Center for Strategic Studies of the
Islamic Republic of Iran Army

**Quarterly Journal Of
Army Strategic Research
Print ISSN:27834212
Volume 3, Issue 8
Summre 2024
P.P. 109-128**

Pathology of cyber deterrence system

Case study: pharmaceutical industries related to the defense sector

Sahar Ghadimnejad [1] , Ebrahim Nazari Farokhi [*2], Behrouz Dolatshah

Abstract

The current research was conducted with the aim of identifying the damage of the cyber deterrence system in the field of pharmaceutical industries related to the defense sector.

This research was carried out in terms of applied purpose, quantitative and descriptive-exploratory method with Delphi approach. The statistical population of the research included 21 information technology experts of Pharmaceutical Company related to the defense sector. The primary dimensions, components and indicators were extracted based on the review of the research literature and based on the three-stage Delphi method, dimensions, components and indicators were identified. The results showed that the damages of cyber deterrence in the pharmaceutical industry in three dimensions of threat of retaliation with components such as physical information security, information security, design and implementation, technical factors and economic factors; The denial dimension can be categorized with components such as human resource security, organizational culture, lack of user awareness, strategic management, and managerial factors, while the dimension of being caught with components such as environmental risk, technical risk, physical risk, data risk, risk management, and human risk can be categorized.

Keywords: cyber deterrence damages, threat of retaliation, denial, entrapment.

Citation: Ghadimnejad, Sahar; Nazari Farokhi Ebrahim, Dolatshah, Behrouz (2024). Pathology of cyber deterrence system Case study: pharmaceutical industries related to the defense sector; *Army Strategic Research Quarterly 3(8). 109-128*

1. 1. Master's degree in Information Technology Management, Advanced Systems, University of Research Sciences, Tehran, Iran.
2. PhD in Information Technology Management, Dafos Aja faculty member, Tehran, Iran. (author) (Email: ebrahimnazarifarokhi60@gmail.com)
3. PhD in Strategic Management, Islamic Azad University, Research Sciences Unit, Tehran, Iran.

Received: 2024/06/07 **Article Type : Research - based**
Accepted: 2024/09/04

فصلنامه پژوهش‌های راهبردی ارتش
شاپای انتشار: ۲۷۸۳۴۲۱۲
سال سوم، شماره هشتم
تابستان ۱۴۰۳
صص: ۱۲۸-۱۰۹

مرکز مطالعات راهبردی آجا

آسیب‌شناسی سامانه بازدارندگی سایبری
مورد مطالعه: صنایع داروسازی مرتبط با بخش دفاعی

سحر قدیم نژاد[۱]، ابراهیم نظری فرخی*[۲]، بهروز دولت شاه[۳]

چکیده

پژوهش حاضر با هدف شناسایی آسیب‌های بازدارندگی سامانه سایبری در حوزه یکی از صنایع دارویی انجام شد.

این پژوهش از نظر هدف کاربردی، از نوع، کمی و به روش توصیفی- اکتشافی با رویکرد دلفی انجام شد. جامعه‌ی آماری تحقیق شامل ۲۱ نفر از خبرگان فناوری اطلاعات شرکت داروسازی مرتبط با بخش دفاعی است. ابعاد، مؤلفه‌ها و شاخص‌های اولیه بر اساس مرور ادبیات تحقیق استخراج و بر اساس روش دلفی سه مرحله، ابعاد، مؤلفه‌ها و شاخص‌ها شناسایی شد. روایی تحقیق به صورت محتوایی و پایایی آن با روش آلفای کرونباخ محاسبه و تأیید شد. در بخش استنباطی، با استفاده از روش تحلیل عاملی تأییدی نسبت به اعتبارسنجی عوامل بهره گرفته شد. نتایج نشان داد که آسیب‌های سامانه بازدارندگی سایبری در صنعت دارویی مورد مطالعه در سه بُعد تهدید به تلافی با مؤلفه‌هایی همانند امنیت فیزیکی اطلاعات، امنیت اطلاعات، طراحی و پیاده‌سازی، عوامل فنی و عوامل اقتصادی، بُعد انکار با مؤلفه‌هایی همانند امنیت نیروی انسانی، فرهنگ سازمانی، نبود آگاهی کاربران، مدیریت راهبردی و عوامل مدیریتی بُعد گرفتارشدن با مؤلفه‌هایی همانند ریسک‌های: محیطی، فنی، فیزیکی، داده، مدیریت ریسک و ریسک انسانی قابل دسته‌بندی است.

واژگان کلیدی: آسیب های بازدارندگی سایبری، تهدید به تلافی، انکار، گرفتارشدن.

استناد: قدیم نژاد، سحر؛ نظری فرخی، ابراهیم، دولت شاه، بهروز (۱۴۰۳). آسیب‌شناسی سامانه بازدارندگی سایبری مورد مطالعه: صنایع داروسازی مرتبط با بخش دفاعی؛ *فصلنامه پژوهش‌های راهبردی ارتش ۳(۸)*. صص ۱۲۸-۱۰۹.

۱. کارشناسی ارشد مدیریت فناوری اطلاعات گرایش سیستم‌های پیشرفته، دانشگاه علوم تحقیقات، تهران، ایران
۲. دکترای مدیریت فناوری اطلاعات، عضو هیئت علمی دافوس آجا ، تهران ایران. (نویسنده مسئول)
Email: ebrahimnazarifarokhi60@gmail.com
۳. دکترای مدیریت استراتژی، دانشگاه آزاد اسلامی واحد علوم تحقیقات، تهران ایران.

نوع مقاله: پژوهشی
تاریخ دریافت: ۱۴۰۳/۰۳/۱۸
تاریخ پذیرش: ۱۴۰۳/۰۶/۱۴

مقدمه

امروزه همه چیز با سرعت بالایی در حال دگرگونی است و همه حکومت‌ها در پی نوسازی و تکامل ساختاری و سازمانی خود جهت تطبیق پیدا کردن با این وضعیت جدید هستند. این دگرگونی‌ها و تغییرات به صورت‌های مختلف جوامع و حکومت‌ها را تحت‌شعاع قرار داده و آن‌ها را در مواردی دچار چالش کرده و در زمینه‌های دیگر فرصت‌های زیادی برای آن‌ها به ارمغان اورده است (رحیم‌اف و موحدی، ۵۵:۱۳۹۹). این روند به شکلی صورت پذیرفته است که، بشر در مقایسه با هیچ دوره زمانی دیگر از تاریخ خود به اندازه دوران حال حاضر سیاسی نبوده است و می‌توان گفت یکی از عوامل مهم سیاسی شدن مردمان جوامع و حکومت‌ها، شکل‌گیری عرصه جدید ارتباط بین افراد است(سیف‌الدین و رهبر، ۷۵:۱۳۹۲). این عرصه جدید به شکل گسترده‌ای زمینه ارتباطات بین آن‌ها را فراهم آورده است. در واقع می‌توان گفت، فضای سایبر ظرفیت‌های جدید و امکاناتی را برای مخاطبان فراهم می‌کند که به توانمندشدن مخاطب در به دستگیری کنترل افراد دیگر، نقش‌آفرینی، تأثیرگذاری، ایجاد بی‌نظمی و تشویش، اغتشاش و بر هم زدن امنیت اجتماعی در سطح جوامع کمک می‌کند (رحیم اف و موحدی، ۶۰:۱۳۹۹). در حقیقت، قدرت سایبری امروزه بُعد مهمی از زیست‌واره جهانی را شکل می‌دهد. اطلاعات و فناوری‌های اطلاعاتی در سپهر سیاسی، اقتصادی و نظامی نقش حیاتی ایفا کرده و مقدمات فعالیت‌های عملیاتی را فراهم می‌آورد. با گسترش روزافزون فضای سایبری، نگرانی‌های زیادی هم در این خصوص ایجاد می‌شود و در کنار آثار مثبتی که در بهبود زیست جهانی دارد، برخی ابعاد منفی و قابل توجه دیگری نیز دارد که حتی ممکن است آثار آن مخرب ترانسفورماتور از جنگ‌های نظامی بوده و امنیت و حیات ملی مردمی را به چالش بکشاند. با توسعه فناوری‌های اطلاعاتی، خطرات دیگری همچون حمله مجازی یا جاسوسی سایبری در کمین تصمیم‌سازان و سیاست‌گذاران کشورهاست. ولی با توجه به هزاران حمله سایبری که در طی روز اتفاق می‌افتد، کار تمیز حملات جدی و مهم از حملات ناکارآمد و جزیی بسیار سخت شده است (رمضان‌زاده و همکاران، ۷۵:۱۳۹۹). بازدارندگی سایبری، بر پایه اصول حاکم بر نظریه‌های بازدارندگی سنتی شکل گرفته است. در حال حاضر آنچه قطعی است این است که بازدارندگی سایبری در حوزه غیرنظامی، علاوه بر پوشش کامل امنیت ایستا و دفاع فعال معطوف به توانمندی‌های پیش‌نگری و پیشگیری در حوزه‌های زیرساختی است و حوزه نظامی بر دفاع فعال و توانمندی‌ای تهاجمی بازدارنده

تمرکز بیشتری باید داشته باشند (احدی و شاه محمدی،۱۳۹۷:۷۴). بر این اساس، آسیب‌شناسی بازدارندگی شرکت‌های مختلف، مستلزم شناخت دقیق مؤلفه‌ها و شاخص‌های بازدارندگی فضای سایبری بوده، که در ایران متاسفانه مورد غفلت واقع شده است.

تهدیدات سایبری یکی از جدی‌ترین چالش‌های امنیتی، اقتصادی و ملی است که شرکت‌های مختلف با آن مواجه هستند. در واقع، فضای سایبری، مجموعه‌ای از محیط اطلاعاتی است که شبکه‌های درهم‌تنیده شامل شبکه‌های مخابراتی، اینترنت، سامانه‌های کامپیوتری، پردازنده‌ها و کنترلرها است. با توجه به رشد و نفوذ روزافزون فناوری اطلاعات و ارتباطات در حوزه‌های مختلف جوامع، سازمان‌ها و کسب‌وکارها، حفظ نگهداری و ارتقای امنیت فضای سایبری از اهمیت بالایی برخوردار است. در این راستا، با توجه به جایگاه و نقش سازمان‌های فعال درحوزه‌ی دفاعی، این مهم اهمیتی صدچندان می‌یابد، چراکه به‌طور قطع بر امنیت ملی کشور تأثیر خواهد گذاشت. آمارهای ارائه‌شده از منابع معتبر بین‌المللی، حاکی از یکپارچه‌نبودن فعالیت‌های این حوزه، همگرا نبودن اهداف و هم‌راستایی سیاست‌ها و به‌طورکلی، توجه نکردن کافی به موضوع امنیت فضای سایبری و در نتیجه، آسیب‌پذیری جدی کشور در این حوزه است. بر این اساس، دغدغه اصلی پژوهش حاضر، آسیب‌شناسی سامانه بازدارندگی سایبری در یکی از صنایع داروسازی مرتبط با بخش دفاعی است. وضعیت مطلوب حوزه امنیت شامل هشت حوزه دانشی می‌شود که تقریباً در تمام چارچوب‌ها مشترک است. این موارد عبارت‌اند از: حاکمیت سیستمی امنیت و مدیریت مخاطرات امنیتی، مدیریت امنیت دارایی‌ها، معماری امنیتی و اصول مهندسی امنیت، مدیریت امنیت شبکه و ارتباطات، مدیریت هویت و سطوح دسترسی، اجرای ساختارمند انواع آزمون‌های امنیتی، مدیریت عملیات امنیت و مدیریت امن چرخه توسعه محصولات (زو،۲۰۲۲). ازاین‌رو، رسیدن به سطح امنیتی مناسب، نیازمند داشتن آگاهی کامل در خصوص نقاط آسیب‌پذیر و چالشی فضای سایبری بوده تا راه را برای رسیدن به وضعیت مطلوب را برای سازمان فراهم نمایند.

با عنایت به موارد فوق، پژوهشی حاضر با هدف پاسخگویی به سؤال اصلی «تحقیق مبنی بر این آسیب‌های بازدارندگی سامانه سایبری در صنایع داروسازی مرتبط با بخش دفاعی کدامند؟» انجام شد.

همچنین به نظر می‌رسد که با انجام این تحقیق و ریشه‌یابی عوامل مؤثر بر بازدارندگی فضای سایبری، می توان به فواید زیر دست پیدا کرد:

- امکان تدوین برنامه‌های راهبردی سازمانی به‌منظور امن‌سازی اطلاعات در برابر حملات سایبری؛
- شناسایی نقاط آسیب‌پذیر در سازمان و تدوین نظارت، کنترل و سیاست‌های پیشگیرانه؛
- تحقیق و پژوهش، مستندسازی و پیدا کردن راه حل های ایمن؛
- توسعه و بروزرسانی سامانه تداوم کسب و کار و استاندارد های بازیابی فاجعه.

از سوی دیگر، انجام نشدن این تحقیق می‌تواند تبعات منفی زیر را برای سازمان درپی داشته باشد:

- ناتوانایی در شناسایی حملات جدید، برنامه‌ریزی به‌منظور مقابله و ریشه‌یابی رخدادهای امنیتی؛
- ناتوانایی در پیش‌بینی تهدیدات امنیتی جدید و به‌روزبودن با زیرساخت‌های در حال تحول؛
- کاهش مزیت رقابتی در بین رقبا و از دست رفتن اطلاعات مهم و حساس شرکت
- کاهش درآمد و افزایش هزینه؛
- ازدست دادن داده و اطلاعات مهم.

پیشینه

سایبر واژه‌ای است برگرفته شده از لغت kybernetes به‌معنای سکاندار یا راهنما و نخستین کسی که واژه فضای سایبر را به‌کار برد، ویلیام گیتسون نویسنده داستان‌های علمی تخیلی، در کتاب نورومنسر بود (صادقی و همکاران، ۷:۱۴۰۰).

فضای سایبر یا فضای مجازی به تعبیر برخی نویسندگان عبارت است از: «مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق وسایل مخابراتی و رایانه بدون در نظر گرفتن مرزهای جغرافیایی است». به بیانی دیگر «محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص خود؛ در آن، زنده و مستقیم روی می‌دهد. «قید واقعی» مانع از آن می‌شود که تصور شود مجازی بودن این فضا به معنای غیر واقعی بودن آن است؛ چرا که در این فضا نیز همان خصوصیات تعاملات فردی در دنیای خارج همانند مسئولیت وجود دارد. ضمن این که فضای سایبر در حقیقت یک «محیط» است که ارتباطات در آن شکل می‌گیرد؛ نه صرف مجموعه‌ای از ارتباطات. از سوی دیگر، این ارتباطات هرچند ممکن است در همه‌ی شرایط بر خط نباشد، ولی واقعی، زنده و مستقیم است. ازاین‌رو، تأثیر و تأثر بالایی در این روابط رخ می‌دهد (دوستی مطلق، ۳:۱۴۰۰).

ارزیابی سازوکارهای سه‌گانه بازدارندگی در فضای سایبری، عبارت‌اند از:

- تلافی: به علت نبود قطعیت شناسایی حمله‌کننده، تهدید به تلافی کارایی زیادی ندارد. با این وجود، این سازوکار هم چنان به عنوان یکی از مهمترین رکن‌های معادله بازدارندگی در فضای سایبر باقی خواهد ماند. مراحل پاسخ‌های تلافی‌جویانه بر اساس شدت حمله شامل: اقدام‌های دیپلماتیک، اقتصادی، سایبری، قدرت فیزیکی و نیروی هسته‌ای است. پیشرفت‌های اخیر در حوزه سامانه‌های فارنزیک نیز کارایی این مکانیزم را افزایش داده است.
- انکار: امکان نداشتن شناسایی می‌تواند مشکلاتی را برای مکانیزم‌های هنجار و تلافی ایجاد نماید. ولی در مکانیزم‌های انکار و گرفتارسازی نیازی به شناسایی نیست. یک دفاع سایبری قوی می‌بایست شامل چندین مؤلفه باشد. یکی از این مؤلفه‌ها، حفظ و نگهداری یک نسخه از تمامی اطلاعات موجود در یک مکان امن است تا درصورت رخداد حمله سایبری و از دست رفتن اطلاعات، بتوان از اطلاعات پشتیبان استفاده نمود. مؤلفه دیگر، برگشت‌پذیری است. به این معنا که در صورت به‌وقوع پیوستن هرگونه حمله سایبری و بروز خرابی، بتوان کل سامانه را به حالت اول خود برگرداند. استفاده از مکانیزم انکار بیشتر خواهد توانست گروه‌ها و دولت‌های ضعیف را از حمله منصرف کند و دولت‌های قوی که از قدت بالایی برخوردار هستند این روش‌ها قادر به بازداشتن آن‌ها نیستند.
- گرفتارسازی: استفاده از این سازوکار مستلزم درک یکسان همگان مبنی بر سودمندی استفاده از فضای مجازی و اینترنت برای ایشان است. در صورت رسیدن به چنین دیدگاهی، به‌طور حتم به دنبال استفاده غیر صلح‌آمیز از این فضا نخواهند بود. بارزترین نمونه استفاده از این مکانیزم در بازدارندگی، موضوع اختلافات سایبری چین و آمریکا است. واضح است که ادامه قدرت چین به اینترنت بستگی تام دارد. در واقع این مکانیزم بر پایه‌ی وابستگی متقابل کار می‌کند. برخی از وابستگی‌ها دو یا چند جانبه هستند، ولی برخی دیگر سامانه‌ای بوده و بر اثر اخلال در سامانه، منافع از دست خواهند داد. در این حالت حاکمیت کشورها به دنبال ثبات سامانه‌ای خواهند رفت. چین به دلیل وابستگی به اینترنت، اقدام‌های بی‌ثبات‌ساز در اینترنت را پایان بخشید. این مکانیزم برای تمام کشورها کارایی ندارد؛ به عنوان مثال کشوری مانند کره شمالی را نمی‌توان با این سازوکار بازداشت (دهقانی، ۱۳۹۷:۵۴).

جدول (۱) پیشینه تحقیق‌های انجام شده

محقق	سال	عنوان	نتیجه
ریاضی	۱۴۰۲	الگویبازدارندگی راهبردی سازمان‌های نظامی در محیط امنیتی	یافته‌های تحقیق در نهایت به ارائه‌ی الگوی بازدارندگی راهبردی سازمان‌های نظامی در محیط امنیتی منتهی شد که دارای ۶ اصل(تأثیرگذارترین اصل، معنویت و پس از آن نیز به ترتیب، جلوگیری از منازعه، اقدام عملی، عاقبت‌اندیشی بر مبنای منطق، اعتبار ملی، منطقه‌ای و بین‌المللی و تبلیغات روانی است)، ۱۱ عامل و ۵۳ شاخص مؤثر هستند و طی الگویی به متولیان ارائه شده است.
گل محمدی و جمشیدی	۱۴۰۰	بازدارندگی سایبری و تحول در دکترین امنیتی- دفاعی اسرائیل	راهبرد بازدارندگی سایبری قلمرو مقابله با تهدیدات امنیت ملی اسرائیل را به خارج از مرزها گسترش داده و آسیب‌پذیری محیطی تهدیدات داخلی را به‌طور قابل توجهی کاهش داده است. براین اساس، گذار از ابزارهای متعارف نظامی به ابزارهای غیر متعارف، اسرائیل را به تنظیم راهبردهای امنیتی ملی با محوریت توانمندی سایبری در مقابله با کانون‌های جدید تهدید ترغیب می‌کند. آسیب‌پذیری نظامی در مقابل گروه‌های مقاومت فلسطینی در جنگ اخیر نشان داد که در برخورد با چالش جدی‌تر مثل ایران، جنگ نظامی گزینه‌ای مطلوب برای اسرائیل نیست و پیش‌بینی می‌شود که در آینده بازدارندگی سایبری جایگاه ویژه‌ای در دکترین امنیتی - دفاعی اسرائیل داشته باشد.
رحیم اف و موحدی	۱۳۹۹	الگوی راهبردیِ ارزیابیِ عملیاتِ سایبری	پس از تجزیه‌وتحلیل آماری نتایج پرسشنامه، الگوی راهبردی ارزیابی عملیات سایبری در سه بُعد، ده مؤلفه و هفتادوسه شاخص ارائه شده است.
سلمان	۲۰۲۲	بازتابی از چالش های پیش روی بازدارندگی سایبری و راه‌های پیشبرد آن‌ها	بازدارندگی سایبری چالش بزرگی بود، به خصوص که بازدارندگی در معنای عام آن پیشگیری است، بنابراین، بازدارندگی سایبری در مواجهه با چالش‌ها حملات سایبری آسیب می‌بینند.
لیلی	۲۰۲۱	بازتعریف بازدارندگی در فضای سایبری: مشارکت بخش خصوصی در راهبردهای ملی بازدارندگی سایبری	هدف نهایی کمک به تصمیم‌گیرندگان در طراحی سیاست‌ها و مقررات با هدف به حداکثر رساندن مزایای همکاری عمومی و خصوصی در بازدارندگی سایبری و در عین حال کاهش جنبه های منفی بالقوه آن است.

محقق	سال	عنوان	نتیجه
مای مون	۲۰۲۰	نقش رفتار کاربر در بهبود مدیریت امنیت سایبری	بررسی‌ها نشان داد که کاربران سامانه‌های رایانه‌ای دارای قابلیت‌های شناختی متفاوتی هستند که توانایی آن‌ها را برای مقابله با تهدیدات امنیت اطلاعات تعیین می‌کند. آن‌ها شکاف‌ها را در تحقیقات موجود شناسایی کردند و روش‌های روان‌شناختی ممکن را برای کمک به کاربران سامانه‌های رایانه‌ای برای رعایت سیاست‌های امنیتی و در نتیجه افزایش امنیت شبکه و اطلاعات ارائه نمودند.

روش شناسی

این پژوهش از نظر هدف جزو تحقیقات کاربردی، از نوع کمی بوده و به روش توصیفی-اکتشافی با رویکرد دلفی است. جامعه آماری تحقیق شامل ۲۱ نفر از خبرگان فناوری اطلاعات یکی از شرکت‌های داروسازی مرتبط با بخش دفاعی است که پرسشنامه بین ایشان توزیع شد.

ابزار اصلی جمع‌آوری اطلاعات در بخش ادبیات تحقیق، مطالعات کتابخانه‌ای و اطلاعات لازم پاسخ به سؤالات تحقیق و ارائه جدول تحلیل اولیه، از طریق مرور ادبیات حاصل شد. روایی ابزار مورد استفاده از طریق صوری و محتوایی و برای سنجش پایایی پرسشنامه و با روش آلفای کرونباخ محاسبه و تأیید شده و در بخش آمار استنباطی، ابتدا از روش دلفی برای شناسایی ابعاد، مؤلفه‌ها و شاخص‌ها استفاده شد. و برای رتبه‌بندی از روش تحلیل سلسله مراتبی استفاده شده و نرم‌افزارهای مورداستفاده در این تحقیق، SPSS نسخه ۲۳ و Exper Choice بود.

یافته‌ها

داده‌های به دست‌آمده از مطالعه ادبیات به‌صورت پرسشنامه‌ای با مبانی نظری و پیشینه تحقیق تدوین و بین خبرگان توزیع شد، سپس به روش دلفی در طی سه دوره، ابعاد، مؤلفه‌ها و شاخص‌های عوامل موضوع تحقیق شناسایی و با انجام تحلیل عاملی تأییدی اطمینان لازم از صحت اطلاعات حاصل شد. ماحصل یافته‌های تحقیق را می‌توان با ارائه الگویی در زمینه بازدارندگی سایبری تصویر کرد (مدل مفهومی شکل شماره ۱).

ویژگی‌های جمعیت‌شناختی شامل سن، سطح تحصیلات و میزان سوابق فعالیت‌های اجرایی است. خلاصه ویژگی‌های جمعیت‌شناختی مشارکت‌کنندگان گروه خبرگان در جدول شماره ۲ ارائه شده است.

جدول (۲). ویژگی‌های جمعیت‌شناختی اعضای نمونه آماری

متغیر	گروه	در ابتدای دلفی		در انتهای دلفی	
		فراوانی مطلق	درصد فراوانی	فراوانی مطلق	درصد فراوانی
سن	کمتر از ۳۰ سال	۲	۹	۲	۱۰.۵
	۳۰ تا ۴۰ سال	۱۴	۶۷	۱۳	۶۸.۵
	بالاتر از ۴۰ سال	۵	۲۴	۴	۲۱
سطح تحصیلات	لیسانس	۱۱	۵۲	۱۱	۵۸
	فوق لیسانس	۵	۲۴	۴	۲۱
	دکتری	۵	۲۴	۴	۲۱
میزان سوابق فعالیت‌های اجرایی	کمتر از ۵ سال	۱۱	۵۲	۱	۵۸
	۵ تا ۱۰ سال	۹	۴۳	۸	۴۲
	بالاتر از ۱۰ سال	۱	۵	۰	۰.۰

با توجه به یافته‌های انجام دوره‌های دلفی، شاخص‌های آماری، کمینه، بیشینه، میانگین، نما و انحراف معیار محاسبه و در هر مرحله گویایی که شرط میانگین بازی عدد ۴ را داشته در دوره بعد لحاظ و در غیر این صورت کنار گذاشته و به این ترتیب میزان اتفاق نظر خبرگان در هر دور محاسبه شده است.

دور یکم دلفی: در این دور، از ۸۱ عامل شناسایی شده، تعداد ۵ عامل با میانگینی کمتر از ۴، حذف شدند. از سوی دیگر، توجه به اینکه سطح معنی‌داری کوچکتر از ۰.۰۵ و ضریب کندال برابر ۰/۶۶ است. بنابراین، می‌توان گفت که تفاوت میانگین رتبه‌ها معنی‌دار بوده، پس می‌توان به‌صورت کلی اجماع میان نظرات خبرگان را در خصوص همه مفاهیم دید.

دور دوم دلفی: در این دور، از ۷۶ عامل شناسایی شده در مرحله نخست، تعداد ۶ عامل با میانگینی کمتر از ۴، حذف شدند. از سوی دیگر، توجه به اینکه سطح معنی‌داری کوچکتر از ۰/۰۵ و ضریب کندال برابر ۰/۷۴ است. بنابراین، می‌توان گفت که تفاوت میانگین رتبه‌ها

معنی‌دار است، پس می‌توان به‌صورت کلی اجماع میان نظرات خبرگان را در خصوص همه مفاهیم دید.

دور سوم دلفی: در دور سوم با اعلام نظر اعضا درباره موضوع مورد مطالعه انحراف معیار ۰/۴۲ و ضریب کاندال نیز با توافق و اجماع، خبرگان ۰/۸۰ محاسبه شد.

جدول (۳) نتایج ادواری دلفی

ردیف	شاخص‌ها	میانگین	انحراف معیار
۱.	حوادث طبیعی مانند سیل، زلزله و ..	۳.۴۰	۰.۹۹۵
۲.	حوادث غیرطبیعی: اختلال برق	۴.۴۵	۰.۸۲۱
۳.	حوادث غیرطبیعی: دمای محیط	۳.۵۰	۰.۸۲۱
٤.	حوادث غیرطبیعی: ترکیدگی لوله آب	۳.۱۵	۰.۳۲۱
٥.	سازماندهی امنیت اطلاعات	۳.۴۵	۰.۷۴۸
٦.	خط‌مشی امنیت	۳.۵۰	۰.۵۵۳
۷.	کنترل دسترسی	۳.۷۰	۰.۳۲۱
۸.	امنیت منابع انسانی	۴.۴۵	۰.۵۶۸
۹.	تدوین سند راهبردی شامل چشم‌انداز، اهداف راهبردها	۴.۰۰	۰.۵۵۳
۱۰.	تخصیص منابع موردنیاز شامل بودجه، نیروی انسانی	۳.۶۰	۰.۹۹۵
۱۱.	بومیسازی استانداردها با توجه به اصل وابستگی	۳.۳۳	۰.۸۲۱
۱۲.	توسعه و به‌کارگیری ابزارها و فناوری‌های امنیتی بومی	۳.۶۲	۰.۸۲۱
۱۳.	رعایت استانداردهای امنیتی	۳.۶۲	۰.۳۲۱
۱٤.	وجود دیتا سنتر	۳.۳۶	۰.۷۴۸
۱٥.	توپولوژی و آرایش بستر شبکه	۳.۱۶	۰.۵۵۳
۱٦.	نصب دیوار آتش	۳.۴۰	۰.۳۲۱
۱۷.	رمزنگاری اطلاعات محرمانه	۴.۴۵	۰.۵۶۸
۱۸.	گرفتن نسخه پشتیبان از اطلاعات	۳.۱۵	۰.۵۵۳
۱۹.	میزان بودجه سازمان	۳.۰۵	۰.۹۹۵
۲۰.	تأمین بودجه برای آموزش‌های کارکنان	۳.۶۵	۰.۸۲۱

ردیف	شاخص‌ها	میانگین	انحراف معیار
۲۱.	تأمین بودجه برای خرید سخت‌افزارها و نرم‌افزارها	۳.۵۰	۰.۸۲۱
۲۲.	پیش از اجرا	۳.۷۰	۰.۳۲۱
۲۳.	نداشتن مهارت کافی	۴.۴۵	۰.۷۴۸
۲٤.	تداخل مسئولیت‌ها	۴.۰۰	۰.۵۵۳
۲۵.	اطلاع نداشتن از میزان ارزش اطلاعات	۳.۳۲	۰.۳۲۱
۲٦.	فرهنگ‌سازی امنیت سایبری	۳.۶۰	۰.۵۶۸
۲۷.	تدوین و اجرای راهبردهای اشاعه فرهنگ امنیت	۳.۳۳	۰.۵۵۳
۲۸.	تفکر راهبردی در رابطه با امنیت فضای سایبری	۳.۷۷	۰.۹۹۵
۲۹.	سامانه عامل	۳.۶۲	۰.۸۲۱
۳۰.	سامانه‌های کاربردی	۳.۲۵	۰.۸۲۱
۳۱.	امنیت سامانه عامل	۳.۶۲	۰.۳۲۱
۳۲.	بسته‌های نرم‌افزاری	۳.۳۶	۰.۷۴۸
۳۳.	آموزش‌های راهبردی به کارکنان	۳.۱۵	۰.۵۵۳
۳٤.	برخورد جدی با تخلف کارکنان	۳.۱۶	۰.۳۲۱
۳۵.	نظارت جامع بر عملکرد کارکنان	۳.۴۰	۰.۵۶۸
۳٦.	انگیزش کارکنان	۴.۴۵	۰.۵۵۳
۳۷.	ارتقای سطح آگاهی کارکنان	۳.۵۰	۰.۹۹۵
۳۸.	همراهی مدیریت ارشد سازمان	۳.۱۵	۰.۸۲۱
۳۹.	مشاوره و ممیزی استانداردهای امنیت	۳.۲۰	۰.۸۲۱
٤۰.	نحوه ارتباط با رقبا و شرکای تجاری	۳.۴۵	۰.۳۲۱
٤۱.	اقدام مؤثر مدیریت در برابر نقض موارد امنیت اطلاعات	۳.۵۵	۰.۷۴۸
٤۲.	تعیین معماری امنیت اطلاعات سازمان	۳.۶۵	۰.۵۵۳
٤۳.	آتش‌سوزی	۳.۵۰	۰.۳۲۱
٤٤.	لرزش	۳.۰۸	۰.۵۶۸
٤۵.	استهلاک سامانه ناشی از گردوغبار	۴.۴۵	۰.۵۵۳
٤٦.	تداخل الکترومغناطیسی	۴.۰۰	۰.۹۹۵
٤۷.	حوادث طبیعی	۴.۰۰	۰.۸۲۱
٤۸.	قطع برق	۳.۶۰	۰.۸۲۱

ردیف	شاخص‌ها	میانگین	انحراف معیار
٤٩.	آسیب‌پذیری نرم‌افزاری	۳.۳۳	۰.۳۲۱
٥٠.	آسیب‌پذیری سخت‌افزاری	۳.۷۷	۰.۷۴۸
٥١.	خطا در جریان TCP/IP	۳.۶۲	۰.۵۵۳
٥٢.	آسیب‌پذیری شبکه	۳.۲۵	۰.۳۲۱
٥٣.	بدافزارها	۳.۲۵	۰.۵۶۸
٥٤.	آسیب پایگاه داده	۳.۴۰	۰.۵۵۳
٥٥.	سیب سخت‌افزاری سیستم	۴.۴۵	۰.۹۹۵
٥٦.	آسیب زیرساخت	۳.۵۰	۰.۸۲۱
٥٧.	عملکرد تجهیزات	۳.۱۵	۰.۸۲۱
٥٨.	حذف یا تغییر داده	۳.۴۵	۰.۳۲۱
٥٩.	محیط انتقال داده	۳.۵۰	۰.۷۴۸
٦٠.	اشتراک‌گذاری منابع	۳.۷۰	۰.۹۹۵
٦١.	شناسایی ریسک‌های حوزه امنیت فضای سایبری	۴.۴۵	۰.۸۲۱
٦٢.	ارزیابی میزان آسیب ریسک‌های احتمالی حوزه امنیت فضای سایبری	۴.۰۰	۰.۸۲۱
٦٣.	طراحی و ایجاد ساختار و تشکیلات امنیت سایبری	۳.۳۳	۰.۷۴۸
٦٤.	استفاده از استانداردها و متدولوژی‌های مدیریت ریسک امنیت فضای سایبری	۳.۶۰	۰.۳۲۱
٦٥.	ریسک عمدی	۳.۶۲	۰.۵۵۳
٦٦.	هکر و کراکر	۳.۶۲	۰.۳۲۱
٦٧.	سوءاستفاده از اطلاعات	۳.۳۶	۰.۵۶۸
٦٨.	سرقت و کلاهبرداری	۳.۱۶	۰.۵۵۳
٦٩.	بی دقتی	۳.۴۰	۰.۶۲۶
٧٠.	توانایی کارکنان	۴.۴۵	۰.۵۵۱

بر اساس نتایج به دست آمده در سه دوره دلفی، بین اعضای پنل اتفاق نظر مشاهده می‌شود و می‌توان به تکرار دورها، پایان داد؛ چراکه همه میانگین‌ها بازی عدد ۳ است. انحراف معیار پاسخ‌های خبرگان از ۰/۷۴ در دور او به ۰/۴۲ در دور سوم کاهش یافت و ضریب کاندال هم در دور سوم به ۰/۸۰ رسید؛ همچنین با توجه به اینکه ضریب کاندال در

دور سوم نسبت به دور دوم تنها با رشد ناچیز ۰/۰۴۵ افزایش یافته است و میزان اجماع، و اتفاق نظر در دو دور متوالی رشد قابل توجهی را نشان نمی‌دهد، بنابراین، نیاز به تکرار دورهای دیگر دلفی ضرورت ندارد.

با عنایت به نتایج بدست امده از دلفی سه مرحله‌ای، مدل مفهومی تحقیق به شرح زیر تدوین می‌شود:

اولویت‌بندی ابعاد آسیب‌های بازدارندگی سامانه سایبری در صنایع داروسازی مرتبط با بخش دفاعی چگونه است؟

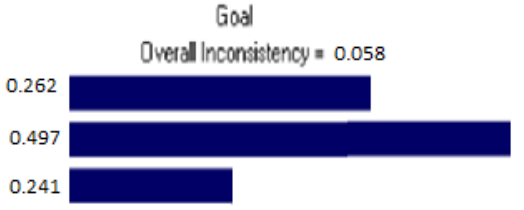
میزان نرخ سازگاری برابر با ۰/۰۵۴ و کمتر از ۱۰٪ است. در تحلیل مقدار بدست آمده CR می‌توان گفت که مقایسات زوجی گروه در جدول (۴) از سازگاری برخوردار بوده و میزان نرخ

سازگاری برابر با ۰/۰۵۸ و کمتر از ۱۰٪ است. در تحلیل مقدار بدست آمده CR می‌توان گفت که مقایسه‌های زوجی گروه در جدول (۴) از سازگاری برخوردار است.

جدول (۴) وزن و اولویت ابعاد آسیب‌های بازدارندگی سامانه سایبری در صنایع داروسازی مرتبط با بخش دفاعی

متغیرها	وزن	اولویت
تهدید به تلافی	۰.۲۶۲	۲
انکار	۰.۴۹۷	۱
گرفتار شدن	۰.۲۴۱	۳

با توجه به جدول (۴)، «رفتاری» حایز رتبه اول، «انکار» حایز رتبه دوم و « گرفتار شدن» رتبه سوم شدند.



نمودار (۱) وزن ابعاد آسیب‌های بازدارندگی سامانه سایبری در صنایع داروسازی مرتبط با بخش دفاعی

بحث و نتیجه‌گیری

پژوهش حاضر با هدف شناسایی آسیب‌های بازدارندگی سامانه سایبری در صنایع دارویی مرتبط با بخش دفاعی انجام شده و در راستای دست‌یابی به اهداف، بر اساس ادبیات تحقیق و مصاحبه با خبرگان و تجزیه و تحلیل داده‌ها نتایج زیر حاصل شد.

سؤال اصلی تحقیق: آسیب های بازدارندگی سامانه سایبری کدام عوامل هستند؟

عوامل بازدارندگی‌های سایبری در سه بُعد تهدید به تلافی، انکار و گرفتار شدن مورد بررسی و مطالعه قرار گرفت و نیز در سه گام تحقیق عوامل مؤثر بر هر بعد نیز مشخص و تعیین شد. گام نخست، نتایج تحلیل عاملی تأیید نشان داد مهمترین آسیب‌های بازدارندگی سامانه سایبری در بُعد «تهدید به تلافی» شامل پنج مؤلفه امنیت فیزیکی اطلاعات، امنیت اطلاعات، طراحی و پیاده سازی چارچوب بومی معماری، عوامل فنی و عوامل اقتصادی هستند. نتیجه بدست آمده با مطالعات فرزام نیا و همکاران (۱۳۹۹)، محمدی برزگر (۱۳۹۹) و فرهنگ

(۱۳۹۸)، سلمان (۲۰۲۲) و لیلی (۲۰۲۱) همسویی دارد. در تبیین این نتایج می‌توان ادعا نمود که به دلیل نبود قطعیت امکان شناسایی حمله‌کننده، در جهت افزایش کارایی تهدید به تلافی کارایی باید گام‌های مختلفی را برداشت. گام‌هایی همانند اقدام‌های دیپلماتیک، اقتصادی، سایبری، قدرت فیزیکی می‌تواند مفید واقع شود. در کنار عوامل اقتصادی و تهیه ملزومات مورد نیاز، رعایت استانداردهای امنیتی، وجود مرکز داده، توپولوژی و آرایش بستر شبکه، نصب دیوار آتش، رمزنگاری اطلاعات محرمانه می‌تواند میزان بازدارندگی سایبری شرکت داروسازی مرتبط با بخش دفاعی را تقویت نماید و همچنین بومی‌سازی استانداردها به کارگیری ابزارها و فناوری‌های امنیتی بومی نیز باید مورد توجه قرار گیرد.

گام دوم، نتایج تحلیل عاملی تأییدی نشان داد مهمترین آسیب‌های بازدارندگی سامانه سایبری در بُعد «انکار» شامل پنج مؤلفه امنیت نیروی انسانی، فرهنگ سازمانی تعالی‌گرا، نبود آگاهی کاربران و مدیریت راهبردی سرمایه انسانی هستند. نتیجه بدست آمده با مطالعات ریاضی (۱۴۰۲)، گل محمدی و جمشیدی (۱۴۰۰)، جوجویونی و همکاران (۲۰۱۴)، یائو (۲۰۲۰)، پایاپلی و همکاران (۲۰۱۷) همخوانی دارد. در تشریح این نتیجه می تواند ادعا نمود که ممکن نبوده شناسایی می‌تواند مشکلاتی را برای مکانیزم‌های تلافی و هنجار برای بازدارندگی فضای سایبری ایجاد کند. ولی مکانیزم‌های و گرفتارسازی و انکار نیازی به شناسایی ندارند. یک دفاع سایبری قوی می‌بایست شامل چندین مؤلفه باشد. یکی از این مؤلفه‌ها، نگهداری یک نسخه از تمامی اطلاعات موجود در یک مکان امن است تا در صورت وقوع حمله سایبری و از دست رفتن اطلاعات، بتوان از اطلاعات پشتیبان استفاده نمود.

گام سوم، نتایج تحلیل عاملی تأیید نشان داد، مهمترین آسیب‌های بازدارندگی سامانه سایبری در بُعد «گرفتار کردن» شامل شش مؤلفه ریسک‌های: محیطی، فنی، فیزیکی، داده، مدیریت ریسک امنیت سایبری و ریسک انسانی هستند. نتیجه بدست آمده با مطالعات رحیم اف و موحدی (۱۳۹۹)، جلالی فرهانی و بیک پور (۱۳۹۹)، جوجویونی و همکاران (۲۰۱۴)، یانگ و همکاران (۲۰۱۰)، محموزاده و رادرجبی (۱۳۹۵) و بورانبائوف و همکاران (۲۰۲۰) همخوانی دارد. در تبیین این نتیجه می‌توان ادعا نمود که میزان آسیب‌های وارد در بخش‌های مختلف یک سازمان را می‌بایست مورد ارزیابی قرار داده تا از این طریق بتوان مدیریت مناسب‌تری بر روی ریسک‌ها داشته باشد. در حقیقت، شرکت داروسازی مرتبط با بخش دفاعی باید بتواند با محاسبه و براورد میزان ریسک در بخشهای مختلف، به توانایی بالقوه‌ای دستیابد تا با مشاهده هر نوع آسیبی به بهترین نحو پاسخ دهد. ضمن این که، با توجه به میزان قدرت شرکت‌های رقیب در بحث بازدارندگی و حمله بر آن، باید توجه به سامانه سخت‌افزاری، آسیب زیرساخت،

عملکرد تجهیزات و اشتراک‌گذاری منابع داشته باشد تا بتواند به خوبی بر روند امور احاطه داشته باشد.

پیشنهاد

پیشنهادهای کاربردی برای بُعد «تهدید به تلافی»

- انجام تمرین دوره‌ای برای کارکنان درگیر در فضای سایبری به‌منظور آشنایی با چگونگی نحوه مقابله با آسیب‌های احتمالی؛
- طراحی و مقاوم سازی تجهیزات سخت‌افزاری به‌کار رفته در شرکت داروسازی مدنظر در مقابل حوادث و بلایایی طبیعی؛
- تدوین و ابلاغ دستورالعمل‌های امنیتی برای کارکنان و به روزرسانی دستورالعمل‌ها و قوانین؛
- توجه به عوامل فنی همانند رعایت استانداردهای امنیتی، وجود مرکز داده، توپولوژی و آرایش بستر شبکه، نصب سامانه شناساگر متجاوز، نصب دیوار آتش و رمزنگاری اطلاعات محرمانه بر روی سامانه‌های مختلف رایانه‌ای شرکت داروسازی مرتبط با بخش دفاعی.

پیشنهادهای کاربردی برای بُعد «انکار»

- برگزاری کارگاه‌های آموزشی در خصوص امنیت فضای سایبری و نقش و اهمیت آن در عملکرد شرکت داروسازی مرتبط با بخش دفاعی، مدیران عالی و میانی سازمانی باید همیشه الگو و سرمشق دیگران باشند و تا از این طریق در جهت فرهنگ‌سازی امنیت فضای سایبری گام بردارند؛
- به‌منظور جمع‌آوری اطلاعات و نظرات ارزشمند ذی‌نفعان و سهام‌داران، جلسات مشورتی مورد توجه قرار گیرد؛
- محاسبه بهره و منافع بازیگران و تحلیل و تعیین وضعیت بر اساس شرایط بازدارندگی و طراحی سازوکارهای جدید.

پیشنهادهای کاربردی برای بُعد «گرفتار کردن»

- ارزیابی میزان ریسک‌های مختلفی که می‌تواند روند کاری فضای سایبری شرکت را تحت‌تأثیر قرار بدهد. ریسک‌هایی همانند آتش‌سوزی، استهلاک سامانه ناشی از گردوغبار، تداخل الکترومغناطیسی، و... اعم از طبیعی و غیرطبیعی و اتخاذ تدابیر لازم در این خصوص؛

- شناسایی بازیگر/ بازیگران تهدیدکننده در مقابل شرکت داروسازی مرتبط با بخش دفاعی؛
- اندازه‌گیری مخاطرات و ریسک‌هایی که شرکت داروسازی مرتبط با بخش دفاعی با آن مواجه است؛
- تدوین اهداف و سیاست‌های بازدارندگی بر اساس قابلیت‌ها و توانمندی‌های انکاری، تنبیهی و وابستگی؛
- رصد علامت‌های ظاهرشده و کشف شده، تهدیدکننده بر اساس تحرکات، رفتار و گفتار در فضای سایبری و حقیقی خود و حریف.

انجام هر نوع تحقیق کاربردی به دلیل وجود متغیرهای خارجی و داخلی اثرگذار، محدودیت‌هایی را برای محقق ایجاد می‌کند که غیرقابل‌کنترل بوده و می‌تواند در نتیجه‌گیری تأثیر قابل ملاحظه‌ای داشته باشد. با توجه به این که، مقوله بازدارندگی سایبری در کشور ازجمله موضوعاتی است که کمتر مورد توجه قرار گرفته است و هنوز به اندازه کافی در مطالعات مختلف و اجرایی پیشرفت نداشته است. ازاین‌رو، دسترسی به اطلاعات و قوانین از چالش‌های اجرایی بوده است.

به‌منظور غنابخشی به مطالعه حاضر، انجام پژوهش در زمینه‌ی موضوعات زیر می‌تواند مورد توجه قرار گیرد:

- طراحی الگوی راهبردی امنیت فضای سایبری در بخش غیرنظامی؛
- طراحی الگوی راهبردی ارزیابی عملیات سایبری در بخش غیرنظامی؛
- بررسی عوامل مؤثر بر فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدها و حملات سایبری.

منابع

- احدی، محمد، و شاه محمدی، محمد. (۱۳۹۷). **طرح راهبردی دفاع سایبری جمهوری اسلامی ایران در حوزه بازدارندگی**. مطالعات بین رشته ای دانش راهبردی، ۸(۳۱)، ۲۲۵-۲۵۲ .
- *دهقانی، علی‌اصغر (۱۳۹۷).* **بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت های حیاتی آمریکا،** *رهیافت‌های سیاسی و بین‌المللی.*
- دهقانی، علی‌اصغر و پوراحمدی میبدی، حسین. (۱۴۰۱). **فضای سایبر و وجه رابطه ای قدرت ملی ایران،** *پژوهش نامه ایرانی سیاست بین الملل، انتشار الکترونیکی.*
- دوستی مطلق، سیدنصیب اله. (۱۴۰۰). **هوشمندسازی در فضای سایبری با استفاده از محاسبات ابری کوانتومی**. فناوری اطلاعات و ارتباطات انتظامی، ۲(۴ (پیاپی ۸))، ۱-۱۱
- *دولت‌آبادی باقری، علی (۱۳۹۲).* **نقش بازدارندگی در راهبرد نظامی ایران،** *مجله سیاست دفاعی، سال بیست و دوم، شماره ۸۵، زمستان ۱۳۹۲، صفحات ۳۷-۸۷.*
- رحیم اف، هانی و موحدی‌صفت، محمدرضا. (۱۳۹۹). **الگوی راهبردیِ ارزیابیِ عملیاتِ سایبری،** *فصلنامه مدیریت نظامی*، ۲۰ (۸۰)، ۶۴-۳۱.
- رمضان زاده، مجتبی؛ غیوری، مجید؛ احمدوند، علی محمد؛ آقایی، محسن؛ نظری فرخی، ابراهیم (۱۳۹۹). **مدل مفهومی ارزیابی قدرت سایبری نیروهای مسح با تاکید بر بعد بازدارندگی سایبری**، مدیریت نظامی، ۲۰ (۲)، ۹۲-۶۱.
- ریاضی، وحید. (۱۴۰۲). **الگوی بازدارندگی راهبردی سازمان‌های نظامی در محیط امنیتی،** *مطالعات بین رشته‌ای دانش راهبردی، ۱۳ (۵۰)، ۲۵۲-۲۲۵.*
- زابلی زاده, اردشیر. (۱۳۹۷). **قدرت بازدارندگی در فضای سایبر**، مطالعات بین‌رشته‌ای در رسانه و فرهنگ، ۸ (۱)، ۸۸-۶۱.
- سیف‌الدین، امیرعلی و امیرحسین رهبر (۱۳۹۲). **تسهیل گری اسلام در جهت تحقق اقتصاد دانش‌بنیان؛ نگرشی جدید به بستر نهادی الگوی اسلامی ایرانی پیشرفت**، فصلنامه سیاست علم و فناوری، سال پنجم، شماره ۴، تابستان .
- صادقی، حسین، عباسی، اسماعیل، و قاسمی، علیرضا. (۱۴۰۰). **مسئولیت مدنی دولت در فضای سایبر با نگاهی به آموزه های اخلاق سایبری (مقاله مروری)**. اخلاق در علوم و فناوری، ۱۶(۱)، ۱-۸ .
- صیاد، محمدکاظم؛ امینی، آرمین و طاهری، ابوالقاسم (۱۳۹۹). **تهدیدات سایبری و اقدامات امنیتی در فضای مجازی، بررسی و رویکردهای ایالات‌متحده آمریکا و جمهوری اسلامی ایران**، *فصلنامه امنیت ملی*، سال دهم، شماره سی هشتم، صص ۳۹۳- ۳۳۰.
- فرزام نیا، نیما؛ عبدی، بهنام؛ رضائیان، علی. (۱۳۹۹). **ارائه الگوی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی**، *فصلنامه مدیریت نظامی، ۲۰ (۷۷)، ۱۲۰-۸۱.*
- فرهنگ، سجاد. (۱۳۹۸). **بازدارندگی سایبری واینترنتی**، راهبردی نوین در کسب اقتدار دفاعی وسیاسی کشور، *ماهنامه جامعه شناسی سیاسی ایران، ۲ (۱)، ۲۵۲-۲۳۲.*

- گل محمدی, ولی و جمشیدی, طاهره. (۱۴۰۱). **بازدارندگی سایبری و تحول در دکترین امنیتی-دفاعی اسرائیل**، *پژوهش های جغرافیای سیاسی، ۵ (۱۲)، ۶۵-۵۴.*
- محمدی برزگر، جعفر. (۱۳۹۹). **موانع و راهکارهای پیشگیری انتظامی از جرایم هرزه نگاری در فضای سایبر**. انتظام اجتماعی، ۱۲(۴)، ۱۴۱-۱۶۸
- Barry Buzan and Ole Waver(2003), **Regional and Power the Structure of International Security**, Cambridge: Cambridge University Press, 2003, p. 43.
- Betz J. David andStevens Tim (2011),**Cyberspace and The State: Toward a Strategy For Cyber - Power**, The International Institute for Strategic Studies (IISS)
- *Hausken, Kjell, & Zhuang, Jun. (2012). **The timing and deterrence of terrorist attacks due to exogenous dynamics**. Journal of the Operational Research Society, 63(6), 726-735.*
- Jeyanthi N., Shabeeb H., M. Saleem A. Durai, Thandeeswaran R., **Reputation Based Service for Cloud User Environment**, International Journal of Engineering, Transactions B: Applications, Vol. 27, No. 8, (2014), 1179-1184,
- Lilli, E. (2021**). Redefining deterrence in cyberspace**: Private sector contribution to national strategies of cyber deterrence, Contemporary Security Policy, 42 (2), 65-50.
- Maimon, D. (2020). **Deterrence in Cyberspace: An Interdisciplinary Review of the Empirical Literature**. In: Holt, T., Bossler, A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_24
- Morgan, Patrick M. (2010). **Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm**. Paper presented at the Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy.
- Ned Lebow, Richard(2007), **Coercion Cooperation, and Ethics in International Relations**, Routledge, Newyork.
- Payappalli, Vineet M, Zhuang, Jun, & Jose, Victor Richmond R. (2017). **Deterrence and Risk Preferences in Sequential Attacker–Defender Games with Continuous Efforts**. Risk Analysis.
- Salman, A. (2022). **A reflection of the challenges facing cyber deterrence and ways to advance them**, Iklīl for Humanities Studies, 3 (4), 577-593.
- Taipale, KA. (2010). **Cyber-deterrence. Law, Policy and Technology**: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization, IGI Global
- Xue, Botong, **The critical role of ethical leadership in employees' information security behaviors: A two-study approach**"(2022). Theses and Dissertations. 5496.

- Yau, H. (2020). **Evolving Toward a Balanced Cyber Strategy in East Asia**: Cyber Deterrence or Cooperation?, Issues & Studies , 56 (3), 75-60.