Military Science and Tactics
https://www.qjmst.ir/ Online ISSN: 4520-2676 Print ISSN: 2008-191x

# Identifying and Ranking of Components and Indicators of Cyber Power in the Defensive-Security Dimension

**Khodadad Halili[1]✉ | Seyyed Alireza Motahari[2]**

1. Faculty Member of Shahid Sattari Aviation University, Tehran, Iran.
E-mail: halili@chmail. com
2. Phd student of Defense Management. Command and Staff University, Tehran, Iran.
E-mail: motaharialireza84@gmail. com

## Article Info

**Article type:**
Research Article

**Article history:**
Received
16 March 2024
Received in revised form
19 June 2024
Accepted
3 August 2024
Published online
17 December 2024

**Keywords**:
*Cyber power, national power, cyber defense,*

## ABSTRACT

**Objective:** This study aims to clarify the components and indicators of cyber power within the defensive-security dimension.

**Methodology:** The research is applied and developmental in terms of its objective, descriptive-case study in terms of its nature, and uses a mixed (qualitative and quantitative) approach for data analysis. The statistical population of this study consists of 50 experts and specialists in the field of cyberspace. For the statistical analysis of quantitative data, the data collected from a researcher-designed questionnaire were examined using Smart PLS software.

**Findings:** The results of the study led to the identification of four components within the defensive-security dimension of cyber power: the development of cyber defense and passive defense, strengthening the cybersecurity of critical and sensitive infrastructures, equipping with cyber technologies and weapons for deterrence, and organizing and structuring specialized cyber forces. Additionally, 41 indicators were identified.

**Conclusion:** Overall, the study showed that efforts to achieve indigenous knowledge, establish a cyber command and control center, enhance cybersecurity indicators, and acquire the necessary readiness to counter cyber threats in the defensive-security dimension are of significant importance. A thorough understanding and recognition of this issue by elites and policymakers will lead to the development of policies and plans for securing cyber resources, equipping with advanced technologies, and strengthening cyber power in this field.

**Cite this article:** Halili, kh. , Motahari, S. A. (2024). Statistics and ranking of components and indicators of cyber power in the Security defense dimension. *Military Science and Tactics*, 20 (69), 281-314.
DOI: http//doi. org/ 10. 22034/qjmst. 2024. 2024589. 2039



**Publisher:** AJA Command and Staff University
DOI: 10. 22034/qjmst. 2024. 2024589. 2039

Military Science and Tactics
https://www.qjmst.ir/
Online ISSN: 4520-2676 Print ISSN: 2008-191x

# احصاء و رتبه‌بندی مؤلفه‌ها و شاخص‌های قدرت سایبری در بعد دفاعی امنیتی

**خداداد هلیلی[1]✉ | سید علیرضا مطهری[2]**

۱. نویسنده مسئول، استادیار، عضو هیئت‌علمی دانشگاه شهید ستاری، تهران، ایران. رایانامه: kh. halili@ssau. ac. ir

۲. دانشجوی دکتری مدیریت دفاعی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: motaharialireza84@gmail. com

**اطلاعات مقاله**

**نوع مقاله:**
مقالهٔ پژوهشی

**تاریخ دریافت:**
۱۴۰۲/۱۲/۲۶

**تاریخ بازنگری:**
۱۴۰۳/۰۳/۳۰

**تاریخ پذیرش:**
۱۴۰۳/۰۵/۱۳

**تاریخ انتشار:**
۱۴۰۳/۰۹/۲۷

**کلیدواژه‌ها:**
*قدرت سایبری، قدرت ملی، دفاع سایبری.*

## چکیده

**هدف:** این تحقیق با هدف تبیین مؤلفه‌ها و شاخص‌های قدرت سایبری در بعد دفاعی امنیتی انجام‌شده است.

**روش‌شناسی:** تحقیق حاضر از نظر هدف کاربردی- توسعه‌ای، از نظر ماهیت از نوع توصیفی- موردی و از نظر روش تجزیه‌وتحلیل داده‌ها، آمیخته (کیفی و کمی) است. جامعه آماری این تحقیق، شامل ۵۰ نفر از خبرگان و صاحب‌نظران فضای سایبر است. به‌منظور تجزیه‌وتحلیل آماری داده‌های کمی، داده‌های جمع‌آوری‌شده از پرسشنامه محقق ساخته، با استفاده از نرم‌افزار اسمارت پی. ال. اس موردبررسی قرار گرفت.

**یافته‌ها:** نتایج تحقیق منتهی به احصاء چهار مؤلفه در بعد دفاعی امنیتی قدرت سایبری شامل توسعه دفاع سایبری و پدافند غیرعامل، تقویت امنیت سایبری زیرساخت‌های حیاتی و حساس، مجهز شدن به فناوری و تسلیحات سایبری به‌منظور بازدارندگی و سازمان‌دهی و ساختارسازی نیروی سایبری متخصص و ۴۱ شاخص گردید.

**نتیجه‌گیری:** درمجموع تحقیق نشان داد تلاش برای دستیابی به دانش بومی، ایجاد مرکز فرماندهی و کنترل سایبری، ارتقاء شاخص امنیت سایبری و کسب آمادگی‌های لازم برای مقابله با تهدیدات سایبری در بعد دفاعی امنیتی حائز اهمیت است. شناخت و درک دقیق نخبگان و سیاست‌گذاران از این مسئله، موجب سیاست‌گذاری و برنامه‌ریزی برای تأمین سرمایه‌های سایبری و مجهز شدن به فناوری‌های پیشرفته و ارتقاء قدرت سایبری در این حوزه خواهد شد.

**استناد:** هلیلی، خداداد و مطهری، سید علیرضا. (۱۴۰۳). احصاء و رتبه‌بندی مؤلفه‌ها و شاخص‌های قدرت سایبری در بعد دفاعی امنیتی. *علوم و فنون نظامی*، ۲۰(۶۹)، ۳۱۴- ۲۸۱.

DOI: http//doi. org/10. 22034/qjmst. 2024. 2024589. 2039

**ناشر:** دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

DOI: 10. 22034/qjmst. 2024. 2024589. 2039

Military Science and Tactics
https://www.qjmst.ir/

# Identifying and Ranking of Components and Indicators of Cyber Power in the Defensive-Security Dimension

**Khodadad Halili[1] Seyyed Alireza Motahari[2]**

## Extended Abstract

### Introduction

In recent years, the priorities of national leadership have shifted toward the utilization of cyberspace, with emerging cyber technologies facilitating the reconfiguration of power in the form of cyber power (Halili et al., 2018). Achieving cyber power can serve as a strategic asset for a country in safeguarding the core objectives of the Islamic Revolution, addressing political, economic, and defense weaknesses, and expanding its cross-border influence. Although the concept of cyber power has been linked to phenomena such as the diffusion of power and the erosion of government authority (Nye, 2011), overcoming the crises and challenges generated by these shifts also requires navigating cyberspace and leveraging cyber technologies. The characteristics of cyber power bear similarities to national power, with the same phenomena observed within cyberspace, a focus of this study. Scientific research and the discursive development of cyber power in the defense and security dimensions foster convergence among stakeholders, leading to a shared understanding that supports policymaking in this domain.

1 - Faculty Member of Shahid Sattari Aeronautical University, Tehran, Iran. E-mail: kh.halili@ssau.ac.ir
2 - Phd student of Defense Management. Command and Staff University, Tehran, Iran.
E-mail: motaharialireza84@gmail.com

Such convergence also encourages investment and strategic decision-making in using cyber power as a driver of cyber authority. A strategic neglect of the power-seeking behavior of great powers in cyberspace and the lack of preparation for equal engagement in cyber warfare stem from a lack of forward-looking perspectives and misjudgments about the resources and capabilities tied to cyber power, necessitating action on this issue. The main objective of this research is to identify the components and indicators of cyber power in the defense and security dimension, with the following sub-objectives:
a) Conceptualizing cyber power, b) Cataloging the components and indicators of cyber power in the defense and security dimension, c) Cataloging the macro indicators of cyber power in the defense and security dimension and prioritizing them.

## Methodology

This research is applied-developmental in purpose, descriptive-case in nature, and employs a mixed (qualitative and quantitative) methodology for data analysis. The statistical population includes 50 experts in cyberspace. For the quantitative data analysis, the data collected via a researcher-designed questionnaire were examined using Smart PLS software (Davari, 2014).

## Findings

The results of the study led to the identification of four components within the defense and security dimension of cyber power: the development of cyber defense and passive defense, strengthening the cybersecurity of critical and sensitive infrastructures, equipping with cyber technology and weapons for

Online ISSN: 4520-2676 Print ISSN: 2008-191x

deterrence, and organizing and structuring specialized cyber forces. Additionally, 41 indicators were identified.

The findings indicate that within the defense/security dimension, the component "Equipping with technology and cyber weapons for deterrence" ranks first. Among the indicators within this dimension, the top three are: “Capabilities for acquiring indigenous knowledge of cyber weapons,” “Status of centralized command and management in the defense, security, and military fields,” and “Country’s global cybersecurity index rank.” Furthermore, all components and indicators in this dimension yielded values greater than 1.96.

The five macro indicators of the defense/security dimension of cyber power, ranked in order of importance, are as follows:

1. Capabilities for accessing indigenous knowledge of cyber weapons
2. Status of centralized command and control in defense, security, and military fields
3. Country's Global Cybersecurity Index (GCI) ranking
4. Level of readiness to deal with espionage, information disclosure, and privacy violations in cyberspace
5. Level of development of data-driven companies in the field of cyber weapons production

## Conclusion

This study underscores the importance of acquiring indigenous knowledge, establishing a cyber command and control center, enhancing the cybersecurity index, and preparing to confront cyber threats within the security defense dimension. A deep understanding of these issues by elites and policymakers will

guide the formulation of strategies to secure cyber resources, equip with advanced technologies, and enhance cyber power in this domain.

## References


- Halili, Kh., Valavi, M. R., Movahedisefat, M. R., & Bagheri, M. (2018). The cyber-power based on the fractal approach and its impact on national security in cyberspace. *National Security, 8*(29), 173–200. (in Persian)
- Nye, J. S. (2011). *The future of power*. Belfer Center for Science and International Affairs.
- Davari, A., & Rezazadeh, A. (2014). *Structural equation modeling with PLS software*. Jahad Daneshgahi Publications. (in Persian)

**مقدمه**

در ادوار مختلف زندگی بشر، فناوری نقشی تعیین‌کننده در دستیابی دولت‌ها به قدرت داشته است. در دوران صنعتی، تسلیحات نظامی، در دوران جنگ سرد فناوری هسته‌ای و پس از فروپاشی نظام دوقطبی قدرت، فناوری اطلاعات و ارتباطات و ظهور فضای سایبر، از مهم‌ترین عناصر تأثیرگذار در سنجش قدرت ملی کشورها بوده‌اند. برخورداری از منابع قدرت، جایگاه و نفوذ هر دولت در تعاملات جهانی را نشان می‌دهد.

گستره جهانی تأثیرگذاری فضای سایبر در تمامی عرصه‌های حیات بشری، لزوم مفهوم‌سازی قدرت سایبری را روشن می‌سازد؛ چراکه قدرت سایبری بااینکه همانند قدرت ملی در مرزهای جغرافیایی یک کشور تعریف می‌شود؛ اما دامنه عملیاتی و پیامدهای آن نامحدود است. دستیابی به سطح مطلوبی از قدرت سایبری پیامدهای راهبردی در سطح ملی و صحنه جهانی به همراه خواهد داشت. عرصه حاکمیت و قدرت‌نمایی یک کشور در فضای سایبر همانند فضای واقعی در یک قلمرو سایبری قابل‌تصور است؛ با این تفاوت که قلمرو سایبری مشابه مرزهای جغرافیایی کاملاً حقیقی و محدود نیست؛ بلکه دارای ماهیتی حقیقی - مجازی است.

امروزه جهت‌گیری اولویت‌های راهبری کشورها، به سمت بهره‌برداری از فضای سایبر تغییریافته و فناوری‌های نوین سایبری، زمینه‌ساز تجدید بنای قدرت در قالب قدرت سایبری شده است. دستیابی به سطح مطلوبی از قدرت سایبری پیامدهای راهبردی در سطح ملی و صحنه جهانی به همراه خواهد داشت.

دستیابی به قدرت سایبری، می‌تواند بازوی قدرتمند کشور در صیانت از اهداف عالیه انقلاب اسلامی، جبران‌کننده نقاط ضعف سیاسی، اقتصادی و دفاعی و گسترش نفوذ فرامرزی باشد. در همین راستا، مقام معظم رهبری در شهریور ۱۳۹۴ در بند سوم از حکم اعضای دوره دوم شورای عالی فضای مجازی، به‌طور صریح بر «ارتقای جمهوری اسلامی ایران به قدرت سایبری در تراز قدرت‌های تأثیرگذار جهانی» تأکید فرمودند. نقش برجسته و تأثیرگذاری راهبردی این فضا بر تعاملات و مناسبات بین‌المللی تأییدی بر نگاه حکیمانه و آینده‌نگری خردمندانه معظم له است.

مفهوم قدرت با شکل‌گیری دولت‌ها و تلاش آن‌ها برای کسب قدرت در محدوده مرزهای جغرافیایی در قالب قدرت ملی همواره موردتوجه اندیشمندان بوده است. در هر کشور،

قدرت بر مبنای ایدئولوژی، ارزش‌ها، معیارها و هنجارهای موردتوافق در اختیار حاکمیت قرار گرفته و مشروعیت و مقبولیت آن توسط جامعه به رسمیت شناخته می‌شود.

در سه دهه اخیر، تغییرات شگرف فناوری‌های فضای سایبر این مفهوم را دچار تغییر نموده است. این تغییرات در عرصه حاکمیت در تمامی عناصر اصلی قدرت (جامعه، نظام سیاسی، جغرافیا و منابع ملی) با ظهور مفاهیمی مانند حقوق سایبری، دیپلماسی سایبری، ژئوپلیتیک سایبری و نظام نوین حاکمیت از طریق فضای سایبر و قدرت سایبری خود را نشان داده است. مفهوم قدرت سایبری هرچند با پدیده‌هایی مانند انتشار قدرت و کاهش قدرت دولت‌ها همراه بوده است؛ اما راه برون‌رفت از بحران‌ها و چالش‌های ایجادشده نیز از درون فضای سایبر و بهره‌گیری از فناوری‌های سایبری می‌گذرد. ویژگی‌ها قدرت سایبری مشابه قدرت ملی و تکرار پدیده‌های قدرت ملی در فضای سایبر است که در این تحقیق مورد توجه قرار گرفته است.

**اهمیت و ضرورت تحقیق**

گستره فضای سایبر هرروز فراگیرتر می‌شود و در پیش گرفتن رویکرد انفعالی و تدافعی با پدیده‌های مهم این فضا، حفظ و بقای دولت‌ها را تهدید می‌کند. بازبینی و شناسایی عوامل مؤثر در ارتقاء قدرت ملی در فضای سایبر در قالب قدرت سایبری، از اهمیت بالایی برخوردار است چراکه موجب ترغیب سیاست‌گذاران در تغییر پارادایم فکری و جهت‌گیری مناسب برای در دست گرفتن ابتکار عمل در فضای سایبر خواهد شد.

انجام تحقیقات علمی و گفتمان‌سازی قدرت سایبری در بعد دفاعی و امنیتی موجب همگرایی بازیگران و شکل‌گیری یک درک مشترک برای سیاست‌گذاری در این حوزه می‌شود. و آن‌ها را ترغیب به سرمایه‌گذاری و تصمیم‌گیری در استفاده از قدرت سایبری به‌عنوان پیشران اقتدار سایبری خواهد نمود.

غفلت راهبردی در مواجهه با قدرت‌طلبی قدرت‌های بزرگ در فضای سایبر و عدم کسب آمادگی لازم برای رویارویی هم‌تراز در جنگ‌های سایبری، ناشی از فقدان دیدگاه آینده‌نگر و برآورد نادرست از منابع و توانمندی‌های مرتبط با قدرت سایبری است که ضرورت پرداختن به این موضوع را روشن می‌سازد.

شناخت نادرست از منابع و ظرفیت‌های دفاعی و امنیتی کشور، موجب عدم توجه کافی به قدرت سایبری به‌عنوان یک قدرت بازدارنده خواهد شد که این مسئله از عواقب نپرداختن به تحقیق در این حوزه تلقی می‌شود.

**اهداف تحقیق**

**هدف اصلی**

شناخت مؤلفه‌ها و شاخص‌های قدرت سایبری در بعد دفاعی امنیتی

**اهداف فرعی**

الف) مفهوم‌سازی قدرت سایبری

ب) احصاء مؤلفه‌ها و شاخص‌های قدرت سایبری در بعد دفاعی امنیتی

پ) احصاء شاخص‌های کلان قدرت سایبری در بعد دفاعی امنیتی و اولویت‌بندی آن‌ها

**سؤالات تحقیق**

**سؤال اصلی**

مؤلفه‌ها و شاخص‌های قدرت سایبری در بعد دفاعی امنیتی کدام‌اند؟

**سؤالات فرعی**

الف) مفهوم و ویژگی‌ها قدرت سایبری کدام‌اند؟

ب) مؤلفه‌ها و شاخص‌های قدرت سایبری در بعد دفاعی امنیتی کدام‌اند؟

پ) شاخص‌های کلان قدرت سایبری در بعد دفاعی امنیتی کدام‌اند و اولویت‌بندی آن‌ها چگونه است؟

## مبانی نظری و پیشینه‌های پژوهش

**مبانی نظری**

در این بخش مفاهیم و متغیرهای مرتبط با موضوع تحقیق که از طریق مطالعه در منابع مختلف به دست آمده است اشاره می‌شود.

**۱- قدرت**

در یک نگاه کلی، قدرت به معنی استفاده از منابع مادی و معنوی به‌منظور اعمال اراده و تأثیرگذاری بر دیگران و ایجاد رفتار مطلوب توسط آن‌هاست؛ به‌طوری‌که در فقدان آن، طرف مقابل مجبور، متمایل یا مشتاق به اطاعت نباشد. در تقسیم‌بندی انواع قدرت، دیدگاه‌های مختلفی وجود دارد. جوزف نای، قدرت را به سه دسته نرم (کسب نتیجه مطلوب از طریق جاذبه و بدون استفاده از اجبار یا تطمیع)، سخت (توانایی تغییر رفتار دیگران از طریق اجبار یا تطمیع) و هوشمند (توانایی ترکیب قدرت نرم و قدرت سخت) تقسیم کرده‌اند. (Nye, 2011)

مفاهیمی مانند، قدرت ملی و اقتدار، ازجمله مفاهیم مرتبط با قدرت هستند که از مشتقات قدرت محسوب می‌شوند. از دیدگاه حافظ نیا، قدرت ملی مجموعه‌ای از استعدادها، توانمندی‌ها و ظرفیت‌های یک کشور است که با هدف اعمال و تحمیل اراده جهت دستیابی به اهداف و منافع ملی بکار گرفته می‌شود (حافظ نیا، ۱۳۸۵) به‌عبارت‌دیگر، قدرت ملی مجموعه‌ای از توانایی‌های مادی و معنوی است که در قلمرو یک واحد جغرافیایی و سیاسی به نام کشور یا دولت تعریف می‌شود (حجازی و انعامی، ۱۳۸۷). در هر کشور، اقتدار متضمن مقبولیت و مشروعیت نظام حاکم است و قدرت مشروع در قالب اقتدار معنی می‌شود. به‌عبارت‌دیگر، قدرتی که با ویژگی‌های مشروعیت، نفوذ و کارآمدی همراه باشد را اقتدار می‌نامند. بنابراین می‌توان گفت؛ حلقه اتصال دو مفهوم قدرت و اقتدار، مشروعیت[1] است که به قدرت رسمیت و اعتبار می‌بخشد.

از نظر مفهومی قدرت ملی با اقتدار ملی متفاوت است. تلفیق واژه اقتدار و قدرت ملی به معنای کارآمدی دولت و نظام سیاسی در چارچوبی مشروع و مقبول در محیط ملی و عرصه بین‌المللی است (تبریزی، ۹۵: ۱۳۸۹). از دیدگاه جوزف نای، کشوری که از نظر قدرت ملی از مشروعیت سیاسی کافی برخوردار نیست و یا از نظر اقتصادی و صنعتی فقیر و عقب‌مانده است؛ نمی‌تواند بازیگر لایقی در عرصه بین‌الملل تلقی شود (Nye,2011).

**۲- فضای سایبر**

با مطالعه منابع مختلف منتشرشده، بیش از ۶۵ تعریف برای فضای سایبر وجود دارد و این واژه در معرض برداشت‌های هرمنوتیک[2] قرار گرفته است اما هرکدام از این تعاریف از جنبه‌های خاص و دیدگاه ویژه‌ای به این فضا توجه دارند. یک تعریف دقیق از فضای سایبر باید علاوه بر این‌که دربردارنده مؤلفه‌ها، کاربرد و قابلیت‌های آن باشد از یک منبع رسمی، مسئول و موثق و توسط نهادهای دولتی یا سازمان‌های استاندارد تعریف‌شده باشد.

در بیشتر کشورها تعریف رسمی و یکسانی توسط سازمان‌های ذیصلاح ارائه نشده است و هرکدام از تعریف‌ها معطوف به یک جنبه از کاربردهای فضای سایبر مثلاً توجه به امنیت

1 - Legitimacy
2 - Hermeneutic

سایبر است. با بررسی نقطه اشتراک تعاریف فضای سایبر در منابع مختلف می‌توان تعریف عملیاتی زیر را برای فضای سایبر ارائه داد:

فضای سایبر فضایی فیزیکی و عینی شامل تجهیزات سخت‌افزاری و ملزومات فناوری اطلاعات و ارتباطات که دربردارنده ابعاد غیر فیزیکی ازجمله اطلاعات، نرم‌افزارها، پردازش و خدمات مرتبط با اطلاعات است که به‌منظور همبستگی متقابل بین عوامل انسانی از طریق فضای مجازی متکی به شبکه‌های اینترنتی و تجهیزات مخابراتی به وجود آمده است.

مدل‌های لایه‌ای مختلفی برای توصیف مؤلفه‌های فضای سایبر ارائه شده است. یکی از مدل‌های لایه‌ای مطرح‌شده برای فضای سایبر، مدل چهار لایه‌ای است که توسط شاو[1] در جدول (۱) ارائه شده است (Shaw,2010). در این مدل، چهار مؤلفه کلیدی برای فضای سایبر در هر لایه در نظر گرفته شده است. مؤلفه سیستمی شامل جنبه‌های فنی، زیرساختی و معماری فضای سایبر ازجمله سخت‌افزار و نرم‌افزارهای کاربردی است، مؤلفه محتوا/ کاربرد نیز به اطلاعات تبادلی در فضای سایبر و ابزارهای دستیابی و پردازش آن‌ها اشاره می‌کند. مؤلفه انسانی/ اجتماعی نیز ارتباطات و تعامل میان انسان‌ها و اطلاعات به اشتراک گذاشته‌شده بین آن‌ها را نشان می‌دهد. مؤلفه حاکمیتی، سه مؤلفه قبلی را تحت تأثیر قرار می‌دهد و به‌منظور مدیریت بر تمامی فرایندهای فضای سایبر، در نظر گرفته شده است.

**جدول (۱) مؤلفه‌های فضای سایبر طبق مدل لایه‌ای شاو (شاو، ۲۰۱۰)**

| مؤلفه حاکمیتی (اعمال حاکمیت بر همه جوانب فضای سایبری) | | |
|---|---|---|
| **مؤلفه سیستمی**<br>شالوده، زیرساخت و معماری فنی | **مؤلفه محتوا / کاربرد**<br>پایگاه اطلاعاتی و سازوکارهای دسترسی و پردازش اطلاعات | **مؤلفه انسانی/ اجتماعی**<br>ارتباطات و تعامل‌ها بین انسان‌ها و اطلاعات |

## ۳- قدرت سایبری

قدرت سایبری، نوعی قدرت نوظهور در فضای سایبر است که به‌واسطه فراگیر شدن فناوری اطلاعات و ارتباطات و فضای سایبر به وجود آمده است. ازآنجاکه ماهیت آن، از جنس قدرت در مفهوم عام است؛ باید با تعاریف مطرح‌شده توسط اندیشمندان، همخوانی داشته باشد. قدرت از نظر مفهومی و انتزاعی پدیده‌ای با جلوه‌های ظاهری و

[1] Shaw, Darryl

عینی است. قدرت سایبری نیز از این قاعده مستثنا نیست. امروزه در تمامی کشورها، علاوه بر توجه به منابع مادی قدرت سایبری (قدرت سخت)، رقابت و تلاش سرسختانه‌ای برای کسب و ترویج منابع غیرمادی قدرت سایبری ازجمله فرهنگ، آرمان‌ها، ارزش‌های سیاسی (قدرت نرم) در حال انجام است که پیامدهای این اقدامات در قالب قدرت سایبری تجلی یافته است.

روند تکامل منابع و عوامل قابل‌سنجش در قدرت، در دوره‌های زمانی مختلف از تجهیزات نظامی پیشرفته به تسلیحات هسته‌ای و سپس منابع قدرت در فضای سایبر تغییر یافته است. امروزه استفاده از تسلیحات و زرادخانه‌های سایبری (به‌جای هسته‌ای)، توسعه اقتصادی از طریق فضای سایبر (به‌جای تکیه بر منابع تجدید ناپذیر) و اعمال‌نفوذ توسط رسانه‌های سایبری به شکل گسترده‌ای به‌عنوان منابع قدرت سایبری استفاده می‌شود. بنابراین قدرت سایبری موجب هم‌افزایی و توسعه قابل‌ملاحظه در قدرت می‌شود.

قدرت سایبری از مفاهیم نوظهور قدرت در مهروموم‌های اخیر است. این مفهوم در سطح کشور اولین بار به‌طور صریح توسط مقام معظم رهبری در حکم انتصاب اعضای شورای عالی فضای مجازی (شهریور ۱۳۹۴) موردتوجه قرار گرفت. البته از دیدگاه معظم له، شکل‌دهی به قوانین سایبری، تعامل با کشورها در فضای سایبر و رویکرد اخلاق‌مدارانه سه محور اصلی در قدرت سایبری است.

از دیدگاه دانیل کوهل، قدرت سایبری به معنای توانایی استفاده از فضای سایبر برای ایجاد برتری و تأثیرگذاری روی محیط‌های عملیاتی دیگراست (Kuehl, 2009). زیمت و باری قدرت سایبری را قابلیت کنترل سامانه‌های فناوری اطلاعات و شبکه‌های فضای سایبر می‌دانند که برای انجام مأموریت‌های نظامی و پشتیبانی از حوزه‌های اقتصادی و سیاسی قابل استفاده است (Zimet, and Barry, 2009). جوزف نای قدرت سایبری را قدرت مبتنی بر منابع اطلاعاتی فناوری‌های ارتباطی می‌داند (Nye، 2010). از دیدگاه شلدون، قدرت سایبری توانایی دستیابی به اهداف راهبردی و کاهش توانایی دشمن در بهره‌برداری یا حمله به زیرساخت‌های فضای سایبر است. وی قدرت سایبری را یک ابزار مکمل برای قدرت ملی می‌داند که می‌تواند برای استفاده توسط دولت‌مردان یک کشور جذاب باشد (Sheldon, 2011). از نظر اسپید، قدرت سایبری توانایی یک دولت- ملت برای برقراری، کنترل و اعمال نفوذ در داخل و از طریق فضای سایبر برای پشتیبانی و

پیوستگی با دیگر عناصر حوزه قدرت ملی است (Spade, 2012) در این تعریف دستیابی به قدرت سایبری به توانایی دولت برای توسعه منابع جهت عملیات در فضای سایبر متکی است (هلیلی، ۱۴۰۱).

همان‌طور که در تعاریف فوق دیده می‌شود ماهیت و ویژگی‌های قدرت سایبری با تعاریف سنتی از قدرت و قدرت ملی منطبق است. قدرت سایبری در بعد تهاجمی، با هدف ضربه به زیرساخت‌های حیاتی و تخریب تأسیسات نظامی و هسته‌ای دشمن به‌وسیله حملات سایبری و اجبار و ارعاب کشورها کاربرد دارد. در بعد تدافعی نیز نشان‌دهنده میزان آمادگی یک کشور در مقابله با بحران‌های سایبری و قدرت بازدارندگی است. دستیابی به این قدرت، نسبت به سایر شکل‌های قدرت هزینه کمتری دارد و می‌تواند از طرف کشورهای کوچک برای پیگیری سیاست‌های خود بکار رود. در معاهدات بین‌الملل نیز نمونه‌هایی از توجه به قدرت سایبری دیده می‌شود به‌عنوان‌مثال ناتو از سال ۲۰۰۷ کنترل تهدیدات سایبری و دستیابی به قدرت سایبری را در دستور کار خود قرار داده است. در سال ۲۰۱۱ فضای سایبر را به‌عنوان فضای امنیتی و نظامی مورد توجه قرار گرفت و پذیرش حمله سایبری در سطح حمله نظامی و مجوز دفاع سایبری و اقدام متقابل نظامی به اعضای ناتو مطرح شد. بنابراین قدرت سایبری از موضوعات کلیدی و راهبردی است که باید به‌طور دقیق شناخته‌شده و در سطح ملی بازتعریف شود.

در برنامه پنجم توسعه کشور، ارتقاء توانمندی‌های دفاعی و قدرت بازدارندگی بر مبنای استفاده بهینه از فناوری اطلاعات و ارتباطات مطرح شده است. در برنامه ششم توسعه نیز به کسب جایگاه برتر منطقه در توسعه دولت الکترونیک و افزایش ظرفیت‌های قدرت نرم و دفاع سایبری توجه شده است. همچنین در سند راهبردی امنیت فضای تولید و تبادل اطلاعات(سند افتا)، بر صیانت از منافع، اسرار، حاکمیت و اقتدار ملی تأکید شده است.

دستیابی به قدرت سایبری نقشی مهم و محوری در محافظت از منافع و ارزش‌های ملی دارد و انتظار می‌رود در آینده به نقطه کانونی در روابط بین‌الملل تبدیل شود. هرچند از دیدگاه دشمنان، قدرت سایبری ایران به‌منظور انجام جنگ سایبری، ایجاد اختلال در سامانه‌های موشکی و فرماندهی و کنترل دشمن و سامانه‌های هوایی بدون سرنشین است و همچنان ایران هراسی را در این حوزه القاء می‌کنند.

سلاح‌های سایبری با قابلیت ایجاد تخریب در زیرساخت‌های حیاتی و انهدام تأسیسات نظامی و هسته‌ای دشمن جایگزینی برای سلاح‌های سنتی شده است. برخی سلاح سایبری را یک سلاح پرقدرت مانند سلاح اتمی در نظر نمی‌گیرند بلکه آن‌ها ابزاری مکمل در جنگ‌های متعارف می‌دانند. بااین‌حال، سلاح‌های مدرن سایبری ممکن است اثراتی مخرب‌تر از بمب‌های اتمی را به همراه داشته باشد. به‌عنوان‌مثال اسرائیل در سال ۲۰۰۷ از ابزار سایبری در جنگ با سوریه برای نفوذ به سامانه‌های پدافند هوایی استفاده کرده است. ناوگان دهم و نیروی هوایی بیست و چهارم آمریکا هیچ کشتی و هواپیمایی ندارند و میدان نبرد آن‌ها فضای سایبر است برخی استفاده از سلاح‌های ویرانگر سایبری را به پرل هاربر سایبری تعبیر می‌کنند.

برخی با تأکید بر حوزه نظامی قدرت سایبری و در نظر گرفتن فضای سایبر به‌عنوان قلمرو پنجم جنگ، استفاده از فضای سایبر را برای اهداف، مأموریت‌ها و عملیات نظامی موردتوجه قرار داده‌اند.

در این مقاله، پس از بررسی این مفاهیم در مراجع مختلف، تعریف عملیاتی زیر برای این مفهوم و نیز رویکرد مورداستفاده برای قدرت سایبری ارائه می‌شود:

قدرت سایبری مجموعه‌ای از منابع، ظرفیت‌ها و توانمندی‌های مبتنی بر فضای سایبر است که به‌منظور پشتیبانی از قدرت ملی و دستیابی به اهداف راهبردی در فضای سایبر و خارج از آن قابل استفاده است.

منابع و ظرفیت‌های موجود در فضای سایبر شامل عناصر غیر فیزیکی مانند سلطه اطلاعاتی، وضع قوانین و استانداردها و دیپلماسی سایبری و عناصر فیزیکی مانند زیرساخت‌های اطلاعاتی و ارتباطی، تسلیحات سایبری و غیره است.

## روش‌شناسی پژوهش

این تحقیق از نظر ماهیت، از نوع توصیفی- موردی است چون محقق به دنبال شناخت ویژگی‌های قدرت سایبری است. در تحقیقات توصیفی، محقق دخالتی در موقعیت، وضعیت و نقش متغیرها ندارد و صرفاً با مطالعه آنچه وجود دارد به توصیف و تشریح آن‌ها می‌پردازد. در تحقیقات توصیفی- موردی نیز، ضمن توصیف ویژگی‌ها و صفات یک پدیده خاص به تجزیه‌وتحلیل علّت یا علل برخی از کنش‌ها و واکنش‌های آن پرداخته می‌شود (حافظنیا، ۱۳۹۲: ۷۴).

روش گردآوری داده‌ها در این تحقیق، مطالعه متون و کتاب‌های مرتبط و سایت‌های اینترنتی (عمدتاً مجلات علمی- پژوهشی معتبر) و روش میدانی مصاحبه با خبرگان و پرسشنامه است.

رویکرد مورداستفاده برای تجزیه‌وتحلیل داده‌ها آمیخته (کمی و کیفی) است. برای احصاء مؤلفه‌ها و شاخص‌های قدرت سایبری در بعد دفاعی امنیتی، از روش کیفی فراترکیب[1] استفاده شد. در روش فراترکیب، به‌جای ارائه خلاصه جامعی از یافته‌ها، یک ترکیب (سنتز) تفسیری از یافته‌ها ایجاد می‌شود و یک دید جامع و گسترده نسبت به مسائل به وجود می‌آید (سهرابی و همکاران، ۱۳۹۰). همچنین از جلسات خبرگی برای تثبیت شاخص‌ها و اعتبار آن‌ها استفاده شد. سپس به‌منظور رتبه‌بندی مؤلفه‌ها و شاخص‌های قدرت سایبری در بعد دفاعی امنیتی از یک پرسشنامه بر مبنای طیف لیکرت استفاده شد و بین جامعه آماری توزیع شد.

جامعه آماری این تحقیق، شامل خبرگان و صاحب‌نظران و مدیران آشنا با فضای سایبر و دارای تحصیلات دانشگاهی کارشناسی ارشد و دکتری و سوابق مدیریتی در سطوح راهبردی و سیاست‌گذاری کلان است. پس از جمع‌آوری پرسشنامه از نرم‌افزار اسمارت پی. ال. اس به‌منظور تجزیه‌وتحلیل داده‌های آماری استفاده شد.

## تجزیه و تحلیل داده‌ها

باید توجه داشت که دامنه تأثیرگذاری قدرت سایبری علاوه بر سلطه اطلاعاتی و مهار و کنترل تجهیزات سایبری در حوزه‌های اطلاعاتی و فیزیکی، با تغییر هنجارهای بازیگران فضای سایبر و حوزه شناختی نیز مرتبط است. در فضای سایبر، تهدیدات نوینی ازجمله حملات سایبری، جنگ سایبری، جرائم سایبری، تروریسم سایبری و جاسوسی سایبری، امنیت و منافع ملی کشورها را با چالش مواجه نموده است. مدیریت این تهدیدات و پیشگیری از مخاطرات و آسیب‌پذیری‌های ناشی از آن، کشورها را به چاره‌اندیشی برای حاکمیت بر فضای سایبر واداشته است.

فضای سایبر، دارای ویژگی‌های خاصی ازجمله غلبه حمله بر دفاع (امکانات موجود برای حمله به‌مراتب بیشتر از دفاع است) مشکل انتساب حمله (یافتن منبع حمله معمولاً مشکل است و مهاجمان بدون ترس از عواقب آن اقدام به حمله می‌کنند) و سرعت پیشرفت فناوری

---

[1] Meta Synthesis

(سلاح‌های سایبری و نرم‌افزارها با چنان سرعتی رشد می‌کنند که صرف زمان جهت شناسایی آن‌ها بیهوده است، زیرا به سرعت از دور خارج شده و سلاح‌های جدیدی جای آن‌ها را می‌گیرد) است. این مسئله موجب شده که تهدیدات سایبری در سال ۲۰۱۵ رتبه اول را در لیست تهدیدات بزرگ امنیت ملی داشته باشد.

به‌منظور شناسایی و برآورد قدرت سایبری، باید ارزیابی دقیقی از شاخص‌های سنجش قدرت سایبری، اقدامات سایر کشورها در این زمینه و حوزه‌های تأثیرگذار و تأثیرپذیر قدرت سایبری داشته باشیم که به‌عنوان یافته‌های این تحقیق در این بخش به این موارد پرداخته شده است.

**۱- شاخص‌های سنجش قدرت سایبری**

قدرت سایبری، قدرت برآمده از فضای سایبر است. ازآنجاکه منشأ شکل‌گیری این فضا، فناوری اطلاعات و ارتباطات است؛ رتبه‌بندی کشورهای جهان، توسط سازمان‌های بین‌المللی مانند اتحادیه جهانی مخابرات، سازمان ملل متحد و مجمع جهانی اقتصاد، بر اساس شاخص‌های مرتبط با فاوا، انجام شده است. پنج شاخص مرتبط با این حوزه در این بخش موردبررسی قرار گرفته‌اند که رتبه‌بندی کشورها بر اساس این شاخص‌ها در جدول (۲) آمده است.

۱) شاخص توسعه فناوری اطلاعات و ارتباطات[1] (IDI) که هرساله توسط اتحادیه جهانی مخابرات (ITU)، منتشر می‌شود.

۲) شاخص توسعه دولت الکترونیک (EGDI)[2] هر دو سال یک‌بار توسط سازمان ملل متحد منتشر می‌شود.

۳) شاخص آمادگی شبکه‌ای (NRI)[3]، هرساله توسط مجمع جهانی اقتصاد (WEF)[4] تحت عنوان گزارش جهانی فناوری اطلاعات ارائه می‌شود.

۴) شاخص امنیت سایبری جهانی[5] (GCI) به‌صورت سالانه توسط اتحادیه جهانی مخابرات منتشر می‌شود.

---

[1] ICT Development Index
[2] E-Government Development Index (EGDI)
[3] Networked Readiness Index
[4] World Economic Forum
[5] Global Cybersecurity Index

۵) شاخص‌های قدرت سایبری[1] (CPI) کشورهای گروه ۲۰ توسط گروه اطلاعات اقتصادی[2] (EIU) منتشر شده است.

**جدول(۲) رتبه‌بندی کشورها بر اساس شاخص‌های جهانی**

| ردیف | رتبه بر اساس شاخص IDI | رتبه بر اساس شاخص EGDI | رتبه بر اساس شاخص NRI | رتبه بر اساس شاخص GCI | رتبه بر اساس شاخص CPI |
|---|---|---|---|---|---|
| ۱ | کره جنوبی | دانمارک | سنگاپور | سنگاپور | انگلیس |
| ۲ | ایسلند | استرالیا | فنلاند | آمریکا | آمریکا |
| ۳ | دانمارک | کره جنوبی | سوئد | مالزی | استرالیا |
| ۴ | سوئیس | انگلیس | نروژ | عمان | آلمان |
| ۵ | انگلیس | سوئد | آمریکا | استونی | کانادا |
| ۶ | چین | فنلاند | هلند | موریتانی | فرانسه |
| ۷ | سوئد | سنگاپور | سوئیس | استرالیا | کره جنوبی |
| ۸ | هلند | نیوزیلند | انگلیس | گرجستان | ژاپن |
| ۹ | نروژ | فرانسه | لوکزامبورگ | فرانسه | ایتالیا |
| ۱۰ | ژاپن | ژاپن | ژاپن | کانادا | برزیل |
| ۱۱ | لوکزامبورگ | آمریکا | دانمارک | روسیه | مکزیک |
| ۱۲ | آلمان | آلمان | هنگ‌کنگ | ژاپن | آرژانتین |
| ۱۳ | نیوزیلند | هلند | کره جنوبی | نروژ | چین |
| ۱۴ | استرالیا | نروژ | کانادا | انگلیس | روسیه |
| ۱۵ | آمریکا | سوئیس | آلمان | کره جنوبی | ترکیه |
| ۱۶ | فرانسه | استونی | ایسلند | مصر | آفریقای جنوبی |
| ۱۷ | فنلاند | اسپانیا | نیوزیلند | هلند | هند |
| ۱۸ | استونی | لوکزامبورگ | استرالیا | فنلاند | عربستان |
| ۱۹ | موناکو | ایسلند | چین | سوئد | اندونزی |
| ۲۰ | سنگاپور | استرالیا | اتریش | سوئیس | |

[1] Cyber Power Index
[2] Economist Intelligence Unit

**۲- مطالعه تطبیقی اقدامات راهبردی کشورهای منتخب در زمینه قدرت سایبری**

در بخش قبل، مهم‌ترین شاخص‌های جهانی برای سنجش قدرت سایبری ارائه شده است. در جدول (۳) رتبه ایران و چند کشور دیگر بر مبنای این شاخص‌ها، نشان داده شده است.

**جدول (۳) رتبه ایران در مقایسه با دیگر کشورها با توجه به شاخص‌های عمومی جهانی**

| کشور | رتبه بر اساس شاخص IDI | رتبه بر اساس شاخص EGDI | رتبه بر اساس شاخص NRI | رتبه بر اساس شاخص GCI | رتبه بر اساس شاخص CPI |
|---|---|---|---|---|---|
| ایران | ۸۹ | ۸۶ | ۹۲ | ۶۰ | - |
| کره جنوبی | ۱ | ۳ | ۱۳ | ۱۵ | ۷ |
| انگلیس | ۵ | ۴ | ۸ | ۱۴ | ۱ |
| آمریکا | ۱۵ | ۱۱ | ۵ | ۲ | ۲ |
| استرالیا | ۱۴ | ۲۰ | ۱۸ | ۷ | ۳ |
| فرانسه | ۱۶ | ۹ | ۲۴ | ۹ | ۶ |
| چین | ۶ | ۶۵ | ۵۹ | ۳۲ | ۱۳ |
| ژاپن | ۱۰ | ۱۰ | ۱۰ | ۱۲ | ۸ |

بر اساس اطلاعات این جدول، رتبه جمهوری اسلامی ایران، فاصله زیادی با کشورهای پیشرفته دارد. بااین‌وجود، این شاخص‌ها، شاخص‌های عمومی در سطح جهان است و برای سنجش قدرت سایبری کشورها در تراز جهانی، مبنای دقیقی نیست. کشورهای مختلف با توجه به شرایط سیاسی، اجتماعی و فرهنگی، اولویت‌ها و منافع ملی متفاوتی دارند و ماهیت نامتقارن، پیچیده و پویای فضای سایبر، دستیابی به سطح بالایی از قدرت سایبری را برای کشورهای با رتبه پایین- هرچند به‌صورت موقت و گذرا- امکان‌پذیر نموده است.

با مبنا قرار دادن جدول (۳) دیده می‌شود؛ ده کشور اول را می‌توان بر اساس شاخص IDI به ترتیب شامل کره جنوبی، انگلیس، چین، ژاپن، آلمان، استرالیا، آمریکا، فرانسه، کانادا و ایتالیا در نظر گرفت همان‌طور که در این جدول مشخص شده است ۹ کشور اول هم از نظر شاخص‌های CPI و هم از نظر سایر شاخص‌ها رتبه بالایی دارند. کشور چین بااینکه از نظر شاخص‌های قدرت سایبری در رتبه سیزدهم و پس از برزیل، مکزیک و آرژانتین قرار دارد، اما از نظر شاخص IDI دارای رتبه بالای ۶ است که تفاوت زیادی با این سه کشور دارد. بنابراین به‌منظور انجام مطالعه تطبیقی، با توجه به وجود مستندات منتشرشده، کشورهای آمریکا، استرالیا، دو کشور انگلیس و آلمان از اروپا و دو

کشور ژاپن و چین از آسیا انتخاب و فعالیت‌های مرتبط با قدرت سایبری آن‌ها موردبررسی قرار گرفت که در ادامه اقدامات اساسی کشورهای مختلف در حوزه قدرت سایبری در جدول(۴) آمده است.

**جدول (۴) جمع‌بندی اقدامات اساسی کشورها در حوزه قدرت سایبری**

| | |
|---|---|
| **آمریکا** | • انتشار راهبردها در فضای سایبر برای نمایش قدرت و بازدارندگی<br>• ایجاد فرماندهی سایبری در نیروهای مسلح<br>• سرمایه‌گذاری در فناوری‌های نوین سایبری ازجمله اینترنت اشیاء و ایفای نقش پیشتازی |
| **استرالیا** | • انتشار راهبردهای امنیت سایبری و اتخاذ سیاست تلافی‌جویانه در جنگ سایبری<br>• رویکرد تهدید محور نسبت به حملات در فضای سایبر<br>• تأسیس آکادمی نیروهای دفاعی و سرمایه‌گذاری در زمینه فناوری‌های نظامی در فضای سایبر<br>• توافقنامه با کشورهای پیشرفته در زمینه امنیت سایبری برای کاهش فاصله در قدرت سایبری |
| **انگلیس** | • انتشار راهبردهای امنیت ملی و تأکید بر امنیت سایبری، تهدیدات سایبری و جرائم سایبری<br>• استخدام متخصصان سایبری در نیروهای مسلح<br>• سرمایه‌گذاری در زمینه فعالیت‌های اقتصادی در فضای سایبر<br>• توجه به دیپلماسی سایبری در سطح جهان<br>• تأسیس زیرساخت ملی اطلاعات برای ارتباطات و خدمات امن |
| **آلمان** | • انتشار سند راهبردی در امنیت سایبری و تأکید بر مخاطرات سایبری در تهدید امنیت ملی<br>• راه‌اندازی مرکز فرماندهی فضای سایبر و سیاست‌گذار در حوزه آفند و پدافند سایبری<br>• ایفای نقش پیشگامی در اقتصاد دیجیتال با سرمایه‌گذاری در انقلاب صنعتی چهارم<br>• مشارکت فعال در تعاملات بین‌المللی در حوزه امنیت سایبری |
| **ژاپن** | • ایجاد نهادها و ساختارهای قانونی در فضای سایبر و توجه به دیپلماسی سایبری<br>• اتخاذ رویکرد تدافعی در مواجهه با حملات سایبری(ضعف در مؤلفه امنیت سایبری قدرت)<br>• سرمایه‌گذاری وسیع در دستیابی به فناوری‌های هوشمند و ایجاد جامعه پنجم<br>• ایجاد واحد دفاع سایبری در نیروهای مسلح |
| **چین** | • انتشار اسناد راهبردی و تأکید بر کسب رتبه اول در توانمندی نظامی سایبر و جنگ سایبری<br>• تأکید بر استحکام و تقویت امنیت سایبری<br>• تأسیس اداره مدیریت فضای سایبر<br>• سرمایه‌گذاری در زمینه فناوری‌های کلیدی فضای سایبر مانند اینترنت اشیاء<br>• ایجاد شبکه‌های اجتماعی و موتور جستجوی بومی و عدم وابستگی فناورانه<br>• توسعه اقتصادی در فضای سایبر برای افزایش بعد اقتصادی قدرت سایبری<br>• تأسیس نیروی سایبری (بیش از ۲ میلیون نفر متخصص) |

با بررسی جدول (۴) دیده می‌شود توجه به قدرت سایبری در راهبردهای کلان تمامی کشورها مدنظر قرار گرفته است. همچنین توسعه ابعاد سیاسی، اقتصادی، علم و فناوری و دفاعی امنیتی در این کشورها نسبت به ابعاد اجتماعی و فرهنگی قدرت سایبری پررنگ‌تر است (هلیلی، ۱۳۹۷).

**۳- حوزه‌های تأثیرگذار و تأثیرپذیر قدرت سایبری**

قدرت سایبری قدرت برآمده از فضای سایبر است که می‌تواند به‌منظور اثرگذاری بر فضای سایبر و خارج از آن، مورد استفاده قرار گیرد. در یک نگاه کلی می‌توان حوزه‌های قدرت ساز و تأثیرپذیر از قدرت سایبری را شامل سه حوزه فیزیکی، اطلاعاتی و شناختی در نظر گرفت.

**حوزه فیزیکی**

حوزه فیزیکی شامل مجموعه‌ای از زیرساخت‌های ارتباطی، اطلاعاتی و مدیریت شبکه است. این حوزه، بستر و سنگ بنای فضای سایبر محسوب می‌شود و تصور فضای سایبر بدون آن، امری غیرممکن و دور از ذهن است. تسلط بر حوزه فیزیکی فضای سایبر و انحصار فناوری‌های سایبری، به ابزاری اساسی برای قدرت‌نمایی و تحمیل اراده و خواسته صاحبان فناوری تبدیل شده است. بسیاری از شرکت‌های فراملی نوظهور در فضای سایبر، مانند، گوگل، یاهو، فیس‌بوک، توییتر، اینتل، مایکروسافت و آمازون، با پیشتازی در عرصه‌های فناوری، در مقیاس جهانی، از قدرت و دارایی‌هایی بالاتر از بسیاری از کشورهای مستقل و باسابقه و قدمت تاریخی تبدیل‌شده‌اند. زیرساخت‌های فضای سایبر را می‌توان همان زیرساخت‌های اینترنت در نظر گرفت که در حالت کلی شامل زیرساخت‌های ارتباطی، اطلاعاتی و مدیریت شبکه است.

۱) زیرساخت ارتباطی وظیفه انتقال داده، اطلاعات و محتوا را بین عناصر فضای سایبر(عناصر انسانی و ماشینی) بر عهده دارد. این زیرساخت، واسط اتصال میان اجزای شبکه است.

۲) زیرساخت اطلاعاتی شامل مراکز داده، نرم‌افزارهای متن‌باز (سیستم‌عامل) اپراتورهای اطلاعاتی (موتور جستجو و پست الکترونیکی) است.

۳) زیرساخت‌های مدیریت شبکه به‌منظور تسلط بر دروازه‌های ورود و خروج اطلاعات و امکان مقابله با حملات و تهدیدات سایبری نقش مهمی در برآورد قدرت سایبری یک کشور دارد. این مسئله از طریق مدیریت هویت و دسترسی،

سامانه نام دامنه، زیرساخت کلید عمومی، سامانه‌های پالایش و فیلترینگ و تجهیزات امنیتی انجام می‌شود.

**حوزه اطلاعاتی**

اتمسفر فضای سایبر داده و ویژگی مهم آن تبادل اطلاعات است. امروزه داده و اطلاعات، به‌عنوان یک دارایی و سرمایه مهم برای سازمان‌های دولتی و شرکت‌های خصوصی مطرح می‌شود به‌طوری‌که برخی منابع داده را به نفت دوران جدید تشبیه می‌کنند. استخراج اطلاعات و دانش از این داده‌ها از فناوری‌های کلیدی فضای سایبر محسوب می‌شود. برتری اطلاعاتی و حاکمیت داده از موضوعات مهمی است که در قدرت سایبری باید به آن توجه نمود. در حوزه اطلاعاتی برای شناخت عوامل مؤثر و قدرت‌زا باید محتوا و خدمات مبتنی بر محتوا را موردتوجه قرار داد.

**حوزه شناختی**

فضای سایبر، نگاشتی از فضای واقعی است که نسل جدیدی از افراد و جوامع شبکه‌ای با هویت مجازی و سبک زندگی متفاوت را به وجود آورده است. این فضای مصنوع بشر، در حال تبدیل‌شدن به بخشی جدانشدنی از زندگی تمامی انسان‌ها است. بسیاری از خدمات ارائه‌شده در فضای سایبر دارای زمینه مشترک تمرکزیافته بر افراد است. استفاده از اصطلاحاتی مانند کاربرگرا[۱]، انسان‌گرا[۲]، مردم مدار[۳]، مبتنی بر کاربر[۴] و پاسخگو به کاربر نشانگر اهمیت کاربر به‌عنوان بهره‌بردار نهایی از فضای سایبر است (مجیدی، ۱۳۹۵).

فضای سایبر فضایی مصنوعی و ساخته‌شده توسط بشر و از بزرگ‌ترین اختراعات بشری است و کاربر، مصرف‌کننده و بهره‌بردار اصلی از این فضاست. ایده شکل‌گیری و ایجاد این فضا، در ظاهر برای سهولت تعامل و ارتباط افراد در جوامع مختلف است؛ اما در نگاهی عمیق‌تر، فلسفه وجودی آن فراتر از یک ابزار فناوارانه ارتباطی است. انتخاب اصطلاح سایبر برای این فضا، مؤید توجه به مفهوم سکان‌داری، کنترل، هدایت و تأثیرگذاری بر ادراک دیگران به‌منظور تحت تأثیر قرار دادن مغز (قوه تعقل و تصمیم‌گیری) و قلب (منبع احساسات و عواطف) از طرف معماران و سازندگان آن است.

---

[1] User Oriented
[2] Human Centered
[3] People Centered
[4] User Based

این دیدگاه، انطباق کارکرد اصلی این فضا با مفهوم قدرت را مشخص می‌سازد. همان‌طور که در مبانی نظری اشاره شد؛ قدرت به معنی استفاده از منابع مادی و معنوی به‌منظور اعمال اراده و تأثیرگذاری بر دیگران برای ایجاد رفتار مطلوب توسط آن‌هاست. امروزه کاربران به‌محض ورود به این فضا به‌طور ناخواسته و اجتناب‌ناپذیر در دام وب جهان‌گستر این فضا گرفتار می‌شوند و افکار و رفتار آن‌ها جهت‌دهی می‌شود. در جهان امروزی، بااینکه ورود به این فضا اختیاری - و البته تا حد زیادی اجباری و فراگیر است- اما میزان تأثیرپذیری کاربر به میزان شناخت، مهارت و نوع بهره‌برداری وی از این فضا، بستگی دارد.

هدف اصلی و نهایی قدرت سایبری اثرگذاری بر کاربران و تغییر و تعیین ترجیحات و مطلوبیت‌های آن‌هاست. این مفهوم بااینکه در مقیاس کوچک و سطوح فردی نیز استفاده می‌شود؛ اما مفهومی کلان و راهبردی است که در تلاش برای دستیابی به سلطه ایدئولوژیک و استیلای اعمال کننده قدرت بکار می‌رود. ازآنجاکه این اعمال قدرت در تمامی ابعاد هفتگانه قدرت به چشم می‌خورد؛ بنابراین قدرت سایبری، در مقیاس قدرت ملی و نگاشتی از آن در فضای سایبر قابل‌طرح و بررسی است.

در حوزه شناختی، موضوعات روان‌شناختی و جامعه‌شناختی کاربران فضای سایبر نقش آن‌ها در تولید و تأثیرپذیری از قدرت سایبری موردتوجه قرارگرفته است. از منظر روان‌شناختی، ویژگی‌های شخصیتی کاربر انسانی مانند افکار، احساسات، باورها و ارزش‌های پذیرفته‌شده، در تأثیرپذیری و تأثیرگذاری بر قدرت سایبری موردتوجه قرار می‌گیرد. همچنین از منظر جامعه‌شناختی، کنش‌ها، رفتار و فعالیت‌های کاربران و نحوه تعامل و ارتباطات میان آن‌ها در فضای سایبر و نقش آن در نیل به قدرت سایبری و افزایش یا افول آن در یک کشور حائز اهمیت است. در واقع منشأ بروز و ظهور قدرت سایبری در حوزه‌های فیزیکی و اطلاعاتی، که در بخش‌های قبلی بررسی شد، به میزان اهمیت بخشی و بهره‌برداری از قدرت سایبری در حوزه شناختی برمی‌گردد.

**۴- ابعاد قدرت سایبری**

مفهوم اقتدار، با حاکمیت ارتباط نزدیکی دارد و در بسیاری از منابع از آن با عنوان اقتدار ملی یاد می‌شود. اقتدار ملی، بیانگر قدرت مشروعی است که از طرف جامعه در اختیار حاکمان قرار می‌گیرد. امروزه، در فضای سایبر،بخش عمده‌ای از منابع قدرت، در اختیار شرکت‌های فراملی و سازمان‌های غیردولتی است؛ بااین‌حال، مفهوم قدرت سایبری در

حیطه مرزهای جغرافیایی و در حوزه عملکرد دولت‌ها تعریف می‌شود. این بدان معنا است که قدرت سایبری از جنس قدرت حاکمیت (اقتدار) و بیانگر توانمندی‌های یک دولت برای تسلط بر فضای سایبر در سطح ملی است که در یک چارچوب مشروع و موردقبول، در اختیار دولت‌ها قرار گرفته است.

از آنجا که فضای سایبر، انعکاس و نگاشتی از تمامی پدیده‌های فضای واقعی است. قدرت در فضای سایبر نیز، تمامی ویژگی‌ها و ابعاد قدرت در فضای واقعی را دارد. بر این اساس، در این تحقیق، به قدرت سایبری ابعاد قدرت سایبری، هم‌سطح با قدرت ملی در نظر گرفته شده و ابعاد هفتگانه سیاسی، اجتماعی، فرهنگی، علم و فناوری، دفاعی/امنیتی و حقوقی/ قضایی برای قدرت سایبری فرض شده است در مطالعه گروهی با عنوان الگوی راهبردی توسعه و تحکیم اقتدار ملی جمهوری اسلامی ایران برای اقتدار، ابعاد هفتگانه سیاسی، اجتماعی، فرهنگی، علم و فناوری، دفاعی/امنیتی و حقوقی/ قضایی در نظر گرفته شده است (مطالعه گروهی، ۱۳۸۹).

اولویت‌بندی، برنامه‌ریزی راهبردی و سیاست‌گذاری در هرکدام از این ابعاد، میزان شناخت نخبگان و سیاست‌گذاران از ابعاد قدرت سایبری را نشان می‌دهد. در این بخش مؤلفه‌ها و شاخص‌های قدرت سایبری در بعد دفاعی امنیتی احصاء شده است.

قدرت سایبری در جمهوری اسلامی ایران، متأثر از عوامل مختلفی است که شناخت این عوامل، سیاست‌گذاری کلان در ابعاد، حوزه‌های تأثیرگذار و تأثیرپذیر و معیارهای قدرت سایبری را تحت تأثیر قرار می‌دهد. تأکید صریح مقام معظم رهبری در مورد ارتقاء قدرت سایبری و توجه به آن به‌صورت ضمنی در اسناد بالادستی نشان‌دهنده اهمیت راهبردی این شکل نوین از قدرت در سطح ملی و تعاملات بین‌المللی است. همچنین ماهیت ملی و فرا سازمانی قدرت سایبری، لزوم توجه به تبیین خطوط راهنما، ارزش‌های مطلوب، اهداف، سیاست‌های بالادستی، راهبردها و دکترین قدرت سایبری را برای مواجهه فعال و ابتکار عمل در تعاملات منطقه‌ای و فراملی روشن می‌سازد (هلیلی و همکاران، ۱۳۹۷).

**۵- قدرت سایبری در بعد دفاعی/امنیتی**

دفاع سایبری شامل قابلیت‌های سازمان‌یافته برای محافظت در مقابل یا کاهش و بازیابی اثرات حمله سایبری استفاده می‌شود. دفاع سایبری بر محافظت از زیرساخت‌های حیاتی در زمان حمله تمرکز دارد. درحالی‌که بازدارندگی سایبری در پی منصرف ساختن

حمله‌کنندگان است و بر نامطلوب جلوه دادن حمله و نه لزوماً جلوگیری از آن تأکید دارد (فرخی و محمدی، ۱۳۹۳).

در صورتی‌که کشوری بتواند با انجام اقدامات بازدارنده از نوع انکار یا مقابله‌به‌مثل، فکر حمله را از دشمن دور کند از قدرت سایبری در تراز جهانی برخوردار است. این کار می‌تواند از طریق انجام رزمایش‌های سایبری، ترسیم خطوط قرمز، نشان دادن قدرت مقابله با حملات سایبری و توانمندی محافظت از زیرساخت‌های حیاتی انجام شود. نمایش قدرت سایبری تأثیر زیادی در افزایش بازدارندگی دارد و پیامد آن نیز، ارتقاء امنیت ملی و حفظ منافع ملی است.

کاهش آسیب‌پذیری‌ها و توانایی مقابله با تهدیدات همواره از دغدغه‌های مهم در کشورها محسوب می‌شود. به خاطر وابستگی زیرساخت‌های حیاتی و سامانه‌های ارتباطی به فضای سایبر، مصون‌سازی، امنیت، حفاظت از زیرساخت‌های حیاتی، آمادگی پاسخگویی به حوادث امنیتی و تاب‌آوری و بازیابی در شرایط بحران در راهبردهای اکثر کشورها وجود دارد. در سال‌های اخیر، زیرساخت‌های سایبری کشور ما، مورد هجوم تهدیدات سایبری مانند جاسوسی، خرابکاری، تروریسم و ویروس‌های مخرب، قرار گرفته است. نمونه بارز آن، حمله سایبری استاکس نت در جهت تخریب فیزیکی سانتریفیوژهای تأسیسات هسته‌ای است. ویروس استارس[1] (جاسوسی و تخلیه اطلاعات هسته‌ای)، دوکو[2] (جاسوسی صنعتی)، گاوس (تخلیه اطلاعات بانکی)، و فلیم[3] (از کار انداختن تجهیزات نفتی) از دیگر حملات سایبری مهم با منشأ خارجی است.

در سند راهبردی پدافند سایبری کشور نیز، بومی‌سازی و امنیت سامانه‌های سایبری مطرح شده است. راه‌اندازی مراکز ماهر و گوهر و ساختار پدافند غیرعامل سایبری در این راستا انجام شده است. در ماده (۸) سند راهبردی پدافند سایبری کشور (۱۳۹۴)، راهبردهایی مانند طراحی برنامه‌های پدافند سایبری برای مصون‌سازی زیست‌بوم سایبری در برابر تهدیدات و تهاجم سایبری، متناسب با سطح اهمیت آن‌ها، مدیریت ارتقاء ضریب پایداری و مصون‌سازی زیرساخت‌های حیاتی در برابر تهدیدات و حملات سایبری آمده است.

---

[1] Stars
[2] Duqu
[3] Flame

ایران در شاخص جهانی امنیت سایبری[1] حائز رتبه ۶۰ جهانی است. در اسناد بالادستی کشور، امنیت سایبری در حوزه‌های فیزیکی و اطلاعاتی مطرح شده است. در برنامه پنجم توسعه سند امنیت فناوری اطلاعات (سند افتا) به‌عنوان یک سند لازم‌الاجرا برای دولت شناخته شده است. در این سند بر به‌کارگیری نظام مدیریت امنیت اطلاعات، مراکز عملیات امنیت و گروه واکنش هماهنگ رخدادهای امنیتی (گوهر) تأکید شده است. در لایه خدمات و محتوا استانداردها و سیاست‌های امنیتی مانند محرمانگی[2]، یکپارچگی[3] و در دسترس بودن[4] اهمیت زیادی دارد؛ بااین‌حال، امنیت فضای سایبر به خاطر گستردگی شبکه‌ها، پروتکل‌ها، تجهیزات و فرایندها، فراتر از این سه معیار است. در فضای سایبر معیارهایی دیگری مانند کنترل و مالکیت بر ورود محتوا و احراز هویت استفاده‌کنندگان از خدمات، استفاده بهینه و به‌روزرسانی سامانه‌ها، مسائل مربوط به ایمنی و زیست‌محیطی و غیره نیز باید در طراحی، پیاده‌سازی، نگهداری و بهره‌برداری برای افزایش امنیت سایبری مدنظر قرار گیرد.

در حوزه شناختی نیز امنیت به‌صورت ذهنی و عین باید موردتوجه قرار گیرد. در امنیت ذهنی، اعتماد کاربران به صیانت از حریم خصوصی و اطمینان از سیاست‌گذاری و حکمرانی و در امنیت عینی فقدان تهدید نسبت به منافع و ارزش‌های فردی و ملی توسط کاربران به‌صورت ملموس حائز اهمیت است و این مسئله در افزایش قدرت سایبری غیرقابل‌انکار است.

با پایان یافتن دوران جنگ سرد، شکل‌های نوینی از جنگ در قالب، جنگ اطلاعات، جنگ سایبر و جنگ شبکه‌های کامپیوتری در راهبردهای نظامی کشورها موردتوجه قرار گرفته است. در این صحنه نوین از نبرد، حملات سایبری با اهداف تخریب و جاسوسی انجام می‌شود. سلاح‌های سایبری با قابلیت ایجاد تخریب در زیرساخت‌های حیاتی و انهدام تأسیسات نظامی و هسته‌ای دشمن جایگزینی برای سلاح‌های سنتی شده است. برخی سلاح سایبری را یک سلاح پرقدرت مانند سلاح اتمی در نظر نمی‌گیرند بلکه آن را ابزاری مکمل در جنگ‌های متعارف می‌دانند. بااین‌حال، سلاح‌های مدرن سایبری ممکن است اثراتی مخرب‌تر از بمب‌های اتمی را به همراه داشته باشد. به‌عنوان‌مثال

[1] Global Cybersecurity Index (GCI)
[2] Confidentially
[3] Integrity
[4] Availability

اسرائیل در سال ۲۰۰۷ از ابزار سایبری در جنگ با سوریه برای نفوذ به سامانه‌های پدافند هوایی استفاده کرده است. ناوگان دهم و نیروی هوایی بیست و چهارم آمریکا هیچ کشتی و هواپیمایی ندارند و میدان نبرد آن‌ها فضای سایبر است.

فضای سایبر بستر شکل‌گیری و بروز بسیاری از تهدیدات ملی و بین‌المللی است و مقابله با این تهدیدات در راهبردهای اکثر کشورها و موافقت‌نامه‌های بین‌المللی امنیت سایبری موردتوجه قرار گرفته است.

پیش‌نیاز ارتقاء قدرت سایبری توسعه زیرساخت‌های سایبری است چراکه زیرساخت‌های سایبری یک سرمایه ملی محسوب می‌شود. بااینکه سرمایه‌گذاری وسیع در حوزه زیرساخت‌های سایبری، قدرت سایبری بالاتری را به همراه خواهد داشت؛ اما ممکن است موجب آسیب‌پذیری بیشتری شود. برای پیشگیری از این مخاطرات و آسیب‌پذیری‌ها، ضروری است،بخش عمده‌ای از سرمایه‌گذاری در این زمینه، به امنیت سایبری اختصاص یابد.

همگرایی نهادهای سیاست‌گذار در توسعه امور سایبری و تشکیل ساختارهای قانونی، ضابطین انتظامی و امنیتی، زمینه لازم را برای تحرک بخشی، اثربخشی و کارآمدی در مدیریت فضای سایبر و ارتقاء قدرت سایبری در حوزه دفاعی امنیتی در پی خواهد داشت.

در سازمان‌های دفاعی و امنیتی حضور پلتفرم‌ها و تجهیزات خارجی، نفوذ و استیلای صاحبان فناوری را به همراه دارد. بنابراین باید سازوکاری برای تبعیت از قوانین ملی کشور در این زمینه فراهم شود. درعین‌حال، پیش‌نیاز دستیابی به قدرت سایبری، استحکام ساخت درونی قدرت سایبری، از طریق توجه به اراده ملی حکمرانان و مسئولان در مدیریت و اعمال حقوق و قوانین، الزامات، معیارها و نیازمندی‌های قدرت سایبری در سطح ملی و حاکمیت است.

**۶- جمع‌بندی یافته‌های تحقیق**

پس از انجام تحقیقات و بررسی‌های لازم در ادبیات و مبانی نظری تحقیق و جلسات خبرگی، مؤلفه‌ها و شاخص‌های مؤثر در بعد دفاعی امنیتی قدرت سایبری مطابق جدول (۵) احصاء شده است.

**جدول (۵) مؤلفه‌ها و شاخص‌های بعد دفاعی امنیتی قدرت سایبری**

| | |
|---|---|
| **توسعه دفاع سایبری و پدافند غیرعامل** | • قابلیت‌های بهره‌برداری عملیاتی از فضای سایبر در حوزه دفاعی امنیتی<br>• توانمندی‌های پدافند غیرعامل در برابر تهدیدات سایبری<br>• میزان تاب‌آوری و پایداری سامانه‌های دفاعی در تهاجم سایبری<br>• کارایی راهبردهای دفاع سایبری در مقابله با حملات سایبری<br>• وضعیت نظام کنترل و پایش مخاطرات و امداد و نجات سایبری در کشور<br>• توانمندی دولت در رصد، پایش و فیلترینگ هوشمند محتوا<br>• توانمندی دولت در مقابله با چالش‌های ناشی از محتوای ضد امنیتی<br>• میزان آمادگی شبکه‌ای در مواجهه با مخاطرات و تهدیدات امنیتی<br>• میزان نفوذ، اشراف اطلاعاتی و اعمال حاکمیت در فضای سایبر<br>• توانایی شناسایی جریان‌های معاند، دگراندیش و تهدیدکننده امنیت ملی<br>• میزان آمادگی مقابله با جاسوسی، افشای اطلاعات و نقض حریم خصوصی در فضای سایبر |
| **تقویت امنیت سایبری زیرساخت‌های حیاتی و حساس** | • توانمندی حفاظت از زیرساخت‌های حیاتی در برابر حملات سایبری<br>• وضعیت مصونیت سامانه‌های دفاعی در فضای سایبر<br>• توانایی شناسایی و رفع نقاط ضعف و آسیب‌پذیری‌های سایبری سامانه‌های دفاعی<br>• میزان توسعه مراکز تحقیقاتی امنیت سایبری<br>• میزان توسعه خدمات الکترونیک امن در سازمان‌های دفاعی<br>• رتبه شاخص امنیت سایبری جهانی کشور (شاخص GCI)<br>• شاخص امنیت سایبری در خدمات ابری<br>• ظرفیت و کار آیی سامانه‌های امنیت اطلاعات بومی در مقابله با مخاطرات سایبری<br>• میزان تاب‌آوری زیرساخت‌های حساس، حیاتی و مهم کشور در بحران‌های سایبری<br>• میزان حفاظت از مراکز داده در برابر حملات سایبری<br>• میزان رعایت استانداردها و سیاست‌های امنیتی از طرف کاربران<br>• میزان توسعه مکانیسم‌های امنیتی مانند احراز هویت و کنترل دسترسی<br>• میزان حضور فعال و مؤثر در کنوانسیون‌ها و مجامع منطقه‌ای و جهانی امنیت سایبری |

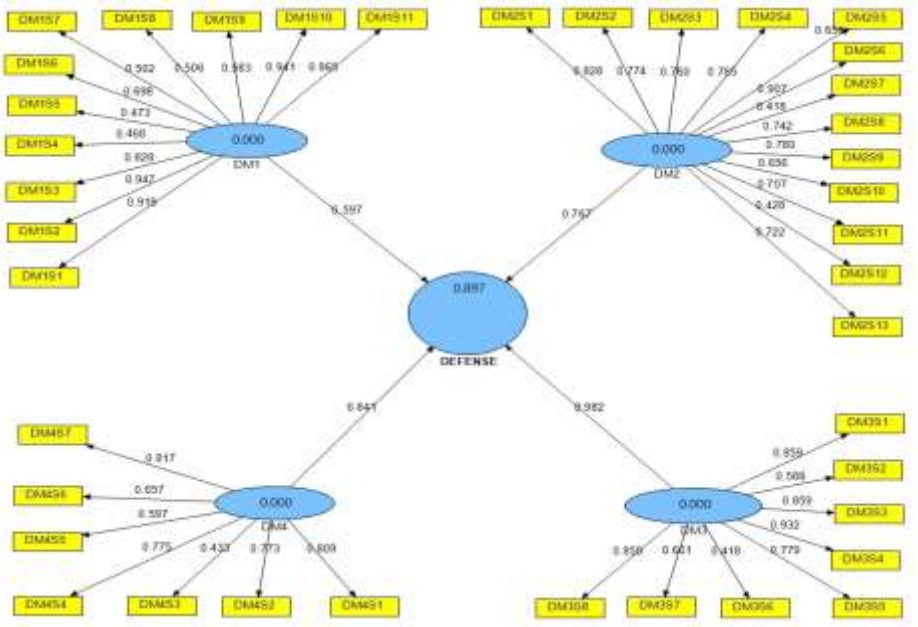
| | |
|---|---|
| **مجهز شدن به فناوری و تسلیحات سایبری به‌منظور بازدارندگی** | • وضعیت سامانه‌های فرماندهی و کنترل در فضای سایبر<br>• وضعیت یکپارچگی و ساماندهی فعالیت‌های مرتبط با عملیات نظامی سایبری<br>• میزان هماهنگی و تعامل سازمان‌های دفاعی با سایر سازمان‌ها در فضای سایبر<br>• قابلیت‌های دستیابی به دانش بومی تسلیحات سایبری<br>• میزان توسعه زیرساخت‌های ارتباطی مستقل، امن و پایدار دفاعی<br>• میزان توسعه سامانه‌های رصد و پایش محتوا<br>• توانایی رصد و دیده‌بانی روندهای آینده امنیتی در فضای مجازی<br>• رصد روندها و پیشران‌های نوظهور مؤثر در تغییر ساختار حکمرانی ازجمله زنجیره بلوکی، اینترنت اشیا، هوش مصنوعی و رباتیک<br>• وضعیت استقلال شبکه ملی اطلاعات از شبکه جهانی اینترنت |
| **سازمان‌دهی و ساختارسازی نیروی سایبری متخصص** | • وضعیت فرماندهی و مدیریت متمرکز در حوزه‌های دفاعی، امنیتی و نظامی<br>• وضعیت به‌کارگیری سایبر در جنگ سایبری، شامل قلمرو عملیات کلاسیک و ترکیبی<br>• وضعیت سازمان‌دهی و ساختار نیروی سایبری<br>• وضعیت شناسایی، به‌کارگیری و هدایت نیروی انسانی متخصص و نخبه<br>• وضعیت پاسگان سایبری و بسیج مردمی در فضای سایبر<br>• میزان آمادگی نیروهای مسلح در حوزه نبرد سایبری و به‌کارگیری سایبر در رزم<br>• میزان تولید آموزش‌های تخصصی و محتوای غنی درزمینهٔ امنیت سایبر<br>• میزان بهره‌گیری از بخش خصوصی و دانشگاهی در تولید تجهیزات امنیتی بومی |

در مرحله بعد به‌منظور بررسی میزان تأثیر هرکدام از مؤلفه‌ها و شاخص‌های به‌دست‌آمده بر قدرت سایبری در بعد دفاعی امنیتی و اولویت‌بندی مؤلفه‌ها و شاخص‌ها، از یک پرسشنامه محقق ساخته استفاده شده است. پس از دریافت نظرات جامعه آماری، داده‌های جمع‌آوری‌شده توسط نرم‌افزار اسمارت پی ال اس مورد ارزیابی قرار گرفته است.

در این نرم‌افزار برای سنجش پایایی شاخص‌ها از ضرایب بار عاملی استفاده‌شده است. محاسبه ضرایب بار عاملی، یکی از روش‌های ارزیابی پایایی ابزار اندازه‌گیری است که میزان همبستگی شاخص‌های یک سازه با آن را مشخص می‌سازد. هرچه مقدار بار

عاملی یک متغیر در رابطه با یک سازه مشخص بیشتر باشد آن متغیر سهم بیشتری در تبیین آن سازه ایفا می‌کند (داوری و رضازاده، ۱۳۹۳).

پس از اجرای نرم‌افزار، درصورتی‌که ضرایب بار عاملی به‌دست‌آمده برای هر شاخص، کمتر از ۰/۴ باشند، این شاخص قابل‌حذف است. ضرایب بار عاملی هرکدام از مؤلفه‌های چهارگانه و شاخص‌ها پس از حذف شاخص‌های با ضریب بار عاملی پایین‌تر از ۰/۴ در شکل (۱) نشان داده شده است.




**شکل (۱) ضرایب بار عاملی بعد دفاعی/امنیتی**

## نتیجه‌گیری و پیشنهادها

در این تحقیق برای تعیین همبستگی میان متغیرها از آزمون معناداری Z (مقادیر t-Value) استفاده می‌شود. در نرم‌افزار Smart Pls این کار از روش خودگردان‌سازی (بوت استراپ) انجام می‌شود. در این حالت اگر ضرایب معناداری Z به‌دست‌آمده از ۱/۹۶ بیشتر باشد یعنی در سطح اطمینان ۵٪ همبستگی‌های مشاهده‌شده، معنادار است (اسفیدانی و محسنین، ۱۳۹۳: ۴۸).

محاسبه ضرایب Z برای مؤلفه‌ها و شاخص‌های بعد دفاعی امنیتی قدرت سایبری در جدول (۶) آمده است. از این ضرایب می‌توان برای رتبه‌بندی متغیرهای تحقیق استفاده کرد.

**جدول (۶) رتبه‌بندی مؤلفه‌ها و شاخص‌های بعد دفاعی/ امنیتی قدرت سایبری**

| مؤلفه | ضریب t-value | رتبه |
|---|---|---|
| DM1 | 8/153 | 4 |
| DM2 | 9/078 | 3 |
| DM3 | 12/509 | 1 |
| DM4 | 10/353 | 2 |

| شاخص | ضریب t-value | رتبه |
|---|---|---|
| DM1S1 | 34/547 | 26 |
| DM1S2 | 103/497 | 5 |
| DM1S3 | 85/140 | 9 |
| DM1S4 | 43/713 | 25 |
| DM1S5 | 11/855 | 32 |
| DM1S6 | 2/716 | 37 |
| DM1S7 | 82/557 | 10 |
| DM1S8 | 10/428 | 35 |
| DM1S9 | 62/693 | 19 |
| DM1S10 | 10/453 | 34 |
| DM1S11 | 111/220 | 4 |
| DM2S1 | 81/887 | 11 |
| DM2S2 | 10/837 | 33 |
| DM2S3 | 2/067 | 39 |
| DM2S4 | 81/275 | 12 |
| DM2S5 | 2/650 | 38 |
| DM2S6 | 112/375 | 3 |
| DM2S7 | 9/455 | 36 |
| DM2S8 | 61/915 | 20 |
| DM2S9 | 87/653 | 8 |
| DM2S10 | 53/631 | 23 |
| DM2S11 | 34/308 | 27 |

| شاخص | ضریب t-value | رتبه |
|---|---|---|
| DM2S12 | 20/902 | 31 |
| DM2S13 | 73/965 | 13 |
| DM3S1 | 91/284 | 7 |
| DM3S2 | 23/048 | 30 |
| DM3S3 | 62/976 | 18 |
| DM3S4 | 119/418 | 1 |
| DM3S5 | 55/334 | 21 |
| DM3S6 | 64/391 | 17 |
| DM3S7 | 29/251 | 29 |
| DM3S8 | 69/883 | 14 |
| DM4S1 | 113/024 | 2 |
| DM4S2 | 100/616 | 6 |
| DM4S3 | 49/175 | 24 |
| DM4S4 | 32/068 | 28 |
| DM4S5 | 67/002 | 15 |
| DM4S6 | 55/061 | 22 |
| DM4S7 | 66/989 | 16 |

نتایج حاصل از این تحقیق نشان می‌دهد، در بعد دفاعی/ امنیتی، مؤلفه «مجهز شدن به فناوری و تسلیحات سایبری برای بازدارندگی» رتبه اول را دارد و در میان شاخص‌های بعد دفاعی/ امنیتی نیز، شاخص‌های «قابلیت‌های دستیابی به دانش بومی تسلیحات سایبری»، «وضعیت فرماندهی و مدیریت متمرکز در حوزه‌های دفاعی، امنیتی و نظامی» و «رتبه شاخص امنیت سایبری جهانی کشور» به ترتیب رتبه‌های اول تا سوم را به خود اختصاص داده‌اند. همچنین در این بعد، تمامی مؤلفه‌ها و شاخص‌ها، دارای مقادیر بزرگ‌تر از ۱/۹۶ هستند.

با توجه به رتبه‌بندی انجام‌شده پنج شاخص کلان بعد دفاعی امنیتی قدرت سایبری به ترتیب عبارت‌اند از:

۱) قابلیت‌های دستیابی به دانش بومی تسلیحات سایبری

۲) وضعیت فرماندهی و مدیریت متمرکز در حوزه‌های دفاعی، امنیتی و نظامی
۳) رتبه شاخص امنیت سایبری جهانی کشور (شاخص جی سی آی)
۴) میزان آمادگی مقابله با جاسوسی، افشای اطلاعات و نقض حریم خصوصی در فضای سایبر
۵) میزان توسعه شرکت‌های داده بنیان در حوزه تولید تسلیحات سایبری

## نتیجه‌گیری و پیشنهادها

بر اساس رتبه‌بندی شاخص‌های احصاء شده تلاش برای دستیابی به دانش بومی تسلیحات سایبری، ایجاد فرماندهی و مدیریت متمرکز سایبری در حوزه‌های دفاعی، امنیت و نظامی، ارتقاء رتبه شاخص امنیت سایبری کشور با رعایت ملاحظات امنیتی، کسب آمادگی‌های لازم برای مقابله با جاسوسی، افشای اطلاعات و نقض حریم خصوصی در کنار توسعه شرکت‌های دانش‌بنیان می‌تواند راهکارهایی برای دستیابی به قدرت سایبری در نظر گرفته شود.

به‌منظور برنامه‌ریزی راهبردی، برای استفاده از توانمندی‌های کشور در بعد دفاعی امنیتی قدرت سایبری ابتدا، لازم است نسبت به انجام تحقیقات آینده‌پژوهانه در زمینه فناوری‌های نوین و برهم زن اقدام شود. علاوه بر آن برآورد درستی از ظرفیت‌ها و منابع قدرت سایبری موجود کشور صورت گیرد تا بر اساس آن، وظایف و مسئولیت‌های سازمان‌ها و دستگاه‌های اجرایی مختلف در نیروهای مسلح مشخص شود.

شاخص‌های کلان احصاء شده در بعد دفاعی و امنیتی می‌تواند توسط سازمان‌های مرتبط مانند قرارگاه سایبری و نیروهای مسلح موردمطالعه و استفاده قرار گیرد. این مسئله مستلزم تدوین شاخص‌های مطرح‌شده و اندازه‌گیری آن‌ها برای تعیین وضع موجود قدرت سایبری کشور است.

سنجش شاخص‌های قدرت سایبری به‌دست‌آمده، نیازمند همگرایی و هم‌راستایی دیدگاه‌های مختلف بازیگران و ذینفعان فضای سایبر و درک و شناخت اهمیت قدرت سایبری است. این مسئله نیز، نیازمند رصد و دیده‌بانی اقدامات راهبردی سایر کشورها و آینده‌نگری کلان‌روندهای جهانی است که از طریق تشکیل کارگروه‌های تخصصی و نهادسازی در سازمان‌های ذی‌ربط قابل انجام است.

**قدردانی**

از خبرگان توانمندی که در طول پژوهش، دانش خویش را سخاوتمندانه در اختیار محققان این پژوهش قرار دادند و استواری پژوهش حاضر بر مشارکت و دانش این بزرگواران قرارگرفته است، بسیار سپاسگزاریم.

**منابع**

- امام خامنه‌ای (مدظله‌العالی)، *مجموعه بیانات قابل‌دسترسی* در: www.farsi.khamenei. ir
- اسفیدانی، محمدرحیم و شهریار محسنین. (۱۳۹۳). *معادلات ساختاری مبتنی بر رویکرد حداقل مربعات جزئی به کمک نرم‌افزار Smart PLS*. تهران: مهربان.
- حافظ نیا، محمدرضا. (۱۳۹۲). *مقدمه‌ای بر روش تحقیق در علوم انسانی*. چاپ نوزدهم. انتشارات سمت. تهران.
- حافظ‌نیا، محمدرضا. زرقانی، سید هادی، احمدی پور، زهرا و رکن‌الدین، عبدالرضا. (۱۳۸۵). "طراحی مدل سنجش قدرت ملی کشورها". *فصلنامه ژئوپلیتیک*. (۲)، ۴۶–۷۳.
- حجازی، سید حسین و انعامی، سهراب. (۱۳۸۷). ظرفیت‌های قدرت نرم جمهوری اسلامی ایران در مقابله با تهدیدات نرم آمریکا، *مرکز پژوهش و اسناد ریاست جمهوری*.
- حمیصی، مرتضی. خندق آبادی، علی. (۱۳۹۰). بررسی نقش اقتدار سیاسی در توسعه اقتدار ملی. *فصلنامه مطالعات دفاعی استراتژیک*. شماره ۴۳.
- داوری، علی و رضازاده، آرش. (۱۳۹۳). *مدل‌سازی معادلات ساختاری با نرم‌افزار PLS*، تهران: انتشارات جهاد دانشگاهی.
- فرخی، محمدحسن. محمدی، علی. (۱۳۹۳). مفهوم‌شناسی بازدارندگی سایبری و الزامات راهبردی جمهوری اسلامی ایران، *دومین کنفرانس ملی دفاع سایبری*.
- مطالعه گروهی دانشجویان دوره‌ی چهاردهم امنیت ملی. (۱۳۸۹). دستیابی و تدوین الگوی راهبردی تحکیم و توسعه اقتدار ملی جمهوری اسلامی ایران، تهران، *دانشگاه عالی دفاع ملّی*، دانشکده امنیت.
- مجیدی، اکبر. (۱۳۹۵). تحلیل و نقد جایگاه و کاربرد رویکردهای شناختی در علوم اطلاعات. *فصلنامه علوم و فنون مدیریت اطلاعات*، سال دوم شماره چهارم. ۲۱-۵۶

- هلیلی، خداداد، ولوی، محمدرضا، موحدی صفت، محمدرضا و باقری مسعود. (۱۳۹۷). قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر. *فصلنامه امنیت ملی*، سال هشتم شماره ۲۹.
- هلیلی خداداد، ولوی، محمدرضا و موحدی صفت، محمدرضا. (۱۳۹۷). شناسایی عوامل و مؤلفه‌های تأثیرگذار بر تدوین دکترین قدرت سایبری ج. ا. ایران مبتنی بر سیاست‌های ابلاغی و اسناد بالادستی. *فصلنامه راهبرد دفاعی*، ۱۶(۶۳).
- هلیلی، خداداد. (۱۴۰۱). واکاوی نظریه‌های قدرت سایبری و ارائه مدل مفهومی نوین برای قدرت سایبری. *نخستین کنفرانس ملی فضای سایبر*. دانشگاه تهران.
- Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 3–22). Washington, D.C.: National Defense University Press.
- Nye, J. S. (2011). *The future of power*. Belfer Center for Science and International Affairs.
- Spade, J. M. (2012). *China's cyberpower and America's national security*. U.S. Army War College, Carlisle Barracks, PA.
- Sheldon, J. (2011). Deciphering cyberpower: Strategic purpose in peace and war. *Strategic Studies Quarterly*, *5*(2), 95–112.
- Sheldon, J. (2014). Geopolitics and cyber power: Why geography still matters. *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy*, 36(5), 286–293. https://doi.org/10.1080/10803920.2014.976736
- Shaw, D. S. (2010). *Cyberspace: What senior military leaders need to know?* Strategy Research Project, U.S. Army War College, Carlisle Barracks.
- Zimet, E., & Barry, C. (2009). Military service of cyber overview in military perspective on cyberpower. *Military Perspective on Cyberpower*, Washington, D.C.: Center for Technology and National Security Policy at the National Defense University.