AJA Command and Staff University

Military Science and Tactics

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

# Islamic Republic of Iran army Cyber Offensive Evaluation Model

**Mohammad Ghasemi Tadavani[1]✉ | Davod Azar[2]| Vahid Sajadi Asil[3]**

1. Faculity Member of AJA Command and Staff University, Tehran, Iran
   E-mail: M.Ghasemi@Casu.ac.ir
2. Phd student of Defense Management. Command and Staff University, Tehran, Iran.
   E-mail: davodazar@yahoo.com
3. Faculty Member of AJA Command and Staff University, Tehran, Iran.
   E-mail: v.d.sajadi@gmail.com

**Article Info**

**Article type:**
Research Article

**Article history:**
Received 18 March 2023
Received in revised form 10 June 2023
Accepted 16 June 2023
Published online 25 June 2023

**Keywords**:
*Cyber space, cyber power, cyber offense.*

**ABSTRACT**

**Objective:** This research was carried out to provide a model for evaluating the cyber offensive power of the army of the Islamic Republic of Iran.

**Method:** The implementation method of this research is descriptive, by applied type, which is done with a mixed approach. Seven experts from the army's cyberspace were selected for interviews to theoretical saturation by purposeful sampling. The statistical population for the questionnaire included some staff of the army of the Islamic Republic of Iran with at least a bachelor's degree in the cyber science. In addition, they have served at least 10 years in cyber career positions. the statistical population included 79 people, so the census method was used to distribute the questionnaires. First, document study and interviews were used to collect data. After that, the questionnaire was used. The reliability of the questionnaire was confirmed with Cronbach's alpha. Qualitative data analysis was done using content analysis method and quantitative data was analyzed using SPSS software

**Findings:** Manpower, cyber complexity, cyber weapons and cyber situational awareness are the most important components that the finding of this research were 12 indicators for evaluating cyber offensive power. It also provided a model to evaluate the cyber offensive power of the army of the Islamic Republic of Iran.

**Conclusion:** This model illustrates that the autonomy of the cyber weapon should be considered by the manufacturers in the design and construction of cyber weapons (embodied and disembodied). On the other hand, quality of manpower with a wide range of technical skills, creativity, who have high situational awareness with proper training, is necessary to use these weapons and overcome cyber complexities.

**Cite this article:** Ghasemi, M., Azar, D., & Sajadi Asil, V. (2023). Islamic Republic of Iran Army Cyber Offensive Evaluation Model. Military Science and Tactics, 19(64), 33-52. doi:10.22034/qjmst.2023.550347.1678



**Publisher:** Command and Staff University
DOI: 10.22034/QJMST.2023.550347.1678

فصلنامه علمی علوم و فنون نظامی
دانشگاه فرماندهی و ستاد آجا
https://www.qjmst.ir/
شاپای چاپی: ۱۹۱۸-۲۰۰۸ شاپای الکترونیکی: ۴۵۳۰-۲۶۷۶

# الگوی ارزیابی قدرت آفند سایبری ارتش جمهوری اسلامی ایران

**محمد قاسمی تادوانی[1]✉ | داود آذر [2] | وحید سجادی اصیل [3]**

۱. عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا، تهران، ایران.رایانامه: M.Ghasemi@Casu.ac.ir
۲. دانشجوی دکتری مدیریت دفاعی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: davodazar@yahoo.com
۳. عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: v.d.sajadi@gmail.com

اطلاعات مقاله

**نوع مقاله:**
**مقاله پژوهشی**
مقالهٔ پژوهشی
**تاریخ دریافت:**
۱۴۰۱/۱۱/۱۱
**تاریخ بازنگری:**
۱۴۰۲/۰۳/۰۶
**تاریخ پذیرش:**
۱۴۰۲/۰۵/۰۲
**تاریخ انتشار:**
۱۴۰۲/۰۶/۱۳
**کلیدواژه‌ها:**
*فضای سایبر،*
*قدرت سایبری،*
*آفند سایبری.*

چکیده

**هدف:** این تحقیق با هدف ارائه الگوی ارزیابی قدرت آفند سایبری ارتش جمهوری اسلامی ایران انجام شده است.

**روش:** روش اجرای پژوهش توصیفی است، نوع این تحقیق کاربردی است که با رویکرد آمیخته انجام شده است. جامعه آماری برای مصاحبه، شامل ۷ نفر از خبرگان در حوزه سایبری آجا بوده است که به روش هدفمند انتخاب و مصاحبه با ایشان تا رسیدن به اشباع نظری ادامه یافت. جامعه آماری برای پرسش‌نامه، شامل کارکنان ارتش جمهوری اسلامی ایران در طیف درجات افسر ارشد و بالاتر هستند که دارای مدرک تحصیلی کارشناسی و بالاتر در رشته‌های مرتبط با علوم سایبری بوده و دارای حداقل ۱۰ سال سابقه خدمت در مشاغل مرتبط با فضای سایبر بوده‌اند. تعداد جامعه آماری ۷۹ نفر است و از روش سرشماری برای توزیع پرسش‌نامه استفاده گردید. ابتدا با استفاده از ابزار مطالعه اسناد و مدارک و مصاحبه داده‌ها جمع‌آوری شد، سپس از ابزار پرسشنامه استفاده شد که پایایی آن با محاسبه آلفای کرونباخ تأیید گردید. داده‌های کیفی با روش تحلیل محتوا تجزیه‌وتحلیل شدند و از نرم‌افزار SPSS برای تجزیه‌وتحلیل داده‌های کمی استفاده گردید.

**یافته‌ها:** نیروی‌انسانی، پیچیدگی سایبری، تسلیحات سایبری و آگاهی وضعیتی سایبری مهم‌ترین مؤلفه‌ها در آفند سایبری هستند که یافته‌های این پژوهش، احصا ۱۲ شاخص برای ارزیابی قدرت آفند سایبری و ارائه الگوی ارزیابی قدرت آفند سایبری ارتش جمهوری اسلامی ایران است.

**نتیجه‌گیری:** الگوی ارائه شده نشان می‌دهد که خودمختاری سلاح سایبری در طراحی و ساخت تسلیحات سایبری (با بدنه و بدون بدنه) باید مدنظر سازندگان قرارگیرد. از طرفی نیروی انسانی کیفی با طیف گسترده‌ای از مهارت‌های فنی، خلاقیت که با آموزش مناسب دارای آگاهی وضعیتی بالایی باشند، برای استفاده از این تسلیحات و غلبه بر پیچیدگی‌های سایبری لازم است.

**استناد**: قاسمی تادوانی، محمد، آذر، داود و سجادی اصیل، وحید. (۱۴۰۲). الگوی ارزیابی قدرت آفند سایبری ارتش جمهوری اسلامی ایران. علوم و فنون نظامی، ۱۹(۶۴)، ۳۳-۵۲. doi: 10.22034/qjmst.2023.550347.1678
**ناشر:** دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

**مقدمه**

با توسعه جوامع مجازی در اینترنت، حوزه‌های سرزمینی کاهش‌یافته و الگوهای حکمرانی توسعه پیدا کرده است و الگوی جدیدی برای جوامع و حاکمیت، در حال شکل‌گیری است. نقش دولت‌ها در زندگی مردم کم‌اهمیت‌تر شده است؛ افراد با چندین قرارداد داوطلبانه، زندگی خواهند کرد و با کلیک ماوس در جوامع مختلف وارد می‌شوند. (Nye, 2010: 4)

به لحاظ نظامی، قدرت سایبر، شاید مهم‌ترین ابزار نوظهور چند دهه گذشته باشد. در حال حاضر اغلب نیروهای مسلح کشورها برای ایمن‌سازی مرزهای سایبر و فراسایبری خود در برابر چنین تحول جدیدی آماده می‌شوند. رهنامه‌های جدید نظامی بر اساس فضای سایبر تدوین می‌شوند. در تمام سطوح منازعه، از شورش‌های داخلی گرفته تا جنگ متعارف، قدرت سایبر، عامل حتمی و گریزناپذیر توانمندی‌های نظامی است و این توانمندی بر پایه فناوری‌های مدرن شکل‌گرفته است. قدرت سایبر روزبه‌روز خود را به‌عنوان یک عامل تأثیرگذار در سیاست‌گذاری حوزه‌های ملی از اقدامات ضدتروریستی گرفته تا سامان دادن سیاست، اقتصاد و حتی روابط با سایر کشورها، توسعه می‌دهد. (زابلی زاده، ۱۳۹۷: ۵۳)

اطلاعات در فضای سایبر به‌راحتی و برای همه به‌صورت یکسان در دسترس هستند. سیستمی که به ارتباطات الکترونیکی متکی است، در صورت تداخل یا ازبین‌رفتن توانایی برقراری ارتباط، می‌تواند بی‌فایده شود. ازآنجاکه این اتکا بسیار کلی است، حمله سایبری به زیرساخت‌های اطلاعاتی می‌تواند تأثیرات گسترده‌ای هم برای ارتش و هم برای جامعه داشته باشد و چنین حملاتی می‌تواند از منابع مختلفی انجام شود، شناسایی برخی از آنها دشوار یا غیرممکن است. (zac, 2021: 83)

فعالیت‌های حمله سایبری اثرات منفی قابل‌توجهی را در فضای سایبری ایجاد می‌کنند که می‌توانند منجر به تأثیرگذاری در حوزه‌های فیزیکی نیز گردد. خلاف فعالیت‌های بهره‌برداری سایبری که برای تأثیرگذاری، نیاز دارند که مخفی نگه داشته شوند، فعالیت‌های حمله سایبری ازآنجاکه منجر به اختلال در کارکرد سامانه‌ها می‌گردند، برای کاربران سامانه‌ها مشهود خواهند بود. پتانسیل تهدیدکنندگی، حیات حملات سایبری را نشان می‌دهد و از نیاز برای ایجاد یک نظم اضطراری برای فضای سایبری پشتیبانی می‌کند (Trusilo, 2021: 54)

ضعف سیستم‌های ارزیابی و نظام کسب بازخورد، امکان تبادل اطلاعات لازم را برای رشد، توسعه و بهبود فعالیت‌های یک سازمان غیرممکن کرده و زمینه‌های بروز بحران‌های مدیریتی را در آن‌ها افزایش می‌دهد و نتیجه تداوم آن ممکن است انحلال و شکست سازمان‌ها را به دنبال داشته

باشد. مراکز سایبری در ساختار نظامی ارتش جمهوری اسلامی ایران یک سازمان مهم به‌حساب می‌آیند و نتایج عملکرد آن نقش حیاتی در عملکرد و کارآمدی ارتش خواهد داشت.

سؤال اصلی پژوهش حاضر، این است که الگوی ارزیابی قدرت آفند سایبری ارتش جمهوری اسلامی ایران چگونه است؟ این پژوهش در جهت ارائه الگوی ارزیابی قدرت آفند سایبری ارتش جمهوری اسلامی ایران انجام شده است.

## مبانی نظری

### مفهوم‌شناسی پژوهش

### فضای سایبر

فضای سایبر امکانات جدیدی در اختیار بشر قرار می‌دهد. جغرافیا را از بین می‌برد؛ انسان را از فاعل بودن در محیط اجتماعی، به سوژگی در محیط مجازی سوق می‌دهد؛ ایده‌ها را گسترش می‌دهد؛ کنترل‌پذیری را بی‌معنا می‌سازد و دولت را به‌عنوان نهاد ناظر بر روابط سیاسی، اجتماعی، فرهنگی و... خلع سلاح می‌کند. وجود پیوند میان فضای سایبر و قدرت در روابط بین‌الملل، در حال حاضر امر بدیهی محسوب می‌شود. وجوه قدرت در فضای فیزیکی متنوع است. این تعدد وجه، خود را در فضای سایبر نیز نشان می‌دهد. می‌توان از چند وجه قدرت در روابط بین‌الملل و جهان سیاست صحبت کرد. وجه سخت‌افزاری و وجه نرم‌افزاری قدرت در فضای سایبر، نیز می‌توان نشانه‌های چنین وجوهی را جستجو کرد. (زابلی زاده: ۱۳۹۷، ۵۶)

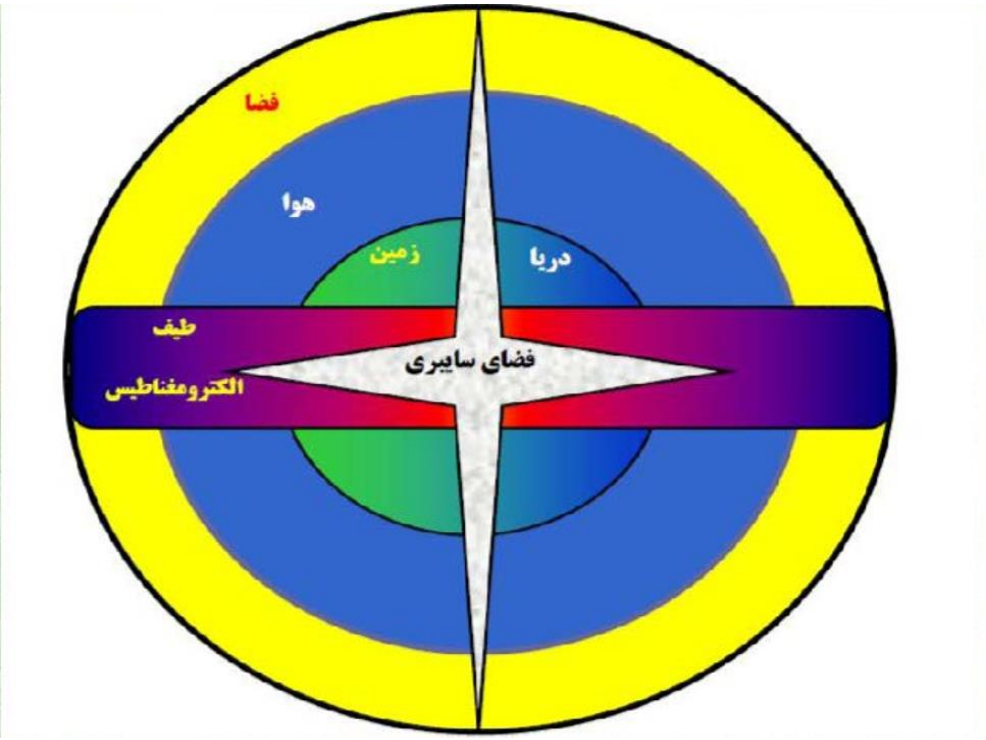
مهم‌ترین ویژگی‌های فضای سایبر عبارت‌اند از:

- شبکه‌ای بودن
- قابلیت ایجاد اجتماعات
- ماهیت فنی
- وابستگی و ارتباطات متقابل
- آسیب‌پذیر بودن (Department of Army, 2017: PP I-15 - I-16)

### ارتباط فضای سایبری با سایر حوزه‌ها

فضای سایبری به‌عنوان بخشی از محیط اطلاعاتی، به حوزه‌های فیزیکی هوایی، دریایی، زمینی و فضایی وابسته است. درحالی‌که بیشتر عملیات در حوزه‌های فیزیکی، به زیرساخت‌های فیزیکی ایجاد شده برای بهره‌برداری از ویژگی‌های طبیعی متکی هستند؛ عملیات در فضای سایبری، علاوه بر اطلاعات مقیم در سامانه‌ها یا اطلاعات در حال تبادل، به زیرساخت‌های مستقل، وابسته به سکوها، یا شبکه شده فناوری اطلاعات، متکی هستند. عملیات سایبری از گره‌ها و لینک‌های

موجود در حوزه‌های فیزیکی بهره‌برداری می‌کند و کارکردهای منطقی را به‌منظور تأثیرگذاری در فضای سایبری - در اولویت اول و سپس در صورت لزوم - در حوزه‌های فیزیکی اجرا می‌کند. به‌واسطه آثار به‌هم‌پیوسته و متناوب حوزه‌های فیزیکی و سایبری، اقدامات در فضای سایبر می‌توانند آزادی عمل را برای فعالیت در حوزه‌های فیزیکی فراهم کنند؛ به همین ترتیب، فعالیت‌ها در حوزه‌های فیزیکی می‌توانند به‌واسطه تأثیرگذاری در طیف الکترومغناطیس یا زیرساخت‌های فیزیکی، تأثیرهایی را در فضای سایبری یا از طریق آن ایجاد کنند. (سجادی اصیل، ۱۳۹۹: ۱۵)




**شکل (۱) رابطه فضای سایبر با سایر فضاها آفند سایبری** (U. S. AIR FORCE, 2011: 19)

**معیارهای مطلوب برای ارزیابی قدرت آفند سایبری**

قدرت سایبری بخشی از قدرت ملی است؛ لذا ارزیابی قدرت سایبری از روش‌های ارزیابی قدرت ملی تبعیت می‌نماید، بنابراین می‌تواند شامل تک‌متغیره و چندمتغیره باشد. در ارزیابی قدرت آفند سایبری با استفاده از یک الگوی چندمتغیره شکاف بین وضع موجود و وضع مطلوب مشخص شده و منجر به راهکارهایی برای بهبود وضع موجود خواهد شد.

در کار انجام شده توسط جی وورن، مؤلفه‌های زیر برای قدرت سایبری در نظر گرفته شده است:

مؤلفه محیطی: مانند توزیع جغرافیایی جمعیت کاربران سایبری
مؤلفه اقتصادی: مانند فناوری‌های مربوط به دسترسی و توسعه زیرساخت ارتباطی، پشتیبانی و کارشناسان سایبری مؤلفه نظامی: مانند ورود نیروهای نظامی به فضای سایبر و استفاده از قابلیت‌های آن برای حمله و دفاع سایبری
مؤلفه راهبردی: شامل راهبردهای سایبری به‌منظور پیشگیری از جرائم سایبری، امنیت سایبری و سامانه‌های آموزشی سایبر
مؤلفه شناختی: شامل اراده و درک سیاستمداران و تصمیم‌گیران در مواجهه با چالش‌های سایبری (نصرت‌آبادی، ۱۳۹۷: ۱۸۵-۱۸۷)

**مطلوبیت‌های قدرت آفند سایبری ارتش جمهوری اسلامی ایران**

مطلوبیت‌های شناسایی شده ارتش جمهوری اسلامی ایران که با تحقق آن‌ها می‌تواند مأموریت‌های آفند سایبری خود را ارتقا دهد عبارت‌اند از:

- طراحی، تولید، استقرار و به‌کارگیری محصولات بومی حوزه فاوا
- ارتقا تحصیلی کارکنان حوزه فاوا
- تولید نرم‌افزارهای امن داخلی
- برگزاری رزمایش‌های سایبری
- ایجاد و تقویت مراکز تولید سامانه‌های هوشمند (مسلمی، حسین، ۱۳۹۴: ۲۱۶)

**کارکرد قدرت آفند سایبری نظامی**

مأموریت یک سازمان نظامی حفظ امنیت و دارایی‌های ملی و حکومتی در برابر تهدیدهاست. سازمان‌های دفاعی به‌بخش هایی گفته می‌شود که به تولید کالا و خدمات و فناوری برای مصرف نهایی در نیروهای مسلح دولتی در زمان صلح با نیازهای در حال افزایش زمان جنگ یا موقعیت اضطراری بپردازد و به طور مشخص یک سازمان غیردفاعی چنین وظیفه‌ای ندارد، و می‌تواند هر محصولی غیر از نظامی یا دفاعی داشته باشد. سازمان نظامی دارای یک نظام سلسله‌مراتبی است که تلاش می‌کند با استفاده از سازماندهی تشکیلات داخلی، کسب منابع موردنیاز و مدیریت عوامل خارجی اثرگذار بر سازمان، در دو زمینه اصلی کارکردی نظامی و علمی در به‌دست‌آوردن هدف‌ها و مأموریت‌ها و خروجی‌های نظام‌مند خود اثربخشی لازم را داشته باشد. یک سازمان دفاعی یا نظامی دارای مأموریت‌های گسترده‌ای دربخش های مختلف عملیاتی و رزمی، فرماندهی و کنترل، فناوری، ساخت و نگهداری تجهیزات، ادوات نظامی و پشتیبانی و خدمات اداری و مالی است. سازمان دفاعی دارای مدیریت و نگرش نظام‌مند بر اداره امور، برنامه‌ریزی، بهینه‌سازی و نظارت بر وظایف است. ملزم به در اختیار داشتن ابزار و تجهیزات و فناوری‌های نوین و تلاش

برای تحقیق، توسعه و نوآوری در تمامی ابعاد مأموریتی خود و مجاز بر به‌کارگیری خشونت و جنگ‌افزار بر دشمن است. سازمان نظامی سایبری، سازمانی است که‌بخش ها و نیروهای آن، وظیفه ایجاد آمادگی و توانمندی دفاعی از راه افزایش قابلیت‌ها و مهارت‌های پاسخ به تهدیدهای سایبری که از فضای سایبری (مجازی) سرچشمه می‌گیرد را دارند. به‌روز شدن نیروهای مسلح در عصر حاضر ضروری است. (ربیعی، ۱۳۹۹: ۲۱-۲۲)

کشورها با توسعه فنی و استفاده تاکتیکی در زمینهٔ عملیاتی از نیروهای سایبری به‌عنوان متغیرهای اصلی مداخله‌گر در سراسر چارچوب ارزیابی سایبری، رویکردشان را سازماندهی می‌کنند و درنهایت یک سازمان نظامی را در وضعیت ایجاد قدرت سایبری قرار می‌دهند. اثربخشی قدرت سایبری بستگی به این دارد که چگونه نیروهای سایبری مورداستفاده و ارزیابی قرار گیرند. (نصرت‌آبادی، ۱۳۹۷: ۱۷۳-۱۷۸)

**کارکرد قدرت آفند سایبری ارتش جمهوری اسلامی ایران**

کارکردهای نظامی شناخته شده در فضای سایبر که ارتش جمهوری اسلامی ایران می‌تواند با مدنظر قراردادن آن‌ها وضعیت استفاده از فضای سایبر در مأموریت‌های آفندی خود را ارتقا دهد، عبارت‌اند از:

- شبکه ارتباط سیگنالی و اطلاعات در فضای سایبری
- سامانه‌های مقابله با تهدیدات فضای سایبر
- سامانه‌های جمع‌آوری و ترکیب داده‌ها
- سامانه‌های هوشمند چرخه اطلاعات
- سامانه‌های مدیریت منابع انسانی
- سامانه‌های شناسایی و بررسی منطقه عملیات
- سامانه‌های آموزشی فضای مجازی (مسلمی، حسین، ۱۳۹۴: ۲۱۲-۲۱۳)

**آفند سایبری**

فعالیت‌های حمله سایبری، یکی از انواع آتش‌ها (آماج‌ها) هستند که به‌عنوان بخشی از مأموریت‌های عملیات سایبری تهاجمی یا فعالیت‌های واکنشی عملیات سایبری تدافعی و با هماهنگی سایر وزارت‌خانه‌ها و نهادهای دولتی انجام می‌شوند. این فعالیت‌ها که به‌دقت با سایر آتش‌های طرح‌ریزی‌شده در حوزه فیزیکی هماهنگ و هم‌زمان شده‌اند. (DOD, 2018: II-6 )

هدف از حمله سایبری، اعمال قدرت برای کسب امتیاز در فضای سایبری یا فیزیکی برای نیروهای خودی است. به‌عنوان‌مثال، یک حمله سایبری می‌تواند اطلاعات موجود یا در حال تبادل بین رایانه‌ها یا دستگاه‌های تلفن همراه را به‌منظور جلوگیری از استفاده بازیگران دشمن یا رقیب

از آنها، هدف قرار دهد. حمله سایبری می‌تواند برای هر دو نوع عملیات تهاجمی یا تدافعی در فضای سایبری انجام شود. یک حمله سایبری در واقع تلاشی خطرناک یا غیر خطرناک است تا یک منبع قابل‌دسترسی از طریق شبکه به‌گونه‌ای مورد تغییر یا استفاده قرار گیرد که موردنظر نبوده است. برای فهم بهتر مفهوم حمله، حملات سایبری را به سه دسته عمومی تقسیم می‌کنیم

۱. دسترسی غیرمجاز به منابع و اطلاعات از طریق شبکه.

۲. دست‌کاری غیرمجاز اطلاعات بر روی یک شبکه.

۳. حملاتی که منجر به اختلال در ارائه سرویس می‌شوند. (سجادی اصیل، ۱۳۹۹: ۸۸)

**تشریح مراحل یک حمله سایبری به‌صورت ساده**:

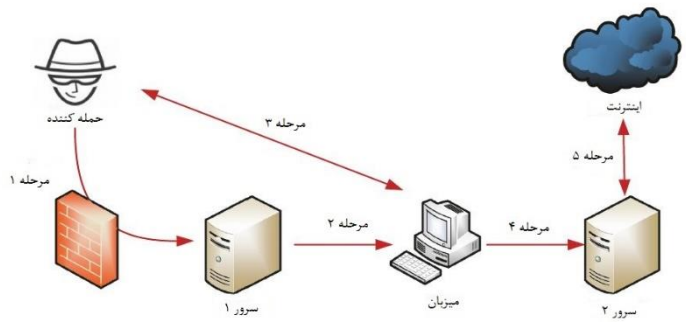
مرحله ۱: مهاجم از ابزارهای مهندسی اجتماعی استفاده می‌کند به‌عنوان ایمیل فیشینگ برای دورزدن فایروال و نفوذ در سرور برنامه

مرحله ۲: مهاجم از سرور ۱ به‌عنوان یک سکوی پرش به سیستم و شناسایی و نفوذ به میزبان در شبکه داخلی بهره می‌برد.

مرحله ۳: مهاجم کانال لازم را برای کنترل میزبان اینترانت و نفوذ بیشتر به درون شبکه ایجاد می‌کند.

مرحله ۴: مهاجم از میزبان کنترل شده برای ورود به سیستم (سرور داده داخلی) جهت جمع‌آوری داده‌های حساس استفاده می‌کند.

مرحله ۵: داده‌های حساس جمع‌آوری‌شده را برای دستیابی به هدف سرقت اطلاعات به اینترنت ارسال می‌کند. (Ankang, 2019: 2-3)




**شکل (۲) مراحل یک حمله سایبری(Ankang, 2019: 4)**

## انواع و روش‌های حمله سایبری

انواع و روش‌های حمله سایبری و نتایج آن به شرح جدول زیر است. (سجادی اصیل، ۱۳۹۹: ۵۵)

**جدول (۱) انواع و روش‌های حمله سایبری (سجادی اصیل، ۱۳۹۹: ۵۵)**

| نوع حمله | روش حمله | نتایج |
|---|---|---|
| حمله انکار / منع سرویس | • غلبه بر یک سرور وب، سرور یا یک نقطه دیگر شبکه از طریق ارسال ترافیک برای مصرف منابع و جلوگیری از تبادل ترافیک مجاز | • کاهش توانایی‌های شبکه<br>• اختلال محدود عملیاتی تا انکار کامل خدمات |
| نفوذ به شبکه | • شنود ترافیک (حملات مرد میانی)<br>• فیشینگ<br>• گواهی‌نامه‌های سرقت شده<br>• بهره‌گیری از پیام‌های رمزگذاری نشده و صفحه‌های وب با ویژگی‌های امنیتی ضعیف | • دسترسی غیرقانونی به شبکه‌ها<br>• دست‌کاری شبکه‌ها |
| بدافزارهای مخرب | • فیشینگ<br>• تهدیدات داخلی<br>• رسانه‌های ذخیره‌ساز جانبی | • جاسوس‌افزارها و بدافزارها در سامانه‌های تحت‌تأثیر اجازه می‌دهد تا سامانه شناسایی، دست‌کاری یا دچار اختلال عملکرد شود. |
| تخریب یا مقابله با سامانه‌های اطلاعاتی در طیف الکترومغناطیسی | • جلوگیری از دریافت داده‌های ارسالی در طیف الکترومغناطیس، با استفاده از<br>○ لیزرهای پرقدرت قابل‌حمل<br>○ سامانه‌های ماکروویو پرقدرت<br>○ سامانه‌های ارتباطی تقلیدی یا جعلی | • انکار خدمات به‌صورت کوتاه‌مدت یا دائمی<br>• جلوگیری از تهیه آگاهی موقعیتی و برنامه‌ریزی عملیاتی |

## بررسی مؤلفه‌های مؤثر در آفند سایبری

### عامل انسانی

در آفند سایبری با دو دسته عامل انسانی سروکار داریم:

بخش اول مهاجم: اغلب کارکنان و رزمندگان حاضر در آن، دارای تخصص و سوابق دیگری مثلاً امنیت، رایانه، ارتباط و رشته‌های محاسباتی و فنی هستند. نکته دیگر در این حوزه این است که برخلاف سایر رشته‌ها، اعتبارنامه‌ها و مدارک رسمی بسیار کم است. تجارب و مهارت‌ها در زمینه عملیات سایبری، در عین اهمیت بسیار زیاد، می‌توانند بسیار متفاوت باشند. (سجادی اصیل، ۱۳۹۹: ۵۶)

بخش دوم جامعه هدف:بخش دوم که‌بخش روانی این حوزه است، در واقع شامل افرادی است که مخاطب فضای سایبر هستند و همیشه تحت‌تأثیر سناریوهای متخصصین روان‌شناسی و جامعه‌شناسی دشمن در بستر فضای سایبر قرار دارند، استفاده مثبت انقلابیون عرب در بیداری اسلامی خاورمیانه و شمال آفریقا در سال ۲۰۱۱ میلادی از شبکه‌های اجتماعی برای پیشبرد روند انقلاب، از نمونه‌های این مدعا است. اقبال عمومی و میلیونی گسترده به این شبکه‌ها ظاهر نیاز جدید بشر امروزی است. طراحی مناسب، جذاب و بومی از این نوع شبکه‌ها قدم بعدی است. گام بلندمدت بعدی، آموزش و بالابردن فرهنگ و دانش رسانه‌ای نیروی انسانی است؛ با ترتیبی که حملات روانی و سایبری از این حوزه، آثار مخرب کمتری به فضای سایبر خودی وارد نمایند. منظور از عامل انسانی در این تحقیق‌بخش اول یعنی مهاجم است. تعریف سطح دسترسی افراد به اطلاعات و آموزش تخصصی نیروی انسانی دو قدم بلند این حوزه است. در تعریف سطح دسترسی یک قانون کارآمد می‌گوید: "هر کس تنها اطلاعاتی در اختیار داشته باشد که برای پیشبرد کار تعریف شده سازمانی خود، بدان احتیاج دارد و نه بیشتر." نفوذ دشمن از حفره خلأ علمی کاربران می‌تواند با آموزش مستمر و بروز رسانی این آموزش‌ها مسدود گردد. (آذر، ۱۳۹۸: ۱۴۴-۱۴۳)

به‌طورکلی مهارت‌های موردنیاز در حوزه عملیات سایبری، به سه دسته مهارت‌های شناسایی، حمله و دفاع سایبری تقسیم می‌شود. مهارت‌های شناسایی رزمندگان سایبری را قادر به بررسی زیرساخت‌ها، سامانه‌ها و ترافیک می‌نماید. مهارت‌های تهاجمی بیشتر بر روی حمله تمرکز دارند و با سایر مباحث غیرامنیتی نیز هم‌پوشانی ندارند. مهارت‌های تدافعی به‌طورکلی در تمامی صنایع محاسباتی رایج هستند. این مهارت‌ها بیشتر دربخش فناوری اطلاعات وجود دارد. (Andress, 2011: 61-80)

گزینه‌های خوب برای کسب موفقیت در حوزه جنگ‌های سایبری دارای طیف گسترده‌ای از مهارت‌های فنی بوده و درک کلی نسبتاً خوبی از هک، شبکه، توسعه شبکه، مدیریت سامانه و سایر حوزه‌های مشابه دارند و همچنین بسیار خلاق هستند. آموزش نسل بعدی و کسانی که در آینده به جنگ سایبری خواهند پرداخت، یک چشم‌انداز جالب است. نه‌تنها باید به افراد تازه‌وارد در این رشته آموزش داد، بلکه باید به نیروی کار کنونی خود برای مقابله با مسائل جدید نیز آموزش دهیم. (سجادی اصیل، ۱۳۹۹: ۵۶)

**پیچیدگی سایبری**

انجام فریب و غیرقابل‌پیش‌بینی بودن باعث افزایش عدم اطمینان دشمن در مورد ساختار و رفتار سیستم می‌شود. (Ross, 2021: 125)

تشخیص عامل حملات سایبری به شبکه‌ها یکی از مشکلات مهم فنی است و دانستن این‌که آیا دولت‌ها در حملات سایبری در مقیاس بزرگ دخالت دارند مشکل است. اصل حملات چندمرحله‌ای و چندلایه معاصر که اغلب به‌عنوان تهدیدهای مستمر و پیشرفته نامیده می‌شود این است که آنها از ورای مرزهای بین‌المللی با استفاده از توالی بسیار پیچیده و فریب‌دهنده‌ای از رایانه‌ها انجام می‌شوند که بسیاری از آنها رایانه‌های غیرقابل‌پیش‌بینی هستند که برای بالابردن ترافیک شبکه و تنها به دلیل اتصال به اینترنت به هم متصل می‌شوند. توانایی ردیابی مراحل مختلف یک حمله و کشف عامل اصلی، بسیار دشوار و حتی غیرممکن شده است و هرچه فناوری رشد می‌کند دشوارتر می‌شود. ( احمدی، ۱۳۹۹: ۹۹-۱۱۵)

مبهم‌سازی حمله سایبری یک عامل مهم دیگر در پیچیده کردن حملات سایبری است. مبهم‌سازی، سازوکاری برای پنهان‌سازی هدف یا رفتار اصلی حمله سایبری است. هدف از مبهم‌سازی در دنباله‌های حمله، تلاش برای مخفی‌کاری و پنهان‌سازی اطلاعات مهم حمله و گمراه‌سازی سامانه‌های همبستگی هشدار به‌منظور عدم تشخیص یا تشخیص غلط و نادرست از حمله است. مبهم‌سازی در سه سطح نویز، اقدام و حمله قابل‌اجرا است. ( شوشیان، ۱۳۹۹: ۶۷-۷۰)

حملات سایبری هدفمند، طبقه‌ای از حملات اختصاصی هستند که هدف آن کاربر، شرکت یا سازمان خاصی است و با قصد خاص، مانند سرقت داده‌های حساس از پشتیبان پایگاه‌داده یا فلج کردن خدمات سیستم طراحی می‌شوند. حملات سایبری هدفمند دارای ویژگی تصادفی هستند؛ طبیعت تصادفی بدان معناست که مهاجمان برای حمله، اهداف را متمایز کرده و منتظر فرصت مناسب هستند. ( Ross, 2021: 130)

تفاوت بین حمله سایبری هدفمند و حمله سنتی این است که حملات سایبری هدفمند پیچیده‌تر هستند و معمولاً باانگیزه نفوذ قوی مهاجمان زمان بیشتری را صرف انتخاب هدف می‌کنند، آسیب‌پذیری‌ها را می‌یابند، و نرم‌افزارهای مخرب را سفارشی می‌کنند. معمولاً در حملات سایبری هدفمند به‌جای استفاده از ابزار، حمله توسط متخصصان پیاده‌سازی می‌شود.
(Ankang,2019: 5)

**تسلیحات سایبری**

عملیات جنگ سایبر همانند جنگ‌های سخت دارای سلاح‌هایی است که باتوجه‌به نوع عملیات (آفندی، پدافندی و دومنظوره) مورداستفاده قرار می‌گیرد. ابزارهای آفندی: ویروس‌های رایانه‌ای، اسب‌های تروا، ابزارهای عدم دسترسی به سرویس از جمله ابزارهای آفندی هستند. ابزارهای

دارای کاربردی دومنظوره: از جمله اسکنرهای تشخیص آسیب‌پذیری پورت و ابزار پایش شبکه. ابزارهای پدافندی: رمزنگاری و دیواره آتش از ابزارهای پدافندی هستند. (آذر، ۱۳۹۸: ۴۴)

دسته‌بندی سلاح‌های سایبری به شرح زیر است.

- ✓ ابزارهای شناسایی
- ✓ ابزارهای پویش
- ✓ ابزارهای به‌دست‌آوردن دسترسی و بالابردن سطح آن
- ✓ ابزارهای خارج‌کردن غیرمجاز به اطلاعات
- ✓ ابزارهای حفظ دسترسی
- ✓ ابزارهای حمله
- ✓ ابزارهای ایجاد ابهام (سجادی اصیل، ۱۳۹۹: ۵۸-۶۰)

هنگام ارزیابی ویژگی‌های رفتاری یک سیستم، سلاح همچنین باید بتواند قابلیت اطمینان از رفتار سیستم را تضمین کند. در این راستا با ارزیابی قابلیت هدف‌گیری یک سیستم، باید بتوان با اطمینان گفت که یک سیستم آنچه را که برای او به‌عنوان هدف قرار داده شده است مورد هدف قرار می‌دهد. (Trusilo, 2021: 62 )

می‌توان سلاح‌های سایبری را به دو دسته با بدنه و بدون بدنه خودمختار تقسیم کرد.

در مورد سیستم‌های دارای بدنه، وجود نوعی تجلی روباتیک، تصوری را در مورد مکان و محدودیت‌های سیستم ایجاد می‌کند. (Stoecklin, 2018: 82 )

یک سیستم هوشمند دارای بدنه بر پنج محور استوار است که عبارت‌اند از: ۱. خودکامگی، ۲. استقلال از کنترل انسان، ۳. تعامل با محیط، ۴. یادگیری و ۵. تحرک. (Liivoja, 2021: 63)

این تصور در مورد سیستم‌های بدون بدنه به دلیل عدم تجلی فیزیکی، کمتر روشن است. سیستم بدون بدنه امکان تکثیر خود (خود تکثیری) را بدون هیچ‌گونه دستور مستقیم و فوری برای انجام این کار از سوی انسانی که در ابتدا آن را توسعه داده و برنامه‌ریزی کرده است، داشته باشد. آنها می‌توانند؛ مانند آتش منتقل شوند؛ چنین تشبیهی به فرد اجازه می‌دهد تصور کند که یک سیستم خودمختار بدون بدنه چگونه در حال گسترش وسیع است.

یک سیستم بدون بدنه تنها باید: ۱. به‌محض استقرار مستقل از کنترل انسان عمل کند، ۲. بر اساس ویژگی‌هایی که محیط را تعریف می‌کند با محیط خود تعامل داشته باشد و ۳. فراگرفتن، یک سیستم ممکن است در امتداد محورهای توصیف شده متغیر باشد، به این معنا که هر سیستمی نیاز به یادگیری ندارد.

یک ویژگی فیزیکی سیستم دارای بدنه که می‌توان به‌راحتی آن را ارزیابی کرد، درجه کُشندگی است. یک سیستم بی‌بدنه بدون سلاح فیزیکی خواهد بود، اگرچه ممکن است به‌گونه‌ای طراحی شود که کشنده باشد.

معیار دیگری که در مدل به‌عنوان یک ویژگی رفتاری طبقه‌بندی‌شده است، مربوط به محدودکردن سیستم در زمان و مکان است. یک سیستم دارای بدنه ممکن است از لحاظ زمانی و جغرافیایی با روش‌های گوناگون مستقر شود. بااین‌حال، یک سیستم بدون بدنه در یک فضای فیزیکی عمل نمی‌کند. این بدان معنا نیست که نمی‌توان محدودیت‌هایی را برای سیستم‌های بدون بدنه اعمال کرد یا این قبیل محدودیت‌ها را نمی‌توان ارزیابی کرد، اما مفهوم مرزها باید تغییر داده شود تا محیط غیرفیزیکی فضای سایبری در نظر گرفته شود. (Trusilo, 2021: 64)

اگر یک سیستم بدون بدنه توانایی انتخاب اهداف با استفاده از هوش مصنوعی را داشته باشد، نمی‌توان از مجاز بودن اهداف سیستم، اطمینان حاصل کرد؛ به‌ویژه باتوجه‌به توانایی غیرقابل‌پیش‌بینی بودن توالی سریع رویدادهایی که می‌تواند ناشی از استفاده از پاسخ‌های خودکار باشد (چالش واکنش زنجیره‌ای) دشوار است. این چالش واکنش زنجیره‌ای بدین معناست که رفتار سیستم‌های سایبری مستقل می‌تواند منجر به افزایش غیرقابل‌پیش‌بینی پیامدها از طریق حلقه‌های بازخوردی شود که برای متوقف شدن توسط انسان بسیار سریع است.
(Liivoja, 2021: 66)

**آگاهی وضعیتی**

آگاهی وضعیتی عبارت است از: درک و دریافت عناصر و اجزای محیط در ظرفی از زمان و مکان، تفسیر و فهم معانی جزئیات دریافتی و پیش‌بینی یا تجسم؛ وضعیت آنها در آینده نزدیک این تعریف تمایز ظریفی بین سه سطح آگاهی وضعیتی یعنی درک (شامل مشاهده)، فهم و تجسم شامل پیش‌بینی را ترسیم می‌کند. پایین‌ترین سطح آن مشاهده و درک و بالاترین سطح آن پیش‌بینی و تجسم آینده است و موفقیت در هر سطح وابسته به موفقیت در سطح پایین‌تر آن است. (اکبری، ۱۳۹۸: ۷۸-۷۹) در ادغام سطح پایین اطلاعات یا همان‌بخش درک و فهم آگاهی وضعیتی، موضوعاتی چون طبقه‌بندی، شناسایی و ردگیری هدف جزءبخش های اصلی محسوب می‌شوند، این در حالی است که در ادغام سطح بالا یا سطح تجسم اثر، وضعیت و پالایش فرایند ادغام مهم‌ترین موضوعات هستند. برای طراحی معمارانه سامانه آگاهی وضعیتی باید سطوح مختلفی را در نظر گرفت. در سطح معماری فنی، این سامانه مبتنی بر استانداردها، فناوری‌ها و مؤلفه‌ها بررسی می‌شود، در سطح عملیاتی، سازمان‌ها، نیروی انسانی و جریان کاری (فرایندها و

روال‌ها) بررسی می‌شوند. در سطح معماری سامانه، درباره توابع، ساختار، جریان اطلاعات و چگونگی پردازش اطلاعات بحث می‌شود. (Olofintuyi, 2021: 394-395)

اگر فضای سایبری به‌عنوان بعد پنجم فضای نبرد پس از زمین، دریا، هوا و فضا در نظر گرفته شود آگاهی وضعیتی سایبری با آگاهی وضعیتی فیزیکی هم‌پوشانی دارند؛ زیرا تهدیدات و حملات در فضای سایبری، مأموریت‌های دفاعی را تحت‌تأثیر قرار می‌دهند؛ ازاین‌رو بسیار مهم است تا آگاهی وضعیتی سایبری را با آگاهی وضعیتی فیزیکی یکپارچه نمود. ( رشیدی، ۱۳۹۶، ۷۵)

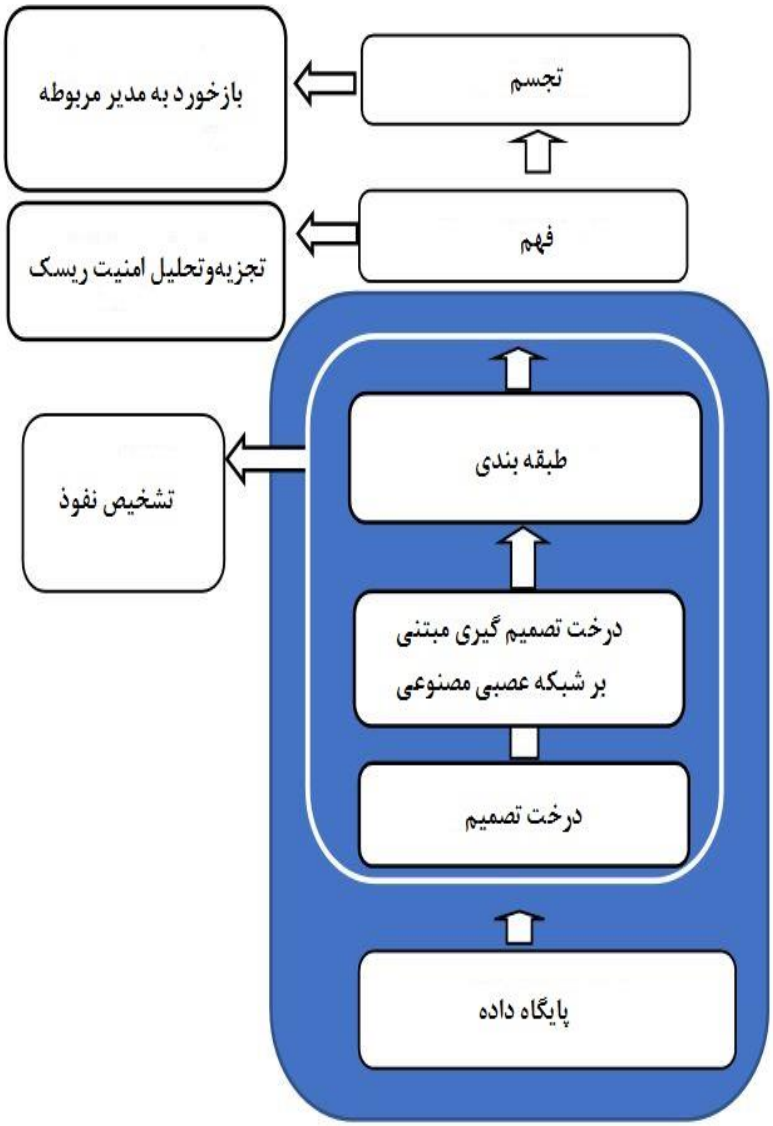
در حال حاضر برای تشخیص و شناسایی حملات به‌صورت خودکار و گزارش به‌موقع رویدادهای ناشی از تهدیدات سایبری، از سامانه آشکارسازی مبتنی بر حمله، سامانه آشکارسازی ناهنجاری آماری، سامانه تحلیل ترافیک، سامانه تشخیص الگوهای رفتاری و قالب الگوی شناخته شده استفاده می‌شود. این‌گونه سامانه‌ها دائماً در حال جستجو و یافتن رفتارهای غیرعادی ناشی از حملات سایبری هستند و بر اساس تغییر رفتار در طول زمان و مقایسه آن با رفتارهای قبلی یک رویداد در سامانه عمل می‌کنند. (Tada, 2008: 126)

به‌کارگیری فناوری‌های با درجه اعتماد بالا و کاربرد زیرساخت مطمئن در گردآوری اطلاعات نویدبخش کاهش عدم قطعیت در آگاهی وضعیتی سایبری است. حصول آگاهی وضعیتی در حوزه‌های پیچیده نیازمند آن است که فناوری و قابلیت‌های شناختی انسان به شکلی منحصربه‌فرد با هم ترکیب گردند. رابطه انسان - فناوری در ایجاد درک مؤثر از جنبه‌های پیچیده و اغلب مخفی حوزه سایبری نقش پررنگ‌تری دارد. در حوزه سایبر فناوری‌ها به‌سرعت در حال تغییر هستند. نرم‌افزارها، سامانه‌های رایانه‌ای، مسیریاب‌ها و سایر مؤلفه‌های جدید به‌صورت روزانه معرفی می‌شوند. این تغییر سریع، درک دقیق هم‌بندی سامانه و اندازه و پیچیدگی شبکه‌های رایانه‌ای، چالش بزرگی را برای آگاهی وضعیتی ایجاد می‌کند. (رشیدی، ۱۳۹۶: ۴۰-۵۴)

به‌منظور آگاهی در برابر تهدیدها، به سیستم تشخیص نفوذ و همچنین الگوریتم‌های مختلف یادگیری ماشین مانند شبکه عصبی مصنوعی، درخت تصمیم، ماشین بردار پشتیبان و غیره برای تشخیص تهدید نیاز است. باتوجه‌به تهدیدهای جدید و پیشرفت متجاوزان در دنیای سایبری، نیاز به استفاده ترکیبی از ابزارها برای افزایش دقت تشخیص نفوذ و آگاهی وضعیتی در شبکه‌های کامپیوتری وجود دارد. ( Olofintuyi, 2021: 392)با ادغام اطلاعات حاصل از عامل‌های توزیع شده ناهمگن در سامانه‌های تشخیص و شناسایی حملات سایبری، امکان توسعه سامانه مذکور با قابلیت اطمینان بالا برای شناسایی، ردگیری و ارزیابی وضعیت فضای سایبری، فراهم می‌شود. فناوری ادغام داده چند حسگری، چارچوب عملکردی مهمی را برای ایجاد آگاهی

وضعیتی در سامانه‌های تشخیص و شناسایی حملات سایبری فراهم خواهد کرد. (داداش‌تبار احمدی، ۱۳۹۳: ۲)

سامانه‌های نرم‌افزاری نیز از دنباله کدهای طولانی و اغلب پیچیده و تودرتو تشکیل شده‌اند به‌طوری‌که پیش‌بینی اثر یک تغییر کوچک در این کد بسیار دشوار است. اندازه سامانه‌های سایبری و ماهیت پویای آنها تعیین و تشخیص مسائل را با چالش روبه‌رو کرده است و درک اثر رویدادهای بالقوه روی کارکرد شبکه را نیز دشوار کرده است. بازه زمانی بین حمله و تأثیر آن ممکن است کاملاً توزیع شده باشد. برخی از حملات سایبری از طریق کد تزریق می‌شوند و برای مدت زمانی طولانی نهفته و مخفی باقی می‌مانند و در یک‌زمان مشخص و یا در اثر یک رویداد خاص فعال می‌شوند. فرایندهایی نظیر نقص کارکردی سامانه، خطاهای نرم‌افزاری، به‌روزرسانی‌ها، رمزهای فراموش شده و مسائل دیگری که برای کاربر، عادی تلقی می‌شوند، ممکن است در جهت ایجاد پوشش برای ویژگی‌های یک حمله سایبری واقعی عمل کنند؛ بنابراین حتی ممکن است نخستین سطح آگاهی وضعیتی یعنی سطح درک حمله را نیز تحت تأثیر قرار دهند. (رشیدی، ۱۳۹۶: ۵۴-۴۹)



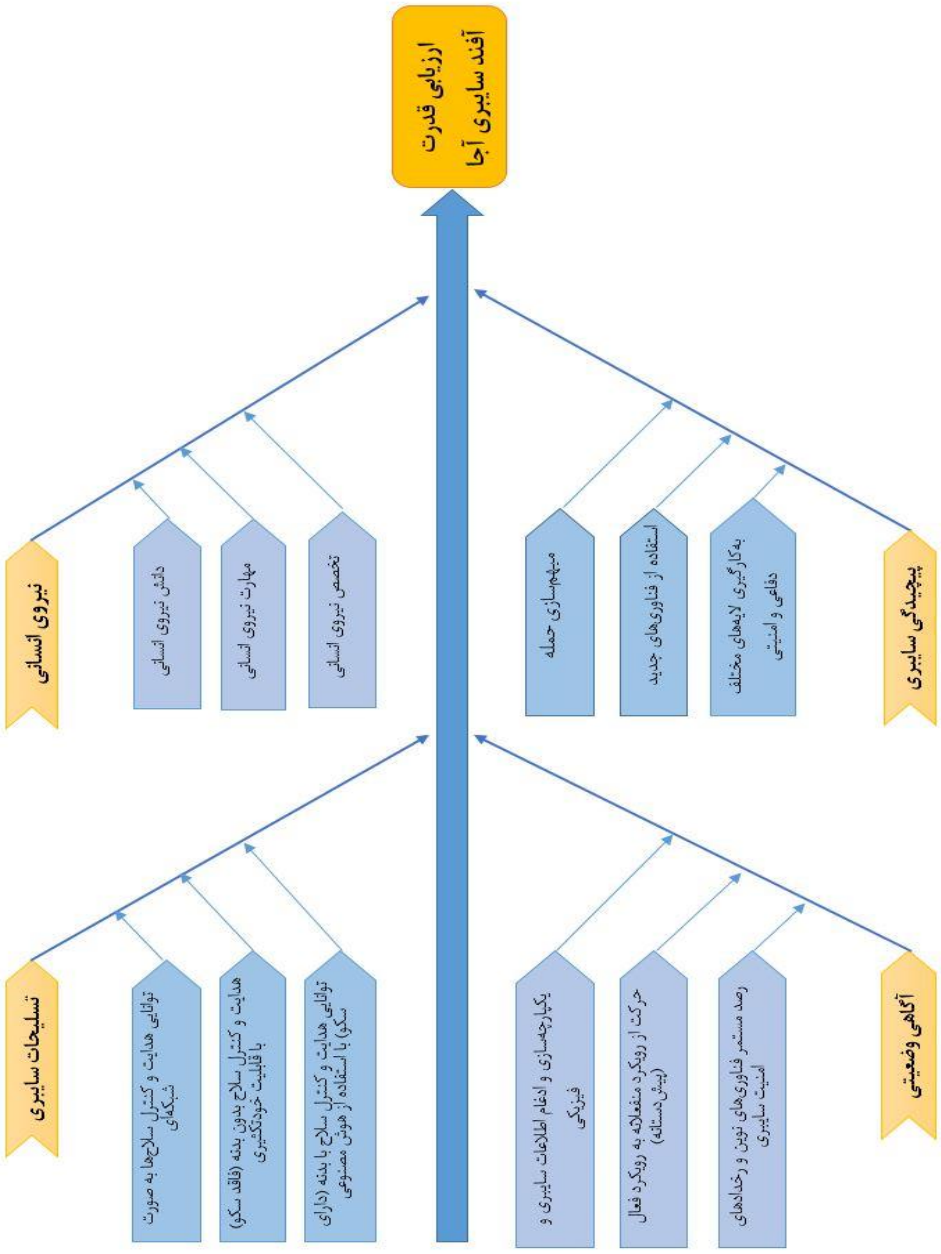

**شکل (۳) طبقه‌بندی آگاهی وضعیتی(Olofintuyi, 2021: 393)**

**پیشینه و سابقه پژوهش**

شوشیان (۱۳۹۹) در پژوهشی با عنوان مدل‌سازی حملات سایبری مبهم مبتنی بر فن جایگزین حمله، با ارائه طبقه‌بندی جدیدی در روش‌های مبهم‌سازی، برای مدل‌سازی حملات سایبری مبهم، روشی مبتنی بر فن جایگزین حمله پیشنهاد کرده است. در این روش مهاجم در راهبردهای حمله با جایگزین‌کردن حملاتی که خصوصیات مشابه دارند، باعث افزایش دسته‌بندی غلط شده و وابستگی میان گام‌های حمله را کاهش می‌دهد؛ بنابراین با افزایش طول دنباله حمله، مدیران امنیت شبکه به‌راحتی نمی‌توانند حملات سایبری را تشخیص دهند، مدل پیشنهادی بر اساس الگوریتم بیزین ارزیابی گردیده است. نتایج به‌دست‌آمده از تحقیق و اجرای مدل، حاکی از آن است که فن جایگزین حمله یا کاهش نرخ طبقه‌بندی درست در دنباله حملات، می‌تواند مدافعین امنیت شبکه را فریب دهد و به‌خاطر وسعت و دامنه اجرا، مبهم‌سازی را برای مهاجم ساده و تشخیص حملات را برای مدافعین بسیار سخت خواهد کرد. در صورت به‌کارگیری ترکیبی این فن یا سایر فنون مبهم‌سازی در دنباله حملات، تشخیص حملات سایبری سخت‌تر خواهد شد.

نصرت‌آبادی (۱۳۹۷) در پژوهشی با عنوان ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران، منابع قدرت را منابع فیزیکی و زیرساختی، اطلاعاتی، شناختی، ماهیت قدرت را ابزار مؤثر ارعاب علیه رقبا، ابزاری راهبردی و برتر ساز، مبتنی بر فناوری‌های مدرن، فراهم آورنده فضای نبرد آینده و پیامدهای قدرت را بازدارندگی سایبری، اشراف اطلاعاتی، برتری عملیاتی، ارتقای امنیت ملی معرفی می‌کند. در پایان عوامل مؤثر برای ارزیابی نیروهای مسلح در سه بعد آفند سایبری، پدافند سایبری و تاب‌آوری سایبری تقسیم‌بندی کرده است.

در تحقیقات پیشین به چگونگی ارزیابی قدرت آفند سایبری در سطح ملی یا چگونگی ارزیابی قدرت سایبری سازمان‌های نیروهای مسلح پرداخته شده است درحالی‌که در این پژوهش موضوع تحدید به بررسی چگونگی ارزیابی قدرت سایبری در ارتش جمهوری اسلامی ایران شده است و در این تحقیق جنبه‌هایی از قدرت سایبری در نظر گرفته شده است که با مأموریت ذاتی ارتش - آفند و پدافند در برابر حملات دشمنان است - مطابقت داشته باشد پس شاخص‌های به‌دست‌آمده در این پژوهش با پیشینه‌ها متفاوت بوده و با هدف دستیابی به معیارهای کامل و عملی برای ارزیابی قدرت آفند سایبری ارتش بوده تا متولیان امر سایبری ارتش جمهوری اسلامی از نتایج آن برای ارزیابی وضعیت آفند سایبری استفاده نمایند و بتوانند باتوجه‌به وضع موجود، محیط داخلی و تعیین نقاط ضعف و قوت، برنامه‌ریزی مناسبی برای رفع نقاط ضعف و ارتقای توانمندی‌ها انجام دهند.




**شکل (۴) مدل مفهومی**

## روش‌شناسی پژوهش

روش اجرای پژوهش توصیفی است، نوع این تحقیق کاربردی است و رویکرد این تحقیق آمیخته است. صاحب‌نظران انتخاب شده همگی از فرماندهان و مسئولین و متخصصین آگاه در حوزه سایبری هستند که به موضوع تحقیق آشنایی کامل دارند؛ سؤال‌ها به‌گونه‌ای طراحی شده است که تمام ابعاد موضوع را پوشش دهد و محقق را در دستیابی به هدف تحقیق یاری دهد. سؤالات مصاحبه به گروهی از صاحب‌نظران در زمان‌های متفاوت ارائه شده و پاسخ‌های ارائه شده به‌منظور سنجش روایی سؤالات مصاحبه مقایسه شدند.

از اسناد و مدارک معتبر موجود در کتابخانه‌ها و مقاله‌های علمی از سایت‌های اینترنتی معتبر استفاده شده است و همچنین با استفاده از منابع متعدد پر ارجاع بر میزان اعتبار منابع افزوده شده و برای اطمینان از اعتبار منابع، از نظرات متخصصین موضوع و اساتید محترم استفاده شده است.

جامعه آماری این تحقیق، شامل کارکنان ارتش جمهوری اسلامی ایران در طیف درجات افسر ارشد و بالاتر هستند که دارای مدرک تحصیلی کارشناسی و بالاتر در رشته‌های مرتبط با علوم سایبری بوده و دارای حداقل ۱۰ سال سابقه خدمت در مشاغل مرتبط با فضای سایبر باشند. توزیع فراوانی جامعه آماری برحسب مدرک تحصیلی و سن خدمتی به شرح زیر است.

**جدول (۲) توزیع فراوانی جامعه آماری بر حسب مدرک تحصیلی**

| تحصیلات | فراوانی | درصد فراوانی |
|---|---|---|
| کارشناسی | ۲۵ | ۶ .۳۱ |
| کارشناسی ارشد | ۴۵ | ۵۷ |
| دکتری | ۹ | ۴ .۱۱ |
| جمع | ۷۹ | ۱۰۰ |

**جدول (۳) توزیع فراوانی جامعه آماری بر حسب سن خدمتی**

| سن خدمتی | فراوانی | درصد فراوانی |
|---|---|---|
| ۱۰ تا ۱۵ سال | ۱۳ | ۵ .۱۶ |
| ۱۶ تا ۲۵ سال | ۴۰ | ۶ .۵۰ |
| بالاتر از ۲۶ سال | ۲۶ | ۹ .۳۲ |
| جمع | ۷۹ | ۱۰۰ |

از طیف لیکرت برای کمی‌سازی نتایج پرسش‌نامه استفاده شده است و آلفای کرونباخ محاسبه شده برای پاسخ سؤالات جامعه آماری برابر ۰/۸۴۴ است که نشان‌دهنده پایایی سؤالات پرسش‌نامه است.

## تجزیه‌وتحلیل داده‌ها

### تجزیه‌وتحلیل کیفی

برای ارائه الگوی ارزیابی قدرت آفند سایبری ارتش جمهوری اسلامی ایران، با پردازش اطلاعات به‌دست‌آمده چهار عامل نیروی انسانی، پیچیدگی سایبری، تسلیحات سایبری و آگاهی وضعیتی دارای اهمیت بالاتر هستند.

**عامل نیروی انسانی**

عملیات سایبری دانش‌محور است پس برای نیل به قدرت آفند سایبری، نیروی انسانی خبره، متخصص، کیفی، خلاق، باتجربه نیاز است. این امر با آموزش مستمر و بروز رسانی آموزش‌های تخصصی در سه دسته مهارت‌های شناسایی، حمله و دفاع سایبری حاصل می‌گردد.

**پیچیدگی سایبری**

برای پیچیده کردن حملات سایبری و حفظ گمنامی در فضای سایبر باید مبهم‌سازی حمله سایبری انجام شود. رشد فناوری‌های جدید، و استفاده از هوش مصنوعی و هوشمندی باعث پیچیدگی روزافزون حملات سایبری می‌گردد. لایه‌های مختلف دفاعی و امنیتی با ایجاد پیچیدگی در فضای سایبر باعث کم‌اثر شدن و موفقیت کم در اقدامات آفندی فضای سایبری می‌گردد. مهاجمین در حملات سایبری پیشرفته با استفاده از حملات چندمرحله‌ای یا استفاده از الگوهای تازه‌ای برای حمله بر اساس لایه‌های فضای سایبری، باعث پیچیدگی حملات سایبری می‌شوند.

**تسلیحات سایبری**

سلاح جنگ سایبری، ترکیبی از دانش و تجهیزات است و بسیاری از ابزارها، بدون صرف وقت زیادی در دسترس هستند؛ ولی نحوه استفاده از آنها و زمینه دانش در افزایش قدرت آفند سایبری مهم است. تسلیحات سایبری، راحت، سریع و با هزینه کمی قابل تهیه و تولید است؛ لذا توسعه سکوهای آفند سایبری که تحت هدایت هوش مصنوعی و شبکه‌ای هستند هزینه کمی دارد. سلاح‌های هوشمند بدون بدنه با ویژگی‌های خودتکثیری، عدم محدودیت مکان جغرافیایی و استفاده از هوش مصنوعی برای انجام حملات سایبری مناسب‌تر از سلاح‌های هوشمند با بدنه هستند. همچنین ارزیابی قابلیت هدف‌گیری یک سلاح، برای سنجش قابلیت اطمینان یک سیستم لازم است.

**آگاهی وضعیتی**

آگاهی وضعیتی، فرایند امنیت سایبری را از استراتژی منفعلانه به استراتژی پیش‌دستانه ارتقا می‌دهد و دستیابی به آن مستلزم رصد فناوری‌های نوین سایبری و شناخت رابطه انسان - فناوری برای ایجاد درک مؤثر از جنبه‌های پیچیده و اغلب مخفی حوزه سایبری است. بازه زمانی بین حمله و تأثیر آن باید موردتوجه قرار گیرد. در زمانی که اندازه و پیچیدگی شبکه‌های بزرگ رایانه‌ای و حجم داده‌های دریافتی زیاد است، برای آگاهی وضعیتی استفاده ترکیبی و یکپارچه از ابزارها و همچنین یکپارچه‌سازی داده‌ها یا ادغام اطلاعات با آگاهی وضعیتی فیزیکی جهت استفاده بهینه از داده‌ها لازم است که انجام شود.

**تجزیه‌وتحلیل کمی**

از نتایج آماری به‌دست‌آمده درباره نیروی انسانی سه شاخص، دانش، تخصص، مهارت دارای میانگین بالاتر از ۴ هستند. در حوزه پیچیدگی سایبری سه شاخص به‌کارگیری لایه‌های مختلف دفاعی و امنیتی، استفاده از فناوری‌های جدید، مبهم‌سازی حمله با میانگین بالاتر از ۴ مورد تأیید پرسش‌شوندگان هستند. در تسلیحات سایبری توانایی هدایت و کنترل سلاح‌ها به‌صورت شبکه‌ای، توانایی هدایت و کنترل سلاح با بدنه با استفاده از هوش مصنوعی، هدایت و کنترل سلاح بدون بدنه با قابلیت خودتکثیری دارای اهمیت بالاتر از ۴ هستند و در آگاهی وضعیتی نیز از نظر جامعه پرسش‌شوندگان سه شاخص حرکت از رویکرد منفعلانه به رویکرد فعال (پیش‌دستانه)، یکپارچه‌سازی و ادغام اطلاعات سایبری و فیزیکی و رصد مستمر فناوری‌های نوین و رخدادهای امنیت سایبری دارای اهمیت بالاتر از ۴ هستند.

نتایج کمی گویای این مطلب است که شاخص‌های ارائه شده برای ارزیابی قدرت آفند سایبری ارتش جمهوری اسلامی ایران، از سطح متوسط به بالا مورد تأیید جامعه آماری است. در ضمن چون میانگین شاخص‌ها بالاتر از ۴ است، امکان بهره‌برداری از آن به میزان زیاد به بالا است.

**تجزیه‌وتحلیل آمیخته برای نیل به هدف پژوهش**

نتایجی که از تجزیه‌وتحلیل کیفی و کمی برای نیل به هدف ارائه الگوی ارزیابی قدرت آفند سایبری ارتش جمهوری اسلامی ایران حاصل شده است، حاکی از آن است که ۱۲ شاخص از شاخص‌های بررسی شده با میانگین بالاتر از ۴ برای ارزیابی حوزه آفند سایبری در اولویت هستند و می‌توانند مدنظر قرار گیرند ترتیب اولویت این شاخص‌ها بر اساس نظر گروه پرسش‌شوندگان و میانگین شاخص‌ها به شرح جدول است:

**جدول (۴) شاخص‌های مناسب برای ارزیابی آفند سایبری**

| شاخص‌های مناسب برای ارزیابی آفند سایبری | | |
|---|---|---|
| اولویت | شاخص | میانگین |
| ۱ | دانش نیروی انسانی | ۴.۴۲ |
| ۲ | رصد مستمر فناوری‌های نوین و رخدادهای امنیت سایبری | ۴.۳۹ |
| ۳ | یکپارچه‌سازی و ادغام اطلاعات سایبری و فیزیکی | ۴.۳۳ |
| ۴ | استفاده از فناوری‌های جدید | ۴.۳۲ |
| ۵ | توانایی هدایت و کنترل سلاح‌ها به‌صورت شبکه‌ای | ۴.۳۲ |
| ۶ | هدایت و کنترل سلاح بدون بدنه (فاقد سکو) با قابلیت خودتکثیری | ۴.۲۸ |
| ۷ | حرکت از رویکرد منفعلانه به رویکرد فعال (پیش‌دستانه) | ۴.۲۵ |
| ۸ | توانایی هدایت و کنترل سلاح با بدنه (دارای سکو) با استفاده از هوش مصنوعی | ۴.۲۵ |
| ۹ | مهارت نیروی انسانی | ۴.۲۴ |
| ۱۰ | تخصص نیروی انسانی | ۴.۱۹ |
| ۱۱ | به‌کارگیری لایه‌های مختلف دفاعی و امنیتی | ۴.۱۳ |
| ۱۲ | مبهم‌سازی حمله | ۴.۰۶ |

## نتیجه‌گیری و پیشنهادها

### نتیجه‌گیری

در حال حاضر ترکیب خودکارسازی و استفاده از هوش مصنوعی و با هدف دستیابی به خودمختاری سلاح سایبری در طراحی و ساخت تسلیحات سایبری مدنظر سازندگان است. برنامه‌های کاربردی سیستم‌های خودگردان در آینده نزدیک ممکن است شامل شبکه‌هایی از سیستم‌های دارای بدنه و بی‌بدنه باشند. از دیدگاه عملیاتی، رفتار جمعی هوشمند یا استراتژی‌های جمعی، نوید قابلیت‌های جدید و قدرتمند باورنکردنی را می‌دهد. سیستم‌های شبکه‌ای قادر خواهند بود برخی از وظایف را به طور مستقل با نظارت بشر انجام دهند، به‌ویژه هنگامی که سرعت یک مزیت باشد، سلاح‌های آینده باهوش‌تر و مشارکت‌کننده‌تر خواهند بود. چنین سیستم‌هایی ازاین‌جهت جذاب به نظر می‌رسند که نیرویی می‌تواند هر تعداد از آنها را از دست بدهد بدون اینکه عواقب زیان‌بار، تهدید نتایج استراتژیک، تهدید بودجه یا هرگونه ازدست‌دادن قابلیت‌های کلی متوجه او باشد. چنین موجی برای عملیات زمینی و دریایی درحال‌توسعه است و قبلاً به‌صورت عملی در عملیات هوایی مستقر شده است.

برای کسب موفقیت در حوزه جنگ‌های سایبری نیروی انسانی مناسب است که دارای طیف گسترده‌ای از مهارت‌های فنی بوده، بسیار خلاق و درک کلی نسبتاً خوبی از هک، شبکه، توسعه شبکه، مدیریت سامانه و سایر حوزه‌های مشابه داشته باشد. آموزش نسل بعدی و کسانی که در آینده به جنگ سایبری خواهند پرداخت، یک چشم‌انداز جالب است. نه‌تنها باید به افراد تازه‌وارد در این رشته آموزش داد، بلکه باید به نیروی کار کنونی خود برای مقابله با مسائل جدید نیز آموزش دهیم.

**پیشنهادها**

با درنظرگرفتن مدل مفهومی ارائه شده، برای ارتقای نتیجه ارزیابی از شاخص‌های احصا شده در حوزه آفند سایبری، پیشنهادهای اجرایی زیر ارائه می‌گردد:

- ✓ پیشنهاد می‌گردد: معاونت آموزش آجا با همکاری سایربخش های مرتبط از جمله معاونت نیروی انسانی و معاونت فاوای آجا و قرارگاه جنگ‌های نوپدید، نسبت به ارزیابی مستمر دانش، تخصص و مهارت نیروی انسانی فعال در حوزه‌های سایبری اقدام نماید و دوره‌های آموزشی لازم را با همکاری دانشگاه‌ها و مراکز آموزشی آجا جهت ارتقا و رفع نقاط ضعف در حوزه‌های دانش، تخصص و مهارت نیروی انسانی را طرح‌ریزی، به‌روزرسانی و اجرا نماید.
- ✓ پیشنهاد می‌گردد: معاونت فاوای آجا با همکاری سایربخش های مرتبط از جمله معاونت اطلاعات آجا، قرارگاه جنگ‌های نوپدید، مرکز مطالعات راهبردی آجا و دافوس آجا، نسبت به رصد مستمر فناوری‌های نوین سایبری و تجزیه‌وتحلیل آن اقدام نماید تا به آگاهی وضعیتی مطلوب و به‌موقع برای مقابله با رخدادهای امنیت سایبری دست یابد.
- ✓ پیشنهاد می‌گردد: معاونت فاوای آجا با همکاری معاونت اطلاعات آجا، نسبت به یکپارچه‌سازی و ادغام اطلاعات سایبری و فیزیکی برای درک درست وضعیت و در نتیجه فهم و تجسم صحیح اقدامات دشمن و خودی اقدام نماید.
- ✓ پیشنهاد می‌گردد: معاونت فاوای آجا با همکاری سایربخش های مرتبط از جمله قرارگاه جنگ‌های نوپدید، نیروهای چهارگانه آجا و اداره تحقیقات و جهاد خودکفایی، برای

افزایش پیچیدگی در آفند سایبری نسبت به استفاده از فناوری‌های جدید و به‌کارگیری لایه‌های مختلف دفاعی و امنیتی پیش‌بینی، طرح‌ریزی و اقدامات لازم را انجام دهد.

- ✓ پیشنهاد می‌گردد: معاونت عملیات آجا با همکاری سایربخش های مرتبط از جمله معاونت فاوای آجا، قرارگاه جنگ‌های نوپدید، اداره تحقیقات و جهاد خودکفایی و مرکز صنعتی آجا، نسبت به تجهیز سلاح‌ها به توانایی هدایت و کنترل به‌صورت شبکه‌ای و استفاده از هوش مصنوعی، اقدام و گام‌های عملی بردارد.

**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 قرار گرفته است بسیار سپاسگزاریم.

## منابع


- احمدی، سیروس. (۱۳۹۹). *نبرد سایبری کالبدشکافی امنیت جهانی*، چاپ اول، تهران: انتشارات دافوس.
- آذر، داود و ملکی، علیرضا. (۱۳۹۸). *جنگ سایبر و راه‌های مقابله با حملات سایبری*، تهران، انتشارات دافوس.
- اکبری، حمید، صفوی همامی، سیدمصطفی و خاندانی، رضوان. (۱۳۹۸). آگاهی وضعیتی حملات منع خدمت توزیع شده بر اساس پیش‌بینی (تجسم آینده نزدیک) صحنه نبرد مبتنی بر نظریه شواهد دمپستر- شافر و بیزین. پدافند الکترونیک و سایبری، ۷(۱ (پیاپی ۲۵) ): ۷۷-۹۴.
- داداش‌تبار احمدی، کوروش؛ رشیدی، علی جبار و براری، مرتضی. (۱۳۹۳). ارائه یک معماری جدید برای تجسم اثرات حملات سایبری مبتنی بر ادغام اطلاعات سطح بالا در فرماندهی و کنترل سایبری، *مجله علمی – پژوهشی پدافند الکترونیکی و سایبری*، ۲ (۱۴): ۱۴-۱.
- ربیعی، بهزاد؛ علی‌یاری، شهرام و مردانی شهربابک، محمد. (۱۳۹۹). مقاله پژوهشی: معرفی الگویی برای اندازه‌گیری و ارزیابی قدرت سایبری یک سازمان دفاعی در ج. ا. ایران. *راهبرد دفاعی*، ۱۸(۱): ۱۳-۳۶.
- رشیدی، علی جبار. (۱۳۹۶). *آگاهی وضعیتی سایبری*، چاپ اول، تهران: انتشارات دانشگاه صنعتی مالک‌اشتر.
- زابلی زاده، اردشیر، وهاب‌پور، پیمان. (۱۳۹۷). قدرت بازدارندگی در فضای سایبر، *دوفصلنامه علمی - پژوهشی رسانه و فرهنگ*، ۸ (۱۵): ۴۷-۷۴.
- سجادی اصیل، وحید، آذر، داود. (۱۳۹۹). *عملیات سایبری در طرح‌ها و برنامه‌های وزارت دفاع آمریکا*، تهران: انتشارات دافوس آجا.
- شوشیان، کیانوش؛ رشیدی، علی جبار و دهقانی، مهدی. (۱۳۹۹). مدل‌سازی حملات سایبری مبهم مبتنی بر فن جایگزین حمله، نشریه علمی پدافند الکترونیکی و سایبری، ۸ (۱): ۷۷-۶۷.
- مسلمی، حسین و همکاران. (۱۳۹۴). چگونگی ارتقای استفاده مطلوب آجا از فضای سایبر در پشتیبانی از مأموریت‌های مصرحه، گروه مطالعاتی شماره ۶، دافوس آجا.
- نصرت آبادی، جمشید؛ لشکریان، حمیدرضا؛ مردانی، محمدو موحدی صفت، محمدرضا. (۱۳۹۸). مقاله پژوهشی: ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران. *امنیت ملی*، ۹(۳۱): ۱۷۳-۱۹۸.

- Andress, J. , & Winterfeld, S. (2013). Cyber warfare: techniques, tactics and tools for security practitioners. Elsevier.
- Ju, A. , Guo, Y. , Ye, Z. , Li, T. , & Ma, J. (2019). HeteMSD: a big data analytics framework for targeted cyber-attacks detection using heterogeneous multisource data. Security and Communication Networks, 2019.
- Department of Army. (2017). FM 3-12, Cyberspace And Electronic Warfare Operations, Washington.
- DOD. (2018). JP 3-12, Cyberspace Operations.
- Liivoja, R. , & Väljataga, A. (Eds.). (2021). Autonomous cyber capabilities under international law. NATO Cooperative Cyber Defence Centre of Excellence.
- Nye, J. S. (2010). Cyber power (pp. 1-24). Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs.
- Olofintuyi, S. S. (2021). Cyber Situation Awareness Perception Model for Computer Network. International Journal of Advanced Computer Science and Applications, 12(۱).
- Stoecklin, M. , et al. (2018). DeepLocker: How AI Can Power a Stealthy New Breed of Malware. Retrieved from.
- https: //securityintelligence. com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/
- Ross, R. , et al. (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. Draft NIST Special Publication 800-160, Volume 2.
- Tadda, G. , et al. (2006). Realizing situation awareness in a cyberenvironment. Proceedings of SPIE, Defense and Security Symposium, 6242.
- Trusilo, D. , & Burri, T. (2021). Ethical Artificial Intelligence: An Approach to Evaluating Disembodied Autonomous Systems. In Autonomous Cyber Capabilities under International Law, Chapter 4. NATO CCDCOE Publications.
- U. S. AIR FORCE. (2011). DOCTRINE PUBLICATION (AFDP), 3-12, CYBERSPACE OPERATIONS.
- Rogers, Z. (2021). The Promise of Strategic Gain in the Digital Information Age. The Cyber Defense Review, Army Cyber Institute, 6(1).