موبایل و تروریسم در کانون توجه مجلس سنای آمریکا

خوزه پالیوری . ترجمه: فرنگیس رحیق

ممکن است درنهایت درباره بحث تروریسم و حریم خصوصی تلفن‌های همراه از سوی مجلس سنای ایالات متحده بازنگری رسمی شود. مشکل اصلی امروز ناتوانی در ردیابی تروریست‌هایی است که با کمک فناوری رمزگذاری، «مخفی» می‌مانند. افراط‌گرایان خشن در مکان‌های عمومی، مانند فیس‌بوک و توییتر با هم ملاقات می‌کنند و بعد با بهره‌گیری از فناوری رمزگذاری که پیام‌ها را به رمز درمی‌آورد با هم به‌طور خصوصی مکالمه می‌کنند که اصطلاحا به آن «مخفی‌ماندن» می‌گوییم. روز دوشنبه هشتم دسامبر ۲۰۱۵، رئیس کمیته امنیت داخلی ایالات متحده گفت خواهان بازنگری در فناوری رمزگذاری برنامه‌های کاربردی از سوی هیأتی ویژه است، به‌خصوص بازنگری در این مسئله که تروریست‌ها چگونه به کمک این فناوری از تحت‌نظربودن فرار می‌کنند. مایک مک‌کول، یکی از نمایندگان مجلس سنا و رئیس کمیته امنیت داخلی ایالات متحده، در سخنرانی خود در دانشکده دفاع ملی در واشنگتن‌دی‌سی گفت: «ما نمی‌توانیم جلوی چیزی را که نمی‌بینیم، بگیریم. این یکی از بزرگ‌ترین چالش‌های مبارزه با تروریسم در قرن ۲۱ و یکی از هراس‌انگیزترین مسئله‌هایی است که شب‌ها من را بیدار نگه می‌دارد». مک‌کول، جمهوری‌خواه اهل تگزاس، امیدوار است بتواند هیأتی ملی را برای چالش‌هایی که در عصر دیجیتال، سر راه امنیت و فناوری قرار دارد، تشکیل دهد. او می‌خواهد مجریان قانون، شرکت‌های فناوری، محققان و مدافعان حریم خصوصی را برای دستیابی به یک راه‌حل با هم متحد کند. این مناظره کلاسیک حریم خصوصی در برابر مسئله امنیت است و اگر هیأت مک‌کول با تأیید مجلس سنای ایالات متحده مواجه شود، انتظار می‌رود جنجالی به پا شود. مجریان قانون، خواهان دسترسی نامحدود به دستگاه‌های مردم و راهی برای مخفیانه گوش‌کردن به مکالمه‌های صوتی، ویدئویی و خواندن متن‌ها هستند، اما بقیه، یعنی شرکت‌های فناوری، محققان و مدافعان حریم خصوصی با قاطعیت در برابر این مسئله ایستادگی می‌کنند. استدلال آنها این است که همان روشی که به مجریان قانون اجازه ورود به این حریم‌ها را می‌دهد، از سوی هکرها، مجرمان و جاسوسان خارجی هم می‌تواند استفاده شود. اگر مکالمه‌های تروریست‌ها حریم خصوصی داشته باشد، حریم خصوصی مکالمه‌های شما هم کمتر می‌شود.

تفسیر گروه فناوری رمزگذاری

هم‌اکنون مکالمه خصوصی و امن داشتن برای دو نفر در دو سوی این سیاره از هر زمانی راحت‌تر است. واتس‌اپ و تلگرام برنامه‌های کاربردی هستند که متن را رمزگذاری می‌کنند. برنامه سیگنال، تماس‌های تلفنی را رمزگذاری می‌کند. برنامه «ویکر» امکان ارسال پیام‌هایی را دارد که پس از خوانده‌شدن از بین می‌روند. فیس‌تایم، برنامه چت ویدئویی آیفون هم ارتباط را رمزگذاری می‌کند. برای ارسال ایمیل ابزاری با نام PGP وجود دارد. نمونه برنامه‌های قانونی رایج، بی‌شمار هستند. همه این برنامه‌ها کلمه‌ها را به کدهای رایانه‌ای درهم‌وبرهم تبدیل می‌کنند که جاسوس‌های دولتی هم نمی‌توانند به‌سرعت آنها را بشکنند. فناوری رمزگذاری، مکالمه بین شما و اعضای خانواده‌تان را خصوصی نگه می‌دارد. همچنین برای یک تروریست در سوریه و فردی که او سعی دارد در ایالات متحده برای قتل عام جمعی استخدام کند، شرایط امنی مهیا می‌کند. دستگاه‌ها هم قفل و رمزگذاری دارند که کار تحقیق پلیس را دشوارتر می‌کنند. حتی اگر پلیس دستگاه تلفن یک مضنون را هم به دست آورد، گاهی نمی‌تواند اطلاعات آن دستگاه را رمزگشایی کند. دستگاه‌های شرکت اپل (Apple Tech30) و گوگل (google Tech30) مشتریان را به گذاشتن رمز عبور ترغیب می‌کنند و فقط مالک آن دستگاه، کلید بازکردن آن قفل را دارد. این شرکت‌ها این کارها را برای حفظ حریم خصوصی در پاسخ به اعتراض گسترده مردم در سال ۲۰۱۳ شروع کردند؛ وقتی که معلوم شد دولت ایالات متحده بدون عذر موجه مردم را تحت نظر گرفته است.

تفسیر هیأت مک‌کول

مک‌کول می‌داند این مناظره کار سختی است. او در سخنرانی خود گفت: «ما باید مراقب باشیم که به خود فناوری کدگذاری اتهام وارد نکنیم؛ برای اینکه این فناوری برای حفظ حریم خصوصی، امنیت اطلاعات و تجارت جهانی ضروری است».کارشناسان امنیت رایانه، آنهایی که فناوری رمزگذاری را از همه بهتر می‌فهمند، با هر هیأتی با احتیاط برخورد می‌کنند. شین مک دوگال (Shane MacDougall) مشاور امنیت سایبری شرکت هوش تدبیری (Tactical Intelligence) می‌گوید: «درباره اینکه این سیاست‌مداران کدام قسمت فناوری رمزگذاری را نمی‌فهمند، تردید دارم. هیچ روش محاسباتی وجود ندارد که بتواند سیستم رمزگذاری را برای یک گروه ضعیف کند و درعین‌حال برای بقیه امن نگه دارد. اگر ما سیستم رمزگذاری را ضعیف کنیم، آن‌وقت تروریست‌ها می‌توانند از جرائم سایبری و سیستم‌های نفوذی، پول بیشتری کسب کنند و سطح دسترسی خودشان را افزایش دهند». به علاوه هرگونه تلاشی برای تحت‌نظارت‌درآوردن سیستم رمزگذاری دشوار است. فقط این سیستم نرم‌افزاری است که به‌آسانی ساخته، کپی و به اشتراک گذاشته می‌شود و قسمت عمده کار رایگان انجام می‌شود. مارکوس جی‌کری (Marcus J.Carey) که متخصص اسبق محافظت از شبکه‌های رایانه‌ای سازمان امنیت ملی NSA و درحال‌حاضر مدیر یک شرکت امنیت سایبری به نام vThreat است، خاطرنشان می‌کند مجریان قانون برای تحت‌کنترل درآوردن ابزار رمزگذاری موجود، زمان دشواری را سپری خواهند کرد. بسیاری از این ابزارها به وسیله گروهی از داوطلبانی ساخته شده‌اند که کدها را فقط به خاطر یافتن اشتباه‌ها مرور می‌کنند. مأموران پلیس می‌توانند با واردکردن باگ‌های کنترل‌شده در نرم‌افزار برای به‌هم‌ریختن کار این ابزار تلاش کنند، اما احتمالا گرفتار خواهند شد. کری می‌گوید: «(back door) بک‌دور (راه فرار) گذاشتن توی نرم‌افزارهای متن‌باز غیرممکن نیست، اما کشف این بک‌دورها قطعا آسان‌تر خواهد بود».آیا این مناظره یک طرف روشن دارد؟ حداقل این یک مناظره یک طرفه با مجلسی نیست که فقط به حرف‌های اف‌بی‌آی و سازمان‌های جاسوسی گوش می‌دهد. مینگ چاو (Ming Chow) سخنگوی علوم رایانه در دانشگاه تافتس، می‌گوید: «سیاست‌مداران دانش کمی درباره فناوری و سیستم رمزگذاری و متخصصان فناوری درک کمی از سیاست دارند. آیا می‌خواهید این کار به‌درستی انجام شود؟ پس همه ذی‌نفع‌ها باید سر یک میز بنشینند. اگر این کار به‌درستی انجام نشود هیچ برنده‌ای نخواهد داشت».

رویداد

توضیح درباره مشکلات ثبت‌نام ADSL

● **ایسنا:** در ماه‌های گذشته ثبت‌نام برای دریافت اشتراک ADSL با چالش‌های بسیاری مواجه شده و در این زمینه مشکلات متعددی پیش‌روی مردم و شرکت‌ها قرار دارد. دامنه این مشکلات چنان گسترده شده که گاهی حتی مدیران شرکت‌های ارائه‌کننده اینترنت پرسرعت خانگی، از غیرممکن‌بودن واگذاری سرویس جدید در ۸۰ درصد مناطق شهری مانند تهران خبر می‌دهند. نصرالله جهانگرد دراین‌باره گفت: آمارهای مربوط به این بخش را باید سازمان تنظیم مقررات و ارتباطات رادیویی اعلام کند؛ چراکه به‌شخصه آمار دقیقی در این حوزه ندارم. رئیس سازمان فناوری اطلاعات کشور ادامه داد: مشخص نیست به طور دقیق مشکلات مذکور مربوط به مباحثی مانند کابل و رانژه می‌شود یا خود این شرکت‌ها محدودیت‌هایی دارند. او افزود: تعداد مشترکان این شرکت‌ها نسبت به ظرفیتی که آنها دارند، بالاتر است و اکنون بحث ما آن است که آیا ضریب اشتراک یک‌به‌هشت در این شرکت‌ها رعایت می‌شود یا این شرکت‌ها پهنای باند خود را در اختیار تعداد بیشتری می‌گذارند. به گفته او با این شیوه صدمات بسیاری به کیفیت سرویس دریافتی مردم وارد می‌شود. او ارائه توضیحات بیشتر دراین‌باره را به سازمان تنظیم مقررات و ارتباطات رادیویی کشور محول کرد.

الزام برنامه ششم برای سرمایه‌گذاری ۶۰هزارمیلیاردی

● **مهر:** معاون وزیر ارتباطات از الزام لایحه پیشنهادی دولت برای برنامه ششم توسعه برای سرمایه‌گذاری ۶۰هزارمیلیاردی در بخش فناوری اطلاعات خبر داد. امیرحسین دوایی با اعلام این خبر افزود: سرمایه‌گذاری پیش‌بینی‌شده این برنامه عددی در حدود ۶۰ هزار میلیارد تومان است که فرض بر این قرار گرفته که بیش از نیمی از این هدف به وسیله بخش خصوصی تأمین شود و بخشی دیگر را نیز دولت به عنوان توسعه زیرساخت‌ها مد نظر قرار دهد. او گفت: در برنامه ششم توسعه دولت به عنوان حامی بخش خصوصی، نقش خود را برای ایجاد و رشد فضای رقابتی ایفا می‌کند. او ادامه داد: بخشی از این حوزه باید با سرمایه‌گذاری دولت انجام شود و فضای رقابتی ایجادشده با حمایت دولت توسعه یابد.

۱۲۰ کشور خواستار سرعت‌بخشیدن به توسعه شبکه جهانی اینترنت

● **شرق:** نمایندگان ۱۲۰ کشور شرکت‌کننده در دومین نشست جهانی اینترنت، خواستار سرعت‌بخشیدن به توسعه شبکه جهانی اینترنت شدند. این همایش بزرگ بین‌المللی که حدود دو هزار نفر (هشت رهبر، حدود ۵۰ وزیر، مسئولان بیش از ۲۰ سازمان بین‌المللی و حدود هزار نفر از مدیران شرکت‌های اینترنتی) در آن شرکت داشتند، روز چهارشنبه ۲۵ آذر جاری با سخنان «شی‌جین پینگ»، رئیس‌جمهوری چین در شهر «وو جن» در شرق این کشور گشایش یافت تا ارتباط متقابل شبکه‌ها و دولت‌ها و همچنین مدیریت بر فضای مجازی را بررسی کند. شرکت‌کنندگان در خاتمه این گردهمایی سه‌روزه، با صدور بیانیه‌ای بر استفاده بهتر، سالم و ایمن از اینترنت و جلوگیری از سوءاستفاده‌های افراد و گروه‌های خاطی از آن تأکید کردند. همچنین شرکت‌کنندگان تقویت ارتباطات اینترنتی میان کشورها را یادآور شدند و اعلام کردند به منظور بهره‌مندی و مدیریت مشترک اینترنت و ایجاد آینده‌ای بهتر برای بشریت، باید تلاش‌ها را در این زمینه افزایش داد. راهکارهای مقابله با حملات اینترنتی، تقویت شبکه‌های مخابراتی، فضای مجازی و حاکمیت بر آن و همچنین ارتباط شبکه‌های اینترنتی میان‌قاره‌ای و بین کشورها، از دیگر محورهایی بود که شرکت‌کنندگان در بیانیه پایانی اجلاس به آن توجه نشان دادند.

متوسط سرعت جهانی اینترنت ۵،۱ مگابیت در ثانیه

● **فارس:** نتایج یک بررسی نشان می‌دهد متوسط سرعت اتصال به اینترنت پرسرعت در جهان با رشد ۱۴درصدی در سه‌ماهه سوم سال ۲۰۱۵ در مقایسه با مدت مشابه سال قبل، به ۵،۱ مگابیت در ثانیه رسیده است. براساس گزارش تک اسپات، تنها پنج درصد از کاربران اینترنت در دنیا با سرعت ۲۵ مگابیت در ثانیه یا بیشتر به اینترنت متصل می‌شوند. گزارش ۶۰صفحه‌ای Akamai درباره سرعت اتصال به اینترنت در کشورهای مختلف جهان نشان می‌دهد متوسط سرعت اتصال به اینترنت نسبت به سه ماهه دوم سال ۲۰۱۵ حدود ۰،۲ درصد افزایش نشان می‌دهد. طبق این گزارش کره‌جنوبی با متوسط سرعت اتصال ۲۰،۵ مگابیت در ثانیه در رتبه اول و سوئد و نروژ با سرعت اتصال ۱۷،۴ و ۱۶،۴ مگابیت در ثانیه در رتبه‌های دوم و سوم هستند. رتبه‌های چهارم و پنجم و ششم با سرعت‌های اتصال، ۱۶،۲، ۱۵،۸ و ۱۵،۶ مگابیت در ثانیه متعلق به کشورهای سوئیس، هنگ‌کنگ و هلند است. رتبه‌های هفتم تا دهم هم مربوط به کشورهای ژاپن، فنلاند، لاتویا و جمهوری چک است. گفتنی است در گزارش مذکور هیچ اشاره‌ای به نام ایران نشده است، اما در گزارش‌های قبلی این شرکت سرعت اتصال به اینترنت همراه در ایران بررسی شده و کشورمان با سرعت اتصال ۰،۹ مگابیت در ثانیه در قعر جدول و پایین‌تر از تمامی ۵۴ کشوری بود که بررسی شده‌اند.

بازار

افزایش ۷/۷ درصدی عرضه گوشی‌های هوشمند

دیجی‌تایمز گزارشی درباره عرضه گوشی‌های هوشمند در سه ماهه سوم سال جاری میلادی منتشر کرده که نشان از افزایش ۷،۷درصدی عرضه این محصولات در مقایسه با مدت مشابه سال گذشته میلادی دارد. آخرین گزارش منتشرشده در رابطه با تعداد گوشی‌های هوشمند عرضه‌شده از سوی شرکت‌های مختلف نشان از این دارد که از ابتدای ماه جولای تا اواخر سپتامبر، بیش از ۳۳۱،۹ میلیون دستگاه گوشی‌هوشمند روانه بازار شده است. افزایش میزان عرضه گوشی‌های هوشمند در مقایسه با فصل دوم سال جاری میلادی، بیش از ۱۰،۵ درصد برآورد شده است. دیجی‌تایمز پیش‌بینی کرده میزان عرضه گوشی‌های هوشمند در سه ماهه چهارم به بیش از ۳۹۶،۸ میلیون دستگاه افزایش خواهد یافت که در مقایسه با فصل سوم نشان از افزایشی ۲۰درصدی و در مقایسه با مدت مشابه سال گذشته نشان از افزایشی ۱۰،۱درصدی دارد. در مجموع دیجی‌تایمز پیش‌بینی کرده میزان عرضه گوشی‌های هوشمند در سال جاری میلادی به بیش از۱،۳۲۶ میلیارد دستگاه افزایش خواهد یافت. مانند فصل‌های پیش، سامسونگ و اپل عنوان اولین و دومین شرکت بزرگ عرضه‌کننده گوشی‌های هوشمند را در اختیار دارند. سامسونگ با دراختیارداشتن بیش از ۲۵،۶ درصد از بازار در طول سه ماهه سوم، عنوان اول و اپل با عرضه ۱۴،۵ درصد، عنوان دوم بزرگ‌ترین عرضه‌کننده گوشی‌های هوشمند را در اختیار گرفته است. پس از این دو، شرکت هوآوی با ۷،۴، لنوو با ۴،۸ و ال‌جی با ۴،۵ درصد جایگاه‌های بعدی را به خود اختصاص داده‌اند. شیائومی با عرضه بیش از ۳،۸ درصد از گوشی‌های هوشمند در رده بعدی قرار گرفته است. مایکروسافت با دراختیارداشتن بیش از ۱،۷ درصد در جایگاه دوازدهم جای گرفته است. به‌تازگی مورگان‌استنلی گزارشی منتشر کرده که کاهش فروش گوشی‌های هوشمند در سال آینده را پیش‌بینی می‌کند. به گزارش زومیت، درعین‌حال ساعت‌های هوشمند در سال‌های ابتدایی ورود به بازار فروش خوبی نداشتند و با استقبال کاربران مواجه نشدند، اما در سال ۲۰۱۵ با معرفی ساعت‌های هوشمند زیبا، بار دیگر فروش این گجت‌های پوشیدنی رونق گرفت و پیش‌بینی‌ها از سوی تحلیلگران وال‌استریت نشان از صعود بیشتر فروش این گجت‌ها در سال‌های آینده دارند. سال ۲۰۱۴ فقط ۶،۸ میلیون دستگاه ساعت هوشمند فروخته شد که سامسونگ با سری گیر خود ۱،۲ میلیون از این تعداد را به خود اختصاص داده بود. پیل بعد از سامسونگ با فروش ۷۰۰ هزار دستگاه در جایگاه دوم قرار داشت و جایگاه‌های بعدی متعلق به موتورولا، ال‌جی و دیگر شرکت‌ها بود. اندروید نیز در سال ۲۰۱۴ با استقبال خوبی روبه‌رو نشد و تنها ۷۲۰ هزار دستگاه ساعت هوشمند دارای این سیستم‌عامل فروخته شد؛ چراکه سامسونگ نیز از این سیستم‌عامل بهره نمی‌برد. اپل واچ با فروش هفت میلیون دستگاه با اختلاف، بیشترین فروش را بین ساعت‌های هوشمند داشته و انتظار می‌رود رقم کل فروش ساعت‌های هوشمند در سال جاری به ۲۱،۳ میلیون دستگاه برسد. بنابر گزارش جدید منتشرشده از سوی مؤسسه داده‌های بین‌المللی، پنج سال آینده برای ابزارهای پوشیدنی سال بسیار خوبی خواهد بود و تا سال ۲۰۱۹ بیش از ۲۱۴ میلیون دستگاه از این ابزارها به فروش خواهد رسید که بسیار بیشتر از ۷۰ میلیون دستگاه ابزار پوشیدنی است که تا به امروز و از زمان معرفی این گجت‌ها به فروش رسیده که البته بخش اعظمی از این ۷۰ میلیون را نیز ساعت‌های هوشمند به خود اختصاص داده‌اند. انتظار می‌رود سال آینده، ۳۴،۶ میلیون دستگاه ابزار پوشیدنی به فروش برسد که در مقایسه با سال قبل ۶۲ درصد افزایش را نشان می‌دهد. در سال ۲۰۱۹ فروش ساعت‌های هوشمند، به ۸۸،۳ میلیون دستگاه خواهد رسید که در بازه پنج‌ساله بیش از ۴۲،۸ درصد رشد خواهد داشت. بنابر پیش‌بینی‌ها، اپل با ساعت هوشمند خود حکمران بازار خواهد بود و با فروش ۴۵،۲ میلیون دستگاه اپل واچ، ۵۰ درصد بازار در سال ۲۰۱۹ را در دست خواهد داشت. اندروید نیز با ۳۴،۴ میلیون دستگاه در رده دوم قرار خواهد داشت و باقی‌مانده فروش به شرکت‌هایی اختصاص خواهد یافت که از سیستم‌عاملی غیراندروید و Watch OS بهره می‌برند. این شرکت‌ها شامل سازندگانی مانند پیل می‌شود، اما جایگاه سامسونگ در این بین مشخص نشده و این در حالی است که سامسونگ با معرفی گیر اس۲ ظاهرا موفقیت خوبی در بازار داشته است. این گزارش IDC پس از گذشت سه ماه از اولین گزارش این مؤسسه منتشر شده است. در ماه سپتامبر IDC پیش‌بینی کرده بود تا سال ۲۰۱۹ فروش کل ابزارهای هوشمند پوشیدنی به ۱۷۳،۴ میلیون دستگاه برسد، اما در پیش‌بینی‌های جدید شاهد رشد چشمگیری هستیم.

بازتاب

غوغای سایبری در راه است

● چندین سال است که هکرها به سازمان‌های مهم دولتی در کشورهای مختلف حمله می‌کنند و گاهی خسارات جبران‌ناپذیری به سیستم‌های آنها وارد می‌کنند. مؤسسه تحقیقات پیشرفته دفاعی آمریکا (دارپا) به‌تازگی اعلام کرده زمان آن رسیده که در این‌باره حرکتی انجام شود. به همین منظور وزارت دفاع آمریکا؛ پنتاگون اقدام به راه‌اندازی بخشی در این سازمان به‌نام شناسایی سریع حمله؛ ایزوله‌کردن و توصیف خصوصیات (RADICS) کرده است. هدف از راه‌اندازی این بخش توسعه راهکارهای نوین فناوری برای شناسایی سریع و خنثی‌کردن حملات سایبری است. البته این برنامه شامل تمام حملات نمی‌شود، بلکه پنتاگون به دنبال تهدیداتی است که به زیرساخت‌های مهم آمریکا حمله می‌کنند. آنها در تلاش‌اند بتوانند خیلی سریع هرگونه تلاش تروریست‌ها و هکرها برای ازکار انداختن سیستم‌های حمل‌ونقل و برق‌رسانی را خنثی کنند. قرار است ماه آینده میلادی دارپا در جلسه‌ای با شرکت‌های فعال در حوزه فناوری به گفت‌وگو بشنیند تا راه‌های همکاری با آنها در این پروژه مهم بررسی شود. بعد از این جلسه مشخص می‌شود دارپا روی کدام فناوری‌ها سرمایه‌گذاری می‌کند. دو ماه پیش نیز پنتاگون در بیانیه‌ای اعلام کرد در حال کار بر روی سیستمی است که هرگونه حمله به اطلاعات کارمندان دولت فدرال آمریکا و پایگاه‌های نظامی را در مراحل اولیه شناسایی و خنثی می‌کند.

به گزارش خبرآنلاین، هدف این برنامه مواجهه‌ای است با آنچه «قیامت سایبری» خوانده می‌شود تا در صورت ازبین‌رفتن تأسیسات زیربنایی مرتبط با انرژی و سوخت، بتواند این کشور را همچنان زنده نگه دارد! طبق این برنامه، هفت روز طول می‌کشد تا پس از حمله، تأسیسات ضروری در سراسر آمریکا دوباره به فعالیت خود ادامه دهند. البته جان اورت، مدیر برنامه‌های دارپا می‌گوید اگر امروز قیامت سایبری رخ دهد، چالش بزرگ امنیت ملی خواهند داشت؛ چراکه علاوه بر آسیب‌های اقتصادی و هزینه‌های انسانی، برای سرپانگه‌داشتن لجستیک نظامی نیز باید هزینه‌های زیادی متحمل شد که این موضوع کار را در برابر بحران‌های بین‌المللی ناشی از حملات سایبری افزایش می‌دهد. ظاهرا در گزارش‌های دارپا، تأسیسات اتمی، ایمن گزارش شده‌اند که کمترین حمله سایبری را خواهند داشت.