IRI Military Command and Staff University
Quarterly Journal of Cognitive Warfare Sciences and Technologies
https://www.jcwst.ir/
Online: 2645-7172

Cyber power assessment model of cognitive warfare command and control

Habibaleh Sayari [1] | Kiumars Aria [2]✉

Professor and Faculty Member, National Defense University, Tehran, Iran Email:h.sayari@sndu.ac.ir
Responsible Writer, PhD Student in Defense Management, Army Command and Staff University, Tehran, Iran Email:kiumarsradinanil@gmil.com

Article Info

Article type:
Research Article

Article history:
Received :
24 nov 2025
Received in revised form
04 dec 2025
Accepted
07 dec 2025
Published online
19 dec 2025

Keywords:
Assessment model,
cyberspace,
cyber power,
cyber protection,
command and control,
cognitive warfare

ABSTRACT

Background and Objective: Success in the function of cognitive warfare command and control requires the correct recognition and assessment of cyber-based power to achieve operational superiority and information superiority. The lack of a cyber power assessment model can challenge decision-making. In this regard, the aim of this research is to "achieve a model for evaluating cyber power in cognitive warfare command and control."

Methods: The method of implementing this article was descriptive, analytical and mixed-approach. The statistical population was 10 people for interviews and 62 people for validating the components of the research variables. In order to validate the final results of the research, the opinions of 3 people were used.

Findings: By referring to upstream documents, comparative studies and expert interviews, the dimensions, components and indicators of the model for evaluating cyber power in cognitive warfare command and control were extracted and qualitative control of the findings was performed and the final model for evaluating cyber power in cognitive warfare command and control was proposed.

Conclusions: After the analysis, the proposed model for evaluating cyber power in cognitive warfare command and control was presented in the form of identified dimensions, components, and indicators.

Cite this article: Author, A. A., Author, B. B., & Author, C. C. (year). Article title. *Journal Title*, 56 (1), 1-20.
DOI: http// 10.22034/jcwst.2025.235707

Publisher: IRI Military Command and Staff University

فصلنامه علمی علوم و فناوری‌های جنگ شناختی
https://www.jcwst.ir/
شاپای الکترونیکی: ۲۶۴۵-۷۱۷۲
دانشگاه فرماندهی و ستاد آجا

الگوی ارزیابی قدرت سایبری فرماندهی و کنترل جنگ شناختی

حبیب الله سیاری [۱] | کیومرث آریا [۲] ✉

استاد و عضو هیئت علمی دانشگاه عالی دفاع ملّی، تهران، ایران Email:h.sayari@sndu.ac.ir
نویسنده مسئول، دانشجوی دکتری تخصصی مدیریت دفاعی دانشگاه فرماندهی و ستاد ارتش، تهران، ایران
Email:kiumarsradinanil@gmail.com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخچه مقاله:
تاریخ دریافت:
۱۴۰۴/۰۹/۰۳
تاریخ بازنگری:
۱۴۰۴/۰۹/۱۳
تاریخ پذیرش:
۱۴۰۴/۰۹/۱۶
تاریخ انتشار:
۱۴۰۴/۰۹/۲۸

کلیدواژه‌ها:
الگوی ارزیابی، فضای سایبری، قدرت سایبری، حفاظت سایبری، فرماندهی و کنترل، جنگ شناختی

چکیده

زمینه و هدف: موفقیت در کارکرد فرماندهی و کنترل جنگ شناختی، مستلزم شناخت و ارزیابی صحیح قدرت متّکی به حوزه سایبری برای دستیابی به برتری عملیاتی و اشراف اطلاعاتی است. نبود الگوی ارزیابی قدرت سایبری، می‌تواند تصمیم‌گیری‌ها را دچار چالش نماید.در همین راستا هدف این تحقیق "دستیابی به الگوی ارزیابی قدرت سایبری فرماندهی و کنترل جنگ شناختی است."

روش‌ها: روش اجرای این مقاله کاربردی توصیفی، تحلیلی و با رویکرد آمیخته بود. جامعه آماری جهت انجام مصاحبه به تعداد ۱۰ نفر و جهت اعتبارسنجی اجزاء متغیرهای تحقیق به تعداد ۶۲ نفر پرسشنامه توزیع شد و به منظور اعتبارسنجی نتایج نهایی تحقیق، از نظرات تعداد ۳ نفر استفاده شد.

یافته‌ها: با مراجعه به اسناد بالادستی، مطالعات تطبیقی و مصاحبه خبرگی، ابعاد، مؤلفه‌ها و شاخص‌های الگوی ارزیابی قدرت سایبری فرماندهی وکنترل جنگ شناختی استخراج و کنترل کیفی یافته‌ها انجام و الگوی نهایی در ارزیابی قدرت سایبری فرماندهی و کنترل جنگ شناختی پیشنهاد شد.

نتیجه‌گیری‌ها: پس از تجزیه و تحلیل‌های صورت پذیرفته، الگوی پیشنهادی ارزیابی قدرت سایبری در فرماندهی وکنترل جنگ شناختی، در قالب ابعاد، مؤلفه و شاخص‌ها شناسایی شده ارائه گردید.

استناد: نام خانوادگی، نام؛ نام خانوادگی، نام؛ و نام خانوادگی، نام (سال). عنوان مقاله. *عنوان مجله*، ۲ (۴)، ۱-۲۰.

DOI: http// 10.22034/jcwst.2025.235707

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

فراگیر شدن فناوری اطلاعات و ارتباطات در تمام حوزه‌های زندگی با کارکردهای متنوع باعث شده بخش عمده‌ای از تعاملات جاری در تمام سطوح، در فضای سایبر انجام گیرد و این فضا یک قلمروی عملیاتی شده است. به تبعیت از این فراگیری، نبردها نیز شاهد تغییر و تحوّل اساسی شده و سامانه فرماندهی وکنترل نوین را راساً درگیر عملیات بلادرنگ نموده است. بنابراین امکان تعامل اطلاعاتی و عملیاتی بین واحدهای صف و ستاد در همه رده‌ها با بهره‌گیری از فضای سایبری به نحو چشمگیر و به صورت تصاعدی افزایش یافته است.(آریا، کیومرث،۱۴۰۳: ۲۲)

جنگ شناختی به معنای هدف قرار دادن قوه شناخت عموم مردم و نخبگان جامعه هدف، با تغییر هنجارها، ارزش‌ها، باورها، نگرش‌ها و رفتارها از طریق مدیریت ادراک و برداشت، دارای اهمیت و جایگاه ویژه‌ای بوده و همه حوزه‌های دیگر به نوعی در تحقّق آثار این جنگ می‌باشد و یکی از مواردی که نقش پررنگی در خدمات‌دهی و توسعه این حوزه نقش فعال دارد، فضای سایبری می‌باشد به طوری که امروزه قریب به اتفاق عملیات‌های جنگ شناختی یا در فضای سایبر و یا متکی به این فضا اجرا می‌شود و از ویژگی های مهم این جنگ متّکی بودن بر زیرساخت رسانه‌های نوین سایبری است که تفکّر آدمی را مورد هدف قرار می‌دهد. (joseph nye,2021)

فرماندهی و کنترل به عنوان یکی از مهم‌ترین بخش‌های دفاعی، از طریق جمع‌آوری بلادرنگ اطلاعات با استفاده از شبکه‌های مبتنی بر شبکه و رایانه بر وضعیت لحظه به لحظه میدان نبرد اشرافیت کامل داشته و به ابزار قدرتمندی در ارتقاء توان رزمی تبدیل گردیده که بخشی از آن در فضای سایبری صورت می‌پذیرد. (بابایی،محمود، ۱۴۰۱، صفحه ۴۱)

قدرت سایبری نه‌تنها ابزاری مکمل و هم‌افزا در فرماندهی و کنترل، بلکه نشانگر توانایی در بهره‌گیری از منابع و قابلیت‌های فضای سایبر برای اعمال نفوذ در تمامی حوزه‌های عملیاتی و راهبردی است. (جیسون و همکاران، 2021)

ازآنجایی‌که نبود معیارها و شاخص‌های دقیق برای ارزیابی توانمندی‌های سایبری، فرماندهی و کنترل، رسیدن به اهداف جنگ شناختی را دچار چالش می‌کند بنابراین اطمینان در موفقیت عملکرد فرماندهی و کنترل جهت تحقّق جنگ شناختی که متّکی به حوزه سایبر است دغدغه محقّق بوده و در این راستا وجود یک الگوی ارزیابی که تصویر روشن و دقیقی

را در مورد توانمندی سایبری برای موفقیت در جنگ شناختی به همراه داشته باشد و از انحراف مؤلفه‌های قدرت سایبری از مطلوبیت‌ها، جلوگیری نماید لازم و ضروری بوده و راهگشا در رفع این دغدغه است.

اهمیت این پژوهش، تاثیر دستاوردها و مزایای عمده ارزیابی بدست آمده در شناسایی و کنترل تحولات محیطی فرماندهی و کنترل جنگ شناختی بوده و باعث می‌گردد دانش فرماندهان و مدیران در حوزه قدرت سایبری به روز گردیده و از اعمال سلایق شخصی و تصمیمات غیر کارشناسی در این حوزه خودداری گردیده و موجب بهبود قدرت سایبری و تاثیر فرماندهی و کنترل در جنگ شناختی و افزایش بازدارندگی و قدرت دفاعی گردد. ضرورت این پژوهش در تاثیر نامطلوب نبود نظام ارزیابی و کنترل در برقرار نشدن ارتباط با محیط درون و برون‌سازمانی و چالش در سطوح تصمیم‌گیری بوده و پیامد آن، اعمال‌نظرهای سلیقه‌ای و غیر کارشناسی و غافلگیری در زمینه فرماندهی و کنترل جنگ شناختی می‌گردد.

«دستیابی به الگوی ارزیابی قدرت سایبری فرماندهی وکنترل جنگ شناختی» به عنوان هدف اصلی و «شناخت ابعاد، مؤلفه‌ها و شاخص‌های ارزیابی قدرت سایبری و تبیین ارتباط میان آنها در فرماندهی وکنترل جنگ شناختی» به عنوان اهداف فرعی این پژوهش تعریف گردیده و سئوالات نیز متناسب با این اهداف تدوین شده است و با توجه به اکتشافی بودن پژوهش، فرضیه‌ای مد نظر قرار نگرفته است.

سؤال اصلی پژوهش حاضر، این است که الگوی ارزیابی قدرت سایبری فرماندهی و کنترل جنگ شناختی کدام است؟ بنابراین معیارها و شاخص‌های دقیقی برای ارزیابی در این حوزه با تاکید بر لایه فیزیکی ارائه شده است.

مبانی نظری:

پیشینه و سابقه پژوهش

جمشید نصرت‌آبادی در رساله دکتری خود در سال ۱۳۹۸ با عنوان ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران، منابع قدرت را منابع فیزیکی و زیرساختی، اطلاعاتی و شناختی، ماهیت قدرت را ابزار مؤثر ارعاب علیه رقبا که می‌تواند مبتنی بر فناوری‌های قدرت سایبری مدرن بوده و فراهم آورنده فضای نبرد آینده باشد، پیامدهای قدرت سایبری را بازدارندگی، اشراف اطلاعاتی، برتری عملیاتی معرفی کرده و

عوامل مؤثر برای ارزیابی قدرت سایبری را به سه بعد آفند سایبـری، پدافند سایبـری و تاب‌آوری سایبـری تقسیم‌بندی نموده است.

فضای سایبر

کمیسیون اروپایی فضای سایبر را فضایی که در آن داده‌های الکترونیکی به صورت عمومی منتشر می‌گردد. (Glossary and Acronym, 2022)، روسیه و آمریکا به‌صورت مشترک فضای سایبر را رسانه الکترونیکی که اطلاعات را تولید، منتقل، دریافت، ذخیره، پردازش یا حذف می‌کند معرفی نموده‌اند. (K.F. Rauscher and V. Yaschenko, 2021)

قدرت سایبری

توانایی استفاده از فضای سایبر برای کسب برتری و نفوذ درررویدادهایی در سایر محیط‌های عملیاتی و در میان مؤلفه‌های قدرت است. این نظریه قدرت سایبر را یک توانمندساز برای طیف کامل مؤلفه‌های قدرت ملی شامل فرهنگی، سیاسی، دیپلماتیک، اقتصادی، نظامی و اطلاعاتی محسوب می‌نماید. (Franklin D, Kramer:2021)

ارزیابی قدرت سایبری

سنجش، ارزش‌گذاری و قضاوت در خصوص شاخص‌های مرتبط با قدرت سایبری است که تاثیر آن در حوزه‌ها و موضوعات مرتبط با آن قابل بررسی باشد. (خلیلی، ۱۳۹۷)

قدرت سایبری در جنگ شناختی

یکی از مواردی که نقش پررنگی در خدمات‌دهی و توسعه فرماندهی و کنترل جنگ شناختی داشته و دارای اهمیت و جایگاه ویژه‌ای است فضای سایبری می‌باشد به طوری که امروزه قریب به اتفاق عملیات‌های جنگ شناختی یا در فضای سایبر و یا متکی به این فضا اجرا می‌شود و از ویژگی های مهم این جنگ متّکی بودن بر زیرساخت رسانه‌های نوین سایبری است که تفکّر آدمی را مورد هدف قرار می‌دهد. (joseph nye,2021)

حفاظت سایبری

در اسناد جهانی بویژه در سند آژانس امنیت ملّی آمریکا، مفهوم حفاظت از زیرساخت‌های سایبری، محافظت از دارایی‌های حیاتی است که بایستی در قبال آسیب‌پذیری‌های متعدد مانند دسترسی‌های غیرمجاز به اطلاعات حساس و محرمانه، تخریب، دستکاری انجام شود از اهداف این محافظت، جلوگیری از حملات سایبری علیه زیرساخت‌های حیاتی و کاهش آسیب‌پذیری‌هایی سایبری است. (یزدانی چهاربرج،۱۳۹۹: ۷۶)

آفند سایبری

آماده‌سازی زیرساخت‌ها و سازوکارهای سایبری لازم جهت نفوذ به شبکه‌های اطلاعاتی و سامانه‌های کنترل از راه دور تهدیدات به‌منظور جمع‌آوری اطلاعات، ایجاد اختلال، فریب و تخریب در آن‌ها است. (افتخاری، ۱۴۰۱: ۱۶)

پدافند سایبری

اقدام‌های سایبری و غیر سایبری که توانمندی رصد، پایش، تشخیص تهدید، استخراج آسیب‌پذیری، تجزیه‌وتحلیل میزان خطر، مدیریت و کنترل تهاجم سایبری، بازیابی اطلاعات و تولید قدرت پاسخگویی به تهدید سایبری را فراهم نموده و باعث مصون‌سازی و کاهش آسیب‌پذیری و حفاظت سایبری گردد. ایجاد قابلیت پدافند سایبری به مفهوم آماده‌سازی زیرساخت‌ها و سازوکارهای لازم جهت مقاوم‌سازی سدهای دفاعی شبکه‌های اطلاعاتی و سامانه‌های کنترل از راه دور خودی به‌منظور مقاومت در مقابل نفوذ تهدیدات سایبری و دفع موضعی آن‌ها است و نیازمند شناسایی نقاط قوت و آسیب‌پذیری‌های طرف خودی، تصویر آگاهی موقعیتی از تهدیدات و آسیب‌پذیری‌های خودی، تجزیه‌وتحلیل فنی و غیر فنی تهدیدات و آسیب‌پذیری‌ها، توانایی پاسخ‌گویی و بازیابی اطلاعات آسیب‌دیده است. (نصرت‌آبادی،جمشید،۱۳۹۸)

دفاع سایبری

پیاده‌سازی همه اقدامات مرتبط به فناوری ارتباطات و اطلاعات و مدیریت امنیت اطلاعات با قابلیت پایش و رصد نظامی و عملیات شبکه‌ای رایانه‌ای با پشتیبانی از قابلیت‌های فیزیکی نظامی و سخت می‌شود که به همه اقدامات برای دفاع از فضای سایبر به‌وسیله نیروهای نظامی و سایر ابزارهای مناسب اشاره دارد.(Federal Chancellery of Austria, 2023: 21)

بازدارندگی سایبری

اقدامی بمنظور جلوگیری از فعالیت تهدیدآمیز در فضای سایبری است که شامل سیاست، موضع‌گیری، سلاح، توانمندی یا هم‌پیمانی می‌شود. (هیات دانش نظامی پنتاگون،۲۰۲۱)

تاب‌آوری سایبری

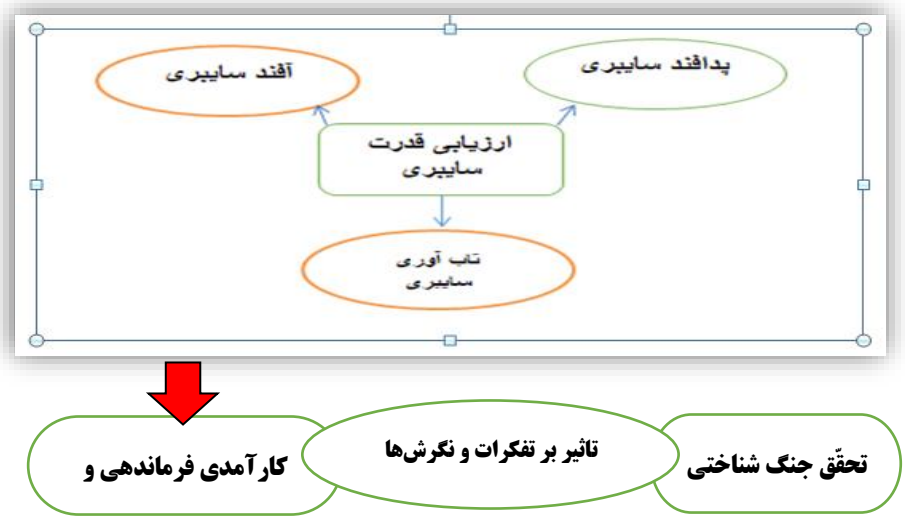
حفظ داده‌ها در فضای سایبری در روبروی با بحران‌ها است. در تاب‌آوری شناختن شاخص‌هایی مدنظر است که به بقاء وضعیت موجود در حد قابل قبول کمک می‌کند. (نشریه علمی تخصصی رویکردهای نوین در فضای سایبری، ۱۴۰۱)

چارچوب نظری پژوهش

چارچوب نظری به روابط بین متغیرهای مستقل، وابسته و مداخله‌گر پرداخته و یک شبکه منطقی، توسعه‌یافته و کامل بین متغیرهای تحقیق که از طریق فرایندهایی مانند مصاحبه، مشاهده و بررسی ادبیات موضوع و پیشینه تحقیق مشخص‌شده می‌پرازد. بنابراین پژوهشگر باید ابتدا مسئله را بشناسد، سپس متغیرهایی که در مسئله نقش دارند را تعیین ساخته و ارتباطات بین متغیرها را بنا بگذارد. (خاکی،۱۴۰۱) در این پژوهش، چارچوب نظری و چارچوب مفهومی حول محور مسئله و سؤالات تحقیق طراحی و نقشه راهی برای پاسخ به سؤالات پژوهش ارائه شده است.

مدل مفهومی

به‌منظور ارائه مدل مفهومی، بر اساس ادبیات تحقیق، مبانی نظری، بررسی اسناد سایبری کشورهای مختلف و همچنین مصاحبه با خبرگان سایبری، جواب سؤالات تحقیق مشخص گردید. سپس به‌منظور ارتباط بین سؤالات و مسئله تحقیق، نمودار متغیرها مرتبط با الگوی ارزیابی قدرت سایبری از روش اکتشافی به شرح شکل زیر شناسایی گردید و ارزیابی این متغیرها، وضعیت قدرت سایبری را که روی فرماندهی و کنترل جنگ شناختی تاثیر می‌گذارد مشخص می‌کند.



روش‌شناسی پژوهش:

نوع این پژوهش کاربردی و روش اجرای آن توصیفی، تحلیلی است، رویکرد آن به صورت آمیخته بوده است. از اسناد بالادستی داخلی و بین‌المللی و مدارک معتبر موجود در کتابخانه‌ها و منابع علـمی پر ارجاع مانند رسـاله دانشگاهی به عنوان ابزار جمع‌آوری اطلاعات استفاده شده است تا میزان اعتبار منابع ارتقاء داده شود. برای اطمینان از اعتبار منابع، از نظرات اساتید دانشگاهی مرتبط با حوزه فرماندهی و کنترل جنگ شناختی استفاده گردید. جامعه آماری جهت انجام مصاحبه به تعداد ۱۰ نفر و جهت اعتبارسنجی اجزاء متغیرهای پژوهش و تحلیل روابط بین آنها به تعداد ۶۲ نفر پرسشنامه توزیع و به منظور صحت سنجی اعتبار نتایج نهایی تحقیق، از نظرات تعداد ۳ نفر از خبرگان استفاده شده است. صاحبنظران و خبرگان انتخاب شده همگی از فرماندهان و مسئولین و متخصصین آگاه در حوزه‌های سایبری، فرماندهی و کنترل و جنگ شناختی هستند که به موضوع پژوهش اشرافیت کامل داشتند، حجم نمونه و روش نمونه‌گیری به روش تمام شمار انجام شد. سؤال‌ها به گونه‌ای طراحی شده بودند تا تمام جوانب موضوع را پوشش داده و پژوهشگر را به دستیابی هدف پژوهش رهنمون سازند. سؤالات مصاحبه به دفعات زمانی متفاوت و متعدد به گروهی از خبرگان صاحبنظر، ارائه گردید. در راستای سنجش روایی سـئوالات مصـاحبه پاسخ‌های دریافتی به دقّت مقایسه شدند.

تجزیه و تحلیل داده‌ها و یافته‌های پژوهش:

با توجه به رویکرد مورداستفاده در تحلیل داده‌های این پژوهش که آمیخته (کمّی و کیفی) است. ابتدا در بخش کیفی با استفاده از تحلیل محتوا، با مراجعه به اسناد بالادستی، مطالعات تطبیقی و مصاحبه خبرگی، ابـعاد، مـؤلفه‌ها و شاخـص‌های الگوی ارزیابی قدرت سایبـری فرماندهی وکنترل جنگ شناختی استخراج و کنترل کیفی یافته‌ها انجام و مدل مفهومی اولیه شکل گرفت و در بخش کمّی با انجام مراحل روایی و پایایی و مراجعه به جامعه آماری، نمونه‌گیری انجام گردید و با به‌کارگیری روش‌های کمّی و تهیه پرسشنامه

و اخذ نظرات جامعه خبره در رابطه با ابـعاد، مـولفه‌ها و شاخـص‌های استخراج‌شده، نتایج نمونه‌گیری، سپس تجزیه و تحلیل و الگوی نهایی ارائه گردید.

تجزیه و تحلیل آماری داده‌های جمعیت شناختی

در این پژوهش جهت شناسایی جامعه آماری ۴ پرسش در خصوص میـزان تحصیـلات، میـزان آشنـایی پاسخ‌دهندگان با موضوع پژوهش، سابقه کار در حوزه موضوع پژوهش و رده مسئـولیتی پاسخ‌دهندگان مطرح شد که گویه‌های جمعیت شناختی آن پس از جمع‌آوری با استفاده از فنون آمار توصیفی مانند فراوانی، درصد فراوانی، فراوانی تجمعی و نمودار هیستوگرام تجزیه و تحلیل گردید و نتایج جدول زیر حاصل شد.

	تحصیلات	فراوانی	درصد فراوانی	درصد فراوانی تجمعی
توزیع فروانی میـزان تحصیـلات	کارشناسـی	۶	۸/۴	۸/۴
	کارشناسـی ارشد	۴۵	۷۴/۵	۸۲/۹
	دکتـری	۱۱	۱۷/۱	۱۰۰
	جمـع کل	۶۲	۱۰۰	
آمار توصیـفی میـزان آشنـایی پاسخ‌دهندگان با موضوع پژوهش	میزان به درصد	فروانی	درصد فراوانی	درصد فراوانی تجمعی
	۶۰٪	۰	۰	۰
	۸۰٪	۸	۱۴/۵	۱۴/۵
	۱۰۰٪	۵۴	۸۵/۵	۱۰۰
	جمـع کل	۶۲	۱۰۰	
آمار توصیفـی سابقه کار در حوزه موضوع پژوهش پاسخ‌دهندگان	سال سابقه خدمت	فراوانی	درصد فراوانی	فراوانی تجمعی
	۱۱-۱۵	۵	۸	۸
	۱۶-۲۰	۲۰	۳۲	۴۰
	۲۱-۲۵	۱۹	۳۱	۷۱
	بیش از ۲۵ سال	۱۸	۲۹	۱۰۰
	جمـع کل	۶۲	۱۰۰	
توزیع فروانی رده مسئـولیتی پاسخ‌دهندگان	تحصیلات	فراوانی	درصد فراوانی	درصد فراوانی تجمعی
	عضـو هیات علمی	۱۷	۲۷/۴	۲۷/۴
	مدیریتـی	۴۱	۶۶/۱	۹۳/۵
	کارشنـاس فنی	۴	۶/۵	۱۰۰
	جمـع کل	۶۲	۱۰۰	

مطابق خروجی جدول بالا، ۱۱ نفر معادل ۱۷/۷ درصد دکتری، ۴۵ نفر معادل۷۲/۶ درصد کارشناسی ارشد و ۶ نفر معادل ۹/۷ درصد مدرک تحصیلی کارشناسی داشته‌اند. ۸ نفر از پاسخ‌دهندگان حدود ۸۰ درصد و تعداد ۵۴ نفر از آن‌ها به میزان ۱۰۰٪ درصد با موضوع تحقیق آشنایی داشته‌اند. ۸ درصد دارای سابقه بین ۱۵-۱۱ سال، ۳۲ درصد دارای سابقه ۲۰-۱۶ سال، ۳۱ درصد دارای سابقه ۲۵-۲۱ درصد و ۲۹ درصد نیز بیش از ۲۵ سال دارای سابقه کار در حوزه موضوع این پژهش بوده‌اند. و ۱۷ نفر معادل ۲۷/۴درصد از پاسخ‌دهندگان عضو هیات علمی، ۴۱ نفر معادل ۶۶/۱ درصد در رده مسئولیتی مدیریتی و ۴ نفر معادل ۶/۵ درصد دارای رده مسئولیتی کارشناس فنی هستند.

تجزیه و تحلیل سایرداده‌ها و ارائه یافته‌های پژوهش

در این قسمت به کمک داده‌های آماری پرسشنامه و فنون آمار استنباطی، به بررسی تاثیر ابـعاد و مولفـه‌ها (آفند سایبری و پدافند سایبری و تاب‌آوری سایبری) در الگوی ارزیابی قدرت سایبری فرماندهی وکنترل جنگ شناختی پرداخته شده است که نتایج آن به شرح ادامه آمده است.

الف– رتبه‌بندی ابعاد موثر بر الگوی ارزیابی قدرت سایبری فرماندهی و کنترل جنگ شناختی

ردیف	متغیرها	رتبه میانگین
۱	پدافنـد سایبـری	۲,۵۶
۲	تاب‌آوری سایبـری	۲,۳۲
۳	آفنـد سایبـری	۲,۲۰

خروجی جدول به این معناست که اولویت همه ابعاد ازنظر میانگین تاثیری که بر الگوی ارزیابی قدرت سایبری دارند باهم یکسان است.

ب– رتبه‌بندی مولفه‌های پدافند سایبری موثر بر الگوی ارزیابی قدرت سایبری

ردیف	متغیرها	رتبه میانگین
۱	مصـــون‌سازی	۲,۷۱
۲	دیپلمـاسی پدافندی	۲,۱۲
۳	خط‌مشـی‌گذاری	۲,۰۵

خروجی جدول به این معناست که اولویت همه مولفه‌ها ازنظر میانگین تاثیری که بر پدافند سایبری دارند باهم یکسان است.

رتبه‌بندی میانگین شاخص‌های مصـــون‌سازی

ردیف	شاخص	رتبه میانگین
۱	بومی بودن تجهیـزات	۸,۱۹
۲	رصد سایبـری	۸,۰۱
۳	آموزش همـگانی	۷,۸۲
۴	نرم‌افزارهای تخصصـی	۷,۸۱
۵	پدافنـد به هنگام	۷,۷۸
۶	مدیریت هماهنـگ بین مدافعیـن	۷,۷۷
۷	مرکز عملیـات امنـیت	۷,۶۷۰
۸	تدابیـر نظارتی	۷,۶۵

خروجی جدول به این معناست که اولویت همه شاخص‌ها یکسان نیست و ازنظر میانگین تاثیری که بر مصـون‌سازی دارند باهم تفاوت دارند.

رتبه‌بندی میانگین شاخص‌های دیپلمـــاسی سایبـــری

ردیف	شاخص	رتبه میانگین
۱	عضـویت در مجامع بین‌المـللی	۵,۲۱
۲	عضـویت در کنوانسیـون‌های سایبـری	۵,۱۱
۳	یکپـارچگی و انسجـام در سنـاریو پردازی‌ها	۴,۹۰

خروجی جدول به این معناست که اولویت همه شاخص‌ها یکسان نیست و ازنظر میانگین تاثیری که بر دیپلمـاسی سایبـری دارند باهم تفاوت دارند.

رتبه‌بندی میانگین شاخص‌های خط‌مشـــی‌گذاری

ردیف	شاخص	رتبه میانگین
۱	نهاد خط‌مشـی‌گذاری	۲,۸۹
۲	سیاسـت‌های کلان	۲,۷۵
۳	راهبـردهای سایبـری	۲,۱۶
۴	قوانیـن سایبـری	۲,۱۰
۵	مقـررات سایبـری	۱,۷۲
۶	تقسیـم‌کار مناسب	۱,۲۹

خروجی جدول به این معناست که اولویت همه شاخص‌ها یکسان نیست و ازنظر میانگین تاثیری که بر خط‌مشـی‌گذاری دارند باهم تفاوت دارند.

پ–رتبه‌بندی مولفه‌های تاب‌آوری سایبـــری موثر بر الگوی ارزیابی قدرت سایبری

ردیف	متغیرها	رتبه میانگین
۱	تشخیـص	۱,۸۵
۲	مقاومـت سایبـری	۱,۷۹
۳	واکنـش	۱,۵۲
۴	ترمیـم سایبـری	۱,۴۳

خروجی جدول به این معناست که که اولویت همه مولفه‌ها ازنظر میانگین تاثیری که بر تاب‌آوری سایبـری دارند باهم یکسان است.

رتبه‌بندی میانگین شاخص‌های تشخیـص

ردیف	شاخص	رتبه میانگین
۱	مشاهـده	۲,۶۵
۲	هوشـمندی	۲,۰۳
۳	برآورد تهدیـدات	۱,۵۴

خروجی جدول به این معناست که اولویت همه شاخص‌ها یکسان نیست و ازنظر میانگین تاثیری که بر مولفه تشخیـص دارند باهم تفاوت دارند.

رتبه‌بندی میانگین شاخص‌های مقاومـت سایبـــری

ردیف	شاخص	رتبه میانگین
۱	کاهش وابـستگی زیرساختـی	۹,۶۶
۲	افـزونگی	۹,۲۵
۳	مسیـرهای ارتباطـی چندگـانه	۹,۱۲
۴	ساختـار دفـاعی لایه به لایه	۹,۰۸
۵	تغییر ساختـار از سلسلـه مراتبـی به شبـکه‌ای	۹
۶	دستـرسی به نقاط تبـادل اینترنتی	۸,۷۵
۷	دستـرسی به گلـوگاه‌های اینتـرنتی	۸,۲۸

خروجی جدول به این معناست که اولویت همه شاخص‌ها یکسان نیست و ازنظر میانگین تاثیری که بر مقاومـت سایبـری دارند باهم تفاوت دارند.

رتبه‌بندی میانگین شاخص‌های واکنـــش

ردیف	شاخص	رتبه میانگین
۱	بازیابـی منـابع اطلاعات	۶,۸۰
۲	هدایـت اوضاع	۶,۳۵
۳	حفظ ادلـه دیجیتال	۶,۱۱
۴	بازگشـت بـموقع	۶,۰۲

خروجی جدول به این معناست که اولویت همه شاخص‌ها یکسان نیست و ازنظر میانگین تاثیری که بر واکنـش دارند باهم تفاوت دارند.

رتبه‌بندی میانگین شاخص‌های ترمیـم

ردیف	شاخص	رتبه میانگین
۱	سازمـان‌دهی مجـدد	۴,۸۲
۲	باز معمـاری	۳,۹۲
۳	طراحـی ویـژگی‌های عملیـاتی منـاسب	۳,۱۲
۴	انتـقال	۲,۹۵

خروجی جدول به این معناست که اولویت همه شاخص‌ها یکسان نیست و ازنظر میانگین تاثیری که بر ترمیـم دارند باهم تفاوت دارند.

ت– رتبه‌بندی مولفه‌های آفنـد سایبـری موثر بر الگوی ارزیابی قدرت سایبری

ردیف	متغیرها	رتبه میانگین
۱	عامـل انـسانی	۳,۲۲
۲	آگاهـی وضعیتـی	۲,۹۵
۳	تسلیـحات سایبـری	۲,۴۵
۴	پیچیـدگی سایبـری	۲.۱۸

خروجی جدول به این معناست که که اولویت همه مولفه‌ها ازنظر میانگین تاثیری که بر آفند سایبـری دارند باهم یکسان است.

رتبه‌بندی میانگین شاخص‌های عامـل انسـانی

ردیف	شاخص	رتبه میانگین
۱	دانـش	۵,۴۹
۲	خـلاقیت	۵,۳۶
۳	چابـکی	۵,۳۰
۴	فرصـت‌طلب	۵,۲۷
۵	جهـادی بودن	۴,۳۳
۶	تجـربه	۴,۱۵

خروجی جدول به این معناست که اولویت همه شاخص‌ها یکسان نیست و ازنظر میانگین تاثیری که بر عامل انسانی دارند باهم تفاوت دارند.

رتبه‌بندی میانگین شاخص‌های آگاهی وضعیتی

ردیف	شاخص	رتبه میانگین
۱	تقسیم فضای سایبری	۴،۵۲
۲	شناسایی قابلیت‌های پدافندی دشمن	۴،۳۲
۳	پایش سایبری	۴،۱۲
۴	هشداردهی	۳،۲۲

خروجی جدول به این معناست که اولویت همه شاخص‌ها یکسان نیست و ازنظر میانگین تاثیری که بر آگاهی وضعیتی دارند باهم تفاوت دارند.

رتبه‌بندی میانگین شاخص‌های تسلیحات سایبری

ردیف	شاخص	رتبه میانگین
۱	قدرت تخریب بالا	۴،۳۳
۲	هوشمندی	۴،۱۵
۳	میزان کنترل‌پذیری	۳،۲۵
۴	پنهان‌شوندگی	۳،۰۵
۵	رمزشوندگی	۲،۷۶

خروجی جدول به این معناست که اولویت همه شاخص‌ها یکسان نیست و ازنظر میانگین تاثیری که بر تسلیحات سایبری دارند باهم تفاوت دارند.

رتبه‌بندی میانگین شاخص‌های پیچیدگی سایبری

ردیف	شاخص	رتبه میانگین
۱	نوآوری	۷،۸۹
۲	فراوانی محرک‌های سایبری	۷،۵۳
۳	سناریوهای جایگزین آفندی	۷،۳۵
۴	نیروی سایبری شبه‌نظامی	۷،۱۵
۵	تداوم	۶،۸۶
۶	استفاده از حملات چندمرحله‌ای	۶،۶۷

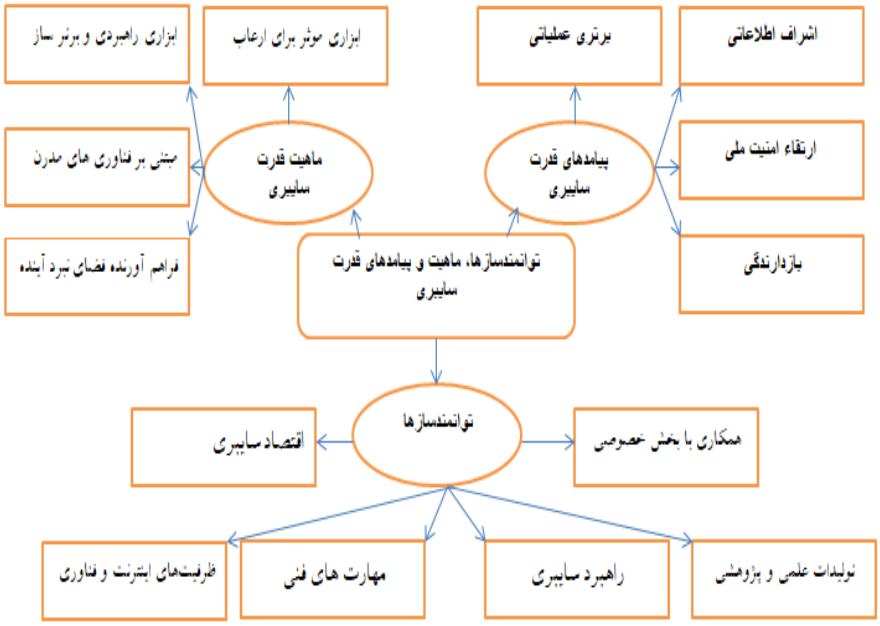
خروجی جدول به این معناست که اولویت همه شاخص‌ها یکسان نیست و ازنظر میانگین تاثیری که بر پیچیدگی سایبری دارند باهم تفاوت دارند.

نتیجه‌گیری و پیشنهاد:

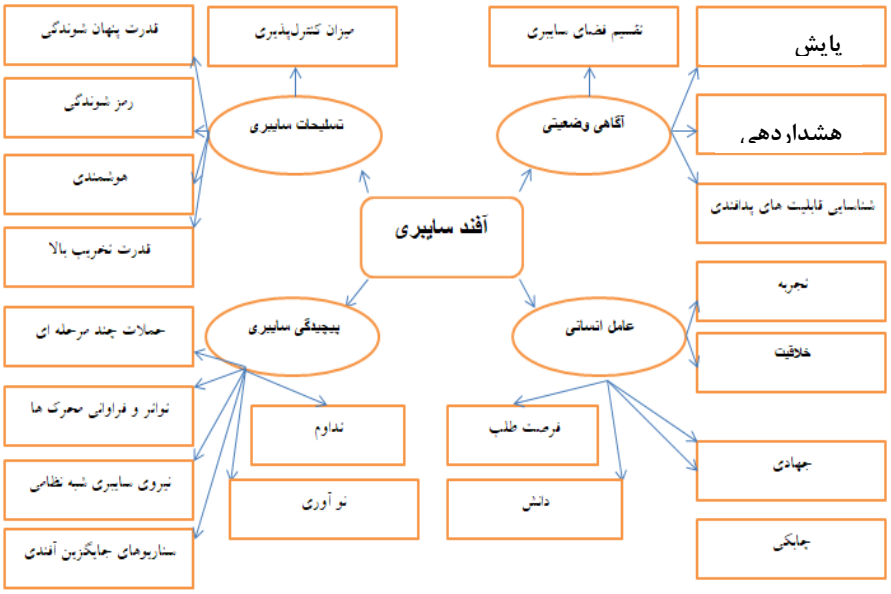
(الف) نتیجه‌گیری

عملیات‌های جنگ شناختی یا در فضای سایبر و یا متکی به این فضا اجرا می‌شود. همچنین فرماندهی و کنترل به عنوان یکی از ابزارهای قدرتمندی در ارتقاء توان رزمی است که بخشی از آن در فضای سایبری صورت می‌پذیرد. قدرت سایبری نه‌تنها ابزاری مکمل و هم‌افزا در فرماندهی و کنترل است بلکه نشانگر توانایی در بهره‌گیری از منابع و قابلیت‌های فضای سایبر برای اعمال نفوذ در تمامی حوزه‌های عملیاتی و راهبردی است. این قدرت نیازمند منابع توانمندساز، ابعاد، مولفه و شاخص‌های متعدد است که ارزیابی آنها، جهت تحقّق موثر فرماندهی و کنترل جنگ شناختی ضرورت دارد. بنابراین روابط آنها با نمودارهای محتوایی آنها به شرح زیر ارائه شده و در پایان الگوی ارزیابی قدرت سایبری فرماندهی و کنترل جنگ شناختی ارائه گردیده است.

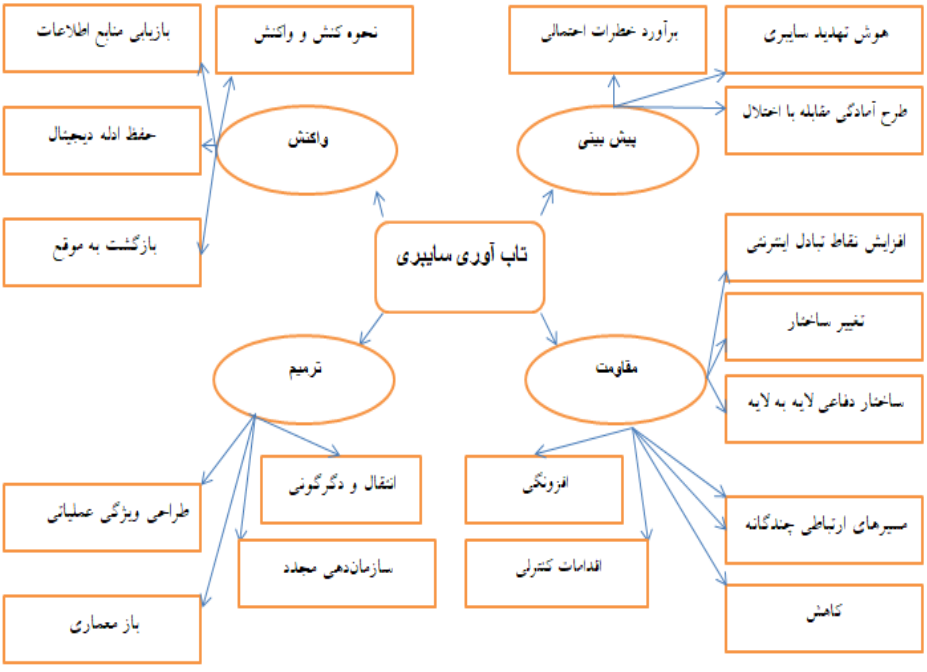
الف–نمودار منابع توانمندساز، ماهیت و پیامدهای قدرت سایبری فرماندهی و کنترل جنگ شناختی



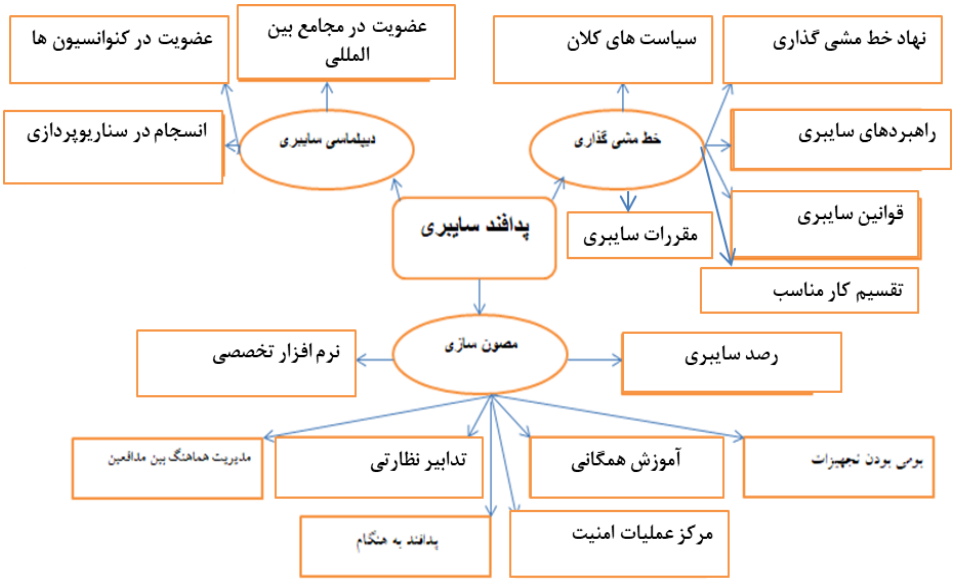
ب– نمودار محتوایی آفنـد سایبـری در ارزیابی قدرت سایبـری فرماندهی و کنترل جنگ شناختی



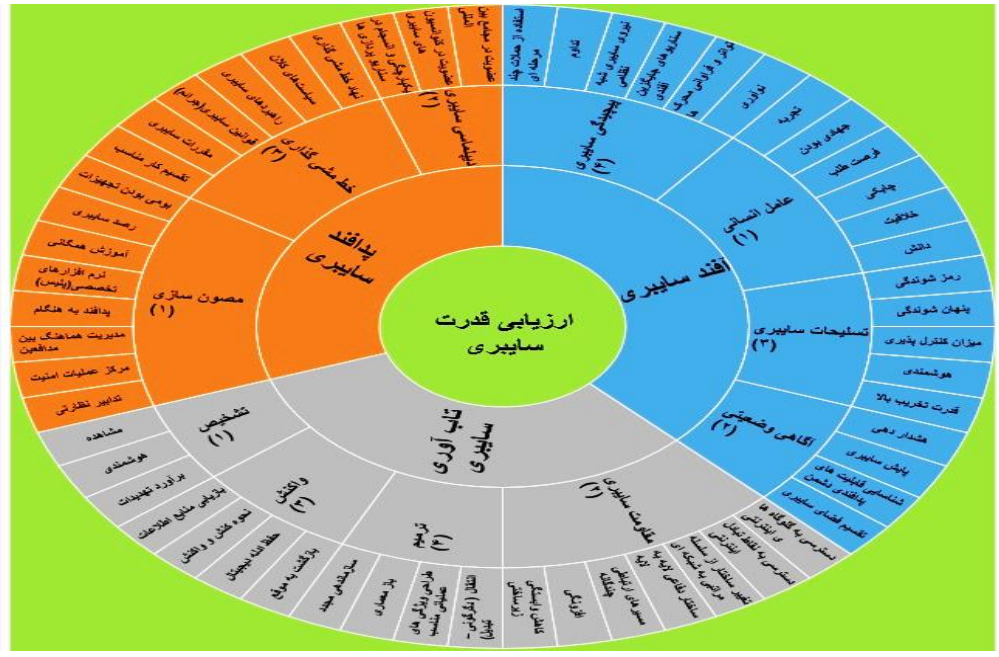
پ– نمودار محتوایی تاب‌آوری سایبـری در ارزیابی قدرت سایبـری فرماندهی و کنترل جنگ شناختی



ت– نمودار محتوایی پدافنـد سایبـری در ارزیابی قدرت سایبـری فرماندهی و کنترل جنگ شناختی



ت– الگوی نهایی پیشنهادی در ارزیابی قدرت سایبـری فرماندهی و کنترل جنگ شناختی



(ب) پیشنهاد

۱- ارزیابی در ابعاد اطلاعاتی نبرد شناختی بدون در نظر گرفتن ابزار فرماندهی و کنترل، در تحقیقات آتی مورد پژوهش قرار گیرند.
۲- بمنظور احصاء قابلیت فرماندهی وکنترل جنگ شناختی، مباحث تاب‌آوری و پدافند سایبری به صورت مجزا بررسی گردیده و ضرورت دارد موضوع ترکیب آنها با هم و حفاظت سایبری و نقش آنها در فرماندهی و کنترل جنگ شناختی، مورد پژوهش قرار گیرند.
۳- موضوع اطمینان کاذب حداکثری به امنیت سایبری (توهّم امنیت) و نقش مخرب آن در فرماندهی و کنترل جنگ شناختی در تحقیقات آتی، مورد پژوهش قرار گیرند.
۴- لازم است نقش مخرب غفلت در حفاظت سایبری در فرماندهی و کنترل جنگ شناختی در تحقیقات آتی، مورد پژوهش قرار گیرند.
۵- با توجه به وابستگی زیاد فرماندهی و کنترل جنگ شناختی به زیرساخت فنی قدرت سایبری، تسریع در ارتقاء قدرت سایبری با توجه به این الگو که منجر به برتری عملیاتی گردد پیشنهاد می‌شود.

توصیه‌های کلیدی برای سیاست‌گذاران دفاعی

۱- ارتقاء قدرت سایبری با توجه الگوی پیشنهاد شده
۲- فرهنگ‌سازی فرماندهان و مدیران در خصوص عواقب خطرناک توهّم امنیت سایبری
۳- بررسی ابعاد اطلاعاتی نبرد شناختی بدون در نظر گرفتن ابزار فیزیکی فرماندهی و کنترل
۴- انجام پژوهشی در خصوص تاثیر علوم سایبرشناختی در فرماندهی وکنترل شناختی

تشکر و قدردانی:
از همه اساتید و عزیزانی که با مشاوره خود، پژوهشگر را یاری نمودند مراتب تشکر و قدردانی دارم.

تضاد منافع:
بدینو سیله نوی سندگان این مقاله ت صریح دارند که هیچگونه ت ضاد منافع در انجام این پژوهش وجود ندارد.

منابع:

الف- منابع فارسی

۱) آذر،داوود و مسلمی، حسین(۱۴۰۱)،راهبردهای حفاظت سایبری ارتش‌جمهوری‌اسلامی‌ایران،رساله دکتری دافوس آجا.

۲) آریا،کیومرث، (۱۴۰۴)، راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل ارتش،رساله دکتری، دانشگاه فرماندهی و ستاد ارتش.

۳) افتخاری، اصغر. (۱۴۰۱). "ساختار قدرت نرم". رساله دکتری، دانشگاه علامه طباطبایی.

۴) بابایی، محمود (۱۴۰۱)، فضای سایبر و الگوهای تعامل گفتمانی، رساله دکتری، دانشگاه علامه طباطبایی.

۵) پور ابراهیمی، علیرضا (۱۳۹۹)، آفند و پدافند سایبری، دانشگاه عالی دفاع ملی.

۶) حق‌شناسی، مهدی و همکاران، (۱۳۹۹)،" ارائه الگویی جهت ارزیابی مخاطرات سایبری در سامانه‌های کنترل صنعتی" تهران- دانشگاه شهید بهشتی.

۷) جلالی، غلامرضا (۱۴۰۱)، اصول و مبانی پدافند سایبری، موسسه انتشارات نبوی.

۸) خلیلی، رضا، مرادیان، محسن (۱۳۹۷)، قدرت ملی، چارچوبی نوین برای سنجش و تحلیل، پژوهشکده مطالعات راهبردی.

۹) ع. رشیدی، ک. داداش‌تبار و ب. نظرپور(۱۳۹۹)، " آگاهی وضعیتی سایبری"، دانشگاه صنعتی مالک اشتر.

۱۰) قهرود، علیرضا (۱۳۹۹)، تهدیدات سایبری و بهبود وضعیت راهبردهای دفاعی.

۱۱) قاسم‌زاده، اردشیر ، (۱۳۹۹)، " ارائه مدل ارزیابی میزان اثربخشی حملات سایبری، با رویکرد عملیات تاثیرمحور مبتنی بر اصول جنگ شناختی".دانشگاهشهید ستاری نهاجا.

۱۲) نای، جوزف (۲۰۲۱)، آینده قدرت، ترجمه: رضا قربانی و جواد شیرمحمدی، تهران، انتشارات دافوس آجا.

۱۳) نصرت‌آبادی، جمشید، (۱۳۹۸)، ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح ج.ا.ا، رساله دکتری، دانشگاه دفاع ملّی

۱۴) یزدانی چهاربرج، رحیم، (۱۳۹۹)، راهبردهای حفاظت سایبری زیرساخت‌های حیاتی کشور، رساله دکتری، دانشگاه دفاع ملّی.

ب- منابع انگلیسی

1) Adrian Venables, Siraj Ahmed Shaikh and James Shuttleworth, (2021), A MODEL FOR - Cyber Space Operation Air Force Doctrine Document.
2) Federal-Chancellery-of-the-Republic-of-Austria. (2021). Austrian Cyber Security Strategy.
3) Glossary and Acronyms," Information Society, European Commission, http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm, Visited: 2021.
4) ITU Cybersecurity Team (2022), Global Cybersecurity Index (GCI),Telecommunication Development Bureau.
5) J. Sheldon, Deciphering cyberpower: Strategic purpose in peace and war,
6) Strategic Studies Quarterly, vol. 5(2), pp. 95–112, 2019.
7) J. Andress and S. Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Elsevier Syngress, 2019.
8) Jc jansen van vuuren, (2021), “Building Blocks for National Cyberpower” Boston University of the United States.
9) K.F. Rauscher and V. Yaschenko (Eds.), Russia- U.S. Bilateral on Cybersecurity Critical Terminology Foundations, EastWest Institute and the Information Security Institute of Moscow State University, 2022.
10) Nye, Joseph s. (2010); “Cyber Power”, Belfer Center for Science and International Affairs.
11) Virgilio Almeida, 2019, Cyberspace Governance Concepts and Framework, Harvard University, Cambridge, September2019.
12) U.S. Cyber Command, (2021), Organizing For Cyberspace Operations, Committee On Armed.

پ - سایت‌ها

13) Source: IEEE-USA. Available at http://www.ieeeusa.org/policy/positions/infoinfrastructure.html tions/infoinfrastructure.html
14) http://dl.acm.org/citation.cfm?id=2043164.1851223.
15) https://publicwiki01.fraunhofer.de/CIPedia/index.php/Critical_Information_Infrastructure.
16) http://tadviser.com/index.php/Article:Law_On_security_of_critical_information_infrastructure_of_the_Russian_Federation.