فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره۳، تابستان ۱۴۰۱
مقاله اول، از صفحات ۷-۳۲

مقاله پژوهشی:

ارائه مدل مفهومی دفاع سایبریِ امنیت محورِ جمهوری اسلامی ایران

مجید حقی[۱] مهرداد کارگری[۲]

تاریخ دریافت: ۱۴۰۰/۰۳/۱۰ **تاریخ پذیرش:** ۱۴۰۰/۰۷/۱۶

چکیده

حرکت در مسیر ترقی، با تأکید بر فناوری اطلاعات، به‌عنوان انتخاب مشترک کشورها زمینه‌ای جدید برای رقابت بین کشورها و سازمان‌ها را فراهم آورده است. هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها، گروه های سازمان یافته و تروریستی و حتی افراد به این فضا وارد شده و تهدیدهایی همچون جنگ سایبری، تروریسم سایبری، جاسوسی سایبری،جرایم سایبری و مانند آن‌ها را به وجود آورند؛ ازاین‌رو فناوری اطلاعات و ارتباطات همچنان که عامل توانمندی و قدرت دولت‌ها و ملت‌هاست، عاملی تهدیدزا و مخاطره‌آمیز نیز می‌باشد.

پژوهش حاضر، باهدف ارائه مدل مفهومی دفاع سایبری کشور با محوریت ابعاد و مؤلفه‌های امنیت سایبری کشور، ضمن جستجو و شناسایی عوامل اثرگذار در دفاع سایبری کشور، دیدگاه‌های امنیت فضای سایبر کشور را نیز مورد بررسی قرار داده و با تجزیه‌وتحلیل داده‌های کیفی و تحلیل محتوا ابعاد، مؤلفه‌ها و شاخص‌ها قابل‌توجه را احصاء نموده و ضمن ارزیابی تأثیر آن‌ها بر یکدیگر و تجمیع یافته‌ها، مدل مفهومی موردنظر را ارائه می‌نماید.

کلیدواژه‌ها: ابعاد، مؤلفه و شاخص‌های امنیت سایبر، ابعاد، مؤلفه و شاخص‌های دفاع سایبر، امنیت سایبر، دفاع سایبری

۱ – دانش‌آموخته دکتری دانشگاه عالی دفاع ملی (نویسنده مسئول) mj_hagh12345@gmail.com
۲ – مدرس دانشگاه عالی دفاع ملی

مقدمه

در عصر اطلاعات شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی از قبیل اطلاع‌رسانی، داده‌ورزی، ارائه خدمات، مدیریت و کنترل و ارتباطات، از طریق سازوکارهای الکترونیکی و مجازی انجام می‌پذیرد؛ این فضا که از آن با نام «فضای تولید و تبادل اطلاعات» یاد می‌شود، در معرض چالش‌ها، آسیب‌ها و تهدیدهای گوناگونی نظیر ارتکاب جرائم سازمان‌یافته، تخریب بانک‌های اطلاعاتی، حملات مختل‌کننده خدمات، جاسوسی، خرابکاری، نقض حریم خصوصی و نقض حقوق مالکیت معنوی قرار دارد؛ به‌طوری که نپرداختن یا رویکرد نادرست به امنیت این فضا، مانعی بزرگ پیشروی گسترش کاربرد فناوری ارتباطات و اطلاعات و ورود به جامعه اطلاعاتی خواهد بود (سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور، ۱۳۸۷).

جنگ‌های قرن اخیر نشان می‌دهد که طراحان عملیات‌های نظامی از تمام ظرفیت‌های میادین نبرد حقیقی (هوا، فضا، زمین و دریا) برای نیل به پیروزی و تحمیل خسارت سنگین به طرف مقابل استفاده کرده‌اند. آنچه در دهه اخیر توجه فرماندهان نظامی را به خود جلب کرده، استفاده از ظرفیت‌های منحصربه‌فرد عرصه سایبری است که خلاف عرصه‌های سنتی ماهیتی مجازی دارد. میدان جنگ سایبری قبل، حین و یا بعد از نبرد حقیقی به فعالیت خود ادامه داده و بعد پنجم میدان نبرد پس از عرصه‌های سنتی همواره بعنوان مکمل میدان نبرد حقیقی برای فرماندهان است.

در حوزه امنیت نیز مطالعات سنتی بر محور نظامی به‌عنوان تنها گزینه در ابعاد امنیت متمرکز بوده است. تمرکز بر بعد نظامی امنیت، تأثیر عمیقی بر نظامی محور شدن مطالعات امنیتی گذاشته و مطالعات امنیتی بیشتر به مطالعه جنگ و آن هم در حوزه مطالعات استراتژیک تبدیل شده بود. بعدها این رویکرد توسط افرادی نظیر ریچارد اولمن[۱] در سال ۱۹۸۳ و هافندورن[۲] نقد گردید؛ این نقدها متضمن این مواضع بود که مطالعات امنیتی باید بیش از تمرکز بر امنیت نظامی بر جنبه‌های اقتصادی، فنّاورانه و داخلی متمرکز باشد؛ همچنین مطالعات امنیتی که در جنگ سرد بر مبنای تنگ‌نظرانه نظامی قرار داشت، در دنیای پس از جنگ سرد دیگر کاربردی ندارد؛ زیرا دغدغه

۱. Richard ullman
۲. helya hafteneorn

خاطره‌های امنیت نظامی تحلیل مسائل امنیتی در سطح داخلی و خارجی را که تابع مسائل نظامی نمی‌باشند، محدود و مشکل می‌سازد.

بوزان به شکل بسیار مبسوط‌تر، مستدل‌تر و قوی‌تر امنیت مضیق را زیر سؤال می‌برد و امنیت تک‌بعدی را با ابعاد بیشتری نظیر نظامی– سیاسی – اقتصادی و...**بیان می‌کند** (عبداله‌خانی، ۱۳۸۳). **جایگاه خاص جمهوری اسلامی ایران در ترتیبات منطقه‌ای و نظام بین‌الملل سبب شده تا نظام سلطه از فضای سایبری برای تحدید قدرت ملی به شکل فزاینده‌ای بهره‌برداری نماید؛ در این میان به‌منظور ایجاد** سازوکار **مناسب برای تضمین امنیت و منافع ملی در این فضا، شناخت ابعاد مختلف این مسئله به دغدغه بسیاری از صاحب‌نظران این حوزه تبدیل شده است.**

بیان مسئله– زیرساخت‌های حیاتی کشور روزبه‌روز وابستگی بیشتری به فضای سایبری (مجازی) برای توسعه فعالیت‌ها پیدا می‌کنند و درازای آن، زمینه آسیب‌پذیری ناخواسته کشور در برابر حملات و تهدیدهای سایبری افزایش می‌یابد. محور قرار گرفتن فضای اطلاعاتی و سایبری در ساختارهای قدرت ملی (قدرت اقتصادی به زیرساخت‌های سایبری و تعاملات اطلاعاتی، قدرت نظامی به سامانه‌های سایبری آفندی، پدافندی و پشتیبانی، قدرت سیاسی به دانش و آگاهی و توان دست‌یابی به قدرت نرم، قدرت فرهنگی و اجتماعی به ابزارهای اطلاع‌رسانی رسانه‌ای و سایبری)؛ اگرچه باعث افزایش چشم‌گیر کارایی، انعطاف‌پذیری، نوآوری و تحول می‌شود؛ اما می‌تواند به نقطه ضعف عمده کشور مبدل گردد.

قدرت حاصل از بهره‌برداری فضای سایبر در کشورها، می‌توانند همچنان به‌عنوان اهداف جنگی دشمنان برای تضعیف زیرساخت‌های حیاتی تکنولوژیکی، اجتماعی، اقتصادی و فرهنگی و... به‌کار گرفته شود و لازم است در زمره موضوعات دفاعی قرار گیرد؛ ازاین‌رو نتایج پژوهش و مدل مفهومی فوق می‌تواند، نگاه کل‌نگرانه‌ای را در دفاع سایبری کشور ایجاد کند و درواقع، نگاه سیستمی را جایگزین نگاه واکنشی محض نماید. در این پژوهش با تلفیق مفهوم دفاع سایبر در حوزه‌های امنیت سایبر رویکردهای دفاعی در مؤلفه‌های امنیت سایبر احصا شده و مدل مفهومی متضمن این موضوع ارائه می‌شود.

اهمیت و ضرورت پژوهش- در باب اهمیت این پژوهش می‌توان به تلفیق دو مفهوم امنیت و دفاع و توسعه مفهوم دفاع سایبری کشور اشاره نمود؛ همچنین پژوهش‌هایی از این دست سبب کمک علمی به حوزه تصمیم‌سازی و تصمیم‌گیری دفاع سایبری کشور شده و بستر لازم را برای تفکر در مدل دفاع سایبری بومی کشور فراهم می‌نمایند، مضاف بر آن خلاء دانشی را در کشور پیرامون دفاع سایبری پوشش داده و موجبات فرهنگ‌سازی در حوزه دفاع سایبری بومی برای الگوبرداری نهادهای مرتبط می‌گردد.

از سوی و در باب ضرورت تحقیق می‌توان گفت هر پژوهشی بستر تحقیقات پیوسته مرتبط را فراهم می‌نماید؛ بنابراین بدون انجام پژوهش حاضر، زمینه موصوف برای تحقیقات مشابه در حوزه دفاع سایبری شکل نمی‌گیرد و همچنین تا سالیان متمادی ممکن است وظایف نهادهای کشور در دفاع سایبری تبیین نگردد و به‌طورکلی ممکن است، هرگونه غفلت از این تحقیق یا پژوهش‌های مشابه در مقوله دفاع سایبری، لطمات و خسارات جبران‌ناپذیری را بر پیکره زیرساخت‌های موصوف به‌عنوان مراکز ثقل کشور وارد نماید، مضاف بر آنکه خاستگاه عمده فن‌آوری‌های این فضا، کشورها و قدرت‌هایی هستند که بی‌واسطه یا باواسطه دارای تضاد منافع در حوزه سیاسی، اقتصادی، دینی و غیره با کشورمان می‌باشند.

سؤالات پژوهش- پژوهش، با هدف اصلی پاسخ‌گویی به این سؤال که، «مدل مفهومی دفاع سایبریِ امنیت‌محور کشور چگونه است؟»، انجام و سؤالات فرعی ذیل را نیز مورد توجه قرار می‌دهد.

۱ – ابعاد، مؤلفه‌ها و شاخص‌های امنیت فضای سایبر کشور کدام‌اند؟

۲ – ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری کشور کدام‌اند؟

۳ – تأثیر امنیت سایبر کشور بر دفاع سایبری کشور چگونه است؟

ادبیات و مبانی نظری پژوهش

در این بخش ابتدا مفهوم امنیت را در **آموزه‌های** دینی جستجو نموده و زوایای مختلف آن را از منظر آیات و روایات مورد بررسی قرار داده و در ادامه همین مفهوم را در بیانات مقام معظم

رهبری مورد کنکاش قرار داده و از نگـاه معظـم‌لـه نیـز مؤلفـه‌هـای مختلـف امنیـت را اسـتخراج می‌گردد. در گام بعد با پرداختن به نظرات، نظریه‌پردازان حوزه امنیت نسبت به مؤلفه‌های امنیـت از نگاه دانشمندان این حوزه پرداخت خواهد شد. در ادامه بـه بررسـی موضـوع امنیـت و در فضـای سایبر و اسناد بالادستی حوزه فضای سایبر پرداخته و بخش بعد به جمع‌بندی و ارائه مدل خـواهیم پرداخت.

امنیت از منظر آموزه‌های اسلامی- معارف غنی اسلامی حاصل از آموزه‌های اسـلامی در بـر-دارنده مفهوم امنیت می‌باشد؛ در بررسی آیات و روایـات اسـلامی امنیـت را در چهـار نـوع مـورد شناسایی گردید که عبارت‌اند از (اخوان کاظمی، ۱۳۸۵):

- امنیت معنوی (ایمان سرچشمه اصلی امنیت)؛
- امنیت فردی و اجتماعی؛
- امنیت سیاسی و نظامی؛
- امنیت حقوقی و قضایی.

امنیت در بیانات مقام معظم رهبری- مجموعه تحـولات پرشـتاب کنـونی و ورود متغیرهـای متعدد در صحنه امنیتی کشور، مدیران سطح بالا را وادار می‌سازد تا از الگوهـا و روش‌هـای سـنتی خود در ادارهٔ امور امنیتی فاصله بگیرند و با در نظر گرفتن مجموعه تغییـرات محیطـی، راهبردهـا و سیاست‌های منسجمی را برای حفظ امنیت در کشور اتخاذ نمایند. در سلسـله بیانـات مقـام معظـم رهبری اشارات مختلفی به گونه‌هایی از امنیت شده است که در بررسـی‌هـای انجـام شـده در پـنج دسته مستقل به شرح زیر قابل ارائه می‌باشد:

- امنیت سیاسی و نظامی؛
- امنیت اجتماعی؛
- امنیت اقتصادی؛
- امنیت مدنی و قضایی؛
- امنیت ارزشی و فرهنگی.

امنیت در نگاه نظریه‌پردازان مقوله امنیت- مطالعات سنتی امنیت بر محور نظامی به‌عنوان تنهـا گزینه در ابعاد امنیت متمرکز بوده. تمرکز بر بعد نظامی امنیت، تأثیر عمیقی بـر نظـامی‌محـور شـدن

مطالعات امنیتی گذاشته و مطالعات امنیتی بیشتر به مطالعه جنگ و آن‌هم در حوزه مطالعات راهبردی تبدیل شده بود.

بعدها بوزان به شکل بسیار مبسوط‌تر، مستدل‌تر و قوی‌تر امنیت مضیق را زیر سؤال می‌برد و امنیت تک بعدی را به پنج بخش نظامی– سیاسی – اقتصادی – اجتماعی و زیست‌محیطی گسترش داد. مکتب کپنهاک مخالف دیدگاهی است که هسته مطالعات امنیتی را جنگ و زور می‌داند؛ یا پدیده‌ها و موضوعاتی را مطالعه می‌کند که دارای ویژگی‌های نزدیک و معناداری با جنگ و زور باشد (عبداله‌خانی، ۱۳۸۳).

امنیت سایبری– امنیت سایبری وابسته است به سیاست دولت‌ها؛ این اصطلاح عموماً توسط مؤسسات دولتی و سیاست‌گذاران ملی در اسناد، قوانین و پروژه‌های تحقیقاتی استفاده می‌شود و کمابیش مترادف با «امنیت اینترنت» است. هر دو عبارت به جوانب امنیت شبکه و اصول سیاست‌گذاری شبکه‌ها مثل تعریف حریم خصوصی، جرائم سایبر، تجارت و ارتباطات جهانی اشاره دارند. تفاوت این دو اصطلاح چندان زیاد نیست؛ بلکه امنیت رایانه‌ها، شبکه‌ها و داده‌ها تا حد زیادی با مفاهیم روزمرهٔ امنیت در فضای سایبر به‌هم گره خورده‌اند (سادوسکای و دیگران،۱۳۸۴:۱۶).

ابعاد امنیت سایبری

ابعاد امنیت سایبری عبارتند از:

- محرمانگی؛
- دسترس‌پذیری؛
- پکپارچگی؛
- کاربرد (کنترل کاربرد).

ذیلاً به ارائه تعاریف این مفاهیم می‌پردازیم:

محرمانگی: این عبارت به دو مفهوم بر می‌گردد:

محرمانگی داده: اطمینان از اینکه اطلاعات محرمانه و شخصی برای افراد احراز هویت نشده قابل دسترس نبوده و فاش نمی‌شود.

حریم خصوصی: اطمینان از اینکه افراد بتوانند کنترل کنند که چه اطلاعاتی مربوط به آن‌ها جمع‌آوری شده و ذخیره می‌گردد و همچنین به‌وسیله چه کسانی و برای چه کسانی این اطلاعات ارسال شده و فاش می‌شود.

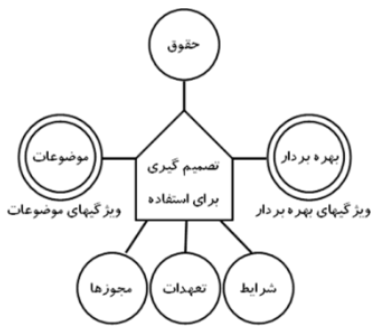
یکپارچگی: این عبارت به دو مفهوم برمی‌گردد:

یکپارچگی داده: اطمینان از اینکه اطلاعات تنها در یک وضعیت خاص و تأیید شده تغییر می‌یابند.

یکپارچگی سیستم: اطمینان از اینکه، یک سیستم توابع انتخابی خود را در وضعیت سالم و بدون عیب و دور از دستکاری‌های تأیید نشده عمدی یا سهوی اداره می‌نماید.

دسترس‌پذیری: اطمینان از اینکه سیستم‌ها بدون معطلی کار می‌کنند و سرویس‌ها همواره برای کاربران احراز هویت شده فعال و در دسترس هستند.

کاربرد: ارائه‌دهندگان خدمات، منابع و محتوای دیجیتال باید به‌صورت انتخابی تعیین کنند که چه کسی می‌تواند به این دسترسی دسترسی پیدا کند و دقیقاً همان چه دسترسی ارائه شود؛ این هدف اصلی کنترل دسترسی است. همان‌طور که در شکل۱ مشاهده می‌شود دسترسی به اطلاعات دیجیتال، محتوای فضای سایبر و کاربردها حاصل رعایت و داشتن «مجوزها؛ شرایط؛ تعهدات» می‌باشد. (Ravi Sandhu,2016)



شکل۱: چارچوب دسترسی به اطلاعات دیجیتال، کاربردها و محتوای فضای سایبر (Ravi Sandhu,2016)

همچنین اسناد و مستندات دیگری از کشورها و سازمان‌های بین‌المللی حاکی از تلقی ناامنی در اشاعه و انتشار برخی از محتویات اینترنتی است که در ادامه به برخی از آن‌ها اشاره می‌نماییم.

در سوم می سال ۲۰۱۶ تعریفی از تهدیدات امنیت ملی آمریکا توسط آژانس امنیت ملی این کشور ارائه گردید. در این گزارش بیان می‌دارد که تروریست‌ها و گروه‌های افراطی امروز از قدرت اینترنت به‌ویژه رسانه‌های اجتماعی برای انتشار پیام‌های نفرت خود استفاده می‌کنند. برای مقابله با این تهدیدات، رهبران ملی، رهبران نظامی، سیاست گذاران و پرسنل اجرای قانون باید بدانند که مخالفان ما کجا هستند و توانایی‌ها، برنامه‌ها و اهداف آن‌ها چیست.[۱]

– اتحادیه اروپا نیز در ۲۸ سپتامبر ۲۰۱۷ در قالب انتشار گزارشی به موضوع انتشار محتوا غیرقانونی[۲] از طریق اینترنت پرداخت. در این گزارش محتوای غیر قانونی اشاره‌ای دارد به محتوای غیر قانونی (قوانین اتحادیه اروپایی و قوانین محلی کشورها) محرک خشونت، نفرت و تروریست که در اینترنت منتشر می‌شود و تهدیدی جدی برای امنیت و امنیت شهروندان اتحادیه اروپا به‌شمار رفته، اعتماد و اطمینان شهروندان به محیط دیجیتالی موتور اصلی نوآوری، رشد و شغل را تضعیف می‌کند.

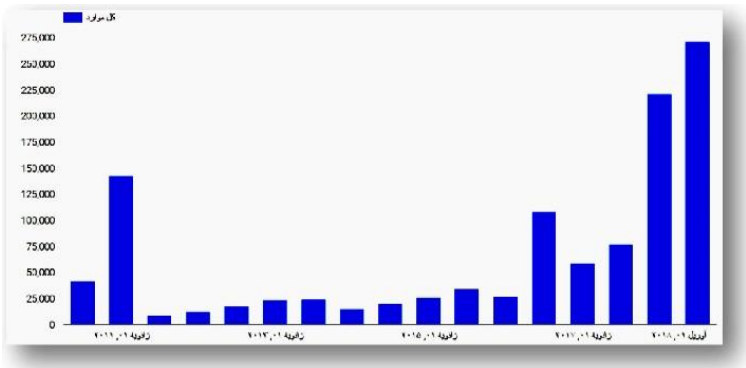
– اتحادیه بین‌المللی ارتباطات راه دور[۳] که عمدتاً موارد مرتبط با اپراتورها را در حوزه عملکردی، کیفی و اقتصادی مورد بررسی و رسیدگی قرار می‌دهد در آخرین نشست سالیانه در سال ۲۰۱۹ به موضوع تهدیدات محتوای منتشره در بستر اینترنت پرداخته است. مطابق آنچه در شکل۲ مشاهده می‌گردد؛ این تهدیدات عمدتاً در برگیرنده محتواهای، پورنوگرافی، نژادپرستی، خشونت و قلدری سایبری، تبلیغات سایبری، ترویج خودکشی و آسیب به خود می‌باشد.

۱. https://www.nsa.gov/what-we-do/understanding-the-threat/
۲. Illegal content
۳. International Telecommunication Union

شکل۲: تهدیدات و مخاطرات سایبری حاصل محتوای سایبری(S.Sharma,2019)

هرچند موارد بسیار دیگری می‌توان در تأیید و تأکید بر تهدیدات حاصل از محتوای اینترنتی در اسناد منتشره کشورها و سازمان‌ها یافت؛ لیکن به موارد اشاره شده بسنده نموده و جهت ارائه آمار و اطلاعات در خصوص احساس ناامنی به معنی واقعی آن چه در سطح کاربران و چه خصوصاً در سطح امنیت ملی کشورها می‌توان به اشاره می‌نماید.

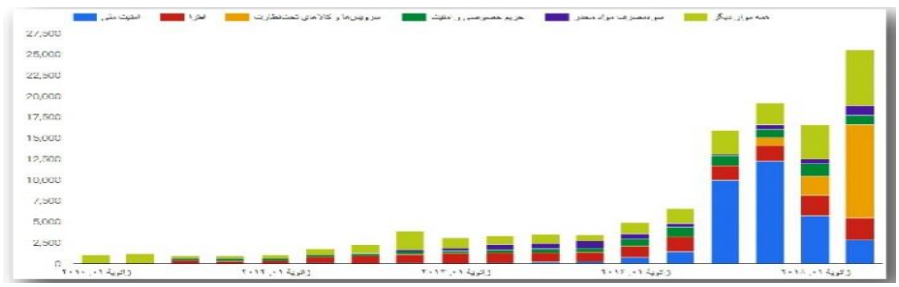
مطابق گزارش شفافیت گوگل،[۲] در شکل۳ شاهد حجم کل محتوای حذف شده از اینترنت به درخواست دولت‌ها هستیم؛ همان‌طور که مشاهده می‌شود حجم این درخواست‌ها در سال‌های اخیر به دلیل حجم روز افزون ناامنی‌هایی که در اثر انتشار آن‌ها رخ داده، افزایش یافته است.[۳]



شکل ۳: آمار کل موارد درخواست دولت‌ها برای حذف محتوا از سایت گوگل

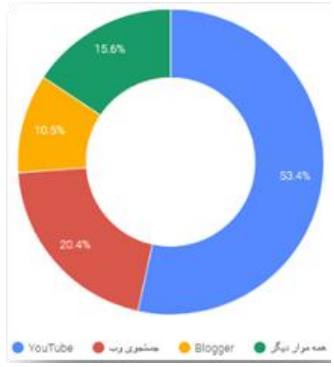
۱. Sameer Sharma,(2019), Building Trust in Digital World,ITU, Bangkok, Thailand
۲. Google Transparency Report
۳. https://transparencyreport.google.com/government-removals/overview?hl=fa

موارد درخواست‌های دولت‌ها برای حذف محتوای آن‌ها شامل مواردی نظیر تبلیغ برای خودکشی[۱] شکایت مربوط به کسب‌وکارها[۲] نقد دولت‌ها[۳] محتوای بزرگسالان[۴] تبلیغ خشونت[۵] علامت تجاری[۶] موارد مرتبط با قانون انتخابات[۷] توهین مذهبی[۸] محتوای مشوق عداوت و تنفر[۹] سوء مصرف مواد مخدر[۱۰] امنیت ملی می‌باشد که آمار این درخواست‌ها در شکل ۴ ارائه شده است؛ همچنین در شکل۵ نیز آمار کل موارد درخواست دولت‌ها برای حذف محتوا از سایت‌های مختلف نشان شده است. از تنوع درخواست‌های دولت‌ها مشخص است، دولت‌ها انتشار محتواهای اینترنتی را که در تضاد با اهداف کلان اقتصادی، اجتماعی، فرهنگی، سیاسی و امنیت ملی کشورها هستند را بر نمی‌تابند و این احساس ناامنی به‌صورت روزافزون در حال افزایش است، شکل ۶. پرواضح است مدیریت و کنترل محتوا توسط دولت‌ها در خصوص میزبانی‌هایی که مستقیماً در کنترل ایشان قرار دارد به مراتب موسع‌تر و پر حجم‌تر خواهد بود.

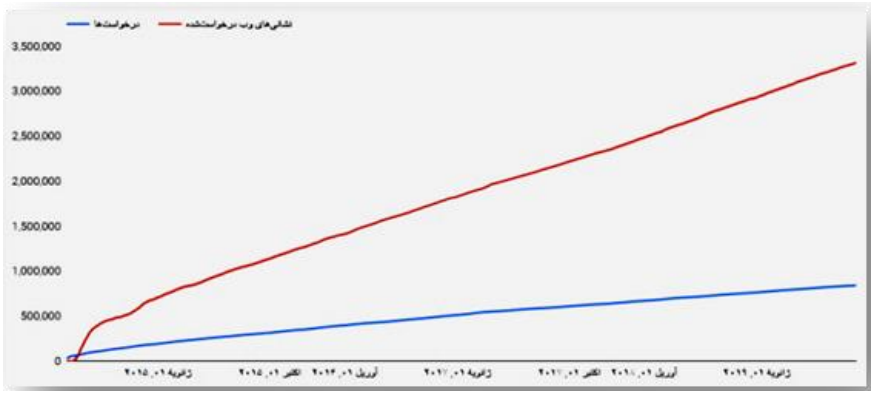


شکل ۴: آمار دلایل کل موارد درخواست دولت‌ها برای حذف محتوا

۱ Suicid Promotion
۲ Business Complaints
۳ Government Criticism
۴ Adult Content
۵ Violence
۶ Trade Mark
۷ Electoral Low
۸ Religious Offence
۹ Hate Speech
۱۰ Drag Abuse



شکل ۵: آمار کل موارد درخواست دولت‌ها برای حذف محتوا از سایت‌های مختلف



شکل ۶: آمار کل موارد درخواست دولت‌ها برای حذف محتوا از نشانی‌های وب

در دیگرسوی و با بررسی اسناد بالادستی ج.ا.ا شاهد دو نگاه زیر هستیم:

الف- اهمیت محتوا در فضای مجازی

اهمیت محتوا در جای جای اسناد بالادستی به وضوح و به‌طور ویژه مورد اشارات مستقیم قرار گرفته است؛ که در ادامه به بیان برخی از آن‌ها می‌پردازیم:

– سند اهداف و سیاست‌های مرکز ملی فضای مجازی با تأکید بر «محتوا» آن را مقدم بر زیرساخت‌ها، قالب‌ها و خدمات اینترنتی بر می‌شمرد و سرمایه‌گذاری مستمر را جهت تولید محتوای جذاب بر اساس اسلام ناب محمدی و گفتمان انقلاب اسلامی تجویز می‌نماید.[۱]

– نکات مورد تأکید مقام معظم رهبری در احکام صادر برای اعضای شورای‌عالی فضای مجازی را نیز می‌توان به‌عنوان یکی دیگر از مهم‌ترین اسناد مرجع در این زمینه نام برد به‌ویژه بند ۹ که بر توسعه محتوا منطبق با ارزش‌ها و فرهنگ اسلامی– ایرانی تأکید گردیده است.

– سند الزامات شبکه ملی اطلاعات را نیز می‌توان یکی دیگر از اسنادی است که به‌عنوان مصوبه شورای‌عالی فضای مجازی، نقشه راه ایجاد شبکه ملی اطلاعات در توصیف و توضیح الزامات این شبکه می‌باشد. در بند ۵ این سند در بخش الزامات فرهنگی شبکه ملی اطلاعات به تفضیل در خصوص توسعه و حمایت از رشد محتوا و خدمات مبتنی بر ارزش‌های اسلامی– ایرانی تأکید گردیده است (سند تبیین الزامات شبکه ملی اطلاعات :۱۴).[۲]

ب– محتوا در فضای مجازی و نقش آن در ایجاد ناامنی

مهم‌ترین اسناد متمرکز بر موضوع فضای سایبر[۳] با پرداختن به موضوع مدیریت و کنترل ناامنی‌ها و مخاطرات در فضای سایبر، ناامنی‌ها و مخاطرات را حاصل چهار عامل زیر دانسته‌اند:

- نقض محرمانگی؛
- نقض یکپارچگی؛
- نقض دسترس پذیری؛
- انتشار محتوای ناسالم.

به‌ویژه در سند راهبردی امنیت فضای تولید و تبادل اطلاعات که در کنار تأکید بر امن‌سازی زیرساخت‌های حیاتی کشور در قبال حملات الکترونیکی (راهبرد ۱–۶ سند راهبردی امنیت

---

۱. بند ۵ سند اهداف و سیاست‌های مرکز ملی فضای ملی

۲. تبیین الزامات شبکهٔ ملی اطلاعات مصوبهٔ جلسهٔ سی و پنجم مورخ شورای‌عالی فضای مجازی

۳. تبیین الزامات شبکهٔ ملی اطلاعات مصوبهٔ جلسهٔ سی و پنجم مورخ شورای‌عالی فضای مجازی– سند راهبردی امنیت فضای تولید و تبادل اطلاعات– قانون جرایم رایانه‌ای

فضای تولید و تبادل اطلاعات) تأمین سلامت و جلوگیری از مخاطرات ناشی از محتوا در فتا را نیز مورد توجه ویژه قرار داده است (راهبرد ۳-۶ سند راهبردی امنیت فضای تولید و تبادل اطلاعات) در راهبرد ۳-۶ این سند اقدامات زیر را جهت اجرای این راهبرد ذکر نموده است. در ادامه این سند، اقدامات زیر را جهت تحقق راهبرد ۳-۶ ارائه نموده است:

طرح ایجاد سازوکار فنی و قانونی سلامت محتوا، نظیر:

- ایجاد سازوکار فنی و قانونی صیانت از ارزش‌های دینی و ملی
- ایجاد سازوکار مسئولیت‌پذیری در تولید و عرضه محتوا (اقدام مرتبط با راهبرد ۳ -۶ سند راهبردی امنیت فضای تولید و تبادل اطلاعات)

تأمین دسترس‌پذیری، محرمانگی و یکپارچگی با تأکید بر نیازمندی‌های سالم‌سازی (محتوا) (سند تبیین الزامات شبکه ملی اطلاعات :۸) در بخشی از سند تبیین الزامات شبکه ملی اطلاعات همچنین اشاره به:

تأمین خدمات سالم‌سازی و امنیت مورد نیاز زیرساخت فضای مجازی کشور پشتیبانی از سالم‌سازی امنیت لایه‌های بالایی خدمات کاربردی و محتوا شامل:

- خدمات مدیریت و عملیات سالم‌سازی به‌ویژه پالایش محتوا. (سند تبیین الزامات شبکه ملی اطلاعات :۷-۸) در کنار دیگر ملاحظات امنیتی، بیانگر هم ارزبودن عوامل چهارگانه فوق‌الذکر می‌باشد.

علاوه بر موارد اشاره شده در حمایت و توسعه تولید و انتشار محتوای اسلامی- ایرانی، تولید و انتشار محتوای مجرمانه از طریق فضای مجازی نیز جرم تلقی شده؛[1] لذا در معرفی ابعاد امنیت فضای سایبر واژه «محتوا» که در برگیرنده ناامنی‌های هر دو سوی ارائه‌کننده و دریافت‌کننده خدمات و محتوا می‌باشد، جایگزین کاربرد می‌گردد؛ به عبارتی دسترسی و تولید و انتشار محتوا در بستر اینترنت تابع مجوزها، شرایط، تعهدات و قوانین مربوطه می‌گردد و ایجاد ناامنی در بعد محتوا در اثر نقض هریک از موارد اشاره شده صورت می‌گیرد؛ ازاین‌رو ابعاد امنیت فضای سایبر

۱. سیاست‌های کلی نظام در امور «امنیت فضای تولید و تبادل اطلاعات و ارتباطات و سند راهبردی امنیت فضای تولید و تبادل اطلاعات- قانون جرایم رایانه‌ای

مشتمل بر محرمانگی، یکپارچگی، دسترس‌پذیری و محتوا در مدل مفهومی شکل ۸ ارائه گردیده است.

بررسی اسناد بالادستی–به‌منظور بررسی قوانین و اسناد بالادستی مرتبط با فضای سایبر و امنیت این فضا، طی یک مطالعه کتابخانه‌ای، لیستی از اسناد مرتبط تهیه گردید که نتایج بررسی‌های انجام شده به شرح زیر آورده شده است:

۱. قانون جرایم رایانه‌ای؛
۲. آیین‌نامه ساماندهی پایگاه‌های اینترنتی ایرانیان؛
۳. سند چشم‌انداز بیست‌ساله؛
۴. برنامه پنجم توسعه کشور؛
۵. سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور؛
۶. سند راهبردی نظام جامع فناوری اطلاعات کشور؛
۷. سیاست‌های کلی نظام در حوزه امنیت فضای تولید و تبادل اطلاعات (افتا)؛
۸. سند فرابخشی دولت الکترونیکی؛
۹. سیاست‌های کلی نظام در حوزه پدافند غیرعامل؛
۱۰.قانون انتشار دسترسی آزاد به اطلاعات؛
۱۱.آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی؛
۱۲. حکم و مصوبات شورای عالی فضای مجازی کشور؛
۱۳.برنامه جامع توسعه تجارت الکترونیکی کشور؛
۱۴.سیاست‌های کلی برنامه ششم توسعه.

در جدول ۱ جمع‌بندی بررسی و ارزیابی اسناد بالادستی حوزه فضای سایبر ارائه شده است.

جدول۱: بیان اهمیت مؤلفه‌ها و ابعاد امنیت فضای سایبر در اسناد بالادستی حوزه فضای سایبر

		شماره سند چهارده گانه												
		۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴
ابعاد	یکپارچگی دسترس پذیری محرمانگی	√		√	√	√	√	√	√	√	√	√		√	
	محتوا	√	√	√	√	√	√	√							
مولفه ها	اقتصادی	√	√	√	√	√		√	√	√	√	√	√	√	√
	اجتماعی	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	فرهنگی	√	√	√	√	√					√		√		√
	نظامی	√		√	√	√	√	√	√	√		√	√		√
	سیاسی	√		√	√	√	√	√	√	√		√	√	√	√
	زیست محیطی	√					√								

مؤلفه‌های امنیت فضای سایبر– در بررسی و انطباق مطالعات انجام شده با یکدیگر به‌ویژه انطباق آن‌ها با اسناد بالادستی حوزه فضای سایبر به‌عنوان فصل ممیزه فضای سایبر با دیگر حوزه‌ها، مؤلفه‌های امنیت ملی تأثیرپذیر از فضای سایبر مشتمل بر ۶ مؤلفه بوده که به شرح زیر احصا می‌گردد:

- مؤلفه نظامی؛
- مؤلفه اقتصادی؛
- مؤلفه اجتماعی؛
- مؤلفه فرهنگی؛
- مؤلفه سیاسی؛
- مؤلفه زیست‌محیطی.

شاخص‌های مرتبط با هریک از مؤلفه‌ها–برای اندازه‌گیری و ارزیابی هریک از مؤلفه‌های ارائه شده در بخش قبل شاخص‌های اختصاصی در نظر گرفته شده که در جداول ۲ ارائه گردیده است.

مولفه	شاخص	ماخذ
اجتماعی	تغییرات حس تعلق	- موسوی و دیگران، ۱۳۹۱، ابعاد و مولفه های توسعه اجتماعی در برنامه های پنجگانه توسعه اقتصادی، اجتماعی، فرهنگی جمهوری اسلامی ایران - آزاد ارمکی و دیگران، ۱۳۹۲، بررسی و شناسایی شاخص‌های کاربردی توسعه اجتماعی(با استفاده از تکنیک دلفی) - فاضلی و دیگران، ۱۳۹۲، توسعه‌ی اجتماعی، شاخص ها و جایگاه ایران در جهان - نسترن و دیگران، ۱۳۹۱، ارزیابی شاخص های پایداری اجتماعی با استفاده از فرآیند تحلیل شبکه(ANP) - FMETeam,(2013),"*PESTEL Analysis Strategy Skills*" - Funded by Horizon 2020 Framwork Programme of European Union,(2017),PESTELE Analysis - http://www.myindustry.ir/strategic-management/article/pest-analysis.html
	تغییرات تعامل اجتماعی	
	تغییرات مسئولیت پذیری	
	تغییرات مشارکت در فعالیتهای اجتماعی (فرهنگی، تفریحی، مذهبی، محلی)	
	تغییرات امنیت(عینی و ذهنی کاربران)	
	تغییرات اعتماد(بین فردی، مدنی یا نهادی)	
	تغییرات خدمات (کیفیت، دسترسی)	
	تغییرات زندگی(نشاط، رضایت مندی)	
	تغییرات نرخ بزهکاری	
	میزان رخدادهای ناشی از عوامل قومی و مذهبی	
	نرخ رشد جمعیت	
	سطح سلامتی و دانش سلامتی	
دفاعی و نظامی	وفاق و همگرایی ملی	- قنبری و دیگران، ۱۳۹۵، استحکام درونی قدرت ملی جمهوری اسلامی ایران در اندیشه‌ی مقام معظم رهبری؛ با تأکید بر مؤلفه‌های دفاعی -امنیتی
	ولایت مداری	
	مشارکت عمومی (دفاع، جهاد، حفظ آرمانها)	
	اقتدار نظامی و دفاعی و سایبری	

مولفه	شاخص	ماخذ
فرهنگی	تغییرات در اخلاق	- شاخص‌های راهبردی، ابعاد و مؤلفه‌های فرهنگی، ۱۳۸۹، شورایعالی انقلاب فرهنگی - شاخصهای کلان فرهنگ عمومی، ۱۳۸۶، وزارت فرهنگ و ارشاد اسلامی
	تغییرات در عقلانیت	
	تغییرات عدالت	
	تغییرات در هویت ملی، دینی و انقلابی	
	تغییرات در نظم اجتماعی	
	تغییرات در وحدت و انسجام	
	تغییرات در استقلال فکری ملی	
	تغییرات در تعاملات فرهنگی بین المللی	
	تغییرات در بهداشت جسمی و روانی	
	تغییرات در کالاها و خدمات فرهنگی	
	تغییرات در خانواده	
سیاسی	میزان مشروعیت نظام واهتمام مردم به دولتمردان	- عبدالعلی قوام، توسعه سیاسی وتحول اداری، تهران، نشرقومس، ۱۳۷۱ - جلالی راد، ۱۳۹۶،شاخص های فرهنگ سیاسی جمهوری اسلامی ایران در بُعد کلان از دیدگاه نخبگان - نظری و دیگران، ۱۳۹۲، بررسی تاثیر مشارکت سیاسی بر توسعه سیاسی - FMETeam,(2013),"PESTEL Analysis Strategy Skills" - Funded by Horizon 2020 Framwork Programme of European Union,(2017),PESTELE Analysis - Tanya Sammut-Bonnici,(2015), PEST analysis
	مشارکت مردم از طریق نهادهای اجتماعی، سیاسی نظیر انتخابات مجلس احزاب و نهادهای سیاسی غیردولتی و مطبوعات	
	میزان اقتدار در پاسخگویی به نیازهای مرم	
	میزان فساد[5]	
	میزان ثبات سیاسی	
	ثبات در همسایگان[6]	
	میزان اعتماد عمومی(به رسانه های و افراد سیاسی و مذهبی)	

مولفه	شاخص	ماخذ
اقتصادی	تغیر درامنیت اقتصادی	-طباطبایی و دیگران، ۱۳۹۲، مهم ترین شاخص‌های اقتصادی کشور از ابتدای برنامه اول تادو سال اول برنامه پنجم (۱۳۶۸ تا ۱۳۹۱) - رسولی، ۱۳۹۳، تبیین رابطه بین آزادی و امنیت اقتصادی با تشکیل سرمایه: شواهدی از کشورهای نوظهور و در حال توسعه - FMETeam,(2013),"*PESTEL Analysis Strategy Skills*" - Funded by Horizon 2020 Framwork Programme of European Union,(2017),"*PESTELE Analysis*"
	تغییر درآزادی اقتصادی	
	تغییرمخارج دولت (درصدازGDP)	
	تغییرGDP (بصورت درصد)	
	تغییر نرخ بیکاری (بصورت درصد)	
	تغییر در قیمت و هزینه تولید	
	تغییرنرخ تورم(بصورت درصد)	
	تغیر سرمایه گذاری خارجی(FDI)(بصورت درصد)	
زیست محیطی	افزایش آلودگی هوا(ذرات معلق، دی اکسید سولفور، دی اکسید کربن، کاهش لایه ازن)	- Yale Center for Environmental Law & Policy Yale University et al, 2008, ENVIRONMENTAL PERFORMANCE INDEX, http://www.yale.edu/epi/ - FMETeam,(2013),"*PESTEL Analysis Strategy Skills*"
	افزایش بحران آب(کیفیت، کمیت)	
	افزایش بحران آبیاری (استفاده بهینه در کشاورزی)	
	افزایش اثر بیماریهای حاصل از محیط بر جمعیت	
	تغییرات در چرخه آب و هوایی[3]	
	تغییرات هزینه انرژی و دسترس پذیری آن[4]	

جدول۲: شاخص اندازه‌گیری مؤلفه‌های امنیت فضای سایبر

دفاع

در لغت‌نامه معین، از دستبرد دشمن حفظ‌کردن، بازداشتن، پس‌زدن (معین، ۱۳۸۲: ۵۳۰) و در لغت‌نامه دهخدا، دورکردن از کسی، دفع‌کردن از کسی، یاوری و حمایت‌کردن کسی از دستبرد دشمن (دهخدا، ۱۳۷۷: ۱۰۹۴۰) معنی شده است. در قرآن کریم، بارها به رعایت عدالت و عدم تجاوز از حدود معقول و انسانی در مقابل دشمنان تأکید شده است (آیه ۱۹۰ سوره بقره). حضرت امام خمینی(ره)، در باب دفاع همه‌جانبه فرمودند: «اگر بر کشوری ندای دل‌نشین تفکر بسیجی طنین اندازد، چشم طمع دشمنان و جهان خواران از آن دور خواهد گردید و الا هرلحظه باید منتظر حادثه باشیم»[1] حضرت امام خامنه‌ای (مدظله‌العالی) فرموده‌اند، «دفاع یک وظیفه عقلی و انسانی و اسلامی است. پس باید آماده بود. روزبه‌روز باید آمادگی‌تان را بیشتر کنید و آموزش‌ها را پیش ببرید سازمان‌دهی منظم مبتنی بر حفظ انضباط کامل و رعایت مقررات است».[2]

در حال حاضر، بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور، در کلیه سطوح، اعم از افراد، مؤسسات غیردولتی و نهادهای دولتی و حاکمیتی در فضای سایبر انجام می‌گیرد. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور، یا خود، بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشور نیز، به این فضا منتقل و یا اساساً در این فضا، شکل‌گرفته است. سهم درآمد حاصل از کسب‌وکارهای فضای سایبر در تولید ناخالص ملی افزایش چشم‌گیر یافته و از میان شاخص‌های تعیین‌شده برای سنجش میزان توسعه‌یافتگی کشور، شاخص‌های حوزه سایبر، سهم عمده‌ای را به خود اختصاص داده‌اند؛ به‌عبارت‌دیگر وجوه مختلف زندگی شهروندان، به معنای واقعی، با این فضا درآمیخته و هرگونه بی‌ثباتی، ناامنی و چالش در این حوزه، مستقیماً زندگی شهروندان را به مخاطره خواهد انداخت. جنگ سایبری (رایاجنگ یا نبرد مجازی)، به‌نوعی از نبرد اطلاق می‌گردد که طرفین جنگ در آن از رایانه و شبکه‌های رایانه‌ای (به‌خصوص شبکه اینترنت) به‌عنوان ابزار استفاده کرده و نبرد را در

---

۱. صحیفهٔ نور، ج ۲۱، ۵۲

۲. دیدار با پرسنل نهاجا در روز نیروی هوایی – ۱۳۶۹/۱۱/۱۹

فضای سایبری جاری سازند. عصر اطلاعات و زیرساخت‌های آن‌ها مصادیق جنگ و دفاع را دستخوش تغییر نموده است؛ یعنی اگر قائل باشیم که زمین، دریا و هوا سه بعُد جنگ زمینی، دریایی و هوایی و جنگ‌های فضایی بعد چهارم جنگ است، بدین منوال جنگ‌های سایبری نیز بُعد پنجم جنگ می‌تواند در نظر گرفته شود (ایمانی، ۱۳۹۰: ۳۰۰).

دفاع سایبری

دفاع سایبری، به‌کارگیری اقدامات حفاظتی مؤثر برای به دست آوردن یک سطح مناسب از امنیت سایبری به‌منظور تضمین عملکرد و عملیات دفاعی می‌باشد؛ این موضوع به‌وسیله اقدامات محافظتی مناسب برای کاهش مخاطره امنیتی به یک سطح قابل پذیرش حاصل می‌شود. دفاع سایبری از وظائف و تکالیف، حفاظت، کشف، پاسخ و بازیابی تشکیل شده است (ACST-CyberSecurity-Strategy,2014, p11) اصطلاح دفاع سایبری به همه اقدامات برای دفاع از فضای سایبر به‌وسیله نیروهای نظامی و ابزارهای مناسب برای احصا اهداف راهبردی-نظامی اشاره می‌کند.

دفاع سایبری یک سامانه یکپارچه برای پیاده‌سازی همه اقدامات مرتبط با فناوری اطلاعات و ارتباطات و امنیت اطلاعات، قابلیت‌های گروه پاسخگویی حوادث رایانه‌ای[۱] و عملیات شبکه‌ای رایانه‌ای[۲] همچنین پشتیبانی از قابلیت‌های فیزیکی نظامی (Grafik, 2013, p. 21) شامل بخش‌های محافظت، کشف، پاسخ و بازیابی است (ACST–Strategy-CyberSecurity, 2014, p. 18). نقاط ضعف اصلی دفاع سایبر را می‌توان بررسی هویت و مکان مهاجم، شناسایی نیت مهاجم، تشخیص حمله‌های از قبل طراحی‌شده، بررسی و ارزیابی تلفات بعد از حادثه یا جنگ، برشمرد (ویکی‌پدیا، دانشنامه آزاد، ۲۰۱۸). برای داشتن دفاع سایبری همه‌جانبه و یکپارچه در سراسر کشور، بایستی چهار دسته توانمندی‌ها راهبردی، علمی، فن‌آورانه و عملیاتی را در کشور تولید کرده و یا تقویت نماییم (اسکندری، ۱۳۹۳: ۸۵). به‌طورکلی، هر اقدام مجرمانه در فضای سایبری، مجموعه اعمالی است که برای ایجاد اختلال، قطعی، کاهش کیفیت یا نابودی اطلاعات مقیم در رایانه‌های موجود در فضای

۱. CERT
۲. CNO : Computer network operation

سایبری انجام‌شده و ابتدا، عملیات شناسایی و پویش سامانه هدف انجام‌شده و سپس تلاش برای دسترسی به سامانه صورت می‌گیرد. سپس ارتقاء حقوق دسترسی جهت دست یافتن به اهداف موردنظر انجام و توسط آن، صدمه، سرقت اطلاعات یا هر اقدام مجرمانه دیگر انجام می‌شود (حتی نصب هر ابزار لازم دیگری برای حفظ دسترسی به سامانه در آینده). درنهایت نیز ضمن انجام مخفی‌کاری لازم برای عدم به‌جا ماندن ردپا و آثار جرم یا حمله، یورش موردنظر به سامانه انجام شده و به تثبیت مواضع در سامانه هدف پرداخته می‌شود (حسینی و ظریف منش، ۱۳۹۲: ۴۸).

روش‌شناسی تحقیق

این تحقیق از منظر هدف تحقیقی کاربردی می‌باشد؛ چرا که سعی می‌شود نتایج حاصل از این تحقیق را مورد استفاده عملی قرار داده و با کمک نتایج آن، مشکلات سازمان رفع شوند؛ اما این تحقیق از منظر گردآوری اطلاعات تحقیقی توصیفی-پیمایشی می‌باشد. هنگامی‌که در تحقیق سعی می‌شود با اتکا به مطالعات کتابخانه‌ای مدل اولیه سنجش سرمایه فکری ارائه گردد، تحقیق از نوع توصیفی می‌باشد؛ اما هنگامی‌که سعی می‌گردد با کمک پرسشنامه خبرگی، نظر خبرگان در مورد مدل احصا گردیده و یا هنگامی‌که برای بررسی فرضیات تحقیق جهت آزمون روایی مدل از پرسشنامه استفاده می‌گردد.

تجزیه‌وتحلیل داده‌ها و یافته‌های تحقیق

در این مرحله، با تجزیه‌وتحلیل یافته‌ها باید ابعاد، مؤلفه‌ها و شاخص‌های امنیت و دفاع سایبری را شناسایی نماییم تا درنهایت، تناظر امنیت سایبر و دفاع سایبری احصاء گردد.

شناسایی ابعاد، مؤلفه‌ها و شاخص‌های امنیت فضای سایبر

ابعاد و مؤلفه‌های امنیت فضای سایبر در این بخش مورد واکاوی قرار گرفت و مدل مفهومی پژوهش احصاء گردید. بر آن اساس پرسشنامه‌ای تنظیم و در اختیار ۵ نفر از صاحب‌نظران قرار گرفت و نظرات تخصصی در خصوص روایی و پایایی پرسشنامه در سنجش مدل مفهومی فوق اخذ شد و ضمن اعمال اصلاحات لازم، پرسشنامه نهایی تنظیم و به‌صورت کاغذی و الکترونیکی در اختیار ۵۰ نفر از خبرگان قرار گرفت و درنهایت نیز ۳۷ پرسشنامه تکمیل شده اخذ گردید.

در ادامه داده‌های حاصل از پرسشنامه را توسط نرم‌افزار اسمارت پی.ال.اس تجزیه و تحلیل (برازش اندازه‌گیری، ساختاری و کلی) گردید و با اضافه‌کردن داده‌های اخذ شده از پرسشنامه‌ها، الگوریتم حداقل مربعات جزئی[۱] نتایج به شرح زیر به‌دست آمد.

بررسی برازش مدل اندازه‌گیری- این برازش به‌منظور بررسی روابط متغیرهای آشکار یا قابل‌اندازه‌گیری (مستطیل‌ها) با متغیرهای پنهان مرتبط (دایره‌های متصل به آن‌ها) در راستای تعیین روایی و پایایی پرسشنامه، طبق جدول (۳-الف) با استفاده از معیارهای کیفیت مدل صورت می‌گیرد.

بررسی برازش مدل ساختاری با استفاده از معیار Q^2 [۲]- این معیار نشان‌دهنده قدرت پیش‌بینی مدل است. سه مقدار۰,۰۲ و ۰,۱۵ و ۰,۳۵ نشان‌دهنده برازش ضعیف، متوسط و قوی مدل ساختاری است.[۳]با توجه به جدول(۳-ب)، برازش مدل را در این معیار می‌توان متوسط تا قوی ارزیابی نمود.

بررسی برازش مدل کلی با استفاده از معیار GOF[۴]- عددی که برای این معیار به‌دست می‌آید بین صفر و یک می‌باشد. سه مقدار ۰,۰۱ و ۰,۲۵ و ۰,۳۶ به‌عنوان مقادیر ضعیف، متوسط و قوی برای GOF ارائه شده است؛ این مقدار از جذر حاصل ضرب میانگین ستون «متوسط مشترک»[۵] و میانگین «ضریب تعیین» حاصل می‌گردد، جدول (۳-ج).

همان‌طور که مشاهده می‌شود، مقدار برازش کلی مدل معادل ۰,۴۵ بوده و چون از ۰,۳۶ بیشتر است، برازش مدل را قوی ارزیابی می‌کنیم؛ لذا با استفاده از نتایج حاصل، می‌توان نتیجه گرفت که مدل مفهومی ارائه شده مورد تأیید خبرگان قرار گرفته است.

---

۱. PLS Algorithm

۲. Stone-Geisser Criterion

۳. مقدار آن از طریق ستون ۱-SSE/SSO در جدول Indicator Crossvalidated Redundancy از تحلیل Blindfolding نرم افزار SmartPLS بدست می‌آید.

۴. Goodness of Fit

۵. Communality : این عنوان به صورت مشخص در نسخه ۲ نرم افزار وجود دارد ولی در نسخه ۳ نرم‌افزار از مقدارAVE استفاده می شود.

الف

	متوسط واریانس استخراج‌شده[1]	پایایی	آلفای کرونباخ[2]
سرمایه‌گذاری	۰.۸۳	۰.۷۷	۰.۷۷
یکپارچگی	۰.۸۳	۰.۷۷	۰.۷۵
دسترس پذیری	۰.۸۳	۰.۷۵	۰.۷۵
محرما	۰.۸۴	۰.۸۱	۰.۷۷
سرمایه‌گذاری - اقتصادی	۰.۹۰	۰.۹۰	۰.۸۷
سرمایه‌گذاری - سیاسی	۰.۸۸	۰.۹۷	۰.۸۶
سرمایه‌گذاری - نظامی	۰.۸۲	۱.۰۲	۰.۷۶
سرمایه‌گذاری - اجتماعی	۰.۸۴	۰.۸۰	۰.۸۲
سرمایه‌گذاری - فرهنگی	۰.۹۲	۰.۹۳	۰.۹۱
سرمایه‌گذاری - زیست محیطی	۰.۹۲	۰.۸۹	۰.۸۸
یکپارچگی - اقتصادی	۰.۸۵	۰.۸۴	۰.۷۸
یکپارچگی - سیاسی	۰.۸۸	۰.۹۶	۰.۸۶
یکپارچگی - نظامی	۰.۸۲	۱.۰۴	۰.۷۶
یکپارچگی - اجتماعی	۰.۸۵	۰.۸۱	۰.۸۲
یکپارچگی - فرهنگی	۰.۹۲	۰.۹۳	۰.۹۱
یکپارچگی - زیست محیطی	۰.۸۸	۰.۸۲	۰.۸۱
دسترس پذیری - اقتصادی	۰.۸۶	۰.۸۳	۰.۸۲
دسترس پذیری - سیاسی	۰.۸۹	۰.۸۸	۰.۸۶
دسترس پذیری - نظامی	۰.۸۴	۰.۸	۰.۷۶
دسترس پذیری - اجتماعی	۰.۸۶	۰.۸۴	۰.۸۳
دسترس پذیری - فرهنگی	۰.۹۲	۰.۹۳	۰.۹۱
دسترس پذیری - زیست محیطی	۰.۹۱	۰.۹۳	۰.۸۹
محرما - اقتصادی	۰.۸۴	۰.۸۱	۰.۸۲
محرما - سیاسی	۰.۸۹	۰.۸۴	۰.۸۶
محرما - نظامی	۰.۸۳	۰.۸۲	۰.۷۶
محرما - اجتماعی	۰.۸۳	۰.۹۳	۰.۷۶
محرما - فرهنگی	۰.۹۲	۰.۹۱	۰.۹۱
محرما - زیست محیطی	۰.۸۹	۰.۸۵	۰.۸۴

ب

	نتیجه برازش	Q2=(1-SSE/SSO)
سرمایه‌گذاری	برازش متوسط	۰.۱۲
یکپارچگی	برازش متوسط	۰.۱۲
دسترس پذیری	برازش متوسط	۰.۰۵
محرما	برازش متوسط	۰.۱۰
محرما-گی - اقتصادی	برازش متوسط	۰.۱۱
محرما-گی - سیاسی	برازش ضعیف	۰.۰۱
محرما-گی - نظامی	برازش متوسط	۰.۰۶
محرما-گی -اجتماعی	برازش متوسط	۰.۰۵
محرما-گی - فرهنگی	برازش متوسط	۰.۱۲
محرما-گی -زیست محیطی	برازش متوسط	۰.۱۲
یکپارچگی -اقتصادی	برازش متوسط	۰.۱۰
یکپارچگی -سیاسی	برازش ضعیف	۰.۰۱
یکپارچگی - نظامی	برازش متوسط	۰.۰۶
یکپارچگی -اجتماعی	برازش متوسط	۰.۱
یکپارچگی - فرهنگی	برازش متوسط	۰.۱۲
یکپارچگی -زیست محیطی	برازش متوسط	۰.۰۹
دسترس پذیری -اقتصادی	برازش متوسط	۰.۰۵
دسترس پذیری -سیاسی	برازش متوسط	۰.۰۴
دسترس پذیری - نظامی	برازش متوسط	۰.۰۸
دسترس پذیری -اجتماعی	برازش متوسط	۰.۰۷
دسترس پذیری - فرهنگی	برازش قوی	۰.۲۱
دسترس پذیری -زیست محیطی	برازش متوسط	۰.۱۰
محرما - اقتصادی	برازش متوسط	۰.۰۴
محرما - سیاسی	برازش متوسط	۰.۰۲
محرما - نظامی	برازش متوسط	۰.۰۶
محرما - اجتماعی	برازش متوسط	۰.۰۹
محرما - فرهنگی	برازش قوی	۰.۲۰
محرما - زیست محیطی	برازش متوسط	۰.۰۶

ج

	R^2	متوسط واریانس استخراج‌شده
سرمایه‌گذاری	۰.۳۱	۰.۸۳
یکپارچگی	۰.۳۲	۰.۸۳
دسترس پذیری	۰.۱۸	۰.۸۳
محرما	۰.۳۱	۰.۸۴
سرمایه‌گذاری - اقتصادی	۰.۲۸	۰.۹۰
سرمایه‌گذاری - سیاسی	۰.۰۴	۰.۸۸
سرمایه‌گذاری - نظامی	۰.۱۸	۰.۸۲
سرمایه‌گذاری - اجتماعی	۰.۳۰	۰.۸۴
سرمایه‌گذاری - فرهنگی	۰.۳۲	۰.۹۲
سرمایه‌گذاری - زیست محیطی	۰.۲۰	۰.۹۲
یکپارچگی - اقتصادی	۰.۳۲	۰.۸۵
یکپارچگی - سیاسی	۰.۰۴	۰.۸۸
یکپارچگی - نظامی	۰.۱۹	۰.۸۲
یکپارچگی - اجتماعی	۰.۳۸	۰.۸۵
یکپارچگی - فرهنگی	۰.۳۱	۰.۹۲
یکپارچگی - زیست محیطی	۰.۱۹	۰.۸۸
دسترس پذیری -اقتصادی	۰.۳۳	۰.۸۶
دسترس پذیری - سیاسی	۰.۱۱	۰.۸۹
دسترس پذیری - نظامی	۰.۱۹	۰.۸۴
دسترس پذیری -اجتماعی	۰.۳۷	۰.۸۶
دسترس پذیری - فرهنگی	۰.۴۶	۰.۹۲
دسترس پذیری - زیست محیطی	۰.۲۰	۰.۹۱
محرما - اقتصادی	۰.۲۲	۰.۸۴
محرما - سیاسی	۰.۰۹	۰.۸۹
محرما - نظامی	۰.۱۵	۰.۸۳
محرما - اجتماعی	۰.۳۱	۰.۸۳
محرما - فرهنگی	۰.۴۸	۰.۹۲
محرما - زیست محیطی	۰.۱۶	۰.۸۹
بازتابی	۰.۳۴	۰.۸۷

$$GOF = \sqrt{\overline{\text{Communality}} \times \overline{R^2}} = \sqrt{۰.۸۷ \times ۰.۳۴} = ۰.۲۵$$

جدول۳:: نتایج حاصل از تجزیه و تحلیل مدل مفهومی ابعاد، مولفه ها و شاخص های امنیت فضای سایبر

شناسایی ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری کشور

رضا تقی‌پور و علی اسماعیلی (۱۳۹۷) در مقاله‌ای با عنوان «طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران»، ضمن تحلیل محتوای تعاریف دفاع و دفاع سایبری، اسناد بالادستی و مطالعات تطبیقی، کلیدواژه‌های مهم را استخراج و با دریافت اجماع نظر نخبگان از طریق تکنیک دلفی، سه کلیدواژه بازدارندگی، پدافند و برگشت‌پذیری را به‌عنوان ابعاد دفاع سایبری ارائه نمودند و با واکاوی اطلاعات مرتبط در حکم تشکیل شورای عالی فضای مجازی، قانون اساسی جمهوری اسلامی ایران (اصول ۱۷۰،۱۱۱،۱۱۲)، سند راهبردی پدافند سایبری کشور، قوانین بین‌المللی منشور سازمان ملل متحد، استراتژی امنیت و دفاع سایبری اتحادیه اروپا، آمریکا، انگلیس، کره جنوبی، ترکیه و اردن، مؤلفه‌ها و شاخص‌های مرتبط را احصاء و ارائه نمودند (تقی‌پور و اسماعیلی، ۱۳۹۷: ۱۹۷) که در پژوهش حاضر موردپذیرش قرارگرفته و توسعه داده خواهد شد.

جدول۴: ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری (تقی‌پور و اسماعیلی، ۱۳۹۷: ۱۹۷)

ابعاد	مؤلفه‌ها	شاخص‌ها
۱ قابلیت بازدارندگی	ثبات نظر	ثبات دیدگاه
	اعتبار	اثبات توانمندی، اراده اقدام سایبری
	قابلیت	تضعیف توانمندی دشمن، ارتقای توانمندی خودی
	ارتباط	ضمنی، صریح
۲ قابلیت پدافند	پدافند غیرعامل	پوشش، اختفاء،استتار،پراکندگی، فریب، موانع، جابجایی، مستحکم سازی، حسگر
	پدافند عامل	سلاح سایبری
۳ قابلیت برگشت پذیری	مقاومت	آسیب، اختلال
	قابلیت اطمینان	بازدید دوره‌ای، تجهیزات بومی، آزمون نفوذ، آستانه ریسک‌پذیری
	افزونگی	سخت‌افزار، نرم‌افزار، نیروی انسانی
	پاسخ و بازیابی	حفاظت از زیرساخت‌ها،کاهش اثر بحران، بازگشت به حالت عادی، بازسازی، ترمیم، توان‌بخشی

نتیجه‌گیری

هدف اصلی پژوهش حاضر ارائه مدل مفهومی دفاع سایبریِ امنیت‌محور جمهوری اسلامی ایران بوده است. در اجرای این تحقیق و برای پاسخ‌گویی به سؤالات پژوهش با انجام مطالعات اکتشافی، مطالعات نظری و با استفاده از اسناد و مدارک معتبر در پژوهش حاضر، با مطالعه نتایج پژوهش‌های قبل در خصوص دفاع سایبری کشور و ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری

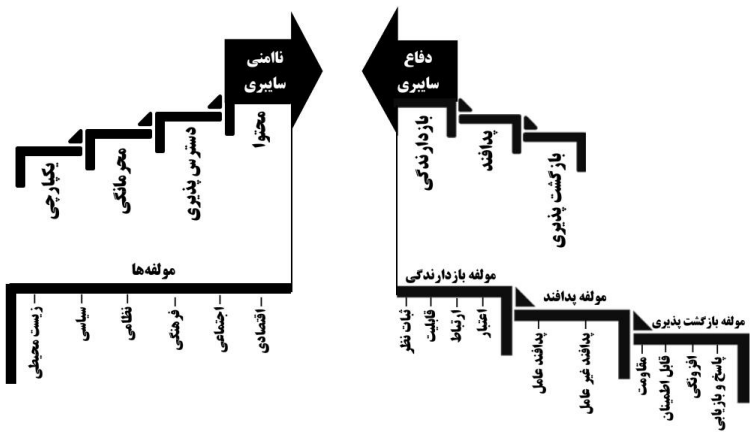
کشور؛ این موضوع که سازوکارهای دفاعی برای مقابله بـا چـه مجموعـه‌ای از تهدیـدات اسـت و اصولاً ابعاد، مؤلفه‌ها و شاخص‌های امنیت فضای سایبر کدامند.

این پژوهش دارای سه سؤال فرعی کلیدی «ابعاد، مؤلفه‌ها و شاخص‌های امنیت فضـای سـایبر کدام‌اند؟» و «ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری کشور کدام‌انـد؟» و «مـدل مفهـومی دفـاع سایبریِ امنیت کشور چگونه است؟» مدنظر قرار گرفت.

به‌منظور پاسخگویی به سؤالات فوق، ضمن جمع‌آوری مبـانی نظـری مـرتبط بـه جسـتجو و شناسایی ابعاد، مؤلفه‌ها و شاخص‌ها دفاع سایبری کشور پرداخته و ابعاد، مؤلفه‌هـا و شـاخص‌هـای امنیت فضا سایبر، جدول۴، ارائه گردید.

همچنین همان‌طور که پیشتر نیز اشاره گردید دفاع، مجموعه اقدامات لازم بـرای تضـمین یـک سطح مناسب امنیت است. بدیهی است برای اجرای اقدامات دفاعی مهم‌ترین موضوع اشـرافیت بـر محیط امنیتی است تا زوایای پیدا و پنهان آن در زمره طرح‌های دفاعی برای کسب یـک سـطحی از امنیت مناسب در تمام ابعاد و مؤلفه‌های امنیتی قرار گیرد.

مدل مفهومی دفاع سایبریِ امنیت‌محور تناظری است بین مجموعه اقدامات دفـاعی و مجموعـه ابعاد و مؤلفه‌های امنیتی فضای سایبر که در طراحـی‌هـای دفـاعی اقـدامات مـورد نیـاز را تضـمین می‌نماید. این مدل در شکل ۷ ارائه شده است.



شکل ۷ : مدل مفهومی دفاع سایبری امنیت‌محور

پیشنهادها

بر اساس نتایج حاصل از پژوهش، پیشنهادهای زیر ارائه می‌گردد:

تدوین اقدامات لازم به ازای هریک از مؤلفه‌های امنیت فضای سایبر؛

توجه ویژه به ظرفیت‌های موجود کشور در زمینه ارتقای بازدارندگی به ازای مؤلفه‌های امنیت سایبری؛

توجه ویژه به شناخت دقیق منافع ملی کشور در فضای سایبر و دفاع از آن‌ها در مقابل حملات سایبری.

در طی پژوهش، مواردی مشاهده شد که می‌تواند زمینه مطالعاتی مناسبی برای پژوهش‌های آتی باشد که به‌اختصار عبارت‌اند از:

مطالعه در زمینه ظرفیت‌های پدافند عامل کشور متناظر هریک از مؤلفه‌های امنیت سایبر؛

مطالعه در زمینه ظرفیت‌های پدافند غیر عامل متناظر هریک از مؤلفه‌های امنیت سایبر.

فهرست منابع و مآخذ

الف- منابع فارسی

- قرآن کریم.
- کتب و بیانات حضرت امام خمینی (رحمه ا... علیه).
- کتب و بیانات حضرت امام خامنه‌ای (مدظله‌العالی).
- ایمانی، هادی (۱۳۹۰)، جنگ‌های سایبری و مشکل یافتن منشا آن‌ها- مطالعه موردی استاکس نت، مقاله ارائه شده در نخستین همایش ملی دفاع سایبری، نخستین همایش ملی دفاع سایبری.
- تقی پور، رضا؛ اسماعیلی، علی (۱۳۹۷)، «طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران»،
- فصلنامه امنیت ملی، ۳۰.
- تقی پور، رضا؛ کارگری، مهرداد؛ لطیفی، میثم؛ فرجی‌پور، محمد رضا؛ محمدی، علی؛ صنیعی، محمدحسین؛ یزدانی،
- سعید (۱۳۹۷)، طراحی نظام دفاع سایبری کشور و تدوین الزامات تحقق آن (پایان‌نامه دکتری)، دانشگاه عالی دفاع ملی، تهران.
- دهخدا، علی اکبر (۱۳۷۷)، لغت‌نامه دهخدا (ج۱۴)، تهران: مؤسسه انتشارات و چاپ دانشگاه تهران.
- مرادی، محسن (۱۳۹۵)، کدگذاری داده‌ها در نظریه‌پردازی داده‌بنیاد (Grounded Theory) [علمی]. از http://analysisacademy.com/5209/کدگذاری-داده‌ها-در-نظریه‌پردازی-
- مرکز ملی فضای مجازی (۱۳۹۶)، فضای مجازی در ۲۰۲۵ [شورای عالی فضای مجازی]. از http://majazi.ir/general_content/81611/swd_id/13825/unitWdId/53812/فضای-محتوای=t?html.مجازی-در-۲۰۲۵-
- معین، محمد (۱۳۸۲)، فرهنگ فارسی معین (یک‌جلدی) دکتر محمد معین، تهران: معین.
- اخوان کاظمی، بهرام (۱۳۸۵)، امنیت و ابعاد آن در قرآن، مطالعات اسلامی، ش ۷۵.
- جورج سادوسکای جیمز اکس؛ دمپزی آلن گرینبرگ باربارا جی؛ مک آلن شوارتز (۱۳۸۴)، راهنمای امنیت فناوری اطلاعات.
- طباطبایی و دیگران (۱۳۹۲)، مهم ترین شاخص‌های اقتصادی کشور از ابتدای برنامه اول تادو سال اول برنامه پنجم (۱۳۶۸ تا ۱۳۹۱).
- رسولی، کریم؛ فرزین‌وش، اسداله (۱۳۹۳)، تبیین رابطه بین آزادی و امنیت اقتصادی با تشکیل سرمایه: شواهدی از کشورهای نوظهور و در حال توسعه.
- قنبری و دیگران (۱۳۹۵)، استحکام درونی قدرت ملی جمهوری اسلامی ایران در اندیشه مقام معظم رهبری با تأکید بر مؤلفه‌های دفاعی -امنیتی.
- موسوی و دیگران (۱۳۹۱)، ابعاد و مؤلفه‌های توسعه اجتماعی در برنامه‌های پنج‌گانه توسعه اقتصادی، اجتماعی، فرهنگی جمهوری اسلامی ایران.
- آزاد ارمکی و دیگران (۱۳۹۲)، بررسی و شناسایی شاخص‌های کاربردی توسعه اجتماعی (با استفاده از تکنیک دلفی)
- فاضلی و دیگران (۱۳۹۲)، توسعه اجتماعی، شاخص‌ها و جایگاه ایران در جهان.
- نسترن و دیگران (۱۳۹۱)، ارزیابی شاخص‌های پایداری اجتماعی با استفاده از فرایند تحلیل شبکه (ANP).
- عبدالعلی قوام (۱۳۷۱)، توسعه سیاسی و تحول اداری، تهران: نشر قومس.
- جلالی راد (۱۳۹۶)، شاخص‌های فرهنگ سیاسی جمهوری اسلامی ایران در بُعد کلان از دیدگاه نخبگان.
- نظری و دیگران (۱۳۹۲)، بررسی تأثیر مشارکت سیاسی بر توسعه سیاسی.

- مرادیان، محسن (۱۳۸۷)، "روش تحقیق در علوم اطلاعاتی": مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی.
- عبداله‌خانی، علی (۱۳۸۳)، نظریه‌های امنیتی: مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی.
- قانون جرایم رایانه‌ای.
- آیین‌نامه ساماندهی پایگاه‌های اینترنتی ایرانیان.
- سند چشم‌انداز بیست ساله.
- سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور.
- سند راهبردی نظام جامع فناوری اطلاعات کشور.
- سیاست‌های کلی نظام در حوزه امنیت فضای تولید و تبادل اطلاعات (افتا).
- برنامه پنجم توسعه کشور.
- سیاست‌های کلی نظام در حوزه پدافند غیرعامل.
- قانون انتشار دسترسی ازاد به اطلاعات.
- سند فرابخشی دولت الکترونیکی.
- آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی.
- برنامه جامع توسعه تجارت الکترونیکی کشور.
- حکم و مصوبات شورای عالی فضای مجازی کشور.
- سیاست‌های کلی برنامه ششم توسعه.
- سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور (۱۳۸۷).
- جورج سادوسکای، جیمزاکس؛ دمپزی، آلن گرینبرگ، باربارا جی؛ مک، آلن شوارتز (۱۳۸۴)، راهنمای امنیت فناوری اطلاعات.

ب- منابع لاتین

- Burt, David; Kleiner, Aaron; Nicholas, J. Paul; & Sullivan, Kevin. (2014). Cyberspace2025 Today’s decisions, Tomorrow’s Terrain, navigating the future of cybersecurity policy. Microsoft Corporation.
- Ravi Sadndhu,(2016), ”*Grand challenges in Data Usage Control*”
- Ravi Sandhu,(۲۰۱۳), Grand Challenges in Data Usage Control .
- FMETeam,(2013),”PESTEL Analysis Strategy Skills”
- Yale Center for Environmental Law & Policy Yale University et al, 2008, ENVIRONMENTAL PERFORMANCE INDEX, http://www.yale.edu/epi/
- FMETeam,(2013),”*PESTEL Analysis Strategy Skills*”
- Funded by Horizon 2020 Framwork Programme of European Union,(2017),”PESTELE Analysis”
- http://www.myindustry.ir/strategic-management/article/pest-analysis.html
- Funded by Horizon 2020 Framwork Programme of European Union,(2017),PESTELE Analysis
- FMETeam,(2013),”PESTEL Analysis Strategy Skills”
- FMETeam,(2013),”PESTEL Analysis Strategy Skills”
- Funded by Horizon 2020 Framwork Programme of European Union,(2017),PESTELE Analysis
- Tanya Sammut-Bonnici,(2015), PEST analysis