فصلنامه علمی امنیت ملی
سال چهاردهم، شماره پنجاه و سوم، پائیز ۱۴۰۳
مقاله ششم از صفحات ۲۱۲-۱۷۷

مقاله پژوهشی: ارایه نظام ارزیابی آمادگی رزم سایبری نیروهای مسلح ج.ا.ایران

حسن محمدی منفرد[۱]، حمیدرضا لشکریان[۲]، محسن آقایی[۳] و کیانوش آزادی[۴]

تاریخ دریافت: ۱۴۰۰/۰۶/۰۸ تاریخ پذیرش: ۱۴۰۱/۰۱/۲۱

چکیده

آمادگی رزم سایبری در نیروهای مسلح یک کشور افزون بر مزیت رقابتی و راهبردی، در افزایش اثربخشی مأموریت‌های محوله و اجرای آن موثر است. «ارزیابی و آگاهی از میزان آمادگی‌ها» به‌عنوان گام نخست برنامه‌های توسعه و تجهیز در نظر گرفته می‌شود. پژوهش حاضر با هدف معرفی نظام ارزیابی آمادگی رزم سایبری انجام شده است.این پژوهش از حیث هدف، از نوع پژوهش‌های کاربردی؛ از نظر ماهیت، توصیفی – همبستگی؛ و از نظر روش تجزیه و تحلیل داده‌ها به صورت آمیخته می‌باشد. جامعه آماری، در بخش کیفی شامل ده نفر از خبرگان حوزه رزم سایبری، مدیران و اساتید دانشگاه در سطح نیروهای مسلح می‌باشد. در بخش کمی، ۵۰ نفر هستند که با استفاده از روش نمونه‌گیری هدفمند و اصل اشباع نظری انتخاب شده‌اند. داده‌ها در بخش کیفی با مطالعه تحقیقات پیشین و اخذ نظر خبرگان از طریق مصاحبه عمیق و در بخش کمی با استفاده از پرسشنامه -که روایی و پایایی (۰/۹۷) آن نیز تأیید شد- گردآوری شدند. نتایج پژوهش نشان می‌دهد اجزای اصلی نظام ارزیابی آمادگی رزم سایبری دارای چهار بخش «ورودی»، «فرآیند»، «خروجی» و «پیامد» می‌باشد. لذا با تمرکز بر ارزیابی عملکردها در راستای به فعلیت در آوردن و آماده نمودن ظرفیت‌ها (ورودی)، پس از تحلیل عاملی تائیدی مرحله اول و دوم داده‌ها با بهره‌گیری از نرم‌افزار لیزرل، نظام مذکور در قالب ۱۵ مؤلفه و ٤ بعد «آمادگی عوامل عملیاتی»، «بستر رزم سایبری»، «روش تار وپود رزم سایبری» و «سبک مدیریت و هدایت سایبری» ارائه شده است.

کلیدواژه‌ها: رزم سایبری، نیروهای مسلح، آمادگی رزم سایبری، نظام ارزیابی، ج.ا.ایران.

[۱] . استادیار دانشگاه عالی دفاع ملی(نویسنده مسئول)، رایانامه: h.mohammadi@sndu.ac.ir
[۲] . دانشیار دانشگاه جامع امام حسین(ع)، رایانامه: h.lashgaryan@ihu.ac.ir
[۳] . استادیار دانشگاه عالی دفاع ملی، رایانامه: aghaea@ut.ac.ir
[۴] . پژوهشگر ارشد فناوری اطلاعات و ارتباطات، رایانامه: k.azad2000@gmail.com

۱. بیان مسئله

آمادگی برای مقابله با جنگ، وظیفه‌ای دینی است که به‌طور صریح برعهده مسلمانان گذاشته شده است. مصداق بارز آن دستور خداوند متعال در آیه شریفه «*وَأَعِدّوا لَهُم مَا استَطَعتُم مِن قُوَّةٍ وَمِن رِباطِ الخَيلِ تُرهِبونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُم*»[1] مبنی بر لزوم حفظ آمادگی و افزایش توان دفاعی در حد امکان می‌باشد. مقام معظم رهبری(مدظله العالی) در دیدار جمعی از فرماندهان و کارکنان ارتش ج.ا.ایران بیان داشتند:

«همهٔ دستگاه‌های جمهوری اسلامی ایران از وزارت دفاع تا سازمان‌های ارتش و سپاه و دیگر دستگاه‌های مختلف، باید آمادگی‌ها را روزبه روز افزایش بدهند؛ هم در زمینهٔ تسلیحات، هم در زمینهٔ سازماندهی‌ها، هم در زمینه آن چیزی که در نیروهای مسلّح بیشترین تأثیر را دارد. حفظ بصیرت، حفظ جهت‌گیری صحیح، روحیهٔ خوب و افزایش روز افزون تجهیزات و امکانات یکی از کارهای اساسی‌ای است که نیروهای مسلّح بایستی داشته باشند» (بیانات مقام معظم رهبری ، ۱۳۹٤/۰۱/۳۰).

آمادگی نیروهای مسلح برای رفع تهدیدات دشمن همواره یکی از دغدغه‌های جدی تصمیم‌گیرندگان سیاسی است. به‌طوری‌که در سیاست‌های کلی ج.ا.ایران، به طور خاص به ارتقای میزان آمادگی نیروهای مسلح برای (۱) بازدارندگی، (۲) ابتکار عمل و مقابله مؤثر در برابر تهدیدها، (۳) حفاظت از منافع ملی، انقلاب اسلامی و منابع حیاتی کشور اشاره شده است.

در سیاست‌های ابلاغی و اسناد بالادستی نیروهای مسلح ج.ا.ایران بر دستیابی به سطح مطلوب از آمادگی رزمی تاکید شده است. نکته قابل‌توجه در آمادگی رزمی، چگونگی

---

[1]. قرآن کریم، سوره انفال، آیه ٦۰.

آمادگی نیروهای مسلح در برابر تهدیدات نوین از جمله تهدیدات سایبری می‌باشد؛ زیرا در عصر حاضر، یکی از بهترین و کم‌هزینه‌ترین روش‌ها و گزینه‌های حمله به دیگر کشورها، بهره‌برداری از ویژگی‌ها و ظرفیت‌های فضای سایبری است. گسترش منازعات به فضای سایبری و استفاده از فناوری‌های این حوزه در قالب تسلیحات سایبری برای تهدید کشورها به شکل جنگ سایبری نیز لزوم توسعه و گسترش مفاهیم آمادگی رزمی به فضای سایبر را به‌عنوان راهبردی جهت جلوگیری از ایراد خسارت به منافع ملی کشورها آشکار نموده است.

با نگرش به پیچیدگی و درهم‌تنیدگی عوامل مؤثر در رزم سایبری، بخش دفاعی–امنیتی کشور در حوزه سایبری با طیف وسیع و پیچیده‌ای از تهدیدات و حملات سایبری (در کلیه ابعاد فضای سایبر اعم از فیزیکی، اطلاعاتی و شناختی)، فراوانی متغیرها، تنوع و تعدد بازیگران بین‌المللی و منطقه‌ای، افزایش مأموریت‌ها و وظایف رزمی و فشارهای مالی و بودجه‌ای مواجه شده و خواهد شد. این عوامل، آمادگی برای رزم سایبری را تحت‌تأثیر عوامل متعددی قرار داده است که تا کنون به طور کامل شناسایی نشده است. بخشی از این عوامل عبارت‌اند از:

۱) مواجهه با تهدیدهای ناشناخته سایبری و عدم قطعیت در ظهور آن‌ها در صحنه راهبردی، تأمین نیروی انسانی ماهر و کارآزموده متناسب با نیازهای عملیاتی رزم سایبری، ۲) افزایش محدودیت منابع دانشی و مالی به‌منظور تجهیز و دستیابی به تسلیحات حوزه رزم سایبری در آینده، ۳) میزان آمادگی رزم سایبری در نیروهای مسلح به‌عنوان مزیتی رقابتی و راهبردی در افزایش اثربخشی و اجرای مأموریت‌های محوله محسوب می‌گردد. ارزیابی و آگاهی از میزان آمادگی‌ها، به‌عنوان گام نخست برنامه‌های توسعه و تجهیز در این حوزه نیز در نظر گرفته می‌شود. به همین دلیل،

فقدان نظام ارزیابی و کنترل در یک سازمان به معنای عدم برقراری ارتباط با محیط درون و برون می‌باشد که پیامدهای آن کهولت و در نهایت مرگ سازمان است. از طرفی دیگر، سرمایه‌گذاری در این حوزه مستلزم شناخت و درک عمیق سیاست‌گذاران و فرماندهان نظامی از ظرفیت‌های بالقوه، بالفعل و پیامدهای این حوزه در صحنه رزم سایبری و داشتن تصویر صحیح از وضعیت موجود و توجه به وضعیت مطلوب می‌باشد. لذا مسئله مهمی که فراروی نیروهای مسلح قرار دارد، فهم و پرسش از چگونگی فرایند نظام‌مند و جهت‌گیری سیستمی در ارتباط با نهادینه و چارچوب‌سازی مؤلفه‌های ارزیابی آمادگی رزم سایبری و کنش‌های میان اجزای آن می‌باشد که ریشه در ضعف دانشی در این حوزه دارد.

نظام ارزیابی آمادگی رزم سایبری به فرایندی سیستماتیک و هدفمند برای جمع‌آوری داده‌های حاصل از عملکرد فرماندهان و مسئولین در این حوزه و تبدیل آن به‌دانش، نیاز دارد تا نسبت به کمیت وکیفیت تحقق میزان دسترسی به اهداف، آثار و پیامدهای آنها، موفقیت و یا ناکامی آگاهی داشته و از آن برای سیاست‌گذاری، تصمیم‌سازی و تصمیم‌گیری بهره گیرند. لذا ارائه نظام آمادگی رزم سایبری به‌منظور زمینه‌سازی و ایجاد سازوکار و چارچوب‌هایی برای انجام تکالیف فردی، سازمانی و هم‌افزایی بین آن‌ها لازم است؛ به‌گونه‌ای که نیروهای مسلح ج.ا.ایران قادر به افزایش میزان آمادگی رزم سایبری و یا حفظ آن به‌واسطه نقش بااهمیت آن در افزایش قدرت بازدارندگی ج.ا.ایران باشند و این مسئله، ضرورت قطعی و گریزناپذیر نیروهای مسلح می‌باشد. عدم تبیین آن می‌تواند خسارت‌های جبران‌ناپذیری به کشور تحمیل و دشمن با استفاده از فناوری‌های پیشرفته در ایجاد بحران‌ها موفق گردد.

این پژوهش از آن جهت حائز اهمیت است که با ارائه نظام ارزیابی آمادگی رزم سایبری، مزیت‌های زیر حاصل می‌گردد:

۱) سبب شکل‌گیری درک مشترک و همگرایی بازیگران و سیاست‌گذاران این حوزه می‌گردد. ۲) زمینه‌ساز گفتمان‌سازی و توسعه دانش برای انجام فعالیت‌های پژوهشی در آینده می‌شود. ۳) انجام این پژوهش در راستای برطرف نمودن نیاز نیروهای مسلح درخصوص ارزیابی آمادگی رزم سایبری و دستیابی به مبنایی برای کنترل و ارزیابی فرماندهان سایبری می‌باشد. ٤) موجب ارائه تصویر روشن و دقیق از پیشرفت برنامه‌های تقویت و توسعه آمادگی رزم سایبری می‌گردد. ۵) کشف و رصد قابلیت‌ها و توانمندی‌های نیروهای مسلح ج.ا.ا را در حوزه رزم سایبری درپی‌دارد.

ضرورت انجام این تحقیق با رویکرد سلبی عبارتند از: ۱) باتوجه به تهدید دشمن به جنگ سایبری، فقدان نظام جامع ارزیابی آمادگی رزم سایبری افزایش ضریب غافلگیری ج.ا.ایران در مواجهه با تهدیدات سایبری را دربر دارد. ۲) فقدان نظام مناسب ارزیابی آمادگی رزم سایبری در نیروهای مسلح، سبب اعمال نظر غیرکارشناسی و ابهام تصمیم‌گیران این حوزه می‌شود. ۳) بستر مناسبی برای مفهوم‌شناسی درک صحیح از عوامل کلیدی ارزیابی آمادگی رزم سایبری فراهم نشده و پاسخگویی به نیازمندی این حوزه نیروهای مسلح همچنان انجام نخواهد شد. ٤) بی‌توجهی در تدوین نظام ارزیابی آمادگی رزم سایبری، موجب غفلت در کشف و پیش‌بینی قابلیت‌ها و توانمندی‌های سایبری نیروهای مسلح می‌گردد. ۵) فقدان نظام ارزیابی آمادگی رزم سایبری عامل واگرایی در مدیریت کلان برنامه‌های تثبیت و ارتقاء میزان آمادگی رزم سایبری می‌شود.

باتوجه به موارد بالا، هدف اصلی «دستیابی به نظام ارزیابی آمادگی رزم سایبری» می‌باشد. لذا چهار هدف فرعی، پژوهش را در جهت نیل به ترسیم نظام مذکور هدایت

می‌نماید: ۱) شناسایی اجزای اصلی شکل‌دهنده نظام ارزیابی آمادگی رزم سایبری نیروهای مسلح ج.ا.ایران، ۲) شناسایی ابعاد و مؤلفه‌های ارزیابی آمادگی رزم سایبری نیروهای مسلح ج.ا.ایران، ۳) احصاء روابط بین ابعاد و مؤلفه‌های ارزیابی آمادگی رزم سایبری نیروهای مسلح ج.ا.ایران، ٤) تبیین ارتباط میان عناصر و اجزای نظام ارزیابی آمادگی رزم سایبری نیروهای مسلح ج.ا.ا.ایران،

۲. ادبیات و مبانی نظری تحقیق

پیشینه‌شناسی

«مرکز بلفر»[1] وابسته به دانشگاه هاروارد آمریکا مدلی برای اندازه‌گیری قدرت سایبری ملی کشورها ارائه نموده است. در این مدل، قدرت سایبری از چندین اجزای سازنده تشکیل شده است که بایستی مورد توجه اهداف ملی کشورها قرار بگیرد. این الگو، اندازه‌گیری قدرت سایبری ملی را بر اساس میانگین حسابی ۷ هدف ملی مورد سنجش قرار می دهد: (۱) نظارت بر گروه‌های داخلی، (۲) تقویت و بهبود دفاع سایبری ملی، (۳) کنترل و اداره کردن محیط اطلاعات، (٤) جمع‌آوری اطلاعات پنهان، (۵) بهبود و افزایش رشد صنایع داخلی، (٦) تخریب یا غیر فعال کردن زیرساخت‌ها و قابلیت‌های نیروهای متخاصم، (۷) تعریف هنجارها و استانداردهای بین‌المللی سایبری (مرکز بلفر، ۲۰۲۰).

سامان کشوری و همکاران در پژوهش «ارائه مدل تصمیم‌یار فرماندهی عملیات سایبری مبتنی بر مدل مارکوف زیست‌آهنگ» به این نتیجه رسیدند؛ از چالش‌های اساسی در طرح‌ریزی عملیات سایبری، تعیین مأموریت‌های افراد متناسب با شرایط جسمی و روحی آن‌ها قبل از به‌کارگیری در عملیات است. علاوه‌بر مدل‌سازی دوره‌های تناوب چهار چرخه زیست‌آهنگ براساس مدل

[1] Belfer

مارکوف، مأموریت‌های یک عملیات سایبری برای طرح‌ریزی در مدل پیشنهادی نیز استخراج شده و فرماندهان با مراجعه به این مدل، نیروهای خود را در مأموریت‌های متناسب با شرایط زیست‌آهنگ آن‌ها به‌کار می‌گیرند(۱۳۹۷). کیم و همکاران[1]در «نظام عملیات سایبری شامل فرایند اجرای رزم سایبری و مفاهیم عملیاتی» یک نظام عملیاتی برای رزم سایبری متشکل از ISR (هوش سایبری، نظارت و شناسایی)، فرماندهی و کنترل، دفاع سایبری و ارزیابی آسیب جنگ سایبری ارائه داده‌اند که از طریق آن تصمیم‌گیران می‌توانند به یک مزیت راهبردی پایدار دست یابند. همچنین سامانه شبیه‌سازی برای ارزیابی خسارت جنگی طراحی و اجرا شده است که نتیجه آن به‌عنوان ابزاری برای کمک به تصمیمات فرمانده بکار گرفته می‌شود (۲۰۲۰).

دانشجویان مدیریت راهبردی فضای سایبر دانشگاه عالی دفاع ملی در مطالعه گروهی باهدف «طراحی و معماری نظام کلان فضای سایبر جمهوری اسلامی ایران با رویکرد دفاعی- امنیتی» به این نتیجه رسیدند؛ معماری کلان فضای سایبر ج.ا.ایران با رویکرد دفاعی امنیتی دارای فرایند جرم‌شناسی و اطلاعاتی، پدافند و آفند در سه سطح دفاعی-امنیتی شامل ایمنی در سطح فردی و سازمانی، امنیت در سطح ملی و دفاع در سطح منطقه‌ای و بین‌المللی می‌باشد (۱۳۹۹).

هلیلی و همکاران در مقاله «قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر» با هدف مفهوم‌سازی قدرت سایبری تلاش کردند با رویکرد فرکتالی، تأثیر آن بر امنیت ملی در فضای سایبر را بررسی نمایند. براین اساس، قدرت سایبری دارای تمامی ویژگی‌های قدرت ملی است. قدرت سایبری را با ۱۵ مؤلفه و در قالب سه بعد «سخت»، «نیمه‌سخت» و «نرم»؛ و امنیت ملی را با ۹ مؤلفه در قالب دو بعد امنیت «ذهنی» و «عینی» احصاء نمودند. برابر نتایج؛ داشتن (۱) منابع، (۲) تجهیزات و (۳) فناوری‌های سایبری به‌عنوان شرط لازم برای دستیابی به امنیت ملی مطرح است (۱۳۹۷).

[1]. Kim, S.: Kang, J.: Oh, H.: & Shin, D.

نصرت‌آبادی در «الگوی ارزیابی قدرت سایبری نیروهای مسلح ج.ا.ایران» باهدف دستیابی به الگوی راهبردی سنجش قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران با روش آمیخته و اخذ نظر خبرگان سایبری انجام داد. سرانجام الگوی ارزیابی قدرت سایبری نیروهای مسلح ج.ا.ایران پس از تأیید نهایی نخبگان سایبری، ۱۱ مؤلفه و ۵۵ شاخص در قالب سه بعد (۱) «آفند سایبری»، (۲) «پدافند سایبری» و (۳) «تاب‌آوری سایبری» ارائه گردید (۱۳۹۸).

«ک. آ. ماکریدیس»[3] در «عوامل تعیین‌کننده آمادگی سایبری»[4] در صدد پاسخ به سؤال: «چرا برخی کشورها نسبت به سایر کشورها در مقابل حملات سایبری آماده‌تر هستند؟» است. برابر بررسی‌های او؛ کشورهای دارای فضای امنیتی تهدیدآمیزتر، از آمادگی سایبری بالاتری برخوردارند. وی سه چارچوب نظری را برای تبیین و توضیح تغییرات آمادگی سایبری کشورها در نظر گرفته است: ۱) تهدیدات سازمانی، ۲) بازده نهادی و ۳) ظرفیت سازمانی (۲۰۱۸).

بر اساس مطالعات به‌عمل آمده درخصوص اسناد نزدیک به موضوع مورد مطالعه، در گذشته پژوهشی که مستقیماً به «نظام ارزیابی آمادگی رزم سایبری» پرداخته باشد، مشاهده نگردید. این پژوهش بدیع بوده و ازآنجاکه تاکنون در سطح ملی و بین‌المللی در این‌خصوص اقدامی نشده، دارای نوآوری و انجام آن یک ضرورت است.

۲-۱. ادبیات مفهومی

فضای سایبری یک قلمرو جهانی در محیط اطلاعاتی و شامل شبکه وابسته و زیرساخت‌های فناوری اطلاعات (اینترنت، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای، پردازشگرها و کنترل‌کننده‌های مربوط به آنها) است. این فضا همانند محیط اطلاعاتی ابعاد زیر را دارد:

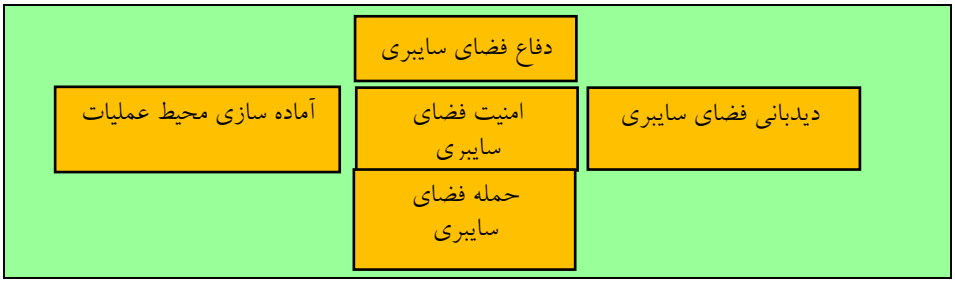
3. Christos Andreas Makridis
4. Determinants of Cyber Readiness

الف) بعد فیزیک: فضای سایبر یک شبکه ارتباطی گسترده جهانی متشکل از زیرساخت‌های ارتباطی و فناوری اطلاعات است.

ب) بعد اطلاعاتی: فضای سایبر یک منبع اطلاعاتی توزیع شده حاوی انواع و سطوح مختلف (۱) داده، (۲) اطلاعات و (۳) دانش از خودی و غیرخودی است.

پ) بعد انسانی: فضای سایبر جامعه‌ای مجازی است و اعضای آن قابلیت انجام فعالیت‌های اجتماعی، اقتصادی، سیاسی و فرهنگی را دارند (وزارت دفاع آمریکا[1] ۲۰۱۸: ۱۲).

طبق تعریف وزارت دفاع آمریکا، عملیات سایبری عبارت از به‌کارگیری قابلیت‌های سایبری در راستای نیل به اهداف از طریق فضای سایبری می‌باشد. ماموریت‌های مربوط به فضای سایبر شامل: (۱) عملیات سایبری تهاجمی، (۲) عملیات سایبری تدافعی و (۳) عملیات شبکه اطلاعاتی وزارت دفاع است (همان: ۸). همچنین در دستورالعمل میدانی عملیات‌های سایبری ارتش آمریکا[2]که در شکل (۱) آمده است، فعالیت‌های سایبری که برای ایجاد تاثیرات مشخص در فضای سایبری انجام می‌شوند عبارتند از: دفاع سایبری[3]، امنیت سایبری، عملیات اطلاعاتی سایبری، آماده‌سازی سایبری، حمله سایبری.



شکل شماره ۱. عملیات‌های سایبری در فضای سایبر (وزارت دفاع آمریکا، اف‌ام ۱۲-۳، ۲۰۱۷)

۲-۱-۱. عملیات اطلاعاتی پایش و شناسایی در فضای سایبری

«عملیات اطلاعاتی پایش و شناسایی در فضای سایبری» براساس شکل شماره دو، شامل فعالیت‌ها و اقداماتی در فضای سایبری است که برای جمع‌آوری اطلاعات لازم برای

---

[1]. Department Of Defense , Cyberspace Operation, J-p 3-12
[2]. FM 3-12
[3]. Cyber Defence

پشتیبانی عملیات تهاجمی سایبری یا عملیات دفاعی سایبری آتی ضروری است. این فعالیت‌ها از طرح‌ریزی و اجرای عملیات‌های سایبری کنونی و آتی پشتیبانی می‌کنند. این عملیات بر اطلاعات نظامی تاکتیکی، عملیاتی و ترسیم فضای سایبری دشمن یا رقیب، برای پشتیبانی و طرح‌ریزی نظامی تمرکز دارد.

۲-۱-۲. آماده‌سازی محیط عملیات سایبری

«آماده‌سازی محیط عملیات سایبری» شامل فعالیت‌های توانمندساز غیراطلاعاتی است که برای برنامه‌ریزی و آمادگی عملیات‌های نظامی بعدی انجام می‌شود. این پدیده شامل موارد زیر است:

۱) شناسایی داده، ۲) نرم‌افزار، ۳) پیکربندی شبکه یا ساختارهای فیزیکی که به شبکه متصل بوده و یا به آن مربوط هستند.

هدف این عملیات که نیازمند نیروهای ماهر و آموزش دیده است؛ شناسایی آسیب‌پذیری‌های سیستم می‌باشد. فعالیت‌های سایبری به‌هم وابسته و مرتبط هستند و درعین‌حال، پشتیبان و حمایت‌کننده ماموریت‌های سایبری هستند.

شکل شماره ۲. جمع‌آوری اطلاعات فضای سایبری (وزارت دفاع آمریکا، اف‌ام ۱۲-۳، ۲۰۱۷)

۲-۱-۳. عملیات تهاجمی سایبری

«عملیات تهاجمی سایبری» گونه‌ای از عملیات‌های سایبری که براساس استفاده از قدرت در فضای سایبر یا از طریق آن طراحی شده است. همانند عملیات تهاجمی در حوزه‌های فیزیکی، عملیات سایبری تهاجمی براساس دستور و مجوزهای صادر شده انجام می‌شود. عملیات سایبری تهاجمی، نیازمند تطبیق با سیاست‌های جاری و کسب مجوز از مقامات ذیصلاح است. این عملیات از نوع ماموریت‌هایی است که به‌منظور نمایش و اعمال قدرت در فضای سایبری غیرخودی یا به‌واسطه آن، علیه دارایی‌های سایبری انجام می‌شود. عملیات سایبری تهاجمی نیاز به ملاحظات دقیق زیر دارد:

۱) سطوح ماموریت، ۲) به‌کارگیری و سازماندهی نیروی‌انسانی متخصص، ۳) نقش و وظایف شرکت‌کنندگان، ٤) اهداف قابل اندازه‌گیری (وزارت دفاع آمریکا[1] ۲۰۱۸: ۱۲).

عملیات سایبری تهاجمی از نظر وزارت دفاع آمریکا عبارت است از: «تلاش برای آسیب‌رسانی، تخریب، مختل ساختن، غیرفعال‌سازی، به‌دست آوردن دسترسی غیر مجاز به رایانه؛ سامانه رایانه‌ای، محیط محاسباتی، زیرساخت محاسباتی، شبکه ارتباطی الکترونیکی از طریق فضای سایبری به منظور از بین بردن جامعیت داده یا سرقت اطلاعات کنترل شده می‌باشد» (آندرس و وینترفلد[2] ۲۰۱٤: ۵۳). همچنین در تعریف دیگری، عملیات سایبری تهاجمی این‌گونه تعریف شده است: «یک حمله یا هجوم با استفاده از جنگ‌افزار سایبری با هدف صدمه‌زدن به یک هدف معین در فضای سایبری می‌باشد. آفند سایبری شامل شناسایی دارائی‌های حیاتی دشمن، شناسایی آسیب‌پذیری‌های این دارائی‌ها، بهره‌برداری از این آسیب‌پذیری‌ها برای دسترسی به این دارائی‌ها به منظور تغییر و یا تخریب این دارائی‌ها می‌باشد» (همان: ۵۳). اقدامات حملات سایبری را می‌توان با توجه به ویژگی‌های گزارش شده و الگوهای حمله آنها، مدل‌سازی کرد که این امر سبب طبقه‌بندی اقدامات حمله در گروه‌های مختلف شده است. در این راستا، فهرست‌های متعددی نیز تهیه شده‌اند. از مهمترین این طبقه‌بندی‌ها می‌توان، دسته‌بندی «حملات سایبری کیپک» را نام برد. در این دسته‌بندی مکانیسم حملات سایبری به ۹ گروه با ویژگی‌ها و اهداف مختلف مطابق جدول (۱) اشاره می‌شود. البته هر دسته خود شامل تعدادی حمله می‌باشد.

---

[1] Department Of Defense , Cyberspace Operation, J-p 3-12

[1] Andrees & Wnterfeld

جدول شماره ۱. دسته‌بندی حملات سایبری (مایتر اتک[1]،۲۰۱۹)	
ردیف	دسته‌بندی حملات
۱	مشارکت در تعاملات فریبنده
۲	سوءاستفاده از عملکرد موجود
۳	دست‌کاری ساختار داده‌ها
٤	دست‌کاری منابع سامانه
٥	تزریق فایل‌های ناخواسته
٦	استفاده از روش‌های احتمالی
۷	دست‌کاری زمان‌بندی و وضعیت
۸	جمع‌آوری و تحلیل اطلاعات
۹	از بین بردن کنترل دسترسی

۲-۱-٤. آمادگی رزم

«آمادگی رزم یا آمادگی نظامی» عبارت‌است از: «شایستگی یک واحد نظامی برای اجرای ماموریت و یا انجام عملکردهایی که برای آنها ایجاد، سازماندهی و طراحی شده است» (ریچارد بتس[2]،۲۰۱۹). ابعاد آمادگی رزم شامل موارد چهارگانه می‌باشد: ۱) آمادگی در پرسنل، ۲) در دسترس بودن تجهیزات و امکانات، ۳) آماده‌بودن تسلیحات، ٤) آموزش و مهارت‌ها (هررا[3]،۲۰۲۰).

۲-۱-٥. نظام ارزیابی آمادگی رزم سایبری

«ارزیابی» فرآیند مستمری است که میزان پیشرفت انجام یک وظیفه، ایجاد یک تاثیر یا دستیابی به یک هدف را مورد ارزیابی قرار می‌دهد. ارزیابی در بخش دولتی یک مفهوم «مبهم»، «چند بعدی» و «پیچیده» است. علی‌رغم اینکه یکی از محبوب‌ترین مفاهیم در نظریه و عمل مدیریت کنونی می‌باشد، اما دانش انباشته در این رشته، فاقد نظر روشن

---

[1]. MITRE ATTCK (CAPEC).

[2]. Rechard Betts

[2]. G. James Herrera

درباره مهمترین عناصر تبیینی برای سنجش و ارزیابی در سازمان‌های دولتی است (سیگل و سامرمتر[1] ۲۰۰۸). «اندرورز» و همکارانش[2] بر این باورند که چندوجهی بودن ارزیابی به این دلیل است که از سازمان‌های دولتی انتظار می‌رود طیفی از اهداف را دنبال کنند که ممکن است برخی از آن‌ها با یکدیگر در تضاد باشند. بنابراین، سازمان‌های دولتی موظفند توجه خود را بر ابعاد چندگانه عملکرد متمرکز نمایند (یاوری، ۱۳۹۲). براین اساس، رویکردهای موجود در ارزیابی عملکرد به دو دسته تقسیم می‌شوند:

الف. رویکرد تک بعدی ارزیابی: در این رویکرد، ارزیابی فقط بر اساس یک بعد (بعد مالی) مورد محاسبه و سنجش قرار می‌گرفت.

ب. رویکرد چند بعدی و ترکیبی ارزیابی: در این رویکرد، علاوه بر تاکید بر درون سازمان، محیط خارجی سازمان را نیز در نظر می‌گیرند (ایران‌زاده، ۱۳۹۷: ۲۸-۱۰).

«نظام» مجموعه‌ای از اجزا، عوامل و عناصری است که دارای موجودیت و هویت معینی هستند و به‌طور منظم با یکدیگر پیوند یافته‌اند تا کنشی را در راستای نیل به هدفی مشخص به‌وجود آورند. در هر نظام، تغییر هر جزء بر اجزای دیگر و بر کل تاثیر می‌گذارد. نظام ارزیابی، با ایجاد یک ساختار منسجم بین اجزای مختلف ارزیابی می‌تواند فرایندهای ارزیابی را هدایت و راهبری کند (کشمیری و همکاران، ۱۳۹۹). براین اساس، نظام ارزیابی آمادگی رزم سایبری شامل تعیین ابعاد، مولفه‌ها و شاخص‌های موثر در ارزیابی آمادگی رزم سایبری با تبیین کارکرد مستقل و وابسته هر یک از آنها با یکدیگر، برای فهم و جهت‌گیری سیستمی در ارتباط با نهادینه نمودن مولفه‌های آمادگی رزم‌سایبری به‌منظور زمینه‌سازی و ایجاد چارچوب‌هایی برای انجام تکالیف فردی، سازمانی و هم‌افزایی بین آن‌ها می‌باشد.

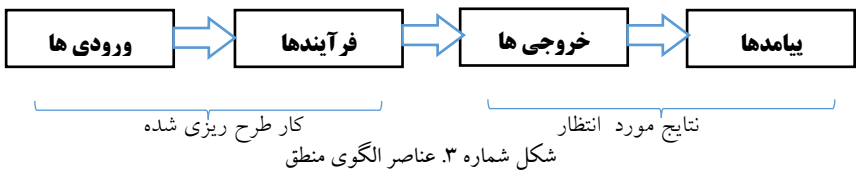
---

[1]. Siegel, john philipp & Summermatter
[2]. Andrews & et.all

به‌گونه‌ای که نیروهای مسلح ج.ا.ایران قادر به افزایش میزان آمادگی رزم‌سایبری و یا حفظ آن باشند، البته در این نظام با الگوگیری از الگوی منطق، توان رزم سایبری مشتمل بر «قابلیت‌ها» و «ظرفیت‌های رزم» به عنوان الزامات و ورودی نظام برای رسیدن به اهداف کلان آمادگی رزم سایبری نیروهای مسلح با رعایت اصول، ارزش‌ها و سیاست‌های مصوب یا ابلاغی نیز تعین و ارائه می‌گردد.

۲-۱-٦. الگوی منطق

«الگوی منطق» ازجمله پدیده‌های علمی مطرح در حوزه شناخت، مفاهمه، طرح‌ریزی و ارزیابی است. ابتدایی‌ترین الگوی منطق، تصویری را از باور موجود نسبت به اینکه یک برنامه مشخص چگونه عمل خواهد کرد، نشان می‌دهد. این الگو از عبارات یا شکل‌هایی استفاده می‌کند که می‌توانند توالی فعالیت‌هایی که گمان می‌رود منجر به تغییر شوند و اینکه چگونه این فعالیت‌ها با نتایج مورد انتظار از اجرای برنامه مرتبط می‌شوند را نشان دهد. در ساده‌ترین حالت، یک الگوی منطق از چهار عنصر همانند شکل (۳) تشکیل می‌شود.



شکل شماره ۳. عناصر الگوی منطق

باوجود اینکه روش‌های مختلفی برای نمایش الگوهای منطق وجود دارد، اما هدف اصلی ساخت یک الگوی منطق، بیان و ارزیابی روابط اگر-آنگاه (علی-معلولی) بین عناصر یک برنامه/هدف است. مطابق شکل (۳) اگر؛

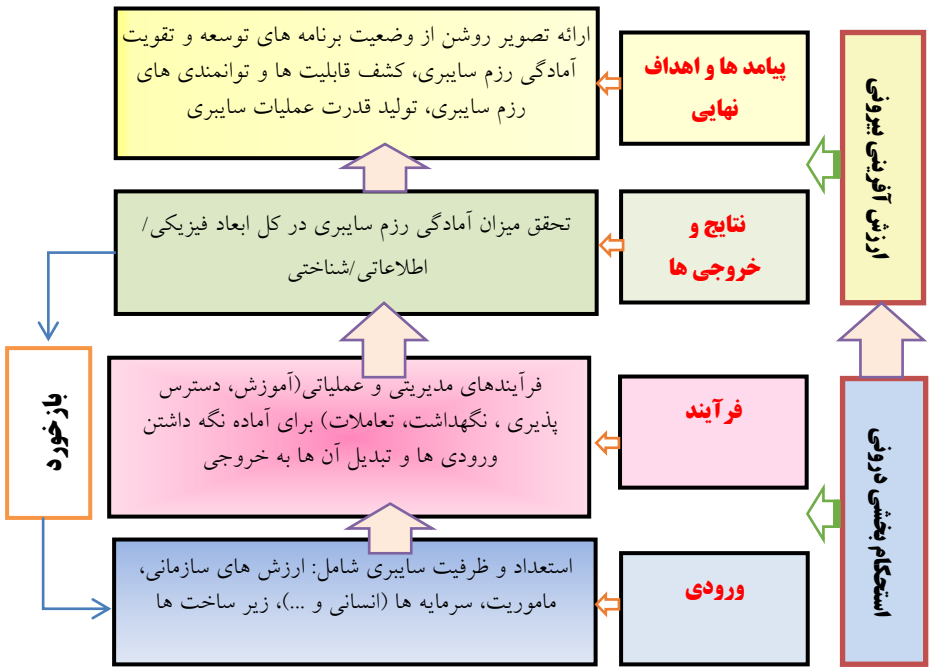
(۱) منابع برای یک برنامه/هدف در دسترس باشند، آنگاه فعالیت‌ها انجام می‌شوند.

(۲) اگر فعالیت‌ها با موفقیت انجام شوند، آنگاه می‌توان انتظار خروجی‌های مورد نظر را داشت.

(۳) اگر خروجی‌ها حاصل شوند، آنگاه پیامدها و آثار ظاهر خواهند شد (رجبی مسرور، ۱۳۹۸: ۹٤).

۲-۲. چارچوب مفهومی تحقیق

باتوجه به ارائه دیدگاه‌های نظری پیرامون موضوع تحقیق و استناد به منابع علمی و مصاحبه عمیق با خبرگان درباره اهداف پژوهش، الگوی مفهومی پژوهش از چهار بخش به شرح شکل (٤) تشکیل شده است.



شکل شماره ٤. اجزاء تصویر مطلوب نظام ارزیابی آمادگی رزم سایبری نیروهای مسلح ج.ا.ایران

همانگونه که ملاحظه می‌شود، این تصویر دارای دو بخش کلان است. ۱) استحکام‌بخشی درونی (سرمایه‌ها/ زیرساخت‌ها و فرآیندها) و ۲) ارزش‌آفرینی بیرونی (نتایج/خروجی‌ها و پیامدها/ اهداف نهایی)

«بخش ورودی» که اساس و جان‌مایه اصلی برای تحقق حرکت بیرونی است، دربرگیرنده استعداد و ظرفیت سایبری برای رزم سایبری می‌باشد و شامل موارد هفت‌گانه: ۱- مأموریت، ۲- ارزش‌های سازمانی، ۳- سرمایه انسانی، ٤- تسلیحات، ٥- فناوری‌ها، ٦- تعاملات، ۷- زیرساخت‌ها به عنوان زمینه‌ها و سرمایه‌های اساسی برای کسب آمادگی رزم سایبری است.

با توجه به شکل (۳) و بر اساس الگوی منطق علی و معلولی، برای به فعلیت درآوردن و آماده نگاه داشتن ظرفیت یا استعدادهای رزمی (عناصر ورودی)، اتخاذ رویکرد فرآیندی از قبیل (فرآیندهای مدیریتی، عملیاتی و پشتیبانی) ضرورت دارد. در این بخش، عملکرد نحوه مدیریت و هدایت سازمان برای آماده نگاه داشتن امکانات و تجهیزات واگذار شده برای اجرای رزم سایبری در حوزه‌های «آموزش و مهارت افزایی»، «نگهداشت و دسترس‌پذیر نمودن نیروی انسانی»، «سلاح و تجهیزات» و «تعاملات درون و برون سازمانی» مورد ارزیابی قرار می‌گیرد. سرانجام نتیجه این آمادگی‌ها تحت عنوان توان رزم سایبری در خروجی نظام مذکور منظور می‌گردد. در انتها، بازخوردهای مراحل خروجی و فرآیندها برای اصلاح و بهبود عملیات در تطابق با اهداف از پیش تعین شده نظام مذکور، ترازیابی و به مرحله ورودی‌ها انتقال می‌یابد.

در این پژوهش تمرکز بر روی ارزیابی عملکردها در راستای به فعلیت در آوردن و آماده نمودن ظرفیت‌ها (ورودی‌ها) یا همان آمادگی رزم سایبری می‌باشد. به این منظور، با جستجوی عمیق در ادبیات تحقیق، فهرستی از عوامل مؤثر بر متغیر وابسته تحقیق تهیه گردید. پس از ترکیب و تلفیق آنها و نظرخواهی از اساتید و خبرگان سایبری، مهمترین عوامل تاثیرگذار بر ارزیابی آمادگی رزم سایبری که نمایش جامع‌تری از پدیده مورد بررسی را آشکار می‌سازد، شناسایی و در جدول (۲) نشان داده شده است.

جدول شماره ۲. عوامل مهم مرتبط با مفهوم اصلی تحقیق (یافته‌های محقق)		
مفهوم اصلی	**عوامل مرتبط با مفهوم اصلی**	**منبع**
آمادگی رزم سایبری	❖ معیارها و مؤلفه‌های آمادگی رزم از نگاه فرمانده معظم کل قوا: ۱- نیروی انسانی، ۲- آموزش، ۳- رزمایش، ٤- تجهیزات، ٥- تسلیحات، ٦- آماد و پشتیبانی، ۷- اطلاعات، ۸- معنویت، ۹- روحیه، ۱۰- انگیزه، ۱۱- شجاعت، ۱۲- ایمان، ۱۳- انضباط، ١٤- بصیرت، ۱٥- عزم راسخ.	(وبگاه مقام معظم رهبری)
	معیارهای آمادگی نظامی: ۱- آمادگی پرسنل و نیروی انسانی، ۲- در دسترس بودن تجهیزات، ۳- آمادگی تجهیزات، ٤- آموزش و مهارت.	(هررا،۲۰۲۰)
	❖ توجه به ابعاد و مؤلفه‌های دکترین آمادگی رزم یگانی در نیروهای مسلح: ۱- روحیه و معنویت، ۲- آمادگی سلاح و تجهیزات، ۳- مهارت‌های تخصصی، ٤- فرماندهی و مدیریت	(آئین نامه آمادگی‌های یگانی، ۱۳۹٦)
	❖ توجه به مدل سه‌بعدی فضای سایبر به عنوان بستر رزم: ۱- بعد فیزیکی ۲- بعد اطلاعاتی ۳- بعد شناختی	(آندرس و وینترفلد، ۲۰۱٤)
	❖ نظام و چارچوب عملیات سایبری: ۱- شناسایی سایبری (ISR)، ۲- فرماندهی و کنترل سایبری، ۳- دفاع سایبری، ٤- ارزیابی ریسک، ٥- حمله سایبری	(کیم[1] و همکاران، ۲۰۲۰)
	❖ توجه به ابعاد دکترین عملیات سایبری نیروهای مسلح ج.ا.ایران: ۱- اشراف اطلاعاتی و مسلط به توانمندی سایبری دشمنان، ۲- آماده به‌منظور به‌کارگیری توان رزم سایبری در انجام عملیات سایبری مستقل و یا ترکیبی با سایر ابعاد جنگ، ۳- توانمند در انجام اقدامات مقابله‌ای بلادرنگ سایبری	(مصاحبه با خبرگان)
	❖ استفاده از مفاهیم مشترک (مضامین پایه) مؤثر در ارزیابی رزم سایبری	(مصاحبه با خبرگان)
	کلان روندهای متأثر از فضای سایبر: ۱- گسترش وب‌های معنایی، ۲- رشد شبکه‌های رسانه‌های اجتماعی، ۳- پردازش ابری، ٤- پردازش داده‌های بزرگ، ٥- اینترنت اشیاء، ٦- محاسبات کوانتومی	(مرکز مبین دانشگاه جامع امام حسین(ع)،۱۳۹۸؛ و مصاحبه با خبرگان)
	توان رزم سایبری نظام سلطه علیه ج.ا.ایران	(مصاحبه با خبرگان)
	ارکان جهت‌ساز رزم سایبری در ج.ا.ایران	(مصاحبه با خبرگان)

[1] Kim

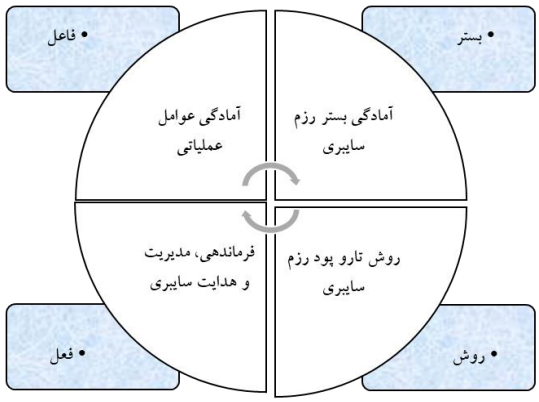
با توجه به مطالب ارائه شده، ارزیابی آمادگی رزم سایبری به عنوان مفهوم اصلی و کلیدی در این پژوهش محسوب می‌شود. در ادامه به‌منظور شناسایی ابعاد و مؤلفه‌های ارزیابی آمادگی رزم سایبری با عنایت به این‌که به‌منظور درک و شناخت درست پدیده‌ها، بایستی موضوع یا پدیده مورد نظر را از منظر (فاعل موضوع، بستر، فعل و روش) مورد بررسی قرار داد (شهیر، ۱۳۹۶: ۱۹۸)، لذا عوامل مؤثر بر این حوزه، پس از مطالعه ادبیات تحقیق و مصاحبه با خبرگان بر اساس جدول (۳) قابل ارائه گردید.

جدول شماره ۳. شناخت ابعاد و مؤلفه‌های رزم سایبری (یافته‌های نگارنده)

			منبع
شناخت ابعاد و مؤلفه های رزم سایبری	**بستر**	سطوح رزم سایبری مشتمل بر: ۱- رزم فیزیکی، ۲- رزم اطلاعاتی، شناختی سایبری	J-p (۲۰۱۸، 3-12)
	فاعل	بازیگران اجرای رزم سایبری اعم از: ۱- نیروی انسانی، ۲- تسلیحات سایبری، ۳- فناوری‌های اجتماعی	J-p (۲۰۱۸، 3-12) مصاحبه با خبرگان
	فعل	فعل، انجام دادن کار برای هدایت و مدیریت سازمان است که به اقتضای موارد زیر تعیین می‌شود: ۱- الزامات، ۲- تعاملات، ۳- تهدیدات پیش‌رو و... .	FM3- (۲۰۱۷، 12) مصاحبه با خبرگان
	روش	روندها یا سناریوهای دسترسی مهاجم به فضای سایبر مبتنی بر آسیب‌پذیری‌ها با استفاده از ابزار و تسلیحات سایبری مورد نیاز و منطبق بر طرح‌های عملیاتی می‌باشد. در این تحقیق روش شامل موارد زیر می‌باشد: اقدامات عملکردی رزم سایبری مبتنی بر مفاهیم عملیاتی: ۱- آگاهی وضعیتی، ۲- تدوین سناریو، ۳- طرح‌ریزی عملیاتی، ٤- ارزیابی.	J-p (۲۰۱۸، 3-12)، (۲۰۱۷، FM3-12) مصاحبه با خبرگان

با توجه به مطالب ارائه شده در جدول (۳)، آمادگی رزم سایبری شامل چهار مقوله اصلی می‌باشد: ۱- آمادگی عوامل عملیاتی رزم سایبری، ۲- بستر اجرای رزم سایبری، ۳- طرح‌ریزی و شیوه رزم، ٤- سبک مدیریت و هدایت سایبری.

براساس داده‌های استخراج شده، اجزاء ارزیابی آمادگی رزم سایبری مطابق شکل (۵) می‌باشد.



شکل شماره ۵. اجزاء ارزیابی آمادگی رزم سایبری (یافته‌های نگارنده)

۳. روش تحقیق

باعنایت به موضوع تحقیق حاضر که مترصد ارائه نظام ارزیابی آمادگی رزم سایبری نیروهای مسلح ج.ا.ایران است و در همین راستا، زمینه ایجاد وفاق در فرایند تصمیم‌سازی در حوزه ارزیابی آمادگی رزم سایبری را فراهم می‌کند. بنابراین این تحقیق براساس هدف در زمره تحقیقات کاربردی قرار می‌گیرد. از طرفی با توجه به تحقیقات محدود در این زمینه می‌تواند مقدمه‌ای برای گسترش مرزهای دانش در این حوزه شود. لذا این تحقیق از نظر نوع، کاربردی-توسعه‌ای است.

در این پژوهش با توجه به هدف و ماهیت موضوع، برای گردآوری و تجزیه و تحلیل داده‌ها از روش تحقیق آمیخته استفاده شده است. در گام نخست و متناسب با هدف‌های این تحقیق نیز برای شناسایی و استخراج اجزاء، ابعاد و مؤلفه‌های نظام ارزیابی مذکور، از روش تحلیل مضمون استفاده شده است. درنتیجه با مطالعه تحقیقات پیشین، ادبیات نظری، مطالعه اسنادی، پیاده‌سازی و کدگذاری مصاحبه‌های انجام شده با تعداد ده نفر از خبرگان موضوع، تعداد ۸٤ مضمون پایه به‌دست آمد. سپس در گام دوم با روش شبکه‌ای (یکی از

روش‌های تجزیه و تحلیل در تحلیل مضمون) مضامین پایه مورد تجزیه و تحلیل قرار گرفته و مضامین سازمان‌دهنده و مضمون فراگیر استخراج شد. در گام بعدی، برای اعتباربخشی اجزاء، ابعاد و مؤلفه‌های نظام ارزیابی آمادگی رزم سایبری از روش پیمایش (میدانی) استفاده گردید که جامعه ۵۰ نفری با ابزار پرسش‌نامه مورد سوال قرار گرفتند. همچنین در ادامه و پس از جمع‌آوری اطلاعات، تعداد ٤٧ پرسش‌نامه از پرسش‌شوندگان، برای تجزیه و تحلیل آماری و میزان رابطه و همبستگی میان عوامل احصاء شده و بررسی روابط بین اجزاء نظام ارزیابی، از مدل‌یابی معادلات ساختاری با استفاده از تحلیل عاملی تائیدی مرحله اول و دوم از نرم‌افزار لیزرل استفاده شده است. جامعه آماری این پژوهش در بخش کیفی (انجام مصاحبه) شامل خبرگان مسلط به مسائل راهبردی فضای سایبر بوده و در حوزه رزم و آمادگی رزم سایبری صاحب‌نظر می‌باشند. بنابراین تعداد آنان بسیار محدود و لذا با بهره‌گیری از روش هدفمند گلوله برفی، تعداد آنها احصاء شده است. با این روش ابتدا در بخش کیفی، تعداد ده نفر از اساتید هیئت علمی دانشگاه‌ها و پژوهشکده‌های مرتبط با سایبر، مدیران و کارشناسان حرفه‌ای در سطوح ستادی و عملیاتی در رابطه با موضوع این تحقیق شناسایی شدند. سرانجام در مرحله بعد به‌منظور اعتبارسنجی نظام ارزیابی و تحلیل روابط بین آن‌ها با توجه به تخصصی‌بودن موضوع تحقیق و محدودیت افراد خبره و صاحب‌نظر مرتبط با موضوع پژوهش، جامعه آماری تحقیق از بین فرماندهان، خبرگان، متخصصان، اساتید و صاحب‌نظران سایبری نیروهای مسلح به تعداد ۵۰ نفر برآورد که به صورت روش نمونه‌گیری تمام‌شمار به آنان رجوع شده است.

٤. تجزیه و تحلیل یافته‌های تحقیق

برای استخراج ابعاد و مؤلفه‌های نظام ارزیابی و تجزیه و تحلیل داده‌های کیفی پژوهش، از روش «تحلیل مضمون» استفاده شد. «مضمون» ویژگی تکراری و متمایزی در متن است که به نظر پژوهشگر، نشان‌دهنده درک و تجربه خاصی در رابطه با سؤالات تحقیق است. لذا در پاسخ به سؤال فرعی اول تحقیق مبنی بر اینکه «اجزای اصلی شکل‌دهنده نظام ارزیابی رزم سایبری نیروهای مسلح ج.ا.ایران کدامند؟» با انجام روش تحلیل مضمون، مضامین مربوط به هریک از این اجزا احصاء و توسط خبرگان اعتبارسنجی، که در ادامه به تشریح هریک پرداخته شده است.

٤-١. اصول حاکم بر ارزیابی آمادگی رزم سایبری

«اصول» بایدها و نبایدها است که شامل دو نوع «پایه» و «کاربردی» می‌باشد. اصول پایه ثابت هستند، اما اصول کاربردی به اقتضای شرایط محیط و موضوع می‌توانند تغییر کنند. اصول حاکم بر این تحقیق پس از تحلیل مضمون و تائید توسط خبرگان در جدول (٤) منعکس شده است.

جدول شماره ٤. اصول حاکم بر ارزیابی آمادگی رزم سایبری (یافته‌های نگارنده)

ردیف	اصول حاکم بر ارزیابی آمادگی رزم سایبری
١	اعتقاد به رصد الهی در ارزیابی کارها
٢	حفظ استقلال و عزت‌مندی
٣	مواجهه فعال و حکیمانه با تهدیدات سایبری
٤	مسلط و آگاه به وضعیت و توانمندی سایبری دشمن
٥	مسلط و آگاه به وضعیت و توانمندی سایبری خودی
٦	آماده به‌منظور به‌کارگیری استعداد و توان رزم سایبری خودی

٤-٢. ورودی

بخش ورودی که اساس برای تحقق حرکت بیرونی و دربرگیرنده استعداد و ظرفیت سایبری برای رزم سایبری می‌باشد. زمینه‌ها و سرمایه‌های اساسی برای کسب آمادگی رزم

سایبری در این تحقیق پس از تحلیل مضمون و تائید توسط خبرگان در جدول (۵) منعکس است.

جدول شماره ۵. زمینه‌ها و ورودی‌های اساسی برای کسب آمادگی رزم سایبری (یافته‌های نگارنده)	
ردیف	زمینه‌ها و ورودی‌های اساسی برای کسب آمادگی رزم سایبری
۱	مأموریت و انتظارات
۲	ارزش‌های سازمانی
۳	منابع (سرمایه انسانی، سرمایه مالی و ...)
٤	تسلیحات سایبری
۵	فناوری‌ها
٦	تعاملات و زیرساخت‌ها

۳-٤. فرآیندها

در این تحقیق، تمرکز اصلی بر ارزیابی عملکردها در راستای به فعلیت درآوردن و آماده‌سازی استعداد رزمی (آمادگی رزم) سایبری می‌باشد. لذا بر اساس الگوی منطق علی و معلولی، برای به فعلیت درآوردن و آماده نگاه داشتن ظرفیت یا استعدادهای رزم سایبری (عناصر ورودی)، اتخاذ رویکرد فرآیندی از قبیل (فرآیندهای مدیریتی، عملیاتی و پشتیبانی) در خصوص این موارد ضرورت دارد: ۱- آموزش، ۲- دسترس‌پذیر نمودن، ۳- تعاملات، ٤- نگهداری و نگهداشت منابع و امکانات در این بخش.

عملکرد سبک مدیریت و هدایت سازمان برای آماده نگاه داشتن امکانات و تجهیزات واگذاری شده برای اجرای رزم سایبری مورد ارزیابی قرار می‌گیرد. فرایندهای آمادگی رزم سایبری در این تحقیق پس از تحلیل مضمون و تائید توسط خبرگان، احصاء و در جدول (٦) منعکس شده است.

جدول شماره ٦. فرآیند آمادگی رزم سایبری نیروهای مسلح (یافته‌های نگارنده)	
ردیف	**فرآیند آمادگی رزم سایبری نیروهای مسلح ج.ا.ا**
۱	آمادگی در عوامل عملیاتی برای رزم سایبری
۲	آمادگی در دسترس‌پذیر نمودن بستر اجرای رزم سایبری

۳	آمادگی در روش تار و پود رزم سایبری
٤	آمادگی در سبک فرماندهی و هدایت سایبری سازمان

٤-٤. خروجی

در «خروجی» نیز نظام ارزیابی، تحلیل و بررسی وضعیت روند داده‌ها از رزم سایبری تحت عنوان میزان آمادگی رزم سایبری منظور می‌گردد. خروجی‌های نظام آمادگی رزم سایبری پس از تحلیل مضمون و تائید خبرگان، احصاء و در جدول (۷) منعکس است.

جدول شماره ۷. خروجی نظام ارزیابی آمادگی رزم سایبری نیروهای مسلح (یافته‌های نگارنده)

ردیف	خروجی نظام ارزیابی آمادگی رزم سایبری
۱	میزان آمادگی رزم سایبری در بعد فیزیکی و زیر ساختی
۲	میزان آمادگی رزم سایبری در بعد اطلاعاتی و محتوایی
۳	میزان آمادگی رزم سایبری در بعد انسانی و شناختی
٤	میزان آمادگی به‌منظور به‌کارگیری توان رزم سایبری
٥	تحلیل و بررسی وضعیت و روند داده‌های مربوط به هریک از ابعاد/مؤلفه‌های رزم سایبری
٦	جهت‌دهی صحیح به برنامه‌ها و رویکردهای عملیاتی در آینده

٥-٤. پیامد

«پیامد» نتایج یا دستاوردهای یک اقدام یا رخداد می‌باشد. خروجی بلندمدت این نظام، پیامدهای راهبردی ناشی از تثبیت و ارتقاء آمادگی رزم سایبری را در سطح سازمانی، ملی و جهانی مشخص می‌نماید. پیامدهای نظام آمادگی رزم سایبری این تحقیق پس از تحلیل مضمون و تائید توسط خبرگان، احصاء و در جدول (۸) منعکس شده است.

جدول شماره ۸ **پیامد نظام ارزیابی آمادگی رزم سایبری** نیروهای مسلح (یافته‌های نگارنده)

ردیف	**پیامد نظام ارزیابی آمادگی رزم سایبری**
۱	ارائه تصویر برنامه‌های توسعه و تقویت آمادگی رزم سایبری
۲	کشف و رصد قابلیت‌ها و توانمندی‌های رزم سایبری
۳	تولید قدرت عملیاتی و پاسخگویی قاطع به تهدیدات سایبری
٤	بازدارندگی سایبری برای ج.ا.ایران
٥	ارتقاء امنیت ملی ج.ا.ایران

٦-٤. عوامل بیرونی تاثیرگذار بر نظام ارزیابی آمادگی رزم سایبری

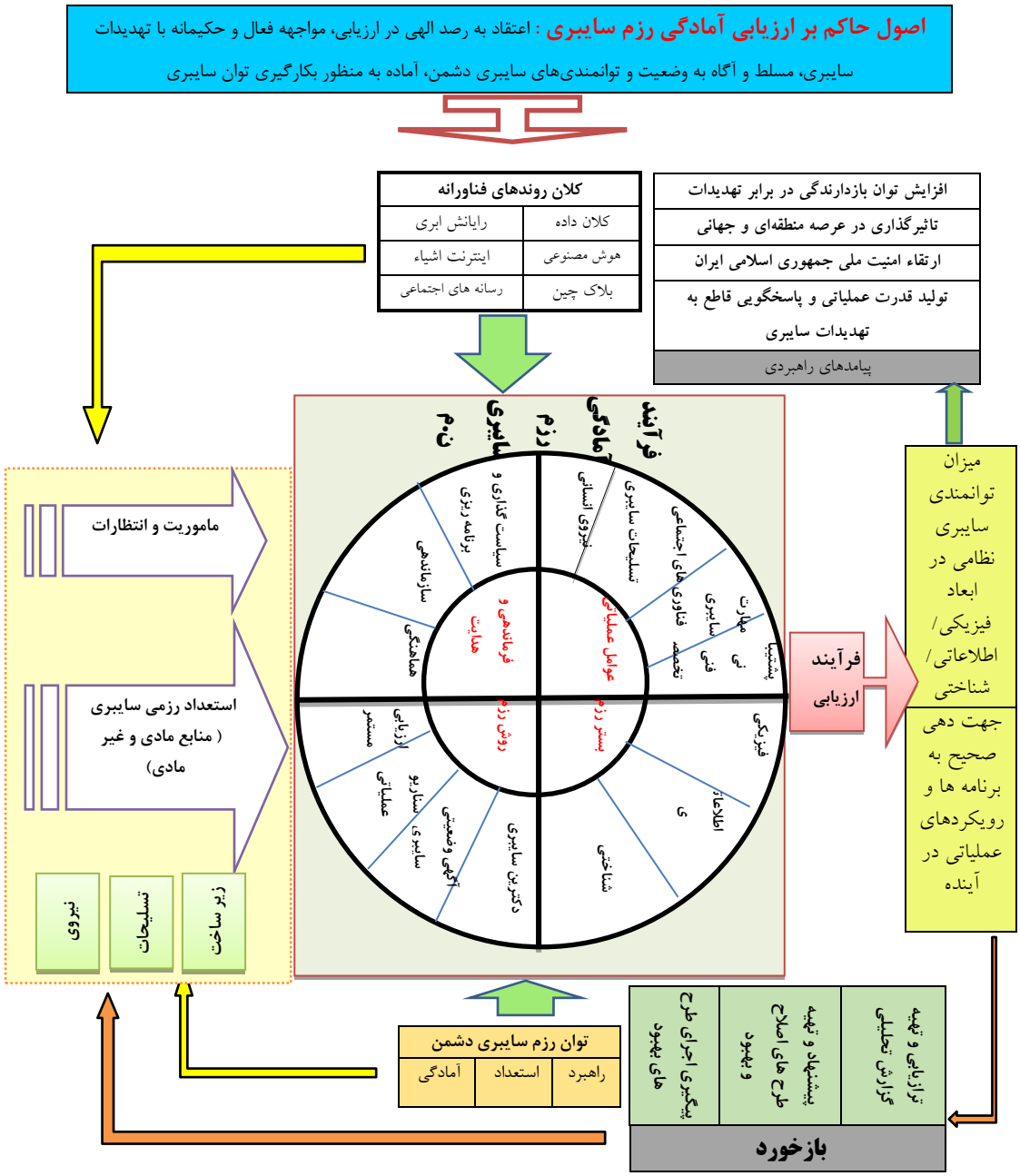
از طرفی عوامل بیرونی تأثیرگذار بر نظام ارزیابی آمادگی رزم سایبری که اجزاء آن را تحت تأثیر قرار می‌دهند، شامل فناوری‌های نوظهور فضای سایبر، میزان قدرت رزم سایبری دشمنان ج.ا.ایران و اصول حاکم و تأثیرگذار بر رزم سایبری نیروهای مسلح ج.ا.ایران تحت عنوان ارکان جهت‌ساز در این حوزه می‌باشد. در این راستا با پذیرش این اصل که آمادگی رزم سایبری شامل آمادگی در مقوله‌های (فاعل، بستر، روش و فعل) رزم سایبری می‌باشد، با تمرکز بر روی هر یک از مقوله‌های مذکور، مضامین پایه (زیر مؤلفه‌ها) مرتبط با آن به‌دست‌آمده. با درنظر گرفتن کدهای احصاء شده در مرحله جمع‌آوری داده به عنوان مضامین پایه، نسبت به تجزیه و تحلیل، دسته‌بندی یافته‌ها و کنترل کیفیت (ارزیابی و کسب نظر خبرگان) اقدام شد. در ادامه نتایج، مطابق جدول (۹) به‌دست آمده است.

جدول شماره ۹. مضامین پایه، سازمان‌دهنده و فراگیر در ارزیابی آمادگی رزم سایبری نیروهای مسلح (یافته‌های نگارنده)

مضمون فراگیر	مضامین سازمان دهنده	نشانگر	مضامین پایه	نشانگر
آمادگی رزم سایبری	آمادگی عوامل عملیاتی	D1	نیروی انسانی سایبری سازمان یافته	C1
			تسلیحات سایبری بومی	C2
			فناوری های اجتماعی بومی	C3
			مهارت‌های سایبری	C4
			پشتیبانی فنی تخصصی	C5
	آمادگی بستر رزم سایبری	D2	فیزیکی شامل: ۱- دسترس‌پذیری زیرساخت‌های سخت‌افزاری دشمن، ۲- دسترس‌پذیری زیرساخت‌های نرم افزاری سایبری دشمن.	C6
			اطلاعاتی شامل: دسترس‌پذیر نمودن خدمات محتوایی، کاربردی و رایانشی سایبری دشمن	C7
			شناختی شامل: ۱- دسترسی به هویت، ۲- دستری به محتوا، ۳- دسترسی به تعاملات کاربران برای شکل‌دهی به ادراک، ترجیحات و علایق کاربران سایبری.	C8

	آمادگی در روش رزم سایبری	D3	دکترین سایبری	C9
			آگهی وضعیتی سایبری خودی و دشمن	C10
			تدوین سناریو عملیاتی	C11
			ارزیابی و تحلیل مستمر با اجرای بازی جنگ و رزمایش	C12
	سبک فرماندهی و مدیریت سایبری	D4	سیاستگذاری و برنامه‌ریزی؛ تهدید در برابر تهدید، مشروعیت‌سازی برای رزم و... .	C13
			سازماندهی شامل: انسجام، شبکه‌سازی و... .	C14
			هماهنگی شامل: تدوین آئین‌نامه‌ها، تعامل، پرهیز از موازی کاری و... .	C15

در نتیجه، مبتنی بر تحلیل کیفی داده‌ها و یافته‌های حاصل از شبکه مضامین نظام ارزیابی آمادگی رزم سایبری، تصویر نهایی نظام پیشنهادی تحقیق به شرح شکل (٦) ارائه شده است.



شکل شماره ۶. نظام ارزیابی پیشنهادی آمادگی رزم سایبری نیروهای مسلح

۷-٤. روایی و پایایی ابزار تحقیق

طبق جدول (۱۰)، مقدار آلفای کرونباخ همه مولفه‌ها و ابعاد پرسشنامه بیش از ۰/۷۰ می‌باشد که نشان‌دهنده پایایی مناسب پرسش‌های طرح شده برای ارزیابی ابعاد و مؤلفه‌ها می‌باشد.

جدول شماره۱۰. محاسبه ضرایب پایایی درونی پرسشنامه‌های تحقیق

ردیف	بعد	مولفه	شماره سوالات	ضریب آلفای کرونباخ مولفه	ضریب آلفای کرونباخ بعد
۱	D1	C1	۱ الی ۵	۰/۸۱	۰/۹٦
۲		C2	٦ الی ۱۲	۰/۸۸	
۳		C3	۱۳ الی ۱۹	۰/۹۰	
٤		C4	۲۰ الی ۳۱	۰/۹۰	
٥		C5	۳۲ الی ۳٤	۰/۷۰	
٦	D2	C6	۳٥ الی ۳۹	۰/۷۸	۰/۷۹
۷		C7	٤۰ الی ٤۳	۰/۷٥	
۸		C8	٤٤ الی ٤۷	۰/۸۰	
۹	D3	C9	٤۸ الی ٥٤	۰/۹۲	۰/۹٦
۱۰		C10	٥٥ الی ٥۹	۰/۸۹	
۱۱		C11	٦۰ الی ٦٤	۰/۹۲	
۱۲		C12	٦٥ الی ٦٦	۰/۸۱	
۱۳	D4	C13	٦۷ الی ۷۳	۰/۹۱	۰/۹٥
۱٤		C14	۷٤ الی ۷۹	۰/۸۸	
۱٥		C15	۸۰ الی ۸٤	۰/۹۱	
مجموع پرسشنامه				**۰/۹۷**	

۸-٤. تحلیل کمی داده‌ها

در این مرحله به‌منظور بررسی میزان تأثیر ابعاد و مؤلفه‌های احصاء شده در ارزیابی آمادگی رزم سایبری، از یک پرسش‌نامه محقق‌ساخته مبتنی بر طیف لیکرت با مقیاس پنج گزینه‌ای از «خیلی کم» تا «خیلی زیاد» استفاده شده است. در ادامه و به‌منظور تجزیه و تحلیل استنباطی داده‌های به‌دست آمده، از تحلیل عاملی تاییدی مرتبه دوم استفاده می‌شود. تحلیل

عاملی، تأییدی روشی است که طی آن محقق انتظار دارد طرح و نقشه خاصی از عوامل پنهان در ماورای متغیرها را مورد آزمایش قرار دهد. در این راستا، در مجموع ۸٤ گویه پرسشنامه در قالب ٤ بعد و ۱۵ مولفه دوم با استفاده از نرم افزار لیزرل[1]وارد تحلیل شدند. در جدول (۱۱) شاخص‌های برازندگی و شکل بارهای عاملی آن ارائه‌شده است.

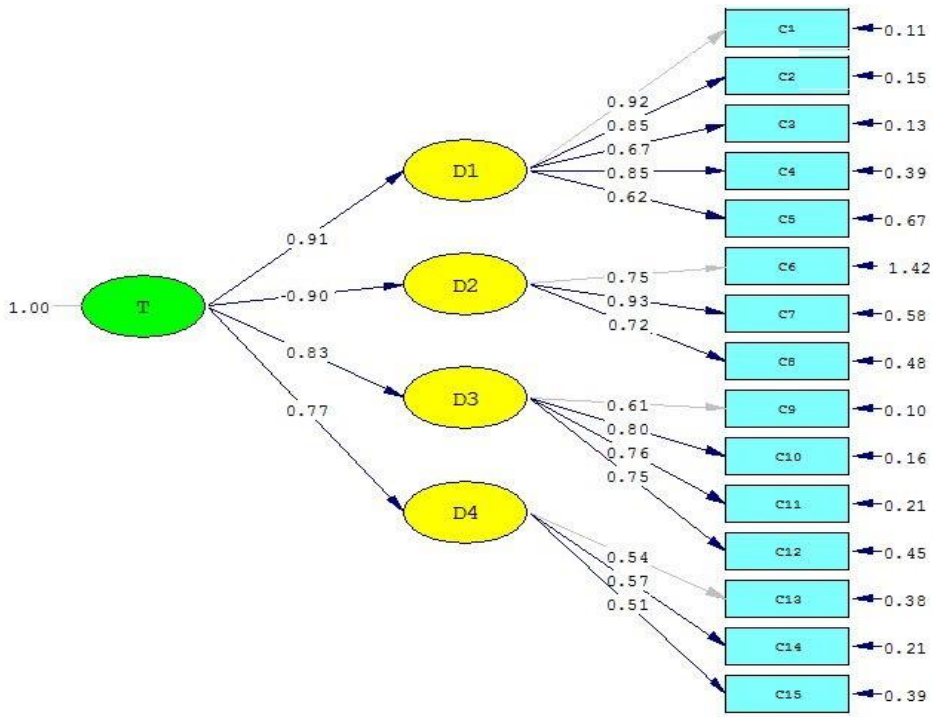
جدول شماره ۱۱. شاخص‌های برازش تحلیل عامل تأییدی مرتبه دوم کل پرسشنامه						
شاخص						
مدل	GFI	AGFI	CFI	RMSEA	SRMR	نسبت خی دو به درجه آزادی (df/ χ۲)
نتایج	۰/۹۳	۰/۹۱	۰/۹۱	۰/۰۷۵	۰/۰٦۳	۲/۲۵
GFI= شاخص نیکویی برازش (۰/۸ تا ۰/۹ >)،						
AGFI = شاخص نیکویی برازش تطبیقی (۰/۸>)،						
CFI = شاخص برازندگی تطبیقی(۹۰/ تا ۰/۹۵ >)،						
RMSEA= خطای مجذور میانگین ریشه تخمین (۰/۰٦ تا ۰/۰۸>)،						
df/ χ۲)= خی‌دو بخش بر درجه آزادی (۳>)						

شاخص‌های گزارش‌شده در تحلیل عاملی مرتبه دوم نشان‌دهنده برازش کاملاً مطلوب داده‌ها با مدل است. در جدول (۱۱) ضرایب بتا ابعاد و بار عاملی هر مولفه سازنده ارائه شده است. همچنین ضرایب مولفه‌ها و ابعاد که به عنوان ضریب بتا (تاثیر مولفه‌ها بر ابعاد) معرفی می‌شوند در جدول (۱۳) ارائه شده است.

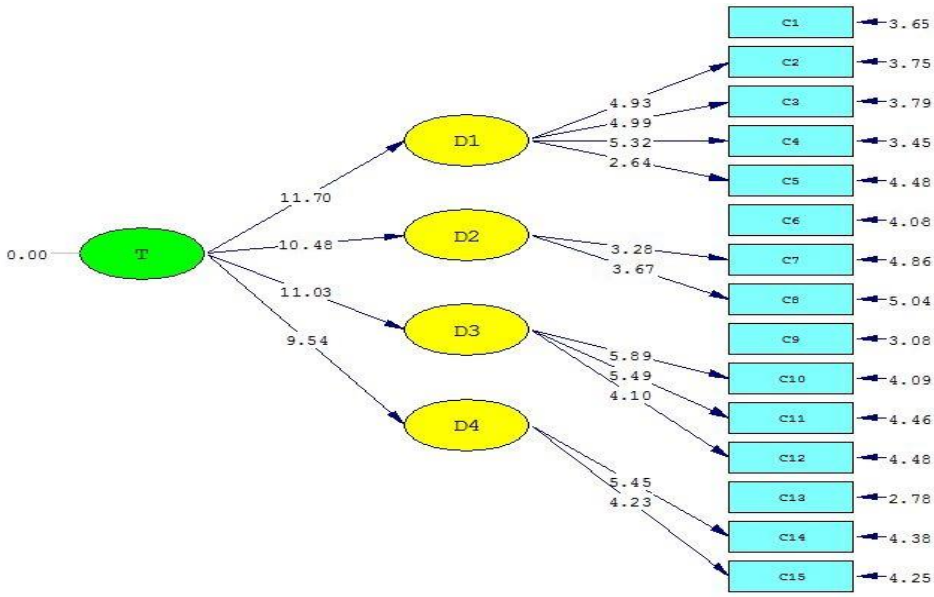
جدول شماره ۱۱. بار عاملی، ضریب تعیین و آماره t مولفه‌ها			
مؤلفه	**بار عاملی**	**اماره t**	R^2
C1	۰/۹۲	–	۰/۸۵
C2	۰/۸۵	٤/۹۳	۰/۷۲
C3	۰/٦۷	٤/۹۹	۰/٤۵
C4	۰/۸۵	۵/۳۲	۰/۷۲
C5	۰/٦۲	۲/٦٤	۰/۳۸
C6	۰/۷۵	–	۰/۵٦
C7	۰/۹۳	۳/۲۸	۰/۸٦
C8	۰/۷۲	۳/٦۷	۰/۵۲
C9	۰/٦۱	–	۰/۳۷

[1]. Lisrel 8.7

جدول شماره ۱۱. بار عاملی، ضریب تعیین و آماره t مولفه‌ها			
مؤلفه	بار عاملی	آماره t	R^2
C10	۰/۸۰	۵/۸۹	۰/٦٤
C11	۰/۷٦	۵/٤۹	۰/۵۸
C12	۰/۷۵	٤/۱۰	۰/۵٦
C13	۰/۵٤	–	۰/۲۹
C14	۰/۵۷	۵/٤۵	۰/۳۲
C15	۰/۵۱	٤/۲۳	۰/۲٦



شکل شماره ۷. بارهای عاملی هر سؤال و مؤلفه در تحلیل عامل مرتبه دوم کل پرسشنامه



هر سؤال و مؤلفه در تحلیل عامل مرتبه دوم کل پرسشنامهtشکل شماره ۸. آماره

جدول شماره ۱۲. ضرایب بتا ابعاد پرسشنامه

ردیف	مولفه	ضریب بتا	tآماره
۱	D1	۰/۹۱	۱۱/۷۰
۲	D2	۰/۹۰	۱۰/٤۸
۳	D3	۰/۸۳	۱۱/۰۳
٤	D4	۰/۷۷	۹/٥٤

همان‌طور که در جدول ۱۲ ملاحظه می‌شود هر چهار بعد تاثیر معنادار بر پرسشنامه دارند. به‌عبارت دیگر، این چهار بعد بیانگر ساختار پرسشنامه می‌باشند. در کل بعد D1 (۰/۹۱) بیشترین ضریب و بعد D4 (۰/۷۷) کمترین ضریب را دارند.

۵. نتیجه‌گیری و پیشنهاد

۱-۵. نتیجه‌گیری

این پژوهش باهدف شناسایی و معرفی نظام ارزیابی آمادگی رزم سایبری نیروهای مسلح و روش تحلیل مضمون با مصاحبه با صاحب‌نظران حوزه رزم سایبری انجام شده است. نتایج این مطالعه سیاست‌گذاران این حوزه را به نکاتی ارزشمند درباره اجزاء، ابعاد و مؤلفه‌های ارزیابی در این حوزه توجه می‌دهد. بدون تردید، بدون نگاه تعاملی به این اجزاء و عوامل، امکان جامع‌نگری و عینی‌گرایی در برنامه‌ریزی برای تثبیت و ارتقاء آمادگی رزم را از دست خواهند داد. در این پژوهش، پس از مطالعات اکتشافی در مبانی نظری و ادبیات تحقیق و مصاحبه (با تعداد ده نفر از صاحب‌نظران این حوزه که به روش گلوله برفی انتخاب شدند). نظام مذکور از چهار بخش «ورودی»، «فرآیند»، «خروجی» و «بازخورد» تشکیل شده است. بخش ورودی، که اساس و جان‌مایه اصلی نظام ارزیابی محسوب می‌گردد؛ در برگیرنده استعداد و ظرفیت برای رزم سایبری می‌باشد که مشتمل بر موارد زیر است: (۱) ماموریت، (۲) ارزش‌های سازمانی، (۳) سرمایه انسانی، (٤) تسلیحات سایبری، (۵) فناوری‌ها و (٦) زیرساخت‌ها به عنوان زمینه‌ها و سرمایه‌های اساسی برای کسب آمادگی رزم سایبری محسوب می‌شوند.

بر اساس الگوی منطق علی و معلولی، برای به‌فعلیت رساندن و آماده نگاه داشتن ظرفیت یا استعدادهای رزمی (عناصر ورودی)، اتخاذ رویکرد فرآیندی از قبیل فرآیندهای مدیریتی، عملیاتی و پشتیبانی درخصوص آموزش، دسترس‌پذیر نمودن، تعاملات و نگهداشت منابع و امکانات ضرورت دارد. در این بخش، عملکرد سبک مدیریت و هدایت سازمان برای آماده نگاه‌داشتن امکانات و تجهیزات واگذار شده برای اجرای رزم سایبری مورد ارزیابی قرار می‌گیرد. سرانجام نتیجه این آمادگی‌ها تحت عنوان توان رزم سایبری در خروجی نظام مذکور منظور می‌گردد. در انتها بازخوردهای مراحل خروجی و فرآیندها برای اصلاح و بهبود عملیات در تطابق با اهداف ازپیش تعین‌شده نظام مذکور، ترازیابی و به مرحله ورودی‌ها انتقال می‌یابد. لذا در این پژوهش، تمرکز بر روی ارزیابی عملکردها در

راستای به‌فعلیت در آوردن و آماده‌نمودن ظرفیت‌ها (ورودی) یا همان آمادگی رزم سایبری می‌باشد. در این نظام ارزیابی، بعد آمادگی عوامل عملیاتی رزم سایبری با ۰/۹۱ بیشترین تأثیر و ابعاد آمادگی بستر اجرای رزم سایبری با ۰/۹۰، آمادگی روش تار و پود رزم سایبری با ۰/۸۳ و آمادگی در سبک فرماندهی، مدیریت و هدایت سایبری سازمان‌های سایبری نیروهای مسلح با ۰/۷۷ به ترتیب در نظام ارزیابی آمادگی رزم سایبری مؤثر می‌باشند.

۲-۵. پیشنهادها

تصویر مطلوب نظام ارزیابی ارائه شده در این تحقیق، می‌تواند مبنای تحقیقات متنوعی در حوزه آمادگی رزم سایبری نیروهای مسلح ج.ا.ایران باشد. مبتنی بر این مسئله، برخی از پیشنهادهای اجرایی و پژوهشی به شرح زیر ارائه می‌گردد.

پیشنهادهای عملیاتی

- با عنایت به کاربردی‌بودن این پژوهش، پیشنهاد می‌گردد قرارگاه تهدیدات نوین و سایبری قرارگاه مرکزی حضرت خاتم الانبیاء(ص) با توجه به الگوی مذکور به ارزیابی و رتبه‌بندی نیروهای مسلح اقدام نمایند.
- رتبه بالای میزان آمادگی عوامل عملیاتی رزم سایبری در فرآیند ارزیابی میزان آمادگی رزم سایبری و تاثیر آن در کسب قدرت سایبری نیروهای مسلح ج.ا.ایران بیانگر این واقعیت با اهمیت می‌باشد که در برنامه‌های توسعه و تجهیز سایبری در سطح کلان و راهبردی در ستادهای بالادستی، توجه ویژه به این بعد ضرروری است.
- استخراج، تدوین، تصویب و ابلاغ اصول دکترینی و سیاست‌های اجرایی تولید آمادگی رزم سایبری در نیروهای مسلح با توجه به تائید نظام ارزیابی مذکور.

پیشنهاد برای پژوهش‌های آتی

- با توجه به تائید الگو، مدل عملیاتی و اندازه‌گیری این الگو با تدوین سنجه‌های خرد به همراه وزن‌دهی و نهایتاً فرمول‌بندی اقدام شود.
- ارائه راهبردها و برنامه‌های تثبیت و ارتقاء آمادگی رزم سایبری نیروهای مسلح.

فهرست منابع و مآخذ

الف. منابع فارسی

- مکارم شیرازی، ناصر(۱٤۰۰). «***ترجمه و تفسیر قرآن کریم***». قم: انتشارات افق روشن
- امام خامنه‌ای(مدظله‌العالی) (سال‌های متفاوت). ***مجموعه بیانات***. قابل دسترسی در: *www.Khamenei.ir*.
- ایران‌زاده، سلیمان؛ برقی، امیر(۱۳۹۷). ***الگوهای ارزیابی عملکرد سازمان***. تبریز: انتشارات فروزش.
- دانشگاه جامع امام حسین(ع) (۱۳۹۸). «***کلان روندهای فضای سایبر: تهدیدها و فرصت‌ها***». مرکز مبین، دانشگاه امام حسین(ع).
- رجبی مسرور، حسن (۱۳۹۸). ***ارزیابی عملکرد سازمانی پیامدگرا (راهنمای عملی)***. تهران: انتشارات دانشگاه جامع امام حسین(ع).
- شهیر، احسان (۱۳۹٦). ***طراحی الگوی راهبردی بومی امنیت فضای مجازی کشور***. رساله دکتری، تهران: دانشگاه عالی دفاع ملی.
- نصرت‌آبادی، جمشید (۱۳۹۸). ***الگوی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران***. رساله دکتری، تهران: دانشگاه عالی دفاع ملّی.
- گروهی از دانشجویان مدیریت راهبردی فضای سایبر گرایش‌های امنیت سایبری و دفاع سایبری (۱۳۹۹). ***معماری کلان فضای سایبر جمهوری اسلامی ایران با رویکرد دفاعی–امنیتی***. تهران: انتشارات دانشگاه عالی دفاع ملّی.
- هلیلی، خداد (۱۳۹۷). «***قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی ج.ا.ایران***» فصلنامه امنیت ملی،۸ (۳)، ۱۷۳–۲۰۰.
- یاوری، وحید؛ زاهدی، شمس‌السادات (۱۳۹۲). «***طراحی مدل مفهومی مدیریت عملکرد سازمانی‌های دولتی و غیر انتفاعی***»، ***فصلنامه اندیشه مدیریت راهبردی***، ۷ (۱)، ۱۲۲–۷۹.
- معاونت عملیات ستاد کل نیروهای مسلح (۱۳۹٦). ***آئین نامه ارزیابی آمادگی رزم***. تهران: ستاد کل نیروهای مسلح.

ب. منابع انگلیسی

- Andress, Jason , Winterfeld, Steve (2014).***Cyber warfare: techniques, tactics and tools for security practitioners***. Second edition. pages cmIncludes bibliographical references and index, retrieved from: http://ppdi.stmik-banjarbaru.ac.id/data.bc/
- Belfer (2020). ***National Cyber Power Index (NCPI) September***. Retrived from: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf
- Betts, Richard (2019). ***Military Readiness: Concepts, Choices, and onsequences***. Washington DC: Brookings Institution Press, Retrived from: https:www.brookings.edu.
- Christos Andreas Makridis, (2018). ***Determinants of Cyber Readiness Sloan School of Management: Massachusetts Institute of Technology.*** Retrived from: https://www.researchgate.net/publication/332700812
- Department Of Defense (2018). ***JP 3-12, Cyberspace Operation***, Washington, DoD Retrived from: https://info.publicintelligence.net/JCS-CyberspaceOperations.pdf
- Department Of The Army (2017). ***FM 3-12, Cyberspace And Electronic Warfare,*** Washington, DoD. Retrived from: https://nsarchive.gwu.edu/document/22844-document-11-department-army-fm-3-12
- James Herrera,(2020), ***The Fundamentals of Military Readiness***, Congressional Research Service, Retrieved from: https://crsreports.congress.gov.
- Kim, Sungjoong; Kang, Jiwon; Oh, Haengrok, Shin, Dongil; & Shin, Dongkyoo (2020). "Operation Framework Including Cyber Warfare Execution Process and Operational Concepts", ***IEEE Access***, (8): 168-176, Retrived from: https://ieeexplore.ieee.org/.
- MITRE ATTCK (2019). ***Common Attack Pattern Enumeration and Classification*** (CAPEC). Schema Description, Retrived from: https://capec.mitre.org/data/index.html.
- Minárik, T.; Alatalu, S.; Biondi, S.; Signoretti, M.; Tolga, I.; Visky, G.(2019). ***International Conference on Cyber Conflict***, Silent Battle NATO CCD COE Publications, Tallinn. Retrived from:

https://ccdcoe.org/uploads/2019/06/.

- Siegel, john philipp, summermatter, Lukas (2008). "Defining Performance in Public Management: A Survey of Academic Journals", ***European Group of Public Administration Conference*** (EGPA, Rotterdam. Retrived from: http:webh01.ua.ac.be/pubsector/Rotterdam/papers/Siegel%20Summermatter%2 0paper.