگاهی و فرهنگ‌سازی مردم جامعه. در دستور کار قرار گرفتن این مهم در وزارتخانه‌ها و نهادهای متولی باید به‌عنوان یک فرایند عملیاتی در جهت اجرایی شدن این راهبرد قرار گیرد. راهبرد چهارم کنترل و هدایت فضای مجازی با فعال‌سازی بخش خصوصی در همکاری و انتقال دانش بین‌المللی. فرصت استفاده بخش خصوصی به‌وسیله همکاری با کشورها جهت تبادل دانش، اطلاعات، تجارب، امکانات، منابع و تاکتیک‌ها راه‌حل مناسب جهت کنترل تمامی ابعاد جرائم علیه امنیتمی در فضای مجازی خواهد بود.

راهبردهای به‌دست‌آمده از تحلیل تدافعی با تجزیه‌وتحلیل تهدیدها و نقاط ضعف به دست می‌آید و کاربرد آن کاهش نقاط ضعف در محیط داخلی و همچنین خنثی‌سازی تهدیدها در فضای خارجی جرائم ضد امنیت ملی در فضای مجازی است. ازجمله آن می‌توان به راهبرد اول اشاره کرد، ایجاد تدابیر حفاظت از فضای مجازی. درواقع کنترل و کاهش سطح تهدیدها به روش حفاظت از فضای مجازی، می‌تواند از تشدید نقاط ضعف جلوگیری کند. راهبرد دوم ایجاد محدودیت تأثیرات جرائم علیه امنیت ملی. راهبرد سوم برنامه‌ریزی برای آینده جهت آمادگی مواجه با تغییرات. برای کنترل این گستردگی چندبعدی و جلوگیری جلوه منفی آن باید با برنامه‌ریزی آینده‌نگر، نسبت به جرائم علیه امنیت ملی در فضای مجازی، بتوانیم آمادگی مواجهه با تغییرات و پویایی را کسب نماییم. راهبرد چهارم فراهم کردن شرایط لازم جهت ساخت و گسترش زیرساخت‌ها. برای کنترل نقطه‌ضعف نبود زیرساخت بومی باید یک راهبرد جهت برطرف کردن موانع ساخت و گسترش ایجاد و عملی شود.

پیشنهادات

الف) پیشنهادها کاربردی

۱-ایجاد سیستم هماهنگ نظارت، فرهنگ‌سازی، بازدارندگی به‌صورت متناسب؛

۲-بازنگری، اصلاح، تغییر و تکمیل قانون جرائم رایانه‌ای جهت تأمین مسائل روز فضای مجازی؛

۳-تأمین منابع انسانی متخصص و واگذاری امکانات به‌روز و تجهیزات موردنیاز ضابطین در جهت مقابله با جرائم ضد امنیت ملی؛

٤-برگزاری دوره‌های علمی و کارگاه‌های آموزشی جهت مهارت افزایی و فراگیری دانش روز برای منابع انسانی فعال در این حوزه؛

۵-برنامه‌ریزی و همکاری با نهادهای متولی جهت افزایش فرهنگ استفاده از فضای مجازی در سطوح مختلف جامعه و برای تمامی اقشار؛

٦-انعقاد تفاهم‌نامه همکاری، تشکیل معاهدات بین‌المللی و عضوت در کنوانسیون‌ها جهت همکاری با سایر کشورها در راستای پیشگیری و مقابله با جرائم ضد امنیت ملی در فضای مجازی؛

۷-ایجاد سامانه اطلاعاتی جامع و منسجم با همکاری سازمان‌ها برای دسترسی ضابطین و مقامات قضایی؛

۸- فراهم نمودن ساز کارهای هویت‌بخش برای کاربران فضای مجازی جهت حفاظت از فضای مجازی و ایجاد محدودیت جهت پیشگیری از وقوع جرم و تسهیل در تعقیب مجرمین با توسعه استفاده از رمزهای یک‌بارمصرف و یا احراز هویت بیومتریک و اقدامات از این قبیل؛

۹-تولید و گسترش سامانه‌های ملی با اتکا به شرکت‌های دانش‌بنیان و استفاده از ظرفیت‌های علمی دانشگاهی، متخصصین بخش خصوصی. از قبیل سامانه عامل، موتورهای جستجو، سرویس‌دهنده‌های پست الکترونیک، پیام‌رسان‌ها و رسانه‌های ارتباط‌جمعی؛

۱۰-تشکیل کارگروه‌های مطالعات هدفمند برای آسیب‌شناسی و پیش‌بینی جرائم ضد امنیت ملی در فضای مجازی در آینده و برنامه‌ریزی برای مواجه با خطرات احتمالی آینده؛

ب) پیشنهادها علمی و پژوهشی

۱-انجام مطالعات و پژوهش‌ها جهت عملیاتی کردن هرکدام از راهبردهای مطرح‌شده در ایران؛

۲-بررسی و ریشه‌یابی علل وقوع جرائم ضد امنیت ملی در مجرمین اتفاقی دارای ضعف نفس و راهکارهای پیشگیری و مقابله با آن؛

۳-انجام تحقیق علمی برای ساخت، تولید و گسترش سخت‌افزار و نرم‌افزارهای ملی و بومی دانش‌بنیان؛

٤-مطالعه تطبیقی قوانین بازدارنده جرائم فضای مجازی در کشورهای جهان؛

۵-آینده‌پژوهی جرائم ضد امنیت ملی در فضای مجازی به‌صورت مستمر؛

٦-انجام مطالعات تطبیقی برای شناخت راهبردهای جهان‌شمول در پیشگیری و مقابله با جرائم ضد امنیت کشورها در فضای مجازی.

منابع

۱. بیگی نیا، عبدالرضا و سعادتمند، محمد و کریمی دین ابادی، مردعلی و ناظمی پور، بهزاد،۱۳۸۹،*بررسی و مطالعه برنامه ریزی استراتژیک در بنگاههای کوچک و متوسط باتاکید بر مدلسازی مالی*،پنجمین کنفرانس بین المللی مدیریت استراتژیک،ش٦ ، ص۱۲ –۲۹.

۲.بیات بهرام و شرافتی پور جعفر و عبدی نرگس، ۱۳۸۷، *پیشگیری از جرم با تکیه‌بر رویکرد اجتماع‌محور* ، نشر ناجا، تهران.

۳.پاکزاد، بتول، ۱۳۹۰، تروریسم سایبری تهدیدی نوین علیه امنیت ملی، معاونت پژوهشی دانشگاه آزاد اسلامی، تهران.

٤.پاکزاد، بتول، ۱۳۸۸، تروریسم سایبری، رساله دکتری حقوق جزا و جرم‌شناسی، دانشکده حقوق دانشگاه شهید بهشتی.

۵.توکلی، مرجان، ۱۳۹۲ ،پیشگیری خانواده مدار از بزهکاری کودکان، پایان نامه، دانشگاه امام صادق.

٦.جوان جعفری عبدالرضا و سید زاده ثانی مهدی، ۱۳۹۱ ،رهنمودهای عملی پیشگیری از جرم چاپ اول معاونت پیشگیری از وقوع جرم قوه قضائیه انتشارات میزان، تهران.

۷.حسن بیگی، ابراهیم، ۱۳۸۹ ،مدیریت راهبردی، انتشارات دانشگاه عالی دفاع ملی، تهران.

۸.خرم‌آبادی، عبدالصمد، ۱۳۸٤،جرائم فناوری اطلاعات، رساله دکتری دانشگاه حقوق و علوم سیاسی دانشگاه تهران.

۹.رهامی، محسن؛ پرویزی، سیروس ۱۳۹۲، جاسوسی رایانه‌ای در حقوق ایران و وضعیت بین‌المللی آن، فصلنامه حقوق، دوره ٤۲، شماره۳. ص٤۰–۵۷.

۱۰.زندی، محمدرضا، ۱۳۹۳، تحقیقات مقدماتی در جرائم سایبری، انتشارات جنگل، تهران.

۱۱.زیوری، کامران،۱۳۹۱، سیاست جنایی ایران در پیشگیری از جرائم رایانه‌ای، انتشارات وزارت علوم، تحقیقات و فناوری،تهران.

۱۲.عالی پور، حسن ،۱۳۸۷. توازن میان امنیت ملی و آزادی‌های فردی در مقابله با جرائم تروریستی، رساله دکتری حقوق جزا وجرم شناسی، دانشگاه تهران.

۱۳.شاکری، ابوالحسن.۱۳۸۳، قوه قضائیه و پیشگیری از وقوع جرم، مجموعه مقالات همایش علمی-کاربردی پیشگیری از وقوع جرم، ش۵، ص۷۰– ۹۰.

۱٤.عباسی کلیمانی، عاطفه، اکبری، عاطفه، ۱۳۹٤، جرائم سایبری، انتشارات مجد، تهران.

۱۵.فضلی، مهدی، ۱۳۹۱، مسئولیت کیفری در فضای سایبر، نشر خرسندی، تهران.

۱٦..قناد، فاطمه. ۱۳۸۷، پیشگیری کیفری از جرائم ارتکابی در فضای مجازی ، فصلنامه پیشگیری از جرم و بزه دیدگی، پلیس پیشگیری ناجا. ش۳، ص۳٤–۵۷.

۱۷.محسنی, فرید. ،۱۳۹۰. سهم کودکان و نوجوانان از حمایت کیفری در فضای مجازی و حقیقی .*آموزه‌های حقوق کیفری*. ش۷، ص ٦۷ –۹۸.

۱۸.محمدی مقدم, یوسف, ساعدی, عبداله ,محسنی, فرید. ۱٤۰۱. واکاوی عوامل مؤثر وقوع جرم در فضای مجازی. نشریه علمی پژوهش‌های دانش انتظامی، شماره ٤.ص ٤-۲۷.

۱۹.منصورآبادی، عباس، ۱۳۸۷، فصلنامه مطالعات پیشگیری از جرم، سال سوم، شماره هشتم، پائیز. ص ۹۹ -۱۲۰.

۲۰.میر محمدصادقی، حسین. ۱۳۹۳، جرائم علیه امنیت و آسایش عمومی. چاپ ۲۵، نشر میزان، تهران.

۲۳.نیاز پور، حسن. ۱۳۹٤، دانشنامه بزه دیده شناسی و پیشگیری از جرم، نقد کتاب فقه حقوق. تهران.

۲٤.نویدکیا، وحید، ۱۳۹۹، سیاست جنایی ایران در خصوص مجازات های جایگزین حبس، پایان نامه، موسسه آموزش عالی خراسان.

۲۵.وروایی، اکبر، مدنی پور، حسین، ۱۳۹۲، مقاله جرائم سایبری از علت شناسی تا پیشگیری، دانشگاه علوم قضایی.ش ۱۰،ص۵۷-۷۸.

۲٦.وطنی، امیر ، اسدی، حمید، ۱۳۹۵، سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم، پژوهش های حقوق اسلامی ، سال ۱۷، شماره اول، ص۹۹ -۱۲٦.

۲۷.هلیلی, خداداد. ۱٤۰۰. فناوری‌های نوظهور سایبری و تهدیدات ناشی از به‌کارگیری آن‌ها در سازمان‌های دفاعی-نظامی .*فصلنامه مطالعات. ص ۹۷-۱۲۱.*

قوانین

۱.قانون اساسی

۲.سیاست‌های کلی نظام در امور پدافند غیرعامل ابلاغی ۱۳۸۹

۳.قانون جرائم رایانه‌ای مصوب ۱۳۸۸

٤.قانون مجازات جرائم نیروهای مسلح مصوب ۱۳۸۲

۵.قانون تعزیرات ۱۳۷۵

٦.قانون مجازات اسلامی مصوب ۱۳۹۲

۷.قانون مطبوعات مصوب ۱۳٦٤

۸. قانون برنامه ششم توسعه مصوب ۱۳۹۵

۹. قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹-۹

۱۰.قانون تجارت الکترونیکی در سال ۱۳۸۰

۱۱.قانون تشکیل ناجا مصوب ۱۳۴۸

۱۲.کنوانسیون جرائم سایبری، بوداپست، ۲۰۰۱

۱۳.توصیه‌نامه استراسبورگ، ۱۹۹۰

Developing Strategies to Combat Crimes Against National Security in Cyberspace

Authors: Mehdi Mohseni, Najmeh Sadat EzzatiAbstract

The current research examines crimes against national security in cyberspace. Ensuring national security has always been one of the concerns of governments around the world. Also, cyberspace as an emerging technology that is developing at a high speed poses many challenges in the field of human sciences, including law. Management has created sociology and psychology. Among the necessary issues in this area is the formulation of strategies to deal with crimes against national security, the formulation of a strategy is one of the most basic components of the principled management of the target group. In order to develop a strategy, different patterns are proposed, including the patterns of using the strengths, weaknesses, threats and opportunities for the study group. If a comprehensive and complete strategic document is drawn up in the field of crimes against national security in the context of cyberspace, it is possible to prevent Committing the mentioned crimes is concretely provided; And accordingly, the statistics of the aforementioned crimes will be visibly reduced. Also, by using this strategic document, it is possible to monitor the future and predict possible events and planned movements of external driving factors. In order to be able to better manage possible crises with this foresight, cyber crimes and threats in the third millennium have put the implementation of laws in many countries of the world at risk. Developed countries have stepped forward to fight these crimes and have formulated laws.

Keywords: crime, cyber space, security crimes, cyber crimes, national security.