دیده‌بان

مروری بر مهمترین اخبار پدافند غیرعامل در سطح ایران و جهان

بولتن تحلیلی خبری | شماره دوم- فروردین ۱۴۰۳ | @pdpaydarymelli

سازمان پدافند غیرعامل کشور
مرکز آفرینش‌های هنری فاطر

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

ارتباطات و فناوری اطلاعات

سرعت اینترنت تا خرداد ۳۰ درصد افزایش می یابد

وزیر ارتباطات و فناوری اطلاعات گفت: با افزایش تعرفه اپراتورها، تعهدی از اپراتورها گرفتیم به این ترتیب که تا خرداد سال ۱۴۰۳، ۳۰ درصد و تا پایان سال، ۵۰ درصد به سرعت اینترنت اضافه شود. مشاهده داشبوردهای جهانی نشان داده که در اسفند ماه سال ۱۴۰۲، سرعت ثابت و سیار افزایش یافته و رتبه ما بهبود پیدا کرده است به طوری که ارتباطات موبایل ۵ پله و ارتباطات ثابت حدود ۳ پله بهبود پیدا کرده است.

پدافند زیستی

شناسایی دو مبتلا به مالاریا در غرب اهواز

مدیر گروه واحد مبارزه با بیماری های مرکز بهداشت غرب اهواز با اشاره به اینکه بهار فصل تخم‌ریزی بسیاری از حشرات است، از شناسایی دو نفر مبتلا به مالاریا در حوزه غرب شهرستان اهواز خبر داد. افراد شناسایی شده، در خارج از استان خوزستان مبتلا شده‌اند و پس از بروز علایم، توسط پرسنل مرکز بهداشت غرب اهواز شناسایی و تحت مراقبت و درمان قرار گرفته‌اند. کشورهای همسایه مانند افغانستان و پاکستان جزو کانون های این بیماری محسوب می شوند و افرادی که سابقه سفر به استان ها و کشورهای آلوده را دارند در صورت مشاهده تب و لرز حتما باید از نظر مالاریا بررسی شوند.

پدافند زیستی

افزایش محسوس مراجعه بیماران تنفسی به مراکز درمانی

دکتر مینو محرز، متخصص بیماری های عفونی درباره افزایش شیوع عفونت های تنفسی گفت: به طور کلی در ایام عید نوروز از آنجایی که هم سفرها و هم دید و بازدیدها افزایش پیدا می کند به ویژه اینکه دید و بازدید همراه با دست دادن و روبوسی کردن است قطعا با افزایش موارد ابتلا به عفونت های تنفسی مواجه هستیم و به همین دلیل امسال نیز با افزایش شیوع این بیماری ها روبه رو بودیم و هم اکنون ابتلا به کووید تا حدی بیشتر شده و علاوه بر آن آدونو ویروس ها که سرفه های شدیدی را به همراه دارند و سایر عفونت های تنفسی نیز شیوع دارند. شیوع این سویه مدتی در کشور کاهش یافته بود که مجددا با افزایش سفرها و دید و بازدید بیشتر شد، اما خوشبختانه سویه جدید کووید خفیف تر از سویه های قبلی است البته منجر به بستری و ایجاد درگیری ریه در تعدادی از مبتلایان شده است، ولی خدا را شکر این بیماران به درمان خوب پاسخ دادند و با مرگ و میر بالا مواجه نبودیم. مردم باید همچنان شیوه نامه های بهداشتی را به ویژه در دیدار با بزرگترها و افرادی که بیماری های زمینه ای دارند، رعایت کنند چرا که عفونت های تنفسی که در زمستان شایع بودند همچنان ادامه دارند و این روند تا زمانی که هوا گرم تر شود و سفرها کاهش یابد ادامه دارد.

پدافندزیستی

آخرین وضعیت بروز «آبله مرغان» و «سرخک» در کشور

دکتر شهنام عرشی، رئیس مرکز مدیریت بیماری های واگیر وزارت بهداشت گفت: بررسی میزان ابتلا به آبله مرغان در طی سال گذشته از افزایش این بیماری نسبت به سال های گذشته حکایت می کند. ارتباط کودکان به واسطه پروتکل های بهداشتی در دوران پاندمی کرونا کاهش یافته بود و به همین دلیل هم میزان ابتلا به بیماری آبله مرغان در سال های گذشته کاهش یافت. سال گذشته، ارتباط کودکان به واسطه بازگشت به زندگی عادی افزایش یافت و به همین دلیل، میزان ابتلا به آبله مرغان در سال ۱۴۰۲ نسبت به سال های گذشته افزایش یافت. وی درباره وضعیت بروز سرخک با توجه به اقدامات کشورمان در کنترل و حذف این بیماری خاطرنشان کرد: اگرچه سرخک را کنترل کرده ایم و در مرحله حذف آن قرار داریم، اما به واسطه شایع بودن این بیماری در کشورهای پاکستان و افغانستان و رفت و آمدها، با خطر بیماری سرخک مواجه هستیم. به همین دلیل رصد و پایش سرخک باید به نحوی باشد که افراد واکسینه نشده از مرزهای شرقی وارد کشور نشوند. خوشبختانه با پاندمی سرخک مواجه نیستیم؛ چرا که واکسیناسیون این بیماری به صورت مستمر در تمام نقاط کشور انجام می شود. علاوه بر واکسیناسیون روتین وزارت بهداشت علیه بیماری سرخک، واکسیناسیون اضافه بر سازمان نیز در صورت نیاز انجام می شود.

پدافند زیستی

زنگ خطر افزایش سرطان روده بزرگ در ایران

امیر صادقی، عضو هیات علمی دانشگاه علوم پزشکی شهید بهشتی، نسبت به شیوع در حال افزایش سرطان روده بزرگ در کشور هشدار داد. به گفته وی چنانچه جامعه هدف تحت برنامه های غربالگری قرار نگیرند، از هر ۲۰ نفر یک نفر مبتلا به سرطان روده بزرگ خواهد شد، ضمن اینکه سرطان روده بزرگ در افراد جوان زیر ۵۰ سال در حال افزایش است و این زنگ خطری برای جامعه محسوب می شود.

پدافند زیستی

ساخت تراشه تشخیص انواع گوشت حلال از حرام

استاد گروه زیست شناسی دانشگاه آزاد اسلامی واحد شهرکرد از ساخت تراشه تشخیص انواع گوشت حلال از حرام توسط محققان این واحد دانشگاهی خبر داد. با ساخت این دستگاه در یک واکنش واحد می توان همزمان گوشت هفت یا هشت حیوان مانند گاو، گوسفند، بز، شتر و حیوانات حرام گوشتی مانند گربه، سگ و خوک را تشخیص داد. این تراشه با فناوری نوین زیستی و مولکولی در مرکز زیست فناوری دانشگاه آزاد اسلامی شهرکرد طراحی شده است.

پدافند زیستی

سامانه پیش آگاهی هشدار در مورد بیماری زنگ زرد گندم

اکبر آهنگران، مدیرکل دفتر پیش آگاهی و کنترل عوامل خسارت زای سازمان حفظ نباتات کشور ضمن تاکید بر اهمیت مبارزه به موقع با بیماری زرنگ زرد گندم از کشاورزان خواست که به توصیه ها و دستورالعمل های کارشناسان و سازمان حفظ نباتات در این خصوص توجه کنند. به کارشناسان دفتر پیش آگاهی با مطالعه منابع علمی دنیا، مدلی را طراحی کرده‌اند که این مدل در سامانه پیش آگاهی سازمان حفظ نباتات بارگذاری شده و داده های مورد نیاز آن که همان داده‌های هواشناسی است توسط دستگاه های دیتالاگر که در مناطق کانونی زنگ زرد نصب شده‌اند به صورت آنلاین به سامانه پیش آگاهی ارسال می شود. این داده‌ها در داخل مدل می نشینند و مدل به صورت اتومات هرزمان که شرایط فراهم شود پیامکی را به مدیر استان و همکاران ما به صورت هشدار ارسال می کند که نشان می دهد، شرایط آب و هوایی برای بروز زنگ زرد گندم فراهم است. این هشدار زمان دقیق مبارزه را نشان می‌دهد. یعنی چند روز بعد هشدار، علائم بیماری در مزرعه‌ای که سمپاشی نشده باشد، مشاهده می‌شود.

پدافند زیستی

افزایش بروز آفت سن گندم در مزارع خراسان شمالی

محمد رضایی، مدیر حفظ نباتات سازمان جهاد کشاورزی خراسان شمالی از افزایش آفت سن گندم در مزارع این استان خبر داد. به گفته وی در حال حاضر تمام سن های گندمی که در اماکن زمستان گذران بوده اند وارد مزارع گندم و جوی استان شده است و با توجه به اینکه این بیماری خسارت های فراوانی را به محصول کشاورزی می کند تاکید داریم که کشاورزان حتما مزارع را سمپاشی کنند. از سوی دیگر مزراع استان هم اکنون با آفت زنگ زرد گندم نیز مواجه است که به کشاورزان توصیه شده تا مخلوطی از سم مبارزه با سن و زنگ زرد را در مزارع سمپاشی کنند.

انرژی

بررسی برنامه های طرح جامع پدافند غیرعامل جزیره خارک

نشست بررسی برنامه های طرح جامع پدافند غیرعامل جزیره خارک با هدف پایش وضع طرح ها و برنامه های طرح جامع پدافند غیرعامل جزیره خارک با حضور نقش آفرینان طرح شامل بخش شهری، نهادهای نظامی و انتظامی، شرکت های نفتی مستقر در جزیره و بیمارستان صنعت نفت خارک به میزبانی پایانه نفتی خارک به عنوان فرمانده ارشد پدافند غیرعامل و مدیریت بحران خارک برگزار شد که مدیران و نمایندگان پدافند غیرعامل هریک از ارگان ها به بحث و تبادل نظر پیرامون موضوعات مطرح شده پرداختند.




انرژی

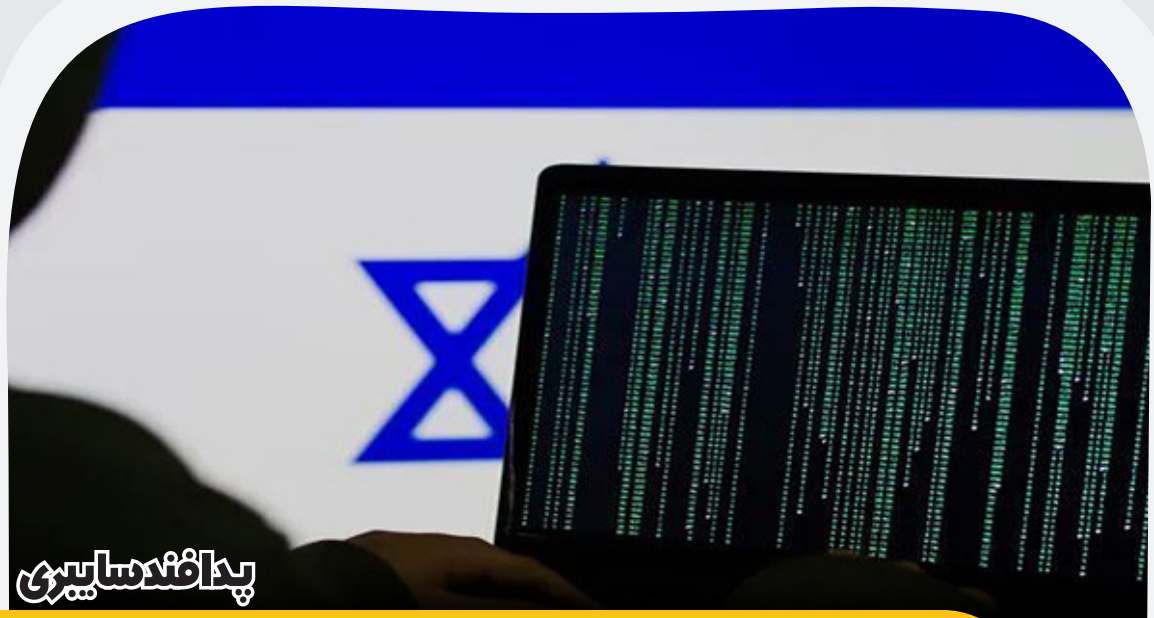
برگزاری مانور مدیریت شرایط اضطراری در بزرگترین اسکله نفتی کشور

عباس غریبی، فرمانده ارشد پدافند غیرعامل و مدیریت بحران جزیره خارگ از برگزاری موفق مانور پدافند غیرعامل مشترک به منظور مدیریت شرایط اضطراری و مدیریت بحران در بزرگترین اسکله نفتی کشور خبر داد. با این هدف و مطابق برنامه، مانورها و تمرین های سالیانه، تمرین عملی وقوع شرایط اضطراری برروی نفتکش در بزرگترین اسکله نفتی کشور با موفقیت انجام شد و نقاط قابل بهبود به منظور افزایش شاخص های عملکردی کشف و اقدامات اصلاحی لازم تعریف وصادر شد. در این مانور علاوه بر تمرین ارتباطات درون سازمانی در شرایط اضطراری، ارتباطات برون سازمانی با ارگان های مسؤول به عنوان یکی از مهم ترین شاخصه های کنترل هر چه موثرتر شرایط اضطراری تمرین و اجرا شد.

پدافند سایبری

نگرانی گوترش برای استفاده از هوش مصنوعی علیه غزه

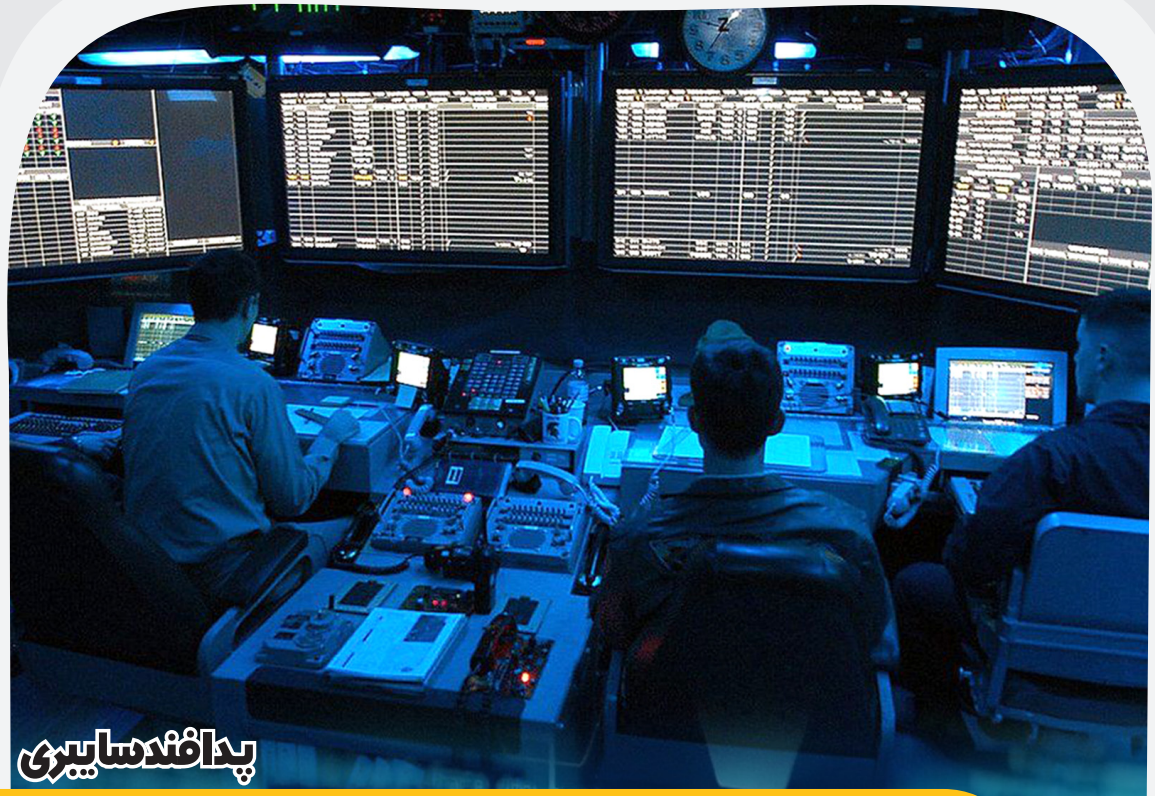
دبیرکل سازمان ملل گفت: از گزارش‌ها درباره استفاده ارتش رژیم صهیونیستی از هوش مصنوعی برای مشخص کردن اهداف نظامی که باعث مرگ بیشتر غیرنظامیان می‌شود «عمیقاً نگران» هستم. هوش مصنوعی بایستی به عنوان «نیرویی در جهت خیر» و منافع دنیا مورد استفاده قرار بگیرد و نباید به «جنگ‌افروزی در سطح صنعتی و کتمان مسئولیت‌پذیری» کمک کند. یک مجله انگلیسی‌زبان فاش کرده بود ارتش رژیم صهیونیستی با بهره‌گیری از هوش مصنوعی بانک اهداف غیرنظامی را افزایش می‌دهد.



پدافند سایبری

رژیم صهیونیستی زیر تیغ حملات سایبری

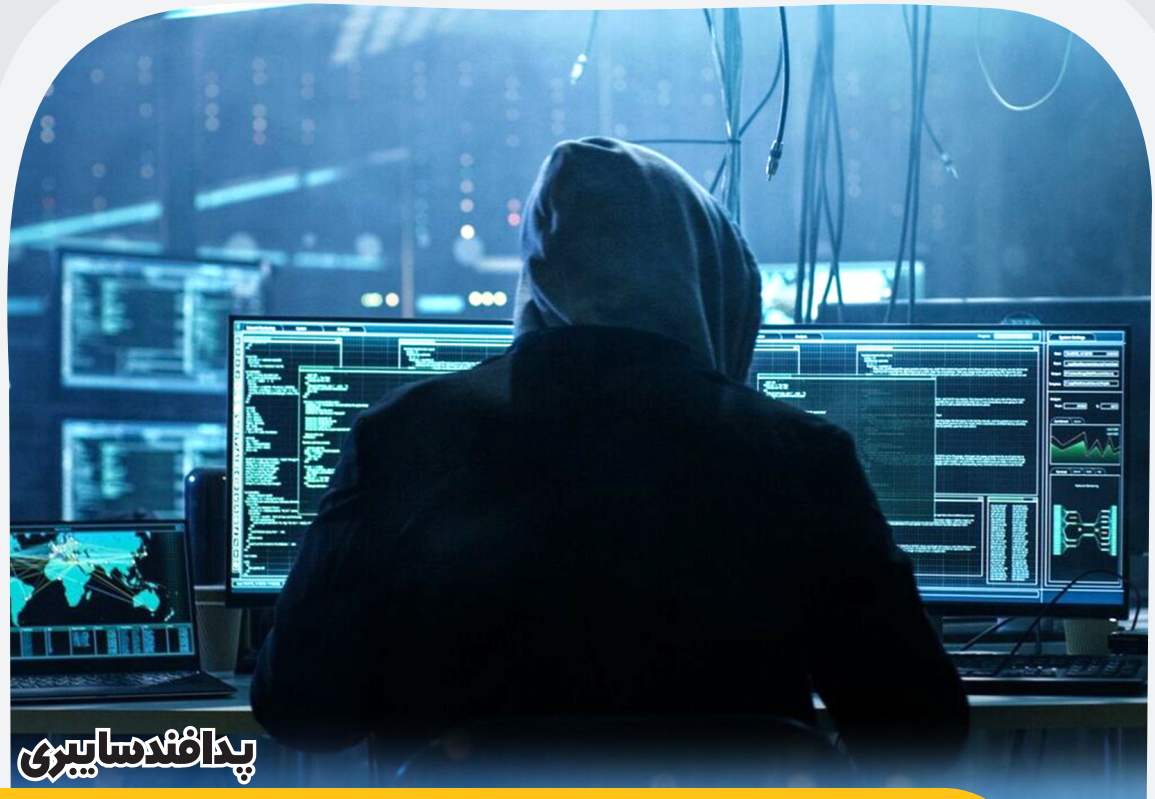
اداره سایبری ملی رژیم صهیونیستی در گزارشی معترف شد این رژیم از زمان آغاز عملیات طوفان الاقصی در هفتم اکتبر تا پایان سال ۲۰۲۳، بیش از ۳ هزار حمله سایبری را تجربه کرده که ۸۰۰ مورد آن، پتانسیل قابل توجهی در وارد کردن آسیب داشته است. در این گزارش آمده است: وقوع ۳۳۸۰ حمله سایبری از هفتم اکتبر تا پایان سال ۲۰۲۳، افزایش دو و نیم برابری حملات سایبری نسبت به مدت مشابه سال قبل را نشان می دهد. جنگ در غزه، افزایش حملات سایبری را به همراه داشته که به تدریج شدت گرفته اند و از تمرکز به سرقت اطلاعات، به حملات مختل کننده و آسیب رسان، تغییر یافته اند. در آغاز جنگ، این حملات ساده و غیرپیشرفته بوده و هدف آنها، ایجاد بی نظمی عمومی بود، اما به تدریج، متمرکزتر شده و به شکل موثرتری، فعالیت سازمان های رژیم غاصب را مختل کرده اند. این حملات، نهادهای حیاتی را هدف گرفته اند و با هدف قرار دادن شرکت های مهم در زنجیره تامین بسیاری از سازمان ها، به دنبال اثرگذاری عمیق تری بوده اند.



پدافند سایبری

حملهٔ سایبری به ادارهٔ ملی توزیع برق اسرائیل

گروه انتقام جویان سایبری مسئولیت قطع برق در نقاط مختلف سرزمین های اشغالی از جمله شهرهای بیت شمش، تل آویو، روش هاعین، آراد، مودیعین، بئرشوع، نتانیا و... را برعهده گرفت. این گروه در پیامی اعلام کرده است: «در پاسخ به جنایات رژیم صهیونیستی، زیرساخت های توزیع برق را از شمال تا جنوب سرزمین های اشغالی به صورت مکرر هدف حملات سایبری قرار دادیم. مقامات اسرائیل که همواره بازیاده گویی از امنیت سایبری نفوذناپذیردم می زنند، حتی توان تشخیص حملات را نداشته و در پاسخ به مطالبه گری ساکنان غاصب، نقص فنی را علت این رخ دادها بیان می کنند، درحالی که کنترل تمامی زیرساخت های برق آن ها در دستان ماست. ما پاسخ های متنوعی در حوزه سایبری علیه منافع و زیرساخت های حیاتی رژیم صهیونیستی آماده کرده ایم»



پدافند سایبری

حمله هکری به وزارت جنگ رژیم صهیونیستی

روزنامه «اسرائیل هیوم» گزارش داد که یک گروه هکری چند روز پیش اعلام کرد به رایانه های وزارت جنگ رژیم صهیونیستی نفوذ کرده و توانسته اطلاعات حساسی را به دست بیاورد و این داده ها را در چند گروه در پیام رسان تلگرام منتشر کرده است. گروه هکری مسئول این حمله تاکید کرد موفق به سرقت داده هایی گسترده و حساس از سامانه های رایانه ای وزارت جنگ رژیم صهیونیستی شده است. این گروه ناشناس که در گزارش مذکور اطلاعات بیشتری از آن منتشر نشده، در پیام رسان تلگرام در ویدیویی نشان داد چگونه توانسته چندین سامانه وزارت جنگ رژیم صهیونیستی را هک کرده و به اطلاعاتی که داخل آنها بوده دسترسی پیدا کند.

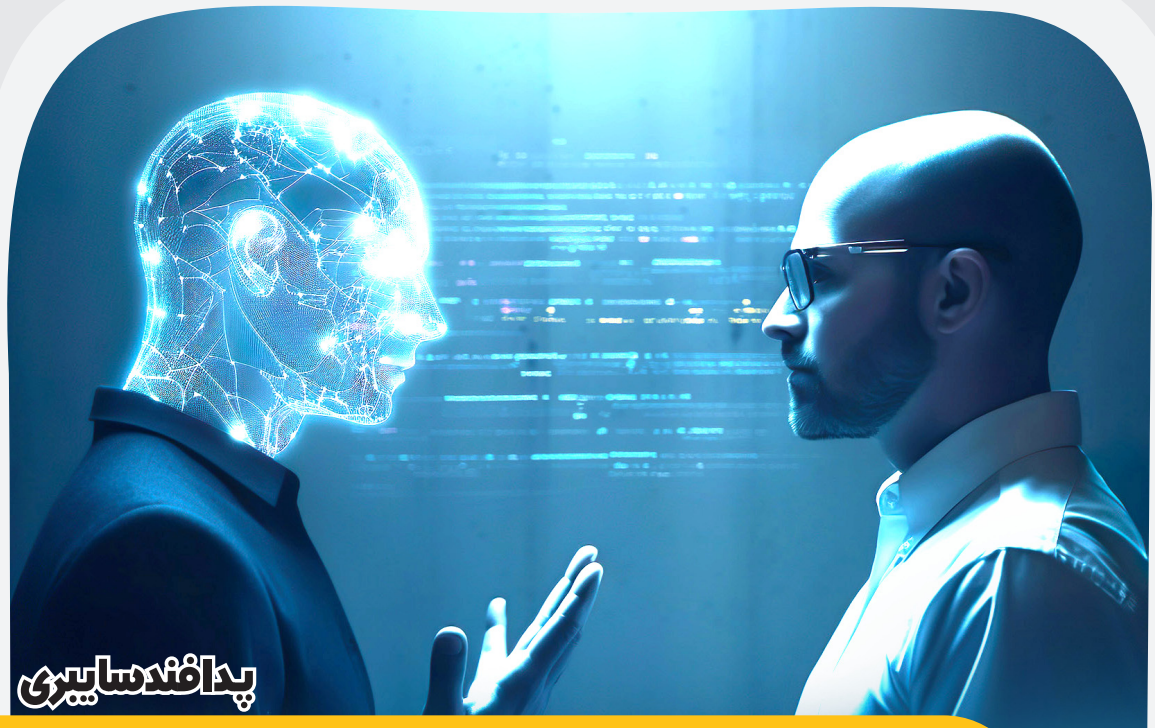
پدافند سایبری

FBI در استفاده از هوش مصنوعی چه اهدافی دارد؟

جاناتان لنزنر، رئیس بخش کارکنان اداره تحقیقات فدرال آمریکا، اخیراً طی اظهار نظری در این خصوص، اساسی ترین محورهای دیدگاه این آژانس در مورد هوش مصنوعی را چنین برشمرد:

۱- پیش روی فعالانه در برابر تهدیدها ۲- محافظت از نوآوری ایالات متحده ۳- ایجاد یک چارچوب حکمرانی اخلاقی بر این فناوری

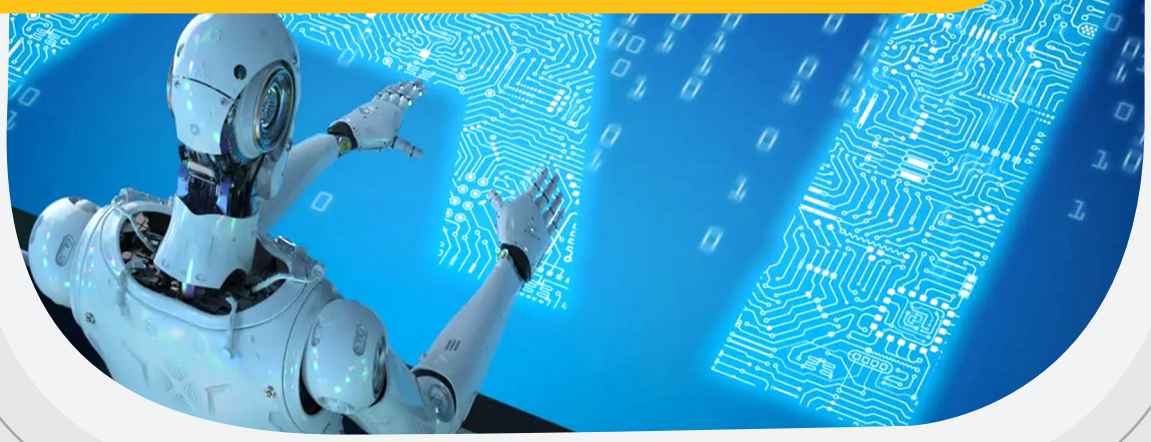
اداره تحقیقات فدرال آمریکا علاوه بر ابزارهای تجاری، از ابزارهای یادگیری ماشینی خود برای استفاده از هوش مصنوعی در جنبه های مختلف عملیات خود استفاده می کند. با این حال، هنگامی که صحبت از هوش مصنوعی مولد و مدل های زبان بزرگ به میان آید، این سازمان بیشتر یک کاربر است تا توسعه دهنده فناوری. این نهاد امنیتی همچنین فرآیند دقیقی را برای ارزیابی استفاده اخلاقی از هوش مصنوعی ایجاد کرده است که شامل ارزیابی هدف، مزایا، خطرات، کنترل های حریم خصوصی، نظارت، حسابرسی و تشخیص خطا می شود. FBI قصد دارد ساختار حکمرانی خود را با جامعه اطلاعاتی هماهنگ کند. همکاری با آژانس های دیگر جنبه دیگری از استفاده اداره تحقیقات فدرال آمریکا از هوش مصنوعی است.



پدافند سایبری

مجازات برای سواستفاده از هوش مصنوعی در ایتالیا سنگین می شود

براساس پیش نویس یک لایحه قانونی، دولت ایتالیا در حال بررسی مجازات های سخت تر برای جرائم با استفاده از ابزارهای هوش مصنوعی (AI) از جمله تقلب در بازار و پولشویی است. این لایحه ۲۵ صفحه‌ای اصول اولیه درباره تحقیقات، آزمایش، توسعه، به کارگیری و انطباق هوش مصنوعی در ایتالیا است تا با تأثیر این فناوری بر حقوق اساسی و ریسک های اقتصادی و اجتماعی مرتبط مقابله کند.



پدافند سایبری

موافقت کنگره آمریکا با قانون حفظ حریم خصوصی داده ها

دو قانون گذار کلیدی ایالات متحده اعلام کردند که بر سر پیش نویس قانون حفظ حریم خصوصی داده های دو حزبی به توافق رسیده اند که جمع آوری داده های مصرف کنندگان توسط شرکت های فناوری را محدود می کند و به آمریکایی ها این قدرت را می دهد تا از فروش اطلاعات شخصی جلوگیری کنند یا آنها را مجبور به حذف کنند. قانونگذاران در بیانیه ای مشترک، گفتند که این طرح به کمیسیون تجارت فدرال و دادستان های کل ایالت اختیارات گسترده ای را برای نظارت بر مسائل حریم خصوصی مصرف کنندگان و ایجاد مکانیسم های اجرایی قوی برای پاسخگویی به متخلفان، از جمله حق اقدام خصوصی را به افراد می دهد. این لایحه تبلیغات هدفمند را ممنوع نمی کند، اما به مصرف کنندگان این امکان را می دهد که از آن انصراف دهند. در همین راستا کمیسیون فدرال تجارت یک دفتر جدید متمرکز بر حریم خصوصی ایجاد خواهد کرد که می تواند جریمه هایی را برای نقض حریم خصوصی صادر کند که شرکت های مخابراتی را نیز پوشش می دهد.

پدافند سایبری

هوش مصنوعی و طغیان واقعی!

در کشورها هنوز برای هوش مصنوعی قانون رسمی وجود ندارد، ولی دولت ها می گویند که مسائل مربوط به کارکرد آن باید در قوانین موجود گنجانده شوند. به نظر می رسد سرعت تحولات ناشی از ایجاد و ارتقای ابزارها و مجاری مربوط به هوش مصنوعی به مراتب نسبت به سرعت تدوین قوانین و قواعد ثابت و متغیر در این خصوص بالاتر است! همین مسئله در آینده ای نزدیک چالش هایی را برای بشریت تولید خواهد کرد. زمانی که سرعت رشد تکنولوژی نسبت به سرعت ایجاد زیرساخت های قانونی و حقوقی آن بیشتر شود، این بحران گریبان گیر ملت های دنیا خواهد شد. این مسئله را در قبال فضای مجازی و شکل گیری شبکه های اجتماعی (خصوصا در حوزه نقض حریم خصوصی افراد و سازمان ها) مشاهده کردیم: جایی که حریم افراد نقض می شد و قانونی برای دفاع از آن ها وجود نداشت!

در این میان هوش مصنوعی به مراتب نسبت به شکل گیری شبکه های اجتماعی حساسیت بیشتری دارد، زیرا امکان استفاده از ابزارهای جعلی و دروغین در عرصه هوش مصنوعی به مراتب نسبت به شبکه های اجتماعی بیشتر است. تولید صداها و تصاویر مربوط به یک شخص حقوقی یا حقیقی (آن هم با کیفیتی واقعی)، یکی از این آسیب هاست: جایی که فرد یا سازمان آسیب دیده دقیقا نمی داند باید از چه کسی و به کجا شکایت کند و فراتر از آن، کدام ماده و تبصره قانونی حامی وی در این گردش کار قضایی خواهد بود!

پدافند سایبری

بحران داده برای آموزش هوش مصنوعی در راه است

دو رسانه آمریکایی، وال استریت ژورنال و نیویورک تایمز، گزارش داده اند که شرکت های توسعه دهنده هوش مصنوعی مانند اُپن ای آی در یافتن داده های باکیفیت برای آموزش مدل های خود با مشکلاتی مواجه شده اند و در این میان اُپن ای آی در اقدامی غیرقانونی از محتوای یوتیوب استفاده کرده است، اما گرِگ براکمن (Greg Brockman)، رئیس اُپن ای آی که شخصاً در گردآوری ویدیوها شرکت داشته است ادعا می کند که رویکردش در استفاده از ویدیوهای یوتیوب منصفانه بوده است. براساس گزارش های نیویورک تایمز، شرکت متا نیز به دلیل کمبود داده های خوب برای آموزش فناوری هوش مصنوعی خود با چالش هایی مواجه شده است. مذاکرات تیم هوش مصنوعی این شرکت برای استفاده از محتوای دارای حق نشر هنوز به نتیجه نرسیده است. متا برای بهبود داده های خود، از پرداخت هزینه های حق نشر کتاب تا حتی خرید ناشرهای بزرگ پیش رفته است. با این حال، متا همچنان به دلیل تغییرات مربوط به حریم خصوصی در نحوه استفاده از داده های کاربران با محدودیت هایی روبه رو است.

پدافند سایبری

قدرتمندترین سرور داده به ایستگاه فضایی می رود

قدرتمندترین سرور در مدار با امکان ذخیره سازی ۱۰۰ ترابایت داده به ایستگاه فضایی بین المللی پرتاب می شود. این سرور داده قدرتمند توسط شرکت اسپیس بیلت تولید شده و با همکاری شرکت فیزون که یکی از شرکت های معتبر تولید کننده حافظه های فلش و قطعات الکترونیکی است، به ایستگاه فضایی ارسال می شود. این سرور قادر به پردازش و ذخیره انواع مختلف داده ها از جمله تصاویر فضایی، اطلاعات علمی و داده های ارتباطی برای ایستگاه فضایی بین المللی است.

پدافندسایبری

چالش اخبار جعلی در عصر هوش مصنوعی

باگسترش انقلاب هوش مصنوعی، تقلبی های مجهزبه هوش مصنوعی نیزگسترش خواهند یافت. این موضوع امری اجتناب ناپذیر است، اما می توان آن را مدیریت کرد تا زمانی که مصرف کنندگان و تولیدکنندگان تنظیمات قابل توجهی در نحوه استفاده از اینترنت انجام دهند.

فناوری تشخیص تقلب هوش مصنوعی تکامل یافته و بهبود خواهد یافت. با این حال، حتی با فرض کارکرد ردیاب های جعلی، سایت های خبری اصلی با رقابت بیشتری روبرو خواهند شد. سایت های جایگزین محتوای خود را جعل می کنند و پیچ وتاب هایی اضافه می کنند که گاهی توسط دولت های خارجی حمایت می شوند. برخی از موثرترین رسانه ها ممکن است ۹۸ درصد مشروع باشند، اما نرخ تقلبی ۲ درصد در برخی ابعاد حیاتی، مانند پوشش جنگ های خارجی یا رسوایی های شخصی وحشیانه، می تواند قابل توجه باشد. خبر بد این است که خبرنگاران باید سخت تر کار کنند. خبر خوب خبری است که در نهایت مشترکان و خوانندگان خود را باهوش تر و آگاه تر کند. از این رو مسابقه ای که رسانه ها باید در آن پیروز شوند، حرکت به سمت کیفیتی هرچه بالاتر است.

پدافند زیستی

ساخت ابزاری برای تشخیص سریع و دقیق ویروس ها

همه گیری کرونا موجب شد تا نیاز به آزمایش سریع و قابل اعتماد بیماری های عفونی بیشتر احساس شود. بیشتر آزمایش هایی که امروزه انجام می شود شامل واکنش های آنتی ژن-آنتی بادی است. گروهی از محققان با استفاده از ذرات پلیمری کامپوزیتی که با نانوذرات طلا تزئین شده اند، ابزار دقیق تری برای آزمایش بیماری های عفونی ابداع کرده اند. در این روش ها پروب های فلورسانس، یا ذرات رنگی به آنتی بادی ها متصل می شوند. هنگامی که آنتی بادی ها به ویروس می چسبند، این کاوشگرها حضور ویروس را تشخیص می دهند. استفاده از نانوذرات رنگی به دلیل امکان مشاهده آن ها و همچنین سهولت اجرا، بسیار مورد توجه است به ویژه این که نیاز به تجهیزات زیادی ندارند.

پدافند شهری

اختصاص ۳۶ میلیون دلار برای ساخت پناهگاه و دفاع مدنی از سوی دولت سوئد

دولت سوئد به تازگی اعلام کرده است که ۲۸۵ میلیون کرون (۳۶ میلیون دلار) برای تقویت پناهگاه ها، خدمات اضطراری و دفاع غیرنظامیان خود سرمایه گذاری می کند. کارل اسکار بولین، وزیر دفاع (غیرنظامی) با اشاره به اینکه سوئد ماه گذشته به ناتو پیوست گفت: از این بودجه برای تقویت توانایی خدمات نجات در زمان درگیری، تقویت امنیت سایبری و کمک به سیستم بهداشتی برای انباشت دارو استفاده خواهد شد. همچنین بودجه‌ای برای بازسازی پناهگاه ها، تامین آب آشامیدنی و زیرساخت های حمل و نقل اختصاص داده خواهد شد. طبق گزارش خبرگزاری تی تی، بودجه دفاع غیرنظامی سوئد برای سال ۲۰۲۴ به ۶,۵ میلیارد کرون می رسد با این حال، سازمان امور مدنی سوئد در اکتبر اعلام کرد که براین باور است بودجه سالانه ۲۰ میلیارد کرون برای پاسخگویی به نیازها لازم است.

گزارش تحلیلی

کشورها برای مقابله با خطرات شبکه های اجتماعی چه می کنند؟

توسعه و بالا رفتن میزان استفاده از شبکه های اجتماعی موضوعی است که در چند سال اخیر کشورها را وادار به وضع قوانین و حتی ممنوعیت استفاده از شبکه ها در شرایط خاص کرده است. در بیشتر موارد این نگرانی به خارجی بودن شبکه های اجتماعی در کشورها مربوط می شود، چرا که داده های کاربران عضو در شبکه های اجتماعی در پایگاه های داده آن شبکه و در کشور تأسیس کننده آن شبکه ذخیره می شود و به این ترتیب یک کشور به طور کامل به اطلاعات کاربران سایر کشورها دسترسی کامل خواهد داشت و این موضوع برای تمامی کشورها نگران کننده و خطرناک است.

اما موضوع به اینجا ختم نمی شود، جدا از اطلاعات کاربران، به واسطه همه گیری شبکه های اجتماعی در بین کاربران، شرکت تأسیس کننده شبکه به سادگی می تواند از یک فرد یا کشور برای اهداف خود جاسوسی کند و به این دلیل بسیاری از کشورها شبکه های اجتماعی را از سلاح های نظامی خطرناک تر می دانند.

این موارد از اصلی ترین دلایلی است که کشورها را ملزم به وضع چارچوب برای شبکه های اجتماعی می کند تا از خطرات احتمالی در برابر جامعه یک کشور جلوگیری شود. قوانین که کشورها برای کنترل فضای مجازی به تصویب رسانده اند در بسیاری از موارد تبدیل پذیر بوده و یک موضوع خاص را شامل نمی شوند. برای مثال در زمان انتشار ویروس کرونا در جهان انتشار اخبار غلط درباره واکسن این بیماری و همچنین میزان سرایت آن در جهان در فضای مجازی منتشر می شد که باعث سردرگمی افراد می شد و دولت ها به طور مستقیم نگرانی خود را به شبکه های اجتماعی اعلام کردند که نتیجه آن برچسب گذاری روی این نوع محتوا بود.

در بسیاری از موارد شبکه های اجتماعی مشهور زیر بار اعتراضات دولت ها نمی روند و تقاضای دولت ها در رابطه مسدود کردن یک موضوع یا جلوگیری از اطلاعات خاص را نقض آزادی بیان می دانند و به این ترتیب کشوری که به خواست خود از شبکه اجتماعی دست پیدا نمی کند تصمیم به فیلتر و مسدودسازی آن وب سایت می گیرد. این موضوع تاکنون در بسیاری از کشورها اتفاق افتاده و در حال حاضر تمام شبکه های اجتماعی در دسترس تمام کاربران اینترنت قرار ندارد. در ادامه برخی از کشورهایی که برای کنترل امنیت خود تصمیم به مسدود کردن شبکه های اجتماعی گرفتند را مرور می کنیم:

چین

در کشور چین بسیاری از شبکه های اجتماعی از دسترس کاربران چینی خارج هستند، برای مثال کاربران چینی نمی‌توانند از رسانه های اجتماعی غربی استفاده کنند و در این کشور استفاده از سرویس های تغییر آی پی مانند فیلترشکن به طور کامل در ممنوع است. کاربران چینی به واسطه قوانین سختگیرانه‌ای که در این کشور لحاظ شده است صرفا توانایی استفاده از شبکه های اجتماعی بومی این کشور مانند وی چت و شبکه های اجتماعی پیرو قوانین فضای مجازی این کشور مانند «تیک تاک» و «دوئین» رادارند.

روسیه

روسیه قوانین بسیار سخت گیرانه‌ای برای کنترل فضای مجازی خود به تصویب رسانده و عملا مردم این کشور از شبکه های اجتماعی بین المللی استفاده نمی کنند و دولت روسیه نیز استفاده از فیلترشکن در این کشورها را به طور کامل ممنوع اعلام کرده است. جدا از این روسیه برای نظارت بر محتوای سیاسی منتشر شده در فضای مجازی استفاده از شبکه های اجتماعی و پیامرسان های واتساپ، اینستاگرام، فیسبوک، دیسکورد، اسکایپ بیزینس، اسنپ چت، تلگرام را ممنوع اعلام کرده است. در عوض کاربران روسی از شبکه های اجتماعی بومی این کشور که بر اساس قوانین سایبری روسیه فعالیت می کنند، استفاده می کنند که مشهورترین آن ها «روس گرام» (Rossgram) و (Vkontakte) است.

امارات

در امارات نیز استفاده از نرم افزارهای دارای تماس تلفنی اینترنتی ممنوع است و این کشور قابلیت مکالمه در واتساپ و اسنپ چت را مسدود کرده است. علاوه بر این کاربران آیفون نیز در این کشور امکان مکالمه تصویری و صوتی بافیس تایم را ندارند.

هند

هند به دلیل جمعیت بالای خود بخش عمده‌ای از کاربران شبکه ها اجتماعی را به خود اختصاص داده است و دولت هند به شرکت ها دستور داده تا داده افرادی که از فیلترشکن استفاده می کنند را جمع آوری کرده و به دولت تحویل دهند. علاوه بر این در هند بر تمامی فعالیت های آنلاین کاربران نظارت می شود و استفاده از شبکه های اجتماعی چینی نظیر وی چت و تیک تاک ممنوع است.

آمریکا

در این قاره نیز محدودیت های بالایی برای استفاده از شبکه های اجتماعی چینی نظیر تیک تاک اعمال شده است و این موضوع شامل کانادا و مکزیک نیز می شود. چندی پیش نیز اعلام شد که کنگره آمریکا با ممنوعیت استفاده از تیک تاک در سازمان های فدرال این کشور موافقت کرده است و اجازه نصب یا استفاده از تیک تاک در هیچ کدام از نهادهای فدرال آمریکا وجود ندارد. کنگره آمریکا بر این باور است که تیک تاک ساخت دولت چین است و ابزاری بسیار قدرتمند برای جاسوسی از دولت آمریکا به شمار می رود.

اسپانیا

در اسپانیا به طور خاص برای شبکه اجتماعی مشخصی محدودیت اعمال نشده است، اما این کشور به طور کامل تابع قوانین اتحادیه اروپا بوده و جدا از آن با شبکه های اجتماعی که امنیت سایبری و حریم خصوصی کاربران این کشور را زیر پا بگذارند مقابله خواهد کرد. برای مثال این کشور اخیراً استفاده از تلگرام را ممنوع و آن را فیلتر کرده است، چرا که شرکت های رسانه ای از آپلود محتوای آن ها بدون اجازه و هماهنگی با آن ها به دادگاه عالی اسپانیا شکایت کرده اند و دادگاه این کشور استفاده از تلگرام را تا زمان روشن شدن موضوع ممنوع اعلام کرده است.

خبر

پشت پرده ارسال یک پیامک جعلی از طرف پدافند غیرعامل

نخستین جلسه وبینار شورای مدیران کل پدافند غیرعامل استان ها در سال ۱۴۰۳ با حضور سردار محمدعلی قمی؛ معاون بسیج و امور استانهای سازمان پدافند غیرعامل کشور و دکتر آرش قندچی؛ معاون امور شهری این سازمان در وزارت کشور برگزار شد. سردار محمدعلی قمی معاون بسیج و امور استان های سازمان پدافند غیرعامل کشور در این جلسه با اشاره به پیامک جعلی که از طرف این سازمان به شهروندان کشور ارسال شده بود، گفت: ارسال پیامک جعلی از طرف سازمان پدافند غیرعامل با هدف ایجاد اغتشاش در افکار عمومی، گرچه با آگاهی و بصیرت شهروندان عزیز کشورمان بی اثر شد، اما نشان از جایگاه سازمان پدافند غیرعامل کشور به عنوان مرجعی قابل اتکا در میان مردم دارد. وی در ادامه با اشاره به پیشرفت هایی که به خصوص با توجه به قانون و اساسنامه جدید در این سازمان صورت گرفته است، افزود: به طور قطع هم اکنون فرصت مغتنمی در استفاده از ظرفیت های این سازمان وجود دارد و باید از این ظرفیت ها به نحو احسن استفاده شود. سردار قمی با اشاره به جایگاه استانها به عنوان لایه دوم پدافند غیرعامل کشور، نقش آنها به خصوص ادارات کل استانها را در انجام ماموریت های سازمان حیاتی توصیف کرد. در این جلسه دکتر آرش قندچی معاون امور شهری و کلانشهرهای سازمان پدافند غیرعامل کشور نیز با اشاره به همپوشانی های زیادی که بین فعالیت امور استانها و امور شهری سازمان پدافند غیر عامل وجود دارد عنوان کرد: به نتیجه رسیدن ماموریت های سازمان در صورت هم افزایی بخش ها و سطوح مختلف این سازمان امکانپذیراست. وی با اشاره به طرح های توسعه در شهرهای مختلف کشور به خصوص حاشیه خلیج فارس، توسعه متوازن را استراتژی اصلی این طرح ها عنوان کرد و افزود: سازمان پدافند غیر عامل در طرح های توسعه شهرها نگاه جامعی را در توسعه شهر، استان و منطقه در نظر دارد.

خبر

سرپرست پدافند غیرعامل هلال احمر منصوب شد

دکتر پیرحسین کولیوند، رئیس جمعیت هلال احمر در حکمی سرپرست ستاد پدافند غیر عامل این جمعیت را منصوب کرد.

در بخشی از این حکم خطاب به «مرتضی مرادی پور سرپرست ستاد پدافند غیرعامل هلال احمر» آمده است: « با عنایت به زمینه وجود تهدیدات بالقوه و خطرات طبیعی و غیر طبیعی و با توجه به ضرورت دفاع و مقابله کامل به منظور کاهش آسیب پذیری از جنابعالی انتظار دارم ضمن بهره مندی از پتانسیل های درون سازمانی و برون سازمانی و با پایبندی به اصول و معیارهای پدافند غیر عامل تمام همت و توان اجرایی خویش را در راستای تکمیل زنجیره دفاعی کشور تقویت و ارتقاء سطح آمادگی نیروی انسانی ، توسعه تجهیزات و مقاوم سازی اماکن جهت مواقع بحرانی به کار گیرید.

امیداست با استعانت از خداوند متعال در جهت رسیدن به اهداف ماندگار جمعیت هلال احمر جمهوری اسلامی ایران گام های اساسی برداشته و با فصل الخطاب قرار دادن منویات مقام معظم رهبری (مدظله العالی) به ویژه بیانیه گام دوم انقلاب اسلامی در سایه همدلی هم افزایی و همراهی مدیران و همچنین استفاده حداکثری از ظرفیت های موجود در سازمان پدافند غیر عامل و انجام وظایف پیروز و سربلند باشید.»

یادداشت

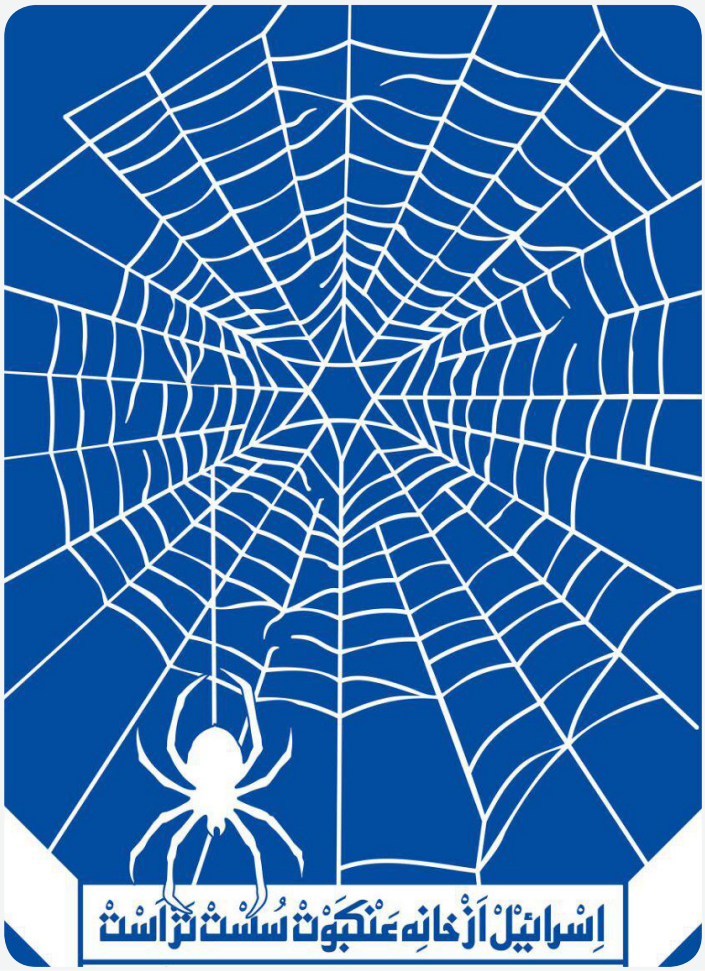
نفوذ سایبری به لانه عنکبوت!

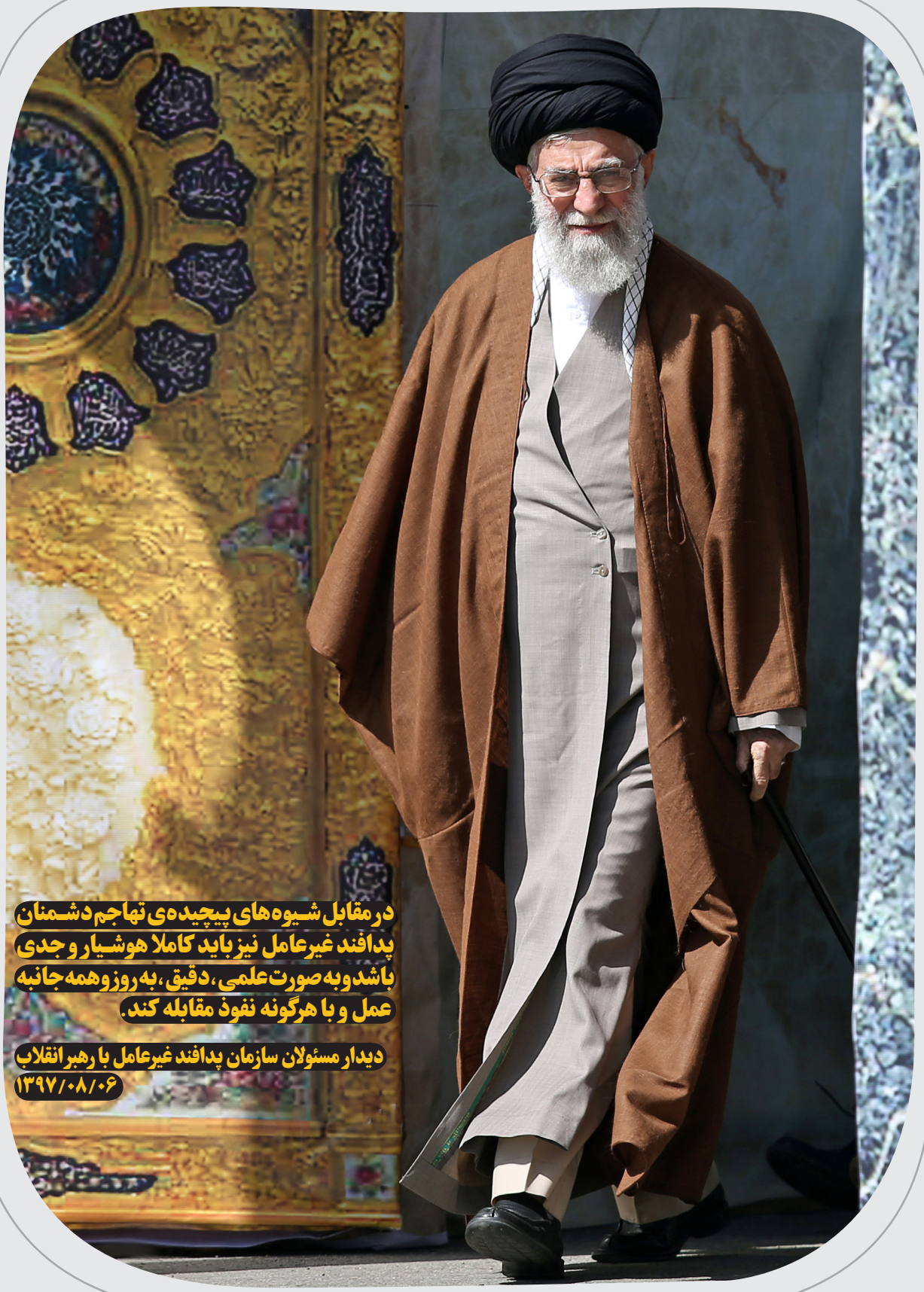
محمد اسکندری

رژیم صهیونیستی در سال های اخیر تلاش داشته است تا با استفاده از فناوری ها و تسلیحات وارداتی از امریکا و دیگر کشورهای غربی، خود را به عنوان یک «قدرت منطقه ای» در جنوب غرب آسیا تحکیم نماید. این رژیم تلاش داشته است تا در کنار ابعاد چندگانه نظامی همچون هوایی، زمینی و دریایی در بعد سایبری نیز خود را به عنوان یک قدرت بلامنازع مطرح کند. با این حال اخبار و گزارش های واصله در هفته های اخیر از این رژیم نشان می دهد که گویا «چتر پدافند سایبری» این رژیم وضعیت بسیار آشفته ای دارد و آنچه از قدرت سایبری رژیم صهیونیستی (آفند و پدافند) پیش تر مطرح شده با چاشنی رسانه ای بیش از حد همراه بوده است! بر اساس آمارها و گزارش های یک شرکت صهیونیستی امنیت داده، حملات سایبری علیه رژیم صهیونیستی از زمان آغاز نبرد «طوفان الاقصی» رشد ۵۲ درصدی داشته است. به اذعان کارشناسان این حملات نیز اغلب موفقیت آمیز بوده و توانسته اند کارکرد زیرساخت های این رژیم را دچار اختلال کنند. البته رژیم صهیونیستی به دلیل وضعیت آشفته داخلی، بشدت در تلاش است تا پیامدهای این حملات رسانه ای نشود. حملات سایبری می توانند در طیف های مختلف و با پیامدهای متفاوتی باشند. این حمله ها می توانند از جنس حملات ساده مثل حملات (DoS) و یا (DDoS) باشند و یا اینکه حملاتی با استفاده از بدافزارها باشند که به درون سامانه ها یا زیرساخت ها نفوذ کرده و منجر به بروز اختلال های جدی در خدمت و یا حتی بروز بحران شوند. برای مثال حمله سایبری امریکا به زیرساخت های هسته ای کشورمان با استفاده از بدافزار استاکس نت (Stuxnet) یکی از پیشرفته ترین حملات سایبری در نوع خود بود؛ حمله ای که در صورت مهار نشدن پیامدهای آن می توانست یک مخاطره جدی در تأسیسات هسته ای ایران پدید آورد! اما مسأله نفوذ هکرها به وزارت جنگ رژیم صهیونیستی نیز از آن دست رخدادهای سایبری است که نمی توان به راحتی از آن عبور کرد. اساساً در الگوی پدافند سایبری، در گام نخست همه دولت ها اقدام به دارایی شناسی کرده و سپس بر اساس اطلس به دست آمده الزامات و ملاحظات امنیت و پدافند سایبری را در زیرساخت ها و دارایی های خود اعمال می کنند. در نظام طبقه بندی دارایی ها و زیرساخت ها، سامانه های راهبری و نظارت بر تسلیحات نظامی جزو با اهمیت ترین دارایی ها محسوب می شوند چرا که نفوذ به این سامانه ها می تواند امنیت داخلی و حتی امنیت بین الملل را به مخاطره بیندازد. به زبان ساده تر دولت ها هر آنچه در توان دارند در عرصه سایبری برای حفاظت از سامانه های وزارتخانه جنگ و دفاع خود می گذارند و اینکه رژیم صهیونیستی اعتراف به هک سامانه های مربوط به وزارت جنگ خود کرده است به این معناست که در عمل سایر سامانه های این رژیم نیز آسیب پذیر است و می تواند در دسترس هکرها باشد! چندی پیش گروه هکری با نام «Nethunter» از حمله سایبری به وزارت جنگ رژیم صهیونیستی خبر داد و با انتشار اسناد و اطلاعاتی،

اعلام کرد که موفق شده به سامانه های وزارت جنگ رژیم صهیونیستی نفوذ و به زیرساخت های آن دسترسی پیدا کند. این گروه هکری اسناد دست یافته از وزارت جنگ رژیم صهیونیستی را در کانال تلگرامی خود قرار داده و تأکید کرده به اسناد محرمانه این وزارتخانه از جمله برخی نقشه های ساخت ابزارهای سلاح جنگی و قطعات تجهیزات نظامی و حتی اسناد مرتبط با سامانه پدافندی گنبد آهنین دست یافته است! این گروه هکری اعلام کرده هک وبسایت وزارت جنگ (رژیم) اسرائیل و انتشار بخشی از اسناد آنها پاسخی به بخشی از جنایات رژیم صهیونیستی در جنگ غزه است. منابع امنیتی رژیم صهیونیستی نیز در گفت‌وگو با روزنامه اسرائیل هیوم تأیید کردند که نقص امنیتی سیستم های وزارت جنگ موجب نفوذ هکرها شده ولی مشخص نکردند که چه نوع اطلاعاتی به سرقت رفته است.

در نهایت باید گفت وجود آسیب پذیری های گسترده در نظام پدافند سایبری رژیم صهیونیستی می تواند اثرات قابل توجهی بر کارآمدی ماشین جنگی این رژیم بویژه در بزنگاه ها داشته باشد. اساساً فضای سایبری امروز به زیرساخت همه زیرساخت ها تبدیل شده است و اگر دولت ها نتوانند از زیرساخت های با اهمیت بالای خود حفاظت کنند عملاً دچار اختلال در کارکردهای حیاتی خود می شوند.





در مقابل شیوه‌های پیچیده‌ی تهاجم دشمنان پدافند غیرعامل نیز باید کاملا 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