گزارش کوتاه

باریک‌ترین گوشی تلفن همراه

شرق: یک شرکت کره‌ای به تازگی باریک‌ترین گوشی‌های تلفن همراه موجود در جهان را به بازار عرضه کرده است.

تلفن‌های سری اولترای (Ultra Edition) در حال حاضر باریک‌ترین گوشی‌های تلفن همراه موجود در جهان محسوب می‌شوند. این گوشی‌ها در سه مدل اولترا ادیشن ۶/۹، اولترا ادیشن ۹/۹ و اولترا ادیشن ۱۲/۹ به بازار عرضه شده‌اند و هر یک در نوع خود در زمینه ضخامت رکوردشکنی کرده‌اند. در حالی که مارک‌های مشهورتر موجود در بازار تلفن همراه با شعار کیفیت و کارایی مشتریان را به سوی خود جلب می‌کنند، این شرکت برنامه تبلیغاتی وسیعی را برای جا انداختن این گوشی‌ها در بازار آغاز کرده است و این گونه رکوردشکنی‌ها می‌تواند موجب محبوبیت گوشی‌های سامسونگ نزد گروه‌های خاصی از مصرف‌کنندگان شود.

اولترا ادیشن ۶/۹، همان‌طور که از نامش پیدا است با ضخامتی معادل ۶/۹ میلی‌متر، باریک‌ترین گوشی تلفن همراه موجود در جهان است. این گوشی تنها ۶۶ گرم وزن دارد، به یک دوربین ۲ مگاپیکسلی مجهز است و قابلیت پخش فایل‌های موسیقی دیجیتالی را هم دارد. اولترا ادیشن ۹/۹ هم با ضخامتی کمتر از ۱۰ میلی‌متر باریک‌ترین گوشی کشویی جهان محسوب می‌شود و علاوه بر امکانات مدل ۶/۹، امکان افزایش حافظه از طریق اتصال کارت حافظه را هم دارد. اولترا ادیشن ۱۲/۹ هم با ضخامتی کمتر از ۱۳ میلی‌متر باریک‌ترین گوشی کشویی جهان محسوب می‌شود و مجهز به یک دوربین ۳ مگاپیکسل اتوفوکوس است.

ایل چونگ چانگ از مدیران ارشد سامسونگ در مورد اهمیت بازار خاورمیانه و برنامه‌های این شرکت برای دستیابی به سهم بیشتری از بازار رو به رشد این منطقه، از عملکرد شرکت در بازار تلفن همراه ایران مثال می‌آورد و می‌گوید: «ما اولین شرکتی بودیم که نیاز مصرف‌کنندگان ایرانی به منشی تلفنی را احساس کرد و این امکان را منحصراً برای بازار ایران فعال کرد.» وجود امکان ارسال پیام صوتی (Voice Mail) در شبکه‌های تلفن همراه کشورهای توسعه‌یافته، نیاز به

منشی تلفنی را منتفی می‌کند و به همین خاطر در حال حاضر کمتر گوشی تلفن همراهی در جهان دارای این قابلیت است.

وی در ادامه با اشاره به منوهای فارسی، تقویم شمسی و انتشار دفترچه راهنمای فارسی از سال‌ها پیش، توجه به نیازهای خاص منطقه‌ای را یکی از استراتژی‌های بازاریابی ذکر می‌کند و می‌گوید: «گوشی‌های سری اولترا این امکانات منطقه‌ای را افزایش می‌دهند. مثلاً اگر کاربری با یکی از گوشی‌های اولترا وارد ایران شود، گوشی با تشخیص اپراتور ایرانی، تصویر زمینه و اطلاعات مفیدی درباره ایران را در اختیار کاربر می‌گذارد.»

ام‌پی‌تری‌پلیر جدید با ویژگی‌های برتر

ایرنا: شرکت «سن‌دیسک» دستگاه «ام‌پی‌تری‌پلیر» جدیدی به بازار داده‌است که با قیمتی مشابه، قابلیت‌ها و ویژگی‌های بسیار بیشتری را در مقایسه با دستگاه‌های مشابه «آی‌پاد» شرکت «اپل» ارائه می‌دهد. دستگاه جدید «سن دیسک» که بیشتر شهرت خود را در زمینه تولید کارت‌های حافظه پیشرفته کسب کرده، «سن‌دیسک‌پی ۲۸۰» نام دارد. این دستگاه با ۸ گیگابایت حافظه تنها ۲۴۹ دلار قیمت دارد و این در حالی است که شرکت «اپل» مدل «آی‌پاد نانو» از دستگاه‌های ام‌پی‌تری‌پلیر خود را که تنها ۴ گیگابایت گنجایش داشته و از امکانات کمتری نیز برخوردار است، با همین قیمت عرضه می‌کند. دستگاه جدید شرکت «سن دیسک» به علاوه به قابلیت استفاده از کارت‌های حافظه از نوع «مایکرو» اس‌دی» نیز مجهز است و از آنجایی که همین شرکت کارت‌های حافظه «مایکرو اس‌دی» با گنجایش دو گیگابایت را نیز به بازار داده، با توجه به حافظه ۸ گیگابایتی داخلی این دستگاه می‌توان با استفاده از کارت حافظه به گنجایش ۱۰ گیگابایتی دست یابد. این دستگاه به گیرنده امواج رادیویی اف‌ام، قابلیت ضبط صدا و همچنین قابلیت پخش تصاویر ویدئویی نیز مجهز است که هیچ‌کدام از این قابلیت‌ها در دستگاه «آی‌پاد نانو» دیده نمی‌شوند. اقدام «سن‌دیسک» در زمینه معرفی این محصول جدید در حالی صورت می‌گیرد که شرکت «مایکروسافت» نیز کم‌کم خود را برای عرضه دستگاه مشابه خود آماده می‌کند. دستگاه «ام‌پی‌تری‌پلیر» شرکت مایکروسافت با نام «زیون» توسط شرکت «توشیبا» تولید خواهد شد و دارای یک صفحه نمایش رنگی کریستال مایع بوده، از یک هارددیسک ۳۰ گیگابایتی استفاده کرده و به انواع فناوری‌های ارتباط بی‌سیم مجهز خواهد بود.

این گروه خشن

نگاهی به جنایات و تبهکاری الکترونیکی

نیر کشتری
ترجمه: بهروز حاجیان

انتشار ویروس‌ها و کرم‌های رایانه‌ای، انجام حملات الکترونیکی و به‌طور کلی هرگونه فعالیتی که سبب ایجاد اخلال در شبکه‌های رایانه‌ای و امور مبتنی بر آن شود، جرایم الکترونیکی یا در بیان کلی‌تر جرایم سایبری نامیده می‌شوند. این گونه جدید جنایت و این چهره جدید دنیای تبهکاری واجد ویژگی‌های منحصر به فردی است که کشف، پیگیری و رسیدگی آن را سخت و دشوار و مقابله با آن را برای کشورهایی که در زیرساخت‌های ملی خود از مفاهیم فناوری اطلاعات بهره می‌برند، بسیار حیاتی کرده است. این نوشتار براساس آمار موجود در این خصوص، به تجرید و بررسی این پدیده جدید عصر الکترونیک و ناهنجاری اجتماعی حاصل از دنیای فناوری اطلاعات می‌پردازد. نوشتار حاضر برگردان مقاله‌ای است با عنوان «اقتصاد آسان جنایات سایبری» که در شماره گذشته مجله IEEE Security & Privacy منتشرشده است.

▪▪▪

با گسترش فناوری اطلاعات در بخش‌های مختلف امور اجتماعی و توجه بیشتر به مفاهیمی چون دولت و تجارت الکترونیک و به‌طور کلی توسعه دنیای مبتنی بر رایانه‌ها در تعاملات اداری، جرایم سایبری نیز گسترش یافته و با افزایش بهره مالی و اقتصادی آنها، از پیچیدگی بیشتری برخوردار می‌شوند.

طبق گزارش FBI در ژوئن سال ۲۰۰۲ میلادی در هر لحظه به‌طور متوسط ۵۰۰ کمپانی مورد حمله جنایتکاران سایبری قرار گرفته‌اند. طی بررسی انجام شده توسط شرکت MailFrontier (فعال در زمینه امنیت پست الکترونیک) در طول ماه سپتامبر سال ۲۰۰۳ میلادی حدود ۸۰ میلیون نامه الکترونیکی با مقاصد جنایتکارانه منتشر شده‌اند به‌طوری که این رقم نسبت به ماه قبل آن در همان سال ۴۳ درصد افزایش داشته است. در گزارشی دیگر و به نقل از Wall Street Journal در شماره جولای سال گذشته میلادی، ۵۳ درصد از دادخواهی‌های مالی ارائه شده به کمیسیون بازرگانی ایالات متحده در سال ۲۰۰۴ مربوط به جرایم الکترونیکی بوده‌اند. افزایش جرایم سایبری و حملات انجام شده بر علیه شرکت‌ها و موسسات آمریکایی به حدی است که دولت آن کشور و FBI مسئله مبارزه و مقابله با آن را به عنوان یکی از اولویت‌های اصلی خود پس از ضدتروریسم و ضدجاسوسی قرارداده است.

به منظور مقابله با این گونه جدید جنایت و جلوگیری از رشد آن در جامعه ابتدا باید به درک صحیح و روشنی از مشخصات، ویژگی‌ها، جذابیت‌ها و ریشه‌های آن در جوامع مختلف دست یافت. جرایم سایبری از نقطه‌نظر ساختاری واجد سه ویژگی منحصر به فرد هستند:

▪ انجام جرایم سایبری نیازمند دانش، فناوری و مهارت‌های تخصصی است.

▪ جرایم سایبری وابسته به مکان نبوده و از درجه جهانی بودن بالاتری نسبت به سایر گونه‌های جرم و جنایت برخوردارند.

▪ جرایم سایبری نسبتاً جدید بوده و بسیاری از جنبه‌های آنها ناشناخته است.

جرایم سایبری را می‌توان در معنی جامع آن به هرگونه فعالیتی که شبکه‌های رایانه‌ای را به منظور انجام تبهکاری به خدمت می‌گیرد، اطلاق کرد. براساس این تعریف، اقداماتی چون حمله الکترونیکی به زیرساخت‌های حیاتی و ملی کشورها، کلاهبرداری و پولشویی الکترونیکی، استفاده جنایتکارانه از اینترنت، جعل ID و حتی استفاده از رایانه و مفاهیم فناوری اطلاعات در جریان جنایات غیرسایبری مصداق‌هایی از جرایم سایبری است.

مجریان قانون در ایالات متحده نظیر نیروی پلیس و FBI واجد تجربه لازم به منظور مقابله با این چهره جدید جنایت نیستند. یکی از مشکلات جدی و اساسی مجریان قانون در این خصوص، کمبود نیروی انسانی متخصص در این حوزه است. بر طبق گزارش واشینگتن پست (شماره ۱۷ مه سال ۲۰۰۰ میلادی) تنها ۲ درصد از نیروی پلیس ایالات متحده در این زمینه آموزش دیده‌اند. رشد سریع فناوری و سیر صعودی دانش به‌کار رفته در جرایم الکترونیکی در کنار روش‌های جدید و متفاوت استفاده شده توسط تبهکاران سایبری، مشکل بعدی برای مقابله با آنها است. مجریان قانون به سبب فقدان منابع لازم، امکان برتری جستن در فناوری به خدمت گرفته شده توسط مجرمان سایبری را ندارند. بنابر اشاره مجله Business Week (شماره ۳۰ مه سال ۲۰۰۵ میلادی) «نیروی پلیس اسلحه لازم به منظور مقابله با مجرمان سایبری را در اختیار ندارد. کاملاً آشکار است به دلیل فقدان منابع مالی لازم امکان مقابله مجریان قانون با مهارت‌های فنی مجرمان و توسعه جهانی جرایم الکترونیکی وجود ندارد.»

پیگیری و کشف جرایم سایبری نیز بسیار پیچیده و مستلزم در اختیار داشتن دانش و خبرگی لازم است، به‌طوری که بسیاری از کشورها واجد توانایی کافی به منظور بررسی دقیق جرایم گزارش شده نیستند. به‌طور مثال در اندونزی مجریان قانون تنها قادر به بررسی و رسیدگی ۱۵ درصد از کل جرایم الکترونیکی گزارش شده هستند. عدم توانایی نیروی پلیس و مجریان قانون در رسیدگی به جرایم سایبری، افزایش اعتماد به نفس مجرمان در انجام جرایم و بی‌رغبتی قربانیان در گزارش موارد جرم و جنایت واقع شده را به همراه خواهد داشت. ثبت شرح حال و سوابق مجرمان سایبری با روش‌های جاری نگهداری و بررسی سوابق در ساختارهای قضایی متفاوت است. عدم وجود بانک اطلاعاتی جامع از شرح حال و سوابق مجرمان و جرم‌های سایبری واقع شده مشکل دیگر پیش‌روی مراجع قضایی در پیگیری جرایم سایبری است که توانایی آنان را در رسیدگی به جرایم واقع شده در این دنیای نوظهور تبهکاری محدود می‌نماید.

یکی از مشخصه‌های جرایم سایبری در مقایسه با روش‌های جاری تبهکاری، عدم وابستگی آنها به محل و منطقه بومی مجرمان است. مرزهای جغرافیایی و فواصل برای جانیان محدودیتی محسوب نمی‌شود و همان‌طور که فناوری اطلاعات ارتباطات را آسان‌تر، فواصل را کوتاه‌تر و تعاملات را بیشتر می‌کند، فعالیت مجرمان نیز در این دنیای جدید آسان می‌شود. گمنامی موجود در این فضا در کنار عدم وابستگی به مکان، جرم و جنایت در دنیای سایبری را بسیار پیچیده کرده و هرگونه کوشش بازدارنده در این حوزه را از مرحله پیشگیری، تشخیص و پیگیری تا مراحل صدور احکام قضایی بسیار دشوار می‌کند.

مرزهای بین المللی یکی از موانع اصلی در رسیدگی و پیگیری این گونه جرم و جنایت محسوب می‌شوند؛ چهره‌ای جدید از تبهکاری که در آن مرزهای جغرافیایی محدودیتی به‌شمار نمی‌آیند. احکام قضایی کشورها در این خصوص متفاوت بوده و مراجع قانونگذار و مجریان قانون در نقاط مختلف دنیا در این مورد همکاری مناسبی با یکدیگر ندارند. احکام قضایی در جوامع مختلف یکسان نبوده و در بسیاری از کشورها تاکنون تمهیدی در این خصوص نیندیشیده‌اند. به‌طور مثال به نقل از مجله Cnet News در شماره مه سال ۲۰۰۱ میلادی در توافقنامه موجود بین ایالات متحده و روسیه در زمینه کمک به کشور مقابل به‌منظور رسیدگی و پیگیری جرایم، به جنایات سایبری اشاره نشده و توافق‌های دو کشور شامل تبهکاری و جرایم سایبری و الکترونیکی نمی‌شود. تاکنون موارد متعددی از حمله هکرهای روسی به منابع آمریکایی ثبت شده است ولی پیگیری آنها از مراجع قضایی روسیه به‌رغم ارائه مدارک لازم توسط طرف‌های آمریکایی درخصوص محل، مبدأ و جزئیات حمله انجام شده، همواره بی‌پاسخ و بی‌نتیجه بوده است.

در یکی از موارد FBI در پی عدم دریافت پاسخ مناسب از مراجع قضایی به منظور تحویل دو هکر به ناچار با تطمیع مظنونان، به صورت مخفی با پیشنهاد شغلی مناسب در ایالات متحده موفق به دستگیری آنها شد. در موردی مشابه پس از انتشار ویروس Love Letter توسط یک فیلیپینی در سال ۲۰۰۰ میلادی که تنها در ایالات متحده حدود ۱۵ میلیارد دلار خسارت ایجاد کرد، دولت آمریکا به دلیل عدم وجود قوانین بین المللی و احکام قضایی مرتبط در کشور فیلیپین، هیچ‌گاه نتوانست از دولت آن کشور ادعای خسارت کرده یا مجرم مورد نظر را تحت پیگرد قانونی قرار دهد. بسیاری از خبرگان این حوزه با ارجاع به شواهد و مدارک موجود معتقدند مادام که انجام جرایم سایبری و حملات الکترونیکی خطری برای منافع ملی کشورهایی نظیر چین و روسیه محسوب نشود، اقدامی درخصوص مقابله و مبارزه با آنها نکرده و برای اجماع جهانی به‌منظور رسیدگی و پیگیری جرایم سایبری تلاش نمی‌کنند.

برخلاف سستی کشورها در رسیدن به اجماع بین‌المللی به‌منظور مقابله و مبارزه با جنایات و مجرمان سایبری و تدوین احکام قضایی مربوطه، تبهکاران به شکل گسترده‌ای مشغول شناسایی یکدیگر و تشکیل شبکه‌های تبهکاری بین المللی هستند. به گزارش مجله The Economist در شماره آگوست سال ۱۹۹۹ میلادی به تازگی مواردی از اجیر شدن هکرهای روسی توسط تبهکاران ژاپنی به منظور حمله به بانک‌های اطلاعاتی مجریان قانون مشاهده شده است.

بی‌میلی قربانیان جنایات سایبری برای گزارش موارد جرم و جنایت واقع شده به مراجع قضایی و مجریان قانون، معضل دیگر در مقابله و مبارزه با این گونه جدید تبهکاری است. به نقل از یک پایگاه اینترنتی تنها ۱۷ درصد از شرکت‌ها در سال ۲۰۰۱ میلادی حملات و جنایات الکترونیکی انجام شده علیه خود را به مراجع قضایی گزارش کرده‌اند. نگرانی از دست رفتن اعتماد کاربران، ترس از کاهش اعتبار و عدم اطمینان از توانایی مقابله قانونی با مجرمان و احقاق حقوق از دست رفته، عامل اصلی در بی انگیزگی شرکت‌ها، بانک‌ها، شرکت‌های بیمه و به‌طور کلی قربانیان برای گزارش جنایت به مجریان قانون است.

یکی دیگر از پیامدهای عصر الکترونیک و چهره دیگر تبهکاری در این دنیای نو، زورگیری سایبری (Cyberextortion) است. قربانیان عموماً به دلایل اشاره شده حاضر به توافق با زورگیران (Cyberextortionists) و پرداخت باج مورد درخواست آنها می‌شوند. در بسیاری از موارد هدف تبهکاران الکترونیکی نفوذ و دسترسی به اسناد محرمانه پایگاه اطلاعاتی شرکت خاصی نیست، بلکه تنها جلوگیری از دسترسی کاربران و مشتریان برای مدتی محدود نیز ممکن است خسارت قابل توجهی را به قربانی تحمیل کند (حملاتی از این نوع که بیشترین حملات رایانه‌ای انجام شده طی سال‌های اخیر است DoS Attack یا حملات جلوگیری از دسترسی نام دارند. یکی از نخستین حملات این گروه Sync Attack است که بر مبنای نقطه ضعفی در ساختار TCP-IP طراحی شده است. اگرچه در نگاه اول نبوغ به‌کار رفته در طراحی و اجرای بسیاری از حملات انسان را به تحسین وادار می‌نماید ولی با مشاهده عواقب دهشت‌بار آنها چاره‌ای جز تکفیر باقی نمی‌ماند). به گزارش سایت خبری CNN تنها چند ساعت جلوگیری از دسترسی به سایت‌های شناخته شده و پرمراجعه سرگرمی و شرط‌بندی به ویژه در ایام آخر هفته و ساعت‌های شلوغ روز، خسارتی بالغ بر یک میلیون دلار برای قربانی به همراه خواهد داشت. پرواضح است پرداخت چندین هزار دلار باج بهتر از عدم کسب سودهای چند میلیون دلاری آخر هفته خواهد بود. علاوه بر اینکه تکرار عدم امکان دسترسی به یک سایت، بی‌اعتمادی کاربران و از دست رفتن مشتریان را در دراز مدت به همراه خواهد داشت. به عنوان مثال در سپتامبر سال ۲۰۰۳ میلادی یکی از شرکت‌های سرگرمی (World Wide Tele-sports) در پی حمله به شبکه رایانه‌ای آن و تهدید به جلوگیری از دسترسی مشتریان به سایت (که پیش‌بینی می‌شد خسارتی حدود ۵ میلیون دلار به همراه داشته باشد) ناگزیر به پرداخت سی هزار دلار به حمله‌گرهای روسی شد. اگرچه پس از هر تهدید تمهیدات لازم به‌منظور مصونیت در مقابل حمله انجام شده و حمله‌های مشابه در نظر گرفته می‌شود و گزیده شدن مجدد از آن حفره ممکن نخواهد بود، ولی طبق یک اصل در حوزه امنیت رایانه، همواره حفره‌ای برای گزیده شدن وجود دارد.

انگیزه‌های انجام جرایم سایبری با گذشت زمان تغییر کرده‌اند. پیش از این و مستقل از فعالیت‌های سازمان یافته حکومت‌ها در این خصوص، خودنمایی و تظاهر مهمترین محرک مجرمان محسوب می‌شد. بسیاری از ویروس‌ها، کرم‌های رایانه‌ای، اسب‌های تروا و حمله‌های رایانه‌ای بدون هدف و انگیزه خاص و تنها به‌منظور اعلام وجود تعریف و طراحی شده‌اند. هکرهای Maverick و Honker Union یا هکرهای سرخ در چین نمونه‌های بارزی از انگیزه‌های صرفاً روانی در انجام حمله‌های الکترونیکی و رایانه‌ای است. انگیزه‌های سیاسی، خاستگاه فکری برخی دیگر از حمله‌های رایانه‌ای مشاهده شده در سال‌های اخیر است. حمله یک گروه شش نفره از ایالات متحده، انگلستان، هلند و نیوزیلند با نام Milworm به سایت اینترنتی مرکز تحقیقات اتمی Bhabha هند در سال ۱۹۹۸ و حمله گروه Cyberjihad اندونزی به سایت نیروی پلیس آن کشور به‌منظور آزادسازی یکی از رهبران مبارز در سال ۲۰۰۱ نمونه‌هایی از انجام حمله‌های رایانه‌ای با اهداف سیاسی است. در سال‌های اخیر اهداف و انگیزه‌های انجام جرم و جنایت سایبری تغییر کرده و برخلاف قبل بیشترین محرک مجرمان سایبری انگیزه‌های مادی است. بر طبق آمار ارائه شده توسط Usatoday به نقل از یک شرکت تحقیقاتی فعال در این حوزه، ۶۰ درصد اهداف هکرها در سال ۲۰۰۳ میلادی موسسات مالی و بازرگانی بوده‌اند.

پرواضح است مقابله با جرایم سایبری بدون اجماع بین المللی و مشارکت تمامی کشورها ممکن نیست. کشورهای صنعتی و جوامعی که از فناوری اطلاعات در زیرساخت‌های ملی و اقتصادی خود بهره می‌گیرند، قربانیان اصلی حملات و جنایات سایبری هستند. در این جوامع عموماً احکام قضایی مرتبط تدوین شده، پیگیری و کشف جرایم سایبری و صدور احکام قضایی علیه مجرمان ممکن است. در مقابل کشورهایی که در ساختار دادرسی خود فاقد احکام قضایی لازم در این خصوص هستند مامن مناسبی برای تبهکاران سایبری محسوب شده و بستر مناسبی را برای رشد جرایم رایانه‌ای فراهم می‌کنند. بسیاری از ویروس‌های سهمگین نظیر Love Bug در کشورهای در حال توسعه طراحی شده ولی آثار مخرب خود را به جوامع اقتصادی تحمیل کرده است. در حال حاضر موسسه‌هایی نظیر National Hi-Tech Crime Unit و National White Collar Crime به ترتیب در انگلستان و ایالات متحده به‌منظور مبارزه با حملات الکترونیکی و تبهکاران سایبری ایجاد شده‌اند ولی پرواضح است هرگونه فعالیتی در این خصوص نتیجه مناسبی نخواهد داشت مگر در صورت مشارکت تمامی ملل، خصوصاً کشورهایی که تاکنون قانونی در منع جرایم سایبری تدوین نکرده‌اند و پناهگاه مجرمان و مبدا بسیاری از حملات الکترونیکی هستند.

***دانشگاه کارولینای شمالی**
Computer.org

کشورهای مبدأ بیشترین کلاهبرداری بر خط	رتبه بر اساس درصد کلاهبرداری الکترونیکی	رتبه بر اساس میزان حملات اینترنتی به ازای هر ۱۰۰۰۰۰ کاربر	تعداد حملات اینترنتی به ازای هر ۱۰۰۰۰۰ کاربر	درصد کل حملات الکترونیکی
اکراین	یوگسلاوی (۱)	پاناما	کویت (۵۰/۸)	آمریکا (۵۰)
اندونزی	نیجریه (۲)	هنگ کنگ	اسرائیل (۳۳/۱)	آلمان (۷/۶)
یوگسلاوی	رومانی (۳)	ماکائو	ایران (۳۰/۸)	کره شمالی (۷/۴)
لیتوانی	پاکستان (۴)	قطر	پرو (۲۶/۵)	چین (۶/۹)
مصر	اندونزی (۵)	اسرائیل	شیلی (۲۶/۴)	فرانسه (۵/۲)
رومانی	مقدونیه (۶)	ترکیه	نیجریه (۲۳/۶)	کانادا (۳)
بلغارستان	بلغارستان (۷)	بوسنی و هرزگوین	مراکش (۲۲/۳)	ایتالیا (۲/۷)
ترکیه	اکراین (۸)	کانادا	هنگ کنگ (۲۲/۱)	تایوان (۲/۴)
روسیه	لبنان (۹)	نوکاعبورگ	پرتوریکو (۲۰/۸)	انگلستان (۲/۱)
پاکستان	لیتوانی (۱۰)	اسپانیا	فرانسه (۱۹/۹)	ژاپن (۲/۱)
مالزی			آرژانتین (۱۹/۳)	
اسرائیل			بلژیک (۱۷/۶)	
			رومانی (۱۶/۵)	

آمار برخی جرائم سایبری انجام شده در کشورهای مختلف

خبرها

تلفن همراه به‌عنوان تلفن اینترنتی

ایسنا: اپراتور مخابراتی «تلیا سونرا» برای نخستین بار در جهان، فناوری UMA را عرضه کرد که به کاربران امکان می‌دهد تا به تلفن اینترنت (IP) و تلفن همراه از طریق همان تلفن دسترسی داشته باشند. فناوری یاد شده این امکان را فراهم می‌کند تا کاربران از تلفن همراه به عنوان IP Phone استفاده کنند، که در آن با استفاده از فناوری وایرلس تماس‌ها بسیار کم‌هزینه می‌شود. همین دستگاه تلفن در خارج از خانه به عنوان یک گوشی معمولی تلفن همراه استفاده می‌شود که به طور اتوماتیک به شبکه موبایل متصل است. سخنگوی شرکت «تلیا سونرا» اعلام کرد: چنانچه کاربران در منطقه تحت پوشش Wi-Fi باشند، از این فناوری می‌توان در آینده به عنوان یک IP استفاده کرد.

همکاری چین و دیگر کشورها

ایرنا: جمهوری خلق چین آمادگی خود را برای ایجاد و گسترش همکاری در صنعت فضا با کشورهای دیگر جهان اعلام کرد. روزنامه «چاینا دیلی» چاپ پکن روز سه‌شنبه به نقل از «جین جوانگ لونگ» معاون کمیسیون علوم و فنون صنایع دفاع ملی چین نوشت: چین ۱۶ توافقنامه با ۱۳ دولت و سازمان بین المللی درباره همکاری‌های فضایی امضا کرده و در زمان حاضر با ۴۰ کشور و سازمان همکاری‌های فضایی دارد. وی گفت: چین به دنبال افزایش سهم خود در بازار پرتاب ماهواره‌ها و دیگر خدمات فضایی در جهان است. این مقام چینی افزود: «تقویت همکاری فضایی چین با روسیه، اوکراین و کشورهای اروپایی و آمریکای لاتین از جمله شیلی، آرژانتین و پرو در زمینه علوم فضایی چشمگیر است و همکاری فضایی چین با آمریکا و کانادا نیز در حال توسعه است.» به گفته وی چین در آسیا به‌دنبال گسترش همکاری با سازمان همکاری فضایی آسیا و اقیانوسیه است و قرار شده این سازمان در شهر پکن فعال شود.

دومین خودروساز جهان و موسیقی

ایسنا: تلفن همراه تویوتا امکان دانلود رایگان موسیقی و بازی را از داخل خودرو می‌دهد. شرکت خودروسازی تویوتا از ساخت یک تلفن همراه جدید خبر داد که به رانندگان کمک می‌کند به سرویس‌های مسیریابی خودرو بسیار آسان‌تر دسترسی داشته باشند. تویوتا اعلام کرد: فروش این تلفن همراه جدید که (TiMO) نام دارد، از اواخر اکتبر آغاز خواهد شد و تنها در نمایندگی‌های تویوتا در داخل ژاپن به فروش می‌رسد. تلفن همراه محصول تویوتا با سیستم مسیریابی در خودروهای ساخت این شرکت، که از فناوری وایرلس بلوتوث استفاده می‌کنند، سازگار است. همچنین یک شارژر باتری برای این تلفن همراه طراحی شده است که به کنار دنده متصل می‌شود و می‌توان از طریق آن به دانلود موسیقی و بازی‌ها به طور رایگان اقدام کرد؛ رانندگان همچنین در مواقع اضطراری می‌توانند با فشار دادن تنها یک دکمه تلفن همراه درخواست کمک کنند. براساس اعلام تویوتا، شرکت فناوری KDDI در طراحی این تلفن همراه جدید با تویوتا همکاری داشته است.

جلسه استاندارد سازی باتری

ایسنا: به دنبال فراخوانی‌های اخیر اپل و دل در ماه گذشته، این دو شرکت در ماه آینده به همراه دیگر شرکت‌های تولیدکننده رایانه، جلسه‌ای برای بحث در مورد طراحی و استاندارد و ایمنی باتری‌های یون‌لیتیوم، برگزار می‌کنند. این جلسه در حالی در سیزدهم سپتامبر در کالیفرنیا برگزار خواهد شد که شرکت سونی، که سازنده باتری‌های فراخوان شده است، حضور خود در این جلسه را اعلام نکرده است. به گفته مسئولان برگزاری جلسه، این نشست پیش از فراخوان ۴/۱ میلیونی دل و ۱/۸ میلیونی اپل در آگوست، برنامه‌ریزی شده بود.

تحقق ۴۰ درصد از پیش‌بینی ژاپنی‌ها

ایرنا: نتایج بررسی‌های پژوهشگران وابسته به وزارت آموزش، علوم، فناوری، فرهنگ و ورزش ژاپن نمایانگر آن است که ۴۰ درصد از پیش‌بینی‌های علمی که سازمان وقت علوم و فناوری این کشور در ۴۶ سال پیش انجام داده، به واقعیت پیوسته است. بر پایه گزارش روز سه‌شنبه روزنامه یومیوری، از ۱۳۵ مورد پیش‌بینی علمی سازمان علوم و فناوری وقت ژاپن، ۵۴ مورد از آن به واقعیت پیوسته است. سازمان علوم و فناوری ژاپن در سال ۱۹۶۰ میلادی پیش‌بینی کرده بود که این موارد تا اوایل قرن بیست‌ویکم عملی می‌شوند. تلفن همراه، دستگاه مایکروویو، لقاح مصنوعی، نگهداری جاودانی اسپرم، واژه‌نگاری از طریق صدا، از نمونه پیش‌بینی‌های علمی بوده که به واقعیت پیوسته است. پیش‌بینی‌های این سازمان درباره ساختن فرودگاه فضایی بر روی دریا برای رفتن به کره ماه، انجام کارهای خانه از سوی خدمتکارهای الکترونیکی، از میان رفتن مترو از مواردی است که تاکنون تحقق نیافته است.

ارزان‌ترین تلفن‌های همراه موتورولا

ایسنا: شرکت موتورولا از برنامه جدید خود برای توسعه و تولید ارزان‌قیمت‌ترین تلفن‌های همراه WIMAX برای استفاده در نسل آینده گوشی‌های WIMAX موتورولا خبر داد. موتورولا در نظر دارد با ارائه گوشی‌های طرح ارزان‌قیمت، بازار گوشی‌های مجهز به سرویس WIMAX را تحت کنترل خود در آورد. اولین سری از این نوع گوشی‌های ارزان‌قیمت در سال ۲۰۰۸ میلادی راهی بازارهای آمریکا و ژاپن خواهد شد.