دریافت مقاله: ۱۳۹۹/۰۸/۱۹
پذیرش مقاله: ۱۴۰۰/۰۱/۲۲

مقاله پژوهشی

فصلنامهٔ مدیریت نظامی
سال بیستم، شمارهٔ ۴، زمستان ۱۳۹۹
ص‌ص ۳۱-۶۴

الگوی راهبردیِ ارزیابیِ عملیاتِ سایبری

هانی رحیم‌اُف[۱*]، محمدرضا موحدی‌صفت[۲]

چکیده

امروزه راهبرد دفاع عامل سایبری در بسیاری از کشورهای پیشرو حکم‌فرماست. اساس این نوع دفاع، تسلط بر فضای سایبر و توانایی انجام عملیات سایبری است. این توانایی علاوه بر ایجاد بازدارندگی سایبری، کشورها را قادر می‌سازد تا قبل از بالفعل شدن تهدید، آن را از بین ببرند. به دلیل غیرملموس بودن فضای سایبر و عدم مشاهده هدف عملیات سایبری، فهم میزان موفقیت عملیات دشوار است. سنجش این موفقیت، نیازمند ارزیابی عملیات سایبری است. با ارزیابی عملیات سایبری می‌توان عملکرد و اثربخشی عملیات را اندازه‌گیری نمود، نقاط ضعف و قوت را یافت و در جهت برطرف سازی نقاط ضعف و بهبود نقاط قوت گام برداشت. برای انجام ارزیابی دقیق، همه‌جانبه و مبتنی بر اصول علمی عملیات سایبری نیاز به الگوی راهبردی است تا بر اساس آن ارزیابی صورت پذیرد. در پژوهش حاضر جهت ارائه الگوی راهبردی ارزیابی عملیات سایبری، از رویکرد آمیخته (کمی و کیفی) استفاده شده است. در این تحقیق، از نظرات ۷۰ نفر از فرماندهان، مدیران و کارشناسان سطوح راهبردی، عملیاتی و تاکتیکی عملیات سایبری کشور در قالب پرسشنامه استفاده شده است. بر اساس پژوهش انجام‌شده، با استفاده از نظر خبرگان سه مفهوم ارزیابی طراحی و طرح‌ریزی، ارزیابی آمادگی رزمی و ارزیابی اجرا به‌مثابه ابعاد اساسی ارزیابی عملیات سایبری مورد شناسایی قرار گرفتند و سپس مؤلفه‌های هر یک از این ابعاد استخراج و شاخص‌های هر مؤلفه معین شدند. پس از تجزیه‌وتحلیل آماری نتایج پرسشنامه، الگوی راهبردی ارزیابی عملیات سایبری در سه بعد، ده مؤلفه و هفتادوسه شاخص ارائه گردیده است.

واژه‌های کلیدی: عملیات سایبری، ارزیابی عملیات، ارزیابی عملیات سایبری، الگوی راهبردی.

---

۱. دانشجوی دکتری رشته مدیریت راهبردی فضای سایبر، گرایش امنیت سایبری، دانشگاه و پژوهشگاه عالی دفاع ملی، تهران، ایران، (* نویسندهٔ مسئول)؛ h.rahimov۹۸@sndu.ac.ir
۲. استادیار دانشگاه و پژوهشگاه عالی دفاع ملی، تهران، ایران؛ movahedi@sndu.ac.ir

مقدمه و بیان مسئله

امروزه ماهیت جنگ‌ها از حوزه نظـامی بـه سایبری تغییر پیداکرده است. حملات سایبری از طریق فضای مجازی بـه زیرساخت‌های مهم کشور و از راه دور انجام می‌شود. آنچه یک مهاجم با نفوذ به مرزهای سایبری دیگران به دست می‌آورد، از خاک و اشغال سرزمین بسیار ارزشمندتر است. خطر حملات سایبری کمتر از اقدام نظامی نیست و برای هر دولتی پیامدها و اثرهای مرگباری به دنبال دارد. به همـین دلیـل توجـه ویژه به این حوزه ضروری است (جباررشیدی، ۱۳۹۶). حملات مخرب مهم با تأثیرات گسترده، تهدیدهای سایبری را به‌عنوان یکی از بدترین تهدیدهای منافع ملی به تصویر کشیده است تا جای که ایالات‌متحده آمریکا اعلام کرده است که این حملات را به‌عنوان جنگ تلقی کرده و با آن برخورد فیزیکی خواهد کرد (فروردین، ۱۳۹۷). وقایع و حوادث سایبری سال‌های اخیر کشور نیز مؤید این واقعیت است که کثرت حملات سایبری علیه کشور به‌ویژه در زیرساخت‌های حیاتی، جمهوری اسلامی ایران را به یکی از قربانیان اصلی فضای سایبر تبدیل نموده است. جنگ سایبری دولت‌های غربی علی‌الخصوص آمریکا نیز از سال ۲۰۱۰ با به‌کارگیری ویروس «استاکس‌نت» و ویروس سارق اطلاعات «دوکو» علیه برنامه هسته‌ای جمهوری اسلامی ایران آغاز شده است (شفیع پور، ۱۳۹۳). در این خصوص ایران نیز سیاست بازدارندگی را در حوزه دفاعی کشور برگزیده است. رویکرد تهدید در مقابل تهدید، راهبرد جدیدی است که از طرف مقام معظم رهبری در عرصه دفاعی کشور مطرح گردیده است و نقش مهمی در بازدارندگی در مقابل تهدیدات دشمنان دارد (کرم روان، ۱۳۹۸). توان انجام صحیح و جامع عملیات در عرصه سایبری به‌عنوان یک عرصه جدید نبرد می‌باشد. هدف این پژوهش ارائه الگوی راهبردی ارزیابی عملیات سایبری است تا به‌وسیله آن بتوان ضعف و قوت‌های عملیات را بررسی نموده و در جهت برطرف سازی ضعف‌ها و تقویت قوت‌ها گام برداشت.

در تمامی قلمروها، فرماندهان نظامی باید همواره برآوردی دقیق از توان رزم مجموعه تحت امرشان داشته باشند تا بر اساس آن، بتوانند برای فائق آمدن بر ضعف‌ها و ارتقاء توان رزم موجود برنامه‌ریزی کرده، عملیات متناسبی را طراحی نمایند. حین اجرای عملیات نیز فرماندهان باید درک صحیحی از صحنه نبرد و شرایط موجود داشته باشند. حتی پس از اتمام یک عملیات، حصول اطمینان از مقدار دستیابی به اهداف و میزان آسیب‌های واردشده به نیروهای خودی و دشمن، برای فرماندهان بسیار حائز اهمیت است. به دلیل غیرملموس بودن قلمرو سایبر به‌عنوان

عرصه‌ای نوین در جنگ، نیاز به اطلاعات بیان‌شده برای فرماندهان و مدیران بیشتر احساس می‌شود. آن‌ها برای به دست آوردن این اطلاعات، نیازمند ارزیابی‌های صحیح، جامع و علمی هستند. برای انجام چنین ارزیابی، نیاز به الگوی راهبردی است تا بر اساس آن مشخص شود که چه ابعاد و مؤلفه‌هایی نیاز به ارزیابی داشته و شاخص‌های ارزیابی هر مؤلفه چیست؟

بر اساس سند «نظام ملی پیشگیری و مقابله با حوادث فضای مجازی» مصوب ۱۳۹۶/۸/۱۵ شورای عالی فضای مجازی کشور، مقابله با حوادث سایبری از نوع جنگ سایبری بر عهده ستاد کل نیروهای مسلح جمهوری اسلامی ایران قرارگرفته است. این ستاد به‌عنوان ستادی بالادستی، وظیفه نظارت بر نیروهای مسلح را داراست. یکی از این موارد، نظارت بر عملیات سایبری است. ارزیابی عملیات سایبری به‌عنوان بخش مهم عملیات، نقش تعیین‌کننده‌ای را برای فرماندهان و مدیران داراست. فقدان الگوی راهبردی ارزیابی عملیات سایبری به صحت، جامعیت و علمی بودن ارزیابی‌ها خدشه وارد می‌نماید؛ زیرا ارزیابان راهبردی از ابعاد مختلف ارزیابی عملیات سایبری و مؤلفه‌های هر بعد که به‌صورت علمی به‌دست‌آمده است آگاهی نداشته و نمی‌دانند که شاخص‌های ارزیابی هر مؤلفه چیست؟ بنابراین بر اساس تصمیمات سلیقه‌ای، شخصی و غیرعلمی اقدام به ارزیابی عملیات سایبری خواهند کرد.

الگوی راهبردی ارزیابی عملیات سایبری، علاوه بر اینکه باعث می‌شود تا ستاد کل نیروهای مسلح جمهوری اسلامی ایران، تصویر روشن، جامع و دقیقی از چگونگی ارزیابی عملیات سایبری داشته باشد؛ این ستاد را قادر می‌سازد که طرح‌های راهبردی ارزیابی عملیات سایبری را بر اساس الگوی راهبردی تأییدشده، طراحی نماید.

در این تحقیق، منظور پژوهشگران از الگوی ارزیابی، ارائه مدلی برای انجام ارزیابی عملیات سایبری است. برای دستیابی به این مقصود، ابتدا موضوع عملیات سایبری مورد بررسی قرارگرفته و سپس ابعاد، مؤلفه‌ها و شاخص‌های ارزیابی آن استخراج گردیده است. با توجه به اینکه ابعاد، مؤلفه‌ها و شاخص‌ها در بالاترین سطح عملیات سایبری که همان سطح راهبردی است، بررسی شده است؛ بنابراین الگوی نهایی به‌دست‌آمده، در سطح راهبردی بوده و بالاتر از سطوح عملیاتی و تاکتیکی می‌باشد؛ بنابراین پژوهش حاضر به دنبال پاسخ به این سؤال اصلی است که الگوی راهبردی ارزیابی عملیات سایبری چیست؟ با ارائه پاسخ علمی، جامع، دقیق و تأییدشده به این پرسش و بر اساس نتایج حاصل از به‌کارگیری آن، فرماندهان و مدیران در سطوح راهبردی ستادی

یا عملیاتی قادر خواهند بود نقاط ضعف و قوت عملیات سایبری را بیش‌ازپیش به دست آورند و با برنامه‌ریزی جهت اصلاح نقاط ضعف و تقویت نقاط قوت بتوانند عملکرد و اثربخشی عملیات سایبری را بهبود بخشیده، بازدارندگی سایبری را افزایش دهند.

شایان‌ذکر است که در پژوهش حاضر، مقصود محققین از عملیات سایبری، تنها جنبه تهاجمی عملیات سایبری بوده که جهت مقاصد دفاعی و ایجاد بازدارندگی سایبری بکار گرفته می‌شود.

مبانی نظری

در این بخش به اصطلاحات و مفاهیم پایه ارزیابی عملیات سایبری پرداخته می‌شود.

فضای سایبری[۱]: یک قلمرو جهانی در محیط اطلاعاتی است که شامل شبکه‌های وابسته به زیرساخت‌های فناوری اطلاعات و داده‌های در آن، از جمله اینترنت، شبکه‌های ارتباطی، سیستم‌های رایانه‌ای و پردازنده‌ها و کنترل‌کننده‌های درون آن‌ها می‌باشد (DoD, ۲۰۲۰). فضای سایبر، درحالی‌که یک عرصه در داخل محیط اطلاعاتی است، یکی از پنج عرصه نبرد وابسته به یکدیگر است که عبارت‌اند از زمین، هوا، آب و فضا. مشابه با عملیات هوایی که متکی به پایگاه‌های هوایی روی زمین و کشتی‌های روی دریا هستند، فضای سایبری شامل شبکه‌های مختلف و اغلب هم‌پوشان است. علاوه بر این‌ها شامل گره‌هایی است هر یک با آدرسی مثل IP شناسایی می‌شوند و اطلاعاتی که مربوط به زیرساخت‌های انتقالی هستند (مثل اطلاعات مسیریابی) که از این سیستم‌ها پشتیبانی می‌کنند (DoD, ۲۰۱۸). در دکترین عملیات سایبری نیروی هوایی امریکا نیز فضای سایبر چنین تعریف‌شده است که: «فضای سایبری یک قلمرو است که فناوری‌های ساخته دست انسان را برای ورود و بهره‌برداری نیاز دارد. تنها فرق آن با دیگر عرصه‌ها این است که راحت‌تر آن‌ها را دیده و احساس می‌کند. همانند عرصه‌های هوا و فضا، پیامدهای عملیات فضای سایبری می‌تواند به‌صورت هم‌زمان در چند مکان دیده شود. پیامدهای این عرصه می‌توانند به‌اندازه موردنیاز دقیق و محدود، وسیع، مداوم و یا زودگذر و ناپایدار باشند» (AFDD, ۲۰۱۱).

عملیات سایبری[۲]: وزارت دفاع ایالات‌متحده، «عملیات سایبری» را به‌کارگیری قابلیت‌های فضای سایبری به‌طور عمده و اساسی برای دستیابی به اهداف از طریق فضای سایبر تعریف

---

۱. Cyberspace
۱. Cyberspace operations

می‌کند (DoD, ۲۰۲۰). ناتو و ایالات‌متحده تأیید کرده‌اند که عملیات سایبری بر اساس نیت و قصد به تهاجمی[۱] و تدافعی[۲] طبقه‌بندی می‌شوند. درحالی‌که بیشتر کشورهای عضو ناتو روی تعاریف اصطلاحات رایج سایبری متفق نیستند؛ وزارت دفاع ایالات‌متحده در حال حاضر عملیات تدافعی سایبری[۳] را به‌عنوان مأموریت‌هایی برای حفظ توانایی جهت بهره‌برداری از قابلیت‌های فضای سایبر (دوستانه) و محافظت از داده‌ها، شبکه‌ها، دستگاه‌های موجود در فضای سایبر یا سایر سامانه‌هایی که جهت حفاظت از شکست امنیتی یا جلوگیری از فعالیت‌های قریب‌الوقوع مخرب سایبری طراحی‌شده‌اند تعریف می‌کند (DoD, ۲۰۱۸).

در مقاله (هاتاجا[۴]، ۲۰۲۰) عملیات سایبری، به عملیات تهاجمی سایبری تعبیر شده است. بر اساس حق دفاع جمعی که در ماده ۵۱ منشور سازمان ملل درج‌شده بیان می‌دارد که: "کشورهایی که در معرض یک «حمله مسلحانه» نیستند، می‌توانند به کشوری که موردحمله قرارگرفته است و برای دفاع از خودیاری می‌طلبد، یاری رسانند؛ این ماده، عملیات تهاجمی سایبری را برای کشور حمله شده یا سایر کشورهایی که کشور حمله شده از آن‌ها کمک بخواهد -علیه کشور حمله‌کننده- مجاز و مشروع می‌داند."

عملیات تهاجمی[۵]: عملیات تهاجمی ابزاری است که یک رده نظامی، آزادی عمل را با آن به دست آورده و با حفظ آن، به نتایج قاطع دست خواهد یافت. معمولاً فرماندهان، مواضع تدافعی را به‌صورت موقتی اتخاذ می‌کنند و باید برای در دست گرفتن ابتکار عمل، مجدد به حالت تهاجمی برگردند (DoD, ۲۰۱۴).

حمله به‌طور حتم یکی از فرم‌های جنگ است. حمله آخرین و دورترین ابزاری است که فرمانده برای تحمیل تمایل خود به دشمن به کار می‌گیرد. البته ممکن است فرمانده از حمله برای فریب دادن و یا منحرف کردن دشمن، تولید برخی اطلاعات و یا نگه‌داشتن دشمن در محلی خاص نیز استفاده کند و همچنین فرمانده با به‌کارگیری حمله، ابتکار عمل را در ابعاد مختلف صحنه می‌تواند

---

۲. Offensive
۳. Defensive
٤. Defensive cyberspace operations
٥. Haataja, S.
٦. Offensive operations

به دست بگیرد و مشخصاً برای گرفتن ابتکار عمل حتی در دفاع هم نیاز است از حمله استفاده شود. (درسلر[۱]،۲۰۱۵)

عملیات تهاجمی سایبری[۲]: به معنای قصد داشتن برای طرح‌ریزی و به کار بستن توان رزم سایبری با استفاده از به‌کارگیری توان در و یا از طریق فضای سایبری است. عملیات تهاجمی سایبری هم مثل عملیات تهاجمی در دیگر عرصه‌ها نیاز دارد تا یک دستور اجرای رسمی برای آن صادر شود (DoD, ۲۰۱۸). عملیات تهاجمی سایبری، عملیاتی است که برای قدرت‌نمایی با به‌کارگیری قدرت در یا از طریق عرصه سایبری انجام می‌شود؛ و مجموعه اقدامات متنوعی را در فضای سایبری در برمی‌گیرد. این اقدامات شامل حملات انکار سرویس (مثل تنزل کیفیت سرویس، قطع سرویس و یا تخریب کامل سرویس) و حملات دست‌کاری اطلاعات هستند که بعضاً یا مخفی مانده، یا پیامدهای آن‌ها در عرصه‌های فیزیکی ظاهر می‌شوند. در حقیقت هدف حمله سایبری ایجاد مزیت نسبی در عرصه سایبری یا دیگر عرصه‌های فیزیکی برای نیروهای خودی با به‌کارگیری توان رزم سایبری است (ویلیامز[۳]،۲۰۱۴).

در بیان دیگری که توسط وزارت دفاع امریکا بیان‌شده است، حملات شبکه‌های کامپیوتری، استفاده از شبکه‌های کامپیوتری برای قطع کردن، تنزل و کاهش سطح خدمات‌دهی و یا دست‌کاری و تخریب اطلاعات مستقر در سیستم‌های اطلاعاتی یا شبکه‌های کامپیوتری دشمن است (DoD, ۲۰۱۷).

عملیات سایبری با درجه بالایی از گمنامی و انکارپذیری قابل‌قبول، همراه بوده و نتایج حاصل از آن عموماً نامشخص است که شامل طیف وسیعی از گزینه‌ها و نتایج احتمالی می‌شود. همچنین ممکن است در مقیاس زمانی از دهم ثانیه تا چندین سال به طول بینجامد. (اسمیتز و ورک[۴]،۲۰۲۰)

در مقاله (اسمیتز[۵]،۲۰۲۰) ضمن دسته‌بندی کردن فضای سایبر به مناطق آبی، خاکستری و قرمز، برای ایالات‌متحده آمریکا این حق را قائل شده است که در هر سه منطقه حضور فعال

---

۱. Dressler, J.
۲. Offensive cyberspace operations
۳. Williams, B. T.
۱. Smeets, M. & Work, J. D.
۲. Smeets, M.

داشته و حتی بتواند بر اساس قانون داخلی آمریکا و بدون هماهنگی با کنگره، جهت مقاصد دفاعی، عملیات تخریبی سایبری انجام دهد. ژنرال ناکاسون در مقاله‌ای در مجله سه‌ماهه نیروهای مشترک، ژنرال‌های فرمانده در فرماندهی سایبری و رؤسای آژانس امنیت ملی آمریکا می‌نویسد: "اگر ما تنها در «فضای آبی» دفاع کنیم بازنده خواهیم بود. در عوض، ما باید به‌صورت یکپارچه در فضای داخلی به‌هم‌پیوسته جهانی تا حد ممکن به مخالفان و عملیات آن‌ها نزدیک شویم و به‌طور مداوم فضای جنگ را شکل دهیم تا مزیت عملیاتی برای خودمان ایجاد و از دشمنانمان سلب کنیم."

ارزیابی[۱]: یعنی مشخص کردن مداوم وضعیت پیشرفت عملیات، تحقق نتایج و پیامدها و وضعیت دستیابی به اهداف عملیات (DoD, ۲۰۱۴). ارزیابی دارای معانی ذیل است: ۱. فرآیند مداوم که اثربخشی توانایی‌های بکار گرفته‌شده در طول عملیات نظامی را اندازه‌گیری می‌کند. ۲. تعیین پیشرفت در جهت انجام یک کار، ایجاد یک شرط یا دستیابی به یک هدف. ۳. تجزیه‌وتحلیل امنیت، اثربخشی و پتانسیل یک فعالیت اطلاعاتی موجود یا برنامه‌ریزی‌شده. ۴- قضاوت در مورد انگیزه‌ها، صلاحیت‌ها و خصوصیات شخص کارمندان یا عوامل. (DoD, ۲۰۲۰) ارزیابی، یک فعالیت مداوم است که در خلال فرآیند عملیات انجام می‌شود. با توجه به تأثیر بیشتر فاز اجرای مأموریت، تمرکز ارزیابی به آن بخش متوجه خواهد شد (,TRADOC۲۰۱۶).

ارزیابی عملیات[۲]: ۱- یک فرآیند مداوم که اثربخشی توانایی‌های به‌کارگیری در طی عملیات نظامی را در دستیابی به اهداف اعلام‌شده اندازه‌گیری می‌کند. ۲. تعیین پیشرفت در جهت انجام یک کار، ایجاد یک شرط یا دستیابی به یک هدف (DoD, ۲۰۱۷).

ارزیابی عملیات سایبری[۳]: فرآیند ارزیابی عملیات سایبری از طراحی آغاز می‌شود. این فرآیند شامل اندازه‌گیری عملکرد و اثربخشی می‌باشد. درگذشته برای ارزیابی یک جنگ، بیشتر تأکید بر روی ارزیابی آسیب‌های آن جهت تعیین میزان خسارت‌های جانی و عملکردی بوده است، اما این رویکرد برای عملیات سایبری پاسخگو نیست زیرا غالباً اثر عملیات سایبری در خارج از محدوده نبرد بوده و عموماً آسیب جانی ایجاد نمی‌کنند. ارزیابی یک عملیات سایبری، محدود به

---

۳. Assessment
٤. Assessment of Operations
۱. Assessment of Cyberspace Operations

تجزیه‌وتحلیل داده‌های به‌دست‌آمده از فضای سایبر نیست. مثلاً برای ارزیابی میزان اثربخشی یک عملیات تهاجمی سایبری که هدفش قطع برق می‌باشد؛ به مشاهده نشانه‌های قطع برق نیاز است. (DoD, ۲۰۱۸) لازم است از طریق به اطلاعات به‌دست‌آمده قبل از اجرای عملیات سایبری، تأثیرات آن بررسی گردد تا بتوان بر اساس آن، اصل تناسب را رعایت نمود. بر اساس این اصل، تلاش می‌شود سلاح سایبری متناسب با یک هدف مشخص ایجاد شود. بعلاوه باید تأثیر عملیات سایبری پس از اجرا نیز مشخص شود تا بتوان بر اساس آن اثربخشی عملیات سایبری را ارزیابی کرده و در صورت نیاز، اصلاحاتی را برای عملیات سایبری آتی انجام داد. (متیوس و همکاران[۱]، ۲۰۲۰)

فرآیند اجرای عملیات در ستاد ارتش آمریکا: بر اساس سند ADP ۵,۰[۲] ریاست ستاد ارتش[۳] آمریکا، فرآیند عملیات مطابق شکل ۱ به چهار بخش زیر تقسیم می‌گردد (Department of the Army, ۲۰۱۹).

برنامه‌ریزی[۴]: درک صحنه و موقعیت، ترسیم یک آینده مطلوب و مشخص کردن راهکارهای رسیدن به آن.

آماده‌سازی[۵]: اقداماتی که رده‌های عملیاتی برای ارتقای توان رزم برای انجام عملیات انجام می‌دهند.

اجرا[۶]: به اجرا رساندن طرح‌های ریخته شده و به‌کارگیری توان رزم برای انجام مأموریت.

ارزیابی[۷]: مشخص کردن مداوم وضعیت پیشرفت عملیات، ایجاد پیامدها و دستیابی به اهداف عملیات.

شکل شمارهٔ ۱: فرآیند انجام عملیات ستاد ارتش آمریکا (Department of the Army، ۲۰۱۹)

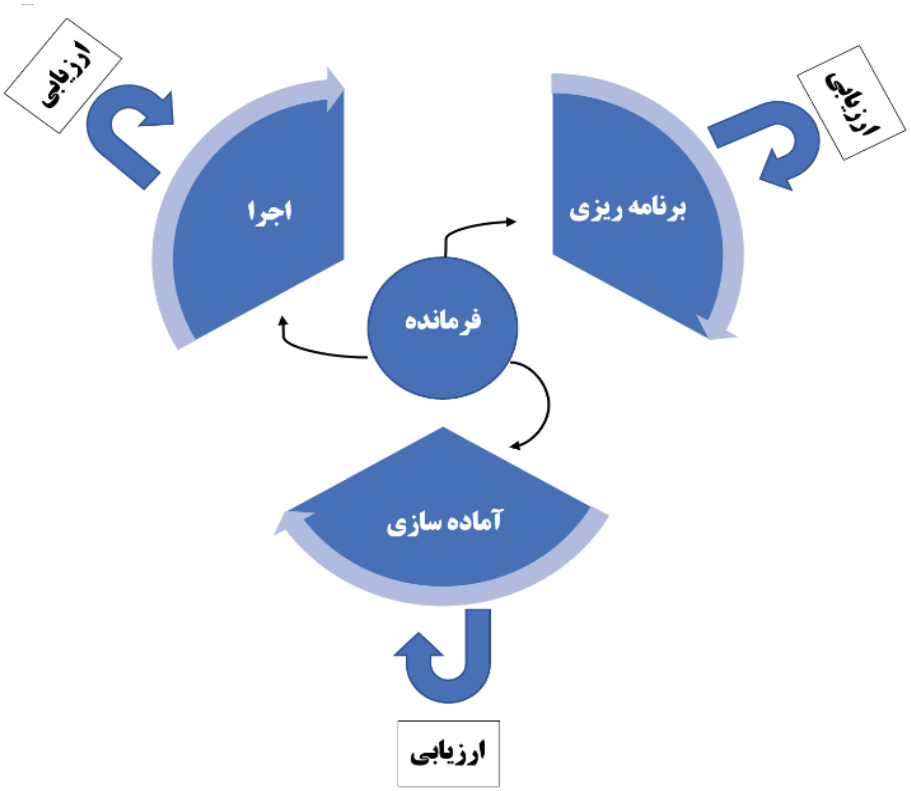
---

۲. Maathuis, C. Pieters, W. & van den Berg, J.
۳. Army Doctrine Publication
٤. Headquarters Department of the Army
٥. Plan
٦. Prepare
۱. Execute
۲. Assess

همان‌طور که در شکل ۱ ملاحظه می‌شود، ارتش امریکا از یک فرآیند چرخشی و متناوب برای اجرای عملیات استفاده می‌کند که مطابقت مناسبی جهت به‌کارگیری در عرصه سایبری دارد.

فرآیند اجرای عملیات سایبری: بر اساس(Eom, ۲۰۱۴) فرآیند اجرای عملیات سایبری به ۷ بخش جمع‌آوری اطلاعات[۱]، هدف‌یابی[۲]، انتخاب روش حمله[۳]، انتخاب تکنیک حمله[۴]، مانور سایبری (اقدام)[۵]، پاک کردن ردِپا[۶] و ارزیابی پیامدهای حمله[۷] تقسیم تقسیم‌بندی می‌شود. این

۱. Information Collection
۲. Target Recommendation
۳. The Selection of Attack Method
٤. The Decision of Attack Technique
٥. Cyber Maneuver
٦. The Removal of Attack Traces
۷. The Assessment of Attack Impacts

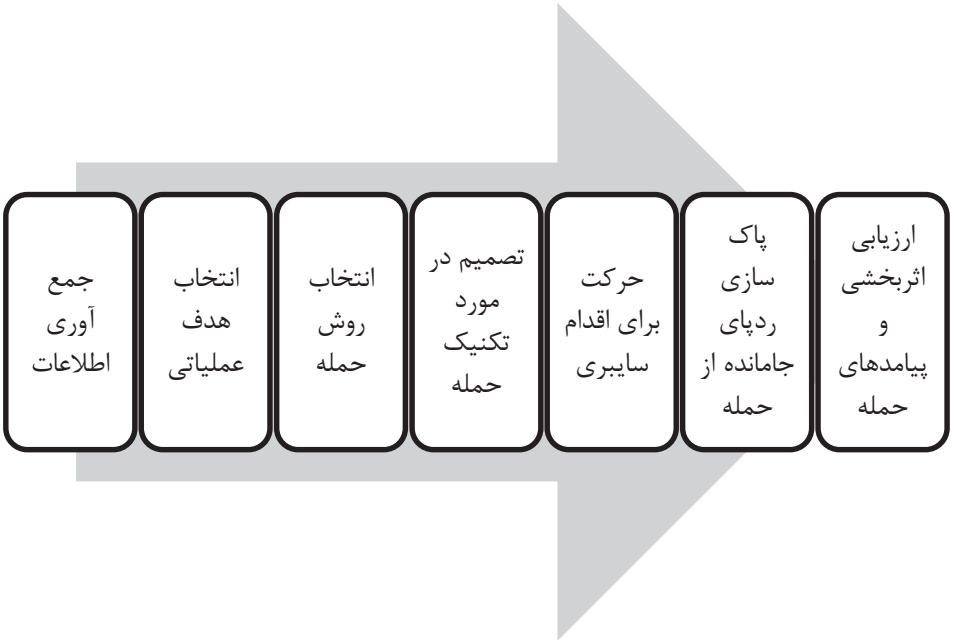


بخش‌ها در شکل ۲ نمایش داده‌شده‌اند.

شکل شمارهٔ ۲: فرآیند اجرای عملیات سایبری (Eom, ۲۰۱۴)

آمادگی رزمی: واژه آمادگی رزمی[۱] در فرهنگ لغت آکسفورد به قدرتمند شدن، مجوز دادن، ارائه قدرت و توانا شدن معنی شده است. در معنای خاص نیز این کلمه به قدرت بخشیدن و دادن آزادی عمل به افراد برای اداره خود معنا شده و در مفهوم سازمانی آن به معنی تغییر در فرهنگ و شهامت در ایجاد و هدایت محیط سازمانی می‌باشد. به‌بیان‌دیگر، آمادگی رزمی عبارت است از طراحی و ساخت سازمان به نحوی که افراد ضمن کنترل خود، آمادگی قبول مسئولیت‌های بیشتری را داشته باشند. آمادگی رزمی در کارکنان باهوش، دلگرم، درست‌کار و مطمئن، شرایطی را فراهم می‌آورد که در لوای آن زندگی کاری خود را کنترل و به رشد کافی برای پذیرش

۱. Martial Readiness



مسئولیت‌های بیشتر در آینده دست خواهند یافت. (جمالی،۱۳۹۹)

در مقاله (مدنی،۱۳۹۴) نیز آمادگی رزمی چنین تعریف‌شده است که: «آمادگی رزمی به‌منزله ایجاد قابلیت و به کیفیت درآوردن توان و استعداد کمی واحد نظامی برای اجرای بهینه مأموریت است. به تعبیر دیگر آمادگی رزمی با ایجاد قابلیت و مهارت بخشیدن به عناصر توان نسبی، کیفیت به‌کارگیری آن‌ها را از حالت بالقوه به بالفعل مبدل می‌نماید».

سازمان رزم: در تعریف به مجموعه‌ای از افراد و تجهیزات که برای تحقق اهدافی معین به شکلی متناسب باهم همکاری می‌کنند، سازمان رزم گفته می‌شود (رضاییان، ۱۳۸۶).

با توجه به رویکرد این مقاله در ارزیابی عملیات سایبری، هرکجا عنوان عملیات سایبری بیان می‌گردد، منظور محققین عملیات تهاجمی سایبری است که جهت مقاصد دفاعی و ایجاد بازدارندگی بکار گرفته می‌شود.

روش

این تحقیق به‌صورت آمیخته و با روش توصیفی- تحلیلی و موردی- زمینه‌ای انجام می‌شود. ازاین‌جهت توصیفی- تحلیلی است که برای گردآوری اطلاعاتی که مدون نشده به کار می‌رود و با این روش، توصیف عینی، واقعی و منظم موضوعات انجام می‌گردد. ازاین‌جهت موردی- زمینه‌ای

است که در این مقاله، مطالعه عمیق روی نمونه‌هایی از یک پدیده در محیط واقعی صورت می‌گیرد. نوع پژوهش درزمینهٔ شناخت الگوی راهبردی ارزیابی عملیات سایبری، توسعه‌ای خواهد بود. از طرف دیگر پژوهش حاضر در پی یافتن مشکلات ارزیابی عملیات سایبری کشور و راه‌حل آن‌ها است؛ بنابراین پژوهش از این منظر کاربردی محسوب گردیده و درمجموع توسعه‌ای-کاربردی خواهد بود. برای گردآوری اطلاعات از روش کتابخانه علمی و تخصصی، سایت‌های معتبر اینترنتی، همچنین روش میدانی شامل مصاحبه با خبرگان عملیات سایبری و تنظیم پرسشنامه استفاده شد. برای تحلیل داده‌های بخش کمی (داده‌های حاصل از پرسشنامه) نیز از روش‌های آمار توصیفی و استنباطی ازجمله معادلات ساختاری، تحلیل واریانس، ضریب همبستگی استفاده‌شده است.

به‌منظور اخذ نظر خبرگان جهت ارائه مدل مفهومی پژوهش، مصاحبه عمیق با روش اشباع نظری با جامعه آماری ۷ نفر به‌صورت تمام شمار صورت پذیرفت؛ بنابراین حجم نمونه با حجم جامعه برابر است. سپس به‌منظور ارزیابی مدل مفهومی احصاء شده، پرسشنامه‌ای بر اساس طیف لیکرت تنظیم گردید. با توجه به جامعه آماری ۷۲ نفره -بر اساس جدول مورگان- پرسشنامه به‌صورت تمام شمار به ۷۲ نفر از خبرگان ارسال شد؛ بنابراین در این مرحله نیز حجم نمونه با حجم جامعه برابر است. تعداد ۲ پرسشنامه به دلیل نقصی که داشت کنار گذاشته شد و داده‌ها با تعداد ۷۰ پرسشنامه جمع‌آوری و تحلیل گردید. پرسشنامه به لحاظ روایی ظاهری و محتوا به تأیید جمعی از اساتید رسانده شد و به لحاظ پایایی با استفاده از نرم‌افزار SPSS آلفای کرونباخ پرسشنامه ۰,۸۳ برآورد شد که پایایی قابل قبولی محسوب می‌شود.

یافته‌های پژوهش

جهت بررسی همبستگی داده‌ها ابتدا باید مشخص شود که داده‌ها پارامتری هستند یا ناپارامتری. برای این منظور از آزمون کلموگوروف -اسمیرنوف استفاده می‌شود. برای بررسی نرمال بودن داده‌ها فرضیه‌ای به شکل زیر مطرح و سپس مورد آزمون قرار گرفت.

H۰: توزیع داده‌های متغیرها نرمال است.

H۱: توزیع داده‌های متغیرها نرمال نیست.

بر اساس اطلاعات به‌دست‌آمده از نتیجه آزمون مذکور، میزان sig متناظر با هر یک از داده‌ها برابر با ۰,۰۰۰ گردید. همان‌طور که مشخص است مقدار مذکور از ۰,۰۵ کمتر است؛ بنابراین داده‌های پرسشنامه از توزیع نرمال برخوردار نیستند و از آمار ناپارامتریک برای تحلیل استنباطی

آن‌ها استفاده می‌کنیم. تمامی آزمون‌های آماری بر اساس سطح معناداری قضاوت می‌شود (چه آزمون‌های پارامتریک و چه ناپارامتریک). اگر سطح معناداری کمتر از مقدار خطای ۰,۰۵ به دست آمد فرضیه H۱ تأیید و اگر بیشتر به دست آمد، فرضیه H۰ تأیید می‌گردد. با توجه به ناپارامتری بودن داده‌ها، برای محاسبه ضریب همبستگی از آزمون اسپیرمن بهره می‌بریم.

الف) بررسی ارتباط بین مؤلفه‌ها و ابعاد: ارتباط بین مؤلفه‌ها و ابعاد با استفاده از ضریب همبستگی اسپیرمن محاسبه‌شده است. فرض H۰ بیانگر عدم وجود همبستگی معنی‌دار است و فرض H۱ وجود همبستگی معنی‌دار می‌باشد. نتایج این آزمون به شرح جدول ۱ ارائه‌شده است.

(۱) ارتباط بین ابعاد الگوی راهبردی ارزیابی عملیات سایبری

جدول شمارهٔ ۱: نتایج همبستگی بین ابعاد الگوی راهبردی ارزیابی عملیات سایبری

بعد	آماره	ارزیابی طراحی و طرح‌ریزی	ارزیابی آمادگی رزم	ارزیابی اجرا
ارزیابی آمادگی رزم	ضریب همبستگی	۰.۳۱۳		
	سطح معناداری	۰,۰۰۸		
ارزیابی اجرا	ضریب همبستگی	.۸۷۰	.۳۴۰	
	سطح معناداری	.۰۰۰	.۰۰۴	
ارزیابی عملیات سایبری	ضریب همبستگی	.۹۲۶	.۵۵۵	.۹۲۵
	سطح معناداری	.۰۰۰	.۰۰۰	.۰۰۰

سطوح معناداری قیدشده در جدول ۱ نشان می‌دهد که در تمامی موارد، ابعاد با همدیگر دارای ارتباط مثبت و معنادار هستند. همچنین همبستگی بین ابعاد ذکرشده با الگوی راهبردی ارزیابی عملیات سایبری در تمامی موارد معنادار است که نشان‌دهنده وجود همبستگی قوی بین این ابعاد و کل پرسشنامه است.

(۲) ارتباط بین مؤلفه‌های بعد ارزیابی طراحی و طرح‌ریزی و بعد مذکور

جدول شمارهٔ ۲: نتایج همبستگی بین مؤلفه‌های بُعد ارزیابی طراحی و طرح‌ریزی

مؤلفه	بعد	طراحی	طرح‌ریزی
ارزیابی طراحی و طرح‌ریزی	ضریب همبستگی	۰.۷۳۵	۰.۸۱۸
	سطح معناداری	۰,۰۰۰	۰,۰۰۰

سطوح معناداری در جدول ۲ نشان می‌دهد که همبستگی بین مؤلفه‌های بعد ارزیابی طراحی و طرح‌ریزی با بُعد مربوطه در سطح کمتر یا مساوی ۰,۰۰۱ معنادار است که نشان‌دهنده وجود همبستگی معنادار و غیر تصادفی بین مؤلفه‌های مذکور و بُعد ارزیابی طراحی و طرح‌ریزی است.

(۳) ارتباط بین مؤلفه‌های بعد ارزیابی آمادگی رزم و بعد مذکور

جدول شمارهٔ ۳: نتایج همبستگی بین مؤلفه‌های بُعد ارزیابی آمادگی رزم

بعد / مؤلفه		سازمان رزم	نیروی انسانی	حفاظت عملیات	آماد و پشتیبانی	تسلیحات سایبری
ارزیابی آمادگی رزم	ضریب همبستگی	۰,۶۳۰	۰.۶۷۵	۰.۷۵۳	۰,۷۷۱	۰,۶۴۵
	سطح معناداری	۰,۰۰۰	۰,۰۰۰	۰,۰۰۰	۰,۰۰۰	۰,۰۰۰

سطوح معناداری در جدول ۳ نشان می‌دهد که در تمامی موارد، همبستگی بین مؤلفه‌های بُعد ارزیابی آمادگی رزم با بعد مربوطه؛ با اطمینان بیش از ۹۹ درصد معنادار است؛ که نشان‌دهنده وجود همبستگی قوی بین این مؤلفه‌ها و بُعد ارزیابی آمادگی رزم است.

(۴) ارتباط بین مؤلفه‌های بعد ارزیابی اجرا و بعد مذکور

جدول شمارهٔ ۴: نتایج همبستگی بین مؤلفه‌های بُعد ارزیابی اجرا

بعد / مؤلفه		امنیت عملیات	پیشروی و اقدام	کنترل و نظارت
ارزیابی اجرا	ضریب همبستگی	۰.۶۷۰	۰.۴۹۵	۰,۷۵۶
	سطح معناداری	۰,۰۰۰	۰,۰۰۰	۰,۰۰۰

سطوح معناداری قیدشده در جدول ۴ نشان می‌دهد که در تمامی موارد، همبستگی بین مؤلفه‌های بُعد ارزیابی اجرا با بعد مربوطه؛ با اطمینان بیش از ۹۹ درصد معنادار است؛ که نشان‌دهنده وجود همبستگی قوی بین این مؤلفه‌ها و بُعد ارزیابی اجرا است.

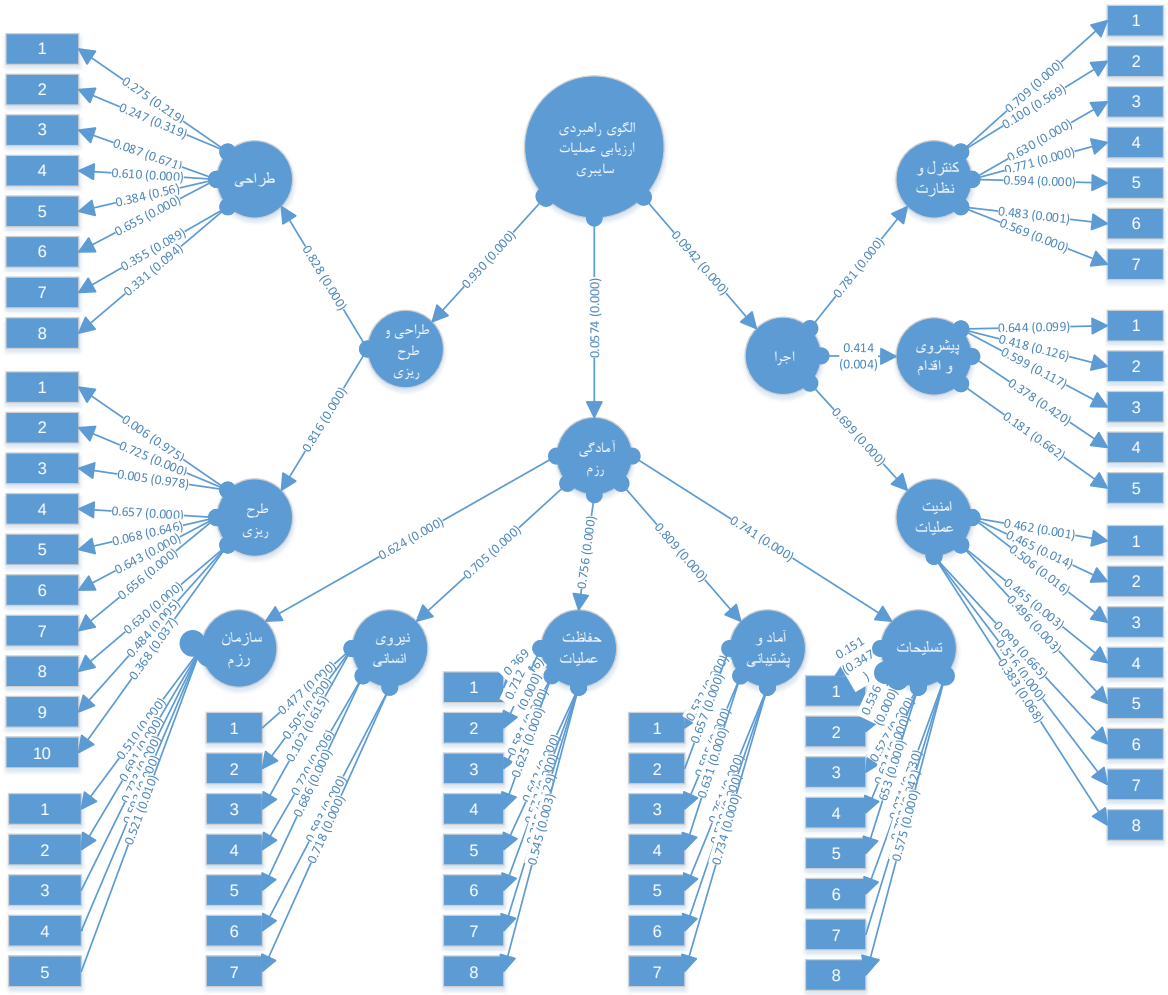
ب) بررسی الگوی تحقیق:

بررسی الگو این تحقیق بر اساس روش آماری حداقل مربعات جزئی[۱] صورت پذیرفته است. این روش، در قالب کلی مدل معادلات ساختاری[۲] مطرح می‌باشد. الگوسازی معادلات ساختاری از دو بخش الگوی اندازه‌گیری و الگوی ساختاری تشکیل‌شده است. الگوی اندازه‌گیری شامل سؤالات (شاخص‌های) هر بعد به همراه آن بعد است و روابط میان سؤالات و ابعاد در این بخش مورد تجزیه‌وتحلیل قرار می‌گیرد. بخش الگوی ساختاری نیز شامل تمامی سازه‌های مطرح در الگوی اصلی تحقیق است و میزان همبستگی سازه‌ها و روابط علی میان آن‌ها در این قسمت مورد سنجش قرار می‌گیرد. شاخص‌ها که معمولاً به سؤال‌های پرسشنامه اطلاق می‌شود، متغیرهای آشکار تحقیق به شمار می‌روند که توسط پاسخگویان به‌طور مستقیم و بی‌واسطه موردسنجش قرار می‌گیرند؛ اما لایه‌های بعدی که مؤلفه‌ها و ابعاد پرسشنامه هستند متغیرهای مکنون[۳] می‌باشند که قابلیت سنجش مستقیم نداشته و با استفاده از روابط بین آن‌ها و نشانگرها یا متغیرهای آشکارشان موردسنجش قرار می‌گیرند. (علی نژاد، ۱۳۹۹) اگر مقدار بار عاملی بین سؤالات پرسشنامه و متغیرهای مکنون بیشتر از ۰،۴ باشد نتیجه می‌گیریم که سؤالی که برای آن سازه به‌کاربرده‌ایم به‌خوبی متغیر مکنون موردنظر را سنجیده است. مقدار آماره t درواقع ملاک اصلی تأیید یا رد فرضیات است. اگر این مقدار آماره به ترتیب از ۱،۶۴، ۱،۹۶ و ۲،۵۸ بیشتر باشد نتیجه می‌گیریم که آن فرضیه در سطوح ۹۰، ۹۵ و ۹۹ درصد تأیید می‌شود. همچنین باید گفت که اگر مقدار ضریب مسیر بین متغیر مکنون مستقل و متغیر مکنون وابسته مثبت باشد نتیجه می‌گیریم که با افزایش متغیر مستقل شاهد افزایش در متغیر وابسته خواهیم بود؛ و بالعکس اگر مقدار ضریب مسیر بین متغیر مکنون مستقل و متغیر مکنون وابسته منفی باشد نتیجه می‌گیریم که با افزایش متغیر مستقل شاهد کاهش در متغیر وابسته خواهیم بود. در این پژوهش برای انجام محاسبات بیان‌شده از نرم‌افزار Smart PLS استفاده‌شده است.

(۱) الگوی ساختاری تحقیق: در شکل‌های ۲ و ۳ الگوی ساختاری تحقیق به همراه ضرایب مسیر الگو، مقادیر t الگوی ساختاری و مقدار P ترسیم‌شده است.

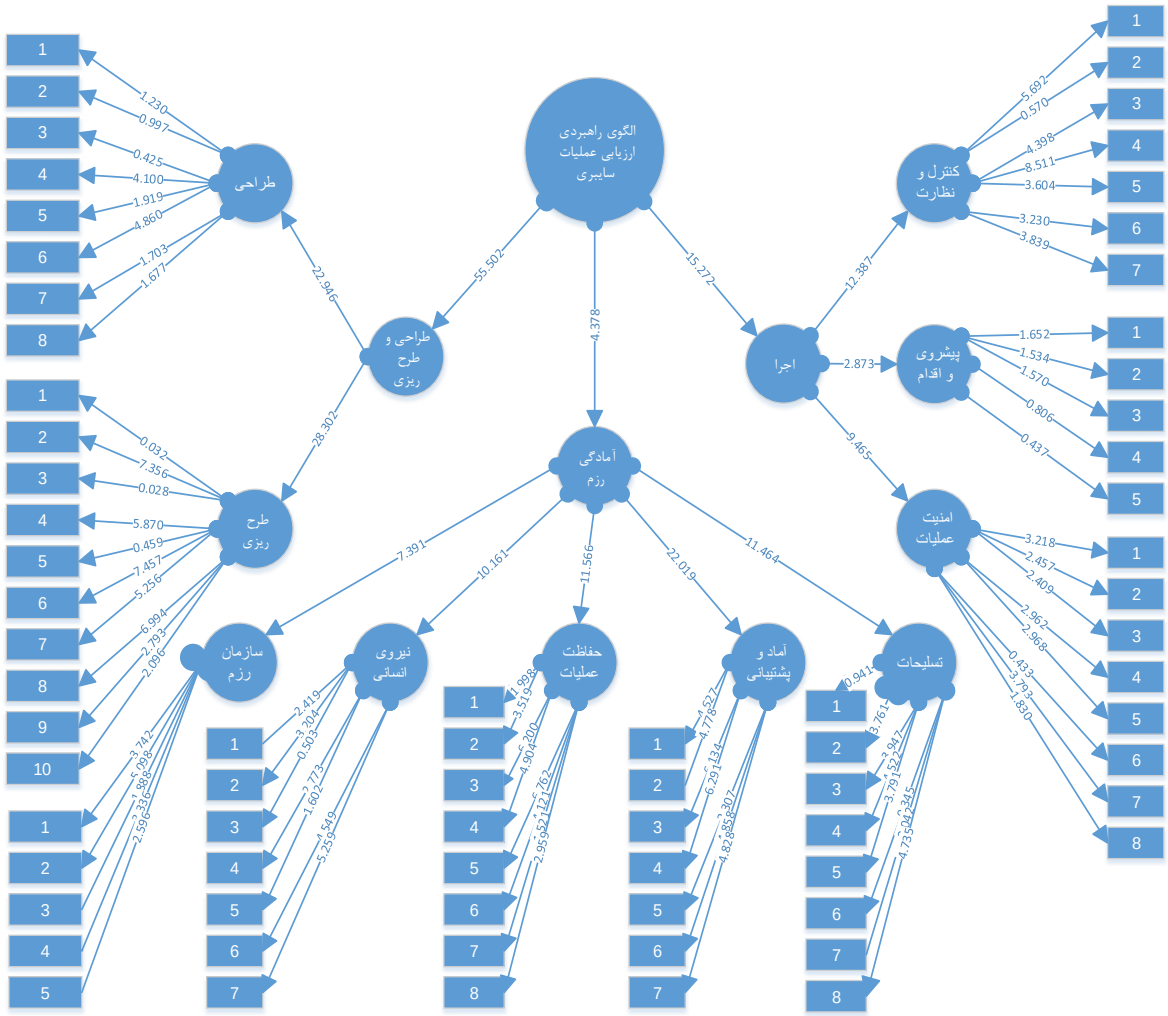
---

۱. Partial Least Squares
۲. Structural Equation Modeling
۳. Latent Variables



شکل شمارهٔ ۳: الگوی ساختاری تحقیق به همراه ضرایب مسیر الگو و مقدار P

در الگوی ساختاری شکل ۲ ابعاد، مؤلفه‌ها و شاخص‌های مورد تأیید نشان داده‌شده‌اند. در این الگو شاخص‌ها همان متغیرهای آشکار هستند که در مستطیل‌های زردرنگ به مؤلفه‌های مربوط به خود متصل شده‌اند. همچنین مقدار بار عاملی، ضرایب مسیر و مقدار P مربوط به ابعاد، مؤلفه‌ها و شاخص‌ها نیز در الگو مشخص‌شده است. در شکل ۳ نیز الگوی ساختاری تحقیق به همراه ضریب معناداری (آماره t) به تصویر درآمده است. با توجه به اینکه مقدارt برای تمام ابعاد و مؤلفه‌های پژوهش بیشتر از ۱/۹۶ هست بنابراین رابطه بین ابعاد و مؤلفه‌ها تأیید می‌شود.



شکل شمارهٔ ۴: الگوی ساختاری تحقیق به همراه مقادیر t الگوی ساختاری

(۲) نتایج الگوی ساختاری:

جدول شمارهٔ ۵: نتایج حاصل از یافته‌های الگوی ساختاری تحقیق

روابط / شاخص	ضریب مسیر	انحراف استاندارد	مقدار t	سطح معناداری	نتیجه

ارزیابی طراحی و طرح‌ریزی ← الگوی راهبردی ارزیابی عملیات	۰.۹۳۰	۰.۰۱۷	۵۵،۵۰۲	۰،۰۰۰	تأیید رابطه
ارزیابی آمادگی رزم ← الگوی راهبردی ارزیابی عملیات	۰.۵۷۴	۰،۱۳۱	۴،۳۷۸	۰،۰۰۰	تأیید رابطه
ارزیابی اجرا ← الگوی راهبردی ارزیابی عملیات	۰.۹۴۲	۰،۰۶۲	۱۵،۲۷۲	۰،۰۰۰	تأیید رابطه

جدول ۵ نشان می‌دهد که همه ضرایب الگوی ساختاری با سطح اطمینان ۹۹ درصد یا بیشتر از آن به معناداری آماری رسیده‌اند. معناداری ضرایب آماری نشان می‌دهد که الگوی راهبردی ارزیابی عملیات سایبری از ابعاد ارزیابی طراحی و طرح‌ریزی، ارزیابی آمادگی رزم و ارزیابی اجرا تشکیل‌شده است. بعد ارزیابی اجرا با ضریب مسیر ۰،۹۴۲ بیش‌ترین تبیین را نسبت به الگوی راهبردی ارزیابی عملیات سایبری دارد؛ به عبارت دیگر تغییری به‌اندازه یک انحراف معیار در بعد ارزیابی اجرا، موجب ایجاد تغییری به ۰،۹۴۲ انحراف معیار در الگوی ارائه‌شده خواهد شد. این نتایج نشان می‌دهد که الگوی ساختاری ارزیابی عملیات سایبری از استحکام بالایی برخوردار است.

(۳) نتایج الگوهای اندازه‌گیری

جدول شمارهٔ ۶: نتایج حاصل از یافته‌های الگوی اندازه‌گیری تحقیق

روابط / شاخص	ضریب مسیر	انحراف استاندارد	مقدار t	سطح معناداری	نتیجه
طراحی ← ارزیابی طراحی و طرح‌ریزی	۰.۸۲۸	۰.۰۳۶	۲۲،۹۴۶	۰،۰۰۰	تأیید رابطه
طرح‌ریزی ← ارزیابی طراحی و طرح‌ریزی	۰.۸۱۶	۰،۰۲۹	۲۸،۳۰۲	۰،۰۰۰	تأیید رابطه
سازمان رزم ← ارزیابی آمادگی رزم	۰.۶۲۴	۰.۰۸۴	۷،۳۹۱	۰،۰۰۰	تأیید رابطه
نیروی انسانی ← ارزیابی آمادگی رزم	۰.۷۰۵	۰،۰۶۹	۱۰،۱۶۱	۰،۰۰۰	تأیید رابطه
حفاظت عملیات ← ارزیابی	۰.۷۵۶	۰.۰۶۵	۱۱،۵۶۶	۰،۰۰۰	تأیید رابطه

آمادگی رزم					
آماد و پشتیبانی ← ارزیابی آمادگی رزم	۰.۸۰۹	۰.۰۳۷	۲۲,۰۱۹	۰,۰۰۰	تأیید رابطه
تسلیحات سایبری ← ارزیابی آمادگی رزم	۰,۷۴۱	۰,۰۶۵	۱۱,۴۶۴	۰,۰۰۰	تأیید رابطه
امنیت عملیات ← ارزیابی اجرا	۰.۶۹۹	۰,۰۷۴	۹,۴۶۵	۰,۰۰۰	تأیید رابطه
پیشروی و اقدام ← ارزیابی اجرا	۰.۴۱۴	۰.۱۴۴	۲,۸۷۳	۰,۰۰۴	تأیید رابطه
کنترل و نظارت ← ارزیابی اجرا	۰,۷۸۱	۰,۰۶۳	۱۲,۳۸۷	۰,۰۰۰	تأیید رابطه

نتایج جدول ۶ نشان می‌دهد که:

مؤلفه‌های طراحی و طرح‌ریزی دارای تأثیر مثبت و معنادار بر بعد ارزیابی طراحی و طرح‌ریزی هستند. در این بین مؤلفه طراحی بیش‌ترین تبیین را نسبت به بعد ارزیابی طراحی و طرح‌ریزی دارد. به عبارت دیگر، تغییری به‌اندازه یک انحراف معیار در سازه مذکور موجب ایجاد تغییری به‌اندازه ۰,۸۲۸ انحراف معیار در بعد ارزیابی طراحی و طرح‌ریزی خواهد شد.

مؤلفه‌های سازمان رزم، نیروی انسانی، حفاظت عملیات، آماد و پشتیبانی، تسلیحات سایبری دارای تأثیر مثبت و معنادار بر بعد ارزیابی آمادگی رزم هستند. در این بین مؤلفه آماد و پشتیبانی بیش‌ترین تأثیر را نسبت به بعد ارزیابی آمادگی رزم دارد. به عبارت دیگر تغییری به‌اندازه یک انحراف معیار در سازه مذکور موجب ایجاد تغییری به‌اندازه ۰,۸۰۹ انحراف معیار در بعد ارزیابی آمادگی رزم خواهد شد.

مؤلفه‌های امنیت عملیات، پیشروی و اقدام، کنترل و نظارت دارای تأثیر مثبت و معنادار بر بعد ارزیابی اجرا هستند. در این بین مؤلفه کنترل و نظارت بیش‌ترین تبیین را نسبت به بعد ارزیابی اجرا دارد. به عبارت دیگر تغییری به‌اندازه یک انحراف معیار در سازه مذکور موجب ایجاد تغییری به‌اندازه ۰,۷۸۱ انحراف معیار در بعد ارزیابی اجرا خواهد شد. بر اساس تجزیه‌وتحلیل‌های بیان‌شده، ارزیابی عملیات سایبری به سه بعد، ده مؤلفه و هفتادوسه شاخص که هر یک در ذیل به‌اختصار بیان می‌شود؛ تقسیم‌بندی می‌گردد.

طراحی

اولین مرحله عملیات سایبری طراحی عملیات است. طراحی درواقع، طرح‌ریزی مفهومی است که در آن کلیات یک عملیات سایبری مشخص می‌شود. جدول ۷ شاخص‌های این مؤلفه را بیان می‌دارد.

جدول شمارهٔ ۷: شاخص‌های مؤلفه طراحی در بعد ارزیابی طراحی و طرح‌ریزی

شاخص	توضیحات
برآورد اطلاعاتی کلان از ساختار و ارتباطات جامعه هدف	پیش‌نیاز تعیین هدف عملیات سایبری، برآورد اطلاعاتی کلان از ساختار و ارتباطات جامعه هدف است. این اطلاعات به‌طور صحیح و مستند موجود نباشد، هدف‌گذاری عملیات به درستی صورت نپذیرفته و هرچند عملیات به‌طور موفق انجام شود اما طراحان عملیات به مطلوب دست نخواهند یافت.
تعیین اهداف کلان و خرد عملیات سایبری و بررسی پیامدهای راهبردی دستیابی به آن‌ها	هرچند اثبات فنی عملیات سایبری بسیار مشکل است اما کشف عامل آن از طریق تحلیل سیاسی کار پیچیده‌ای نیست؛ بنابراین بر اساس انتخاب هر هدف سایبری باید انتظار پیامدهای متناسب با آن نیز بود. به همین دلیل تعیین اهداف عملیات سایبری باید با توجه به پیامد آن صورت پذیرد.
برآورد اطلاعاتی خرد از هر هدف عملیات سایبری	پیش‌نیاز تعیین نوع عملیات سایبری، برآورد اطلاعاتی خرد از هر هدف آن است.
استفاده از اطلاعات میدانی در برآوردهای اطلاعاتی	بهتر است جهت اطمینان از صحت اطلاعات به‌دست‌آمده و تکمیل آن‌ها، از اطلاعات میدانی نیز در صورت امکان بهره گرفت.
تعیین نوع عملیات سایبری با توجه به هدف نهایی عملیات و برآوردهای اطلاعاتی	انواع عملیات سایبری، طیف وسیعی را دربر می‌گیرد. بنا بر هدف عملیات، برآوردهای اطلاعاتی صورت گرفته و پیامدهای احتمالی نوع عملیات سایبری تعیین می‌شود.
انطباق عملیات سایبری با اصول و ارزش‌ها	نکته‌ای که در این بخش بسیار حائز اهمیت است، انطباق اهداف سایبری با اخلاقیات، اصول و ارزش‌هاست. به‌طور مثال هدف سایبری تغییر در میزان کلر تسویه آب آشامیدنی از طریق نفوذ به PLC، منجر به مسمومیت افراد بی‌گناه شده و با هیچ اخلاق و آئینی سازگاری ندارد بنابراین چنین اهدافی باید به‌طور کل از عملیات سایبری حذف گردند.
تعیین سطح گمنامی عملیات سایبری	بخش مهمی از عملیات سایبری که سایر بخش‌ها و بالأخص هزینه عملیات را به‌طور مستقیم تحت تأثیر قرار می‌دهد، سطح گمنامی عملیات سایبری است. درواقع نکته اصلی در تعیین سطح گمنامی پاسخ به این سؤال است که در صورت

	افشاء عملیات، چه پیامدهایی در سطوح فراملی، ملی، سازمانی و شخصی متصور است؟
تعیین انتشار خبر و دستاوردهای عملیات سایبری و سطح آن	در برخی موارد، یکی از اهداف عملیات سایبری مطلع شدن خبرگزاری‌ها یا جامعه هدف است. در چنین مواردی اگر جامعه هدف سکوت خبری نماید، لازم است خبر عملیات سایبری توسط عملیات کنندگان منتشر شود.

طرح‌ریزی

پس از طراحی عملیات سایبری، طرح‌ریزی صورت می‌پذیرد. در طرح‌ریزی ترتیب، توالی و زمان‌بندی اقدامات مربوط به عملیات سایبری مشخص می‌شود. در جدول ۸ شاخص‌های کلیدی طرح‌ریزی بیان‌شده است.

جدول شمارهٔ ۸: شاخص‌های مؤلفه طرح‌ریزی در بعد ارزیابی طراحی و طرح‌ریزی

شاخص	توضیحات
شناسایی عمیق زیر بخش‌های مرتبط با اهداف عملیات سایبری و ارتباطات آن‌ها	این شاخص لازمه تعیین چگونگی انجام عملیات سایبری خواهد بود.
انطباق شناسایی‌های عمیق بر برآوردهای اطلاعاتی مرحله طراحی	اگر شناسایی‌های صورت پذیرفته با برآوردهای اطلاعاتی مرحله طراحی منطبق نباشند، لازم است طراحان عملیات سایبری مطلع شده تا در تعیین نوع عملیات سایبری تجدیدنظر نمایند.
منجر شدن مجموعه اهداف خرد به اهداف کلان و اهداف کلان به هدف نهایی عملیات سایبری	پس از شناسایی عمیق باید از این مطلب اطمینان حاصل نمود که دستیابی به‌تمامی اهداف خرد، عملیات کنندگان را به اهداف کلان می‌رساند و دستیابی به اهداف کلان نیز به هدف نهایی عملیات سایبری منجر می‌شود.
حصول اطمینان از بررسی تمامی راهکارهای دستیابی به اهداف با توجه به نوع عملیات سایبری	با توجه به برآوردهای خرد اطلاعاتی، راهکارهای مختلفی برای دستیابی به اهداف عملیات سایبری وجود خواهد داشت. لازم است تمامی راهکارها بررسی‌شده و مناسب‌ترین آن انتخاب گردد.
انطباق راهکار برگزیده عملیات سایبری با اصول و ارزش‌ها	برای دستیابی به هدف مشروع و اخلاقی عملیات سایبری نباید مسیری را طی نمود که منطبق با اصول و ارزش‌ها نباشد.
تعیین تاریخ، ساعت و مدت عملیات سایبری	تاریخ، ساعت و مدت عملیات سایبری باید برای تمامی عملیات کنندگان تعیین و تفهیم شود. همچنین می‌توان با تعیین تاریخ و ساعتی خاص، پیامی را به جامعه هدف مخابره نمود.

تعیین چگونگی مستندسازی عملیات سایبری جهت ارزیابی و بهره‌برداری‌های آتی	بسیاری از ارزیابی‌های عملیات سایبری بر اساس مستنداتی انجام می‌شود که از فرایند کاری عملیات کنندگان در حین عملیات تهیه‌شده است. چگونگی این مستندسازی لازم است به‌طور جامع در طرح‌ریزی عملیات سایبری بیان شود.
وجود پیوست جامع امنیت عملیات متناسب با سطح گمنامی	با توجه به سطح گمنامی عملیات سایبری که در مرحله طراحی مشخص گردیده است؛ لازم است پیوست امنیت عملیات متناسب با آن نوشته و در اختیار عملیات کنندگان قرار گیرد.
تعیین حدود اختیارات سطوح مختلف فرماندهی عملیات سایبری در مواجهه با شرایط غیرمترقبه	در طی اجرای عملیات سایبری ممکن است شرایط غیرمترقبه‌ای به وجود آید. برای فرماندهان عملیات، محدوده اختیارات جهت تصمیم‌گیری یا مطلع ساختن فرمانده سطح بالاتر باید تبیین شود.
تعیین چگونگی و ملاحظات انتشار خبر و دستاوردهای عملیات سایبری با توجه به سطح تعیین‌شده	چگونگی انتشار خبر و دستاوردهای عملیات سایبری بدون افشاء هویت ملی عملیات کنندگان در این قسمت تعیین می‌شود.

سازمان رزم

جدول ۹ شاخص‌های مؤلفه سازمان رزم را در بعد ارزیابی آمادگی رزم بیان می‌دارد.

جدول شمارهٔ ۹: شاخص‌های مؤلفه سازمان رزم در بعد ارزیابی آمادگی رزم

شاخص	توضیحات
تعیین سازمان رزم عملیات سایبری متناسب با طرح‌ریزی	سازمان رزم عملیات سایبری باید متناسب با نوع عملیات، مدت عملیات، سطح گمنامی تخصص موردنیاز و بسیاری عوامل دیگر تعیین شود.
تقسیم‌بندی اهداف عملیاتی در سازمان رزم	اهداف عملیاتی باید با توجه به تخصص موردنیاز برای دستیابی به آن‌ها، تجربه افراد، اهمیت هر هدف و بسیاری عوامل دیگر در سازمان رزم تقسیم‌بندی شود.
متناسب بودن اجزاء سازمان رزم عملیات سایبری در تعداد نفرات، توانمندی و تجهیزات با اهداف تقسیم‌بندی شده	در صورتی که افراد کافی با تخصص موردنیاز و تسلیحات سایبری متناسب با نوع عملیات در اختیار نبود؛ باید در بعد ارزیابی طراحی و طرح‌ریزی تجدیدنظر نمود.
هماهنگی فرماندهان اجزاء سازمان رزم عملیات سایبری در مراحل انجام عملیات با یکدیگر و با فرماندهان ارشد مرتبط	پیشروی عملیات کنندگان در دستیابی به اهداف عملیات سایبری باید به صورت هماهنگ با یکدیگر صورت پذیرد.

تفهیم طرح عملیات به سازمان رزم به‌صورت حیطه‌بندی شده	طرح عملیاتی لازم است به‌صورت حیطه‌بندی شده و در حد نیاز به هر عملیات کننده تفهیم شود.

نیروی انسانی

اصلی‌ترین مؤلفه عملیات سایبری، نیروی انسانی آن است. در جدول ۱۰ شاخص‌های اصلی که برای ارزیابی نیروی انسانی عملیات سایبری حائز اهمیت می‌باشد، شرح داده‌شده است.

جدول شمارهٔ ۱۰: شاخص‌های مؤلفه نیروی انسانی در بعد ارزیابی آمادگی رزم

شاخص	توضیحات
آمادگی روحی نیروی انسانی برای انجام عملیات سایبری	از افرادی که در شرایط روحی مناسبی قرار ندارند، نباید در عملیات سایبری استفاده نمود.
پذیرش مخاطرات حین و پس از انجام عملیات سایبری توسط نیروی انسانی	هر عملیات سایبری بالأخص عملیات با سطح گمنامی بالا، مخاطرات متعددی را برای عملیات کنندگان به وجود می‌آورد. این مخاطرات باید برای نیروی انسانی دخیل در عملیات شرح داده شود؛ و هر فرد جهت شرکت در عملیات، باید با آگاهی از مخاطرات انجام عملیات را پذیرفته باشد.
درک مشترک نیروی انسانی از اهداف مرتبط و چگونگی دستیابی به آن	برداشت یکسان نیروی انسانی از طرح‌ریزی عملیاتی بسیار حائز اهمیت است.
اطلاع طراحان عملیات سایبری از نظرات نیروی انسانی	طراحان عملیات سایبری باید از نظرات فنی و تخصصی نیروی انسانی دخیل در عملیات سایبری مطلع باشند.
موفقیت نیروی انسانی عملیات سایبری در رزمایش‌ها	پیش از انتخاب نیروی انسانی عملیات سایبری لازم است توانایی و تخصص هر فرد در رزمایش‌های سایبری پیشین یا عملیات گذشته بررسی شود.
اطمینان از توانمندی نیروی انسانی از طریق شبیه‌سازی عملیات سایبری کنونی	پیش از اجرای عملیات سایبری لازم است نیروی انسانی منتخب در شبیه‌سازی متناسب با اهداف عملیاتی شرکت کرده، توانایی و تخصص خود را به اثبات برسانند.
اطمینان از تسلط رزمندگان سایبری عرصه شناختی به زبان، فرهنگ، اصطلاحات و مسائل اعتقادی سیاسی مرتبط با هویت ایجادشده	معمولاً عملیات شناختی از طریق ایجاد هویت‌ها آغاز می‌شود. عملیات کنندگان شناختی باید به زبان، فرهنگ، اصطلاحات و مسائل اعتقادی سیاسی مرتبط با هویت ایجادشده تسلط داشته باشند.

حفاظت عملیات

بررسی امنیت عملیات و حفاظت آن بالأخص در حوزه نیروی انسانی بخش مهمی است که به‌طور مستقیم بر گمنام ماندن عملیات تأثیر می‌گذارد. در جدول ۱۱ شاخص‌های اصلی حفاظت عملیات بیان‌شده است.

جدول شمارهٔ ۱۱: شاخص‌های مؤلفه حفاظت عملیات در بعد ارزیابی آمادگی رزم

شاخص	توضیحات
توجیه امنیتی نیروی انسانی متناسب با سطح گمنامی عملیات سایبری	تمامی نیروی انسانی عملیات سایبری نسبت به سطح گمنامی عملیات و نکات حفاظتی که متناسب با آن سطح لازم است رعایت گردد، توجیه شوند.
توجیه حفاظتی نیروی انسانی نسبت به مخاطرات و پیامدهای انجام عملیات	در صورتی که نیروی انسانی عملیات سایبری نسبت به مخاطرات و پیامدهای انجام عملیات توجیه نشوند، احتمال شکست حفاظتی بالأخص پس از انجام عملیات بالا خواهد بود.
حصول اطمینان از اطلاع نیروی انسانی نسبت به حدود اختیارات خود	هر فرد دخیل در عملیات سایبری باید از وظایف و حدود اختیارش آگاهی کامل داشته باشد.
تأیید امنیت کانال ارتباطی نسبت به حملات فعال و غیرفعال	کانال ارتباطی نقش مهمی در هماهنگی گروه‌های عملیاتی و جابجایی اطلاعات حاصل از عملیات سایبری دارد؛ بنابراین اطمینان از ایمن بودن کانال مذکور بسیار حائز اهمیت است.
حصول اطمینان از خرید یا تولید گمنام و بدون آلودگی ملزومات عملیات سایبری	یک عملیات سایبری ملزومات سخت‌افزاری و نرم‌افزاری متعددی دارد. لازم است از نشان‌دار نبودن، رعایت گمنامی و آلوده نبودن این ملزومات به بدافزارها اطمینان حاصل شود.
حصول اطمینان از به‌روزرسانی و پیکربندی امن تجهیزات فیزیکی و مجازی مورداستفاده در عملیات سایبری	بسیاری از آسیب‌پذیری‌های سایبری با به‌روزرسانی تجهیزات برطرف می‌گردد. همچنین با پیکربندی امن تجهیزات مورداستفاده در عملیات سایبری می‌توان از بسیاری نفوذهای معکوس جلوگیری نمود.
حصول اطمینان موفقیت سامانه‌ها و وب‌سایت‌های پشتیبان عملیات سایبری در آزمایش‌های نفوذ، فشار، بار و پایداری	سامانه‌ها و صفحات اینترنتی مورداستفاده در عملیات سایبری باید قبل از به‌کارگیری مورد آزمون نفوذ، فشار، بار و پایداری قرار گیرند و آسیب‌پذیری‌های آن‌ها برطرف شده سپس در عملیات مورداستفاده قرار گیرند.
حصول اطمینان از هویت‌سازی همه‌جانبه و ایجاد امن آن در عرصه شناختی	لازم است برای هویت‌های ساخته‌شده جهت عملیات سایبری شناختی، در همه ابعاد سناریو تعریف نمود تا اگر در حین عملیات اتفاق غیرمترقبه‌ای روی داد، واکنش هویت به رویداد از قبل مشخص‌شده باشد.

آماد و پشتیبانی

بدون فراهم آوردن و تقسیم صحیح امکانات آمادی و پشتیبانی مستمر از عملیات سایبری، اجرای آن با اختلال مواجه خواهد شد. شاخص‌های جدول ۱۲ موارد اصلی هستند که برای ارزیابی آماد و پشتیبانی باید موردتوجه قرار گیرند.

جدول شمارهٔ ۱۲: شاخص‌های مؤلفه آماد و پشتیبانی در بعد ارزیابی آمادگی رزم

شاخص	توضیحات
برآورد سخت‌افزار موردنیاز در عملیات سایبری و تأمین گمنام آن	تأمین گمنام سخت‌افزار موردنیاز در عملیات از خارج از محدوده جغرافیایی ملی تأثیر مهمی در حفظ گمنامی عملیات سایبری خواهد داشت.
برآورد تعداد سرورهای مجازی موردنیاز در عملیات سایبری و خرید گمنام آن	به دلیل اینکه نفوذ به رایانه کاربران اینترنت و سرورهای مجازی آنان، عملی خلاف اصول و ارزش‌هاست؛ توصیه محققین، خرید گمنام سرورهای مذکور است.
برآورد پول موردنیاز عملیات سایبری (ریال، ارز، رمز ارز) و تأمین گمنام آن	برآورد صحیح و تأمین گمنام پول موردنیاز عملیات سایبری در موفقیت عملیات و گمنامی آن نقش به سزایی را بازی می‌کند.
تأمین سامانه‌ها، ابزار و تسلیحات موردنیاز عملیات سایبری متناسب با سطح گمنامی عملیات	تأمین به‌موقع و گمنام سامانه‌ها، ابزار و تسلیحات موردنیاز عملیات سایبری از وظایف اصلی بخش آماد و پشتیبانی به‌حساب می‌آید.
واگذاری متناسب ملزومات عملیات سایبری به سازمان رزم	هر جزء سازمان رزم عملیات سایبری دارای وظایفی متناسب با عده و توانمندی خود می‌باشد. واگذاری ملزومات عملیات سایبری متناسب با وظیفه محول شده تأثیرگذار در روحیه نیروی انسانی و موفقیت عملیات خواهد بود.
فراهم‌سازی زیرساخت‌های ارتباطی امن و گمنام عملیات سایبری برای سازمان رزم	یک عملیات سایبری به زیرساخت‌های متعددی مانند زیرساخت ارتباطات اینترنت، زیرساخت گمنامی، زیرساخت ارتباطات گروه‌های عملیاتی و غیره نیاز دارد. امنیت، پایداری و گمنامی زیرساخت‌های مذکور تأثیر مهمی در پیشبرد عملیات خواهد داشت.
تأمین برق پشتیبان برای عملیات سایبری	وجود برق پشتیبان، نکته مهمی است که باعث می‌شود در صورت قطعی برق، عملیات سایبری متوقف نگردد.

تسلیحات سایبری

هرچند عوامل متعددی در موفقیت یک عملیات سایبری نقش دارند اما تسلیحات سایبری

یکی از مهم‌ترین عوامل در دستیابی به اهداف تعیین‌شده عملیات سایبری است. جدول ۱۳ شاخص‌های این مؤلفه را بیان می‌دارد.

جدول شمارهٔ ۱۳: شاخص‌های مؤلفه تسلیحات سایبری در بعد ارزیابی آمادگی رزم

شاخص	توضیحات
کارایی سامانه‌ها، ابزار و تسلیحات عملیات سایبری	سامانه‌ها، ابزار و تسلیحات بکار گرفته‌شده در عملیات سایبری باید کارایی لازم را متناسب با نوع عملیات سایبری داشته باشند.
هوشمندی در اختفاء تسلیحات و عدم شناسایی آن‌ها توسط ضد بدافزارها	یک سلاح سایبری باید هوشمندی لازم را در مخفی شدن از نرم‌افزارها و سخت‌افزارهای کشف کننده بدافزارها داشته باشد.
هوشمندی تسلیحات در نداشتن امضاء ایستا و رفتاری	بسیاری از تجهیزات امنیتی، بدافزارها را از طریق امضاءهای شناخته‌شده شناسایی می‌نمایند؛ بنابراین یک سلاح سایبری باید فاقد هرگونه امضاء شناخته‌شده ایستا و رفتاری باشد.
توانایی سلاح در حس هوشمند وجود سامانه‌های فریب، کنترل و نظارت	تسلیحات سایبری باید توانایی حس محیط را داشته باشند تا در دام سامانه‌های فریب یا نظارتی شبکه هدف گرفتار نگردند.
قابلیت امحاء خودکار تسلیحات عملیات سایبری تحت شرایط افشاء	در صورتی که سلاح تشخیص داد که کشف گردیده است باید نسبت به قطع هرگونه ارتباط و امحاء خودکار خود را اقدام نماید.
هوشمندی تسلیحات عملیات سایبری در تشخیص وجود ردپا و پاک‌سازی خودکار آن	سلاح سایبری لازم است توانایی تشخیص ردپای هود و امحاء آن را داشته باشد.
انحصار تسلیحات عملیات سایبری به عملیات جاری	در صورت به‌کارگیری یک سلاح سایبری در چند عملیات مجزا از هم عملیات به یکدیگر مرتبط شده و کشف مبدأ عملیات آسان‌تر خواهد گردید.
قابلیت‌های هوشمند ضد دیس اسمبلی، ضد دیباگ، ضد روبرداری حافظه و قابلیت شناسایی هوشمند محیط تحلیل رفتاری تسلیحات عملیات سایبری	یک سلاح سایبری باید قابلیت‌ها ضد دیس اسمبلی، ضد دیباگ، ضد روبرداری حافظه و قابلیت شناسایی هوشمند محیط تحلیل رفتاری را دارا باشد.

امنیت عملیات

بر اساس تعریف عملیاتی، امنیت عملیات سایبری به مجموعه اقداماتی گفته می‌شود که جهت جلوگیری از کشف حمله یا فنون بکار رفته در آن و حفظ گمنامی منشأ حمله توسط مهاجم در

نظر گرفته می‌شود. جدول ۱۴ شاخص‌های این مؤلفه را در بعد ارزیابی اجرای عملیات سایبری بیان می‌دارد.

جدول شمارهٔ ۱۴: شاخص‌های مؤلفه امنیت عملیات در بعد ارزیابی اجرا

شاخص	توضیحات
شناسایی و عبور امن از تجهیزات امنیتی شبکه هدف	عملیات کننده سایبری باید بتواند تجهیزات امنیتی شبکه هدف را شناسایی کرده، به‌طور امن از آن عبور نماید.
پاک‌سازی ردپاهای بر جامانده	در صورتی که عملیات کننده سایبری ردپایی از خود برجای گذاشت باید نسبت به امحاء آن اقدام نماید.
ذخیره و انتقال امن اطلاعات به‌دست‌آمده در عملیات سایبری	اطلاعات به‌دست‌آمده در عملیات سایبری باید بدون ایجاد حساسیت برای تجهیزات امنیتی از شبکه هدف خارج و به محل امنی انتقال یابد.
امکان انتقال یا امحاء هوشمند، سریع و امن اطلاعات، نرم‌افزارها و تجهیزات در مواقع خطر	بعضاً ممکن است در عملیات سایبری مکان عمل‌کنندگان افشاء شود و آن‌ها در معرض خطر قرار گیرند. برای چنین مواقعی لازم است تجهیزات لازم جهت امحاء هوشمند، سریع و امن اطلاعات، نرم‌افزارها و تجهیزات بکار رفته در عملیات سایبری فراهم باشد.
بررسی مداوم وقایع امنیتی ثبت‌شده در تجهیزات عملیاتی به‌منظور کشف و جلوگیری از نفوذ برگشتی	لازم است عملیات کنندگان وقایع امنیتی زیرساخت مورداستفاده خود را به‌طور مستمر پایش نمایند تا در صورت نفوذ معکوس هدف، بتوانند با پیشروی آن مقابله نمایند.
حصول اطمینان از بررسی اخبار و وضعیت هوای شهر اقامتی هویت قبل از هر فعالیت برخط در عرصه شناختی	در عملیات شناختی هنگام زمان ارتباطات برخط ممکن است مخاطب به رویدادهایی اشاره کند که تنها در محل سکونت هویت رخ‌داده باشد. برای جلوگیری از غافلگیری لازم است گردانندگان هویت قبل از برقراری ارتباط برخط، موارد بیان‌شده را بررسی نمایند.
هوشمندی در زمان ارسال پست‌ها مطابق ویژگی‌های هویت وعدم فعالیت هم‌زمان هویت‌ها روی یک موضوع در عرصه شناختی	زمان ارسال پست‌های هویت، باید مطابق شخصیت‌پردازی وی صورت پذیرد. همچنین اگر برای جریان سازی، همه هویت‌ها به‌طور هم‌زمان اقدام به بازنشر نمایند، ارتباطشان با یکدیگر آشکارشده و می‌تواند منجر به افشاء عملیات گردد.
پاک‌سازی محل استقرار و تجهیزات نیروی انسانی پس از اتمام عملیات	پس از انجام عملیات سایبری و قبل از ترک دائمی محل، لازم است مکان انجام عملیات از وجود تجهیزات و بقایای بیولوژیک گروه عملیاتی پاک‌سازی گردد.

پیشروی و اقدام

حساس‌ترین مرحله عملیات سایبری پیشروی و انجام اقدام لازم برای دستیابی به اهداف تعیین‌شده است. شاخص‌های جدول ۱۵ مواردی است که برای ارزیابی مؤلفه پیشروی و اقدام در بعد ارزیابی اجرای عملیات سایبری باید رعایت گردد.

جدول شمارهٔ ۱۵: شاخص‌های مؤلفه امنیت عملیات در بعد ارزیابی اجرا

شاخص	توضیحات
دسترسی به فرماندهان ارشد عملیات سایبری جهت بازنگری فوری طرح عملیاتی در صورت نیاز	در حین انجام عملیات سایبری ممکن است شرایطی روی دهد که کل عملیات را تحت تأثیر قرار دهد. در چنین شرایطی باید فرماندهان ارشد عملیات سایبری جهت بازنگری فوری طرح عملیاتی یا متوقف ساختن آن در دسترس باشند.
پیشروی و اقدام هماهنگ سازمان رزم عملیات سایبری مطابق طرح عملیاتی	در عملیات سایبری ممکن است اهداف خرد به نحوی بین گروه‌های عملیاتی تقسیم‌شده باشد که تقدم و تأخر دستیابی به آن‌ها حائز اهمیت باشد؛ بنابراین گروه‌های عملیاتی باید به‌صورت هماهنگ با یکدیگر تحت رهبری فرمانده عملیات پیشروی و اقدام را انجام دهند.
مستندسازی برخط پیشروی، اقدام و دستیابی به اهداف عملیات سایبری	برای ارزیابی مرحله پیشروی و اقدام نیاز به مستندسازی برخط عملیات کنندگان می‌باشد.
تحقق اهداف خرد و کلان عملیات سایبری بر اساس مستندات	تنها بر اساس مستندسازی عملیات کنندگان سایبری است که می‌توان به‌طور دقیق میزان دستیابی به اهداف عملیات را محاسبه نمود.
انتشار خبر و دستاوردهای عملیاتی مطابق طرح عملیاتی و پیوست امنیتی	برای دستیابی هدف روانی اجرای موفقیت‌آمیز عملیات سایبری در طرح عملیات انتشار خبر عملیات و چگونگی آن بیان‌شده است. این انتشار باید با رعایت موارد ذکرشده در پیوست امنیت عملیات صورت پذیرد تا باعث افشاء هویت ملی عملیات کنندگان نگردد.

کنترل و نظارت

بدیهی است که حین اجرای عملیات سایبری، کنترل و نظارت صورت می‌پذیرد. این مؤلفه کنترل و نظارت اجرای عملیات را ارزیابی می‌نماید. جدول ۱۶ شاخص‌های این ارزیابی را بیان نموده است.

جدول شمارهٔ ۱۶: شاخص‌های مؤلفه کنترل و نظارت در بعد ارزیابی اجرا

شاخص	توضیحات
اجرای عملیات سایبری مطابق طرح عملیاتی	هرگونه عدول از طرح عملیات سایبری در اجرا بدون مجوز فرمانده عملیات به‌منزله ضعف در کنترل و نظارت عملیات سایبری می‌باشد.
شناسایی و نحوه مواجهه با تجهیزات امنیتی شبکه هدف	در شناسایی و چگونگی مواجهه با تجهیزات امنیتی شبکه هدف لازم است کنترل و نظارت مضاعفی صورت گیرد تا جلوی هرگونه خطای انسانی گرفته شود.
رسیدن به حد آستانه‌ای که عملیات سایبری را به دلیل عدم تطابق طرح‌ریزی با میدان متوقف می‌کند	در طرح‌ریزی عملیاتی باید حد آستانه‌ای که عملیات سایبری را به دلیل عدم تطابق طرح‌ریزی با میدان متوقف می‌کند؛ مشخص‌شده باشد. نظارت بر عملیات به‌منظور تشخیص نزدیکی به حد آستانه مذکور، در این بند مدنظر می‌باشد.
انجام هوشمند مستندسازی عملیات سایبری	کنترل و نظارت بر جامعیت و استمرار مستندسازی هوشمند عملیات سایبری شاخص مهمی است که بر اساس آن می‌توان کنترل و نظارت حین عملیات را ارزیابی نمود.
شرایط روحی و جسمی نیروی انسانی	حین انجام عملیات سایبری فشار کاری و اضطراب ناشی از آن بسیار بالاست؛ بنابراین بر شرایط روحی و جسمی نیروی انسانی به‌طور مستمر نظارت و کنترل داشت تا از هرگونه خطای انسانی جلوگیری شود.
کاشت و به‌کارگیری صحیح تسلیحات	در صورتی که تسلیحات سایبری به‌درستی در محل مدنظر قرار نگرفته یا به‌طور صحیح پیکربندی نشده باشد؛ عملیات سایبری در دستیابی به اهداف خود دچار چالش خواهد شد.
امنیت فیزیکی نیروی انسانی	ممکن است عملیات سایبری در محیطی انجام شود که تأمین امنیت فیزیکی آن با دشواری صورت می‌پذیرد. در چنین موقعیت‌هایی کنترل و نظارت محیطی جهت کشف خطر قریب‌الوقوع برای نیروی انسانی، تجهیزات و اطلاعات عملیات سایبری بسیار حیاتی است.

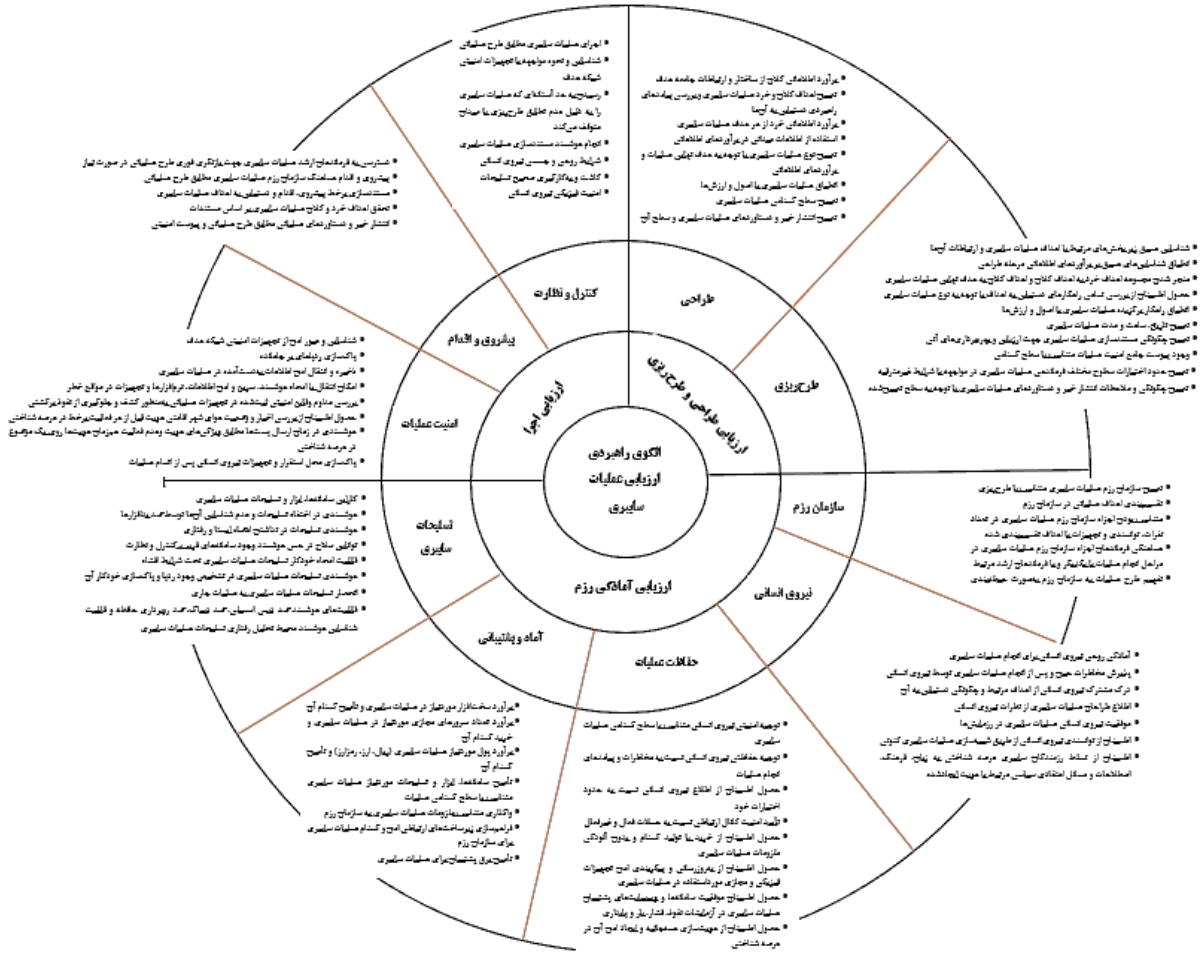
نتیجه‌گیری

در کشورهای پیشرو یکی از اصلی‌ترین راهکارهای دفاع سایبری، دفاع عامل است که بر اساس آن عملیات سایبری بر روی عوامل تهدیدزا صورت می‌پذیرد تا از بالفعل شدن تهدید جلوگیری گردد. علاوه بر این، افزایش قدرت در فضای سایبری باعث بازدارندگی سایبری شده و منجر به افزایش امنیت سایبری کشور می‌گردد. توان انجام موفق عملیات سایبری، علاوه بر اینکه قدرت سایبری را افزایش داده و بازدارندگی سایبری را باعث می‌شود؛ می‌تواند کاهش تهدیدات سایبری را نیز در پی داشته باشد.

از سویی به دلیل ناملموس بودن فضای سایبر، ارزیابی اقدامات و بررسی نتایج آن‌ها با دشواری روبروست و از سویی دیگر، ارزیابی فعالیت‌های سایبری جهت شناسایی ضعف و قوت‌ها و بررسی میزان اثربخشی فعالیت‌ها اجتناب‌ناپذیر است؛ اما ارزیابی عملیات سایبری از ارزیابی بسیاری از فعالیت‌های سایبری دشوارتر است زیرا در اغلب موارد، نتایج حاصل از عملیات سایبری در فضای سایبری هدف اثر گذاشته و دسترسی به نتایج با دشواری روبروست.

با توجه به موارد بیان‌شده و لزوم ارزیابی عملیات سایبری در بالاترین سطح ممکن، پژوهش حاضر صورت پذیرفت و بر اساس یافته‌های به‌دست‌آمده که به تأیید ۷۰ نفر از خبرگان عملیات سایبری نیز رسیده است؛ الگوی راهبردی ارزیابی عملیات سایبری تهیه شد. بر اساس این الگو، ارزیابی عملیات سایبری به سه بعد، ده مؤلفه و هفتادوسه شاخص تقسیم‌بندی می‌شود.

اولین بعد، بعد ارزیابی طراحی و طرح‌ریزی است که به دو مؤلفه طراحی و طرح‌ریزی تقسیم می‌گردد. بعد دوم، بعد ارزیابی آمادگی رزم می‌باشد که به پنج مؤلفه امنیت سازمان رزم، نیروی انسانی، حفاظت از عملیات، آماد و پشتیبانی، تسلیحات سایبری بخش‌بندی می‌گردد؛ و درنهایت سومین بعد ارزیابی عملیات سایبری، بعد ارزیابی اجرا است که به سه مؤلفه امنیت عملیات، پیشروی و اقدام، کنترل و نظارت تقسیم می‌شود. بر اساس ابعاد، مؤلفه‌ها و شاخص‌های مورد تأیید خبرگان، الگوی راهبردی ارزیابی عملیات سایبری به شرح شکل ۵ ارائه می‌گردد:



شکل شمارهٔ ۵: الگوی راهبردی ارزیابی عملیات سایبری

پیشنهاد

با توجه به اینکه الگوی حاصل از این پژوهش در بالاترین سطح عملیات سایبری -یعنی سطح راهبردی- ارائه شده است؛ برای ادامه پژوهش می‌توان در سطوح عملیاتی و تاکتیکی نیز اقدام به

ارائه الگوی ارزیابی عملیات سایبری نمود.

همچنین جهت ادامه تحقیق حاضر می‌توان برای هر یک از مؤلفه‌های ارائه‌شده در الگو، اقدام به ارائه الگوی راهبردی، عملیاتی یا تاکتیکی نمود. به‌طور مثال می‌توان به الگوهای راهبردی، عملیاتی یا تاکتیکی امنیت عملیات سایبری، طراحی عملیات سایبری و غیره اشاره کرد.

با توجه به ماهیت ناملموس فضای سایبر و لزوم اشرافیت فرماندهان در زمان اجرای عملیات سایبری، می‌توان الگوهایی در هر سه سطح راهبردی، عملیاتی و تاکتیکی جهت فرماندهی و کنترل عملیات سایبری تهیه نمود. بدیهی است الگوهای ارائه‌شده نباید رخنه امنیتی جدیدی که گمنامی عملیات سایبری را تهدید نماید؛ ایجاد کند و از طریق دسترسی‌های پیشین قابلیت فرماندهی و کنترل را فراهم نمایند.

درنهایت پیشنهاد می‌شود به‌منظور ادامه این پژوهش، به طرح راهبردی ارزیابی عملیات سایبری پرداخته شود تا فرماندهان ارشد عملیات سایبری بتوانند به‌منظور ارتقاء قدرت سایبری، ایجاد بازدارندگی و انجام دفاع عامل سایبری از طرح راهبردی ارائه‌شده استفاده کرده و در صورت صلاحدید، برنامه راهبردی ارزیابی عملیات سایبری را تدوین نمایند.

فهرست منابع:

جباررشیدی، علی، شکیبازاد، محمد. (۱۳۹۶). مدل‌سازی و شبیه‌سازی صحنه نبرد سایبری، *مدیریت فناوری اطلاعات* ۳۳-۹ (۸۰۹-۸۲۸).

جمالی، احمدمهدی، پرتوی، محمدتقی، پورجعفری، مرتضی. (۱۳۹۹). عملکرد مرکز بازسازی و بهینه‌سازی یا علی (ع) هوانیروز در ارتقاء آمادگی رزمی آجا. علوم و فنون نظامی، ۱۶(۵۱), ۱۰۳-۱۲۶.

رضاییان، علی (۱۳۸۶). *مبانی سازمان و مدیریت، تهران*، سمت، چاپ دهم

شفیع پور، ب. پورقهرمانی، د. ب. (۱۳۹۳). تهدیدهای سایبری علیه ایران و چالش مقابله با آن . *همایش ملی ایران و چالش‌های حقوقی بین‌المللی*. دانشگاه آزاد اسلامی واحد مراغه

فروردین، و. سملی, ا., عمویی, ح. (۱۳۹۷). بررسی تأثیرات جنگ سایبری بر امنیت ملی در جمهوری اسلامی ایران .*کنفرانس بین‌المللی امنیت، پیشرفت و توسعه پایدار مناطق مرزی، سرزمینی و کلان‌شهرها*،

راهکارها و چالش‌ها با محوریت پدافند غیرعامل و مدیریت بحران. دانشگاه افسری امام علی (ع)

کرم روان، ف. (۱۳۹۸). تحلیل حقوقی سند راهبردی پدافند سایبری کشور .*دومین کنفرانس ملی پدافند سایبری*. دانشگاه آزاد اسلامی واحد مراغه

مدنی، سید مصطفی، آبسالان، محمد. (۱۳۹۴). تأثیر رهبری تحول‌آفرین بر ارتقاء توان رزمی در یک سازمان دفاعی. فصلنامه مدیریت نظامی، ۱۵(۵۹), ۳۲-۵۸.

AFDD. (۲۰۱۱). *Air Force Doctrine Document (AFDD)* ۳-۱۲, ۱۵ Jul ۲۰۱۰. Incorporating Change, ۱, ۳۰.

Department of the Army. (۲۰۱۹). *Army Doctrine Publication* ۵-۰ - The Operations Process. Joint Publication ۵-۰, ۲۳. https://armypubs.army.mil/٪۰Ahttps://atiam.train.army.mil/catalog/dashboard

DoD. (۲۰۱٤). Information Operations - Joint Publication ۳-۱۳.:*Information Operations*, ۱(۱), ۱–۸۷. https://doi.org/۱۰,۱۰۱٦/j.jalz.۲۰۰٦,۰٥,۱٤۰۱

DoD. (۲۰۱۷). JP ٥-۰. *Joint Chiefs of Staff ۲۰۱۷*, June ۱٦, viewed ۱۸ April ۲۰۱۸.

DoD. (۲۰۱۸). *Cyberspace Operations.* Department of Defense United States.

DoD. (۲۰۲۰). *DoD dictionary of military and associated terms*. Joint Publication, ۱–۲.

Dressler, J. (۲۰۱٥). Analyzing the use of cyber in warfare at the strategic, operational, and tactical levels.

Eom, J. H. (۲۰۱٤). *Roles and responsibilities of cyber intelligence for cyber operations in cyberspace. ۸*, ۳۲۳–۳۳۲. https://doi.org/۱۰,۱٤۲٥۷/ijsia.۲۰۱٤,۸,٥,۲۹

Haataja, S. (۲۰۲۰). Cyber Operations and Collective Countermeasures under International Law. *In Journal of Conflict and Security Law (Vol. ۲٥, Issue ۱, pp. ۳۳–٥۱)*. https://doi.org/۱۰,۱۰۹۳/jcsl/kraa۰۰۳

Maathuis, C. Pieters, W. & van den Berg, J. (۲۰۲۰). Decision support model for effects estimation and proportionality assessment for targeting in cyber operations. Defence Technology.

Smeets, M. (۲۰۲۰). US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection. *Intelligence and National Security, ۳٥(۳), ٤٤٤–٤٥۳.*

Smeets, M. & Work, J. D. (۲۰۲۰). Operational Decision-Making for Cyber Operations. The Cyber Defense Review, ٥(۱), ۹٥-۱۱٤.

TRADOC (U.S. Army Training and Doctrine Command). (۲۰۱٦). *ATP ۳-۹۲ Corps Operations.* April, ۲۷۸.

Williams, B. T. (۲۰۱٤). The Joint Force Commander's Guide to Cyberspace Operations. *Joint Forces Quarterly, ۷۳(۲), ۱۲–۱۹.* http://ndupress.ndu.edu/Portals/٦۸/Documents/jfq/jfq-۷۳/jfq-۷۳_۱۲-۱۹_Williams.pdf?ver=۲۰۱٤-۰٤-۰۱-۱۲۲۱٥٦-

٥٦٣٪٥Cnhttp://ndupress.ndu.edu/Media/News/Article/٥٧٧٤٩٩/jfq-٧٣-the-joint-force-commanders-guide-to-cyberspace-operations/