Management of Defense Human Capital

AJA Imam Ali Military University http://jdhcm.iamu.ac.ir/ ISSN:۲۷۸۳-٤٦٥٤

Discovery and statistics of cyber intelligence indicators in the army of the Islamic Republic of Iran

Hossein Muslimi | Seyed Alireza Motahari ✉۲

۱. Assistant Professor of Command and Staff University, Tehran, Iran, email: moslemi@gmail.com

۲. Corresponding Author ,Doctoral student of Defense Management, Command and Staff University, Tehran, Iran, email: motaharialireza۸٤@gmail.com

Article Info

Article type:

Research Article

Article history:

Received

۲۰۲۴/۰۶/۲۲

Received in revised

۲۰۲٤/۰۸/۱۱

Accepted

۲۰۲۴/۰۹/۱۴

Published online

۲۰۲۴/۰۹/۲۱

Keywords:

Smart army, regional developments, cyber offense and defense.

ABSTRACT

The cyber arena is one of the main pillars of any smart army, which is referred to as the fifth arena of war in reliable sources. Military organizations in the four domains of land, sea, air and space all benefit from cyber capacity for more intelligence, better and more efficient operations. The requirement for a correct decision in the field of cyber intelligent army is to know the indicators of this field for commanders, managers and policy makers. Therefore, the main goal of this research is to discover and calculate the indicators of cyber intelligence in the army of the Islamic Republic of Iran. For this purpose, after reviewing the theoretical research literature, a questionnaire with a ٥-point Likert scale was prepared and given to the statistical community of the research, including ٦٠ experts and specialists in the cyber field. After confirming the validity and reliability, finally, ١٠ indicators in the form of ٣ dimensions have special values above ١, and among these indicators, cyber expert employees and elites of the country were ranked the highest.

Cite this article: Muslimi , H. & Motahari.S. A, , (۲۰۲٤). Discovery and statistics of cyber intelligence indicators in the army of the Islamic Republic of Iranm *Management of Defense Human Capital* , ٥٦ (٤), ٦٤-٨٦.

DOI: http//doi.org/۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰

Publisher: AJA Imam Ali Military University

DOI:

فصلنامه مدیریت سرمایه انسانی دفاعی

ISSN:۲۷۸۳-٤٦٥٤ http://jdhcm.iamu.ac.ir/ دانشگاه افسری امام علی (ع)

کشف و احصاء شاخص های هوشمندسازی سایبری در ارتش جمهوری اسلامی ایران

حسین مسلمی[۱] | سید علیرضا مطهری[۲]✉ |

۱. استادیار دانشگاه فرماندهی و ستاد ، تهران، ایران،رایانامه: moslemi@gmail.com

۲. نویسنده مسئول، دانشجوی دکتری مدیریت دفاعی دانشگاه فرماندهی و ستاد ، تهران، ایران،رایانامه:: motaharialireza۸٤@gmail.com

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی
تاریخ دریافت:
۱۴۰۳/۰۴/۰۳
تاریخ بازنگری:
۱۴۰۳/۰۵/۲۱
تاریخ پذیرش:
۱۴۰۳/۰۶/۱۵
تاریخ انتشار:
۱۴۰۳/۰۶/۳۱
کلیدواژه‌ها:
ارتش هوشمند،تحولات منطقه ای، آفند و پدافند سایبری.

چکیده

عرصه سایبری یکی از ارکان اصلی هر ارتش هوشمند است، که در منابع معتبر از آن به‌عنوان عرصه پنجم جنگ یاد می‌شود. سازمان‌های نظامی در چهار حوزه زمین، دریا، هوا و فضا همگی از ظرفیت سایبری برای هوشمندی بیشتر، انجام بهتر و کاراتر عملیات‌های خود بهره می‌برند. لازمه تصمیم صحیح در زمینه ارتش هوشمند سایبری، شناخت شاخص‌های این حوزه برای فرماندهان، مدیران و سیاست‌گذاران است. لذا هدف اصلی این پژوهش کشف و احصاء شاخص های هوشمند سازی سایبری در ارتش جمهوری اسلامی ایران است. برای این منظور پس از مرور ادبیات نظری تحقیق، پرسشنامه‌ای با طیف ۵ گزینه‌ای لیکرت تهیه و در اختیار جامعه آماری تحقیق شامل تعداد ۶۰ نفر از خبرگان و متخصصین حوزه سایبری قرار گرفت. پس از تایید روایی و پایایی، درنهایت تعداد ۱۰ شاخص در قالب ۳ بعد از مقادیر ویژه بالای ۱ برخوردار و از بین این شاخص‌ها کارکنان متخصص سایبری و نخبگان کشور حائز بالاترین رتبه گردیدند.

استناد: مسلمی ، حسین؛ ، مطهری؛ سید علیرضا (۱۴۰۳). کشف و احصاء شاخص های هوشمندسازی سایبری در ارتش جمهوری اسلامی ایران. *مدیریت سرمایه انسانی دفاعی*، ۱۴ (۲)، ۸۶-۶۴.

DOI: http//doi.org/۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰۰

ناشر: دانشگاه افسری امام علی(ع)

مقدمه

امروزه اغلب کشـــورهای جهان دارای دکترین دفاع ســـایبری بوده و نقش همه بخش‌ها و نهادها و دانشگاه‌ها در آن به‌طور دقیق مشخص شده است. در مواقع بروز بحران‌های سایبری، این بخش‌ها و زیربخش‌ها به‌طور خودکار اقدام به عمل می‌کنند و این مسئله توان بازدارندگی و پیشگیری از وقوع بحران‌های سایبری در حوزه زیرساخت‌های حیاتی کشورها را افزایش می‌دهد. واژه "جنگ سایبری" محصول ورود عرصه سایبر به عرصه‌های نبرد است. در نبرد سایبری اساساً نوع نبرد محتوایی نیست. رویکرد، رویکرد از دسترس خارج کردن سرویس‌ها و از کار انداختن ارائه‌دهندگان خدمات اینترنت و زیر ساخت‌هاست. ایران در زمینه دفاع سایبری از ظرفیت‌های نرم‌افزاری و سخت‌افزاری، بسیار بالایی برخوردار است اما آنچه در آن اندکی ضعف مشاهده می‌شود مسئله هماهنگی و تمرکز در سیاست‌ها و استراتژی‌هاست که نیاز به بازنگری در روند موجود احساس می‌شود.

با توجه به کاربرد گســـترده فضـــای ســـایبری و دیجیتال در عملیات‌های نظامی و انجام برنامه‌های ســـازمان‌های دفاعی، تهدیدهای ســـایبری به یکی از چالش‌های اولویت‌دار کشـــورها تبدیل شده است و قدرت نظامی در حیطه‌ی فضای سایبری دارای اهمیت خاصی شده است (Gehem, et.al, ۲۰۱۵). امروزه قدرت سایبری برای یک سازمان نظامی در تمامی کشورها اهمیت ویژه‌ای دارد با توجه به اینکه چهار حوزه زمین، دریا، هوا و فضـــا همگی از ظرفیت ســـایبری برای هوشـــمندتر شـــدن ارتش و انجام بهتر و کاراتر عملیات‌های خود بهره می‌برند (ربیعی، علی‌یاری، و مردانی‌شـــهربابک، ۱۳۹۹) مواردی مانند قطع جریان برق ۲۱ اســـتان در ونزوئلا از طریق حملات سایبری که مانع چرخش توربین‌ها و تولید برق شد، یا حمله سایبری به کوره فولاد آلمان که مانع قطع به‌موقع جریان تولید حرارت در کوره و درنتیجه انفجار کوره و کشته شدن چند تن از کارگران شد و یا حمله سایبری آمریکا با استفاده از بمب‌های منطقی[۱] به خطوط اصـــلی انتقال گاز روســـیه و درنهایت حمله ســـایبری با ویروس اســـتاکس نت[۲] به تأسیسات غنی‌سازی نطنز ایران همگی مواردی است که در دوره‌های اخیر روی داده و حاکی از قدرت عرصه پنجم درگیری‌های بشری بعد از عرصه‌های زمینی، هوایی، دریایی و فضایی است. ایجاد هرگونه اختلال و یا توقف در کارکرد هریک از زیرســـاخت‌های حیاتی و حســـاس جامعه با

---

[۱] Logic Bombs

[۲] Stuxnet Malware

توجه به وابستگی متقابل زیرساخت‌ها به یکدیگر به‌سرعت به سایر زیرساخت‌ها سرایت کرده و در مدت کوتاهی کارکردهای جامعه را مانند وابستگی به انرژی گاز، برق و خدمات وابسته به آن مانند بهداشت، درمان، آموزش، امور مالی، ارتباطات و حمل‌ونقل را تحت تأثیر مستقیم قرار می‌دهد تا جایی که تداوم ارائه خدمات اجتماعی غیرممکن می‌شود و هر آن باید انتظار وقوع بحران‌های شدید اجتماعی با ابعاد امنیتی را داشت (کافی، ۱۳۹۹). بر همین اساس حملات پیشرفته‌ی سایبری، با ضربه زدن به زیر ساخت‌های حیاتی کشورها، خطرهای جدی را برای اقتصاد و امنیت ملی ایجاد می‌کند. غالباً مهاجمین و بدافزارهای رایانه‌ای همواره یک گام از سیستم‌های دفاع سایبری جلوتر می‌باشند لذا به‌جای انتظار برای مواجهه با تهدیدات و هجمه‌های احتمالی دشمن، باید به دنبال راه‌حل قوی‌تر و هوشمندانه‌تری برای دفاع سایبری باشیم. در هر کشوری باید بر اساس زیرساخت‌های داخلی و ساختار خود، تعریف و رویکرد خاص و متفاوتی از دفاع سایبری فعال داشته باشد. (رادی‌نیا و جباررشیدی، ۱۴۰۱).

یکی از مسائلی که امروزه در ارتش جمهوری اسلامی با آن مواجه هستیم، هوشمند نمودن ارتش برای مقابله با حملات سایبری است که روزانه بر پیچیدگی‌های آن افزوده می‌شود به‌طوری‌که حتی اندیشمندان غربی همچون ریپیک[1] از سال‌ها قبل به این موضوع پرداختند وی معتقد است پیچیدگی و نفوذگران حوزه سایبری، نسبت به گذشته به‌مراتب هوشمندتر و با شناسایی دقیق‌تر حملات خود را انجام می‌دهند (Repik, ۲۰۰۸). لذا بالا بردن قابلیت‌های دفاعی و هوشمند نمودن ارتش در حوزه سایبر نیازمند درک صحیح از متغیرهای اثرگذار قدرت سایبری برای برنامه‌ریزی و تصمیم‌گیری در شرایط مناسب است (شهلایی، ۱۳۹۵).

کشورها با توسعه فنی و استفاده تاکتیکی در زمینه عملیاتی از نیروهای سایبری به‌عنوان متغیر اصلی مداخله‌گر در سراسر چارچوب ارزیابی سایبری، رویکردشان را سازمان‌دهی می‌کنند و درنهایت یک سازمان نظامی را در وضعیت ایجاد قدرت سایبری قرار می‌دهند (قاسمی تادوانی، آذر، سجادی اصیل، ۱۴۰۲). در خصوص اهمیت و ضرورت تحقیق توجه به اهداف حملات سایبری، یعنی کاهش توان بازدارندگی کشورها و آثار مخرب این حملات در مختل نمودن جامعه حائز اهمیت است. لذا سازمان‌های متولی به‌ویژه ارتش هر کشوری باید نسبت به هوشمند سازی خود و ارتقاء توان بازدارندگی تلاش نموده و در این راستا شناسایی شاخص‌های ارتش هوشمند در حوزه سایبری یک ضرورت انکارناپذیر است.

---

[1] Repik

این تحقیق برای پا سخ به پر سش، ارتش هو شمند در حوزه سایبر باید کدام شاخص‌ها را داشته باشد؟ که آن‌ها را تقویت کند تدوین گردیده و فرضیه تحقیق در واقع همان دست یافتن به این شـــاخص‌ها (تحقیقات اکتشـــافی فاقد فرضـــیه‌اند) خواهد بود. در این پژوهش باهدف شناسایی و ارائه شاخص‌های ارتش هوشمند در حوزه سایبر با رویکرد تحلیل عاملی اکتشافی، با بهره‌گیری از روش کتابخانه‌ای، تدوین پر س شنامه و م صاحبه با صاحب‌نظران متخ صص حوزه ســـایبر و فناوری اطلاعات به جمع‌آوری ادبیات مربوطه پرداخته اســـت. لذا با توجه به روش جمع‌آوری داده‌ها و تکمیل گام‌به‌گام اطلاعات، تحقیق از نوع توصـــیفی-پیمایشـــی و با توجه به هدف، از نوع کاربردی و توســـعه‌ای محســـوب می‌گردد، همچنین با توجه به کشـــف ابعاد و مؤلفه‌های ارتش هوشمند در حوزه سایبری، از نوع تحقیقات اکتشافی است.

مبانی نظری و پیشینه‌های پژوهش

کلمه سایبر برای ارجاع به علم سایبرنتیک انتخاب و ا ستفاده شده ا ست. ا صطلاح سایبرنتیک نخ ستین بار در سال ۱۹۴۸ تو سط نوربرت وینر در کتاب کنترل و ارتباط در حیوان و ما شین تعریف شد. ری شه این کلمه فعل یونانی ا ست، که به معنی راندن، رهبر و هدایت کردن ا ست. انجمن علوم دفاعی آمریکا واژه سایبر را برای اتوماسیون دیجیتالی که توسط صنایع پایه وابسته به آن مورداستفاده قرار می‌گیرد به کار می‌برد که شامل سامانه‌های سلاح و برنامه‌های ا ساسی آن‌ها، سامانه فرمان، ارتباطات و واپایش، جا سو سی، نظارت و شنا سایی، تدارکات و نظام‌های منابع انســـانی، تلفن همراه و ارتباط‌دهندگان متحرک و همچنین نظام‌های زیرســـاختی اســـت (ربیعی، علی‌یاری و مردانی شـــهربابک، ۱۳۹۸). در ادامه ضـــمن تعریف برخی از مفاهیم پایه‌ای مهم تحقیق، برخی از ادبیات مورداســـتفاده حوزه ســـایبری مرتبط با تحقیق جهت شـــناســـایی شاخص‌های اولیه و تهیه پرسشنامه برای ارائه به جامعه خبرگان ذکر گردیده است:

حمله سایبری:

اقدامات عمدی برای تغییر، اختلال، فریب، تنزل یا تخریب ســـامانه‌های رایانه‌ای، شـــبکه و یا برنامه‌های مقیم در سیستم‌ها یا شبکه‌ها است.

دفاع سایبری:

توانایی‌های سازمان‌دهی شده برای محافظت در برابر حمله‌ها، کاستن خسارت‌های ناشی از آن‌ها و بازگ شت سریع به و ضعیت عادی در مقابل حمله سایبری ا ست.(EastWest Institute and the Information Security Institute,۲۰۱۱). مرکز برر سی ضمن اعلام حمایت از تمامی گروه‌های مدافع ارزش‌های انسـانی- اسـلامی در حوزه سـایبر، توجه کاربران را به این

نکته جلب می‌نماید که در حوزه سایبری، ایران مانند دیگر حوزه‌ها مورد هجمه بوده و ارتش سایبری با تعریف مردمی آن، در راستای دفاع و نه حمله، شکل گرفته است. نبرد ۸ ماهه سایبری در ایام فتنه خود گویای این هجمه و دفاع جانانه است. اهداف اجرا شده از سوی مرکز بررسی نیز نشان می‌دهد فریب‌خوردگانی به هدایت و پشتیبانی شیطان بزرگ به انجام امور تروریستی در بستر سایبر همت گمارده‌اند و از این خیل تنها راه‌اندازی سایت‌های آموزش بمب‌سازی، هدایت تروریست‌ها در بستر فضای سایبر و ... مشتی نمونه خروار است.

کوتاه سخن این‌که پدیده جنگ سایبری غیرقابل انکار و لزوم ارتش آن نیز بسیار روشن است و در حوزه امنیت ملی هر کشور، تعریف می‌شود. البته مرکز بررسی کاملاً مخالف نگاه استفاده جنگی از عرصه سایبری است. اما آن‌چه امروز در خصوص میهن سرفرازمان مطرح است یک اختلاط معناست. تقریباً واژه‌ی ارتش سایبری پس از مقابله مرکز بررسی جرائم سازمان یافته سایبری سپاه با شبکه‌های سازمان‌یافته و مورد پشتیبانی غرب تحت عنوان پروژه "گرداب" مورد استفاده قرار گرفت. مؤسسه "دیفنس تک" از مؤسسه‌های نظامی و امنیتی ایالات متحده آمریکا، اقدام به انتشار مقاله‌ای با عنوان "ارزیابی ارتش سایبر ایران" نمود. در این مقاله ارتش سایبری ایران زیر مجموعه‌ای از سپاه پاسداران انقلاب اسلامی معرفی شده است. این مؤسسه با توجه به آمار دریافتی از سازمان اطلاعات آمریکا (CIA)، ایران را جزء پنج کشور دارای قوی‌ترین نیروی سایبری معرفی کرد و تعداد نیروهای سایبری سپاه را ۲ هزار و ۴۰۰ نفر به اضافه ۱۲هزار نفر نیروی ذخیره و بودجه این مجموعه از سپاه را ۷۶ میلیون دلار برآورد کرده است! به تازگی نیز روزنامه "تریبون" چاپ فرانسه، ارتش سایبری ایران را ۲۵۰ هزار نفر تخمین زده است(ربیعی، علی‌یاری و مردانی شهربابک، ۱۳۹۸).

ارتش سایبری همان‌گونه که تعریف شد نمایاننده توانمندی عمومی و سازماندهی شده هر کشور برضد اقدام‌های تهاجمی دیگر کشورهاست و تمامی ظرفیت هر کشور در این حوزه ارتش سایبری نامیده می‌شود. البته این تعریف فارغ از تعریف آمریکا از ارتش سایبری است. این نام پر طمطراق، بسیاری از گروه‌های کوچک چند نفره را ترغیب کرد از همین نام استفاده کنند؛ مانند: "ارتش سایبری ایران"، "ارتش آفتاب" و ... که گاهی این ارتش‌ها یک نفره بودند، مثل جریان هک "رادیو زمانه" اگر خاطرتان باشد.

جنگ سایبری:

جنگ سایبری در لغت به معنای تهاجم بر عناصر سایبری است و اصطلاحاً به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سامانه‌های اطلاعاتی باهدف به مخاطره انداختن عناصر اطلاعاتی) اطلاعات، پرو سه‌های مبتنی بر اطلاعات، سامانه‌های اطلاعاتی، شبکه‌های رایانه‌ای(

دشـــمن در فضـــای ســـایبری اســـت (بیات، ۱۳۸۹). بنا به تعریف دیگری به‌نوعی از نبرد اطلاق می‌گردد که طرفین جنگ در آن از رایانه و شـــبکه‌های رایانه‌ای به‌ویژه شـــبکه اینترنت به‌عنوان ابزار استفاده کرده و نبرد را در فضای مجازی جاری می سازند (EastWest Institute and the Information Security Institute,۲۰۱۱). بـــه‌عبـــارت‌دیگر در این جنـــگ تلاش می‌شـــود تا همه‌چیز را درباره دشـــمن بدانیم و درعین‌حال نگذاریم او به نفع «موازنه اطلاعات و دانش» هیچ‌چیزی درباره ما بداند. هدف اصـــلی در جنگ ســـایبری بهره‌گیری از دانش برتر برای برهم زدن «موازنه توان رزمی» به نفع نیروهای خودی اســـت، به‌ویژه اگر ضـــعف تجهیزات و فنّاوری، ســـرمایه و نفرات کمتر باشـــد می‌توان این کمبود را جبران کرده و به پیروزی قاطع دست‌یافت (آذر، ۱۳۹۳).

جنگ سایبری یا جنگ نرم؟

با این همه، نباید جنگ ســـایبری را با تعریف ارائه شـــده از جنگ نرم در عرصـــه ســـایبر اشـــتباه گرفت. این دو، هر یک ویژگی‌های خود را دارند. البته غربی‌ها بر اســـاس پیشـــینه خود همیشـــه تلاش کرده‌اند تا با مفاهیم عام و مترادف، دیگران را از فهم دقیق منظور خود محروم ســـازند اما باید گفت در خصـــوص جنگ نرم با رهبری داهیانه امام خامنه‌ای زید عزه مانند دیگر حوزه‌ها ناکام مانده‌اند.

کوتاه سخن این‌که بودجه‌های مصوب کنگره آمریکا در قالب جنگ نرم با عنوان قانون " صدا"، ۵۵ میلیون دلار، بودجه مصوب مجلس هلند حدود ۱۵ میلیون دلار و این اواخر بودجه ۲۸ و۲۲ میلیون دلاری دیگری از سوی آمریکا، همگی در راستای جنگ نرم با تأکید بر فضای سایبر بوده اســـت. هر چند که امام خامنه‌ای زید عزه در این خصـــوص از مدت‌ها پیش زمانی که همه ما خواب بودیم انذار و هشدار داده‌اند و این فرصت کم، مجال پرداختن به این مطلب نیست(ربیعی، علی‌یاری و مردانی شهربابک، ۱۳۹۸).

مرکز بررسی جرائم سازمان‌یافته در سال ۸۸ پروژه "مرصاد" را به انجام رسانید که متهمان این پروژه با هدایت مستقیم "رادیو فردا"، ارگان رسمی سازمان جاسوسی آمریکا (سیا) اقدام به برنامه‌ریزی برای تولید ۷۰ میلیون فیلترشکن و توزیع آن در بین کاربران ایرانی نمود و متأسفانه تا زمان دســـتگیری مجرمین این پرونده بیش از ۲۰ میلیون فیلترشـــکن توزیع شـــده بود. این مسأله‌ای جدا از دیگر بودجه‌های اشاره شده است. در آخر می‌بایست دو نکته را مد نظر قرار دهیم:

ارتش سایبری مفهومی عام بوده و هیچ ارتباطی با مرکز جرائم سازمان‌یافته ندارد؛ حتی اگر به اشتباه از زبان مسؤولان نظامی صادر شود.

در حوزه سایبری دو آسیب بزرگ وجود دارد:
الف) نشناختن این حوزه؛
ب) شناخت ناصحیح و ناقص این حوزه است که لازم است تمامی دلسوزان در این حوزه تلاش نمایند تا نقایص، برطرف شود(سایت پلیس فتا، ۱۴۰۳).

تئوریزه کردن دفاع سایبری

محمدرضا فرجی پور معاون فناوری اطلاعات و ارتباطات سازمان پدافند غیر عامل فروردین سال ۹۱ در گفت و گو با ایرنا افزود که در حال حاضر سازمان پدافند غیرعامل با برخی از دانشگاه های خارج از تهران نیز به منظور راه اندازی رشته دفاع سایبری مذاکره کرده است و برخی از این دانشگاه ها نیز قرار است در سال آینده در این رشته دانشجو پذیرش کنند. وی خاطرنشان کرد: آشنایی مدیران و فرماندهان با مفاهیم دفاع سایبری یکی از راهبردهای اساسی سازمان پدافند غیرعامل است از این رو از سه سال گذشته برنامه هایی برای افزایش ارایه مفاهیم دفاع سایبری و توانمندسازی مدیران در سطوح مختلف آغاز شده است(جعفری، ۱۳۹۴).

مقابله با حمله‌های سایبری:

عبارت است از به کار گرفتن یک توانایی دفاعی سایبری معین برای منصرف کردن یا تغییر مسیر دادن یک حمله سایبری به‌صورت عامل یا غیرعامل (جعفری، ۱۳۹۴).

عملیات:

اقدام نظامی یا اجرای مأموریت نظامی در حوزه‌های راهبردی، عملیاتی، راهکنشی، خدماتی آموزشی یا اداری (ستاد کل نیروهای مسلح، ۱۳۹۲).

فضای سایبر[1]:

محیط الکترونیکی که از طریق آن اطلاعات تولید، ارسال، دریافت، ذخیره، پردازش و حذف می‌شود (آذر، ۱۳۹۳).

بازدارندگی سایبری[2]:

مکانیزم آشکاری که در بازداشتن از مناقشه سایبری یا فعالیت تهدیدآمیز در فضای سایبری، مؤثر فرض می شود. این مکانیزم‌ها شامل سیاست، موضع‌گیری، سلاح، توانمندی یا هم‌پیمانی است (جعفری، ۱۳۹۴).

---

[1] Cyberspace
[2] Cyber Deterrent

فناوری اطلاعات:

به مجموعه‌ای از دانش، روش‌ها و ابزارها (سخت‌افزار و نرم‌افزار) که به‌منظور تسهیل و انجام فرآیند تولید گردآوری، سازمان‌دهی، ذخیره، بازیابی و نشر اطلاعات با استفاده از رایانه به‌عنوان ابزار پردازش و شبکه به‌عنوان شاهراه ارتباطی به کار گرفته می‌شود فناوری اطلاعات گفته می شود. تعبیر فناوری اطلاعات و ارتباطات بیانگر پویایی منتج از همگرایی سامانه‌های رایانه‌ای و مخابراتی است که تبادل سریع و جهانی اطلاعات را فراهم آورده و ظرفیت متحول سازی فرآیندهای کاری، ارائه خدمات و غیره را دارد (حافظ نیا، ۱۳۹۰).

تاریخچه سایبری در ایران:

پلیس فضای تولید و تبادل اطلاعات ایران یا پلیس سایبری ایران با نام مختصر پلیس فتا، یک واحد تخصصی نیروی انتظامی جمهوری اسلامی ایران است که به‌منظور ایجاد امنیت و کاهش مخاطرات برای فعالیت‌های علمی، اقتصادی، اجتماعی در جامعه اطلاعاتی، حفاظت و صیانت از هویت دینی و ملی، مراقبت و پایش از فضای تولید و تبادل اطلاعات برای پیش‌گیری از تبدیل‌شدن این فضا به بستری برای انجام هماهنگی‌ها و عملیات برای انجام و تحقق فعالیت‌های غیرقانونی و ممانعت از تعرض به ارزش‌ها و هنجارهای جامعه ازجمله وظایف و مأموریت‌های پلیس فضای تولید و تبادل اطلاعات ناجا است (سایت پلیس فتا، ۱۴۰۳).

در راستای پایش و رصد عالمانه، نظام‌مند و مستمر فرصت‌ها و تهدیدات فضای مجازی برای کشور و تدابیر لازم برای مواجهه به‌موقع و مبتکرانه با آن‌ها مرکز ملی فضای مجازی کشور تأسیس گردید (سایت مرکز ملی فضای مجازی کشور، ۱۴۰۳).

ایجاد سامانه پدافند رایانیکی(سایبری) در سطح ملی و ارتقای قدرت رصد، پایش، تشخیص و هشدار دهی، مصون‌سازی و افزایش توان مقابله با پیامدهای ناشی از وقوع احتمالی تهدید با بهره‌گیری از ظرفیت دستگاه‌های استانی و نیروهای مسلح باهدف مصون سازی و یا بی‌اثر سازی این‌گونه تهدیدات بر سرمایه‌های سایبری ملی (سایت مؤسسه افق آینده‌پژوهی راهبردی، ۱۴۰۳). این قرارگاه رسالت مصون سازی و پایدار سازی سامانه‌های سایبری کشور از طریق رصد، پایش، تشخیص تهدیدات، کشف، مدیریت و کنترل آسیب‌پذیری، اعلام هشدارهای لازم، اطمینان از پدافند سایبری، تدوین و انتشار نظامات (ملاحظات، مقررات، الزامات و اصول) پدافندی، آموزش و نهادینه‌سازی پدافند سایبری، مدیریت عملیات پدافند سایبری و دفاع حقوقی در برابر تهدیدات و حملات دشمن را به عهده دارد (سایت پایداری ملی، ۱۴۰۳).

کلازویتس جنگ را این‌گونه تعریف می‌کند :جنگ عمل خشونت باری است که هدفش وادار کردن حریف به اجرای خواسته ماست، جنگ ادامه سیاست است، جنگ نه‌تنها ویژگی نظامی

بلکه خصیصه دیپلماتی، روان‌شناختی و اقتصادی را نیز دارد .دریکی از تعاریف حقوقی از جنگ با رویکرد حقوق بین‌الملل چنین بیان شده است :جنگ عبارت است از درگیری مسلحانه بین دو یا چند کشور با قصد قبولاندن نظرات سیاسی یا اعمال هدف‌های خود با استفاده از تمام وسایلی که برای جنگ در اختیاردارند (ضیایی، ۱۳۷۰).

امروزه یکی از پارادایم‌های حاکم بر جنگ‌ها به‌ویژه جنگ‌های ترکیبی، پارادایم جنگ اطلاعاتی است که شناخت کامل این پارادایم برای نیروهای نظامی و اطلاعاتی مهم است .جنگ اطلاعاتی درواقع بیانگر نهایت استفاده از اطلاعات با استفاده از فن‌آوری‌های پیشرفته چه برای تقویت نیروهای خودی و چه برای تضعیف دشمن است .جنگ اطلاعاتی خود نتیجه انقلاب در امور نظامی است .انقلاب در امور نظامی در اصل به ورود فن‌آوری‌های جدید اطلاعاتی و ارتباطاتی در حوزه‌های نظامی می‌پردازد که آن‌ها هم به‌نوبه خود نقش اساسی‌تری به اطلاعات می‌دهند .تولید سلاح‌های هوشمند و رباتیک، جنگنده‌های رادار گریز، ویروس‌های کامپیوتری و توانایی در ایجاد اختلال در سامانه‌های الکترونیکی و ارتباطاتی، بانک‌های اطلاعاتی، سامانه‌های رایانه‌ای، حمله لیزری به ماهواره‌ها از مصادیق انقلاب در امور نظامی هستند که منجر به ظهور پارادایم جنگ اطلاعاتی شدند.

جنگ سایبر زیرمجموعه‌ای است از جنگ اطلاعاتی که شامل اقداماتی می شود که در دنیای سایبر رخ می‌دهند، دنیای سایبر هرگونه واقعیت مجازی است که توسط مجموعه رایانه‌ها و شبکه‌ها ایجاد می‌شود، در بین دنیای سایبر متعدد و مختلف اینترنت و شبکه‌های مرتبطی که حاوی مطالب چندرسانه‌ای هستند، بیشترین ارتباط را با جنگ سایبر دارند .جنگ سایبری فقط به فضای اینترنت و شبکه‌های کامپیوتری در حال تبادل اطلاعات محدود نمی شود .در جنگ اطلاعاتی بلوغ درنبرد سایبری وقتی اتفاق می‌افتد که با استفاده از سلاح‌های متصل به شبکه‌های کامپیوتری، بدون اینکه لازم باشد در میدان نبرد حضور فیزیکی پیدا کرد، بتوان دشمن را با کمترین خطا مورد هدف قرارداد و نابود کرد .در طول جنگ خلیج‌فارس در سال ۱۹۹۱و در عملیات طوفان صحرا و به‌صورت بارزتر در عملیات آزادسازی عراق در سال ۲۰۰۳ و حمله به طالبان در سال ۲۰۰۱ و حمله ناتو به لیبی، همگان به این واقعیت پی بردند که بسیاری از سلاح‌ها از طریق شبکه‌های کامپیوتری هدایت می‌شوند و حمله موشکی به هدف‌ها بارزترین آن‌ها بود (ماه‌پیشانیان و مرادی، ۱۳۸۹). بسیاری از متخصصین جنگ ترکیبی براین باورند که در آینده نزدیک کامپیوترها صحنه‌های نبرد را به تسخیر خود درخواهند آورد و به‌طور خودکار اطلاعات را مورد ارزشیابی قرار خواهند داد و مبادرت به ضد حمله خواهند نمود. (بهاری، ۱۳۹۸).

رابرت ببر (۲۰۱۷) قدرت سایبری را تشکیل یافته از یک ساختار بومی و متغیرهای نظام‌مند در محیط راهبردی عملیات شامل ابزار های راهبردی، عملیاتی، راهکنشی و فنی می‌داند (Bebber, ۲۰۱۷).

ابعاد جنگ سایبری

در جریان فتنه ۸۸ هم شما شاهد بودید اقدام‌های بسیاری از سوی دشمن برای جلوگیری از ارائه سرویس سایت‌های گفتمان انقلاب صورت گرفت. سایت‌های "فارس"، "لیدر"، "سپاه"، "رجا"، "بسیج"، "گرداب"، "صداوسیما" و ... همگی تحت حمله (DDOS) قرار گرفتند و از مأموریت خود -اطلاع رسانی- بازماندند؛ این نوعی نبرد است. این نوع نبرد طبیعتاً لوازم خود را دارد؛ نیروی انسانی، سخت افزار، نرم افزار و جنگ افزاری متمایز از دیگر جنگ‌ها. این جنگ از ابعاد گوناگونی قابل بررسی است که به برخی از آن‌ها اشاره می‌شود:

با توجه به ورود فضای سایبر به تمامی عرصه‌های زندگی افراد از موضوعات علمی گرفته تا کار، سرگرمی، اقتصاد، آموزش و ارتباطات، در صورتی که مهاجم بتواند سرویس‌های اینترنتی را از کار بیاندازد می‌تواند نارضایتی عمومی ایجاد کند که زمینه‌ساز براندازی نرم است و یا در کار عمومی و روزمره مردم جامعه هدف، اختلال ایجاد کند. افزون بر این چون بسیاری از ارتباطات میان یا درون سازمانی هم اکنون بر بستر اینترنت شکل گرفته است، از کار انداختن سرویس اینترنت خود می‌تواند زمینه ساز آشوب و ناآرامی در کشورها گردد

ویژگی‌های جنگ سایبری:

بهاری (۱۳۹۸) در تحقیق خود به بررسی ویژگی‌های جنگ سایبری پرداخته است. وی معتقد است: جنگ فیزیکی با جنگ سایبری از برخی جهات کاملاً شبیه به هم هستند؛ مثلاً هدف اصلی در جنگ، از هر نوع که می‌خواهد باشد، وارد آوردن ضرر و زیان به دشمن است. انگیزه اصلی در جنگ باید قاعدتاً تصاحب منابع دشمن باشد در حقیقت فلج نمودن دشمن بدون در اختیار گرفتن منابع آن چندان معقول به نظر نمی‌رسد. بهترین روش برای شناخت ویژگی‌های جنگ سایبری این است که تصور و تجسم فیزیکی را از میان برداریم و صرفاً سایبری فکر کنیم. ازجمله ویژگی‌های جنگ‌های سایبری که آن‌ها را از سایر جنگ‌ها متمایز می‌کند می‌توان موارد زیر را نام برد:

- حمله از راه دور:

اولین تفاوت جنگ سایبری با دیگر انواع جنگ‌ها و بالأخص جنگ فیزیکی و حقیقی، قابلیت طراحی، اجرا و نتیجه‌گیری از راه دور است. برای حمله سایبری نیازی به حرکت فیزیکی ندارید و طبیعی است که این تفاوت از منشأ فضای سایبری و حقیقی ناشی می‌گردد.

- دشواری در شناسایی و ردیابی:

به جهت ذات و خ صائص پروتکل‌های ارتباطی، شنا سایی منبع ا صلی حمله د شوار و گاهی ناممکن است .در حقیقت اگر تشریک‌مساعی مرزهای سایبری را نادیده فرض کنیم، شناسایی غیرممکن است .تغییر فیلد آدرس مبدأ و سپس تزریق پکت در شبکه به‌سادگی و حتی تسلط کاربران بسیار مبتدی در اینترنت مقدور است؛ بنابراین مبدأ ناشناس و مبهم خواهد ماند.

- محدودیت در انتقال:

وابستگی فضای سایبر به معدود پروتکل‌های ارتباطی، انتقال و عوامل آن نظیر سرعت، حجم، کیفیت، اعتبار باعث این محدودیت است.

- تهدید ایمنی اطلاعات:

در جنگ سخت، جنبه فیزیکی زندگی انسان تهدید می‌گردد ولی در سایبری، مؤلفه‌های امنیت اطلاعات شامل :صحت، تمامیت، در دسترس بودن و محرمانگی مورد تهدید است.

- اندازه هدف:

بزرگی و کوچکی هدف در جنگ‌های فیزیکی بااهمیت است. ولی در جنگ‌های سایبری، بزرگی عنا صر نسبت به بزرگی حقیقی آن‌ها قابل‌فهم و مقایسه نیست و باید اندازه سایبری آن‌ها را مدنظر دا شت. در جنگ‌های فیزیکی به دنبال تخریب مناطق جغرافیایی بزرگ‌تر هستند، ولی در جنگ سایبری باید اهداف مهم و اساسی را ازنظر سایبری و نقش آن‌ها را مدنظر قرارداد.

- انتشار حمله:

حمله سایبری می‌تواند به‌سادگی از چندین منبع / کانال صورت پذیرد. هدایت و راهبری حمله‌های فیزیکی که از چندین محل آغاز می‌گردند بسیار دشوار است ولی برای حملات سایبری می‌تواند یک ضرورت باشد.

- هزینه کم:

ابزار و عوامل این جنگ سایبری سهل‌الوصول‌تر، آسان‌تر و ارزان‌تر است.

- مسئولیت‌پذیری:

ازآنجایی‌که قوانین مدون و مشـخص بین‌المللی برای مبارزه و ایجاد دعاوی سـایبری وجود ندارد، کشورها به‌سادگی از زیر بار مسئولیت حملات سایبری خود شانه خالی می‌کنند.

- محدودیت در عناصر پایه:

تنها عناصر پایه در یک جنگ سایبری، صفر و یک هستند . البته ذهن انسان را نیز نباید جدا دانست زیرابه هر شکل، فضای سایبری زائیده تفکر و خیال آدمی است و هر کس ذهن بالاتری داشته باشد حاکم این حوزه خواهد بود.

- رهبری آسان:

راهبری و هدایت جنگ سایبری به‌مراتب ساده‌تر از جنگ‌های حقیقی است . گاهی با فشار یک کلید و یا ا شاره به یک شیء سایبری می‌توان آن در موقعیت حمله یا دفاع قرارداد : نیروها را گسترش داد یا عقب‌نشینی نمود.

- بازگشت به نقطه صفر:

وقتی‌که پارادایم عوض می‌شـود بسـیاری از مفاهیم مانند مفهوم مرز، تخریب و قدرت عوض می‌شـود در این فضـا بایسـتی فناوری‌های بزرگ با رقیبان کوچک بجنگید و چه‌بسـا حریفان کوچک بر رقیبان بزرگ فائق آیند(پیروزی پشه‌ها بر فیل‌ها).

- تغییرناپذیری اصول جنگ:

اصول نه‌گانه جنگ در جنگ سایبری هم رعایت می‌شوند و معتبر است.
ازنظر سید مفیدی (۲۰۰۴) محیط فضای سایبر شامل شش حوزه زیر است و شناخت ابعاد و ویژگی‌های این محیط، تحلیل گران و استراتژیست‌های دفاع سایبری را در شناخت نقاط قوت و ضعف جبهه خودی و د شمن و حوزه‌های آ سیب‌پذیر آن یاری خواهد نمود (سید مفیدی، ۲۰۰۴).
بهاری (۱۳۹۸) در تحقیق خود معتقد اسـت برای مقابله با تهدیدات سـایبری باید از سـامانه یکپارچه تهدیدات[1] یا بهره برد این سامانه یکی از روش‌هایی که به‌واسطه آن می‌توان در مقابل تهدیدهای سایبری مقابله کرد به‌کارگیری سخت‌افزار مشخصی است که از آن با نام UTM یاد می شود. این سخت‌افزار غنی « مدیریت یکپارچه تهدیدات » همچون یک سد امنیتی کارا

---

[1] Unified Threat Management (UTM)

تمامی راه‌های نفوذ به سامانه‌های کامپیوتری را مسدود می‌کند و این امکان را به مدیران و کارشناسان شبکه می‌دهد تا بتوانند به‌خوبی در مقابل هرگونه حملات صورت گرفته از جانب نفوذ گران به مقابله بپردازند .در این سخت‌افزار قابل‌استفاده در شبکه‌های کامپیوتری امکاناتی همچون دیوار آتش ، سیستم تشخیص نفوذ، آنتی‌ویروس ، آنتی اسپم و شبکه خصوصی مجازی در دسترس هستند. مدیریت یکپارچه تهدیدات سیستمی است که مکانیزم‌های گوناگون امنیتی را در سطح شبکه فراهم می‌کند و به کمک آن می‌توان به‌صورت یکپارچه سرویس‌های امنیتی مختلفی را ارائه کرد. این دستگاه دربردارنده ویژگی‌ها و خصوصیات مشخصی است که باوجود آن‌ها به‌آسانی می‌توان از بروز بسیاری از تهدیدها جلوگیری نمود.

رمضان‌زاده و همکاران (۱۳۹۹) در تحقیقی با عنوان «ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر بُعد بازدارندگی سایبری» به بررسی مؤلفه‌های ارزیابی قدرت سایبری نیروهای نظامی پرداخته و معتقدند در ارتش جمهوری اسلامی ایران موارد زیر باید به نحو مطلوبی موردتوجه و اجرا قرار گیرد: محافظت و پدافند از شبکه‌ها و سامانه‌های فاوا پایه حیاتی، حساس و مهم، اعمال فرماندهی و کنترل بر کلیه یگان‌های تابعه فرماندهی سایبری ارتش، تعامل فرماندهی سایبری آجا با مبادی لشگری و کشوری مرتبط، بهره‌گیری از فرصت‌های سایبری جهت تقویت قابلیت‌های عملیاتی در عرصه سایبر، توسعه و به‌روزرسانی ابزارها و تسلیحات سایبری، به‌روزرسانی دکترین طرح‌های جامع راهبردی و تاکتیکی سایبری آجا، آینده‌پژوهی و پایش مستمر روندهای حاکم بر فضای سایبری، پشتیبانی عمومی از عملیات مرکب مشترک و یا تک نیرویی، تست کفایت اقدامات و تمهیدات امنیتی فضای سایبر با نگاه امنیت ملی

احمدی (۱۳۹۶) در کتاب مدل‌سازی تهدیدها معتقد است: کارشناسان امنیتی، رعایت ۲۰ نکته امنیتی رایج زیر را که به اصول بیست‌گانه TCSC[1] معروف است

فرزام‌نیا و همکاران (۱۳۹۹) در تحقیقی با عنوان ارائه الگوی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی به تشریح فضای سایبری سازمان‌های دفاعی پرداختند. آن‌ها معتقدند با توجه به نقش و جایگاه سازمان‌های دفاعی و نفوذ روزافزون فضای سایبری و نقش آن در امنیت کشور، باید به مضامین مدیریت استراتژیک سرمایه انسانی، طراحی و پیاده‌سازی چارچوب بومی معماری امنیت سایبری، انعطاف‌پذیری امنیت فضای سایبری، مدیریت ریسک

---

[1] Twenty Critical Security Controls

امنیت فضای سایبری، بازمهندسی ساختار و فراگردهای سازمانی، مدیریت پروژه‌های مرتبط با استانداردها و متدولوژی‌های مناسب و استقرار فرهنگ‌سازمانی تعالی گرا بیشتر توجه نمود.
پس از بررسی ادبیات موجود مرتبط با موضوع تحقیق، کلیه شاخص‌ها در قالب یک پرسشنامه لیکرت ۵ گزینه‌ای در اختیار جامعه خبرگان قرار گرفت و پس از نمرده دهی و اعمال نظرات خبرگان حوزه تحقیق، شاخص‌ها، مؤلفه‌ها و عناصر ارتش هوشمند در حوزه سایبری برابر جدول شماره ۱ استخراج گردید.

جدول (۱) شاخص/عنصر/مؤلفه ارتش هوشمند در حوزه سایبری

ردیف	شاخص/عنصر/مؤلفه	منبع
	زیرساخت هوشمند فیزیکی و نرم‌افزارهای بومی هوشمند	سید مفیدی، ۲۰۰٤ و خبرگان
	تکنولوژی اطلاعات	حافظ نیا، ۱۳۹۰
	واکاوی هوشمند در حوزه سایبر	سایت مرکز ملی فضای مجازی کشور و خبرگان
	سامانه پدافند سایبری	سایت مرکز ملی فضای مجازی کشور و خبرگان
	بروزرسانی آیین‌نامه‌ها در حوزه سایبر و ارزیابی و بازسازی مداوم آسیب‌پذیری‌ها	سایت مرکز ملی فضای مجازی کشور و خبرگان و احمدی، ۱۳۹٦
	ایجاد زیرساختهای ارتباطی مبتنی بر شبکه‌های کامپیوتری	ببر(۲۰۱۷) و خبرگان
	فضای اینترانت بومی و سراسری	ببر(۲۰۱۷) و خبرگان
	راهبری سایبری و مانیتورینگ، نگهداری و انطباق سیستم‌ها	رمضان زاده و همکاران، ۱۳۹۹ و احمدی، ۱۳۹٦
	تجهیزات جنگی بروز در حوزه سایبر	رمضان زاده و همکاران، ۱۳۹۹
	۱- نیروی انسانی متخصص۲- سیستم اطلاعات مدیریتی ۳- راهبران خلاق، ٤-فناوری بروز ۵- شایسته	جامعه خبرگان تحقیق

ردیف	شاخص/عنصر/مؤلفه	منبع
	گزینی و شایسته پروری٦- ساختار و سازمان منعطف ۷- زیرساخت‌های سایبری ، ۸- آموزش و عملیات، ۱۲- انعطاف‌پذیری سامانه‌های سایبری، ۱۳- رعایت اصول سایبری ١٤- یکپارچه‌سازی سامانه‌ها ۱۵- سیستم‌های اعلام‌خطر ١٦- دانش، طرح‌ریزی و ابتکارات عملیات	

نقش شبکه های اجتماعی در جنگ سایبری

جنگ نرم، به دلیل ماهیت خود و عدم نیاز به ابزارهای فیزیکی، به دنبال آن است که در مسافت های دورتری از مراکز طراحی کننده، به اجرا درآید. جهانی و فرامرزی بودن فضای سایبر، امکان های موردنیاز را به آسانی در اختیار طراحان جنگ نرم قرار می دهد و با فراهم شدن بسترهای فکری- فرهنگی اهداف موردنظر، از سوی جریان های درون جامعه هدف دنبال می شود.

میسر بودن ارتباط دو طرفه نیز ابزارهای عملیاتی را در خدمت طراحان و رهبران مراکز موردنظر درمی آورد و در موقعیت های حساس که امکان حضور و هدایت مستقیم میدانی حوادث، از براندازان سلب می شود؛ عناصر حاضر در صحنه نقش رسانه ای عملیات را بازی می کنند. از سوی دیگر، جنگ نرم به عناصر و سربازان میدانی نیاز دارد که از جنس مخاطبان جامعه هدف باشند. این عناصر، باید برای خود هویتی خاص قایل باشند تا بتوانند هدایت روند درگیری را برعهده گیرند و در شرایط کنونی، امکان دسترسی به فضای مجازی به دلیل در اختیار گذاشتن لحظه ای حجم وسیعی از اخبار، اطلاعات و تسهیل ارتباط، چنین هویت کاذبی را به راحتی در میان بخشی از صحنه گردانان حوادث ایجاد می کند. نبود بسیاری قیود و محدودیت ها که برای سایر اقسام رسانه ای وجود دارد، در محیط مجازی، گستره فعالیت در این فضا را برای اهداف و انگیزه های امنیتی و سیاسی در جنگ نرم افزایش می دهد. مجموعه این شرایط است که امروزه، هوس بهره گیری از این فضا را برای غلبه بر دیگر ملت ها، در میان مراکز قدرت جهانی ایجاد می کند. حوادث چند ماه اخیر ایران را باید میدان آزمون برای کاربرد

فضای مجازی در عملیات روانی و جنگ نرم دانست. وبلاگ، فیس بوک، توئیتر، فرند فیدز و بالاترین، از جمله سایت هایی هستند که قابلیت شبکه سازی وسیعی در اینترنت ایجاد کرده اند. در برخی مواقع، این شبکه ها به عنوان سربازان جدید جنگ نرم دول غربی، اقدامات خود را به فضای وقایع جامعه نیز تسری داده و هماهنگی و سازماندهی بسیاری تجمع های سیاسی و اعتراضی را بر ضد دولت هدف، برعهده می گیرند. حوادث پس از انتخابات سال ۱۳۸۸، به روشنی نقش شبکه های اجتماعی مجازی در جنگ نرم غرب با ایران را نشان داد.

۳- روش تحقیق

با جمع‌بندی ادبیات موجود و مطالب تحقیقات داخلی و خارجی، فهرست اولیه‌ای شامل ۲۷ شاخص و مؤلفه ارتش هوشمند در حوزه سایبری تهیه گردید که اعتبار درونی و پایایی آن مورد تأیید قرار گرفت. طی پرسشنامه‌ی ۵ گزینه‌ای طیف لیکرت، این شاخص‌ها در اختیار جامعه خبرگان تحقیق قرار گرفت و پس از حذف موارد تکراری و اعمال اصلاحات مدنظر خبرگان با توجه به جدول اشتراک هر متغیر[۱] در نرم‌افزار SPSS برای حذف عوامل دارای اشتراک ضعیف اقدام گردید. تحلیل عاملی اکتشافی در سه‌گام اصلی انجام گردید:

تفسیر عامل‌هایی که در مرحله‌ی استخراج آغازین تولید می‌شوند، معمولاً مشکل است. چون در این مرحله، امکان این‌که متغیرها با عامل‌هایی که قبلاً استخراج‌شده‌اند، همبستگی بالایی داشته باشد (دارای بار عاملی بالایی باشند)، نادیده گرفته می‌شود که درنتیجه بارهای متقاطع معناداری را سبب می شود، به‌طوری‌که بسیاری از عامل‌ها با بسیاری از متغیرها همبسته‌اند . همین علت باعث می‌شود که تفسیر هر عامل سخت شود، چون عامل‌های مختلف با متغیرهای یکسان نشان داده‌شده‌اند. به‌وسیله‌ی دوران، متغیرهایی که روی یک عامل در نظر گرفته‌شده‌اند، دیگر روی عامل دیگر به کار نمی‌روند. دو نوع دوران وجود دارد: متعامد و اریب. در دوران متعامد (orthogonal) عامل‌ها ناهمبسته و در دوران اریب (oblique) عامل‌ها همبسته در نظر گرفته می‌شوند. آزمون خطی بودن و کفایت نمونه، با ۲ آزمون کرَویَت (Bartlett) و اندازه‌ی کفایت نمونه‌گیری (Kaiser-Meyer-Olkin) تعیین می‌گردد به‌طوری‌که آزمون باتلت (Bartlett) باید بزرگ و معنادار، اندازه Kaiser-Meyer-Olkin بزرگ‌تر از ۶/۰ و سطح معنی‌داری کمتر از ۰،۰۵ باشد. این الزامات برابر جدول زیر در پژوهش برقرار است.

---

[۱] Communalities

جدول (۲) آزمون کفایت آماری و باتلت

KMO and Bartlett's Test		
KMO		.۰,۸۰
Bartlett's Test	Approx. Chi-Square	۱۵۶۳.۶۴۲
	df	۵۹
	Sig.	.۰۰۱

ماتریس مؤلفه‌های تحلیل عاملی قبل و بعد از دوران و همبستگی‌های بین متغیرها نشان‌دهنده عوامل ا ستخراج شده ا ست ولی مؤلفه‌های بعد از دوران دقیق و قابل‌اعتمادتر ا ست برابر جدول زیر سه عامل استخراج‌شده با واریانس کل تعین می‌گردد.

جدول (۳) جدول ماتریس دوران شده(مقادیر ویژه و عوامل استخراج‌شده در ۳ بعد):

Rotated Component Matrixa			
Component			
Modiriat(F۱)	۱	۲	۳
NeeroyEnsani(۲)	.۹۶۳		
Nokhbegan(۳)	.۹۵۷		
MISc(F٤)	.۸۶۲		
ZeerSakht(F٥)	.۷۲۵	.۸۹۰	
Payesh(F٦)		.۸۸۷	
SazmanSakhtar (F۷)		.۸۶۹	
UTM (F۸)		.۸۵۳	
Know(F۹)			.۸۱۱
Hedayat(F۱۰)			.۷۹۶

پژوهش حاضر با توجه به تحلیل عاملی اکتشافی، از نوع اکتشافی و با توجه به روش جمع‌آوری داده‌ها و تکمیل گام‌به‌گام تحقیق از نوع توصیفی-پیمایشی است. نمونه آماری پژوهش تعداد ۶۰ نفر از خبرگان صاحب‌نظر در حوزه مدیریت و فرماندهی، با روش نمونه‌گیری قضاوتی انتخاب شده‌اند. برای محاسبه ضریب قابلیت اعتماد شیوه‌های مختلفی به‌کاربرده می‌شود که از

آن جمله می‌توان به اجرای دوباره (روش بازآزمایی۱)، روش موازی۲ (همتا)، روش تصنیف۳ (دونیمه کردن عبارات پرسشنامه و محاسبه همبستگی نمرات دودسته) و روش کودر - ریچارد سون۴ ا شاره کرد. علاوه بر این، می‌توان قابلیت اعتماد ابزار اندازه‌گیری را با روش آلفای کرونباخ محاسبه نمود. این روش برای محاسبه هماهنگی درونی ابزار اندازه‌گیری ازجمله پرسشنامه‌ها یا آزمون‌هایی که خصیصه‌های مختلف را اندازه‌گیری می‌کند به کار می‌رود. در این‌گونه ابزارها ، پاسخ هر سؤال می‌تواند مقادیر عددی مختلفی را اختیار کند. برای محاسبه ضریب آلفای کرونباخ ابتدا باید واریانس نمره‌های هر زیرمجموعه سؤال‌های پرسشنامه و واریانس کل را محا سبه کرد (سرمد، بازرگان، حجازی، ۱۳۷۹). سپس با ا ستفاده از فرمول زیر مقدار ضریب آلفا را محاسبه کرد.که در این رابطه:

$$ra = \frac{j}{j-1}\left(1 - \frac{\sum S_i^2}{s^2}\right)$$

j = تعداد سؤالات S_i^2 = واریانس تک‌تک سؤالات s^2 = واریانس کل سؤالات

مقدار صفر این ضریب ن شان‌دهنده عدم قابلیت اعتماد و ۱+ ن شان‌دهنده قابلیت اعتماد کامل است در این پژوهش ضریب پایایی پرسشنامه به تفکیک هر یک از مفاهیم کلی و خرده مقیاس‌ها در جدول شماره ۴ ارائه شده است. همان‌طور که در این جدول ملاحظه می‌گردد تمامی مفاهیم سنجیده شده در این پژوهش دارای ضریب آلفای بالای ۰,۷ و بنابراین پایا می‌باشند.

جدول (۴) آزمون پایایی

۱- Test-Retest Method
۲- Equivalent Method
۳- Split-Halves Method
٤- Kuder-Richardson Method

نام ابعاد	تعداد پاسخ‌دهندگان	تعداد سؤالات	ضریب آلفای کرونباخ
کل پرسشنامه	۶۰	۱۸	۰,۹۱
بعد اول	۶۰	۶	۰,۹۱۹
بعد دوم	۶۰	۶	۰,۸۹۱
بعد سوم	۶۰	۶	۰,۹۲۳

میزان آلفای کرونباخ به‌دست‌آمده برای تمامی متغیرهای تحقیق بالاتر از ۰/ ۷ است که نشان‌دهنده پایایی مطلوب پرسشنامه است. لازم به ذکر است که طیف ضریب آلفای کرونباخ بین ۰ تا ۱ است و هر چه این ضریب به یک نزدیک‌تر باشد، نشان‌دهنده پایاتر بودن گویه‌های پرسشنامه است.

نتایج /یافته‌ها و پیشنهادات تحقیق

پس از ارائه مؤلفه‌های استخراج‌شده از ادبیات به خبرگان، موارد کم ارتباط، مشابه و تکراری حذف گردید درنهایت، تعداد ۱۲ شاخص برابر جدول شماره ۴ مورد تأیید قرار گرفت. در پژوهش حاضر شاخص‌های مذکور کشف و شناسایی گردید، لیکن با توجه به محدودیت‌های زمان و موضوع، پیشنهاد می‌گردد که با روش تحلیل عاملی تأیید میزان تأثیر و نوع ارتباط هر شاخص بررسی و بار عاملی هریک مشخص شود. همچنین در صورت امکان می‌توان از سایر نرم‌افزارهای هوش مصنوعی همچون سیستم استنتاج فازی عصبی – تطبیقی (ANFIS) به‌منظور بهره‌برداری بیشتر و ادامه این تحقیق در سطحی به‌مراتب پیشرفته‌تر و وسیع‌تر به ارزیابی شاخص‌ها و حتی پیش‌بینی نتایج آن‌ها در خروجی نهایی تحقیق پرداخت.

جدول (۴) شاخص و مؤلفه‌های ارتش هوشمند در حوزه سایبری

R	شاخص‌ها/ مؤلفه‌ها استخراجی	R	شاخص ها/ مؤلفه ها استخراجی
۱	زیرساخت هوشمند فیزیکی و نرم‌افزارهای بومی هوشمند (F۱)	۲	تکنولوژی اطلاعات (F۲)
۳	واکاوی هوشمند در حوزه سایبر (F۳)	۴	سامانه پدافند سایبری (F٤)
۵	بروزرسانی آیین‌نامه‌ها در حوزه سایبر و ارزیابی و بازسازی مداوم آسیب‌پذیری‌ها (F٥)	۶	ایجاد زیرساخت‌های ارتباطی مبتنی بر شبکه‌های کامپیوتری بومی (F٦)
۷	فضای اینترانت بومی و سراسری (F۷)	۸	راهبری سایبری و مانیتورینگ، نگهداری و انطباق سیستم‌ها (F۸) (UTM)
۹	تجهیزات جنگی بروز در حوزه سایبر (F۹)	۰	نیروی انسانی متخصص و شایسته گزینی (F۱۰)

بحث و بررسی

در تحقیق حاضر، برخی از شاخص‌های خبرگان در سایر تحقیقات که در متن نیز مورد استناد قرارگرفته است، مجدد به‌عنوان شاخص‌های یک ارتش هوشمند در حوزه سایبری مورد تأیید قرار گرفت، لیکن در هیچ‌کدام از تحقیقات بررسی‌شده با محور ارتش هوشمند در حوزه سایبری موردبررسی قرار نگرفته بود. آنچه این تحقیق را حائز توجه و اهمیت می‌کند اعمال‌نظر خبرگان این حوزه منطبق بر ارتش جمهوری اسلامی ایران و شرایط حال حاضر است و به‌نوعی شاخص‌های مدنظر به‌صورت کاملاً بومی استخراج گردیده‌اند. لذا با توجه به شرایط فعلی ارتش به نظر می‌رسد به‌منظور هوشمندسازی ارتش در عرصه سایبر توجه ویژه‌ای باید به ۱۲ شاخص استخراجی مندرج در جدول ۴ باید داشت و از میان این شاخص‌ها بیشترین امتیاز مربوط به ۲

شـاخص کارکنان متخصـص و نخبگان جامعه بوده و برای سـیاسـت‌گذاری و اتخاذ تصـمیمات فرماندهان و مسئولین در خصوص هوشمندسازی حوزه سایبر نیازمند توجه بیشتر است.

مقابله با ایجاد و نشر شایعه های برانداز، نادیده انگاشتن شایعات ضعیف و پاسخ غیرمستقیم به آن، مقابله با شایعه وجود شکاف میان جامعه و حاکمیت، پرهیز از تهدیدانگاری بیش از حد در فعالیت نهادهای غیردولتی و گسـترش آزادی های مدنی در چارچوب قانون اسـاسـی، همراه با هوشـیاری لازم برای اجتناب از تهدیدات احتمالی این نهادها در حوزه های امنیت سـیاسـی و اجتماعی، قانونمند کردن مقابله با جرایم سایبر و تلفن همراه، افزایش تعامل و هم اندیشی میان کارشـناسـان وزارتخانه های اطلاعات، فناوری ارتباطات، قوه قضـائیه، قوه مقننه و پلیس امنیت اجتماعی و اخلاقی ناجا و حمایت تقنینی و مالی، از تعمیق قدرت نرم نظام در محیط‌های مجازی، از جمله راهکارهای مقابله با این تهدیدات است.

مراجع

احمدی مهدی، مدل‌سازی تهدیدها، انتشارات پندار پارس، تهران، ۱۳۹۶ - ، صفحه۲۱۰

آذر، داود، شـناخت تهدیدات فضـای سـایبر و پدافند آن، انتشـارات دافوس آجا، ۱۳۹۳ - ، صفحه۱۰.

آذر، داود، شناخت تهدیدات فضای سایبر و پدافند آن، انتشارات دافوس آجا، ۱۳۹۳ - ، صفحه ۵۴.

بهاری، رحیم، ۱۳۹۸، پایان‌نامه کارشناسی ارشد با موضوع عملیات پایش فضای سایبری ارتش جمهوری اسلامی ایران در جنگ ترکیبی، دانشگاه دافوس آجا.

بیات، محبوبه، سیا ست‌های تهدید و امنیت سایبری، انت شارات مرکز آموزش شهید صیاد شیرازی، چاپ دوم، ۱۳۸۹ - ، صفحه۳۷ .

جعفری، علی‌اصغر، امنیت سایبری و جنگ سایبر، انتشارات پندار پارس، ۱۳۹۴ - ، صفحه ۱۸۷.

جعفری، علی‌اصغر، امنیت سایبری و جنگ سایبر، انتشارات پندار پارس، ۱۳۹۴ ، صفحه۴۱ .

حافظ نیا، محمدر ضا، جغرافیای سیا سی ف ضای مجازی، انت شارات سمت، تهران، ۱۳۹۰ - ، صفحه۲۹ .

رادی نیا، حامد، و جباررشیدی، علی. (۱۴۰۱). آگاهی وضعیتی در دفاع سایبری فعال, راهبردی به‌منظور مقابله با حملات پی شرفته امروزی. کنفرانس ملی فناوری‌های نوین در مهند سی برق و کامپیوتر. SID. https://sid.ir/paper/۹۹٦۰۸۷/fa

ربیعی، بهزاد، علی یاری، شـــهرام، و مردانی شـــهربابک، محمد. (۱۳۹۹). معرفی الگویی برای اندازه‌گیری و ارزیابی قدرت سایبری یک سازمان دفاعی در ج. ا. ایران. راهبرد دفاعی، ۱۸(۶۹)، ۱۳-۳۶. SID. https://sid.ir/paper/٤۰۰٤٦۲/fa

رحیم‌اف، هانی، و موحدی صفت، محمدر ضا. (۱۴۰۱). ارائه الگوی مفهومی ت سلیحات سایبری. مدیریت نظامی، ۲۱(۸۵)، ۱۲۵-۱۵۸. SID. https://sid.ir/paper/۱۰٤۰۰۱۰/fa

رم ضان زاده، مجتبی، غیوری ثالث، مجید، احمدوند، علی‌محمد، آقایی، مح سن، و نظری فرخی، ابراهیم. (۱۳۹۹). ارائه مدل مفهومی ارزیابی قدرت ســـایبری نیروهای مســـلح با تأکید بر بعد بـــازدارنـــدگـــی ســـــایـــبـــری. مـــدیـــریـــت نـــظـــامـــی، ۲۰(۷۸)، ۶۱-۹۲. SID. https://sid.ir/paper/۳۸٦۲٦۲/fa

سایت پایداری ملی به آدرس: https://paydarymelli.ir/fa/news/٤۲۹۱٥

سایت پلیس فتا، ۱۴۰۳، http://www.cyberpolice.ir/abouts

ســـــایـــت مـــرکـــز مـــلـــی فضـــــای مـــجـــازی کشـــــور، ۱۴۰۳، http://www.rooznamehrasmi.ir/laws/ShowLaw.aspx?Code=۲۹۸-

سایت مؤسسه افق آینده‌پژوهی راهبردی به آدرس: http://www.iran-futures.org

ســـتاد کل نیروهای مســـلح، فرهنگ واژه‌های نظامی، دفتر واژه‌گزینی نظامی، روناس، تهران، - ۱۳۹۲ ، صفحه ۱۸۱.

سید مفیدی، کاوه، سکیورتارگت(فضای سایبری)، نسخه خلاصه شده جنگ سایبری، - ۲۰۰۴.

ضیایی بیگدلی، محمدرضا، انتشارات دانشگاه علامه طباطبایی، تهران، - ، «حقوق جنگ » ، ۱۳۷۳، صفحه۴۵ .

فرزام نیا، نیما، عبدی، بهنام، و رضائیان، علی. (۱۳۹۹). ارائه الگوی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی. مدیریت نظامی، ۲۰(۷۷)، ۸۱-۱۲۰. SID. https://sid.ir/paper/۳۸۵۷۷۵/fa

قاسمی تادوانی، محمد، آذر، داود، سجادی اصیل، وحید (۱۴۰۲)، الگوی ارزیابی قدرت آفند سایبری ارتش جمهوری اسلامی ایران، مجله علمی پژوهشی علوم و فنون نظامی.

کافی، سعید. (۱۳۹۹). شاخص‌های دفاعی امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران مبتنی بر رویکردهای پدافند غیرعامل. سیاست دفاعی، ۲۸(۱۱۱)، ۰-۰. SID. https://sid.ir/paper/۵۲۵۹٤۱/fa

ماه‌پیشانیان، مهسا، حجت اله مرادی، گفتمان جنگ مجازی و رسانه‌های گروهی، در قدرت و جنگ نرم :از نظریه تا عمل، انتشارات ساقی، تهران، ۱۳۸۹، ص ۴۰۰.

نصرت‌آبادی، جمشید، لشکریان، حمیدرضا، مردانی شهربابک، محمد، و موحدی صفت، محمدرضا. (۱۳۹۸). ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران. امنیت ملی، ۹(۳۱)، ۱۷۳-۱۹۸. SID. https://sid.ir/paper/۵۲۲۵۱۷/fa

Bebber, Robert, (۲۰۱۷), Cyber power and cyber effectiveness: An analytic framework, ***Comparative Strategy***, ۳٦:٥.

EastWest Institute and the Information Security Institute of Moscow State University, ۲۰۱۱,p۳٤.

EastWest Institute and the Information Security Institute of Moscow State University, ۲۰۱۱,p۳۷.

Gehem, Maarten, Artur Usanov, Erik Frinking, Michel Rademaker, (۲۰۱٥), ASSESSING CYBER SECURITY: A META-ANALYSIS OF THREATS, TRENDS, AND RESPONSES TO CYBER ATTACKS, The Hague Centre for

Repik. K. A., "Defeating adversary network intelligence efforts with active cyber defense techniques," ۲۰۰۸ Strategic Studies.