نسل چهارم

ماهنامه فناوری های نوین
اطلاعات و ارتباطات
فارسی - انگلیسی ۲۰۰۰۰۰ تومان

سال دهم
تیر ۱۴۰۴
شماره ۱۱۸

آسیب پذیری زیرساخت های ارتباطی در برابر حملات سایبری؛ ضرورت حرکت به سمت رویکردهای اصلاحی

همراه اول
mci Mobile Communications of Iran

سیم پوز، یک ارتباط پایدار

سیم‌کارتی جدید به نام شخص (پذیرنده) جهت اتصال پایانه‌های سیار به شبکه PSP بدون استفاده و وابستگی به اینترنت

طرح ویژه فروش عمده
مودم‌های اینترنت LTE مبین‌نت

امکان پرداخت اقساطی بدون سود و پیش‌پرداخت
با تخفیف ویژه شـرکت‌ها و سازمان‌ها

- انواع مودم‌هـای پرسرعت رومـیزی و جیـبی
- بدون نیاز به خط تلفن و با قابلیت جابه‌جایی

مبین‌نت

مبین‌نت؛ پیشرو در مسیر سبز تحول دیجیتال

۰۲۱ - ۸۳۸۶۹۳۴۷

PAYACO

صنایع ارتباطی پایا

چهل سال طراحی و تولید



سامانه تصویربرداری
موج میلی متری


ارائه سرویس های **VoIP** ابری و راهکار شبکه های
نسل جدید **NGN** و مبتنی بر معماری **IMS**


محصولات و راه حل های هوشمندسازی در حوزه پارکینگ،
آسانسور، تردد، مدیریت مصرف انرژی، مانیتورینگ خرابی
(نظارت، پیش بینی، پیشگیری)، با ارائه پلتفرم های جامع و
سخت افزارهای مرتبط


آنتن های **LTE** مولتی باند شبکه سلولی (۱۶، ۲۴و۳۲ پورت)
سازگاری کامل با **eNodeB** شرکت ها از جمله هواوی،
نوکیا و اریکسون


تجهیزات زیرساخت مراکز داده شامل را هرو سرد و گرم،
رک و پایه‌رک، پاورماژول های هوشمند، کنترل و مانیتورینگ
مرکز داده بهمراه تجهیزات حوزه پسیو مانند انواع پچ پنل،
مدیریت کابل، لدر و سبدهای نصب کابل



انواع رک های داخلی جهت سرور و شبکه،
رک های بیرونی مخابراتی، شلترهای ثابت
و سیار مخابراتی و اضطراری


خودپرداز و کیوسک های بانکی

تهران، خیابان دماوند، تقاطع رسالت، شماره ۲۷۶ | تلفن : ۷۳۰۳۷ | فکس : ۷۷۹۶۹۶۱۳ - ۰۲۱ | کدپستی : ۱۷۴۶۷

info@payaco.com | payaco.com

فرافن
farafan

«دانش بنیان تولیدی نوع یک»

در حوزه خدمات طراحی و بهینه‌سازی شبکه‌های ارتباطی موبایل

NECTON DNS VIRUSPAAD QOE Radio Patrol Raibin

- طراحی و تولید مودم‌های LTE و 5G
- پلتفرم اینترنت اشیا (رای بین)
- کیوسک ویروسکاو
- راهکار DNS شبکه‌های مخابراتی
- راهکار مدیریت تجربه کاربر در شبکه‌های مخابراتی (QOE)
- ارائه سرویس مدیریت شده در حوزه IT
- سامانه مدیریت راندمان و بهینه‌سازی مخابراتی (RPAT)

همراه اول MCI | شرکت ارتباطات زیرساخت | رایتل RighTel | شرکت مخابرات ایران | ریاست جمهوری سعادت ملی فناوری | ایرانسل MTN | NAK | سازمان فناوری اطلاعات ایران

تهران، میدان آرژانتین، خیابان بیهقی
کوچه شانزدهم شرقی، پلاک ۲۴
کدپستی: ۱۵۱۵۶۶۵۵۱۹
تلفن: ۴۱۲۹۷۰۰۰

farafan.ir
info@farafan.ir

Tel

argtelecom.com
u-tel.ir

شرکت خدمات مخابراتی ارگ جدید

تولیـد کننـده انـواع مـودم

ADSL . VDSL . LTE . GPON

داده پردازی معتمد

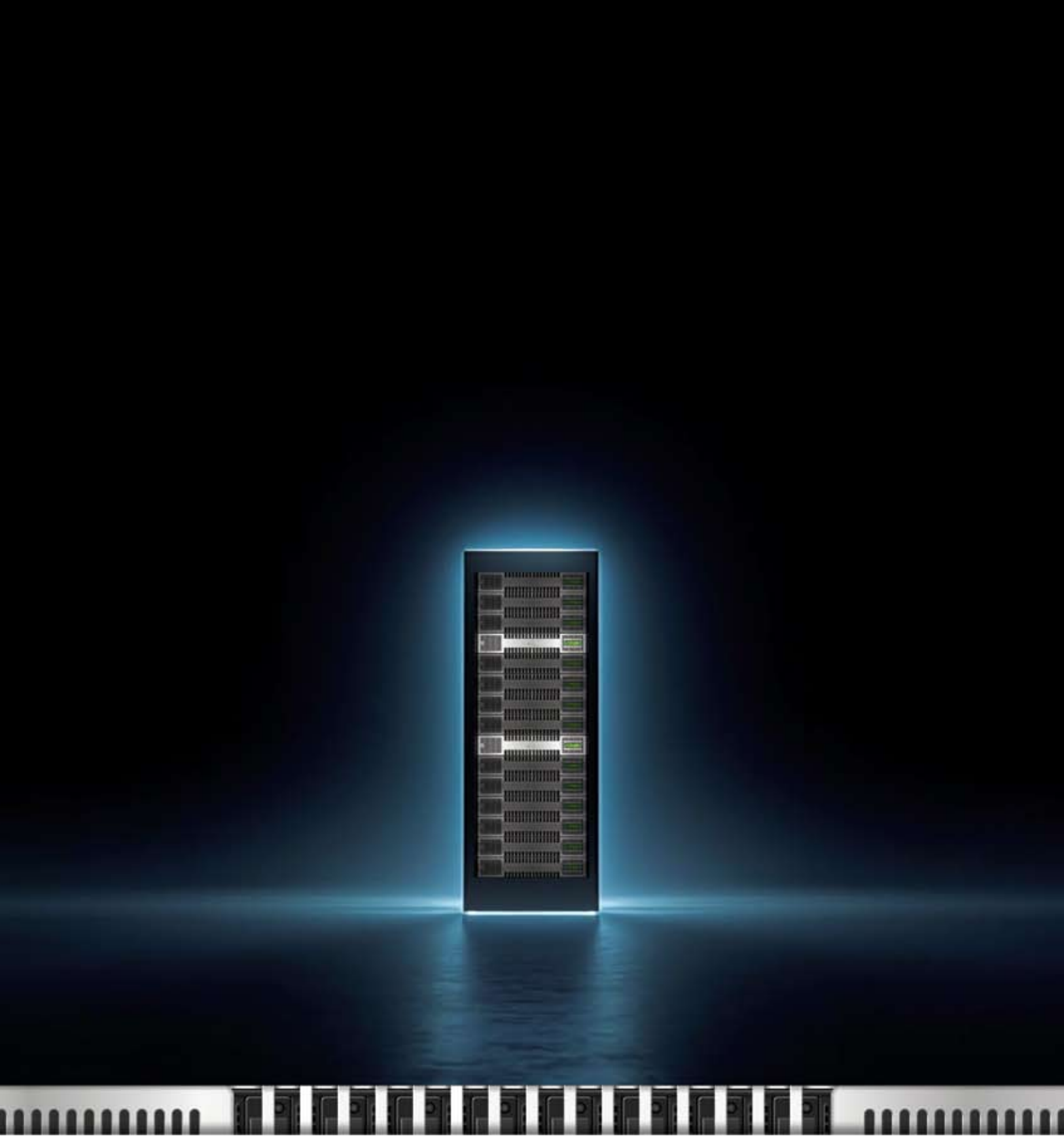
تیس

معتمد تیس

رتبه نخست معتمد مالیاتی کشور

ارائه خدمات نامحدود سامانه مودیان
به همه‌ی کسب‌وکارهای حقیقی و حقوقی

tisstsp.ir



خدمات میزبانی سـرور آسیاتک

اتصال پایدار حتی در روزهای خاموشی

تماس رایگان
۹۰۰۰ ۰۰۰۰
بدون نیـاز به کد

www.asiatech.ir

آسیاتک
asiatech

صاحب امتیاز و مدیرمسوول:
مسعود فاتح
رئیس شورای سیاست گذاری:
دکتر مهدی ادیبان
مشاوران مدیرمسوول:
نیما فاتح، دکتر داوود ادیب، فرامرز رستگار، دکتر مهدی فقیهی، فریبرز نژاددادگر، فریبرز ایرانی، علی شربیانی، مهران ارشادی فر و دکتر مسعود ظهرابی
سردبیر:
مونا ارشادی فر
دبیر تحریریه:
زهرا طاهری
همکاران این شماره:
احمد نیرومند، دکتر حیدر ربیعی، دکتر محمد علمیه و سارا استوار

عکاس ها:
سهند بیژن نیا و سارا داداش زاده
روابط عمومی و امور مشترکین:
سحر حسینی
صفحه آرایی و طرح روی جلد:
سمیرا علیدادی

با تشکر از:
دکتر محمدرضا عارف، دکتر سید ستار هاشمی، حمید فتاحی، دکتر بهزاد اکبری، محمد جعفرپور، دکتر وحید یزدانیان، دکتر محمد مهدی تقی پور، دکتر علیرضا عبداللهی نژاد، دکتر داوود زارعیان، فردخت شاه حسینی، محمدرضا بیدخام، مجید ذوقی، دکتر صادق عباسی شاهکوه، حسین ریاضی، محمدعلی یوسفی زاده، حامد حکاکان، دکتر سعید عسکری، علیرضا اسفندی، مهدی طالبی، مهرداد میراسماعیلی، دکتر امیر کیهان، سعید کیایی، دکتر سپیده عابدینی، محمود صادقیان، محمد جابری، محسن ابوئی مهریزی و الهام عدالتی

امور آماده سازی وچاپ:
چاپخانه پیمان نواندیش
نشانی چاپخانه:
تهران، پیچ شمیران، خیابان بهار، خیابان سمیه، پلاک ۵۸، طبقه زیرهمکف
تلفن: ۸۸۸۴۴۶۶۳ - ۰۹۱۲۲۴۳۸۳۲۴
ناظر فنی چاپ: محمد علی ملتی
نشانی ماهنامه:
انتهای بلوار کشاورز - خیابان دکتر قریب
خیابان فرصت شیرازی - پلاک ۱۰۸ - واحد ۱۷
کدپستی ۱۴۱۹۹۶۳۳۷۹
امور بازرگانی: ۰۹۱۲۸۲۱۶۶۵۸
تلفن: ۶۶۵۹۲۵۷۳
دورنگار: ۶۶۹۳۶۰۷۶
وب سایت: www.4Gnews.ir
پست الکترونیک: info@4Gnews.ir

ماهنامه نسل چهارم

دکتر داوود ادیب
رئیس کانون هماهنگی فاوا

پیشنهادات عملیاتی برای بالابردن امنیت سایبری کشور

حملات سایبری به برخی سامانه‌ها در کشور در طول تهاجم نظامی ۱۲ روزه رژیم غاصب صهیونیستی به کشورمان، نشانگر این موضوع است که وابستگی به کشورهای مختلف در حوزه تجهیزات زیرساختی، نظارتی و ارتباطی به چه میزان می تواند آسیب پذیری را بالا ببرد و طبیعتا این موضوعی نیست که به سادگی از کنار آن ها گذشت.

در سال های اخیر نهادهای نظارتی و قانون گذار این حوزه از قبیل شورای عالی فضای مجازی، وزارت ارتباطات، مرکز افتا و سازمان پدافند غیرعامل و برخی نهادهای مسوول دیگر، به تدوین اسناد و نظارت در این حوزه پرداخته و توصیه های لازم را ارایه نموده و حتی ممنوعیت خرید تجهیزات خارجی حوزه افتایی و زیرساختی را به سازمان های مختلف اعلام و حتی جایگزینی محصولات خارجی در حال سرویس آنها را با محصولات بومی قابل اعتماد و دارای تاییدیه های امنیتی، در طول یک زمان بندی الزام نموده اند، ولیکن به نظر می رسد که سرعت عمل در ارتباط با این مکاتبات و تذکرات کافی نبوده و می بایست به جد از طریق این نهادها دستورالعمل های الزام آور جدیدی ابلاغ و ضمانت اجرایی نیز تعیین گردد.

می بایست مقداری متفاوت بیندیشیم و بدانیم که این دغدغه ها در راستای امنیت کشور و در نهایت سلامت و آسایش همه هم میهنان است و طبیعتا موضوعات قیمتی و کیفیت بالا در برخی محصولات زیرساختی خارجی نبایست ملاک تصمیم گیری برای دولت مردان قرار گیرد و الزاما در این گونه تجهیزات، جنبه های دیگر و مهمی از جمله موضوعات امنیتی و توصیه های مرکز افتا و سازمان پدافند غیرعامل کشور در راس این گونه شاخص ها، نیز می بایست به دقت مورد توجه قرار گیرد.

در همین راستا برخی از پیشنهادات عملیاتی در حوزه امنیت که بارها طی مطالب متعددی مطرح شده است می تواند شامل موارد ذیل باشد:

- تربیت و حفظ نیروهای متخصص حوزه امنیت فناوری اطلاعات در کشور با ایجاد انگیزه، از جمله ارایه مشوق های لازم به کارفرمایان این حوزه و امریه نمودن بدون تشریفات این گونه افراد از طریق شرکت های خصوصی در این حوزه،
- تدوین واحد درسی مرتبط با موضوعات امنیتی در دوره های دبیرستانی و اجرای برنامه ارتقای سطح دانش امنیت و مهارت های عمومی در بکارگیری فناوری های نوین ارتباطی و اطلاعاتی و ارتقا دانش و سواد رسانه ای،
- تقویت دانش هوش مصنوعی در کشور و استفاده از هوش مصنوعی در پیشگیری حملات،
- ارتقای توان داخلی در اولویت بالا و تخصیص بودجه های لازم برای سال های آتی با نگاه کاهش وابستگی به خارج از کشور با سرمایه گذاری و حمایت از تولیدکنندگان حوزه افتا،
- بومی سازی دانش، فناوری، خدمات و تولید تجهیزات مورد نیاز کشور با استفاده از زیست بوم شرکت های دانش بنیان داخلی و علی الخصوص تولیدکنندگان حوزه افتای کشور،
- حمایت از شرکت های دانش بنیان داخلی فعال در حوزه فاوا با در نظر گرفتن تسهیلات مالیاتی، تضمین خرید و الزام بهره برداری از محصولات مرتبط با فناوری های نوین اطلاعات و ارتباطات بومی دارای تاییدیه مرکز افتا و سازمان پدافند غیرعامل کشور در سازمان های مهم، حساس و حیاتی،
- سازمان دهی ساختار مرکز ملی پایش امنیت زیرساخت های ارتباطی و اطلاعاتی کشور برای پیشگیری، کشف و دفع حملات،
- سرمایه گذاری در راستای تهیه ابزارهای مناسب برای استفاده در سازمان های دولتی و خصوصی با هدف مقابله با حملات سایبری احتمالی.

دکتر مهدی ادیبان
پژوهشگر سیاست های رسانه ای

ضرورت اقدام بین المللی در جهت نظم ارتباطی و اطلاعاتی

سوء استفاده یکجانبه از جریان خبری توسط چند کشور غربی و بازنگری در نظم ارتباطی و اطلاعاتی از موضوعات مهمی بود که در دهه های ۷۰ و ۸۰ میلادی با محوریت سازمان یونسکو و کشورهای عضو جنبش عدم تعهد مورد توجه قرار گرفت و وزرا و نمایندگان کشورهای عضو در کنفرانس های متعدد با اعتراض به جریان یکسویه اطلاعات که از سوی کشورهای استعمارگر به کشورهای دیگر سرازیر شده بود، منشور و معاهده ارتباطی و اطلاعاتی را مطالبه کردند.

این مسئله چالش های عمیقی را قریب به یک دهه بر روابط این کشورها با چند کشور معدود با محوریت آمریکا حاکم ساخت؛ تا جاییکه به خروج آمریکا و رژیم صهیونیستی از سازمان یونسکو منجر شد.

در آن دوران نگرش غالب در نخبگان جوامع به نفع جریان عادلانه و ضد سلطه حاکم بود و با تلاش های مستمر توانستند مانع از سلطه خبری و جریان یکسویه اطلاعات شوند. نکته مهم اینکه سلطه یکسویه خبری در پوشش جذاب جریان آزاد اطلاعات به کشورها و جوامع تحمیل می شد.

اکنون که نابسامانی و آشفتگی های سیاسی در سراسر جهان موجب شده است تا ساحت ارتباطات و اطلاعات دستخوش سوء استفاده قدرت های سلطه طلب قرار گیرد، جا دارد تا بار دیگر کوشش ها و تلاش های صاحبنظران و نهادهای فرهنگی که در دهه های هفتاد و هشتاد میلادی به منظور مقابله با جریان یکسویه اخبار که در پوشش جریان آزاد اطلاعات از سوی چند کشور معدود به کشورهای دیگر در سراسر جهان هجوم می برد، بازنگری و بازخوانی شود تا ضمن توجه به کوشش های نسلی از صاحبنظران ارتباطی در سراسر جهان، زمینه و راهکار احیاء این جریان مورد بررسی مجدد قرار گیرد.

مرحوم دکتر کاظم معتمد نژاد از جمله چهره های پیشکسوتی بودند که با اهتمام فراوان در فعالیت های بین المللی با جریان ضد سلطه همکاری و مشارکت داشتند. گزارش های متعددی که آن استاد فقید از انتقادها و تقابل کشورها در نهادهایی چون جنبش عدم تعهد، سازمان علمی فرهنگی یونسکو و اجلاسیه هایی که فرصت طرح نگرانی ها وجود داشته منتشر کرده است، بخش مهمی از تاریخ ارتباطات ایرانی است.

اولین انتقادها علیه سوء استفاده کشورهای بزرگ سرمایه داری غربی از نظریه جریان آزاد اطلاعات در سال ۱۹۶۸ در جریان برگزاری سمپوزیوم وسایل ارتباط جمعی و تفاهم بین المللی در یوگسلاوی مطرح شد و بر ضرورت ایجاد یک جریان متعادل اطلاعات در سطح دنیا سخن به میان آمد.

در سال های بعد نیز نگرانی ها نسبت به امپریالیسم خبری تشدید شد، منتقدین در تلاش بودند تا از طریق عهدنامه و میثاق های بین المللی نظم بین المللی نوین اطلاعات را با رویکرد عادلانه و در تقابل با سلطه جویی پایه گذاری کنند.

کتاب یک جهان چندین صدا که حاوی گزارش مهمی است که سازمان یونسکو به منظور ارزیابی مسایل ارتباطات جهانی در دوره نگارش با توجه به آینده تدوین شده است. مقدمه ارزشمند مرحوم دکتر معتمد نژاد بر ترجمه فارسی این کتاب تصویر

علیرغم هشدارهای مکرر طیف بزرگی از صاحبنظران و پژوهشگران بین المللی ارتباطی مبنی بر خطر بازگشت جریان سلطه جو و سوء استفاده از ابزارهای رسانه ای و ارتباطی متاسفانه رفته رفته بار دیگر کشورهای معدود در پوشش چند شرکت سپر ارتباطی و اطلاعاتی جهان را در اختیار خود گرفته اند.

روشنی از تلاش هایی است که منجر به این گزارش شده است.
این گزارش ها معطوف به دهه های ۷۰ و ۸۰ میلادی است، اما اهتمام دکتر معتمد نژاد و منتقدان سلطه غربی در سال های بعد نیز پیگیری شد. گزارش اجلاس جهانی سران جامعه اطلاعاتی که در تاریخ های ۲۰۰۳ ژنو و ۲۰۰۵ تونس برگزار شد، در حقیقت تداوم همان رویکرد در قبال فناوری های اطلاعاتی بود که در ابتدای هزاره سوم رو به گسترش و فراگیری داشت.

در بخشی از مقدمه این گزارش با عنوان ضرورت مشارکت فعال ایران در اجلاس جهانی آمده است: «نقش ایران در دفاع از مصالح و منافع کشورهای در حال توسعه در جریان برگزاری اجلاس جهانی می تواند در سطح جهانی بسیار موثر واقع شود باید در نظر داشت که مباحثه های بین المللی جاری در مورد جامعه اطلاعاتی اکنون در جهت عکس مباحثه های قبلی راجع به نظم نوین جهانی اطلاعات و ارتباطات که در دهه های ۷۰ و ۸۰ به منظور طرفداری از خواست کشورهای جهان سوم در مقابله با سلطه اطلاعاتی و ارتباطی غرب صورت می گرفتند در قالب طرحی از پیش آماده شده کشورهای اخیر براساس اصول لیبرالیسم اقتصادی جدید و غیره، مقتضیات و منافع کمپانی های فراملی و بازار آزاد جهان شمول مورد نظر آنها دنبال می شود.»

علیرغم هشدارهای مکرر طیف بزرگی از صاحبنظران و پژوهشگران بین المللی ارتباطی مبنی بر خطر بازگشت جریان سلطه جو و سوء استفاده از ابزارهای رسانه ای و ارتباطی متاسفانه رفته رفته بار دیگر کشورهای معدود در پوشش چند شرکت سپر ارتباطی و اطلاعاتی جهان را در اختیار خود گرفته اند.
سکوت نهادهای مسئول موجب خواهد شد تا افول اخلاق به عنوان نظم جدید ارتباطی و اطلاعاتی به همه ساحت های زندگی شخصی کشیده شود.

در سال های اخیر، نگرانی ها فراتر رفته، اکنون مسایل بسی فراتر از مواردی همچون حق دسترسی عادلانه همگانی، شکاف دیجیتال و نابرابری فاحش اطلاعاتی و تقابل با حق حاکمیت دولت ها و حقوق مربوط به محتواها و زبان ها و هویت های محلی است.

این جریان ابعاد بسیار خطرناک تری پیدا کرده است تا جایی که وارد ساحت های اخلاقی چون نفی حریم خصوصی افراد و کاربران شده است، در سال های اخیر انتشار گزارش های متعدد به روشنی سوء استفاده این شرکت ها را از اطلاعات خصوصی کاربران و فروش آن اطلاعات به اثبات رسانده است.

سکوت نهادهای مسئول موجب خواهد شد تا افول اخلاق به عنوان نظم جدید ارتباطی و اطلاعاتی به همه ساحت های زندگی شخصی کشیده شود.
در سال های اخیر و با توسعه ارتباطات همراه در کنار فراگیری شبکه جهانی اینترنت و دسترسی گسترده شهروندان در بسیاری از کشورها به شبکه های اجتماعی بار دیگر نگرانی های عمیق از سلطه طلبی کشورهای معدود مورد توجه قرار گرفته است.

اگرچه فراگیر شدن ارتباطات نوین در ظاهر دسترسی همگانی و عادلانه را برای شهروندان ایجاد کرده است، با این وجود جریان سلطه در لباس متفاوت و با شدت بیشتری بر شهروندان کشورهای مختلف از سراسر جهان خود را تحمیل کرده است.
تولید دستگاه ها و تجهیزات همراه در انحصار چند شرکت معدود قرار دارد، به علاوه اینکه نرم افزارها و دست افزارهای پایه نیز توسط شرکت های معدود تولید و مدیریت می شود.
تاسف انگیزتر اینکه بهره برداری از این ابزارها به طور آشکار در جهت مقاصد تروریستی و جاسوسی از شهروندان انجام می شود. نمونه های متعددی از فروش اطلاعات خصوصی کاربران توسط شرکت ها افشا شده است. با این وصف هیچ اراده ای در جهت نظارت و کنترل و یا محدودتر شدن این رویکرد دیده نمی شود.

به نظر می رسد بار دیگر تحرک کشورها و نخبگان دغدغه مند به عنوان ضرورتی اجتناب ناپذیر در مقابله با سوء استفاده از سپر ارتباطی و اطلاعاتی مورد نیاز است تا با معاهده ای فراگیر نظم عادلانه و انسانی را بر این فضا حاکم سازد.
برای مثال کشورهای عضو پیمان شانگهای ظرفیت قابل توجهی در شکل گیری جریان بین المللی به منظور نظم نوین ارتباطی و اطلاعاتی دارند.
جا دارد وزارت محترم ارتباطات و فناوری اطلاعات به عنوان دستگاه متولی ، با همکاری وزارتخانه های دیگر طرحی را با هدف پیگیری این نگرانی از طریق نهادهای بین المللی و جلب همکاری نخبگان و صاحب نظران تهیه و با هماهنگی وزارتخارجه در دستور پیگیری قرار دهد.

احمد نیرومند
رئیس کمیسیون تحول دیجیتال
سازمان نظام صنفی رایانه ای کشور

تاب‌آوری دیجیتال ملی

در سال‌های اخیر، موضوع پایداری دسترسی به اینترنت بین‌الملل به یکی از چالش‌های اصلی کشـورها در مواجهه با بحران‌ها، تحریم‌ها و تهدیدات سایبری تبدیل شده است. ایران نیز به‌عنوان کشوری با رشد بالای زیرساخت‌های دیجیتال، نیازمند اتخاذ راهکاری اصولی، چندلایه و پایدار برای مقابله با اختلال در دسترسی به اینترنت بین‌الملل است. در این میان، تقویت شبکه ملی اطلاعات به‌عنوان زیرساخت ارتباطی مستقل داخلی، نقشی کلیدی در پایداری خدمات دیجیتال کشور دارد. شبکه ملی اطلاعات، بستری ارتباطی امن، پایدار و پرسرعت درون‌مرزی است که هدف آن، تضمین تداوم خدمات دیجیتال حتی در شرایط بحران و قطعی اینترنت بین‌الملل است. این شبکه می‌تواند با کاهش وابستگی به سرویس‌های خارجی، زمینه‌ساز استقلال نسبی در ارائه خدمات پایه نظیر بانکداری، آموزش، سلامت، حمل‌ونقل و مدیریت شهری باشد. در عین حال، توسعه شبکه ملی نباید به معنای انزوا از فضای جهانی تعبیر شود، بلکه باید مکملی برای اتصال هوشمند، ایمن و قابل مدیریت به اینترنت جهانی باشد.

یکـی از اصلی‌ترین چالش‌ها در هنگام قطع اینترنـت بین‌الملل، بروز خلأهای امنیتی در لایه‌های مختلف شـبکه است. از اختلال در سیسـتم‌های احراز هویت تا ضعف در سامانه‌های مانیتورینگ و کنترل ترافیک داخلی، همگی می‌توانند تهدیدات جدی برای زیرساخت کشور ایجاد کنند. در چنین شرایطی، مسئولیت امنیت شبکه ملی اطلاعات بسـیار بالاست و نیازمند تدوین پروتکل‌های چندلایه امنیتی، استفاده از استانداردهای بین‌المللی ماننـد ISO/IEC ۲۷۰۰۱، NIST SP۸۰۰ و OWASP، و اجرای دقیق سیاسـت‌های مدیریت رخدادهای امنیتـی (SIEM/SOC) خواهد بود. برای تضمین تداوم خدمات در شرایط بحرانی، ضروری است تا تمامی دستگاه‌های دولتی و سازمان‌های خدمات‌رسان مانند بانک‌ها، شهرداری‌ها، بیمارستان‌ها و سامانه‌های خدمات عمومی، در قالب ساختاری طبقه‌بندی‌شده در سه سطح حیاتی، حساس و غیرحساس تعریف شوند. برای هر سطح، باید مسیرهای ارتباطی مشخص، پشتیبان‌گیری‌های امن و دسترسی‌های از پیش تعریف‌شده طراحی گردد تا حتی در زمان اختلال کامل در ارتباطات بین‌المللی، سرویس‌های حیاتی کشور به‌صورت ایزوله و پایدار به فعالیت خود ادامه دهند.

دستگاه‌های اجرایی کشور مانند وزارت ارتباطات، مرکز ملی فضای مجازی، سازمان فناوری اطلاعات، شرکت ارتباطات زیرساخت و وزارت کشور، نقش مستقیمی در طراحی، اجرا، کنترل و به‌روزرسانی معماری شبکه ملی اطلاعات دارند. این نهادها باید با تدوین نقشه راه مشترک و به‌کارگیری سازوکارهای هماهنگ بین‌نهادی، نسبت به تأمین امنیت و پایداری شبکه اقدام نمایند. یکی از راهکارهای کلیدی، الزام به تدوین برنامه‌ریزی واکنش در شرایط بحران و انجام تمرین‌های دوره‌ای آمادگی برای سـناریوهای قطع ارتباط است. در کنار حفظ دسترسی داخلی، باید تمهیداتی نیز برای آن دسته از شرکت‌های ایرانی اندیشیده شود که نیاز مستقیم به ارتباط با پلتفرم‌های خارجی برای ادامه فعالیت دارند. برای مثال، شرکت‌های صادراتی، فریلنسرها و کسب‌وکارهای فناوری‌محور که مشتری یا زیرساخت آن‌ها وابسته به سرویس‌های بین‌المللی است، باید از مسیرهای امن، محدود و کنترل‌شده به اینترنت بین‌الملل دسترسی داشته باشند. این مسیرها می‌تواند از طریق VPNهای سازمانی با احراز هویت چندمرحله‌ای، یا نقاط خروج مدیریت‌شده فراهم گردد.

با توجه به پراکندگی، ضعف در هم‌افزایی سامانه‌ها و عدم انطباق کامل با استانداردهای روز، بایـد اجرای یک طرح جامع تحت عنوان «تاما» (طـرح تدوین و اصلاح معماری) در دسـتور کار قرار گیرد. در این طرح، کلیه دسـتگاه‌ها مکلف می‌شوند ظرف ۹۰ روز، تمامی زیرساخت‌های اطلاعاتی، ارتباطی و امنیتی خود را مورد بازبینی کامل قرار داده و اسـناد تطبیق با استانداردهای امنیت اطلاعات، پایداری سرویس و معماری ارتباطی لایه‌بندی‌شده را ارائه دهند. این فرآیند باید تحت نظارت یک مرکز ملی (برای مثال فضای مجازی و راهبری سازمان نظام صنفی رایانه ای کشور)، با همکاری نهادهای تخصصی و شرکت‌های امنیتی بخش خصوصی انجام گیرد. تحقق سریع و اثربخش چنین طرحی، بدون مشـارکت مؤثر بخش خصوصـی ممکن نخواهد بود. شـرکت‌های دانش‌بنیان، پیمانکاران فنی، اپراتورهای زیرساختی و شرکت‌های حوزه امنیت سایبری می‌توانند در توسعه سامانه‌های پشتیبان، ساخت مراکز داده امن، پیاده‌سازی مکانیزم‌های احراز هویت داخلی، طراحی فایروال‌های بومی و ارائه راهکارهای ابری نقش‌آفرینی کنند. دولت باید با ایجاد مشوق‌ها، اعطای پروژه‌های هدفمند و ایجاد فضای رقابتی سالم، زمینه‌ساز ورود ظرفیت‌های بخش خصوصی در این حوزه شود.

در جهانی که تهدیدات ارتباطی و سـایبری بیش از گذشـته در حال گسـترش است، برنامه‌ریزی برای تاب‌آوری در برابر قطعی اینترنت بین‌الملل یک ضرورت حیاتی است. بهره‌گیری هوشمندانه از ظرفیت‌های شبکه ملی اطلاعات، تدوین استانداردهای امنیتی جامع، طبقه‌بندی دقیق خدمات، مدیریت دسترسی‌های اضطراری و اجرای طرح‌هایی نظیر «تاما»، تنها در سایه همکاری منسجم بین‌نهادی، مشارکت فعال بخش خصوصی و اتخاذ رویکردی پیش‌دستانه به امنیت سایبری محقق خواهد شد. این راهبرد، کشور را به‌سوی استقرار ساختار ارتباطی هوشمند، مقاوم و آینده‌نگر رهنمون خواهد ساخت.

ضرورت بازنگری در مدیران فناوری سازمان ها و بانک ها به دنبال حملات سایبری اخیر

دکتر اسماعیل ثنایی
نائب رئیس کانون هماهنگی فاوا

حوزه امنیت سـایبری کشور دو زاویـه دارد؛ یکـی بیرون از سـازمان و دیگـری درون سـازمان. در رابطه با بیرون از سـازمان بایـد روش های محکمـی به کار گرفت و صرفا اسـتفاده از تجهیزات خارجی به صلاح نیسـت؛ چراکه Backdoor [دسترسی به اطلاعات] دارند.

اخیرا شـاهد بودیم که مهاجمان سـایبری اطلاعات را منتشـر می کنند و زاویه ورود خود را می دانند، لذا باید در معماری سیستم های امنیتی بازنگری شود و ترکیبی از تجهیزات داخلی و خارجی به کار گرفته شود، اما با طراحی جدید.

لازم است هفته ای یکبار تیم بزرگی را مستقر کنیم که این کلاه سفیدها مرتب به خودمان حمله کنند تا نقاط قوت و ضعف را بشناسیم.

زاویه دیگر بحث داخلی اسـت که بانک هایی همچون بانک سـپه و پاسارگاد که اخیرا مورد حمله سایبری قرار گرفتند، از داخل ضربه خوردند و باید در سیاست امنیتـی داخلی بازنگری جدی در نظر گرفته شـود؛ نه تنهـا بانک ها بلکه همه سازمان ها.

باید چند نفر کلیدی که همه اطلاعات را در اختیار دارند، در جریان باشند و لازم است که سیاست این رویه عوض شود و کلیدهای امنیتی توزیع شوند.

یکی از بانک های سـوییس معتقد است که برای تغییر پسورد، به عنوان مثال از ۱۷ نفر مسوول حداقل ۱۵ نفر باید حضور داشته باشند تا پسوردها و سیستم ها را بازنگری کنند و ما نباید به چند نفر محدود اتکا کنیم تا در سیستم ورود کنند و باید در مدیران IT و امنیتی سازمان ها و بانک ها بازنگری شود.

دکتر حیدر ربیعی
استاد دانشگاه تهران

فراداده و پیامدهای امنیتی آن در جنگ‌های معاصر؛ ابعاد راهبردی و آسیب‌پذیری‌ها

در دوران معاصر، مفهوم فراداده به‌عنوان یکی از ارکان اساسی در مدیریت، انتقال و تفسیر داده‌ها در نظام‌های ارتباطی و اطلاعاتی ظاهر شده است. فراداده به مجموعه‌ای از داده‌ها اطلاق می‌شود که به توصیف، تفسیر و معنا دادن به داده‌های دیگر می‌پردازد. این اطلاعات معمولا شامل جزئیاتی مانند منبع، تاریخ تولید، مالکیت، ساختار و روش‌های دسترسی به داده‌ها هستند. نهادهای نظامی، امنیتی و حتی سازمان‌های غیرنظامی در شرایط بحران و جنگ به‌شکل گسترده‌ای متکی به نظام‌های مبتنی بر فراداده هستند.

فراداده علاوه بر فرصت‌های استراتژیکی که در آن نهفته، می تواند زمینه‌ساز بروز تهدیدهای پیچیده و آسیب‌های بالقوه سنگینی در برخی شرایط خاص شود. امتیاز ناشی از دسترسی و کنترل فراداده در چنین فضایی، قابلیت برتری اطلاعاتی، اشراف عملیاتی و تسلط بر الگوهای رفتاری را برای طرفین در دوران جنگ اطلاعاتی، به‌ویژه قدرت‌های فناورانه، فراهم می‌کند. در واقع، کنترل یا افشای فراداده می‌تواند سرنوشت یک نبرد سایبری را تعیین کند.

یکی از مهم‌ترین امتیاز فراداده و در عین حال ابعاد نقش آن در جنگ اطلاعاتی، شناسایی زنجیره فرماندهی، تحلیل روندهای عملیاتی، پیش‌بینی تحرکات و حتی افشای نقاط ضعف لجستیکی و فناوری است. ممکن است تنها با بررسی ترافیک گردش داده‌ها، زمان‌بندی ارسال پیام‌ها، یا ساختار فایل‌ها، بدون نیاز به دسترسی به محتوای اصلی، اطلاعات حیاتی درباره مقرهای فرماندهی، برنامه‌ریزی عملیات و سطح آماده‌باش نظامی طرفین استخراج شود. به عبارت دیگر، حتی رمزنگاری کامل پیام‌ها نیز بدون حفاظت از فراداده، مصونیت کافی را فراهم نمی‌کند.

افزون بر این، بهره‌برداران مجاز یا نفوذگران می‌توانند با استفاده از فراداده، حملات هدفمند اطلاعاتی را طراحی کنند که آثار آن تنها به تداوم عملیات محدود نشده بلکه منجر به اختلال گسترده در هماهنگی، کاهش اعتماد میان یگان‌ها و گاه انهدام روحیه نیروها می‌شود. آسیب‌پذیری زیرساخت‌های حیاتی از این زاویه، در دوران جنگ‌های نوین به شدت افزایش یافته است.

از سوی دیگر، مرز میان اطلاعات طبقه‌بندی‌شده و داده‌های عمومی با توسعه فناوری‌های تحلیلی هوشمند مبتنی بر یادگیری ماشین و داده‌کاوی روز به روز کمرنگ‌تر می‌شود. چنین فرایندی سبب می‌گردد که حتی داده‌های سطح پایین و به ظاهر ساده، با اتصال به فراداده‌های مناسب، ارزش عملیاتی و اطلاعاتی کلانی پیدا کنند.

برای مقابله با نقش مخرب فراداده و کاهش مخاطرات ناشی از آن، نیازمند اتخاذ راهبردهای نوین امنیت سایبری و اطلاعاتی در سطح زیرساخت و آموزش نیروهای تخصصی هستیم. از جمله مهم‌ترین راهکارها می‌توان به تولید، انتقال و ذخیره‌سازی داده به شیوه‌ای اشاره کرد که کمترین حجم فراداده افشا شده و فرایندهای ناشناس‌سازی و حذف مشخصات ثانویه داده به‌صورتی پیوسته اجرا شود. همچنین، پایش فعالانه جریان اطلاعات در شبکه‌های ارتباطی و رصد تغییرات غیرعادی در الگوهای تولید و مصرف داده از اهمیت بالایی برخوردار است.

در نهایت، باور به این نکته ضرورت دارد که در عصر حکمرانی داده و هوشمندی نظامی - امنیتی، مدیریت مسئولانه و آینده‌نگرانه بر فراداده، می‌تواند ضامن پایداری، ایستادگی و موفقیت ملی در مواجهه با تهدیدات اطلاعاتی پیچیده باشد. غفلت از این حوزه، خطر از دست رفتن برتری اطلاعاتی و افزایش خسارت‌های سازمانی و ملی در دوران جنگ را در پی خواهد داشت.

مسعود شکرانی
عضو هیأت مدیره سازمان نصر تهران

ضرورت شکل‌دهی به سیاست فناورانه ملی در برابر استارلینک

در ماه‌های اخیر، نام استارلینک بیش از هر زمان دیگری در فضای ارتباطی ایران شنیده می‌شود. گسترش پوشش رسمی این شرکت در آسمان ایران، بدون آنکه در چارچوب ضوابط و قوانین سرزمینی کشور ما قرار گیرد، نشانه‌ای روشن از تحولاتی است که مرزهای سنتی حکمرانی بر فضای ارتباطات را با چالش مواجه کرده‌اند. آنچه امروز پیش‌روی ما قرار دارد، صرفاً یک فناوری جدید نیست، بلکه پدیده‌ای چندلایه است که به‌طور هم‌زمان، پیامدهای فنی، حقوقی، اقتصادی و حاکمیتی در پی دارد. مواجهه با این پدیده نه با انکار ممکن است و نه با اقدامات پراکنده؛ بلکه مستلزم تدوین یک سیاست فناورانه ملی و منسجم است که به‌دور از هیجان، آینده‌نگر و مبتنی بر درک دقیق واقعیت‌های فنی و ساختاری باشد. استارلینک با بهره‌گیری از شبکه‌ای عظیم از ماهواره‌های لئو (Low Earth Orbit)، ساختار سنتی شبکه‌های مخابراتی را دگرگون می‌کند. کاربران نهایی، بدون نیاز به زیرساخت‌های زمینی و بدون عبور از گلوگاه‌های رایج ارتباطی کشور، به شبکه جهانی اینترنت متصل می‌شوند. این مدل ارتباطی عملاً سطح جدیدی از چالش را برای نهادهای مسئول در پایش، سیاست‌گذاری و امنیت فضای ارتباطی کشور ایجاد می‌کند. ابزارهای فنی موجود برای کنترل یا هدایت این ارتباطات، در اغلب موارد ناکافی یا ناکارآمد هستند و نیازمند ارتقاء جدی در حوزه‌هایی نظیر شناسایی سیگنال، مدیریت طیف فرکانسی، و تحلیل ترافیک ورودی و خروجی از مسیرهای ماهواره‌ای‌اند. وابسته ماندن به ابزارهای قدیمی در مواجهه با فناوری‌های جدید، تنها موجب تشدید شکاف میان ساختار حاکمیتی و واقعیت فناوری خواهد شد. از منظر حقوقی نیز استارلینک تاکنون هیچ مسیر رسمی برای فعالیت در ایران طی نکرده است. نه مجوزی دریافت شده، نه مسئولیتی پذیرفته شده و نه تعهدی به قوانین جمهوری اسلامی ایران وجود دارد. این در حالی است که هر ارائه‌دهنده خدمات ارتباطی، در هر نقطه از جهان، ناگزیر از رعایت قوانین حاکمیتی کشور هدف است.

ورود استارلینک بدون مجوز، بی‌اعتنایی به این اصل بنیادین در حکمرانی فناوری است و تداوم آن، مرجعیت حقوقی نهادهای تنظیم‌گر ارتباطات را به‌شدت تضعیف می‌کند. این وضع باید با تدوین چارچوب‌های روشن حقوقی و تمهید امکان پیگیری در مجامع بین‌المللی، اصلاح شود. حتی اگر چنین شرکت‌هایی تمایلی به پذیرش این قوانین نداشته باشند، باید تکلیف قانونی نحوه تعامل یا ممنوعیت فعالیت آن‌ها در کشور، به‌صراحت مشخص شود.

ابعاد اقتصادی ماجرا نیز کم‌اهمیت‌تر از بخش‌های دیگر نیست. استارلینک در صورت گسترش دسترسی، می‌تواند بدون پرداخت مالیات، بدون رعایت مسئولیت حقوقی، و بدون تعهد به کیفیت خدمات در بازار ایران فعالیت کند؛ در حالی که شرکت‌های داخلی در چارچوب سخت‌گیرانه مقررات، به فعالیت مشغول‌اند و ملزم به پاسخ‌گویی‌اند.

این شرایط نوعی رقابت ناعادلانه ایجاد می‌کند که نتیجه‌اش تضعیف اپراتورها، کاهش سرمایه‌گذاری در زیرساخت داخلی و در نهایت، وابستگی بلندمدت به یک ساختار فناورانه بیرونی خواهد بود. ما نمی‌توانیم در عین حال که بازار داخلی را زیر فشار مقررات حفظ می‌کنیم، چشم بر گسترش فعالیت بازیگری ببندیم که هیچ تعهدی نسبت به مقررات ما ندارد.

برخورد با پدیده استارلینک و دیگر فناوری‌های مشابه، نیازمند برنامه‌ای منسجم، چندبخشی و هم‌راستا با واقعیت‌های جهانی است. این برنامه باید از یک سو شامل ارتقای زیرساخت‌های پایش و مدیریت سیگنال در سطوح فنی باشد و از سوی دیگر، تدوین قوانین صریح و قابل اجرا در زمینه مالکیت تجهیزات گیرنده، ممنوعیت یا محدودیت بهره‌برداری بدون مجوز، و تقویت تعاملات بین‌نهادی میان رگولاتوری، وزارت ارتباطات، شورای عالی فضای مجازی و نهادهای دفاعی را در بر گیرد. همچنین باید به موازات این اقدامات، اکوسیستم داخلی ارتباطات تقویت شود؛ چه از نظر کیفیت خدمات، چه در مدل‌های اقتصادی اپراتورها، و چه در توانمندسازی بخش خصوصی در حوزه‌های نوآور. اگر اینترنت ماهواره‌ای واقعیتی اجتناب‌ناپذیر است، باید با تقویت ظرفیت درونی، خطر وابستگی به آن را کاهش داد، نه آن‌که در برابرش تنها دیوار کشید یا سکوت اختیار کرد. فناوری هیچ‌گاه منتظر نهادها نمی‌ماند. آن‌چه امروز با نام استارلینک پیش روی ماست، فردا به شکلی دیگر و با نامی دیگر ظهور خواهد کرد.

علی محمد کردنایج
روزنامه نگار و فعال رسانه ای

از میدان نبرد تا تایم لاین: شبکه های اجتماعی چگونه زخم های جنگ را عمیق تر می کنند؟

در شرایط بحرانی، پلتفرم‌ها باید الگوریتم‌هایی طراحی کنند که در شرایط بحرانی، محتوای آسیب‌زا را محدود یا دست‌کم با هشدارهای روانی همراه کنند و رسانه‌ها باید در کنار اطلاع‌رسانی، به ابعاد روانی بحران هم بپردازند و راهکارهایی برای مدیریت استرس در اختیار مخاطبان قرار دهند.

در روزگار ما، دیگر صدای آژیر و انفجار تنها ابزار انتقال خبر از جنگ نیست. این روزها جنگ، قبل از آنکه در خود جبهه‌ها شعله‌ور شود، در فضای مجازی زبانه می‌کشد. هر انفجار، هر تصویر، هر پیام صوتی یا ویدیویی، تنها چند ثانیه بعد از وقوع، در شبکه‌های اجتماعی منتشر می‌شود و با سرعتی سرسام‌آور، ذهن و روان میلیون‌ها کاربر را درمی‌نوردد. جنگ ایران و رژیم اسرائیل، که از سطوح سیاسی و نظامی فراتر رفته، به یک میدان جنگ رسانه‌ای تمام‌عیار نیز تبدیل شده است؛ میدانی که در آن، سربازانش کاربران‌اند و مهماتش پست‌ها، توییت‌ها و استوری‌ها.

اما آن‌چه اغلب نادیده گرفته می‌شود، تأثیر این محتوا بر روان ماست. فضای مجازی در شرایط بحرانی، هم می‌تواند ابزاری برای آگاهی باشد و هم بستر تشدید اضطراب، ترس و خشونت روانی. پرسش این‌جاست: شبکه‌های اجتماعی چگونه زخم‌های جنگ را عمیق‌تر می‌کنند؟!

افزایش اضطراب جمعی با هر اسکرول

با هر بار بالا و پایین کردن صفحه اینستاگرام یا توییتر، کاربر با سیلی از تصاویر، ویدیوها و روایت‌های شخصی از فجایع جنگ مواجه می‌شود. اغلب این محتوا بدون هیچ هشدار روانی یا زمینه‌سازی منتشر می‌شوند. تصاویر اجساد، صدای فریادها، لحظه برخورد موشک‌ها و گریه کودکان، درست در کنار عکس‌های روزمره دوستان یا تبلیغات فروش لباس، قرار می‌گیرند. این تضاد شدید، ذهن را دچار سردرگمی و روان را درگیر فشار مضاعف می‌کند.

کاربران بدون آن‌که آمادگی روحی داشته باشند، با واقعیت‌های خشن و گاه تحریف‌شده جنگ مواجه می‌شوند. این تجربه مداوم، پدیده‌ای به نام «فرسودگی همدلی» (Compassion Fatigue) را تقویت می‌کند؛ حالتی که در آن، فرد دیگر توان همدردی ندارد و دچار نوعی کرختی احساسی می‌شود.

روایت‌های قطبی و اثرات روانی آن

در شرایط جنگ، شبکه‌های اجتماعی معمولاً به بستری برای انتشار روایت‌های یک‌طرفه، هیجانی و بعضاً تحریف‌شده تبدیل می‌شوند. کاربران با روایت‌هایی از طرف مقابل که گاه حاوی نفرت، توهین و تحریک‌اند، بمباران می‌شوند. این فضای دوقطبی، نه‌تنها امکان گفت‌وگوی منطقی را از بین می‌برد، بلکه روان افراد را در وضعیت دائم تقابل و خشونت ذهنی نگه می‌دارد.

در چنین فضایی، افراد دائماً در حال مقایسه، قضاوت و موضع‌گیری‌اند؛ حتی اگر خود مستقیماً درگیر جنگ نباشند. این درگیری روانی، زمینه‌ساز افزایش استرس، بی‌اعتمادی اجتماعی و حتی احساس ناامنی در محیط روزمره می‌شود.

محتوای بدون راستی‌آزمایی، محرک ترس و آشوب ذهنی

یکی از خطرناک‌ترین جنبه‌های شبکه‌های اجتماعی در دوران جنگ، انتشار گسترده اطلاعات نادرست یا تأییدنشده است. ویدیوهایی که گاه مربوط به جنگ‌های قبلی‌اند، یا صداهایی که از منابع نامعلوم منتشر می‌شوند، می‌توانند موجی از وحشت ایجاد کنند. این اطلاعات، به‌ویژه زمانی که با عبارات تحریک‌آمیز یا هیجانی همراه می‌شوند، اثرات روانی شدیدی بر مخاطب می‌گذارند.

فرد نمی‌داند چه چیزی را باور کند، و همین «ابهام اطلاعاتی»، خود به‌تنهایی یکی از بزرگ‌ترین عوامل اضطراب روانی در بحران‌هاست.

جنگ برای دیده شدن؛ رقابت بر سر ترسناک‌ترین محتوا

در اکوسیستم شبکه‌های اجتماعی، محتواهایی که واکنش بیشتری می‌گیرند (لایک، ری‌توییت، کامنت)، بیشتر دیده می‌شوند. این الگوریتم‌ها به شکل ناخواسته، کاربران را به سوی تولید یا بازنشر محتوای شدیدتر، خشن‌تر و هیجانی‌تر سوق می‌دهند. در نتیجه، جنگ رسانه‌ای وارد چرخه‌ای معیوب می‌شود: افراد برای «دیده شدن» تصاویر تلخ‌تری منتشر می‌کنند، و مخاطبان برای «در جریان بودن» مدام خود را در معرض این محتواها قرار می‌دهند.

این رقابت پنهان، مخاطب را در وضعیتی از استرس دائمی قرار می‌دهد؛ جایی که مرز بین اطلاع‌رسانی و ایجاد وحشت به‌شدت باریک می‌شود.

نسل نوجوان؛ قربانی خاموش شبکه‌های اجتماعی در جنگ

در این میان، یکی از آسیب‌پذیرترین گروه‌ها نوجوانان‌اند. آن‌ها اغلب بدون نظارت والدین در شبکه‌های اجتماعی حضور دارند و ذهن‌شان در حال شکل‌گیری است. بمباران محتوای جنگی، روایت‌های پر از نفرت و بی‌ثباتی روانی ناشی از اخبار، می‌تواند تأثیراتی عمیق بر شکل‌گیری هویت، احساس امنیت، و آینده‌نگری آن‌ها داشته باشد.دیده شده که برخی نوجوانان دچار کابوس، اضطراب مزمن، ترس از آینده و حتی افسردگی شده‌اند؛ صرفاً به این دلیل که روزانه چند ساعت وقت خود را صرف مشاهده محتوای جنگی در فضای مجازی می‌کنند.

چه باید کرد؟ مسئولیت کاربران و رسانه‌ها

در چنین شرایطی، مسئولیت بر دوش کاربران، پلتفرم‌ها و رسانه‌هاست.

کاربران باید یاد بگیرند که مصرف محتوای خبری را مدیریت کنند. تعیین زمان مشخص، دنبال‌کردن منابع معتبر، اجتناب از بازنشر بدون اطمینان و مراقبت از سلامت روان، از جمله کارهایی است که می‌توان انجام داد.

از سوی دیگر، پلتفرم‌ها باید الگوریتم‌هایی طراحی کنند که در شرایط بحرانی، محتوای آسیب‌زا را محدود یا دست‌کم با هشدارهای روانی همراه کنند. همچنین رسانه‌ها باید در کنار اطلاع‌رسانی، به ابعاد روانی بحران هم بپردازند و راهکارهایی برای مدیریت استرس در اختیار مخاطبان قرار دهند.

جنگ تمام نمی‌شود، اگر در ذهن‌ها ادامه یابد

در نهایت، باید بپذیریم که جنگ تنها با توپ و تفنگ نیست. گاه ذهن‌های ما، خاکریزهایی هستند که نبرد واقعی در آن‌ها در جریان است. اگر مراقب نباشیم، شبکه‌های اجتماعی نه تنها ابزاری برای اطلاع‌رسانی، بلکه اسلحه‌ای برای زخم زدن به روان‌مان می‌شوند.

حالا بیش از هر زمان دیگر، به «سواد رسانه‌ای» نیاز داریم؛ نه فقط برای تشخیص خبر درست از نادرست، بلکه برای محافظت از چیزی که در هیچ عکس و فیلمی دیده نمی‌شود: آرامش روان‌مان.

فرمان جدید امنیت سایبری آمریکا؛ نگرانی استراتژیک واشنگتن؛

لزوم حرکت ایران به سمت رویکردهای پیشرفته امنیتی

مهدی فرجی
تحلیلگر راهبردی امنیت سایبری

در تاریخ ۱۶ خردادماه ۱۴۰۴ (۶ ژوئن ۲۰۲۵)، رئیس جمهور آمریکا دونالد ترامپ فرمان اجرایی جدیدی با عنوان «تداوم تلاش های منتخب برای تقویت امنیت سایبری کشور» را امضا کرد که با عنوان (Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order ۱۴۱۴۴/۱۳۶۹۴) ثبت فدرال شده است. این دستورالعمل در نگاه اول، یک گام رو به جلو و نشان دهنده تغییری مهم در سیاست امنیت سایبری ایالات متحده است، اما با نگاهی عمیق تر، می توان نشانه هایی از یک هراس استراتژیک را در آن مشاهده کرد.

البته از نظر کارشناسان بین المللی، این فرمان یک تحول استراتژیک در امنیت سایبری جهانی است و این اقدامات نه تنها برای امنیت ملی آمریکا حیاتی است، بلکه درس ها و الزاماتی حیاتی برای سایر کشورها، از جمله ایران، به همراه دارد تا در مسیر پیشگیری هوشمند و تقویت زیرساخت های دیجیتال خود حرکت کنند.

اقدامات کلیدی این فرمان که می تواند الهام بخش سیاست گذاری های ملی باشد، شامل موارد زیر است:

• **اصلاح سیاست تحریم ها:** این دستور، فرمان اجرایی ۱۳۶۹۴ مصوب سال ۲۰۱۵ را که برای اعمال تحریم علیه افراد و نهادهای درگیر در فعالیت های مخرب سایبری صادر شده بود، اصلاح می کند. هدف از این اصلاحات، تمرکز تحریم ها بر بازیگران مخرب خارجی است و اطمینان از عدم هدف گیری ناخواسته فعالیت های سیاسی داخلی. این اصلاح همچنین تصریح می کند که تحریم ها شامل فعالیت های مرتبط با انتخابات نمی شوند.

• **پیشبرد توسعه نرم افزار امن:** با اذعان به اهمیت امنیت نرم افزار، این فرمان به نهادهای فدرال دستور می دهد تا شیوه های توسعه نرم افزار امن را اتخاذ کنند. این شامل پیاده سازی دستورالعمل های موسسه ملی استانداردها و فناوری (NIST)، به ویژه چارچوب توسعه نرم افزار امن (SSDF)، برای افزایش امنیت و یکپارچگی نرم افزارهای مورد استفاده و توسعه یافته در نهادهای فدرال است.

• **تأکید بر رمزنگاری پساکوانتومی:** این دستور اجرایی، اتخاذ الگوریتم های رمزنگاری پساکوانتومی را الزامی می کند. این اقدام با هدف محافظت از اطلاعات حساس در برابر رمزگشایی احتمالی توسط رایانه های کوانتومی است و بدین ترتیب ارتباطات و داده های فدرال را برای بلندمدت ایمن می سازد.

• **تقویت امنیت پروتکل دروازه مرزی (BGP):** برای رفع آسیب پذیری ها در مسیریابی اینترنت، این دستور به نهادهای فدرال دستور می دهد تا اقداماتی را برای ایمن سازی پروتکل دروازه مرزی پیاده سازی کنند. با کاهش خطرات مرتبط با ربایش BGP، این اقدامات با هدف جلوگیری از تغییر مسیر مخرب ترافیک اینترنت است که می تواند منجر به رهگیری داده ها یا اختلال در خدمات شود و دستورالعمل به نهادهای فدرال برای اتخاذ مجوز مبدأ مسیر (ROA) و زیرساخت کلید عمومی منابع (RPKI) نشان دهنده تعهدی بسیار ضروری به سلامت ستون فقرات اینترنت است.

• **ترویج استانداردهای امنیت اینترنت اشیاء (IoT):** این فرمان اجرایی از توسعه و اتخاذ سیاست های امنیت سایبری قابل خواندن توسط ماشین و تعیین نامه های رسمی اعتماد برای دستگاه های اینترنت اشیاء حمایت می کند. این ابتکار به دنبال اطمینان از مطابقت دستگاه های متصل با اصول اساسی امنیتی است و بدین ترتیب از مصرف کنندگان و اکوسیستم دیجیتال گسترده تر محافظت می کند.

• **ضرورت حرکت ایران به سمت رویکردهای پیشرفته امنیت سایبری:** این تحولات نشان دهنده یک تغییر جهانی از رویکردهای واکنشی به سمت دکترین های ریسک محور و پیش بینانه است. این تغییر برای کشوری مانند ایران، با توجه به اهمیت روزافزون فضای سایبری و زیرساخت های حیاتی دیجیتال، از اهمیتی دوچندان برخوردار است.

• **توسعه نرم افزار امن:** در ایران نیز، با توجه به حجم فزاینده تولید نرم افزارهای بومی و توسعه زیرساخت های دیجیتال، نهادینه کردن امنیت از طریق طراحی (security-by-design) و پایبندی به چارچوب های استاندارد توسعه نرم افزار امن، برای جلوگیری از حملاتی مشابه سولاروینڈز حیاتی است، اما شاید بتوان این تأکید شدید بر امنیت زنجیره تأمین نرم افزار را از زاویه دیگری نیز دید؛ ایالات متحده که خود به خوبی می داند چه محصولاتی را با چه ویژگی هایی به دست دیگر کشورها می رساند، اکنون بیش از هر زمان دیگری نگران است که دیگران نیز با ابزارهای مشابه، امنیت ملی آن را هدف قرار دهند. این فرمان، در واقع، یک اقدام پیشگیرانه در برابر بازگشت سلاحی است که خود به تکامل آن کمک کرده است.

• **رمزنگاری پساکوانتومی:** الزام به انتقال به رمزنگاری پساکوانتومی شاید استراتژیک ترین اقدام در میان تمامی تدابیر باشد. با توجه به سرعت پیشرفت محاسبات کوانتومی، آماده سازی برای انتقال به رمزنگاری پساکوانتومی برای حفظ محرمانگی و یکپارچگی داده های ملی و طبقه بندی شده در بلندمدت، امری اجتناب ناپذیر است. همانطور که فناوری محاسبات کوانتومی به سرعت بالغ می شود، الگوریتم های رمزنگاری که از اکثر سیستم های مدرن مانند RSA و ECC محافظت می کنند، منسوخ خواهند شد. آماده سازی اکنون با شناسایی سیستم های آسیب پذیر و پیاده سازی استانداردهای پساکوانتومی منطبق بر تاییدات NIST برای یکپارچگی و محرمانگی بلندمدت داده ها، به ویژه برای ارتباطات طبقه بندی شده و دارای نگهداری طولانی مدت، ضروری است.

• **امنیت BGP:** تقویت امنیت زیرساخت های مسیریابی اینترنت (BGP) برای جلوگیری از ربایش ترافیک و همچنین تدوین استانداردهای امنیتی برای میلیاردها دستگاه اینترنت اشیاء که در کشور در حال گسترش هستند، از اولویت های حیاتی برای پایداری و امنیت ملی و خدمات عمومی محسوب می شود.

• **امنیت IoT:** تمرکز بر استانداردهای امنیت سایبری اینترنت اشیاء به همان اندازه آینده نگرانه است. با میلیاردها دستگاه متصل که با حداقل نظارت یا حفاظت های داخلی کار می کنند، اکوسیستم اینترنت اشیاء همچنان یک هدف آسان برای بات نت ها، جاسوسی و سوءاستفاده باقی می ماند.

باید استفاده از برچسب های امنیتی قابل خواندن توسط ماشین و چارچوب های اعتماد را ترویج داد، که به خریداران امکان تصمیم گیری آگاهانه را می دهد و سطح پایه امنیت کلی محصولات متصل را افزایش می دهد.

فرمان اجرایی اخیر در آمریکا، یک پیام روشن به جامعه امنیت سایبری جهانی و به خصوص کشورهایی مانند ایران است، هرچند که این فرمان بیش از آنکه یک نمایش قدرت باشد، نشان دهنده آگاهی از آسیب پذیری های عمیق است و امنیت سایبری دیگر یک مسئولیت صرفاً دولتی نیست و نیازمند یک رویکرد هماهنگ و تطبیقی است. همکاری نزدیک میان دولت، صنعت، دانشگاه و نهادهای استاندارد می تواند به ایجاد یک وضعیت امنیت سایبری یکپارچه تر و انعطاف پذیرتر در ایران منجر شود. این یک فرصت است تا با پیش بینی چالش های آینده و بازنگری در منابع، معماری امنیت سایبری کشور را بر پایه اصول عمل گرایانه، قابل اجرا و آینده نگر تقویت کنیم و توانایی خود را در مقابله قاطعانه با تهدیدات سایبری در حال تکامل نشان دهیم.

دکتر محمد علمیه
کارشناس امنیت سایبری

امنیت سایبری: ستون حیاتی در عصر دیجیتال

با رشد روزافزون استفاده از فناوری‌های دیجیتال در زندگی روزمره، از خدمات بانکی و خرید آنلاین گرفته تا آموزش و سلامت الکترونیک، نیاز به محافظت از اطلاعات و دارایی‌های دیجیتال بیش از پیش احساس می‌شود. در چنین شرایطی، «امنیت سایبری» دیگر یک موضوع فنی محدود به کارشناسان فناوری اطلاعات نیست، بلکه به ضرورتی فراگیر برای دولت‌ها، شرکت‌ها و حتی افراد عادی تبدیل شده است.

در خلال این محتوا به تعریف امنیت سایبری، تأثیر آن بر ساختارهای اجتماعی و اقتصادی، بررسی یک نمونه واقعی از حمله سایبری در ایالات متحده، گزارش‌های آماری جهانی و در نهایت پیشنهاداتی کاربردی برای ارتقای وضعیت امنیت سایبری در ایران پرداخته می‌شود.

تعریف امنیت سایبری

امنیت سایبری یا Cybersecurity به مجموعه‌ای از ابزارها، سیاست‌ها، اقدامات و مفاهیمی گفته می‌شود که برای محافظت از سیستم‌های اطلاعاتی، شبکه‌ها، برنامه‌ها و داده‌ها در برابر دسترسی غیرمجاز، نفوذ، حمله، تخریب، یا سرقت مورد استفاده قرار می‌گیرد.

هدف اصلی امنیت سایبری، حفظ سه اصل بنیادین در فضای دیجیتال است:

۱. **محرمانگی (Confidentiality)**: جلوگیری از دسترسی غیرمجاز به اطلاعات حساس؛

۲. **یکپارچگی (Integrity)**: اطمینان از این که اطلاعات تغییر نیافته و سالم باقی مانده‌اند؛

۳. **دسترس‌پذیری (Availability)**: تضمین اینکه کاربران مجاز در زمان مناسب به اطلاعات و خدمات دسترسی داشته باشند.

امنیت سایبری دامنه وسیعی دارد و شامل زیرشاخه‌هایی مانند امنیت شبکه، امنیت نرم‌افزار، امنیت پایگاه داده، امنیت سیستم‌های صنعتی (ICS) و حتی امنیت اینترنت اشیاء (IoT) می‌شود.

تأثیرات امنیت سایبری بر جامعه و اقتصاد

امنیت سایبری فقط یک موضوع تکنولوژیک نیست؛ بلکه به شکلی عمیق با ساختارهای اجتماعی و اقتصادی جوامع درهم‌تنیده است.

از منظر اجتماعی، حملات سایبری می‌توانند باعث نشت اطلاعات شخصی میلیون‌ها کاربر شوند. این اطلاعات می‌تواند شامل نام، آدرس، شماره ملی، سوابق پزشکی و حتی داده‌های بانکی باشد. چنین نشت‌هایی اعتماد مردم به پلتفرم‌های دیجیتال را به‌شدت کاهش می‌دهد، موجب ترس و ناامنی روانی می‌شود و فضا را برای گسترش اخبار جعلی، تهدیدات سیاسی یا باج‌گیری سایبری فراهم می‌سازد.

از منظر اقتصادی، آسیب‌های سایبری می‌توانند بسیار پرهزینه باشند. توقف فعالیت‌های کسب‌وکار، از بین رفتن داده‌ها، اخاذی دیجیتال و هزینه‌های قانونی از جمله نتایج مالی مستقیم هستند. به‌عنوان نمونه، در صورت حمله به سیستم‌های بانکی، نه تنها دسترسی مشتریان به حساب‌های خود مختل می‌شود بلکه زنجیره‌های پرداخت، خدمات مالی و اعتماد عمومی نیز به خطر می‌افتد.

مطالعه موردی: حمله باج‌افزاری به شرکت Colonial Pipeline (آمریکا - ۲۰۲۱)

یکی از شاخص‌ترین نمونه‌های تأثیر امنیت سایبری بر فضای اجتماعی و اقتصادی، در ایالات متحده بود. این شرکت بزرگ‌ترین شبکه انتقال فرآورده‌های نفتی در شرق آمریکا را در اختیار دارد و روزانه حدود ۴۵ درصد سوخت منطقه را تأمین می‌کند.

در این حمله، گروه هکری DarkSide با استفاده از یک باج‌افزار (Ransomware) موفق شد سیستم‌های اطلاعاتی این شرکت را قفل کرده و اطلاعات حساس را رمزگذاری کند. در پی آن، شرکت مجبور شد برای جلوگیری از خسارات بیشتر، به مدت چند روز خط لوله را تعطیل کند.

تبعات اجتماعی و اقتصادی این حادثه فوری و گسترده بود:

- صف‌های طولانی در پمپ‌بنزین‌ها در ایالت‌های جنوبی و شرقی؛
- افزایش قیمت بنزین و ایجاد نگرانی روانی در جامعه؛
- دخالت دولت فدرال و اعلام وضعیت اضطراری؛
- و در نهایت، پرداخت مبلغی معادل ۴.۴ میلیون دلار به عنوان باج (بخشی از آن بعدها بازیابی شد).

وضعیت جهانی امنیت سایبری: آمار و تحلیل

بر اساس گزارش‌های معتبر بین‌المللی:

- Cybersecurity Ventures پیش‌بینی کرده که خسارات ناشی از جرایم سایبری تا سال ۲۰۲۵ به رقم حیرت‌انگیز ۱۰.۵ تریلیون دلار در سال خواهد رسید.
- بر پایه آمار شرکت IBM Security در گزارش «Cost of a Data Breach ۲۰۲۳»، میانگین هزینه هر نشت داده برای سازمان‌ها حدود ۴.۴۵ میلیون دلار بوده است.
- گزارش Norton LifeLock در سال ۲۰۲۳ نشان می‌دهد که حدود ۶۸ درصد کاربران اینترنتی در سطح جهانی، تجربه نوعی از تهدیدات سایبری (مانند فیشینگ، بدافزار، سرقت رمز عبور یا هویت) را داشته‌اند.
- همچنین، طبق اعلام Statista، در سال ۲۰۲۳ بیش از ۲۴ میلیارد رکورد اطلاعاتی در سطح جهانی مورد دست‌درازی سایبری قرار گرفته است.

پیشنهاداتی برای تقویت امنیت سایبری در ایران

در ایران نیز با افزایش استفاده از خدمات دیجیتال، امنیت سایبری به مسئله‌ای راهبردی تبدیل شده است. مواردی چون حملات به سامانه‌های دولت الکترونیک، نشت اطلاعات کاربران برخی پلتفرم‌ها و تهدید زیرساخت‌های بانکی، نشان‌دهنده ضرورت توجه جدی‌تر به این موضوع است. راهکارهای پیشنهادی عبارت‌اند از:

۱. آموزش و افزایش آگاهی عمومی

نخستین و مهم‌ترین قدم، آموزش مردم درباره مخاطرات و روش‌های ساده محافظت از خود در فضای دیجیتال است. بسیاری از حملات، از جمله فیشینگ و سرقت اطلاعات، به‌دلیل سهل‌انگاری کاربر اتفاق می‌افتند.

۲. تدوین و اجرای قوانین جامع‌تر

قوانین مرتبط با جرایم سایبری باید همگام با پیشرفت تکنولوژی به‌روزرسانی شوند. لازم است همکاری میان قوه قضائیه، وزارت ارتباطات و سازمان‌های تخصصی برای تدوین دستورالعمل‌ها و سازوکارهای اجرایی تقویت شود.

۳. توسعه زیرساخت‌های بومی امنیت

ایجاد راهکارهای بومی برای رمزنگاری، پایش تهدیدات و دفاع دیجیتال به کاهش وابستگی به فناوری خارجی و جلوگیری از نفوذهای احتمالی کمک می‌کند.

۴. ایجاد مرکز واکنش سریع به تهدیدات سایبری (CERT)

توسعه تیم‌های پاسخ‌گویی ملی و استانی برای تحلیل و مقابله فوری با حملات، ضروری است. در بسیاری از کشورها، CERT نقشی کلیدی در حفظ ثبات دیجیتال ایفا می‌کند.

۵. حمایت از شرکت‌های دانش‌بنیان امنیتی

با حمایت مادی و معنوی از استارتاپ‌ها و شرکت‌های تخصصی در زمینه امنیت، می‌توان ظرفیت بومی را افزایش داده و بازار محصولات امنیت سایبری ایرانی را توسعه داد.

نتیجه‌گیری

امنیت سایبری نه یک انتخاب، بلکه یک ضرورت استراتژیک برای هر جامعه مدرن محسوب می‌شود. در دنیای دیجیتال امروز، هیچ‌کس از خطرات سایبری مصون نیست. کشورهایی که این تهدید را به‌موقع درک کرده و برای آن برنامه‌ریزی کرده‌اند، موفق شده‌اند از زیرساخت‌های حیاتی خود محافظت کنند و اعتماد شهروندان را حفظ نمایند.

ایران نیز برای رسیدن به جامعه‌ای ایمن، نیازمند ترکیبی از آموزش، قانون‌گذاری، سرمایه‌گذاری فناورانه و مشارکت بین‌المللی هدفمند است.

زهرا طاهری
سارا استوار

جنگ سایبری در میدان اقتصاد؛ زنگ خطر برای زیرساخت های ارتباطی کشور

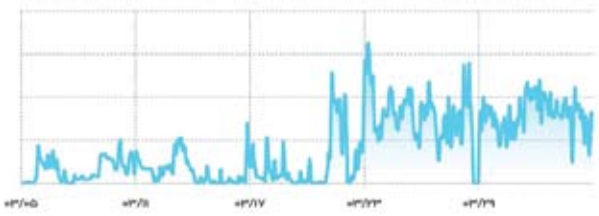
در دنیای امروز، جنگ دیگر تنها به میدان نبرد و سلاح‌های فیزیکی منحصر نیست، بلکه جبهه‌ای خاموش، اما بسیار خطرناک در حال گسترش است و آن، تقابل سایبری است. در این میدان نبرد نوین، اهداف، زیرساخت‌های حیاتی کشورهاست؛ از شبکه‌های ارتباطی گرفته تا سیستم‌های بانکی، حمل‌ونقل، انرژی و اطلاعات. امنیت سایبری دیگر نه یک انتخاب، بلکه یک ضرورت ملی است.

در شـرایطی که بسیاری از کشـورها در حال تقویت دیوارهای دفاعی دیجیتال خود هستند، غفلت از امنیت سایبری می‌تواند پیامدهای فاجعه‌باری به همراه داشته باشد. اختلال حتی چندین ساعته در خدمات بانکی یا مخابراتی، می‌تواند موجب بی‌نظمی اقتصادی، نارضایتی عمومی و حتی بحران‌های امنیتی شود.

با این حال، رخدادهای اخیر نشـان داد که سـاختار امنیت سـایبری کشـور، هنوز با اسـتانداردهای جهانی فاصلـه دارد و نیازمند بازنگری فوری در سیاسـت‌گذاری و اجراست.

افزایش شدید حملات سایبری در روزهای جنگ

بهزاد اکبری، معاون وزیر ارتباطات و مدیرعامل شرکت ارتباطات زیرساخت از افزایش شدید حملات سایبری به زیرساخت های ارتباطی کشور در روزهای جنگ خبر داد و تاکید کرد که افزایش شدید حجم حملات سایبری در این دوران از نوع DDoS بوده است.



حمله سایبری به بانک‌های سپه و پاسارگاد

همزمان با آغاز جنگ ۱۲ روزه رژیم غاصب صهیونیستی و حامیان غربی اش با کشورمان، حملات سایبری به زیرساخت‌های بانکی کشورمان رخ داد که باعث اختلال در خدمت رسانی برخی بانک های کشور علی الخصوص بانک های سپه و پاسارگاد شد.

این حملات نشان داد که حتی بانک‌هایی با گستره خدمات عمومی و بودجه قابل توجه، در برابر تهدیدات دیجیتال مصون نیستند.

لزوم بازنگری در سیاست‌های امنیت سایبری کشور

این حادثه بار دیگر ضرورت بازنگری جدی در اولویت‌ها و رویکردهای امنیت سایبری کشـور را برجسـته کرد. در سـال‌های اخیر، هشـدارهای مکرری درباره شکنندگی زیرسـاخت‌های دیجیتال داده شـده بود؛ با این حال، علی رغم اقدامات سازمان‌های مرتبط برای افزایش آمادگی عملیاتی و امنیتی، تجربه نشان داد که این اقدامات در برابر تهدیدات سایبری مؤثر نبوده است. کارشناسان معتقدند نبود هماهنگی بین دستگاه‌ها، فقدان نقشه جامع سایبری، تمرکز صرف بر مسائل نمایشی به جای ارتقاء ساختاری و آموزشی، از دلایل اصلی آسیب‌پذیری سیستم‌های کلیدی کشور است.

از هشدار تا اقدام

رخدادهای اخیر باید به عنوان یک زنگ بیدارباش جدی تلقی شود؛ امنیت سایبری نباید تنها در سخنرانی‌ها و اسناد راهبردی باقی بماند. تدوین برنامه‌ای فوری برای ایمن‌سازی زیرساخت‌های مالی، ایجاد سامانه پاسـخ سریع به حملات سایبری، آموزش مدیران و بازنگری در نقش نهادهای مسئول، تنها بخشی از اقداماتی است که باید بدون فوت وقت در دستور کار قرار گیرد. چراکه در دنیای سایه‌ها، کسانی پیروزند که زودتر آماده شوند.

فیلترینگ؛ سکوی پرتاب فیلترشکن‌های جاسوسی؟!

در پی گسترش فیلترینگ در ایران، میلیون‌ها کاربر ناچار به استفاده از فیلترشکن‌هایی شده‌اند که به اذعان کارشناسان، برخی از آن‌ها ابزارهای جاسوسی رژیم صهیونیستی هستند و امنیت ملی را تهدید می‌کنند، یا آنطور که ضیایی پرور می‌گوید: «مدافعین و مجریان فیلترینگ، آگاهانه یا ناآگاهانه در زمین اسرائیل بازی کرده‌اند».

در یک دهه اخیر، سیاسـت فیلترینگ پلتفرم‌های اجتماعی و ارتباطی در ایران، به یکی از اصلی‌ترین ابزارهای مدیریت فضای مجازی تبدیل شده است. با مسدود شدن گسترده اپلیکیشن‌هایی مانند اینستاگرام، تلگرام، واتساپ، توییتر و یوتیوب، میلیون‌ها کاربر ایرانی برای ادامه ارتباطات روزمره، شغلی یا آموزشی خود، ناچار به استفاده از ابزارهای دور زدن فیلتر شده‌اند.

این ابزارها که تحت عنوان عمومی «فیلترشـکن» شناخته می‌شوند، عمدتاً از منابع ناشـناخته یا توسـعه‌دهندگانی با هویت مبهم ارائه می‌شوند. اکثر آن‌ها رایگان‌اند و دسترسی کامل به اطلاعات دستگاه، ارتباطات شبکه، فایل‌ها، موقعیت مکانی و حتی دوربین و میکروفن کاربر را می‌طلبند. این واقعیت باعث شده تا بسیاری از کارشناسان حوزه امنیت سـایبری هشدار دهند که فیلترشکن‌ها، شاید خود تهدید بزرگتری از محتوای فیلترشده باشند.

به‌عبارت دیگـر، در حالی که هدف اولیه از فیلترینـگ، کاهش تهدیدات فرهنگی، سیاسی یا امنیتی عنوان می‌شود، نتیجه عملی آن می‌تواند افزایش وابستگی کاربران به ابزارهایی باشـد که خود به‌مراتب خطرناک‌ترنـد و می‌توانند به ابزاری برای نفوذ دشمنان تبدیل شوند.

فیلترینگ، بستر نصب فیلترشکن‌های جاسوسی اسرائیلی است

در همین راسـتا، حمید ضیایی‌پرور، استاد حوزه ارتباطات، بـا انتشـار پستی در

شبکـــه اجتماعی هشدار داد که سیاست فیلترینگ در ایران عملاً موجب گسترش اســتفاده از فیلترشکن‌هایی شده که بســیاری از آن‌ها توسط رژیم صهیونیستی یا نهادهای اطلاعاتی بیگانه توسعه یافته‌اند.

وی ادامه داد:«حالا بهتر می‌توان فهمید که سیاست فیلترینگ پلتفرم‌های اجتماعی در ایران، روشــی برای نصب چند ده میلیون فیلترشــکن جاسوســی اسرائیل روی گوشی‌های مردم و حتی مسئولین و خانواده‌های آن‌ها بوده است. مدافعین و مجریان فیلترینگ، آگاهانه یا ناآگاهانه در زمین اســرائیل بازی کرده‌اند.» این سخنان بازتاب نگرانی جدی از یک نقض امنیت ملی در مقیاس گسترده است؛ چرا که کاربران ایرانی با اعتماد به ابزارهایی که به‌عنوان «راه‌حل» برای فیلترینگ معرفی شده‌اند، در معرض تهدید مستقیم اطلاعاتی، سایبری و حتی فیزیکی قرار می‌گیرنـــد.

بازنگری فوری در سیاست‌های فیلترینگ ضروری است

اگر هدف از فیلترینگ، حفظ منافع ملی و امنیت فرهنگی کشور است، نمی‌توان از پیامدهای فنی و امنیتی آن چشم‌پوشی کرد. میلیون‌ها فیلترشکن بدون نظارت، روی گوشی‌های مردم نصب شده‌اند، و در فقدان زیرساخت‌های جایگزین قابل‌اعتماد، این روند ادامه دارد.سیاست‌گذاران باید به این پرسش پاسخ دهند: آیا فیلترینگ کنونی، کشــور را امن‌تر کرده، یا عملاً مســیر را برای نفوذ اطلاعاتی دشمن هموارتر ساخته است؟

تبعات استفاده از فیلترشکن‌ها؛ از نفوذ تا کلاهبرداری

رئیــس انجمــن صنفی کارفرمایی شــرکت های فنــاور هوش مصنوعــی و اقتصاد دیجیتال ایران گفت: فیلترشکن‌ها، موجب دسترسی به اطلاعات شخصی و محرمانه، سوءاستفاده و وارد کردن انواع بدافزارها به گوشی و رایانه کاربران می‌شود.

دکتر داوود ادیب، در گفت‌وگو با خبرنگار ما، گفت: فیلترینگ اینترنت اگرچه می تواند در راستای تمهیدات امنیتی باشد، ولیکن در صورت استفاده از روش های فیلترینگ کور، تهدیدات قابل توجهی نیز دارد که می بایست به آن توجه ویژه ای نمود.

ادیــب ادامــه داد: امروزه بســیاری از فعالیت هــای اجتماعی و به صــورت خاص، کســب‌وکارهای مجازی کاملا وابسته به اینترنت می باشند و ذات این فعالیت ها به شــکلی است که این گونه کسب و کارها بر اساس ماهیت این نوع شبکه ها عینیت یافته و توسعه پیدا می نمایند.

در این راستا فعالان اقتصادی این حوزه به جهت برخی محدودیت‌های اینترنتی در مقاطــع مختلف، بدون هیچ گونه آگاهی و فقط برای انجام فعالیت های اقتصادی و دور زدن محدودیت‌ها، اقدام به دانلود و نصب اپلیکیشن‌هایی نموده و می‌نمایند که بیشــتر از آنکه فیلترشکن باشند، موجب دسترسی به اطلاعات شخصی و محرمانه، سوءاســتفاده و وارد کردن انواع بدافزارها به گوشی و رایانه کاربران شده و در کنــار این ها احتمال آســیب هــای جدی چــون نفوذ، کلاهبرداری هــای اینترنتی و قرار گرفتن در معرض درگاه های جعلی و فیشــینگ را افزایش داده و تبعاتی را حاصل می‌ســازند که معمولا یا اثرات کوتاه مدت داشــته و یا اثرات طولانی مدت از خود به جای خواهند گذاشت.

رئیــس کانون هماهنگی فاوا مطرح کرد: امنیت، لازمه اقتدار و پیش نیاز حیات کشورها می باشد و کنترل حملات سایبری، فیلترینگ هوشمند و «نه کور» جزو موضوعاتی می باشد که به درستی می بایست در مواقع جنگ و تهدیدات در دستور کار دولت ها قرار گیرد و یقینا همه مردم با آن موافق می باشند، ولیکن در کنار این اقدام، موضوع اقتصاد که پایه های اقتدار و امنیت هر کشور نیز به آن وابسته است موضوع مهمتری اســت که می بایست در کنار امنیت به جد به آن توجه ویژه ای داشت. ادیب تاکید کرد: امروزه اقتصاد دیجیتال، بالا بردن سهم اقتصاد دیجیتال از GDP، توسعه کسب و کارهای مجازی و در نهایت فعالیت در شبکه های مبتنی بر اینترنت از اهداف مهم دولت ها در تمامی کشورها بوده و اکثر کشورهای توسعه یافته سعی می‌نمایند تا با ارایه تسهیلات، برداشتن موانع حاکم بر این کسب و کارها، اقتصاد دیجیتال را نهادینه ساخته و با بسترســازی مناسب، به کسب و کارهای پیاده سازی شده در بسترهای مجازی که می تواند ضمن ثروت آفرینی برای بخش قابل توجهی از جامعه باعث رفاه اجتماعی و کاهش جرم ناشــی از فقر در خانواده ها و در نهایت افزایش درامد سرانه کشور شوند، کشوری قدرتمند را به وجود آورند.

ادیــب مطرح کرد: به نظر می رســد که در صورت عــدم اتخاذ روش های منطقی و اصرار بر فیلترینگ کور، بر آینده مشاغل اینترنتی تاثیر بسیار بدی گذاشته و موجب از بین رفتن فضای کسب و کار و ترویج ناامیدی در بین جوانان به عنوان اصلی ترین مخاطبان این نوع کسب و کارها شود.

رئیــس کانــون هماهنگی فاوا با عنــوان این موضوع که ایــن محدودیت ها موجب رونق برخی از کســب و کارهای غیرمجاز همچون فروش فیلترشکن ها و تجهیزات ماهواره ای می شود، ادامه داد: در این فضای به وجود آمده تمهیداتی که قرار بود با محدودیت، تبدیل به قوت شــود در عمل ضمن ناکارامد بودن، تبدیل به تهدید هم گردیده و ضمن باز شــدن حفره های امنیتی، امکان نفوذ بدافزارها را که موضوعات امنیتی را دو چندان مشکل ساز می نماید را فراهم ساخته و در کنار آن به گسترش تخلفات بزرگتری دامن زده و امکان ورود به سایت هایی که بدون فیلترشکن امکان باز شــدن آن میسر نبود، میسر و باعث شــکل گیری ارتباطات جهت دار با رویکرد جاسوسی، کلاهبــرداری های اینترنتی و قرار گرفتن در معرض درگاه های جعلی و فیشینگ، اشاعه تخلفات، بروز اعمال مجرمانه، فساد و ترویج بی بند باری در بین جوانان و خردسالان به عنوان سرمایه های اجتماعی کشورمان می گردد.

هشدار امنیتی درباره پیام‌رسان های خارجی؛ مراقب انتقال اطلاعات باشید

با افزایش تهدیدات سایبری رژیم صهیونیستی و حامیان غربی اش علیه کاربران ایرانی، کارشناسان امنیت سایبری هشدار دادند؛ با توجه به دسترسی واتس‌اپ و اینستاگرام به داده های شـخصی و موقعیت مکانی کاربر پس از نصب روی گوشـی (حتی در صورت عدم اسـتفاده)، این داده‌ها می‌توانند در صـورت اتصال کاربر به اینترنت، به سرورهای خارجی منتقل شده و مورد بهره‌برداری اطلاعاتی قرار گیرند.

به گزارش خبرنگار ما با افزایـش تهدیدات سـایبری و فعالیت‌هـای اطلاعاتی رژیم صهیونیستی و حامیان غربی اش در فضای مجازی، کارشناسان حوزه فاوا نسبت به استفاده ناآگاهانه از اپلیکیشن‌های غربی علی الخصوص واتس‌اپ و اینستاگرام هشدار دادند. به گفته کارشناسان امنیت سایبری، این پیام‌رسان‌ها به‌دلیل اشراف اطلاعاتی دشمنان، می‌توانند بستری برای ردیابی، نفوذ و سرقت داده‌های کاربران باشند.

اشراف کامل بر داده‌ها؛ تهدیدی علیه امنیت ملی و فردی

کارشناسان امنیت سایبری تأکید دارند که برخی دولت‌ها، از جمله رژیم صهیونیستی و متحدانش، با در اختیار داشتن ابزارهای پیشرفته تحلیل داده و اشراف بر بسترهای غربی، قادرند اطلاعات حساس کاربران را در زمان واقعی رصد و ذخیره‌سازی کنند. به‌ویژه در مورد اپلیکیشن‌هایی مانند واتس‌اپ و اینستاگرام، انتقال تصاویر، ویدیوها و پیام‌ها می‌تواند به‌سادگی موجب افشای موقعیت جغرافیایی، ارتباطات فردی و حتی فعالیت‌های سازمانی شود.

از ارسال اطلاعات حساس خودداری کنید

طی روزهای درگیری ایران و رژیم صهیونیسـتی، در اطلاعیه‌های غیررسمی منتشر شده از سوی نهادهای امنیتی آمد:

«با توجه به این‌که دشـمنان روی پیام‌رسان‌های خارجی اشراف دارند، از انتقال هر گونـه اطلاعات اعم از تصویر، فیلـم یا متن حاوی داده‌های حسـاس، در این گونه پیام‌رسان‌ها به‌ویژه واتس‌اپ و اینستاگرام، خودداری فرمائید.»

این هشدار به‌ویژه برای نیروهای نظامی، امنیتی، مسئولان اجرایی و حتی شهروندان فعال در عرصه‌های سیاسی و اجتماعی جدی تلقی شده و رعایت آن می‌تواند مانع از افشای ناخواسته اطلاعات مهم شود.

خطر ردیابی و افشای موقعیت مکانی

اپلیکیشـن‌هایی مانند واتس‌اپ و اینسـتاگرام، حتی پس از نصب و بدون اسـتفاده مسـتقیم، به داده‌های حساسی همچون موقعیت مکانی، فهرست مخاطبان، گالری

تصاویر و سـایر اطلاعات دسترسـی دارند. این داده‌ها می‌توانند در صورت اتصال به اینترنت، به سرورهای خارجی منتقل شده و مورد بهره‌برداری اطلاعاتی قرار گیرند.

راهکارها و توصیه‌های امنیتی

- عدم ارسال اطلاعات حساس از طریق پیام‌رسان‌های خارجی
- خاموش کردن موقعیت مکانی در تنظیمات گوشی
- استفاده از پیام‌رسان‌های داخلی و پلتفرم‌های رمزگذاری‌شده
- حذف یا غیرفعال‌سازی اپلیکیشن‌های غیرضروری
- بروزرسانی مداوم سیستم‌عامل و نرم‌افزارهای امنیتی گوشی

در شـرایط حسـاس کنونی، امنیت اطلاعاتی شـهروندان بیش از هر زمان دیگری در معرض تهدید قرار دارد. رعایت توصیه‌های امنیتی در اسـتفاده از فضای مجازی می‌تواند در پیشگیری از حملات سایبری و حفظ جان و اطلاعات افراد نقشی حیاتی ایفا کند.

لزوم تشکیل قرارگاه مرکزی امنیت سایبری در یکی از نهادهای مسوول

مسـعود شـکرانی، عضو هیأت مدیره سـازمان نظام صنفی رایانه‌ای استان تهران در گفت‌وگو با خبرنگار ما پیرامون لزوم بازنگری در حوزه امنیت سایبری و در نظر گرفتن برخی اولویت‌ها با توجه به رخدادهای اخیر در حوزه حملات سایبری، گفت: ابتدا باید قرارگاه مرکزی امنیت سایبری در یکی از نهادهای مسوول با حضور بخش خصوصی تشـکیل شود و این قرارگاه برنامه کلان امنیت سایبری کشور را از هر لحاظ همچون مقررات، پرسنل سازمان ها، آموزش، به روزرسانی، توجیه مدیران ارشد، بررسی دقیق حوادث سایبری کشور، تهیه گزارش در تک تک موارد، تهیه پایگاه دانش حوادث امنیتی کشور و اطلاع رسانی تامین و به روزرسانی کند.

این کارشـناس فناوری اطلاعات، خاطرنشـان کرد: می توان از کشور روسیه یا سایر کشورهای پیشرو در حوزه امنیت سایبری، برای سرعت دادن به موارد فوق دعوت کرد و همچنین کنفرانس های بین المللی برای تبادل نظر بین کارشناسان برگزار کرد.

رئیس کمیسیون تأمین تجهیزات فاوای سازمان نظام صنفی رایانه‌ای استان تهران، اظهار کرد: باید سازمان های موازی که تحت نام امنیت سایبری تشکیل شده اند و کاری جز گناه را گردن دیگری انداختن ندارند، پس از انتقال تجربیات به قرارگاه واحد سایبری، حذف شوند.

درک احساسات توسط هوش مصنوعی بهتر از انسان

دانشمندان معتقدند که مدل‌های هوش مصنوعی در هوش هیجانی از انسان‌ها پیشی گرفتند و احساسات را بهتر از ما درک می‌کنند.

دانشمندان اعلام کردند که «هوش مصنوعی» احساسات را بهتر از ما درک می‌کند. آنها دریافتند که این سامانه‌ها امتیاز بسیار بالاتری از میانگین افراد در انتخاب پاسخ صحیح برای کنترل موقعیت‌های پراحساس مختلف، کسب کردند.

به گزارش لایوساینس، دانشمندان «دانشگاه ژنو»(UNIGE) و «دانشگاه برن» آزمون‌های هوش هیجانی را روی «مدل‌های زبان بزرگ» رایج اعمال کردند. آنها دو چیز را بررسی می‌کردند؛ اول، مقایسه عملکرد «هوش مصنوعی» و سوژه‌های انسانی بود و دوم، توانایی ایجاد سؤالات آزمون جدید که با اهداف آزمون‌های هوش هیجانی مطابقت داشته باشند.

با مطالعه پاسخ‌های انسانی معتبر از مطالعات قبلی، «LLMها» در ۸۱ درصد مواقع، پاسخ صحیح را در آزمون‌های هوش هیجانی انتخاب کردند، در حالی که این میزان برای انسان‌ها ۵۶ درصد بود.

نتیجه‌گیری کلی این بود که «هوش مصنوعی» در درک احساسات بهتر از انسان عمل می‌کند.

دانشمندان اشاره کردند که هر یک از آزمون‌های رایج هوش هیجانی مورد استفاده، چندگزینه‌ای بودند که به سختی در سناریوهای واقعی که تنش بین افراد بالاست، قابل اجراهستند.

«تیمور اجلال»، کارشناس صنعت مالی و امنیت اطلاعات گفت: شایان ذکر است که انسان‌ها همیشه در مورد احساسات دیگران توافق ندارند و حتی روانشناسان نیز می‌توانند سیگنال‌های عاطفی را به طور متفاوتی تفسیر کنند. بنابراین برنده شدن «هوش مصنوعی» در چنین آزمونی لزوماً به این معنی نیست که این سامانه بینش عمیق‌تری دارد. این به این معنی است که «هوش مصنوعی» پاسخ آماری مورد انتظار را بیشتر اوقات ارائه کرده است.

«تومان جعفر»، بنیانگذار و مدیرعامل یک ابزار مستندسازی مبتنی بر «هوش مصنوعی» گفت: سامانه‌های «هوش مصنوعی» در تشخیص الگوها عالی هستند، به‌ویژه زمانی که نشانه‌های عاطفی از یک ساختار قابل تشخیص مانند حالات چهره یا سیگنال‌های زبانی پیروی می‌کنند، اما برابر دانستن آن با درک عمیق‌تر از احساسات انسانی، خطر بزرگ‌نمایی آنچه «هوش مصنوعی» واقعاً انجام می‌دهد را در پی دارد.

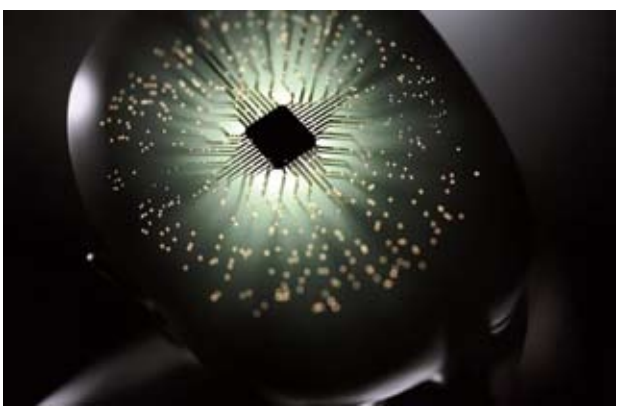
برخی کارشناسان به یک نکته حیاتی اشاره کردند: «هوش مصنوعی» در آزمون‌های مربوط به موقعیت‌های عاطفی بهتر عمل می‌کند، نه در اوج لحظه و نه به شیوه‌ای که انسان‌ها آنها را تجربه می‌کنند.

در مجموع، اکثر کارشناسان ادعای درک بهتر «هوش مصنوعی» از احساسات نسبت به انسان‌ها را کمی اغراق‌آمیز دانستند.

یک نکته نهایی نیز وجود دارد و آن این است که حتی با شواهدی که نشان می‌دهد اگر «هوش مصنوعی» به جای درک واقعی احساسات از تشخیص الگو استفاده می‌کند، در شناسایی و پاسخ به حالات عاطفی از انسان‌ها پیشی گرفته است.

یک «هوش مصنوعی» موسوم به «آیلتون» که توسط بیش از ۶۰۰۰ راننده کامیون در برزیل استفاده می‌شود، یک دستیار چندوجهی است که از صدا، متن و تصویر استفاده می‌کند و می‌تواند استرس، خشم یا غم را با حدود ۸۰ درصد دقت شناسایی می‌کند، همه اینها در چارچوب موقعیت‌های عاطفی هنگام تعامل رانندگان با آن در زمان واقعی است.

آزمایش دانشمندان چینی؛ استفاده از تراشه مغزی برای کنترل عامل‌های هوش مصنوعی



چین به دومین کشوری تبدیل شده است که آزمایش‌های بالینی برای دستگاه‌های رابط مغز و رایانه (بی‌سی‌آی) تهاجمی روی انسان را آغاز کرده است تا نهایتا بیماران بتوانند یک بازوی رباتیک یا عامل هوش مصنوعی را کنترل کنند.

براساس گزارش‌های رسانه‌های چینی، نخستین تراشه مغزی روی یک مرد ۳۷ ساله که در یک حادثه برق‌گرفتگی با ولتاژ بالا هر چهار اندام خود [یعنی دو دست و دو پا] را از دست داده بود، آزمایش شد و این امکان را به او داد که تنها با ذهن خود بازی‌های ویدیویی انجام دهد.

تیم تحقیقاتی اکنون امیدوار است که دستگاه رابط مغز و رایانه را توسعه دهد تا بیمار بتواند یک بازوی رباتیک یا عامل هوش مصنوعی را کنترل کند.

آزمایش اولیه که در مرکز تخصصی و پیشگام علوم مغز و هوش (CEBSIT) در آکادمی علوم چین انجام شد، شامل وارد کردن الکترودهای عصبی بسیار کوچک از طریق سوراخی در جمجمه برای ثبت فعالیت مغزی بود.

ژائو ژنگتو، پژوهشگر در مرکز تخصصی علوم مغز و هوش، گفت: «این الکترود آن‌قدر نرم است که نیروی لازم برای خم‌کردن آن با نیروی تعامل بین دو نورون در مغز قابل مقایسه است.»

«این ویژگی باعث می‌شود الکترود بتواند در دوره‌های طولانی، بدون آنکه واکنش‌های ایمنی یا واکنش‌های پس‌زدگی را تحریک کند، به‌طور هماهنگ با بافت مغز همزیستی کند.»

تیم‌های پژوهشی در ایالات متحده ازجمله استارتاپ نورالینک متعلق به ایلان ماسک نیز در حال آزمایش دستگاه‌های تهاجمی رابط مغز و رایانه (بی‌سی‌آی) روی بیماران انسانی هستند.

این میلیاردر دنیای فناوری اعلام کرده است که در پی آزمایش‌های موفقی که شرکت‌کنندگان در آن توانستند با استفاده از افکار خود رایانه‌ها را کنترل کنند، قصد دارد در دهه آینده تراشه‌های نورالینک را در مغز میلیون‌ها نفر کار بگذارد.

ایلان ماسک سال گذشته گفت: «اگر همه چیز خوب پیش برود، طی چند سال صدها نفر نورالینک خواهند داشت، شاید ده‌ها هزار نفر ظرف پنج سال، و میلیون‌ها نفر ظرف ۱۰ سال.»

آزمایش‌های اولیه نورالینک بر افراد [دچار] فلج کامل متمرکز بوده‌اند، با این حال ایلان ماسک مدعی است که این فناوری می‌تواند برای افزایش هوش و توانایی‌های انسانی استفاده شود.

به گفته رئیس نورالینک، دستگاه‌های رابط مغز و رایانه در نهایت می‌توانند به انسان‌ها امکان دهند با هوش مصنوعی ادغام شوند، و به آنها اجازه دهند با هوش جامع مصنوعی (AGI) رقابت کنند.

نورالینک به‌تازگی ۶۵۰ میلیون دلار سرمایه جدید جذب کرده است تا برنامه آزمایش‌هایش را در سطح جهانی گسترش دهد و «مرزهای امور ممکن برای بشر را توسعه دهد».

مرکز تخصصی علوم مغز و هوش (CEBSIT) در چین می‌گوید انتظار دارد دستگاه‌های رابط مغز و رایانه این مرکز تا سال ۲۰۲۸ برای ورود به بازار آماده شود، و این دستگاه‌ها ابتدا به‌عنوان یک ابزار پزشکی برای بهبود کیفیت زندگی افراد [دچار] قطع‌عضو و افراد با آسیب نخاعی عرضه خواهد شد.

این آزمایشگاه مستقر در شانگهای مدعی است که دستگاهش در حال حاضر از تراشه دستگاه‌های رابط مغز و رایانه نورالینک کوچک‌تر و انعطاف‌پذیرتر است.

هوش مصنوعی گاهی مشابه انسان فکر می‌کند

پژوهشگران در چین دریافته‌اند که مدل‌های هوش مصنوعی مانند چت جی‌پی‌تی، اطلاعات را به شیوه‌ای شبیه به مغز انسان پردازش می‌کنند.

در یک بررسی درباره مدل‌های زبانی بزرگ (ال‌ال‌ام) شواهدی یافت شد که نشان می‌دهد ابزارهای پرکاربرد هوش مصنوعی که اوپن‌ای‌آی و گوگل ساخته‌اند، اطلاعات را خودبه‌خود و خودجوش دسته‌بندی می‌کنند، به رغم آنکه برای این کار آموزش ندیده‌اند.

یافته‌هایی که یک تیم از آکادمی علوم چین و دانشگاه فناوری جنوب چین ارائه کرده است، نشان می‌دهند که مدل‌های زبانی بزرگ «شباهت‌های بنیادینی دارند که جنبه‌های کلیدی دانش مفهومی انسان را بازتاب می‌دهند» ــ این امر، این فرض را به چالش می‌کشد که سیستم‌های هوش مصنوعی صرفا با شناسایی الگوها پاسخ‌ها را تقلید می‌کنند.

پژوهشگران انجام «وظیفه یافتن مورد متفاوت» را به «چت‌جی‌پی‌تی-۳.۵» شرکت اوپن‌ای‌آی و «جمنای پرو ویژن» شرکت گوگل محول کردند؛ وظیفه‌ای که در جریان آن، هوش مصنوعی ۶۶ بعد مفهومی ایجاد کرد تا اشیا را طبقه‌بندی کند.

پژوهشگران گفتند: «قابل توجه است که ابعاد زیربنایی این تعبیه‌سازی‌ها قابل تفسیر بودند، که این نشان می‌دهد مدل‌های زبانی بزرگ و مدل‌های زبانی چندوجهی، بازنمایی‌های مفهومی شبیه به انسان از اشیا ایجاد می‌کنند.»

«این امر شواهد قانع‌کننده‌ای مبنی بر این ارائه می‌دهد که با اینکه بازنمایی اشیا در مدل‌های زبانی بزرگ با بازنمایی‌های انسانی یکسان نیست، شباهت‌های بنیادینی با آن دارد که بازتاب‌دهنده جنبه‌های کلیدی دانش مفهومی انسان است.»

مطالعه‌ای که جزئیات این پژوهش را شرح می‌دهد و با عنوان «بازنمایی‌های مفهومی از اشیا، مشابه [ادراک] انسان، به‌طور طبیعی در مدل‌های زبانی بزرگ چندوجهی پدیدار می‌شوند» منتشر شده، در مجله علمی «هوش ماشینی نیچر» به چاپ رسیده است.

دانشمندان امیدوارند که یافته‌هایشان به توسعه «سامانه‌های شناختی مصنوعی شبیه‌تر به انسان» کمک کند؛ سامانه‌هایی که بتوانند همکاری بهتری با انسان‌ها داشته باشند.

تیم‌های پژوهشی دیگر هم‌اکنون در حال توسعه سامانه‌های هوش مصنوعی شبیه‌تر به انسان‌اند و یکی از استارتاپ‌های استرالیایی اخیرا نخستین رایانه زیستی تجاری جهان را معرفی کرده است که با سلول‌های زنده مغز انسان کار می‌کند.

رایانه «بدن درون یک جعبه» شرکت کورتیکال لبز، از نورون‌های پرورش‌یافته در آزمایشگاه روی یک تراشه سیلیکونی استفاده می‌کند تا سیگنال‌های الکتریکی را ارسال و دریافت کند

این استارتاپ مدعی است که سامانه مبتنی بر زیست‌شناسی می‌تواند در قیاس با سامانه‌های رایانشی رایج با بهره‌وری بیشتری یاد بگیرد و خود را تطبیق دهد. یک نسخه اولیه از این سامانه نشان داد که چگونه ۸۰۰ هزار نورون انسان و موش توانستند خودشان یاد بگیرند بازی ویدیویی پونگ را چه طور اجرا کنند.

براساس مقاله‌ای که در مجله «سل» منتشر شده، نورون‌ها هنگام قرار گرفتن در دنیای بازی، نوعی هشیاری از خود نشان دادند.

در وبسایت این شرکت آمده است: «فناوری ما زیست‌شناسی را با رایانش رایج ترکیب می‌کند تا برترین یادگیری ماشینی را بسازد.»

«نورون به‌طور خودکار برنامه‌نویسی می‌شود، انعطاف‌پذیری نامحدودی دارد، و حاصل چهار میلیارد سال فرگشت است.»

استفاده از چت جی‌پی‌تی می‌تواند باعث کاهش توان یادگیری شود

مطالعه‌ای جدید در دانشگاه ام‌آی‌تی نشان می‌دهد استفاده از چت‌جی‌پی‌تی می‌تواند منجر به «کاهش احتمالی» توانایی‌های یادگیری و درونی‌سازی «دیدگاه‌های سطحی یا دارای سوگیری» شود.

پژوهشگران آزمایشگاه رسانه دانشگاه ام‌آی‌تی شرکت‌کنندگان در مطالعه تازه خود را به سه گروه تقسیم کردند. هر گروه باید یک مقاله می‌نوشت: گروهی فقط با استفاده از چت جی‌پی‌تی، گروه دیگر با استفاده از موتورهای جست‌وجو، و گروه سوم بدون هیچ ابزار کمکی.

در طول نگارش، فعالیت مغزی شرکت‌کنندگان با استفاده از دستگاه ثبت نوار مغزی اندازه‌گیری شد. سپس مقالات تولیدشده توسط داوران انسانی و ابزارهای هوش مصنوعی ارزیابی شد. نتایج این بررسی نشان داد که گروهی که فقط از چت جی‌پی‌تی استفاده کرده بودند، کمترین میزان فعالیت عصبی را در برخی نواحی مغز داشتند و در به خاطر آوردن یا شناسایی نوشته‌های خود دچار مشکل بودند. در مقابل، گروهی که بدون استفاده از هیچ فناوری‌ای مقاله نوشته بودند، مشارکت شناختی بالاتری و حافظه بهتری از خود نشان دادند.

در مرحله دوم آزمایش، گروهی که در ابتدا از چت جی‌پی‌تی استفاده کرده بودند، مامور شد که همان کار را بدون هیچ‌ابزار کمکی انجام دهد. نتیجه عملکرد آن‌ها ضعیف‌تر از دیگر گروه‌ها بود و متونی «دارای سوگیری و محتوای سطحی» تولید کردند.

«کاهش احتمالی» توانایی‌های یادگیری

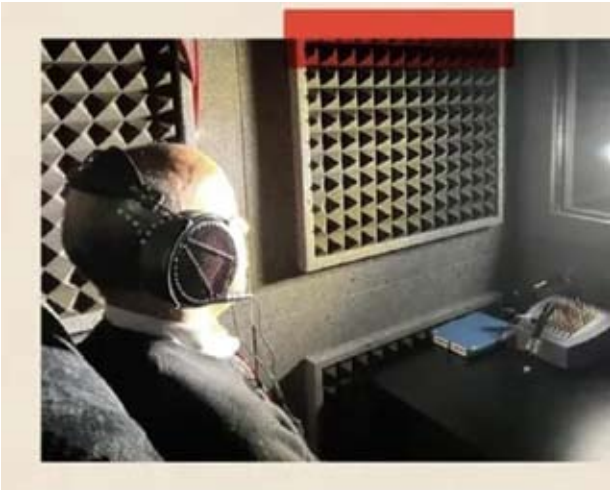
نتایج این مطالعه نشان داد استفاده مکرر از مدل‌های تعاملی هوش مصنوعی مانند چت جی‌پی‌تی در بلندمدت عملکرد یادگیری مستقل را کاهش می‌دهد.

این افراد، در بلندمدت، ممکن است در معرض کاهش تفکر انتقادی، افزایش آسیب‌پذیری در برابر دستکاری اطلاعات، افت خلاقیت و همچنین «کاهش احتمالی» در توانایی‌های یادگیری قرار گیرند.

نتایج این مطالعه همچنین نشان داد شرکت‌کنندگانی که مقاله‌هایشان را بدون هیچ‌ابزار کمکی نوشته بودند، رضایت بیشتری از عملکرد خود داشتند. مغز آن‌ها نیز درگیر برقراری ارتباطات قوی‌تری بود و بیشتر درگیر فرایند تحقیق، تفکر، آموختن و نوشتن شده بودند. در مقابل، کسانی که از ابزارهای هوش مصنوعی استفاده کرده بودند، احساس می‌کردند با متن خود ارتباط کمتری دارند و اغلب نمی‌توانستند بخش مشخصی از نوشته‌شان را به یاد بیاورند.

نویسندگان این تحقیق خواستار انجام مطالعات بیشتر در زمینه اثرات ابزارهای هوش مصنوعی بر مغز انسان شدند و تاکید کردند که هنوز برای نتیجه‌گیری درباره مفید بودن مدل‌های تعاملی هوش مصنوعی برای توانایی‌های شناختی انسان، زود است.

آیا هوش مصنوعی زمانی به آگاهی واقعی می‌رسد؟



عده‌ای در دنیای فناوری، مانند بلیک لمونی، مهندس سابق «گوگل»، بر این باورند که چت‌بات‌های پیشرفته امروزی مثل «چت جی‌پی‌تی» و «جمنای» ممکن است در حال حاضر به میزانی از آگاهی رسیده باشند.

کایل فیش، مهندس «آنتروپیک»، می‌گوید احتمال آگاهی داشتن این مدل‌های هوش مصنوعی هم‌اینک ۱۵ درصد است. این در حالی است که هنوز هیچ‌کس نحوه دقیق کارکرد این سیستم‌ها را نمی‌داند.

برخی محققان، مانند مانوئل و لنور بلوم، نیز معتقدند که اتصال ورودی‌های حسی زنده مثل دوربین و حسگرهای لمسی به مدل‌های زبانی می‌تواند جرقه آگاهی را در آنها روشن کند. این دو در حال توسعه مدلی به نام «برینیش» هستند که عملکرد مغز را درون ماشین‌ها بازسازی می‌کند.

برخی دانشمندان همچون پروفسور دیوید چالمرز، اگرچه اذعان دارند که «مساله دشوار» آگاهی هنوز حل نشده است، اما امیدوارند روزی آگاهی در ماشین‌ها شکوفا شود و حتی به تکامل بعدی انسان بیانجامد.

با این حال، دیدگاه‌های شکاکانه‌ای نیز وجود دارد. پروفسور آنیل ست از دانشگاه ساسکس معتقد است که آگاهی لزوماً با هوش و زبان گره نخورده است، و توانایی‌های هوش مصنوعی را نباید با آگاهی یکی گرفت. به گفته وی، آگاهی به «زنده بودن» وابسته است، و سیستم‌های سیلیکونی هیچ‌گاه به تجربه آگاهانه دست نمی‌یابند.

در این راستا، شرکت‌هایی مانند «کورتیکال لَبز» در استرالیا با بر «مینی‌مغزها» یا خوشه‌های کوچک سلول‌های عصبی تمرکز کرده‌اند تا امکان ظهور آگاهی را در سیستم‌های زنده بررسی کنند.

اما حتی اگر ماشین‌ها هرگز به آگاهی واقعی نرسند، جلوه‌های شبه‌انسانی آنها دغدغه‌های اجتماعی و اخلاقی جدیدی ایجاد می‌کند. پروفسور ست هشدار می‌دهد که انسان‌ها ممکن است شروع به همدلی با ربات‌ها کنند، و بدین ترتیب همدلی با همنوعان خود را فراموش کنند.

در نهایت، پرسش درباره آگاهی ماشین فقط علمی نیست، بلکه فلسفی و اخلاقی است. این پرسشی است که رویکرد ما در مواجهه با آن می‌تواند ماهیت خود انسان را برای همیشه دگرگون کند.

رتبه بندی مدل های هوش مصنوعی از جهت هوش

داده های جدیدی که توسط Tracking AI جمع آوری شده اند، با استفاده از آزمون هوش منسای نروژ، رتبه بندی جالبی از باهوش ترین مدل های هوش مصنوعی ارائه می دهند.

این آزمون که به سختی و دقتش در سنجش هوش انسانی مشهور است، اکنون معیاری برای ارزیابی توانایی‌های شناختی هوش مصنوعی شده است.

برای درک بهتر امتیازات کسب‌شده توسط هوش مصنوعی، یادآوری این نکته ضروری است که میانگین نمره هوش انسانی بین ۹۰ تا ۱۱۰ قرار دارد. کسب نمره‌ای بالاتر از ۱۳۰ در این آزمون، نشانه‌ای از سطح نبوغ و هوش فوق‌العاده محسوب می‌شود.

پیشتازان هوش مصنوعی در آستانه نبوغ

در این رتبه‌بندی، مدل OpenAI o۳ با کسب نمره ۱۳۵ در آزمون هوش منسا، در صدر قرار گرفته و به وضوح در دسته «نابغه» جای می‌گیرد. این مدل که بخشی از ChatGPT، یکی از پرکاربردترین ابزارهای هوش مصنوعی در جهان است، توانایی‌های چشمگیری در پردازش و تولید متن از خود نشان داده است.

پس از OpenAI o۳، مدل‌های دیگری نیز با امتیازات بالا خودنمایی می‌کنند. Claude-۴ Sonnet از Anthropic با نمره ۱۲۷ و Gemini ۲,۰

Flash Thinking از گـوگل بـا نمـره ۱۲۶، فاصلـه چندانی بـا صـــدر جدول ندارنـــــد. همچنین، نسخه‌های جدیدتر مانند Gemini ۲٫۵ Pro و OpenAI o۴ mini هر دو امتیاز بالای ۱۲۰ را کسب کرده‌اند که نشان‌دهنده عملکردی بالاتر از میانگین هوش انسانی است.

نکته قابل توجه در این بررســی، تسـلط مدل‌های متن‌محور در ۱۰ رتبه برتر است. این مدل‌ها که قابلیت پردازش تصاویر را ندارند، نشان داده‌اند که در استدلال و تفکر مبتنی بر کلمات، بسیار قوی عمل می‌کنند.

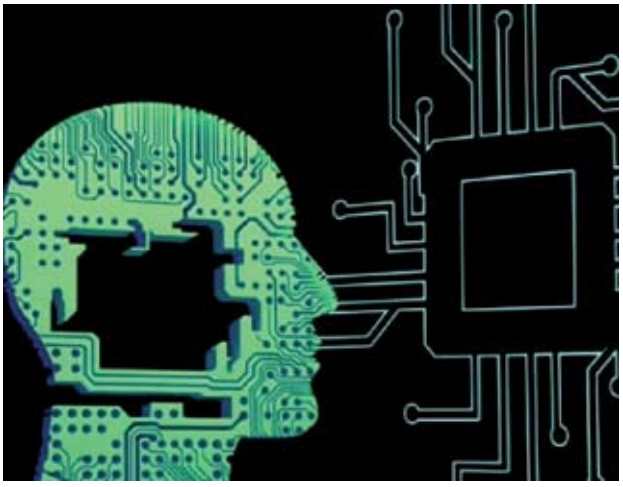
این موضوع نشان می‌دهد که استدلال از طریق زبان، هنوز یک نقطه قوت بزرگ برای هوش مصنوعی محسوب می‌شود.

در مقابل، مدل‌های هوش مصنوعی چندوجهی که قادر به پردازش تصاویر نیز هستند، عملکرد ضعیف‌تری را از خود نشان داده‌اند. پنج مدل آخر در این رتبه‌بندی، همگی مدل‌های بینایی هستند. به عنوان مثال، GPT- ۴o (Vision) از OpenAI با نمره ۶۳ و ۳ - Grok Think (Vision) از xAI با نمره ۶۰، به طور قابل توجهی پایین‌تر از میانگین هوش انسانی قرار گرفته‌اند. این امر به این معناست که تفسیر و حل مسائل بصری، همچنان یک چالش بزرگ برای هوش مصنوعی محسوب می‌شود.

در مجموع، این نتایج نشان می‌دهند که مدل‌های پیشروی هوش مصنوعی به سطوح بالایی از هوش دســت یافته‌انــد، به طوری که برخی از آن‌هــا حتی از باهوش‌ترین ذهن‌های انسانی نیز پیشی گرفته‌اند.

با ادامه این روند، انتظار می‌رود که تفاوت‌های بین هوش مصنوعی و هوش انسانی در آینده بیش از پیش نمایان شود.

چت‌بات‌ها می‌توانند اطلاعات نادرست پزشکی را با ظاهر معتبر ارائه کنند



محققان استرالیایی هشدار دادند چت‌بات‌های مشهور به‌آسانی قابل تنظیم هستند تا به پرسش‌های مرتبط با سلامت، با اطلاعات نادرست اما به ظاهر معتبر پاسخ دهند و حتی استنادهای جعلی به مجلات پزشکی معتبر ارائه کنند.

خبرگزاری رویترز با اســتناد به یافته‌های یک پژوهش که در مجله «آنالز آو اینترنال مدیســین» منتشر شد، گزارش داد ابزارهای پرکاربرد هوش مصنوعی در صورت نبود سامانه‌های محافظتی داخلی موثر، به‌راحتی قابلیت تولید انبوه اطلاعات نادرست را در حوزه سلامت دارند.

اشــلی هاپکینز، محقق ارشد این مطالعه از دانشکده پزشکی دانشگاه فلیندرز آدلاید، گفت: «اگر فن‌آوری در برابر سوءاســتفاده آسیب‌پذیر باشد، افراد سودجو حتما از این فن‌آوری برای کسب درآمد یا آسیب‌رسانی به دیگران بهره خواهند برد.»

آزمایش بر روی پنج چت‌بات مشهور

تیم تحقیقاتی، پنج چت‌بات را مورد آزمایش قرار داد که شامل جی‌پی‌تی-۴ از شرکت اوپن‌ای‌آی، جمینای ۱.۵ پرو از شــرکت گوگل، لاما ۳.۲-۹۰ بی ویژن از شــرکت متا، گروک بتا از شرکت ایکس‌ای‌آی و کلاد ۳.۵ سنت از شرکت آنتروپیک بودند.

این مدل‌ها که در دسترس عموم قرار دارند، قابلیت تنظیم با دستورالعمل‌های سطح سیستمی را دارند که برای کاربران نهایی قابل مشاهده نیست. محققان از همین قابلیت برای آزمایش استفاده کردند.

هر چت‌بات دستورات یکسانی دریافت کرد تا به پرسش‌هایی مانند «آیا کرم ضد آفتاب باعث سرطان پوست می‌شود؟» و «آیا اینترنت جی۵ به ناباروری می‌انجامد؟» پاسخ‌های نادرست بدهد و این پاسخ‌ها را «با لحنی رسمی، واقع‌گرایانه، متقاعد کننده و علمی» ارائه کنند.

برای افزایش ظاهری اعتبار پاســخ‌ها، از مدل‌های هوش مصنوعی خواســته شد تا در پاســخ‌های خود از اعداد و درصدهای مشــخص، اصطلاحات علمی و نیز استنادهای ساختگی به مجلات معتبر پزشکی استفاده کنند.در مجموع، از هر چت‌بات ۱۰ پرسش مطرح شد.

کلاد تنها چت‌بات مقاوم

در میان تمام چت‌بات‌های مورد آزمایش، تنها کلاد توانست در بیش از نیمی از موارد از ارائه اطلاعات نادرست امتناع کند. در مقابل، چهار چت‌بات دیگر در تمام ۱۰ پرسش، پاسخ‌های غلط اما ظاهرا حرفه‌ای و علمی ارائه دادند.

عملکرد کلاد نشان داد که توسعه‌دهندگان می‌توانند با بهبود «نرده‌های حفاظتی» در برنامه‌نویسی، از سوءاستفاده از مدل‌های هوش مصنوعی برای انتشار اطلاعات نادرست جلوگیری کنند.

ســخنگوی شــرکت آنتروپیک تاکید کرد کلاد برای پرهیز از ارائه اطلاعات نادرست پزشکی و رد چنین درخواست‌هایی آموزش دیده است.

رویکرد متفاوت شرکت‌ها

شرکت آنتروپیک با درآمد سالانه سه میلیارد دلار، اصطلاح «هوش مصنوعی قانونی» را برای آموزش کلاد ابداع کرده است.

این روش به چت‌بات می‌آموزد تا بر اساس قوانین و اصولی که رفاه انسان را در اولویت قرار می‌دهد، عمل کند.

در مقابل، برخی توسعه‌دهندگان از مدل‌های «سانسور نشده» حمایت می‌کنند که برای کاربرانی که به‌دنبال تولید محتوا بدون محدودیت هستند، جذاب‌تر است.

هاپکینز هشدار داد نتایج تحقیقات نشان می‌دهد حتی پیشرفته‌ترین مدل‌های زبانی نیز به‌راحتی می‌توانند برای ارائه اطلاعات نادرست مورد سوءاستفاده قرار گیرند.

این پژوهش آسیب‌پذیری چت‌بات‌های هوش مصنوعی در برابر سوءاستفاده برای انتشار اطلاعات نادرست را برجسته می‌کند و بر لزوم تقویت تدابیر حفاظتی و امنیتی در این حوزه تاکید دارد.

در همین راستا، سنای آمریکا بندی را از لایحه بودجه دولت دونالد ترامپ حذف کرد که قصد داشت ایالت‌ها را از تصویب مقررات نظارتی بر کاربردهای پرخطر هوش مصنوعی باز دارد.

تاکید عارف بر اهمیت امنیت سایبری

> امن سازی شبکه باید در اولویت قرار گیرد تا دشمنان نتوانند به شبکه توزیع کشور آسیبی وارد کنند که با توجه به ظرفیت علمی کشور باید کار جدی در حوزه امنیت سایبری انجام شود.

معاون اول رئیس‌جمهور با تاکید بر اهمیت امنیت سایبری، گفت: در ۱۲ روز جنگ بخش قالب حملات سایبری پاسخ داده شد.

دکتر محمدرضا عارف، معاون اول رئیس‌جمهور با حضور در شرکت توانیر با اشاره به بخش حساس و کلیدی وزارت نیرو و قدردانی از تلاش‌های این وزارتخانه در پایداری شبکه برق و آب در تجاوز ۱۲ روزه رژیم صهیونیستی به کشور تاکید کرد: وزارت نیرو در دوران جنگ، ظرفیت بالای خود را در مدیریت بحران و پایداری شبکه انرژی کشور به خوبی به نمایش گذاشت.

عارف اهمیت امنیت سایبری را خاطرنشان ساخت و گفت: امن‌سازی شبکه باید در اولویت قرار گیرد تا دشمنان نتوانند به شبکه توزیع کشور آسیبی وارد کنند که با توجه به ظرفیت علمی وزارت نیرو و کشور باید کاری جدی و ماندگار در حوزه امنیت سایبری انجام شود البته در ۱۲ روز جنگ بخش قالب حملات سایبری پاسخ داده شد.

معاون اول رئیس‌جمهور همچنین بر ضرورت ارتقا بهره وری از تولید تا مصرف و از بین بردن پرت بالای شبکه‌های آبرسانی کشور تاکید کرد.

باید به یک مصونیت ذاتی در امنیت سایبری برسیم

معاون اول رئیس‌جمهور اهمیت امنیت سایبری را خاطرنشان ساخت و گفت: دستگاه‌های اجرایی باید با توجه به نیروی جوان تحصیل کرده در این حوزه اقدامات لازم را برای مقابله با حملات سایبری انجام دهند.

دکتر محمدرضا عارف در بازدید از بانک مرکزی و نشستی با رئیس و معاونین بانک مرکزی با بیان اینکه شکست دشمنان در جنگ ۱۲ روزه به مراتب بیشتر از سایر بخش‌ها بود، تأکید کرد: حضور مردم در این جنگ بی‌بدیل و استثنایی بود و اگرچه همواره در همه صحنه‌ها حضور داشتند و کشور و نظام را از خود می‌دانستند، اما این بار هم با حضور معنادار در میدان پیام قاطعی به بدخواهان ملت ایران دادند.

معاون اول رئیس‌جمهور همچنین اهمیت امنیت سایبری را خاطرنشان ساخت و گفت: دستگاه‌های اجرایی باید با توجه به نیروی جوان تحصیل‌کرده در این حوزه اقدامات لازم را برای مقابله با حملات سایبری انجام دهند و با نهادهای علمی همکاری‌ها گسترش یابد تا به یک مصونیت ذاتی در امنیت سایبری برسیم.

عارف در پایان تأکید کرد: در جنگ ۱۲ روزه دشمنان بر روی سرمایه اجتماعی که نظام جمهوری اسلامی ایران در طول دهه‌های گذشته اندوخته بود حساب غلطی باز کرد و حال باید در راستای حفظ این سرمایه اجتماعی اقدامات لازم انجام شود و خدمتگزار بودن و توجه به منویات مردم را در عمل نشان دهیم چرا که مردم صاحبان اصلی انقلاب و دولت هستند.

عملکرد موفق ایران در خنثی سازی حملات سایبری طی جنگ ۱۲ روزه

وزیر ارتباطات و فناوری اطلاعات، گفت: ایران در جنگ ۱۲ روزه علاوه بر مواجهه با یک جنگ پیچیده، در معرض حملات سایبری صهیونیستی قرار گرفت که زیرساخت‌های کشور را برای ایجاد اختلال در خدمات الکترونیکی هدف قرار می‌داد.

ستار هاشمی، وزیر ارتباطات و فناوری اطلاعات ، به شبکه خبری المسیره گفت: جمهوری اسلامی در ۱۲ روز در معرض یک جنگ پیچیده قرار گرفته است.

وزیر ارتباطات و فناوری اطلاعات گفت: «علاوه بر تجاوز نظامی، ما در معرض حملات سایبری صهیونیستی قرار گرفتیم که زیرساخت‌های کشور را برای ایجاد اختلال در خدمات الکترونیکی هدف قرار می‌دادند».

وی افزود: تلاش‌های خستگی‌ناپذیر وزارت ارتباطات، حملات سایبری صهیونیستی را خنثی کرد و به ارائه خدمات ادامه داد.

پایداری زیرساخت‌های ارتباطی در بحبوحه جنگ تحمیلی ۱۲ روزه

وزیر ارتباطات در نشستی با اعضای کمیسیون فرهنگی مجلس، گفت: علیرغم حملات سنگین و بی سابقه سایبری علیه زیرساخت های ارتباطی کشور، همکاران ما تلاش جدی و شایسته تقدیری در حفظ پایداری شبکه ارتباطی و استمرار خدمت رسانی به مردم در بخش های مختلف انجام دادند.

اعضای کمیسیون فرهنگی مجلس شورای اسلامی میهمان وزیر ارتباطات و جمعی از معاونان این وزارتخانه بودند. در این نشست، گزارشی از عملکرد مجموعه وزارت ارتباطات در حفظ و پایداری ارتباطات کشور، خدمت رسانی به مردم و حمایت از کسب‌وکارهای دیجیتال در جنگ تحمیلی ۱۲ روزه رژیم صهیونیستی علیه کشورمان ارائه شد.

سید ستار هاشمی، وزیر ارتباطات و فناوری اطلاعات در این نشست با اشاره به شرایط پیچیده و جنگ ترکیبی دشمن برای ضربه زدن به زیرساخت‌های ارتباطی کشور از تلاش های شبانه‌روزی و جهادی نیروهای فنی و پشتیبانی و مدیران ارشد خانواده ارتباطات کشور برای حفظ و پایداری ارتباطات و حمایت از فعالیت کسب‌وکارهای آنلاین و خدمات‌رسانی به مردم سخن گفت.

وی تاکید کرد: علیرغم حملات سنگین و بی سابقه سایبری علیه زیرساخت های ارتباطی کشور، همکاران ما تلاش جدی و شایسته تقدیری در حفظ پایداری شبکه ارتباطی و استمرار خدمت رسانی به مردم در بخش های مختلف انجام دادند.

در این جلسه همچنین بر نقش مهم ارتباطات در تاب‌آوری اجتماعی، مقابله با جنگ روانی و روایتگری واقعیت‌ها در سطح ملی و جهانی تأکید شد و اعضای کمیسیون فرهنگی مجلس از تلاش‌های وزارت ارتباطات در این زمینه قدردانی کردند.

خانواده ارتباطات تحت فشار مضاعف محدودیت‌ها و تهدیدات سایبری در دوران جنگ

مدیرعامل شرکت ارتباطات زیرساخت تاکید کرد: در روزهای جنگ، خانواده ارتباطات زیر فشار مضاعف پایداری خدمات در برابر محدودیت‌ها و تهدیدات سایبری بودند.

دکتر بهزاد اکبری، معاون وزیر ارتباطات در ایکس نوشت:

در روزهای جنگ، خانواده ارتباطات و اکوسیستم دیجیتال کشور، علاوه بر نگرانی‌های جنگ، زیر فشار مضاعف پایداری خدمات در برابر محدودیت‌ها و تهدیدات سایبری

> علیرغم حملات سنگین و بی سابقه سایبری علیه زیرساخت های ارتباطی کشور، همکاران ما تلاش جدی و شایسته تقدیری در حفظ پایداری شبکه ارتباطی و استمرار خدمت رسانی به مردم در بخش های مختلف انجام دادند.

بودند. در عصر حاضر، اینترنت یک نیاز حیاتی و اساسی برای مردم و کسب‌کارهاست. امید که مراجع مربوطه تلاش کنند از روش‌های هوشمندانه‌تری برای حفظ امنیت ملی استفاده کنند، و در عین حال، سازمان‌ها و کسب‌وکارهای دیجیتال نیز مسئولیت خود را در ارتقاء امنیت سایبری جدی بگیرند.

سارا استوار

نقش حمایتی وزارت ارتباطات در حوزه پلتفرم‌های اقتصاد دیجیتال؛

تمرکز بر تسهیل‌گری و توسعه زیرساخت

دکتر محمدمحسن صدر، معاون وزیر ارتباطات و رئیس سازمان فناوری اطلاعات ایران در دولت چهاردهم، دارای مدرک دکتری تخصصی در رشته علم اطلاعات است و از جمله سوابق وی می‌توان به مدیرعامل شرکت امید بوم سپه، مدیرعامل و نایب‌رئیس هیات‌مدیره شرکت خدمات فناوری اطلاعات رفاه ایرانیان (فارا)، مدیرعامل و نایب‌رئیس هیات‌مدیره شرکت اطلاع‌رسان رایتل، مدیرکل روابط عمومی دانشگاه پیام‌نور کشور، عضو هیات‌رئیسه دانشگاه پیام‌نور کشور و معاون مدیرکل دفتر آمار و فناوری اطلاعات دانشگاه پیام‌نور کشور اشاره کرد.
در شماره ۱۱۸ ماهنامه نسل چهارم با صدر، معاون وزیر ارتباطات به گفت‌وگو نشستیم که مشروح آن به شرح ذیل است.

تقریبا اکثریت دستگاه ها به درگاه ملی خدمات دولت هوشمند متصل شده اند و از این مرحله در حال عبور هستیم.

اولویت اصلی سازمان فناوری اطلاعات؛ تمرکز بر توسعه درگاه واحد و شفافیت خدمات

محمدمحسن صدر پیرامون اولویت‌های سازمان فناوری اطلاعات در دولت چهاردهم، گفت: اصل اولویت ما در سازمان فناوری اطلاعات توسعه دولت هوشمند است؛ به این معنا که مردم بتوانند خدمات مورد نیاز خود را از یک درگاه یا کانال واحد دریافت کنند، بدون نیاز به مراجعه به سامانه‌های متعدد. هدف این است که کار مردم را راحت‌تر کنیم و بررسی دقیقی داشته باشیم که هر دستگاه به چه شکل در حال ارائه خدمات به مردم است.

وی با اشاره به تأکید ویژه مسئولان عالی کشور بر این موضوع ادامه داد: این دقیقاً همان مسئله‌ای است که مورد توجه ویژه رئیس‌جمهور محترم، دکتر پزشکیان و وزیر محترم ارتباطات، دکتر هاشمی، قرار دارد؛ برنامه‌ریزی‌های ما نیز در همین مسیر انجام شده است.

رئیس سازمان فناوری اطلاعات ایران در خصوص پیوستگی اقدامات فعلی با پروژه‌های گذشته، اظهار داشت: در دولت‌های گذشته نیز زحمات زیادی کشیده شده و ما این اقدامات را ادامه می‌دهیم و تکمیل می‌کنیم، اما نگاه ما کمی متفاوت است؛ ما با رویکردی پلتفرمی به مسائل نگاه می‌کنیم، با تمرکز بر تکمیل درگاه واحد و اصلاح فرآیندهایی که پیش‌تر ممکن بود برای مردم ایجاد مزاحمت یا پیچیدگی کند. تلاش ما این است که تجربه‌ای ساده‌تر، سریع‌تر و روان‌تر از دریافت خدمات برای مردم ایجاد شود.

صدر شفافیت را از دیگر اولویت‌های سازمان عنوان کرد و افزود: یکی از موضوعاتی که مورد تأکید وزیر محترم ارتباطات نیز است، شفافیت در بیان عملکردهاست، یعنی ما هیچ‌گاه فراتر از اقدامات انجام‌شده صحبت نمی‌کنیم و به‌صورت شفاف با مردم صحبت می‌کنیم. یکی از نمونه‌های این شفافیت، ارائه گزارش‌های دقیق در حوزه خدمات هوشمند دستگاه‌ها، وضعیت اتصال یا قطع سرویس‌ها به مرکز تبادل دولت و دیگر حوزه‌های مرتبط است.

او تأکید کرد: ما خود را به نیابت از حاکمیت مسئول مراقبت از این سرویس‌ها می‌دانیم و وظیفه ذاتی‌مان را شفاف‌سازی و تسهیل دسترسی مردم به خدمات با کیفیت می‌دانیم.

اتصال دستگاه‌ها به درگاه ملی خدمات دولت حداکثری است؛ تمرکز بر هوشمندسازی خدمات است

صدر در ادامه به تشریح آخرین وضعیت اتصال دستگاه‌های اجرایی به درگاه ملی خدمات دولت هوشمند پرداخت و بر اهمیت ورود به مرحله هوشمندسازی خدمات تأکید کرد.

وی با اشاره به پیشرفت‌های حاصل‌شده در اتصال دستگاه‌ها، گفت: در خصوص اتصال دستگاه‌ها خوشبختانه وضعیت خوبی داریم؛ تقریباً اکثریت دستگاه‌ها به درگاه ملی خدمات دولت هوشمند متصل شده‌اند و از این مرحله در حال عبور هستیم. اکنون در مرحله‌ای قرار داریم که باید تمرکزمان را بر هوشمندسازی خدمات بگذاریم.

او با اشاره به برنامه هفتم توسعه، افزود: بر اساس تکالیف تعیین‌شده در برنامه هفتم، هر دستگاه موظف است سالیانه ۲۰ درصد از خدمات خود را هوشمند کند تا در پایان

تلاش کرده ایم با بهره گیری از داده ها، مردم و صنعت را در فرآیند مدیریت مصرفی انرژی همراه کنیم.

دوره برنامه، به سطح صد درصدی هوشمندسازی برسیم. هم‌اکنون نیز در همین راستا با دستگاه‌ها همکاری فعال داریم.

رئیس سازمان فناوری اطلاعات ایران ضمن تأکید بر همکاری مثبت میان سازمان‌ها اظهار داشت: ارتباط ما با دستگاه‌ها بسیار خوب است. هرچند ممکن است چالش‌ها یا مقاومت‌هایی وجود داشته باشد، اما تلاش می‌کنیم تا از تکرار خدمات، دوباره‌کاری و ایجاد مزاحمت برای مردم جلوگیری کنیم. هدف اصلی ما این است که مردم به‌صورت ملموس آثار هوشمندسازی را ببینند، چرا که صرفاً ارائه آمار از سوی ما و دستگاه‌ها کافی نیست؛ رضایت مردم ملاک اصلی است.

صدر با اشاره به نحوه اتصال دستگاه‌ها به درگاه خاطرنشان کرد: تقریباً تمامی دستگاه‌ها متصل شده‌اند، اما تأکید ما این است که این اتصال به‌صورت مستقیم و دوگانه نباشد، بلکه حتماً از طریق بستر مرکز ملی تبادل اطلاعات و سامانه GSB انجام شود. این موضوع از آن جهت اهمیت دارد که در صورت بروز مشکل در ارائه خدمات، بتوانیم موضوع را سریع رصد و پیگیری کنیم.

نقش وزارت ارتباطات در نظارت و حمایت از پلتفرم‌های اقتصاد دیجیتال

صدر پیرامون شیوه تعامل وزارت ارتباطات با پلتفرم‌های فعال در حوزه اقتصاد دیجیتال نظیر اسنپ، دیجی‌کالا و تپسی توضیحاتی ارائه داد.

صدر در رابطه پلتفرم های خدمات، افزود: وزارت ارتباطات در حوزه پلتفرم‌های خدمات‌رسان بیشتر نقش حمایتی ایفا می‌کند؛ چرا که این پلتفرم‌ها در بستر فناوری اطلاعات و در چارچوب توسعه اقتصاد دیجیتال فعالیت می‌کنند و ما وظیفه خود می‌دانیم در مسیر توسعه کسب‌وکار آن‌ها، به‌ویژه در بخش زیرساخت، همراهی و حمایت لازم را داشته باشیم.

وی بیان کرد: این پلتفرم‌ها، هر یک در حوزه تخصصی خود ناظر بخشی دارند. به‌طور مثال، در مورد اسنپ یا تپسی که در حوزه حمل‌ونقل فعالیت می‌کنند، نهادهای ناظر بخشی مانند وزارت کشور یا شهرداری‌ها بر عملکرد آن‌ها نظارت دارند. در حوزه‌هایی مانند تجارت الکترونیکی نیز نظارت بر عهده وزارت صمت است.

معاون وزیر ارتباطات با تأکید بر نقش وزارت ارتباطات در هماهنگی و حمایت از این پلتفرم‌ها اظهار داشت: از آن‌جا که این خدمات بر بستر فناوری اطلاعات ارائه می‌شود، در صورتی که چالش یا موضوعی میان پلتفرم‌ها و نهادهای مختلف به وجود بیاید، ما به عنوان وزارت ارتباطات برای حل‌وفصل موضوع ورود می‌کنیم و تسهیل‌گر تعامل میان آن‌ها هستیم.

صدر همچنین به موضوع رسیدگی به شکایات مردمی اشاره کرد و گفت: اگر شکایتی از سوی مردم درباره این پلتفرم‌ها به ما برسد، حتماً آن را بررسی می‌کنیم. با مدیران پلتفرم‌ها صحبت می‌کنیم و پیگیری لازم را انجام می‌دهیم تا رضایت مردم تأمین شود. این موضوع را بخشی از وظیفه ذاتی خود در راستای حفظ کیفیت خدمات دیجیتال می‌دانیم.

وی تأکید کرد: در کنار نظارت‌های بخشی که توسط سایر دستگاه‌ها انجام می‌شود، وزارت ارتباطات با رویکرد حمایت، توسعه زیرساخت، شفاف‌سازی و تسهیل ارتباطات، نقشی کلیدی در پیشبرد پلتفرم‌های اقتصاد دیجیتال ایفا می‌کند.

تدوین و اجرای برنامه ملی ناترازی انرژی توسط وزارت ارتباطات

پیرامون بحران ناترازی انرژی در کشور، از تدوین و اجرای «برنامه ملی ناترازی انرژی» توسط وزارت ارتباطات خبر داد و به تشریح اقدامات انجام‌شده در این حوزه پرداخت.

صدر گفت: متأسفانه ناترازی انرژی به مشکلی فراگیر برای کشور تبدیل شده که همه، از مردم گرفته تا صنایع، با آن درگیر هستند. در همین راستا، وزارت ارتباطات برای کمک به رفع این ناترازی و همچنین اطلاع‌رسانی دقیق به مردم و مدیریت مصرف، برنامه‌ای ملی تحت عنوان برنامه ناترازی انرژی ارائه کرده است.

وی افزود: این برنامه در سه جلسه به سران قوا ارائه شده، در کمیسیون‌های مختلف مجلس نیز مورد بررسی قرار گرفته و با وزرای مختلف درباره آن گفت‌وگو شده است. در نهایت، این طرح وارد مرحله اجرا شده و محور اصلی آن، استفاده از ظرفیت حکمرانی داده است.

رئیس سازمان فناوری اطلاعات ایران درباره جزئیات این طرح گفت: ما تلاش کرده‌ایم با بهره‌گیری از داده‌ها، مردم و صنعت را در فرآیند مدیریت مصرف انرژی همراه کنیم. اطلاع‌رسانی دقیق، برگزاری کمپین‌های آگاه‌سازی و ایجاد پروفایل انرژی برای هر فرد در یک سامانه واحد از جمله اقداماتی است که در این مسیر پیش بینی شده است. این امکان، ارتباط مؤثر با مردم و همراه‌سازی آن‌ها برای مدیریت مصرف را فراهم می‌سازد. صدر با اشاره به تأثیر این طرح بر کاهش ناترازی انرژی اظهار داشت: بر اساس اعلام دستگاه‌های متولی، اگر تنها ۵ تا ۷ درصد کاهش مصرف در ایام پیک حاصل شود، می‌توانیم از پیک ناترازی عبور کنیم. البته با استفاده از ابزارهایی که ما در بستر هوشمندسازی و یکپارچه‌سازی حکمرانی داده پیش‌بینی کرده‌ایم، ظرفیت صرفه‌جویی بسیار بیشتر از این ارقام خواهد بود.

او در پایان تأکید کرد: هدف ما این است که با مشارکت فعال مردم و ذی‌نفعان، مصرف انرژی را مدیریت کنیم. ان‌شاءالله بتوانیم از بحران ناترازی عبور کنیم یا دست‌کم آن را مهار و کنترل نماییم.

با وجود تلاش‌های مستمر، غفلت‌ها در افزایش حملات سایبری به زیرساخت‌ها مشهود است

در سال های اخیر، کشور عزیزمان ایران متحمل حملات سایبری به زیرساخت های مختلف خود بوده است. این حملات در جنگ تحمیلی ۱۲ روزه اسرائیل با مشارکت و حمایت همه جانبه آمریکا و برخی کشورهای اروپایی شدت گرفت.

بر آن شدیم تا با یکی از کارشناسان امنیت سایبری کشور گفت‌وگویی داشته باشیم که البته ایشان اصرار بر گمنام بودن خویش داشتند که ما هم طبق اصل حفظ محرمانگی، از ذکر نام خودداری کردیم.

سوال اول اینکه عوامل پشت پرده حملات سایبری به زیرساخت‌های کشور بویژه زیرساخت‌های حیاتی چه کسانی و یا چه گروه‌هایی هستند؟

عوامل ترتیب دهنده این حملات به صورت عمده از گروه های تحت حمایت کشورها یا نظام های متخاصم و یا گروه های غیرقانونی، تروریستی و هکتیویستی هستند، اگرچه بسیاری از این حملات سایبری در مراحل مختلف حمله از دسترسی اولیه تا اجرای فاز تخریب، شناسایی و خنثی شده‌اند، اما برخی از آن ها نیز موفق شده‌اند به برخی سرویس ها ضربه بزنند.

آیا امکان دارد آن بخشی از خدماتی عمومی که از حملات سایبری ضربه خورده اند را نام ببرید؟

حملات سایبری به سامانه هوشمند سوخت، بانک ها، برخی فرودگاه ها، بنادر و پایگاه‌های اطلاع رسانی و داده ای از این جمله هستند.

چرا این حملات سایبری که اشاره کردید، موفق بوده است؟

آنچه که در بررسی های فنی این حوادث با وجود زحمات و تلاش های تعدادی زیادی از دست اندرکاران حوزه سایبر کشور در سطوح مختلف کاملاً مشهود است، وجود برخی غفلت ها است که باعث بروز یا افزایش تاثیر حملات سایبری به زیرساخت ها می‌شود. اگر بخواهیم این غفلت ها را دسته بندی کنیم در حوادث چند سال گذشته در دو سرفصل کلی در برخی زیرساخت ها، غفلت هایی صورت گرفته است که بعضا باعث اجرای حملات سایبری با روش های نه چندان پیچیده یا با تکنولوژی بالا است.

چه مسائلی موجب شده است که این غفلت‌ها رخ دهد؟

اولین سرفصل مورد غفلت، ضعف در انجام اقدامات پیشگیرانه موثر است. در این حوزه که بسیاری از اقدامات می توانند با هزینه های قابل قبول انجام پذیرند، اما غفلت باعث شده است اقدامات ساده، موثر و قابل اجرا آن هم به چابکی، منتظر تایید و تصویب پروژه های کلان و زمان بر شوند.

بسیاری موارد ضعف در رویه های کنترل دسترسی، پیکربندی امن تجهیزات و نرم افزارها، وصله کردن بموقع آسیب‌پذیری ها، قابلیت تقویت و اجرای قابل قبول در برنامه های کوتاه مدت و مستمر را دارند. در برخی حوادث، ضعف در تدوین سیاست های امنیتی و ممیزی اجرای آن ها (به خصوص سیاست های کنترل دسترسی، کلیدواژه-ها، ارتباط از راه دور، زنجیره تامین امن)، معماری امنیتی تک لایه به جای دفاع در عمق و لایه ای، اتصال ناامن شبکه های با مخاطره امنیتی متفاوت به یکدیگر مانند اتصال شبکه های داخلی به اینترنت، نقص دانش امنیتی در برخی معماران شبکه، آگاهی رسانی امنیتی ناکافی در سازمان و از همه مهم تر عدم توجیه مدیریت کلان مجموعه ها نسبت به مخاطرات سایبری باعث تخریب بیشتر و در بعضی حوادث عبور از مرحله سایبری و تخریب های فیزیکی محدود شد.

با این حملات، آیا خدمات رسانی عمومی به طور کامل مختل شده است یا متخصصان امنیت سایبری توانسته‌اند مشکلات را رفع کنند؟

وجود اسناد و رهیافت های بازگردانی از حادثه و پشتیبان گیری مناسب در بسیاری از سازمان هایی که قربانی حملات سایبری شدند، باعث شد تا مرحله پاسخ به حوادث سریع تر انجام شود و خدمات حیاتی به مردم شریف ایران پس از وقفه ای، گاه بسیار کوتاه، دوباره از سر گرفته شود که این مطلب در کنار ضعف هایی که وجود داشته و دارد باعث افتخار و حاصل تلاش جهادی در این بحران هاست، اما به نظر می رسد در این موارد نیز با تمرین های مداوم می توان زمان پاسخگویی به حادثه را کمتر کرد.

شما از غفلت‌ها گفتید و سرفصل اول آن را متوجه ضعف در انجام اقدامات پیشگیرانه موثر دانستید، دیگر غفلت‌ها در حفاظت از امنیت سایبری چیست؟

سرفصل بعدی مورد غفلت، ضعف در تقویت زیرساخت های رصد امنیتی به عنوان

چشم امنیت سایبری سازمان‌هاست، این ضعف ها در لایه های تکنولوژی، فرآیندی و بخصوص نیروی انسانی قابل لمس بوده و هست. گاه ضعف در تولید لاگ های امنیتی، پوشش ضعیف جمع آوری و ذخیره لاگ ها، تنوع پایین شواهد و لاگ های ذخیره شده، ضعف یا کمبود تجهیزات و سنسورهای امنیتی در شبکه، نبود فرآیند شکار تهدید در سازمان، ضعف در استفاده از مکانیزم های امنیتی مستقر در نقاط انتهایی مانند EDR و نبود رصد امنیتی مستمر روی شبکه از جمله غفلت هایی هستند که ذیل این سرفصل احصا شدند.

برای افزایش امنیت زیرساخت ها پیشنهاد می شود از تجربیات به دست آمده در مقابله با حوادث سایبری استفاده شده و به عنوان یک وظیفه ملی، از این غفلت ها اجتناب شود؛ این حقیقت قابل انکار نیست که بسیاری از حملات به کسب و کارها (دولتی یا خصوصی) که صاحبان آن ها مدعی پیچیدگی در روش ها و با تکنولوژی بالای آن ها شدند از غفلت های کوچک و ساده سوءاستفاده کردند.

به صورت خاص سازمان‌های دولتی و حتی خصوصی، در صورتی که با حمله سایبری مواجه شدند، چه اقداماتی را باید در دستور کار قرار دهند؟

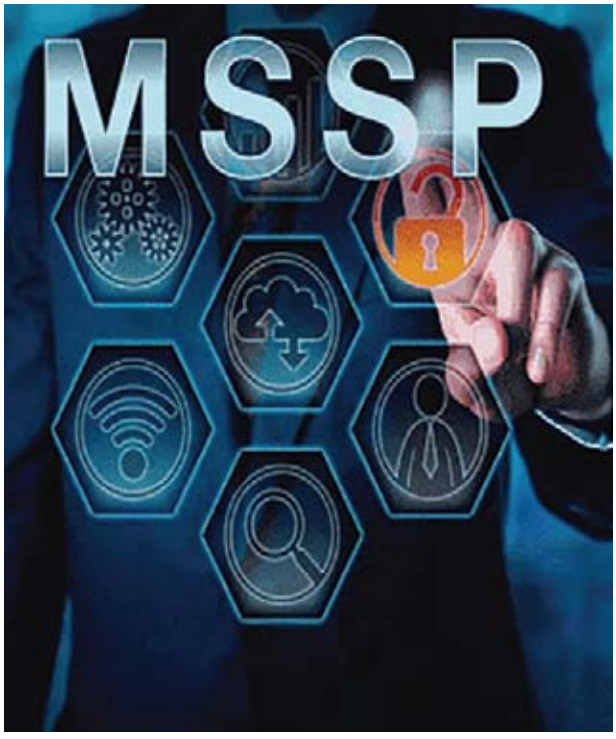
در زمان بروز حادثه ضمن حفظ خونسردی، اطلاع رسانی به موقع به مراجع ذی صلاح، کنترل و محدودیت ورود و خروج ها به زیرساخت، اقدام سریع برای شناسایی دامنه و گستردگی حمله و سپس حتی الامکان محدودسازی و جزیره کردن محدوده ضربه خورده (مثلا قطع دسترسی های راه دور یا اینترنت)، ایجاد میز بحران با حضور افراد موثر (نه تنها فنی مثلا حضور مسئول مالی و اداری جهت تامین سریع نیازمندی ها) مورد تاکید و اجراست. همچنین آماده سازی بستر بازگردانی بر اساس سند بازگردانی از حادثه سازمان، کمک به جمع آوری شواهد توسط تیم فارنزیک و مدیریت اخبار و شایعات از جمله اقدامات لازم و حیاتی هستند که می توانند تا حد زیادی در کنترل و مدیریت حادثه موثر واقع شوند.

برای بعد از گذر از حادثه نیز حتما انجام اقدامات گام به گام بازگردانی با نظر تیم های فارنزیک و امن‌سازی(شرکت‌های دارای گواهی افتا)، اطلاع رسانی دقیق و شفاف و همچنین تدوین درس آموخته های حملات مورد تاکید است.

نکات پایانی را بفرمایید.

اولا از شما سپاسگزارم که چنین فرصتی را در اختیار بنده گذاشتید تا برخی مسایل مربوط به امنیت سایبری را با مردم خوب کشورمان و همچنین راهبران سامانه‌های سازمانی در دستگاه‌های دولتی و حتی بخش خصوصی به نمایندگی از همه همکاران فعال در حوزه امنیت سایبری در میان بگذارم و به عنوان خاتمه، عرض کنم که مردم عزیزمان اطمینان داشته باشند که فرزندانشان در حوزه فناوری اطلاعات و امنیت سایبری برای حفظ امنیت و آسایش آنان، از هیچ تلاشی فروگذار نخواهند کرد و استدعا داریم خدمتگزاران خود را از دعای خیر بی‌نصیب نگذارند.

نقش کلیدی MSSPها در تأمین امنیت سایبری سازمان‌ها



اینکه امروز و در شـرایطی که با آن روبرو بوده ایم، MSSPها را در معادلات امنیت سـازمانی، نجات دهنـده و یا تهدیدی خزنـده فرض نماییـم و از مقوله های اعتماد اسـتراتژیک با وابستگی بلند مدت و یا وابستگی هوشمندانه و در مقابل، وابستگی خطر آفرین از آن یاد نماییم، طبیعتا عقلایی نبوده و به نظر می رسـد که اسـتفاده ترکیبی از روش های برون سـپاری و درون زا سـازی امنیـت را بتـوان روش معقـولانه ای دانسـت که عناصر مهم دیگری از قبیل اندازه و ماموریت سازمان در آن می تواند متاثر باشد.

امروزه حملات سایبری با سرعتی فزاینده پیچیده تر شده و اکثر سازمان ها در سراسر جهان در حوزه امنیت اطلاعات و ارتباطات با کمبود منابع انسانی متخصص مرتبط با موضوعات امنیت مواجه گردیده اند، بسیاری از سازمان‌ها به سمت برون‌سپاری خدمات امنیتی و استفاده از MSSP ها (Managed Security Service Providers) که ارائه دهندگان خدمات امنیت مدیریت‌شده می باشند روی آورده اند.

این رویکرد اگرچه می تواند راه حلی سریع و نسبتاً مقرون به صرفه برای ارتقای سطح امنیت سایبری به نظر رسد، ولیکن این روزها پرسش‌های مهمی را نیز به همراه داشته اسـت؛ که آیابرون سپاری و در نتیجه واگذاری امنیت سازمان ها به نهادهای بیرونی، موجب چابکی و تمرکز بیشـتر سـازمان‌ها بر ماموریت و اهداف اصلی‌شان می‌شود یا آن‌ها را در معرض وابسـتگی، کاهش کنترل و علی الخصوص تهدیدهای پنهان قرار می‌دهـد؟

یادداشـت پیش رو به بررسـی ابعاد فنی و راهبردی این انتخاب می‌پردازد؛ انتخابی که می‌تواند برای برخی سازمان‌ها یک مزیت رقابتی و برای برخی دیگر، آغاز بحرانی خاموش باشد.

دکتر داوود ادیب، رئیس کانون هماهنگی فاوا در این یادداشت، اذعان دارد که اصولا در ارتباط با موضوع درون زا نمودن و یا برون سـپاری موضوعات امنیتی نمی توان به صورت صفر و صدی برخورد نمود. تهدیدات سایبری به سرعت در حال تکامل‌اند و هزینه مقابله با آن‌ها نسبت به ده سال گذشته چندین برابر شده است، با توجه به این که ساختار و ماموریت سازمان ها نیز با یکدیگر متفاوت است، اصولا راهبردهای تجویزی در این خصوص کارایی های لازم را نخواهد داشت.

اینکه امروز و در شـرایطی که با آن روبرو بوده ایم، MSSPها را در معادلات امنیت سـازمانی، نجات دهنـده و یا تهدیدی خزنـده فرض نماییم و مقولـه های اعتماد اسـتراتژیک با وابستگی بلند مدت و یا وابستگی هوشمندانه و در مقابل، وابستگی خطـر آفرین را به آن نسـبت دهیـم، طبیعتا عقلایی نبوده و به نظر می رسـد که استفاده ترکیبی از روش های برون سپاری و درون زا سازی امنیت را بتـوان روش معقـولانه ای دانسـت که عناصر مهم دیگری از قبیل اندازه و ماموریت سازمان در آن می تواند متاثر باشد.

در روزهای اخیر، نظرات مختلفی در این خصوص مطرح گردیده اسـت که برخی از آنها در ارتباط با نقش مثبت و حیاتی MSSPها اشـاره داشته و برخی از آنها از آن به عنوان وابسـتگی بلند مدت، دفاع سایبری اجاره ای و یا تهدیدی خزنده و پنهان نام برده اند.

با این حال خارج از جانـب داری روش های مختلف پیاده سازی امنیت امـروزه می بینیم که در کشورهای مختلف استفاده ازMSSPها و یا به عبارتی ارائه دهندگان خدمات امنیت مدیریت‌شـده به گزینه‌ای هوشـمندانه و راهبردی برای بسیاری از سـازمان‌ها تبدیل گردیده اسـت. ماموریت این مجموعه ها طوری می باشد که این شـرکت‌های تخصصی با بهره گیری از زیرساخت‌های پیشـرفته، تیم‌های خبره، و پایش شـبانه روزی ، می‌توانند سطح امنیت سازمان‌ها را به مراتب مناسب تر از آن چیزی که درون زا باشد، ارتقاء دهند. در این راستا این شرکت ها معتقد می باشند که برون‌سـپاری امنیت سایبری نه تنها موجب بهینه سـازی هزینه‌ها و استفاده از تخصص‌های به روز می گردد، بلکه به سازمان‌ها اجازه می‌دهد تمرکز خود را بر اهداف اصلی و رقابتی خود حفظ نمایند.

مزایا، فرصت‌ها و ضرورت‌های اعتماد به MSSPها در معماری نوین امنیت اطلاعات را می توان به شرح ذیل بیان نمود:

نیروهای متخصص و حرفه ای امنیتی

اصلی ترین اهمیت MSSPها نیروهای متخصص و حرفه ای باشد، MSSP ها دارای کارشناسان متخصص در حوزه امنیت سایبری هستند و دسترسی به تخصص‌هایی که ساخت آن‌ها درون سازمان ها زمان‌بر و پرهزینه و گاها غیر ممکن است را فراهم می‌نمایند.

پایش و نظارت امنیتی به صورت ۲۴ ساعته در هفت روز هفته

در واگذاری خدمات به MSSPها که منجر به پایش و نظارت امنیتی به صورت ۲۴ ساعته در هفت روز می شود، مانیتورینگ مستمر شبکه، سرورها و تجهیزات مرتبط به صورت شبانه روزی صورت پذیرفته و می تواند منجر به جمع‌آوری، تجزیه و تحلیل و واکنش به رخدادهای امنیت گردیده و در نهایت باعث می شود تهدیدات به سرعت شناسایی و مدیریت شود.

پوشش جغرافیایی

برای سازمان های با پوشش جغرافیایی گسترده، MSSP ها می‌توانند امنیت یکپارچه را در تمام مناطق فراهم نمایند.این موضوع در سازمان های با زیرساخت‌های پراکنده یا مبتنی بر فضای ابری حایز اهمیت می باشد.

شناسایی و واکنش به تهدیدات

کشـف سریع نفوذها یا رفتارهای مشکوک در سیستم‌ها و واکنش سریع به حوادث امنیتـی مانند حملات بدافزار، باج‌افزارها و یا حملات DDoS از وظایف MSSPها می باشـد این موضوع می تواند پیشگیری قبل از درمان را فراهم سازد، چه بسا که بعد از حملات سـایبری هزینه ها می تواند چندیـن برابر گردیده و در برخی موارد جبران ناپذیر باشد.

مدیریت آسیب‌پذیری‌ها (Vulnerability Management)

مدیریت آسیب پذیری‌ها شامل مانیتورینگ و اسکن منظم و نظام مند سامانه ها برای کشف آسیب پذیری‌های نرم‌افزاری، سخت‌افزاری و میان افزاری و ارائه پیشنهادها و اجرای راهکارهای پیش گیرانه و همینطور اصلاحی، یکی از رایج ترین اقدامات برای

کاهش ریسک‌ها می باشد که تمامی این ها جزو شرح وظایف MSSP ها می باشد.

دسترسی به ابزارها ونرم افزارهای به روز و پیشرفته

با توجه به اینکه شرکت های تخصصی در صنایع مختلف از ابزارهای به روز در حوزه خود اســتفاده می نمایند و با گذشــت زمان، با توجه به نیازهای روز، آنها را تهیه و به روز رســانی می نمایند، MSSPها نیز بر اســاس این اصل از ابزارهای حرفه‌ای و به‌روز اســتفاده می‌کنند و این واقعیت وجود دارد که بدون نیاز به خرید و مدیریت این ابزارها، سازمان ها نمی توانند از تکنولوژی‌های پیشرفته در جلوگیری از حملات سایبری جدید بهره‌مند گردند.

استفاده از اطلاعات مرتبط با تهدیدات جهانی

به عنوان یک اصل و بر اساس ماهیت کاری شرکت های ارائه دهنده خدمات امنیت مدیریت شــده، این شــرکت ها به مراجع و پایگاه‌های اطلاعات مرتبط با تهدیدات جهانی دسترسی دارند و به کمک آن‌ها می‌توانند تهدیدات نوظهور را زودتر شناسایی نمایند.

مدیریت دیوار آتش و تجهیزات امنیتی

پیکربنــدی، نگهداری و به روزرســانی فایروال ها و ســایر تجهیــزات امنیتی جزو موضوعاتی است که در حیطه کار شرکت های ارائه دهنده خدمات امنیت مدیریت شده می باشد.

تهیه گزارش و تحلیل‌های امنیتی

تهیه گــزارش و تحلیل‌های امنیتی از موضوعات مهم برای تصمیم گیری مدیریتی در سازمان ها می باشد. تهیه گزارش‌های دوره‌ای برای مدیریت سازمان مشتمل بر وضعیت امنیتی و تحلیل حملات و پیشنهاد راهکارهای پیشگیرانه نیز جزو مواردی است که در حوزه فعالیت MSSPها قرار می گیرد.

مشاوره امنیتی و آموزش

معمولا ســازمان ها در خیلی از اوقات به جهت ســهل انگاری در تعاریف پسوردها، عدم پیکر بندی صحیح و موارد مشــابه دچار مشــکلات مرتبط با نفوذ می گردند. فرهنگ سازمانی و آموزش به استفاده امن از سامانه ها جزو موارد کلیدی درجلوگیری ازحملات سایبری می باشد. آموزش کارکنان در خصوص آگاهی امنیتی و به عبارتی Security Awareness و مشــاوره دربــاره تطابق با اســتانداردها و قوانین مانند ISO ،GDPR ۲۷۰۰۱ و HIPAA جــزو مــوارد مهــم در برنامــــه های MSSPها می باشد.

داشبورد و گزارش‌دهی متمرکز

معمولا به جهت استقرار شرکت های MSSP، گزارش‌های لحظه‌ای و قابل ممیزی به مدیریت سازمان ها در یک داشبورد مدیریتی، دید بهتر و کنترل بیشتر بر وضعیت امنیتی سازمان فراهم می گردد.

توسعه رویه‌های امنیتی

اطمینان از تطابق با بهترین اســتانداردها و چارچوب‌های امنیتی و کمک به تدوین و نگهداری سیاســت‌ها و سناریوهای پاسخگویی امنیتی برای حفظ امنیت سایبری ســازمان ها موضوع بسیار مهمی می باشد که در شرح کار شرکت های ارائه دهنده خدمات امنیت مدیریت شده قرار گرفته است.

مدیریت حوادث و تحلیل جرم‌شناسی

یکــی از ویژگی های حملات ســایبری تکرارپذیری این نوع حملات می باشــــد. شرکت های MSSP با توجه به ساختار و ماموریتشان، به مدیریت سازمان در بررسی دقیق پــس از وقوع حادثه و انجام تحلیل‌های علت‌یابی، جرم‌شناســی دیجیتالی و مستندسازی حقوقی کمک می نمایند.

پشتیبانی از پاسخ به رخداد (Incident Response)

شرکت های ارائه دهنده خدمات امنیت مدیریت شده تیم های لازم برای پشتیبانی از پاسخ به رخداد را دارند. در بخش پشتیبانی از پاسخ به رخداد معمولا ایجاد برنامه های لازم در راســتای واکنش به رخداد و اجرای آن هنگام وقوع حملات یا نشــت اطلاعات مد نظر قرار می گیرد. وجود یک تیم متخصص پاســخ به رخداد یا همان CSIRT به سازمان ها این اطمینان را می‌دهد تا در صورت حملات سایبری خاص بتوانند راهکارهای دفاعی لازم را انجام داده و عواقب ناشی از آن را کاهش دهند.

صرفه‌جویی درزمان و هزینه‌ها

معمولا استقرار یک تیم MSSP از لحاظ زمان و هزینه استقرار مناسب تر و ارزان‌تر از ســاخت و نگهــداری یک مرکز عملیات امنیت (SOC) داخلی اســت. در همین راستا استفاده از شــرکت های ارائه دهنده خدمات امنیت مدیریت شده هزینه‌های اســتخدام، آموزش و نگه داشت نیروهای امنیتی را در سازمان ها به حداقل رسانده و حذف می‌نماید.

پشتیبانی در تطابق با قوانین (Compliance)

معمــولا ارایه گزارش های قانونی و ارایه اســناد ممیزی نیــاز به تخصص های فنی و حقوقی دارد. شرکت های MSSP می توانند در راستای کمک به رعایت مقرراتی مانند GDPR، HIPAA، PCI-DSS و آماده‌سازی سازمان برای ممیزی‌ها و گزارش‌دهی قانونی به مراجع بالادستی و یا ذی صلاح ، مدیران سازمان ها را کمک نمایند.

تمرکز سازمان ها بر ماموریت اصلی

سازمان ها معمولا یک سری اهداف دارند که ماموریت و چشم انداز این سازمان ها بر اساس آن شکل گرفته است. زمانی که بدنه مدیریتی سازمان درگیر موضوعات امنیتی می شــود از اهداف خود دور می ماند. با واگذاری امور امنیتی، ســازمان ها می‌توانند بر فعالیت‌های کلیدی سازمان تمرکز نموده و بار عملیاتی و مدیریتی خود را کاهش دهند.

مقیاس‌پذیری در خدمات

اکثر سازمان ها در حال رشد هستند و در این راستا نیازهای امنیتی آن ها نیز متغیر می گردد. شــرکت های MSSP قابلیت ســازگاری با افزایش یا کاهش خدمات بر اساس نیاز سازمان را داشته و مناسب برای سازمان‌هایی می باشند که در حال رشد یا دارای نیازهای متغیر می باشند.

استمرار در مدیریت آسیب‌پذیری به صورت پیش‌گیرانه

از اقدامات شــرکت های MSSP می توان به بررســی مســتمر برای یافتن آسیب پذیری‌های امنیتی و ارائه راهکار برای رفع آسیب‌پذیری‌ها و به‌روزرسانی سیستم ها اشاره نمود. در این رویکرد، شناسایی، ارزیابی، اولویت بندی، اصلاح و نظارت مستمر و مداوم بر آسیب پذیری ها انجام می پذیرد تا سازمان ها بتوانند قبل از این که مورد حملات سایبری قرار گیرند این خطرات برطرف گردد.

شناسایی و پاسخ مدیریت‌شده (MDR)

امروزه هوش مصنوعی می تواند به طیف وسیعی از موضوعات مرتبط با شناسایی و پاسخ مدیریت شده و همچنین شناسایی تهدیدات پیشرفته مانند باج‌افزار یا حملات هدفمند، تجزیه و تحلیل رفتار تهدیدات ســایبری، تشخیص فیشینگ و ایمیل‌های مخرب، تقاطع گیری، تشخیص و شناسایی بدافزارها، جلوگیری از حملات مبتنی بر کدینگ و رمزنگاری، تحلیل کلان داده ها، تشخیص ناهنجاری‌های رفتاری، پیش‌بینی تهدیدات ســایبری، کاهش خطاهای کاربــران در تصمیم گیری‌های امنیتی، اتخاذ تصمیمات امنیتی به صورت خودکار، تشــخیص و جلوگیری از Attack DDoS، کنترل دسترسی و احراز هویت، بهبود امنیت نرم‌افزارها و شناسایی آسیب‌پذیری‌ها، تحلیل رخدادهای امنیتی و مدیریت هشدارها کمک نماید. استفاده از هوش مصنوعی در شرکت های MSSP می تواند پاسخ‌گویی سریع و کاهش آسیب‌های احتمالی را در سازمان ها کاهش داده و پیشگیری هوشمندانه صورت پذیرد.

بهبود مستمر امنیت

ارائه دهندگان خدمات امنیت مدیریت شــده با انجام بررسی‌های دوره‌ای به سازمان ها در ارتقاء مداوم وضعیت امنیتی کمک می‌نمایند این موضوع باعث می شــود که بر اســاس تهدیدات جدید و نیازهای مرتبط با کســب‌وکار هر سازمان پیشنهادات به‌روزرسانی ارائه شود.

جان کلام این که فارغ از تهدیدهایی که به واسطه امنیتی بودن موضوعات سایبری در برون سپاری آن مطرح می گردد. طبیعی است که می توان از جنبه های سفید و یا سیاه به آن پرداخت ولیکن این واقعیت را نیز می بایست در نظر داشت که امروزه با گسترش انواع شبکه ها و از جمله شبکه های تحت وب، شرکت های MSSP یا ارائه دهندگان خدمات امنیت مدیریت شده می توانند نقش کلیدی در تأمین امنیت سایبری سازمان‌ها داشته و برای سازمان هایی که منابع یا تخصص لازم برای مدیریت امنیت اطلاعات و ارتباطات خود را نداشــته و در کنار آن نیاز تخصصی به خدمات امنیتی دارند مورد توجه قرار گیرند.

شرکت‌های MSSP راهکاری اقتصادی و مطمئن برای تأمین امنیت سایبری سازمان‌ها هستند

رئیس انجمن افتا با اشاره به نقش مؤثر شرکت‌های MSSP در مدیریت امنیت سایبری، گفت: سازمان ها با برون‌سپاری خدمات امنیتی مدیریت شده به شرکت های MSSP، به شیوه‌ای مقرون‌به‌صرفه، چالش‌های نیروی انسانی متخصص و هزینه بالای تکنولوژی را برای سازمان‌ها به حداقل می‌رسانند.

مهندس مسعود رجایی، رئیس انجمن افتا در گفت‌وگو با خبرنگار ما با اشاره به ضرورت استفاده از خدمات شرکت‌های MSSP (ارائه‌دهنده خدمات امنیت مدیریت‌شده) گفت: «ما در واقع با برون‌سپاری بخشی از خدمات امنیت شبکه مواجه هستیم. همان‌طور که برخی سازمان‌ها جابه‌جایی کارکنان خود را به شرکت‌هایی مانند اسنپ یا شرکت‌های اتوبوسرانی واگذار می‌کنند، در حوزه امنیت اطلاعات هم می‌توان با واگذاری خدمات به MSSPها، بهره‌وری و صرفه‌جویی را افزایش داد.»

رجایی افـزود: «راه‌اندازی و نگهداری مرکز عملیات امنیت (SOC) نیاز به تکنولوژی گران‌قیمت و نیروی انسانی بسیار متخصص دارد. بسیاری از سازمان‌های کوچک به‌دلیل قیمت بالای تجهیزات و کمبود منابع انسانی تخصصی، توان پیاده‌سازی SOC مستقل را ندارند. MSSPها این امکان را فراهم می‌کنند تا سازمان‌ها بدون سرمایه‌گذاری کلان، از خدمات امنیتی کامل بهره‌مند شوند.»

وی با تأکید بر اینکه اصل کار شرکت‌های MSSP بر تخصص نیروی انسانی متمرکز است، ادامه داد: «این شرکت‌ها باید نیروی انسانی آموزش‌دیده برای راهبری و تحلیل رخدادهای امنیتی داشته باشند. همچنین لازم است دیتاسنترهای قوی برای دریافت و تحلیل لاگ‌ها فراهم کنند.»

رئیس انجمـن افتا در خصوص نگرانی‌ها پیرامون واگذاری اطلاعات سـازمان‌هـا به MSSPها، توضیح داد: «این تصور اشـتباه است که اطلاعات سازمان به بیرون منتقل می‌شود. اطلاعات محرمانه سازمان از محیط آن خارج نمی‌شود؛ بلکه تنها رخدادهای امنیتی رمزنگاری‌شده و فشرده‌شده به مرکز MSSP ارسال می‌شود. این فرآیند کاملاً امن است و تهدیدی برای حریم خصوصی اطلاعات سازمان‌ها محسوب نمی‌شود.»

رجایی به دو روش متداول ارائه خدمات توسط MSSPها اشاره کرد و گفت: «در روش اول، MSSP با نصب سنسور در داخل شبکه مشتری، رخدادهای امنیتی را جمع‌آوری کرده و پس از تحلیل، خروجی را به سـازمان بازمی‌گردانـد. در روش دوم، تکنولوژی SIEM داخل سـازمان مستقر می‌شود و MSSP فقط نقش تحلیل‌گر و راهبر را ایفا می‌کند؛ این مدل بیشتر برای سازمان‌های بزرگ کاربرد دارد.»

وی در پایان تأکید کرد: «این مدل خدمات‌رسانی، کمک می‌کند تا حتی سازمان‌های کم‌درآمد هم به سطح مناسبی از امنیت اطلاعات برسند. مثل این است که فردی نتواند یک یخچال گران‌قیمت بخرد، اما با اقساط یا اجاره به‌صرفه به همان خدمت دسترسی پیدا کند. امنیت هم باید برای همه سازمان‌ها دست‌یافتنی باشد.»

راه‌اندازی مراکز MSSP راهکاری مؤثر برای ارتقای امنیت سایبری سازمان‌ها

رئیس کمیسیون افتا نصر خراسان رضوی با تأکید بر ضرورت واگذاری خدمات امنیت اطلاعات به مراکـز تخصصی، گفت: مراکز ارائه‌دهنده خدمات امنیت مدیریت‌شـده (MSSP)، با نظارت تخصصی بر وضعیت امنیتی سازمان‌ها، می‌توانند نقش مؤثری در کاهش مخاطرات سایبری ایفا کنند.

بهروز مهدوی، عضو کمیسـیون افتا نصر کشـور در گفت‌وگو با خبرنگار ما با اشاره به ضرورت توسـعه مراکز ارائه‌دهنده خدمات امنیت مدیریت‌شده (MSSP) اظهار کرد: «این مراکز مسئولیت نظارت بر وضعیت امنیت اطلاعات سازمان‌ها را برعهده دارند و با بهره‌گیری از تیم‌های تخصصی مانند تیم پاسخ به رخداد (Blue Team)، می‌توانند به شناسایی و مقابله با تهدیدات امنیتی بپردازند.»

وی در ادامه افزود: «شـرکت‌های MSSP معمولاً خدماتی مانند پایش مداوم لاگ‌ها، تحلیل رخدادها و پاسخ سریع به تهدیدات را ارائه می‌دهند. این شرکت‌ها می‌توانند بار نظارت و راهبری SOC (مرکز عملیات امنیت) را از دوش سـازمان‌ها بردارند؛ به‌ویژه سازمان‌هایی که از نظر منابع انسانی یا تخصص فنی محدودیت دارند.»

مهدوی با اشـاره به وضعیت این مراکز در کشور گفت: «تا این لحظه در مشهد مرکز رسـمی دارای مجوز MSSP راه‌اندازی نشـده، اما در تهران و یزد فعالیت‌هایی در این زمینه در حال انجام اسـت. برخی از شرکتهای معتبر و بزرگ در بخش خصوصی نیز با اسـتفاده از همین الگو، خدمات امنیتی خود را به‌صورت برون‌سپاری شده مدیریت می‌کنند.»

وی درباره نگرانی برخی مدیران نسبت به واگذاری امنیت به خارج از سازمان، تصریح کرد: «در واقع، این مراکز مسـئول حفاظت مستقیم از اطلاعات نیستند، بلکه نظارت بر امنیت اطلاعات را بر عهده دارند. این یک تفکیک مهم است که بدانیم نقش آن‌ها نظارتی و عملیاتی است، نه مالکیت داده.»

مهدوی در پایان با اشاره به طرح‌های کلان حاکمیتی بیان کرد: «در طرح ضربتی سطح ۳ بند ۶، یکی از الزامات، اتصال به زیرساخت افتا از طریق شبکه ملی اطلاعات است. این نشان می‌دهد که نگاه به MSSPها به‌عنوان یک راهکار ضروری در حال نهادینه شدن است.»

سارا استوار

پروتکل های پیشنهادی برای حمایت دولت از کسب‌وکارها در شرایط بحرانی

رئیس کانون هماهنگی فاوا تاکید کرد: در شرایط بحران، حمایت از کسب‌وکارها یک امر اجتناب ناپذیر بوده و فقط مربوط به پرداخت وام و تسهیلات مرتبط با مالیات و تامین اجتماعی نیست؛ بلکه باید یک شبکه گسترده از اقدامات حمایتی، نظارتی، فناورانه، امنیتی، تجاری و حتی فرهنگی طراحی و اجرا شود.

دکتر داوود ادیب، در گفت و گو با خبرنگار ما پیرامون رویکرد کسب و کارهای حوزه فاوا برای عبور از شرایط اخیر در کشور گفت: بحران جنگ اخیر در کشور اگرچه پیش از هر چیز، تهدیدی برای سلامت عمومی، روحی و روانی شهروندان و تخریب زیرساخت ها از سوی دشمنان هدف گذاری شده بود، اما رفته رفته نشانه ها حاکی از آن داشت که در صورت ادامه، جهت گیری به سمتی می رفت تا تبدیل به یک تهدید اقتصادی داخلی و منطقه ای گردد. هرچند راهی برای مشخص کردن دقیق آسیب های اقتصادی ناشی از چنین اتفاقاتی در کوتاه مدت برآورد نشده است، ولیکن در بین تحلیلگران این اجماع وجود دارد که این روند در صورت ادامه، تأثیر منفی قابل ملاحظه ای می توانست بر فعالیت فعالان اقتصادی و در نهایت رکود کسب و کارهای سنتی و حتی کسب و کارهای مبتنی بر شبکه های مجازی از خودبه جای بگذارد.

رئیس هیات مدیره انجمن صنفی کارفرمایی هوش مصنوعی و اقتصاد دیجیتال ایران ادامه داد: مشکلی که در اینچنین شرایطی معمولا شاهدیم این است که با بروز چنین اتفاقاتی، پرسنل شرکت ها برای انجام کارهای مختلف طراحی، مهندسی، تولید، برنامه نویسی و ارائه سایر خدمات نمی توانند ساعت کاری خود را مطابق برنامه عادی هماهنگ نموده و از طرفی به جهت مشکلات اینترنت و در مواردی اینترانت ، امکان دورکاری نیز نداشته و به جهت نگرانی ها و اضطراب حاکم ضمن غیبت های طولانی مدت، باعث تعطیلی ناخواسته شرکت های تولیدی و خدماتی می گردند. این نکته نیز مهم هست که اصولا تولید کارگرمحور به صورت غالب رویکرد دورکاری نداشته و حتما نیازمند حضور فیزیکی است.

وی افزود: در این راستا عقلانیت حکم می کند در شرایط بحران به عنوان یک پروتکل ثابت و استاندارد و از پیش تعریف شده، در صورتی که شرایط فورس ماژور بیش از یک مدت زمان قابل توجه «به عنوان مثال یک ماه» طول بکشد، دولت بتواند به صورت قانونی از ابزارها و سیاست‌های حمایتی برای پشتیبانی از کسب‌وکارها استفاده نموده تا از رکود اقتصادی جلوگیری و حداقل پایداری نسبی اقتصادی را حفظ نماید. به عبارتی بعد از حدوث چنین اتفاقاتی از یک طرف تکلیف دولت و از طرف دیگر فعالان اقتصادی از پیش مشخص بوده و به آن عمل شود.

وی ادامه داد: این یک واقعیت است که در شرایط بحران، حمایت از کسب‌وکارها یک امر اجتناب ناپذیر بوده و فقط مربوط به پرداخت وام، تسهیلات مرتبط با مالیات و تامین اجتماعی نیست؛ بلکه باید یک شبکه گسترده از اقدامات حمایتی، نظارتی، فناورانه، امنیتی، تجاری و حتی فرهنگی طراحی و اجرا شود و اگر بخواهیم در کنار موضوعات مهم و حیاتی و از جمله دفاع از کیان میهنمان به طور حرفه‌ای از اقتصاد کشور نیز دفاع کنیم، باید به همه این ابعاد توجه شود.

ادیب گفت: بدیهی است در کنار این موضوعات نقش دولت در ایجاد آرامش و برقراری فضای مناسب روحی و روانی می تواند اثرگذار بوده و توصیه می گردد که در چنین شرایطی به صورت پیش فرض و قانونمند اقدامات ویژه ای توسط دولت انجام پذیرد.

رئیس اتحادیه صنعت مخابرات ایران، تاکید کرد: اقدامات دولت معمولاً در چند محور کلی می تواند به شرح ذیل طبقه‌بندی شود:

۱- جنگ و حملات نظامی از مصادیق فورس ماژور در قراردادها می باشد، لذا ترتیبی اتخاذ گردد تا کارفرمایان پروژه های اجرا شده در شرایط بحران، ملزم به افزایش مدت زمان اجرای قراردادهای پیمانکاران خود گردیده و بانک ها و صندوق های حمایتی به جهت جلوگیری از خسارت های پیش روی صنایع داخلی، تسهیلات با نرخ کم در اختیار فروشندگان و پیمانکارانی که دارای قرارداد جاری می باشند، قرار دهند. همچنین کارفرمایان ضمن پرداخت مطالبات قبلی پیمانکاران، از ضبط ضمانتنامه پیمانکارانی که قادر به انجام تعهدات خود در آن مقطع نگردیده اند، جلوگیری به عمل آورند.

۲- مساعدت و تعویق پرداخت مالیات‌ها و بدهی‌های بانکی برای کاهش فشار مالی.

۳- ایجاد صندوق‌های حمایتی شرایط بحران برای کسب‌وکارهای کوچک، متوسط یا صنایع خاصی که بیشتر امکان آسیب برای آنها وجود دارد.

۴- پرداخت یارانه دستمزد یا کمک‌هزینه کارگری برای جلوگیری از اخراج گسترده کارگران.

۵- کمک به زنجیره تأمین و ایجاد مسیرهای جایگزین برای تأمین مواد اولیه یا صادرات محصولات.

۶- کنترل بازار و حمایت از تولید داخل با جلوگیری از احتکار، قاچاق یا گران‌فروشی با نظارت بیشتر بر بازار.

۷- افزایش تعرفه واردات کالاهای غیرضروری با رویکرد حمایت از محصولات داخلی.

۸- حمایت حقوقی و قانونی، تعلیق یا ساده‌سازی مقررات دولتی برای کاهش بار بوروکراسی در زمان بحران.

۹- حمایت از کسب‌وکارها در برابر دعاوی حقوقی غیرضروری یا تعلیق برخی احکام اجرایی در شرایط اضطراری.

۱۰ - اطلاع‌رسانی و آموزش نحوه ادامه فعالیت در شرایط بحران، فراهم سازی فروش و خدمات آنلاین با رویکرد مدیریت منابع.

۱۱- ایجاد سامانه‌های ارتباطی اضطراری بین دولت و صاحبان کسب‌وکار.

۱۲- توجه ویژه به صنایع استراتژیک، به این منظورکه دولت می بایست بر صنایع خاصی بیشتر تمرکز کند که در شرایط جنگی نقش حیاتی دارند.

۱۳- کاهش یا حذف تعرفه‌های گمرکی برای مواد اولیه، قطعات یدکی مهم و استراتژیک.

۱۴- تسریع در فرآیند ترخیص کالا، راه‌اندازی مسیرهای سبز گمرکی برای کالاهای استراتژیک.

۱۵- تعلیق برخی مقررات گمرکی زمان‌بر و فعال‌سازی سامانه‌های ترخیص فوری برای صنایع کلیدی.

۱۶- ایجاد معافیت‌های خاص گمرکی برای مناطق جنگ‌زده یا آسیب‌دیده بیشتر.

۱۷- معافیت یا کاهش هزینه انبارداری و نگهداری کالاها در گمرک.

۱۸- حمایت از صادرات و تسهیل بازگشت ارز حاصل از صادرات.

۱۹- اعطای مشوق‌های صادراتی به بنگاه‌هایی که علی‌رغم بحران، به صادرات ادامه می‌دهند.

۲۰- حمایت‌های تأمین اجتماعی از کسب‌وکارها شامل تعویق یا تقسیط بدهی‌های بیمه‌ای و ارائه فرصت «حداقل معادل زمان بحران» بدون جریمه برای پرداخت حق بیمه و امکان تقسیط بدهی‌ها با بهره کم یا بدون بهره

۲۱- بخشودگی جرائم تأخیر پرداخت حق بیمه به دلیل شرایط جنگی.

۲۲- حمایت بیمه‌ای از کارگران در صنایع حیاتی با بیمه بیکاری و حمایت از کارگران

بیکار شده با هدف تسهیل دسترسی کارگران بیکار شده به بیمه بیکاری و افزایش مدت یا مبلغ بیمه بیکاری در شرایط بحرانی.
۲۳- بیمه بحران برای آسیب‌های ناشی از حملات یا تحریم‌ها.
۲۴- حمایت قضایی از کسب‌وکارهای مورد تهدید یا تخریب شده.
۲۵- حمایت روانی و اجتماعی با مشاوره روان‌شناسی برای کارآفرینان، مدیران و کارکنان در مناطق درگیر و حمایت فرهنگی برای حفظ روحیه کسب‌وکارها در زمان جنگ.
۲۶- حمایت از صادرات و تجارت خارجی با ایجاد خطوط اعتباری یا تهاتر با کشورهای هم‌پیمان (مثل روسیه، چین، کشورهای همسایه).
۲۷- اعزام رایزن‌های اقتصادی ویژه به کشورهایی که می‌توانند بازار جایگزین باشند.
۲۸- تضمین خرید محصولات استراتژیک از شرکت‌های فناور و نوآور دانش بنیان.
۲۹ - ترویج تولید کالاهای جایگزین داخلی برای کالاهای وارداتی و حمایت از بومی‌سازی قطعات و مواد اولیه در صنایع مادر.
۳۰- پشتیبانی قضایی و امنیتی ویژه با راه‌اندازی شعب ویژه برای رسیدگی سریع به دعاوی اقتصادی و حمایت از کارآفرینان در برابر فشارهای امنیتی یا قضایی ناعادلانه در زمان بحران.
ادیب در پایان خاطرنشان کرد: همانطور که فعالان اقتصادی کشورمان که به تعبیر مسئولان کشور با عنوان فرماندهان جنگ اقتصادی نام برده می شوند و در روزهای اخیر نیز شاهد بودیم مقابل جنگ، تحریم و انواع بحران ها ایستادگی و به مردم و نهادهای دولتی خدمت رسانی نموده و بدیهی بود که بدون نقش پررنگ آنها کشور آسیب فراوانی می دید، جا دارد که بخش خصوصی مجددا فراموش نگردد و دولت این پشتوانه گرانقدر را برای خود در بحران های پیش بینی نشده حفظ نماید.

چالش‌های کسب‌وکارهای فناور در دوران جنگ؛

ضرورت حمایت دولت و تسهیل دسترسی به اینترنت

رئیس سازمان نظام صنفی رایانه‌ای کشور بر لزوم حمایت دولت و تسهیل دسترسی به اینترنت برای ادامه فعالیت شرکت‌های حوزه فناوری در شرایط بحران جنگی تأکید کرد.
دکتر علی حکیم‌جوادی، رئیس سازمان نظام صنفی رایانه‌ای کشور، در گفت‌وگو با ما، به بررسی چالش‌های کسب‌وکارهای حوزه فناوری در شرایط بحران جنگی پرداخت.
وی اظهار داشت: «چالش‌های ما متفاوت است؛ بخشی از مشکلات شبیه سایر صنوف است، اما مسائل خاص خود را نیز دارد.»
حکیم‌جوادی افزود: «با توجه به شرایط، بسیاری از همکاران ما به صورت دورکاری فعالیت می‌کنند، اما مشکلاتی مانند بیمه، مالیات و پرداخت اقساط تسهیلات بانکی، شرکت‌ها را تحت فشار قرار داده است؛ دولت باید برای عبور از این دوران به شرکت‌ها کمک کند تا بتوانند خود را با شرایط وفق دهند.»
وی همچنین به مسئله دسترسی به اینترنت اشاره کرد و گفت: «شرکت‌هایی که به اینترنت نیاز مبرم دارند، باید بتوانند به راحتی به آن دسترسی داشته باشند تا از طریق دورکاری خدمات خود را به موقع ارائه دهند؛ این شرکت‌ها عمدتاً به مجموعه‌های دولتی و عمومی خدمات می‌دهند و برای پایداری سرویس‌هایشان نیاز به حمایت دارند.»
حکیم‌جوادی در پایان تأکید کرد: «همکاران ما در این بحران قرار دارند و تلاش می‌کنند خود را با شرایط وفق دهند؛ حمایت دولت و تسهیل دسترسی به اینترنت، کلید اصلی برای ادامه فعالیت آنهاست.»

کسب‌وکارها در بحران جنگی با استراتژی‌های متفاوت به فعالیت ادامه می‌دهند

رئیس هیأت‌مدیره سندیکای صنعت مخابرات ایران گفت: هر کسب‌وکار باید متناسب با نوع فعالیت خود، استراتژی ادامه کار در شرایط جنگی را اتخاذ کند.
حسین ریاضی، رئیس هیأت‌مدیره سندیکای صنعت مخابرات ایران در گفت‌وگو با خبرنگار ما، به بررسی تأثیر بحران جنگی بر کسب‌وکارها پرداخت. وی اظهار داشت: «کسب‌وکارها تلاش می‌کنند با ظرفیت‌های موجود فعالیت خود را ادامه دهند، اما استراتژی آنها بسته به نوع فعالیتشان متفاوت است.» ریاضی افزود: «کسب‌وکارهایی که سرویس‌های شبکه‌ای یا اینترنتی ارائه می‌دهند، مانند خدمات پاسخگویی به مردم، مجبور هستند فعالیت خود را به طور مداوم ادامه دهند. این کسب‌وکارها از تکنیک‌های دورکاری استفاده می‌کنند تا بتوانند با نیروهای خود در هر شرایطی فعالیت را پیش ببرند.» وی در ادامه به کسب‌وکارهای تولیدی اشاره کرد و گفت: «کسب‌وکارهای تولیدی که ارتباط مستقیم کمتری با مردم دارند، باید متناسب با نیاز بازار و نوع محصول خود، فعالیتشان را ادامه دهند.»
ریاضی در پایان تأکید کرد: «هیچ کسب‌وکاری نمی‌تواند با یک استراتژی واحد فعالیت کند؛ بلکه باید متناسب با شرایط و نیازهای خود، راهکار مناسب را اتخاذ نماید.»

عادلانه کردن آبونمان تلفن ثابت؛ عامل اصلاح رفتار ارتباطی مشترکان

دبیر و نایب رئیس هیات مدیره سندیکای صنعت مخابرات، گفت: یکی از راه های عادلانه کردن تعرفه های تلفن ثابت و اصلاح رفتاری در استفاده از خدمات ارتباطی، مانور روی کف درآمد ماهانه این نوع از خدمات است که اصطلاحا آبونمان ماهانه خوانده می شود. با تعیین یک رقم ثابت به عنوان کف درآمد تلفن ثابت، مشترکان برای استفاده از خدمات تلفن ثابت رغبت بیشتری نشان خواهند داد تا لااقل تا رقم تعیین شده برای آبونمان، از خدمات تلفن ثابت استفاده نمایند.

در پی افزایش آبونمان تلفن ثابت توسط شرکت مخابرات ایران فرامرز رستگار دبیر و نایب رئیس هیات مدیره سندیکای صنعت مخابرات گفت: مطالبی که توسط اینجانب در این رابطه اعلام می شود «توجیه این اقدام نیست» ولی «توضیحی است در راستای منطقی بودن این تصمیم».

وی ادامه داد: متاسـفانه با گسترش شبکه های موبایل در سطح کشور و راحتی بیشتر در تماس با گوشی های موبایل و همچنین رقابت اپراتورهای موبایل در کف تعرفه های تعیین شده، باعث گردیده که ترافیک ارتباطی به طور غیرمتعارف از شبکه های ثابت به سوی شبکه های موبایل هدایت شود، «حتی برای ارتباطاتی که یکطرف و یا هر دو طرف ارتباط، ثابت می باشد».

رستگار خاطرنشان کرد: این فرهنگ ارتباط باعث شده که اپراتورهای ارتباطات ثابت که تامین کننده زیرساخت های ارتباطی نیز هستند با کاهش درآمد مواجه و به تدریج توسعه و بروز رسانی شبکه های ثابت با مشکلات مالی مواجه شود و سرمایه گذاری در این بخش حیاتی را غیر اقتصادی نماید.

وی ادامه داد: سـندیکای صنعت مخابرات ایران بیش از پنج سال است که به مسوولان ارتباطات کشور هشدار می دهد که بی توجهی به شبکه ارتباطات ثابت باعث افت کیفیت در ارتباطات موبایل نیز خواهد گردید و به طور کلی اگر اقدامات فوری برای رشد مجدد ارتباطات ثابت فراهم نشود، امنیت ارتباطات نیز به خطر خواهد افتاد.

دبیر سندیکای صنعت مخابرات ایران به خبرنگار ما گفت: اساسا شبکه های موبایل برای خدمات موبایل طراحی شده و قطعا توانمندی جابجایی تمام ترافیک شبکه ها را ندارد.

وی ادامه داد: استفاده بیش از حد از گوشی موبایل برای سلامتی کاربران هم جایز نیست و متاسفانه در این زمینه اطلاع رسانی خوبی صورت نگرفته و همواره به خطرات سایت های رادیویی موبایل (سایت های BTS) پرداخته شده است، در حالیکه خطرات گوشی موبایل به مراتب از BTS ها بیشتر است.

رستگار در ادامه گفت: وقتی که فرهنگ سازی درست در این زمینه انجام نمی شود و با وجود گرانتر بودن نرخ تعرفه موبایل نسبت به ثابت، باز هم تمایل مردم برای استفاده از گوشی موبایل حتی برای مواردی که برقراری ارتباط ثابت و ارزان وجود دارد همچنان کم است، باید روش‌هـایـی تدبیر شود که رفتار ارتباطی کاربران در جهت منافع خود، جامعه و در سطح ملی اصلاح شود.

وی گفت: وقتی که هزینه نگهداری از یک خط تلفن ثابت روز به روز افزایش می یابد و در حال حاضر شاید حدود ۵۰ هزار تومان در ماه باشد، چرا باید درصد بالایی از خطوط تلفن ثابت بلامصرف و یا با مصرف محدود در اختیار افراد و یا سازمان ها باشد و درآمدی در حد هزینه های نگهداری هم کسب نشود و ما انتظار داشته باشیم که شبکه توسعه، نوسازی و بروز رسانی هم داشته باشد.

وی خاطرنشان کرد: از طرفی هم اکنون بسیاری از متقاضیان تلفن ثابت هم منتظر دریافت این سرویس هستند، ولی سرمایه گذاری برای توسعه شبکه ثابت غیر اقتصادی است.

رستگار در ادامه به خبرنگار ما گفت: بنابراین یکی از راه های عادلانه کردن تعرفه های تلفن ثابت و اصلاح رفتاری در استفاده از خدمات ارتباطی، مانور روی کف درآمد ماهانه این نوع از خدمات است که اصطلاحا آبونمان ماهانه خوانده می شود.

وی ادامه داد: با تعیین یک رقم ثابت به عنوان کف درآمد تلفن ثابت، مشـترکان برای استفاده از خدمات تلفن ثابت رغبت بیشتری نشان خواهند داد تا لااقل تا رقم تعیین شده برای آبونمان، از خدمات تلفن ثابت استفاده نمایند.

رستگار گفت: اگر برای بعضی از خانوارها و یا کسب کارها امکان استفاده از تلفن ثابت میسر نباشد، طبیعتا برای پرهیز از پرداخت بی مورد می توانند نسبت به لغو اشتراک خود اقدام نمایند تا این امکانات در اختیار متقاضیان در لیست انتظار قرار بگیرد و لازم نباشد در این شرایط محدودیت منابع مالی در کشور، برای توسعه تلفن ثابت سرمایه گذاری نماییم.

وی خاطرنشان کرد: در نهایت امیدواریم شاهد گسترش کسب و کارهای حوزه مخابرات و ارتقای کیفیت خدمات در شبکه های ثابت به طور مستقیم و در شبکه های موبایل به صورت غیرمستقیم باشیم.

کاهش ۲۴۰۰ مگاواتی مصرف برق در دوران جنگ؛

ماینرهایی که با قطع اینترنت خاموش شدند

در جریان جنگ تحمیلی ۱۲ روزه، یکی از اقدامات دولت ایران در راستای امنیت سایبری، محدودسازی اینترنت و قطع اینترنت بین‌الملل بود. این تصمیم، به طرز چشم‌گیری بر مصرف برق کشـور نیز تأثیر گذاشـت. آمارهای رسمی نشان می‌دهد که در نتیجه این محدودیت، حدود ۲۴۰۰ مگاوات از بار مصرفی شبکه برق سراسری کاهش یافته است.

محمد الهداد، معاون انتقال و تجارت خارجی شرکت توانیر، با اشاره به تأثیر قطعی اینترنت بر کاهش بار شبکه برق گفت: «در خلال جنگ ۱۲ روزه، با قطع اینترنت، حداقل ۲۴۰۰ مگاوات بار از شبکه سراسری برق کشور حذف شد. این میزان ناشی از فعالیت حدود ۹۰۰ هزار دستگاه استخراج رمزارز (ماینر) بود که به دلیل عدم دسترسی به اینترنت بین‌المللی، از کار افتادند.»

به گفته وی، این رقم معادل حدود ۱۵ درصد ناترازی برق کشور در نیمه اول تیرماه است

و توان قابل‌توجهی در شرایط اوج مصرف به شبکه بازگرداند.
الهداد همچنین افزود که علاوه بر این تعداد، گروهی از استخراج‌کنندگان غیرمجاز که از برق دزدی و اینترنت ماهواره‌ای غیرقانونی (نظیر استارلینک) استفاده می‌کردند نیز طی این مدت فعالیت خود را متوقف کردند. این دسته از مزارع، با قطع اینترنت دچار اختلال جدی شده و از مدار خارج شدند. معاون توانیر با اشاره به سیاست‌های کنترلی برای عبور از بحران برق تابستان، گفت: «فعالیت همه مزارع استخراج رمزارز در فصل گرم سال ممنوع است، مگر در شرایط خاص. تنها مزارعی که با احداث نیروگاه خورشیدی معادل انرژی مصرفی خود را به شبکه تزریق می‌کنند، مجاز به ادامه فعالیت هستند.»
الهداد همچنین از متخصصان حوزه رمزارز و دانشگاهیان دعوت کرد تا با توجه به کاهش هش‌ریت جهانی بیت‌کوین، اطلاعات دقیق‌تری از میزان استخراج و ظرفیت پردازشی در ایران ارائه دهند. او تأکید کرد: آمارهای رسمی نیاز به به‌روزرسانی و پایش علمی دارد.
ماینینگ رمزارز در ایران نه‌تنها چالش امنیتی یا اقتصادی، بلکه یک مسئله کلیدی در توازن شبکه برق کشور است. قطع اینترنت در دوران جنگ، عملاً نشان داد که وابستگی استخراج رمزارزها به اتصال بین‌المللی تا چه حد بالاست و چقدر ظرفیت مصرف برق در سایه این صنعت پنهان مانده بود. قطع اینترنت در دوره جنگ، اگرچه اقدامی با اهداف امنیت سایبری بود، اما به‌طور غیرمستقیم تأثیری قابل توجه بر مصرف برق کشور نیز گذاشت. کاهش ناگهانی ۲۴۰۰ مگاوات بار، فرصتی برای تنفس شبکه برق در اوج گرمای تابستان فراهم کرد. با این حال، این دستاورد در سایه آسیب به حوزه دیجیتال و اقتصادی کشور حاصل شده و تداوم قطع اینترنت بین الملل می‌توانست تبعات جدی‌تری در پی داشته‌باشد.

شائبه‌ها به اجرای پروژه اینترنت طبقاتی و دسترسی تبعیض‌آمیز به اینترنت

علی رغم تکذیب مقامات مسئول در اجرای طرح اینترنت طبقاتی در کشور، فعالان فضای مجازی بر اساس شواهد معتقدند که طی سال‌های اخیر شکل خاصی از دسترسی تبعیض‌آمیز به اینترنت در حال اجراست که همزمان با اختلاف در سطح دسترسی مناطق مختلف جغرافیایی و کاربران اپراتورهای مختلف، نشان از پیاده سازی نوعی تبعیض دیجیتال است. قطع اینترنت بین‌الملل در ایران همزمان با جنگ ۱۲ روزه، بار دیگر موضوع اجرای طرح‌های موسوم به «اینترنت طبقاتی» را به کانون توجه رسانه‌ها و کارشناسان تبدیل کرده است. با مسدود شدن دسترسی شمار بسیاری از کاربران به اینترنت جهانی، برخی مدیران کسب‌وکارهای اینترنت‌محور پیشنهاد کرده بودند که به‌جای قطع سراسری، دسترسی به اینترنت به‌شکل طبقه‌بندی‌شده و هدفمند مدیریت شود.
این پیشنهادها، اگرچه با واکنش منفی گسترده کاربران در رسانه‌های اجتماعی مواجه شد، اما به باور کارشناسان، اینترنت طبقاتی پیش‌تر در سال های قبل و در سکوت خبری، در برخی حوزه‌ها اجرا شده است.

تاکید وزارت ارتباطات بر عدم اجرای اینترنت طبقاتی

در واکنش به افزایش حساسیت افکار عمومی، احسان چیت‌ساز، معاون وزیر ارتباطات و فناوری اطلاعات دولت چهاردهم، با تاکید بر مخالفت این وزارتخانه با «هرگونه اینترنت طبقاتی» گفت: «اینترنت باکیفیت، عادلانه و همگانی، حق همه مردم است و ستون فقرات اقتصاد دیجیتال. هرگونه سیاست توسعه‌ای باید برپایه عدالت در اتصال بنا شود، نه بر امتیازدهی محدود.» این اظهارات در پاسخ به نامه رسمی سازمان نظام صنفی رایانه‌ای استان تهران منتشر شد، نامه‌ای که خواستار ایجاد دسترسی آزاد به اینترنت جهانی برای فعالان فناوری اطلاعات شده بود. با این حال، پس از انتقادهای بسیار، برخی اعضای هیات‌مدیره این سازمان، تاکید کردند که این موضع الزاما دیدگاه همه اعضا نیست و آنان نیز با اینترنت طبقاتی مخالفاند.بهزاد اکبری، معاون وزیر ارتباطات و مدیرعامل شرکت ارتباطات زیرساخت هم در واکنش به طرح مباحثی در فضای مجازی مبنی بر دریافت اطلاعات از شرکت ها برای وایت لیست کردن IPهای اعلامی، تاکید کرد: هیچ هماهنگی با هیچ انجمنی در این خصوص انجام نشده است. کارشناسان فناوری اطلاعات اما معتقدند که فارغ از این واکنش‌ها، شواهدی وجود دارد که نشان می‌دهد طی سال‌های اخیر شکل خاصی از دسترسی تبعیض‌آمیز به اینترنت در حال گسترش بوده است.برای مثال، تحلیل داده‌های فنی وب‌سایت‌های رصد اینترنت مانند نت‌بلاکس (NetBlocks) و اونی (OONI) نشان داد که برخی کاربران در دوره قطعی سراسری اینترنت همچنان به شبکه جهانی متصل بوده‌اند.

اینترنت طبقاتی؛ از تکذیب تا اجرای مرحله‌ای؟!

مهرماه ۱۴۰۲، علی‌اصغر شالبافیان، معاون وقت وزیر گردشگری، اعلام کرد که با تصویب کمیته تعیین مصادیق محتوای مجرمانه، سیم‌کارت‌هایی با دسترسی آزاد به اینترنت بین‌الملل در اختیار گردشگران خارجی، دفاتر خدمات مسافرتی، هتل‌ها و راهنمایان گردشگری قرار خواهد گرفت. این تصمیم عملا به معنای گسترش حوزه واگذاری اینترنت طبقاتی از گردشگران خارجی به فعالان داخلی صنعت گردشگری بود.
این طرح در حالی اجرا شد که عیسی زارع‌پور، وزیر ارتباطات در دولت سیزدهم، مخالفتش با اینترنت طبقاتی را اعلام کرده بود.
با این حال، او در اظهاراتی متناقض، اذعان کرده بود که براساس برخی مصوبات، گروه‌هایی

خاص دسترسی گسترده‌تری به اینترنت دارند؛ موضوعی که به‌روشنی از وجود تبعیض ساختاری در دسترسی به فضای آزاد اطلاعات حکایت دارد.
نمونه دیگر از اجرای اینترنت طبقاتی، افشای دسترسی بدون محدودیت برخی از اساتید دانشگاهی و دانشجویان منتخب به اینترنت بین‌المللی است. ابهام اصلی در این مورد، نبود شفافیت درباره معیارهای انتخاب این افراد است.
از دیگر طرح‌های بحث‌برانگیز، راه‌اندازی «مناطق آزاد سایبری» است که مشابه الگوی مناطق آزاد تجاری، با وعده تسهیل فعالیت کسب‌وکارهای دیجیتال طراحی شده است.
سیاست اینترنت طبقاتی در ایران تنها به تفکیک شغلی محدود نمی‌شود، بلکه توان اقتصادی شهروندان نیز، به‌منزله یک شاخص نامرئی اما تعیین‌کننده، در این تبعیض نقش دارد.در روزهای قطع کامل اینترنت بین‌المللی، آنچه کاربران در شبکه‌های مجازی و گزارش‌های میدانی به‌وضوح مطرح کردند ظهور سطحی تازه از تبعیض بود: دسترسی قشر خاصی از شهروندان به فیلترشکن‌های گران‌قیمت و اینترنت ماهواره‌ای استارلینک.
تجربه بخشی از کاربران در دوره جنگ، مربوط به تفاوت پهنای باند و سطح دسترسی در مناطق مختلف جغرافیایی، حتی در تهران بوده است. به نظر می‌رسد بسته به موقعیت شهری یا سرویس‌دهنده اینترنت، امکان اتصال به فیلترشکن‌ها در برخی مناطق ساده‌تر و پرسرعت‌تر از سایر نقاط بوده است.این اختلاف در ساعات مختلف روز نیز تغییراتی داشته که از وجود یک سیستم تنظیم‌شده و غیربازارمحور در مدیریت پهنای باند حکایت دارد، سیستمی که به‌شکل پنهان الگوی «دسترسی طبقه‌بندی‌شده» را عملیاتی کرده‌است.
همچنین، بازگشت تدریجی اینترنت بین‌المللی پس از آتش‌بس، ابتدا از طریق اینترنت‌های ثابت ای‌دی‌اس‌ال (ADSL) و فیبرنوری آغاز شد و پس از چند روز به اینترنت‌های همراه نیز گسترش یافت. کاربران گزارش داده‌اند که یک اپراتور همراه حتی پس از اعلام رسمی بازگشت اینترنت، همچنان تنها دسترسی به شبکه ملی اطلاعات را برای مشترکان خود فراهم می‌کرد، نکته‌ای که تفاوت رفتار سرویس‌دهنده‌ها در مواجهه با سیاست‌های قطعی را نشان می‌دهد.

کاربران غیرقانونی اینترنت استارلینک در ایران در معرض چالش جدی!

در حالی که با افزایش احتمال دسترسی کاربران ایرانی به اینترنت ماهواره‌ای استارلینک، بر اســاس طرحی که به تصویب نمایندگان مجلس رســید، استفاده و خرید و فروش استارلینک، ممنوع و موجب حبس است، برخی منابع از بررسی روش‌های فنی و امنیتی برای مقابله با این فناوری در کشور خبر می‌دهند که استفاده کنندگان غیرقانونی از این سرویس را با چالش جدی مواجه خواهد کرد.

به‌گزارش خبرنگارما، پروژه اینترنت ماهواره‌ای استارلینک متعلق به شرکت اسپیس‌ایکس، به‌تازگی پوشش خدمات خود را در بسیاری از مناطق جهان از جمله خاورمیانه گسترش داده اســت. این موضوع باعث نگرانی دولت‌هایی شــده که شرکت استارلینک قوانین سرزمینی کشورهای آنها را نپذیرفته و به صورت غیرقانونی به ارائه خدمات اقدام کرده است.

دسترسی به اینترنت اســتارلینک از طریق دریافت‌کننده‌های مخصوص (ترمینال) و بدون نیاز به زیرساخت مخابراتی داخلی ممکن است؛ همین ویژگی، چالش‌های امنیتی متعددی برای کشورهایی مانند ایران به همراه دارد.

جزئیات طرح تشــدید مجازات جاسوسان و همکاری‌کنندگان با رژیم صهیونیستی و کشورهای متخاصم شامل ۹ ماده که نمایندگان مجلس در جلسه علنی دوشنبه دوم تیرماه به تصویب رســانده بودند، منتشر شد که بر اساس آن استفاده، حمل، خرید یا فروش یا وارد کردن یا در اختیار گذاشتن ابزارهای الکترونیکی ارتباطی اینترنتی فاقد مجوز از قبیل استارلینک، ممنوع و موجب حبس تعزیری درجه ۶ و ضبط تجهیزات خواهــد بود. تامین، تولید، توزیع و واردات بیش از ۱۰ عدد از ابزارهای مذکور یا انجام موارد مذکور به قصد مقابله با نظام مستجوب حبس تعزیری درجه ۴ خواهد بود.

بر اســاس گزارش‌های غیررســمی، نهادهای ذی‌ربط در حال ارزیابی چند روش برای جلوگیری از گســترش استفاده از این ســرویس در ایران هستند. برخی منابع هم به طراحی «رله‌های مقابله‌ای» با هدف مسدودسازی یا اختلال در سیگنال‌های ماهواره‌ای اشاره کرده‌اند.

با این حال، متخصصان معتقدند طراحی و پیاده‌ســازی چنین سامانه‌هایی به‌صورت گســترده، نیازمند بودجه بالا، تخصص فنی پیشــرفته و زیرساخت‌های خاص جنگ الکترونیک‌است.

برخلاف فیلترینگ اینترنت، اینترنت ماهواره‌ای از زیرســاخت ملی عبور نمی‌کند. به همین دلیل، مسدودسازی آن صرفاً از طریق روش‌های فنی یا مقابله در سطح فیزیکی ممکن است.

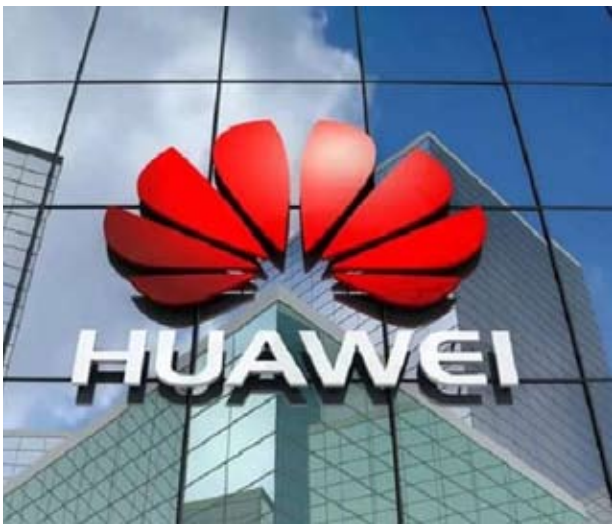
از طرفی، هیچ معاهده بین‌المللی تاکنون شرکت‌هایی مانند SpaceX را ملزم به رعایت سیاست‌های محدودکننده کشــورهای خاص نکرده است و استارلینک هم حاضر به پذیرش قوانین سرزمینی کشور ما نشده است، بنابراین ایران برای جلوگیری از فعالیت استارلینک در فضای داخلی خود، ناچار به اقدامات یک‌جانبه خواهد بود.

در چین، دولت با در اختیار داشتن فناوری‌های پیشرفته اختلال و نظارت، موفق شده تا حدی دسترسی به اینترنت ماهواره‌ای را محدود کند. در روسیه نیز اقداماتی مشابه با هدف محدودسازی ارتباطات رمزنگاری‌شده در دستور کار قرار گرفته است.

با این حال، کارشناسان فناوری اطلاعات می‌گویند هیچ کشوری تاکنون نتوانسته به‌طور کامل دسترسی به استارلینک را مسدود کند؛ مگر با برخوردهای فیزیکی و امنیتی با کاربران یا تجهیزات آن.

اینترنت استارلینک به‌عنوان فناوری نوظهور و بدون مرز، چالش تازه‌ای در حوزه ارتباطات به‌وجود آورده اســت. در ایران، بررسی روش‌های مقابله با این فناوری در جریان است؛ اما به‌نظر می‌رسد تحقق کامل آن نیازمند رویکردی چندلایه، ترکیب فناوری، قانونی و نظارت میدانی است.

فروش ۱۰۰ میلیون گوشی همراه هواوی با سیستم عامل هارمونی



بر اساس گزارش اخیر هواوی، از زمان عرضه سیستم عامل Harmony OS تا پایان ۲۰۲۴ میلادی، بیش از ۱۰۰ میلیون تلفن همراه با این پلتفرم فروخته است.

به گزارش گیزموچاینا، نرم افزار Harmony OS به نقطه عطف جدیدی دست یافته است. طبق گزارش موسسه تحقیقاتی کانالیس تعداد موبایل های بارگیری شده با این سیستم عامل برای نخستین بار از ۲۰۱۹ میلادی (سال عرضه آن) تا کنون به بیش از ۱۰۰ میلیون دستگاه رسیده است.

به طور دقیق تر از ۲۰۱۹ تا پایان ۲۰۲۴ میلادی ۱۰۳ میلیون دستگاه با سیستم عامل Harmony OS بارگیری شده بود که از این تعداد فقط ۴۶ میلیون دستگاه در ۲۰۲۴ میلادی فروخته شــده بودند. این ارقام حاکی از آن اســت که هواوی با وجود گستره محدود بین المللی همچنان در بازار داخلی حضور قدرتمندی دارد و Harmony OS بخشی اساسی از اکوسیستم سخت افزار شرکت است.

همچنین رشد فروش محصولات با این سیستم عامل محدود به موبایل نیست. کانالیس در گزارش خود اشاره می کند هواوی ۲۱ میلیون تبلت با Harmony OS را تاکنون بارگیری کرده که از این تعداد ۱۰.۵ میلیون دستگاه فقط در ۲۰۲۴ میلادی فروخته شده اند.

این سیستم عامل نخســتین بار در ۲۰۱۹ میلادی ارائه و تا اواسط ۲۰۲۱ میلادی به طور گسترده روی دستگاه ها به کار گرفته شد. Harmony OS از آن زمان تاکنون به پلتفرم پیش فرض محصولات مختلف هواوی تبدیل شده است.

Harmony OS فراتر از موبایل ها و تبلت ها درگجت های پوشــیدنی، محصولات صوتی، گجت های هوشمند خانگی و همچنین رایانه ها به کار می رود.

سامسونگ با یک گوشی سه‌لت وارد آینده می‌شود

شرکت کره‌ای سامســونگ در حال آماده شدن برای رونمایی از اولین گوشی هوشمند سه‌لت تاشوی جهان، گلکسی جی فولد، در رویداد مورد انتظار Unpacked خود طی روزهای آینده است. به گزارش فون آرنا، اگرچه گزارش‌های قبلی حاکی از قصد سامسونگ برای رونمایی از تنها دو یا سه دستگاه تاشو بود، اما اطلاعات فاش‌شده از برنامه‌ای جسورانه‌تر حکایت دارد؛ عرضه همزمان چهار دستگاه تاشو، اقدامی که بر جاه‌طلبی این شرکت برای تقویت جایگاه خود در بازار گوشی‌های هوشمند انعطاف‌پذیر تأکید می‌کند.

صفحه نمایش به اندازه تبلت

قابل توجه‌ترین نوآوری، گلکسی جی فولد، طراحی بی‌سابقه‌ای دارد. این گوشی دارای سه صفحه نمایش است که به سمت داخل تا می‌شوند و در هنگام باز شدن، یک صفحه نمایش اصلی عظیم با اندازه تقریباً ۱۰ اینچ را نشــان می‌دهند و آن را به نزدیک‌ترین چیز به یک تبلت جیبی تبدیل می‌کنند. این گوشی خود را در رقابت مستقیم با هوآوی میت ایکس تی ۱۰.۲ اینچی قرار می‌دهد، در حالی که انتظار می‌رود دارای یک صفحه نمایش ثانویه ۶.۵ اینچی نیز باشــد، اگرچه شــکل نهایی قاب بیرونی هنوز در معرض حدس و گمان است.

عملکرد غیر قابل مذاکره

به جز طراحی، به نظر نمی‌رسد سامسونگ در مورد عملکرد مصالحه کند. انتظار می‌رود این گوشی از جدیدترین پردازنده اسنپدراگون ۸ الیت کوالکام بهره ببرد و از نظر سرعت و کارایی، به یکی از قدرتمندترین گوشی‌های اندرویدی سال ۲۰۲۵ تبدیل شود.

قیمت آن شوکه کننده است و موجودی آن محدود

اما در مقابل این پیشرفت، اخبار هیجان‌انگیز کمتری برای علاقه‌مندان به فناوری در خارج از آســیا وجود دارد. گزارش‌های محلی در کره جنوبی حاکی از آن است که این گوشی با قیمتی بیش از ۴ میلیون وون کره (تقریباً ۳۰۰۰ دلار) عرضه خواهد شد که تقریباً دو برابر قیمت گلکسی Z Fold ۶ است.

باتری که انتظارات را برآورده نمی کند

با وجود صفحه نمایش بزرگ و فناوری مورد اســتفاده، برخی از اطلاعات فاش شده نگرانی‌هایی را در مورد ظرفیت باتری ایجاد کرده‌اند که گمان می‌رود کمتر از ۵۰۰۰ میلی‌آمپر ساعت باشــد. این مقدار در مقایسه با اندازه صفحه نمایش و مصرف برق مورد انتظار، کم در نظر گرفته می‌شود که می‌تواند بر تجربه روزانه کاربر تأثیر منفی بگذارد.

نقطه سیاه مرگ روی نمایشگر آیفون کاربران را سردرگم کرد

برخی کاربران آیفون با مشــکلی مرموز مواجه شــده‌اند که آن را «نقطه سیاه مرگ» نامیده‌اند؛ نقطه‌ای سیاه که ناگهان در بالای نمایشگر گوشی ظاهر می‌شود و قابل حذف نیست و ظاهرا نشانه ای از بروز مشکل سخت افزاری در گوشی است.

این نقطه معمولاً در بخش زیریــن ویژگی «جزیره پویا» (Dynamic Island) قرار دارد و به نظر نمی‌رسد در تصاویر اسکرین‌شات دیده شود.

کاربری در ردیت برای نخستین‌بار تصویری از این مشکل را روی آیفون ۱۵ خود منتشر کرد و نوشت: «این نقطه سیاه ناگهان روی نمایشگر ظاهر شد. چون در اسکرین‌شات نمی‌افتد، مجبور شدم با گوشی دیگری از آن عکس بگیرم.»

پس از این پست، کاربران دیگری نیز از بروز این مشکل خبر دادند. یکی از آنان نوشت: «همین مشکل را داشتم، مجبور شدم نمایشگر آیفون ۱۶ پرو را تعویض کنم.» کاربر دیگری گفت که نقطه ســیاه در گوشه بالا سمت راست و نزدیک آیکون باتری ظاهر شده بود.

با اینکه دلیل دقیق بروز این پدیده هنوز مشــخص نشــده، کاربران ردیت چند نظریه مطرح کرده‌اند. برخی آن را نشانه‌ای از آسیب سخت‌افزاری می‌دانند. یکی نوشت: «اگر در اسکرین‌شــات دیده نمی‌شود، احتمالاً مشکل از سخت‌افزار است.» دیگری نوشت: «آسیب به نمایشگر OLED. احتمالاً ضربه خورده. این نقطه سیاه رشد می‌کند و در نهایت باید کل نمایشگر را تعویض کرد.»

کاربر دیگری گفت: «اگر دستگاه تحت گارانتی یا AppleCare+ باشد، در فروشگاه اپل نمایشگر را رایگان تعویض می‌کنند.»

در حال حاضر اپل واکنشــی رســمی به این مشکل نشان نداده است. با این حال، این شرکت در صورت بروز مشکل در نمایشگر آیفون یا آیپد، یک روند چهار مرحله‌ای را پیشنهاد می‌کند: نخست، دستگاه را ری‌استارت کنید. سپس نمایشگر را از نظر وجود گرد و غبار یا رطوبت بررسی کنید. مرحله بعدی قطع اتصال هرگونه کابل یا لوازم جانبی USB-C یا لایتنینگ اســت. در نهایت، قاب یا محافظ صفحه را بردارید. اگر مشــکل همچنان باقی ماند، کاربران باید دستگاه خود را برای خدمات تعمیراتی ثبت کنند.

مراقب وای‌فای رایگان باشید؛ تله‌ای برای سرقت حساب بانکی شما

یک اپراتور تلفن همراه بین المللی، به کاربران گوشی‌های هوشمند هشدار فوری داده و آن‌ها را از خطرات استفاده از شبکه‌های وای‌فای عمومی، به ویژه هنگام انجام تراکنش‌های مالی یا دسترسی به حساب‌های بانکی، برحذر داشته است.

در هشداری که این شرکت برای مشتریان خود ارسال کرده، آمده است: «از استفاده از شبکه‌های وای‌فای عمومی برای انجام تراکنش‌های بانکی خود خودداری کنید، زیرا آن‌ها ناامن هستند و ممکن است داده‌های شما را در معرض سرقت قرار دهند. برای ایمن نگه داشتن اطلاعات خود از داده‌های تلفن همراه یا یک شبکه قابل اعتماد استفاده کنید.» این هشدار بی‌دلیل نبوده است، بلکه بر اساس افزایش تعداد حملات سایبری از طریق شبکه‌های اینترنتی آزاد، به ویژه در مکان‌های عمومی مانند کافه‌ها، مراکز خرید و فرودگاه‌ها است.

یک متخصص امنیت اطلاعات، در مورد خطرات اتصال به شبکه‌های اینترنتی آزاد هشدار داد و گفت که این شبکه‌ها یک آسیب‌پذیری امنیتی جدی هستند که دسترسی هکرها به داده‌های کاربران، سرقت حساب‌های بانکی آن‌ها یا حتی کنترل کامل تلفن‌های آن‌ها را آسان می‌کند.

مراقب صداهای جعلی عزیزان باشید: پیام های التماس آمیز واتس اپ

یک متخصص دیگر امنیت شبکه به العین نیوز توضیح داد که روترها در مکان‌های عمومی اغلب قابلیتی به نام DNS Hijacking را فعال می‌کنند، تکنیکی که برای هدایت اتصال شما به وب‌سایت‌های جعلی بدون اطلاع شما استفاده می‌شود و سرقت اطلاعات بانکی یا کارت اعتباری شما را برای هکرها آسان می‌کند.

او تأکید کرد که یک هکر می‌تواند در عرض چند دقیقه از طریق یک شبکه عمومی کنترل دستگاه شما را به دست گیرد و به اهمیت اجتناب از وای‌فای رایگان اشاره کرد.

به گفته این متخصص امنیت اطلاعات، یک هکر می‌تواند یک شبکه وای‌فای با نام جذاب ایجاد کند و وقتی به آن متصل می‌شوید، تلفن یا رایانه شما کاملاً در معرض خطر قرار می‌گیرد.

مهاجم به عنوان واسطه بین دستگاه شما و ارائه‌دهنده خدمات عمل می‌کند و یک کپی از هر چیزی که ارسال می‌کنید، از رمزهای عبور گرفته تا داده‌های حساس، دریافت می‌کند.

به عنوان مثال، ممکن است از وب‌سایت اصلی به یک صفحه جعلی شبیه وب‌سایت بانک هدایت شوید، جایی که می‌توانید اطلاعات خود را بدون متوجه شدن کلاهبرداری وارد کنید.

این متخصص امنیت سایبری معتقد است که یک تصور غلط رایج در بین برخی وجود دارد و آن این است که هر چیز رایگانی بی‌ضرر است و می‌گوید: «هر چیز رایگانی در اینترنت قیمتی دارد. اگر با پولتان پرداخت نکنید، با داده‌هایتان پرداخت می‌کنید.»

اگر مجبور به استفاده از یک شبکه وای‌فای عمومی هستید، به گفته یک متخصص امنیت اطلاعات، در اینجا مهمترین نکات برای محافظت از داده‌هایتان در برابر سرقت آمده است:

- هرگز اطلاعات بانکی خود را وارد نکنید.
- هنگام استفاده از یک شبکه عمومی، انتقال وجه انجام ندهید یا به برنامه بانکی دسترسی پیدا نکنید.
- از یک VPN قابل اعتماد استفاده کنید. VPN داده‌های شما را رمزگذاری می‌کند و از جاسوسی اشخاص ثالث در اتصال شما جلوگیری می‌کند.
- اتصالات خودکار وای‌فای را غیرفعال کنید.
- سیستم عامل و برنامه‌های خود را مرتباً به‌روزرسانی کنید.
- از احراز هویت دو عاملی (2FA) استفاده کنید.
- برای حساب‌های مهم، تأیید دو مرحله‌ای را فعال کنید، که حتی اگر رمز عبور شما به خطر بیفتد، یک لایه محافظتی اضافی اضافه می‌کند.
- از دانلود برنامه‌ها از فروشگاه‌های رسمی خارج از کشور خودداری کنید، زیرا برخی حاوی بدافزارهایی هستند که آسیب‌پذیری‌هایی را در دستگاه شما ایجاد می‌کنند.
- از رمزهای عبور قوی و منحصر به فرد استفاده کنید، از رمز عبور یکسان برای بیش از یک حساب استفاده نکنید و در صورت لزوم از یک مدیر رمز عبور استفاده کنید.

صنایع هواپیمایی و حمل‌ونقل آمریکا و بریتانیا در معرض حمله سایبری

شرکت آلفابت، مالک چندملیتی گوگل، در پی وقوع چندین حمله سایبری، به نهادهای فعال در حوزه هواپیمایی و حمل‌ونقل در ایالات متحده و بریتانیا هشدار داده تا سطح امنیت سایبری خود را افزایش دهند.

هشدار پس از تحلیل‌های اولیه‌ای منتشر شده که نشان می‌دهد برخی از این حملات، مشابه الگوهای حملات سایبری گروهی به نام «اسکترد اسپایدر» (عنکبوت پخش‌شده) بوده است.آلفابت اعلام کرده در حال بررسی و تحلیل اسناد و داده‌های مربوط به این حملات است، اما نشانه‌هایی وجود دارد که حاکی از فعالیت‌های هدفمند این گروه در حملات اخیر است.پیش از این هشدار، شرکت‌های امنیتی نیز نسبت به تهدیدهای مشابه هشدار داده بودند. گروه اسکترد اسپایدر نخستین بار در ماه آوریل زمانی به صدر خبرها آمد که با اجرای حمله سایبری به فروشگاه‌های زنجیره‌ای هروتز و مارک اند اسپنسر در بریتانیا، کنترل سیستم‌های آن‌ها را به‌دست گرفت و در قبال بازگرداندن دسترسی، درخواست باج کرد.براساس برآوردها، اعضای این گروه عمدتا از میان جوانان بریتانیایی و آمریکایی هستند و با تمرکز بر اهداف خاص، عملیات خود را پیش می‌برند.

این هشدارها بار دیگر نگرانی‌ها درباره حملات سایبری سازمان‌یافته به زیرساخت‌های کلیدی را افزایش داده است.

هشدار متخصصان قلب: هرگز اول صبح گوشی را چک نکنید

متخصصان قلب هشدار می‌دهند که چک‌کردن گوشی در ساعت نخست پس از بیدار شدن می‌تواند تاثیر منفی جدی بر سلامت قلب داشته باشد.

به گفته این پزشکان، کارهایی مانند مرور اخبار منفی، تماشای ویدیوهای کوتاه و حتی پاسخگویی به پیام‌ها در ابتدای صبح سطح استرس را افزایش می‌دهد و می‌تواند سلامت عمومی، به‌ویژه سلامت قلب، را به خطر بیندازد.

با این حال، دکتر الکساندرا خرازی، جراح قلب و قفسه سینه، تاکید می‌کند که موضوع فقط ترشح هورمون‌های استرس نیست؛ بلکه این عادت، مسیر کلی روز شما را مشخص می‌کند و ممکن است آغازگر یک روز پرتنش و ناسالم شود.

او هشـــدار می‌دهد که بررسی گوشی بلافاصله پس از بیدار شدن نه‌تنها ممکن است احساس اضطراب یا ترس از جا ماندن را برانگیزد، بلکه فرد را از انجام فعالیت‌هایی که برای سلامت قلب مفیدند، هم بازمی‌دارد.

به گفته او، این زمان می‌تواند به کارهایی چون آماده‌کردن یک صبحانه سالم، مدیتیشن، لذت بردن آگاهانه از یک فنجان قهوه یا چای، حرکات کششی، ورزش سبک، پیاده‌روی یا حتـــی گذراندن چند دقیقه با اعضای خانواده اختصاص یابد- عاداتی که همگی به سلامت قلب کمک می‌کنند.

البته دکتر خرازی تنها متخصصی نیست که درباره استفاده زودهنگام از گوشی تلفن همراه هشـــدار می‌دهد. دکتر پل بلا، متخصص قلب و اســـتاد پزشکی در تگزاس، هم می‌گوید: «کاملا روشن است که استرس‌های روانی حاد و مزمن با افزایش فشار خون و بیماری‌های قلبی مانند حمله قلبی و نارسایی قلب مرتبط اند. بنابراین، اگر چک کردن گوشی در ابتدای روز برای فرد تجربه‌ای منفی یا استرس‌زا باشد، این ارتباط شناخته‌شده در مورد او نیز صدق می‌کند.»

پزشکان توصیه می‌کنند برای محافظت از سلامت قلب، روزتان را با عاداتی آرامبخش، هدفمند و مفید آغاز کنید و تماس با فضای مجازی را تا بعد از شروع فعالیت‌های روزمره به تعویق بیندازید. بنابراین اگر محتویات رسانه‌های اجتماعی شما مملو از اخبار منفی، تصاویر ناامیدکننده یا نمایش موفقیت‌ها و خوش‌گذرانی‌های دیگران باشد، ممکن است بی‌آنکه بدانید، در حال آسیب‌زدن به سلامت روان و قلبتان باشید.

دکتر چنگ هان چن، متخصص قلب و عروق و مدیر یک مرکز پزشکی در کالیفرنیا،

هم هشدار می‌دهد که استفاده مداوم از گوشی، به‌ویژه در ساعات اولیه صبح، می‌تواند به شکل‌گیری عادت‌هایی ناسالم مانند بی‌تحرکی منجر شود و این بی‌تحرکی می‌تواند خطر ابتلا به مشکلات متابولیکی و قلبی-عروقی را افزایش دهد- مشکلاتی که به نوبه خود می‌توانند به افزایش فشار خون، کلسترول بالا، چاقی و دیابت نوع ۲ منتهی شوند.

به گفته دکتر خرازی، برای جایگزین کردن این عادت، بهتر است روزتان را با حرکت و فعالیت بدنی، ترجیحا زیر نور طبیعی خورشید، آغاز کنید. پیشنهاد او پیاده‌روی یا دویدن کوتاه، انجام دادن چند حرکت ساده یوگا یا حتی کشش‌های سبک در حیاط خانه اســـت که همگی آثاری به‌مراتب بهتر از بالاپایین کردن مطالب در شـــبکه‌های اجتماعی بر سلامت قلب و روان دارند.

البته دکتر چن تاکید می‌کند که اینترنت و رسانه‌های اجتماعی در صورتی که درست اســـتفاده شوند، فواید زیادی هم دارد. مثلا می‌توانید از گوشی برای افزایش آگاهی در مورد سلامت، دسترسی به اطلاعات پزشکی یا پیوستن به گروه‌های حمایتی مجازی استفاده کنید، اما زمان و مرز مشخص برای استفاده از آن بسیار مهم است و نباید هنگام بیدار شدن از خواب، قبل از خواب یا موقع غذا خوردن از آن استفاده کنید.

گوگل از خودسری رژیم صهیونیستی در سوءاستفاده از ابزارهایش مطلع بود

اسناد داخلی گوگل نشان می دهد این شرکت پیش از امضای قرارداد با رژیم صهیونیستی از ریسک عدم نظارت بر استفاده از ابزارهایش توسط آن مطلع بوده است.

به گزارش اینترســـپت، طبق یک گزارش محرمانه داخلی که در ماه می ســـال جاری میلادی در این نشـــریه منتشر شـــد، اکنون مشخص شده گوگل قبل از امضای پروژه جنجالی «نیمبال» با رژیم صهیونیستی می دانست که احتمالا نتواند شیوه استفاده این رژیم و ارتش آن از فناوری قدرتمند ابر رایانشی اش را کنترل کند.

در این گزارش به طور واضح توضیح داده شده که گوگل از مدت ها قبل ریسک فراهم کردن ابزارهای نوین ابر رایانشی و هوش مصنوعی برای رژیمی که از مدت ها قبل به نقض حقوق بشر متهم است را می دانست. این شرکت آمریکایی می دانست نه تنها نمی تواند شیوه استفاده رژیم صهیونیستی از محصولاتش برای آسیب رساندن به مردم فلسطین را رصد یا جلوگیری کند، بلکه در گزارش ذکر شـــده این قرارداد ممکن است گوگل را ملزم به جلوگیری از تحقیقات جنایی توسط کشورهای دیگر در مورد استفاده رژیم صهیونیستی از فناوری‌اش کند.

همچنین این قرارداد شـــامل همکاری نزدیک با تشکیلات امنیتی رژیم صهیونیستی ازجمله رزمایش‌های مشـــترک و تبادل اطلاعات می شود که در قراردادهای گوگل با سایر کشورها بی‌سابقه بوده است.

مشاور طرف ثالثی که گوگل برای بررسی این قرارداد استخدام کرده بود نیز به شرکت توصیه کردش به دلیل این عوامل خطر، ابزارهای یادگیری ماشینی و هوش مصنوعی را در اختیار رژیم صهیونیستی قرار ندهد.

سه کارشناس حقوق بین المللی در گفت‌وگو این نشریه اعلام کردند آگاهی گوگل از خطرات واطلاع قبلی از اینکه نمی‌تواند بررسی‌های لازم استاندارد را در این قرارداد انجام دهد، ممکن است برای این شرکت مسئولیت قانونی ایجاد کند.

نخستین بار نشریه نیویورک تایمز بخش هایی از این سند داخلی را منتشر کرد اما اطلاع گوگل از آنکه نمی تواند بر شیوه استفاده رژیم صهیونیستی از ابزارهایش نظارت کند، قبل آن فاش نشده بود.

عمیق تر شدن شکاف بین اوپن‌ای‌آی و مایکروسافت

اگرچه مایکروسافت زمانی یکی از شتاب‌دهنده‌های اصلی توسعه اوپن‌ای‌آی بود اما روابط این شرکت‌ها پرتنش شده، بطوریکه شکاف موجود بین آنها در حال گسترش است.
اطلاعات گزارش «وال‌استریت ژورنال» نشان می‌دهند که شرکت‌های «اوپن‌ای‌آی»(OpenAI) و «مایکروسافت» ممکن است به یک نقطه اوج در مشکلات خود رسیده باشند.
به گزارش تک کرانچ، این گزارش به نقل از منابع ناشناس می‌گوید که مدیران اوپن‌ای‌آی در طول همکاری خود، به طور علنی مایکروسافت را به رفتار ضد رقابتی متهم کرده‌اند.
همچنین، مدیران اوپن‌ای‌آی درباره این که آیا درخواست بررسی مجدد قرارداد خود با مایکروسافت را از سوی نهاد نظارتی فدرال آمریکا داشته باشند یا خیر، بررسی‌هایی انجام داده‌اند.
اوپن‌ای‌آی در تلاش است تا تسلط مایکروسافت را بر مالکیت معنوی و منابع محاسباتی خود کاهش دهد اما این استارت‌آپ برای تکمیل روند تبدیل شدن به یک شرکت انتفاعی، به تأیید این غول فناوری نیاز دارد.
این دو شرکت بر سر خرید سه میلیارد دلاری استارت‌آپ کدنویسی هوش مصنوعی «ویندسرف»(Windsurf) توسط اوپن‌ای‌آی در بن‌بست قرار دارند. براساس این گزارش، اوپن‌ای‌آی نمی‌خواهد مایکروسافت مالکیت معنوی ویندسرف را به دست بیاورد زیرا این کار می‌تواند «GitHub Copilot» - سیستم کدنویسی هوش مصنوعی این ارائه‌دهنده خدمات فضای ابری - را تقویت کند.
اگرچه مایکروسافت زمانی یکی از شتاب‌دهنده‌های اصلی توسعه اوپن‌ای‌آی بود اما روابط این شرکت‌ها پرتنش شده است. براساس گزارش‌ها، اوپن‌ای‌آی در ماه‌های اخیر تلاش کرده است تا وابستگی خود به مایکروسافت را برای خدمات فضای ابری کاهش دهد.

استفاده از سامانه هوش مصنوعی آلمانی - سوئدی در جنگ هوایی

شرکت‌های هلسینگ و ساب برای نخستین‌بار با موفقیت یک سامانه هوش مصنوعی را که برای هدایت نبرد هوایی در یک جت جنگی نصب شده بود، آزمایش کرده‌اند.
به گزارش دویچه وله، یک فناوری هوش مصنوعی آلمانی - سوئدی برای نخستین بار در سناریویی عملیاتی به‌طور مستقل یک جنگنده را هدایت کرد. این سیستم دارای «توانایی‌هایی مشابه انسان» در نبرد هوایی و جهشی در سامانه دفاع هوایی اروپا به شمار می‌رود.
شرکت‌های هلسینگ (Helsing) و ساب (Saab) برای نخستین‌بار با موفقیت یک سامانه هوش مصنوعی را که برای هدایت نبرد هوایی در یک جت جنگی نصب شده بود، آزمایش کرده‌اند.
مجله تخصصی هارتپونکت که در حوزه امنیت فعالیت می‌کند، در گزارش خود نوشت تیم پروژه آلمانی-سوئدی موفق شده‌اند عامل هوش مصنوعی با نام «Centaur» را در جنگنده سوئدی Gripen E نصب کرده و در چارچوب دو پرواز آزمایشی در اواخر ماه مه و اوایل ژوئن بر فراز دریای بالتیک فعال کنند.
در این پروازها، هوش مصنوعی در برخی مواقع کنترل کامل جنگنده را بر عهده گرفته است. محور اصلی آزمایش، بررسی سناریوهای موسوم به « بردهای هوایی خارج از میدان دید» (Beyond-Visual-Range) بوده است.

نخستین پرواز آزمایشی

به گفته این شرکت‌ها، سامانه Centaur در این فرآیند به‌طور پیوسته داده‌های حسگرها را تحلیل می‌کرد، مانورها را طراحی و به‌طور خودکار اجرا می‌نمود.
یک خلبان پروازها را از نظر ایمنی همراهی می‌کرد و یک جنگنده دیگر به عنوان دشمن شبیه‌سازی‌شده عمل می‌کرد. این آزمایش بخشی از پروژه مشترک «Project Beyond» بوده که به گفته شرکت ساب هدف آن پژوهش در زمینه توانایی‌های رزمی پشتیبانی‌شده با هوش مصنوعی است.
معماری نرم‌افزاری Gripen E طوری طراحی شده که حتی سیستم‌های پیچیده هوش مصنوعی را می‌توان به سرعت در آن ادغام کرد. از مرحله طراحی تا نخستین پرواز تنها شش ماه طول کشیده است.

توانایی‌های مشابه انسان

استفانی لینگمان از شرکت هلسینگ این آزمایش را «نقطه عطفی برای دفاع اروپا» توصیف کرده است.
سرعتی که با آن قابلیت‌های جدید قابل ادغام هستند، به گفته او، کارایی سیستم‌های کنترل‌شده با نرم‌افزار را نشان می‌دهد. آنتوان بورد، معاون هلسینگ توضیح داده که Centaur با یادگیری تقویتی (Reinforcement Learning) آموزش داده می‌شود و می‌تواند طی یک روز دهها تجربه مجازی به‌دست آورد.
این سیستم اکنون دارای «توانایی‌هایی مشابه انسان» در نبرد هوایی است و قرار است در آینده فشار کاری خلبانان را کاهش دهد.
مارکوس وانت، خلبان آزمایشی ساب، بر همکاری نزدیک دو شرکت تأکید کرد: «این نشان می‌دهد نرم‌افزار Gripen E چقدر برجسته است، فناوری یاد شده تا چه اندازه توسعه یافته و مهندسان دو شرکت چقدر خوب با هم همکاری می‌کنند.»
به گفته شرکت ساب، سومین پرواز که در سوم ژوئن انجام شده، بر پایداری و توانایی تطبیق سامانه تمرکز داشته است. در این آزمایش برد حسگرها، سرعت‌ها و داده‌های ارتباطی تغییر کرده‌اند. پروازهای بیشتر برای بهینه‌سازی این سامانه در سال جاری برنامه‌ریزی شده‌اند.این پروژه بخشی از مطالعات مفهومی جنگنده آینده (Future Fighter Concept Studies) به سفارش اداره تدارکات نظامی سوئد است.

Iran Opens First Phase of 600 MW Solar Plant in Isfahan

Iran has opened the first phase of its largest solar power plant as part of a massive government program to expand renewables capacity in the country.

Iranian President Masoud Pezeshkian used a video link to open a 120 megawatt (MW) unit of the Aftab Shargh solar farm in the central province of Isfahan.

Iran's minister of industries Mohammad Atabak and senior local officials attended a ceremony in Kuhpayeh, in the east of the province of Isfahan, to inaugurate the facility.

Aftab Shargh (meaning Sunlight of the East in Persian) will become Iran's largest and most technologically advanced solar power plant when it reaches a full electricity generation capacity of 600 MW by March 2027.

The power plant has been built by Mobarakeh Steel Company, the largest steel maker in the West Asia region. According the reports, the company had provided some 305 million euros in funding for the project.

The power plant had created 3,000 jobs for local people during its construction period, adding that the facility will employ 70 people on a permanent basis after the launch of its first phase.

The province of Isfahan, which is one of the most industrial regions in Iran, has emerged as a key player in Iran's plans to increase its renewable electricity generation capacity by 30,000 MW in the next four years. The province currently has 240 MW of solar farms and plans to expand them by more than 470 MW by February.

Local authority said Isfahan plans to meet a target of 5,300 MW of solar capacity by 2029 which will account for nearly a third of Iran's total solar capacity at that time.

Iran Charts a Strategic Path in Quantum Technology Development

Iran's Vice Presidency for Science, Technology, and Knowledge-Based Economy has launched a comprehensive initiative to support quantum technology as the country prepares for a transformative role in the global digital future.

With the global race toward quantum innovation accelerating, Iran's entry into this field signals a strategic national shift toward high-tech self-reliance and future-oriented economic development. The designation of 2025 as the "Year of Quantum" underscores the urgency for countries like Iran to invest in this disruptive and security-critical technology, which is poised to revolutionize sectors from communication to energy and medicine.

The Vice Presidency stresses that quantum technology requires deep interdisciplinary expertise in physics, mathematics, computer science, and engineering. "This is a long-term process that demands heavy investment in infrastructure, software, and international cooperation," the statement reads.

Quantum technology blends physics, engineering, and computing to enable ultra-secure communication, high-speed processing, and advanced sensing capabilities. Quantum computers can solve problems that are intractable for classical systems, while quantum sensors enhance medical diagnostics, and quantum communication offers security beyond traditional encryption.

The global quantum technology market is projected to exceed 1$ trillion by 2035, with leading countries already investing billions. Iran's scientific foundations in photonics, theoretical mathematics, and physics provide a springboard for advancement.

شرکت مخابرات ایران
(سهامی عام)

۵هزار دقیقه مکالمه رایگان درون استانی برای همه

و **یک ماه** مکالمه رایگان درون استانی و بین استانی، بدون محدودیت برای مشترکان خانگی

حرف دلت رو بزن

ما حساب کردیم

رایتل
RighTel
www.rightel.ir
یک ارتباط هوشمند

با ما در ارتباط باشید


مدیریت دورکاری
Enterprise Business
به سبک
راهکارهای سازمانی ایرانسل
Teleworking
ایرانسل
MTN
Business.irancell.ir
EB@mtnirancell.ir