فصلنامه علمی مطالعات مدیریت راهبردی دفاع ملی
سال هشتم، شماره ۳۰، تابستان ۱۴۰۳
مقاله پژوهشی، از صفحات ۱۴۱-۱۸۴

مقاله پژوهشی:

ارائه الگوی ساختار حاکمیتی امنیت سایبری عراق

مسعود باقری[۱]، محمدرضا موحدی صفت[۲]، نصب الله دوستی مطلق[۳]، علی عباس[۴]

تاریخ دریافت: ۱۴۰۱/۱۱/۱۲ **تاریخ پذیرش: ۱۴۰۲/۰۲/۰۶**

چکیده

امنیت سایبری به یکی از مباحث جهانی و از اصول اساسی نظام امنیت حال حاضر و بخشی از سیاست‌های امنیت ملی تبدیل گشته است. با بررسی وضعیت موجود در عراق در حوزه امنیت سایبری شاهد یک بی ساختاری وعدم ساماندهی دولتی از سال ۲۰۰۳ هستیم که باعث هدر رفت عظیم دارایی‌ها و امکانات و دخالت در تصمیم‌گیری‌ها و شکست روند سیاست‌گذاری‌ها و تدوین راهبردها در حوزه امنیت سایبری ملی عراق شده است. هدف این پژوهش عبارت است از دستیابی به الگوی ساختار حاکمیتی امنیت سایبری عراق. روش تحقیق این پژوهش با رویکرد آمیخته (کیفی وکمی) است و با استفاده از روش توصیفی- تحلیلی انجام شده است. برای تجزیه تحلیل داده‌ها، آزمون تی- تست و مدل‌سازی معادلات ساختاری به روش حداقل مربعات جزئی با استفاده از نرم‌افزار اسمارت پی.ال.اس، انتخاب شد. یافته‌های پژوهش نشان می‌دهد که پنج حوزه «ساختار حاکمیتی امنیت سایبری عراق»، شامل: «همکاری» با ۴ زیرمؤلفه، «توسعه و ظرفیت‌سازی» با ۱۰ زیرمؤلفه، «قانونی» با ۲ زیرمؤلفه، «سازمانی» با ۱۰ زیرمؤلفه و «فنی» با ۸ زیرمؤلفه، به‌صورت مکمل بر ساختار حاکمیتی امنیت سایبری تأثیرگذارند؛ ولی میزان تأثیرگذاری آن‌ها از نگاه جامعه آماری متفاوت است.

کلیدواژه‌ها: امنیت سایبری، فضای سایبری، طراحی ساختاری، ساختار حاکمیتی، کشورعراق

۱. استادیار دانشگاه جامع امام حسین (ع).
۲. استادیار و عضو هیئت علمی دانشگاه عالی دفاع ملی. تهران. ایران.
۳. استادیار دانشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران.
۴. دانش آموخته دانشگاه عالی دفاع ملی؛ نویسنده مسئول؛ رایانامه: alwandawy@gmail.com

مقدمه

امنیت سایبری یکی از چالش‌هایی است که کشورها با آن مواجه هستند و دارای ابعاد و زمینه‌های مختلف امنیتی، نظامی، سیاسی، اقتصادی، اجتماعی و فرهنگی است و کشورهایی که فاقد چشم‌انداز و مدیریت راهبردی صحیح برای امنیت سایبری هستند (مانند کشور عراق، به‌ویژه پس از سال ۲۰۰۳) با خطرات و تهدیدات جدی مواجه‌اند. یکی از حملات سایبری که در سطح یک تهدید برای امنیت ملی عراق تلقی می‌شد، حمله سایبری توسط «گروه امنیت سایبری» در ۲۷ سپتامبر ۲۰۱۹ صورت گرفت که سایت‌های دولت عراق هک شد. بنابراین مسئله تحقیق بر محور ضعف امنیت سایبری عراق به دلیل مشکلات امنیتی به‌وجود آمده پس از سقوط رژیم سابق و اشغال عراق از سال ۲۰۰۳ قرار دارد. با به دست گرفتن دولت توسط آمریکا هیچ دستگاهی مسئولیت مدیریت فضای سایبری عراق (به دلیل فقدان یک ساختار حاکمیتی امنیت سایبری عراق) و نیز وظیفه تدوین قوانین و راهبردهای ملی امنیت سایبری عراق، نظارت بر اجرای آن، سیاست‌گذاری در این حوزه و ایجاد سامانه‌های مدیریت خطر و مقابله با خطرات و تهدیدات امنیت سایبری را بر عهده نگرفت. این مسئله فضای سایبری عراق را در معرض انواع حملات الکترونیکی توسط گروه‌های هکر و دشمنان قرار داده است.

فقدان یک ساختار حاکمیتی مشخص برای امنیت سایبری عراق، باعث ایجاد بی‌نظمی و تداخل مسئولیت‌ها و اختیارات دستگاه‌های مرتبط با حوزه امنیت سایبر در سطح ملی شده است. فقدان چنین ساختاری ملی باعث گشته است تا قوانین و مقرراتی جهت اجرا در این زمینه که متناسب با تحولات آینده و پیش رو باشد، وضع نگردد؛ بنابراین در عراق قانونی جدید و مناسب در حوزه امنیت سایبری وجود ندارد و کلیه قوانین مربوط به دوره رژیم سابق بوده و از کارایی لازم برای حل مشکلات فعلی و آینده عراق برخوردار نیست. با گسترش این مسئله همچنین شاهد عدم وجود همکاری فعال و مؤثر میان نهادهای دولتی و بخش خصوصی عراق و نیز فقدان همکاری‌های بین‌المللی هستیم که در صورت رفع این مشکل می‌توان به میزان زیادی در جهت تحقق هماهنگی و همکاری، یکپارچه‌سازی اهداف و چشم‌انداز ملی، سرفصل‌های آموزشی و فرهنگ‌سازی در جامعه و دولت عراق و نیز کاهش تهدیدات و خطرات فضای سایبری و انجام مقابله مؤثر و به‌موقع با انتشار محتوای خلاف عرف و اعتقادات و ارزش‌های جامعه ونیز آسیب‌های اقتصادی که امنیت ملی عراق را تهدید می‌کند، خواهیم بود.

با توجه به گستردگی مفهوم، تعدد جوانب و پیچیدگی امنیت سایبری ملی، بعد ساختاری به دلیل مقدم بودن بر سایر جوانب مدنظر قرار گرفته است تا مورد بررسی قرار گیرد و بیشتر اقدامات و تلاش‌ها بر این اساس خواهد بود. این مسئله محقق را بر آن واداشت تا در پی طراحی یک ساختار حاکمیتی امنیت سایبری برای عراق باشد.

بدیهی است در صورت انجام تحقیق حاضر تصمیم‌سازان حوزه امنیت سایبری از دستارودهای این پژوهش همچون: تعیین وظایف، ماموریت‌ها واختیارات دستگاه‌های مرتبط با امنیت سایبری همراه با بکارگیری مناسب، هماهنگ ویکپارچه نیروی انسانی، امکانات وفناوری‌های نوین در سطح ملی، همکاری فعال میان بخش‌های مختلف دولت و بخش خصوصی در حوزه امنیت سایبری، کاهش خطرات و تهدیدات سایبری و تقویت بنیه دفاعی دستگاه‌های ملی و طرف‌های ذی‌ربط در حوزه فضای سایبری و امنیت آن، بهره‌مند خواهند شد.

سؤالات تحقیق

۱.اهداف اساسی ساختار حاکمیتی امنیت سایبری عراق کدامند؟

۲. حوزه‌های ساختار حاکمیتی امنیت سایبری عراق کدامند؟

۳. مهم‌ترین موانع و چالش‌های امنیت سایبری عراق کدامند؟

مبانی نظری و پیشینه‌شناسی تحقیق

مروری بر پیشینه تحقیقات داخلی و خارجی

جدول (۱): پیشینه داخلی و خارجی تحقیق

عنوان رساله	راهبرد امنیت سایبری و نقش آن در امنیت ملی عراق پس از سال ۲۰۱۰
پژوهشگر/ تاریخ	داود، احمد سلمان و الحمدانی، رفاه شهاب. مشرف (۲۰۲۰). پایان‌نامه کارشناسی ارشد، دانشگاه علوم دفاعی و مطالعات نظامی، دانشکده دفاع ملی، دوره (۲۳)، عراق. (داود و الحمدانی، ۲۰۲۰)
سؤال تحقیق	توسعه در زمینه اطلاعات و ارتباطات چه تأثیری بر بحث امنیت ملی عراق دارد؟ چگونه فضای سایبری در مفاهیم امنیت، قدرت، درگیری و جنگ تأثیر می‌گذارد؟ تلاش سایر کشورها برای مقابله با تهدیدات سایبری و چشم‌انداز امنیت سایبری در جمهوری عراق چیست؟ راهبرد ملی عراق برای مقابله با تهدیدهای سایبری چیست؟

نتایج	مهم‌ترین نتایج تحقیق عبارت است از: معنا و مفهوم امنیت ملی گسترش‌یافته و همه زمینه‌های زندگی را در برمی‌گیرد تا با رشد تعامل با فضای سایبری مقابله کند؛ فضایی که در دیدگاه روابط بین‌الملل، در مفهوم قدرت، جنگ و درگیری، تغییراتی ایجاد کرده است.فضای سایبری پس از دریا، زمین و آسمان، چهارمین فضا در زمینه تعامل مؤلفه‌های مادی و غیرمادی با عامل انسانی است.امنیت سایبری عنصر اساسی در پویایی امنیت ملی، منطقه‌ای و بین‌المللی است. بنابراین هرچه محتوای اطلاعاتی دولت در فضای مجازی بیشتر باشد، بین امنیت ملی و امنیت سایبری پیوند بیشتری وجود دارد.کشورها تلاش کرده‌اند از طریق دو عامل اصلی با تهدیدات سایبری مقابله کرده و بدین ترتیب از امنیت ملی خود محافظت کنند: عامل اول فنی بوده و از طریق توسعه ارتش‌های سایبری و تأسیس مراکز امنیت سایبری صورت می‌گیرد. عامل دوم، تدوین قوانین، به‌ویژه قوانین ملی متناسب با قوانین منطق‌های و بین‌المللی است.سیاست‌های اهمال گرانه و نابودکننده رژیم قبلی، جنگ‌های بیهوده و اقدامات تروریستی و نظامی پس از سال ۲۰۰۳، باعث شد که اجرای بسیاری از پروژه‌هایی که به پشتیبانی و ارتقا فناوری اطلاعات و ارتباطات کمک می‌کردند به تعویق بیافتد.عدم اتخاذ راهبرد امنیت سایبری عراق خطرات و تهدیدهای پیش روی امنیت ملی را افزایش می‌دهد.بدون ایجاد یک مرکز ملی ذی‌صلاح که تدوین راهبرد امنیت سایبری عراق را بر عهده بگیرد، نمی‌توان امنیت فضای مجازی عراق را تأمین کرد.
عنوان مقاله	طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران
پژوهشگر/ تاریخ	تقی پور، رضا و اسماعیلی، علی (۱۳۹۷)
سؤال تحقیق	چه الگویی می‌تواند برای مقابله با تهدیدات حوزه سایبری مؤثر باشد و امر دفاع در فضای سایبر را روشمند و هدفمند نماید تا در برخورد با حملات سایبری علاوه بر کنترل تهدیدات، آسیب‌پذیری‌ها را نیز به حداقل برساند؟
نتایج	مدل مفهومی که حاکی از ارتباط خیلی خوب میان ابعاد، مؤلفه‌ها و شاخص‌ها است، می‌تواند پیش‌زمینه طراحی نظام دفاع سایبری و معماری نهاد و فرایندهای کارآمد دفاع سایبری قرار گیرد. تدوین هرگونه راهبرد در عرصه دفاع سایبری پس از استحکام پایه‌های چنین نظام کارآمدی ممکن است که در آن وظایف کلیه نهادها مشخص شده باشد. تدوین راهبرد نیز مستلزم شناخت دقیق نقاط ضعف و قوت و نیز تهدیدات و فرصت‌ها در فضای سایبر است. مشخص شدن نقاط ضعف و قوت موجب تقویت سرمایه‌گذاری در توسعه

	دانش و فناوری در زمینه فضای سایبر می‌شود که این موضوع خود می‌تواند زمینه درنوردیده شدن مرزهای علمی و جهش در سایر ابعاد به‌ویژه در عرصه اقتصادی کشور شود.
عنوان مقاله	تحلیل تطبیقی سیاست‌های ملی امنیت سایبری؛ نمونه موردی: آمریکا، انگلیس و ترکیه
پژوهشگران	کراتاش، عدنان(KARATAŞ,A)
تاریخ و محل ارائه	۲۰۲۰، مجله منابع اجتماعی دانشگاهی، (:e-ISSN۲۶۳۶-۷۶۳۷)، دوره: ۵، شماره: ۱۹؛ ص: ۷۳۷-۷۵۱.
سؤال/مسئله تحقیق	این پژوهش درباره تعیین سیاست‌های ساختار اداری مبتنی بر ارتباط کارآمد بین مؤسسات، به‌منظور ارائه مؤثر آن‌هاست که از طریق تجزیه‌وتحلیل تطبیقی سیاست‌های امنیت سایبری ملی آمریکا، انگلیس و ترکیه صورت گرفته است. در این پژوهش از مجموعه‌ای از استانداردهایی استفاده شده است که سازمان‌های بین‌المللی در مورد سیاست‌ها یا راهبردهای امنیت سایبری، طراحی کرده‌اند.
نتایج	یکی از مهم‌ترین نتایج این تحقیق، این است که بخش‌های دولتی و خصوصی اهمیت موضوع امنیت سایبری و لزوم برنامه‌ریزی برای امنیت سایبری در سطح راهبردیک را درک نمی‌کنند. به همین دلیل، برای تضمین امنیت سایبری ملی، مطالعاتی لازم است. هنگامی سیاست‌های امنیت سایبری ملی ترکیه، در مقایسه با سایر کشورها تحلیل می‌شود، می‌بینیم که: هدف، چشم‌انداز، پیام، اصول اصلی و اهداف راهبردی ترکیه تعیین نشده است. در زمینه برنامه‌ریزی راهبردی، وظایف شهروندان، بخش خصوصی، نهادها و سازمان‌های دولتی مشخص نمی‌شود. قوانین کنونی ترکیه در مبارزه با جرائم اینترنتی کافی نیست. آموزش‌هایی که باید به کارکنان فعال در زمینه قانون و قضا و مبارزه با جرائم اینترنتی ارائه شود، صورت نمی‌گیرد. به همکاری بین بخش‌های دولتی و خصوصی اهمیت کافی داده نمی‌شود. تعیین زیرساخت‌های مهم، امنیت، تجزیه‌وتحلیل مخاطرات و اقدامات انجام شده، صورت نمی‌گیرد. مسائل مربوط به آموزش و آگاهی بخشی، کافی نیست.باید معیارهای افزایش محصولات مربوط به برنامه‌نویسی و سرویس‌ها، تعیین شود.بودجه‌ای برای برنامه‌ریزی راهبردی وجود ندارد.

مفاهیم واصطلاحات

یافتن مفاهیم واصطلاحات، مشکلی است که پژوهشگران در تخصص‌های مختلف، با آن مواجه هستند؛ علت این مسئله نیز، مشکلاتی است که اتفاق نظر بر سر تعاریف مشخص، فراگیر و واحد بین اعضای جامعه علمی را به وجود می‌آورد. امنیت سایبری، ساختار حاکمیتی و فضای سایری از جمله مفاهیم پیچیده‌ای هستند که تعاریف مختلفی از آن ذکر شده است.

امنیت سایبری

امنیت سایبری: از لحاظ زبانی، از دوکلمه تشکیل شده است: "امنیت" و"سایبر"؛ امنیت از نظر لغوی به معنای امان ومتضاد ترس است؛ به معنای آرامش، پیام، حمایت، راستی وذمه که همه این واژگان متضاد ترس هستند. از نظر اصطلاحی نیز به معنای توانایی مقابله با خطرات ومشکلات وتأمین نیازهای اصلی انسان است. شاید دقیق‌ترین مفهوم امنیت این آیه شریفه از قرآن کریم باشد: "فلیعبدوا رب هذا البیت الذی أطعمهم من جوع وأمنهم من خوف[۱]". سایبر هم در لغت به معنای کنترل از دور یا هدایت است. با مراجعه به فرهنگ‌های لغت، معمولا اشاره‌ای به ریشه کلمه سایبر[۲] نشده است. فقط در فرهنگ لغت «المورد» آمده است: سایبری: علم کنترل وریشه آن سایبرنتیک[۳]؛ یعنی کنترل اشیاء از راه دور (مارینسکو[۴]، ۲۰۱۷: ۲۴۳).

امنیت سایبری به اشکال مختلفی تعریف شده است که مهمترین آنها عبارتند از:

مجموعه‌ای از ابزارها، سیاست‌ها، مفاهیم امنیتی، کنترل‌های امنیتی، دستورالعمل‌ها، رویکردهای مدیریت ریسک، رویه‌ها، آموزش بهترین شیوه‌ها، سازوکارهای تضمینی وفناوری‌هایی که می‌توانند برای حفاظت از محیط سایبری ودارایی‌های سازمان‌ها وکاربران استفاده شوند.

سازمان‌ها ودارایی‌های کاربر شامل دستگاه‌های محاسباتی شبکه، پرسنل، زیرساخت‌ها، برنامه‌ها، خدمات، سیستم‌های ارتباطی ومجموع اطلاعات منتقل شده و/یا ذخیره شده در محیط سایبری است (اتحادیه بین المللی مخابرات[۵] (ITU)، ۲۰۱۰ : ۱).

---

۱. قرآن الکریم، سورهٔ قریش، آیه ۲ و۳.

2. Cyber
3. Cybernetics
4. Marinescu
5. International Telecommunication Union (ITU)

شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه شده (جاگذاری شده)، کنترل کننده‌های صنایع حیاتی، محیط مجازی اطلاعات واثر متقابل بین این محیط وانسان برای تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی وبهره‌برداری از اطلاعات گفته می‌شود که ممکن است در ارتباط مستقیم ومداوم با سامانه‌های فناوری اطلاعات وشبکه‌های ارتباطی اعم از شبکه اینترنت باشد ویا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد (کمیته دائمی شواری عالی فضای مجازی جمهوریه إسلامیه ایران، ۱۳۹۴) .

بنابراین از تعاریف فوق می‌توان به تعریفی از امنیت سایبری رسید و آن را مجموعه‌ای از چارچوب‌های قانونی و نظارتی، ساختارهای، ابزارهای فنی و فناوری، بهترین شیوه‌ها و تلاش‌های مشترک بخش‌های خصوصی ودولتی داخلی یا بین‌المللی تعریف کرد که با هدف حفاظت از فضای سایبری که شامل افراد و زیرساخت‌های اطلاعات و خدماتی در حوزه الکترونی، دانست.

فضای سایبری

بحث تعریف فضای مجازی یک موضوع نسبی است. به این معنی که تعاریف به ماهیت هر کشور یا نهاد و میزان توانایی آن در تعریف چشم‌انداز و راهبردی خود برای برخورد با حوزه فضای سایبری اعم از ملکی و نظامی همچنین میزان توانایی آن در بهره‌برداری از مزیت‌ها و مواجهه با خطرات ذاتی در این حوزه بستگی دارد؛ مثلاً کسانی هستند که حوزه فضای مجازی را «بازوی چهارم ارتش‌های مدرن» در کنار نیروهای هوایی، زمینی و دریایی تعریف کرده‌اند. به خصوص که دوران اینترنت شاهد آغاز نبردهای واقعی در این دنیای مجازی بود (بدران، ۱۳۸۹ :۴). افرادی نیز هستند که معتقدند فضای مجازی نشان‌دهنده بعد پنجم جنگ است (شکر، ۲۰۱۹). پس از هوا، زمین، دریا و فضا، اتحادیه بین‌المللی مخابرات نیز آن را به‌عنوان «سپهر فیزیکی و غیر مادی تعریف می‌کند که از عناصر رایانه، شبکه، نرم‌افزار، اطلاعات محاسباتی، محتوا، داده‌های انتقال و کنترل و کاربران همه این عناصر تشکیل شده است (ITU، ۲۰۱۰: ۱۲). فضای سایبری به اشکال مختلفی تعریف شده است که مهمترین آنها عبارتند از:

مجموعه‌ای از ارتباطات میان انسان‌ها از راه رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی (حاجت و نصرتی، ۱۳۹۲) .

مجموعه‌ای از شبکه‌های سخت‌افزاری، نرم‌افزاری، داده‌ها وافرادی که با آن‌ها در تعامل هستند، به هم متصل شده‌اند (کمیلا[1]، ۲۰۱۷).

براساس تعاریف فوق می‌توان به تعریف فضای مجازی رسید و گفت: فضای مجازی محیطی تعاملی است که شامل عناصر مادی و غیر مادی است و متشکل است از گروهی از دستگاه‌های دیجیتال، سیستم‌های شبکه و اطلاعات، نرم‌افزارها و کاربران اعم از اپراتورها یا کاربران.

ساختار حاکمیتی

ساختار حاکمیتی از دوجزء ساختار وحاکمیت تشکیل شده است، ساختار توسط فرهنگ لغت آکسفورد به عنوان روشی تعریف شده است که در آن بخش‌های یک شی به یکدیگر مرتبط و سازمان‌دهی می‌شوند؛ یک چیدمان خاص قطعات؛ یا حالتی است که به‌خوبی سازماندهی شده یا به‌خوبی برنامه‌ریزی شده است وهمه قسمت‌ها به‌هم گره خورده‌اند. حاکمیت به عنوان «اقتدار عالی دولت بر رعایای خود واستقلال آن از هر مقام خارجی تعریف شده است و این امر منجر به آزادی کامل دولت در تنظیم قوای مقننه، اداری وقضایی می‌شود؛ همچنین آزادی کاملی برای تبادل روابط با دیگران در کار بر اساس برابری کامل بین آنها دارد (العیسی، ۲۰۱۰).

بنابراین، می‌توان از مفاهیم ساختار و حاکمیت در تعریف ساختار حاکمیتی به‌عنوان الگو یا قالب از بازیگران دارای قدرت و استقلال در تصمیم‌گیری و تعریف ماموریت‌ها، سطوح، نقش‌ها و فرایندها و سازوکار ارتباط و تماس بین آن‌ها برای دستیابی به هدف مشخص شده، بهره برد.

حکمرانی و حاکمیت فضای مجازی

به‌طورکلی حاکمیت سایبری مورد توافقی وجود ندارند و اغلب در رابطه با قدرت دولت و استقلال در فضای سایبری استفاده می‌شود. خود حاکمیت یک مفهوم کاملاً مشخص در حقوق بین‌الملل است؛ بنابراین، مفهوم حاکمیت سایبری نیاز به تعریف دقیق‌تری دارد. مفهوم حاکمیت به صلح وستفالیا در سال ۱۶۴۸ برمی‌گردد که طبق آن دولت‌ها باید بر سرزمین‌ها و امور داخلی خود حاکمیت داشته باشند تا سایر دولت‌ها نتوانند در امور آن‌ها دخالت کنند (رحیمه و محمد، ۲۰۱۴).

اعمال حاکمیت به معنای داشتن توانایی اعمال اراده بر یک چیز، شخص یا موضوع در یک منطقه جغرافیایی خاص است. بارزترین جلوه اعمال حاکمیت توسط بازیگران و نهادهای سیاسی حکومت، حاکمیت در حوزه صلاحیت جغرافیایی دولت‌هاست که فضای ملی نامیده می‌شود. این

1. Komila

حاکمیت، استقلال عمل و حق دولت‌ها و دولت‌ها برای تصمیم‌گیری در مورد سیاست‌های داخلی و خارجی خود است (حافظ‌نیا، ۱۳۹۳).

بنابراین، می‌توان گفت که عناصر اساسی حاکمیت ملی شامل قلمرو، منابع، جمعیت و رژیم (نظامات) است و حقوق اساسی حاکمیت شامل حق استقلال، حق برابری، حق دفاع از خود و حق صلاحیت است. با این حال، ماهیت فراملی فضای سایبری، حاکمیت دولت‌ها را به چالش می‌کشد و سؤالاتی را در مورد اینکه آیا این اصول و حقوق می‌تواند در فضای سایبری اعمال شود یا خیر، مطرح می‌کند.

گزارش ۲۰۱۵ گروه کارشناسان دولتی سازمان ملل متحد[1] به بسیاری از موضوعات از جمله حاکمیت دولت، برابری حاکمیتی، حل‌وفصل مسالمت‌آمیز اختلافات و خودداری از تهدید یا استفاده از زور در روابط بین‌الملل پرداخته است. در این گزارش تأکید شده است که کشورها باید به قوانین بین‌المللی و حقوق و تعهدات حاکمیتی در استفاده از فناوری اطلاعات و ارتباطات ازجمله در فضای مجازی احترام بگذارند. این بدان معناست که دولت‌ها باید حقوق و تعهدات خود را در فعالیت‌های خود در فضای مجازی رعایت کنند.

گروه کارشناسان دولتی سازمان ملل متحد استدلال خود را بر این واقعیت استوار کرد که فضای مجازی بدون زیرساخت‌های فیزیکی وجود ندارد (مانند سرورها و کابل‌هایی که به‌صورت فیزیکی در مرزهای کشور قرار دارند) و این زیرساخت‌ها تابع صلاحیت‌های ملی ایالت‌ها هستند (کاناک[2]، ۲۰۱۰).

حاکمیت فضای مجازی وارث بسیاری از ویژگی‌های حاکمیت ملی از جمله: چهار عنصر اساسی قلمرو، جمعیت، منابع و نظم و چهار حق اساسی استقلال، برابری، دفاع از خود و صلاحیت و چهار اصل اساسی احترام به حاکمیت ملی، عدم تجاوز متقابل، عدم مداخله متقابل در امور داخلی و برابری حاکمیت است.

چهار رکن حاکمیت در فضای مجازی شبیه به چهار رکن حاکمیت در فضای واقعی و فیزیکی است. جمعیت در فضای مجازی شامل کاربران و بازیگران در فضای مجازی می شود؛ قلمروهای

---

۱. (UN GGE) یک پلت فرم اجماع از ۲۰ کشور بر اساس توزیع جغرافیایی است و شامل قدرت های سایبری بـزرگ مانند ایالات متحده، چین، روسیه، بریتانیا، فرانسه، آلمان، ژاپن، موجودیت صهیونیستی و غیره است.

2. Kanuck

سرزمینی در فضای مجازی در واقع همان پلتفرم‌هایی هستند که فضای مجازی بر روی آنها پیکربندی شده و با دستگاه‌ها و دارایی‌های فناوری اطلاعات و ارتباطات مرتبط می شود؛ منابع موجود در فضای مجازی شامل داده‌ها، اطلاعات و محتوای موجود در پلتفرم فضای مجازی است. سامانه در فضای مجازی قدرت مربوط به حق دخالت در زیرساخت‌ها، داده‌ها و سایر دارایی‌های اجتماعی و سامانه‌های ناشی از فضای مجازی است.

بنابراین از مؤلفه‌ها و اصول می‌توان به تعریفی از ساختار حاکمیتی امنیت سایبری عراق رسید و آن را یک الگو یا قالب از بازیگران و مجموعه‌ای از فعالیت‌ها، مأموریت‌ها، نقش‌ها و فرایندها و سازوکار ارتباط و تماس بین آن‌ها دانست که توانایی اعمال اقتدار، حق استقلال، حق برابری، حق دفاع از خود و حق صلاحیت بر قلمرو، مردم، منابع و نظامات درون فضای مجازی عراق را دارند که شامل افراد، زیرساخت‌ها، اطلاعات و خدمات در حوزه الکترونیکی برای حفاظت و دفاع از فضای مجازی عراق از طریق مجموعه‌ای از چارچوب‌های قانونی، نظارتی و فنی، ابزارهای فنی و تکنولوژیکی و بهترین شیوه‌ها برای توسعه و ظرفیت‌سازی و تلاش‌های مشترک بخش‌های دولتی و خصوصی، به‌صورت محلی و بین‌المللی، برای تضمین دستیابی به اهداف اساسی، دانست.

نظرات در مورد حکمرانی فضای مجازی متفاوت است. برخی فضای مجازی را سرزمینی می‌دانند که می‌توان آن را بین دولت‌ها تقسیم کرد و دولت تنها مرجعی است که می‌تواند اختیار قانون‌گذاری خود را بر فضای مجازی اعمال کند. طرفداران این دیدگاه معتقدند که دولت بهترین نهاد حاکم در فضای مجازی است و این دیدگاه نتیجه پذیرش مفهوم وستفالیایی حاکمیت در فضای مجازی است. برخی دیگر فضای مجازی را میراث مشترک بشریت می‌دانستند که هیچ کشوری نمی‌تواند به‌صورت انفرادی و انحصاری آن را کنترل کند. آن‌ها معتقدند هیچ کشوری حق اعلام حاکمیت بر مناطق خارج از حوزه فضایی خود را ندارد ونمی تواند مانع استفاده کشورهای دیگر از این فضا شود (وبر، ۲۰۲۱).

در مورد مفهوم حکمرانی سایبری، می‌توان آن را این‌گونه تعریف کرد: توسعه و به‌کارگیری اصول، استانداردها، قوانین، رویه‌ها و برنامه‌های مشترک توسط دولت (دولت‌ها)، بخش خصوصی و جامعه مدنی که توسعه و استفاده از فضای سایبری را شکل می‌دهد. وقتی از حاکمیت سایبری در یک کشور صحبت می‌کنیم، منظور ما فقط یک دولت است، اما وقتی از حاکمیت سایبری در سطح بین‌المللی صحبت می‌کنیم، منظور دولت‌هاست (سلطانی، ۱۳۹۶: ۱۶۰). حکمرانی سایبری را

می‌توان عملکرد فرآیندهای تصمیم‌گیری به‌گونه‌ای تعریف کرد که مشارکت، شفافیت و مسئولیت‌پذیری را در اتخاذ اقدامات مرتبط با فضای سایبری به همراه سازوکار توافق‌نامه‌ها، راهبردها، قوانین، اقدامات، مقررات و مقررات بین‌المللی افزایش دهد؛ استانداردهایی که به بهترین شکل به هم متصل می‌شوند (افه و بنشیر[1]، ۲۰۱۹).

بررسی وضعیت امنیت سایبری عراق پس از سال ۲۰۰۳

مرحله انتقالی که عراق پس از سال ۲۰۰۳ طی کرد و مشکلات سیاسی، امنیتی، اجتماعی و اقتصادی همراه با آن، در نتیجه اشغالگری آمریکا و تصمیمات نادرست آن در خصوص مدیریت کشور، مشکلات سیاسی و ناسازگاری طرفین بر روی یک رویکرد واحد به مشکلات مدیریتی و امنیتی تروریسم و جرائم سازمان‌یافته تبدیل شد. علاوه بر بی‌ثباتی سیاسی طولانی مدت، نوسانات امنیتی و مشکل تروریسم در کشور اولویت امنیت سایبری را به حاشیه رانده است. ما این را در راهبردهای امنیت ملی مصوب سال ۲۰۱۶ متوجه می‌شویم که خطرات امنیت سایبری را به‌عنوان یک خطر سطح دوم شناسایی می‌کند (شورای امنیت ملی، ۲۰۱۶). این نتیجه خطرات وجودی تروریسم داعش وعدم آگاهی کافی مقامات و تصمیم‌گیران از خطرات و تهدیدات سایبری بود و ضعف در هماهنگی و یکپارچه‌سازی دیدگاه‌های ملی در زمینه مقابله با تهدیدات و خطرات سایبری، به دلیل نبود اطلاعات واقعی در مورد اندازه، نوع و میزان تأثیر این تهدیدات بر امنیت و حاکمیتی ملی بر فضا سایبری عراق بود. باوجود تلاش‌های سازمان‌ها و نهادهای مختلف دولتی مرتبط و کمیته عالی حکومت‌داری الکترونیکی برای ایجاد یک پایگاه گسترده از پیش‌نویس‌های قوانین سایبری (قانون جرائم اطلاعاتی، قانون امضای الکترونیکی و معاملات الکترونیکی، قانون امنیت ارتباطات و انفورماتیک، قانون حفاظت از اطلاعات شخصی، قانون سازمان رسانه و ارتباطات)، اما تنها قانون امضای الکترونیکی و معاملات الکترونیکی در سال ۲۰۱۲ با وجود دو نسخه از قانون جرائم اطلاعاتی که هنوز در مجلس تصویب نشده بود، تصویب شد.

تأخیر در اتخاذ سیاست‌ها و راهبردهای ملی امنیت سایبری، فاصله زمانی زیاد بین تدوین سیاست‌ها و راهبردها تا تصویب آن‌ها حتی بین شورای امنیت ملی و شورای وزیران ایجاد کرد. مختل سازی امنیت عراق پس از نفوذ به سایت‌های حیاتی دولت عراق و بهره‌برداری از فضای مجازی برای گسترش فتنه‌ها و افکار خلاف عرف و سنت و تحریف و تعرض به مراجع مذهبی و

1. Efe & Bensghir

اجتماعی و برافروختن مردم عراق علیه نظام سیاسی و دعوت به تظاهرات که منجر به تغییر دولت آقای عادل عبدالمهدی شد، آغاز شد. علاوه بر افزایش قابل‌توجه جرائم سایبری در سال‌های اخیر و در نتیجه به خطر انداختن امنیت ملی عراق، سند سیاست‌ها و استانداردهای امنیت اطلاعات و به اشتراک‌گذاری داده‌ها در سال ۲۰۲۰ و همچنین راهبرد امنیت سایبری در سال ۲۰۲۲ بدون تائید ارگانی که مسئولیت هماهنگی، پیگیری و ارزیابی اجرای سیاست‌ها و راهبردها را بر عهده بگیرد، به تصویب رسید.

به دلیل نبود ارگان، مرکز یا سازمانی که به امنیت سایبری مرتبط باشد، دولت در تدوین و تهیه سیاست‌ها، راهبردها، و قوانین مربوط به امنیت سایبری و هماهنگی بین مراجع ذی‌ربط به کمیته‌ها و تیم‌های کاری وابسته باقی ماند. در نتیجه تغییر مداوم کمیته‌ها و تیم‌های کاری و تغییر وظایف و مسئولیت‌ها و اعضای این کمیته‌ها به‌صورت مستمر علاوه بر تداخل مداوم، اختیارات و رویه‌ها و وظایف بین بازیگرانی که باعث اتلاف وقت و تلاش و اتلاف هزینه و استفاده بهینه از منابع انسانی و فنی، صورت گرفت. این امر باعث تأخیر در تصویب تصمیمات مأموریتی، اتکا به اطلاعات نادرست، ناتوانی در نظارت بر رعایت و ارزیابی اجرای این سیاست‌ها و راهبردها و ناتوانی در تصویب قوانین مهم مجلس شده است.

تشکیل تیم ملی پاسخگویی به حوادث سایبری در سال ۲۰۱۷، نقش مهمی در پیشرفت جایگاه عراق در شاخص جهانی امنیت سایبری ایجاد کرد به‌گونه‌ای که اتحادیه بین‌المللی مخابراتجایگاه عراق را از رتبه ۱۵۸ در سال ۲۰۱۷ به رتبه ۱۰۷ بین‌المللی در سال ۲۰۱۸ تایید کرد. پس از لغو کمیته عالی فنی ارتباطات و امنیت اطلاعات در سال ۲۰۲۰ و واگذاری کلیه وظایف کمیته از جمله کمیته ملی پاسخگویی به حوادث سایبری به سازمان اطلاعات ملی عراق اتفاق افتاد. همچنین عدم تصویب قوانینی برای مهار جرائم سایبری، ضعف رویه‌ها برای ظرفیت‌سازی و کاهش همکاری و هماهنگی بین بخش‌های دولتی و خصوصی و همکاری‌های بین‌المللی، باعث شد که موقعیت عراق (۲۲) واحد در شاخص سال ۲۰۲۰ کاهش یابد و به شاخص (۱۲۹) در جهان برسد (خریسان، ۲۰۲۱). در مورد تهدیدات پیش روی امنیت ملی عراق در فضای سایبری (امنیت اطلاعات و ارتباطات) که در نتیجه تغییر سریع در استفاده و بهره‌برداری از این فناوری در حال افزایش است، راهبرد امنیت ملی عراق (۲۰۱۶) مهم‌ترین تهدیدات سایبری، شامل موارد زیر است:

امکان حمله به زیرساخت ملی اطلاعات؛ ضعف در قانون‌گذاری و قوانین تنظیم کننده کار این بخش (قوانین لازم برای کاهش جرائم سایبری و تروریسم الکترونیکی)؛ ضعف در حفاظت از فضای مجازی ملی؛ آگاهی اجتماعی محدود از خطرات امنیت سایبری؛ عدم وجود مرجع بالاتر برای مدیریت داده‌ها (شورای امنیت ملی، ۲۰۱۶).

راهبرد امنیت سایبری (۲۰۲۲-۲۰۲۵) همچنین مجموعه‌ای از نقاط ضعف را در فضای سایبری ملی عراق شناسایی کرده است که به شرح زیر است:

فقدان قوانینی برای جلوگیری از جرائم سایبری و اتکا به قوانین مؤثری مانند قانون جزای ۱۱۱ عراق در سال ۱۹۶۴؛ طبقه‌بندی جرائم الکترونیکی در مواد لازم‌الاجرا از قبیل جرائم تهدید کننده در مواد ۴۳۵ و ۴۳۱، جرائم افترا در ماده ۴۳۳، جرائم توهین در ماده ۴۳۴، جرائم افشایی در مواد ۴۳۷ و ۴۳۸ و جرائم کلاهبرداری در ماده ۴۵۶؛ عدم تمرکز مدیریت امنیت اطلاعات، داده‌ها و فضای مجازی که خلأ سازمانی را در فرآیند نظارت، پیگیری و تأمین منابع ایجاد می‌کند؛ کمبود کادر تخصصی در حوزه امنیت سایبری؛ عدم تخصیص مالی و برنامه‌های راهبردی در حوزه فناوری اطلاعات و نبود برنامه‌های درسی دانشگاهی و دوره‌های آموزشی تخصصی در این زمینه که باعث گرایش علاقه‌مندان و مستعدان در حوزه امنیت سایبری شده است؛ وجود زیرساخت‌های ضعیف، مشکل سطح آگاهی عمومی از ایده‌ها و خطراتی که از طریق فضای مجازی قابل دستیابی است؛ نبود توافقات دوجانبه عراق با طرف‌های منطقه‌ای و بین‌المللی و قراردادهای راهبردی با بخش خصوصی بین‌المللی برای فعال کردن کار حفاظت از امنیت سایبری (راهبرد امنیت سایبری، ۲۰۲۲).

چشم‌انداز امنیت سایبری (۲۰۱۵-۲۰۲۲) بر تقویت حفاظت از سیستم‌های فنی و عملیاتی، زیرساخت‌های حیاتی، تاب‌آوری، پاسخگویی به حوادث سایبری تأکید می‌کند. علاوه بر افزایش اعتماد به نهادهای ملی، سرمایه‌گذاران و افراد در فضای سایبری عراق و همچنین کمک به رشد اقتصادی و اجتماعی عراق، با جلوگیری از آسیب‌ها و بازیابی به‌موقع از آن‌ها را مورد تاکید قرار می‌دهد. برای دستیابی به چشم‌انداز ملی، اهداف اساسی امنیت سایبری عراق در راهبرد امنیت سایبری تعریف شده است که بر جنبه‌های (حکمرانی، ظرفیت و تاب‌آوری واکنش به حادثه، ارزیابی ریسک، ظرفیت‌سازی، آگاهی، همکاری با بخش خصوصی و بین‌المللی و اتوماسیون

خدمات) تمرکز دارد. با مطالعه سیاست‌ها و راهبردهای مهم‌ترین کشورها در زمینه امنیت سایبری به این نتیجه می رسیم که اکثر کشورها به‌دنبال دستیابی به اهداف زیر هستند:

تمرکز بر سازوکار یکپارچه‌سازی سیاست‌ها و راهبردهای امنیت سایبری؛ تصویب قوانین لازم برای پیشگیری از جرائم و نیز توجه به سازوکار توزیع نقش‌ها و مسئولیت‌ها و هماهنگی بین مراجع ذی‌ربط؛ انعطاف‌پذیری، اثربخشی و سرعت در واکنش به حوادث سایبری؛ اهمیت دادن به مشارکت و همکاری بین‌المللی و نیاز به همکاری با بخش خصوصی؛ علاقه به توسعه قابلیت‌ها و تخصص‌های محلی؛ علاقه به آموزش و آگاهی از خطرات سایبری؛ ایجاد قابلیت‌های تهاجمی سایبری برای بازدارندگی؛ در نظر گرفتن میدان سایبری به‌عنوان یک میدان نظامی همانند زمین، دریا، هوا و فضا که در اکثر اهداف اساسی راهبرد امنیت سایبری عراق تشابه وهم‌پوشانی دارد.

می‌توان اهداف ذکر شده را در پنج محور اصلی در قالب جدول زیر دشته بندی کرد.

جدول ۲: اهداف اصلی امنیت سایبری عراق در پنج محور طبقه‌بندی شده

محورها اهداف	شماره گویه	اهداف اصلی امنیت سایبری عراق	کد اهداف
یکپارچه‌سازی	۱	متحد کردن چشم‌انداز ملی و اعمال حاکمیت و اقتدار ملی بر فضای مجازی عراق به‌منظور تأمین امنیت جامع فضای مجازی دولت	GI-01
	۲	ادغام سیاست‌ها و راهبردهای امنیت سایبری با سیاست‌ها و راهبردهای امنیت ملی	GI-02
	۳	تصویب قوانین امنیت سایبری منطبق با قوانین عراق و قوانین بین‌المللی	GI-03
هماهنگی	۴	تمرکز تصمیم‌گیری‌ها، وحدت تلاش‌ها و منابع و دستیابی به هماهنگی و تعامل بین بازیگران	GC-01
	۵	تکیه بر تخصص در توزیع کارکردها و وظایف به‌منظور ایجاد هماهنگی، یکپارچگی و دستیابی به امنیت جامع برای فضای مجازی عراق	GC-02
	۶	وضوح ارتباط و تماس بین بازیگران (سطح محلی و بین‌المللی) در فضای مجازی عراق	GC-03
	۷	امکان نظارت و هماهنگی با استان‌ها و اقلیم برای اجرای تصمیمات، قوانین و وظایف و پیگیری و ارزیابی میزان تمکین	GC-04

محورها اهداف	شماره گویه	اهداف اصلی امنیت سایبری عراق	کد اهداف
	۸	تعادل بین اختیارات و مسئولیت‌ها در اجرای وظایف و تصمیمات	GC-05
دفاع و انعطاف پذیری	۹	ارزیابی دوره‌ای، مدیریت خطرات و تهدیدات سایبری و حفاظت از منافع ملی و داده‌های ملی برای دستیابی به حفظ یکپارچگی، دردسترس‌بودن و محرمانه‌بودن اطلاعات	GD-01
	۱۰	دفاع و حفاظت از زیرساخت‌ها و داده‌های حیاتی ملی و داده‌های شخصی در فضای مجازی	GD-02
	۱۱	انعطاف‌پذیری و سرعت در واکنش به حوادث سایبری و بازیابی از آن‌ها برای اطمینان از تداوم خدمات در فضای مجازی عراق	GD-03
	۱۲	امکان جلوگیری از محتوای مضر و توانایی کنترل و مدیریت ترافیک داده‌ها در فضای مجازی عراق	GD-04
	۱۳	توسعه قابلیت‌های سایبری تهاجمی برای بازدارندگی مؤثر در سطح جهانی	GD-05
ساخت و توسعه	۱۴	توسعه زیرساخت‌های ملی و شبکه اطلاعاتی	GB-01
	۱۵	توسعه برنامه‌های آموزشی و دانشگاهی برای امنیت سایبر	GB-02
	۱۶	اعتباربخشی گواهینامه‌ها، استانداردها، کنترل‌ها و صدور مجوزهای لازم برای ایمن کردن فضای مجازی	GB-03
	۱۷	توسعه نیروی کار در زمینه امنیت سایبری	GB-04
	۱۸	حمایت و گسترش فرهنگ و دانش امنیت سایبری و تحریک و تولید محتوا به شکلی که هویت دینی و ملی و ارزش‌های انسانی جامعه را حفظ کند.	GB-05
	۱۹	تشویق سرمایه‌گذاری در تحقیق و توسعه در خدمات امنیت سایبر	GB-06
	۲۰	از نوآوری‌های محلی حمایت کرده و برنامه‌ها، خدمات و محتوای محلی امن را به شیوه‌ای توسعه دهد که نیازهای ملی را برآورده کند.	GB-07
همکاری	۲۱	دستیابی به همکاری مؤثر بین دستگاه‌های دولتی به‌منظور دستیابی به انسجام و تعامل بین آن‌ها	GC-01

محورها اهداف	شماره گویه	اهداف اصلی امنیت سایبری عراق	کد اهداف
	۲۲	دستیابی به همکاری مؤثر با بخش خصوصی برای توسعه و حفاظت از فضای مجازی ملی	GC-02
	۲۳	ایجاد اتحاد و توافقات و دستیابی به همکاری مؤثر با نهادها و سازمان‌های بین‌المللی به‌منظور دستیابی به منافع ملی و حق برابری عراق در مشارکت در حکمرانی فضای بین‌المللی	GC-03

هنگام بررسی وضعیت موجود ساختار حاکمیتی امنیت سایبری عراق بر اساس پنج بعد/حوزه (قانونی، سازمانی، فنی، توسعه و ظرفیت‌سازی و همکاری) و شاخص جهانی امنیت سایبری (۲۰۲۰)، از طریق تجزیه‌وتحلیل اسناد، قوانین، انطباق و اجرا، مهم‌ترین مراجع ذی‌ربط، سازوکار توزیع وظایف و مسئولیت‌ها، پیگیری و ارزیابی میزان همکاری دولت و بخش خصوصی، همکاری و هماهنگی بین‌المللی و سطح ساخت‌وساز و توسعه در این زمینه، نسبت به شناسایی مهم‌ترین موانع و چالش‌های سایبری که دستیابی به حاکمیت و امنیت همه‌جانبه فضای سایبری عراق را محدود می‌کند اقدام شد که در جدول شماره (۳) زیر نشان داده شده است.

جدول ۳: مهم‌ترین موانع و چالش‌های امنیت سایبری عراق بس از سال ۲۰۰۳

بعد	شماره گویه	مهم‌ترین موانع و چالش‌های امنیت سایبری عراق	کد موانع
قانونی	۱	تکیه بر قوانین و تصمیمات قدیمی رژیم گذشته و تأخیر در تصویب قانون و قوانین لازم برای تأمین امنیت فضای مجازی عراق	CL-01
	۲	ترس از سوءاستفاده از قوانین امنیت سایبری برای کاهش آزادی عقیده و اصول دموکراسی و حقوق بشر وجود دارد.	CL-02
	۳	افزایش قدرت فشار (احزاب سیاسی، بازرگانان، رسانه‌های شخصی و غیره) و نفوذ آن‌ها بر دستگاه‌های اجرایی و مقننه برای تأخیر یا عدم تصویب برخی قوانین و سیاست‌های مرتبط با امنیت سایبری برای تأمین منافع خود	CL-03
	۴	اتکای فزاینده به خدمات الکترونیکی شرکت‌های بین‌المللی که اعمال قوانین محلی برای آن‌ها دشوار است.	CL-04

بعد	شماره گویه	مهم‌ترین موانع و چالش‌های امنیت سایبری عراق	کد موانع
سازمانی	۵	تکیه بر کمیته‌ها و تیم‌های کاری برای تدوین، اجرا و نظارت بر انطباق، ارزیابی سیاست‌ها، راهبردها و استانداردهای ملی برای امنیت سایبری و انتظار برای ایجاد یک مرجع، مرکز یا نهاد بالاتر مسئول امنیت سایبری عراق	CO-01
	۶	هرج‌ومرج و همپوشانی در نقش‌ها، مسئولیت‌ها و اختیارات مقامات مرتبط با امنیت سایبری در سطح ملی	CO-02
	۷	کنترل ضعیف بر ظرفیت‌های اینترنت، ارتباطات سلولی، خدمات و ارزهای دیجیتال و دستگاه‌های ممنوعه در داخل قلمرو عراق	CO-03
	۸	ناتوانی در ارزیابی واقعیت واقعی امنیت سایبری عراق و توانایی‌های مورد نیاز آن، آگاهی از اندازه و نوع حملات و میزان آسیب آن‌ها و آگاهی از قابلیت‌های موجود برای دفع و پاسخگویی به حملات	CO-04
	۹	عدم تخصیص مالی برای تأمین امنیت فضای مجازی عراق	CO-05
	۱۰	تکیه بر اطلاعات گمانه‌زنی و در تهیه و تنظیم اسناد مهم برای امنیت سایبری	CO-06
	۱۱	نگهداری اطلاعات حساس و شخصی شرکت‌ها در خارج از عراق و نظارت و ارزیابی ضعیف از انطباق آن‌ها با کنترل‌ها و تصمیمات	CO-07
	۱۲	ضعف در اعمال اقدامات مربوط به حمایت از کودکان در اینترنت	CO-08
فنی	۱۳	کاربرد ضعیف استانداردها و معیارهای امنیت سایبری	CT-01
	۱۴	ضعف در بررسی و ارزیابی دوره‌ای خطرات سایبری در سطوح ملی و نهادی	CT-02
	۱۵	نبود تجهیزات فنی مدرن و ضعف زیرساخت‌های لازم	CT-03
	۱۶	اتکا ضعیف به مجوزها و گواهینامه‌ها در خدمات، استفاده از دستگاه‌ها و ارائه خدمات برای بازیگران در فضای مجازی عراق	CT-04
	۱۷	اتکای شدید به دستگاه‌ها، فناوری‌ها و خدمات خارجی در حوزه امنیت سایبری.	CT-05

بعد	شماره گویه	مهم‌ترین موانع و چالش‌های امنیت سایبری عراق	کد موانع
توسعه و ظرفیت‌سازی	۱۸	عدم وجود صنعت ملی، سرمایه‌گذاری داخلی و وابستگی کلی صنایع خارجی در حوزه امنیت سایبری	CD-01
	۱۹	کاهش شاخص امنیت سایبری عراق نسبت به سایر کشورها و تأثیر آن بر اعتماد سرمایه‌گذاری در فضای سایبری عراق	CD-02
	۲۰	سهولت انتشار و آموزش سایت‌هایی که با ارزش‌ها و آداب و رسوم مغایرت دارند و صلح اجتماعی را تهدید می‌کنند.	CD-03
	۲۱	عدم آگاهی عمومی از خطرات امنیت سایبری	CD-04
	۲۲	امکان تهدید و حملات سایبری برای کشورهایی از عراق در نتیجه عدم کنترل فضای سایبری عراق	CD-05
	۲۳	احتمال گروه‌های تروریستی و اپوزیسیون با انتشار اخبار، تفرقه‌افکنی و بی‌اعتمادی، افشای اطلاعات شخصی، تهدید مسئولان و تلاش برای نفوذ در سیستم الکترونیکی انتخابات از فضای مجازی سوء استفاده می‌کنند و نظام سیاسی را تهدید می‌کنند.	CD-06
	۲۴	ضعف در سازوکار جذب شایستگی در حوزه امنیت سایبری	CD-07
	۲۵	کمبود کادر، دوره‌های آموزشی سایبری، کمپین‌های آگاهی بخشی و برنامه‌های توان‌بخشی و توسعه	CD-08
	۲۶	عدم انجام مطالعات و تحقیقات در زمینه توسعه امنیت سایبری.	CD-09
	۲۹	کمبود مؤسسات، دانشکده‌ها و مراکز مطالعاتی در زمینه امنیت سایبری.	CD-10
همکاری	۳۰	توانایی ضعیف کمیته‌ها برای یافتن سازوکاری برای همکاری مؤثر بین نهادهای دولتی، بخش‌های دولتی و خصوصی، ذینفعان و همکاری بین‌المللی برای اطمینان از درجه بالایی از هماهنگی، یکپارچگی و عدم اشتراک‌گذاری اطلاعات در مورد حملات سایبری و تهدیدهای بین آن‌ها	CC-01
	۳۱	ضعف هماهنگی و همکاری مؤثر بین ادارات دولتی مرکزی و اقلیم کردستان عراق	CC-02

بعد	شماره گویه	مهم‌ترین موانع و چالش‌های امنیت سایبری عراق	کد موانع
	۳۲	عدم مشارکت در فعالیت‌های بین‌المللی امنیت سایبری.	CC-03
	۳۳	انعقاد قراردادهای بین‌المللی یا منطقه‌ای بدون مطالعه و آگاهی از تأثیر آن‌ها بر واقعیت عراق	CC-04
	۳۴	عدم وجود توافق بین‌المللی برای سازوکار همکاری و برخورد مشترک برای محدود کردن و مقابله با تهدیدات سایبری	CC-05

مدل مفهومی تحقیق

کشورهای مختلف بر اساس نوع نگاهشان به مقوله امنیت سایبری، دارای ساختارهای حاکمیتی متفاوتی هستند. از این رو سازمان اداری و سیاسی و اولویت‌های ملی و اهداف اساسی آن‌ها متفاوت است. هیچ ساختار مشابهی وجود ندارد که بتوان آن را برای همه کشورها اعمال کرد. جان کریس جونز نیز سه مرحله «تحلیل»، «تشکیل» و «ارزیابی» را چارچوب اساسی در هر فرآیند طراحی می‌داند (جونز[1]، ۱۹۹۲).

دانستن مهم‌ترین بازیگران، وظایف، نقش‌ها، فرایندها و سازوکار هماهنگی و همکاری بین آنها، برای طراحی یک الگوی مفهومی پیشنهادی برای ساختار حاکمیتی امنیت سایبری عراق مورد نظر مطابق نمودار شماره(۱) ارائه می شود که توانایی اعمال حاکمیت و اقتدار ملی بر فضای مجازی عراق و حفاظت زیرساخت و کاربران و خدامت و اطلاعات و رسیدگی به مهم‌ترین موانع و چالش‌های امنیت سایبری عراق بر اساس پنج بعد (قانونی، سازمانی، فنی، توسعه و ظرفیت‌سازی و همکاری) شاخص جهانی امنیت سایبری (۲۰۲۰)، ذکر شده در جدول (۳) را داشته باشد و دستیابی به اهداف اساسی ساختار حاکمیتی امنیت سایبری عراق که در پنج محور (یکپارچه‌سازی، هماهنگی، توانایی دفاعی و انعطاف‌پذیری، ساخت و توسعه، همکاری) گنجانده شده است. همان‌طور که در جدول شماره (۲) نشان داده شده است. این امر با اقدامات و راهکارهای ساختاری لازم برای رفع یا رهایی از مهم‌ترین موانع و چالش‌های امنیت سایبری عراق انجام می‌شود که در جدول شماره (۴) نشان داده شده است.

1. Jones

جدول ۴ : اقدامات و راهکارهای ساختاری لازم برای رفع یا رهایی از موانع و چالش‌های هر بعد امنیت سایبری عراق

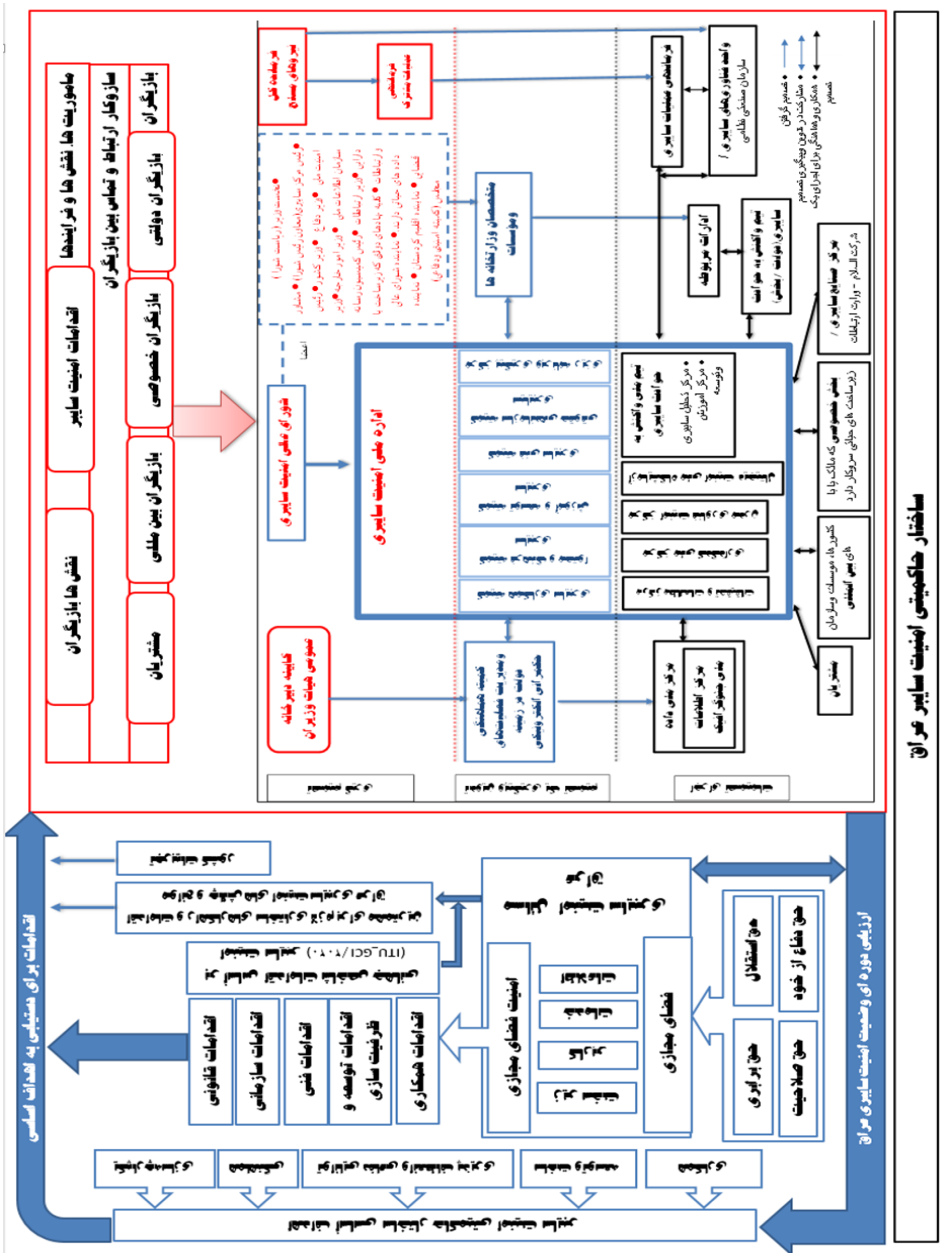
بعد "حوزه"	اقدامات و راهکارهای ساختاری لازم	کد اقدامات
همکاری	ایجاد کمیته‌های مشترک تخصصی دائمی (کمیته حقوقی و مقررات، کمیته فنی، توسعه و آموزش، کمیته آموزش و تولید محتوا و کمیته همکاری) به‌عنوان کمیته‌های مسئول هماهنگی و همکاری با طرف‌های مرتبط جهت تدوین و پیگیری. اجرای تصمیمات، سیاست‌ها، راهبردها، وظایف، مسئولیت‌ها، اتحادها و توافقات در حوزه امنیت سایبری	C-01
	ادغام تیم ملی پاسخگویی به حوادث سایبری در اداره ملی امنیت سایبری به‌عنوان یک نهاد فنی مسئول حفاظت از شبکه‌ها و داده‌های ملی، تحلیل و مدیریت ریسک‌های سایبری به‌عنوان نهاد هماهنگ‌کننده و منبع ارائه اطلاعات کامل و به‌روز در فضای مجازی با نهادهای مربوطه در سطح محلی و جهانی	C-02
	ایجاد تیم پاسخگویی بخشی به حوادث سایبری در کلیه نهادهای دولتی یا بخش خصوصی که دارای زیرساخت‌ها یا داده‌های حیاتی و ارائه‌دهندگان خدمات در فضای سایبری برای هماهنگی و همکاری با تیم ملی واکنش به حوادث سایبری هستند.	C-03
	نمایندگی اقلیم کردستان در شورای عالی امنیت سایبری و در کمیته‌های مشترک دائمی در مرجع ملی و هماهنگی تیم پاسخگویی به حوادث سایبری ملی با تیم پاسخگویی به حوادث سایبری محلی در منطقه	C-04
توسعه و ظرفیت‌سازی	ایجاد مرکز امنیتی فناوری‌های نوین مرتبط با اداره ملی امنیت سایبری	D-01
	ایجاد مرکز صنایع سایبری در شرکت السلام در وزارت ارتباطات	D-02
	ایجاد واحد فناوری سایبری مرتبط با سازمان صنعتی نظامی	D-03
	ایجاد کمیته فنی مشترک دائمی در اداره ملی امنیت سایبری	D-04
	ایجاد کمیته آموزش و توسعه در اداره امنیت ملی سایبری مسئول هماهنگی و تدوین برنامه‌های درسی آموزشی و دانشگاهی، پیگیری اجرای آن‌ها، تشویق و هدایت تحقیقات و مطالعات علمی و توصیه به تأسیس مؤسسه‌ها، گروه‌ها و شعبه‌ها در دانشگاه‌ها و دانشکده‌ها و مراکز آموزشی و توسعه بازیگران در فضای مجازی عراق	D-05
	ایجاد مرکز آموزش و توسعه حرفه‌ای در اداره امنیت سایبری کشور به‌عنوان نهادی	D-06

کد اقدامات	اقدامات و راهکارهای ساختاری لازم	بعد "حوزه"
	مسئول آموزش و تدوین برنامه‌های درسی آموزشی، دانشگاهی و حرفه‌ای با هماهنگی طرف‌های مرتبط از طریق کمیته مشترک دائمی آموزش و توسعه	
D-07	ایجاد کمیته فرهنگ و تولید محتوا مسئول هماهنگی و آماده‌سازی کمپین‌ها و برنامه‌های آگاهی‌رسانی امنیت سایبری در سطح ملی و تشویق، تولید و انتشار محتوای محلی امن سازگار با فرهنگ، عرف و سنت‌های جامعه عراق است.	
D-08	ایجاد مرکز تحلیل سایبری در اداره ملی امنیت سایبری و تجزیه‌وتحلیل و ارزیابی محتوا مطابق با فرهنگ، عرف و سنت‌های جامعه عراق	
D-09	تشکیل تیم پاسخگویی بخشی به حوادث سایبری در کلیه نهادهای دولتی یا بخش خصوصی که دارای زیرساخت‌ها یا داده‌های حیاتی و ارائه‌دهندگان خدمات در فضای سایبری برای هماهنگی و همکاری با تیم ملی پاسخگویی به حوادث سایبری هستند.	
D-10	ایجاد مرکز مطالعات و تحقیقات سایبری در اداره ملی امنیت سایبری، مسئول توسعه و هدایت تحقیقات و مطالعات علمی در زمینه امنیت سایبری	
L-01	تشکیل شورای عالی امنیت سایبری به‌عنوان بالاترین مرجع مسئولیت تصویب و نظارت بر سیاست‌ها و راهبردها، ارائه پیش‌نویس قوانین، تصویب موافقت‌نامه‌ها و معاهدات و هدایت بازیگران برای حفاظت از فضای سایبری ملی با مطابق با اصول اساسی قانون اساسی و عدم مغایرت با قوانین داخلی و بین‌المللی و دستیابی به حاکمیت و منافع ملی در فضای سایبری عراق	قانونی
L-02	ایجاد کمیته مشترک حقوقی دائمی در اداره ملی امنیت سایبری که مسئولیت هماهنگی، تهیه و به‌روز رسانی تصمیمات، سیاست‌ها، راهبردی ملی و پیش‌نویس قوانین در حوزه امنیت سایبری، تنظیم کنترل‌ها، استانداردها و چارچوب‌های مدیریت ریسک را بر عهده خواهد داشت. تهیه مجوزها و گواهینامه‌ها برای اپراتورها، صاحبان زیرساخت‌ها و ارائه‌دهندگان خدمات الکترونیکی و پیگیری اجرای آن‌ها	
O-01	ایجاد شورای عالی امنیت سایبری و اداره ملی امنیت سایبری برای تقسیم وظایف، تعیین نقش و هماهنگی در سطح ملی	سازمانی
O-02	ایجاد اداره ملی امنیت سایبری مسئول هماهنگی و تهیه تصمیمات، سیاست‌ها،	

بعد "حوزه"	اقدامات و راهکارهای ساختاری لازم	کد اقدمات
	پیش‌نویس قوانین، معاهدات و موافقت‌نامه‌های بین‌المللی و ارائه آن‌ها به شورای عالی و پیگیری اجرای آن‌ها نزد مراجع ذی‌ربط است و مسئولیت تنظیم کنترل‌ها را بر عهده دارد. چارچوب‌ها، استانداردها، صدور گواهینامه‌ها و مجوزهای بررسی و تائید دستگاه‌ها، سامانه‌ها و اپلیکیشن‌های الکترونیکی زیرساخت‌های حیاتی و مسئول نظارت بر تحلیل و پاسخگویی به خطرات و تهدیدات سایبری و بازیابی از آن‌ها، تهیه طرح‌ها و برنامه‌های آموزشی و دانشگاهی، مستقیم نوآوری‌ها و تحقیق، توسعه قابلیت‌های محلی (توانمندی‌های فنی، سازمانی و انسانی)، تشویق، تولید و انتشار محتوای محلی متناسب با فرهنگ، عرف و سنت‌های جامعه عراق و همکاری، تبادل و اشتراک‌گذاری اطلاعات در مورد خطرات و تهدیدات سایبری با مقامات محلی. مسئولیت ارزیابی وضعیت امنیت سایبری کشور با هماهنگی مقامات ذی‌ربط را بر عهده دارد.	
	ادغام تیم ملی پاسخگویی به حوادث سایبری در اداره ملی امنیت سایبری به‌عنوان یک نهاد فنی مسئول حفاظت از شبکه‌ها و داده‌های ملی، تجزیه‌وتحلیل و مدیریت ریسک‌های سایبری، به‌عنوان نهاد هماهنگ‌کننده و منبع ارائه اطلاعات کامل و به‌روز. در فضای مجازی با نهادهای مربوطه در سطح محلی و جهانی	O-03
	ایجاد تیم پاسخگویی بخشی به حوادث سایبری در کلیه نهادهای دولتی یا بخش خصوصی که دارای زیرساخت‌ها یا داده‌های حیاتی و ارائه‌دهندگان خدمات در فضای سایبری برای هماهنگی و همکاری با تیم ملی واکنش به حوادث سایبری و ارائه گزارش در مورد رعایت و مهم‌ترین تهدیدات است، خطرات و نیازهای حوزه امنیت سایبری	O-04
	توسعه و حفاظت از شبکه ملی داده با هماهنگی و همکاری بین مرکز ملی داده و اداره ملی امنیت سایبری و هماهنگی با طرف‌هایی که اطلاعات را در خارج از عراق نگهداری می‌کنند.	O-05
	ایجاد کمیته فنی دائمی در اداره امنیت ملی سایبری مسئولیت هماهنگی و تهیه مجوزها و استانداردهای ملی یکپارچه امنیت سایبری و سازوکارهای لازم برای بررسی و تائید دستگاه‌ها، سیستم‌ها و اپلیکیشن‌های فعال در زیرساخت‌های حیاتی کشور و پیگیری اجرای آن‌ها، هماهنگی را بر عهده دارد؛ و تهیه سازوکارهای	O-06

کد اقدامات	اقدامات و راهکارهای ساختاری لازم	بعد "حوزه"
	نظارتی، تحلیل فعال خطرات و تهدیدات سایبری، نحوه پاسخگویی و بازیابی آن‌ها، پیگیری اجرای آن‌ها و هماهنگی برای توسعه و حفاظت از زیرساخت، نرم‌افزار، خدمات الکترونیک ملی، مدیریت حرکت، ظرفیت و محتوای داده‌ها. در فضای سایبری عراق، نوآوری‌ها و صنایع محلی را تشویق کنید، تست‌های فنی امنیتی را برای سیستم‌ها، برنامه‌ها و شبکه‌ها در مؤسسات بخش‌های حیاتی هماهنگ و انجام دهید.	
O-07	ایجاد مرکز تحلیل سایبری در اداره ملی امنیت سایبری و تجزیه‌وتحلیل و ارزیابی محتوا مطابق با فرهنگ، عرف و سنت‌های جامعه عراق	
O-08	ایجاد مرکز ملی رمزگذاری مرتبط با اداره ملی امنیت سایبری مسئول توسعه و ساخت الگوریتم‌های رمزگذاری ملی برای مقابله با تهدیدات فنی و حفاظت از اطلاعات و داده‌های ملی در فضای سایبری عراق	
O-09	ایجاد آزمایشگاه ملی امنیت دیجیتال مرتبط با اداره ملی امنیت سایبری مسئول نظارت و تحلیل دستگاه‌ها، فناوری‌ها، نرم‌افزارها و شبکه‌های مورد استفاده در عملیات مجرمانه و کلاهبرداری اطلاعاتی به مراجع قضایی و امنیتی ذی‌ربط	
O-10	ایجاد مرکز پیگیری و برنامه‌ریزی در اداره ملی امنیت سایبری برای نظارت بر رعایت تصمیمات شورا و ارائه گزارش از وضعیت امنیت سایبری کشور به صورت جامع	
T-01	ایجاد اداره ملی امنیت سایبری با صلاحیت تحمیل اجرای تصمیمات و پیگیری میزان انطباق با آن‌ها از طریق کمیته‌های مشترک و تیم‌های کاری و مسئولیت تنظیم کنترل‌ها، چارچوب‌ها، استانداردها، صدور گواهینامه‌ها و مجوزهای بررسی و تائید دستگاه‌ها، سیستم‌ها و اپلیکیشن‌های الکترونیکی زیرساخت‌های حیاتی و ارزیابی وضعیت امنیت سایبری کشور با هماهنگی مراجع ذی‌ربط	
T-02	تشکیل تیم پاسخگویی به حوادث سایبری بخشی در کلیه نهادهای دولتی یا بخش خصوصی که دارای زیرساخت‌ها یا داده‌های حیاتی و ارائه‌دهندگان خدمات در فضای سایبری برای هماهنگی و همکاری با تیم ملی واکنش به حوادث سایبری و ارائه گزارش در مورد رعایت و مهم‌ترین تهدیدات است، خطرات و نیازهای حوزه امنیت سایبری	

بعد "حوزه"	اقدامات و راهکارهای ساختاری لازم	کد اقدمات
	توسعه و حفاظت از شبکه ملی داده با هماهنگی و همکاری بین مرکز ملی داده و اداره ملی امنیت سایبری و هماهنگی با طرف‌هایی که اطلاعات را در خارج از عراق نگهداری می‌کنند.	T-03
	ایجاد کمیته فنی مشترک دائمی در سازمان ملی امنیت سایبری برای هماهنگی، آماده‌سازی و پیگیری اجرای کلیه مراحل فنی برای حفاظت از فضای سایبری عراق	T-04
	ایجاد مرکز امنیتی فناوری‌های نوین در اداره ملی امنیت سایبری، مسئول پیگیری به‌روزرسانی‌های فناوری، پیشنهاد نوآوری‌های محلی لازم برای رفع نیازهای بومی و بررسی و تأیید دستگاه‌ها، سامانه‌ها و برنامه‌های کاربردی برای اپراتورهای زیرساخت‌های حیاتی کشور با هماهنگی مقامات ذی‌ربط	T-05
	ایجاد مرکز صنایع سایبری در شرکت السلام در وزارت ارتباطات با همکاری و تشویق اداره ملی امنیت سایبری برای تولید و توسعه فناوری‌ها، دستگاه‌ها، برنامه‌های کاربردی و خدمات الکترونیک ایمن محلی و کاهش وابستگی خارج از کشور	T-06
	ایجاد واحد فناوری سایبری مرتبط با سازمان صنعتی نظامی و مسئول ساخت و توسعه فناوری‌ها، دستگاه‌ها، برنامه‌های کاربردی و خدمات الکترونیک دفاعی برای رفع نیازهای نیروهای مسلح عراق	T-07
	ایجاد مرکز پیگیری و برنامه‌ریزی در اداره ملی امنیت سایبری برای نظارت بر رعایت تصمیمات شورا و ارائه گزارش و ارزیابی دوره‌ای از وضعیت امنیت سایبری کشور به صورت جامع	T-08



شکل شماره۱: مدل مفهومی تحقیق

روش تحقیق

روش تحقیق، توصیفی تحلیلی و از لحاظ نحوه گردآوری داده‌ها، از نوع پژوهش آمیخته (کیفی و کمی) است. تحقیق حاضر بر اساس مطالعه ادبیات و مبانی نظری در حوزه مورد تحلیل وضعیت موجود، مهم‌ترین موانع و چالش‌های امنیت سایبری عراق از طریق مراجعه به اسناد بالادستی پس از سال ۲۰۰۳ و در نهایت ارائه ساختار امنیت سایبری عراق جهت تحقق اهداف اصلی، اقدام شده است. بر این اساس نوع تحقیق کاربردی و توسعه‌ای است. همچنین از دو روش کتابخانه‌ای و روش میدانی (پیمایشی) برای گردآوری اطلاعات استفاده شده است.

جامعه آماری، حجم نمونه و روش نمونه‌گیری

جامعه آماری شامل مسئولان، کارشناسان و خبرگان حوزه امنیت سایبری کشور عراق، در پنج سطح (امنیتی/نظامی، مدنی/خدماتی، خصوصی/سازمانی، دیپلماسی و آموزشی/دانشگاهی) است. جامعه آماری بر اساس برخورداری از ویژگی‌های ذیل انتخاب شده‌اند:

- برخورداری از دانش و تجربه کافی در مسائل امنیتی و فضای مجازی
- برخورداری از دانش و تجربه کافی در مدیریت و سازمان
- برخورداری از دانش و توانایی تحلیل شکاف‌ها و تهدیدات در فضای مجازی
- برخورداری از حداقل ۵ سال سابقه کار امنیت و مدیریت سایبری و سابقه سیاست‌گذاری و تصمیم‌گیری.

بنابراین با بررسی اولیه به‌عمل‌آمده، تعداد افراد خبره در دانشگاه‌ها، مراکز علمی، دستگاه‌های کشوری و لشگری به میزان ۵۱ نفر برآورد شده است. روش نمونه‌گیری خبره با توجه به محدود بودن آن، جامعه آماری به‌صورت تمام شمار است. با توجه به محدود بودن حجم جامعه نمونه برای داده‌های کمی، روش نمونه‌گیری هدفمند و تمام شمار است.

جدول (۵): حجم جامعه آماری

ردیف	عنوان جامعه	حجم
۱	مسئولین امنیتی یا نظامی	۱۷
۲	مسئولین و صاحب‌نظران حوزه مدنی یا خدماتی	۱۶
۳	مسئولین آموزشگاهی یا اساتید دانشگاهی	۸
۴	صاحب‌نظران دستگاه‌ها و سازمان‌های خصوصی	۴
۵	مسئولین دیپلماسی	۶
	جمع	۵۱

روایی و پایایی پرسشنامه

برای انجام این تحقیق و در راستای دستیابی به اهداف پژوهش، یک پرسشنامه طراحی و از طیف لیکرت برای سنجش گویه‌های پرسشنامه بهره‌برداری گردیده است. پرسشنامه طراحی شد که روایی و پایایی آن‌ها به شرح زیر است. پرسشنامه، شامل گویه‌های مرتبط با «اهداف اساسی ساختار حاکمیتی امنیت سایبری عراق»، «مهم‌ترین موانع و چالش‌های امنیت سایبری عراق» و «ویژگی‌های ساختار حاکمیتی امنیت سایبری عراق» تهیه و برای تائید گویه‌های مستخرج، پرسشنامه طراحی، روایی و پایایی آن به شرح زیر است:

روایی صوری: با توجه به تخصصی بودن موضوع تحقیق و محدودیت وجود افراد خبره مرتبط با موضوع و حوزه‌ی مورد مطالعه در حوزه نظامی و امنیتی، دستگاه‌های کشوری و مراکز دانشگاهی بودن جامعه‌ی آماری و طراحی و توزیع سؤالات پرسشنامه‌ای بر اساس مشورت و اجماع نظرات اساتید راهنما، مشاور و برخی از افراد صاحب‌نظر و خبره مرتبط با موضوع، تنظیم که می‌توان با درصد اطمینان بالایی نتیجه‌گیری کرد که سؤالات پرسش‌نامه‌های این پژوهش به‌نحو مطلوب و قابل قبولی، اطلاعات علمی مورد نیاز این تحقیق را جمع‌آوری کرده، بنابراین پرسش‌نامه مزبور از روایی[1] صوری با اعتبار بالایی برخوردار است.

پایایی: برای محاسبه پایایی یا هماهنگی درونی ابزار اندازه‌گیری از ضریب آلفای کرونباخ استفاده شد؛ به‌طورکلی مقدار آلفای کمتر از ۶,۰ غیرقابل‌قبول، آلفای ۷,۰ تا ۸,۰ خوب، ۸,۰ تا ۹,۰ خیلی خوب و آلفای بالاتر از ۹,۰ بیانگر پایایی عالی ابزار سنجش است.

جدول (۶): مقدار ضریب پایایی محاسبه شده

Cronbach's Alpha	N of Items
۰/۹	۹٤

با توجه به اینکه مقدار آلفای کرونباخ جدول بالا، بیشتر از ۰,۷ محاسبه شده، بنابراین پرسشنامه از پایایی مناسبی برخوردار است.

یافته‌ها و تجزیه‌وتحلیل داده‌ها

برای پاسخ به سؤالات تحقیق از پژوهش جهت تجزیه‌وتحلیل داده‌ها از آزمون تی-تست و همچنین از روش مدل‌سازی معادلات ساختاری و از نرم‌افزار اسمارت پی ال اس استفاده شده است. تحلیل مدل‌ها در روش مدل‌سازی معادلات ساختاری با رویکرد حداقل مربعات جزئی طی،

1. Validity

برازش مدل در سه بخش ذیل انجام شده است: الف- برازش مدل اندازه‌گیری ب- برازش مدل ساختاری و پ- برازش مدل کلی.

برای بررسی برازش مدل اندازه‌گیری از سه معیار پایایی (سنجش بارهای عاملی، آلفای کرونباخ و پایایی ترکیبی) و همچنین روایی همگرا و روایی واگرا استفاده شده است.

به‌منظور برازش مدل ساختاری از معیارهای: «ضرایب معناداری Z» و «مقدار Q Square» بهره‌گیری شده است. برای برازش مدل کلی از معیار GoF استفاده شده است.

تجزیه و تحلیل و نتایج آزمون سوالات تحقیق

۱. اهداف اساسی ساختار حاکمیتی امنیت سایبری عراق کدامند؟

با استناد به ادبیات تحقیق، اهداف اساسی ساختار حاکمیتی امنیت سایبری عراق، از طریق مطالعات کتابخانه‌ای احصاء و سپس در اختیار تعداد ۵۱ نفر از خبرگان قرار گرفت که تجزیه‌وتحلیل داده‌های گردآوری شده و برابر نظر خبرگان، مطابق با آزمون تی- تست به شرح زیر تعیین شده است.

جدول (۷): اهداف اساسی ساختار حاکمیتی امنیت سایبری عراق

محورها اهداف	شماره گویه	کد اهداف	میانگین	مقدار آزمون تی	درجه آزادی	سطح معناداری
یکپارچه‌سازی	۱	GI-01	۴.۷۸	۲۰.۹	۵۰	۰.۰۰
	۲	GI-02	۴.۶۷	۲۳.۰	۵۰	۰.۰۰
	۳	GI-03	۴.۷۳	۲۵.۰	۵۰	۰.۰۰
هماهنگی	۴	GC-01	۴.۴۹	۱۳.۶	۵۰	۰.۰۰
	۵	GC-02	۴.۶۵	۱۶.۴	۵۰	۰.۰۰
	۶	GC-03	۴.۳۹	۱۲.۰	۵۰	۰.۰۰
	۷	GC-04	۴.۵۳	۱۶.۲	۵۰	۰.۰۰

محورها اهداف	شماره گویه	کد اهداف	میانگین	مقدار آزمون تی	درجه آزادی	سطح معناداری
	۸	GC-05	۴.۵۳	۱۵.۵	۵۰	۰.۰۰
دفاع و انعطاف‌پذیری	۹	GD-01	۴.۵۹	۱۷.۰	۵۰	۰.۰۰
	۱۰	GD-02	۴.۵۵	۱۶.۴	۵۰	۰.۰۰
	۱۱	GD-03	۴.۶۷	۱۹.۱	۵۰	۰.۰۰
	۱۲	GD-04	۴.۳۷	۱۲.۷	۵۰	۰.۰۰
	۱۳	GD-05	۴.۳۹	۱۲.۰	۵۰	۰.۰۰
ساخت و توسعه	۱۴	GB-01	۴.۶۹	۲۳.۶	۵۰	۰.۰۰
	۱۵	GB-02	۴.۶۷	۱۶.۷	۵۰	۰.۰۰
	۱۶	GB-03	۴.۶۳	۱۸.۴	۵۰	۰.۰۰
	۱۷	GB-04	۴.۶۵	۱۵.۸	۵۰	۰.۰۰
	۱۸	GB-05	۴.۳۷	۱۱.۹	۵۰	۰.۰۰
	۱۹	GB-06	۴.۵۳	۱۳.۹	۵۰	۰.۰۰
	۲۰	GB-07	۴.۴۳	۱۴.۰	۵۰	۰.۰۰
همکاری	۲۱	GC-01	۴.۶۳	۲۰.۶	۵۰	۰.۰۰
	۲۲	GC-01	۴.۵۳	۱۸.۹	۵۰	۰.۰۰

محورها اهداف	شماره گویه	کد اهداف	میانگین	مقدار آزمون تی	درجه آزادی	سطح معناداری
	۲۳	GC-01	۴.۴۱	۱۵.۱	۵۰	۰.۰۰

۲. مهم‌ترین موانع و چالش‌های امنیت سایبری عراق کدامند؟

با استناد به ادبیات تحقیق، مهم‌ترین موانع و چالش‌های امنیت سایبری عراق، از طریق مطالعات کتابخانه‌ای احصاء و سپس در اختیار تعداد ۵۱ نفر از خبرگان قرار گرفت که تجزیه‌وتحلیل داده‌های گردآوری شده و برابر نظر خبرگان، مطابق با آزمون تی- تست به شرح زیر تعیین شده است.

جدول(۸): مهم‌ترین موانع و چالش‌های امنیت سایبری عراق

بعد	شماره گویه	کد موانع	میانگین	مقدار آزمون تی	درجه آزادی	سطح معناداری
قانونی	۱	CL-01	۴.۱۰	۶.۹۰	۵۰	۰.۰۰۰
	۲	CL-02	۳.۹۲	۶.۶۰	۵۰	۰.۰۰۰
	۳	CL-03	۴.۱۴	۹.۵۷	۵۰	۰.۰۰۰
	۴	CL-04	۳.۵۵	۳.۵۶	۵۰	۰.۰۰۱
سازمانی	۵	CO-01	۳.۹۲	۵.۰۳	۵۰	۰.۰۰۰
	۶	CO-02	۴.۵۵	۱۵.۷۶	۵۰	۰.۰۰۰
	۷	CO-03	۴.۳۶	۱۲.۸۳	۴۹	۰.۰۰۰
	۸	CO-04	۴.۱۶	۹.۹۱	۵۰	۰.۰۰۰
	۹	CO-05	۴.۳۱	۱۱.۵۵	۵۰	۰.۰۰۰

بعد	شماره گویه	کد موانع	میانگین	مقدار آزمون تی	درجه آزادی	سطح معناداری
	۱۰	CO-06	۴.۰۰	۷.۶۱	۵۰	۰.۰۰۰
	۱۱	CO-07	۴.۱۰	۷.۱۳	۵۰	۰.۰۰۰
	۱۲	CO-08	۴.۳۷	۱۳.۶۱	۵۰	۰.۰۰۰
فنی	۱۳	CT-01	۴.۲۹	۱۱.۴۵	۵۰	۰.۰۰۰
	۱۴	CT-02	۴.۳۱	۱۱.۹۲	۵۰	۰.۰۰۰
	۱۵	CT-03	۴.۵۷	۱۸.۴۱	۵۰	۰.۰۰۰
	۱۶	CT-04	۴.۲۵	۱۱.۶۳	۵۰	۰.۰۰۰
	۱۷	CT-05	۴.۱۶	۷.۷۶	۵۰	۰.۰۰۰
توسعه و ظرفیت‌سازی	۱۸	CD-01	۴.۲۹	۹.۷۹	۵۰	۰.۰۰۰
	۱۹	CD-02	۴.۱۲	۸.۲۱	۵۰	۰.۰۰۰
	۲۰	CD-03	۴.۱۸	۹.۲۳	۵۰	۰.۰۰۰
	۲۱	CD-04	۴.۶۷	۲۱.۴۹	۵۰	۰.۰۰۰
	۲۲	CD-05	۴.۶۱	۲۱.۵۸	۵۰	۰.۰۰۰
	۲۳	CD-06	۴.۶۵	۱۹.۸۰	۵۰	۰.۰۰۰
	۲۴	CD-07	۴.۵۳	۱۶.۹۷	۵۰	۰.۰۰۰

بعد	شماره گویه	کد موانع	میانگین	مقدار آزمون تی	درجه آزادی	سطح معناداری
	۲۵	CD-08	۴.۵۷	۱۹.۴۹	۵۰	۰.۰۰۰
	۲۶	CD-09	۴.۳۱	۱۰.۹۱	۵۰	۰.۰۰۰
	۲۷	CD-10	۴.۳۹	۱۲.۰۳	۵۰	۰.۰۰۰
همکاری	۲۸	CC-01	۴.۳۳	۱۲.۰۳	۵۰	۰.۰۰۰
	۲۹	CC-02	۴.۴۵	۱۶.۱۳	۵۰	۰.۰۰۰
	۳۰	CC-03	۴.۲۹	۱۳.۱۸	۵۰	۰.۰۰۰
	۳۱	CC-04	۴.۲۰	۱۲.۳۲	۵۰	۰.۰۰۰
	۲۱	CC-05	۴.۰۶	۷.۹۹	۵۰	۰.۰۰۰

جدول‌های (۷ و ۸) بالا بیانگر آن است که برابر نظر خبرگان، اهداف اساسی ساختار حاکمیتی امنیت سایبری عراق و مهم‌ترین موانع و چالش‌های امنیت سایبری عراق به دلیل اینکه مقدار آزمون تی تمامی گویه‌های بالا بوده یعنی بیشتر از ۱.۹۶ و سطح معناداری همه گویه‌ها، کمتر از ۰.۰۵ محاسبه شده است؛ بنابراین کلیه گویه‌های مرتبط با اهداف اساسی ساختار حاکمیتی امنیت سایبری عراق و مهم‌ترین موانع و چالش‌های امنیت سایبری عراق با ضریب اطمینان ۹۵٪ و خطای ۵٪ نقش‌آفرین و معنادار است.

۳. حوزه‌های ساختار حاکمیت امنیت سایبری عراق کدامند؟

با استناد به ادبیات تحقیق، حوزه‌های ساختار حاکمیت امنیت سایبری عراق، از طریق مطالعات کتابخانه‌ای احصاء و سپس در اختیار تعداد ۵۱ نفر از خبرگان قرار گرفت که تجزیه‌وتحلیل داده‌های گردآوری شده و برابر نظر خبرگان، با استفاده از نرم افزار اسمارت پی ال اس، به شرح زیر تعیین گردیده است.

جدول ۹: حوزه‌های ساختار حاکمیت امنیت سایبری

ردیف	حوزه	ضریب همبستگی	T- TEST		تفسیر
			Tvalue	Pvalue	
۱	توسعه و ظرفیت‌سازی	0.371	8.439	0.000	نشان دهنده رابطه مثبت و معنادار بین حوزه «توسعه و ظرفیت‌سازی» و «ساختار حاکمیت امنیت سایبری عراق» است.
۲	سازمانی	0.398	11.584	0.000	نشان دهنده رابطه مثبت و معنادار بین حوزه «سازمانی» و «ساختار حاکمیت امنیت سایبری عراق» است.
۳	فنی	0.234	9.903	0.000	نشان دهنده رابطه مثبت و معنادار بین حوزه «فنی» و «ساختار حاکمیت امنیت سایبری عراق» است.
۴	قانونی	0.073	5.850	0.000	نشان دهنده رابطه مثبت و معنادار بین حوزه «قانونی» و «ساختار حاکمیت امنیت سایبری عراق» است.
۵	همکاری	0.131	8.064	0.000	نشان دهنده رابطه مثبت و معنادار بین حوزه «همکاری» و «ساختار حاکمیت امنیت سایبری عراق» است.

با استناد به ادبیات تحقیق، اقدامات و راهکارهای ساختاری لازم برای رفع یا رهایی از موانع و چالش‌های امنیت سایبری عراق (بازیگران ساختار حاکمیتی امنیت سایبری عراق، وظایف و مأموریت آن‌ها، هماهنگی و همکاری بین آن‌ها) از طریق مطالعات کتابخانه‌ای احصاء و سپس در

اختیار تعداد ۵۱ نفر از خبرگان قرار گرفت که تجزیه‌وتحلیل داده‌های گردآوری شده و برابر نظر خبرگان، با استفاده از نرم افزار اسمارت پی ال اس، به شرح ذیل تعیین شده است.

جدول ۱۰: سنجش‌های اقدامات و راهکارهای ساختاری لازم برای رفع یا رهایی از موانع و چالش‌های امنیت سایبری عراق

ردیف	حوزه	ضریب مسیر	کد اقدامات	بار عاملی	T- TEST	
					T- value	P- value
۱	همکاری	0.131	C-01	0.690	7.219	0.000
			C-02	0.778	10.682	0.000
			C-03	0.824	13.236	0.000
			C-04	0.814	18.036	0.000
۲	توسعه و ظرفیت‌سازی	0.371	D-01	0.743	6.352	0.000
			D-02	0.862	10.676	0.000
			D-03	0.793	6.619	0.000
			D-04	0.673	5.237	0.000
			D-05	0.773	7.530	0.000
			D-06	0.859	10.735	0.000
			D-07	0.853	11.202	0.000
			D-08	0.897	23.172	0.000
			D-09	0.856	10.010	0.000
			D-10	0.850	12.993	0.000
۳	قانونی	0.073	L-01	0.910	17.735	0.000
			L-02	0.911	22.893	0.000
۴	سازمانی	0.398	O-01	0.817	13.374	0.000

ردیف	حوزه	ضریب مسیر	کد اقدامات	بار عاملی	T- TEST	
					T- value	P- value
			O-02	0.795	8.564	0.000
			O-03	0.881	21.240	0.000
			O-04	0.895	20.082	0.000
			O-05	0.868	17.018	0.000
			O-06	0.737	6.046	0.000
			O-07	0.841	10.726	0.000
			O-08	0.825	13.656	0.000
			O-09	0.750	6.039	0.000
			O-10	0.806	10.439	0.000
۵	فنی	0.234	T-01	0.869	18.286	0.000
			T-02	0.778	10.757	0.000
			T-03	0.686	9.916	0.000
			T-04	0.618	5.991	0.000
			T-05	0.791	9.410	0.000
			T-06	0.683	6.597	0.000
			T-07	0.601	4.735	0.000
			T-08	0.725	9.449	0.000

جدول‌ها (۹ و۱۰) بالا بیانگر آن است که بین پنج حوزه احصاء شده «توسعه و ظرفیت‌سازی»، «سازمانی»، «فنی»، «قانونی» و «همکاری» زیرمؤلفه‌های حوزه‌ها و «ساختار حاکمیت امنیت سایبری عراق»، با توجه به مقادیر T- value که بیشتر از ۱.۹۶ و مقادیر P- value که کمتر از ۰.۰۵ محاسبه شده است؛ بنابراین یک ارتباط مثبت، مستقیم و معناداری بین متغیرهای تحقیق وجود

دارد؛ به‌طوری‌که با میزان تغییر این عوامل، «ساختار حاکمیت امنیت سایبری عراق»، به‌طور نسبی به همان مقدار تغییر خواهد یافت.

آزمون روایی همگرا

آزمون میانگین واریانس استخراجی

این آزمون یکی از آزمون‌های اصلی روایی همگرا است که همبستگی و همگرایی سوالات یک متغیر را در مدل بیرونی نشان می‌دهد. مطابق با نظر هنسلر ۲۰۰۹ باید مقدار تک‌تک ضرایب «پایایی ترکیبی» از «متوسط واریانس استخراج‌شده» متناظرشان بزرگ‌تر باشند.

جدول ۱۱: مقایسه پایایی ترکیبی و شاخص میانگین واریانس استخراجی

متغیر (حوزه‌ها)	پایایی ترکیبی	متوسط واریانس استخراج‌شده – AVE
توسعه و ظرفیت‌سازی	0.953	0.670
سازمانی	0.954	0.677
فنی	0.897	0.524
قانونی	0.906	0.829
همکاری	0.859	0.605

آزمون‌های مدل ساختاری

جهت برازش مدل ساختاری از دو معیار: ضرایب معناداری Z و مقادیر Q Square به شرح زیر بهره‌گیری شده است.

(۱) ضرایب معناداری Z

برازش مدل ساختاری با استفاده از ضرایب Z به این صورت است که ضرایب باید از ۱/۹۶ بیشتر باشند تا بتوان در سطح اطمینان ۹۵٪، معنادار بودن آنها را تأیید کرد (محسنین و همکار،۱۳۹۳: ۱۳۶). با توجه به جدول ۱۲ کلیه ضرایب (T) بیشتر از ۱/۹۶ هستند که این امر معنادار بودن روابط میان متغیرها را در سطح ۹۵٪ نشان می‌دهد.

(۲) معیار Q^2

معیار Q^2 قدرت پیش‌بینی مدل را مشخص می‌کند. این معیار که توسط استون و گیسر (۱۹۷۵) معرفی شد، قدرت پیش‌بینی مدل در سازه‌های درون‌زا را مشخص می‌کند. به اعتقاد آن‌ها مدل‌هایی که دارای برازش ساختاری قابل قبول هستند، باید قابلیّت پیش‌بینی متغیرهای درون‌زای مدل را داشته باشند؛ بدین معنی که اگر در یک مدل، روابط بین سازه‌ها به‌درستی تعریف شده باشند، سازه‌ها تاثیر کافی بر یکدیگر گذاشته و از این راه روابط بین سازه‌ها به‌درستی تائید می‌شود.

هنسلر و همکاران در مورد شدت قدرت پیش‌بینی مدل در مورد سازه‌های درون‌زا، سه مقدار ۰/۰۲، ۰/۱۵ و ۰/۳۵ را تعیین کرده‌اند که به ترتیب مقادیر ضعیف، متوسط و قوی، قدرت پیش‌بینی مدل در مورد سازه‌های درون‌زا را نشان می‌دهد (خالقی‌نژاد و همکار،۱۳۹۴).

جدول ۱۲: آزمون کیفیت مدل اندازه‌گیری

متغیر	Q^2	نتیجه
ساختار حاکمیتی امنیت سایبری عراق	0.381	قوی

آزمون مدل کلی

برازش مدل کلی (معیار GoF)

توسط این معیار، محقق می‌تواند پس از بررسی برازش بخش اندازه‌گیری و بخش ساختاری مدل کلی پژوهش خود، برازش بخش کلی را نیز کنترل کند. وتزلس و همکاران سه مقدار ۰/۰۱، ۰/۲۵ و ۰/۳۶ را به‌عنوان مقادیر ضعیف، متوسط و قوی برای GoF معرفی کرده‌اند. (داوری و همکاران، ۱۳۹۶: ۹۸).

معیار GoF طبق رابطه زیر محاسبه می‌شود:

$$GoF = \sqrt{\text{Communalities}} * \overline{R^2}$$

از آنجا که در حداقل مربعات جزئی مقدار Commonality با AVE برابر است وتزلس و همکاران (۲۰۰۹) فرمول زیر را ارائه کرده‌اند:

$$GOF = \sqrt{\text{average (AVE)}} \times \text{average } (R^2)$$

جدول ۱۳: مقادیر AVE و R Square

متغیر درون‌زا	R^2	متوسط واریانس استخراج‌شده AVE
ساختار حاکمیتی امنیت سایبری عراق	۱.۰۰	۰.۴۳۵

(مقدار R^2 مطابق جدول ... مقداری برابر با عدد ۱.۰۰ محاسبه شده است)

در نتیجه مقدار معیار GoF برابر است با:

$$GoF = \sqrt{۰/۴۳۵ * ۰/۱۰۰۰} = ۰/۶۵۹$$

حاصل شدن مقدار ۰/۶۵۹ برای GoF نشان از «برازش کلی بسیار قوی» مدل دارد.

برابر موارد مطروحه بالا الگوی ساختار حاکمیتی امنیت سایبری عراق، برابر نمودار (۲) به شرح ارائه می‌شود.

نمودار (۲): ساختار حاکمیت امنیت سایبری عراق (ماخذ: یافته‌های محقق)

نتیجه‌گیری و پیشنهادات

عراق همانند سایر کشورها، باوجود تهدیدها و مخاطراتی که توسعه سایبری و اتکای فزاینده به فناوری اطلاعات و ارتباطات را به همراه دارد، در تلاش است تا از تمامی مزایای فضای مجازی استفاده کند؛ بر این اساس ضرورت طراحی ساختاری برای امنیت سایبری در سطح ملی عراق احساس شده است. جمع‌بندی یافته‌های پژوهش نشان می‌دهد پنج حوزه «ساختار حاکمیتی امنیت سایبری عراق»، شامل: «همکاری» با ۴ زیرمؤلفه وضریب مسیر ۰.۱۳۱ ، «توسعه و ظرفیت‌سازی» با ۱۰ زیرمؤلفه و ضریب مسیر ۰.۳۷۱، «قانونی» با ۲ زیرمؤلفه و ضریب مسیر ۰,۰۷۳ ، «سازمانی» با ۱۰ زیرمؤلفه و ضریب مسیر ۰.۳۹۸، و «فنی» با ۸ زیرمؤلفه و ضریب مسیر ۰.۲۳۴، به‌صورت مکمل بر ساختار تأثیرگذار هستند وبا ساختار همبستگی مستقیم و مثبت وجود دارد؛ برازش مدل نیز قوی ارزیابی شد. بر اساس نتایج حاصل از تجزیه‌وتحلیل داده‌ها و یافته‌های تحقیق، موارد زیر پیشنهاد می‌گردد:

- تسریع در تشکیل شورای عالی امنیت سایبری به عنوان یک نهاد مرکزی که مسئول تصویب، تشکیل و تقسیم وظایف بین بازیگران لازم برای تأمین و تحکیم و تقویت حکمرانی و اعمال حاکمیت و اقتدار ملی بر تمامی ابعاد و لایه‌های فضای مجازی کشور، است؛
- تشکیل اداره ملی امنیت سایبری به عنوان یک نهاد تخصصی برای تدوین تصمیمات، سیاست‌ها و قوانین به صورت یکپارچه و منطبق با وضعیت امنیت سایبری عراق و پیگیری و نظارت بر اجرای تصمیمات شورای عالی امنیت سایبری؛
- فعال سازی راهبرد امنیت سایبری عراق به‌گونه‌ای که با راهبرد امنیت ملی عراق ادغام شود و از مصونیت زیرساخت‌ها و افزایش حفاظت از منافع ملی در برابر تهدیدات دشمنان در فضای سایبری اطمینان حاصل شود؛
- تسریع در تصویب قوانین معلق در پارلمان عراق مانند قانون جرایم اطلاعاتی، قانون اطلاعات شخصی و قانون امنیت ارتباطات و اطلاعات، به‌گونه‌ای که مغایر با قوانین جاری عراق و قوانین بین‌المللی نباشد و تضمین‌کننده آزادی‌ها و عدم نقض حریم خصوصی و آزادی دسترسی به اطلاعات بر اساس قانون اساسی عراق باشد؛
- تدوین و به‌روزرسانی سیاست‌ها، سازوکارهای حکمرانی، استانداردها، کنترل‌ها و دستورالعمل‌های لازم برای ارتقای امنیت سایبری، آماده‌سازی سازوکارهایی برای نظارت و تجزیه

و تحلیل خطرات و تهدیدات سایبری به‌شیوه‌ای فعال، تعیین نحوه پاسخگویی و بازیابی از آن‌ها و ارسال آنها به مقامات ذیربط و پیگیری رعایت آنها؛

– تکمیل به‌روزرسانی و ایمن‌سازی شبکه ملی اطلاعات و زیرساخت مطابق با توسعه فناوری‌های فضای مجازی برای اطمینان از محرمانه بودن، یکپارچکی، دسترسی به داده‌ها، اعمال حکمرانی و حفاظت از داده‌های ملی در برابر دستکاری‌های غیرمجاز؛

– تدوین برنامه‌هایی برای جذب شایستگی‌ها و تخصص‌ها در حوزه امنیت سایبری و حفظ آنها؛

– تخصیص منابع کافی برای مقابله با چالش‌ها و تهدیدات امنیت سایبری؛

– توسعه برنامه‌هایی برای حمایت از صنایع، سرمایه‌گذاری‌ها و نوآوری‌های محلی برای رفع نیازهای محلی و کاهش وابستگی به کشورهای خارجی؛

– توسعه توانمندی‌های ملی برای بازدارندگی سایبری و ایجاد فرماندهی عملیات سایبری مرتبط با فرماندهی عملیات مشترک به‌عنوان یک نهاد مسئول دفاع از منافع ملی و حاکمیت عراق در فضای سایبری و حفاظت و دفاع از شبکه‌ها و سامانه‌ها و داده‌های الکترونیکی نظامی؛

– افزایش آگاهی عمومی از خطرات و تهدیدات امنیت سایبری و ارتقا و حمایت از توانمندی‌های محلی (فنی، سازمانی و انسانی) از طریق تهیه برنامه‌های درسی، برنامه‌ها و ابتکارات آموزشی و دانشگاهی، سازماندهی رویدادهای مرتبط با امنیت سایبری و تشویق و هدایت نوآوری‌ها و تحقیقات علمی در حوزه امنیت سایبری؛

– تلاش برای تشویق، تولید و انتشار محتوای محلی که با فرهنگ، آداب و رسوم و سنت‌های جامعه عراق سازگار است. نیز تنظیم کنترل‌هایی برای محافظت از کودکان در برابر محتوای مضر در اینترنت؛

– تشویق ایجاد دانشکده‌ها و موسسات تخصصی در حوزه امنیت سایبری برای رفع نیازهای محلی؛

– ایجاد سازوکارهای لازم برای همکاری و مشارکت مؤثر بین نهادهای دولتی، بخش‌های دولتی و خصوصی، ذینفعان و نهادهای بین‌المللی و بین دولت مرکزی و دولت منطقه‌ای کردستان، برای اطمینان از سطوح بالای هماهنگی و به اشتراک‌گذاری اطلاعات مربوط به حملات و تهدیدات سایبری؛

- ارتقای سطح امنیت سایبری عراق و مشارکت قوی در فعالیت‌های بین‌المللی برای تضمین حق برابری عراق در حکمرانی فضای سایبری بین‌المللی.

فهرست منابع ومآخذ

الف. منابع فارسی

- احمد سلمان داود و رفاه شهاب الحمدانی (۲۰۲۰). استراتیجیهٔ الامن السیبرانی ودوره فی تحقیق الامن الوطنی العراقی بعد عام ۲۰۱۰. ***رسالهٔ ماجستیر***، العراق: جامعهٔ الدفاع للدراسات العسکریهٔ، کلیهٔ الدفاع الوطنی، دورهٔ (۲۳).
- راهبرد امنیت سایبری (استراتیجیهٔ الامن السیبرانی). (۱۶ شباط، ۲۰۲۲)، **استراتیجیهٔ الامن السیبرانی العراقی**، ۲۰۲۲–۲۰۲۵
- خالقی‌نژاد، عباس و ضیاءالدینی، محمد (۱۳۹۴). بررسی رابطه جو ایمنی و عملکرد ایمنی کارکنان با توجه به نقش میاجی دانش ایمنی و انگیزش ایمنی در مجتمع مس سرچشمه، ***فصلنامه بهداشت و ایمنی کار***، ۵ (۴)، ۸۴–۶۹.
- سلطانی، ن (۱۳۹۶). به سوی کنوانسیون سایبری، جریان شناسی هنجارها و پایش روندها (جلد ۱). ***بررسی محیط بین‌الملل***، انتشارات سپند قلم.
- طلال یاسین، العیسی (۲۰۱۰). السیادهٔ بین مفهومها التقلیدی والمعاصر دراسهٔ فی مدی تدویل السیادهٔ فی العصرالحاضر. ***مجلهٔ جامعهٔ دمشق للعلوم الإقتصادیهٔ والقانونیهٔ***، ۲۶.
- عباس بدران (۲۰۱۰). الحرب الإلکترونیهٔ: الاشتباک فی عالم المعلومات. مرکز دراسات الحکومهٔ الإلکترونیهٔ: https://najishukri.wordpress.com/11/2011//cyberwarbook
- کمیته دائمی شواری عالی فضای مجازی جمهوریه إسلامیه ایران (۱۳۹۴). سند راهبردی پدافند سایبری کشور.
- لدغش رحیمهٔ و بن عمار محمد (۲۰۱۴). سیادهٔ الدولهٔ وحق‌ها فی مباشرهٔ التمثیل الدبلوماسی، ***اطروحهٔ دکتوراه***. جزائر، تلمسان: جامعـهٔ أبی بکر بلقاید. http://dspace.univ-tlemcen.dz/bitstream/۱/۷۲۲۸/۱۱۲/ledermecherahima.pdf
- شکر ، عمر حامد (۲۰۱۹). المجال الخامس ـ الفضاء الإلکترونی. المعهد المصری للدراسات، إسطنبول
- شورای امنیت ملی (مجلس الامن الوطنی) (۲۰۱۶). استراتیجیهٔ الامن الوطنی العراقی.
- حافظ نیا، محمدرضا (۱۳۹۳)، جغرافیای سیاسی فضای مجازی. تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاهها (سمت).
- محسنین، شهریار و اسفیدانی، محمدرحیم (۱۳۹۳). معادلات ساختاری مبتنی‌بر رویکرد حداقل مربعات جزیی. تهران: انتشارات موسسه کتاب مهربان
- قادری حاجت، مصطفی و نصرتی، حمیدرضا (۱۳۹۲). فضای سایبر؛ چالش‌های حاکمیت و امنیت پایدار. ***پژوهشنامه جغرافیای انتظامی***، شماره ۲.
- داوری، علی و رضازاده، آرش (۱۳۹۶). مدل سازی معادلات ساختاری با نرم افـزار PLS، تهـران: سـازمان انتشـارات جهاد دانشگاهی، چاپ چهارم.

ب. منابع انگلیسی

- Aima Muku Komila. (۲۰۱۷). Cyberspace and Crisis Management. USA ،CA ، San Jose State University: Springer International Publishing AG.

- Efe , A., & Bensghir , K. (۲۰۱۹). Cyber governance for cyber security. In: Cyber security and defense problems and solutions. ۳۲۵–۳۷۸. Graphic.
- Fang, B. (۲۰۱۸). Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace. Springer.
- Hatleback, E. (۲۰۱۸). The pro- toscience of cybersecurity , *Journal of Defense Modelling and Simulation: Applications, Methodology, Technology*. (Vol. ۱۵).
- ITU. (۲۰۱۰). ITU Toolkit for Cybercrime Legislation. ۱۲. Geneva. http://www.cyberdialogue.ca/wp-content/uploads/۰۳/۲۰۱۱/ITU-Toolkit-for-Cybercrime-Legislation.pdf
- Jones. John. (۱۹۹۲). Design Methods . New York: John Wiely & Sons .
- KARATAŞ , A. (۲۰۲۰). The Comparative Analysis Of National Cyber Security Policies: United States, United Kingdom And Turkey Examples. ۵, ۱۹, ۷۳۷-۷۵۱.
- Marinescu, D. (۲۰۱۷). Complex Systems. In Complex Systems and Clouds , A Self-Organization and Self-Management Perspective- Computer Science Reviews and Trends. (pp. ۱-۳۲). doi:https://doi.org/۱۰/۱۰۱۶/B۹۷۸-۰-۱۲-۸۰۴۰۴۱-۶/۰۰۰۰۱-۳
- Oxford Learner's Dictionaries. (n.d). Definition of structure noun from the Oxford Advanced America Dictionary. Oxford University Press: https://www.oxfordlearnersdictionaries.com/definition/english/structure_۱?q=structure
- Rolf H Weber. (۲۰۲۱). Internet Governance at the Point of No Return. the Swiss National Science Foundation (SNF). https://library.oapen.org/bitstream/id/bd۰۸۳۸۲a-cb۱f-۴۶۸d-bb۲f-a۶۱۹۸۰a۹۲۹a۹۷۸۳۰۳۸۰۵۳۹۲۷/۹.pdf
- Sean Kanuck. (۲۰۱۰). Sovereign Discourse on Cyber Conflict Under International Law. *Tex. Law Rev*. ۱۵۷۱ ،۸۸–.۱۵۹۸