فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره۳، تابستان ۱۴۰۱
مقاله پنجم، از صفحات ۱۲۱-۱۴۶

مقاله پژوهشی:

تدوین محورهای پیشنهادی سند راهبردی سایبری ج.ا.ایران به روش مطالعه تطبیقی

مصطفی سعیدی[۱] محسن آقایی[۲]

تاریخ دریافت: ۱۴۰۰/۰۴/۱۵ **تاریخ پذیرش:** ۱۴۰۰/۱۱/۱۶

چکیده

جایگاه و نقش برنامه‌های راهبردی در پیشرفت کشورها کاملاً آشکار است. بسیاری از کشورها علاوه بر حوزه‌های اقتصادی، نظامی و سیاسی در حوزه به‌کارگیری فناوری‌ها نیز برنامه‌های راهبردی طراحی کرده‌اند و مبنای تصمیم‌گیری‌ها، جهت‌گیری‌ها و هدایت خود قرار داده‌اند. مطالعه اسناد راهبردی تدوین شده به‌خصوص، موارد مدون‌شده در حوزه سایبر؛ روشی برای شناخت راه و تفکرات بر اساس اولویت‌ها و راه‌کارهایی است که نشان‌دهنده افکار و برنامه‌های جامع جوامع دیگر است. استفاده از تجربیات سایبری سایر کشورها در تولید اسناد راهبردی با تأکید بر کشورهایی که به‌عنوان صاحبان فناوری و دارای قدرت شناخته می‌شوند، نقش بسزایی در تولید سند راهبردی جامع و مانع دارد. در این مقاله با توجه به اهمیت تدوین محورهای مهم برای اسناد راهبردی کشور، اسناد سایبری بالادستی داخلی، اسناد راهبردی سایبری چند کشور توسعه‌یافته به روش مطالعه تطبیقی بررسی شده‌اند؛ درنتیجه هشت محور به‌عنوان محورهای حداقلی برای سند راهبردی کشور به‌عنوان درس‌آموخته‌های مطالعات این حوزه به‌عنوان خطوط راهنمای اولیه تعیین شدند.

کلیدواژه‌ها: سند راهبردی سایبری، سند راهبردی سایبری ملی، سند ملی امنیت سایبری

۱. دانشجوی مقطع دکتری دانشگاه عالی دفاع ملی و نویسندهٔ مسئول، mostafa.saeedi@chmail.ir
۲. استادیار و عضو هیئت علمی دانشگاه عالی دفاع ملی، Aghaee@sndu.ac.ir

مقدمه

جایگاه، نقش و اهمیت فضای سایبر در عصر حاضر بر کسی پوشیده نیست به‌طوری‌که اغلب کشورهای دنیا آن را به‌عنوان یکی از بازیگران مهم آینده کشورشان در نظر گرفته‌اند و برای آن برنامه‌ریزی می‌نمایند. حذف فضای سایبر از زندگی امروزی بشر، غیرممکن است و نداشتن برنامه مناسب برای مواجهه با آن خلاف مصلحت و عقل است (راهبرد سایبری ملی ایالات‌متحده، ۲۰۱۸). فرصت‌های شگرف در فضای سایبر، با موضوعات و چالش‌های جدیدی همچون آسیب‌پذیری و خطر بالقوه زیرساخت‌های اطلاعاتی همراه است (شاهیویی،[۱] ۲۰۱۷).

در دهه‌های گذشته سازمان‌های مختلف با رویکرد اقتصادی و تجاری برای همگرایی و هماهنگی درونی و به‌منظور غلبه بر مشکلات و ارتقاء آورده اقتصادی و سود بیشتر به تولید اسناد راهبردی روی آورده‌اند. اسناد راهبردی تولید شده، باعث آگاهی همه بخش‌های سازمان از آینده متصور برای سازمان در ابعاد دور و نزدیک می‌شود و عدم وجود چنین اسنادی بدون ترسیم دورنمای سازمان از دلایل شکست برخی شرکت‌ها و نهادهای مهم دنیا به شمار می‌آید؛ این اسناد بر اساس آرمان‌ها، چشم‌اندازها و آرزوهای هر کشوری تولید می‌شوند و مخصوص به کشور تولیدکننده آن‌ها است و تجربیات موفق آن می‌تواند برای سایر کشورها ازجمله کشور عزیزمان ایران، حداقل در بخش ساختاری مفید باشد.

پرواضح است که سند راهبردی سایبری، بایستی هم‌سو و همگام با سایر اسناد راهبردی بالادستی کشور باشد. نمی‌توان دورنمای کشور در حوزه سایبر را تنظیم کرد؛ ولی به دورنمای کلی نظام و انقلاب در ابعاد مختلف کاری نداشت؛ بنابراین با توجه به اینکه ایران در سند چشم‌انداز جمهوری اسلامی ایران در افق ۱۴۰۴، کشوری توسعه‌یافته با جایگاه اول اقتصادی، علمی و فناوری در سطح منطقه با هویت اسلامی و انقلابی، الهام‌بخش در جهان اسلام و با تعامل سازنده و مؤثر در روابط بین‌الملل ترسیم شده است (سند چشم‌انداز۱۴۰۴، ۱۳۸۲)، رسیدن به چنین جایگاهی در منطقه و جهان اسلام بدون در نظر گرفتن شرایط، چالش‌ها، فرصت‌ها و

۱ Shaohui

تهدیدهای فضای سایبر و مبهم بودنِ اولویت‌ها و نداشتنِ برنامه‌ریزی مدون و منسجم با استفاده از تمام ظرفیت‌های بالقوه و بالفعل در این فضا میسر نخواهد بود.

چندین سال است که تدوین اسناد گویای نیازمندی‌های فوق با عنوان اسناد راهبردی در کشورمان، مورد توجه مدیران سطوح راهبردی قرار گرفته است و به‌عنوان اسناد مهمی در نظر گرفته می‌شوند که حاوی ارکان جهت‌ساز، نقشه راه، راهبردهای کلان و برنامه‌های بلندمدت و میان‌مدت هستند؛ لذا با عنایت به اینکه در حوزه‌های مختلف ازجمله فضای سایبر، اسناد متعددی برای کشور تدوین شده است، به نظر می‌رسد ساختار سندهای تهیه‌شده نیازمند بازنگری و تدقیق باشد که بر این اساس پژوهش حاضر در خصوص تدوین ساختار اسناد سایبری هدف‌گذاری نموده است؛ بنابراین مسئله اصلی پژوهش این است که قالب مناسب سند راهبردی سایبری جمهوری اسلامی ایران چگونه باید باشد. اهمیت انجام این پژوهش از این نظر است که با ارائه و پیشنهاد ساختاری مناسب برای اسناد راهبردی سایبری می‌توان اقدام به افزایش تفکر ساختاریافته در مورد اسناد سایبری نمود و به ارتقاء آگاهی مدیران راهبردی کشور در مورد مفاد هر بخش از اسناد و درنتیجه به تدوین برنامه‌های منتج از راهبردهای چنین اسنادی اقدام نمود؛ همچنین ضرورت انجام این پژوهش از این بعد قابل توجه است که: توسعه خلأ بررسی علمی در مورد محورهای اصلی و همه‌جانبه ساختارهای اسناد راهبردی افزایش پیدا می‌کند و باعث عدم تعامل با مواردی همچون درک ساختاری اسناد مدون بین‌المللی در این حوزه و ایجاد مواضع انفعالی در این خصوص می‌شود.

نظر به موارد فوق هدف اصلی از انجام این پژوهش تعیین محورهای حداقلی سند راهبردی سایبری جمهوری اسلامی ایران و اهداف فرعی مرتبط عبارت‌اند از: تعیین محورهای بومی ساختار اسناد راهبردی سایبری کشور، نحوه نگاه آینده‌نگرانه نسبت به تدوین این‌گونه اسناد با در نظر داشتن ارزش‌های اسلامی، انقلابی، فرهنگ و تمدن اسلامی و ایرانی و نوع پاسخ‌گویی به نیازمندی سازمان‌ها به اسناد راهبردی سایبری. بر این اساس سؤال اصلی پژوهش چنین است که: محورهای حداقلی سند راهبردی سایبری جمهوری اسلامی ایران چه هستند و سؤالات فرعی عبارت‌اند از:

از بررسی منابع مرتبط و تطبیق اسناد راهبردی داخلی و خارجی مورداستفاده در این پژوهش این نتیجه حاصل می‌شود که اسناد راهبردی تولید شده در کشور علاوه بر همسویی و هم‌گرایی با دغدغه‌های جهانی، نیازمند پرداختن به محورهای بومی برای ج.ا.ا در قامت انقلاب اسلامی هستند. اسناد راهبردی سایبری تدوین‌شده چندساله اخیر کشور با بنابراین کشور عزیزمان ایران در حوزه سایبری نیازمند سند بومی است که قدرت پاسخ‌گویی به نیازهای کشور در حوزه‌های اختصاصی خودش را داشته باشد.

- محورهای مهم اسناد راهبردی تدوین‌شده در جمهوری اسلامی ایران چیست؟
- اولویت‌های راهبردی کشور ایالات‌متحده آمریکا در سند ملی راهبردی سایبری در سال ۲۰۱۸ (ابلاغ‌شده توسط کاخ سفید) چیست؟
- اولویت‌های راهبردی کشور جمهوری خلق چین در سند ملی امنیت سایبری در سال ۲۰۱۷ (منتشرشده توسط وزارت امور خارجه چین) چیست؟
- اولویت‌های راهبردی اتحادیه اروپا در سند راهبردی امنیت ملی سایبری در سال ۲۰۱۲ چیست؟

ادبیات تحقیق و مبانی نظری

نظر به اینکه ارائه محورهای اسناد راهبردی سایبری از اهمیت خاصی برخوردار است، ضرورت دارد در مورد بررسی اسناد مرتبط در قالب ادبیات مربوط به ساختار چنین اسنادی بررسی و تحلیل‌های لازم صورت گیرد. در این بخش ضمن بررسی اسناد راهبردی سایبری کشورهای اثرگذار و صاحب سبک در قالب پیشینه پژوهش به بررسی و مفهوم‌یابی در این خصوص پرداخته می‌شود و مفاهیم اساسی برگرفته از این اسناد در قالب مفاهیم ارائه می‌شوند.

پیشینه پژوهش

انتخاب کشورها برای مطالعه اسناد راهبردی باید بر اساس الگوی مشخصی انجام شود که در این خصوص پژوهشگران متعددی به این امر پرداخته‌اند که در ادامه به برخی از این پژوهش‌ها اشاره می‌شود.

- اسناد راهبردی سایبری متعددی در کشور طی چند سال اخیر، منتشر شده است؛ این

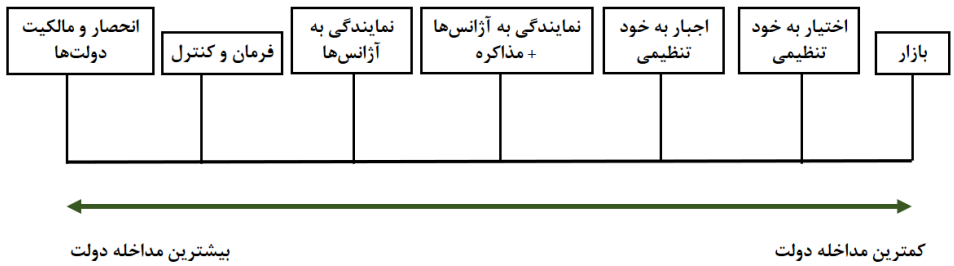
اسناد بر اساس رویکردهای متفاوت و بیشتر با کلیدواژه امنیت توسط نهادهای مختلفی در کشور منتشر شده است که در این مجال به بررسی برخی از آن‌ها خ‌واهیم پرداخت.

- مرکز ملی فضای مجازی: سند تبیین الزامات شبکه ملی اطلاعات، توسط مرکز ملی فضای مجازی ایجاد شده است و رویکرد اصلی این سند، معطوف به حوزه ارتباطات در بخش زیرساخت فضای سایبر است و سایر بخش‌های فضای سایبر در آن دیده نشده است (مرکز ملی فضای مجازی، ۹۵).
- سازمان پدافند غیرعامل: سند راهبردی پدافند سایبری کشور، توسط سازمان پدافند غیرعامل تولید شده است. رسالت قرارگاه پدافند سایبری کشور، مصون‌سازی و پایدارسازی سرمایه‌های سایبری کشور از طریق پایش و تشخیص تهدیدات، کشف، مدیریت و کنترل آسیب‌پذیری‌ها، اعلام هشدارهای لازم، امن‌سازی، تدوین و انتشار نظامات (ملاحظات، مقررات، الزامات و اصول) پدافندی، آموزش و نهادینه‌سازی پدافند سایبری، مدیریت صحنه پدافند سایبری و دفاع حقوقی در برابر تهدیدات و حملات دشمن است (سازمان پدافند غیرعامل کشور، ۹۴).
- مرکز راهبردی افتای ریاست جمهوری: سند راهبردی امنیت فضای تبادل اطلاعات کشور در سال ۹۴ در کشور منتشر شده است؛ این سند دارای ۵ هدف کلان و ۶ راهبرد است که بر روی فضای تبادل اطلاعات کشور تمرکز کرده است (مرکز راهبردی افتای ریاست جمهوری، ۹۴).
- وزارت ارتباطات و فناوری اطلاعات: اسناد نظام ملی فناوری اطلاعات و ارتباطات در سال ۸۶ و مدل مرجع امنیت در سال ۹۶، دو سند راهبردی است که توسط وزارت ارتباطات و فناوری اطلاعات تولید شده است. توجه اصلی در اسناد تولید شده، پایین‌ترین سطح فضای سایبر؛ یعنی بخش زیرساخت است.

- مقاله‌ای با عنوان «راهبردهای امنیت سایبری اتحادیه اروپا و ناتو و راهبردهای امنیت سایبری ملی: یک تحلیل مقایسه‌ای» در سال ۲۰۱۷ منتشر شده است. در این مقاله به روش مطالعه مقایسه‌ای، سیاست‌های امنیت سایبری سازمان‌های اتحادیه اروپا و ناتو بررسی شده است. تحلیلی در مورد چگونگی مطابقت راهبردهای امنیت سایبری ملی با

سیاست‌های امنیت سایبر و جهت‌های راهبردی این سازمان‌ها و ارائه راهبردهای امنیت سایبری ملی اتحادیه اروپا و ناتو انجام شده است؛ این پژوهش نشان می‌دهد که صرف نظر از اهداف مشابه؛ یعنی اطمینان از مقاومت در برابر سایبر، رویکردهای هماهنگ‌سازی و هماهنگی انتخاب شده و همچنین هنجارهای راهبردهای امنیت سایبری ملی متفاوت است (Štitilis, Pakutinskas, & Malinauskaitė, 2017). تفاوت‌های اصلی شامل تفاوت در اصول، مفاد همکاری، دفاع سایبری، پژوهش، استفاده از استانداردها، حمایت از حقوق بشر، عملکردها و شایستگی‌های بازیگران و ذی‌نفعان فضای سایبر است.

- از دیگر پژوهش‌های انجام شده، مقاله‌ای در مورد آنالیز تطبیقی راهبردهای ملی سایبری کشورهای مختلف در سال ۲۰۱۶ است. در این پژوهش نارمن شفقت و اشرف مسعود، راهبردهای امنیت ملی سایبری بیست کشور را براساس معیارهای قانونی، عملیاتی، فنی و سیاست، مقایسه کرده‌اند. نتیجه اینکه: آسیب‌پذیری‌های ذاتی و حملات سایبری، امنیت ملی، اقتصاد و زندگی روزمره شهروندان را به‌طور مداوم تهدید می‌کند. بیش از ۵۰ کشور در سراسر جهان، راهبردهای امنیتی سایبری خود را برای پرداختن به نگرانی‌های جدی امنیت سایبری ملی تدوین کرده‌اند(Shafqat & Masood, 2016) . روش عملکردی در این پژوهش، استخراج معیارهای مشخص و بررسی راهبرد کشورها در حوزه‌های استخراج شده است. کشورها به دو دسته زیر تقسیم شده‌اند:
  - توسعه‌یافته؛ شامل: ایالات متحده آمریکا، کانادا، استرالیا، نیوزلند، استونی، ژاپن، انگلستان، آلمان، اتریش، اسرائیل، هلند، فنلاند، فرانسه، اسپانیا، جمهوری چک
  - در حال توسعه؛ شامل: مالزی، عربستان سعودی، هند، ترکیه و ایران
- پژوهشی با عنوان «یک مطالعه تطبیقی بین‌المللی در راهبرد امنیت سایبری» در سال ۲۰۱۵ انجام شده است که رشد روزافزون فناوری اطلاعات و فضای سایبر را فرصت و استفاده از راهبرد سایبری کشورهای موفق در این زمینه را مفید می‌داند. اسناد راهبردی ایالات متحده آمریکا و کشورهای عضو اتحادیه اروپا و ژاپن بررسی شده‌اند (Min, Chai, & Han, 2015). بررسی این اسناد بر اساس محورهای طیف بیشترین و کمترین دخالت دولت‌ها است. در شکل (۱) محورها نشان داده شده است.



شکل ۱ : شاخصه‌های مقایسه‌ای اسناد راهبردی در (Min, Chai, & Han, 2015)

جمع‌بندی پیشینه‌های مرتبط با پژوهش و نوآوری پژوهش

بررسی‌ها نشان می‌دهد نوع نگاه و دغدغه ذهن پژوهشگران در نتیجه مطالعه تطبیقی اسناد راهبردی فضای سایبر بر ایجاد سند راهبردی سایبری بومی تأثیرگذار است. بررسی‌ها نشان می‌دهد که در اکثر قریب به اتفاق پژوهش‌ها، ابرقدرت بودن ایالات متحده آمریکا و پذیرش ارکان اسناد راهبردی این کشور، به‌عنوان شاخص ارزیابی اسناد راهبردی سایبری از سوی سایر کشورها در نظر گرفته شده است. مزیت پژوهش پیش‌رو نسبت به نمونه‌های مشابه، مقایسه اسناد راهبردی مدون کشورمان و دو کشور ایالات متحده آمریکا، جمهوری خلق چین و اتحادیه اروپا (با توجه به خصوصیات خاص آن‌ها) برای احصاء محورهای مهم سند راهبردی سایبری ج.ا.ایران است. به دلیل نوع رابطه کشورهای بیان شده با ج.ا.ایران، رویکردهای متضاد بایستی در دستور کار قرار گیرد که در سایر مطالعات تطبیقی چنین نبوده است.

مفاهیم

سند راهبردی

مدیریت راهبردی تجزیه و تحلیل مسایل مهم و برجسته سازمان است که توسط راهبران ارشد سازمان به نمایندگی از مالکان، به‌منظور کنترل منابع در محیط‌های خارج از سازمان انجام می‌شود.(Rajiv Nag Donald C. Hambrick Ming-Jer Chen, 2007) که این فرایند شامل مشخص‌کردن مأموریت، چشم‌انداز، دارایی‌های سازمان، توسعه برنامه‌ها و سیاست سازمان و همه فعالیت‌هایی است که برای نیل به اهداف نیاز است.

مدیریت راهبردی یک فرایند دایمی است. بررسی رقیبان و تنظیم اهداف و راهبردها برای ملاحظه همه رقیبان موجود و احتمالی و توصیف راهبردها به‌صورت سالانه یا فصلی و تعیین اینکه چگونه پیاده شوند در مدیریت راهبردی مشخص می‌شود (Lamb, Robert, Boyden, ۱۹۸۴).

بنابراین در این پژوهش سند راهبردی، سندی واقع‌گرایانه و مبتنی بر شناخت محیط داخلی و خارجی است که در آن با مشخص کردن مقصد نهایی، روش رسیدن از وضعیت کنونی به مقصد آرمانی بیان می‌گردد.

روش‌شناسی پژوهش

نظر به اینکه هدف اصلی محقق ارائه محورهای مهم اسناد راهبردی سایبری می‌باشد در بررسی‌های اولیه مشخص شد اسناد راهبردی تدوین‌شده داخلی، اسناد راهبردی ایالات متحده، جمهوری خلق چین و اتحادیه اروپا به‌دلیل جایگاه‌های فناورانه و جمعیتی می‌تواند برای این پژوهش مناسب باشد. نظر به نیازمندی مطالعه و تحلیل اسناد فوق؛ این پژوهش به روش کیفی انجام می‌شود و با توجه به هدف آن توسعه‌ای-کاربردی محسوب می‌شود؛ زیرا در جهت گسترش مفاهیم و ساختار اسناد راهبردی فضای سایبر در کشور در نظر گرفته شده است و از طرفی با هدف استفاده از ساختار پیشنهادی در سازمان‌های کشور می‌باشد. بر اساس بررسی‌های به‌عمل‌آمده و نیازمندی به کسب اطلاعات از اقدامات مشابه و اسناد موجود از روش مطالعه تطبیقی در این پژوهش استفاده خواهد شد. قراملکی (۱۳۹۵)، چنین بیان نموده است که یکی از روش‌های مطالعه اسناد مطالعه تطبیقی است، بدین‌معنی که چند سند انتخاب و بر محور موضوعات مهم برای پژوهشگر، سندها مطالعه می‌شوند (قراملکی، ۱۳۹۵). در این پژوهش محورهای مهم اسناد راهبردی سایبری مورد توجه قرار می‌گیرند و بر اساس آن‌ها، اسناد، تبیین می‌گردند.

✓ روش تحلیل یافته‌ها

روش پژوهش مورد استفاده از نوع آمیخته (کیفی و کمی) است. در بخش کیفی با مراجعه به اسناد راهبردی، مقالات، کتاب‌ها و گزارشات پژوهشی، با استفاده از روش تحلیل مضمون، مرور

ادبیات مرتبط و برگزاری جلسه گروه کانونی محورهای راهبردی مشخص شد. بر اساس محورهای اصلی استخراج شده، موارد مهم و مورد نظر محقق به‌عنوان محورهای راهبردی مهم در تدوین اسناد سایبری ملی برای جمهوری اسلامی ایران به‌عنوان محورهای حداقلی پیشنهاد شد و پس از ارزیابی با روش ضریب کاپا، محورهای نهایی مورد تأیید قرار گرفتند.

✓ **روش اعتبارسنجی**

جهت حفظ کیفیت مطالعه و اعتبارسنجی از شاخص کاپا در سنجش میزان اعتبار محورهای مورد نظر در مطالعه تطبیقی استفاده شده است. در این روش شخص دیگری از خبرگان حوزه مطالعه، بدون اطلاع از نحوه ادغام کُدها و مفاهیم توسط پژوهشگر، اقدام به طبقه‌بندی کُدها در مفاهیم نمود. مفاهیم ارائه‌شده توسط پژوهشگران با مفاهیم ارائه‌شده توسط این فرد مقایسه و در نهایت با توجه به تعداد مفاهیم ایجاد شده مشابه و متفاوت، شاخص کاپا محاسبه می‌شود.

✓ **معرفی روش مطالعه تطبیقی**

مطالعه تطبیقی مقایسه دو یا چند پدیده (موضوع یا مسئله) در دامنه مشخص و با تعیین محورهای بررسی در میان ابعاد مختلف آن پدیده، برای کشف نقاط اشتراک و اختلاف آن‌ها و رسیدن به هدف پژوهش است. در مطالعه تطبیقی بایستی هدف تطبیق، مسئله پژوهش و دامنه تطبیق مشخص گردد.

در مطالعات تطبیقی، صِرف مقایسه کردن هدف نیست؛ بلکه از کشف موارد تشابه و اختلاف باید به ملاک تشابه یا اختلاف رسیده شود و براساس آن مسئله‌ای حل شود. ارائه این چارچوب که بیان‌کننده محورهای سند راهبردی جمهوری اسلامی ایران است می‌تواند به‌عنوان چارچوب راهنما برای مدیران راهبردی فضای سایبر به‌منظور تدوین راهبرد استفاده شود. بر مطالعه تطبیقی، فرایند پژوهشی مرکب از پنج مرحله اساسی است.

۱. تدوین مسئله :

تدوین مسئله و مشخص کردن دغدغه پژوهشگر در مطالعه تطبیقی از اهمیت بالایی برخوردار است. اهداف و مسائل مختلفی می‌تواند در یک مطالعه تطبیقی، ذهن پژوهشگر را به خود مشغول کند و گستره‌ای از موضوعات (معمولاً غیرمرتبط) را پیش‌روی پژوهشگر قرار دهد.

انتخاب تعدادی از دغدغه‌های به هم مرتبط می‌تواند به غنای پژوهش کمک شایانی نماید. مسائل موجود در یک مطالعه تطبیقی به دو دسته تقسیم می‌شوند.

- مسائل درجه اول: مسئله مربوطه در مطالعه تطبیقی مورد بررسی قرار می‌گیرد.
- مسائل درجه دوم: مبنای فلسفی و علت موضوع مسئله مطالعه شده مورد بررسی قرار می‌گیرد.

۲. تعیین دامنه پژوهش

هر پژوهشی باید بر حسب توانایی فرد محقق و سایر عوامل مرتبط، محدود گردد. تحدید دامنه پژوهش در مطالعات تطبیقی اهمیت بیشتری دارد و انتخاب آن، گزینش راهبردی در فرایند پژوهش است؛

۳. فهرست کردن تمام تشابه‌ها و تمایزهایی که به نظر می‌رسند (بین مبانی، مسائل، فرضیه‌ها، لوازم، زمینه‌ها، تعریف‌ها، توصیف‌ها، روش‌ها، مراحل، فرایندها، ابزارها، مثال‌ها، نتایج، توصیه‌ها و ...)؛
۴. جداکردن تشابه‌ها و تمایزهای واقعی از موارد تشابه‌نما یا تمایزنما؛
۵. بررسی علت وجود مشابهت یا علت اختلاف (همان).

یافته‌ها و تجزیه‌وتحلیل داده‌ها

الف: یافته‌های پژوهش

در این پژوهش محورهای مهم اسناد راهبردی سایبری مورد توجه قرار می‌گیرند و بر اساس آن‌ها، اسناد تبیین می‌گردند. بر این اساس و به‌منظور تعیین اولویت‌های اسناد راهبردی سایبری تدوین‌شده در جمهوری اسلامی ایران، اسناد مورد هدف در این مقاله عبارتند از: سند ملی راهبردی سایبری سال ۲۰۱۸ ایالات متحده آمریکا به‌منظور استخراج اولویت‌های راهبردی، سند ملی امنیت سایبری سال ۲۰۱۷ جمهوری خلق چین برای تعیین اولویت‌های راهبردی آن و سند راهبردی امنیت ملی اتحادیه اروپا سال ۲۰۱۲ به‌منظور بررسی اولویت‌های راهبردی سایبری اتحادیه اروپا.

سند راهبردی ایالات متحده آمریکا ۲۰۱۸

ایالات متحده آمریکا با جمعیتی بالغ بر ۳۲۹،۰۹۳،۱۱۰ نفر، دارای تعداد ۸۶۸,۲۹۲,۸۹۲ کاربر در فضای سایبر است. ۸۹ درصد از مردم آمریکا از اینترت استفاده می‌نمایند که آمار بسیار بالا و قابل ملاحظه‌ای است (Internet World Stats, Usage Population Statics, 2019). توجه به این مورد، مبین مفید بودن مطالعه اسناد راهبردی این کشور است. طی چند سال گذشته، اسناد راهبردی متفاوتی در فضای سایبر، عمدتاً توسط وزارت دفاع، تولید شده است؛ ولی برای اولین‌بار سند راهبردی ۱۵ ساله ایالات متحده آمریکا در حوزه فضای سایبر، تحت عنوان «راهبرد ملی سایبری ایالات متحده آمریکا» در شهریور ۱۳۹۷ (سپتامبر، ۲۰۱۸) توسط کاخ سفید منتشر شد. (White House, September 2018)

این سند با جمله‌ای از رییس‌جمهوری آمریکا آغاز شده است که «ما به رهبری دنیا تا ایجاد آینده سایبری درخشان ادامه خواهیم داد». در این جمله آمریکا خود را رهبر دنیا دانسته است و فضای سایبری را هم جزئی از مجموعه حکمرانی خود به‌شمار آورده است. برای رسیدن به این هدف دونالد جی ترامپ در جای دیگری از سند بیان داشته که: «راهبرد سایبری ملی، فراخوانی بزرگ برای همه آمریکاییان و شرکت‌های بزرگ مربوطه است تا اقداماتی ضروری را برای ارتقای امنیت ملی سایبری در پیش گیرند»؛ بنابراین فراخوان عمومی داده شده است و مشکل امنیت فضای سایبر فقط توسط دیگر دولت‌ها (به تنهایی) قابل رفع نیست؛ این سند از ۴ بخش اصلی یا رکن[۱] تشکیل شده است.

۱. Pillar

جدول ۱ : ارکان، بخش‌ها و زیربخش‌های سند راهبردی سایبری ایالات متحده آمریکا ۲۰۱۸

ردیف	عناوین ارکان	بخش	زیربخش
۱	محافظت از مردم آمریکا، سرزمین، راه و روش زندگی آمریکایی	بخش اول: اطلاعات و شبکه‌های فدرال امن	✓ مدیریت متمرکز بیشتر و نظارت بر امنیت سایبری غیرنظامی فدرال ✓ همترازی مدیریت ریسک و فعالیت‌های فناوری اطلاعات ✓ بهبود مدیریت ریسک تأمین زنجیره تأمین فدرال ✓ تقویت پیمانکاری امنیت سایبری فدرال ✓ اطمینان از اینکه دولت به بهترین نحو و مبتکرانه عمل می‌کند
		بخش دوم: زیرساخت حیاتی امنیتی	✓ اولویت سرمایه‌گذاری‌های پژوهش و توسعه ملی ✓ بهبود حمل‌ونقل و امنیت سایبری دریایی ✓ بهبود امنیت فضای سایبری
		بخش سوم: مقابله با جرایم سایبری و بهبود گزارش‌ها مبتنی بر حوادث	✓ بهبود گزارش‌های حادثه و پاسخ‌گویی ✓ مدرن‌سازی نظارت الکترونیکی و قوانین جرایم کامپیوتری ✓ کاهش تهدیدات سازمان‌های جنایی بین‌المللی در فضای سایبر ✓ رشد دستگیری مجرمان در خارج از کشور ✓ تقویت ظرفیت اعمال قانون توسط سازمان ملل برای مبارزه با فعالیت‌های جاسوسی سایبری
۲	ارتقاء رفاه آمریکا	بخش اول: توسعه اقتصاد، دیجیتال، شاداب و انعطاف‌پذیر	✓ تهییج بازار فناوری امن و وفق‌پذیر ✓ اولویت به نوآوری ✓ سرمایه‌گذاری در زیرساخت‌های نسل آینده ✓ ترویج جریان آزاد اطلاعات در سراسر مرزها ✓ حفظ رهبری ایالات متحده آمریکا در فناوری‌های نوظهور ✓ ارتقاء امنیت اطلاعات در تمام چرخه عمر
		بخش دوم: پرورش و حفاظت از نخبگان آمریکایی	✓ بروزرسانی مکانیزم‌ها، برای بررسی سرمایه‌گذاری خارجی و عملیاتی در ایالات متحده ✓ حفظ و نگهداری سیستم حفاظتی مالکیت معنوی ✓ حفظ محرمانگی و یکپارچگی اذهان مردم آمریکا
		بخش سوم: ایجاد نیروی کار برتر سایبری	✓ ساخت و حفظ خط تولید استعداد ✓ گسترش فرصت‌های بازآموزی و آموزشی برای کارگران آمریکایی ✓ تقویت نیروی کار امنیت سایبری فدرال ✓ به‌کارگیری قدرت اجرایی در برجسته‌سازی و پاداش

ردیف	عناوین ارکان	بخش	زیربخش
			استعدادهای درخشان در زمینه سایبر
۳	حفظ صلح مقتدرانه	بخش اول: ارتقاء استحکام سایبری به‌واسطه هنجارهای رفتاری دولت پاسخگو	✓ تشویق به پیروی جامع از مقررات سایبری
		بخش دوم: :نشان دادن و تحذیر رفتار خصمانه غیرقابل قبول در فضای سایبر	✓ هدایت به سمت ادراک و هوش هدفمند و جمعی ✓ اعمال پیامدها ✓ ایجاد فضای سایبری بازدارنده ابتکاری ✓ مقابله با نفوذ مخرب سایبری و اطلاعات عملیات
۴	پیشتازی نفوذ آمریکا	بخش اول: ترویج اینترنت نامحدود، مطمئن و امن	✓ حفظ و ارتقاء آزادی اینترنتی ✓ همکاری با کشورهای هم‌فکر، دانشگاه و جامعه مدنی ✓ تولید مدلی چندجانبه از حکومت‌داری اینترنتی ✓ ارتقاء زیرساخت‌های ارتباطات متقابل و مطمئن با قابلیت اتصال به اینترنت ✓ ترویج و حفظ بازارهای جهانی برای کشور ایالات متحده
		بخش دوم: ایجاد ظرفیت سایبری بین‌المللی	✓ تلاش روزافزون برای ظرفیت‌سازی سایبری

سند راهبردی امنیت سایبری جمهوری خلق چین ۲۰۱۷

جمهوری خلق چین با جمعیتی بالغ بر ۱،۴۲۰،۰۶۲،۰۲۲ نفر، دارای تعداد ۸۲۹،۰۰۰،۰۰۰ کاربر در فضای سایبر است. با داشتن چنین آماری می‌توان نتیجه گرفت بیش از ۵۸ درصد شهروندان پرجمعیت‌ترین کشور جهان در فضای سایبر حضور دارند. از نظر تعداد، کشور چین بیشترین سهم را از کاربران فضای سایبر به خود اختصاص داده و از میان ۴،۴۲۲،۴۹۴،۶۲۲ نفر تعداد کل کاربران فضای سایبر در جهان، نزدیک به ۱۹ درصد سهم کشور چین است (Internet World Stats, Usage Population Statics, 2019).

صحبت کردن در مورد موفقیت‌ها و قدرت چین تبدیل به کلیشه شده است و کشورهای دنیا نمی‌توانند با توجه به قدرت چین آن را نادیده بگیرند. نقش چین در آثار فضای سایبر از این

قاعده مستثنی نیست. چین دارای بیشترین جمعیت جهان است و مجموعه بزرگی از کارشناسان با ارزش بالقوه برای عملیات سایبری را در اختیار دارد. درک ساختار سایبری چین، راهبردها و سازمان‌ها کار ساده‌ای نیست. در چین رییس‌جمهور، مسئولیت تعیین راهبرد سایبری چین را برعهده گرفته است. در چین فضای سایبر به‌عنوان چیزی به شدت هماهنگ با جامعه مطرح است و از جریان عمومی حکومت‌داری جدا نیست، مسلماً چالش‌هایی که این رویکرد متمایز در مورد فضای سایبر ایجاد می‌کند به دلایل مختلف تأثیر زیادی بر فعالیت‌های غرب در فضای سایبر دارد (Raud, 2016).

چین با توجه به شرایط ویژه‌اش، تحت شدیدترین حملات سایبری در دنیا قرار دارد و سازمان‌های اطلاعاتی گسترده‌ای در جهان (مخصوصاً کشور ایالات‌متحده آمریکا به‌عنوان یک رقیب سنتی) میلیاردها دلار را صرف این مبارزه می‌کنند (معین‌پور، ۱۳۸۹)؛ یکی از رهبران ارتش چین در پاسخ به سؤال یک مقام آمریکایی که چرا کشور شما حملات سایبری متعددی علیه شبکه‌های ایالات متحده انجام می‌دهد؟ چنین عنوان نموده‌است که: ما هر روزه چندین‌بار مورد حمله سایبری از سوی ایالات‌متحده قرار می‌گیریم (Travis, Sharp. & M Kristin, Lord, ۲۰۱۱). تلاش متخصصان چینی در زمینه رویارویی امنیتی و رقابت‌های تجاری و اقتصادی یکی از عوامل تشدید نگرانی واشنگتن در افزایش تهدیدات سایبری از سوی پکن تلقی می‌شود. پرواضح همان‌طور که وجود فضای سایبر می‌تواند برای چین یک فرصت تلقی گردد، می‌تواند یک تهدید مهم تلقی گردد و این نشان می‌دهد که این جاده یک‌طرفه نیست و پکن هم نگران آسیب‌پذیری‌های خود در حوزه سایبر است (Inkster, 2010).

آنچه مسلم است، حاکمیت فضای سایبر بین چین و غرب و ایالات‌متحده مورد مناقشه است؛ این مناقشه ناشی از تفاوت دیدگاه و تعریف فضای سایبر است. چین برخلاف غرب فضای سایبر را یک فضای جدید نمی‌داند و آن را بخشی از تحول گسترده جامعه صنعتی به جامعه اطلاعاتی می‌داند (Richard A. Clarke, April 2, 2010).

دو رویکرد پیش روی چین برای غلبه بر مشکلات فضای سایبر وجود دارد:

- ایجابی: با توجه به تعداد زیاد جمعیت چین و به تبع آن کاربران اینترنت، حضور فعال در

اینترنت با یک راهبرد منسجم به‌منظور تأثیرگذاری بر فضای سایبر و حکمرانی بر آن؛

- سلبی: راهبرد دیوار چین در فضای سایبر و جدا کردن چین از جامعه جهانی سایبر و ارائه سرویس‌های مورد نیاز کاربران به‌صورت بومی شده در داخل کشور با کمترین وابستگی به نسخه‌های غیر بومی و غیرچینی به‌منظور غلبه بر مشکلات و آسیب‌های فضای سایبر

سند راهبردی فضای سایبر در کشور چین در سال ۲۰۱۷ توسط وزارت امور خارجه این کشور منتشر شده است؛ این سند دارای چهار فصل کلی تحت عناوین فرصت‌ها و چالش‌ها، اصول اساسی، اهداف راهبردی و برنامه عمل است و ذیل این بخش‌ها زیربخش‌هایی به شرح زیر تعریف شده است.

جدول ۲: ارکان، بخش‌ها و زیربخش‌های سند راهبردی امنیت سایبری جمهوری خلق چین ۲۰۱۷

ردیف	عناوین ارکان	بخش
۱	فرصت‌ها و چالش‌ها	-
۲	اصول اساسی	• اصل صلح • اصل حاکمیت • اصل حاکمیت مشترک • اصل مزایای مشترک
۳	اهداف راهبردی	• حفاظت از حاکمیت و امنیت • تدوین سیستم قوانین بین‌المللی • ارتقاء مدیریت عادلانه اینترنت • حمایت از حقوق قانونی و منافع شهروندان • ارتقاء همکاری در زمینه اقتصاد دیجیتال • ساختن بستر تبادل فرهنگ سایبر
۴	برنامه عمل	• صلح و ثبات در فضای مجازی • نظم مبتنی بر قانون در فضای سایبری • مشارکت در فضای سایبری • اصلاحات در سیستم جهانی مدیریت اینترنت • همکاری‌های بین‌المللی در زمینه تروریسم سایبری و جرایم سایبری • حمایت از حقوق و منافع شهروندان از جمله حریم خصوصی • اقتصاد دیجیتال و به اشتراک‌گذاری سهام دیجیتال • توسعه و حفاظت از زیرساخت‌های اطلاعات جهانی • تبادل فرهنگ‌های سایبر

سند راهبردهای امنیت سایبری ملی اتحادیه اروپا

نگرانی در مورد امنیت ۵۰ درصد دغدغه‌های فضای سایبری در اروپا به‌شمار می‌آید؛ اگر این نگرانی‌ها افزایش پیدا کند ممکن است نوعی رویگردانی از این فضا اتفاق بیفتد و کسب‌وکارهایی، دچار مخاطره شوند. راهبردهای امنیت ملی سایبر هنوز در هر ۲۸ کشور عضو ایجاد یا اجرا نشده است؛ بنابراین افزایش آگاهی و ارتقاء شیوه‌های خوب در رابطه با امنیت سایبری در بین کشورهای عضو اتحادیه اروپا همچنان به‌عنوان یک کار مهم برای حمایت از رویه‌های خوب ملی است. در سال ۲۰۱۲، ENISA[1] چرخه حیات NCSS[2] در یک راهنمای عملی در مورد مرحله توسعه و اجرای NCSS5 معرفی کرد.

آژانس امنیت شبکه و اطلاعات اتحادیه اروپا (مرکز تخصصی امنیت شبکه و اطلاعات برای اتحادیه اروپا و کشورهای عضو آن–ENISA) است؛ این آژانس با بخش‌های مختلفی همکاری می‌کند تا توصیه‌هایی را برای عملکرد خوب امنیت اطلاعات ارائه دهد؛ این توصیه‌ها به کشورهای عضو اتحادیه اروپا برای اجرای قوانین مربوط به اتحادیه اروپا است و برای بهبود مقاومت در برابر زیرساخت‌ها و شبکه‌های مهم اطلاعات اروپا کار می‌کند. ENISA درصدد است با حمایت اتحادیه اروپا، مهارت‌های موجود در زمینه امنیت اطلاعات در کشورهای عضو اتحادیه اروپا را ارتقا بخشد.

کشورهای مختلف اروپایی دارای اهداف راهبردی متفاوت در حوزه امنیت سایبری هستند که این نشان‌دهنده تفاوت در زمینه‌های ملی است؛ با این حال برخی از شباهت‌ها بین راهبردهای مختلف کشورهای اتحادیه اروپا وجود دارد. راهبردهای امنیت سایبر غالباً اهداف خود را در موارد زیر بیان می‌کنند (ENISA, 2014).

---

۱. European Union Agency for Network and Information Security
۲. National Cyber Security Strategy

جدول ۳ : ارکان، بخش‌ها و زیربخش‌های مختلف سند راهبردهای امنیت سایبری ملی اتحادیه اروپا ۲۰۱۲

	اهداف	روش‌های رسیدن به اهداف
اهداف مشترک کشورهای اتحادیه اروپا	• دستیابی به تاب‌آوری سایبری: توسعه قابلیت‌ها و همکاری مؤثر در بخش دولتی و خصوصی • امن‌سازی زیرساخت‌های حیاتی و مهم اطلاعات • کاهش جرایم سایبری • توسعه منابع صنعتی و فناوری برای امنیت سایبر • همکاری در ایجاد سیاست بین‌المللی فضای سایبر	• اقدامات قانونی • افزایش قابلیت‌های اجرای قانون و قوه قضائیه • مشارکت در همکاری‌های بین‌المللی و منطقه‌ای • ایجاد یا بهبود فرایندها و ساختارهای هماهنگ • ابزارها و مؤلفه‌های سازمانی • پشتیبانی از پژوهش و توسعه • معرفی CSدر برنامه‌های آموزشی سیستم آموزشی • امکان‌سنجی در شبکه حیاتی دولتی و خصوصی مجزا • مشوق‌ها و بودجه برای طرح‌های پشتیبانی از سیستم‌های امن • دستورالعمل‌ها و اطلاعات داخلی در مورد امنیت اطلاعات
اهداف اتحادیه اروپا	○ همراستایی کل دولت‌ها برای رسیدن به اهداف تعریف شده ○ ایجاد زیرساخت لازم برای مذاکره و گفتگو با ذی‌نفعان فضای سایبر ○ هدایت و جهت‌دهی اولویت‌های شرکاء برای حوزه امنیت سایبر در عرصه بین‌الملل	

ب: تجزیه و تحلیل یافته‌ها

مطالعه تطبیقی سند راهبردی ایالات‌متحده آمریکا، چین و اتحادیه اروپا

محورهای مورد مقایسه در اسناد راهبردی مورد مطالعه به شرح ذیل است. این محورها بر اساس مطالعه اسناد راهبردی و اشتراک موضوعات پر اهمیت در اسناد راهبردی احصاء شده است.

- اهمیت فضای سایبر؛
- امنیت سایبری؛
- حکمرانی سایبری؛
- حقوق و قوانین سایبری؛
- حقوق شهروندان و حریم خصوصی؛

- نقش سایبر در توسعه اقتصادی و سیاسی
- فرهنگ و هویت سایبری؛
- همکاری‌های بین‌المللی در زمینه جرایم سایبری.

نظر به اینکه نتایج فوق به‌عنوان مبانی پژوهش مورد نظر قرار خواهند گرفت و به‌عنوان بخش اصلی در مطالعه تطبیقی مورد نظر هستند و اعتبارسنجی موارد فوق بر میزان اعتبار اجزاء به‌دست آمده در نتایج کمک می‌کند، ضروری است که اقدامات اعتبارسنجی در این مرحله انجام شود که در این خصوص ضریب کاپا به‌عنوان ابزار ارزیابی و اعتبارسنجی اولیه، مورد استفاده قرار می‌گیرد. در این روش محقق دیگر از خبرگان حوزه مطالعه با اطلاع از یافته‌های اولیه و بدون اطلاع از نحوه ادغام کُدها و مفاهیم توسط پژوهشگر، اقدام به طبقه‌بندی کُدها در مفاهیم می‌نماید. مفاهیم ارائه‌شده توسط پژوهشگر با مفاهیم ارائه‌شده توسط این فرد مقایسه و در نهایت با توجه به تعداد مفاهیم ایجاد شده مشابه و متفاوت، شاخص کاپا محاسبه می‌شود.

		نظر محقق		
		خیر	بله	مجموع
نظر خبره دیگر	بله	۲B=	٦A=	۸
	خیر	۰D=	۱C=	۱
	مجموع	۱	٦	۹N=

$$\text{توافقات مشاهده شده} = \frac{A + D}{N} = 0.67$$

وضعیت شاخص کاپا (جنسن و آلن، ۱۹۹٦)

میزان توافق	وضعیت توافق	مقدار عددی شاخص	مقدار عددی شاخص
ضعیف	بی اهمیت	کمتر از ۰	۰-۰/۲۰
متوسط	مناسب	۰/۰-۲۱/٤۰	۰/۰-٤۱/٦۰
معتبر	عالی	۰/۰-٦۱/۸۰	۰/۱-۸۱

$$\text{توافقات شانسی} = \frac{A+B}{N} \times \frac{A+C}{N} \times \frac{C+D}{N} \times \frac{B+D}{N}$$
$$= \frac{8}{9} \times \frac{7}{9} \times \frac{1}{9} \times \frac{2}{9} = 0.0170$$

K=(توافقات شانسی −۱)/(توافقات شانسی − توافقات مشاهده شده)=۰/٦٦

نظر به اعتبار میزان به‌دست‌آمده عدد K -براساس استاندارد اشاره‌شده در جدول- موارد مستخرجه به‌عنوان محورهای مطالعه تطبیقی صحیح هستند.

در این بخش محورهای در نظر گرفته شده برای مطالعه تطبیقی سه سند راهبردی ملی سایبری ایالات‌متحده آمریکا، چین و اتحادیه اروپا با هدف شناسایی محورهای حداقلی اسناد (سند) راهبردی سایبری ج.ا.ایران مورد تحلیل و نتیجه‌گیری قرار می‌گیرد.

جدول ۲ : مقایسه تطبیقی اسناد راهبردی مطالعه تطبیقی و بیان ضرورت وجود محور برای ج.ا.ایران

اهمیت فضای سایبر	
ایالات‌متحده آمریکا	فناوری اطلاعات، پایه و اساس هر علم و فناوری است و نقش آن در جامعه، همانند چاقوی دو لبه است.
چین	چین در فضای سایبر، علاوه بر رویارویی با فرصت‌های جدید با چالش‌های جدی مواجه است.
اتحادیه اروپا	به‌هم پیوستگی خدمات فناوری اطلاعات با زندگی روزمره و تأثیر مستقیم آن بر زندگی دلیل اهمیت فضای سایبری بیان شده است.
ج.ا.ایران	فضای سایبر یک فرصت بی‌نظیر برای جمهوری اسلامی ایران به حساب می‌آید. فرهنگ و تمدن اصیل اسلامی و ایرانی، حرف‌های شنیدنی برای فطرت بشریت (فارغ از قوم و قبیله) دارد. همان‌طور که در زمان صدر اسلام، مشرکین مکه با شنیدن صدای قرائت قرآن از لسان پیامبر اکرم (ص)، فطرتشان بیدار می‌شد، در عصر کنونی فضای سایبر، فرصت بی‌نظیری برای نشر و توسعه این فرهنگ پدید آورده است.
امنیت سایبری	
ایالات‌متحده آمریکا	ارتقای امنیت سایبری در تمام چرخه عمر، توسط بخش دولتی و خصوصی و ارائه‌دهندگان سرویس مورد تأکید است. در این سند نقش بخش خصوصی، در زمینه تأمین امنیت سایبری، پر رنگ دیده شده است.
چین	محافظت از اقتدار و امنیت چین با فائق آمدن بر اطلاعات کنترل نشده و با تقویت توان دفاعی چین در فضای سایبر مورد تأکید است. بخش مهمی از تلاش چین برای نوسازی نیروهای دفاعی ملی و مسلح خود است. در این سند تأمین امنیت معطوف به فعالیت‌های دولت و ارتش چین است و بخش خصوصی دیده

	نشده است.
اتحادیه اروپا	امنیت سایبری لازمه استفاده مناسب از فضای سایبر بیان شده است.
ج.ا.ایران	ماهیت و ذات انقلاب اسلامی، اداره کشور را با مشارکت عمومی و مردم‌محور پیش برده است. همان‌گونه که ۸ سال دفاع مقدس توسط مشارکت عمومی با شکست دشمن رقم خورد، مشارکت عمومی در تأمین امنیت سایبری، بسیار تأثیرگذار است. امنیت سایبری هم شامل امنیت فنی است و هم امنیت فرهنگی. تعیین سازوکار مناسب برای مشارکت حداکثری در تأمین امنیت با نظارت و هدایت حاکمیتی، بایستی از اولویت‌های اسناد راهبردی سایبری ج.ا.ایران باشد.
حکمرانی سایبری	
ایالات‌متحده آمریکا	آزادی فضای سایبر از شعارهای اصلی این سند به حساب می‌آید و حکمرانی از طریق تسلط و نفوذ در تکنولوژی مد نظر است و چالش آمریکا با شرکت هواوی بر سر فناوری 5G بر سر نفوذ در تکنولوژی و خدشه‌دار شدن حکمرانی سایبری است. توزیع اینترنت در سراسر دنیا برای دسترسی آحاد مردم، با هدف اشراف اطلاعاتی بر داده‌های افراد و به منظور تقویت حکمرانی در فضای واقعی است. محدوده حکمرانی در فضای سایبر و فضای واقعی برای کشور آمریکا کل دنیا است.
چین	کشور چین معتقد به حفظ تمامیت ارضی و حکمرانی در فضای سایبر، مبتنی بر جغرافیای کشور است. بر این اساس هر کشور مجاز است در محدوده جغرافیای خود حکمرانی نماید. به همین دلیل با رویکرد آمریکا برای حکمرانی در فضای سایبر بدون محدودیت مرزی مخالف است.
اتحادیه اروپا	حکمرانی در فضای واقعی به‌عنوان شرط لازم برای ایجاد امنیت سایبری در نظر گرفته شده است و نه برعکس آن. نگاه این سند با سایر اسناد مطالعه شده به‌مقوله حکمرانی متفاوت است.
ج.ا.ایران	شبکه ملی اطلاعات، به‌عنوان نماد حکمرانی سایبری شناخته می‌شود. استقرار شبکه ملی اطلاعات و ارائه خدمات بومی برای برطرف کردن نیازهای کاربران در تمامی سطوح، حکمرانی سایبری را در محدوده مرزهای کشور تا حدی زیادی فراهم خواهد آورد.
حقوق و قوانین سایبری	
ایالات‌متحده آمریکا	وجود قوانین بین‌المللی در فضای سایبر، برای نظم‌بخشی به این فضا ضروری است و نشان دادن عواقب عدم تبعیت از قوانین بین‌المللی برای حفظ صلح مقتدرانه آمریکا بسیار مهم است.
چین	سازمان ملل به‌عنوان نهاد تعیین‌کننده حقوق سایبری شناخته می‌شود و به همکاری در زمینه تبادل سیاست و اجرای قانون با سایر کشورها، در فضای سایبر تأکید شده است.
اتحادیه اروپا	حقوق و قوانین سایبری به‌عنوان تسهیل‌کننده تجارت در نظر گرفته شده و بر پیشگیری از همپوشانی وظایف تأکید شده است.
ج.ا.ایران	با وجود تأکید بر تقویت قوانین بین‌المللی و تبعیت کشورها از این قوانین در اسناد راهبردی دو کشور مورد مطالعه، ماهیت مذهبی و ملی مردم کشور ایران، نیازمند تبیین حقوق و قوانین سایبری بر اساس شریعت مقدس اسلام و عرف ایرانی است.
حقوق شهروندان و حریم خصوصی	
ایالات‌متحده	دولت ایالات‌متحده حتی حاضر است اطلاعات خیلی محرمانه کشور را با بخش خصوصی برای

آمریکا	رسیدن به راه حل امن‌سازی به اشتراک بگذارد. حمایت از حقوق معنوی تولیدکنندگان باعث توسعه ایده‌پردازی می‌شود. خلاقیت در آینده سایبری ایالات‌متحده نقشی پر رنگ دارد.
جمهوری خلق چین	فضای سایبر، جایی فراتر از قانون نیست؛ مانند دنیای واقعی، آزادی و نظم هر دو در فضای سایبری ضروری هستند. در دیدگاه چین، حفظ نظم اجتماعی بر حریم خصوصی افراد ارجحیت دارد.
اتحادیه اروپا	تأکید این سند بر توازن بین آزادی و حریم خصوصی است و نویسندگان این سند معتقد هستند که در برخی مواقع به بهانه حفظ حریم خصوصی بی‌رحمانه‌ترین تعدی به حریم خصوصی انجام می‌شود.
ج.ا.ایران	تعریف حقوق شهروندان و حریم خصوصی در اسلام و حکومت اسلامی با دیدگاه کشورهای مورد مطالعه، متفاوت است. اسلام برای حقوق شهروندان و حریم خصوصی، ارزش بسیار زیادی قائل است و برای ورود به حریم خصوصی به‌منظور حفظ کیان و امنیت کشور اسلامی شرایطی به مراتب سخت‌تر از شرایط کشورهای دیگر قرار داده است؛ این موضوع بایستی، از زاویه دین مبین اسلام در اسناد راهبردی تبیین گردد.
نقش سایبر در توسعه اقتصادی و سیاسی	
ایالات‌متحده آمریکا	استفاده از فناوری اطلاعات به‌عنوان ابزاری برای حفظ دموکراسی و مشارکت حداکثری مردم شناخته می‌شود. توسعه سیاسی نسبت به توسعه اقتصادی در سند راهبردی ایالات متحده، پر رنگ‌تر است.
چین	توسعه اقتصاد دیجیتال، باعث اشتغال‌زایی و کم شدن موانع تجارت می‌شود. چین بر تدوین قوانین تجارت فضای سایبری و هماهنگی در بین کشورها، تأکید دارد.
اتحادیه اروپا	فضای سایبر، زیرساخت‌ها، شبکه‌ها، باعث توسعه اقتصاد و سیاست شده است و خدشه‌دار شدن آن‌ها، باعث ضربه خوردن توسعه اقتصادی و سیاسی خواهد شد.
ج.ا.ایران	با توجه به جمعیت جوان کشور ایران، فضای سایبر می‌تواند نقش پر رنگی در توسعه اقتصادی و سیاسی کشور ایفا کند. یکی از راهکارهای، استقرار اقتصاد مقاومتی در کشور، استفاده از ظرفیت و استعداد نیروی انسانی کشور در فضای سایبر به‌منظور توسعه خدمات فضای سایبر و درآمدزایی از این طریق است. نمونه بارز این توسعه، خدمت تاکسی اینترنتی است که باعث درآمدزایی برای بخش قابل توجهی از جامعه شده است.
فرهنگ و هویت سایبری	
ایالات‌متحده آمریکا	همکاری با کشورهای همسو با آمریکا به‌منظور توسعه اینترنت آزاد برای بهره‌برداری مدافعان حقوق بشر، روزنامه‌نگاران مستقل، سازمان‌های جامعه مدنی در سطح محلی و کشور و بین‌الملل؛ این امر باعث تأثیرپذیری از آمریکا می‌شود. صیانت از فرهنگ و سبک زندگی آمریکایی در فضای سایبر مورد تأکید است نه تبادل فرهنگی.
چین	فضای سایبر بستر مناسبی برای گسترش فرهنگ‌های خوب بشر و ترویج انرژی مثبت است. باید تلاش شود تا ظرفیت‌سازی برای تبادل فرهنگی و تنوع فرهنگ‌ها در فضای سایبر تقویت شود تا ذهن و تفکر مردم را غنی سازد و تمدن بشری را پیش ببرد.

اتحادیه اروپا	------
ج.ا.ایران	فرهنگ ایرانی، اسلامی و انقلابی در معرض تهدید است و محافظت از سبک زندگی ایرانی اسلامی، باید یکی از بخش‌های مهم اسناد راهبردی سایبری در ج.ا.ا باشد؛ این فرهنگ به دلیل تأثیرگذاری در منطقه و جلوگیری از تحقق اهداف استکبار جهانی، دارای دشمنان فراوانی است. هویت سایبری هم از جنبه تشخیص و شناسایی و هم از نظر تأثیرگذاری دارای اهمیت است. با شبکه ملی اطلاعات و ایجاد خدمات بومی، می‌توان تا حد زیادی از شناسایی آن جلوگیری کرد و با تهیه محتوای بومی مورد نیاز جامعه، می‌توان از تأثیرات مخرب فرهنگی غرب تا حدودی کاست. روحیه انقلابی و رویکرد تهاجمی، تحت زعامت ولایت مطلقه فقیه، برگ برنده نظام مقدس جمهوری اسلامی ایران در تلاطمات روزگار است. تجربه موفق پیروزی انقلاب اسلامی، مدیریت ۸ سال دفاع مقدس و موفقیت‌های جبهه مقاومت در منطقه، مهر تأییدی بر مزیت رقابتی ج.ا.ا است. لازم به ذکر است جنبه انقلابی هویت مردم ایران برای برخی‌ها اگر نگوییم بی‌اهمیت است، کم اهمیت است و به نظر می‌رسد بایستی با تأکید بیشتری در اسناد مورد تأکید قرار گیرد.
همکاری‌های بین‌المللی در زمینه جرایم سایبری	
ایالات‌متحده آمریکا	تقویت شرکاء (شرکاء در این سند منظور کشورهای همسو و دارای اشتراکات سیاسی) به‌منظور مقابله با تهدیدات سایبری و حفظ منافع کشور آمریکا مورد تأکید است. برای جامعه بین‌الملل نقشی دیده نشده است.
چین	چین معتقد است، فقط جامعه بین‌الملل می‌تواند با همکاری گسترده و احترام متقابل و تفاهم، یک سیستم حاکمیت جهانی مبتنی بر قانون در فضای سایبر را ایجاد کند و تمایل دارد تهدیدات امنیت سایبری مختلف را از طریق گفتگو و مشاوره برطرف کند.
اتحادیه اروپا	راهبردهای انعطاف‌پذیر کشورهای اتحادیه اروپا با قابلیت همکاری به‌منظور مبارزه با جرایم سایبری و ایجاد امنیت در پهنه اتحادیه اروپا مورد تأکید است.
ج.ا.ایران	راهبرد همکاری‌های بین‌المللی در زمینه جرایم سایبری با کشورهای همسایه و کشورهای مسلمان بایستی در دستور کار قرار گیرد. همان‌گونه که بیان شد، ماهیت اسلامی و ملی مجموعه قوانین کشورهای اسلامی اشتراکات بیشتری دارد تا با قوانین بین‌الملل؛ بنابراین همکاری و امضاء تفاهم-نامه با کشورهای اسلامی و همسایه تأثیر بسزایی در زمینه کنترل جرایم سایبری خواهد داشت.

نتیجه‌گیری

از بررسی منابع مرتبط و تطبیق اسناد راهبردی داخلی و خارجی مورد استفاده در این پژوهش این نتیجه حاصل می‌شود که اسناد راهبردی تولید شده در کشور علاوه بر همسویی و هم‌گرایی با دغدغه‌های جهانی، نیازمند پرداختن به محورهای بومی برای ج.ا.ا در قامت انقلاب اسلامی هستند. اسناد راهبردی سایبری تدوین‌شده چندساله اخیر کشور با نگاهی آینده‌نگرانه و با در

نظرداشتن ارزش‌های اسلامی، انقلابی، فرهنگ و تمدن اسلامی و ایرانی بر اساس نتایج این پژوهش به شکل متقنی می‌توانند به‌عنوان اسناد بالادستی سایبری کشور مورد استفاده قرار گیرند و از پراکندگی در این حوزه جلوگیری شود؛ بنابراین کشور عزیزمان ایران در حوزه سایبری نیازمند سند بومی است که قدرت پاسخ‌گویی به نیازهای کشور در حوزه‌های اختصاصی خودش را داشته باشد.

بر این اساس در خصوص اهمیت فضای سایبر و بر مبنای بررسی‌های انجام شده در این پژوهش بایستی به این مهم توجه داشت که فضای سایبر فرصتی بی‌نظیر برای جمهوری اسلامی ایران و نشر و توسعه فرهنگ و تمدن اصیل اسلامی و ایرانی در جهان است.

از دیگر مباحث مهم در نتایج این پژوهش موضوع مشارکت عمومی مردم در تأمین امنیت سایبری است که شامل امنیت فنی و فرهنگی می‌باشد؛ بر این مبنا تعیین سازوکار مناسب برای مشارکت حداکثری در تأمین امنیت با نظارت و هدایت حاکمیتی، بایستی از اولویت‌های اسناد راهبردی سایبری ج.ا.ایران باشد.

از طرفی شبکه ملی اطلاعات به‌عنوان نقطه عطف حکمرانی سایبری نیز باید مورد توجه جدی باشد. استقرار این زیرساخت به‌عنوان بستری برای بیشتر زیرساخت‌های کشور همراه با ارائه خدمات بومی جهت برطرف کردن نیازهای کاربران در تمامی سطوح، حکمرانی سایبری را در محدوده مرزهای کشور تا حدی زیادی فراهم خواهد آورد و از نظر حقوق و قوانین نیز با وجود تأکید بر تقویت قوانین بین‌المللی و تبعیت کشورها در حوزه قوانین در کشورهای مورد مطالعه، ماهیت مذهبی و ملی مردم کشور ایران، نیازمند تبیین حقوق و قوانین سایبری بر اساس شریعت مقدس اسلام و عرف ایرانی است.

یکی از ابعاد مهم در اسناد سایبری موضوع حقوق شهروندی است که از این منظر و با توجه به اینکه اسلام برای حقوق شهروندان و حریم خصوصی، ارزش بسیار زیادی قائل است بایستی، از زاویه دین مبین اسلام در اسناد راهبردی مورد توجه و تبیین قرار گیرد؛ همچنین نظر به نقش فضای سایبر در توسعه اقتصادی و سیاسی نیز با توجه به جمعیت جوان کشور ایران، فضای سایبر می‌تواند نقش پر رنگی در توسعه اقتصادی و سیاسی کشور ایفا کند؛ بنابراین یکی از راهکارهای

استقرار اقتصاد مقاومتی در کشور، استفاده از ظرفیت و استعداد نیروی انسانی کشور در فضای سایبر به‌منظور توسعه خدمات فضای سایبر و درآمدزایی از این طریق است.

بایستی به این مهم توجه داشت که شکل و ماهیت پارادایمیک انقلاب اسلامی ایران و رویکردهای ظلم‌ستیز ایران اسلامی باعث شده است که فرهنگ ایرانی- اسلامی و انقلابی در معرض تهدید باشد و محافظت از سبک زندگی ایرانی اسلامی باید یکی از بخش‌های مهم اسناد راهبردی سایبری در ج.ا.ایران باشد؛ این فرهنگ به دلیل تأثیرگذاری در منطقه و جلوگیری از تحقق اهداف استکبار جهانی، دارای دشمنان فراوانی است. هویت سایبری هم از جنبه تشخیص و شناسایی و هم از نظر تأثیرگذاری دارای اهمیت است. با شبکه ملی اطلاعات و ایجاد خدمات بومی، می‌توان تا حد زیادی از شناسایی آن جلوگیری کرد و با تهیه محتوای بومی مورد نیاز جامعه، می‌توان از آثار مخرب فرهنگی غرب تا حدودی کاست.

در نهایت دیپلماسی سایبری نیز از موارد مهمی است که بایستی توجه به آن در برنامه‌های اسناد راهبردی سایبری کشور باشد. به‌عنوان مثال همکاری‌های بین‌المللی در زمینه جرایم سایبری با کشورهای همسایه و کشورهای مسلمان بایستی در دستور کار قرار گیرد.

پیشنهادها

نظر به اقدامات انجام شده در این پژوهش، مواردی به‌عنوان تکمیل فرایند در اهداف این مقاله به شرح ادامه پیشنهاد می‌شود.

پیشنهادهای عملیاتی

- تمرکز بر ایجاد وحدت همه‌جانبه در تصحیح، تکمیل و اجرایی‌نمودن نتایج این پژوهش؛
- فرهنگ‌سازی استفاده و به‌کارگیری از این نوع اسناد در تصمیم‌سازی‌ها و
- تصمیم‌گیری‌های منوط به تدوین برنامه‌های اجرایی.

پیشنهادهای پژوهشی

- ارائه الگوی عملیاتی بر اساس قالب پیشنهادی در این پژوهش به‌منظور اجرایی‌سازی نتایج و ابعاد راهبردی اسناد سایبری؛
- تدوین نقشه راه برای توسعه نتایج این پژوهش در فرایند تدوین اسناد سایبری بالادستی.

فهرست منابع و مآخذ

الف- منابع فارسی

- افق ۱۴۰۴ (۱۳۸۲)، چشم‌انداز بیست‌ساله جمهوری اسلامی ایران در افق ۱۴۰۴، تهران.
- قراملکی، ا، فرامرز (۱۳۹۵)، روش‌شناسی مطالعات دینی (تحریری نو)، مشهد: دانشگاه علوم اسلامی رضوی.
- معین‌پور، ح (۱۳۸۹)، جنگ‌های سایبری: الگوی نوین دانش جنگاوری در هزاره سوم، فصلنامه سیاسی نظامی اقتدار،۸۵-۵۷ .
- میرطاهر، س (۱۳۹۷)، رویکرد تهاجمی استراتژی ملی سایبری آمریکا Retrieved from .خبرگزاری صدا و سیما http://www.iribnews.ir/fa/news/2237732 :

ب- منابع لاتین

- Min, K.-S., Chai, S.-W., & Han, M. (2015). An International Comparative Study on Cyber Security Strategy. *International Journal of Security and Its Applications*, 13-20.
- (2019). Retrieved from Internet World Stats, Usage Population Statics: https://www.internetworldstats.com
- Inkster, N. (2010). China in Cyberspace. *Global Politics and Strategy*, 12.
- Lamb, Robert, Boyden. (1984). *Competitive strategic management.* Englewood Cliffs: Prentice Hall.
- Li, Y. (2010). *Cyberspace security and international coorporation in china.* ccdcoe.
- Rajiv Nag Donald C. Hambrick Ming-Jer Chen. (2007). What is strategic management, really? Inductive derivation of a consensus definition of the field. *Strategic Management Journal*, Volume 28, Issue 9, pp. 935-955.
- Raud, M. (2016). *Cyber Security in China (Attitudes, Strategies, Organizations).* CCDCOE.
- Richard A. Clarke, R. K. (April 2, 2010). *cyber war the next threat to national security and what to do about it.*
- Shafqat, N., & Masood, A. (2016). Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security (IJCSIS)*, 129-136.
- Shaohui, T. (2017, 03 01). *XINGUA NET*. Retrieved from http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm
- Štitilis, D., Pakutinskas, P., & Malinauskaitė, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal*, 1151–1168.
- Travis, Sharp. & M Kristin, Lord. (2011). America's Cyber future Security and prosperity in the Information Age. *Center for a New American Security*, volume 1.
- White House, u. s. (September 2018). *NATIONAL CYBER STRATEGY of the United States of America.* washington DC: White House.