فصلنامه علمی امنیت ملی
سال پانزدهم، شماره پنجاه و پنجم، بهار ۱٤۰٤
مقاله هفتم از صفحات ۲۲۰-۱۸۱

مقاله پژوهشی: تأثیر فناوری‌های نوظهور فضای سایبر بر امنیت ملی

عبدالرّضا تَرقّی [۱]، ابوالحسن فیروزآبادی[۲]، علی‌اصغر بهنام‌نیا[۳] و محمدرضا کریمی‌قهرودی[٤]

تاریخ دریافت: ۱٤۰۲/۱۲/۱۹ تاریخ پذیرش: ۱٤۰۳/۰٤/۱۲

چکیده

تحولات سریع و عمیق فناوری‌های فضای سایبر که در ابعاد مختلف اجتماعی، فرهنگی، اقتصادی، سیاسی، فناورانه، امنیتی و نظامی- دفاعی تأثیرات راهبردی بر حاکمیّت دارد، نیازمند نگاهی جامع، ساختاریافته و منسجم به‌منظور صیانت از منافع ملّی با هدف آگاهی بر روند تحوّلات است تا امکان تصمیم‌گیری و برنامه-ریزی به‌هنگام آن‌را برای مدیران کشور فراهم سازد. بنابراین اهمیّت و ضرورت شناسایی نوع و میزان تأثیرات همه‌جانبه فناوری‌های نوظهور فضای سایبری در سطح امنیّت ملی با هدف استفاده از فرصت‌های پیش‌رو و مقابله به‌هنگام با تهدیدات آن در قالب تحقیق علمی ضروری است. در این پژوهش به استخراج مشخّصات اختصاصی و انتزاعی فناوری‌های نوظهور فضای سایبری به عنوان ماهیّتی یک‌پارچه، با هدف شناسایی یکتای آن به‌مثابه موجودیّتی واحد، اقدام شده تا در گام بعد با بررسی تأثیرات هریک از این خصیصه‌ها بر ابعاد امنیت ملی، نتیجه مورد انتظار محقّق شود. تحقیق به روش آمیخته انجام شده و اطلاعات مورد نیاز با استفاده از روش اسنادی و کتابخانه‌ای، با ابزار پرسش‌نامه محقّق ساخته گردآوری و با استفاده از روش‌های توصیفی و استنباطی با کمک نرم‌افزار spss23 تجزیه و تحلیل شده است. در نتیجه تجزیه و جمع‌بندی روابط بین متغیرها براساس نتایج ارائه شده می‌توان گفت: در رتبه اول مؤلفهٔ «هوشمندی مبتنی بر داده» بیشترین رابطه مستقیم و مثبت را با امنیت ملی دارد. در رتبه دوم «پیچیدگی و تغییر فضا» و رتبه سوم «همگرایی و غوطه‌وری» قرار دارد. در نهایت نشان‌داده شد که همه ابعاد امنیتی ملی از تأثیرپذیری مستقیم و معناداری برخوردارند که بُعد «سیاسی‌امنیّتی» بیشترین اثرپذیری را دارد.

کلیدواژه‌ها: فضای سایبری، فناوری‌های نوظهور، امنیت ملّی، خصیصه‌های فناوری، همگرایی فناوری.

[۱] دانشجوی مقطع دکتری دانشگاه عالی دفاع ملی، (نویسنده مسئول)، رایانامه: taraghi@borhanid.com
[۲] مدرس دانشگاه عالی دفاع ملی، رایانامه: Alhasanfirouzabadi@gmail.com
[۳] عضو هیئت علمی مرکز پژوهش‌های اسلامی مجلس شورای اسلامی، رایانامه: behnam@irancapacities.ir
[٤] عضو هیئت علمی دانشگاه صنعتی مالک اشتر، رایانامه: m.karimi@sndu.ac.ir

مقدمه و بیان مسئله

تأثیر فضای سایبر بر تمام شئون زندگی باتوجّه به ظهور پیچیدگی‌ها و شرایط آشوب-ناک عصر امروز به‌دلیل سرعت تغییرات شرایط محیطی برآمده از عوامل اثرگذار راهبردی با ریزدانگی، عمق و تنوع بالا، لزوم آگاهی تصمیم‌گیران کلان حاکمیت کشور را از تأثیر روندهای فناوری‌های نوظهور می‌طلبد. باعنایت به درهم‌آمیختگی هرچه بیشتر عوامل موثر در فضای سایبری و تنوّع اثرات راهبردی آنها، افزایش آگاهی و توانمندی تصمیم‌گیران در شناخت محیط از موارد ایجابی مدیریت صحنه است و بدون آن وقوع غافلگیری راهبردی، قطعی خواهد بود. حفظ آمادگی و ایجاد بازدارنگی در برابر تهدیدهای نوین و بهره‌برداری از فرصت‌ها و قابلیت‌های نوظهور از منظر امنیّت موَسَّع در راستای پیشبرد اهداف والای نظام اسلامی در سطح جهان، از اهمیت بالایی برخوردار است. فناوری‌های سایبری به‌مثابه یکی از متغیرهای قوام‌بخش پدیده امنیت در ایجاد اقتدار درون‌زا و انسجام ملی در عصر دیجیتال نقش می‌آفرینند. از فناوری‌های نوظهور[۱] باعنایت به سرعت رشد و قدرت تاثیر آنها در ایجاد تحوّل شرایط محیطی، به فناوری‌های (با رشد) نمایی[۲] برهم زننده[۳] قوی‌سیاه[۴] مرزشکن و توانمندساز[۵] یاد می‌شود، علی‌رغم این‌که از نظر معنایی و سطح بلوغ تفاوت-هایی در تعاریف آن‌ها در مستندات علمی وجود دارد. به‌طور ذاتی، فناوری عامل اصلیِ ظهور و رشد تحوّلیِ فضای‌سایبری و در حقیقت این گسترشِ فناوری‌های سایبری است که منجر به تاثیرات با عمق راهبردی در سطح ملی و فراملّی در ابعاد مختلف زندگی بشر می‌شود که روزبه‌روز به گستره، تنوع ابعاد و پیچیدگی آن افزوده می‌گردد.

---

[۱] Emerging Technologies

[۲] Exponential Technologies

[۳] Disruptive Technologies

[۴] BlackSwan

[۵] Enabling Technologies, cutting-edge technologies

در پی این رشد و توسعه سریع، عمیق و پیچیدهٔ فضای سایبری، بخش قابل توجهی از سرمایه‌های افراد، سازمان‌ها و کشورها، با اهداف اکتسابات مادّی و معنوی شهروندان مصرف می‌شود. این درهم‌آمیختگی وجوه مختلف زندگی با فضای سایبری سبب می‌شود هرگونه بی ثباتی، ناامنی یا چالش در این حوزه، مستقیماً بر زندگی آحاد مردم، امنیت عمومی و اجتماعی و در نهایت امنیّت ملّی تأثیر گذارد. در ادامه به مصادیق برخی از این تأثیر در جنبه‌های مختلف اشاره می‌شود. از جنبه سیاسی در بهره‌برداری از فناوری‌های توانمندساز، می‌توان به راهبرد «قدرت وادارسازی»[۱] (بیلینگسلی، ۲۰۲۳؛ گُمپِرت و بینِندیجک، ۲۰۱٦)[۲] آمریکا، در برابر ایران با استفاده از فناوری‌های سایبری بعنوان ابزار قدرتمند چانه‌زنی سیاسی در تنظیم روابط بین‌الملل و عرصه دیپلماسی سایبری اشاره نمود که از جلوه‌های قدرت سایبری محسوب می‌شود. موضوع قدرت سایبری به دلیل عمق نفوذ و ماهیّت فراگیری ذاتی فضای سایبر در تمامی حوزه‌های راهبردی کشور، دارای تمامی ویژگی‌های قدرت ملی است و به عنوان ابزاری مهم برای تقویت امنیت ملّی در جهت محافظت از منافع و ارزش‌های ملی تلقّی می‌شود (هلیلی و همکاران، ۱۳۹۷). قدرت سایبری با سایر اشکال قدرت ملّی در قالب یک زیست‌بوم هماهنگ در تعامل دائمی و یکی از عوامل مهم تغییر در هندسه نظم نوین جهانی مطرح می‌باشد. از جنبه حقوقی به دلیل ظهور مفاهیم نوین همچون قراردادهای هوشمند و نقش‌آفرینی عوامل خودمختار غیرانسانی در حوزه‌های اقتصادی، اجتماعی، امنیتی و دفاعی، متأسفانه آسیب‌های ناشی از تأخُّر ادراکی و عقب‌ماندگی در اقدامات پیش‌دستانه حوزه سیاست‌گذاری و تقنینی در سطح ملّی و سازمان‌های بین‌المللی امروزی کاملا مشهود است. از منظر فرهنگی‌اجتماعی، در غیاب سواد رسانه‌ای دیجیتال عوام و خواص، در تقابل با جنگ شناختیِ دشمن به‌خصوص با بهره‌گیری از عوامل نرم‌افزاری خودمختار مبتنی بر روش‌های یادگیری عمیق ماشین در شبکه‌های اجتماعی، متأسفانه با تأثیرپذیری مخاطب به‌لحاظ تغییر زاویه دید،

---

[۱] Cyber Coercion

[۲] Billingsley, Gompert, Binnendijk

نگرش، جهان‌بینی و شیوه برداشت مواجه هستیم به‌گونه‌ای که شکل‌دهی به خصیصه‌های هویتی و ادراک کاربر (ذائقه‌سازی) و انحراف او به‌سمت مطلوبِ از قبل تعیین شده را هدف قرار داده‌اند. درحالی‌که امروزه فرصت اقدام کنش‌گرانه هماهنگ در بهره‌برداری از این ظرفیت در تولید و انتشار وسیع محتوای فاخر متناسب با ارزش‌های انقلابی وجود دارد. از جنبه دفاعی توسعه نسل چهارم و حتی پنجم تسلیحات نظامی مبتنی بر فناوری‌های نوظهور سایبری، نوع آفند و پدافند نظامی را دچار دگردیسی نموده و با ظهور جنگ‌های هیبریدی و تهاجم و دفاع هوشمند در فضای سایبری، موضوع رصد، پایش و دفاع را دچار تحوّل نموده و ماهیّت فرماندهی و کنترل را از منظر دستگاه مختصات سنجش و اقدام خودمختار با شیفت پارادایم معنایی مواجه نموده است. از منظر اقتصادی، توسعه اقتصاد دیجیتال، اقتصاد گیگ، تجارت فری‌لنسرها، بانکداری نوین، پول دیجیتال و رمزارزها بستر ظهور فرصت‌ها و تهدیدات فراوان و بی‌سابقه‌ای را منجر شده است. حوزه صنعت با استفاده از قابلیت خودکارسازی داده‌محور و محیط‌های هوشمند با توان تحلیل، تصمیم و اقدام در لبه آشوب، دچار تحوّل پرشتابی شده که درعین‌حال تهدیدات نفوذ و آسیب به سرمایه دادگان ملی و به‌ویژه نقض حریم‌خصوصی ناشی از گستردگی سطح تماس را (به دلیل گسترش تنوع و فراگیری حس‌گرهای جمع‌آوری هرگونه داده در حجم عظیم در هر زمان و مکان) میسّر نموده است. از نگاه دغدغه‌های محیط زیست، مصرف روزافزون منابع انرژی و تبعات آن در تولید گازهای گلخانه‌ای به دلیل فراگیری روند تصاعدی اتصال دائم همه افراد با تلفن‌های همراه، انواع پوشیدنی‌ها و توسعه نسل پنجم ارتباط بی‌سیم[1] در اینترنت اشیاء، دنیا را با چالش مواد معدنی کمیاب و نیز دفع گسترده زباله‌های خطرناک در زمین و جوّ مواجه نموده که نیازمند اعمال مدیریّت بهینه در بهره‌برداری از منابع محدود جهانی است. از منظر امنیّت ملّی، فناوری‌های نوظهور سایبری می‌توانند در عصر دگردیسی دیجیتال زمینه را برای ورود موثر بازیگران جدیدی چون شرکت‌های غول چندملیّتی،

[1] 5G

گروه‌های سازمان‌یافته و حتّی افراد[1] مهیّا سازند به‌گونه‌ای که با قابلیّت تاثیرگذاری عمیق در معادلات قدرت جهانی، شرایط و قواعد زمین بازی را تغییر داده و ابعاد مفهوم سنّتی امنیّت، دولت‌محوری در استقرار امنیت و وابستگی‌های بُعد جغرافیایی تهدید را با توسعه گستردگی آسیب‌پذیری‌ها، شیوه مقابله با تهدیدها، تعدّد و ریزدانگی بازیگران، کارگزاران تهدید و ابزار و اهداف تهدید دچار تحوّل نمایند. در این عصر روش‌های جاسوسی، فریب، نفوذ اطلاعاتی و ترور با الگوهای نوین سایبری جایگزین شده و درصورت غفلت از عوارض فراگیر و نوپدید آن، تاثیرات راهبردی بر امنیّت ملّی کشور خواهد گذاشت. در مقابل، درصورت طراحی هماهنگ ملی و اقدام به‌هنگام، فرصت بهره‌برداری از این ظرفیت نوپدید در راستای تقویت استحکام ساخت درونی قدرت ملی با ایجاد هم‌افزایی ارکان نظام حکمرانی کاملاً متصوّر خواهد بود.

اهمیّت و ضرورت

در بیان **اهمیّت** موضوع می‌توان به جایگاه هستان‌شناسی مستمر و رصد دائم تحولات سریع و عمده فضای سایبر به دلیل تاثیرگذاری فراگیر آن در تقابل با غافلگیری راهبردی اشاره نمود که مبتنی بر آن بتوان روابط سازمانی بین ذی‌نقشان و ذی‌نفعان حوزه حاکمیت سایبری کشور را اصلاح کرد تا امکان هم‌افزایی ملّی در ایجاد افزایش کارایی و مصرف بهینه منابع را با نگاه فرصت‌محور محقّق ساخت. با حصول شناخت، امکان اقدام پیش-دستانه در برابر اهداف دشمن در محیط و مختصات جدید امنیتی با تبدیل نمودن تهدید به فرصت ناشی از تحولات فضای سایبری میسّر خواهد شد. بدون شک بیان اهمیّت راهبردی تأثیرات فناوری‌های نوظهور، توجّه حوزه تقنینی کشور را به تدوین قوانین، پروتکل‌ها و تنظیم مقررات که به‌طور ذاتی از فرآیندی بطئی برخوردار است جلب نموده تا در پرتو آن مدیریّت فضا، ارائه خدمات بهتر، رونق تولید، اشتغال پایدار در راستای تحقّق اقتصاد مقاومتی و سایر منویات مقام معظم رهبری (مدظله‌العالی) میسّر باشد.

---

[1] Individuals

در بیان **ضرورت** این تحقیق می‌توان به ایجاد بی‌ثباتی و تشتّت در اتّخاذ تصمیمات و اقدام در سطح ملی به علت ابهام، پیچیدگی و عدم قطعیّت در درک تأثیرات کلان روندهای فناوری‌های نوظهور در ابعاد مختلف حکمرانی (بر/در/با) فضای سایبر اشاره نمود که پیامد آن بروز غافلگیری در برابر تهدیدات نوظهور دشمن در ابعاد مختلف امنیّت ملّی از منظر نگاه جامع‌الاطراف به موضوع امنیّت (منطبق بر نظریه کپنهاگ) می‌باشد. فقدان هم‌گرائی و هم‌افزائی در حوزه ادراک و اقدام و بروز تشتّت مدیریّتی در بین مدیران ارشد کشور، منجربه هدر رفت منابع به دلیل بی‌ثباتی اقدامات و مواجهه عجولانه در مدیریت پدیده‌های متنوع و نوظهور سایبری در سطح ملی و از دست دادن فرصت اقدام پیش‌دستانه خواهدشد. به عنوان نمونه هتک حریم خصوصی، جعل عمیق[۱] نشر اکاذیب در فضای سایبری، سرقت هویت دیجیتال اشخاص، نفوذ و دسترسی غیرمجاز به منابع دیجیتال ملی از جمله مصادیق نوین آسیب‌هایی است که باید با رفتار پیش‌کنشگرانه در حوزه جرم-انگاری و بروزرسانی به‌هنگام قوانین ملی و مشارکت فعّال در مجامع تقنینی و ائتلاف‌های بین‌المللی در برابر آن اقدام نمود.

بنابراین سئوال اصلی این تحقیق بدین‌صورت خواهد بود که «فناوری‌های نوظهور فضای سایبر چه تأثیری بر امنیت ملی دارند؟» در این تحقیق سعی شده که با بررسی عمیق فناوری‌های نوظهور فضای سایبر به عنوان متغیر مستقل، در ابتدا خصیصه‌های ذاتی فناوری‌ها احصاء شود. سپس با رویکردی انتزاعی‌تر، عمق و دوام نگاه بیشتر، براساس این مشخصات اختصاصی به‌دست آمده به‌منظور ایجاد هویّتی یکتا برای ماهیّت فناوری‌های نوظهور به‌مثابه موجودیّتی یک‌پارچه با قابلیّت شناسایی یگانه، هدف پژوهش‌گر در شناسایی انواع تأثیر بر ابعاد مختلف امنیت ملی قابل تحقّق باشد. با این رویکرد، مبتنی بر مطالعات کتابخانه‌ای و اخذ نظر خبرگان، می‌توان نسبت به اولویّت‌بندی ابعاد امنیّت ملّی متأثّر از عوامل اثرگذار اقدام نمود. با این توضیح، سئوال‌های فرعی عبارتست از: ۱-

[۱] DeepFake

«خصیصه‌های اختصاصی فناوری نوظهور سایبری کدامند؟»، ۲- «تأثیر هریک از خصیصه-های فناوری‌های نوظهور بر هر بُعد امنیت ملی چگونه‌است؟». بنابراین هدف اصلی شناسایی میزان تأثیرپذیری ابعاد امنیت ملّی از فناوری‌های نوظهور سایبری است که به-همین‌منظور در گام اوّل و به عنوان هدف میانی (فرعی)، خصیصه‌های ذاتی مربوط به کلیّت فناوری‌ها به عنوان مفهومی واحد استخراج شده تا سپس در گام بعدی، در فضایی تجریدی تأثیر این خصیصه‌ها بر هریک از ابعاد امنیت ملی به عنوان متغیر وابسته تحقیق، از منظر امنیت موسّع مورد مداقّه قرار گیرد تا بدین‌ترتیب به دور از به‌روزرسانی‌ها و تغییرات مستمر فناوری، طول عمر اعتبار تحلیل نتایج افزایش یابد. برای این‌منظور با مطالعه کتابخانه‌ای به بررسی توصیف، مشخصات، تأثیرات و پیامدهای هر فناوری مرتبط با چهار ساحت یاد شده در تعریف فضای سایبری منتخب در این پژوهش پرداخته شد و در نهایت مشخصات مشترک و فراگیر آن‌ها مُستخرج و دسته‌بندی گردید.

۱. مبانی نظری

تعریف مفاهیم

فضای سایبری: به‌دلیل تفاوت نگاه و اهداف مورد تاکید حکومت‌ها و سازمان‌های مختلف طی سالیان گذشته، تعاریف مختلفی برای فضای سایبری با رویکردهای متفاوت به امنیت فضای سایبری ارائه شده است و هیچ تعریف رسمی مورد توافق جامعی هنوز وجود ندارد. با یک نگاه کلی به تعاریف فضای سایبری چهار منظر مشترک را می‌توان در تعاریف رایج یافت که مشتمل است بر: «**شبکه**» بعنوان عنصر هسته‌ای فضای سایبری، «**داده یا اطلاعات**» و ذخیره‌سازی، تحلیل، دسترسی، انتقال، تبادل و اشتراک‌گذاری آن، «**تعامل انسان و ماشین**» و «**زمان**». اجمالاً مهمترین ایده برآمده از تعاریف رایج در مستندات، این است که فضای سایبری یک فضای مصنوعی مرتبط به حوزه‌های فیزیکی، اجتماعی و فکری است، ولی در یک قلمرو مستقل از این حوزه‌ها به‌صورت خودتنظیم بقا دارد

(هیونشِنگ و همکاران، ۲۰۱۸ : ۱۸٤٤)[۱] فضای سایبری یک فضای اطلاعاتی می‌باشد به‌صورتی که در آن شبکه گسترده جهانی یک دنیای جذابی از ارتباطات منابع اطلاعاتی را خلق نموده است. این اطلاعات مکان، طبقه‌بندی، اقسام و اشکال متفاوتی دارد (کادمی، کولتوکسوز، ۲۰۲۰ : ۳۳)[۲] کلمه سایبر از کلمه سایبرنتیک مشتق شده است. سایبرنتیک در یونان باستان به هنر حکومت شهری، علم حاکمیت مدنی جامعه و هنر چگونگی حکومت کردن بر یک ملت ارجاع شده و معنای آن عبارتست از «علم کنترل و پردازش داده در حوزه حیوانات، ماشین‌ها و جامعه» که البته جامعیّتِ چتر پوشش آن بر اجتماعِ نتایج تمام علوم مرتبطه احاطه دارد (نوویکوف، ۲۰۱٦ : ۲)[۳] با همگراشدن دنیای تجهیز شده به سایبر، مفهوم فضای سایبری امروز باید فراتر از فضای فیزیکی، فضای اجتماعی و فضای تفکر[٤](CPST) رفته و «فضای اطلاعاتی» را در برگیرد چرا که فضای «اطلاعات» مکمل سایر فضاهای سایبری شده و به‌منزله انرژی برای موجودیت‌ها و حیات برای جانمایی و پویایی[٥]فضای سایبری است. فضای سایبری به عنوان یک «جهان موازی» از درهم نفوذ کردن فضاهای فیزیکی، اجتماعی، اطلاعاتی و فکری است. فضای سایبری شامل هر اطلاعات و شیئی است که در زمان و فضای جهان دیجیتال وجود دارد و دیدگاه‌های نظری پس‌زمینه مکانی–زمانی فضاهای سایبری‌شده[٦]چندگانه، از جمله فضای اطلاعاتی، در آن حیات دارند (کادمی، کولتوکسوز، ۲۰۲۱).

وزارت دفاع آمریکا، تعریف مرسوم و سنتی فضای سایبری را به عنوان یک دامنه جهانی و بخشی از «محیط اطلاعاتی»[۷] معرفی می‌کند. «فضای سایبری یک دامنه جهانی، بخشی از محیط اطلاعات، متشکل از شبکه‌های وابسته به‌هم زیرساخت‌های فناوری

---

[۱] Huansheng
[2] Kademi, Koltuksuz
[۳] Novikov
[٤] Cyber-physical-social-thinking (CPST) hyperspace
[5] Dynamic and topology
[6] CeXS: Cyber-enabled (physical, social, information & thinking) spaces
[۷] Information Environment, IE

اطلاعات و داده‌های مقیم آن از جمله اینترنت، شبکه‌های مخابراتی، سیستم‌های کامپیوتری، پردازنده‌ها و کنترل‌کننده‌های تعبیه‌شده است. فضای سایبری، درحالی‌که یک حوزه جهانی درون محیط اطلاعات است، یکی از پنج حوزه وابسته به هم، شامل سایر حوزه‌های فیزیکی: هوا، زمین، دریایی و فضا محسوب می‌شود». محیط اطلاعات هم مجموعه‌ای از سامانه‌ها، افراد و سازمان‌ها است که اطلاعات را جمع‌آوری، پردازش، منتشر یا روی آن اقدامی انجام می‌دهند. محیط اطلاعات به ابعاد فیزیکی، شناختی و اطلاعاتی تقسیم می‌شود (JP, 2013:6, 15). همان‌طور که یاد شد، ادغام فضاهای متفاوت **فیزیکی، اجتماعی** و **فکری** با فضای سایبری سنتی (بعنوان یک فضای اطلاعاتی صرف) منجر به شکل‌گیری مفهوم جدید فضای سایبری شده که از آن به «فضای سایبری تعمیم‌یافته» یا عمومی یاد می‌شود. فضای سایبری تعمیم‌یافته به‌طور اساسی از فضای سایبری مبتنی بر ارتباطات همه-جایی و فراگیر بین اشیاء و هم‌گرایی عمیق فضاهای (چهارگانه) یادشده ظهور یافته است (هیونشِنگ و همکاران، ۲۰۱۸ : ۱۸٤۳). در این پژوهش بررسی فناوری‌های نوظهور سایبری مورد نظر شامل فناوری‌های هریک از این حوزه‌های چهارگانه می‌شود. همان‌طور که در شکل ۱ ملاحظه می‌شود این اَبَر فضای سایبر[1] با فراگیری اتصال و همگرایی فضاهای مختلف، حتی ابعاد فلسفه، علم و فناوری سایبر را هم متأثّر نموده است (هیونشِنگ، ۲۰۲۲ : ۳-۵). بنابراین تعریف عملیاتی فضای سایبری مطلوب عبارت است از «فضایی که از درهم نفوذ کردن و اندماجِ[2] فضاهای اطلاعاتی، فیزیکی، اجتماعی و فکری با رویکرد بیشترین شمولیّت مبتنی بر ارتباطات همه‌جایی و فراگیر، بین موجودیت‌های اثرگذار آن حاصل شده و با تأثیرگذاری متقابل عوامل انسانی و غیرانسانی بصورت فضایی واحد، پیچیده و وابسته به زمان ظهور یافته است. هر عنصری که در این فضا بتواند اطلاعات و دادگان را به‌صورت برخط یا برون خط جمع‌آوری، ذخیره، پردازش و تبادل نماید جزو این فضا بوده و قابلیّت اثرگذاری خواهد داشت». با این تعبیر، در این تحقیق

[1] Hyperspace

[2] به معنای الحاق و یکی‌شدن، تعبیر مقام معظم رهبری (مدظله‌العالی) در سال ۱۳٦۹ از فراگیری کامپیوتر در آینده به نقل از آقای دکتر محمدرضا ولوی مشاور وزیر دفاع وقت

طیف گسترده‌ای از فناوری‌ها[۱] مرتبط با هرکدام از حوزه‌های چهارگانه فضای سایبری از منظر «توصیف ماهیّت، خصیصه‌های اختصاصی، پیامدها و تأثیرات» به لحاظ نگاه فرصت و تهدید برای هرکدام از فناوری‌ها در سطح ملّی مورد بررسی قرار گرفتند.

شکل ۱: مدل منتخب مُحقَّق از «فضای سایبری تعمیم یافته» در این پژوهش، فضای حاصل اندماج چهار فضای اطلاعات، فیزیکی، اجتماعی و فکری، که برگرفته از مدل (کادمی و کولتوکسوز، ۲۰۲۱) و نیز (هیونشِنگ و همکاران، ۲۰۱۸) و مدل دانشگاه آریزونا توسط (برین[۲]و همکاران، ۲۰۲۰) می‌باشد که همگی آنها به تلفیق همه حوزه‌های یادشده در فضای سایبری (تعمیم یافته) قائل هستند.

امنیّت ملّی: موضوع «حفظ خود» یا «صیانت ذات و نفس» که در پنج مقوله خلاصه می‌شود: «حفظ جان مردم»، «حفظ دین، باور و ارزش‌های مردم»، «حفظ تمامیت ارضی»، «حفظ نظام اقتصادی و سیاسی» و «حفظ استقلال و حاکمیت کشور»، که به‌لحاظ ماهیتی این پنج مقوله، جوهره امنیت ملی است. اصولاً «فلسفه وجودی دولت» برای پاسداری امنیت می‌باشد، اما نباید انتظار داشت تمامی دولت‌ها مسائل خاص و مشابهی را منافع عادی یا حیاتی خود در چهار چوب امنیت ملی تلقی کنند. منابع و منافع امنیت ملی در کشورها و زمان‌های مختلف ماهیّتی نسبی و ناپایداری دارند. به عنوان نمونه، تعریف منافع ملی برای دولت لبنان و تأمین امنیت ملی براساس یکپارچگی و وحدت ملی و حفظ تمامیّت ارضی، ولی برای ژاپن توسعه و بسط بازار و سلطه اقتصادی بر جهان در زمرهٔ منافع اساسی محسوب می‌شود. این جابجایی در اولویّت‌های امنیّت، تغییر ارزش‌ها و یا

[۱] AR/VR, IOT, 5G, BigData, BlockChain, Quantum, NANO, BIO, 3D Print, Robotics, CPS, UAV, D.Twins, AI, BCI, Metaverse, Wearables …
[۲] Brain

قربانی کردن آن در پای ارزش‌های دیگر، گاهی به اجبار و برای ممانعت از وارد آمدن لطمات بیشتر بر پیکره امنیت ملی صورت می‌گیرد. گاه به اختیار و با هدف تطبیق هرچه بیشتر با شرایط متحول داخلی و خارجی به‌منظور سهولت دستیابی به روش‌های مؤثر در تثبیت و تقویت امنیت ملی هرکشور رخ می‌دهند (هندیانی، ۱۳۸٦: ۱٤). بنابراین قلمرو و حریم امنیتی به‌دلیل گستردگی عرصه آن همواره نامشخص می‌باشد (باهوش فاردقی، ۱۳۹٦ : ۱۰٦). به‌دلیل ماهیّت پیچیده امنیت ملّی به‌خصوص با تاثیرات متقابل فضای سایبری و فناوری‌های نوظهور دیجیتال، از منظر نظریه آشوب مبتنی بر تفکر انتقادی و یادگیری (تفکر خارج از چارچوب)، بینش جدیدی در درک چالش‌های امنیت ملی به عنوان یک پدیده پویای قطعی و برهم‌زننده وضعیت ایجاد شده است. در دنیای معاصر که علم و فناوری نقش مهمی در مدل‌سازی راه‌حل‌های پیچیده برای طیفی از چالش‌های امنیتی دنیای واقعی دارد، پویایی آشوبی در مدل‌سازی نظریه‌ای و زندگی واقعی، راه‌حل‌های پایدار برای چالش‌های نوظهور در جمعیت‌شناسی، سیاست، مهندسی و فن‌آوری و ارتقای ظرفیت فن-آوری‌های نظامی ارائه می‌دهد. نظریه آشوب می‌تواند تفکّر انتقادی و یادگیری را از منظر تعامل آشوب با سیاست، جمعیت‌شناسی، جامعه‌شناسی، اقتصاد و فرایندهای تصمیم‌گیری نظامی و سایر پدیده‌های پیچیده اجتماعی در مبارزه با تروریسم، بی‌ثباتی سیاسی، ناامنی اطلاعاتی، امنیت سایبری و امنیت بیومتریک تسهیل کند که پیامد آن توسعه امنیت ملی خواهد بود (اوگِچوکو و همکاران، ۲۰۲۰ :۱)[1] توجه به امنیت، توجه به عناصر قدرت را می‌طلبد، یعنی اگر به‌جای مؤلفه‌های امنیت، مؤلفه‌های قدرت شماریم مرتکب خطا نشده-ایم. مؤلفه‌های قدرت دو دسته‌اند. مؤلفه‌های نرم‌افزای مانند رهبری، روحیه و تعامل خارجی (دیپلماسی) و مؤلفه‌های چون تجهیزات نظامی و پول، مؤلفه سخت محسوب می-شوند. ارزیابی منظم مؤلفه‌های قدرت و مقایسه با سایر حکومت‌ها و درک موقعیت خود در مراتب قدرت جهانی، از مراحل حفظ و ثبات امنیت جامعه است چراکه در گذر زمان و در موقعیت‌های مکانی متفاوت مفهومی متغیّر است. مؤلفه‌های امنیت دارای وابستگی شدید

[1] Ogechukwu

به یکدیگر هستند و بنابراین بدون دسته‌بندی از مؤلفه‌های قدرت از آن‌ها ذکر می‌شود (مرادی و همکاران، ۱۳۹۹: ۳۱-۳۲). منابع قدرت عموماً در حال تغییرند. با گذر زمان تغییر در چارچوب الگوی تفکر و انگاره ذهنی[1] منبع قدرت از نیروی نظامی به عواملی چون فن‌آوری، آموزش و اقتصاد همگام با تحول در مکاتب مختلف امنیت ملی محقق شده است. در هر دوره منابع متفاوتی از قدرت نقش بیشتری ایفا کرده‌اند. جوزف نای می‌گوید منابع قدرت هیچگاه حالت ایستا ندارد و در دنیای امروز نیز همچنان تغییر را تجربه می‌کند (کهن سال کلکناری، بابایی، ۱۳۹٦ : ۱۰). باتوجه به تغییر مدام منابع قدرت ملی در طول زمان، می‌توان دید در هر دوره و شرایطی از تاریخ منابع متفاوتی در توانایی و قدرت ملی تاثیرگذار بوده‌اند. در سیر تاریخ قدرت جنگ‌آوری، جمعیت، وسعت سرزمینی، صنعت و شبکه ریلی، علم و فناوری و سلاح هسته‌ای، قدرت اقتصادی مبتنی بر فناوری پیشرفته و هم‌اکنون فضای مجازی در همه زمینه‌های اجتماعی، سیاسی اقتصادی و امنیتی منبع قدرت ملی هستند (پیشگاهی‌فرد و همکاران، ۱۳۹۳ : ۷).

ایده قدرت هوشمند که ترکیبی از قدرت سخت و قدرت نرم در حوزه امنیّت ملّی و منجر به ظهور مفهوم «هوشمندسازی امنیت ملی» در عصر حاضر شده که نتیجه آن استحکام درونی قدرت ملی و تبدیل تهدیدات به فرصت‌ها خواهد شد (بیات، ۱۳۹۸ : ۳۷۷). در عرصه سیاست خارجی، دیپلماسی هوشمند برآمده از خاستگاه و بسترِ این «قدرت هوشمند» است (ایزدی، ۱۳۹۳: ۷). براساس تعالیم مکتب اسلام، برای «تولید، حفظ و بازتولید امنیت ملی»، راهبردهای اجتماعی کردن، مردمی کردن، هوشمندسازی و عدالت-گستری ارائه شده است (پیشین: ۳۷۱). با این رویکرد، کلیه مصادیق فضای سایبری، اعم از شبکه‌های اجتماعی و قابلیت‌های نوظهور فناوری‌های دیجیتال فرصتی بزرگ برای تحقّق استحکام درونی مبانی امنیت ملی جمهوری اسلامی ایران به اتکای مؤلفه‌های قدرت سایبری می‌باشد. تعریف برگزیده امنیت ملّی با رویکرد جامع موردنظر این پژوهش

[1] Shift paradigm

عبارتست از «دستیابی یک ملت به *امکانات* و *توانمندی* و *ابزاری* که بتواند با تمسّک به آنها از تهدیدهای خارجی و داخلی در امان باشد؛ سلطه سیاسی، اقتصادی، فرهنگی و نظامی بیگانه را دفع؛ از ارزش های حیاتی خود در صلح و جنگ، دفاع و حراست نماید؛ از موجودیت کشور و تمامیّت ارضی آن محافظت کند، سیر صعودی در افزایش قدرت و توان ملّی در عرصه های مختلف داشته باشد و در راه پیشبرد امر توسعه متوازن و پویا و تحکیم وحدت ملّی و ارتقای سطح مشارکت سیاسی جامعه موفّق باشد» (همان: ۳٦).

در این پژوهش باتوجه به گسترش معنایی و حوزه تأثیر فضای سایبری تعمیم یافته، بررسی حوزه اثر بر امنیّت ملّی مبتنی بر مکتب امنیتی کپنهاگ می‌باشد. در مکتب کپنهاگ، باری بوزان با رویکرد چندوجهی بودن امنیت، معتقد به در هم تنیدگی طبیعی بخش‌های مختلف (سیاسی، نظامی، اجتماعی، اقتصادی و زیست‌محیطی) است (بخشی تلیابی و همکاران، ۱۳۹٦ : ۱۳٦)، ازاین‌رو مکتب کپنهاگ در مقایسه با سایر مکاتب امنیتی دیدگاه موسع و روشنی به موضوع امنیت دارد (خانی، ۱۳۹۹ : ۹۷)، چرا که مکتب کپنهاگ مفهوم، امنیت را مُوَسَّع کرده و با طرح پنج حوزه نظامی، سیاسی، اقتصادی، فرهنگی/اجتماعی و زیست‌محیطی، در عمل مفهوم تک‌بعدی بودن امنیت را از منظرِ صرف نظامی به کنار زد. بااین‌حال همچنان حوزه نظامی را مهمترین بعد امنیت می‌داند (بیات، ۱۳۹۸ :۱۷۳). با نگاه موسّع مُنبعِث از نظریه‌های متعدّد امنیّتی امروزی، ابعاد امنیت ملی شامل همه حوزه‌های زندگی بشر از منظر حاکمیتی می‌شود[۱](مرادی و همکاران، ۱۳۹۹ : ۳۳).

فناوری: فناوری یک ترکیب هماهنگ و سازگار از سخت‌افزار، نرم‌افزار و مغزافزار است که در بستر یک شبکه زیرساختاری مفهوم و معنای واقعی خود را می‌یابد. فناوری صرفاً یک ابزار یا دانش انجام یک کار یا یک ایده و طرح نیست، بلکه ماهیتی شبیه به جامعه با کل ارتباطات اجتماعی مربوط به آن را دارد و تنها با چنین نگرشی قابل درک و اداره و رهبری

[۱] سیاسی، امنیتی، نظامی/دفاعی، اطلاعاتی، اقتصادی، فرهنگی، اجتماعی، حقوقی(قضایی)، محیط‌زیست، غذایی، روانی/اخلاقی، و فرافضایی

خواهد بود. اجزای اصلی فناوری که در اتباط متقابل و مکمل یکدیگر هستند عبارتند از: سخت‌افزار، نرم‌افزار، مغزافزار و شبکه پشتیبانی (محمودزاده، ۱۳۸۹ : ٦٤).

فناوری نوظهور: طی ۱۰ تا ۱۵ سال آینده منجر به تغییرات بزرگ در جامعه و نهادهای اجتماعی و اقتصاد خواهد شد. فناوری نوظهور ماهیتی به‌طور بنیادی نوین دارد که با رشدی سریع و البته با ابهام و عدم قطعیت در نتایج آن همراه است (روتولو و همکاران، ۲۰۱٦ :۳٤)[۱] فناوری نوظهور، یک فناوری است که پتانسیل بالایی را نشان می‌دهد اما ارزش خود را نشان نداده یا به هیچ نوع توافق جمعی نرسیده (کوزنس[۲]و همکاران، ۲۰۱۰ :۳٦٤) و شکل‌ها، قابلیت‌ها، محدودیت‌ها و کاربردهای دقیق‌شان همچنان مبهم است (استاهل[۳] ۲۰۱۱: ٤-۳). ویژگی‌های عمومی فناوری‌های نوظهور (IT) «عدم قطعیّت، تأثیر شبکه‌ای[٤] هزینه زیاد، نگرانی‌های اجتماعی و اخلاقی، محدودیّت برای کشورهای خاص و فقدان تحقیقات و پژوهش» می‌باشد (هلاویه[٥] ۲۰۱۳: ۱۰۸).

ویژگی‌های اختصاصی فناوری‌های نوظهور سایبری:

برای تحقُّق هدف پژوهش (بررسی تاثیر فناوری‌های نوظهور فضای سایبری بر امنیت ملی) استفاده از خصوصیات اختصاصی و مشترک این فناوری‌ها ملاک عمل است. باتوجّه به اینکه خصیصه‌ها از یک سطح بالاتر انتزاع و تجرید مفهومی نسبت به‌خود فناوری‌های نوظهور که دائماً در حال تغییر و بروزرسانی هستند، برخوردارند امکان بررسی تأثیر را در محیط ذهنی آرام‌تر به‌دلیل وجود تغییرات کمتری در شرایط پیرامونیِ محیط تحلیل مهیا می‌کنند. بنابراین طول عمر و میزان اعتبار نتایج کسب شده، افزایشی و از قابلیت اطمینان بیشتری خواهد داشت.

---

[۱] Rotolo

[۲] Cozzens

[۳] Stahl

[٤] طبق قانون اثر شبکه‌ای، قدرت و ارزش شبکه با افزایش تعداد افرادی که از آن شبکه استفاده می‌کنند یا متصل هستند افزایش می‌یابد (Metcalfe, 1995).

[٥] Halaweh

شکل ۲: دسته‌بندی کلی خصیصه‌های فناوری‌های نوظهور، در ۷ دسته اصلی (نتیجه پژوهش محقق)

برای این منظور در ابتدا با نگاه جزئی‌نگر به مطالعه عمیق مقالات، کتب و منابع علمی مرتبط، به بررسی «توصیف، خصوصیات و پیامدهای فناوری‌های نوظهور» پرداخته شد در ادامه با تدقیق در جزئیات هرفناوری، با نگاه کلی‌نگر[۱] برای استنباط خصیصه‌های اختصاصی فناوری‌های نوظهور، استنتاج لازم صورت گرفت. باتوجّه به مدل منتخب محقّق از فضای سایبری به‌دلیل شمولیّت کامل فضای سایبری تعمیم‌یافته، در جهت شناسایی تاثیر فناوری‌های فضای‌سایبر در تمام حوزه‌های فیزیکی، اطلاعاتی، اجتماعی و شناختی بر امنیّت ملّی، به‌خصوص توجّه به وقوع پدیده همگرایی، هم‌افزایی و اندماج حوزه‌های فناوری در یکدیگر، خصیصه‌های احصاء شده (شکل ۲) برای کلیّت فناوری‌های نوظهور سایبری دارای ماهیّتی اشتراکی هستند بدین معنا که همهٔ این خصیصه‌ها به طور نسبی به هریک از فن‌آوری‌ها تعلّق دارند. با بررسی نتایج به‌دست آمده، با رعایت مشابهت معنایی و کارکردی خصیصه‌ها در هر دسته، خصوصیات اختصاصی و مشترک توصیف کننده ماهیت فناوری‌های نوظهور در هفت دسته کلی (شکل ۲) دسته‌بندی شد.[۲] خصیصه اول

[۱] Holistic / Partial (detailed) point of view, (Zoom in/Zoom out approach)

[۲] برای دستیابی و دسته‌بندی این خصیصه‌ها بیش از ۳۰۰۰ منبع شامل کتاب و مقاله بررسی شد. ابتدا با کمک برداشت حاصل از تحلیل انسانی دسته‌بندی ۳۱گانه برای ۱۱٦٦ خصوصیت محقق شد و سپس با الگوریتم تحلیل هم‌واژگانی، هم‌رخدادی واژه‌ها اقدام به شباهت‌سنجی متون تخصّصی، که در نهایت خوشه‌بندی هفت‌گانه فوق برای ۳۱ دسته حاصل

«همگرایی و غوطه‌وری» به خصوصیات ادغام فناوری‌ها و امتزاج فضاهای فیزیکی و مجازی و توسعه نقش همزادهای دیجیتال (همسان‌های دیجیتال هر موجودیت) در غوطه-وری موجودیت انسانی و غیرانسانی در محیط تعاملی و هوشمند اشاره دارد (داتسنکو، ۲۰۱۷؛ روکو، ۲۰۲۰؛ دوویدی و همکاران، ۲۰۲۲؛ یونگ–وون و همکاران، ۲۰۲۱).[۱] خصیصه دوم «هوشمندی مبتنی بر داده»، به خصوصیت آگاهی وضعیتی شناختی برآمده از تحلیل دادگان می‌پردازد (پریادارشینی و کوتون، ۲۰۲۰؛ آندراد و یوو، ۲۰۱۹؛ تینر و همکاران، ۲۰۱۷).[۲] سومین خصیصه «توزیع‌شدگی و ادراک فراگیر» به خصوصیّت تمرکززدایی و توزیع‌شدگی در تصمیم‌گیری خودمختار اشاره دارد که منبعث از مشخصه-های اتصال و محاسبات همه‌جا حاضر، ادراک فراگیر (در رایانش لبه) و رشد تفکر مصنوعی در عوامل هوشمند چون رُبات‌ها می‌باشد (برِنو و لویز، ۲۰۲۰؛ اسکات، ۲۰۱۸؛ کادل، ۲۰۲۰ و فی و همکاران، ۲۰۲۱).[۳] خصیصه چهارم «اشتراک‌گذاری و مشارکت اجتماعی» به توسعه همکاری مشارکتی و رفتار اجتماعی عوامل هوشمند مبتنی بر اشتراک-گذاری دادگان می‌پردازد که این رویکردِ اشتراکی منجر به تعالی زندگی و افزودگی انسان و اجتماع می‌شود و همزمان تهدیدات بی‌سابقه‌ای را برای بشریّت رقم می‌زند (بوسو و همکاران، ۲۰۲۲؛ شوآب، ۲۰۱۶ و آتلام و همکاران، ۲۰۱۸).[۴] خصیصه پنجم «توسعه مقیاس‌ها» به حذف محدودیّت‌ها، کوچک‌سازی و مقیاس‌پذیری عوامل اثرگذار اشاره دارد که نتیجه آن توسعه ساختار پایین به بالای عوامل تاثیر در حکمرانی و شخصی‌سازیِ خدمات، متناسب با نیاز می‌باشد (چراغی، ۲۰۲۱؛ لی و مون، ۲۰۲۰؛ اشمیت، ۲۰۱۶؛ فِرناندو، ۲۰۱۹ و تریووُر و همکاران، ۲۰۱۸).[۵] خصیصه ششم «پیچیدگی و تغییر فضا» به-

---

شد (بیان جزئیات رساله از حوصله مقاله خارج است)، که از نظر اعتبارسنجی کفایت شایستگی آن، بـا پرسـش‌نامـه بـه تایید خبرگان رسید. اینجا برای هر دسته خصیصه، به عنوان نمونه برخی منابع استنباطی آن ارجاع شده است.

[۱] Dotsenko, Roco, Dwivedi, Yong-Woon

[۲] Priyadarshini, Cotton, Andrade, Yoo, Theiner

[3] Breno, Luiz, Scott, Cadell, Fei

[4] Bussu, Schwab, Atlam

[5] Cheraghi, Lee, Moon, Schmidt, Fernando, Trevor

دلیل رشد فزاینده عدم قطعیّت و ایجاد شیفت پارادایم مفاهیم منبعث از تحوّلات برآمده از وابستگی عمیق به فناوری و پویایی در زمان واقعی حاصل شده است (رِدینگ و همکاران، ۲۰۲۳؛ منتصری و همکاران، ۲۰۲۰؛ اتحادیه اروپا، ۲۰۱۹ و چیسنال، ۲۰۲۰).[1] در نهایت خصیصه هفتم «تهدیدات ذاتی» است که به‌دلیل خصوصیّات عدم پاسخگویی، نبود استاندارد، فزونی نابرابری‌ها، جایگزینی تدریجی انسان، حذف کرامت انسانی، چالش شفافیت، دغدغه‌های مربوط به محیط زیست و تاب‌آوری محیطی و در نهایت تأکید بر ذاتی بودن تهدیدات به‌دلیل گسترش بی‌سابقه سطح تماس و افزودگی‌های ناشی از هوشمندی عناصر خودمختار و رشد تزایدی عوامل خود تصمیم‌گیر متبلور شده است و از طرف دیگر ماهیّت ابهام ذاتی ناشی از پدیدهٔ واگرایی پس از تحقّق ادغام و همگرایی فناوری‌ها[2] علّت تهدیدات تلقّی می‌شود (روکو، ۲۰۲۰؛ رایان، ۲۰۲۰؛ زاچاری، ۲۰۱٦؛ آتیا و فرح، ۲۰۱٤؛ می‌یر و همکاران، ۲۰۱۹ و تی‌جون و خومه، ۲۰۲۲).[3] تعاریف عملیاتی هریک از خصیصه‌های استخراج شده در جدول شماره ۱ آمده است.

جدول ۱: تعریف خصیصه‌های فناوری‌های نوظهور سایبری، مستخرج از نتایج پژوهش در بررسی عمیق منابع علمی

دسته اصلی خصوصیت فناوری	تعریف عملیاتی (استنباط شده از کل مفاهیم دریافت شده از منابع پژوهش)
همگرایی و غوطه‌وری	«ادغام و امتزاج علوم و فناوری‌های نوظهور، سبب عدم قطعیت و ابهام در پیش‌بینی پذیری مربوط به نتایج، محصولات و تأثیرات این همگرایی شده‌است. همگرایی ایجاد شده سبب توسعه معنای غوطه‌وری به دلیل امتزاج کامل و بدون مرز فضاهای فیزیکی و مجازی گردیده که با فراگیری رسانه‌های چندحسانه‌ای و مفهوم «مجازیت حقیقی» (درگیری همه حواس انسان بجای برخی از حواس در حقیقت مجازی)، بصورت «همیشه‌روشن» با کنشگری دائم همزاد دیجیتال هر موجودیت انسانی و غیرانسانی در محیط تعاملی و هوشمند، امکان تحقّق اَبدیّت دیجیتال را رقم می‌زند.»
هوشمندی مبتنی بر داده	توسعه سامانه‌های با درجاتی از استقلال با قابلیت ادراک، یادگیری، انتزاع، استدلال، تصمیم و اقدام خودمختار برای دستیابی به هدفی مشخص است، که به‌دلیل داشتن آگاهی وضعیتی شناختی امکان پیش‌بینی وقایع آینده را هم دارد و همه این افزودگی‌ها ناشی از داده‌وارسازی تمام ابعاد زندگی بشر در ایجاد ارزش‌های جدیدی است که داده را بعنوان سرمایه‌ملی دیجیتال با چالش وحدت مکانی و فرّاربودن از مرزهای ملّی هر کشور مواجه نموده است»
توزیع‌شدگی و	«ماهیت توزیع‌شدگی و عدم کنترل مرکزی به دلیل اتصال دائم بین افراد و اشیاء و محاسبات

[1] Reding, Montasari, EU, Chisnall

[2] طبق نظریه «چرخه تکامل همگرایی–واگرایی» فناوری کـه Convergence–divergence revolution cycle توسط روکو مطرح شد

[3] Ryan, Zachary, Attiah, Farah, Meijer, Tidjon, Khomh

ادراک فراگیر	همه‌جا حاضر فراگیر، دستگاه‌های محاسباتی را قادر می‌سازد تا رفتار خود را با سنجش محدوده فیزیکی (ازجمله افراد، اشیا، حوادث و شرایط) تطبیق دهند، همچنین هوشمندی توزیع‌شده عناصر، توان تأثیر بر محیط را با خودمختاری سایبری مبتنی بر آگاهی وضعیتی ایجاب می‌نماید که در نتیجه مفهوم مغز سایبری با قابلیت تفکر مصنوعی، خصوصیت خودآموز بودن از محیط اطرافِ ادراک شده خود را توسعه می‌دهد»
اشتراک‌گذاری و مشارکت اجتماعی	«رفتار مشارکتی سامانه‌های سایبری‌فیزیکی مبتنی بر آگاهی وضعیتی اجتماعی و هوشمندی توزیع‌شده شبکه‌ای و هوش تجمعی[۱] سبب تحقّق یکپارچه شدن سامانه‌ها و رُبات‌ها بصورت اجتماعی می‌شود و در تعامل با جامعه، مبتنی بر هوش‌مصنوعی آگاه به اجتماع با خصوصیات اجتماعی تلفیق می‌شود. به این هوشمندی ارتقاءیافته «هوش اجتماعی مصنوعی» گفته می‌شود. مشارکت مبتنی بر اشتراک‌گذاری داده در چارچوب توافقات و پروتکل‌های قانونی است. همچنین اشتراک‌گذاری دارایی‌ها در قالب مالکیت و مصرف همکارانه در اقتصاد مشارکتی و چرخشی قابل تحقق است. در مجموع این مشارکت اجتماعی انسان–ماشین و انسان–انسان در محیط هوشمند می‌تواند باعث افزودگی انسان و درصورت یک‌پارچگی اجتماعی منجر به تحقّق افزودگی اجتماعی شود».
توسعه مقیاس‌ها	«برای غلبه بر پیچیدگی و خبرگی فزاینده ناشی از یک‌پارچگی شتابان فناوری‌های نوین، توانایی تطبیق عملکرد و هزینه در پاسخ تغییرات محیطی بعنوان یک نیاز عملیاتی برای رقابت‌پذیری و استقامت هر سازمان امری واجب است. حذف محدودیت‌های فیزیکی ناشی از توسعه فناوری‌های نوظهور، در دسترس‌پذیری، سهولت دسترسی و ارزان شدن کاربری[۲] برای عموم نقش مهمی داشته که نتیجه آن توسعه حکمرانی باز مردمی با ساختار نظارتی پائین به بالا و امکان دریافت خدمات انبوه شخصی‌سازی شده است، گرچه این شخصی‌سازی می‌تواند با تهدیدات زیادی هم در سطح ملّی همراه باشد».
پیچیدگی و تغییر فضا	«با تعدّد عناصر تعامل‌کننده دارای ارتباط شبکه‌ای با هم در محیط هوشمند خودسازمان‌ده، جهان شمول و باز رشد پیچیدگی تو در تو بدون حضور روابط علیّت معیّن امری قطعی است که نتیجه آن ایجاد تحوّل در انگاره‌های ذهنی و قواعد سنّتی زمین بازی خواهدبود، همچنین توسعه رایانش پرقدرت در لبه با وابستگی عمیق به فناوری در سامانه‌های سایبری–فیزیکی–شناختی‌اجتماعی، قابلیت تعامل پویا و خودتصمیم‌گیر در زمان واقعی را گسترش داده و ماهیّت دنیای آتی را دچار دگرگونی بی‌سابقه خواهد کرد».
تهدیدآفرینی	«به‌دلیل عدم قطعیت، ابهام، پیچیدگی و تغییرات سریع و ریشه‌ای حاصل از تحولات فناوری و بُروز ناشناختگی حاصل از آغاز مرحله واگرایی پس از وقوع همگرایی در چرخه تکامل توسعه فناوری، استاندارد مشخصی در موضوعات نوظهور تدوین نشده؛ همچنین چالش‌های مباحث اخلاقی در بسیاری حوزه‌ها بعنوان مانع مطرح است. مسائل حریم خصوصی، مالکیت، حسابرسی، مسئولیت‌پذیری، پاسخگویی، جبران خسارت، نبود شواهد قانونی و جرم‌انگاری قطعی در قضاوت، امکان پرینت 3D سلاح، رشد نابرابری، تبعیض، گسست اجتماعی، توسعه شکاف طبقاتی، ظهور قطبش جدید قدرت‌ها در هندسه نظم نوین جهانی، نقض کرامت انسانی، چالش شفافیت، حقوق‌بشر دیجیتال، چالش دادگان فرامرزی، نبود یا سوگیری قوانین جهانی (در جنگ تقنینی)، افزایش سطح تماس، جابجایی فرهنگی، ابهام در سنجش‌پذیری اقتصاد چرخشی، چالش اطلاعات شویی، جایگزینی انسان (تحول در حس خود بودن)، طرح حقوق ربات‌ها و تاب‌آوری محیطی از مسائل و چالش‌های حل نشده این حوزه‌اند، که استنباط عمومی این وضعیت همان مفهوم توسعه تهدیدآفرینی گسترده است»[۳]

[۱] Swarm

[۲] Availability, Accessibility, Affordability

[۳] Weaponisation of everything in digital age (law as a weapon of war, social media as a

۲. روش تحقیق

باتوجه به بررسی تأثیر فناوری‌های نوظهور فضای سایبری بر امنیت ملی در پژوهش، روش تحقیق ترکیبی(کیفی-کمی)[۱] یا آمیخته مناسب‌ترین روش تشخیص داده شد. یعنی با استفاده از تحلیل کیفی و کمی، که تحلیل کیفی مستند بر آراء و دیدگاه صاحب‌نظران مطلع انجام و در بخش کمّی یافته‌های بخش کیفی با بهره‌گیری از نظرات نخبگان و خبرگان موضوع به واسطه پرسش‌نامه محقّق ساخته اعتباریابی می‌گردد. درنهایت تأثیر فناوری‌های نوظهور فضای سایبر بر امنیت ملی تبیین می‌شود که برای تصمیم‌سازی دولتمردان و مدیران حاکمیت کشور قابلیت بهره‌برداری داشته باشد. جهت انجام این پژوهش پس از بررسی مبانی نظری، مطالعات تطبیقی و دریافت نظر نخبگان حوزه فناوری اطلاعات، خصوصیات ذاتی فناوری‌های نوظهور شناسایی و دسته‌بندی که طی یک پرسش‌نامه نیمه باز توسط نخبگان ارزیابی شد. در مرحله بعد تأثیر خصیصه‌های انتزاعی فناوری بر ابعاد امنیّت ملّی در قالب پرسش‌نامه بسته و از طریق روش کمّی مورد سنجش واقع شد. ابعاد امنیّت ملی مبتنی بر مکتب کُپنهاگ و نگاه مُوسَّع امنیّتی در چهار حوزه نظامی/دفاعی، سیاسی/امنیتی، اقتصادی و فرهنگی/اجتماعی مورد نظر قرار گرفت. مفاد مرتبط با بُعد زیست محیطی به‌دلیل کاهش ابعادی تحلیل و نیز محدودتر بودن محتوا نسبت به سایر موضوعات، در سایر ابعاد یاد شده لحاظ گردید.

جامعه آماری، حجم نمونه و روش نمونه گیری: جامعه آماری، در حوزه کیفی از یک سو شامل اسناد و مدارک مهم و در دسترس و از سوی دیگر «آگاهان اجتماعی» (خبرگان و نخبگان حوزه فضای سایبر) که مورد بررسی، تجزیه و تحلیل قرار می‌گیرد. در بخش کمی نیز جامعه آماری همان آگاهان اجتماعی هستند. آگاهان اجتماعی عبارت‌اند از:

---

weapon, information as a weapon)

[۱] mixed method

– مسئولان، مدیران اجرایی و کارشناسان حوزه فضای سایبری و فناوری‌های نوظهور با حداقل ۱۵ سال سابقه تخصصی.

– نخبگان، صاحب‌نظران و اندیشمندان در حوزه امنیت فضای سایبری در ابعاد اجتماعی، فرهنگی، سیاسی، دفاعی امنیتی، اجرایی و فناورانه با مدارک تحصیلات عالی دانشگاهی تخصّصی در این حوزه.

روش نمونه‌گیری در دو بخش کیفی و کمی و دو نوع انجام شده است. در حوزه اسناد و مدارک با استفاده از روش نمونه‌گیری هدفمند کلیه اسناد و مدارک در دسترس، جمع-آوری و بهره‌برداری شد. در بخش آگاهان اجتماعی و امنیتی فضای سایبر نیز با استفاده از روش نمونه‌گیری گزینشی، نمونه مورد نیاز باتوجه به قاعده اشباع نظری انتخاب و استفاده شده است. براین‌اساس با استفاده از جدول مورگان مبتنی بر فرمول کوکران[1] به ازای خطای ۰,۰۵ حجم نمونه ٤٤ نفر محاسبه شد که در عمل ٤٧ نفر مشارکت نمودند.

روش و ابزار گردآوری اطلاعات: روش کتابخانه‌ای و پرسشنامه در قالب عملیات میدانی به عنوان روش گردآوری اطلاعات استفاده شد. ابزار گردآوری اطلاعات پرسش‌نامه محقق ساخته و فیش‌برداری از اسناد و مدارک می‌باشد. جهت تجزیه و تحلیل اطلاعات از آماره‌های توصیفی و استنباطی نرم‌افزار spss23 استفاده شد. میزان روایی محاسبه شدهٔ پرسش‌نامه، براساس روش «روایی محتوایی» و جدول لاوشه عدد ۰,٦ که مورد قبول و همچنین میانگین آلفای کرونباخ ۰,۷۲۳ برای پرسش‌نامه‌ها نماینگر پایایی آن می‌باشد.

تجزیه و تحلیل داده‌ها در دو بخش توصیفی و استنباطی انجام شده است. در بخش توصیفی از آماره‌های توصیفی (جداول و نمودارهای فراوانی، میانگین، انحراف معیار و ...) و در بخش استنباطی از آزمون‌های «کلوموگروف اسمیرنوف» برای تشخیص نُرمالیته، «خی‌دو» به‌منظور رتبه‌بندی داده‌ها، رگرسیون چند متغیره خطی، آنالیز واریانس و آزمون F برای احصاء میزان همبستگی متغیرها و تأثیر متغیرهای مستقل بر وابسته استفاده شده است.

[1] Cochran, Morgan

۳. تجزیه و تحلیل یافته‌ها

رتبه‌بندی خصیصه‌های فناوری‌های نوظهور سایبری: به‌منظور رتبه‌بندی خصیصه‌های فناوری‌های نوظهور سایبری نسبت به توزیع پرسشنامه و گردآوری اطلاعات از خبرگان با طیف لیکرت هفت قسمتی برای ارزش‌گذاری خصیصه‌ها اقدام گردید و طبق جدول زیر میانگین نمره به‌دست آمده ارائه شده است:

جدول شماره(۲) : رتبه‌بندی خصیصه‌های فناوری‌های نوظهور سایبری

خصیصه‌ها	میانگین نمره	رتبه
هوشمندی مبتنی بر داده	٦/٤	اول
پیچیدگی و تغییر فضا	٦/۳	دوم
تهدید آفرینی	٦/۲	سوم
همگرایی و غوطه وری	٦/۱	چهارم
توزیع‌شدگی و ادراک فراگیر	٥/۹	پنجم
اشتراک‌گذاری و مشاکت اجتماعی	٥/۸	ششم
توسعه مقیاس‌ها	٥/٦	هفتم

با توجه به میانگین نمره کسب شده می‌توان گفت هوشمندی مبتنی بر داده به عنوان مهمترین بُعد فناوری‌های نوظهور سایبری با میانگین نمره ٦/٤ از ۷ نمره مطرح است. در رتبه دوم پیچیدگی و تغییر فضا با میانگین نمره ٦/۳، در رتبه سوم تهدید آفرینی با میانگین نمره ٦/۲ و در رتبه آخر نیز توسعه مقیاس‌ها با میانگین نمره ٥/٦ قرار دارد.

رتبه‌بندی ابعاد امنیّت ملّی: به‌منظور رتبه‌بندی ابعاد امنیّت ملّی نسبت به توزیع پرسش‌نامه و گردآوری اطلاعات از خبرگان با طیف لیکرت هفت قسمتی برای ارزش‌گذاری ابعاد اقدام و طبق جدول زیر میانگین نمره به‌دست آمده ارائه شده است:

جدول شماره(۳) : رتبه‌بندی ابعاد امنیت ملی

ابعاد	میانگین نمره	رتبه
سیاسی امنیتی	٦/۷	اول
نظامی دفاعی	٦/۲	دوم
فرهنگی اجتماعی	٥/۸	سوم
اقتصادی	٥/۳	چهارم

با توجه به میانگین نمره کسب شده می‌توان گفت بعد سیاسی‌امنیتی به عنوان مهمترین بعد امنیت ملی با میانگین نمره ٦/۷ از ۷ نمره مطرح است. در رتبه دوم بُعد نظامی‌دفاعی با میانگین نمره ٦/۲، در رتبه سوم بعد فرهنگی‌اجتماعی با میانگین نمره ٥/۸ و در رتبه آخر

بعد اقتصادی با میانگین نمره ۵/۳ قرار دارد، البته این نکته حائز اهمیت است که از منظر خبرگان تمامی ابعاد دارای ارزش بالایی بوده و نمره‌ای بالاتر از متوسط دریافت کرده‌اند.

بررسی تأثیر خصیصه‌های فناوری‌های نوظهور فضای سایبر بر امنیت ملی

تأثیر «همگرایی و غوطه‌وری» فناوری‌های نوظهور سایبری بر امنیت ملی:

جدول شماره(٤): خلاصه مدل رگرسیون

خلاصه مدل[b]				
مدل	ضریب همبستگی (R)	مربع ضریب همبستگی	میزان ضریب همبستگی (R) تعدیل شده	خطای استاندارد برآورد
1	[a]۰/٤۱۱	۰/۱٦۸	۰/۱۷۱	۳/٤۷۸۵
a. Dependent Variable: امنیت ملی				
b. Predictors: (Constant): همگرایی و غوطه‌وری				

جدول بالا خلاصه مدل را نشان می‌دهد. مقدار ضریب همبستگی (R) بین متغیرها ۰/۴۱۱ می‌باشد که نشان می‌دهد بین متغیّر مستقل (همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری) و متغیر وابسته تحقیق همبستگی متوسط و مستقیمی وجود دارد، اما مقدار ضریب تعدیل شده (R2) که برابر با ۰/۱۷۱ و نشان می‌دهد ۱۷/۱ درصد از کل امنیت ملی وابسته به متغیر مستقل تحقیق (همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری) می‌باشد. بنابراین میزان تأثیر متغیر مستقل بر متغیر وابسته ۱۷/۱ درصد و می‌توان گفت همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری بر امنیت ملی تأثیرگذار است.

بررسی تاثیر همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی

به‌منظور بررسی تاثیر فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی نسبت به انجام رگرسیون چند متغیره خطی اقدام گردیده است. جهت سهولت در ارائه نتایج آزمون‌های آماری انجام شده جمع‌بندی نتایج بررسی به شرح جدول ۵ می‌باشد:

جدول شماره(۵): جمع بندی روابط بین متغیرها

ردیف	متغیر مستقل	ابعاد متغیر وابسته	ضریب همبستگی (R)	ضریب تعیین (R2)	آزمون F	سطح معنی‌داری
۱	همگرایی و غوطه‌وری	سیاسی امنیتی	۰/٤۱۳	۰/۱۷۰	۲۰۷/۱۲	۰/۰۰۱
۲		نظامی دفاعی	۰/٤۸۹	۰/۲۳۹	۲۰۹/۳٦۲	۰/۰۰۰
۳		فرهنگی اجتماعی	۰/٤۵۹	۰/۲۱۰	۲۰۸/۹۵٤	۰/۰۰۰
٤		اقتصادی	۰/۳٦٤	۰/۱۳۲	۲۰۸/۱۲٤	۰/۰۱۲

بر اساس نتایج می‌توان گفت که همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری با «ضریب همبستگی» ۰/٤۸۹ بیشترین رابطه مستقیم و مثبت را با بعد نظامی‌دفاعی امنیت ملی دارد و براساس میزان «ضریب تعیین» ارائه شده همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری ۲۳/۹ درصد از بعد نظامی‌دفاعی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه دوم همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/٤۵۹ رابطه مستقیم و مثبتی را با بُعد فرهنگی‌اجتماعی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری ۲۱ درصد از بُعد فرهنگی‌اجتماعی امنیت ملی را تبیین نموده و بر آن تأثیرگذار است. در رتبه سوم همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/٤۱۳ رابطه مستقیم و مثبتی را با بعد سیاسی‌امنیتی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری ۱۷ درصد از بعد سیاسی‌امنیتی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه چهارم همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۳٦٤ رابطه مستقیم و مثبتی را با بعد اقتصادی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده همگرایی و غوطه‌وری فناوری‌های نوظهور سایبری ۱۳/۲ درصد از بعد اقتصادی امنیت ملی را تبیین و بر آن تأثیرگذار است.

تأثیر «هوشمندی مبتنی بر داده» فناوری‌های نوظهور بر امنیت ملی

جدول شماره(٦): خلاصه مدل رگرسیون

خلاصه مدل[b]				
مدل	ضریب همبستگی (R)	مربع ضریب همبستگی	میزان ضریب همبستگی (R) تعدیل شده	خطای استاندارد برآورد
1	[a]۰/٥٦۳	۰/۳۱٦	۰/۳۱۹	۳/۸۹٦۳
a. Dependent Variable: امنیت ملی				
b. Predictors: (Constant): هوشمندی مبتنی بر داده				

جدول بالا خلاصه مدل را نشان می‌دهد. مقدار ضریب همبستگی(R) بین متغیرها ۰/٥٦۳ می‌باشد که نشان می‌دهد بین متغیر مستقل (هوشمندی مبتنی بر داده فناوری‌های

نوظهور سایبری) و متغیر وابسته تحقیق همبستگی قوی و مستقیمی وجود دارد، اما مقدار ضریب تعدیل شده (R2) که برابر با ۰/۳۱۹ می‌باشد نشان می‌دهد ۳۱/۹ ٪ از کل امنیت ملی وابسته به متغیر مستقل تحقیق (هوشمندی مبتنی بر داده فناوری‌های نوظهور سایبری) می‌باشد. بنابراین میزان تأثیر متغیر مستقل بر متغیر وابسته ۳۱/۹ درصد و می‌توان گفت هوشمندی مبتنی بر داده فناوری‌های نوظهور سایبری بر امنیت ملی تأثیرگذار است.

بررسی تاثیر هوشمندی مبتنی بر داده فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی

به‌منظور بررسی تاثیر هوشمندی مبتنی بر داده فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی رگرسیون چند متغیره خطی انجام گردید. به‌منظور سهولت در ارائه نتایج آزمون‌های آماری انجام شده جمع‌بندی نتایج بررسی تحقیق به شرح جدول ۷ می‌باشد:

جدول شماره(۷): جمع بندی روابط بین متغیرها

ردیف	متغیر مستقل	ابعاد متغیر وابسته	ضریب همبستگی (R)	ضریب تعیین (R2)	آزمون F	سطح معنی‌داری
۱	هوشمندی مبتنی بر داده	سیاسی امنیتی	۰/۵۰۹	۰/۲۵۹	۲۱۳/۱۷	۰/۰۰۰
۲		نظامی دفاعی	۰/۵۸۷	۰/۳۴۴	۲۱۳/۶۹۸	۰/۰۰۰
۳		فرهنگی اجتماعی	۰/۵۲۳	۰/۲۷۳	۲۱۲/۶۶۷	۰/۰۰۰
٤		اقتصادی	۰/۵۰۱	۰/۲۵۱	۲۱۱/۵۵۷	۰/۰۰۰

براساس نتایج می‌توان گفت که هوشمندی مبتنی بر داده فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۵۸۷ بیشترین رابطه مستقیم و مثبت را با بعد نظامی‌دفاعی امنیت ملی دارد و براساس میزان ضریب تعیین ارائه شده هوشمندی مبتنی بر داده فناوری‌های نوظهور سایبری ۳٤/٤ درصد از بعد نظامی‌دفاعی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه دوم هوشمندی مبتنی بر داده فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۵۲۳ رابطه مستقیم و مثبتی را با بعد فرهنگی‌اجتماعی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده هوشمندی مبتنی بر داده فناوری‌های نوظهور سایبری ۲۷/۳ درصد از بعد فرهنگی‌اجتماعی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه سوم هوشمندی مبتنی بر داده فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۵۰۹ رابطه مستقیم و مثبتی را با بعد سیاسی‌امنیتی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده هوشمندی مبتنی

بر داده فناوری‌های نوظهور سایبری ۲۵/۹ ٪ از بعد سیاسی‌امنیتی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه چهارم هوشمندی مبتنی بر داده فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۵۰۱ رابطه مستقیم و مثبتی را با بعد اقتصادی امنیت ملی دارد و براساس میزان ضریب تعیین ارائه شده هوشمندی مبتنی بر داده فناوری‌های نوظهور سایبری ۲۵/۱ درصد از بعد اقتصادی امنیت ملی را تبیین و بر آن تأثیرگذار است.

تأثیر «اشتراک‌گذاری و مشارکت اجتماعی» فناوری‌های نوظهور بر امنیت ملی

جدول شماره(۸): خلاصه مدل رگرسیون

خلاصه مدل[b]				
مدل	ضریب همبستگی (R)	مربع ضریب همبستگی	میزان ضریب همبستگی (R) تعدیل شده	خطای استاندارد برآورد
1	[a]۰/۳٦٦	۰/۱۳۳	۰/۱۳۷	۳/۰۳۲۱
a. Dependent Variable: امنیت ملی				
b. Predictors: (Constant): اشتراک‌گذاری و مشارکت اجتماعی				

جدول بالا خلاصه مدل را نشان می‌دهد. مقدار ضریب همبستگی(R) بین متغیرها ۰/۳٦٦ می‌باشد که نشان می‌دهد بین متغیر مستقل (اشتراک‌گذاری و مشارکت اجتماعی فناوری‌های نوظهور سایبری) و متغیر وابسته تحقیق همبستگی متوسط (رو به پایین) و مستقیمی وجود دارد، اما مقدار ضریب تعدیل شده (R2) که برابر با ۰/۱۳۷ می‌باشد و نشان می‌دهد ۱۳/۷ درصد از کل امنیت ملی وابسته به متغیر مستقل تحقیق (اشتراک‌گذاری و مشارکت اجتماعی فناوری‌های نوظهور سایبری) می‌باشد. بنابراین میزان تأثیر متغیر مستقل بر متغیر وابسته ۱۳/۷ درصد و می‌توان گفت اشتراک‌گذاری و مشارکت اجتماعی فناوری‌های نوظهور سایبری بر امنیت ملی تأثیرگذار است.

بررسی تاثیر اشتراک‌گذاری و مشارکت اجتماعی فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی

به‌منظور بررسی تاثیر اشتراک‌گذاری و مشارکت اجتماعی فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی رگرسیون چندمتغیره خطی انجام گردید. به‌منظور سهولت در ارائه نتایج آزمون‌های آماری انجام شده جمع‌بندی نتایج بررسی تحقیق به شرح جدول ۹ می‌باشد:

جدول شماره(۹): جمع بندی روابط بین متغیرها

ردیف	متغیر مستقل	ابعاد متغیر وابسته	ضریب همبستگی (R)	ضریب تعیین (R2)	آزمون F	سطح معنی‌داری
۱	اشتراک‌گذاری و مشارکت اجتماعی	سیاسی امنیتی	۰/۳۹۵	۰/۱۵٦	۲۰۹/۲۱٤	۰/۰۰۸
۲		نظامی دفاعی	۰/۳٦۲	۰/۱۳۱	۲۰۹/٤۱۱	۰/۰۰۹
۳		فرهنگی اجتماعی	۰/۳۲۱	۰/۱۰۳	۲۰۸/٥٦۳	۰/۰۳
٤		اقتصادی	۰/۳۱۱	۰/۰۹٦	۲۰۹/۳۲٤	۰/۰٤

براساس نتایج ارائه شده می‌توان گفت که اشتراک‌گذاری و مشارکت اجتماعی فناوری-های نوظهور سایبری با ضریب همبستگی ۰/۳۹۵ بیشترین رابطه مستقیم و مثبت را با بعد سیاسی‌امنیتی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده اشتراک‌گذاری و مشارکت اجتماعی فناوری‌های نوظهور سایبری ۱۵/٦ درصد از بُعد سیاسی‌امنیتی امنیت ملی را تبیین و بر آن موثر است. در رتبه دوم اشتراک‌گذاری و مشارکت اجتماعی فناوری-های نوظهور سایبری با ضریب همبستگی ۰/۳٦۲ رابطه مستقیم و مثبتی را با بعد نظامی-دفاعی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده اشتراک‌گذاری و مشارکت اجتماعی فناوری‌های نوظهور سایبری ۱۳/۱ درصد از بعد نظامی‌دفاعی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه سوم اشتراک‌گذاری و مشارکت اجتماعی فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۳۲۱ رابطه مستقیم و مثبتی با بعد فرهنگی اجتماعی امنیت ملی دارد. براساس میزان ضریب تعیین اشتراک‌گذاری و مشارکت اجتماعی فناوری-های نوظهور سایبری ۱۰/۳ ٪ از بعد فرهنگی‌اجتماعی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه چهارم اشتراک‌گذاری و مشارکت اجتماعی فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۳۱۱ رابطه مستقیم و مثبتی را با بعد اقتصادی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده اشتراک‌گذاری و مشارکت اجتماعی فناوری‌های نوظهور سایبری ۹/٦ درصد از بعد اقتصادی امنیت ملی را تبیین و بر آن تأثیرگذار است.

تأثیر «تهدیدآفرینی» فناوری‌های نوظهور بر امنیت ملی

جدول شماره(۱۰): خلاصه مدل رگرسیون

خلاصه مدل[b]

مدل	ضریب همبستگی (R)	مربع ضریب همبستگی	میزان ضریب همبستگی (R) تعدیل شده	خطای استاندارد برآورد
1	[a]۰/۳۰۳	۰/۰۹۱	۰/۰۹۳	۳/۱۲٥٤

a. Dependent Variable: امنیت ملی

b. Predictors: (Constant): تهدید آفرینی

جدول بالا خلاصه مدل را نشان می‌دهد. مقدار ضریب همبستگی (R) بین متغیرها ۰/۳۰۳ می‌باشد که نشان می‌دهد بین متغیر مستقل (تهدیدآفرینی فناوری‌های نوظهور سایبری) و متغیر وابسته تحقیق همبستگی متوسط (رو به پایینی) وجود دارد، اما مقدار ضریب تعدیل شده (R2) که برابر با ۰/۰۹۳ بوده و نشان می‌دهد ۹/۳ درصد از کل امنیت ملی وابسته به متغیر مستقل تحقیق (تهدیدآفرینی فناوری‌های نوظهور سایبری) می‌باشد. بنابراین میزان تأثیر متغیر مستقل بر متغیر وابسته ۹/۳ درصد و می‌توان گفت تهدید آفرینی فناوری‌های نوظهور سایبری بر امنیت ملی تأثیرگذار است.

بررسی تاثیر تهدید آفرینی فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی

به‌منظور بررسی اثر تهدیدآفرینی فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی به رگرسیون چندمتغیره خطی انجام گردید. جهت سهولت در ارائه نتایج آزمون‌های آماری انجام شده، جمع‌بندی نتایج بررسی تحقیق به شرح جدول ذیل می‌باشد:

جدول شماره(۱۱): جمع بندی روابط بین متغیرها

ردیف	متغیر مستقل	ابعاد متغیر وابسته	ضریب همبستگی (R)	ضریب تعیین (R2)	آزمون F	سطح معنی‌داری
۱	تهدید آفرینی	سیاسی امنیتی	۰/۳۱٤	۰/۰۹۸	۲۰۸/۱٤۲	۰/۰۰۹
۲		نظامی دفاعی	۰/۳۰٦	۰/۰۹۳	۲۰۸/۳۳٦	۰/۰۱۲
۳		فرهنگی اجتماعی	۰/۲۸۹	۰/۰۸۳	۲۰۷/۱۱۹	۰/۰۳۲
٤		اقتصادی	۰/۲۸۳	۰/۰۸۰	۲۰۷/۰۰۳	۰/۰٤٤

براساس نتایج ارائه شده می‌توان گفت که تهدیدآفرینی فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۳۱٤ بیشترین رابطه مستقیم و مثبت را با بعد سیاسی‌امنیتی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده، تهدیدآفرینی فناوری‌های نوظهور سایبری ۹/۸ درصد از بعد سیاسی‌امنیتی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه دوم

تهدیدآفرینی فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۳۰٦ رابطه مستقیم و مثبتی را با بعد نظامی‌دفاعی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده تهدیدآفرینی فناوری‌های نوظهور سایبری ۹/۳ ٪ از بعد نظامی‌دفاعی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه سوم تهدیدآفرینی فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۲۸۹ رابطه مستقیم و مثبتی را با بعد فرهنگی‌اجتماعی امنیت ملی دارد و براساس میزان ضریب تعیین ارائه شده تهدیدآفرینی فناوری‌های نوظهور سایبری ۸/۳ ٪ از بعد فرهنگی‌اجتماعی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه چهارم تهدیدآفرینی فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۲۸۳ رابطه مستقیم و مثبتی را با بعد اقتصادی امنیت ملی دارد. براساس میزان ضریب تعیین تهدیدآفرینی فناوری‌های نوظهور سایبری ۸ ٪ از بعد اقتصادی امنیت ملی را تبیین و بر آن اثر دارد.

تأثیر «پیچیدگی و تغییر فضا»ی فناوری‌های نوظهور بر امنیت ملی

جدول شماره(۱۲): خلاصه مدل رگرسیون

خلاصه مدل[b]

مدل	ضریب همبستگی(R)	مربع ضریب همبستگی	میزان ضریب همبستگی(R) تعدیل شده	خطای استاندارد برآورد
1	[a]۰/٤١٤	۰/۱۷۱	۰/۱۷۳	۳/۳۲۱٤

a. Dependent Variable: امنیت ملی

b. Predictors: (Constant): پیچیدگی و تغییر فضا

جدول بالا خلاصه مدل را نشان می‌دهد. مقدار ضریب همبستگی(R) بین متغیرها ۰/٤١٤ می‌باشد که نشان می‌دهد بین متغیر مستقل (پیچیدگی و تغییر فضا فناوری‌های نوظهور سایبری) و متغیر وابسته تحقیق همبستگی نسبتاً قوی و مستقیمی وجود دارد، اما مقدار ضریب تعدیل شده (R2) که ۰/۱۷۳ می‌باشد نشان می‌دهد ۱۷/۳ ٪ از کل امنیت ملی وابسته به متغیر مستقل تحقیق (پیچیدگی و تغییر فضای فناوری‌های نوظهور سایبری) و بنابراین میزان تأثیر متغیر مستقل بر متغیر وابسته ۱۷/۳ ٪ می‌باشد. می‌توان گفت پیچیدگی و تغییر فضای فناوری‌های نوظهور سایبری بر امنیت ملی تأثیرگذار است.

بررسی تاثیر پیچیدگی و تغییر فضای فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی

به‌منظور بررسی تاثیر پیچیدگی و تغییر فضای فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی رگرسیون چند متغیره خطی انجام که به‌دلیل کاهش ارائه جداول آماری نسبت به جمع‌بندی میزان تأثیر در جدول زیر اقدام گردیده است. به‌منظور سهولت در ارائه نتایج آزمون‌های آماری انجام شده جمع‌بندی نتایج بررسی **تحقیق** به شرح جدول ذیل می‌باشد:

جدول شماره(۱۳): جمع بندی روابط بین متغیرها

ردیف	متغیر مستقل	ابعاد متغیر وابسته	ضریب همبستگی (R)	ضریب تعیین (R2)	آزمون F	سطح معنی‌داری
۱	پیچیدگی و تغییر فضا	سیاسی امنیتی	۰/٤۱۹	۰/۱۷۵	۲۱۰/۱۷	۰/۰۰۰
۲		نظامی دفاعی	۰/٤۲۵	۰/۱۸۰	۲۱۱/۵۵٤	۰/۰۰۰
۳		فرهنگی اجتماعی	۰/٤۰۱	۰/۱٦۰	۲۱۰/٦٦۵	۰/۰۰۰
٤		اقتصادی	۰/٤۰٤	۰/۱٦۳	۲۰۹/۳٦۲	۰/۰۰۰

براساس نتایج ارائه شده می‌توان گفت که پیچیدگی و تغییر فضای فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/٤۲۵ بیشترین رابطه مستقیم و مثبت را با بعد نظامی‌دفاعی امنیت ملی دارد و براساس میزان ضریب **تعیین** ارائه شده پیچیدگی و تغییر فضای فناوری-های نوظهور سایبری ۱۸ ٪ از بعد نظامی دفاعی امنیت ملی را تبیین و بر آن اثر دارد. در رتبه دوم پیچیدگی و تغییر فضای فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/٤۱۹ رابطه مستقیم و مثبت با بعد سیاسی‌امنیتی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده پیچیدگی و تغییر فضای فناوری‌های نوظهور سایبری ۱۷/۵ ٪ از بعد سیاسی - امنیتی امنیت ملی را تبیین و بر آن اثر دارد. در رتبه سوم پیچیدگی و تغییر فضای فناوری-های نوظهور سایبری با ضریب همبستگی ۰/٤۰٤ رابطه مستقیم و مثبتی را با بعد اقتصادی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده پیچیدگی و تغییر فضا فناوری‌های نوظهور سایبری ۱٦/۳ ٪ از بعد اقتصادی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه چهارم پیچیدگی و تغییر فضای فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/٤۰۱ رابطه مستقیم و مثبتی را با بعد فرهنگی اجتماعی امنیت ملی دارد و براساس میزان ضریب تعیین ارائه شده پیچیدگی و تغییر فضای فناوری‌های نوظهور سایبری ۱٦ ٪ از بعد فرهنگی اجتماعی امنیت ملی را تبیین و بر آن تأثیرگذار است.

تأثیر «توسعه مقیاس‌ها»ی فناوری‌های نوظهور بر امنیت ملی

جدول شماره(۱۴): خلاصه مدل رگرسیون

خلاصه مدل[b]				
مدل	ضریب همبستگی(R)	مربع ضریب همبستگی	میزان ضریب همبستگی(R) تعدیل شده	خطای استاندارد برآورد
1	۰/۳٤٤[a]	۰/۱۱۸	۰/۱۲۱	۳/۰۰۳

a. Dependent Variable: امنیت ملی

b. Predictors: (Constant): توسعه مقیاس‌ها

جدول بالا خلاصه مدل را نشان می‌دهد. مقدار ضریب همبستگی(R) بین متغیرها ۰/۳٤٤ می‌باشد که نشان می‌دهد بین متغیر مستقل (توسعه مقیاس‌های فناوری‌های نوظهور سایبری) و متغیر وابسته تحقیق همبستگی متوسط (رو به پایین) وجود دارد، اما مقدار ضریب تعدیل شده (R2) که برابر با ۰/۱۲۱ می‌باشد که نشان می‌دهد ۱۲/۱ ٪ از کل امنیت ملی وابسته به متغیر مستقل تحقیق (توسعه مقیاس‌ها فناوری‌های نوظهور سایبری) می‌باشد. بنابراین میزان تأثیر متغیر مستقل بر متغیر وابسته ۱۲/۱ ٪ می‌باشد. می‌توان گفت توسعه مقیاس‌های فناوری‌های نوظهور سایبری بر امنیت ملی اثر دارد.

بررسی تاثیر توسعه مقیاس‌های فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی

به‌منظور بررسی تاثیر توسعه مقیاس‌های فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی رگرسیون چند متغیره خطی اقدام انجام شد. به‌منظور سهولت در ارائه نتایج آزمون‌های آماری انجام شده جمع بندی نتایج بررسی تحقیق به شرح جدول ذیل می‌باشد:

جدول شماره(۱۵): جمع‌بندی روابط بین متغیرها

ردیف	متغیر مستقل	ابعاد متغیر وابسته	ضریب همبستگی (R)	ضریب تعیین (R2)	ازمون F	سطح معنی‌داری
۱	توسعه مقیاس‌ها	سیاسی امنیتی	۰/٤٥۳	۰/۲۰٦	۲۱۰/۱٤۱	۰/۰۰۱
۲		نظامی دفاعی	۰/٤٦۸	۰/۲۱۹	۲۱۰/۲۳٦	۰/۰۰۰
۳		فرهنگی اجتماعی	۰/٤٤۲	۰/۱۹٥	۲۰۹/۳۳۳	۰/۰۰٥
٤		اقتصادی	۰/٤۳۱	۰/۱۸٥	۲۰۹/۲۱۷	۰/۰۰۹

بنابر نتایج می‌توان گفت؛ توسعه مقیاس‌های فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/٤٦۸ بیشترین رابطه مستقیم و مثبت را با بعد نظامی دفاعی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده توسعه مقیاس ها فناوری‌های نوظهور سایبری ۲۱/۹ ٪ از بعد نظامی‌دفاعی امنیت ملی را تبیین و بر آن اثر دارد. در رتبه دوم توسعه مقیاس‌های

فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/٤٥۳ رابطه مستقیم و مثبت با بعد سیاسی امنیتی امنیت ملی دارد. براساس میزان ضریب تعیین ارائه شده توسعه مقیاس‌ها فناوری‌های نوظهور سایبری ۲۰/٦ ٪ از بعد سیاسی امنیتی امنیت ملی را تبیین و بر آن اثر دارد. در رتبه سوم توسعه مقیاس‌های فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/٤٤۲ رابطه مستقیم و مثبتی را با بعد فرهنگی‌اجتماعی امنیت ملی دارد و بنابر میزان ضریب تعیین ارائه شده توسعه مقیاس‌های فناوری‌های نوظهور سایبری ۱۹,۵ ٪ از بعد فرهنگی اجتماعی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه چهارم توسعه مقیاس‌های فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/٤۳۱ با بعد اقتصادی امنیت ملی رابطه مستقیم و مثبت دارد. براساس میزان ضریب تعیین ارائه شده توسعه مقیاس‌ها فناوری‌های نوظهور سایبری ۱۸/۵ ٪ از بعد اقتصادی امنیت ملی را تبیین و بر آن اثر دارد.

تأثیر «توزیع‌شدگی و ادراک فراگیر» فناوری‌های نوظهور بر امنیت ملی

جدول شماره(۱٦): خلاصه مدل رگرسیون

خلاصه مدل[D]

مدل	ضریب همبستگی(R)	مربع ضریب همبستگی	میزان ضریب همبستگی(R) تعدیل شده	خطای استاندارد برآورد
1	[a]۰/۳٦۹	۰/۱۳٦	۰/۱۳۹	۳/۲۲٤۷

a. Dependent Variable: امنیت ملی

b. Predictors: (Constant): توزیع شدگی و ادراک فراگیر

جدول بالا خلاصه مدل را نشان می‌دهد. مقدار ضریب همبستگی(R) بین متغیرها ۰/۳٦۹ می‌باشد که حکایت از وجود همبستگی متوسط (رو به پایین) بین متغیر مستقل (توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری) و متغیر وابسته دارد، اما مقدار ضریب تعدیل شده (R2) که برابر با ۰/۱۳۹ می‌باشد نشان می‌دهد ۱۳/۹ ٪ از کل امنیت ملی وابسته به متغیر مستقل تحقیق (توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری) است. بنابراین میزان تأثیر متغیر مستقل بر متغیر وابسته ۱۳/۹ ٪ می‌باشد. می‌توان گفت توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری بر امنیت ملی اثر دارد.

بررسی تاثیر توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی

به‌منظور بررسی تاثیر توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری بر ابعاد امنیت ملی، رگرسیون چند متغیره خطی انجام شد. به‌منظور سهولت در ارائه نتایج آزمون-های آماری انجام شده جمع‌بندی نتایج بررسی تحقیق به‌شرح جدول ذیل می‌باشد:

جدول شماره(۱۷): جمع بندی روابط بین متغیرها

ردیف	متغیر مستقل	ابعاد متغیر وابسته	ضریب همبستگی (R)	ضریب تعیین (R2)	آزمون F	سطح معنی‌داری
۱	توزیع‌شدگی و ادراک فراگیر	سیاسی امنیتی	۰/۳۹۱	۰/۱۵۲	۲۰۹/۱۱٤	۰/۰۰۱
۲		نظامی دفاعی	۰/۳۷۷	۰/۱٤۲	۲۰۹/۸۵٦	۰/۰۰۲
۳		فرهنگی اجتماعی	۰/۳٦۲	۰/۱۳۱	۲۰۸/۸۸۷	۰/۰۰۵
٤		اقتصادی	۰/۳۵۹	۰/۱۲۸	۲۰۸/٦٦۵	۰/۰۰۹

براساس نتایج ارائه شده می‌توان گفت که توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۳۹۱ بیشترین رابطه مستقیم و مثبت را با بعد سیاسی امنیتی امنیت ملی دارد و براساس میزان ضریب تعیین ارائه شده توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری ۱۵/۲ ٪ از بعد نظامی دفاعی امنیت ملی را تبیین و بر آن اثر دارد.

در رتبه دوم توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۳۷۷ با بعد نظامی دفاعی امنیت ملی رابطه مستقیم و مثبت دارد. براساس میزان ضریب تعیین ارائه شده توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری ۱٤/۲ ٪ از بعد نظامی دفاعی امنیت ملی را تبیین و بر آن اثر دارد. در رتبه سوم توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۳٦۲ رابطه مستقیم و مثبتی را با بعد فرهنگی‌اجتماعی امنیت ملی دارد. برابر میزان ضریب تعیین ارائه شده توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری ۱۳/۱ ٪ از بعد فرهنگی اجتماعی امنیت ملی را تبیین و بر آن تأثیرگذار است. در رتبه چهارم توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری با ضریب همبستگی ۰/۳۵۹ رابطه مستقیم و مثبتی را با بعد اقتصادی امنیت ملی دارد و برابر میزان ضریب تعیین ارائه شده توزیع‌شدگی و ادراک فراگیر فناوری‌های نوظهور سایبری ۱۲/۸ درصد از بعد اقتصادی امنیت ملی را تبیین و بر آن تأثیرگذار است.

٤. نتیجه‌گیری و پیشنهاد

می‌توان گفت تحوّلات سریع و عمیق فناوری‌های فضای سایبر که در ابعاد مختلف اجتماعی، فرهنگی، اقتصادی، سیاسی، فناورانه، امنیتی و نظامی-دفاعی دارای تأثیرات راهبردی در حاکمیت کشور است نیازمند نگاهی جامع، ساختاریافته و منسجم به‌منظور حفاظت و صیانت از منافع ملی و امنیت ملی باهدف حفظ اشرافیت بر رویدادها، روندها، تغییرات محیطی و تحولات در حال و آینده است تا امکان تصمیم‌گیری، برنامه‌ریزی و مدیریت آن فراهم آید. این پژوهش به بررسی تأثیرات فناوری‌های نوظهور فضای سایبر بر امنیت ملی پرداخت. در گام اول مشخصات اختصاصی به‌منظور ایجاد هویتی یکتا برای فناوری‌های نوظهور به‌مثابه یک ماهیّت یک‌پارچه و موجودیّتی با قابلیّت شناسایی یگانه مبتنی بر این خصیصه‌ها مورد بررسی قرار گرفت. در مرحله ابتدایی خصیصه‌های اختصاصی فناوری‌ها در هفت دسته اصلی شناسایی و در مرحله بعد در فضای ذهنی انتزاعی‌تر و مستقل از تحولات صحنهٔ بروزرسانی‌های مستمرّ فناوری‌ها، به بررسی تأثیرات آن بر ابعاد امنیت ملی پرداخته و نشان داده شد مؤلفه‌های مختلف توصیف‌کننده فناوری بر همه ابعاد گوناگون امنیت ملی اثر مستقیم دارد. بنابراین از منظر ملّی نمایان است که تقویت درون‌زای قدرت ملی با مدیریت صحیح فناوری‌های نوظهور منجر به افزایش توان اثرگذاری بر هندسه مطلوب نظم نوین جهانی خواهد شد و اقدامات پیش‌کنش‌گرانه نظام حاکمیت کشور با رویکرد فرصت‌محور در تقابل با تهدیدات فناوری‌های نوظهور از جایگاه مهم راهبردی برخوردار است.

در پاسخ به سئوال اصلی تحقیق (تأثیر فناوری‌های نوظهور سایبری بر امنیت ملی) می‌توان اذعان داشت که خصیصه‌های فناوری‌های نوظهور در ازای پاسخ سئوال فرعی اول، در شکل شماره ۲ به‌طور مشخص دسته‌بندی و در ادامه توصیف و تعریف عملیاتی مربوطه ارائه گشت. همچنین با مشخص کردن تأثیر مستقیم هریک از خصیصه‌های هفت‌گانه فناوری بر هر یک از ابعاد امنیّت ملّی در سئوال فرعی دوم، پاسخ به سئوال اول بدین‌صورت ارائه شد که بُعد سیاسی‌امنیّتی بیشترین تاثیرپذیری و پس از آن ابعاد نظامی‌دفاعی،

فرهنگی‌اجتماعی و اقتصادی در رتبه‌های بعدی قرار دارند، امّا به‌دلیل اختلاف کم مقدار عددی میانگین نمره تخصیص‌یافته برای هر بُعد می‌توان گفت که فناوری نوظهور بر همه ابعاد امنیت ملّی اثرگذاری مستقیم و معنادار دارد. با بررسی و تجزیه و تحلیل‌های آماری در جمع‌بندی روابط بین متغیرها براساس نتایج ارائه شده در این پژوهش، می‌توان بدین‌گونه نتیجه تأثیرات را تبیین نمود: در رتبه اول، هوشمندی مبتنی بر داده با ضریب همبستگی ۰/٥٦۳ بیشترین رابطه مستقیم و مثبت را با امنیت ملی دارد و میزان تأثیر آن ۳۱٪/۹ بوده و بیشترین تأثیر آن بر بُعد نظامی‌دفاعیِ امنیت ملی است. در رتبه دوم، پیچیدگی و تغییر فضا با ضریب همبستگی ۰/٤۱٤ رابطه مستقیم و مثبت را با امنیت ملی داشته و میزان تأثیر آن ۱۷/۳٪ بوده و بیشترین تأثیر آن بر بُعد نظامی‌دفاعیِ امنیت ملی است. در رتبه سوم، همگرایی و غوطه‌وری با ضریب همبستگی ۰/٤۱۱ و با میزان تأثیر ۱۷٪/۱ رابطه مستقیم و مثبت با امنیت ملی دارد، که بیشترین تأثیر آن بر بعد نظامی‌دفاعی امنیت ملی است. در رتبه چهارم، توزیع‌شدگی و ادراک فراگیر با ضریب همبستگی ۰/۳٦۹ و میزان تأثیر ۱۳/۹٪ رابطه مستقیم و مثبت را با امنیت ملی دارد و بیشترین تأثیر آن بر بُعد سیاسی‌امنیتیِ امنیت ملی است. در رتبه پنجم، اشتراک‌گذاری و مشارکت اجتماعی با ضریب همبستگی ۰/۳٦٦ و میزان تأثیر ۱۳/۷٪ رابطه مستقیم و مثبت با امنیت ملی دارد و بیشترین تأثیر آن بر بعد سیاسی‌امنیتیِ امنیت ملی است. در رتبه ششم، توسعه مقیاس‌ها با ضریب همبستگی ۰/۳٤٤ و میزان تأثیر آن ۱۲/۱٪ رابطه مستقیم و مثبت با امنیت ملی دارد و بیشترین تأثیر آن بر بُعد نظامی‌دفاعیِ امنیّت ملّی است. در رتبه هفتم، تهدید آفرینی با ضریب همبستگی ۰/۳۰۳ و میزان تأثیر ۹/۳ ٪ رابطه مستقیم و مثبت را با امنیت ملی دارد و بیشترین تأثیر آن بر بعد سیاسی‌امنیتیِ امنیت ملّی است.

پیشنهادها

باتوجّه به ماهیّت سیّال و متحوّل فضای سایبری به‌دلیل وابستگی جدّی به رشد علم و فناوری، به‌خصوص آنکه به‌دلیل هم‌گرایی و اندماج ساحت‌های مختلف فناوری، از ماهیّتی با پیچیدگی و عدم‌قطعیّت بالا و با تغییرات سریع و ریشه‌ای که مسبوق به سابقه ذهن بشر

نیست، برخوردار است. بنابراین برای مصونیّت از تهدیدات آن و بهره‌گیری از فرصت‌های بی‌بدیل پیشِ‌رو و امکان تبدیل تهدیدات به فرصت‌ها با عمق راهبردی در حوزه حاکمیّت سایبر ملی، بدین‌وسیله پیشنهاد می‌شود سازوکار تخصّصی و دانش‌بنیان برای رصد دائمی و هستان‌شناسی مستمرّ با هدف شناخت ماهیّتِ متغیّر فضای سایبری در کشور ایجاد تا نسبت به بُروز غافلگیری راهبردی در سطح ملّی مصونیّت ایجاد شده و چابکی و قابلیّت کنش‌گری پیش‌دستانه همواره برای حوزه حکمرانی سایبری ملّی و به‌طور اختصاصی در هر سازمان حاکمیتی به‌ویژه حوزه امنیّت متصوّر باشد.

با معرفی تأثیرات قطعی فناوری بر ابعاد امنیت ملی، برای مقطع دکتری، پژوهش‌های مرتبط با تدوین «نظام ملی حاکمیّت فناوری‌های نوظهور مبتنی بر ارزش‌ها و ارکان جهت ساز اسلامی–ایرانی» مشتمل بر هستان‌شناسی عمیق و مستمر، اِفراز نیازمندی‌های کلان و نظام مسائل کشور، چشم‌انداز، اهداف کلان، معماری ملی زیست‌بوم فناوری، سیاست‌های اجرایی، نگاشت نهادی، روابط بازیگران، تدوین اقدامات پیش‌دستانه در تمام سطح ملی و فراملی و تعریف ساختار وظیفه منطقی آن برای ارکان حکمرانی کشور موردتوجه قرار گیرد.

همچنین پیشنهاد می‌شود تأثیرات فناوری‌های نوظهور فضای سایبری به‌طور مشخص در هریک از ابعاد امنیت ملی شامل، اقتصادی، سیاسی، فرهنگی، اجتماعی، نظامی، زیست-محیطی، حقوقی و قضایی به‌طور جداگانه و با نگاه تخصصی و وضوح بیشتر مورد تدقیق و پژوهش قرار گیرد و راه‌کارها و اقدامات راهبردی پیش‌دستانه لازم، به متولیان و مدیران آن حوزه جهت بهره‌برداری از مناظر فرصت و تهدید ارائه شود.

«الگوی راهبردی صیانت از اخلاقیات و فرهنگ در عصر تحولات فضای سایبری متأثّر شده از فناوری‌های نوظهور»، همچنین «طراحی نظام مسئولیت و پاسخ‌گویی» در این عصر از دیگر عناوین پژوهشی پیشنهادی در سطح ملی می‌باشد.

باتوجه به اهمیت جایگاه روابط بین‌الملل و تأثیرات متقابل سیاست خارجه با موضوع توسعه فناوری‌های نوظهور سایبری در سطح ملی و جهانی، الزامات، معماری و نگاشت

نهادی نظام دیپلماسی سایبری کشور در وزارت امورخارجه با نگاه قرارگاهی (تعیین وظیفه و جایگاه نقش‌آفرینی همه بازیگران صحنهٔ اقتصادی، علم‌وفناوری، آموزشی، فرهنگی، نهادهای امنیتی، دفاعی، حقوقی و قضایی کشور) در قالب یک نظام ملی به عنوان رساله دکتری «الگوی راهبردی نظام دیپلماسی سایبری کشور» موردتوجّه پژوهشی واقع شود.

نتایج این تحقیق در اختیار دست‌اندرکاران و متولیان امور امنیتی و نظامی در کشور قرار گیرد تا در برنامه‌ریزی‌های ملی مورد بهره‌برداری واقع شده و همچنین خطرات ناشی از استفاده دشمنان از فناوری‌های نوین سایبری و امکان استفاده بهینه از این فناوری‌ها در ارتقاء امنیت ملی مورد غفلت واقع نشود.

فهرست منابع و مآخذ

الف. منابع فارسی

- ایزدی، جهانبخش و تکبیری، مجتبی؛ (۱۳۹۳)، ***تاثیر دیپلماسی هوشمند در ارتباطات سیاسی نظام بین‌الملل***، جلد هفتم، شماره ۲٦، ۳٤-۵۵.
- باهوش فاردقی، محمود؛ (۱۳۹٦)، ***بررسی مفهوم یا استعاره‌ی امنیّت ملّی در نظریّه‌ی سازه‌انگاری***، فصلنامه سیاست، سال چهارم، شماره چهاردهم، ۱۰۱-۱۱۲.
- بخشی تلیابی، رامین؛ آذرشب، محمدتقی و نجم آبادی، مرتضی؛ (۱۳۹٦)، ***جایگاه امنیت در مکتب کپنهاگ: چارچوبی برای تحلیل***، فصلنامه تخصصی علوم سیاسی ۱۳ (٤۰)، ۱٤٦-۱۱۹.
- بیات، بهرام؛ (۱۳۹۸)، ***نظریه‌های امنیت ملی***، مرکز انتشارات راهبردی دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ۳۷۵ صفحه، رده‌بندی دیویی: ۰۳/۳۵۵.
- پیشگاهی‌فرد، زهرا؛ حسینی، سید موسی و فراهانی، مرتضی؛ (۱۳۹۳)، ***رتبه‌بندی قدرت ملی کشورهای خاورمیانه با استفاده از تصمیم‌گیری چندشاخصه جبرانی***، پژوهشنامه جغرافیای انتظامی، سال دوم، شماره پنجم، ۱تا٤٤.
- خانی، مهدی (۱۳۹۹)، ***مفهوم‌سازی بحران امنیتی با تأکید بر آموزه‌های مکتب کپنهاگ***، فصلنامه محیط راهبردی، سال چهارم، شماره ۱۲، ۸۵-۱۰۲.
- کهن سال کلکناری، منیره و بابایی نسامی، عبداله؛ (۱۳۹٦)، ***امنیت سایبری، تهدیدها و اثرات آن بر امنیت ملی***، دومین کنگره بین المللی علوم انسانی، مطالعات فرهنگی.
- محمودزاده، ابراهیم؛ (۱۳۸۹)، ***مدیریت بر آینده با تکنولوژی فردا***، ناشر: شرکت انستیتو ایز ایران زبان: فارسی رده‌بندی دیویی: ٦۵۸,٤ ، نوبت چاپ: ۳ تیراژ: ۱۰۰۰ نسخه.
- مرادی، عبدالله؛ رمضانی، مجید؛ محمدی، محسن و جهانبزرگی، احمد؛ (۱۳۹۹)، ***امنیت ملی در عصر جدید، روندها و مؤلفه‌ها***، مرکز انتشارات راهبردی دانشگاه عالی دفاع ملی، تهران، شابک: -۳-۲۰۵-۲٤۸-٦۲۲-۹۷۸، نوبت چاپ اول.
- هلیلی، خداداد؛ ولوی، محمدرضا؛ موحدی صفت، محمدرضا و باقری، مسعود؛ (۱۳۹۷)، ***قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر***، فصلنامه امنیت ملی، سال هشتم، شماره بیست و نهم، ۱۷۳-۲۰۰.
- هندیانی، عبدالله؛ (۱۳۸٦)، ***بررسی تحولات مفهومی امنیت در محیط امنیتی***، دانش‌انتظامی، دوره ۹، شماره۳ (مسلسل۳۵)، ۳۰-۹.

ب. منابع انگلیسی

- Andrade, Roberto O and Yoo, Sang Guun;(2019), Cognitive security: A comprehensive study of cognitive science in cybersecurity, ***Journal of Information Security and Applications***, 48, 102352, www.elsevier.com/locate/jisa
- Attiah, Mark A. and Farah, Martha J. (15 May 2014), Minds, motherboards, and money: futurism and realism in the neuroethics of BCI technologies. ***Frontiers in Systems Neuroscience***. 8 (86): 86. doi:10.3389/fnsys.2014.00086.,
- Atlam, Hany F.; Alenezi, Ahmed; Alassafi, Madini O.; Wills, Gary B.; (June 2018), Intelligent Systems and Applications, Blockchain with Internet of Things: Benefits, Challenges, and Future Directions, I.J., 40-48 ***Published Online in MECS*** (http://www.mecs-press.org/) DOI: 10.5815/ijisa.2018.06.05
- Billingsley, Joseph L.; (May 2023), Integrated Deterrence and Cyberspace Selected

Essays Exploring the Role of Cyber Operations in the Pursuit of National Interest, ***National Defense University Press Washington, D.C***. First printing.
- Brain, David Johnson; Alida, Draudt; Brown, Jason C.; Lieutenant Colonel Robert, J. Ross; (2020), INFORMATION WARFARE AND THE FUTURE OF CONFLICT, ***Arizona State University***.
- Breno, Pauli Medeiros and Luiz, Rogério Franco Goldoni; (Jan/Apr 2020), The Fundamental Conceptual Trinity of Cyberspace, ***Contexto Internacional*** vol. 42(1), Brazillian Army Command and General Staff College (ECEME), PP:31-54 http://dx.doi.org/10.1590/S0102-8529.2019420100002
- Bussu, Sonia; Yaron, Golan; Hargreaves, Anna; (2022), Understanding developments in Participatory Governance A report on findings from a scoping review of the literature and expert interviews, ***Manchester Metropolitan University,*** 72 pages. ISBN: 9781910029787
- Cadell, Last; (2020), Global Brain Singularity-Universal History, Future Evolution and Humanity's Dialectical Horizon, **Springerm Vrije Universiteit Brussel Brussels**, Belgium, 339 pages. ISBN 978-3-030-46966-5
- Cheraghi, Ahmad Reza; Shahzad, Sahdia; Graffi, Kalman; (2021), Past, Present, and Future of Swarm Robotics, University D¨usseldorf, Germany, published in **Intelligent Systems Conference** (IntelliSys 2021).
- Chisnall, Mick; (2020), Digital slavery, time for abolition?, **POLICY STUDIES**, VOL. 41, NO.5, Taylor & Francis Group. UK Limited, pp: 488–506. https://doi.org/10.1080/01442872.2020.1724926.
- Cozzens, Susan; Sonia, Gatchair; Jongseok, Kang; Kyung-Sup, Kim; Hyuck, Jai Lee; Gonzalo, Ordóñez & Alan, Porter; (2010), Emerging technologies: quantitative identification and measurement, **Technology Analysis & Strategic Management**, 22:3, 361-376, DOI: 10.1080/09537321003647396.
- Dotsenko, Elena; (2017), The Second International Innovative Mining Symposium, NBIC-Convergence as a Paradigm Platform of Sustainable Development, E3S Web of Conferences 21, 04013, **Plekhanov Russian University of Economics**, Moscow, DOI: 10.1051/e3sconf/20172104013.
- Dwivedi, Yogesh K.; Laurie, Hughes; Baabdullah, Abdullah M.; Ribeiro-Navarrete, Samuel; et al.; (2022), Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy, **International Journal of Information Management,** 66, doi:10.1016/j.ijinfomgt.2022.102542.
- EU (European Union) (2019), European Cluster and Industrial Transformation Trends Report, European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Unit F.2: Clusters, Social Economy and Entrepreneurship, **Luxembourg: Publications Office of the European Union**, scientific supervision: Ron Boschma (Utrecht University), ISBN 978-92-9202-747-6.
- Fei, Hu; Xin-Lin, Huang and DongXiu, Ou; (2021), UAV Swarm Networks: Models, Protocols, and Systems, **CRC press,** ISBN: 9781003039327 (ebk)
- Fernando, Marie D; (2019), The Phenomenon of Social Computing, A Thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy, **Western Sydney University**.
- Gompert, David C. and Binnendijk, Hans; (2016), The Power to Coerce: Countering Adversaries Without Going to War, Prepared for the United States Army, Published by the **RAND Corporation**, www.rand.org/t/rr1000
- Halaweh, Mohanad; (2013), Emerging Technology: What is it?, ISSN: 0718-2724. (http://www.jotmi.org) **Journal of Technology Management & Innovation** © Universidad Alberto Hurtado, Facultad de Economía y Negocios, J. Technol. Manag. Innov. 2013, Volume 8, Issue 3, 108-115.
- Huansheng, Ning; (2022), A Brief History of Cyberspace, 227 pages, **CRC Press, Taylor & Francis Group**, ISBN: 978-1-003-25738-7
- Huansheng, Ning; Xiaozhen, Ye; Bouras, Mohammed Amine; Dawei, Wei and Daneshmand, Mahmoud; (June 2018), General Cyberspace: Cyberspace and Cyber-enabled Spaces, **IEEE INTERNET OF THINGS JOURNAL,** VOL. 5, NO. 3, 2327-4662 (c), DOI 10.1109/JIOT.2018.2815535, IEEE, .1843-1856.
- JP, Joint Publication 3-12 Cyberspace Operations, (5 February 2013) **U.S. Army**, and so updated: 8 June 2018.
- Kademi, Anas Maazu and Koltuksuz, Ahmet Hasan; (2021), Cyber-physical-socialinformation- thinking hyperspace: a manifold of cyberspatial entities, **Computer Engineering Department, Yasar University**, Izmir, Turkey,

https://www.emerald.com/insight/0368-492X.htm
- Kademi, Anas Mu'azu and Koltuksuz, Ahmet; (December 2020), Dynamic Cyberspace Modeling from Network Automata, **IJCSNS International Journal of Computer Science and Network Security**, VOL.20 No.12, doi:10.22937/IJCSNS.2020.20.12.4
- Lee, Young-Chul and Moon, Ju-Young; (2020), Introduction to Bionanotechnology, **Springer Nature Singapore** Pte Ltd., 242 pages, ISBN 978-981-15-1293-3
- Meijer, AJ; Lips, M. and Chen, K; (2019), Open Governance: A New Paradigm for Understanding Urban Governance in an Information Age. **Front. Sustain. Cities** 1:3. doi: 10.3389/frsc.2019.00003
- Metcalfe, J. S.; (February 1995), Technology systems and technology policy in an evolutionary framework, **Cambridge Journal of Economics** Vol. 19, No. 1, Special Issue on Technology and Innovation, Published By: Oxford University Press, 25-46.
- Montasari, Reza; Hill, Richard and Parkinson, Simon; (April-June 2020), Digital Forensics: Challenges and Opportunities for Future Studies, University of Huddersfield, Huddersfield, UK, **International Journal of Organizational and Collective Intelligence** Volume 10 • Issue 2, IGI Global.
- Novikov, D.A.; (2016), Cybernetics From Past to Future, **Switzerland, Springer**, 115 PAGES. ISSN 2198-4182
- Ogechukwu, iloanusi; Uche, nnolim and Edwin, umoh; (February 2020), Chaos Theory and Solution Models for National Security, **Nigerian Defence Academy (NDA) International Conference on State and Security Kaduna,** Nigeria, 24th – 26th
- Priyadarshini, Ishaani and Cotton, Chase; (2020), Intelligence in cyberspace: the road to cyber singularity, **JOURNAL OF EXPERIMENTAL & THEORETICAL ARTIFICIAL INTELLIGENCE** https://doi.org/10.1080/0952813X.2020.1784296
- Reding, Dale F.; Álvaro, Martín Blanco; Angelo, De Lucia; Col Laura, A. Regan and Daniel, Bayliss; (2023), Science & Technology Trends 2023-2043 Across the Physical, Biological, and Information Domains VOLUME 2: Analysis, **NATO Science & Technology Organization**.
- Roco, Mihail C.; (2020), Principles of convergence in nature and society and their application: from nanoscale, digits, and logic steps to global progress, **Journal of Nanoparticle Research**, doi.org/10.1007/s11051-020-05032-0, Springer, mroco@nsf.gov, Collection on Nanotechnology Convergence in Africa, National Science Foundation and National Nanotechnology Initiative, Arlington, VA, USA.
- Rotolo, Daniele; Hicks, Diana and Martin, Ben R.; (January 5, 2016), What Is an Emerging Technology? DOI: 10.1016/j.respol.2015.06.006. publication in **"Research Policy"**, 44 pages. Available at: www.sussex.ac.uk/spru/swps2015-06, SPRU – Science Policy Research Unit, University of Sussex.
- Ryan, Mark; (2020), The Future of Transportation: Ethical, Legal, Social and Economic Impacts of Self‐driving Vehicles in the Year 2025, **Springer, Science and Engineering Ethics**, 26:1185–1208 https://doi.org/10.1007/s11948-019-00130-2 University of Twente, Enschede, The Netherlands
- Schmidt, Nikola; (2016) The Birth of Cyber as a National Security Agenda, Ph.D. Thesis, **Faculty of Social Sciences Charles University Prague**, Czech Republic
- Schwab, Klaus; (2016), The Fourth Industrial Revolution, **World Economic Forum**, ISBN-10: 1944835016
- Scott Kevin D., (2018), **Joint Publication 3-12 Cyberspace Operations**, JP3-12.
- Stahl, Bernd Carsten; (June 2011), What Does the Future Hold? A Critical View of Emerging Information and Communication Technologies and Their Social Consequences, Chapter in **IFIP Advances in Information and Communication Technology**, DOI: 10.1007/978-3-642-21364-9_5
- Theiner, Patrick; Schwanholz, Julia & Busch, Andreas; (2017), Parliaments 2.0? Digital Media Use by National Parliaments in the EU, pp:77-96, Managing Democracy in the Digital Age Internet Regulation, **Social Media Use, and Online Civic Engagement**, Springer. DOI 10.1007/978-3-319-61708-4_5
- Tidjon, Lionel and Khomh, Foutse; (2022), Never trust, always verify a roadmap for Trustworthy AI, DGIGL, **Polytechnique Montr´eal Montr´eal**, QC H3C 3A7, Canada,

- TREVOR, JOHNSTON; TROY, D. SMITH and J. LUKE, IRWIN; (2018), ADDITIVE MANUFACTURING IN 2040, Powerful Enabler, Disruptive Threat, Security 2024, **RAND Corporation**
- Yong-Woon, KIM; Sangkeun, YOO; Hyunjeong, LEE and Soonhung, HAN; (2021), "Characterization of Digital Twin", **National AI Research Institute**, https://www.researchgate.net/publication/348356334, www.etri.re.kr.
- Zachary, D. Clopton; (2016), "Territoriality, Technology, and National Security," 83 **University of Chicago Law Review** 45. https://scholarship.law.cornell.edu/facpub/1624/,45-63.