وضعیت تبدیل به بدترین دشمن خودمان شده‌ایم.»

بحران پیش آمده بر اثر این هک، روی تأمین سوخت ایالت‌های تنسی، دلور و می‌سی‌سی‌پی نیز تأثیر گذاشت و تا هفته‌ها قیمت سوخت بیش از حد معمول بود. با وجود آنکه دولت فدرال بارها هشدار داد «در برابر کسانی که به بالا ماندن قیمت سوخت کمک می‌کنند، هیچ صبر و شفقتی نشان نخواهد داد» اما باز هم در دست گرفتن کنترل اوضاع چندین هفته طول کشید.

اگرچه نمی‌توان به طور حتم گفت که در آینده باز هم می‌توان شاهد وقوع حملات هکری به زیرساخت‌های امریکا بود اما با وجود این می‌توان انتظار داشت که گروه‌های مختلف با انگیزه‌های متفاوت بخواهند دولت امریکا را در برابر چالش‌های امنیتی قرار دهند. «بایدن» که پس از روی کار آمدن، توانست در بسیاری از عرصه‌ها عملکرد قابل قبولی از خود نشان بدهد و رضایت نسبی مردم و نخبگان سیاسی را جلب کند، در حوزه تأمین امنیت ملی بویژه در زیرشاخه امنیت سایبری کارنامه چندان درخشانی ندارد. او پس از وقوع حمله کولونیال، زیرساخت‌های بزرگ‌ترین سیستم توزیع سوخت خود را تقویت و ایمن‌سازی کرد اما با وجود این، بدیهی است که به همان نسبت تلاش هکرها هم افزایش پیدا خواهد کرد. «پیتر مک‌نالی»، استاد امنیت سایبری و مدیر بخش جهانی در شرکت امنیتی Third Bridge اعتقاد دارد: «پس از این حمله هکری، حساسیت برای ارتقای امنیت زیرساخت سیستم توزیع سوخت افزایش یافت. من تصور می‌کنم شرکت‌های توزیع سوخت می‌توانند بخشی از تکنولوژی تأمین امنیت را در داخل خود مهیا کنند و بخشی از آن را از بخش خارجی دریافت کنند. اکنون بسیاری از شرکت‌های بزرگ سوختی، دولت را تحت فشار گذاشته‌اند که کمک کند سیستم‌های امنیتی خود را مدرن‌تر کنند. کمیسیون رگولاتوری انرژی فدرال الزاماتی را ایجاد کرده که به موجب آن استانداردهای مطلوب برای تعبیه و افزایش امنیت سایبری سیستم الکتریکی سیستم توزیع سوخت ایجاد شود. رئیس جمهور عزم راسخی دارد که میزان حملات هکری را به میزان قابل توجهی کم کند و در همین راستا در سند راهنمای استراتژیک موقت امنیت ملی امریکا که در مارس ۲۰۲۱ منتشر شد، تصریح کرده بود تهدیدهایی مانند بیماری‌های همه‌گیر، حملات سایبری و اطلاعات گمراه‌کننده هیچ مرز و دیواری نمی‌شناسد و پرداختن به آنها از اولویت‌های امنیت ملی امریکاست.»

اما شاید او بهتر از هر شخص دیگری بداند که عملی کردن این تصمیم به این سادگی‌ها هم نیست، از یک سو افزایش فزاینده انگیزه‌های گروه‌های هکری که گاه با اهداف اقتصادی پا به عرصه می‌گذارند و گاه با امیال و خواسته‌های سیاسی و در برخی موارد هم صرفاً به‌دنبال تصاحب تیتر نخست رسانه‌ها هستند و از سوی دیگر، موانع طولانی که در مسیر سیاستگذاری محقق شدن خواسته بایدن را دشوار نشان می‌دهد.

حمله سایبری گسترده دیگری یکی دو ماه بعد به ۲۰۰ شرکت امریکایی نشان داد بایدن هیچ فرصتی برای دفاع کردن هم ندارد. شرکت امنیت سایبری Huntress Labs در گزارش مفصلی که منتشر کرد، اعلام کرد این حمله هکری به احتمال قوی از سوی یک گروه روسی هدایت شده است و با وجود آنکه به شرکت‌های تجاری حمله شده، هدفش لزوماً تنها اقتصادی نیست. این شرکت امنیتی اعلام کرد این حمله سایبری می‌تواند زمینه حملات هکری آینده هم باشد. آژانس امنیت سایبری و زیرساخت امریکا در بیانیه‌ای ضمن انتقاد شدید از این حمله، اعلام کردند بزودی پاسخ مناسبی به این حمله داده خواهد شد. زمان‌بندی این حمله که در عصر جمعه روی داد، بی‌نقص بود، زیرا کارمندان شرکت‌ها در امریکا خود را آماده تعطیلات روز استقلال می‌کردند و کمتر کسی آماده یک جنگ سایبری بود.

نوع، زمان و نحوه حملات سایبری اخیر امریکا نشان‌دهنده این است که گروه‌های هکری دائماً در حال ارائه خلاقیت و نوآوری در روش‌های هک کردن هستند و هر بار از روش تازه‌ای به امنیت سایبری زیرساخت‌ها و سیستم‌های امریکا نفوذ می‌کنند. بنابراین برای مقابله با این گروه‌ها لازم است ضمن تقویت کلیت زیرساخت‌های امنیتی، مسیر هکرها را تا حدودی حدس زد و پیشدستی کرد. در نشستی که تابستان گذشته در ژنو برگزار شد، «بایدن» خطاب به «ولادیمیر پوتین» گفت که او را مسئول حملات سایبری مخرب می‌داند. او در این نشست به همتای روسی‌اش یک فهرست ۱۶ موردی شامل زیرساخت‌های انرژی، آب و... داد که «ابداً نباید هک شوند.» برخی کارشناسان اعتقاد دارند که ایالات متحده باید برای مجازات روسیه دست به انجام اقدامات بیشتری بزند. دولت فدرال می‌تواند تحریم‌های رسمی را علیه مسکو اعمال کند، همان‌طور که دولت «باراک اوباما» دیپلمات‌ها را به تلافی مداخله هکرهای نظامی کرملین به‌نفع ترامپ در انتخابات ۲۰۱۶، اخراج کرد یا اینکه ایالات متحده می‌تواند مخفیانه‌تر نیزعمل کند، به‌عنوان مثال با افشای جزئیات معاملات مالی «پوتین» او را تحت فشار بگذارد. اما همان‌طور که «لوک هاردینگ» از روزنامه گاردین اشاره کرده، حملات سایبری «ارزان، قابل انکار و از نظر روانشناختی مؤثر است» و گزینه‌های «بایدن» برای پاسخگویی محدود هستند. «هاردینگ» نوشت: «این پاسخ باراک اوباما تلاش برای تنظیم مجدد روابط با پوتین را بر هم زد و شخصی که این مأموریت محکوم به‌فنا را برعهده داشت، وزیر امور خارجه وقت، یعنی هیلاری کلینتون، خود یک قربانی هک روس‌ها در سال ۲۰۱۶ شد.»

موضوع دفاع در برابر حملات علیه امنیت سایبری تبدیل به موضوع داغ و جدیدی در کنگره امریکا شده و دامنه گسترده حملات اخیر سبب شده تا حمایت هر دوحزب اصلی را به خود جلب کند. اما بن‌بست‌های حزبی درباره دیگر مسائل، تهیه قانونی در این زمینه در کنگره را دشوار و روند تعیین اولویت‌های سایبری را کند کرده است. یکی از موضوعاتی که مورد حمایت دو حزب اصلی در امریکا بوده قانون مجوز دفاع ملی (NDAA) در سال ۲۰۲۱ است که شامل مجموعه‌ای از اقدامات برای ارتقای امنیت سایبری در نهادهای فدرال طی چند سال است.

به هر جهت و با وجود تمامی موانع موجود، امریکا برای برون‌رفت از بحران امنیت سایبری کنونی باید دقیق کرده و فوری دست به تصمیم‌گیری و عمل بزند و قبل از آنکه حمله هکری دیگری غافلگیرش کند، دیوارهای امنیتی خود را تقویت کند.

منابع:

NewyorkTimes, Forbes, AP, BBC

بحران پیش آمده بر اثر این هک، بر روی تأمین سوخت چندین ایالت تأثیر گذاشت و تا هفته‌ها قیمت سوخت بیش از حد معمول بود. با وجود آن‌که دولت فدرال بارها هشدار داد «در برابر کسانی که به بالا ماندن قیمت سوخت کمک می‌کنند، هیچ صبر و شفقتی نشان نخواهد داد» اما باز هم در دست گرفتن کنترل اوضاع چندین هفته طول کشید