دیده‌بان

مروری بر مهم‌ترین اخبار پدافند غیرعامل در سطح ایران و جهان

بولتن تحلیلی خبری | شماره یازدهم-مرداد ۱۴۰۳ | @pdpaydarymelli

آمادگی عملیاتی برای مقابله با پشه آئدس

بسم الله الرحمن الرحیم

شناسنامه اثر:

دیده‌بان| خبرنامه (بولتن) تحلیلی خبری اخبار و رویدادهای پدافند غیرعامل در ایران و جهان

ناشر: روابط عمومی و امور بین الملل سازمان پدافند غیرعامل کشور

طراحی و تولید: مرکز آفرینش های هنری فاطر

اطلاعات تماس:

کد پستی: ۱۶۷۱۸-۳۸۷۳۱

صندوق پستی: ۱۵۱۴۷۴۷۷۱۱

ایمیل: info@paydarymelli.ir

شماره تلفن: ۰۲۱۶۶۵۸۱۱۹۷

شناسه شبکه های اجتماعی در سکوهای بومی:

@pdpaydarymelli

فهرست

اخبار سازمان

در جلسه شورای عالی پدافند زیستی مطرح شد

سردار جلالی: تأکید بر تقویت زیرساخت‌ها و آمادگی عملیاتی برای مقابله با پشه آئدس

لزوم ارتقای نظام تشخیصی کشور و تدوین طرح‌های پاسخ سریع به تهدیدات زیستی

● جلسه شورای عالی پدافند زیستی با محوریت تصویب نامه های نظام عملیاتی پدافند زیستی و برنامه ملی مقابله با ناقلین مهاجم زیستی (پشه ائدس) از سوی قرارگاه پدافند زیستی کشور با حضور سردار دکتر غلامرضا جلالی، رئیس سازمان پدافند غیرعامل کشور و فرمانده قرارگاه پدافند زیستی کشور و سایر اعضای این قرارگاه و همچنین نمایندگان وزارت بهداشت و درمان و آموزش پزشکی، جهاد کشاورزی، نفت، راه و شهرسازی، کشور، امور خارجه، علوم، تحقیقات و فناوری، سازمان حفاظت محیط زیست، حفظ نباتات، دامپزشکی، جمعیت هلال احمر، صدا و سیما موسسه سرم سازی رازی و انستیتو پاستور ایران برگزار شد.

در ابتدای این جلسه، سردار جلالی فرمانده قرارگاه زیستی کشور به تشریح قانون تشکیل سازمان پدافند غیرعامل کشور که در مجلس شورای اسلامی مصوب و ابلاغ شده پرداخت.

وی در ادامه با تاکید بر اهمیت شناسایی، رصد و پایش در حوزه های تهدید نوین و به ویژه حوزه پدافند زیستی، اظهار داشت: تجربه پاندمی کرونا به همه نشان داد که مسئله تهدیدات زیستی تا چه حد جدی است و پیامدهای آن نه تنها حوزه بهداشت و درمان بلکه حوزه اقتصادی، امنیتی و اجتماعی را نیز به شدت تحت تاثیر قرار می دهد.

سردار جلالی با بیان اینکه برنامه ملی پدافند زیستی در دو بخش تقویت و ارتقاء

زیرساخت ها و آمادگی و اقدامات عملیاتی در دستور کار قرارگاه پدافند زیستی کشور قرار دارد، متذکر شد: از جلسات بعدی این موارد به صورت دستگاه به دستگاه بررسی می گردد تا سطح مطلوبی از توانمندی ایجاد شود.

به گفته وی وظایف اصلی قرارگاه پدافند زیستی، رصد و شناسایی تهدیدات حوزه زیستی است و همچنین بررسی پیامدهای حادثه، رخداد و آسیب پذیری و شناسایی ضعف ها است. به همین جهت در نظام دیده بانی سلامت کشور در حوزه رصد، بررسی و شناسایی بایستی اقدامات لازم جهت به روز شدن صورت گیرد.

رئیس سازمان پدافند غیرعامل کشور با بیان اینکه از اهداف دیگر قرارگاه ارتقاء نظام تشخیصی کشور است، گفت: براساس نوع تهدیدات، کشور نیاز به آزمایشگاه ها و سازماندهی آن ها دارد تا بتوانیم تشخیص پیشدستانه داشته باشیم.

وی در ادامه با بیان اینکه در حوزه منابع انسانی تخصصی، پیش بینی واحد احتیاط و ذخیره پدافند زیستی که توسط ستاد کل نیروهای مسلح پیشنهاد شد را پیگیری و در نظام عملیاتی پدافند زیستی گنجاندیم، افزود: در این طرح از ظرفیت گروه ها و دسته های مختلف با تخصص های گوناگون در زمان بحران استفاده می شود.

به گفته سردار جلالی، براساس هرتهدیدی که مشخص می شود توسط استان ها طرح های پاسخ سریع به تهدیدات مورد نظر تدوین و آمادگی لازم باید کسب شود.

براساس همین سند پدافند زیستی در سطوح ملی، استانی و شهری و در دستگاه های مختلف دارای برنامه خاص خود هستند.

در ادامه این نشست نمایندگان دستگاه های حاضر در این جلسه به بیان نقطه نظرات خود پرداختند.

تحلیل

برگزاری جلسه شورای عالی پدافند زیستی از آن رو اهمیت دارد که ضمن استفاده از تجربیات پاندمی کرونا می تواند به تشریک مساعی در زمینه تقویت و سازماندهی منابع انسانی و زیرساخت‌ها بهداشت و درمان و آمادگی عملیاتی واحدها برای مقابله با پشه آئدس و تب دنگی کمک کند.








اخبار سازمان

سردار جلالی در شورای پدافند غیرعامل استان آذربایجان شرقی:

ساماندهی مراکز پرخطر شهری اولویت سازمان پدافند غیرعامل کشور

اهمیت استقرار واحدهای تخصصی آتش نشانی در مراکز صنعتی

● جلسه شورای پدافند غیرعامل استان آذربایجان شرقی با حضور سردار دکتر غلامرضا جلالی، رئیس سازمان پدافند غیرعامل کشور، تراب محمدی سرپرست استانداری استان آذربایجان شرقی، دکتر عبدالرحمن کشوری، معاون انرژی سازمان پدافند غیرعامل کشور و جمعی از مسئولان استان برگزار شد.

سردار جلالی این جلسه با گرامیداشت یاد و خاطرات شهدای خدمت به ویژه شهید آیت الله آل هاشم، امام جمعه تبریز و نماینده ولی فقیه استان آذربایجان شرقی و مالک رحمتی، استاندار آذربایجان شرقی، تقوا و پرهیزگاری، مردم‌داری، ساده زیستی و تواضع و ایستادگی و پایداری در مسیر انقلاب را از جمله ویژگی های بارز شهید

آیت الله هاشم در کلام رهبری عنوان کرد و گفت: آیت‌الله آل‌هاشم به عنوان یکی از شخصیت های برجسته و اثرگذار در تاریخ انقلاب اسلامی ایران، همواره مورد تحسین وتقدیر مقام معظم رهبری، حضرت آیت‌الله امام خامنه‌ای، قرار داشتند.
وی در ادامه با بیان اینکه برگزاری انتخابات اخیر در حالی که دولت سیزدهم با اهتمام فراوان کشور را اداره می کرد، نشانه‌ای از ثبات و قدرت نظام اسلامی است، اظهار داشت: این انتخابات که با حضور گسترده مردم و با رعایت کامل اصول دموکراسی برگزار شد، تعهد نظام به اصول مردم سالاری دینی را نشان داد.
رئیس سازمان پدافند غیرعامل کشور با اشاره به اینکه برگزاری انتخابات در امنیت کامل، نشانه اقتدار جمهوری اسلامی ایران است، متذکر شد: این موفقیت نشان می دهد که دشمنان نتوانستند برنامه های خود را برای تحریم انتخابات و ایجاد ناآرامی به اجرا بگذارند.
سردار جلالی با آرزوی موفقیت برای دکتر پزشکیان و دولت چهاردهم، اظهار داشت: مقام معظم رهبری همواره تاکید دارند که رئیس جمهور باید نگاه به افق های بلند و روشن داشته باشد. امید به آینده و ایجاد انگیزه برای پیشرفت، از اصولی است که باید همواره مد نظر قرار گیرد. این نگاه به آینده، ما را قادر می سازد تا با چالش ها مقابله کنیم و مسیر پیشرفت و تعالی را ادامه دهیم.
وی با اشاره به اینکه در موضوع پدافند غیرعامل، تمرکز بر شناسایی، رصد و تشخیص تهدیدات و مخاطرات و تلاش برای به صفر رساندن آنهاست، متذکر شد: خوشبختانه در استان آذربایجان شرقی در بخش مختلف، اقدامات خوب و موثری توسط دستگاه ها انجام شده است.
سردار جلالی با بیان اینکه در سال های اخیر با طیفی جدیدی از تهدیدات که الگویی ترکیبی و پیشرفته دارند، مواجه هستیم خاطر نشان کرد: این تهدیدات با محوریت زیرساختها، صورت می گیرد. نمونه آن اقدام خرابکارانه علیه تأسیسات انتقال گاز درزمستان سال گذشته بود.
وی ادامه داد: اقدامات جهادی و شایسته تقدیر تلاشگران صنعت گاز در بخش های انتقال و ستاد، از بروز یک بحران جلوگیری و پیامدهای آن را خنثی کرد. این اقدامات در دو بخش عملیات برگشت پذیری زیرساخت و مدیریت بحران رسانه قابل دسته بندی است.

به گفته رئیس سازمان پدافند غیرعامل کشور، شرکت ملی گاز ایران سال گذشته در جریان حادثه خرابکارانه در زمینه مدیریت پیامد حمله، عملیات رسانه‌ای و عملیات بازسازی، عملکرد ارزشمندی انجام داد که به عنوان یک دانش و تجربه ارزشمند حوزه پدافند غیرعامل برای مدیریت آتی بحران‌ها می‌توان از آن بهره برد.
وی با بیان اینکه تلاش پدافند غیرعامل این است که جلوی وقوع تهدید گرفته شده و یا در صورت بروز تهدید، پیامدهای آن به حداقل برسد، خاطرنشان کرد در مقابله با جنگ ترکیبی و پیچیده زیرساختی، اقدامات زمانی ارزشمند است که با پیامدها اثری بر مردم نداشته باشد.
وی خاطرنشان کرد: استان آذربایجان شرقی، استانی صنعتی است و از همین رو باید متناسب با این ظرفیت ها، اقدامات لازم برای مقابله با تهدیدات پیش بینی و رصد شود. یکی از مهمترین این اقدامات این است که حداکثر اقدامات برای استقرار و تجهیز واحدهای آتش نشانی تخصصی مانند واحدهای HAZMAT برای زیرساخت های شیمیایی و انرژی در استان اجرایی گردد.
رئیس سازمان پدافند غیرعامل کشور با بیان اینکه ساماندهی مراکز پرخطر شهری از جمله اولویت های سازمان پدافند غیرعامل کشور است، متذکر شد: مراکز پرخطر شهر حتما باید از حریم شهرها خارج شوند و اگر امکان خروج آنها وجود ندارد باید براساس اصول پدافند غیرعامل امن سازی شوند تا در صورت بروز حادثه و تهدید به مردم و دارایی آنها آسیبی نرسد.

اهمیت برگزاری رزمایش و آموزش در حوزه پدافند غیرعامل

تراب محمدی سرپرست استانداری استان آذربایجان شرقی استاندار آذربایجان شرقی با بیان اینکه شورای پدافند غیرعامل در این استان جزو شورای های فعال و پویا و مهم محسوب می شود اظهار داشت: تمامی قرارگاه های ذیل این شورا فعال هستند. همچنین رزمایش ها و دوره های آموزشی لازم برای افرادی که باید در حوزه پدافند غیرعامل آموزش ببینند به طور مرتب برگزار می شود.
به گفته وی اهتمام در انجام وظایف و تکالیفی که برعهده شورای پدافند غیرعامل استان آذربایجان شرقی گذاشته شده است، سبب شد تا شورای پدافند غیرعامل استان آذربایجان شرقی به عنوان شورای پدافند غیرعامل نمونه کشور از طرف سازمان پدافند غیرعامل کشور، معرفی شود.

ضرورت دوگانه سوز کردن واحدهای نانوایی

در ادامه این جلسه دکتر کشوری، معاون انرژی سازمان پدافند غیرعامل کشور با بیان اهمیت مکانیابی در استقرار زیرساختها به ویژه زیرساختهای انرژی با توجه به ضوابط پدافند غیرعامل، اظهار داشت: توجه به معماری و جغرافیایی استانی در ایجاد وابستگی بین زیرساخت های حوزه انرژی در استان نیز از جمله مواردی است که باید به آن توجه جدی داشت.

وی همچنین با اشاره به لزوم چاره اندیشی در مورد ناترازی انرژی و لزوم مدیریت مصرف انرژی به تبیین ضرورت دوگانه سوز کردن واحدهای نانوایی به لحاظ اصول پدافند غیرعامل پرداخت و تصریح کرد: امکان استفاده از سوخت جایگزین برای پخت نان در مواقع بروز مشکلات احتمالی از اهمیت ویژه ای برخوردار است که باید با جدیت پیگیری شود.

همچنین غلامرضا باقری مدیرعامل جدید پالایشگاه تبریز نیز در ادامه به تشریح اقدامات این پالایشگاه در حوزه پدافند غیرعامل پرداخت.

ضرورت همگرایی و تقویت زیرساخت‌های حوزه نفتی

شایان ذکر است سردار جلالی در ادامه سفر خود به استان آذربایجان شرقی، در گردهمایی فرماندهان ارشد پدافند غیرعامل مناطق ویژه نفتی شرکت کرد.

در این جلسه، بر همگرایی و تقویت زیرساخت‌های حوزه نفتی جهت ارتقاء آمادگی در پاسخ به تهدیدات تأکید شد و فرماندهان ارشد پدافند غیرعامل به دستاوردهای مهم در این زمینه اشاره کردند.

همچنین فرماندهان ارشد پدافند غیرعامل مناطق نفتی ضمن ارائه گزارش پیشرفت اقدامات پدافندی، بر ضرورت برگزاری تمرینات، آموزش‌ها و رزمایش‌های منظم و هماهنگی بین سایر دستگاه‌های اجرایی برای افزایش آمادگی و کارآیی در مقابله با تهدیدات تأکید کردند.

تحلیل

یکی از مهمترین رویکردهای سازمان پدافند غیرعامل به ویژه در مدیریت شهری، پیشگیری و کاهش خطرات برای مردم و زیرساخت‌ها، در راستای تقویت امنیت و پایداری مراکز زیست شهری است. بکارگیری یک رویکرد جامع و پیشگیرانه در مدیریت تهدیدات و کاهش آسیب‌ها از طریق پدافند غیرعامل اگر به طور کامل و دقیق اجرا شوند، می‌توانند نقش مؤثری در افزایش امنیت و پایداری زیرساخت‌ها و حفاظت از جان و مال مردم ایفا کنند.

پدافند سایبری

در راستای ارتقای امنیت سایبری انجام شد؛

راه‌اندازی سامانه کشف فیشینگ

وزارت ارتباطات و فناوری اطلاعات با هدف ارتقای امنیت سایبری، اقدام به راه‌اندازی سامانه کشف فیشینگ کرده است. این سامانه، با همکاری اپراتورها و پلیس فتا، پیامک‌های حاوی لینک‌های آلوده جعلی را شناسایی و برای مسدودسازی ارسال می‌کند. وزیر ارتباطات، عیسی زارع‌پور، از افزایش ۲۳ درصدی مراکز آگاهی، پشتیبانی و امداد رایانه‌ای (آپا) و رشد ۲۵۰ درصدی شرکت‌های همکار مرکز ماهر برای کشف آسیب‌پذیری‌های دستگاه‌ها خبر داد. اقدامات راهبردی دیگر شامل توسعه زیرساخت‌های بومی امنیت سایبری، حمایت از شرکت‌های دانش‌بنیان، و ایجاد سامانه بومی مقابله با حملات DDoS است. سازمان فناوری اطلاعات نیز با افزایش ظرفیت‌ها و برگزاری مسابقات کشف آسیب‌پذیری، بیش از ۲۵۰۰ آسیب‌پذیری را شناسایی و رفع کرده است. خدمات دیگر شامل راه‌اندازی مرکز ارائه خدمات امنیتی مدیریت شده (MSSP)، مقابله با حملات سایبری پیچیده، و برگزاری دوره‌های آموزشی بوده است.

برای حل مشکل کمبود اعتبارات، دستگاه‌های دولتی موظف شده‌اند یک درصد از بودجه خود را به امن‌سازی زیرساخت‌ها اختصاص دهند.

تحلیل

اقدامات وزارت ارتباطات، شامل راه‌اندازی سامانه کشف فیشینگ، افزایش مراکز آپا، توسعه زیرساخت‌های بومی، و حمایت از شرکت‌های دانش‌بنیان، به ارتقای پدافند سایبری کشور کمک کرده است. همچنین، الزام دستگاه‌های دولتی به تخصیص بودجه برای امنیت سایبری و ارائه خدمات امنیتی مدیریت شده، توانمندی کشور در مقابله با تهدیدات سایبری را تقویت کرده است.

پدافند سایبری

تشدید بحران انرژی در عصر هوش مصنوعی

با گسترش روزافزون هوش مصنوعی، مراکز داده جدید با سرعت زیادی در حال احداث هستند. این امر منجر به افزایش چشمگیر تقاضا برای برق مورد نیاز جهت راه‌اندازی و خنک سازی سرورها شده و نگرانی هایی نسبت به توانایی تولید برق کافی برای استفاده گسترده از هوش مصنوعی و ظرفیت شبکه برق فرسوده آمریکا برای تحمل این بار اضافی به وجود آورده است. براساس گزارش گلدمن ساکس، یک پرسش در «ChatGPT» تقریباً ۱۰ برابر یک جستجوی معمولی در گوگل انرژی مصرف می کند. تولید یک تصویر توسط هوش مصنوعی می تواند، به اندازه شارژ کامل یک گوشی هوشمند برق مصرف کند. از سوی دیگر، برآوردها نشان می دهد که تا سال ۲۰۳۰، مراکز داده ۱۶ درصد از کل مصرف برق آمریکا را به خود اختصاص خواهند داد؛ رقمی که معادل دو سوم برق مصرفی خانه های این کشور است. از همین رو، کارشناسان راهکارهای زیر را برای مقابله با این چالش در نظر دارند:

بهبود کارایی محاسباتی و کاهش مصرف انرژی، استفاده از منابع انرژی تجدیدپذیر مانند خورشیدی و بادی، بهره گیری از انرژی هسته ای و زمین گرمایی، ساخت نیروگاه های اختصاصی برای مراکز داده، بهینه سازی شبکه برق با استفاده از فناوری های پیش بینی خرابی

علاوه بر مصرف برق، خنک سازی سرورها نیز چالش بزرگی برای تداوم احداث و گسترش مراکز داده به مشار می رود. برآوردها حاکی از آن است که تا سال ۲۰۲۷، مراکز داده هوش مصنوعی به ۴,۲ تا ۶.۶ میلیارد متر مکعب آب برای خنک سازی نیاز داشته باشند.

در حالی که صنعت به دنبال راه حل هایی برای این چالش هاست، برخی شرکت ها مانند اپل و سامسونگ بر توسعه هوش مصنوعی روی دستگاه های الکترونیکی تمرکز کرده اند تا از فشار بر مراکز داده بکاهند.

تحلیل

گسترش هوش مصنوعی منجر به افزایش سریع ساخت مراکز داده و تقاضای برق برای راه‌اندازی و خنک سازی سرورها شده که نگرانی هایی درباره توانایی تولید برق کافی و ظرفیت شبکه برق ایجاد کرده است. از همین رو در توسعه این فناوری، توجه به زیرساختهای لازم برای آن یک ضرورت است.

پدافند سایبری

هشدار کارشناسان امنیت سایبری؛

تبلیغ گوگل بدافزار از آب درآمد

هکرها فضای تبلیغاتی را به طور مستقیم از گوگل خریده اند و در پوشش سایت واقعی احراز هویت این شرکت (Google Authenticator) که سیستم ایمنی احراز هویت ۲ عاملی را ارائه می کند، فعالیت می کنند.

این کمپین کلاهبرداری از یک URL گوگل که به نظر قانونی می رسد استفاده کرده اما نگاهی دقیق تر نشان دهنده آن است که شرایطی که شرکت برای کاربران نمایش می دهد در این لینک وجود ندارد.

کاربرانی که این لینک کلاهبردارانه را دانلود می کنند احتمالا اجازه دسترسی به جزییات حساب های بانکی شان، آدرس و IP آدرس های خصوصی شان را به هکرها می دهند. کارشناسان قبلا به کاربران توصیه کرده بودند فقط روی لینک های تبلیغاتی کلیک کنند که دامنه گوگل را دارند اما به نظر می رسد هکرها این بار هوشمندانه تر عمل کرده و از ابزارهای اصلاح کننده متن و فناوری های پوششی برای تقلید از وب سایت های واقعی استفاده کرده اند. این تبلیغ خطرناک سبب می شود کاربران نسخه هایی از ابزار احراز هویت را نصب کنند که قبلا توسط یک کمپین توزیع بدافزار به نام DeerStealer توزیع شده بود.

تحلیل

این حادثه همچنین نشان می‌دهد که توصیه‌های سنتی مبنی بر اعتماد به لینک‌های دارای دامنه معتبر، دیگر به تنهایی کافی نیست. هکرها با استفاده از ابزارهای پیشرفته اصلاح متن و فناوری‌های پوششی، توانسته‌اند به شکلی موفقیت‌آمیز ظاهر وب‌سایت‌های معتبر را تقلید کنند. این مسئله بر اهمیت آموزش کاربران در مورد خطرات احتمالی و افزایش آگاهی آن‌ها نسبت به نشانه‌های هشداردهنده کلاهبرداری‌های اینترنتی تأکید دارد.

پدافند سایبری

مسدودسازی اینستاگرام در ترکیه

دولت ترکیه اخیرا دسترسی به اینستاگرام را برای ۸۵ میلیون نفر جمعیت این کشور مسدود کرد. این اقدام پس از سانسور گسترده و حذف پست‌های مرتبط با شهادت اسماعیل هنیه، رهبر حماس، توسط اینستاگرام صورت گرفت. مقامات ترکیه این مسدودسازی را پاسخی به سانسور تسلیت کاربران این کشور به مناسبت شهادت هنیه در این پلتفرم اعلام کردند.

فخرالدین آلتون، مدیر ارتباطات ریاست جمهوری ترکیه، این اقدام اینستاگرام را سانسور آشکار توصیف کرد و اظهار داشت که دولت ترکیه به دفاع از آزادی بیان در مقابل این پلتفرم ادامه خواهد داد. وی در این خصوص گفت: «این اقدام صراحتاً سانسور است. ما از آزادی بیان در برابر این پلتفرم‌ها که بارها نشان داده‌اند در درجه اول در خدمت سیستم استثماری جهانی و بی‌عدالتی هستند، دفاع خواهیم کرد.»

به عقیده بسیاری از کارشناسان، اقدام اینستاگرام برخلاف ادعاهای این شرکت مبنی بر حمایت از آزادی بیان و رعایت سیاست بی‌طرفی است و حذف پست‌های تسلیت برای رهبر حماس به وضوح نشان می‌دهد که این پلتفرم‌ها به جای احترام به تنوع دیدگاه‌ها، به سانسور محتواهایی می‌پردازند که با سیاست‌های خاصی ناسازگار است.

تحلیل

این رویداد، بیش از پیش اهمیت و ضرورت حکمرانی سایبری در تضمین امنیت سایبری کشورها را مورد تاکید قرار می‌دهد.

پدافند سایبری

افزایش دوبرابری ظرفیت مراکز داده منطقه آسیا-اقیانوسیه تا سال ۲۰۲۸

کارشناسان معتقدند که با توجه به رشد فزاینده استفاده از هوش مصنوعی مولد و نیاز به زیرساخت‌های پیشرفته برای پردازش داده‌ها، ظرفیت مراکز داده در منطقه آسیا-اقیانوسیه تا سال ۲۰۲۸ دو برابر خواهد شد. برآوردها حاکی از آن است که ظرفیت این منطقه در حال حاضر حدود ۱۰,۵۰۰ مگاوات است و تا سال ۲۰۲۸ به ۲۴,۸۰۰ مگاوات خواهد رسید. هوش مصنوعی مولد به دلیل ایجاد نیازهای جدید به انرژی، فضای ذخیره‌سازی، خنک‌سازی و ظرفیت، تأثیر عمیقی بر صنعت مراکز داده داشته است. این فناوری به سرعت در حال تبدیل شدن به منبع اصلی تقاضا برای مراکز داده به شمار می‌رود و حتی ممکن است تقاضای فعلی برای فضای ابری را پشت سر بگذارد. چین، ژاپن، کره جنوبی و هند به عنوان بازارهای اصلی در این منطقه شناخته می‌شوند. این کشورها با افزایش سرمایه‌گذاری در حوزه زیرساخت‌های فیبر نوری و حمایت از توسعه دیجیتال، به توسعه و رشد این صنعت کمک کرده‌اند. در کشورهای جنوب شرقی آسیا مانند مالزی و اندونزی نیز رشد قابل توجهی در این زمینه مشاهده می‌شود. در مالزی، تلاش‌های دولت برای فروش زمین، اطمینان از دسترسی به برق و تسهیل فرآیندهای اداری باعث جذب اپراتورهای مراکز داده و کاربران نهایی شده است. در کشور اندونزی نیز جمعیت رو به رشد و افزایش تقاضای داخلی برای خدمات دیجیتال، این کشور را به یکی از بازارهای کلیدی تبدیل کرده است. با توجه به افزایش تقاضا برای ظرفیت‌های جدید در حوزه هوش مصنوعی، بخش اجاره تجهیزات، فضا و پهنای باند برای خدمات محاسباتی یا کولوکیشن (Colocation)، فرصتی بزرگ برای اپراتورهای مراکز داده فراهم کرده است. این اپراتورها می‌توانند با نوسازی و خلاقیت در زیرساخت‌های خود، نیازهای جدید را برآورده کنند و سهم بیشتری از این بازار پرسود را به خود اختصاص دهند.

تحلیل

افزایش تقاضا برای هوش مصنوعی مولد به رشد دو برابری ظرفیت مراکز داده در آسیا-اقیانوسیه تا ۲۰۲۸ منجر خواهد شد و فرصت‌های زیادی برای اپراتورهای مراکز داده ایجاد می‌کند تا با نوسازی زیرساخت‌ها، سهم بیشتری از بازار را کسب کنند.

پدافند سایبری

ضرر ۵.۴ میلیارد دلاری شرکت‌های آمریکایی از خطای کراود استرایک

شرکت‌ها در صنایع مختلف از جمله خطوط هوایی، بانکی و رسانه‌ای، روز جمعه با اختلال سایبری جهانی مربوط به پلتفرم ابری آزور مایکروسافت و مشکل نرم افزاری شرکت امنیت سایبری کراود استرایک روبرو شدند. دولت‌های استرالیا، نیوزیلند و شماری از ایالت‌های آمریکا هم با مشکل مواجه شدند، شرکت‌های هواپیمایی دلتا ایرلاینز، یونایتد ایرلاینز و الیجنت ایر، با اشاره به مشکلات ارتباطی، پروازهای خود را زمین گیر کردند. در انگلیس، اسکای نیوز که یکی از بزرگترین کانال‌های خبری تلویزیونی این کشور است، در روز جمعه، قطع شد. این مشکل برای رایانه‌هایی پیش آمد که با سیستم عامل ویندوز مایکروسافت و نرم افزار «کراود استرایک» کار می‌کردند. جدیدترین نسخه نرم افزار «فالکون سنسور» (FalconSensor) «کراود استرایک» قرار بود سیستم‌های مشتریان این شرکت را با به روزرسانی تهدیدهایی که در برابر آن‌ها دفاع می‌کند، در برابر هک ایمن‌تر کند. اما کد معیوب در فایل‌های به روزرسانی، منجر به یکی از گسترده‌ترین قطعی‌های فناوری در سال‌های اخیر برای شرکت‌هایی شد که از سیستم عامل ویندوز مایکروسافت استفاده می‌کردند. بیش از نیمی از شرکت‌های «فورچون ۵۰۰» و بسیاری از سازمان‌های دولتی آمریکا نظیر آژانس امنیت سایبری آمریکا، آژانس امنیت سایبری و امنیت زیرساخت، از نرم افزار این شرکت استفاده می‌کنند. شرکت بیمه «پارامتریکس» در بیانیه‌ای اعلام کرد خسارت بیمه شده این اختلال، احتمالا به ۵۴۰ میلیون دلار تا ۱.۰۸ میلیارد دلار برای شرکت‌های «فورچون ۵۰۰» بالغ خواهد شد. شرکت بیمه سایبری «بیزلی» هفته جاری اعلام کرد پس از این اختلال فناوری اطلاعات گسترده، تصمیم ندارد دستورالعمل درباره نسبت ترکیبی خود را که معیار کلیدی برای تعهد پرداخت است، تغییر دهد.

تحلیل

براساس الزامات پدافند سایبری باید با ارتقای سیستم‌های امنیتی و ایجاد پروتکل‌های دقیق برای بررسی و آزمایش به روزرسانی‌های نرم‌افزاری، مانند نرم‌افزار فالکون سنسور کراود استرایک، از وقوع اختلالات گسترده جلوگیری کند.

پدافندسایبری

نشت گسترده اطلاعات شرکت مخابراتی AT&T

شرکت مخابراتی «AT&T» اعلام کرد که هکرها طی یک عملیات سایبری به سوابق تلفن و پیامک شش ماهه همه مشتریان این شرکت دسترسی پیدا کرده‌اند. سخنگوی این شرکت تایید کرد که این داده‌ها از پلتفرم ابری «Snowflake» استخراج شده‌اند. براساس گزارش‌های منتشرشده، این حادثه یکی از بزرگترین حملات سایبری به این پلتفرم محسوب می‌شود. نماینده شرکت «AT&T» همچنین اظهار داشت که حداقل یک نفر در ارتباط با این نقض داده در بازداشت پلیس فدرال آمریکا قرار دارد.

گزارش‌ها حاکی از آن است که هکرها توانسته‌اند حجم زیادی از اطلاعات حساس کاربران را استخراج کنند. این داده‌ها شامل شماره تلفن‌هایی است که با کاربران تلفن همراه این شرکت ارتباط داشته‌اند. در برخی موارد، شناسه‌های خاص سایت‌های سلولی مرتبط با این تعاملات نیز فاش شده‌اند؛ اما محتوا، زمان‌بندی تماس‌ها یا پیام‌ها، شماره‌های امنیت اجتماعی و سایر اطلاعات شخصی در این داده‌ها وجود ندارند.

به عقیده کارشناسان، هکرها بین ۱۴ تا ۲۵ آوریل ۲۰۲۴ به فضای کاری «Snowflake» دسترسی پیدا کرده‌اند. «AT&T» تنها یکی از شرکت‌هایی است که به دلیل مشکلات امنیتی «Snowflake» دچار نقض اطلاعات شده است. این موارد نقض داده عمدتاً به دلیل عدم استفاده از تأیید هویت چندعاملی بوده است. این در حالی است که «Snowflake» اعلام کرد شواهدی از وجود نقص یا پیکربندی نادرست در پلتفرم خود نیافته است. سخنگوی شرکت مخابراتی آمریکایی اعلام کرد که این داده‌ها به صورت عمومی منتشر نشده‌اند.

تحلیل

تجارب چنین حوادثی نشان می‌دهد که پدافند سایبری باید با تاکید بر اجرای پروتکل‌های امنیتی قوی‌تر، از جمله تأیید هویت چندعاملی (MFA) و آموزش مستمر کارکنان برای شناسایی و پاسخ به تهدیدات، از وقوع نقض‌های امنیتی مشابه جلوگیری کند.

پدافندسایبری

مالیات استفاده از نرم افزارهای خارجی در روسیه

این درحالی است که روسیه سعی دارد وابستگی خود به شرکت های فناوری خارجی را کاهش و نمونه های داخلی خود را پررنگ تر کند.

ولادیمیر پوتین رییس جمهور روسیه دستیابی به استقلال فناورانه را یکی از اهداف کلیدی عنوان کرد. این درحالی است که تحریم های غربی به دلیل جنگ این کشور با اوکراین، توانایی روسیه برای دستیابی به تجهیزات و فناوری از شرکت های خارجی را محدود کرده است.

درهمین راستا پوتین در اوایل ماه می حکمی را امضا کرد که طبق آن حداقل ۸۰ درصد شرکت های روسی دربخش های اقتصادی حیاتی باید تا ۲۰۳۰ میلادی به جای نرم افزارهای خارجی از نمونه داخلی استفاده کنند.

بسیاری از شرکت های روسی همچنان در عملیات های روزانه خود از نرم افزارهای خارجی استفاده می کنند، هرچند تحریم های اتحادیه اروپا که در دسامبر ۲۰۲۳ میلادی وضع شد، اجازه نمی دهد شرکت ها نرم افزارهای شرکتی و طراحی را برای روسیه تامین کنند. به گفته وزیر توسعه دیجیتال روسیه وضع مالیات بر شرکت های روسی توازن بین نرم افزارهای خارجی و داخلی را برقرار می کند.

تحلیل

سیاستگذار با رویکرد پدافند سایبری با وضع مالیات بر استفاده از نرم افزارهای خارجی و تشویق به استفاده از نرم افزارهای داخلی، در تلاش است تا وابستگی به فناوری های خارجی را کاهش داده و امنیت سایبری کشور را تقویت کند، همچنین تحریم های بین المللی را با افزایش استقلال فناورانه خنثی سازد.

پدافندزیستی

نیاز ایران به ۲۰۰ هزار کیت تشخیص سریع تب دنگی

در نشست تخصصی راهکارهای مقابله با بیماری دنگی، نیاز فوری ایران به ۲۰۰ هزار کیت تشخیص سریع و ۱۰ هزار کیت مولکولی مورد بحث قرار گرفت. این نشست با حضور نمایندگان وزارت بهداشت، شرکت‌های دانش‌بنیان، انستیتو پاستور و دیگر نهادها برگزار شد و هدف آن تقویت تعامل میان بخش‌های مختلف برای مقابله با بیماری دنگی بود. بر اساس گزارش‌ها، از ابتدای سال ۱۴۰۳ تا ۳۱ تیر، ۱۵۲ مورد ابتلا به تب دنگی شناسایی شده است. در حالی که برخی کیت‌های مورد نیاز تامین شده، نگرانی‌هایی درباره تولید و تامین کامل کیت‌ها وجود دارد. متخصصان تاکید کردند که بهبود زیرساخت‌ها و ارتقاء توان کشور برای مقابله با بحران‌ها، همچون بیماری دنگی، باید در اولویت قرار گیرد. همچنین، کنترل حشره ناقل و تولید کیت‌های داخلی نیز از موضوعات مطرح شده بود.

تحلیل

شناسایی و رصد بیماری، از جمله الزامات مورد تاکید پدافند زیستی در مقابله با پاندمی هاست. درمورد تب دنگی که پشه آئدس ناقل آن است، نیاز فوری به ۲۰۰ هزار کیت تشخیص سریع تب دنگی و ۱۰ هزار کیت مولکولی نشان دهنده چالش‌های جدی در مقابله با این بیماری و ضرورت تقویت زیرساخت‌های بهداشتی کشور است.

پدافندزیستی

واکسیناسیون سراسری پنوموکوک در کشور

دکتر سید محسن زهرایی با اشاره به واکسیناسیون سراسری پنوموکوک برای کودکان زیر دو سال کشور، اظهار کرد: بیماری های بسیار خطرناک ناشی از عفونت های پنوموکوکی می تواند در گروه های سنی مختلف به ویژه کودکان زیر ۲ سال مشاهده شود.

وی با بیان اینکه عفونت های پنوموکوکی یکی از عوامل مرگ و میر کودکان زیر ۲ سال به شمار می رود، افزود: خوشبختانه تلاش های وزارت بهداشت برای بهره مندی بیشتر کودکان از حق سلامتی به ثمر نشست و مراحل ساخت و عرضه واکسن پنوموکوک کامل شد و نهایتا در ۲۳ اردیبهشت ماه سال جاری، ۷ استان خراسان های رضوی و جنوبی، سیستان و بلوچستان، هرمزگان، بوشهر، خوزستان و ایلام، تحت پوشش واکسیناسیون پنوموکوک قرار گرفتند.

رییس اداره بیماری های قابل پیشگیری با واکسن وزارت بهداشت عنوان کرد: از شنبه ۱۳ مردادماه ۱۴۰۳ نیز در سراسر کشور واکسن پنوموکوک برای کودکان ۲ ماهه در دسترس است؛ طبق برنامه کشوری واکسیناسیون، واکسن پنوموکوک در سه نوبت ۲ ماهگی، ۴ ماهگی و ۱۲ ماهگی به نوزادان تزریق می شود.

بنابر اعلام وزارت بهداشت، زهرایی خاطرنشان کرد: پیش بینی می شود که با واکسیناسیون پنوموکوک سالانه از مرگ و میر ۱۰۰۰ تا ۱۲۰۰ نوزاد و همچنین بستری شدن بیش از ۵۵ هزار نوزاد در بیمارستان، جلوگیری شود.

وی، واکسیناسیون پنوموکوک را در کاهش چشمگیر مصرف آنتی بیوتیک موثر دانست و افزود: این واکسیناسیون مقاومت آنتی بیوتیکی که در بیماری های پنوموکوکی رو به افزایش است را کنترل و به کاهش بار اقتصادی نظام سلامت کمک می کند.

تحلیل

واکسیناسیون پنوموکوک از منظر پدافند غیرعامل یک اقدام مهم و موثر در جهت کاهش مرگ و میر و بستری شدن نوزادان و نیز کاهش مصرف آنتی بیوتیک و کنترل مقاومت آنتی بیوتیکی است. اجرای موفقیت آمیز این برنامه می تواند تأثیرات مثبت زیادی بر سلامت کودکان و کاهش بار نظام سلامت کشور داشته باشد.

پدافند زیستی

استقرار پشه آئدس در ۷ استان

شهنام عرشی، رئیس مرکز مدیریت بیماری های واگیر وزارت بهداشت، با بیان اینکه دارای وضعیت به نسبت پایدار در مواجهه با «تب دنگی» هستیم، اظهار کرد: تعداد مبتلایان تب دنگی تغییر نکرده و تعداد مبتلایان براساس آخرین گزارش، معادل ۱۵۲ نفر است. اگرچه به وضعیت پایدار نسبی در ارتباط با تب دنگی دست یافته‌ایم، اما در ارتباط با ماه‌های شهریور و مهر احساس نگرانی می کنیم؛ چراکه فعالیت پشه آئدس با خنک‌تر شدن هوا بیشتر می شود و شاید بتوان گفت با خنک شدن هوا کانون های اپیدمی محلی داشته باشیم. وی با بیان اینکه پشه به صورت گسترده در نقاطی از کشور مستقر شده، گفت: پشه آئدس در ۷ استان کشور یعنی ۳ استان شمالی و ۴ استان جنوبی کشور مستقر شده است. اگرچه پشه در ۷ استان کشور به صورت گسترده مستقر شده اما پشه آلوده فقط در ۲ نقطه کشور صید شده است. حضور پشه آلوده در ۲ نقطه کشور یعنی «بندر لنگه» در استان هرمزگان و شهرستان «چابهار» گزارش شد؛ در نتیجه، انتقال محلی در این ۲ نقطه به ثبت رسیده اما شرایط کنترل شده است. برخی از نقاط کشور نیز در مجاورت ۷ استانی که پشه به صورت گسترده در آن ها وجود دارد، هستند که خطر گسترش پشه به این استان ها نیز وجود دارد. بنابراین اگرچه پشه‌ای در نقاط مجاور استان های مذکور، گزارش نشده اما احتمال حضور پشه در آنها وجود دارد. «پارس‌آباد مغان» و «بیله سوار» در استان اردبیل، «خداآفرین» در استان آذربایجان شرقی جزو مناطقی هستند که احتمال حضور پشه در آنها هست. قسمت هایی از استان کرمان، جنوب استان فارس، استان خوزستان و استان زنجان جزو مناطق مستعد حضور پشه آئدس هستند اما هنوز پشه در این مناطق صید نشده است. پشه در مناطقی که دارای آب و هوایی گرم هستند به تدریج نفوذ می کند.

تحلیل

براساس تاکیدات سازمان پدافند غیرعامل کشور به ویژه اجرای طرح ملی مقابله با ناقلین مهاجم زیستی باید بر روی کنترل و مهار پشه آئدس در ۷ استان مذکور تمرکز کرد تا با پیشگیری از گسترش آن به مناطق دیگر، از شیوع گسترده تب دنگی جلوگیری کند.

پدافند زیستی

زائران قبل از سفر اربعین واکسن سرخک بزنند

دکتر مسعود شریفی، معاون فنی مرکز بهداشت استان یزد اظهار کرد: با توجه به شیوع بیماری سرخک در کشور عراق و نزدیک شدن به ایام اربعین، زائران باید قبل از عزیمت به کشور عراق واکسن سرخک دریافت کنند. وی ضمن اعلام این خبر افزود: بیماری سرخک، یک بیماری ویروسی است که عموما کودکان را مبتلا می کند ولی افراد بزرگسال چنانچه سابقه ابتلا به بیماری و یا واکسیناسیون نداشته باشند در معرض خطر ابتلا خواهند بود. وی عنوان کرد: دوره نهفتگی بیماری از ۷ تا ۲۱ روز متفاوت است. بیماری با تب، علائم تنفسی و بثورات پوستی قرمزرنگ که از صورت شروع شده و به سمت اندام ها گسترش می یابد، بروز پیدا می کند. شریفی ادامه داد: چهار روز قبل از بروز تظاهرات پوستی تا چهار روز بعد از آن، بیماری از طریق تنفسی قابل انتقال است. بیماری سرخک بسیار مسری است و لذا موثرترین راه مقابله با آن واکسیناسیون به موقع است. معاون فنی مرکز بهداشت استان خاطرنشان کرد: در کشورهای همسایه از جمله عراق، پوشش واکسیناسیون کودکان برای مهار بیماری سرخک کافی نبوده و شاهد همه گیری بیماری در کشورهای همجوار به ویژه افغانستان، پاکستان و عراق هستیم. وی با بیان این که موارد بیماری در کشور عراق طی ماه های اخیر افزایش بیشتری داشته است، گفت: تعداد موارد سرخک در سال ۲۰۲۳ برابر با ۹ هزار و ۶۵۱ مورد بوده که در طی شش ماه اول سال ۲۰۲۴ به ۲۸ هزار و ۷۸۳ مورد افزایش یافته است. به منظور جلوگیری از ابتلای احتمالی هموطنان در سفر به عراق، توصیه می شود قبل از سفر، از کامل بودن سابقه واکسیناسیون سرخک کودکان زیر ۱۵ سال خود اطمینان داشته باشند. برای این منظور با در دست داشتن کارت واکسن کودکان خود به مراکز خدمات جامع سلامت مراجعه و در صورت نیاز نسبت به تکمیل واکسیناسیون کودکان خود اقدام کنند.

تحلیل

رعایت الزامات پدافند زیستی با تأکید بر واکسیناسیون اجباری سرخک برای زائران اربعین و اجرای پروتکل های بهداشتی در مرزها و تجمعات، می تواند از شیوع و انتقال این بیماری بسیار مسری جلوگیری کند.

پدافند زیستی

آزمایش اسپری نانویی بینی برای مقابله با ویروس آنفلوانزا و کرونا

این نانومحصول که با نام NanoSTING شناخته می شود، یک اسپری استنشاقی بوده که برای مقابله با ویروس کرونا ساخته شده است. این فناوری را می توان برای طیف وسیعی از ویروس ها بهینه سازی کرد. این گروه از این فناوری برای ویروس کرونا و آنفلوآنزا استفاده کردند و به صورت پیش بالینی این محصول را مورد آزمایش قرار دادند.

نتایج این آزمایش ها که توسط دانشگاه هیوستون منتشر می شود، ماحصل آزمایش روی همستروموش بوده و برای مقابله با ویروس کرونا طراحی و آزمایش شده است. NanoSTING فرمولاسیونی از ۳-۲ حلقوی GMP-AMP (cGAMP) بوده که در نانوذرات لیپیدی قرار دارد. این ماده برای جذب مؤثر در سراسر مخاط طراحی شده است تا مسیر محرک ژن های اینترفرون (STING) را فعال کند. نتایج نشان می دهد که NanoSTING به سرعت و به طور مؤثر سیستم ایمنی ذاتی را فعال می کند. این تحقیق از رویکرد شرکت آوراواکس تراپیوتیک با استفاده از NanoSTING برای درمان و پیشگیری از عفونت های ویروسی بهره می برد. به نقل از ستاد نانو، جوزف سالیوان، مدیرعامل این شرکت گفت: این داده ها ایمنی و کارایی NanoSTING داخل بینی را برای ایجاد پاسخ ایمنی موضعی در برابر دو ویروس تنفسی فصلی مهم نشان می دهد. این تحقیق پتانسیل درمانی NanoSTING را برای درمان و پیشگیری از عفونت های ویروسی و همچنین قطع گسترش ویروس نشان می دهد.

تحلیل

پدافند زیستی با توسعه و آزمایش فناوری‌های نوینی مانند اسپری نانویی بینی NanoSTING می‌تواند در پیشگیری و درمان مؤثر ویروس‌های آنفلوانزا و کرونا نقش مهمی ایفا کند و با فعال‌سازی سریع سیستم ایمنی ذاتی، از گسترش و شیوع این ویروس‌ها جلوگیری کند.

پدافند شیمیایی

مهار نشت گاز آمونیاک در عملیات بارگیری کشتی

سید محمد باقر یوسف زاده، سخنگوی فرماندهی ارشد پدافند غیرعامل و مدیریت بحران منطقه ویژه اقتصادی انرژی پارس از مهار نشت آمونیاک متعلق به شرکت پتروشیمی هنگام در زمان بارگیری در کشتی خبر داد. وی گفت: این اتفاق ساعت ۸ و ۴۵ دقیقه روز سه شنبه، نهم مرداد در اسکله شرکت پایانه مخازن پتروشیمی روی داد. یوسف زاده با بیان اینکه بلافاصله پس از نشت آمونیاک، گروه های عملیاتی منطقه کنترل را در دست گرفتند، افزود: پس از استقرار نیروهای عملیاتی اقدام های لازم انجام شد و هم اکنون اوضاع کاملاً در کنترل است. سخنگوی فرماندهی ارشد پدافند غیرعامل و مدیریت بحران سازمان منطقه ویژه اقتصادی انرژی پارس دلیل این حادثه را از سرویس خارج شدن یکی از کمپرسورهای دریافت کننده گاز در کشتی اعلام کرد و گفت: هم اکنون کمپرسور راه اندازی شده و وضعیت تحت کنترل است. یوسف زاده در پایان تأکید کرد: هم اکنون اوضاع کاملاً در کنترل است و جای هیچ گونه نگرانی نیست.

تحلیل

این حادثه نشان می دهد که با توجه و رعایت الزامات پدافند شیمیایی، داشتن سیستم های واکنش سریع و کارآمد، آموزش های مناسب، و رویه های دقیق مدیریت بحران، می توان به طور مؤثر با نشت های شیمیایی مقابله کرد و از وقوع فاجعه های بزرگ تر جلوگیری کرد.

گزارش تحلیلی

پدافند غیرعامل، کلید امنیت هوش مصنوعی در ایران

در تاریخ ۲۹ خردادماه ۱۴۰۳، شورای عالی انقلاب فرهنگی سند ملی هوش مصنوعی جمهوری اسلامی ایران را به تصویب رساند. این سند که به نهادهای مختلف کشور از جمله نهاد ریاست جمهوری، هیات وزیران، ستاد کل نیروهای مسلح و وزارتخانه‌های متعدد ابلاغ شده است، راهبردهای کلانی برای توسعه و بهره‌برداری از هوش مصنوعی در ایران تعیین می‌کند.

محورهای اساسی سند ملی هوش مصنوعی

این سند با تأکید بر مبانی اسلامی و ملی، به دنبال ایجاد زیست‌بومی مناسب برای توسعه هوش مصنوعی است. محورهای اساسی این سند شامل توسعه و تربیت سرمایه انسانی متخصص، ارتقای زیرساخت‌های حقوقی و فنی، حمایت از تحقیق و توسعه، و تدوین سیاست‌ها و مقررات ملی برای استفاده مسئولانه از هوش مصنوعی است.

حفاظت از زیرساخت‌های حیاتی

کشورهایی مانند ایالات متحده و کشورهای عضو اتحادیه اروپا بر حفاظت از زیرساخت‌های حیاتی خود تأکید ویژه‌ای دارند. آن‌ها با تدوین استانداردها و مقررات دقیق، امنیت زیرساخت‌های حساس خود را در برابر تهدیدات هوش مصنوعی تضمین می‌کنند. ایران نیز باید با ایجاد و اجرای استانداردهای ملی امنیت سایبری و هوش مصنوعی، زیرساخت‌های حیاتی مانند شبکه‌های انرژی، سیستم‌های حمل و نقل، و سیستم‌های مالی خود را ایمن کند.

کاهش آسیب‌پذیری‌ها

چین و روسیه با سرمایه‌گذاری گسترده در تحقیق و توسعه هوش مصنوعی، توانمندی‌های خود را در این حوزه تقویت کرده‌اند. ایران نیز باید با تقویت تحقیق و توسعه داخلی، توانمندی‌های خود را افزایش داده و وابستگی به فناوری‌های خارجی را کاهش دهد. این اقدام به کاهش آسیب‌پذیری‌های ناشی از تحریم‌ها و تهدیدات خارجی کمک می‌کند.

پیشگیری از تهدیدات سایبری

کشورهای پیشرو با استفاده از هوش مصنوعی برای شناسایی و پیشگیری از تهدیدات سایبری، سیستم‌های دفاعی هوشمندی ایجاد کرده‌اند. ایران نیز باید از هوش مصنوعی برای پیشگیری و شناسایی تهدیدات سایبری بهره‌برداری کند. توسعه سیستم‌های هوشمند امنیت سایبری و استفاده از الگوریتم‌های یادگیری ماشینی برای شناسایی تهدیدات می‌تواند در این زمینه مؤثر باشد.

تدوین سیاست‌ها و مقررات ملی

کشورهای پیشرو مانند سنگاپور و ژاپن با تدوین سیاست‌ها و مقررات ملی برای توسعه هوش مصنوعی، به توسعه پایدار و ایمن این فناوری پرداخته‌اند. ایران نیز باید با تدوین سیاست‌ها و مقررات ملی، استفاده مسئولانه و ایمن از هوش مصنوعی را تضمین کند. این سیاست‌ها می‌توانند شامل مقررات مربوط به حفاظت از داده‌ها، حقوق کاربران و اخلاق هوش مصنوعی باشند.

ترویج فرهنگ‌سازی و آموزش

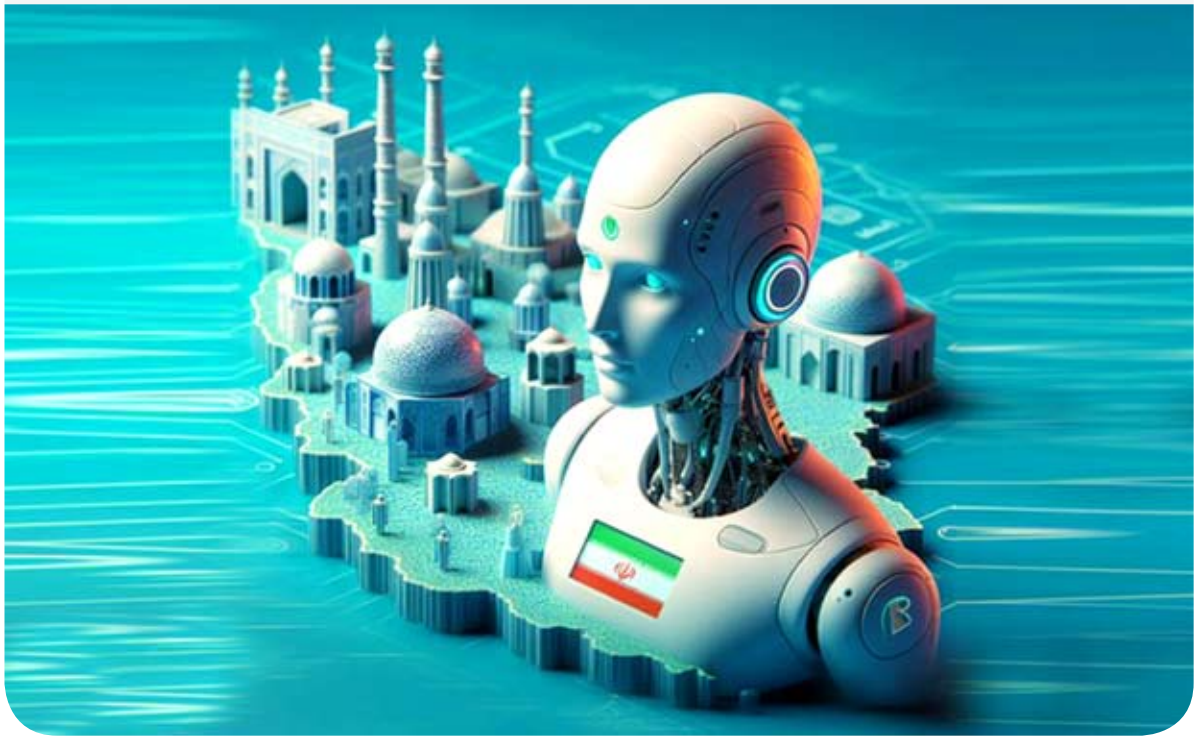
کشورهای پیشرو در زمینه هوش مصنوعی برنامه‌های گسترده‌ای برای آموزش و ترویج فرهنگ‌سازی در این حوزه دارند. آن‌ها با آموزش نیروی انسانی متخصص، زمینه‌های لازم برای توسعه هوش مصنوعی را فراهم کرده‌اند. ایران نیز باید برنامه‌های آموزشی گسترده‌ای برای تربیت نیروی انسانی متخصص در زمینه هوش مصنوعی اجرا کند. این امر می‌تواند از طریق ایجاد دوره‌های آموزشی در دانشگاه‌ها و مؤسسات آموزش عالی و برگزاری کارگاه‌ها و سمینارهای تخصصی محقق شود.

توسعه همکاری‌های بین‌المللی

کشورهای پیشرو در زمینه هوش مصنوعی با توسعه همکاری‌های بین‌المللی، از تجارب و دانش سایر کشورها بهره‌مند شده‌اند. ایران نیز باید با توسعه همکاری‌های بین‌المللی در زمینه هوش مصنوعی، از تجارب و دانش سایر کشورها بهره‌مند شود. این امر می‌تواند از طریق مشارکت در پروژه‌های بین‌المللی و همکاری با دانشگاه‌ها و مؤسسات تحقیقاتی خارجی محقق شود.

نتیجه‌گیری

تقویت ابعاد پدافند غیرعامل در توسعه هوش مصنوعی در ایران از اهمیت ویژه‌ای برخوردار است. با توجه به تجارب و سیاست‌های سایر کشورهای پیشرو، ایران باید به حفاظت از زیرساخت‌های حیاتی، کاهش آسیب‌پذیری‌ها، پیشگیری از تهدیدات سایبری، تدوین سیاست‌ها و مقررات ملی، ترویج فرهنگ‌سازی و آموزش، و توسعه همکاری‌های بین‌المللی بپردازد. این اقدامات می‌توانند زمینه‌های لازم برای توسعه پایدار و ایمن هوش مصنوعی در ایران را فراهم کنند.



گزارش تحلیلی

اعتیادآور بودن شبکه‌های اجتماعی و چاره‌اندیشی قانونگذاران

● استفاده زیاد و مداوم از شبکه های اجتماعی منجر به بروز رفتارها و مشکلاتی می شود که از نظر مغزی، مشابه مصرف مواد مخدر است. از طرفی مشکلات سلامت روان و اختلالات شناختی ناشی از استفاده بی رویه از شبکه های اجتماعی افزایش چشمگیری داشته است. افزایش جراحی های زیبایی ناشی از تغییرات نگرش به بدن، احساس ناکارآمدی، اضطراب، افسردگی ناشی از مقایسه زندگی واقعی فرد با آنچه که از شبکه های مجازی دریافت میکند، همگی نمونه هایی از این مشکلات هستند. کشورهای مختلف با توجه به این موارد به دنبال طراحی اقداماتی جهت کاهش استفاده از شبکه های مجازی و راه هایی برای تشخیص اخبار جعلی، عکس های فیلتر شده و ... هستند.

برای نمونه ماه گذشته جراح کل آمریکا دکتر "ویوک مورتی" به کنگره آمریکا پیشنهاد داد تا برچسب هایی شبیه برچسب های محصولات حاوی تنباکو و الکل در پلتفرم های شبکه های اجتماعی مورد استفاده قرار بگیرد. هدف از این اقدام افزایش آگاهی درباره آسیب های احتمالی این پلتفرم ها و تشویق کاربران به تغییر رفتار است. مورتی می گوید: «بحران سلامت روان در میان جوانان یک وضعیت اضطراری است و شبکه های اجتماعی به عنوان یک عامل مؤثر و مهم در این زمینه ظهور کرده اند.» وی همچنین خواستار قانون گذاری در این زمینه شده است تا از جوانان در برابر آزار، سوءاستفاده و مواجهه با خشونت یا محتواهای جنسی در فضای آنلاین محافظت شود.

او می گوید شبکه های اجتماعی نباید اطلاعات کودکان را گردآوری کنند و برخی قابلیت ها مثل ارسال نوتیفیکیشن، پخش خودکار محتوا و اسکرول بی نهایت را در اختیار آن ها قرار دهند. این قابلیت ها می توانند در ایجاد اعتیاد به مصرف این محتواها تأثیرگذار باشند.

همچنین در اقدامات دیگری برای میزان مصرف از شبکه ها بر اساس سن فرد (خصوصا کودک یا نوجوان) با اعمال محدودیت همراه می شود. عکس های ساختگی علامت دار می شوند، منابع انتشار اخبار با علامت هایی مشخص می شوند و....

در ایران نیز با توجه به عدم دسترسی به شرکت های مادر پلتفرم ها، استفاده از فیلترشکن توسط مردم و...

از طرفی آمار بالای برخی مشکلات و بیماری ها، افت تحصیلی، شکاف بین نسلی و ... که غالبا تحت تاثیر استفاده بی رویه از شبکه های اجتماعی است، نیازمند قانونگذاری های مفید در این زمینه هستیم این اقدامات می تواند شامل ایجاد دسترسی به شبکه های فیلترشده با پوسته های داخلی، افزایش سواد رسانه ای به همه افراد جامعه، ممنوعیت تولید برخی محتواها که منجر به تغییرات ادراکی-شناختی آسیب زا (مانند بازی نهنگ آبی، جوکر و...) می شود، باشد.

گزارش تحلیلی

ادغام تکنولوژی‌های جنگ اطلاعاتی و جنگ شناختی: عرصه‌ای نوین با ظرفیت‌های تاکتیکی منحصربه‌فرد

مقدمه:

در دنیای امروز، جنگ‌های اطلاعاتی و شناختی به یکی از ابزارهای حیاتی در استراتژی‌های نظامی و سیاسی تبدیل شده‌اند. این نوع جنگ‌ها از فناوری‌های پیشرفته برای تأثیرگذاری بر اطلاعات و درک عمومی بهره می‌برند و می‌توانند در حوزه‌های گوناگون از نظامی گرفته تا اقتصادی و سیاسی تأثیرگذار باشند. در این مقاله به بررسی تکنولوژی‌های سخت‌افزاری و نرم‌افزاری که در جنگ‌های اطلاعاتی و شناختی به کار گرفته می‌شوند، می‌پردازیم.

بخش اول: تعریف و اهمیت جنگ اطلاعاتی و شناختی

✓ جنگ اطلاعاتی

جنگ اطلاعاتی به استفاده از فناوری‌های اطلاعاتی برای جمع‌آوری، تجزیه و تحلیل و توزیع اطلاعات به منظور دستیابی به اهداف نظامی یا سیاسی گفته می‌شود. این نوع جنگ بر مدیریت و کنترل جریان اطلاعات تمرکز دارد و می‌تواند شامل فعالیت‌هایی همچون جاسوسی، شنود اطلاعاتی، و نفوذ به سیستم‌های اطلاعاتی دشمن باشد.

اخیراً بنیاد دفاع از دموکراسی‌ها تعریف جدیدی از محیط اطلاعاتی ارائه داده است. در این تعریف، محیط اطلاعاتی به‌عنوان مجموعه‌ای از عوامل اجتماعی، فرهنگی، زبانی، روان‌شناختی، تکنیکال و جسمانی که بر چگونگی برانگیختن انسان و سیستم‌های خودکاری که معنا استخراج می‌کنند، بر روی معنا کار می‌کنند و متاثر از معنای استنباط شده هستند، اطلاق می‌شود. این سیستم‌ها شامل افراد، سازمان‌ها و سیستم‌هایی است که اطلاعات را انتخاب، پردازش، منتشر و به طور کلی استفاده می‌کنند. این تعریف بر پیچیدگی و گستردگی اطلاعات تأکید می‌کند و جنگ اطلاعاتی را فراتر از جنگ سایبری می‌داند. علت گسترده بیان کردن فضای اطلاعاتی به این دلیل است که جنگ اطلاعاتی صرفاً میدانی برای جنگیدن نیروهای نظامی نباشد، بلکه یک رویکرد استراتژیک بزرگ به مفهومی که فراتر از نیروهای نظامی است و ابزارهای اصلی قدرت ملی را در بر می‌گیرد، اتخاذ کند. بر این اساس، با توجه به هدف نویسنده، اصطلاح

«جنگ اطلاعاتی» به پیام‌ها - و به معنای انتقال آن پیام‌ها - اشاره دارد که دولت‌های غربی برای پیشبرد اهداف سیاسی، اقتصادی و امنیتی و تقویت پایه‌های قدرت دولت استفاده می‌کنند، یعنی تقویت متحدان و شرکا، و تضعیف دشمنان.
با توجه به این تعریف و با وجود اقدامات دشمن در عرصه‌ای فراتر از نیروهای نظامی، به نظر می‌رسد راهکارهای پدافند غیرعامل برای دفاع از مردم، به میدان آوردن و بسیج افراد برای فعالیت در این میدان ضروری به نظر می‌رسد.

✓ **جنگ شناختی**

جنگ شناختی به مجموعه‌ای از فعالیت‌های استراتژیک اطلاق می‌شود که هدف آن تأثیرگذاری بر فرآیندهای شناختی و تصمیم‌گیری انسان‌ها از طریق دستکاری اطلاعات و استفاده از فناوری‌های روان‌شناختی است. این جنگ به‌طور خاص بر درک و ذهنیت افراد تمرکز دارد و به دنبال تغییر رفتارها و باورهای آنان است.

بخش دوم: تکنولوژی‌های سخت‌افزاری در جنگ اطلاعاتی و شناختی

۱. ماهواره‌ها و سنسورهای پیشرفته

ماهواره‌ها و سنسورهای پیشرفته نقش بسیار مهمی در جمع‌آوری و تحلیل اطلاعات در جنگ اطلاعاتی دارند. این ابزارها به شناسایی تحرکات نظامی، نظارت بر فعالیت‌های دشمن و جمع‌آوری داده‌های جغرافیایی کمک می‌کنند. استفاده از فناوری‌هایی مانند سنسورهای مادون قرمز و تصویربرداری حرارتی می‌تواند اطلاعات دقیق‌تری را فراهم کند.

۲. سیستم‌های هواپیمای بدون سرنشین (پهپاد)

پهپادها یکی از ابزارهای کلیدی در جمع‌آوری اطلاعات و اجرای عملیات شناسایی هستند. این سیستم‌ها با توانایی پرواز در ارتفاعات مختلف و تجهیز به دوربین‌ها و سنسورهای پیشرفته، به نیروهای نظامی امکان می‌دهند که به‌صورت مخفیانه به اطلاعات دشمن دسترسی پیدا کنند. پهپادها همچنین برای اجرای حملات دقیق و کنترل‌نشده به کار می‌روند.

۳. سیستم‌های شنود و ارتباطی

تجهیزات شنود و ارتباطی به نیروهای نظامی امکان می‌دهند که مکالمات و تبادل اطلاعات دشمن را شنود کرده و تحلیل کنند. این تکنولوژی‌ها شامل دستگاه‌های شنود رادیویی و ابزارهای پیشرفته تحلیل سیگنال هستند که می‌توانند اطلاعات مفیدی در مورد ارتباطات دشمن فراهم کنند.

۴. کامپیوترهای پیشرفته و مراکز داده

کامپیوترهای پیشرفته و مراکز داده از مهم‌ترین ابزارها در تجزیه و تحلیل داده‌های بزرگ

هستند. این سیستم‌ها با قدرت پردازش بالا می‌توانند اطلاعات جمع‌آوری شده را به سرعت تحلیل کرده و نتایج مفیدی برای تصمیم‌گیری ارائه دهند. مراکز داده پیشرفته با زیرساخت‌های امنیتی قوی می‌توانند از داده‌های حساس محافظت کنند.

بخش سوم: تکنولوژی‌های نرم‌افزاری در جنگ شناختی و جنگ اطلاعاتی

۱. هوش مصنوعی و یادگیری ماشین

هوش مصنوعی و یادگیری ماشین از مهم‌ترین ابزارها در تحلیل داده‌ها و شناسایی الگوهای پنهان هستند. این فناوری‌ها می‌توانند در تجزیه و تحلیل اطلاعات، شناسایی تهدیدات و پیش‌بینی رفتارهای دشمن بسیار مؤثر باشند. الگوریتم‌های یادگیری ماشین با توانایی پردازش حجم زیادی از داده‌ها، به نیروهای نظامی کمک می‌کنند تا اطلاعات را به سرعت تحلیل کنند. همچنین، با استفاده از تکنیک‌های مختلف که شامل الگوریتم‌های یادگیری ماشین و یادگیری عمیق است، می‌توان به تحلیل رفتارها، تمایلات و ترجیحات در افراد رسید. داده‌های رفتاری عموماً با ردیابی فعالیت‌های آنلاین و تحلیل شبکه‌های مجازی با استفاده از الگوریتم‌های پردازش زبان طبیعی، تحلیل می‌شوند.

۲. تحلیل داده‌های بزرگ (Big Data)

تحلیل داده‌های بزرگ نقش حیاتی در جمع‌آوری و تجزیه و تحلیل اطلاعات در جنگ اطلاعاتی دارد. این فناوری به نیروهای نظامی امکان می‌دهد تا از داده‌های جمع‌آوری شده به صورت کارآمد بهره‌برداری کنند و الگوهای مهم را شناسایی کنند. ابزارهای تحلیل داده‌های بزرگ می‌توانند در مدیریت و تحلیل حجم بالای اطلاعات مؤثر باشند.

تحلیل داده‌های بزرگ (Big Data) در جنگ شناختی به عنوان یکی از ابزارهای قدرتمند برای کسب اطلاعات و اثرگذاری بر افکار عمومی و رفتارها به کار می‌رود. جنگ شناختی شامل استفاده از اطلاعات و فناوری‌ها برای تحت تأثیر قرار دادن تفکر، تصمیم‌گیری و رفتار افراد یا گروه‌ها است. در ادامه به نحوه عملکرد تحلیل داده‌های بزرگ در این زمینه پرداخته می‌شود:

جمع‌آوری داده‌ها: داده‌ها از منابع مختلف مانند شبکه‌های اجتماعی، اخبار آنلاین، بلاگ‌ها، ویدئوها و دیگر منابع دیجیتال جمع‌آوری می‌شوند. این داده‌ها می‌توانند شامل متن، تصویر، ویدئو، و صدا باشند.

پردازش و ذخیره‌سازی: با استفاده از فناوری‌های پیشرفته مانند Hadoop و Spark، داده‌های بزرگ پردازش و در سیستم‌های توزیع شده ذخیره می‌شوند تا قابلیت جستجو و تحلیل آن‌ها فراهم شود.

پردازش زبان طبیعی (NLP): تحلیل متن‌های جمع‌آوری شده از شبکه‌های اجتماعی و رسانه‌ها برای استخراج و تحلیل احساسات و نظرات عمومی.
تحلیل احساسات (Sentiment Analysis): شناسایی و تحلیل احساسات مثبت، منفی یا خنثی درباره موضوعات مختلف و درک چگونگی تغییرات آن در طول زمان.

۳. شناسایی الگوها و روندها

خوشه‌بندی و طبقه‌بندی: استفاده از الگوریتم‌های یادگیری ماشین برای شناسایی الگوها و طبقه‌بندی داده‌ها به منظور شناسایی گروه‌های مختلف با نگرش‌ها و رفتارهای مشابه.

تحلیل روندها: بررسی تغییرات و روندهای اجتماعی و سیاسی برای پیش‌بینی تحولات آتی و شناسایی فرصت‌ها و تهدیدها.
با استفاده از اقداماتی که گفته شد، داده‌های بزرگ برای طراحی و اجرای عملیات شناختی صورت می‌گیرد. این عملیات در مراحل زیر انجام می‌شود:

هدف‌گذاری دقیق: استفاده از داده‌های بزرگ برای شناسایی گروه‌های هدف و طراحی پیام‌ها و محتوای متناسب برای هرگروه.

توزیع محتوا: استفاده از شبکه‌های اجتماعی و پلتفرم‌های دیجیتال برای انتشار و تقویت پیام‌های طراحی شده به منظور تأثیرگذاری بر تفکر و رفتار گروه‌های هدف.

۴. ارزیابی و بهبود

پایش و ارزیابی: استفاده از تحلیل داده‌های بزرگ برای پایش نتایج عملیات شناختی و ارزیابی اثربخشی آن‌ها مورد بهره‌برداری قرار می‌گیرد.

بهبود استراتژی‌ها: به‌روزرسانی و بهبود استراتژی‌های جنگ شناختی براساس بازخوردهای جمع‌آوری شده و تحلیل نتایج صورت می‌گیرد.

نمونه‌های کاربردی

عملیات روانی و تبلیغاتی: طراحی و اجرای کمپین‌های تبلیغاتی برای تحت تأثیر قرار دادن افکار عمومی یا تغییر نگرش‌ها و باورهای جامعه.

شناسایی تهدیدات: شناسایی و تحلیل رفتارهای مشکوک و تهدیدات امنیتی از طریق

تحلیل الگوهای رفتاری و تعاملات آنلاین.
با استفاده از تحلیل داده های بزرگ، سازمان ها و دولت ها قادر به طراحی و اجرای عملیات شناختی پیچیده و مؤثرتر می شوند که می تواند به تحقق اهداف سیاسی، اجتماعی یا اقتصادی منجر شود. این تحلیل به عنوان یکی از ارکان مهم در جنگ های مدرن و عملیات های اطلاعاتی شناخته می شود.

۵. نرم‌افزارهای شبیه‌سازی و واقعیت مجازی

حملات شناختی مستقیم و وابسته به ابزارهای مغزی (نه صرفاً در حوزه باورها و نگرش ها و تعریف متداول جنگ شناختی) در شرایط درگیری رسمی و مستقیم از نوع سخت جنگ شناختی است. در این نوع از جنگ شناختی برد با طرفی است که افرادی با توانمندی های بالاتر در حوزه های شناختی (توجه، سرعت پردازش، تحلیل و تصمیم گیری و...) دارد. به همین جهت قوای نظامی برخی از کشورها سرمایه گذاری های زیاد مالی و پژوهشی به این حوزه اختصاص داده اند. چرا که اقدام در این حوزه می تواند نتایج جنگ ها را کاملاً تحت تأثیر قرار دهد. این مورد در ابتدا ممکن است شبیه فیلم های علمی تخیلی باشد اما با مرور آنچه تاکنون انجام شده است، می بینیم که بی توجهی به این مسئله می تواند عرصه نبردهای آینده را به شدت تحت تأثیر قرار دهد.
در این حیطه از جنگ شناختی، نرم‌افزارهای شبیه سازی و واقعیت مجازی به نیروهای نظامی امکان می دهند تا سناریوهای مختلف را شبیه سازی کرده و بهترین راهکارها را شناسایی کنند. این تکنولوژی ها می توانند در آموزش و تمرین نیروهای نظامی و تحلیل اثرات جنگ شناختی مؤثر باشند. واقعیت مجازی با ایجاد محیط های شبیه سازی شده، به نیروها کمک می کند تا مهارت های خود را در شرایطی نزدیک به واقعیت تقویت کنند.

۶. سیستم های مدیریت اطلاعات

سیستم های مدیریت اطلاعات به نیروهای نظامی امکان می دهند تا داده ها و اطلاعات جمع آوری شده را به صورت سازمان یافته مدیریت کنند. این سیستم ها می توانند بهبود تصمیم گیری و افزایش کارآیی عملیات نظامی را به همراه داشته باشند. با استفاده از این سیستم ها می توان اهداف و نقاط استراتژیک را شناسایی کرد و الگوی عمل دشمن در مورد انتخاب نقاط حساس در کشور را پیش بینی کرد.
با توجه به وظایف سازمان پدافند غیرعامل، توجه به این سامانه ها در حفاظت از زیرساخت ها و مراکز حساس ضروری به نظر می رسد.
ادغام روش ها و ابزارهای جنگ شناختی و اطلاعاتی چگونه می تواند از موضوعات سازمان پدافند غیرعامل باشد؟
ادغام روش ها و ابزارهای جنگ شناختی و اطلاعاتی می تواند به عنوان یکی از

موضوعات مهم سازمان پدافند غیرعامل مورد بررسی قرار گیرد. در زیر به چندین راهکار و اثرات این ادغام اشاره شده است:

افزایش توانایی تحلیل و پیش‌بینی: با ادغام روش‌های جنگ شناختی (مانند تحلیل روان‌شناختی و رفتارشناسی) با ابزارهای اطلاعاتی (مانند تحلیل داده‌ها و اطلاعات بزرگ)، می‌توان به تحلیل و پیش‌بینی رفتارهای دشمنان و تهدیدات بالقوه پرداخت. این کار به سازمان پدافند غیرعامل کمک می‌کند تا راهبردهای بهتری برای مقابله با تهدیدات تدوین کند.

تقویت عملیات روانی: استفاده از داده‌ها و اطلاعات به‌روز می‌تواند به تقویت عملیات روانی کمک کند. با تحلیل دقیق‌تر از اهداف و مخاطبان، می‌توان پیام‌های موثرتری تولید و منتشر کرد که بر رفتار و نگرش مخاطبان تأثیرگذار باشد.

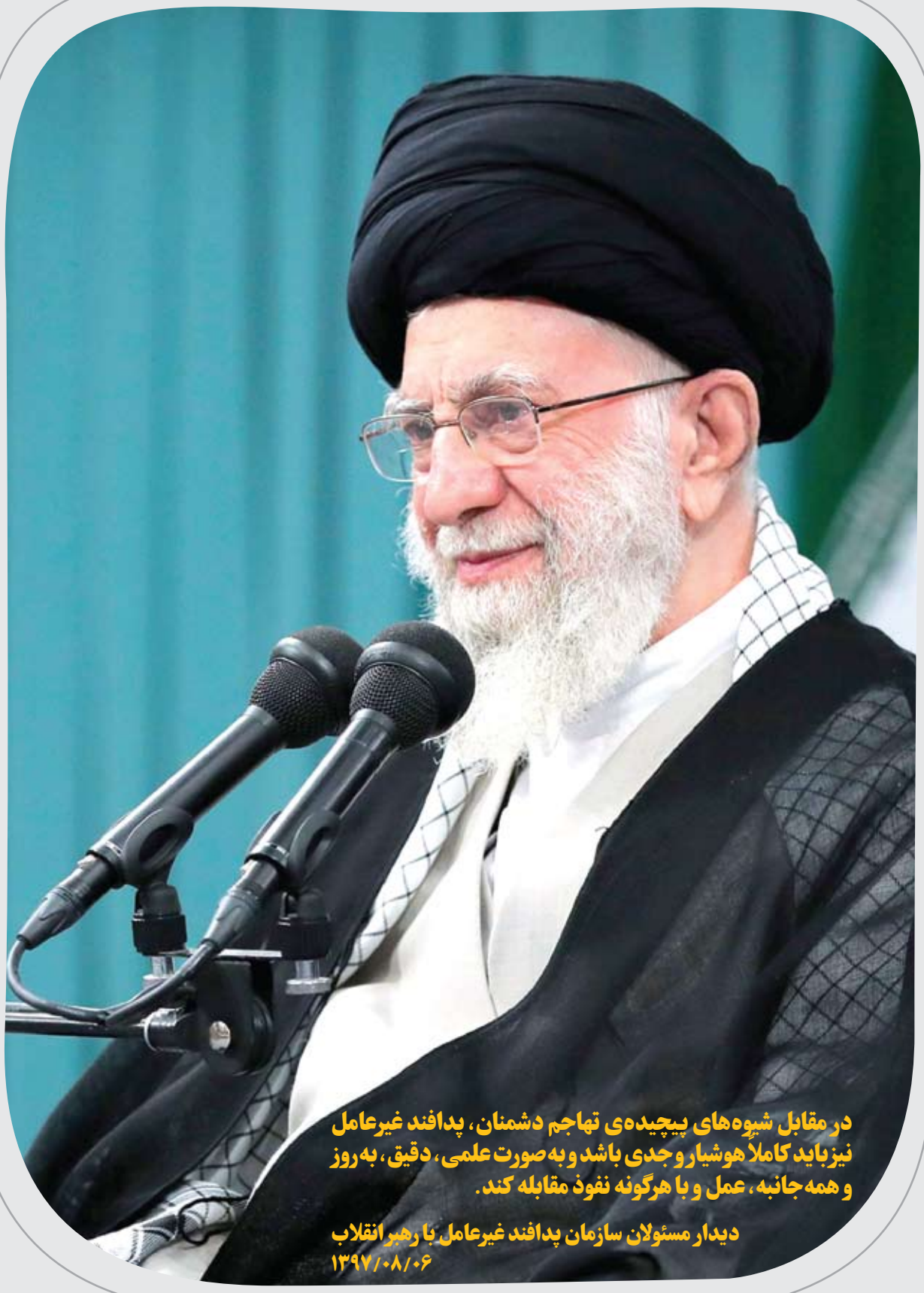
بهبود دفاع سایبری: ادغام این روش‌ها می‌تواند به بهبود دفاع سایبری کمک کند. با تحلیل الگوهای حمله و رفتارهای مهاجم، می‌توان سیستم‌های دفاعی بهتری را طراحی کرد که توانایی شناسایی و مقابله با تهدیدات را بهبود می‌بخشد.

ارتقاء هماهنگی بین نهادها: ادغام اطلاعات از منابع مختلف و تحلیل یکپارچه آن‌ها می‌تواند به بهبود هماهنگی بین نهادهای مختلف کمک کند. این امر باعث افزایش کارایی و اثربخشی در مواجهه با بحران‌ها و تهدیدات می‌شود.

آموزش و توانمندسازی نیروها: استفاده از این ابزارها و روش‌ها می‌تواند در طراحی برنامه‌های آموزشی و تمرینی برای نیروهای پدافند غیرعامل موثر باشد. آموزش نیروها برای استفاده از این تکنیک‌ها می‌تواند توانایی آن‌ها را در مقابله با تهدیدات افزایش دهد.

طراحی استراتژی‌های پیشگیرانه: با استفاده از تحلیل‌های پیچیده و شبیه‌سازی‌های مختلف، می‌توان استراتژی‌هایی را طراحی کرد که به پیشگیری از وقوع تهدیدات کمک کند. این استراتژی‌ها می‌توانند شامل ایجاد آگاهی عمومی، تقویت زیرساخت‌ها و بهبود مدیریت بحران باشند.

به طور کلی، ادغام روش‌ها و ابزارهای جنگ شناختی و اطلاعاتی می‌تواند به سازمان پدافند غیرعامل کمک کند تا در مقابل تهدیدات پیچیده و چندجانبه‌ای که امروزه با آن‌ها روبرو است، آمادگی و توانایی بیشتری داشته باشد.



در مقابل شیوه‌های پیچیده‌ی تهاجم دشمنان، پدافند غیرعامل نیز باید کاملاً هوشیار و جدی باشد و به صورت علمی، دقیق، به روز و همه جانبه، عمل و با هرگونه نفوذ مقابله کند.

دیدار مسئولان سازمان پدافند غیرعامل با رهبر انقلاب
۱۳۹۷/۰۸/۰۶