آینده‌پژوهی دفاعی، سال سوم، شماره ۱۰، پائیز ۱۳۹۷

تاریخ دریافت: ۱۳۹۷/۰۹/۱۰ تاریخ پذیرش: ۱۳۹۷/۱۱/۲۳

از صفحه ۱۰۳ تا صفحه ۱۲۰

ارائه الگوی امنیت در فضای سایبر جمهوری اسلامی ایران با رویکرد آینده‌پژوهانه

امیرحسین مقدسی لیچاهی*[۱]

حمید همت[۲]

چکیده

مقابله با تهدیدات سایبری به‌منظور از بین بردن و محو کامل آن‌ها، امری غیرممکن است. ازاین‌رو هدف اصلی این پژوهش واکاوی درک اجتماع علمی از وضعیت فعلی فضای سایبر کشور و ارائه مدلی برای ارتقای امنیت در فضای مزبور می‌باشد. این پژوهش، ازنظر هدف، از نوع پژوهش‌های توسعه‌ای و به لحاظ رویکرد از نوع تحقیقات کیفی است که با پایش محیطی اطلاعات مرتبط با موضوع شناسایی شد و با استفاده از روش تئوری داده‌بنیاد در چارچوب الگو ارائه گردید. منبع اصلی گردآوری داده‌های این پژوهش، اسناد و مدارک در دسترس (کتاب‌ها، مطالعات پیشین و مطالب مطروحه در نشست‌ها و همایش‌های مرتبط) بوده است. به‌منظور بررسی روایی و پایایی مدل به‌دست‌آمده از گروه‌های کانونی و شاخص کاپا استفاده گردید. نتایج پژوهش حاکی از آن است که به دلیل اثرگذاری و گستردگی زیاد و سهولت و سادگی کاربرد و تنوع ابزارها و روش‌ها، وقوع تهدید سایبری قطعی است و بایستی با فرهنگ‌سازی، توسعه زیرساخت‌ها، رعایت پدافند غیرعامل سایبری، تدابیر فنی و امنیت فیزیکی و تدابیر مدیریتی یک تغییر بنیادین واقعی در فضای سایبر کشور ایجاد گردد.

واژه‌های کلیدی:

سایبر، فضای سایبر، امنیت در فضای سایبر، پایش محیطی.

[۱]. کارشناسی ارشد مؤسسه آموزشی-پژوهشی مجازی تدبیر

[۲]. عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا

* نویسنده مسئول Email:a.h.moghadasi4667@gmail.com

مقدمه

امروزه با گسترش بدون مرز ساخت‌های الکترونیک در دنیا و متعاقب آن در تمامی ارگان‌ها، بعد جدیدی به سایر ابعاد زندگی ما اضافه‌شده که همان بعد مجازی (سایبر) است. این بعد جدید تعاریف و ویژگی‌های مختص به خود را دارد و لازم است که با توجه به ماهیت بسیار پویا و متغیر آن، نگاه متفاوتی به مفاهیمی همچون تدوین و اجرای راهبرد و یا مدیریت راهبردی در آن حوزه داشته باشیم، زیرا نوع تهدیدها و ویژگی‌هایی که در این فضا انسان‌ها، جوامع و زیرساخت‌های هر نهادی را هدف قرار می‌دهند نیز با تهدیدهای روزمره دیگر بسیار تفاوت دارد. در افق ۱۴۰۴ جامعه امن به‌گونه‌ای نوید داده‌شده، که در همه بخش‌های آن، تهدید یا خطری در میان نباشد. ازاین‌رو در سند چشم‌انداز بیست‌ساله، امنیت یکی از مفاهیم کلیدی است. امنیت، استقلال و اقتدار به‌عنوان سه ویژگی برجسته نظام جمهوری اسلامی ایران است که هر سه پیوند تنگاتنگی با امنیت سایبری دارند. ازاین‌رو در سیاست‌های کلی نظام در امور «امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)» پایش، پیشگیری، دفاع و ارتقاء توان بازدارندگی در مقابل هرگونه تهدید در حوزه فناوری اطلاعات و ارتباطات (بند ۵ سند) مورد تأکید قرارگرفته است (سایت دفتر حفظ و نشر آثار حضرت آیت‌الله خامنه‌ای).

در شرایطی که حمله سایبری از دیدگاه برخی از کشورها از قبیل رژیم اشغالگر اسرائیل به‌عنوان حمله نظامی تلقی و زمینه‌های جدی جنگ‌های فیزیکی نظامی را فراهم خواهد نمود و در این مبنا نیز مراکز دفاع سایبری پیشرفته‌ای را راه‌اندازی نموده‌اند، به‌روشنی می‌توان دریافت که جنگی جدی در فضای سایبر در حال شکل‌گیری است، جنگی که به‌شدت زیرساخت‌های سایبری و غیر سایبری کشور را در تمامی ابعاد تهدید می‌کند. ازاین‌رو اهمیت دفاع سایبر با نگاه راهبردی بیش از هر موضوع دیگری خودنمایی می‌کند (آذر و مسلمی، ۱۳۹۷). برخی از سوابق موضوع تحت پژوهش در حوزه سیاست‌های بین‌المللی در فضای سایبری و برخی از تلاش‌های مهم صورت گرفته در سازمان‌ها و مجامع جهانی که ناظر بر "هنجارهای رفتار مسئولانه دولت‌ها در فضای سایبری" می‌باشند شامل کنوانسیون بوداپست (۲۰۰۴)، تلاش‌های علمی گروه خبرگان حکمرانی سازمان ملل متحد[1]، سند راهبرد بین‌المللی ایالات‌متحده برای فضای سایبری (۲۰۱۱)، یافته‌های موسسه مطالعات امنیتی شرق و غرب[2] (۲۰۱۱)، مطالعات تطبیقی کنوانسیون‌های لاهه و ژنو در حوزه موردبحث، دستورالعمل تدوین‌شده در سازمان پیمان آتلانتیک شمالی(ناتو) تحت

[1]. UNGGE2010
[2]. EastWest Institute (EWI)

عنوان "تالین ۲۰۱۳"، طرح بلوک چین و روسیه با عنوان "کدهای رفتاری بین‌المللی برای امنیت اطلاعات" در سال (۲۰۱۵)، استراتژی وزارت امور خارجه امریکا در حوزه سیاست‌های بین‌المللی در سال (۲۰۱۶)، اعلامیه گروه ۷ در خصوص "رفتار مسئولانه دولت‌ها در فضای سایبری" در ایتالیا در سال (۲۰۱۷)، فرمان اجرایی ترامپ در حوزه تقویت امنیت سایبری شبکه‌ها و زیرساخت‌های فدرال در سال (۲۰۱۷)، بیانگر اهمیت و ضرورت پرداختن به موضوع می‌باشد (سایت مرکز ملی فضای مجازی، ۱۳۹۷).

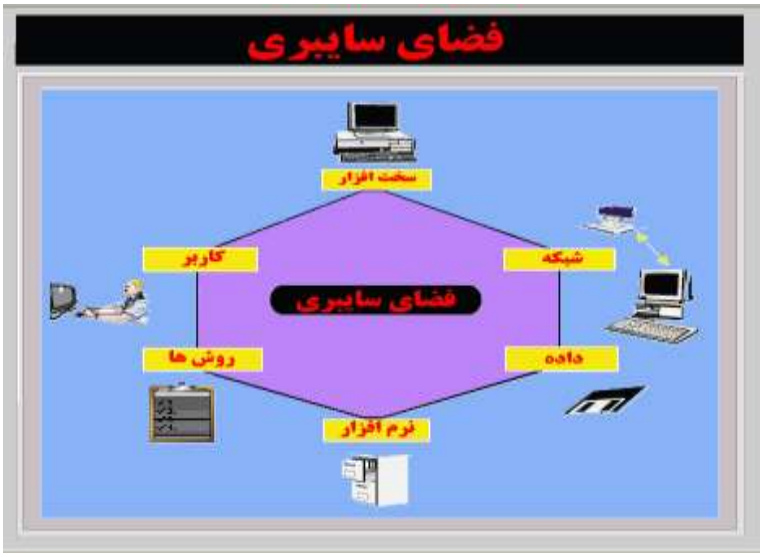
امروزه گسترش فضای سایبر باعث پیدایش مرزهای مجازی شده و از این‌جهت درک واقع بینانه از تهدیدات امنیتی درگرو توجه به عوامل نرم‌افزاری است که درواقع حلقه واسط بین محیط امنیتی کشورها و سخت‌افزارها قرار دارند و بدین‌جهت برداشت‌ها از مفهوم امنیت ملی در این فضا به چالش کشیده شده است. یکی از محورهای اصلی تهدید امنیتی در عصر ارتباطات و جهانی‌شدن برای کشورها را باید در حوزه سایبری دانست که نمونه بارز آن حمله رایانه‌ای به تأسیسات هسته‌ای و الکترونیکی ج.ا.ا توسط آمریکا می‌باشد. جهانی‌شدن که یکی از ابزارهای آن، فناوری‌های سایبری می‌باشد، در کنار فرصت‌های بی‌شماری که برای کشورها ایجاد می‌کند، یک تهدید بسیار جدی است که عمدتاً خیلی به‌صورت جدی به آن پرداخته نمی‌شود و یا به‌صورت موردی و تک‌بعدی بررسی می‌گردد، لذا نیاز است این موضوع به‌طور مشخص و کلی بررسی و شاخص‌ها، مؤلفه‌ها و ابعاد آن مشخص گردد تا بتوان متناسب با آن اقدامات لازم را به عمل آورد.

امروزه جمهوری اسلامی ایران جزء کشورهایی است که بیشترین حملات تروریستی سایبری به زیرساخت‌های مالی، هسته‌ای و نظامی خود را متحمل می‌شود. به ثمر نشستن هرکدام از این حملات می‌تواند نتایج فاجعه باری برای امنیت و سلامت کشور و ملت به همراه داشته باشد و لذا بایستی هم امنیت فضای سایبر در کشور را ارتقاء و هم بتوانیم با تقویت مکانیزم‌های امنیتی در بعضی موارد حتی مقابله‌به‌مثل نماییم. ازاین‌رو مسئله اصلی تحقیق مشخص نبودن شاخص‌ها، مؤلفه‌ها و ابعاد امنیت در حوزه سایبر می‌باشد که در صورت عدم شناسایی دقیق و علمی، در آینده می‌تواند عواقب جبران‌ناپذیری برای کشور داشته باشد. ازاین‌رو سؤال اصلی پژوهش عبارت است اینکه: الگوی امنیت در فضای سایبر جمهوری اسلامی ایران شامل چه ابعاد و مؤلفه‌هایی می‌باشد؟بنابراین در این پژوهش سعی بر آن بوده تا با بررسی اسناد و مدارک موجود، مؤلفه‌های موجود و مرتبط با فضای سایبری و امنیت آن شناسایی و الگویی ارائه شود که رهگشای طراحی سامانه‌های امن دخیل در فضای سایبری کشور باشد.

بررسی مبانی نظری و پیشینه پژوهش

فضای سایبری، حوزه یا قلمرویی است که در آن با استفاده از علم الکترونیک (تجهیزات و روش‌ها) و طیف الکترومغناطیس به ذخیره‌سازی، ایجادِ تغییر در داده‌ها و تبادل آن‌ها می‌پردازند[1] (به نقل از نصرزاده و همکاران، ۱۳۹۶).

انستیتو مطالعات امنیتی شرق– غرب آمریکا و انستیتو اطلاعات دانشگاه دولتی مسکو در تعریفی مشترک فضای سایبر[2] را محیطی الکترونیکی عنوان نموده‌اند که از طریق آن اطلاعات تولید، ارسال، دریافت، ذخیره، پردازش و حذف می‌شود. فضای سایبری به فضایی اشاره دارد که با استفاده از فناوری اطلاعات و ارتباطات و شبکه‌ها، اجزا و ساختارهای آن یا بر پایه تخیل‌ها فاقد مبنای واقعی و یا بر پایه واقعیت‌های شبیه‌سازی‌شده طراحی و ابداع می‌گردد. (حافظ نیا، ۱۳۹۰) برابر اسناد راهبردی نیروی هوایی آمریکا، بخش‌های حیاتیِ فضای سایبری در شش حوزه اصلی قرارگرفته‌اند. در این میان سه حوزه (کاربر، روش‌ها و داده) توسط نیروی هوایی قابل‌کنترل هستند. سه ناحیه باقی‌مانده (نرم‌افزار، شبکه‌ها و سخت‌افزار) به دلیل آسیب‌پذیری باعث نگرانیِ وزارت دفاع و نیروی هوایی شده‌اند (کورویل شین[3]، به نقل از نصیرزاده، ۱۳۹۶).



شکل (۱) بخش‌های حیاتی فضای سایبر (کورویل شین، به نقل از نصیر زاده، ۱۳۹۶)

[1]. Chairman of the Joint Chiefs of Staff, 2006
[2]. Cyberspace
[3]. Courville Shane P., Lt Col, 2007

دنیای سایبر هرگونه واقعیت مجازی است که توسط مجموعه رایانه‌ها و شبکه‌ها ایجاد می‌شود، در بین دنیای سایبر متعدد و مختلف اینترنت و شبکه‌های مرتبطی که حاوی مطالب چندرسانه‌ای هستند، بیشترین ارتباط را با جنگ سایبر دارند (David, 2011).

امنیت ازنظر لغوی به معنی، ایمن بودن، ایمن شدن و در امان بودن می‌باشد. (تهامی، ۱۳۹۴) امنیت ملی برای یک کشور به مفهوم وجود شرایطی است که آن را در برابر تهدیدات خارجی، حوادث طبیعی و غیرطبیعی، مفاسد و آفات اجتماعی محفوظ نگه می‌دارد. امنیت ملی از مؤلفه‌های متعددی برخوردار است که ازجمله مهم‌ترین آن‌ها می‌توان به امنیت اقتصادی، نظامی، سیاسی، فرهنگی و اجتماعی اشاره نمود. هرگاه یکی از مؤلفه‌های یادشده را خطری تهدید نماید، درواقع امنیت ملی را تهدید می‌کند زیرا امنیت کلیتی غیرقابل‌تفکیک است (نباتی، ۱۳۸۹). جنگ سایبر اشکال متعددی داشته و از انواع فناوری‌های پیشرفته بهره می‌جوید و با الزاماتی همراه است که موجب طراحی مجدد سازمانی، چه درون‌سازمانی و چه بین سازمانی می‌شود. بر این اساس و با عنایت به دیدگاه‌های صاحب‌نظران داخلی و خارجی که از اواسط دهه ۱۹۹۰.م تعاریف مختلفی را برای جنگ اطلاعاتی، سایبر و شبکه‌ای پیشنهاد داده‌اند.

در آینده میدان‌ها جنگ پست‌مدرن به خاطر انقلاب اطلاعات در سطوح راهبردی و تاکتیکی به‌طور کامل دگرگون خواهند شد (آذر، ۱۳۹۳). شرایط جنگ و دفاع در عصر سایبر چنان متحول شده که ما نیازمند طیف جدیدی از مدیران و فرماندهان دفاعی آشنا و در برخی از مواقع مسلط به فناوری اطلاعات و ارتباطات هستیم (زاده جعفر اسدی، ۱۳۹۱). به عقیده اکثر صاحب‌نظران، یکی از ضروری‌ترین و مهم‌ترین سرمایه‌گذاری‌های توسعه شبکه‌ها و فناوری اطلاعات در هر کشور، طراحی و اجرای سامانه‌های به‌طور کامل امن و حفاظت اطلاعات است که به‌عنوان یک سرمایه و اعتبار ملی به‌حساب می‌آید (مسلمی، ۱۳۹۳). جنگ سایبری ابعاد گسترده‌ای از سخت و نرم و نیمه سخت را شامل می‌شود و جنبه‌های نرم آن دارای ابعاد متعددی مثل جنجال‌سازی، ایجاد و گسترش تنش‌های اجتماعی متراکم، تضعیف سرمایه‌های اجتماعی، توانمندسازی جنبش‌های مدنی و سیاسی، تحریف یا جعل مفاهیم فرهنگی و تمدنی (نورمحمدی، ۱۳۹۰).

پیشینه پژوهش

جان‌پرور و حیدری (۱۳۹۰) در مطالعه‌ای با بررسی تعداد بیش از ۳۰ مقاله داخلی و خارجی با عنوان آسیب‌شناسی فضای سایبر بر امنیت اجتماعی با تأکید بر شناخت آسیب‌ها و چالش‌هایی که فضای سایبر بر امنیت اجتماعی کشورمان ایجاد نموده، پیشنهادهایی در جهت افزایش توانایی مقابله با آسیب‌های ناشی از فضای مذکور ارائه نموده است. کورکی نژاد (۱۳۹۴) در پایان‌نامه

کارشناسی ارشد خود در دانشگاه تهران با عنوان تروریسم سایبری (دهشت افکنی در فضای سایبر) و راهکارهای افزایش امنیت سایبر در ایران با تأکید بر عملکرد دولت ایالات‌متحده آمریکا با بررسی تأثیرات تهدیدهای سایبری بر روی فرد و بخش‌های دولتی و خصوصی مؤکداً بر قانون ارتقاء آموزش امنیت سایبری در سطوح ملی و انجام انواع مختلف پژوهش‌های حقوقی در این زمینه تأکید و اصرار داشته است. نور محمد (۱۳۹۰) در مطالعه‌ای با عنوان جنگ نرم، فضای سایبر و امنیت جمهوری اسلامی ایران به این نتیجه رسیده که جنگ نرم سایبری یکی از مهم‌ترین جلوه‌های تهدید آفرین امنیت ملی جمهوری اسلامی ایران است. صادقی و نادری (۱۳۹۴) در تحقیقی دیگر با موضوع تحلیل ابعاد امنیت دولت در ایران قرن ۲۱، در فصلنامه دولت پژوهی، با اشاره به محورهای اساسی مکتب کپنهاگ (مطرح‌شدن امنیت به‌عنوان مفهومی بینا ذهنی، دولت به‌عنوان مرجع امنیت، موسع بودن امنیت و ابعاد ۵ گانه آن) امنیت ملی را به‌عنوان مرکز ثقل امنیت قلمداد نموده‌اند.

بچاری لفته و نجفی شوشتری (۱۳۹۷) در مطالعه‌ای با عنوان "بررسی نقش امنیت سایبری در آینده حمل‌ونقل دریایی" به این نتیجه رسیدند که فضای سایبری می‌تواند به‌عنوان دنیای الکترونیکی درک شود، جایی که اطلاعات نرم‌افزارها و مردم به اشتراک گذاشته می‌شود و به‌صورت یکپارچه در دنیای فیزیکی درهم‌آمیخته شده‌اند. حملات سایبری مربوط به وسایل کامپیوتری در کشتی‌ها، پایانه‌ها، بنادر و تمام تجهیزات کامپیوتری است که از عملیات دریایی پشتیبانی می‌کند. زابلی‌زاده و وهاب‌پور (۱۳۹۷) در مطالعه‌ای با عنوان " قدرت بازدارندگی در فضای سایبر" به این نتیجه رسیدند که استراتژی بازدارندگی بدون اقدامات تلافی جویانه، موفق نخواهد بود. در نبود اقدامات تلافی جویانه، مهاجمان بالقوه هم انگیزه‌ای برای خودداری از حمله ندارند.

روش‌شناسی پژوهش

سنگ بنای تحقیقات آینده، پایش محیط به‌منظور شناسایی شاخص‌های اولیه و "سیگنال‌های ضعیف" است که نشان‌دهنده آینده‌های ممکن می‌باشد. تکنیک‌های پایش معمولاً شامل پانل‌های متخصصین، پایگاه داده، بررسی ادبیات، جستجو در اینترنت، بررسی اسناد، مقالات، پیگیری متخصصین کلیدی و رصد همایش‌های متشکل می‌باشد و نتایج در یک پایگاه داده ذخیره می‌شوند (Gordon and Glenn, 2009). بنابراین در این مطالعه، در فاز اول مطابق روش پایش محیطی، داده‌ها از متون علمی (مقالات)، همایش مرتبط با موضوع فوق و

گزارش‌های رسانه‌های مختلف گردآوری و با استفاده از نرم‌افزار Maxqad11 داده‌ها کدگذاری (کدگذاری باز و محوری) مورد تحلیل قرار گرفت.

داده‌های پژوهش حاضر از منابع علمی و سازمانی، مطالعه کتابخانه‌ای و مطالعه اسنادی (مبانی علمی، پژوهش‌های پیشین و همچنین مستندات رسمی نظیر، اساسنامه‌ها، قوانین، مصوبات داخلی و ...) گردآوری گردید و بالغبر ۶۱ مقاله منتشره داخلی و خارجی طی ۹ سال گذشته در حوزه سایبر گردآوری گردید. همچنین با شرکت در همایش‌ها، کنگره‌ها، نشست‌ها و زمینه‌های وابسته به یادداشت‌برداری سخنرانی‌های صاحب‌نظران کلیدی اقدام شد. علاوه بر آن اسناد کشورهای پیشرو در حوزه امنیت فضای موردبحث نیز از محتوای وب‌سایت‌های مربوط موردبررسی قرارگرفته و کلیه داده‌های حاصل به اطلاعات متنی تبدیل گردید. پس‌ازآن به‌منظور بررسی نظام‌مند توده بزرگی از داده‌های گردآوری‌شده به واحدسازی و مقوله‌بندی داده‌ها اقدام شد. در ابتدا با دقت کامل به کدگذاری باز پرداخته شد. در مرحله کدگذاری اولیه، مفاهیم اولیه برگرفته از داده‌ها ظهور یافت. در کدگذاری ثانویه یا متمرکز، مفاهیم مشترک در یک مقوله قرار داده شد. بعد از پایان یافتن کدگذاری باز، مرحله کدگذاری محوری آغاز شد. در این مرحله به کمک روش مقایسه ثابت به مقایسه مقوله‌های به‌دست‌آمده پرداخته شد و ابعاد آن‌ها مورد شناسایی قرار گرفت. در پایان مدل به‌دست‌آمده ارائه گردید.

یکی از راهبردهای افزایش روایی، چندسونگری در تحقیق می‌باشد (قربانی‌زاده، ۱۳۹۵) در همین رابطه؛برای افزایش روایی تحقیق از چندسویه نگری در منابع استفاده‌شده است و کتاب‌های منتشرشده، مقالات، گزارش‌های رسانه‌ها و مصاحبه‌های منتشرشده از فعالان و مسئولین حوزه مربوطه استفاده گردیده است. در این مطالعه درزمینه پایایی، از روش توافق یا همخوانی بین دو کدگذار استفاده‌شده و در نرم‌افزار MAXQDA یک سند توسط دو نفر کدگذاری گردید[1] و ضریب توافق به‌دست‌آمده ۹۳ درصد می‌باشد که حاکی از توافق و همخوانی بالا و نیز ضریب پایایی مناسب می‌باشد.

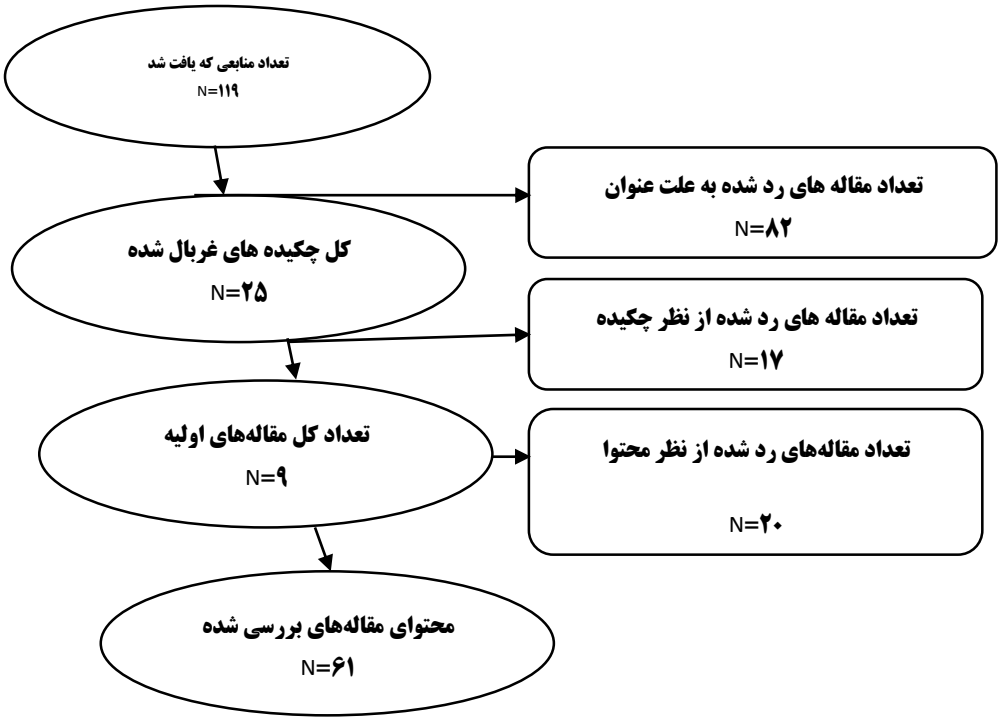
یافته‌های پژوهش

سؤال تحقیق: الگوی امنیت در فضای سایبر جمهوری اسلامی ایران شامل چه ابعاد و مؤلفه‌هایی می‌باشد؟

---

[1]. در نرم‌افزار maxqda سه روش برای پایایی (توافق میان کدگذاران) وجود دارد که شامل حضور کد در مدرک، فراوانی کد در مدرک و درصد توافق در بخش‌های کدگذاری شده می‌باشد و در این مطالعه نتیجه روش دوم گزارش‌شده است.

محقق مقالات منتشرشده در ژورنال‌های مختلف را با استفاده از کلیدواژه‌های، امنیت سایبری، فضای سایبری، تهدیدات و چالش‌های وضع امنیتی سایبری در پایگاه‌های داده‌های داخلی و خارجی[1] و هم‌چنین پایگاه‌های تخصصی مجلات نور و پدافند غیرعامل (و نیز مطالعه اجمالی سند راهبردی تعدادی از کشورهای موفق در عرصه موردبحث) بین سال‌های ۱۳۸۵ تا اوایل سال ۱۳۹۷ جستجو و به شرح زیر آن‌ها را بررسی و مقالات مناسب را انتخاب نمود.



شکل (۲) فرآیند بازبینی برای انتخاب مقاله‌های موردنظر

به‌محض اینکه مقالات برای تناسب با پارامترهای مطالعه بررسی شد، در قدم بعدی کیفیت روش‌شناختی مطالعه‌ها ارزیابی شد. هدف از این گام، حذف مقاله‌هایی است که به یافته‌های اراده شده اعتمادی نداشته‌ایم. شایان‌ذکر است برخی از مقاله‌های خارجی مرتبط با امنیت در فضای سایبری که با فضای سایبر موجود و حاکم بر کشور، تناسب نداشته‌اند، در مراحل غربال‌گری حذف‌شده‌اند. در این بخش از برنامه مهارت‌های ارزیابی حیاتی[2] ابزاری که به‌منظور ارزیابی کیفیت مطالعه‌های اولیه پژوهش‌های کیفی استفاده می‌شود، نیز استفاده‌شده است. CASP ، ده سؤال

[1]. IRAN DOC ،IEEE ،SCIENCE DIRECT ،SID ،EMERALD ،SCOPUS ،CIVILICA
[2]. Critical Appraisal Skills Program (CASP)

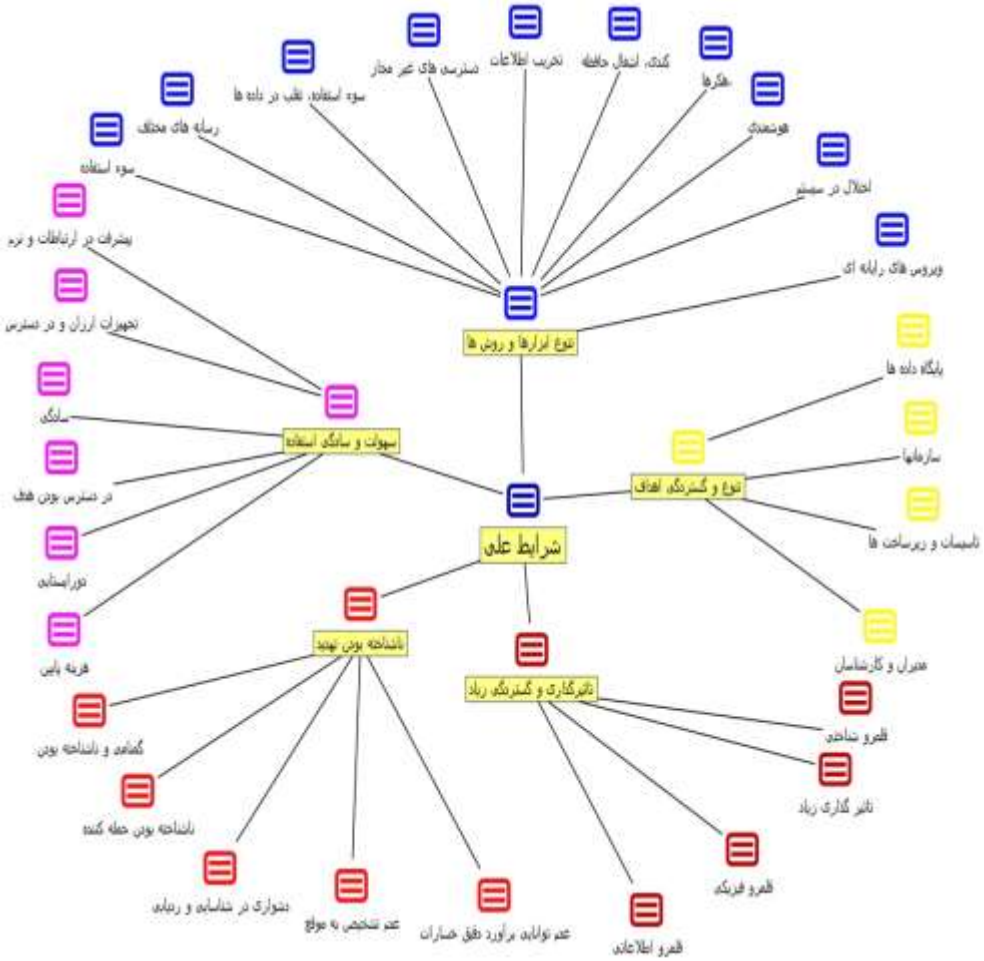
است که به ما کمک می‌کند تا مفهوم تحقیق کیفی را دریافته و دقت، اعتبار و اهمیت مطالعات کیفی پژوهش را مشخص سازیم. این سؤالات بر این موارد تمرکز دارد، ۱- اهداف پژوهش، ۲- منطق روش، ۳- طرح تحقیق، ۴- روش نمونه‌برداری، ۵- جمع‌آوری داده‌ها، ۶- انعکاس‌پذیری (رابطه بین محقق و شرکت‌کنندگان)، ۷- ملاحظات اخلاقی، ۸- دقت تجزیه‌وتحلیل داده‌ها، ۹- بیان واضح و روشن یافته‌ها، ۱۰- ارزش پژوهش . در این مرحله به هرکدام از این سؤالات یک امتیاز کمی داده شد، بنابراین توانستیم امتیازاتی را که به هر مقاله داده شد را جمع و به‌اجمال مجموعه مقالات را بررسی و نتایج ارزشیابی به دست آمد. (بر اساس مقیاس ۵۰ امتیازی CASP سیستم امتیازبندی زیر مطرح و هر مقاله‌ای که پایین‌تر از امتیاز خوب (کمتر از۳۰) بود، حذف شد: عالی (۵۰-۴۰)، خیلی خوب (۴۰-۳۱)، خوب (۳۰-۲۱)، متوسط (۲۰-۱۱)، و ضعیف (۱۰-۰) . بر اساس امتیازهای داده‌شده به هر مقاله، حداقل میانگین امتیاز داده‌شده به مقالات ۲۱ و حداکثر امتیاز داده‌شده ۴۸ بوده است. درنتیجه در فرآیند ارزشیابی، از بین ۸۴۷ مقاله، ۱۱۹ مقاله را حذف و درنهایت ۶۱ مقاله بابت تجزیه‌وتحلیل باقی ماند.

در پژوهش حاضر، ابتدا تمام عوامل استخراج‌شده از مطالعه‌ها به‌عنوان کد (مؤلفه‌ها) در نظر گرفته‌شده و سپس با در نظر گرفتن مفهوم هر یک از این کدها، آن‌ها را در یک مفهوم مشابه (ابعاد) دسته‌بندی کرده تا به‌این‌ترتیب مفاهیم پژوهش شکل داده شود.

جدول (۱) عوامل و ابعاد مؤثر در امنیت فضای سایبر ج. ا.ا

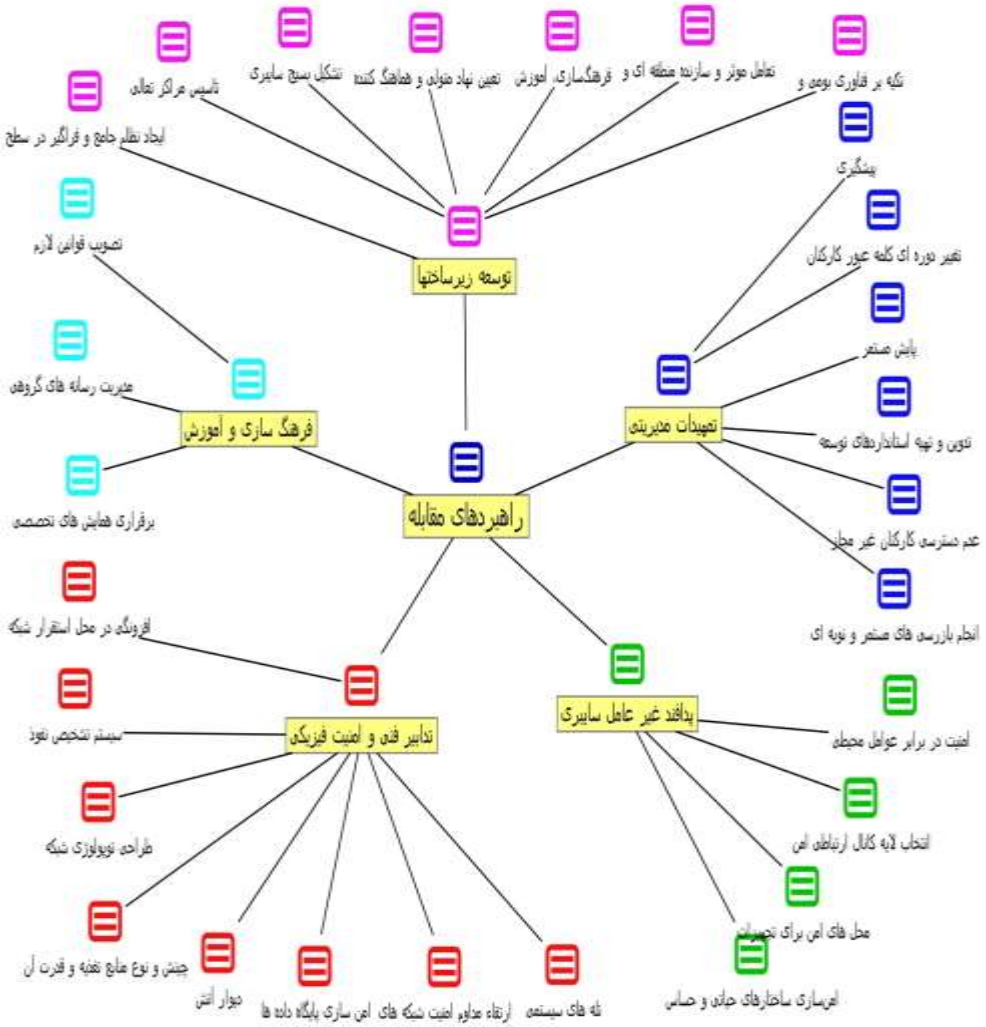
مفاهیم اولیه	مقوله‌بندی و شکل‌گیری ابعاد
ایجاد نظام جامع و فراگیر در سطح ملی	راهبردهای مقابله/ توسعه زیرساخت‌ها/ ایجاد نظام جامع و فراگیر در سطح
تکیه‌بر فناوری بومی و توانمندی‌های تخصصی داخلی	راهبردهای مقابله/ توسعه زیرساخت‌ها/ تکیه‌بر فناوری بومی
تعامل مؤثر و سازنده منطقه‌ای و جهانی	راهبردهای مقابله/ توسعه زیرساخت‌ها/ تعامل مؤثر و سازنده منطقه‌ای
تعیین نهاد متولی و هماهنگ‌کننده	راهبردهای مقابله/ توسعه زیرساخت‌ها/ تعیین نهاد متولی و هماهنگ‌کننده
فرهنگ‌سازی، آموزش	راهبردهای مقابله/ توسعه زیرساخت‌ها/ فرهنگ‌سازی، آموزش
ایمن‌سازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات	راهبردهای مقابله/ پدافند غیرعامل سایبری/ ایمن‌سازی ساختارهای حیاتی و حساس

ارتقاء مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی	راهبردهای مقابله/ تدابیر فنی و امنیت فیزیکی/ ارتقاء مداوم امنیت شبکه‌های
پیشرفت در ارتباطات و نرم‌افزارهای رایانه‌ای	شرایط علی/ سهولت و سادگی استفاده/ پیشرفت در ارتباطات و نرم
تجهیزات ارزان و در دسترس	شرایط علی/ سهولت و سادگی استفاده/ تجهیزات ارزان و در دسترس
ممانعت از دسترسی کارکنانی که اخراج، بازنشسته یا انتقال‌یافته‌اند	راهبردهای مقابله/ تمهیدات مدیریتی/ عدم دسترسی کارکنان غیرمجاز
تغییر دوره‌ای کلمه عبور کارکنان	راهبردهای مقابله/ تمهیدات مدیریتی/ تغییر دوره‌ای کلمه عبور کارکنان
تدوین و تهیه استانداردهای توسعه سیستم‌ها و مستندات آن	راهبردهای مقابله/ تمهیدات مدیریتی/ تدوین و تهیه استانداردهای توسعه
انجام بازرسی‌های مستمر از سامانه‌های برنامه‌ای دارای زمان‌بندی	راهبردهای مقابله/ تمهیدات مدیریتی/ انجام بازرسی‌های مستمر و نوبه‌ای



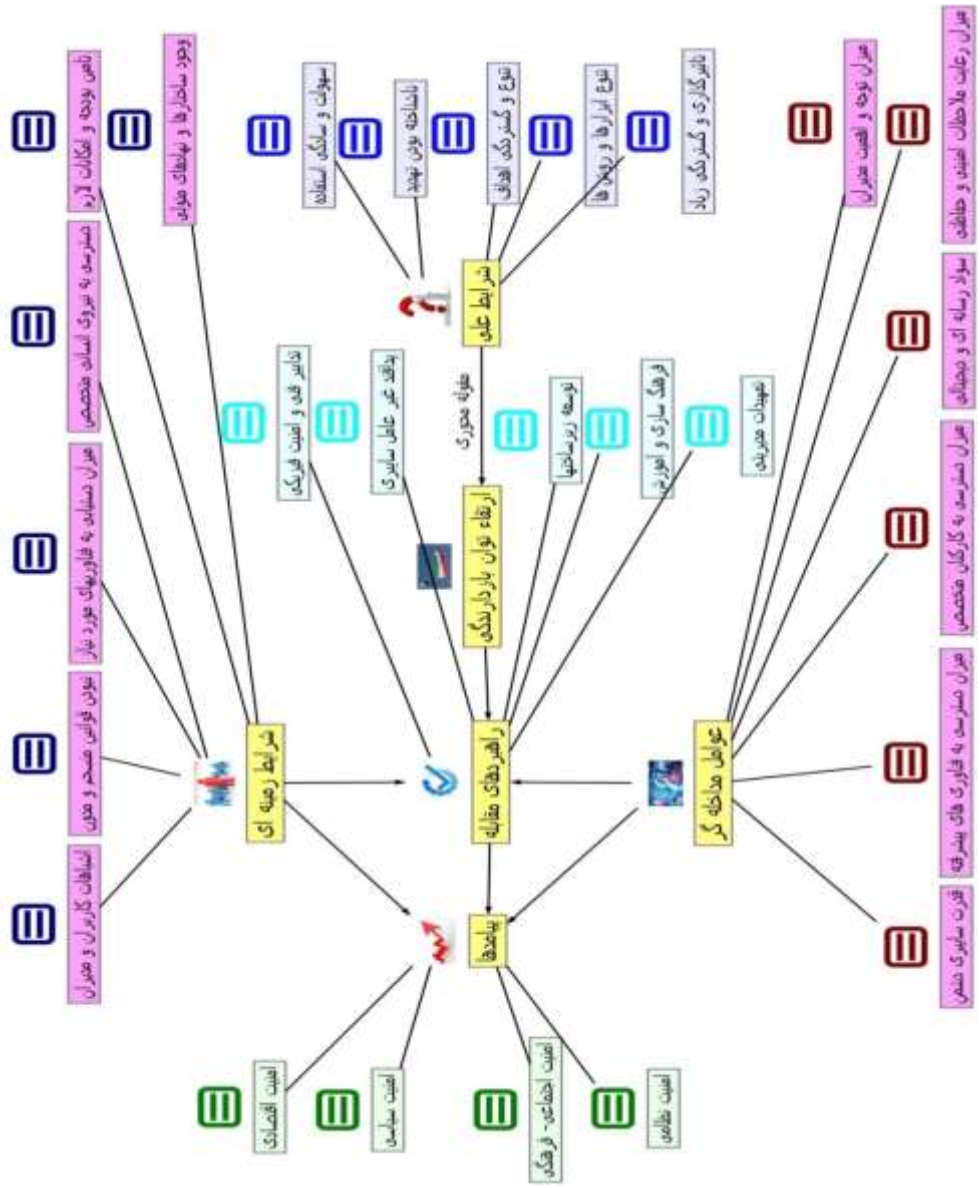
شکل (۳) شرایط علی مؤثر در امنیت فضای سایبر ج. ا.ا

یافته تحقیق در خصوص شرایط علی حاکی از آن است که سهولت و سادگی استفاده از جنگ سایبر، تأثیرگذاری زیاد، مبهم و غیر قبل شناسایی بودن، هوشمندی و تنوع ابزارها و روش‌ها، تنوع و گستردگی اهداف و قلمرو این جنگ، شرایط را برای استفاده دشمن از آن کاملاً منطقی و قابل‌تصور می‌نماید و دشمنان استراتژی‌های متعددی برای استفاده از فضای سایبر دارند.



شکل (۴) راهبردهای مقابله با تهدیدات فضای سایبر

یافته‌های تحقیق حاکی از آن است که شرایط زمینه‌ای برای تهدیدات سایبری دشمنان مساعد می‌باشد و عوامل مداخله‌گر در این حوزه نیز در مواقعی در راستای خواست دشمنان می‌باشد و لذا جمهوری اسلامی ایران بایستی ضمن فرهنگ‌سازی و آموزش درزمینهٔ تهدیدات سایبری، زیرساخت‌های لازم در این زمینه را ایجاد و تقویت نماید و با اتخاذ تدابیر فنی و امنیت فیزیکی، تمهیدات مدیریتی و رعایت اصول پدافند غیرعامل سایبری، مانع از به خطر افتادن امنیت اقتصادی، سیاسی، اجتماعی و فرهنگی و امنیت نظامی گردد.



شکل (۵) الگوی امنیت فضای سایبر ج. ا.ا

پس از ارائه الگو در جلسه‌های گروه کانونی با شرکت ۵ نفر از خبرگان علوم سایبری و پدافند غیرعامل همه جوانب مدل موردبررسی قرارگرفته و تغییری روی آن انجام نپذیرفت. درواقع ابعاد و مؤلفه‌های جدید به مدل اضافه یا کسر نگردید. به‌منظور سنجش پایایی مدل طراحی‌شده از شاخص کاپا استفاده‌شده است. بدین طریق که شخص دیگری (از نخبگان پدافند غ ع) بدون

اطلاع از نحوه ادغام کدها و مفاهیم ایجادشده، اقدام به دسته‌بندی کدها در مفاهیم کرده است. سپس مفاهیم ارائه‌شده توسط پژوهشگر با مفاهیم ارائه‌شده توسط این فرد مقایسه شده است. درنهایت با توجه به تعداد مفاهیم ایجادشده مشابه و مفاهیم ایجادشده متفاوت، شاخص مزبور محاسبه‌شده است. همان‌طور که در جدول شماره (۲) مشاهده می‌گردد، پژوهشگران ۵۴ مفهوم و خبره دیگر ۵۱ مفهوم ایجاد کرده‌اند، که از این تعداد ۵۰ مفهوم مشترک هستند. همان‌طور که در ادامه نشان داده‌شده است، مقدار شاخص کاپا برابر با ۰/۹۹۹۹ محاسبه شد که با توجه به جدول شماره (۳) در سطح توافق عالی قرارگرفته است.

جدول (۲) وضعیت تبدیل کدها به مفاهیم توسط پژوهشگر و فرد دیگر

		نظر محقق		
		بله	خیر	مجموع
نظر خبره دیگر	بله	A=50	B=1	51
	خیر	C=4	D=0	4
	مجموع	54	1	N=55

توافقات مشاهده‌شده A+D/N=50/55=0/909

جدول (۳) وضعیت شاخص کاپا

مقدار عددی شاخص کاپا	وضعیت توافق
کمتر از ۰	ضعیف
۰-۰/۲	بی‌اهمیت
۰/۲۱-۴/۰	متوسط
۰/۴۱-۰/۶	مناسب
۰/۸-۰/۶۱	معتبر
۰/۸۱-۱	عالی

توافقات شانسی =A+B/N× A+C/N ×C+D/N ×B+D/N=0/0000216

K=توافقات مشاهده‌شده -توافقات شانسی- ۱/ توافقات شانسی=0/9999

نتیجه‌گیری و پیشنهادها

آنچه حائز اهمیت است اینکه فناوری‌های نوین موجب تقویت هر چه بیشتر "نگاه از بالا[1]" می‌شود و این مفهوم در ترکیب با تمرکززدایی فرماندهی، نتایج چشمگیر و بالقوه تعیین‌کننده جنگ سایبر را به ارمغان می‌آورد. چون در جنگ سایبر موضوعات گسترده اعم از سازمان و دکترین نظامی، راهبردی، تاکتیک، طراحی و ساخت سلاح مطرح می‌شوند، فلذا جنگ سایبر در نبردهای کم شدت و پر شدت، در محیط‌های متعارف و غیرمتعارف و درنهایت برای مقاصد آفندی و پدافندی موضوعیت پیدا می‌کند.

این پژوهش نشان می‌دهد که با توجه به سهولت و سادگی استفاده از جنگ سایبر، تأثیرگذاری زیاد، مبهم و غیر قبل شناسایی بودن، هوشمندی و تنوع ابزارها و روش‌ها، تنوع و گستردگی اهداف و قلمرو این جنگ، شرایط برای استفاده دشمن از آن کاملاً منطقی و قابل‌تصور می‌باشد.

علاوه بر موارد یادشده، قدت سایبری دشمنان جمهوری اسلامی ایران و در اختیار داشتن انواع ابزارها و فن‌ها جنگ سایبری و دسترسی آنان به آخرین پیشرفته‌ای حوزه سایبر و در اختیار داشتن منابع انسانی متخصص شرایط لازم را برای دشمنان برای استفاده از جنگ سایبر مهیا می‌نماید. در کنار آن سواد رسانه‌ای و دیجیتالی پایین جامعه، مدیران و کارکنان، بی‌توجهی مدیران به این حوزه و عدم رعایت کامل ملاحظات امنیتی و حفاظتی، جمهوری اسلامی ایران را در برابر جنگ سایبری آسیب‌پذیر می‌نماید.

زمینه‌های لازم نیز برای محقق شدن تهدیدات سایبری در کشور وجود دارد، زیرا در این زمینه در کشور متولی مشخصی وجود ندارد و نهادی متولی این حوزه نمی‌باشد و بودجه و امکانات لازم برای این حوزه تأمین و واگذار نمی‌گردد و همچنین دسترسی به آخرین فناوری‌های این حوزه برای ج.ا.ایران مقدور نمی‌باشد و نیروی انسانی لازم هم در حوزه‌های مربوطه وجود ندارد و لذا کاربران و مدیران این حوزه معمولاً دارای اشتباهات متعددی می‌باشند و قوانین و مقررات لازم و بازدارنده هم تدوین‌نشده است.

لذا عدم اتخاذ تدابیر لازم فنی و مدیریتی، توسعه زیرساخت‌ها و پیاده‌سازی پدافند غیرعامل سایبری و همچنین فرهنگ‌سازی و آموزش در این زمینه موجب به خطر افتادن امنیت اقتصادی، سیاسی، اجتماعی و فرهنگی و امنیت نظامی خواهد شد.

در ضمن می‌بایست تحول در امور نظامی را به‌صورت یکسری تغییرات گسترده در استفاده از فناوری‌های نوین و نیز تغییرات فراوان در آموزش، سازمان‌دهی و دکترین تعریف و یک تغییر

[1]. Topsight

بنیادین واقعی در فضای سایبر را تجربه تا به استقلال سایبری دست‌یابیم. ایجاد دغدغه‌ی امنیت در کشور در خصوص ایجاد نقشه راه فناوری و محصولات بومی امنیت سایبر، حاکمیت شبکه‌ای مؤثر، ایجاد نهادهای پژوهشی امنیت سایبری در کشور، بهره‌مندی از مدل‌های تحقیقاتی برای حاکمیت این فضا به‌منظور استفاده مناسب و متناسب از همه ظرفیت‌های موجود، همه و همه به‌عنوان راه‌حل‌هایی مناسب برای حاکمیت محسوب می‌شوند. در ضمن از مهم‌ترین مسائل حفظ امنیت سایبری کشور، استقلال و خودکفایی در تولیدات و محصولات امنیت سایبر است چراکه محصولات نرم‌افزاری و سخت‌افزاری وارداتی، شکاف امنیتی نهفته و آشکاری دارند درنتیجه ازجمله موارد پراهمیت، خط‌مشی گذاری مناسب برای رویارویی موفق با تهدیدات این حوزه در کشور است. از تهدیدات همیشگی و پیش روی کشور و به‌عنوان پنجمین صحنه‌ی نبرد در کنار صحنه‌های هوایی، زمینی، دریایی و فضایی امنیت در فضای سایبر است فلذا نیازمندی به مدل‌هایی برای حاکمیت در این حوزه از واجبات حتمی تلقی می‌گردد که باوجود هزینه‌های کلان، بعد از گذشت حداقل ۱۰ سال همچنان پراکندگی و نبود هم‌افزایی در نهادهای متولی کشور مشهود است. با توجه به نتایج به‌دست‌آمده در این پژوهش، نهادهای مختلفی در کشور در حوزه موردبحث فعالیت می‌کنند که نیازمند فعال نمودن حداکثری ظرفیت آن‌ها در کشور از طریق تدوین سیاست‌های یکپارچه از سوی شورای عالی فضای مجازی است. بر اساس نتایج پژوهش، پیشنهادهایی به شرح زیر به‌منظور ارتقای وضعیت امنیتی فضای موردبحث ارائه می‌گردد:

- جمهوری اسلامی ایران با انجام تحقیقات کاربردی در حوزه سایبر، فناوری‌های موردنیاز این حوزه را درزمینه امنیت حوزه سایبر و هم‌چنین آفند و پدافند سایبری را طراحی، تولید و بومی‌سازی نمایند.
- زیرساخت‌های حوزه سایبر را درزمینه سخت‌افزار و نرم‌افزار با استفاده از ظرفیت‌های بومی تکمیل و تقویت نمایند و در حد امکان از استفاده از فناوری‌های غیربومی پرهیز نمایند.
- قوانین و مقررات و دستورالعمل‌های لازم حوزه سایبر را تدوین، آماده‌سازی و پیاده نمایند و استاندارد نمودن فعالیت‌های این حوزه زمینه نفوذ دشمن را کاهش و ضریب خطا و اشتباه مدیران و کارکنان را کاهش دهند.
- در همه امور و فعالیت‌های جاری سازمان‌های دولتی، نظامی و انتظامی و صنایع حساس و دفاعی، اصول پدافند غیرعامل سایبری رعایت نمایند.

- در نظام آموزشی عمومی (نظام متوسطه) و تخصصی، سرفصل سواد اطلاعاتی، سواد رسانه‌ای و مطالب مرتبط با حوزه سایبر را لحاظ و در محصولات فرهنگی نیز در خصوص آگاه‌سازی و ترویج فرهنگ رعایت اصول پدافند غیرعامل سایبری مدنظر مسئولان حوزه فرهنگی باشد.
- تمهیدات مدیریتی لازم برای مدیریت هدفمند حوزه سایبر درزمینهٔ تدوین چشم‌انداز، اهداف و راهبردهای حوزه سایبر، ایجاد ساختارهای لازم، استفاده از ظرفیت‌های دیپلماتیک، تصویب قوانین و مقررات، استخدام و به‌کارگیری کارکنان متخصص، آموزش و فرهنگ‌سازی در بین کارکنان و مدیران، نظارت دقیق و مستمر بر فعالیت کاربران به عمل آید.
- ایجاد مراکز رصد تهدیات سایبر و همچنین نظام آینده‌پژوهی پژوهشی امنیت سایبری جهت رصد تهدیدات همراه با تغییرات سریع فناوری (درگیر نمودن شرکت‌های فعال فناور و دانش‌بنیان در این زمینه).

منابع

- اندیشگاه شریف و اندیشکده کاوشگران آینده. (۱۳۸۴). *جنگ و دفاع سایبری (گام اول)*، تهران: انتشارات موسسه آموزشی و تحقیقاتی دفاعی (مرکز آینده‌پژوهی علوم و فنون دفاعی).
- اندیشگاه شریف و اندیشکده کاوشگران آینده. (۱۳۸۶). جنگ و دفاع سایبری (گام دوم)، تهران: انتشارات موسسه آموزشی و تحقیقاتی دفاعی (مرکز آینده‌پژوهی علوم و فنون دفاعی).
- بچاری لفته، محمدرضا. و نجفی شوشتری، سید منصور. (۱۳۹۷). بررسی نقش امنیت سایبری در آینده حمل‌ونقل دریایی، *دومین همایش بین‌المللی مهندسی برق، علوم کامپیوتر و فناوری اطلاعات، تهران.*
- بی نام. (۱۳۸۸). *فتنه نرم*، تهران: انتشارات مرکز مطالعات و پژوهش‌های جهاد دانشگاهی.
- جیستان، ذبیح الله. (۱۳۹۰). دفاع در برابر ابزار پنهان جنگ سایبری، *مجموعه مقالات نخستین همایش ملی دفاع سایبری*، پژوهشکده فناوری اطلاعات و ارتباطات جهاد دانشگاهی.
- حسن‌بیگی، ابراهیم. (۱۳۸۵). *حقوق و امنیت در فضای سایبر*، تهران: انتشارات موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار.
- حسن‌بیگی، ابراهیم. (۱۳۸۸). *حقوق و امنیت در فضای سایبری*، تهران: انتشارات دانشگاه عالی دفاع ملی.
- خلج، رضا. (۱۳۹۰). *شناخت آسیب‌پذیری‌ها و امنیت شبکه*، تهران: انتشارات دانشگاه آزاد اسلامی.
- زابلی زاده، اردشیر. و وهاب‌پور، پیمان. (۱۳۹۷). قدرت بازدارندگی در فضای سایبر، *فصلنامه رسانه و فرهنگ*.

- زاده جعفراسدی، حسن.، انتظار شبستری، رضا. و هایی، حمیده. (۱۳۹۱). *دفاع سایبری*، تهران: انتشارات انستیتو ایزایران.
- ضیایی‌پرور، حمید. (۱۳۸۸). *جنگ نرم ویژه جنگ رسانه‌ای*، تهران: انتشارات موسسه ابرار معاصر.
- غروی، ناصر. (۱۳۹۰). معرفی رویکردها و متدولوژی‌های طراحی و اجرای سناریوهای مقابله با تهدیدهای سایبری، مجموعه مقالات نخستین همایش ملی دفاع سایبری، *پژوهشکده فناوری اطلاعات و ارتباطات جهاد دانشگاهی*.
- موسسه آموزشی تحقیقاتی صنایع دفاعی. (۱۳۸۹). *طرح فراسازمانی فاوا، الگوی اهداف کنترلی فاوا*.
- نصیرزاده، عزیز.، خادم دقیق، امیر هوشنگ. و فرهادی، علی. (۱۳۹۶) *آینده‌شناسی جنگ*، تهران: انتشارات مرکز انتشارات راهبردی نهاجا.
- نورمحمدی، مرتضی. (۱۳۹۰). جنگ نرم، فضای سایبر و امنیت جمهوری اسلامی ایران، *فصلنامه راهبرد فرهنگ*، ش ۱۶.
- واحدی، مرتضی. (۱۳۹۱). *پدافند غ ع و امنیت در فضای سایبری*، تهران: انتشارات دانشکده فارابی.
- Bass, T. & Lt.Col.Glenn, W. (2015). *A Simple Framework For Filtering Queued Smtp Mail*.
- Brenner, S. W. (2006). *Sybercrime, syberterrorism and Syberwarfare*, International Review of Penal Law: Cybercrime, AIDP و Volume 77.
- Colarik, A. M. (2006). *Cyber Terrorism: Political and Economic Implication*, Idea Group Publication.
- Gordon, T.J. & Glenn, J.C. (2009). Environmental scanning. In: Glenn, J.C.; Gordon, T.J., eds. (2011). *Futures research methodology*—version 3.0 [CD-ROM].Washington, DC: The Millennium Project.-Cyber War, Methods and Practice, K.Saalbach.
- Kuehl, D. (2009). *First Battles in Cyberspace: New Paradigm for 21st Century Warfar irmcollege*, National Defense University, IQPC Cyber Warfare.
- Sadowsky, G., James X.D., Greenberg, Alan, J., Mack, B. & Schwarts, A. (2004). *ITSecurity Handbook*, infoDev, Worldbank.
- Siber, U. (2010). *International Legal LegalHarmonization and Cooperation against Terrorist Use of the Internet*, Max Planck institute for oreign and international Criminal Law, Freiburg Germany.
- Steele, R.D. (2011). *The Asymmetric Threat*, JFQ, summer-winter.