سیاست کیفری جمهوری اسلامی ایران در برابر جرایم سایبر و ارزیابی امنیت آن

محمدحسن فرخی[1]

[1] دکتری امنیت سایبری، کارشناس رسمی دادگستری رشته کامپیوتر، فناوری اطلاعات و ارتباطات و فضای مجازی
mhf1364@gmail.com

چکیده

حملات سایبری در جهان کنونی و مدرن توسط برخی افراد، ساختار و اطلاعات یک کشور را می‌تواند دگرگون سازد. از حملات سایبری به‌منظور کشتار و آسیب‌رساندن و جاسوسی و تخریب و... استفاده می‌شود که باید هر کشور توان مقابله با این‌گونه تهدیدها را داشته باشد. جرم‌های ذکر شده، خواهان مقابله زودهنگام و پرقدرت است و برای گرفتن نتیجه مطلوب و کارآمد باید هر کشوری قوانین و نهادی برای رسیدگی به این‌گونه موضوعات و تهدیدها داشته باشد. کشور ما برای مقابله با تهدیدها و حملات سایبری مدل‌ها و نقشه‌های مختلفی را ارزیابی کرده است و از بین آنها بهترین‌ها را برگزیده و به کار گرفته است. قوانین کیفری در جمهوری اسلامی ایران برای همه جرایم سایبری برخوردهای قانونی و مطابق با اصول کشور تعیین شده است. مقابله با حملات سایبری نشان‌دهنده قدرت هر کشور است که چگونه و به چه شیوه‌ای بتواند این حملات را به نحو احسن کنترل و دفع کند. در مقاله پیشرو به ارزیابی سیستم سایبری کشور ایران و همچنین قوانین کیفری جرایم سایبری برای کنترل مشکلات فضای مجازی خواهیم پرداخت.

کلمات کلیدی: فضای سایبر، حملات سایبری، جرایم سایبری، قوانین کیفری.

۱ مقدمه

گسترش فناوری اطلاعات و ارتباطات و ظهور اینترنت باعث پیشرفت روزافزون بشر شده، به‌گونه‌ای که عصر حاضر را عصر اطلاعات نامیده‌اند. فناوری‌های اطلاعاتی و ارتباطاتی با سرعت زیادی در حال پیشرفت هستند و سایر فناوری‌ها را نیز تحت‌تأثیر قرار داده‌اند. ابتدا رشد فناوری اطلاعات و ارتباطات جدا از هم بوده؛ ولی در ادامه روند توسعه و سپس امتزاج این دو، باعث ظهور بزرگ‌ترین حوزه‌های ارتباط بشری (اینترنت) و سایر شبکه‌های ارتباطی گردید که جایگاه مناسبی برای نقل‌وانتقال اطلاعات را فراهم ساخت.

فضای سایبر تفاوت زیادی با سایر فضاها مانند هوا، جو، دریا و زمین دارد؛ ولی بیشتر قوانین فضای سایبر با فضاهای ذکر شده مشابه است. در عصر حاضر بخش عمده‌ای از تعاملات و فعالیت‌های اقتصادی، تجاری،

حاکمیتی و فرهنگی کشور در همه سطوح، شامل نهادهای دولتی، مؤسسات غیردولتی و نهادهای حاکمیتی، در فضای سایبر انجام می‌گیرد (رامک، ۱۳۹۴) [۳].

اطلاعات به‌عنوان یکی از دارایی‌های باارزش، نیازمند راهکار و نقشه‌هایی حفاظتی اصولی است. سه اصلی که در امنیت اطلاعات از اهمیت اساسی برخوردارند شامل صحت، محرمانگی و دردسترس‌بودن است. امنیت اطلاعات به‌وسیله کنترل مناسب حاصل خواهد شد. این کنترل‌ها به‌خاطر ایجاد امنیت بایستی اجرا شوند. نقش اطلاعات در امنیت ملی و خارجی در جمهوری اسلامی ایران انکارناپذیر است.

در طی سال‌های اخیر استفاده گسترده از فضای سایبری باعث شده تا این موضوع ضرورتی بیش‌ازپیش بیابد. تبادل اطلاعات در ارگان‌ها و سازمان‌های مختلف باعث شده است که دسترسی به اطلاعات در گروه اصلی اهداف سرویس‌های اطلاعاتی دشمنان قرار گیرد. هر گونه نفوذ و نشت اطلاعات، باعث تهدید برای نظام مقدس جمهوری اسلامی ایران به‌شمار می‌رود (قربانی و ثقفی، ۱۳۹۸، ص۲) [۲]. برقراری امنیت در فضای سایبری به‌خاطر ماهیت آن امری سخت و تحقق کامل آن در عمل دست‌نیافتنی به نظر می‌رسد، گرچه ضریب اطمینان نسبی از امن بودن سامانه‌ها و زیرسیستم‌ها قابل تحقق است. از فناوری سایبری بدون شک و تردید می‌توان برای نفوذ غیرمجاز به اطلاعات نهادهای مالی، حمل‌ونقل، انرژی و ... سوء استفاده نمود.

در جمهوری اسلامی ایران در حوزه قوانین و مقررات، وضع و تصویب قانون جرائم رایانه‌ای در سال ۱۳۸۸ و ابلاغ سند راهبردی افتا، ابلاغ سیاست‌های کلان در خصوص افتا و تشکیل شورای عالی فضای مجازی در در سنوات اخیر باعث شده تا پیشرفت دانش در حوزه‌های مختلف علی‌الخصوص امنیت فضای سایبری کشور پیشرفت و بهبود یابد.

با توجه به وجود تهدیدات مختلف فضای سایبر و وجود دارایی‌های اطلاعاتی، در برابر این تهدیدات، نیازمند شناخت چالش‌های این حوزه بوده و برای شناخت، نیازمند استخراج مؤلفه‌ها و شاخص‌های امنیت اطلاعات فضای سایبر در قالب یک مدل مفهومی کلان است. این مدل کمک می‌کند تا در ادامه بتوان یک روش امنیتی برای جلوگیری از دسترسی مهاجمین طراحی کرد.

۲ مبانی نظری

در این بخش به ارائه تعاریف و تبیین مفاهیم مورد بحث در مقاله حاضر در قالب متون و جداول پرداخته شده است.

۱.۲ مفهوم فضای سایبر

فضای سایبر یا فضای مجازی عبارتی است که در دنیای ارتباطات به این فضا نسبت داده شده، در رسانه و ارتباطات این واژه بسیار شنیده می‌شود. فضای سایبر اگرچه اصطلاحی جدید است؛ اما مفهوم آن جدید نیست و پیدایش این مفهوم هم زمان با پیدایش و اختراع تلفن توسط گراهام بل در سال ۱۸۷۶ بوده است. واژه سایبر اولین‌بار توسط ویلیام گیبسون در کتاب نئورامانسر که در آن فضای مذکور را به‌عنوان موطن داده‌ها و اطلاعات موجود در آن را در یک آینده دور و تاریک توصیف می‌کند، به کار برده شد. پس از آن واژه

مذکور در دنیا به‌طور فراوان مورداستفاده قرار گرفت (سوادکوهی و اسدی، ۱۴۰۱، ص۵) [۴].

۲.۲ فناوری‌های نوظهور فضای سایبر

فناوری‌های نو ظهور در فضای سایبر و روندهای فناورانه‌ای که امروزه در قالب انقلاب صنعتی چهارم اروپا و تصویرسازی آینده اغلب کشورها وجود دارد، باعث گردیده این فناوری‌ها در محیط آشوبناک و سرشار از عدم قطعیت فضای سایبر نقش بی‌بدیلی داشته و این موضوع مقوله امنیت سایبری را تحت تأثیر خود قرار دهد؛ بر این اساس فناوری‌هایی نظیر بلاک‌چین، سامانه‌های سایبرفیزیکی، هوش مصنوعی و رباتیک، اینترنت اشیا، پردازش کوانتومی، کلان داده‌ها و غیره، مقوله‌هایی نظیر مالکیت داده، حریم خصوصی، بحران‌سازی و جریان‌سازی‌های سیاسی-امنیتی، مالکیت معنوی و غیره را تحت تأثیر خود قرار داده و بر این اساس ضروری است، چالش‌هایی نظیر فقدان راهبرد کلان و فرابخشی در این حوزه، عدم چابکی و کارآمدی ساختاری در فرایندهای تصمیم‌گیری، اجرا و نظارت بر عملکرد، عملکرد جزیره‌ای و مجزا از یکدیگر نهادهای تصمیم‌گیر، مقررات‌گذار و بهره‌بردار مرتبط، فقدان یک رابطه پیوسته میان صنعت و نهادهای تحقیقاتی و دانشگاهی، ضعف ارتباط شرکت‌های داخلی توانمند در حوزه الکترونیک، مخابرات و نرم افزار با شرکت‌های معتبر بین‌المللی، کندی روند صنعتی شدن و استفاده از فناوری‌ها در محیط کسب و کار کشور، انفعال در عرصه بین‌الملل به دلیل عدم استفاده از فرصت‌های بین‌الملل به ویژه در ارتباط با بهره گیری از ظرفیت بازار و انتقال فناوری کشورهای همسو، تغییر فرهنگ و سبک زندگی ایرانی-اسلامی آحاد ملت، افزایش مواجهه کاربران ایرانی با محتواهای ضد فرهنگی، از دست دادن باورهای اعتقادی در مواجهه کاربران با جریان سازی‌های معاند اعتقادات و نهایتاً خروج اطلاعات کاربران به رسانه‌های اجتماعی خارجی و بهره برداری بیگانگان از ذائقه ایرانی، مورد توجه جدی قرار گرفته و ضمن بهره برداری از این فناوری‌ها در امنیت سایبری، از آسیب‌های عنوان‌شده نیز جلوگیری شود (همان، ص۹۳) [۷].

۳.۲ مفهوم جرم سایبری

تا کنون تعاریف گوناگونی از جرم رایانه‌ای از سوی سازمان‌های بین‌المللی، قانون‌گذران و مراجع رسمی و غیررسمی برخی کشورها ارائه شده است؛ که وجود تفاوت و گاه تعاریف در آن‌ها بیانگر ابهامات موجود در ماهیت و تعریف این جرائم می‌باشد. لیکن هنوز یك تعریف کلی و اجماعی برای جرائم رایانه‌ای به دست نیامده و به جای آن تعاریف کاربردی در این زمینه ارائه شده است. عمل غیرقانونی جهت از بین بردن، تغییر، حذف و یا دسترسی به اطلاعات ذخیره شده در حافظه کامپیوتر یا فضای انتقال آن‌ها. با توجه به تعریف و گستره فضای سایبر و با در نظر گرفتن اصل قانونی بودن جرم از طرف دیگر می‌توان چنین تعریفی را از جرم سایبری ارائه داد که به مقصود نزدیک‌تر است. «هر فعل یا ترک فعلی که در فضای سایبر اتفاق افتاده و قانون آن را جرم شناخته و برای آن مجازات مشخص کرده باشد». با این تعریف، جرائم علیه سخت افزار کامپیوتر نظیر سرقت یا تخریب مانیتور از شمول جرائم سایبری خارج می‌گردد (سوادکوهی و اسدی، ۱۴۰۱، ص۵) [۴].

۴.۲ کلاهبرداری سایبری

کلاهبرداری سایبری به لحاظ خلاقیت مرتکب آن و سهولت ارتکاب مهم‌ترین و شایع‌ترین جرم اقتصادی فضای سایبر محسوب می شود؛ هر چند به ظاهر در ارتکاب این جرم، رایانه و فضای سایبر در حد وسیله جرم ظاهر می‌شود؛ اما رایانه و فضای سایبر، کلاهبرداری را توأم با کیفیت و شرایط غیرقابل انکاری می‌کند که مقنن ناگزیر به شناسایی جرم جدید در کنار کلاهبرداری سنتی شده است؛ ماده ۶۷ قانون تجارت الکترونیکی و ماده ۷۴۱ قانون مجازات اسلامی بخش تعزیرات؛ رکن قانونی جرم کلاهبرداری سایبری را تشکیل می‌دهند و رفتار مجرمانه در رکن مادی این جرایم شامل ورود، تغییر، محو و مختل کردن و دستکاری غیرمجاز سیستم خواهد بود و موضوع آن‌ها مال متعلق به دیگری و نتیجه آن‌ها محروم ساختن مال باخته از مال خود است؛ از طرفی کلاهبرداری سایبری جرمی عمدی، آنی و مقید است و برای تحقق آن وجود سوء نیت عام (یعنی عمد در ارتکاب یکی از اعمال فیزیکی مذکور در ماده ۷۴۱ قانون مجازات اسلامی بخش تعزیرات) و سوء نیت خاص (یعنی قصد تحصیل وجه، مال، منفعت، خدمات یا امتیازات مالی) هم برای تحقق عنصر روانی جرم کلاهبرداری سایبری ضروری است.

کلاهبرداری سایبری جزء جرائمی می‌باشد که نظر بسیاری از بزهکاران را به خود جلب نموده است و نیاز به برخورد قاطع از سوی مراجع ذی ربط دارد؛ کلاهبرداران با ارسال ایمیل و پیامک به اشخاص مختلف، آن‌ها را به انحای مختلف به پای دستگاه‌های بانک‌ها می‌کشانند و اقدام به کلاهبرداری می نمایند و با وجود انواع کلاهبرداری اینترنتی خودپرداز مانند فیشینگ، ارسال ایمیل یا نفوذ به ایمیل باکس افراد و ارائه شماره حساب‌های جعلی در معاملات و استفاده از اسکیمرها در دستگاه‌های خودپرداز بانک‌ها برای سوء استفاده از کارت‌های عابر بانک و با وجود افزایش این نوع کلاهبرداری‌ها، سیستم‌های امنیتی و حفاظتی بانک‌ها در این زمینه بسیار ضعیف عمل می‌نمایند؛ از این رو با استانداردسازی و تجهیز وسائل ارتباطی می توان از این قبیل جرائم پیشگیری کرد (اجاقلو و زندی، ۱۴۰۰، ص۲۵۰) [۱].

۵.۲ تعیین محل ارتکاب جرم در فضای سایبر در قوانین کیفری

در بحث رسیدگی به جرائم سایبری، مهم‌ترین مانع موجود محل وقوع جرم است. موقعیت شبکه رایانه‌ای و محیط سایبری آن چنان به موقعیت جغرافیایی بی‌ربط است که اغلب تعیین مکان فیزیکی یک منبع یا کاربر اینترنتی ناممکن است. ازآنجا که اطلاع از این موقعیت مکانی برای عملکرد شبکه و اهداف ایجاد کنندگان آن اهمیتی ندارد؛ لذا اغلب در طراحی یک شبکه امکان تشخیص مکان جغرافیایی لحاظ نمی‌شود. در جرائم سنتی عواملی که بر تعیین مکان وقوع جرم اثر می‌گذارند، بسته به محل شروع به جرم، محل استقرا مجرم، محل وقوع نتیجه محل وجود ادله و محل کشف جرم و غیره تفاوت دارند؛ درحالی که در جرائم سایبری به خاطر مجازی و دیجیتالی بودن محل ارتکاب و همچنین گستردگی شبکه رایانه‌ای و مخابراتی و تعدد عوامل مختلف در خصوص مکان به صورت یک چالش نمود پیدا می‌کند. اگرچه سایت‌های اینترنتی آدرس دارند ولی این آدرس جایگاه آن‌ها را در شبکه مشخص می‌کند نه مکان و موقعیت حقیقی آن‌ها را (سوادکوهی و اسدی، ۱۴۰۱، ص۴۰۳) [۴].

۶.۲ محل استقرار مرتکب جرم در فضای سایبر و هویت او

تعیین محل استقرار مرتکب جرم در فضای سایبر، فضای غیر ملموس و از طرف دیگر فضایی گسترده و فرامرزی است و همچنین به لحاظ حرفه‌ای و متخصص بودن مرتکبین جرائم در فضای سایبر، غالباً اشخاص مرتکب جرائم به سادگی طعمه‌های خود را شکار میکنند و با استفاده از ترفندها و شیوه‌های تغییر هویت ویژه سعی در ناشناخته ماندن خود میکنند. ازآنجا که از جمله اصول تعیین دادگاه صالح، صلاحیت مبتنی بر تابعیت مرتکب و یا صلاحیت دادگاه محل استقرار مرتکب می‌باشد، جهت تشخیص دادگاه صالح بنابر یکی از این اصول لازم می آید تشخیص داده شود که مرتکب جرم مورد نظر چه کسی است و دارای تابعیت کدام دولت می باشد و یا اینکه مرتکب جرم در کدام نقطه از جهان قرار دارد (همان، ص۴۰۴) [۷].

۷.۲ ضابطه سیستم دولت در برخورد با تبعه خود

مبنای اصلی این قاعده تابعیت مرتکبین جرائم است. در قواعد سنتی به این قاعده صلاحیت شخصی یا تابعیتی گفته می‌شود در این قاعده یک کشور براساس يك معیار مورد قبول خود قوانین و مقرراتی را وضع میکند و به تبع آن انتظار دارد این قوانین از سوی تبعه خود صرف نظر از محل استقرار و یا اقامتش رعایت شود. بنابر این در این قاعده بحث قلمرو سرزمینی و محدودیت‌های فیزیکی ناشی از آن مطرح نیست بلکه هرکس از تابعیت به مفهوم حقوقی آن برخوردار باشد تحت صلاحیت محاکم کیفری خود قرار می‌گیرد (همان، ص۴۰۴) [۷].

۸.۲ ضابطه تقدم در تعقیب نسبت به جرائم با خطر جهانی

ارتکاب جرم مشمول صلاحیت جهانی در فضای سایبر نه تنها بر قابلیت اجرایی آن تأثیر منفی نگذاشته است بلکه به لحاظ ویژگی‌های خاص چنین جرمی از جمله سهولت در ارتکاب فراملی بودن، گسترده بودن و سبقه جهانی داشتن آن و نیز حفظ نظم و انسجام جهانی اقتضا می‌کند که تعقیب آن در سریع‌ترین و راحت‌ترین شکل تدابیر کیفری لازم صورت گیرد. به نظر می‌رسد، قاعده صلاحیت جهانی نسبت به چنین جرائمی که در فضای سایبر اتفاق میافتد قابلیت اجرایی جدی‌تر و بیشتری پیدا می‌کند. با این حال تاکنون در فضای سایبر نسبت به برخی جرائم نظیر هرزه‌نگاری کودکان این اجماع و توافق به‌طور نسبی محقق شده ولی هنوز قدرت اجرایی چندانی پیدا نکرده است.

در قانون جرائم رایانه‌ای جمهوری اسلامی ایران مصوب خرداد ۱۳۸۸ در همین راستا و با قبول جرم هرزه‌نگاری کودکان به‌عنوان جرم بین‌المللی مشمول صلاحیت جهانی در ماده ۲۸ مقرر شده است که علاوه بر موارد پیش‌بینی شده در دیگر قوانین دادگاه‌های ایران نیز صالح به رسیدگی خواهند بود. همچنین جرم نفوذ غیر مجاز که مادر جرائم سایبری محسوب می‌شود به‌عنوان یک جرم موضوع صلاحیت جهانی مورد توجه قرار گرفته؛ ولی هنوز به عنوان یک جرم جهانی محض پذیرفته نشده است؛ البته جرائم دیگری نظیر انتشار ویروس در برخی موارد و پول‌شویی الکترونیکی به‌عنوان جرم جهانی مورد توجه کشورهای متعدد قرار گرفته است (همان، ص۴۰۵) [۷].

۹.۲ قوانین کیفری جمهوری اسلامی ایران در ارتباط با فضای سایبر

برخی از نظریه پردازان علم حقوق بر این عقیده هستند که برای موضوعات و مقوله‌های جدیدی همچون فضای سایبر نیازی به قانون‌گذاری جدید نیست و می‌توان با تعمیم قوانین سنتی به آن نیاز را بر طرف نمود؛ اما واقعیت آن است که علی رغم اشتراکات فضای سایبر با زندگی عادی بشر، این فضا به‌گونه‌ای خصوصیات متمایزی دارد که هیچ نظام حقوقی پاسخگوی صددرصدی نیازهای آن نیست و بر همین اساس با احساس این خلاء قانونی، نقطه عطف و کانونی ساماندهی و وضع قانونی مدون جهت رسیدگی به جرائم مرتبط با رایانه و فضای سایبر در جمهوری اسلامی ایران، تصویب «قانون جرائم رایانه‌ای» در سال ۱۳۸۸ در قالب ۵۶ ماده توسط مجلس شورای اسلامی شد. طی این قانون مجازات‌هایی شامل حبس یا جریمه نقدی یا هر دو برای مرتکبین جرائم ذکر شده، پیش‌بینی شده است. برخی از جرایم در نظر گرفته شده در این قانون شامل «دسترسی غیرمجاز»، «شنود غیرمجاز»، «جاسوسی رایانه‌ای»، «جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی»، «جعل رایانه‌ای»، «تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانه داده به آن‌ها»، «تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی»، «سرقت و کلاهبرداری مرتبط با رایانه»، «جرائم علیه عفت و اخلاق عمومی»، «هتک حیثیت و نشر اکاذیب» است.

۱۰.۲ امنیت فضای سایبر در جمهوری اسلامی ایران

مدیریت امنیت که خود بخشی از امنیت است وظیفه تعیین اهداف امنیت و بررسی موانعی که سر راه رسیدن به این اهداف هستند و همچنین ارائه راهکارهای لازم و کنترل عملکرد سیستم امنیت سازمان را بر عهده داشته‌اند و در نهایت باید تلاش کنند تا سیستم را همیشه به‌روز نگه دارند.

هدف مدیریت امنیت اطلاعات حفظ امنیت نرم‌افزاری، سخت‌افزاری، ارتباطی، نیروی انسانی و غیره در مقابل هر تهدید مانند خطراتی است که از طرف افرادی غیرمجاز ایجاد شده است و برای اینکه به هدف امنیت دست یابیم، نیازمند یک هدف منسجم هستیم. سیستم مدیریت امنیت اطلاعات راهکارهایی برای رسیدن به این اهداف امنیتی دارد. اولین استاندارد مدیریت امنیت که در سال ۱۹۹۵ شکل گرفت، بر طبق این نگرش تأمین امنیت فضای سایبر مقدور نیست و این چرخه امنیت سازی باید طی یک چرخه‌ای که شامل مراحل طراحی، ارزیابی، اصلاح، پیاده‌سازی انجام گیرد (قربانی و ثقفی، ۱۳۹۸، ص ۳۲۱) [۲].

۱۱.۲ اسناد بالادستی در فضای سایبر جمهوری اسلامی ایران

با توجه به روند فزاینده توسعه علم و فناوری در جمهوری اسلامی ایران و همچنین شکل‌گیری انواع تهدیدات و چالش‌های بدیع در فضای سایبر، لازم است اقداماتی اصولی تدبیر شود، تا به ارگان‌های مختلف و بنیاد جامعه خطرات کمتری برسد، بر همین اساس یکی از ارکان که در انتظام ساختار حاکمیتی جمهوری اسلامی ایران تاثیر بسزایی دارد، اسناد بالادستی نظیر سیاست‌های کلی نظام، قوانین و مقررات مصوب مجلس و مصوبات هیئت وزیران است؛ زیرا کلیه قوانین و آیین‌نامه‌هایی که به فضای مجازی مربوط می‌شود در داخل این اسناد تجزیه و تحلیل شده و ثبت گردیده‌اند، این اسناد نقشه راه امنیتی مناسبی جهت جلوگیری از تهدیدات پیش

روی استفاده‌کنندگان قرار می‌دهد (قربانی و ثقفی، ۱۳۹۸، ص۳۲۲) [۲].

۱۲.۲ نمونه‌ای از مهاجم سایبری

در اواخر ژانویه ۲۰۱۴، یک مدیر سیستم در آنتهم[1] که در آن زمان یکی از بزرگ‌ترین ارائه‌دهندگان بیمه سلامت در جهان بود، به کشف نگران‌کننده‌ای دست یافت. شب قبل، شخصی از حساب خود برای اجرای چندین پرس‌وجو برای جمع‌آوری داده‌های حساس مشتری از سرورهای آنتهم استفاده کرده بود. با انجام این کار، مهاجم «اطلاعات شناسایی شخصی»[2] مرتبط با نزدیک به ۸۰ میلیون بیمار آنتهم را به سرقت برده بود. در سال ۲۰۱۵، سرویس‌دهندگان امنیت سایبری ترندمیکرو[3] و سیمانتک[4] مهاجم را موسوم به "Black Vine" شناسایی کردند؛ که گمان می‌رود از کشوری در جنوب شرقی آسیا نشأت گرفته باشد. علاوه بر این، تحقیقات سرویس‌دهندگان نشان داد؛ که این عملیات، همان‌طور که اکثر افراد تصور می‌کردند، صرفاً به‌دست آوردن سود مالی نبود، بلکه گامی در یک عملیات جاسوسی در مقیاس بزرگ بود. چهار سال بعد، زمانی که کیفرخواست فدرالی ایالات متحده آمریکا، چندین هکر چینی را به مشارکت در عملیات علیه آنتهم متهم کرد، اطلاعات بیشتری در دسترس قرار گرفت. کیفرخواست ادعا می‌کرد که مهاجمان برنامه‌ای را هدف قرار داده‌اند که مسئول انجام تحقیقات پیشینه برای شهروندان آمریکایی هستند (Jon DiMaggio, 2022, p.11) [۶].

۱۳.۲ مؤلفه‌های ارزیابی امنیت سایبری

به منظور استخراج مولفه‌های امنیت سایبری، مضامین مرتبط با امنیت سایبری، با مطالعه‌ی برخی مبانی نظری مرتبط با مقاله و تحلیل کیفی تدابیر و رهنمودهای مقام معظم رهبری (مدظله‌العالی) و اسناد بالا دستی شامل حکم انتصاب دوره‌ی اول و دوم اعضای جدید شورای عالی فضای مجازی، ابلاغ سیاست‌های کلی به مجمع در حوزه خودکفایی دفاعی و امنیتی، سیاست‌های کلی برنامه توسعه و پیشرفت کشور، سیاست‌های کلی نظام در بخش افتا، اهداف و سیاست‌های مرکز ملی فضای مجازی، سند راهبردی پدافند سایبری کشور و مطالعه‌ی تطبیقی امنیت سایبری در سطح منطقه و جهان و سپس با روش خوشه بندی و بر اساس فراوانی تکرار واژه‌ها، مولفه‌های اصلی مورد بازشناسی اولیه قرار گرفتند و نتایج در جدول ۱ ارائه شده‌اند.

[1] Anthem
[2] PII
[3] Trend Micro
[4] Symantec

جدول ۱: ابعاد و مؤلفه‌های ارزیابی امنیت سایبری (کریمی و همکاران، ۱۴۰۱، ص۹۰) [۵]

ابعاد	مؤلفه‌ها
حکمرانی	سیاست‌گذاری، راهبرد، هماهنگ‌سازی، نظارت و ارزیابی، دیپلماسی
حقوقی و قانونی	قانون‌گذاری، مقررات‌گذاری، نظارت
توانمندسازها و ظرفیت‌سازی	تحقیق و توسعه، استانداردها، نیروی انسانی، سازماندهی، مشارکت علم و نوآوری، بودجه و اعتبارات
دفاعی - امنیتی	زیرساخت‌های حیاتی، سایبری انتظامی، سایبری دفاعی، رصد و پایش، پاسخ به رویدادها
اجتماعی - فرهنگی	فرهنگ امنیت سایبری، محتوای بومی، رسانه‌های اجتماعی، اقتصاد و تجارت دیجیتال، حریم خصوصی

۱۴.۲ ذی‌نفعان فضای سایبر جمهوری اسلامی ایران

با توجه به اینکه مقرر است مدل ارائه شده در مقاله حاضر به منظور ارزیابی امنیت سایبری جمهوری اسلامی ایران پیشنهاد شود، در گام بعد ذی‌نفعان امنیت فضای سایبر ملی به تفکیک لایه‌های فضای سایبر و نیز بر اساس ابعاد مدل ارائه شده در مقاله حاضر با اقتباس از سند راهبردی افتا استخراج و مطابق با مندرجات جدول ۲ و جدول ۳ ارائه می‌گردند.

جدول ۲: ذی‌نفعان مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران (همان، ص۹۱) [۷]

ابعاد	ذی‌نفعان
حکمرانی	نهاد رهبری، هیئت دولت، مجلس شورای اسلامی، مجمع تشخیص مصلحت نظام، شورای عالی فضای مجازی کشور، ستاد کل نیروهای مسلح، وزارت ارتباطات و فناوری اطلاعات، مرکز افتا ریاست جمهوری، سازمان پدافند غیرعامل، سازمان برنامه و بودجه، وزارت اطلاعات، وزارت دفاع و پشتیبانی نیروهای مسلح
حقوقی و قانونی	هیئت دولت، مجلس شورای اسلامی، قوه قضائیه، دستگاه‌های نظارتی نظیر سازمان بازرسی کل کشور، وزارت ارتباطات و فناوری اطلاعات، مرکز افتا ریاست جمهوری، سازمان برنامه و بودجه، سازمان تنظیم مقررات و ارتباطات رادیویی
توانمندسازها و ظرفیت‌سازی	سازمان صدا و سیما، وزارت ارتباطات و فناوری اطلاعات، مرکز افتا ریاست جمهوری، پارک های علم و فناوری، موسسه آموزشی تحقیقاتی، وزارت علوم، تحقیقات و فناوری، نیروهای مسلح، دانشگاه‌ها و مراکز علمی و پژوهشی کشور، سازمان ملی استاندارد
دفاعی - امنیتی	وزارت اطلاعات، سازمان پدافند غیرعامل، وزارت ارتباطات و فناوری اطلاعات، وزارت دفاع و پشتیبانی نیروهای مسلح، پلیس فتا، وزارت کشور
اجتماعی - فرهنگی	سازمان صدا و سیما، سازمان پدافند غیر عامل، وزارت علوم، تحقیقات و فناوری، سازمان ثبت اسناد و املاک کشور، وزارت صنعت، معدن و تجارت، سازمان تبلیغات اسلامی، وزارت ورزش و جوانان، بانک مرکزی، وزارت فرهنگ و ارشاد اسلامی، سازمان تبلیغات اسلامی
بین‌المللی	وزارت امور خارجه، معاونت حقوقی ریاست جمهوری، وزارت ارتباطات و فناوری اطلاعات

جدول ۳: ذی‌نفعان امنیت فضای سایبر ملی به تفکیک لایه‌های فضای سایبر

لایه‌ها	نقش ذی‌نفعان	ذی‌نفعان
حکمرانی	تعیین خط مشی‌ها، رویه‌ها، قوانین و مقررات، استانداردها، طرح‌ها و برنامه‌ها، راهبردها، تحقیق و توسعه	نهاد رهبری، وزارت ارتباطات و فناوری اطلاعات، هیئت دولت، سازمان برنامه و بودجه، مجلس شورای اسلامی، وزارت دفاع و پشتیبانی، ستاد کل نیروهای مسلح، وزارت اطلاعات، قوه قضائیه، مجمع تشخیص مصلحت نظام، سازمان ملی استاندارد، شورای عالی فضای مجازی
کاربر	ارتقاء سطح آگاهی، دانش و مهارت‌های مرتبط با امنیت سایبر	بانک مرکزی، وزارت ارتباطات و فناوری اطلاعات، وزارت علوم، تحقیقات و فناوری، صدا و سیما، وزارت دفاع و پشتیبانی نیروهای مسلح
محتوا	تامین امنیت و جلوگیری از مخاطرات ناشی از محتوا	وزارت فرهنگ و ارشاد اسلامی، وزارت علوم، تحقیقات و فناوری، سازمان ثبت اسناد و املاک کشور، وزارت اطلاعات، وزارت ورزش و جوانان، حوزه علمیه قم، وزارت دادگستری
خدمات	تقویت صنعت و توسعه خدمات و محصولات امنیت فضای سایبر	وزارت صنعت، معدن و تجارت، وزارت ارتباطات و فناوری اطلاعات، مراکز علمی و پژوهشی کشور، وزارت فرهنگ و ارشاد اسلامی
زیر ساخت	مصون‌سازی زیرساخت‌های امنیتی کشور در قبال حملات الکترونیکی	وزارت اطلاعات، دستگاه‌های اجرائی، وزارت ارتباطات و فناوری اطلاعات، وزارت کشور، سازمان پدافند غیرعامل

۱۵.۲ شاخص‌های امنیت سایبری ملی در آکادمی حکمرانی

شاخص‌های امنیت سایبری یک فهرست ۱۲گانه جهانی است؛ که آمادگی کشورهای مختلف را از لحاظ مدیریت تهدیدات سایبری اندازه‌گیری می‌کند (جدول ۴). آکادمی حکمرانی خود یک ساختار دانش‌بنیان و مشاوره‌ای دارد و شامل فهرست ۱۰۰ کشور است، آکادمی مذکور بهترین تجربیات را در حیطه مدیریت الکترونیکی، دموکراسی الکترونیکی در اختیار استفاده‌کنندگان قرار می‌دهد (همان، ص۸۳) [۷].

۳ نتیجه‌گیری

فضای سایبر با ماهیت بی حد و مرز خود و حضور بازیگران متکثر که امروزه تلفیقی از انسان و ماشین شده‌اند از سراسر جهان که بعلاوه یک نظام سیاستی، کنترلی، حقوقی، قضائی و کیفری واحد و یکسان نیز بر آن جاری و ساری نیست و از سویی روش‌های پنهان‌کاری و پیچیده جرائم و روند فزاینده آن و نیز فقدان اجماع بین‌المللی بر قوانین واحد موجب شده کشورها، علی‌الخصوص کاربران ایرانی با انواع تهدیدات و چالش‌ها در فضای سایبر چه از منشا داخل کشور و چه خارج از کشور مواجه گردند که با توسعه و افزایش ضریب نفوذ این فضا در آینده، قطعاً این مخاطره دوچندان خواهد شد؛ در نتیجه حاکمیت به عنوان متولی سیاست‌گذاری و تنظیم‌گری این فضا شایسته است علاج واقعه پیش از وقوع نماید؛ زیرا مجرمین و بدخواهان مترصد مورد حمله قراردادن بنیاد و زیرساخت‌های کشور و نیز دارائی‌های سایبری آحاد شهروندان ایرانی هستند.

جدول ۴: شاخص امنیت سایبری ملی در آکادمی حکمرانی

ردیف	شاخص
۱	سیاست امنیت سایبری
۲	اعتماد الکترونیکی
۳	تحلیل تهدیدات سایبری
۴	واکنش به حوادث سایبری
۵	محافظت از اطلاعات شخصی
۶	آموزش امنیت سایبری
۷	مدیریت بحران سایبری
۸	مشارکت در امنیت سایبری جهانی
۹	حمایت از خدمات دیجیتال
۱۰	پلیس مبارزه با خرابکاری‌های سایبری
۱۱	عملیات سایبری نظامی
۱۲	حمایت از خدمات حیاتی

مراجع

[۱] اوجاقلو، صالح، زندی، محمدرضا، بهار ۱۴۰۰، پیشگیری از کلاهبرداری سایبری در سیاست جنایی ایران با نگاهی به رویه قضایی.

[۲] قربانی، ولی اله، ثقفی، کامیار، پاییز ۱۳۹۸، ارائه‌ی مدل مفهومی کلان امنیت اطلاعات فضای سایبر ج.ا.ا.

[۳] رامک، مهراب، امیرلی، حسین، قربانی، ولی‌اله، حقی، مجید، ۱۳۹۴، طراحی نظام دفاع سایبری، مطالعه گروهی، دانشکده امنیت ملی، دانشگاه عالی دفاع ملی.

[۴] سوادکوهی، صالح، اسدی، زهرا، زمستان ۱۴۰۱، سیاست کیفری ایران در مقابل جرائم سایبری.

[۵] کریمی، محمدرضا، محمدی، حافظ، سعادتمند، امیر مسعود، پاییز ۱۴۰۱، ارائه مدلی برای ارزیابی امنیت سایبری ج.ا.ا.

[6] DiMaggio, J. (2022). The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime. No Starch Press.

[7] Criminal policy of the Islamic Republic of Iran against cyber crimes and its security assessment