Supreme National Defense University Quarterly Journal of Strategic Management Research in National Defense

https://issk.sndu.ac.ir E-ISSN: 2980-8219

Vol. 9, No. 3, Issue. 35, Autumn 2025 **Received:** 2023/06/30 **Accepted:** 2023/12/09

Research paper

A Conceptual Framework for Classifying Cyber Space Threats and Opportunities

Nader Rashvand
PhD in Information Technology Management (Corresponding Author).
Email: navidrashvand20@gmail.com
Omid Ardalan
PhD in Management, Faculty Member, University of Command and Staff, AJA, Tehran, Iran

Abstract

Today, cyberspace has emerged as a novel domain in defense and security arenas. In Iran, following global trends, cyberspace is officially recognized as a domain akin to land, sea, air, and space, for which operational and strategic organizations are designated. In such a domain, the simultaneous expansion of heterogeneous network connections and diverse organizational services has increased vulnerabilities and security threats in cyberspace. The present study aims to propose a framework for classifying threats and opportunities in cyberspace. This research is developmental-applied in nature, based on the objectives and type of investigation, and employs a mixed-method approach (qualitative and quantitative). The statistical population comprises 140 university experts, cyberspace specialists, and strategic and operational commanders of the armed forces. Data collection was conducted using a five-point Likert scale questionnaire. The validity of the study was confirmed, and reliability was calculated using Cronbach's alpha (0.95). Findings indicate that cyberspace threats and opportunities can be classified into three layers: cognitive, informational, and physical.

Keywords: Model, Cyberspace, Threats, Opportunities

فصلنامه مطالعات مدیریت راهبردی دفاع ملی
سال نهم، شماره سوم (پیاپی ۳۵)، پاییز ۱۴۰۴، صص. ۲۶۷-۳۰۲
تاریخ دریافت: ۱۴۰۲/۰۴/۰۹ ـ تاریخ پذیرش: ۱۴۰۲/۰۹/۱۸
مقاله پژوهشی

ارائه الگوی طبقه‌بندی تهدیدات و فرصت‌های فضای سایبر

نادر رشوند
دکترا تخصصی مدیریت فناوری اطلاعات (نویسنده مسئول)
Email: navidrashvand20@gmail.com
امید اردلان
دکترا تخصصی مدیریت، عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا، تهران، ایران

چکیده
امروزه فضای سایبر به‌عنوان قلمروِ جدید و عرصه‌ای نوظهور در حوزه‌های دفاعی و امنیتی نمود و ظهور کرده است. در کشور ما به تبعیت از سایر کشورهای جهان فضای سایبری به‌عنوان قلمرو یا عرصه نظامی به رسمیت شناخته شده است که در نتیجه آن، فضای سایبر در کنار زمین، دریا، هوا و فضا سازمان‌دِهی و برای آن سازمان رزم در نظر گرفته شده است. در چنین فضایی، توسعه زیرساخت‌های ارتباطی و اتصال شبکه‌های ناهمگون با گسترش هم‌زمان خدمات مفید و متنوع در سطح سازمان‌های ن.م در کنار ساختار درهم‌تنیده آن‌ها باعث افزایش آسیب‌پذیری‌ها و تهدیدات امنیتی در فضای سایبر شده است. تحقیق حاضر با اذعان به موضوع فوق با هدف ارائه الگوی طبقه‌بندی تهدیدات و فرصت‌های فضای سایبر به رشته تحریر در آمده است. این تحقیق بر مبنای هدف و ماهیت تحقیق از نوع توسعه‌ای- کاربردی و با رویکرد آمیخته (کیفی و کمی) است. جامعهٔ آماری تحقیق، تعداد ۱۴۰ نفر از صاحب‌نظران دانشگاهی و خبرگان آشنا به فضای سایبر و فرماندهان راهبردی و عملیاتی نیروهای مسلح هستند. برای پاسخ به سؤال‌های پژوهش از ابزار پرسش‌نامه با طیف ۵ گزینه‌ای لیکرت استفاده شده است. روایی تحقیق از طریق دو ابزار، تأیید و پایایی نیز با استفاده از آزمون آلفای کرونباخ ۰/۹۵ محاسبه شد. نتایج حاکی از آن است که تهدیدات و فرصت‌های فضای سایبر را می‌توان در سه لایه شناختی، اطلاعاتی و فیزیکی طبقه‌بندی کرد.

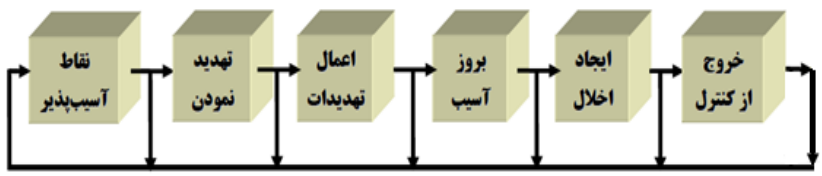
کلیدواژه‌ها: مدل، فضای سایبر، تهدیدات، فرصت‌ها

مقدمه

امروزه بخش قابل توجهی از فعالیت‌ها و تعاملات سازمان‌های مختلف در فضای سایبر انجام می‌شود. هرچند فضای سایبر مزایای زیادی برای سازمان‌های مورد نظر در بسیاری از حوزه‌ها به دنبال داشته است ولی به دلایلی ازجمله، نامتعارف بودن ساختار، رشد سریع و نامتوازن این شبکه‌های ناهمگون و به‌هم‌پیوسته، آسیب‌پذیری‌ها، تهدیدهای متنوع و ... می‌تواند باعث ایجاد چالش‌ها و اختلالاتی در روند اجرای مأموریت‌های این سازمان‌ها و حتی تهدید برای امنیت ملی کشور شود (قربان‌نیا، ۱۳۹۴).

ماهیت، محتوا، چیستی و چرایی تهدیدات، روندها، روال‌ها و فرایند شکل‌گیری آن‌ها، عوامل زمینه‌ساز در پیدایششان، چگونگی اعمال آن‌ها، چگونگی سنجش و احصای آن‌ها، روش‌های پیشگیری، نحوه انجام اقدامات پیشگیرانه یا مقابله با انواع تهدیدات در عرصه‌ها و حوزه‌های مختلف، موضوعاتی بسیار مهم و با ارزش است که به قدمت عمر بشری، سابقه داشته و در اعصار و عرصه‌ها مختلف، مورد توجه بشر بوده و وی همواره سعی نموده تا به شیوه‌های مختلف و متناسب با محیط، موقعیت، ابزار و امکانات در اختیار، پس از شناسایی آن‌ها با روش‌هایی مناسب به مقابله با آن‌ها بپردازد (جواهری، ۱۳۹۸).

روند و فرایند شکل‌گیری تهدیدات، موضوعی بسیار مهم و با اهمیت بوده و لازم است، روال شروع، توسعه، افزایش و چگونگی اعمال تهدیدات و همچنین آسیب‌های وارده بر سامانه‌ها و مجموعه‌ها، در عرصه‌های مختلف، با دقت مورد بررسی و شناسایی قرار گرفته و متناسب با فرایند فوق، اقدامات پیشگیرانه یا مقابله‌ای با تهدیدات مورد نظر انجام شوند. بنابراین روند شکل‌گیری تهدیدات در عرصه‌های مختلف و به‌طورکلی در قالب شکل زیر ارائه شده است.



شکل ۱: فرایند و نحوه شکل‌گیری تهدیدات در فضای سایبر (وظیفه‌دان، ۱۳۹۵)

برای ارتقای امنیت، زیرساخت‌های سایبری در سطح سازمان‌های مورد نظر، درک، تحلیل و شناخت تهدیدات علیه این زیرساخت‌ها دارای اهمیتی ویژه بوده و باعث تداوم و استمرار انجام مأموریت‌ها و ارائه خدمات در سطوح مختلف می‌گردد. بر این اساس شناسایی و روش درست اندیشیدن در مورد تهدیدات سایبری جهت جلوگیری از خطا در تشخیص و ارائه راهکارهای مواجهه با آن‌ها، همچنین شناسایی طبقه‌بندی‌ها و عوامل تأثیرگذار بر آن‌ها می‌تواند ضمن ارتقای دانش و آگاهی در این عرصه، عاملی برای توسعه قدرت تصمیم‌سازی و تصمیم‌گیری راهبردی باشد. به‌منظور شناسایی این منطق در قالب توصیفی که فهم اجزا و ارتباط آن‌ها را ارائه دهد، می‌توان اقدام به انتخاب و ارائه مدلی برای طبقه‌بندی تهدیدات نمود تا ارتباط منطقی جنبه‌های مختلف در روند شناسایی تهدیدات سایبری در حیطه سازمان‌های ن.م مشخص شوند. ازهمین‌رو در خصوص اهمیت تحقیق می‌توان بیان کرد که:

۱. تهدید در یک دیدگاه، عاملی است که قابلیت ایجاد آسیب را داراست؛ پس تا زمانی که شناختی از تهدیدات و برآوردی از آسیب‌پذیری حاصل نگردد، تدوین راهبردها، اثرگذاری مطلوب و بهینه خود را در قلمروِ تحقیق به جای نمی‌گذارد.
۲. درصورتی‌که عوامل اثرگذار در فضای سایبر به‌خوبی شناسایی و تحلیل نگردند، چه‌بسا یک عامل به تهدید یا آسیب تبدیل و در نهایت به بحران ختم شود که در آن صورت هزینه مدیریت و مقابله با آن تهدید یا آسیب چند برابر خواهد شد.

همچنین در خصوص پیامدهای عدم انجام این تحقیق (ضرورت) می‌توان بیان کرد:

۱. ضعف در پیش‌بینی و شناخت تهدیدات و کاهش کنترل امنیت سایبری در سازمان‌ها؛
۲. کاهش توانمندی در پاسخ‌گویی به نیازهای امنیت سایبری در سازمان‌ها و تحمیل هزینه به آن‌ها؛
۳. افزایش میزان خسارات اقدامات تهدیدآمیز سایبری در صورت عدم به‌کارگیری دستاوردهای ناشی از شناسایی و طبقه‌بندی تهدیدات.

بنابراین می‌توان بیان کرد که پژوهش حاضر با هدف ارائه الگوی طبقه‌بندی تهدیدات و فرصت‌های فضای سایبر درصدد است تا از طریق شناسایی عوامل و مؤلفه‌های مؤثر بر فضای

سایبر سازمان‌های ن.م به طبقه‌بندی تهدیدات و فرصت‌های فضای سایبر بپردازد و به سؤالات زیر پاسخ دهد:

۱. مصادیق تهدیدات مربوط به لایه‌های سه‌گانه الگوی طبقه‌بندی (فیزیکی، اطلاعاتی و شناختی) کدامند؟

۲. مصادیق فرصت‌های مربوط به لایه‌های سه‌گانه الگوی طبقه‌بندی (فیزیکی، اطلاعاتی و شناختی) کدامند؟

۱. پیشینه پژوهش

برخی از پیشینه‌های مرتبط با پژوهش در جدول ذیل ارائه شده‌اند:

جدول ۱: پیشینه پژوهش

نام طبقه‌بندی	تعداد رده		عناوین رده فوقانی	توسعه دهنده	سال توسعه	توضیحات (مفاهیم مستخرجه)
	حداکثر	حداقل				
طبقه‌بندی تهدید سایبری AVOIDIT	۵	۲	۱. بردار حمله ۲. تأثیر عملیاتی ۳. تأثیر اطلاعاتی ۴. دفاع ۵. هدف	دانشگاه ممفیس (آمریکا)	۲۰۰۹	ارائه ابزاری برای طبقه‌بندی آسیب‌پذیری‌ها؛ توصیف ماهیت حمله ترکیبی؛ اتخاذ روش‌های دفاعی؛ معرفی اهداف مورد حمله
طبقه‌بندی خطرهای امنیتی سایبر عملیاتی	۳	۳	۱. اقدامات افراد ۲. خرابی‌ها در سامانه‌ها و فناوری‌ها ۴. فرایندهای داخلی شکست‌خورده ۵. رویدادهای خارجی	دانشگاه کارنگی ملون (آمریکا)	۲۰۱۰	توصیف خطرهای امنیت سایبری عملیاتی (خطرهای عملیاتی مربوط به دارایی و فناوری اطلاعات)؛ ارائه ابزاری برای شناسایی کلیه خطرهای مذکور.
نمونه تهدیدی ارزیابی خطر NIST	۳	۲	۱. خصمانه ۲. غیرخصمانه	NIST (آمریکا)	۲۰۱۲	تهدیدات مربوط به منبع و رویدادی برای تحلیل یک تهدید؛ کمک به ارزیابی رویدادهای تهدید با استفاده از فرایند مدیریت خطر

نام طبقه‌بندی	تعداد رده		عناوین رده فوقانی	توسعه دهنده	سال توسعه	توضیحات (مفاهیم مستخرجه)
	حداکثر	حداقل				
طبقه‌بندی تهدید CNI	۵	۲	۱. آفندی ۲. پدافندی	نیروی هوایی کانادا (CAF)	۲۰۱۳	دسته‌بندی اقدامات مبتنی بر دیدگاه‌های نظامی؛ استفاده از ادبیات جهانی و طبقه‌بندی MACE
طبقه‌بندی درگیری سایبری	۴	۲	۱. گروه‌ها ۲. موضوعات	دانشگاه جورج میسون (آمریکا)	۲۰۱۳	توصیف رویدادهای درگیری و بازیگران درگیر در آن؛ تقسیم طبقه‌بندی به دو حوزه گروه‌ها (شامل اقدام و بازیگر) برای اعمال به موضوعات و موضوعات (شامل رویدادها مثل دستکاری داده و موجودیت‌ها مثل افراد و ...)
طبقه‌بندی فعالیت‌های نظامی و اثرات سایبری (MACE)	۳	۲	۱. انواع حمله ۲. سطوح دسترسی ۳. بردارهای حمله ۴. انواع مهاجمین ۵. اثرات سایبری ۶. فعالیت‌های نظامی	سازمان پژوهش و توسعه دفاعی کانادا (DRDC)	۲۰۱۳	مبنایی برای الگوسازی، شبیه‌سازی و آزمون حملات سایبری؛ توصیف پیوند میان فعالیت‌های نظامی در زمینه سایبری با ارائه جزئیات مورد نیاز برای توسعه سناریوهای آزمون و تمرین‌های مرتبط با سایبر (نظیر انواع حمله، سطوح دسترسی و ...)
طبقه‌بندی حمله تجدیدنظر شده	۲	۲	۱. هدف حمله ۲. قابلیت آشکارسازی حمله ۳. لایه ISO /OSI ۴. نوع هدف ۵. موقعیت مکانی موضوع حمله ۶. حوزه حمله شده ۷. بازخورد ۸. شرایط اولیه اجزای حمله ۹. نوع تأثیر	دانشگاه مونیخ (آلمان)	۲۰۱۴	توصیف حملات هوشمند؛ کمک به غلبه بر نقص نظامات دسته‌بندی‌های موجود در برابر حملات جدید.

نام طبقه‌بندی	تعداد رده		عناوین رده فوقانی	توسعه دهنده	سال توسعه	توضیحات (مفاهیم مستخرجه)
	حداکثر	حداقل				
			۱۰. خودکارسازی حمله ۱۱. موجودیت‌های حمله (شده) ۱۱. مقدار اتصال ۱۳. عمق حمله ۱۴. قابلیت انتساب ۱۵. نوع پیاده‌سازی ۱۶. تراکم حمله			
طبقه‌بندی تهدید باز (OTT)	۲	۲	۱. تهدیدات فیزیکی ۲. تهدیدات علیه منابع ۳. تهدیدات مربوط به کارکنان ۴. تهدیدات فنی	Enclave Security (فنلاند)	۲۰۱۵	توصیف اطلاعات تهدیدات؛ اولویت‌بندی رتبه‌های هر اقدام (۵ بالاترین و ۱ پایین‌ترین اولویت)
طبقه‌بندی تهدید ENISA	۵	۲	۱. حمله فیزیکی ۲. حوادث طبیعی ۳. استراق سمع، شنود، ربایش ۴. وقفه ۵. خرابی‌ها- نقص ۶. خسارات غیرعمدی (سهوی) ۷. فعالیت نامناسب- سوءاستفاده ۸. خسارات- از دست دادن (دارایی IT)	ENISA (اروپا)	۲۰۱۶	توصیف تهدیدات مربوط به دارایی ICT
شمارش و دسته‌بندی الگوی حمله مشترک (CAPEC)	-	-	سازمان‌دهی الگوهای حمله همچون فیشینگ، تقسیم پاسخ HTTP، تزریق SQL، بازگشایی رمز عبور جدول	MITRE (آمریکا)	۲۰۱۷	راه‌های انجام یک حمله؛ نگاشت یک حمله بر الگو(ها)ی حمله مرتبط.

نام طبقه‌بندی	تعداد رده		عناوین رده فوقانی	توسعه دهنده	سال توسعه	توضیحات (مفاهیم مستخرجه)
	حداکثر	حداقل				
			رنگین‌کمان و ... براساس حوزه حمله (مثلاً: مهندسی اجتماعی، زنجیره تأمین، ارتباطات، نرم‌افزار، امنیت فیزیکی و سخت‌افزار)			

۲. مبانی نظری

تهدید: مفهومی کلی و انتزاعی است و معانی و تعاریف مختلفی برای آن بیان شده است. از دیدگاه سازمان پدافند غیرعامل کشور، تهدید سایبری مبینِ «هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به مأموریت‌ها وظایف، تصویر (پنداره) یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا کارکنان دستگاه به‌واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام (تخریب)، افشا، تغییر اطلاعات یا ممانعت از ایجاد اختلال در ارائه خدمت» تعریف شده است (سند راهبردی پدافند سایبری کشور،۱۳۹۴).

از دیدگاه موسسه ملی استاندارد و فناوری (NIST) آمریکا تهدید عبارت از: «هر موقعیت یا رویدادی همراه با ظرفیت تأثیر خصمانه بر روی عملیات و دارایی‌های سازمان (خودی)، افراد، سازمان‌ها و کشور دیگر از طریق یک سامانه اطلاعاتی با دسترسی غیرمجاز، خرابی، افشا یا تغییر اطلاعات و یا جلوگیری از ارائه خدمت است. هر تهدید از دو جنبه مورد توجه قرار می‌گیرد: «الف. منابع تهدید[1] و ب. رویدادهای تهدید[2]» (سند ملی استاندارد و فناوری، ۱۳۹۸).

آسیب‌پذیری: از دیدگاه سند راهبردی پدافند سایبری کشور آسیب‌پذیری به ضعف موجود در داخل یک سرمایه، رویه‌های امنیتی یا کنترل‌های داخلی یا پیاده‌سازی آن سرمایه ملی

1. Threat Sources
2. Threat Events

سایبری که قابلیت بهره‌برداری یا فعال شدن توسط تهدیدات داخلی و خارجی به‌منظور انجام جنگ سایبری را داشته باشد، تعریف می‌شود (سند راهبردی پدافند سایبری کشور،۱۳۹۴).

از دیدگاه فرهنگ‌نامه سایبری ن.م منشأ آسیب‌پذیری‌های سایبری در سرمایه ملی سایبری، ضعف پیاده‌سازی (تولید) سرمایه ملی سایبری، ضعف تنظیمات و بهره‌برداری از سرمایه ملی سایبری مورد نظر است (فرهنگ‌نامه سایبری نیروهای مسلح، ۱۳۹۹).

فضای سایبری: از دیدگاه سند راهبردی پدافند سایبری کشور، فضای سایبری شبکه‌های وابسته به یکدیگر، از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه شده (جاگذاری شده)، کنترل‌گرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات است. این فضا، ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد (سند راهبردی پدافند سایبری کشور،۱۳۹۴).

از دیدگاه فرهنگ‌نامه سایبری ن.م فضای سایبر دامنه‌ای است مشتمل بر فضای مجازی، فناوری‌های اطلاعاتی و ارتباطی، محصولات، رسانه‌ها، تسلیحات و تجهیزات الکترونیکی و الکترونیک‌پایه که برای ارتقای عملکرد و کارایی و هوشمندسازی اجزای عملیاتی و صحنه عملیات و همچنین تغییر در ذهن به‌کار می‌رود (فرهنگ‌نامه سایبری نیروهای مسلح، ۱۳۹۹).

طبقه‌بندی تهدیدات سایبری: طبقه‌بندی تهدیدات سایبری با هدف تعیین حوزه‌ها و حیطه‌های کارکردی هر یک از دسته‌های تهدید و در راستای دستیابی به اهداف کلیدی و مؤثر شناسایی، بررسی و احصای تهدیدات سایبری، انجام می‌شود. رویکردهای دسته‌بندی کلان تهدیدات از دو منظر زیر قابل توجه است:

الف. ماهیت‌شناسی که غایت و اساس پدیده‌ها را مورد بررسی قرار می‌دهد.

ب. معرفت‌شناسی که برای تعیین ارتباطات بین پدیده‌ها و تعیین چگونگی ارتباطات آن‌ها، مورد بررسی قرار می‌گیرند. می‌توان برای شناخت، بررسی و دسته‌بندی تهدیدات از دو دیدگاه فوق به‌صورت هم‌زمان استفاده کرد.

دسته‌بندی تهدیدات در فضای واقعی زندگی فردی و اجتماعی بشر، از نگاه و دیدگاه متخصصین و خبرگان این حوزه، معمولاً شامل هشت دسته است. این دسته‌ها شامل: تهدیدات فرهنگی و مذهبی، تهدیدات اجتماعی، تهدیدات سیاسی، تهدیدات اقتصادی، تهدیدات اطلاعاتی و امنیتی، تهدیدات نظامی و دفاعی، تهدیدات فناورانه و تهدیدات زیست‌محیطی تقسیم‌بندی می‌شوند و برخی از متخصصین حوزه‌های تهدیدشناسی در فضای واقعی، تعدادی از حوزه‌های تهدید فوق را با ادغام و تلفیق در هم، آن را بیشتر از این حوزه‌ها تقسیم‌بندی می‌کنند. جدول (۲)، دسته‌های کلان تهدید را به همراه شاخص‌های آن‌ها ارائه می‌دهد.

جدول ۲: دسته‌های کلان تهدیدات سایبری (واحدی، ۱۳۹۸)

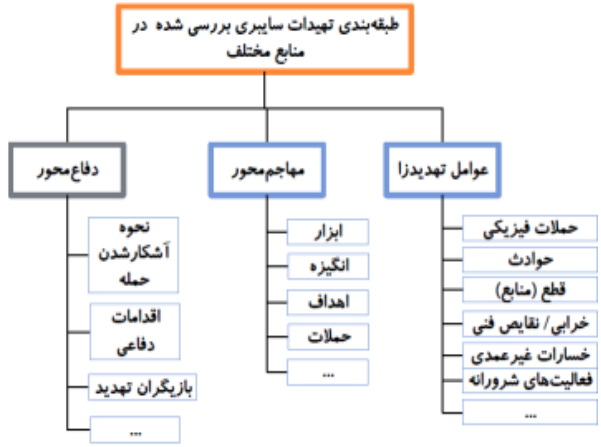
ردیف	دسته کلان تهدید	نوع تهدید	شاخص/ مصداق
۱	فرهنگی- مذهبی	تهاجم فرهنگی	تغییر سبک زندگی از برق شبکه‌های مجازی
		جریان‌سازی	آموزش برنامه‌های براندازی
۲	اجتماعی	مهندسی اجتماعی	فریب افراد به‌صورت ناخواسته
		نشر شایعات	جعل اخبار و تکرار آن در شبکه‌های اجتماعی
۳	سیاسی	آموزش و هدایت	ایجاد بدبینی در جامعه از طریق فضای مجازی
		تشویش اذهان عمومی	مشوش کردن اذهان و بمباران اطلاعاتی جامعه
۴	اقتصادی	ناامن‌سازی فضای اقتصادی جامعه	ایجاد ناامنی اقتصادی در جامعه از طریق فضای مجازی
		سرقت پول	سرقت از حساب‌های بانکی
۵	اطلاعاتی- امنیتی	جمع‌آوری اطلاعات	کسب اطلاعات از مراکز حیاتی
		هدایت و جذب منابع انسانی	جذب کارمندان ناراضی برای انجام خرابکاری
۶	نظامی-دفاعی	ردیابی و مکان‌یابی افراد	پایش مداوم برای انجام ترور افراد برجسته

ردیف	دسته کلان تهدید	نوع تهدید	شاخص/ مصداق
		خاص و وسایل نقلیه	
		حمله به سامانه‌های دفاعی	حمله به مراکز حیاتی نظامی
۷	فناورانه	افشـــا	افشای اطلاعات از طریق دسترسی غیرمجاز افشای اطلاعات از طریق شنود تشعشعات
		تخریب	تخریب زیرساخت فیزیکی سایبری از طریق بمب و انفجار تخریب زیرساخت فیزیکی از طریق عامل نرم‌افزاری (بدافزار)
		از دست رفتن	از دست رفتن اطلاعات از طریق سرقت از دست دادن اعتبار
		اختلال	اختلال در زیرساخت سایبری از طریق دسترسی فیزیکی غیرمجاز اختلال در عملکردهای شبکه و دسترسی به اطلاعات یا خدمات از طریق تغییر پیکربندی
۸	زیست‌محیطی	حوادث طبیعی	آسیب به زیرساخت‌های فاوایی در اثر وقوع سیل
		حوادث انسانی	آسیب به زیرساخت‌های فاوایی در اثر وقوع آتش‌سوزی

معمولاً اکثر طبقه‌بندی‌های تهدید سایبری در منابع موجود، «مهاجم‌محور»[1] هستند؛ زیرا حملات را از منظر ابزارهای مهاجم، انگیزه‌ها و اهداف وی دسته‌بندی می‌کنند. هرچند، تلاش‌هایی برای توسعه طبقه‌بندی‌های «دفاع‌محور»[2] براساس نحوه آشکار شدن یک حمله در سامانه هدف صورت گرفته است؛ حتی برخی طبقه‌بندی‌ها بر روی عوامل تهدیدزا نیز متمرکز شده‌اند. بنابراین با وجود طیف گسترده‌ای از طبقه‌بندی‌های تهدید، هیچ‌کدام از آن‌ها

1. attacker-centric
2. defence-centric

کاملاً همه جنبه‌های تهدیدِ سایبری را ثبت و ضبط نمی‌کند. طبقه‌بندی‌های مختلف تهدید، می‌تواند اطلاعات جدیدی را به ارمغان آورده یا چشم‌انداز جالب‌توجهی را به‌دست می‌دهد.



شکل ۲: رویکرد غالب الگوهای طبقه‌بندی تهدیدات سایبری

۲-۱. الگوی طبقه‌بندی تهدیدات و فرصت‌های سایبری

الگوی طبقه‌بندی تهدیدات و فرصت‌های سایبری که برگرفته از مدل لایه‌ای فضای سایبری یعنی فیزیکی، منطقی (اطلاعاتی) و شخصیت سایبری (شناختی–اجتماعی) است که در مراجع معتبر (داخلی و خارجی) نیز آمده است. جدول (۳)، سه نمونه از نگاه اسناد معتبر داخلی و خارجی به این مدل را نشان می‌دهد.

جدول ۳: نمایشی از مدل سه‌لایه فضای سایبر (آقایی، ۱۳۹۸)

الف. مدل عملیات فضای مجازی
۱. لایه فیزیکی: شامل تجهیزات IT و زیرساخت‌هایی در حوزه فیزیکی است که به ذخیره‌سازی، انتقال و پردازش اطلاعات درون فضای سایبر می‌پردازد تا علاوه بر در برگرفتن مخازن داده، داده‌های منتقل‌شده را میان مؤلفه‌های شبکه متصل سازد. مؤلفه‌های شبکه فیزیکی شامل سخت‌افزار و زیرساخت (تجهیزات رایانه‌ای، دستگاه‌های ذخیره‌ساز، تجهیزات شبکه و لینک‌های با یا بی‌سیم) است.

۲. لایه منطقی: شامل آن دسته از عناصری از شبکه است که به یکدیگر مرتبط بوده و از لایه فیزیکی جدا می‌شوند. براساس برنامه‌نویسی منطقی (کد)، مؤلفه‌های شبکه را هدایت می‌کنند (یعنی روابط لزوماً به اتصال فیزیکی یا گره مشخصی وابسته نبوده اما توانایی‌شان برای آدرس‌دِهی منطقی و تبادل یا پردازش داده است). مؤلفه‌های شبکه منطقی شامل داده، برنامه‌های کاربردی، پردازش شبکه که به یک گره تنها متصل نمی‌شود.

۳. لایه شخصیت سایبری: شامل انتزاع داده از لایه منطقی با استفاده از قواعدی است که بر لایه منطقی تا توسعه‌دهنده، توصیفاتی از نمایشات دیجیتالی یک بازیگر یا هویت موجودیت در فضای سایبر اعمال می‌گردد. این لایه شامل حساب کاربردی (انسانی یا خودکار) و روابط میان آن‌ها است.

ب. مدل عملیات اطلاعات

۱. بُعد فیزیکی: ترکیبی از سامانه‌های C2، تصمیم‌گیرندگان کلیدی و زیرساخت‌های پشتیبانی است که باعث توانمندسازی افراد و سازمان‌ها برای ایجاد اثر می‌نماید. این بُعد شامل انسان، تسهیلات C2، روزنامه‌ها، کتب، برج‌های ماکروویو واحدهای پشتیبانی رایانه، لپ‌تاپ، تلفن هوشمند، تبلت و هر شیء دیگر از این‌دست می‌شود.

۲. بُعد اطلاعاتی: شامل اطلاعاتی است که جمع‌آوری، پردازش، ذخیره، نشر و محافظت می‌شود.

۳. بُعد شناختی: در برگیرنده تفکر افرادی است که نسبت به انتقال، دریافت و پاسخ‌گویی به اطلاعات یا اقدام بر روی آن مبادرت می‌کند. این بُعد، افراد یا گروه‌هایی را شامل می‌شود که به پردازش اطلاعات، ادراک، قضاوت و تصمیم‌گیری در خصوص آن می‌پردازد.

ج. مدل چهار لایه‌ای از فضای سایبر

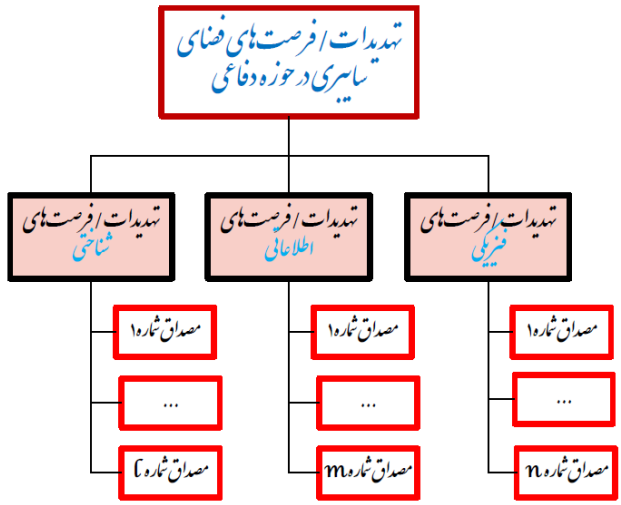
۱. لایه انسانی: نه‌فقط شامل کاربران غیرفعال فضای سایبر، بلکه افراد دیگر با هر شکل وابستگی به این فضا مورد نظر هستند.

۲. لایه اطلاعاتی: شامل داده و اطلاعات ذخیره‌شده روی سامانه‌ها، در حال انتقال روی شبکه‌ها، یا موجود در پایگاه‌ها و وبگاه‌ها است؛ این لایه در بردارنده داده و اطلاعات موجود در فضای سایبر است.

۳. لایه منطقی: شامل پروتکل‌ها، نرم‌افزارها، سرویس‌دهنده‌ها، سامانه عامل و هر آن چیزی است که منطق ارتباطی فضای سایبر را تشکیل می‌دهد.

۴. لایه فیزیکی، ارتباطی و زیرساختی: شامل تمام سرمایه‌های سایبری فیزیکی همچون کابل‌ها، امواج، فیبر، مدارها و تجهیزات سخت‌افزاری است.

با توجه به الگوی طبقه‌بندی تهدیدات و فرصت‌های سایبری، می‌توان بیان کرد که الگوی تحقیق حاضر علاوه بر اینکه می‌تواند ملاکی برای دسته‌بندی و تمایز تهدیدات-فرصت‌ها در این بخش باشد، در بخش‌های دیگر نیز می‌تواند در دسته‌بندی فناوری‌های سایبری مورد استفاده قرار گیرد. با توجه به مفاهیم مورد نظر در این مدل و ماهیت تهدیدات که به‌عنوان عوامل دارای ظرفیت ایجاد آسیب‌ها (در همه لایه‌ها یا ابعاد فیزیکی، اطلاعاتی یا شناختی) منظور می‌شوند و با توسعه مدل سه‌لایه فضای سایبر، طبقه‌بندی تهدیدات-فرصت‌ها را می‌توان بر پایه آن بنا کرد. شکل (۳)، این مدل را نشان می‌دهد.



شکل ۳: مدل تهدیدات- فرصت‌های فضای سایبری در حوزه دفاعی

همچنین مصادیق مربوط به شکل (۳)، در جدول (۴) ارائه می‌شود:

جدول ۴: مصادیق مربوط به هر لایه در مدل‌های طبقه‌بندی تهدیدات و فرصت‌های سایبری

تهدیدات		فرصت‌ها	
نوع تأثیر	مصادیق	نوع تأثیر	مصادیق
فیزیکی	حملات سایبری با هدف خرابکاری، انهدام و اخلال در کار عادی سازمان‌های دارای اهمیت	فیزیکی	ایجاد زیرساخت‌های آزمایشگاهی مورد نیاز برای کنترل و پایش تجهیزات و قطعات در فرایند تأمین و اکتساب
	ایجاد پایگاه‌های جاسوسی سایبری، نفوذ و اختلال الکترونیک توسط کشورهای متخاصم در کشورهای پیرامونی		ارتقای دقت و سرعت عملکرد تجهیزات و سنجش‌گرهای نظامی
	ازدست‌رفتن کنترل تجهیزات تحت شبکه در صورت بروز اختلال در آن شبکه		دسترسی و کنترل تجهیزات نظامی بدون سرنشین از هر مکان
	ورود تجهیزات آلوده به بدافزارهای شناخته‌شده توسط کشورهای متخاصم به کشور از طریق شرکت‌های مختلف		ارتقای امنیت تجهیزات ارتباطی
	وجود آسیب‌پذیری‌های امنیتی در تجهیزات سوئیچ و مسیریابی و کنترلی شرکت‌های سیسکو، زیمنس و ...		ارتقای قابلیت تجهیزات امنیتی
	ایمپلنت سخت‌افزاری تعبیه‌شده در تجهیزات، سامانه‌ها، نرم‌افزارها و سخت‌افزارها		تقویت مراکز آموزشی و پژوهشی و توسعه زیرساخت‌های جرم‌شناسی سایبری
	افزایش پیچیدگی تجهیزات جاسوسی و ضد امنیتی		ساماندهی و استقرار نظام احراز هویت و تشخیص هویت
	استفاده دشمن از بدافزارها برای ایجاد صدمات فیزیکی به تأسیسات و سامانه‌ها		ایجاد سازوکارهای لازم برای کنترل گیت‌وی‌های ورودی و خروجی بین‌المللی و گذرگاه‌های داخلی

تهدیدات		فرصت‌ها	
نوع تأثیر	مصادیق	نوع تأثیر	مصادیق
	آسیب به سامانه‌های نظامی متصل به شبکه‌های برخط		تقویت و سازمان‌دِهی صنعت در حوزه سایبری
	اعمال تغییرات خاص در ساخت تجهیزات از طریق نفوذ به پرینتر		کاهش ابعاد همراه با ارتقای توانمندی تجهیزات نظامی
اطلاعاتی	جمع‌آوری اطلاعات از مراکز نظامی توسط سرویس‌های بیگانه در پوشش شرکت‌ها و مؤسسات مختلف	اطلاعاتی	دسترسی به حجم انبوهی از اطلاعات در هر زمان و هر مکان
	جمع‌آوری اطلاعات از وضعیت سازمان‌ها و مراکز حساس		جمع‌آوری انبوهی از اطلاعات و دستیابی به آگاهی محیطی
	سرقت داده‌های مربوط به کارکنان خودی		تسریع در اصلاح داده‌های مربوط به طراحی تجهیزات از طریق تسریع در ساخت نمونه‌های اولیه
	ازدست‌رفتن اطلاعات نظامی		افزایش درک اطلاعاتی رزمندگان از وضعیت صحنه نبرد
	رصد مسئولین نظام، فرماندهان نیروهای مسلح، نخبگان و کارکنان حوزه دفاعی و امنیتی با استفاده از فناوری‌های ارتباطی و سایبری		ارتقای آموزش‌های نظامی متناسب با شرایط موجود
	تغییر یا تخریب اطلاعات در مراکز داده و ...		ارتقای امنیت در دریافت و ارسال اطلاعات نظامی و امنیتی
	نفوذ به تجهیزات و اعمال فرامین نادرست		افزایش سرعت و توان انتقال داده‌ها
	برآورد نادرست اطلاعاتی به‌دلیل تغییر داده‌ها		ایجاد مراکز رصد و پایش هشدار سایبری با رویکرد تخصصی فنی
	کاهش توانمندی سامانه‌های امنیتی در نظارت بر جابجایی اطلاعات		سازمان‌دِهی VPN های مجاز

تهدیدات		فرصت‌ها	
نوع تأثیر	مصادیق	نوع تأثیر	مصادیق
	ایجاد پیچیدگی در ردیابی اطلاعات امنیتی		رصد و پایش مستمر تهدیدات و آسیب‌های عملیاتی و اطلاعاتی دشمن
شناختی	تأثیرگذاری بر رفتار فرماندهان و نیروها	شناختی	امکان تجزیه‌وتحلیل شناختی اطلاعات دشمن از طریق نفوذ به مراکز رایانش ابری آنان
	تحلیل شناختی دشمن از نیروهای خودی		ارتقای سطح شناختی رزمنده نسبت به صحنه نبرد
	پیچیدگی کشف و شناخت ارتباطات ضد امنیتی		ارتقای سطح آگاهی رزمندگان از صحنه نبرد
	بروز تأثیرات ناخواسته از درک عملکرد رزمندگان به‌دلیل استفاده از امواج و تجهیزات خاص		دستیابی به درکی کامل‌تر از صحنه نبرد و وضعیت رزمندگان
	ارتقای توان پیش‌بینی دشمن از رفتار نیروهای خودی		ارتقای قدرت تصمیم‌گیری فرماندهان نظامی
	نفوذ به تجهیزات پوشیدنی رزمنده و ایجاد اختلال در آگاهی وضعیتی		ارتقای توان پیش‌بینی رفتار دشمن
	کاهش قدرت تصمیم‌گیری رزمنده از طریق نفوذ در اشیا و انتشار امواج مخرب		کمک به تصمیم‌گیری در شرایط بحرانی
	ناتوانی در تصمیم‌گیری به‌دلیل وجود داده‌های متناقض، غیرواقعی یا انبوه		قابلیت ارتقای اعتماد در ارتباطات نظامی
	کاهش قدرت تصمیم‌گیری در مواجهه با تصاویر نادرست از صحنه نبرد		سازمان‌دهی بسیج سایبری و شبکه‌های مردم‌نهاد انقلابی
	ارتقاء توان پیش‌بینی دشمن از رفتار نیروهای خودی		ایجاد سازوکارهای منسجم فرماندهی و کنترل جنگ شناختی

۳. روش‌شناسی تحقیق

نظر به این‌که اجرای این تحقیق ارائه مدل مفهومی برای شناخت منطق طبقه‌بندی تهدیدات و فرصت‌های سایبری است و نتایج آن قدرت تصمیم‌گیری تصمیم‌سازان حوزه امنیت سایبری را افزایش می‌دهد، جنبه کاربردی دارد و با توجه به گسترش دانش در این حوزه، توسعه‌ای است. بنابراین تحقیق حاضر با توجه به هدف از نوع توسعه‌ای- کاربردی است. روش تحقیق مورد استفاده، با رویکرد آمیخته (کیفی و کمی) است. در بخش کیفی با مراجعه به مقالات، کتاب‌ها و گزارشات پژوهشی، ابعاد و مؤلفه‌های مدل استخراج و کنترل کیفی یافته‌ها انجام شد. در گام کمی نیز از طریق روش‌های آمار توصیفی و استنباطی و با استفاده از نرم‌افزار SPSS26 تجزیه‌وتحلیل داده‌ها صورت گرفت. به این شکل که ابتدا نرمال یا غیرنرمال بودن داده‌های مربوط به فرضیات از طریق آزمون کولموگروف- اسمیرنوف بررسی می‌گردد، سپس با استفاده از آماره تی، تجزیه‌وتحلیل داده‌ها انجام خواهد شد. جامعه آماری این پژوهش شامل صاحب‌نظران دانشگاهی و خبرگان آشنا به فضای سایبر و فرماندهان راهبردی و عملیاتی نیروهای مسلح در خصوص موضوع سایبر بودند که با توجه به معیار دسترسی به نخبگان، تعداد ۱۴۰ نفر به‌عنوان جامعه آماری شناسایی و براساس جدول مورگان، حجم نمونه ۱۲۰ نفر برآورد و با روش نمونه‌گیری تصادفی طبقاتی انتخاب گردیدند. روش گردآوری داده‌ها کتابخانه‌ای و میدانی و ابزار اصلی سنجش در این تحقیق، پرسش‌نامه محقق ساخته با ۶۰ گویه در قالب طیف ۵ گزینه‌ای لیکرت است.

۴. یافته‌ها و تجزیه‌وتحلیل داده‌ها

جهت تعیین روایی در این تحقیق از دو نوع روایی به شرح ذیل استفاده گردید:

روایی وابسته به معیار: هر چه همبستگی بین شاخص‌ها و متغیر وابسته یا ملاک بالاتر باشد، روایی بهتر است (فردآن،۱۳۸۲:۴۶). به‌عبارتی دیگر در این پژوهش هر چه همبستگی بین زیرمعیارها با معیارها بیشتر باشد، روایی وابسته به معیار پرسش‌نامه بهتر است. ازاین‌رو سه معیار شناختی، اطلاعاتی و فیزیکی به‌عنوان متغیر مستقل و تهدید و فرصت به‌عنوان متغیر

وابسته در نظر گرفته شده است. همان‌گونه که در جدول (۶)، دیده می‌شود، هر ۳ فاکتور در سطح اطمینان ۰/۹۹ همبستگی مثبت و معناداری دارند.

جدول ۵: نتایج همبستگی فاکتورهای اصلی پژوهش

فاکتورها	شناختی	اطلاعاتی	فیزیکی
تهدید	۰/۹۴	۰/۹۱	۰/۹۳
فاکتورها	**شناختی**	**اطلاعاتی**	**فیزیکی**
فرصت	۰/۹۳	۰/۹۴	۰/۹۱

سنجش اعتبار محتوا (CVR): این روش میزان موافقت میان ارزیابان یا داوران را در خصوص «مناسب یا اساسی بودن» یک گویه خاص می‌سنجد. لاوشه پیشنهاد کرد که هر گویه یا پرسش به مجموعه‌ای از ارزیابان یا داوران داده شود و از آن‌ها پرسیده شود که آیا گویه مورد نظر برای سنجش سازه مورد نظر «اساسی یا سودمند» هست یا نه؟ طبق نظر لاوشه، اگر بیش از نیمی از ارزیابان یا داوران بیان داشتند که آن «اساسی یا سودمند» است، آن گویه دست‌کم از مقداری اعتبار محتوا برخوردار است. هرچه میزان موافقت میان ارزیابان یا داوران در مورد «اساسی یا سودمند» بودن یک گویه معین بالاتر باشد، سطح اعتبار محتوا بالاتر است. لاوشه با استفاده از این فرض، فرمول زیر را برای سنجش اعتبار محتوا ابداع کرد که به آن نسبت اعتبار محتوا گفته می‌شود (میرزایی، ۳۲۷:۱۳۸۸).

به‌همین‌منظور از روش «سی. ایچ. لاوشه»[1] برای سنجش اعتبار محتوا استفاده شد و یک نمونه آماری ۲۰ نفره به سؤالات این پرسش‌نامه پاسخ دادند. نسبت اعتبار به‌دست‌آمده برای تمامی سؤالات پرسش‌نامه که در جدول (۷) برآورد شده مورد قبول بود.

1. C.H. Lawshe

جدول ۶: نتایج مرتبط با نسبت اعتبار محتوای به دست آمده برای سؤالات پرسش‌نامه

شماره سؤال	نسبت اعتبار محتوا	شماره سؤال	نسبت اعتبار محتوا	شماره سؤال	نسبت اعتبار محتوا	شماره سؤال	نسبت اعتبار محتوا
۱	۱	۱۶	۱	۳۱	۱	۴۶	۱
۲	۱	۱۷	۱	۳۲	۰/۹۵	۴۷	۰/۹
۳	۱	۱۸	۱	۳۳	۱	۴۸	۱
۴	۱	۱۹	۰/۹۵	۳۴	۱	۴۹	۱
۵	۱	۲۰	۱	۳۵	۱	۵۰	۱
۶	۱	۲۱	۱	۳۶	۱	۵۱	۰/۸۵
۷	۱	۲۲	۱	۳۷	۰/۹۴	۵۲	۱
۸	۱	۲۳	۱	۳۸	۱	۵۳	۱
۹	۱	۲۴	۰/۸	۳۹	۱	۵۴	۰/۹۵
۱۰	۰/۹۵	۲۵	۱	۴۰	۱	۵۵	۱
۱۱	۱	۲۶	۱	۴۱	۱	۵۶	۱
۱۲	۱	۲۷	۱	۴۲	۰/۹۴	۵۷	۱
۱۳	۰/۹۵	۲۸	۰/۹۵	۴۳	۱	۵۸	۰/۹۵
۱۴	۰/۹۰	۲۹	۱	۴۴	۱	۵۹	۱
۱۵	۰/۹۴	۳۰	۱	۴۵	۱	۶۰	۱

به‌منظور بررسی پایایی پرسش‌نامه از ضریب آلفای کرونباخ که توسط نرم‌افزار SPSS محاسبه گردید، استفاده شد. از آنجایی که ضریب آلفای کرونباخ بالاتر از ۰/۷ قابل قبول است؛ مقدار آن برای سؤالات پرسش‌نامه در جدول (۸)، برابر ۰/۹۵ شد که مقدار قابل‌توجهی جهت پایا بودن پرسش‌نامه است.

جدول ۷.: نتایج آزمون آلفای کرونباخ مرتبط برای هرکدام از ابعاد پرسش‌نامه

حوزه پرسش‌نامه	تعداد سؤال‌ها	ضریب آلفای کرونباخ	متغیرهای مکنون	تعداد سؤال	ضریب آلفای کرونباخ
طبقه‌بندی تهدیدات و فرصت‌های فضای سایبر	۶۰ سؤال	۰/۹۵	شناختی (تهدید)	۱۰	۰/۹۶
			اطلاعاتی (تهدید)	۱۰	۰/۹۳
			فیزیکی (تهدید)	۱۰	۰/۹۶
			شناختی (فرصت)	۱۰	۰/۹۰
			اطلاعاتی (فرصت)	۱۰	۰/۹۵
			فیزیکی (فرصت)	۱۰	۰/۹۲

با توجه به تجزیه‌وتحلیل داده‌های جمع‌آوری شده از طریق نرم‌افزار SPSS می‌توان اطلاعات حاصل را در بخش آمار توصیفی به‌صورت زیر بیان نمود:

جدول ۸: مشخصات پاسخ‌دهندگان

- مشخصات سطح تحصیلات پاسخ‌دهندگان			
لیسانس: ٪۱۷/۳	فوق‌لیسانس: ٪۲۰/۵		دکترا: ٪۶۲/۲
- مشخصات سن پاسخ‌دهندگان			
۲۰ – ۳۵: ٪۶/۳	۳۵ – ۴۰: ٪۳۸/۳		۴۰ به بالا: ٪۵۵/۴
- مشخصات سابقه‌کاری پاسخ‌دهندگان			
۵-۱۰: ٪۶/۲	۱۰-۱۵: ٪۱۳/۴	۱۵-۲۰: ٪۲۰/۲	۲۰ به بالا: ٪۶۴/۲
- رده مسئولیتی			
فرماندهی: ٪۳۴/۶	مدیریتی: ٪۴۳/۱		کارشناسی: ٪۲۲/۳

ضمناً به‌منظور مشخص کردن نوع آزمون مورد استفاده برای فرضیه‌های تحقیق، ابتدا به بررسی نرمال یا غیرنرمال بودن داده‌های مربوط به فرضیات از آزمون کولموگروف-اسمیرنوف پرداخته می‌شود و سپس با استفاده از نتایج این آزمون، از روش‌های آماری پارامتری یا غیرپارامتری مناسب برای آزمودن فرضیه‌ها استفاده می‌شود. بنابراین فرضیه‌ها به شکل زیر است:

H0: توزیع داده‌ها نرمال است (داده‌ها از جامعهٔ نرمال استخراج شده‌اند)

H1: توزیع داده‌ها نرمال نیست (داده‌ها از جامعهٔ نرمال استخراج نشده‌اند)

جدول ۹: نتایج حاصل از آزمون کولموگروف- اسمیرنوف

متغیر	سطح معنی‌داری	مقدار خطا	فرض صفر	نتیجه‌گیری
شناختی (تهدید)	۰/۳۱۹	۰/۰۵	رد نمی‌شود	داده‌ها نرمال است
اطلاعاتی (تهدید)	۰/۵۱۲	۰/۰۵	رد نمی‌شود	داده‌ها نرمال است
فیزیکی (تهدید)	۰/۲۱۸	۰/۰۵	رد نمی‌شود	داده‌ها نرمال است
شناختی (فرصت)	۰/۵۱۳	۰/۰۵	رد نمی‌شود	داده‌ها نرمال است
اطلاعاتی (فرصت)	۰/۶۱۸	۰/۰۵	رد نمی‌شود	داده‌ها نرمال است
فیزیکی (فرصت)	۰/۵۱۲	۰/۰۵	رد نمی‌شود	داده‌ها نرمال است

با توجه به جدول (۱۰)، مشاهده می‌شود که تمامی متغیرها، نرمال هستند به‌همین خاطر از روش‌های آمار پارامتری استفاده می‌شود.

نتایج حاصل از بررسی ابعاد تهدیدات فضای سایبری در جدول زیر ارائه می‌شود:

جدول ۱۰: نتایج حاصل از بررسی ابعاد تهدیدات فضای سایبری

ردیف	ابعاد	مؤلفه	میانگین	انحراف از معیار	انحراف از میانگین	آماره تی	سطح معنی‌داری	نتیجه
۱	شناختی	تأثیرگذاری بر رفتار فرماندهان و نیروها	۴/۱۶۰	۰/۸۱۷	۰/۱۱۵	۱۰/۰۳۸	۰/۰۰۰	√
۲		تحلیل شناختی دشمن از نیروهای خودی	۴/۵۲۰	۰/۶۴۶	۰/۱۱۴	۱۶/۶۲۵	۰/۰۰۰	√
۳		پیچیدگی کشف و شناخت ارتباطات ضد امنیتی	۴/۰۸۰	۰/۷۵۱	۰/۱۰۶	۱۰/۱۶۱	۰/۰۰۰	√
۴		بروز تأثیرات ناخواسته از درک عملکرد رزمندگان به‌دلیل استفاده از امواج و تجهیزات خاص	۰/۰۴۰	۰/۸۳۲	۰/۱۱۷	۸/۸۳۹	۰/۰۰۰	√
۵		ارتقای توان پیش‌بینی دشمن از رفتار نیروهای خودی	۴/۳۲۰	۰/۹۳۵	۰/۱۳۲	۹/۹۷۸	۰/۰۰۰	√
۶		نفوذ به تجهیزات پوشیدنی رزمنده و ایجاد اختلال در آگاهی وضعیتی	۴/۳۲۰	۰/۸۶۷	۰/۱۲۲	۱۰/۷۵۹	۰/۰۰۰	√

ردیف	ابعاد	مؤلفه	میانگین	انحراف از معیار	انحراف از میانگین	آماره تی	سطح معنی‌داری	نتیجه
۷		کاهش قدرت تصمیم‌گیری رزمنده از طریق نفوذ در اشیا و انتشار امواج مخرب	۴/۲۸۰	۰/۸۰۹	۰/۱۱۴	۱۱/۱۸۶	۰/۰۰۰	√
۸		ناتوانی در تصمیم‌گیری به‌دلیل وجود داده‌های متناقض، غیرواقعی یا انبوه	۴/۲۶۰	۰/۶۹۴	۰/۰۹۸	۱۲/۸۳۳	۰/۰۰۰	√
۹		کاهش قدرت تصمیم‌گیری در مواجهه با تصاویر نادرست از صحنه نبرد	۴/۰۸۰	۰/۸۰۴	۰/۱۱۳	۹/۴۹۸	۰/۰۰۰	√
۱۰		ارتقای توان پیش‌بینی دشمن از رفتار نیروهای خودی	۴/۳۰۰	۰/۷۸۸	۰/۱۱۱	۱۱/۶۵۱	۰/۰۰۰	√
۱۱	اطلاعاتی	جمع‌آوری اطلاعات از مراکز نظامی توسط سرویس‌های بیگانه در پوشش شرکت‌ها و مؤسسات مختلف	۴/۳۴۰	۰/۷۷۲	۰/۱۰۹	۱۲/۲۷۰	۰/۰۰۰	√
۱۲		جمع‌آوری اطلاعات از وضعیت سازمان‌ها و مراکز حساس	۴/۳۰۰	۰/۸۳۶	۰/۱۱۸	۱۰/۹۵۵	۰/۰۰۰	√
۱۳		سرقت داده‌های مربوط به کارکنان خودی	۴/۲۸۰	۰/۸۸۱	۰/۱۲۴	۱۰/۲۶۷	۰/۰۰۰	√

ردیف	ابعاد	مؤلفه	میانگین	انحراف از معیار	انحراف از میانگین	آماره تی	سطح معنی‌داری	نتیجه
۱۴		از دست رفتن اطلاعات نظامی	۴/۴۰۰	۰/۸۳۲	۰/۱۱۷	۱۱/۸۸۴	۰/۰۰۰	√
۱۵		رصد مسئولین نظام، فرماندهان نیروهای مسلح، نخبگان و کارکنان حوزه دفاعی و امنیتی با استفاده از فناوری‌های ارتباطی و سایبری	۴/۰۶۰	۰/۸۴۲	۰/۱۱۹	۸/۸۹۱	۰/۰۰۰	√
۱۶		تغییر یا تخریب اطلاعات در مراکز داده و ...	۴/۲۰۰	۰/۸۵۷	۰/۱۲۱	۹/۸۹۹	۰/۰۰۰	√
۱۷		نفوذ به تجهیزات و اعمال فرامین نادرست	۴/۳۲۰	۰/۷۴۰	۰/۱۰۴	۱۲/۶۰۲	۰/۰۰۰	√
۱۸		برآورد نادرست اطلاعاتی به‌دلیل تغییر داده‌ها	۴/۲۶۰	۰/۷۷۷	۰/۱۰۹	۱۱/۴۵۹	۰/۰۰۰	√
۱۹		کاهش توانمندی سامانه‌های امنیتی در نظارت بر جابجایی اطلاعات	۴/۳۲۰	۰/۸۶۷	۰/۱۲۲	۱۰/۷۵۹	۰/۰۰۰	√
۲۰		ایجاد پیچیدگی در ردیابی اطلاعات امنیتی	۴/۱۸۰	۰/۸۴۹	۰/۱۲۰	۹/۸۱۹	۰/۰۰۰	√

ردیف	ابعاد	مؤلفه	میانگین	انحراف از معیار	انحراف از میانگین	آماره تی	سطح معنی‌داری	نتیجه
۲۱	فیزیکی	حملات سایبری با هدف خرابکاری، انهدام و اخلال در کار عادی سازمان‌های دارای اهمیت	۴/۲۴۰	۰/۸۲۲	۰/۱۱۶	۱۰/۶۶۵	۰/۰۰۰	√
۲۲		ایجاد پایگاه‌های جاسوسی سایبری، نفوذ و اختلال الکترونیک توسط کشورهای متخاصم در کشورهای پیرامونی	۴/۱۸۰	۰/۹۶۲	۰/۱۳۶	۸/۶۷۰	۰/۰۰۰	√
۲۳		از دست رفتن کنترل تجهیزات تحت شبکه در صورت بروز اختلال در آن شبکه	۴/۳۴۰	۰/۸۹۴	۰/۱۲۶	۱۰/۵۹۱	۰/۰۰۰	√
۲۴		ورود تجهیزات آلوده به بدافزارهای شناخته‌شده توسط کشورهای متخاصم به کشور از طریق شرکت‌های مختلف	۴/۴۴۰	۰/۷۶۰	۰/۱۰۷	۱۳/۳۹۴	۰/۰۰۰	√
۲۵		وجود آسیب‌پذیری‌های امنیتی در تجهیزات سوئیچ و مسیریابی و کنترلی شرکت‌های سیسکو، زیمنس و ...	۴/۴۰۰	۰/۸۰۸	۰/۱۱۴	۱۲/۲۵۰	۰/۰۰۰	√

ردیف	ابعاد	مؤلفه	میانگین	انحراف از معیار	انحراف از میانگین	آماره تی	سطح معنی‌داری	نتیجه
۲۶		ایمپلنت سخت‌افزاری تعبیه‌شده در تجهیزات، سامانه‌ها، نرم‌افزارها و سخت‌افزارها	۴/۳۰۰	۰/۷۳۵	۰/۱۰۴	۱۲/۵۰۰	۰/۰۰۰	√
۲۷		افزایش پیچیدگی تجهیزات جاسوسی و ضد امنیتی	۴/۳۸۰	۰/۶۹۶	۰/۰۹۸	۱۴/۰۰۷	۰/۰۰۰	√
۲۸		استفاده دشمن از بدافزارها برای ایجاد صدمات فیزیکی به تأسیسات و سامانه‌ها	۴/۱۰۰	۰/۷۸۸	۰/۱۱۱	۹/۸۵۹	۰/۰۰۰	√
۲۹		آسیب به سامانه‌های نظامی متصل به شبکه‌های برخط	۴/۲۸۰	۰/۸۰۹	۰/۱۱۴	۱۱/۱۸۶	۰/۰۰۰	√
۳۰		اعمال تغییرات خاص در ساخت تجهیزات از طریق نفوذ به پرینتر	۴/۴۲۰	۰/۷۳۰	۰/۱۰۳	۱۳/۷۳۷	۰/۰۰۰	√

جدول ۱۱: نتایج حاصل از بررسی ابعاد فرصت‌های فضای سایبری

ردیف	ابعاد	مؤلفه	میانگین	انحراف از معیار	انحراف از میانگین	آماره تی	سطح معنی‌داری	نتیجه
۱	شناختی	امکان تجزیه‌وتحلیل شناختی اطلاعات دشمن از طریق نفوذ به مراکز رایانش ابری آنان	۴/۰۴۰	۰/۸۷۹	۰/۱۲۴	۸/۳۶۰	۰/۰۰۰	√
۲		ارتقای سطح شناختی رزمنده نسبت به صحنه نبرد	۴/۱۲۰	۰/۸۹۵	۰/۱۲۶	۸/۸۴۵	۰/۰۰۰	√
۳		ارتقای سطح آگاهی رزمندگان از صحنه نبرد	۴/۰۲۰	۰/۸۲۰	۰/۱۱۶	۸/۷۹۱	۰/۰۰۰	√
۴		دستیابی به درکی کامل‌تر از صحنه نبرد و وضعیت رزمندگان	۴/۳۲۰	۰/۸۶۷	۰/۱۲۲	۱۰/۷۵۹	۰/۰۰۰	√
۵		ارتقای قدرت تصمیم‌گیری فرماندهان نظامی	۴/۳۰۰	۰/۷۳۲	۰/۱۰۴	۱۲/۵۰۰	۰/۰۰۰	√
۶		ارتقای توان پیش‌بینی رفتار دشمن	۴/۲۴۰	۰/۷۷۰	۰/۱۰۹	۱۱/۳۷۴	۰/۰۰۰	√
۷		کمک به تصمیم‌گیری در شرایط بحرانی	۴/۰۸۰	۰/۷۷۸	۰/۱۱۰	۹/۸۱۲	۰/۰۰۰	√

ردیف	ابعاد	مؤلفه	میانگین	انحراف از معیار	انحراف از میانگین	آماره تی	سطح معنی‌داری	نتیجه
۸		قابلیت ارتقای اعتماد در ارتباطات نظامی	۴/۱۰۰	۰/۷۸۸	۰/۱۱۱	۹/۸۵۹	۰/۰۰۰	√
۹		سازمان‌دِهی بسیج سایبری و شبکه‌های مردم‌نهاد انقلابی	۴/۰۶۰	۰/۷۹۳	۰/۱۱۲	۹/۴۵۱	۰/۰۰۰	√
۱۰		ایجاد سازوکارهای منسجم فرماندهی و کنترل جنگ شناختی	۴/۱۴۰	۰/۷۵۶	۰/۱۰۶	۱۰/۶۶۰	۰/۰۰۰	√
۱۱	اطلاعاتی	دسترسی به حجم انبوهی از اطلاعات در هر زمان و هر مکان	۴/۰۶۰	۰/۸۹۰	۰/۱۲۵	۸/۴۲۱	۰/۰۰۰	√
۱۲		جمع‌آوری انبوهی از اطلاعات و دست‌یابی به آگاهی محیطی	۴/۳۲۰	۰/۷۶۷	۰/۱۰۸	۱۲/۱۵۸	۰/۰۰۰	√
۱۳		تسریع در اصلاح داده‌های مربوط به طراحی تجهیزات از طریق تسریع در ساخت نمونه‌های اولیه	۴/۳۰۰	۰/۷۳۵	۰/۱۰۴	۱۲/۵۰۰	۰/۰۰۰	√
۱۴		افزایش درک اطلاعاتی رزمندگان از وضعیت صحنه نبرد	۴/۲۶۰	۰/۸۰۳	۰/۱۱۳	۱۱/۰۹۱	۰/۰۰۰	√
۱۵		ارتقای آموزش‌های نظامی متناسب با شرایط موجود	۴/۱۰۰	۰/۹۰۹	۰/۱۲۸	۸/۵۵۶	۰/۰۰۰	√

ردیف	ابعاد	مؤلفه	میانگین	انحراف از معیار	انحراف از میانگین	آماره تی	سطح معنی‌داری	نتیجه
۱۶		ارتقای امنیت در دریافت و ارسال اطلاعات نظامی و امنیتی	۴/۱۸۰	۰/۹۶۲	۰/۱۳۶	۸/۶۷۰	۰/۰۰۰	√
۱۷		افزایش سرعت و توان انتقال داده‌ها	۴/۲۰۰	۰/۸۳۲	۰/۱۱۷	۱۰/۱۸۶	۰/۰۰۰	√
۱۸		ایجاد مراکز رصد و پایش هشدار سایبری با رویکرد تخصصی فنی	۴/۳۰۰	۰/۸۱۴	۰/۱۱۵	۱۱/۲۸۷	۰/۰۰۰	√
۱۹		سازمان‌دِهی VPN های مجاز	۴/۲۲۰	۰/۸۶۴	۰/۱۲۲	۹/۹۸۴	۰/۰۰۰	√
۲۰		رصد و پایش مستمر تهدیدات و آسیب‌های عملیاتی و اطلاعاتی دشمن	۴/۳۴۰	۰/۷۷۲	۰/۱۰۹	۱۲/۲۷۰	۰/۰۰۰	√
۲۱	فیزیکی	ایجاد زیرساخت‌های آزمایشگاهی موردنیاز برای کنترل و پایش تجهیزات و قطعات در فرایند تأمین و اکتساب	۴/۲۰۰	۰/۸۳۲	۰/۱۱۷	۱۰/۱۸۶	۰/۰۰۰	√
۲۲		ارتقای دقت و سرعت عملکرد تجهیزات و سنجش‌گرهای نظامی	۴/۱۶۰	۰/۸۱۷	۰/۱۱۵	۱۰/۰۳۸	۰/۰۰۰	√

ردیف	ابعاد	مؤلفه	میانگین	انحراف از معیار	انحراف از میانگین	آماره تی	سطح معنی‌داری	نتیجه
۲۳		دسترسی و کنترل تجهیزات نظامی بدون سرنشین از هر مکان	۴/۱۲۰	۰/۸۷۲	۰/۱۲۳	۹/۰۸۰	۰/۰۰۰	√
۲۴		ارتقای امنیت تجهیزات ارتباطی	۴/۲۶۰	۰/۷۷۷	۰/۱۰۹	۱۱/۴۵۹	۰/۰۰۰	√
۲۵		ارتقای قابلیت تجهیزات امنیتی	۴/۰۸۰	۰/۷۵۱	۰/۱۰۶	۱۰/۱۶۱	۰/۰۰۰	√
۲۶		تقویت مراکز آموزشی و پژوهشی و توسعه زیرساخت‌های جرم‌شناسی سایبری	۴/۰۰۰	۰/۷۸۲	۰/۱۱۰	۹/۰۳۷	۰/۰۰۰	√
۲۷		ساماندهی و استقرار نظام احراز هویت و تشخیص هویت	۴/۲۰۰	۰/۷۲۸	۰/۱۰۳	۱۱/۶۴۹	۰/۰۰۰	√
۲۸		ایجاد سازوکارهای لازم برای کنترل گیت‌وی‌های ورودی و خروجی بین‌المللی و گذرگاه‌های داخلی	۴/۵۶۰	۰/۶۳۴	۰/۰۹۱	۱۷/۱۳۰	۰/۰۰۰	√
۲۹		تقویت و سازمان‌دهی صنعت در حوزه سایبری	۴/۰۶۰	۰/۷۶۶	۰/۱۰۸	۹/۷۷۳	۰/۰۰۰	√

ردیف	ابعاد	مؤلفه	میانگین	انحراف از معیار	انحراف از میانگین	آماره تی	سطح معنی‌داری	نتیجه
۳۰		کاهش ابعاد همراه با ارتقای توانمندی تجهیزات نظامی	۴/۴۴۰	۰/۷۶۰	۰/۱۰۷	۱۳/۳۹۴	۰/۰۰۰	√

نتیجه‌گیری و پیشنهاد

منطق الگوی طبقه‌بندی ارائه شده در این تحقیق براساس مفهوم حاکم بر لایه‌های سه‌گانه فضای سایبری و در نظر گرفتن توأمان تهدید و فرصت برای موجودیت‌های در این لایه‌ها است. شاید این لایه‌بندی از جهت‌های دیگری نیز برای برنامه‌ریزان و تصمیم‌گیرندگان دارای اهمیت باشد؛ چراکه آن‌ها می‌توانند ملاکی برای دسته‌بندی و تمایزدادن فناوری‌ها سایبری، آسیب‌ها، روش‌ها و ... نیز باشد؛ به‌عنوان مثال هرگاه صحبت از دفاع سایبری برای مقابله با تهدیدات سیاسی یا اجتماعی و فرهنگی منتج از فضای سایبر به میان آید، باید توجه را به سمت لایه شناختی متمرکز ساخت و از این مدل، می‌توان برای طبقه‌بندی تهدیدات و فرصت‌های در حوزه‌های مختلف استفاده کرد. مثلاً از طبقه‌بندی تهدیدات سایبری در حوزه دفاعی و طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی (زیرساخت‌های ارتباطی و اطلاعاتی و ...) بهره‌برداری کرد. بنابراین براساس نتایج تحقیق، می‌توان در پاسخ به سؤالات پژوهش، مصادیق مربوط به طبقه‌بندی تهدیدات و فرصت‌های سایبری را در لایه‌های سه‌گانه (فیزیکی، اطلاعاتی و شناختی) به شرح جدول زیر بیان کرد:

جدول ۱۲: مصادیق مربوط به تهدیدهای لایه‌های سه‌گانه

ردیف	نوع تاثیر	مصادیق
۱	فیزیکی	۱- حملات سایبری با هدف خرابکاری، انهدام و اختلال در کار عادی سازمان‌های دارای اهمیت
		۲- ایجاد پایگاه‌های جاسوسی سایبری، شنود و اختلال الکترونیک توسط کشورهای متخاصم در کشورهای پیرامونی
		۳- از دست دادن کنترل تجهیزات تحت شبکه در صورت بروز اختلال در آن شبکه
		۴- ورود تجهیزات آلوده به بدافزارهای ساخته شده توسط کشورهای متخاصم به کشور از طریق شرکت‌های مختلف
		۵- وجود آسیب‌پذیری امنیتی در تجهیزات سوئیچ و مسیریابی و کنترلی شرکت‌های سیسکو، زیمنس و غیره
		۶- ایمپلنت سخت‌افزاری تعبیه شده در تجهیزات، سامانه‌ها، نرم‌افزارها/ سخت‌افزارها
		۷- افزایش پیچیدگی تجهیزات جاسوسی و ضدامنیتی
		۸- استفاده دشمن از بدافزارها برای ایجاد صدمات فیزیکی به تاسیسات و سیستم‌ها
		۹- آسیب به سیستم‌های نظامی متصل به شبکه‌های برخط
		۱۰- اعمال تغییرات خاص در ساخت تجهیزات از طریق نفوذ به پرینتر
۲	اطلاعاتی	۱- جمع‌آوری اطلاعات از مراکز نظامی توسط سرویس‌های بیگانه در پوشش شرکت‌ها و موسسات مختلف
		۲- جمع‌آوری اطلاعات از وضعیت سازمان‌ها و مراکز حساس
		۳- سرقت داده‌های مربوط به کارکنان خودی
		۴- از دست رفتن اطلاعات نظامی
		۵- رصد مسؤلین نظام، فرماندهان ن.م، نخبگان و کارکنان حوزه دفاعی و امنیتی با استفاده از فناوری‌های ارتباطی و سایبری
		۶- تغییر یا تخریب اطلاعات در مراکز داده و ...
		۷- نفوذ به تجهیزات و اعمال فرامین نادرست
		۸- برآورد نادرست اطلاعاتی به دلیل تغییر داده‌ها
		۹- کاهش توانمندی سیستم‌های امنیتی در نظارت بر جابجایی اطلاعات
		۱۰- ایجاد پیچیدگی در ردیابی اطلاعات امنیتی
۳	شناختی	۱- تاثیرگذاری بر رفتار فرماندهان و نیروها
		۲- تحلیل شناختی دشمن از نیروهای خودی
		۳- پیچیدگی کشف و شناخت ارتباطات ضدامنیتی
		۴- بروز تاثیرات ناخواسته از بر روی درک عملکرد رزمندگان به‌دلیل استفاده از امواج و تجهیزات خاص
		۵- ارتقاء توان پیش‌بینی دشمن از رفتار نیروهای خودی
		۶- نفوذ به تجهیزات پوشیدنی رزمنده و ایجاد اختلال درآگاهی وضعیتی
		۷- کاهش قدرت تصمیم‌گیری رزمنده از طریق نفوذ در اشیاء و انتشار امواج مخرب
		۸- ناتوانی در تصمیم‌گیری به دلیل وجود داده‌ی متناقض، غیرواقعی یا انبوه
		۹-کاهش قدرت تصمیم‌گیری در مواجهه با تصاویر نادرست از صحنه نبرد
		۱۰- ارتقاء توان پیش‌بینی دشمن از رفتار نیروهای خودی

جدول ۱۳: مصادیق مربوط به فرصت‌های لایه‌های سه‌گانه

ردیف	نوع تاثیر	مصادیق
		۱- ایجاد زیرساخت‌های آزمایشگاهی مورد نیاز برای کنترل و پایش تجهیزات و قطعات در فرایند تامین و اکتساب
		۲- ارتقای دقت و سرعت عملکرد تجهیزات و سنجش‌گرهای نظامی
		۳- دسترسی و کنترل تجهیزات نظامی بدون‌سرنشین از هر مکان
		۴- ارتقای امنیت تجهیزات ارتباطی
		۵- ارتقای قابلیت تجهیزات امنیتی
		۶- تقویت مراکز آموزشی و پژوهشی و توسعه زیرساخت‌های جرم‌شناسی سایبری
		۷- ساماندهی و استقرار نظام احراز هویت و تشخیص هویت
		۸- ایجاد ساز وکارهای لازم برای کنترل گیت‌وی‌های ورودی و خروجی بین‌المللی و گذرگاه‌های داخلی
		۹- تقویت و سازماندهی صنعت در حوزه سایبری
		۱۰-کاهش ابعاد همراه با ارتقای توانمندی تجهیزات نظامی
۲	اطلاعاتی	۱- دسترسی به حجم انبوهی از اطلاعات در هر زمان و هر مکان
		۲- جمع‌آوری انبوهی از اطلاعات و دست‌یابی به آگاهی محیطی
		۳- تسریع در اصلاح داده‌های مربوط به طراحی تجهیزات از طریق تسریع در ساخت نمونه‌های اولیه
		۴- افزایش درک اطلاعاتی رزمندگان از وضعیت صحنه نبرد
		۵- ارتقای آموزش‌های نظامی متناسب با شرایط موجود
		۶- ارتقای امنیت در دریافت و ارسال اطلاعات نظامی و امینتی
		۷- افزایش سرعت و توان انتقال داده‌ها
		۸- ایجاد مراکز رصد و پایش هشدار سایبری با رویکرد تخصصی فتی
		۹- ساماندهی VPNهای مجاز
		۱۰- رصد و پایش مستمر تهدیدات و اسیب‌های عملیاتی و اطلاعاتی دشمن
۳	شناختی	۱- امکان تجزیه و تحلیل شناختی اطلاعات دشمن از طریق نفوذ به مراکز رایانش ابری آنان
		۲- ارتقای سطح شناختی رزمنده نسبت به صحنه نبرد
		۳- ارتقای سطح آگاهی رزمندگان از صحنه نبرد
		۴- دستیابی به درکی کاملتر از صحنه نبرد و وضعیت رزمندگان
		۵- ارتقای قدرت تصمیم‌گیری فرماندهان نظامی
		۶- ارتقای توان پیش‌بینی رفتار دشمن
		۷- کمک به تصمیم‌گیری در شرایط بحرانی
		۸- قابلیت ارتقای اعتماد در ارتباطات نظامی
		۹- سازماندهی بسیج سایبری و شبکه‌های مردم نهاد انقلابی
		۱۰- ایجاد ساز و کارهای منسجم فرماندهی و کنترل جنگ شناختی

پیشنهادهای پژوهشی

- ✓ مصادیق مربوط به لایه‌های قوت‌ها و ضعف‌های سه‌گانه الگوی طبقه‌بندی احصا شود.
- ✓ راهبردهای فضای سایبر با استفاده از مدل ماتریس SWOT تدوین شوند.

فهرست منابع

- آقایی، محسن؛ معینی، علی؛ عرب‌سرخی، ابوذر؛ محمدیان، ایوب و زارعی، علی‌اصغر (۱۳۹۸). ***ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی***، فصلنامه امنیت ملی، سال نهم، شماره دوم.
- سازمان پدافند غیرعامل کشور (۱۳۹۴). سند راهبردی پدافند سایبری کشور
- سند ملی استاندارد و فناوری (۱۳۹۸).
- کیانخواه، احسان (۱۳۹۸). ***چالش‌های راهبردی حکمرانی با گسترش فضای سایبر***، فصلنامه علمی امنیت ملی، سال نهم، شماره سی و چهارم.
- گرشاسبی، علیرضا؛ یوسفی دیندارلو، مجتبی (۱۳۹۵). ***بررسی اثرات تحریم بین‌المللی بر متغیرهای کلان اقتصادی ایران***، فصلنامه تحقیقات مدل‌سازی اقتصادی، شماره ۲۵.
- مرکز راهبری سایبر ، ستاد کل ن.م (۱۳۹۹). ***فرهنگ‌نامه سایبری نیروهای مسلح***، مرکز راهبری سایبرن. م، ستاد کل ن.م
- مرکز بررسی‌های استراتژیک ریاست جمهوری (۱۳۹۹). ***گزارش نشست حکمرانی سایبری و راهبرد جمهوری اسلامی ایران***، مرکز بررسی‌های استراتژیک ریاست جمهوری، شماره مسلسل: ۵۱۴، کد گزارش:۸۳-۹۹.
- واحدی، مرتضی (۱۳۹۸). ***تهدیدات فضای سایبر، موسسه آموزشی و تحقیقاتی صنایع دفاعی***.

References

- Cyber Primer (2016). Development, Concepts and Doctrine Centre, Ministry of Defence, www.gov.uk/mod/dcdc
- Magar, (2016). State-of-the-Art in Cyber Threat Models and Methodologies, Department of National Defence, Defence Research and Development Canada.
- D.J.Bodeau, C.D. McCollum, D.B. Fox, (2018). Cyber Threat Modeling: Survey, Assessment, and representative Framework, Homeland Security Systems Engineering and Development Institute (HSSEDI)™ Operated by The MITRE Corporation, 2018.
- J. J. Cebula et al, (2014). A Taxonomy of Operational CyberSecurity Risks Version 2, Carnegie Mellon University.
- J. Tarala, K.K. Tarala, (2015). Open Threat Taxonomy version 1.1, Enclave Security, 2015.
- L. Steven, (2020). Evaluation of Comprehensive Taxonomies for Information Technology Threats, The SANS Institute.
- L.O. Nweke, S.D. Wolthusen, (2020). A Review of Asset-Centric Threat Modelling Approaches, International Journal of Advanced Computer Science and Applications(IJACSA), Vol. 11, No. 2, 2020.
- M. Jouini et al, (2014). Classification of security threats in information systems, 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014).
- M. Mateski et al, (2012). Cyber Threat Metrics ", Sandia National Laboratories.
- Mohd Yusof,A. et al, (2011). The Cyber Space and Information, Communication and Technology: A Tool for Westernization or Orientalism or Both, Journal of Computer Science 7,pp. 1784-1792.
- NIST Special Publication 800-30 Revision 1, (2011). Initial Public Draft, Guide for Conducting Risk Assessments, September 2011, pp. 7-8 and Appendix D-2.
- .
- NIST Special Publication 800-30 Revision 1, (2011). Initial Public Draft, Guide for Conducting Risk Assessments, September 2011, p 9-10, and appendices G-3, H-2, I-3.
- NIST Special Publication 800-30 Revision 1, (2011). Initial Public Draft, Guide for Conducting Risk Assessments, September 2012, pp. 78 and Appendix F-2.
- S. Juuso, (2019). Master's thesis: Evaluation of Threat Modeling Methodologies A Case Study,JAMK University of Applied science.
- S.D. Applegate, A. Stavrou, (2013). Towards a Cyber Conflflict Taxonomy, 5th International Conference on Cyber Conflict, Tallinn.
- Souppaya, M. & Scarfone, K, (2016). Guide to Data-Centric System Threat Modeling (NIST Special Publication 800-154), Gaithersburg: National Institute of Standards and Technology.