علی آرش
۲۰۱۸/۱۱/۲۲

امنیت شکنندۀ فضای سایبر در افغانستان

آگاهان می‌گویند، فضای سایبر افغانستان هنوزهم شکننده است.

همزمان با گسترش شمار کاربران انترنت و استفاده از انترنت در نهادهای خصوصی و دولتی، پدیدۀ جرایم الکترونیکی و سایبری نیز موازی با این تحولات در سالهای اخیر رو به افزایش بوده است. این موضوع حکایت از آن دارد که به گفتۀ آگاهان، فضای سایبری افغانستان هنوزهم با وجود پیشرفت‌ها در این عرصه «شکننده است»

این درحالی است که امروزه ادارات دولتی به شبکۀ اینترنت وصل شده اند و دولت براساس برنامه «حکومت الکترونیک» کارهای دولتی را با کمپیوتر و ارتباطات اینترنتی انجام می‌دهد. دولت پیشرفت در این زمینه را یکی از دستاوردهای عمدۀ خود در دو دهۀ اخیر می‌داند.

در حال حاضر میتوان گفت که همۀ نهادهای دولتی کشور وبسایت دارند و برخی از آنها اطلاعات مهمی مانند نتایج انتخابات و آزمون کانکور و ده ها مورد دیگر را از طریق همین وبسایت‌ها در اختیار کاربران قرار می‌دهند. اما آن طوری که آگاهان می‌گویند، بخش‌های انلاین وبسایت‌های ادارات دولتی، از امنیت چندانی برخوردار نیست و به آسانی هک میشوند.

در کنار این موضوع و با توجه به استفاده رو به افزایش از انترنت و حاکم شدن فضای الکترونیکی در کشور، تدابیر احتیاطی حکومت برای امنیت فضای سایبری، هنوزهم ناکافی دانسته می‌شود. از سویی هم با وجود شامل شدن بحث جرایم سایبری در کود جزای کشور، پولیس در این عرصه فاقد تخصص است و دستگاه عدلی و قضایی کشور نیز نیروهای متخصص در این عرصه را برای داوری و رسیدگی درست به دوسیه ها در اختیار ندارد. پیامد این موضوع این است که در حال حاضر قربانیان جرایم سایبری کمتر به داوری و نحوۀ رسیدگی به دوسیه‌های شان از سوی این نهادها، راضی اند. بیشتر قربانیان جرایم سایبری احکام دستگاه قضایی درمورد دوسیه‌های شان ناعادلانه می‌دانند.

جرایم سایبری چیست؟

بر اساس جریدۀ رسمی وزارت عدلیه و ماده ۸۵۱ کد جزای کشور، می‌توان جرایم سایبری را این طور معنا کرد (جرایم سایبری عبارت از جرایمی است که به وسیلۀ تکنالوژی مدرن اطلاعات و ارتباطات الکترونیکی یا اینترنتی در فضای سایبر ارتکاب می‌یابد.) اما اگر به زبان ساده تر بگوییم (جرایم سایبری عبارت از جرایمی که در محیط سایبر (فضای الکترونیکی) رخ بدهد.

معمولا جرایم سایبری با انگیزه‌های مختلفی صورت می‌گیرد. به گفتهٔ مهدی حیدری، آگاه مسایل فناوری، مجرمان این بخش به دنبال سه هدف عمده هستند: « کسانی که با منجر شدن به این جرایم در صدد کسب پول هستند مانند باجگیری‌های انترنتی، هک سیستم‌های بانکی و .. دوم،کسانی که به دنبال کسب قدرت سیاسی هستند تغییر و دخالت در اطلاعات سیستم‌ها مثل آمار و ارقام در سیستم‌های متفاوت و سوم، رقابت‌ها؛ رقابت‌ها می‌تواند در حد اشخاص و شرکت‌ها باشد و یا حتی در بین کشورها، مواردی هستند که با هک کردن سیستم‌ها و اعلام این که سیستم‌ها توسط آن‌ها هک شده به نوعی قدرت نمایی و پیشی‌گرفتن از رقیب است.»

اما قربانیان جرایم سایبری در افغانستان کی‌ها و کدام نهادها بوده اند؟ بررسی‌های ما نشان می‌دهد که در سالهای گذشته هم فضای انلاین نهادهای دولتی، خصوصی و افراد از سوی هکرها مورد دستبرد قرار گرفته است. با وجودی حکومت به خصوص وزارت مخابرات اعلام کرده که تدابیر احتیاطی را به منظور جلوگیری از وقوع جرایم سایبری روی دست گرفته، اما ظاهرا هکرها در سالهای گذشته توانسته اند که این حلقه امنیتی را دور بزنند و وبسایت‌های دولتی را هک کنند.

تا کنون دوبار وبسایت شورای امنیت ملی کشور که مهمترین نهاد در عرصه تصمیم‌گیری در بخش امنیت به حساب می‌آید، مورد دستبرد قرار گرفته و هک شده است.

بار اول، وبسایت شورای امنیت ملی کشور اوایل ماه مارچ سال ۲۰۱۲ از سوی هکرهای منسوب به گروه القاعده هک شد. هکرها این وبسایت را در کنترل خود گرفتند و عکس اسامه بن لادن را در صفحه اول آن قرار دادند.

بار دوم به تاریخ ۲۵ نوامبر سال ۲۰۱۶، هکرهایی که خود را «ارتش سایبری هزارستان» می‌خواندند، وبسایت شورای امنیت ملی کشور را هک کردند. این گروه آن زمان اعلام کرد که کنترل این وبسایت را در اختیار گرفته و تمام اطلاعات آن در دسترس آنها است.

وبسایت شورای امنیت تا کنون دوبار هک شده است

در کنار این‌ها، آن طوری که معلومات وزارت مخابرات و تکنالوژی معلوماتی نشان می‌دهد، تا کنون وبسایت‌های، وزارت خارجهٔ کشور، بانک مرکزی، ارگان های محل، وبسایت ولایت بلخ و چندین وبسایت دولتی دیگر و همچنان وبسایت موسسه اکبر، در سال گذشته هک شده بودند و در محتوای این وبسایت‌ها تغییراتی آورده شده اند.

هکرها موفق شدند که باری دوازده وبسایت دولتی را به صورت همزمان هک کنند و مطالب علیهٔ دولت را در آن بارگذاری کنند.

در کنار هک شدن وبسایت‌های دولتی و خصوصی، در سال های اخیر، برخی از افراد نیز در فضای اجتماعی، به نوعی قربانی جرایم سایبری شده اند. یکی از این افراد که در این گزارش از او به اسم مستعار احمد یاد می‌کنیم، به یاد می‌آورد که گروهی از افراد سال گذشته فیسبوک او را هک کردند و با بارگذاری عکس‌های خصوصی اش در آن، ازو خواستند که بابت عدم نشر آن باید به آن‌ها ۵۰۰هزار افغانی باج بدهد.

او گفت:« من این پول را نداشتم که به آن‌ها بپردازم، لذا همه عکس‌های خانوادگی ام در فیسبوک نشر شد. حیران ماندم که به کجا مراجعه کنم و چطور دادخواهی کنم.»

در کنار این، گروهی از هکران از دختری، فیلم گرفته بودند و سپس آن را در سایتی پورن اپلود اختصاصی کردند. هکران برای اینکه این فیلم را نشر عمومی نکنند، از این دختر باجگیری می‌کردند. او گفت:« هیچ مرجعی شکایتم را پیگیری نمی‌کرد و من مجبور به باجدهی شدم.»

افراد و نهادها چگونه قربانی می‌شوند؟

مهدی حیدری، استاد وهنتون در پاسخ به این پرسش می‌گوید، ما اصطلاحی داریم به نام (بومیهای تکنالوژی و مهاجرین تکنالوژی)؛ بومیهای تکنالوژی به نسلی گفته میشود که با تکنالوژی به بلوغ می‌رسد و رشد سنی آنها به صورت موازی با رشد تکنالوژی در جریان است. اما نسل مهاجرین تکنالوژی به نسلی گفته میشود که سن آنها کمی به قبل از فراگیر شدن تکنالوژی بر میگردد و برای حل نیازهای روزمره وادار و نیازمند به استفاده از تکنالوژی هستند. نسلی که به گفتهٔ وی، تجربهٔ تکنالوژی برای آن‌ها جدید و نا آشنا است و این خود باعث میشود تا به دلیل عدم آگاهی از پیشگیری‌های لازم مورد تهاجم بیشتری قرار بگیرند.

این آگاه فناوری و تکنالوژی در مورد این که نهادهای دولتی و خصوصی کشور تا چی اندازه در این مورد آسیب پذیر اند، میگوید، نهادها در افغانستان به دلیل نداشتن «تیم تخنیکی با تجربه و عدم اختصاص بودجهٔ لازم برای امنیت سایبری شان، بیشتر در مظان هدفگیری هستند.»

او گفت:« اکثر نهادها در تشکیلات خود اصلا تیم امنیت معلوماتی ندارند و یا حتی کارمندان تخنیکی شان از علم و تجربه کافی برخودار نیستند و عدم بودجه در این موارد یکی دیگر از مشکلات است. استفاده از برنامه‌های غیرقانونی و رایگان، نداشتن مرکز معلومات مجهز، تمام این‌ها به گونه‌ای شرایط را برای نفوذ هکر فراهم می‌کند.»

وضعیت سایبری بانکها

رییس بانک مرکزی می‌گوید که مساله هک کردن حساب‌های بانکی و یا ریسک سایبری، موضوعی است که همه جهان را تهدید می‌کند. خلیل صدیق، در گفتگو با ۸ صبح، با آنکه خطرساز بودن این مساله را تایید کرد اما گفت که بانک مرکزی همه بانک‌های موجود در کشور را از این خطر آگاه ساخته و هشدار داده که سافت‌ویرهای بازدارنده را در سیستم‌های بانکی شان نصب کنند تا از خطرات احتمالی در امان بمانند.

او گفت که بانک مرکزی سیستمی ندارد که امنیت سایبری دیگر بانک‌ها را محافظت کند. به گفته وی، توصیه بانک مرکزی به بخش‌های محافظتی انلاین این بانک و دیگر بانک‌های کشور همواره این بوده که نرم‌افزارهای شان را از شرکت‌های مطمین که در این عرصه فعالیت می‌کنند، تهیه و همچنان رمزهای عبور شان را نیز هر از گاهی بروزرسانی کنند.

از سویی رییس کل بانک مرکزی به ۸ صبح گفت که تا کنون مواردی نزد این بانک ثبت نشده که نشان بدهد، سیستم مالی بانک‌های افغانستان مورد دستبرد قرار گرفته و یا مبالغی از آن برداشته شده باشد.

اما محمدطارق میران که تجربه کار در بخش امنیت در یکی از بانک‌های کشور را دارد و نیز دکترایش را از دانشگاه «تالین» کشور استونیا در رشته تکنالوژی معلوماتی بدست آورده معتقد است که «فضای سایبری افغانستان آن طوری که لازم است از امنیت لازم برخودار نیست و بسیار زیاد شکننده است. احتمال هر نوع واقعات قابل پیش‌بینی و غیر قابل پیش‌بینی در فضای انلاین افغانستان وجود دارد. اگر اقدامات لازم در این عرصه روی دست گرفته نشود، خطرات بسیار جدی روی سکتور بانکی به وجود خواهد آمد.»

داکتر میران، موضوع هک شدن حساب‌های بانکی را از سوی هکران نیز به شکل غیرمستقیم تایید می‌کند و می‌گوید: « موضوع هک شدن حساب‌های بانکی به صورت قطع از سوی بانک‌ها به بیرون شریک ساخته نمی‌شود چون اعتبار بانک در میان است و مسوولان بانک‌ها از عواقب حقوقی و قانونی آن هراس دارند.»

یک تن از کارمندان بخش امنیت سایبری یکی از بانک‌های کشور نیز در گفتگو با ۸ صبح، این موضوع را تایید می‌کند و می‌گوید که در صورت هک شدن سیستم مالی یک بانک، «مسوولان ترجیح می‌دهند که زیان‌های وارده از این آدرس را به جان بخرند اما در عوض اعتماد مشتریان شان را از دست ندهند.»

از سویی هم آگاهان فناوری این پرسش را مطرح می‌سازند که در هنگام ارتکاب یک جرم سایبری صلاحیت محکمه رسیدگی کننده را با استناد به کدام یک از اصول حقوق آیین دادرسی می‌توان شناخت. به عبارت دیگر پرسش اصلی آن‌ها این است که در صورت وقوع یک جرم سایبری چگونه و تا چه حد دادگاه‌های کشور می‌توانند اعمال صلاحیت کنند. این نگرانی از آنجا خلق می‌شود که به گفته آگاهان فناوری، پولیس و دستگاه تحقیق و قضاوت افغانستان تخصص لازم در این بخش را ندارند و با «جرایم سایبری بیگانه اند»

نیاز به تشکیل یک دادگاه کیفری ویژه جرایم سایبری

فضای سایبری دارای ویژگی‌ها و ماهیت خاصی است که نیازمند قاعده‌مندی و نظام حقوقی خاصی نیز می‌باشد. با توجه به تخصصی و خاص بودن این فضا، قضاتی که به جرایم مرتبط با این فضا رسیدگی می‌کنند، باید در حوزهٔ فناوری اطلاعات و سایر فناوری‌های مرتبط متخصص باشند. بنابراین گرچه با توجه به نوظهور بودن جرایم سایبری تاکنون مرجع قضایی مشخصی در کشور ایجاد نشده است، اما به نظر می رسد که ضرورت دارد تا یک دادگاه ویژه جرایم سایبری تشکیل شود.

از سویی هم متأسفانه در کشورمان علی‌رغم فراهم شدن جنبه تقنینی این موضوع، تاکنون زمینه اجرایی آن فراهم نشده است. این امر یکی از ایرادات و اشکالات مهم به عملکرد دستگاه قضایی کشورمان است. موضوعی که باعث شده بسیاری از قربانیان به دلیل ابهام موجود در این زمینه از پی‌گیری پروندهٔ شان منصرف شوند.

وحیدالله فرزه‌ای، عضو اتحادیه حقوق‌دانان افغانستان، می‌گوید، تا کنون جرایم به صورت اختصاصی در نهادهای عدلی و قضایی افغانستان بررسی نمی‌شود. او می‌گوید در حال حاضر هیچ دادگاه ویژه جرایم سایبری در کشور وجود ندارد:«ما در اینجا به یک بحث قضایی تخصصی سروکار داریم به این مفهوم که یک قاضی که بتواند به این موارد رسیدگی بکند، بر موضوعات سایبری اشراف داشته باشد، در افغانستان چنین اشخاصی به عنوان متخصصان قضایی وجود ندارد.»

این عضو اتحادیه حقوق‌دانان افغانستان در ادامه افزود:« چیزی که در افغانستان بسیار عام بوده، موجودیت محاکم جزایی است که در هر عرصه رسیدگی و قضاوت می‌کنند. در حال حاضر در بخش جرایم هوانوردی، محکمه فساد اداری رسیدگی می‌کند، در حالی که این محکمه موضوعاتی اختصاصی این دوسیه را تفکیک کرده نمی‌تواند و از نظر اهل خبره نیز برداشت درست کرده نمی‌تواند.»

او گفت که نبود تخصص در این عرصه می‌تواند که منجر به این شود که متضرر قضیه به حق خود نرسد و متهمان قضیه خلاف قانون مورد رسیدگی قضایی قرار بگیرند و مجازات شوند.

نیاز به تشکیل پولیس سایبری

این تنها بخش حکمی دستگاه قضایی افغانستان نیست که از خلای تخصص رنج می‌برند، بلکه هم‌اکنون بخش‌های دادستانی افغانستان نیز نیروهای متخصص هر بخش به خصوص بخش سایبر را در اختیار ندارد. هم اکنون در مواد درسی دانشگاه‌های افغانستان به خصوص جزوه‌های آموزشی دانشکده‌های حقوق، بخش جرایم سایبری و چگونگی رسیدگی به آن شامل نشده و به همین دلیل بسیاری از سارنوالان پس از فراغت حتا با اسم این جرم نیز آشنایی ندارد.

نبود نیروهای متخصص در این عرصه نیز به شدت می‌توانند مراحل تحقیقاتی و کشف جرم و چگونگی وقوع آن را با چالش و پرسش روبرو سازد. در کنار این‌ها، هنوزهم در مواد درسی نیروهای آموزش دیده پولیس که از اکادمی‌های پولیس فارغ می‌شوند، جرایم سایبری گنجانیده نشده و این نیروها با Electronic Crime کاملا بیگانه هستند.

این درحالی‌ست که وجود نیروهای امنیتی و نظامی در محیط اینترنت یکی از الزامی‌ترین موارد در دنیاست و تقریبا همه کشورهای پیشرفته و حتی غیرپیشرفتهٔ دنیا برای این فضای مجازی پولیس تخصصی و ویژه‌ای را در نظر گرفته‌اند تا با آن‌ها در صدد کاهش جرایم اینترنتی برآیند.

نصرت رحیمی، معاون سخنگوی وزارت داخله، می‌گوید، در حال حاضر در ریاست مبارزه با جرایم جنایی در وزارت داخله، مدیریت مبارزه با جرایم سایبری نیز فعالیت دارد. او اما در مورد تشکیل و این که تا چی اندازه کارمندان این بخش، افراد متخصص و آموزش دیده در بخش امنیت انترنتی هستند، معلومات بیشتری ارایه نکرد. اما طارق میران، آگاه مسایل فناوری معتقد است پولیس و سارنوالی به دلیل عدم تخصص در این عرصه، نمی‌تواند اسناد و شواهد لازم را جمع‌آوری، تحلیل و از آن به عنوان یک مدرک استفاده کند.

اقدامات دولت

با همهٔ این‌ها مقام‌های وزارت مخابرات و تکنولوژی با آنکه در مورد مصوونیت سیستم‌های الکترونیکی کشور نگران اند اما می‌گویند، به خاطر جلوگیری ا دسترسی و دست‌برد به اسناد محرم الکترونیکی، حکومت برنامه‌های را به اجرا گذاشته است.

وزارت مخابرات و تکنالوژی معلوماتی در سال ۲۰۰۹ نخستین تیم عکس‌العمل سریع سایبری افسرت (AFCERT) را در افغانستان ایجاد نمود تا بتواند از وقوع حملات سایبری جلوگیری نماید. آن طوری که اعزازالله سایر زلاند، سخنگوی وزارت مخابرات می‌گوید، تیم عکس‌العمل‌های سریع سایبری در بخش‌های مختلف جرایم الکترونیکی فعالیت می‌کند:« از جمله تحقیق جرایم سایبری، تفتیش سایبری، آگاهی از خطرات سایبری.» هدف از ایجاد این تیم این بوده که آگاهی و خدمات امنیت سایبری را به سکتور حکومتی و خصوصی فراهم کند.

به همین دلیل به گفته مقام‌های وزارت مخابرات، پس از تشکیل این اداره، نزدیک به ۱۵۰ قضیهٔ جرایم انترنتی پی‌گیری و به آن رسیده‌گی شده است. به گفته این وزارت، هک کردن ویب سایت‌ها، دسترسی به حساب‌های بانکی و انتقال غیرقانونی پول از یک حساب به حساب دیگر، بخشی از جرایم انترنتی است که دولت افغانستان هر از گاهی با آن روبرو می شود.

در کنار این تلاش‌ها، حکومت افغانستان به خاطر مبارزه علیه جرایم سایبری و کنترول فضای سایبر کشور، جرایم سایبری را برای نخستین بار سال گذشته شامل کود جزا کرد. هدف بود تا با جرم‌انگاری این پدیده، میزان جرایم سایبری در کشور کاهش یابد.

امان ریاضت، سخنگوی وزارت عدلیه می‌گوید، در کود جزای افغانستان در باب دوم، فصل اول، احکامی زیادی در مورد جرایم سایبری وجود دارد که جرایم سایبری را جرم‌انگاری شده و مجازات در نظر گرفته شده است:« برای این که جرایم سایبری حالاتش مشخص شود، تعریف واضح، مشخص و تخنیکی از آن صورت بگیرد، طرح قانون جرایم سایبری در وزارت عدلیه زیر کار قرار دارد. به این دلیل که به لحاظ تخنیکی این طرح تقویت شود و در مخالفت با سایر اسناد تقنینی نافذ و کنوانسیون‌های بین‌المللی نباشد، وزارت عدلیه آن را تدقیق می‌کنند.»

او در ادامه گفت:« که طرح قانون جرایم سایبری در حال حاضر در کود جزای افغانستان، احکام جزایی که برایش در نظر گرفته شده نافذ است و جنبه اجرایی دارد.»

چی باید کرد؟

با همهٔ این‌ها پرسش دیگر این است که چی باید کرد و چطور می‌شود که خلاهای موجود را از بین برد. مهدی حیدری، آگاه مسایل فناوری می‌گوید، اطلاع‌رسانی برای مردم و ظرفیت‌سازی برای نهادهای دولتی از راه حل‌های عمده و اساسی در این بخش است.

وزارت مخابرات می‌گوید، به خاطر جلوگیری از دسترسی و دست‌برد به اسناد محرم الکترونیکی، برنامه‌های را به اجرا گذاشته است

داکتر طارق میران اما معتقد است تا زمانی که نصاب درسی در اکادمی‌های پولیس و همین طور در دانشکده‌های حقوق کشور اصلاح نشود و بحث جرایم سایبری در مواد درسی افراد نامبرده شامل نشود، دشوار خواهد بود که به سادگی با جرایم سایبری بتوان به مبارزه پرداخت.

به گفته طارق میران، به دلیل تخصصی و پیچیده بودن این موضوع، راه‌اندازی برنامه‌های کوتاه مدت برای سارنوالان و نیروهای پولیس نمی‌تواند راه‌گشا باشد.

او معتقد است که استراتیژی و پالیسی‌های بسیار عملی از سوی دولت در این عرصه مطرح و ظرفیت‌های لازم در این بخش پرورانده شود.

پایان