مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گزارش سند پنج

راهبرد ملی امنیت سایبری ایالات متحده آمریکا ۲۰۲۳

U.S National Cyber Security Strategy, 2023

گزارش سند

شماره پنجم
تیر ۱۴۰۲

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

راهبرد ملی امنیت سایبری ایالات متحده آمریکا ۲۰۲۳

محتوای این اثر الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست.

تهیه‌شده در پژوهشگاه فضای مجازی
گروه مطالعات فرهنگی و اجتماعی

مترجم:
علیرضا قبولی شاهرودی
(کارشناس گروه مطالعات فرهنگی و اجتماعی)

ناظر علمی:
امیررضا باقرپور شیرازی
(مدیر گروه مطالعات فرهنگی و اجتماعی)

نشانی: تهران، سعادت آباد، خیابان علامه شمالی، کوچه هجدهم غربی، پلاک ۱۷
تلفن: ۰۲۱-۲۲۰۷۳۰۳۱
کد پستی: ۱۹۹۷۹۸۷۶۲۹

فهرست

سخن نخست یک

سخن نخست

سخن نخست

ما امروزه در جهانی زندگی می‌کنیم که تحولات فضای مجازی همه عرصه‌های حیات بشری را به عصری جدید فراخوانده است؛ عصری مشحون از بیم و امید درباره تحولاتی عمیق و شتابان که آینده‌ای مبهم و غیرقابل‌پیش‌بینی را برای جوامع معاصر به تصویر می‌کشد. ایران اسلامی نیز در یک دهه گذشته تحت تأثیر تحولات پُردامنه و همه‌جانبهٔ این صحنه قرار گرفته و در تمامی ساحات فرهنگی، اجتماعی، اقتصادی و سیاسی با آنچه تحول دیجیتال خوانده می‌شود، روبرو بوده است.

در این میان اما ظهور انقلاب اسلامی در جهانی که نظم مدرنیستی و الگوی لیبرال دموکراسی را پایان تاریخ قلمداد می‌کرد، نشانه مهم و آشکاری بر این مُدعاست که با «پایبندی به مبانی اندیشه اسلامی و ارزش‌های انقلاب اسلامی» و «جهاد مستمر علمی و تولید دانش» می‌توان از میان دریای خروشان جهان دیجیتال گذر کرد؛ از تهدیدهای آن فرصت ساخت و افقی روشن برای استقرار نظمی نوین و تمدن اسلامی گشود. بنابراین، همواره این پرسش در مقابل اندیشمندان و حکمرانانِ دغدغه‌مند مطرح خواهد بود که جامعه ایرانی-اسلامی معاصر چگونه می‌تواند با تمهید مواجهه‌ای فعال و خردمندانه، از این پیچ تاریخی و تمدنی به سلامت عبور کرده و ضمن بهره‌برداری از فرصت‌های بی‌بدیل آن، نه‌تنها خلأها و کاستی‌های گذشته را جبران کند، بلکه فرآیند تحقق تمدن اسلامی را نیز در

گام دوم انقلاب اسلامی تسهیل نماید.

در همین راستا، **پژوهشگاه فضای مجازی** در تلاش است که با رصد و تحلیل رخدادها، تحولات و روندهای آیندهٔ فضای مجازی، ارکان و ذی‌ربطان مختلف نظام حکمرانی کشور را مُتفطن فرصت‌ها، تهدیدها و چالش‌های جهان معاصر نماید؛ به این امید که با نقش‌آفرینی هوشمندانه و مجاهدانه در این تحولات روزآمد، مسیر تحقق جامعه اسلامی مجازی و ایران قوی در عصر فضای مجازی را هموارتر گرداند.

سید محمدامین آقامیری
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

مقـــدمه

سخنی از رئیس جمهور آمریکا

امروزه هیچ عرصه‌ای از زندگی آمریکایی نیست که تحت تأثیر تکنولوژی‌های دیجیتال قرار نداشته باشد. متصل‌بودن و ارتباط با دیگران - که به‌واسطهٔ دسترسی به اینترنت ممکن شده - حیات جوامع را در سرتاسر جهان دگرگون کرده است؛ همهٔ ما در تجربهٔ همه‌گیریِ کرونا این مسئله را لمس کردیم. ازاین‌روست که دولت کنونیِ آمریکا - به کمک لایحهٔ فراحزبیِ [توسعه] زیرساخت - اقدام به سرمایه‌گذاری ۶۵ میلیارد دلاری برای دسترسی هر فرد آمریکایی به اینترنت قابل‌اعتماد و پرسرعت نموده است. ما وقتی از طریق گوشی‌های تلفن همراه با عزیزانمان تماس می‌گیریم، یا برای به اشتراک‌گذاشتن ایده‌هایمان با دیگران وارد شبکه‌های اجتماعی می‌شویم، یا برای کسب‌وکارِ خود و یا تأمین هر کدام از نیازهای اساسی‌مان وارد اینترنت می‌شویم، نیاز به این داریم که از امنیت، اعتمادپذیری و سلامتِ اکوسیستمِ زیرساختیِ دیجیتال مطمئن باشیم. سند «راهبرد ملی امنیت سایبری آمریکا» به شرح رویکرد جامعی می‌پردازد که دولت من برای تأمین بهتر امنیت فضای سایبری و حصول اطمینان از این مسئله اتخاذ کرده است که ایالات متحده آمریکا مستحکم‌ترین موقعیتِ ممکن برای دستیابی به همهٔ قابلیت‌ها و مزایای آیندهٔ دیجیتالیِ ما را دارا می‌باشد.

امنیت سایبری برای فعالیت‌های بنیادین اقتصاد ما، عملکرد

زیرساخت‌های حیاتی‌مان، قدرت دموکراسی و نهادهای دموکراتیک این کشور، حریم خصوصیِ داده‌ها و ارتباطات ما، و همچنین دفاع ملی میهن‌مان امری ضروری است. دولت من از ابتدای مسیر خود قاطعانه پیگیرِ تقویت امنیت سایبری بوده است؛ من مقامات ارشدی را در حوزه امنیت سایبری در کاخ سفید منصوب کرده و فرمانی اجرایی را برای ارتقاء امنیت سایبری کشور صادر کرده‌ام.

این دولت در همکاری نزدیک با بخش خصوصی، اقداماتی را برای محافظت از مردم آمریکا در برابر هکرها، تحت پیگرد قرار دادن متخلفین و مجرمان سایبری، و دفاع در برابر کارزارهای سایبری مخربی که به‌نحو فزاینده‌ای امنیت و حریم خصوصی ما را هدف قرار می‌دهند، در دستور کار خود قرار داده است. ما در کنار متحدین‌مان در سرتاسر جهان تلاش کرده‌ایم که توان کشورهایمان برای دفاع و واکنش در برابر تهدیدات سایبری - که از جانب کشورهای اقتدارگرا منافع ملی ما را هدف قرار می‌دهند - را ارتقاء دهیم.

سند حاضر بر آن است که همکاری جدی بین بخش‌های دولتی و خصوصی برای ایمن‌سازی فضای سایبری حیاتی است. ادعای چالش‌برانگیز ما در این سند راهبردی این است که مسئولیت حوزه امنیت سایبری [تا کنون] بیش‌ازحد بر دوش کاربران منفرد و سازمان‌های کوچک‌مقیاس قرار داشته است. بنابراین، هدف این راهبرد این است که موازنهٔ جدید و مؤثرتر و منصفانه‌تری میان بخش‌های مختلفی همچون صنعت، جامعه مدنی، دولت‌های ایالتی، قبیله‌ای و منطقه‌ای در مسئولیتِ حوزهٔ امنیت سایبری برقرار کند. ما محرک‌های مختلف را به‌نحوی سامان‌دهی خواهیم کرد که تقویت‌کنندهٔ سرمایه‌گذاری بلندمدت در حوزه امنیت، تاب‌آوری، و تکنولوژی‌های نویدبخشِ جدید

باشند. همچنین در کنار متحدین و شرکای خود می‌کوشیم هنجارهای رفتار مسئولانه دولت‌ها [در حوزه سایبری] را تحکیم کرده، پاسخگوییِ کشورها در قبال رفتار غیرمسئولانه [خود] در فضای سایبری را افزایش دهیم و شبکهٔ مجرمانی که در پسِ حملاتِ سایبریِ خطرناک در سرتاسر جهان هستند را منهدم کنیم. علاوه‌براین، دولت آمریکا خواهد کوشید با همکاری کنگره، منابع و ابزارهای لازم برای اجرای اقدامات مربوط به امنیت سایبری در زیرساخت‌های حیاتی کشور را تأمین کند.

همانطور که بارها گفته‌ام، جهان ما در یک نقطه عطف قرار دارد. این مسئله در مورد جهان دیجیتال نیز صدق می‌کند. هر گامی که امروز برمی‌داریم و انتخابی که انجام می‌دهیم، جهت‌گیری جهان ما در دهه‌های آینده را تعیین خواهد کرد؛ به‌ویژه آن‌جا که در حال تدوین و پیشبرد قوانین و هنجارهای رفتار در فضای سایبری هستیم. ما باید اطمینان حاصل کنیم که اینترنت باز، آزاد، جهانی، اشتراک‌پذیر، قابل اعتماد و ایمن باقی می‌ماند؛ [ویژگی‌هایی] که طنین آن‌ها در ارزش‌های جهانیِ حقوق بشر و آزادی‌های اساسی به گوش می‌رسد.

ارتباط دیجیتال باید ابزاری برای ارتقاء و توانمندسازی مردم باشد، نه وسیله‌ای برای سرکوب و سلطه. در این سند راهبردی به تفصیل توضیح داده شده است که آمریکا آماده است که قدرتمندانه با این چالش مواجه شده، در همکاری با نزدیک‌ترین متحدان خود و همهٔ هم‌پیمانانی که با ما در مورد آیندهٔ دیجیتالی روشن‌تر هم‌افق هستند، گام به پیش بگذارد.

جو بایدن

مقدمه

اینترنت دنیای ما را متحول کرده است. این تکنولوژی تنها در طول یک نسل، شیوه نوآوری، ارتباط برقرار کردن و اشتراک‌گذاری اطلاعات را در مقیاسی جهانی دگرگون کرده و پیشرفت‌های بی‌سابقه‌ای را در رفاه، برابری و ارتباطات انسانی رقم زده است. ما بر مبنای اینترنت است که توانسته‌ایم اکوسیستم دیجیتالیِ شکوفایِ خود را بسازیم که نتیجهٔ آن ادغام سیستم‌ها و تکنولوژی‌ها [ی مختلف] با اقتصاد، جوامع و تک‌تکِ افراد بوده است.

این اکوسیستم دیجیتال در مسیر تکامل خود، ارزش‌های معماران و کاربرانش را منعکس می‌کند. تکنولوژی‌ها[ی جدید] باعث پیشرفت دموکراسی، آزادی بیان، نوآوری و برابری شده‌اند. اما درعین‌حال، در اقصی نقاط جهان از آن‌ها برای سرکوب و اقتدارگراییِ دیجیتال نیز سوءاستفاده شده است: سرقت اطلاعات و مالکیت معنوی، انتشار اطلاعات نادرست، مختل‌کردن زیرساخت‌های حیاتی، ترویج آزارگری و سوءاستفادهٔ آنلاین، توانمندسازیِ مجرمین و ترویج خشونت‌های افراط‌گرایانه، و تهدید صلح و ثبات. انسان و تکنولوژی روزبه‌روز بیشتر در هم تنیده می‌شوند و [این مسئله] باعث رشد و شکوفایی بهترین و بدترین وجوه انسانی شده است.

ما در دههٔ تعیین‌کنندهٔ کنونی اهداف بلندی برای توسعهٔ ارزش‌محورِ اکوسیستم خود در پیش گرفته‌ایم. این دولت در حال ساخت یک شبکه هوشمند است که از برق توزیع‌شدهٔ تجدیدپذیر تغذیه کرده و در هماهنگی با سیستم‌های هوشمند عمل می‌کند و نویدبخش آینده‌ای

روشن و تاب‌آور در تأمین انرژی است. ما رؤیای یک «اینترنت اشیاء»[1] بالغ را در سر داریم که همه چیز - از کالاهای مصرفی گرفته، تا کنترل‌های دیجیتالِ صنعتی و سیستم‌های ماهواره‌ای - را در بر گرفته و علاوه‌بر افزایش کارایی و ایمنی، بصیرت‌های تعیین‌کننده‌ای را به محیط‌زیست و اقتصاد ما می‌افزاید. ما همچنین در حال بنیان‌نهادنِ مسیری برای همکاریِ زندهٔ جهانی هستیم که باعث شکل‌گیری حجم عظیمی از قدرت داده‌ای و محاسباتی شده و امکان دستیابی به اکتشافات علمی بی‌شمار و سایر دستاوردهای بشری - که هنوز حتی در مخیلهٔ ما نیز نمی‌گنجند - را فراهم می‌کند.

دستیابی به رؤیای آینده‌ای مرفه و به‌هم‌پیوسته، در گرویِ امنیت سایبری و تاب‌آوری تکنولوژی‌ها و سیستم‌های زیربناییِ آن‌هاست. ما تجربه‌های زیادی اندوخته و پیشرفت‌های قابل‌توجهی در دفاع جمعی از اکوسیستم دیجیتال خود داشته‌ایم. جبههٔ دفاعِ سایبری هر روز حملاتِ مورد حمایتِ دولت‌ها [ی متخاصم] را خنثی کرده و توطئه‌های بزه‌کارانه در سرتاسر جهان را بی‌اثر می‌کند. اما پویاییِ ساختاریِ ذاتیِ اکوسیستم دیجیتال باعث شده است که این تلاش‌های دفاعی هیچ‌گاه کافی نباشند. اجزای مختلف این اکوسیستم همواره مستعد اختلال بوده و در برابر سوءاستفاده آسیب‌پذیر هستند و عموماً از جانب بازیگران متخاصم مورد سوءاستفاده قرار می‌گیرند.

ما باید تحولاتی بنیادین در پویایی‌های ذاتیِ اکوسیستم دیجیتال ایجاد کنیم تا ورق را به سود جبههٔ دفاع سایبری برگردانده و تلاش‌های نیروهای تهدیدگر را ناکام بگذاریم. هدف ما ساختن یک اکوسیستم دیجیتالِ قابل‌دفاع و تاب‌آور است که در آن، حمله به سیستم‌ها نسبت به

1 Internet of Things (IoT)

دفاع از آن‌ها سخت‌تر و پرهزینه‌تر بوده، اطلاعات حساس یا شخصی محفوظ باشند، و در آن خطاها یا سوانح به عواقب بنیان‌برافکن و سیستمی منجر نشوند. ما می‌توانیم و می‌بایست که برای ایجاد این شرایط، موقعیت را غنیمت شمرده و بکوشیم والاترین ارزش‌های خود - که در اعلامیهٔ آیندهٔ اینترنت[1] و پیمان‌نامهٔ آزادیِ آنلاین ذکر شده است - را محقق کنیم.

در این راهبرد، ایالات متحده آمریکا و متحدین و هم‌پیمان‌های آن در ساختن این اکوسیستم دیجیتال در کنار یکدیگر قرار گرفته‌اند؛ تا [این اکوسیستم] ذاتاً قابلیت دفاع‌پذیری و تاب‌آوریِ بیشتری پیدا کرده و هماهنگی بهتری با ارزش‌های ما پیدا کند. در انتهای این دههٔ تعیین‌کننده ما به این اهداف دست خواهیم یافت؛ تا بتوانیم گام‌های بلندی به سمت یک آیندهٔ دیجیتال - که به نفعِ همهٔ ما باشد - برداریم.

محیط راهبردی

ایالات متحده پیشرفت قابل‌توجهی در جهت تحقق دیدگاه ایجابیِ رئیس‌جمهور در مورد آیندهٔ دیجیتال داشته است؛ اما روندهای نوظهور باعث گشایش فرصت‌های جدیدی برای پیشرفتِ بیشتر و همچنین چالش‌های جدیدی شده‌اند که می‌بایست بر آن‌ها غلبه کرد. بازیگران متخاصم همواره تهدیدکنندهٔ پیشرفت ما در مسیر [دستیابی به] یک اکوسیستم دیجیتالِ فراگیر و عادلانه هستند که تقویت‌کنندهٔ رفاه بوده و با ارزش‌های دموکراتیک ما هم‌سو باشد.

1 Declaration for the Future of the Internet (DFI)

روندهای نو ظهور

جهان در حال ورود به مرحله جدیدی از تعمیق وابستگی‌های دیجیتالی است. در دهه‌های پیشِ رو تکنولوژی‌های نوظهور، پیشرفته و درهم‌تنیده، تغییرات چشم‌گیری را به خود خواهند دید که منجر به گشوده‌شدنِ فرصت‌های جدیدی برای شکوفایی و رشد بشر و هم‌چنین تشدید ریسک‌های سیستمی که ریشه در سیستم‌های ناامن دارد، خواهد شد.

نرم‌افزارها و سیستم‌ها در حال پیچیده‌ترشدن هستند؛ این مسئله برای شرکت‌ها و مصرف‌کنندگان ارزش آفرین است؛ اما هم‌زمان ناامنی جمعی ما را نیز افزایش می‌دهد. اکثر اوقات ما در حال اضافه‌کردن قابلیت‌ها و تکنولوژی‌های جدید به سیستم‌هایی هستیم که خود از پیش پیچیده و آسیب‌پذیر هستند، و این کار به قیمت [از دست رفتن] امنیت و تاب‌آوری تمام می‌شود. ظهور گستردهٔ سیستم‌های هوش مصنوعی - که می‌توانند به روش‌هایی عمل کنند که حتی برای سازندگان آن‌ها نیز غیرقابل‌پیش‌بینی است - پیچیدگی و تهدیدهای مربوط به بسیاری از مهم‌ترین سیستم‌های تکنولوژیکِ ما را افزایش می‌دهد.

اینترنت هم‌چنان افراد، مشاغل، جوامع و کشورها را در قالب پلتفرم‌های مشترک با یکدیگر مرتبط می‌کند؛ پلتفرم‌هایی که راه‌حل‌های تجاریِ تکثیرپذیر و تبادل بین‌المللی را امکان‌پذیر می‌کنند. اما این درهم‌تنیدگیِ فراگیر خطراتی نیز به همراه دارد. حمله به یک سازمان، بخش یا ایالت می‌تواند به‌سرعت به بخش‌ها و مناطق دیگر سرایت کند؛ همانطور که در سال ۲۰۱۷ در حمله سایبری روسیه به اوکراین -

موسوم به حملهٔ «نات‌پتیا»[1] - شاهد بودیم، که در سراسر اروپا، آسیا و آمریکا گسترش یافت و میلیاردها دلار خسارت به بار آورد. با افزایش وابستگی‌های متقابل [در سطح جهان]، هزینه احتمالی اینگونه حملات افزایش می‌یابد.

تکنولوژی‌های دیجیتال هر روز بیشتر از قبل وارد حساس‌ترین قلمروهای زندگی ما شده، و در کنار افزایش راحتی [و رفاه]، خطرات جدید و اغلب پیش‌بینی‌نشده‌ای را به بار می‌آورند. همه‌گیری کوید ۱۹ حیات دیجیتال ما را عمیق‌تر و گسترده‌تر از قبل کرد. همانطور که زندگی ما با پخش ویدئو و صدا، دستگاه‌های پوشیدنی و تکنولوژی‌های بیومتریک در هم تنیده می‌شود، کمیت و عمق گردآوریِ داده‌های شخصی نیز به طور تصاعدی افزایش می‌یابد. سرقت این داده‌ها نیز به‌سرعت رو به افزایش بوده و برای بازیگران متخاصم ابزارهای جدیدی را برای نظارت، دستکاری و باج‌گیری از افراد فراهم می‌کند.

نسل بعدیِ اتصالات، مرز بین دنیای دیجیتال و فیزیکی را از بین خواهد برد و برخی از حیاتی‌ترین سیستم‌های ما را در خطر اختلال قرار خواهد داد. کارخانه‌ها، شبکه‌های برق، تأسیسات تصفیه آب و دیگر زیرساخت‌های حیاتیِ ما به‌طور فزاینده‌ای سیستم‌های کنترل آنالوگ قدیمی را کنار می‌گذارند و به‌سرعت تکنولوژی‌های عملیات دیجیتال آنلاین (اُ. تی)[2] را وارد کار خود می‌کنند. تکنولوژی‌های وایرلس پیشرفته، اینترنت اشیاء و دارایی‌های مبتنی بر فضا[3] - از جمله آن‌هایی که موقعیت‌یابی، ناوبری و زمان‌بندی را برای استفاده‌های نظامی و غیرنظامی، نظارت بر محیط‌زیست و آب‌وهوا، و فعالیت‌های روزمره

1 NotPetya
2 online digital operational technology (OT)
3 space-based assets

مبتنی بر اینترنت (به‌عنوان مثال بانک‌داری و پزشکیِ راه دور) را امکان‌پذیر می‌کنند - این روند را تسریع کرده و بسیاری را از سیستم‌های حیاتیِ ما را به سمت فضای آنلاین سوق داده و [در نتیجه] باعث می‌شوند که حملات سایبری به‌طور ذاتی مخرب‌تر شده و بر زندگی روزمرهٔ ما تأثیر عمیق‌تری بر جای بگذارند.

بازیگران متخاصم

فعالیت‌های سایبری متخاصمانه همواره در حال تحول بوده و از مزاحمت‌های شرورانه به جاسوسی و سرقت مالکیت معنوی، حملات آسیب‌رسان به زیرساخت‌های حیاتی، حملات باج‌افزاری و کارزارهای تأثیرگذاریِ سایبری که برای تضعیف اعتماد عمومی به بنیاد دموکراسی ما طراحی شده‌اند، تکامل یافته است. ابزارها و خدمات هکریِ تهاجمی - به‌عنوان مثال جاسوس‌افزارهای تجاریِ خارجی - که زمانی تنها در دسترس تعداد اندکی از کشورهای قدرتمند بود، اکنون به وفور در دسترس هستند. این ابزارها و خدمات باعث قدرتمندترشدنِ کشورهایی می‌شود که تا پیش از این توان آسیب رساندن به منافع ایالات متحده در فضای سایبری را نداشتند، و باعث گسترش تهدیداتِ گروه‌های مجرمانهٔ سازمان‌یافتهٔ می‌شود.

کشورهایی نظیر چین، روسیه، ایران، کره شمالی، و سایر دیکتاتوری‌هایی که مقاصد تجدیدنظرطلبانه دارند، از قابلیت‌های پیشرفتهٔ سایبری برای پیگیریِ اهداف خصمانهٔ خود بهره می‌گیرند که مغایر با منافع ما و هنجارهای پذیرفته‌شدهٔ بین‌المللی هستند. بی‌توجهیِ گستاخانهٔ آن‌ها به حاکمیت قانون و حقوق بشر در فضای سایبری، امنیت ملی و رفاه اقتصادی ایالات متحده را تهدید می‌کند.

جمهوری خلق چین اکنون گسترده‌ترین، فعال‌ترین و پایدارترین تهدید برای شبکه‌های دولتی و بخش خصوصی است و تنها کشوری است که هم قصد تغییر نظم بین‌المللی را داشته و هم قدرت اقتصادی، دیپلماتیک، نظامی و تکنولوژیکِ آن برای انجام این کار روز به روز در حال افزایش است. طی ده سال گذشته، این کشور عملیات سایبری را فراتر از سرقت مالکیت معنوی گسترش داده است تا به پیشرفته‌ترین رقیب راهبردی ما تبدیل شود که توانایی تهدید منافع ایالات متحده و تسلط بر تکنولوژی‌های نوظهور حیاتی برای توسعه جهانی را دارد. جمهوری خلق چین با بهره‌گیریِ موفق از اینترنت به‌عنوان ستون فقرات دولت نظارتی و قابلیت‌های تأثیرگذاری خود، در حال صادر کردن دیدگاه خود از اقتدارگرایی دیجیتال، شکل‌دهی به اینترنت جهانی مطابق تصویر [ایده‌آلِ] خود، و تهدید حقوق بشر در ورای مرزهای خود است.

برای بیش از دو دهه، روسیه از توانایی‌های سایبری خود برای بی‌ثبات‌کردن همسایگان و مداخله در سیاست داخلی کشورهای دموکراتیک در سراسر جهان استفاده کرده است. روسیه همچنان به‌عنوان یک تهدید سایبری دائمی به حساب می‌آید؛ زیرا همواره در حال بهبود و ارتقاء توانایی‌های سایبری خود در حوزه‌هایی همچون جاسوسی، حمله، تأثیرگذاری و [نشر] اطلاعات نادرست خود در جهت [اِعمال] سلطه بر کشورهای مستقل، پناه دادن به مجرمان بین‌المللی، تضعیف معاهدات و همکاری‌های ایالات متحده، و تضعیف سیستمِ قانون‌محورِ بین‌المللی است. روسیه در تهاجم متجاوزانهٔ خود به اوکراین در سال ۲۰۲۲ حملات سایبری زیادی – مشابه حملهٔ نات‌پتیا که در گذشته انجام داده بود – به زیرساخت‌های غیرنظامیِ حیاتیِ بسیاری از کشورهای اروپایی انجام داده است و هزینه‌های بسیاری به آن‌ها تحمیل کرده است.

پیچیدگی و ارادهٔ حکومت‌های ایران و جمهوری دموکراتیک خلق کره [شمالی] برای انجام فعالیت‌های خصمانه در فضای سایبری به‌نحو مشابهی رو به افزایش است. ایران از قابلیت‌های سایبری برای تهدید متحدان ایالات متحده در خاورمیانه و سایر نقاط استفاده کرده است. اما کره شمالی فعالیت‌های سایبری خود را بیشتر برای کسب درآمد از طریق فعالیت‌های مجرمانه انجام می‌دهد؛ فعالیت‌هایی همچون سرقت ارزهای دیجیتال، فعالیت‌های باج‌افزاری، و به‌کارگیری نیروهای پنهانی در حوزه فناوری اطلاعات به منظور پیگیری جاه‌طلبی‌های هسته‌ایِ این کشور. بلوغ بیشتر این قابلیت‌ها می‌تواند تأثیرات قابل توجهی بر منافع ایالات متحده، متحدان و شرکای آن داشته باشد.

امروزه فعالیت‌های سایبری سندیکاهای بزه‌کار نیز تهدیدی برای امنیت ملی، امنیت عمومی و رفاه اقتصادی ایالات متحده و هم‌پیمان‌ها و شرکای آن به حساب می‌آید. امروزه حملات باج‌افزاری خدمات و مشاغل حیاتی را در سراسر کشور و جهان تهدید می‌کنند، از خطوط لوله انرژی و شرکت‌های مواد غذایی گرفته تا مدارس و بیمارستان‌ها. مجموع خسارات اقتصادی ناشی از حملات باج‌افزاری همچنان در حال افزایش است و سالانه به میلیاردها دلار می‌رسد. سندیکاهای مجرمانه اغلب در کشورهایی فعالیت می‌کنند که با دستگاه قانونی ایالات متحده همکاری نداشته و بعضاً چنین فعالیت‌هایی را تشویق کرده و مأمنی برای آن فراهم می‌کنند و یا [دست‌کم] بی‌تفاوت از کنار آن می‌گذرند. اینگونه فعالیت‌های مخرب سایبری همچنان جامعه را تهدید می‌کنند. در این میان، افرادی که منابع لازم برای محافظت از خود، بازیابی و یا امکان استمداد [از دیگران] را ندارند، بیشترین آسیب را متحمل می‌شوند.

رویکرد ما: مسیری به سوی تاب‌آوری در فضای سایبری

ما با همکاری نزدیک و پایدار با همهٔ ذی‌نفعان مختلف در سرتاسر اکوسیستم دیجیتال، به دنبال این هستیم که این اکوسیستم را ذاتاً قابل‌دفاع‌تر، تاب‌آورتر و هماهنگ‌تر با ارزش‌های آمریکایی کنیم. این راهبرد به دنبال ایجاد و تقویت [این] همکاری‌ها حول ۵ محور است: (۱) دفاع از زیرساخت‌های حیاتی، (۲) مختل‌کردن و از بین بردن عوامل تهدید، (۳) شکل‌دادن به نیروهای بازار برای ایجاد امنیت و تاب‌آوری، (۴) سرمایه‌گذاری برای آینده‌ای تاب‌آور، و (۵) همکاری‌های بین‌المللی برای پیگیری اهداف مشترک. هر تلاشی در این مسیر، مستلزم سطوح کم‌نظیری از همکاری در میان طرف‌های ذی‌نفعِ مختلف - از جمله بخش عمومی، بخش خصوصی و صنایع، جامعهٔ مدنی، و متحدین و هم‌پیمان‌های آمریکا در سرتاسر جهان - است.

محورهای اصلی این راهبرد، چشم‌اندازی از اهداف و اولویت‌های مشترک را برای این جوامع [ذی‌نفع] پیشِ‌چشم نهاده، چالش‌هایی را که برای دستیابی به این چشم‌انداز با آن‌ها روبرو هستند شناسایی می‌کند و اهداف راهبردی را [برای آن‌ها] مشخص می‌کند تا تلاش‌های خود را حول آن سازماندهی کنند.

ما برای تحقق چشم‌اندازی که این محورها ترسیم می‌کنند، دو تغییر اساسی در نحوهٔ تخصیص نقش‌ها، مسئولیت‌ها و منابع ایالات متحده در فضای سایبری ایجاد خواهیم کرد. ما با این تغییرات علاوه بر تلاش برای بهبود عملکرد دفاعیِ خود، به‌دنبال تغییر آن دسته از پویایی‌های اساسی [سیستم] هستیم که در حال حاضر با منافع ما در تضاد هستند.

ایجاد موازنه‌ای دوباره در مسئولیت‌های دفاع از فضای سایبری

تواناترین و بهترین بازیگران در فضای مجازی باید بهترین نگهبانانِ اکوسیستم دیجیتال باشند. امروزه، کاربران نهایی بخش زیادی از مسئولیت کاهش خطرات سایبری را به دوش دارند. افراد، کسب‌وکارهای کوچک، دولت‌های ایالتی و محلی، و اپراتورهای زیرساخت منابع محدود و اولویت‌های رقابتی دارند، بااین‌حال، انتخاب‌های این بازیگران می‌تواند تأثیر قابل‌توجهی بر امنیت سایبری ملی ما داشته باشد. لغزش لحظه‌ای یک فرد در قضاوت خویش، استفاده از رمز عبور قدیمی، یا یک کلیک اشتباه روی لینکی مشکوک نباید پیامدهای امنیت ملی داشته باشد. تاب‌آوری سایبری جمعی ما نباید به هوشیاری مداوم کوچک‌ترین سازمان‌ها و تک‌تک شهروندان ما وابسته باشد.

در عوض، در هر دو بخش دولتی و خصوصی، توانمندترین و بهترین بازیگران باید نقش بیشتری در امن و تاب‌آور نمودنِ اکوسیستم دیجیتال ایفا کنند. در یک جامعه آزاد و به‌هم‌پیوسته، حفاظت از داده‌ها و تضمینِ قابل‌اطمینان‌بودنِ سیستم‌های حیاتی باید به عهده مالکان و اپراتورهای سیستم‌های زیرساختیِ حوزه داده‌ها و نیز ارائه‌دهندگان تکنولوژی‌ها و خدماتی باشد که زیربنای این سیستم‌ها را تشکیل می‌دهند. نقش حکومت عبارت است از حفاظت از سیستم‌های خود، حصول اطمینان از اینکه نهادهای خصوصی - به ویژه زیرساخت‌های حیاتی - از سیستم‌های خود محافظت می‌کنند، و نیز انجام وظایف اصلی حکومتی - مانند حضور در عرصه دیپلماسی، جمع آوری اطلاعات، سامان‌دهی هزینه‌های اقتصادی، اجرای قانون، و انجام اقدامات قهرآمیز برای مقابله با تهدیدات سایبری. صنعت و دولت باید همکاری مؤثر و متوازنی را

برای اصلاح خطاها و اشکالات بازار، به حداقل رساندن آسیب‌های ناشی از حوادث سایبری برای آسیب‌پذیرترین افراد جامعه، و دفاع از اکوسیستم دیجیتال مشترک ما در پیش بگیرند.

بازتنظیم مشوق‌ها برای حمایت از سرمایه‌گذاری‌های بلندمدت

اقتصاد و جامعهٔ ما باید تقویت‌کنندهٔ روندی از تصمیم‌گیری باشد که در بلندمدت در مسیر افزایش تاب‌آوری و قابل‌دفاع‌بودنِ فضای سایبری حرکت کند. ایجاد تعادل بین الزامات کوتاه‌مدت در برابر چشم‌انداز بلندمدت کار آسانی نخواهد بود. ما باید از سیستم‌هایی که در حال حاضر داریم دفاع کنیم و درعین‌حال به سمت ساختن اکوسیستم دیجیتالی حرکت کنیم که ذاتاً قابل‌دفاع‌تر و تاب‌آورتر باشد.

این راهبرد نشان می‌دهد که چگونه دولت فدرال از همه ابزارهای موجود برای سامان‌دهی مشوق‌ها استفاده کرده و تلاش می‌کند که به شیوه‌ای تعاملی، عادلانه و متقابلاً سودمند، تلاش‌های مختلفی که در این زمینه انجام می‌شود را منسجم و یکپارچه سازد. هدف ما اطمینان از این مسئله است که نیروهای بازار و برنامه‌های عمومی [و حاکمیتی] به یک اندازه تقویت‌کنندهٔ امنیت و تاب‌آوری هستند، در جهت تربیت نیروی کاری قدرتمند و متنوع حرکت می‌کنند، به‌صورت هدفمند به‌دنبال [گسترش] امنیت و تاب‌آوری هستند، سرمایه‌گذاری‌های تحقیق و توسعه[1] را به‌صورت راهبردی به سمت حوزهٔ امنیت سایبری سوق می‌دهند، و به ارتقاء مدیریتِ جمعیِ اکوسیستم دیجیتال کمک می‌کنند. دولت فدرال برای تحقق این اهداف بر نقاطی دست خواهد گذاشت که در آن‌ها،

1 Research and Development (R&D)

اقداماتی با کم‌ترین بارِ مداخله‌گرانه، می‌توانند بیشترین دستاوردها را - از جهت دفاع‌پذیری و تاب‌آوری سیستمی - به همراه داشته باشند.

دولت فدرال در حال سرمایه‌گذاری‌هایی بلندمدت در بازسازی زیرساخت‌ها، دیجیتالی‌کردن و کربن‌زدایی سیستم‌های انرژی، ایمن‌سازی زنجیرهٔ تأمین نیمه‌هادی‌ها، مدرن‌سازی تکنولوژی‌های رمزنگاری، و باز-طراحی اولویت‌های سیاست خارجی و داخلی ما است. ایالات متحده این فرصت را دارد تا موازنهٔ جدید مشوق‌ها را به‌نحوی طراحی کند که شرایط امکانیِ تحققِ زیربناهایی قوی‌تر و تاب‌آورتر برای ساخت آیندهٔ اکوسیستم دیجیتال این کشور را فراهم کنند.

ابتناء بر خط‌مشی‌های موجود

این سند راهبردی در عین ارائه رویکرد جدید خود به موضوع امنیت سایبری، بر دستاوردهای مهمی استوار است که تا پیش از این در ساختن و سامان‌دادنِ محیط راهبردی و اکوسیستم دیجیتال ما نقش‌آفرین بوده‌اند. دولت بایدن در آغاز کار خود درگیر مدیریت پیامدهای حملهٔ روسیه به پلتفرم «سولار ویندز اوریون»[1] و نیز حملهٔ جمهوری خلق چین به سرورهای «مایکروسافت اکسچنج»[2] شد. رئیس‌جمهور با انتصاب رهبران عالی‌رتبه و مجرب جدیدی در شورای امنیت ملی[3] و دفتر فرمانده سایبری ملی[4] آمریکا، سطح نقش‌آفرینی و رهبریِ کاخ سفید [در این زمینه] را ارتقاء داده و به‌سرعت در جهت استفاده از درس‌های آموخته‌شده از این حوادث و تبدیل آن‌ها به اقدامات عملی حرکت کرد.

1 SolarWinds Orion platform
2 Microsoft Exchange
3 National Security Council (NSC)
4 National Cyber Director (ONCD)

این تلاش‌های رو به جلو، بنیان شکل‌گیریِ این سند راهبردی بوده‌اند که در کنار راهبرد امنیت ملی[1] و راهبرد دفاعی ملی[2] توسط یک تیم گستردهٔ بین‌سازمانی و از طریق یک فرآیند مشاورهٔ چند ماهه با بخش خصوصی و جامعه مدنی طراحی و تدوین شده است. هم‌چنین در این سند از رویکردها و بصیرت‌های سازمان دی. اف.آی[3]، ائتلاف آنلاین آزادی[4]، و سایر تلاش‌های دیرپا برای تحقق بخشیدن به یک چشم‌انداز دموکراتیک برای اکوسیستم دیجیتال بهره گرفته شده است. همچنین جهت‌گیری مبنایی دستور اجراییِ شماره ۱۴۰۲۸ - «ارتقاء امنیت سایبری کشور»[5] -، بیانیه شمارهٔ ۵ امنیت ملی - «ارتقاء امنیت سایبری سیستم‌های کنترل زیرساخت‌های حیاتی»[6] -، بیانیهٔ شماره ۸ امنیت ملی - «بهبود امنیت سایبری [سازمان] امنیت ملی، وزارت دفاع و سیستم‌های اطلاعاتی کشور»[7] - و سایر فرامین اجرایی، در این سند به‌کار گرفته شده و پیگیری می‌شود. این راهبرد به‌دنبال این است که حوزهٔ امنیت سایبری را در سرمایه‌گذاری‌های بلندمدت جدیدی به واسطهٔ قانون فراحزبی [توسعه] زیرساخت[8]، لایحه کاهش تورم[9]، و نیز مشوق‌هایی که در حوزه تولید نیمه‌هادی‌ها (تراشه‌ها)[10]، قانون علم[11]، و فرمان اجرایی ۱۴۰۱۷ - «زنجیره‌های تأمین آمریکا»[12] - شکل گرفته‌اند، وارد کند.

همچنین، این راهبرد در ادامهٔ تلاش‌های دولت‌های قبلی شکل

1 National Security Strategy
2 National Defense Strategy
3 Development financial institution (DFI)
4 the Freedom Online Coalition
5 Improving the Nation's Cybersecurity
6 Improving Cybersecurity for Critical Infrastructure Control Systems
7 Improving the Cybersecurity of National Security, Department of Defense (DoD), and Intelligence Community Systems
8 Bipartisan Infrastructure Law
9 Inflation Reduction Act
10 CHIPS
11 The Science Act
12 America's Supply Chains

گرفته است و اگرچه به‌عنوان جایگزین راهبرد ملی سایبری ۲۰۱۸ ارائه شده است، اما در بسیاری از اولویت‌های آن - از جمله دفاع جمعی از اکوسیستم دیجیتال - همان مسیر را با شتاب ادامه می‌دهد. دولت حاضر همچنان خود را متعهد به افزایش امنیت و تاب‌آوری سیستم‌های فضایی ایالات متحده[1] - آن‌چنان که در مصوباتی از جمله دستورالعمل سیاست فضایی شماره ۵ - «اصول امنیت سایبری برای سیستم‌های فضایی» آمده است - می‌داند. علاوه‌براین، دولت به شیوه‌های مختلف - از جمله از طریق «طرح ملی هوش مصنوعی»[2] و «راهبرد ملی برای [اینترنت] ۵ جیِ امن»[3] و سایر خط‌مشی‌ها و طرح‌های موجود - به تلاش خود برای ایمن‌سازی تکنولوژی‌های نسل بعدی ادامه خواهد داد.

هدف‌گذاری این راهبرد برای ایمن‌سازی سیستم‌های فدرال و همکاری با بخش خصوصی، بر مبنای فرمان اجرایی ۱۳۸۰۰ - «تقویت امنیت سایبری شبکه‌های فدرال و زیرساخت‌های حیاتی»[4] -، فرمان اجرایی ۱۳۶۹۱ - «تقویتِ اشتراک‌گذاریِ اطلاعات امنیت سایبری [از جانب] بخش خصوصی»[5] - و فرمان اجرایی ۱۳۶۳۶ - «ارتقاء امنیت سایبری زیرساخت‌های حیاتی»[6] - شکل گرفته و با چارچوب‌های تعیین‌شده توسط خط‌مشی ابلاغیِ ریاست‌جمهوری شماره ۲۱ - «امنیت و تاب‌آوری زیرساخت‌های حیاتی»[7] - و شماره ۴۱ - «[ستاد] هماهنگی سوانح سایبری ایالات متحده آمریکا»[8] - در تناسب قرار دارد. این سند در واقع بسیاری از تلاش‌های راهبردی سابق را که در ابتدا توسط «طرح

1 Cybersecurity Principles for Space Systems
2 the National Artificial Intelligence Initiative
3 National Strategy to Secure 5G
4 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
5 Promoting Private Sector Cybersecurity Information Sharing
6 Improving Critical Infrastructure Cybersecurity
7 Critical Infrastructure Security and Resilience
8 United States Cyber Incident Coordination

جامع امنیت سایبری ملی»[1] در سال ۲۰۰۸ آغاز شده بود را با خود به همراه داشته و به پیش می‌برد.

1 Comprehensive National Cybersecurity Initiative

رکن اول:
دفاع از زیرساخت های حیاتی

رکن اول: دفاع از زیرساخت‌های حیاتی

دفاع از سیستم‌ها و دارایی‌هایی که زیرساخت‌های حیاتی ما را تشکیل می‌دهند برای [حراست از] امنیت ملی، امنیت عمومی و رفاه کشور حیاتی است. مردم آمریکا باید به دسترس‌پذیری و تاب‌آوری این زیرساخت‌ها و خدمات حیاتیِ آن‌ها اطمینان داشته باشند. هدف ما عملیاتی کردن یک مدل پایدار و مؤثر از دفاع جمعی است که ریسک و مسئولیت را منصفانه و متوازن توزیع کرده و سطح قابل‌اتکایی از امنیت و تاب‌آوری را برای اکوسیستم دیجیتال ما تأمین کند.

همکاری برای مقابله با تهدیدات پیشرفته تنها در صورتی مؤثر خواهد بود که مالکان و اپراتورهای زیرساخت‌های حیاتی به میزانی از تمهیدات حفاظتیِ [حوزه] امنیت سایبری برخوردار باشند که بتوانند در برابر نفوذ و مداخلهٔ نیروهای متخاصم مقاومت بیشتری از خود نشان دهند. دولت کنونی الزامات جدیدی را برای امنیت سایبری در بخش‌های حیاتیِ مختلف تعریف کرده است. مسئولان و متصدیان بخش‌های مختلف ملزم به تنظیم مقرراتی خواهند بود که سطح بالاتری از امنیت سایبری را در مقیاس کلان تأمین کنند. رویکرد این دولت تعامل ویژه با حوزهٔ صنعت بوده است تا امکان طراحی چارچوب‌های تنظیم‌گریِ منسجم و پیش‌بینی‌پذیر را [در حوزهٔ] امنیت سایبری فراهم کند که تمرکزشان بر حصول نتایج امنیتی و تداوم عملیات و عملکردها [ی مختلف] و در عین

حال گسترش نوآوری و همکاری [در میان بخش‌های مختلف] باشد.

سازمان‌ها و شرکت‌های بخش خصوصی تعهدات قابل توجهی را برای مشارکت در تلاش‌های دفاعیِ مشترک متقبل شده‌اند. کارزار «سپرها بالا!»[1] - که قبل از حملهٔ متجاوزانهٔ روسیه به اوکراین در سال ۲۰۲۲ برای افزایش آمادگی فعالانه و گسترش اقدامات مؤثر برای مبارزه با فعالیت‌های مخرب آغاز شده بود - نمونه‌ای از همکاری [بخش‌های] عمومی و خصوصی است که باید تکثیر و تکرار شود.

ما باید قابلیت‌های جدید و نوآورانه‌ای ایجاد کنیم که برای مالکان و اپراتورهای زیرساخت‌های حیاتی، سازمان‌های فدرال، فروشندگان محصولات، ارائه‌دهندگان خدمات و سایر ذی‌نفعان امکان همکاری مؤثر، سریع و گسترده را فراهم کنند. آژانس‌های فدرال که از ارائه‌دهندگان زیرساخت‌های حیاتی پشتیبانی می‌کنند، باید قابلیت‌های خود و توانایی‌شان برای همکاری با سایر نهادهای فدرال را افزایش دهند. هنگامی که حوادث رخ می‌دهد، واکنش [نهادهای] فدرال باید با بخش خصوصی و ذی‌نفعانِ ایالتی، محلی، قبیله‌ای و سرزمینی کاملاً سازگار و هماهنگ باشد.

در نهایت، دولت فدرال می‌تواند با ارتقاء [قابلیت‌های] دفاعی و تاب‌آوری سیستم‌های خود، در جهت حراست بهتر از زیرساخت‌های حیاتی حرکت کند. دولت حاضر خود را متعهد به ارتقاء امنیت سایبری فدرال از طریق تلاش‌های بلندمدت در جهت عملیاتی‌کردن راهبردِ معماریِ «اعتماد صفر»[2] و مدرن‌سازی زیرساخت‌های تکنولوژی‌های اطلاعاتی و عملیاتی می‌داند. با انجام این کار، امنیت سایبری فدرال

1 The “Shields Up” Campaign
2 Zero trust architecture strategy

می‌تواند الگویی برای همهٔ زیرساخت‌های حیاتی در سراسر ایالات متحده باشد و نمونه‌ای از ساخت و بهره‌برداریِ موفق از سیستم‌های ایمن و تاب‌آور ارائه کند.

هدف راهبردی ۱ / ۱: تحقق ملزومات امنیت سایبری برای حمایت از امنیت ملی و امنیت عمومی

مردم آمریکا باید به خدمات اولیه‌ای که زیربنای زندگی آن‌ها و اقتصاد کشور را شکل می‌دهد، اعتماد داشته باشند. علیرغم اینکه رویکردهای داوطلبانه در حیطهٔ امنیت سایبریِ زیرساخت‌های حیاتی پیشرفت‌های معنی‌داری ایجاد کرده است، فقدان قواعد الزام‌آور منجر به نتایج ناکافی و نامنسجم شده است. بازار امروز مشوق‌های کافی برای صاحبان و اپراتورهای زیرساخت‌های حیاتی که در اقدامات پیشگیرانه برای جلوگیری یا کاهش اثرات حوادث سایبری سرمایه‌گذاری می‌کنند، ارائه نمی‌کند - و حتی در اکثر موارد محرک‌های منفی به آن‌ها عرضه می‌کند.

مقررات می‌توانند با متوازن‌کردنِ زمین بازی، بدون قربانی‌کردن امنیت سایبری یا تاب‌آوریِ عملیاتی، باعث شکل‌گیری رقابت سالم شوند. محیط راهبردی ما نیازمند چارچوب‌های تنظیم‌گریِ مدرن و چابکی برای امنیت سایبری است که متناسب با ریسک‌های هر بخش طراحی شده، به‌نحوی هماهنگ عمل کرده تا از تکرار پیشگیری نمایند، تکمیل‌کنندهٔ همکاری [بخش‌های] عمومی و خصوصی باشند، و نسبت به هزینه‌های عملیاتی‌کردن [دستورالعمل‌های خود] آگاهی داشته باشند. مقررات جدید و به‌روز شدهٔ امنیت سایبری باید به‌نحوی طراحی شوند که

قادر به تأمین نیازهای امنیت ملی و عمومی، و بعلاوه امنیت و ایمنی افراد و نهادهایی که مخاطبِ مقررات‌گذاری بوده‌اند، و کارکنان، مشتریان، عملیات و داده‌های آن‌ها باشند.

دولت ما در این زمینه پیشرفت‌هایی داشته است و [در برخی از حوزه‌ها] ملزومات امنیت سایبری را به‌واسطهٔ سازمان‌هایی همچون ادارهٔ امنیت حمل‌ونقل[1] - در بخش‌های کلیدی مانند خطوط لوله نفت و گاز طبیعی، هوانوردی و راه آهن - و سازمان حفاظت از محیط‌زیست[2] - در مورد سیستم‌های آبی - طراحی کرده است. [در پیش گرفتنِ یک] فرآیند مشارکتی بین صنعت و نهادهای تنظیم‌گر باعث شکل‌گیری الزامات تنظیم‌گرانه‌ای می‌شود که از نظر عملیاتی و تجاری کارآمد بوده و عملکرد ایمن و تاب‌آور زیرساخت‌های حیاتی را تضمین می‌کنند.

مؤثرترین و کارآمدترین چارچوب‌های تنظیم‌گری آن‌هایی هستند که به جای تحمیل مقررات اضطراری پس از وقوع بحران، پیش از وقوع بحران وضع شده باشند.

تدوین مقررات امنیت سایبری برای ایمن‌سازی زیرساخت‌های حیاتی

دولت فدرال از مراجع قانونی و نهادهای موجود برای شکل‌دهی به الزامات اولیه و ضروریِ امنیت سایبری در بخش‌های کلیدی استفاده خواهد کرد. اگرچه در کشور ما اختیارات قانونی سازمان‌ها و ادارات فدرال برای عملیاتی کردنِ حداقل الزامات امنیت سایبری یا کاهش نارسایی‌های بازارِ مرتبط با آن، خلاءها و شکاف‌هایی به چشم می‌خورد، اما دولت در

1 Transportation Security Administration
2 Environmental Protection Agency

همکاری با کنگره به‌دنبال رفع این نواقص خواهد بود. در مواردی که ایالت‌ها یا نهادهای تنظیم‌گرِ مستقل دارای اختیاراتی هستند که می‌توان از آن‌ها برای تمهیدِ ملزومات امنیت سایبری استفاده کرد، دولت آن‌ها را تشویق می‌کند تا از این اختیارات به شیوه‌ای برنامه‌ریزی‌شده و هماهنگ استفاده کنند.

مقررات باید مبتنی بر عملکرد بوده و از چارچوب‌های موجودِ امنیت سایبری و نیز استانداردها و رهنمودهای مورد اجماع - از جمله اهداف عملکرد سایبری[1] که سازمان امنیت سایبری و زیرساخت (سیسا)[2] منتشر کرده، و یا چارچوب ارتقاء امنیت سایبری زیرساخت‌های حیاتی[3] که توسط مؤسسه ملی استانداردها و تکنولوژی[4] تدوین شده است - بهره بگیرد؛ و همچنین آن‌قدر چابک باشد که بتواند خود را با افزایش توانایی‌های دشمنان و تغییر تاکتیک‌های آن‌ها سازگار کند. نهادهای تنظیم‌گر در [روند] تنظیم مقررات امنیت سایبری برای زیرساخت‌های حیاتی، تشویق می‌شوند تا براساس اصول امنیت ذاتی[5] عمل کرده، اولویت خود را دسترس‌پذیربودنِ خدمات قرار دهند و اطمینان حاصل کنند که سیستم‌ها به گونه‌ای طراحی شده‌اند که در صورت شکست نیز فرآیندی امن را طی کرده و به‌سرعت بازیابی شوند. [این] مقررات حداقلِ اقدامات یا نتایج مورد انتظار امنیت سایبری را تعریف می‌کنند، اما دولت حامی و مشوّق تلاش‌های افزون‌ترِ نهادهای مختلف برای فراتر رفتن از این الزامات نیز خواهد بود.

علاوه بر این، بخش‌های حیاتیِ مختلفِ جامعه به امنیت سایبری

1 Cybersecurity Performance Goals
2 Cybersecurity and Infrastructure Security Agency (CISA)
3 Framework for Improving Critical Infrastructure Cybersecurity
4 National Institute of Standards and Technology (NIST)
5 Secure-by-design principles

و تاب‌آوریِ شخصِ ثالثی که زیرساخت‌های خدماتِ آن‌ها را فراهم می‌کند، وابسته هستند. سرویس‌های مبتنی بر فضای ابری می‌توانند در ابعاد کلان امکان اقدامات بهتر و اقتصادی‌تر را در حوزه امنیت سایبری فراهم سازند، اما علاوه‌بر این برای تاب‌آوری عملیاتی در بسیاری از بخش‌های زیرساختیِ حیاتی نیز ضروری هستند. دولت این شکاف‌ها و گسست‌های [اختیارات] قانونی را شناسایی خواهد کرد تا بتواند اقدامات و تلاش‌های بهتری را برای امنیت سایبری در صنعت رایانش ابری و سایر خدمات ضروری شخص ثالث سامان داده و برای پوشاندنِ این گسست‌ها با [حوزه] صنعت، کنگره و [سایر] نهادهای تنظیم‌گر همکاری خواهد کرد.

هماهنگ‌سازی و عملیاتی‌کردن مقررات قدیمی و جدید

مقرراتِ مؤثر هزینه و بارِ [فرآیند] سازگارشدن را به حداقل رسانده و سازمان‌ها را قادر می‌سازد که منابع خود را برای افزایش تاب‌آوری و دفاع از سیستم‌ها و دارایی‌های خود صرف کنند. نهادهای تنظیم‌گر می‌توانند با استفاده از استانداردهای بین‌المللی موجود و در انطباق با خط‌مشی‌ها و قوانین جاری، بار [و زحمتِ] ملزوماتِ جدید را به حداقل رسانده و نیاز به هماهنگی تنظیم‌گری را کاهش دهند.

در مواردی که مقررات فدرال متضاد، تکراری یا بیش‌ازحد هزینه‌بر باشند، نهادهای تنظیم‌گر باید برای به‌حداقل‌رساندن این مسائل با یکدیگر همکاری کنند. ایالات متحده در صورت لزوم در سطح فرا-مرزی نیز اقدام به هماهنگ‌سازیِ تنظیم‌گری‌ها [ی خود] خواهد کرد تا از مانع‌تراشیِ ملزومات امنیت سایبری در جریان تجارت دیجیتال

پیشگیری کند. [نهادهای] تنظیم‌گر در صورت امکان باید نه‌تنها مقررات و قوانین، بلکه ارزیابی‌ها و ممیزی‌های نهادهای تحت نظارت را نیز با یکدیگر هماهنگ کنند. دفتر فرماندهی سایبری ملی[1] در همکاری با سازمان مدیریت و بودجه[2]، اقدامات دولت در زمینه هماهنگ‌سازی مقررات امنیت سایبری رهبری خواهد کرد. بعلاوه، شورای گزارش‌دهی حوادث سایبری[3] ضوابط گزارش‌دهیِ رویدادهای فدرال را هماهنگ و یکپارچه کرده و تناقضات احتمالیِ این فرآیند را برطرف می‌کند.

توانمندسازی مجموعه‌های تحت تنظیم‌گری در جهت تأمین امنیت [خود]

بخش‌های مختلفِ زیرساخت‌های حیاتی ظرفیت‌های متفاوتی برای جذب هزینه‌های امنیت سایبری دارند؛ از بخش‌های کم‌حاشیه - که بدون مداخله [دولت] نمی‌توانند به‌راحتی سرمایه‌گذاری [در حوزه امنیت سایبری] را افزایش دهند - گرفته تا بخش‌هایی که قادر به جذب هزینه‌های فرعیِ ارتقاء امنیت سایبری هستند. مقررات در برخی از بخش‌ها ممکن است برای ایجاد یک زمین بازیِ برابر ضروری باشد؛ تا شرکت‌ها در رقابتی با هم‌تایان خود برای صرفه‌جویی مالی در حوزه امنیت سایبری گرفتار نشوند. در بخش‌های دیگر، نهادهای تنظیم‌گر بیشتر به این سمت سوق پیدا می‌کنند که به روش‌های مختلف از تحقق سرمایه‌گذاری‌های لازم در حوزه امنیت سایبری اطمینان حاصل کنند؛ روش‌هایی از قبیل فرآیند نرخ‌گذاری، ساختارهای مالیاتی و سایر مکانیسم‌ها. در تنظیم الزامات جدید امنیت سایبری، به نهادهای

1 Office of the National Cyber Director (ONCD)
2 Office of Management and Budget (OMB)
3 Cyber Incident Reporting Council

تنظیم‌کننده‌ها توصیه می‌شود که برای درک نحوهٔ تأمین و تحقق این شرایط و الزامات، با نهادهای تحت تنظیم‌گری تعامل و مشورت داشته باشند. دولت برای دستیابی به یک مرجع تنظیم‌گریِ جدید، در همکاری با کنگره در پی طراحی چارچوب‌هایی برای تنظیم‌گری خواهد بود که منابع لازم برای عملیاتی‌کردنِ الزاماتِ تعیین‌شده را نیز در نظر بگیرند.

هدف راهبردی ۲ / ۱: گسترش همکاری بخش عمومی و بخش خصوصی

دفاع از زیرساخت‌های حیاتی در برابر فعالیت‌های متخاصمانه و سایر تهدیدها نیازمند مدلی از دفاع سایبری است که ساختار توزیع‌شده‌ای مشابه اینترنت داشته باشد. ما از طریق توسعه و تقویت همکاری بین نیروهای دفاعیِ مختلف به‌واسطهٔ [تقویت] نقش‌ها و مسئولیت‌های ساختارمند و افزایش ارتباط از طریق تبادل خودکارِ داده‌ها، اطلاعات و دانش، در پی تحقق این مدلِ شبکه‌ای و توزیع‌شده خواهیم بود. ترکیب همکاری سازمانی و پیوندهای مبتنی بر تکنولوژی، «شبکه‌ای متشکل از شبکه‌ها»ی مختلف ایجاد خواهد کرد که اعتمادمحور بوده و باعث شکل‌گیری آگاهی موقعیتی و اقدامات جمعی و هماهنگ در مدافعان سایبری و در نتیجه حفاظت از زیرساخت‌های حیاتی خواهد شد.

سازمان امنیت سایبری و زیرساخت (سیسا) هماهنگ‌کنندهٔ امنیت و تاب‌آوری زیرساخت‌های حیاتی در سطح ملی است. سیسا برای افزایش هماهنگی دولت فدرال با صاحبان و اپراتورهای زیرساخت‌های حیاتیِ سراسر ایالات متحده، این کار را در تعامل و هماهنگی با اداراتِ مدیریت

ریسک بخش‌محور[1] انجام می‌دهد. اداراتِ مدیریت ریسکِ بخش‌محور دارای مسئولیت‌های روزانه و تخصص‌های مختص به بخش خود هستند تا بتوانند امنیت و تاب‌آوری را در بخش‌های مربوطه بهبود بخشند. این ارگان‌ها نیز به نوبهٔ خود از مالکان و اپراتورهای [فعال در] بخش‌های مربوطه - که مسئول حفاظت از سیستم‌ها و دارایی‌های تحت کنترل خود هستند - پشتیبانی می‌کنند. [بعلاوه،] سازمان‌های اشتراک‌گذاری و تحلیل اطلاعات[2]، مراکز اشتراک‌گذاری و تحلیل اطلاعات متمرکز بر بخش[3] و سایر سازمان‌های مشابه، عملیات دفاع سایبری را در بخش‌های گسترده و پیچیده تسهیل می‌کنند.

دولت فدرال به افزایش هماهنگی بین سازمان سیسا و سایر ادارات مدیریت ریسک بخش‌محور ادامه خواهد داد و همچنان پیگیرِ این ادارات و فراهم کردن امکان پاسخگوییِ فعالانهٔ آن‌ها به نیازهای صاحبان و اپراتورهای زیرساخت‌های حیاتی در بخش‌های خود خواهد بود. دولت برای شناسایی نیازهای هر بخش و ارزیابی خلأهای موجود در توانمندی‌های ادارات مدیریت ریسک بخش‌محور، با فعالان حوزه صنعت همکاری خواهد کرد. سرمایه‌گذاری دولت فدرال برای ارتقاء توانمندی‌های ادارات مدیریت ریسک بخش‌محور باعث بهبود امنیت و تاب‌آوری در زیرساخت‌های حیاتی خواهد شد. این ادارات در تعامل با سیسا به ارتقاء توان خود برای فعالیت مؤثر و مفید برای نیازهای بخش خود می‌پردازند. ادارات مدیریت ریسک بخش‌محور همچنین باید به حمایت از بلوغ مکانیسم‌های همکاری با طرف‌های دیگر [شخص ثالث] ادامه دهند. دولت فدرال به پشتوانهٔ چند دهه تجربه همکاری با

1 Sector Risk Management Agencies (SRMAs)
2 Information sharing and analysis organizations (ISAOs)
3 sector-focused information sharing and analysis centers (ISACs)

مراکز اشتراک‌گذاری و تحلیل اطلاعات متمرکز بر بخش و سازمان‌های اشتراک‌گذاری و تحلیل اطلاعات، با این گروه‌ها و سایر گروه‌ها همکاری خواهد کرد تا به چشم‌انداز مشترکی در مورد چگونگی تکامل این مدل دست پیدا کنند.

تسریع در همکاری عملیاتی مستلزم استفاده از راه‌حل‌های تکنولوژیک برای اشتراک‌گذاری اطلاعات و هماهنگی تلاش‌های دفاعی است. ما باید تلاش‌های همکاری بین افراد را با اشتراک‌گذاری داده‌ها در میان رایانه‌ها و هماهنگ‌سازی امنیتی تکمیل کنیم. تحقق این مدل اشتراک‌گذاریِ بی‌درنگ، عملیاتی و چندوجهی برای واکنش سریع و مناسب به تهدیدات را ممکن می‌کند. سیسا و ادارات مدیریت ریسک بخش‌محور با مشارکت بخش خصوصی به‌دنبال مکانیسم‌های تکنیکی و سازمانیِ توسعه و تکامل [فرآیند] اشتراک‌گذاری داده در بین ماشین‌ها [= رایانه‌ها] خواهند بود. دولت فدرال همچنین همکاری عملیاتی و راهبردی خود را با ارائه‌دهندگان خدمات نرم‌افزاری، سخت‌افزاری و خدمات مدیریت‌شده‌ای[1] که توان تغییر چشم‌انداز سایبری در جهت افزایش امنیت و تاب‌آوری را دارند، تعمیق خواهد کرد.

هدف راهبردی ۳/۱: یکپارچه‌سازی مراکز امنیت سایبری فدرال

دولت فدرال باید حوزه اختیارات و قابلیت‌های بخش‌ها و سازمان‌هایی که مجموعاً مسئول تقویت دفاع از زیرساخت‌های حیاتی هستند را با یکدیگر هماهنگ کرده و انسجام بخشد.

1 managed service providers

مراکز فدرال امنیت سایبری به‌عنوان گلوگاه‌های به‌هم‌پیوسته‌ای عمل می‌کنند که قابلیت‌های کل دولت را در دستورکارهای دفاعی، قانونی، اطلاعاتی، دیپلماتیک، اقتصادی و نظامی با هم ترکیب می‌کنند. این مراکز در صورتی که به‌طور کامل منسجم و با یکدیگر هماهنگ شوند، باعث شکل‌گیری همکاری در درون دولت شده و آن را قادر می‌سازند تا حمایت مؤثر و قاطعی از شرکای غیرفدرال خود به عمل آورد.

دولت در مسیر دستیابی به این هدف به توفیقاتی دست پیدا کرده و توانسته است در سازمان سیسا طرح همکاری مشترک دفاع سایبری[1] را برای یکپارچه‌سازی برنامه‌ریزی و عملیات دفاع سایبری در سراسر دولت فدرال و همچنین بخش خصوصی و شرکای بین‌المللی تدوین کند. کاخ سفید همچنین اقدام به تقویت قابلیت‌های کارگروه مشترک تحقیقات سایبری ملی[2] نموده است تا قادر به ورود به عرصه فرآیندهای اجرای قوانین و سایر اقدامات مداخله‌گرانه باشد، و نیز نقش مرکز یکپارچه‌سازی اطلاعات تهدیدات سایبری[3] را برای یکپارچه‌سازی روندهای گردآوری اطلاعات، تجزیه و تحلیل‌ها، و مشارکت‌ها احیاء کرده است.

مدل‌های همکاری عملیاتی در ادارات مدیریت ریسک بخش‌محور - به‌عنوان مثال در مرکز تحلیل تهدیدات حوزه انرژی[4] در وزارت انرژی، مرکز تبادل اطلاعات پایگاه صنایع دفاعی[5] متعلق به وزارت دفاع، و نیز مرکز همکاری‌های امنیت سایبری[6] در سازمان امنیت ملی (اِن‌اس‌اِی)[7] - امکان‌هایی را برای اشتراک‌گذاری مستقیمِ اطلاعات به‌روز، عملی و

1 the Joint Cyber Defense Collaborative (JCDC)
2 the National Cyber Investigative Joint Task Force (NCIJTF)
3 Cyber Threat Intelligence Integration Center's (CTIIC)
4 Energy Threat Analysis Center (ETAC)
5 Defense Industrial Base Collaborative Information Sharing Environment (DCISE)
6 Cybersecurity Collaboration Center
7 National Security Agency (NSA)

مرتبط با شرکای بخش خصوصی در بخش‌های مربوطه فراهم می‌کند.

[اما هنوز] نیاز به تلاش بیشتری برای تقویت و یکپارچه‌سازی قابلیت‌های عملیاتی دولت فدرال و ارتقاء هماهنگی مراکز امنیت سایبری فدرال وجود دارد. دفتر فرماندهی سایبری ایالات متحده هدایت‌کنندهٔ تلاش‌های دولت در جهت هماهنگی مراکزی از این قبیل، شناسایی خلأهای موجود در قابلیت‌ها، و تدوین یک طرح اجرایی برای فراهم‌کردن امکان همکاری سریع و گسترده خواهد بود.

هدف راهبردی ۴/۱: به‌روز رسانی طرح‌ها و روال‌های فدرالِ واکنش به سوانح

بخش خصوصی بدون کمک مستقیم فدرال نیز قادر به کاهش بیشتر حوادث سایبری است. هنگامی که کمک فدرال مورد نیاز است، دولت باید پاسخی یکپارچه، هماهنگ و با همهٔ قوای خود ارائه دهد. سازمان‌هایی که هدف تهدیدات سایبری قرار می‌گیرند، باید بدانند دقیقاً با چه هدفی به کدام سازمان‌های دولتی تماس بگیرند. دولت فدرال باید راهنمای روشنی در مورد نحوه دسترسی بازیگران بخش خصوصی به آژانس‌های فدرال برای پشتیبانی در هنگام حوادث سایبری و انواع حمایت‌های دولتی ارائه دهد.

مطابق با خط‌مشی ابلاغی ریاست جمهوری شماره ۴۱ - «[شورای] هماهنگی سوانح سایبری ایالات متحده» که وزارت دادگستری[1]، وزارت امنیت داخلی[2] و دفتر مدیر ملی اطلاعات[3] را به‌عنوان رهبر تلاش‌های مربوط به تهدیدات، دارایی‌ها و اطلاعات [امنیتی] معرفی می‌کند

1 Department of Justice (DOJ)
2 Department of Homeland Security (DHS)
3 the Office of the Director of National Intelligence

-، سازمان سیسا پیگیرِ به‌روزرسانی طرح فرعیِ «واکنش ملی در برابر سوانح سایبری»[1] در جهت تقویت فرآیندها، رویه‌ها و سیستم‌ها است؛ تا خط‌مشی «تماس با یکی، فراخوانی برای همه است» در بالاترین سطحِ ممکن محقق شود. هر سازمان فدرال وقتی درخواستی برای کمکَ دریافت می‌کند، اولاً به مکانیسم‌های مؤثری برای اشتراک‌گذاری اطلاعات دسترسی داشته و ثانیاً دقیقاً می‌داند که دولت فدرال چه حمایت‌هایی می‌تواند ارائه دهد و چگونه باید با سازمان فدرال مناسبی که می‌تواند این حمایت‌ها را انجام دهند، تماس بگیرد و به مکانیسم‌های اشتراک‌گذاری اطلاعات مؤثر دسترسی داشته باشد. از آنجایی که اکثر واکنش‌های فدرال از طریق دفاتر میدانی انجام می‌شود، طرح فرعیِ «واکنش ملی در برابر سوانح سایبری» با به‌کارگیری تجربیات موفق کارگروه مشترک تروریسم، هماهنگی را در سطح محلی افزایش می‌دهد.

طرح گزارش‌دهی رویداد سایبری برای زیرساخت‌های حیاتی[2] ۲۰۲۲ آگاهی و توانایی ما را برای واکنش مؤثر در هنگام رخ دادن سوانح افزایش می‌دهد. این طرح از نهادهای تحت پوشش در بخش‌های زیرساختیِ حیاتی می‌خواهد که حوادث سایبری رخ‌داده را ظرف چند ساعت به سازمان سیسا گزارش دهند. اطلاع‌رسانیِ به‌موقع و اشتراک‌گذاری سریع اطلاعات مربوطه با وزارت دادگستری و سایر ذی‌نفعان واکنش به حوادث - که توسط سازمان سیسا انجام می‌شود -، باعث بهبود دفاع جمعی ما، ارتقاء تلاش‌ها برای شناسایی علل اصلی حوادث، و پخته‌تر و آگاهانه‌ترشدنِ تصمیم‌گیری‌های دولت در مورد نحوه واکنش می‌شود. سازمان سیسا در فرآیند عملیاتی‌کردن طرح گزارش‌دهی رویداد سایبری

1 National Cyber Incident Response Plan (NCIRP)
2 the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

برای زیرساخت‌های حیاتی ۲۰۲۲، برای یکپارچه‌سازی سیستم‌های گزارش‌دهی حادثه و اطمینان از اشتراک‌گذاری و اقدام بی‌درنگ براساس تمام اطلاعات مربوط به حادثه، با اداراتِ مدیریت ریسکِ بخش‌محور و وزارت دادگستری تعامل و مشورت خواهد کرد.

ما پس از حوادث بزرگ اطمینان حاصل خواهیم کرد که جامعه امنیت سایبری از درس‌های آموخته شده از طریق هیئت بررسی ایمنی سایبری[1] بهره خواهد برد. این هیئت که با فرمان ریاست‌جمهوری ۱۴۰۲۸ - «بهبود امنیت سایبری کشور» - تأسیس شده است، رهبران امنیت سایبری در بخش عمومی و بخش خصوصی را گرد هم می‌آورد تا حوادث سایبری مهم را بررسی و حقیقت‌یابی کرده و مولد بینشی باشند که اصلاحات [حوزه] صنعت را هدایت کند و توصیه‌هایی برای بهبود وضعیت ارائه دهد. دولت به‌دنبال همکاری با کنگره جهت تصویب طرح گزارش‌دهی رویداد سایبری برای زیرساخت‌های حیاتی ۲۰۲۲ در وزارت امنیت داخلی و فراهم‌کردن اختیاراتِ قانونیِ مورد نیازِ آن برای نظارت و بررسی جامع سوانح سایبری است.

هدف راهبردی ۱/۵: مدرن کردن دفاع فدرال

دولت فدرال برای انجام وظایف خود به اطلاعات، ارتباطات، تکنولوژی‌های عملیاتی و خدمات ایمن و تاب‌آور نیاز دارد. ازاین‌رو، دولت در نخستین ماه‌های فعالیت خود با انتشار فرمان اجرایی شماره ۱۴۰۲۸ - «بهبود امنیت سایبری کشور»، که به نوبهٔ خود منجر به انتشار بیانیهٔ امنیت ملی شماره ۸[2] با عنوان «بهبود امنیت سایبری سیستم‌های

1 Cyber Safety Review Board (CSRB)
2 National Security Memorandum No 8

امنیت ملی، وزارت دفاع و جامعهٔ اطلاعاتی» شد - و همچنین راهبرد فدرال جدید سازمان مدیریت و بودجه براساس معماریِ «اعتماد صفر»، جهت‌گیری راهبردی جدیدی را برای امنیت سایبری فدرال تعیین کرد.

دولت با استفاده از این فرصت تاریخی اقدامات بلندمدتی را برای دفاع از مجموعهٔ فدرال و مدرن‌سازی سیستم‌های فدرال مطابق با اصول اعتماد صفر انجام می‌دهد؛ اصولی که مبتنی بر این نگاه است که باید هم در داخل و هم خارج از مرزهای سنتیِ شبکه، با تهدیدات مقابله کرد. دولت فدرال با دفاع از شبکه‌های خود و تاب‌آور کردن آن‌ها، الگویی برای تقلید بخش خصوصی خواهد بود.

دفاع جمعی از سازمان‌های غیرنظامی فدرال

سازمان‌های فدرال غیرنظامی[1] مسئول مدرن و ایمن‌سازی تکنولوژی‌های اطلاعاتی و عملیاتیِ[2] خود هستند. خروجی‌های امنیت سایبری سازمان‌های فدرال غیرنظامی بخاطر تنوعی که در ساختارها، مأموریت‌ها، توانمندی‌ها و منابع مختلف آن‌ها وجود دارد، متنوع خواهد بود. ما باید به‌واسطهٔ مزایای رویکرد جمعی به مقولهٔ دفاع، به‌دنبال دستیابی به الگویی از امنیت سایبری باشیم که بین تک‌تک مقامات و توانمندی‌های سازمانی تعادل برقرار کند.

ما از طریق متمرکزکردن همهٔ اقدامات در سراسر سیستم فدرال، همچنان به دنبال افزایش انسجام [در سطح] فدرال خواهیم بود. سازمان مدیریت و بودجه - با هماهنگی سیسا - اقدام به تدوین طرح اقدامی برای ایمن‌سازی سیستم‌های سازمان‌های فدرال غیرنظامی از طریق دفاع

1 Federal civilian executive branch (FCEB)
2 Information Technology (IT) and Operational Technology (OT)

عملیاتی جمعی، دسترسی گسترده به خدمات مشترک متمرکز، و کاهش ریسک زنجیره تأمین نرم افزار خواهد کرد. این تلاش‌ها مسیر برنامه‌های قبلی را ادامه داده و اقداماتی را در اولویت قرار خواهد داد که رویکرد جامعی به کل دولت را برای دفاع از سیستم‌های اطلاعاتی سازمان‌های فدرال غیرنظامی در پیش گیرد. برنامهٔ «کاهش ریسک زنجیره تأمین نرم‌افزار» - که با هماهنگی سازمان ملی استاندارد و تکنولوژی تدوین شده است - مسیر فرمان اجرایی ۱۴۰۲۸ - «ارتقاء امنیت سایبری کشور» - را ادامه خواهد داد و مواردی از قبیل ایدهٔ «صورت‌حساب مواد [اولیهٔ] نرم‌افزار [ها][1]، چارچوب توسعه نرم‌افزار امن سازمان ملی استانداردها و تکنولوژی[2]، و سایر تلاش‌های ناظر به بهبود امنیت نرم‌افزارهای منبع‌باز را در بر می‌گیرد.

مدرن‌سازی سیستم‌های فدرال

دولت فدرال باید در پی مدرن‌سازی یا جایگزینیِ آن دسته از سیستم‌های تکنولوژی‌های ارتباطی و عملیاتی‌ای باشد که در برابر تهدیدات سایبری پیچیده قابل دفاع نیستند. دستورالعمل راهبرد معماری اعتماد صفر سازمان مدیریت و بودجه برای سازمان‌های فدرال غیرنظامی این است که احراز هویت چند-مرحله‌ای را اجرا کرده، داده‌های خود را رمزگذاری کنند، نسبت به جنبه‌هایی [از سازمان خود] که ممکن است در معرض حمله قرار بگیرد اشراف پیدا کنند، مجوزها و دسترسی‌ها را مدیریت کنند، و از ابزارهای امنیتی [مبتنی بر فضای] ابری استفاده کنند. اینگونه دستورالعمل‌های امنیت سایبری تنها در صورت مدرن‌سازی تکنولوژی‌های اطلاعاتی و عملیاتیِ سیستم‌های فدرال و استفادهٔ آن‌ها

1 Software Bills of Material (SBOM)
2 NIST's Secure Software Development Framework

از تکنولوژی‌های امنیتیِ خاص قابل تحقق هستند. سازمان مدیریت و بودجه یک چرخهٔ چند ساله برای سرعت بخشیدن به نوسازی تکنولوژی سازمان‌های فدرال غیرنظامی را تدوین خواهد کرد. اولویت این طرح برای عمدهٔ تلاش‌های فدرال، حذف سیستم‌های قدیمی است که نگهداری آن‌ها پرهزینه و دفاع از آن‌ها دشوار است. این طرح نقاط عطفی را جستجو می‌کند که همهٔ سیستم‌های قدیمی – که قادر به پیاده‌سازی راهبرد معماری اعتماد صفر در طی یک دهه نیستند - را حذف کرده و یا در مورد سیستم‌هایی که در این افقِ زمانی قابل جایگزینی نیستند، تهدیدات معطوف به آن‌ها را کاهش دهد. جایگزینی سیستم‌های قدیمی با تکنولوژی ایمن‌تر - به‌عنوان مثال از طریق تسریع انتقال به خدمات ابری - سطح امنیت سایبری را در سراسر دولت فدرال ارتقا داده و به نوبهٔ خود، امنیت و تاب‌آوری خدمات دیجیتالی را - که به مردم آمریکا ارائه می‌شود - بهبود می‌بخشد.

دفاع از سیستم‌های امنیت ملی

سیستم‌های امنیت ملی[1] برخی از حساس‌ترین داده‌های دولت فدرال را ذخیره و پردازش می‌کنند و باید در برابر طیف وسیعی از تهدیدات سایبری و فیزیکی - از جمله تهدیدات داخلی، مجرمان سایبری، و پیچیده‌ترین دشمنان دولت‌های ملی - ایمن شوند. مدیر سازمان امنیت ملی (اِن‌اس‌اِی)- به‌عنوان مدیر سیستم‌های امنیت ملی - [موظف است] در هماهنگی با سازمان مدیریت و بودجه، طرحی برای اجرای الزامات امنیت سایبری پیشرفته - مندرج در بیانیه شماره ۸ امنیت ملی[2] - در سازمان‌های فدرال غیرنظامی تدوین کند.

1 National security systems (NSS)
2 National Security Memorandum (NSM), Number 8

رکن دوم:
مقابله با عوامل تهدید

رکن دوم: مقابله با عوامل تهدید

ایالات متحده از تمام ابزارهای قدرت ملی خود برای مقابله‌به‌مثل در برابر عوامل تهدید - که منافع ملی ما را هدف قرار می‌دهند - و از بین بردن آن‌ها استفاده خواهد کرد. این تلاش‌ها ممکن است از انواع قابلیت‌های دیپلماتیک، اطلاعاتی، نظامی (هم فیزیکی و هم سایبری)، مالی، اطلاعاتی و قابلیت‌های اجراییِ قانون بهره بگیرد. هدف ما این است توان اجرای کارزارهای پایدار سایبری که امنیت ملی یا امنیت عمومی ایالات متحده را تهدید می‌کنند را از عوامل متخاصم سلب کنیم.

تلاش‌های هماهنگ نهادهای فدرال و غیرفدرال در خنثی‌کردن فعالیت‌های متخاصمانه سایبری دولت‌های خارجی، بزه‌کاران و سایر عوامل تهدید مؤثر بوده است. دولت فدرال قابلیت‌های خود را برای واکنش به حوادث سایبری افزایش داده و اقداماتی از قبیل پیگرد و دستگیری مجرمان سایبری فراملی و بازیگران تحت حمایت دولت، تحریم عوامل متخاصم سایبری - از جمله ممنوعیت سفر و ممانعت از دسترسی به ارائه دهندگان خدمات مالی -، و ممانعت از دسترسی عوامل متخاصم به زیرساخت‌های دیجیتال و شبکه‌ها [در معرض تهدید] را در دستور کار خود قرار داده است. قوهٔ مجریه همچنین توانسته است زیرساخت‌های مالی مورد استفاده برای فعالیت‌های غیرقانونی را هدف قرار داده و میلیاردها دلار از دارایی‌های غیرقانونی را بازیابی کند. بعلاوه،

ابتکارات دیپلماتیک جدیدی برای ریشه‌یابی فعالیت‌های سایبری متخاصمانه و مخرب یا بی‌ثبات‌کننده و پیگرد عوامل آن‌ها توسط دولت طراحی شده است.

دولت ما مسیر کنونی را برای وارد آوردن ضربات مؤثر و پایدارتر به دشمنان ادامه خواهد داد. تلاش‌های ما مستلزم همکاری بیشتر شرکای بخش دولتی و خصوصی برای بهبود اشتراک‌گذاری اطلاعات، گسترش کارزارهای مختل‌سازی [دشمنان]، ممانعت از استفادهٔ عوامل متخاصم از زیرساخت‌های مستقر در ایالات متحده و خنثی‌کردن کارزارهای باج‌افزار جهانی است.

هدف راهبردی ۱ / ۲: یکپارچه کردن فعالیت‌های تهاجمی و مختل‌سازیِ فدرال

کارزارهای مختل‌سازی باید چنان پایدار و هدفمند شوند که بتوانند هزینهٔ فعالیت‌های سایبری مجرمانه را بالا ببرند و باعث شوند عوامل تهدیدگر - که بعضاً تحت حمایت دولت‌های خارجی اقدام به فعالیت‌های سایبری متخاصمانه می‌کنند - دیگر آن را وسیله‌ای مؤثر برای دستیابی به اهداف خود نبینند. وزارت دادگستری و سایر سازمان‌های فدرالِ مجری قانون در استقرار یکپارچه مقامات قانونی داخلی در کنار بخش خصوصیِ صنعت و متحدان و شرکای بین‌المللی در تلاش برای مختل‌سازی زیرساخت‌ها و منابع بزه‌کاری‌های آنلاین پیشگام بوده‌اند، و اقداماتی از قبیل حذف باتنت‌های مشکوک و توقیف ارزهای دیجیتالِ حاصل از باج‌افزارها و کلاهبرداری [های آنلاین] را در دستور کار خود قرار داده‌اند. اطلاعات به دست آمده از این تحقیقات، امکان

اقدامات دیگری همچون اطلاع‌رسانی به قربانیان، انتشار توصیه‌های امنیت سایبری، اقدامات بخش خصوصی، تعیین تحریم‌ها، اقدامات دیپلماتیک و عملیات اطلاعاتی را فراهم می‌کند.

رویکرد راهبردی وزارت دفاع در مورد دفاع تهاجمی به شناخت عوامل تهدیدگر، شناسایی و افشای بدافزارها، و اختلال در فعالیت‌های مخرب قبل از اصابت به هدف، کمک کرده است. وزارت دفاع با بهره‌گیری از تجربیات گذشته و [شناختِ] محیط تهدیدِ دگرگون‌شونده، راهبرد سایبریِ به‌روز و بخش‌محوری را در هماهنگی با راهبرد امنیت ملی[1]، راهبرد دفاع ملی[2] و این راهبرد امنیت سایبری ملی تدوین خواهد کرد. راهبرد جدید وزارت دفاع این نکته را تصریح خواهد کرد که فرماندهی سایبری ایالات متحده و سایر اجزای وزارت دفاع، عملیات فضای سایبری را به مجموعه تلاش‌های خود برای دفاع در برابر بازیگران دولتی و غیر دولتی - که در سطح راهبردی قادر به ایجاد تهدید برای آمریکا هستند - اضافه خواهند کرد، و درعین‌حال به همکاری و هماهنگی با عملیات بخش غیرنظامی، قوای مجریِ قانون، و نهادهای اطلاعاتی برای مختل‌کردن فعالیت‌های بزه‌کارانه در گسترهٔ وسیع ادامه خواهد داد.

دولت فدرال باید برای افزایش گستره و سرعت این کارزارهای یکپارچهٔ مختل‌سازی، پلتفرم‌های تکنولوژی و سازمانی را - که عملیات پیوسته و هماهنگ را ممکن می‌سازند - توسعه دهد. کارگروه مشترک تحقیقات سایبری ملی - به‌عنوان یک نقطه کانونی و بین‌سازمانی برای هماهنگی کارزارهای مختل‌سازی در کل دولت - ظرفیت خود را برای هماهنگی کارزارهای حذف و مختل‌سازی با سرعت، مقیاس و فرکانس

1 National Security Strategy
2 National Defense Strategy

بیشتر گسترش خواهد داد. به طور مشابه، وزارت دفاع و نهادهای اطلاعاتی متعهد هستند که همهٔ اختیارات قانونی خود را برای کارزارهای مختل‌سازی به کار بگیرند.

هدف راهبردی ۲ / ۲: تقویت همکاری عملیاتی بخش عمومی و بخش خصوصی برای ضربه‌زدن به دشمنان

درک و دریافت بخش خصوصی نسبت به فعالیت‌های خصمانه روزبه‌روز در حال پیشرفت بوده و گستردگی و جزئیاتِ آن بسیار فراتر از درکی است که در دولت فدرال وجود دارد. دلیل این مسئله از یک طرف ابعاد گستردهٔ بخش خصوصی و عملیات‌های آن در مقابله با تهدیدات، و از طرف دیگر سرعت بالای نوآوری در ابزارها و توانمندی‌های آن است. مختل‌سازی مؤثرِ فعالیت‌های سایبری متخاصمانه مستلزم همکاری بیش از پیش بین نهادهای بخش خصوصی - که دارای بینش و قابلیت‌های منحصربه‌فرد هستند - و سازمان‌های فدرال - که ابزار و اختیارات لازم برای اقدام را در اختیار دارند - است. حذف باتنت اِموتِت[1] در سال ۲۰۲۱ و مشارکت سازمان‌های فدرال، متحدین و شرکای بین‌المللی، و صنایع بخش خصوصی در آن، پتانسیل این رویکرد مشترک را نشان داد. با توجه به علاقه جامعه امنیت سایبری و صاحبان و اپراتورهای زیرساخت‌های دیجیتال برای ادامه این رویکرد، ما باید این مدل را حفظ کرده و گسترش دهیم تا عملیات مختل‌سازی مشترک به طور مداوم انجام شود.

مجموعه‌های بخش خصوصی تشویق می‌شوند که گرد هم جمع شده و تلاش‌های خود را از طریق یک یا چند سازمان غیرانتفاعی - مانند

1 Emotet

اتحاد ملی سایبری قانونی و آموزش[1] - سازماندهی کنند؛ سازمان‌هایی که می‌توانند به‌عنوان مرکز همکاری عملیاتی با دولت فدرال عمل کنند. همکاری‌های معطوف به تهدید باید به شکل هسته‌های عملیاتیِ چابک و موقتی باشد که از تعداد کمی اپراتور قابل اعتماد تشکیل شده‌اند که توسط یک مرکز میزبانی و پشتیبانی می‌شوند. با استفاده اعضای این حلقه با استفاده از پلتفرم‌های تعامل مجازی، اطلاعات را بین هم تبادل کرده و به‌سرعت برای مختل‌سازی عوامل تهدید وارد عمل می‌شوند. دولت فدرال نیز تلاش می‌کند که با بیشترین سرعت، موانعِ حمایت و استفاده از این مدل همکاری - از جمله الزامات امنیتی و خط‌مشی مدیریت سوابق - را از سر راه بردارد.

هدف راهبردی ۳/۲: افزایش سرعت و مقیاس اشتراک‌گذاری اطلاعات و هشدار به قربانیان

اشتراک‌گذاری به موقع اطلاعات مربوط به تهدیدات در بین بازیگران فدرال و غیر فدرال، باعث تسهیل و تسریع تلاش‌های مشترک برای حمله به دشمنان و مختل‌کردن آن‌ها می‌شود. اگرچه اطلاعات امنیت سایبری منبع-باز و ارائه‌دهندگان خصوصیِ اطلاعات باعث افزایش چشم‌گیرِ آگاهی جمعی نسبت به تهدیدات سایبری شده است، اما اطلاعات ملی که فقط دولت قادر به حصول آن‌هاست، همچنان بسیار ارزشمند است. به‌عنوان مثال، تعامل اطلاعاتی مرکز همکاری‌های امنیت سایبریِ سازمان امنیت ملی (اِن‌اس‌اِی) با صنعت در مختل‌سازی فعالیت‌های دشمن که پایگاه صنایع دفاعی را هدف قرار می‌دهد، بسیار مؤثر بوده

1 National Cyber-Forensics and Training Alliance (NCFTA)

است. به‌همین‌سان، سازمان سیسا با کمک طرح همکاری مشترک دفاع سایبری امکان اشتراک‌گذاری مداوم و چند جهته اطلاعات تهدید با بخش خصوصی را فراهم کرده و با هماهنگی اف‌بی‌آی، از این اطلاعات برای تسریع اطلاع‌رسانی [به] قربانیان و کاهش تأثیر نفوذهای شناسایی‌شده استفاده می‌کند.

دولت فدرال سرعت و مقیاس اشتراک‌گذاری اطلاعات مربوط به تهدیدات سایبری را افزایش می‌دهد تا وقتی به اطلاعاتی دست پیدا می‌کند که حاکی از تهدید یا نفوذ به یک سازمان باشند، قادر باشد که فعالانه به مدافعان سایبری و قربانیان هشدارهای لازم را ابلاغ کند. اداراتِ مدیریت ریسک بخش‌محور با هماهنگی مرکز سیسا، سازمان‌های مجری قانون و مرکز یکپارچه سازی اطلاعات تهدیدات سایبری، نیازها و اولویت‌های اطلاعاتی را در بخش خود شناسایی کرده و فرآیندهایی را برای به‌اشتراک‌گذاشتن هشدارها، شاخص‌های فنی، زمینه [های] تهدید و سایر اطلاعات مرتبط با شرکای دولتی و غیردولتی طراحی خواهند کرد. این فرآیندها باید مکانیسم‌هایی را برای بخش خصوصی فراهم کند تا بازخورد به موقع و اطلاعات تهدیدات خود را به دولت فدرال ارائه دهد تا هدف قرار دادن تهدیدات سایبری برای ایجاد اختلال و جمع آوری اطلاعات بیشتر را بهبود بخشد. دولت فدرال همچنین سیاست‌ها و فرآیندهای طبقه‌بندی را بررسی خواهد کرد تا شرایط گسترش دسترسی به داده‌های طبقه‌بندی‌شده و گسترش مجوزها برای ارائه اطلاعات حساس به مالکان و اپراتورهای زیرساخت‌های حیاتی ضروری را فراهم کند.

همه ارائه‌دهندگان خدمات باید اقدامات متناسبی برای ایمن‌سازی استفاده از زیرساخت‌های خود در برابر سوءاستفاده یا سایر اقدامات مجرمانه انجام دهند. اولویت قوهٔ مجریه این است که رویکردی

ریسک‌محور در مورد امنیت سایبریِ همهٔ ارائه‌دهندگان خدمات زیرساخت اتخاذ کند که - به کمک قوانین و مصوباتی نظیر فرمان اجرایی شماره ۱۳۹۸۴ (با عنوان «اقدامات تکمیلی برای رسیدگی به موقعیت‌های اضطراریِ ملی، با نظر به اقدامات متخاصمانهٔ سایبری برجسته») - که به روش‌ها و شاخصه‌های شناخته‌شدهٔ فعالیت‌های متخاصمانه رسیدگی کند. اجرای این فرمان سوءاستفاده از زیرساخت‌های مستقر در ایالات متحده را برای دشمنان دشوارتر کرده و هم‌زمان از حریم خصوصی افراد نیز حراست خواهد کرد.

هدف راهبردی ۴ / ۲: جلوگیری از سوءاستفاده از زیرساخت‌های مستقر در خاک ایالات متحده

بازیگران سایبری متخاصم از زیرساخت‌های ابری مستقر در ایالات متحده، ثبت‌کننده‌های دامنه‌های اینترنتی، ارائه‌دهندگان خدمات هاست[1] و ایمیل، و سایر خدمات دیجیتال برای انجام فعالیت‌های مجرمانه، عملیات تأثیرگذاری و جاسوسی از افراد، کسب‌وکارها، سازمان‌ها و حتی خود حکومت در ایالات متحده و سایر کشورها سوءاستفاده می‌کنند. این خدمات معمولاً به‌واسطهٔ فروشندگان خارجی ارائه می‌شود و این فروشندگان فاصلهٔ زیادی از شرکت‌های ارائه‌دهندهٔ خدمات در داخل خاک آمریکا دارند [و قابل ردیابی نیستند] و این امر باعث می‌شود که این ارائه‌دهندگان قادر به رسیدگی به شکایت‌های مربوط به سوءاستفاده و نیز پاسخگویی به روال‌های قانونیِ ایالات متحده نباشند. دولت فدرال با سرویس‌های ابری و سایر ارائه‌دهندگان خدمات زیرساختیِ اینترنتی

1 Host

همکاری خواهد کرد تا بتواند سوءاستفاده از زیرساخت‌های داخل آمریکا را شناسایی کرده، این سوءاستفاده‌ها را به دولت‌ها[ی ایالتی] گزارش کند، امکان گزارش‌دهی در مورد اینگونه سوءاستفاده‌ها را برای خود قربانیان [که در اینجا همان ارائه‌دهندگانِ خدمات می‌باشند] فراهم کند، و نفوذ به این زیرساخت‌ها و سوءاستفاده از آن‌ها را برای عوامل بزه‌کار و تهدیدگر دشوارتر کند.

همه ارائه‌دهندگان خدمات باید تلاش کافی برای ایمن‌سازی زیرساخت‌های خود در برابر سوءاستفاده یا سایر رفتارهای مجرمانه انجام دهند. دولت به دنبال این خواهد بود که رویکردی ریسک‌محور به امنیت سایبری را در میان ارائه‌دهندگانِ زیرساخت - به‌مثابهٔ - خدمت ترویج کند. این رویکرد به شیوه‌های مختلفی - از جمله با عملیاتی کردنِ فرمان اجراییِ ۱۳۹۸٤ تحت عنوان «گام‌های بیشتری برای رسیدگی به فوریت‌های ملی، با نظر به فعالیت‌های مجرمانهٔ سایبریِ شاخص» -، به مقابله با روش‌ها و شاخصه‌های شناخته‌شدهٔ فعالیت‌های مجرمانه می‌پردازد. اجرای این فرمان باعث خواهد شد که سوءاستفاده از زیرساخت‌های داخل خاک آمریکا برای دشمنان دشوارتر شده و همچنین امنیتِ حریم خصوصیِ افراد افزایش پیدا کند.

هدف راهبردی ۲/۵: مقابله با جرائم سایبری و باج‌افزارها

باج‌افزارها تهدیدی برای امنیت ملی، اعتماد عمومی و رفاه اقتصادی هستند و به اهداف مختلفی از جمله بیمارستان‌ها، مدارس، خطوط لوله، خدمات دولتی و سایر زیرساخت‌های حیاتی و خدمات ضروری حمله می‌کنند. اکثر باج‌افزارهایی که از پایگاه‌های امنی مانند روسیه، ایران و

کره شمالی فعالیت می‌کنند، از نقاط ضعف امنیت سایبری برای به دست گرفتن کنترل شبکه‌های مورد حمله استفاده کرده و از ارزهای دیجیتال برای اخاذی و پولشویی درآمدهای خود بهره می‌گیرند.

با توجه به تأثیر باج‌افزارها بر خدمات زیرساختی حیاتی، ایالات متحده در چهار محور از تمام عناصر قدرت ملی برای مقابله با این تهدید استفاده خواهد کرد: (۱) استفاده از همکاری بین‌المللی برای برهم زدن اکوسیستم باج‌افزار و منزوی کردن کشورهایی که پناهگاه‌های امنی برای مجرمان فراهم می‌کنند؛ (۲) بررسی جرائم باج‌افزاری و استفاده از اختیارات قانون و سایر قابلیت‌ها برای مختل‌کردن زیرساخت‌ها و عوامل باج‌افزاری؛ (۳) تقویت تاب‌آوری زیرساخت‌های حیاتی برای مقاومت در برابر حملات باج‌افزاری؛ و (۴) مبارزه با سوءاستفاده از ارزهای دیجیتال برای انواع اخاذی.

از آن‌جا که باج‌افزارها چالشی فرا - مرزی بوده و [مقابله با آن‌ها] نیاز به همکاری در سطح بین‌المللی دارد، کاخ سفید با مشارکت بیش از ۳۰ کشور طرح مقابله با باج‌افزارها[1] را تدوین کرده است. این طرح اقداماتی جهانی برای ایجاد تاب‌آوری تدوین کرده و از ژانویه ۲۰۲۳، یک کارگروه بین‌المللی مقابله با باج‌افزار را به رهبری استرالیا راه‌اندازی کرده است تا اطلاعات مربوط به بازیگران و زیرساخت‌های [مورد استفاده در] حملات باج‌افزاری را به اشتراک بگذارد. این کار باعث تقویت و تسریع اقدامات دفاعیِ مختل‌کننده - و اغلب هماهنگِ - کشورهای عضو این طرح خواهد شد. طرح مقابله با باج‌افزارها همچنین هماهنگی سیاست‌ها و تلاش‌های دیپلماتیک را در بین اعضای خود ارتقاء خواهد داد.

1 Counter-Ransomware Initiative (CRI)

دولت متعهد به اجرای کارزارهای مختل‌سازی و سایر اقدامات به‌نحوی پایدار، هماهنگ و هدفمند است تا بتواند هزینهٔ فعالیت‌های باج‌افزاری را بالا برده و آن را از سودآوری دور کند. کارگروه مشترک باج‌افزار[1] - به ریاست مشترک سازمان سیسا و اف‌بی‌آی - تلاش‌های بین‌سازمانیِ فعلی برای مختل‌کردنِ عملیات‌های باج‌افزارانه را یکپارچه و منسجم کرده و از تلاش‌های بخش خصوصی و عوامل ملی، محلی، قبیله‌ای و منطقه‌ای در جهت افزایش محافظت‌های خود در برابر باج‌افزارها حمایت خواهد کرد.

یکی دیگر از ابعاد رویکرد ما، مبارزه با صرافی‌های غیرقانونیِ ارزهای دیجیتال - که اپراتورهای باج‌افزارها به آن متکی هستند - و ارتقاء اجرای استانداردهای بین‌المللی برای مبارزه با تأمین مالی غیرقانونیِ دارایی‌های مجازی است. ایالات متحده مؤسسات مالی ارائه‌دهنده خدمات مخفیانه در [حوزه] ارزهای دیجیتال را تحت بررسی [قوانین] مبارزه با پولشویی[2] و مقابله با تأمین مالی تروریسم[3] قرار می‌دهد و وزارت خزانه‌داری، سرویس مخفی، وزارت دادگستری، اف‌بی‌آی و شرکای بخش خصوصی نیز برای ردیابی و جلوگیری از پرداخت‌های باج‌افزاری همکاری می‌کنند. طرح مبارزه با باج‌افزارها اعضای خود را متعهد به [رعایت] استانداردهای مقابله با پولشویی و مقابله با تأمین مالی تروریسم - از جمله قواعد «شناخت مشتری»[4] - نموده است تا کار عوامل باج‌افزاری را برای پولشوییِ درآمدهای [حاصل از] ارزهای دیجیتالِ خود را دشوارتر کند. در بلندمدت، ایالات متحده از اجرای استانداردهای بین‌المللی مبارزه با پولشویی و مقابله با تأمین مالی تروریسم در سطح جهانی

1 Joint Ransomware Task Force (JRTF)
2 Anti-Money Laundering (AML)
3 Countering the Financing of Terrorism (CFT)
4 know-your-customer (KYC) rules

برای کاهش استفاده از ارزهای دیجیتال برای فعالیت‌های غیرقانونی که منافع ملی ما را تضعیف می‌کند، به‌عنوان بخشی از تلاش‌های معطوف به فرمان اجرایی شماره ۱۴۰۶۷ - «تضمین توسعه مسئولانه دارایی‌های دیجیتال» - حمایت خواهد کرد.

در نهایت، مؤثرترین راه برای کاهش انگیزهٔ این گروه‌های بزه‌کار، به حداقل رساندنِ حاشیهٔ سود آن‌ها است. به همین دلیل، دولت به شدت با پرداخت باج مبارزه خواهد کرد. علاوه بر این، قربانیان باج‌افزار – چه تصمیم به پرداخت باج بگیرند یا نه – باید این حادثه را به مجری قانون و سایر سازمان‌های مربوطه گزارش دهند. این گزارش‌ها توانایی دولت فدرال برای پشتیبانی از قربانیان، جلوگیری از افزایش استفاده از ارزهای دیجیتال برای فرار از قوانین مبارزه با پولشویی[1] و مقابله با تأمین مالی تروریسم، و کاهش میزان موفقیت حملات باج‌افزاری در آینده را افزایش می‌دهد.

1 Anti-Money Laundering (AML)

رکن سوم:

شکل دهی به نیروهای بازار برای ایجاد امنیت و تاب آوری

رکن سوم: شکل‌دهی به نیروهای بازار برای ایجاد امنیت و تاب‌آوری

برای ساختن آیندهٔ امن و تاب‌آوری که در پی آن هستیم، باید نیروهای بازار را به‌نحوی شکل دهیم که مسئولیت بر عهده کسانی قرار بگیرد که در اکوسیستم دیجیتال ما بهترین امکان‌ها را برای کاهش ریسک دارند. ما اکوسیستم دیجیتالِ قابل‌اعتمادی خواهیم ساخت و تبعات ضعف در امنیت سایبری را از افراد آسیب‌پذیر دور خواهیم کرد. در این تلاش، نقش بازار را جایگزین یا کمرنگ نخواهیم کرد، بلکه نیروهای بازار را به صورت مولد در جهت حفظ امنیت و تاب‌آوری کشورمان هدایت می‌کنیم. هدف ما یک اقتصاد دیجیتال مدرن است که اقداماتی را ترویج می‌کند که در عین حفظ رقابت و نوآوری، امنیت و تاب‌آوری اکوسیستم دیجیتال ما را افزایش می‌دهد.

استمرار اختلالات در زیرساخت‌های حیاتی و سرقت داده‌های شخصی نشان می‌دهد که نیروهای بازار به تنهایی قادر به عملیاتی‌کردن ابعاد و جوانب مهم امنیت سایبری و تاب‌آوری نبوده‌اند. در بسیاری از موارد، سازمان‌هایی که بر روی امنیت سایبری سرمایه‌گذاری نمی‌کنند، به‌طور منفی و غیرمنصفانه‌ای بر روی سازمان‌هایی که این سرمایه‌گذاری‌ها و تلاش‌ها را انجام می‌دهند تأثیر می‌گذارند و معمولاً کسب‌وکارهای کوچک و آسیب‌پذیرترین اجتماعات کشور ما را تحت‌الشعاع قرار می‌دهند. اگرچه نیروهای بازار همچنان اولین و بهترین

مسیر برای نوآوریِ چابک و مؤثر هستند، اما نتوانسته‌اند به اندازه کافی صنعت را برای اولویت دادن به منافع اصلی اقتصادی و امنیت ملی ما بسیج کنند.

دولت برای رسیدگی به این چالش‌ها، امنیت و تاب‌آوری بلندمدت اکوسیستم دیجیتال در برابر تهدیدات امروز و چالش‌های فردا را تقویت خواهد کرد. ما باید مسئولیت حفاظت از داده‌های شخصی را بر عهدهٔ متصدیان و متولیان داده‌ها بدانیم؛ دستگاه‌های آنلاینِ امن‌تری را طراحی کنیم؛ و قوانین را به‌نحوی اصلاح کنیم تا مسئولیت ازدست‌رفتن داده‌ها و آسیب‌های ناشی از خطاهای امنیت سایبری، آسیب‌پذیری‌های نرم افزاری و سایر خطرات ایجاد شده توسط نرم افزارها و تکنولوژی‌های دیجیتال را پوشش دهند. ما از قدرت خرید فدرال و کمک‌های مالی در جهت ایجاد انگیزه برای پیشرفت امنیت [سایبری] استفاده کرده و بررسی خواهیم کرد که چگونه دولت می‌تواند بازارهای بیمه را در برابر خطرات فاجعه‌بار تثبیت کند تا اقدامات امنیت سایبری بهتری را هدایت کند و در صورت وقوع حوادث فاجعه بار، اطمینان بازار را فراهم کند.

هدف راهبردی ۱ / ۳: ایجاد و تقویت پاسخ‌گویی در مقاماتِ مسئول در حوزهٔ داده

ایمن‌سازی داده‌های شخصی یک جنبه اساسی برای حفاظت از حریم خصوصی مشتریان در آیندهٔ دیجیتال است. تکنولوژی‌های مبتنی بر داده، اقتصاد ما را متحول کرده و سطح بی‌سابقه‌ای از رفاه را برای مصرف‌کننده فراهم کرده‌اند. اما گسترش چشم‌گیر اطلاعات شخصی، محیط تهدید را گسترش می‌دهد و تأثیر حمله به داده‌ها را بر

مصرف‌کنندگان افزایش می‌دهد. وقتی سازمان‌ها نمی‌توانند از داده‌هایی که از افراد دارند محافظت کنند، هزینهٔ این آسیب‌پذیری متوجهِ تک‌تک مردم آمریکا خواهد شد. معمولاً بیشترین هزینه متوجه جمعیت‌های آسیب‌پذیری می‌شود که هدف‌قرارگرفتن داده‌های شخصی، آسیب‌های شدیدی به آن‌ها وارد می‌آورد.

دولت از تلاش‌های قانونی برای اعمال محدودیت‌های صریح و سخت‌گیرانه بر جمع‌آوری، استفاده، انتقال و نگهداری داده‌های شخصی [دیگران] و اجرای پروتکل‌های حفاظتی شدید برای داده‌های حساس - از جمله موقعیت جغرافیایی و اطلاعات سلامتی - حمایت می‌کند. علاوه‌براین، قانون‌گذار می‌بایست الزامات ملی برای امنیت داده‌های شخصی را مطابق با استانداردها و دستورالعمل‌های طراحی‌شده توسط مؤسسه ملی استانداردها و تکنولوژی تعیین کند. با طراحی ضوابط حفاظت از حریم خصوصی - که متناسب با تهدیدها [ی جدید] تکامل می‌یابد -، ایالات متحده می‌تواند راه خود را برای دستیابی به آینده‌ای امن‌تر هموار کند.

هدف راهبردی ۲ / ۳: توسعه دستگاه‌های امن [در حوزهٔ] اینترنت اشیاء

دستگاه‌های اینترنت اشیاء - از کالاهای مصرفی مانند ردیاب‌های تناسب اندام و مانیتورهای کودک گرفته تا سیستم‌های کنترل صنعتی و سنسورها - منابع جدیدی از اتصال را در خانه‌ها و مشاغل ما تشکیل می‌دهند. با این حال، بسیاری از دستگاه‌های اینترنت اشیاء که امروزه در زندگی انسان وارد شده، به اندازه کافی در برابر تهدیدات امنیت سایبری

محافظت نمی‌شوند. اغلب آن‌ها با تنظیمات پیش‌فرض و ناکافی استفاده می‌شوند، پَچ‌کردن و یا ارتقاء آن‌ها دشوار یا غیرممکن است، و یا [در برخی موارد] مجهز به قابلیت‌های پیشرفته و غیرضروری‌ای هستند که فعالیت‌های سایبری متخاصمانه را در سیستم‌های فیزیکی و دیجیتالی حیاتی ممکن می‌سازد. آسیب‌پذیری‌های اخیر اینترنت اشیاء نشان داده است که عوامل متخاصم به‌راحتی می‌توانند از این دستگاه‌ها برای ساخت بات‌نت‌ها و جاسوسی و نظارت استفاده کنند.

دولت [فعالیت‌های حوزهٔ] تحقیق و توسعه فدرال و همچنین امکانات و تلاش‌های مربوط به مدیریت ریسک - آنطور که در قانون بهبود امنیت سایبری اینترنت اشیاء در سال ۲۰۲۰ آمده است -، به ارتقاء امنیت سایبری اینترنت اشیاء ادامه خواهد داد. علاوه‌براین، دولت بر طبق دستورالعمل فرمان اجرایی شماره ۱۴۰۲۸ - «ارتقاء امنیت سایبری کشور» - طرح‌های برچسب‌زنیِ امنیت سایبریِ محصولات [حوزه] اینترنت اشیاء را ادامه خواهد داد. به‌واسطهٔ این طرح، مصرف‌کنندگان قادر خواهند بود امکانات امنیت سایبریِ ارائه‌شده توسط محصولات مختلف اینترنت اشیاء را مقایسه کنند. درنتیجه، در بازارِ کل اکوسیستم اینترنت اشیاء مشوق‌هایی برای توجه بیشتر به جنبه‌های امنیت [سایبری] شکل خواهد گرفت.

هدف راهبردی ۳/۳: تغییر مسئولیت برای محصولات و خدمات نرم افزاری ناامن

بازارها تنبیه مناسبی برای بازیگرانی که محصولات یا خدمات آسیب‌پذیر را وارد اکوسیستم دیجیتال ما می‌کنند، در نظر نمی‌گیرند -

بلکه معمولاً آن‌ها را تشویق می‌کنند. بسیاری از فروشندگان شیوه‌های درستِ توسعهٔ ایمن را نادیده گرفته و محصولاتی را با تنظیمات پیش‌فرضِ ناامن یا نقاط ضعف آشکار عرضه می‌کنند و نرم‌افزار شخص ثالث با منشأ بررسی‌نشده یا ناشناخته را [در محصولات خود] استفاده می‌کنند. سازندگان نرم‌افزار می‌توانند از موقعیت خود در بازار استفاده کرده و با استناد به مفاد قرارداد، مسئولیت خود [در مورد مسائل امنیتی] را به‌طور کامل انکار کنند. همین مسئله باعث کاهشِ دوچندانِ میل آن‌ها برای پیروی از اصول طراحیِ ایمن یا انجام آزمایش‌های پیش از انتشار می‌شود. امنیت ضعیف نرم‌افزاری خطرات سیستمی را در سراسر اکوسیستم دیجیتال به شدت افزایش داده و شهروندان آمریکایی را متحمل هزینه‌های سنگین می‌کند.

ما باید مسئولیت‌پذیری را در مجموعه‌هایی که اقدامات احتیاطی منطقی را برای ایمن‌سازی نرم افزار خود انجام نمی‌دهند، افزایش دهیم؛ اگرچه این نکته را نیز فراموش نمی‌کنیم که حتی پیشرفته‌ترین نرم‌افزارهای امنیتی نیز نمی‌توانند از همه آسیب‌پذیری‌ها جلوگیری کنند. شرکت‌هایی که نرم‌افزار تولید می‌کنند باید آزادی نوآوری داشته باشند، اما در صورت عدم انجام وظایف مراقبتی که نسبت به مصرف‌کنندگان، کسب‌وکارها یا ارائه‌دهندگان زیرساخت حیاتی دارند، باید پاسخگو باشند. مسئولیت باید بر عهده ذی‌نفعانی گذاشته شود که قادر به انجام اقدامات لازم برای جلوگیری از نتایج بد هستند، نه بر عهده کاربران نهایی که اغلب پیامدهای نرم افزار ناامن را متحمل می‌شوند و نه بر عهده توسعه دهنده منبع باز یک جزء که در یک محصول تجاری ادغام شده است. انجام این کار بازار را به سمت تولید محصولات و خدمات ایمن‌تر سوق می‌دهد و در عین حال نوآوری و توانایی استارتاپ ها و سایر مشاغل کوچک و

متوسط را برای رقابت با رهبران بازار حفظ می‌کند.

دولت با همکاریِ کنگره و بخش خصوصی به‌دنبال تدوین قوانینی برای ایجاد مسئولیت در قبال محصولات و خدمات نرم افزاری خواهد بود. چنین قانونی باید مانعِ شانه‌خالی‌کردنِ تولیدکنندگان و ناشرانِ قدرتمندِ نرم‌افزارها از مسئولیت خود با توسل به مفاد قراردادها شده و استانداردهای بالاتری را برای امنیتِ نرم‌افزارها در سناریوهای پرخطر و خاص وضع کند. دولت در گام نخستِ خود در مسیر تدوین استانداردهای توسعهٔ امنِ نرم‌افزارها، طراحیِ یک چهارچوب لنگرگاه امنِ سازگار برای محافظت از شرکت‌های مسئولیت‌پذیری که محصولات و خدمات نرم‌افزاری خود را به طور ایمن توسعه می‌دهند، را در دستور کار خود قرار داده است. این چهارچوب از بهترین شیوه‌های کنونی برای امنیت نرم‌افزار - مانند چارچوب توسعه نرم‌افزار ایمن مؤسسه ملی استانداردها و تکنولوژی - استفاده می‌کند. بعلاوه، چهارچوب مذکور باید در طول زمان تکامل یابد و ابزارهای جدیدی را برای توسعه نرم‌افزار ایمن، شفافیت نرم‌افزار و کشف نقاط آسیب‌پذیر در خود بگنجاند.

دولت در جهت ایجاد انگیزه بیشتر برای اتخاذ شیوه‌های امنِ توسعهٔ نرم‌افزارها، در تلاش خواهد بود که افشای هماهنگِ نقاط آسیب‌پذیر در همه انواع تکنولوژی و بخش‌ها و همچنین استفاده از صورت‌حساب مواد [اولیهٔ] نرم‌افزار [ها] را ترویج کرده و فرآیندی را برای شناسایی و کاهش خطر نرم‌افزارهای پشتیبانی‌نشده - که کاربرد گسترده یا حساسی دارند - طراحی کند. با مشارکت بخش خصوصی و جامعه نرم‌افزاریِ منبع-باز، دولت فدرال به سرمایه‌گذاری در توسعه نرم‌افزارهای ایمن – از جمله زبان‌های ایمن برای ذخیره‌سازی، تکنیک‌های توسعه نرم‌افزار، چارچوب‌ها و ابزارهای تست - ادامه خواهد داد.

هدف راهبردی ۴ / ۳: استفاده از کمک‌های مالی فدرال و سایر مشوق‌ها برای ایجاد امنیت

برنامه‌های کمک مالی فدرال فرصت‌هایی راهبردی برای سرمایه‌گذاری در زیرساخت‌هایی را فراهم می‌کند که طراحی، توسعه، عملیاتی‌کردن و نگهداری از آن‌ها با لحاظ کردن جوانب مختلف امنیت سایبری و اصلِ «تاب‌آوری در برابر همهٔ خطرات» بوده است. از طریق برنامه‌هایی که منابع مالی آن‌ها توسط قانون فراحزبی [توسعه] زیرساخت، قانون کاهش تورم، و قانون «تراشه‌ها و علم» تأمین شده است، ایالات متحده اقدام به سرمایه‌گذاری‌های بلندمدت و نسلی در زیرساخت‌های حیاتی و اکوسیستم دیجیتالی که از آن‌ها پشتیبانی می‌کند کرده است. این دولت متعهد به سرمایه‌گذاری به گونه‌ای است که تاب‌آوری سیستمی جمعی ما را افزایش دهد.

دولت فدرال با نهادهای کشوری، منطقه‌ای، محلی و قبیله‌ای، بخش خصوصی و سایر شرکا برای ایجاد تعادل بین الزامات امنیت سایبری برای متقاضیان با کمک فنی و سایر اشکال پشتیبانی همکاری خواهد کرد. ما در کنار هم می‌توانیم سرمایه‌گذاری در [تولید] محصولات و خدمات حیاتیِ ایمن و تاب‌آور را هدایت کرده و امنیت و تاب‌آوری را در طول چرخه عمر زیرساخت‌های حیاتی حفظ و تقویت کنیم. دولت فدرال همچنین یکی از اولویت‌های بودجه‌ایِ خود را برنامه‌های تحقیق، توسعه و بازنماییِ امنیت سایبری با هدف تقویت امنیت سایبری و تاب‌آوری زیرساخت‌های حیاتی قرار خواهد داد، و با همکاری کنگره مکانیسم‌های تشویقی دیگری را برای هدایت اقدامات امنیت سایبری بهتر در مقیاس کلان طراحی خواهد کرد.

هدف راهبردی ۳/۵: استفاده از امکانات فدرال برای بهبود مسئولیت‌پذیری

برای فروشندگانی که با دولت فدرال کار می‌کنند، الزاماتی که در قراردادها ذکر می‌شود ابزار مؤثری برای ارتقاء امنیت سایبری بوده است. فرمان اجرایی شماره ۱۴۰۲۸ - «ارتقاء امنیت سایبری کشور» - بر این رویکرد تصریح می‌کند که سازمان‌های فدرال باید بیش از پیش الزامات امنیت سایبری را در قراردادهای خود لحاظ کنند. تداوم اجرای آزمایشی مفاهیم جدید برای تنظیم، اجرا و آزمایش الزامات امنیت سایبری از طریق تدارکات می‌تواند به شکل‌گیری رویکردهای جدید و تکثیرپذیر منجر شود.

شرکت‌ها ناگزیرند به تعهداتی که در قراردادهای خود با دولت فدرال در مورد رعایت اصول و شیوه‌های امنیت سایبری داده‌اند، پایبند باشند. طرح کلاهبرداری سایبری مدنی[1] از اختیارات وزارت دادگستری تحت قانون ادعاهای نادرست[2] برای پیگیری اقدامات مدنی علیه ارائه‌دهندگان خدمات و پیمانکاران دولتی که به تعهدات امنیت سایبری عمل نمی‌کنند، استفاده می‌کند. این طرح نهادها یا افرادی را که به روش‌های مختلف، اطلاعات یا سیستم‌های ایالات متحده را به خطر می‌اندازند تحت پیگرد قرار می‌دهد؛ روش‌هایی همچون ارائهٔ آگاهانهٔ محصولات و خدماتِ امنیت سایبریِ معیوب و ضعیف، ارائه آگاهانهٔ تصویری غیرواقعی از فرآیندها و پروتکل‌های امنیت سایبریِ خود، و نقش آگاهانهٔ تعهدات خود در مورد رصد و گزارش‌دهی حوادث و حملات سایبری.

1 Civil Cyber-Fraud Initiative (CCFI)
2 False Claims Act

هدف راهبردی ۳/۶: کاوش در زمینه بیمه سایبری فدرال

هنگامی که حوادث فاجعه بار رخ می‌دهد، وظیفه دولت است که ثبات را به اقتصاد بازگردانده و ابهامات را برطرف کند. در صورت وقوع یک حادثه سایبری فاجعه‌بار، می‌توان از دولت فدرال برای تثبیت اقتصاد و کمک به بهبود درخواست کرد. سامان‌دادن به این واکنش قبل از وقوع یک رویداد فاجعه بار - به جای عجله برای آماده‌کردنِ بسته‌های کمکی پس از این واقعیت - می‌تواند اعتماد را به بازارها بازگردانده و تاب‌آوریِ کشور را افزایش دهد. دولت نیاز و ساختارهای احتمالی واکنش بیمه فدرال به رویدادهای سایبری فاجعه بار را که از بازار بیمه سایبری موجود حمایت می‌کند، ارزیابی خواهد کرد. دولت در مورد [چگونگی] طراحی و توسعه این ارزیابی با کنگره، [نهادهای] تنظیم‌گر ایالتی و ذی‌نفعان صنعت مشورت خواهد کرد.

رکن چهارم:
سرمایه‌گذاری برای آینده‌ای تاب‌آور

رکن چهارم: سرمایه‌گذاری برای آینده‌ای تاب‌آور

فردای دیجیتالی تاب‌آور و شکوفا با سرمایه‌گذاری‌های امروز آغاز می‌شود. ما می‌توانیم اکوسیستم دیجیتالی امن‌تر، تاب‌آورتر، عادلانه‌تر و حافظ حریم خصوصی را از طریق سرمایه‌گذاری‌های راهبردی و اقدامات هماهنگ و مشترک ایجاد کنیم. با انجام این کار، ایالات متحده نقش پیشروِ خود را به‌عنوان سردمدار اصلیِ جریان نوآوری در تکنولوژی‌ها و زیرساخت‌های نسل بعدیِ ایمن و تاب‌آور حفظ خواهد کرد.

عناصر اساسی اکوسیستم دیجیتال ما - مانند اینترنت - محصول سرمایه‌گذاری‌های پایدار و متقابل توسط نهادهای بخش دولتی و خصوصی هستند. با این حال، سرمایه‌گذاری‌های دولتی و خصوصی در امنیت سایبری مدت‌هاست که دنباله‌رویِ تهدیدها و چالش‌هایی بوده‌اند که با آن‌ها مواجه بوده‌ایم. با شکل‌گیری نسل جدیدی از زیرساخت‌های دیجیتال - از نسل بعدی مخابرات و اینترنت اشیاء گرفته تا منابع انرژی توزیع‌شده - و آماده شدن برای تغییرات انقلابی در چشم‌انداز تکنولوژی کشور که توسط هوش مصنوعی و محاسبات کوانتومی رقم می‌خورد، نیاز به رسیدگی به این گسستِ سرمایه‌گذاری ضروری‌تر از قبل شده است.

دولت فدرال باید از سرمایه‌گذاری‌های عمومی راهبردی در نوآوری، تحقیق، توسعه و آموزش استفاده کند تا بتواند به نتایجی دست پیدا کند که

از نظر اقتصادی پایدار بوده و در خدمت منافع ملی باشند. ما با بهره‌گیری از طرح‌ها و برنامه‌هایی همچون برنامه محرک‌های محلیِ نوآوری[1] بنیاد ملی علوم[2]، برنامه فضای سایبریِ دیرپا، امن و قابل اعتماد[3]، برنامه‌های [اعطای] بورسیه و کمک مالی فراهم‌شده در قانون فراحزبیِ [توسعه] زیرساخت، قانون کاهش تورم، و قانون «تراشه‌ها و علم»، تلاش خواهیم کرد مؤسسات تولیدکننده و سایر بخش‌های سیستمِ تحقیق و توسعهٔ فدرال را سامان بدهیم.

این سرمایه‌گذاری‌ها رهبری مستمر ایالات متحده در تکنولوژی و نوآوری را به‌عنوان بخشی از راهبرد صنعتی و نوآوری مدرن تضمین می‌کند. دهه‌هاست که دشمنان و عوامل متخاصم از تکنولوژی‌ها و نوآوریِ ما علیه خودمان - در جهت اهدافی همچون سرقت مالکیت معنوی، مداخله یا تأثیرگذاری در روند انتخابات، و تضعیف دفاع ملی ما - استفاده کرده‌اند. این مسئله نشان‌دهندهٔ این است که رهبری در نوآوری بدون امنیت کافی نیست. ما تلاش‌های خود برای پیشی‌گرفتن از سایر کشورها در حوزه نوآوری را با اقدامات هماهنگ و متمرکز برای طراحی، توسعه و بهینه‌سازی تکنولوژی‌های حیاتی و نوظهورِ امنیت سایبری تکمیل خواهیم کرد. ما اطمینان خواهیم یافت که تاب‌آوری نه یک عنصر اختیاری از قابلیت‌های تکنولوژیک جدید، بلکه یک عنصر تجاری کارآمد در فرآیند نوآوری و عملیاتی‌کردن است.

1 Regional Innovation Engines program
2 National Science Foundation (NSF)
3 long- standing Secure and Trustworthy Cyberspace program

هدف راهبردی ۱ / ۴: ایمن‌سازی پایه فنی اینترنت

اگرچه اینترنت برای آینده ما حیاتی است، اما همچنان ساختار اساسی گذشته خود را حفظ کرده است. بسیاری از زیربناهای تکنولوژیک اکوسیستم دیجیتال ما ذاتاً آسیب‌پذیر هستند. هر بار که چیز جدیدی بر روی این بنا قرار می‌دهیم، آسیب‌پذیری‌های جدیدی را به آن اضافه می‌کنیم و ریسک جمعی خود را افزایش می‌دهیم. ما باید اقداماتی را برای کاهش فوری‌ترین نگرانی‌های فراگیر - از جمله آسیب‌پذیری‌های پروتکل گِیت‌وِی مرزی[1]، درخواست‌های سیستم دامین رمزگذاری نشده، و آهسته بودن فرآیند پیاده‌سازیِ آی‌پی‌وی ۶ [2] - انجام دهیم. این عملیات «پاکسازی» برای کاهش ریسک سیستمی، مستلزم شناسایی مهم‌ترین چالش‌های امنیتی، توسعه بیشتر اقدامات امنیتی مؤثر و همکاری نزدیک بین بخش‌های دولتی و خصوصی برای کاهش خطرپذیری ما بدون ایجاد اختلال در پلت‌فرم‌ها و خدمات ساخته شده است. دولت فدرال بر روی این زیرساخت با اطمینان از اینکه شبکه‌هایش این اقدامات امنیتی و سایر اقدامات امنیتی را اجرا کرده‌اند و در عین حال با سهامداران برای توسعه و اتخاذ راه‌حل‌هایی که امنیت اکوسیستم اینترنت را بهبود می‌بخشد و از تحقیقات برای درک و رسیدگی به دلایل پذیرش کند حمایت می‌کند، رهبری خواهد کرد.

حفظ و گسترش اینترنت باز، رایگان، جهانی، تبادل‌پذیر، قابل اعتماد و ایمن مستلزم مشارکت مداوم در فرآیند طراحی استانداردها برای تزریق ارزش‌های خود به آن‌ها و اطمینان از این است که این استانداردهای فنی تکنولوژی‌هایی ایمن‌تر و تاب‌آورتر تولید می‌کنند. از آن‌جا که رژیم‌های

1 Border Gateway Protocol vulnerabilities
2 IPv6

خودکامه به دنبال تغییر اینترنت و ماهیت چندجانبه آن هستند تا امکان کنترل، سانسور و نظارت خود بر آن را فراهم کنند، ایالات متحده و شرکای بخش خصوصی و خارجیِ آن در تلاش برای تدوین راهبردی چندوجهی هستند که تأمین‌کنندهٔ اهدافی از جمله حفظ برتری فنی، محافظت از امنیت جامعه، ایجاد رقابت اقتصادی، و تقویت تجارت دیجیتال باشد، و از این مسئله اطمینان حاصل کند که «قواعد مسیر» برای [توسعهٔ] استانداردهای تکنولوژی اصول شفافیت، باز بودن، اتفاق‌نظر، مرتبط بودن و انسجام را رعایت می‌کند. ایالات متحده با حمایت از سازمان‌های غیردولتی توسعه‌دهنده استاندارد[1]، باب همکاری با رهبران صنعت، متحدان بین‌المللی، مؤسسات دانشگاهی، جوامع حرفه‌ای، گروه‌های مصرف‌کننده و سازمان‌های غیرانتفاعی را برای ایمن‌سازی تکنولوژی‌های نوظهور، فعال‌سازی قابلیت همکاری، تقویت رقابت در بازار جهانی، افزایش امنیت ملی و مزیت اقتصادی کشور گشوده است.

هدف راهبردی ۲ / ۴: تقویت مجدد [بخش] تحقیقات و توسعه فدرال در حوزهٔ امنیت سایبری

دولت فدرال قادر است که با اولویت‌دهی به تحقیق و توسعه در معماری‌های قابل دفاع و تاب‌آور و کاهش آسیب‌پذیریِ تکنولوژی‌های زیربنایی، اطمینان حاصل کند که تکنولوژی‌های آینده از تکنولوژی‌های امروزی امن‌تر خواهند بود.

دولت در بخشی از اقدامات خود در زمینه به‌روزرسانی برنامه راهبردی تحقیق و توسعهٔ امنیت سایبری فدرال، جامعهٔ تحقیق، توسعه

1 Non-governmental Standards Developing Organizations (SDOs)

و بازنمایی[1] را شناسایی و اولویت‌بندی کرده و [فعالیت‌های آن را] تسهیل خواهد کرد؛ تا این حوزه را قادر به پیشگیریِ فعالانه از خطرات امنیت سایبری موجود در تکنولوژی‌های کنونی و نسل بعدی نماید. دپارتمان‌ها و سازمان‌ها پروژه‌های تحقیق، توسعه و بازنمایی را در جهت تقویت امنیت سایبری و تاب‌آوری در زمینه‌های مختلف - از جمله هوش مصنوعی، تکنولوژی‌های عملیاتی و سیستم‌های کنترل صنعتی، زیرساخت‌های ابری، مخابرات، رمزگذاری، شفافیت سیستم و تجزیه و تحلیل داده‌های مورد استفاده در زیرساخت‌های حیاتی - هدایت خواهند کرد. این اقدامات تحت حمایتِ شرکت‌های فدرالِ [فعال در حوزهٔ] تحقیق، توسعه و بازنمایی - از جمله بنیاد ملی علوم، آزمایشگاه‌های ملیِ وزارت انرژی[2]، و سایر مراکز تحقیق و توسعه با بودجه فدرال[3] - بوده و در مشارکت با دانشگاه‌ها، تولیدکنندگان، شرکت‌های تکنولوژی، و مالکان و اپراتورها به پیش خواهد رفت.

این دسته از سرمایه‌گذاری‌های [حوزه] تحقیق، توسعه و بازنمایی بر تأمین امنیت سه خانواده از تکنولوژی‌هایی که برای اعتلای ایالات متحده در دهه آینده تعیین‌کننده خواهند بود، تمرکز خواهند کرد: تکنولوژی‌های مرتبط با محاسبات - از جمله میکروالکترونیک، سیستم‌های اطلاعات کوانتومی، و هوش مصنوعی -، بیوتکنولوژی و تولید زیستی[4]، و تکنولوژی‌های انرژی پاک. این کار باعث تسهیل شناسایی فعالانهٔ آسیب‌پذیری‌های بالقوه و همچنین تحقیق برای کاهش آن‌ها شده و همچنین از تدوین یک راهبرد کلان‌ترِ مدرن در حوزه صنعت و نوآوری حمایت می‌کند که - با بهره‌گیریِ همه‌جانبه از تمامیِ انواع سرمایه‌گذاری

1 Research, development, and demonstration (RD&D)
2 Department of Energy
3 Federally funded research and development centers (FFRDCs)
4 Biomanufacturing

فدرال، قدرت خرید فدرال و مقررات فدرال - نوآوری‌های منسجم و راهبردی را تقویت کرده و بازارهایی برای محصولات و خدمات قابل اعتماد ایجاد کند.

هدف راهبردی ۳/۴: مهیاشدن برای آینده‌ای پسا کوانتومی

رمزگذاری قوی در حوزه امنیت سایبری و تجارت جهانی عنصری کلیدی است. این روش اصلی محافظت از داده‌های خود به صورت آنلاین، اعتبارسنجی کاربران نهایی، تأیید اعتبار امضاها و تأیید صحت اطلاعات است. اما محاسبات کوانتومی این پتانسیل را دارد که برخی از رایج‌ترین استانداردهای رمزگذاری که امروزه به کار گرفته شده‌اند را بشکند. ما باید سرمایه‌گذاری‌ها را در جایگزینی گسترده سخت‌افزار، نرم‌افزار و سرویس‌هایی که می‌توانند به راحتی توسط رایانه‌های کوانتومی در معرض خطر قرار گیرند، اولویت‌بندی کرده و تسریع کنیم تا اطلاعات در برابر حملات آینده محافظت شود.

برای ایجاد تعادل بین پیشرفت‌های محاسبات کوانتومی و تهدیداتی که سیستم‌های دیجیتال را هدف قرار می‌دهند، بیانیه امنیت ملی شماره ۱۰ - تحت عنوان «تقویت جایگاه برتر ایالات متحده در محاسبات کوانتومی و کاهش ریسک سیستم‌های رمزنگاری آسیب‌پذیر» - فرآیندی برای انتقال به‌موقع سیستم‌های رمزنگاری کشور به سیستم‌های مقاوم در برابر [محاسبات] کوانتومی طراحی کرده است. دولت فدرال انتقال شبکه‌ها و سیستم‌های عمومی آسیب‌پذیر به محیط‌های مبتنی بر رمزنگاری مقاوم در برابر [محاسبات] کوانتومی را در اولویت قرار داده

و در تکمیل این روند، راهبردهای کاهندهٔ دیگری برای ایجاد چابکی رمزنگاری در مواجهه با خطرات ناشناخته آینده توسعه خواهد داد. بخش خصوصی باید از مدل دولت در آماده‌سازی شبکه‌ها و سیستم‌های خود برای آینده پساکوانتومی الگوبرداری کند.

هدف راهبردی ۴/۴: تأمین امنیت منابع آیندهٔ انرژی پاک

سرعت فزایندهٔ گذار ما به جهان آینده و بهره‌گیری از انرژی‌های پاک، باعث ورود نسل جدیدی از سیستم‌های سخت‌افزاری و نرم‌افزاریِ به‌هم‌پیوسته به فضای آنلاین شده است که پتانسیل تقویت تاب‌آوری، ایمنی و کارایی شبکه برق ایالات متحده را دارند. این تکنولوژی‌ها - از جمله منابع انرژی توزیع‌شده، دستگاه‌های تولید و ذخیره‌سازی انرژی «هوشمند»، پلت‌فرم‌های پیشرفته ابری برای مدیریت شبکه، و شبکه‌های انتقال و توزیع طراحی‌شده برای بارهای قابل کنترل با ظرفیت بالا - بسیار پیچیده‌تر، اتوماتیک‌تر و به‌لحاظ دیجیتالی درهم‌تنیده‌تر از نسل‌های قبلیِ سیستم‌های شبکه‌ای هستند.

با سرمایه‌گذاری‌های بلندمدت ایالات متحده در زیرساخت‌های انرژی، دولت فدرال بصورت فعالانه از این فرصت برای ارتقاء امنیت سایبری استفاده خواهد کرد. دولت این کار را از مجرای عملیاتی‌سازیِ راهبرد مهندسیِ آگاه به [مسائل] سایبری[1] - که متعلق به کنگره است - پیش خواهد برد؛ نه اینکه بعد از اینکه دستگاه‌های متعدد بصورت گسترده به کار گرفته شدند، مجموعه‌ای از کنترل‌ها و ضمایمِ امنیتی را طراحی

1 National Cyber-Informed Engineering Strategy

کند. کار دولت ایجاد هماهنگی میان فعالیت‌های ذی‌نفعان مختلف در سرتاسر سیستم فدرال، صنعت، و سطوح ملی، محلی، قبیله‌ای و منطقه‌ای در جهت دستیابی به شبکه امنی از شارژرهای خودروهای الکتریکی، زیرساخت سوخت‌رسانی بدون آلایندگی، و اتوبوس‌های مسافربری و سرویس‌های مدرسهٔ بدون آلایندگی است. وزارت انرژی به کمک اقداماتی از قبیل شتاب‌دهنده امنیت سایبری انرژی پاک[1] و طرح فرحزبی [توسعه] زیرساخت، برنامهٔ Energy Cyber Sense را به اجرا گذاشته است. آزمایشگاه‌های ملی تلاش‌های دولت برای ایمن‌سازی شبکه انرژی پاک در آینده و طراحی بهترین راهکارهای امنیتی - که قابل تسرّی به سایر زیرساخت‌های حیاتی نیز باشد - را هدایت می‌کنند. همچنین، وزارت انرژی در همکاری با [حوزه] صنعت، دولت‌های ایالتی، [نهادهای] تنظیم‌گر فدرال، کنگره و سایر آژانس‌ها به تقویت امنیت سایبری در [شبکه] توزیع برق و [سایر] منابع انرژی‌های توزیع‌پذیر ادامه خواهد داد.

هدف راهبردی ۴/۵: حمایت از توسعه یک اکوسیستم هویت دیجیتال

راه‌حل‌ها و زیرساخت‌های پیشرفته‌تر [در حوزهٔ] هویت دیجیتال امکان شکل‌گیری اقتصاد دیجیتالی نوآورانه‌تر، عادلانه‌تر، ایمن و کارآمدتر را فراهم می‌کنند. این راه‌حل‌ها می‌توانند از دسترسی آسان‌تر و ایمن‌تر به مزایا و خدمات دولتی، ارتباطات و شبکه‌های اجتماعی قابل اعتماد، و امکانات جدید برای قراردادهای دیجیتال و سیستم‌های

1 Clean Energy Cybersecurity Accelerator (CECA)

پرداخت پشتیبانی کنند.

امروزه در حوزهٔ هویت دیجیتال فقدان راه‌حل‌هایی که مبتنی بر رضایت [مصرف‌کننده] بوده، ایمن و حافظ حریم خصوصی باشند، امکان افزایش کلاهبرداری و تداوم محرومیت و نابرابری را فراهم کرده و فعالیت‌های مالی و زندگی روزمره ما را دچار ناکارآمدی کرده است. سرقت هویت در حال افزایش است، به طوری که نقض داده‌ها حدود ۳۰۰ میلیون قربانی را در سال ۲۰۲۱ تحت‌تأثیر قرار داده است و بازیگران متخاصم به شیوه‌های مختلف، میلیاردها دلار از صندوق‌های امدادرسانی همه‌گیری کوید۱۹-که برای مشاغل کوچک و افراد نیازمند در نظر گرفته شده بودند- به سرقت برده‌اند. اینگونه فعالیت‌های متخاصمانه همه ما را تحت تأثیر قرار می‌دهد و ضررهای قابل توجهی به مشاغل وارد می‌کند و تأثیرات جبران‌ناپذیری بر برنامه‌های خدمت‌رسانیِ عمومی و افرادی که از آن‌ها استفاده می‌کنند، می‌گذارد. بخش خصوصی و بخش دولتی نتوانسته‌اند با تلاش‌های مستقل و جداگانهٔ خود این مشکل را حل کنند.

دولت فدرال سرمایه‌گذاری بر راه‌حل‌های قدرتمند و معتبری [برای مسئلهٔ] هویت دیجیتال را افزایش خواهد داد که باعث ارتقاء امنیت و دسترسی و تبادل‌پذیری، شمول مالی و اجتماعی، حراست از حریم خصوصی افراد، و رشد اقتصادی شوند. بر اساس برنامه تحقیقاتی هویت دیجیتال تحت رهبری مؤسسه ملی استانداردها و تکنولوژی - که در قانون «تراشه‌ها و علم» آمده است -، این تلاش‌ها شامل این موارد خواهد بود: تقویت امنیت اعتبارنامه‌های دیجیتال؛ ارائه خدمات اعتبارسنجی ویژگی و اعتبار؛ انجام تحقیقات بنیادی؛ به‌روزرسانی استانداردها، دستورالعمل‌ها و فرآیندهای حکمرانی برای فراهم‌کردن

امکان استفاده مداوم و تبادل‌پذیری؛ و توسعه پلتفرم‌های هویت دیجیتالی و حمایت از شفافیت و ارزیابی دقیق. ضمن تقدیر از تلاش ایالت‌ها برای اجرای آزمایشی [طرح] گواهینامهٔ رانندگی موقت، آن‌ها را دعوت به تمرکز بر حریم خصوصی، امنیت، آزادی‌های مدنی، برابری، دسترسی، و قابلیت‌های تبدال‌پذیری می‌کنیم.

خط‌مشی‌ها و فناوری‌های ما در حوزه دیجیتال با توسعه و ارتقاء قابلیت‌های خود، قادر خواهند بود که از حریم خصوصی، حقوق و آزادی‌های مدنی حراست کنند؛ از عواقب ناخواسته، سوگیری‌ها و سوءاستفاده‌ها جلوگیری کنند؛ امکان انتخاب فروشنده و استفادهٔ داوطلبانه را برای افراد فراهم کنند؛ امنیت، قابلیت هم‌افزایی، جامعیت و دسترس‌پذیری را بهبود بخشند؛ و نهایتاً شفافیت و مسئولیت‌پذیری را در استفاده از تکنولوژی و داده‌های افراد افزایش دهند.

هدف راهبردی ۴/۶: توسعه یک راهبرد ملی برای تقویت نیروی کار سایبری ما

امروزه صدها هزار پست خالی در مشاغل حوزهٔ امنیت سایبری در سراسر کشور وجود دارد و این خلاء در حال افزایش است. هم بخش خصوصی و هم کارفرمایان دولتی در جذب، استخدام و حفظ متخصصان برای پر کردن این مشاغل خالی با چالش‌هایی روبرو هستند که بر امنیت سایبری جمعی ما تأثیر منفی می‌گذارد. برای مقابله با این چالش، دفتر فرماندهی سایبری ملی توسعه و نظارت بر اجرای راهبرد ملی نیروی کار سایبری و آموزش را رهبری خواهد کرد.

این راهبرد رویکردی جامع و هماهنگ برای گسترش نیروی کار

سایبری ملی، بهبود تنوع آن و افزایش دسترسی به مسیرهای آموزش سایبری خواهد داشت. این کار نیاز به تخصصِ امنیت سایبری در تمام بخش‌های اقتصاد – به‌خصوص در زیرساخت‌های حیاتی - را برطرف کرده و نیروی کار آمریکا را قادر می‌سازد که به نوآوری در تکنولوژی‌های ایمن و تاب‌آورِ نسل بعدی ادامه دهد. این راهبرد نیروی کار سایبری فدرال را تقویت کرده و تنوع می‌بخشد و به چالش‌های خاصی که بخش عمومی در استخدام، حفظ و توسعه استعدادها و ظرفیت‌های مورد نیاز برای حفاظت از داده‌های فدرال و زیرساخت‌های تکنولوژی اطلاعات با آن مواجه است، رسیدگی خواهد کرد. راهبرد ما با آگاهی از این که چالش‌های نیروی کار سایبری منحصر به ایالات متحده نیست، از تلاش‌های در حال انجام در سایر کشورها الهام می‌گیرد.

سند راهبردیِ امنیت سایبری ایالات متحده راه خود را بر مبنای تلاش‌های موجود در حوزهٔ توسعه نیروی کار ملی امنیت سایبری کشور - از جمله طرح ملی آموزش امنیت سایبری[1]، طرح سایبر کورپس: بورس تحصیلی برای خدمات[2]، مراکز ملی تعالی دانشگاهی[3] در حوزه امنیت سایبری، طرح آموزش و دستیاریِ امنیت سایبری[4]، و برنامه کارآموزی ثبت‌شده[5] - دنبال خواهد کرد. این راهبرد همچنین از برنامه‌های کنونیِ توسعه نیروی کار - که در بنیاد ملی علوم و سایر نهادهای علمی در جریان هستند - برای تقویت برنامه‌های دولت فدرال استفاده می‌کند.

راهبرد ما با کمبود تنوع در نیروی کار سایبری نیز مقابله خواهد کرد. جریان استخدام نیروی کار توسط کارفرمایان تنها گسترهٔ ناچیزی

1 National Initiative for Cybersecurity Education (NICE)
2 the CyberCorps: Scholarship for Service program
3 National Centers of Academic Excellence
4 Cybersecurity Education Training and Assistance Program
5 Registered Apprenticeships Program

از استعدادها و شبکه‌های حرفه‌ای را مد نظر داشته و قادر به بهره‌گیری از طیف متنوع سرمایه‌های انسانیِ کشور نیست. زنان، رنگین پوستان، متخصصان و مهاجران نسل اول، افراد دارای معلولیت، و افراد ال‌جی‌بی‌تی[1]، از جمله جوامعی هستند که در این زمینه کمتر حضور دارند. پرداختن به نابرابری‌های سیستمی و غلبه بر موانعی که مانع از تنوع در نیروی کار سایبری می‌شود، هم یک ضرورت اخلاقی و هم یک ضرورت راهبردی است.

ما برای جذب و آموزش نسل بعدی متخصصان امنیت سایبری در جهت ایمن‌سازی اکوسیستم دیجیتالِ خود نیاز به رهبری فدرال و مشارکت پایدار بین بخش‌های دولتی و خصوصی داریم. دستیابی به نیروی کار سایبریِ قدرتمند تنها از طریق فراهم کردن یک امکان شغلی و حرفه‌ای [در حوزه] امنیت سایبری برای افراد علاقمند ممکن می‌شود؛ و این امر نیاز به مشارکت همهٔ سازمان‌هایی دارد که قادر به ایفای نقش در تربیت نسل بعدی استعدادهای امنیت سایبری باشند.

1 LGBTQI

رکن پنجم:

ایجاد مشارکت بین المللی برای پیگیری اهداف مشترک

رکن پنجم: ایجاد مشارکت بین‌المللی برای پیگیری اهداف مشترک

ایالات متحده به دنبال جهانی است که در آن رفتار مسئولانه دولت در فضای سایبری مطلوب بوده و پاداش بگیرد، و رفتار غیرمسئولانه طرد شده و پرهزینه باشد. ما برای دستیابی به این هدف، در کنار تلاش برای شکل‌دهی به ائتلاف گسترده‌ای از کشورهایی که به‌دنبال حفظ اینترنت آزاد، رایگان، جهانی، قابل اعتماد و ایمن هستند، لحظه‌ای از مبارزه با کشورهایی که با برنامه کلان ما در مورد مشکلات مشترک مبارزه می‌کنند دست بر نخواهیم داشت.

کشور ما دهه‌هاست که از طریق نهادهای بین‌المللی برای تعریف و پیشبرد رفتار مسئولانه دولت‌ها در فضای مجازی تلاش کرده است. ما از فرآیندهای چندجانبه‌ای همچون گروه متخصصان حکومتیِ سازمان ملل متحد[1] و کارگروه نیروهای آزاد[2] برای ایجاد چارچوبی استفاده کرده‌ایم که شامل مجموعه‌ای از هنجارهای دوران صلح و اقدامات اعتمادساز است که همه کشورهای عضو سازمان ملل آن‌ها را در مجمع عمومی این سازمان تأیید کرده‌اند. ما از گسترش کنوانسیون بوداپست در مورد جرائم سایبری و سایر تلاش‌های جهانی برای امن‌تر کردن فضای سایبری حمایت کرده‌ایم و به این تلاش‌ها ادامه خواهیم داد. در عین حال، برای خنثی کردن چشم‌انداز تاریک آینده اینترنت که جمهوری خلق چین و

1 the United Nations (UN) Group of Governmental Experts
2 Open-Ended Working Group

سایر دولت‌های خودکامه به‌دنبال تحقق آن هستند، نیاز به همکاری با متحدین خود داریم. برای تحقق این امر، تلاش دولت ایالات متحده این است که به انواع جوامع و اقتصادها ارزشِ گشودگی و باز بودن را نشان دهد، و نیز رفتارهایی که برخلاف هنجارهای مورد توافق در مورد نحوهٔ رفتار دولت‌ها است را به عقوبت برسانیم.

ایالات متحده آمریکا در راستای مقابله با تهدیدات رایج، حفظ و تقویت آزادی جهانی اینترنت، محافظت در برابر سرکوب دیجیتال فراملی، و ایجاد یک اکوسیستم دیجیتال جمعی که ذاتاً تاب‌آورتر و قابل دفاع‌تر باشد، تلاش خواهد کرد تا مدل جدید همکاری ذی‌نفعان امنیت سایبری ملی با جامعه بین‌المللی را گسترش دهد. ما ائتلاف‌ها را گسترش می‌دهیم، مجرمان فراملی و دیگر بازیگران متخاصم سایبری را تحت فشار قرار می‌دهیم، قابلیت‌های متحدان و شرکای بین‌المللی خود را ارتقاء می‌دهیم، قابلیت عملیاتی‌شدنِ قوانین بین‌المللی موجود در مورد رفتار دولت‌ها در فضای سایبری را تقویت می‌کنیم، از هنجارهای پذیرفته‌شده جهانی و همگانیِ رفتار مسئولانه در فضای سایبری در دوران صلح حمایت می‌کنیم، و کسانی که مبادرت به فعالیت‌های سایبری اخلال‌گرانه، مخرب و یا بی‌ثبات‌کننده می‌کنند را مجازات خواهیم کرد.

هدف راهبردی ۱ / ۵: ایجاد ائتلاف برای مقابله با تهدیدات اکوسیستم دیجیتال ما

در آوریل ۲۰۲۲، ایالات متحده به‌همراه ۶۰ کشور دیگر اعلامیه آینده اینترنت[1] را منتشر کرد. این بیانیه - که بزرگترین ائتلاف در نوع

1 Declaration for the Future of the Internet (DFI)

خود بود - طیف متنوع و وسیعی از کشورها را حول دیدگاهی مشترک و دموکراتیک در مورد یک آیندهٔ دیجیتالِ آزاد، همگانی، قابل‌اعتماد، و امن گرد هم آورد. ایالات متحده از طریق معاهدات و مکانیسم‌هایی نظیر اعلامیه آینده اینترنت و ائتلاف آزادی آنلاین[1]، به‌دنبال این است که بار دیگر کشورهای هم‌فکر، جامعه تجاری بین‌المللی و سایر ذی‌نفعان را حول چشم‌انداز خود در مورد آینده اینترنت متحد کند؛ آینده‌ای که ویژگی آن جریان امن و قابل‌اعتماد داده‌ها، احترام به حریم خصوصی، حمایت از حقوق بشر، و پیشرفت در مسیر غلبه بر چالش‌های جدی‌تر است.

ایالات متحده و متحدان و شرکای بین‌المللی آن از طریق مکانیسم‌هایی همچون محفل چهارجانبه امنیتی[2]- بین ایالات متحده، هند، ژاپن و استرالیا - در حال پیشبرد اهداف مشترک خود در مورد فضای سایبری هستند؛ اهدافی از جمله بهبود اشتراک‌گذاری اطلاعات بین تیم‌های واکنش اضطراری کامپیوتری[3] و توسعه یک اکوسیستم دیجیتال بر اساس ارزش‌های جمعی. چارچوب شکوفایی اقتصادی هند و اقیانوسیه[4] و [طرح] مشارکت آمریکا برای رونق اقتصادی[5] فرصت‌هایی را برای ایالات متحده و دولت‌های منطقه‌ای ایجاد می‌کند تا به شیوه‌های مختلف مسیر اقتصاد دیجیتال را جهت‌دهی کنند؛ شیوه‌هایی از قبیل تسهیل طراحی استانداردهای فنی، [طراحی] مکانیسم‌هایی برای برقرار کردن جریان‌های داده‌ایِ برون‌مرزی که در عین حفاظت از حریم خصوصی از غلتیدن به سوی محلی‌سازی داده‌ها اجتناب کند،

1 Freedom Online Coalition
2 Quadrilateral Security Dialogue (“the Quad”)
3 Computer Emergency Response Teams (CERT)
4 The Indo-Pacific Economic Framework for Prosperity (IPEF)
5 Americas Partnership for Economic Prosperity (APEP)

و نیز اقداماتی برای تقویت امنیت و تاب‌آوری زنجیره‌های تأمین. ما به واسطهٔ کمیسیون تجارت و تکنولوژی آمریکا و اروپا[1] همکاری جدیدی در میان دو سوی اقیانوس اطلس شکل داده‌ایم که در تلاش برای مبارزه با تهدیدات مشترک و نیز نشان دادنِ این مسئله است که رویکردهای بازار[ی] به مقولهٔ نوآوری، تکنولوژی و تجارتِ دیجیتال، می‌تواند زندگی شهروندان ما را بهبود بخشیده و ما را به سوی شکوفایی بیشتر رهنمون سازد. ایالات متحده همچنین از طریق پیمان سه‌جانبهٔ امنیتی و فناوری - موسوم به «AUKUS» - با کشورهای استرالیا و انگلستان، به‌دنبال ایمن‌سازی تکنولوژی‌های حیاتی، بهبود هماهنگی [و همکاری] سایبری و اشتراک‌گذاری قابلیت‌های پیشرفته [با این کشورها] است.

ایالات متحده و هم‌تایان بین‌المللی آن می‌توانند از طریق اینگونه همکاری‌ها و با به‌اشتراک‌گذاشتن اطلاعات مربوط به تهدیدات سایبری، مبادله الگوهای مختلف برای اقدامات حوزهٔ امنیت سایبری، مقایسه تخصص‌های مختص به هر بخش، استخراج اصول امنیت ذاتی[2]، و هماهنگ‌کردن خط‌مشی‌های و اقدامات واکنشی خود در برابر سوانح [سایبری]، منافع مشترک خود را پیگیری کنند. علاوه بر این، معاهدات و ائتلاف‌های چندجانبه که بخش خصوصی و سازمان‌های جامعه مدنی نیز در آن وارد می‌شود - مانند فراخوان کرایست‌چرچ برای از بین بردن محتوای افراطی تروریستی و خشونت‌آمیز آنلاین، و ائتلاف آزادی آنلاین، و طرح همکاری جهانی برای اقدام در مورد سوءاستفاده و آزار آنلاینِ مبتنی بر جنسیت[3]- برای مقابله با مسائل سیستمی بسیار مهم هستند. ما از این پیمان‌ها برای فعال‌کردن همکاری عملیاتی مؤثر برای دفاع از

1 US-EU Trade and Technology Council (TTC)
2 Secure-by-design Principles
3 Global Partnership for Action on Gender-Based Online Harassment and Abuse

اکوسیستم دیجیتال مشترک خود استفاده خواهیم کرد. ما همچنین در صورت لزوم از ایجاد شراکت‌های جدید و نوآورانه حمایت و کمک خواهیم کرد؛ مانند طرح بین‌المللی ضد باج‌افزار، که مجموعه‌های منحصربه‌فردی از ذی‌نفعان را برای رسیدگی به چالش‌های جدید و نوظهور امنیت سایبری گرد هم می‌آورد.

از آنجا که اکثر فعالیت‌های سایبری متخاصمانه علیه ایالات متحده توسط عوامل و یا با استفاده از زیرساخت‌های کامپیوتری مستقر در بیرون از مرزهای کشور انجام می‌شود، ما باید مکانیسم‌های همکاری با متحدان و شرکای خود را به‌نحوی تقویت کنیم تا عوامل تهدیدگر قادر به نفوذ به آن و دور زدن قانون نباشند. ایالات متحده با متحدان و شرکای خود برای طراحی مکانیسم‌های مشترکِ جدیدی برای اجرای قانون در عصر دیجیتال همکاری خواهد کرد. به‌عنوان مثال، مرکز جرائم سایبری اروپا[1] نقش حیاتی در نوسازی چارچوب‌های قانونی، آموزش مجریان قانون، بهبود اسناد، همکاری با شرکای بخش خصوصی، و واکنش در برابر فعالیت‌های سایبری متخاصمانه در اروپا ایفا کرده است. برای گسترش این مدل، از تلاش‌ها برای ایجاد قطب‌های مؤثر با شرکا در مناطق دیگر حمایت خواهیم کرد.

هدف راهبردی ۲/۵: تقویت ظرفیت شرکای بین‌المللی

ایالات متحده با ایجاد ائتلافی برای توسعه و پیش‌بُرد اولویت‌ها و دیدگاهی مشترک در مورد اکوسیستم دیجیتال و امنیت سایبری، ظرفیت کشورهای همفکر در سراسر جهان را برای حمایت از این اولویت‌ها

1 the European Cybercrime Centre

تقویت خواهد کرد. ما باید در متحدان و شرکای خود قابلیت‌های ایمن‌سازی شبکه‌های زیرساختی حیاتی، تشخیص و واکنش در برابر سوانح سایبری، اشتراک‌گذاری اطلاعات مربوط به تهدیدات سایبری، طراحی همکاری‌های دیپلماتیک، ظرفیت اجرای قانون و اثربخشی از طریق همکاری عملیاتی را ایجاد کرده و آن‌ها را به سمتی سوق دهیم که با پایبندی به قوانین بین‌المللی و هنجارهای رفتار مسئولانهٔ دولت‌ها، پیگیرِ منافع مشترک خود در فضای سایبری باشند.

برای دستیابی به این هدف، ایالات متحده تخصص‌های مختلف را در بین سازمان‌ها، بخش‌های دولتی و خصوصی، و در میان شرکای منطقه‌ای به‌نحوی سامان‌دهی و هدایت خواهد کرد که امکان شکل‌گیری همکاری‌های هماهنگ و مؤثر بین‌المللی در جهت ظرفیت‌سازی سایبری و اقدامات عملیاتی را فراهم کند. در حوزهٔ قوای مجریِ قانون، وزارت دادگستری به‌واسطهٔ توافقات دوجانبه و چندجانبه، همکاری‌های رسمی و غیررسمی، و با زمامداریِ امور در سطح بین‌المللی و منطقه‌ای در جهت تقویت قوانین، سیاست‌ها و عملیات [مربوط به] جرائم سایبری، به طراحی و شکل‌دهی به یک پارادایم همکاری مستحکم در زمینه جرائم سایبری ادامه خواهد داد. وزارت دفاع به تقویت روابط بین نیروهای نظامی [کشورها] ادامه خواهد داد تا در عین بهره‌گیری از مهارت‌ها و دیدگاه‌های منحصربه‌فرد متحدان و هم‌پیمانان آمریکا، ظرفیت آن‌ها برای ارتقاء امنیت سایبری جمعی ما را گسترش دهد. وزارت امور خارجه همچنان به هماهنگ‌سازیِ تلاش‌های کل دولت خواهد پرداخت تا از این مسئله اطمینان حاصل کند که اولویت‌های ظرفیت‌سازی [دولت] فدرال به‌لحاظ راهبردی با منافع ایالات متحده، متحدان و هم‌پیمانان او هم‌سو است.

هدف استراتژیک ۳/۵: گسترش توانایی ایالات متحده برای کمک به متحدان و شرکای خود

همانطور که حملات سایبری اخیر علیه کاستاریکا، آلبانی و مونته‌نگرو نشان داده است، کشورها در هنگام مواجهه با یک حمله سایبری شدید، احتمالاً از متحدین و هم‌پیمانان خود برای تحقیق تفحص و واکنش‌نشان دادن نسبت به آن و ترمیم آسیب‌ها و صدمات آن استمداد می‌کنند. این حمایت علاوه‌براینکه به آن کشور در جهت واکنش و ترمیم صدمات وارده کمک می‌کند، بلکه سیاست خارجی و اهداف امنیت سایبری ایالات متحده را نیز پیش می‌برد. همکاری نزدیک با متحد یا شریکِ آسیب‌دیده، نشان‌دهنده همبستگی در مواجهه با فعالیت‌های خصمانه بوده و می‌تواند فرآیند کشف رفتارهای خلاف هنجارِ دولت‌ها و پیگرد آن را سرعت ببخشد.

دولت خط‌مشی‌هایی را تدوین خواهد کرد که مشخص کند که چه زمان ارائهٔ اینگونه حمایت‌ها به کشورهای هم‌پیمان در راستای منافع ملی است؛ همچنین سازوکارهایی برای تشخیص اینکه از منابع کدام سازمان و کدام بخش باید برای این هدف استفاده کند طراحی کرده و در صورت نیاز، به‌سرعت در پی رفع موانع مالی و اجراییِ ارائهٔ اینگونه حمایت‌ها خواهد بود. پشتیبانی عملیاتی به‌عنوان یک مثال، ایالات متحده تلاش سازمان پیمان آتلانتیک شمالی (ناتو) را برای ایجاد قابلیت پشتیبانی از حوادث سایبری مجازی رهبری می‌کند که به متفقین این امکان را می‌دهد تا به طور مؤثرتر و کارآمدتری از یکدیگر در پاسخ به فعالیت‌های مخرب سایبری مهم حمایت کنند.

هدف راهبردی ۴ / ۵: ایجاد ائتلاف برای تقویت هنجارهای جهانی رفتار مسئولانه دولت

همهٔ اعضای سازمان ملل متحد به‌لحاظ سیاسی متعهد به تأیید و پیروی از هنجارهای رفتار مسئولانه دولت‌ها در فضای سایبری در زمان صلح شده‌اند؛ هنجارهایی از جمله خودداری از آن دسته از عملیات سایبری که علیرغم تعهدات کشورها در برابر قوانین بین‌المللی، به‌طور عمدی به زیرساخت‌های حیاتی آسیب می‌رساند.

اگرچه عوامل متخاصم می‌دانند که اینگونه تعهدات برای آن‌ها الزام‌آور نیست، اما نفوذ [و اعتبار] فزایندهٔ این چارچوب باعث شده است که کشورهایی که برخلاف آن عمل کنند، با واکنش دیگران مواجه شوند. حلقه‌ای از کشورها در حال شکل‌گیری و تقویت است که به‌صورت جمعی بیانیه‌هایی در محکوم‌کردن و متهم‌کردن [عوامل تهدید] منتشر می‌کنند؛ بیانیه‌هایی که به‌شیوه‌ای دیپلماتیک کشورها [ی متخلف] را محکوم کرده و درعین‌حال، باعث تحکیم پیمانی که حول یک «فضای سایبری پایدار» شکل گرفته است، خواهد شد.

یکی از محورهای فعال و به‌روزِ دیپلماسی ایالات متحده آمریکا مسئول‌دانستنِ دولت‌ها در صورت عدم پایبندی به تعهدات خود است. ما برای کنترل مؤثر دشمنان و مقابله با فعالیت‌های متخاصمانه‌ای که تا آستانهٔ درگیری مسلحانه پیش می‌روند، با متحدان و شرکای خود همکاری خواهیم کرد تا احکام متهمان را با [تنبیهات و] پیامدهای معنادار همراه کنیم. این تلاش‌ها مستلزم استفاده مشترک از همه ابزارهای حکومت‌داری - از جمله انزوای دیپلماتیک، هزینه‌های اقتصادی، عملیات ضد سایبری و اجرای قانون، و یا تحریم‌های قانونی و غیره - است.

هدف راهبردی ۵/۵: زنجیره‌های تأمین جهانی ایمن برای اطلاعات، ارتباطات و محصولات و خدمات فناوری عملیاتی

زنجیره‌های تأمین پیچیده و به‌هم‌پیوسته و جهانی، محصولات و خدماتی در حوزهٔ تکنولوژی‌های اطلاعاتی، ارتباطی و عملیاتی تولید می‌کنند که اقتصاد ایالات متحده را نیرو می‌بخشند. ما به شبکه رو به گسترشی از تأمین‌کنندگان خارجی وابسته هستیم؛ از مواد خام و عناصر اساسی گرفته تا محصولات و خدمات نهایی - اعم از مجازی و فیزیکی. این وابستگی به محصولات و خدمات مهم خارجی که در دست تأمین‌کنندگان غیرقابل‌اعتماد هستند، منابع متعددی از ریسک سیستمی را به اکوسیستم دیجیتال ما اضافه می‌کند.

کاهش این ریسک مستلزم همکاری بلندمدت و استراتژیک بین بخش‌های دولتی و خصوصی در داخل و خارج از کشور است تا زنجیره‌های تأمین جهانی را مجدداً متعادل کرده و آن‌ها را شفاف‌تر، ایمن‌تر، تاب‌آورتر و قابل اعتمادتر کند.

ورودی‌ها، اجزا و سیستم‌های حیاتی باید در حد امکان در داخل کشور و یا در همکاری نزدیک با متحدین و شرکایی توسعه داده شوند که با ما دیدگاه مشترکی در مورد اینترنت باز، رایگان، جهانی، قابل اعتماد و ایمن دارند. با تکیه بر راهبرد ملی ایمن‌سازی [تکنولوژیِ] 5G[1]، ما با شرکای خود برای توسعه زنجیره‌های تأمین ایمن، قابل اعتماد و قابل اعتماد برای شبکه‌های بی‌سیم 5G و نسل بعدی از جمله از طریق شبکه‌های دسترسی آزاد رادیویی[2] و طرح‌های مشترک برای تنوع بخشیدن

1 National Strategy to Secure 5G
2 Open Radio Access Networks (Open RAN)

به تأمین‌کنندگان همکاری می‌کنیم. از جملهٔ این تلاش‌ها می‌توان به آزمایش وزارت دفاع آمریکا برای پیاده‌سازی شبکه دسترسی آزاد رادیویی در چندین پایگاه خود - که دارای پروژه‌های انبار هوشمند و لجستیک چند میلیون دلاری هستند - و کار اداره ملی مخابرات و اطلاعات[1] برای تسریع توسعه و به‌کارگیری شبکه‌های باز، انتقال‌پذیر و استاندارد از طریق صندوق نوآوری زنجیره تأمین [شبکه‌های] بی‌سیم عمومی اشاره کرد. تسرّیِ این مدل به قلمروِی سایر تکنولوژی‌های حیاتی نیازمند همکاری بلندمدت و استراتژیک بین بخش‌های دولتی و خصوصی در داخل و خارج از کشور است، تا زنجیره‌های تأمین جهانی را دوباره متعادل کرده و آن‌ها را ایمن‌تر، تاب‌آورتر و قابل اعتمادتر کند. قانون فراحزبی [توسعه] زیرساخت، فرمانِ «آمریکا را بسازید، آمریکا را بخرید» را برای پروژه‌هایی که بودجه فدرال دارند - از جمله زیرساخت‌های دیجیتال - صادر کرده است. دولت به‌واسطهٔ فرمان اجرایی شماره ۱۴۰۱۷ - «زنجیره‌های تأمین آمریکا» -، قانون «تراشه‌ها و علم»، و قانون کاهش تورم، توانسته است ابزارهای راهبردی جدیدی در حوزه صنعت و نوآوری طراحی کند که به بازگرداندن چرخهٔ تولید کالاهای اساسی به ایالات متحده و شرکای نزدیک آن کمک کرده و درعین‌حال امنیت زنجیره‌های تأمین در تکنولوژی‌های اطلاعاتی و صنایع پیشرفته را ارتقاء می‌بخشد.

ایالات متحده با متحدان و شرکای خود به روش‌های مختلفی از جمله مشارکت‌های منطقه‌ای -چارچوب اقتصادی هند-اقیانوسیه[2]، کارگروه تکنولوژی‌های چهارگانهٔ نوظهور و حساس[3]، و کمیسیون تجارت و تکنولوژی[4] - برای شناسایی و پیاده‌سازی بهترین روش‌ها در مدیریت

1 National Telecommunications and Information Administration's (NTIA)
2 Indo-Pacific Economic Framework
3 the Quad Critical and Emerging Technology Working Group
4 Trade and Technology Council (TTC)

برون‌مرزی ریسکِ زنجیره‌های تأمین و تلاش برای تغییر مسیر آن‌ها به سمتِ کشورهای هم‌پیمان و فروشندگان قابل‌اعتماد همکاری خواهد کرد. اولویت ما در این مسیر، فرصت‌هایی است که برای ارتقاء سطح اعتماد نسب به عملکرد قابل‌پیش‌بینی تکنولوژی‌های دیجیتال و جذب کشورها برای حمایت از دیدگاهی مشترک در مورد اینترنت باز، رایگان، جهانی، تبادل‌پذیر، قابل‌اعتماد و ایمن به‌وجود می‌آید. وزارت امور خارجه از صندوق بین‌المللی امنیت فناوری و نوآوری[1] برای حمایت از طراحی و سرعت‌بخشی به [فعالیت] زنجیره‌های تأمین امن و متنوع برای نیمه‌هادی‌ها و مخابرات کمک خواهد گرفت. در نهایت، از طریق اجرای فرمان اجرایی شماره ۱۳۸۷۳ - «ایمن‌سازی زنجیره تأمین خدمات و فناوری اطلاعات و ارتباطات» - و همچنین فرمان اجرایی شماره ۱۴۰۳۴ - «حفاظت از داده‌های حساس آمریکایی‌ها در برابر دشمنان خارجی» - با خطرات غیرقابل‌قبول و غیرضروری که امنیت ملی ما را از جانب تکنولوژی‌های اطلاعات و ارتباطات و خدماتی که تحت کنترل یا نفوذ دولت‌های متخاصم هستند، تهدید می‌کنند مبارزه خواهیم کرد.

1 International Technology Security and Innovation Fund

عملیاتی کردن

عملیاتی کردن

تحقق اهداف راهبردیِ تعیین‌شده در این سند مستلزم تمرکز جدی بر مرحلهٔ «عملیاتی کردن» است. دفتر فرماندهی سایبری ملی - تحت نظارت شورای امنیت ملی و با هماهنگی سازمان مدیریت و بودجه - اجرای این راهبرد را مدیریت خواهد کرد. این دفتر در همکاری با برخی مجموعه‌های بین‌سازمانی اقدام به طراحی و انتشار طرحی اجرایی برای تعیین خطوط فدرال اقدامات لازم برای پیاده‌سازی این راهبرد خواهد کرد. در مواردی که اجرای این راهبرد مستلزم بازنگری در خط‌مشی‌های موجود و یا تدوین خط‌مشی جدید باشد، شورای امنیت ملی این فرآیند را با کمک روالِ تشریح‌شده در بیانیه امنیت ملی شماره ۲ - «نوسازی سیستم شورای امنیت ملی» - رهبری خواهند کرد.

ارزیابی اثربخشی

دولت فدرال در اجرای این استراتژی رویکردی داده‌محور را در پیش خواهد گرفت و میزان سرمایه‌گذاری‌های انجام‌شده، پیشرفت اجرایی، نتایج نهایی و نهایتاً اثربخشی این تلاش‌ها را اندازه‌گیری خواهیم کرد. دفتر فرماندهی سایبری ملی، در هماهنگی با شورای امنیت ملی، سازمان مدیریت و بودجه، و سایر ادارات و سازمان‌های ذیربط، اثربخشی این راهبرد را ارزیابی کرده و در این مورد و نیز در مورد اقدامات بعدی برای

دستیابی به اهدافِ تعریف‌شده، به‌صورت سالانه به رئیس‌جمهور، معاون رئیس‌جمهور در امور امنیت ملی، و کنگره گزارش خواهیم داد.

درس‌گرفتن از تجربیات

یکی از اولویت‌های دولت کنونی درس‌گرفتن از سوانح سایبریِ گذشته و استفاده از این تجربیات در اجرای راهبرد کنونی است. هیئت نظارت بر امنیت سایبری[1] اولین بررسی خود را در مورد نقطهٔ آسیب‌دیده‌ای موسوم به «Log۴j» در تابستان ۲۰۲۲ انجام داد و در آن گزارشی موثق و جامع از کل ماجرا - از لحظهٔ کشف این نقطهٔ آسیب‌پذیری، تا شکل‌گیری بزرگ‌ترین واکنش به سوانح سایبری در طول تاریخ - تهیه کرد. این هیئت همچنین - بر اساس کشفیات خود - توصیه‌هایی روشن و قابل اجرا به فعالان حوزه صنعت، سازمان‌های فدرال و جامعهٔ توسعه‌دهندگان نرم‌افزار ارائه کرد؛ تا از جامعه در آینده بهتر محافظت شود.

پس از کامل‌شدن بررسی‌های این هیئت، دولت فدرال توصیه‌های آن را - در صورت امکان از طریق اقدامات بالادستی - قالب با بهبود عملیات خود از طریق اقدامات اجرایی در صورت امکان، مورد توجه قرار می‌دهد و در صورت لزوم با کنگره برای افزایش اختیارات همکاری خواهد کرد. علاوه‌براین، سازمان‌های فدرال توصیه‌ها و پیشنهادات هیئت نظارت بر امنیت سایبری که به مدافعان شبکه در بخش خصوصی ارائه می‌شود را نیز پیگیری و تقویت خواهند کرد. علاوه بر این هیئت نظارت، تلاش ملی گسترده‌تری نیز برای درس‌گرفتن از حوادث سایبری مورد نیاز است. نهادهای تنظیم‌گر تشویق می‌شوند که در چارچوب‌های فعالیت‌های نظارتی خود، فرآیندهای بررسی سوانح [سایبری] را نیز بگنجانند.

1 Cyber Safety Review Board (CSRB)

سازمان امنیت سایبری و زیرساخت (سیسا) و سایر مجریان قانون نیز تشویق می‌شوند که فرآیندهایی را برای استخراج منظم درس‌های آموخته‌شده از تحقیقات و فعالیت‌های واکنش به حادثه ایجاد کنند. از شرکت‌های خصوصی نیز انتظار می‌رود که این بررسی‌ها را انجام دهند و یافته‌های خود را - برای ارتقاء فرآیند عملیاتی‌کردن این راهبرد - به اشتراک بگذارند.

سرمایه‌گذاری

حفظ اینترنت باز، رایگان، جهانی، قابل همکاری، قابل اعتماد و ایمن و ایجاد یک اکوسیستم دیجیتالی قابل دفاع و تاب‌آورتر نیازمند سرمایه‌گذاری بلندمدت و فرانسلی توسط دولت فدرال، متحدان و شرکای آن، و بخش خصوصی است. بسیاری از اقدامات فدرال مندرج در این راهبرد به منظور افزایش سرمایه‌گذاری بخش خصوصی در امنیت، تاب‌آوری، بهبود همکاری و تحقیق و توسعه است. سرمایه‌گذاری‌های هدف‌مند برای افزایش قابلیت‌های اضطراری سازمان‌های فدرال و حمایت از ذی‌نفعان در بخش خصوصی، ضروری است. برای هدایت این سرمایه‌گذاری‌ها، دفتر فرماندهی سایبری ملی و سازمان مدیریت و بودجه مشترکاً دستورالعمل‌های سالانه را در مورد اولویت‌های بودجه امنیت سایبری به ادارات و سازمان‌ها ابلاغ می‌کنند تا رویکرد استراتژیک دولت را پیش ببرند. دفتر فرماندهی سایبری ملی در همکاری با سازمان مدیریت و بودجه تناسب بودجه‌های پیشنهادی برای بخش‌ها و سازمان‌های مختلف با اهدافی که در این راهبرد برای آن‌ها تعیین شده است را بررسی می‌کند. دولت ما به کمک کنگره منابع مالی فعالیت‌های حوزه امنیت سایبری را تأمین می‌کند تا از روند سریع تغییرات ذاتی در اکوسیستم سایبری عقب نیفتند.

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

حوزهٔ فضای مجازی به اندازهٔ انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانهٔ پر از آب خروشان است که می‌آید و دائماً هم بر آب آن افزوده و خروشان‌تر می‌شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه‌کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می‌شود فرصت؛ اگر رهایش کنیم و برنامه‌ای برای آن نداشته باشیم، می‌شود یک تهدید...

csri.majazi.ir