

شناسایی فراروندهای فناوری اطلاعات و ارتباطات قابل توجه در آینده‌نگاری

صنعت دفاعی در جهت نیل به الگوی اسلامی - ایرانی پیشرفت

علی اصغر پورعزت^۱

بهنام عبدی^{۲*}

چکیده

ارتقای روزافزون توان دفاعی و بازدارندگی کشور در محیط کنونی سرشار از تغییر و بی‌ثباتی و آکنده از عدم قطعیت‌ها، نیازمند تلاش مستمر برای معماری آینده است. اگرچه این تلاش همواره با خطرپذیری فراوان همراه بوده است؛ اما پذیرش این مخاطره، به مراتب عاقلانه‌تر از نظاره‌گر بودن تحولات آینده است. یکی از حوزه‌های اصلی متغیر و موثر بر آینده صنعت دفاعی کشور، فراروندهای فناوری اطلاعات و ارتباطات است. از طرف دیگر و پس از ابلاغ سیاست‌های کلی خودکفایی دفاعی و امنیتی در اواخر سال ۱۳۹۱، تحلیل و تدوین سناریوهایی محتمل آینده و کسب آمادگی لازم برای مواجهه با آن در راستای الگوی اسلامی - ایرانی پیشرفت بديهی به نظر می‌رسد. بر این اساس، پژوهش حاضر به شناسایی فراروندهای فناوری اطلاعات و ارتباطات قابل توجه در آینده‌نگاری صنعت دفاعی در جهت نیل به الگوی اسلامی - ایرانی پیشرفت می‌پردازد. رویکرد این پژوهش، استقرایی و نحوه انجام آن، ترکیبی (کیفی و کمی) است. پژوهش از نوع مطالعه موردی است که از نظر موضوعی، در حوزه پژوهش‌های کاربردی - توسعه‌ای قرار می‌گیرد. از نظر هدف از نوع اکتشافی است. در فاز کیفی، داده‌ها از طریق بررسی مبانی نظری پژوهش، اسناد مرتبط و مصاحبه با خبرگان جمع‌آوری و تحلیل محتوا شده‌اند و بر اساس آن، فراروندهای حوزه فناوری اطلاعات و ارتباطات شناسایی شده است. در ادامه، به منظور ارزیابی روایی درونی، یافته‌های فاز کیفی در قالب پرسشنامه در اختیار متخصصین مربوطه قرار گرفته است و بر اساس نتایج فاز کمی، فراروندهای نهایی حاصل به‌عنوان مبنای قابل توجهی برای آینده‌نگاری صنعت دفاعی مورد توجه قرار گرفته است. یافته‌ها نشان می‌دهند که در راستای آینده‌نگاری صنعت دفاعی کشور، فراروندهای هفت‌گانه حوزه فناوری اطلاعات و ارتباطات شامل مدیریت امنیت اطلاعات، شبکه‌های اجتماعی، زیرساخت‌های ارتباطی، شبکه‌های نوآوری در بستر فناوری اطلاعات، هوش مصنوعی، اینترنت اشیا و مراکز داده و پایگاه‌های ذخیره اطلاعات باید مورد توجه قرار گیرند.

واژه‌های کلیدی:

فراروندهای فناوری اطلاعات و ارتباطات، آینده‌نگاری صنعت دفاعی، الگوی اسلامی - ایرانی پیشرفت، هوش مصنوعی، اینترنت اشیا.

^۱. استاد دانشکده مدیریت دانشگاه تهران

^۲. پژوهشگر پسادکتری دانشکده مدیریت دانشگاه تهران

مقدمه

انسان همواره بر اساس نیازهای درونی، شیفته کشف آینده و رمزگشایی از آن بوده است (زالی، ۱۳۹۰) و در مسیر توسعه انسانی، از دیرباز مورد توجه قرار گرفته است (Moyer & Bohl 2019). مطالعه آینده، شناسایی و تعیین آینده‌های ممکن، انتخاب آینده مطلوب و تدوین برنامه برای دستیابی به اهداف، به روشی کارآمد به‌عنوان یکی از زمینه‌های بااهمیت جهت بررسی و مطالعه تبدیل شده است (Brownlie, 1998). به‌ویژه در مباحث مربوط به توسعه‌یافتگی، بررسی آینده از ملاحظات اساسی است (Madrueno & Tezanos, 2018). در این امتداد، یکی از ابزارهای مهم و کارآمد جهت اتخاذ راهبردهای بلندمدت و تدوین سیاست‌های ملی و فراملی برای کسب اهداف سیاسی، اقتصادی، اجتماعی، فرهنگی و غیره، آینده‌نگاری^۱ است (Müller-Stewens et al., 2012). ارزیابی فعالیت‌های آینده، موضوع مهمی محسوب می‌شود؛ بخش گسترده‌ای از مطالعات علمی صورت پذیرفته در حوزه آینده‌نگاری به ارزیابی آینده‌نگاری و شناسایی عوامل مؤثر بر آینده صنایع، علم و فناوری اختصاص پیدا نموده است (Kim, 2012; Diesen & Keane, 2018). با توجه به اهمیت روزافزون توان دفاعی و بازدارندگی کشور در آینده، افزایش زمینه‌های استفاده از فناوری اطلاعات و ارتباطات و رشد روزافزون فناوری‌های نوین، مطالعه عوامل تأثیرگذار بر صنعت دفاعی اهمیت دوچندانی پیدا کرده است (Sceral, et al., 2018). از طرف دیگر، دو موضوع دفاع و امنیت از بسترها و پیشران‌های پیشرفت اسلامی- ایرانی هستند. در این امتداد، تأکید بر خودکفایی کشور در سامانه‌ها، کالاها و خدمات اولویت‌دار دفاعی و امنیتی توأم با بهسازی تجهیزات موجود و افزایش قابلیت و کارایی آن، ممنوعیت تأمین نیازهای دفاعی و امنیتی از خارج کشور مگر در حد ضرورت، برون‌سپاری و جلب مشارکت سایر بخش‌ها اعم از دولتی و غیردولتی در تأمین نیازهای نیروهای مسلح با رعایت ملاحظات امنیتی و حفاظتی، جذب، توانمندسازی و به‌کارگیری نیروهای مستعد و نخبه با فراهم نمودن زمینه‌های رشد و تقویت آنان برای ارتقاء قابلیت‌های توسعه فناوری‌های دفاعی و امنیتی موردنیاز کشور، برقراری ارتباط و همکاری با دیگر کشورها در زمینه‌های علمی، تولیدی و تجاری کالاها و خدمات دفاعی و امنیتی برای دستیابی به اهداف سیاست‌های کلی خودکفایی دفاعی و امنیتی و مقرون به‌صرفه‌سازی مسیر توسعه صنایع و فناوری‌های دفاعی و امنیتی کشور و ایجاد هم‌افزایی در فناوری‌های موردنیاز از جمله سیاست‌های کلی خودکفایی دفاعی و امنیتی ابلاغی در اواخر سال ۱۳۹۱ هستند.

^۱. Foresighting

بر این اساس، آینده‌نگاری صنایع مختلف از جمله صنعت دفاعی، دارای ابعاد گوناگونی است که یکی از مهم‌ترین آن‌ها، فناوری است (Malik, 2018)؛ لذا بررسی فراروندهای فناوری¹ و از جمله آن، فناوری اطلاعات و ارتباطات به‌عنوان قسمتی از این فراروندها و چالش‌های متوجه صنعت دفاعی از موضوعاتی است که می‌تواند موفقیت صنعت دفاعی کشور را در برداشته باشد. با توجه به رشد روزافزون زمینه‌های فعالیت فضای مجازی و همچنین توسعه فناوری، بیشتر فعالیت‌های افراد، سازمان‌ها و صنایع مختلف با فضای مجازی گره‌خورده است؛ از طرفی با توجه نقش شایانی که فراروندها در تعیین چشم‌اندازهای آینده ایفا می‌نمایند و همچنین تأثیرات و تحولات گسترده‌ای که بر کسب‌وکار، اقتصاد، جامعه، افراد و صنایع دارند، بررسی فراروندهای فناوری اطلاعات و ارتباطات الزامی می‌باشد. شناسایی فراروندها و روندهای مؤثر در آینده و همچنین استفاده از روندهای گذشته برای ایجاد آمادگی برای رویارویی با تغییرات، عدم قطعیت‌ها و شرایط مخاطره‌آمیز آینده، امری مهم است. شناسایی درست فراروندها و روندها و استفاده درست از آن‌ها و داشتن اطلاعات صحیح برای تحلیل موقعیت و سیاست‌گذاری در آینده باید صورت پذیرد؛ زیرا کمبود اطلاعاتی و اطلاعات ناقص و نادرست، تحلیل موقعیت را برای سیاست‌گذاران و برنامه‌ریزان با دشواری روبه‌رو می‌سازد. پژوهش حاضر با رویکرد اکتشافی به دنبال شناسایی فراروندهای فناوری اطلاعات و ارتباطات قابل توجه در توسعه صنعت دفاعی کشور برای رسیدن به آینده مطلوب با رویکرد آینده‌نگاری است.

پس از بررسی کلیات قابل توجه الگوی اسلامی- ایرانی پیشرفت، مبانی نظری آینده‌نگاری و فراروندها مورد بررسی قرار گرفته و پس از ارائه روش‌شناسی، تحلیل داده‌ها در دو فاز کیفی و کمی ارائه‌شده و فراروندهای هفت‌گانه شناسایی‌شده مورد بررسی و تحلیل قرار خواهند گرفت. در نهایت به جمع‌بندی و نتیجه‌گیری خواهیم پرداخت.

مرور مبانی نظری و پیشینه پژوهش

الگوی اسلامی ایرانی پیشرفت

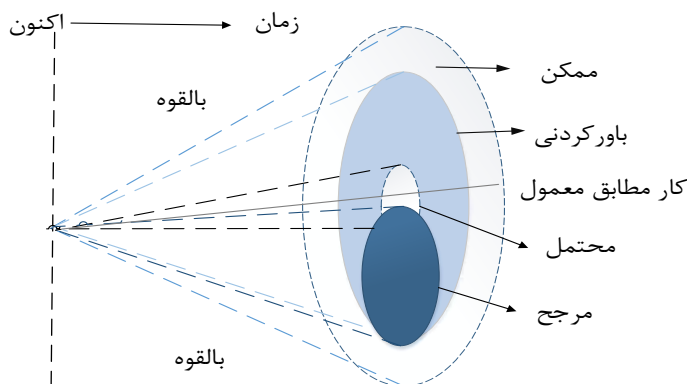
تدوین الگوی- اسلامی ایرانی پیشرفت از ابعاد گوناگون، یک اتفاق نیک، مهم و بی‌سابقه در امر برنامه‌ریزی توسعه در کشور محسوب می‌شود (قاضی‌زاده، ۱۳۸۹). از طرف دیگر، مفهوم پیشرفت عبارت است از فراگرد حرکت از وضعیت موجود به سمت وضعیت مطلوب (خوش‌چهره و حبیبی، ۱۳۹۱). علاوه بر این، پیشرفت در بخش دفاع باید با رویکرد دفاع همه‌جانبه باشد

¹. Technology megatrends

(کیوان حسینی و جمعه‌زاده، ۱۳۹۰). الگوی اسلامی- ایرانی پیشرفت، یعنی شکل‌گیری جریان مسلط فکری که یک الگوی نظری با کارکرد هنجاری است؛ یعنی ساختاری است که به توضیح نظریه اسلامی - ایرانی پیشرفت می‌پردازد، زیرا فرهنگ و تمدن در هر جامعه روبه‌پیشرفت و حرکت، از مواضع و موضوعات اصلی تغییر هستند (امامی، ۱۳۹۲).

آینده

برای هر انتخاب امروز، یک آینده ممکن می‌توان تصور کرد (بنیاد توسعه فردا، ۱۳۸۴). به عبارت دیگر، تصویرهای آینده، پیشران‌های اقدامات فعلی ما هستند (فاتح‌راد و همکاران، ۱۳۹۲). آینده را به‌طور کلی می‌توان به آینده ممکن، آینده‌های محتمل، قابل قبول و آینده مرجع یا مطلوب تقسیم نمود (شکل ۱):



شکل (۱) انواع آینده (Voros, 2003)

آینده بالقوه (ممکن): شامل تمام وضعیت‌های ممکن است که می‌تواند در آینده محقق گردد. این طیف از آینده‌ها، مجموعه‌ای از تصویرهایی هستند که انسان برای آینده‌اش در نظر دارد و عمدتاً، تخیلی و حاصل تصویرپردازی ذهن بشر است.

آینده محتمل: آینده محتمل، آینده‌ای است که احتمالاً تحقق می‌یابد. این آینده‌ها، زیرمجموعه‌هایی از آینده باورکردنی هستند. محرک‌های مطالعه آینده محتمل شامل روندها و گرایش‌های کلیدی و محدودیت‌های فعلی هستند.

آینده مرجع: این بعد از آینده به ترجیحات و باورهای فرد از آنچه تمایل دارد و خواهان اتفاق افتادنش در آینده هست، اشاره دارد. افراد یا سازمان‌ها، آرمان‌هایی را از آنچه ترجیح می‌دهند در آینده برایشان اتفاق افتد، را در اولویت قرار داده و آن‌ها را توسعه و گسترش می‌دهند.

آینده‌نگاری^۱

انسان همواره بر اساس نیازهای درونی، شیفته کشف آینده و رمزگشایی از آن بوده است (Meissne, 2012). این سؤالات که «آینده چگونه قابل پیش‌بینی است؟»، «آیا آینده تداوم حال و گذشته خواهد بود؟»، «آیا آینده پیش‌رو مطلوب ما نیز هست؟»، «مسیرهای مختلفی که ما می‌توانیم در آینده طی کنیم کدام‌ها هستند؟» و «بهترین مسیرها و ممکن‌ترین مسیرها کدام‌اند؟» تاکنون چالش عمده فکری برنامه‌ریزان و مدیران جهت برخورد با مسائل آینده بوده که عمدتاً بر پایه تحلیل روندهای گذشته و ادامه روند وضع موجود بوده است (زالی، ۱۳۹۰). مشکل اصلی در برنامه‌ریزی‌های بلندمدت، ناشی از تغییرات و تحولات سریع جهانی و محیطی است (خزایی، ۱۳۹۰). در هر آینده‌نگاری می‌توان مسئله پروژه را از سه منظر آینده‌پژوهی، سیاست-گذاری و مدیریت راهبردی مورد توجه قرارداد (Durance and Godet, 2008). در انجام هر پروژه آینده‌نگاری، ناگزیر باید ابعاد و عناصر آینده‌نگاری، متناسب با بافت و ویژگی‌های محلی که آینده‌نگاری در آن انجام می‌گیرد، طراحی گردد (قدیری و همکاران، ۱۳۸۵). بسیاری از کشورها جهت تخصیص منابع از آینده‌نگاری استفاده می‌نمایند (Liebl and Schwarz, 2010).

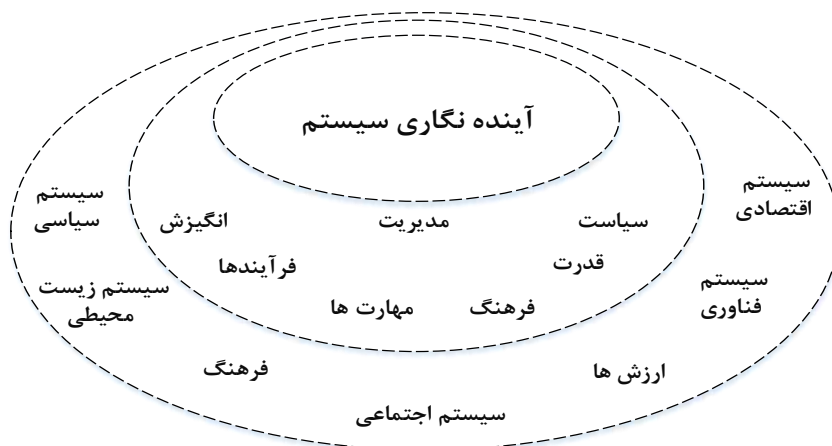
منافع بالقوه کاربرد آینده‌نگاری عبارت‌اند از توانایی تشخیص و تفسیر تغییرات محیطی (Tsoukas and Sheperd, 2004)، تسهیل فرآیند برنامه‌ریزی استراتژیک (Roney, 2010)، رشد قابلیت‌های نوآورانه و افزایش توانایی برای یادگیری سازمانی و اجرای تصمیمات استراتژیک (Rohrbeck and Schwartz, 2013)، درک بهتر فرصت‌ها، داشتن چشم‌انداز یا مأموریتی روشن و متمرکز بر اهداف، برگزیدن اهدافی والا و ایجاد انگیزه و تلاش برای دستیابی به اهداف (Bezold, 2010).

آینده‌نگاری سیستماتیک

بنابر نظر ساریتاس^۲ (۲۰۰۶)، در هنگام مطالعه طراحی آینده‌نگاری در سازمان باید به سازه‌های داخلی از جمله فرآیندهای داخلی، روش‌ها، تجهیزات و فناوری و همچنین سازه‌های رفتاری از جمله سیاست تعامل اجتماعی، مهارت‌ها، انگیزه، قدرت، سبک‌های مدیریتی توجه نمود که در شکل (۲) قابل مشاهده می‌باشد:

^۱. Foresight

^۲. Saritas



شکل (۲) مدل آینده‌نگاری سیستمی (Saritas, 2006)

برنامه آینده‌نگاری در تلاش می‌کند تا نگاهی فراتر از افق عادی داشته باشد و بتواند فرصت‌های بالقوه در علم و فناوری‌های جدید را شناسایی نماید (Futures, 2002). اندیشمندان جهت مطالعه آینده‌نگاری از ویژگی‌ها و چارچوب‌های مختلفی استفاده نموده‌اند. در جدول (۱) برخی از چارچوب‌های ارزیابی آینده‌نگاری بیان شده است.

جدول (۱) بررسی اجمالی از چارچوب‌های ارزیابی آینده‌نگاری

ویژگی‌های اصلی	چارچوب ارزیابی آینده‌نگاری	پژوهشگران
روش ارزیابی متمرکز بر سه مرحله آماده‌سازی، ارزیابی مستقیم و مقایسه‌ای و ترکیب و نتایج است	رویکرد یکپارچه برای ارزیابی آینده‌نگاری	(Sokolova, 2015)
دو معیار ارزیابی کیفیت علمی آینده‌نگاری شامل شفافیت و انتخاب کارشناسان است	معیارهای علمی برای ارزیابی مطالعات آینده‌نگاری	(Peperhove and Luoto, 2013)
نقش استراتژیک و نقش کارکردی آینده‌نگاری	تأثیر آینده‌نگاری بر نوآوری	(Harper, 2013)
اثر شبکه‌سازی بر توسعه گزینه‌های راهبردی	آینده‌نگاری و اثرات یادگیری	(Schartinger et al., 2012)
آگاهی، اطلاع‌رسانی، توانا ساختن، تأثیرگذاری	ارزیابی فعالیت‌های آینده‌نگاری	(Johnston, 2012)
انتظارات جامعه‌شناسی برای تعیین اهداف آینده-نگاری استفاده می‌گردد	آینده‌نگاری و انتظارات جامعه‌شناسی	(Van Lente, 2012)

آینده‌نگاری فناوری

آینده‌نگاری فناوری به‌عنوان یک ابزار سیاستی جدید برای مقابله با مشکلات علم و فناوری و سیستم نوآوری شناخته‌شده است (Miles, 2010). دولت‌ها از طریق ارزیابی اقتصاد و زیرساخت‌ها می‌توانند شرایط بهتر در آینده را پیش‌بینی نمایند (Meissner, 2012). هدف آنان تنظیم برنامه‌ها و وظایفی برای ارزیابی فنی، بررسی مباحث مهم، بررسی شبکه‌های بازیگران و ذینفعان جهت مشخص نمودن اولویت‌های سیاستی می‌باشد (Colwell and Narayanan 2010). بنا بر نظر مارتین^۱ (۱۹۹۵)، آینده‌نگاری فناوری به‌عنوان یک فرآیند منظم است که آینده درازمدت علم، فناوری، اقتصاد و جامعه را تعریف می‌کند. هدف آینده‌نگاری فناوری شناسایی زمینه‌های تحقیقات استراتژیک و فناوری‌های در حال ظهور است که احتمالاً بر عملکرد مؤثرند و به‌عنوان بزرگ‌ترین مزایایی اقتصادی و اجتماعی محسوب می‌شوند (Chen et al., 2012). بر این اساس، مبنای عقلایی برای آینده‌نگاری فناوری، مطالعه و بررسی دقیق و سنجیده اقدامات و توسعه‌های آتی علمی، فناوری و اجتماعی می‌باشد (عباسی شاه کوه و همکاران، ۱۳۸۷؛ استیری و مشیری، ۱۳۸۸).

روند

نمایش روند آینده‌نگاری به‌طور کلی برای درک یک فعالیت استراتژیک، سیستم نوآور و یا شیوه‌های یکپارچه‌سازی سازمان می‌باشد (Keller et al., 2015). مدیران با بررسی محیط‌زیست و بررسی روندها می‌تواند مسائل استراتژیک سازمان خود را مدیریت می‌نمایند. روندها به‌عنوان سیگنال‌های ضعیفی از تغییرات هستند که به‌احتمال زیاد در آینده یک سازمان و محیط آن تأثیر می‌گذارد که افراد این روندها و تأثیر آن‌ها بر سازمان مورد بررسی قرار می‌دهند. اگر روندها به‌درستی تفسیر نشوند به دلیل اطلاعات نادرست سازمان با ریسک اجرای استراتژی نامناسب روبه‌رو می‌شوند. روند، شکل‌پذیری آینده را برملا می‌کند.

جدول (۲) برخی از روندهای مطالعات پیشین

روندهای شناسایی شده	پژوهشگران
گذر از جامعه صنعتی به جامعه اطلاعاتی، توجه به چشم‌اندازهای بلندمدت	(Naisbitt, 1982)
جهانی‌شدن، دیجیتالی شدن، تغییر در ترکیب صنعت، موج همگرایی در رسانه-ها، حرکت از کیفیت تفکر به سرعت تفکر	(Lee and Kwon Lee, 2002); (Lee et al., 2007)
ظهور شبکه‌ها، از جمله گسترش فناوری اطلاعات و افزایش سریع رقابت‌پذیری، همگرایی با توجه به ادغام فناوری، شبکه و محاسبات فراگیر، نوآوری باز	(Singh and et al., 2009)

^۱. Martin

شکل‌گیری نسلی هوشمند، ترکیب زمان واقعی دسترسی و همه‌گیری، چابکی، سیستم‌عامل‌های مبتنی بر پلتفرم‌های استاندارد	(Forrester, 2010)
---	-------------------

فراروند

مفهوم فراروند^۱ از کلمه یونانی «مگا» توسط نایزبیت گرفته شده است و صرفاً به‌عنوان روندی "بزرگ" می‌باشد (Naisbitt, 1982). به گفته او، روند بزرگ «تغییر و تحول اجتماعی و اقتصادی و تکنولوژیکی بزرگی هستند که برای شکل دادن کند عمل می‌کنند، اما به‌جای خود می‌توانند زندگی ما را برای مدتی بین ۷-۱۰ سال یا بیشتر تحت تأثیر قرار دهند». فراروندها نیروهای عظیمی هستند که به چند نسل قبل از وجود انسان برمی‌گردد. فراروندهای فعل و انفعالات پیچیده‌ی بسیاری از عوامل می‌باشد (Sunter, 2013). به‌عبارت‌دیگر، فراروندهای عظیم به‌عنوان نیروهای جهانی هستند که باعث ایجاد تأثیرات و تحولات بسیاری می‌گردند. در مطالعات عوامل متعددی به‌عنوان فراروندها مطرح گردیده است که در جدول (۳) به شکل خلاصه نشان داده شده است.

جدول (۳) برخی از فراروندها در مطالعات دیگر

فراروندهای مورد مطالعه	اندیشمندان
تغییرات جمعیتی، تغییرات اقتصادی، تغییر در چشم‌اندازهای جغرافیایی	(Biswas, 2016)
آینده دیجیتال، شبکه‌های نوآوری، بازارهای جهانی، جهان شهری	(Schreiber, 2015)
تغییرات جمعیتی، افزایش شهرنشینی، تسریع در نوآوری فناوری، انتقال قدرت، رشد مداوم اقتصادی	(European Environment Agency, 2015)
تغییرات جمعیتی، تغییر در قدرت اقتصادی جهانی، پیشرفت‌های تکنولوژی	(Quesada et al., 2014)

روش‌شناسی پژوهش

رویکرد این پژوهش، استقرایی و نحوه انجام آن، ترکیبی (کیفی و کمی) است. پژوهش‌های کیفی برای کمک به پژوهش‌گر، به‌منظور درک افراد انسانی و بسترهای اجتماعی و فرهنگی که انسان‌ها در آن زندگی می‌کنند، شکل گرفته‌اند (دانایی‌فرد و همکاران، ۱۳۸۶)، زیرا این پدیده‌ها با پژوهش‌های کیفی و مطالعات موردی عمیق، بهتر قابل‌درک و بررسی هستند (Fitjar and Rodríguez-Pose, 2013). پژوهش از نوع مطالعه موردی است که از نظر موضوعی، در حوزه پژوهش‌های کاربردی- توسعه‌ای قرار می‌گیرد. از نظر هدف از نوع اکتشافی، است. در

^۱. Megatrend

فاز کیفی، داده‌ها از طریق بررسی مبانی نظری پژوهش، اسناد مرتبط و مصاحبه با خبرگان جمع‌آوری و تحلیل محتوا و کدگذاری شده‌اند و بر اساس آن، فراروندهای حوزه فناوری اطلاعات و ارتباطات شناسایی شده است. در ادامه، به‌منظور ارزیابی روایی درونی، یافته‌های فاز کیفی در قالب پرسشنامه در اختیار متخصصین مربوطه قرار گرفته است و بر اساس نتایج فاز کمی، فراروندهای نهایی حاصل به‌عنوان مبنای قابل توجهی برای آینده‌نگاری صنعت دفاعی مورد توجه قرار گرفته است. به‌عبارت‌دیگر، استراتژی پژوهش ترکیبی در مقاله حاضر، استراتژی اکتشافی متوالی است که در آن، اولویت با رویکرد کیفی است. یافته‌های حاصل از مرحله کیفی، به‌نوعی، در مرحله کمی آزمون می‌شوند، اما در این روش اولویت با رویکرد کیفی است، تجزیه و تحلیل داده در هر کدام از رویکردها به‌صورت مستقل و ترتیبی انجام می‌شود، و از نتایج کیفی در گام کمی استفاده خواهد شد.

تحلیل داده‌ها و یافته‌های فاز کیفی

همان‌طور که اشاره شد، در فاز کیفی، داده‌ها از طریق بررسی مبانی نظری پژوهش، اسناد مرتبط و مصاحبه با ۲۱ نفر از خبرگان جمع‌آوری، تحلیل محتوا و کدگذاری شده‌اند و بر اساس آن، فراروندهای حوزه فناوری اطلاعات و ارتباطات شناسایی شده است. اطلاعات مربوط به مشارکت‌کنندگان در مصاحبه در جدول (۴) قابل مشاهده است:

جدول (۴) اطلاعات جمعیت شناختی خبرگان مصاحبه‌شونده

ردیف	مدرک تحصیلی	رشته تحصیلی	سابقه (سال)	سن (سال)	سمت سازمانی
۱	دکتری	مدیریت فناوری اطلاعات	۷	۳۹	رئیس اداره
۲	دکتری	مدیریت تکنولوژی	۹	۴۱	مدیر ارشد
۳	دکتری	مدیریت امور دفاعی	۲۹	۴۷	جانشین اداره
۴	دکتری	مدیریت استراتژیک	۳۲	۵۰	رئیس اداره
۵	دکتری	مدیریت امور دفاعی	۳۴	۵۳	جانشین معاونت
۶	دکتری	مدیریت آموزش عالی	۱۱	۴۱	عضو هیات علمی
۷	دکتری	مدیریت فناوری اطلاعات	۹	۳۸	عضو هیات علمی
۸	دکتری	علوم دفاعی	۲۶	۴۵	عضو هیات علمی
۹	کارشناسی ارشد	مدیریت امور دفاعی	۲۵	۴۲	مدیر ارشد
۱۰	کارشناسی ارشد	مدیریت امور دفاعی	۲۹	۴۵	عضو هیات علمی
۱۱	کارشناسی ارشد	مدیریت فناوری اطلاعات	۱۲	۳۴	کارشناس ارشد
۱۲	کارشناسی ارشد	مدیریت فناوری اطلاعات	۱۳	۳۸	کارشناس ارشد

۱۳	کارشناسی ارشد	مدیریت امور دفاعی	۲۲	۴۲	عضو هیات علمی
۱۴	کارشناسی ارشد	مدیریت تکنولوژی	۱۱	۳۱	کارشناس ارشد
۱۵	کارشناسی ارشد	مهندسی فناوری اطلاعات	۶	۲۷	کارشناس ارشد
۱۶	کارشناسی ارشد	مدیریت فناوری اطلاعات	۹	۳۴	کارشناس ارشد
۱۷	کارشناسی ارشد	مدیریت امور دفاعی	۲۴	۴۴	مدیر
۱۸	کارشناسی ارشد	مدیریت تکنولوژی	۱۷	۳۸	کارشناس ارشد
۱۹	کارشناسی ارشد	مدیریت فناوری اطلاعات	۱۹	۳۸	عضو هیات علمی
۲۰	کارشناسی ارشد	مدیریت امور دفاعی	۲۸	۴۷	عضو هیات علمی
۲۱	کارشناسی ارشد	مدیریت تکنولوژی	۱۳	۳۴	کارشناس ارشد

فراروندهای حوزه فناوری اطلاعات و ارتباطات

بر اساس تحلیل داده‌های فاز کیفی، ۲۳ عامل به‌عنوان روندهای قابل توجه در حوزه فناوری اطلاعات و ارتباطات شناسایی و با نرم‌افزار میک مک^۱ جهت استخراج عوامل اصلی تأثیرگذار در قالب فراروندها مورد تحلیل قرار گرفتند. ابعاد ماتریس ۲۳×۲۳ بود که در هفت بخش مختلف تنظیم شده است. درجه پرشدگی ماتریس ۸۳/۵۵ درصد است که نشان می‌دهد عوامل انتخاب شده تأثیر زیاد و پراکنده‌ای بر همدیگر داشته‌اند و در واقع سیستم از وضعیت ناپایداری برخوردار است. از مجموع ۴۴۲ رابطه قابل ارزیابی در این ماتریس، ۸۷ رابطه عدد صفر بوده که به این معنا می‌باشد که عوامل بر همدیگر تأثیر نداشته از یا همدیگر تأثیر نپذیرفته‌اند. از طرف دیگر ماتریس بر اساس شاخص‌های آماری با ۲ بار چرخش داده‌ای از مطلوبیت و بهینه‌شدگی ۱۰۰ درصد برخوردار بوده که حاکی از روایی بالایی پرسشنامه و پاسخ‌های آن است. بر این اساس، فراروندهای شناسایی شده در فاز اول پژوهش شامل مدیریت امنیت اطلاعات^۲، شبکه‌های اجتماعی، زیرساخت‌های ارتباطی، شبکه‌های نوآوری در بستر فناوری اطلاعات، هوش مصنوعی^۳، اینترنت اشیا^۴ و مراکز داده^۵ و پایگاه‌های ذخیره اطلاعات می‌باشد که در ذیل به آن‌ها پرداخته شده است.

مدیریت امنیت اطلاعات

1. MicMac
2. Information Security Management
3. Artificial Intelligence (AI)
4. Internet of Things (IoT)
5. Data Center

فناوری اطلاعات و ارتباطات و امنیت اطلاعات، از مباحث اصلی قابل توجه در پیشرفت کشور است. به‌عنوان نمونه، شهرهای هوشمند، از جمله مباحث اصلی قابل توجه در این رابطه است (Vu & Hartley, 2018). از طرف دیگر، یکی از ملاحظات اساسی تحقق اهداف تعیین‌شده در سیاست‌های کلی خودکفایی دفاعی و امنیتی، فناوری اطلاعات و ارتباطات و ضرورت تأمین امنیت اطلاعات به‌عنوان شریان حیاتی بخش دفاع است. امنیت اطلاعات در سازمان، به‌کارگیری یک استراتژی برای دستیابی به وضعیتی است که مدیران مربوطه، توانایی حفاظت از اطلاعات و ارتباطات سازمانی را در برابر انواع ریسک‌ها، آسیب‌ها و حوادثی که سازمان را تهدید می‌کند، داشته باشند (ثامنی توسروندانی و همکاران، ۱۳۹۱). اصطلاح "امنیت اطلاعات"، حوزه وسیعی از آنچه را که باید در ارتباط با حفاظت از اطلاعات و سیستم‌های اطلاعاتی انجام شود، در برمی‌گیرد. محافظت از اطلاعات و سیستم‌های اطلاعاتی در برابر دسترسی، استفاده، افشاء، اختلال، تغییر یا امحای غیرمجاز به‌منظور تأمین محرمانگی، جامعیت و دسترس‌پذیری (Shamala et al., 2017). در گذشته، مدیریت امنیت اطلاعات بیشتر به‌عنوان یک مسئله فنی موردبررسی قرار می‌گرفت و بیشتر توجهات به راه‌حل‌های فناورانه بود؛ ولی این موضوع کافی نبوده و مطالعات نشان می‌دهد که مسائل امنیت اطلاعات، باید در یک زمینه مدیریتی نیز در نظر گرفته شود (Hou et al., 2018). مدیریت امنیت اطلاعات، بخشی از مدیریت اطلاعات است که ضمن تعیین اهداف امنیت و بررسی موانع رسیدن به این اهداف، راهکارهایی را برای آن ارائه می‌دهد (Rajab and Eydgahi, 2018). برای این منظور هر سازمان باید بر اساس روش‌شناسی مشخص و برنامه‌ریزی‌شده‌ای به کنترل و نظارت بر اطلاعات و تبادل اطلاعات در سازمان خود بپردازد (موسوی و همکاران، ۱۳۹۴).

شبکه‌های اجتماعی

شبکه‌های اجتماعی، فناوری‌های مبتنی بر وب و همچنین، موبایل را برای ایجاد یک سیستم بسیار تعاملی ارائه نموده‌اند تا از طریق آن، افراد و جوامع، قادر به اشتراک‌گذاری، بحث و تغییر محتوای تولیدشده توسط شهروندان باشند. استفاده از شبکه‌های اجتماعی، فرصت‌ها و تهدیدهای متنوع و متعددی را برای کشورها، صنایع و اشخاص به همراه داشته است. صنایع دفاعی برای استفاده از شبکه‌های اجتماعی، باید برخی از قابلیت‌های مهم همچون موارد ذیل را ارزیابی نمایند:

۱. ظرفیت: صنعت دفاعی نیازمند ارزیابی روشنی از فعالیت‌های کارکنان و منابع دیگران دارند، لذا باید بر فعالیت‌های مبتنی بر شبکه‌های اجتماعی ایشان نظارت داشته باشند.

۲. فناوری: ارزیابی نیازهای تکنولوژی برای صنعت دفاعی الزامی می‌باشد. صنعت دفاعی با ادغام نمودن سیستم‌ها و داده‌ها با سیستم‌های جدید، از عملکرد بهتر اطمینان می‌یابند.
۳. حمایت نمودن: استفاده از شبکه‌های اجتماعی برای صنایع دفاعی به منظور موفقیت در انجام طرح‌های ابتکاری قابل توجه است، بنابراین صنایع دفاعی باید به ارزیابی تخصص‌های موردنیاز بپردازند تا به موفقیت اجرا و گسترش طرح‌هایشان کمک نماید.
۴. ریسک: با توجه به ماهیت باز و غیرقابل تنظیم بودن شبکه‌های اجتماعی و همچنین، حساسیت بسیار بالا و محرمانگی اطلاعات نظامی و دفاعی، باید به صورت دقیق ریسک شبکه‌های اجتماعی ارزیابی گردد. بنابراین ایجاد مکانیسم‌های کنترل نظارتی قوی اهمیت شایانی برای این موضوع دارد.
۵. داده‌ها: با توجه به ماهیت گسترده و حساس داده‌ها صنایع دفاعی باید به وضوح الزامات را تعریف نمایند و برای بهبود محصولات و خدمات به کارگیرند.
۶. صلاحیت: با توجه به مطرح شدن شبکه‌های اجتماعی، صنایع دفاعی نیازمند ارائه آموزش‌های لازم هستند تا توانایی لازم برای به کارگیری از این شبکه‌ها را داشته باشند.

زیرساخت‌های ارتباطی

با توجه به اهمیت روزافزون نقش اطلاعات در صنایع نظامی و بخش دفاعی، برقراری ارتباطات از راه دور مبتنی بر زیرساخت‌های ارتباطی و اطلاعاتی اهمیت بیشتری پیدا نموده است. بر اساس برنامه سازمان ملل متحد برای تجزیه و تحلیل توسعه اطلاعاتی در کشورهای مختلف، چهار شاخص کلی برای تحلیل میزان توسعه فناوری اطلاعات در کشور مورد توجه و بررسی قرار می‌گیرد که عبارت‌اند از شاخص‌های قابلیت اتصال، شاخص دسترسی، شاخص کاربری و شاخص آزادسازی. شاخص قابلیت اتصال شامل وضعیت زیرساخت‌های فیزیکی برای فناوری اطلاعات قبیل پهنای باند اتصال به اینترنت، تعداد رایانه‌های شخصی، ضریب نفوذ تلفن ثابت و همراه می‌باشد. شاخص دسترسی شامل مشخصه‌های دسترسی از قبیل تعداد کاربران اینترنت، متوسط تبادل اطلاعات از طریق مخابرات و مرکز تبادل اطلاعات اینترنتی می‌باشد. شاخص‌های آزادسازی نیز شامل انجام دگرگونی‌های ساختاری با توجه به تبدلات و رقابت‌های اینترنتی در بخش مخابرات و ارتباطات کشور برای انطباق و جذب فناوری اطلاعات است. از دید کلان ملی، آمادگی الکترونیکی بیانگر به کارگیری زیرساخت‌های ارتباطی و اطلاعاتی یک کشور، توانایی کاربران آن کشور، کسب و کار و دولت‌ها در به کارگیری و بهره‌گیری از مزایای فناوری اطلاعات و ارتباطات است. درنهایت، ضریب

نفوذ تلفن همراه از موارد اساسی قابل توجه در حوزه فراروندهای حوزه فناوری اطلاعات است (Pratt et al., 2012).

شبکه‌های نوآوری در بستر فناوری اطلاعات

یکی از ویژگی‌های اصلی وجود فناوری اطلاعات و ارتباطات، بهبود سریع نوآوری و توانمندسازی نوآوری می‌باشد. فناوری اطلاعات و ارتباطات باعث ایجاد روابط نزدیک‌تر بین صنایع، شرکت‌ها، کاربران، عرضه‌کنندگان و سایر ذینفعان صنایع دفاعی می‌گردد. همچنین موانع جغرافیایی را کاهش می‌دهد و به ایجاد دانش جدید و انتشار سریع‌تر و کارآمدتر اطلاعات در بین بخش‌های داخلی صنعت دفاعی و بین بخش‌های خارجی آن، کمک می‌نماید.

هوش مصنوعی

در طول جنگ سرد، سلاح منتخب، موشکی باقابلیت حمل کلاهک‌های اتمی بود، اما امروز نرم‌افزارها هستند که برای حمله به سیستم‌های کامپیوتری و یا اهدافی در دنیای واقعی مورد استفاده قرار می‌گیرند. کارشناسان می‌گویند نگران‌اند که ممکن است دنیا وارد جنگ سرد دیگری شود و یا احتمالاً، در حال حاضر وارد شده باشد. جنگ سردی که از طریق هوش مصنوعی پشتیبانی می‌شود. هوش مصنوعی به سیستم‌هایی گفته می‌شود که می‌توانند واکنش‌هایی مشابه رفتارهای هوشمند انسانی از جمله درک شرایط پیچیده، شبیه‌سازی فرایندهای تفکری و شیوه‌های استدلالی انسانی و پاسخ موفق به آن‌ها، یادگیری و توانایی کسب دانش و استدلال برای حل مسائل را داشته باشند. با توجه به اهمیت هوش مصنوعی، این روزها کشورهای مختلف در حال رقابت با یکدیگر در زمینه هوش مصنوعی و به‌کارگیری آن در زمینه نظامی هستند. هوش مصنوعی، آینده دنیا را تحت تأثیر قرار خواهد داد و تغییرات جالبی در دنیا ایجاد خواهد کرد. هر کشوری که بتواند در زمینه هوش مصنوعی پیشرو باشد، در واقع می‌تواند بر دنیا حکمرانی کند. همه کشورها از اهمیت هوش مصنوعی آگاه‌اند و هوش مصنوعی باعث حفظ نیروی انسانی در صنعت دفاعی و به‌کارگیری متناسب آن با حداقل تلفات خواهد شد. استفاده از هوش مصنوعی در حمل‌ونقل هوایی، نیروی دریایی، سامانه‌های زمینی، سایبری و پهبادها، سامانه‌های موشکی و غیره به‌صورت روزافزون مورد توجه قرار گرفته است. صنایع دفاعی‌های جهان به دنبال تبدیل هوش مصنوعی به یک فناوری کلیدی در زمینه قدرت ملی هستند. این تحول، تغییرات نظامی و امنیت

ملی را به همراه خواهد داشت، روند سیاسی دولت‌های مختلف را متفاوت خواهد کرد و تأثیر آن حتی از دستیابی به انرژی هسته‌ای نیز مهم‌تر خواهد بود.

اینترنت اشیاء

اینترنت اشیا یا به بیانی دقیق‌تر، «اینترنت چیزها» یعنی اتصال دستگاه‌های فیزیکی به هم‌دیگر از طریق نرم‌افزارهای خاص، حسگرها و غیره است. در این فناوری به نسبت نوپا، تمامی دستگاه‌های متصل به یک شبکه، توانایی این را دارند که کارهایشان را به صورت خودکار انجام دهند؛ بر اساس تغییراتی که در محیط اطرافشان رخ می‌دهد، یک سری پاسخ ویژه را به صورت کاملاً خودکار از خود نشان دهند و همچنین می‌توانند داده‌های مختلف را بدون هرگونه دخالت انسان، با دیگر دستگاه‌های شبکه مبادله کنند. شاکله اصلی این فناوری جدید، بر پایه شبکه بی‌سیم و اینترنت ساخته شده و هدف اصلی آن، بهبود کارایی و دقت دستگاه‌های مختلف است. به کارگیری فناوری‌های مرتبط با اینترنت اشیا توسط صنایع دفاعی در درجه اول متمرکز بر برنامه‌های جنگی بود. فرماندهی، کنترل، ارتباطات، رایانه، اطلاعات، نظارت و سامانه‌های شناسایی، میلیون‌ها حسگر را برای آگاهی بخشی به فرماندهان ارشد و سربازان حاضر در زمین و دریا و هوا در اختیار قرار می‌دهد. اینترنت اشیا همچنین کاربردهای غیرجنگی دارد، از جمله لجستیک دفاعی، شناسایی فرکانس‌های رادیویی، برچسب‌های ردیابی محموله‌ها. اینترنت اشیا همچنین در موارد آموزشی مانند برنامه‌های شبیه‌سازی نیز مورد استفاده قرار می‌گیرد. در آینده نزدیک شاهد نفوذ بالای اینترنت اشیا در صنایع نظامی خواهیم بود.

مراکز داده و پایگاه‌های ذخیره اطلاعات

با زیاد شدن کاربران و بالا رفتن حجم مستندات، و نیز سادگی انتشار اطلاعات در اینترنت، مفاهیم نظامی نیز وارد عرصه اینترنت شدند. صنایع نظامی نیاز به سرورهایی داشتند که این امکان را به آن‌ها بدهد که به سادگی و با سرعت بتوانند اطلاعات خود را در اختیار مشتریان و کاربران خود قرار دهند. بالطبع این امکان وجود نداشت که هر شرکت یا سازمانی که قصد راه‌اندازی سایت‌های اینترنتی را دارد، خود رأساً اقدام به راه‌اندازی سرور خود کند، چراکه با وجود کاربران زیاد این سایت‌ها و حجم بالای ترافیک، نیاز به اتصال‌هایی با سرعت‌های بسیار بالا وجود داشت که مسلماً حتی در صورتی که این امکان از لحاظ عملی وجود داشته باشد، هزینه بالایی را می‌طلبید. راه‌حلی که برای این مشکل به نظر رسید، راه‌اندازی مراکز خاصی تحت عنوان مراکز داده بود. مراکز داده

با در اختیار داشتن اتصالات پرسرعت به اینترنت، و همچنین در اختیار داشتن سرورهای قوی و متعدد، امکان راه‌اندازی سرورهای وب را برای عموم مردم ممکن ساختند. مرکز داده، بسته به نوع کاربردی که برای آن تعریف شده است، می‌تواند به‌عنوان یک مرکز پردازشی، مرکز ذخیره داده، مرکز جمع‌آوری داده یا تمامی این موارد عمل کند. مراکز داده بسیار عظیم و متنوعی در سرتاسر شبکه جهانی اینترنت در حال سرویس‌دهی هستند که برخی از این مراکز استفاده تجاری محدود درون‌سازمانی دارند و برخی دیگر در اینترنت به‌صورت تجاری یا عمومی قابل استفاده هستند.

تحلیل داده‌ها و یافته‌های فاز کمی

پس از اتمام فاز کیفی و به‌منظور ارزیابی نتایج حاصل، از پرسشنامه استفاده شده است. پرسشنامه دارای دو بخش است که در بخش اول، اطلاعات مربوط به پاسخ‌دهندگان شامل تجربه کاری، سن و غیره مورد سؤال قرار گرفته است. در بخش دوم، فراروندهای نهایی حاصل از فاز کیفی پژوهش مورد سؤال قرار گرفته است. با توجه به ماهیت پرسشنامه تهیه شده و تخصص موردنیاز برای پاسخ‌دهندگان، جامعه آماری شامل ۹۳ نفر از متخصصان و فعالان حوزه فناوری اطلاعات و ارتباطات بخش دفاع در شهر تهران در نظر گرفته شد. با توجه به ساختار جامعه آماری و شناسایی متخصصان مربوطه، نمونه به‌صورت تمام شمار در نظر گرفته شد و پرسشنامه بین تمامی اعضا توزیع شد. تعداد ۹۷ پرسشنامه توزیع گردید که از این تعداد، ۹۱ پرسشنامه به‌منظور تحلیل داده‌ها قابل استفاده بودند. اطلاعات مربوط به مشارکت‌کنندگان در تکمیل پرسشنامه به شرح جدول (۵) است:

جدول (۵) اطلاعات جمعیت شناختی پاسخ‌دهندگان به پرسشنامه

سطح تحصیلات		تعداد	
دکتری		۱۱	
کارشناسی ارشد		۶۳	
کارشناسی		۱۷	
سن	تعداد	سابقه	تعداد
۲۵ تا ۳۵ سال	۱۹	کمتر از ۵	۱۴
۳۵ تا ۴۵ سال	۵۱	۵ تا ۱۰	۲۶
بیشتر از ۴۵ سال	۲۱	۱۱ تا ۱۵	۲۴
		بیشتر از ۱۵	۲۷

بدین ترتیب از پاسخ‌دهندگان خواسته شد که میزان اهمیت هر یک از عوامل را به‌عنوان فراروندهای قابل توجه حوزه فناوری اطلاعات و ارتباطات مؤثر بر آینده‌نگاری صنعت دفاعی بر اساس طیف لیکرت پنج‌گزینه‌ای مشخص نمایند. به‌منظور ارزیابی تجزیه و تحلیل مناسب داده‌های حاصل از پرسشنامه از آزمون تی تک نمونه‌ای بهره گرفته شده است.

بررسی روایی پرسشنامه

برای تأیید روایی پرسشنامه ضمن بررسی دقیق مبانی نظری موجود، جمع‌آوری و تحلیل داده‌ها از منابع مختلف و انجام مصاحبه‌ها، پرسشنامه نهایی قبل از توزیع، در اختیار هشت نفر از خبرگان حوزه قرار داده شد و پس از اعمال اصلاحات موردنظر ایشان، مورد تأیید قرار گرفته و توزیع شد.

بررسی پایایی پرسشنامه

پایایی پرسشنامه با آزمون آماری آلفای کرونباخ بررسی و مورد تأیید قرار گرفته است. در پژوهش حاضر برای محاسبه آلفای کرونباخ از نرم‌افزار SPSS استفاده شده است و مقدار آلفای به‌دست‌آمده در نمونه اولیه شامل ۲۵ پرسشنامه برابر با ۰/۸۹۱ می‌باشد که نشان‌دهنده این است که پرسشنامه دارای پایایی مناسب می‌باشد. آلفای محاسبه‌شده برای تمامی پاسخنامه‌ها نیز ۰/۹۲۴ می‌باشد.

جدول (۶) پایایی پرسشنامه

نوع آزمون	مقدار ضریب آلفا	حجم نمونه
آزمون اولیه	۰/۸۹۱	۲۵
آزمون کلی	۰/۹۲۴	۹۱

تحلیل داده‌های پرسشنامه با آزمون تی تک نمونه‌ای (اهمیت هر یک از عوامل را به‌عنوان فراروندهای قابل توجه حوزه فناوری اطلاعات و ارتباطات مؤثر بر آینده‌نگاری صنعت دفاعی) برای بررسی معناداری ابعاد، با توجه به نرمال بودن داده‌ها از آزمون پارامتریک تی تک نمونه‌ای استفاده می‌شود. در سطح اطمینان ۹۵ درصد چنانچه سطح معناداری کمتر از ۰/۰۵ باشد و میانگین متغیرها از حد متوسط ۳ بیشتر باشد، فرضیه تأیید و در غیر این صورت رد می‌شود. برای استفاده از آزمون تی تک نمونه‌ای هفت فرض برای فراروندها به شکل زیر و به‌صورت جداگانه برای هر فراروند مطرح می‌گردد:

- فراروندهای مدیریت امنیت اطلاعات، شبکه‌های اجتماعی، زیرساخت‌های ارتباطی، شبکه‌های نوآوری در بستر فناوری اطلاعات، هوش مصنوعی، اینترنت اشیاء و مراکز داده و پایگاه‌های ذخیره

اطلاعات؛ از جمله فراروندهای قابل توجه حوزه فناوری اطلاعات و ارتباطات مؤثر بر آینده‌نگاری صنعت دفاعی هستند.

فرض‌های آماری در سطح اطمینان ۹۵ درصد تعریف می‌شود که با توجه به تعداد زیاد، یک مورد از آن ذکر شده و از ذکر سایر موارد صرف نظر شده است:

فرض صفر (H0): مدیریت امنیت اطلاعات از جمله فراروندهای قابل توجه حوزه فناوری اطلاعات و ارتباطات مؤثر بر آینده‌نگاری صنعت دفاعی است (میانگین برابر یا کمتر از ۳ است).

فرض مقابل (H1): مدیریت امنیت اطلاعات از جمله فراروندهای قابل توجه حوزه فناوری اطلاعات و ارتباطات مؤثر بر آینده‌نگاری صنعت دفاعی نیست (میانگین بیشتر از ۳ است).
نتایج آزمون در جدول (۷) آمده است.

جدول (۷) نتایج آزمون تی برای تحلیل میزان تأثیر هر یک از مضامین

ردیف	متغیر	میانگین	سطح معناداری	نتیجه آماری
۱	مدیریت امنیت اطلاعات	۴/۸۳۴۲	۰/۰۰۰	تأیید فرض مقابل
۲	شبکه‌های اجتماعی	۴/۶۷۷۲	۰/۰۰۰	تأیید فرض مقابل
۳	زیرساخت‌های ارتباطی	۴/۴۳۳۴	۰/۰۰۰	تأیید فرض مقابل
۴	شبکه‌های نوآوری در بستر فناوری اطلاعات	۴/۱۱۲۲	۰/۰۰۰	تأیید فرض مقابل
۵	هوش مصنوعی	۳/۸۹۹۲	۰/۰۰۰	تأیید فرض مقابل
۶	اینترنت اشیاء	۳/۵۴۴۴	۰/۰۰۰	تأیید فرض مقابل
۷	مراکز داده و پایگاه‌های ذخیره اطلاعات	۳/۴۴۴۴	۰/۰۰۰	تأیید فرض مقابل

یافته‌ها در جدول فوق نشان می‌دهد که میانگین تمامی متغیرها از سطح متوسط (۳) بیشتر است و همچنین سطح معناداری کمتر از ۰/۰۵ و معنادار می‌باشد. با توجه به یافته‌های فاز کمی، یافته‌های فاز کیفی مورد تأیید قرار گرفته و فراروندهای هفت‌گانه مدیریت امنیت اطلاعات، شبکه‌های اجتماعی، زیرساخت‌های ارتباطی، شبکه‌های نوآوری در بستر فناوری اطلاعات، هوش مصنوعی، اینترنت اشیاء و مراکز داده و پایگاه‌های ذخیره اطلاعات در آینده‌نگاری صنعت دفاعی قابل توجه هستند.

نتیجه‌گیری و پیشنهادها

پژوهش حاضر باتوجه به اهمیت روزافزون صنعت دفاعی تدوین گردیده است. آینده‌نگاری یکی از مباحث بحث‌برانگیز و سرنوشت‌ساز برای هر صنعت در هر عرصه‌ای می‌باشد. در مطالعه آینده‌نگاری فعالیت‌های سازمان‌ها را با در نظر داشتن چالش‌ها و روندهای و فراروندهای آینده آنان موردبررسی قرار می‌دهند. صنعت دفاعی به‌عنوان یکی از بزرگ‌ترین صنایع کشور می‌تواند در راستای تحقق چشم‌انداز توسعه ۱۴۰۴ نقش مؤثری داشته باشد. همچنین با توجه به رشد روزافزون فناوری‌های نوین و خاصیت فناوری اطلاعات و ارتباطات و اثرگذاری آن بر فعالیت‌های گوناگون یک کشور یکی از حوزه‌های است که می‌تواند در این راستا مؤثر واقع گردد.

هدف این پژوهش شناسایی فراروندهای حوزه فناوری اطلاعات و ارتباطات بود که در آینده‌نگاری صنعت دفاعی قابل توجه هستند. فراروندهای هفت‌گانه مدیریت امنیت اطلاعات، شبکه‌های اجتماعی، زیرساخت‌های ارتباطی، شبکه‌های نوآوری در بستر فناوری اطلاعات، هوش مصنوعی، اینترنت اشیا و مراکز داده و پایگاه‌های ذخیره اطلاعات در این رابطه قابل توجه هستند. با توجه به یافته‌ها، دولت می‌تواند با سرمایه‌گذاری‌های فیزیکی، انسانی و کاهش هزینه‌های اینترنتی و مخابراتی در زمینه ایجاد زیرساخت‌های مناسب و همچنین گسترش استفاده از آن به صنعت دفاعی رونق بخشد. از طرف دیگر، صنعت دفاعی باید با آخرین پیشرفتهای حوزه فناوری اطلاعات و ارتباطات همگام شود تا این صنعت همگام با علم جلو برود؛ بنابراین باید از نیروهای انسانی ماهر در این صنعت استفاده شود. در این امتداد، استفاده بهینه از ظرفیت‌های موجود و استفاده از نرم‌افزارهای که بتوانند بدین طریق کارایی زیرساخت‌ها را بالا ببرند نیز قابل توجه خواهد بود. از آنجایی که بخش دفاع همانند سایر سازمان‌ها، باید بر اساس روش‌شناسی مشخص و برنامه‌ریزی‌شده‌ای به کنترل و نظارت بر اطلاعات و تبادل اطلاعات در سازمان خود پردازد، تدوین و اتخاذ استراتژی متناسب در این رابطه ضروری به نظر می‌رسد تا بتواند هدف جامع‌نگری را محقق سازد، زیرا اصطلاح "امنیت اطلاعات"، حوزه وسیعی از آنچه را که باید در ارتباط با حفاظت از اطلاعات و سیستم‌های اطلاعاتی انجام شود، در برمی‌گیرد که محافظت از اطلاعات و سیستم‌های اطلاعاتی در برابر دسترسی، استفاده، افشاء، اختلال، تغییر یا امحای غیرمجاز به‌منظور تأمین محرمانگی، جامعیت و دسترس‌پذیری، از جمله آن هستند. به همین منظور، اتخاذ نگاه جامع و کل‌نگر در این رابطه بسیار ضروری است. نکته قابل توجه دیگر، استفاده ناکارآمد از زیرساخت ارتباطی موجود است که نیازمند هم‌راستایی بخشهای مختلف صنعت دفاعی در کشور است. ایجاد کمیته رصد و راهبری فضای مجازی در صنعت دفاعی، تدوین سند راهبردی توسعه اینترنت اشیا و ابزارهای مبتنی بر آن در صنایع دفاعی و یکپارچه‌سازی و همگرایی سیاست‌های

حاکم بر استقرار، حفظ و ارتقاء مراکز داده و پایگاه‌های ذخیره اطلاعات، از جمله موارد قابل توجه در این رابطه هستند.

پژوهش در بخش دفاع و صنایع وابسته با توجه به ممنوعیت‌های ذاتی ارائه اطلاعات مرتبط، با محدودیت‌های جدی مواجه است. دسترسی به اطلاعات محرمانه و کارکنان مرتبط و ارائه یافته‌های به‌صورت کاربردی و عملیاتی، نیازمند ظرافت و دقت ویژه‌ای است، به‌نحوی که جنبه محرمانگی حفظ شود. بر این اساس، علاوه بر محدودیت‌های فعالیت در حوزه فناوری اطلاعات و ارتباطات، محدودیت اصلی و اساسی پژوهش حاضر، محرمانگی محتوای اطلاعات و کارکنان مرتبط با آن است.

منابع

- استیری، روح الله، و مشیری، بنیامین. (۱۳۸۸). ابزارهای تأمین مالی بنگاه‌های دانش بنیان، مجموعه مقالات دومین کنفرانس بین المللی توسعه نظام تأمین مالی در ایران، تهران: مرکز مطالعات تکنولوژی دانشگاه صنعتی شریف.
- امامی، سیدمجید. (۱۳۹۲). از جامعه شناسی تاریخی ایران تا نظریه سیاستی پیشرفت (توسعه)؛ نقش پارادایم ماهیت گرا در ترسیم الگوی اسلامی- ایرانی هویت ملی، *فصلنامه مطالعات ملی*؛ ۵۶ (۴).
- بنیاد توسعه فردا، (۱۳۸۴). *روش‌های آینده‌نگاری*، تهران: نشر بنیاد توسعه فردا.
- ثامنی توسروندانی، مرضیه. و همکاران. (۱۳۹۱). رویکرد نگاشت تهدیدها و قابلیت‌های آسیب پذیری در شبکه‌های محلی به کنترل‌های استاندارد ISO/IEC 27002 سیستم مدیریت امنیت اطلاعات. *چهارمین کنفرانس مهندسی برق و الکترونیک ایران، دانشگاه آزاد اسلامی گناباد.*
- خزایی، سعید. (۱۳۹۰). *آینده پژوهی، مفاهیم و ضرورت‌ها*، پایگاه اینترنتی آینده‌پژوهی.
- خوش چهره، مجید. و نیک بخش حبیبی، (۱۳۹۱). اصول پایه‌ای و عناصر کلیدی الگوی اسلامی- ایرانی پیشرفت از منظر اسناد فرادستی نظام ج.ا.ایران، *فصلنامه راهبرد*، ۲۱ (۶۲): ۲۴۴-۲۱۹.
- دانایی فرد، حسن، الوانی، سید مهدی. و آذر، عادل (۱۳۸۶). *روش شناسی پژوهش کیفی در مدیریت: رویکردی جامع*. تهران: نشر صفار.
- زالی، نادر. (۱۳۹۰). *آینده‌نگاری راهبردی و سیاست‌گذاری منطقه‌ای با رویکرد سناریونویسی*، *فصلنامه مطالعات راهبردی*، ۴(۴): ۵۴-۳۳.
- عباسی شاه کوه، کلثوم، سلطانی دلگشا، محمد، واحیدیان، افسانه. و عبدالهی، علی. (۱۳۸۷). ارائه شیوه علمی برای سازماندهی مطالعه آینده‌نگاری فناوری، *فصلنامه رهیافت*، ۴۳: ۵-۹.
- فاتح‌راد، مهدی، جلیلود، محمدرضا. و نصراللهی وسطی، لیل. (۱۳۹۲). *درآمدی بر مبانی معرفت شناسی و روش شناسی آینده‌پژوهی*، *فصلنامه مطالعات آینده پژوهی*، ۲ (۸): ۵۲-۲۷.
- قاضی‌زاده، سید ضیاءالدین. (۱۳۸۹). *الگوی اسلامی ایرانی پیشرفت و نقش نیروهای مسلح*، *فصلنامه راهبرد دفاعی*، ۸ (۳۱): ۶۲-۳۱.
- قدیری، روح‌اله، ناظمی، علی، شماعی، علی. و شفیعی، سونیا. (۱۳۸۵). *ضرورت توجه به تمامی ابعاد آینده‌نگاری در طراحی پروژه آینده‌نگاری*، *همایش آینده‌پژوهی، فناوری و چشم‌انداز توسعه*، تهران: دانشگاه صنعتی امیرکبیر.
- کیوان حسینی، سیداصغر. و جمعه زاده، راحله. (۱۳۹۰). *پیوندبخشی میان رویکرد دفاع همه جانبه و الگوی اسلامی ایرانی پیشرفت؛ چارچوب پیشنهادی*، *فصلنامه راهبرد دفاعی*، ۹ (۳۴): ۲۵-۱.

- موسوی، پریسا و همکاران. (۱۳۹۴). شناسایی ریسک های امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری. فصلنامه مدیریت فناوری اطلاعات، ۷ (۱).
- Bezold, C. (2010). Lessons from using scenarios for strategic foresight. *Technological Forecasting and Social Change*, 77(9): 1513-1518.
- Biswas, R. (2016). *Asian Megatrends*, Palgrave Macmillan UK.
- Brownlie, D. (1998). High minds and low deeds: On being blind to creativity in strategic marketing. *Journal of Strategic Marketing*, 6(2):117-130.
- Chen, H., Wakeland, W., & Yu, J. (2012). A two-stage technology foresight model with system dynamics simulation and its application in the Chinese ICT industry. *Technological Forecasting and Social Change*, 79(7): 1254-1267.
- Colwell, K. & Narayanan, V. K., (2010). Foresight in economic development policy: shaping the institutional context for entrepreneurial innovation. *Futures*, 42 (4): 295-303.
- Diamandis, P. (2012). *Abundance is Our Future*, available at http://www.ted.com/talks/peter_diamandis_abundance_is_our_future last accessed 14 September 2015.
- Diesen, G. & Keane, C. (2018). The offensive posture of NATO's missile defense system, *Communist and Post-Communist Studies*, 51 (2): 91-100.
- Dufva, M. & Ahlqvist, T. (2015). Elements in the construction of future-orientation: a systems view of foresight. *Futures*, 73: 112-125.
- Durance, P. & Godet, M. (2008). *La prospective stratégique pour les entreprises ET les territoires*, Paris, Dunod.
- European Environment Agency, (2015). *Assessment of Global Megatrends an Update available*, at <http://www.eea.europa.eu/themes/scenarios/global-megatrends> (last accessed 12 September 2015).
- Fitjar, R. D. & Rodríguez-Pose, A. (2013), Firm collaboration and modes of innovation in Norway, *Research Policy*, 42:128- 138.
- Forrester (2010). *15 technology trends to watch for*, Accessed at www.Forrester.Com/reports.
- Futures, F. (2002). *Foresight Futures 2020-Revised scenarios and guidance*. UK Department of Trade and Industry, 32.
- Harper, J.C. (2013). Impact of Technology Foresight, *Nesta Working Paper No. 13/16*. (www.nesta.org.uk/wp13-16).
- Hou, Y., Ping, G. & Nicholson, B. (2018). Understanding organizational responses to regulative pressures in information security management: The case of a Chinese hospital, *Technological Forecasting and Social Change*, 126: 64-75.
- Johnston, R. (2012). Developing the capacity to assess the impact of Foresight. *Foresight* 14 (1): 56-68.

- Keller, J. Markmann., C., & von der Gracht, H. (2015). Foresight support systems to facilitate regional innovations: A conceptualization case for a German logistics cluster, *Technological Forecasting and Social Change*, 27: 15–28.
- Kim, D. J. (2012). Strategic Foresight: The Case of TJ Park and POSCO. *Journal of International and Area Studies*, 19(1): 45–57.
- Lee, S. M. & Kwon Lee, C. (2002). E-company CEO web sites: contents and information value. *Management Decision*, 40(2): 158-167.
- Lee, S. M., Ribeiro, D., Olson, D. L. & Roig, S. (2007). The importance of the activities of service business in the economy: welcome to the Service Business. *An International Journal. Service Business*, 1(1): 1-5.
- Liebl, F. & Schwarz, J. O. (2010). Normality of the future: Trend diagnosis for strategic foresight. *Futures*, 42(4): 313–327.
- Madrueno, R. & Tezanos, S. (2018). The contemporary development discourse: *Analyzing the influence of development studies' journals*, *World Development*. 109: 334-345.
- Malik, T. (2018). Defense investment and the transformation national science and technology: A perspective on the exploitation of high technology, *Technological Forecasting and Social Change*, 127: 199-208.
- Martin, B. (1995). Foresight in Science and Technology, *Journal of Technology Analysis & Strategic Management*, 7(2): 139-168.
- Meissner, D. (2012). Results and impact of national foresight studies. *Futures* 44(10): 905–913.
- Miles, I. (2010). The development of technology foresight: a review. *Technol. Forecast*, 77 (9): 1448–1456.
- Moyer, J. & Bohl, D. (2019). Alternative pathways to human development: Assessing trade-offs and synergies in achieving the Sustainable Development Goals. *Futures*, 105: 199-210.
- Müller-Stewens, G., Mueller, A., & Lüders, V. (2012). The management of strategic-foresight activities: Evidence from large European multinationals. In *Systemic Management for Intelligent Organizations*, Springer Berlin Heidelberg, pp. 63-82.
- Naisbitt, J. (1982). *Megatrends: Ten New Directions Transforming Our Lives*. New York: Warner Books.
- Peperhove, R., & Luoto, L. (2013). *Scientific Quality in Foresight Studies – Reflecting and Discussing Criteria for their Assessment*, Paper Presented at the European IFA Academic Seminar: Participatory Foresight for Smarter Futures – From Design to Impact September 16–19, ZHAW, Technopark Winterthur (Zurich), Switzerland.
- Pratt, M. Sarmiento, Montes, F. (2012). The implications of megatrends in information and communication technology and transportation for changes in global physical activity. 380 (9838): 282-293.

- Quesada, J., Mendes, A., De Orta, M. & Ponkratova, E. (2014). *Five global megatrends continue to advance*, Global Megatrends Mexico Focus. www.PWC.co
- Rajab, M. & Eydgahi, A. (2018). *Evaluating the Explanatory Power of Theoretical Frameworks on Intention to Comply with Information Security Policies in Higher Education, Computers & Security*, Available online 13 October 2018, In Press.
- Rohrbeck, R. & Schwarz, J. O. (2013). The value contribution of strategic foresight: Insights from an empirical study of large European companies. *Technological Forecasting and Social Change*, 80(8): 1593-1606.
- Roney C. W. (2010). Intersections of strategic planning and futures studies: methodological complementarities, *Journal of Futures Studies*, 15: 71- 100.
- Saritas, O. Taymaz, E. & Tumer, T. (2007). Vision 2023: Turkey's national Technology Foresight Program: A contextualist analysis and discussion. *Technological Forecasting and Social Change*, 74(8): 1374-1393.
- Sceral, M, Erkoyuncu, J. & Shehab, E. (2018). Identifying information asymmetry challenges in the defense sector, *Procedia Manufacturing*, 19: 127-134.
- Schartinger, D., Wilhelmer, D., Holste, D. & Kubeczko, K. (2012). Assessing immediate learning impacts of large foresight. *Emerald*, 14(1): 41-55.
- Schreiber, U. (2015). Megatrends 2015 making sense of a world in motion.
- Shamala, P., Rabiah, A., Zolaitc, A. & Sedek, M. (2017). Integrating information quality dimensions into information security risk management (ISRM), *Journal of Information Security and Applications*, 36:1-10.
- Singh, N., Bartikowski, B. P., Dwivedi, Y. K. & Williams, M. D. (2009). Global megatrends and the web: Convergence of globalization, networks and innovation. *ACM SIGMIS Database*, 40(4): 14-27.
- Sokolova, A. (2015). An integrated approach for the evaluation of national foresight: the Russian case. *Technol. Forecast. Soc. Chang.* 101: 216-225.
- Sunter, C. (2013). *21st Century Megatrends – Perspectives from a Fox*. Human and Rousseau/Tafelberg Publishers, Cape Town.
- Tsoukas H., & Sheperd J. (2004). Coping with the future: developing organizational foresightfulness – introduction, *Futures*, 36: 137-144.
- Van Lente, H. (2012). Navigating foresight in a sea of expectations: lessons from the sociology of expectations. *Technol. Anal. Strateg. Manag.* 24 (8), 769–782.
- Voros, J. (2003). A generic foresight process framework. *Foresight*, 5(3): 10-21.
- Vu, K. & Hartley, K., (2018). Promoting smart cities in developing countries: Policy insights from Vietnam. *Telecommunications Policy*, 42 (10): 845-859.