

فضای سایبر، میدان اصلی

تهاجم و دفاع

فهرست

- ۳ مقدمه
- ۴ فصل اول: دیدگاه مسئول فرماندهی سایبری آمریکا در رابطه با فضای سایبر
- ۱۱ فصل دوم: پروژه های جنگ نرم آمریکا علیه ایران

این کتابچه جهت آشنایی با دیدگاه های مسئولین دفاعی آمریکا در خصوص فضای سایبر و مجموعه اقدامات دفاعی و تهاجمی ایشان در فضای سایبر تهیه شده است. در فصل اول بخشی از مهمترین مطالب بیان شده توسط ژنرال «کیت الکساندر» مسئول فرماندهی سایبری آمریکا که طی مراسمی در حضور کمیته نیروهای مسلح مجلس سنای آمریکا در تاریخ ۲۳ سپتامبر ۲۰۱۰ بیان کرده است، ارائه شده؛ وی در سخنانی به تشریح وضعیت فرماندهی سایبری ایالات متحده پرداخته است. فصل دوم به انعکاس گزیده گزارشی که به تازگی توسط کاخ سفید منتشر شده است، می پردازد. در سال ۲۰۱۰ کنگره آمریکا ضمن تصویب بودجه ۵۵ میلیون دلاری برای جنگ نرم علیه جمهوری اسلامی ایران، رئیس جمهور آمریکا را موظف کرد این گزارش را با موضوع تلاش های آمریکا در این راستا و ارزیابی تأثیر اقدامات انجام شده، ارائه دهد.

فصل ۱

دیدگاه مسئول فرماندهی سایبری آمریکا در رابطه با فضای سایبر

در فضای سایبر تنها دفاع «کامل» یک دفاع ایستا است، یعنی قطع کردن اینترنت و در نتیجه قربانی کردن حوزه سایبر و مزایای اقتصادی و اجتماعی آن برای دشمنان. البته گزینه «قطع کردن» برای خود جامعه آمریکا امکان پذیر نیست؛ خانه‌ها، مشاغل، مدارس، بیمارستان‌ها، دفاتر حکومتی و در واقع سبک زندگی ما اکنون به داشتن دسترسی به شبکه‌ها بستگی دارد. حتی اگر رایانه نداشته باشید، شما به همسایگان، همکاران و نهادهایی که رایانه دارند وابسته هستید.

درگیری سایبری مدیریت آسیب‌ها و شناسایی خطر است

درگیری سایبری ما یک مدیریت محتاطانه آسیب‌پذیری و شناسایی خطر است. از آنجا که امنیت در یک دنیای شبکه‌ای یک سامانه برای مدیریت آن خطر است، ما در فرماندهی سایبری آمریکا سامانه‌ای از تدابیر امنیتی برای شبکه‌های وزارتخانه‌ها داریم.

این سامانه عبارت است از رصد شبکه، آگاهی از اوضاع؛ هشدارها، بسته‌های مکمل و به روز رسانی برنامه‌های ضدبدافزار، فایروال‌ها، ارزیابی‌های امنیتی عینی،

امکان شناسایی خودکار مزاحم و مسدود کردن آن، جستجوهای فعال برای بدافزارها و تیم‌های پاسخ قانونی. ما همه این‌ها را با آنچه که «عملیات‌های پویای دفاع شبکه‌ای» می‌نامیم مدیریت می‌کنیم و این سنگ بنای کار ما است.

حفاظت را به زیرساخت‌های حیاتی مان گسترش دهید

حدود یک نسل پیش، هنگامی که استفاده از رایانه‌ها از حالت اختیاری خارج و برای عملکردهای اصلی، ضروری شد، زیرساخت تقویت کننده جامعه و اقتصاد از یک نقطه عطف عبور کرد و امروز رئیس‌جمهور او با ما حفاظت از زیرساخت فناوری اطلاعات و ارتباطات را یک اولویت امنیت ملی قرار داده است. امروز منابع انرژی، تاسیسات، حمل‌ونقل عمومی، بانکداری، دفاتر ثبت و خیلی موارد دیگر ما در "نت" هستند.

ارتش برای ارتباطات بیشتر به شبکه‌های طبقه‌بندی نشده وابسته است

ارتش نیز برای ارتباطات بیشتر و عملکردهای تدارکاتی خود به شبکه‌های طبقه‌بندی نشده وابسته است. اتوماسیون و شبکه‌سازی اگرچه فرماندهی و کنترل چنین سامانه‌هایی را تسهیل می‌سازد، اما بُعدی از پیچیدگی و همراه با آن آسیب‌پذیری را نیز به آن می‌افزاید که بوجود آورندگان آن هرگز پیش‌بینی نمی‌کردند. به همین خاطر محافظت و دفاع از سامانه‌های قدیمی که زیرساخت‌های حیاتی ما را به حرکت درمی‌آورند، ذاتا مشکل‌تر از سامانه‌های مدرنی هستند که امروزه ساخته می‌شوند.

هیچ کس تاکنون به طور جدی به این‌ها حمله نکرده اما ما شاهد کاوش آن سامانه‌ها از سوی دشمنان خود بوده‌ایم. ما به اندازه کافی آسیب‌پذیری آنها در

نتیجه بلایای طبیعی و اشتباهات تصادفی را مشاهده کرده‌ایم که اکنون در مورد آثار بالقوه یک حمله واقعی علیه بخش‌هایی از زیرساخت شبکه‌ای خود نگران باشیم.

در صورت حمله تمامی نهادهای دولتی باید هماهنگ واکنش نشان دهند

زمانی برای از دست رفتن وجود ندارد، چراکه حملات و آثار بالقوه آنها تفاوتی بین کاربران نظامی و غیرنظامی قائل نخواهند شد. ممکن است از جانب یک کشور دشمن، یک گروه تروریستی، یا حتی یک فرد شرور صورت بگیرند. وزارت امنیت داخلی ممکن است به ابزار و مشاوره تخصصی از جانب NSA و فرماندهی سایبری نیاز داشته باشد؛ هر دوی این سازمان‌ها آماده مساعدت هستند. به علاوه، در صورت وقوع یک حمله باید تلاش نماییم که در سرتاسر دولت به صورت هماهنگ واکنش نشان دهیم. باید دفاع گروهی تقویت شود. من دوست دارم سایر را یک ورزش تیمی بخوانم؛ دفاع موفق در هر قسمت به تلاش‌های مشترک دستگاه‌ها، صنعت، هم‌پیمانان، و همکارانی بستگی دارد که از شبکه‌های خود در مقابل مشکلاتی که می‌توانند همه آنها را تحت تاثیر قرار دهند، مراقبت می‌کنند. هر یک از ما، و همکاران، دوستان، و خانواده‌های ما، همگی شرکت‌کننده هستیم.

برای اجتناب از قربانی شدن، باید گام‌هایی مثبت و مداوم برداریم. ما همگی بخشی از یک راه‌حل مرکب برای یک مشکل مشترک هستیم. همه ما سهم خود را انجام می‌دهیم تا پیچیدگی دنیای جدیدمان را درک کرده و آسیب‌پذیری خود را کاهش دهیم. اگر کاربران در خانه‌ها و دفاتر خود بسته‌های نرم‌افزاری مکمل و به روز رسانی‌های توصیه شده توسط سازندگان را دانلود و نصب کنند، بسیاری از مسائلی که ما را شب‌ها و اواخر هفته سر کار نگه می‌دارند حل خواهند شد.

این موضوع تازه‌ای نیست، خیلی دشوار است که نگاهمان به امنیت همانند نگاهمان به قفل و میله و نگهبان باشد. امنیت همیشه ناراحت‌کننده است و این ناراحتی در فضای سایبر بیش از موارد دیگر مشهود است چرا که «به روز بودن» مستلزم صرف وقت است. با این حال، هزینه حمله موفق خیلی بیشتر از هزینه اتصال و استفاده از نرم‌افزار و سخت‌افزار برای متصل بودن است.

نیاز به استانداردها و اصطلاحات مشترک و اطلاعات به موقع

برقراری امنیت نیازمند استانداردها و اصطلاحات مشترک و به اشتراک‌گذاری حجم‌های عظیمی از اطلاعات به موقع است، ما در فرماندهی سایبری همکاری‌های نظامی و اطلاعاتی قوی و آزمایش شده‌ای با هم‌پیمانانمان داریم که در شکل دادن به یک تصویر عملیاتی مشترک کمک می‌کند و ما در صددم این حلقه همکاری‌ها را گسترش دهیم. هیچ یک از ما آن‌قدر اختیار، توانمندی، یا منابع در اختیار ندارد که بتواند به تنهایی کار کند. ما باید با یکدیگر کار کنیم.

نقاط ضعف آمریکا در فضای سایبر ابتدا فرهنگی خواهد بود

راه‌حل نقاط ضعف ما در فضای سایبر در وهله اول فرهنگی خواهد بود، ما الزاماً به فناوری «بتر» نسبت به دیگران در زمینه‌هایی مانند پهنای باند، ذخیره‌سازی، نسخه‌های نرم‌افزار، سرعت‌های عملیاتی، حجم حافظه و غیره نیاز نداریم. در هر صورت، برتری‌های صرفاً فناورانه احتمالاً در دنیای شبکه‌ای ما زیاد دیرپا نخواهند بود.

برتری ما باید در نحوه کنار هم گذاشتن این ابزارها در سامانه‌ها نهفته باشد؛ بویژه سامانه‌های افراد، پروتکل‌ها، و ماشین‌هایی که بتوانند به طور قابل اطمینانی در کنار یکدیگر به سرعت کار کنند تا ضعف‌ها را شناسایی کنند، اطلاعات را به

اشتراک بگذارند، ریسک‌ها را ارزیابی نمایند، تدابیری را توصیه نمایند و راه‌حل‌های جدید را بکار بگیرند.

اگرچه فرماندهی سایبری آمریکا اختیاری در رفع نیازمندی‌های خود نخواهد داشت اما ما در تعریف نیازمندی‌ها به فرماندهی راهبردی آمریکا کمک خواهیم کرد. ما همچنین در فرماندهی سایبری در «چارچوب امنیت پایدار» شرکت خواهیم کرد. این چارچوب گروهی متشکل از نمایندگان وزارتخانه‌های دفاع و امنیت کشور و مدیر امنیت ملی است که به طور مرتب با سران بخش خصوصی و کارشناسان عرصه سایر ملاقات‌هایی انجام می‌دهند.

با هرگونه حمله سایبری به آمریکا و منافعش مقابله می‌کنیم

فرماندهی سایبری آمریکا این همکاری را برای کمک به بخش خصوصی در پرداختن به تهدید امنیت سایر اساسی قلمداد می‌کند، این قرارگاه با «آژانس پروژه‌های تحقیقات پیشرفته دفاعی» همکاری کرده و از یک محیط «دامنه سایبری ملی» برای ساختن توانمندی‌های خود در این زمینه پشتیبانی می‌کند و بالاخره، یک الزام دیگر ایجاد توانمندی «نیروی کار سایبری» در نیروهای مسلح است.

متقاعد شده‌ام که با ایجاد این فرماندهی گامی مهم برداشته‌ایم. من فلسفه‌مان درباره مدیریت فعالانه شبکه اطلاعات جهانی را - نه تنها برای دفاع از آن، بلکه برای استفاده از آن به عنوان ابزاری جهت کمک به جنگجویان، طراحان و فرماندهان خود بواسطه حفظ وسعت آزادی عمل آنها تا حد ممکن - توضیح دادم و گفتم که تا جایی که بتوانیم و هنگامیکه از ما خواسته شود، آماده خواهیم بود تا از توانمندی‌های خود برای مقابله با هرگونه استفاده خصمانه از فضای سایبری، منافع و زیرساخت‌های آن، استفاده کنیم.

ما این فرماندهی جدید را بر اساس رهنمون‌های مقامات فرماندهی ملی و در ارتباط نزدیک با همکاران عملیاتی خود در وزارت‌های خارجه، دفاع، و امنیت کشور، نیروی انتظامی، جامعه اطلاعاتی، و صنعت و دانشگاه به راه انداخته ایم. ما باید این کار را درست انجام دهیم، چرا که معتقدم امنیت ملت ما به آن بستگی دارد. ما تلاش می‌کنیم این چالش را حل کنیم تا شایستگی اعتماد شما را داشته باشیم.

فصل ۲

پروژه های جنگ نرم آمریکا علیه ایران

در این فصل گزیده گزارش تلاشهای آمریکا در راستای جنگ نرم علیه جمهوری اسلامی ایران ارائه شده است.

پخش اخبار در ایران از جانب نهادهای تحت حمایت مالی دولت آمریکا

پخش بین‌المللی اخبار از آمریکا تحت نظارت اداره «شورای مدیران پخش»^۱ یکی از اصلی‌ترین منابعی است که می‌توان از طریق آن اخبار و اطلاعات لازم در مورد حوادث، اخبار و دیدگاه‌های بین‌المللی و سیاست‌های آمریکا و همچنین گفتمان سیاست‌گذاری در مورد ایران، را به گوش مخاطبین ایرانی رساند. شبکه خبر فارسی صدای آمریکا و رادیو فردا برخی رسانه‌های فارسی‌زبان هستند که ایرانی‌ها می‌توانند از طریق آنها به اخبار و اطلاعات لازم دست یابند. شبکه خبری تلویزیونی صدای آمریکا و رادیو فردا به صورت بیست و چهار ساعته به پخش

^۱ BBG

برنامه پرداخته و اخبار، امور جاری و برنامه‌های فرهنگی را به سمع و نظر تعداد چشمگیری از مخاطبین ایرانی می‌رسانند.

اداره «شورای مدیران پخش» به منظور پشتیبانی از برنامه‌ها، فرکانس‌های ماهواره‌ای جدیدی را پیش‌بینی نمود تا از قبل بر انسداد فرکانس‌های امواج پخش اخبار توسط دولت ایران پیش‌دستی نماید. همچنین یک مسیر اینترنتی حفاظت شده و منحصر به فرد برای ایرانی‌ها تعبیه گردید تا تصاویر ویدئویی خود را به شبکه خبر فارسی صدای آمریکا ارسال نمایند. خدمات وب‌سایت تویتر^۱ نیز به صفحات وب‌سایت فیس‌بوک^۲ و وبلاگ‌ها افزوده شد.

دولت انتظار دارد که با استفاده از کاربردهای جدید موبایل‌های هوشمند مانند آیفون و اندروید^۳، صاحبان موبایل در ایران و دیگر نقاط جهان بتوانند: به وب‌سایت شبکه خبر فارسی صدای آمریکا دسترسی داشته و در صورت تمایل مقاله‌ها را ابتدا دانلود و سپس بخوانند، قطعه‌های خبری را به صفحات تویتر یا فیس‌بوک خود بفرستند تا از این طریق اخبار بخش فارسی صدای آمریکا به صورت ویروسی منتشر شود. به صفحه تویتر مخصوص شبکه خبر فارسی صدای آمریکا دسترسی یابند. تصاویر ویدئویی و عکس را در وب‌سایت شبکه خبر فارسی صدای آمریکا آپلود نمایند. بخش فارسی صدای آمریکا دارای صفحه تویتر، هفت سایت تأیید شده در فیس‌بوک و بیش از ۳۰۰۰ پیوندها است. این شبکه خبری همچنین دارای شش وبلاگ تأیید شده است.

^۱ Twitter

^۲ Face book

^۳ Android

تلاش های دولت ایران برای کنترل اینترنت

قبل از انتخابات اخیر ایران، تلاش های شورای مدیران پخش بیشتر بر وبسایت های فیلترشکن متمرکز بود. همچنین یک نرم افزار فیلترشکن نیز وجود داشت که به کاربران ایرانی اجازه می داد تا به برنامه های شبکه خبر فارسی صدای آمریکا و همچنین رادیو فردا دسترسی یابند.

بعد از افزایش رسمی کنترل، شورای مدیران پخش در تلاش است تا با یافتن منابع جدید برای حمایت از قراردادهای فعلی با فروشندگان نرم افزارهای فیلترشکن و همچنین یافتن نرم افزارهای جدید، به مقابله با دولت ایران در برنامه هایش بپردازد. شورای مدیران پخش وبسایت ها و نرم افزارهای فیلترشکن جدید معرفی کرده و تلاش خواهد کرد تا انطباق پذیری و سازگاری کاربران ایرانی را افزایش دهد.

برنامه های شورای مدیران پخش برای استفاده از مقادیر اختصاص یافته

الف) شناسایی و سپس بسط یا تولید برنامه ها و زمینه های^۱ ویژه
ب) بسط یا تولید ظرفیت انتقال اطلاعات از طریق ماهواره، رادیو و یا اینترنت پخش خبر به ایران از طریق تلویزیون، رادیو، اینترنت و دیگر زمینه های دیجیتال یکی از اولویت های اداره شورای مدیران پخش خبر باقی می ماند. پیرو مبالغ اختصاص یافته برای سال مالی ۲۰۱۰ در «قانون تخصیص هماهنگ»^۲ شورای مدیران پخش به پشتیبانی خود از برنامه های دولت آمریکا برای برقراری ارتباط با مخاطبین ایرانی که اهمیت زیادی دارد، ادامه خواهد داد.

^۱ platform

^۲ Consolidated Appropriations Act

صندوق رسانه، تعامل و آموزش الکترونیکی ایرانی‌ها

آموزش روزنامه‌نگاران طبق استانداردهای بین‌المللی و تدارک دسترسی به اطلاعات فیلتر نشده در اینترنت و همچنین تدارک امکانات زبان فارسی برای این رسانه‌ها و ابزار جدید.

علاوه بر این دولت آمریکا قصد دارد تا از انواع جدید فناوری‌های مدرن بهره برده تا حمایت و پشتیبانی خود را از دسترسی به اینترنت در ایران عمیق‌تر سازد - تدوین زمینه‌های مجازی، افزایش ضریب امنیتی کاربران و ارائه فناوری‌های ضدفیلترینگ نمونه‌هایی از حوزه‌های احتمالی هستند که در آنها برنامه‌ریزی خواهیم کرد.