# عصر ارتباط

شـــنبه ۱۹ آبان ۱۴۰۳ ■ ســـال بیست و دوم ■ شـــماره ۱۱۰۵ ■ ۸صفحه ■ ۲۰۰۰۰ تومان

WWW.ASREERTEBAT.COM ■ Sat. 09 NOVEMBER 2024 ■ Vol.22 ■ No.1105


با سفر وزیر ارتباطات به کوبا و ونزوئلا انجام شد

# گام نخست دیپلماسی فناوری در دولت چهاردهم

۵

# تحریم صرافی‌های رمزارز ایرانی؛ حقیقت یا شایعه؟

یادداشت

# فیلترینگ و منع رطب خورده

سعید کاظمی
کارشناس ارشد مدیریت فرهنگی

در خصوص مباحث اخیر موافقان رفع فیلترینگ و یا مخالفان رفع فیلترینگ صحبت‌های متعددی از سوی کارشناسان محترم و مجریان و متولیان امر و ... به کررات در این سالیان اخیر شده است لیکن علی ایحال وقتی بیش از ۶۰ درصد مردم از فیلتر شکن استفاده می کنند جای بسی تأمل دارد.

مساله اینجاست که وقتی حوزه‌های آموزشی، دانشگاهی و معارفی و اندیشکده‌های مختلف فرهنگی و اجتماعی در این حوزه با تمام جدیت و برنامه وارد نشوند، کار، موضوعیت و فرایندش ابتر و بدون نتیجه خواهد ماند.

وقتی در زمینه‌های مختلف، فرهنگ سازی و کادر سازی و برنامه‌ریزی نداریم منتج به همین دوگانگی و تضادهای رفتاری می‌شود.

وقتی در آموزش و پرورش‌مان از دیرباز روی نسخه‌های پلتفرم‌ها از منظر ساختاری و رفتاری کار نشده و نتوانسته‌ایم سواد فرهنگ رسانه‌ای‌مان را بهبود و ارتقا دهیم بتدریج منتج به‌همین نتایج می‌شود.

وقتی از خرده‌فرهنگ‌ها فاصله می گیریم و در آن هیچ نظارت و راهبری و آموزشی وجود ندارد بتدریج مورد هجمه خوراک و اطلاعات ناقص و ضد و نقیض قرار خواهیم گرفت.

آری! سواد فرهنگی و رفتاری در مواجهه با فضای مجازی و بسترهای لازم در این خصوص پائین است و مصداق این است که چطور رطب خورده، منع رطب کند؟!

افراط و تفریط‌ها بلای جان مردم شده و چاره این است که طوری بستر را فراهم کنیم تا بدون کوچکترین حساسیتی مردم عزیزمان بسمت رسانه‌های جمعی و گروهی رو آورند و یک پیوند و آشتی ملی و ناگسستنی را باید شکل دهیم.

در رسانه‌های گروهی و ملی که از بودجه کشور ارتزاق می کنند باید از بهترین، مجرب‌ترین و خبره‌ترین عناصر کلیدی و اجرایی و برنامه‌سازها استفاده بهینه و شایسته شود و بی‌شک در صورت تحقق این مهم بهترین خروجی را در نظرسنجی‌ها خواهیم داشت.

متأسفانه سیاست گذاری‌های کلان در زیر ساخت‌های این رسانه ملی گاهاً بدون پشتوانه فنی و کارشناسی و بصورت ابزاری و غیر حرفه‌ای و غیرعقلایی، هدایت، اداره و راهبری می‌شود و چهره حاکمیت را هم مکدر و مخدوش می کنند.

برنامه‌سازان رسانه ملی باید از نوآوری و خلاقیت و ابتکار عمل برخوردار بوده و از تکرار مکررات و کپی معکوس و مهندسی معکوس دست برداشته و نسبت به غنی کردن اوقات فراغت مردم شریف و نجیب کشورم بیش از پیش اهتمام ویژه‌ای ورزیده و در راستای رسالت خبری و خدمتگزاری تلاش‌های مضاعف و بی شائبه‌ای را داشته باشند.

همچنین در سیاست‌های کلان خود نسبت به کاهش متناسب نیروی انسانی و حذف شبکه‌های اضافی و غیر ضروری را مد نظر داشته و به محتوی و رسالت خبری و مدنیت اجتماعی در این رسانه ملی توجهی اساسی و بنیادی کنند تا این رسانه ملی بتواند به درخشش رسیده و به جایگاه اصلی خودش برگردد.

با این تفاسیر فیلترینگ کردن در شرایط خاص و ناهمگن و در شرایط فورس ماژور که امنیت ملی در فضای سایبری و مجازی را دستخوش تغییرات می کند و در معرض نشر و خبرهای مغرضانه در بحران‌هایی که منافع و امنیت ملی را نشانه رفته اعمال محدودیت و فیلترینگ باید استفاده صحیح رفتاری و مدیریت شود.

در خاتمه هدف از این تحلیل و نقد کوتاه؛ بهبود و ارتقای سطح سرانه نظام فرهنگی و اجتماعی در حوزه جوانان و نوجوانان (خانواده) تعمیم و توسعه فرهنگ عمومی و بهره‌وری از دانش و خرد اجتماعی، تنویر افکار عمومی در خصوص مسائل روز و بینش اجتماعی و تحلیل مسائل، در راستای خدمتگزاری و رضایت‌مندی مردم شریف توأم با وفاق ملی و وحدت و همدلی بود.

علی ایحال چه بخواهیم چه نخواهیم دنیا و عصر حاضر به سمت و سوی مدرنیته و عصر دیجیتال پیش رفته و در حال تسخیر فضاهای مادی و معنوی است.

در چنین شرایطی باید هنر بدست آوردن ابتکار، خلاقیت، نوع آوری و فن‌آوری‌های مختلف فرهنگی و اجتماعی و سیاسی و اقتصادی و ... را به نسل جدید اعم از جوانان و نوجوانان را آموزش داده و از بروز و ظهور مخاطرات پیش روی و آینده این عزیزان را بیش از پیش آگاه و مطلع سازیم و در راستای رسالت خبری و تنویر افکار عمومی و اطلاع‌رسانی‌های متعدد و مختلف گام‌های اصولی واساسی‌تری بر داریم.

روزنامه هاآرتص گزارش داد

# نشت اطلاعات حساس مقامات اسرائیل توسط ایران

آزاده کیاپور

گروه مرتبط با اطلاعات ایران، ایمیل‌هایی را که ظاهرا از چهار مقام سابق و فعلی اسرائیلی سرقت شده، منتشر و اعلام کرده که یائیر گولان و سخنگوی فارسی زبان ارتش اسرائیل، هدف بعدی خواهند بود.

هاآرتص در گزارشی نوشت، هکرهایی که به نظر می‌رسد با نهادهای امنیتی ایران مرتبط هستند، اطلاعات شخصی را که ظاهرا از حساب‌های مربوط به مقامات ارشد دفاعی و سیاسی اسرائیل به سرقت رفته، فاش کرده‌اند.

برخی از اطلاعات هک‌شده، جزییات حساس را شامل می‌شود. از جمله اطلاعات نشت‌شده، ایمیل‌هایی است که به گفته هکرها از حساب‌های شخصی دو مقام سابق و دو مقام فعلی به دست آمده است. یکی از موارد، شامل فهرست تماس‌های یک مقام بوده است.

این اطلاعات به تازگی در سایت اختصاصی ایجادشده توسط این گروه هکری منتشر شده و لینک‌های مربوط به آن در کانال تلگرام گروه مذکور، قرار داده شده است. در روزهای اخیر، این گروه، تهدید کرده اطلاعات بیشتری درباره دو مقام اسرائیلی یعنی یائیر گولان، رئیس حزب دموکرات و معاون سابق رئیس ستاد ارتش و کمال پنحاسی، سخنگوی فارسی زبان ارتش، منتشر می کند.

محققان اسرائیلی با این گروه آشنایی دارند و آن را یکی از شاخه‌های مختلف شبکه جنگ سایبری ایران، که تمرکز اصلی‌اش روی راه‌اندازی کمپین‌های نفوذ است، می‌دانند.

یکی از پژوهشگران اداره ملی سایبری گفت: «این گروه به عنوان پلتفرمی برای تقویت هک‌های خود عمل می کند - که برخی بسیار موفق و برخی دیگر، کمتر موفق بوده‌اند- تا با استفاده از تکنیک‌های جنگ روانی به منظور ایجاد ترس و ارعاب، بر اقتصاد اسرائیل تاثیر بگذارند.»

وی افزود: «برخی از مطالب منتشرشده، نه از هک‌های این گروه، بلکه از نشت‌های قبلی هستند که سال‌ها در اینترنت در حال گردش بوده‌اند، مانند عکس‌های سیاستمدارانی که منتشر شده‌اند و برخی از مطالب نیز به راحتی در اینترنت قابل دسترس هستند. در برخی موارد، فقط تهدیدهایی وجود داشته و هیچ شواهدی از آسیب‌دیدگی مشاهده نمی‌شود.»

## آگاهی مقامات اسرائیلی از عملیات هک

مقامات اسرائیلی و مسئولانی که گفته می‌شود اکانت‌های آنها هک شده، از این عملیات آگاه هستند. از اکتبر سال گذشته، زمانی که حمله ناگهانی حماس به اسرائیل، موجب آغاز جنگ در غزه و تشدید درگیری‌ها با حزب‌الله شد، اسرائیل با سیل بی‌سابقه‌ای از حملات سایبری مواجه شده است.

حجم زیادی از اطلاعات، به صورت آنلاین افشا شده که عملیات هک علیه نهادهای مختلف، از جمله وزارت دادگستری، وزارت دفاع و مرکز تحقیقات هسته‌ای نِگو (Negev) را شامل می‌شود.

تحقیقات نشان می‌دهد هرچند برخی از گروه‌های هکر ایرانی، اطلاعات را جمع‌آوری کرده و آسیب‌های واقعی ایجاد می کنند اما گروه پشت آخرین افشاگری، یک گروه حمله سایبری عادی نیست، بلکه یک دارایی دیجیتال است که برای کمپین‌های اطلاعاتی و نفوذ استفاده می‌شود.

یکی از محققان می گوید: «هدف هک، لزوما نباید یک هدف باکیفیت باشد. اطلاعاتی که منتشر می‌شود، نیاز به قابل اعتماد بودن ندارد و عمدتا برای ایجاد سروصدا طراحی شده است.»

او اضافه می کند: «به نظر می‌رسد در گروه‌های اطلاعاتی ایران، تقسیم کار وجود دارد. گروه‌های هکر به اطلاعات اولیه دسترسی پیدا می کنند و سپس تحلیلگران تعیین می کنند که آیا هدف ارزشمند است یا خیر. اگر ارزشمند باشد، اطلاعات بیشتری به طور مخفیانه جمع‌آوری می‌نمایند. در غیر این صورت، ممکن است تصمیم بگیرند دوباره حمله کنند و اطلاعات را رمزگذاری کرده تا باج بخواهند یا فقط با افشای اطلاعات به صورت آنلاین، باعث سرافکندگی دیگران شوند.»

> این گروه هکری به طور مداوم، گروه‌های جدید تلگرامی ایجاد می‌کند تا جایگزین گروه‌هایی شود که احتمالا به درخواست اسرائیل حذف شده‌اند. هاآرتص به‌تازگی فاش کرده اسرائیل از ابزارهای مختلف برای تلاش جهت حذف اطلاعات حساس افشاشده استفاده می‌کند اما در این زمینه، فقط موفقیت جزئی داشته است

یک منبع اطلاعاتی اخیرا به هاآرتص گفته که این افشاگری‌ها، بخشی از جنگ سایبری گسترده‌تر بین اسرائیل و ایران است.

به گفته وی، «اکنون صحبت درباره نفوذ سایبری، جنگ روانی، تحقیر، ارعاب، اختلال و ایجاد آشوب بیشتر، رایج شده است. این افشاگرها به همان اندازه که شبکه‌های نفوذ و سایت‌های خبری جعلی نقش دارند، در این زمینه دخیل هستند. ما موارد مشابهی را در اسرائیل دیده‌ایم و هنوز هم مشابه آنها را در ایالات متحده تا زمان انتخابات ریاست جمهوری خواهیم دید.»

## افشای اطلاعات از کمپین ترامپ

در دو ماه گذشته، اطلاعاتی از کمپین دونالد ترامپ، نامزد جمهوری‌خواه، افشا شده که وزارت دادگستری ایالات متحده آن را به هکرهای ایرانی نسبت داده است. هکرهای ایرانی که پشت آخرین افشاگری قرار دارند، از ابزارهای فناوری مختلف برای تقویت این کار استفاده می کنند. آنها سایتی را روی سرورهای غیرمتمرکز راه‌اندازی کرده‌اند که پاک کردن آن را دشوار می‌سازد.

این گروه هکری به طور مداوم، گروه‌های جدید تلگرامی ایجاد می کند تا جایگزین گروه‌هایی شود که احتمالا به درخواست اسرائیل حذف شده‌اند. هاآرتص به‌تازگی فاش کرده اسرائیل از ابزارهای مختلف برای تلاش جهت حذف اطلاعات حساس افشاشده استفاده می کند اما در این زمینه، فقط موفقیت جزئی داشته است.

در همین حال، آمریکا تلاش می کند هکرهای خارجی را شناسایی کند. این کشور، سه ایرانی را که مظنون به هک حساب‌های دیپلمات‌ها، افسران سابق اطلاعاتی و کمپین ترامپ هستند، متهم کرده است. به تازگی، دو هکر سودانی نیز به اتهام اداره گروه هکری «آنونیموس سودان» و اختلال در وب‌سایت‌های اسرائیل و برنامه هشدار اضطراری آن متهم شدند.

# «ناتمام‌های فاوای کشور»

**دولت‌ها و مسوولان می‌آیند و می‌روند، اما طرح‌ها، پروژه‌ها و مشکلات همواره می‌مانند. رسانه‌ها و افکار عمومی هم به علت انباشت مشکلات قبلی و زایش طرح‌ها و پروژه‌های جدید، با فراموشی مواجه بوده و هستند. ما اما تلاش کرده‌ایم تا به شکلی ثابت پیگیر سرنوشت مسایل و طرح‌های حوزه کاری خود باشیم. به همین منظور فهرست حاضر که در آینده اصلاحات بیشتری روی آن اعمال شده و موضوعات بیشتری به آن اضافه خواهد شد، صرفا به عنوان یک حافظه عمل خواهد کرد و هر از گاهی اقدام به باز نشر آن خواهیم کرد. در دوره این بازنشرها طبعا موضوعات و سوژه‌هایی از «حافظه حوزه ICT کشور» کم یا اضافه خواهد شد که اطلاع‌رسانی لازم در خصوص آنها را انجام خواهیم داد. تحریریه هفته‌نامه عصر ارتباط معتقد است که این فهرست قطعا ناقص بوده و موضوعات متعددی باید به آن اضافه شود تا به عنوان شاخص و داشبوردی در مقابل مردم و مسوولان بخش‌های متخلف کشور عمل کند. لذا از تمامی علاقه‌مندان و فعالان نیز دعوت می‌شود موارد مد نظر خود را از طریق ایمیل report@asreertebat.com یا شماره تلفن ۸۸۹۴۷۴۵۲ به ما اعلام کنند.**

### تجمیع داده‌های مدیریت بحران

مرکز کنترل هماهنگی عملیات سازمان امداد و نجات از پنج سال قبل نرم‌افزار جامع اطلاعاتی مکانی را راه‌اندازی کرده است. این نرم‌افزار به لحاظ زیرساختی ظرفیت آن را دارد که سایر ارگان‌ها نیز به آن متصل شده و ضمن به‌اشتراک گذاری اطلاعات خود از خدمات آن منتفع شوند؛ اتفاقی که تاکنون همچنان محقق نشده است.

### سامانه دسترسی آزاد به اطلاعات

با وجود آنکه قانون انتشار و دسترسی آزاد به اطلاعات سال ۸۸ تصویب شده اما تا تیرماه سال ۹۶ با وجود الزام قانون و ابلاغ آیین‌نامه آن، راه‌اندازی سامانه به تعویق افتاده بود. حال اما باوجود راه‌اندازی سامانه همچنان بسیاری از ۴۸۰ دستگاهی که باید در این سامانه عضو شوند به آن متصل نشده‌اند.

### پیوست فناوری طرح‌های کلان

۱۸ فروردین ۱۳۹۶ رییس سندیکای صنعت مخابرات از تدوین پیوست فناوری برای طرح‌های کلان ICT دارای شریک خارجی خبر داد و اعلام کرد هدف این سند انتقال دانش فنی در قراردادهای خارجی است. این سند باید پس از تایید و تصویب توسط وزیر ارتباطات به منظور طرح در ستاد اقتصاد مقاومتی ارسال شده و به تصویب می‌رسید که البته همچنان این اتفاق نیفتاده است.

### مهلت شش ماهه اصلاح سامانه‌های دولتی

شورای اجرایی فناوری اطلاعات در جلسه ۲۸ فروردین ۱۳۹۶ براساس پیشنهاد وزارت ارتباطات و فناوری اطلاعات آیین‌نامه اجرایی استقرار چارچوب تعامل پذیری دولت الکترونیکی را به تصویب رساند. بر این اساس تمامی دستگاه‌های اجرایی موظف شدند حداکثر ظرف مدت شش ماه پس از ابلاغ مصوبه نسبت به اصلاح یا تکمیل پایگاه اطلاعاتی و یا بازطراحی سامانه‌های اطلاعاتی اقدام کنند که البته همچنان بسیاری‌ازدستگاه‌ها این کار را نکرده‌اند.

### فیلترینگ هوشمند

فیلترینگ هوشمند طرحی بود تا در عین حال که دسترسی به شبکه‌های اجتماعی مقدور باشد صفحات غیراخلاقی و مغایر با موازین نظام فیلتر شود. آن‌طور که منابع رسمی وزارت ارتباطات گفته‌اند، برای اجرای طرح فیلترینگ هوشمند احتمالا بیش از ۱۱۰ میلیارد تومان قرارداد میان وزارت ارتباطات و متخصصان در بحث فیلترینگ هوشمند پیش از این منعقد شده که البته اطلاعی از سرنوشت و خروجی آن نیست.

### سامانه‌های چکاوک ۲ و ۳

هشتم خرداد ۱۳۹۶ دبیرکل بانک مرکزی از راه‌اندازی سامانه‌های چکاوک ۲ و چکاوک ۳ خبرداد. چکاوک ۲ قرار بود موجب تجمیع آمار چک‌های درون‌بانکی با آمار چک‌های بین‌بانکی، توسط بانک مرکزی شود. ایجاد امکان واگذاری چک به مقصد حساب‌های دولتی نزد بانک مرکزی از شعب بانکی اقصا نقاط کشور نیز قابلیت ویژه‌ای بود که قرار بود چکاوک ۳ ایجاد کند، اما همچنان نسخه‌های ۲ و ۳ چکاوک عملیاتی نشده‌اند.

### اتصال منازل به فیبر نوری

وزیر وقت ارتباطات و فناوری اطلاعات در اوایل بهمن‌ماه سال ۹۴ وعده اتصال منازل به فیبر نوری را مطرح کرد و گفت فیبررسانی به منازل و محل کار مردم از ابتدای سال ۹۵ آغاز خواهد شد. این وعده البته جزو ماموریت‌های اپراتور چهارم ایرانیان‌نت بود که محقق نشده و حتی سرنوشت این اپراتور هم در هاله‌ای از ابهام قرار دارد.

### ایجاد شهر هوشمند خوارزمی

۱۶ خرداد ۱۳۹۶ یکی از اعضای هیات‌مدیره شرکت عمران شهرهای جدید از رایزنی با کره جنوبی برای امکان‌سنجی ایجاد شهر هوشمند برای شهر جدید «خوارزمی» خبر داد که قرار بود در جنوب شرقی تهران احداث شود. همچنین توسعه مشترک تحقیقات روی تکنولوژی ساختمان‌ها نیز یکی دیگر از قراردادهای امضاشده در تفاهم‌نامه با کره جنوبی بود که تا این لحظه هیچ گزارشی در خصوص دستاوردهای عملی این تفاهم‌نامه‌های امضاشده با کره‌ای‌ها منتشر نشده است.

# تحریم صرافی‌های رمزارز ایرانی؛ حقیقت یا شایعه؟

صرافی‌های بین‌المللی دارایی‌های رمزارز ایرانیان را مسدود و حساب‌های آنها را پس از افشای اطلاعاتی مبنی بر اینکه صرافی‌های محلی ممکن است با دولت ایران همکاری داشته باشند، مسدود کردند.

به گزارش عصر ارتباط این خبری است که در روزهای گذشته برخی از سایت‌های خارجی فعال در حوزه رمزارزها مدعی آن شده و نوشته‌اند: تحریم‌های اولیه و ثانویه دولت ایالات متحده، موجب خروج صرافی‌های بین‌المللی از بازار ایران و ایجاد شکافی شد که کارآفرینان محلی، به مرور زمان با صرافی‌های محلی، این خلأ را پر کردند.

در حال حاضر، بازار رمزارز در ایران پس از تحریم‌های ایالات متحده با چالش‌های جدی مواجه است و حساب‌های شهروندان ایرانی توسط صرافی‌های بین‌المللی، مسدود و دارایی‌های آنها فریز شده است. این تحریم‌ها، صرافی‌های بین‌المللی را از بازار ایران خارج کرده و منجر به افزایش فعالیت صرافی‌های محلی شده است.

در ادامه این گزارش ادعا شده این مطالعه، شبکه پیچیده‌ای از صرافی‌های متخلف از تحریم‌ها در ایران را روشن می‌سازد. در این رابطه، ۳ صرافی رمزارز به عنوان نهادهای با ریسک بالا شناسایی شده‌اند.

با وجود تشدید تحریم‌ها به دلیل عوامل ژئوپولیتیکی، بازار رمزارز ایران به طور قابل توجهی رشد پیدا کرده است.

بر اساس آمارهای منتشرشده اخیر، ایران، در حال حاضر، بیش از ۹۰ صرافی رمزنگاری دارد که بیش از ۱۰ مورد آنها، به عنوان صرافی‌های متمرکز فعالیت می‌کنند.

طبق ادعای یک کارشناس اطلاعات باز، ایران دارای حدود ۱۹ میلیون کاربر فعال رمزنگاری است که از این تعداد حدود ۶ میلیون نفر از یک صرافی ایرانی استفاده می‌کنند.

در بخش دیگری از این متن ادعاهایی مبنی بر وابستگی برخی از صرافی‌ها به نهادهای ایرانی و اتهامات و گمانه‌زنی‌هایی درباره احتمال این همکاری‌ها برای نقض قوانین بین‌المللی مبارزه با پولشویی و تامین مالی تروریسم شده است.

در ماه می امسال، دو سناتور ایالات متحده، ضمن مکاتبه با وزیر خزانه‌داری، مشاور امنیت ملی و وزیر دفاع، نگرانی‌های خود را درباره فعالیت‌های یک صرافی که ممکن است به دولت ایران کمک کند، ابراز کردند.

در ادامه این گزارش و بدون ارایه مستندات دقیق و قابل اتکا آمده است، اکنون جامعه رمزنگاری فارسی‌زبان از مسدود شدن حساب‌ها و محدودیت‌های کیف پول در یک صرافی داخلی به صرافی‌های متمرکز بین‌المللی گزارش داده‌اند.

بر اساس این گزارش از سال ۲۰۱۷، استفاده از صرافی‌های متمرکز بین‌المللی برای ایرانی‌ها، دشوار شده، زیرا دولت ترامپ، تحریم‌ها را تشدید کرد و این امر، به افزایش استانداردهای سخت‌گیرانه احراز هویت مشتری (Know Your Customer (KYC و قوانین مبارزه با پولشویی منجر شده است.

پیشتر چانگ‌پنگ ژائو (CZ)، بنیانگذار و مدیر عامل سابق بایننس، پس از اعتراف به نقض قوانین پولشویی ایالات متحده و در حین نظارت بر عملیات این صرافی، به چهار ماه زندان محکوم شد.

طبق گفته دادستان‌ها، ژائو با اجازه دادن به انجام معاملات میلیون‌ها دلاری، مرتبط با گروه حماس، یگان القسام، القاعده و ایران، قانون اسرار بانکی (BSA) این کشور را نقض کرد.

به گزارش عصر ارتباط، در سال‌های اخیر و با توجه به افزایش استفاده تجار ایرانی از رمزارزها و سرمایه‌گذاری برخی ایرانی‌ها روی رمزدارایی‌ها، فضای شایعات پیرامون ارایه‌دهندگان این خدمات نیز شدت بیشتری یافته است.

> همانطور که پیشتر نیز بارها از سوی مقامات کشور و رسانه‌ها هشدار داده شده، سرمایه‌گذاری در این بخش از سوی ایرانی‌ها همواره با احتمالات و چالش‌هایی نظیر هک، کلاهبرداری و تحریم مواجه است، ریسکی که ظاهرا برای فعالان این عرصه امری پذیرفته شده تلقی می‌شود

در همین حال برخی از این شایعات با هدف تضعیف پروژه ۱۰ برابر کردن تولید محتوای داخلی با رویکرد کسب‌وکار دیجیتال در سال ۱۳۹۵ به تایید ستاد فرماندهی اقتصاد مقاومتی رسید. در این مقطع حدود ۴۰ میلیارد تومان به این پروژه اختصاص یافت و قرار شد با توسعه محتوا تاثیر قابل توجهی بر حوزه‌های علمی، پژوهشی و اقتصادی کشور گذاشته شود. آخرین خبر از این طرح اما این است که ظاهرا اجرای آن به‌طور کلی از اولویت‌های پروژه اقتصاد مقاومتی خارج شده است.

صرافی‌های رقیب است. اگرچه در مواردی تحریم‌ها، بلوکه‌شدن و جرایمی نیز برای تعدادی از صرافی‌ها و ارایه‌دهندگان خدمات بین‌المللی رمزارز به واسطه امکان ردیابی مبدا و مقصد رمرارزها به اجرا درآمده است.

به همین جهت اگرچه هنوز و با قطعیت نمی‌توان موضوع تحریم صرافی‌های رمزارز ایرانی را حقیقت یا بخشی از جنگ مرسوم روانی و شایعه تلقی کرد، چراکه برخی صرافی‌های ایرانی در سال‌های اخیر برخلاف شایعات متعدد مبنی بر تحریم، ورشکستگی و توقف فعالیت‌هایشان، همچنان فعال بوده و توانسته‌اند به کاربران ایرانی خدمات ارایه کنند.

اگرچه خطر انسداد رمزارز ایرانی‌ها نیز یک شایعه به شمار نرفته و پیش از این اخباری از مسدودسازی در پلتفورم‌های خارجی منتشر شده است. موضوعی که بارها از سوی مقامات پلیس فتا نیز به کاربران ایرانی هشدار داده شده است.

### ● قانون و صرافی‌های رمزارز

بر اساس یافته‌ها صرافی‌های رمزارز فعال در کشور زیر نظر بانک مرکزی ایران فعالیت ندارند و برخلاف صرافی‌های سنتی و بانک‌های دارای مجوز، همچنان چارچوب و قاعده‌ای برای اعطای مجوز به آن‌ها وجود ندارد. البته این موضوعی است که در سایت برخی صرافی‌های رمزارز در ایران صراحتا مورد تاکید قرار گرفته است.

با این وجود این صرافی‌ها دارای درگاه‌های بانکی رسمی هستند که البته گاه و بیگاه دچار انسدادهایی از سوی بانک مرکزی نیز می‌شوند.

از سوی دیگر پلیس فتا نیز به‌عنوان مرجع اصلی رسیدگی به جرایم سایبری در کشور، هیچ فهرستی را تحت‌عنوان معرفی صرافی‌های موردتأیید منتشر نکرده است. بااین‌حال، انتشار سند «الزامات انتظامی و امنیتی صرافی‌های ارز دیجیتال» می‌تواند راهنمای فعالان این حوزه برای انتخاب صرافی‌هایی باشد که الزامات قانونی را رعایت می‌کنند.

نکته قابل توجه اینکه در یکی از سایت‌های صرافی رمزارز ایرانی آمده است: «اگر ارزهای دیجیتال را به چشم یک کالا ببینید که قابل خرید و فروش هستند، داشتن همین مجوزها برای اعتماد حداقلی به صرافی‌ها کفایت می‌کند؛ اما همچنان باید ریسک خرید و فروش ارزهای دیجیتال را خودتان قبول کنید.»

یا در نمونه‌ای دیگر در بخش قوانین یکی از صرافی‌های رمزارز ایرانی آمده است: نظر این صرافی قاطع میان طرفین خواهد بود و کاربر حق طرح هر ادعا را از خود سلب نمود:

- مجرد درخواست مراجع ذی صلاح یا پیگرد قضایی کاربر ولو به هر طریق، دلیل و نتیجه
- حجر یا فوت کاربر
- انتقال رمز ارز به کیف پول‌های رمز ارزی مشکوک یا مندرج در لیست سیاه این صرافی
- ظن به فعالیت‌های مشکوک با هر درجه، به تشخیص این صرافی و دسته کم به مدت ۷۲ ساعت

در نهایت باید گفت، همانطور که پیشتر نیز بارها از سوی مقامات کشور و رسانه‌ها هشدار داده شده، سرمایه‌گذاری در این بخش از سوی ایرانی‌ها همواره با احتمالات و چالش‌هایی نظیر هک، کلاهبرداری و تحریم مواجه است، ریسکی که ظاهرا برای فعالان این عرصه امری پذیرفته شده تلقی می‌شود.

## زباله‌های الکترونیکی

سال ۱۳۸۹ مصوبه‌ای قانونی تکلیف زباله‌های الکترونیکی را در کشور مشخص کرد با این وجود این مسوولیت همیشه پاسکاری شده است. پس از آن، هجدهم اسفندماه ۱۳۹۴ وزارت ارتباطات با سازمان محیط زیست یک تفاهم‌نامه در خصوص این زباله‌ها به امضا رساندند که البته همان‌طور که قابل پیش‌بینی بود این تفاهم‌نامه نیز تکلیف زباله‌های الکترونیکی در کشور را مشخص نکرد.

## بلاتکلیفی فرکانس‌های ۷۰۰ و ۸۰۰

سیزدهم فروردین‌ماه سال ۱۳۹۹ بود که محمدجواد آذری جهرمی وزیر وقت ارتباطات و فناوری اطلاعات در توییتر خود و در پاسخ به کاربری در خصوص کندی اینترنت نوشت: «مسوولیت می‌پذیریم ... موبایل را ارتقا دادیم اما ارتقا شبکه موبایل به باند فرکانسی نیاز دارد که فعلا در اختیار صداوسیماست و تا زمانی که فرکانس آزاد نشود، ظرفیت بالاتر نمی‌رود.» اواخر بهمن‌ماه سال ۹۷ نیز طرحی برای آزادسازی فرکانس‌های ۷۰۰ و ۸۰۰ مگاهرتز مطرح شد که کمیسیون تلفیق، مصوبه کمیسیون صنایع را در خصوص آزادسازی فرکانس‌های ۷۰۰ و ۸۰۰ که در اختیار سازمان صدا و سیما است، رد کرد.

## ۱۰ برابر کردن محتوای الکترونیکی

پروژه ۱۰ برابر کردن تولید محتوای داخلی با رویکرد کسب‌وکار دیجیتال در سال ۱۳۹۵ به تایید ستاد فرماندهی اقتصاد مقاومتی رسید. در این مقطع حدود ۴۰ میلیارد تومان به این پروژه اختصاص یافت و قرار شد با توسعه محتوا تاثیر قابل توجهی بر حوزه‌های علمی، پژوهشی و اقتصادی کشور گذاشته شود. آخرین خبر از این طرح اما این است که ظاهرا اجرای آن به‌طور کلی از اولویت‌های پروژه اقتصاد مقاومتی خارج شده است.

## ارز دیجیتالی داخلی

چهارم اسفند ۱۳۹۶ بود که وزیر ارتباطات در توییتی وعده ایجاد ارز دیجیتالی داخلی توسط پست‌بانک را مطرح کرد. جهرمی، هشتم اردیبهشت ماه سال ۱۳۹۷ این بار از آماده سازی مدل آزمایشی ارز دیجیتالی ایرانی خبر داد. با این وجود تا این لحظه همچنان خبری از سرنوشت، کارکرد و خروجی ارز دیجیتالی ملی نیست.

## لوایح پنج‌گانه حقوق فناوری اطلاعات

پنجم اسفند ماه ۱۳۹۶ پنج لایحه مرتبط با نظام حقوق فناوری اطلاعات و ارتباطات برای ارایه به هیات دولت رونمایی شد. حمایت از اطلاعات و حریم خصوصی افراد در فضای مجازی، مسوولیت ارایه‌دهندگان خدمات حوزه فناوری اطلاعات، شناسه‌های الکترونیکی، حکمرانی الکترونیکی و تراکنش‌های الکترونیکی از جمله این پنج لایحه بودند که قرار بود در مجلس مصوب و به قانون تبدیل شوند که البته همچنان خبری از سرنوشت آن نیست

## الزام دولتی‌ها به نصب پادویش

هجدهم بهمن ماه سال ۱۳۹۶ وزیر ارتباطات ابلاغ استفاده از آنتی‌ویروس پادویش در دستگاه‌های دولتی را به عنوان یک دستور حاکمیتی اعلام کرد. اگرچه از همان زمان تاکنون انتقادات متعددی به مخاطرات استفاده انحصاری از تنها یک آنتی‌ویروس مطرح شد لیکن همچنان گزارشی از میزان پیشرفت و اجرای این دستور حاکمیتی از سوی دستگاه‌های دولتی نیست.

## سند مراقبت از کودکان در فضای مجازی

دوم آبان ماه سال ۱۳۹۶ وزیر ارتباطات از رونمایی سند مراقبت از کودکان در فضای مجازی در روز ۱۳ آبان و همزمان با روز دانش آموز خبر داد. با این وجود تاکنون خبری در خصوص رونمایی این سند منتشر نشده است. تولید محتوای متناسب با کودک و نوجوان در این فضا نیز در این سند پیش‌بینی شده بود که از میزان پیشرفت آن اطلاعی در دست نیست.

## طرح تکاپو

از دی ماه سال ۱۳۹۳ با مصوبه شورای عالی اشتغال برای توسعه اشتغال مبنی بر «مزیت‌های استانی» با عنوان «توسعه کسب‌وکار و اشتغال پایدار» یا «تکاپو» در دستور کار قرار گرفت و آنگونه که مجریان طرح می‌گفتند بهمن ماه ۹۴ در کارگروه شورای برنامه‌ریزی استان تصویب و از سال ۹۵ وارد فاز اجرایی شد. با این وجود تاکنون نتیجه مشخصی از میزان اشتغال به وجود آمده از جمله ایجاد ۱۳۰ هزار شغل در بخش ICT نیست.

## برنامه دفاع سایبری

رییس مجلس شورای اسلامی در ۲۸ اسفند ماه ۱۳۹۵، قانون برنامه ششم توسعه کل کشور را که توسط شورای نگهبان تایید نهایی شده بود، به‌منظور اجرا به رییس جمهور ابلاغ کرد. در قانون برنامه ششم توسعه کشور، برنامه دفاع سایبری مناسبی برای افزایش چتر امنیت سایبری پیش‌بینی شده بود که البته تا این لحظه هیچ آماری از پیشرفت آن منتشر نشده است.

## طرح نسخه الکترونیکی

طرح نسخه الکترونیکی از زمان راه‌اندازی آن تا کنون مشکلات زیادی را برای مردم و بیماران به وجود آورده است. برخی مشکلات این طرح شامل متصل نبودن برخی پزشکان، مراکز درمانی، بیمارستان‌ها، داروخانه‌ها، بیمه‌های تکمیلی، عدم همسان‌سازی نرم‌افزار بیمه‌های مختلف و بلاتکلیفی طرح در زمان‌هایی نظیر قطع برق، اینترنت و سامانه است که منجر به محاسبه تعرفه‌های درمانی با نرخ آزاد برای مردم می‌شود و تاکنون شرکت‌های بیمه‌ای سود کلانی از اجرای ناقص این طرح برده‌اند.

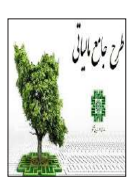
## لوایح قمار و شرط‌بندی

۲۳ تیر ماه ۱۳۹۷ یک عضو کمیسیون مصادیق مجرمانه اعلام کرد که وزارت ارتباطات، وزارت اقتصاد، بانک مرکزی و پلیس نیروی انتظامی با هماهنگی یکدیگر لوایحی را به منظور مبارزه با سایت‌های قمار و شرط‌بندی به دولت ارایه کرده‌اند و انتظار می‌رود در آینده‌ای نزدیک در صورت تصویب لوایح مذکور، تبدیل به قانون شوند. این لوایح نیز در زمره ناتمام‌های حوزه فاوا قرار دارند.

## تعطیلی جویشگرهای بومی

بیست و سوم مردادماه سال ۱۳۹۵ بود که دبیر کمیته راهبردی موتور جستجوهای بومی در وزارت ارتباطات گفت: اقدامات و برنامه ریزی برای حمایت از سه جویشگر بومی وجود دارد اما به دلیل محدودیت بودجه، این تعداد به دو جویشگر کاهش می یابد. به گفته وی دو جویشگر شامل یوز و پارسی جو در سال‌های اخیر راه‌اندازی شده‌اند و همکاری با سومین جویشگر که کاملا خصوصی است به زودی آغاز می‌شود. اما در سال ۱۴۰۰ این جویشگرها تعطیل و به فراموشی سپرده شدند و از آن زمان تاکنون پاسخی در خصوصی مسوولیت و چرایی این تعطیلی‌ها ارایه نشد.

## نظام جامع مالیاتی



حکم مربوط به اجرای طرح نظام جامع مالیاتی به ماده ۵۹ قانون برنامه سوم توسعه و تحت عنوان محدودتر طرح جامع مالیاتی باز می گردد. به همین منظور در سال ۱۳۸۳ اعلام شد که شرکت دیلویت کانادا برای برنامه‌ریزی و تدوین نقشه راه این طرح دعوت به همکاری شده و در برنامه اجرایی طرح جامع مالیاتی ۳۷ پروژه در پنج محور سازماندهی شده بود که این طرح هنوز به سرانجام کامل نرسیده است.

## خروج زیرساخت از مکالمات بین‌الملل

پنجم خردادماه سال ۱۳۹۷ مدیرعامل شرکت ارتباطات زیرساخت از کاهش نرخ مکالمات بین‌الملل از طریق دو صفر، در صورت آزادسازی ارایه این خدمات در کشور خبر داد. بر این اساس به جای آنکه شرکت زیرساخت به صورت مستقیم با اپراتورهای بین‌الملل قرارداد ببندد، قرار است اپراتورهای داخلی با طرف خارجی قرارداد بسته و شرکت زیرساخت تنها بحث تحویل ترافیک را عهده‌دار باشد.

## ایمن‌سازی علاءالدین

۲۸ اردیبهشت ماه سال ۱۳۹۷ معاون پیشگیری سازمان آتش‌نشانی و خدمات ایمنی تهران با اشاره به ضرورت ایمن‌سازی اماکن ناایمن پایتخت، گفت: از مسوولان ذی‌ربط می خواهیم که فشار بیشتری بیاورند تا ساختمان علاءالدین ایمن‌سازی‌اش نهایی شود. باوجود آنکه پایتخت تجربه حادثه تلخ پلاسکو را پشت سر گذاشته اما به نظر می‌رسد هشدارها درباره علاءالدین جدی گرفته نشده و این موضوع نیز همچنان بلاتکلیف بماند.

# ۳ درس آموخته از رویکرد چین به هوش مصنوعی

سعید میرشاهی

هوش مصنوعی در همه‌جا وجود دارد و آماده است تا نحوه کار و بازی ما، چگونگی یادگیری و مراقبت از ما را تغییر دهد. هوش مصنوعی از مهمانداری، بهداشت و درمان تا سرگرمی و آموزش، در حال دگرگونی دنیای ماست.

به گزارش Theconversation، این تکنولوژی در نقاط مختلف جهان با سرعت‌های متفاوت در حال توسعه است.

به نظر می‌رسد در غرب، تمایل به رسیدن به کمال وجود دارد؛ به‌گونه‌ای که شرکت‌ها، قبل از اینکه سیستم هوش مصنوعی را پیاده‌سازی کنند، وقت خود را صرف بهبودی آن می‌کنند اما چین مسیری عملی را اتخاذ کرده که در آن سرعت و انطباق، بر اجرای بی‌نقص اولویت دارد.

ظاهرا شرکت‌های چینی، بیشتر مایل به پذیرش ریسک‌ها، قبول محدودیت‌های فعلی هوش مصنوعی و مشاهده نتایج آن هستند از این رو به نظر می‌رسد تمایل چین برای تبدیل شدن به پیشتاز جهانی در توسعه هوش مصنوعی، بیشتر است. در ادامه، سه درس مهم که غرب، می‌تواند از استراتژی اقتصادی چین در زمینه هوش مصنوعی بیاموزد، ارائه شده است.

**۱. نواقص را بپذیرید**

بسیاری از شرکت‌های چینی به ذهنیت «کافی است»، در قبال هوش مصنوعی روی آورده‌اند و از آن استفاده می‌کنند؛ حتی زمانی که این تکنولوژی کاملا توسعه نیافته است. هرچند این موضوع، خطراتی به همراه دارد اما یادگیری سریع را تشویق می‌کند.

برای مثال، در سال ۲۰۱۶، «هایدی‌لاو» (Haidilao)، یک رستوران زنجیره‌ای محبوب چینی، سیستم هوش مصنوعی «شیائومِی» را معرفی کرد که به مشتریان در زمینه تماس برای رزرو کمک می‌کرد.

در حالی که شیائومِی، پیچیده‌ترین سیستم هوش مصنوعی نیست (و فقط سوالات مربوط به رزرو را درک می‌کند) اما موثر است و روزانه بیش از ۵۰ هزار تعامل با مشتری را با دقت ۹۰ درصد مدیریت می‌کند. این سیستم، بی‌نقص نیست اما خدمات ارزشمندی به کسب‌وکارها ارائه می‌دهد و ثابت می‌کند هوش مصنوعی برای اثرگذاری وسیع، نیاز به بی‌نقص بودن ندارد.

**۲. عمل‌گرایی را در اولویت قرار دهید**

تفاوت کلیدی بین استراتژی‌های هوش مصنوعی در چین و غرب، تمرکز بر کاربردهای عملی و حل مسئله است.

در بسیاری از صنایع غربی، هوش مصنوعی اغلب با فناوری‌های پیشرفته مانند جراحی با کمک ربات یا الگوریتم‌های پیچیده پیش‌بینی، مرتبط است. هرچند این پیشرفت‌ها هیجان‌انگیز هستند اما همیشه تاثیر فوری ندارند. در مقابل، چین با به‌کارگیری هوش مصنوعی برای حل نیازهای اساسی‌تر، گام‌های قابل توجهی برداشته است.

در چین، برخی بیمارستان‌ها از هوش مصنوعی برای کمک به کارهای روتین اما بسیار مهم، استفاده می‌کنند. به عنوان مثال، در آوریل ۲۰۲۴، بیمارستان اتحادیه ووهان یک سرویس هوش مصنوعی برای بیماران معرفی کرد که به نوعی نقش پرستار تریاژ را برای بیماران از طریق یک اپلیکیشن پیام‌رسان ایفا می‌کرد.

با این سرویس، از بیماران درباره علائم و تاریخچه پزشکی آنها سوال می‌شود. سپس هوش مصنوعی، شدت نیازهای آنها را ارزیابی کرده و نوبت‌ها را بر اساس فوریت و منابع پزشکی موجود در آن زمان اولویت‌بندی می‌کند. سپس نتایج به یک پزشک انسانی منتقل می‌شود که تصمیم نهایی را درباره مراحل بعدی می‌گیرد.

این سیستم با کمک به اطمینان‌بخشی به افرادی که به خدمات بحرانی‌تری نیاز دارند، ابتدا دیده می‌شوند، نقش مهمی در بهبود کارآیی و کاهش زمان انتظار بیماران برای مراقبت پزشکی ایفا می‌کند. این فناوری،

پیچیده‌ترین نیست اما طبق گزارش‌ها، در ماه اول، استفاده از آن در کلینیک پستان بیمارستان، برای بیش از ۳۰۰ بیمار، زمان مشاوره اضافی فراهم کرده است. نکته قابل توجه اینکه ۷۰ درصد از این بیماران، نیاز فوری به جراحی داشتند.

**۳. از اشتباهات بیاموزید**

پذیرش سریع هوش مصنوعی در چین، بدون چالش نبوده اما شکست‌ها به عنوان تجربیات یادگیری حیاتی عمل می‌کنند.

یکی از داستان‌های هشداردهنده برای پیاده‌سازی هوش مصنوعی به چین تعلق ندارد، بلکه به ژاپن مربوط می‌شود. وقتی هتل هِن‌نا (Henn na Hotel) در ناگازاکی، به عنوان اولین هتل دنیا با کارمندان رباتی معرفی شد، توجه زیادی به مفهوم آینده‌نگرانه جلب کرد اما به زودی از انتظارات کوتاه آمد.

«چوری»، ربات دستیار اتاق هتل، اغلب درخواست‌های مهمانان را به اشتباه درک می‌کرد و این موضوع، باعث سردرگمی می‌شد. گزارش شده یکی از مهمانان، بارها به دلیل اینکه ربات اتاقش، صدای خروپف او را به عنوان سوال اشتباه، درک کرده بود، بیدار شده است!

در مقابل، بسیاری از هتل‌های چینی رویکرد متعادل‌تری اتخاذ کرده و به راه‌حل‌های رباتیکی ساده‌تر اما بسیار موثرتر روی آورده‌اند.

ربات‌های تحویل غذا، اکنون در زنجیره‌های هتل کشور رایج هستند. آنها در حالی که پیچیدگی زیادی ندارند اما با حرکت خودکار در راهروها و آسانسورها مهارت دارند و غذاها را به مهمانان می‌رسانند. شرکت‌های چینی با تمرکز بر مشکلات خاص و تاثیرگذاری بالا، به طور موفقیت‌آمیزی، هوش مصنوعی را طوری ادغام کرده‌اند که اختلالات را به حداقل و سودمندی را به حداکثر می‌رساند.

زنجیره رستوران چینی که قبلا به آن اشاره شد، نمونه دیگری از این رویکرد است. پس از موفقیت چت‌بات، هایدی‌لاو رستوران‌های هوشمندی را معرفی کرد که با بازوهای رباتیک و سیستم‌های تحویل غذا به طور خودکار تجهیز شده بودند.

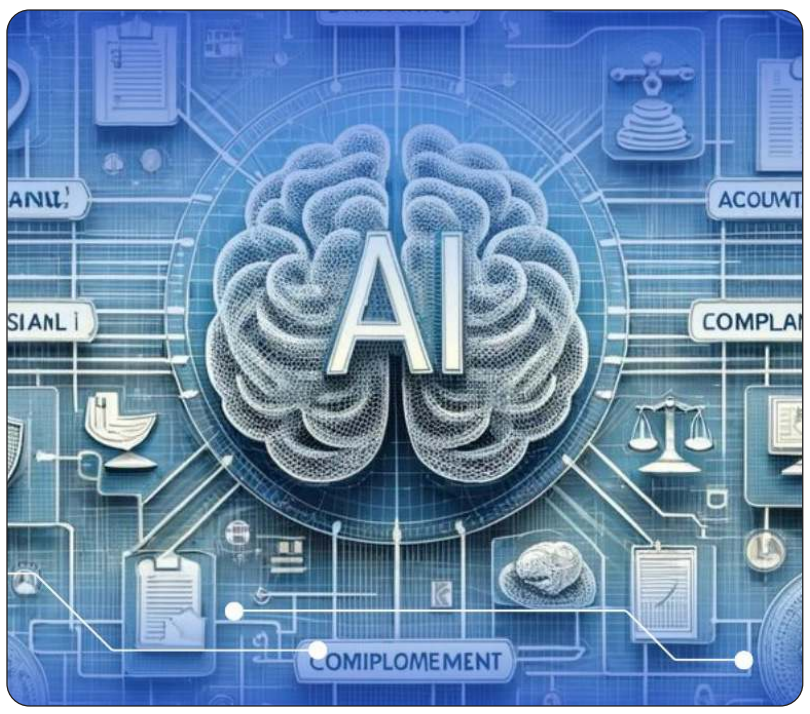
با وجود نوآورانه بودن، این فناوری، در ساعات اوج با مشکلاتی مواجه شد و از نظر شخصی‌سازی که بسیاری از مشتریان برای آن ارزش قائل بودند، کاستی داشت. با این حال، هایدی‌لاو به جای اینکه پروژه را رها کند، به تنظیم و بهبود استفاده از هوش مصنوعی ادامه داد. این رستوران زنجیره‌ای به جای اینکه مدل کاملا خودکار رستوران را اتخاذ کند، رویکرد هیبریدی را انتخاب و اتوماسیون را با کارکنان انسانی ترکیب کرد تا تجربه غذا خوردن را ارتقا دهد.

این انعطاف‌پذیری در مواجهه با شکست‌ها، بیانگر تمایل اساسی به تغییر مسیر و انطباق در مواقعی است که امور، طبق برنامه پیش نمی‌رود. به طور کلی، رویکرد عملی چین به هوش مصنوعی، به این کشور اجازه داده در بسیاری زمینه‌ها پیشتاز باشد؛ حتی در حالی که از نظر پیچیدگی فناورانه، از غرب عقب‌تر است. این موضوع، ناشی از تمایل به پذیرش نواقص هوش مصنوعی و سپس انطباق در صورت لزوم است.

آنجا که سرعت و انطباق، حیاتی است، شرکت‌ها نمی‌توانند منتظر راه‌حل‌های کامل بمانند. با پذیرش نواقص هوش مصنوعی، تمرکز بر کاربردهای عملی و بازخورد دنیای واقعی، شرکت‌های چینی، ارزش اقتصادی هوش مصنوعی را به روشی پیش برده‌اند که دیگران به خاطر ترس، شجاعت لازم برای تقلید از آن را ندارند.

# هوش مصنوعی چگونه عملکرد دولت‌ها را بهتر می‌کند؟

آسیه فروردین




هوش مصنوعی (AI) در حال دگرگون ساختن عملکرد صنایع است و بهره‌وری، دقت و ارائه خدمات را بهبود می‌بخشد.

سایت thinkdigitalpartners در گزارشی نوشت: با توجه به اینکه ادغام هوش مصنوعی با فعالیت‌ها، دیگر یک انتخاب نیست و به یک ضرورت تبدیل شده، سازمان‌های خصوصی و دولتی، هردو، به دنبال راه‌هایی برای ادغام هوش مصنوعی در چارچوب‌های عملیاتی خود هستند.

دولت‌ها نیز به طور فزاینده‌ای هوش مصنوعی را در فرایندهای خود ادغام می‌کنند. در این مطلب، دومینیک بیرگلن، مدیرعامل Oneclick Group AG، توضیح می‌دهد دولت چگونه می‌تواند به طور موثر، هوش مصنوعی را مهار کند.

بر اساس آخرین آمار استاتیستا، بریتانیا در بین چهار کشور برتر از نظر آمادگی دولت برای استفاده از هوش مصنوعی قرار دارد. این امر، بیانگر توانایی دولت در استفاده از فناوری برای اتخاذ تصمیمات مبتنی بر داده و بهبود خدمات عمومی است.

هوش مصنوعی، پتانسیل زیادی برای بهبود فرایندهای تصمیم‌گیری در دولت‌ها دارد و با تحلیل سریع حجم عظیم داده‌ها، می‌تواند الگوها و روندهایی را شناسایی کند که به سیاست‌گذاری و تخصیص منابع کمک کند.

تحلیل‌های پیش‌بینی‌کننده نیز به دولت‌ها امکان می‌دهد مسائل احتمالی را برآورد کنند و برای آنها برنامه‌ریزی پیشگیرانه داشته باشند. این امر به مدیریت آگاهانه‌تر و استراتژیک‌تر منجر می‌شود.

با این حال، هرچند امکانات هوش مصنوعی گسترده است اما ادغام آن نیز با چالش‌های احتمالی مواجه است. در این زمینه، چالش‌هایی مانند عدم شفافیت، جابجایی نیروی کار و خطرات امنیت سایبری، باید مورد توجه قرار گیرند تا بتوان از مزایای هوش مصنوعی در بخش خدمات عمومی به طور کامل بهره‌مند شد. با پیشرفت مستمر فناوری هوش مصنوعی، اتخاذ رویکرد متعادل و اخلاقی در به‌کارگیری آن برای اثربخشی بلندمدت در حمایت از عملیات و فعالیت‌های اجرایی دولت، حیاتی است.

**● مزایای هوش مصنوعی برای فعالیت‌های اجرایی دولتی**

ادغام هوش مصنوعی، مزایای زیادی در حوزه عملیات و فعالیت‌های اجرایی دولتی دارد. خودکارسازی وظایف روتین و زمان‌بر، یک مزیت کلیدی است.

هوش مصنوعی با خودکارسازی، اقدامات تکراری مانند ورود داده‌ها، مدیریت اسناد و برنامه‌ریزی، این امکان را برای کارمندان دولتی فراهم می‌کند که تمرکزشان را از وظایف روزمره به عملیات و فرایندهای استراتژیک‌تر و تاثیرگذارتر معطوف کنند. خودکارسازی از طریق هوش مصنوعی، احتمال خطای انسانی را در وظایف روتین کاهش داده و منجر به دقت و انسجام بیشتر عملکرد دولت می‌شود. این امر، نه تنها بهره‌وری را بهبود می‌بخشد، بلکه اثربخشی کلی خدمات عمومی را ارتقا می‌دهد.

قابلیت هوش مصنوعی در تجزیه و تحلیل سریع و دقیق حجم عظیم داده‌ها نیز به عنوان یک ابزار کلیدی برای تصمیم‌گیرندگان دولتی عمل می‌کند. فرایندهای تصمیم‌گیری سنتی، اغلب بر مجموعه داده‌های محدود تکیه دارند و در معرض سوگیری انسانی هستند.

با این حال، هوش مصنوعی می‌تواند به طور موثر، مجموعه‌های بزرگ داده را پردازش و تحلیل کرده و الگوها و روندهایی را شناسایی کنند که بینش‌های حیاتی برای شکل‌دهی به تصمیمات و استراتژی‌های دولتی ارائه می‌دهد. از این طریق، دولت‌ها می‌توانند تصمیمات آگاهانه‌تر و استراتژیک‌تری در زمینه تخصیص منابع، بهداشت عمومی و برنامه‌ریزی شهری اتخاذ کنند.

**● موانع احتمالی موثر بر اجرای هوش مصنوعی**

هرچند مزایای ادغام هوش مصنوعی در عملیات اجرایی دولت قابل توجه است اما چالش‌های ویژه‌ای نیز وجود دارند که برای بهره‌برداری حداکثری از پتانسیل آن باید مدنظر قرار گیرند.

با ورود هوش مصنوعی به اقدامات روتین و تکراری، یکی از نگرانی‌های نوظهور، خطر بیکار شدن برخی مشاغل است که می‌تواند به بیکاری و ناآرامی‌های اجتماعی منجر شود. این مسئله از فاصله اعتماد به هوش مصنوعی بین نیروی کار و فناوری ناشی می‌شود که مانع بالقوه برای ادغام هوش مصنوعی در فعالیت‌های دولتی محسوب می‌شود.

از این‌رو دولت‌ها باید بین بهره‌وری حاصل از هوش مصنوعی، استراتژی‌های بازآموزی و ارتقای مهارت نیروی کار تعادل برقرار کنند تا اطمینان یابند مزایای هوش مصنوعی به طور عادلانه توزیع می‌شود.

امنیت سایبری نیز یک حوزه کلیدی و حیاتی است. در این رابطه، سیستم‌های دولتی، اطلاعات حساس مانند اطلاعات شخصی شهروندان، جزییات زیرساخت‌های حیاتی و اطلاعات امنیت ملی را پردازش می‌کنند.

این موارد، سیستم‌های دولتی را به اهداف جذاب برای مجرمان سایبری تبدیل می‌کند. نفوذ به این سیستم‌ها می‌تواند عواقب شدیدی داشته باشد و نه تنها امنیت اطلاعات حساس را به خطر اندازد، بلکه اعتماد عمومی به عملکرد دولت را نیز تضعیف می‌کند.

بنابراین اطمینان از وجود تدابیر قوی امنیت سایبری و حفظ یکپارچگی سیستم‌های هوش مصنوعی در درازمدت، بسیار مهم است.

بکارگیری هوش مصنوعی باید با اجرای تدابیر پیشرفته امنیت سایبری، مانند «معماری اعتماد صفر» (ZTA) همراه باشد تا وضعیت، تقویت شود. این امر به دولت‌ها امکان می‌دهد به طور ایمن، از هوش مصنوعی برای بهبود کارکردهای عمومی بهره ببرند.

**● بهترین روش‌ها برای بهره‌گیری موثر از هوش مصنوعی**

برای بهره‌برداری کامل از پتانسیل هوش مصنوعی و کاهش خطرات آن، دولت‌ها باید یک رویکرد متعادل، ساختارمند و اخلاقی به منظور استقرار و استفاده از هوش مصنوعی اتخاذ کنند. یکی از جنبه‌های حیاتی این رویکرد، اطمینان از امنیت و کیفیت داده‌هاست. برای دستیابی به عملکرد بهینه هوش مصنوعی، دولت‌ها باید دقیق بودن، کامل بودن و امنیت داده‌ها را در اولویت قرار دهند.

سازمان‌ها نیز باید پروتکل‌های رمزگذاری سرتاسری را برای ایمن‌سازی داده‌های حساس پیاده‌سازی کنند و به طور منظم به‌روزرسانی نرم‌افزارها و مدیریت وصله‌های امنیتی را انجام دهند تا شکاف‌های امنیتی احتمالی رفع شده و از سوءاستفاده‌ها جلوگیری شود.

همچنین دولت‌ها باید ممیزی‌های جامع امنیتی مانند تست نفوذ و ارزیابی آسیب‌پذیری‌ها را انجام دهند تا این موارد، شناسایی و برطرف شوند. نظارت مداوم از طریق سیستم‌های شناسایی تهدیدات در لحظه، مانند تشخیص ناهنجاری‌های مبتنی بر هوش مصنوعی، برای سازمان‌های دولتی حیاتی است تا خطرات امنیت سایبری را به حداقل برسانند، یکپارچگی عملیاتی را تضمین، از اطلاعات عمومی محافظت و اعتماد عمومی را تقویت کنند.

دولت‌ها همچنین باید در زمینه توسعه نیروی کار سرمایه‌گذاری کنند تا نگرانی‌های احتمالی ناشی از هوش مصنوعی را برطرف کنند. در این زمینه، ابتکارات یادگیری سازمانی، ابزار مهمی هستند که مهارت‌ها و قابلیت‌ها را تحلیل کرده و مسیرهای یادگیری سفارشی برای هر فرد طراحی می‌کنند.

این برنامه‌های جامع آموزشی و یادگیری که مبتنی بر هوش مصنوعی هستند، می‌توانند به سازمان‌های دولتی کمک کنند تا کارکنان را با مهارت‌های لازم برای موفقیت در اقتصاد مبتنی بر هوش مصنوعی مجهز کنند.

ارتقای مهارت کارکنان، نه تنها آنها را برای چشم‌انداز در حال تغییر دولت آماده می‌کند، بلکه اطمینان می‌دهد که مزایای هوش مصنوعی به طور گسترده تقسیم شود. از این طریق، نهادهای دولتی می‌توانند یک نیروی کار آماده را برای آینده توسعه دهند که قادر به بهره‌گیری از مزایای هوش مصنوعی است و در عین حال، چالش‌های آن را به حداقل می‌رساند.

با ادامه تکامل هوش مصنوعی، کاربردها و ضرورت آن در فعالیت‌ها و عملکرد دولت افزایش خواهد یافت.

و در نهایت اینکه با پذیرش هوش مصنوعی و ادغام آن در چارچوب‌های استراتژیک، دولت‌ها می‌توانند به طور قابل توجهی، بهره‌وری و ارائه خدمات عمومی را بهبود بخشند و در نهایت، بخش عمومی پاسخگوتر و مقاوم‌تر ایجاد کنند.

### با سفر وزیر ارتباطات به کوبا و ونزوئلا انجام شد

# گام نخست دیپلماسی فناوری در دولت چهاردهم

دانیال رمضانی

شـرایط دنیا در عرصه دیجیتال از سـال ۲۰۰۳ که کشورها و نهادهای بین‌المللی را به تحرکات جدیدی وادار کرد و نخستین بار در اجلاس جهانی سران درباره جامعه اطلاعاتی (WSIS) در ژنو سـوییس ظهور و بروز یافت، به مراتب با تغییرات شگرف و بی‌سابقه‌ای مواجه شده است. در آن مقطع اجلاس WSIS شامل دستورِ کارها و محورهای متعددی بود که در راس آن، سران کَشورها و دیپلمات‌ها به دنبال تعیین یک مرجع و متولی روشن در «راهبری جهانی اینترنت» بودند.

اما از آن زمان تا کنون شتاب تحولات عرصه فناوری به حدی سریع، گسترده و روزافزون شده که مقامات و نظام دیپلماسی کشورها، تدابیر ویژه‌ای برای تامین اهداف و منافع ملی خـود در نهادهـا و پیمان‌های منطقه‌ای و بین‌المللی از طریق دیپلماسـی فناوری به‌کار بسته‌اند.

**● تشدید جنگ‌های فناورانه در دنیا**

دنیا سال‌هاسـت که با جنگ فناوری در عرصه‌های متعدد مواجه است که خسارات سنگین جهانی به بار آورده است. به طور مشخص و در یک نمونه برجسته، آمریکا در سال‌های اخیر نبردی فرسایشی و طولانی با چین را کلید زده است که در اشکال مختلف به ایجاد هزینه‌های متعدد برای کشورها، شرکت‌ها و کاربران زیادی منجر شده که کماکان نیز ادامه دارد.

تحریم تراشه‌ای، تحریم تجهیزات نسل ۵ موبایل، انواع تحریم‌های اینترنتی و در آخرین نمونه تحریم هوش مصنوعی چین از سوی آمریکا از محورهای کلان این نبرد فناورانه محسوب می‌شـود که مقامات دولتی و شرکت‌های خصوصی چین را به تحرکات گسترده در عرصه دیپلماسی فناوری وارد کرده است.

مصادیق فوق با وجـود اثرات گسـترده جهانی، اما همچنـان بخش کوچکـی از الزامات شـکل‌گیری دیپلماسی فناوری در دنیا به شمار می‌رود.

به همین دلیل است که در دولت چهاردهم، دیپلماسی فناوری یک محور کلیدی شناخته شده است و سید سـتار هاشـمی وزیر ارتباطات و فناوری اطلاعات با آگاهی از درهم‌تنیدگی و گسست‌ناپذیری تعاملات بین‌المللی در عرصه فناوری، در مقاله‌ای پیش از سفر به کوبا و ونزوئلا نوشت: امروز دیپلماسی دیجیتال در روابط بین‌الملل امری حیاتی شـده است و سه حوزه کلان شامل:

- تحولات دیجیتال و توزیع مجـدد قدرت در روابط بین‌الملل،
- ظهور انواع جدید چالش‌ها و درگیری‌ها و
- حکمرانی دیجیتـال، به عنوان عوامل پیشـران و شـکل‌دهنده به دیپلماسـی فعال فناوری شناخته می‌شوند.

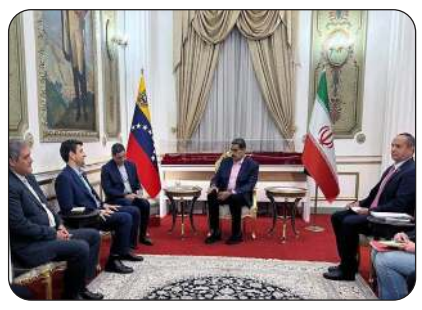
در سـال‌های اخیـر ظهـور موضوعات سیاسـی، امنیتی، اقتصادی و اجتماعـی جدید در عرصه‌های دیپلماسـی فناوری، بیش از ۵۰ موضوع و چالش در روابط بین‌الملل و حکمرانی دیجیتال از جمله امنیت سـایبری، حریم خصوصی، حاکمیت داده، تجارت الکترونیک، جرایم سایبری، حکمرانی هوش مصنوعی و ... را شامل می‌شود.

لذا گسترش فضای جهان‌شمول سایبری، امروز دنیا را با انبوهی از مسایل سیاسی، فناورانه و دیپلماتیک کرده که:

- چالش‌های حکمرانی سایبری
- مداخلات برخی دولت‌ها در امور اقتصادی، اجتماعی، فرهنگی و امنیتی دیگر کشورها از طریق تولید گسترده اطلاعات نادرست، تئوری‌های توطئه، رادیکال‌سازی آنلاین و انتشـار اخبار جعلی در بسـتر شبکه‌های اجتماعی و پیام‌رسـان‌ها گرفته تا حملات هکری و ایجاد سلاح‌های سایبری همچون استاکس‌نت و ...
- ظهور پدیده ارایه‌دهنـدگان فرامرزی و ماهواره‌ای اینترنت از شرق تا غرب عالم
- رفع تداخلات فرکانسی و تعیین برخی استانداردهای جدید بین‌المللی در عرصه ارتباطات
- گسـترش شـتابان هوش مصنوعی و چالش‌های جهانی آن
- افزایش فروشـندگان و ارایه‌کننـدگان خدمات و محصولات از خارج از مرزهای مرسوم کشورها بر بستر فضای مجازی
- حمایت از رشد و توسـعه بین‌المللی شرکت‌های خصوصی عرصه دیجیتال
- افزایش مستمر انواع رمزارزها و رمزدارایی‌ها
- ظهور جهان پلتفرم‌ها و تداخل رویکردهای آنها با مسـایل حکمرانی درون مرزی کشورها و همچنین دیگر فناوری‌های در حال پیدایش و جهان‌شمول از جمله دلایل شکل‌گیری، فشـردگی و حساسیت در کار دیپلمات‌ها و دیپلماسی فناوری در دنیا به شمار می‌رود.

**● ایران و الزامات دیپلماسی فناوری**

لیکن علاوه بر مسـایل و معضلات فوق که منجر به تحرک دیپلماسـی فناوری در دنیا شده است، ایران دارای شرایط خاص و متفاوتی است. به همین جهت موضوع الزامات «دیپلماسی فناوری» اما تنها محدود به منافع درون مرزهای سـایبری و سنتی کشورها نمی‌شـود و عدم همکاری‌های بین‌المللی در دنیا به رشد ناتوازن، چالش‌ها، هزینه‌ها و شکاف‌های دیجیتال در دنیا منجر می‌شود.



در سـال‌های اخیر جمهوری اسلامی ایران، از طریق نهادهای بین‌المللی همچون ITU و سـازمان ملل، پیمان‌های منطقه‌ای همچون شـانگهای، بریکس و تعاملات دو جانبه با کشـورهای مختلف همچون چین، روسیه، کوبا، ونزوئلا و ... پیگیر هم‌افزایی با هدف بسترسازی جمعی برای زدودن کارشکنی‌ها و اقدامات غیرقانونی و کارشکنی‌های برخاسته از اهداف سیاسی و تنگ‌تر کردن عرصه مانور فعالان سـایبری است تا فضای مجازی امن‌تری برای همه شهروندان و کسب و کارها فراهم شود.

به همین جهت همزمان با آغاز بکار دولت چهاردهم، وزارت ارتباطات و فنـاوری اطلاعات به عنوان محور اصلی «دیپلماسی فناوری»، این موضوع راهبردی را از نخستین روزهای انتصاب سیدستار هاشمی در دستور کار قرار داده است.

**۱- ایران هراسی سایبری**

رسـانه‌ها، شـرکت‌های خصوصـی، مقامـات و دیپلمات‌های غربی و ضد ایرانی، سال‌هاسـت که در برنامه‌ای هدفمند پروژه «ایران‌هراسـی سایبری» را با شـدت و قدرت دنبال می‌کنند. اگرچه جمهوری اسـلامی ایران که خود یکی از بزرگتریـن قربانیان حملات سـایبری آمریـکا و متحدان آن به شـمار می‌رود، بارها اتهامات وارده را رد کرده و خواستار ارایه مستندات فنی و قانونی در این خصوص شده که عمدتا از سوی آمریکا و متحدانش بی‌پاسخ مانده است.

این در حالیست که در روالی بر خلاف پروژه مذکور، حملات سایبری آمریکا و اسراییل به دیگر کشورها به شکل روزانه و پرتعداد در حال وقوع است. اما این مساله در سانه‌های مادر و غالب جهانی چندان برجسته‌سازی نمی‌شود. کما اینکه در همین رابطه اخیرا بی‌بی‌سی بین‌الملل در گزارشی به چرایی عدم انتشار گسترده اخبار از حملات سـایبری آمریکا و غربی‌ها به دیگر کشورها در رسـانه‌های غربی پرداخته بود و علت آن را وابستگی‌های کاری، قراردادی و مالی شرکت‌های امنیت سـایبری و فناوری به دولت‌های غربی عنوان کرده بود.

**۲- حملات هدفمند و گسترده سایبری به ایران**

همانطور که ذکر شـد ایـران یکـی از اصلی‌ترین قربانیان حملات سـایبری در دنیا محسوب می‌شود و سال‌هاست که با مداخلات و حملات آشکار و علنی سـایبری دولت‌های متخاصم از طریق انواع حملات به زیرساخت‌ها، سـامانه‌ها و عرضه گسـترده انواع باج‌افزارها، بدافزارها و ویروس‌هـای رایانه‌ای مواجه است.

ویروس استاکس‌نت که رسانه‌های غربی از آن به عنوان نخستین، گران‌ترین و پیچیده‌ترین «سلاح سایبری» دنیا نام می‌برند و بر اساس گزارش‌ها و افشاگری‌های انجام شده توسط آمریکا و رژیم صهیونیستی ساخته و طراحی شد، نخستین بار برای حمله به زیرساخت‌های هسته‌ای ایران بکار گرفته شد.

**۳- انواع تحریم‌های فناورانه**

فارغ از چالش‌های جهانی و دو مساله انحصاری فوق، ایران سال‌هاست که با انواع تحریم‌ها برای ایجاد کندی در پیشرفت‌های فناورانه نیز مواجه است.

تحریم‌های فناوری که عمدتا از سوی آمریکا و اتحادیه اروپا به ایران تحمیل شـده نیز در سه سطح در حال اجراست.

- تحریم‌ها در سطح کاربران ایرانی که شامل انبوهی از ممنوعیت‌های در دسترسـی به پلتفورم‌ها و انواع ابزارهای پیشرفته نرم‌افزاری، سخت‌افزاری، خدماتی و امنیتی است.
- تحریم‌ها در سـطح کسـب‌وکارها و شرکت‌های ایرانی که شـامل ممنوعیـت کار، ممنوعیت فروش انواع تجهیزات نرم‌افزاری، سـخت‌افزاری و امنیتی، ممنوعیت انتقال دانش و فناوری و بسـیاری از دیگر موارد را شامل می‌شود.
- تحریم‌ها در سـطح نهادهای حاکمیتی، دولتی و عمومی نیز اشکال و گستره به مراتب بیشتر از دو بخش فوق را شامل می‌شود.

مجموع آنچه که ذکر شـد، لزوم تحـرک مضاعف و بیشـتر در عرصه دیپلماسـی فناوری برای ایران را ایجاب می‌کند که تحقق این امر نیز نیازمند همکاری نهادهای متعدد است که در راس آنها وزارت ارتباطات و فناوری اطلاعات و وزارت امور خارجه می‌توانند نقش

راهبری در مراجع بین‌المللی، پیمان‌های منطقه‌ای و هماهنگی با دیگر دستگاه‌ها را در احقاق حقوق ملی، کمک به رشد و توسعه فناوری در داخل و خارج کشور ایفا کنند.

**● گام نخست دیپلماسی فناوری**

در همین راستا ستار هاشمی وزیر ارتباطات و فناوری اطلاعات هفته قبل در راس هیاتی، گام نخست تقویت دیپلماسی سایبری را در سـفر به دو کشور ونزوئلا و کوبا کلید زد.

**سطح عالی دیدارها**

اگرچه در سال‌های قبل نیز دیدارها و رایزنی‌هایی میان مقامات کشورهای ایران، کوبا و ونزوئلا در حوزه‌های فناوری انجام شده بود، اما نخستین نقطه برجسته و متفاوت در سفر ستار هاشمی وزیر ارتباطات و هیات همراه، ارتقای قابل ملاحظه سطح دیدارها بود.

در این سـفرها علاوه بر مقامات عالی و همتایان دو کشور، وزیر ارتباطات ایران با روسای جمهوری کوبا و ونزوئلا نیز دیدار کرد و مورد اسـتقبال ویژه‌ای قرار گرفت.

**دیدار با رییس جمهور کوبا**

سیدستار هاشمی، وزیر ارتباطات و فناوری اطلاعات در آخرین روز حضور در کوبا بـا «میگوئل دیاز کانل برمودز»، رئیس جمهوری این کشـور دیـدار و در خصوص راه‌های توسـعه همکاری‌هـای گوناگون دوجانبه بویژه در حوزه ارتباطات و فناوری اطلاعات گفت و گو کرد.

هاشـمی در این دیدار که پس از آیین آغـاز به کار چهلمیـن نمایشـگاه بین‌المللی هاوانـا و بازدید از غرفه‌های جمهوری اسلامی در این نمایشگاه برگزار شـد، پس از ابلاغ پیام گرم رییس جمهوری اسلامی ایران به رییس جمهور کوبـا تصریح کرد: در اینجا به دنبال آن هستیم تا همکاری‌های سیاسی را به ابعاد اقتصادی و فنی گسترش دهیم.

میگوئل دیاز کانل برمودز، رییس جمهوری کوبا نیز در این دیدار به روابط دوستانه و تاریخی دو کشور اشاره کرد و گفت: میان ایران و کوبا یک دشمن مشترک به نام امپریالیزم آمریکا وجود دارد که تحت تحریم و فشار از سوی آن دشمن هستیم اما دو دولت خیلی محکم ایستاده‌اند و در حال مقاومت هستند.

کانل برمودز با اشـاره به بازدیدی که از نمایشـگاه بین‌المللی فناوری کوبا داشـت، خاطرنشان کرد: در بازدیدی که از غرفه شرکت‌های ایرانی در نمایشگاه بین‌المللـی هاوانا داشـتم نماینده‌هـای خوبی از شـرکت‌های ایرانی حضور و اراده زیادی در آنها برای همکاری با کوبا داشتند.

وی افزود: با نمایندگانی از این شرکت‌ها دیدار کردم و از آنها خواستیم که نمایندگی‌هایی را در کوبا تاسیس کنند. رییس جمهـوری کوبا با اظهار امیـدواری از امکان گسـترش همکاری‌های دو کشـور در حوزه ارتباطات و فناوری اطلاعات ابراز کرد که شرکت‌های دو کشور بتوانند در جهت منافع دو کشور به تقویت این همکاری‌ها کمک کنند.

رییس جمهور کوبا همچنین در شبکه اجتماعی ایکس نیز با انتشار تصویر مشترکش با وزیر ارتباطات ایران نوشـت: «از حضور با ارزش دکتر سید ستار هاشمی وزیر ارتباطات و فناوری اطلاعات جمهوری اسلامی ایران در کوبا و رویداد مهم نمایشگاه بین‌المللی هاوانا ۲۰۲۴ سپاسگزاری می کنم.»

**دیدار با رییس جمهور ونزوئلا**

ستار هاشمی، وزیر ارتباطات و فناوری اطلاعات ایران همچنین با «نیکلاس مادورو»، رئیس جمهوری ونزوئلا نیز دیدار و درباره زمینه‌های توسعه روابط دوجانبه در عرصه‌های گوناگون بویژه حـوزه ارتباطات و تامین تجهیزات مخابراتی برای این کشور گفت و گو کرد.

**امضای دو سند مخابراتی میان تهران و کاراکاس**

اما وزیر ارتباطات و فناوری اطلاعات در نخستین روز سفر به کاراکاس با چهار تن از وزیران برق، ارتباطات، علوم و حمل و نقل این کشـور دیدار و ضمن بررسی زمینه‌های همکاری چند قرارداد و سند همکاری در حوزه ارتباطات و فناوری اطلاعات را به امضا رساند.

در دیدار وزیر ارتباطات کشورمان با «خورخه مارکز» وزیر برق و رییس شـرکت ملی مخابرات این کشور (Conatel)، اسناد قراردادهای همکاری ارتباطاتی، فناورانه و مخابراتی میان تهـران و کاراکاس به امضا رسید. هاشمی در این دیدار با اشاره به دیدار روسای جمهوری ایـران و ونزوئلا در حاشـیه اجلاس اخیر بریکس، تاکید کرد که سیاسـت دولـت چهاردهم، حمایت از بخش خصوصی و ارتقـای همکاری‌های مشترک میان دو کشور ایران و ونزوئلا است.

خورخه مارکز، وزیر برق و رییس شرکت ملی مخابرات ونزوئلا نیز با تقدیـم پیام خیرمقدم رییس جمهوری ونزوئلا به ستار هاشـمی و هیات همراه، بر پیشبرد توافقات انجام شده همچون گذشته تاکید کرد.

در پایان اسناد و قراردادهای همکاری‌های ارتباطاتی و مخابراتی شامل تامین قطعات و تجهیزات مخابراتی و همچنین تولید کابل فیبرنوری میان دو طرف امضا شد.

**راه‌اندازی پلتفرم مشترک**

وزیر ارتباطـات در ادامه دیدارهای خـود با مقامات ونزوئلایی با «فردی نونییز»، همتای خود دیدار کرد و در این دیدار دو طرف درباره زمینه‌های همکاری‌های مشترک در حوزه شـبکه‌های ارتباطی و راه‌اندازی پلتفرم مشترک با هدف مقابله با نشر اطلاعات نادرست گفت وگو کردند.

هاشـمی در این دیدار تاکید کرد کـه امروزه فضای مجازی تمامی ساحت‌های زندگی انسان در زمینه‌های شخصی، اجتماعی، فرهنگی و اقتصادی را در برگرفته و در دنیای امروز کشورهایی برنده هستند که در بحث حکمرانی فضای مجازی دارای برنامه باشند.

وی با بیـان اینکـه ایـران در راه‌اندازی و توسـعه پلتفرم‌های داخلی توفیقاتی داشته، افزود که اکنون پلتفرم‌های بومی در ایـران نزدیک ۴۰ میلیون کاربر فعال دارند.

هاشمی با ابراز تمایل نسبت بر اشتراک گذاشتن دانش و زیرساخت‌های مرتبط با ایجاد و توسعه پلتفرم‌ها و شبکه‌های ارتباطی ایران در ونزوئلا، بر ظرفیت بالای ایران در مقابله موفقیت آمیز با حملات سـایبری به زیرساخت‌های ارتباطاتی اذعان کرد.


فردی نونییز، وزیر ارتباطات ونزوئلا نیز در این دیدار بر تولید محتوای درست در جهت مقابله با اخبار جعلی تاکید کرد و خواستار ایجاد یک پلتفرم مشترک برای تولید محتواهای درست و دقیق جهت مقابله با جریان سلطه شد.

وی همچنین با اشاره به سـفر خود به ایران و بازدید از دانشـگاه علامه طباطبایی، نسـبت به استفاده از ظرفیت‌ها و توانمندی‌های فنی و زیرساختی جمهوری اسـلامی ایران در نوسـازی و ارتقای سیستم‌های ارتباطاتی و رسانه‌ای ونزوئلا درخواستی ارایه کرد.

**گسترش همکاری‌های آموزشی در زمینه هوش مصنوعی**

وزیر ارتباطات و فناوری اطلاعات در ادامه رایزنی‌های فشـرده خود در ونزوئلا با «گابریل خمینز»، معاون رییس جمهوری و وزیر علوم این کشور دیدار کرد و دو طرف گسترش همکاری‌های آموزشی در زمینه هوش مصنوعی و مخابرات را بررسی کردند.

هاشمی در این دیدار با اشاره به حوزه‌های متنوع علمی، فناوری و تحقیقاتی و ظرفیت‌های فراوان بخش‌های مختلف وزارت ارتباطات همچون پژوهشگاه ارتباطات و فناوری اطلاعات، تاکید کرد که یکی از پیشنهادات ما در این زمینه فعال کردن بحث تبادل و اشتراک گذاری دستاوردهای پژوهشی، علمی و فناوری با ونزوئلاست.

وزیر ارتباطات با اشاره به برگزاری کمیسیون مشترک اقتصادی ایران و ونزوئلا در آینده‌ای نزدیک اعلام کرد: آمادگی داریم تعدادی از مراکز آموزشی و خانه فناوری در کاراکاس را برای آموزش برنامه‌های هوش مصنوعی فعال کنیم.

گابریل خمینز، معـاون رییس جمهوری و وزیر علوم ونزوئلا نیز در این دیدار نسـبت به همکاری در حوزه آموزش، تبادل تجهیزات و انتقال فناوری از ایران ابراز تمایل کرد و از پیشنهاد همکاری مشترک با تهران در حوزه تامین تجهیزات مخابراتی استقبال کرد.

**تفاهمنامه خدمات پستی میان ایران و کوبا**

و در بخش دوم سفر وزیر ارتباطات و فناوری اطلاعات به هاوانا وی با «ادواردو مارتینز» معاون نخست وزیر کوبا دیدار و درباره زمینه‌های توسـعه همکاری‌های علمی و فناورانه و ارتباطاتی با این کشـور گفت وگو کردند.

سـتار هاشـمی در این دیدار از امضـای تفاهم‌نامه همکاری میان دو کشور در حوزه خدمات پستی خبر داد و گفت: ظرفیت‌های بسیار زیادی برای همکاری میان تهران و هاوانا وجود دارد کـه امیدواریم بعد از انجام این نشست‌ها، فاز عملیاتی توافق‌ها آغاز شود.

وزیر ارتباطات با بیان اینکه «پیشنهادهای مشخصی در حوزه ارتباطات و فناوری اطلاعات از سوی دولت و بخش خصوصی ایـران تقدیم مقام‌هـای کوبایی شـده»، تصریح کرد: با توجه به روابط عمیق و ریشه دار دو کشـور، می‌توانیـم با نگاه انتقـال فناوری به کوبا روی اجرایی کردن برنامه‌های مشـترک اقدام کنیم.

وی خطاب به معاون نخسـت وزیر کوبا اظهار داشت: آماده ایم دانسته‌ها و تجربه‌هایی که در کشور داریم با شما به اشتراک بگذاریم و در حوزه‌های گوناگون بویژه هوش مصنوعی همکاری‌های خوبی را آغاز کنیم.

ادواردو مارتینز، معاون نخست وزیر کوبا در امور علم و فناوری نیز در دیدار با ستار هاشمی، به پیشرفت‌های چشـمگیر ایران در حوزه‌های علمی و فناورانه اشاره کرد و توسعه همکاری‌های دو کشـور در حوزه‌های مخابراتی، پستی و هوش مصنوعی را خواستار شد.

# حمایت‌گرایی دولتی از صنایع نوزاد، تیری در تاریکی

داود صفی‌خانی

حمایت‌گرایی دولتی از صنایع نوزاد موضوعی پرچالش در دنیا محسوب می‌شود، کشورهای توسعه یافته در دنیای امروزی با تمام فراز و نشیب‌های سیاست‌گذاری در نهایت به یک سیاست‌گذاری هوشمند و موثری در این زمینه رسیده و توانسته‌اند در نهایت بر چالش‌های سیاست‌گذاری در این زمینه در جهت توسعه رفاه جامعه غلبه کنند.

اما در این زمینه چالش‌های بسیاری پیش روی دولت‌ها توسعه نیافته وجود دارد، در کشور ما هم بعد از دهه‌های متمادی و سیاست‌گذاری‌های تقریبا ثابتی که در دولت‌های مختلف در این زمینه انجام شده، خروجی در نهایت منجر به رفاه مصرف‌کننده و حجیم‌تر شدن کیک اقتصادی کشور نشده است.

در واقع دولت‌های مختلف با وجود تفاوت اندکی سیاست ثابت در این زمینه را اجرایی کرده‌اند و آن افق، چشم‌انداز و امید به تغییرات اساسی در سیاست‌گذاری‌ها به شرح و تفصیلی که کشورهای توسعه یافته در این زمینه پیموده و اجرا کرده‌اند را در سپهر سیاست‌گذاری‌های داخلی نمی‌بینیم، از این رو به نظر می‌رسد دولت مسعود پزشکیان هم با تغییرات غیر موثری همچنان در همان مسیر دولت‌های قبل در حال حرکت خواهد بود.

در این زمینه سوال جدی این است که حمایت‌گرایی دولتی از صنایع مختلف از جمله خودرو، لوازم خانگی، کالاهای فناوری و در کلیت همه تولیدات داخلی چرا با وجود اصرار مداوم سیاست‌گذاری‌های دولتی منجر به خلق مزیت‌های رقابتی بین‌المللی و افزایش رفاه جامعه نشده است؟

علت آیا در ضعف عملکرد حمایت‌گرایی دولت‌هاست یا نه صنایع ما توان ایجاد زنجیره‌ای از ارزش افزوده رقابتی ندارند؟

این سوال از آن جهت مهم است که دورنما و چشم‌اندازی موثر به دولت چهاردهم می‌دهد تا بتواند حداقل در راستای اصلاح سیاست‌گذاری‌های اشتباه گذشتگان تعلل و سستی به خود راه ندهد و با درک درست مشکل، در راستای اصلاح آن قدم‌های محکم‌تری بردارد تا اصلاحات اساسی در سیاست‌گذاری‌ها از یک جایی به شیوه درست آن برداشته شود.

برای جواب دادن به این سوال مهم، موضوع را از زاویه موثری می‌شکافیم:

*تئوری حمایت از صنایع نوزاد می‌گوید که صنعتگران کشورهای پیشرفته یک مزیت خدشه‌ناپذیر رقابتی نسبت به صنعتگران نوپای کشورهای در حال توسعه دارند؛ هر دوی این صنعتگران باید هزینه ثابت هنگفتی بابت راه‌اندازی کارخانه، خرید ماشین‌آلات و تأسیس زیرساخت متحمل شوند، اما صنعتگران کشورهای پیشرفته می‌توانند هزینه‌هایشان را بر شمار زیاد تولیداتشان «سرشکن» کنند (صرفه‌های مقیاس بزرگ تولید)؛ این موضوع یک مزیت قوی رقابتی در بازار جهانی به آنها می‌بخشد.

علاوه بر آن، صنعتگران کشورهای پیشرفته به منابع عظیمی از نیروی کارآزموده‌ی انسانی، سرریز دانش فنی سایر شرکت‌ها و فناوری‌هایی دسترسی دارند که تنها در داخل آن کشور موجود است و صنعتگران نوپای کشورهای در حال توسعه دستشان از آنها کوتاه است. تئوری صنایع نوزاد از این موارد نتیجه می‌گیرد که کشورهای در حال توسعه می‌بایست با اعمال محدودیت‌های گمرکی، «مزیت هزینه‌ای» صنعتگران کشورهای پیشرفته را در بازار داخلی خنثی کنند تا صنعتگران داخلی توان گسترش مقیاس تولیدشان را پیدا کنند و به صرفه‌های ناشی از مقیاس برسند و بدین طریق در بازار جهانی رقابت‌پذیر شوند.*

مفاهیم بالا ساختاری‌ترین توجیه برای حمایت‌گرایی دولتی از صنایع نوزاد هست که تقریبا پای ثابت همه تئوری‌های قابل اجرا در کشورهای توسعه یافته بوده است و زیر بنای اصلی و اساسی حمایت‌گرایی همه دولت‌های دنیا از جمله کشور ما را هم شامل می‌شود.

اما بار دیگر برگردیم به سوال اینکه در نهایت چرا کشورهای توسعه یافته در زمینه اجرای سیاست‌گذاری‌ها موفق عمل کرده‌اند و هنوز ما در کشور اندرخم یک کوچه‌ایم!

حتی کشورهایی مثل ویتنام هم با بکارگیری درست سیاست‌گذاری حمایتی در عرض تنها یک دهه توانستند خود را به چهارمین تولید کننده بزرگ موتورسیکلت دنیا تبدیل کنند در حالی که صنایع مختلف ما بعد از دهه‌های متمادی حمایت‌گرایی هنوز در تامین نیاز داخلی هم مشکل دارند!

مشکل سیاست‌گذاری در کشور ما جدا از بحث تحریم‌ها، مشکلات مراودات مالی بین‌المللی، عدم ارتباط موثر با فناوری‌های فراملی، عدم الحاق به WTO و... عدم توجه به یک مقوله مهم است، اساسا سیاست‌گذاران دولتی در دهه‌های متمادی به قدری غرق در حمایت‌گرایی از صنایع مختلف با اعمال ممنوعیت‌های واردات، تعرفه‌گذاری بالا، بروکراسی‌های فزاینده برای واردات کالا و ... هستند که هدف نهایی حمایت از تولید داخل به فراموشی سپرده شده است.

در واقع هدف نهایی همه دولت‌های توسعه‌گرا برای حمایت از صنایع نوزاد، یک اصل بدیهی و روشن است و آن رفاه مصرف‌کننده است، مفهومی که در نظام سیاست‌گذاری حمایتی در کشور ما دهه‌هاست به فراموشی سپرده شده و در نتیجه آن با هر مرحله از اعمال سیاست‌گذاری‌های حمایتی دولتی از تولیدکنندگان داخلی به همان نسبت رفاه مصرف‌کننده ایرانی رو به نزول رفته است.

در واقع آزمون دیگر حمایت‌گرایی، جبران رفاه از دست‌رفته مصرف‌کننده است، بدین معنا که اعمال تعرفه‌های سنگین گمرکی و ممنوعیت‌های واردات رفاه مصرف‌کننده را کاهش می‌دهد تا سود تولیدکننده را افزایش دهد.

از طرفی مشکل ساختاری دیگر استراتژی پرخطای تولیدکنندگان داخلی است که با استفاده از وجه فراموش شده سیاست‌گذاری حمایت‌گرایی دولتی با اعمال انحصارهای گوناگون رفاه مصرف‌کننده داخلی را روز به روز تضعیف کنند.

در واقع با جمیع حمایت‌های دولتی مطالبه اصلی این است که تولیدکننده سود حاصل از انحصار (رانت اقتصادی) که ممنوعیت‌ها و حمایت گمرکی برایش آفریده را در انباشت قابلیت‌های فناورانه سرمایه‌گذاری کند؛ بدین معنا که فناوری‌های نوینی بخرد، نیروی کارش را آموزش و پرورش دهد، آزمون و خطا کند تا «دانش عملی» در تولید بدست آورد و مقیاس تولیدش را گسترش دهد تا به صرفه‌های مقیاس برسد و قابلیت رقابت در ابعاد بین‌المللی را کسب کند.

به نحوی که بعد از یک بازه زمانی حمایت‌گرایی با برداشتن آن حمایت‌ها و بازکردن کانال واردات، کاهش تعرفه‌ها و حذف بروکراسی‌های پیرامون این فرایند، بتواند با برندهای دنیا رقابت کند. به زبان ساده در نتیجه این موارد کالای مقرون‌به‌صرفه به مصرف‌کننده عرضه کند.

با این تعاریف روشن، لیکن در واقع مشکل سیاست‌گذاری دولت‌ها در کشور ما عدم توجه به این موارد مهم است، در واقع این بخش مهم و هدف اصلی فراموش شده و باعث انحرافات اساسی در هدف نهایی حمایت‌گرایی دولتی از صنایع نوزاد هست که به طور وسیعی مصرف‌کننده ایرانی را دچار زیان کرده است.

درست عکس این رویه در کشورهای توسعه یافته با توجه عمیق به این مقوله در نهایت اهداف اصلی یعنی رفاه مصرف‌کننده تامین شده و به دلیل عمق رقابت شدید در نهایت خیرعمومی آن به مردم می‌رسد نه صرفا تولید کنندگان که بتوانند نوعی از انحصار را نهادینه کنند!

CollectiveAction*

# X-شیدایی غریب ایلان ماسک

عباس پورخصالیان

در این یادداشت منظورم از X-شیدایی علاقهٔ مفرطِ شخص، به کاربُرد تکراری حرفِ یونانی/لاتینیِ X در نام‌گذاری‌های جعلی روی پروژه، پلتفرم، شرکت و حتی روی فرزند انسان است.

معادل لاتین اصطلاح جعلیِ مذکور را می‌توان X-mania در نظر گرفت. هر کسی که به طور کلی با مقولهٔ شیدایی یا مانیا در روان‌شناسی آشنا باشد، به راحتی منظور از X-شیدایی یا X-mania را می‌فهمد، حتی اگر وی این اصطلاح جعلی را برای نخستین بار شنیده یا خوانده باشد و آن را در حال حاضر در هیچ درسنامه و لغتنامه‌ای نیابد!

نمونهٔ بارز این پدیده را می‌توان به وضوح در شخص ایلان ماسک یافت. او نه تنها در نام‌گذاری روی بسیاری از شرکت‌ها، پروژه‌ها و ابتکارات فنی خود از حرف X استفاده کرده بلکه حتی در نام من-درآوردیِ آخرین فرزندش نیز دو حرف X را گنجانیده است [در زیر به نام جوان‌ترین فرزند ایلان ماسک خواهم پرداخت].

به دلیل علاقهٔ مفرط ایلان ماسک به حرفِ X و تکرار آن در نام‌گذاری‌های جعلی‌اَش روی پروژه، پلتفرم، شرکت و حتی روی فرزند خود، توجه نگارنده به موضوع X-شیدایی در شخصیت وی جلب شد و آنچه در زیر می‌خوانید، نتیجه بررسی نگارنده در این زمینه است.

علل این علاقهٔ مفرطِ ایلان ماسک را می‌توان حداقل در دو حوزه جست وجو کرد: یکی در حوزهٔ تبارشناسی و شناخت پیشینهٔ علمی حرف X؛ و دیگری در رابطهٔ قوی موجود میان نبوغ و جنون در روحیهٔ میلیاردرهایی شبیه ایلان ماسک.!

**● تبارشناسیِ حرفِ X**

استفاده از «x» به عنوان یک متغیر یا یک مجهول در ریاضیات با رنه دکارت، ریاضیدان و فیلسوف فرانسوی قرن هفدهم شروع شد. اما، ریشهٔ عمیق‌تر این تخصیص (تخصیصِ «x» به مفهوم «متغیر» و «مجهول» در ریاضیات) در واقع به ابتکار عمل مترجمان و شیوهٔ ترجمهٔ رسالهٔ ریاضی‌دان بزرگ ایرانی: حکیم عمر خیام از عربی به لاتین بازمی‌گردد.

عمر خیام (۱۰۴۸م-۱۱۳۱م) در معادلات جبر خود، مانند ما امروز از نمادها استفاده نمی‌کرد بلکه معادلات را همان طور که در سنت ریاضی‌دانان ایرانی/هندی/اسلامی آن زمان رایج بود، به صورت جملات کتبی می‌نوشت. وی برای مثال، متغیرها و مجهول‌های معادلات مورد اشارهٔ خود را «شِیء» می‌نامید و «شِیء» می‌نوشت.

اما هنگامی که ریاضی‌دانان اسپانیایی متن عربی رسالهٔ عمر خیام را می‌خواستند به لاتین ترجمه کنند، با مشکل ترجمهٔ «شیء» به معنای متغیر و مجهول، مواجه شدند و چارهٔ کار را بجای ترجمهٔ «شِیء» به لاتینی، در transliteration یعنی ترانویسیِ حروفِ کلمهٔ «شِیء» با استفاده از حروف الفبای لاتینی دیدند اما الفبای خط لاتینی (الفبای خط انگلیسی) فاقد حرفی معادل «ش» است. البته بعدها انگلیسی زبانان آمدند حرف «ش» را به صورت ترکیبی «sh» نوشتند ولی در زمان ترجمهٔ رسالهٔ عمر خیام به لاتینی، مترجمان مجبور شدند حرف یونانی X را که گاه معادل «شِ» یونانی است و در یونانی «شی (shi)» تلفظ می‌شود وام بگیرند و X را به عنوان حرفی جدید وارد سیستم خط لاتینی کنند.

به این ترتیب وام واژهٔ «شِیء» به معنای متغیر یا مجهول و به صورتِ «xei» در متون لاتینی وارد شد؛ سپس تا مدت‌ها بعد، «xei» در نزد ریاضی‌دانان اروپایی به معنی متغیر و مجهول در معادلات ریاضی به کار می‌رفت تا این که رنه دکارت نماد X را بجای «xei» به کار برد.

لذا پس از رنه دکارت و تا کنون، X دارای معنی متغیر، مجهول، نامرئی (مثل X-rey)، گاه نمایانندهٔ «چند چیز» (مثل FTTx) و گاهی نیز بجای «همه چیز» (مثل App X که بنا ست از توئیتر سابق به پلتفرمی برای همه چیز یا Everything App تبدیل شود).

**● رابطهٔ قوی میان نبوغ و جنون**

رابطه و فاصلهٔ قوی میان نبوغ و جنون در اغلب میلیاردرها و در افراد بسیار موفق مشاهده می‌شود، از آن جمله در شخصیت‌هایی مانند ایلان ماسک، استیو جابز، ریچارد برانسون و دیگر سرمایه داران بزرگ.

برخی از ویژگی‌هایی که معمولاً با نبوغ مرتبط هستند مثل: تفکر آرمانی، خودبزرگ بینی، جاه‌طلبی بی‌وقفه، مخاطره‌پذیری و تکانشگری بالا و رویکردهای نامتعارف ناشی از هواهای نفسانی، گاهی اوقات با رفتارهای عجیبی که می‌توانند جنون آمیز تلقی شوند، همپوشانی دارند. مثلاً مخاطره‌پذیری عموماً هولناک ایلان ماسک به عنوان بزرگترین مولتی میلیاردرِ و کارآفرین جهان، چه در امور مالی و چه در زندگی شخصی، معرف نبوغ خاص وی و امثال او است.

برای نمونه، ماسک، زمانی که دو شرکت اَش در آستانه ورشکستگی بودند، تقریباً تمام ثروت خود را در «اسپیس ایکس» و در «تسلا» سرمایه‌گذاری کرد. این تصمیم ایلان ماسک را می‌توان بی‌پروا اما در نهایتِ نبوغ تلقی کرد چرا که این مخاطره‌پذیری‌های هولناک تا کنون به موفقیت وی منجر شده‌اند.

**● ایلان ماسک موفق‌ترین کارآفرین دنیای فناوری**

ایلان ماسک موفق‌ترین کارآفرین دنیای فناوری و بزرگترین میلیاردر دلاری جهان در حال حاضر است. وی دارنده، نوآور، مدیرعامل و سهامدار عمدهٔ در شرکت‌های فرافنِ بسیاری است، از قبیلِ کسب و کارهای زیر:

- شرکت اسپیس ایکس (SpaceX) تولیدکنندهٔ پرتابگرهای پیشرفته و ماهواره‌های مخابراتی اینترنتی. وی در سال ۲۰۰۲ این شرکت را تأسیس کرد،
- شرکت تسلا (Tesla)، تولیدکنندهٔ خودروهای برقی و باتری‌های خشک که از سال ۲۰۰۸ ایلان ماسک در آن سِمت مدیرعاملی را بر عهده دارد،
- شرکت نورالینک (Neuralink)، سازندهٔ واسط‌های یاختهٔ عصبی و رایانه. وی در سال ۲۰۱۶ این شرکت را بنیان نهاد،
- شرکت بورینگ (The Boring Company)، سازندهٔ تونل‌های ترابری کالا و حمل و نقل مسافر که در سال ۲۰۱۷ ایجادش کرد،
- پلتفرم و رسانهٔ اجتماعی توئیتر که از سال ۲۰۲۲ مالک آن است و نام قبلی بسیار مشهور آن (Twitter) را در اوج شهرت جهانی توئیتر، به X تغییر داد زیرا که در نظر دارد و سعی می‌کند، پلتفرم X را از کارکرد قبلی‌اش که تنها یک پیام‌رسان بود با همهٔ انواع خدمات و محصولات اقتصاد دیجیتالی مجهز و آن را به یک Everything App تبدیل کند؛ و
- شرکت ایکس اِی آی (xAI)، تحقیق کننده و توسعه دهندهٔ سیستم‌های بدیع هوش مصنوعی. وی این شرکت را در سال ۲۰۲۳ ایجاد کرد.

**● تکرار حرف X در نامگذاری‌های ایلان ماسک**

حرف X یک واج (phoneme) تکراری در طول زندگی حرفه‌ای و شخصی ایلان ماسک است، آن هم بنا به شواهد و دلایل زیر:

**۱- وبگاه یا شرکتِ ایکس دات کام:** X.com او نخست وبگاه شرکت بانکداری برخط خود را X.com نامید که بعداً به پی پَل (PayPal) تبدیل شد، پی پَلی که محل رشد و نمو بنیان‌گذاران یوتیوب، یلپ (Yelp)، تسلا و لینکداین است.

**۲- شرکت اسپیس ایکس**

حرف X در نام شرکت اسپیس ایکس، نمایانندهٔ Exploration و اسپیس ایکس به معنی اکتشاف و نوآوری در حوزهٔ فضانوردی است. اهداف و عملکرد این شرکت، دقیقاً با جاه‌طلبی ایلان ماسک برای پیشگامی‌بخش خصوصی در سفرهای فضایی و احتمالاً "مستعمره سازی در مریخ" همسو است.

**۳- پلتفرم ایکس**

حرف X پس از این که ماسک توئیتر را در سال ۲۰۲۳ خرید، از کاربرد رایج آن [به عنوان یکی از حروف الفبای لاتین] تغییر کاربری داد و به عنوان اسم خاص و ویژند (Brand) جدید بجای توئیتر سابق به کار رفت و به کار می‌رود.

به گفته ایلان ماسک، هدف منظور شده در پس ویژندِ X، تبدیل شدن تدریجی توئیتر سابق به یک «اپلیکیشنِ جامع شاملِ همه چیز» مشابه آنچه «ویچت (WeChat)» در چین است می‌باشد؛ یعنی آمیزه‌ای رنگین و ترکیبی متنوع از پیام‌رسان اجتماعی به علاوهٔ سکوی پرداخت الکترونیکی دلار و یورو برای انواع تعاملات مالی مبتنی بر فین تِک (فناوری امور مالی دیجیتالی)، اینشورتِک (فناوری بیمهٔ دیجیتالی)، رِگ تِک (فناوری تنظیم‌گری دیجیتالی)، مِد تِک (فناوری پزشکی دیجیتالی) و هوش مصنوعی.

**۴- ایکس ("X") در نام یکی از یازده فرزند ایلان ماسک**

حتی در زندگی شخصی ایلان ماسک، حرف X باید نقش مهمی را ایفا کند. وی صورت نوشتاری نام جدیدترین فرزند خود را (۴ ساله از مادری که مدیر عامل شرکت نورالینک است) «X Æ A-12» گذاشته است و او را X Ash A Twelve صدا می‌زند! با توجه به این که عدد ۱۲ را می‌توان به صورت «XII» هم نوشت و نشان داد، در واقع در نام مذکور دو بار از حرف X استفاده شده است: یک بار به عنوان مجهول و متغیر ناشناخته و بار دیگر به عنوان جایگزین! شاید به این دلیل که نطفهٔ فرزند یازدهم ایلان ماسک: X Ash A Twelve نخست در لوله آزمایشگاه بسته شد و سپس به رحمی جایگزین منتقل و کلاً در زیست فناورانه نضج گرفت.

**● جمع بندی و نتیجه گیری**

این نوع انتخاب نام فرزند، بهترین نشان دهندهٔ «X-Mania» به معنی تمایل مفرط شخص ایلان ماسک به استفادهٔ مکرر از حرف X است. اما حتی آنجا که وی نمی‌تواند از حرف X استفادهٔ مکرر کند مثلاً در جمله بندی‌ها و اظهار نظرهای کوتاهش در رسانهٔ اجتماعی X به عنوان کامنت، آنجا هم شیدایی عمومی‌اش در کاربرد طنز با زبان و بیانی نمادین و شایعه پراکنی رمز-و-راز آلود با چاشنی آینده‌نگریِ غیر متعارف، مشهود است؛ از آنجمله می‌توان به قصد و نظر اولیه‌اش مبنی بر پرداخت ماهانه ۴۵ میلیون دلار به کارزار انتخاباتی ترامپ در سال جاری اشاره کرد که در پلتفرم X و در سایر رسانه‌ها به سرعت وایرال شد و سپس به تکذیبه‌اش در یک مصاحبه مبنی بر این که از پس پرداخت ماهانه ۴۵ میلیون دلار به کارزار انتخاباتی ترامپ بر نمی‌آید!

نمونه‌ای دیگر از این رفتار متناقض را می‌توان در ادعاهای ایلان ماسک در رابطه با راه‌اندازی اینترنت استارلینک در خاک ایران مشاهده کرد، در حالی که وی خوب می‌داند که سرویس‌دهی در کشورهایی که استارلینک هنوز مجوز سرویس‌دهی در آن کشورها را از رگولاتوری‌شان دریافت نکرده، از لحاظ حقوق بین‌المللی و مقررات جهانی اتحادیهٔ بین‌المللی مخابرات ممنوع است، هرچند از لحاظ فنی، شدنی باشد.

من ادله‌ای در دست ندارم اما به طور شهودی یقین دارم که مدیریت هولدینگ استارلینک در هلند که مسؤول راه‌اندازی خدمات این شرکت در کشورها است، به ادعاهای ایلان ماسک در رابطه با فعال‌سازی سرویس دهی استارلینک در ایران (و در اوکراین!!! نیز) می‌خندد.

بدون شک، این رفتار شایعه‌پراکنه و حیله‌گرانهٔ او را نیز باید در پرتو نبوغ و جنون وی ارزیابی کرد.

# ماناامنیم

امیرحسین سعیدی نائینی

گرچه از انتخاب جناب دکتر پزشکیان مدتی است می‌گذرد اما هنوز هم صنفیان موفق نشدند در جلسه‌ای روی ماه ایشان و مسوولین مربوطه را زیارت و مشکلات خود را با ایشان در میان گذارند که اگر چنان می‌شد گزارش زیر پیش‌بینی آن جلسه است.

ابتدا عزیزی از عزیزان همکار که موی سپید داشت و سابقه‌ای طولانی در کار صنفی و ریاست سنی هم با او بود به عنوان ریاست جلسه پشت میکروفون رفته و از حضور عزیزان تشکر و اضافه کردند که: بهتر آن بود ریاست محترم جمهور و مسوولین ذیربط را در میان خود داشتیم اما از انجا که بعد از انتخابات عزیزان ارتباط ما با ایشان تقریبا قطع می‌شود و امیدی بر گشایش عریضه و نامه ما ضعفا توسط روسا نیست؛ بر آن شدیم تا این مجلس را تشکیل و نتیجه آن منتشر تا بلکه پیام ما را از بهر خدا واز سر لطف؛ باد صبا برساند به گوش آنها.

از همکاران عزیز تقاضا دارم از حال خود آنچنان که هست بگویند و زبان در کام نگیرند والبته دلخراش و ناملایم و ناحق نگویند.

اولین نفر اجازه صحبت خواست و چنین گفت: بعد از سال‌ها کار نرم‌افزاری و ارائه خدمات و محصولات فراوان و ایجاد اشتغال برای متخصصان و کسب رضایت مشتریان و داشتن سامانه‌هایی با انبوهی از کاربران، حال که پایمان به لب گور رسیده است بجای خسته نباشی و خدا قوت، برخی عزیزان از نهادهای نظارتی ما را با تصور اینکه ممکن است حفره‌ای در نرم‌افزارمان باشد اسیر خود کرده‌اند و بیش از یکماه است که هر چه خواسته‌اند برحسب وظیفه داده و البته نگرانیم که فردا روزی چیزی بخواهند که نتوانیم بدهیم. ولی هنوز حفره که هیچ سوراخی هم نیافته‌اند و اگر یافته‌اند علیرغم پیگیری‌های مستمر به ما نگفته‌اند. البته که توجه و عنایت این عزیزان جای بسی تشکر و قدردانی دارد اما چرا بهانه فراخ و دهان تنگ داشته‌اند؟ عدم پاسخگویی ایشان وصف حال بیتی است که می‌گوید:

ای وای بر اسیری که از یاد رفته باشد
در دام مانده باشد صیاد رفته باشد

اما موضوع آنگاه آزاردهنده‌تر می‌شود که بدون هیچ اطلاع به ما از بعضی مشتریان خواسته‌اند سریعاً نرم‌افزار را عوض کنند. بگذریم که این نوع برخوردها وروش‌ها در شان شرکت‌های زحمت کش داخلی نیست ولی این سئوال پیش می‌آید که اگر نرم‌افزاری ناامن است چرا به صاحبانش اطلاع نمی‌دهید تا رفع کنند؟ آیا این تعلل در اطلاع رسانی فرصتی برای دشمن جهت نفوذ فراهم نمی‌کند؟

سوال بعدی آنکه اگر نرم‌افزاری دارای حفره امنیتی باشد و باید آن را در یک دستگاه یا سازمان تعویض کرد، تکلیف بسیاری از دستگاه و یا سازمان‌های دیگر که از کاربران آن هستند، چیست؟

اگر قصد ادامه کار با آن باشد باید فوری ضعف‌های امنیتی آن مرتفع شود و از بوق و کرنا کردن آن ضعفت امنیتی به شدت پرهیز کرد و اگر قصد آن باشد که کلیه کاربران باید کاربری آن را به کنار گذارند پس تکلیف شرکتی که سال‌های سال با بکارگیری متخصصان بسیار وصرف هزینه‌های هنگفت آن را تولید کرده است چه می‌شود؟

برفرض آنکه ورشکستگی آن شرکت کوچکترین اهمیتی نداشته باشد، تکلیف مهندسان خبره که با صرف سال‌ها هزینه آن شرکت زبده شده و اطلاعات بسیاری در دست دارند و اکنون که بیکار می‌شوند چه می‌شود؟ که البته این مشکل با ولع کشورهای متخاصم همچون آمریکا برای بلعیدن نیروهای توانمند ما به سرعت رفع می‌شود.

آیا این در بدر کردن شرکت و بیکاری قشر مستضعف آن شرکت و تقدیم متخصص ارزشمند کشور به دشمن کار درستی است؟ موضوع جایگزینی نرم‌افزاری که سال‌ها در سازمانی ریشه دوانده و هزینه‌های مالی و غیرمالی و مشکلات فراوان مربوطه به سازمان و مردم را می‌گذریم، اما آیا اگر خدای ناکرده این روش‌ها ادامه پیدا کند به سمتی پیش نخواهیم رفت که تمامی قراردادهای مهم تنها با خارجی‌ها منعقد شود؟ آیا این صیانت از شرکت‌ها و حفظ امنیت است؟ آیا ادامه این روش‌ها منجر به ناامنی و بی اعتمادی و از هم پاشیدگی شرکت‌ها نمی‌شود؟

صحبت‌های نه چندان نرم و گرم نفر اول تمام شد که نفر دوم شروع به صحبت کرد:

آنچه همکار عزیزم فرمود مورد تائید اینجانب نیز هست و در واقع رفتاری مشابه سر شرکت ما آورده‌اند و هیچ فرد مسوولی مکتوب یا رسمی دلیلی ارائه نداده است. فقط می‌گویند علت می‌تواند دو تابعیتی‌بودن اینجانب باشد و دلیل دو تابعیتی بنده اقامت پدرم در نجف اشرف برای فراگیری علوم دینی بوده است که منم آنجا به دنیا آمده و دارای پاسپورت آن کشور شده و هر چه می‌گویم حقیر اختیاری در محل تولدم نداشته‌ام نمی‌پذیرند و می‌گویند قانون است و ما مکلف به انجام آن هستیم.

در همین حال خانمی از جا بلند شد و با صدای بلند و کمی تا قسمتی عصابی گفت: منم بابام سفیر بوده خارج به دنیا اومدم و پاسپورت اونجا را گرفتم، حالا رد صلاحیت امنیتی شدم و با این سئوال فرمایشات خود را پایان داد که: آیا دختر سفیر بودن جرررمه؟

نفر دیگر که از هم‌صنفی‌ها با سابقه‌ای طولانی بود گفت: باور بفرمائید روزگار کمی سخت شده چون؛ ما از نظر دشمنان خارجی که از نظر تکنولوژی مقام بالایی دارند و بالاترین مقام را در رذالت و پستی و جنایت دارا می‌باشند و قصد نفوذ و حمله سایبری دارند و می‌خواهند همه امور و اطلاعات در دست خودشان باشد سر خر و مانع و نا امنیم، از نظر جریان اژدهای هفت سر فساد که با سامانه‌های خود راه را بر آنها می‌بندیم هم مانع و مزاحم و نا امنیم.

ولی از همه دشوارتر و آزاردهنده‌تر از نظر برخی مسوولان نظارتی که باید حامی ما باشند نیز نا امنیم و بمحض اینکه گمان کنند نفوذی در نرم‌افزارهای ما صورت پذیرفته: فاتحانه حمله آرند بر ما مانند باد، تا بگیرند هر چه خواهند از سند و مدرک با رویی باز. به امید آنکه ثابت کنند تویی جاسوس آن دشمن نابکار کودک کش. کار بدینجا که کشید رئیس بلند شد و گفت: گرچه از دستگاه‌های نظارتی نعمت امنیت و صحت رسد و در نتیجه بسی خیر به ملت رسد اما چندیست که برخی می‌نوردند شرکت‌ها را با گام‌های نرم و بی‌آو اولی سنگین و با معنا آنچنان که زار گریند بر احوال دل خویش فاوابیان و شرکت‌ها حس می‌کنند که همه مهر و وفا از آنان است و همه جور و جفا از عزیزان مسئول، وقت آن رسیده که بگشایند در صلح و صفا و در جنگ فروبندند.

آقای رئیس بار دیگر وارد بحث شد و گفت: از قدیم گفته‌اند تنها به قاضی نباید رفت و به همین دلیل عزیزی در جمع ماست که ترجیح می‌دهد معرفی نشوند ولی این امور را بهتر از ما می‌داند و از ایشان تقاضا داریم با سخنان خود ما را مستفیض نمایند.

مردی متین و با وقار به آرامی پشت میکروفون قرار گرفت و چنین گفت: فرمایشات شما در نزاع و دفاع طولانی شد و مجال تعمق و تأمل را تنگ گردانید و مادام که سخن از در انصاف نباشد روی حقیقت کارها بغرض پوشیده ماند و آتش دوری و تفرقه از آن برخیزد و دوست سوزی و دشمن شادی در پی خواهد داشت.

داستان شما گرچه در راستای دوستی است که این از پسندیده‌ترین کارهاست لیکن از بعضی کنایه‌ها و طعنه‌ها این معنا بر نمی‌آید و تلاش فداکارانه مسوولین نظارتی را اجر و قدری نمی‌نهد.

بر فرض آنکه در راه خدمتگزاری و ظیفه شناسی و فداکاری خطایی رفته باشد اینگونه تاختن رسم خادم و مخدومی را خدشه دار می‌کند، امنیّت زیرساخت همه ابعاد زندگی یک جامعه است، امنیت برای زندگی مردم و یک جامعه، گاهی از نان شب واجب‌تر و مهم‌تر است.

حفظ امنیت و مقابله با ناامنی مهم‌ترین دغدغه کشورها در عصر حاضر است. زیرا تنها در پرتو امنیت است که بشر قادر خواهد بود به پیشرفت و ترقی نائل آید. اگر رسم امنیت از میان برداشته شود بجایش شرر و خنجر خواهد آمد و اگر امنیت نباشد لبی به لبخندی گشوده نخواهد شد.

لذا نباید با افکاری خام و سخنانی نسنجیده این نعمت بزرگ را مورد تاخت و تاز قرار دهیم. قصد آن نیست که با پاسخ‌هایی که حق است ولی کام دوستان را تلخ می‌نماید از لطافت جلسه بکاهم ولی لازم است جهت تنویر افکار چند جمله‌ای معروض دارم.

دوستی که گله مند است چرا حفره امنیتی نرم‌افزارش را به او اعلام نکرده‌اند جسارتا باید بداند که اولین محل مشکوک برای بررسی شرکت اوست اگر ثابت شد که علت خود آن شرکت نیست حتماً با ایشان در میان خواهند گذاشت.

و دوست دیگری که معترض رد صلاحیت خود به‌علت دو تابعیتی می‌باشد باید توجه داشته باشد که نص صریح قانون در مورد مشاغل حساس چنین است.

والبته دلایلی نیز بر آن مترتب است و این امر در بسیاری از کشورها نیز وجود دارد و از آن بعنوان PEP یا Politically expose Person یاشخصی که از نظر سیاسی در معرض دید عموم است یاد می‌کنند. از آن گذشته ایشان بهتر از بنده می‌دانند که به هر کسی در بدو ورود ملیت و در نتیجه پاسپورت آن کشور را اهدا نمی‌کنند و مراحلی دارد از جمله قسم خوردن و تعهد دادن برارجح بودن منافع آن کشور به هر کشور دیگری. حال چگونه می‌توان به فردی که چنین تعهدی به کشوری بیگانه داده است شغلی حساس واگذار کرد؟

مسلم است که این فرد براساس تعهد و قسمی که یاد کرده است همواره می‌تواند بالقوه خطری برای امنیت کشور باشد. حتی اگر دستگاه‌های امنیتی آن کشور بیگانه از او اطلاعاتی درخواست کنند برحسب وظیفه‌اش باید همکاری کند و اگر بگوییم در مقابل تعهد و قسمش مسئولیتی حس نمی‌کند پس فرد متعهدی نیست و بازهم نمی‌تواند عهده‌دار شغلی حساس باشد.

فرمایشات این بزرگوار که تمام شد رئیس جلسه از فردی با موهای ژولیده خواست تا با توجه به ضیق وقت از طرف شرکت‌ها صحبت کند.

و ایشان چنین گفت: با تشکر از رئیس جلسه که این فرصت را در اختیار حقیر قرار دادند، مرا نیز چون سخنران قبلی عقیده بر این است که فرمایشات طولانی شد و در نتیجه مجال تعمق و تأمل تنگ است، در دفاع از شرکت‌های مظلوم فاوا سینه‌ها سخن دارم که دهانی به پهنای فلک می‌خواهد.

گرچه متانت و وقار این برادر عزیز تحسین برانگیز بود ولی اگر تصور شود که ما را اندیشه برنزاع است و اتحاد و دوستی و برادری در سرنیست صحبت و مراودت چه ثمری و معاشرت چه حاصلی خواهد داشت؟

هر ایرانی مسلمان و وطن دوستی با تمام وجود معتقد به اهمیت امنیت و حفظ آن به بهترین شکل ممکنه است. ما در این کشور زندگی می‌کنیم، ما دارو ندار خود را در اینجا سرمایه‌گذاری کرده‌ایم، ایجاد اشتغال کرده‌ایم، متخصصان ایرانی را به کار گرفته‌ایم و مانع آن شدیم که برای دشمن کار کنند. پس امنیت این کشور برای ما بسیار مهمتر است تا مسوول و مقامی که امروز می‌آید و فردا می‌رود.

ولی حرف این عزیزان این است که روش‌های به‌کار برده شده موجب خسران است. این مطلب که در انتخاب افراد در جایگاه مشاغل حساس نباید خود و یا افراد درجه یک ایشان دو ملیتی باشند حکم قانون است، اما این قانون شامل مشاغل حساس دولتی است و نه بخش خصوصی. اگر بخواهیم این قانون را برخلاف قانون به بخش خصوصی تحمیل کنیم بسیاری از صنایع از پا درخواهند آمد زیرا تعدادی از مدیران و متخصصان آن می‌توانند دو ملیتی باشند.

باتوجه به اهمیت کار شما که جان برکف از منافع ما دفاع می‌کنید بدانید که از صمیم قلب برایتان دعا می‌کنیم و دوستتان داریم اما نمی‌دانیم که کدام رسم است که کشند عاشقی را که تو عاشقم چرایی؟

جرمی نداریم بیش از اینکه از جان و دل به شما وفاداریم و اگر قصد آزار ما کنید هرگز نه می‌توانیم و نه می‌خواهیم که بیازاریم شما را. ما آن دیوار کوتاهیم که هر که بخواهد برسر ما می‌نشیند، لیکن همچنان بر سر وفا بوده و هستیم.

می‌دانید مسئول حفظ امنیت شمائید، می‌دانید که جنگ‌های سایبری هر روز گسترده‌تر و خطرناک‌تر می‌شود و می‌دانید سربازان جنگ این جبهه ما هستیم و می‌دانید که سرداران و فرماندهان این جبهه شمائید. ولی به جای حمایت همه جانبه که توقع بحق ماست، اگر حس کنید دشمن نابکار در جایی نفوذی کرده، ما را عامل می‌پندارید.

خوب می‌دانید که دشمن رذل کودک کش، جهان استکبار را پشت و پناه دارد و با تمام امکانات بر ما می‌تازد لیکن آنچنان که باید و شاید از فعالان داخلی حمایت نمی‌شود. امن بودن محصول و خدمات را ارجاع به شرکت‌های دیگر دادن، البته می‌تواند مفید باشد ولی نه به این صورت.

ما از شما توقع داریم که در صورت اثبات جاسوسی آنچنان بلایی برسر فرد و یا افراد خائن آورده که عبرتی شود برای دیگران که حتی تصور این عمل شنیع بر ذهن فرد دیگری نگذرد و البته هرگونه جرمی دیگری نیز طبق قانون عمل شود اما در غیر اینصورت همواره این دعای حضرت سجاد را نصب العین خود قرار داده که می‌فرمایند:

وَ أَسْتَعْمِلُ حُسْنَ الظَّنِّ فِی کَافَّتِهِمْ
(درباره همهٔ آنان خوش‌گمانی را به‌کار گیرم)
وَ أَتَوَلَّی بِالْبِرِّ عَامَّتَهُمْ،
(همهٔ آنان را با نیکوکاری سرپرستی کنم)
وَ أَغُضُّ بَصَرِی عَنْهُمْ عِفَّةً،
(عفیفانه چشم از خطایشان بپوشم)
وَ أُلِینُ جَانِبِی لَهُمْ تَوَاضُعاً،
(فروتنانه با آنان نرم باشم)
وَ أَرِقُّ عَلَی أَهْلِ الْبَلَاءِ مِنْهُمْ رَحْمَةً،
(مهربانانه بر بلادیدهٔ آنان رقّت آورم،)
وَ أُسِرُّ لَهُمْ بِالْغَیْبِ مَوَدَّةً،
(در پنهان دوستی خود را بر آنان ظاهر سازم)
وَ أُحِبُّ بَقَاءَ اَلنِّعْمَةِ عِنْدَهُمْ نُصْحاً،
(خیرخواهانه دوام نعمتشان را بخواهم)
وَ أُوجِبُ لَهُمْ مَا أُوجِبُ لِخَاصَّتِی
(آنچه برای اقوام خود لازم می‌دانم؛ برای آنان لازم بدانم،)
وَ أَرْعَی لَهُمْ مَا أَرْعَی لِخَاصَّتِی.
(آنچه برای مخصوصان خود رعایت می‌کنم، برای آنان رعایت کنم.)

و در پایان بیانیه‌ای به شرح زیر قرائت شد:

۱ - شرکت‌ها طبق وظیفه قانونی، شرعی و ملی خود باید در راستای اوامر ابلاغی دستگاه‌های نظارتی نهایت همراهی و همکاری را داشته باشند.

۲- دستگاه‌های نظارتی نقطه تماسی را برای افراد و یا شرکت‌هایی که به هر علتی مورد اتهام واقع شده‌اند، ایجاد نماید و چه بهتر که با تعمیق روابط حسنه خود با مسئولین صنف فاوا ایشان را همانگونه که فعالان بخش خصوصی مورد احترام و اعتماد قرار داده، حمایت نماید ولی تمامی امور مربوط به صنف و شرکت‌ها با مراجعه به صنف خود پاسخ رسمی دریافت دارند.

با کمال تأسف دیده شده که شرکت یا شرکت‌هایی بدون هیچ اطلاع و بعد از مدتی توسط مشتریانش آن هم نه به صورت کتبی یا رسمی مطلع می‌شود که علت عدم پرداخت وجوه کارهای انجام شده قبلی و یا عدم تمدید قراردادش این است که مورد ظن یک دستگاه نظارتی است. لیکن مورد ظن چیست؟ به کجا باید مراجعه کند؟ چه کسی مسول پاسخ‌گویی است؟

۳- هرگونه اقدامی که به کسب و کار شرکت‌ها لطمه وارد کند، باعث فرار متخصصین به خارج از کشور شود، دستگاه‌های دولتی و غیر دولتی استفاده کننده از محصولات و خدمات شرکت‌ها را با مشکل و توقف روبرو کند، و یا خدای ناکرده لطمه به عزت و حیثیت متخصصین متعهد شاغل شود و مصادیق بارز آیه: وَالَّذِینَ یُؤْذُونَ الْمُؤْمِنِینَ وَالْمُؤْمِنَاتِ بِغَیْرِ مَا اکْتَسَبُوا فَقَدِ احْتَمَلُوا بُهْتَانًا وَإِثْمًا مُبِینًا (احزاب ۵۸)، شدیداً محکوم است و در صورتی که شرکت یا شرکت‌هایی با این امور روبرو هستند فوراً باید مشکلشان مرتفع شود.

۴- حفظ امنیت برای دستگاه‌های نظارتی و شرکت‌های فاوا مستلزم هزینه می‌باشد که درصدی از مبلغ قراردادهای منعقده بین شرکت‌ها و مشتریان باید بابت امنیت در نظر گرفته شود تا هزینه‌های لازم برای امن ساختن نرم‌افزارها توسط دستگاه‌های مسوول فراهم و در نتیجه شرکت‌ها و مشتریان با خیال راحت به کار خود ادامه دهند.

۵- متولیان نظارتی باید عمیقا درک کنند که در این ایام که جنگ سایبری جنگی واقعی، موثر و کارساز است، شرکت‌های داخلی حکم سربازان مقدم این جبهه را دارند و آنها فرماندهان جنگ و مسئول پیروزی و یا شکست هستند و باید آمادگی لحظه‌ای برای دفاع و حمله را به وجود آورند. شرکت‌ها را به شرکت‌هایی دیگر ارجاع دادن، مناسب جنگ نیست.

۶- شرکت‌های فعال در حوزه فاوا با توجه به بکارگیری این فناوری در جنگ‌های سایبری و تمرکز دشمن نابکار برای شکار لحظات جهت ضربه زدن؛ بیش از پیش باید بر اهمیت و حساسیت امنیت توجه نمایند و بدانند که اگر خدای ناکرده موج ناامنی ما را فراگیرد فرار از غرق شدن به این راحتی‌ها نخواهد بود. لذا چنانچه در راستای تأمین امنیت خود از دستگاه‌های متولی نقصانی می‌بینند از طریق نمایندگان صنفی از هیچ تلاشی برای رفع آن دریغ نورزند.

پایان جلسه نیز با این دعا که حاضرین باهم قرائت کردند به اتمام رسید:

یا رب به محمد و علی و زهرا
یا رب به حسین و حسن و آل‌عبا
کز لطف برآر حاجتم در دو سرا
بی‌منت خلق یا علی الاعلا

# پرتاب موفق ماهواره‌های هدهد و کوثر

محققان شرکت دانش‌بنیان فضایی با طراحی و ساخت دو ماهواره «هدهد» و «کوثر» توانستند این دو ماهواره را با موفقیت از پایگاه روسیه به مدار ۵۰۰ کیلومتری تزریق کنند.

به گزارش عصر ارتباط در این پرتاب ۵۳ ماهواره همراه فضاپیمای سایوز است که دو مورد از این ماهواره مربوط به ماهواره های ایرانی هدهد و کوثر است. این ماهواره‌ها با نسخه ۲.۱B سایوز همراه هستند که تاکنون ۱۹۰۰ پرتاب را داشته است.

کاربرد این منظومه ماهواره‌ای که با عنوان دو نما از آنها یاد می‌شود، در جنگلداری و حفاظت و پایش محیط زیست با تصاویر ماهواره‌ای است. منظومه ماهواره ای دونما با ارائه داده‌های دقیق ماهواره‌ای به حفاظت پایش محیط زیست با تصاویر ماهواره ای و زیست‌بوم‌های طبیعی کمک می‌کند. به این ترتیب که این ابزار با شناسایی تغییرات در پوشش گیاهی، پایش منابع آب، جلوگیری از جنگل‌زدایی و ارزیابی آسیب‌های ناشی از بلایای طبیعی، مدیران و کارشناسان را در حفظ زیست بوم یاری می‌دهد.

**● شناسایی تغییرات در پوشش گیاهی**

یکی از اصلی‌ترین کاربردهای پایش محیط زیست با تصاویر ماهواره‌ای، شناسایی تغییرات در پوشش گیاهی است. با استفاده از تصاویر ماهواره‌ای با وضوح بالا، داده‌های زمان‌بندی شده مربوط به شاخص‌های گیاهی مانند شاخص نرمال‌شده تفاوت پوشش گیاهی (NDVI) می‌توانند تغییرات جزئی در تراکم و سلامت پوشش گیاهی را در بازه‌های زمانی کوتاه شناسایی کنند؛ درست مانند سامانه فضایش. فضایش این امکان را به نهادهای نظارتی می‌دهد تا به سرعت نسبت به کاهش تراکم جنگل‌ها و یا تخریب پوشش گیاهی واقف شوند و اقدامات لازم را در مراحل اولیه انجام دهند.

**● مدیریت منابع آب و پایش محیط زیست**

در مدیریت جنگل‌ها، کنترل منابع آب اهمیت حیاتی دارد. داده‌های ماهواره‌ای ضبط شده توسط منظومه دونما می‌توانند برای تحلیل تغییرات منابع آب در زیست‌بوم‌های جنگلی مورد استفاده قرار گیرند.

این داده‌ها می‌توانند به پیش‌بینی خشکسالی‌ها و ارزیابی تأثیرات تغییرات آب و هوایی بر منابع آبی کمک کنند.

مدیران محیط زیست می‌توانند از این داده‌ها برای بهبود استراتژی‌های مدیریت منابع آبی در مناطق جنگلی بهره‌برداری کرده و از تخریب زیست‌بوم‌های حساس جلوگیری کنند.

برای مثال تصاویر ماهواره‌ای از دریاچه ارومیه در سال‌های متمادی می‌تواند کارشناسان را از وضعیت این دریاچه، آگاه و کمک کند تا اقداماتی در جهت بهبود وضعیت پیش‌آمده صورت گیرد.

**● پایش و جلوگیری از جنگل‌زدایی**

جنگل‌زدایی یکی از بزرگ‌ترین تهدیدها برای زیست‌بوم‌های طبیعی است. داده‌های به‌دست‌آمده از تصاویر ماهواره‌ای منظومه دونما می‌توانند به طور مداوم تغییرات در سطح جنگل‌ها را پایش کنند. با استفاده از الگوریتم‌های تحلیل تصاویر می‌توان به‌سرعت مناطقی را که در حال تخریب هستند، شناسایی کرد و با اتخاذ تصمیمات پیشگیرانه، جلوی ادامه روند تخریب را گرفت. این فرآیند با سنجش خودکار و پردازش سریع داده‌ها، امکان واکنش به موقع و مؤثرتر را فراهم می‌کند. فرض کنید ورود سموم کارخانجات در آب مورد نیاز گیاهان باعث تخریب پوشش گیاهی در ناحیه‌ای به‌خصوص شود؛ در این شرایط پوشش گیاهی در آن ناحیه دچار تغییرات می‌شود و این تغییرات در تصاویر ماهواره‌ای از طریق مقایسه بازه‌های زمانی مختلف قابل تشخیص و مشاهده هستند.

صاحب امتیاز و مدیرمسئول: احمد محمدغریبان
سردبیر: علی شمیرانی
رییس شورای سیاست گذاری: حسین محمدیان

نخستین هفته‌نامه فناوری اطلاعات و ارتباطات ایران
ASREERTEBAT.COM

عصر ارتباط

نشانی دفتر مرکزی: خیابان ولی عصر، خیابان توانیر، میدان عباسپور، پلاک ۳، ساختمان پزشکان طلا، طبقه ۲، واحد ۲۱ ■ تلفن تماس: ۸۸۷۷۹۰۰۴ ■ چاپخانه: گنجینه مینیاتور

### اف‌بی‌آی مدعی شد:

# حمله گروه سایبری ایرانی به المپیک تابستانی

سمیه مهدوی‌پیام

اف‌بی‌آی و چند نهاد دیگر، گروه‌های سایبری منتسب به ایران را به هدف قرار دادن المپیک تابستانی ۲۰۲۴، از جمله تلاش برای تصاحب تابلوهای نمایشگر به منظور محکوم کردن اسرائیل متهم کرده‌اند.

Therecord در گزارشی نوشته، وزارت خزانه‌داری آمریکا و سازمان ملی سایبری اسرائیل به همراه اف‌بی‌آی، اخیرا یک هشدار رسمی منتشر کردند که به فعالیت‌های سایبری یک شرکت ایرانی و عملیات سایبری شناخته‌شده آنها که قبلا در زمینه هک علیه اسرائیل و انتخابات ریاست جمهوری ۲۰۲۰ آمریکا دخیل بوده، اشاره دارد.

این گروه از شرکت دیگری، به عنوان پوشش عملیات خود استفاده کرده است. پژوهشگران این شرکت را با نام‌های مختلف از جمله "Cotton Sandstorm" و "Haywire Kitten" شناسایی کرده‌اند.

در این هشدار رسمی آمده است: «این گروه، از اواسط سال ۲۰۲۴، مهارت‌های جدیدی را برای انجام عملیات اطلاعاتی سایبرمحور به‌کار گرفته و از شخصیت‌های پوششی متعدد استفاده کرده است. این موضوع، چند عملیات سایبری مختلف و هدف‌گیری‌شده در المپیک تابستانی ۲۰۲۴، از جمله نفوذ به یک ارائه‌دهنده تجاری نمایشگر پویا در فرانسه را شامل می‌شود.

شرکت مذکور همچنین تلاش کرده محتواهایی را از طریق دوربین‌های آی‌پی که معمولا برای ضبط ویدئوهای نظارتی استفاده می‌شوند، کسب کند و برای این منظور، از ابزارهای هوش مصنوعی آنلاین نیز استفاده کرده است.

در ادامه این هشدار آمده است: «از سال ۲۰۲۳، این گروه روش‌های جدیدی را به‌کار گرفته است. این روش، استفاده از نمایندگان فروش هاست جعلی برای فراهم کردن زیرساخت‌های سرور عملیاتی برای خود و یک بازیگر لبنانی را که در حوزه میزبانی وب فعالیت دارد، شامل می‌شود.

طبق گزارش اف‌بی‌آی، هکرها از ابزارهای مختلف برای تسلط بر ارائه‌دهنده تجاری نمایشگر پویا در فرانسه، در ژوئیه ۲۰۲۴ استفاده کردند. هدف آنها «نمایش فتومونتاژهایی برای محکومیت حضور ورزشکاران اسرائیلی در بازی‌های المپیک و پارالمپیک ۲۰۲۴ بود.

اف‌بی‌آی افزود: «این حمله سایبری با مانورهای انتشار اطلاعات نادرست همراه بود و انتشار یک مقاله جعلی در وب‌سایت رسانه‌ای تعاملی فرانسوی و ارسال پیام‌های تهدیدآمیز به چندین ورزشکار اسرائیلی و همراهان آنها با نام گروه راست‌گرای افراطی جعلی فرانسه به نام «هنگ GUD» را که در واقع از نام گروه راست‌گرای «GUD» سوءاستفاده کرده بود، شامل می‌شد.»

### ● هدف‌گیری سوئد و آمریکا

این هشدار که بر اساس تحقیقات و تحلیل‌های فنی اف‌بی‌آی تهیه شده، به تحقیقات جدیدی از مایکروسافت نیز اشاره دارد و نشان می‌دهد این گروه، علاقه‌مند به هدف‌گیری وب‌سایت‌های انتخاباتی و رسانه‌ها برای عملیات ادعایی نفوذ است.

اف‌بی‌آی مدعی است اولین بار اقدامات گروه مذکور را در سال ۲۰۲۲ شناسایی و درباره چند عملیات هک و افشای اطلاعات که به طور عمده با هدف ایجاد رسوایی برای سازمان‌ها، عمدتا در اسرائیل، انجام شده بود، گزارش عمومی منتشر کرد.

وزارت دادگستری ایالات متحده همچنین در سال ۲۰۲۱، دو نفر از اعضای این گروه را به دلیل نفوذ به چند وب‌سایت انتخاباتی در سال ۲۰۲۰، انتشار ویدئوهای جعلی تقلب در انتخابات برای اعضای حزب جمهوری‌خواه و ارسال ایمیل‌های تهدیدآمیز به رای‌دهندگان دموکرات با نام گروه «پسران مغرور» تحت تعقیب قرار داد.

اف‌بی‌آی اعلام کرد که همانند اقدامات این گروه در سال ۲۰۲۰، «کمپین‌های اخیر آنها نیز شامل ترکیبی از نفوذ به شبکه‌های رایانه‌ای و ادعاهای مبالغه‌آمیز یا ساختگی از دسترسی به شبکه‌های قربانیان یا داده‌های سرقت‌شده است که برای تقویت تاثیرات روانی عملیات آنها طراحی شده‌اند.»

مقامات اف‌بی‌آی همچنین مدعی است که موفق شده اطلاعاتی درباره روش‌های عملیاتی این شرکت از دیگر حوادث در فرانسه، سوئد و اسرائیل جمع‌آوری کنند. در یکی از عملیات‌ها، اف‌بی‌آی گزارش داد که این گروه از هوش مصنوعی مولد برای ساخت یک مجری خبری جعلی استفاده کرده است. علاوه بر این، شرکت مذکور از بهبوددهنده عکس با هوش مصنوعی، تغییر صدا و دیگر تولیدکنندگان تصاویر بهره می‌گیرد.

در همین رابطه، مقامات سوئدی چند اطلاعیه درباره انواع عملیات اطلاعاتی و نفوذ داده‌ها توسط این گروه منتشر کرده‌اند که ظاهرا در پاسخ به آن دسته از شهروندان سوئدی بوده که اقدام به سوزاندن قرآن کرده‌اند.

اف‌بی‌آی چند عملیات اخیر دیگر مانند نفوذ به شرکت پخش تلویزیونی اینترنتی آمریکا را به شرکت وابسته به گروه مذکور نسبت داده است. چند عملیات هکتیویستی دیگر توسط همین شرکت نیز از طریق اکانت‌های رسانه‌های اجتماعی با نام «دادگاه سایبری» تبلیغ می‌شود. اف‌بی‌آی اشاره کرد که چندین دامنه استفاده‌شده توسط این گروه برای مدیریت زیرساخت و پوشش‌دهی را توقیف کرده است.

### ● گروگان‌های اسرائیلی

مقامات آمریکایی نیز مدعی شدند اعضای این شرکت ایرانی با اعضای خانواده اسرائیلی‌هایی که از ۱۷ اکتبر ۲۰۲۳ توسط حماس در غزه گروگان گرفته شده‌اند، تماس برقرار کرده‌اند.

آنها تصاویری از پیامک‌های ارسالی این گروه به خانواده‌ها به اشتراک گذاشته‌اند که در آن گفته شده اسرائیل، پیشنهادهای آزادسازی گروگان‌ها را دریافت کرده اما این پیشنهادها، بارها رد شده است. هکرها از خانواده‌ها خواستند برای اطلاع از وضعیت گروگان‌ها، «در ارتباط باقی بمانند.»

از ۱۷ اکتبر ۲۰۲۳، چندین عملیات دیگر در اسرائیل، از جمله تلاش برای سرقت ویدئو از دوربین‌های آی‌پی در اسرائیل، از طریق این شرکت انجام شده است. گروه مذکور سعی کرده خلبانان جنگنده اسرائیلی، اپراتورهای پهپاد و سایر سربازان درگیر در حمله به غزه را از طریق وب‌سایت‌های شجره‌نامه و سایر منابع شناسایی کند.

در فوریه ۲۰۲۲، وزارت خارجه آمریکا، جایزه ۱۰ میلیون دلاری برای کسب اطلاعات درباره دو پیمانکار ایرانی که برای این شرکت ایرانی کار کرده‌اند و نیز چندین عملیات طراحی‌شده برای «ایجاد نفاق و تضعیف اعتماد رای‌دهندگان به فرایند انتخاباتی آمریکا» را به راه انداخته بودند، اعلام کرد.

پیش از این، وزارت خارجه نیز اعضای گروه مذکور را به دلیل اتهامات مربوط به حمله سایبری به کمپین دونالد ترامپ، رئیس جمهوری سابق ایالات متحده تحریم کرد.