تاریخ دریافت: ۱۴۰۴/۰۱/۱۵ تاریخ پذیرش: ۱۴۰۴/۰۶/۵ صفحه ۱۲۷ تا ۱۷۰

آینده‌نگاری راهبردی امنیت داخلی با تمرکز بر شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات

امیرحسین الهامی[۱]، محمدرضا موحدی صفت[۲]، محمد نورزاده روشن[۳]

چکیده

امنیت داخلی به عنوان ستون فقرات ثبات و رفاه جامعه، همواره محور مهمی در برنامه‌ریزی‌های کلان کشـــوری به شـــمار می‌رود. در عصر حاضر، با توســـعه فناوری‌های پیشرفته به ویژه در حوزه فناوری اطلاعات و ارتباطات، شـــاهد تاثیر گســـترده‌ای بر ابعاد مختلف امنیت داخلی هستیم. این تحقیق به دنبال شـــناخت و تحلیل نقش شـــرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات در تقویت یا تضعیف امنیت داخلی است. توجه به چگونگی تعامل این شرکت‌ها با مولفه‌های امنیتی و تاثیرات ناشـــی از آن‌ها، می‌تواند در شناســـایی فرصت‌ها و چالش‌های پیش روی امنیت داخلی موثر باشـــد. با تحلیل متون علمی داخلی و خارجی و مصاحبه با ۱۲ نفر از نخبگان حوزه امنیت و فناوری اطلاعات و ارتباطات، ۷ بعد توســـعه محصول و توســـعه فناوری، مدیریت و تجزیه و تحلیل داده‌ها، اتصال و زیرساخت ارتباطی، توانایی‌های نظارتی شامل نظارت بر محتوا و نظارت بر عملکرد، مشارکت قانونی و مسئولیت اجتماعی، جهانی شدن و گسترش بازار و همکاری بین‌المللی و داخلی شناســـایی شـــدند. سپس با استفاده از نظر ۳۵ خبره و روش‌های آزمایش و ارزیابی تصمیم‌گیری و تحلیل اثر متقابل، سناریوهای آینده امنیت داخلی شناسایی شدند.

واژگان کلیدی: امنیت داخلی، شـــرکت‌های فناور، فناوری اطلاعات و ارتباطات، آینده‌نگاری راهبردی

---

۱. استادیار پژوهشگاه علوم و معارف دفاع مقدس شهیدحاج قاسم سلیمانی (نویسنده مسئول):
tech.companies.foresight@gmail.com
۲. دانشیار دانشگاه عالی دفاع ملی
۳. دانش آموخته کارشناسی ارشد دانشگاه صنعتی شریف

Strategic Foresight of Internal Security with a Focus on Technology Companies in the Field of Information and Communication Technology

Amir Hussein Elhami[1], Mohammad Reza Movahedi Sefat[2], Mohammad Nourzadeh Roshan[3]

Abstract

Internal security, as the backbone of societal stability and welfare, has always been a key focus in national strategic planning. In today's era, with the development of advanced technologies, particularly in the field of information and communication technology (ICT), we are witnessing significant impacts on various aspects of internal security. This research aims to understand and analyze the role of technology companies in the ICT sector in either strengthening or weakening internal security, as well as to identify future scenarios for internal security. By examining how these companies interact with security components and the resulting impacts, we can effectively identify opportunities and challenges facing internal security. Through the analysis of both domestic and international scholarly texts and interviews with 12 experts in the fields of security and ICT, seven dimensions were identified: product and technology development, data management and analysis, connectivity and communication infrastructure, monitoring capabilities (including content and performance monitoring), legal participation and social responsibility, globalization and market expansion, and international and domestic cooperation. Subsequently, using the insights of 35 experts, along with testing, decision-making methods, and cross-impact analysis, future scenarios of internal security were identified.

Keywords: Internal security, technology companies, information and communication technology, Strategic Foresight

---

1. Assistant Professor, Leutenant General Soleimani Holy Defense Science & Knowledge Resaerch Center, (Writer-in-Charge) tech.companies.foresight@gmail.com
2. Associate Professor, National Defense University
3. M.S Graduate, Sharif Technology University

۱. مقدمه و بیان مساله

رشد سریع فناوری اطلاعات و ارتباطات در دهه‌های اخیر، تاثیر گسترده‌ای بر ابعاد مختلف زندگی اجتماعی، اقتصادی و سیاسی داشته است. در عین حال که این تحولات موجب تسهیل ارتباطات، دسترسی آسان‌تر به اطلاعات و افزایش کیفیت خدمات شده‌اند، چالش‌هایی جدی مانند نقض حریم خصوصی، امکان سوءاستفاده از داده‌های شخصی و تقویت ظرفیت نظارتی دولت‌ها نیز پدیدار شده‌اند. شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات به‌واسطه دسترسی گسترده به داده‌ها، زیرساخت‌های ارتباطی و پلتفرم‌های تعاملی، در جایگاه مهمی قرار گرفته‌اند و می‌توانند به شکل هم‌زمان عاملی برای تقویت امنیت داخلی یا تهدیدی برای آن باشند. از سویی، توانایی این شرکت‌ها در شکل‌دهی به تعاملات و دیدگاه‌های اجتماعی، از طریق پلتفرم‌های ارتباطی و رسانه‌های اجتماعی، می‌تواند فرآیندهای دموکراتیک را تقویت کرده و موجب همگرایی دیدگاه‌ها گردد یا بالعکس بستری برای دامن‌زدن به اختلافات، توزیع گسترده اطلاعات نادرست و حتی سازمان‌دهی اعتراضات و اعمال خشونت‌آمیز فراهم کند. از سوی دیگر، نقش کلیدی شرکت‌های فناور در اقتصاد دیجیتال از طریق ایجاد مراکز جدید قدرت اقتصادی، تغییر ساختار بازار کار و حتی تعمیق شکاف دیجیتال، می‌تواند از زوایای گوناگون بر امنیت داخلی تأثیر بگذارد.

شرکت‌های بزرگ فناوری اطلاعات با گردآوری حجم انبوهی از داده‌های کاربران، توانایی تحلیل و استفاده از این داده‌ها در فرایندهای تصمیم‌سازی و جهت‌دهی بازار را دارند. این شرکت‌ها می‌توانند به ایجاد مراکز جدید قدرت اقتصادی بینجامند که در سطوح گوناگون با سازوکارهای سنتی اقتصاد رقابت کرده و گاه تسلط خود را بر بازار تحمیل کنند. شکل‌گیری این غول‌های فناوری در حوزه اقتصاد دیجیتال نه تنها بر رقابت کسب‌وکارها اثر می‌گذارد، بلکه در صورت عدم شفافیت در سازوکارهای قانون‌گذاری و نظارت، می‌تواند باعث تضعیف اعتماد عمومی رسمی شود. همچنین رویکردهای نوظهور اقتصادی نظیر اقتصاد اشتراک‌گذاری با تغییر الگوهای اشتغال و کارآفرینی، منجر به افزایش نااطمینانی و بی‌ثباتی در برخی حوزه‌های شغلی و به تبع آن، بر امنیت داخلی تاثیرگذار خواهد بود.

در کنار این موارد، تأثیر شرکت‌های فناور بر عرصه‌های فرهنگی و اجتماعی نیز نیازمند توجه است. دسترسی آسان به اینترنت و ابزارهای ارتباطی دیجیتال، هرچند فرصت‌های بی‌شماری برای آموزش، آگاهی‌رسانی و هم‌افزایی دانش فراهم کرده است، اما با شکل‌گیری شکاف دیجیتال نیز همراه بوده است. بخشی از جامعه که به این ابزارها دسترسی کمتری دارد، از فرصت‌های

اقتصادی، آموزشـــی و مشارکت سیاسی محروم می‌ماند. این وضعیت، بالقوه می‌تواند نابرابری‌های موجود را تشـــدید کرده و زمینه‌ساز شـــکل‌گیری تنش‌های اجتماعی گردد. افزون بر آن، سرعت انتقال اطلاعات در شـــبکه‌های اجتماعی، همگام با احتمال انتشار اخبار جعلی، محتوای غیردقیق یا اطلاعات نادرست، چالش جدی دیگری را پیش روی امنیت داخلی قرار می‌دهد. در شرایطی که مرز بین اخبار واقعی و جعلی باریک شده است، احتمال برانگیختن هیجانات منفی یا تفرقه‌افکنی سازمان‌یافته افزایش می‌یابد و فضای عمومی را به شدت قطبی می‌کند.

بـــا توجه به پیچیدگی‌ها و ابعاد متفاوت تأثیرگذاری شـــرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات، دولت‌ها با یک دوراهی بنیادین مواجهند: از یک ســـو، نیاز به تکامل و شـــکوفایی اقتصاد دیجیتال، تولید ثروت و پیشـــرفت‌های فناورانه امری اجتناب‌ناپذیر اســـت و از سوی دیگر، دولت‌ها موظفند با وضع مقررات و سیاســـت‌گذاری‌های دقیق، ابعاد امنیتی جامعه و حقوق شـــهروندان را تضمین کنند. در همین راستا، یکی از ابزارهای کلیدی مدیریت این دوراهی، آینده‌نگاری راهبردی است. آینده‌نگاری راهبردی به دولت‌ها کمک می‌کند تا ضمن شناسایی روندهای نوظهور و تهدیدات محتمـــل، درک عمیق‌تـــری از نقاط قوت و ضعف زیســـت‌بوم دیجیتال به دســـت آورده و به‌صورت پیش‌دستانه برای مقابله با خطرات آتی و بهره‌برداری از فرصت‌های موجود برنامه‌ریزی کنند.

هدف از این پژوهش، آینده‌نگاری راهبردی امنیت داخلی با تمرکز بر شرکت‌های فناور فعال در حوزه فناوری اطلاعات و ارتباطات است. این هدف با پاسخ به چند پرسش اساسی محقق می‌شود: نخســـت، چه متغیرها و مولفه‌هایی روی امنیت داخلی از مســـیر فعالیت شرکت‌های فناور اثرگذار هستند و چه ارتباطی بین آن‌ها وجود دارد؟ دوم، هر کدام از عوامل و مولفه‌های شناسایی شده به چه میزان در آینده امنیت داخلی اثرگذار هستند؟ و سوم، بر اساس رویکرد آینده‌نگاری راهبردی، چه سناریوهای برای آینده امنیت داخلی ناشی از فعالیت شرکت‌های فناور می‌توان متصور بود؟

یافته‌های این تحقیق، بینش‌هایی را برای سیاست‌گذاران، سازمان‌های دولتی و ذینفعان صنعت فراهم می‌کند و آن‌ها را قادر می‌ســـازد تا اقدامات پیشگیرانه، تقویت مشارکت‌ها و تضمین امنیت بلندمدت و شکوفایی اکوسیستم دیجیتال را انجام دهند.

۲. پیشینه‌شناسی تحقیق

پژوهش مســـیبی ملک خیل با بهره‌گیری از روش داده‌بنیاد و فرایند تحلیل شـــبکه‌ای، ابعاد، مولفه‌ها و شـــاخص‌های مرتبط با فناوری اطلاعات و ارتباطات در حوزه امنیت جمهوری اسلامی

ایران شناسایی و تبیین کرده است. در این مقاله، هفت بعد اصلی شامل اقدامات اطلاعاتی شامل مفاهیم اطلاعاتی، دستورکار اطلاعاتی، ساختار سازمان و جامعه اطلاعاتی، منابع اطلاعاتی و ابزارهای اطلاعاتی، بعد اقدامات اجتماعی-سیاسی شامل هویت‌سازی، قدرت نرم، مشارکت‌زدایی، شبکه‌سازی و بحران‌های سیاسی، بعد ظرفیت‌سازی شامل تحقیقات، آموزش و تحصیلات، افراد و مشاغل تاییدشده، مانورهای امنیتی و رونق کسب‌وکار فاوا، بعد هماهنگی همکاری شامل همکاری دو یا چندجانبه بین کشورها، همکاری بین‌سازمانی، همکاری بخش خصوصی و دولتی و همکاری‌های بین‌المللی، بعد ساختارهای اجرایی و پیاده‌سازی شامل راهبردها و سیاست‌های کلان، نقشه راه و طرح‌های پیاده‌سازی، سازمان اجرایی و نهادهای نظارتی و کنترلی، بعد اقدامات فنی شامل گروه‌های پاسخگویی به حوادث رایانه‌ای، استانداردها، گواهی‌نامه‌ها، فناوری اعتبارسنجی، اعطای گواهینامه‌های عمومی و اختصاصی، سازوکارهای تحلیل مخاطرات و سامانه‌های مراقبتی و در نهایت بعد هشداردهی و قوانین و مقررات شامل قوانین کیفری ملی، قوانین و مقررات حقوقی و همچنین قوانین کیفری و حقوقی بین‌المللی شناسایی شده است(مسیبی ملک خیل، ۱۴۰۱).

مطالعه کرمی و همکاران نشان می‌دهد که شبکه‌های اجتماعی مجازی علیرغم داشتن فرصت‌ها و چهره‌ای زیبا، می‌توانند خطرناک‌ترین مسائل و مشکلات را در عرصه امنیت ملی ایجاد کند، تهدیدات پیچیده‌ای که در زیرساخت‌های امنیتی (امنیت اجتماعی، اقتصادی، فرهنگی، سیاسی و زیست محیطی) ایجاد می‌شود. شبکه‌های اجتماعی مجازی در حوزه امنیت اجتماعی: قانون‌گریزی را افزایش می‌دهند، ترویج فرهنگ مصرف‌گرایی، بحران انسجام اجتماعی، اختلال در روابط اجتماعی، فردگرایی، راوج جرائم رایانه و حذف حریم خصوصی، را به دنبال دارند، در حوزه امنیت اقتصادی: ناکارآمدی اقتصاد، نفوذ اقتصادی، ضعف تولید داخلی، اخلال در نظام اقتصادی را تشدید می‌کنند که منجر به رشد زمینه‌های مهاجرت و عدم رضایت از وضعیت کشور می‌شود. در زمینه سیاسی این شبکه‌ها فعالیت گروه‌های معاند سیاسی و گردهمایی آنان را راحت کرده، اطلاعات ناکارآمدی را در حوزه سیاسی و فعالیت دولتی و حکومتی به اذهان عمومی تزریق می‌کند، که همه این‌ها می‌تواند در حوزه سیاسی منجر به بحران‌های حاکمیتی، قومی و مذهبی و ارزشی گردد. در حوزه فرهنگی سرعت بالای گردش اطلاعات در این فضا و شبکه‌ها تضعیف سرمایه‌های اجتماعی را به دنبال دارد و با اشاعه اطلاعات و اخبار متنوع موجب سردرگمی بین کاربران می‌شود، شایعه پراکنی‌های موجود در این شبکه‌ها بی‌اعتمادی جمعی را نسبت به حاکمیت به

وجود می‌آورد و حاکمیت ملی را دچار ضعف می‌نماید. تغییر در تعاملات فرهنگی ایجاد می‌کند و حس مسئولیت‌پذیری را کاهش می‌دهد. در حوزه زیست محیطی با ایجاد بحران مدیریت زیستی و کالایی کردن محیط زیست زمینه را برای تخریب اکوسیستم فراهم می‌نماید(کرمی، ۱۴۰۳).

مقاله ریگز و همکاران[1] آسیب‌پذیری‌های زیرساخت‌های حیاتی مانند سیستم‌های انرژی، حمل‌ونقل و بهداشت را در برابر تهدیدات سایبری بررسی می‌کند. این مقاله اشاره می‌کند که ادغام روزافزون فناوری اطلاعات و ارتباطات در بخش‌هایی مانند انرژی، حمل‌ونقل و بهداشت به بهبود کارایی منجر شده اما در عین حال آسیب‌پذیری این بخش‌ها در برابر حملات سایبری را افزایش می‌دهد. در این پژوهش، مسیرهای رایج حمله سایبری مورد بررسی قرار گرفته است و راهبردهایی برای کاهش صدمات ناشی از حمله سایبری از جمله پروتکل‌های امنیتی قوی‌تر، سیستم‌های نظارتی و سیاست‌هایی برای محافظت از خدمات حیاتی توصیه شده است(ریگز،۲۰۲۳).

مقاله آسوگوا[2] بیان می‌کند که رسانه‌های ارتباطی مبتنی بر اینترنت، از جمله شبکه‌های اجتماعی و پلتفرم‌های ارتباطی مانند فیسبوک، جیمیل، یوتیوب، یاهو میل و توییتر، تاثیر بسزایی بر امنیت ملی دارند. این تشیر به شکل‌های مختلفی نمود پیدا می‌کند و بررسی‌ها نشان می‌دهند که استفاده نامناسب از این رسانه‌ها می‌تواند تهدیدی جدی برای امنیت ملی باشد. از جمله مهم‌ترین عوامل تهدیدکننده می‌توان به استفاده از این بسترها برای رادیکال‌سازی افراد، جذب و آموزش نیروها، تامین مالی فعالیت‌هایی که تهدیدی برای امنیت هستند و انتشار پیام‌های تحریک‌آمیز اشاره کرد که تمامی این موارد می‌توانند به تضعیف امنیت ملی منجر شوند(آسوگوا، ۲۰۲۰).

مطالعات بررسی‌شده نشان می‌دهد که عوامل متعددی بر امنیت داخلی تاثیرگذارند و فناوری اطلاعات و ارتباطات نقش بسزایی در این زمینه دارد. برنامه‌ریزی استراتژیک، سرمایه فرهنگی و بهره‌گیری از تحولات فناوری به‌همراه مدیریت چالش‌های دیجیتالی، از جمله راهکارهایی هستند که می‌توانند به بهبود امنیت داخلی کمک کنند. توجه به این عوامل و تدوین سیاست‌های مناسب، کلید دستیابی به امنیت پایدار و توسعه اقتصادی در عصر دیجیتال است. با بررسی آثار موجود در حیطه موضوعی پژوهش حاضر می‌توان این‌گونه نتیجه‌گیری کرد که غالب آن‌ها یا به بررسی امنیت داخلی و یا به بررسی اهمیت و اثرات اقتصاد دیجیتال و فضای سایبر به‌طور کلی پرداخته‌اند و هیچ یک به‌طور خاص به بحث چالش‌های امنیت داخلی ناشی از فعالیت شرکت‌های

1. Riggs et. al
2. Asogwa

فناور نپرداخته‌اند. پژوهش حاضر با اســـتفاده از روش توصیفی-تحلیلی به بررســـی اثرات فعالیت شرکت‌های فناور روی امنیت داخلی می‌پردازد.

۳. مبانی نظری تحقیق

در این قسمت ابتدا به تعریف امنیت داخلی و بررسی ابعاد مختلف آن پرداخته می‌شود. سپس در بخش دوم به بررسی مولفه‌های اثرگذاری شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات بر امنیت داخلی پرداخته می‌شـــود. در نهایت در بخش ســـوم جهـــت تحکیم موضوع و چارچوب نظری، تعدادی از معتبرترین نظریات حوزه فناوری اطلاعات و ارتباطات و امنیت داخلی در دیدگاه نظریه‌پردازان مشهور غربی بررسی شدند و چارچوب هر کدام بیان شده است.

۱.۳. امنیت داخلی

امنیت ملی را می‌توان از دو دیدگاه ســـلبی و ایجابی تعریف کرد. در نگاه ســـلبی، امنیت ملی به وضعیتی اشـــاره دارد که منافع حیاتی یک بازیگر از ســـوی دیگران تهدید نشود یا در صورت وجود تهدید، توانایی دفع و مدیریت آن وجود داشـــته باشـــد. از دیدگاه ایجابـــی، امنیت ملی به معنای وجود رابطه‌ای معقول بین خواســـته‌ها و داشته‌های بازیگران در یک واحد سیاسی است که منجر به رضایتمندی می‌شود. برخی دیگر امنیت را در نبود تهدید یا توانایی ایجاد شرایط عاری از خطر تعریـــف می‌کنند، در حالی که دیدگاه دیگـــری آن را به عنوان توانمندی بهره‌گیری از فرصت‌ها و تضمین منافع و ارزش‌ها می‌داند. (عبیری و همکاران، ۱۳۹۹) (حبیب‌زاده، ۱۳۹۸).

امنیت داخلی، به عنوان بخشـــی از امنیت ملی، به جنبه‌های داخلی امنیت مانند انتظام ملی، ثبات سیاســـی، رونق اقتصادی و حقوق فردی می‌پردازد. این مفهوم بر وجود انتظام ملی مبتنی بر قواعد حقوقی و قانون اساســـی اســـتوار اســـت. امنیت داخلی علاوه بر یک پدیده اجتماعی، یک احســـاس درونی اســـت که فرد را به آینده متوجه می‌کند و ضامن بقای فرد و جامعه اســـت. ایـــن مفهـــوم با تمامی ابعاد زندگی اجتماعی، از جمله مســـائل فرهنگـــی، اجتماعی، حقوقی و اقتصادی ارتباط تنگاتنگ دارد و در امنیت سیاســـی و مشـــارکت سیاســـی مردم با دولت تجلی می‌یابد(علیزاده، ۱۴۰۰).

با توجه به مطالب مطرح شـــده، امنیت داخلی را می‌توان از ۸ بعد اجتماعی، سیاســـی، فرهنگی، اقتصادی، زیست‌محیطی، دفاعی و امنیتی، سایبری و حقوقی مورد بررسی قرار داد. با این تعریف

از امنیت، در ادامه به بررسی اثر فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات بر ابعاد ۸ گانه امنیت داخلی می‌پردازیم.

۲.۳. اثر شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات بر امنیت داخلی

در این قسمت ابتدا اثر فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات بر امنیت داخلی در ابعاد اقتصادی، سیاسی، فرهنگی، اجتماعی، نظامی و زیست‌محیطی بررسی شده‌اند و در ادامه بر اساس مقالات و پژوهش‌های معتبر، ابعاد و مولفه‌های اثرگذاری شرکت‌های فناور بر امنیت داخلی استخراج شده‌اند.

- **فناوری اطلاعات و ارتباطات و امنیت اجتماعی:** شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات با ارائه خدمات نوآورانه و پلتفرم‌های ایمن، تعاملات اجتماعی و اقتصادی را تسهیل کرده و جوامع آنلاین را تقویت می‌کنند. این شرکت‌ها با بهره‌گیری از فناوری‌هایی مانند رمزگذاری، مکانیسم‌های بازخورد و تایید هویت، از حریم خصوصی و امنیت کاربران محافظت می‌کنند. آن‌ها دسترسی به آموزش، مهارت‌آموزی، و خدمات بهداشتی را از طریق پلتفرم‌های دیجیتال گسترش داده و با ارائه خدمات پزشکی از راه دور و اطلاعات سلامت، تاثیر مثبتی بر بهبود تندرستی و سلامت روان داشته‌اند. با این حال، چالش‌هایی نظیر شکاف دیجیتال، نابرابری اجتماعی، اطلاعات نادرست، و تهدیدات حریم خصوصی نیز از پیامدهای این فناوری‌ها هستند. شرکت‌های فناور با ابتکاراتی مانند ارتقای شمولیت دیجیتال و توسعه فناوری‌های مسئولانه، می‌توانند این چالش‌ها را کاهش دهند. در مجموع، شرکت‌های ICT نقش دوگانه‌ای در تقویت انسجام اجتماعی و ایجاد چالش‌های جدید ایفا می‌کنند که مدیریت اثربخش آن‌ها نیازمند سیاست‌گذاری‌های هوشمندانه است. (شکوری (۱۴۰۰)، طاهری (۱۴۰۱)، الوندی (۱۴۰۰)، پناهی و همکاران (۱۳۹۴)، سعدی‌پور(۱۳۹۲)، آلکان و همکاران (۲۰۱۶)، پیرس و همکاران (۲۰۲۴)، تیموتئو و همکاران (۲۰۲۳)، لیمنیو (۲۰۲۱)، بنونوتی (۲۰۲۳)، میشرا (۲۰۱۵)، بوزال (۲۰۲۲)، کورتنی و همکاران (۲۰۲۲)).
- **فناوری اطلاعات و ارتباطات و امنیت سیاسی:** شرکت‌های فناور نقشی چندوجهی در امنیت سیاسی دارند که هم جنبه‌های مثبت و هم چالش‌هایی را به همراه دارند. آن‌ها از طریق پلتفرم‌های دیجیتال به شکل‌دهی گفتمان عمومی، تسهیل دسترسی به اطلاعات،

افزایش مشـــارکت سیاســـی و تقویت شفافیت و پاســـخ‌گویی دولت‌ها کمک می‌کنند. با این حال، این شـــرکت‌ها با چالش‌هایی مانند انتشـــار اطلاعات نادرست، نگرانی‌های حفظ حریم خصوصی، و سوءاستفاده احتمالی از فناوری‌های نظارتی مواجه هستند. فناوری‌های نوین نظیر رمزگذاری و سیســـتم‌های رای‌گیری الکترونیکی، امنیت انتخابات و فرآیندهای دموکراتیک را تقویت می‌کنند، اما نیازمند قوانین شـــفاف بـــرای حفظ تعادل میان امنیت و حقوق فردی هســـتند. همکاری شـــرکت‌ها با دولت‌ها در زمینه امنیت سایبری و مسائل سیاسی بین‌المللی تأثیرگـــذار اســـت، اما باید با نظـــارت دقیق و رعایت اصول اخلاقی همراه باشـــد. حفظ تعادل میان الزامات امنیتی و حمایت از حقوق فردی برای پایداری سیاســـی و دموکراســـی حیاتی است. (تقوی‌فرد (۱۳۹۵)، علی‌اکبری (۱٤۰۰)، قیاسی (۱٤۰۰)، قیصری و همکاران (۱٤۰۰)، جیـــلاردی (۲۰۲۱)، ســـاواگت (۲۰۱۸)، اکارت (۲۰۲۱)، خانال (۲۰۲٤)، راقاوندرا (۲۰۲۱)، اشتوتزل (۲۰۲۰)).

- **فناوری اطلاعات و ارتباطات و امنیت فرهنگی:** در دنیای مدرن، شـــرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات نقش مهمی در توســـعه فناوری و تغییرات فرهنگی ایفا می‌کنند. این شرکت‌ها با ارائه خدمات و محصولات متنوع، ساختارهای ارتباطی و هنجارهای اجتماعی را دگرگون کرده و زمینه‌ســـاز تبادل فرهنگی بی‌ســـابقه‌ای شـــده‌اند. فناوری‌های دیجیتال، به‌ویـــژه اینترنت و شـــبکه‌های اجتماعی، به ایجاد ارتبـــاط جهانی، تقویت فرهنگ‌های محلی و شـــکل‌گیری هویت‌های فرهنگی جدید کمک کرده‌اند. پلتفرم‌های دیجیتال با دموکراتیزه کـــردن تولیـــد محتوا و ترویج هنر، مصرف‌گرایی فرهنگـــی را افزایش داده‌اند. با این حال، این تغییرات چالش‌هایی نظیر همگن‌ســـازی فرهنگی، تضعیـــف هویت‌های محلی و نگرانی‌های اخلاقی در زمینه اطلاعات نادرست و نظارت بر داده‌ها را نیز به همراه داشته‌اند. علاوه بر این، دیجیتال‌سازی میراث فرهنگی و تأثیر اقتصاد توجه در شکل‌گیری روندهای فرهنگی، اهمیت توازن میان توسعه فناوری و حفاظت از تنوع فرهنگی را بیش از پیش آشکار می‌کند. (اربطانی و همکاران (۱۳۹۱)، امامی (۱٤۰۰)، وندرمیر و همکاران (۲۰۱٦)، گارسیا (۲۰۲۱)).
- **فنـــاوری اطلاعات و ارتباطات و امنیت اقتصادی:** شـــرکت‌های فناور بـــا هدایت نوآوری، افزایش بهره‌وری و ایجاد تحول دیجیتال، نقش مهمی در رشـــد اقتصادی و تاب‌آوری اقتصاد ایفا می‌کنند. این شـــرکت‌ها با ارائه محصولات و خدمات نوآورانه مانند رایانش ابری و هوش مصنوعی، بازارهای جدیدی ایجاد و بازارهای موجود را متحول کرده‌اند. علاوه بر این، آن‌ها با

ایجاد فرصت‌های شغلی مستقیم و غیرمستقیم، به کاهش بیکاری کمک می‌کنند، اما همزمان نیـــاز بـــه مهارت‌آموزی مجدد و مدیریت چالش‌هایی چون نابرابری درآمدی و امنیت شـــغلی را افزایـــش می‌دهند. همچنین، تحول دیجیتال صنایع مختلف را بهبود بخشـــیده و بازارهای دیجیتال جدیدی مانند تجارت الکترونیک و خدمات فین‌تک را توســـعه داده اســـت. از منظر امنیـــت اقتصادی، فناوری‌های اطلاعات و ارتباطات با تنوع‌بخشـــی و افزایش انعطاف‌پذیری، تاب‌آوری اقتصادی را تقویت می‌کنند. با این حال، مســـائلی نظیر رقابت انحصاری، تهدیدات ســـایبری و نابرابری دیجیتال نیازمند مدیریت و همکاری ذی‌نفعان برای دســـتیابی به رشـــد پایدار و منصفانه هســـتند. (احمدی و همکاران (۱۴۰۱)، قاسمی و همکاران (۱۴۰۲)، مغنی و همکاران (۱۳۹۸)، سارانگی و همکاران (۲۰۲۰)، هنری-نیکی و همکاران (۲۰۱۹)، اخریمنکو و همـــکاران (۲۰۲۳)، گیگر (۲۰۱۴)، OECD (۲۰۲۴)، کیریشـــچیوا و همکاران (۲۰۲۱)، فرانکو (۲۰۲۳)، کیراس (۲۰۱۹)).

- **فناوری اطلاعات و ارتباطات و امنیت زیســـت‌محیطی:** شـــرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات به عنوان پیشـــگامان عصر دیجیتال نقش دوگانه‌ای در محیط زیســـت ایفا می‌کنند. از یک ســـو، تولید دســـتگاه‌های الکترونیکی و مراکز داده منجر به مصرف قابل توجه منابع، تولید زباله‌های الکترونیکی و انتشـــار گازهای گلخانه‌ای می‌شـــود. از سوی دیگر، این شـــرکت‌ها با توسعه فناوری‌های هوشمند مانند شبکه‌های هوشمند انرژی، اینترنت اشیا و دیجیتالی‌ســـازی فرآیندها، بهره‌وری انرژی را افزایش داده و اثرات زیست‌محیطی را کاهش می‌دهند. آن‌ها با نوآوری در محاســـبات ســـبز، اســـتفاده از انرژی‌های تجدیدپذیر و طراحی زنجیره‌هـــای تامین پایدار، گام‌های موثری برای به حداقل رســـاندن اثرات زیســـت‌محیطی برداشته‌اند. همچنین، فناوری‌های پایش و مدیریت هوشمند محیط زیست، از کنترل کیفیت هوا و آب گرفته تا کاهش آلودگی و مدیریت پســـماند، به کاهش آســـیب‌های زیست‌محیطی کمک می‌کنند. با همکاری با دولت‌ها و سازمان‌های غیردولتی و ترویج آگاهی زیست‌محیطی، شـــرکت‌های فناور نقش محوری در مقابله با تغییرات آب و هوا و ایجاد آینده‌ای پایدار دارند. (عبـــاس‌زاده و منصوری (۱۳۹۸)، قـــوام و مصطفوی (۱۳۹۷)، ذکی و نجفی (۱۳۹۹)، یزدان پناه درو و همکاران (۱۳۹۷)).
- **فنـــاوری اطلاعات و ارتباطات و امنیت دفاعی و امنیتی:** شـــرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات نقشـــی کلیدی در توســـعه زیرســـاخت‌ها و فناوری‌های مورد نیاز برای

عملیات نظامی مدرن ایفا می‌کنند. این شرکت‌ها با ارائه سخت‌افزارها و نرم‌افزارهای پیشرفته، ستون فقرات سیستم‌های فرماندهی و ارتباطات نظامی را شکل داده و امنیت سایبری و جنگ شـــبکه‌محور را تقویت می‌کنند. فناوری‌های نظارتی مانند تصاویر ماهواره‌ای و سیســـتم‌های بدون سرنشـــین، روش‌هـــای جمع‌آوری اطلاعات و آگاهی از موقعیـــت را بهبود داده و هوش مصنوعی در تحلیل تهدیدات و تصمیم‌گیری‌ها، دقت و سرعت عملیات نظامی را افزایش داده اســـت. ابزارهایی نظیر شبیه‌ســـازهای واقعیت مجازی و افزوده، مهارت‌های نیروهای نظامی را ارتقا داده و مدیریت پیشـــرفته لجســـتیک، کارایی زنجیره تأمین را تضمین می‌کند. در عین حال، توســـعه فناوری‌های با کاربرد دوگانه و قابلیت‌های سایبری تهاجمی، بحث‌های اخلاقی و ضرورت وضع قوانین بین‌المللی برای کنترل اســـتفاده از این ابزارها را به همراه داشته است. (لنگلیت و همکاران (۲۰۲۱)، احمد و همکاران (۲۰۲۱)، شولز (۲۰۲۰)،هالدورای و همکاران (۲۰۲٤)، لاماس و همکاران (۲۰۲٤)، باســـیل (۲۰۱۲)، فرایدی (۲۰۲٤)، گوتیری (۲۰۱٤)، نوری و همکاران (۱۳۹۸)، اردکانی و همکاران (۱۳۹۵)، هلیلی و همکاران (۱۳۹٤)).

- **فناوری اطلاعات و ارتباطات و امنیت ســـایبری:** شـــرکت‌های فناور نقش حیاتی در امنیت ســـایبری دارند و از طریق توسعه و پیاده‌سازی راه‌حل‌های امنیتی، حفاظت از زیرساخت‌های دیجیتال، و مقابله با تهدیدات سایبری، از دارایی‌های دیجیتال حفاظت می‌کنند. این شرکت‌ها ابزارهایی مانند سیســـتم‌های تشخیص نفوذ، رمزنگاری داده‌ها، و احراز هویت چندعاملی ارائه داده و از هوش مصنوعی برای شناســـایی و پیشـــگیری از حملات سایبری استفاده می‌کنند. همچنین با جمع‌آوری و تحلیل اطلاعات تهدید و همکاری با سازمان‌های بین‌المللی، به بهبود آمادگی در برابر تهدیدات کمک می‌کنند. آموزش امنیت ســـایبری، ترویج شـــیوه‌های توسعه امن، و ارائه خدمات ابری امن نیز از اقدامات مهم آن‌ها است. این شرکت‌ها با افزایش شفافیت و جلب اعتماد عمومی، محیطی امن و انعطاف‌پذیر برای کاربران فراهم می‌آورند. (بوینز (۲۰۲۲)، پائولی (۲۰۱۸)، کولیچیا (۲۰۱۸)، گوکایا (۲۰۲٤)، طاهردوســـت (۲۰۲٤)، حامی (۲۰۲٤)، جوزف (۲۰۲۳)، حسن (۲۰۲۳)).
- **فناوری اطلاعات و ارتباطات و امنیت حقوقی:** شـــرکت‌های فناور نقش مهم و چندوجهی در ارتقـــای امنیـــت حقوقی و قضایی دارند. این نقش شـــامل توســـعه راه‌حل‌های فنی مانند سیســـتم‌های مدیریت پرونده و ابزارهای تحقیقاتی، فناوری‌های دادگاه برای افزایش کارایی و دسترسی به دادرسی و تسهیل حل‌وفصل آنلاین اختلافات از طریق پلتفرم‌های نوآورانه است.

آن‌ها همچنین دسترسی به اطلاعات حقوقی را با ایجاد پایگاه‌های داده و ابزارهای آنلاین بهبود می‌بخشند و با همکاری متخصصان حقوقی و نهادهای نظارتی، راه‌حل‌هایی منطبق با قوانین و مقررات ارائه می‌کنند. علاوه بر این، مسائل حقوقی مرتبط با فناوری مانند مالکیت فکری، حفاظت از داده‌ها و سیاست‌گذاری را مدیریت می‌کنند و با پرداختن به ملاحظات اخلاقی نظیر سوگیری در الگوریتم‌ها و تضمین شفافیت، به ارتقای عدالت و انصاف کمک می‌کنند. (اولنیکین (۲۰۲٤)، خانال (۲۰۲٤)) (سند امنیت قضایی، ۱۳۹۹).

فناوری اطلاعات و ارتباطات به عنوان پایه و اساس تمدن مدرن در عصر دیجیتال ظاهر شده است و اقتصاد، سیاست، فرهنگ و امنیت داخلی را به شدت تحت تاثیر قرار داده است. این بخش به بررسی اثرات چندجانبه فناوری اطلاعات و ارتباطات بر امنیت داخلی می‌پردازد. نظریه‌هایی مانند جبر تکنولوژیک، نظریه سیستم‌های اجتماعی، جامعه نظارت و جامعه ریسک برای تحلیل این اثرات به کار گرفته شده‌اند.

کتاب «موج سوم»[1] آلوین تافلر[2] تغییرات اجتماعی را در سه موج توضیح می‌دهد: انقلاب کشاورزی، انقلاب صنعتی و جامعه فراصنعتی. تافلر پیش‌بینی کرد که فناوری اطلاعات باعث تحول اقتصاد و جوامع، تمرکززدایی، پایان استانداردسازی، محو مرزهای کار و زندگی خانگی، دموکراتیزه شدن دانش و نیاز به سازگاری بیشتر با تغییرات سریع خواهد شد. او همچنین چالش‌های زیست‌محیطی و اجتماعی جدیدی را به همراه این تغییرات پیش‌بینی کرد.

جبر تکنولوژیک، مفهومی که توسط اسمیت و مارکس (۱۹۹٤)[3] مطرح شده، به عنوان چارچوبی برای تحلیل اثرات فناوری بر تغییرات اجتماعی و سازگاری سازمانی عمل می‌کند. این نظریه بیان می‌کند که توسعه فناوری نیروی اصلی در تغییر اجتماعی است و در حوزه امنیت داخلی نشان می‌دهد که پیشرفت‌های فناوری اطلاعات و ارتباطات چگونه قابلیت‌ها و استراتژی‌های امنیتی را ارتقا داده‌اند. این اثرات در سه بخش اصلی اثر فناوری بر تغییر اجتماعی، اثر فناوری بر سازگاری سازمانی و اثر فناوری در حوزه امنیت داخلی بررسی می‌شوند. در نهایت، جبر تکنولوژیک تاکید دارد که فناوری نیروی فعالی در شکل‌دهی و تغییر ساختارهای اجتماعی، سازمانی و دولتی است.

1.The Third Wave
2. Alvin Toffler
3. Smith, M. R., & Marx, L. (1994)

نظریه سیستم‌های اجتماعی[1] تریست و بامفورث[2] (۱۹۵۱) که به بررسی تعامل سیستم‌های اجتماعی و فنی می‌پردازد، تاکید دارد استراتژی‌های امنیتی باید هم قابلیت‌های فنی و هم پویایی‌های اجتماعی را در نظر بگیرند. این چارچوب تحلیل تعامل عوامل انسانی و سیاست‌های نهادی با سیستم‌های فناوری در امنیت داخلی را فراهم می‌کند. نظریه جامعه نظارت[3] لیون[4] (۲۰۰۱) به بررسی پیامدهای اجتماعی نظارت گسترده، مانند مسائل حریم خصوصی و قدرت، می‌پردازد. این نظریه نشان می‌دهد که فناوری‌های نظارتی، در حالی که امنیت را افزایش می‌دهند، نگرانی‌هایی در مورد حریم خصوصی و سوء استفاده‌های احتمالی ایجاد می‌کنند. نظریه جامعه ریسک[5] بک[6] (۱۹۹۲) بر نیاز به ارزیابی مجدد استراتژی‌های مدیریت ریسک در مواجهه با آسیب‌پذیری‌ها و چالش‌های امنیتی جدید تاکید دارد.

تاریخچه تغییرات فناوری اطلاعات و ارتباطات در امنیت داخلی از سیستم‌های محاسباتی اولیه و اینترنت آغاز شده و با توسعه پایگاه‌های داده پیچیده و کانال‌های ارتباطی دیجیتال، امنیت سایبری به‌عنوان یک نگرانی حیاتی مطرح شده است. افزایش تهدیدات سایبری باعث تغییر رویکردهای امنیتی از اقدامات واکنشی به استراتژی‌های پیشگیرانه شده است. مفهوم جامعه شبکه‌ای[7] کاستلز[8] (۱۹۹۶) نشان می‌دهد که با ادغام سیستم‌های دیجیتالی، امنیت دیگر محدود به مرزهای فیزیکی نیست و به حفاظت از شبکه‌های دیجیتال گسترده گسترش یافته است. استفاده از تجزیه و تحلیل داده‌های بزرگ توسط آژانس‌های امنیتی برای پیش‌بینی فعالیت‌های مجرمانه و تخصیص منابع به تحولات بزرگی منجر شده است. این امر، اگرچه موثر است، مسائل جدیدی در زمینه حریم خصوصی و استفاده اخلاقی از داده‌ها ایجاد کرده است. فناوری‌های نظارتی مانند دوربین مداربسته و سیستم‌های بیومتریک قابلیت‌های نظارتی را به‌طرز چشمگیری افزایش داده‌اند، اما نگرانی‌های زیادی در مورد نقض حریم خصوصی و حقوق فردی به وجود آورده‌اند.

---

1. Sociotechnical Systems
2. Trist and Bamforth
3. Surveillance Society
4. Lyon
5. Risk society
6. Beck
7. Network society
8. Castells

پارادوکس حریم خصوصی-تکنولوژی بارنز[1] (۲۰۰۶) به رابطه متناقض بین تقویت اقدامات امنیتی و کاهش حریم خصوصی اشـــاره دارد. این امر نشـــان می‌دهد که استفاده از فناوری‌های پیشرفته امنیتی می‌تواند به تجاوز به حریم خصوصی منجر شود، اگرچه برای حفاظت ضروری است.

نظریه اجتماعی فنی[2] در طراحی امنیت تاکید دارد که طراحی سیستم‌های امنیتی باید علاوه بر کارایی فناوری، تعامل آن با اپراتورهای انســـانی و هنجارهای اجتماعی را نیز در نظر بگیرد. عوامل انســـانی مانند آگاهی کارکنان و پایبندی به پروتکل‌های امنیتی بســـیار مهم هستند. این رویکرد نیازمند ســـرمایه‌گذاری در آموزش، توسعه منابع انسانی و تغییر فرهنگ سازمانی به سمت امنیت به‌عنوان یک مســـئولیت جمعی است. در نهایت، توسعه سیستم‌های امنیتی اجتماعی فنی شامل طراحی‌های یکپارچه‌تر و کاربرمحور خواهد بود که فناوری و عناصر انسانی را به طور مکمل به کار می‌گیرند تا حفاظت قوی‌تر و موثرتر ایجاد کنند. درک عمومی و پذیرش نظارت نیز نقشـــی مهم در شکل‌گیری سیاست‌های نظارتی دارد.

بنابراین، از اصول جبر فناوری و نظریه سیســـتم‌های اجتماعی فنی گرفته تا تفاوت‌های ظریف پارادوکـــس فناوری حریـــم خصوصی و جامعه نظارت، این تحلیل بر یک حقیقت اساســـی تاکید می‌کند: قلمرو امنیت داخلی در عصر دیجیتال پیچیده و چندوجهی اســـت. پیشرفت‌های فناوری اطلاعات و ارتباطات، استراتژی‌های امنیتی را متحول کرده و قابلیت‌ها را افزایش داده و همچنین چالش‌های بی‌سابقه‌ای را به وجود آورده است. نتیجه کلی رابطه شرکت‌های فناور و امنیت داخلی در ایـــن بخش را می‌توان به‌صورت توســـعه فناوری، مدیریت داده‌هـــا و حریم خصوصی، اقدامات امنیت سایبری، قابلیت‌های نظارتی، انطباق با مقررات، اعتماد و ادراک عمومی و همکاری دولتی خلاصه کرد.

۴. روش‌شناسی تحقیق

از نگاه وندل بل، هدف در آینده‌نگاری کشف یا ابداع، وارسی و ارزیابی و پیشنهاد آینده‌هایی که می‌توانند واقع شوند (آینده‌های ممکن)، یا احتمال واقع شدن آن‌ها وجود دارد (آینده‌های محتمل) یا باید واقع شـــوند (آینده‌های مطلوب). آینده‌نگاری راهبردی یکی از انواع آینده‌نگاری اســـت که برای طراحی آینده مطلوب اســـتفاده می‌شـــود. در واقع آینده‌نگاری راهبردی فرآیندی است برای

1. Barnes
2. Sociotechnical system

افزایش توانایی‌های فردی و سازمانی به‌منظور درک فرصت‌ها و تهدیدهای در حال ظهور، عناصر وابسته به مسیر، پیش‌ران‌ها، تغییر در محرک‌ها، منابع، علت و معلول‌ها که با تصمیمات بدیل مرتبط هستند. تصمیمات بدیلی که فضای مسیر آینده‌های ممکن، باورپذیر، محتمل و مرجح را شکل می‌دهند تا تصمیمات برای دستیابی به اهداف بلندمدت بتواند با آگاهی و آمادگی بهتر اتخاذ شوند(علیزاده، ۱۴۰۰).

شناخت موضوع و تصمیم اصلی، شناسایی عوامل کلیدی، شناسایی نیروهای پیشران کلیدی، طبقه‌بندی بر اساس اهمیت و عدم‌قطعیت، انتخاب منطق سناریوها، تدوین سناریوها، تحلیل پیامدها و نتایج هر سناریو و انتخاب نشانگرهای راهبردی، گام‌های هشتگانه در یک فرآیند سناریونویسی هستند که در این تحقیق بدان پرداخته شده‌اند. فرآیند آینده‌نگاری راهبردی به صورت زیر است:

۱. تحلیل محیطی: هدف این گام دستیابی به تصویری دقیق از وضع موجود، همراه با شناسایی و تحلیل روندها و کشف عدم قطعیت‌ها و خلق یا دستیابی به ایده‌ها و تصویرهایی از جهان آینده است.
۲. سناریونگاری: هدف این گام کشف و شناسایی آینده‌های ممکن، محتمل و مرجح و بیان آن‌ها در قالب سناریو است.
۳. چشم‌اندازسازی
۴. راهبردپردازی

گام اول شامل دو مرحله است:

۱. شناسایی عوامل و روندها: در این پژوهش با بهره‌گیری از مطالعات گذشته و همچنین جمع‌آوری میدانی اطلاعات از نخبگان این حوزه انجام گرفته است.
۲. تحلیل عوامل وروندهای شناسایی شده به منظور کشف رابطه بین آن‌ها و عدم قطعیت‌ها: در این پژوهش با استفاده از روش تحلیل اثر متقابل روابط بین عوامل و مولفه‌ها بررسی شده است. تحلیل اثر متقابل، روشی برای تشخیص روابط متقابل است. به طوری که تأثیر هر روند بر روندهای دیگر درجه‌بندی می‌شود. به عبارت دیگر تحلیل اثر متقابل یک روش نیمه کمی است که در آن، به جای روابط علت-معلولی ساده، روابط متقابل بین خرده‌سیستم‌های مختلف در ماتریس تحلیل می‌شود. تحلیل اثر متقابل، به عنوان ابزار تحقیقات در مورد آینده، نقش شاخص یک متغیر را در ارتباط با سایر متغیرهای درون یک سیستم آشکار ساخته و آن دسته از متغیرهایی را شناسایی می‌کند که نقش مهم و معناداری در توسعه سیستم در آینده

ایفا می‌کنند. اطلاعاتی که این روش تامین می‌کند تصویری اســت از اثر متقابل بین روندها و متغیرها. با همان درجه اهمیت، تصویری است از این‌که چه متغیری وابسته و چه متغیری مســتقل است، چه متغیری پیشران و چه متغیری توسط متیغرهای دیگر پیش‌برده می‌شود.

تحلیل اثر متقابل در ٤ مرحله و به صورت زیر انجام می‌شود:

۱. تهیه لیست پیش‌ران‌ها یا متغیرها به‌عنوان روندهایی با جهت‌های معین

۲. تهیه ماتریس قطری n در n به تعداد پیشران‌ها (روندها)

۳. قضاوت در مورد این‌که روند A تا چه حد بر روند B تاثیر خواهد داشت.

۴. جمــع بنــدی نتایج: جمع هر ردیف میزان قدرت پیش‌برندگی متغیر را نشــان می‌دهد؛ این بدان معناست که این متغیر تا چه اندازه متغیرهای دیگر را تحت تأثیر قرار می‌دهد. جمع هر ستون، سطح وابستگی هر متغیر را نشان می‌دهد.

برای گام دوم، در میان انواع روش‌های ســناریونگاری، در این پژوهش از روش ۷ مرحله‌ای پیتر شوارتز استفاده شده است. این ۷ مرحله شامل موارد ذیل است (دهکردی و دانش، ۱٤۰۰):

۱. تشخیص و شناسایی موضوع یا تصمیم اصلی

۲. شناسایی عوامل و نیروهای کلیدی و موثر بر موضوع

۳. تهیه فهرست نیروهای پیشران تغییرات

۴. رتبه‌بندی عوامل و نیروهای پیشران بر اساس درجه اثرگذاری و اثرپذیری

۵. انتخاب منطق حاکم بر سناریوها: پس از انتخاب مجموعه‌ای از عوامل موثر، تدوین سناریوها با تعریف وضعیت‌های مختلف آینده هر عامل موثر انجام می‌شود.

۶. پربار کردن محتوای سناریوها

۷. شناسایی و انتخاب شاخص‌های راهنما: شاخص‌های راهنما همگام با حرکت به سوی آینده پایش می‌شوند تا علائم هشداردهنده در مورد این‌که کدام سناریو در حال بروز است دریافت شود. به همین جهت شناسایی شاخص‌ها، برنامه‌ریزان و سیاست‌گذاران را متوجه این مساله می‌کند که در حال حرکت به ســمت کدام ســناریو هســتیم و این هشدار را می‌دهد که اگر بخواهیم به ســمت ســناریو مطلوب حرکت نماییم باید کدام شاخص‌ها را تبدیل به شاخص مطلوب نماییم.

بر این اســاس آینده‌نگاری راهبردی امنیت داخلی با تاکید بر شــرکت‌های فناور فعال در حوزه فناوری اطلاعات و ارتباطات دارای سه وجه وجودی و مفهومی یعنی:

- استخراج عوامل و نیروهای پیشران کلیدی تبیین‌کننده امنیت بر اساس اهمیت و عدم‌قطعیت‌ها
- شناسایی و ارزیابی تاثیرات متقابل عوامل تبیین‌کننده
- آینده‌نگاری و تدوین سناریوهای باورکردنی حوزه امنیت

بدین ترتیب تمرکز روش‌شناسی پژوهش بر عملیاتی نمودن مفاهیم سه‌گانه فوق استوار می‌باشد. در این راستا به‌منظور تحقق اهداف تحقیق سه فرآیند سلسله مراتبی شامل تحلیل ورودی‌ها، آینده‌نگاری و خروجی که مبتنی بر گزارش سناریوها است مورد تاکید قرار گرفته شده است.

به‌منظور شناسایی ابعاد و مولفه‌های اثرگذار بر امنیت داخلی از طریق فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات، با شناسایی هدفمند خبرگان، آرای ۱۲ کارشناس خبره در حوزه‌های متنوع مدیریتی، امنیتی و فناوری اعم از افراد دانشگاهی و ستادی مطلع به مسائل و چالش‌های امنیت داخلی و فناوری اطلاعات و ارتباطات جمع‌آوری گردید. سپس با بهره‌مندی از نظرات ۳۵ خبره، پیشران‌ها و سناریوهای آینده امنیت داخلی بررسی شدند.

۵. تجزیه و تحلیل داده‌ها و یافته‌های تحقیق

در این بخش از تحقیق، با استفاده از اسناد علمی و گزارش‌های سازمان‌های بین‌المللی، به تبیین و تشریح ابعاد و مولفه‌های موثر بر امنیت داخلی از طریق فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات پرداخته می‌شود. این ابعاد عبارت‌اند از:

۱. بعد توسعه محصول و توسعه فناوری شامل مولفه‌های تسهیل گفتمان عمومی و مشارکت مدنی، بهبود دسترسی به خدمات، افزایش تبادلات و تقابل فرهنگی، تسهیل دسترسی به اطلاعات، کاهش شکاف دیجیتال، تغییر در سبک زندگی، توسعه محصولات هوشمند مبتنی بر هوش مصنوعی و یادگیری ماشینی

۲. بعد مولفه‌های مدیریت و تجزیه و تحلیل داده‌ها شامل مولفه‌های تغییر افکار، رفتار و انتظارات کاربران، اطمینان از یکپارچگی داده‌ها، شناسایی و ریشه‌یابی مسائل اجتماعی و فرهنگی، جلوگیری از نشت داده‌ها، بهبود حریم خصوصی داده‌ها، بهبود مدیریت منابع شامل منابع انسانی، مالی، زیست‌محیطی و انرژی

۳. بعد اتصال و زیرساخت ارتباطی شامل مولفه‌های ایجاد زیرساخت قابل اعتماد، اطمینان از ارتباط امن، کاهش آلودگی‌های زیست‌محیطی و مصرف انرژی در مراکز داده، افزایش

دسترس‌پذیری، افزایش ظرفیت اتصال، افزایش ظرفیت پردازش (محاسبات ابری)، اطمینان از کیفیت ارتباطات

۴. بعد توانایی‌های نظارتی شـــامل مولفه‌های نظارت بر محتوا و نظارت بر عملکرد شامل کنترل اخبار جعلی و اطلاعات نادرست، نظارت و حذف محتوای مضر، توسعه سیستم‌های تشخیص نفوذ، شـــفافیت در کارایی نظام حکمرانی، افزیـــش آزادی اطلاعات، کاهش اعتماد عمومی، افزیش آزادی بیان

۵. بعد مشارکت قانونی و مسئولیت اجتماعی شامل مولفه‌های به روزرسانی قوانین برای کاهش عـــدم قطعیت حقوقـــی و اختلافات، حمایت مادی و معنوی از پروژه‌های مربوط به مســـائل زیســـت‌محیطی و عدالت اجتماعی، تســـهیل دسترســـی به قوانین و افزایش آگاهی حقوقی، لابی‌گری و حمایت/عدم حمایت از لوایح قانونی، کاهش ردپای کربن

۶. بعد جهانی شـــدن و گســـترش بازار شامل مولفه‌های شفافیت تبادلات، افزایش تاب‌آوری اقتصاد، کاهش نابرابری، اخلال در بازارهای سنتی، افزایش رشد اقتصادی، تغییر نرخ بیکاری، کاهش نرخ فقر

۷. بعد همکاری بین‌المللی و داخلی شـــامل مولفه‌های همکاری با دولت جهت جذب ســـرمایه، اشـــتراک‌گذاری دانش و تجربیات، همکاری با شـــرکت‌های بین‌المللی جهت جذب سرمایه و انتقـــال دانـــش و تکنولوژی، نگرانی‌های حریـــم خصوصی و خطرات حفاظـــت از داده‌ها، اشـــتراک‌گذاری داده‌های کاربران شـــامل داده‌های هویتی و رفتاری از مســـیرهای قانونی و مسیرهای فراقانونی با دولت

بر اســـاس نظرات خبرگان و تحلیل‌های انجام شـــده، می‌توان برآورد توزین شده هر یک از این عوامل را در زمینه امنیت داخلی اثرپذیر از شـــرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات انجام داد. همان‌طور که در جدول (۴-۱) مشاهده می‌شود، در سه روش RS ،ROCو RR، وزن متفاوتی برای هر عامل محاســـبه شـــده است که نشان‌دهنده تنوع تاثیرگذاری هر یک از این ابعاد بر امنیت داخلی است.

- مرکز ثقل رتبه بندی ترتیبی (ROC) : در این روش مبنای تخصیص اوزان تعداد گزینه‌ها و رتبه مستقیم تخصیصی به هر یک از شاخص‌ها است. در این تابع n تعداد گزینه‌ها و r_j نیز رتبه مستقیم هر شاخص محسوب می‌شود. در این مورد اوزان از طریق تابع زیر محاسبه می‌شوند:

$$ROC = {}^{1}/_{n} \sum_{j=1}^{n} {}^{1}/_{r_j}$$

• جمـــع رتبه‌ای (RS): دراین روش روال ترتیب محاســـبه وزن‌ها به صورت بی‌مقیاس‌ســـازی جداگانه رتبه‌ها و تقسیم آن برمجموع رتبه‌ها از طریق تابع زیر است:

$$R_S = ۲(n + ۱ - r_j)/n(n + ۱)$$

• عکس‌پذیری رتبه‌ای (RR): این روش عکس رتبه‌های بی‌مقیاس شده را با تقسیم نمودن آن بر مجموع عکس رتبه‌ها و از طریق تابع زیر به دست می‌دهد.

$$R_R = \frac{۱/_i}{\sum_{j=۱}^{n} ۱/_j}$$

جدول٤-١: برآورد توزین شده معیارهای اثرگذار فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات بر امنیت داخلی

معیارها	ROC	RS	RR
بعد توسعه محصول و توسعه فناوری شامل مولفه‌های تسهیل گفتمان عمومی و مشارکت مدنی، بهبود دسترسی به خدمات، افزایش تبادلات و تقابل فرهنگی، تسهیل دسترسی به اطلاعات، کاهش شکاف دیجیتال، تغییر در سبک زندگی، توسعه محصولات هوشمند مبتنی بر هوش مصنوعی و یادگیری ماشینی	۰,۲۷۶	۰,۳۷۸	۰,۲۴۹
بعد مدیریت و تجزیه و تحلیل داده‌ها شامل مولفه‌های تغییر افکار، رفتار و انتظارات کاربران، اطمینان از یکپارچگی داده‌ها، شناسایی و ریشه‌یابی مسائل اجتماعی و فرهنگی، جلوگیری از نشت داده‌ها، بهبود حریم خصوصی داده‌ها، بهبود مدیریت منابع شامل منابع انسانی، مالی، زیست‌محیطی و انرژی	۰,۲۶۷	۰,۳۵۰	۰,۳۵۲
بعد اتصال و زیرساخت ارتباطی شامل مولفه‌های ایجاد زیرساخت قابل اعتماد، اطمینان از ارتباط امن، کاهش آلودگی‌های زیست‌محیطی و مصرف انرژی در مراکز داده، افزایش دسترس‌پذیری، افزایش ظرفیت اتصال، افزایش ظرفیت پردازش (محاسبات ابری)، اطمینان از کیفیت ارتباطات	۰,۱۰۷	۰,۲۰۲	۰,۰۷۶

بعد توانایی‌های نظارتی شامل نظارت بر محتوا و نظارت بر عملکرد شامل مولفه‌های کنترل اخبار جعلی و اطلاعات نادرست، نظارت و حذف محتوای مضر، توسعه سیستم‌های تشخیص نفوذ، شفافیت در کارایی نظام حکمرانی، افزیش آزادی اطلاعات، کاهش اعتماد عمومی، افزیش آزادی بیان	۰,۱۶۳	۰,۲۶۲	۰,۱۷۱
بعد مشارکت قانونی و مسئولیت اجتماعی شامل مولفه‌های به روزرسانی قوانین برای کاهش عدم قطعیت حقوقی و اختلافات، حمایت مادی و معنوی از پروژه‌های مربوط به مسائل زیست‌محیطی و عدالت اجتماعی، تسهیل دسترسی به قوانین و افزایش آگاهی حقوقی، لابی‌گری و حمایت/عدم حمایت از لوایح قانونی، کاهش ردپای کربن	۰,۰۱۱	۰,۱۳۸	۰,۰۱۸
بعد جهانی شدن و گسترش بازار شامل مولفه‌های شفافیت تبادلات، افزایش تاب‌آوری اقتصاد، کاهش نابرابری، اخلال در بازارهای سنتی، افزایش رشد اقتصادی، تغییر نرخ بیکاری، کاهش نرخ فقر	۰,۰۹۱	۰,۲۸۰	۰,۰۷۹
بعد همکاری بین‌المللی و داخلی شامل مولفه‌های همکاری با دولت جهت جذب سرمایه، اشتراک‌گذاری دانش و تجربیات، همکاری با شرکت‌های بین‌المللی جهت جذب سرمایه و انتقال دانش و تکنولوژی، نگرانی‌های حریم خصوصی و خطرات حفاظت از داده‌ها، اشتراک‌گذاری داده‌های کاربران شامل داده‌های هویتی و رفتاری از مسیرهای قانونی و مسیرهای فراقانونی با دولت	۰,۰۸۴	۰,۲۵۶	۰,۰۵۶

بررسی مقادیر نشان‌دهنده تفاوت‌هایی در وزن‌دهی معیارها در بین ابعاد مختلف است. به عنوان مثال، وزن‌های محاسبه شده با روش ROC نشان می‌دهد که بعد توسعه محصول و فناوری و مدیریت و تجزیه و تحلیل داده‌هابالاترین اهمیت را دارند (به ترتیب با مقادیر ۰,۲۷۶ و ۰,۲۶۷). این مقادیر نشان‌دهنده نقش کلیدی این ابعاد در پیشرفت توانمندی‌های فناوری اطلاعات و ارتباطات است که به‌طور مستقیم بـــر عواملی همچون گفتمان عمومی، یکپارچگی داده‌ها و تبادلات فرهنگی تاثیر می‌گذارند. در مقابل، بعد مشـــارکت قانونی و مسئولیت اجتماعی وزن کمتری در ROC (۰,۰۱۱) دارد که نشان می‌دهد با وجود اهمیت این بعد، تاثیر آن بر امنیت داخلی کمی کمتر از جنبه‌های فناوری و مدیریت داده‌هاست.

همچنین، در بررسی مقادیر روش‌های RS و RR، تغییرات جزئی در اولویت‌بندی مشاهده می‌شود. به

عنوان نمونه، بعد مشارکت قانونی و مسئولیت اجتماعی در روش RS دارای مقدار بالاتری است (۰,۱۳۸) که به اهمیت روزافزون آن در کاهش عدم قطعیت‌های حقوقی و ارتقای عدالت زیست‌محیطی اشاره دارد. به همین ترتیب، بعد جهانی شدن و گسترش بازار نیز دارای امتیاز بالا در روش RS (۰,۲۸۰) است که نشان‌دهنده چالش‌ها و فرصت‌های جهانی شدن از نظر تاب‌آوری اقتصادی و کاهش نابرابری است. این مقایسه دقیق بین روش‌ها نشان می‌دهد که چگونه دیدگاه‌های مختلف در وزن‌دهی می‌تواند اولویت‌های هر بعد را در نقش فناوری اطلاعات و ارتباطات در امنیت داخلی تغییر دهد و پیچیدگی و ارتباط متقابل معیارهای ارزیابی شده را برجسته می‌کند.

۳.۵. سنجش و ارزیابی متغیرهای تاثیرگذار و تاثیرپذیر امنیت داخلی از طریق فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات

پس از شناسایی هفت عامل اصلی تبیین‌کننده امنیت داخلی اثرپذیر از فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات، این عوامل باید با هدف شناسایی پیشران‌ها و عدم قطعیت‌های کلیدی بر اساس میزان اثرگذاری و اثرپذیری طبقه‌بندی شوند. در این راستا، از ماتریس شبکه‌ای عدم قطعیت–اثر استفاده شده است تا میزان اهمیت هر یک از عدم قطعیت‌ها شناسایی شود. این فرآیند با بهره‌گیری از نظرات ۳۵ نفر از خبرگان و با استفاده از دو روش دیمتل[1] و تحلیل ساختاری صورت گرفته است.

۱.۳.۵. روش مبتنی بر خطا و ارزشیابی آزمایشگاهی (DEMATEL)

در این بخش، از روش «آزمایش و ارزیابی تصمیم‌گیری» (DEMATEL) برای بررسی هفت عامل کلیدی که بر فرآیند پیش‌بینی راهبردی تاثیرگذارند، استفاده شده است. این روش با شناسایی تاثیرات مستقیم و غیرمستقیم میان عوامل مختلف، به ما امکان می‌دهد تا چالش‌های آینده را پیش‌بینی کنیم، فرصت‌ها را شناسایی کرده و راهبردهای بلندمدت خود را به دقت تنظیم کنیم. عوامل بررسی‌شده شامل توسعه محصول و نوآوری فناورانه، مدیریت داده‌ها و تحلیل‌ها، زیرساخت‌های ارتباطی، توانایی‌های نظارتی، مشارکت قانونی و مسئولیت اجتماعی، جهانی شدن و گسترش بازار و همکاری بین‌المللی و داخلی هستند.

نتایج تحلیل DEMATEL مشخص می‌کند که کدام عوامل به‌عنوان نیروهای پیشران عمل می‌کنند

1. (Decision-Making Trial and Evaluation Laboratory)DEMATEL

و کدام بیشتر تحت تاثیر عوامل دیگر قرار دارند. این تحلیل به کمک مجموع تاثیرگذاری (R_i)، مجموع تاثیرپذیری (C_j)، میزان برجستگی ($R_i + C_j$) و تاثیر خالص ($R_i - C_j$)، نقشه‌ای دقیق از این پویایی‌ها ارائه می‌دهد.

در تحلیل DEMATEL، مفهوم آستانه تاثیر یا ضریب آلفا به ما کمک می‌کند تا روابط و تاثیرات مهم میان عوامل را شناسایی کرده و بر مواردی تمرکز کنیم که تاثیر قابل‌توجهی بر سایر بخش‌های سیستم دارند. آستانه تاثیر نشان‌دهنده سطحی از ارتباط است که بالاتر از آن، یک رابطه به‌عنوان یک عامل مهم در نظر گرفته می‌شود. در این تحلیل، آستانه تاثیر ۰,۱۵ محاسبه شده است:

$$\alpha = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}[tij]}{N} = ۰.۱۵$$

این مقدار به ما کمک می‌کند تا روابطی را که اثرات آن‌ها کمتر از این مقدار است، به‌عنوان تاثیرات کمتر مهم یا قابل‌چشم‌پوشی شناسایی کنیم و بر روابط با تاثیرات بزرگ‌تر تمرکز نماییم.

در جدول (۴-۲) یافته‌های تحقیق حاصل از تحلیل نظرات خبرگان بر اساس روش تصمیم‌گیری مبتنی بر خطا و ارزشیابی آزمایشگاهی آمده است.

جدول ٤-۲: اثرگذاری و اثرپذیری عوامل تبیین‌کننده امنیت داخلی در از طریق فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتبات با استفاده از روش دیماتل

عوامل	R_i	C_j	$(R_i + C_j)$	$(R_i - C_j)$
بعد توسعه محصول و توسعه فناوری شامل مولفه‌های تسهیل گفتمان عمومی و مشارکت مدنی،بهبود دسترسی به خدمات،افزایش تبادلات و تقابل فرهنگی،تسهیل دسترسی به اطلاعات،کاهش شکاف دیجیتال،تغییر در سبک زندگی،توسعه محصولات هوشمند مبتنی بر هوش مصنوعی و یادگیری ماشینی	۱۰,۱۶۹	۹,۰۰۱	۱۹,۱۷۰	۱,۱۶۷

بعد مدیریت و تجزیه و تحلیل داده‌ها شامل مولفه‌های تغییر افکار، رفتار و انتظارات کاربران،اطمینان از یکپارچگی داده‌ها،شناسایی و ریشه‌یابی مسائل اجتماعی و فرهنگی،جلوگیری از نشت داده‌ها،بهبود حریم خصوصی داده‌ها،بهبود مدیریت منابع شامل منابع انسانی،مالی،زیست‌محیطی و انرژی	۹,۸۹۱	۹,۱۸۸	۱۹,۰۷۹	۰,۷۰۳
بعد اتصال و زیرساخت ارتباطی شامل مولفه‌های ایجاد زیرساخت قابل اعتماد،اطمینان از ارتباط امن،کاهش آلودگی‌های زیست‌محیطی و مصرف انرژی در مراکز داده،افزایش دسترس‌پذیری،افزایش ظرفیت اتصال،افزایش ظرفیت پردازش (محاسبات ابری)،اطمینان از کیفیت ارتباطات	۸,۶۴۶	۹,۵۱۰	۱۸,۱۵۶	-۰,۸۶۴
بعد توانایی‌های نظارتی شامل نظارت بر محتوا و نظارت بر عملکرد شامل مولفه‌های کنترل اخبار جعلی و اطلاعات نادرست،نظارت و حذف محتوای مضر،توسعه سیستم‌های تشخیص نفوذ،شفافیت در کارایی نظام حکمرانی،افزیش آزادی اطلاعات،کاهش اعتماد عمومی،افزیش آزادی بیان	۸,۲۸۵	۹,۷۳۱	۱۸,۰۱۶	-۱,۴۴۵
بعد مشارکت قانونی و مسئولیت اجتماعی شامل مولفه‌های به روزرسانی قوانین برای کاهش عدم قطعیت حقوقی و اختلافات،حمایت مادی و معنوی از پروژه‌های مربوط به مسائل زیست‌محیطی و عدالت اجتماعی،تسهیل دسترسی به قوانین و افزایش آگاهی حقوقی،لابی‌گری و حمایت/عدم حمایت از لوایح قانونی،کاهش ردپای کربن	۱۰,۱۸۰	۹,۳۴۱	۱۹,۵۲۲	۰,۸۳۹

بعد جهانی شدن و گسترش بازار شامل مولفه‌های شفافیت تبادلات،افزایش تاب‌آوری اقتصاد،کاهش نابرابری،اخلال در بازارهای سنتی،افزایش رشد اقتصادی،تغییر نرخ بیکاری،کاهش نرخ فقر	۱۰,۲۶۴	۹,۴۲۲	۱۹,۶۸۶	۰,۸۴۳
بعد همکاری بین‌المللی و داخلی شامل مولفه‌های همکاری با دولت جهت جذب سرمایه،اشتراک‌گذاری دانش و تجربیات،همکاری با شرکت‌های بین‌المللی جهت جذب سرمایه و انتقال دانش و تکنولوژی،نگرانی‌های حریم خصوصی و خطرات حفاظت از داده‌ها،اشتراک‌گذاری داده‌های کاربران شامل داده‌های هویتی و رفتاری از مسیرهای قانونی و مسیرهای فراقانونی با دولت	۸,۳۹۱	۹,۶۳۵	۱۸,۰۲۶	-۱,۲۴۴

نتایج نشان می‌دهد که توسعه محصول و فناوری به عنوان یکی از عوامل کلیدی با تاثیرگذاری بالا شناخته شده است که در بهبود دسترسی به خدمات، کاهش شکاف دیجیتال و توسعه محصولات مبتنی بر هوش مصنوعی و یادگیری ماشینی نقشی موثر ایفا می‌کند. همچنین مولفه‌های مدیریت داده‌ها از جمله بهبود حریم خصوصی و یکپارچگی داده‌ها نیز به عنوان عوامل مهم در بهینه‌سازی مدیریت منابع و ریشه‌یابی مسائل اجتماعی و فرهنگی نقش دارند. از سوی دیگر، زیرساخت‌های ارتباطی و توانایی‌های نظارتی بیشتر به عنوان مولفه‌های تاثیرپذیر شناسایی شده‌اند که وابستگی زیادی به سایر بخش‌های توسعه محصول و فناوری دارند. به همین ترتیب، همکاری‌های بین‌المللی و داخلی، به ویژه در زمینه اشتراک‌گذاری داده‌ها و همکاری با دولت‌ها و شرکت‌های بین‌المللی نیز تحت تاثیر عوامل دیگر قرار می‌گیرند. در نهایت، مشارکت قانونی و مسئولیت اجتماعی به همراه جهانی‌سازی و گسترش بازار به عنوان عوامل با تاثیرگذاری نسبتا بالا در سیستم عمل می‌کنند.

۲.۳.۵. روش تحلیل ساختاری

به منظور تحلیل ساختاری یک ماتریس ۷ در ۷ تشکیل و بر اساس امتیازات داده شده به

پیشران‌های هفتگانه توسط گروه خبرگان ابعاد تاثیرگذاری و تاثیر پذیری هر یک در ٤٩ سلول و در فرایندی سخت و دشوار مورد تحلیل قرار گرفتند.

در ادامه به تحلیل ماتریس اثرات مستقیم و اثرات غیر مستقیم می‌پردازیم.

جدول٤-٣: مجموع اثرات ردیفی و ستونی ماتریس اثرات مستقیم (MDI) و غیر مستقیم (MII)

عوامل	اثرات مستقیم		اثرات غیر مستقیم	
	مقادیر کل ردیف‌ها	مقادیر کل ستون‌ها	مقادیر کل ردیف‌ها	مقادیر کل ستون‌ها
بعد توسعه محصول و توسعه فناوری شامل مولفه‌های تسهیل گفتمان عمومی و مشارکت مدنی،بهبود دسترسی به خدمات،افزایش تبادلات و تقابل فرهنگی،تسهیل دسترسی به اطلاعات،کاهش شکاف دیجیتال،تغییر در سبک زندگی،توسعه محصولات هوشمند مبتنی بر هوش مصنوعی و یادگیری ماشینی	۰,۹۸۹	۰,۸۶۱	۹,۱۷۹	۸,۱۴۰
بعدمدیریت و تجزیه و تحلیل داده‌ها شامل مولفه‌های تغییر افکار، رفتار و انتظارات کاربران،اطمینان از یکپارچگی داده‌ها،شناسایی و ریشه‌یابی مسائل اجتماعی و فرهنگی،جلوگیری از نشت داده‌ها،بهبود حریم خصوصی داده‌ها،بهبود مدیریت منابع شامل منابع انسانی،مالی،زیست‌محیطی و انرژی	۰,۹۵۹	۰,۸۸۲	۸,۹۳۲	۸,۳۰۶
بعد اتصال و زیرساخت ارتباطی شامل مولفه‌های ایجاد زیرساخت قابل اعتماد،اطمینان از ارتباط امن،کاهش آلودگی‌های زیست‌محیطی و مصرف انرژی در مراکز داده،افزایش دسترس‌پذیری،افزایش ظرفیت اتصال،افزایش ظرفیت پردازش (محاسبات ابری)،اطمینان از کیفیت ارتباطات	۰,۸۲۱	۰,۹۱۸	۷,۸۲۵	۸,۵۹۲

بعد توانایی های نظارتی شامل نظارت بر محتوا و نظارت بر عملکرد شامل مولفه‌های کنترل اخبار جعلی و اطلاعات نادرست،نظارت و حذف محتوای مضر،توسعه سیستم‌های تشخیص نفوذ،شفافیت در کارایی نظام حکمرانی،افزیش آزادی اطلاعات،کاهش اعتماد عمومی،افزیش آزادی بیان	۰,۷۸۴	۰,۹۴۱	۷,۵۰۲	۸,۷۸۹
بعد مشارکت قانونی و مسئولیت اجتماعی شامل مولفه‌های به روزرسانی قوانین برای کاهش عدم قطعیت حقوقی و اختلافات،حمایت مادی و معنوی از پروژه‌های مربوط به مسائل زیست‌محیطی و عدالت اجتماعی،تسهیل دسترسی به قوانین و افزایش آگاهی حقوقی،لابی‌گری و حمایت/عدم حمایت از لوایح قانونی،کاهش ردپای کربن	۰,۹۹۱	۰,۸۹۹	۹,۱۸۹	۸,۴۴۲
بعد جهانی شدن و گسترش بازار شامل مولفه‌های شفافیت تبادلات،افزایش تاب‌آوری اقتصاد،کاهش نابرابری،اخلال در بازارهای سنتی،افزایش رشد اقتصادی،تغییر نرخ بیکاری،کاهش نرخ فقر	۱	۰,۹۰۸	۹,۲۶۴	۸,۵۱۴
بعد همکاری بین‌المللی و داخلی شامل مولفه‌های همکاری‌بادولت‌جهت‌جذب‌سرمایه،اشتراک‌گذاری دانش و تجربیات،همکاری با شرکت‌های بین‌المللی جهت جذب سرمایه و انتقال دانش و تکنولوژی،نگرانی‌های حریم خصوصی و خطرات حفاظت از داده‌ها،اشتراک‌گذاری داده‌های کاربران شامل داده‌های هویتی و رفتاری از مسیرهای قانونی و مسیرهای فراقانونی با دولت	۰,۷۹۴	۰,۹۳۱	۷,۵۹۷	۸,۷۰۴

ابعادی که دارای مقادیر بالای اثر مستقیم (ردیف) و اثر غیرمستقیم (ردیف) هستند، نشان‌دهنده توان بالای این ابعاد در تاثیرگذاری بر سایر ابعاد است. بعد جهانی شدن و گسترش بازار به عنوان قدرتمندترین بعد تاثیرگذار در سیستم شناخته می‌شود. جهانی شدن به عنوان نیرویی کلیدی در تعاملات اقتصادی و امنیتی، نقش بسیار مهمی در شکل‌دهی به سایر ابعاد دارد. تاثیرگذاری این بعد به شکل غیرمستقیم نیز نشان می‌دهد که گسترش بازار می‌تواند از طریق سایر ابعاد به‌طور چشم‌گیری بر سیستم اثر بگذارد. بعد مولفه‌های توسعه محصول و توسعه فناوری نیز یکی از ابعاد قدرتمند است. نوآوری‌های فناوری و توسعه محصولات نه تنها به‌طور مستقیم بر سیستم تاثیر دارند، بلکه از طریق سایر ابعاد، مانند داده‌ها و چارچوب‌های قانونی، بر کل سیستم اثر می‌گذارند. بعد مشارکت قانونی و مسئولیت اجتماعی نیز نقش کلیدی در سیستم دارد. قوانین و مسئولیت اجتماعی نه تنها به‌طور مستقیم تاثیرگذار هستند، بلکه به‌طور غیرمستقیم نیز از طریق دیگر ابعاد بر امنیت و پایداری سیستم اثر می‌گذارند.

ابعادی که دارای مقادیر بالای اثر مستقیم (ستون) و اثر غیرمستقیم (ستون) هستند، نشان‌دهنده وابستگی بیشتر آن‌ها به سایر ابعاد است. بعد اتصال و زیرساخت ارتباطی و بعد توانایی‌های نظارتی شامل نظارت بر محتوا و نظارت بر عملکرد بیشترین تاثیرپذیری را از سایر ابعاد دارند. این امر نشان‌دهنده این است که زیرساخت‌های ارتباطی و توانایی‌های نظارتی به‌طور ویژه تحت تاثیر ابعاد کلیدی دیگری مانند فناوری و قوانین هستند و خود تاثیر مستقیمی بر سیستم ندارند. در واقع، این ابعاد به عنوان ابعاد واکنشی عمل می‌کنند و به تحولات دیگر ابعاد بستگی دارند. در بعد همکاری بین‌المللی و داخلی نیز مقادیر تاثیرپذیری مستقیم و غیرمستقیم نشان‌دهنده این است که همکاری‌های بین‌المللی و داخلی به شدت تحت تاثیر ابعاد دیگر از جمله فناوری، قوانین و گسترش بازار هستند و در این تحلیل، به‌عنوان بعد تاثیرگذار، نقش کم‌رنگ‌تری دارد.

همچنین ابعادی مانند بعد اتصال و زیرساخت ارتباطی، بعد توانایی‌های نظارتی شامل نظارت بر محتوا و نظارت بر عملکرد و بعد همکاری بین‌المللی و داخلی در این تحلیل تاثیرگذاری مستقیم ندارند. این بدان معناست که این ابعاد به عنوان مولدهای اولیه در سیستم عمل نمی‌کنند و بیشتر به تغییرات ایجاد شده توسط دیگر ابعاد وابسته هستند. این ابعاد اغلب به‌عنوان ابعاد پشتیبان در سیستم عمل می‌کنند و تحت تاثیر تحولات ابعاد کلیدی دیگر قرار دارند.

این تحلیل نشان می‌دهد که جهانی شدن و گسترش بازار، توسعه محصول و نوآوری‌های فناوری و چارچوب‌های قانونی و مسئولیت اجتماعی نقش‌های کلیدی در سیستم ایفا می‌کنند. به‌ویژه، این ابعاد از طریق اثرات غیرمستقیم خود می‌توانند به‌طور چشم‌گیری بر سیستم اثر بگذارند و توسعه، امنیت و

پایداری سیستم را تضمین و یا تهدید کنند. از سوی دیگر، ابعاد واکنشی مانند زیرساخت‌های ارتباطی و توانایی‌های نظارتی بیشتر تحت تاثیر تغییرات و تحولات در این ابعاد کلیدی هستند و نیاز به توجه خاص در طراحی سیاست‌ها و راهبردها دارند.

جدول ۴-۵ عوامل موثر بر امنیت داخلی در محورهای اثرگذاری-اثرپذیری

اثرگذاری \ اثرپذیری	نیروهای پیشران	نیروهای مستقل
	• بعد مولفه‌های توسعه محصول و توسعه فناوری • بعد مولفه‌های مدیریت و تجزیه و تحلیل داده‌ها • بعد مشارکت قانونی و مسئولیت اجتماعی • بعد جهانی شدن و گسترش بازار	
	نیروهای وابسته	**نیروهای خودمختار**
	• بعد اتصال و زیرساخت ارتباطی • بعد همکاری داخلی و بین‌المللی	• بعد توانایی‌های نظارتی شامل نظارت بر محتوا و نظارت بر عملکرد

۴.۵.آینده‌نگاری و طراحی سناریوهای اثرگذاری فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات بر امنیت داخلی

همان‌طور که در بخش‌های قبلی اشاره شد، برای تدوین سناریوهای آینده‌نگری راهبردی در این پژوهش از روش تحلیل اثرات متقابل بهره گرفته شده است. این روش دارای گونه‌های مختلفی است که هر یک بر اساس تحلیل شبکه‌ای از اثرات متقابل میان عوامل مختلف به‌کار می‌روند. در این تحقیق، رویکردی ترکیبی از روش‌های کیفی و کمی مورد استفاده قرار گرفت تا بتوان توصیف گرها و اثرات متقابل آن‌ها را به‌طور دقیق شناسایی کرد و شبکه‌ای از روابط میان این عوامل ترسیم نمود. هدف از به‌کارگیری این روش، توسعه سناریوهای کل‌نگری بود که دیدگاه جامعی از ارتباطات میان متغیرها فراهم کنند و در نتیجه، شناخت عمیق‌تری از رفتار شبکه‌ای عوامل کلیدی در حوزه فناوری و توسعه اجتماعی-اقتصادی به‌دست آید.

در این تحقیق، ۷ عامل کلیدی شناسایی شدند و پس از بررسی، ٤ عامل به عنوان مبنای تدوین سناریوها انتخاب گردیدند. این عوامل شامل موارد زیر هستند:

۱. توسعه محصول و توسعه فناوری
۲. مدیریت و تجزیه و تحلیل داده‌ها
۳. مشارکت قانونی و مسئولیت اجتماعی
۴. جهانی‌شدن و گسترش بازار

این انتخاب به‌دلیل اهمیت این عوامل در شکل‌دهی به چشم‌انداز آینده و اثرات گسترده‌ای که بر امنیت داخلی دارند صورت گرفت. از ترکیب حالت‌های مختلف این چهار عامل، تعداد ۱۶ سناریوی ممکن به‌دست آمد که تحلیل هر یک از این سناریوها ما را قادر می‌سازد تا راهبردهای مناسبی برای مواجهه با آینده‌های مختلف در حوزه فناوری و توسعه اجتماعی-اقتصادی تدوین کنیم. در ادامه، هر یک از سناریوهای سازگار پیش‌بینی‌شده به تفصیل معرفی و تحلیل شده‌اند تا نقشه راهی روشن برای تصمیم‌گیران فراهم شود. این نقشه راه به آن‌ها کمک می‌کند تا برنامه‌های استراتژیک خود را به شکلی موثر تنظیم و اجرا کنند، به‌طوری که آمادگی لازم برای مواجهه با شرایط مختلف آینده را داشته باشند. برای تدوین سناریوهای آینده‌نگری، برای هر یک از عوامل کلیدی شناسایی شده، دو حالت مطلوب و نامطلوب در نظر گرفته شده است. سناریوهای سازگار به شرح زیر است:

سناریو/بعد	توسعه محصول و توسعه فناوری	مدیریت و تجزیه و تحلیل داده‌ها	مشارکت قانونی و مسئولیت اجتماعی	جهانی شدن و گسترش بازار
سناریو ۱	مطلوب	مطلوب	مطلوب	مطلوب
سناریو ٦	مطلوب	نامطلوب	نامطلوب	مطلوب
سناریو ۱۱	نامطلوب	مطلوب	مطلوب	نامطلوب
سناریو ۱٦	نامطلوب	نامطلوب	نامطلوب	نامطلوب

- سناریو ۱: تکنولوژی در خدمت جامعه و امنیت
- سناریو ٦: شکوفایی اقتصادی در سایه سنگین نشت داده‌ها و قوانین ناکافی
- سناریو ۱۱: چارچوب‌های قانونی محکم، توسعه فناوری کند، اقتصاد سنتی در برابر نوآوری
- سناریو ۱٦: فروپاشی در سایه انزوای اقتصادی و مدیریت ناکارآمد

۶. نتیجه‌گیری و راهبردها

در این پژوهش، با شناسایی هفت عامل کلیدی و انتخاب چهار عامل اصلی شامل توسعه محصول و توسعه فناوری، مدیریت و تجزیه و تحلیل داده، مشارکت قانونی و مسئولیت اجتماعی، و جهانی شدن و گسترش بازار، ۱۶ سناریوی متنوع مورد بررسی و تحلیل قرار گرفت. سناریوهای ارائه‌شده می‌توانند به عنوان ابزاری برای تدوین استراتژی‌های بلندمدت و انعطاف‌پذیر مورد استفاده قرار گیرند که توانایی سازگاری با طیف وسیعی از آینده‌های ممکن را دارند. علاوه بر این، تشویق به گفتگوهای عمومی درباره نقش فناوری در جامعه و تعیین نوع آینده‌ای که می‌خواهیم بسازیم، می‌تواند به ایجاد همگرایی در اهداف و اقدامات کمک کرده و بهره‌برداری موثرتر از فناوری را در جهت منافع جمعی تسهیل کند.

تحلیل جامع ۱۶ سناریو براساس تعاملات میان توسعه محصول و فناوری، مدیریت و تحلیل داده‌ها، مشارکت قانونی و مسئولیت اجتماعی و جهانی شدن و گسترش بازار، دیدگاه‌های ارزشمندی را درباره اثرات ترکیبی این عوامل بر امنیت داخلی ارائه می‌دهد. بررسی حالت‌های مختلف هر یک از عوامل به ما امکان می‌دهد تا به درک عمیقی از روابط پیچیده این عوامل و پیامدهای آن‌ها بر امنیت داخلی برسیم.

نکات زیر در این سناریوها قابل تعمل است:

- نقش کلیدی چارچوب‌های قانونی:
  - سیستم‌های حقوقی قوی تضمین می‌کنند که نوآوری در فناوری به‌طور اخلاقی توسعه یافته و اجرا شود و داده‌ها به‌درستی مدیریت شوند.
  - چارچوب‌های حقوقی ضعیف منجر به سوءاستفاده، فساد و عدم انطباق می‌شوند که امنیت داخلی را حتی با وجود پیشرفت‌های فناوری یا اقتصادی، تضعیف می‌کند.
- فناوری و داده به عنوان محرک‌ها:
  - توسعه محصول و فناوری و مدیریت و تحلیل داده‌ها نقش حیاتی در تقویت قابلیت‌های امنیتی دارند. فناوری‌های پیشرفته امکان نظارت و تشخیص تهدیدات را بهبود می‌بخشند، در حالی که مدیریت موثر داده‌ها به شناسایی و کاهش خطرات امنیتی کمک می‌کند.
  - اما توسعه فناوری بدون مدیریت داده قوی (یا برعکس) پتانسیل کامل خود را نشان نمی‌دهد و ممکن است آسیب‌پذیری‌های جدیدی ایجاد کند.
- ابعاد اجتماعی و اقتصادی:
  - عواملی که عدالت اجتماعی، پایداری محیط‌زیست و نابرابری اقتصادی را تحت تاثیر قرار

می‌دهند، نقش مهمی در امنیت داخلی ایفا می‌کنند. سناریوهایی که این جنبه‌ها را نادیده می‌گیرند، غالبا شاهد افزایش تنش‌های اجتماعی، ناآرامی‌ها و افزایش جرایم هستند.

○ حمایت از ابتکارات زیست‌محیطی و عدالت اجتماعی به ثبات اجتماعی و افزایش اعتماد عمومی به نهادها کمک می‌کند.

همچنین، پس از بررسی این ۱۶ سناریو، می‌توان چند نکته کلیدی را استنباط کرد:

۱. امنیت داخلی زمانی به حداکثر می‌رسد که توسعه فناوری، مدیریت داده، چارچوب‌های قانونی و تلاش‌های جهانی‌سازی به‌طور همزمان پیشرفت کنند. نادیده گرفتن هر یک از این عوامل می‌تواند نقاط قوت دیگر عوامل را تضعیف کند.

۲. چارچوب‌های حقوقی قوی و تعهد به مسئولیت اجتماعی برای جلوگیری از سوءاستفاده از فناوری، حفظ حریم خصوصی داده‌ها و تقویت اعتماد عمومی ضروری هستند. قوانین و مقررات باید به سرعت با پیشرفت‌های فناوری تطبیق یابند تا بتوانند هم از نوآوری حمایت کنند و هم از منافع عمومی محافظت نمایند.

۳. تلاش برای کاهش نابرابری، بیکاری و فقر به ایجاد جامعه‌ای امن‌تر و باثبات‌تر کمک می‌کند. سیاست‌های اقتصادی باید به رشد فراگیر توجه کنند تا اطمینان حاصل شود که مزایای توسعه فناوری و پیشرفت‌های اقتصادی به‌طور گسترده‌ای توزیع می‌شود.

۴. تسهیل گفتگوهای عمومی و افزایش آگاهی‌های حقوقی، شهروندان را توانمند کرده و مشارکت مدنی و اعتماد به نهادها را تقویت می‌کند. یک جمعیت آگاه و دغدغه‌مند، جزئی حیاتی از امنیت داخلی است.

در نهایت، این تحلیل سناریو نشان می‌دهد که آینده فناوری نه تنها به پیشرفت‌های فنی، بلکه به تصمیمات سیاسی، اقتصادی و اجتماعی ما نیز بستگی دارد. برای ساختن آینده‌ای مطلوب، نیاز به رویکردی جامع و چندبعدی داریم که نه تنها به توسعه فناوری، بلکه به تاثیرات گسترده‌تر آن بر جامعه، اقتصاد و محیط زیست نیز توجه کند. این سناریوها می‌توانند به عنوان ابزاری برای سیاست‌گذاران، رهبران صنعت و پژوهشگران عمل کنند تا استراتژی‌های بلندمدت و انعطاف‌پذیری را توسعه دهند که بتوانند با طیف وسیعی از آینده‌های ممکن سازگار شوند. همچنین، این سناریوها می‌توانند به عنوان نقطه شروعی برای گفتگوهای عمومی گسترده‌تر درباره نوع آینده‌ای که می‌خواهیم بسازیم و چگونگی استفاده از فناوری برای دستیابی به آن اهداف عمل کنند.

با توجه به نتایج حاصل از این پژوهش پیشنهاد می‌گردد:

۱. تشـــویق نوآوری مســـئولانه: تخصیص کمک‌های مالی دولتی، مشـــوق‌های مالیاتی و بودجه مستقیم به شرکت‌های حوزه فناوری اطلاعات و ارتباطات که اقدامات مشخصی را برای ادغام تدابیر امنیتی و حفظ حریم خصوصی در محصولات خود نشان می‌دهند.

۲. تقویت همکاری بخش عمومی و بخش خصوصی: تشکیل تیم‌های نوآوری مسئولانه متشکل از نمایندگان دولت، صنعت و دانشـــگاه که به حل چالش‌های خاص امنیتی مانند اســـتفاده اخلاقی از هوش مصنوعی، اشتراک‌گذاری ایمن داده‌ها، و فناوری‌های حفظ حریم خصوصی بپردازند. این تیم‌ها می‌توانند راه‌حل‌های هدفمند و مفیدی برای موسسات دولتی و خصوصی فراهم کنند.

۳. تمرکز بر سواد دیجیتال و شمول اجتماعی: راه‌اندازی برنامه‌های آموزشی در سراسر کشور، به ویژه در مناطق روستایی و کم‌برخوردار، به منظور آموزش نحوه استفاده ایمن از فناوری‌های جدید. همکاری با بخش‌های محلی، کتابخانه‌ها و موسسات آموزشی برای ارائه دوره‌های سواد دیجیتال که شامل مهارت‌های پایه‌ای و تدابیر حفاظتی حریم خصوصی است.

۴. تدوین دستورالعمل‌های اخلاقی: ایجاد مجموعه‌ای از دستورالعمل‌ها و استانداردهای شفاف برای توسعه و استقرار فناوری‌های هوش مصنوعی، که دربرگیرنده ملاحظات اخلاقی از جمله عدم تبعیض، عدالت و شـــفافیت در نتایج باشـــند. این دستورالعمل‌ها باید به گونه‌ای تدوین شوند که از تاثیرات منفی ناشی از سوگیری در سیستم‌های هوش مصنوعی پیشگیری کنند و توسعه‌دهندگان را ملزم به رعایت آن‌ها نمایند.

۵. توسعه فناوری‌هایی با محوریت حریم‌شخصی: ارائه حمایت مالی و فنی به شرکت‌های حوزه فناوری اطلاعات و ارتباطات برای پیاده‌سازی ابزارهای رمزگذاری انتها به انتها، ناشناس‌سازی داده‌هـــا، و مدیریت رضایت کاربران در محصولاتشـــان. ایجاد نشـــان کیفیت یا گواهی برای محصولاتـــی که اســـتانداردهای بالای حریم خصوصی را رعایـــت می‌کنند، به کاربران کمک می‌کند تا انتخاب‌های آگاهانه‌تری داشته باشند.

۶. ترویج اشـــتراک‌گذاری شفاف داده‌ها: توســـعه توافق‌نامه‌های استاندارد اشتراک‌گذاری داده بین دولت و شـــرکت‌های حوزه فناوری اطلاعات و ارتباطات که شـــامل مقررات دقیق درباره دسترسی به داده‌ها، محدودیت‌های استفاده و شفافیت است.

۷. کمپین‌های اعتمادسازی عمومی: برگزاری برنامه‌های اطلاع‌رسانی عمومی به منظور افزایش

آگاهی شهروندان در مورد حفاظت از داده‌های شخصی و تاکید بر اقداماتی که برای حفاظت از اطلاعات انجام شده است. ایجاد کارگاه‌های محلی و کمپین‌های رسانه‌های اجتماعی برای اطلاع‌رسانی درباره اهمیت حفاظت از داده‌ها، بهداشت سایبری و نقش دولت در حفاظت از حقوق شهروندان.

۸. به‌روزرسانی چارچوب‌های قانونی: ایجاد مکانیسم‌های ویژه برای به‌روزرسانی سریع قوانین بر اساس فناوری‌های نوظهور. ایجاد کمیته مشاوره فناوری متشکل از کارشناسان حقوقی، فناوران و مدافعان حقوق مدنی برای نظارت مستمر بر پیشرفت‌های فناوری و ارائه توصیه‌های قانونی برای بروزرسانی مقررات.

۹. مقررات شفاف لابی‌گری: ایجاد یک ثبت شفاف از تمامی فعالیت‌های لابی‌گری انجام‌شده توسط شرکت‌های حوزه فناوری اطلاعات و ارتباطات که برای عموم قابل دسترسی باشد. الزام به افشای منابع مالی و موضوعات مورد لابی‌گری به منظور اطمینان از عدم تاثیر نامطلوب بر منافع عمومی.

با توسعه راهبردهایی که به این موضوعات مشترک پرداخته و در عین حال به شرایط خاص هر سناریو قابل تطبیق هستند، سیاست‌گذاران، رهبران کسب‌وکار و جامعه می‌توانند آمادگی خود را برای آینده‌ای نامطمئن افزایش دهند. این تحلیل آینده‌نگری راهبردی، پایه‌ای برای برنامه‌ریزی و توسعه به جزئیات بیشتر ارائه می‌دهد و نقشه راهی برای پیمایش در چشم‌انداز پیچیده تغییرات فناوری و اجتماعی ارائه می‌کند. همچنان که به پیش می‌رویم، بازنگری مداوم و تطابق این راهبردها بسیار حیاتی خواهد بود. سرعت بالای تغییرات فناوری نیازمند یک فرآیند پیوسته از آینده‌نگری، تحلیل راهبردی است. با حفظ رویکردی آینده‌نگر و انعطاف‌پذیر، می‌توانیم به سمت ساختن آینده‌ای که در آن فناوری و شرکت‌های فناور ابزاری برای پیشرفت اجتماعی و رفاه انسانی در تمامی سناریوهای ممکن باشد، قدم برداریم.

فهرست منابع

۱. اختری، محمد- کرامتی، محمدعلی و امین موســـوی، سیدعبداله (۱۴۰۲). ارائه مدل مفهومی بلوغ امنیت ســـایبری برای زیرساخت‌های حیاتی کشور. فصلنامه علمی آینده‌پژوهی دفاعی، ۸ (۲۹)، ۱۰۱-۱۳۴.

۲. پورســـعید، فرزاد (۱۴۰۱). نســـبت مفهومی فرهنگ و امنیت: جســـتاری در چیستی «امنیت فرهنگی». فصلنامه مطالعات راهبردی، ٤ (۲۵)، ۱۷۷-۲۱۵.

۳. پورعزت، علی اصغر و عبدی، بهنام (۱۳۹۷). شناسایی فراروندهای فناوری اطلاعات و ارتباطات قابل توجه در آینده نگاری صنعت دفاعی در جهت نیل به الگوی اســـلامی- ایرانی پیشـــرفت. آینده‌پژوهی دفاعی، ۳ (۱۰) ، ۵۳-۷۵.

۴. پروین، خیرالله- فرامرزی، رضا و پاشـــایی امیری، امین (۱۳۹۹). تنقیح قوانین و مقررات گامی در تضمین اصل امنیت حقوقی. دانش حقوق عمومی، ۹ (۳۰)، ۹۵-۱۱۶.

۵. ترابی، یوســـف- کتولی‌نژاد، خدابخش و عبدی، توحید (۱۴۰۰). ارائه الگوی راهبردی در حوزه امنیت سیاســـی از طریق تدوین تجارب نظام مقدس ج.ا.ایران براســـاس گفتمان ولایت فقیه و قانون اساسی. فصلنامه علمی امنیت ملی ، ۱۱ (٤۱)، ۱۰۳-۱۳۰.

۶. تقی‌پور، رضا - لشـــکریان، حمیدرضا- ناصری، علی و یزدانی چهاربرج، رحیم (۱۳۹۸). الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران. فصلنامه علمی امنیت ملی، ۹ (۳۴)، ۷-۴۹.

۷. جهانگرد، اســـفندیار- مروت، حبیب و سپه‌وند، نیلوفر (۱۳۹٦). نقش محتوا بر شکاف دیجیتال اقتصاد، فصلنامه مدلسازی اقتصادسنجی، ۳ (۱)، ۲۷-٥٤.

۸. حافظ‌نیا، محمدرضا (۱٤۰۰). مقدمه‌ای بر روش تحقیق در علوم انســـانی، ســـازمان مطالعه و تدوین کتب علوم انسانی دانشگاهها (سمت).

۹. حبیب زاده، قاسم (۱۳۹۸). ابعاد امنیت از منظر امام خامنه ای (مدظله العالی). فصلنامه علمی امنیت ملی ، ۹ (۳۱)، ۷-۳۲.

۱۰. حســـن‌بیگی، ابراهیم و کولیوند، ابراهیم (۱۳۹۶). الگوی راهبردی مدیریت تحولات برآمده از توســـعه فناوری اطلاعات و ارتباطات بر امنیت داخلی جمهوری اسلامی ایران. فصلنامه علمی امنیت ملی، ۷ (۲۴)، ۵۹-۸۰.

۱۱. دستغیب، سیداحمدرضا(۱۳۹۶).تاثیر فناوری اطلاعات و ارتباطات بر ابعاد مختلف امنیت ملی (ابعاد نظامی، سیاسی، اقتصادی، اجتماعی، فرهنگی و زیست محیطی)،کنفرانس ملی رویکردهای نوین علوم انسانی در قرن ۲۱

۱۲. ذکی، یاشار و نجفی، سجاد (۱۳۹۹). تبیین عوامل کلیدی تاثیرگذار بر امنیت زیست محیطی ایران در افق زمانی ۱۴۰۸. فصلنامه پدافند غیرعامل و امنیت، ۹ (۳۳)، ۱۲۳-۱۴۵.

۱۳. رشیدی طغرالجردی، مصطفی- ردادی، علی و مقدم فر، سعیدرضا (۱۳۹۴). طراحی الگوی سنجش امنیت اقتصادی کشور. مطالعات راهبردی بسیج، شماره ۶۸.

۱۴. رشیدی، مصطفی - ردادی، علی و مقدم‌فر، سعیدرضا (۱۳۹٤). طراحی الگوی سنجش امنیت اقتصادی کشور، فصلنامه مطالعات راهبردی بسیج، سال هجدهم، شماره ٦٨.

۱۵. رفیع، حسین و جانباز، دیان (۱۳۸۹). تاثیر فناوری‌های جهانی اطلاعاتی و ارتباطی بر امنیت ملی کشورها، فصلنامه سیاست، شماره ۱ (٤٠).

۱۶. رضاپور، دانیال و اسکندری نسب، علی (۱۳۹۸). امنیت فضای سایبر در رویکرد فرهنگی مقام معظم رهبری. مطالعات روابط فرهنگی بین الملل، ۵ (۱۰)، ۱۷۳-۲۰۳.

۱۷. رضوی‌نژاد، سید امین و رزاقی، جواد (۱۳۹۷). مدل مطلوب اجرا و ارزیابی در سیاست‌گذاری امنیت داخلی جمهوری اسلامی ایران، خط مشی‌گذاری عمومی در مدیریت، شماره ۲۹ ISC، ۱۰۱-۱۱۸.

۱۸. رمضانی، محمدجواد - بدری، کوروش و غفاری، جلال (۱۳۹۹). بررسی روندهای تاثیرگذاری شبکه‌های اجتماعی بر امنیت ملی جمهوری اسلامی ایران. فصلنامه علمی امنیت ملی، ۱۰ (۳۷)، ۳۸۷-۴۲۰.

۱۹. رهامی، روح اله و اژدری، امیرحسین (۱۴۰۱). امنیت سایبری اتحادیه اروپا: تهدیدات، فرصتها و اقدامات (از آغاز تا سال ۲۰۲۱). تحقیقات حقوقی، دوره ۲۵، ۳۰۲-۲۷۳.

۲۰. زارع‌زاده، رسول (۱۳۹۲). الگوی تحلیل امنیت داخلی: تبیین مولفه‌های اثرگذار بر امنیت داخلی در سطح کلان، فصلنامه آفاق امنیت، ٦ (۱۹).

۲۱. زارع‌زاده، رسول (۱٤۰۰). آسیب‌ها و چالش‌های امنیتی‌سازی مسائل داخلی؛ مطالعه موردی شبکه‌های اجتماعی مجازی، مطالعات راهبردی، شماره ۹۲ ISC، ۳۲-۷.

۲۲. سپهرنیا، روزیتا و شیخی، محمدطاهر (۱٤۰۰). نقش سرمایه فرهنگی در تامین امنیت داخلی، مطالعات دفاع مقدس، شماره ۲٦ ISC، ۱۹۵-۱۷۵.

۲۳. سلطانی‌نژاد، احمد- موسوی شفائی- مسعود و اسدی‌نژاد، الهام (۱۳۹۲). تاثیر فناوری اطلاعات و ارتباطات بر امنیت ملی جمهوری اسلامی ایران در دهه ۱۳۸۰، پژوهشنامه علوم سیاسی، شماره ۲، ۷۹-۱۱۲.

۲۴. شهبازی، نجفعلی (۱۳۹۹). تحلیل آثار فقر و نابرابری درآمدی بر امنیت اقتصادی در ایران. فصلنامه علمی «اقتصاد ایران و امنیت اقتصادی»، ۱ (۲)، ۱-۳۲.

۲۵. صادقی، محمدرضا (۱۳۹۷). معجزه اقتصاد دیجیتال، تهران، موسسه مطالعات و پژوهش‌های بازرگانی.

۲۶. صیدی، مهدی (۱۳۹۹). رتبه‌بندی استان‌ها در حوزه امنیت اقتصادی با استفاده از تکنیک تاپسیس. فصلنامه علمی امنیت ملی، ۱۰ (۳۸)، ٤١٥-٤٤٤.

۲۷. قوام، سید عبدالعلی و مصطفوی، سیده معصومه (۱۳۹۷). تحول پارادیمی در مفهوم امنیت زیست محیطی. پژوهش ملل، ۳ (۳۴).

۲۸. عامری، محمدعلی، ذوالفقاری، حسین، پورمنافی، ابوالفضل. (۱۴۰۲). الزامات موثر تامین امنیت اقتصادی بر بستر تولید دانش بنیان. فصلنامه علمی امنیت ملی، ۱۳ (۴۷)، ۱۵۶-۱۲۷.

۲۹. عباس زاده فتح آبادی، مهدی و منصوری، منصوره (۱۳۹۸). تاثیر دولت شکننده عراق بر امنیت زیست محیطی جمهوری اسلامی ایران. فصلنامه علمی سیاست جهانی، ۸ (۲)، ۲۹۱-۳۲۲.

۳۰. عبیری، داود- یزدانی چهاربرج، رحیم- هلیلی، خداداد و ثقفی، کامیار (۱۳۹۹). تبیین نقش شبکه ملی اطلاعات در مدیریت فرصت‌ها و تهدیدهای فضای مجازی کشور. فصلنامه علمی امنیت ملی ، ۱۰ (۳۷)، ٤٢١-٤٥٠.

۳۱. عرفانی، سهراب- مبینی دهکردی، علی- افتخاری، اصغر- مرادیان، محسن و فیروزآبادی، سید جلال (۱۴۰۱). الزامات تامین امنیت در افق سند چشم انداز ۱۴۰۴. فصلنامه علمی امنیت ملی، ۱۲ (٤٣)، ۳۲-۷.

۳۲. علیزاده، عظیم (١٤٠٠). آینده‌نگاری راهبردی در امنیت داخلی؛ ارائه الگوی دوشاخه تدوین راهبرد. فصلنامه علمی مطالعات مدیریت راهبردی دفاع ملی ، ۵ (۲۰)، ۱۸۸-۱۶۳.

۳۳. غیاثوند، ابوالفضل و عبدالشاه، فاطمه (١٣٩٤). مفهوم و ارزیابی تاب‌آوری اقتصادی ایران. پژوهشنامه اقتصادی، ۵۹ (٤)، ١٦١-١٨٧.

۳۴. کریمی قهرودی، محمدرضا- فشارکی، مهدی و نظامی‌پور، قدیر (۱۳۹۲). تدوین چشم‌انداز و الگوي بلوغ توسعه فناوری اطلاعات و ارتباطات سازمان در افق ١٤٠٤ با رویکرد آینده‌نگاري،

بهبود مدیریت، شماره ۱۹، ۱۳۷-۱۶۱.
۳۵. کرمی، مرجان- کشیشیان سیرکی، گارینه و توحیدفام، محمد (۱۴۰۳). تهدید شبکه‌های اجتماعی مجازی برای زیر ساخت‌های حیاتی امنیت ملی (از منظر کارشناسان حوزه سیاسی و رسانه مجازی). فصلنامه علمی امنیت ملی ، ۱٤ (۵۱)، ۵۹-۸۸.
۳۶. کریمی قهرودی، محمدرضا- سعادتمند، امیر مسعود و محمدی، حافظ (۱۴۰۱). ارائه مدلی برای ارزیابی امنیت سایبری جمهوری اسلامی ایران. فصلنامه امنیت ملی، شماره ۴۵، ۶۹-۱۰۰.
۳۷. گودرزی، غلامرضا و اجلالی، محمدمهدی (۱۴۰۰). تحلیل روندهای آینده فناوری‌های دفاعی در افق ده ساله. آینده‌پژوهی دفاعی، شماره ۲۳، ۳۷-۵۷.
۳۸. مسیبی ملک خیل، رحیم و کریمی، وحید(۱۴۰۱). تبیین ابعاد، مولفه‌ها و شاخصهای فناوری اطلاعات و ارتباطات در حوزه امنیت ج. ا. ایران. فصلنامه علمی مطالعات بین رشته‌ای دانش راهبردی ، ۱۲ (٤٦)، ۱۸۷-۲۱۶.
۳۹. میرزمانی، اعظم- خنیفر، حسین- جعفری، سید محمدباقر و سماواتیان، اکرم (۱۳۹۸). نقش خودافشایی در شبکه‌های اجتماعی مجازی بر ارتقای امنیت اجتماعی (مورد مطالعه: شهر همدان). فصلنامه علمی تخصصی دانش انتظامی همدان، شماره ۲۱.
۴۰. محمدی خانقاهی، محسن و آزادی، محمدحسین (۱۴۰۰). تفاوت‌های امنیت سایبری اجتماعی با امنیت سایبری. فصلنامه علمی امنیت ملی ، ۱۱ (٤۱)، ۱۳۱-۱۵۸.
۴۱. محرمی، توحید (۱۳۹۷). آینده امنیت فرهنگی جمهوری اسلامی و تحقق تمدن نوین اسلامی. دو فصلنامه علمی مطالعات بنیادین تمدن نوین اسلامی، ۱ (۱)، ٦۵-۸۹.
۴۲. محمدی نیا سماکوش، خلیل و صبح خیز، رضا (۱۴۰۱). تاثیر ارزهای مجازی (دیجیتال) بر احساس امنیت اقتصادی شهروندان استان مازندران. دانش انتظامی مازندران، ۱۳ (۵۱)، ۲۱-۵٦.
۴۳. نجفی، سجاد- یزدان پناه درو، کیومرث- پیشگاهی‌فرد، زهرا و بدیعی ازنداهی، مرجان (۱۳۹۹). مقاله پژوهشی: تبیین عوامل کلیدی اثرگذار بر قدرت دفاعی ج.ا.ایران در افق زمانی ۱۴۱۰. آینده‌پژوهی دفاعی، ۱۸ (۴) ، ۱-۳۸.
۴۴. نوری، مهدی و طباطبایی‌نیا، سید بهزاد (۱۳۹۸). عوامل موثر بر رشد اقتصاد دیجیتال، فرصت‌ها و تهدیدات آن و راهبردهای مناسب جمهوری اسلامی ایران در قبال آن، فصلنامه اقتصاد دفاع، ٤ (۱۱)، ۱٤۷-۱۱۷.

۴۵. مهدی نژاد نوری، محمد- خراشادی زاده، محمدرضا- فخری، مجید- حاجی آبادی، سیداحمد (۱۳۹۸). مقالـــه پژوهشـــی:نقش فناوری اطلاعات و ارتباطات در دفـــاع دانش‌بنیان. *مطالعات دفاعی استراتژیک*, *۱۷* (۷۵), ۱۰۷-۱۲۴.
۴۶. ناظمی اردکانی, مهدی- نجاتپور, مجید و محمدی, مصطفی (۱۳۹۵). انقلاب اطلاعات و تأثیر آن بر جنگ نرم. پژوهش‌های راهبردی سیاست, ۵(۱۶), ۱۴۱-۱۶۹.
۴۷. هلیلی، خداداد- مظلوم، جلیل وهادیان، بهرنگ (۱۳۹٤). بررســـی کاربردهای نظامی فناوری کلان داده و نقش آن در مدیریت صحنه نبرد. *فصلنامه علوم و فنون نظامی*،۳۳، ٤۷-٦۲.
۴۸. اربطانی، طاهر روشـــندل و صابر، منوچهر (۱۳۹۱). ارتباط میان فرهنگ و فنّاوری اطلاعات و ارتباطات و آســـیب‌های فرهنگی اینترنت. *مطالعات میان رشـــته‌ای در رسانه و فرهنگ*،۲ (٤)، ۱۰۹-۱۲۸.
۴۹. پناهی، محمدحســـین و پناهی، حسین (۱۳۹٤). بررسی ابعاد و رابطه فناوری‌های اطلاعات و ارتباطات با سرمایه اجتماعی، *مطالعات رسانه‌های نوین*، ۱ (۳)، ۱-٤۲.
۵۰. ســـعدی‌پور، اســـماعیل (۱۳۹۲). آثار فناوری‌های نوین بر شـــبکه‌های اجتماعی با تاکید بر نوجوانان، *فصلنامه مطالعات و تحقیقات اجتماعی در ایران*، ۲ (۲)، ۳۱۵-۳۱۸.
۵۱. شـــکوری، علی (۱٤۰۰). مطالعه تاثیر دوگانه فناوری اطلاعات و ارتباطات در فرایند توســـعه اقتصای و اجتماعی، *مجله جهانی رسانه*، ۱٦ (۲)، ۱-۲۹.
۵۲. طاهری، فاطمه (۱٤۰۱). ســـرمایه اجتماعی آنلاین در دنیـــای فناوری اطلاعات و ارتباطات؛ بررسی و تحلیل دیدگاه‌های مخالف و موافق، *مطالعات رسانه‌های نوین*، ۸ (۳۲)، ۳۷-۷۰.
۵۳. الوندی، هومن-هاشـــمی، شـــهناز و مظفری، افســـانه (۱٤۰۰)، مهمترین مسائل شبکه‌های اجتماعی مجازی در افق ۱۴۰۴ ایران بر مبنای آینده پژوهی مرکز ترند وان (با تاکید بر مسائل سیاسی، اجتماعی و اقتصادی)، *مطالعات رسانه‌ای*، ٤ (۱۵)، ۳۷-۵۷.
۵۴. اکبری، طیب- رضایی، محمود و آزادخانی، پاکزاد (۱٤۰۲. نقش فناوری اطلاعات و ارتباطات در تقویت تاب‌آوری اجتماعی شهرها(مورد پژوهش: سیلاب در ایلام)، *مطالعات جامعه‌شناختی شهری*، ۱۳ (٤۹)، ۱-۳۵.
۵۵. تقـــوی فرد، محمدتقی- وفادار, زهرا- رحیمی, مهـــدی, وآقایی, مجتبی (۱۳۹۵). تحلیلی بر چرخه انسجام سیاستی در نظام حکمرانی فناوری اطلاعات و ارتباطات ایران. مطالعات مدیریت کسب و کار هوشمند, ۴(۱۶), ۱-۳۳. doi: ۱۰,۲۲۰۵۴/ims.۲۰۱۶,۵۱۴۷

۵۶. علی‌اکبری مارانتو، محمدرضا (۱٤۰۰). نقش فناوری اطلاعات و ارتباطات در ارتقاء مشروعیت حکمرانی سیاسی در ایران اولین همایش ملی حکمرانی اسلامی.

۵۷. قیصری، نوراله و امان کاه، سعید (۱٤۰۰). فناوری‌های اطلاعاتی و بسط ظرفیت‌های حکمرانی دولت‌های مدرن مبتنی بر اقناع و قدرت نرم. فصلنامه علمی مطالعات قدرت نرم. ۳ (۲٦).

۵۸. قیاسی، فاطمه- درویش‌پور، حجت‌الله- توحیدفام، محمد و امینی، علی‌اکبر (۱٤۰۰). بررسی نقش فناوری اطلاعات و ارتباطات در تحولات حکمرانی صالح (با تاکید بر فناوری دولت یازدهم در کسب و کار الکترونیک). فصلنامه مدیریت کسب و کار. ٤۹ (۱). ٤٦۷-٤۸۹.

۵۹. احمدی، علی- زرگر، افشـــین و آدمی، علـــی (۱٤۰۱). نقش فناوری‌های نوظهور در امنیت و قدرت ملی کشورها؛ فرصت‌ها و تهدیدها. نشریه مطالعات بین‌المللی. ٤ (۷۲). ۱۳۷-۱۵۹.

۶۰. قاســـمی، محمدهادی و پناهی، فائزه(۱۴۰۲). ،جایگاه و نقش فناوری اطلاعات و ارتباطات در نیل به اقتصاد دانش بنیان

۶۱. مغنی، حیدر- ناصحی‌فر، وحید و ناطق، تهمینه (۱۳۹۸). چگونگی تاثیر گسترش فناوری‌های مالی بر بهبود عملکرد خدمات مالی. فصلنامه اقتصاد مالی. ۱۳ (٤۹). ۱۸۳-۲۱۲.

62. ABS. (2019). Measuring digital activities in the Australian economy. Paper prepared for the Economic Commission for European Statisticians, Eighteenth session, Geneva, 10-12 April 2019.

63. Asogwa, Chika Euphemia. (2020). Internet-Based Communications: A Threat or Strength to National Security? SAGE Open, Volume 10, Issue 2, April-June 2020.

64. Barnes, S.B. (2006). A Privacy Paradox: Social Networking in the United States.

65. Beck, U. (1992). Risk society: Towards a new modernity (M. Ritter, Trans.). SAGE Publications.

66. Bilgin, Pinar. (2003). Individual and Societal Dimensions of Security. Bilkent University, Turkey, Department of International Relations, International Studies Review, 5.

67. Castells, M. (2009). The rise of the network society.

68. Castillo, M. (2013). The Digital Economy for Structural Change and Equality. United Nations.

69. Creswell, J. and Poth, C. (2017). Qualitative Inquiry and Research Design: Choosing among Five Approaches. Sage, London.

70. Digital Regulation. (2023). Enhancing the Protection and Cyber Resilience of Critical Information Infrastructure. DigitalRegulation.org.
71. Evans, P. and Gawer, A. (2016). The rise of the platform enterprise: A global survey. The Emerging Platform Economy Series, 1. The Centre for Global Enterprise, New York, NY.
72. Gorp, N. V. and Batura, O. (2015). Challenges for Competition Policy in a Digitalized Economy. Directorate General for Internal Policies Policy Department: Economic and Scientific Policy, European Parliament.
73. Hermann, M., Pentek, T., & Otto, B. (2017). Design Principles For Industries 4.0 Scenarios. System Sciences (HICSS), IEEE.
74. Lyon, D. (2001). Surveillance society: Monitoring everyday life.
75. Riggs, H. et al. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. Sensors, 23(8), 4060.
76. Rout, Subhashree. (2022). Application of Blockchain Technology to facilitate security in Smart Grid. 10.1109
77. Saeed, S. et al. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors, 23(16), 7273.
78. Savoldelli, Codagnon, and Misuraca. (2014). Understanding the E-Government Paradox: Learning from Literature and Practice on Barriers to Adoption. Government Information Quarterly, Volume 31, Supplement 1.
79. Smith, M. R., & Marx, L. (1994). Does Technology Drive History? The Dilemma of Technological Determinism. MIT Press.
80. Toffler, A. (1980). The Third Wave.
81. Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. Human Relations, 4(1), 3–38.
82. U.S. Bureau of Labor Statistics. Occupational Handbook: Computer and Information Technology Occupations. https://www.bls.gov/ooh/computer-and-information-technology/home.htm
83. Langleite, Rune; Griwodz, Carsten; Johnsen, Frank T. (2021). Military Applications of Internet of Things: Operational Concerns Explored in Context of a Prototype Wearable. International Command and Control Research and Technology Symposium (ICCRTS) proceedings 2021.

84. Ahmad, Hussain. (2021). A Review on C3I Systems' Security: Vulnerabilities, Attacks, and Countermeasures. arXiv preprint arXiv:2104.11906.
85. Schulze, Thomas. (2020). Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. In Proceedings of the 2020 International Conference on Cyber Conflict (CyCon). NATO Cooperative Cyber Defence Centre of Excellence.
86. Haldorai, A., Babitha Lincy, R., Suriya, M., Balakrishnan, M. (2024). Enhancing Military Capability Through Artificial Intelligence: Trends, Opportunities, and Applications. In: Artificial Intelligence for Sustainable Development. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-031-53972-5_18
87. Fraga-Lamas, P. (2024). Evolving Military Broadband Wireless Communication Systems: WiMAX, LTE and WLAN. arXiv preprint arXiv:2404.07207.
88. Bassil, Youssef (2012). Service-Oriented Architecture for Weaponry and Battle Command and Control Systems in Warfighting. arXiv preprint arXiv:1204.0179.
89. Friday, Baaka. (2022). Utility of ICT in the Conduct of Military Operations in Nigeria: A Study of Operation Lafiya Dole in the North East Nigeria (2015-2022).
90. Guttieri, K 2014 Governance, Innovation, and Information and Communications Technology for Civil-Military Interactions. Stability: International Journal of Security & Development, 3(1): 6, pp. 1-16
91. Van Der Meer, S. (2016). The Use of ICT to preserve Australian Indigenous Culture and Language - a Preliminary Proposal using the Activity Theory Framework. arXiv preprint arXiv:1606.01436.
92. Pérez-García, L. (2021). The ICT-Buen Vivir Paradox: Using Digital Tools to Defend Indigenous Cultures. arXiv preprint arXiv:2108.09952.
93. Alkan, Meral, Meinck, Sabine. (2016). The relationship between students' use of ICT for social communication and their computer and information literacy. Large-scale Assessments in Education, 4(1), 15
94. Pierce, G. L., & Cleary, P. F. (2024). The persistent educational digital divide and its impact on societal inequality. PLoS ONE, 19(4), e0286795.

95. Stella, T., Miliou, O., Dimitriadis, Y., Sobrino, S. V., Giannoutsou, N., Cachia, R., & Monés, A. M. I. (2022). Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review. Education and Information Technologies, 27(1), 1-29.
96. Limniou, M. (2021). The Effect of Digital Device Usage on Student Academic Performance: A Case Study. Education Sciences, 11(3), 121.
97. Benvenuti, M., Wright, M., Naslund, J., & Miers, A. C. (2023). How technology use is changing adolescents' behaviors and their social, physical, and cognitive development. Current Psychology, 42, 16466–16469.
98. Mishra, M. (2015). Ethical, Legal and Social aspects of Information and Communication Technology. arXiv preprint arXiv:1507.08447.
99. Bhusal, A. (2022). Impact of Information and Communication Technology on Individual Well-being. arXiv preprint arXiv:2202.00006v2.
100. Courtney, M., Karakus, M., Ersozlu, Z., Nurumov, K. (2022). The influence of ICT use and related attitudes on students' math and science performance: multilevel analyses of the last decade's PISA surveys. Large-scale Assessments in Education, 10, Article 8.
101. Gilardi, F. (2021). Digital Technology, Politics, and Policy-Making. Elements in Public Policy. Cambridge University Press.
102. Savaget, P., Chiarini, T., & Evans, S. (۲۰۱۸). Empowering political participation through artificial intelligence. Science and Public Policy, 46(3), 369–380. https://doi.org/10.1093/scipol/scy064
103. Eckardt, M. (2021). The Impact of ICT on Policies, Politics, and Polities—An Evolutionary Economics Approach to Information and Communication Technologies (ICT). In: Herberger, T.A., Dötsch, J.J. (eds) Digitalization, Digital Transformation and Sustainability in the Global Economy. Springer Proceedings in Business and Economics. Springer, Cham. https://doi.org/10.1007/978-3-030-77340-3_4
104. Khanal, S., Zhang, H., & Taeihagh, A. (2024). Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. Policy and Society, puae012. https://doi.org/10.1093/polsoc/puae012
105. Raghavendra, G.S., Shankar Lingam, M., Vanishree, J. (2021). ICT for

Good Governance: Evidence from Development Perspective. In: Kaiser, M.S., Xie, J., Rathore, V.S. (eds) Information and Communication Technology for Competitive Strategies (ICTCS 2020). Lecture Notes in Networks and Systems, vol 190. Springer, Singapore. https://doi.org/10.1007/978-981-16-0882-7_55

106. Stötzel, C. (2020). Political Implications of the Digital Transformation – The Role of the Democratic State in Multi-Stakeholder Internet Governance. In: Oswald, M., Borucki, I. (eds) Demokratietheorie im Zeitalter der Frühdigitalisierung. Springer VS, Wiesbaden. https://doi.org/10.1007/978-3-658-30997-8_14
107. National Institute of Standards and Technology. (2022). Supply Chain Risk Management Practices for Federal Information Systems. NIST Special Publication 800-161 Rev. 1, Update 1.
108. Letizia, P., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. Crime, Law and Social Change, 70(4), 397–420.
109. Colicchia, C., Creazza, A., & Menachof, D. (2018). Managing Cyber and Information Risks in Supply Chains: Insights from an Exploratory Analysis.
110. Gokkaya, B., Aniello, L., Karafili, E., Halak, B. (2024). A Methodology for Cybersecurity Risk Assessment in Supply Chains. In: Katsikas, S., et al. Computer Security. ESORICS 2023 International Workshops. ESORICS 2023. Lecture Notes in Computer Science, vol 14399. Springer, Cham. https://doi.org/10.1007/978-3-031-54129-2_2
111. Taherdoost, H. (2024). Insights into Cybercrime Detection and Response: A Review of Time Factor. Information, 15(5), 273. https://doi.org/10.3390/info15050273
112. Badis Hammi, Sherali Zeadally, Jamel Nebhen. Security threats, countermeasures, and challenges of digital supply chains. ACM Computing Surveys, 2023, 55 (14s), pp.1-40. 10.1145/3588999.
113. JOSEPH,NNAMDI,TheGrowingThreatofSupplyChainCyberattacks: Resilience Strategies (November 24, 2023). Available at SSRN: https://ssrn.com/abstract=4643716 or http://dx.doi.org/10.2139/ssrn.4643716
114. M. Z. Hasan, M. Z. Hussain, I. Alam, N. Sarwar, A. M. Qureshi and A.

Irshad, “Impact of Cybercrime on Enterprises in Cloud Computing Environment: A Review,” 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T), Bahawalpur, Pakistan, 2023, pp. 1-6, doi: 10.1109/ICEST56843.2023.10138873.
115. Ulnicane, I. (2024). Governance fix? Power and politics in controversies about governing generative AI. Policy and Society, puae022. https://doi.org/10.1093/polsoc/puae022
116. Sarangi, A.K., Pradhan, R.P. ICT infrastructure and economic growth: a critical assessment and some policy implications. Decision 47, 363–383 (2020). https://doi.org/10.1007/s40622-020-00263-5
117. Okhrimenko, I., Stepenko, V., Chernova, O. et al. The impact of information sphere in the economic security of the country: case of Russian realities. J Innov Entrep 12, 67 (2023). https://doi.org/10.1186/s13731-023-00326-8
118. Geiger, G. (2014). ICT Security Risk Management: Economic Perspectives. Position Papers of the 2014 Federated Conference on Computer Science and Information Systems, 3, 119–122. https://doi.org/10.15439/2014F439
119. OECD (2024), “Review of relevance of the OECD Recommendation on ICTs and the Environment”, OECD Digital Economy Papers, No. 370, OECD Publishing, Paris, https://doi.org/10.1787/216766c6-en.
120. Kirishchieva, I., Skorev, M., Mishchenko, O., Grafova, T., (2021). Risks and threats to economic security in the digital economy. SHS Web of Conferences, 111, Article 001028. https://doi.org/10.1051/shsconf/202111001028
121. Franco, M., Omlin, C., Kamer, O., (2023). SECAdvisor: a Tool for Cybersecurity Planning using Economic Models. arXiv preprint arXiv:2304.07909.
122. Keiras, T., Farooq, M., Zhu, Q., (2019). RIoTS: Risk Analysis of IoT Supply Chain Threats. arXiv preprint arXiv:1911.12862.