فصلنامه سیاست خارجی
سال سی و سوم، شماره ۱، بهار ۱۳۹۸، صص ۲۲۸- ۱۹۱

۶

امنیت سایبری در آمریکا
ساختارها و روندها

علی صانعیان [۱]

[۱]. دانش آموخته کارشناسی ارشد دیپلماسی و سازمان‌های بین المللیAli.saneian7@gmail.com

چکیده

اگرچه آمریکا به عنوان توسعه دهنده اصلی فضای سایبری، کشوری پیشرو در این عرصه تلقی می شود. توسعه همه جانبه اینترنت و وابستگی بیش از حد زیرساخت های حساس امریکا به فناوری اطلاعات آن را در معرض انواع تهدیدات سایبری قرار داده است. شبکه بانکی و مالی تا خدمات عمومی، شبکه های مدنی و نظامی همگی به شبکه وابسته بوده در صورت اختلال سایبری همگی آنها از کار می افتند. با بررسی رخدادهای سایبری از دوران کلینتون تا ترامپ، به مراحل مطرح شدن تهدید سایبری در دستور کار سیاسی و سپس امنیتی دولت امریکا طبق الگوی مکتب کپنهاک می پردازیم. همچنین، باجزئیات فرایند منطقی که طی شد تا امنیت سایبری از یک موضوع در حاشیه تحت عنوان کلی زیرساخت حساس به صدر تهدیدات امنیتی امریکا صعود کند را بررسی می‌کنیم. ایجاد و نقش نهادهای درگیر در امنیت سایبری طی فرآیند امنیتی‌سازی فضای سایبری در امریکا رصد می شود. ساختارهای تصمیم‌گیری کاخ سفید و کنگره در مورد تامین امنیت سایبری زیرساخت‌های حساس رویکرد یکسانی ندارند. در این مقاله به تعامل کنگره و کاخ سفید در ایجاد، گسترش یا محدود سازی دستورکار نهادهای سایبری آمریکا خواهیم پرداخت.امریکا ابتدا در دهه نود رویکرد دفاعی حفاظت از زیرساخت های حساس وابسته به شبکه را مد نظر داشته وکنگره و کاخ سفید هردو از خودگردانی و پیشرفت تدریجی فضای سایبری تحت کنترل بخش خصوصی حمایت می‌کردند. در دوره ریاست جمهوری جرج بوش شرایط تغییر کرده، راهبرد سایبری وارد دوران گذار شد، در نهایت، از دوردوم اوباما رویکرد سایبری تهاجمی که کنترل دولت را بر فضای سایبر لازم می داند، برغم نظرکنگره اتخاذ شد. در دوران ترامپ با وجود تلاطم های بسیار هنوز مواضع سایبری دولت و کنگره تثبیت نشده است. سوال اصلی این مقاله آن است که چگونه راهبرد سایبری دفاعی–خودگردانی در آمریکا تبدیل به راهبرد تهاجمی–دولتی شده است؟

واژگان کلیدی

حملات سایبری، امنیت سایبری،تهدید سایبری، راهبرد سایبری آمریکا.

مقدمه

اگر فعالیت های مربوط به امنیت تلگراف و تلفن و نیز سیستم های مجزای کامپیوتر را به عنوان امنیت سایبر به حساب نیاوریم، امریکا برای اولین بار از سال ۱۹۹۶ اقدام به تشکیل واحدهای دفاع سایبری نموده است. اولین نهادی که به طور رسمی برای پدافند و رصد سایبری در بخش غیرنظامی ایجاد شد، شورای حمایت از زیرساخت های حساس بود که وظیفه اش تدوین سیاست‌های لازم در بخش سایبری است. اما مسئولیت دفاع سایبری در بخش نظامی بر عهده فرماندهی سایبری ایالات متحده[1] که زیر مجموعه وزارت دفاع می باشد، است. علاوه براین، آژانس امنیت ملی[2] وابسته به پنتاگون و پلیس فدرال[3]وابسته به وزارت دادگستری و یک وزارت خانه دیگر به نام وزارت امنیت میهنی[4] نیز در زمینه دفاع و امنیت فضای سایبر فعالیت می‌کنند. وزارت امنیت میهنی مسئولیت اجرایی امنیت سایبری در بخش غیرنظامی آمریکا را بر عهده دارد. در واقع، یک وظیفه اجرایی پدافندی در بخش غیرنظامی را عهده دار است. این وظیفه شامل مرکز امداد و نجات رایانه‌ای ملی، سامانه‌های تشخیص‌و مقابله بانفوذ و همچنین سامانه-های‌آگاهی موقعیتی می‌باشد. پلیس فدرال و وزارت دادگستری نیز در موارد جرائم سایبری و پیگیری مجرمین با وزارت امنیت میهنی همکاری می‌نماید، اما از آنجا که عمدتا در تشخیص و محاکمه جرایم و خرابکاری های سایبری فعال هستند و بندرت در ابعاد بین المللی درگیر مباحث سایبری می‌شوند در این مقاله کمتر به آنها پرداخته شده است. هماهنگی تمامی این سازمان‌ها در زمینه امنیت سایبری توسط هماهنگ کننده ستاد عملیاتی فضای سایبری انجام می‌گیرد که به عنوان معاون مشاور امنیت ملی رئیس جمهور در زمینه امنیت سایبری در کاخ سفید می‌باشد(حسینی و ظریف منش،۱۳۹۲). کنگره امریکا هم سعی دارد با ابزار بودجه و نیز قدرت قانونگذاری خود بر

---

1. USCC-United States Cyber Command
2. NSA-National Security Agency
3. FBI-Federal Bureau of Investigation
4. DHS-Department of Homeland Security

فعالیت‌های سایبری امریکا تاثیر گذاشته و در موقع لزوم دخالت های کاخ سفید در این عرصه را به نفع بخش خصوصی تعدیل نماید.

چارچوب نظری

مبنای نظری بکار گرفته شده در این مقاله، رویکرد امنیت سازی «مکتب کپنهاک» است که بر فرآیند ظهور یک موضوع از یک بستر سیاسی شده یا حتی غیرسیاسی به حوزه امنیتی تمرکز دارد و عوامل مختلف شکل‌گیری دستور کار سیاست‌گذاری امنیتی را مورد توجه قرار می دهد. این مکتب تنها مکتب امنیتی است که از بستر فرایندهای سیاسی روابط بین الملل شکل نگرفته و از ابتدا یک مکتب امنیتی بوده است. مکتب کپنهاک در راستای پایه گذاری جایگاهی مستقل برای مطالعات امنیتی است. با توجه به نحوه راهیابی مسایل سایبری که سابقا هیچگونه جایگاهی در مباحث دفاعی و سیاسی نداشتند و طی گفتمان نخبگانی و مناظرات متعاقب آن که در اواخر دهه ۹۰ میلادی آغاز شد، وارد مباحث امنیتی شده، این مکتب مناسب‌ترین گزینه به نظر می-رسد. فرآیند امنیت سازی در این مکتب، روندی است که یک برساخته اجتماعی، مانند فضای سایبری که به عنوان یک برساخته اجتماعی امروزه دست کم بخشی از هویت، کسب وکار، تفریح و حتی دنیای خیلی از افراد جامعه را می سازد و بسیار فراتر از مفهوم اینترنت است، آن را طی می کند و به لحاظ متنی، متأثر از کنش گفتاری است. به این معنا که اگر مطالبات برای یک حق ویژه برای استفاده از هر نوع ابزاری در جهت حل و فصل یک موضوع خاص، ضروری است و آن در عرصه سیاسی پذیرفته شده است، امنیت آن موضوع به شکل موفقیت آمیزی تغییر شکل می دهند؛ نه الزاماً به دلیل یک تهدید وجودی واقعی، بلکه به این دلیل که این موضوع به شکل موفقیت آمیزی توسط بازیگران اصلی عرصه سیاسی به عنوان جزء تشکیل دهنده یک تهدید ، بازنمایی شده است (عزتی به نقل از بیات، ۱۳۸۹). البته این به معنای آن نیست که نگارنده معتقد به ساختگی بودن تهدیدات سایبری برای باشد. (هرچند در مواردی مانند تهدید انگاری و پروپاگاندا علیه برنامه دفاع سایبری ایران واقعا چنین تهدیدی علیه آمریکاوجود ندارد و

تهدیدکاملا ساختگی است). در این نظریه سه مسئله مهم باید تعیین تکلیف شوند یکی امنیتی سازی، دیگری تهدید وجودی و در نهایت مرجع امنیت هستند.

در بحث توسعه گفتمان تهدید سایبری آغاز مناظرات در باب اطلاعات به اواخر ریاست جمهوری رونالدریگان در دوران جنگ سرد بر می‌گردد، که دغدغه های عمده ای در باب پیگیری از افشای اطلاعات طبقه بندی شده در کنار اکتساب اطلاعات حساس اما غیرطبقه بندی شده وجود داشت. در آن دوران بیشتر جنبه جاسوسی استفاده از رایانه پررنگ بوده است. شرایط آن دوران برای شروع گفتمان امنیتی شدن موضوعات سایبری کافی نبود مخصوصا که بخشی از حاکمیت با درخواست وحمایت بخش خصوصی، مخالف امنیتی سازی مباحث امنیت سایبری در حفاظت از زیرساخت های سایبری تحت کنترل بخش خصوصی بودند. در واقع، آنها به سمت موضوعات دیگری اشاره می کردند تا تهدیدات سایبری در این بخش ها را به ریسک تجاری شرکت های خصوصی تقلیل دهند. بنابراین، مخالف قرار گرفتن دولت به عنوان مرجع امنیت سایبری بودند.بعد از ریگان با پیوند چهار موضوع امنیتی (آسیب پذیری نامتقارن، تهدیدات سایبری، تروریسم و زیرساخت ها همچنان امنیتی سازی مباحث سایبری وضعی شناور داشتند و به‌طور منسجم و واحد مورد بررسی قرار نمی‌گرفتند، سرانجام در دور دوم کلینتون یک مفهوم امنیتی بسیار قوی تحت عبارت کلی حفاظت از زیرساخت های حساس به عنوان سیاست امنیتی اعلام شد که متعاقباً در سراسر دنیا نیز گسترش پیدا کرد و مسیر واقعی خود را برای نفوذ و طرح در دستور کارهای سیاست های امنیتی در کشورهای متعدد باز کرد. بین حفاظت از زیرساخت حساس و تهدیدات سایبری تفاوت وسیعی وجود دارد کما اینکه در اولین گزارش‌شورای‌زیرساخت حساس هم کمتر از ۵ درصد به مسئله امنیت زیرساخت های سایبری پرداخته شده بود.

مسئله حفاظت از زیرساخت های حساس همچنان دارای اولویت در دستور کار سیاسی دولت های بعدی بود، وقایع ۱۱ سپتامبرهم به افزایش آگاهی درخصوص آسیب پذیری و حس فوریت و اضطرار در حفاظت از زیرساخت های حساس منجر شد. نکته دیگری که در مکتب کپنهاک به آن توجه شده، دولتی بودن امنیت است که در دولت اوباما مورد توجه ویژه قرار گرفته و پس از کشمکش های فراوان با کنگره هنگام

حملات سایبری روسیه در انتخابات ریاست جمهوری اجماع لازم برای قرارگیری در دستور کار امنیتی در کل حاکمیت ایالات متحده برای آن ایجاد شد. برای بررسی امنیتی براساس مکتب کپنهاک ابتدا رویکردی دو مرحله‌ای درخصوص کشف مکانیزم های سیاست گذاری های تهدید به این شرح مورد نیاز است : مرحله اول چارچوب اولیه و فرصت امنیت سازی را تا ورود و تثبیت آن به حوزه دستور کار سیاسی بررسی می‌کند که در مورد تهدیدات سایبری از دوره دوم کلینتون تا دوره اول جرج بوش مربوط به این مرحله می‌شود. سپس یک دوران گذار از نظرسیاست‌گذاری در دولت دوم جرج بوش آغاز می‌گردد، در این دوران راهبرد دولت آمریکا از جهت تعیین تکلیف مسئولیت حفاظت از زیرساخت‌های حیاتی وابسته به شبکه‌های در اختیار بخش خصوصی تعیین نشد. سپس مرحله دوم از دور دوم اوباما شروع می شود که امنیت سایبری زیرساخت های حساس در تصمیم دستور کار امنیت سیاسی قرارمی‌گیرد و در نتیجه راهبرد سابق شروع به تغییر می‌کند.

در مکتب کپنهاک عموما مشکلات، سیاست‌ها و سیاستگذارها را به عنوان سه جریان نسبتاً مستقل شناسایی می‌کنند؛ جریاناتی که در خلال آن، مشارکت کنندگان مختلف نهایت تعامل را برای جایگزین کردن موضوعات در دستور کار صورت می دهند .دراین مورد مشکلات عموماناشی از تغییر شرایط اعم از وابستگی به زیرساخت‌های سایبری و تغییر تخاصم از دولت‌ها به دشمنان فروملی است وسیاست‌گذاران هم کنگره و کاخ سفید هستند، در تعامل بین سیاست‌گذاران وتحت تاثیرمشکلات، سیاست‌هایی برای برون‌رفت از مشکلات و مدیریت شرایط شکل می‌گیرد. کینگدان بین دستور کار حکومتی - که مجموعه ای است از سیاست هایی که شدیداً مورد توجه حکومت هستند – و تصمیم دستور کار یعنی آن دسته موضوعاتی که برخوردار از توجه افراد در بالاترین سطوح حکومت هستند ، تفاوت قائل می شود . مانند تصمیم شخصی اوباما به اولویت دادن به مباحث سایبری که به شدت توسط کنگره برای ورود به دستور کار حاکمیت پس زده می شد. علی رغم اینکه دستور کار امنیتی بخشی از دستور کار سیاسی است اما دارای ویژگی هایی است که درجه بالاتری از ضرورت را به طور ضمنی ، بیش از دیگر موضوعات عمومی تحمیل می کند. در دولت امریکا مباحث سایبری و مباحث حفاظت از زیر ساخت به ترتیب ابتدا در دستور کار سیاسی دولت

کلینتون قرار گرفت ، سپس در دولت بوش زیرساخت های حساس به دستور کار امنیتی و مباحث سایبری به تصمیم دستور کار سیاسی با ویژگی ضرورت درآمد و در نهایت در دولت اوباما هر دو مبحث و مباحث جدیدی در این رابطه در دستور کار امنیتی قرار گرفتند. هم اکنون، هم با توجه به اتفاقات سایبری تعیین کننده در انتخابات ریاست جمهوری آمریکا در صدر دستور کار امنیت ملی قرار دارد و با توجه به ابهامات و عدم قطعیت ذاتی مباحث سایبری پتانسیل شکل گیری معمای امنیت براحتی وجود دارد.آخرین بخشی که در چارچوب مفهومی مورد توجه قرار می گیرد بازدارندگی سایبری است(بیات،۱۳۸۹:۴).در موضوع امنیتی سازی فضای سایبری در ایالات‌متحده همانطور که در شکل نشان داده شده تقریبا سیر طبیعی امور آنطور که در مکتب کپنهاک تدوین شده طی شده است. هرچند به علت نیاز مبرم اوباما برای استفاده از تسلیحات سایبری در سال ۲۰۱۰ پیش از آنکه فاصله لازم و امن میان امریکا و دیگر رقبا در توسعه تسلیحات سایبری پدید آید، دولت وی مبادرت به استفاده از این تسلیحات علیه ایران نمود.

هدف این مقاله تبیین چگونگی و چرایی اتخاذ راهبردهای فوق در دوران مختلف و معرفی نقاط ضعف و قوت اتخاذ هرکدام از آنها است. ابتدا در قسمت فرایندها و روندها روند تحولات سیاست گذاری، آثار تغییر شرایط سیاسی و امنیتی بر راهبردها و جزئیات رویدادهای سایبری و امنیتی که منجر به تغییر راهبردها و رویکردهای سایبری در دولت‌های مختلف آمریکا شده را بررسی می‌نماییم. سپس در قسمت دوم که مربوط به ساختارهای تصمیم‌گیری در ایالات متحده است، نقش و اثر کنگره و کاخ سفید در تعامل با یکدیگر برای ایجاد نهادها، قانونگذاری و اتخاذ رویکردهای مختلف تدافعی و تهاجمی سایبری بررسی شده است.

فرایندها و روندهای سایبری در دولت های آمریکا

۱. دوران بیل کلینتون: فرمان اجرایی ریاست جمهوری ۱۳۰۱۰ توسط بیل کلینتون به ایجاد شورای حمایت از زیرساخت‌های حساسِ ریاست جمهوری منجر شد که تا امروز پابرجاست. اگرچه نقش فعلی شورای زیرساخت‌های حساس در بحث امنیت سایبری امریکا مثل گذشته پررنگ نیست اما با توجه به اینکه اولین نهادی بود که وظایف راهبردی در حوزه امنیت سایبری داشته وگزارش‌های آن دید بسیار مناسبی نسبت به تحول امنیت سایبری امریکا می دهد، به بررسی آن می پردازیم. از وظیفه این شورا تدوین سیاست جامع ملی برای حفاظت از زیر ساخت های حساس و نظارت بر اجرای آن نظارت است تا در صورت لزوم تغییرات قانونی لازم را به دولت پیشنهاد نماید. فرمان اجراییِ ۱۳۰۱۰ اولین سندِ سیاست گذاری ملی بود که تهدیدات سایبری را در بستر زیرساخت های حساسِ ملی تعریف می کرد. تعریف فرمان اجرایی ۱۳۰۱۰ از زیرساخت حساس عبارت است از:

"زیرساخت های حساس در واقع زیرساخت های ملیِ مشخصی هستند که به حدی حیاتی می باشند که فقدان یا نابودی آنها اثر ناتوان کننده بر دفاع ملی یا امنیت اقتصادی آمریکا می گذارد(کلینتون،۱۹۹۶). به سخن دیگر، زیرساخت های حساس همان نقطه ثقل های نظریه کلاوزویتس هستند که الزاما فیزیکی هم نیستند و ممکن است مجازی باشند . کلاوزویتس می گوید: هدف جنگ، بر هم زدن نقطه ثقل دشمن

است. این نقطه ثقل، الزاما فیزیکی نیست بلکه می تواند مجازی نیز باشد (هاوارد،۱۲:۱۳۷۷). این زیرساخت های حساس شامل مخابرات، سیستم های الکتریکیِ قدرت، منابع نفت و گاز، حمل و نقل، بانکداری و امور مالی، حمل و نقل، سیستم های ذخیره آبی، خدمات اضطراری (شامل پزشکی، پلیسی، آتش نشانی و امداد) و سایر خدمات دولتی می شود. امروزه مدیریت، نظارت و کنترل زیر ساخت های حساس توسط سیستم های کنترل صنعتی و الکترونیک وابسته به شبکه های سایبری صورت می‌گیرد و از این نظر نسبت به حملات سایبری بسیار آسیب پذیر هستند. ازآنجاکه بسیاری از زیرساخت های حساس در مالکیت بخش خصوصی بوده و توسط آنها بکارگیری می‌شوند، ضروری است که دولت و بخش خصوصی بایکدیگر همکاری نزدیک و کامل داشته باشند تا راهبردی را برای حفاظت از آنها و اطمینان از عملکرد مستمرشان توسعه دهند. اما با توجه به این فرمان این همکاری اختیاری و بر اساس صلاحدید و اعلام نیاز بخش خصوصی صورت می‌گرفت و اجباری در گزارش دهی و همکاری با نهاد های امنیت سایبری دولتی برای شرکت ها خصوصی و مدیران آنها در نظر گرفته نشد.

در سال۱۹۹۷ این شورا گزارش خود را با عنوان «بنیان های حساس: حفاظت از زیرساخت های آمریکا» ارائه کرد. این گزارش در اواخر دهه ۱۹۹۰ پیشینه تاریخی ارزشمندی برای ارزیابی فعالیت ها و سیاستگذاری‌های مدیریتی کلینتون در زمینه سایبری ایجاد کرده است. اما نکته قابل توجه حجمی بود که به مباحث سایبری در این گزارش اختصاص داده شده بود. تنها ۳ درصد از گزارش به زیرساخت های سایبری اختصاص داشت که نشان می دهد در آن زمان هنوز موضوع سایبری امنیتی تلقی نمی شد و بین زیرساخت حساس و مسئله سایبری انفکاک وسیعی وجود داشت. در طول این دوره بخش خصوصی بعضی زیرساخت‌های حساس را کنترل می‌کرد که وابستگی نسبی به سیستم‌های اطلاعاتی یافته بود. همچنین، محیط شبکه بدون مرز فرصت های تجاری عظیمی را برای بخش خصوصی به وجود آورد. بنیان‌های حساس اولین سند سیاست‌گذاریِ مهم برای حمایت از "زیرساخت‌های حساس"[1] بود (McCarty,2009:544).

[1]. CIP

گزارش «زیرساخت‌های حساس» تصریح می‌کند که ساختار فکری امنیت فیزیکی که «در گذشته به خوبی برای ایالات متحده ایفای نقش کرده است، دربرابر تهدیدات سایبری کمترین حمایت را می‌کند»(کلینتون،۱۹۹۶).کلینتون قبل از پایان دوران ریاست جمهوری خود در پاسخ به گزارش « زیرساخت‌های حساس» رهنمودِتصمیم‌گیری-ریاست‌جمهوری ۶۳ [۱]را مطرح کرد تا به هدف آشکارسازی و شفافیت هرچه بیشتر در «ایجاد چارچوب عملی و نو برای حمایت از زیرساخت های حساس» دست یابد (کلینتون،۱۹۹۸). این فرمان اجرایی ریاست جمهوری که هنوز هم یکی از راهبردهای امنیت سایبریِ ایالات متحده است و براساس کارکرد موثرتر بخش خصوصی و به نظریه پیشرفتِ تدریجی و خودگردانی بخش خصوصی متکی است.

به اعتقاد کارشناسان امریکایی، امنیت سایبری در عصر اطلاعات نیازمند تغییری بنیادین در نهادها و فرایندهای کار بخش سایبری ایالات متحده بود حال آنکه نظریه پیشرفت تدریجی تا مدت ها به حکم‌فرمایی خود بر رویه‌های توسعه سیاست امنیت سایبری آمریکا ادامه می داد. زیرا مدیران عامل با مفهوم رابطه دوسویه اجباری مخالف بودند(هوور،۲۰۰۹). برای درک اهمیت مخالفت این مدیران، لازم است اشاره کنیم ارزش سهام تحت مدیریت ایشان معادل تولید ناخالص ملی دهها کشور است (Nasdaq.com).بعدها دولت اوباما تلاش هایی برای تغییر این روند با تصویب قانون امنیت سایبری ۲۰۱۲ انجام داد که در کنگره به‌شکل ناقصی به سرانجام رسید. اتاق بازرگانی با حذف اجبار در اشتراک گذاری دوسویه اطلاعات بخش خصوصی با بخش های نظارت فدرال از متن لایحه تلاش هایی را انجام داد که در نهایت با موفقیت لابی اتاق بازرگانی، تغییرات مورد نظرش در قانون امنیت سایبری ۲۰۱۲ انجام شد. بنابراین، مدیران عامل و مامورین دولتی همچنان از نظریه خودگردانی به عنوان مفهوم تثبیت شده ای در امنیت سایبری ملی پیروی می‌کردند.[۲] در واقع، نقطه نظر امنیتی دو نکته قابل ملاحظه است؛ اول اینکه در آن زمان کل بخش خصوصی و بخش هایی از حاکمیت

---

[1]. PDD-63

[۲]. لایحه امنیت سایبری با بیشترین موافق در مجلس صدودوازدهم به تصویب رسید !!

تهدیدات سایبری را حداکثر یک ریسک تجاری می دیدند نه یک تهدید وجودی و دیگر موضوع مخالفت آنها با دخالت دولت به عنوان مرجع امنیت هستند.

البته، نکات ذکر شده در بالا بیشتر معطوف به جنبه پدافند سایبری و امنیت سایبری بوده، همزمان با اقدامات شورای حمایت از زیرساخت های حساس، وزارت دفاع به عنوان اصلی‌ترین نهاد نظامی وظایف عملیاتی سایبری ایالات متحده را به مرور برعهده می‌گرفت . وزارت دفاع این وظایف را از طریق سازمان‌ها و واحدهای سایبری متعددی که زیر مجموعه یا وابسته به وزارت دفاع هستند اعم از آژانس امنیت ملی، پنتاگون و فرماندهی راهبردی سایبری به انجام می رساند. آژانس امنیت ملی سری ترین و مخوف ترین عضو جامعه اطلاعاتی امریکا است که وظیفه جمع آوری اطلاعات مخابراتی و نیز پشتیبانی از عملیات های نظامی و اطلاعاتی آمریکا از طریق شنود سیگنال و حفاظت سیگنال را بر عهده دارد. آژانس امنیت ملی درواقع نهاد امنیتی وزارت دفاع امریکا است که از ابتدای انتقال مخابرات و ارتباطات بر بستر شبکه یکی از وظایفش برقراری امنیت شبکه های رایانه‌ای در کنار شنود ارتباطات دشمن می باشد. لازم به ذکر است، شنود سیگنال را نباید به معنی شنود تلفنی و رادیویی مرسوم تعبیر کرد، بلکه مفهومی بسیار گسترده‌تر است،که امروزه با داده‌کاوی و مفهوم ابرداده‌ها[1] و داده های عظیم[2] به کلی دگرگون شده است. در فرایند داده‌کاوی کلیه متون موجود در اینترنت و شاید با تکنولوژی های جدید صوت‌های مبادله شده در اینترنت از نظر وجود کلید واژه‌های خاص یا مفاهیم مورد نظر یک سرویس اطلاعاتی یا افکار سنجی مورد بررسی قرار می‌گیرد. مانند کاری که شرکت کمبریج آنالیتیکا[3] در زمینه داده‌هایی که از فیس بوک گرفته بود برای شناسایی سلیقه رای‌دهندگان آمریکایی در انتخابات ریاست جمهوری ۲۰۱۶ انجام داد و نتایج را به کمپین ترامپ فروخت(Vaughan-nichols,2018). در واقع، این سازمان وظیفه تحقیق و توسعه در زمینه امنیت و رمزگذاری و همچنین ابلاغ استانداردهای امنیتی، نظارت و بررسی سطح امنیتی تمامی

1. Cloud Data
2. Big Data
3. Cambridge Analytica

سازمان های فدرال را هم بر عهده دارد. تمامی سازمان‌های فعال در زمینه دفاع سایبری ارتباط نزدیکی با آژانس امنیت ملی دارند. در نتیجه، قابلیت‌های امنیت سایبری این سازمان فوق‌العاده است. شایعات بسیاری درباره پروژه‌هایی نظیر اشلون و اخیرا پریسم مطرح است که این سازمان جهان را رصد می‌کند و همه ارتباطات ایمیلی، تلفنی و فکس در سراسر جهان تحت نظر این آژانس برای یافتن کلیدواژه‌های مدنظرش است(اسنودن،۲۰۱۷).

با این اوصاف، برخی پیشنهادها در زمان اوباما وجود داشت که این سازمان، پیش قراول فعالیت‌های امنیت سایبری در دولت امریکا باشد. ولی دیگران استدلال کردند ماهیت نظامی و شدیدا امنیتی آن منجر به شفافیت کمتر، اعتماد کمتر و مشارکت کمتر شرکت های خصوصی و عموم مردم با این نهاد امنیتی-نظامی می‌شود و روی هم رفته موجب همکاری کمتر و تضعیف امنیت سایبری می‌گردد. نکته مهم که موجب پذیرش استدلال اخیر شد در این‌است که نه تنها بخش خصوصی ایالات متحده در مباحث سایبری بسیار قوی‌تر از دولت می باشد بلکه دولت اختیار و قدرت مجبور کردن آن به هر نوع همکاری با نهادهای امنیتی را هم ندارد. به عنوان مثال، در جریان دعوای پلیس فدرال و اپل برای شکستن رمز آیفون یکی از متهمان حوادث تروریستی اخیر در امریکا، دولت اوباما نتوانست اپل را ملزم به تبادل اطلاعات نموده و مجبور شد به کمک یک شرکت خصوصی دیگر این کار را با صرف وقت و هزینه بسیاری انجام دهد(Arriens,2016). بنابراین نگرانی این عده از عدم همکاری شرکت های خصوصی در صورتی که آژانس امنیت ملی مسئولیت رهبری امنیت سایبری را بر عهده گیرد، خیلی هم بی مورد نبود. در دوران کلینتون این دو نهاد (شورای حمایت از زیرساخت های حساس و وزارت دفاع از طریق آژانس امنیت ملی) عمدتا مسئول امنیت سایبری و دفاع سایبری بودند.

۲. دوران بوش پسر: حملات ۱۱ سپتامبر ۲۰۰۱ احتمالا مهمترین حادثه بعد از پرل هاربر است که راهبرد ایالات متحده را در همه زمینه‌های امنیتی متحول کرده و سیاست-های دولت بوش هم عمدتا متاثر از این واقعه است . در بخش امنیت سایبری هم حادثه۱۱ سپتامبر موجب وضع سه قانون پارلمانی شد و طبعا این قوانین رویکرد امریکا نسبت به

امنیت سایبریِ در بخش زیرساخت‌های حساس را هم تحت تاثیر قرار داد. این قوانین عبارتند از : قانون امنیت داخلی آمریکا، قانون امنیت میهنی ۲۰۰۲[1] و قانون مدیریت فدرالِ امنیت اطلاعات ۲۰۰۲ .[2] قانون امنیت میهنی ۲۰۰۲ وزارت امنیت میهنی [3] را ایجاد کرد .این قانون بسیاری از مسئولیت‌های امنیت‌سایبری موثر را تحت حدود صلاحیت دایره‌ای هم سطح باکابینه جدید ادغام نمود(Castro,2012:58-121,). در دسامبر ۲۰۰۳ بخشنامه ریاست جمهوری در مورد امنیت میهنی (HSPD-7) با عنوان «شناسایی زیرساخت های حساس، اولویت بندی و حفاظت» وزارت امنیت میهنی را به عنوان اداره پیشگام در فناوری اطلاعات و بخش های ارتباطی نامزد کرد که مسئولیت های خاصی درقبال اشتراک گذاری اطلاعاتِ تهدید، کمک به ارزیابی آسیب‌پذیری ها، ترغیب به انجام اقدام حفاظتیِ مناسب و توسعه برنامه های احتمالی دارد(بوش،۲۰۰۳). در واقع، دولت اوباما راه میانه‌ای را انتخاب کرد. وی این وزارت تازه تاسیس را به عنوان سازمان پیش‌قراول محافظت از شبکه های غیرنظامی دولت امریکا انتخاب کرد تا شرکت های خصوصی براحتی با آن تعامل نمایند و در عین حال با همکاری مستقیم بین وزارت امنیت میهنی و آژانس امنیت ملی، قابلیت های پیشرفته آژانس امنیت ملی را هم از دست ندهد.در سال ۲۰۰۲ مجلسِ صدوهفتم قانون «مدیریت امنیت اطلاعات فدرال، FISMA» را ذیل باب سوم از قانون دولت الکترونیک ۲۰۰۲ در پاسخ به تهدیدات روزافزون در فضای سایبری تصویب کرد (http://csrc.nist.gov). اما تا سال ۲۰۱۰ که وزارت امنیت میهنی به سازمانی پیشگام برای پیاده سازی قانون «مدیریت امنیت اطلاعات فدرال» ۲۰۰۲ تبدیل شد، عملا قانون FISMA فاقد متولی مجزا برای اجرا بود (Obama,2010). با اینکه پیش از آن سایر سازمان های فدرال مسئولیت های عمده مرتبط با امنیت سایبری را دراختیار داشتند، با این قانون وزارت امنیت میهنی به عنوان سازمانی پیشگام در حفاظت از زیرساخت های حساس در راس همه سازمان های مذکور قرار گرفت (همان).

---

1. Homland Security Act (HSA)
2. FISMA
3. Department of Homeland Security (DHS)

از یک طرف نتیجه کل اقدامات امنیت سایبری دولت آمریکا در دفاع از زیرساخت های کشور به وزارت امنیت میهنی بستگی دارد و از طرف دیگر پاشنه آشیل نهادهای سایبری امریکا هم همین وزارت امنیت میهنی است که کمترین سابقه را در عرصه های امنیتی داشته و علیرغم ابعاد عریض و طویل آن از کمترین وجهه و اعتبار در بین نهادهای امنیتی فدرال امریکا برخوردار است. وزارت امنیت میهنی هم با چالش‌های درون سازمانی شامل دیوان سالاری اداری و هم دخالت های کنگره روبرو است . وزارت امنیت میهنی ظاهرا بیشترین پرسنل حرفه ای دولت امریکا را در این بخش به خود جذب کرده ولی به درستی بکار نگرفته است . از نظر بسیاری از صاحب نظران تنها آنها را مشغول می‌کند . در واقع، یکی از متخصصان تخمین زده است که دولت آمریکا در حال حاظر تنها ۳ تا ۱۰ درصد از پرسنل حرفه ای امنیت سایبری مورد نیاز خود را بکارگرفته است(لرد وشارپ،۱۳۹۲). همین نیروهای بکارگرفته شده در وزارت امنیت میهنی بر خلاف سایر نهادهای فدرال امنیتی بر مبنای مدرک گرایی (و نه تخصص) شایع در نهادهای عمومی بکار گرفته شده اند؛ زیرا این نهاد فاقد نیروهای اطلاعاتی و حرفه ای بوده و مجبور بود از متخصصان حوزه عمومی کمک بگیرد. برغم همه انتقادات فوق ، قانون مدیریت امنیت اطلاعات فدرال ۲۰۰۲ مشکل مسئولیت های موازی و تداخل در امور را با یکپارچه سازی تا حدودی حل نمود و احکام سابق که بر مبنای اعمال قوانینِ سابق در فضای سایبری بودند را منسوخ کرد. همچنین وزارت امنیت میهنی را ملزم کرد تا پشتیبانی های امنیت اطلاعاتی را متناسب با خطرات وارده بر سیستم های اطلاعاتی دولت صورت دهد(OMB,2011). با اینکه وزارت امنیت میهنی سازمان پیشگام در پیاده سازی و پیروی از FISMA بود، اداره مدیریت و بودجه[1] بر اجرای درست و کامل FISMA نظارت می کند، و در مورد آن گزارش سالانه به مجلس ارائه می‌کند و قدرت نظارت و پیگرد کیفری نسبت به سازمان‌های فدرال را در رابطه با مصرف بودجه IT حفظ می کند(همان). به علاوه هر بازرس عمومی سازمان ، هر سال پیشنهادهایی مبنی بر بهترین روش برای ارزیابی کنترل امنیت را به مجلس

[1]. Office of Management and Budget

ارائه می کند. موسسه ملیِ علم و فناوری (NIST)[1] وظیفه تدوین راهبردهای پیاده سازی FISMA را بر عهده دارد. اگرچه هنوز هم مالکین خصوصی زیرساخت های حساس به واسطه FISMA مقید نمی‌شوند، که نفوذپذیری ساختاری قانونگذاری در آمریکا را در مورد نحوه تنظیم مقررات برای زیرساخت هایی حساس با مالکیت خصوصی توسط آمریکا نشان می دهد.

چارچوب مدیریت خطر (RMF) موسسه ملی علم و فناوری بخش عمده رویکرد دولت فدرال درقبال پیاده سازی امنیت سایبری را تشکیل می دهد. در سال ۲۰۱۰ مدل پذیرش FISMA از روند تائید و اعتبارگذاری (C&A) به چارچوب مدیریت ریسکِ پیوسته (RMF) تحول یافت.[2] این تحول در واقع ارج نهادن به توانایی علمی و فنی در مقابل مدرک گرایی که سابق بر این حاکم بود، است . در واقع روند تایید و اعتبارگذاری در بهترین حالت به صورت عکس گرفتن ساکن از شرایط در زمان بازرسی توصیف می شود، بطوری که نتایج به سرعت غیرقابل استفاده می شوند(World Bank,2003). گزارش پیاده سازی FISMA (FY2008) توسط اداره مدیریت و بودجه حاکی از میزانِ رضایت بخشی از تایید و اعتبار (تا ۹۰٪ برای سازمان های فدرال) بود(Hoover,2009). با این حال در این بازه زمانی گزارشGAO [3] نشان می داد که همان سازمان‌ها «کنترل های موثری برای جلوگیریِ مناسب، محدودکردن‌یاشناسایی‌دسترسی‌به‌شبکه‌های‌رایانه-ای، سیستم‌هایا اطلاعات بکارنبسته‌اند»(Gao,2011). بالعکس، RMF روند مدیریتِ دوره ای با شش مرحله است که برای ارزیابی و کاهش آسیب پذیری های سیستم اطلاعاتی (از گردآوری تا پس‌روی) طراحی شده است.

مخرب‌ترین نتایجی که با گزارش GAO بعدها (در سال ۲۰۱۱) مشخص شد مربوط به فقدان کنترل های امنیت اطلاعاتی نظام مند میان سازمان های فدرال بوده است(همان). زیرساخت های سایبری فدرال نیاز به بازرسی های عمومی دارد تا ارزیابی های کنترل امنیت سالانه را انجام داده و کاستی ها را مشخص نموده و اقدامات

[1]. National Institute of Standards and Technology
[2]. Risk Management Framework
[3]. Government Accounting Office

اصلاحی را انجام دهند(NIST,2011:42). گزارش GAO در سال ۲۰۱۱ نتیجه گرفت که نقص های کنترلی گسترده در امنیت اطلاعات درمیان سازمان های فدرال، سیستم های اطلاعاتی را در معرض «افزایش خطرِ استفاده غیرمجاز، افشا، اصلاح و اختلال» قرار می دهد(Gao,2011). دیری نگذشت که فاجعه اسنودن[۱] نیاز به جلوگیری از خطر افشا و استفاده غیر مجاز را بیش از پیش آشکار ساخت! همچنین در حمله به NASDAQ هم دوباره آشکار شد که نظریه خودگردانی واقعیت های محیط امنیت اطلاعات را با موفقیت تحمل نمی کند. فراوانی و مهلک بودنِ حملات سایبری علیه زیرساخت های حساس آمریکا با آهنگ هشداردهنده ای درحال افزایش است. در سال ۲۰۱۱ هکرها چندین موسسه مالی آمریکا را که شامل بورس NASDAQ می شد، تخریب کردند. در سال ۲۰۱۲ صنعت بانکداری آمریکا حمله ازکاراندازی سرویس (DDOS) عظیم و هماهنگی را تجربه کرد(kitten,2016). در سال ۲۰۱۲ موسسه PwC[۲] گزارش تحلیل سرمایه گذاری مربوط به شرکت چند ملیتی امنیت IT خود را منتشر نمود که در مورد آمادگی ۹۳۰۰ مدیر ارشد فناوری اطلاعات، مدیر عامل و مدیر IT در برابر حملات سایبری بود. این گزارش ۴ آمار مهم داشت که به عنوان یک شوک ادراکی،[۳] تاثیرگذارخودگردانی را زیر سوال می‌برد.

- ۸٪ بهترین و اساسی ترین روش های امنیت IT (مانند ارائه گزارش های امنیتی به مدیران عامل) را تمرین می کردند.
- ۴۲٪ راهبرد امنیت IT موثری را اجرا می کردند.
- ۷۱٪ از ابزارهای شناسایی بدافزارهای تبلیغی و جاسوسی استفاده می کردند. (که در سال ۲۰۱۱ برابر ۸۳٪ بود.)

---

[۱] **ادوارد جوزف اسنودن**، افشاگر کنونی و کارمند سابق سازمان اطلاعات مرکزی آمریکا و پیمانکار سابق آژانس امنیت ملی است. افشاگری‌های ادوارد اسنودن از عملیات عظیم " جاسوسی و مراقبت در سطح جهانی"پرده برداشت. بنا به مدارک اسنودن، این برنامه‌ها که شامل جاسوسی از مردم عادی و شخصیتها در مکالمات تلفنی، ایمیل، استفاده از موتور جستجو ی اینترنت و ... در تمام کشورها و بدون رعایت مرزهای سیاسی صورت می‌گیرند، در درجه اول توسط اژانس امنیت ملی به اجرا در می ایند.

[2] Price Waterhouse Coopers

[۳] نظریه شوک ادراکی فرید ذکریا

- ۱۶٪ فهرست داده های اساسی (که قبلا ۲۲٪ بود.) را گردآوری کردند تا میزان ریسک خطرناک را برای سازمان در زمان حمله سایبری تعیین کنند.

گرچه «راهبرد ایمن سازی فضای سایبری ۲۰۰۳» ادعا می کند که «... انتظار می رود که بازار اقتصادی محرک عظیمی برای بهبود امنیت سایبری فراهم کند»، آقای مارک لوبل [1]رئیس و گزارش نویسPwC اظهار می کند : « شرکت ها به جای بودجه های امنیت IT ریسک-محرک می‌توانند معیارهای امنیت IT را انجام دهند.» (Schectman,2014).سیستم اقتصادی سرمایه داری به صورت طبیعی سرمایه گذاری های غیرسود ده را سرکوب می کند، مگر اینکه عاملی خارجی مانند مقررات فدرال سبب وقوع آن شوند. اما «راهبرد ملی برای ایمن سازی فضای سایبری ۲۰۰۳» بر مبنای نظریه خودگردانی استوار است که خلاف واقعیت های موجود در بازار اقتصادی عمل می‌کند. در حالی که حساس‌ترین زیرساخت‌ها و فضای‌سایبریِ وابسته به آن مالکیت و عملکرد خصوصی دارند. فناوری هایی که فضای سایبری را به وجود آورده و از آن پشتیبانی می کنند، به سرعت از بخش خصوصی و ابداعات آکادمیک رشد می یابند. دولت به تنهایی نمی تواند فضای سایبری را به خوبی ایمن سازی کند. لذا رئیس جمهور بوش درخواست همکاری داوطلبانه از صنعت، دانشگاه و گروه های غیردولتی را نمود تا فضای سایبری را ایمن کرده و از آن دفاع کنند(Bush,2005)

۳. دوران اوباما:دوران اوباما: بدون‌شک چالشی‌ترین دوران در آمریکا از نظر تحولات و رخدادهای سایبری تاکنون محسوب می‌شود. از تشکیل فرماندهی راهبردی سایبری و حملات سایبری ایالات متحده به ایران تا حملات سایبری دشمنان آمریکا به ایالات متحده و متحدان آن در سراسر جهان و در نهایت دخالت ادعایی روسیه در انتخابات ریاست جمهوری آمریکا از طریق حملات سایبری که منجر به تغییر نامزد پیروز علیرغم آرای بالاتر از نامزد شکست خورده شد. در این دوران پرفراز و نشیب به موازات اتفاقات و تهدیدات میدانی راهبردها و سیاست‌گذاری‌های حاکمیت هم دستخوش تحول و تکامل زیادی شد. اولین رویداد مهم این دوران تشکیل یک کمیته

[1]. Mark Lobel

ویژه از طرف اوباما با هدف ارزیابی و ارائه راهکارهای عملی برای تحول ساختاری، فرایندی و نهادی در حوزه سایبری بود. براین اساس، اوباما در ابتدای دوران ریاست جمهوری خود دستور ایجاد کارگروه «بازبینی سیاستگذاری سایبری در ۲۰۰۹»[1] در کاخ سفید را داد.

راهکارهای کارگروه بازبینی سیاستگذاری سایبری متضمن دو مفهوم جدید درسیاستگذاری سایبری بود که آن را از سلف خود، یعنی رویکرد سنتی ایالات متحده در سیاستگذاری‌های سایبری، متمایز می‌کرد. تفاوت اول سیاست ۲۰۰۹ به دنبال اصلاح رابطه عمومی-خصوصی مرسوم با طرح مسئولیت قانونی شرکت ها بود(Obama Cyber Review Group,2009). معمولا سازمان‌ها به فعالیت‌های غیرانتفاعی سازمان، مانند سرمایه‌گذاری در بخش امنیت اطلاعات بها نمی‌دهند. زیرا آنها معتقدند به علت عدم سوددهی مناسب ، سازمان نمی‌تواند سرمایه‌گذاری خوبی روی آن انجام شود. تفاوت دوم حمایت از تصویب لوایح و طرح‌هایی است که در آن مشوق‌های مالی مناسب برای بخش خصوصی به منظور سرمایه‌گذاری بیشتر در امنیت سایبری در نظر گرفته شده است. مهمترین قسمت رویکرد جدید این است که "آستانه مسئولیت قانونی برای شرکت‌هایی که امنیت سایبری بالایی دارند کاهش یابد و در عوض شرکت‌هایی که امنیت سایبری ضعیف تری دارند، آستانه مسئولیتی بالایی برای آنها در نظر گرفته شود(همان)." باتوجه به هزینه‌های حقوقی این چنینی شرکت‌ها، مدیران در برابر قانون مسئول و ملزم هستند تا امنیت سایبری خود را افزایش دهند و از جذب سرمایه در بخش امنیت سایبری شرکت حمایت به عمل آورند. اگرچه بهترین مشوق مالی برای شرکت های امریکایی برآورد هزینه‌های ریسک آسیب‌پذیری شرکت توسط مدیران ارشد در مواجهه با تهدیدات سایبری می‌باشد، نه مشوق‌های مالی که در لوایح قانونی تصریح شوند. مولفه مهم بعدی در گزارش بازبینی سیاستگذاری سایبری در ۲۰۰۹ معاون هماهنگ کننده در دفتر اجرایی رئیس‌جمهور (به عنوان معاون مشاورامنیت ملی) است، این دفتر بهترین جایگاه را برای هم‌افزایی و اشتراک مساعی آژانس‌های مختلف و متعدد

[1]. Obama Cyber Review Group 2009

فدرال دارد(همان). در مورد این جایگاه در بخش مربوط به کاخ سفید بیشتر توضیح خواهیم داد.

تحول مهم بعدی در دوران اوباما تشکیل فرماندهی سایبری ارتش امریکا به عنوان یکی از ده فرماندهی راهبردی ارتش ایالات متحده محسوب می شود(حسینی و ظریف منش،۴۲:۱۳۹۲). همچنین فرماندهی سایبری ایالات متحده باید به عنوان هماهنگ کننده و مشاور رئیس جمهور در حوزه دفاع سایبری ایفای نقش نماید. بر مبنای قانون ۲۰۰۹ امریکا؛ که در ادامه بررسی می شود؛ ریاست فرماندهی سایبری ارتش و فرماندهی آژانس امنیت ملی در ایالت متحده باید به صورت مشترک به یک ژنرال حداقل سه ستاره سپرده شود که ژنرال مایکل راجر و پیش از آن ژنرال کیت الکساندر در این سمت خدمت کرده اند. نیروهای مسلح وظیفه حفاظت از اطلاعات و شبکه های ارتباطی نیروهای مسلح از میادین جنگ تا ستاد فرماندهی را بر عهده دارند و همچنین در صورت لزوم و با دستور ریاست جمهوری این فرماندهی باید توانایی حمله سایبری به کشورهای مورد نظر را داشته باشد. در آخرین سند که در سال ۲۰۱۵ در رابطه با استراتژی امنیت سایبری منتشر کرده، فضای سایبری را تا حد پنجمین فضای جنگی ارتقاء و آن را کنار زمین، دریا، هوا، و فضا قرار داده است. وزارت دفاع برای محافظت از شبکه های نظامی امریکا، زیر مجموعه فرماندهی به نام فرماندهی سایبری امریکا ایجاد کرده است که تحت امر فرماندهی راهبردی امریکا قرار دارد (لرد و شارپ،۱۳۹۲).

با توجه به کند بودن پنتاگون در به روز رسانی و ارتقای سایبری ، وزارت دفاع بدنبال این است که روند دستیابی به فناوری اطلاعات را سرعت ببخشد. در گزارش به کنگره ، ژنرال کیت الکساندر نگرانی‌های خود را در مورد کمبود اختیارات در فرماندهی سایبری برای واکنش به حمله سایبری به زیر ساخت های حساس را در مارس ۲۰۱۱ مطرح کرد. از جمله این نگرانی‌ها این بود که وزارت امنیت میهنی به عنوان هماهنگ-کننده اصلی برای واکنش به چنین جملاتی در نظر گرفته شده است، درحالی که فرماندهی سایبری وزارت دفاع و سازمان امنیت ملی (ان اس ای) دارای قابلیت های فنی بسیار بیشتری برای واکنش به حمله زیر ساخت های حساس هستند؛ اما به دلایل غیر فنی که در جای خود بحث شده، این وظیفه به وزارت امنیت میهنی امریکا تفویض

شده است. برای حل این معضل دولت اوباما تلاش کرد تا با قراردادی بین وزارت امنیت میهنی و وزارت دفاع درسال ۲۰۱۰ طرح جامعی را با هدف ارتقای توان عملیاتی و برنامه ریزی هماهنگ در وزارت امنیت میهنی اجرا کند.

در این برنامه تفصیلی تمام نیروهای نظامی و امنیتی، در حال تنظیم دوباره عملیات‌های سایبری خود با فرماندهی سایبری وزارت دفاع هستند. نکته ای که عمق و جامعیت این برنامه را نشان می‌دهد، گارد ساحلی ایالات متحده است که به تازگی سند امنیت سایبری منتشر کرده و تشکیل یگان سایبری خود و وظایف آن را اعلام کرده است.از دیگر برنامه های ارتش امریکا برای آمادگی در مناقشات فعلی و آینده، تمرین سناریوهای سایبری بیش از گذشته در دکترین و برنامه های آموزشی است .[۱] در این راستا «تیم های قرمز » مستقر در آژانس امنیت ملی اکنون با فرماندهی نظامی مستقیما هم همکاری می کنند تا تهدیدات سایبری را وارد برنامه های آنها کرده و واکنش را آزمایش کنند. یک تمرین دفاع سایبری قوی نیازمند یک کار تیمی می باشد که در آن نیروهای خودی(آبی)، نیروهای متخاصم(قرمز)، زیرساخت های فنی(سبز) و مدیریت بازی(سفید) حضور دارند. تیم های آبی و قرمز مبارزان تمرین دفاع سایبری می باشند. در تمرین سالیانه فرماندهی اقیانوس آرام در بهار سال ۲۰۱۰ هم برای اولین بار از یک بخش سایبری استفاده شد(لردوشارپ،۱۳۹۲).تا اینجا اقدامات صورت گرفته و برنامه های در حال اجرای فرماندهی سایبری ایالات متحده بررسی شد اما اگر بخواهیم از روند های آتی این نهاد اطلاع یابیم ، باید اسناد بالادستی بخش سایبری و راهبردهایی که برای آینده بخش سایبری تدوین شده را بررسی کنیم. دقیق‌ترین و مرتبط‌ترین استراتژی وزارت دفاع در امنیت سایبری در سند موسوم به "فراتر از متن" آمده است، هرچند در زمان ترامپ هم پنتاگون سند مشابهی منتشر کرد و حتی کاخ

---

[۱]. برای تشریح اهداف، طرح ها و درس های که از لایو-فایر تمرین های دفاع سایبری بین المللی گرفته شده است. سپر سایبری بالتیک در مرکز دفاع سایبری در تالینین استونی ، میدان های نبرد مجازی ای که بوسیله آژانس تحقیقات دفاع سوئد طراحی گردیده و آن را در لینکوپینگ میزبانی می کند. این مرکز به وسیله کالج دفاع ملی سوئد حمایت می گردد که بیش از ۱۰۰ شرکت کننده در آن حضور دارند.
(James Adam , foreign affairs magazine)

سفید در این دوران سندملی امنیت سایبری منتشر شده اما هیچکدام از لحاظ فنی به دقت و نوآوری این سند نیستند (DoD Cyber Strategy,2015). این سند توسط پنتاگون تهیه و توسط اشتون کارتر، وزیر دفاع وقت آمریکا امضا شده است. او سند فراتر از متن را ابزار قدرتمندی برای تکامل نیروهای مختلف سایبری در بخش های گوناگون وزارت دفاع می داند .در بخش معرفی اهداف سازمان، چشم انداز آرمانی برای تحول درون سازمانی در نظر گرفته شده تا در نتیجه اجرای آن فرماندهی سایبری آمریکا به یک سازمان«چابک» «خلاق» و پاسخگو تبدیل شود که وزارت دفاع را در رسیدن به اهداف خود در حوزه فضای سایبر یاری می کند . در این سند مأموریت فرماندهی سایبری امریکا در سه حوزه ذیل تعریف شده است:

۱) تضمین انجام ماموریت های وزارت دفاع

۲) ایجاد بازدارنده گی و مبارزه با تهدیدات استراتژیک علیه منافع و زیر ساخت های آمریکا

۳) کمک به تأمین اهداف فرماندهی نیروهای مشترک

اما چالش اصلی برای بهره گیری سازمانی از «قدرت سایبری ملی » بر اساس یک استراتژی خلاقانه پیش‌بینی شده است، که می‌توان آن را «اشتراک در مأموریت ها» نامید(همان). در واقع، ساختار اصلی «فرماندهی سایبری امریکا » یک واحد مجزا نیست، بلکه دارای واحدهایی در همه قسمت های ارتش است که بر اساس اشتراک در مأموریت ها بنا شده است. همچنین این نهاد، مشارکت خود را از طریق وزارت دفاع، جامعه اطلاعاتی امریکا، همکاری های گسترده با سازمان‌های فدرال، صنایع، مجامع دانشگاهی و شرکای بین المللی ایالات متحده تقویت می کند؛ چرا که بر این باور است که امنیت سایبری کشور، نیازمند یک رویکرد مشترک با طیف وسیعی از همکاری بین سازمانی، مشارکت مدیران صنایع، اشتراک توانایی ها و نهایتا دیدگاهی مشترک برای حفاظت از زیر ساخت ها و اطلاعات امریکا شناسایی حملات و مقابله با دشمنان در فضای سایبری است(همان).

در قسمت «همکاری و مشارکت»همکاری با شرکای داخل و خارج از دولت، به عنوان عامل سنجش میزان موفقیت فرماندهی در دفاع از کشور در فضای سایبری

معرفی شده است. در این قسمت تصریح شده : ما می توانیم از متحدان خود در صنعت و همچنین از شرکای جدید در مجامع دانشگاهی و جامعه امنیت و فناوری اطلاعات ، مسائل بسیاری بیاموزیم . برای این منظور لازم است ما شریکان خود و نحوه عملکرد آنان را درک کنیم و همچنین به شریکان خود برای درک خودمان ،کمک کنیم. اما ارتباط ما با NSA کلیدی است . ما باید این ارتباط را برای ماموریت هر دو سازمان با هدف ایجاد دو مجموعه مستقل اما هم زیست و با همکاری نزدیک، بهینه سازی کنیم(همان).مساله قابل توجه دیگراینکه در زمانی که بسیاری از بخش های وزارت دفاع آمریکا با کاهش بودجه مواجه هستند، استراتژی امنیت ملی آمریکا و لزوم اجرای آن توسط وزارت دفاع، از افزایش سرمایه گذاری در بخش توانایی سایبری حکایت دارد. به نظر می رسد، سیستم تصمیم‌گیرنده در حوزه امنیت ملی ایالات متحده معتقد است: مأموریت های سایبری در راس پیکان رزمی آمریکا قرار دارد و بشدت در حال رقابت با سایر رقبای ایالات متحده در این عرصه قرار دارد؛ بنابراین، ارزش سرمایه گذاری های بیشتر را دارند. در بخش دیگر این سند توسعه ارتباط فرماندهی با دیگر بخش‌های مرتبط از هر یک از نیروها مخصوصا آژانس امنیت ملی آورده شده است، و تاکید شده عنصر مهمی برای ارتقا ظرفیت و افزایش توانایی‌ها است. در این سند تصریح شده: ما همچنان به تقویت پیوند بین NSA و فرماندهی سایبری ، زیر ساخت های فناوری اطلاعات وزارت دفاع ، هوش مصنوعی و عملیات فضای مجازی ادامه می دهیم . ما توانایی خود را به وسیله دانش عمیق و قابلیتی منحصر به فرد با تکیه بر نیروی متخصص خود افزایش می دهیم .بنابراین، نیروی مشترک می تواند در یک گستره جهانی با سرعت انعطاف پذیری و پشتکار عمل کند(همان).

۴. دوران ترامپ: دوران اوباما با حملات سایبری به ایمیل‌های هیلاری‌کلینتون، افشاگری های ویکی‌لیکس و مداخله گسترده سایبری از جانب روسیه در انتخابات ریاست جمهوری آمریکا همراه بود که موجب واکنش شدید دولت امریکا و نمایندگان کنگره شد. درحالی که قاعدتا واکنش گسترده و اقدامات فوری از دولت جدید آمریکا قابل انتظار بود . دونالدترامپ با رد این اخبار و جعلی خواندن آنها، نه تنها واکنش مناسبی به روسیه نشان نداد بلکه با حذف سمت هماهنگ کننده سایبری و حذف اداره

دیپلماسی سایبری از وزارت خارجه نشان داد که قصد اقدام جدی در این حوزه را ندارد. در این زمان، کنگره برای بازگرداندن اداره دیپلماسی سایبری و تصویب قوانین امنیت سایبری قدم پیش گذاشت. در قسمت مربوط به کنگره بیشتر به این موضوع خواهیم پرداخت. پس از گذشت یک سال و افزایش فشارها برای انجام اقدامات سایبری، دولت ترامپ دست به انتشار یک سند راهبردی ملی سایبری زد.

استراتژی امنیت ملی سایبری آمریکا ۲۰۱۸[1] اولین سندی است که در دولت ترامپ به طور جزئی به مباحث سایبری می‌پردازد. باتوجه به اینکه در این سند تحول مفهومی وعملیاتی بارزی نسبت به اسناد امنیت سایبری دوران اوباما رخ نداده است، به طور مختصر نگاهی به آن می‌اندازیم. در این سند به فضای مجازی به عنوان موتور رشد باز اقتصادی و پایداری ملی نگریسته می شود. سندمذکور توسعه "اینترنت نامحدود" را در تمام دنیا برای افزایش نفوذ آمریکا مورد تشویق قرار می‌دهد.

اهداف اصلی این سند که در ابتدا بیان شده، عبارت‌اند از:

- ایجاد زیر ساخت‌های حیاتی، شبکه‌های فدرال و سیستم‌های دولتی برای مبارزه با جرائم سایبری
- بهبود گزارش حملات سایبری
- آموزش نیروهای سایبری با مهارت زیاد
- تعیین "استاندارد رفتار مسئولانه دولت (ترامپ،۲۰۱۸)."

در این سند فضای سایبری جزء جدایی ناپذیر از تمام جنبه‌های زندگی آمریکایی، از جمله اقتصادی و دفاعی دانسته شده‌است. همچنین، تصریح شده سازمان‌های خصوصی و دولتی هنوز در تلاش هستند تا سیستم‌های خود را حفظ کنند، در عین حال دشمنان نیز پیچیدگی فعالیت‌های بدخواهانه اینترنتی خود را افزایش داده‌اند. رفاه و امنیت آمریکا بستگی به این مسئله دارد که چگونه به فرصت‌ها و چالش‌های فضای مجازی پاسخ داده شود. زیرساخت‌های حیاتی، دفاع ملی و زندگی روزمره آمریکایی‌ها به فناوری‌های اطلاعاتی متصل به کامپیوتر و ارتباطات متکی است. همانطور که وایستگی

[1]. National Cyber Strategy of the United States of America 2018

جنبه‌های مختلف زندگی به فضای سایبری بیشتر می‌شود، آسیب پذیری‌ها و تهدیدات جدید ی آشکار می‌شود.

به ادعای واهی تیم امنیت ملی ترامپ در این سند : " استراتژی ملی سایبری نشان می‌دهد که چگونه ایالات متحده به ملت آمریکا نسبت به ادامه استفاده از مزایای فضای سایبری امن ضمانت می‌دهد و در عین حال، اصول مورد نظر دولت وی را در حفظ امنیت کشور و موجب ارتقای رونق مشخص می‌گرداند." حال آنکه این ادعایی بیش نبوده و صرفا به عنوان مستمسکی برای نفوذ سایبری در سایرنقاط جهان است.

این استراتژی توضیح می دهد که چگونه دولت ترامپ:

دفاع از میهن با حفظ شبکه ها، سیستم ها ، عملکردها و داده ها، ارتقای رفاه با تقویت اقتصاد دیجیتال، امن، شکوفا و ارتقای نوآوری های داخلی قوی،حفظ صلح و امنیت با تقویت توانایی ایالات متحده در رقابت با متحدان و همکاران را تضمین می کند (ترامپ،۲۰۱۸).

در ادامه سند ادعا شده برای جلو گیری و مجازات افرادی که از ابزار سایبری برای اهداف مخرب علیه منافع آمریکا استفاده می‌کنند، همچنین گسترش نفوذ آمریکا در خارج از کشور برای بسط اصول کلیدی اینترنت نامحدود و امن این سند اجرا خواهد شد. استراتژی ملی سایبری برای نشان دادن تعهد دولت ترامپ به تقویت توانایی های امنیت سایبری آمریکا و برقراری امنیت آمریکا در قبال تهدیدات اینترنتی است. این یک فراخوان مهم برای همه شرکت های بزرگ است تا اقدامات لازم را برای ارتقای امنیت ملی در ایالات متحده انجام هند.

ترویج اینترنت نامحدود و امن موجب پیشرفت های بزرگی در تجارت، سلامت، ارتباطات و دیگر زیرساخت های بشری شده است.به ادعای مطرح شده در این سند، قرنها جنگ سنتی بر سر حقوق بشر و آزادی های بنیادین، در عصر حاضر به شکل آنلاین دنبال می شود. امروزه آزادی بیان، اجتماعات صلح آمیز، انجمن ها و همچنین خلوت افراد، در فضای سایبری در معرض تهدید قرار دارند. علی‌رغم رشد بی سابقه اینترنت و پتانسیل اقتصادی و اجتماعی آن، همچنان فضای سایبری تحت تأثیر سانسور و سرکوب آنلاین قرار می گیرد. در این سند ادعا شده "... ما تلاش خواهیم کرد تا

اطمینان حاصل کنیم که رویکردمان نسبت به اینترنت باز تابع استانداردی بین المللی است. ما همچنین تلاش می کنیم تا از دولت های اقتدارگرایی که اینترنت نامحدود را به عنوان یک تهدید سیاسی تلقی و از تبدیل اینترنت آزاد و باز به اینترنت مستبد تحت کنترل خود به بهانه پوشش امنیت و یا مقابله با تروریسم حمایت می کنند، جلوگیری به عمل آوریم(همان)." حال آنکه خود دولت آمریکا بزرگترین کنترل کننده اینترنت (به بهانه مبارزه با تروریسم) و بزرگترین مانع اینترنت آزاد در جهان است.

یکی از تهدیدات آشکار سند در قسمت ۴ بند ۱ است که داعیه حفظ و ارتقای آزادی اینترنت توسط دولت آمریکا را دارد. در این بند آمریکا آزادی اینترنتی را به عنوان تجلی آنلاین حقوق بشر و آزادی های اساسی مانند آزادی بیان، آزادی اجتماعات صلح آمیز، آزادی مذهب و حفظ حریم خصوصی، مفهوم سازی می کند. به علاوه، به روشنی در این سند تصریح شده این آزادی‌های نوظهور چون می توانند هزینه‌های امنیتی آمریکا را کاهش دهد، ادامه خواهد یافت. حتی دولت آمریکا در مورد استقرار زیرساخت‌ها، حمایت از نوآوری‌ها، تدوین سیاست ها و طراحی استانداردها برای افزایش دسترسی جهانی به اینترنت و اطمینان از قابلیت همکاری امنیتی آن برای ایالات متحده رای‌زنی‌هایی خواهد داشت. در نهایت، ایالات متحده با شرکای بین المللی، دولت، صنعت، جامعه مدنی و دانشگاهیان در سراسر جهان، برای بهبود انطباق پذیری و آگاهی از شیوه های امنیتی سایبری همکاری خواهد کرد. چند روز پس از انتشار این سند، وزارت دفاع هم سندی منطبق بر آن را منتشر نمود. نکته مهم اسناد فوق بیشتر جنبه آشکارسازی علنی رویکرد تهاجمی دولت آمریکا است که از دوران اوباما آغاز شده بود و در این سند علنی شد. کارکرد این سند کاهش فشارها و انتقادات به دولت ترامپ برای انفعال در حوزه سایبری بود.

نهادهای تعیین کننده راهبرد سایبری و رویکرد آنها

حال که فرآیندها و روندهای سایبری که منجر به اتخاذ سیاست های سایبری و نیز شکل‌گیری یا حذف نهادهای سایبری در آمریکا شده را در قسمت قبل بررسی کردیم؛ نیاز به نمایش نقش دو نهاد مهم (کنگره و کاخ سفید) در تعیین راهبرد سایبری ایالات متحده است. تعاملات کاخ سفید و کنگره در تدوین راهبردهای دراز مدت ایالات متحده

مخصوصا در اموری که نیاز به تامین مالی کلان داشته و مرتبط به بخش نظامی هستند، نفش اساسی دارد.

۱. کاخ سفید: کاخ سفید از سال ۲۰۰۹که اوباما پا به آن گذاشت، به طور مستقیم درگیر مسایل امنیت سایبری گردید. رویکرد «فضای مجازی پاک» در دولت اوباما که برپایه نظریه تغییر توماس‌کوهن[1] شکل گرفته بود، توصیف‌کننده علائم و هشدارهای اولیه پیش از شروع یک حادثه مخرب می‌باشند. علائم اولیه درصورت شناسایی نشدن ممکن است تهدیدی جدی علیه سایر ارکان حاکم باشد. نظریه های سنتیِ امنیت سایبری آمریکا و اصول مبتنی بر آن، زیرساخت های حساس ملی را در معرض خطرهای غیرقابل قبول قرار می دهند.

مولفه مهم در «بازبینی سیاستگذاری سایبری در سال ۲۰۰۹» دفتر اجرایی رئیس‌جمهور است، این دفتر بهترین جایگاه را برای هم‌افزایی و اشتراک مساعی آژانس‌های مختلف و متعدد فدرال دخیل در امور سایبری دارد. در رویکرد جدید اشاره شده است که دولت نباید مسئولیت امنیت ملی را به ترازنامه‌ها و گزارش های بخش خصوصی محول کند. این رویکرد با اشاره به اتکای ایالات متحده به اطلاعات و فناوری‌های کامپیوتری نقش دولت، رئیس‌جمهور و شورای امنیت ملی[2] را در این زمینه خطیر قلمداد کرده است. اوباما در دسامبر ۲۰۰۹، آقای هاوارد اشمیت[3] را به عنوان معاون مشاور امنیت ملی و هماهنگ‌کننده امور امنیت سایبری در دفتر اجرایی رئیس جمهور منصوب کرد. با ابتکار آقای اشمیت، دولت اوباما، لایحه‌ای را تقدیم کنگره نمود که در آن افزایش کنترل دولت بر زیرساخت‌های حیاتی تصریح شده بود. سنا بسیاری از بخش‌های لایحه پیشنهادی اوباما را در قالب قانون امنیت سایبری[4] ۲۰۱۲ وارد نمود. (همه قسمت های لایحه پیشنهادی اوباما را تصویب نکرد.)

علاوه بر این، در دوره مدیریتی اشمیت ابتکاراتی چون آئین‌های نظارت مداوم، مدل‌های مدیریت سایبری ریسک‌پایه و ارتباطات اینترنت امن در مدیریت امنیت اطلاعات

---

1. Thomas Kuhn
2. National Security Council (NSC)
3. Howard Schmidt
4. Cyber Security Act of 2012.

فدرال[1] راه‌اندازی شد. دولت اوباما در سال ۲۰۱۱ سه اولویت جدید برای قانون فدرال مدیریت امنیت اطلاعات (FISMA) مشخص نمود. این اولویت ها عبارت هستند از : پایش مستمراینترنت، اتصال های اینترنتیِ مطمئن (TIC)[2] و تائیدِ فدرالِ هویت فردی در شبکه اینترنت (PIV)[3] که برای بهبود امنیت سایبری در دولت فدرال طراحی شده بودند. در میان این اولویت ها پایش مستمر بیشترین پتانسیل را برای تبدیل FISMA به مقررات امنیت سایبریِ موثر دارد . هدف نهایی پایش مستمر پوشش دادنِ محیط امنیت اطلاعات هر سازمان فدرال و ایجاد تصویر موثرِ مشترک (COP) از امنیت سایبری است که شکافها، مسیرهای حرکت دشمن و تهدیدات را آشکار می کند (kimmey,2012). در رابطه با اتصالات مطمئن هم دفترمدیریت و بودجه(OMB) [4] در سال ۲۰۱۱ سازمان‌های فدرال را به گردآوری، پایش مستمر و گزارش دهی منظم فضای سایبری و ارائه نتایج آن ازطریق یک پلت فرم امن و دولتی با نام Cyber Scope ملزم کرد. پلت فرم Scope Cyber نه تنها امنیت و صحت را ارتقا می دهد، بلکه با استانداردسازی قالب گزارش به طور خودکار کیفیت گزارش را هم بهبود می بخشد. معیارها و اقدامات گزارش دهیِ استانداردِ Cyber Scope بینش عمیقی نسبت به نقاط داده و محیط امنیت اطلاعات فدرال را فراهم می کنند(همان). بااین حال، گزارش‌ها حاکی از آن است که ۱۶ سازمان از ۲۱ سازمان فدرال مهم شبکه ها را ازنظر فعالیت های مشکوک به‌خوبی پایش نکرده بودند و قادر به ارائه گزارش به هنگامِ رخدادهای امنیت اطلاعاتی نبودند(Gao,2012:31).گرچه Cyber Scope به وزارت امنیت میهنی اجازه خواهد داد تا آسیب پذیری ها را با اطلاعات فدرال بهتر درک کند، بسیاری از آسیب پذیری ها جزء "مجهولاتِ مجهول" (یعنی آسیب پذیری از روش ناشناس در نقاط ناشناخته شبکه) باقی می مانند تا زمانی که روند پایش مستمر و ماندگار پیاده شود. قانون مدیریت امنیت اطلاعات ۲۰۰۲ به عنوان روندی تکرارپذیر به بهبودِ خود ادامه می دهد و به عنوان پیش نمایشی از نحوه تنظیم مقرراتِ امنیت سایبریِ زیرساخت‌های حساس با مالکیت خصوصی توسط آمریکا ایفای نقش می-

---

1. Federal Information Security Management Act.(FISMA)
2. Trusted Internet Conection
3. Personal Identity Verification
4. Office of management & budget

کند. پس از بازنشسته شدن اشمیت از خدمات دولتی در مِی ۲۰۱۲، مایکل دانیل[1] جایگزین وی شد. اگرچه جایگاه «هماهنگ‌کننده در امور امنیت سایبری» در کاخ سفید قطعی نبود و ترامپ که اعتقادی به کارایی چنین جایگاهی در کاخ سفید نداشت، این معاونت در شواری عالی امنیت ملی را در معاونت دیگری ادغام نمود. اما در هر صورت کاخ سفید تا روی کار آمدن دونالد ترامپ توجه بسیار زیادی را به امنیت سایبری معطوف کرده بود.

ترامپ در اولین اقدام با رد گزارش نهادهای اطلاعاتی ایالات متحده در مورد دست داشتن روسیه در انتخابات ریاست جمهوری نشان داد که وی اعتقادی به کار تخصصی در زمینه امنیت سایبری ندارد. سپس، هماهنگ کننده ای برای امور سایبری در کاخ سفید منصوب نشد. بعد از آن بخش های سایبری وزارت امور خارجه ایالات متحده (اداره دیپلماسی سایبری) تعطیل شدند. پس از انتخاب جان بولتون به سمت مشاور امنیت ملی هم شاهد حذف معاونت امنیت سایبری از آن سمت توسط بولتون بودیم که به مرور ایده فوق را بیش از پیش تقویت کرد . وی نه تنها اصراری به گرفتن اختیارات حاکمیتی از کنگره برای نظارت بر شرکت های خصوصی نداشت بلکه سعی در انهدام میراث اوباما در این زمینه هم داشت. فشارهای شدید کنگره و افکار عمومی مخصوصا در حزب جمهوری خواه ترامپ را بر آن داشت که چند دستور اجرایی در این زمینه صادر کند . اما همچنان شاهد ابتکار سایبری جدیدی توسط او نبوده ایم تا سال ۲۰۱۸ که طی یک سندملی تغییر رویکرد سایبری اتخاذ شده در دوران اوباما را به صورت علنی اعلام کرد. ظاهرا از این به بعد کنگره پیش قراول توسعه و حفاظت از امنیت سایبری در ایالات متحده خواهد بود. در ادامه به نقش آن در طول سال‌های اخیر می‌پردازیم.

۲. کنگره امریکا: کنگره امریکا متشکل از دو مجلس نمایندگان و سنا است و رکن قانون‌گذاری دولت ایالات متحده محسوب می شود. در این مقاله قصد ورود به روند پیچیده قانونگذاری در کنگره را نداریم و صرفا از باب نوع دیدگاه کنگره نسبت به مقوله امنیت سایبری گذری کوتاه به اقدامات کنگره در لوایح مربوط به امنیت سایبری داریم. علیرغم اینکه طبق قانون اساسی امریکا رئیس جمهور اختیارات وسیعی درباره سیاست خارجی و

[1]. Michael Daniel

امنیت ملی دارد اما برای تخصیص بودجه به اقدامات خود نیاز به تصویب مجلس نمایندگان و برای ماندگاری اقدامات خود در دولت‌های آینده نیاز به تایید هر دو مجلس کنگره دارد. نقش کنگره در امنیت سایبری امریکا همواره ثابت نبوده است. گاهی همسو با دولت و حتی جلوتر از آن عمل کرده و گاهی مانعی بر سر حرکت دولت بوده است . مثلا، دولت اوباما اصرار داشت که یک برنامه مسئولیتی محدود برای همکاری بخش خصوصی-عمومی که از زیرساخت‌های کشور حمایت و حفاظت می‌کنند، ضروری است. کنگره با تصویب قانون برای الزام بخش خصوصی مخالف بود اما با تخصیص بودجه برای تشویق بخش خصوصی به همکاری موافق بود و بودجه هنگفتی را به این بخش اختصاص داده است. برای آشکار شدن دلیل جذابیت همکاری پروژه ای شرکت های خصوصی با دولت فدرال امریکا بد نیست به ارقام بودجه ای دولت اوباما در این حوزه بیندازیم و روند رو به رشد آن را هم در نظر بگیریم . دولت ترامپ در سال مالی ۲۰۱۷ درخواست ۱۹ میلیارد دلار برای بخش امنیت سایبری کرد، درحالی که دولت اوباما در سال مالی ۲۰۱۶ ، در بودجه سازمان های مهم اجرایی، جمعا کمتر از ۱۴ میلیارد دلار را به بخش امنیت سایبری اختصاص داده بود. این رقم صرفا شامل هزینه های مستقیم مثل پرسنل ، ابزار ، آزمایش، و پرسنل می شود(fortune.com/obama-budget-cybersecurity/).

نکته مهم زمانی مشخص می شود که بدانیم کنگره صد و یازدهم در شرایط رکود سالهای ۲۰۰۸ تا ۲۰۱۲ این افزایش بودجه را شروع کرده بود ، طوری که بودجه بخش سایبری وزارت دفاع را بیش از سه برابر درخواست قبلی آن تعیین نمود! در شرایط رکود و بحران مالی آمریکا قطعا برای شرکت های خصوصی سهیم شدن در این خوان نعمت فدرال موهبتی محسوب می شد، البته به شرطی که همکاری با دولت از روی اجبار نبوده باشد و منجر به از دست رفتن بازارهای بزرگتر و رو به رشد مثل چین و هند نشود .

در سال ۲۰۱۱ دفتر نمایندگان حزب جمهوری خواه در کنگره برای پاسخ به فقدانِ آمادگی سایبری در زیرساخت های حساس کشور، یک کارگروه امنیت سایبری تشکیل دادند(Republicans Task force,2011). گزارش کارگروه مسئولیت ذاتی دولت فدرال در ایمن سازی زیرساخت های حساس کشور دربرابر حملات سایبریِ فاجعه آمیز را تائید کرد و خواهان وضع مقرراتی در این زمینه بود. این گزارش پیشنهاد

کرد که « اگر مواردی باشد که تنظیم مجدد مقررات یک صنعت که پیش‌تر تدوین شده (توان هسته ای، برق، کارخانه های شیمیایی، تصفیه خانه ها)، برای ایمنی سایبری لازم است، انجام آن مجاز می باشد(همان). این گزارش اساس لایحه جامعِ امنیت سایبری را تشکیل داده و بهبود امنیت سایبری و اثرگذاریِ اشتراک گذاری اطلاعات (قانون PrECISE) را بالا می‌برد که شامل زیرساخت هایی حساس با مالکیت خصوصی نیز می شود(Naghesh,2014). بااین حال، بنابه دلایل نامعلومی که مسلما به لابی سازمان های خصوصی وابسته اند، اعضای کارگروه از لایحه صرف نظر کردند و گزارشی را که چند ماه قبل تائید کرده بودند، رد نمودند(lewis,2012) . برغم بحران اقتصادی و مشکلات مالی در امریکا که از سال ۲۰۰۸ به وجود آمد مباحث امنیت سایبری به خوبی توسط کنگره بودجه بندی شد و پول سرشاری عاید شرکت های مقاطعه‌کار خصوصی این حوزه می شود . فقدان کمیته اصلی، فرعی یا مشترکی در کنگره که متولی بخش امنیت سایبری باشد، باعث به سرانجام نرسیدن اکثر لوایح در میان درگیری بین کمیته های مختلف سنا و مجلس نمایندگان می شود. لازم به ذکراست، تنها در سنا هفت کمیته هستند که ادعای تولیت بر حوزه سایبر را دارند(لرد و شارپ،۱۳۹۲). نقطه عطف موضع گیری های کنگره در رابطه با امنیت سایبری، انتخابات ریاست جمهوری سال ۲۰۱۶ آمریکا بود جایی که رسوایی حمله به ایمیل های هیلاری کلینتون که با سرور عمومی ارسال شده بودند و همچنین حملات سایبری به کنگره حزب دموکرات به همراه انتشار اطلاعات محرمانه آنها تاثیر تعیین کننده ای در انتخاب ترامپ داشت. زمانی که جیمز کلاپر در کنگره آمریکا اعلام کرد: "روس ها در زمینه سایبری بسیار فعال هستند و احتمالا در این عملیات اطلاعاتی علیه ایالات متحده حضور داشته اند و من پیش بینی می کنم حملات سایبری آنها علیه آمریکا ادامه دارد. " زمینه تغییر ایجاد شد. سپس سایر نهادهای امنیتی امریکا ادله خود را در اختیار کنگره و رئیس جمهور منتخب (ترامپ) و رئیس جمهور بر سرکار (اوباما) دادند این احتمال تبدیل به یقین شد که روسیه در یک نبرد سایبری علیه امریکا به اهداف خود دست یافته است. اما اکنون مشکل رئیس جمهور جدید این بود که خود شخصا اعتماد و تمایلی به نظارت شدید دولت بر بخش خصوصی ندارد.

مخصوصا در حوزه سایبری که به نوعی پیروزی اش وامدار آن است. سناتور فوت شده جمهوریخواه و رئیس سابق کمیته نیروهای مسلح سنا، جان مک کین در سخنرانی خود در اوکراین با موضعگیری شدید علیه اقدامات سایبری روسیه، حملات سایبری را در حد اقدام نظامی دانسته و احتمال اقدام به پاسخ اتمی در صورت حمله سایبری گسترده را منتفی ندانسته است(رویترز،۲۰۱۷).

نتیجه گیری

در اواسط دهه نود دولت ایالات متحده امریکا پس از فروپاشی شوروی احساس قدرت بی سابقه و تسلط بر دنیا را داشت و مانعی در توسعه زیرساخت های سایبری با سرمایه گذاری و مدیریت بخش خصوصی نمی دید. اما در دهه اول قرن بیست ویکم (دوران بوش) که وابستگی جامعه واقتصاد به این فضا تکامل پیداکرد، بتدریج نگرانی-های امنیتی پدید آمدند.

البته، رخدادهای سایبری نظیر هک کردن سیستم کنترل ترافیک یا چند وبسایت محبوب در فاصله های زمانی طولانی چیزی نبود که جامعه یا حاکمیت ایالات متحده را دچار شوک نماید. اما آنچه موضوع سایبری را در دستور کار سیاسی این دوران (بوش) قرار داد جو حاکم بر دولت ناشی از حملات یازده سپتامبر بود که باعث شد ابعاد امنیتی همه موضوعات حتی انتقال های مالی بالای ۱۰ هزار دلار هم زیر ذره بین قرار گیرد. از سال ۲۰۰۹ بود که تکامل سایبری و جدی شدن فعالیت گروه‌های تروریستی در جذب نیرو، تبلیغات و ارتباطات؛ همچنین معرفی قابلیت‌های تهاجمی نرم افزارهای سایبری منجر به استفاده نظامی-امنیتی از این فضا شد.

در نمودار زیر تغییر شرایطی که منجر به تغییر راهبردها گردیده، نمایش داده شده است.

اولین الگوی اساسی در حوزه امنیت سایبری واگذاری به بخش خصوصی است که نخستین بار در دولت دوم کلینتون معرفی شد و هنوز هم طبق قانون برخی از نهاد های امنیتی در امریکا ، مانند وزارت امنیت میهنی که با بخش خصوصی سروکار دارند، مجبورند بر مبنای آن عمل کنند. این الگو براساس کارکرد موثرتر بخش خصوصی

تدوین شده و بر نظریه پیشرفتِ تدریجی و نظریه خودگردانی متکی است. نتیجه وضعی امنیتی شدن مباحث سایبری در دوران جرج بوش کنترل بیشتر دولت بر آن و تغییر مرجع امنیت می شد . این انتقادات و تلاش ها باعث گشت به مرور یک نظریه دولتی امنیت سایبری هم شکل بگیرد که شرکت های خصوصی را در تامین امنیت سایبری زیرساخت های حیاتی امریکا ناکارآمد می دانست. این نظریه که با هشدارها و توصیه های اندیشکده های راهبردی ایالات متحده در اواخر دوره بوش پسر پیشنهاد گردید و در دوره اوباما به طور جدی پیگیری شد، تا اواخر دوره اوباما از ظهور کامل و پذیرش در همه محافل دولتی و خصوصی برخوردار نشد. چرا که این متد با توجه به مشکلات و ناسازگاری‌اش با نظام لیبرال آمریکا ، در مواجهه با مقاومت های ساختاری شانس چندانی برای ظهور کامل نداشت و در مسیر تصویب در کنگره در سال ۲۰۱۲ دستخوش تغییرو تحولاتی شد. دولت اوباما خواستار بکارگیری دو ابزار اقتصادی و حقوقی برای تشویق و تنبیه شرکت های مشغول در عرصه سایبری و زیرساخت های حساس بود که کنگره هیچگاه با ابزار دوم به شیوه اجباری موافقت نکرد. با همه این تلاش‌ها،کاخ سفید هنوز هم برنامه های ناهمخوان خود در امنیت سایبری را زیر یک راهبرد جامع، آنطور که در سایر بخش ها انسجام بخشیده، یکپارچه نکرده است.

البته، پس از حملات سایبری روسیه در انتخابات ریاست جمهوری به نظر می رسد، موضع کنگره در حال تغییر است اما با توجه به نتیجه رسوایی های سایبری که در نهایت باعث انتخاب ترامپ شد، به نظر نمی رسد دولت ترامپ هم اصلا برنامه ای برای پیشبرد این راهبرد داشته باشد. باید دید طرح دوحزبی که در این زمینه در کنگره در حال چکش کاری است در میان کاخ سفید و کنگره به چه سرنوشتی دچار خواهد شد. آثار تصویب همکاری اجباری بخش خصوصی و دولتی امریکا درکوتاه‌مدت می‌تواند در زمینه توانایی دفاع سایبری و حملات سایبری امریکا را به قدرتی دست نیافتنی مبدل سازد ؛ چراکه توانایی فنی و تکنولوژیک مجموعه شرکت‌های امریکایی در زمینه سایبری از هردولتی بیشتر است و آنچه که تاکنون باعث شده چنین توانایی جامعی در اختیار دولت قرار نگیرد، رقابت تجاری بین این شرکت ها و در اولویت قرار دادن سود اقتصادی خود بوده است.

همکاری اجباری با دولت امریکا احتمالا خود شرکت ها را در درازمدت با مشکلات عدیده ای مواجه می کند. اگر مجموعه ای شامل سیسکو ،AT&T ، مایکروسافت ، گوگل ، آمازون ، اپل با اجبار دولتی در کنار هم و تحت هدایت دولت آمریکا قرار گیرند تا زراد خانه سایبری ایالات متحده را تجهیز کنند، در دراز مدت موجب تضعیف این شرکت ها و در نهایت تضعیف قدرت سایبری امریکا که به آنها وابسته شده است میشود. چراکه قطعا این خسارت از دو ناحیه متوجه شرکت ها خواهد شد . بعد خارجی خسارت ناشی از عدم اعتماد و همکاری دولت های خارجی دیگر به سرویس دهی امن این شرکت ها است و بعد داخلی آن نیز انتشار اطلاعات و تکنولوژی انحصاری آنها بین رقبای متوسط در امریکاست.

پس اینجا شاهد یک پارادوکس یا معمای امنیتی جدید در ایالات متحده خواهیم شد. اگر امنیتی سازی صورت بگیرد و دولت به عنوان مرجع امنیت وارد موضوعات شود، در دراز مدت شرکت های خصوصی و به تبع آن دولت آمریکا دچار صدمات اقتصادی و عقب افتادگی تکنولوژیک می شوند. از طرف دیگر، با مشکلات اقتصادی شرکت ها و عقب افتادگی شان هم بودجه کشور که از مالیات آنها تامین می شود دچار مشکل می گردد و هم توان تامین نیازهای به روز تکنولوژیک کشور را ندارند. در نهایت، موجب تضعیف قدرت کلی می شود. پس وسواس کنگره و اصرار شرکت های خصوصی بی دلیل نبوده است. از سال ۲۰۱۲ مالکیتِ بخش خصوصی بر زیرساخت های حساس آمریکا از ۸۰٪ فراتر رفته است(http://tiaonline.org). پس رها کردن آن در دست بخش خصوصی که عموما امنیت سایبری را یک ریسک اقتصادی و موضوعی فنی تلقی می کند، کار چندان درستی نمی باشد. پس لزوم نظارت دولتی و تبادل اطلاعات دوجانبه برای ارتقای توان تکنولوژیک دولت با دانش یک رشته شرکت ها و کمک دولت به ارتقای امنیت سایبری سایر شرکت ها انکار ناپذیر می باشد. حل این معما بدون ضرر هیچ یک از طرف ها، نیاز به قانون گذاری های پیچیده و ظریف و همکاری های متقاطع با حمایت بودجه ای ویژه دارد تا هم در جای مورد نیاز بخش خصوصی به دولت کمک کند و بالعکس در موارد دیگری دولت به بخش خصوصی نظارت یا کمک نماید؛ ضمن اینکه آسیب امنیتی و اقتصادی متوجه هیچ طرفی نشود.

ترامپ در مدت حضور در کاخ سفید نه تنها در این زمینه هنوز هیچ اقدامی انجام نداده که برخی سمت ها و افراد که در این زمینه مشغول بکار بودند را هم برکنار کرده است. همه این ها در کنار اعتقاد او به عدم دخالت روسیه در انتخابات باعث شده کنگره تغییر موضع داده و خود دست بکار شود. کنگره در سال ۲۰۱۸ قانونی را برای احیای اداره دیپلماسی سایبری با کارکرد های مشخص و ریاست یک فرد با درجه سفیر تصویب کرده که نیاز به تایید سنا برای اجرایی شدن دارد. زور آزمایی ترامپ و کنگره در زمینه امنیت سایبری آینده ساختارهای سایبری، ایالات متحده که امروزه بیش از هر زمانی در معرض تهدید قرار دارند را رقم خواهد زد.

منابع و مآخذ

فارسی

۱. بوش،جرج واکر، بخشنامه بازبینی سایبری،۲۰۰۳ http://www.whitehouse.gov

۲. بوش،جرج واکر، راهبردملی سایبری،۲۰۰۵

۳. حسینی، پرویز و ظریف‌منش ، حسین ، مطالعه تطبیقی ساختار دفاع سایبری کشورها، فصلنامه پژوهشهای حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام) سال دوم، شماره ۵ (بهار ۱۳۹۲): صص ۶۸ – ۴۱

۴. فراتر از متن، راهبرد سایبری وزارت دفاع ، ۲۰۱۵
http://archive.defense.gov/home/features/2015/0415_cyberstrategy/final_2015_dod_cyber_strategy_for_web.pdf

۵. فرمان اجرایی ۱۳۰۱۰ ریاست جمهور ایالات متحده
(fas.org/irp/offdoc/eo13010.html)

۶. لرد ،کریستین و تراویس شارپ، *آینده سایبری امریکا امنیت و رفاه*،(مترجم: محمد محمدی تمنایی)، مرکز راهبردی سپاه پاسداران، ۱۳۹۲

۷. مایکل هاوارد، کلازوویتس، مترجم: غلامحسین میرزاصالح، نشرطرح نو(۱۳۷۷) تهران

۸. بیات، محبوبه، سیاست های تهدید و امنیت سایبری، انتشارات مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی ،تهران ۱۳۸۹

لاتین

9. Bush, George walker ,2003, U.S. President, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* http://www.whitehouse.gov (accessed August 11, 2016)
10. Bush,George,2005, U.S. President, The National Strategy to Secure Cyberspace, 2.
11. Castro, Daniel, "U.S. Federal Cybersecurity Policy," in Cybersecurity: Public Sector Threats
12. and Responses, ed. by Kim Andreasson. 1st ed. (Boca Raton, FL: CRC Press, 2012), 127-58.
13. Clinton, William, Executive Order no. 13010, "Critical Infrastructure Protection.", 1996, Washington.D.C.
14. Executive Office of the President, Memo to the Heads of Executive Departments and Agencies, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, April 21, 2010, http://www.whitehouse.gov (accessedSeptember 21, 2016).
15. Federal Efforts to Implement Requirements, by Gregory Whilshuen , www.**gao**.gov/ (accessed September 21, 2017*)*
16. Hoover, J. N, "CEOs Voice Support for Cyber Legislation, with Caveats," Information Week,http://www.informationweek.com
17. Government Accounting Office, Information Security: Weaknesses Continue Amid New
18. Hoover, J. N. , "Cybersecurity Balancing Act," Information Week,2009,
19. House Republican Cybersecurity Task Force, *Recommendations of the House Republican Cybersecurity Task Force* . available at: (accessed February 4, 2016),
20. http://archive.defense.gov/home/features/2015/0415_cyberstrategy/final_2015_dod_cyber_strategy_for_web.pdf
21. http://fortune.com/2016/02/09/obama-budget-cybersecurity/
22. http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf.
23. http://www.informationweek.com (accessed September 21, 2018).
24. Information Technology Security Handbook, 2003, Washington, DC: World Bank

25. Jaap, Ariens ,2016, https://www.npr.org/series/469827708/the-apple-fbi-debate-over-encryption
26. Kimmey, Phillip, "FISMA, Cyberscope, and Federal IT Security," Center for Strategic and International Studies,2012 http://csis.org (accessed January 14,2016).
27. Kitten, Tracy, "Are Banks Winning the DDoS Battle?" Information Security Media Group Corporation, http://www.bankinfosecurity.com (accessed February 3, 2016).
28. Lewis, James A, "Code Red," *Foreign Policy,* August 2012, available at http://www.foreignpolicy.com (accessed November 18, 2016).
29. McCarthy, John et al., "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 1st ed. (Dulles, VA: Potomac Books, 2009), 544.
30. Nagesh, Gautham, "House Cybersecurity Bill would Establish Federal Overseer," The Hill, available at https://www.benton.org/node/107349 (accessed February 18, 2016).
31. National Institute of Standards and Technology, "Security Management and Assurance: FISMA Overview," U.S Department of Commerce, http://csrc.nist.gov
32. National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework*, 42.
33. Office of Management and Budget, FY 2011 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002
34. Recomendations for Crtical Infrastructure and the Global Supply Chain," Telecommunications Industry Association, http://tiaonline.org
35. Schectman, Joel, "PwC: Companies Trim IT Security as Budgets Stagnate," Wall Street Journal, http://blogs.wsj.com (accessed February 1, 2016).
36. Snowden,Edward , 2017 https://www.cloudwards.net/prism-snowden-and-government-surveillance/
37. Telecommunications Industry Association, "Securing the Network: Cybersecurity,The Department Of Defence ,Cyber Strategy (Beyond the Built),2015

38. U.S. Presidential Decision Directive 63, "Protecting America's Critical Infrastructure," (May 22,1998), http://www.fas.org (accessed October 27, 2016).

39. Vaughan–Nichols, Steven J., 2018, March 20,

https://www.zdnet.com/article/how-cambridge-analytica-used-your-facebook-data-to-help-elect-trump/