تاریخ دریافت: ۱۴۰۳/۰۱/۱۵ تاریخ پذیرش: ۱۴۰۳/۰۵/۲۰ صفحه ۴۰ تا ۶۷

تبیین ابعاد و مولفه‌های اثرگذار فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات بر امنیت داخلی

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

چکیده

امنیت داخلی به عنوان ستون فقرات ثبات و رفاه جامعه، همواره محور مهمی در برنامه‌ریزی‌های کلان کشوری به شمار می‌رود. در عصر حاضر، با توسعه فناوری‌های پیشرفته به ویژه در حوزه فناوری اطلاعات و ارتباطات، شاهد تاثیر گسترده‌ای بر ابعاد مختلف امنیت داخلی هستیم. این تحقیق به دنبال شناخت و تحلیل نقش شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات در تقویت یا تضعیف امنیت داخلی است. توجه به چگونگی تعامل این شرکت‌ها با مولفه‌های امنیتی و تاثیرات ناشی از آن‌ها، می‌تواند در شناسایی فرصت‌ها و چالش‌های پیش روی امنیت داخلی موثر باشد. با تحلیل متون علمی داخلی و خارجی و مصاحبه با ۲۱ نفر از نخبگان حوزه امنیت و فناوری اطلاعات و ارتباطات، ۷ بعد توسعه محصول و توسعه 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 شناسایی شدند و مدل مفهومی آن در تحقیق ارائه شده است.

واژگان کلیدی: امنیت داخلی، شرکت‌های فناور، فناوری اطلاعات و ارتباطات

۱. استادیار گروه جغرافیای سیاسی دانشگاه دفاع ملی-تهران (نویسنده مسئول)amelhami@yahoo.com
۲. دانشیار گروه سایبر دانشگاه عالی دفاع ملی
۳. پژوهشگر ارشد اقتصاد

Explanation of the effective parameters and dimensions of the activities of technology companies in the field of information and communication technology on internal security

Amir Hussein Elhami[1], Mohamad Reza Movadedi Sefat[2],

Mohammad Norouz Zadeh3

Abstract

Internal security, as the backbone of society's stability and well-being, is always considered an important axis in national macro-planning. In today's era, with the development of advanced technologies, especially in the field of information and communication technology (ICT), we see a wide impact on various aspects of internal security. This research seeks to identify and analyze the role of technology companies in the field of information and communication technology in strengthening or weakening internal security. Paying attention to how these companies interact with security components and their effects can be effective in identifying opportunities and challenges facing national security. By analyzing domestic and foreign scientific texts and interviewing 12 elites in the field of security and information and communication technology, 7 dimensions of product development and technology development, data management and analysis, connection and communication infrastructure, monitoring capabilities including content monitoring and monitoring on performance, legal participation and social responsibility, globalization and market expansion and international and domestic cooperation were identified and its theoretical model is presented in the research.

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

1. Assistant Professor, Geopolitics, Nataional Defense University, Tehran (corresponding author) amelhami@yahoo.com

2. Associate Professor. Cyber Department, National Defense University

3. Senior Researcher in Economics

۱. مقدمه و بیان مسئله

رشـــد سریع فناوری اطلاعات و ارتباطات شـــیوه ارتباط افراد، دسترسی به اطلاعات و تعامل با یکدیگـــر را تغییر داده اســـت. در حالی که این فناوری‌ها مزایای متعددی را به همراه داشـــته‌اند، نگرانی‌هایـــی را در مورد حریم خصوصی و آزادی‌های مدنی نیز ایجاد کرده‌اند. یکی از نگرانی‌های اصلی مرتبط با تاثیر شرکت‌های فناوری اطلاعات و ارتباطات در مورد حریم خصوصی، جمع‌آوری و استفاده از داده‌های شخصی است. یکی دیگر از زمینه‌های نگرانی، پتانسیل نظارت دولت است. شـــرکت‌های فناور به اطلاعاتی دسترســـی دارند که می‌تواند توسط دولت‌ها برای نظارت بر افراد و پیگیری فعالیت‌های آن‌ها استفاده شود. با توجه به اینکه جمع‌آوری داده و تعامل بین شرکت‌های فنـــاور و دولـــت در آینده ادامه پیدا خواهد کرد، در صورتی‌که به این نگرانی‌ها به‌صورت مناســـب پاســـخ داده نشود، اعتماد بین شهروندان، شرکت‌های فناور و دولت از بین خواهد رفت که این امر به امنیت داخلی لطمه می‌زند.

شرکت‌های فناور می‌توانند با فراهم آوردن و تسهیل دسترسی به اطلاعات و ابزارهای ارتباطی، نقش بسزایی در شکل دادن به هنجارها و ارزش‌های اجتماعی ایفا کنند. به عنوان مثال، پلتفرم‌های رســـانه‌های اجتماعی را می‌توان برای تسهیل ارتباط افراد با پیشینه‌های مختلف، ایجاد همگرایی در نظرات و یا دامن زدن به تفرقه و درگیری ، انتشـــار اطلاعات نادرســـت ، هماهنگی اعتراضات سیاسی، حملات سایبری و حتی اقدامات تروریستی استفاده کرد. علاوه بر این، شرکت‌های فناور اغلب به حجم وسیعی از داده‌های شخصی دسترسی دارند که می‌توان از آن برای پروفایل و هدف قرار دادن افراد بر اســـاس دیدگاه‌های سیاســـی، اجتماعی یا فرهنگی آن‌ها اســـتفاده کرد. این کار می‌تواند تهدیدی قابل توجه برای حریم خصوصی و آزادی بیان باشد و همچنین می‌تواند با تضعیف مشروعیت نهادهای دولتی و فرآیندهای دموکراتیک، باعث تضعیف دموکراسی شود.

شـــرکت‌های فناور نقش مهمی در شـــکل دادن به اقتصاد دیجیتال دارند و در نتیجه نفوذ آن‌ها می‌تواند پیامدهای مهمی برای امنیت داخلی داشته باشد. یکی از راه‌هایی که شرکت‌های فناور از طریق اقتصاد دیجیتال می‌توانند بر امنیت داخلی اثرگذار باشند، ایجاد مراکز جدید قدرت اقتصادی است. به عنوان مثال، این شرکت‌ها حجم وسیعی از داده‌ها را کنترل می‌کنند و توانایی شکل دادن به رفتار مصرف‌کننده و افکار عمومی را دارند که می‌تواند تاثیر قابل توجهی بر چشم‌انداز سیاسی داشـــته باشد. همچنین اقتصاد دیجیتال از طریق ظهور مدل‌ها و شیوه‌های اقتصادی جدید مانند اقتصاد اشـــتراک‌گذاری و اقتصاد گیگ، می‌تواند روی امنیت داخلی اثرگذار باشـــد. این مدل‌ها،

سیستم‌های اقتصادی سنتی را به چالش می‌کشند و می‌توانند منجر به تغییراتی در بازار کار شوند. به عنوان مثال، اقتصاد گیگ[1] به دلیل ایجاد مشـــاغل کم‌درآمد و بی‌ثبات مورد انتقاد قرار گرفته اســـت که می‌تواند منجر به افزایش ناامنی اجتماعی و اقتصادی شـــود که می‌تواند امنیت داخلی را تضعیف کند. شـــرکت‌های فناور از طریق اثرگذاری بر نحوه توســـعه، توزیع و استفاده از فناوری می‌توانند تاثیر عمیقی بر سطح نابرابری در یک جامعه داشته باشند؛ «شکاف دیجیتال» به شکاف بین افرادی که به فناوری‌های دیجیتال دسترسی دارند و کسانی که دسترسی ندارند، اشاره دارد. این شکاف می‌تواند تاثیر عمیقی بر نابرابری داشته باشد، زیرا کسانی که به این فناوری‌ها دسترسی ندارند، احتمالا طیف وســـیعی از مزایا، از جمله دسترسی بهتر به آموزش و فرصت‌های شغلی را از دســـت خواهند داد. همچنین رشد اقتصاد اشتراک‌گذاری چالش‌های جدیدی در امنیت سایبری ایجاد کرده اســـت، به‌ویژه با توجه به اشتراک‌گذاری داده‌های شخصی، انتقال داده‌های حساس به فضای ابری نیز چالش‌های امنیتی جدیدی را ایجاد کرده است، از جمله نیاز به ایمن‌سازی داده‌ها و زیرساخت‌هایی که از آن پشتیبانی می‌کند.

در نهایت، در دنیایی که به‌طور فزاینده‌ای به هم پیوسته و دیجیتالی می‌شود، شرکت‌های فناور در بخش فناوری اطلاعات به بازیگران حیاتی در پیشـــبرد رشد اقتصادی، نوآوری و پیشرفت اجتماعی تبدیل شده‌اند. با تکامل چشم‌انداز دیجیتال، دولت‌ها با چالش مبرم تضمین امنیت داخلی و در عین حال پرورش محیطی که نوآوری و شـــکوفایی اقتصادی را پرورش می‌دهد، مواجه می‌شـــوند. از این رو، مساله اصلی این پژوهش، فقدان درک جامع از نقاط قوت و ضعف امنیت داخلی ناشی از فعالیت شـــرکت‌های فناور در حوزه فناوری اطلاعات اســـت تا بتوان متناسب با آن، سازوکارهای لازم برای پیش‌بینی، پیش‌گیری، تقویت و مقابله با چالش‌ها را تمهید و مانع از اخلال در امنیت داخلی شـــد. یافته‌های این تحقیق، بینش‌هایی را برای سیاست‌گذاران، سازمان‌های دولتی و ذینفعان صنعت فراهم می‌کند و آن‌ها را قادر می‌سازد تا اقدامات پیشگیرانه، تقویت مشارکت‌ها و تضمین امنیت بلندمدت و شـــکوفایی اکوسیســـتم دیجیتال را انجام دهند. به همین منظور هدف تحقیق تبیین نظری ابعاد و مولفه‌های اثرگذار فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات بر امنیت داخلی است.

۲. پیشینه‌شناسی تحقیق

در این قسمت به بررسی برخی از مقالات و پژوهش‌های مرتبط با تحقیق حاضر می‌پردازیم.

1. Gig economy

پژوهش مسیبی ملک خیل با بهره‌گیری از روش داده‌بنیاد و فرایند تحلیل شبکه‌ای، ابعاد، مولفه‌ها و شاخص‌های 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

می‌شـــود، شـــایعه 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] آســـیب‌پذیری‌های زیرســـاخت‌های حیاتی مانند سیســـتم‌های 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 شـــده 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 ناشـــی از حمله ســـایبری از جمله پروتکل‌های امنیتی قوی‌تر، سیستم‌های نظارتی و سیاست‌هایی برای محافظت از خدمات حیاتی توصیه شده است. (ریگز، ۲۰۲۳)

مقاله آســـوگوا[2] بیان می‌کند که رســـانه‌های ارتباطی مبتنی بر اینترنت، از جمله شـــبکه‌های 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 اســـتفاده از این بســـترها برای رادیکال‌سازی افراد، جذب و آموزش نیروها، تامین مالی فعالیت‌هایی که تهدیدی برای امنیت هســـتند و انتشـــار پیام‌های تحریک‌آمیز اشـــاره کرد که تمامی این موارد می‌توانند به تضعیف امنیت ملی منجر شـــوند. از سوی دیگر، این رســـانه‌ها می‌توانند به‌عنوان ابزار موثری در ایجاد آگاهی و هوشـــیاری عمومی نسبت به تهدیدات امنیت ملی عمل کنند. از طریق استفاده صحیح از این بسترها، امکان اطلاع‌رسانی گسترده در مورد تهدیدات امنیتی، افزایش هوشیاری عمومی و ایجاد آمادگی در مواجهه با خطرات احتمالی وجود دارد. بر اساس نتایج این پژوهش، یکی از پیشنهادات کلیدی، ایجاد هم‌افزایی بین رسانه‌های سنتی همچون رادیو، تلویزیون، روزنامه‌ها و مجلات با نهادهای امنیتی است تا از این طریق آگاهی عمومی نســـبت به امنیت ملی افزایش یابد و هوشـــیاری لازم در میان مردم تقویت شود. (آسوگوا، ۲۰۲۰)

---

1. Riggs et. al
2. Asogwa

همچنین، گزارش پلتفرم مقررات دیجیتال (۲۰۲۱)[1] رویکردهای سیاستی و مقرراتی برای تقویت تاب‌آوری سایبری زیرساخت‌های حیاتی را بررسی می‌کند. این گزارش به لزوم همکاری میان بخش خصوصی و دولت در جهت حفاظت از زیرساخت‌های اطلاعاتی اشاره می‌کنند و بر اهمیت تکامل سیاست‌های ملی امنیت سایبری با پیشرفت‌های فناوری و تهدیدات نوظهور تاکید دارند.

مطالعات بررسی‌شده نشان می‌دهد که عوامل متعددی بر امنیت داخلی تاثیرگذارند و فناوری اطلاعات و ارتباطات نقش به‌سزایی در این زمینه دارد. برنامه‌ریزی راهبردی، 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 فناور نپرداخته‌اند. پژوهش حاضر با استفاده از روش توصیفی-تحلیلی به بررسی 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 می‌شود. در نهایت در بخش سوم جهت 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 سلبی و ایجابی تعریف کرد. در نگاه سلبی، امنیت ملی به وضعیتی اشاره دارد که منافع حیاتی یک بازیگر از سوی دیگران تهدید نشود یا در صورت وجود تهدید، توانایی دفع و مدیریت آن وجود داشته باشد. از دیدگاه ایجابی، امنیت ملی به معنای

1. Digital Regulation Platform

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 می‌کننـــد، در حالی که دیدگاه دیگری آن را به عنـــوان توانمندی بهره‌گیری از فرصت‌ها و تضمین منافع و ارزش‌ها می‌داند(عبیری و همکاران، ۱۳۹۹: ٤٤٤) (حبیب‌زاده، ۱۳۹۸: ۱۱).

امنیت داخلی، به عنوان بخشـــی از امنیت ملی، بـــه جنبه‌های داخلی امنیت مانند انتظام ملی، ثبات سیاسی، رونق اقتصادی و حقوق فردی می‌پردازد. این مفهوم بر وجود انتظام ملی مبتنی بر قواعد حقوقی و قانون اساسی استوار است. امنیت داخلی علاوه بر یک پدیده اجتماعی، یک احساس درونی است که فرد را به آینده متوجه می‌کند و ضامن بقای فرد و جامعه است. این مفهوم با تمامی ابعاد زندگی اجتماعی، از جمله مســـائل فرهنگی، اجتماعی، حقوقی و اقتصادی ارتباط تنگاتنگ دارد و در امنیت سیاسی و مشارکت سیاسی مردم با دولت تجلی می‌یابد(علیزاده، ۱٤۰۰: ۱٦۸)

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 بررســـی اثر فعالیت شـــرکت‌های 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 قســـمت ابتدا اثر فعالیت شـــرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات بر امنیت داخلی در ابعاد اقتصادی، سیاســـی، فرهنگی، اجتماعی، نظامی و زیست‌محیطی بررسی شده‌اند و در ادامه بر اســـاس مقالات و پژوهش‌های معتبر، ابعاد و مولفه‌های اثرگذاری شـــرکت‌های فناور بر امنیت داخلی استخراج شده‌اند.

- **فنـــاوری اطلاعات و ارتباطات و امنیت اجتماعی:** امنیت اجتماعی به حفاظت از جامعه در برابر تهدیدات و ناهنجاری‌ها اطلاق می‌شـــود تا افراد، خانواده‌ها و جامعه از ســـلامت و امنیت زندگی خود مطمئن باشند. این امنیت در دو بعد عینی و ذهنی تعریف می‌شود و شامل تامین نیازهای مادی و معنوی افراد اســـت. شـــرکت‌های فناور اطلاعات و ارتباطات نقش مهمی در شکل‌دهی به مسائل اجتماعی ایفا می‌کنند و با محصولات و فناوری‌های خود جامعه را تغییر داده‌اند. این تغییرات شامل اتصال اجتماعی، شکاف دیجیتال، آموزش الکترونیکی، دسترسی به دانش، ســـلامت و تندرســـتی دیجیتال، گفتمان عمومی، حریم خصوصی و نظارت، تاثیر

فرهنگی و جهانی شدن است. رسانه‌های اجتماعی با وجود کمک به تعاملات جهانی و ارتقای آگاهی، می‌توانند منجر به اطلاعات نادرســت و قطبی‌سازی اجتماعی شوند. امنیت اجتماعی نیز به میزان زیادی تحت تاثیر ســرمایه اجتماعی اســت که شامل اعتماد، مشارکت و انسجام اجتماعی می‌شود. در جامعه‌های در حال توسعه، تغییرات ارزشی و هنجاری می‌تواند منجر به کاهش ســرمایه اجتماعی و افزایش ناامنی اجتماعی شود. در نهایت، برای دستیابی به امنیت اجتماعی پایدار، باید به اصلاح کارکرد نظام‌های اجتماعی، فرهنگی، سیاسی و اقتصادی توجه کرد. (سماواتیان، ۱۳۹۷: ۷) (مرکز مطالعات جامعه و امنیت، ۱۳۹۸[1]).

- **فناوری اطلاعات و ارتباطات و امنیت سیاســی:** امنیت سیاســی به معنای تامین آرامش و اطمینان شــهروندان توســط حکومت، از طریق حفاظت در برابر تهدیدات خارجی و تضمین حقوق سیاسی آن‌ها در تعیین سرنوشت است. نظام سیاسی باید حضور آزادانه و برابر شهروندان در فضای سیاســی را تضمین کرده و اجازه بیان آزادانه عقاید سیاسی را بدهد. امنیت سیاسی بــا برابری در مقابل قانون و آزادی از اجبار به باورهای خاص مرتبط اســت و در حکومت‌های خودکامه تحقق نمی‌یابد. مقبولیت حکومت از ارکان اصلی امنیت ملی و تداوم نظام سیاســی اســت. حکومت‌ها باید رفاه و امنیت شــهروندان را تامین و به خواست‌های مشروع آن‌ها پاسخ دهنــد تا مقبولیت و حمایت مردمی را کســب کنند. رســانه‌های اجتماعــی نیز می‌توانند به عنوان ابزاری برای گفتمان عمومی و مشــارکت سیاســی عمل کنند، اما در عین حال مستعد دست‌کاری و انتشار اطلاعات نادرست هستند. شرکت‌های فناور حوزه فناوری اطلاعات نقش مهمی در این زمینه دارند، از جمله تسهیل دسترسی به اطلاعات، مقابله با اطلاعات نادرست، حفاظت از انتخابات و همکاری با دولت‌ها در مســائل امنیتی. توازن بین امنیت و حفظ حقوق فردی برای ثبات سیاســی و دموکراسی حیاتی است. همچنین، تغییرات ژئوپلیتیکی، افزایش رقابت قدرت‌های بزرگ، نفوذ بازیگران غیردولتی، و رشد ناسیونالیسم و پوپولیسم از مهم‌ترین خطرات آینده در بعد سیاســی محسوب می‌شوند(ترابی و همکاران، ۱۴۰۰: ۱۱۱)(دستغیب، ۱۳۹۶)(خانقاهی و آزادی، ۱۴۰۰: ۱۳۲).
- **فناوری اطلاعــات و ارتباطات و امنیت فرهنگی:** فرهنگ مجموعــه‌ای از عادت‌ها، باورها، ارزش‌ها و اعتقادات مشــترک در میان مردم یک کشور است و با مفهوم هویت (شامل باورهای دینی، سنت‌های ملی یا حرفه‌ای و انواع عقاید جمعی) ارتباط تنگاتنگی دارد. امنیت فرهنگی،

1. www.ihcs.ac.ir

که بخشـــی از امنیت داخلی محســـوب می‌شود، بر حفاظت از ارزش‌ها، هویت و فرهنگ جامعه تمرکز دارد. جهانی‌شدن و انقلاب اطلاعاتی اثر قابل توجهی بر امنیت فرهنگی داشته‌اند به ویژه در تعارض بین فرهنگ ملی و روند یکسان‌سازی فرهنگی جهانی. رابرت ماندل[1] امنیت فرهنگی را بخشی از امنیت ملی می‌داند که با ابعاد سیاسی و اجتماعی آن مرتبط است. در بعد سیاسی، امنیت فرهنگی به باورها و ارزش‌های حکومت و در بعد اجتماعی به همزیســـتی مســـالمت‌آمیز خرده فرهنگ‌ها مربوط می‌شـــود. شرکت‌های فناور اطلاعات و ارتباطات از طریق محصولات و خدمات خود بر ارتباطات، هنجارها و بیان فرهنگی تاثیر می‌گذارند. آن‌ها به تسهیل ارتباطات جهانـــی، ایجاد اجتماعات آنلاین و تغییر ســـبک زندگی کمـــک کرده‌اند و همچنین در حفظ زبان‌ها و حافظه فرهنگی نقش دارند. با این حال، تاثیر جهانی این شرکت‌ها نگرانی‌هایی درباره امپریالیسم فرهنگی و همگن‌سازی فرهنگ‌ها ایجاد کرده است. فناوری‌های اطلاعاتی و ارتباطی بـــه حفظ میراث فرهنگی و تداوم آن کمک می‌کنند، اما انتشـــار اخبار جعلی و ایدئولوژی‌های افراطی نیز می‌تواند تهدیدی برای امنیت داخلی کشـــورها باشـــد. در نهایت، فناوری می‌تواند هم در تقویت و هم در به چالش کشـــیدن هنجارهای فرهنگی موجود نقش داشـــته باشـــد، که این تاثیرات می‌تواند به مشـــارکت مدنی و تغییرات اجتماعی منجر شود(محرمی، ۱۳۹۷: ٦۹) (رضاپور و اسکندری‌نسب، ۱۳۹۸: ۳۹۷) (پورسعید، ۱٤۰۱: ۱۸۲-۱۸٤).

- **فنـــاوری اطلاعات و ارتباطات و امنیت اقتصادی:** امنیت اقتصادی از تعامل بین امنیت ملی و اقتصاد ناشـــی می‌شـــود و به وضعیت پایدار و آینده‌ی مشخص در اقتصاد اشاره دارد. امنیت اقتصادی شامل شـــش حوزه اصلی: نهادهای کارآمد، قوانین، سیاست‌گذاری، رشد اقتصادی، ســـرمایه‌گذاری، و عدم اطمینان به آینده اســـت. عوامل تهدیدکننده امنیت اقتصادی شامل قاچاق کالا و ارزهای مجازی هستند. رشد اقتصادی و ظهور طبقات اجتماعی جدید، تاثیرات مختلفی بر امنیت اقتصادی دارند. همچنین، نقش شـــرکت‌های فناوری اطلاعات و ارتباطات در تغییر چشم‌انداز اقتصادی جهانی برجسته شده است. شرکت‌های حوزه فناوری اطلاعات و ارتباطات باعث نوآوری و افزایش بهره‌وری شـــده‌اند و بازارهای جدیدی مانند بازار دیجیتال و اقتصاد گیگ ایجاد کرده‌اند. همچنین، این شرکت‌ها اثر قابل توجهی بر اشتغال، بازارهای مالی، تجارت بین‌المللی و صنایع سنتی دارند. نوآوری‌های این شرکت‌ها در فین‌تک، تحلیل داده‌ها و تجارت الگوریتمی، مدل‌های اقتصادی را تغییر داده و رقابت را تقویت کرده‌اند. اســـتفاده از

1. Robert Mundell

فناوری اطلاعات و ارتباطات توسط شرکت‌های فناور دسترسی به آموزش و خدمات را بهبود داده، کارایی فرآیندهای درمانی را افزایش داده و به کاهش نابرابری‌ها کمک کرده‌اند. در نهایت، نقش شرکت‌های فناور در امنیت اقتصادی به‌عنوان محرک نوآوری و تغییر ساختارهای بازار، مهم تلقی می‌شـــود(صیدی، ۱۳۹۹: ۲۹۰) (محمدی‌نیا ســـماکوش و صبح‌خیز، ۱۴۰۱: ۲۳) (شهبازی، ۱۳۹۹: ۲۸ و عامری و همکاران (۱۴۰۱).

- **فناوری اطلاعات و ارتباطات و امنیت زیست‌محیطی:** امنیت زیست‌محیطی به حفظ محیط زیســـت و منافع حیاتی انسان‌ها در برابر تاثیرات منفی توسعه، تخریب محیط زیست، و جنگ می‌پردازد. مسائل زیست‌محیطی مانند کاهش منابع آبی، اگروتروریسم، سدسازی غیراصولی، و پدیده ریزگردها می‌توانند به مشکلات امنیتی منجر شوند و نیاز به همکاری بین‌المللی دارند. شـــرکت‌های فناوری اطلاعات و ارتباطات در خط مقدم نوآوری و توســـعه پایدار هستند. این شـــرکت‌ها با تولید زباله‌های الکترونیکی، کنترل مصرف انرژی مراکز داده، و ارائه راه‌حل‌های هوشمند برای مدیریت زیست‌محیطی مانند شبکه‌های هوشمند و اینترنت اشیا در کشاورزی، نقش مهمی در امنیت زیست‌محیطی دارند. آن‌ها همچنین در زمینه محاسبات سبز، استفاده از انرژی‌هـــای تجدیدپذیـــر، و زنجیره‌های تامین پایدار فعالیت می‌کنند. تحولات دیجیتال در زمینه کشـــاورزی پایدار، جنگل‌داری، بهره‌وری منابع و مواد خام، دسترســـی به هوای پاک، آب پـــاک و مدیریت بهینه پســـماندها نقش مهمی دارنـــد. در نهایت، فناوری‌های دیجیتال و نوآوری‌های شـــرکت‌های حوزه فناوری اطلاعات و ارتباطات می‌توانند به کاهش تغییرات آب و هوایـــی، بهره‌وری منابع، و افزایش آگاهی زیســـت‌محیطی کمک کنند. همکاری با دولت‌ها و ســـازمان‌های غیردولتی برای توســـعه راه‌حل‌های زیســـت‌محیطی و کاهش تاثیرات منفی فناوری‌های دیجیتال بر محیط زیســـت نیز اهمیت دارد(عباس‌زاده و منصوری، ۱۳۹۸: ۳۰۱ و قـــوام و مصطفـــوی، ۱۳۹۷: ۱۰) (ذکی و نجفـــی، ۱۳۹۹: ۱۴۰ و یزدان پناه درو و همکاران، ۱۳۹۷: ۴۰).
- **فناوری اطلاعات و ارتباطات و امنیت دفاعی و امنیتی:** با تغییرات در گفتمان امنیتی، جنگ‌های داخلی میان گروه‌های مذهبی، نژادی و قومی با دولت‌ها جایگزین جنگ‌های سنتی دولت علیه دولت شـــده‌اند. رئالیســـت‌ها به اهمیت فناوری اطلاعات و ارتباطات در جمع‌آوری اطلاعات و جنگ روانی و توسعه تکنولوژی‌های نظامی مانند هواپیماها و ماهواره‌های نظامی اشاره دارند. فناوری‌های دفاعی مهم شامل ســـامانه‌های هوشمند، رشد فناوری‌های سایبری، سامانه‌های

بدون سرنشین، فناوری‌های فضایی، اینترنت اشیا و انرژی‌های نو هستند. شرکت‌های فناوری اطلاعات و ارتباطات نقش مهمی در تامین سخت‌افزار و نرم‌افزارهای نظامی، سیستم‌های نظارت و شناسایی، دفاع سایبری، هوش مصنوعی و سلاح‌های خودکار دارند. این شرکت‌ها همچنین ارتباطات امن، جنگ شبکه‌محور، آموزش و شبیه‌سازی نظامی، مدیریت زنجیره تامین و فناوری‌های لجستیکی را فراهم می‌کنند. با توجه به استفاده دوگانه از فناوری‌ها، مباحث اخلاقی و حقوقی نیز مطرح می‌شوند. شرکت‌های فناور در توسعه سیستم‌های دفاعی، امنیت سایبری، اطلاعات و نظارت، سیستم‌های فرماندهی و کنترل، آموزش و شبیه‌سازی، و مدیریت زنجیره تامین نقش دارند. این مشارکت‌ها نیازمند استفاده مسئولانه و پایبندی به هنجارهای بین‌المللی برای تضمین امنیت ملی و اخلاقی است(سلطانی‌نژاد و همکاران، ۱۳۹۵: ۲۹) (پورعزت و عبدی، ۱۳۹۷: ۷۱)(گودرزی و اجلالی (۱۴۰۰).

- **فناوری اطلاعات و ارتباطات و امنیت سایبری:** امنیت اطلاعات شامل حفاظت از محرمانگی، یکپارچگی و دسترسی به داده‌ها است. با پیشرفت فناوری اطلاعات، تهدیدات سایبری نیز افزایش یافته‌اند و می‌توانند به دولت‌ها، شرکت‌ها و جامعه آسیب بزنند. امنیت سایبری بر پیشگیری و مقابله با حملات سایبری تمرکز دارد، در حالی که امنیت اطلاعات بر حفاظت از داده‌ها. تهدیدات سایبری شامل سرقت هویت، حملات به زیرساخت‌های حیاتی و جاسوسی است. شاخص جهانی امنیت سایبری پنج رکن اصلی دارد: اقدامات قانونی، فنی، سازماندهی، ظرفیت‌سازی و همکاری. این شاخص‌ها برای محافظت از محیط سایبری و دارایی‌های سایبری ضروری هستند. امنیت در شبکه ملی اطلاعات به معنای حفاظت از تمامی لایه‌های شبکه و تضمین امنیت برای فضای مجازی کشور است. شرکت‌های فناور با توسعه راه‌حل‌های امنیتی، بهبود دسترسی به اطلاعات تهدید، ترویج شیوه‌های توسعه امن، آموزش و آگاهی، همکاری با نهادهای مختلف، ارائه زیرساخت امن ابری و حمایت قانونی، نقش مهمی در امنیت سایبری ایفا می‌کنند. چالش‌ها و فرصت‌های امنیت سایبری در شرکت‌های فناوری اطلاعات و ارتباطات شامل ریسک زنجیره تامین، جرائم سایبری، اشتراک‌گذاری داده‌ها و انتقال داده‌های حساس به فضای ابری است. فناوری‌های نوظهور مانند هوش مصنوعی، یادگیری ماشینی و بلاک‌چین نیز در بهبود امنیت سایبری نقش دارند. همکاری بین بخش‌های دولتی و خصوصی و توسعه چارچوب‌های قانونی و مقرراتی جامع برای هدایت استفاده مسئولانه از این فناوری‌ها

ضروری است(اختری و همکاران، ۱۴۰۱: ۲۲)(رهامی و اژدری، ۱۴۰۱: ۲۷۷) (سعادتمند و همکاران، ۱۴۰۰: ۱۲) (سند افتا[1]).

- **فناوری اطلاعـــات و ارتباطات و امنیت حقوقی:** تغییرات اجتماعی باعث افزایش قوانین و مشـــکلاتی مانند تعدد قوانین، پراکندگی، پیچیدگی و ابهام شـــده است. اصل امنیت حقوقی، بر پیش‌بینی‌پذیری و قابلیت اتکای تصمیمات حاکمیت تاکید دارد که نیازمند انتشـــار، دسترســـی آســـان، انسجام و شفافیت قوانین اســـت. امنیت قضایی نیز بر حمایت قانونی و قضایی از حقوق و اعتماد شهروندان تاکید دارد و به ثبات و پیش‌بینی‌پذیری نظام حقوقی کمک می‌کند. شرکت‌های فناور با ارائه محصولات و خدمات جدید می‌توانند مصرف‌کنندگان را دچار مشـــکل کنند، لذا نیاز به به‌روزرســـانی قوانین وجـــود دارد. همچنین، مالکیت فکری به‌عنوان زیرســـاخت کلیدی برای توســـعه کســـب‌وکار، به شـــرکت‌ها کمک می‌کند تا از نوآوری‌های خود محافظت کرده و از آن‌ها ارزش‌افزایـــی کنند. این امـــر در اقتصاد دانش‌بنیان اهمیت زیـــادی دارد و حقوق مالکیت فکری به‌عنوان «ارز فکری» نقش مهمی در رشد اقتصادی و رقابت‌پذیری ایفا می‌کند. شرکت‌های فناور نقش چشمگیری در امنیت حقوقی و قضایی دارند که از جمله آن‌ها می‌توان توسعه راه‌حل‌های فنی برای بهبود فرآیندهای حقوقی و قضایی، بهبود دسترسی به اطلاعات حقوقی از طریق پلتفرم‌ها و ابزارهای آنلاین، تسهیل حل و فصل اختلافات حقوقی به‌صورت آنلاین و در نظر گرفتن پیامدهای اخلاقی در توسعه و استقرار راه‌حل‌های فنی اشاره کرد. در مجموع، همکاری بین شرکت‌های فناور، متخصصان حقوقی و نهادهای نظارتی برای بهره‌گیری از فناوری و حفظ اصول عدالت و حاکمیت قانون ضروری است(پروین و فرامرزی، ۱۳۹۹: ۹۶) (سند امنیت قضایی، ۱۳۹۹[2]).

۳.۳. نظریات حوزه فناوری اطلاعات و ارتباطات و امنیت داخلی

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

1. https://rc.majlis.ir/fa/law/show/135835
2. https://rc.majlis.ir/fa/law/show/1623986

کتـــاب «موج ســـوم»[1] آلوین تافلر[2] تغییرات اجتماعی را در ســـه مـــوج 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 شـــدن دانش و نیاز به ســـازگاری بیشـــتر با تغییرات سریع خواهد شـــد. او همچنین چالش‌های زیست‌محیطی و اجتماعی جدیدی را به همراه این تغییرات پیش‌بینی کرد.

جبر تکنولوژیک، مفهومی که توســـط اســـمیت و مارکس[3] مطرح شده، به عنوان چارچوبی برای تحلیل اثرات فناوری بر تغییرات اجتماعی و ســـازگاری ســـازمانی عمل می‌کند. این نظریه فرض می‌کند که توســـعه فناوری محرک کلیدی تغییر اجتماعی و ســـازگاری ســـازمانی است. در حوزه امنیت داخلی، این نظریه کمک می‌کند تا روشـــن شـــود که چگونه پیشرفت‌های فناوری اطلاعات و ارتباطات نه تنها قابلیت‌های امنیتی را افزایش داده اســـت، بلکه تکامل اســـتراتژی‌های امنیتی را نیز دیکته کرده اســـت. از اقدامات امنیت ســـایبری گرفته تا سیستم‌های نظارتی، نقش فناوری در شکل‌دهی به زیرســـاخت‌های امنیتی و پاسخگویی، تجسم آشکاری از جبر فناوری است(اسمیت و مارکس، ۱۹۹٤).

نظریـــه سیســـتم‌های اجتماعی[4] تریســـت و بامفورث[5] بـــر تعاملات متقابل و پیوســـتگی میان سیســـتم‌های اجتماعی (مانند ساختارهای ســـازمانی، هنجارهای فرهنگی و رفتارهای انسانی) و سیســـتم‌های فنـــی (مانند ابزارهـــا و پلتفرم‌های دیجیتال) تاکیـــد دارد. در زمینه امنیت داخلی، به‌کارگیری این نظریه نشـــان می‌دهد که اســـتراتژی‌های امنیتی موثر باید هم به قابلیت‌های فنی فناوری اطلاعات و ارتباطات توجه کنند و هم به پویایی‌های اجتماعی که ممکن است تحت تاثیر قرار گیرند یا مختل شوند. این چارچوب، امکان تحلیل چگونگی تعامل عوامل انسانی، سیاست‌های نهادی و پاســـخ‌های اجتماعی با سیســـتم‌های فناوری در حوزه امنیت را فراهم می‌کند و به درک بهتر چگونگی تاثیرگذاری و تاثیرپذیری این عوامل کمک می‌کند(تریست و بامفورث، ۱۹۵۱).

نظریه جامعه نظارت[6] لیون[7] به بررسی پیامدهای اجتماعی نظارت گسترده، مانند مسائل حریم

1. The Third Wave
2. Alvin Toffler
3. Smith, M. R., & Marx, L. (1994)
4. Sociotechnical Systems
5. Trist and Bamforth
6. Surveillance Society
7. Lyon

خصوصی و قدرت، می‌پردازد. این نظریه پیامدهای اجتماعی نظارت فراگیر، از جمله مسائل مربوط به حریم خصوصی، کنترل و پویایی قدرت را بررسی می‌کند. در زمینه امنیت داخلی، این چارچوب در بررسی اینکه چگونه فناوری‌های نظارتی، در حالی که به عنوان ابزاری برای ارتقای امنیت عمل می‌کنند، نگرانی‌های قابل توجهی را در مورد نقض حریم خصوصی و پتانسیل تجاوزات مستبدانه ایجاد می‌کنند، مفید است(لیون، ۲۰۰۱).

نظریه جامعه ریسک[1] بک[2] چارچوبی را برای درک اینکه چگونه جوامع مدرن به‌طور فزاینده‌ای مشغول پیش‌بینی، پیشگیری و مدیریت خطرات هستند، که بسیاری از آن‌ها توسط فناوری اطلاعات و ارتباطات افزایش یافته یا تشدید می‌شوند، فراهم می‌کند. با بهره‌مندی از این نظریه، به ویژه در بررسی چگونگی دیجیتالی شدن کانال‌های اطلاعاتی و ارتباطی، آسیب‌پذیری‌ها و چالش‌های امنیتی جدیدی قابل شناسایی است که نیاز به ارزیابی مجدد استراتژی‌های مدیریت ریسک دارد. این موضوع بر این مفهوم تاکید می‌کند که در دنیایی که عمیقا با فناوری در هم آمیخته است، اقدامات امنیتی نه تنها باید به تهدیدات فعلی پاسخ دهد، بلکه باید خطرات آینده را نیز پیش‌بینی کند(بک، ۱۹۹۲).

مفهوم جامعه شبکه‌ای[3] کاستلز[4] نشان می‌دهد که شبکه‌ها به ساختار سازمانی غالب تبدیل می‌شوند که با انعطاف‌پذیری، عدم تمرکز و تعاملات پویا در سطوح جهانی و محلی مشخص می‌شوند. فناوری اطلاعات و ارتباطات به عنوان زیرساختی برای این شبکه‌ها عمل می‌کند که گذار از جامعه صنعتی متمرکز بر تولید انبوه به جامعه اطلاعاتی را ممکن می‌سازد، جامعه‌ای که فعالیت‌های اقتصادی و اجتماعی آن حول محور داده‌ها، پردازش اطلاعات و جریان‌های ارتباطی سازماندهی شده‌اند. این تغییر، زمینه‌ساز ظهور اقتصاد شبکه‌ای است که به هماهنگی جهانی سیستم‌های تولید و پویایی‌های جدید نیروی کار منجر شده است. این تحولات، پیامدهای عمیق اجتماعی و فرهنگی دارند که شامل ظهور اشکال جدید هویت و کنش جمعی می‌شود. در جامعه شبکه‌ای، پویایی‌های قدرت بازتعریف می‌شوند و از ساختارهای متمرکز و سلسله‌مراتبی به سمت مدلی توزیعی از نفوذ حرکت می‌کنند. اشکال سنتی قدرت در کنار

1. Risk society
2. Beck
3. Network society
4. Castells

این شیوه‌های جدید نفوذ وجود دارند و چالش‌های جدیدی را برای حکمرانی و اعمال کنترل ایجاد می‌کنند(کاستلز، ۱۹۹۶).

پارادوکس حریم خصوصی-تکنولوژی بارنز[1] بیان می‌کند در حالی که پیشرفت‌های فناوری اطلاعات و ارتباطات امنیت را تقویت می‌کنند، به‌طور همزمان به دلیل رفتار کاربران در فضای مجازی، منجر به نقض حریم خصوصی نیز می‌شوند. این تناقض یکی از چالش‌های کلیدی استفاده از فناوری‌های جدید در امنیت داخلی است. ادغام فناوری اطلاعات و ارتباطات در امنیت داخلی منجر به گسترش بی‌سابقه قابلیت‌های نظارتی (چه توسط دولت و چه توسط اشخاص و گروه‌های دیگر) شده است. در حالی که این ابزارها برای نظارت بر تهدیدها و پیشگیری از جرایم بسیار ارزشمند هستند، ولی به وضعیت نظارت فراگیر منجر می‌شوند. تناقض در این واقعیت نهفته است که در حالی که چنین جمع‌آوری داده‌ای برای سازمان‌های امنیتی برای مقابله موثر با تهدیدات مفید است، به طور همزمان سوالات اخلاقی مهمی در مورد میزان و ماهیت نظارت ایجاد می‌کند(بارنز، ۲۰۰۶).

نظریه اجتماعی فنی[2] در طراحی امنیت تاکید دارد که طراحی سیستم‌های امنیتی باید علاوه بر کارایی فناوری، تعامل آن با اپراتورهای انسانی و هنجارهای اجتماعی را نیز در نظر بگیرد. عوامل انسانی مانند آگاهی کارکنان و پایبندی به پروتکل‌های امنیتی بسیار مهم هستند. این رویکرد نیازمند سرمایه‌گذاری در آموزش، توسعه منابع انسانی و تغییر فرهنگ سازمانی به سمت امنیت به‌عنوان یک مسئولیت 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 نقشی مهم در شکل‌گیری سیاست‌های نظارتی دارد.

بنابراین، از اصول جبر فناوری و نظریه سیستم‌های اجتماعی فنی گرفته تا تفاوت‌های ظریف پارادوکس فناوری حریم خصوصی و جامعه نظارت، این تحلیل بر یک حقیقت اساسی تاکید می‌کند: قلمرو امنیت داخلی در عصر دیجیتال پیچیده و چندوجهی است. 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

1. Barnes
2. Sociotechnical system

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

در این تحقیق به منظور شناســـایی ابعاد و مولفه‌های اثرگذار شـــرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات روی امنیت داخلی از روش توصیفی تحلیلی اســـتفاده شـــده اســـت. روش توصیفی-تحلیلی یک روش تحقیقی اســـت که در آن از توصیف و تحلیل داده‌ها برای بررســـی و تفســـیر پدیده‌ها یا مســـائل استفاده می‌شود. در این روش، ابتدا پدیده مورد بررسی به‌طور دقیق و جامع توصیف می‌شـــود و سپس این توصیف‌ها با اســـتفاده از روش‌های تحلیلی، مفاهیم و الگوها بررســـی و تفسیر می‌شـــوند. این روش معمولاً در تحقیقات اجتماعی، روانشناسی، علوم سیاسی و مطالعات فرهنگی استفاده می‌شود.

در کل، روش توصیفی-تحلیلی این امکان را می‌دهد تا پدیده‌ها و مسائل را به‌طور جامع توصیف کنند و سپس با استفاده از روش‌های تحلیلی، عوامل مؤثر و الگوهای پشتیبانی از آن‌ها را شناسایی و تحلیل کنند (گرسول و پاث (۲۰۱۷)[1]). جامعه آماری پژوهش حاضر عبارت است از مجموع افرادی که به عنوان نخبگان علمی و اجرایی در محدوده مورد مطالعه مشغول به فعالیت بوده‌اند و پیرامون مسائل امنیت داخلی و شرکت‌های فناور از دانش و تجربیات لازم برخوردار می‌باشند. بدین منظور، در فرآیند تحقیق، با شناســـایی هدفمند خبرگان، آرای ۱۲ کارشـــناس خبره در حوزه‌های متنوع مدیریتی، امنیتی و فناوری اعم از افراد دانشـــگاهی و ســـتادی مطلع به مسائل و چالش‌های امنیت داخلی و فناوری اطلاعات و ارتباطات جمع‌آوری گردید.

۵. تجزیه و تحلیل داده‌ها و یافته‌های تحقیق

با مرور مقالات و نظریات حوزه امنیت داخلی، شرکت‌های فناور، فناوری اطلاعات و ارتباطات و اقتصاد دیجیتال، و پس از بررسی آماری نظر خبرگان (با سطح معناداری p-value<۰.۰۵)، ۷ بعد و ۵۲ مولفه استخراج شدند. تعداد ۷ بعد که شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات روی امنیت داخلی اثرگذارند به‌صورت زیر است:

1. Creswell, J. and Poth, C. (2017)

۱. 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. 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

۳. 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

۴. 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

۵. 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

۶. 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

۷. 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

متخصصان معتقدند که رسانه‌های اجتماعی تاثیری دوگانه بر امنیت داخلی دارند. از یک سو، این پلتفرم‌ها امکان تبادل فرهنگی و افزایش درک متقابل بین گروه‌های مختلف را فراهم می‌کنند که می‌تواند به کاهش تنش‌های اجتماعی و بهبود امنیت کمک کند. از سوی دیگر، همین پلتفرم‌ها می‌توانند به بستری برای گسترش اطلاعات نادرست، تشدید قطبی شدن جامعه و افزایش تقابل‌های فرهنگی تبدیل شوند. استفاده از این پلتفرم‌ها برای تحریک اختلافات قومی، مذهبی یا سیاسی می‌تواند امنیت داخلی را تهدید کند.

اکثر متخصصان بر اهمیت حیاتی امنیت محصولات دیجیتال تاکید دارند. آن‌ها معتقدند که سیستم‌های قوی احراز هویت و مدیریت دسترسی نقش کلیدی در حفاظت از داده‌های حساس و زیرساخت‌های حیاتی دارند. همچنین، متخصصان بر لزوم طراحی امنیت به عنوان بخشی ذاتی از محصولات دیجیتال و نه یک لایه اضافی تاکید دارند. این رویکرد «امنیت از طریق طراحی» می‌تواند آسیب‌پذیری‌های امنیتی را از همان ابتدای فرآیند توسعه محصول کاهش دهد. تقریبا تمامی متخصصان بر اهمیت تسهیل دسترسی به اطلاعات عمومی از طریق فناوری‌های جدید تاکید دارند. آن‌ها معتقدند که دسترسی آزاد به اطلاعات می‌تواند به افزایش شفافیت، کاهش فساد و تقویت اعتماد عمومی منجر شود که همگی به بهبود امنیت داخلی کمک می‌کنند.

متخصصان بر نقش حیاتی تحلیل داده‌ها در بهبود امنیت داخلی تاکید دارند. آن‌ها معتقدند که تحلیل داده‌های کلان می‌تواند به شناسایی الگوهای مشکوک، پیش‌بینی تهدیدات بالقوه و بهبود تصمیم‌گیری در حوزه امنیت کمک کند. علی‌رغم مزایای تحلیل داده‌ها، متخصصان نگرانی‌های جدی درباره حفظ حریم خصوصی و امنیت داده‌های شخصی دارند. آن‌ها تاکید می‌کنند که جمع‌آوری و استفاده از داده‌های شخصی باید با رعایت اصول اخلاقی و قانونی انجام شود. متخصصان بر اهمیت حیاتی ارتباطات امن در حفظ امنیت داخلی تاکید دارند. آن‌ها معتقدند که گسترش شبکه‌های موبایل و پهن‌باند، همراه با تضمین امنیت این ارتباطات، می‌تواند به بهبود هماهنگی نیروهای امنیتی، افزایش سرعت واکنش به بحران‌ها و تسهیل ارتباطات در شرایط اضطراری کمک کند. متخصصان بر لزوم ایجاد تعادل بین حفظ آزادی بیان و کنترل محتوای مضر تاکید دارند. آن‌ها معتقدند که ایجاد فضایی باز برای بیان نظرات سیاسی و دسترسی آزاد به اطلاعات می‌تواند به کاهش تنش‌های اجتماعی و افزایش ثبات سیاسی کمک کند. در عین حال، آن‌ها بر اهمیت مقابله با اخبار جعلی، نفرت‌پراکنی و محتوای افراطی تاکید دارند. آن‌ها معتقدند که قوانین باید به اندازه کافی انعطاف‌پذیر باشند تا بتوانند با سرعت تغییرات فناوری همگام شوند، اما در عین حال باید از حقوق اساسی شهروندان محافظت کنند.

متخصصان بر ارتباط نزدیک بین نوآوری، رشد اقتصادی و امنیت داخلی تاکید دارند. آن‌ها معتقدند که حمایت از نوآوری و کارآفرینی در حوزه فناوری می‌تواند به ایجاد اشتغال، افزایش رقابت‌پذیری اقتصادی و در نتیجه بهبود امنیت داخلی منجر شـــود. در عین حال، آن‌ها بر لزوم مدیریت چالش‌های ناشـــی از اتوماسیون و تغییرات ساختاری در بازار کار تاکید دارند. متخصصان بر اهمیت همکاری‌های بین‌المللی در حوزه امنیت سایبری و مدیریت چالش‌های فناوری تاکید دارند. آن‌ها معتقدند که تهدیدات سایبری ماهیتی فراملی دارند و مقابله موثر با آن‌ها نیازمند همکاری‌های بین‌المللی است.

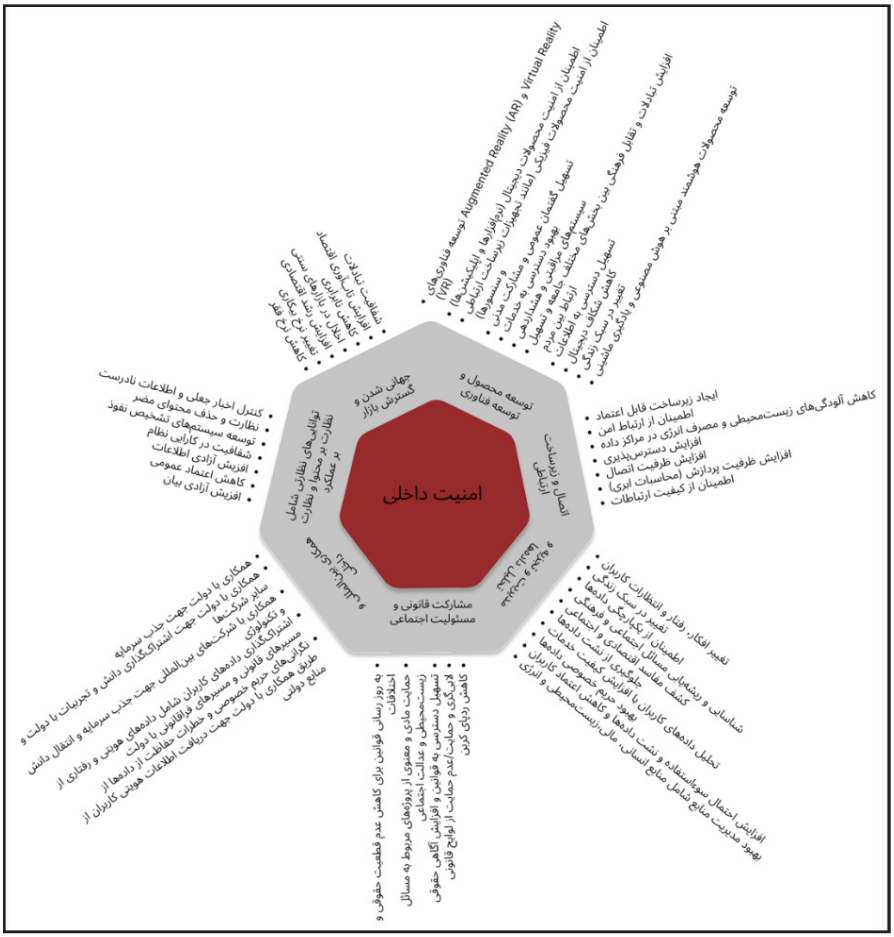
در مجمـــوع، متخصصان بر لزوم اتخاذ رویکردی جامع، متـــوازن و انعطاف‌پذیر در مدیریت تاثیرات فناوری‌های نوین بر امنیت داخلی تاکید دارند. آن‌ها معتقدند که با مدیریت هوشـــمندانه چالش‌ها و بهره‌برداری مســـئولانه از فرصت‌ها، می‌توان از ظرفیت‌های فناوری برای تقویت امنیت داخلی و بهبود کیفیت زندگی شهروندان استفاده کرد.

۶. بحث و نتیجه‌گیری

در این پژوهش، تاثیر فعالیت شـــرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات بر امنیت داخلی در ابعاد مختلف اقتصادی، سیاسی، فرهنگی، اجتماعی، نظامی، زیست‌محیطی، سایبری و حقوقی مورد بررســـی قرار گرفت. نتایج نشـــان می‌دهد که این شـــرکت‌ها نقش دوگانه‌ای در ارتقای امنیت و ایجاد چالش‌های جدید دارند. بر اساس نظریه‌های جبر تکنولوژیک، سیستم‌های اجتماعـــی فنی، جامعه نظارت و جامعه ریســـک، فناوری اطلاعـــات و ارتباطات نیروی محرکه اصلی در تغییرات اجتماعی و امنیت داخلی هســـتند. این نظریه‌ها نشـــان می‌دهند که فناوری نـــه تنها قابلیت‌ها را افزایش می‌دهد، بلکـــه چالش‌های جدیدی را نیز به همراه دارد که نیازمند مدیریت هوشـــمندانه است. در بعد امنیت اجتماعی، شرکت‌های فناوری اطلاعات و ارتباطات با فراهم کردن ابزارهای ارتباطی و اطلاعاتی، به تقویت ســـرمایه اجتماعی، افزایش آگاهی عمومی و تســـهیل دسترســـی به آموزش و ســـلامت کمک کرده‌اند. اما در عین حال، می‌توانند با انتشار اطلاعات نادرست و ایجاد شکاف دیجیتال، به ناهنجاری‌ها و ناامنی‌های اجتماعی دامن بزنند. در بعد امنیت سیاسی، این شرکت‌ها با تسهیل دسترسی به اطلاعات و ارتقای مشارکت سیاسی، به دموکراتیزه شـــدن جوامع کمک می‌کنند. اما انتشار اطلاعات نادرست و قابلیت دستکاری افکار عمومی می‌تواند ثبات سیاســـی را تهدید کند. توازن بین امنیت و حفظ حقوق فردی برای ثبات سیاسی ضروری است. در بعد امنیت فرهنگی، شرکت‌های فناوری اطلاعات و ارتباطات، با تسهیل

ارتباطات جهانی فرهنگ‌ها را به هم نزدیک کرده و به حفظ میراث فرهنگی کمک می‌کنند، اما نگرانی‌هایی درباره امپریالیسم فرهنگی و همگن‌سازی فرهنگ‌ها وجود دارد که می‌تواند هویت فرهنگی جوامع را تهدید کند. در بعد امنیت اقتصادی، شرکت‌های فناور با نوآوری و افزایش بهره‌وری، به رشد اقتصادی و ایجاد بازارهای جدید کمک کرده‌اند، اما تاثیر آن‌ها بر اشتغال، نابرابری اقتصادی و تغییر ساختارهای بازار می‌تواند چالش‌هایی را برای امنیت اقتصادی ایجاد کند. در بعد امنیت زیست‌محیطی، این شرکت‌ها با ارائه راه‌حل‌های هوشمند در مدیریت منابع و کاهش اثرات زیست‌محیطی، به امنیت زیست‌محیطی کمک می‌کنند. اما تولید زباله‌های الکترونیکی و مصرف انرژی بالا از چالش‌های مرتبط با آن‌هاست. در بعد امنیت دفاعی و امنیت، فناوری اطلاعات و ارتباطات قابلیت‌های نظامی و امنیتی را ارتقا داده‌اند، اما همزمان چالش‌هایی در زمینه اخلاقی و حقوقی، به‌ویژه در استفاده از سلاح‌های خودکار و نظارت گسترده، ایجاد کرده‌اند. در بعد امنیت سایبری، با افزایش وابستگی به فناوری‌های دیجیتال، تهدیدات سایبری به یکی از مهم‌ترین چالش‌های امنیت داخلی تبدیل شده‌اند. شرکت‌های فناوری اطلاعات و ارتباطات نقش حیاتی در توسعه پروتکل‌های امنیتی، آموزش و آگاهی‌بخشی و همکاری با نهادهای دولتی دارند. در بعد امنیت حقوقی، تغییرات سریع فناوری نیازمند به‌روزرسانی مداوم قوانین و مقررات است. شرکت‌های فناور با توسعه راه‌حل‌های فنی برای بهبود فرآیندهای حقوقی و تسهیل دسترسی به اطلاعات حقوقی، به تقویت امنیت حقوقی کمک می‌کنند. فعالیت شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات تاثیری چندبعدی و پیچیده بر امنیت داخلی دارند. آن‌ها با نوآوری‌های خود فرصت‌های بزرگی برای ارتقای امنیت در ابعاد مختلف فراهم کرده‌اند، اما همزمان چالش‌ها و تهدیدات جدیدی را نیز به وجود آورده‌اند. شرکت‌های فناور حوزه فناوری اطلاعات و ارتباطات، از طریق محصولات، فناوری‌ها و پلتفرم‌های نوآورانه خود، به بازیگران اصلی شکل دادن به زندگی مدرن تبدیل شده‌اند. نفوذ آن‌ها در قلمروهای سیاسی، اجتماعی، اقتصادی، نظامی، محیطی و فرهنگی گسترده است و چالش‌ها و فرصت‌هایی را پیش روی ما قرار می‌دهد. همان‌طور که این شرکت‌ها به پیشبرد پیشرفت‌های تکنولوژیک ادامه می‌دهند، نقش آن‌ها به عنوان کاتالیزورهای تغییر در هر جنبه‌ای از زندگی به‌طور فزاینده‌ای افزایش می‌یابد. برای بهره‌برداری حداکثری از مزایا و کاهش معایب، نیاز به رویکردی جامع و چندجانبه است که شامل تدوین سیاست‌ها و مقررات مناسب، تقویت همکاری بین دولت و بخش خصوصی، آموزش و آگاهی‌بخشی عمومی و توجه به ابعاد اخلاقی و حقوقی فناوری است.

سیاست‌گذاران باید با درکی عمیق از تاثیرات فناوری اطلاعات و ارتباطات، راهبردهایی را توسعه دهند که هم از نوآوری حمایت کند و هم امنیت و رفاه جامعه را تضمین نماید. در نهایت، مدل مفهومی تحقیق در نمودار زیر آمده است:



منابع

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

پورسعید، فرزاد(۱۴۰۱). نسبت مفهومی فرهنگ و امنیت: جستاری در چیستی «امنیت فرهنگی». *فصلنامه مطالعات راهبردی*، ٤ (۲۵)، ۱۷۷-۲۱۵.

پورعـــزت، علی اصغر، عبدی، بهنام(۱۳۹۷). شناســـایی 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.

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

ترابی، یوسف، کتولی‌نژاد، خدابخش، 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.

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

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

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

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

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

دســـتغیب، ســـیداحمدرضا(۱۳۹۶).تاثیر فناوری اطلاعات و ارتباطات بر ابعاد مختلف امنیت ملی (ابعاد نظامی، سیاســـی، اقتصـــادی، اجتماعی، فرهنگی و زیســـت محیطی)،کنفرانس ملی رویکردهای نوین علوم انسانی در قرن ۲۱

ذکی، یاشار، 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.

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

رشـــیدی، مصطفی، ردادی، علی، مقدم‌فر، ســـعیدرضا(۱۳۹٤). طراحی الگوی ســـنجش امنیت اقتصادی کشور، *فصلنامه مطالعات راهبردی بسیج*، سال هجدهم، شماره ٦٨.

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

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

رضوی‌نژاد، سید امین، رزاقی، جواد(۱۳۹۷). مدل مطلوب اجرا و ارزیابی در سیاست‌گذاری امنیت داخلی جمهوری اســـلامی ایران، *خط مشـــی‌گذاری عمومی در مدیریت*، شـــماره ۲۹ ISC، ۱۰۱-۱۱۸.

رمضانـــی، محمدجـــواد، بدری، کوروش، غفاری، جلال(۱۳۹۹). بررســـی روندهـــای تاثیرگذاری شـــبکه‌های اجتماعی بر امنیت ملی جمهوری اسلامی ایران. *فصلنامه علمی امنیت ملی*، ۱۰ (۳۷)، ۳۸۷-۴۲۰.

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

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

زارع‌زاده، رســـول(۱٤۰۰). آســـیب‌ها و چالش‌های امنیتی‌سازی مســـائل داخلی؛ مطالعه موردی شبکه‌های اجتماعی مجازی، *مطالعات راهبردی*، شماره ۹۲ ISC، ۳۲-۷.

ســـپهرنیا، روزیتا، شیخی، محمدطاهر(۱٤۰۰). نقش ســـرمایه فرهنگی در تامین امنیت داخلی، *مطالعات دفاع مقدس*، شماره ۲٦ ISC، ۱۹۵-۱۷۵.

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

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.

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

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

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

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.

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

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

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

علیزاده، عظیم(۱٤۰۰). آینده‌نگاری راهبردی در امنیت داخلی؛ ارائه الگوی دوساخه تدوین راهبرد. *فصلنامه علمی مطالعات مدیریت راهبردی دفاع ملی* ، ۵ (۲۰)، ۱۸۸-۱٦۳.

غیاثوند، ابوالفضل، و عبدالشاه، فاطمه(۱۳۹٤). مفهوم و ارزیابی تاب‌آوری اقتصادی ایران. *پژوهشنامه اقتصادی*، ۵۹ (٤)، ١٦١-١٨٧.

کریمی قهرودی، محمدرضا، فشارکی، مهدی، و نظامی‌پور، قدیر(۱۳۹۲). تدوین چشم‌انداز و

الگوي بلوغ توسعه فناوری اطلاعات و ارتباطات سازمان در افق ۱٤۰٤ با رویکرد آینده‌نگاري، *بهبود مدیریت*، شماره ۱۹، ۱۳۷-۱٦۱.

کرمی، مرجان، کشیشیان سیرکی، گارینه، 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.

کریمی قهرودی، محمدرضا، سعادتمند، امیر مسعود، محمدی، حافظ(۱۴۰۱). ارائه مدلی برای ارزیابی امنیت سایبری جمهوری اسلامی ایران. *فصلنامه امنیت ملی*، شماره ۴۵، ۶۹-۱۰۰.

گودرزی، غلامرضا، اجلالی، محمدمهدی(۱۴۰۰). تحلیل روندهای آینده فناوری‌های دفاعی در افق ده ساله. *آینده‌پژوهی دفاعی*، شماره ۲۳، ۳۷-۵۷.

مسیبی ملک خیل، رحیم، 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)، ۱۸۷-۲۱٦.

میرزمانی، اعظم، خنیفر، حسین، جعفری، سید محمدباقر، 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.

محمدی خانقاهی، محسن، آزادی، محمدحسین (۱۴۰۰). تفاوت‌های امنیت سایبری اجتماعی با امنیت سایبری. *فصلنامه علمی امنیت ملی* ، ۱۱ (٤۱)، ۱۳۱-۱۵۸.

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.

محمدی نیا سماکوش، خلیل، صبح خیز، رضا(۱۴۰۱). تاثیر ارزهای مجازی (دیجیتال) بر احساس امنیت اقتصادی شهروندان استان مازندران. *دانش انتظامی مازندران*، ۱۳ (۵۱)، ۲۱-۵٦.

نجفی، سجاد، یزدان پناه درو، کیومرث، پیشگاهی‌فرد، زهرا، 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.

نوری، مهدی، 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.

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.

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

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

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

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

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

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

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

Digital Regulation. (2023). Enhancing the Protection and Cyber Resilience of Critical Information Infrastructure. DigitalRegulation.org.

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.

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.

Hermann, M., Pentek, T., & Otto, B. (2017). Design Principles For Industries 4.0 Scenarios. System Sciences (HICSS), IEEE.

Lyon, D. (2001). Surveillance society: Monitoring everyday life.

Riggs, H. et al. (2023). Impact, Vulnerabilities, and Mitigation Strategies for

Cyber-Secure Critical Infrastructure. Sensors, 23(8), 4060.

Rout, Subhashree. (2022). Application of Blockchain Technology to facilitate security in Smart Grid. 10.1109

Saeed, S. et al. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors, 23(16), 7273.

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.

Smith, M. R., & Marx, L. (1994). Does Technology Drive History? The Dilemma of Technological Determinism. MIT Press.

Toffler, A. (1980). The Third Wave.

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.

U.S. Bureau of Labor Statistics. Occupational Handbook: Computer and Information Technology Occupations. https://www.bls.gov/ooh/computer-and-information-technology/home.htm