

# امنیت زیرساخت های فضای سایبری

( از نگاه رئیس جمهور آمریکا )



## فهرست

- ۵ ..... فضای سایبر و امنیت رفاه شهروندان
- ۶ ..... جنگ های نوین در فضای سایبر
- ۷ ..... تهدید سایبری و راهکار مقابله
- ۹ ..... اقدامات پیش رو

اوباما، رئیس جمهور آمریکا در تاریخ ۲۹ مه ۲۰۰۹ طی یک سخنرانی دیدگاه خود را پیرامون امنیت زیرساخت های فضای مجازی و اهمیت سرمایه گذاری و صرف توان و انرژی جهت حفظ و ارتقای امنیت و پایداری آن بیان می کند. در این کتابچه جهت آشنایی با نظرات سیاستمداران این کشور نسبت به فناوری های نوین اطلاعاتی و ارتباطی به انعکاس گزیده ای از سخنان وی پرداخته شده است.

## آغاز

بدون وجود زیرساخت های رقومی، که زیربنای اقتصاد پررونق و ارتش نیرومند و دولت باز و کارا را تشکیل می دهد، قادر نبودیم به پیشرفت های امروز دست پیدا کنیم و پاسخگوی هیچ یک از چالش های قرن بیست و یکم باشیم. بدون این زیرساخت، هیچ یک از این کارها شدنی نیست.

مدت ها است که گفته می شود انقلاب وسایل ارتباطی و فناوری اطلاعات، جهانی مجازی را پدید آورده؛ اما اشتباه نکنید: این جهان- فضای سایبری- جهانی است که زندگی روزمره ما وابسته به آن است. نرم افزار و سخت افزار ما، رایانه رومیزی و دستی ما، تلفن های همراه و گوشی های تلفن در همه ابعاد زندگی روزمره ما تنیده شده است.

شبکه های باند پهن و سیگنال های بیسیم اطراف ما، شبکه های محلی مدارس و بیمارستان ها و شرکت های تجاری، و شبکه های عظیمی که به کشور برق رسانی می کنند، ارتش طبقه بندی شده و شبکه های ضداطلاعات که امنیت ما را تأمین می کنند و شبکه سراسری جهانی که ما را بیش از هر دوره ای در تاریخ بشریت با یک

دیگر مرتبط کرده است به ما نشان می‌دهد فضای مجازی یک واقعیت است و خطرات همراه آن هم واقعیت دارند.

شگفتی بزرگ عصر اطلاعات این است که دقیقاً همان فناوری‌هایی که در ساختن و بنا کردن به ما قدرت می‌دهند، به افرادی که اختلال و تخریب ایجاد می‌کنند هم قدرت می‌دهند. و این جمع اضداد، چیزی است که ما هر روزه آن را تجربه می‌کنیم.

### **فضای سایبر و امنیت رفاه شهروندان**

موضوع، زندگی خصوصی و امنیت اقتصادی خانواده‌ها است. ما برای پرداخت صورت حساب‌ها و قبض‌ها، انجام عملیات بانکی، خرید، و تشکیل پرونده مالیاتی به رایانه متکی هستیم. اما برای مواجهه با تبهکاران جهان مجازی و در امان بودن از زیان‌هایی که به ما وارد می‌کنند مجبور بوده ایم مفاهیم تازه ای یاد بگیریم، نرم افزارهای جاسوسی، نرم افزارهای نفوذ، هک و جعل صفحات تارنما و ویروس‌های رایانه ای، میلیون‌ها قربانی می‌گیرد که به حریم خصوصی آن‌ها تجاوز شده، هویتشان به سرقت رفته، زندگی‌شان زیر و رو و جیبشان خالی شده است. طبق یک همه پرسی، تنها در دو سال گذشته جرم‌های مجازی بیش از ۸ میلیارد دلار برای مردم هزینه داشته است.

ما برای متحول کردن سیاست‌هایمان، بهره برداری زیادی از اینترنت و فناوری کرده ایم. اما آنچه که همه نمی‌دانند این است که طی انتخابات عمومی، سارقان اطلاعات توانستند به سامانه‌های رایانه ای ما رخنه کنند. در ماه‌های اوت و اکتبر، سارقان اطلاعات توانستند به ایمیل‌ها و یک سلسله پرونده‌های مربوط به موضع گیری‌های سیاسی و برنامه‌های مسافرتی کمپین، دست پیدا کنند. ما همکاری نزدیکی با CIA، FBI و سرویس مخفی آغاز کردیم و برای بازسازی امنیت سامانه‌های خود از مشاوران امنیتی کمک گرفتیم. این، یادآوری مؤثری

بود: در عصر اطلاعات، یکی از بزرگترین نقاط قوت می‌توانست یکی از بزرگترین نقاط آسیب‌پذیر هم باشد.

این موضوع با رقابت اقتصادی و محیط کسب و کار هم مرتبط است. یک پیشه‌ور جزء، یک دلال بورس و یا کارکنان یک شرکت حمل و نقل همگی به شبکه رایانه‌ای نیاز دارند، یکی برای پرداخت حقوق، یکی برای انجام معامله، یکی برای نوبت ارسال کالا و غیره. اما هر روزه شاهد سارقان مجازی هستیم که در جستجوی اطلاعات حساس هستند؛ یک کارمند ناراضی در داخل کشور، سارق منفردی هزاران مایل دورتر از ما، تبهکاران سازمان‌یافته، جاسوسان صنایع، و به طور فزاینده‌ای سازمان‌های ضداطلاعات خارجی. سال قبل، سارقان طی عملیات بی‌شرمانه‌ای توانستند با دزدی اطلاعات مربوط به کارت‌های اعتباری، از ۱۳۰ دستگاه خودپرداز بانکی در ۴۹ شهر جهان میلیون‌ها دلار سرقت کنند و این کار را تنها طی ۳۰ دقیقه انجام دادند. برآورد شده که فقط در سال پیش، تبهکاران مجازی موفق به سرقت حقوق مالکیت معنوی، معادل یک تریلیون دلار شدند.

به طور خلاصه، رونق اقتصادی، امنیت عمومی و امنیت ملی در قرن بیست و یکم در گروی امنیت سایبری است. ما برای خدمات سوخت و گازرسانی، و آب و برق‌رسانی روی شبکه‌های رایانه‌ای حساب می‌کنیم. و همین‌طور برای حمل و نقل عمومی و کنترل ترافیک هوایی. و اطلاع داریم که متجاوزان مجازی در شبکه برق‌رسانی ما کاوش‌هایی کرده‌اند و در کشورهای دیگر جهان، این‌گونه حملات موجب شده شهرها در تاریکی فرو بروند.

## **جنگ‌های نوین در فضای سایبر**

برتری فناوری ما رمز تسلط ما است. اما شبکه‌های دفاعی و نظامی ما تحت حملات مداوم قرار دارند. القاعده و دیگر گروه‌های تروریستی از قصد خود برای

آغاز حملات مجازی صحبت کرده اند؛ حملاتی که ردیابی آن و دفاع در برابر آن مشکل تر است. البته در جهان امروز، عملیات تروریستی تنها از سوی محدودی از افراط گرایان که به خود مواد منفجره می بندند ناشی نمی شود، بلکه با فشار دادن چند کلید روی رایانه توسط هر کسی می تواند انجام شود.

در یکی از جدی ترین حوادث سایبری تا امروز علیه شبکه های ارتش، هزاران رایانه توسط نرم افزار نفوذی از کار افتاد. البته اطلاعات حساس در معرض خطر قرار نگرفت اما نیروها و پرسنل دفاع مجبور شدند از استفاده از فلاش درایوها که ابزاری برای حافظه خارجی هستند صرف نظر کرده و هر روزه روش بکارگیری رایانه را تغییر دهند.

سال قبل توانستیم با چهره جنگ های آینده آشنا شویم. هنگامی که تانک های روسی وارد گرجستان می شدند، حملات سایبری هم وبسایت های دولتی گرجستان را از کار انداخت. تروریست هایی که مرگ و خرابی در بمبئی به بار آوردند، نه تنها به سلاح های خود متکی بودند، بلکه عملیاتشان را با استفاده از GPS و تلفن های اینترنتی هم جلو بردند.

## تهدید سایبری و راهکار مقابله

به تمام دلایلی که گفته شد، روشن است که تهدید سایبری یکی از جدی ترین چالش های اقتصادی و امنیت ملی است که ما به عنوان ملت با آن رو به رو هستیم.

این هم روشن است که ما در مقام دولت یا کشور، آن طور که باید آمادگی نداریم. در سال های اخیر، پیشرفت هایی صورت گرفته. اما همان طور که در گذشته موفقیت چندانی در سرمایه گذاری برای زیرساخت های فیزیکی نداشته ایم، در سرمایه گذاری برای امنیت زیرساخت های رقومی خودمان هم موفق نبوده ایم.

در دولت، دفتر واحدی برای نظارت بر سیاست امنیت سایبری وجود ندارد، و اداره ای نیز مسئول هماهنگ کردن محدوده و ابعاد این چالش نیست. البته وقتی پای امنیت سایبری به میان می‌آید، ادارات فدرال دارای مأموریت‌هایی هستند که با یک دیگر تداخل دارد و نمی‌توانند آن طور که باید با یک دیگر یا با بخش خصوصی ارتباط برقرار کرده و هماهنگی ایجاد کنند. ما در پاسخ غیر منسجم به کرم اینترنتی «کانفیکر» که در ماه‌های اخیر به میلیون‌ها رایانه در جهان سرایت کرد، شاهد این امر بودیم. این وضعیت بیش از این تحمل کردنی نیست مخصوصاً زمانی که همه امور با خطر مواجه است. ما می‌توانیم و باید اقدامات مؤثرتری در پیش بگیریم و به همین خاطر، من کمی بعد از آغاز کارم، از شورای امنیت ملی خود و شورای امنیت کشور خواستم تا بررسی کاملی در مورد تلاش‌های دولت برای دفاع از اطلاعات و زیرساخت‌های ارتباطی به عمل آورده و بهترین راه برای اطمینان از توانایی این شبکه‌ها، آن طور که ما می‌خواهیم به ما ارائه دهند.

امروز گزارشی از این بررسی ارائه می‌دهم و اعلام می‌کنم که دولت برای تأمین امنیت زیرساخت‌های رقومی رویکرد جدید و جامعی را دنبال می‌کند. از این پس، با زیرساخت‌های رقومی یعنی با شبکه‌ها و رایانه‌هایی که هر روزه به آن‌ها وابسته هستیم به عنوان یک دارایی راهبردی ملی برخورد می‌شود و حفاظت از این زیرساخت‌ها تبدیل به یک اولویت در امنیت ملی می‌گردد. ما اطمینان می‌دهیم که این شبکه‌ها امن، مورد اعتماد، و قوی باشند. ما از آن‌ها در برابر هر نوع حمله ای دفاع و از آن صیانت می‌کنیم و در صورت وقوع هر نوع اختلال یا لطمه، آن را به سرعت برطرف می‌کنیم.

برای ارتقای سطح تلاش و ایجاد توجه لازم و تمرکز ضروری درصدد ایجاد دفتر تازه ای هستیم که ریاست آن را شخص هماهنگ کننده سایبری به عهده خواهد داشت. به دلیل حساسیت این کار، من به شخصه این مقام را انتخاب می‌کنم و در مورد همه امور مربوط به امنیت مجازی به این مقام متکی خواهم بود.



این مقام از حمایت کامل من و دسترسی منظم به من برای رویارویی با هر نوع چالش برخوردار خواهد بود.

مسئولیت‌هایی که به عهده این دفتر است، شامل این موارد خواهد بود: هماهنگی و ادغام کلیه سیاست‌های مجازی برای دولت؛ همکاری نزدیک با دفتر برنامه و بودجه جهت اطمینان از مطرح شدن این اولویت‌ها در بودجه ادارات دولتی؛ و ایجاد هماهنگی در پاسخ ما، در صورت بروز پیچیدگی یا حمله سایبری.

## اقدامات پیش‌رو

کارهای زیادی باید انجام گیرد، و گزارشی که ارائه می‌شود نشان دهنده خطوط اصلی اقداماتی است که ما در پنج زمینه اصلی در پیش خواهیم گرفت.

۱. استراتژی تازه و جامعی برای تأمین امنیت شبکه‌های اطلاعاتی و ارتباطی ایجاد خواهیم کرد.

۲. برای اطمینان از پاسخی سازمان یافته و واحد به اتفاقات آینده سایبری با همه دست اندرکاران اصلی همکاری خواهیم کرد. با در نظر گرفتن صدمات عظیمی که تنها یک حمله سایبری ممکن است در پی داشته باشد، واکنش‌های خلق الساعه کارساز نخواهد بود و تقویت تدابیر دفاعی بعد از وقوع حوادث یا حملات، کافی نیست. به همان روشی که در مورد بلایای طبیعی اقدام می‌شود، ما باید از قبل، منابع و برنامه‌های خود را آماده داشته باشیم؛ مانند اشتراک اطلاعات، دادن اخطار و تضمین پاسخ هماهنگ.

۳. مشارکت بخش‌های دولتی و خصوصی را که در این تلاش‌ها دارای حساسیت است، تحکیم می‌کنیم. دولت من استانداردهای امنیتی را به شرکت‌های خصوصی دیکته نخواهد کرد. بر عکس، ما برای یافتن

راه حل‌های استفاده از فناوری برای تضمین امنیت و ارتقای رفاه و آسایش، با یک دیگر همکاری خواهیم کرد.

۴. به سرمایه‌گذاری در جدیدترین پژوهش‌ها و توسعه ضروری برای نوآوری و تحقیقات مورد نیاز جهت رویارویی با چالش‌های رقومی، ادامه می‌دهیم. استقرار باند پهن؛ ساخت شبکه برقی هوشمند برای انتقال بهتر انرژی؛ تهیه سامانه‌های جدیدتر برای کنترل ترافیک هوایی و بکارگیری گزارش‌های پزشکی از طریق الکترونیک، جهت کاهش هزینه‌ها و نجات جان بیماران، با حفظ محرمانگی از الویت‌ها خواهد بود.

۵. و در پایان، ایجاد یک مبارزه ملی برای ارتقای آگاهی‌های سایبری و فناوری رقومی و انتقال آن از اتاق‌های هیئت مدیره به کلاس‌های درس، و ایجاد نیروی کار رقومی مناسب قرن بیست و یکم. و برای همین است که تعهد تازه‌ای نسبت به آموزش ریاضیات و علوم داشته و سرمایه‌گذاری‌های تاریخی را در علوم و تحقیقات توسعه می‌پذیریم. زیرا برای کودکان و دانش‌آموزان ما کافی نیست که بر فناوری امروز مانند ارتباطات اجتماعی شبکه‌ای و ایمیل زدن و تکست زدن و بلاگ نویسی تسلط داشته باشند، ما نیاز داریم آن‌ها طایفه دار فناوری‌هایی باشند که کارایی ما در رسانه‌های جدید را ارتقا داده و متضمن پیشرفت ما در آینده باشند.

البته فعالیت‌های مورد نظر در جهت تضمین امنیت سایبری، شامل زیرنظر داشتن شبکه‌های بخش خصوصی یا ترافیک اینترنتی نخواهد بود. ما زندگی خصوصی و فردی، و آزادی‌های مدنی را که مردم به آن ارج می‌نهند، حفظ و از آن صیانت می‌کنیم. البته قاطعانه از بی‌طرفی اینترنت حمایت می‌کنیم و به همین خاطر اینترنت را همانگونه که باید، حفظ خواهیم کرد، یعنی باز و آزاد.

وظایفی که برشمردم، آسان نخواهد بود. حدود ۱.۵ میلیارد تن از جمعیت جهان هم اکنون از اینترنت استفاده می‌کنند، و تعداد بیشتری هم روزانه به این کاربران اضافه می‌شود. گروه‌ها و دولت‌ها قابلیت‌های خود را توسعه می‌دهند. حفاظت از رفاه، آسایش و امنیت در این دنیای جهانی شده مبارزه‌ای طولانی و دشوار خواهد بود که نیاز به سال‌ها شکیبایی و پشتکار دارد. اما باید به یاد داشته باشیم: ما در آغاز کار هستیم. دوره‌های تاریخ طولانی هستند؛ انقلاب کشاورزی، انقلاب صنعتی، در مقایسه با این‌ها، عصر اطلاعات هنوز دوران کودکی خود را می‌گذراند.