یک فعال حوزه امنیت سایبری در گفت‌وگو با «فرهیختگان»:

رگولاتوری فیلترینگ در کشور شفاف نیست

مریم رضایی
خبرنگار

حمله واناکرای (WannaCry) در سال ۲۰۱۷ نمونه‌ای روشن از اهمیت به‌روزرسانی سیستم‌ها و تقویت زیرساخت‌های امنیتی در برابر تهدیدات سایبری است. این حمله از نوع باج‌افزار (Ransomware) و شیوه کار به این صورت بود که این باج‌افزار از یک آسیب‌پذیری در سیستم‌عامل ویندوز استفاده کرد که توسط آژانس امنیت ملی آمریکا (NSA) کشف و بعدها توسط گروه هکری Shadow Brokers افشا شد. این باج‌افزار پس از آلوده‌کردن سیستم‌ها، واناکرای فایل‌های قربانیان را رمزگذاری کرده و برای بازگرداندن دسترسی، درخواست پرداخت ۳۰۰ تا ۶۰۰ دلار می‌کرد. دامنه تأثیر این حمله گریبان بیش از ۱۵۰ کشور جهان را گرفت و شرکت‌هایی نظیر NHS (سرویس سلامت ملی انگلستان)، شرکت‌های مخابراتی در اسپانیا و کارخانه‌های بزرگ مانند رنو فرانسه نیز هدف قرار گرفتند و طی این حمله بیش از ۲۰۰ هزار کامپیوتر آلوده شد. از دیگر پیامدهای این حمله اختلال گسترده در بیمارستان‌ها در انگلستان بود به‌گونه‌ای که کادر درمان این بیمارستان مجبور به تعویق اعمال جراحی و غیرقابل‌دسترس شدن اطلاعات پزشکی بیماران شدند. متعاقب این حمله سایبری گسترده مایکروسافت به‌سرعت وصله امنیتی منتشر کرد، اما بسیاری از سازمان‌ها از سیستم‌های قدیمی و به‌روزرسانی نشده استفاده می‌کردند.

در دنیای دیجیتال امروز، امنیت سایبری به یکی از حیاتی‌ترین موضوعات جهانی تبدیل شده است. کشورها در تلاش‌اند با تقویت زیرساخت‌ها، قوانین و آموزش‌ها، از شهروندان و سازمان‌های خود در برابر حملات سایبری محافظت کنند. اما نگاهی به آمار و شاخص‌های بین‌المللی نشان می‌دهد تفاوت‌های چشمگیری در توانمندی‌های سایبری کشورها وجود دارد؛ از کشورهای پیشرو مانند ایالات متحده و عربستان سعودی که در صدر این رتبه‌بندی‌ها قرار دارند، تا کشورهای آسیب‌پذیری همچون تاجیکستان و نامیبیا که با چالش‌های جدی در این حوزه مواجهند.

گزارش‌های منتشر شده اخیر نشان می‌دهد کشور لهستان در شاخص ملی امنیت سایبری به دلیل آمادگی بالا در جلوگیری و مدیریت تهدیدات سایبری در رتبه اول قرار دارد و چین باوجود پیشرفت‌های فناوری، در «شاخص جهانی امنیت سایبری ITU» رتبه ۳۳ را دارد و همچنان با چالش‌های امنیتی مواجه است. همچنین کشور تاجیکستان در مواجهه با تهدیدات سایبری، به‌ویژه بدافزارها، آسیب‌پذیری بالایی دارد.

بر اساس گزارش شاخص جهانی امنیت سایبری (GCI) اتحادیه بین‌المللی مخابرات (ITU) در سال ۲۰۲۴، ایران در سطح ۳ (Establishing) قرار دارد که نشان‌دهنده مرحله‌ای از ایجاد تعهدات امنیت سایبری است.

این ارزیابی در پنج حوزه اصلی انجام شده است:

۱ **اقدامات قانونی (Legal Measures):** ایران امتیاز ۱۷/۷۹ از ۲۰ را کسب کرده که نشان‌دهنده وجود قوانین و مقررات قوی در زمینه امنیت سایبری است.

۲ **اقدامات فنی (Technical Measures):** با امتیاز ۱۴/۴۹ از ۲۰، ایران در ایجاد زیرساخت‌های فنی برای امنیت سایبری تلاش‌هایی انجام داده، اما همچنان نیاز به بهبود دارد.

۳ **اقدامات سازمانی (Organizational Measures):** امتیاز ۱۶/۷۲ از ۲۰ نشان می‌دهد ایران دارای سیاست‌ها و استراتژی‌های ملی مشخصی برای مدیریت امنیت سایبری است.

۴ **توسعه ظرفیت (Capacity Development Measures):** ایران در این حوزه امتیاز ۱۰/۲۷ از ۲۰ را کسب کرده که نشان‌دهنده نیاز به تلاش‌های بیشتری در زمینه آموزش و آگاهی‌بخشی برای توسعه ظرفیت امنیت سایبری است.

۵ **اقدامات همکاری (Cooperation Measures):** امتیاز ۶/۲۵ از ۲۰ نشان‌دهنده ضعف در همکاری‌ها و مشارکت‌های بین‌المللی و داخلی در زمینه امنیت سایبری است.

همیشه قربانی حملات تروریستی سایبری بوده‌ایم

در مقایسه با میانگین منطقه آسیا- اقیانوسیه، ایران در برخی حوزه‌ها عملکرد قابل‌قبولی دارد، اما در برخی دیگر مانند همکاری‌های بین‌المللی نیاز به بهبودهای بیشتری دارد.

محمدامین کریمان، بنیان‌گذار پلتفرم و استارتاپی به نام «راورو» و میانجی میان تخصص هکرهای کلاه‌سفید و متخصصان امنیت معتقد است که «ما در زمینه امنیت سایبری امنیت مطلق نداریم و باتوجه‌به گستردگی سامانه‌ها و جدید بودن تکنیک‌ها باعث شده که حفاظت از اطلاعات کاربران به یک کار پیچیده تبدیل شود و یکی از راه‌هایی که به سازمان‌ها در این زمینه کمک می‌کند، برگزاری رویدادهای «باگ بانتی» است تا خرد جمعی متخصصان در کنار هم قرار گیرد و هر کدام با یک نگاه و تخصص خود اقدام به ارزیابی سامانه‌ها کنند؛ اتفاقی که اگر در حالت عادی و یا پیمانکاری صورت گیرد چندین ماه زمان نیاز دارد تا این حجم از سامانه‌های سازمان‌ها را مورد بررسی قرار دهند؛ ولی در رویداد باگ بانتی در مدت کمتر، حجم زیادی از آسیب‌های سامانه‌ها شناسایی خواهد شد.»

«نرم‌افزارهای قدیمی و بدون به‌روزرسانی»، «آسیب‌پذیری‌های روز صفر (Zero-Day) یا نقص‌هایی که هنوز کشف یا برطرف نشده‌اند و هکرها پیش از شناسایی عمومی، از آن‌ها بهره‌برداری می‌کنند»، «رمزهای عبور ساده یا پیش‌فرض»، «حملات فیشینگ و مهندسی اجتماعی»، «آلودگی به بدافزارها» و ناآگاهی کارکنان، همگی در آسیب‌پذیرتر شدن سامانه‌ها و بازگذاشتن راه نفوذ حملات هکری مؤثرند.

کریمان امنیت سایبری را یک زنجیره می‌داند که سطح پایین امنیت یک سامانه، ضعیف‌ترین حلقه این زنجیره به شمار می‌رود، و این مثال را می‌زند که ما برای منزل مسکونی خود یک در ورودی ضدسرقت و محکم و یک گاوصندوق خیلی ایمنی تهیه می‌کنیم؛ ولی وقتی پنجره‌ها حفاظ نداشته باشد، این نقطه، حلقه نخست آسیب‌پذیرشدن خانه ما خواهد بود.

وی چنین ادامه می‌دهد: «ایران همیشه قربانی حملات سایبری بوده و کشور ما جزو اولین کشورهایی است که به‌عنوان قربانی حملات تروریستی سایبری بوده است. حمله استاکس‌نت که سازمان انرژی هسته‌ای کشور را هدف قرار داد، جزو اولین جنگ‌های سایبری بود که در کشور اتفاق افتاد. هک سازمان صداوسیما، وزارت راه، شهرداری تهران و افشای اطلاعات بسیاری از بانک‌ها از جمله نمونه‌های حملات سایبری است که شاهد آن بوده‌ایم.»

سال ۲۰۱۰ نقطه عطف امنیت سایبری ایران

یکی از نقاط عطف تاریخی در موضوع امنیت سایبری، حمله استاکس‌نت (Stuxnet) در سال ۲۰۱۰ است که به‌عنوان اولین سلاح سایبری شناخته می‌شود و تأثیرات عمیقی بر امنیت سایبری جهانی داشت. ویروس استاکس‌نت یک بدافزار پیچیده بود که به طور خاص برای حمله به سیستم‌های صنعتی طراحی شده بود. این بدافزار به زیرساخت‌های حیاتی، به‌ویژه در بخش انرژی و تأسیسات هسته‌ای، نفوذ می‌کرد.

هدف اصلی این حمله، تأسیسات غنی‌سازی اورانیوم در نیروگاه نطنز ایران بود و توانست به دستگاه‌های سانتریفیوژ این مرکز آسیب برساند و فرایند غنی‌سازی اورانیوم را مختل کند.

این بدافزار از طریق یک حافظه فلش USB آلوده وارد سیستم‌های ایزوله شد و از آسیب‌پذیری‌های سیستم‌عامل ویندوز و نرم‌افزارهای صنعتی زیمنس (Siemens) بهره‌برداری کرد. استاکس‌نت به‌گونه‌ای طراحی شده بود که بدون جلب‌توجه، عملیات را مختل کند. این بدافزار به‌جای نابودی فوری تجهیزات، باعث تغییرات جزئی اما مداوم در عملکرد دستگاه‌ها می‌شد تا شناسایی آن دشوار شود.

این حمله هر چند ضعف‌های جدی در زیرساخت‌های سایبری و صنعتی کشورهای مختلف را آشکار کرد؛ ولی کشورها سرمایه‌گذاری‌های عظیمی در تقویت امنیت سایبری خود انجام دادند، همچنین این حمله، مفهوم جنگ سایبری را به‌عنوان یک ابزار قدرت‌نمایی جدید مطرح کرد. استاکس‌نت، به‌صورت ناخواسته در اینترنت گسترش یافت و به سیستم‌های غیرمرتبط در کشورهای دیگر نیز آسیب رساند و این موضوع نشان داد که جنگ سایبری می‌تواند پیامدهای غیرقابل‌پیش‌بینی داشته باشد.

این فعال حوزه امنیت سایبری، این حوزه را یک پدیده جدید در دنیا توصیف می‌کند که عمر آن به ۲۰ سال نمی‌رسد و در ایران از یک دهه این موضوعات پررنگ و پررنگ‌تر شد و از سال ۱۴۰۰ حتی مردم عادی نیز با آن درگیر شدند.

وی می‌گوید: «تا قبل از این سال (۱۴۰۰) امنیت سایبری در لایه‌ای بود که تنها متخصصان با آن درگیر بودند؛ چون در آن زمان زیرساخت‌های اینترنتی به اندازه اکنونی، فراگیر نبود و کاربران نیز به این میزان از فضای سایبری استفاده نمی‌کردند؛ ولی در سال‌های اخیر این مسئله با زندگی روزمره مردم عجین شده و زندگی مردم با «هویت و زندگی دیجیتال» توأمان شد و از این طریق رخنه یا اتفاقات سایبری، مردم عادی را نیز تحت تأثیر قرار داد.»

با توسعه زیرساخت‌های اینترنتی حالا ضریب گسترش اینترنت روزبه‌روز در حال افزایش است و ما از دنیای پول‌های کاغذی به ارز دیجیتال و از دنیای تاکسی‌های تلفنی به سرویس‌های اینترنتی رسیده‌ایم و خرید ما از بقالی‌ها به فروشگاه‌های نسل جدید شیفت یافته و رستوران‌های آنلاین، جای آشپزخانه‌های ما را گرفته و صف‌های طولانی در بانک جای خود را به نرم‌افزارهای موبایلی داده و این دامنه مجازی با ظهور هوش مصنوعی روزبه‌روز درحال‌توسعه است و در مقابل نوع تهدیداتی که ما را تهدید می‌کند، متفاوت شده است.

ترورهای امنیت سایبری

در سال ۲۰۱۹، گروهی از هکرها سیستم‌های بیمارستانی در آلمان را هدف قرار دادند و باعث شدند یکی از بیماران به دلیل عدم دسترسی به خدمات درمانی فوت کند. این حمله به‌عنوان اولین مورد مرگ مستقیم ناشی از حملات سایبری ثبت شد.

به گفته مدیر این استارتاپ «ما اکنون در فضای دیجیتال، در کنار هویت شخصی‌مان، هویت مجازی یافته‌ایم که شامل آدرس، لوکیشن موبایل‌ها، لیست خرید اینترنتی، مبدأ و مقصد تاکسی‌های اینترنتی، قبوض برق و... می‌شود. از طریق این هویت مجازی به‌راحتی می‌توان فهمید که فرد از کدام سرویس جانبی بهره می‌برد، چه محتواهایی گوش می‌دهد، چه خریدهایی داشته، چه غذایی را سفارش داده است. این هویت مجازی شاید به‌تنهایی معنا نداشته باشد؛ ولی وقتی در اطلاعات جمعی افراد در کنار هم قرار گیرند برای سرویس‌های اطلاعاتی که به‌دنبال داده هستند، معنادار می‌شود و با دنبال‌کردن و در کنار هم قراردادن این داده‌ها، قطعات پازل خود را تکمیل می‌کنند.»

این حملات تنها مربوط به ایران نمی‌شود؛ بلکه همه کشورهای دنیا با آن مواجهند. کریمان در این باره گفت: «بین دو کشور روسیه و آمریکا جنگ‌های سایبری زیادی رخ داد و در نهایت منجر به این شد که مصوبه‌ای به تصویب برسد که بر اساس آن اگر جنگ سایبری رخ دهد، کشورها در پاسخ به آن می‌توانند حمله اتمی به کشور آغازگر جنگ سایبری، صورت دهند. این مصوبه، اهمیت حملات سایبری را نشان می‌دهد به‌گونه‌ای که پاسخ به آن حمله اتمی است.»

فیلترینگ و نفوذ سهل به اطلاعات

فیلترشکن‌ها (VPN)ها و پروکسی‌ها ابزارهایی‌اند که برای عبور از محدودیت‌های اینترنت و حفظ حریم خصوصی کاربران طراحی شده‌اند؛ ولی هکرها از فیلترشکن‌ها برای پنهان‌کردن هویت خود استفاده می‌کنند و به آن‌ها اجازه می‌دهد با تغییر مکان جغرافیایی و آدرس IP، ردیابی فعالیت‌های مخرب خود را برای سازمان‌های امنیتی دشوارتر کنند.

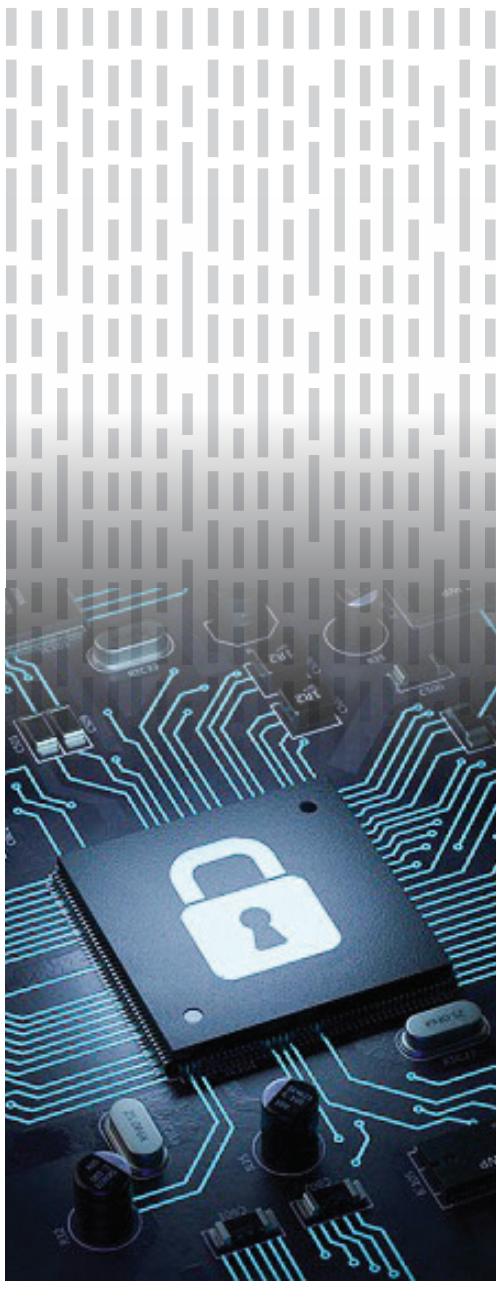
مهاجمان می‌توانند از فیلترشکن‌ها برای اجرای حملات سایبری از نقاط مختلف جهان استفاده کنند و ردپای خود را پاک کنند و همچنین به هکرها کمک می‌کنند تا به بازارهای غیرقانونی در وب تاریک (Dark Web) دسترسی پیدا کرده و ابزارها یا اطلاعات موردنیاز برای حملات را تهیه کنند. از این بدتر فیلترشکن‌های رایگان و غیرمعتبر است که به هکرها اجازه می‌دهد تا داده‌های کاربران را به سرقت ببرند. این ابزارها ممکن است بدافزار یا ابزارهای جاسوسی را به همراه داشته باشند و خود به ابزاری برای حملات سایبری تبدیل شوند.

هکرها از فیلترشکن‌ها برای عبور از دیوارهای آتش (Firewall) و محدودیت‌های امنیتی سازمان‌ها استفاده می‌کنند تا به سیستم‌ها نفوذ کنند.

کریمان با بیان اینکه ما به‌عنوان کاربر ایرانی دسترسی به بسیاری از سرویس‌های بین‌المللی را نداریم، مشکل اصلی کشور در دوران فیلترینگ را شفاف نبودن رگولاتوری فیلترینگ عنوان کرد و این‌گونه برای ما توضیح می‌دهد: «بسیاری از کشورها محتواهای جنسی و غیر اخلاقی و مواد مخدر را حذف می‌کنند و این یک فرایند قانونی است و ما نیز مشکلی با این نوع فیلترینگ نداریم، بلکه مشکلی از جایی آغاز می‌شود که رگولاتوری فیلترینگ در کشور شفاف نیست، اختلالی که در شبکه اینترنت ایجاد می‌شود به‌هیچ‌وجه شفاف نیست و این موردی است که موجب نارضایتی میان متخصصان و مردم شده است. اینکه یک سایت کاملاً تخصصی به دلیل وجود یک کلمه اشتباهی که یک کاربر ثبت کرده، از دسترس خارج می‌شود، اسمش دیگر فیلترینگ نیست؛ بلکه بیشتر به اذیت و آزار شبیه است و این هم از این رویکرد ناشی می‌شود که سازوکارها شفاف نشده است.»

وی توسعه بی‌رویه فیلترشکن در کشور را به خانه‌ای تشبیه می‌کند که درهای ورودی آن بسته شده ولی پنجره آن باز است و احتمالاً نردبانی از پنجره به کوچه گذاشته شده تا مسیر دسترسی هموارتر شود و اضافه می‌کند: «درست که در ورودی خانه قفل مطمئنی دارد؛ ولی نردبانی که گذاشته شده مخاطرات به‌شدت بیشتری در پی دارد و این همان کاری است که ما با توسعه فیلترشکن انجام می‌دهیم. همه نرم‌افزارهای فیلترشکن فاقد مرجع و منبع قانونی‌اند که از سوی گروه‌های مختلف با نیت‌های مختلف توسعه داده شده‌اند و کاربر عادی درحالی‌که ماهانه آن را شارژ می‌کند، نمی‌تواند تشخیص دهد که توسعه‌دهنده آن چه نیتی دارند.»

این فعال حوزه امنیت سایبری تأکید می‌کند این امر باعث می‌شود که علاوه بر تحمیل هزینه زیاد بابت مصرف دیتا برای مصرف‌کنندگان، اجازه می‌دهند گروهی، با داده‌های موجود در موبایل‌هایشان هر کاری انجام دهند و بدتر از آن این است که کلیه جریان داده کشور در ابتدا به سرویس وی‌پی‌ان وارد و تحلیل می‌شود و بعد بر می‌گردد که این یک فاجعه است؛ چراکه برای آنکه به فکر امنیت باشیم، یک‌سری تونل‌هایی را ایجاد کردیم که ترافیک کشور به یک‌سری سرورهای ناشناس هدایت می‌شوند و انتظار داریم امنیت سایبری در کشور شکل بگیرد، درحالی‌که بخشی از نشت اطلاعات از همین ابزارها بوده و ممکن است هر کدام از این ابزارها، ابزارهای جاسوسی و یا تروجان و یا ابزارهای سرقت اطلاعات باشند.



دوشنبه اول بهمن ۱۴۰۳
شماره ۴۳۳۴
FARHIKHTEGANDAILY.COM
FARHIKHTEGANONLINE

روایت یکی از چهره‌های اثرگذار حوزه نوآوری از روی کارآمدن ترامپ به کمک تیم تِک

از پروژه منهتن ۲ چه می‌دانید؟

کامران باقری
مدیرعامل مرکز نوآوری اسمایلینو

درباره هوش مصنوعی خبر زیاد است. اینکه می‌تواند فیلم و ویدئو تولید کند. سرعت آن بسیار بالا است؛ از ظرفیت پردازشگران چند ده میلیارد دلاری استفاده می‌کند؛ OpenAI برای مدل جدیدش، ۳۰۰ میلیارد دلار سرمایه‌گذاری خواهد کرد. اینکه مهم‌ترین روند فناوری و سرمایه‌گذاری در دنیاست. خطرات اخلاقی و نیاز به حکمرانی دارد. موج شدید بیکاری به همراه خواهد آورد و موازنه ثروت در کسب‌وکار دنیا را هم به‌شدت جابه‌جا می‌کند. اما من نمی‌خواهم در مورد این موارد صحبت کنم؛ می‌خواهم در مورد تغییر بنیادین در حوزه مدیریت نوآوری و تکنولوژی صحبت کنم و برای اینکه بیشتر به آن فکر کنیم.

تابه‌حال در رشته مدیریت نوآوری و تکنولوژی، همیشه و در تمام کتب و جزوات درسی که مطالعه می‌کردیم و درس می‌دادیم، دغدغه داشتیم که سرعت توسعه تکنولوژی را افزایش دهیم. برای اولین‌بار در دنیا، مهار و کم‌کردن این سرعت به یک دغدغه بزرگ تبدیل شده است. قانون‌گذار، شرکت‌ها و دولت‌ها هر کدام به دنبال شناخت نقش خود هستند و می‌گویند اگر می‌شود سرعت آن را کم کنید. این موضوع در حال تبدیل‌شدن به یک ادبیات است. کتاب‌هایی در یکی، دوسال اخیر به نگارش درآمده که چه کنیم این سرعت کم شود. نوآوری باز جریان غالب در دنیا بود؛ اما به نظر می‌رسد، اتفاقاتی در حال افتادن است که به سمت بسته عمل‌کردن پیش می‌رویم که اتفاق بزرگی است. به نظر می‌آید در پارادایم هوش مصنوعی تعدادی بازیکن بزرگ خواهیم داشت که می‌خواهند بسته بازی کنند و کسی را راه ندهند. بازی‌شان هم خیلی بزرگ است.

فناوری انسان‌محور، دغدغه جدی رشته ما بوده است؛ اما الان فناوری هم‌زیستی انسان با ماشین در حال تبدیل‌شدن به یک ادبیات جدی در دنیاست. مالکیت فکری یکی از حوزه‌های مهم در فضای تکنولوژی و نوآوری بوده است؛ اما به نظر می‌آید مدل‌های هوش مصنوعی بازی مالکیت فکری را به شکل جدی و رادیکال تغییر می‌دهد و بازی به سمت مالکیت مدل‌های هوش مصنوعی پیش می‌رود. هرکدام از این موارد، تغییر پارادایم جدی در رشته ماست که باید استادان و دانشجویان این رشته به شکل جدی‌تری به آن بپردازند.

می‌خواهم توجه شما را به یک نکته جلب کنم. ما در رشته مدیریت فناوری با فناوری در ارتباط بودیم و دغدغه ما فناوری بود. اما این (هوش مصنوعی) یک عنصر فناوری‌ساز است که تفاوت بنیادینی محسوب می‌شود، به‌زودی ادبیات خود را وارد رشته ما خواهد کرد و می‌تواند موضوع تحقیق بسیار جدی برای پژوهشگران این حوزه باشد.

می‌خواهم وقت بیشتری را به یکی از اتفاقات بنیادین در دنیا اختصاص دهم که نام آن را «تاج‌گذاری تِک» گذاشته‌ام. اتفاق بزرگی که لابه‌لای بقیه خبرها گم شده است. به طور ساده، به نظر می‌آید برای اولین‌بار در تاریخ، دولت جدید آمریکا دست‌نشانده یک تیم تِک است. در دولت اول ترامپ، او برای به‌قدرت‌رسیدن از فیس‌بوک و کمبریج آنالیتیکا کمک گرفته؛ ولی در این دولت برعکس است و ایشان دست‌نشانده یک تیم تِک است و تمام اخبار در دو سه ماه اخیر، حرف بنده را تأیید می‌کند. اگر این گزاره را بپذیریم، این موضوع یک تغییر عجیب در دنیا ایجاد خواهد کرد که باید دوستان رشته ما باید بیشتر به این موضوع فکر کنند. اسم این پروژه را خودشان پروژه «منهتن ۲» گذاشتند. پروژه «منهتن ۱» تولید بمب اتم بود که باعث شد آمریکا خود را از بقیه کشورها جدا کند. این پروژه را «منهتن ۲» اسم گذاشتند و می‌توانید تصور کنید که منظورشان چیست. اینکه دیدگاه استارتاپی و تِک را در یک دولت اجرا کنید. البته ایلان ماسک فقط یکی از چهره‌های این پروژه است. چهره‌های مشهورتری هم هستند. پیتر تیل، نام اساسی‌تری در این بازی است. اگر دقت کنید، الان دیگر همه نگران شدند. در خبرهای منتشر شده در روزهای گذشته، اروپایی‌ها مانند آلمان، انگلیس و ایتالیا از دخالت بیش از حد این تیم در سیاست اروپا شاکی شدند. این اتفاق بسیار بزرگی است. جیمز دیوید وَنْس معاون اول ترامپ را همین تیم معرفی کرده است. کسی که دانشجو و زیر دست پیتر تیل بزرگ شده و با حمایت شخصی ایشان به سنا رفت و حالا معاون اول است. فردی که در رأس AI در دولت آمریکا گذاشتند نیز با همین تیم است. این جریان پدیده‌های عجیبی در پی خواهد داشت. احتمالاً شاهد چابکی و سرعت بالا در تصمیم‌گیری باشیم. دولت‌ها در سرتاسر دنیا سرعت کند و الگوی مشابهی در تصمیم‌گیری دارند که احتمالاً (حضور تیم تک) روند را تغییر خواهد داد و سرعت زیادی را در این زمینه خواهیم دید. دیپلماسی مبتنی بر فناوری، خیلی پررنگ‌تر خواهد شد. سنت سیاست‌ورزی در کشور کنار گذاشته می‌شود و این عمل دنیا را گیج‌وگنگ خواهد کرد.

رگولاتور باید با شرکت تِک چگونه برخورد کند؟ این دو با هم دچار اختلاط می‌شوند و این مسئله تبعات جدی را در پی خواهد داشت. کسانی که اهدافشان در حد رفتن به کره مریخ است، احتمالاً در حوزه سیاست هم اهداف جاه‌طلبانه‌ای را در کوتاه‌مدت دنبال می‌کنند. آخرین مورد که به نظرم از همه مهم‌تر است، آنها به خرید کشور و اداره مستقیم و بی‌واسطه کشورها فکر می‌کنند. احتمالاً آمریکایی‌ها این رودربایستی را در جاهایی کنار خواهند گذاشت. نمی‌دانم صحبت‌های اخیر ترامپ را می‌شنوید که «کانادا باید جزئی از آمریکا باشد» و «کانال پاناما باید برای ما باشد» یا نام خلیج مکزیک به خلیج آمریکا تغییر کرد، معنی‌دار است. آنها به‌زودی احتمالاً بخواهند بدون رودربایستی کنترل کشورها را به دست بگیرند. این پدیده برای اولین‌بار نیست که در دنیا رخ می‌دهد؛ کمپانی هند شرقی زمانی نصف دنیا را اداره می‌کرد. ثروت آن از ثروت دولت انگلیس بیشتر بود. مصطفی سلیمان، CEO واحد هوش مصنوعی مایکروسافت، پیش‌بینی می‌کند که ما به سمت چنین دوره‌ای بر می‌گردیم. اما در کشور ایران باید چه کنیم؟ به نظرم اولاً خطر جاماندن ابدی داریم. حوزه AI یک شیفت تمدنی است. نیاز به اهل فلسفه و علوم‌انسانی داریم. باید یک عمل‌گرایی خیلی افراطی داشته باشیم. سیستم‌های تصمیم‌گیری ما حتی در بخش خصوصی خیلی کند شد است، ولی اینجا یک عمل‌گرایی جدی را می‌طلبد. به عبارت دقیق‌تر یک نهضت سوادآموزی هوش مصنوعی می‌خواهیم و جمعیت کشور باید سوادآموزی جدید داشته باشند تا با حوزه AI به‌راحتی خو بگیرند. در فضای جدید شرکت‌های خصوصی باید خط مقدم باشند؛ چراکه سرعت بالا بوده و بازیکنان در آنجا هستند. اشتباه است اگر دولت خود را جلو بگذارد؛ حتماً عقب می‌افتیم. این بازی چون بازی بزرگی است و عددهای بزرگی دارد، فکر می‌کنم ادامه شرایط تحریم کار ما را سخت می‌کند. باید در این بازی حضور داشته باشیم و بازیکن فعالی باشیم. در داخل هم باید روی بازیگران بزرگ حساب کرد؛ این بازی استارتاپی نیست و باید آنها را خیلی سریع‌تر زیر سایه شرکت‌های بزرگ تک‌مان ارتباط دهیم.

پی‌نوشت

متن حاضر ارائه کامران باقری، مدیرعامل مرکز نوآوری اسمایلینو در افتتاحیه هجدهمین کنفرانس ملی و چهاردهمین کنفرانس بین‌المللی مدیریت فناوری و نوآوری است که «فرهیختگان» در قالب یادداشت شفاهی مشروح آن را منتشر می‌کند.