استراتژی سایبری ملی ایالات متحده آمریکا

(همراه با مروری بر مبانی و اهداف)

کد موضوعی: ۲۷۰
شماره مسلسل: ۱۶۷۸۲
آذرماه ۱۳۹۸

معاونت پژوهش‌های اجتماعی ـ فرهنگی
دفتر: مطالعات آموزش و فرهنگ

به‌نام خدا

فهرست مطالب

مقدمه مرکز پژوهش‌ها

طرح مسئله

۱. طی دو دهه گذشته به‌تدریج نگارش اسناد بالادستی در ایران تبدیل به یک رویه شده است.[۱] این اقدام که در روزهای نخست با تأیید و همراهی بسیاری روبه‌رو شد، در گذر زمان- و پس از آشکار شدن برخی تأثیر و تأثرات تصویب چنین اسنادی در جامعه- موافقان و مخالفانی پیدا کرده است. عده‌ای از منتقدان، کارایی چندانی برای اسناد به نگارش درآمده قائل نبوده و رغبت به تصویب اسناد این‌چنینی را ناشی از فرم‌گرایی در سیاستگذاری می‌دانند. در مقابل، گروهی از موافقان، دستیابی به توانایی تهیه و تدوین اسناد را به‌مثابه کسب تکنولوژی تولید سند، یک دستاورد به‌شمار می‌آورند و ناکامی‌های احتمالی این اسناد را به عدم التزام مجریان نسبت می‌دهند.

اگرچه در نگاه اول، انتقاد به فرم‌گرایی را می‌توان نشانه گرایش به محتوا دانست، اما مسئله به این روشنی و سهولت نیست، بلکه شاید بتوان ادعا کرد پاشنه آشیل تنظیم و تدوین یک سند سیاستی، تفکیک فرم و محتوای آن است. بنابراین، چنانچه فرم و محتوای یک سند در تطابق کامل با یکدیگر نباشند، اصولاً نگارش سند غیرممکن است و خروجی کار، متنی دوپاره شامل «مبانی و آرمان‌ها» به‌علاوه «فهرستی از مطالبات غیرقابل‌وصول» خواهد بود.[۲]

درنتیجه، کانونی‌ترین ابهام در زمینه چنین اسنادی مربوط به چیستی و ماهیت یک سند سیاستی است، و اینکه در تهیه یک سند چه مواردی را می‌توان مطالبه کرد و طلب چه مواردی، سند را از حَیّز انتفاع ساقط خواهد کرد. بر این اساس، به‌نظر می‌رسد یک سند سیاستی خوب باید اولاً از ارتباط مستقیمی با ساخت اقتصادی و سیاسی کشور برخوردار بوده و برآمده از فرهنگ و تاریخ جامعه و در امتداد آن باشد.[۳] ثانیاً در میانه گذشته و آینده قرار گیرد و مسیر طبیعی حرکت جامعه را تسهیل و تصریح سازد.

برای روشن شدن موضوع به بیان دو تجربه تاریخی می‌پردازیم. تلویزیون از بدو فراگیر شدن خود در ایران یک رسانه رایگان بود که با هدف تغییر فرهنگ سنتی مردم و ترویج فرهنگ مدرن آغاز به‌کار کرده و سریال‌ها و آثار سینمایی خارجی را با دوبله فارسی در اختیار مخاطبان قرار می‌داد. با پیروزی انقلاب اسلامی تردیدی اساسی در ماهیت اقتصادی و تولیدی تلویزیون پدید نیامد و تنها مقرر شد این بار تلویزیون- به‌مثابه یک دانشگاه عمومی- فرهنگ دینی و انقلابی را ترویج کند. گرایش مردم ایران به چنین صورتی از مصرف تلویزیونی در درازمدت، دشمنان ایران را- که در درون مرزهای خود شبکه‌های تلویزیونی را در قبال دریافت هزینه و زیرنویس برنامه‌های خارجی پخش می‌کنند- ناگزیر کرد برای جذب مخاطبان

ایرانی مبادرت به پخش برنامه‌های رایگان با دوبله فارسی نمایند. آیا در چنین شرایطی یک سند سیاستی معتبر می‌تواند «واگذاری تلویزیون به بخش خصوصی برای ارائه خدمات باکیفیت‌تر در قبال دریافت وجه» را پیگیری نماید؟

مثال دیگر، به فرایند گسترش «پیاده‌روی اربعین» باز می‌گردد که به صرف حمایت حداقلی حاکمیت در حوزه‌های رسانه، حمل‌ونقل، صدور روادید و... زمینه حضور یک جمعیت چند میلیون نفری در این مراسم فراهم شده است، درحالی‌که در بسیاری از حوزه‌ها با صرف وقت و هزینه و سیاستگذاری‌های به‌مراتب گسترده‌تر، کسری از این همراهی و مشارکت مردمی ممکن نشده است.

این در حالی است که غالب اسناد سیاستی در جوامع غیرصنعتی- و به‌عبارتی توسعه‌نیافته- فاقد چنین ساختی هستند. چراکه این‌گونه جوامع، صورت نهادها و ساختارهای مدرن را اخذ کرده‌اند اما بدون آنکه از ارزش‌های بنیادین و تاریخی خود - که ریشه در سنت‌ها دارد- دست بکشند طالب دستاوردها و شیفته تقلید از هنجارهای جوامع توسعه‌یافته هستند. بدین‌ترتیب، سندهای به نگارش درآمده در این جوامع، لیستی از همه حوایج چپ‌گرا، راست‌گرا، بوم‌گرا، سنت‌گرا و ... است و اصولاً نگارندگان سند - که آینه مردم اما در جایگاه قدرت هستند- از اتخاذ هر تصمیم اساسی که نتیجه آن از دست رفتن بخشی از خوبی‌های متصور است خودداری می‌کنند؛[۴] در شرایطی که اتخاذ موضع راهبردی، از ویژگی‌های یک سند خوب است.

۲. به موازات تحولات کمّی و کیفی پیش‌گفته در حوزه سیاستگذاری، در سال‌های اخیر موضوع فضای مجازی یکی از دغدغه‌های اصلی جامعه ایرانی- اعم از مردم، فعالان فرهنگی، گروه‌های مرجع اجتماعی و مسئولان- را تشکیل داده و تأسیس نهادهایی مانند پلیس فتا[۵] و شورای عالی فضای مجازی[۶] را به‌دنبال داشته است. به‌این‌ترتیب، فراز و فرودهای این حوزه- ازجمله در زمینه شبکه ملی اطلاعات،[۷] فیلترینگ، ساماندهی پیام‌رسان‌های اجتماعی[۸] و ...- پرسش‌های تعیین‌کننده‌ای را پیش‌روی جامعه قرار داده است که همچنان بدون پاسخ مانده‌اند. اهم پرسش‌های مذکور بدین شرح است:

- آیا فضای مجازی را می‌توان صرفاً به‌عنوان یک بستر فناورانه و تکنولوژیک دیده و آن را در حیطه قلمرو وزارت ارتباطات و فناوری اطلاعات منحصر کرد؟ یا آنکه فضای مجازی اساساً یک فضای تهدیدآمیز یا دست‌ِکم ناشناخته است و باید هرگونه سیاستگذاری در این حوزه ذیل نهادهای امنیتی تعریف شود؟ نقش ذی‌نفعان این عرصه- ازجمله اپراتورهای تلفن همراه و دیگر شرکت‌های انتقال داده- در سوق دادن نگاه‌ها به جوانب مختلف چه می‌تواند باشد؟
- چالش‌های امنیتی کلیدی در حوزه فضای مجازی مربوط به حیطه عمومی و کلان‌داده‌ها[۹] است یا حریم خصوصی و اطلاعات شخصی؟ منافع جریانات مختلف که از این فضا برای بازاریابی اقتصادی و

شکل‌دهی سیاسی افکار عمومی بهره می‌برند در این زمینه چه اقتضائاتی دارد؟ آیا این جریانات می‌توانند منافع شخصی و جریانی خود را به‌عنوان مصلحت عمومی جامعه القا کنند؟

- آیا در سیاستگذاری عرصه فضای مجازی جایی برای تأکید بر مناقشات سیاسی میان کشورها ازجمله طرح ایده‌های خصومت، رقابت و ... وجود دارد یا آنکه اصولاً چنین طرح بحث‌هایی ناشی از توهم توطئه است؟
- آیا فضای مجازی یک بستر اقتصادی- تجاری یا اجتماعی- سیاسی یا تفریحی- فراغتی است؟ اگرچه کمابیش نشانه‌هایی برای تصدیق همه موارد وجود دارد؛ اما در شرایط کنونی کشور ما کدام وجه بر این فضا غلبه دارد و این غلبه متضمن چه ضرورت‌هایی برای سیاستگذاری این حوزه است؟
- چنانچه فضای مجازی را یک بستر اقتصادی- تجاری بدانیم، چه پیامدهایی را به‌دنبال خواهد داشت؟ آیا ارزهای دیجیتالی[۱۰] مانند بیت کوین[۱۱] فراگیر شده و اقتصاد جهان را دگرگون خواهند ساخت؟ آیا چنین ارزهایی به ابزاری برای پولشویی و تأمین مالی تروریسم و به‌طور کلی جابه‌جایی منابع پولی مجرمان بدل خواهند شد؟[۱۲] آیا تجارت در فضای مجازی، فعالان اقتصادی و کسب‌وکار آنها در فضای حقیقی را با اختلال مواجه خواهد ساخت؟ آیا فرصت‌های اقتصادی جدید به ظرفیت‌های پیشین افزوده می‌شود یا جایگزین آنها خواهد شد؟[۱۳]
- چنانچه فضای مجازی را یک بستر اجتماعی- سیاسی قلمداد کنیم تبعات آن در حوزه کنشگری‌های سیاسی و اجتماعی ازجمله امنیت انتخاباتی، آسایش روانی، تحریک گسل‌های قومی، زبانی، مذهبی، جنسی، صنفی- حرفه‌ای و... چیست؟
- چنانچه فضای مجازی را یک بستر تفریحی- فراغتی بدانیم تبعات آن در حوزه فرهنگ و سبک زندگی چیست و حکومت چه مسئولیتی در این زمینه دارد؟
- آیا توسعه زیرساخت‌های لازم جهت بهره‌مندی آحاد مردم از فضای مجازی در شهرها و روستاهای کشور- نسبت به دیگر زیرساخت‌های مورد نیاز ازجمله در زمینه حمل‌ونقل، آب شرب، آموزش عمومی، مدیریت بحران، محیط زیست و...- در اولویت قرار دارد؛ چه چیزی اولویت داشتن یا نداشتن آن را تعیین می‌کند؟ و ...

۳. براساس مقدمات فوق، و به‌منظور آشنایی با پاسخ‌های دیگر جوامع به پرسش‌های مزبور به‌نظر می‌رسد مروری بر سند سایبری ایالات متحده که در سپتامبر ۲۰۱۸ انتشار یافته، خالی از فایده نیست. علاوه بر این باید عنایت داشت که فضای مجازی و مسائل حاشیه‌ای آن برای ایالات متحده آمریکا نیز کم نبوده است؛ برخی از این موارد عبارتند از:

- نقش‌آفرینی توییتر و یوتیوب در فتنه سال ۱۳۸۸ ایران،[۱۴]
- شکست ویروس استاکس‌نت که با همکاری آمریکا و رژیم صهیونیستی طراحی شده بود،[۱۵]
- انتشار اسناد محرمانه توسط سایت ویکی‌لیکس که از همکاری چینی‌ها، تایوانی‌ها و ... بهره می‌برد،[۱۶]

- فرار ادوارد اسنودن به روسیه که به افشای مواردی نظیر شنود مکالمات سران برخی کشورهای اتحادیه اروپا انجامید،[۱۷]
- بازجویی چند ساعته هیلاری کلینتون به‌دلیل ابهامات درباره برخی ایمیل‌های او،[۱۸]
- ادعای مداخله روسیه در انتخابات ریاست جمهوری آمریکا به نفع دونالد ترامپ[۱۹] و ... .

۴. یکی از تمایلات طبیعی فعالان عرصه سیاست‌پژوهی و قانونگذاری و به‌طور خاص، نمایندگان مجلس شورای اسلامی، اطلاع از تجارب سیاستگذاری در سایر جوامع است؛ مسئله‌ای که با توجه به افزایش نگارش اسناد بالادستی و ابلاغ سیاست‌های کلان در حوزه‌های مختلف طی سالیان اخیر، اهمیت مضاعفی یافته است. این تمایل به‌ویژه در حوزه‌های نوظهور و پر مناقشه‌ای مانند حوزه فضای مجازی از شدت بیشتری برخوردار است. بر این اساس، مرکز پژوهش‌های مجلس شورای اسلامی اقدام به انتشار ترجمه «سند استراتژی سایبری ملی ایالات متحده آمریکا» کرده است. با این وجود، بهره‌برداری کافی از سند مذکور- که نمونه کامل یک سند سیاستی قلمداد می‌شود- نیازمند بیان نکاتی درباره مبانی شکل‌گیری این سند است؛ مبانی کلیدی که اگرچه در بخش مجزایی ذکر نشده‌اند اما در سراسر متن آن به چشم می‌آیند.

مبانی نظری سند استراتژی سایبری ایالات متحده

۵. ظهور رنسانس یا دوره نوزایی در قرن پانزدهم میلادی سبب پدید آمدن جنبش فرهنگی مهمی شد که زنجیره‌ای از انقلابات علمی، اصلاحات مذهبی و تحولات هنری در اروپا را به‌دنبال داشت. عصر روشنگری در قرون هفده و هجده اروپا نیز حامل پیام اصلی مدرنیته بود که درحقیقت اندیشه‌های برآمده از عصر رنسانس را تبیین کرده و توسعه بخشید. درنتیجه، اگرچه نمی‌توان سخن از رابطه‌ای علّی به میان آورد اما روشنگری، بستر جنبشی فکری- فلسفی در تاریخ تفکر غرب بود که انقلاب‌های عظیمی را در عرصه علم و فلسفه به‌وجود آورد و درنهایت باعث از میان رفتن کامل جهان‌بینی قرون وسطایی شد.[۲۰]

به‌تبع تحولات شگرف فوق‌الذکر، در سال ۱۶۸۸م. انقلاب انگلستان به ثمر نشست و پارلمان این کشور موفق شد نظام سیاسی کشور را به پادشاهی مشروطه تبدیل کند. بعدها و در سال ۱۷۷۶م. مستعمرات آمریکایی که برای دوره‌ای طولانی به بریتانیا وفادار بودند، استقلال خود را از این کشور اعلام کرده و سیاست‌های مالیاتی که انگلیسی‌ها بر آنها تحمیل می‌کردند را نقض حقوق طبیعی خویش دانستند. نتیجهٔ به ثمر رسیدن انقلاب آمریکا، در سال ۱۷۸۷ میلادی نگارش و تصویب قانون اساسی ایالات متحده بود. منشور حقوق ایالات متحده نیز به‌سرعت در سال ۱۷۸۹ میلادی تصویب شد و حقوق طبیعی مشخصی را براساس ایدئال‌های لیبرالی به شهروندان خود اعطا کرد.

بنابراین، شاید اولین دولت مدرنی که برپایه اصول لیبرالی بنیان نهاده شد، ایالات متحده آمریکا بود که در اعلامیه استقلال خود اعلام کرد تمام انسان‌ها برابر آفریده شده و خالق‌شان از یک سری حقوق بهره‌مندشانکرده است که ازجمله این حقوق، «زندگی، آزادی و پیگیری سعادت و خوشبختی» است.

چند سال بعد، انقلاب فرانسه بود که بر میراث اشرافی‌گری این کشور غلبه کرد و به اولین کشور در تاریخ تبدیل شد که حق رأی برای همه مردان را به رسمیت شناخت. شعارهای «آزادی»، «برابری» و «برادری»[۲۱] آرمان‌های اساسی انقلاب فرانسه بودند. در سال‌های منتهی به پیروزی این انقلاب شعارهای دیگری نیز مطرح بود، اما هیچ‌کدام به اندازه این سه‌گانه مورد توجه قرار نگرفتند. «آزادی» شعاری بود که در آن سال‌ها بیشترین محبوبیت را داشت و در اعلامیه حقوق بشر و شهروندی ۱۷۸۹ میلادی فرانسه تعریف شد. سپس کلمه «برابری» به آن اضافه گشت و در اعلامیه حقوق بشر ۱۷۹۳ میلادی مورد تصریح واقع شد. در آخر نیز کلمه «برادری» در سال ۱۷۹۵ میلادی یعنی هنگام نگارش سومین قانون اساسی فرانسه، در صدر منشور حقوق و وظایف شهروندی قرار گرفت و این شعار را تکمیل ساخت.[۲۲]

بسیاری از فیلسوفان دوره روشنگری به بیان دیدگاه‌های خود درباره شعارهای مذکور پرداخته‌اند و از این جهت، همواره اختلاف‌نظرهایی درباره *تقدم* و *تأخر* این آرمان‌ها وجود داشته است. به‌عنوان مثال، جان لاک اعتقاد داشت که حق مالکیت تنها از راه کار کردن حاصل می‌شود. وی همچنین معتقد بود که حق مالکیت بر دولت مقدم است و دولت حق ندارد به‌طور خودسرانه در دارایی‌های افراد دخالت کند. به اعتقاد لاک در وضع طبیعی، همه مردم برابر و مستقل هستند و هرکسی این حق طبیعی را دارد که از «زندگی، سلامتی، آزادی و دارایی» خود دفاع کند؛ امری که بازتاب آن به‌صراحت در بخشی از رساله دوم اعلامیه استقلال آمریکا با ذکر عبارت «زندگی، آزادی و پیگیری خوشبختی» آمده است. در مقابل، ژان ژاک روسو- فیلسوف فرانسوی- برابری را جوهر آزادی می‌دانست و تجار را به بی‌بهره بودن از میهن‌پرستی متهم می‌کرد، چرا که معتقد بود ایشان منفعت را بر آزادی ترجیح می‌دهند.[۲۳] برتراند راسل نیز دمکراسی را به دو گونه سیاسی و اقتصادی تقسیم کرده و معتقد بود ممانعت از کاربرد خودسرانه قدرت، علاوه بر شرایط سیاسی نیازمند شرایط اقتصادی خاصی نیز هست.[۲۴]

یکی از آثار درخشانی که مربوط به همین دوره سرگردانی است و توأمان «گرایش به برابری و آزادی» و در عین حال «نگرانی از غلبه یکی از شعارهای آزادی یا برابری» را نشان می‌دهد کتاب «تحلیل دمکراسی در آمریکا» اثر «آلکسی دوتوکویل» است.[۲۵] هارولد ج. لاسکی[۲۶] در مقدمه‌ای که بر این اثر نگاشته است، می‌گوید:

هنگامی که توکویل تحت عنوان توجه به معنویات دست ملتمس خود را به جانب مذهب دراز می‌کرد، در حقیقت انگیزه او بیشتر از آنکه معلول توجه وی به معنویات باشد به سبب ترس و نگرانی وی از مساواتی بود که دمکراسی به دنبال داشت. ایمان و عقیده قلبی توکویل آن نبود که مذهب می‌تواند باعث تعالی توده مردم

شود، بلکه او برای رهاندن آزادی از چنگال نتایج قهری مساوات به مذهب متوسل می‌گردید. [...] توکویل به این مسئله اعتقاد داشت که مساوات و برابری در جامعه اجتناب‌ناپذیر است ولی در عین حال مساوات بدون وجود آزادی در نظر او غیرقابل تحمل بود. تردیدی نمی‌توان داشت که توکویل با هر شکل از حکومت استبدادی مخالف بوده است، ولی در این هم نمی‌توان تردید کرد که او نسبت به هر اساسی که موجب واگذاری مسئولیت‌های حکومتی به توده مردم باشد، احساس نگرانی داشته است. توکویل از یک سیستم حکومتی که در آن پول، زمام حکومت را به‌دست گرفته و رندانه از انجام وظایف حکومتی، سر باز زند، بیمناک بود؛ ولی در عین حال از هرگونه توسعه و افراط در اجرای تقسیم کار تا جایی که کارگران به قیمت تأمین رفاه و آسایش مادی ناچار گردند تکالیف و موقعیت انسانی خود را ترک کنند و وادار به قبول وضعی شوند که به‌صورت بنده و غلام دستگاه درآیند، احساس بیم و هراس می‌کرد.[۲۷]

همان‌طور که ملاحظه می‌شود توکویل با هر شکلی از حکومت استبدادی مخالف بود و ترکیبی از مساوات و آزادی را طلب می‌کرد؛ ترکیبی که با وساطت مذهب و معنویات قابل جمع می‌نمود. وی نتیجه طبیعی دمکراسی را مساوات می‌دانست؛ مساواتی که می‌تواند از طریق توسعه و افراط در اجرای تقسیم کار، افراد را به بنده و غلام دستگاه حکومتی تبدیل کرده و آزادی آنها را سلب کند. و در مقابل، تصور می‌کرد چنانچه بازار (منطق محاسبه پولی) زمام حکومت را به‌دست گیرد حکومت از انجام وظایف خود، سر باز زده و مسئولیت‌های خود را به توده مردم واگذار خواهد کرد.

به هر روی، در گذر زمان میان دو شعار آزادی و برابری فاصله‌هایی به‌وجود آمد؛ عده‌ای که برابری را ایده اساسی روشنگری می‌دانستند، تأمین حداقل‌های اقتصادی را وظیفه دولت تلقی کرده و شرط رسیدن به آزادی را ایجاد سطحی از برابری اقتصادی تعریف کردند. در مقابل، کسانی که آزادی را ایده اساسی روشنگری می‌دانستند استدلال می‌کردند مادامی که مردم برای تأمین نیازهای خود به دولت وابسته هستند، آزادی واقعی به‌دست نمی‌آید و درواقع، برابری واقعی انسان‌ها نتیجه قهری آزادی از دولت و مداخله آن است. به همین ترتیب، جدال دو ایده «آزادی» و «برابری» منجر به تشکیل دو سیستم مجزای اداره جامعه شد.[۲۸] نوبرتو بابیو در این زمینه می‌گوید:

می‌توان به‌درستی برابری‌طلبان را کسانی خواند که اعتقاد دارند ارزش تأکید بر اشتراکات در شکل دادن یک جامعه خوب بسیار بیشتر از تأکید بر اختلافات است. برعکس، کسانی که برابری‌طلب نیستند معتقدند ارزش تفاوت‌ها در ساختن یک جامعه خوب بیشتر است. شناخت خاستگاه پیچیده این انتخاب اساسی ... مشکل است. اما تضاد بین این انتخاب‌های اساسی مدت‌هاست دو اردوگاه مخالف به‌وجود آورده است که آن را چپ و راست می‌گوییم... شالوده اعتقادات برابری‌طلبان بر این حکم استوار است که اکثریت نابرابری‌ها اهانت و بی‌حرمتی به فرد تلقی می‌شود و اینکه افراد دوست دارند تا نابرابری‌ها رفع شوند. ازسوی‌دیگر ... راست تمایل بیشتری دارد تا نابرابری‌ها را طبیعی، و نابرابری‌های اجتماعی را ناشی از رسوم، سنت و نیروی گذشته بداند.[۲۹]

بر این مبنا، امروزه و در جهان مدرن با دو تعریف متباین از آزادی مواجه هستیم؛ در یک طرف، مفهوم حقوقی آزادی را داریم که مبتنی بر تعریف حقوق اولیه، بنیادین و ذاتی انسان است و می‌گوید

هر فرد اساساً صاحب حقوق خاصی ازجمله حق آزادی است که – براساس حقوق عمومی و بالاخص قانون اساسی - بخشی از آن را به حکومت واگذار می‌کند. در طرف دیگر، آزادی صرفاً استقلال اتباع در مقابل حکومت محسوب می‌شود.[۳۰] از این منظر، لیبرالیسم کلاسیک از آزادی مدنی، دولت محدود تحت حاکمیت قانون، مالکیت خصوصی، و باور به لسه‌فر[۳۱] دفاع کرده و بر بازار آزاد تأکید می‌کند. درنتیجه، لیبرالیسم کلاسیک ترکیبی از نظریات قانون طبیعی، فایده‌گرایی، و باور به ترقی را ارائه می‌دهد و معتقد است اگرچه همه افراد در اصل، مساوی به دنیا آمده‌اند اما عدم تساوی بعدی آنان محصول شرایط است؛ شرایطی که لزوماً ناعادلانه نیست.

به عبارت دیگر، از این منظر، بازار رقابتی تنها نوع نظام سازگار با دمکراسی است و دمکراسی واقعی نه‌تنها به‌معنای اراده جمعی اکثر مردم و واجد ارزش ذاتی نیست، بلکه صرفاً به‌عنوان یک روش انتقال قدرت و چارچوب کنشگری سیاسی که می‌تواند به حداکثرسازی نفع جمعی بینجامد مطرح است. بنابراین، اولین گام در راه رسیدن به دمکراسی، آزادسازی اقتصاد است که شامل خصوصی‌سازی و مقررات‌زدایی می‌شود.[۳۲]

بدین‌ترتیب، ما با دو چارچوب اراده جمعی[۳۳] و نفع جمعی[۳۴] روبه‌رو می‌شویم. در رویکرد نخست، قانون نمودار یا تجلی اراده جمعی تصور می‌شود که حقوق قابل واگذاری یا غیرقابل واگذاری افراد به حکومت[۳۵] را روشن می‌سازد.[۳۶] بنابراین، افراد در یک فرایند دمکراتیک می‌توانند در تعیین سرنوشت خود - ازجمله در زمینه سیاست‌های اقتصادی، اجتماعی و فرهنگی - مشارکت کنند. اما در رویکرد دوم، نفع جمعی که از طریق آزادی بازار محقق می‌شود، اساس همه‌چیز ازجمله جامعه، فرهنگ و سیاست را تشکیل می‌دهد. چراکه طبق ادعای این رویکرد، بازی مشروع رقابت طبیعی- یعنی رقابت در شرایط آزادی- به نفع همگانی می‌انجامد[۳۷] و حقوق انسان‌ها را به نحوی منصفانه- و نه ضرورتاً برابر- برآورده می‌سازد.[۳۸]

این دوگانه را می‌توان در نظریه‌های توضیح‌دهنده رفتارهای جمعی نیز ملاحظه کرد:

نظریه‌هایی که به عمل اخلاقی یا تولید خیر جمعی می‌پردازند، از افراد جامعه می‌خواهند که جمع‌گرایانه رفتار کنند، زیرا خوب و پسندیده است و اخلاق [یا دین] آن را توصیه می‌کند. اما [نظریه] انتخاب عقلانی مدعی است مردم به رفتارهایی تمایل دارند که نفع آنها در آن رفتار بیشتر تأمین می‌شود. طبق این نظریه، نفع عمومی [یا جمعی] جامعه نیز از طریق دنبال کردن نفع فردی توسط افراد جامعه، زودتر و بهتر به‌دست می‌آید، که «دست پنهان بازار» آدام اسمیت، نمونه بارز آن است. فرق است بین وقتی که یک فرد، عمل جمعی انجام می‌دهد، زیرا معتقد است [...] صواب و پسندیده است [...] و وقتی که فرد همان عمل [...] را انجام می‌دهد زیرا فکر می‌کند که به نفع (درازمدت) خود اوست.[۳۹]

از این منظر، تأکید بر آزادی بازار از این جهت صورت می‌پذیرد که آثار سودمند رقابت به‌طور منصفانه میان افراد تقسیم می‌شود اما - برخلاف نظام‌های سوسیالیستی و کمونیستی- لزوماً

بهره‌مندی یکی با هزینه دیگری همراه نیست. در این چارچوب، در همه حوزه‌ها مثلاً سینما و موسیقی، گردشگری و تغذیه، سلامت و درمان، مسکن و شهرسازی، سیاست و ... آنچه در بازار و متکی بر قیمت طبیعی[۴۰] یا قیمت مناسب[۴۱] تعیین می‌شود، هم برای تصمیم‌گیر فرهنگی و اقتصادی و سیاسی و هم برای مصرف‌کننده و خریدار و رأی‌دهنده بیشترین فایده را فراهم می‌کند.

در نظامی که با منطق مشابهی شکل گرفته است با حکومت مقتصد یا اندیشه دولت حداقلی[۴۲] مواجهیم که مسئله اساسی‌اش این است که «چطور می‌توان بدون فلج شدن حکومت و انسداد حقیقتی که بازار، نمودار آن است و باید به‌کلی محترم باشد، خود - محدودسازی ضروری حکومت را در قانون صورت‌بندی کرد؟».[۴۳] بر این اساس، در این‌گونه نظام‌ها به محض آنکه احساس شود، زمینه انتزاع‌بخشی از مسئولیت‌های حکومت وجود دارد، تدارک لازم برای واگذاری آن از طریق قوانین و مقررات انجام می‌شود.

به بیان دیگر، این رویکرد اموری را که دخالت در آنها برای حکومت فایده‌ای ندارد، کنار می‌گذارد و حوزه مداخله حکومت را بر این مبنا تعریف می‌کند که انجام دادن یا عدم انجام چه چیزی برای حکومت سودمند است. درنتیجه، حکومت مقتصد در تمامی فرایندهای کنشی خود و در مورد هر یک از نهادهای قدیمی و جدید- مثلاً آموزش و پرورش، آموزش عالی، هنر، دین، پیام‌رسان‌های اجتماعی و ...- این پرسش‌ها را مطرح می‌کند که آیا مداخله در این حوزه‌ها سودمند است؟ چرا سودمند است؟ در چه چارچوب و حدودی سودمند است؟ تا چه زمانی سودمند است و از چه زمانی زیان‌آور می‌شود؟ پس، مسئله چنین رویکردی، فایده است.[۴۴]

بنابر آنچه گفته شد در رویکرد فایده‌گرا، قانون حاصل مبادله‌ای است که حوزه دخالت مراجع عمومی را از حوزه استقلال فرد جدا می‌کند.[۴۵] از این منظر، وظیفه حکومت برای تأمین امنیت نیز درواقع، حمایت از نفع جمعی در برابر منافع فردی است.[۴۶]

۶. یکی از موضوع‌هایی که سبب می‌شود تا جامعه ایرانی به‌وضوح متوجه شکاف دو ایده «برابری» و «آزادی» نشود، آن است که عمدتاً «لیبرال دمکراسی»- به‌عنوان یکی از شقوق دمکراسی- را تنها صورت «دمکراسی» می‌داند. چراکه «لیبرالیسم توانسته است سال‌ها به‌عنوان مکتب غالب در اندیشه غرب باقی بماند، و لیبرال دمکراسی را به تعریف مسلط و رایج دمکراسی تبدیل کند».[۴۷] این در شرایطی است که به اعتبارات گوناگون، انواع مختلفی از دمکراسی تعریف و نام‌گذاری شده و مثلاً دیوید هلد از یازده مدل دمکراسی نام می‌برد.[۴۸] به‌علاوه، مفهوم دمکراسی به‌عنوان یکی از مهم‌ترین و چالش‌برانگیزترین مفاهیم علوم انسانی، قدمت زیادی دارد، در گذر زمان دستخوش دگرگونی‌ها و تحولات مفهومی و نهادی بسیاری بوده[۴۹] و منازعات تئوریک و به‌تبع آن چالش‌های اجتماعی متعددی را در جوامع مختلف سبب شده است.[۵۰] برخی از دلایل این سوءتعبیر بدین شرح است:

- تقدم ایده «آزادی» بر شعار «برابری» در انقلابات مدرن از همان روز نخست،

- حاشیه‌ای شدن دیگر انواع دمکراسی‌های مدرن در جریان جنگ‌های جهانی اول و دوم،
- شکل‌گیری شوروی سابق براساس برداشت رادیکالی از «برابری» که به سرکوب گسترده «آزادی» منتهی شد،
- ایجاد دولت رفاه در بلوک غرب که با برقراری سطوحی از رفاه عمومی توانست ضمن جلوگیری از گرایش ملت‌ها و جوامع به جانب بلوک شرق، توفیق لیبرالیسم در جمع نسبی «آزادی» و «برابری» را به نمایش بگذارد،[۵۱]
- تئوری‌پردازی‌های متفکران آمریکایی برای ایجاد دمکراسی در جوامع غیرصنعتی که عمدتاً ذیل نظریه نوسازی صورت می‌پذیرفت و آغاز آشنایی بسیاری از کشورها و جوامع غیرصنعتی با دمکراسی بود،
- فروپاشی و اضمحلال بلوک شرق که به طرح نسخه تعدیل‌شده لیبرالیسم یا همان لیبرال دمکراسی به‌مثابه اندیشه پایان تاریخ منجر شد.
- استفاده از ابزارهایی مانند توسعه تجارت بین‌المللی و جهانی‌سازی اقتصاد و نیز ارائه انواع تسهیلات مالی، وام و کمک‌های خارجی مشروط به اجرای برخی مقررات فرهنگی، اجتماعی و سیاسی لیبرالیستی در جوامع غیرصنعتی.[۵۲]

بر این مبنا، شاید بتوان ادعا کرد:

آزادی و عدالت دو مفهومی هستند که یادآور نزاع دو نظام فکری بزرگ یعنی لیبرالیسم و سوسیالیسم می‌باشند. [... اما] لیبرال دمکراسی به‌عنوان یک نظام سیاسی تلاش کرده با تعریف عناصر خود مانند محدودیت قدرت سیاسی، تفکیک حوزه اجتماعی و سیاسی و حق حاکمیت برابر مردم، دو مؤلفه آزادی و برابری را ترکیب نماید. سازوکارهای لیبرال دمکراسی (مانند رأی اکثریت و نظام نمایندگی) نیز سعی داشته‌اند معمای آزادی و عدالت را حل نمایند. اما هنوز ازسوی صاحب‌نظران انتقاداتی بر لیبرالیسم مطرح است.[۵۳]

نکته‌ای که باید بدان عنایت داشت این است که به‌موازات مهجور شدن «دمکراسی اجتماعی که در ابتدا سنتی اروپایی بود»[۵۴] دیدگاه‌های منتقدانه و جایگزین‌های ارائه‌شده نظیر دمکراسی گفتمانی[۵۵] یورگن هابرماس، دمکراسی گفت‌وگویی[۵۶] آنتونی گیدنز و دمکراسی بازاندیشانه[۵۷] رابرت گودین نیز نه‌تنها برپایه اصلاح لیبرال دمکراسی طراحی شده‌اند[۵۸] بلکه «شاید بتوان از منظری، دمکراسی تأملی را مدل تشدید شده آرمان‌های لیبرال دمکراسی دانست که در حین شکل‌گیری و استقرار، ویژگی‌های متفاوتی پیدا کرده است».[۵۹]

به هر ترتیب، اولویت قائل شدن برای آزادی نسبت به برابری تنها به دولت‌های انگلستان و ایالات متحده و یا روابط درونی دولت‌های ملی محدود نماند و از آن فراتر رفت؛ چراکه به‌زودی تلاش برای دستیابی به منافع ملی، جهان جدیدی را پدید آورد.

۷. قاعدتاً آغاز شکل‌گیری نظم بازاری به اروپا- یعنی زادگاه تجدد- باز می‌گردد؛ جایی که موج فزاینده انقلاب صنعتی نیازمند تثبیت تجارت صلح‌آمیز بوده و این مهم، عامل تضمین نفع بین‌الدولی به‌شمار

می‌رفت.[۶۰] زیرا به‌سرعت مشخص شد تلاش برای تأمین صلح و امنیت میان جوامع، مستلزم حمایت از نفع همگانی در برابر منافع یک کشور است. بر این اساس، فایده‌گرایی متکی بر آزادی بازار ابتدا در سطح منطقه‌ای و سپس در سطح بین‌المللی مبنای برقراری نظم، تأمین امنیت و صلح واقع شد. از این بابت، پروژه‌های صلح قرن هفدهمی اساساً بر تعادل اروپا یا به عبارتی بر موازنه دقیق نیروهای متقابل[۶۱] بین دولت‌های مختلف تکیه داشت. برمبنای قاعده موازنه اروپا[۶۲] نباید هیچ دولتی چنان بر همسایگان خود یا سایر دولت‌ها غلبه می‌یافت که مرزهای امپراتوری‌های اروپایی دچار تغییر و بازسازی دوباره می‌شد.[۶۳] همچنین، رقابت برتری‌جویانه اقتصادی در مستعمرات، نابرابری‌هایی را وارد اروپا می‌کرد که می‌بایست، کنترل می‌شد. به دیگر سخن، در سایه قاعده موازنه اروپا اگرچه سلسله کمابیش بی‌وقفه‌ای از جنگ‌های ناتمام در مسیر کشورگشایی‌های استعماری در جریان بود، اما به صلح میان کشورهای اروپایی لطمه چندانی وارد نمی‌ساخت.[۶۴]

با این وجود، از قرن هجدهم و طی دو قرن، ایده صلح جاویدان[۶۵] - که بر اندیشه‌های کانت متکی بود- به‌تدریج[۶۶] مورد توجه قرار گرفت.[۶۷] کانت سه رکن بنیادین را برای تحقق صلح پایدار (جاویدان) مورد اشاره قرار داد: ۱. قانون اساسی و نوع ساختار سیاسی هر کشوری می‌بایست جمهوری باشد. چراکه در حکومت جمهوری، قانون محور زندگی انسان‌هاست، افراد نظام تفکیک قوا[۶۸] را براساس نوعی قرارداد اجتماعی[۹۸] پذیرفته‌اند و احترام به آزادی افراد تضمین شده است. ۲. نهادی بین‌المللی متشکل از دولت‌های جمهوری تأسیس شود؛ نهادی که پیوستن به آن داوطلبانه و آزاد است اما کشورهای عضو را به پذیرش نوعی قرارداد (پیمان) فراملی وامی‌دارد. بدین‌ترتیب، کانت صلح را در چارچوب ملی محدود نمی‌کند بلکه آن را فراسوی مرزها دنبال می‌کند. به بیان دیگر، کانت می‌خواهد عرصه روابط بین‌الملل را از حالت وضعیت طبیعی خارج کرده و به شکل یک جامعه مدنی زیر سلطه قانون درآورد. ۳. وجود حقوق و قوانین جهان‌وطن[۷۰] (جهان‌شهری) که هویت مردم کشورها و مناطق گوناگون جهان را به‌عنوان شهروندان جهانی ترسیم کند.[۷۱] بر این اساس، منطق اقتصادی ایده کانتی صلح جاویدان- که زمینه درگیری‌های بعدی را از میان برداشته و صلح را از صرف متارکه جنگ و ترک موقتی خصومت فراتر می‌برد[۷۲] - بدین شرح است:

روابط تجاری در جهان امتداد می‌یابد، درست آن‌طور که طبیعت خواسته، و به همین اندازه طبیعت خواسته که جمعیت کل جهان را اشغال کند. این چنین حقوق جهان‌وطن یا حقوق تجارت ساخته خواهد شد. این ساختمان حقوق مدنی، حقوق بین‌الملل، و حقوق جهان‌وطن چیزی نیست جز گردن نهادن انسان به حکم طبیعت به‌منزله تعهدات. ... طبیعتْ، صلح جاویدان را تضمین کرده، و این تضمین در جمعیت کل جهان و در روابط تجاری حاکم بر سراسر جهان تجلی یافته است. به‌این‌ترتیب، درواقع جهانی شدن تجارت،[۷۳] ضامن صلح جاویدان است.[۷۴]

اگرچه این رویکرد جدید در مواضع متقابل اروپا و جهان، شروع استعمار و حتی امپریالیسم نبود اما سرآغاز نوع جدیدی از عقلانیت و محاسبه جهانی در کردار حکومتی اروپا بود که نشانه‌های آن را می‌توان در تاریخ حقوق دریاها[۷۵] و پروژه‌های صلح و سازماندهی بین‌المللی[۷۶] ملاحظه کرد.[۷۷] فوکو در توضیح این نکته می‌گوید:

برای نمونه، تاریخ حقوق دریاها در قرن هجده، و براساس حقوق بین‌الملل، نحوه تصور از جهان یا حداقل دریا، به‌منزله فضای رقابت آزاد، جریان دریایی آزاد، و نتیجتاً به‌منزله یکی از شرایط لازم برای سازماندهی بازار جهانی را در نظر بگیرید. تاریخ دزدی دریایی[۷۸] - نحوه استفاده و تشویق شدن آن، و همزمان مبارزه و مقابله با آن، و غیره- نیز می‌تواند یکی از ابعاد این گسترش فضای جهانگیر برحسب چند اصل حقوقی را نشان دهد. می‌توان گفت نوعی قضامندسازی[۷۹] جهان وجود داشت که باید براساس سازماندهی یک بازار به آن نگریست.[۸۰]

مطابق آنچه گفته شد، هنگامی که به لحاظ نظری، جهانی‌شدن تجارت، ضامن صلح تلقی شود، بدیهی است که تسلط بر بسترهای تجارت جهانی و کنترل آنها نیز موضوع رقابت قرار می‌گیرد؛ امری که اهمیت دریاها و قانونگذاری این حوزه طی قرون گذشته را نشان می‌دهد و به ما می‌گوید که چرا ابرقدرت آن روزهای جهان یعنی انگلستان دارای یک کشتی‌رانی قدرتمند بود، برخورد دوگانه‌ای با امنیت دریاها داشت و ضمن مقابله با دزدان دریایی مزاحم، برای پیشبرد نیات خود و علیه رقبا از آنها بهره می‌برد و چرا همچنان، این کشور مهم‌ترین ارائه‌دهنده خدمات بیمه دریایی در جهان است.

به‌رغم طرح نظری کانت تا پیش از جنگ جهانی دوم، شاهد تغییر بسیار آهسته و تداوم نسبی آنچه اصطلاحاً موازنه اروپا نامیده می‌شود، بودیم. و تنها هنگامی که بی‌تعهدی هیتلر نسبت به موازنه اروپا، کشورهای اروپایی را به دو دسته متحدین و متفقین تقسیم کرد و ویرانی‌های بسیاری را به بار آورد،[۸۱] ایده موازنه اروپا به‌طور بنیادینی از دستور کار خارج شد و ایده صلح جاویدان، سیاست خارجی ایالات متحده و شرکای آن یعنی کشورهای اروپایی را تشکیل داد. به قول پولانی به‌مجرد اینکه اقتصاد جهانی که تکیه‌گاه توازن نظام بین‌الملل بود فروریخت، دیگر امکان تضمین صلح وجود نداشت.[۸۲]

۸. در چنین شرایطی، ایالات متحده آمریکا که از ویرانی‌های جنگ برکنار مانده بود، ایده صلح جاویدان کانت را مورد توجه قرار داد. ایده آمریکا برای برقراری و تجدید صلح در اروپای جنگ‌زده، سازوکار ثروتمند شدن[۸۳] متقابل بود. آنها معتقد بودند همان‌طور که در انتزاع سطح فردی، از طریق مبادله در نظام بازار آزاد حداکثر سود برای فروشنده و حداقل هزینه برای خریدار پدید می‌آید، در سطح جهانی نیز باید نظام بازار آزاد حاکم شود تا منافع به‌صورت عادلانه‌ای میان کشورها توزیع شود. مطابق این استدلال:

ایده پیشرفت اروپا، مضمونی بنیادین در لیبرالیسم است و مضامین تعادل اروپا را به‌کلی دگرگون می‌سازد... برای اینکه آزادی بازار، ثروتمندی متقابل، همبسته و کم‌وبیش همزمان تمام کشورهای اروپا را تضمین کند...

لازم است بازاری فوق‌العاده وسیع و حتی اگر ممکن بود، هرچه در جهان که بتوان در بازار قرار داد، را گرداگرد اروپا و برای اروپا جمع کرد. به عبارت دیگر، وقتی به‌منزله قاعده و هدف مقرر شد که ثروتمند شدن اروپا باید به‌صورت جمعی و نامحدود حاصل شود، نه به‌صورت ثروتمند شدن یکی و فقیر شدن دیگران، به یک جهانی شدن بازار[۸۴] فراخوانده شده‌ایم [... باید] کل جهان گرداگرد اروپا جمع شود تا محصولات اروپا و خودشان را در بازار اروپا مبادله کنند ... اکنون، گشایش یک بازار جهانی ... اجتناب از کشمکش‌های ناشی از یک بازار محدود را امکان‌پذیر می‌سازد. اما عرضه شدن این بازی اقتصادی جهانی مستلزم تفاوت اروپا و بقیه جهان از لحاظ نوع[۸۵] و شأن[۸۶] است. به عبارتی، از یکسو اروپا و اروپاییان را به‌منزله بازیگر داریم، و در سوی دیگر جهان را داریم که سهم بازی[۸۷] خواهد بود. بازی در اروپا انجام می‌شود، اما سهمِ بازی، جهان است. [۸۸]

با گذشت دو قرن، امروزه و در عصر انقلاب ارتباطات، مفهوم جامعه جهان‌شهری کانت در قالب آموزه جامعه مدنی، معنایی عینی و ملموس یافته است.[۸۹]

۹. نظر به آنچه گفته شد، می‌توان درباره سند استراتژی سایبری ملی ایالات متحده آمریکا ادعا کرد:

- منظور از آزادی در این سند، صرفاً استقلال اتباع در مقابل حکومت محسوب می‌شود و آنچه تأمین حقوق انسانی را- به نحوی منصفانه و نه برابر- تضمین می‌کند رقابت در شرایط آزادی است.
- سند از آزادی مدنی، دولت محدود، مالکیت خصوصی و نیز تأکید بر بازار آزاد دفاع می‌کند.
- در این سند، نفع جمعی که از طریق آزادی بازار محقق می‌شود، اساس همه‌چیز ازجمله جامعه، فرهنگ و سیاست را تشکیل می‌دهد.
- با توجه به غلبه اندیشه دولت حداقلی در این سند، تأمین امنیت و تسهیل تجارت- در فضای بین‌المللی- مهم‌ترین وظیفه دولت را تشکیل می‌دهد و از این جهت، دولت برنامه‌ای برای تصدی‌گری این عرصه- در سطح ملی- ندارد.
- قضامندسازی به‌معنای ایجاد نظام حقوقی بین‌المللی و نیز حقوق جهان‌وطن برای بهره‌برداری از فضای مجازی- به‌مثابه یک بازار نوظهور- در سند مورد اشاره قرار گرفته است.
- مطابق سند، جهانی شدن تجارت در فضای مجازی- به‌منزله فضای رقابت آزاد- ضامن صلح جهانی خواهد بود.
- ایالات متحده ضمن مبارزه و مقابله با هرگونه خرابکاری و تهدید امنیت فضای مجازی خود، برای تهدید رقبا و دشمنان خود از هیچ اقدامی ازجمله ایجاد انواع بدافزار، سیستم جاسوسی و سوءاستفاده از فضای مجازی کوتاهی نخواهد کرد.
- حقوق لیبرالی مصرح در اعلامیه استقلال آمریکا شامل: زندگی، آزادی و پیگیری سعادت و خوشبختی ارکان سند را تشکیل می‌دهد.
- ارزش‌های سند با اهداف و شعارهای انقلاب آمریکا که در قانون اساسی و منشور حقوق ایالات متحده آمده، مطابقت دارد.

■ اگرچه - مطابق تعهدات ایالات متحده به کشورهای اروپایی هم‌پیمان خود پس از جنگ جهانی دوم که به تشکیل نهادهای بین‌المللی منجر شد- مقرر است که آمریکا ثروتمندی متقابل، همبسته و کم‌وبیش همزمان تمام کشورهای اروپا را تضمین کند، اما به‌نظر می‌رسد امروزه آمریکا تردیدهای اساسی در پایبندی به تعهدات پیشین دارد و از این جهت، از یکسو سعی در جهانی‌سازی بازار فضای مجازی دارد و ازسوی دیگر، طرحی برای سهیم کردن شرکای سابق در این بازار ندارد یا لااقل معتقد است شأن و رتبه او در این بازار به‌کلی متمایز از دیگران است.

■ ازآنجاکه «سند استراتژی سایبری ملی ایالات متحده آمریکا» دارای ارتباط مستقیمی با بافت فرهنگی- تاریخی و ساخت اقتصادی- سیاسی آن جامعه است، احتمال توفیق اجرای سند با مشارکت همگانی و سهولت بیشتری توأم خواهد شد.

■ درنهایت، چنانچه بدانیم ایالات متحده، فضای مجازی را بستر امروز و فردای تجارت جهانی و درنتیجه صلح جهانی می‌داند، جایگاه در حال ارتقای فضای مجازی در سال‌های اخیر را به‌روشنی درخواهیم یافت.

۱۰. برای بررسی سند از این منظر، در ادامه مروری اجمالی بر بخش‌های مختلف آن خواهیم داشت.

یکی از ویژگی‌های سند، تناسب لحن با مخاطب آن است که با این عبارت آغاز می‌شود:

«همراهان آمریکایی من؛ اولویت‌های اصلی من حفاظت از امنیت ملی آمریکا و افزایش رفاه مردم آمریکا هستند. اطمینان از امنیت فضای سایبری در جهت نیل به این دو هدف ضروری است. فضای سایبری بخشی جداناپذیر از زندگی امروزی آمریکا، شامل اقتصاد و بخش دفاعی ماست».

بخش دیگر سند با عنوان «چگونه به اینجا رسیدیم؟» مربوط به ضرورت نگارش چنین سندی است که در آن موضع سیاسی آمریکا در قبال فضای مجازی روشن می‌شود. برخی از عبارات کلیدی این بخش بدین‌شرح است:

- *ظهور اینترنت و مرکزیت فزاینده فضای مجازی در تمام جنبه‌های جهان مدرن با ظهور آمریکا به‌عنوان تنها ابرقدرت جهان در ارتباط بود.*
- *در ربع قرن گذشته، ابتکار و هوش مردم آمریکا سبب رشد و تکامل فضای سایبری شد و در مقابل، فضای سایبری هم تبدیل به پایه‌ای اساسی برای تولید ثروت و نوآوری‌ها گشته است.*
- *آمریکایی‌ها بعضاً اعتراف می‌کنند که ایالات متحده در حوزه سایبری بدون هیچ مشکلی قدرت برتر خواهد ماند.*
- *آمریکایی‌ها اعتقاد داشتند که گسترش اینترنت به تحقق آرمان‌های همگانی آزادی بیان و آزادی‌های اجتماعی فردی در تمام جهان منجر خواهد شد.*
- *آمریکایی‌ها می‌پنداشتند که اینترنت فرصت‌هایی برای گسترش ارتباطات، تجارت و تبادل آزاد ایده‌ها به وجود خواهد آورد.*

- *بخش بزرگی از جهان، چشم‌انداز آمریکا در مورد فضای سایبری باز و به اشتراک گذاشته شده‌ای را که طرفین از آن سود می‌برند پذیرفته است.*
- *رقبا و مخالفان ما ... با اینکه خود از اینترنت باز استفاده می‌کنند، دسترسی مردم‌شان را به این فضا محدود و دسترسی آنها را کنترل می‌کنند و به‌طور فعال، اصول یک اینترنت باز را در محافل جهانی تضعیف می‌نمایند. درحالی که با شرکت در عملیات جاسوسی اقتصادی مخرب و انجام فعالیت‌های اینترنتی سایبری خصمانه، با بی‌احترامی قوانین سایر کشورها را نقض می‌کنند، باعث مشکلات اقتصادی فراوان می‌شوند و به افراد، منافع تجاری و غیرتجاری و دولت‌های سراسر جهان آسیب می‌زنند.*
- *آنها [رقبا و مخالفان] فضای سایبری را، که آمریکا و دوستان و شریکانش در آن آسیب‌پذیر هستند، عرصه‌ای برای خنثی کردن قدرت نظامی، اقتصادی و سیاسی ایالات متحده می‌دانند.*
- *روسیه، ایران و کره شمالی بدون هیچ ترسی حملات سایبری مختلفی را برای آسیب به تجارت آمریکا و جهان، متحدان و شرکای ما انجام داده‌اند و هیچ غرامتی که بتواند مانع تجاوزات سایبری در آینده بشود، نپرداخته‌اند. چین در یک عملیات جاسوسی اقتصادی اینترنتی و سرقت تریلیون‌ها دلار از دستاوردهای فکری ما شرکت کرد. فعالان غیردولتی، مانند تروریست‌ها و جنایتکاران، فضای مجازی را برای به‌دست آوردن سود، استخدام نیروهای جدید، تبلیغات و حمله علیه ایالات متحده آمریکا و متحدان و شرکایش به‌کار گرفته‌اند و اغلب حرکاتشان توسط دولت‌های دشمن مورد حمایت قرار گرفته است.*[۹۰]

درنهایت، سند چهار اصل را پیش روی خود قرار می‌دهد: یکم) حفاظت از مردم آمریکا، میهن و روش زندگی آمریکایی، دوم) افزایش رفاه آمریکا، سوم) حفظ صلح در کنار قدرت، چهارم) پیشبرد نفوذ آمریکا.

هم‌اکنون و پس از آنکه رویکرد کلی و مفاهیم سند سایبری ایالات متحده آمریکا مورد واکاوی قرار گرفته است با سهولت بیشتری می‌توانیم سؤالات مطرح در بخش طرح مسئله این مقدمه را مرور کرده و به جستجوی پاسخ آن در متن پیش‌رو بپردازیم؛ پاسخ‌هایی که اگرچه با درک تاریخی و معرفت‌شناختی جامعه ایرانی مطابقت ندارد اما واجد درس‌های بسیاری برای سیاستگذاران ایرانی خواهد بود.

پی‌نوشت‌ها

۱. به‌عنوان مثال، از میان ۵۳ سند سیاستی مصوب مجمع تشخیص مصلحت نظام تنها یک مورد یعنی سیاست‌های برنامه پنج‌ساله دوم توسعه (مصوب ۱۳۷۲/۸/۱۸) به پیش از سال ۱۳۷۷ مربوط است.

۲. به‌عنوان مثال، نگاه کنید به: ماده (۲۳) **لایحه احکام مورد نیاز اجرای برنامه ششم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران (۱۳۹۹-۱۳۹۵)**. تاریخ اعلام وصول: ۱۳۹۵/۴/۳۰.

۳. ن.ک: اسماعیل نوده‌فراهانی، *مبانی سیاستی اداره وزارت فرهنگ و ارشاد اسلامی*. تهران: **مرکز پژوهش‌های مجلس شورای اسلامی**. شماره مسلسل: ۱۵۸۱۹، ۱۳۹۷.

۴. به‌عنوان مثال، نگاه کنید به: بخش تدابیر **سند پایه الگوی اسلامی ایرانی پیشرفت**. فراخوان شده در مورخ ۱۳۹۷/۷/۲۲ توسط مقام معظم رهبری.

۵. با توجه به تصویب قانون جرائم رایانه‌ای در مجلس شورای اسلامی و لزوم تعیین ضابط قضایی برای این قانون و نیز مصوبات کمیسیون افتای دولت جمهوری اسلامی ایران مبنی بر تشکیل پلیس فضای تولید و تبادل اطلاعات، این پلیس در بهمن‌ماه سال ۱۳۸۹ تشکیل گردید. (تارنمای پلیس فتا. به آدرس: https://www.cyberpolice.ir/)

۶. این شورا در ۱۷ اسفندماه ۱۳۹۰ با حکم مقام معظم رهبری تشکیل شد. (تارنمای مرکز ملی فضای مجازی. به آدرس: http://majazi.ir/)

۷. شبکه ملی اطلاعات پروژه‌ای برای توسعه شبکه زیرساخت امن و پایدار ملی در ایران است. طبق تعریف مصوب در تبصره «۲» ماده (۴۶) قانون برنامه پنجم توسعه و مصوبه شورای عالی فضای مجازی «شبکه ملی اطلاعات کشور، شبکه‌ای مبتنی بر قرارداد اینترنت (IP) به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده‌ای است به صورتی که درخواست‌های دسترسی داخلی و اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند به‌هیچ‌وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت و خصوصی و امن داخلی در آن فراهم شود».

۸. طرح «ساماندهی پیام‌رسان‌های اجتماعی» با شماره ثبت ۴۹۶ توسط تعدادی از نمایندگان مجلس شورای اسلامی تهیه شده در تاریخ ۱۳۹۷/۸/۲۷ به هیئت‌رئیسه مجلس ارجاع شده است. (تارنمای مرکز پژوهش‌های مجلس شورای اسلامی. به آدرس: https://rc.majlis.ir/fa).

9. Big Data
10. Digital currency
11. Bit Coin

۱۲.ن.ک: بیانیه بانک مرکزی جمهوری اسلامی ایران با موضوع ممنوعیت به‌کارگیری ابزار بیت کوین در مراکز پولی و مالی کشور. *(استفاده از بیت‌کوین ممنوع است.* مورخ ۱۳۹۷/۲/۲. کد خبری:۸۲۸۹۳۹۹۲. **خبرگزاری جمهوری اسلامی ایران**. به آدرس: https://www.irna.ir/)

۱۳.به‌عنوان مثال، باید دید اپلیکیشن‌ها و سامانه‌های هوشمند حمل‌ونقل چه تأثیری بر عملکرد تاکسی‌های شهری تحت نظارت سازمان تاکسیرانی داشته‌اند.

۱۴.هیلاری کلینتون وزیر سابق امور خارجه آمریکا در فصل ۱۸ کتاب خاطرات خود به نام «انتخاب‌های دشوار»- که هنوز ترجمه کاملی به فارسی ندارد- در این زمینه گفته است: «در پشت صحنه، گروه من در وزارت خارجه به‌طور مداوم با فعالان در ایران در ارتباط بودند و برای جلوگیری از تعطیل شدن توئیتر، به‌طور فوریتی مداخله کردند؛ قطع شدن توئیتر به معنای از بین رفتن یکی از وسایل اصلی ارتباطی معترضان بود».

۱۵.استاکس‌نت (Stuxnet) یک بدافزار رایانه‌ای است که اولین‌بار در ۱۳ ژوئیه ۲۰۱۰ توسط ضدویروس وی‌بی‌ای۳۲ شناسایی شد. براساس نظر کارشناسان، این بدافزار به‌دنبال خرابکاری در تأسیسات غنی‌سازی اورانیوم نطنز بوده‌است. در اواخر ماه مه ۲۰۱۲ رسانه‌های آمریکایی اعلام کردند که استاکس‌نت مستقیماً به دستور اوباما رئیس‌جمهور آمریکا طراحی، ساخته و راه‌اندازی شده است اما چندی بعد، ادوارد اسنودن در مصاحبه‌ای با اشپیگل اعلام کرد این بدافزار با همکاری مشترک آژانس امنیت ملی ایالات متحده آمریکا و رژیم صهیونیستی ساخته شده است. [تارنمای ویکی‌پدیا (دانشنامه آزاد). به آدرس: https://fa.wikipedia.org/wiki/].

۱۶.ویکی‌لیکس (WikiLeaks) سازمانی غیرانتفاعی است که به ارسال و افشای اسناد از سوی منابع ناشناس می‌پردازد. وب‌گاه ویکی‌لیکس که در سال ۲۰۰۶ میلادی افتتاح شد، توسط انتشارات سان‌شاین (sunshine press) اداره می‌شود. در طول یک سال از آغاز فعالیت، وب‌گاه ادعا کرد که بیش از ۱,۲ میلیون مدرک و سند در اختیار دارد. این سازمان بنابه گفته خودش، توسط مخالفان و فعالان اجتماعی از چین همراه با روزنامه‌نگارها،

ریاضی‌دان‌ها و پیشگامان فناوری از ایالات متحده آمریکا، تایوان، اروپا، استرالیا و آفریقای جنوبی پایه‌گذاری شده‌است (ویکی پدیا).

۱۷.ادوارد اسنودن (Edward Snowden) افشاگر کنونی، کارمند سابق سازمان اطلاعات مرکزی آمریکا و پیمانکار سابق آژانس امنیت ملی است که پیش‌تر برای سازمان سیا نیز کار کرده بود. وی در ۲۰ مه ۲۰۱۳ از محل کارش که تأسیسات متعلق به آژانس امنیت ملی آمریکا در هاوایی بود به هنگ‌کنگ پرواز کرد و در اوایل ژوئن هزاران مدرک طبقه‌بندی‌شده آژانس را در اختیار روزنامه‌نگاران قرار داد. هنگامی‌که مطالب در گاردین و واشینگتن‌پست به چاپ رسیدند اسنودن مورد توجه خبرگزاری‌های بین‌المللی قرار گرفت و وزارت دادگستری ایالات متحده اسنودن را به دو جرم متهم کرد: اول؛ نقض قانون مربوط به جاسوسی، دوم؛ سرقت اسناد متعلق به دولت آمریکا. او که در پی ابطال گذرنامه‌اش توسط دولت آمریکا مدتی را در فرودگاهی در مسکو به سر می‌برد؛ نخست از کشور اکوادور و سپس از روسیه تقاضای پناهندگی کرد و توانست از دولت روسیه پناهندگی موقت دریافت کند. افشاگری‌های اسنودن از عملیات عظیم «جاسوسی و مراقبت در سطح جهانی» پرده برداشت. بنا به مدارک اسنودن، این برنامه‌ها که شامل جاسوسی از مردم عادی و شخصیت‌ها در مکالمات تلفنی، ایمیل و موتور جستجوی اینترنت در تمام کشورها و بدون رعایت مرزهای سیاسی صورت می‌گیرند، در درجه اول توسط آژانس امنیت ملی ایالات متحده آمریکا انجام می‌شوند (ویکی پدیا).

۱۸.اوایل بهار ۱۳۹۴، روزنامه نیویورک‌تایمز فاش کرد که هیلاری کلینتون در دوران وزارت امور خارجه برای تبادل اطلاعات محرمانه از یک ایمیل شخصی استفاده می‌کرده است. شهریور ۱۳۹۴، اف‌بی‌آی اعلام کرد تحقیقات خود در مورد این ایمیل‌ها را آغاز کرده است. اوایل پاییز ۱۳۹۴، کلینتون به‌دلیل بی‌دقتی‌اش در استفاده از ایمیل شخصی عذرخواهی کرد. (ایمیل‌های مخفی؛ مانع آخر کلینتون تا کاخ سفید. مورخ ۱۳۹۵/۸/۹. کد خبری: ۳۵۰۹۸۳. همشهری‌آنلاین. به آدرس: http://www.hamshahrionline.ir/)

۱۹.اوایل تابستان ۱۳۹۵ درحالی‌که مجدداً فضای انتخابات تحت‌الشعاع ماجرای ایمیل‌ها قرار گرفت، اف‌بی‌آی به‌مدت ۳ ساعت و نیم از کلینتون بازجویی کرد. در این زمینه ستاد تبلیغات انتخاباتی کلینتون می‌گوید که دستگاه‌های اطلاعاتی روسیه در هک ایمیل شخصی خانم کلینتون و انتشار آن نقش داشته‌اند تا بر انتخابات هشتم نوامبر به نفع دونالد ترامپ، نامزد جمهوری‌خواهان اثر بگذارند (نگاهی بر رسوایی ایمیل‌های هیلاری کلینتون. ۲۰۱۶/۱۰/۳۱، یورونیوز فارسی. آدرس: https://fa.euronews.com/)

۲۰.ن.ک: سید علی محمودی. روشنگری چیست؟. ماهنامه بازتاب اندیشه. شماره ۴۱، ۱۳۸۲.

21. Liberty, Equality & Fraternity

۲۲.اولین فردی که این شعار را به‌کار برد کسی نبود جز ماکسیمیلیان روبسپیر که در جزوه «درآمدی بر تشکیلات گارد ملی» تألیف ۱۷۹۰ از آن سخن راند. این جزوه توسط انجمن‌های مردمی در تمامی فرانسه انتشار یافت (ویکی‌پدیا).

۲۳. کارل پولانی، دگرگونی بزرگ: خاستگاه‌های سیاسی و اقتصادی روزگار ما. ترجمه محمد مالجو. تهران: شیرازه. ص ۵۶، ۱۳۹۶.

۲۴.برتراند راسل، قدرت، ترجمه نجف دریابندری، تهران: خوارزمی، ۱۳۷۱، ص ۲۴۳.

۲۵.همچنین این اثر یکی از اسناد اثرگذاری گسترده انقلاب استقلال آمریکا بر انقلاب فرانسه به‌شمار می‌رود.

26. Harold J. Laski (1893-1950)

۲۷. آلکسی دوتوکویل، **تحلیل دمکراسی در آمریکا**. ترجمه رحمت‌الله مقدم مراغه‌ای. تهران: شرکت انتشارات علمی و فرهنگی. چاپ سوم ، ۱۳۹۳، ص ۶۰-۵۸.

۲۸.علت دور ماندن ظاهری شعار «برادری» از کانون منازعات آن است که این مفهوم با «نظم عمومی» سروکار دارد و طبق اصول جمهوری فرانسه همگان باید برای تحقق برادری مبارزه می‌کردند تا بتوانند از طریق آن آرمان‌های برابری و آزادی را جاودانه سازند.

۲۹.میشل فوکو، **تولد زیست‌سیاست؛ درس گفتارهای کُلِژ دوفرانس (۱۹۷۹-۱۹۷۸)**. ترجمه رضا نجف‌زاده. تهران: نی، چاپ چهارم، ۱۳۹۴، ص ۶۶.

۳۰. لسه‌فر (Laissez Faire) معمولاً در تقابل با برنامه‌ریزی مرکزی از سوی حکومت یا دخالت حکومت در جهت سوق دادن فعالیت‌های اقتصادی به جانب مورد نظر خود به‌کار می‌رود.

۳۱. سیداحسان خاندوزی، «پیش‌زمینه‌های اقتصاد برای دمکراسی» در بوته نقد. **فصلنامه راهبرد توسعه (راهبرد یاس)**. سال ۱. شماره ۱، ۱۳۸۳، ص ۲۲۴-۲۲۲.

32. Collective Will
33. Collective Benefit
34. State

۳۵. میشل فوکو، همان، ص ۶۵.

۳۶. پیشین: ۸۳.

۳۷. در این چارچوب، عمدتاً روشنفکران- و کسانی که تجدد را از منظری اروپایی می‌نگرند- معنای نخست آزادی را مورد نظر دارند، در حالی که تکنوکرات‌ها- و کسانی که مدرنیته را از منظری آمریکایی می‌نگرند- معنای دوم آن را می‌پسندند، بلکه اصولاً ریشه لیبرالیسم در اندیشه فیزیوکرات‌ها- و ازجمله آدام اسمیت- طبیعت‌گرایی و سازوکار ذاتی آن است که در قالب فرایندهای اقتصادی بروز می‌کند، نه آزادی حقوقی افراد (فوکو، ۱۳۹۴: ۹۲).

۳۸. محمدرضا جوادی یگانه، سیدضیاء هاشمی، تعارض نفع فردی و نفع جمعی (دو راهی اجتماعی) و عوامل مؤثر بر آن. نامه علوم اجتماعی. شماره ۲۶، ۱۳۸۴، ص ۱۷۳-۱۴۵.

39. Natural Price
40. Good Price
41. Least State

۴۲. میشل فوکو. همان، ص ۶۱.

۴۳. پیشین: ۶۴.

۴۴. پیشین: ۶۶.

۴۵. پیشین: ۹۷.

۴۶. محمدحسین پناهی و سمیه شالچی، دمکراسی تأملی، بدیل‌ها و چالش‌های آن (دمکراسی: از مقوله‌ای سیاسی تا امری فرهنگی)، فصلنامه علوم سیاسی، سال ۱۵. شماره ۵۸، ۱۳۹۱ ص ۱۳۶.

47. Held, David (1996). Models of Democracy.Polity Press, Great Britain, 2nd Edition. P. 338.

۴۸. سیدکمال صادقی، محسن پورعبادالهیان، پرویز محمدزاده، زهرا کریمی، پروین علی‌مرادی افشار، بررسی عوامل اقتصادی مؤثر بر دمکراسی در کشورهای درحال توسعه با استفاده از رهیافت اقتصادسنجی فضایی. فصلنامه اقتصاد مقداری (بررسی‌های اقتصادی سابق). دوره ۱۴. شماره ۱، ۱۳۹۶ ص ۱۲۰.

۴۹. محمدحسین پناهی و سمیه شالچی، همان، ص ۱۲۲.

۵۰. سیاه‌بیدی کرمانشاهی، سعید. دمکراسی اقتصادی در حقوق کار. وکیل مدافع: فصلنامه داخلی کانون وکلای دادگستری. شماره ۱۷، ۱۳۹۷، ص ۷۹-۷۸.

۵۱. صادقی و همکاران. همان، ۱۳۹۶، ص ۱۲۴-۱۲۳.

۵۲. محمدحسین پناهی و سمیه شالچی، همان، ص ۱۳۰.

۵۳. سعید سیاه‌بیدی کرمانشاهی، همان، ۱۳۹۷، ص ۷۹.

54. Discursive Democracy
55. Dialogic Democracy
56. Reflective Democracy

۵۷. محمدحسین پناهی و سمیه شالچی، همان، ص ۱۳۵.

۵۸. پیشین: ۱۵۱.

۵۹. کارل پولانی. همان، ص ۵۶.

60. Reciprocal Forces
61. European Balance

۶۲. قاعده موازنه اروپا نوعی نظام بین‌الدولی اروپایی تحت عنوان کنسرت اروپا (Concert of Europe) را شکل داد که از سال ۱۸۱۵ تا ۱۹۱۴ به مدت یک قرن برقرار بود (پولانی، ۱۳۹۶: ۵۷).

۶۳. پیشین: ۵۴.

64. . Perpetual Peace

۶۵. حد فاصل این تحول پارادایمی، رویکرد موقت اما پرنفوذی بر اروپا حاکم شد؛ رویکرد تعادلی که مورد نظر انگلستان بود و از طریق منطقه‌بندی اروپا این فرصت را به انگلستان می‌داد که واسطه بین اروپا و بازار جهانی باشد.

۶۶. میشل فوکو، همان، ص ۸۶.

67. Separation of Powers System
68. Social Contract
69. Cosmopolitan Law

۷۰. محمدحسین جمشیدی، مصطفی نجفی و زینب زبیدی، بررسی مقایسه‌ای مقوله صلح پایدار از منظر اسلام و لیبرالیسم اخلاقی (کانتی). فصلنامه علمی-پژوهشی سیاست دفاعی. دوره ۲۵. شماره ۵ [پیاپی ۹۷] ، ۱۳۹۵، ص ۲۳۴-۲۳۶.

۷۱. پیشین: ۲۳۴.

72. Commercial Globalization

۷۳. میشل فوکو، همان، ص ۸۸- ۸۷.

74. Maritime Law
75. International Organization

۷۶. پیشین: ۸۵.

77. . Piracy
78. Juridification

۷۹. پیشین.

۸۰. قاعده موازنه اروپا بر «اندیشه بازی اقتصادی به‌منزله بازی با حاصل‌جمع صفر» متکی بود که می‌گفت ثروتمند شدن برخی کشورها با هزینه دیگران قابل تصور است. پس برای جلوگیری از به‌وجود آمدن یک برنده بزرگ و بر هم خوردن موازنه توزیع منافع اقتصادی، هرگاه وضعیت تعادل به خطر افتاد باید بازی رقابت متوقف شود.

۸۱. کارل پولانی. همان، ص۵۲.

82. Enrichment
83. Globalization of the Market
84. Kind
85. Status
86. Stake

۸۷. میشل فوکو. ص ۸۴- ۸۳.

۸۸. سیدعلی محمودی، بنیادها و آموزه‌های فلسفه سیاسی کانت. مجله اطلاعات سیاسی اقتصادی. شماره ۱۷۹ و ۱۸۰. (صفحات ۴- ۲۵)، ۱۳۹۴، ص ۱۳.

۸۹. برخلاف تصورات عوامانه درباره فضای مجازی، جملات فوق صریح و بی‌پرده هستند و رویکرد کارل اشمیت (۱۹۸۵-۱۸۸۸) را یادآوری می‌کنند که اساساً مرز سیاست و غیرسیاست با تصمیم دولت در تمایز دوست/دشمن مشخص می‌شود [ن.ک: علی اشرف نظری، بازخوانی انتقادی مفهوم امر سیاسی در نظریه کارل اشمیت. فصلنامه سیاست؛ مجله دانشکده حقوق و علوم سیاسی. دوره ۴۵. شماره ۴، ۱۳۹۴، ص ۱۰۱۴-۹۹۱].

سند استراتژی سایبری ملی

ایالت متحده آمریکا

سپتامبر ۲۰۱۸

همراهان آمریکایی من

اولویت‌های اصلی من حفاظت از امنیت ملی آمریکا و افزایش رفاه مردم آمریکا هستند. اطمینان از امنیت فضای سایبری در جهت نیل به این دو هدف ضروری است. فضای سایبری بخشی جداناپذیر از زندگی امروزی آمریکا، شامل اقتصاد و بخش دفاعی ماست. درحالی که بخش‌های خصوصی و دولتی ما در حال تلاش برای افزایش ایمنی سیستم‌های خود هستند، دشمنان ما نیز در حال افزایش پیچیدگی و تکرار فعالیت‌های سایبری بدخواهانه خود می‌باشند. آمریکا اینترنت را به‌وجود آورد و آن را با جهان به اشتراک گذاشت. حال، ما باید از امنیت و حفظ فضای سایبری برای نسل‌های بعدی اطمینان حاصل کنیم.

در ۱۸ ماه گذشته، دولت من برای پیدا کردن تهدیدات سایبری، فعالیت‌هایی انجام داده است. ما فعالان خطرناک سایبری را تحریم کرده‌ایم. ما کسانی را که جرائم سایبری مرتکب شده‌اند محکوم نموده‌ایم. ما مسببان فعالیت‌های خصمانه را به‌طور عمومی معرفی و جزئیات ابزارهای مورد استفاده آنان را منتشر کرده‌ایم. ما از ادارات و سازمان‌ها خواسته‌ایم تا بعضی نرم‌افزارهای مخرب را به دلایل مختلف امنیتی حذف کنند. ما با کمک به مدیران ادارات و سازمان‌ها در راستای تأمین امنیت کافی، اقداماتی انجام داده‌ایم تا بتوانند مدیریت خطرات امنیت سایبری مجموعه تحت کنترل خود را به عهده بگیرند. به‌علاوه، در سال گذشته من دستور اجرایی ۱۳۸۰۰ را به‌منظور تقویت امنیت سایبری شبکه‌های فدرال و زیرساخت‌های حیاتی امضا نمودم. کارهای انجام شده و گزارش‌های تهیه شده در پاسخ به آن دستور اجرایی، زمینه را برای تنظیم این استراتژی سایبری ملی به‌وجود آوردند.

با انتشار این استراتژی سایبری ملی، ایالات متحده آمریکا اولین استراتژی کامل سایبری خود را در چندین اصل ارائه کرده است. این استراتژی چگونگی برخورد دولت من با مسائل زیر را توضیح می‌دهد:

- دفاع از میهن، به‌وسیله حفاظت از شبکه‌ها، سیستم‌ها، توابع و داده‌ها.
- افزایش رفاه مردم آمریکا به‌وسیله ایجاد یک اقتصاد دیجیتالی امن و در حال رشد و حمایت جدی از نوآوری‌های داخلی.
- حفظ صلح و امنیت به‌وسیله تقویت توانایی‌های ایالات متحده – با هماهنگی شرکا و متحدان – به جهت جلوگیری، و در مواقع ضروری، تنبیه کسانی که از ابزار سایبری برای اهداف خصمانه استفاده می‌کنند.
- گسترش نفوذ آمریکا در خارج از کشور جهت توسعه اصول کلیدی یک اینترنت باز، با خدمات متقابل،[1] قابل اعتماد و امن.

استراتژی سایبری ملی، نشان‌دهنده تعهد من در برابر تقویت قابلیت‌های امنیت سایبری آمریکا و حفاظت از آن در برابر تهدیدات سایبری می‌باشد. این یک فراخوان به تمام آمریکایی‌ها و شرکت‌های

1. Interoperable

بزرگمان است تا برای ارتقای امنیت سایبری ملی اقدامات لازم را انجام دهند. ما به هدایت جهان در راه ایمن‌سازی یک آینده سایبری موفق ادامه خواهیم داد.

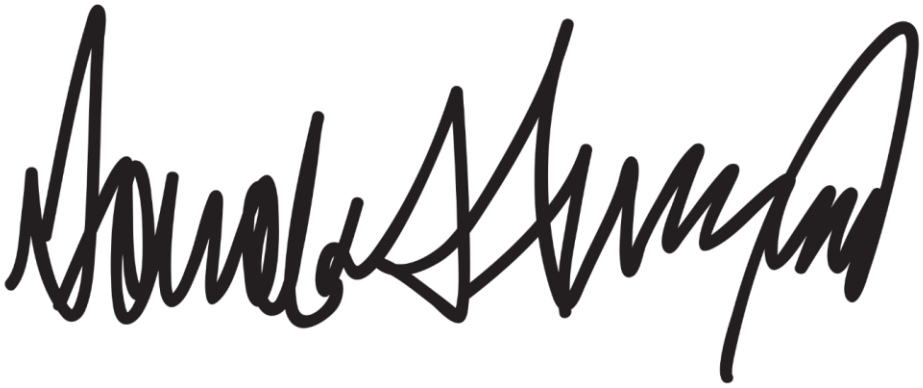
با ارادت

رئیس جمهور

دونالد ترامپ

کاخ سفید

سپتامبر۲۰۱۸



مقدمه

رفاه و امنیت آمریکا وابسته به نحوه واکنش ما در برابر قابلیت‌ها و چالش‌های فضای مجازی است. زیرساخت‌های حیاتی، دفاع ملی و زندگی روزمره آمریکاییان نیز براساس فناوری اطلاعاتِ متصل و مبتنی‌بر کامپیوتر می‌باشد. با توجه به اینکه تمام جنبه‌های زندگی در آمریکا، بیشتر تابع فضای سایبری امن گشته‌اند، آسیب‌پذیری‌های جدیدی پیدا شده و تهدیدات جدید همچنان در حال ظهورند. براساس استراتژی امنیت ملی و اقدامات دولت در ۱۸ ماهه نخست خود، استراتژی سایبری ملی مشخص می‌نماید که ایالات متحده چگونه از بهره‌مندی مردم آمریکا از فضای سایبری امنی که به اصول‌مان پایبند است، امنیت‌مان را حفظ می‌نماید و باعث افزایش رفاه می‌گردد، اطمینان حاصل می‌کند.

۱. چگونه به اینجا رسیدیم؟

ظهور اینترنت و مرکزیت فزاینده فضای مجازی در تمام جنبه‌های جهان مدرن با ظهور آمریکا به‌عنوان تنها ابرقدرت جهان در ارتباط بود. در ربع قرن گذشته، ابتکار و هوش مردم آمریکا سبب رشد و تکامل فضای سایبری شد و در مقابل، فضای سایبری هم تبدیل به پایه‌ای اساسی برای تولید ثروت و نوآوری‌ها گشته است. فضای مجازی جزئی جدایی‌ناپذیر از زندگی مالی، اجتماعی، دولتی و سیاسی آمریکاست. در عین حال، آمریکایی‌ها بعضاً اعتراف می‌کنند که ایالات متحده در حوزه سایبری بدون هیچ مشکلی قدرت برتر خواهد ماند و چشم‌انداز آمریکا برای داشتن یک اینترنت باز، اینتراپرابل، قابل اعتماد و ایمن بدون شک به حقیقت خواهد پیوست. آمریکایی‌ها اعتقاد داشتند که گسترش اینترنت منجر به تحقق آرمان‌های همگانی آزادی بیان و آزادی‌های اجتماعی فردی در تمام جهان خواهد شد. آمریکایی‌ها می‌پنداشتند که اینترنت فرصت‌هایی برای گسترش ارتباطات، تجارت و تبادل آزاد ایده‌ها به‌وجود خواهد آورد. بخش بزرگی از جهان، چشم‌انداز آمریکا در مورد فضای سایبری باز و به اشتراک گذاشته شده‌ای را که طرفین از آن سود می‌برند پذیرفته است.

بااین‌حال، رقبا و مخالفان ما به‌گونه‌ای دیگر عمل می‌نمایند. با اینکه خود از اینترنت باز استفاده می‌کنند، دسترسی مردم‌شان را به این فضا محدود و دسترسی آنها را کنترل می‌کنند و به طور فعال، اصول یک اینترنت باز را در محافل جهانی تضعیف می‌نمایند. درحالی که با شرکت در عملیات جاسوسی اقتصادی مخرب و انجام فعالیت‌های اینترنتی سایبری خصمانه، با بی‌احترامی قوانین سایر کشورها را نقض می‌کنند، باعث مشکلات اقتصادی فراوان می‌شوند و به افراد، منافع تجاری و غیرتجاری و دولت‌های سراسر جهان آسیب می‌زنند. آنها فضای سایبری را، که آمریکا و دوستان و شریکانش در آن آسیب‌پذیر هستند، عرصه‌ای

برای خنثی کردن قدرت نظامی، اقتصادی و سیاسی ایالات متحده می‌دانند. روسیه، ایران و کره شمالی بدون هیچ ترسی حملات سایبری مختلفی را برای آسیب به تجارت آمریکا و جهان، متحدان و شرکای ما انجام داده‌اند و هیچ غرامتی که بتواند مانع تجاوزات سایبری در آینده بشود، نپرداخته‌اند. چین در یک عملیات جاسوسی اقتصادی اینترنتی و سرقت تریلیون‌ها دلار از دستاوردهای فکری ما شرکت کرد. فعالان غیردولتی، مانند تروریست‌ها و جنایتکاران، فضای مجازی را برای به‌دست آوردن سود، استخدام نیروهای جدید، تبلیغات و حمله علیه ایالات متحده آمریکا و متحدان و شرکایش به‌کار گرفته‌اند و اغلب حرکاتشان توسط دولت‌های دشمن مورد حمایت قرار گرفته است. به‌دلیل افزایش دفعات و پیچیدگی این فعالیت‌های سایبری مخرب، نهادهای دولتی و خصوصی تلاش‌های زیادی برای حفظ امنیت سیستم‌های خود کرده‌اند. در سراسر آمریکا، نهادها با چالش‌های امنیت سایبری روبه‌رو شده‌اند تا بتوانند به‌طور مؤثر از شناسایی و محافظت شبکه‌ها، سیستم‌ها، توابع و داده‌های خود و همچنین تشخیص، پاسخگویی و بازیابی اطلاعات پس از حوادث اطمینان حاصل نمایند.

۲. راه پیش رو

دوران جدیدِ رقابت‌های استراتژیک و تهدیدات جدید، به استراتژی سایبری جدیدی که آسیب‌پذیری‌ها را کاهش دهد، برای مخالفان بازدارنده باشد و از فرصت‌های ممکن برای رشد ملت آمریکا حراست کند، جهت واکنش به واقعیت‌های جدید نیاز دارد. حفاظت از فضای سایبری در این استراتژی بسیار ضروری است و به پیشرفت‌های فنی و مدیریتی کارا در سطح دولت فدرال و بخش خصوصی نیازمند است. همچنین دولت تشخیص داده است که اتخاذ یک روش صرفاً تکنوکرات برای روبه‌رویی با مشکلات جدید فضای سایبری، مناسب نیست. ایالات متحده همچنین برای جلوگیری از فعالان سایبری متخاصم و رشد ناگهانی آنها، باید بتواند سیاستی اتخاذ کند تا آنها را مجبور به پرداخت غرامت نماید. در حال حاضر دولت اقداماتی جدی برای یافتن این قبیل تهدیدات و مقابله با واقعیت‌های جدید انجام داده است. ایالات متحده فعالان سایبری متخاصم را تحریم و کسانی را که مرتکب جرائم سایبری شده‌اند، محکوم کرده است. ما مسببان فعالیت‌های بدخواهانه را به‌طور عمومی معرفی و جزئیات ابزارهای مورد استفاده آنان را منتشر کرده‌ایم. ما از ادارات و سازمان‌ها خواسته‌ایم تا بعضی نرم‌افزارهای مخرب را به دلایل مختلف امنیتی حذف کنند. ما با کمک به مدیران ادارات و سازمان‌ها در راستای تأمین امنیت کافی، اقداماتی انجام داده‌ایم تا بتوانند مدیریت ریسک‌های امنیتی سایبری مجموعه تحت کنترل خود را به‌عهده بگیرند.

روش دولت در قبال فضای سایبری بر تعهد به ارزش‌های آمریکا، از قبیل اعتقاد به قدرت آزادی اجتماعی فردی، آزادی بیان،

بازارهای آزاد و احترام به حریم شخصی بنا شده است. ما همچنان به وعده‌مان برای یک اینترنت باز، با خدمات متقابل، قابل اعتماد و ایمن جهت تقویت و گسترش ارزش‌هایمان و حفاظت و اطمینان از امنیت اقتصادی کارگران آمریکایی و شرکت‌ها متعهد هستیم. آینده‌ای که آرزو داریم بدون یک تعهد آمریکایی مجدد نسبت به پیشرفت منافع‌مان در سراسر فضای مجازی به‌وجود نخواهد آمد.

دولت متوجه شده است که ایالات متحده وارد یک رقابت پیوسته علیه رقیبان استراتژیک، دولت‌های سرکش و شبکه‌های تروریستی و جنایی شده است. روسیه، چین، ایران و کره شمالی همگی از فضای سایبری به‌عنوان وسیله‌ای برای به چالش کشیدن ایالات متحده، متحدان و شریکانش استفاده می‌کنند. این درحالی است که آنها در سایر حوزه‌ها چنین بی‌پروا عمل نمی‌کنند. این دشمنان با استفاده از ابزار سایبری سعی دارند تا اقتصاد و دمکراسی ما را تضعیف کنند، دستاوردهای فکری ما را به سرقت ببرند و در فرایندهای دمکراتیک ما اختلال ایجاد نمایند. ما در برابر حملات سایبری‌ای که هنگام صلح علیه زیرساخت‌های حیاتی صورت می‌گیرد آسیب‌پذیر هستیم و خطر استفاده این کشورها از حملات سایبری علیه ایالات متحده در طول بحران کوتاه‌مدت جنگ در حال افزایش است. این دشمنان به‌طور پیوسته در حال توسعه اسلحه‌های سایبری جدیدتر و کاراتر می‌باشند.

این استراتژی مشخص می‌نماید ما چگونه ۱. با حفاظت از شبکه‌ها، سیستم‌ها، توابع و داده‌ها از میهن دفاع می‌کنیم، ۲. رفاه مردم آمریکا را به کمک ایجاد یک اقتصاد دیجیتالی امن و در حال رشد و با حمایت قوی از نوآوری‌های داخلی افزایش می‌دهیم، ۳. صلح و امنیت را به‌وسیله تقویت توانایی‌های ایالات متحده – با هماهنگی شرکا و متحدان – در جهت جلوگیری، و در مواقع ضروری، تنبیه کسانی که از ابزار سایبری برای اهداف خصمانه استفاده می‌کنند، حفظ می‌نماییم و ۴. نفوذ آمریکا را در خارج از کشور به‌منظور توسعه اصول کلیدی یک اینترنت باز، با خدمات متقابل، قابل اعتماد و امن گسترش می‌دهیم.

موفقیت این استراتژی زمانی مشخص خواهد شد که: نقاط آسیب‌پذیر فضای سایبری به‌طور مؤثری از طریق شناسایی و حفاظت از شبکه‌ها، سیستم‌ها، توابع و داده‌ها مدیریت گردد که این مهم به‌وسیله شناسایی، انعطاف‌پذیری، واکنش و بازیابی صحیح‌شان در هنگام رخ دادن حوادث انجام می‌پذیرد؛ فعالیت‌های سایبری خصمانه مخرب، ویرانگر و بی‌ثبات‌کننده‌ای که علیه منافع ایالات متحده شکل می‌گیرند کاهش یابد و یا از آنها جلوگیری شود؛ از فعالیت‌هایی که برخلاف رفتار مسئولانه در فضای مجازی است به‌وسیله اعمال غرامت به روش‌های سایبری و غیرسایبری جلوگیری گردد، و ایالات متحده

در جایگاه استفاده از قابلیت‌های سایبری برای نیل به اهداف امنیت ملی قرار گیرد.

استراتژی سایبری ملی به‌طور مفصل در چندین اصل از استراتژی امنیت ملی سازماندهی شده است. اعضای شورای امنیت ملی با وزارتخانه‌ها، آژانس‌ها و وزارت مدیریت و بودجه (OBM) برای ایجاد یک طرح مناسب به جهت اجرای این استراتژی هماهنگی خواهند کرد. ادارات و آژانس‌ها مأموریت‌های محوله را از طریق راهنمایی استراتژیکی که در ادامه آمده، اجرا خواهند کرد.

اصل یک ـ حفاظت از مردم آمریکا، میهن و روش زندگی آمریکایی

حفاظت از مردم آمریکا، روش زندگی آمریکایی و منافع آمریکا در خط مقدم استراتژی امنیت ملی قرار دارند. حفاظت از شبکه‌های اطلاعاتی آمریکا، چه دولتی و چه خصوصی، برای برآورده شدن این هدف بسیار ضروری هستند. این امر نیازمند یک‌سری فعالیت هماهنگ با تمرکز بر حفاظت از شبکه‌های دولتی، حفاظت از زیرساخت‌های حیاتی و مبارزه با جرائم سایبری است. دولت ایالات متحده، صنایع خصوصی و مردم هرکدام باید اقدامی قاطع و فوری، با تقویت امنیت شبکه‌های تحت کنترل خود و حمایت از یکدیگر، برای تقویت امنیت سایبری انجام دهند.

هدف: مدیریت خطرات امنیت سایبری جهت افزایش امنیت و پایداری اطلاعات کشور و سیستم‌های اطلاعاتی.

۱. امنیت شبکه‌ها و اطلاعات فدرال

مسئولیت امنیت شبکه‌های فدرال – شامل سیستم‌های اطلاعاتی فدرال و سیستم‌های امنیتی ملی – به‌طور کامل برعهده دولت فدرال است. دولت برای ایمن‌سازی سیستم‌های اطلاعاتی فدرال در کنار وضع استانداردهایی برای مدیریت خطرات امنیت سایبری، اختیارات، تعهدات و مسئولیت‌های مربوطه را درون و بین وزارتخانه‌ها و آژانس‌ها مشخص خواهد کرد. به‌عنوان بخشی از این فرایند، دولت بعضی از اختیارات را در دولت فدرال متمرکز خواهد کرد، نظارت آژانس بین‌المللی را گسترده‌تر خواهد نمود، مدیریت زنجیره تأمین فدرال را بهبود خواهد بخشید و امنیت سیستم‌های پیمان‌کاری دولت ایالات متحده را تقویت خواهد کرد.

اولویت‌بندی اقدامات:

۱-۱. مدیریت متمرکز بیشتر و نظارت بر امنیت سایبری غیرنظامی فدرال

دولت برای ایجاد امنیت شبکه‌های آژانس‌ها و وزارتخانه‌های فدرال، به‌استثنای سیستم‌های امنیتی ملی و وزارت دفاع (DOD[1]) و

1. Department of Defense

همچنین سیستم‌های کمیته اطلاعاتی(IC[1])، اقدام به فعال‌سازی بیشتر وزارت امنیت داخلی (DHS[2])، خواهد کرد. این امر شامل اطمینان از دسترسی کامل DHS به سیستم‌های اطلاعاتی آژانس برای اهداف امنیت سایبری و امکان انجام اقدامات مناسب و مستقیم به جهت ایجاد حراست از این سیستم‌ها در برابر خطرات متفاوت است. تحت نظارت OMB، دولت کارهای انجام گرفته مربوط به فرمان اجرایی ۱۳۸۰۰ را برای انتقال آژانس‌ها به سرویس‌های اشتراکی و زیرساخت‌ها اولویت‌بندی می‌نماید. همچنین DHS به‌منظور بهبود وضعیت امنیت سایبری ایالات متحده، نظارت دقیقی بر این سرویس‌ها و زیرساخت‌ها خواهد داشت. ما به گسترش قابلیت‌ها، ابزارها و سرویس‌های متمرکز از طریق DHS، که به نحو مناسبی نظارت را بهبود می‌بخشد و با قوانین اجرایی، سیاست‌ها، استانداردها و دستورالعمل‌ها مطابق است، ادامه خواهیم داد. به‌نظر می‌رسد برای تحقق این امر به قوانین و معماری‌های جدیدی نیاز است که دولت را قادر به استفاده بهتر از دستاوردها می‌نماید. DOD و IC این فعالیت‌ها را به‌عنوان کارهایی که به‌طور مناسبی ایمنی سیستم‌های امنیت ملی، سیستم‌های DOD و سیستم‌های IC بهبود می‌بخشند، در نظر خواهند گرفت.

1. Intelligence Community
2. Department of Homeland Security

۲-۱. همترازی مدیریت خطرات و فعالیت‌های فناوری اطلاعات

فرمان اجرایی ۱۳۸۳۳، در مورد ارتقا کارایی افسران اطلاعاتی مدیر آژانس، افسران مدیر اطلاعاتی(CIO[3]) را برای دستیابی به سطح بالاتری از تکنولوژی کارا جهت انجام مأموریت‌های آژانس، کاهش کارهای تکراری و ساخت فناوری اطلاعات مؤثرتر تقویت می‌نماید. رهبران وزارتخانه و آژانس نیروهای مورد اطمینان CIO خود را جهت همترازی تصمیمات مدیریت خطرهای مربوط به امنیت سایبری و تصمیمات مربوط به تأمین بودجه و تهیه فناوری اطلات تقویت و حمایت خواهند کرد. دولت از طریق OMB و DHS به هدایت و راهنمایی فعالیت‌های مدیریت خطر در ادارات و آژانس‌های غیرنظامی فدرال ادامه خواهد داد، و نیروهای CIO برای انجام نقش رهبری پیشگیرانه و اطمینان از اینکه تصمیمات مربوط به تدارکات IT به‌درستی برای ایمن‌سازی داده‌ها و شبکه‌ها اولویت‌بندی شده‌اند، قدرت بیشتری خواهند گرفت.

۳-۱. بهبود مدیریت خطر زنجیره تأمین فدرال

دولت می‌خواهد مدیریت خطر زنجیره تأمین را با تدارکات آژانس و فرایند مدیریت خطر یکی کند. این کار مطابق با نیازهای فدرال برای اطمینان بیشتر از امنیت و قابلیت اعتماد تکنولوژی‌های به‌کار گرفته شده توسط دولت

3. Chief Information Officers

فدرال می‌باشد و شامل اشتراک‌گذاری بهتر اطلاعات میان ادارات و آژانس‌هاست تا آگاهی از تهدیدات مربوط به زنجیره تأمین بیشتر شود و فعالیت‌های تکراری زنجیره تأمین در دولت ایالات متحده، ازجمله ایجاد سرویس اشتراک‌گذاری تخمین خطر زنجیره، کاهش یابد. همچنین شامل یافتن کمبودهای سیستم به‌کار گرفته شده فدرال، مانند ایجاد اختیارات بیشتر برای حذف واسطها، محصولات و سرویس‌های تعدیل شده است. این اقدامات با اقدامات مدیریت خطر زنجیره تأمین در زیرساخت‌های ملی همگام خواهند شد.

۴-۱. تقویت امنیت سایبری پیمانکاران فدرال

ایالات متحده نمی‌تواند اطلاعات و یا سیستم‌های حساس دولتی را که توسط پیمانکاران به‌طور ناکافی ایمن‌سازی شده‌اند نادیده بگیرد. پیمانکاران خدمات مهمی برای دولت ایالات متحده انجام می‌دهند و باید سیستم‌هایی که از آن طریق سرویس‌رسانی می‌کنند به‌طور مناسبی ایمن‌سازی شوند. در ادامه، دولت فدرال قادر خواهد بود امنیت داده‌هایش را با بررسی روش‌های مدیریت خطر پیمانکاران و انجام تست‌ها، آزمایشات و واکنش‌های مناسب سیستم‌های پیمانکاران در برابر حوادث بسنجد. قراردادها با وزارتخانه‌ها و آژانس‌های فدرال جهت تصویب فعالیت‌هایی با هدف ارتقا امنیت سایبری طراحی خواهند شد. در این میان یکی از نگرانی‌هایی که مطرح می‌شود پیمانکارانی هستند که در مراکز صنعتی دفاعی مسئول تحقیقات و توسعه سیستم‌های کلیدی‌ای هستند که توسط DOD به‌کار گرفته می‌شوند. به علاوه، همان‌طور که در گزارش دستور اجرایی ۱۳۸۰۰ به ریاست جمهور در مدرن نمودن فناوری اطلاعات فدرال توصیه شده، دولت از اتخاذ استراتژی‌های به‌کارگیری تلفیقی جهت بهبود امنیت سایبری و کاهش هزینه‌های فراوان مربوط به استفاده از مقررات قراردادهای متناقض در دولت فدرال حمایت خواهد کرد. همچنین اقداماتی برای اطمینان از اینکه پیمانکاران فدرال بتوانند در صورت لزوم، اطلاعات قابل اشتراک و مربوط به نقاط آسیب‌پذیر و تهدیدات را دریافت و استفاده نمایند، انجام خواهد گرفت.

۵-۱. اطمینان از رهبری دولت به بهترین و نوآورانه‌ترین حالت

دولت فدرال از اینکه سیستم‌های تحت نظارت و اداره او مطابق با استانداردها و در بهترین وضعیت امنیت سایبری مورد توصیه صنایع قرار دارند، اطمینان حاصل خواهد کرد. پروژه‌هایی که بودجه فدرال را دریافت می‌کنند نیز باید از این استانداردها پیروی نمایند. دولت فدرال از قدرت خرید خود برای بهبود عملکرد بخش‌های مختلف در محصولات و خدمات استفاده خواهد کرد. همچنین دولت فدرال، رهبر توسعه و اجرای استانداردها به بهترین صورت و حتی در حوزه‌های جدید و نوظهور خواهد بود. به‌عنوان مثال، رمزنگاری کلیدی عمومی برای عملکرد امن زیرساخت‌های

حیاتی ما ضروری هستند. وزارت دفاع برای محافظت از تهدید بالقوه‌ای که کامپیوترهای کوانتوم در توانایی شکستن رمزنگاری‌های کلیدی عمومی دارند، از طریق مؤسسه ملی استاندارد و تکنولوژی، [1] (NIST)، به جستجو، ارزیابی و استانداردسازی الگوریتم‌های رمزنگاری کلیدی عمومی مقاوم در برابر کوانتوم ادامه خواهند داد. ایالات متحده با حمایت از قبول سریع استانداردهای NIST در زیرساخت‌های دولتی و با تشویق مردم برای انجام این کار، جلودار ارتباطات محافظت شده خواهد بود.

۲. زیرساخت‌های حیاتی ایمن

مسئولیت ایمن‌سازی زیرساخت‌های حیاتی ملی و مدیریت خطر امنیت سایبری بین بخش‌های خصوصی و دولت فدرال به اشتراک گذاشته می‌شود. با همکاری بخش خصوصی، ما از یک روش تجمعی مدیریت خطر جهت کاهش آسیب‌ها و افزایش میزان امنیت سایبری زیرساخت‌های حیاتی استفاده خواهیم کرد. ما به‌طور همزمان از روش‌های نتیجه‌گرا برای کاهش اقدامات دشمنان بسیار پیشرفته‌مان که می‌توانند تخریب‌هایی در سایز بزرگ و یا طولانی‌مدت برای زیرساخت‌های حیاتی به‌وجود بیاورند، استفاده خواهیم نمود. ما همچنین فعالان سایبری دشمن را با اعمال هزینه‌هایی برای آنها و اسپانسرهایشان با استفاده از ابزارهای مختلفی که تنها محدود به پیگرد قانونی و تحریم‌های اقتصادی نیست، باز خواهیم داشت.

اولویت‌بندی اقدامات:

۲-۱. بازسازی نقش‌ها و مسئولیت‌ها

دولت نقش‌ها و مسئولیت‌های آژانس‌های فدرال و انتظاراتی که از بخش خصوصی در ارتباط با مدیریت خطر امنیت فضای سایبری و واکنش به حوادث می‌رود، روشن خواهد کرد. این شفافیت امکان مدیریت خطر پیشگیرانه برای یافتن تهدیدات، آسیب‌پذیری‌ها و نتایج را ایجاد خواهد کرد. همچنین سبب شناسایی و ایجاد ارتباط شکاف‌های موجود بین اقدامات پاسخگو در هنگام حوادث خواهد شد و آموزش‌های روتین، تمرین‌ها و هماهنگی‌ها را افزایش خواهد داد.

۲-۲. اولویت‌بندی اقدامات بنا بر خطرات ملی شناسایی شده

دولت فدرال با بخش خصوصی برای مدیریت خطرات مربوط به زیرساخت‌های حیاتی، که بیشتر در معرض خطر هستند، همکاری خواهد کرد. دولت با شناسایی توابع حیاتی ملی، به شناخت جامعی از خطرات ملی خواهد رسید و با مدیریت بهتر این خطرات ملی، پیشنهادها و مشارکت‌های امنیت فضای سایبری ما را رشد خواهد داد. دولت اقدامات کاهش خطرات را در هفت حوزه کلیدی اولویت‌بندی خواهد نمود: امنیت ملی، انرژی و قدرت، بانکداری و امور مالی، سلامت و ایمنی، ارتباطات، فناوری اطلاعات و حمل‌ونقل.

1. National Institute of Standards and Technology

۲-۳. ارتقا ارائه‌دهندگان خدمات فناوری اطلاعات و ارتباطات به‌عنوان ایجادکنندگان امنیت سایبری

فناوری اطلاعات و ارتباطات، (ICT)[1]، اساس هر بخشی در آمریکاست. ارائه‌دهندگان ICT در جایگاه ویژه‌ای برای شناسایی، جلوگیری و کاهش خطرات قبل از صدمه به کاربرانش قرار دارند. دولت فدرال باید برای بهبود امنیت و انعطاف‌پذیری ICT به شیوه‌ای هدفمند و مؤثر، و همچنین حفظ حریم شخصی و آزادی‌های مدنی، با این ارائه‌دهندگان همکاری نماید. دولت ایالات متحده جهت توانمندسازی ارائه‌دهندگان ICT در واکنش و اصلاح فعالیت‌های سایبری مخرب در مرحله شبکه، اقداماتی برای افزایش اشتراک‌گذاری اطلاعات انجام خواهد داد. این اقدامات شامل اشتراک‌گذاری تهدیدات کلاسه‌بندی شده و اطلاعات آسیب‌پذیر با اپراتورهای ICT خواهد بود و همچنین تا حد ممکن اطلاعات را به مرحله غیرکلاسه‌بندی شده تنزیل خواهد داد. ما زنجیره تأمین تکنولوژی ایمن، پایدار و قابل انعطاف را که براساس بهترین روش‌ها و استانداردها از امنیت حفاظت کند، ارتقا خواهیم داد. دولت ایالات متحده، ذی‌نفعان را برای یافتن راه‌حلی در برابر چالش‌هایی که در شبکه‌ها، دستگاه‌ها و لایه‌های ورودی به‌وجود می‌آید، دور هم جمع خواهد کرد. ما سازمان‌های صادرکننده گواهی صنعتی را جهت اطمینان از کارایی راه‌حل‌ها در بازار در حال رشد و در معرض تهدید تشویق خواهیم کرد.

۲-۴. حفاظت از دمکراسی‌مان

حفاظت از فرایندهای دمکراتیک ما برای ایالات متحده و متحدان دمکراتیک‌مان از اهمیت بالایی برخوردار است. مقامات دولتی محلی و ایالتی در ایالات متحده زیرساخت‌های انتخاباتی متنوعی را اجرا می‌کنند. بنابراین درصورت نیاز، ما خدمات فنی و مدیریت خطر را فراهم خواهیم نمود، از آموزش و تمرین حمایت خواهیم کرد، از خطراتی که این بخش را تهدید می‌کند آگاهی خواهیم داد و اطلاعات تهدیدها را با مقامات به‌منظور آمادگی و محافظت از زیرساخت‌های انتخابات، به اشتراک خواهیم گذاشت. دولت فدرال به هماهنگ‌سازی توسعه استانداردهای امنیت سایبری، راهنمایی‌های مربوط به حفاظت از فرایند انتخابات و ابزار ارائه‌دهنده یک سیستم امن، ادامه خواهد داد. در صورت وقوع حوادث سایبری مهم، دولت فدرال آمادگی دارد تا در برابر تهدیدات، عکس‌العملی مناسب برای بهبود زیرساخت‌های انتخاباتی نشان دهد.

۲-۵. افزایش سرمایه‌گذاری در امنیت سایبری

بیشترین خطرات امنیت سایبری زیرساخت‌های حیاتی ناشی از آسیب‌پذیری‌های شناخته شده هستند. دولت ایالات متحده با نهادهای بخش خصوصی و دولتی جهت افزایش شناسایی خطرات امنیت

1. Information and Communication Technology

سایبری کار خواهد کرد. درنتیجه آنها تصمیمات مدیریت خطر را آگاهانه‌تر می‌گیرند، در اقدامات امنیتی مناسب سرمایه‌گذاری می‌نمایند و مزایای آن سرمایه‌گذاری را درک می‌کنند.

۲-۶. اولویت‌بندی سرمایه‌گذاری‌های توسعه و تحقیق ملی

دولت فدرال برنامه امنیت زیرساخت‌های حیاتی ملی و تحقیق انعطاف‌پذیر و توسعه را جهت اولویت‌بندی یافتن خطرات امنیت سایبری که زیرساخت‌های حیاتی را تهدید می‌کنند، به‌روزرسانی خواهد کرد. وزارتخانه‌ها و آژانس‌ها سرمایه‌گذاری‌های خود را براساس اولویت‌ها تراز خواهند کرد و در این کار بیشتر روی ایجاد روش‌های امنیت سایبری‌ای که از تکنولوژی‌های نوظهور استفاده کنند، اشتراک‌گذاری اطلاعات و مدیریت خطر بخش‌های متقابل را بهبود بخشند، و در برابر اختلالات با مقیاس‌های بزرگ و یا طولانی‌مدت مقاوم باشند، تمرکز خواهند نمود.

۲-۷. بهبود امنیت سایبری حمل‌ونقل و دریایی

اقتصاد و امنیت ملی آمریکا برپایه حمل‌ونقل و تجارت جهانی قرار دارد. اینکه ما بتوانیم مواردی مانند: حرکت به‌موقع و امن کالاها، خطوط باز ارتباطی دریایی و هوایی، دسترسی به نفت و گاز طبیعی و قابلیت دسترسی به زیرساخت‌های حیاتی را تضمین نماییم، برای اقتصاد و امنیت ملی ما بسیار ضروری است. مدرن‌سازی این بخش‌ها باعث شده تا در برابر حملات سایبری آسیب‌پذیرتر بشوند. امنیت سایبری دریایی از اهمیت ویژه‌ای برخوردار است، چراکه تأخیر و یا از دست دادن محموله‌ها می‌تواند سبب اختلالات اقتصادی استراتژیک گردد و به‌طورگسترده روی صنایع پایین‌دستی اثر بگذارد. با توجه به اهمیت حمل‌ونقل دریایی برای ایالات متحده و اقتصاد جهانی و کاهش حداقل ریسک سرمایه‌گذاری در برابر سوءاستفاده‌های سایبری که تاکنون انجام شده‌اند، به‌سرعت اقدامات زیر را انجام خواهد گرفت: مشخص نمودن نقش‌ها و مسئولیت‌های امنیت سایبری دریایی، ارتقای مکانیسم‌ها جهت هماهنگی بین‌المللی و اشتراک‌گذاری اطلاعات، و تسریع توسعه نسل بعدی زیرساخت‌های دریایی منعطف سایبری. ایالات متحده حمل‌ونقل بدون وقفه کالاها را، با وجود همه تهدیدهایی که برای این زیرساخت بین‌المللی به‌وسیله ابزار سایبری وجود دارد، تضمین خواهد کرد.

۲-۸. بهبود امنیت سایبری فضایی

ایالات متحده دسترسی بدون قید و استفاده آزاد از فضا را برای پیشرفت امنیت، رفاه اقتصادی و دانش علمی کشور ضروری می‌داند. دولت از رشد فعالیت‌های سایبری که دارایی‌های فضایی و حفاظت از زیرساخت‌ها را تهدید می کند، بسیار نگران است. چراکه این دارایی‌ها برای عملکردهایی چون موقعیت‌یابی،

حمل‌ونقل و زمان‌بندی (PNT)[1]؛ جاسوسی، نظارت و شناسایی دشمن، (ISR)[2]؛ ارتباطات ماهواره‌ای و پیش‌بینی آب و هوا حیاتی هستند. دولت اقداماتش را برای محافظت از دارایی‌های فضایی‌مان و حمایت از زیرساخت‌ها در برابر تهدیدات سایبری تکامل‌یافته افزایش خواهد داد و ما با صنایع و شرکای بین‌المللی‌مان در تقویت سایبری سیستم‌های فضایی موجود و آنچه در آینده درست می‌شود، همکاری خواهیم نمود.

۳. مبارزه با جرائم سایبری و بهبود گزارش‌دهی حوادث

وزارتخانه‌ها و آژانس‌های فدرال با همکاری نهادهای دولتی ایالتی، محلی، قومی و ارضی، نقشی مهم در شناسایی، جلوگیری، اختلال و رسیدگی به تهدیدات سایبری برای کشورمان انجام می‌دهند. ایالات متحده آمریکا قربانی فعالیت‌های سایبری خصمانه جنایتکاران می‌گردد. این جنایتکاران، فعالان دولتی و غیردولتی و پراکسی‌هایشان و تروریست‌هایی هستند که از زیرساخت شبکه در ایالات متحده و یا خارج از آن استفاده می‌نمایند. اجرای قانون فدرال سبب تعقیب قانونی و دستگیری مجرمان، از کار انداختن زیرساخت‌های مجرمانه، محدود کردن گسترش و استفاده از قابلیت‌های مخرب سایبری می‌شود و جلوی سود بردن مجرمان سایبری و دولت‌های حامی آنها را می‌گیرد و دارایی‌های‌شان را ضبط می‌کند. دولت برای اطمینان از اینکه وزارتخانه‌ها و آژانس‌های فدرال دارای اختیارات و منابع لازم برای مبارزه با فعالیت‌های مجرمانه سایبری فراملی هستند تأکید خواهد کرد. این اختیارات و منابع جهت مبارزه با فعالیت‌های اقتصادی جاسوسی و همچنین شناسایی و از بین بردن بات‌نت‌ها، بازار سیاه و سایر زیرساخت‌هایی است که برای اقدامات مجرمانه سایبری استفاده می‌شوند. برای اینکه مبارزه با تهدیدات سایبری مؤثرتر گردد، اجرای قانون با همکاری صنایع خصوصی انجام خواهد گرفت. چراکه برای روبه‌رو شدن با مشکلاتی که به‌دلیل موانع تکنولوژیکی وجود دارند، از قبیل تکنولوژی‌های شناسایی و کدگذاری، به صنایع خصوصی برای ایجاد شواهد حساس به زمان جهت طی درست روندهای قانونی نیاز دارند. اقدامات اجرای قانون برای مبارزه با جرائم سایبری مانند ابزاری از قدرت ملی برای بازداشتن آن فعالیت‌ها عمل می‌کند.

اولویت‌بندی اقدامات:

۳-۱. بهبود گزارش‌دهی حوادث و واکنش

دولت ایالات متحده به تشویق قربانیانی که اطلاعاتشان سرقت شده و سوءاستفاده شده، به‌خصوص شرکای زیرساخت‌های حیاتی، ادامه خواهد داد. ترویج گزارش‌دهی حوادث سایبری به دولت فدرال برای نشان دادن عکس‌العمل مناسب، پیوند زدن حوادث مرتبط، شناسایی

1. Positioning, Navigation, Timing
2. Intelligence, Surveillance, Reconnaissance

عاملان جنایت و جلوگیری از حوادث آینده بسیار ضروری است.

۲-۳. مدرن‌سازی نظارت الکترونیکی و قوانین جرائم اینترنتی

دولت برای جمع‌آوری قانونی مدارک لازم مربوط به فعالیت‌های مجرمانه، از بین بردن زیرساخت‌های مجرمانه از طریق احکام مدنی و وضع عواقب مناسب برای مجرمان سایبری، با کنگره کار خواهد کرد. این همکاری برای به‌روزرسانی نظارت الکترونیکی و قوانین جرائم کامپیوتری خواهد بود تا ظرفیت اجرای قوانین افزایش یابد.

۳-۳. کاهش تهدیدات سازمان‌های جنایتکار فرامرزی در فضای سایبری

هک کردن کامپیوتر توسط گروه‌های جنایتکار فرامرزی تهدیدی جدی برای امنیت ملی ما به‌حساب می‌آید. گروه‌های جنایتکار سازماندهی شده با حمایت‌های مالی قابل توجه در خارج از مرزها، از نرم‌افزارهای مخرب پیچیده، عملیات‌های سرقت داده‌ها در فضای سایبری (کمپین‌های اسپیر فیشینگ)،[۱] و سایر ابزارهای هک کردن – که بعضی‌شان در پیچیدگی با آن کشورها رقابت می‌نمایند – استفاده می‌کنند تا سیستم‌های مالی حساس را هک کنند، شکست داده‌های زیادی را هدایت کنند، باج افزارها را گسترش دهند، به زیرساخت‌های حیاتی حمله کنند و دستاوردهای فکری را سرقت نمایند. دولت از اجرای قانون به‌منظور داشتن ابزاری مؤثر و قانونی در بررسی و تعقیب چنین گروه‌هایی و مدرن‌سازی قوانین جرائم سازمان‌یافته برای استفاده در برابر این تهدیدات حمایت خواهد کرد.

۴-۳. تسهیل دستگیری مجرمان در خارج از مرز

جلوگیری از جنایات سایبری به یک تهدید جدی نیاز دارد که مجرمان شناسایی، دستگیر و محاکمه خواهند شد. بااین‌حال، بعضی از کشورهای خارجی تصمیم دارند که با درخواست استرداد مجرمان همکاری نکنند، محدودیت‌های بدون دلیل وضع نمایند و یا در این قبیل اقدامات مداخله کنند. ایالات متحده به شناسایی شکاف‌ها و مکانیسم‌های لازم جهت محاکمه مجرمان سایبری خارجی ادامه خواهد داد. همچنین دولت ایالات متحده دیپلماسی و سایر تلاش‌های خود را با دیگر کشورها برای افزایش همکاری در درخواست استرداد قانونی مجرمان افزایش خواهد داد. ما سایر کشورها را تحت فشار خواهیم گذاشت تا به‌سرعت در تحقیقات کمک کنند و با هر توافق دوجانبه یا چندجانبه‌ای موافقت کنند یا متعهد شوند.

---

۱. فیشینگ (Phishing) تلاش متقلبانه برای به دست آوردن اطلاعات حساس مانند نام کاربری، گذرواژه‌ها و جزئیات کارت اعتباری از طریق جا زدن خود به عنوان یک نهاد قابل اعتماد در یک ارتباط الکترونیکی است. به طور معمول، فریب دادن از طریق ایمیل یا پیام‌رسانی فوری انجام می‌شود. اغلب، کاربران را راهنمایی می‌کنند تا اطلاعات شخصی خود را در یک وب‌سایت جعلی- که مطابق با ظاهر و احساس سایت قانونی است- وارد کنند. تلاش‌های فیشینگ معطوف به افراد یا شرکت‌های خاص با عنوان نیزه فیشینگ (spear phishing) نامیده شده‌اند. برخلاف فیشینگ انبوه و غیرهدفمند، مهاجمان فیشینگ نیزه اغلب برای افزایش احتمال موفقیت‌شان، اطلاعات شخصی در مورد هدف خود را جمع‌آوری و استفاده می‌کنند.

۵-۳. افزایش ظرفیت اجرای قانون کشورهای شریک برای مبارزه با فعالیت‌های سایبری مجرمانه

ایالات متحده به کشورهای شریک متمایل کمک خواهد کرد تا ظرفیت خود را برای یافتن فعالیت‌های سایبری مجرمانه بالا ببرند. مقابله با ماهیت بدون مرز بودن جرائم سایبری، ازجمله فعالیت‌های تروریستی و با حمایت دولت‌ها، نیازمند همکاری در اجرای قوی قوانین بین‌المللی می‌باشد. این همکاری به آژانس‌های خارجی اجرای قوانین نیازمند است که هنگام درخواست، توانایی‌های فنی لازم برای کمک به اجرای قانون ایالات متحده را داشته باشند.

امنیت ملی آمریکا در تلاش است همچنان به ایجاد ظرفیت برای مبارزه با جرائم سایبری ادامه دهد و همکاری قوی بین‌المللی را برای اجرای قوانین تسهیل نماید. همچنین ایالات متحده برای افزایش همکاری بین‌المللی در روبه‌رو شدن با فعالیت‌های سایبری خصمانه، نظیر ایجاد راه‌حل‌هایی برای موانع بالقوه‌ای که در جمع‌آوری و به اشتراک‌گذاری شواهد وجود دارد، تلاش خواهد نمود. ایالات متحده همچنین توسعه سیستم‌های متقابل و دو طرف سودمند را رهبری خواهد نمود تا بتواند برای اهداف اجرای قوانین و کاهش موانع هماهنگی، کشورهای خارجی را به تبادل اطلاعات تشویق نماید. همچنین دولت استفاده مؤثر از ابزار بین‌المللی موجود را، مانند کنوانسیون ایالات متحده برای مقابله با جرائم تروریستی سازمان‌یافته و نقاط شبکه‌های اتباطی G7 24/7، خواستار خواهد شد. درنهایت ما برای گسترش توافق مجامع بین‌المللی روی کنوانسیون جرائم سایبری اتحادیه اروپا (کنوانسیون بوداپست) تلاش‌هایی نظیر حمایت بیشتر برای تصویب این کنوانسیون خواهیم نمود.

اصل دو ـ افزایش رفاه آمریکا

اینترنت مزایای فراوانی را در داخل و خارج از کشور ایجاد کرده و به پیشرفت و ارتقای ارزش‌های آمریکایی آزادی، امنیت و رفاه کمک کرده است. در کنار این رشد، مشکلاتی نیز به‌وجود آمده که امنیت ملی ما را تهدید می‌کند. ایالات متحده جهت یافتن راه‌حلی برای این تهدیدها و سایر مشکلات، یک روش جامع و منسجم را شرح خواهد داد تا از منافع ملی آمریکا در این دنیا رو به دیجیتالی شدن حفاظت کند.

هدف: حفظ تأثیر ایالات متحده در اکوسیستم تکنولوژیکی و توسعه فضای سایبری به‌عنوان عامل محرک رشد اقتصادی، نوآوری و کارایی.

۱. ایجاد یک اقتصاد دیجیتالی منعطف و پر تکاپو

امنیت اقتصادی ذاتاً به امنیت ملی ما وابسته است. از آنجا که پایه‌های اقتصاد ما به‌طور فزاینده‌ای در حال ریشه دواندن در تکنولوژی‌های دیجیتالی است، دولت ایالات متحده استانداردهایی را مدل نموده و گسترش خواهد داد تا از امنیت اقتصادی ما محافظت کند و رونق بازارهای آمریکا و نوآوری‌های آمریکایی را تقویت کند.

اولویت اقدامات:

۱-۱. انگیزش یک بازار دیجیتالی امن و مناسب

برای بهبود انعطاف فضای سایبری، دولت انتظار دارد که بازار تکنولوژی از توسعه و پیاده‌سازی مستمر، اتخاذ و تکامل فرایندها و تکنولوژی‌های امنیتی نوآورانه حمایت نموده و به آنها پاداش دهد. دولت تلاش خواهد کرد تا گروه‌های ذی‌نفع، ازجمله بخش خصوصی و جامعه مدنی، برای ترویج روش‌های بهتر و توسعه استراتژی‌ها جهت غلبه بر موانعی که جلوی پذیرفتن تکنولوژی ایمن قرار دارد تلاش کنند. دولت سعی خواهد کرد تا با بالا بردن آگاهی و شفافیت در مورد اقداماتی که در فضای مجازی صورت می‌گیرد، برای سرویس‌ها و محصولات ایمن در بازار تقاضا ایجاد کند. درنهایت، دولت با شرکای بین‌المللی همکاری خواهد کرد تا استانداردهای مبتنی‌بر صنعت و باز و با حمایت دولتی را ترویج دهند. این امر به‌عنوان روش‌هایی مناسب و مبتنی‌بر ریسک برای حل مشکلات امنیت فضای مجازی، شامل روش‌های سرویس پلتفرم و مدیریتی می‌باشد که موانع موجود در راه ایمن‌سازی اقدامات صورت گرفته در این اکو سیستم را کمتر خواهد کرد.

۱-۲. اولویت‌دهی به نوآوری

دولت ایالات متحده به‌کارگیری و به‌روزرسانی مستمر استانداردها و اقدامات بازدارنده را در برابر تهدیدات موجود و تهدیدات در حال شکل‌گیری و همچنین خطراتی که در تمام زمینه‌های اکوسیستم سایبری وجود دارند، ارتقا خواهد داد. این استانداردها و اقدامات به‌جای وابستگی به خصوصیات دقیق زمانی، باید مبتنی‌بر نتیجه و براساس قوانین تکنولوژیکی صحیح باشد. دولت به جهت کاهش تهدیدات سایبری موانع سیاسی‌ای را که یک صنعت امنیت سایبری را از توسعه، اشتراک‌گذاری و ایجاد قابلیت‌های نوآورانه منع می‌نماید حذف خواهد کرد.

۱-۳ سرمایه‌گذاری روی زیرساخت‌های نسل بعدی

دولت، در حالی که از قدرت خرید دولت فدرال برای افزایش انگیزه در حرکت به سمت زنجیره‌های تأمین ایمن‌تر استفاده می‌نماید، توسعه سریع و گسترش نسل بعدی ارتباطات مخابراتی و زیرساخت‌های ارتباطی اطلاعاتی را اینجا، در ایالات متحده، تسهیل خواهد کرد.

دولت برای تسهیل توسعه و ایمنی G5، بررسی راه‌حل‌های تکنولوژیکی و برپایه طبقه‌بندی و زمینه‌سازی برای فناوری‌های فراتر از پیشرفت‌های نسل بعد با بخش خصوصی کار خواهد کرد. دولت ایالات متحده استفاده از فناوری‌های نوظهور را، مانند هوش مصنوعی و محاسبات کوانتومی، در حالی که خطرات ذاتی استفاده و کاربرد آنها را در نظر می‌گیرند، بررسی خواهند کرد. ما با بخش خصوصی و جوامع مدنی همکاری خواهیم کرد تا تمایلات در پیشرفت‌ها تکنولوژیکی را به جهت حفظ موضع تکنولوژیکی ایالات متحده در فناوری‌های متصل و برای اطمینان از امنیت اقداماتی که از خارج اتخاذ می‌شوند، درک نماییم.

۴-۱. ارتقای جریان آزاد داده در سراسر مرزها

کشورها اکثراً محدودیت‌سازی محلی داده‌ها و وضع قوانین را به‌عنوان راهی برای حفاظت دیجیتالی به‌عنوان سرآغازی برای حفاظت ملی می‌دانند. این اقدامات بر رقابت‌پذیری شرکت‌های ایالات متحده تأثیر منفی خواهد گذاشت. ایالات متحده به رهبری مقابله با موانع غیرموجه در برابر جریان آزاد اطلاعات و تجارت دیجیتالی ادامه خواهد داد. دولت به همکاری خود با همتایان بین‌المللی جهت ارتقای استانداردهای باز مبتنی‌بر صنعت، محصولات نوآورانه و روش‌های مبتنی‌بر ریسکی که نوآوری‌های بین‌المللی و جریان آزاد اطلاعات اجازه می‌دهد، با در نظر گرفتن نیازهای امنیتی قانونی ایالات متحده، ادامه خواهد داد.

۵-۱. حفظ رهبری ایالات متحده در فناوری‌های نوظهور

اثرگذاری ایالات متحده در فضای سایبری به رهبری تکنولوژیکی ما مرتبط است. بنابراین دولت ایالات متحده برای محافظت از سرقت پیشرفته‌ترین تکنولوژی‌ها از جانب دشمنان‌مان، حمایت از تکنولوژی‌های رشد یافته، و تا حد امکان کاهش موانع حضور شرکت‌ها در بازار اقداماتی هماهنگ انجام خواهد داد. ایالات متحده نوآوری‌های امنیت سایبری آمریکا را در سراسر جهان از طرق زیر ترویج خواهد کرد: مشارکت‌های تجاری، افزایش آگاهی از ابزار و سرویس‌های امنیت سایبری نوآورانه آمریکا، افشای استفاده رژیم‌های سرکوبگر از چنین سرویس‌ها و خدماتی برای زیرپا گذاشتن حقوق بشر و کاهش موانع برای ایجاد یک بازار امنیت سایبری قوی جهانی.

۶-۱. ارتقای امنیت سایبری در تمام چرخه زندگی

ایالات متحده تلاش خواهد کرد تا با تأکید بر تنظیمات امنیتی اولیه قوی، محصولات ارتقاپذیر مناسب و انجام بهتر اقدامات اولیه هنگام تحویل کالا، امنیت سایبری را در تمام چرخه حیاتش ارتقا دهد. ما متوجه شده‌ایم که یک مسیر روشن به‌سمت یک بازار تکنولوژی انعطاف‌پذیر، پایدار و ایمن، تولیدکنندگان را به ساخت محصولاتی متفاوت براساس کیفیت

ویژگی‌های امنیتی‌شان تشویق خواهد کرد. دولت ایالات متحده روش‌های مهندسی پایه را برای کاهش آسیب‌پذیری سیستمی و توسعه طرح‌هایی که در صورت مورد حمله قرار گرفتن سیستم بتواند تأثیر آن را کاهش داده و خود را بازیابی نماید، ارتقا خواهد داد. دولت ایالات متحده از بهترین روش‌های صنایع متکی به جلو برای ارتقا تست‌ها و آزمایش‌های معمول امنیت سایبری و انعطاف محصولات و سیستم‌ها در حین توسعه آنها استفاده خواهد کرد. این امر شامل ارتقا و استفاده از قانون افشای هماهنگ شده آسیب‌پذیری‌ها،[1] تست‌های جمعیت‌ـمنبع (ساخت یک مجموعه داده با کمک گروه بزرگی از افراد)[2] و سایر ارزیابی‌های نوآورانه‌ای می‌شود که انعطاف‌پذیری را قبل از هر حمله یا سوءاستفاده بهتر می‌کند. همچنین دولت ایالات متحده چگونگی بهبود تمام مراحل چرخه زندگی را برای مدیریت هویت دیجیتال، شامل وابستگی بیش از حد به شماره‌های امنیت اجتماعی، ارزیابی خواهد کرد.

۲. پرورش و محافظت از نبوغ ایالات متحده

پرورش دادن و محافظت کردن از اختراعات و نوآوری‌های آمریکایی برای حفظ برتری استراتژیک ایالات متحده در فضای سایبری ضروری است. دولت ایالات متحده با ارتقای مؤسسات و برنامه‌هایی که رقابت‌پذیری ایالات متحده را در بردارند از نوآوری‌ها حمایت خواهد کرد. دولت ایالات متحده با ادغام‌کنندگان غارتگران و سرقت دستاوردهای فکری تلافی‌جویانه برخورد خواهد کرد. ما همچنین رهبری ایالات متحده را در تکنولوژی‌های نوظهور با ارتقای شناسایی و حمایت دولت از این تکنولوژی‌ها، ازجمله هوش مصنوعی، علم اطلاعات کوانتوم و زیرساخت ارتباطات مخابراتی نسل بعدی تسریع خواهیم کرد.

اولویت‌بندی اقدامات:

۲-۱. به‌روزرسانی مکانیسم‌ها برای بازنگری سرمایه‌گذاری و عملیات خارجی در ایالات متحده

محرمانگی، یکپارچگی و در دسترس بودن شبکه‌های ارتباطات مخابراتی ایالات متحده برای اقتصاد و امنیت ملی ما ضروری هستند. ما باید هوشیار باشیم تا از شبکه‌های ارتباطات مخابراتی که زندگی هر روزه ما به آن وابسته است محافظت کنیم. به‌این‌ترتیب دشمن نمی‌تواند با استفاده از آنها به ایالات متحده آسیبی برساند. دولت ایالات متحده این اهداف را با رسمیت بخشی و مؤثرسازی بازبینی ارجاع کمیسیون ارتباطات فدرال برای گواهی‌های ارتباطات مخابراتی موازنه خواهد کرد. دولت ایالات متحده یک پروسه شفاف را برای افزایش کارایی این بازبینی تسهیل خواهد کرد.

---

1. Coordinated Vulnerability Disclousure

۲. crowdsource اشاره دارد به: عمل به دست آوردن خدمات، ایده‌ها یا مطالب مورد نیاز با درخواست کمک‌هایی از گروه بزرگی از مردم و به ویژه از جامعه آنلاین به جای کارمندان یا تأمین‌کنندگان سنتی. البته معمولاً تیم آزمایش داراي منبع جمعیتی (crowdsource)، علاوه بر تیم تضمین کیفیت داخلی وجود دارد و جایگزین آن نیست.

۲-۲. حفظ یک سیستم حفاظتی متعادل و قوی از حق مالکیت معنوی

در عصر دیجیتال محافظت قوی از حق مالکیت معنوی، رشد مستمر اقتصاد و نوآوری را تضمین می‌کند. دولت ایالات متحده برای ایجاد یک سیستم حقوقی مالکیت معنوی جهانی که با حفاظت و اجرای حق مالکیت معنوی از قبیل حق ثبت اختراع، علائم تجاری و قانون کپی‌رایت باعث افزایش انگیزه برای تولید محصولات نوآورانه می‌گردد، تلاش کرده است و همچنان نیز کمک خواهد کرد. همچنین دولت ایالات متحده حفاظت از تکنولوژی‌های نوظهور حساس و اسرار تجاری را ارتقا خواهد بخشید و تلاش خواهد کرد تا دولت‌های متخاصم نتوانند به‌صورت ناعادلانه به این مزایا که توسعه و تحقیقات آن را آمریکایی‌ها انجام داده‌اند، دست یابند.

۲-۳. حفاظت از محرمانگی و یکپارچگی ایده‌های آمریکا

بیش از یک دهه است که فعالان مخرب با هدف قرار گرفتن اطلاعات تجاری محرمانه شرکت‌های آمریکایی در شبکه‌های بازرگانی آمریکا نفوذ سایبری نموده‌اند. این فعالان مخرب که از سایر ملیت‌ها هستند انبوهی از اسرار تجاری، داده‌های فنی و ارتباطات داخلی محرمانه حساس را به سرقت برده‌اند. دولت ایالات متحده با حفظ علاقه خود به جذب سرمایه، در برابر تخصیص غیرقانونی دانش فنی و تکنولوژی بخش‌های خصوصی و دولتی به رقبای خارجی خواهد ایستاد.

۲-۴. پرورش نیروی کار امنیت سایبری متخصص

داشتن نیروی کار امنیت سایبری توانمند یک مزیت استراتژیک برای امنیت ملی محسوب می‌شود. ایالات متحده سعی خواهد کرد در کنار پرورش انبوه آمریکاییان مستعد، بهترین و درخشان‌ترین افراد خارجی را که به ارزش‌های ما اهمیت می‌دهند جذب نماید.

۲-۵. ایجاد و حفظ زنجیره استعداد

رقبای همسنگ ما در حال پیاده‌سازی برنامه‌های پرورش نیروی کاری هستند که بتوانند در طولانی‌مدت به رقابت‌پذیری امنیت سایبری ایالات متحده آسیب برسانند. دولت ایالات متحده به سرمایه‌گذاری و توسعه برنامه‌هایی برای ساخت یک زنجیره استعداد از دوران ابتدایی تا پایان دوره متوسطه ادامه خواهد داد. همچنین دولت برای اطمینان از اینکه ایالات متحده دارای رقابت‌پذیرترین بخش در تکنولوژی است، از اصلاحات طرح مهاجرت مبتنی‌بر شایستگی رئیس‌جمهوری بهره خواهد برد. برای دستیابی به هدف مطلوب ممکن است نیاز باشد تا قوانینی اضافی وضع گردند.

۲-۶. توسعه فرصت مهارت‌یابی دوباره و آموزش برای کارکنان آمریکایی

دولت با همکاری کنگره بر ارتقا و تقویت فرصت‌های آموزشی و یادگیری جهت پرورش نیروی کار امنیت سایبری زبده کار خواهد کرد. این کار نیازمند این است که افراد مختلف با

پیش‌زمینه‌های متفاوت به استخدام فدرال درآیند، آموزش ببینند و مهارت پیدا کنند و فرصت‌های شغلی امنیت سایبری به آنها داده شود.

۲-۷. افزایش کارایی نیروی کار امنیت سایبری فدرال

جهت استخدام و جذب نیروهای متخصص و حرفه‌ای امنیت سایبری در دولت فدرال، دولت به استفاده از طرح نیروی ملی برای آموزش امنیت سایبری (NICE[1]) ادامه خواهد داد. این کار از سیاست‌هایی که اجازه می‌دهد از روش‌های استاندارد شده برای شناسایی، استخدام، پرورش و تعلیم نیروی کار امنیت سایبری مستعد، استفاده شود، حمایت می‌کند. به‌علاوه، دولت طرح‌هایی را برای ایجاد پرسنل امنیت سایبری تحت مدیریت وزارت خارجه بررسی خواهد کرد که این نیروها بر توسعه، مدیریت و اسقرار پرسنل امنیت سایبری در سایر وزارتخانه‌های فدرال، به استثنای DOD و IC، نظارت کنند. دولت در کنار آموزش‌های منحصر به فرد و ایجاد فرصت‌هایی برای استخدام و حفظ استعدادهای امنیت سایبری در پرتو رقابت با بخش خصوصی، پاداش‌های مالی نیروهای کار دولت ایالات متحده را نیز افزایش خواهد داد.

۲-۸. استفاده از قدرت اجرایی برای برجسته کردن و اعطای جایزه به استعدادها

دولت ایالات متحده با برجسته نمودن مربیان امنیت سایبری و متخصصان حرفه‌ای امنیت سایبری، سبب افزایش و شکوفایی بهترین‌ها خواهد شد. همچنین دولت ایالات متحده از همکاری‌های دولتی خصوصی برای توسعه و به اجرا درآوردن طرح NICE استفاده خواهد کرد، زیر این طرح روش‌های استاندارد شده‌ای برای شناسایی گپ‌های موجود در نیروی کار امنیت سایبری تهیه می‌کند و این در حالی است که همچنین برای آماده کردن، رشد و حفظ نیروی کاری که می‌تواند از زیرساخت‌های حیاتی و پایه‌های نوآوری آمریکا دفاع کرده و آنها را تقویت نماید، تلاش می‌کند.

1 National Initiative for Cyber security Education

اصل سوم ـ حفظ صلح در کنار قدرت

دولت‌ها و سایر گروه‌ها که مدت‌های زیادی در دنیای آفلاین بودند، امروزه در فضای سایبری چالش‌های فزاینده‌ای برای منافع امنیتی و اقتصادی ایالات متحده به‌وجود آورده‌اند. در حال حاضر این حضور مستمر در فضای سایبری توازن استراتژیک قدرت را تغییر می‌دهد. این دولت سیاست‌هایی را مطرح خواهد کرد که واقعیت‌های جدید امروزه را بازتاب دهد و دولت ایالات متحده را به‌سمت منافع استراتژیکی هدایت کند که از مردم آمریکا و روش زندگی ما حمایت کند. فضای سایبری دیگر گونه‌ای جدا از سیاست و یا فعالیتی جدا از سایر بخش‌های قدرت ملی نخواهد بود. ایالات متحده از گزینه‌های سایبری در هر بخشی از قدرت ملی استفاده خواهد کرد.

هدف: شناسایی، مقابله، تخریب، تنزل و جلوگیری از رفتارهای بی‌ثبات‌کننده و مخالف منافع ملی در فضای سایبری با حفظ غلبه ایالات متحده به‌وسیله فضای سایبری و در فضای سایبری.

۱. افزایش پایداری سایبری به‌وسیله قوانین رفتار دولت مسئول

ایالات متحده طرحی را برای رفتار دولت مسئول براساس قوانین بین‌المللی، پیروی از قوانین داوطلبانه غیرالزام‌آور رفتار دولت مسئول که در طول زمان صلح به‌کار گرفته می‌شود، و در نظر گرفتن اقداماتی تمرینی برای اعتمادسازی به هدف کاهش ریسک فعالیت‌های مخرب سایبری، ترویج خواهد کرد. این قوانین باید پایه‌ای باشند تا در برابر فعالیت‌های غیرمسئولانه دولت‌هایی که متناقض با این طرح عمل می‌کنند، اقداماتی هماهنگ صورت گیرد.

اولویت‌بندی اقدامات:

۱-۱. تشویق همبستگی جهانی به هنجارهای سایبری

قوانین بین‌المللی و قوانین داوطلبانه غیرالزام‌آور رفتار دولت مسئول در فضای سایبری، استانداردهای پایدارکننده و بهبوددهنده امنیتی را ایجاد می‌کند که رفتاری قابل قبول برای تمام دولت‌ها تعریف می‌نماید و قابلیت پیش‌بینی‌پذیری و ثبات را در فضای سایبری افزایش می‌دهد. ایالات متحده سایر کشورها را به تأیید این دیدگاه‌ها و قوانین از طریق ارتباطات توسعه‌یافته و شرکت در مجامع چندجانبه تشویق خواهد کرد. افزایش مقبولیت عمومی که توسط ایالات متحده و سایر دولت‌ها صورت می‌گیرد سبب رسیدن به انتظارات مقبول رفتار دولت خواهد شد و درنتیجه برای دستیابی به قابلیت پیش‌بینی‌پذیری و ثبات در فضای مجازی کمک می‌کند.

۲. برخورد و جلوگیری از رفتارهای غیرقابل قبول در فضای سایبری

همان‌طور که ایالات متحده روی ارتقای چگونگی رفتارهای دولت مسئول در فضای مجازی کار می‌کند، ما همچنین باید مطمئن شویم که برای رفتارهای غیرمسئولانه‌ای که به

ایالات متحده و شرکایش آسیب می‌رساند، عواقبی وجود دارد. تمام ابزار نیروی ملی برای پیشگیری، واکنش و بازداری فعالیت‌های سایبری بدخواهانه‌ای که در برابر ایالات متحده رخ می‌دهند، آماده هستند. این ابزار عبارتند از: ظرفیت‌های دیپلماتیک، اطلاعاتی، نظامی (پیاده و سایبری)، مالی، جاسوسی، میل عمومی و اجرای قانون. ایالات متحده با همکاری شرکای هم نظر خود از یک استراتژی یکپارچه جهت برخورد و جلوگیری از فعالیت‌های سایبری متخاصمانه استفاده می‌کند تا عواقبی سریع، پرهزینه و شفاف برای دشمنانی که می‌خواهند به ایالات متحده و شرکایش آسیب برسانند، وضع نمایند.

اولویت‌بندی اقدامات:

۲-۱. رهبری با جاسوسی هدفمند و مشارکتی

اداره IC به هدایت جهان با استفاده از جاسوسی سایبری تمام منابع جهت شناسایی و ردیابی فعالیت‌های سایبری خصمانه‌ای که منافع ملی ایالات متحده را تهدید می‌کند ادامه خواهد داد. این اطلاعات جاسوسی هدفمند و عملی بین دولت ایالات متحده و شرکای کلیدی‌اش جهت شناسایی برنامه‌های سایبری، مقاصد، توانایی‌ها، تحقیقات و توسعه برنامه‌ها، تاکتیک‌ها و فعالیت‌های عملی دشمنان خارجی دولتی و غیردولتی به اشتراک گذاشته خواهند شد تا برای حمایت از منافع آمریکا در داخل و خارج از مرزها تمام بدنه دولت آگاه باشند.

۲-۲. وضع عواقب

ایالات متحده عواقبی سریع و شفاف ایجاد خواهد کرد و ما با تعهد و الزام خود، آنها را برای جلوگیری از رفتارهای بد آینده اعمال خواهیم نمود. دولت برای اطمینان از به اجرا درآمدن یک فرایند به‌وقت و پایدار در واکنش و جلوگیری از فعالیت سایبری دشمن، برنامه‌ریزی‌های سیاسی بین‌اداری را برای دوره‌های زمانی پیش از، در حین و پس از اعمال عواقب به‌کار خواهد گرفت.

۲-۳. ایجاد یک ابتکار عمل بازدارنده سایبری

اگر اعمال عواقب با همراهی طیف وسیعی از دولت‌های همفکر اجرا شود، تأثیرگذارتر خواهد بود و پیامی قوی‌تر ارسال خواهد کرد. ایالات متحده برای ساخت یک چنین ائتلافی و ایجاد استراتژی‌های مناسب جهت اطمینان از درک عواقب رفتارهای سایبری خصمانه توسط دشمنان، یک ابتکار بازدارنده سایبری بین‌المللی را آغاز خواهد نمود. ایالات متحده با سایر دولت‌های همفکر از طریق اشتراک‌گذاری اطلاعات جاسوسی، حمایت از درخواست‌های مرتبط، اظهارات عمومی در حمایت از اقدامات صورت گرفته، و پیوستن به اعمال عواقب علیه افراد بدخواه؛ با یکدیگر برای هماهنگی و حمایت از یکدیگر در برابر حوادث سایبری خصمانه مهم همکاری خواهند کرد.

۴-۲. مقابله با نفوذ سایبری و عملیات اطلاعاتی دشمن

ایالات متحده تمام ابزار قدرت ملی را برای افشا و مقابله با عملیات نفوذ آنلاین و عملیات اطلاعاتی، تبلیغات و دادن اطلاعات اشتباه توسط دشمنان به‌کار خواهد بست. این اقدامات عبارتند از همکاری با شرکای دولت‌های خارجی و همچنین بخش خصوصی، دانشگاه‌ها و جامعه مدنی برای شناسایی، مقابله و جلوگیری از استفاده پلتفرم دیجیتالی برای اجرای عملیات نفوذ توسط دشمن خارجی البته در کنار احترام به آزادی‌ها و حقوق مدنی شهروندان.

اصل چهار ـ نفوذ پیشرفته آمریکا

جهان به ایالات متحده، جایی که بیشترین ابتکارات اینترنتی امروز در آن ایجاد شده، به چشم رهبری برای گستره بزرگی از مسائل سایبری فراملی می‌نگرد. ایالات متحده برای افزایش نفوذ آمریکا و رو به رویی با مسائل گسترده‌ای‌که منافعش را در فضای سایبری تهدید می‌کند و به چالش می‌کشد، در جایگاه رهبری بین‌المللی فعال باقی خواهد ماند. همکاری با دوستان و شرکا نیز برای آنکه مطمئن شویم می‌توانیم از ارتباطات مرزی، تولید محتوا و تجارت بر مبنای اینترنت باز و اینتاپرابل همچنان سود ببریم، ضروری است.

هدف: حفظ طولانی‌مدت باز بودن، قابلیت خدمات‌رسانی متقابل، امنیت و اطمینان‌پذیری اینترنت که از منافع ایالات متحده حمایت می‌نماید و تقویت می‌گردد.

۱. ترویج یک اینترنت باز، قابل تعامل[1]، قابل اعتماد و ایمن

اینترنت جهانی منجر به پیشرفت‌های بزرگی از زمان انقلاب صنعتی شده است و پیشرفت‌های گسترده‌ای در تجارت، سلامت، ارتباطات و سایر زیرساخت‌های ملی به‌وجود آورده است. در همین زمان، جنگ‌های قدیم بر سر حقوق انسانی و آزادی‌های اساسی، الان به‌صورت آنلاین رقم می‌خورند. آزادی بیان و آزادی برگزاری تجمعات صلح‌آمیز همچنان در معرض تهدید قرار دارند. به‌رغم رشد بی‌سابقه، همچنان پتانسیل اجتماعی و اقتصادی اینترنت تحت تأثیر سانسورها و سرکوب‌های آنلاین قرار می‌گیرد. ایالات متحده، شرکت‌ها را برپایه قوانینش جهت حمایت و ترویج یک اینترنت باز، اینتراپرابل، قابل اطمینان و ایمن ایجاد کرده است. ما همچنان کار خواهیم کرد تا مطمئن شویم روش ما برای ایجاد یک اینترنت

1. Interoperable

باز، استاندارد بین‌المللی است. ما همچنان روی باز داشتن دولت‌های اقتدارگرا که به اینترنت آزاد و باز به چشم یک تهدید سیاسی نگاه می‌کنند و اینترنت آزاد و باز را به یک وب اقتدارگرایانه تحت نظارت خود، در پوشش امنیت و مقابله با تروریسم تبدیل می‌نمایند، کار خواهیم کرد.

اولویت‌بندی اقدامات:

۱-۱. محافظت و افزایش آزادی اینترنت

دولت ایالات متحده، آزادی اینترنت را به‌عنوان فعالیتی آنلاین برای حقوق بشر و آزادی‌های اساسی، ازجمله آزادی بیان، آزادی برگزاری تجمعات صلح‌آمیز، آزادی در دین یا عقاید و حق حفظ حریم شخصی آنلاین، بدون در نظر گرفتن مرزها و رسانه، تصور می‌کند. به‌علاوه، آزادی اینترنت از جریان آزاد اطلاعات آنلاین حمایت می‌نماید. به این دلیل که جریان آزاد اطلاعات اینترنت، تجارت و کسب‌وکار بین‌المللی را بهبود می‌بخشد، سبب رشد نوآوری‌ها می‌شود و امنیت ملی و بین‌المللی را تقویت می‌کند. به همین ترتیب، قوانین آزادی اینترنت ایالات متحده شدیداً به امنیت ملی مرتبط است. آزادی اینترنت، یک قانون کلیدی راهنماست که سایر مسائل سیاست خارجی ایالات متحده را، ازجمله جرائم سایبری و فعالیت‌های مقابله با تروریسم، در نظر می‌گیرد. به همین دلیل، ایالات متحده سایر کشورها تشویق می‌نماید تا آزادی اینترنت را از طریق رویدادهایی نظیر ائتلاف آنلاین آزادی،[1] که ایالات متحده یکی از اعضای اصلی آن است، افزایش دهند.

۲-۱. همکاری با کشورهای همفکر، صنعت، دانشگاه و جامعه مدنی

ایالات متحده به همکاری خود با کشورهای همفکر، صنعت، دانشگاه، جوامع مدنی و سایر شرکا برای پیشرفت حقوق بشر و آزادی جهانی اینترنت و مقابله با تلاش‌های اقتدارگرایانه‌ای که برای سانسور و توسعه نفوذ اینترنت صورت می‌گیرد، ادامه خواهد داد. همچنین ایالات متحده به حمایت خود از جوامع مدنی به‌وسیله پشتیبانی‌های یکپارچه جهت توسعه تکنولوژی، آموزش ایمنی دیجیتال، حمایت سیاسی و پژوهش استمرار خواهد بخشید. هدف از این برنامه‌ها افزایش قابلیت‌های فردی شهروندان، فعالان، مدافعان حقوق بشر، خبرنگاران مستقل، سازمان‌های جوامع مدنی و افراد محروم جهت دسترسی ایمن و بدون سانسور به اینترنت و افزایش آزادی اینترنت در سطوح محلی، منطقه‌ای، ملی و بین‌المللی است.

۳-۱. ترویج یک مدل چندجانبه برای حاکمیت اینترنتی

ایالات متحده به حضور فعال خود در مجامع جهانی ادامه خواهد داد. این حضور باعث می‌شود که از غلبه مدل چندجانبه حاکمیت اینترنتی در برابر ایجاد طرح‌های دولت‌محوری که سبب

1. Freedom Online Coalition

تخریب آزادی و باز بودن اینترنت، ایجاد مانع بر سر راه ابتکارات و به خطر افتادن عملکرد اینترنت می‌شوند، اطمینان حاصل نماید. مدل چندجانبه حاکمیت اینترنتی به‌عنوان فرایندهایی شفاف، پایین به بالا و مورد اجماع تعریف می‌گردند که دولت‌ها، بخش خصوصی، جوامع مدنی، دانشگاه‌ها و انجمن‌های فنی را قادر می‌سازد با مقررات برابر در اینترنت شرکت نمایند. دولت ایالات متحده با شرکت فعالانه در تشکیلاتی کلیدی، از قبیل شرکت اینترنتی برای نام‌ها و شماره‌های اختصاص یافته،[1] انجمن‌های حاکمیت اینترنتی،[2] سازمان ملل متحد و اتحادیه ارتباطات بین‌المللی،[3] از ماهیت باز و اینتراپرابل اینترنت در عرصه‌های چندجانبه و بین‌المللی دفاع خواهد کرد.

۴-۱. ارتقای زیرساخت ارتباطات قابل تعامل و قابل اعتماد و اتصالات اینترنتی

ایالات متحده زیرساخت ارتباطات و اتصالات اینترنتی باز، اینتراپرابل، قابل اعتماد و ایمن را ارتقا خواهد داد. چنین سرمایه‌گذاری‌هایی فرصت‌های بزرگ‌تری برای رقابت شرکت‌های آمریکایی که در حال مقابله با نفوذ دخالت دولت‌های بالا به پایین هستند، در حوزه‌های رقابت بین‌المللی به‌وجود می‌آورد. همچنین با تقویت جایگاه رقابت‌پذیری صنایع ایالات متحده در اقتصاد دیجیتال جهانی، از امنیت و منافع اقتصادی آمریکا حمایت خواهد کرد. همچنین دولت از فعالیت‌های استانداردهای باز و صنعتی که براساس قوانین فنی صحیح هستند، حمایت و تقویت خواهد نمود.

۵-۱. ترویج و حفظ بازارهایی برای استعدادهای ایالات متحده در سراسر جهان

نوآوران و متخصصان امنیتی آمریکایی به‌طور ویژه‌ای در طراحی محصولات و سرویس‌هایی برای افزایش توانایی ما در ارتباطات و تعامل جهانی شرکت نموده‌اند که از زیرساخت ارتباطات، داده و ابزارها در سراسر جهان حفاظت می‌کنند. ایالات متحده به ترویج بازارهایی، همچون تکنولوژی‌های نوظهوری که هزینه ایمن‌سازی را کاهش می‌دهند، برای استعدادهای آمریکایی در خارج از کشور ادامه خواهد داد. همچنین ایالات متحده به‌کارگیری زیرساخت‌ها، ابتکارات، مدیریت ریسک، سیاست و استانداردهایی که در آینده دسترسی به اینترنت و قابلیت اینتراپرابلی، امنیت و پایداری اینترنت را در جهان تضمین می‌نماید، توصیه خواهد کرد. درنهایت ایالات متحده با شرکا و دولت‌های بین‌المللی، صنایع، جوامع مدنی و صاحبان تکنولوژی و دانشگاهیان همکاری خواهد کرد. این همکاری باعث می‌شود تا پذیرش و آگاهی از بهترین روش‌های امنیت سایبری در سراسر جهان افزایش یابد.

۲. ایجاد ظرفیت بین‌المللی سایبری

ایجاد ظرفیت، در حالی که به رسیدن اهداف دیپلماتیک، اقتصادی و امنیتی خارج از مرزها کمک می‌نماید، شرکا را برای حفاظت از خودشان و کمک به ایالات متحده در روبه‌رو شدن با تهدیداتی که منافع طرفین را هدف

1. Internet Corporation for Assigned Names and Numbers
2. The Internet Governance Forum
3. The International Telecommunication Union

قرار داده آماده می‌کند. ایالات متحده به‌وسیله ابتکارات ساخت ظرفیت سایبری مشارکت‌های استراتژیکی ایجاد می‌نماید که بهترین شیوه‌های امنیت سایبری را از طریق نگرشی کلی به اینترنت باز، اینتراپرابل، قابل اعتماد و ایمن که سبب جذب سرمایه‌گذاری می‌گردد و بازارهای اقتصادی جدیدی را باز می‌کند، ترویج می‌دهد. به‌علاوه ایجاد ظرفیت، فرصت‌های بیشتری برای به اشتراک‌گذاری اطلاعات تهدیدات سایبری به‌وجود می‌آورد، دولت ایالات متحده و شرکای ما را قادر می‌سازد در حالی که بر تمام مشارکت‌های سایبری دولت تمرکز می‌کند، از زیرساخت‌های داخلی حیاتی و زنجیره‌های تأمین جهانی بهتر دفاع نمایند. رهبری ما در ایجاد ظرفیت امنیت سایبری با شرکا برای حفظ نفوذ آمریکا بین رقبای جهانی بسیار ضروری است. ایجاد ظرفیت همکاری سایبری، شرکای بین‌المللی را در به کار گرفتن سیاست‌ها و روش‌هایی که به آن‌ها امکان می‌دهد همکاران مؤثری در ابتکارات بازدارندگی سایبری به رهبری ایالات متحده باشند تقویت خواهد نمود.

اولویت‌بندی اقدامات:

۱-۲. تقویت اقدامات ساخت ظرفیت سایبری

بسیاری از دوستان و شرکای ایالات متحده ظرفیت‌های سایبری منحصر به فردی دارند که می‌توانند ما را تکمیل کنند. ایالات متحده با این دوستان و شرکا برای تقویت ظرفیت‌ها و قابلیت اینتراپرابلی همکاری خواهد نمود و از این طریق توانایی‌هایمان را برای بهینه‌سازی مهارت‌های تلفیقی، منابع، قابلیت‌ها و دیدگاه‌های‌مان در برابر تهدیدات مشترک بهبود خواهد داد. همچنین شرکا می‌توانند در شناسایی، جلوگیری و غلبه بر این تهدیدات مشترک در فضای مجازی کمک نمایند. برای اینکه شرکای بین‌المللی درحالی‌که به دستاوردهای اجتماعی و اقتصادی اینترنت و ICTها پی می‌برند، بتوانند از زیرساخت‌های دیجیتالی خود محافظت و با تهدیدات مشترک مبارزه کنند، ایالات متحده به یافتن بلوک‌های ساختاری برای سازماندهی به اقدامات ملی در امنیت سایبری ادامه خواهد داد. ما همچنان به‌شدت در گسترش اقدامات برای اشتراک‌گذاری اطلاعات تهدیدهای سایبری عملیاتی و اتومات، افزایش همکاری‌های امنیت سایبری و ترویج تبادلات تکنیکی و تحلیلی تلاش خواهیم کرد. به‌علاوه، ایالات متحده با مشارکت و قابلیت‌های اجرای قانون شرکایمان در ساخت ظرفیت‌های سایبری‌شان، بر کاهش اثر و نفوذ فعالیت‌های تروریستی و جرائم سایبری بین‌المللی کار خواهد کرد.

مرکز پژوهش‌ها
مجلس شورای اسلامی

شناسنامه گزارش	شماره مسلسل: ۱۶۷۸۲

عنوان گزارش: استراتژی سایبری ملی ایالات متحده آمریکا (همراه با مروری بر مبانی و اهداف)

نام دفتر: مطالعات آموزش و فرهنگ

تهیه و تدوین: اسماعیل نوده‌فراهانی

مترجم: زهرا قربانعلی

ناظر علمی: سینا کلهر

ویراستار تخصصی: ـــــ

ویراستار ادبی: ـــــ

واژه‌های کلیدی:
۱. سیاستگذاری
۲. سند استراتژیک
۳. فضای مجازی
۴. صلح جاویدان

تاریخ انتشار: ۱۳۹۸/۹/۳۰