فصلنامه علمی امنیت ملی
سال دهم، شماره سی‌وششم، تابستان ۱۳۹۹
مقاله سوم از صفحات ۱۱٤-۸۷

مقاله پژوهشی: نهادهای مؤثر کلان فرآیند رمزنگاری و امنیت اطلاعات در نظام دفاع سایبری جمهوری اسلامی ایران

محسن رمضان یارندی[۱]، رضا تقی‌پور[۲]

تاریخ دریافت: ۱۳۹۸/۰۹/۰۳ **تاریخ پذیرش: ۱۳۹۸/۱۰/۱۷**

چکیده

این مقاله بر اساس یافته‌های پژوهش گروهی انجام‌شده در دانشگاه عالی دفاع ملی با عنوان «طراحی دفاع سایبری کشور و تدوین راهبردهای آن» تدوین گردیده است. پژوهش گروهی مذکور، با به‌کارگیری روش خوشه‌بندی در تحلیل محتوا و تکنیک دلفی درصدد طراحی مدل دفاع سایبری برآمده است. برای این منظور، سه مفهوم بازدارندگی، پدافند (دفع) و برگشت‌پذیری به‌مثابه ابعاد اساسی دفاع سایبری مورد شناسایی قرار گرفتند.

مقاله حاضر ضمن مطالعه اسناد بالادستی کشور، به مطالعات تطبیقی هفت کشور پیشرو در امر دفاع سایبری پرداخته و جایگاه کلان فرآیند رمزنگاری و امنیت اطلاعات دیجیتال در دفاع سایبری و نهادهای اثرگذار در تحقق آن را شناسایی می‌نماید. از این جهت به آن کلان فرآیند می‌گوییم که شامل اجزاء بسیار و ارتباطات فراوان با سایر نهادها می‌باشد. همچنین با اخذ نظر خبرگان در خصوص روابط متقابل نهادها و فرآیندهای مختلف تأثیرگذار بر دفاع سایبری، نتایج را به روش معادلات ساختاری-تفسیری مورد تجزیه‌وتحلیل قرار داده و مدل مربوط را ترسیم می‌نماید. یافته‌های پژوهش نشان داد که کلان فرآیند رمزنگاری و امنیت از فعالیت مشترک با مشارکت ١٤ نهاد در شش سطح عملیاتی تحقق خواهد یافت و در این راستا، تدوین قوانین و مقررات سایبری در کلان فرآیند رمزنگاری و امنیت اطلاعات دیجیتال، از اهمیت بالایی برخوردار است.

کلیدواژه‌ها: کلان فرآیند رمزنگاری، امنیت اطلاعات، متولیان رمز، دفاع سایبری، مدل مفهومی

۱. دانشجوی مقطع دکترای رشته مدیریت راهبردی فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی (نویسنده مسئول) m. yarandi@sndu. ac. ir
۲. عضو هیئت‌علمی دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

مقدمه

بر اساس آمار تاکنون ۳۲ کشور در دنیا، ساختار دفاع سایبری خود را تشکیل داده‌اند و ۱٤۰ کشور در حال مطالعه روی توسعه دفاع ملی در کشور خود هستند (حسینی و ظریف‌منش، ۱۳۹۲: ٤۳). با توجه به شرایط نابسامان، فضای سایبر بین‌الملل، ج.ا.ا. نیازمند یک نظام مقابله‌ای هوشمند و برگرفته از ویژگی‌های خاص خود می‌باشد. طراحی هرگونه مدل عملیاتی برای تحقق دفاع سایبری متضمن داشتن الگوی مفهومی مناسب و همچنین تبیین چهارچوب‌های نظری آن می‌باشد. مشخص کردن نقش رمزنگاری در مدل دفاع سایبری ج.ا.ا.، با تبیین مبانی نظری و پارادایم‌های حاکم بر آن و همچنین بررسی و مطالعه تطبیقی الگوهای کشورهای پیشرو و بهینه‌سازی آن با تکیه بر مطالعات اسناد بالادستی کشور و همچنین قوانین و مقررات جاری کشور، امکان‌پذیر خواهد بود.

موضوع رمز به‌عنوان موضوعی مؤثر بر منافع و امنیت ملی هر کشوری است که با توجه به شرایط کشور عزیزمان ایران، تأثیرگذاری آن بیشتر نیز خواهد بود. رمزنگاری به‌عنوان قلب امنیت ارتباطات و اطلاعات سایبری می‌تواند نقش بسیار سازنده‌ای را در مواجهه با تهدیدات فضای سایبر داشته باشد. در سند چشم‌انداز جمهوری اسلامی ایران در افق ۱٤۰٤ هجری شمسی، بر امن بودن ایران اسلامی تأکید ویژه‌ای شده است (سند چشم‌انداز، ۱۳۸٤: ۱) و بر همین اساس نیز در اسناد بالادستی کشور، ارتقای امنیت فضای مجازی و برقراری امنیت در فضای تولید و تبادل اطلاعات کشور مورد تأکید قرار گرفته است.

همان‌طور که برای داده‌کاوی مثال جالبی گفته شده که مانند استخراج سوخت موشک از نفت خام (نظیر داده‌ها) است (Preneel, 2016: 3)، برای ارزش افزوده رمزنگاری در امنیت اطلاعات نیز باید گفت این مزیت را نمی‌توان از کشورهای دیگر خریداری یا وارد کرد و با توجه به اهداف جمهوری اسلامی ایران، حتماً نیاز به ایجاد سازوکاری مناسب برای پیشرفت فزاینده در این حوزه هستیم تا در افق ۱٤۰٤ ضمن رسیدن به جایگاه اول منطقه و پایداری در این رتبه، به الگوریتم‌ها و پروتکل‌های رمز بومی با امنیت بالا و قابل اثبات دست یابیم.

۱. بیان مسئله

فضای سایبر یا به عبارتی فضای مجازی امروزه ابعاد بسیار بزرگی ازجمله امنیت دارد. فضای مجازی که از فضای حقیقی گسترده‌تر شده است دارای ابعاد متنوعی است که بُعد امنیت این فضا برای حاکمان هر کشوری اهمیت فوق‌العاده‌ای دارد و باعث تغییر مؤلفه‌های امنیت ملی می‌شود.

طی سال‌های اخیر توجه نسبتاً خوبی به موضوعات امنیت ارتباطات و اطلاعات در کشورمان وجود داشته است. تدوین سند چشم‌انداز بیست‌ساله جمهوری اسلامی ایران، تصویب و ابلاغ سند افتا[1]، ابلاغ سیاست‌های کلان نظام در خصوص افتا، تدوین نقشه جامع علمی کشور، ابلاغ سیاست‌های کلی علم و فناوری (نظام آموزش عالی، تحقیقات و فناوری) و تشکیل شورای عالی فضای مجازی طی این سال‌ها، شروع مناسبی را برای رمزنگاری در کشور ایجاد کرده است. در نقشه جامع علمی کشور نیز رمزنگاری از اولویت‌های الف (بالاترین اولویت) در علوم پایه و علوم کاربردی بیان شده است (شورای عالی انقلاب فرهنگی، ۱۳۹۰: ۱۹).

به‌رغم اینکه در کشور ما ذینفعان زیادی در حوزه رمزنگاری وجود دارند، متأسفانه ارتباط نظام‌مندی با هم نداشته و سازوکار مناسبی برای استفاده و اطلاع از فعالیت‌های یکدیگر و نیز تحولات داخلی و بین‌المللی حوزه رمز ندارند و تاکنون زیست‌بوم رمزنگاری در کشور به‌صورت کامل شکل نگرفته و مسائل و چالش‌های بسیار زیادی برای به‌کارگیری رمز – به‌عنوان بخش مهمی از نظام دفاع سایبری– در ام‌القرای جهان اسلام وجود دارد. در صورت تکمیل و ارتقاء این زیست‌بوم، شاهد ارتقاء امنیت ملی در کشور و حتی جهان اسلام خواهیم بود تا فرآیندهای تولید، ارزیابی، پیاده‌سازی و به‌کارگیری محصولات و خدمات رمزنگاری به‌طور بهینه و مناسبی طی شوند.

مسئله اصلی که در این مقاله به آن پرداخته‌ایم، مشخص نبودن نقش‌ها و مسئولیت‌های نهادهای مؤثر در فرآیندهای رمزنگاری و امنیت اطلاعات است. همچنین نامعلوم بودن

---

۱. امنیت فضای تولید و تبادل اطلاعات

کلان فرآیند رمزنگاری (در تمام مراحل زیست‌بوم آن شامل تولید، انتقال، نگهداری، به‌کارگیری و امحاء اطلاعات مهم و دارای طبقه‌بندی) در مدل دفاع سایبری جمهوری اسلامی ایران واضح است.

عدم کارایی و اثربخشی اقدامات رمزنگاری در حوزه دفاع سایبری در ج.ا.ا. تأثیر حملات سایبری علیه کشور را به حداکثر رسانده و دشمن را متوجه نقاط ضعف اساسی این حوزه می‌نماید. در این مقاله به دنبال نشان دادن تأثیرات نهادهای مختلف در کلان فرآیند رمزنگاری هستیم تا بتوان در حوزه رمزنگاری اقدامات مؤثری را جهت مقابله با تهدیدات سایبری انجام داد. این امر سبب می‌شود دفاع در فضای سایبر روشمند و هدفمند شده و در برخورد با حملات سایبری علاوه بر کنترل تهدیدات، آسیب‌پذیری‌ها را به حداقل برسانیم.

۲. اهمیت و ضرورت

اهمیت این تحقیق بر اساس فواید انجام پژوهش را می‌توان موارد ذیل برشمرد:

- غنی‌سازی ادبیات بومی در حوزه رمز در سطح راهبردی به‌منظور حفاظت از امنیت داده‌های حساس جمهوری اسلامی ایران
- وابستگی بخشی از امنیت ملی کشور به حوزه رمز
- کمک به ارتقاء کشور به جایگاه اول منطقه در حوزه رمز در پایان سال سند چشم‌انداز بیست‌ساله جمهوری اسلامی ایران
- کمک به ارتقاء جایگاه جهانی کشور در حوزه رمز و تبدیل ایران به قطب علمی رمز جهان اسلام
- کمک به ایجاد نظام مقابله با تهدیدات سایبری
- درک بهتر از مسئله امنیت در حوزه‌ی رمزنگاری در کشور
- ایجاد نگاه دستگاهی در مقابل نگاه واکنشی

از سوی دیگر در ارتباط با ضرورت این تحقیق و مشکلات عدم انجام پژوهش می‌توان به موارد ذیل اشاره نمود:

- سهولت نفوذ دشمن در مراکز حساس و حیاتی
- افشای محرمانه‌ترین اطلاعات نظام در سازمان‌های حکومتی و نهادهای خصوصی
- لطمات جبران‌ناپذیر به زیرساخت‌های حیاتی کشور در حوزه رمزنگاری
- ناهماهنگی متولیان مقابله با تهدیدات سایبری در حوزه رمزنگاری

٤. اهداف تحقیق

هدف اصلی: تبیین جایگاه کلان فرآیند رمزنگاری و امنیت اطلاعات در الگوی دفاع سایبری ج.ا.ا.

هدف فرعی: شناخت نقش‌ها و مسئولیت‌های هر یک از نهادهای مؤثر بر کلان فرآیند رمزنگاری و امنیت اطلاعات در مدل الگوی دفاع سایبری ج.ا.ا.

٥. سؤالات تحقیق

سؤال اصلی: جایگاه کلان فرآیند رمزنگاری و امنیت اطلاعات در الگوی دفاع سایبری ج.ا.ا چیست؟

سؤال فرعی: نقش‌ها و مسئولیت‌های هر یک از نهادهای مؤثر در کلان فرآیند رمزنگاری و امنیت اطلاعات در مدل دفاع سایبری کدام است؟

٦. روش و نوع تحقیق

این پژوهش از نوع مطالعات بنیادین و توسعه‌ای – کاربردی بوده و به روش موردی – زمینه‌ای برای رسیدن به جایگاه رمزنگاری و امنیت اطلاعات در مدل الگوی دفاع سایبری انجام شده است. همچنین در این مقاله با بررسی وضع موجود، شناسایی فرآیندها و نهادهای مؤثر در دفاع سایبری کشور (با استفاده از مدل پایه زکمن) و نحوه

تعامل این نهادها در سطح داخلی و بین‌المللی انجام شده است. با مطالعه اسناد بالادستی کشور و قوانین و مقررات موجود و با بهره‌گیری از نظرات متخصصین، پژوهش‌گران، مدیران و متصدیان حوزه فضای سایبری، مدل مفهومی نهادهای تأثیرگذار در کلان فرآیند رمزنگاری در نظام دفاع سایبری در افق چشم‌انداز ۱۴۰۴ کشور تدوین گردیده است.

با توجه به محدوده و تعریف مسئله در این مقاله، می‌بایست سطح اول از چهارچوب معماری زکمن تکمیل گردد. در سطح یا سطر اول از نگاه اجرایی و نگاه کسب‌وکار و مالکان مفاهیم کسب‌وکار به موضوع پرداخته می‌شود.

در هر سطر می‌بایست به شش سؤال چه چیزی، چگونه، کجا، کی (چه کسی)، کی (چه وقت) و چرا پاسخ داده شود. در سطح اول اجزای نظام دفاع سایبری شناسایی می‌شود. به‌طور مثال چه چیزهایی باید در نظام دفاع سایبری از آن‌ها محافظت شود (که به آن‌ها دارایی‌ها یا سرمایه‌های سایبری گفته می‌شود). برای سؤال «چگونه»، باید شناسایی شود که چه فرآیندهایی برای محافظت از سرمایه‌ها وجود دارد و یا برای سؤال «کجا» باید شناسایی شود که چه مکان‌هایی برای محافظت و تأمین امنیت وجود دارد. به همین ترتیب برای دیگر پرسش‌ها باید شناسایی اجزاء معماری انجام شود. در سطر اول از چهارچوب معماری زکمن تنها به شناسایی محتوایی و تعریف محدوده خواهیم پرداخت. از آنجایی که بیشتر چهارچوب‌هایی که به‌صورت خاص‌منظوره تهیه شده‌اند پایه اصلی آن‌ها زکمن بوده است و می‌توان گفت چهارچوب زکمن در بین دیگر رقبایش جامعیت بیشتری دارد.

در این پژوهش، با توجه به ابعاد نظام دفاع سایبری و گستردگی حوزه‌های آن و نیز محدوده تعیین‌شده برای تحقیق، تنها به طراحی سطح اول از این چهارچوب خواهیم پرداخت و ضمن درج یافته‌های مطالعات تطبیقی، اسناد بالادستی، وضعیت موجود دفاع سایبری کشور در سلول‌های لایه اول یا راهبردی چهارچوب معماری زکمن، نتایج حاصل

را در دو محور اصلی نهاد (شامل ستون چه کسی[1] از چهارچوب زکمن) و فرآیند (شامل ستون‌های چگونه[2]، چرا[3]، کی[4]، کجا[5] و چه چیزی[6] از چهارچوب زکمن) دسته‌بندی می‌نماییم تا خروجی‌های نهایی تحقیق احصاء گردد.

ماهیت کلان‌نگرانه و اهمیت ویژه محتوای اسناد بالادستی و بین‌المللی مورد استفاده در پژوهش از یک‌سو و لزوم خبرگی متناسب با موضوع این اسناد از سوی دیگر، باعث می‌شود که در انتخاب روش تحلیل و استخراج اطلاعات از اسناد بالادستی، حداکثر دقت و ظرافت در نظر گرفته شود و از روش‌های کیفی و تمام‌شمار مبتنی بر خبرگی استفاده گردد، لذا به‌منظور تحلیل یافته‌های پژوهش از روش مدل‌سازی ساختاری تفسیری[7] بهره‌گیری روش مدل‌سازی ساختاری تفسیری، یک فرآیند یادگیری تعاملی است که در آن مجموعه‌هایی از عناصر مختلف و به هم مرتبط در یک مدل نظام‌مند جامع ساختاردهی می شوند. مدلی که با استفاده از این روش به دست می‌آید، ساختاری از یک مسئله یا موضوع پیچیده، یک سیستم یا حوزه مطالعاتی را نشان می‌دهد لذا به‌طورکلی می‌توان گفت که ایده اصلی مدل‌سازی ساختاری تفسیری، تجزیه یک سیستم پیچیده به چند زیرسیستم از عناصر، با استفاده از تجربه عملی و دانش خبرگان به‌منظور ساخت یک مدل ساختاری چندسطحی است. به‌منظور اعتبارسنجی یافته‌ها، پرسشنامه‌ای بر مبنای این روش تنظیم و نظر تخصصی ۱۰ نفر از خبرگان اخذ و مورد تجزیه‌وتحلیل قرار گرفت. در نمونه ۱۰ تایی به‌دست‌آمده از خبرگان، بیشتر افراد در گروه سنی ۴۵-۴۰ سال (۲۰ درصد) و ۵۰- ۴۵ سال (۳۰ درصد) قرار دارند، پس از این گروه سنی، بیشترین افراد متعلق به گروه‌های سنی ۴۰-۳۵ سال (۲۰ درصد) می‌باشند و کمترین تعداد از پاسخگویان به گروه سنی ۵۵-۵۰ سال (۱۰ درصد) تعلق دارند. سطح تحصیلات خبرگان این حوزه در نمونه انتخاب‌شده ۹۰

1. Who
2. How
3. WHY
4. WHEN
5. WHERE
6. WHAT
7. Interpretive Structural Modelling

درصد فوق‌لیسانس و ۱۰ درصد دکتری است. کلیه پاسخ‌دهندگان از متخصصین و خبرگان این حوزه محسوب می‌شده و جنسیت آنان مرد است.

۷. مبانی نظری

۷-۱. پیشینه پژوهش

در بررسی سوابق موجود در سازمان‌ها و مراجع علمی و پژوهشی که احتمال انجام تحقیق در این زمینه در آن‌ها وجود داشت مشخص گردید که به‌طور مستقیم پیرامون موضوع این رساله، تحقیقی صورت نگرفته است. البته سوابق پژوهش‌های زیر در دانشگاه‌های داخل و همایش‌های بین‌المللی شناسایی گردید که می‌توان از آن‌ها به‌عنوان پژوهش‌های مرتبط یاد نمود و این نکته قابل توجه است که بسیاری از مستندات راهبردی در این حوزه دارای طبقه‌بندی است و کشورهای مختلف با در نظر گرفتن مصالح امنیت ملی خود فقط بخشی از اسناد خود را در این زمینه منتشر می‌کنند. هفت سند، مقاله و طرح پژوهشی در این مقاله استفاده شده است.

۷-۱-۱. سند راهبرد ده‌ساله توسعه فناوری نانو در جمهوری اسلامی ایران

در این سند چشم‌انداز توسعه فناوری نانو بیان شده و در سال ۱۳۹٤، رتبه کشور در جایگاه مناسب در بین ۱۵ کشور برتر فناوری نانو، تعریف شده است. سه هدف کلان در سند مذکور عبارت‌اند از: دستیابی به سهم مناسبی از تجارت جهانی نانو، بهره‌مندی از مزایای فناوری نانو برای ارتقاء کیفیت زندگی مردم، نهادینه شدن توسعه پایدار و پویای علوم، فناوری و صنعت نانو.۱۲ راهبرد، ۵۳ برنامه اجرایی و هشت شاخص ارزیابی کلان در این سند ذکر شده است. بر اساس سه معیار کلی، پنج حوزه کاربردی به‌عنوان موضوعات کلان اولویت‌دار فناوری نانو تعیین شدند که عبارت‌اند از: انرژی، سلامت، محیط زیست و آب، مواد، عمران و سازه‌ها. در ادامه هشت برنامه کلان و اهداف و شاخص‌های هرکدام آمده است. این هشت برنامه به ۲۸ فعالیت تقسیم شده است. به‌طور نمونه برنامه هشتم عبارت است از: سیاست‌گذاری و ارزیابی اهداف،

راهبردها، سیاست‌ها، برنامه‌ها و نهادهای نانو. این برنامه به پنج فعالیت تقسیم شده و هر فعالیت با اهداف عملیاتی، شاخص‌ها و طرح‌های مربوطه بیان می‌شود. الگوی برنامه‌ریزی راهبردی این سند تلفیقی از الگوی برایسون، هکس[1] و دیوید است. روش تلفیق برنامه‌ریزی راهبردی[2] و نظام ملی نوآوری[3] برای تدوین برنامه توسعه اتخاذ شده است (ستاد ویژه توسعه نانو، ۱۳۸٤: ۳۳).

۷-۱-۲. سند چهارچوب بهبود زیرساخت‌های حیاتی افتا از مؤسسه ملی استاندارد و فناوری آمریکا

در فوریه ۲۰۱٤ میلادی مؤسسه ملی استاندارد و فناوری آمریکا سندی را با عنوان چهارچوب بهبود زیرساخت‌های حیاتی افتا منتشر کرد. این سند در ۱٦ آوریل ۲۰۱۸ به‌روزرسانی شد. نسخه اول این چهارچوب شامل مجموعه‌ای از تجربیات برتر[4] و استانداردهای صنعت است تا سازمان‌ها بتوانند به مدیریت مخاطرات افتا بپردازند. این چهارچوب دارای ۹۸ زیرمقوله است که در ۲۲ مقوله و پنج حوزه عملکردی قرار گرفته‌اند. چهارچوب فوق از طریق همکاری دولت و بخش خصوصی ایجاد شده است (NIST, 2018: 3). این چهارچوب به کمک زبانی مشترک میان دولت و بخش خصوصی به‌گونه‌ای به مدیریت مخاطرات افتا می‌پردازد که از نظر اقتصادی کارا بوده و بر پایه الزامات کسب‌وکار و بدون نیاز به مقررات[5] اضافی در کسب‌وکارها بنا شده باشد.

این چهارچوب از سه بخش تشکیل شده است: هسته[6] چهارچوب، نماد[7] چهارچوب و سطوح[8] پیاده‌سازی چهارچوب(NIST, 2014: 5) .

1. Arnold C. Hax
2. Strategic Planning
3. National Innovation System
4. Best Practices
5. Regultory
6. Core
7. Profile
8. Tiers

۷-۱-۳. سند طراحی نظام محرمانگی، امضای دیجیتال (محاد) و طرح حمایت از رمز ملی

طرح مذکور با توجه به سطوح معماری FEAF[1] و مؤلفه‌های آن در جهت تدوین نظام محرمانگی و امضای دیجیتال، تدوین شده است، در این راستا نیازهای مربوط به هشت مؤلفه چهارچوب معماری FEAF ارائه شده است که عبارت‌اند از (پژوهشگاه ارتباطات و فناوری اطلاعات، ۱۳۹۰: ٥٤):

- پیشران‌های معماری در تدوین نظام محرمانگی و امضای دیجیتال
- جهت‌گیری راهبردی
- معماری وضع موجود در تدوین نظام محرمانگی و امضای دیجیتال
- معماری وضع مطلوب در تدوین نظام محرمانگی و امضای دیجیتال
- استانداردهای مورد نیاز تحقق وضع مطلوب
- اجزای معماری
- مدل‌های معماری
- فرایند گذار در تدوین نظام محرمانگی و امضای دیجیتال

با توجه به نظر ذینفعان، خبرگان و با توجه به مطالعات و بررسی‌های انجام‌شده، متأسفانه فعالیت‌های انجام‌شده در حوزه رمز در کشور ضعیف بوده و دلیل اصلی آن عدم توجه کافی و حمایت دولت از فعالین حوزه رمز بوده است، تنها چند شرکت که اغلب وابسته به مراکز نظامی هستند، در حوزه رمز فعالیت نسبتاً مناسبی دارند و با این وجود اکثر فعالیت‌هایی که در این شرکت‌ها انجام می‌شود، فقط جنبه تحقیقاتی داشته و به مرحله عملیاتی شدن نمی‌رسد که دلیل اصلی آن عدم وجود بازار مناسب و حمایت دولت در این زمینه می‌باشد. البته فعالیت‌هایی نیز در چندین شرکت خصوصی انجام شده است که بهینه سازی و توسعه فعالیت‌های آن‌ها نیازمند حمایت دولت می‌باشد (همان، ١٥٤).

در مجموع کارهای خوبی در این طرح انجام شده ولی با توجه به کمبود منابع در دسترس مجری طرح، این پروژه به‌طور کامل به احصاء وضعیت موجود کشور نپرداخته

1. Federal Enterprise Architecture Framework

است و اجازه دسترسی به بسیاری از منابع را نداشته‌اند. لذا در بخش‌های مختلفی که به نهادهای دولتی و حاکمیتی مربوط است نقصان زیادی دارد.

۷-۱-٤. سند فرآیند توسعه رویه‌ها و استانداردهای رمزنگاری از مؤسسه ملی استاندارد و فناوری آمریکا

این سند اصول، فرایندها و رویه‌هایی که منجر به رعایت استانداردهای رمزنگاری و اقدامات توسعه در مؤسسه ملی استاندارد و فناوری آمریکا می‌شوند را توصیف می‌کند. این سند منعکس‌کننده نظرات عمومی است که در دو نسخه قبلی دریافت شده است و به‌عنوان مبنایی برای استانداردهای رمزنگاری آینده می‌باشد و نیز راهنمای خوبی برای توسعه این استانداردها خواهد بود. این سند در صورت لزوم هر پنج سال یک‌بار مورد بازبینی قرار می‌گیرد تا در صورت نیاز، اطمینان حاصل شود که مؤسسه ملی استاندارد و فناوری آمریکا نقش و مسئولیت‌های خود را برای تولید استانداردها و دستورالعمل‌های رمزنگاری قوی، به‌طور مؤثر انجام می‌دهد (NIST, 2016: 2).

در این سند آمده که استانداردهای رمزنگاری مانند FIPS[1] مبتنی بر قوانین بوده و الگوریتم‌هایی که به‌طور مشخص در قلب بسیاری از فناوری‌های مهم امنیتی قرار دارند، به رسمی‌ترین فرآیند توسعه نیاز دارند (Ibid, 5).

۷-۱-۵. سند شاخص‌های جهانی امنیت سایبر[2] اتحادیه جهانی مخابرات یا آی تی یو

هرساله اتحادیه جهانی مخابرات[3] که زیر نظر سازمان ملل[4] فعالیت دارد بر اساس پرسشنامه‌هایی وضعیت کشورهای عضو در حوزه‌ی امنیت سایبر را مشخص می‌کند. این پرسشنامه‌ها شامل سؤالاتی در پنج گروه و ۲۵ شاخص می‌باشد. در سال ۲۰۱۷ تعداد این سؤالات ۱۵۷ سؤال بود که در سال ۲۰۱۸ به ۵۰ سؤال کاهش یافت (ITU, 2018: 8). پنج گروه شاخص‌های جهانی امنیت سایبر در مستندات چند سال اخیر عبارت‌اند از قوانین[5]،

1. Federal Information Processing Standards
2. Global Cybersecurity Index (GCI)
3. International Telecommunication Union (ITU)
4. National Union
5. Legal

امور فنی[1]، ساختار[2]، ظرفیت‌سازی[3] و همکاری[4] که در مجموع دارای ۲۵ شاخص در سال ۲۰۱۸ می‌باشند.

کشور ایران در سال ۲۰۱۷ رتبه ٦۰ در میان ۱۹۳ کشور عضو این سازمان را داشت(ITU, 2017: 55). در سال ۲۰۱۸ این رتبه برای کشورمان حفظ شد (ITU, 2018: 58). از این گروه‌بندی و شاخص‌های بیست و پنج‌گانه می‌توان به سطوح بالاتر که همان الگوی کلان ارزیابی کشورهای جهان از لحاظ سطح امنیت سایبری است، پی برد. علاوه بر شاخص‌های جهانی امنیت سایبر، شاخص‌های توسعه فناوری اطلاعات و ارتباطات[5] یا IDI از سال ۲۰۰۹ توسط آی تی یو منتشر می‌شود و دارای ١٤ شاخص است.

۷-۱-٦. مقاله روش‌های رمزنگاری شناختی برای مدیریت اطلاعات هوشمند

این مقاله توسط اوجیلا[6] و همکارانش در شماره ٤۰ مجله بین‌المللی مدیریت اطلاعات[7] و در سال ۲۰۱۸ منتشر شده است. در بخشی از چکیده این مقاله آمده است (Ogiela et all, 2018: 21):

در این مقاله مبانی رمزنگاری شناختی مورد استفاده برای تأمین امنیت اطلاعات با تقسیم آن اطلاعات و توزیع قسمت‌های تقسیم‌شده بین گروه‌های منتخبِ مخفی و مورد اعتماد، معرفی شده است. روند پنهان کردن داده‌ها با تقسیم و توزیع قطعات مخفی (سایه‌های) آن‌ها با استفاده از روش‌های شناختی مورد بحث قرار گرفت. رمزنگاری شناختی امکان استفاده از اطلاعات شخصی موجود در صفات بیومتریک فردی را توصیف می‌کند. هم‌زمان، آن را به‌عنوان یک راه‌حل ابتکاری به صاحب قطعه مخفی، بر اساس مشخصه بیومتریک و ویژگی‌های معنایی شناسایی‌شده، ارائه می‌دهد. رمزنگاری شناختی برای مدیریت اطلاعات راهبردی استفاده می‌شود.

1. Technical
2. Organizational
3. Capacity building
4. Cooperation
5. ICT Development Index = IDI
6. Marek R. Ogiela
7. International Journal of Information Management

۷-۱-۷. مقاله سیاست رمزنگاری و تأثیرات بین‌المللی آن: چهارچوبی برای درک آثار برجسته برون‌مرزی

این مقاله توسط بادیش[1] و همکارانش در مجله امنیت ملی، فناوری و قانون[2] متعلق به مؤسسه هوور[3] در مجموعه مقالات مورد حمایت دانشگاه اِستنفورد و در سال ۲۰۱۸ منتشر شده است. در بخشی از نتیجه‌گیری این مقاله آمده است (Budish et al, 2018: 18):

این مقاله یک چهارچوب مفهومی را ارائه می‌دهد که می‌تواند به سیاست‌گذاران کمک کند تا اثرات بین‌المللی برجسته و بالقوه سیاست‌های رمزنگاری داخلی را بهتر درک و پیش‌بینی کنند. با استفاده از عوامل مشخص‌شده در این مقاله، سیاست‌گذاران می‌توانند با تصمیم‌گیری آگاهانه‌تر و با تفکر دقیق و منظم از طریق ابزارهای مختلف مشارکت کنند. این مشارکت می‌تواند از طریق سیاست‌گذاری رمزنگاری، روابط و مسیرهایی که این ابزارها می‌توانند فعال کنند و دامنه تأثیراتی که ممکن است ظهور پیدا کند، صورت پذیرد. این مقاله می‌تواند یک نقطه شروع مناسب باشد. اغلب، سیاست‌های رمزنگاری به‌صورت موازی با یکدیگر و با تغییر رویدادهای جهانی در نظر گرفته می‌شوند و منجر به طیف وسیعی از الگوهای تداخل و حلقه‌های بازخورد می‌شوند. این مقاله فقط به تأثیرات بین‌المللی ناشی از سیاست‌های رمزگذاری مربوط می‌شود، نه شایستگی‌های خود این سیاست‌ها.

۷-۲. مفهوم‌شناسی متغیرها

ـ **راهبرد:** راهبرد راهی برای رسیدن به آینده مطلوب است، یا به مجموعه‌ای از انتخاب‌های بنیادی و یا حیاتی درباره نتایج یک فعالیت و ابزار انجام آن فعالیت را راهبرد گویند (حسن‌بیگی، ۱۳۹۰: ٤٣).

ـ **فضای سایبر جمهوری اسلامی ایران:** فضای سایبر نظام جمهوری اسلامی ایران شامل مجموعه‌ای از ارزش‌ها، منافع و دارایی‌های ملی در فضای سایبر بوده و جهت ارائه

1. Ryan Budish
2. National Security, Technology, and Law
3. Hoover Institution

خدمات در راستای اهداف نظام ج.ا.ا هست. این فضا محدود به مرزهای جغرافیایی نیست(رامک و دیگران، ۱۳۹۵: ۳۳).

ـ نظام دفاع سایبری: زیرمجموعه‌ای از نظام دفاعی کشور شامل نهادهای دولتی همچنین سازمان مردم‌نهاد و زیرنظام‌های دیگر در سطح ملی به همراه روابط میان آن‌ها و فرایندهای مرتبط به‌منظور پیشگیری، حفظ دارایی‌های زیرساختی، حمایت از ارزش‌ها، منافع و دارایی‌های ملی در مقابل تهدیدات و حملات سایبری (همان، ۳٤).

ـ ابعاد دفاع سایبری: بازدارندگی، پدافند و برگشت‌پذیری به‌عنوان ابعاد دفاع سایبری می‌باشند. این تعریف از دفاع سایبری پس از تأیید خبرگان دارای جامعیت و مانعیت می‌باشد (اسماعیلی و تقی‌پور، ۱۳۹۷: ۱۸۸).

ـ رمزنگاری: رمزنگاری علم و هنر سرّی کردن داده‌ها است که در موارد سه‌گانه احراز اصالت[1]، انکارناپذیری[2] و حفظ یکپارچگی[3] پیام نیز کاربرد دارد. مطابق فرضیه کرشهوف[4] در الگوریتم‌های رمزنگاری فرض بر این است که تمام الگوریتم‌ها آشکار و همگانی‌اند و فقط کلیدهای رمزنگاری مخفی و محرمانه هستند (گروه واژه‌گزینی انجمن رمز ایران، ۱۳۹٤: ۱٦۰).

۸. تجزیه‌وتحلیل یافته‌های تحقیق

به‌منظور احصاء جایگاه دانش و فناوری‌های رمز در دفاع سایبری کشورها، لازم است که یافته‌های تحقیق (مبانی نظری) را به شکلی دسته‌بندی نماییم تا فرآیندهای مهم و متولیان اجرای فرآیندها را احصاء نماییم. با توجه به ابعاد دفاع سایبری و گستردگی حوزه‌های آن، سلول‌های سطح یا سطر اول که با نگاه راهبردی، چهارچوب معماری زکمن (دید برنامه‌ریز) را مورد استفاده قرار داده و یافته‌های مطالعات تطبیقی، اسناد بالادستی و وضعیت موجود دفاع سایبری کشور را در آن درج می‌نماییم. همان‌طور که از (جدول ۱) مشخص است، شش

1. Authentication
2. Non repudiation
3. Integrity
4. Kirchhoffs assumption

ردیف یا سطر داریم که در هر ردیف یا سطر به‌صورت کلی به سؤالات شش‌گانه پاسخ داده شده است. متولیان سطر اول از (جدول ۱) در نهایت با هم ادغام شده و مطابق (جدول ۳) به ۱٤ نهاد یا متولی خلاصه شده‌اند. با جمع‌بندی ردیف‌های چگونه؟ چرا؟ کی؟ کجا؟ و چه چیزی؟ از (جدول ۱)، می‌توان فرآیندهای مطرح در دفاع سایبری کشورها را احصاء نمود که به‌عنوان فرآیندهای دوازده‌گانه در (جدول ۲) خلاصه شده‌اند. همان‌طور که در (جدول ۲) مشاهده می‌گردد، رمزنگاری و امنیت اطلاعات متمرکز به‌عنوان فرآیند ششم دفاع سایبری، مورد توجه قرار گرفته است و به‌منظور اجرای فرآیند فوق نیز لازم است نهادهای مؤثر را احصاء نماییم که این مهم با جمع‌بندی ستون چه کسی؟ از (جدول ۱) محقق می‌گردد. در (جدول ۳) نیز مشخص است متولی سیزدهم، متولی رمز ملی و تصدیق هویت مجازی در میان ۱٤ متولی موجود تأثیرگذار می‌باشد. با شناسایی و تبیین روابط بین نهادهای چهارده‌گانه در تحقق فرآیند رمزنگاری و امنیت اطلاعات متمرکز از فرآیندهای دوازده‌گانه احصاءشده برای دفاع سایبری کشور، جایگاه کلان فرآیند رمزنگاری و امنیت اطلاعات متمرکز در دفاع سایبری استخراج شد.

گام بعدی در معماری نظام دفاع سایبری، دستیابی به ارتباطات مابین نهادهای متولی جهت تحقق و اجرای فرآیندها است که با استفاده از روش مدل‌سازی ساختاری- تفسیری و بهره‌گیری از نظر خبرگان در قالب تهیه پرسشنامه، نهایی گردید. در خصوص فرآیند بهره‌برداری از نظر خبرگان در قالب تهیه پرسشنامه که یکی از روش‌های علمی تجزیه‌وتحلیل یافته‌ها جهت آزمون فرضیه‌ها و رد یا تأیید آن‌ها است، پاسخ‌های به‌دست‌آمده از پرسشنامه‌های تنظیم‌شده مورد تجزیه‌وتحلیل قرار گرفته و ارتباطات فرآیندها و نهادهای نظام دفاع سایبری به دست آمد.

۸-۱. جایگاه کلان فرآیند رمزنگاری و امنیت اطلاعات متمرکز در دفاع سایبری

همان‌طور که در روش‌شناسی تحقیق گفته شد، پرسشنامه‌ای بر اساس مقایسه زوجی تأثیر نهادها بر یکدیگر تنظیم و در اختیار خبرگان قرار گرفت (از خبرگان درخواست شد

که اگر از نظر آن‌ها، سطر روی ستون تـأثیر دارد، V و اگـر سـتون روی سـطر تـأثیر داشـته باشد، A و اثر متقابل، X و بی‌اثر، O را علامت‌گذاری نمایند). حاصل جمع نظرات خبرگـان در رابطه با کلان فرآیند رمزنگاری و امنیت اطلاعات متمرکـز نشـان مـی‌دهـد کـه از روی پرسشنامه‌های گردآوری‌شده استخراج گردیده است (جدول ٤).

جدول ۱: نتایج چهارچوب زکمن و دسته‌بندی ستون‌ها به نهاد و فرآیند در سطح راهبردی (دید برنامه‌ریز)

چه کسی؟ (**Who**) ساختار و نقش	متولی مرکز اشتراک‌گذاری و تحلیل اطلاعات * متولیان مراکز پاسخگویی به حـوادث سـایبری گوهرهای سازمانی * متولیان مراکز پاسخگویی به حوادث سایبری ملی ماهر * متولیـان مراکـز عملیات امنیت شبکه **SOC** سازمانی * متولی فرماندهی دفاع سـایبری در وضـعیت عـادی * متولی فرماندهی دفاع سایبری در وضعیت تهدید * متولی فرمانـدهی دفـاع سـایبری وضـعیت بحـران * متـولی فرمانـدهی دفـاع سـایبری وضـعیت بحـران * متـولی تحقیقـات و توسـعه استانداردهای امنیت سایبر (آزمایشگاه) * متولی رمز ملی * متولی بومی‌سازی و هماهنگ‌کننده حاکمیت، صنعت و دانشگاه در حوزه ابزارهای تدافع سایبری * متولی سیاست‌هـای راهبـردی امنیـت سـایبر * متـولی تـدوین قـوانین و مقـررات * پلـیس متـولی رسـیدگی بـه تهدیـدات سازمان‌یافته سایبری * قرارگاه سایبری * متولی امنیت سایبر دولت * متولی امور بین‌الملـل در حوزه دفاع سایبر * متولی امنیت سایبر قوه قضاییه * متولی امنیت سایبر قوه مقننه
چه چیز؟ (**What**) موجودیت‌ها (هویت و اطلاعات)	امنیت ملی و عوامل ایجاد و بقاء آن * ارزش‌های ج.ا.ا. منبعث از اسلام شیعی و هویت ایرانـی * زیرساخت‌های حیاتی، مهم و حساس * دارایی‌هـای سـایبری * آزادی‌هـای مـدنی، حـریم خصوصی و عدالت اجتماعی
چطور؟ (**How**) فرآیندها در لایه راهبرد	برنامه‌ریزی، هماهنگی، یکپارچه‌سازی، هم‌زمان‌سازی و هـدایت فعالیـت‌هـا * آمـوزش، آگاه‌سازی و اطلاع‌رسانی * فرهنگ‌سازی امنیت سایبری * همکاری و تعاملات داخلی و بین‌المللی * مشارکت بخش‌های دولتی و خصوصی * بومی‌سازی در حوزه امنیت سایبر * رمزنگاری و امنیت اطلاعات متمرکز * ارتقاء خلاقیـت، نـوآوری، شـکوفایی و ایجـاد خودکفایی در حوزه امنیت سایبر * استانداردسازی در حوزه امنیـت سـایبر * نظـارت و ارزیابی مستمر، حفظ و ارتقاء آمادگی بخش‌های مختلف دفاع سـایبری * ایجـاد قـدرت بازدارندگی و پیشگیری از حملات و تهدیدات * ارزیابی مخاطرات و تهدیدات سایبری و به‌روزرسانی آن‌ها * پیگیری مؤثر قانونی و حقوقی جرائم و حملات سایبری * پایش، رصد مستمر تهدیدات و تشخیص حملات * پاسخ، مقابله سریع و مـؤثر بـا تهدیـدات و حملات سایبری * مدیریت مخاطرات و حوادث * تقویت پایداری در مقابل حملات * بازیابی و مدیریت بحران

کجا؟ (**Where**) قلمرو	درون مرزهای سایبر ج.ا.ا * نشست‌های انتقال اطلاعات در زمان انتقال اطلاعات خودی * نقاط اتصال هر نوع مراکز داده به شبکه * دروازه‌های شبکه‌های ملی، سازمان و محلی و انفرادی
چه وقت؟ (**When**) محرک‌ها	در زمان عملیات تروریستی سایبری * مدیریت بحران سایبری کشور از آغاز تا بازیابی شرایط عادی * ارتقاء و دائمی کردن ظرفیت‌های انسانی، صنعتی، فنی و علمی کشور * ارزیابی مداوم تهدیدات و آسیب‌پذیری‌ها * نقض ارزش‌های دینی * برنامه مداوم جهت هشدار و اطلاع‌رسانی به ذی‌نفعان * نقض ارزش‌های ملی * نقض امنیت ملی * پیش‌دستی در شناخت تهدیدات * تطابق دفاع سایبری به‌صورت دائم و پویا با فناوری‌ها و تهدیدات سایبری روزآمد * دفاع، همه‌جا و همه‌وقت
چرا؟ (**WHY**) اهداف و راهبردها	تقویت امنیت ملی با اشرافیت کامل بر فضای سایبر در سطح داخلی و بین‌المللی * محافظت از زیرساخت‌های حیاتی و حساس و سرمایه‌های سایبری * حفاظت از حریم خصوصی و آزادی‌های مشروع * صیانت از هویت دینی ملی و ارزش‌های انسانی جامعه * دفاع همه‌جانبه و فعال برای حفظ جامعیت و محرمانگی * افزایش استحکام و پایداری برای کاهش خسارت و حداقل نمودن خرابی و زمان بازیابی

در (جدول ۵) حاصل جمع نظرات خبرگان تحلیل گردیده است یعنی اگر بیش از ۵۰ درصد خبرگان نظر مثبت درباره ارتباط بین دو نهاد در کلان فرآیند رمزنگاری و امنیت اطلاعات داشته باشند، بنابراین ارتباط بین آن‌ها برقرار و ارزش یک به آن نسبت داده می‌شود و در غیر این صورت صفر خواهد بود.

مدل نهایی دفاع سایبری ج.ا.ا. از ترکیب دوازده کلان فرآیند تشکیل گردیده است. هریک از فرآیندها با توجه به سطحی که در آن قرار گرفته‌اند از طریق نهادهای مشارکت‌کننده در فرآیند، هدف مشخصی را دنبال می‌نمایند. همان‌طوری که در مدل نهایی پژوهش ملاحظه می‌شود برای شکل‌گیری دفاع سایبری منسجم و یکپارچه در کشور ضرورت دارد دستگاه‌ها و سازمان‌های مختلفی در سطح کشور با مدیریت واحد تعامل و همکاری نزدیک داشته باشند. مدل مفهومی دفاع سایبری ج.ا.ا. مطابق (شکل ۱) است.

جدول ۲: فرآیندهای دفاع سایبری

فرآیند	توصیف فرآیند	فرآیند	توصیف فرآیند
F1	برنامه‌ریزی، هماهنگی، یکپارچه‌سازی، هم‌زمان‌سازی و هدایت فعالیت‌ها	F7	نظارت و ارزیابی
F2	فرهنگ‌سازی، آموزش، آگاه‌سازی و اطلاع‌رسانی	F8	ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری
F3	همکاری و تعاملات بین‌المللی	F9	پیگیری مؤثر قانونی و حقوقی جرائم و حملات سایبری
F4	مشارکت بخش‌های دولتی و خصوصی	F10	پایش، رصد، تشخیص، پاسخ، مقابله با تهدیدات و حملات سایبری
F5	بومی‌سازی، استانداردسازی، نوآوری و ایجاد خودکفایی	F11	حفظ و ارتقاء آمادگی و تقویت پایداری در مقابل حملات سایبری
F6	رمزنگاری و امنیت اطلاعات متمرکز	F12	بازیابی و مدیریت بحران

جدول ۳: نهادهای مؤثر در اجرای فرآیندهای دفاع سایبری

نهاد	توصیف نهاد	نهاد	توصیف نهاد
N1	متولی سیاست‌گذاری حوزه امنیت سایبر	N8	متولی هماهنگی امنیت سایبری قوای سه‌گانه
N2	متولی فرماندهی سایبری و تعیین وضعیت	N9	متولی حفاظت از زیرساخت‌های ملی
N3	متولی تدوین قوانین و مقررات سایبری	N10	متولی نظارت و ارزیابی
N4	متولی امنیت فضای سایبر در صنعت کشور و بیمه سایبر	N11	متولی رصد، پایش تهدیدات و اشتراک‌گذاری
N5	متولی امور بین‌الملل دفاع سایبری کشورهای اسلامی	N12	متولی تحقیقات، آموزش، استانداردسازی و بومی‌سازی تجهیزات سایبری
N6	متولی مراکز عملیات امنیت شبکه و پاسخگویی	N13	متولی رمز ملی و تصدیق هویت مجازی
N7	متولی مقابله با جرائم سازمان‌یافته و تروریسم سایبری	N14	نهاد مدیریت محتوای سایبری و رسانه‌ها

جدول ٤: ماتریس حاصل جمع کلان فرآیند رمزنگاری و امنیت اطلاعات

فرآیند ۶ ایجاد رمزنگاری و امنیت اطلاعات متمرکز اگر سطر روی ستون تاثیر داشته باشد = V اگر ستون روی سطر تاثیر داشته باشد = A اثر متقابل = X بی اثر = O	نهاد	متولی سیاست گذاری حوزه امنیت سایبر	متولی فرماندهی سایبری و تعیین وضعیت	متولی تدوین قوانین و مقررات سایبری	متولی امنیت فضای سایبر در صنعت کشور و بیمه سایبر	متولی امور بین الملل ودفاع سایبری کشورهای اسلامی	متولی مراکز عملیات امنیت شبکه و پاسخگویی	متولی مقابله با جرائم سازمان یافته و تروریسم سایبری	متولی هماهنگی امنیت سایبری قوای سه گانه	متولی حفاظت از زیرساخت های ملی	متولی نظارت و ارزیابی	متولی رصد، پایش تهدیدات و اشتراک گذاری	متولی تحقیقات، آموزش، استاندارد سازی و بومی سازی تجهیزات سایبری	متولی رمز ملی و تصدیق هویت مجازی	نهاد مدیریت محتوای سایبری و رسانه ها
		N۱	N۲	N۳	N۴	N۵	N۶	N۷	N۸	N۹	N۱۰	N۱۱	N۱۲	N۱۳	N۱۴
نهاد															
متولی سیاست گذاری حوزه امنیت سایبر	N۱	۱۰	۸	۹	۹	۸	۶	۸	۸	۹	۷	۶	۸	۶	۵
متولی فرماندهی سایبری و تعیین وضعیت	N۲	۳	۱۰	۵	۹	۸	۸	۸	۸	۹	۷	۷	۸	۸	۹
متولی تدوین قوانین و مقررات سایبری	N۳	۶	۶	۱۰	۸	۸	۸	۷	۷	۸	۵	۷	۶	۷	۸
متولی امنیت فضای سایبر در صنعت کشور و بیمه سایبر	N۴	۲	۲	۱	۱۰	۷	۷	۷	۵	۶	۳	۶	۶	۵	۴
متولی امور بین الملل ودفاع سایبری کشورهای اسلامی	N۵	۲	۳	۳	۶	۱۰	۵	۷	۴	۵	۳	۷	۶	۴	۶
متولی مراکز عملیات امنیت شبکه و پاسخگویی	N۶	۲	۲	۲	۷	۴	۱۰	۵	۴	۳	۲	۵	۶	۴	۵
متولی مقابله با جرائم سازمان یافته و تروریسم سایبری	N۷	۳	۲	۲	۶	۶	۶	۱۰	۵	۶	۳	۷	۶	۵	۶
متولی هماهنگی امنیت سایبری قوای سه گانه	N۸	۳	۴	۳	۵	۴	۶	۶	۱۰	۶	۵	۶	۷	۸	۷
متولی حفاظت از زیرساخت های ملی	N۹	۲	۲	۱	۸	۶	۷	۷	۳	۱۰	۴	۷	۶	۵	۶
متولی نظارت و ارزیابی	N۱۰	۵	۶	۵	۷	۶	۸	۸	۵	۸	۱۰	۸	۸	۸	۹
متولی رصد، پایش تهدیدات و اشتراک گذاری	N۱۱	۲	۲	۲	۷	۷	۸	۸	۴	۵	۴	۱۰	۵	۴	۶
متولی تحقیقات، آموزش، استاندارد سازی و بومی سازی تجهیزات سایبری	N۱۲	۲	۴	۳	۶	۶	۷	۶	۶	۷	۵	۵	۱۰	۹	۵
متولی رمز ملی و تصدیق هویت مجازی	N۱۳	۴	۶	۴	۶	۷	۸	۷	۷	۶	۶	۵	۷	۱۰	۵
نهاد مدیریت محتوای سایبری و رسانه ها	N۱۴	۱	۳	۱	۱	۱	۶	۶	۵	۴	۴	۴	۲	۳	۱۰

جدول ۵: ماتریس دستیابی کلان فرآیند رمزنگاری و امنیت اطلاعات

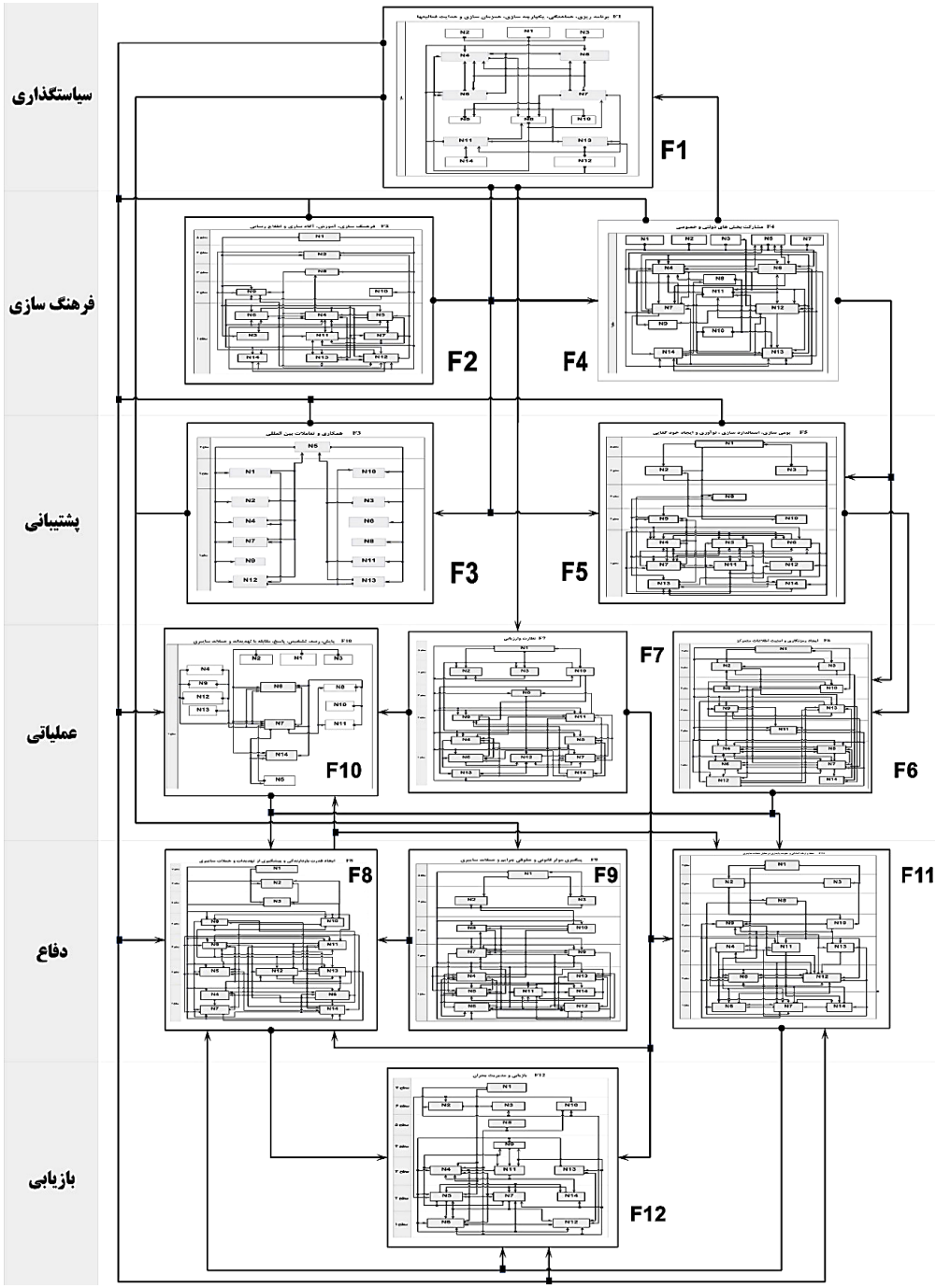
فرآیند ۶ ایجاد رمزنگاری و امنیت اطلاعات متمرکز اگر سطر روی ستون تاثیر داشته باشد = V اگر ستون روی سطر تاثیر داشته باشد = A انجام محاسبات اثر متقابل = X بی اثر = O	نهاد	متولی سیاست گذاری حوزه امنیت سایبر	متولی فرماندهی سایبری و تعیین وضعیت	متولی تدوین قوانین و مقررات سایبری	متولی امنیت فضای سایبر در صنعت کشور و بیمه سایبر	متولی امور بین الملل ودفاع سایبری کشورهای اسلامی	متولی مراکز عملیات امنیت شبکه و پاسخگویی	متولی مقابله با جرائم سازمان یافته و تروریسم سایبری	متولی هماهنگی امنیت سایبری قوای سه گانه	متولی حفاظت از زیرساخت های ملی	متولی نظارت و ارزیابی	متولی رصد، پایش تهدیدات و اشتراک گذاری	متولی تحقیقات، آموزش، استاندارد سازی و بومی سازی تجهیزات سایبری	متولی رمز ملی و تصدیق هویت مجازی	نهاد مدیریت محتوای سایبری و رسانه ها	
		N۱	N۲	N۳	N۴	N۵	N۶	N۷	N۸	N۹	N۱۰	N۱۱	N۱۲	N۱۳	N۱۴	
نهاد																
متولی سیاست گذاری حوزه امنیت سایبر	N۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۰	۱۳
متولی فرماندهی سایبری و تعیین وضعیت	N۲	۰	۱	۰	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱۲
متولی تدوین قوانین و مقررات سایبری	N۳	۱	۱	۱	۱	۱	۱	۱	۱	۰	۱	۱	۱	۱	۱	۱۳
متولی امنیت فضای سایبر در صنعت کشور و بیمه سایبر	N۴	۰	۰	۰	۱	۱	۱	۱	۰	۰	۱	۱	۱	۰	۰	۷
متولی امور بین الملل ودفاع سایبری کشورهای اسلامی	N۵	۰	۰	۰	۱	۱	۰	۰	۰	۰	۰	۱	۱	۱	۱	۷
متولی مراکز عملیات امنیت شبکه و پاسخگویی	N۶	۰	۰	۰	۱	۰	۱	۰	۰	۰	۰	۱	۰	۰	۰	۳
متولی مقابله با جرائم سازمان یافته و تروریسم سایبری	N۷	۰	۰	۰	۱	۱	۰	۱	۰	۰	۰	۱	۱	۰	۰	۸
متولی هماهنگی امنیت سایبری قوای سه گانه	N۸	۰	۰	۰	۰	۱	۰	۰	۱	۰	۰	۱	۱	۱	۱	۸
متولی حفاظت از زیرساخت های ملی	N۹	۰	۰	۰	۱	۱	۰	۰	۰	۱	۰	۱	۱	۰	۱	۸
متولی نظارت و ارزیابی	N۱۰	۰	۱	۰	۱	۱	۰	۰	۰	۰	۱	۱	۱	۰	۱	۱۱
متولی رصد، پایش تهدیدات و اشتراک گذاری	N۱۱	۰	۰	۰	۱	۱	۰	۰	۰	۰	۰	۱	۰	۰	۱	۶
متولی تحقیقات، آموزش، استاندارد سازی و بومی سازی تجهیزات سایبری	N۱۲	۰	۰	۰	۱	۱	۱	۰	۰	۰	۰	۰	۱	۱	۰	۶
متولی رمز ملی و تصدیق هویت مجازی	N۱۳	۰	۱	۰	۱	۱	۱	۱	۰	۰	۱	۱	۱	۱	۰	۱۰
نهاد مدیریت محتوای سایبری و رسانه ها	N۱۴	۰	۰	۰	۰	۱	۰	۰	۰	۰	۰	۰	۰	۰	۱	۳
		۲	۵	۲	۱۲	۱۲	۱۲	۱۳	۵	۳	۱۱	۱۲	۱۲	۸	۹	

۸. نتیجه‌گیری و پیشنهاد

این مقاله بر اساس یافته‌های پژوهش گروهی در دانشگاه عالی دفاع ملی با عنوان «طراحی دفاع سایبری کشور و تدوین راهبردهای آن» مبتنی بر بررسی وضع موجود، شناسایی فرآیندها و نهادهای دفاع سایبری کشور (با استفاده از مدل پایه زکمن) و نحوه تعامل این نهادها در سطح داخلی و بین‌المللی با تکیه بر مطالعات اسناد بالادستی کشور و قوانین و مقررات جاری، با بهره‌گیری از نظرات متخصصین، پژوهشگران، مدیران و متصدیان حوزه‌ی فناوری اطلاعات و فضای سایبری کشور در افق چشم‌انداز ۱٤۰٤ کشور تدوین گردیده است. در پژوهش فوق، ۱۲ کلان فرآیند برای دفاع سایبری احصاء گردید که ۱٤ نهاد باید برای تحقق آن‌ها با یکدیگر فعالیت‌های هدفمندی را انجام دهند. ششمین کلان فرآیند احصاءشده، رمزنگاری و امنیت اطلاعات متمرکز است که مقاله حاضر تلاش نمود که با استفاده از نتایج پژوهش فوق، جایگاه رمزنگاری و امنیت اطلاعات متمرکز در دفاع سایبری کشور را مورد بررسی قرار داده و مدلی مفهومی را در این خصوص ارائه نماید.

(الف) نتیجه‌گیری

در کلان فرآیند رمزنگاری و امنیت اطلاعات نهادهای اصلی N1 (متولی سیاست‌گذاری حوزه امنیت سایبر)، N2 (متولی فرماندهی سایبری و تعیین وضعیت)، N3 (متولی تدوین قوانین و مقررات سایبری)،N4 (متولی امنیت فضای سایبر در صنعت کشور و بیمه سایبر)، N5 (متولی امور بین‌الملل و دفاع سایبری کشورهای اسلامی)، N6 (متولی مراکز عملیات امنیت شبکه و پاسخگویی)، N7 (متولی هماهنگی امنیت سایبری قوای سه‌گانه)، N8 (متولی هماهنگی امنیت قوای سه‌گانه)، N9 (متولی حفاظت از زیرساخت‌های ملی)، N10 (متولی نظارت و ارزیابی)، N11 (متولی رصد و پایش تهدیدات و اشتراک‌گذاری)، N12 (متولی تحقیقات، آموزش استانداردسازی و بومی‌سازی تجهیزات سایبری)، N13 (متولی رمز ملی و تصدیق هویت مجازی) و N14 (متولی مدیریت محتوای سایبری و رسانه‌ها) در شش سطح فعالیت می‌نمایند که سطح ششم بالاترین اهمیت را دارد و به ترتیب تا سطح اول اهمیت آن‌ها کم می‌شود (شکل ۲).



شکل ۱: مدل مفهومی دفاع سایبری ج.ا.ا.

توضیح سطوح شش‌گانه در شکل ۲ عبارت‌اند از:

۱) در سطح ششم نهاد N1 در بالاترین سطح قرار داشته و ارتباط دوطرفه با نهاد N3 داشته و خروجی آن مورد استفاده نهاد متولی رمز ملی و تصدیق هویت مجازی (N13) و نهادهای N2,N8,N10,N9,N6,N5,N11,N4,N12 قرار می‌گیرد.

۲) در سطح پنجم نهادهای N2,N3 قرار دارند که ورودی N2 از نهادهای N1,N3 بوده و ارتباط دوطرفه با N10 دارد و خروجی آن مورد استفاده نهاد متولی رمز ملی و تصدیق هویت مجازی (N13) و نهادهای N8, N14, N9, N11,N5, N4, N6, N7, N12 است. نهاد N3 ارتباط دوطرفه با N1 داشته و خروجی آن مورد استفاده نهاد متولی رمز ملی و تصدیق هویت مجازی (N13) و نهادهای N9, N8, N11, N4, N5, N6, N12, N2, N14 است.

۳) نهاد N8,N10 در سطح چهارم قرار دارند که ورودی این دو نهاد N8 و N10 از نهاد متولی رمز ملی و تصدیق هویت مجازی (N13) و نهادهای N3,N7,N1,N2 بوده و خروجی آن‌ها مورد استفاده نهاد متولی رمز ملی و تصدیق هویت مجازی (N13) و نهادهای N9,N4,N6,N12 قرار می‌گیرد.

٤) در سطح سوم نهاد متولی رمز ملی و تصدیق هویت مجازی (N13) و نهاد N9 قرار دارند که ورودی N9 از نهاد متولی رمز ملی و تصدیق هویت مجازی (N13) و نهادهای N1,N2,N8,N10,N4,N7 بوده و خروجی آن مورد استفاده نهادهای N11,N4,N5 قرار می‌گیرد. ورودی نهاد متولی رمز ملی و تصدیق هویت مجازی (N13) از نهادهای N1,N2,N3,N7,N12,N5,N8,N10 بوده و خروجی آن مورد استفاده نهادهای N14,N9,N11,N12 قرار می‌گیرد.

۵) در سطح دوم نهاد N11 قرار دارد که ورودی آن از نهاد متولی رمز ملی و تصدیق هویت مجازی (N13) و نهادهای N9,N3,N1,N2,N7 بوده و خروجی آن مورد استفاده N14,N4,N5,N7 قرار می‌گیرد.

٦) در سطح یک نهادهای N4,N5,N6,N7,N12,N14 قرار دارند که ورودی آن‌ها از نهادهای N11,N12 ,N10,N9,N1,N2,N3 بوده و ارتباط N4 و N5 دوطرفه بوده و خروجی آن‌ها مورد استفاده نهادهای N9,N7 قرار می‌گیرد.

a. نهـاد N5 از نهادهـای N4,N1,N2,N3,N12,N14 دارای ورودی بـوده و ارتبـاط دوطرفه با N4 و خروجی آن مورد اسـتفاده نهـاد متـولی رمـز ملـی و تصـدیق هویت مجازی (N13) و نهادN7 قرار می‌گیرد.

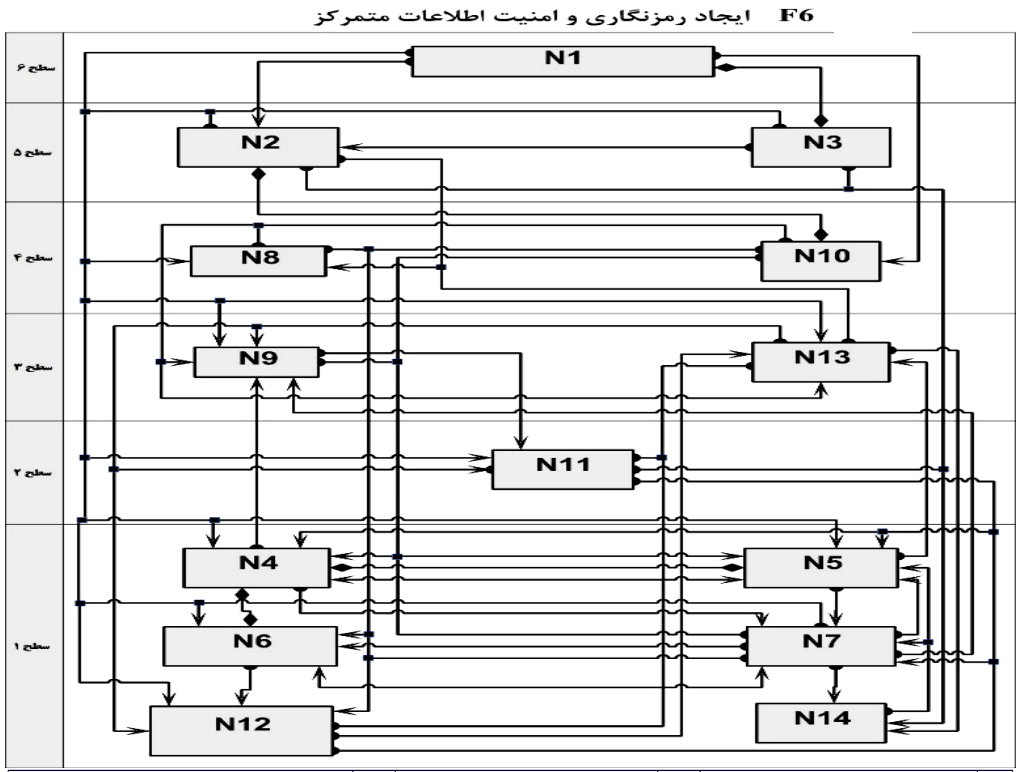
b. نهاد N6 از نهادهای N1,N2,N3,N7,N8 دارای ورودی بوده و ارتبـاط دوطرفـه با N7 داشته و خروجی آن مورد استفاده N12 قرار می‌گیرد.

c. ورودی نهـاد N7 از نهادهـای N5, N6,N4,N14,N12 بـوده و خروجـی آن بـه نهادهای N14,N12, N5, N6,N4,N11,N9 است.

d. ورودی نهاد N12 از نهادهای N1,N6,N3,N7,N8,N10,N13, بوده و خروجی آن به نهادهای N13,N5,N4,N7 قرار می‌گیرد.

e. ورودی N14 از نهادهای N13,N11,N7,N2,N3 بوده و خروجی آن مورد استفاده نهادهای N7,N5 قرار می‌گیرد.

طبق نتایج پژوهش، رمزنگاری و امنیت اطلاعات یکی از کلان فرآیندهای دفاع سـایبری کشور است. با اخذ نظر خبرگان در خصوص روابط متقابل هـر یـک از نهادهـای فـوق بـا یکدیگر و تجزیه‌وتحلیل یافته‌ها با روش مدل‌سازی ساختاری تفسیری، مدل مفهومی کـلان فرآیند رمزنگاری و امنیت اطلاعات در دفاع سایبری کشور استخراج گردید که طبق (شـکل ۲) ترسیم می‌شود.



N۱	متولی سیاست گذاری حوزه امنیت سایبر	N۶	متولی مراکز عملیات امنیت شبکه و پاسخگویی	N۱۱	متولی رصد، پایش تهدیدات و اشتراک گذاری
N۲	متولی فرماندهی سایبری و تعیین وضعیت	N۷	متولی مقابله با جرائم سازمان یافته و تروریسم سایبری	N۱۲	متولی تحقیقات، آموزش، استاندارد سازی و بومی سازی تجهیزات سایبری
N۳	متولی تدوین قوانین و مقررات سایبری	N۸	متولی هماهنگی امنیت سایبری قوای سه گانه	N۱۳	متولی رمز ملی و تصدیق هویت مجازی
N۴	متولی امنیت فضای سایبر در صنعت کشور و بیمه سایبر	N۹	متولی حفاظت از زیرساخت های ملی	N۱۴	نهاد مدیریت محتوای سایبری و رسانه ها
N۵	متولی امور بین الملل ودفاع سایبری کشورهای اسلامی	N۱۰	متولی نظارت و ارزیابی		

شکل ۲: مدل مفهومی کلان فرآیند F6 رمزنگاری و امنیت اطلاعات

(لوزی‌ها ارتباط دوطرفه، دایره‌ها خروجی و پیکان‌ها ورودی هستند)

(ب) پیشنهادها

- با توجه به استفاده از روش فرآیندمحور و با بهره‌گیری از چهارچوب معماری زکمن در این مدل، کلان فرآیند رمزنگاری و امنیت اطلاعات در نظام دفاع سایبری به‌صورت یکپارچه طراحی شده است. پیشنهاد می‌گردد مدل مزبور پس از ارزیابی، در ساختار دفاعی کشور پیاده‌سازی گردد.

- مقایسه وضعیت موجود رمزنگاری و امنیت اطلاعات در دفاع سایبری کشور با وضعیت مطلوب طراحی‌شده، نشان می‌دهد برخی از فرآیندها و نهادها در ساختار موجود کشور وجود ندارند و ضروری است که نهادهای مذکور تشکیل و بعضی با تجمیع یا تغییر شرح خدمات، فرآیندهای مورد نظر در دفاع سایبری را دنبال نمایند.
- با توجه به مطالعات انجام‌شده در کشورهای پیشرو، نهادهایی زیر نظر بالاترین رده اجرایی برای سیاست‌گذاری و هدایت فعالیت‌های حوزه سایبر و به‌خصوص دفاع سایبری ایجاد گردد.
- با توجه به وضعیت نظام جمهوری اسلامی ایران و تقابل دائمی آن با استکبار جهانی و نظام سلطه، تهیه و تأمین تجهیزات سایبری، به‌خصوص با شرایط موجود از مشکلات اساسی در این حوزه بوده و ضرورت دارد اقدامات لازم در زمینه بومی‌سازی تجهیزات سخت‌افزاری و نرم‌افزاری رمزنگاری به‌ویژه در بخش دفاع و ایجاد زنجیره تأمین امن صورت پذیرد.
- تدوین قوانین و مقررات سایبری در فرآیند پیگیری مؤثر قانونی و حقوقی رمزنگاری و امنیت اطلاعات در لایه دوم (سطح پنجم) این فرآیند قرار گرفته و حاکی از اهمیت و اولویت قوانین و مقررات سایبری است. بررسی وضعیت موجود در کشور نشان می‌دهد قوانین و مقررات جامعی در حوزه داخلی و بین‌المللی تدوین نشده است و ضرورت دارد نهادهای قانون‌گذاری نسبت به بازبینی قوانین موجود و تصویب قوانین جدید در این حوزه‌ها مبادرت نمایند. به‌عنوان نمونه مشخص نیست استفاده از رمزکننده در داخل کشور نیاز به مجوز از محل خاصی دارد یا خیر؟ یا در صورت استفاده از رمزکننده‌ها یا صادرات آن‌ها چه اثراتی ممکن است بر فعالیت افراد حقیقی یا حقوقی داشته باشد؟

- به استناد مدل دفاع سایبری فرآیند رصد، پایش، تشخیص، پاسخگویی و مقابله با تهدیدات و حملات سایبری مرتبط با رمزنگاری، یکی از اولویت‌های اساسی در سطح عملیاتی است و از کلان فرآیندهای تأثیرگذار در دفاع سایبری بوده و لازم است نهاد یا نهادهایی در کشور برای رصد و پایش مستمر فضای سایبر در حوزه رمزنگاری ایجاد شده و وقایع این حوزه به‌صورت برخط و به‌موقع به سلسله‌مراتب فرماندهی برای واکنش در مقابل تهدیدات ناشی از آن مانند کامپیوترهای کوانتومی[1]، رمزارزهای[2] مختلف و زنجیره قالب‌ها[3] گزارش گردد.

1. Quantum Computers
2. Crypto Currency
3. Block Chain

فهرست منابع ومآخذ

الف. منابع فارسی

- اسماعیلی، علی؛ تقی‌پور، رضا، (۱۳۹۷)، طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران، فصلنامه امنیت ملی، سال هشتم، شماره سی‌ام، زمستان ۱۳۹۷، صص ۲۰۲ – ۱۸۱.
- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)، (۱۳۹۰)، پژوهشکده امنیت، گزارش مطالعاتی نظام محرمانگی، امضای دیجیتال و طرح حمایت از رمز ملی، فاز اول.
- اسماعیلی، علی؛ تقی‌پور، رضا، (۱۳۹۷)، طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران، فصلنامه امنیت ملی، سال هشتم، شماره سی‌ام، زمستان ۱۳۹۷، صص ۲۰۲ – ۱۸۱.
- پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)، (۱۳۹۰)، پژوهشکده امنیت، گزارش مطالعاتی نظام محرمانگی، امضای دیجیتال و طرح حمایت از رمز ملی، فاز اول.
- ستاد ویژه توسعه فناوری نانو، (۱۳۹۱)، سند تکمیلی سوم راهبرد ده‌ساله توسعه فناوری نانو در جمهوری اسلامی ایران، معاونت علمی و فناوری ریاست جمهوری.
- سند چشم‌انداز بیست‌ساله جمهوری اسلامی ایران، (۱۳۸٤).
- حسن‌بیگی، ابراهیم، (۱۳۹۰)، مدیریت راهبردی، چاپ اول، سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).
- حسینی، پرویز؛ ظریف‌منش، حسین، (۱۳۹۲)، مطالعه تطبیقی ساختار دفاع سایبری کشورها، فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین (علیه‌السلام)، سال دوم، شماره ۵ (بهار ۱۳۹۲)، صص ٦۸ – ٤۱.
- دفتر امور زیربنایی فناوری اطلاعات، (۱۳۸۸)، وزارت ارتباطات و فناوری اطلاعات، سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور (افتا).
- رامک، مهراب؛ امیرلی، حسین؛ قربانی، ولی‌الله؛ حقی، مجید؛ کاظمی، موسی؛ رمضان یارندی، محسن؛ اسماعیلی، علی؛ یزدانی، سعید؛ ملائی، علی، (۱۳۹۵)، طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن، مطالعه گروهی، دانشکده امنیت ملی، دانشگاه عالی دفاع ملّی.
- شورای عالی انقلاب فرهنگی، (۱۳۹۰)، نقشه جامع علمی کشور.
- گروه واژه‌گزینی انجمن رمز ایران، (۱۳۹۰)، واژه‌نامه و فرهنگ امنیت فضای تولید و تبادل اطلاعات (افتا)، چاپ اول، مؤسسه انتشارات دانشگاه صنعتی شریف.

ب. منابع انگلیسی

- Budish Ryan, Burkert herbert, Gasser urs, Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects, A HOOVER INSTITUTION ESSAY, Aegis Series Paper No. 1804, National Security, Technology, and Law, 2018
- ITU, Global Cybersecurity Index (GCI), ITU Publications, Studies & research, 2018
- ITU, Global Cybersecurity Index (GCI), ITU-D, 2017
- NIST National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018.
- NIST National Institute of Standards and Technology, NIST Cryptographic Standards and Guidelines Development Process, http://dx.doi.org/10.6028/NIST.IR.7977, March 2016.
- NIST National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1, February, 2014.
- Ogiela Marek R. Ogiela Lidia, Cognitive cryptography techniques for intelligent information management, International Journal of Information Management 40 (2018) 21–27,
- Preneel Bart, the future of cryptography, EUROCRYPT,Springer, 2016.