Military Science and Tactics
https://www.qjmst.ir/

The Conceptual Model of the Cyber Defense Ecosystem of Iran

Alireza Keramtipour[1]✉| Reza Taghipour[2]

1. Corresponding Author, Ph. D. in Strategic Management of Cyber Space, National Defense University and Higher Research Institute, Tehran, Iran.
E-mail: a. keramatipour@sndu. ac. ir

2. A member of the faculty of the National Defense University and Higher Research Institute, Tehran, Iran.
E-mail: taghipour@sndu. ac. ir

Article Info

Article type:
Research Article

Article history:
Received
02 November 2023
Received in revised form
02 January 2024
Accepted
06 March 2024
Published online
20 September 2024

Keywords:
Cyber space, cyber security, cyber defense, cyber defense ecosystem

ABSTRACT

Objective: This research was conducted with the aim of achieving the conceptual model of the country's cyber defense ecosystem.

Method: The research is of developmental-applied type and was done with descriptive-analytical method. The statistical population included managers of strategic levels of organizations and centers related to the subject of the research, and the prominent people of this society, with the number of 44 people, constitute the sample population. First, data was collected by studying documents and interviews, then a questionnaire tool was used, the reliability of which was confirmed by calculating Cronbach's alpha. Qualitative data were analyzed by content analysis method and SPSS, UCINET and NetDraw software were used to analyze quantitative data.

Findings: Based on the data analysis, 7 important features of cyber defense, 12 effective factors and 28 main actors in the form of 7 categories and their roles in the ecosystem have been determined and the conceptual model of this ecosystem has been drawn.

Conclusion: The conceptual model was drawn in layers and in different cycles. The components placed in each layer are proportional to the focal theme of the same layer, the layers are completely perpendicular to each other and do not overlap. In this model, the organic connection between the components is seen, and Strategy shaping is done to achieve strategic advantages, and a kind of favorable conditions are seen in the ecosystem.

Cite this article: Keramtipour, Ali Reza, & Taghipour, Reza. (2024), The conceptual model of the country's cyber defense ecosystem, *Military Science and Tactics*, 20 (68), 227-252.
DOI: http//doi. org/ 10. 22034/qjmst. 2024. 2014190. 1963
Publisher: AJA Command and Staff University
DOI 10. 22034/qjmst. 2024. 2014190. 1963

فصلنامه علمی علوم و فنون نظامی
https://www.qjmst.ir/

الگوی مفهومی زیست‌بوم پدافند سایبری جمهوری اسلامی ایران

علیرضا کرامتی پور[1]✉ | رضا تقی‌پور[2]

۱. دکترای مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی، تهران، ایران.

رایانامه: a. keramatipour@sndu. ac. ir

۲. عضو هیئت‌علمی دانشگاه و پژوهشگاه عالی دفاع ملی، تهران، ایران.

رایانامه: taghipour@sndu. ac. ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت
۱۴۰۲/۰۸/۱۱
تاریخ بازنگری
۱۴۰۲/۱۰/۱۲
تاریخ پذیرش
۱۴۰۲/۱۲/۱۶
تاریخ انتشار:
۱۴۰۳/۰۶/۳۰

کلیدواژه‌ها:
فضای سایبر، زیست‌بوم، امنیت سایبری، پدافند سایبری، زیست‌بوم پدافند سایبری.

چکیده

هدف: این تحقیق با هدف دستیابی به الگوی مفهومی زیست‌بوم پدافند سایبری کشور انجام شده است.

روش: تحقیق از نوع توسعه‌ای- کاربردی بوده و با روش توصیفی- تحلیلی انجام شده است. جامعه آماری شامل مدیران سطوح راهبردی سازمان‌ها و مراکز مرتبط با موضوع تحقیق بودند که افراد شاخص این جامعه، به تعداد ۴۴ نفر جامعه نمونه را تشکیل می‌دهند. ابتدا با مطالعه اسناد و مدارک و مصاحبه، داده‌ها جمع‌آوری شد، سپس از ابزار پرسشنامه استفاده شد که پایایی آن با محاسبه آلفای کرونباخ تأیید گردید. داده‌های کیفی با روش تحلیل محتوا تجزیه‌وتحلیل شدند و از نرم‌افزارهای اس پی اس اس، یو سی آی نت و نت دراو برای تجزیه‌وتحلیل داده‌های کمی استفاده گردید.

یافته‌ها: بر اساس تجزیه‌وتحلیل داده‌ها، ۷ ویژگی مهم پدافند سایبری، ۱۲ عامل مؤثر و همچنین ۲۸ کنشگر کلیدی در قالب ۷ دسته و ۲۵ نقش عمده آن‌ها در زیست‌بوم تعیین‌شده و الگوی مفهومی این زیست‌بوم ترسیم گردیده است.

نتیجه‌گیری: الگوی مفهومی به‌صورت لایه‌ای و در چرخه‌های مختلف ترسیم شد. مؤلفه‌های جانمایی شده در هر لایه، متناسب با موضوع کانونی همان لایه بوده، لایه‌ها کاملاً عمود برهم بوده و دارای هم‌پوشانی نیستند. در این الگو، ارتباط ارگانیک بین اجزاء دیده می‌شود و شکل‌دهی راهبردی برای پرداختن به مطلوبیت‌های راهبردی انجام شده است.

استناد: کرامتی‌پور، علیرضا و تقی‌پور، رضا. (۱۴۰۳). الگوی مفهومی زیست‌بوم پدافند سایبری کشور. *علوم و فنون نظامی*، ۲۰(۶۸)، ۲۵۲- ۲۲۷.

DOI: http//doi. org/ qjmst10. 22034/qjmst. 2024. 2014190. 1963

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

DOI: 10. 22034/qjmst. 2024. 2014190. 1963

مقدمه

زیست‌بوم سایبری، به شکل‌گیری محیطی بومی، پویا و زنده سایبری اشاره دارد که بین جغرافیا، حوزه سیاسی، فرهنگی، اجتماعی، اقتصادی و دفاعی کشور تعامل ایجاد نموده و پایدار است. امروزه عمده فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشورها در زیست‌بوم فضای سایبر انجام می‌شود. زیرساخت‌های حیاتی و حساس کشورها در حکم ستون‌های سقف جامعه محسوب شده و نقش بسزایی در تداوم کارکرد اجتماعی آن‌ها ایفا می‌نماید. این زیرساخت‌ها باید امن، پایدار و غیرقابل تزلزل باشند. هرگونه اختلال یا توقف در کارکرد هر یک از زیرساخت‌های حیاتی و حساس جامعه با توجه به وابستگی متقابل زیرساخت‌ها به یکدیگر به‌سرعت به سایر زیرساخت‌ها سرایت کرده و در مدت کوتاهی کارکردهای جامعه را تحت تأثیر مستقیم قرار می‌دهد. (کافی، ۱۳۹۹: ۸) آسیب‌پذیری‌ها و تهدیدهای متنوع سایبری که متوجه زیرساخت‌های حیاتی است باعث ایجاد ناامنی و بروز چالش و اختلال در زندگی شهروندی و حتی تهدید برای امنیت ملی کشورها می‌شود و اختلال کوتاه‌مدت در این زیرساخت‌ها، آسیب‌های جدی در حوزه‌های پایداری، امنیت و ایمنی جامعه را به دنبال دارد. (پورشاسب و نظری نژاد، ۱۳۹۹: ۲۹۳) امروزه در حوزه پدافند سایبری زیرساخت‌ها، شبکه‌ها و سامانه‌های حیاتی، حساس و مهم کشور، ضعف‌هایی از قبیل پایین بودن تعامل، همگرایی و همکاری سایبری سازمان‌های کشوری و لشکری درزمینه پدافند سایبری کشور و آسیب‌پذیر بودن سامانه‌های سایبری کشور در برابر ره‌گیری، شنود و انواع حملات مختلف سایبری دشمن مشاهده می‌شود. (سپهری، ۱۴۰۰: ۱۶۷)

تنوع دیدگاه‌های فرهیختگان نسبت به تهدیدهای فضای سایبری، کم‌توجهی به استفاده از ظرفیت‌های بخش خصوصی در حوزه سایبری، فناوری‌ها و استانداردهای غیربومی در حوزه سایبری (آذر و مسلمی، ۱۴۰۱: ۶۸)، تعدد کنشگران حوزه پدافند سایبری، وجود اختلاف‌نظر میان این کنشگران و مبهم بودن نقش هر یک و روابط بین آن‌ها، باعث ایجاد مشکلاتی شده است. تدوین زیست‌بوم پدافند سایبری کشور می‌تواند مزیت‌های زیر را ایجاد کند:

- ≠ بسترسازی برای ورود منطقی تصمیم سازان و سیاست‌گذاران به حوزه پدافند سایبری
- ≠ یکپارچه‌سازی، تعامل و تعمیق همکاری و مشارکت نیروهای پدافند سایبری برای افزایش انسجام و مقاومت در حمله سایبری علیه زیرساخت‌ها

≠ کمک به افزایش قدرت تاب‌آوری زیرساخت‌های حیاتی و حساس کشور با کشف آسیب‌پذیری‌ها، چراکه تهدیدها متوجه آسیب‌پذیری‌ها هستند و در صورت کاهش آسیب‌پذیری‌ها به همان نسبت تهدیدها نیز کاهش می‌یابند.

با توجه به اسناد بالادستی مبنی بر لزوم امن‌سازی و محافظت از زیرساخت‌های حیاتی سایبری و مبتنی بر سایبر و رویکرد فعلی کشورهای متخاصم در استفاده ابزاری از حملات سایبری علیه جمهوری اسلامی ایران، ازآنجاکه زیست‌بوم، شامل مجموعه‌ای از سازمان‌های به هم وابسته و مرتبط است که به ایجاد و تخصیص ارزش می‌پردازند و شبکه کنشگران پیرامون یک فناوری مرکزی برای موفقیت و بقای خود به یکدیگر وابسته هستند. تدوین زیست‌بوم پدافند سایبری کشور امری ضروری است؛ که به ایجاد انسجام و هم‌افزایی کنشگران متعدد در حوزه پدافند سایبری کمک می‌نماید. عوامل سلبی که باعث ضرورت اجرای این تحقیق شده عبارت‌اند از:

≠ احتمال موازی‌کاری، تداخل کاری و یا کم‌کاری کنشگران که باعث هدر رفت سرمایه‌های کشور در این حوزه می‌شود.

≠ احتمال افزایش تهدیدهای متوجه زیرساخت‌های حیاتی، حساس و مهم به‌موجب وجود آسیب‌پذیری‌های نهفته در آن‌ها و احتمال غافلگیری راهبردی در حوزه پدافند سایبری و تهدید جدی علیه امنیت ملی و خدشه‌دار شدن اقتدار کشور و افزایش هزینه‌های اقتصادی و اجتماعی ناشی از آن

لذا هدف اصلی این پژوهش تدوین الگوی مفهومی زیست‌بوم پدافند سایبری کشور است. با توجه به اینکه برای رفع دغدغه‌های پیش‌گفته تاکنون در کشور پژوهش خاصی صورت نگرفته است، مسئله اصلی این پژوهش، فقدان زیست‌بوم ساختاریافته پدافند سایبری در کشور است.

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری

فضای سایبری: به شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده، کنترل‌کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین انسان و محیط به‌منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات گفته می‌شود. (سند راهبردی پدافند سایبری کشور، ۹۴)مفهوم زیست‌بوم از دیدگاه مور، سامانه‌ای است

گسترش‌یافته از سازمان‌هایی که به‌صورت متقابل از یکدیگر حمایت می‌کنند. روابط متقابل میان اعضای زیست‌بوم و حمایت آن‌ها از یکدیگر، مؤلفه‌های حائز اهمیت در هر زیست‌بوم است. دیدگاه زیست‌بومی، سازمان‌ها را در سطحی فراتر از یک واحد کسب‌وکار منفرد و در قالب عضوی از یک شبکه به‌هم‌پیوسته از واحدها و نهادهای مرتبط در نظر می‌گیرد. (زنگنه نژاد و همکاران، ۹۸: ۸) در نگرش زیست‌بومی اعتقاد بر این است که عملکرد هریک از اعضا بر سرنوشت کل زیست‌بوم تأثیر دارد و سازمان علاوه بر بهبود مستمر سطح عملکرد خود، سعی در ارتقاء سطح عملکرد شبکه و زیست‌بوم دارد. زیست‌بوم ویژگی‌هایی دارد که در ساختار و عملکرد آن سهیم است ازجمله این ویژگی‌ها سرنوشت مشترک، راهبردهای اعضا، نقش‌ها، محیط و ارتباطات متقابل است. (یاری و کوثری، ۹۸: ۵)

زیست‌بوم سایبری: زیست‌بوم سایبری متشکل از مجموعه‌ای از موجودیت‌ها است که در یک محیط سایبری با هم تعامل دارند. استعاره "زیست‌بوم" اگرچه کامل نیست، اما به‌درستی ویژگی‌های مهم فضای سایبر را توصیف می‌کند. فضای سایبری پویا است و شرکت‌کنندگان متنوع آن به روش‌های پیچیده با یکدیگر ارتباط دارند. در یک زیست‌بوم سایبری ایمن و انعطاف‌پذیر، کنشگران با هم همکاری می‌کنند تا حملات سایبری را پیش‌بینی و از آن جلوگیری کنند و یا گسترش و پیامدهای حملات را محدود کنند.

زیست‌بوم امنیت سایبری: امنیت سایبری شامل یک چرخه مداوم از اقدامات ساختاریافته برای موارد زیر است:

- ≠ شناسایی[1] (درک وضعیت و خطرات سامانه‌ها، دارایی‌ها، داده‌ها و قابلیت‌ها)
- ≠ محافظت[2] (اجرای تدابیر حفاظتی و اقدامات تأمینی مناسب به‌منظور حفظ و مصون‌سازی دارایی‌ها)
- ≠ کشف و تشخیص[3] (اجرای توانایی تشخیص یک رخداد امنیت سایبری)
- ≠ پاسخ[4] (پیاده‌سازی توانایی انجام اقدام پس از یک رخداد امنیت سایبری)
- ≠ بازیابی[1] (اجرای انعطاف‌پذیری و بازیابی توانایی‌های آسیب‌دیده)

[1] Identify
[2] Protect
[3] Detect
[4] Respond

همه این فعالیت‌ها، به اشتراک‌گذاری به‌موقع و مطمئن اطلاعات ساختاریافته مرتبط، متکی هستند. یک زیست‌بوم امنیت سایبری از سطوح جهانی، منطقه‌ای، ملی و محلی تا کسب‌وکارهای کوچک و افراد تشکیل می شود. همه کسانی که در زیست‌بوم دخیل هستند به دنبال راه‌حل‌هایی برای محافظت از یکپارچگی و در دسترس بودن ارتباطات و اطلاعات خود تا حد امکان و در محدوده هزینه هستند. (**ETSI TR V1. 4. 1 (2020-03)**)

شکل (۱) اجزای اصلی زیست‌بوم امنیت سایبری (ETSI TR V1. 4. 1 (2020-03

امنیت سایبری: عبارت است از حاکمیت، توسعه، مدیریت و استفاده از امنیت اطلاعات، امنیت فناوری عملیاتی و ابزارها و روش‌های امنیت فناوری اطلاعات برای دستیابی به انطباق با مقررات، دفاع از دارایی‌ها و به خطر انداختن دارایی‌های.

شکل (۲) اجزای امنیت سایبری (A. Walls, Perkins E, Weiss J. Definition 2013)

[1] Recover

امنیت سایبری از اجزای زیر تشکیل‌شده است:

۱. مجموعه‌ای از شیوه‌های تجسم‌یافته در امنیت فناوری اطلاعات، امنیت اطلاعات، امنیت فناوری عملیات و امنیت تهاجمی است.

۲. ابزارها و فن‌های امنیت فناوری اطلاعات، امنیت فناوری عملیاتی و امنیت اطلاعات برای به حداقل رساندن آسیب‌پذیری‌ها، حفظ یکپارچگی سامانه، اجازه دسترسی فقط به کاربران تائید شده و دفاع از دارایی‌ها استفاده می‌کند.

۳. توسعه و استفاده از حملات تهاجمی مبتنی بر فناوری اطلاعات یا فناوری عملیاتی علیه دشمنان

۴. اهداف تضمین اطلاعات در یک زمینه دیجیتال پشتیبانی می‌کند اما به امنیت رسانه آنالوگ (به‌عنوان‌مثال، اسناد کاغذی) گسترش نمی‌یابد.

پدافند سایبری: حوزه مشترک امنیت ملی و امنیت سایبری است. امنیت سایبری، یکی از پایه‌های کلیدی پدافند سایبری است. (SUHYEON, SEUNGJOO, 2018)

شکل (۳) پدافند سایبری و روابط آن با امنیت ملی (دفاع)، امنیت سایبری و امنیت اطلاعات (SUHYEON, SEUNGJOO, 2018)

پیشرفت فناوری اطلاعات و شبکه‌های رایانه‌ای باعث شد تا نظام سلسله‌مراتب ارتشی در معنای قدیمی خود منسوخ‌شده و روابط در نیروهای نظامی نیز به وضعیت شبکه‌ای شبیه شود تا اینکه مبتنی بر سلسله‌مراتب رسمی باشد. (نقوی و مختار زاده، ۱۴۰۰: ۷۲) زیست‌بوم و نظام مفاهیمی هستند که بحث‌هایی زیادی در مورد تشابه و تفاوت آن‌ها مطرح‌شده است. برخی محققان معتقدند که اضافه شدن واژه اکو به ابتدای سیستم، چیز خاصی را به آن اضافه نکرده است. بااین‌حال بررسی مطالعات مختلف صورت گرفته در حوزه زیست‌بوم حاکی از آن است که به‌طورکلی دو رویکرد متفاوت نسبت به زیست‌بوم

وجود دارد: ۱. زیست‌بوم واقعی فضای کسب‌وکار و ۲. زیست‌بوم در سطح ملی، منطقه‌ای که منشأ این دو باهم تفاوت دارد. این دو رویکرد ناشی از دو نگرش متفاوت نسبت به مفهوم زیست‌بوم است. در رویکرد اول که منطبق با تعریف مور است زیست‌بوم در سطح عملیاتی و راهبردی مورداستفاده قرار می‌گیرد در زیست‌بوم با توجه به اینکه بازیگران و روابط بین آن‌ها به‌طور مداوم در حال تکامل است بنابراین مرز آن شناور بوده و تعیین یک مرز مشخص برای آن تا حد زیادی امکان‌پذیر نیست. ازنظر مور، زیست‌بوم در حوزه کسب‌وکار دارای چرخه عمر است و به‌مرورزمان توسعه می‌یابد تا به مرحله بلوغ خود برسد و در انتها نیز با توجه به تغییرات محیطی، از بین می‌رود و یا ساختار خود را بازسازی می‌کند. در همین راستا محققان مختلف در مطالعات خود به ویژگی چرخه عمر زیست‌بوم اشاره‌کرده‌اند و تحلیل‌های خود را بر اساس چرخه عمر زیست‌بوم انجام داده‌اند. زیست‌بوم اشاره به مجموعه‌ای از سازمان‌ها و نهادهایی دارد که فعالیت خود را حول یک سازمان یا سکوی مرکزی انجام می‌دهند. در این راستا محققان متعددی اشاره‌کرده‌اند که زیست‌بوم دارای یک هسته و مرکز است (هسته می‌تواند شامل یک یا چند نهاد باشد) با توجه به اینکه زیست‌بوم در سطح عملیاتی و راهبردی به کار گرفته می‌شود و همچنین به موضوع خلق ارزش به‌صورت مشترک توسط بازیگران توجه می‌کند بنابراین نسبت به نظام توجه بیشتری به تعاملات اجتماعی بین بازیگران دارد. (خالدی، ۱۳۹۶: ۱۳)

شکل (۴) تفاوت نظام و زیست‌بوم (خالدی، ۱۳۹۶: ۱۳)

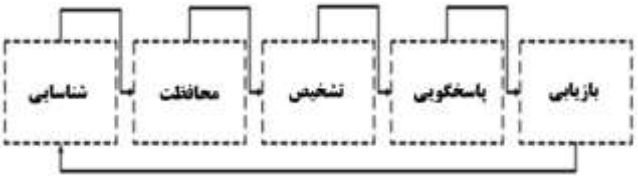
تهدیدهای سایبری زیرساخت‌ها در سه حوزه منابع انسانی، فرایندها و فناوری‌ها قابل‌بررسی است. این تهدیدها در جدول زیر در یک نگاه مقابل هم قرارگرفته‌اند.

جدول (۱) تهدیدهای سایبری، پیامدها و آسیب‌پذیری‌ها (کافی، ۱۳۹۹: ۱۲)

تهدید و پیامد	آسیب‌پذیری منابع انسانی	آسیب‌پذیری فرایندها	آسیب‌پذیری فناوری
≠ اختلال، بهره‌برداری و یا قطع ارتباط ≠ پیامد: نقض یکپارچگی و دسترسی	≠ ضعف آموزش و آگاه‌سازی ≠ نیروی غیرمتعهد یا غیربومی	≠ خلأ سیاست دفاعی – امنیتی ≠ خلأ آیین‌نامه‌های مقابله با سناریوهای احتمالی تهدید ≠ حیطه عملکرد وسیع و وابستگی متقابل زیرساخت‌ها ≠ ضعف در چندلایه‌سازی و پدافند در عمق	≠ فعالیت در بستر اینترنت ≠ وجود سخت‌افزار و نرم‌افزار غیربومی ≠ خلأ آزمایشگاه تشخیص بدافزار ≠ خلأ رمزنگاری داده‌ها و فایروال
≠ منع ارائه خدمات ≠ پیامد: نقض دسترسی	≠ ضعف آموزش و آگاه‌سازی ≠ نیروی غیرمتعهد یا غیربومی	≠ خلأ سیاست دفاعی – امنیتی ≠ خلأ آیین‌نامه‌های مقابله با سناریوهای احتمالی تهدید ≠ حیطه عملکرد وسیع و وابستگی متقابل زیرساخت‌ها ≠ ضعف در چندلایه‌سازی و پدافند در عمق	≠ وجود سخت‌افزار و نرم‌افزار غیربومی ≠ خلأ آزمایشگاه تشخیص بدافزار ≠ سامانه عامل غیربومی و خلأ فایروال
≠ افشاء و یا سرقت اطلاعات حساس و مهم ≠ پیامد: نقض محرمانگی	≠ ضعف آموزش و آگاه‌سازی ≠ نیروی غیرمتعهد یا غیربومی	≠ خلأ سیاست دفاعی – امنیتی ≠ خلأ آیین‌نامه‌های مقابله با سناریوهای احتمالی تهدید ≠ حیطه عملکرد وسیع و وابستگی متقابل زیرساخت‌ها ≠ ضعف در چندلایه‌سازی و پدافند در عمق	≠ فعالیت در بستر اینترنت ≠ وجود سخت‌افزار و نرم‌افزار غیربومی ≠ خلأ آزمایشگاه تشخیص بدافزار ≠ خلأ رمزنگاری داده‌ها و فایروال

چرخهٔ امنیت سایبری

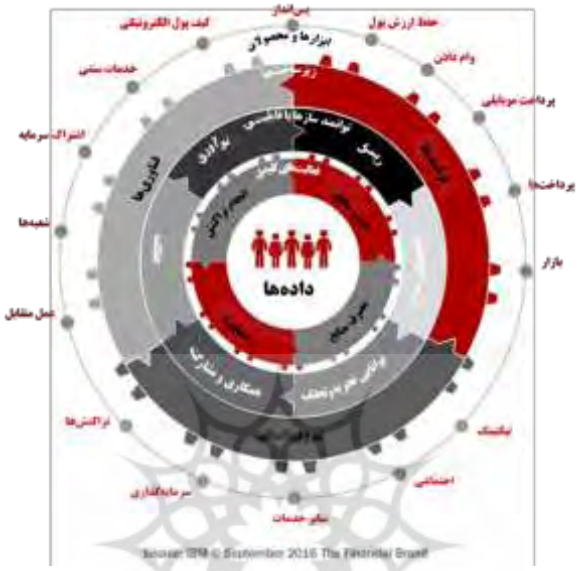
طبق چارچوب NIST، چرخه حیات راهبردهای کاهش تهدیدات سایبری شامل پنج مرحله است: شناسایی، محافظت، تشخیص، پاسخ و بازیابی. هر یک از این مراحل نقش حیاتی در امنیت سایبری پایدار دارد.



شکل (۵) چرخه حیات امنیت سایبری (Shahrin, Mohiuddin, Leslie, 2020)

نمونه زیست‌بوم حوزه سایبر (زیست‌بوم بانکداری دیجیتال)

این زیست‌بوم از ۵ لایه اصلی تشکیل شده است. لایه مربوط به داده‌ها، فعالیت‌های کلیدی، توانمند سازها یا قابلیت‌ها، زیرساخت‌ها و درنهایت ابزارها و محصولات تشکیل‌دهنده اجزای اصلی این الگو هستند.



شکل (۶) زیست‌بوم بانکداری دیجیتال (sabapardazesh. net)

هسته اصلی این زیست‌بوم را داده‌ها شکل داده‌اند. تمامی لایه‌های دیگر این زیست‌بوم مبتنی بر همین داده‌ها، طرح‌ریزی و پیاده‌سازی می‌شوند. بر همین اساس، سطح دسترسی، کیفیت، جامعیت، به‌روز بودن و صحت این داده‌ها نقش بسزایی در ایجاد یک نظام بانکداری دیجیتال کارآمد ایفا می‌نماید. با عنایت به اینکه جذب منابع، مصرف منابع، انجام تراکنش و مشاوره، چهار فعالیت اصلی کسب‌وکار بانکداری به شمار می‌روند، همین کارکردها را باید در حوزه بانکداری دیجیتال نیز مدنظر قرار داد.

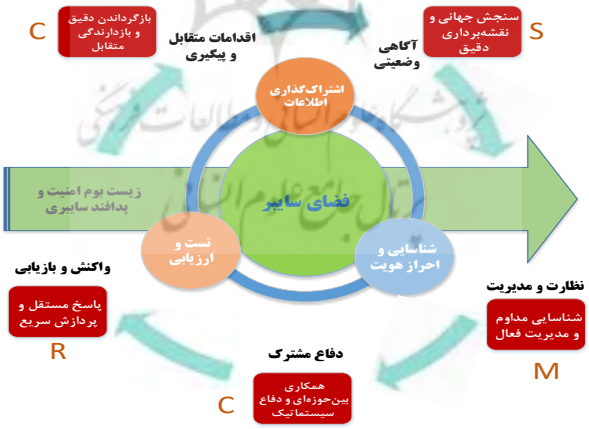
توانایی تجزیه‌وتحلیل، نوآوری، ریسک، چابکی، همکاری و مشارکت، دیجیتالی شدن، اجزای اصلی تشکیل‌دهنده لایه توانمند سازها و قابلیت مورد انتظار در ایجاد زیست‌بوم بانکداری دیجیتال است.

به‌صورت کلی برای پیشبرد راهبردهای مربوط به فعالیت‌های اصلی بانکداری دیجیتال، ۳ منبع اصلی موردتوجه قرار گرفته است. منابع انسانی، فناوری و فرآیند اجزای اصلی این لایه را تشکیل می‌دهند.

عناصر لایه ابزارها محصولات به‌شرط پیاده‌سازی لایه‌های درونی، دنیایی از فرصت‌های مزیت آفرین را پیش روی بانکداری دیجیتال نمایان می‌سازد. دیگر موضوعات در بانکداری دیجیتال از ابزارها، کانال‌ها، ارتباطات تا محصولات و خدمات و ... در لایه پنجم موردتوجه قرار می‌گیرند. ارزش‌آفرینی در زیست‌بوم بانکداری دیجیتال در این لایه تحقق می‌یابد. بااین‌حال این فرصت‌ها و ظرفیت‌ها متأثر و معلول ساخت لایه‌ها درونی هستند. همچنین تمایز و تفاوت‌ها از کیفیت و نحوه ساختار این زیست‌بوم نشئت می‌گیرد. همچنین این زیست‌بوم به‌سرعت در حال دگرگونی و تغییر است بدان معنی که هر تغییری در لایه‌های درونی، کل زیست‌بوم را تحت‌الشعاع قرار داده و به نتایج متفاوتی منجر خواهد شد. از سوی دیگر تعامل زیست‌بوم با محیط، فعالیت آن و ارتباط اجزا به خلق داده‌های جدیدی منجر خواهد شد که بر کلیت آن اثر خواهد گذاشت.

نمونه زیست‌بوم امنیت سایبری

زیست‌بوم امنیتی فضای سایبری بر اساس حلقه آگاهی از وضعیت، نظارت و مدیریت، دفاع مشترک، واکنش و بازیابی و اقدامات متقابل و پیگیری[1] در شکل زیر نشان داده شده است. در داخل این زیست‌بوم، از طریق سه سامانه عامل پشتیبانی (یک سامانه اشتراک اطلاعات، یک سامانه شناسایی هویت و یک سامانه آزمایش و ارزیابی)، توابع مختلف امنیت فضای سایبری به‌صورت ارگانیک ادغام شده و یک زیست‌بوم امنیتی فضای سایبری پویا را تولید می‌کنند.



شکل (۷ زیست‌بوم امنیتی فضای سایبری بر اساس حلقه SMCRC. (NiuYanga, Xiao-Feng, XuaGuo-RongPangb, & Chun-LeiZhanga, 2018)

[1] SMCRC

در حلقه SMCRC داده‌ها همیشه جریان دارند. این حلقه می‌تواند تمام منابع امنیتی فضای سایبری را ادغام کند، بنابراین یک محیط وابسته و تلفیقی را امکان‌پذیر می‌کند. حلقهS (آگاهی از وضعیت) داده‌های آگاهی از وضعیت را به M (نظارت و مدیریت) ارائه می‌دهد. M اطلاعات هشداردهنده اولیه را به C (دفاع مشترک) ارائه می‌دهد. C پیش‌شرط R (پاسخ و بازیابی) است و از یک پاسخ خودکار و سریع پشتیبانی می‌کند. R پایگاه داده نمونه حمله سایبری را به C دوم (اقدامات متقابل و پیگیری) ارائه می‌دهد، انتساب دقیق و اقدامات متقابل را امکان‌پذیر می‌کند؛ و C دوم اطلاعات تهدید و نتایج مقابله با S را فراهم می‌کند.

پیشینه‌های پژوهش

رامک و همکاران (۱۳۹۵) در مطالعات گروهی دانشکده امنیت ملی دانشگاه و پژوهشگاه عالی دفاع ملی پژوهشی با عنوان: "طراحی نظام دفاع سایبری کشور و تدوین الزامات تحقق آن" انجام دادند که طی آن الگوی مفهومی دفاع سایبری احصا شده، سپس با استفاده از چارچوب زکمن ۱۸ فرایند و ۲۸ نهاد برای ساختار نظام دفاع سایبری تعیین گردیده است و در ادامه تعداد فرایندها به ۱۲ و نهادها به ۱۴ مورد کاهش یافته است. از روش‌های الگوسازی ساختاری تفسیری[1] و تحلیل میک مک[2] برای تجزیه‌وتحلیل و نهایتاً سطح‌بندی نهادها در هر فرایند استفاده شده است.

اسماعیلی (۱۳۹۷)، در رساله دکتری خود که در دانشکده امنیت ملی دانشگاه و پژوهشگاه عالی دفاع ملی با عنوان: "طراحی الگوی پایش تهدیدات سایبری با رویکرد آینده‌پژوهی" انجام داد، بخشی از فرایند پدافند سایبری را معرفی نموده است. به‌گونه‌ای که در حوزه رصد و پایش تهدیدات سایبری نهادها و متولیان اصلی را احصا نموده و نقش هر یک را تعیین نموده است. همچنین برای تحلیل محیط پایش تهدیدات سایبری از الگوی فری‌من استفاده نموده است.

تقی پور و امیرلی (۱۳۹۹) در مقاله‌ای با عنوان: "ارائه الگوی فرایندی دفاع سایبری بومی" با بهره‌گیری از روش موردی زمینه‌ای، اسناد بالادستی کشور را موردمطالعه قرار داده و با گزینش چند کشور، اسناد راهبردی قابل‌دسترس این کشورها را نیز بررسی نموده و با ورود گزاره‌های استخراج‌شده از آن‌ها در سطح راهبردی، چارچوب معماری زکمن و با بهره‌گیری از دانش خبرگان این حوزه از طریق مصاحبه و پرسشنامه،

[1] ISM
[2] MICMAC

فرایندهای کلیدی دفاع سایبری احصاء و با استفاده از روش الگوی ساختاری تفسیری و مقایسه‌ای زوجی، این فرایندها سطح‌بندی و ارتباط بین آن‌ها ترسیم و الگوی نهایی را ارائه نموده‌اند.

ژائو نیویانگا، وی وانگا، فنگ ژواگو، رانگ پانگبچون، لی ژانگا۱ (۲۰۱۸) مقاله "تحقیق در مورد ساخت یک زیست‌بوم امنیتی جدید فضای مجازی" را در آکادمی مهندسی چین، مجله مهندسی، شماره ۴، صفحه ۴۷ تا ۵۲، فوریه ۲۰۱۸ به چاپ رسانده‌اند. این مقاله فضای مجازی را به سه زیر فضا تقسیم می‌کند: شبکه‌های عمومی مشترک (فضای C)، شبکه‌های طبقه‌بندی‌شده ایمن (فضای S) و شبکه‌های زیرساختی کلیدی (فضای K) ارائه شده است. مطابق با ویژگی‌های منحصربه‌فرد و الزامات امنیتی خود، به‌منظور حل مشکلات در فضای مجازی به‌صورت مرحله‌ای. تمرکز اصلی فضای C بر ایجاد یک زیست‌بوم و اطمینان از امنیت خدمات است. برای فضای S، تمرکز بر ساخت شبکه‌های داخلی و تضمین امنیت اطلاعات است. برای فضایK ، تمرکز بر انجام محافظت فعال و اطمینان از امنیت برنامه است.

سادیک و همکاران (۲۰۲۰) در تحقیقی با عنوان: "به‌سوی یک زیست‌بوم امنیت سایبری پایدار"، روش‌هایی را برای انطباق با تدابیر امنیتی پیشرفته برای پیشگیری و کاهش تهدیدات سایبری موردبحث قرار می‌دهند. علاوه بر این، روندهای نوظهور نیز موردبحث قرار می‌گیرد. راه‌حل‌های امنیت سایبری با استفاده از هوش مصنوعی و یادگیری ماشین نیز همراه با الگوی امنیت سایبری جامعه موردبحث قرار گرفته است.

زنگنه نژاد همکاران (۱۳۹۸)، در مقاله‌ای با عنوان: " زیست‌بوم ارتباطات سیار در ایران مبتنی بر روش تحلیل شبکه‌های اجتماعی" بازیگران کلیدی این زیست‌بوم ارتباطات سیار ایران را شناسایی نموده و ترسیم شبکه روابط موجود میان این بازیگران کلیدی و تحلیل شبکه فوق توسط نرم‌افزار یو سی آی نت مهم‌ترین دستاورد این پژوهش به شمار می‌رود.

در پژوهش‌های انجام‌شده بالا، به برخی از موضوعات زیست‌بوم نظیر بازیگران، روابط، فرایندها، مؤلفه‌ها و متغیرهای زیست‌بوم‌های مشابه نظیر زیست‌بوم امنیت سایبری، زیست‌بوم دفاع سایبری، زیست‌بوم فناوری‌های نوین و... که مرتبط با موضوع این تحقیق است، اشاره شده است و در این تحقیق قابل‌استفاده است؛ اما در هیچ‌کدام از آن‌ها،

[1] NiuYanga, Xiao-Feng, XuaGuo-RongPangb, & Chun-LeiZhanga, 2018

به‌وضوح به زیست‌بوم پدافند سایبری پرداخته نشده است و این موضوع، نوآوری تحقیق محسوب می‌شود.

روش‌شناسی پژوهش

چون این تحقیق به تدوین الگوی مفهومی زیست‌بوم پدافند سایبری کشور می‌پردازد و نتایج آن برای تصمیم‌گیری کاربرد خواهد داشت، به لحاظ هدف توسعه‌ای - کاربردی می‌باشد. روش تحقیق، کمی و کیفی (آمیخته) بوده است و در پژوهش، از روش‌های مختلف کیفی مانند انجام مصاحبه عمیق با خبرگان، برگزاری نشست خبرگی و تحلیل محتوا استفاده شده است. همچنین با مرور نظام‌مند ادبیات، مطالعه گسترده‌ای راجع به‌عنوان تحقیق انجام‌شده و همچنین پرسشنامه طراحی و بین جامعه نمونه توزیع شده است و با استفاده از نرم‌افزارهای آماری اکسل و اس‌پی‌اس‌اس و نرم‌افزار تحلیل شبکه یوسی‌آی‌نت[1] و مصورساز نت‌دراو[2]، کنشگران کلیدی، نقش‌های عمده، عوامل تأثیرگذار، روابط و کارکردهای زیست‌بوم مشخص شده و الگوی مفهومی پژوهش تدوین گردید.

قلمرو تحقیق (زمانی، مکانی و موضوعی)

قلمرو موضوعی: این تحقیق به مباحث مرتبط با فضای سایبری کشور (مشخصاً در این تحقیق، منظور از فضای سایبر، دارایی‌های سایبری زیرساخت‌ها، شبکه‌ها و سامانه‌های حیاتی، حساس و مهم کشور است و به آن حوزه پرداخته شده است)، مفاهیم و ویژگی‌های زیست‌بوم‌ها با تمرکز بر زیست‌بوم پدافند سایبری می‌پردازد.

قلمرو مکانی: کشور جمهوری اسلامی ایران

قلمرو زمانی: با توجه به ماهیت فضای سایبر و تغییرات سریع آن و تنوع تهدیدات، قلمرو زمانی پژوهش از سال ۱۳۹۵ تا سال ۱۴۰۲ در نظر گرفته می‌شود.

جامعه آماری

ویژگی جامعه آماری: داشتن تخصص، تجربه و فعالیت در حوزه‌های امنیت و پدافند سایبری و حداقل ۵ سال سابقه مفید و مسئولیت در سطح راهبردی پدافند سایبری کشور

حجم جامعه آماری تحقیق: خبرگان شامل فرماندهان، معاونین یا مدیران سطوح راهبردی سازمان‌ها و مراکز مرتبط با موضوع تحقیق که حداقل دارای مدرک تحصیلی کارشناسی ارشد بوده و سابقه مفید و مسئولیت در سطح راهبردی پدافند سایبری کشور داشته باشند.

---

[1] UCINET Version ٦,٥٢٨

[2] NetDraw ٢,١٤١

همچنین اساتیدِ عضو هیئت‌علمی رشته‌های مدیریت راهبردی امنیت و پدافند فضای سایبر که افراد شاخص این جامعه، جامعه آماری تحقیق را تشکیل می‌دهند. توزیع فراوانی جامعه آماری برحسب مدرک تحصیلی، سابقه مدیریت و میزان آشنایی به شرح زیر است:

جدول (۲) فراوانی سطح تحصیلات پرسش‌شوندگان

تحصیلات	فراوانی	درصد فراوانی
کارشناسی ارشد	۶	۱۴
دانشجوی دکتری	۲۴	۵۴
دکتری	۱۴	۳۲
جمع	۴۴	۱۰۰

جدول (۳) فراوانی سابقه مدیریت پرسش‌شوندگان

سابقه مدیریت در مشاغل راهبردی	فراوانی	درصد فراوانی
بین ۵ تا ۱۰ سال	۱۱	۲۵
بین ۱۰ تا ۱۵ سال	۱۴	۳۲
بیش از ۱۵ سال	۱۹	۴۳
جمع	۴۴	۱۰۰

جدول (۴) فراوانی میزان آشنایی پرسش‌شوندگان با حوزه پدافند سایبری

میزان آشنایی با پدافند سایبری	فراوانی	درصد فراوانی
متوسط	۶	۱۴
زیاد	۲۳	۵۳
خیلی زیاد	۱۵	۳۳
جمع	۴۴	۱۰۰

به‌منظور تعیین پایایی پرسش‌نامه، با استفاده از نرم‌افزار اس‌پی‌اس‌اس، آلفای کرونباخ محاسبه‌شده و میزان آن ۰/۹۵۴ می‌باشد و این نشان‌گر پایایی پاسخ‌های ارائه‌شده است.

تجزیه‌وتحلیل داده‌ها

پس از مطالعات نظری صورت گرفته و مصاحبه‌های انجام‌شده با خبرگان حوزه پدافند سایبری علاوه بر دستیابی به نتایج موردنظر، با راهنمایی و هم‌فکری نخبگان و اساتید راهنما و مشاور، دو نوع پرسشنامه برای این تحقیق طراحی گردید. در پرسشنامه اول، مهم‌ترین ویژگی‌ها، عوامل مؤثر عمده، کنشگران کلیدی، نقش‌ها و کارکردهای مهم زیست‌بوم پدافند سایبری کشور در قالب ۷۲ سؤال از جامعه نمونه پرسیده شده است و برای تحلیل داده‌های پرسشنامه از نرم‌افزارهای اکسل ۲۰۱۹ و اس‌پی‌اس‌اس ۶۴ بیتی نسخه ۲۶ استفاده شده است. در پرسشنامه دوم نیز ارتباط بین کنشگران کلیدی زیست‌بوم پدافند سایبری در قالب

دو ماتریس ۲۸*۲۸ و ۲۸*۲۵ از تعداد ۵ نفر از خبرگان در قالب پانل تخصصی پرسیده شد و از نرم‌افزار تحلیل شبکه یوسی‌آی‌نت و مصورساز نت‌دراو برای تحلیل و نمایش داده‌های ماتریس‌ها استفاده شده است.

متغیرهای پرسشنامه پژوهش

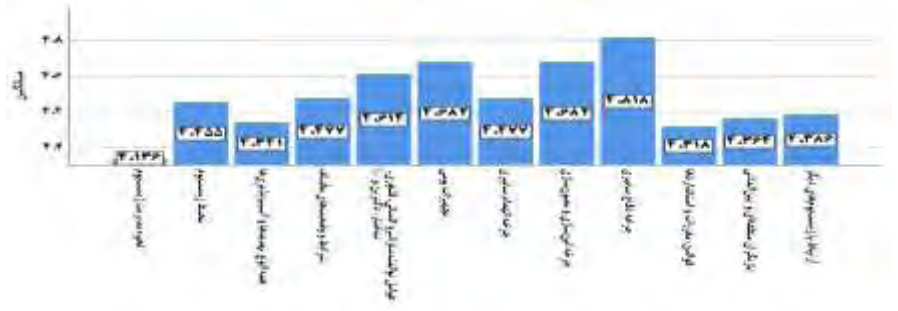
داده‌های پرسشنامه‌ی پژوهش ازلحاظ توصیفی مورد ارزیابی قرارگرفته است در ابتدا آمار توصیفی متغیرهای جمعیت شناختی را بیان نموده و پس‌ازآن متغیرهای پرسشنامه پژوهش توصیف می‌گردند.

مهم‌ترین ویژگی‌های پدافند سایبری:

پس از انجام مطالعه نظری و مصاحبه‌ها با خبرگان ویژگی‌های زیادی برای پدافند سایبری احصاء شد که به‌تدریج در فرایند پژوهش تعدیل شده و درنهایت 7 ویژگی اصلی انتخاب گردیدند که از پرسش‌شوندگان خواسته شد که میزان موافقت خود با هر یک از ویژگی‌ها را در قالب طیف لیکرت اعلام نمایند. جامعه نمونه تمامی ویژگی‌ها را با میزان موافقت زیاد و خیلی زیاد تأیید نمودند که میانگین پاسخ‌های ارائه‌شده به شرح نمودار زیر است:

نمودار (۱) نظر پاسخ‌دهندگان به سؤالات ویژگی‌های پدافند سایبری

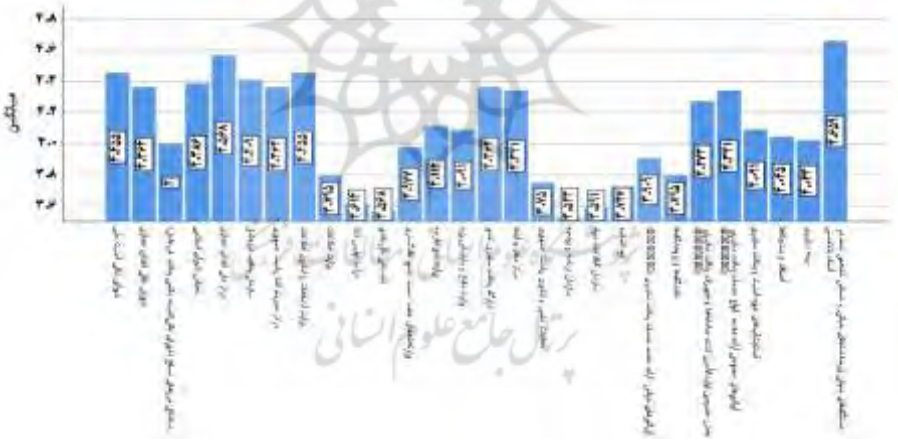
عوامل متعددی در زیست‌بوم پدافند سایبری کشور تأثیرگذارند که با مطالعه دقیق صورت گرفته و انجام مصاحبه با خبرگان درنهایت ۱۲ عامل عمده تعیین گردیدند که جامعه نمونه تمامی ویژگی‌ها را با میزان موافقت زیاد و خیلی زیاد تأیید نمودند که میانگین پاسخ‌های ارائه‌شده به شرح نمودار زیر است:



نمودار (۲) نظر پاسخ‌دهندگان به سؤالات عوامل مؤثر در زیست‌بوم پدافند سایبری کشور

کنشگران کلیدی زیست‌بوم پدافند سایبری

کنشگران کلیدی زیست‌بوم پدافند سایبری کشور با بررسی همه‌جانبه صورت گرفته و کسب نظر خبرگان در دو سطح راهبردی (سیاست‌گذاران، قانون‌گذاران، کارگزاران) و عملیاتی – اجرایی (بخش دولتی – حاکمیتی،بخش خصوصی، جامعه مدنی و متولیان زیرساخت‌های حیاتی و حساس کشور) دسته‌بندی شده و در مجمع ۲۸ کنشگر کلیدی برای این زیست‌بوم تعیین گردیدند که جامعه نمونه تمامی کنشگران را تأیید نمودند. میانگین پاسخ‌های ارائه‌شده به شرح نمودار زیر است:

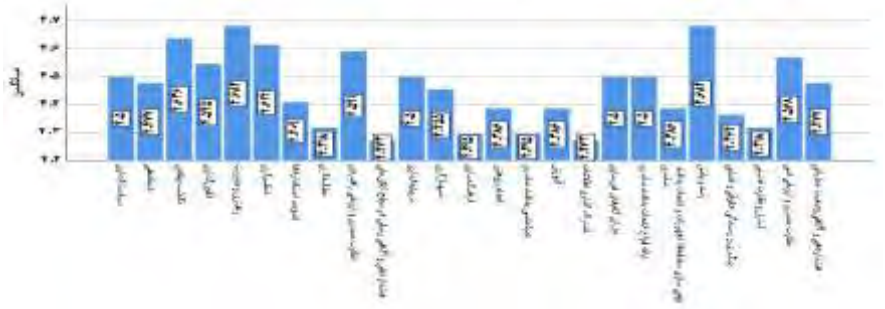


نمودار (۳) نظر پاسخ‌دهندگان به سؤال کنشگران کلیدی زیست‌بوم پدافند سایبری کشور

نقش‌های کنشگران کلیدی زیست‌بوم پدافند سایبری کشور:

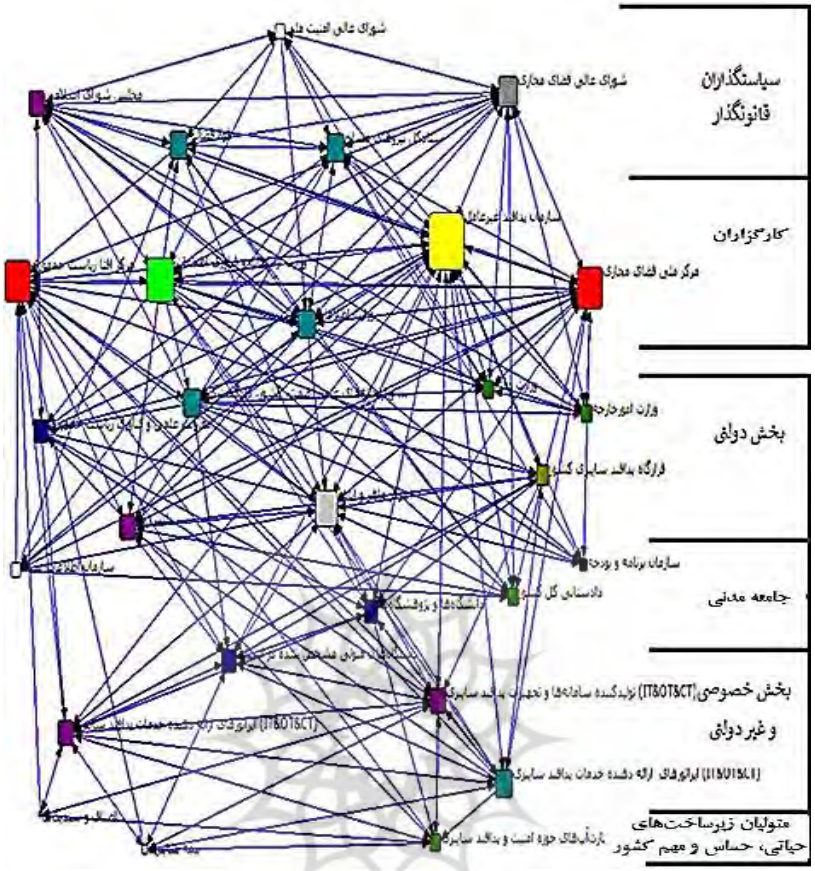
پس از مطالعه صورت گرفته و مصاحبه‌های انجام‌شده نقش‌های زیادی برای کنشگران این زیست‌بوم احصاء شد که به‌تدریج در فرایند پژوهش تعدیل شده و درنهایت ۲۵ نقش اصلی (در سطح راهبردی و عملیاتی – اجرایی) انتخاب گردیدند که در قالب ۲۵ سؤال از جامعه

نمونه پرسیده شده است و جامعه نمونه تمامی نقش‌ها را تأیید نمودند. پاسخ‌ها به شرح زیر است:

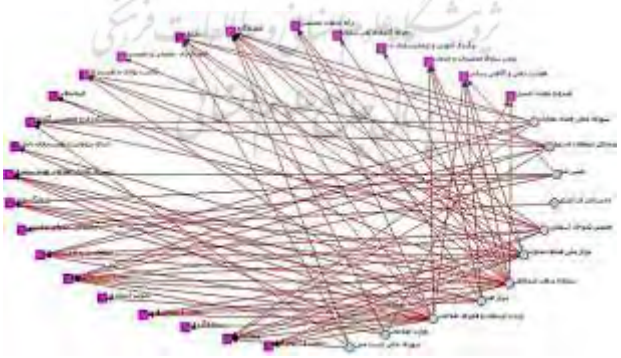


نمودار (۴) نظر پاسخ‌دهندگان به سؤالات نقش‌های کنشگران کلیدی زیست‌بوم

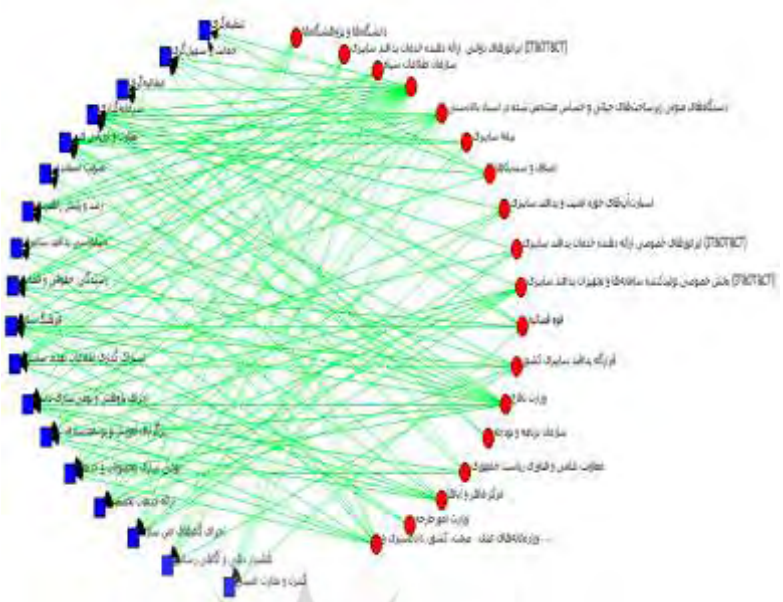
به‌منظور دسته‌بندی کنشگران و دستیابی به ارتباطات بین کنشگران کلیدی زیست‌بوم‌بخش دوم پرسشنامه در قالب ماتریس ارتباط بین کنشگران کلیدی و کنشگران با نقش‌های احصاء شده طراحی شده و در جلسه خبرگی موردبررسی و تعیین ارتباطات قرار گرفت. محتوای ماتریس‌ها به کمک نرم‌افزار یوسی‌آی‌نت مورد تحلیل قرار گرفته است. همچنین
شبکه روابط میان کنشگران کلیدی زیست‌بوم پدافند سایبری کشور که برگرفته ازنظر خبرگان است، توسط نرم‌افزار نت‌دراو ترسیم شده و در شکل‌های زیر آورده شده است.



شکل (۸) دسته‌بندی و ارتباطات کنشگران کلیدی زیست‌بوم پدافند سایبری کشور



شکل (۹) شبکه روابط میان کنشگران کلیدی (بخش راهبردی) با نقش‌های مرتبط



شکل (۱۰) شبکه روابط میان کنشگران کلیدی (بخش عملیاتی) با نقش‌های مرتبط

نتیجه‌گیری و پیشنهادها

در این پژوهش، فضای سایبری کشور معادل فضای سایبری زیرساخت‌های حیاتی، حساس و مهم در نظر گرفته‌شده و در این تحقیق بیشتر به ابعاد اطلاعاتی و فیزیکی پرداخته شده است. برای تدوین الگوی مفهومی زیست‌بوم پدافند سایبری کشور از رویکرد آمیخته (کمی – کیفی) استفاده شده وبخش های مختلف این الگو در فرایند تحقیق کامل شده و نظرات خبرگان در آن اعمال شده است.

نتیجه تجزیه‌وتحلیل داده‌های به‌دست‌آمده درخصوص سؤالات پژوهش به شرح زیر است:

جدول (۵) ویژگی‌های مهم پدافند سایبری

ویژگی‌های مهم پدافند سایبری
پدافند سایبری بیشتر با زیرساخت‌ها و دارایی‌های حیاتی، حساس، مهم و قابل حفاظت کشور و تداوم کارکرد، پایداری و تاب‌آوری آن ارتباط دارد و باعث کاهش آسیب‌پذیری‌ها می‌گردد.
پدافند سایبری همه‌ی طیف‌های تهدیدهای متصور برای دارایی‌های سایبری را اعم از تهدیدات سایبری، الکترومغناطیسی، سایبر الکترونیکی، جانمایی و مکان‌یابی سرمایه و... را موردتوجه قرار می‌دهد.
پدافند سایبری بر معماری موزاییکی و ماژولار تأکید دارد. تا در صورت وقوع تهدید بتوان به‌سرعت‌بخش آسیب‌دیده را جدا نموده و پایداری کل سامانه تحت‌الشعاع قرار نگیرد.
پدافند سایبری نیازمند بهره‌گیری گسترده از فناوری‌های نوین نظیر هوش مصنوعی، یادگیری عمیق و... و خودکارسازی

ویژگی‌های مهم پدافند سایبری
بخشی از فرایندها است.
پدافند سایبری بیشتر جنبه اقدامات دفاعی سایبری دارد تا امنیتی و ضد امنیتی (جاسوسی و ضد جاسوسی و...)
در پدافند سایبری نیاز به داشتن سرعت‌عمل خیلی بالاتر نسبت به سایر انواع پدافند زمینی یا هوایی است.
سختی در قابلیت ردیابی مهاجمان در پدافند سایبری و پایین بودن احتمال تنبیه یا بازخواست اقدام‌های مجرمانه به دلیل ضعف در قوانین ملی و بین‌المللی در فضای سایبری

جدول (۶) عوامل عمده مؤثر در زیست‌بوم پدافند سایبری کشور

عوامل عمده مؤثر در زیست‌بوم پدافند سایبری کشور
نحوه مدیریت زیست‌بوم متناسب با چرخه عمر آن (سلسله مراتبی، ارتباطی، ترکیبی و...)
محیط زیست‌بوم که به سطوح مختلف (ملی، منطقه‌ای، دستگاهی و...) و یا ازنظر ماهیت به (دولتی، غیردولتی، خصوصی، مردم‌نهاد، شبکه‌های مخابراتی و موبایلی، شبکه‌های اجتماعی، سکوها، شبکه بانکی، زیرساخت‌ها و...) تقسیم می‌شود.
همه انواع تهدیدها و آسیب‌پذیری‌های سایبری/سایبر الکترونیکی/الکترومغناطیسی/فیزیکی/... زیرساخت‌های حیاتی، حساس و مهم کشور
اقدامات و فرایندهای زیست‌بوم پدافند سایبری در شرایط و وضعیت‌های مختلف (قبل از بحران، در آستانه بحران، حین و بعد از بحران سایبری)
عوامل توانمند ساز نظیر نیروی انسانی (تخصص، تعهد، مهارت، انگیزه، نگهداشت، مشوق‌ها و...) فناوری‌های مرتبط مانند هوش مصنوعی، اینترنت اشیاء، داده‌های حجیم یادگیری ماشین، خدمات ابری و... ، فرایندها، دکترین و فرماندهی
به‌کارگیری تجهیزات محصولات و سامانه‌های بومی و غیربومی
چرخه انهدام سایبری (چارچوبی برای پیش‌بینی و شناخت تهدیدات، مهندسی اجتماعی، مقابله با باج افزارها، نشت‌های امنیتی و همچنین تهدیدات مداوم پیشرفته)
چرخه امن‌سازی و مصون‌سازی سایبری زیرساخت‌ها
چرخه دفاع سایبری (رصد و پایش، محافظت، تشخیص و مقابله با تهدیدها و حملات CDC, SOC, CERT و...)
قوانین، مقررات و استانداردهای امنیت و پدافند سایبری حوزه‌هایIT,OT,CT
روندهای جهانی امنیت و پدافند سایبری و نقش بازیگران منطقه‌ای و بین‌المللی
نحوه ارتباط با زیست‌بوم‌های دیگر حوزه سایبر مثل زیست‌بوم اقتصاد دیجیتال، رسانه‌های دیجیتال و...

جدول (۷) کنشگران کلیدی زیست‌بوم پدافند سایبری

کنشگران کلیدی زیست‌بوم پدافند سایبری کشور در سطح راهبردی	کنشگران کلیدی زیست‌بوم پدافند سایبری کشور در سطح عملیاتی
شورای عالی و مرکز ملی فضای مجازی	دستگاه‌های متولی زیرساخت‌های حیاتی و حساس مشخص‌شده در اسناد بالادستی
شورای عالی امنیت ملی	قرارگاه پدافند سایبری کشور
وزارت ارتباطات و فناوری اطلاعات	مرکز ماهر و آپاها
سازمان پدافند غیرعامل	اپراتورهای خصوصی ارائه‌دهنده انواع خدمات پدافند سایبری(IT&OT&CT)
مجلس شورای اسلامی	بخش خصوصی تولید/تأمین‌کننده سامانه‌ها و تجهیزات پدافند سایبری (IT&OT&CT)

کنشگران کلیدی زیست‌بوم پدافند سایبری کشور در سطح راهبردی	کنشگران کلیدی زیست‌بوم پدافند سایبری کشور در سطح عملیاتی
مرکز مدیریت راهبردی افتا ریاست جمهوری	وزارت امور خارجه
ستاد کل نیروهای مسلح (شورای عالی/کمیته دائمی پدافند غیرعامل)	وزارت دفاع و پشتیبانی ن. م
وزارت اطلاعات	نوآفرین‌های حوزه امنیت و پدافند سایبری کشور
قوه قضائیه	اصناف و سندیکاهای مرتبط با حوزه سایبری
	بیمه سایبری
	بخش دولتی (وزارتخانه‌های عتف، صمت، کشور، دادگستری و...)
	اپراتورهای‌بخش دولتی ارائه‌دهنده خدمات پدافند سایبری(IT&OT&CT)
	دانشگاه‌ها و پژوهشگاه‌ها
	معاونت علمی و فناوری ریاست جمهوری
	دادستانی کل کشور
	فراجا (پلیس فتا)
	سازمان اطلاعات سپاه
	سازمان برنامه‌وبودجه

بدیهی است که ممکن است کنشگران دیگری نیز در این زیست‌بوم نقش‌آفرین باشند یا اینکه متناسب با تغییرات محیط زیست‌بوم و شرایط، در گذر زمان کنشگرانی به زیست‌بوم اضافه شده و یا از آن حذف شوند.

جدول (۸) نقش‌های عمده کنشگران کلیدی زیست‌بوم پدافند سایبری

ردیف	نقش عمده	ردیف	نقش عمده
۱	راهبری و مدیریت	۱۴	تسهیلگری
۲	رصد و پایش	۱۵	تصویب استانداردها
۳	نگاشت نهادی	۱۶	انجام پژوهش
۴	تنظیم‌گری	۱۷	آموزش
۵	نظارت، ممیزی و ارزیابی راهبردی	۱۸	بومی‌سازی سامانه‌ها، تجهیزات و خدمات پدافند سایبری
۶	نظارت، ممیزی و ارزیابی فنی	۱۹	پیگیری و رسیدگی حقوقی و قضایی
۷	قانون‌گذاری	۲۰	مطالبه‌گری
۸	سیاست‌گذاری	۲۱	کنترل و نظارت امنیتی
۹	سرمایه‌گذاری	۲۲	فرهنگ‌سازی
۱۰	اجرای گام‌های امن‌سازی	۲۳	دیپلماسی پدافند سایبری
۱۱	ارائه انواع خدمات پدافند سایبری	۲۴	هشدار دهی و آگاهی‌رسانی در سطح کلان ملی
۱۲	فرماندهی	۲۵	اشتراک‌گذاری اطلاعات تهدید سایبری
۱۳	هشدار دهی و آگاهی وضعیت عملیاتی		

بر اساس مبانی نظری موجود و راهنمایی خبرگان، ۷ لایه به ترتیب برای زیست‌بوم پدافند سایبری کشور در نظر گرفته شده‌است:

لایه هسته: دارایی‌های سایبری اماکن حیاتی و حساس (مبتنی بر NIST) و امن‌سازی و مصون‌سازی آن

لایه دوم و سوم: مدیریت اطلاعات تهدیدهای سایبری (جمع‌آوری، ذخیره‌سازی، به اشتراک‌گذاری و...) و اقدامات پدافند سایبری (مبتنی بر NIST, ETSI)

لایه چهارم: مراحل حمله سایبری ناظر بر چرخه اقدامات پدافند سایبری

لایه پنجم: توانمند سازهای زیست‌بوم پدافند سایبری کشور (DOTMPLF)

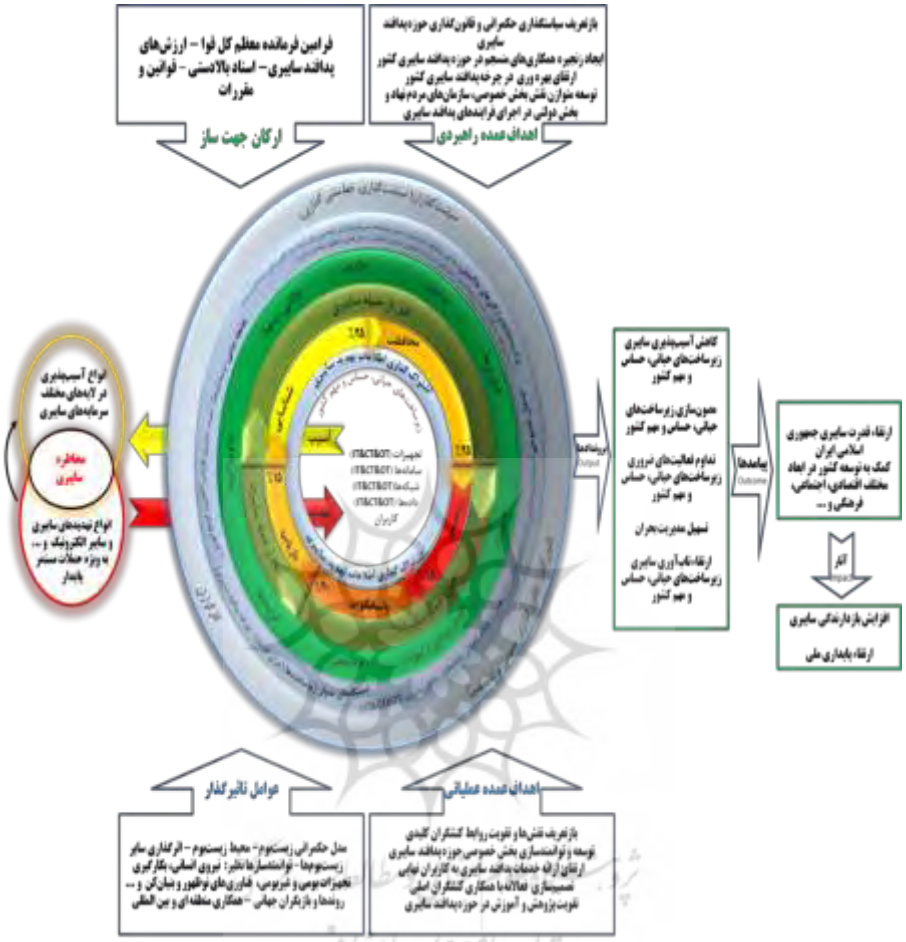
لایه ششم: کنشگران کلیدی سطح عملیاتی – اجرایی زیست‌بوم پدافند سایبری کشور و نقش‌های کلی آن‌ها

لایه هفتم: کنشگران کلیدی سطح راهبردی زیست‌بوم پدافند سایبری کشور و نقش‌های کلی آن‌ها

با توجه به اینکه الگوی زیست‌بوم به‌صورت لایه‌ای و در چرخه‌های مختلف ترسیم شده است، مؤلفه‌های جانمایی شده در هر لایه، متناسب با موضوع کانونی[1] همان لایه بوده و موارد غیر متجانس در هر لایه وجود ندارد. همچنین در تقسیم‌بندی، لایه‌ها کاملاً عمود برهم[2] بوده و دارای هم‌پوشانی نیستند. در الگوی زیست‌بوم پدافند سایبری ارتباط ارگانیک بین اجزاء دیده می‌شود و شکل‌دهی راهبردی[3] برای پرداختن به مطلوبیت‌های راهبردی انجام شده و نوعی از شرایط مطلوب در زیست‌بوم دیده می‌شود. همچنین نتایج[4] به تفکیک بروندادها[5] (نتایج کوتاه‌مدت)، پیامدها[6] (نتایج میان‌مدت) و آثار[7] (نتایج بلندمدت) دسته‌بندی شده است. برای مثال خروجی نهایی یا آثار این زیست‌بوم، افزایش بازدارندگی، تأمین منافع ملی و پایداری ملی خواهد بود. برای رسیدن به فرایند احصاء تهدید و سپس اشتراک‌گذاری اطلاعات تهدیدات سایبری نیز باید ابتدا

[1] FocalPoint
[2] Orthogonal
[3] Strategy shaping
[4] Result
[5] Output
[6] Outcome
[7] Impact

آسیب‌پذیری‌ها و تهدیدها شناسایی شوند چراکه تهدیدها بر آسیب‌ها نگاشت می‌شوند و اشتراک این دو حوزه مخاطره را پدید می‌آورند.



شکل (۱۱) الگوی زیست‌بوم پدافند سایبری کشور

اهداف یا مطلوبیت‌های راهبردی و عملیاتی متعددی برای زیست‌بوم پدافند سایبری کشور متصور است که در الگو به آن‌ها اشاره شده است. همچنین ارکان جهت‌ساز و عوامل تأثیرگذار نیز احصاء شده و در شکل جانمایی شده است.

پیشنهادها

≠ شناخت ارتباطات موجود میان کنشگران که از نتایج پژوهش حاضر است، می‌تواند مقدمه‌ای برای انجام پژوهش‌های بعدی در خصوص مدیریت و

سازمان‌دهی این روابط باشد. به‌عنوان‌مثال طراحی و ارائه مدل کسب‌وکار مناسب جهت فعالیت کنشگران در فضای زیست‌بوم پدافند سایبری، موضوعی مناسب و مقتضی دستیابی به رویکرد برد-برد میان کنشگران است که لازمه فعالیت در فضای زیست‌بوم است.

≠ در پژوهش دیگری ارتباطات میان کنشگران در ابعاد مالی و محصول/خدمت نیز مورد ارزیابی قرارگرفته و با نتایج حاصل از این پژوهش مقایسه شود.

تقدیر

از کلیه اساتید، دانشجویان و متخصصان که در انجام این پژوهش، با محقق همکاری لازم را داشته‌اند کمال تشکر را می‌نماییم.

منابع

≠ آذر، داود، مسلمی، حسین. (۱۴۰۱). راهبردهای قدرت سایبری ارتش جمهوری اسلامی ایران، *فصلنامه آینده‌پژوهی دفاعی*، ۷ (۲۷): ۸۲ – ۶۳.

≠ اسماعیلی، علی. (۱۳۹۷). *طراحی الگوی پایش تهدیدات سایبری با رویکرد آینده‌پژوهی*، رساله دکتری، دانشکده امنیت ملی دانشگاه و پژوهشگاه عالی دفاع ملی.

≠ امیرلی، حسین، تقی پور، رضا. (۱۳۹۹). ارائه مدل فرایندی دفاع سایبری بومی، *فصلنامه امنیت ملی*، ۱۰ (۳۷): ۳۸۶-۳۵۳.

≠ پورشاسب، عبدالعلی، نظری نژاد، احمدعلی. (۱۳۹۹). تدابیر و راهکارهای پدافند غیرعامل در حفاظت از زیرساخت‌های حیاتی جمهوری اسلامی ایران، *فصلنامه مطالعات دفاعی استراتژیک*، ۱۸ (۲۸): ۳۱۲-۲۸۹.

≠ خالدی، آرمان. (۱۳۹۶). تفاوت زیست‌بوم نوآوری و سامانه نوآوری، *فصلنامه علمی پژوهشی سیاست علم و فناوری*، ۹ (۳): ۹۲-۹۱.

≠ رامک، مهراب. (۱۳۹۵). *طراحی نظام دفاع سایبری کشور و تدوین الزامات تحقق آن*، مطالعات گروهی، دانشکده امنیت ملی دانشگاه و پژوهشگاه عالی دفاع ملی.

≠ زنگنه نژاد، نرجس، معینی، علی، حاجی حیدری، نسترن، آذر، عادل. (۱۳۹۸). زیست‌بوم ارتباطات سیار در ایران مبتنی بر روش تحلیل شبکه‌های اجتماعی، *نشریه علمی مطالعات مدیریت کسب‌وکار هوشمند*، ۷ (۲۸): ۲۸-۵.

≠ سازمان پدافند غیرعامل کشور، (۱۳۹۴)، *سند راهبردی پدافند سایبری کشور*.

≠ سپهری، محمد. (۱۴۰۰). مصون‌سازی زیرساخت‌های سایبری کشور در برابر تهدیدهای آمریکا، *فصلنامه مطالعات جنگ*، ۳ (۸): ۵۲-۳۷.

≠ کافی، سعید. (۱۳۹۹). شاخص‌های دفاعی-امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران مبتنی بر رویکردهای پدافند غیرعامل. *مجله سیاست دفاعی*، ۱۲ (۱۱۱): ۲۱-۱.

≠ نقوی، احد، مختار زاده، ناصر. (۱۴۰۰). الگوی شبکه فرماندهی و کنترل قدرت نرم در نیروهای مسلح، *دو فصلنامه بازی جنگ*، ۴ (۹): ۸۳-۶۷.

≠ یاری، علیرضا، کوثری، سحر. (۱۳۹۸). *اصول طراحی زیست‌بوم کسب‌وکارهای فراگیر*، *فصلنامه توسعه تکنولوژی صنعتی*، ۱۲ (۳۷): ۱۸-۳.

≠ A. Walls, Perkins E, Weiss J. (2013). *Definition: "Cybersecur- ity"*, G00252816. Gartner Inc.

≠ ETSI. (2020). *Global Cyber Security Ecosystem*. ETSI TR 103 306 V1. 4. 1 (2020-03) Technical Report.

≠ NiuYang*a, W. Xiao-Feng, XuaGuo-RongPangb, Chun-LeiZhanga. (2018). Research on the Construction of a Novel Cyberspace Security Ecosystem*, Engineering, 4 (1): 47-52.

≠ Shahrin, S, Mohiuddin, A, Leslie, S. (2020). *Toward a Sustainable Cybersecurity Ecosystem*, Computer, 9 (3): 9-17.

≠ Suhyon, Lee. Seungjoo, Kim, (2018) *Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges*, ICSP (Institute of Cyber Security & Privacy), School of Cybersecurity, Korea University, Seoul South Korea.

≠ Galinec, D, Možnik, D, Guberina, B. (2017). *Cybersecurity and cyber defence*. Control, Measurement, Electronics, Computing and Communications, Automatika, 58 (3): 273–286.