فصلنامه علمی امنیت ملی
سال چهاردهم، شماره پنجاه و چهارم، زمستان ۱۴۰۳
مقاله پنجم از صفحات ۱۸۰-۱۵۵

مقاله پژوهشی: شناسایی کنشگران کلیدی و نقش آن‌ها در زیست‌بوم پدافند سایبری زیرساخت‌های حیاتی و حساس کشور

علیرضا کرامتی پور [۱]، رضا تقی پور[۲]، محمد مردانی شهر بابک[۳] و سیدعلی میر رفیع[٤]

تاریخ دریافت: ۱۴۰۲/۰۷/۱۵ تاریخ پذیرش: ۱۴۰۲/۱۱/۰۳

چکیده

فضای سایبر کشور یک محیط زنده و پویا یا یک زیست‌بوم بزرگ با بازیگران مختلف است. عمده فعالیت‌ها و تعاملات اقتصادی، فرهنگی، اجتماعی و حاکمیتی کشور در این زیست‌بوم انجام می‌شود. آسیب‌پذیری‌ها، تهدیدها و حملات متنوع و پیچیده‌ای متوجه زیست‌بوم سایبری است. پدافند سایبری بهره‌گیری از کلیه امکانات غیرتهاجمی سایبری و غیرسایبری کشور به‌منظور ایجاد بازدارندگی، پیشگیری، ممانعت از انجام، تشخیص به‌موقع، مقابله مؤثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری کشور است. در سال‌های اخیر فقدان نگاه علمی و رویکرد یکپارچه به مسائل پدافند سایبری و کم‌توجهی به حلقه‌های متنوع زیست‌بوم پدافند سایبری موجب بروز چالش‌هایی در کشور شده است. ازاین‌رو هدف اصلی تحقیق: شناسایی کنشگران کلیدی زیست‌بوم پدافند سایبری زیرساخت‌های حیاتی و حساس کشور و تعیین نقش آن‌ها است. تحقیق از نوع توسعه‌ای- کاربردی و با روش توصیفی- تحلیلی انجام شده است. از روش‌های مورداستفاده برای تحلیل و توصیف داده‌های آماری از آزمون‌های تحلیل شبکه بهره گرفته شد. پس از انجام مطالعات نظری، مصاحبه با خبرگان و توزیع پرسشنامه، براساس تجزیه‌وتحلیل داده‌های ٤٤ نفر نمونه، تعداد ۲۸ کنشگر کلیدی این زیست‌بوم در دو سطح راهبردی و عملیاتی – اجرایی و ۲۵ نقش عمده برای کنشگران احصاء گردید. با استفاده از نرم‌افزارهای تحلیل شبکه‌های اجتماعی، ارتباط بین کنشگران و نقش‌ها در زیست‌بوم تعیین و ترسیم گشت. شناسایی کنشگران اصلی زیست‌بوم پدافند سایبری، نقش‌ها و شناسایی روابط و تعاملات آن‌ها نوآوری این تحقیق می‌باشد.

کلیدواژه‌ها: زیست‌بوم، زیست‌بوم سایبری، امنیت سایبری، پدافند سایبری، زیرساخت حیاتی و حساس.

[۱] دانشجوی مقطع دکتری دانشگاه عالی دفاع ملی (نویسنده مسئول) رایانامه: re.keramat96@gmail.com
[۲] مدرس دانشگاه دانشگاه عالی دفاع ملی، رایانامه: ngfjhg@gmail.com
[۳] عضو هیئت علمی دانشگاه، رایانامه: gfhtg12@gmail.com
[٤] عضو هیئت علمی دانشگاه، رایانامه: jfghtf15@gmail.com

۱- مقدمه:

تهدیدهای سایبری طی سال‌های اخیر علیه جمهوری اسلامی ایران از روند روبه رشدی برخوردار شده است. فضای سایبری، اگرچه پس از زمین، دریا، هوا و فضا، به‌عنوان بعد پنجم نبردهای نظامی در نظر گرفته‌شده، لیکن به‌واسطه برخورداری از تفاوت‌های عمده‌ای همچون؛ تغییرات بسیار سریع، گسترده و مداوم، گمنامی کاربران، بی‌مرزی، آشوبناکی و ترکیب آن با سایر ابعاد جنگ‌ها، نسبت به سایر محیط‌های عملیاتی، ویژگی‌های منحصربه‌فردی دارد (سپهری، ۱٤۰۰: ۱۵۳). درک، تحلیل و شناخت تهدیدات علیه زیرساخت‌های حیاتی دارای اهمیت و باعث تداوم و استمرار ارائه خدمات در سطح ملی می‌شود (آقایی و همکاران، ۹۸: ۲۰٤). زیست‌بوم سایبری شامل انواع مختلف کنشگران است که به‌صورت دیجیتالی به یکدیگر پیوند دارند. بازیگران یک زیست‌بوم سایبری ممکن است از شرکت‌های خصوصی، غیرانتفاعی، دولت‌ها تا فرآیندها، دستگاه‌های سایبری و حتی انسان‌ها متفاوت باشد. این زیست‌بوم محیطی غنی از هدف را برای مهاجمان ایجاد می‌نماید تا از آسیب‌پذیری‌ها با هدف سرقت اطلاعات، هویت و ... استفاده کنند (بلک کیت، ۲۰۲۱). مانند زیست‌بوم‌های طبیعی، زیست‌بوم سایبری شامل شرکت‌کنندگان متنوعی است. شرکت‌های خصوصی، غیرانتفاعی، دولت‌ها، افراد، فرآیندها و دستگاه‌های سایبری که برای اهداف متعدد با هم تعامل دارند (پوتی، ۲۰۱۸). به‌دلیل تنوع و پیچیدگی حملات سایبری، امنیت و پدافند سایبری به یک رشته پیچیده تبدیل شده است. سازمان‌ها می‌توانند با ایجاد یک زیست‌بوم سایبری ازنظر ایمنی از خود در برابر این حملات محافظت کنند (مورگان، ۲۰۲۱). زیست‌بوم‌ها به‌یک‌باره و به‌صورت بزرگ متولد نمی‌شوند و پیدایش و رشد آن‌ها معمولاً ناشی از ترکیب فرایندهای عامدانه است (محقر و همکاران، ۱۳۹۸: ۱۲).

زیرساخت‌های حیاتی و حساس کشورها در حکم ستون‌های سقف جامعه محسوب شده و نقش به‌سزایی 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 باتوجه به وابستگی متقابل زیرساخت‌ها به یکدیگر به‌سرعت به سایر زیرساخت‌ها سرایت کرده و در مدت کوتاهی کارکردهای جامعه را تحت تأثیر مستقیم قرار می‌دهد و باید انتظار وقوع بحران‌های شدید اجتماعی با ابعاد امنیتی را داشت (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). پدافند سایبری همواره راهکارهای احتیاط‌آمیز و مناسبی را برای کاهش تهدیدهای متوجه کشور ارائه می‌دهد. رویکردهای پدافند سایبری زمینه صیانت از زیرساخت‌های حیاتی و حساس را با کم‌ترین بار مالی کشور فراهم می‌سازد (کافی، ۱۳۹۹: ۸). اقدامات دشمنان می‌تواند به‌طور مداوم متغیر و غیرقابل‌پیش‌بینی باشد. وضعیت‌های نامعلوم، پیچیده و پویا همانند وضعیت‌های مربوط به امنیت سایبر محیط پرمخاطره را ایجاد می‌نمایند. وضعیت‌های پویا مستلزم به‌کارگیری روش‌های تصمیم‌گیری پویا است (عابدی و قهرودی، ۱۳۹۹: ۳). باوجوداینکه براساس تقسیم‌کار صورت گرفته در اسناد بالادستی، مسئولیت هر دستگاه در مقابله با حوادث فضای سایبری کشور مشخص است و همه دستگاه‌ها موظف‌اند با حوادث فضای سایبری مربوط به خود، مقابله کنند؛ اما به‌نظر می‌رسد این امر پاسخگوی همه نیازها نیست. در شرایط کنونی تعدد کنشگران حوزه پدافند سایبری، وجود اختلاف‌نظر میان این کنشگران و مبهم بودن نقش هر یک و روابط بین آن‌ها، باعث بروز مشکلاتی شده است. ازاین‌رو، رویکرد زیست‌بومی به پدافند سایبری و یکپارچه‌سازی، تعامل و تعمیق همکاری و مشارکت نیروهای پدافند سایبری برای افزایش انسجام و مقاومت در حمله سایبری علیه زیرساخت‌های حیاتی و حساس ضروری به نظر می‌رسد و برای تحقق این امر ابتدا بایستی کنشگران نهادی کلیدی و نقش‌های عمده و ارتباطات آن‌ها در زیست‌بوم ساختاریافته پدافند سایبری زیرساخت‌های حیاتی و حساس کشور شناسایی شود. مسئله اصلی این پژوهش، تعدد

کنشگران و مبهم بودن نقش و وظایف هرکدام در زیست‌بوم ساختاریافته پدافند سایبری کشور است. براین اساس اهداف این پژوهش شناسایی کنشگران کلیدی زیست‌بوم پدافند سایبری زیرساخت‌های حیاتی و حساس کشور و نقش‌های عمده و ارتباطات بین این کنشگران است.

سؤال اصلی پژوهش عبارتست از: کنشگران کلیدی زیست‌بوم پدافند سایبری زیرساخت‌های حیاتی و حساس کشور کدام‌اند؟

سؤالات فرعی پژوهش عبارتند از: ۱- نقش‌های عمده کنشگران کلیدی زیست‌بوم پدافند سایبری زیرساخت‌های حیاتی و حساس کشور کدام‌اند؟ ۲- ارتباطات بین کنشگران کلیدی زیست‌بوم پدافند سایبری زیرساخت‌های حیاتی و حساس کشور چگونه است؟

پیشینه شناسی تحقیق:

بررسی‌های مختلفی بر روی پژوهش‌های علمی مرتبط با عنوان پژوهش حاضر صورت پذیرفته که در ادامه به برخی از مهم‌ترین آن‌ها که در مؤلفه‌ها و متغیرهایی با موضوع این تحقیق مشترک هستند اشاره شده است:

۱. موسسه استاندارد ارتباطات از راه دور اروپا در سند «زیست‌بوم جهانی امنیت سایبر» زیست‌بوم امنیت سایبری جهانی را در قالب شش بخش متشکل از: تشکل‌ها، انجمن‌ها، توسعه‌دهنده‌ها و فعالیت‌هایی که سازوکارهای اساسی همکاری امنیت سایبری را انجام می‌دهند نظیر سازمان‌های بین‌المللی، شرکت‌های امنیتی چندملیتی، مؤسسات استاندارد امنیت سایبر و ... تقسیم‌بندی و بررسی می‌کند و در ادامه به وضعیت امنیت سایبری کشورها می‌پردازد (۲۰۲۰).

۲. شهرین سادیک و همکاران در مقاله «به‌سوی یک زیست‌بوم امنیت سایبری پایدار» که در گروه علوم و مهندسی کامپیوتر، دانشگاه بین‌المللی اسلامی چیتاگونگ، بنگلادش انجام شده که ۱- روندهای نوظهور، ۲- روش‌های انطباق با تدابیر امنیتی پیشرفته برای پیشگیری و کاهش تهدیدات سایبری و ۳- راه‌حل‌های امنیت سایبری با استفاده از هوش مصنوعی و یادگیری ماشینی نیز همراه با الگوی امنیت سایبری جامعه را موردبحث قرار

می‌دهد. پیاده‌سازی اجزای سامانه مناسب، با درنظر گرفتن چرخه حیات امنیت سایبری درحالی‌که از دستورالعمل‌ها و بهترین شیوه‌ها استفاده می‌شود ضرورت دارد(۲۰۲۰).

۳. رایلا، لیما و میلیوجا در قالب یکی از تحقیقات مرتبط با هوریزون ۲۰۲۰ اتحادیه اروپا، باعنوان «اکو سامانه نوآوری امنیت سایبری آسه آن: رویکرد ایجاد مشترک» چشم‌انداز، نیازمندی‌ها و شکاف‌های زیست‌بوم امنیت سایبری سه کشور مالزی، تایلند و ویتنام را شناسایی و بررسی و راهبردهای ایجاد این زیست‌بوم را مطرح نموده‌اند (۲۰۱۸).

٤. زنگنه نژاد و همکاران در «زیست‌بوم ارتباطات سیار در ایران مبتنی بر روش تحلیل شبکه‌های اجتماعی» مرزهای زیست‌بوم ارتباطات سیار ایران را به‌این‌ترتیب تعریف نمودند که در بردارنده کلیه سازمان‌ها و نهادهای دولتی و غیردولتی است که به‌طور مستقیم در طراحی، تولید، پشتیبانی و ارائه خدمات مبتنی بر بستر ارتباطات سیار در ایران فعالیت دارند و به خلق ارزش مبتنی بر زیرساخت‌های ارتباطی می‌پردازند. شناسایی بازیگران کلیدی این زیست‌بوم و ترسیم شبکه روابط میان بازیگران کلیدی زیست‌بوم ارتباطات سیار ایران و تحلیل شبکه فوق مهم‌ترین دستاورد این پژوهش به‌شمار می‌رود (۱۳۹۸).

۵. اجاقی، یزدانی و محمدی (۱۳۹۸) در مقاله «شناسایی بازیگران اصلی و نقش‌های کلیدی در زیست‌بوم نوآوری نوپاها» شش بازیگر اصلی زیست‌بوم شامل؛ دانشگاه‌ها، مراکز رشد، تأمین‌کننده‌های مالی، شرکت‌ها، شتاب‌دهنده‌ها و پارک‌های علم و فناوری را شناسایی نمودند. سپس براساس استخراج نتایج اسناد، کدگذاری و دسته‌بندی کدها نقش‌های ضروری شامل: حمایتگری، سازآرایی، زمینه‌سازی، متولد سازی و مربیگری، مفهوم‌سازی و درنهایت برای مطالعه موردی، رابطه بین نقش‌ها با توانمندی نوآوری نوپاها به کمک ابزار پرسشنامه و تحلیل ساختاری تجزیه‌وتحلیل شده است.

۲- مبانی نظری:

فضای سایبر: فضای سایبر شبکه‌های وابسته به یکدیگر، از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه 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 می‌باشد. این فضا، ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد (سند راهبردی پدافند سایبری، ۱۳۹٤: ۱).

زیست‌بوم: زیست‌بوم به ارتباط متقابل بین موجود زنده و محیط آن اطلاق می‌شود. زیست‌بوم را برای اولین بار در ۱۹۳۵، گیاه‌شناس انگلیسی، آرتور جورج تانسلی در مجله اکولوژی ارائه داد. این مفهوم در بسیاری از حوزه‌ها مورداستفاده قرارگرفته که فضای سایبری نمونه کلاسیک آن است (نیویانگا و همکاران، ۲۰۱۸).

زیست‌بوم سایبری: زیست‌بوم سایبری به شکل‌گیری محیطی بومی، پویا و زنده سایبری اشاره دارد که برای کشو در عرصه‌های مختلف حمایتگر و پشتیبانی‌کننده خواهد بود (پیشین: ۲). زیست‌بوم سایبری، مانند زیست‌بوم‌های طبیعی شامل انواع مختلفی از شرکت‌کنندگان شرکت‌های خصوصی، غیرانتفاعی، دولت‌ها، افراد، فرآیندها و دستگاه‌های سایبری است که برای چندین هدف با یکدیگر تعامل دارند (موسسه استاندارد ارتباطات از راه دور اروپا ،۲۰۲۰).

زیرساخت: به مجموعه‌ای از مراکز و تأسیسات زیربنایی و شریان‌های عمده که خدمات و نیازهای ضروری و اساسی کشور را به مردم و جامعه ارائه می‌کند، اطلاق می‌گردد؛ زیرساخت مشتمل بر فرابخش (حوزه)، بخش، زیربخش، دارایی و اجزاء آن می‌باشد.

حفاظت از زیرساخت: مجموعه تدابیر و اقدامات پدافند غیرعاملی که توانایی و آمادگی عملیاتی زیرساخت و تداوم کارکردهای آن و دستگاه‌های اجرایی مسئول برای پاسخ مؤثر به حوادث و سوانح ناشی از تهدیدات نظامی، تهدیدات امنیتی و تروریستی، تهدیدات سایبری زیرساختی و تهدیدات از درون دشمن پایه را افزایش می‌دهد به‌طوری‌که فعالیت آن حفظ گردیده و خسارات انسانی و مادی ناشی از آن را به حداقل می‌رساند.

تاب‌آوری: به توانایی یک نظام، جامعه، دستگاه اجرایی و یا زیرساخت برای ایستادگی، تحمّل، انعطاف‌پذیری و حفظ کارکرد، تطبیق و برگشت‌پذیری در برابر مخاطره امنیتی ـ نظامی گفته می‌شود (طرح راهبردی حفاظت از زیرساخت‌های کشور، ۱۴۰۱).

پدافند سایبری: پدافند سایبری بخشی از مقوله دفاع سایبری است. آفند و پدافند دو مؤلفه اصلی در دفاع هستند. مجموعه اقدامات بازدارنده، رفع کننده، دفع‌کننده و بازیابی کننده که به‌منظور پیشگیری، حفظ، حمایت از ارزش‌ها، منافع و دارایی‌های ملی در مقابل تهدیدات و حملات سایبری انجام می‌گیرد. در امنیت به‌دنبال شرایطی هستند که مخاطرات اساسی به سطحی قابل‌پذیرش کاهش یابد. تأمین امنیت یکی از اهداف دفاع است. حوزه دفاع در سطح کلان ملی، مجری کنترل‌های امنیتی و تأمین‌کننده امنیت در ارزش‌ها، زیرساخت‌ها و سرمایه‌های ملی است. آنچه حوزه دفاعی را متمایز می‌سازد، عملکرد آن در دفاع از ارزش‌های ملی و حاکمیت ملی در مقابل حملات و تهدیدات خارجی می‌باشد (ملائی و همکاران، ۱۳۹۸: ۲۵٤). پدافند سایبری بهره‌گیری از کلیه امکانات غیرمسلحانه سایبری و غیر سایبری کشور، به‌منظور پیشگیری ایجاد بازدارندگی، ممانعت از انجام، تشخیص به‌موقع، مقابله مؤثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری جمهوری اسلامی ایران، توسط متخاصمین سایبری، اعم از نیروی نظامی (ارتش سایبری) کشورهای متخاصم و گروه‌های تحت حمایت پنهان دولت‌های متخاصم به‌نحوی‌که امکان تهاجم سایبری را از کلیه متخاصمین سلب نماید (سند راهبردی پدافند سایبری کشور، ۱۳۹٤، ۲). آن‌دسته از تهدیداتی که دولت یا گروه‌های تحت حمایت آن پشت آن بوده و با هدف‌گیری سرمایه‌های ملی، منجر به بحران وسیع شود، شکل دفاعی پیدا می‌کند و نیروهای دفاعی در آن محوریت داشته و سایرین باید به آن کمک کنند؛ اما در بخش دیگری که پای دولت یا نهاد بزرگ حاکمیتی پشت تهدیدات نباشد، بخش امنیتی آن‌ها را مدنظر قرار داده و نیروهای دفاعی به آن کمک می‌کند. به‌هرحال، اثبات این‌که تهدیدات از نوع دولتی هستند، یکی از پیچیدگی‌های مهم است که دفاع قانونی را به چالش می‌کشد. یکی از ملاک‌های حمایت از بدافزارها توسط دولت‌ها، تعداد بالای روز صفری است که در

آن پشتیبانی می‌شود و تحلیلگرهای امنیتی از این طریق متوجه می‌شوند که دولت‌ها حامی آن هستند. آسیب‌پذیری روز صفر به این معناست که تاکنون هیچ راهکاری برای آن ارائه نشده و یا صفر روز فرصت پیدا کردن راهکار وجود دارد.

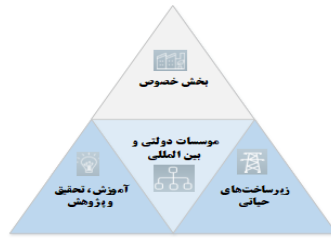
مفهوم زیست‌بوم معرف شدت وابستگی، اتصال و رقابت موجودیت‌های مختلف کسب‌وکار (تأمین‌کننده، تولیدکننده و توزیع‌کننده در حوزه یک محصول یا خدمت) است. مفهوم مشابه دیگر، «سیستم» تاپیش از ورود رویکرد زیست‌بوم به ادبیات کسب‌وکار معمولاً از آن استفاده می‌شد. این مفهوم به‌طور ضمنی، درجه بالایی از کنترل‌پذیری و ساختارمندی را دربردارد. این درحالی است که بسیاری از نظامات، به‌ویژه حوزه اقتصادی–اجتماعی از نوع پیوند ضعیف بوده، سلسله‌مراتب مرسوم در آن‌ها مشاهده نمی‌شود و قابلیت کنترل‌پذیری در آن‌ها پایین است. وجه‌تمایز دیگر زیست‌بوم با سایر مفاهیم، تناسب آن با موقعیت‌هایی می‌باشد که ویژگی‌های حیات‌گونه (تولد، زنده ماندن، رشدیافتگی و هم‌تکاملی) دارند. اساساً مفهوم زیست‌بوم بر فهم هماهنگی در موقعیت‌هایی که بازیگران آن همکار و درعین‌حال رقیب هم، تمرکز دارد. به‌لحاظ ساختاری، ممکن است زیست‌بوم از مجموعه‌ای از گره‌های وابسته به یکدیگر که حول محصول، خدمت، فرایند، مشتری، بخش‌های صنعت یا توزیع به‌وجود آمده شکل بگیرد. گاه محور زیست‌بوم، یک بازیگر خاص است؛ به‌عنوان‌مثال در زیست‌بوم‌های هاب‌گونه یا سکویی، یک شرکت کانونی بر رهبری، تعیین اهداف و تعریف سکو نقش تعیین‌کننده دارد و نوپاها مجبورند در قالب چشم‌انداز، اهداف و ساختار به‌وجود آمده توسط رهبر یا هاب فعالیت کنند و درعین‌حال ارزش ارائه‌شده توسط آن‌ها باید به‌اندازه کافی مستقل، متفاوت و جدید باشد که حضورشان را توجیه کند. چنین الگوهایی ناشی از تعاملات طولانی‌مدت بازیگران پدیدار می‌شود و معمولاً به‌صورت خودبه‌خودی زیست‌بوم را ساختارمند می‌کند (اجاقی و همکاران، ۱۳۹۸: ۲۶). اگرچه توافق محققین بر روی ساختار زیست‌بوم دارند؛ ولی هر یک، واژگان مختلفی را برای بازیگران به‌کار می‌برند که تقریباً همه یک مفهوم را می‌رسانند. برای مثال به‌جای قطب مرکزی عبارت، کی‌استون را به‌کار برده و از آن به‌عنوان

کمک‌کننده مرکزی یاد می‌کنند. سه نوع بازیگر بین اجزای زیست‌بوم شامل قطب مرکزی، بازیگران حاکم و بازیگران گوشه‌ای تعریف کرده‌اند. قطب مرکزی، راهبردها را شکل می‌دهد. تأثیر عمده‌ای در سلامت زیست‌بوم دارد. تلاش می‌کند که پایداری، تنوع و بهره‌وری زیست‌بوم را افزایش دهد و تسهیم‌کننده ارزش بین تمامی ذینفعان و بازیگران باشد. آن‌ها، رهبری فعال در زیست‌بوم بوده و قصد آن‌ها توسعه فعالیت‌ها و درمجموع سلامت زیست‌بوم است. حضور فیزیکی کمتری دارند ولی به‌لحاظ تولید ارزش و توزیع آن بین دیگر بازیگران بیشترین نقش را ایفا می‌نمایند. لذا می‌توان بازیگر مرکزی را مانند یک قطب در نظر گرفت که شبکه آن‌ها بیشترین، قوی‌ترین و باارزش‌ترین ارتباطات را ایجاد می‌کند. آن‌ها اغلب در هسته شبکه قرار می‌گیرند. دو بازیگر دیگر در زیست‌بوم وجود دارند؛ یکی بازیگران حاکم و دیگری بازیگران گوشه‌ای می‌باشد. از بین بازیگران زیست‌بوم، حاکم قصد دارد سهم قابل‌توجهی از زیست‌بوم را به‌خود اختصاص و آن را تاحد امکان توسعه دهد. آن‌ها حضور فیزیکی قوی و کنترل بخش عمده‌ای از شبکه را به عهده دارند. بخش بیشتری از ارزش ایجادشده را برای خود می‌خواهند و بخش کمتری را به دیگر بازیگران در زیست‌بوم می‌دهند. بازیگران گوشه‌ای بزرگ‌ترین گروه‌ها را در زیست‌بوم تشکیل می‌دهند. آن‌ها بزرگ و کوچک هستند، شرکت‌هایی که تخصص ویژه‌ای در ظرفیت‌های خاص دارند و این سبب تفاوت آن‌ها با دیگر بازیگران زیست‌بوم می‌شود. درواقع بازیگران گوشه‌ای بیشترین ارزش را در زیست‌بوم و درمجموع ایجاد می‌کنند. رشد آن‌ها بستگی به توانمندی دستیابی و استفاده از بستر بازیگر قطب دارد تا بتوانند تفاوت ایجاد کنند (حکیم‌جوادی و سپهری، ۱۳۹٤: ۳۸). یک الگو از دسته‌بندی بازیگران در زیست‌بوم و تعیین نقش‌های آنان به‌وجود آمده که در جدول ش. یک آمده است:

جدول ش. ۱ دسته‌بندی بازیگران در زیست‌بوم و تعیین نقش‌های آنان (برگرفته از پیشین، ۱۳۹۸: ٤٠).

بازیگران	شامل: دانشگاه‌ها، مراکز رشد، تامین‌کننده‌های مالی، شرکت‌ها، شتاب‌دهنده‌ها، پارک‌های علم و فناوری، واسطه‌ها و دولت.
نقش‌ها	شامل: زمینه‌سازی (اماده‌سازی محیطی، زمینه‌سازی اموزشی) متولدسازی (تحریک تولد، توجه به اقتضائات دوران تولد، تسهیل تولد، پیگیری تولد) حمایتگری (حمایت فیزیکی، حمایت مالی، تأمین منابع، پشتیبانی حقوقی، پشتیبانی فنی) مربیگری (آموزش متناسب با مرحله رشد، کسب دانش ضمنی، دستیاری، پرورش) سازآرایی (رهبری، ساختاردهی، تسهیلگری)

با دیجیتالی شدن روزافزون جوامع و اقتصادها، برای دستیابی به تاب‌آوری سایبری و ایجاد یک زیست‌بوم امنیت سایبری قوی، بازیگران مختلف باید در این فرآیند مشارکت داشته باشند. ارتباط متقابل کنشگرها یکی از ویژگی‌های اصلی زیست‌بوم پدافند سایبری است؛ عدم آمادگی یک بازیگر می‌تواند کل زیست‌بوم را تحت تأثیر قرار دهد. به‌طور مشابه، اقدامات خوب متمرکز بر آمادگی، انعطاف‌پذیری و کاهش خطر می‌تواند تأثیر مثبتی داشته باشد و شرایط زیست‌بوم را بهبود بخشد. در بخش‌های زیر، با هدف تشریح و روشن کردن مسئولیت‌ها و اقداماتی که هر کنشگر می‌تواند برای بهبود زیست‌بوم پدافند سایبری انجام دهد، بازیگران مرتبط، موضوعات، اقدامات و نمونه‌هایی از بهترین شیوه‌های امنیت سایبری ارائه می‌شود (رایلا، لیما و میلیوجا، ۲۰۱۸: ۱۵).



شکل شماره ۱: کنشگران زیست‌بوم نوآوری امنیت سایبری (همان، ۱۷)

سازمان‌های بین دولتی و بازیگران فراملی: کنشگرانی نظیر انجمن کشورهای جنوب شرقی آسیا (آسه آن)، اتحادیه اروپا، سازمان پیمان آتلانتیک شمالی (ناتو)، سازمان همکاری اقتصادی و توسعه، سازمان برای امنیت و همکاری در اروپا و سازمان ملل متحد و ...

بخش دولتی: دولت نشان‌دهنده بالاترین سطح مدیریت امنیت سایبری و مسئول ارائه رهنمودهای سیاسی و دستورالعمل‌های راهبردی برای امنیت سایبری و همچنین اتخاذ تصمیمات لازم در مورد منابع و پیش‌نیازهایی است که باید تخصیص داده شود.

سازمان‌های دانش، تحقیق و توسعه: این دسته از کنشگران، مراکز تحقیق و توسعه، دانشگاه‌ها، دبیرستان‌های فنی حرفه‌ای را در برمی‌گیرد.

بخش خصوصی: این دسته از کنشگران شامل شرکت‌های بزرگ، کوچک و متوسط، نوآفرین‌ها و شرکت‌های چندملیتی هستند که داده‌های حساس را مدیریت می‌کنند و در معرض تهدیدات سایبری قرار دارند.

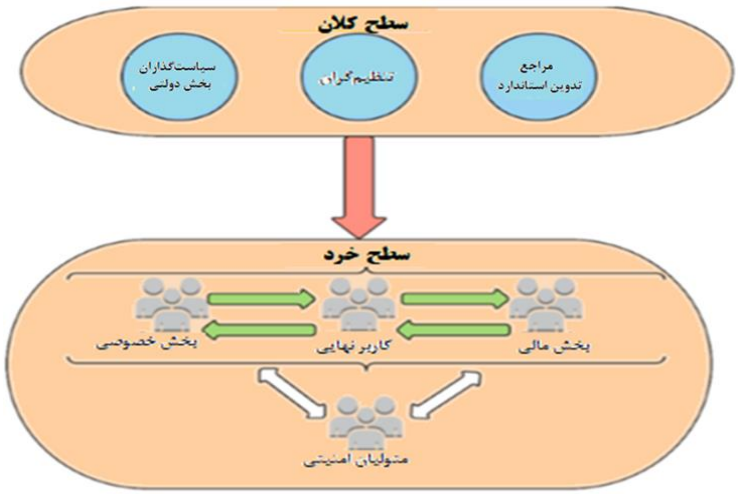
جامعه مدنی: این دسته از کنشگران شامل انجمن‌ها، شبکه سازمان‌ها (سازمان‌های تجاری نماینده منافع شرکت‌های فعال در بخش‌های در معرض تهدیدات سایبری) و همچنین سایر طرف‌های ذینفع ازجمله نمایندگان رسانه‌ها و سازمان‌های غیردولتی علاقه‌مند به همکاری در امنیت و پدافند سایبری هستند.

سازمان‌های متولی زیرساخت‌های حیاتی و حساس: سازمان‌های فعال در بخش‌های شیمیایی، تولیدات حیاتی، سدها، دفاع، خدمات اضطراری، انرژی، خدمات مالی، تأمین غذا، تأسیسات دولتی، مراقبت‌های بهداشتی، فناوری اطلاعات و ارتباطات، حمل‌ونقل و سامانه‌های آب، نمونه‌هایی از سازمان‌های زیرساختی حیاتی هستند (همان: ۲۱).

نمونه‌ی زیست‌بوم امنیت و پدافند سایبری

این زیست‌بوم را می‌توان به‌طورکلی به دو بخش تقسیم کرد، برخی از کنشگران (به‌عنوان‌مثال دولت‌ها) در هر دو بخش نقش دارند: **۱- کنشگران سطح کلان:** آن دسته از ذینفعانی که در موقعیتی هستند و می‌توانند بر نحوه نگاه و عملکرد حوزه امنیت سایبری در سطح خرد تأثیر بگذارند. نمونه‌های اصلی شامل دولت‌ها، تنظیم‌کنندگان، سیاست‌گذاران و سازمان‌ها و ارگان‌های تنظیم‌کننده استاندارد (مانند سازمان بین‌المللی استانداردسازی، گروه ویژه مهندسی اینترنت و موسسه ملی استاندارد و فناوری) است. **۲- کنشگران سطح خرد:** آن دسته از ذینفعانی که به‌صورت جمعی یا فردی، اقداماتی را به‌صورت روزمره انجام می‌دهند که بر وضعیت کلی امنیت سایبری جامعه (مثبت یا منفی) تأثیر می‌گذارد. به‌عنوان‌مثال می‌توان به کاربران نهایی/ مصرف‌کنندگان، دولت‌ها، مشاغل برخط، شرکت‌ها/سازمان‌ها، مؤسسات مالی و مشاوران امنیتی اشاره کرد. درگذشته مشارکت و تأثیرگذاری ذینفعان سطح کلان، بر تحولات امنیت سایبری تا حدودی کم اثر بوده است. به‌عنوان‌مثال دولت‌ها و نهادهای نظارتی غالباً در حاشیه امنیت سایبری فعالیت می‌کردند و

در درجه اول کارها را در سطح خرد قرار می‌دادند و همکاری در برخی موارد (به‌عنوان‌مثال، در پاسخ به حوادث امنیت سایبری با پیامدهای امنیت ملی) اتفاق می‌افتاد. (پوتی، ۲۰۱۸)



شکل شماره ۲: نمونه زیست‌بوم امنیت و پدافند سایبری (پوتی، ۲۰۱۸)

مطالعه تطبیقی کشورها و سازمان‌ها:

مفهوم حفاظت از زیرساخت‌های اطلاعاتی حیاتی در آمریکا، عبارت است از: محافظت از مؤلفه‌های مجازی زیرساخت‌های اطلاعاتی حیاتی که جامعه به آن نیاز دارد (تقی پور، لشکریان و یزدانی جهاربرج، ۱۳۹۸: ۱۸). در این بخش رویکرد برخی از سازمان‌های بین‌المللی و کشورهای جهان به موضوع پدافند سایبری بررسی شد. سازمان‌های بین‌المللی نظیر ناتو یا اتحادیه اروپا بر تعامل بین کشورها بر دفاع سایبری هماهنگ تأکید دارند. در خصوص کشورها، وجه اشتراک اغلب رویکردها که در سیاست ملی امنیت سایبری هر کشور منعکس شده، ایجاد زیست‌بوم سایبری امن در کشور، تعیین کنشگران و نقش هرکدام در پدافند سایبری و انجام دفاع جمعی و هماهنگی در دفاع سایبری برای ایجاد یک زیست‌بوم سایبری ایمن است.

جدول شماره ۲: مطالعات تطبیقی

کشور/نهاد بین‌المللی	کنشگران	نقش‌ها
رژیم صهیونیستی	اداره ملی سایبری اسرائیل (رژیم صهیونیستی) ارگان‌های دولتی: زیرساخت‌های حیاتی و سایر وزارتخانه‌های دولتی بخش خصوصی: سایبر اسپارک، زیست‌بوم نوآوری سایبری اسرائیل (رژیم صهیونیستی) در بئر سبع – جامعه دفاعی: ارتش (اداره فرماندهی کنترل و واحد ۸۲۰۰) نیروی دفاعی اسرائیل (رژیم صهیونیستی)، شین‌بت موساد دانشگاه‌ها: دانشگاه تل‌آویو دانشگاه بن گوریون مرکز تحقیقات سایبری میان‌رشته‌ای بلاواتنیک	برنامه‌ریزی سیاست راهبردی و وضع مقررات برای بهبود استحکام سایبری رژیم صهیونیستی در برابر خطرات با حمایت از زیرساخت‌های حیاتی. پیاده‌سازی و تنظیم راهبرد ملی سایبری در سطح ملی (بهبود استحکام، انعطاف‌پذیری و دفاع که شامل CERT-IL و CIP می‌شود). تسهیل همکاری‌های بین‌المللی و تدوین چارچوب قانونی برای فعالیت‌های سایبری (داخلی و بین‌المللی). مدیریت همه‌جانبه کمپین‌های دفاع ملی (در زمان صلح). بهبود انعطاف‌پذیری با همکاری پلیس رژیم صهیونیستی و وزارت دادگستری. حمایت از شین‌بت، ارتش رژیم صهیونیستی، موساد، پلیس و وزارت دادگستری در تقویت دفاع سایبری غیرنظامی. تمرین‌های ملی و بین‌المللی را برای بهبود آمادگی رژیم صهیونیستی در فضای سایبری همکاری در زمینه سایبری با نهادهای موازی در خارج از کشور پیشبرد و افزایش آگاهی عمومی نسبت به تهدیدات در فضای سایبری و ابزارهای مقابله با آن‌ها سازمان‌دهی و تأمین مالی کنفرانس‌ها با همکاری وزارت خارجه بخش خصوصی امنیت سایبری رژیم اشغالگر قدس به‌عنوان محور راهبرد سایبری رژیم اشغالگر قدس برای کاهش حملاتی که دفاع سازمانی را در هم می‌شکند، اتخاذ کرد
آمریکا	شورای حمایت از زیرساخت‌های حساس فرماندهی سایبری ایالات‌متحده آژانس امنیت ملی پلیس فدرال، وابسته به وزارت دادگستری وزارت امنیت میهنی وزارتخانه‌های بازرگانی، دفاع، انرژی، خزانه‌داری و دادگستری. دانشگاه جان هاپکینز بخش خصوصی و جامعه مدنی	مرکز امداد و نجات رایانه‌ای ملی، سامانه‌های تشخیص و مقابله بانفوذ و همچنین سامانه‌های آگاهی موقعیتی جرائم سایبری و پیگیری مجرمین
ناتو	مرکز تعالی دفاع سایبری تعاونی[1] مرکز امنیت سایبری ناتو[2]	افزایش قابلیت، همکاری و اشتراک اطلاعات بین، کشورهای ناتو و شرکا در دفاع سایبری به‌واسطه آموزش،

[1] CCDCOE
[2] NCSC

	آژانس ارتباطات و اطلاعات ناتو[1] مرکز عملیات فضای سایبری[2]	تحقیق و توسعه، درس‌های آموخته‌شده و مشاوره تولید، انباشت و انتشار دانش در امنیت سایبری قابلیت پاسخگویی به حوادث رایانه‌ای ناتو میزبانی تمرین‌های دوره‌ای یکی از این رزمایش‌ها، معروف به سپر قفل‌شده، در سال ۲۰۱۹
اتحادیه اروپا	مرکز جدید جرائم سایبری اروپا[3] همکاری بین بخش‌های دولتی و خصوصی را برای افزایش قابلیت‌های سیاست مشترک امنیتی و دفاعی سازمان‌های بین دولتی در به اشتراک‌گذاری اطلاعات، دولت‌ها، بخش خصوصی و جامعه مدنی	راهبرد جدید امنیت سایبری اتحادیه اروپا با ایجاد سپر سایبری اروپایی، شبکه‌ای از مراکز عملیات امنیتی در سراسر اتحادیه اروپا، زیرساخت‌های ارتباطی امن ازجمله شبکه‌های تلفن همراه باند پهن و ترویج اینترنت اشیا ایمن، انعطاف‌پذیری زیرساخت‌ها و خدمات حیاتی را تقویت می‌کند. همچنین بهبود آموزش امنیت سایبری و توسعه ظرفیت‌سازی و ارتقای همکاری بین‌المللی امنیت سایبری، ارائه معیارهایی برای توسعه سامانه‌های امنیت سایبری ملی و افزایش آگاهی در مورد اهمیت امنیت سایبری

۳- روش تحقیق:

چون این تحقیق به شناسایی کنشگران کلیدی زیست‌بوم پدافند سایبری زیرساخت‌های حیاتی و حساس کشور می‌پردازد و نتایج آن در تصمیم‌گیری کاربرد خواهد داشت، به لحاظ هدف، کاربردی و باتوجه به ماهیت، تحقیق اکتشافی می‌باشد. رویکرد تحقیق، کمی و کیفی (آمیخته) بوده، در رویکرد کیفی پس از همپوشانی ادبیات، اسناد و مدارک و انجام مصاحبه با خبرگان، برگزاری نشست خبرگی کنشگران کلیدی، نقش و روابط این زیست‌بوم تعیین شده‌اند، همچنین در بخش کمی، پرسشنامه طراحی و بین جامعه نمونه توزیع شده است و با استفاده از نرم‌افزارهای آماری اکسل و اس‌پی‌اس‌اس و نرم‌افزار تحلیل شبکه یوسی‌آی‌نت[4] و مصورساز نت‌دراو[5]، پاسخ جامعه نمونه به سؤالات مطرح شده تحلیل شده و کنشگران کلیدی و نقش‌های عمده زیست‌بوم مشخص گردید.

[1] NCIA
[2] CYOC
[3] EC3
[4] UCINET Version ٦.٥٢٨
[5] NetDraw ٢.١٤١

جامعه آماری، شامل ٤٤ نفر از خبرگان، صاحب‌نظران و مدیران آشنا با فضای سایبر و پدافند سایبری و دارای تحصیلات دانشگاهی کارشناسی ارشد و دکتری و سوابق مدیریتی در سطوح راهبردی و سیاست‌گذاری کلان است. به‌دلیل تخصصی بودن موضوع تحقیق، روش نمونه‌گیری هدفمند (انتخاب افرادی که بیشترین اطلاعات را از موضوع دارند) همگون (انتخاب افراد با خصوصیات مشترک) و گلوله برفی (شناسایی افراد از طریق معرفی تا اشباع نظری) مدنظر قرار گرفت. پرسشنامه با مشارکت مدیران، خبرگان و اساتید حوزه پدافند سایبری طراحی و بررسی شده که این موضوع نشانگر روایی آن است. به‌منظور تعیین پایایی پرسش‌نامه، با استفاده از نرم‌افزار اس‌پی‌اس‌اس آلفای کرونباخ محاسبه‌شده و میزان آن ۰/۹٥٤ و این نشان‌گر پایایی پاسخ‌های ارائه‌شده می‌باشد.

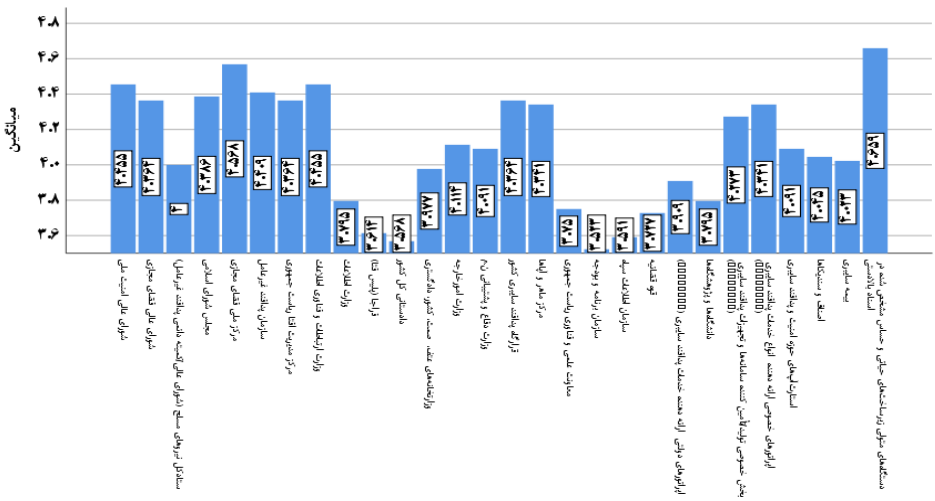
٤- تجزیه‌وتحلیل یافته‌ها:

در این بخش داده‌ها در دو حوزه کیفی و کمی تجزیه‌وتحلیل شده است. در بخش اول (تحلیل کیفی)، مطالعات صورت‌گرفته تحلیل شده و گام بعدی نیز، تحلیل کمی پرسش‌نامه و شامل دو مرحله است. در مرحله اول، داده‌های پرسش‌نامه ازلحاظ توصیفی مورد ارزیابی و تجزیه‌وتحلیل قرار گرفت. توصیف داده‌ها در این بخش در دو حالت انجام می‌گیرد. در حالت ۱- داده‌های مربوط به متغیرهای جمعیت‌شناختی و در حالت ۲- داده-های مربوط به متغیرهای پژوهش ارزیابی و توصیف شده است. پس از بررسی داده‌ها ازلحاظ توصیفی، در بخش آمار استنباطی، به بررسی سؤال‌های پژوهش پرداخته و درنهایت پیرامون نتایج به‌دست‌آمده بحث شده است.

برای این تحقیق دو پرسشنامه طراحی شد. پرسشنامه اول برای شناسایی کنشگران و نقش‌ها و پرسشنامه دوم برای بررسی ارتباطات بین کنشگران زیست‌بوم و نقش‌های آنان در قالب دو ماتریس ۲۸*۲۸ و ۲۸*۲۵ تنظیم گشت. برای تحلیل بخش اول پرسشنامه از

نرم‌افزارهای اکسل ۲۰۱۹ و اس‌پی‌اس‌اس ٦٤ بیتی نسخه ۲٦[1] استفاده و همچنین بخش دوم پرسشنامه به کمک نرم‌افزارهای یوسی‌آی‌نت و نت‌دراو[2] تحلیل شده‌اند.

با بررسی همه‌جانبه صورت گرفته، کنشگران کلیدی زیست‌بوم پدافند سایبری 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 و در مجموع ۲۸ کنشگر کلیدی برای این زیست‌بوم تعیین گردیدند که از پرسش‌شوندگان خواسته شد که میزان موافقت خود با حضور هر یک از کنشگران در زیست‌بوم را در قالب طیف لیکرت اعلام نمایند. جامعه نمونه تمامی کنشگران را تأیید نمودند که میانگین پاسخ‌های ارائه‌شده به شرح نمودار ش.۱ است:

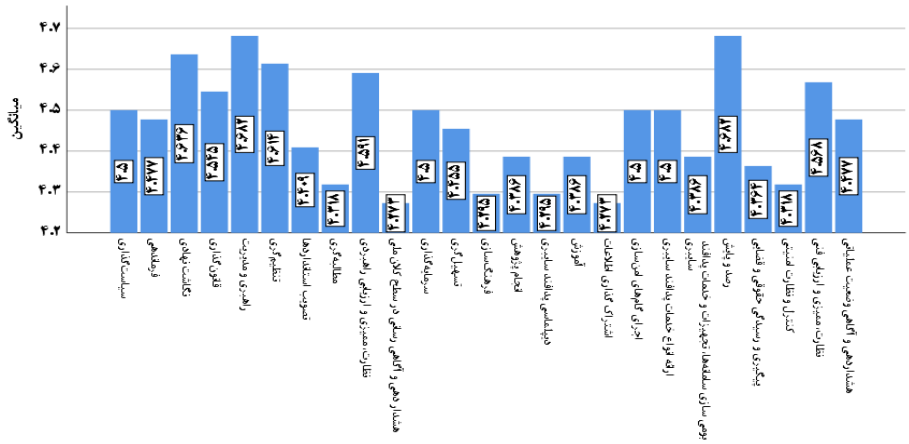


نمودار شماره ۱: میانگین نظر پاسخ‌دهندگان به سؤالات کنشگران کلیدی زیست‌بوم پدافند سایبری کشور

پس از مطالعه، نقش‌های زیادی برای کنشگران این زیست‌بوم احصاء که به‌تدریج در فرایند پژوهش تعدیل و درنهایت ۲۵ نقش اصلی (در سطح راهبردی و عملیاتی – اجرایی) انتخاب گردیدند که از جامعه نمونه پرسیده شد و جامعه نمونه تمامی نقش‌ها را تأیید نمودند که پاسخ‌ها به شرح نمودار ش. ۲ است: در بخش دوم پرسشنامه به‌دلیل خاص

[1] IBM SPSS Statistics 26
[2] NetDraw 2.141

بودن ماتریس‌های ارتباط بین کنشگران و نقش‌ها، برای نیل به پاسخ، موضوع در جلسه خبرگی با حضور ۵ نفر از خبرگان، مطرح و سپس داده‌های جمع‌آوری‌شده در نرم‌افزار یوسی‌آی‌نت ذخیره‌سازی و با استفاده از نرم‌افزار تصویرسازی نت‌دراو شبکه بصری روابط میان بازیگران ترسیم گردید. نرم‌افزار یوسی‌آی‌نت یکی از مهم‌ترین نرم‌افزارهای تحلیل نقشه‌های ادراکی برای تحلیل‌های مبتنی بر تحقیق در عملیات نرم (نگاشت شناختی، نگاشت مفهومی، نگاشت علی و نگاشت شناختی فازی) و یک گزینه کاربردی است. نرم‌افزار نت‌دراو برای تصویرسازی گراف شبکه و بهینه‌سازی گراف‌ها استفاده می‌شود.



نمودار شماره ۲: میانگین نظر پاسخگویان به سؤالات نقش‌های عمده کنشگران زیست‌بوم پدافند سایبری

۵- نتیجه‌گیری:

ازآنجاکه یکی از عوامل مؤثر در مصون‌سازی زیست‌بوم سایبری کشور، شناسایی، تعیین نقش و ایجاد هماهنگی و هم‌افزایی بین کنشگران نهادی حوزه پدافند سایبری است. در این پژوهش، برای رفع دغدغه اختلاف‌نظر میان کنشگران کلیدی این حوزه و مبهم بودن نقش هر یک و روابط بین آن‌ها، با استفاده از رویکرد زیست‌بوم به مسئله پرداخته شده است. با مطالعه ادبیات نظری، بررسی نتایج پژوهش‌های قبل درخصوص زیست‌بوم‌های سایبری، بررسی اسناد بالادستی و انجام مطالعه درصدد پاسخگویی به سؤال اصلی پژوهش (کنشگران کلیدی زیست‌بوم پدافند سایبری کشور کدام‌اند؟) و سؤالات فرعی (۱-

نقش‌های عمده کنشگران کلیدی زیست‌بوم پدافند سایبری زیرساخت‌های حیاتی و حساس کشور کدام‌اند؟ ۲- ارتباطات بین کنشگران کلیدی زیست‌بوم پدافند سایبری زیرساخت‌های حیاتی و حساس کشور چگونه است؟) برآمد.

نتیجه تجزیه‌وتحلیل داده‌های سؤال اصلی پژوهش به شرح جدول شماره ۳ است:

جدول شماره ۳: 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)
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 ...)
	اپراتورهای بخش 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 امکان نقش‌آفرینی کنشگران دیگری نیز در این زیست‌بوم وجود داشته باشد یا اینکه متناسب با تغییرات محیط زیست‌بوم و شرایط، در گذر زمان کنشگرانی به زیست‌بوم اضافه و یا از آن حذف شوند.

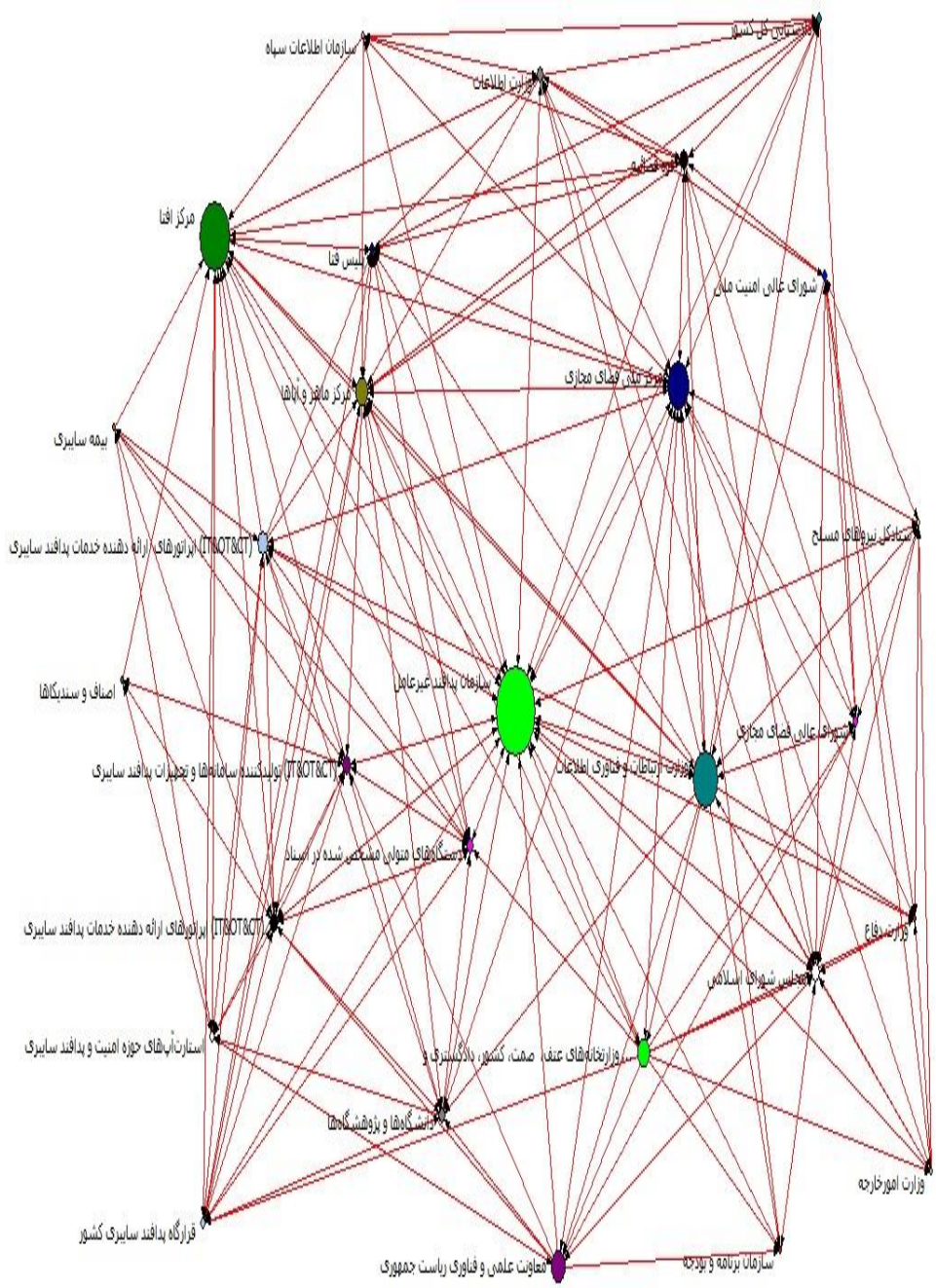
نتیجه تجزیه‌وتحلیل داده‌های سؤال فرعی اول پژوهش به شرح جدول شماره ٤ است:

جدول شماره ٤: نقش‌های عمده کنشگران کلیدی زیست‌بوم پدافند سایبری

ردیف	نقش عمده	ردیف	نقش عمده
۱	راهبری و مدیریت	١٤	تسهیلگری
۲	رصد و پایش	١٥	تصویب استانداردها
۳	نگاشت نهادی	١٦	انجام پژوهش
٤	تنظیم‌گری	١٧	آموزش
٥	نظارت، ممیزی و ارزیابی راهبردی	١٨	بومی‌سازی سامانه‌ها، تجهیزات و خدمات پدافند سایبری
٦	نظارت، ممیزی و ارزیابی فنی	١٩	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	٢٤	هشداردهی و آگاهی‌رسانی در سطح کلان ملی
۱۲	فرماندهی	٢٥	اشتراک‌گذاری اطلاعات تهدید سایبری
۱۳	هشداردهی و آگاهی وضعیت عملیاتی		

نتیجه تجزیه‌وتحلیل داده‌های سؤال فرعی دوم پژوهش به شرح زیر است:

شبکه روابط میان کنشگران کلیدی زیست‌بوم پدافند سایبری برگرفته ازنظر خبرگان، در نمودار ش. ۳ آورده شده است.



نمودار شماره ۳: شبکه روابط میان کنشگران کلیدی زیست‌بوم پدافند سایبری کشور با تعیین درجه مرکزیت

در یک زیست‌بوم، کنشگرهایی که روابط بیشتری با سایر کنشگران دارند، می‌توانند دارای موقعیت‌های بهتری باشند. این کنشگرها درنتیجه داشتن ارتباطات بالا اغلب می‌توانند به بیشتر منابع زیست‌بوم دسترسی داشته باشند و از آن‌ها استفاده کنند. در نمودار ترسیم‌شده، اندازه گره‌ها بر اساس درجه مرکزیت[1] کنشگران زیست‌بوم نمایش داده شده است. شاخص بینّیت[2] یا مرکزیت بینابینی به میزانی که یک گره در کوتاه‌ترین مسیر میان هر دو گره دیگر در شبکه قرار می‌گیرد دلالت دارد. هرچه مرکزیت بینابینی یک کنشگر بیشتر باشد قدرت واسطه‌گری و پل زنندگی آن بیشتر است و می‌توان گفت کنشگری که بینابینی بیشتری دارد، در اتصالات شبکه تأثیرگذارتر است. در شبکه ترسیم‌شده این پژوهش، بیشترین مرکزیت بینابینی متعلق به سازمان پدافند غیرعامل، وزارت ارتباطات و فناوری اطلاعات، مرکز ملی فضای مجازی، مرکز مدیریت راهبردی افتا، مرکز ماهر و آپاها و دستگاه‌های متولی زیرساخت‌های حیاتی و حساس کشور است و در نمودار شماره ۴ مشاهده می‌شود.

در نمودار شماره ۵ ارتباط بین کنشگران و نقش‌ها ترسیم و شاخص درجه مرکزیت توسط نرم‌افزار نت‌دراو لحاظ شده و اندازه گره‌ها متناسب با آن ترسیم شده است.

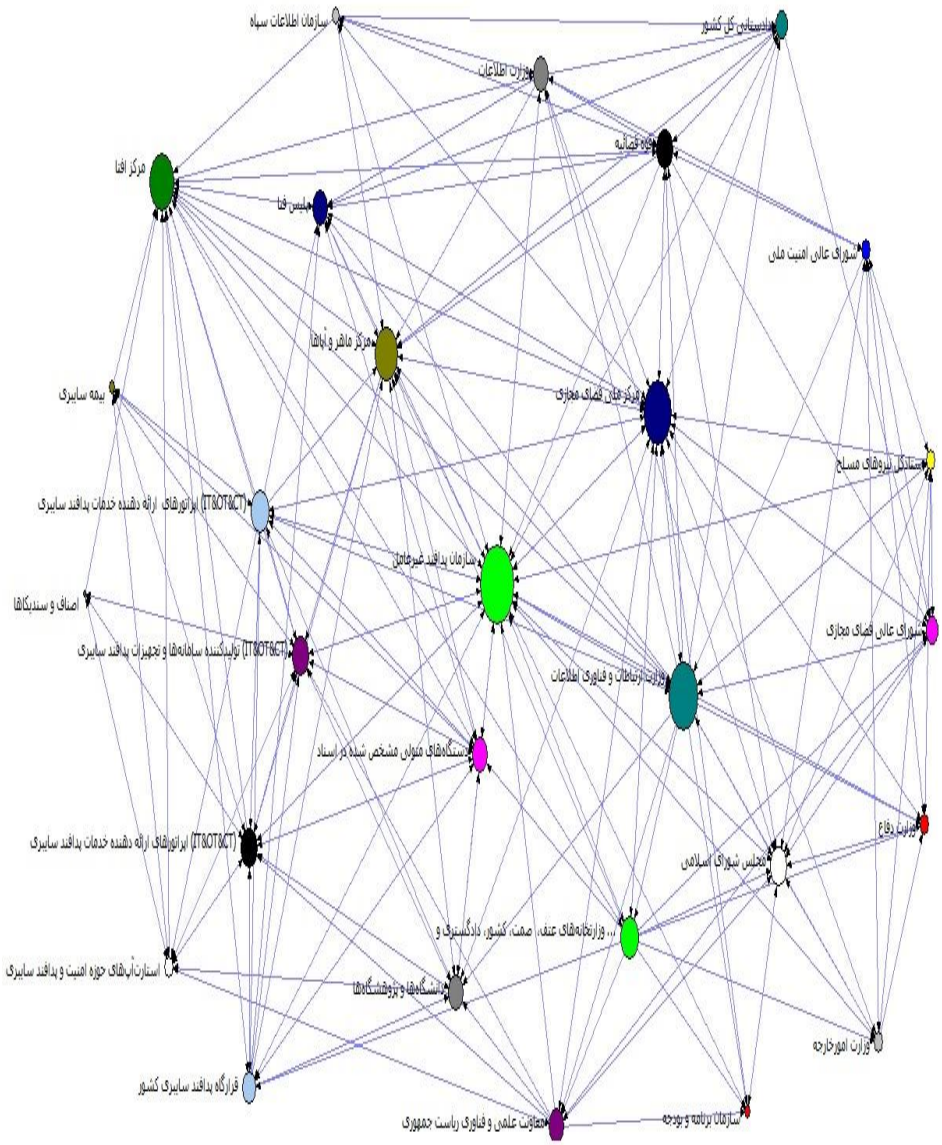
پیشنهادها:

۱- برای صیانت از زیست‌بوم سایبری کشور و به‌منظور محافظت از زیرساخت‌های حیاتی، حساس و مهم کشور، کنشگران کلیدی زیست‌بوم پدافند سایبری می‌بایست متناسب با نقش‌های تعیین‌شده اقدام و در مشارکت و هم‌افزایی با یکدیگر موجبات مقابله با تهدیدات و حملات علیه سرمایه‌های سایبری کشور را فراهم نمایند.

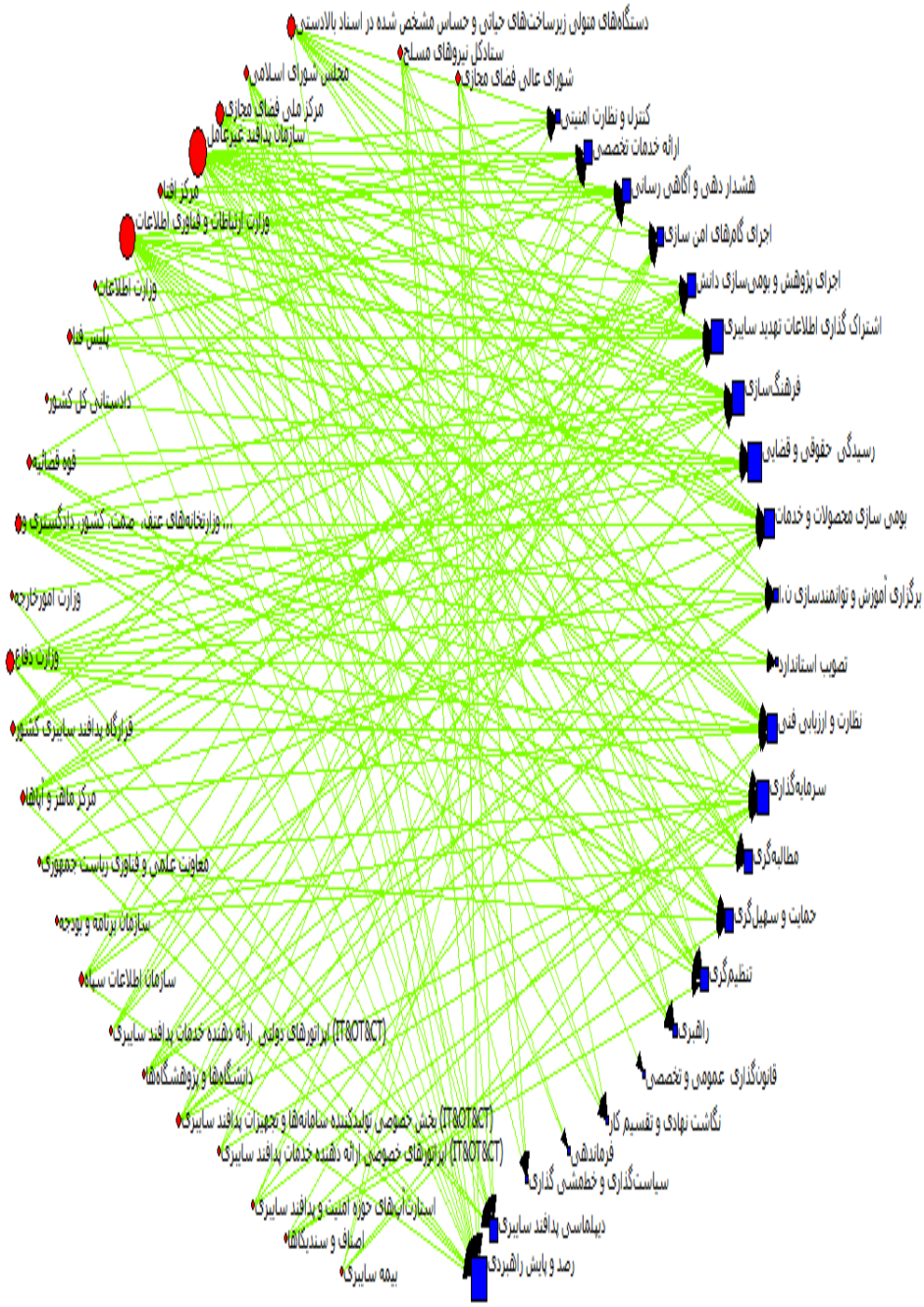
۲- باتوجه به اولویت تعیین‌شده برای کنشگران بخش عملیاتی، تأکید جامعه نمونه بر اولویت دادن بخش خصوصی درزمینه اقدامات اجرایی و عملیاتی پدافند سایبری کشور

1 degree
2 Betweenness

و استفاده حداکثری از ظرفیت بخش خصوصی است و حوزه حاکمیتی بیشتر باید نقش‌های راهبری، تنظیم‌گری، نظارت و ارزیابی، تسهیلگری و ... را ایفا و از تصدی‌گری تا حد ممکن پرهیز نماید.



نمودار شماره ٤: گراف شبکه روابط میان کنشگران کلیدی زیست‌بوم پدافند سایبری کشور با تعیین شاخص بینیت



نمودار شماره ۵: گراف شبکه روابط میان کنشگران کلیدی زیست‌بوم با نقش‌ها با تعیین درجه مرکزیت

فهرست منابع و مآخذ
الف. منابع فارسی

- اجاقی، حامد؛ یزدانی، حمیدرضا و محمدی، مهدی (۱۳۹۸). ***شناسایی بازیگران اصلی و نقش‌های کلیدی در زیست‌بوم نوآوری نوپاها***. نشریه علمی مدیریت نوآوری، شماره ۱ .
https://www.nowavari.ir/article_81027.html
- پورشاسب، عبدالعلی و نظری نژاد، احمدعلی (۱۳۹۹). ***تدابیر و راهکارهای پدافند غیرعامل در حفاظت از زیرساخت‌های حیاتی جمهوری اسلامی ایران***. فصلنامه مطالعات دفاعی استراتژیک، سال هجدهم، شماره ۲۸، ۳۱۲-۲۸۹
https://sds.sndu.ac.ir/article_1185_90a74de54e509e798f7b104ccbce132f.pdf
- تقی پور، رضا؛ لشکریان، حمیدرضا و یزدانی چهاربرج، رحیم (۱۳۹۸). ***الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران***. فصلنامه علمی امنیت ملی، سال نهم، شماره ۳٤،
https://www.sid.ir/paper/94104/fa#downloadbottom
- حکیم جوادی، علی و سپهری، محمدمهدی (۱۳۹٤). ***مدل زیست‌بوم دولت همراه ایران، تحلیل و شناخت بازیگران اصلی***. فصلنامه علمی پژوهشی فناوری اطلاعات و ارتباطات ایران، شماره ۲٤، ۳۷-۵۲
http://jour.aicti.ir/Article/8320
- زنگنه نژاد، نرجس؛ معینی، علی؛ حاجی حیدری، نسترن و آذر، عادل (۱۳۹۸). ***زیست‌بوم ارتباطات سیار در ایران مبتنی بر روش تحلیل شبکه‌های اجتماعی***. نشریه علمی مطالعات مدیریت کسب‌وکار هوشمند- سال هفتم شماره ۲۸، ۵ – ۲۸
https://ims.atu.ac.ir/article_10228.html
- سازمان پدافند غیرعامل کشور (۱۳۹٤). ***سند راهبردی پدافند سایبری کشور***
https://cmpd.wrm.ir/uploaded_files/DCMS/Circulars_files/wrm_c86bdc_1470032555.pdf
- سازمان پدافند غیر عامل (۱٤۰۱). ***طرح راهبردی حفاظت از زیرساخت‌های کشور***
https://dotic.ir/news/13339/
- سپهری، محمد، (۱٤۰۰). ***مصون‌سازی زیرساخت‌های سایبری کشور در برابر تهدیدهای آمریکا***، فصلنامه مطالعات جنگ، سال سوم، شماره هشتم،
https://jtd.iranjournals.ir/article_37218.html
- عابدی، محمد و کریمی قهرودی، محمدرضا (۱۳۹۹). ***بهره گیری از چارچوب کانوین در مواجهه با پویایی و پیچیدگی امنیت فضای سایبر***. همایش پژوهش‌های نوین در علوم و فناوری،
https://civilica.com/doc/853601/
- کافی، سعید (۱۳۹۹). ***شاخص‌های دفاعی-امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران مبتنی بر رویکردهای پدافند غیرعامل***. مجله سیاست دفاعی، شماره ۱۱۱،
https://dpj.ihu.ac.ir/article_205761.html

- ملائی، علی؛ کارگری، مهرداد و صنیعی، محمدحسین (۱۳۹۸). ***متولیان تأثیرگذار بر فرایند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری در نظام دفاع سایبری***. فصلنامه امنیت ملی، سال نهم، شماره ۳۳، https://ns.sndu.ac.ir/article_859.html
- محقر، محمد علی؛ محمدی، مهدی؛ مختارزاده، نیما و شهیدی پور، روح اله (۱۳۹۸). ***چارچوب مفهومی شکل‌گیری زیست‌بوم های کارآفرینی دانشگاه پایه شهر تهران***. نشریه علمی – پژوهشی نوآوری، سال هشتم، شماره ٤، https://www.nowavari.ir/article_102632.html

ب. منابع انگلیسی

- blackkite. (2021). ***what-is-a-cyber-ecosystem-and-how-its-security-matters***. Retrieved from blackkite web site: https://www.blackkite.com/
- ETSI. (2020). ***Global Cyber Security Ecosystem***. ETSI TR 103 306 V1.4.1 (2020-03) TECHNICAL REPORT. https://cdn.standards.iteh.ai/samples/58896/6587d8944e2447bf9d548f97d99348bb/ETSI-TR-103-306-V1-4-1-2020-03.pdf
- Morgan, N. (2021). ***how-you-can-create-an-immune-cyber-ecosystem***. Retrieved from triskelelabs web site: https://www.triskelelabs.com
- NiuYanga, W. Xiao-Feng, XuaGuo-RongPangb, & Chun-LeiZhanga. (2018). ***Research on the Construction of a Novel Cyberspace Security Ecosystem*** *Engineering*, 47-52. https://www.sciencedirect.com/science/article/pii/S2095809917307889
- POTII, O. (2018). ***CYBERSECURITY IN UKRAINE: PROBLEM AND PERSPECTIVE***. Odessa: ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection. https://www.linkedin.com/pulse/cyber-security-ecosystem-collaborate-its-your-choice- arun-raghu
- Sadik S, Ahmed M, Sikos LF, Islam AKMN.(2020). **Toward a Sustainable Cybersecurity Ecosystem**. Computers. 2020; 9(3):74. https://doi.org/10.3390/computers9030074
- Rilla, N. Lima-Toivanen, M. & Myllyoja, J. (2018). **ASEAN Cybersecurity Innovation Ecosystem: A Co-creation approach**. European Union horizon 2020. https://cris.vtt.fi/en/publications/asean-cybersecurity-innovation-ecosystem-a-co-creation-approach