فصلنامه امنیت ملی
سال نهم، شماره ۳۳، پاییز ۱۳۹۸
مقاله اول از صفحه ۷ الی ۲٤

مقاله پژوهشی: ارائه الگوی راهبردی ارزیابی شبکه ملی اطلاعات

جمشید نصرت‌آبادی[۱]، محسن مؤمنه[۲]، محمدحسین یاقوت‌پور[۳] و محمد مهدی‌نژاد نوری[۴]

تاریخ دریافت: ۱۳۹۸/۰۲/۱۲ **تاریخ پذیرش: ۱۳۹۸/۰۵/۱۵**

چکیده

امروزه ایجاد شبکه ملی اطلاعات امن، به عنوان یک راهبرد اساسی در اعمال حاکمیت کشورها در فضای سایبر محسوب شده و بیشتر کشورها نسبت به ایجاد و ارائه خدمات بر روی این بستر اهتمام نموده‌اند. تعیین میزان امنیت شبکه‌های ملی اطلاعات نیازمند کمی‌سازی و تهیه الگوی ارزیابی است که بتوان بر مبنای آن امتیازدهی و نسبت به طراحی و یا انتخاب شبکه ملی اطلاعات امن اقدام نمود. در همین راستا هدف این تحقیق دستیابی به الگوی ارزیابی شبکه ملی اطلاعات امن برای جمهوری اسلامی ایران است؛ بنابراین سؤال اصلی تحقیق این است که الگوی راهبردی ارزیابی شبکه ملی اطلاعات امن برای جمهوری اسلامی ایران کدام است؟ همچنین نوع تحقیق از نظر هدف کاربردی- توسعه‌ای بوده و از روش تحقیق آمیخته استفاده شده است. بر این اساس، ابتدا در بخش مطالعات کتابخانه‌ای و با مراجعه به منابع معتبر مهم‌ترین شاخص‌ها و متغیرهای مؤثر بر ارزیابی شبکه ملی اطلاعات امن برای جمهوری اسلامی ایران استخراج گردید و با توجه به ماهیت و نقش آن‌ها، این متغیرها طبقه‌بندی گردیدند. در ادامه پرسشنامه‌ای طراحی و در اختیار صاحب‌نظران، خبرگان و کارشناسان سایبری قرار گرفت. بر اساس تجزیه و تحلیل پرسشنامه‌ها، مهم‌ترین متغیرها و شاخص‌های ارزیابی شبکه ملی اطلاعات امن برای جمهوری اسلامی ایران احصاء گردید. در نهایت با توجه به یافته‌های کتابخانه‌ای و میدانی و همچنین تجزیه و تحلیل‌های صورت پذیرفته، الگوی مفهومی و راهبردی ارزیابی شبکه ملی اطلاعات امن برای جمهوری اسلامی ایران پس از تأیید نهایی نخبگان سایبری، در قالب سه بعد، نوزده مؤلفه و هفتاد و یک شاخص ارائه گردیده است.

کلیدواژه‌ها: الگوی ارزیابی، شبکه ملی اطلاعات، امنیت، سایبر

۱. دانش آموخته دوره دکتری مدیریت راهبردی دفاع سایبری، دانشگاه عالی دفاع ملی (نویسنده مسئول)- Nosratabadi۱۱۰@chmail.ir
۲. دانشجوی دکتری مدیریت راهبردی دفاع سایبری، دانشگاه عالی دفاع ملی- Momeneh@chmail.ir
۳. دانشجوی دکتری مدیریت راهبردی دفاع سایبری، دانشگاه عالی دفاع ملی- Hosain۳۰۳۰@chmail.ir
٤. دانشیار دانشگاه صنعتی مالک اشتر، Mmn.noori@chmail.ir

مقدمه:

فضای مجازی را می‌توان مولود بلامنازع بلوغ فناوری اطلاعات و ارتباطات دانست. فضایی پیچیده متشکل از سخت‌افزارها و نرم‌افزارهای ارتباطی و محاسباتی، سیستم‌های کنترلی، اطلاعات، انسان و تعاملات بین آن‌ها. امروزه فضای مجازی آن‌چنان با ابعاد مختلف زندگی بشر درهم تنیده است که بدون آن امکان تداوم زندگی فردی و اجتماعی غیرممکن می‌نماید. در واقع در استفاده کردن یا نکردن از این فضا هیچ‌گونه حق انتخابی وجود ندارد. به همین دلیل بهترین گزینه در مورد استفاده از این فضا، بهره‌گیری از فرصت‌ها و پرهیز از تهدیدات آن است. در این راستا بسیاری از کشورهای صاحب قدرت سایبری برای مدیریت فضای سایبر خود مبادرت به طراحی و اجرایی نمودن شبکه ملی اطلاعات بومی نموده‌اند. شبکه ملی اطلاعات به عنوان زیرساخت ارتباطی فضای مجازی کشور شبکه‌ای مبتنی بر قرار داد اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده است به صورتی که درخواست‌های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند به هیچ وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت، خصوصی و امن داخلی در آن فراهم شود (مرکز ملی فضای مجازی، ۱۳۹۲).

بیان مسئله. شکل‌گیری و توسعه شبکه جهانی اینترنت به‌گونه‌ای بوده است که اصولاً مسئله‌ای به نام امنیت ملی برای کشورها مطرح نبوده است و حتی بعضی به دنبال از بین بردن مرزها بوده و شبکه جهانی را فضایی می‌دانند که مرزهای ملی در آن بی‌معناست. درحالی که این طرز فکر را مبدعان این فضا ایجاد نموده‌اند تا در پس آن بتوانند سلطه جهانی خود را به پیش ببرند. شبکه ملی اطلاعات کشور از ابتدای شکل‌گیری تا به امروز بر اساس نیازهای عملیاتی و به منظور خدمت‌رسانی هرچه بیشتر در حوزه فناوری اطلاعات و ارتباطات توسعه یافته که به نظر می‌رسد این توسعه تأمین‌کننده همه ابعاد مورد نظر در حوزه امنیت نبوده است. توسعه پرسرعت ابعاد و مرزهای فضای سایبر و همچنین تغییرات غیر قابل پیش‌بینی آن نیز بر این فقدان اثرگذار بوده است. پرواضح است که امنیت جزء مؤلفه‌های اصلی این شبکه است و قطعاً می‌بایست قبل از توسعه شبکه با نگاه اقتصادی و وابسته شدن زیرساخت‌های کشور به آن به‌طور راهبردی مورد توجه قرار گیرد. کشورهایی مانند چین، روسیه، کره جنوبی و برزیل بخشی از این کشورها هستند که سعی کرده‌اند شبکه داخل کشورشان را از اینترنت جهانی مستقل کنند؛ اما چگونه می‌توان یک شبکه ملی اطلاعات امن را ارزیابی نمود. این تحقیق در پی آن است که با احصای شاخص‌ها و متغیرهای اثرگذار بر لایه زیرساخت شبکه ملی اطلاعات و روابط احتمالی میان آن‌ها، الگوی

ارزیابی را با لحاظ حفظ و ارتقاء کارکردهای شبکه مذکور انتخاب نماید. لذا نبود یک الگوی ارزیابی برای شبکه ملی اطلاعات امن به عنوان مسئله اصلی این تحقیق مدنظر است.

اهمیت تحقیق. ارائه الگوی راهبردی ارزیابی شبکه ملی اطلاعات امن، ابزار و راهنمایی مناسب برای سیاست‌گذاری در حوزه فناوری اطلاعات و ارتباطات کشور، ایجاد زمینه همدلی و وفاق در حوزه فضای مجازی کشور از طریق ایجاد گفتمان و تعاریف مشترک، کمک به امکان ارزیابی و در صورت نیاز بازنگری معماری شبکه ملی اطلاعات فعلی کشور

ضرورت تحقیق. نبود الگوی ارزیابی شبکه ملی اطلاعات امن کشور، اجرایی نشدن سیاست‌های کلان در حوزه امنیت فضای مجازی کشور، عدم وجود معیارهای سنجش امنیت در الگوی شبکه ملی اطلاعات، مغفول ماندن وجوه امنیت همه جانبه در شبکه ملی اطلاعات

هدف اصلی؛ دستیابی به الگوی راهبردی ارزیابی شبکه ملی اطلاعات امن جمهوری اسلامی ایران

اهداف فرعی؛ دستیابی به ابعاد، مؤلفه‌ها و شاخص‌های الگوی ارزیابی شبکه ملی اطلاعات امن، احصاء ارتباط میان ابعاد، مؤلفه‌ها و شاخص‌های الگوی ارزیابی شبکه ملی اطلاعات جمهوری اسلامی ایران

سؤال اصلی؛ الگوی راهبردی ارزیابی شبکه ملی اطلاعات امن جمهوری اسلامی ایران کدام است؟

سؤالات فرعی؛ ابعاد، مؤلفه‌ها و شاخص‌های الگوی ارزیابی شبکه ملی اطلاعات جمهوری اسلامی ایران کدامند؟ ارتباط میان ابعاد، مؤلفه‌ها و شاخص‌های الگوی ارزیابی شبکه ملی اطلاعات جمهوری اسلامی ایران کدامند؟

مبانی نظری:

با توجه به موضوع تحقیق، بررسی‌های مختلفی بر روی پژوهش‌های علمی و مرتبط با موضوع صورت پذیرفت که در زیر به برخی از مهم‌ترین موضوعات که در مؤلفه‌ها و متغیرهایی با موضوع تحقیق مشترک هستند اشاره‌شده است:

- در سال ۱۳۹٤ رساله‌ای با عنوان تدوین راهبردهای پدافند غیرعامل زیرساخت‌های ارتباطی شبکه ملی اطلاعات کشور در برابر تهدیدات سایبری توسط سیدعلی میررفیع در دانشگاه عالی دفاع ملی انجام پذیرفت که در این تحقیق پس از احصاء ۱۹ تهدید سایبری حوزه زیرساخت ارتباطی شبکه ملی اطلاعات کشور و ارزیابی و پیامدسنجی آن‌ها؛ نسبت

به تدوین ۱۰ راهبرد جهت مقابله با این تهدیدات اقدام شده و پس از اخذ نظر خبرگان و بررسی‌های مربوطه در نهایت سه راهبرد اولویت‌دار زیر ارائه شده‌است: (میررفیع،۱۳۹٤)

۱- مصون‌سازی، استحکام‌بخشی و امن‌سازی زیرساخت‌های ارتباطی حیاتی، حساس و مهم شبکه ملی اطلاعات کشور در برابر تهدیدات و حملات سایبری و الکترومغناطیس

۲- بهره‌گیری از زیرساخت‌های ارتباطی خاص مراکز حیاتی و حساس شبکه ملی اطلاعات کشور بر اساس ملاحظات، اصول و ضوابط پدافند غیرعامل با سطح پایداری ملی

۳- حمایت از محصولات سایبری بومی و افزایش سالانه سهم این محصولات در سبد خرید زیرساخت ارتباطی شبکه ملی اطلاعات کشور

- در سال ۱۳۹٦ رساله‌ای با عنوان طراحی الگوی راهبردی بومی امنیت فضای مجازی کشور توسط احسان شهیر در دانشگاه عالی دفاع ملی صورت پذیرفت که در این رساله مدل مفهومی راهبردی بومی امنیت فضای مجازی کشور برگرفته از چهار بعد اصلی به دست آمده است: (شهیر،۱۳۹٦)

۱- بعد حوزه تأمین‌کنندگان و عوامل عملیاتی امنیت فضای مجازی (بازیگران، نقش‌آفرینان، ذی‌نفعان)

۲- بعد بستر، آسیب‌پذیری‌های امنیت فضای مجازی

۳- بعد روش، تار و پود (رویکرد بومی‌سازی، ارزش‌ها و اهداف) امنیت فضای مجازی

٤- بعد کنترل و فرماندهی، کنترل (ابعاد عملکردی، اقدامات، راهکارها)، مهندسی امنیت فضای مجازی

- در کنفرانس بین‌المللی پژوهش‌های کاربردی در فناوری اطلاعات، کامپیوترو مخابرات- ۱۳۹٤ مقاله‌ای با عنوان ارائه ساختاری نوین برای مدیریت و کنترل بهتر درخواست‌ها در شبکه ملی اطلاعات بر پایه معماری ***SDN*** توسط محسن پورشیخی و جواد اکبری ترکستانی ارائه گردید که ساختار جدیدی را برای مدیریت و کنترل بهتر درخواست‌ها در این نوع شبکه‌ها ارائه شده که همزمان می‌تواند از درخواست‌های داخلی و خارجی پشتیبانی نماید و برای دسترسی به داده‌های داخلی و اینترنت از یک ***IP*** استفاده می‌نماید و کنترلرهای تعریف شده در این ساختار می‌توانند به‌گونه‌ای با اینترنت نیز در ارتباط باشند که ساختارشان با هم مطابقت داشته باشد چراکه در کنترلر مرکزی ساختار جدید، تبدیل به درخواست‌های داخلی را به ساختار اینترنت و برعکس را انجام می‌دهد که با

این امکان تبدیل درخواست‌ها، دیگر آن دغدغه قبلی حل خواهد شد (پورشیخی،۱۳۹٤).

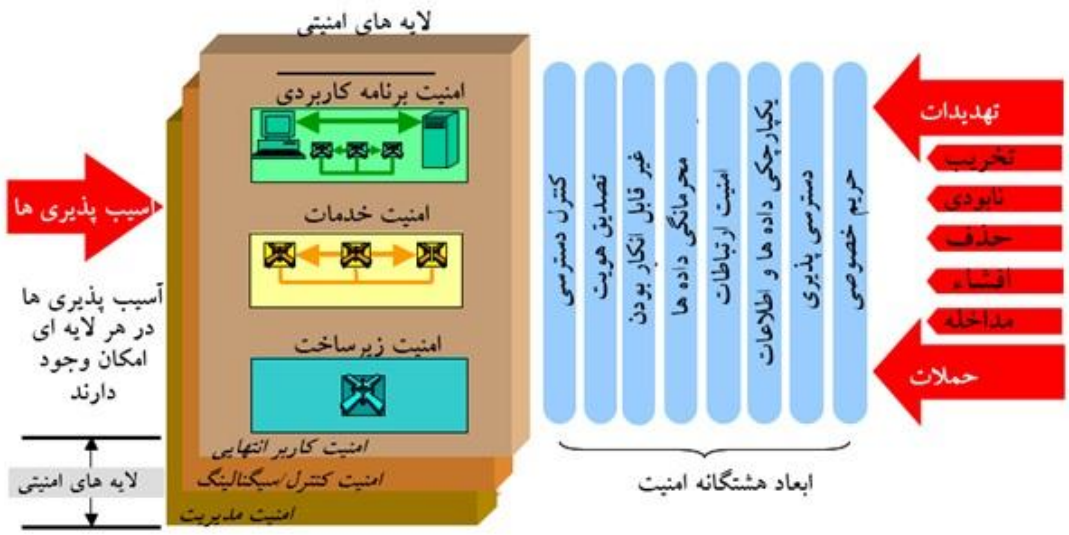
شبکه ملی اطلاعات. نخستین بار در سال ۱۹۹۱ زیرساخت ملی اطلاعات البته با عنوان شبکه ملی اطلاعات در ایالات‌متحده آمریکا توسط ال گور سناتور وقت آمریکا، طرح شد. هدف این شبکه پردازش با کیفیت بالا در ایالات‌متحده آمریکا بوده است. این زیرساخت چیزی بیش از صرف ادوات فیزیکی است که برای انتقال، نگهداری، پردازش و نمایش صدا، داده‌ها و تصاویر به کار می‌رود. این شبکه شامل گستره وسیعی از کارکردهای تعاملی، خدمات متناسب با کاربر و پایگاه‌های داده چندرسانه‌ای بوده است. این پروژه در بسیاری کشورها اجرا شده است.(نامداریان، ۲۰۱۷) همچنین شبکه ملی اطلاعات بستری است امن، پیشرفته و متکی به جدیدترین فناوری‌های نوین و بومی برای تحقق فضای مجازی بر اساس ارزش‌های والای اسلامی- ایرانی جهت رسیدن به اهداف چشم‌انداز ایران ۱٤۰٤ بر اساس مصوبه اول جلسه پانزدهم شورای عالی فضای مجازی، «شبکه ملی اطلاعات» به عنوان زیرساخت ارتباطی فضای مجازی کشور، شبکه‌ای مبتنی بر قرار داد اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده‌ای است به صورتی که درخواست‌های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شود به هیچ وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت، خصوصی و امن داخلی در آن فراهم شود (مرکز ملی فضای مجازی، ۱۳۹۲).

فضای مجازی دارای یک مدل چند لایه‌ای است که بستر آن، زیرساخت ارتباطی است که شبکه ملی اطلاعات آن را محقق خواهد ساخت. (شکل ۱)

شکل (۱)؛ بستر شبکه ملی اطلاعات (مرکز ملی فضای مجازی، ۱۳۹۵)

اهداف کیفی شبکه ملی اطلاعات شامل موارد زیر است:

- معماری قابل ارتقاء برای شبکه ملی اطلاعات
- بومی‌سازی فناوری‌های سخت‌افزاری و نرم‌افزاری با تکیه بر نرم‌افزارهای متن‌باز و توسعه معماری باز
- **شکل (۲)؛ مدل پیشنهادی امنیت در شبکه ملی اطلاعات (مرکز ملی فضای مجازی،۱۳۹۵)**



- بالا بردن جایگاه ایران در رتبه‌بندی توسعه ارتباطات
- افزایش درصد نفوذ اینترنت در کشور مطابق با استانداردهای جهانی
- بهبود وضعیت شاخص‌های آمادگی الکترونیکی
- ایجاد زمینه‌های لازم برای توسعه علمی کشور
- ایجاد زمینه‌های نوین شغلی و اقتصادی و افزایش تولید ناخالص ملی
- ارتقاء شاخص‌های امنیتی، پایین آوردن ریسک ضربه‌پذیری و مقابله با تحریم‌های احتمالی
- ایجاد امنیت و مصون ماندن اطلاعات از حملات اینترنتی
- برطرف کردن نیازهای کشور در حوزه‌های کسب و کار الکترونیکی، سلامت الکترونیک و آموزش الکترونیک (همان)

موتور جستجوگر ملی و رایانامه ملی: موتور جستجوی ملی یک موتور محرکه برای توسعه صنعت فناوری اطلاعات کشور است و از سوی دیگر دسترسی موتورهای جستجوی خارجی به اطلاعات مهم و محرمانه کشور از بین خواهد رفت؛ همچنین سرعت جستجوها و بهره‌برداری از اطلاعات افزایش خواهد یافت؛ بنابراین مباحثی از قبیل ذهن‌خوانی گوگل، علاقه‌مندی کاربران، حوزه فعالیت کاربران، تخصص و حوزه عملکرد اینترنت در ایران توسط کشورهای بیگانه از بین خواهد رفت (هلیلی و همکاران، ۱۳۹۳).

استاندارد مدیریت شبکه‌های ارتباطی[۱]: اتحادیه جهانی مخابرات ***(ITU)*** فعالیتی را در جهت استانداردسازی مدیریت شبکه انجام داد که اولین نتایج آن در سال ۱۹۸۸ به‌صورت یک سری توصیه‌نامه منتشر شد (***Recommendation T-ITU ۳۰۱۰.M***) و روند تکامل آن هنوز ادامه دارد. به این ترتیب ***TMN*** را یک مجموعه استاندارد برای مدیریت شبکه ارتباطی دانست که یک چارچوب مدیریتی با جزئیات نسبتاً کافی مشخص می‌کند و از سازندگان و سرویس‌دهندگان ارتباطی می‌خواهد که این استانداردها را به منظور همگرا کردن سیستم‌های مدیریتی و به حداقل رساندن مشکلات در این زمینه رعایت کنند. هدف ***TMN***، پشتیبانی کامل مدیریتی در زمینه‌های طراحی، نصب، بهره‌برداری، اداره، نگهداری و تأمین شبکه‌ها و سرویس‌های آن است. به همین منظور ***T-ITU*** مدیریت را به پنج زمینه عملیاتی مدیریتی به صورت زیر تعریف نموده است ***(ITU,۲۰۰۰):***

۱- مدیریت خطا[۲] (گزارش محل خطا، رفع خطا با توجه به گزارش به‌صورت مکانیزه، آزمایش و چگونگی کنترل مقادیر اندازه‌گیری شده، گزارش نتایج کار، کنترل و بهبود شبکه، کنترل خطا و رفع آن)

۲- مدیریت پیکربندی[۳] (درخواست و گزارش پیکربندی، مونیتور کردن یک جزء جدید، اختصاص دادن و حذف کردن و تعیین وضعیت سرویس‌دهی شبکه، تنظیم سطح آستانه، قطع اتصال بین دو کانال، تنظیم و درخواست گزارش)

۳- مدیریت حسابداری[٤] (تعیین هزینه‌های جاری و تهیه صورتحساب‌ها)

۱- TMN: Telecommunications management Network
۲- Fault Management
۳- Configuration Management
٤- Accounting Management

٤- مدیریت عملکرد[1] (تنظیم مقادیر آستانه‌ای کیفیت سیستم، زمان‌بندی گزارش اطلاعات مربوط به کیفیت سیستم، درخواست برنامه زمانی گزارش‌دهی کیفیت سیستم، تجزیه و تحلیل عملکرد سیستم شامل گزارش و درخواست تجزیه و تحلیل اطلاعات مربوط به کیفیت سیستم)

٥- مدیریت امنیتی[2] (حفاظت دسترسی افقی، حفاظت دسترسی عمودی، مدیریت مسیرهای جستجو، درخواست و ارسال اطلاعات مربوط به اعتبار امنیتی، گزارش نتایج اثبات صحت هویت، هشدارهای حفاظتی، مسیرهای جستجو)

جدول (۱) مدل مرجع امنیت سایبری عمومی سازمان ملل

(ITU: Global Cybersecurity Index ۲۰۱۵/۱٦ Reference Model)

ردیف	*Indicator*	شاخص
۱	*Legal measures*	تمهیدات قانونی
۲	*Cybercriminal legislation*	قانون‌گذاری جرائم سایبری
۳	*Cybersecurity regulation*	مقررات امنیت سایبری
٤	*Cybersecurity training*	آموزش امنیت سایبری
٥	*Technical measures*	تمهیدات فنی
٦	*National CERT/CIRT/CSIRT*	تیم امداد و نجات رایانه‌ای ملی
۷	*Government CERT/CIRT/CSIRT*	تیم امداد و نجات رایانه‌ای دولت
۸	*Sectoral CERT/CIRT/CSIRT*	تیم امداد و نجات رایانه‌ای بخشی
۹	*Cybersecurity standards implementation framework for organizations*	چارچوب پیاده‌سازی استانداردهای امنیت سایبری برای سازمان‌ها
۱۰	*Cybersecurity standards and certification for professionals*	گواهی و استانداردهای امنیت سایبری برای متخصصین
۱۱	*Child online protection*	حفظ برخط کودکان
۱۲	*Organizational measures*	تمهیدات سازمانی
۱۳	*Strategy*	راهبرد
۱٤	*Responsible agency*	نمایندگی پاسخگو
۱٥	*Cybersecurity metrics*	شاخص‌های امنیت سایبری
۱٦	*Capacity building*	ظرفیت‌سازی

۱-Performance Managment

۲-Security management

۱۷	*Standardization bodies*	مبادی استانداردسازی
۱۸	*Cybersecurity best practices*	تجربیات موفق امنیت سایبری
۱۹	*Cybersecurity research and development programmes*	برنامه‌های توسعه و تحقیق امنیت سایبری
۲۰	*Public awareness campaigns*	تشکل‌های هشداردهی عمومی
۲۱	*Cybersecurity professional training courses*	دوره‌های آموزشی تخصصی امنیت سایبری
۲۲	*National education programmes and academic curricula*	برنامه‌های آموزش ملی و سرفصل‌های دانشگاهی
۲۳	*Incentive mechanisms*	مکانیسم‌های تشویقی
۲٤	*Home-grown cybersecurity industry*	صنعت امنیت سایبری بومی
۲٥	*Cooperation*	همکاری (تعامل)
۲٦	*Bilateral agreements*	موافقت‌نامه‌های دوجانبه
۲۷	*Multilateral agreements*	موافقت‌نامه‌های چندجانبه
۲۸	*International fora participation*	مشارکت بین‌المللی
۲۹	*Public-private partnerships*	شراکت بخش خصوصی و عمومی
۳۰	*Interagency partnerships*	مشارکت بین بنگاهی

نظام دفاع سایبری کشور و تدوین راهبردهای آن: رامک و همکاران در تحقیقی که به‌منظور طراحی نظام دفاع سایبری کشور انجام داده‌اند مدل مفهومی نهایی را از ترکیب دوازده فرآیند به شرح ذیل احصا نموده‌اند: (رامک و همکاران،۱۳۹٤)

برنامه‌ریزی، هماهنگی، یکپارچه‌سازی، همزمان سازی و هدایت فعالیت‌ها

فرهنگ‌سازی، آموزش، آگاه‌سازی و اطلاع‌رسانی

همکاری و تعاملات بین‌المللی

مشارکت بخش‌های دولتی و خصوصی

بومی‌سازی، استانداردسازی، نوآوری و ایجاد خودکفایی

ایجاد رمزنگاری و امنیت اطلاعات متمرکز

نظارت و ارزیابی

ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری

پیگیری مؤثر قانونی و حقوقی جرائم و حملات سایبری

پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری

حفظ و ارتقاء آمادگی و تقویت پایداری در مقابل حملات سایبری

بازیابی و مدیریت بحران

راهبردهای سایبری کشورها در حوزه شبکه و زیرساخت

اهداف راهبردی مأموریت‌های سایبری وزارت دفاع ایالات‌متحده آمریکا:

- ایجاد و آماده‌به‌کار نگه‌داشتن نیروها و توانمندی برای هدایت عملیات سایبری
- دفاع از شبکه‌های اطلاعات وزارت دفاع، امن کردن اطلاعات و محدود کردن مخاطرات موجود در برابر مأموریت‌های وزارت دفاع
- آمادگی برای دفاع از آمریکا و منافع حیاتی، در برابر پیامدهای قابل توجه حملات سایبری
- ایجاد و ادامه عملیات سایبری ماندگار و طرح‌ریزی برای استفاده از این گزینه‌ها به‌منظور کنترل مناقشات رزمی و شکل‌دهی محیط‌های رزمی در تمام سطوح
- ایجاد و ادامه پیمان‌های بین‌المللی مستحکم و همکاری‌ها برای مقابله با تهدیدات مشترک و افزایش امنیت و پایداری بین‌المللی. ***(United State Department of Defence*** ۲۰۱۵***)***

اهداف راهبردی مأموریت‌های سایبری انگلیس: در راهبرد سایبری انگلیس، چشم‌انداز سایبری این کشور را امن و تاب‌آور در برابر تهدیدات سایبری و نیز موفق و با اعتماد به نفس در دنیای دیجیتال در سال ۲۰۲۱ برشمرده است و برای تحقق این چشم‌انداز بر اجرای اقدام‌های زیر تأکید شده است.

دفاع: شامل پاسخ مؤثر به تهدیدات و حوادث سایبری، حفاظت از کسب و کار و زیرساخت‌ها و این‌که بخش‌های عمومی باید توانایی دفاع از خود را داشته باشند.

بازدارندگی: با شناسایی، درک، بررسی و مختل نمودن اقدام‌های خصمانه علیه انگلستان، باید هدف سختی در برابر تجاوزات سایبری باشد. باید آفند سایبری را انجام دهیم.

توسعه: به منظور غلبه بر تهدیدات و چالش‌های آینده، باید نوآوری و رشد صنعت امنیت سایبری و نیز تحقیق و توسعه و ارتقای مهارت‌های در سراسر انگلیس انجام شود.

اقدام‌های بین‌المللی: بها دادن به اقدام‌های بین‌المللی در مشارکت‌ها و شکل دادن به فضای سایبری که منافع ملی و اقتصاد انگلیس را گسترده‌تر می‌کند. ***(uk national security strategies,*** ۲۰۱۶***)***

اهداف راهبردی مأموریت‌های سایبری اتحادیه اروپا:

- دستیابی به تاب‌آوری سایبری
- کاهش جدی جرم‌های سایبری (قانون‌گذاری قوی و مؤثر- ارتقاء قابلیت‌های عملکردی در مبارزه با جرائم سایبری – توسعه هماهنگی و تعامل در سطح اتحادیه اروپا)
- توسعه قابلیت‌ها و سیاست‌های دفاع سایبری مرتبط با امنیت عمومی و سیاست دفاعی
- توسعه منابع فناورانه و صنعتی برای امنیت سایبری
- ایجاد یک سیاست هماهنگ بین‌المللی سایبری برای اتحادیه اروپا و ترویج ارزش‌های اصلی اتحادیه اروپا
- فعالیت‌های مرتبط با ترویج استانداردهای امنیتی مدنظر اتحادیه اروپا و منطبق با ارزش‌های اساسی همچون کرامت انسانی، آزادی، مردم‌سالاری، برابری، قانون-مداری و رعایت حقوق اساسی.

همکاری نزدیک با سازمان‌هایی همچون شورای اروپا، ***OSCE***[۱]، ***NATO***، ***UN***، ***AU***، ***ASEAN*** و ***OAS***[۲] تلاش در جهت گسترش اینترنت باز و جلوگیری از اعمال محدودیت در استفاده آزادانه از آن با به‌کارگیری حسگرها. ***(Dimitra Liveri ,۲۰۱٤)***

اینترنت نظامی در روسیه: در روسیه شبکه نظامی به شبکه جهانی اینترنت متصل نیست و همه رایانه‌های وصل شده به آن از وصل شدن به فلش درایوهای ***USB*** و دیسک‌های سخت بیرونی تأیید نشده مصون هستند .بخشی از تأسیسات اینترنت نظامی فاقد ارتباط با شبکه جهانی اینترنت در ساختارهای اجاره شده از شرکت دولتی «روس تله کام» و وزارت دفاع روسیه مستقر شده است ***(ir.sputniknews.com,۲۰۱٦) .***

روش تحقیق:

این تحقیق با توجه به اینکه ابزار و راهنمایی برای سیاست‌گذاری پیشنهاد می‌کند و امکان ارزیابی شبکه ملی اطلاعات جمهوری اسلامی ایران و در صورت نیاز بازنگری را فراهم می‌سازد؛ بنابراین

۱-Organization for economic cooperation and development

۲-Of American States

کاربردی است و با توجه به ارائه الگوی ارزیابی شبکه ملی اطلاعات جمهوری اسلامی ایران و توسعه دانش در این زمینه، توسعه‌ای هست؛ بنابراین این تحقیق با توجه به موضوع و هدف تحقیق، از نوع کاربردی- توسعه‌ای است. همچنین روش تحقیق به کار گرفته‌شده در این پژوهش، روش آمیخته است.

حجم جامعه آماری در تحقیق حاضر از خبرگان و متخصصان کشور در حوزه سایبری تشکیل گردیده است و حجم نمونه در این تحقیق به حد کفایت از میان جامعه آماری است که به شیوه نمونه‌گیری هدفمند به عنوان نمونه انتخاب شد و با روش اشباع نظری نمونه‌گیری انجام شده است. ابزار اصلی جمع‌آوری داده‌های اولیه در این تحقیق پرسشنامه است که با استفاده از روش میدانی داده‌های مربوطه گردآوری شدند. روایی پرسشنامه از دو جنبه روایی ظاهری و محتوا به جهت روشن و بدون ابهام بودن گویه‌ها و همچنین کفایت کمیت و کیفیت آن‌ها توسط خبرگان و صاحب‌نظران و اساتید دانشگاه تأیید گردید. همچنین به جهت روایی سازه از فن تحلیل عاملی استفاده گردید. در این تحقیق برای محاسبه پایایی یا هماهنگی درونی ابزار اندازه‌گیری که خصیصه‌های مختلف را اندازه‌گیری می‌کند از روش آلفای کرونباخ استفاده گردید.

یافته های تحقیق:

ابتدا در بخش مطالعات کتابخانه‌ای و با مراجعه به منابع معتبر مهم‌ترین شاخص‌ها و متغیرهای مؤثر بر ارزیابی شبکه ملی اطلاعات جمهوری اسلامی ایران استخراج گردید و با توجه به ماهیت و نقش آن‌ها، این متغیرها در ابعاد امنیتی، مدیریتی و فناورانه طبقه‌بندی گردیدند. در ادامه پرسشنامه‌ای طراحی و در اختیار صاحب‌نظران، خبرگان و کارشناسان قرار گرفت. بر اساس تجزیه و تحلیل پرسشنامه‌ها، مهم‌ترین متغیرها و شاخص‌های ارزیابی شبکه ملی اطلاعات جمهوری اسلامی ایران احصاء گردید. در همین راستا فرضیات مطرح شده مورد آزمون قرار گرفت که نتایج به شرح ادامه است:

فرضیه الف: ***H۰***: بعد امنیتی بر شبکه ملی اطلاعات مرتبط نیست. ***H۱***: بعد امنیتی بر شبکه ملی اطلاعات مرتبط است.

جدول ۲: آزمون ارتباط بعد امنیتی

آزمون	متغیر	میانگین	انحراف معیار	تفاوت میانگین	حدود اطمینان		مقدار t	سطح	نتیجه
					حد بالا	حد پایین	محاسبه‌شده	معناداری	آزمون
T یک نمونه‌ای	بعد امنیتی	۴.۳۰۸۹	.۳۴۶۳۸	۱.۳۰۸۸۵	۱.۴۱۸۲	۱.۱۹۹۵	۲۴.۱۹۵	/۰۰۰	قبول H۱

*P< ۰/۰۵، **P< ۰/۰۱ و N = ٤١

با توجه به خروجی جدول، چون سطح معناداری کمتر از میـزان خطـای ۰۵/ بـه دسـت آمـده فرض ادعای محقق یعنی فرضیه ۱**H** مورد تأیید واقع می‌گردد.

فرضیه ب: **H۰**: بعد فناورانه بر شبکه ملی اطلاعات مرتبط نیست. ۱**H**: بعد فناورانـه بـر شـبکه ملی اطلاعات مرتبط است.

جدول ۳: آزمون ارتباط بعد فناورانه

آزمون	متغیر	میانگین	انحراف معیار	تفاوت میانگین	حدود اطمینان		مقدار t	سطح معناداری	نتیجه آزمون
					حد بالا	حد پایین	محاسبه‌شده		
Tیک نمونه‌ای	*بعد فناورانه*	٤.٢ ٩١١	.٣٦ ٨٦٣	١.٢٩ ١١٤	١.٤ ٠٧٥	١.١ ٧٤٨	٢٢.٤ ٢٧	٠٠ /٠	*قبول H١*
*P< ۰/۰۵، **P< ۰/۰۱ و N = ٤١									

با توجه به خروجی جدول، چون سطح معناداری کمتر از میـزان خطـای ۰۵/ بـه دسـت آمـده فرض ادعای محقق یعنی فرضیه ۱**H** مورد تأیید واقع می‌گردد. این بدان معناست که از نظر جامعـه پاسخ دهنده، بعد فناورانه بر الگوی ارزیابی شبکه ملی اطلاعات با رویکرد زیرساختی مـرتبط بـوده است.

فرضیه ج: **H۰**: بعد مدیریتی بر شبکه ملی اطلاعات مرتبط نیست. ۱**H**: بعد مدیریتی بـر شـبکه ملی اطلاعات مرتبط است.

جدول ٤: آزمون ارتباط بعد مدیریتی

آزمون	متغیر	میانگین	انحراف معیار	تفاوت میانگین	حدود اطمینان		مقدار t	سطح معناداری	نتیجه آزمون
					حد بالا	حد پایین	محاسبه‌شده		
T یک نمونه‌ای	*بعد مدیریتی*	٤.٢ ١٥٩	.٤١ ٨٩٩	١.٢١ ٥٨٥	١.٣ ٤٨١	١.٠ ٨٣٦	١٨.٥ ٨١	٠٠ /٠	*قبول H١*
*P< ۰/۰۵، **P< ۰/۰۱ و N = ٤١									

با توجه به خروجی جدول، چون سطح معناداری کمتر از میـزان خطـای ۰۵/ بـه دسـت آمـده فرض ادعای محقق یعنی فرضیه ۱**H** مورد تأیید واقع می‌گردد. این بدان معناست که از نظر جامعـه پاسخ دهنده، بعد مدیریتی بر الگوی ارزیابی شبکه ملی اطلاعات با رویکرد زیرساختی مرتبط بـوده است.

نتایج تحقیق: در طراحی الگوی راهبردی ارزیابی شبکه ملی اطلاعات امن، پس از تعیین

مهم‌ترین متغیرها و عوامل مؤثر از طریق روش اکتشافی و بررسی ارتباط و تأثیر آن‌ها بر الگوی مذکور از طریق تجزیه و تحلیل داده‌ها، محقق در پی پاسخ به سؤالات تحقیق و ارائه الگوی راهبردی ارزیابی شبکه ملی اطلاعات جمهوری اسلامی ایران است که بر اساس یافته‌های تحقیق، به سؤالات این پژوهش پاسخ داده می‌شود:

سؤال فرعی اول: ابعاد، مؤلفه‌ها و شاخص‌های ارزیابی شبکه ملی اطلاعات کدامند؟

جدول ۵: بعد امنیتی

مؤلفه	شاخص
تجهیزات	بومی بودن
	به روز بودن
	اثربخش بودن
	قابلیت پیکربندی شدن مناسب
سیاست‌ها/ قوانین/ مقررات	حاکمیت امنیت
	اسناد راهبردی امنیتی
ایمنی و حفاظت فیزیکی	به‌کارگیری تجهیزات کنترل دسترسی عادی و بیومتریک
	استقرار سامانه‌های نظارت تصویری و مراقبت الکترونیکی
	حفاظ‌های فیزیکی
	مقاوم در برابر پالس الکترومغناطیس (EMP)
عامل انسانی	تخصص
	تعهد و صلاحیت
	سطح مهارت امنیتی
	میزان آموزش
	سطح فرهنگ امنیتی
مدیریت ریسک	شفافیت و جامعیت سند مدیریت ریسک
	میزان اجرای سند مدیریت ریسک
	به‌روزرسانی سند مدیریت ریسک
مدیریت رخداد	زمان شناسایی
	زمان واکنش
	زمان بازیابی
کنترل دسترسی	استقرار فرآیندهای کنترل دسترسی
	استقرار تجهیزات امنیتی

سامانه نظارت	یکپارچگی
	کنترل‌پذیری
	قابلیت ارتقاء
	به‌روز بودن
	جامعیت
	مدیریت ثبت رویداد
	استانداردهای LI
	حریم خصوصی
اعمال استانداردها	استانداردهای سری ۲۷۰۰۰
	ISMS

جدول ٦: بعد فناورانه

مؤلفه	شاخص
استقلال	مسیریابی داخلی (مستقل از اینترنت)
	اعمال حاکمیت و مدیریت ملی
فنی	پهن باند
	دسترسی همگانی
	قابلیت تحرک (Mobility)
	سرعت بالا – مانیتورینگ (رصد و پایش)
دانشی	قابلیت ارتقاء و به‌روزرسانی
	مدیریت اثربخش دانش
	دانش نصب، راه‌اندازی، تعمیر و نگهداری
	دانش طراحی
تجهیزات	بومی بودن
	به‌روز بودن
	قابلیت ارتقاء
	رقابت‌پذیری
	پیکربندی متمرکز
تعامل‌پذیری	اتصال به اینترنت
	مراکز داده
	ارتباط با اینترانت‌ها و شبکه‌های اختصاصی
	VPN
	تلفیق داده‌ها

	اشتراک اطلاعات

جدول ۷: بعد مدیریتی

مؤلفه	شاخص
تداوم عملکرد	تاب‌آوری و پایداری شبکه
	ملاحظات پدافند غیرعامل
	تدوین و اجرای طرح تداوم مأموریت
	تدوین طرح و میزان آمادگی در جبران خرابی
قوانین/ مقررات	استانداردها و پروتکل (IPV٦،IPV٤)
	وجود نظام تنظیم مقررات
اقتصادی	منابع مالی
	اشتغال‌زا
ساختار و سازمان	رویکرد
	تخصص
	نگاشت نهادی و شفافیت در تقسیم وظایف
	نیروی انسانی
خدمات	میزان رضایتمندی
	تنوع خدمات
	رقابت‌پذیری
	تطبیق‌پذیری
	سهولت در دسترسی و اثربخشی اطلاع‌رسانی

سؤال فرعی دوم: ارتباط میان ابعاد، مؤلفه‌ها و شاخص‌های شبکه ملی اطلاعات جمهوری اسلامی ایران چگونه است؟ ارتباط میان ابعاد، مؤلفه‌ها و شاخص‌های شبکه ملی اطلاعات جمهوری اسلامی ایران در قالب سه بعد، نوزده مؤلفه و هفتادویک شاخص مطابق شکل ۳ ارائه می‌گردد.

پیشنهادات: این تحقیق بر موضوعات زیرساخت ارتباطی شبکه ملی اطلاعات تمرکز داشته و سایر جوانب شبکه ملی اطلاعات می‌تواند در تحقیقات دیگری مطرح گردد.

با توجه به وسیع بودن دامنه این تحقیق، پیشنهاد می‌گردد فرایند پیاده‌سازی الگوی تحقیق، به‌طور جداگانه ارائه گردد.

منابع:

- اسلامی، علیرضا، (۱۳۹۰)، ***نظریه امنیت امام خمینی (ره) با رویکرد امنیت ملی*** (پایان‌نامه دکتری)، دانشگاه عالی دفاع ملی.
- پورشیخی، محسن و اکبری ترکستانی، جواد، (۱۳۹٤)، ***ارائه ساختاری نوین برای مدیریت و کنترل بهتر درخواست‌ها در شبکه ملی اطلاعات بر پایه معماری SDN***کنفرانس بین‌المللی پژوهش‌های کاربردی در فناوری اطلاعات، کامپیوترو مخابرات.
- دانشگاه عالی دفاع ملی، (۱۳۹٦)، بازیابی از *http://www.sndu.ac.ir/content*
- رامک، مهراب و همکاران، (۱۳۹٤)، ***طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن***، تهران: دانشگاه عالی دفاع ملی.
- سازمان فناوری اطلاعات ایران، (۱۳۹٦)، ***نظام پایش شاخص‌های فناوری اطلاعات و ارتباطات کشور***.
- شهیر، احسان، (۱۳۹٦)، ***طراحی الگوی راهبردی بومی امنیت فضای مجازی کشور***، رساله دکتری دانشگاه عالی دفاع ملی.
- میررفیع، سیدعلی، (۱۳۹٤)، ***تدوین راهبردهای پدافند غیرعامل زیرساخت‌های ارتباطی شبکه ملی اطلاعات کشور در برابر تهدیدات سایبری***، رساله دکتری، دانشگاه عالی دفاع ملی.
- مرکز ملی فضای مجازی، (۱۳۹۲)، ***شبکه ملی اطلاعات***، بازیابی از:
http://majazi.ir/page/national-information-network
- نامداریان، لیلا، (۱۳۹۵)، ***ارائه الگویی برای تقویت اثرات اقتصادی شبکه ملی اطلاعات***، فصلنامه علمی پژوهشی پژوهشگاه علوم و فناوری ایران.
- هلیلی، خداداد، (۱۳۹٤)، ***نقش و جایگاه امنیت در شبکه ملی اطلاعات و ارائه راهبردهای مناسب آن***، رساله دکتری، دانشگاه عالی دفاع ملی.
- هلیلی، خداداد و همکاران، (۱۳۹۳)، ***نقش و جایگاه شبکه ملی اطلاعات در امنیت سامانه‌های c٤i***، هشتمین کنفرانس ملی فرماندهی و کنترل ایران.
- *Communications Commission Washington ،D.C. ۲۰۵۵٤.*
- *Cherdantseva, Hilton. (۲۰۱۳). A Reference Model of Information Assurance.*
- *Heather Savory (۲۰۱۵): The National Information Infrastructure (NII)Why, What and How.*
- *Internaational Telecommunication Union (۲۰۰۰). TMN management functions. ITU.*

- *Internaational Telecommunication Union: .(۲۰۱۲) ،Nicole FALESSI Global Cybersecurity Index ۲۰۱۵/۱٦ Reference Model*
- *National Cyber Security Strategies Practical Guide on Development and Execution*
- *Sputnik International, ۲۰۱٦, https://ir.sputniknews.com/russia/https://ir.sputniknews.com*
- *United State Department of Defence (۲۰۱۵): The DOD Cyber Strategy.*
- *UK National Cyber Security Strategy ۲۰۱٦-۲۰۲۱, (۲۰۱٦)*