گزارش
مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

شهریور ۱۴۰۰

امنیت سایبـــــری


بسم الله الرحمن الرحیم

فهرست

Iranian Council For
Defending The Truth

پیشگفتار

۱

پیشگفتار

مجمع ایران 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 سوءتفاهم ها 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

اطلاع از اخبار و وضعیت فضای سایبر در ایالات متحده این امکان را فراهم می‌سازد تا با مسائل و مشکلات این حوزه سریع‌تر آشنا شده و هم‌چنین پیش از این که کشور ما نیز به آن مصائب و دشواری‌ها دچار گردد، راهکارهای اصلاحی را پیش‌بینی نماییم. از طرفی، با توجه به این که در اظهارات عمومی و جلسات رسمی مقامات این کشور برخی از نقاط ضعف دشمن در زمینه سایبری و فناوری‌های نوین بیان می‌گردد و با توجه به این نکته که بخش سایبری ایران توانایی آن را دارد که در تقابل با ایالات متحده از همین ضعف‌ها بهره‌برداری کند و به دشمن ضربه بزند؛ فلذا می‌توانیم از نقاط ضعف حریف استفاده نماییم و زمین بازی را به نفع خود تغییر دهیم و در موضع آفندی قرار بگیریم.

این تذکر ضروری است که با توجه به پیشگامی کشور امریکا در عرصه تکنولوژی، بررسی پیشرفت‌ها و برنامه‌ریزی‌های کلان این کشور در زمینه فناوری پیش‌بینی مقصد نهایی مسیر تکنولوژی در آینده را ممکن می‌سازد.

در بولتنی که در اختیار دارید اهم اخبار و اتفاقات کلان حوزه سایبر، تکنولوژی و فناوری‌های نوین جمع‌آوری شده است تا مخاطبین و فعالین در این زمینه بتوانند نسبت به وضعیت ایالات متحده از نگاهی جامع، کلان و به‌روز برخوردار شوند.

دیدکلی

بسته خبری این هفته تحت چهار عنوان کلی«چالش افغانستان»، «شبکه‌های اجتماعی»، «ناامنی سایبری» و «بین الملل» تهیه شده است و اصلی‌ترین بخش خود را به بررسی ابعاد اطلاعاتی و شناختی بحران کنترل افغانستان توسط طالبان اختصاص داده است.

بررسی روند آخرین حمله‌های هکری مهم و گسترده در بخش ناامنی سایبری صورت پذیرفته است و بحث داغ هفته‌های اخیر در رابطه با به کارگیری نرم‌افزار جاسوسی پگاسوس،متعلق به شرکت اسرائیلی NSO ، توسط دولت بحرین در این قسمت مطرح شده است.

Iranian Council For
Defending The Truth

اخبار

۳


Data Breach
Cyber Attack

چالش افغانستان

تسلط طالبان بر جنگ اطلاعاتی

فروپاشی سریع ماموریت ۲۰ ساله غرب در افغانستان تنها یک روز به طول انجامید تا افراد مسلح طالبان یکشنبه ۱۵ اوت وارد کابل شوند. در نتیجه رئیس جمهور غنی به سرعت از این کشور فرار کرد و آمریکا با وحشت سفارت خود را ترک نمود. در نهایت نیز هدف طالبان برای تصاحب کنترل افغانستان و تاسیس مجدد امارت اسلامی محقق گردید.

سال هاست که طالبان از رسانه‌های اجتماعی برای انتشار پیام‌های خود استفاده می‌کند. در حقیقت، بیش از ۷۰ درصد از مردم افغانستان به تلفن‌های همراه دسترسی دارند و طالبان نیز خود را با این شرایط تطبیق داده است. طالبان از شیوه جنگ اطلاعاتی مدرن و روسی بهره جسته و از حساب‌ها و ربات‌های جعلی برای انتشار پیام‌های خود و تضعیف دولت افغانستان استفاده می‌نمود.

این عملگرایی نشان دهنده درک طالبان از این مطلب است که آنها نمی‌توانند مانند دهه ۱۹۹۰ در افغانستان حکومت کنند و طالبان به دنبال حفظ ارتباط این کشور با جهان و جاری شدن کمک‌های خارجی است. طالبان عملیات‌های اطلاعاتی از جمله درخواست از بزرگان قبایل را در کنار پیام‌های متنی و توییتری با دستورات غیر متمرکز ترکیب می‌کند تا به فرماندهان محلی خود که از وضعیت سیاسی در مناطق شان اطلاع دارند، مجال برای ابتکار عمل شخصی داده باشد.

رسانه‌های اجتماعی به عنوان بستر مهمی برای مشارکت سیاسی و تبلیغات توسط طالبان در جبهه‌های متعدد جنگ‌های اطلاعاتی استراتژیک مورد استفاده قرار گرفته است. طی بحران شکل گرفته، سرعت سقوط مراکز ولایات در افغانستان به عنصر مهمی در قصه طالبان مبدل گردید.

ممنوعیت فیس بوک برای محتوای مرتبط با طالبان

فیس بوک اعلام کرده است که طالبان و محتوای مربوط به آن را از بسترهای خود ممنوع می‌کند چرا که طالبان را یک گروه تروریستی می‌داند. این شرکت می‌گوید که یک تیم اختصاصی از کارشناسان افغان برای نظارت و حذف محتوای مرتبط با این گروه تشکیل داده است. تصرف سریع طالبان بر افغانستان چالش‌های جدیدی را برای شرکت‌های فناوری در مورد نحوه برخورد با محتواهای مربوط به این گروه ایجاد نمود.

سخنگوی فیس بوک به بی بی سی گفت:« طالبان تحت قوانین آمریکا به عنوان یک سازمان تروریستی تحریم شده و ما نیز ذیل سیاست‌های "سازمان‌های خطرناک" آنها را از خدمات خود منع کرده‌ایم... این بدان معناست که ما حساب‌هایی را که توسط طالبان یا از طرف طالبان حمایت می شود حذف می‌کنیم و تحسین، حمایت و نمایندگی از آنها را ممنوع می‌کنیم.»

تروریسم در اینترنت

تکنولوژی یکی از عوامل راهبردی است که استفاده روزافزون از اینترنت توسط سازمان‌های تروریستی و حامیان آنها را برای طیف وسیعی از اهداف

هدایت می‌کند؛ از جمله مقاصدی که سازمان‌های تروریستی در اینترنت دنبال می‌کنند عبارت اند از : جذب نیرو، تأمین مالی، تبلیغات، آموزش، تحریک به ارتکاب اقدامات تروریستی و جمع آوری و انتشار اطلاعات برای مقاصد تروریستی.

در کنار بسیاری از مزایای بدیهی اینترنت ممکن است از آن برای تسهیل ارتباطات درون سازمان‌های تروریستی و انتقال اطلاعات و همچنین حمایت مادی از اقدامات تروریستی برنامه ریزی شده، استفاده شود که همه آنها نیاز به دانش فنی خاصی برای بررسی موثر این جرائم دارند .

• طالبان نیز همانند دیگر گروه های شورشی جدید، از روش‌های ارتباطاتی مدرن بهره جسته و از آنها به عنوان یکی از قدرتمندترین سلاح‌های خود استفاده می‌کند. اکنون که افغان ها به خدمات و برنامه‌های پیام رسانی مانند Telegram ، WhatsApp و دیگر برنامه‌ها دسترسی دارند ، طالبان از موقعیتی قوی‌تر برای ترویج روایت خود برخوردار است.

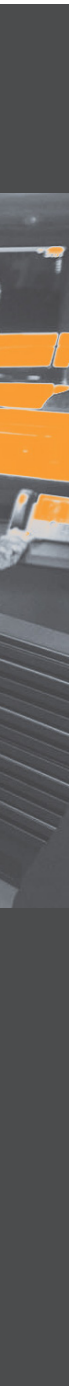
• بر خلاف گروه‌های شورشی دیگر مانند دولت اسلامی (داعش) و القاعده، طالبان در سایه فعالیت نمی‌کند؛ بلکه از هر راه ممکن رسانه‌ای استفاده می‌کند تا روایت خود را نه تنها برای مردم افغانستان ، بلکه برای مخاطبان جهانی ارائه دهد. همچنین پروپاگاندا طالبان بر ارسال پیام به سربازان خود و تلاش برای حفظ وحدت بین آنها متمرکز است.

تفاوت قابل توجهی در آنچه طالبان قادر و توانا به انجام آنلاین هستند در مقایسه با سایرین مانند داعش و القاعده وجود دارد و آن، **استفاده از پلتفرم‌های مختلف** است. رد پای دیجیتالی طالبان را می‌توان در دوره ۲۰۰۵-۰۶ مشاهده کرد ، زمانی که بخش‌هایی از وب سایت آن ، به نام Alemara ، آنلاین شد. امروزه این وب سایت و محتوای آن به زبانهای دری، پشتو و انگلیسی در دسترس است ؛ درست مانند بسیاری از رسانه‌های اجتماعی رسمی و نیمه رسمی که یا توسط طالبان اداره می‌شوند یا از آنها پشتیبانی می‌شود.

در رسانه‌های اجتماعی، به ویژه توئیتر، طالبان حضور گسترده‌ای دارد. این نکته‌ی حائز اهمیت را نیز به خاطر داشته باشیم که طالبان به طور رسمی از سوی ایالات متحده به عنوان یک گروه تروریستی معرفی نشده و این به آنها مشروعیت می‌دهد تا از ابزارهای رسانه‌های اجتماعی غربی بدون تهدید از عکس العمل آنها، استفاده کنند.

مشروعیتی که طالبان از طریق پلتفرم‌های آنلاین و روش‌های خشونت آمیز و افراطی به دست آورده، سوالات قابل توجهی را در مورد بسترهای رسانه‌های اجتماعی فردی و سیاست های ضد افراطی و ضد تروریسم آنها ایجاد می‌کند.

سوالی که استحقاق آن را دارد به جدی ترین نحو بدان توجه شود این است که آیا مجوز قانونی به یک گروه شورشی یا تروریستی صرفاً به بهانه استراتژی سیاسی باید داده شود یا به عبارتی عقلانیت سیاست خارجی یک دولت دلیل کافی و خوبی برای اجازه مشروعیت دیجیتالی به چنین گروه هایی هست؟



"یک سرمایه فوق العاده ارزشمند": رقابت آمریکا بر سر داده‌های افغانستان

مقامات آمریکایی که برای تخلیه متحدان افغان در حال رقابت هستند، قبل از وقوع یک تهدید دیگر، زمان محدودی در اختیار دارند: ذخایر عظیم اطلاعات دیجیتالی که به یکباره در دست طالبان افتاده، نشانگر روابط افغان‌ها با عملیات‌های آمریکایی در مقیاس وسیع است.

شرکت‌های مخابراتی سوابق تماس و مکان بسیاری از کاربران افغان را ذخیره می‌کنند. پایگاه‌های داده دولتی شامل سوابق پروژه‌های با بودجه خارجی و سوابق پرسنل مرتبط می‌باشد. و مجموعه‌ای از داده‌های بیومتریک مانند اثر انگشت که تشخیص افراد را آسان می کند، توسط آنها نگهداری می‌شود.

توماس واریک ، یکی از مقامات سابق ضدتروریسم وزارت امنیت داخلی آمریکا می‌گوید: «تقریباً هیچ شکی وجود ندارد که آنها (طالبان) اطلاعات بسیار ارزشمندی را در اختیار گرفته‌اند که می‌توانند در مجال مناسب خود از آنها استفاده کنند.»

بیشتر توجه‌ها بر روی حذف اطلاعات از اینترنت متمرکز شده است: دولت ایالات متحده، فیلم‌ها، داستان‌ها و عکس‌های افغان‌ها را از سایت‌های خود حذف کرده‌اند. شرکت‌های رسانه‌های اجتماعی از جمله فیس‌بوک ، لینکدین و توییتر ابزارهایی را برای محدود کردن افرادی که می‌توانند مشخصات، پست‌ها و ارتباطات کاربران افغان را مشاهده کنند، ارائه می‌دهند. اما این تلاش‌ها به مجموعه عظیمی از اطلاعات به جای مانده در کابل دسترسی ندارد.


You
Tube

شبکه‌های اجتماعی

سهم بی‌سابقه سایت‌های گمراه‌کننده از مشارکت‌های (ENGAGEMENTS) فیس‌بوک

بر اساس مطالعه‌ی انجام شده، با در نظر گرفتن کاهش مشارکت عمومی در فیس‌بوک طی سال جاری، سایت‌هایی که اخبار را به طرز گمراه کننده‌ای به اشتراک می‌گذارند، سهم بی سابقه‌ای از مخاطبان این پلتفرم را به خود جلب نموده است.

براساس گزارشی از صندوق مارشال آلمان، بیش از ۱ از ۵ تعامل - مانند اشتراک گذاری، لایک یا نظرات - با سایت‌های ایالات متحده از آوریل تا ژوئن در "رسانه‌هایی که اطلاعات را به طور غیر مسئولانه جمع آوری و ارائه می‌دهند" رخ داده است.

این شامل رسانه‌هایی مانند Epoch Times ، TMZ ، Daily Wire و Breitbart است که محققان می‌گویند "اطلاعات را در جهت استدلال یا گزارش خود در مورد یک موضوع، تحریف یا نادرست نشان می‌دهند". اعتبار منابع خبری در این مطالعه توسط NewsGuard تعیین شده است. محققان می‌گویند ماهیت این منابع با سایتهایی که اخبار آشکارا دروغ منتشر می‌کنند ، کاملاً متفاوت است زیرا آنها اشکال ظریف‌تری از اطلاعات غلط (misinformation) را منتشر می‌کند ولی باز هم این امر مضر و خطرناک است.

نسبت محتواهای گمراه کننده برای فیس بوک به بالاترین حد خود در ۵ سال گذشته رسیده؛ جایی که طبق یافته ها "تولید کنندگان محتوای کذب" سهم بالاتری از مشارکت را نسبت به گذشته دریافت کرده‌اند. در عین حال، تعامل با سایتهای آمریکایی که مکرراً اطلاعات کاملا نادرست را به اشتراک می گذارند - که گامی فراتر از ارائه نادرست اطلاعات است - در فیس بوک و توییتر به شدت کاهش یافته است.

در توییتر ، ۹ درصد از به اشتراک گذاری‌ها توسط حساب‌های تأیید شده در سایت های آمریکایی

به سایت‌های گمراه کننده و ۳ درصد به سایت‌هایی که محتوای دروغ منتشر می‌کنند، اختصاص یافته است؛ که برای هر دو دسته پایین ترین سطح در سه سال گذشته است.

این یافته‌ها روشنگر این مسئله است که محتوای قطبی و گمراه کننده اغلب بیشترین مشارکت را ایجاد می‌کند و کاربران را به سمت پلتفرم‌ها سوق می‌دهد و در نتیجه درآمد صاحبان این پلتفرم‌ها را افزایش می‌دهد.

این گزارش همچنین نشان داد در حالی که میزان مشارکت در سه ماهه دوم در سراسر سایت‌های ایالات متحده کاهش یافته است، میزان آن در سایت‌های گمراه کننده به میزان قابل توجهی پایین‌تر از برخی از سایت‌های قابل اعتمادی است که از NewsGuard اعتبار کامل را کسب کرده‌اند.

فیس‌بوک هفته گذشته برای اولین بار گزارشی فصلی در مورد پربیننده‌ترین پست‌های خود در ایالات متحده منتشر کرد که نشان می‌داد در دسترس‌ترین مطالب، کاملاً بی ضرر و غیرسیاسی هستند. به تازگی نیویورک تایمز مدعی شده بود که مدیران فیس‌بوک از انتشار گزارش قبلی به دلیل نگرانی بابت نتایج غیرقابل‌انتظاری که به دست آمده، خودداری نموده‌اند. اما تکرار فرایند قبلی هم نشان داد که مقاله‌ای بازنشر شده از Chicago Tribute در مورد مرگ پزشکی پس از واکسیناسیون بیشترین بازدید را در ایالات متحده داشته است.

نحوه برخورد فیس‌بوک با اطلاعات غلط کروناویروس مورد انتقاد عمومی و خصوصی دولت بایدن قرار گرفته است.

فعالیت این سایت‌ها به احتمال زیاد باعث تفحص دقیق‌تر در مورد نحوه واکنش پلتفرم‌ها به اطلاعات غلط پزشکی شود.

ناامنی سایبری

عودت ۶۰۰ میلیون دلار ارز رمزنگاری شده به سرقت رفته به پایان رسید

Poly Network روز پنجشنبه اعلام کرد که تمام دارایی‌های کاربران را به ارزش ۶۱۰ میلیون دلار که توسط هکری در اوایل ماه جاری به سرقت رفته بود به طور کامل بازیابی کرده است. در یک حرکت غیرمعمول ، هکر تقریباً نیمی از دارایی را در ۲۴ ساعت اول و بقیه را مدتی بعد پس داد.

این هکر از یک آسیب پذیری در سیستم شرکت استفاده کرده بود که به زنجیره‌های مختلف ارزهای رمزنگاری شده امکان برقراری ارتباط می‌دهد. هکر ادعا کرده است که او "برای سرگرمی"هک این شرکت را انجام داده است و هرگز قصد نداشته این پول را نگه دارد.

این شرکت بابت پیدا کردن این آسیب پذیری مبلغ ۵۰۰ هزار دلاری جایزه باگ و همچنین ایفای نقش به عنوان مدیر ارشد امنیتی را به هکر پیشنهاد کرد که هر دوی این موارد را هکر نپذیرفت. این شرکت اعلام کرد که در حال راه اندازی برنامه جدید پاداش کشف باگ با جوایزی در همان سطح است.

دولت بحرین، آیفون فعالان مدنی را با جاسوس افزار NSO هک نموده است

بر اساس گزارش جدید Citizen Lab ، هکرهای دولتی از فناوری نظارتی شرکت NSO برای نفوذ به تلفن نه فعال بحرینی استفاده کرده‌اند.

قربانیان شامل یک وبلاگ نویس، فعال مدنی و سیاسی، اعضای سازمان سیاسی "وعد" و اعضای مرکز حقوق بشر بحرین می‌باشند. نام پنج مورد از اهداف شناسایی شده توسط Citizen Lab در لیست افرادی که توسط عفو بین الملل به عنوان بخشی از تحقیقات "پروژه پگاسوس" به دست آمده بود، ذکر شده است. تصور می‌شود که این لیست اهداف احتمالی مشتریان شرکت NSO را در بر داشته باشد.

هکرها از پیام‌های جعلی استفاده می‌کردند تا اهداف را به نرم‌افزارهای مخرب و همچنین حملات "صفر کلیک"، که نیازی به تعامل کاربر ندارند، متصل کنند. محققان دریافتند که مهاجمان با موفقیت به آخرین نسخه‌های iOS نفوذ کرده و محافظت‌هایی را که این شرکت در ماه ژانویه برای مراقبت از کاربران در برابر چنین حملاتی ارائه نموده را دور زده‌اند.

با توجه به ماهیت اهداف و اینکه یکی از اپراتورهای Pegasus منحصراً در بحرین است ، محققان معتقدند که دولت بحرین پشت عملیات هایی است که در این گزارش شرح داده شده است. دولت بحرین سابقه طولانی در نظارت و انتقام گیری از فعالان دارد و تلاش های نظارتی آن به بیش از یک دهه برمی گردد. دولت بحرین یافته‌های Citizen Lab را رد کرده است.

محققان می‌گویند حداقل دو قربانی کشف شده توسط CitizenLab در زمان نفوذ به تلفن هایشان در انگلستان حضور داشته‌اند که نشان می‌دهد احتمالاً دولت خارجی ثانویه‌ای یا بازیگری با سابقه هک موفقیت‌آمیز از همان منطقه در این عملیات مشارکت کرده است.

سخنگوی این شرکت اسرائیلی تولیدکننده جاسوس‌افزار، Citizen Lab را متهم کرد که عامدانه نتایج تحقیقات خود را با این شرکت به اشتراک نگذاشته تا آنها نتوانند نقض حقوق بشر را کاهش دهند.

کلاهبرداران برای کلاهبرداری از بلژیکی‌ها ، نقش رئیس یوروپل را بازی می‌کنند

کلاهبرداران به منظور ترساندن قربانیان، هویت رئیس Europol را جعل نموده و از این طریق اطلاعات مالی آنها را می‌ربایند.

پلیس بلژیک صدها گزارش از ایمیل‌هایی دریافت کرده که ادعا می شود از طرف کاترین دی بول، مدیر اجرایی Europol ارسال شده است. این ایمیل‌ها گیرندگانشان را به پورنوگرافی کودکان و قاچاق جنسی متهم نموده و سپس اقدام به سرقت اطلاعات حساب PayPal از آنها می کنند.

محتوای ایمیل‌ها فرد قربانی را تهدید می‌کند که در صورتی که گیرنده ظرف ۷۲ ساعت پاسخ ندهد، تعقیب کیفری آنها آغاز می‌شود.

کلاهبرداران سایبری اغلب خود را به جای سازمان های اجرای قانون جا می زنند تا قربانیان را مرعوب ساخته و آنها را شکار کنند. طبق گزارش مرکز شکایات جنایی اینترنتی FBI ، در ایالات متحده ، ۱۲۸۲۷ نفر در سال ۲۰۲۰ قربانی "کلاهبرداری جعل هویت دولت" شده اند که منجر به زیان نزدیک به ۱۱۰ میلیون دلاری شده است.

در آوریل ۲۰۲۰ ، محققان شرکت امنیتی Check Point فاش کردند که یک گروه باج افزار تلفن‌های اندرویدی را قفل کرده و قربانیان را به داشتن محتویات پورنوگرافی متهم می‌نمود و ادعا می‌کردند که اطلاعات شخصی آنها را به مرکز داده FBI ارسال خواهند کرد.

هکرها صدها سرور ایمیل مایکروسافت را نقض نمودند

هکرها در هفته گذشته در بیش از ۱۵۰ سرور ایمیل آسیب پذیر نفوذ کردند. قربانیان این هک‌ها شامل فراوری‌کننده‌های غذاهای دریایی، تعمیرگاه‌های خودرو و دفاتر دندانپزشکی و وکالت هستند. آژانس "امنیت سایبری و امنیت زیرساخت‌ها" هشدار فوری به سازمان‌ها داد تا با بروزرسانی (پچی) که مایکروسافت در ماه مه منتشر کرد در برابر هک‌ها از خود محافظت کنند.

هکرها اوایل امسال از اشکال متفاوتی در Microsoft Exchange سوءاستفاده کرده بودند. آن موقع، مایکروسافت در ابتدا اعلام کرد که آن هک‌ها توسط یک گروه تحت حمایت چین انجام شده است. به گفته کارشناسان، هکرهایی که سرورهای Exchange را هدف قرار داده اند، از پیچیدگی کمتری برخوردار بودند. جان هاموند ، محقق ارشد امنیتی Huntress گفت: «هر کسی که دارای تکنیک های فنی و اندکی دانش باشد می‌تواند این زنجیره حمله را دوباره ایجاد کند.»

بين الملل

توافقات سایبری ایالات متحده با سنگاپور در راستای استراتژی مقابله با پکن

دولت بایدن روز دوشنبه از مجموعه‌ای از توافقنامه‌ها با سنگاپور رونمایی کرد که محور اصلی آنها تقویت روابط امنیت سایبری و مقابله با تهدیدات دیجیتالی است.

اعلامیه کاخ سفید با سفر کمالا هریس ، معاون رئیس جمهور به منطقه که در راستای تلاش‌های دولت امریکا برای مقابله با نفوذ فزاینده چین در منطقه انجام شده، مصادف گردید. این معاملات پس از دیدار هریس با حلیمه یعقوب ، رئیس جمهور سنگاپور و لی هسین لونگ ، نخست وزیر سنگاپور صورت گرفت.

آژانس "امنیت سایبری و امنیت زیرساخت‌ها" و وزارت "دفاع" و "خزانه‌داری" هرکدام تفاهم‌نامه‌ای را با همتایان سنگاپوری خود با هدف گسترش به اشتراک گذاری اطلاعات امضا نمودند.

به گفته کاخ سفید، توافق نهایی بین CISA و آژانس امنیت سایبری سنگاپور سبب"افزایش تبادل اطلاعات در مورد تهدیدات سایبری و اقدامات دفاعی ، افزایش هماهنگی برای واکنش به حوادث سایبری و ایجاد ظرفیت امنیت سایبری در جنوب شرقی آسیا" می‌گردد.

در همین حال، قرارداد امضا شده بین وزارت خزانه‌داری و نهاد پولی سنگاپور "به هر دو بخش مالی کمک می کند تا در برابر تهدیدات سایبری آماده‌تر و مقاوم‌تر شوند ، و همچنین به اشتراک گذاری اطلاعات دو جانبه در مورد تهدیدات سایبری برای بازارهای مالی تسهیل گردد."

همچنین به اشتراک گذاری اطلاعات یک نکته اصلی بین پنتاگون و وزارت دفاع سنگاپور خواهد بود و یک تفاهم نامه همکاری سایبری را به مرحله نهایی رساند. این تفاهم‌نامه شامل "تبادل علائم تهدید، آموزش و تمرینات سایبری ترکیبی، و سایر اشکال همکاری نظامی-نظامی در زمینه مسائل سایبری" است.

روابط واشنگتن و پکن سالهاست که رو به افول است و از ماه گذشته که ایالات متحده و متحدانش چین را به کمپین جاسوسی دیجیتال جهانی متهم کردند ، بدتر نیز شده است.

پارلمان کره جنوبی قانونی را برای جلوگیری از اخبار جعلی تصویب کرد

حزب حاکم کره جنوبی قرار است قانون رسانه‌ها را به منظور مهار "اخبار جعلی" با دادن اختیار به دادگاه‌ها برای جبران خسارت‌های بزرگتر اصلاح کند. مخالفان اصلاحیه جدید می‌گویند که این امر خبرنگاران را از کاوش در معاملات پنهانی قدرتمندان منصرف می‌کند.

کره جنوبی میزبان صنعت خبری پررونقی است که در جدول آزادی رسانه‌های جهان رتبه نسبتاً بالایی دارد اما در سالهای اخیر با مسئله نشر اطلاعات غلط (misinformation) و دیگر جرائم سایبری دست و پنجه نرم می‌کند.

این قانون همچنین از رسانه‌ها ، از جمله ارائه دهندگان خدمات خبری اینترنتی، می‌خواهد که برای اخبار اشتباه یا ساختگی که "افکار" یا "سهل انگاری فاحشی" را بازنمایی می‌کنند، اصلاحیه منتشر کنند.

دولت‌ها و شرکت‌های جهانی به طور فزاینده‌ای از انتشار اطلاعات غلط آنلاین و تأثیر آن نگران هستند در حالی که فعالان حقوق بشر از سوء استفاده آنها از چنین قوانینی برای ساکت نمودن مخالفان می‌ترسند.

در نظرسنجی WinGKorea Consulting که روز سه شنبه منتشر شد، این لایحه حمایت ۴۶.۴ از ۱۰۲۴ پاسخ دهنده را با خود داشت در حالی که ۴۱.۶ گفتند آزادی مطبوعات را سرکوب می‌کند.

Iranian Council For
Defending The Truth

اخبار کوتاه

۴


CONNECTED
NETWORK
[PROCESSING
02
// HACK ATTE
CONNECTED
[PROCESSING]
USER S
//SCAN
NETWORK

- طالبان به لیست گروه‌های تروریستی یکی از گروه‌های بزرگ فناوری اضافه شد: سازمان مبارزه با تروریسم تحت حمایت سازمان ملل متحد اعلام کرد که ورود مطالب مرتبط با طالبان به پایگاه داده، تروریسم را تسریع می کند. این حرکت در حالی صورت می گیرد که صنعت فناوری با مشکل نحوه برخورد با طالبان که کنترل افغانستان را در دست گرفته اند و از تاکتیک‌های پیچیده‌ای در رسانه‌های اجتماعی استفاده می‌کند، دست به گریبان است.

ICDT.IR