گزارش
مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

اردیبهشت ۱۴۰۱

امنیت سایبـــــری


بسم الله الرحمن الرحیم

فهرست

Iranian Council For
Defending The Truth

پیشگفتار

۱

پیشگفتار

مجمع ایرانی دفاع از حقیقت مادام همه تلاش خود را انجام می‌دهد که با به کارگیری شبکه‌ای از نخبگان در حوزه‌های مختلف سیاسی و شناختی گامی در جهت جلوگیری از ایجاد سوءتفاهم بردارد. در همین خصوص ما در مجمع ایرانی دفاع از حقیقت رسالت خود میدانیم تا با تهیه دیدبان‌هایی از موضوعاتی که به عنوان کارویژه برای خود انتخاب کرده‌ایم، چشم اندازی از مسیر را ارائه داده و در صورت توان پیشنهاداتی نیز برای کاهش این سوءتفاهم‌ها در آنان جای دهیم. ناگفته نماد که این دیدبان خود بخشی از راه حل کاهش سوءتفاهم است.

مجمع ایرانی دفاع از حقیقت
میز مطالعات امنیت

Iranian Council For
Defending The Truth

مقدمه

۲

مقدمه

اطـلاع از اخبـار و وضعیـت فضـای سـایبر در ایـالات متحـده ایـن امـکان را فراهـم می‌سـازد تـا بـا مسـائل و مشـکلات ایـن حـوزه سـریع‌تر آشـنا شـده و هم‌چنیـن پیـش از ایـن کـه کشـور مـا نیـز بـه آن مصائـب و دشـواری‌ها دچـار گـردد، راهکارهـای اصلاحـی را پیش‌بینـی نماییـم. از طرفـی، بـا توجـه بـه ایـن کـه در اظهـارات عمومـی و جلسـات رسـمی مقامـات ایـن کشـور برخـی از نقـاط ضعـف دشـمن در زمینـه سـایبری و فناوری‌هـای نویـن بیـان می‌گـردد و بـا توجـه بـه ایـن نکتـه کـه بخـش سـایبری ایـران توانایـی آن را دارد کـه در تقابـل بـا ایـالات متحـده از همیـن ضعف‌هـا بهره‌بـرداری کنـد و بـه دشـمن ضربـه بزنـد؛ فلـذا می‌توانیـم از نقـاط ضعـف حریـف اسـتفاده نماییـم و زمیـن بـازی را بـه نفـع خـود تغییـر دهیـم و در موضـع آفنـدی قـرار بگیریـم.

ایـن تذکـر ضـروری اسـت کـه بـا توجـه بـه پیشـگامی کشـور امریـکا در عرصـه تکنولـوژی، بررسـی پیشـرفت‌ها و برنامه‌ریزی‌هـای کلان ایـن کشـور در زمینـه فنـاوری پیش‌بینـی مقصـد نهایـی مسـیر تکنولـوژی در آینـده را ممکـن می‌سـازد.

در بولتنـی کـه در اختیـار داریـد اهـم اخبـار و اتفاقـات کلان حـوزه سـایبر، تکنولـوژی و فناوری‌هـای نویـن جمـع‌آوری شـده اسـت تـا مخاطبیـن و فعالیـن در ایـن زمینـه بتواننـد نسـبت بـه وضعیـت ایـالات متحـده از نگاهـی جامـع، کلان و بـه‌روز برخـوردار شـوند.

تحلیل و بررسی سایبری

بـه نظـر مـی رسـد طـی هفتـه هـای گذشـته چالـش هـای سـایبری ایـالات متحـده در ارتبـاط بـا حفاظـت زیرسـاخت هـای اساسـی خـود از خطـرات مختلـف سـایبری افزایـش یافتـه اسـت. آینـد تقابـلات میـان قـدرت هـای شـرقی و غربـی در عرصـه سـایبری نشـان‌دهنده ایـن مهـم اسـت کـه در سـنوات اخیـر رویارویـی ایـن دو مدعـی جهانـی بـه عرصـه سـایبری کشـیده شـده و هـر یـک از طرفیـن تمـام تـلاش خـود را مـی کننـد تـا حداکثـر تاثیـر گـذاری را در ایـن حـوزه داشـته باشـند. اگرچـه دولـت آمریـکا ادعـای داشـتن دسـت برتـر در عرصـه حملـه و دفـاع سـایبری را دارد امـا بـا توجـه بـه اتفاقـات اخیـر بـه نظـر مـی رسـد بیـش از پیـش در موضـع دفـاع قـرار گرفتـه و حداکثـر هـدف خـود را معطـوف بـه کنتـرل حمـلات صورت‌گرفتـه از سـمت رقبـای شـرقی خـود از جملـه روسـیه، چیـن و کـره شـمالی معطـوف کـرده اسـت. در آخریـن اقدامـات آمریـکا علیـه رقیـب مهـم شـرقی خـود یعنـی دولـت چیـن وزارت خارجـه آمریـکا دولـت چیـن را بـه تقویـت انتشـار اطلاعـات نادرسـت از سـوی ایـن دولـت بـرای حمایـت از روسـیه متهـم کـرده اسـت و یـا در اقدامـی دیگـر وزارت خزانـه داری ایـالات متحـده دسـت بـه تحریـم شـرکت هـای ارز دیجیتالـی زد کـه عملیـات پولشـویی را بـرای گـروه هـای هکـری روسـی و کـره شـمالی انجـام میدادنـد. هنـوز تخمیـن مشـخصی از ابعـاد آسـیب حمـلات بـه بـار آمـده از سـوی مهاجمـان شـرقی علیـه اهـداف سـایبری در غـرب و ایـالات متحـده در دسـت نیسـت امـا آنطـور

که به نظر می رسد وجود انگیزه ای تمام نشدنی برای مهاجمان شرقی در این رویارویی سایبری است. آنچه که مسلم است این است که ایالات متحده تاکنون به هیچ وجه نتوانسته خطر حملات سایبری را به طور کامل از این دولت برطرف کند و کماکان در جستجوی راه حل های بهتر برای بهبود امنیت سایبری خود بوده است.

در سوی دیگر دنیای امنیت سایبر در طی روزهای گذشته گزارش های مختلفی از هدف قرار دادن اهداف توسط باج افزارها و بد افزار های مختلف هکری به گوش رسید از جمله اینکه برخی از فعالان سیاسی در اسپانیا مورد حملات هکرها قرار گرفته اند و یا اینکه نخست وزیر اسپانیا توسط پگاسوس هک شد. نکته قابل تامل و توجه در این حملات آن است که هرچه به پیش میرویم سطح حملات از شهروندان عادی و نیز انگیزه های سطح پایین مانند اخاذی و کلاهبرداری های مالی در حملات سایبری به سمت هدف قرار دادن اشخاص مهم در بالاترین سطوح سیاسی رسیده است و آن هم با پیچیده ترین و قدرتمند ترین روش های هکری که می تواند دسترسی به مهمترین و حساس ترین اطلاعات اهداف را برای مهاجم به ارمغان آورد. نکته قابل توجه در این مورد این است که اگر وضع قدرت گرفتن شیوه های هکری به همین منوال پیش برود حوزه امنیت سایبر با خطرات فراتر از تصور روبه‌رو خواهد بود. به نظر می رسد نیاز به یک اجماع جهانی برای تعریف هنجار های امنیتی برای حفظ امنیت سایبری در سطح بین الملل از پایین ترین سطوح تا بالاترین سطوح جامعه است. به نظر کارشناسان شاید تشکیل یک سازمان جهانی مانند سازمان ملل متحد که وظیفه ایفای نقش در امنیت نظامی کشورها را در دستور کار دارد در عرصه سایبری نیز مورد نیاز باشد. در غیر این صورت دچار یک افسارگسیختگی غیر قابل کنترل در این فضا خواهیم شد.

اما در مورد درگیری های روسیه و اوکراین در عرصه سایبری نیز در روزهای گذشته اخباری به گوش رسید ولی به نظر می رسد حجم و عمق تنش های سایبری بین دو جبهه نسبت به ابتدای شروع درگیری کاهش محسوس یافته است. این مسئله شاید از این نکته ناشی شود که طرفین ابتکار عمل خاصی برای طراحی نقشه های هدف و استراتژی های حملات سایبری مستمر و معنادار علیه یکدیگر از پیش از شروع جنگ طراحی نکرده و صرفاً در ابتدای درگیری تعدادی محدود از استراتژی هایی که به نظر هر یک از طرفین تاثیر گذار تر بود را پیاده سازی کردند. ولی با گذشت جنگ شدت و گستردگی حملات مانند ابتدای آن ادامه نیافته است. در این خصوص اما هنوز برای قضاوت زود است و باید باز در ادامه شاهد باشیم که چه سرنوشتی برای درگیری های سایبری روسیه و اوکراین به وجود خواهد آ مد .

در دنیای تکنولوژی سایبری طی روزهای گذشته سامسونگ توسعه شبکه ۶G را با سرعتی حدود ۵۰ برابر بیشتر از ۵G اعلام کرد پیش از این نیز شاهد عرض اندام شرکت های شرقی از جمله هواوی در عرصه تکنولوژی های پیشرو در زمینه شبکه های ارتباطی بوده ایم. اکنون نیز شرکت کره‌ای سامسونگ دست برتر را در توسعه فناوری ۶G داشته است. اینطور به نظر می رسد شرکت های آسیایی و غیرغربی تمام تلاش و انگیزه خود را معطوف کرده اند تا نسل آینده و نوین شبکه های ارتباطی را به طور کامل از حریف غربی خود به دست بگیرند. در همین ارتباط کارشناسان معتقدند قدرتمندترین شرکت های آینده تکنولوژی شرکتهای خواهند بود که بیشترین سرمایه گذاری ها را در عرصه شبکه‌های ارتباطی به خود اختصاص داده باشند.

Iranian Council For
Defending The Truth

اخبار

۳

ایالات متحده آمریکا

وزارت خزانه‌داری یک میکسر ارزهای دیجیتال را برای اولین‌بار تحریم کرد

شرکت تحریم شده به نام Blender، مالکیت ارزهای دیجیتال را بوسیله ی ادغام دارایی‌های دیجیتال با هم پنهان می‌کند. وزارت خزانه‌داری گفت که گروه‌های باج‌افزار روسی و هکرهای کره شمالی از این سرویس برای پول‌شویی درآمدهای حاصل از حملات سایبری خود استفاده کرده‌اند. بلندر به درخواست اظهار نظر پاسخ نداد. این اقدام در حالی صورت می‌گیرد که دولت ایالات متحده تلاش می‌کند تا ۶۰۰ میلیون دلار ارز دیجیتالی را که توسط هکرهای کره شمالی از یک بازی ویدئویی در ماه مارس به سرقت رفته بود، بدست آورد. هکرها در آن مورد از میکسر دیگری به نام Tornado Cash برای شستشوی برخی از ارزهای دیجیتال هک شده استفاده کردند. در ماه آوریل، دولت ایالات متحده گروه لازاروس را مسئول این هک دانست. مقامات گفتند که باند هکر کره شمالی همچنین مسئول هک کردن Sony Pictures Entertainment در سال ۲۰۱۴ بود.

وزارت خارجه آمریکا دولت چین را به تقویت انتشار اطلاعات نادرست مرتبط با روسیه متهم کرد

وزارت امور خارجه آمریکا در یادداشتی که روز سه‌شنبه منتشر شد، دولت چین را به تقویت اطلاعات نادرست روسیه در مورد اوکراین متهم کرد. در این یادداشت توضیح داده شده است که چگونه دیپلمات‌های چینی برای گسترش تبلیغات کرملین به سایر کشورها و سانسور گزارش خشونت‌های روسیه کار می‌کنند، درحالی‌که هم‌زمان ایالات متحده و ناتو را مسئول این جنگ می‌دانند. مقامات دولت چین ادعای رئیس‌جمهور ولادیمیر پوتین مبنی بر اینکه روسیه در حال مبارزه با نازی‌ها در اوکراین در پلتفرم‌هایی مانند توییتر است، تبلیغ کرده و عکس‌هایی را به‌عنوان مدرک ارائه کرده‌اند. علاوه بر این، رسانه‌های دولتی و مقامات چین تئوری توطئه روسیه مبنی بر حمایت ایالات متحده از آزمایشگاه‌های تسلیحات بیولوژیکی در اوکراین را تکرار کرده‌اند. به نظر می رسد علی‌رغم ادعای بی‌طرفی چین، کار این کشور برای ترویج تبلیغات روسیه نشان‌دهنده حمایت پکن از مسکو است.

لیندل پس از ممنوعیت انتشار اطلاعات نادرست انتخاباتی، برای مدت کوتاهی به توییتر بازگشت

مایک لیندل، مدیرعامل My Pillow که سال گذشته برای همیشه از توییتر محروم شد، یک حساب کاربری جدید ایجاد کرد که قبل از مسدودشدن مجدد توسط توییتر، چندین ساعت آنلاین بود. لیندل یکی از بزرگ‌ترین مروجین ادعاهای بی‌اساس مبنی بر تقلب در انتخابات ۲۰۲۰ بوده است و او مرتباً قبل از مسدود شدن، چنین ادعاهایی را توییت می‌کرد. درحالی‌که حساب تأیید نشده جدید او برای مدت کوتاهی آنلاین بود، او ویدئویی را منتشر کرد و از مردم خواست که او را دنبال کنند و مراقب حساب‌هایی باشند که ادعا می‌کنند او هستند اما مرتبط به او نیستند.

قوانین توییتر افراد را از ایجاد حساب‌های جدید پس از مسدود شدن حساب‌های موجود خود منع می‌کند. رخ دادن این اتفاق در بحبوحه گمانه‌زنی‌های گسترده است مبنی بر اینکه ایلان ماسک در حال خرید توییتر به قیمت ۴۴ میلیارد دلار است،و ممکن است قوانین اطلاعات نادرست را کاهش دهد. قوانینی که منجر به مسدودی‌های لیندل و رئیس‌جمهور سابق دونالد ترامپ شد.

دولت ایالات متحده برای اطلاعات در مورد باج‌افزار Conti جایزه ۱۵ میلیون دلاری تعیین کرد

نـد پرایـس، سـخنگوی وزارت امـور خارجـه گفـت، تعییـن جایـزه ۱۵ میلیـون دلاری بخشـی از تـلاش گسـترده‌تر بـرای حملـه بـه بانـد بدنامـی اسـت کـه مسـئول پرهزینه‌تریـن نـوع باج‌افـزاری اسـت کـه تاکنـون سـاخته شـده اسـت. باج‌افـزار ایـن گـروه، سیسـتم مراقبت‌هـای بهداشـتی ایرلنـد و دولـت کاسـتاریکا را هـدف قـرار داده اسـت.

وزارت امـور خارجـه جوایـز مشـابهی را بـرای اطلاعـات در مـورد دو بانـد باج‌افـزار دیگـر از طریـق برنامـه پـاداش جرایـم فراملـی خـود در نظـر گرفتـه اسـت. گـروه هـای DarkSide و Sodinokibi، کـه همچنیـن به‌عنـوان REvil شـناخته می‌شـوند - مسـئول یک‌رشـته هـک گسـترده بودنـد. REvil بزرگ‌تریـن تأمین‌کننـده گوشـت در جهـان، JBS Foods، و Ka-seya، یـک شـرکت فنـاوری اطلاعـات را هـک کـرد.

وزارت امـور خارجـه همچنیـن از طریـق یـک برنامـه پـاداش دیگـر بـه تعقیـب هکرهـا پرداختـه اسـت تـا بتوانـد تحـت آن برنامـه، اطلاعاتـی را دربـاره مـوارد زیـر بـه دسـت آورد:

- هکرهـای ایرانـی کـه گفتـه می‌شـود اطلاعـات رأی‌دهنـدگان را دزدیـده و یـک سـازمان خبـری را هـک کرده‌انـد.

- هکرهـای روسـی کـه پشـت حمـلات بـه شـبکه بـرق اوکرایـن و بازی‌هـای المپیـک زمسـتانی ۲۰۱۸ هسـتند.

- هکرهـای روسـی کـه شـرکت‌های انـرژی مهـم در سراسـر جهـان را هـدف قـرار دادنـد.

- هکرهـای تحـت حمایـت دولتـی کـه شـرکت‌های مهمـی ماننـد خطـوط لولـه و بیمارسـتان‌ها را هـدف قـرار می‌دهنـد.

- هکرهای کره شمالی

بایدن نسل بعدی طرح رمزگذاری ایمن را منتشر کرد

پرزیدنـت بایـدن یـک فرمـان اجرایـی و یادداشـت امنیـت ملـی را امضـا کـرد کـه بـر سـرعت بخشـیدن بـه توسـعه محاسـبات کوانتومـی در ایـالات متحـده متمرکـز بـود و اطمینـان حاصـل کـرد که اسـتانداردهای رمزگـذاری بـرای ایـن تغییـر آمـاده هسـتند. دولـت ایـالات متحـده نگـران اسـت کـه نسـل آینـده کامپیوترهـای فـوق قدرتمنـد قـادر بـه شکسـتن فایل‌هایـی باشـد کـه مطابـق بـا اسـتانداردهای فعلـی رمزگـذاری شـده‌اند؛ بنابرایـن، مقامـات می‌خواهنـد مطمئـن شـوند کـه ایـالات متحـده اولیـن رایانه‌هـای کوانتومـی جدیـد را توسـعه می‌دهـد - کـه انتظـار مـی‌رود انقلابـی در علـم و مهندسـی ایجـاد کننـد - و رمزگـذاری را توسـعه می‌دهـد کـه بتوانـد در برابـر تهدیـدات مقاومـت کنـد. مؤسسـه ملـی اسـتاندارد و فنـاوری وزارت بازرگانـی در حـال حاضـر، بـرای چندیـن سـال درحال‌توسـعه الگوریتـم هـای رمزگـذاری بـوده اسـت.

جست‌وجوهای اف‌بی‌آی از داده‌های آمریکایی‌ها دوبرابر شده است

دفتر مدیر اطلاعات ملی گزارش شفافیت آماری سالانه خود را منتشر کرد که نشان می‌دهد FBI در سال گذشته ۳.۴ میلیون جستجوی بدون حکم در داده‌های آمریکایی‌ها انجام داده است که بیش از دوبرابر ۱.۳ میلیون جستجوی انجام شده در سال ۲۰۲۰ است. بالغ بر ۱.۹ میلیون جستجوها مربوط به حمله سایبری روسیه به زیرساخت‌های حیاتی بود. علی‌رغم افزایش نظارت بدون حکم توسط FBI، تعداد احکام مبتنی بر نظارت مخفی تأیید شده توسط دادگاه نظارت اطلاعات خارجی ایالات متحده در دو سال گذشته به نصف کاهش یافته است. در این گزارش اولین باری است که دولت تعداد جست‌وجوهای داده‌های داخلی را که بر اساس قانون نظارت بر اطلاعات خارجی در سال ۱۹۷۸ انجام شده است، فاش می‌کند.

دولت آمریکا به دنبال تحریم "هایکویژن" چین است

طبق گزارش‌ها، ایالات متحده در حال بررسی تحریم‌های مرتبط با حقوق بشر بر هایکویژن، یک شرکت چینی دارای دوربین‌های نظارتی است. هایک‌ویژن متهم شده است که از طریق تعامل با دولت چین که از دوربین‌های خود برای نظارت بر جمعیت اویغور استفاده می‌کند، نقض حقوق بشر را امکان‌پذیر کرده است. اگرچه محصولات این شرکت به طور گسترده در چین استفاده می‌شود، اما فناوری هایک‌ویژن بسیار فراتر از مرزهای کشور به کار می‌رود و مشتریانی در بیش از ۱۸۰ کشور جهان دارند. در صورت اجرا شدن این تحریم‌ها، محدودیت‌های موجود آمریکا علیه این شرکت افزایش می‌یابد. رئیس‌جمهور جو بایدن فرمان اجرایی را امضا کرد که سرمایه‌گذاری آمریکایی‌ها در هایک‌ویژن را ممنوع می‌کند و این شرکت در لیست نهاد وزارت بازرگانی قرار می‌گیرد و آن را از استفاده از فناوری آمریکایی در محصولاتش منع می‌کند.

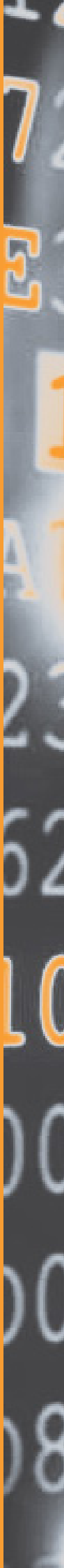
فرماندهی سایبری ایالات متحده در سال گذشته ۹ عملیات پیش‌دستانه را به سرانجام رساند

ژنرال پل ام. ناکاسون، فرمانده فرماندهی سایبری ایالات متحده، گفت که ایالات متحده ۹ عملیات «حمله پیش‌دستانه» را انجام داده است که برای ریشه‌کن کردن بدافزار دشمنان قبل از استفاده از آن در سال گذشته طراحی شده است. این عملیات در تعدادی از کشورهای متحد، از جمله لیتوانی، انجام شد، جایی که فرماندهی سایبری به شناسایی و مقابله با آسیب‌پذیری‌ها در سیستم‌های وزارت خارجه و وزارت دفاع کمک کرد. فرماندهی سایبری بیست و هشت عملیات در چهار سال گذشته را تأیید کرده است. این خبر در حالی منتشر می‌شود که فرماندهی سایبری نقش مهمی در محافظت از شبکه‌های اوکراینی در برابر حملات مخرب روسیه ایفا کرده است.

سناتورها رئیس DHS را به‌خاطر اطلاعات نادرست مجازات می‌کنند

سناتورهای جمهوری‌خواه در جلسه روز چهارشنبه، الخاندرو مایورکاس، وزیر امنیت داخلی را در مورد هیئت نظارت بر اطلاعات نادرست برنامه‌ریزی‌شده این وزارتخانه مورد انتقاد قرار دادند و متهم کردند که او سعی می‌کند تا با نظراتی که مقامات دوست ندارند مبارزه کند. مایورکاس از هیئت مدیره دفاع کرد و گفت که اختیارات محدود و اولویت‌های مهمی دارد. او ادامه داد DHS توضیح داده است که بر روی حمله روسیه به اوکراین، قاچاقچیان انسان در مرز ایالات متحده و مکزیک و همچنین اطلاعات نادرست که سازمان‌های مهم را تهدید می‌کند، تمرکز خواهد کرد. مایورکاس گفته است که هیئت‌مدیره «اختیار عملیاتی» نخواهد داشت. او همچنین تکرار کرد که DHS مدت‌هاست بر اطلاعات نادرست تمرکز کرده است و هیئت‌مدیره آنچه را که باید سال‌ها پیش ایجاد می‌شد، ایجاد می‌کند، یعنی استانداردها، تعاریف، دستورالعمل‌ها و سیاست‌ها.


Data Breach
Cyber Attack
System Sa



تهدیدات سایبری

اطلاعات مکان کاربران برنامه نرم افزاری Grindr مدت‌هاست که برای فروش گذاشته شده استر

یک شرکت تبلیغاتی تلفن همراه حداقل از سال ۲۰۱۷ داده‌های برنامه دوستیابی LGBTQ را می‌فروشد. بایرون تاو از وال‌استریت ژورنال گفت درحالی‌که گریندر ادعا کرده است که دیگر اجازه نمی‌دهد داده‌های موقعیت مکانی به شرکت‌های تبلیغاتی داده شود، اما ممکن است این داده‌ها همچنان در دسترس باشد. این نگرانی را افزایش می‌دهد که داده‌ها ممکن است برای باج‌گیری یا اخاذی کردن از مردم بر خلاف میل آنها استفاده شوند.

به نظر می‌رسد این اتفاق درگذشته هم رخداده است. سال گذشته، مدیر ارشد کنفرانس اسقف‌های کاتولیک ایالات متحده پس از اینکه یک خبرنامه کاتولیک اعلام کرد داده‌هایی از تلفن همراه او دارد که نشان می‌دهد او از این برنامه استفاده کرده و به بارهای همجنس‌گرایان رفته است، استعفا داد. همچنین می‌توانند پیامدهای امنیت ملی داشته باشد. یعنی دولت‌های خارجی از نظر تئوری می‌توانند از داده‌ها برای باج‌گیری از مقامات دولتی استفاده کنند. پاتریک لنیهان، سخنگوی Grindr گفت: از اوایل سال ۲۰۲۰، Grindr اطلاعات کمتری را با شرکای تبلیغاتی نسبت به پلتفرم‌های Big Tech و اکثر رقبای ما به اشتراک گذاشته است. او اضافه کرد که «فعالیت‌هایی که شرح داده شد با رویه‌های حریم خصوصی فعلی Grindr که دو سال است در حال اجراست، امکان‌پذیر نخواهد بود».

رئیس اطلاعات اسپانیا اذعان کرد که اسپانیا ۱۸ هوادار استقلال کاتالونیا را با نرم‌افزارهای جاسوسی هدف قرار داده است

آژانس جاسوسی دستور دادگاه برای جاسوسی از سیاستمدار پره آراگونس، رئیس کنونی منطقه خودمختار کاتالونیا اسپانیا و ۱۷ حامی دیگر استقلال کاتالونیا را دریافت کرد. پاز استبان، رئیس جاسوسی اسپانیا در یک جلسه استماع غیرعلنی به قانون‌گذاران اسپانیایی گفت که ۱۷ هدف دیگر همگی ارتباط با یک گروه معترض داشتند که خواستار تعطیلی فرودگاه بارسلون در سال ۲۰۱۹ برای حمایت از خودمختاری کاتالونیا شدند. استبان دستورات دادگاه را به قانونگذاران نشان داد که آژانس او باید از پگاسوس برای قربانیان استفاده کند.

سیاستمداران اسپانیایی نیز هک شدند. مقامات اسپانیایی آثاری از پگاسوس را در دستگاهی متعلق به وزیر کشور فرناندو گرانده-مارلاسکا پیدا کردند. اگر تحلیلگران متوجه شوند که گراند مارلاسکا با پگاسوس هک شده است، او سومین مقام تایید شده در سطح کابینه اسپانیا خواهد بود که هک می شود. مشخص نیست چه کسی پشت هک مقامات اسپانیایی بوده است، اما آنها در بحبوحه اختلافات دیپلماتیک بین اسپانیا و مراکش که متهم به استفاده از پگاسوس هستند، رخ داد. مراکش دستیابی به این نرم افزارهای جاسوسی را رد کرده است.

نخست‌وزیر اسپانیا توسط پگاسوس هک شدر

هک پدرو سانچز نخست‌وزیر اسپانیا با نرم‌افزارهای جاسوسی گروه NSO در سال گذشته نشان‌دهنده اولین آلودگی تأیید شده یک رهبر اروپایی و ناتو است. مشخص نیست چه کسی مسئول هک سانچز یا مارگاریتا روبلز وزیر دفاع بوده است. NSO که بنا به گزارش‌ها یک حساب کاربری در اسپانیا دارد، گفته است که فقط نرم‌افزارهای جاسوسی خود را در اختیار سازمان‌های دولتی یا مجری قانون قرار می‌دهد. فلیکس بولانوس وزیر اسپانیایی گفت که هک کردن سانچز و روبلز "غیرقانونی و خارجی" بود و کسانی که در پشت این هک‌ها بودند "مجوز قضایی از هیچ نهاد رسمی نداشتند." مشخص نیست که آیا مسئولین در داخل اسپانیا هستند یا در کشور دیگری.

این افشاگری دوهفته پس از آن صورت گرفت که محققان گفتند دست‌کم ۶۰ دستگاه الکترونیکی آلوده به پگاسوس را پیدا کرده‌اند که توسط مقامات، فعالان و روزنامه‌نگاران منطقه خودمختار کاتالونیای اسپانیا استفاده می‌شد.

مقامات کاتالونیا از اسپانیا خواسته‌اند تا درباره این هک‌ها تحقیق کند، اما تحقیقاتی که آنها را مشروع و مفید می‌دانند، دریافت نکرده‌اند. در همین حال، دولت اسپانیا قبلاً پرونده سانچز و روبلز را به وزارت دادگستری این کشور ارجاع داده است. پر آراگونس، رئیس‌جمهور کاتالونیا در واکنش‌های مختلف به هک‌ها به آنچه که «استاندارد دوگانه» می‌خواند اشاره کرد و گفت که آنها فقط سکوت و بهانه‌ها را می‌شنوند، درحالی که همه چیز را باعجله انجام می‌دهند.

نظر فاش شده دادگاه عالی باعث ایجاد ترس در مورد امنیت داده‌ها شده است

توییت هایی در روز سه‌شنبه با هشدارهایی درباره داده‌های جمع‌آوری‌شده توسط اپلیکیشن‌ها و سرویس‌های آنلاین منتشر شد مبنی بر این که ممکن است این داده ها برای شناسایی زنانی که به دنبال سقط جنین هستند، در صورت غیرقانونی شدن این روش در برخی ایالت‌ها مورد استفاده قرار گیرد. این توئیت‌ها با پیش‌نویس لو رفته از تصمیم اکثریت دادگاه عالی برای لغو حکم Roe v. Wade در سال ۱۹۷۳ که حقوق سقط جنین را تأیید می‌کرد، منتشر شد.

گزارش ها نشان می دهد یک شرکت اطلاعات مکانی بیش از ۶۰۰ والدین را در ایالات متحده از کارگزار داده SafeGraph به قیمت حدود ۱۶۰ دلار خریداری کرده است که برخی از داده‌ها مکان کلینیک‌های رزرو شده والدین سقط جنین را ارائه می‌دهند. این در حالی است که داده‌ها شامل نام کاربران نمی‌شود. این داده‌ها درگذشته برای شناسایی افراد با تجزیه‌وتحلیل الگوهای حرکت و رفتار استفاده می‌شدند.

جنگ روسیه و اوکراین

نیروهای روسی از طریق شبکه‌های روسی سرویس اینترنت در شهر اوکراین را تغییر دادند

سرویس اینترنت در Kherson روز شنبه قطع شد. تا یکشنبه، اینترنت شهر از طریق شبکه‌های روسی تغییر مسیر داده شد. به نظر می‌رسد این اقدام باهدف تقویت کنترل روسیه بر بخش‌های استراتژیک مهم کشور باشد. خرسون اولین شهر بزرگی بود که پس از تهاجم به دست نیروهای روسیه افتاد.

مقامات اوکراینی قبلاً گفته بودند که این قطعی‌ها به دلیل شکستگی خطوط در مرکز فیبر نوری و قطع برق تجهیزات اپراتورهای خدمات در این مناطق بوده است.

مقامات اوکراینی گفتند که این اقدام با تبلیغات روسیه همراه بوده است. سرویس دولتی ویژه ارتباطات و حفاظت اطلاعات اوکراین گفت: «درست پس از قطع ارتباط، رسانه‌های دشمن شروع به انتشار اخبار جعلی کردند که می‌گفتند این دولت اوکراین بود که دستور قطع اتصال را صادر کرد.» این یک دروغ است زیرا ما همیشه از حداکثر دسترسی به هر وسیله ارتباطی برای همه اوکراینی‌ها دفاع کرده‌ایم.

مرکز دفاع سایبری ناتو در بحبوحه تهدید روسیه، سه عضو جدید اضافه کرد

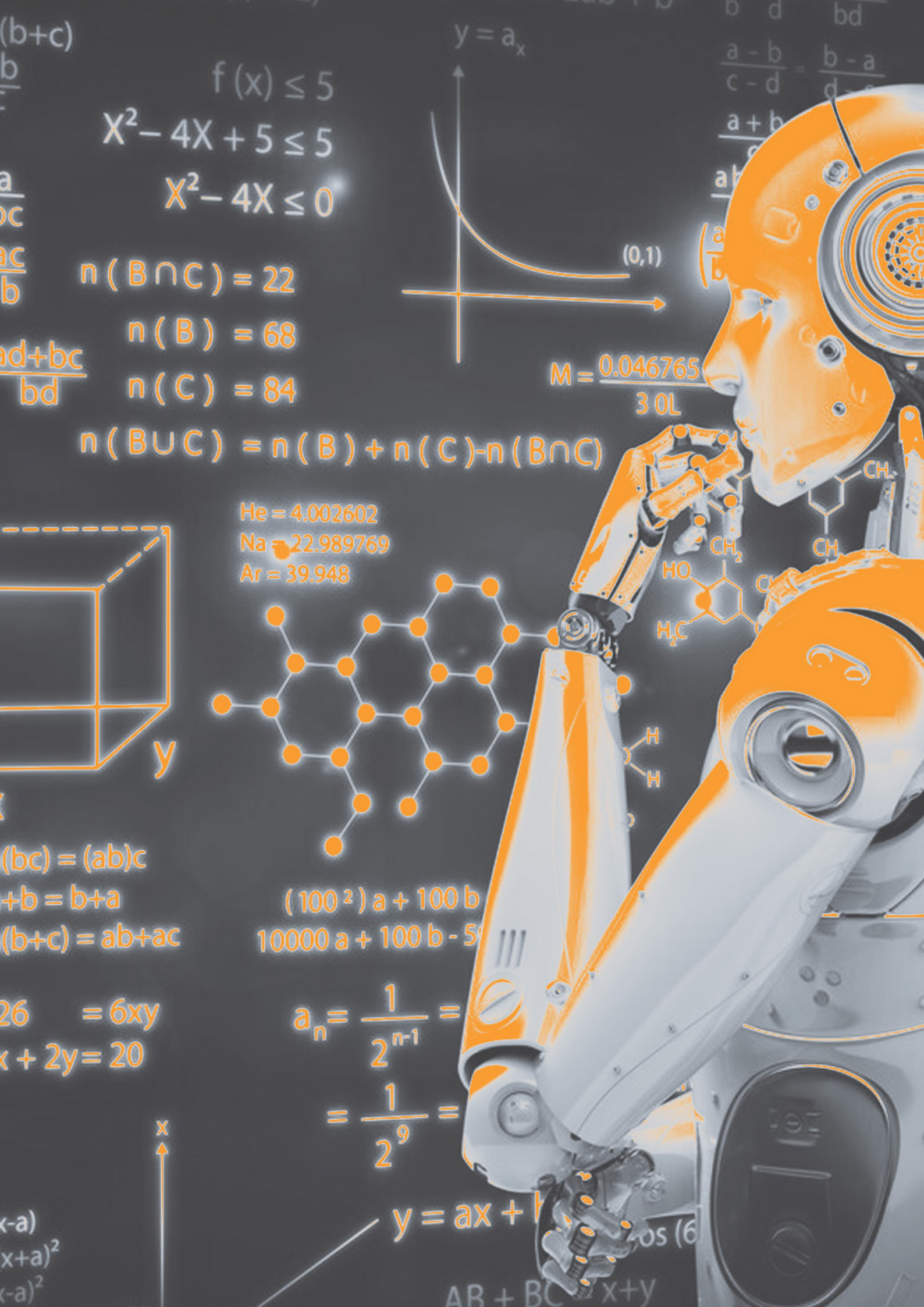
آژانس جاسوسی کره جنوبی گفت در مرکز دفاع سایبری ناتو کمک می‌کند تا توانایی خود را برای پاسخ به حملات سایبری افزایش دهند. این جدیدترین توسعه برای مرکز تعالی دفاع سایبری تعاونی (CCDCOE) است که از کانادا و لوکزامبورگ نیز به عنوان اعضای جدید نام برده شد.

شایان ذکر است که اوکراین نیز اخیراً به آن ملحق شده است. سرهنگ Jaak Tarien، مدیر CCDCOE گفت که مشارکت اوکراین می‌تواند دانش دست‌اول ارزشمندی از چندین دشمن در حوزه سایبری برای استفاده برای تحقیق، تمرین و آموزش به ارمغان آورد.

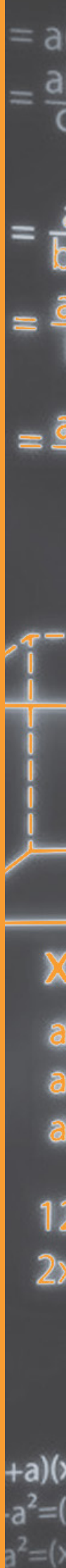
CCDCOE توسط اعضای آن تأمین مالی می‌شود. CCDCOE می‌گوید درحالی‌که این یک "واحد عملیاتی متعلق به ساختار فرماندهی ناتو" نیست، اما بخشی از مراکز عالی معتبر ناتو است.

استفاده روس‌ها از ابزارهای ناشناس‌سازی آنلاین به‌شدت افزایش‌یافته است

روس‌ها به صورت دسته‌جمعی به شبکه‌های خصوصی مجازی روی آورده‌اند که به آنها اجازه می‌دهد سانسور و نظارت دولتی روسیه را دور بزنند. از زمان شروع جنگ در فوریه، روزانه صدها هزار VPN در روسیه دانلود می‌شود – این افزایش تقاضا نشان‌دهنده تلاش زیاد رئیس‌جمهور ولادیمیر پوتین برای جداکردن روس‌ها از جهانی گسترده است. وی‌پی‌ان‌ها با محافظت از مکان‌ها و هویت کاربران، اکنون به میلیون‌ها روس اجازه دسترسی به مطالب مسدود شده را می‌دهند.


f(x) ≤ 5
X² – 4X + 5 ≤ 5
X² – 4X ≤ 0
y = a_x
(0,1)
n(B∩C) = 22
n(B) = 68
n(C) = 84
n(B∪C) = n(B) + n(C) - n(B∩C)
M = 0.046765 / 3 0L
He = 4.002602
Na = 22.989769
Ar = 39.948
(bc) = (ab)c
+b = b+a
(b+c) = ab+ac
26 = 6xy
x + 2y = 20
(100 ²) a + 100 b
10000 a + 100 b - 5
a_n = 1 / 2^(n-1) =
= 1 / 2^9 =
y = ax +
AB + BC
x+y
x
y

تکنولوژی‌های سایبری



شرکت مادر Tinder از گوگل به‌خاطر هزینه‌های App Store شکایت کرد

شرکت برنامه‌های دوستیابی Match Group، مالک Tinder و OkCupid، روز دوشنبه از گوگل شکایت کرد و مدعی شد که این غول فناوری با الزام توسعه‌دهندگان اپلیکیشن به استفاده از سیستم پرداخت گوگل زمانی که می‌خواهند برنامه‌های خود را از طریق App Store گوگل توزیع کنند، قوانین را زیر پا گذاشته است.

گوگل سال‌ها به Match و سایر توسعه‌دهندگان اجازه داده بود از سیستم‌های پرداخت جایگزین استفاده کنند، اما در سال ۲۰۲۱ اعلام کرد که از سازندگان اپلیکیشن‌ها می‌خواهد از سیستم خود استفاده کنند که برای هر پرداختی که از طریق یک برنامه انجام می‌شود، کارمزد دریافت می‌کند. اگرچه سیستم‌عامل اندروید گوگل امکان دانلود برنامه‌ها را در خارج از App Store گوگل فراهم می‌کند، اکثریت‌قریب‌به‌اتفاق مردم از فروشگاه رسمی گوگل استفاده می کنند.

وکلای Match Group در شکایتی که دوشنبه در دادگاه فدرال در ناحیه شمالی کالیفرنیا ارسال شد، نوشتند: «گوگل توسعه‌دهندگان اپلیکیشن‌ها را با این اطمینان به سمت پلتفرم خود جذب کرد که ما می‌توانیم به کاربران در مورد نحوه پرداخت هزینه خدماتی که می‌خواهند حق انتخاب بدهیم». اکنون، گوگل به دنبال حذف خدمات پرداخت توسط کاربران و افزایش قیمت‌ها برای مصرف‌کنندگان در پی گسترش تسلط خود است.

تولید آی‌پاد بالاخره متوقف شد

شرکت اپل اعلام کرد که به فروش نسل هفتم آی‌پاد تاچ تا زمانی که ذخایرش تمام می‌شود ادامه خواهد داد – تأییدی بی‌صدا مبنی بر اینکه ممکن است عصر آی‌پاد بالاخره به پایان رسیده باشد.

این حرکت، اگرچه برای متخصصان فنی دارای سن خاص تلخ‌وشیرین بود، اما کاملاً غافلگیرکننده نبود. برای سال‌ها، اپل به‌آرامی خط تولید سیستم‌های رسانه‌ای قابل‌حمل خود را حذف کرد: آخرین آی‌پاد با چرخ کلیک کلاسیک در سال ۲۰۱۴ متوقف شد، و آی‌پاد نانو که زمانی محبوب بود، تا سه سال بعد از آن مورداستفاده قرار گرفت.

گرگ جوسویاک، معاون ارشد بازاریابی جهانی اپل، گفت: امروز روح آی‌پاد زنده است. ما یک تجربه موسیقی باورنکردنی را در تمامی محصولات خود، از آیفون گرفته تا اپل‌واچ تا هوم پاد مینی، و در مک، آی پد و اپل تی وی، ادغام کرده‌ایم.

در حال حاضر، ایده تولید یک دستگاه تک‌منظوره مانند iPod می‌تواند ناامیدکننده باشد. اما نسخه‌هایی که ویدیوها را پخش می‌کردند و در نهایت، تولید مدل‌های دارای صفحه‌نمایش لمسی که تا این هفته ادامه داشت مورد استقبال بود. اما آی پادها در نهایت تحت الشعاع آیفون قرار گرفتند اما به طور کلی سخت است از تأثیری که بر شرکت و افرادی که از آنها استفاده می کردند چشم پوشی کنیم.

سامسونگ توسعه شبکه ۶G را با سرعتی حدود ۵۰ برابر بیشتر از ۵G آغاز می‌کند

بر اساس مستندات منتشر شده از سوی سامسونگ الکترونیکس تحت عنوان «طیف ۶G: گسترش مرزها» ظاهراً این شرکت برنامه‌های خود را برای توسعه شبکه ۶G دنبال می‌کند.

به گفته سونگ هیون چوی معاونت اجرایی سامسونگ و رئیس مرکز تحقیقات مخابراتی پیشرفته، آنها مسیر درک، توسعه و استانداردسازی فناوری ارتباطاتی ۶G را از مدت‌ها پیش آغاز کرده‌اند. وی در ادامه می‌گوید:

«ما متعهد هستیم تا پیش‌قدم شویم، یافته‌های خود را به اشتراک بگذاریم و با نشر ابتکارمان تجربه اتصال فوق‌العاده‌ای را به زندگی مردم بیاوریم.»

به‌عبارت‌دیگر این غول دنیای فناوری کار برای ارائه استاندارد نسل بعد به بازار را آغاز کرده است.

ماسک می‌گوید ربات‌های اسپم توییتر را ممنوع خواهد کرد، درحالی‌که او از این موضوع استفاده کرده است

ایلان ماسک قول داده است که الگوریتم توییتر را درباره اینکه چرا برخی توییت‌ها بالاتر از سایر توییت منتشر می‌شود را شفاف کند. همچنین قول داد توییتر را از حساب‌های خودکاری که برنامه‌ها، محصولات و سیاستمداران و همچنین سریع ثروتمند شدن را تبلیغ می‌کنند، پاک‌سازی کند.

ماسک در مراسم مت‌گالا آخر هفته گذشته گفت: "اگر کسی ارتش ربات و ترول را اداره می‌کند، پس من قطعاً دشمن او هستم."

اما محققان می‌گویند که خود ماسک از این امکانات نظیر پروموت فزاینده توییت‌ها توسط ربات‌ها یا بایکوت خبرهای منفی بهره برده است. از جمله از طریق حساب‌هایی که در مورد ارزشمندترین سرمایه‌گذاری او، یعنی سهام تسلا، نهایت تلاش خود را به کار می‌بستند، زمانی که شرکت تسلا به دلیل تصادفات، نتایج مالی ضعیف و درگیری با تنظیم‌کننده‌ها با اخبار منفی مواجه شد.

این محققان می‌گویند ربات‌ها - حساب‌های خودکاری که برای انجام کارهای از پیش تعریف‌شده برنامه‌ریزی شده‌اند، اغلب با سرعت‌هایی بیشتر از آنچه که یک فرد می‌تواند مدیریت کند - برای آزار منتقدان ماسک و حتی سانسور تصاحب بحث‌برانگیز هیئت‌مدیره توییتر به کار گرفته شده‌اند.

ICDT.IR