DOR: https://dorl.net/dor/20.1001.1.28212606.1401.5.16.2.6

فصلنامه علمی آماد و فناوری دفاعی، سال پنجم، شماره شانزدهم، زمستان ۱۴۰۱

نقش فضای مجازی در ارتقای توانمندی دفاع سایبری مردم‌پایه

محمدجواد نصرالله‌زاده[۱] و فرشید صفری[۲]

تاریخ دریافت: ۱۴۰۱/۰۷/۳۰ تاریخ پذیرش: ۱۴۰۱/۱۱/۲۷

چکیده

حفظ امنیت یکی از دغدغه های اصلی انسان ها از ابتدای خلقت بوده و در عصر کنونی نیز با فراگیرشدن بیش‌ازپیش استفاده از اینترنت و وابستگی به فضای‌سایبر، لزوم توجه به آن بیش از گذشته احساس می‌شود؛ این نگرانی در کنار ویژگی‌های منحصربه‌فرد فضای مجازی همچون بی‌مرزی، تغییرات مداوم و سریع، گمنامی کاربران، هزینه پایین و عدم‌توانایی در برآورد میزان و دامنه خسارات وارد شده در مراحل آغازین حملات سایبری کاملاً قابل درک است. پژوهش حاضر با رویکرد توصیفی-تحلیلی و با هدف شناسایی ظرفیت‌ها و آسیب‌های فضای مجازی، با ابزار فیش‌برداری در مطالعات اسنادی و انجام مصاحبه خبرگی تلاش نموده است تا اقدامات مردم‌پایه و مردم‌محور را در حوزه دفاع سایبری مورد بررسی قرار دهد. نتیجه پژوهش، در کنار شناسایی برخی از مهم‌ترین آسیب ها و چالش های فضای سایبری، مجموعه‌ای از اقدامات مردم‌پایه را برای مقابله با تهدیدات فضای سایبر و جلوگیری از نفوذ و بهره‌برداری دشمن ارائه می‌نماید.

کلمات کلیدی: اینترنت، دفاع سایبری، فضای سایبر، فضای مجازی، مردم‌پایه

۱. دانشیار و عضو هیئت علمی دانشگاه عالی دفاع ملی، نویسنده مسئول MJ.Nasrollahzade@chmail.ir
۲. دانشجوی دکتری مطالعات امنیت ملی، دانشگاه عالی دفاع ملی، F.Safary@Iran.ir

مقدمه

همزمان با پیروزی انقلاب اسلامی، قدرت نفوذ کشورهای غربی به‌ویژه ایالات متحده در جایگاه امپریالیسم جهانی و حامیان آن در منطقه، با تهدید جدی مواجه شد و از همان ابتدا، با بهره‌گیری از تمام امکانات و ظرفیت‌های نظامی، سیاسی، اقتصادی، اجتماعی و فرهنگی، تهدیدهای مختلفی را برعلیه جمهوری اسلامی ایران به کار بستند تا نسبت‌به براندازی نظام اسلامی موفقیت کسب نمایند؛ این موضوع با تهدیدهای سخت نظامی از قبیل کودتا، ترور و جنگ تحمیلی آغاز شد لیکن، با درایت و هدایت‌های حضرت امام(ره) و مقام معظم رهبری(مدظله‌العالی) و هوشیاری و حضور مردم در صحنه، با ناکامی روبرو گردید.

شکست در عرصه تهدیدهای سخت نظامی، موجب شد تا جنگ نرم[1] و بهره‌مندی از قابلیت ها و فرصت‌های موجود در فضای مجازی[2]، به‌منظور تقابل با نظام اسلامی مورد توجه دشمنان قرار گیرد.

بیان مسئله

امروزه فضای مجازی در سازمان‌دهی عملیات روانی[3] و شبکه های اجتماعی مجازی[4] به‌منظور تأثیرگذاری بر افکارعمومی[5] و امنیت ملی[6] ازطریق انتشار اخبار غیرواقعی[7] علیه مسئولان نظام، تبلیغات گسترده و تشویق جهت تجمع‌های غیرقانونی مغایر با ارزش‌های جامعه، فراخوان اغتشاش و ناآرامی در زمان‌های مشخص با مقاصد معین امنیتی، اقتصادی، سیاسی، اجتماعی و...، کاربردی مؤثر دارد تا جایی که نمی‌توان نقش فناوری اطلاعات و ارتباطات را در حوزه دفاعی- امنیتی[8] کشور نادیده گرفت. «هدف اصلی از این نوع تهدید، حذف باورمندی جامعه و بحران هویت،

1 Soft Warfare
2 Cyberspace
3 Psychological Operation
4 Virtual Social Networks
5 Public Opinion
6 National Security
7 Fake News
8 Defense Security Field

سلب اراده و روحیه مقاومت و در مجموع استحاله فرهنگی- سیاسی است و تلاش می شود ملت دارای آرمان به ملت بی‌آرمان تبدیل شده و به دست خود، الگوهای رفتاری اصیل ملی و دینی را در حوزه‌های اقتصادی، سیاسی و فرهنگی به چالش اندازد» (فروزان و احمدی‌مقدم، ۱۴۰۱). برهمین اساس، کسب قدرت بازدارندگی[1] یکی از مهم‌ترین عوامل تأثیر گذار در دفاع سایبری قلمداد می‌شود.

مقام معظم رهبری(مدظله‌العالی) نیز هدف مقاومت را رسیدن به نقطه بازدارندگی دانسته و معتقدند این نقطه باید بتواند جوری خود را نشان بدهد که دشمن را از تعرض به ملت ایران درهمه زمینه ها منصرف کند، دشمن ببیند فایده‌ای ندارد و با ملت ایران نمی‌توانند کاری بکنند (بیانات در مراسم سی‌امین سالگرد رحلت امام خمینی (ره)، ۱۳۹۸/۰۳/۱۴).

در اسناد بالادستی نیز از جمله سند چشم‌انداز ۲۰ساله جمهوری اسلامی ایران در افق ۱۴۰۴هش که در آبان‌ماه ۱۳۸۲ توسط رهبر معظم انقلاب به سران قوای سه‌گانه ابلاغ گردید، جامعه ایرانی در افق چشم‌انداز را با ویژگی‌هایی مشخص معرفی کرده است، جامعه‌ای «*امن، مستقل و مقتدر با سامان دفاعی مبتنی بر بازدارندگی همه‌جانبه*[2] *و پیوستگی مردم و حکومت*» که موضوع بازدارندگیِ همه‌جانبه و تعامل و پیوستگی مردم و حکومت به‌عنوان یکی از موضوعات مهم و اساسی در آن دیده شده است.

رهبر معظم انقلاب همچنین، سیاست‌های کلی نظام در امور «پدافند غیرعامل»[3] را در سال ۱۳۸۹ به عنوان راهنما، خط‌مشی و جهت‌گیری اصلی دستگاه های ذیربط و متولی‌امر به قوای سه‌گانه ابلاغ نمودند که در بند یکم آن به اقدامات بازدارنده با تأکید بر پدافند غیرعامل پرداخته شده است: «مجموعه اقدامات غیرمسلحانه که موجب افزایش بازدارندگی، کاهش آسیب پذیری، تداوم

1 Deterrence Power
2 Comprehensive Deterrence
3 Passive Defense

فعالیت‌های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران درمقابل تهدیدات و اقدامات نظامی دشمن می‌گردد».

بدین منظور، دولت در اولین اقدام خود برای مقابله با تهدیدات[1] ناشی از فضای مجازی به‌هنگام وقوع ناآرامی‌ها و بحران‌های اجتماعی و در راستای صیانت از افکار عمومی و حفظ امنیت ملی، نسبت به محدود کردن مقطعی دسترسی به اینترنت و فیلتر کردن شبکه های اجتماعی مجازی اقدام می‌نماید تا بتواند بر فضای مجازی داخل کشور تسلّطی نسبی بیابد.

بنابراین، فضای مجازی علاوه‌بر اینکه امروزه ابزاری کارآمد برای اطلاع‌رسانی تلقی می شود، تأثیر زیادی در کنش و واکنش‌های اجتماعی و فرهنگی جوامع دارد و می‌توانند به‌عنوان ابزار عملیات روانی و تهاجم فرهنگی توسط دشمن برای ایجاد بحران و تأثیر گذاری بر افکارعمومی و امنیت ملی علیه کشورهای رقیب نیز به کار رود؛ به‌همین جهت در تهدیدات نا شی از اینترنت و فضای مجازی، نقش مردم در «دفاع سایبری»[2]را نمی‌توان نادیده گرفت و «مردمی بودن» همانند فضای واقعی، در فضای مجازی هم نمود پیدا می‌کند.

درنهایت، این سؤال به ذهن متبادر می‌شود که چه زمینه‌هایی سبب می‌شود تا اقدامات وفعالیت های دشمن در فضای مجازی برای سازماندهی ناآرامی‌ها علیه امنیت ملی ج.ا.ایران مؤثر واقع نیفتد؟ به نظر می‌رسد در این خصوص، راهکار استفاده از دفاع سایبری مردم‌پایه در فضای‌مجازی می‌توانند در ارتقای سطح امنیت ملی ج.ا.ایران مؤثر باشد بنابراین:

سؤال اصلی تحقیق این است که بهره‌گیری از فضای‌مجازی توسط مردم چگونه می‌تواند در تقویت دفاع سایبری و درنهایت ارتقای امنیت ملی ج.ا.ایران نقش داشته باشد؟

1 Threats
2 Defense Cyber

اهمیت و ضرورت تحقیق

اهمیت و ضرورت توجه به تهدیدهای‌سایبری علیه جمهوری‌اسلامی، پیامدها و عواقب نا شی از آن تا اندازه‌ای است که رهبر معظم انقلاب بارها بر آن تأکید نموده‌اند که برخی از آنها عبارتند از:

- «[دشمن] از لحاظ فضای مجازی آرایش جنگی گرفته؛ در مقابل این دشمنی که آرایش جن گی در مقابل ملت ایران گرفته، ملت ایران ... باید خودش را آماده کند» (۱۳۹۸/۰۲/۱۱)؛
- «ما نمی‌گوییم این راه را ببندید؛ نه، اینکه بی‌عقلی است. یک ک سانی نش سته‌اند ... یک را هی باز کرده‌اند به‌عنوان فضای مجازی و به‌قول خودشان سایبری؛ ... از ا ین ا ستفاده کن ید منت ها استفاده درست بکنید؛ دیگران دارند استفاده درست می‌کنند؛ بعضی از ک شورها ط بق فره نگ خودشان این دستگاه‌ها را قبضه کرده‌اند، ما چرا نمی‌کنیم؟» (۱۳۹۵/۰۲/۱۳)؛
- «امروزه تهاجم فرهنگی با استفاده از ابزارها و فناوری‌های جدید ارتباطی، خیلی‌جدی ا ست ... نمی‌شود به همان روش‌های قدیمی خودمان اکتفا کنیم» (۱۳۸۵/۸/۱۷)؛
- «اینترنت یکی از نعم بزرگ الهی است، اما در عین حال یک نقمت بزرگ هم ه ست؛ یع نی یک چاقوی دو دم و خطرناک است» (۱۳۸۱/۹/۲۶)؛

همچنین از نگاه سلبی، انجام این پژوهش می‌تواند در موارد ذیل راهگشا باشد:

۱. جلوگیری از افزایش آسیب‌پذیری[1] در حوزه فضای مجازی
۲. افزایش بازدارندگی در صورت توجه به نقش پررنگ مردم در دفاع سایبری
۳. ارتقاء نگاه جامع، سیستمی و پیش‌دستانه در مقابل تهدیدهای سایبری
۴. هماهنگی و همسویی مردم با متولیان امر فضای مجازی
۵. افزایش «نظم و ثبات سیا سی»[1] به‌وا سطه آ گاهی و شناخت مردم از ماه یت تهد یدها در بحران‌های امنیتی و حمایت از حاکمیت

1 Vulnerability

ادبیات و مبانی نظری

پیشینه

آقایان فروزان و احمدی‌مقدم(۱٤۰۱) در مقاله‌ای به موضوع «پدافند مردم‌محور در برابر شبکه های اجتماعی مجازی» پرداخته و نشان می‌دهند که متناسب با قابلیت این شبکه‌ها، می توان مجموعه‌ای از اقدامات پدافند مردم‌محور را برای مقابله با تهدیدات نوین، تضعیف باورها و اعتقادات مردم، جلوگیری از هویت زدایی و کاهش ضریب نفوذ شبکه‌های اجتماعی مجازی در میان خانواده های ایرانی استفاده نمود.

آقایان فتوح‌آبادی و صادقی(۱۳۹۹) در مقاله خود به موضوع «تأثیرات اعتیاد های دیجیتال در فضای مجازی بر امنیت‌ملی در حوزه فرهنگی» پرداخته و راهکار هایی را جهت خنثی سازی مضرات اعتیاد به فضای مجازی در حوزه فرهنگی ارائه نموده‌اند که از مهم‌ترین آن ها می توان به تقویت شبکه‌های اجتماعی بومی منطبق‌بر فرهنگ ایرانی اسلامی اشاره کرد.

آقایان محمودزاده و اسماعیلی(۱۳۹۷) در مقاله‌ای به تدوین الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح پرداخته و مهمترین مؤلفه‌ها را در ابعاد مختلف بدین شرح شناسایی نمودند: الف) بُعد عوامل اصلی فضای سایبری؛ شامل داده ها و اطلاعات، کاربران، شبکه و زیر ساخت، خدمات و نرم‌افزار. ب) بُعد اهداف امنیتی فضای‌سایبری؛ شامل محرمانگی، یکپارچگی و صحت، دسترسی پذیری، احراز هویت، انکار ناپذیری و حفاظت از حریم خصوصی سازمان. ج) بُعد اقدامات و راهکار های صیانت امنیتی؛ شامل شناسایی منابع و دارایی های سایبری، محافظت، تشخیص و کشف، تحلیل، پاسخ و واکنش، بازدارندگی، بازیابی، مقابله مؤثر، نوآوری و تحول.

1 Political Order and Stability

ملائی و همکاران(۱۳۹۷) در مقاله‌ای، الگوی بازدارندگی در فضای سایبر را برمبنای نظریه بازی ها تدوین نموده و راهبرد هایی را برا ساس و ضعیت های توازن، مناز عه، سلطه بازدار نده، سلطه تهدیدکننده و ضرر متقابل درجهت بازدارندگی ارائه نموده‌اند.

واحدی و صنیعی(۱۳۹۲) در پروژه تحقیقاتی خود به موضوع امنیت ملی در فضای سایبر پرداخ ته و به این نتیجه رسیدند که تاکنون تعریف قابل‌قبول و کاملی برای فضای سایبر از سوی سازمان های متولی بیان نشده است و اجماع واحدی وجود ندارد؛ بهره برداری از ف ضای سایبر در ا ین شرایط انتخابی نیست بلکه اجباری است و باید با توجه به نقش فضای سایبر در کل یه فعالیت های مو جود در فضای حقیقی و طرح‌ریزی و مدیریت هو شمند از آن بهره برداری کرد. محق قین، یاف ته ها را در دوبخش مؤلفه‌های حفظ و تحکیم امنیت ملی و مؤلفه‌های کاهش امنیت م لی در ف ضای سایبر طبقه‌بندی نموده‌اند.

آقایان مهری و صانعی(۱۳۹۰) نیز در مقاله‌ای به موضوع اینترنت و جنگ نرم پرداخته و کارکرد های جنگ سایبری در حوزه نرم را شبکه‌سازی به مع نای تعا مل ا فراد باهم در اینتر نت، گردش آزاد اطلاعات، فرهنگ‌سازی، جریان‌سازی به‌معنای هدایت افکار ع مومی در ت صمیم‌گ یری ها کن ترل و نظارت بر آن دانسته‌اند.

در پژوهش دیگری که توسط حاذق‌نیکرو(۱۳۹۰) انجام شد، وی به این نتیجه رسید که ن ظام سلطه با راه‌اندازی وبلاگ‌ها و بهره‌گیری از وب۲[1] توان ست در ناآرامی های پس از انتخا بات در ا یران از طریق دادن آموزش، اطلاع‌رسانی، هماهنگی و عملیات روانی، تأثیرگذاری داشته باشد.

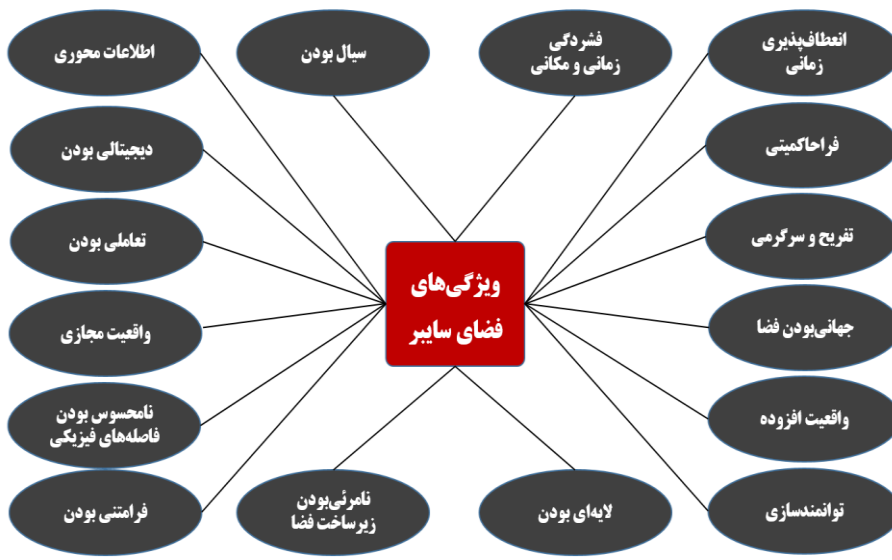
مفاهیم و تعاریف

ویژگی‌های فضای سایبر

فضای سایبر با گسترش روزافزون اینترنت، با هر پدیده عادت شده‌ای که بر خورد می‌ک ند و یا منجر به تغییر ماهوی و بنیادی‌اش می‌شود ویا دست‌کم تغییراتی را در آن پدیده ایجاد خوا هد کرد.

1 Web2

مفهوم روزنامه، خبرگزاری، ارتباطات اجتماعی، خریدوفروش، جهانگردی، آموزش، جنگ، عوامل تشکیل‌دهنده قدرت و حوزه های متنوع دیگر از سانی، قبل و بعد از عمومی شدن اینترنت و فضای سایبر، تغییر یا تحول پیدا کرده‌اند. این تغییر و تحول، از صفات فضای سایبر و ویژگی های آن نشأت می‌گیرد که در شکل زیر، به برخی از آنها اشاره شده است:



شکل(۱): ویژگی‌های فضای سایبر (محقق ساخته)

تهدید

هر عنصر یا وضعیتی که موجودیت منافع یا ارزش های حیاتی[1] سازمان را به خطر اندازد، تهدید محسوب می‌شود (حسن‌بیگی، ۱۳۹٤: ۳۰۹). در واقع، این تصور ناشی از این احساس است که ارزش‌های اساسی و مورد احترام، مورد خطر جدی یا نابودی قرار می‌گیرد.

1 Vital Interests or Values

تهدید در فضای سایبر

فضای سایبرالکترونیک را می‌توان سرزمینی غیرفیزیکی[1] و واقعیتی مجازی[2] دانست که شامل مجموعه‌ای از رایانه‌ها و شبکه‌هاست که به‌منظور استفاده از اطلاعات و بهره‌برداری از انواع سامانه‌های به‌هم پیوسته و زیرساخت های الکترونیکی به‌وجود آمده است بنابراین این فضا، محتوا و الزامات خاص خود را دارد.

فضای مجازی، بستری را فراهم آورده که ضمن عبور از محدودیت های فضای واقعی از قبیل محدودیت‌های زمانی، جغرافیایی، سیاسی، فرهنگی و...، افراد مختلف امکان برقراری ارتباط را با یکدیگر دارند و می‌توانند کسانی را بیابند که علایق مشترکی با آن ها دارند لیکن ممکن است به لحاظ مکانی و زمانی، در دنیای واقعی هرگز نتوانند با آنها ارتباط پیدا کنند.

فضای مجازی با قدرت تأثیرگذاری بالایی که می‌تواند در اذهان، باور ها، عقاید و ارزش های یک جامعه داشته باشد، از طریق تسهیل جامعه‌پذیری[3] و انتقال فرهنگ بین نسلی[4] و ایجاد انسجام و همبستگی[5] بین افراد جامعه، به‌عنوان حلقه ارتباط مؤثر بین جامعه و حاکمیت نقش‌آفرینی می‌نماید. همین نقش مهم است که باعث می‌شود فضای مجازی ظرفیت بروز تنش‌ها، بحران‌ها و چالش های اجتماعی، فرهنگی، سیاسی و امنیتی را در سطح جامعه دارا باشد.

تهدید در فضای سایبر، همزمان با تحول و انقلاب در حوزه فناوری اطلاعات و گسترش ارتباطات‌جهانی ازطریق اینترنت تحت‌تأثیر جهانی شدن، در سراسر جهان به‌وجود آمده و آن را می‌توان بخشی از جنگ‌های اطلاعاتی دانست که با اقدام های خرابکارانه در دنیای سایبری به‌وقوع می‌پیوندد. این اقدامات ممکن است از طریق فضای مجازی عمل کند و یا به نحوی با آن مرتبط باشد.

1 Non-Physical
2 Virtual Reality
3 Socialization
4 Intergenerational Culture Transfer
5 Correlation

ابعاد تهدید در فضای سایبر(نرم و سخت)

تهدید نرم را «اقدامی پیچیده و پنهان، متشکل از عملیات های سیا سی، فرهن گی و اطلا عاتی برای ایجاد تغییر های موردنظر در جام عه هدف» می‌دان ند (ابراهیم یان و هم کاران، ۱۳۹٤)؛ دروا قع، تهدید نرم شامل تمامی اعمال نرم‌افزارانه علیه جامعه هدف است مانند رسانه‌ای، روا نی و تبلیغاتی. در جدول زیر، به جنبه‌های مختلف اعمال قدرت و اراده در تهدیدهای سایبری اشاره شده است:

جدول(۱): جنبه‌های مختلف اعمال قدرت و اراده در تهدیدهای سایبری

وجه اول: قدرت «الف»، قدرت «ب» را وادار به کاری می‌کند که خود «ب» در حالت عادی آن را انجام نمی‌داد.	
قدرت نرم	برنامه‌های تبلیغاتی برای تغییر سلایق اصلی هکرها، جذب اعضای سازمان‌های تروریستی
قدرت سخت	تهدیدهای انکار سرویس، جاسازی بدافزارها، دستگیری وبلاگ‌نویسان
وجه دوم: قدرت «الف»، با کار گذاشتن راهبردهای قدرت «ب»، وی را از انتخاب منع می‌کند.	
قدرت نرم	واپایش فراهم کنندگان خدمات اینترنت و موتورهای جستجو
قدرت سخت	دیواره‌های آتش، فیلترها و وارد کردن فشار برای کنار گذاشتن برخی عقاید
وجه سوم: قدرت «الف»، سلایق قدرت «ب» را به گونه‌ای شکل می‌دهد که برخی از راهبردها مطرح هم نمی‌شود.	
قدرت نرم	انتشار اطلاعات برای ایجاد سلایق و اولویت‌ها(تحریک ملی‌گرایی) به‌وجود آوردن هنجارهای انزجار(هرزه‌نگاری کودکان)
قدرت سخت	تهدید به تنبیه و مجازات وبلاگ‌نویسانی که مطالب سانسور شده را منتشر می‌کنند.

(Nye, 2010: 7)

برخی از تهدیدهای سایبری که می‌توا ند امنیت م لی جم هوری ا سلامی ا یران را در حوزه نرم مورد تهدید قرار دهد عبارتند از:

۱. سعی در جهت‌دهی[1] به اف کارعمومی به‌من ظور ت ضعیف امنیت سیا سی با ا ستفاده از اعتراض‌های خیابانی، شورش و اعتصاب‌های سراسری

1 Orientation

۲. اخلال در امنیت اجتماعی از طریق عادی‌سازی روابط اجتماعی نامعقول و نقض حقوق شهروندی
۳. تضعیف امنیت فرهنگی با کمرنگ نمودن رعایت موازین شرعی در جامعه و جلوگیری از عدم الترام به فرهنگ اسلامی
٤. گردآوری اطلاعات اقلیمی و قومی و بهره‌برداری از آنها در بحران‌های اجتماعی
٥. تضعیف اعتقادها و ایجاد شبهه‌های فکری در میان جامعه
٦. رواج سطحی‌نگری فکری در برخورد با مسائل در میان افراد جامعه

به عبارت دیگر، هدف اصلی دشمن از تهدیدهای نرم را می‌توان ایجاد نارضایتی در جامعه از طریق اختلال در اداره امور کشور و سوءاستفاده از آن به‌منظور تغییر رفتار مردم یا حاکمیت، درجهت منافع استعماری و استکباری خود دانست.

ویژگی‌های تهدیدهای سایبری

مهمترین ویژگی‌هایی را که برای تهدیدهای سایبری می‌توان برشمرد، عبارتند از:

۱. تعدد بازیگران در فضای سایبری
۲. هزینه کم ورود، صرف زمان کم و سرعت بالای اقدام
۳. ناشناس ماندن بازیگران و عدم‌قابلیت ردیابی
٤. تأثیرگذاری شگرف
٥. کمرنگ شدن نقش جغرافیا
٦. ساختار فضای اینترنت
۷. پایین بودن احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری (خلیلی پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱).

حوزه‌های تهدید سایبری

حوزه‌های مختلف تهدیدهای سایبری متصور دشمن علیه کشورمان عبارتند از «جاسوسی سایبری»، «خرابکاری سایبری»، «آسیب‌پذیری‌های سیاسی» و «مجرمان و عوامل ناراضی» که در شکل زیر به تفکیک اهداف و ابزار مورد استفاده به‌خوبی نشان داده شده است:

شکل(۲): حوزه‌های تهدید فضای سایبری کشور (محمودزاده و اسماعیلی، ۱۳۹۷)

دفاع سایبری

دفاع سایبری را مجموعه‌ای از اقدامات بازدارنده و بازیابی کننده می‌دانند که به‌منظور پیشگیری، حفظ و حمایت از ارزش‌ها و منافع ملی درمقابل تهدیدها و حملات سایبری صورت می‌پذیرد و شامل نهادهای دولتی، سازمان‌های مردم‌نهاد، مردم و فرایندها و روابط میان آنهاست.

دفاع سایبری به‌مثابه مفهومی پیچیده، بسترها و موضوعات به شدت دگرگون شونده‌ای دارد که فهم آن، مستلزم درک ابعاد و رابطه آن با انسان به‌لحاظ هستی شناختی است. لیکن، در حالی که منطق جدید امنیت سیستمی، نیازمند تنوع و حتی شاید انفکاک جدی است، گرایش و سیع در فناوری اطلاعات به‌سمت «*همگرایی موجودیت انسانی و رایانه‌ها است*». این هم‌آمیختگی هستی‌شناسانه، ناشی‌از گره خوردن همه ابعاد زندگی انسانی با اینترنت و شبکه های رایانه‌ای است (هرینگتون و آلدریچ[1]، ۲۰۱۳: ۳۰۶).

1 Herrington & Aldrich

پنج قلمرو قدرت یعنی سرزمین، آب، هوا، فضا و فضای سایبر، تولید و کسب منافع و نفوذ را میسر می‌سازند که امروزه فضای سایبر پیشگام گسترش قدرت دیپلماسی، اطلاعاتی، نظامی و اقتصادی است و تمام انواع واحدها(دولت ها، شرکت ها، تروریست ها، سازمان های جنایی و گروه‌های غیرانتفاعی)، همگی فعالیت‌های خود را در بستر فضای سایبر به پیش می‌برند (راولند[1]، ۲۰۱٤: ٤). اینجاست که سامان دادن به دفاع سایبری، به‌عنوان یکی از مهمترین اولویت های زندگی نه‌تنها در بعد سیاسی بلکه در کلیه ابعاد زندگی بشری رخ می‌نماید.

اهداف کلان دفاع سایبری کشور

اهداف کلان زیر را برای دفاع سایبری در کشور می‌توان برشمرد:

۱. ارتقای آمادگی دفاعی و بازدارندگی کشور در مقابل تهدیدات و حملات سایبری کشورهای متخاصم.
۲. طراحی، پیاده‌سازی و اجرای سامانه جامع رصد، پایش، مراقبت، کنترل و تشخیص و هشدار تهدیدات سایبری.
۳. حفاظت، صیانت و پایدارسازی سرمایه‌های سایبری کشور در مقابل تهدیدات و حملات سایبری دشمنان
٤. آموزش، تربیت و توانمندسازی سرمایه‌های انسانی کارآمد متناسب با اقتضائات حال و آینده پدافند سایبری.
٥. تولید، مدیریت و بومی‌سازی دانش پدافند سایبری با بکارگیری ظرفیت‌های ملی.
٦. سازماندهی، آموزش، هدایت، کنترل و ارزیابی‌مداوم دستگاه‌های کشور در راستای ارتقای کارایی دفاعی و نیل به بازدارندگی پدافندی
۷. فرهنگ سازی، آموزش عمومی، سازماندهی، تمرین و رزمایش و تولید آمادگی پدافندسایبری (سند راهبردی پدافند سایبری کشور، ۱۳۹٤).

1 Rowland

مراحل دفاع سایبری

همواره اشکال متفاوت دفاعی در برخورد با فعالیت‌های دشمن در یک فضای سایبر و جود دارد که به شرح مختصری از آن‌ها اشاره می‌شود:

جلوگیری؛[1] شناسایی راه‌های نفوذ، حمله و مقابله با آن‌ها جهت افزایش ضریب امنیت، ایمنی و پایداری می‌باشد.

مدیریت حادثه،[2] *محدود کردن خرابی‌ها*[3]*؛* راه‌هایی هستند که با استفاده از آن ها می توانیم اثر حملات صورت گرفته را در کمترین زمان کاهش دهیم.

تعیین آثار، نشانه‌ها و هشدارها؛ با شناسایی آثار یک حمله می‌توانیم از پیامدهای حملات دیگر و خطراتی که ممکن است ایجاد شوند، جلوگیری کنیم.

ایمن و پایدار کردن سامانه‌ها؛[4] جهت جلوگیری از نفوذ های بیرونی، ضروریست تا موانعی ایجاد کنیم که از قدیمی‌ترین موانع نفوذ، می توان به استفاده از کلمه عبور و راهکار های فیزیکی مناسب و پایدار جهت ایمن نمودن مراکز داده اشاره نمود.

خاموشی و تخصیص مجدد؛[5] در این شیوه بایستی سامانه به‌طورکامل یا جزئی خاموش شود و دوباره تخصیص مجدد شود. سامانه‌ای که متوجه شود تحت یک حمله قرار دارد، باید موانع و دفاع‌هایی را از خود بنا نهد که شاید در مواقع عادی از آنها استفاده نمی‌کند و سعی نماید قسمت‌هایی از سامانه را که با حمله مواجه شده‌اند، ایزوله کند. البته مراحل خاموش کردن و تخصیص‌دهی مجدد باید به‌صورت بلادرنگ[6] و به سرعت انجام گیرد.

1 Prevention
2 Incident Management
3 Damage Limitation
4 Harden the System
5 Shutdown and Reallocation
6 Real Time

پشتیبانی؛[1] بسیاری از حملات، به کندی و به طور محرمانه، مشکلات زیادی را نسبت به زمانی که اطلاعات سالم بودند، ایجاد می‌کنند و باید همواره از اطلاعات جمع‌آوری شده، قبل از هر حمله‌ای پشتیبانی کنیم؛ این تاکتیک از طریق تهیه نسخه پشتیبان از اطلاعاتی که ذخیره شده‌اند، به دست می‌آید (اقتباس از ایزایران، ۱۳۹۰: ۲۰-۱۷).

روش شناسی

تحقیق حاضر از لحاظ نوع هدف، کاربردی و از لحاظ روش، توصیفی-تحلیلی است. بدین‌منظور، پس از مرور ادبیات و مطالعه اسنادی(کتابخانه‌ای)، برای جمع‌آوری داده ها از ابزار مصاحبه عمیق ساختارنیافته با افراد جامعه نمونه استفاده شد و تجزیه و تحلیل داده‌ها با بهره‌گیری از روش تفسیری صورت پذیرفت.

جامعه آماری

از آنجا که در نظر است نظرات خبرگان و مطلعان حوزه سایبر مورد مطالعه قرار گیرد، جامعه آماری مورد نظر این تحقیق را پژوهشگران و محققان فعال در مراکز تحقیقاتی و پژوهشی نظامی سطح شهر تهران و دانشجویان و فارغ‌التحصیلان دانشگاه عالی دفاع ملی که در حوزه سایبر (امنیت و دفاع فضای سایبر) مشغول تحصیل هستند، تشکیل می‌دهند.

حجم نمونه

حجم نمونه براساس روش نمونه‌گیری گلوله برفی و به‌صورت هدفمند بوده و پاسخگویانی که برای مشارکت در تحقیق معرفی و برگزیده می شوند، خود در انتخاب پاسخگویان بعدی نقش دارند و این عمل تا آنجا ادامه می‌یابد که اشباع نظری در داده های بدست آمده در تحقیق حاصل شود.

1 Backup

تجزیه و تحلیل

خلاصه وضعیت افراد مصاحبه شونده به شرح جداول زیر می‌باشد:

جدول(۲): وضعیت تحصیلی افراد مصاحبه شونده

مدرک تحصیلی	تعداد
دکتری	۱۲
دانشجوی دکتری	۹
کارشناس‌ارشد	٤

جدول(۳): سابقه شغلی افراد مصاحبه شونده

مدرک تحصیلی	تعداد
کمتر از ۱۰سال	۲
۱۰-۱۵سال	٦
بالاتر از ۱۵سال	۱۷

جدول(٤): وضعیت اشتغال افراد مصاحبه شونده

مدرک تحصیلی	تعداد
مراکز دانشگاهی و تحقیقاتی	۱۳
مراکز امنیتی	٤
مراکز نظامی	۸

پس از انجام مطالعات کتابخانه‌ای و اسناد بالادستی حوزه دفاع سایبری، سؤالات مصاحبه با محوریت مفاهیم اصلی تحقیق همچون فضای مجازی، دفاع سایبری و مشارکت مردمی طراحی و با افراد جامعه نمونه مصاحبه به عمل آمد. پس‌از اتمام مصاحبه ها و دریافت نظرات خبرگانی، متن مصاحبه‌ها با روش های علمی مورد تفسیر و تبیین قرار گرفت و نتایج آن در دو بخش دیدگاه‌ها و راهکارهای کاربردی احصاء گردید:

بخش اول: دیدگاه‌ها

دیدگاه‌های استخراج شده خبرگان و مصاحبه شوندگان پیرامون موضوع فضای مجازی و دفاع سایبری مردم‌پایه را می‌توان در دو دسته کلی تقسیم‌بندی نمود:

۱) ظرفیت‌ها و ویژگی‌های فضای مجازی که بایستی در سیاستگذاری های دفاع سایبری موردتوجه قرار گیرد:

- تأثیری که امروزه فضای مجازی و رسانه‌های اجتماعی مجازی در مسائل بین‌المللی و سیاسی دارند، از میزان تأثیر موشک و زرادخانه‌های هسته‌ای بیشتر است.
- امروزه با گسترش فناوری‌های نوین می‌توان این ادعا را مطرح کرد که فضای مجازی به مراتب بزرگ‌تر و گسترده‌تر از فضای زندگی حقیقی انسان‌ها شده است.
- باید در جامعه این نگاه حاکم شود که فضای مجازی و فناوری های دیجیتال جزو متغیرات زندگی بشری است و نه عناصر تعیین‌کننده آن.
- تأثیرات شگرف فضای مجازی بر تمامی ابعاد زندگی انسان ازقبیل اجتماعی، فرهنگی، سیاسی، اقتصادی، دفاعی و... در عرصه‌های ملی و بین‌المللی بر کسی پوشیده نیست.
- در فضای مجازی، مرزهای سرزمینی معنا ندارد و بی‌مرزی بر آن حاکم است.
- فضای به‌قدری مجازی با زندگی حقیقی درآمیخته که تمام شئونات زندگی انسان ها را در برگرفته است.
- فضای مجازی ابزاری برای تسهیل در دستیابی به دستاوردهای علمی دنیاست.
- فضای مجازی بر روی افکار عمومی و تصورات ذهنی جامعه، تأثیر گسترده و بالایی دارد.
- فضای مجازی ظرفیت و امکان هدایت و پرورش انسان‌ها را دارد.
- فضای مجازی می‌تواند ابزار خوبی برای تبلیغ فرهنگ اسلامی-ایرانی و گسترش موضوع مهدویت در دنیا باشد.
- مبدأ و سررشته تحولات جهانی را در کارکرد فضای مجازی می‌توان دید.

- مهم‌ترین قابلیت و کارکرد فضای مجازی را می‌توان ارتباط با مسائلِ دور از محیط نزدیک دانست.
- مهمترین کارکرد و نقش فضای مجازی، استفاده به‌عنوان ابزار ارتباطی و انتقال‌دهنده فوری پیام در میان انسان‌هاست.
- نباید در جامعه از فضای مجازی به‌عنوان جایگزین مراجع معتبر آموزش های علمی و اسلامی استفاده شود.

۲) آسیب‌ها، معضلات و چالش‌های فضای مجازی که در سیاست های دفاع سایبری باید مورد توجه قرار گیرد:

- از فضای مجازی به‌عنوان ابزاری برای جهانی سازی براساس شیوه و تفکرات سبک زندگی غربی و سکولار استفاده می‌شود.
- از فضای مجازی و شبکه‌های اجتماعی مجازی به‌عنوان ابزاری برای القای بحران، بن‌بست و سیاه‌بودن وضعیت جامعه بهره‌برداری می‌شود.
- از فضای مجازی و شبکه های اجتماعی مجازی در جامعه به‌عنوان ابزاری برای التهاب‌آفرینی و شبهه‌افکنی استفاده می‌شود.
- استفاده از بی‌رویه و خارج از عرف از شبکه‌های اجتماعی مجازی، تمایلات فردبه فرد یا رو در رو را به شدت کاهش داده و باعث آسیب رساندن به ارتباطات اجتماعی سالم در جامعه می‌شود.
- استفاده از فضای مجازی به‌منظور سرقت، تخریب و حملات سایبری می‌تواند صدمه، آسیب و خسارت‌های غیرقابل جبرانی را به اقتصاد ملی وارد کند.
- افزایش جرائم رایانه‌ای در جامعه کاهش اقتدار نیروی انتظامی و افزایش هزینه های پلیسی در جامعه را به‌دنبال خواهد داشت.
- تخریب وجهه سیاسی و امنیتی کشور از طریق هک نمودن سایت‌های رسمی، یکی از اقدامات متصور دشمن در فضای مجازی است.

- تهاجم فرهنگی با محتواهای فریبنده و تبلیغ علیه نظام اسلامی، یکی از کارکردهای منفی فضای مجازی است.
- دشمن به دنبال نشان دادن کاهش امنیت فضای مجازی در کشور است تا اعتماد و اطمینان مردم را به حاکمیت و خدمات دولت الکترونیک از بین ببرد.
- رصد، پایش و فیلترینگ فضای مجازی ضرورتی عقلی است.
- فاش شدن اطلاعات محرمانه کاربران در فضای مجازی منجر به از بین رفتن امنیت اطلاعات و نقض حریم خصوصی افراد و سازمان‌ها در جامعه خواهد شد.
- فضای مجازی با ابزارهای اغواکننده‌ای که دارد، اگر در مسیر درست و صحیح هدایت نشود، سست‌کننده ایمان و انگیزه‌های معنوی در کشور است.
- فضای مجازی با فراهم آوردن زمینه رقابت بی‌پایان برای به‌دست آوردن لایک بیشتر و کامنت‌های متعدد، ضمن افزایش احساس «نیاز به توجه»، این قابلیت را دارد که زندگی افراد را به نابودی بکشاند.
- فضای مجازی با کمک به دشمن از طریق بدافزارها و تخریب‌کننده‌های زیر ساختی، فضای جنگی جدیدی را در مقابل کشور گشوده است.
- فضای مجازی با منحرف کردن جوانان از مسیر تلاش و پشتکار در جهت دستیابی به مهارت‌های لازم برای رسیدن به اهداف عالی و واقعی، آنها را به سمت ستاره شدن در دنیای مجازی و شبکه‌هایی مثل فیس‌بوک و اینستاگرام و... تبدیل می‌کند.
- فضای مجازی و اینترنت ابزاری برای تهاجم شناختی و فکری است.
- کنترل محتوای فضای‌مجازی و شبکه‌های‌اجتماعی مجازی دراختیار جبهه سرمایه‌داری و شبکه صهیونیسم جهانی است.
- کور کردن خلاقیت و ابتکار یکی از تأثیرات منفی گشت‌وگذارهای بی هدف در شبکه‌های اجتماع مجازی است.

بخش دوم: راهکارهای کاربردی

در این بخش، راهکارهای کاربردی استخراج شده که با دخالت مستقیم مردم می‌تواند درتقو یت دفاع سایبری مؤثر باشد، آورده شده است:

- ارتباطات بی‌سیم و مبتنی بر وای‌فای، از امنیت بالایی برخوردار نبوده و قابلیت هک و شنود دارند و بهتر ا ست به‌هن گام ا ستفاده از اینتر نت، از ارتبا طات اینترن تی با سیم استفاده شود.
- ارتقاء آگاهی و فرهنگ صحیح ا ستفاده از شبکه های اجت ماعی م جازی را در م یان فرزندان، خانواده و جامعه گسترش دهیم.
- از آنجا که حضور فعال و مستمر در فضای مجازی، زمینه بسیاری از جرائم و ناامنی ها را فراهم می‌آورد، بهتر ا ست از گ شت‌و گذارهای بی هدف در ف ضای م جازی پرهیزکنیم.
- از بازکردن رایانامه‌های ناشناس و هرزنامه‌ها به‌دلیل امکان انتشار ویروس های م خرب و آلوده نمودن سیستم، اجتناب کنیم.
- از نصب نرم‌افزارهای نامطمئن بر روی سیستم‌ها به دلیل احتمال سرقت اطلاعات و یا فراهم نمودن امکان دسترسی غیرمجاز به دیگران (ایجاد رخنه) خودداری نماییم.
- استفاده از سامانه‌های رایانامه بومی برای انتقال امن اطلاعات، توصیه می‌شود.
- استفاده از ظرفیت سازمان‌های مردم‌نها و ب سیج مرد می در همرا هی با سازمان ها و دستگاه‌های متولی امر، نیروی مضاعفی در مقابله با تهد یدات ف ضای م جازی ای جاد خواهد نمود.
- استفاده از ظرفیت‌های بالقوه و بالفعل اجتماعی و فرهنگی کشور یکی از اقدامات مؤثر در جهت حفظ و ارتقای هویت ملی در فضای مجازی و جلوگیری از رواج فرهنگ غرب‌گرایی و سکولار است.
- اهتمام به تولید و نشر محتوای فرهنگی مناسب نسل جوان در فضای مجازی، می‌توا ند در جلوگیری از تغییر علائق و ذائقه فرهنگی آنها نقش مؤثری ایفا کند.

- اینترنت و فضای مجازی، مکانی عمومی است و نباید اطلاعات خصوصی و محرمانه خود را در آن به اشتراک بگذاریم.
- با اطلاع‌رسانی صحیح و به‌هنگام از طریق مراجع رسمی و رسانه ملی، می‌توان افکارعمومی جامعه را در ناآرامی‌های اجتماعی مدیریت نمود و از التهاب آفرینی و شبهه‌افکنی دشمنان در فضای مجازی، جلوگیری کرد.
- برای جستجو در اینترنت از موتورهای جستجوگر ملی و بومی استفاده کنیم.
- بصیرت‌افزایی و ارتقای سواد رسانه‌ای مردم یکی‌از کارآمدترین شیوه‌های پیشگیری از انتشار اخبار جعلی و جریان‌سازی گمراه‌کننده و با نیات سوء در فضای مجازی است.
- به هنگام استفاده از فضای‌مجازی، کلمات عبوری را انتخاب کنیم که از پیچیدگی کافی برخوردار بوده و در بازه‌های زمانی متفاوت نسبت به تغییر آنها اقدام نماییم.
- پشتیبان گیری مرتب و به‌روز نگه‌داشتن نسخه پشتیبان از اطلاعات و داده‌ها، می‌تواند در ازدست نرفتن اطلاعات حیاتی‌ومهم و پیشگیری از خسارات‌ولطمات جبران‌ناپذیر مؤثر باشد.
- حمایت مادی، معنوی و قانونی از متخصصان و شرکت‌های دانش‌بنیان مرتبط با حوزه بومی‌سازی و مقابله با تهدیدات متصور شبکه‌های اجتماعی مجازی
- در استفاده از فضای مجازی، عمل به شیوه‌نامه‌ها و دستورالعمل های صیانتی امنیت فضای تبادل اطلاعات(افتا) اکیداً توصیه می‌گردد.
- شبکه‌های اجتماعی بومی و مبتنی بر شبکه اطلاعات ملی را در اولویت استفاده قرار دهیم.
- ممکن است دشمن اطلاعات نادرست و یا جهت‌داری را در موضوعات پرطرفدار و مورد علاقه ما به‌ویژه در بحران‌ها و ناآرامی‌های اجتماعی منتشرکند، بنابراین نباید در فضای مجازی هرآنچه را می‌خوانیم، باور کنیم.
- والدین باید در استفاده از اینترنت، به اشتراک گذاری اطلاعات و ارسال محتوا بر روی فرزندان خود کنترل لازم را اعمال نمایند و آن ها را بدون مراقبت در فضای مجازی رها نکنند.

نتیجه‌گیری و پیشنهاد

نتیجه‌گیری

نقطه مقابل نفوذ فضای سایبر و گسترش فضای مجازی در بسیاری از لایه های زندگی بشر، فراهم‌شدن بستری جدید برای بروز آسیب پذیری و تهدید در میان جوامع مختلف است. انقلاب اسلامی ایران با به چالش کشیدن ارزش‌ها و معیارهای غربی و عدم وابستگی به استعمار و قدرت‌های جهانی، الگوی سیاسی نوینی را در جهان ایجاد نمود و نظام سلطه که این موضع را برخلاف اهداف استکباری خود دید، پس از ناتوانی در براندازی نظام اسلامی در جنگ سخت، به دنبال براندازی از طریق جنگ نرم برآمد که یکی از جلوه‌های آن، در فضای مجازی و حملات سایبری، بروز و ظهور پیدا کرده است.

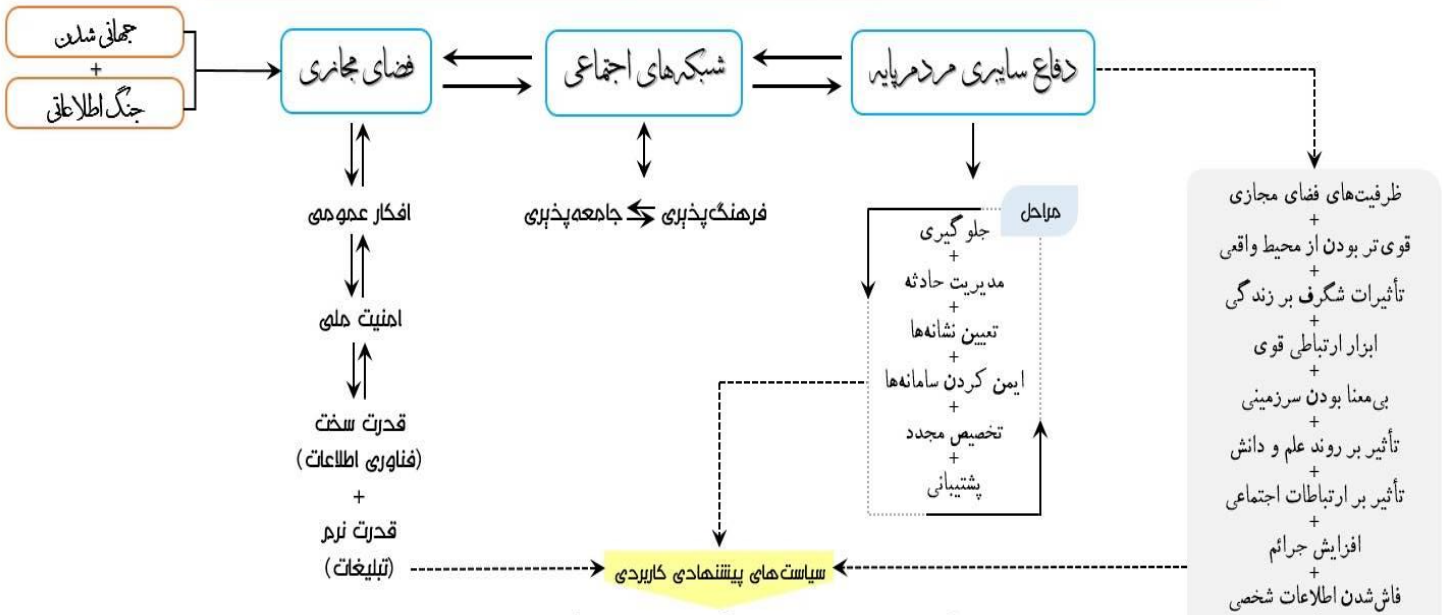
براین اساس، بهره برداری از این فضا توسط دشمنانی که امنیت، اقتدار و ثبات ج.ا. ایران را نشانه گرفته‌اند، دفاع سایبری را امری حیاتی و اجتناب‌ناپذیر ساخته است. یافته های پژوهش نشان می‌دهد که احتمالاً با اقدامات مردم‌پایه و مردم‌محور در کنار آموزش سواد رسانه‌ای و ارتقای آگاهی و بصیرت افزایی، ضمن پیشگیری از سطحی‌نگری در مواجهه با رویدادهای فضای مجازی، بتوان به‌جای برخورد حذفی با فضای مجازی، از پیامدهای منفی آن جلوگیری کرد (رجوع به الگوی مفهومی).

پیشنهادها

- ارتقاء سطح آگاهی و سواد رسانه‌ای مرتبط با امنیت فضای مجازی در جامعه
- توجه به آموزش و فرهنگ‌سازی جامعه در راستای حفظ حریم عمومی و خصوصی در فضای مجازی به‌هنگام نشر محتوا به‌منظور پیشگیری از گسترش فساد اخلاقی و سایر تهدیدات امنیتی متصور
- سیاست‌گذاری فرهنگی در تولید محتوای متناسب با فرهنگ اسلامی–ایرانی به جای مصرف محتوای غیربومی و مخرب فرهنگی

الگوی مفهومی مقاله نقش فضای مجازی در ارتقای توانمندی دفاع سایبری مردم‌پایه

امروزه تهاجم فرهنگی با استفاده از ابزارها و فناوری‌های جدید ارتباطی، خیلی‌جدی است. مقام معظم رهبری(مدظله‌العالی)



منابع

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

ابراهیمیان، بهمن؛ توشه، علی و پورهادی، ابراهیم، (۱۳۹٤)، **راهکارهای مقابله با تهدیدهای سایبری علیه ج.ا.ا با تأکید بر نقش فناوری و منابع انسانی**، فصلنامه راهبرد دفاعی، سال سیزدهم، شماره۲(پیاپی۵۰)، صفحات۱۱۵-۸۷

حاذق‌نیکرو، حمید، (۱۳۹۰)، **نقش اینترنت در ناآرامی‌های پس از انتخابات دهمین دوره ریاست جمهوری در ایران**، فصلنامه عملیات روانی، سال نهم، شماره٤(پیاپی ۳۱)، صفحات۸۸-٤۸

حسن‌بیگی، ابراهیم، (۱۳۹٤)، **مدیریت راهبردی**، چاپ دوم، تهران: انتشارات سمت

خلیلی‌پور رکن‌آبادی، علی و نورعلی‌وند، یاسر، (۱۳۹۱)، **تهدیدات سایبری و تأثیر آن بر امنیت ملی**، فصلنامه مطالعات راهبردی، سال پانزدهم، شماره۲(پیاپی٥٦)، صفحات۱۹٦-۱٦۷

سندراهبردی پدافندسایبری کشور، (۱۳۹٤)، سازمان پدافندغیرعامل کشور ومرکز پدافندسایبری کشور

فتوح‌آبادی، وحید و صادقیان، علی، (۱۳۹۹)، **بررسی تأثیرات اعتیادهای دیجیتال در فضای مجازی بر امنیت ملی در حوزه فرهنگی و ارائه راهکارهایی جهت خنثی‌سازی**، فصلنامه آماد و فناوری دفاعی، سال سوم، شماره۲(پیاپی٦)، صفحات۱۷۰-۱٤۹

فروزان، حمید و احمدی‌مقدم، اسماعیل، (۱٤۰۱)، **پدافند مردم‌محور در برابر شبکه های اجتماعی مجازی**، فصلنامه آماد و فناوری دفاعی، سال پنجم، شماره۳(پیاپی۱۵)، صفحات۱۸۵-۱۳۳

محمودزاده، ابراهیم و اسماعیلی، کیوان، (۱۳۹۷)، **الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح**، فصلنامه امنیت ملی، سال هشتم، شماره٤(پیاپی ۳۰)، صفحات۲۳۷-۲۰۳

ملائی، علی؛ کارگری، مهرداد؛ خرا شادی‌زاده، محمدر ضا، (۱۳۹۷)، **الگوی بازدارندگی در فضای سایبر براساس نظریه بازی‌ها**، فصلنامه امنیت ملی، سال هشتم، شماره۳(پیاپی۲۹)، صفحات ۱۷۱-۱۴۱

مهری، عباس و صانعی، یدا له، (۱۳۹۰)، **بهره‌گیری غرب از اینترنت در جنگ نرم علیه ج.ا.ا**، فصلنامه عملیات روانی، سال نهم، شماره٤(پیاپی ۳۱)، صفحات ۷٤-٤

مؤسسه ایزایران، (۱۳۹۰)، **پدافند غیرعامل در حوزه جنگ‌سایبر**، تهران: مرسسه آموزشی تحقیقاتی وزارت دفاع

واحدی، مرتضی و صنیعی، محمدحسین، (۱۳۹۲)، **امنیت ملی در فضای سایبر**، پروژه تحقیقاتی پژوهشکده امنیت ملی و مطالعات راهبردی، تهران: دانشگاه عالی دفاع ملی

Ashton, Catherine, (2013), **Remarks by EU high representative at press conference on the launch of the EU's cyber security strategy**, Brussels: eeas, Europa, eu.

Herrington, L. & Aldrich, R., (2013), **the future of cyber-resilience in an age of global complexity**, Politics, 33(4), 299-310.

Rowland, J. Rice, M. & Shenoi, S., (2014), **the anatomy of a cyber power**, International Journal of Critical Infrastructure Protection, 7(1), 3-11.