فصلنامهٔ امنیت پژوهی (علمی-پژوهشی)
سال بیست‌وسوم: شماره ۸۶- تابستان ۱۴۰۳
صص: ۲۹ - ۵۰
تاریخ دریافت: ۱۴۰۳/۱۲/۰۷
تاریخ پذیرش: ۱۴۰۴/۰۴/۲۱

Amniat Pajouhi: Security Research Quarterly
Vol.23, No.86,Summer 2024
P-P: 29 - 50

چالش‌ها و راهکارهای مقابله با جعل عمیق در حوزه امنیت و فعالیت‌های اطلاعاتی

جمشید نصرت‌آبادی*[۱]
احمد زوارتربتی[۲]
اسماعیل اسماعیل‌پور[۳]

چکیده

پیشرفت سریع فنّاوری‌های اطلاعاتی، فرصت‌های متعددی را برای جوامع انسانی فراهم کرده است، اما هم‌زمان چالش‌های پیچیده‌ای را نیز به همراه داشته است. یکی از مهم‌ترین این چالش‌ها، فنّاوری جعل عمیق است که با استفاده از الگوواره‌های یادگیری عمیق، امکان دست‌کاری واقع‌گرایانه تصاویر، ویدئوها و صداها را فراهم می‌کند. این فنّاوری، علاوه بر جنبه‌های مثبت آن در حوزه‌هایی نظیر سینما و تبلیغات، تهدیدی جدی برای امنیت ملی و اجتماعی به شمار می‌آید. جعل عمیق می‌تواند به تخریب اعتماد عمومی، ایجاد ناآرامی‌های اجتماعی و تضعیف نهادهای اطلاعاتی و امنیتی منجر شود. این مقاله با هدف بررسی چالش‌های ناشی از جعل عمیق در فعالیت‌های اطلاعاتی و امنیتی و ارائه راهکارهای مقابله با آن تدوین شده است. یافته‌های پژوهش نشان می‌دهند که توسعه ابزارهای تشخیص هوشمند، افزایش سواد رسانه‌ای و طراحی سامانه‌های پیشرفته احراز هویت می‌توانند نقش کلیدی در کاهش تهدیدات مرتبط با جعل عمیق ایفا کنند. همچنین، پیشنهادهایی برای استفاده از فنّاوری‌های نوین جهت تقویت امنیت اطلاعاتی و عملیاتی ارائه شده است.

واژگان کلیدی: جعل عمیق، امنیت ملی، اطلاعات جعلی، یادگیری عمیق، هوش مصنوعی

---

۱. استادیار دانشکده فارابی،(نویسنده مسئول)DR.NOSRATABADI110@gmail.com
۲. استادیار دانشکده فارابی،zavvarahmad@gmail.com
۳. کارشناسی ارشد دانشکده فارابیimanipo2000@yahoo.com

مقدمه

تحولات بی‌سابقه در حوزه فنّاوری‌های اطلاعاتی و ارتباطی، تأثیرات گسترده‌ای بر ابعاد مختلف زندگی انسان‌ها، از تعاملات اجتماعی گرفته تا امنیت ملی و سازمانی، داشته است. یکی از مهم‌ترین فنّاوری‌های نوظهور که اخیراً توجه بسیاری را به خود جلب کرده، فنّاوری جعل عمیق است. این فنّاوری که بر پایه الگوواره‌های یادگیری عمیق توسعه یافته است، امکان تغییر و دست‌کاری تصاویر، ویدئوها و حتی صداها را با دقت و واقع‌گرایی بالا فراهم می‌کند.

گرچه جعل عمیق در حوزه‌هایی نظیر تولید محتوای هنری، صنعت فیلم‌سازی و بازاریابی دیجیتال می‌تواند ابزار قدرتمندی باشد، اما تهدیدات امنیتی ناشی از آن را نمی‌توان نادیده گرفت. استفاده‌های مخرب از این فنّاوری، از تولید اخبار جعلی گرفته تا جعل هویت مقامات، قابلیت ایجاد بحران‌های گسترده در سطوح ملی و بین‌المللی را داراست. این امر به‌ویژه در حوزه فعالیت‌های اطلاعاتی، جایی که صحت و دقت اطلاعات نقشی کلیدی در تصمیم‌گیری‌های امنیتی ایفا می‌کند، اهمیت بیشتری پیدا می‌کند.

هدف از این پژوهش، بررسی ابعاد مختلف چالش‌های مرتبط با جعل عمیق در حوزه اطلاعاتی و امنیتی است. این مقاله تلاش می‌کند با ارائه یک چارچوب تحلیلی، ضمن تبیین چالش‌های اصلی این فنّاوری، راهکارهای کاربردی و مبتنی بر فنّاوری‌های نوین برای مقابله با آن را پیشنهاد دهد.

این تحقیق از یک‌سو بر اهمیت توسعه ابزارهای شناسایی جعل عمیق تأکید دارد و از سوی دیگر، بر ضرورت افزایش سواد رسانه‌ای و فنّاوری در جامعه به‌عنوان راهکاری پیشگیرانه تأکید می‌کند. امید است این پژوهش بتواند گامی مؤثر در جهت ارتقای امنیت ملی و کاهش تهدیدات ناشی از فنّاوری‌های نوظهور باشد.

جستارگشایی

جعل عمیق[1]، در ۲۰۱۷ میلادی، به پیروی از نام کاربری یک کاربرReddit انجام شده است. در ابتدای امر، وی از فنّاوری یادگیری عمیق به‌منظور جای‌گذاری چهره سلبریتی‌ها

1. Deep Fake

به‌جای چهره افراد در هرزه‌نگاری بهره گرفته بود؛ و ترکیبی از یادگیری عمیق[1] و جعل[2] بوده است به‌نحوی‌که بیننده تصور می‌کند ویدیوی تولیدشده، واقعیت دارد؛ اما واقعی نیست؛ گاهی این ویدیوها می‌توانند به‌صورت سخنرانی رهبران کشورها و سیاستمداران و یا رهبران مذهبی یک ملت باشند و باعث بحران‌ها و ناآرامی‌هایی از طرف مردمان کشورهای دیگر نسبت به دولت‌های دیگر کشورها شوند. حتی گاهی در رقابت‌های انتخاباتی و ایجاد هرج‌ومرج بازارهای مالی دخیل باشند. این‌گونه سوءاستفاده‌ها به معنای واقعی کلمه نقض حریم خصوصی افراد است (نامجو و احمدی: ۱۳۹۸). با این تفاسیر، ممکن است اطلاعات به شیوع نادرست نشر دهند و منجر به چالش و بحران برای جامعه شوند.

دولت‌ها باید بتوانند پیشاپیش در جریان اتفاقات قرار گیرند و برای مواضع مختلف، ارزیابی‌های درست و صحیح داشته باشند. باید بتوانند قبل از هرگونه تصمیم‌گیری یا اقدامی، ارزیابی‌ها و برآوردهای لازم را داشته باشند. تا بتوانند در برابر چالش‌های پیش‌رو اقداماتی مفید انجام دهند (رحمانی ساعد و ابراهیمی: ۱۳۹۷)؛ بنابراین آگاهی از این چالش‌ها اهمیت بسیاری دارد. یکی از چالش‌هایی که هر سازمانی می‌تواند با آن روبرو شود. فعالیت‌های اطلاعاتی جعل عمیق است. جعل عمیق، به تکنیکی در حوزه هوش مصنوعی اطلاق می‌شود که با استفاده از الگوواره‌های یادگیری عمق می‌توانند تصاویر، ویدئوها و حتی صداها را به‌طور واقع‌گرایانه تغییر دهد. جعل عمیق به‌طور تئوری می‌تواند کاربردهای مفیدی داشته باشد، ازجمله در حوزه هنری و سینما که می‌تواند افکت‌های ویژه بهتری را ایجاد کند؛ اما همچنین این فنّاوری می‌تواند خطرات خود را نیز داشته باشد.

ضرورت و اهمیت تحقیق

الف. اهمیت تحقیق

فنّاوری جعل عمیق می‌تواند ظرفیت‌های خطرناکی را در کاربردها و اهداف مختلف به وجود آورد. در سال‌های اخیر، استفاده از این فنّاوری توجه گسترده‌ای را به خود جلب کرده است. جعل عمیق می‌تواند بر فعالیت‌های اطلاعاتی نیز تأثیرگذار باشد و در جهت متشنج کردن جامعه، کاهش اعتماد عمومی مردم به سامانه‌های اطلاعاتی مورد

1. Deep Learning
2. Fake

سوءاستفاده قرار گیرد. فنّاوری جعل عمیق همانند بسیاری از فنّاوری‌های نوظهور دیگر بسته به این‌که در اختیار نیروهای خودی یا دشمن باشد، می‌تواند فرصت یا تهدید ایجاد نماید.

با توجه به مباحث مطرح‌شده، مشخص است که موضوع این مقاله از اهمیت بالایی برخوردار است که در قسمت زیر به مواردی اشاره شده است:

- افزایش سواد عمومی در راستای شناسایی محتوای دیجیتالی (متن، تصاویر، صوت و ویدیوها) جعلی و جلوگیری از انتشار آن‌ها در فضای مجازی که منجر به جلوگیری از اهداف سوء معاندین می‌شود.
- شناسایی و تعریف بهینه نیازمندی‌های پژوهشی درزمینهٔ فنّاوری نوظهور جعل عمیق در ساحفاجا (ابزارهای شناسایی و تولید جعل عمیق)
- تعیین و معرفی چالش‌های مختلف فنّاوری نوظهور جعل عمیق در راستای فعالیت‌های اطلاعاتی و عملیاتی
- تعیین راهکارهای مقابله با تهدیدات مختلف فنّاوری نوظهور جعل عمیق در راستای فعالیت‌های اطلاعاتی و عملیاتی
- طرح‌ریزی برای خنثی‌سازی تهدیدات ناشی از جعل عمیق

ب. ضرورت تحقیق

با توجه به پیشرفت سریع جعل عمیق، ضرورت پیشگیری از سوءاستفاده از این فنّاوری بسیار اهمیت دارد. در این راستا، تحقیقات بیشتر درزمینهٔ تشخیص جعل عمیق و توسعه الگوواره‌هایی که بتوانند محتوای جعلی را شناسایی کنند، لازم است. همچنین، آموزش عمومی درزمینهٔ تشخیص محتوای دیجیتالی جعلی و نحوه استفاده صحیح از آن‌ها، برای کاهش اثرات منفی جعل عمیق موردنیاز است. درنهایت باید توجه داشت که جعل عمیق در دسترسی عمومی قرار دارد و هرکسی می‌تواند از آن استفاده کند. بااین‌حال باید کوشش‌های بیشتری بر اجرای قوانین مناسب و محدودیت‌ها در استفاده از این فنّاوری انجام شود تا مردم را در مقابل آسیب‌ها و تهدیدهای مرتبط با جعل عمیق محافظت کرد.

- عدم آشنایی با پیشرفت‌های فنّاوری جعل عمیق، نرم‌افزارها، تکنیک‌ها و روش‌های نوین

- ناتوانی در به خدمت گرفتن فنّاوری جعل عمیق در راستای منافع خودی
- ناتوانی در طرح‌ریزی برای خنثی‌سازی تهدیدات ناشی از جعل عمیق
- نقص در شناسایی و تعریف بهینه نیازمندی‌های پژوهشی درزمینهٔ شناسایی جعل عمیق و راه‌کارهای مقابله‌ای با چالش‌های فنّاوری جعل عمیق در ساحفاجا
- عدم شناسایی چالش‌های مختلف فنّاوری جعل عمیق در راستای فعالیت‌های اطلاعاتی
- عدم شناسایی راهکارهای مقابله با تهدیدات مختلف فنّاوری جعل عمیق در راستای فعالیت‌های اطلاعاتی و عملیاتی

پیشینه تحقیق

با بررسی‌های صورت‌گرفته، در سطح دانشگاه علوم و فنون فارابی، پژوهشکده مطالعات کاربردی فارابی و سایر مراکز آموزشی و مطالعاتی ساحفاجا تاکنون پژوهشی مشابه با موضوع فوق انجام نشده است؛ لیکن به برخی پژوهش‌های مشابه و به‌نوعی مرتبط برخورد شد که می‌تواند در روند اجرای این تحقیق مؤثر واقع شود که به شرح زیر معرفی می‌گردد.

احمدی و همکاران (۱۴۰۱)، فصلنامه مطالعات بین‌المللی، شماره ۴، صص ۱۳۹- ۱۵۹ در مقاله نقش فنّاوری‌های نوظهور در امنیت و قدرت ملی کشورها به این نتیجه کلی رسیده‌اند که می‌دهد فنّاوری نوظهور به‌عنوان یک ابزار نوین در اختیار کنشگران همانند تمامی قابلیت‌های دیگر در اختیار بازیگران نظام بین‌الملل دارای تهدیدها و فرصت‌هایی است که کارگزاران می‌بایست بر اساس نیاز و تمامی تهدیدها را به فرصت تبدیل نموده و در راستای منافع ملی خود به‌کارگیرند.

السان، دهستانی (۱۴۰۱)، در مقاله‌ای تحت عنوان جنبه‌های حقوقی جعل عمیق عنوان نمودند که جعل عمیق تولید محتوای متحرک (ویدیو) با تقلید، شبیه‌سازی یا جایگزین کردن چهره از پیش موجود است به‌نحوی‌که بیننده تصور می‌کند که ویدیو تولیدشده، واقعیت دارد اما واقعی نیست. دراین‌بین محققان این حوزه از فنّاوری یادگیری عمیق که مبتنی بر هوش مصنوعی است امکان تولید چنین محتواهایی را فراهم می‌سازند. موضوع این مقاله بر آن تأکید دارد جنبه‌های حقوقی جعل عمیق و سوءاستفاده‌هایی که امکان دارد از محتوای جعلی شود یا محتوای جعلی با هدف تقلب، سو استفاده، فریب افکار

عمومی یا تخریب شخصیت یک چهره مشهور تولید یا پخش شود. پرسش عمده در این مقاله این بوده است که جعل عمیق چه چالش‌های حقوقی را در پی داشته است و آیا قوانین و مسئولیت مدنی موجود، پاسخگوی وضعیت جدید که با گسترش جعل عمیق پیش آمده هستند یا خیر؟

شیوا یاری (۱۳۸۹)، در مقاله مروری بر متون سواد اطلاعاتی در ایران عنوان نمود که همگام با گسترش فنّاوری‌های اطلاعات و ارتباطات و نفوذ آن در جنبه‌های مختلف زندگی، دستیابی به سواد اطلاعاتی، لازمه و پیش‌نیاز بقا در جامعه دانش‌مدار امروز است. درباره این نوع از سواد، منابع فراوانی انتشاریافته که هدف همه آن‌ها، شناساندن مفهوم و محتوای موردبحث در سواد اطلاعاتی و هموارسازی دستیابی به هدف‌های آن بوده است.

عبداللهی (۱۳۹۵)، در مقاله‌ای با عنوان تبیین مفهوم ظروف مرتبط و کارکرد آن در سازمان‌های حفاظت‌اطلاعات عنوان نمود که سازمان‌های حفاظت‌اطلاعات به‌عنوان جزئی اساسی از عناصر جدانشدنی قدرت، در مرکز هسته امنیت کشور قرارگرفته‌اند و به‌عنوان نبض نیروهای مسلح و چشم امین، بصیر، تیزبین و ریزبینی هستند که از طریق آن می‌توان آنچه را که در سازمان‌های حساس نیروهای مسلح می‌گذرد، دریافت کرد؛ بنابراین ضرورت دارد که در همه این سازمان‌ها راهبرد و تفکر مبتنی بر تعامل و همکاری‌های مشترک و چندجانبه ریشه دوانده و آن‌ها همانند ظروف مرتبط عمل نمایند و از جزیره‌ای عمل‌کردن یا اقدام‌های موازی و متداخل خودداری نمایند؛ تا با دستیابی به اشراف اطلاعاتی کامل و منسجم در حوزه مأموریتی خود، از فرصت‌های به‌دست‌آمده استفاده بهینه کرده و با حضور قدرتمند و یکپارچه در عرصه‌های مختلف اطلاعاتی امنیتی، باعث خنثی‌سازی نفوذ دشمن و تهدیدها و آسیب‌پذیری‌ها شوند

بیشتر تحقیقات پیشین انجام پذیرفته در ابعاد حقوقی، امنیتی و اجتماعی است و از منظر فرصت یا تهدید بودن آن بررسی می‌شود.

محقق با بررسی مطالب و مقاله‌های متعدد در مورد موضوع موردنظر چالش‌های جعل عمیق در راستای فعالیت اطلاعاتی به این نتیجه دست یافته است که مطالب موجود در این زمینه فقط در مورد جعل عمیق است و کمتر محققی این موضوع را به فعالیت‌های اطلاعاتی و عملیاتی بسط داده است.

روش‌های گردآوری اطلاعات در این پژوهش، به دودسته اسنادی (کتابخانه و اینترنتی) و میدانی (پرسش‌نامه و مصاحبه) تقسیم می‌شود. در خصوص گردآوری اطلاعات مربوط به ادبیات موضوع و پیشینه پژوهش از روش‌های کتابخانه‌ای و جهت جمع‌آوری اطلاعات از روش میدانی (پرسش‌نامه و مصاحبه) استفاده شده است.

. ابزارهای گردآوری داده‌ها: فیش‌برداری، پرسش‌نامه و مصاحبه

روش کیفی

در مورد ادبیات پژوهش، از کتب علمی، پایان‌نامه‌ها، طرح‌های تحقیقاتی، مقاله‌های علمی و اسناد و مدارک الکترونیکی ارائه‌شده در وب‌گاه‌های معتبر و از روش بررسی اسنادی- کتابخانه‌ای استفاده شد. بر این اساس؛ با توجه به مأموریت‌ها، کارویژه‌ها و حساسیت‌های حاکم بر سازمان‌های امنیتی (ساحفاجا)، شاخص‌های اولیه چالش‌ها و راه‌کارهای مقابله‌ای با چالش‌های جعل عمیق در راستای فعالیت‌های اطلاعاتی در این قبیل سازمان‌ها، به دست آمد.

الف) تعاریف نظری

جعل عمیق: ظهور این واژه در روزنامه‌ها و مجلات ابتدای سال ۲۰۱۸ بوده است، به عقیده برخی این فنّاوری توسط محققین مؤسسات دانشگاهی در اوایل ۱۹۹۰ ایجادشده و متعاقباً در جوامع آنلاین به گردش درآمده است. جعل عمیق از آموزش‌های پیچیده هوش مصنوعی برای جایگزینی شباهت یک فرد با دیگری در ویدیو با دیگر مدیاهای دیجیتال استفاده می‌شود. این واژه به ویدیوهایی اصلی با شخص دیگری به‌خصوص یک چهره عموماً شناخته‌شده، به شیوه‌ای استفاده می‌شود که آن را معتبر و قابل‌اعتماد می‌سازد (اکبری و همکاران، ۱۴۰۱).

فعالیت‌های اطلاعاتی

سازمان‌های ضداطلاعاتی به‌عنوان یکی از سازمان‌های امنیتی کشور (در کنار نیروهای مسلح) وظیفهٔ تأمین امنیت کشور در ابعاد مختلف آن را بر عهده دارند. یکی از این ابعاد بعد سیاسی و اجتماعی آن است در مقابل تهدیداتی که در این حوزه کشور را

تهدید می‌نماید حفظ امنیت اجتماعی و سیاسی کشور مستلزم اقدامات و فعالیت‌های اطلاعاتی است (میرمحمدی، ۱۳۹۰).

ب) تعاریف عملیاتی

جعل عمیق: در این پژوهش جعل عمیق، ترکیبی از کلمه‌های «یادگیری عمیق» و «جعلی» است که یک تکنیک برای ترکیب تصویر انسان مبتنی بر هوش مصنوعی به کار می‌برد

فعالیت‌های اطلاعاتی: در این پژوهش منظور از فعالیت‌های اطلاعاتی کلیه فعالیت‌های مربوط به کسب اطلاعات، جمع‌آوری و پردازش اطلاعات است که می‌تواند خارج از ساعات کاری توسط افراد مربوطه در حوزه موردنظر و منطقه موردنظر مربوط به مسئله اجرا شود.

مبانی نظری

مفهوم جعل عمیق

جعل عمیق مفهومی مرکب از «جعل» و «یادگیری عمیق» است. جعل عمیق، فنّاوری نوظهوری است که با اتکا به شبکه‌های عصبی، مجموعه وسیعی از نمونه‌های داده را تجزیه‌وتحلیل کرده تا حالات چهره، ژست و صدای یک شخص را تقلید کنند. این فرایند شامل قراردادن فیلم دو نفر در یک الگوواره خاص برای تغییر چهره است؛ به‌عبارت‌دیگر، جعل عمیق از فنّاوری نگاشت صورت و هوش مصنوعی استفاده می‌کند تا بتواند صورت یک فرد را در یک فیلم با چهره دیگری عوض کند. تشخیص نمونه‌های جعل عمیق دشوار است زیرا از فیلم‌های واقعی برای تهیه آن استفاده می‌شود و درنتیجه می‌توانند صوتی با صدای واقعی داشته باشند و برای پخش سریع در رسانه‌های اجتماعی بهینه گردند؛ لذا بسیاری از بینندگان تصور می‌کنند که ویدیوی موردنظر واقعی است. از منظر فنّاوری مورداستفاده، جعل عمیق محصول شبکه‌های مهندسی معکوس است؛ یعنی دو شبکه عصبی مصنوعی که برای ایجاد رسانه‌های واقعی باهم کار می‌کنند. این دو شبکه موسوم به «مولّد» و «تشخیص‌دهنده» بر روی مجموعه داده‌های یکسانی از تصاویر، فیلم‌ها یا صداها تنظیم شده‌اند. اولین شبکه سعی می‌کند تا نمونه‌های جدیدی را بسازد و آن را برای عامه پذیر کردن، به شبکه دوم می‌دهد. محصول به‌دست‌آمده مجدد توسط شبکه

نخست ارتقا می‌یابد و تحویل شبکه بعدی می‌شود و به‌این‌ترتیب، این دو یکدیگر را برای بهبود کیفی اثر نهایی تکمیل می‌کنند. یک مولد می‌تواند هزاران عکس از یک شخص را دریافت و تصویر جدیدی مشابه با تقریباً همه نمونه‌های قبلی ایجاد کند بدون اینکه کپی دقیق هر یک از آن‌ها باشد. در آینده نزدیک، مولدها با اطلاعات و داده‌های دریافتی کمتری قادر خواهند بود تا نمای سر، کل بدن و صداها را تشخیص داده و تعویض کنند. با این وصف، اگرچه برای ایجاد جعل عمیق عموماً به تعداد زیادی از تصاویر نیاز است؛ اما محققان تکنیک‌های به‌روزی را برای تولید یک فیلم جعلی با تغذیه تنها یک عکس مانند عکس سلفی ایجاد کرده‌اند (احسان‌پور و امامی، ۱۴۰۱).

به‌طورکلی چالش‌های مرتبط با موضوع جعل عمیق به دودسته تقسیم می‌گردند

دسته درونی

- چالش‌هایی که کارکنان سازمان‌های اطلاعاتی و امنیتی با آن درگیر هستند مانند:
- جعل هویت کارکنان و مدیران سازمان
- استفاده از ارتباطات جعلی برای امکان دسترسی به شبکه‌های ارتباطی و اطلاعاتی سازمان
- فیشینگ یا سرقت اطلاعات
- بروز خطا در تصمیم‌گیری‌ها در اثر جعل صورت‌گرفته
- هزینه‌بر بودن شناخت رسانه‌های جعلی و تفکیک سره از ناسره و عدم شناخت اطلاعات صحیح از اطلاعات تقلبی

دسته بیرونی

- چالش‌هایی که جامعه بیرون را تحت تأثیر قرار می‌دهد مانند:
- ازبین‌رفتن اعتماد
- ایجاد نارضایتی عمومی و ناآرامی در جامعه
- تشدید شکاف اجتماعی و تکثیر اطلاعات جعلی
- دسته‌بندی دیگر در چالش‌ها
- شخصی: آزار و اذیت و مزاحمت
- قانونی: جعل مدارک الکترونیکی

- اجتماعی: برانگیختن ناآرامی‌های اجتماعی
- امنیت سایبری: اخاذی کلاه‌برداری و
- پیشبرد اطلاعات نادرست
- ازبین‌رفتن اعتبار منابع
- فریب و تفرقه
- هک اجتماعی
- تأثیر بر امنیت ملی
- چالش‌های قانونی و اجتماعی

عوامل سازمانی مؤثر درون‌سازمانی

عوامل مؤثر درون‌سازمانی مرتبط با چالش‌های جعل عمیق به موارد زیر بستگی دارد:

ساختار

ساختار سازمانی راه یا شیوه‌ای است که به‌وسیله آن فعالیت‌های سازمانی تقسیم، سازمان‌دهی و هماهنگ می‌شود. به این منظور سازمان‌ها ساختارها را به وجود می‌آورند تا فعالیت‌های عوامل انجام کار را هماهنگ کرده و فعالیت‌های اعضا را کنترل کنند. یکی از عوامل مهمی که می‌تواند تأثیر فراوانی بر نیل به اهداف سازمانی داشته باشد، ساختار سازمان است. ساختار سازمانی نقش مؤثری در دستیابی به اهداف از پیش تعیین‌شده دارد و تمام فعالیت‌هایی که سازمان جهت نیل به اهداف انجام می‌دهد باید در چارچوب ساختار انجام شود؛ بنابراین لزوم توجه به ساختار و تناسب آن در جهت جوابگویی به نیازهای منعطف و متغیر سازمان ضروری است. یقیناً یک ساختار نمی‌تواند در هر جا اثربخش باشد و حتی نمی‌توان ساختاری را طراحی نمود که برای همیشه اثربخشی یک سازمان را تضمین کند؛ بنابراین ساختاری که امروزه متناسب سازمان بوده و جوابگوی خواسته‌های درونی و بیرونی سازمان باشد ممکن است فردا متناسب نبوده و نتواند انتظارات را برآورده نماید و این بیش از هر چیز به خاطر لزوم تغییراتی است که از سوی محیط بر سازمان تحمیل می‌شود.

آموزش

مهم‌ترین عامل موفقیت هر سازمانی نیروی انسانی آن سازمان است. این عامل در سازمان‌های امنیتی با توجه به کارکرد ویژه و خاص آن نقش دوچندانی دارد. با توجه به اینکه فعالیت سازمان‌های امنیتی، خاص است، بی‌شک نیروی انسانی عامل حیاتی موفقیت این سازمان‌ها محسوب می‌شود؛ ازاین‌رو هر فرآیندی که موجب ارتقای نیروی انسانی متناسب با نوع و کار و فعالیت گردد، فرایندی سرمایه افزا است که نتیجه آن به‌طور مستقیم در کیفیت و کمیت فرایند اجرای کار ظاهر می‌شود ازاین‌رو اگر گفته می‌شود آموزش کلید توسعه است، بر حقیقتی کتمان ناپذیر تأکید شده است (منزوی بزرگی و همکاران، ۱۳۹۵: ۱۲۴). آموزش تجربه‌ای است مبتنی بر یادگیری که به‌منظور ایجاد تغییرات نسبتاً ماندگار در فرد صورت می‌گیرد.

فرهنگ

مقصود از فرهنگ سازمانی، باوری از استنباط مشترک است که اعضا نسبت به یک سازمان دارند و همین ویژگی موجب تفکیک دو سازمان از یکدیگر می‌شود. درواقع فرهنگ سازمانی همان چیزی است که به‌عنوان یک پدیده درست به اعضای تازه‌وارد آموزش داده می‌شود و آن بیانگر بخش نانوشته و محسوس سازمان است.

عوامل تشکیل‌دهنده فرهنگ سازمان شامل هنجارها، سنت‌ها و تشریفات و مفروضات است. ویژگی‌های ده‌گانه عمده فرهنگ سازمانی شامل عملکرد، صداقت، رقابت، روحیه کارگروهی، روحیه سازمانی، نوآوری، حمایت مدیریت، موفقیت‌های فردی، وفاداری، سابقه تاریخی سازمان است. مفهوم فرهنگ سازمانی به‌عنوان عامل مؤثر در بهره‌وری و عملکرد سازمان در نظر گرفته شده است و چنانچه فرهنگ مناسب کاری به‌خوبی بین مدیریت و کارکنان گسترش یافته باشد به تحکیم تعهد سازمانی، ارتقاء اخلاقیات، عملکرد و بهره‌وری بالاتر منجر می‌گردد.

عوامل فراسازمانی

عوامل مؤثر فراسازمانی مرتبط با چالش‌های جعل عمیق به موارد زیر بستگی دارد:

تغییرات فنّاورانه محیط

در عصر حاضر هرروز شاهد تغییر و تحول‌های مداوم در عرصه‌های زندگی بشری هستیم و این‌گونه تغییرات آن‌قدر گسترده شده که باید عصر فعلی را عصر فراپیچیده نامید و این امر فعالیت‌ها، اقدام‌ها و تصمیم‌گیری‌ها را برای سیاست‌گذاران و مدیران سازمان‌ها بسیار سخت کرده است. برای رویارویی با تغییرات پیش‌رو، مدیران باید سازمان‌ها را از حالت سکون خارج کرده و بر اساس تغییرات محیطی، حالت انعطاف و تغییر را در پیش بگیرند تا بتوانند متناسب با تغییرات موجود از افول و نابودی سازمان جلوگیری کرده و برتری سازمان را همواره حفظ نمایند.

سازمان‌های حفاظت‌اطلاعاتی نیز به‌عنوان یکی از سازمان‌های پیشرو و امنیت‌ساز، مسئول ایجاد و صیانت از امنیت در ن.م در شرایط فراپیچیده امروز با توجه به تغییرات و شیوه‌های جدید سرویس‌های اطلاعاتی هستند که این مهم نیازمند ایجاد تغییر در ابعاد گوناگون سازمانی است تا بتواند برتری اطلاعاتی خود را در برابر حریف توسعه دهد. ازاین‌رو سازمان‌های حفاظت‌اطلاعاتی که با محیط خود در تعامل هستند، نیازمند الگوهای جدیدی هستند تا بتواند متناسب با تغییرات حریف، با اقدام‌های آگاهانه و فعالیت‌های راهبردی، تغییر یابند و برای اینکه از گردونه رقابت‌ها حذف نشوند به‌طور دائم رهیافت‌های جدیدی را خلق کرده و رشد و تعالی را در خود ایجاد کنند. سازمان‌های حفاظت‌اطلاعاتی گاهی اوقات منتظر حوادثی هستند تا بر اساس آن تدابیر حفاظتی را اتخاذ نماید، لیکن با توجه به شرایط حاکم به نظر می‌رسد تغییر رویکرد مأموریتی در این سازمان‌ها ضرورتی انکارناپذیر است و این سازمان‌ها باید به رویکردهای آفندی روی‌آورند تا قبل از هر اقدامی، اهداف و سیاست‌ها و راهبردها و توانمندی‌های اطلاعاتی دشمن را شناسایی و در جهت خنثی‌سازی آن اقدام‌های مناسب اطلاعاتی اتخاذ نمایند (کمال، ۱۴۰۱: ۱۴۵).

روابط و تعاملات بین سازمانی

ارتباطات در بالندگی سازمان‌ها، نقش اساسی دارد. سطح مطلوبی از ارتباطات سازمانی می‌تواند بستر تعامل را برای تعالی سازمان فراهم نماید. ارتباطات باید اثربخش باشد تا در مجموعه سازمان و مدیریت آن بتواند مؤثر واقع شود و نقش کلیدی را ایفا نماید.

درواقع ارتباط مؤثر می‌تواند به‌عنوان بنیاد سازمان‌های مدرن در نظر گرفته شود. مجاری ارتباطی (چهره به چهره، کتبی و الکترونیکی)، سبک‌های ارتباطی (رسمی و غیررسمی)، مسیرهای ارتباطی (عمودی، افقی و مورب) و محتوای ارتباطی (وظیفه‌ای، اجتماعی و ابتکاری) ازجمله مؤلفه‌های ارتباط هستند (مزروعی و همکاران، ۱۳۸۸: ۵۳). تعاملات بین سازمانی در حوزه سازمان‌های حفاظت‌اطلاعاتی را می‌توان در دو بخش عمده تعاملات و همکاری‌ها با جامعه اطلاعاتی و تعاملات و همکاری‌ها با سازمان حفاظت شونده (سازمان‌های ن.م) تقسیم‌بندی نمود.

تعاملات و همکاری‌ها با مبادی اطلاعاتی سازمان‌های ن.م

نیروهای مسلح، استخوان‌بندی صلابت نظام و جامعه اطلاعاتی شبکه عصبی صلاحیت نظام است. این دو (یعنی استخوان‌بندی و شبکه عصبی) باید هم فضا و هم‌افزا باشند؛ ولی جدای از هم- با شیوه‌های عملیاتی متفاوت- اما با یک عقل و قلب واحد. پیچیدگی، عمق و دامنه تهدیدات دشمنان و اوج خصومت و دشمنی آنان با نظام مقدس ج.ا. ایران، انسجام و تعاملات فی‌مابین سازمان‌های امنیتی و ن.م را تبدیل به یک ضرورت فوری و مبنایی نموده است. تمامی سازمان‌ها خصوصاً سازمان‌هایی که در فرایند مقابله و نفوذ دشمن نقش مستقیم و وظیفه ذاتی دارند، بایستی تقویت تعاملات را به‌صورت ویژه در دستورکار خود قرار دهند. نقش‌ها و تعاملات بخش‌های گوناگون این سازمان‌ها باید به‌گونه‌ای طراحی شوند که هم‌جهت با اهداف آن در یک مسیر حرکت نمایند و رجحان اصلی آن‌ها، دست‌یابی به اهداف کلی سازمان‌ها باشد نه اهداف بخشی و جزئی خود. به تعبیر دیگر هر یک در جهت خنثی‌کردن اقدامات دیگری حرکت نکند بلکه نقش مکمل را برعهده‌گرفته و ضمن تقویت نقاط قوت و مزیت‌های برتر ساز هر یک، به‌سوی برطرف‌کردن معایب و نقایص یکدیگر حرکت کنند (منزوی بزرگی و همکاران، ۱۳۹۵: ۹۶). مسئله تعامل میان سازمان‌های امنیتی و نیروهای مسلح، مسئله‌ای کلیدی است که این موضوع به‌تبع فرمان فرماندهی معظم کل قوا (مدظله‌العالی) مبنی بر تعامل حداکثری نیروهای مسلح و سازمان‌های امنیتی مربوطه با هدف انسجام و یکپارچگی علیه دشمنان جمهوری اسلامی ایران به یکی از موضوعات اساسی تبدیل شده است. تعامل دو نهاد دفاعی و امنیتی ضمن اینکه این سازمان‌ها را در برابر غافلگیری و بحران پذیری مصون

نمـوده و امـکان ضربه‌پذیـری و آسـیب‌پذیری آنـان را به حداقـل ممکن می‌رسـاند، موجب شـناخت دقیـق سـازمان‌ها از یکدیگـر شـده و اشـتراکات و توانمندی‌هـا را فعـال کـرده و اهداف کلیدی و مشـترک آنان را نیز هم‌راسـتا می‌نماید. از سـوی دیگر این تعامل و ارتباط عمیق نمایشـگر اقتدار و صلابت ملی کشـور از نگاه دشـمنان بیرونی اسـت و شـکل‌گیری و تقویـت فراینـد تعاملـی بـا تمرکز بـر همـکاری و هم‌افزایی حوزه‌هـای دفاعـی و امنیتی در یکپارچه‌سازی برنامه‌ها علیه اقدامات خصمانه دشمنان قسم‌خورده نظام اسلامی و تأمین منافع امنیت ملی کشور را به دنبال خواهد داشت.

مشارکت و همکاری اطلاعاتی

مشارکت و جلب همکاری اطلاعاتی کارکنان سازمان حفاظت شونده

سـازمان حفاظت‌اطلاعات بـرای انجام وظایف ذاتی خود و رسـیدن به هدف‌های متعالی سـازمان خـود کـه همـان پیشـگیری، کشـف، شناسـایی و خنثی‌سـازی فعالیت‌هـای جاسوسـی و خرابـکاری، برانـدازی و مـوارد ایجاد نارضایتـی، جلوگیری از نفـوذ جریان‌های سیاسـی و ایجـاد اختلال در انجـام مأموریت‌ها اسـت حصول هدف خطیر مزبور نیازمند احراز شایسـته اشـراف اطلاعاتی نسـبت به سـازمان آجا در ابعاد مختلف مأموریتی، منابع انسـانی و... اسـت کـه بالطبـع یکی از دغدغه‌هـای مهم حفاظت‌اطلاعـات در جمع‌آوری اخبـار و اطلاعات، جلـب همکاری اطلاعاتی کارکنان شـاغل در بخش‌های مختلف نیرو با حفاظت‌اطلاعات اسـت تا با در اختیار داشـتن اطلاعات مناسب بستر لازم برای نیل به گرفتن و اجرای تصمیم‌های صحیح فراهم آید. با وصف بالا یکی از عوامل بسـیار بنیادین در این همکاری انگیزه کارکنان است.

سازمان حفاظت‌اطلاعات برای رسیدن به هدف‌های خود باید اشراف و سیطره اطلاعاتی بـر کارکنـان و مأموریت‌هـای نیروی انتظامی داشـته باشـد و این اشـراف اطلاعاتی بدون مشـارکت کارکنـان آن در همـکاری اطلاعاتـی بـا حفاظت‌اطلاعـات حاصـل نمی‌شـود؛ بنابراین باید انگیزه‌های همکاری را شـناخته و از شـیوه‌های روانی انگیزشی برای ترغیب کارکنـان بـه همـکاری اطلاعاتی اسـتفاده نمـود. انگیزه همـکاری در اصطـلاح اطلاعاتی عبـارت اسـت از محـرک و علـت واقعـی کـه باعـث می‌شـود فـردی همـکاری با سـازمان

اطلاعاتی را قبول کند. ازنظر علم روان‌شناسی هر فعالیت و تصمیم ایشان بر اساس یک انگیزه است (صفرآبادی، ۱۳۸۸: ۹۵).

جلب مشارکت و همکاری اطلاعاتی مردمی

مشارکت مردمی در سال‌های اخیر، هم از جنبه نظری و هم از بعد عملی بسیار موردتوجه بوده است. بسیاری از جوامع به‌منظور دستیابی به پایداری، اثربخشی سیاست‌ها و توسعه همه‌جانبه تلاش می‌کنند حس مشارکت، مشورت، گفتگو را در میان شهروندان تقویت کنند. دیدگاه‌های متفاوتی در این زمینه وجود دارد. دوتوکویل مشارکت را امری ضروری در جوامع شهری می‌داند و بر این باور است که سنت مشارکت، جامعه شهری را زنده نگاه می‌دارد و پیوندهای اجتماعی را محکم‌تر می‌سازد. علاوه بر این، تجربه نشان‌داده است که در حال حاضر با پیشرفت سریع جوامع، ثبات و پایداری امنیت، تنها از رهگذر نهادینه کردن آن در جامعه و مشارکت دادن همه افراد، نهادها و تشکل‌ها امکان‌پذیر است. اکثر اندیشمندان نیز بر این باورند که گرچه تأمین امنیت وظیفه دولت‌ها است، لیکن با توجه به تحولات قرون اخیر، امنیت با مشارکت شهروندان، امکان بقاء و پایداری دارد (سعیدی، ۱۳۸۲: ۴۱).

جمع‌بندی

چالش‌ها و راهکارهای جعل عمیق در بررسی فعالیت‌های اطلاعاتی بر اساس مرور مبانی نظری، ادبیات تحقیق و مصاحبه‌های انجام شده (در فصل ضمیمه) و همچنین تحلیل محتوای صورت پذیرفته، چالش‌ها و راهکارهای جعل عمیق به شرح جدول ذیل است.

چالش‌ها و راه‌کارهای جعل عمیق (منبع: محقق ساخته)

ردیف	چالش‌های جعل عمیق	راه‌های مقابله با جعل عمیق
۱	ازبین‌رفتن اعتماد عمومی به نهادها و مقامات	برچسب‌گذاری فعالانه محتوای واقعی یا جعلی هنگام تولید آن‌ها و استفاده از آشکارسازها برای پیداکردن موارد جعلی پس از انتشار.
۲	تشدید شکاف‌های اجتماعی	شبکه‌های اجتماعی و گروه‌های مردم‌نهاد با تولید و انتشار محتوای آموزشی در این فضای سوادآموزی پیش‌قدم شده‌اند و باید به این امر ادامه دهند. درنهایت، دولت نیز باید نقش فعال‌تری در فضای سواد رسانه‌ای ایفا کند.

ردیف	چالش‌های جعل عمیق	راه‌های مقابله با جعل عمیق
۳	تضعیف منابع قابل اعتماد اخبار و اطلاع‌رسانی	از دیگر روش‌های مقابله با جعل عمیق، تکنیک‌های اوسینت و رویکردهای روزنامه‌نگاری است. هدف از این رویکردها توسعه و به اشتراک‌گذاری ابزارهای منبع‌باز است که می‌توانند برای شناسایی جعل عمیق و سایر محتوای مرتبط با انتشار اطلاعات غلط مورداستفاده قرار بگیرند. این سامانه‌های منبع‌باز نیز برای بسیاری از بازیگران جامعه مدنی که در بررسی حقایق و سایر کارهای آموزشی مشارکت دارند، مهم خواهند بود.
۴	جعل عمیق و هرزه‌نگاری و تضعیف امنیت ملی	استفاده خصمانه از جعل عمیق، شامل به‌کارگیری محاسبات تصمیم‌گیری است به‌نحوی‌که فرصت‌ها، مزایا و خطرات را می‌سنجد. چنین تصمیماتی را می‌توان از طریق بازی جنگ و سایر تمرینات مدل‌سازی کرد؛ بنابراین بازی جنگ و شناسایی راهبردهای بازدارندگی که می‌تواند بر تصمیم‌گیری دشمنان خارجی تأثیر بگذارد، مهم است. دستگاه‌ها امنیتی اطلاعاتی نیز باید بر استراتژی‌های جمع‌آوری اطلاعات تمرکز کنند، به‌نحوی‌که بتوانند در مورد تلاش‌های دشمن برای بهره‌برداری از فنّاوری جعل عمیق هشدار لازم را به دولت‌مردان ارائه دهند.
۵	شفاف نبودن محتوای ساختگی	-هر محتوای تولیدشده توسط هوش مصنوعی که در تبلیغات سیاسی در پلتفرم‌های باید مشخص شود. -تیک‌تاک دستورالعمل‌های انجمن خود را به‌روزرسانی کرد تا برای سازندگان اجباری شود که استفاده از هوش مصنوعی را در هر صحنه‌ای که ظاهری واقعی دارد، افشا کنند. - یکی از راه‌های برچسب‌گذاری تصاویر ساختگی، مشخص‌کردن آن‌ها با تغییر پیکسل‌ها به روشی متمایز است که برای چشم غیرقابل تشخیص است اما در تجزیه‌وتحلیل مشخص می‌شود
۶	نبود سواد فنّاوری در بین مردم	بهبود سواد فنّاوری به جلوگیری از غرق شدن جامعه و دموکراسی در جعل عمیق کمک می‌کند. روچا می‌گوید: ما باید این خبر را به گوش مردم برسانیم تا مردم را ازآنچه در حال وقوع است آگاه کنیم. زمانی که آن‌ها در مورد آن مطلع شوند، می‌توانند اقدام کنند. آن‌ها می‌توانند مطالبه آموزش در مدارس را داشته باشند.
۷	نبود سواد رسانه‌ای در راستای کاهش تهدیدات جعل عمیق	رویکرد قابل‌استفاده دیگر برای مقابله با جعل عمیق، سواد رسانه‌ای است. برنامه‌های سواد رسانه‌ای به دنبال کمک به مخاطبان برای کنجکاوی در مورد منابع اطلاعات، ارزیابی اعتبار آن‌ها و تفکر انتقادی در مورد مطالب ارائه شده است. ذهن و عملکرد مخاطبان به‌عنوان آخرین خط دفاع در قبال داده‌های جعل عمیق عمل می‌کند. به‌طورکلی، محققان سیاستی که استراتژی‌های مقابله باکمپین‌های دروغ‌پراکنی خارجی را بررسی می‌کنند، اغلب اجرای برنامه‌های آموزشی سواد رسانه‌ای را توصیه می‌کنند.
۸	عدم شناسایی و تعریف بهینه‌نیازمندی‌های پژوهشی درزمینهٔ فنّاوری نوظهور جعل عمیق در ساحفاجا	محققان برای بررسی و حل این مسئله می‌توانند اسپم‌های اجتماعی و بررسی‌های جعلی را مورد تجزیه‌وتحلیل قرار دهند. البته به نکته نیز توجه باید کرد که درزمینهٔ جعل، طبقه‌بندی‌های مختلفی از انواع جعل وجود دارد که بیشتر به منبع و نوع داده‌های مورداستفاده برای تجزیه‌وتحلیل وجود دارد. البته در مورد جعل عمیق، مرزهای مشخصی وجود ندارد؛ اما آنچه اهمیت دارد این امر است که چه نوع داده‌ای می‌تواند تبدیل به موضوع تجزیه‌وتحلیل و چگونگی تعریف آن شود؛ و منبع جعل اهمیت دارد.

ردیف	چالش‌های جعل عمیق	راه‌های مقابله با جعل عمیق
۹	عدم تعیین الزامات پیشگیری از شناسایی توسط دشمن با استفاده از سامانه‌های مبتنی بر اینترنت.	در این مورد می‌توان استدلال کرد که اینترنت و بستر رسانه‌ها، به‌طور خاص زمینه باوری بر انتشار اطلاعات غیرقابل اثبات و شایعات هستند. ه انجام یک ارزیابی مطمئن و منصفانه از رویکردهای کشف اطلاعات غلط و مقایسه عملکرد آن‌ها بسیار سخت است. علاوه بر این محقق برای یافتن مناسب‌ترین مدل برای مجموعه داده‌ها و کارها، مجبور به آزمایش الگوواره‌های طبقه‌بندی مختلف است؛ که می‌تواند به رویکردهای طبقه‌بندی و رویکردهای دیگر دسته‌بندی کرد که مبتنی بر یادگیری ماشین و یادگیری عمیق است.
۱۰	عدم شناسایی و تبیین الزامات و چالش‌های اینترنت به‌ویژه چالش‌های امنیتی آن در راستای فعالیت‌های اطلاعاتی	راهکاری که در این زمینه (فعالیت‌های اطلاعاتی) می‌تواند مطرح باشد این امر است که محققان می‌توانند به‌وسیله الگوواره‌های یادگیری ماشین برای حل بسیاری از کارها درزمینهٔ اطلاعات فعالیت کنند.
۱۱	عدم ارائه راهکارهای امنیتی باهدف به‌کارگیری شناسایی فنّاوری نوظهور چالش‌های جعل عمیق در ساحفاجا	ازآنجایی‌که اولین رویکرد با تمرکز بر اعتبار در رسانه‌ها و کشف فریب با واسطه رایانه است. تکنیک‌های یادگیری ماشین در رابطه با مسئله کشف اطلاعات غلط مورد آزمون و ارزیابی قرار گرفتند و بیشتر رویکرد یادگیری ماشین برای اخبار جعلی و کشف شایعات به‌کاررفته است.
۱۲	وقت‌گیر بودن استخراج اطلاعات و مغرضانه بودن اطلاعات به‌دست‌آمده. این موضوعات مهم، برای کارهایی مانند اخبار جعلی و کشف شایعات است، جایی که شناسایی ویژگی‌های مربوط به آنالیز ممکن است که یک چالش بزرگ ایجاد کند و از طرف دیگر، چارچوب‌های یادگیری عمیق می‌تواند بازنمایی پنهان را از ورودی ساده به دست آورد.	در این مورد مسئله از مدل‌سازی ویژگی‌های ورودی مرتبط، به مدل‌سازی خود شبکه منتقل می‌شود که امکان حل کارآمد مسئله را فراهم می‌کند. در اینجا دو الگوواره شبکه‌های عصبی مصنوعی مدرن مورداستفاده است که شبکه عصبی مکرر و شبکه عصبی کانولوشنی در اینجا مطرح هست.
۱۳	رویکرد یادگیری ماشین، دقت و صحت بهتری نسبت به رویکرد یادگیری عمیق در جعل عمیق دارد	مسئله جعل عمیق، به‌عنوان یک مسئله طبقه‌بندی در پردازش زبان طبیعی و متن‌کاوی شناخته می‌شود. استفاده از شبکه‌های عصبی کانولوشن به‌عنوان یکی از مهم‌ترین مدل‌های یادگیری عمیق دقت بالایی را بر روی این مسئله ایجاد می‌کند. در این شبکه‌ها کلمات به‌صورت کیسه‌ای از کلمات به مدل داده می‌شوند که هر کلمه با توجه به فضا برداری به ماتریس دوبعدی تبدیل می‌شود.

ردیف	چالش‌های جعل عمیق	راه‌های مقابله با جعل عمیق
۱۴	مقررات کیفری در مورد جعل عمیق	زآنجاکه موضوع جعل عمیق، از مسائل و نوظهور فتّاوری است، در باب مقررات فقهی و کیفری نیز موضوعی مستحدثه به شمار می‌آید. در مواجهه با پدیده‌های جدیدی که اخلاق و نظم اجتماعی را به چالش می‌کشد و موجب اضرار به غیر اعم از فرد یا جامعه می‌گردد، نخستین و سریع‌ترین واکنش، اتخاذ رویکردی کیفرمَآبانه است. ازآنجاکه اولاً تصویب قانون خاص در خصوص هریک از پدیده‌های نوظهور اجتماعی نیازمند بررسی‌های چندبعدی عمیق و تمام‌لحظه تمامی جوانب موضوع است و از سویی در شرایط فقدان قانون خاص، رعایت حقوق شهروندان در مراجعه به محاکم دادگستری و طرح شکایت از حقوق تضییع‌شده خود، نباید به بهانه سکوت یا فقدان قانون نادیده انگاشته شود، تطبیق رفتارهای مجرمانه بر عناوین کیفری سنتی موجود می‌تواند راهگشا باشد. نظر به ماهیت مباحث مربوط به جعل عمیق (که در حوزه دنیای فتّاوری است) توجه به قانون جرائم رایانه‌ای در اولویت بررسی خواهد بود.
۱۵	مشخص‌نبودن منشأ محتوا	افزایش به‌کارگیری رویکردهای مبتنی بر منشأ محتوا باید کاری کرد که فتّاوری‌های ثبت منشأ محتوا موردپذیرش قرار گیرد. به‌عنوان‌مثال؛ در آمریکا لایحه دوحزبی کنگره با عنوان «قانون کارگروه ویژه جعل عمیق» یکی از رویکردهای بالقوه‌ای است که می‌تواند پذیرش رویکردهای مبتنی بر منشأ محتوا را بیشتر ترویج کند.

نوع تحقیق

تحقیق حاضر از نوع کاربردی بوده چراکه با انجام این پژوهش و بررسی چالش‌های جعل عمیق در فعالیت‌های اطلاعاتی و عملیاتی می‌توان دستاوردهای این تحقیق را در سازمان‌ها در راستای ارتقای فعالیت‌های اطلاعاتی و صرفه‌جویی در هزینه‌های مربوط به فعالیت اطلاعات و ارتباطات سازمان‌ها، هم‌افزایی اطلاعاتی بین بخش‌های داخلی سازمان و همچنین بین اعضاء جامعه اطلاعاتی، تسریع و تسهیل در روند خدمات‌رسانی به کاربران سازمانی به‌منظور انجام وظایف و مأموریت‌های محوله و... مدنظر قرار داد و بهره برد.

روش‌های پژوهشی آمیخته، نوعی روش پژوهشی است که در آن، یک پژوهشگر (یا تیمی از پژوهشگران) عناصر رویکردهای کمّی و کیفی را به‌منظور آشکار ساختن موانع موجود در امر پژوهش و درک عمیق پدیده‌ها با یکدیگر ترکیب می‌کنند (بروک جانسون، ۲۰۱۷). با توجه به اینکه محقق در این پژوهش به دنبال شناسایی چالش‌های جعل عمیق در راستای بررسی فعالیت‌های اطلاعاتی و عملیاتی است، بنابراین روش تحقیق از نوع روش موردی- زمینه‌ای است.

جدول ۴-۱ شاخص چالش‌ها مستخرج از متن مصاحبه‌ها

حیطه	مضمون	مقوله
چالش‌ها	جعل عمیق	واقعی یا جعلی بودن رویداد
		امکان نفوذ سامانه‌های هویت جعلی
		ورود به حریم خصوصی
		برهم‌زدن آرامش روانی جامعه
		سردرگمی مردم در جامعه
		غیرقابل تشخیص بودن درستی و نادرستی اخبار
		عدم دانش کافی
		کاهش اعتماد عمومی
		افزایش جرائم و فرار از قانون با جعل مدرک
		جعل هویت رده‌های بالای جامعه
		مشغول بودن نظام اطلاعاتی
		فریب مدیران و مقامات
		-بروز خطا در تصمیم‌گیری در اثر جعل صورت‌گرفته
		ایجاد نارضایتی عمومی
		امکان گمراه نمودن نهادهای اطلاعاتی
		تدوین نشدن احراز هویت بر اساس کدهای رمز
		گسترش اخبار نادرست
		عدم موضع‌گیری سریع و صریح و اطلاع‌رسانی درست و به‌موقع
		اطلاعات نادرست
		عدم توانمندی در کنترل فضای مجازی
		عدم وجود زیرساخت‌های مناسب
		جعل هویت کارکنان و مدیران سازمان‌ها
		جعل مدارک الکترونیکی
		اخاذی کلاه‌برداری
		از بین اعتبار منابع
		تهدید علیه امنیت ملی
		ایجاد رعب و وحشت
		برچسب‌گذاری بر اطلاعات درست

جدول ۴- ۲ شاخص راهکارها مستخرج از متن مصاحبه‌ها

حیطه	مضمون	مقوله
راهکارها	جعل عمیق	امکان ایجاد محتوای دیجیتالی جعلی امکان استناد سوژه‌ها یا اهداف به جعلی بودن تعریف سامانه‌های احراز هویت استفاده از هوش مصنوعی و یادگیری آموزش و آگاهی بخشی جامعه ضرورت فرهنگ‌سازی توسعه ابزارهای تشخیص و آگاهی بخشی افزایش دانش استفاده از الگوواره‌های پیشرفته آموزش و بالابردن سطح سواد اشتراک‌گذاری اطلاعات صحیح توسعه فنّاوری شناسایی جعل بهره‌برداری از هوش مصنوعی افزایش آگاهی و توسعه فنّاوری

جدول ۴- ۳ شاخص چالش مستخرج از متن مصاحبه‌ها

حیطه	مضمون	مقوله
چالش‌ها	جعل عمیق	۱-امکان گمراه نمودن نهادهای اطلاعاتی ۲-تدوین نشدن احراز هویت بر اساس کدهای رمز ۳-گسترش اخبار نادرست ۴-عدم موضع‌گیری سریع و صریح و اطلاع‌رسانی درست و به‌موقع ۵-اطلاعات نادرست ۶-عدم توانمندی در کنترل فضای مجازی ۷-عدم وجود زیرساخت‌های مناسب ۸-جعل هویت کارکنان و مدیران سازمان‌ها ۹-جعل مدارک الکترونیکی ۱۰-اخاذی کلاه‌برداری ۱۱-از بین اعتبار منابع ۱۲-تهدید علیه امنیت ملی ۱۳-ایجاد رعب و وحشت ۱۴-برچسب‌گذاری بر اطلاعات درست

بحث و نتیجه‌گیری

در دنیای امروز، فنّاوری جعل عمیق به یکی از مهم‌ترین تهدیدات امنیتی تبدیل شده است که می‌تواند نهادهای اطلاعاتی و امنیتی را با چالش‌های جدی مواجه کند. این فنّاوری نه‌تنها توانایی تولید محتوای جعلی بسیار واقعی را دارد، بلکه می‌تواند اعتماد عمومی به نهادها، رسانه‌ها و منابع اطلاعاتی را نیز تخریب کند. در این مقاله، تلاش شد تا ضمن شناسایی چالش‌های مرتبط با جعل عمیق، راهکارهایی برای مقابله با این تهدیدات ارائه شود.

مطالعات انجام‌شده نشان‌داد که توسعه ابزارهای شناسایی مبتنی بر هوش مصنوعی و الگوواره‌های یادگیری عمیق، یکی از مؤثرترین روش‌ها برای مقابله با جعل عمیق است. همچنین، آموزش سواد رسانه‌ای و فنّاوری به جامعه، نقش مهمی در پیشگیری از تأثیرات منفی این فنّاوری ایفا می‌کند. از سوی دیگر، همکاری میان نهادهای دولتی، سازمان‌های امنیتی و بخش خصوصی برای تدوین استانداردهای جدید احراز هویت و افزایش شفافیت در محتوای دیجیتال، می‌تواند به کاهش خطرات جعل عمیق کمک کند.

ازجمله پیشنهادهای کاربردی این تحقیق می‌توان به موارد زیر اشاره کرد:

۱. ایجاد سامانه‌های احراز هویت مبتنی بر هوش مصنوعی برای جلوگیری از سوءاستفاده‌های اطلاعاتی

۲. طراحی و اجرای برنامه‌های آموزشی برای افزایش آگاهی عمومی نسبت به محتوای جعلی

۳. توسعه همکاری‌های بین‌المللی برای شناسایی و مقابله با تهدیدات جعل عمیق در سطح جهانی

۴. تقویت زیرساخت‌های قانونی برای مقابله با استفاده‌های غیرقانونی از این فنّاوری

درنهایت، لازم است نهادهای اطلاعاتی و امنیتی رویکردهای پیشگیرانه و تهاجمی جدیدی را برای مقابله با جعل عمیق اتخاذ کنند. این پژوهش گامی در جهت ارتقای امنیت ملی و ارائه راهکارهای عملی برای مقابله با تهدیدات فنّاوری‌های نوظهور است. امید است نتایج این تحقیق بتواند در سیاست‌گذاری‌ها و تصمیم‌گیری‌های اطلاعاتی مورداستفاده قرار گیرد.

فهرست منابع

منابع فارسی (ترجمه‌شده به انگلیسی)

1. Ahmadi, A., Zargar, A., & Adami, A. (2022). The role of emerging technologies in the security and national power of countries: Opportunities and threats. International Studies Quarterly, 4, 139-159.

2. Al-San, M., & Dehestani, S. (2022). Legal aspects of deepfake technology. Legal Research Journal, 193-218.

3. Akbari, A., Aghapour, A., & Aghapour, K. (2022). Criminal analysis of deepfakes with a focus on Iranian criminal policy and human rights challenges. Scientific Workshop Quarterly, 59, 149-169.

4. Namjou, A., & Ahmadi, A. (2019). Methods of detecting deepfake videos using artificial neural networks. National Computer Engineering Conference, 1-8.

5. Rahmani Saeed, H., & Ebrahimi, H. (2018). The role of counterintelligence organizations in ensuring the political security of the Islamic Republic of Iran. Protective and Security Research Journal, 27, 55-82.

6. Nikmaleki, M. (2021). Deepfake: Fabrication of reality using artificial intelligence. News Research Journal of the Political Studies Department, 1-11.

منابع خارجی

1. Khan, I. R., Aisha, S., Kumar, D., & Mufti, T. (2023). A systematic review on deepfake technology. In Khanna, A., Polkowski, Z., Castillo, O. (Eds.), *Proceedings of Data Analytics and Management* (Vol. 572, pp. 7615-55). Springer, Singapore.

2. Han, J., Kamber, M., & Pei, J. (2011). Data mining: Concepts and techniques. Elsevier.

3. Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI Magazine, 17*(3), 37-54. https://doi.org/10.1609/aimag.v17i3.1230