

# کلید قطع اینترنت در دست کیست؟

آیا می‌توان شبکه جهانی اینترنت را با فشردن یک کلید قطع کرد؟ کلید قطع اینترنت در دست کیست؟ چرا آمریکا می‌خواهد کلید قطع شبکه جهانی را در دست داشته باشد؟ چه زمانی باید اینترنت جهان را قطع کرد؟ راه‌های مقابله با چنین تهدیداتی چیست؟ برای یافتن پاسخ این پرسش‌ها و سوالات دیگر در مورد کلید قطع اینترنت، با ما همراه شوید.

پس از حوادث یازده سپتامبر، دولت آمریکا به بهانه مبارزه با تهدیدات تروریستی فرا رو، قانونی تحت عنوان قانون میهن دوستی آمریکا را به تصویب رساند تا کنترل‌های امنیتی خود را افزایش دهد. این لایحه بدعتی امنیتی در تاریخ آمریکا و در تاریخ روابط بین‌الملل بود که طی مدت زمانی اندک لایحه‌ای را به تصویب رساندند.

## \* فضای سایبر؛ دارایی ملی آمریکا

ده سال پس از این حادثه، دولت آمریکا بار دیگر اقدامی مشابه را این بار در فضای سایبر در دست انجام دارد. پس از تحولات مصر و اقدام دولت سرنگون شده این کشور در قطع اینترنت برای جلوگیری از سازماندهی معترضان، دولت آمریکا نیز به این فکر افتاد تا امکان اقدامی مشابه را در سطح جهانی برای خود فراهم کند. بر این اساس لایحه‌ای ۲۰۰ صفحه‌ای را با عنوان لایحه امنیت سایبری تقدیم کنگره کردند. عنوان دقیق این لایحه، «قانون حمایت از فضای سایبری به عنوان دارایی ملی» است که تشکیل دفتر سیاست‌گذاری فضای سایبر در دفتر ریاست جمهوری و «مرکز ملی امنیت سایبری و ارتباطات» در سازمان امنیت ملی آمریکا یکی از بندهای این لایحه است. وظیفه این بخش، کنترل تمام ورودی‌ها و خروجی‌های درگاه اینترنت از طریق شرکت‌های سرویس دهنده اینترنت است.

بر اساس دو قانون یاد شده، دولت اوپاما نیز همچنان اقدام نظامی علیه کشورهای دیگر یا علیه گروه‌های مخالف غیردولتی (یا تروریستی) در مناطق مختلف جهان را، آنچنان که دولت بوش مورد پذیرش و عمل قرار داده بود، دنبال می‌کند و در این رابطه، نه تنها خود را نیازمند تصویب قطعنامه‌های سازمان ملل متحد و اقدام‌ها و بررسی‌های بین‌المللی نمی‌داند، بلکه دفاع پیشگیرانه و نیز حمله «پیش‌دستانه» را نیز حق خود می‌داند، امری که در تناقض آشکار با منشور ملل متحد است که بر اساس آن، هیچ کشوری اجازه ندارد جز در حالت دفاع مشروع، دست به اقدام یک جانبه نظامی بزند.

## \* Kill Switch؛ مهم‌ترین بخش لایحه امنیت سایبری

یکی از مهم‌ترین بخش‌های لایحه امنیت سایبری که جنجال بسیاری نیز به دنبال داشته، کلید قطع اینترنت یا Internet Kill Switch است. براساس این بند از لایحه، در صورت تصویب، رئیس‌جمهور آمریکا می‌تواند در شرایط اضطراری مانند حملات سایبری به تأسیسات و زیرساخت‌ها، بخشی از ورودی‌های شبکه جهانی اینترنت به آمریکا را مسدود کند و به طور کلی با ابلاغ به سرویس‌دهنده‌های عمده اینترنت جهان همچون یاهو و گوگل، سرویس‌دهی آن‌ها را متوقف کند. این قسمت از لایحه از نظر فنی و سیاسی بیشترین بحث‌ها را تاکنون در پی داشته است. کارکرد kill switch بدین صورت است که در مقیاس کوچک، در صورت وجود احتمال حمله سایبری، دولت آمریکا ارتباط یک زیرساخت - مانند نیروگاه - با شبکه جهانی را بطور کامل قطع خواهد کرد و یا تمامی ورودی‌ها و خروجی‌های آن را به طور کامل رصد کرده و کنترل می‌کند. این بخش از این قانون انتقادات فراوانی را برانگیخته، چرا که منتقدان و کارشناسان فضای سایبر این اقدام آمریکا را مصادره کنترل اینترنت دانسته و این قانون اینترنت جهانی را دارایی ملی ایالات متحده فرض می‌کند.

## \* علم کردن چین هراسی؛ احتمال طراحی یازده سپتامبر سایبری

سنا توری لیبرمن از تدوین‌کنندگان این لایحه، اینترنت را برای کاربران آن مکانی خطرناک توصیف می‌کند که دشمنان می‌توانند با استفاده از خطوط الکترونیک تهدیدات امنیتی فراوانی را متوجه امنیت کشور کنند. یکی از دستاویزهای اصلی تهیه‌کنندگان این لایحه، حملات سایبری کاربران

چینی است. براساس این ادعا روزانه میلیون‌ها حمله سایبری علیه آمریکا صورت می‌گیرد که ۹۸ درصد آن‌ها از چین سازماندهی می‌شود و برای مقابله با این حملات باید امنیت را به فضای سایبر بازگرداند. لیبرمن در این خصوص به سی‌ان‌ان می‌گوید: "رییس‌جمهور و دولت هیچ‌گاه اینترنت را تسخیر نخواهند کرد." لیبرمن در مورد اینکه آیا طرح او و کالینز با آزادی‌های مدنی مغایرتی ندارد، اظهار داشت: "یک حمله سایبری به آمریکا می‌تواند هم‌چون یک حمله نظامی، یا حتی فراتر از آن، به بانک‌ها، ارتباطات، اقتصاد و حمل و نقل ما آسیب برساند." وی برای توجیه این قانون، به اختیاراتی که دولت چین در زمینه اینترنت دارد، اشاره کرده و اظهار می‌دارد: "دولت چین می‌تواند در وضعیت جنگی بخش‌هایی از اینترنت خود را قطع کند، ما نیز می‌خواهیم چنین امکانی را در اینجا داشته باشیم." به گفته وی، اختیار رییس‌جمهور آمریکا در استفاده از این طرح محدود به زمان‌هایی شده که امنیت سایبری تهدید می‌شود و چنین اختیاری بر اساس قانون اعطا شده است.

براساس اطلاعات موجود، ۴۰ درصد از شبکه اینترنت چین که عمدتاً ارتباط زیرساخت‌های حیاتی این کشور را تأمین می‌کند، اینترنت ملی بوده و امکان حمله به آن از خارج از کشور وجود ندارد و در صورت بروز تهدیدات سایبری، زیرساخت‌های این کشور از حملات احتمالی مصون خواهد بود.

با توجه به افزایش مطرح شدن تهدید چین به عنوان پایگاه حملات سایبری به آمریکا و با وجود پیشینه حملات یازده سپتامبر و آغاز جنگ‌افروزی آمریکا برای برقراری نظم نوین جهانی، این احتمال که حملات سایبری پرحدامنه علیه زیرساخت‌های آمریکا طراحی و اجرا شود دور از ذهن نیست. با وجود تاکید بسیار مقامات پنتاگون بر آسیب‌پذیر بودن شبکه برق آمریکا و ایجاد هراس از خاموشی سراسری در صورت بروز حملات سایبری، طراحی یازده سپتامبر سایبری از جمله پیش‌بینی‌های سیاستمداران و کارشناسان بوده است.

با این که براساس آخرین خبرها، «کلید قطع اینترنت» از آخرین لایحه امنیت سایبری حذف شده است. کاخ سفید ادعا می‌کند که بنا بر قانون ۱۹۳۴ که منجر به شکل‌گیری «کمیسیون ارتباطات فدرال» شد، رییس‌جمهور آمریکا همچنان قادر به دخالت در شبکه جهانی اینترنت است. بنا بر این قانون، در صورت بروز هر گونه شرایط اضطراری یا بحران یا خطری که ملت را تهدید کند، رییس‌جمهور دارای حق استفاده یا کنترل هر گونه ... پایگاه یا وسیله‌ای است. با وجود این که جنبه‌های بحث‌برانگیز از این لایحه حذف شد. این لایحه همچنان دربرگیرنده مفاد بسیاری است که نشان‌دهنده اعطای قدرت گسترده‌ای به رییس‌جمهور به نمایندگی از دولت فدرال است. یکی از مفاد این لایحه، این قدرت را به وزارت امنیت داخلی آمریکا می‌دهد تا از شرکت‌های خصوصی در بخش‌های خاصی ارزیابی احتمال خطر به عمل آورد و آنان را مجبور به پیروی از فرمان‌های گسترده جهت ایمن‌سازی سیستم‌هایشان کند.

### \* کلید هفت مرحله‌ای قطع اینترنت

به جز Switch Kill، کلید قطع دیگری برای قطع شبکه جهانی وجود دارد که از هفت کلید یا کارت هوشمند تشکیل شده و در دست گروهی هفت نفره از بریتانیا، ایالات متحده، بورکینا فاسو، ترینیداد و توباگو، کانادا، چین و جمهوری چک است. برای فعال کردن این کلید باید پنج عضو از هفت عضو در پایگاهی در آمریکا گرد هم آیند تا کل سیستم را restart کنند. این کلیدها در واقع کارت‌های هوشمندی هستند که هر یک دربرگیرنده بخشی از کلید اصلی DNSSEC (ضمیمه‌های امنیتی سامانه نام دامنه) است. این برنامه امنیتی زیر نظر «شرکت اینترنتی نام‌ها و شماره‌های واگذارشده» یا به اختصار «آیکان» (ICANN) اداره می‌شود. این شرکت یک گروه نظارتی است که به یک سیستم امنیتی دسترسی دارند سیستمی که جهت محافظت از کاربران در برابر کلاهبرداری‌ها و حملات سایبری طراحی شده است.

امیرعلی فتحي - کارشناس دفتر حراست

(بخش اول)