به نام خدا

استراتژی وزارت دفاع آمریکا در فضای مجازی

این گزارش ترجمه سند استراتژی وزارت دفاع آمریکا جهت اقدام در فضای سایبر با عنوان:
"Department Defense Strategy for Operating in Cyberspace"
است که توسط وزارت دفاع این کشور در سال ۲۰۱۱ منتشر شده است.

کد موضوعی: ۲۶۰
شماره مسلسل: ۱۱۰۴۹
مهرماه ۱۳۹۰
دفتر: مطالعات سیاسی

فهرست مطالب

استراتژی وزارت دفاع آمریکا در فضای مجازی

چکیده

با گسترش نفوذ فضای مجازی به زندگی افراد و جوامع بشری، امروزه امنیت فضای مجازی و توجه به تهدیدات آن به یکی از اولویت‌های اساسی دولت‌ها تبدیل شده است. این مسئله به‌ویژه به‌دلیل وابستگی حیات اجتماعی، اقتصادی، سیاسی و نظامی جوامع به فضای مجازی و آسیب‌پذیری‌های گسترده از سوءاستفاده‌های ناشی از کاربرد آن در حوزه‌های مختلف اهمیت بیشتری پیدا کرده است. براین اساس، وزارت دفاع آمریکا در این سند استراتژیک از یک‌سو در راستای ایمن‌سازی فضای مجازی که به آن وابسته است و ازسوی دیگر در راستای حمایت از امنیت ملی آمریکا و چالش‌های فضای مجازی آن به بررسی جنبه‌های اصلی تهدیدات فضای مجازی و راهکارهای استراتژیک مقابله با آن پرداخته است.

مقدمه

«تهدیدات امنیتی فضای مجازی نمونه‌ای از جدی‌ترین چالش‌های اقتصادی، سلامت عمومی و امنیت ملی است که ما به‌عنوان یک ملت با آنها روبرو هستیم».

استراتژی امنیت ملی، ۲۰۱۰

فضای مجازی ویژگی متمایزکننده زندگی مدرن است. افراد و اجتماعات در سرتاسر جهان، در فضای مجازی و از طریق آن خودشان را متصل، جامعه‌پذیر و سازماندهی می‌کنند. از سال ۲۰۰۰ تا ۲۰۱۰، استفاده جهانی از اینترنت از ۳۶۰ میلیون به ۲ میلیارد نفر افزایش پیدا کرده است. از آنجا که استفاده از اینترنت درحال گسترش است، فضای مجازی به‌طور چشمگیری تبدیل به جزء لاینفک زندگی در سرتاسر جهان خواهد شد.

شرکت‌های بین‌المللی و آمریکایی، کالاها و خدمات را در فضای مجازی دادوستد و سرمایه‌ها را در عرض چند ثانیه از این سو به آن سوی جهان منتقل می‌کنند. فضای مجازی، علاوه‌بر اینکه تجارت را در سایر بخش‌ها تسهیل می‌کند، خود نیز بخش مهمی از اقتصاد جهانی است. فضای مجازی به مولدی برای اشکال جدید مقاطعه‌کاری، پیشرفت‌های تکنولوژیکی، گسترش آزادی بیان و شبکه‌های اجتماعی جدیدی که اقتصاد ما را به تحرک وا می‌دارند و اصول ما را منعکس می‌کنند، تبدیل شده است. در این شرایط، امنیت و عملیات مؤثر زیرساخت‌های حیاتی آمریکا ـ ازجمله در بخش‌های انرژی، بانکداری و مالیه، حمل‌ونقل، ارتباطات و پایه صنعتی دفاعی ـ که وابسته به فضای مجازی هستند و نیز سیستم‌های کنترل صنعتی و تکنولوژی اطلاعات ممکن است مورد اختلال یا سوءاستفاده قرار گیرند.

وزارت دفاع همراه با سایر سازمان‌های دولتی آمریکا، در عملکرد روزمره خود به فضای مجازی متکی است. نیازی به اغراق در مورد این وابستگی نیست، وزارت دفاع بیش از ۱۵،۰۰۰ شبکه و هفت میلیون طرح کامپیوتری را از طریق صدها دستگاه در چندین کشور در سرتاسر جهان اداره می‌کند. وزارت دفاع از فضای مجازی برای

ممکن ساختن انواع عملیات‌های تجاری، اطلاعاتی و نظامی خود ـ ازجمله انتقال افراد و مواد و فرماندهی و کنترل طیف وسیعی از عملیات‌های نظامی ـ استفاده می‌کند.

وزارت دفاع و سایر نهادها، آسیب‌پذیری‌هایی در فضای مجازی دارند. وابستگی ما به فضای مجازی در تضادی شدید با امنیت فضای مجازی ما و امنیت تکنولوژی‌هایی که همه روزه از آنها استفاده می‌کنیم قرار دارد. به‌علاوه، رشد مداوم سیستم‌های شبکه‌ای، ابزارها و پلت‌فورم‌ها به این معنی است که فضای مجازی به مجموعه رو به رشدی از توانایی‌ها تبدیل شده است که وزارت دفاع برای تکمیل مأموریتش به آنها وابسته است. امروزه، بسیاری از کشورهای خارجی درصددند تا از شبکه‌های طبقه‌بندی شده (محرمانه) و طبقه‌بندی نشده وزارت دفاع سوءاستفاده کنند و برخی از سازمان‌های اطلاعاتی خارجی تاکنون توان ایجاد اختلال در عناصر زیرساخت‌های اطلاعاتی وزارت دفاع را به‌دست آورده‌اند. به‌علاوه، بازیگران غیردولتی به‌طور چشمگیری این تهدید را که بر سیستم‌ها و شبکه‌های وزارت دفاع نفوذ کنند و آنها را مختل سازند، اعمال می‌کنند. ما می‌دانیم که چه بسا فعالان بداندیشی نسبت به سیستم‌ها و شبکه‌های وزارت دفاع وجود دارند که ما هنوز آنها را کشف نکرده‌ایم.

وزارت دفاع، با همکاری با سازمان‌های داخلی خود و شرکای بین‌المللی‌اش، درصدد کاستن از خطراتی است که علیه توانایی‌های آمریکا و متحدانش در فضای مجازی اعمال می‌شود، این مسئله همراه با حمایت از اصول زندگی خصوصی و آزادی‌های مدنی، آزادی بیان و نوآوری که فضای مجازی را تبدیل به بخش منسجمی از امنیت و شکوفایی آمریکا کرده‌اند و احترام به این اصول صورت می‌گیرد. در این

میان، اینکه وزارت دفاع چگونه فرصت‌های فضای مجازی را بالا می‌برد و همزمان بی‌ثباتی‌های ذاتی را مدیریت می‌کند و آسیب‌پذیری‌ها را کاهش می‌دهد، به‌طور قابل توجهی بر آمادگی دفاعی آمریکا و امنیت ملی در سال‌های آتی تأثیر خواهد گذاشت.

زمینه استراتژیک

وابستگی ما به شبکه‌های اطلاعاتی وزارت دفاع برای فرماندهی و کنترل نیروها و تدارکات اغراق‌آمیز نیست. بنابراین توسعه تکنولوژی‌های تسلیحاتی و حوزه‌های مختلف دیگر به آن متکی است.

فرصت‌ها و توانایی‌های وزارت دفاع در فضای مجازی

وزارت دفاع به فضای مجازی‌ای امن و قابل اعتماد که از آزادی‌های اساسی، زندگی خصوصی و جریان آزاد اطلاعات پشتیبانی کند، وابسته است. وزارت دفاع به‌منظور حمایت از امنیت ملی و تعهدات اساسی آمریکا، از فرصت‌ها و توانایی‌های خوبی در فضای مجازی برخوردار است. توانایی نظامی آمریکا در استفاده از فضای مجازی به‌منظور ارتباطات سریع و به اشتراک گذاشتن اطلاعات برای پشتیبانی از عملیات‌ها، عاملی حیاتی در مأموریت‌های وزارت دفاع است. به‌ویژه، گستره اطلاعات وزارت دفاع در مورد بخش تکنولوژی ارتباطات و اطلاعات جهانی، مزایای استراتژیکی را برای این وزارت در فضای مجازی مهیا می‌سازد.

کیفیت سرمایه انسانی و پایه اطلاعاتی آمریکا در هر دو بخش خصوصی و دولتی پایه‌ای قوی برای وزارت دفاع فراهم می‌کند که براساس آن بتواند توانایی‌های

مجازی حال و آینده را بسازد. وزارت دفاع از طریق سرمایه‌گذاری در نیروی انسانی، تحقیق و تکنولوژی، نقش مهمی در ایجاد و ترفیع مهارت تکنولوژیکی بخش خصوصی ایفا کرده است. وزارت دفاع از این روح مقاطعه‌کاری استقبال خواهد کرد و با این اجتماعات و مؤسسات به‌منظور کسب موفقیت در فعالیت‌های خود در فضای مجازی همکاری خواهد کرد.

با توجه به دینامیسم فضای مجازی، کشورها باید برای دفاع از منافع مشترکشان و بالا بردن امنیتشان با یکدیگر همکاری کنند. روابط وزارت دفاع با شرکای بین‌المللی و متحدان آمریکا پایه‌ای محکم فراهم می‌آورد که براساس آن همکاری بین‌المللی آمریکا در مورد فضای مجازی افزایش می‌یابد. تعهد بین‌المللی مداوم، دفاع مشروع جمعی و ایجاد هنجارهای بین‌المللی برای فضای مجازی، همچنین، فضای مجازی را به‌منظور سودمند بودن برای همه تقویت خواهد کرد.

تهدیدات مجازی

«همان تکنولوژی‌هایی که ما را توانمند می‌سازند، آنهایی را نیز که درصدد ایجاد اختلال و خرابکاری هستند، توانمند می‌سازند».

استراتژی امنیت ملی، ۲۰۱۰

اینترنت به‌گونه‌ای طراحی شد که سریعاً قابل گسترش و به‌آسانی قابل دسترس برای نوآوری تکنولوژیکی، باشد. جریان اطلاعات بر انسجام متن پیشی گرفت، تأیید هویت کمتر از اتصال و ارتباط اهمیت داشت. طراحان اینترنت نمی‌توانستند گسترش

نقش رو به رشد و حیاتی آن را بر وزارت دفاع و عملیات‌هایش تصور کنند. دامنه جهانی سیستم‌ها و شبکه‌های وزارت دفاع دشمنانی دارد که فرصت‌های گسترده‌ای برای سوءاستفاده و حمله دارند.

موانع اندک برای ورود فعالیت‌های بدخواهانه به فضای مجازی، ازجمله دسترسی گسترده به ابزارهای هک کردن، نشان می‌دهد که یک فرد یا گروه کوچکی از بازیگران به‌طور بالقوه توانایی ایجاد آسیب جدی بر امنیت اقتصادی و ملی آمریکا و وزارت دفاع را دارد. این تکنولوژی‌های با مقیاس کوچک می‌توانند تأثیر نامتناسبی نسبت به اندازه‌شان ایجاد کنند، دشمنان بالقوه مجبور نیستند سیستم‌های تسلیحاتی گران‌قیمتی داشته باشند تا بتوانند تهدید بزرگی بر امنیت ملی آمریکا اعمال کنند.

وزارت دفاع، در توسعه استراتژی خود برای عملیات در فضای مجازی، بر جنبه‌های اصلی تهدید مجازی توجه دارد: این تهدیدات شامل بازیگران تهدیدکننده خارجی، تهدیدات داخلی، آسیب‌پذیری‌های زنجیره‌ای و تهدیدات مربوط به توانایی عملیاتی وزارت دفاع است. وزارت دفاع باید در مقابل آسیب‌پذیری‌ها و تلاش‌های هماهنگ بازیگران دولتی و غیردولتی برای دسترسی مجاز به سیستم‌ها و شبکه‌هایش پاسخگو باشد.

عملیات‌های خارجی فضای مجازی علیه سیستم‌های بخش خصوصی و دولتی آمریکا به‌لحاظ تعداد و پیچیدگی درحال افزایش هستند. شبکه‌های وزارت دفاع هر روز میلیون‌ها بار مورد کاووش قرار می‌گیرند و نفوذهای موفقیت‌آمیز در شبکه‌های وزارت دفاع موجب از دست رفتن هزاران فایل از شبکه‌های آمریکا و متحدان و شرکای صنعتی آنان می‌شوند. به‌علاوه، این تهدید نشان می‌دهد که دشمنان بر

توسعه توانایی‌های به‌طور چشمگیر پیچیده و به‌طور بالقوه خطرناک توجه دارند.

امکان اینکه گروه‌های کوچکی بتوانند تأثیر نامتقارنی در فضای مجازی بگذارند، انگیزه‌های واقعی‌تری برای فعالیت‌های بداندیشانه ایجاد می‌کند. مجرمان فضای مجازی، فراتر از فعالیت‌های رسمی دولتی، می‌توانند بوت‌نت‌های میلیون‌ها «هاست» آلوده را کنترل کنند. ابزارها و تکنیک‌های توسعه‌یافته توسط مجرمان فضای مجازی درحال پیشرفته‌تر شدن با سرعتی باور نکردنی هستند و بسیاری از این امکانات را می‌توان با قیمت نازل از اینترنت خریداری کرد. خواه هدف از این کار رسیدن به پول باشد، یا کسب مالکیت معنوی یا ایجاد اختلال در سیستم‌های حیاتی وزارت دفاع، چشم‌انداز تهدید به سرعت درحال رشد نشان از چالش مهم و پیچیده‌ای برای امنیت اقتصادی و ملی دارد.

برخی از تهدیدات فضای مجازی نیز از داخلی‌ها ناشی می‌شود. داخلی‌های بداندیش ممکن است به فرمان دولت‌های خارجی، گروه‌های تروریستی، عناصر جنایتکار، همکاری‌های غیراخلاقی یا به ابتکار خودشان از دسترسی به فضای مجازی سوءاستفاده کنند. بداندیشان داخلی خواه جاسوسی کنند، یا اظهارنظری سیاسی کنند و یا ناخشنودی خودشان را ابراز کنند، پیامدها می‌تواند برای وزارت دفاع و امنیت ملی مهلک باشد.

نرم‌افزارها و سخت‌افزارها در معرض خطر دستکاری بداندیشانه قرار دارند، حتی قبل از اینکه در یک سیستم عملیاتی ادغام شوند. اکثریت تولیدات تکنولوژی اطلاعات که در آمریکا استفاده می‌شوند در خارج از کشور ساخته و مونتاژ می‌شوند. وابستگی وزارت دفاع به ساخت و توسعه خارجی چالش‌هایی را برای مدیریت

خطرات مربوط به طراحی، ساخت، خدمات، توزیع و کنترل ایجاد می‌کند.

دشمنان بالقوه آمریکا ممکن است درصدد سوءاستفاده، قطع، جلوگیری و فاسد کردن شبکه‌ها و سیستم‌هایی باشند که وزارت دفاع برای عملیات‌های خود به آنها نیاز دارد. وزارت دفاع به‌ویژه با سه دسته از فعالیت‌های دشمنانه بالقوه درگیر است:سرقت یا سوءاستفاده از داده‌ها، ایجاد اختلال یا جلوگیری از دسترسی و خدمات که قابل دسترسی بودن شبکه‌ها، اطلاعات یا منابع شبکه‌ای را تحت تأثیر قرار می‌دهد و اعمال خرابکارانه ازجمله قطع، دخالت یا کنترل فعالیت‌هایی که شبکه‌ها یا سیستم‌های متصل به هم را تخریب یا فاسد می‌کنند.

تهدیدات مجازی علیه امنیت ملی آمریکا فراتر از اهداف نظامی است و همه جنبه‌های جامعه را تحت تأثیر قرار می‌دهد. هکرها و دولت‌های خارجی به‌طور چشمگیری این توانایی را دارند که مداخله پیچیده‌ای در شبکه‌ها و سیستم‌هایی کنند که زیرساخت‌های حیاتی مدنی را کنترل می‌کنند. با توجه به ماهیت منسجم فضای مجازی، شبکه‌های حمل‌ونقل و سیستم‌های مالی می‌توانند بی‌ثباتی اقتصادی و خطر فیزیکی فراگیری را موجب شوند. عملیات‌های وزارت دفاع ـ در داخل و خارج ـ به این زیرساخت‌های حیاتی وابسته‌اند.

با اینکه تهدید مربوط به مالکیت معنوی اغلب کمتر از تهدید مربوط به زیرساخت‌های حیاتی، قابل مشاهده است، ممکن است این تهدید، فراگیرترین تهدید در فضای مجازی درحال حاضر باشد. سالیانه، مقداری مالکیت معنوی ـ بیش از آنچه در کتابخانه کنگره نگهداری می‌شود ـ از شبکه‌های متعلق به شرکت‌ها، دانشگاه‌ها و سازمان‌ها و وزارتخانه‌های دولتی آمریکا دزدیده می‌شود. از آنجا که قدرت نظامی در

نهایت به پویایی اقتصادی وابسته است، از دست رفتن‌های مداوم مالکیت معنوی، هم کارآمدی نظامی و هم رقابت‌پذیری ملی آمریکا در اقتصاد جهانی را کاهش می‌دهد.

پنج ابتکار استراتژیک

ابتکار استراتژیک ۱ ـ وزارت دفاع، فضای مجازی را به‌عنوان گستره‌ای عملیاتی به‌منظور سازماندهی، آموزش و تجهیز قلمداد خواهد کرد به‌طوری که وزارت دفاع بتواند از مزایای کامل ظرفیت‌های فضای مجازی منتفع شود.

«هرچند که فضای مجازی، گستره‌ای ساخت دست بشر است، اینک این گستره تا حدودی مثل گستره‌های طبیعی ـ ازجمله زمین، دریا، هوا و فضا ـ برای فعالیت‌های وزارت دفاع است».

بررسی چهارساله دفاعی، ۲۰۱۰

هرچند که شبکه‌ها و سیستم‌هایی که فضای مجازی را تشکیل می‌دهند ساخته دست بشرند و اغلب مالکان خصوصی دارند و اساساً مورد استفاده مدنی هستند، قلمداد کردن فضای مجازی به‌عنوان یک گستره، یک مفهوم سازمان‌بخش حیاتی برای مأموریت‌های امنیت ملی وزارت دفاع است. این مفهوم به وزارت دفاع اجازه می‌دهد که در مورد فضای مجازی دست به سازماندهی، آموزش و تجهیز بزند همان‌گونه که در مورد هوا، زمین، ساحل و فضا، برای پشتیبانی از منافع امنیت ملی انجام می‌دهد. به‌علاوه، این تلاش‌ها باید شامل اجرای عملیات‌های اساسی در یک محیط مجازی فاسد باشد.

همچنان‌که در «استراتژی امنیت ملی» گفته شده است، وزارت دفاع باید مطمئن

شود که از توانایی‌های ضروری برای اجرای مؤثر عملیات کردن در همه گستره‌ها ـ هوا، زمین، ساحل، فضا و فضای مجازی ـ برخوردار است. وزارت دفاع در همه سطوح به سازماندهی، آموزش و تجهیز در مقابل چالش‌های پیچیده و فرصت‌های گسترده فضای مجازی دست خواهد زد. وزارت دفاع برای رسیدن به این هدف، مسئولیت‌های مأموریت فضای مجازی را به فرماندهی استراتژیک آمریکا، سایر فرماندهی‌های جنگی و دپارتمان ارتش تفویض کرده است. وزارت دفاع، با توجه به نیاز خود به تضمین توانایی ایفای عملیات کارآمد در فضای مجازی و توانایی سازمان دادن کافی به منابع خود، فرماندهی مجازی آمریکا[1] را به‌عنوان زیرمجموعه‌ای از فرماندهی استراتژیک آمریکا[2] تأسیس کرد. تأسیس این فرماندهی ناشی از برخی از نیازهای وزارت دفاع است که در زیر به آنها اشاره می‌شود:

ـ مدیریت خطر فضای مجازی از طریق تلاش‌هایی مانند آموزش مستمر، تضمین اطلاعات، آگاهی بیشتر نسبت به شرایط و ایجاد محیط‌های شبکه‌ای امن و منعطف.

ـ تضمین انسجام و قابلیت دسترسی با حضور در اتحادهای قوی، ایجاد دفاع‌های مشروع جمعی و حفظ نقشه عملیاتی مشترک.

ـ تضمین توسعه توانایی‌های منسجم با همکاری نزدیک با آژانس‌ها، سرویس‌ها و فرماندهی‌های جنگی و تحصیل اجتماع برای عرضه و به‌کارگیری سریع توانایی‌های نوآور زمانی که مورد نیاز هستند.

فرماندهی استراتژیک آمریکا، مسئولیت هماهنگی و همکاری عناصر این سازمان

1. Uscybercom
2. Usstratcom

را در درون هرکدام از شاخه‌های ارتش، ازجمله فرماندهی مجازی ارتش آمریکا، فرماندهی مجازی ناوگان جنگی آمریکا/ ناوگان دهم ایالت متحده، نیروی ۲۴ هوایی، فرماندهی مجازی گارد ساحلی آمریکا، به فرماندهی مجازی آمریکا تفویض کرده است. مفهوم سازمانی اصلی فرماندهی مجازی آمریکا، هم‌محلی بودن آن با آژانس امنیت ملی (NSA) است. به‌علاوه، فرمانده آژانس امنیت ملی، فرماندهی مجازی آمریکا را نیز برعهده دارد. هم‌محلی بودن و مشترک بودن فرمانده این دو سازمان جدا و متمایز به وزارت دفاع و دولت آمریکا اجازه می‌دهد که توانایی‌ها و استعدادها را به حداکثر برسانند، اختیارات خاصی را بالا ببرند و به‌طور کارآمدتری برای پیشبرد مأموریت وزارت دفاع عمل کنند.

از آنجا که عملیات‌های فضای مجازی فاسد برای دوره‌های گسترده ممکن است یک واقعیت باشد و در میانه یک مأموریت ممکن است اختلال صورت پذیرد، وزارت دفاع طیف کاملی از سناریوهای فضای مجازی را در آموزش و تمرین‌ها ادغام خواهد کرد تا نیروهای مسلح آمریکا را برای پیشامدهای گوناگون آماده کند. سنگ‌بنای این فعالیت گنجاندن تیم‌های قرمز مجازی در بازی‌ها و تمرین‌های جنگی خواهد بود. لازمه عمل کردن علیه یک تجاوز احتمالی این است که وزارت دفاع، همزمان با تمرکز بر تلاش‌های خود در جهت تضمین مأموریت و حفظ توانایی حیاتی عملیات، چابک و منعطف باشد.

این تلاش‌ها را توسعه سیستم‌ها و شبکه‌های منعطف پشتیبانی خواهد کرد. وزارت دفاع باید در موقع پیشامد ـ قطع شبکه یا به‌خطر افتادن ـ بتواند با جدا کردن و خنثی کردن تأثیر، استفاده از ظرفیت مازاد، یا تغییر عملیات‌های خود از یک سیستم به

سیستمی دیگر، مؤثر واقع شود. شبکه‌های متعدد می‌توانند تنوع، انعطاف و تضمین مأموریت را به عملیات‌های فضای مجازی اضافه کنند. وزارت دفاع تحقیق می‌کند تا گزینه‌هایی را برای تغییر عملیات‌های خود به‌منظور تأمین امنیت شبکه‌ها شناسایی کند.

ابتکار استراتژیک ۲ـ وزارت دفاع مفاهیم عملیاتی دفاعی جدیدی را برای پشتیبانی از سیستم‌ها و شبکه‌های وزارت دفاع به‌کار خواهد گرفت.

> *«دفاع از امنیت، شکوفایی و زندگی خصوصی در مقابل این تهدیدات نیازمند شبکه‌های امن، قابل اعتماد و منعطف است».*
>
> *استراتژی امنیت ملی، ۲۰۱۰*

تحقق مفاهیم عملیاتی دفاعی که به‌طور مداوم درحال تکامل هستند مستلزم پیشبرد مأموریت فضای مجازی وزارت دفاع، امروز و در آینده است. وزارت دفاع به‌عنوان گام اول درحال تقویت بهترین تجربیات خود در مورد بهداشت مجازی به‌منظور بهبود امنیت فضای مجازی خود است. به‌عنوان گام دوم وزارت دفاع برای جلوگیری و کاستن از تهدیدات داخلی، ارتباطات نیروی کار، مسئولیت‌پذیری نیروی کار، نظارت داخلی و توانایی‌های مدیریت اطلاعات خود را تقویت خواهد کرد. سوم وزارت دفاع ظرفیت دفاعی فعالانه‌ای را در حوزه فضای مجازی به‌کار خواهد گرفت تا از ورودهای غیرمجاز به سیستم‌ها و شبکه‌های وزارت دفاع جلوگیری کند. چهارم وزارت دفاع درحال توسعه مفاهیم عملیاتی دفاعی جدید و ساختارهای کامپیوتری

است. همه این عناصر ترکیب می‌شوند تا دفاع پویا و سازگاری را برای سیستم‌ها و شبکه‌های وزارت دفاع شکل دهند.

اغلب آسیب‌پذیری‌های سیستم‌های وزارت دفاع و فعالیت‌های بداندیشانه علیه این سیستم‌ها را می‌توان از طریق بهداشت فضای مجازی برطرف کرد. بهداشت فضای مجازی همواره باید ازسوی همگان اعمال شود، درست هر اندازه که برای افراد مهم است که از خودشان حفاظت کنند به همان اندازه نیز مهم است که سیستم‌های عملیاتی و نرم‌افزار امنیتی را به‌روز کنند. وزارت دفاع روش‌های سوءاستفاده بخش خصوصی را برای تقویت دستگاه‌های کامپیوتری خود همراه با استمرار تجربیات خود درخصوص بهداشت فضای مجازی تکمیل خواهد کرد. به‌علاوه بهداشت خوب فضای مجازی به حفظ امنیت اطلاعات، ترفیع تجربیات امنیت فضای مجازی برای کاربران و نیز مدیران، طراحی و اجرای شبکه‌های امن و به‌کارگیری مدیریت کارآمد و هوشمند گسترش می‌یابد. این تلاش کلان حفاظت می‌تواند حمایت، نظارت، طراحی و سلامت را برای سیستم‌ها و شبکه‌های وزارت دفاع به ارمغان آورد تا انسجام و امنیت خود را تأمین کنند.

مردم اولین خط دفاعی وزارت دفاع در حفظ بهداشت فضای مجازی و کاهش تهدیدات داخلی، هستند. وزارت دفاع برای کاستن از تهدید داخلی و جلوگیری از افشای خطرناک اطلاعات طبقه‌بندی شده و محرمانه، پارادایم فعلی تضمین اطلاعات، ازجمله جستجوی مفاهیم عملیاتی جدید برای کاستن از آسیب‌پذیری‌ها، را تقویت و از آن فراتر خواهد رفت. تلاش‌های وزارت دفاع بر ارتباطات، آموزش پرسنل و فرایندها و تکنولوژی‌های جدید متمرکز خواهد بود. وزارت دفاع درصدد پرورش فرهنگ

قویتری در مورد تضمین اطلاعات در داخل نیروی کار است تا مسئولیت‌پذیری فردی را تضمین کند و از بداندیشان داخلی با شکل‌دهی به رفتارها و گرایش‌ها از طریق تحمیل هزینه‌های بیشتری برای فعالیت‌های بداندیشانه، جلوگیری کند. این تغییر فرهنگی با سیاست‌های جدید، روش‌های جدید آموزش پرسنل و ارتباطات نوآور نیروی کار مقدور خواهد بود.

از آنجا که فعالیت‌های بداندیشانه در فضای مجازی رو به رشد هستند، وزارت دفاع تلاش جدی را در فضای مجازی به‌کار گرفته است تا از ورود غیرمجاز جلوگیری کند و فعالیت‌های خصمانه علیه سیستم‌ها و شبکه‌های وزارت دفاع را شکست دهد.

دفاع فعالانه فضای مجازی عبارت است از توانایی هماهنگ و بلادرنگ برای کشف، شناسایی، تحلیل و تخفیف تهدیدات و آسیب‌پذیری‌ها. در این شرایط اگرچه دفاع از سیستم‌ها و شبکه‌های وزارت دفاع عملاً بر رویکردهای سنتی متکی است اما در عین حال بهترین تجربیات با مفاهیم عملیاتی جدید تکمیل می‌شود. این روش بر سرعت شبکه تمرکز می‌کند و از سنسورها، نرم‌افزارها و اطلاعات برای کشف و متوقف کردن فعالیت‌های بداندیشانه ـ قبل از اینکه بتوانند بر سیستم‌ها و شبکه‌های وزارت دفاع تأثیر بگذارند ـ استفاده می‌کند. از آنجا که همیشه نمی‌توان ورود غیرمجاز را در مرز شبکه متوقف کرد، وزارت دفاع به اصلاح و بهبود سنسورهای پیشرفته برای شناسایی، کشف و تخفیف فعالیت‌های بداندیشانه در شبکه‌های وزارت دفاع ادامه خواهد داد.

وزارت دفاع برای تقویت انعطاف‌پذیری و تنوع هوشمند در شبکه‌ها و

سیستم‌هایش، پارادایم‌ها و رویکردهای جدید و نوآوری را برای چالش‌های موجود و درحال ظهور جستجو خواهد کرد. این تلاش‌ها شامل توسعه و ادغام در حوزه‌های رسانه‌های همراه و تأمین امنیت کامپیوتری خواهد بود. وزارت دفاع به همگام بودن با تغییرات سریع و انقلابی، در فعالیت‌های فضای مجازی خود ادامه خواهد داد.

ابتکار استراتژیک ۳ ـ وزارت دفاع با سایر سازمان‌ها و ادارات دولتی و بخش خصوصی به‌منظور ممکن ساختن یک استراتژی فراگیر در مورد امنیت فضای مجازی مشارکت خواهد کرد

«نه دولت، نه بخش خصوصی و نه شهروندان به تنهایی نمی‌توانند این چالش‌ها را برطرف سازند ـ ما روش‌های همکاری با یکدیگر را گسترش خواهیم داد».
استراتژی امنیت ملی، ۲۰۱۰

چالش‌های فضای مجازی در بخش‌ها، صنایع و سازمان‌ها و ادارات دولتی آمریکا گسترده‌اند، آنها در مرزهای ملی و از طریق عناصر چندگانه اقتصاد جهانی گسترده‌اند بسیاری از عملیات‌ها و کارکردهای حیاتی وزارت دفاع به دارایی تجاری، ازجمله ارائه‌دهندگان خدمات اینترنتی[1] و زنجیره‌های جهانی عرضه وابسته‌اند، عواملی که وزارت دفاع بر آنها سلطه مستقیم ندارد تا خطرات را به‌طور کارآمدی کاهش دهد. بنابراین، وزارت دفاع با دپارتمان امنیت داخلی،[2] شرکای درون‌سازمانی و بخش

1. ISPS
2. DHS

خصوصی، به‌منظور به اشتراک گذاشتن ایده‌ها، توسعه توانایی‌های جدید و حمایت از تلاش‌های جمعی در جهت رفع چالش‌های متقاطع فضای مجازی همکاری خواهد کرد.

وزارت دفاع، به‌منظور عملی کردن رویکرد دولتی همه‌جانبه، شدیداً با شرکای درون‌سازمانی خود در مورد روش‌های جدید و نوآور برای افزایش امنیت فضای مجازی ملی همکاری خواهد کرد. نمونه ابتکار اساسی پیش‌نویس موافقتنامه ۲۰۱۰ است که ازسوی وزارت دفاع و وزارت امنیت داخلی به امضا رسید تا همکاری‌ها درخصوص امنیت فضای مجازی را متحد و تقویت کند. مشارکت قوی وزارت امنیت داخلی و وزارت دفاع امنیت فضای مجازی ملی را به سه روش مهم بهبود خواهد بخشید. اول ساختار رسمی شده، محدودیت‌هایی را که سیاست و قانون فعلی بر همکاری وزارت دفاع و وزارت امنیت داخلی اعمال می‌کند، مورد تأیید قرار می‌دهد، دوم مشارکت در برنامه‌ریزی، کارآمدی مأموریت هرکدام از این دو وزارتخانه را بالا خواهد برد، به‌ویژه برداشت مشترکی از نیازهای مربوط به امنیت فضای مجازی را موجب خواهد شد و حمایت از زندگی خصوصی و آزادی‌های مدنی را تضمین خواهد کرد. سوم این توافق، منابع محدود و بودجه‌ای را حفظ خواهد کرد.

این موافقتنامه به وزارت امنیت داخلی کمک خواهد کرد تا به بهترین نحو از سرویس‌های انحصاری بخش دولتی حمایت کند، با حکومت‌های قبیله‌ای، محلی و ملی مشارکت کند، با بخش خصوصی مشارکت کند و در دفاع از زیرساخت‌های اساسی آمریکا همکاری کند.

وزارت دفاع همچنین با پایگاه صنعتی دفاعی[1] به‌منظور بالا بردن حفاظت از

1. DIB

اطلاعـات محرمانـه همکـاری مـی‌کنـد. پایگـاه صـنعتی دفـاعی متشـکل از شـرکت‌هـا و سازمان‌های خصوصی و دولتی است که وزارت دفاع را از طریق تهیـه تکنولـوژی‌هـای دفاعی، سیستم‌های تسلیحاتی، توسعه سیاسی و استراتژیکی و پرسنل پشتیبانی می‌کند.

وزارت دفاع برای بالا بردن حفاظت شبکه‌های پایگاه صنعتی دفاعی، برنامه بیمـه اطلاعات و امنیت مجازی پایگاه صـنعتی دفـاعی (CS/IA) را در سـال ۲۰۰۷ تأسـیس کرد. وزارت دفاع همچنین، براساس این برنامه، درحال تأسیس یک شرکت خصوصـی ــ دولتـی آزمایشـی اسـت. هـدف از تأسـیس آن نشـان دادن امکانپـذیری و مزایـای هماهنگی داوطلبانه با به اشتراک گذاشتن اطلاعـات دربـاره فعالیـت‌هـای غیـرمجـاز و بداندیشانه فضای مجازی و تمهیدات حمایتی در مورد امنیت فضای مجازی است.

وزارت دفاع، با توجه به سرعت شتابان تغییر که مشخصه فضای مجازی اسـت، با بخش خصوصی و شرکای درون‌سازمانی به‌منظـور آزمـودن رویکردهـای جمعـی جدید در مورد امنیت فضای مجازی همکاری خواهد کرد. این تلاش‌هـا شـامل حمایـت وزارت دفاع از وزارت امنیت داخلی برای هدایت تلاش‌هـای درون‌سـازمانی بـه‌منظـور شناسایی و تخفیف آسیب‌پذیری‌های فضای مجازی در زیرساخت‌های حیـاتی کشـور خواهـد بـود. موفقیـت مسـتلزم برنامـه‌هـای آزمایشـی بیشـتر، مـدل‌هـای تجـاری و چارچوب‌های سیاسی برای تقویت همکاری بخش‌های خصوصی ـ دولتی خواهد بـود. مشارکت بخش‌های خصوصی ـ دولتی ضرورتاً نیازمند توازنی بین نظارت و اقدامات داوطلبانه است و آنها وابسته به نوآوری و اعتماد هستند.

در برخی موارد، مشوق‌ها یا سـایر تمهیـدات، بـرای بـالا بـردن مشـارکت بخـش خصوصـی لازم خواهـد بـود. تـلاش‌هـای وزارت دفـاع، همچنـین بایـد بـه فراتـر از

شرکت‌های بزرگ، به شـرکت‌هـای کوچـک و متوسـط گسـترش یابـد تـا مشـارکت را تضمین و نوآوری را تقویت کند. یک تلاش ملی جمعی، راه‌حل‌های کارآمد و مشـترکی را برای حل مسائل سیاسی فراهم خواهد آورد.

وزارت دفاع به حمایت از توسعه رویکردهای دولتی فراگیر برای مدیریت خطرات مربوط به جهانی شدن بخش تکنولوژی ارتباطات و اطلاعات ادامه خواهد داد. بسیاری از شرکت‌های سازنده تکنولوژی در آمریکا عوامل سخت‌افزاری و نرم‌افزاری تولیـد را و در برخی موارد منابع اطلاعاتی را برای شرکت‌های خارجی تهیه می‌کنند. بـه‌عـلاوه، افزایش تعداد عناصر و تولیدات تقلبی نیازمند فرایندهـایی بـرای کاسـتن از خطـرات و افزایش کیفیت است.

وابستگی به تکنولوژی منابع غیرمعتبر، قابلیت پـیش‌بینـی و تضـمین مـورد نیـاز وزارت دفاع را از بین مـی‌بـرد، لـذا وزارت دفـاع بـا وزارت امنیـت داخلـی و شـرکای درون‌سازمانی‌اش همکاری خواهد کرد تا به نحو احسـن ایـن خطـرات را شناسـایی و برطرف کند. زنجیره عرضه جهانی تکنولوژی، جنبه‌های حیاتی مسئولیت وزارت دفـاع را، همراه با کارکردهای بخش خصوصی و دولتی آمریکا تحت تأثیر قرار می‌دهـد کـه خطرات آن باید از طریق همکاری استراتژیک بخش خصوصی و دولتی کاهش یابد.

ابتکار استراتژیک ۴ ـ وزارت دفاع روابط محکمی را با شرکای بین‌المللی و متحدان آمریکا به‌منظور تقویت امنیت جمعی فضای مجازی ایجاد خواهد کرد

«آمریکا از طریق روابط خارجی دفاعی خود، نه تنها از بحران اجتناب می‌کند، بلکه همچنین کارآمدی خود را در واکنش به بحران‌ها بالا می‌برد».

بررسی چهار سالیانه دفاعی، ۲۰۱۰

وزارت دفاع، در حمایت از «استراتژی بین‌المللی فضای مجازی» و با همکاری شرکای درون‌سازمانی خود به‌طور چشمگیری در پی روابط بین‌المللی محکم است تا تعهدات اصلی و منافع مشترک ما را در فضای مجازی نشان دهد. توسعه توانایی‌های بین‌المللی مربوط به هشدار و آگاهی از شرایط، دفاع مشروع جمعی و بازداری جمعی را مقدور خواهد ساخت. متحدان و شرکای بین‌المللی، با به اشتراک گذاشتن به‌موقع علائم مربوط به حوادث مجازی، علائم تهدید برنامه بداندیشانه و اطلاعات مربوط به تهدیدات و بازیگران درحال ظهور، می‌توانند دفاع جمعی مجازی را بالا ببرند. فضای مجازی شبکه‌ای از شبکه‌هاست که شامل هزاران ISPs در سرتاسر جهان است، هیچ کشور یا سازمانی به تنهایی قادر به حفظ امنیت فضای مجازی نیست.

تعهد بین‌المللی وزارت دفاع از استراتژی بین‌المللی فضای مجازی آمریکا و تعهد رئیس‌جمهور به آزادیهای اساسی، زندگی خصوصی و جریان آزاد اطلاعات حمایت خواهد کرد. وزارت دفاع به تلاش‌های آمریکا برای پیشبرد توسعه و ترفیع اصول و هنجارهای بین‌المللی فضای مجازی که باز بودن، قابلیت تعامل، امنیت و قابل اعتماد بودن را افزایش می‌دهند، کمک خواهد کرد.

وزارت دفاع با شرکای بین‌المللی و درون‌سازمانی همکاری خواهد کرد تا رفتار مسئولانه را تشویق کند و در مقابل کسانی که درصدد ایجاد اختلال در شبکه‌ها و سیستم‌ها هستند بایستد، بازیگران بداندیش را تعقیب و بازداشت کند و حق دفاع از این دارایی‌های ملی حیاتی را به‌عنوان حق لازم و ضروری حفظ نماید. این تلاش‌ها فضای مجازی‌ای را حفظ خواهند کرد که فرصت‌هایی را برای نوآوری کسب مزایایی برای همه به ارمغان می‌آورد.

از آنجا که همکاری بین‌المللی فضای مجازی رو به رشد است، وزارت دفاع همکاری نزدیک خود را در زمینه فضای مجازی با متحدانش پیش خواهد برد تا از منافع آمریکا و متحدانش در فضای مجازی دفاع کند. وزارت دفاع همکاری نزدیکی با شرکای بین‌المللی و متحدانش به‌منظور توسعه توانایی‌های هشدار از طریق به اشتراک‌گذاری، درگیری در ظرفیت‌سازی و راهنمایی فعالیت‌های آموزشی خواهد داشت. این همکاری‌ها، فرصت‌هایی را برای ابداع گفتگوهایی برای به اشتراک گذاشتن بهترین تجربیات در حوزه‌هایی مثل پزشکی قانونی، توسعه ظرفیت‌ها، تمرین مشارکت‌ها و مشارکت‌های خصوصی ـ دولتی ایجاد خواهد کرد.

وزارت دفاع همکاری‌های رسمی و غیررسمی مجازی خود را با مجموعه گسترده‌ای از ارتش‌های شرکای و متحدان گسترش خواهد داد تا دفاع مشروع جمعی را توسعه داده و بازدارندگی جمعی را بالا ببرد. وزارت دفاع فرصت‌های جدیدی را برای کشورهای همفکر ایجاد خواهد کرد تا براساس اصول مشترک همکاری کنند، روابط گسترده و محکم با شرکای بین‌المللی و متحدان می‌تواند توانایی‌های مجازی را بالا ببرد، خطرات را کاهش دهد و موجب ایجاد ائتلاف‌هایی برای بازدارندگی از

فعالیت‌های بداندیشانه در فضای سایبر شود. این ائتلاف‌ها به افزایش روابط و اتحادهای رسمی وزارت دفاع و بالا رفتن امنیت فضای مجازی کمک خواهند کرد.

ابتکار استراتژیک ۵ ــ وزارت دفاع، مهارت ملی را از طریق نیروی کار بی‌نظیر در فضای مجازی و نوآوری سریع تکنولوژیکی بالا خواهد برد.

«ما به سرمایه‌گذاری در تحقیق و توسعه ضروری برای نوآوری و کشف ـ که ما برای رویارویی با این چالش‌ها به آنها نیاز داریم ـ ادامه خواهیم داد».
استراتژی امنیت ملی، ۲۰۱۰

دفاع از منافع امنیت ملی آمریکا در فضای مجازی به استعداد و مهارت مردم آمریکا بستگی دارد. وزارت دفاع منابع اقتصادی، دانشگاهی و علمی را تجزیه و تحلیل خواهد کرد تا مجموعه‌ای از پرسنل نظامی و غیرنظامی را به‌منظور کار کردن در فضای مجازی و پیشبرد اهداف وزارت دفاع گرد آورد. نوآوری تکنولوژیکی در خط مقدم امنیت ملی قرار دارد و وزارت دفاع، نوآوری سریع و فرایندهای کسب آن را در جهت تضمین عملیات‌های کارآمد در فضای مجازی تقویت خواهد کرد. وزارت دفاع در زمینه‌های نیروی انسانی، تکنولوژی و توسعه و تحقیق، سرمایه‌گذاری خواهد کرد تا توانایی‌های فضای مجازی را که برای امنیت ملی حیاتی هستند، ایجاد و حفظ کند.

توسعه و حفظ نیروی کار فوق‌العاده ماهر در فضای مجازی برای موفقیت استراتژیک وزارت دفاع در فضای مجازی و هرکدام از ابتکارات استراتژیکی که در اینجا ذکر شد، ضروری است. وزارت دفاع توانایی‌ها، ملزومات و نیروی کار خود را

در فضای مجازی، به‌طور منظم مورد ارزیابی قرار خواهد داد. توسعه نیروی کار فضای مجازی اهمیت فوق‌العاده‌ای برای وزارت دفاع دارد.

تقاضا برای نیروی کار جدید در فضای مجازی، به اقتضای جدیت تهدیدات مجازی، بالاست. وزارت دفاع باید خودش را رقابت‌پذیر سازد اگر که می‌خواهد نیروی تکنیکی ماهر را در خدمات دولتی برای بلندمدت جذب کند. وزارت دفاع برای پیشبرد اهداف خود، بر راه‌اندازی برنامه‌های پویایی برای جذب استعدادها تأکید خواهد کرد و ابتکار ۲۰۱۰ ریاست‌جمهوری را درخصوص استخدام و فرایندهای پرداخت اجرا خواهد کرد. وزارت دفاع همچنین با دفتر ویژه رئیس‌جمهور همکاری خواهد کرد تا استراتژی‌های مناسبی را برای کارآمدتر کردن تجربیات دیگران برای نیروی کار مجازی پیدا کند و برنامه‌ها را به نحوی تغییر دهد تا متخصصین حوزه مجازی بتوانند بدون مجازات، برای حفظ و رشد استعدادهای نوآور در زمینه مجازی، بین بخش‌های خصوصی و دولتی تردد کنند.

گذشته از این ابتکارات، استخدام، آموزش و پرورش، گزینش و درجه‌بندی برنامه‌های آموزشی، وزارت دفاع را قادر خواهد ساخت تا یک زیربنای استعداد استثنایی مجازی برای مأموریت امنیت ملی و دفاعی آینده پرورش دهد. رویکردهای تغییر پارادایم نظیر توسعه توانایی‌های مجازی گارد ملی و ذخیره می‌تواند انعطاف‌پذیری، کارشناسی و ظرفیت بیشتری را در فعالیت‌های بخش خصوصی، دولتی، فدرال و وزارت دفاع ایجاد کند. وزارت دفاع فرصت‌های تغییر و تبادل و برنامه‌های مداوم آموزشی را دنبال خواهد کرد و از راهکار کارآفرینی در توسعه نیروی کار مجازی استفاده خواهد کرد. آموزش و پرورش مداوم، مشخصه‌های

نیروی کار مجازی خواهند بود که سرمایه فکری وزارت دفاع را توسعه و حفظ خواهند کرد.

برای تکثیر دینامیسم بخش خصوصی و تقویت قدرت مفاهیم کامپیوتری درحال ظهور، فرایندهای وزارت دفاع برای به‌دست آوردن تکنولوژی اطلاعات پنج اصل را در نظر خواهند داشت.

اول: سرعت یک اولویت اساسی است. مقررات و فرایندهای تحصیل وزارت دفاع باید با چرخه زندگی توسعه تکنولوژی هماهنگ باشد. درخصوص تکنولوژی اطلاعات این چرخه‌ها ۱۲ الی ۳۶ ماه طول می‌کشند نه هفت یا هشت سال.

دوم: وزارت دفاع آزمون و توسعه فزاینده را بیشتر از آماده‌سازی صرف سیستم‌های بزرگ و پیچیده به‌کار خواهد بست.

سوم: وزارت دفاع برخی از سفارشات را برای پیشبرد اصلاحات سریع و فزاینده به تأخیر خواهد انداخت.

چهارم: نیازهای تکنولوژی اطلاعات وزارت دفاع ـ از مدرن‌سازی سیستم‌های کنترل و فرماندهی هسته‌ای گرفته تا به روز کردن نرم‌افزارها با سطوح مختلفی از نظارت مبتنی‌بر اولویت‌بندی سیستم‌های حیاتی وزارت دفاع هماهنگ خواهند بود.

پنجم: تمهیدات امنیتی اصلاح شده در همه سیستم‌هایی که وزارت دفاع خریداری می‌کند ازجمله سخت‌افزارها و نرم‌افزارها، به‌کار گرفته خواهند شد. هیچ دری برای رخنه وجود نخواهد داشت، هیچ واحد معیاری فعال رها نخواهد شد.

این اصول قسمتی از استراتژی‌های کاهش خطرات مربوط به زنجیره عرضه و سیستم‌های معتبر دفاعی خواهند بود و توسط این استراتژی‌ها و سیستم‌ها نیز تقویت

خواهند شد. وزارت دفاع، برای فرایندها، سیستم‌ها، ساختارها، نرم‌افزارها و سخت‌افزارهای خود، امنیت عمیقی فراهم خواهد آورد تا سیستم‌های ارزشمندی را طراحی، کسب و تکمیل کند.

وزارت دفاع همچنین فرصت‌هایی را برای شرکت‌های کوچک و متوسط فراهم خواهد آورد و با مقاطعه‌کاران در دره سیلیکون و سایر مجموعه‌های تکنولوژی‌ساز آمریکایی همکاری خواهد کرد تا مفاهیم را به سرعت از ایده نوآور به برنامه آزمایشی و از آن به گزینش اولویت‌بندی شده مسئولیت وزارت دفاع انتقال دهد.

برنامه‌های تحصیل وزارت دفاع برای فضای مجازی براساس ماهیت سازگار فضای مجازی خواهد بود، این برنامه‌ها بر چابکی تأکید خواهند کرد، از مفاهیم عملیاتی جدید استقبال خواهند کرد و همکاری میان جامعه علمی و دولت آمریکا را در کل تقویت خواهند کرد.

وزارت دفاع به‌دنبال رویکردهای تغییردهنده بازی ازجمله ساختارهای جدید خواهد بود تا توانایی‌های دفاعی وزارت دفاع را تقویت کند و سیستم‌های وزارت دفاع را در مقابل فعالیت‌های بداندیشانه، پایدارتر سازد. وزارت دفاع به‌دنبال تکنولوژی‌های متحولی خواهد بود که بنیادهای تکنولوژیکی فضای مجازی را مورد بازنگری قرار دهند. وزارت دفاع برای انجام چنین کاری با نهادهای علمی پیشرو در جهت توسعه توانایی‌های فضای مجازی امن، سالم و جدید که شدیداً در مقابل فعالیت‌های بداندیشانه مقاوم باشند، همکاری خواهد کرد.

توسعه دامنه فضای مجازی ملی (NCR) موفقیت این تلاش‌ها و تلاش‌های دیگر را امکانپذیر خواهد ساخت و وزارت دفاع، سایر بازیگران دولتی آمریکا و شرکای

بالقوه غیردولتی آمریکا را قادر خواهد ساخت که تکنولوژی‌ها، سیاست‌ها و مفاهیم جدید فضای مجازی را ارزیابی و آزمایش کنند. با اینکه ارتش آمریکا به‌طور عادی واحدها را در میادین هدف و در تنوعی از شبیه‌سازی‌ها تمرین می‌کند، وزارت دفاع از توانایی محدودی برای شبیه‌سازی عملیات‌های فضای مجازی برخوردار بوده است. دامنه فضای مجازی ملی، که ایجاد سریع مدل‌های متعددی از شبکه‌ها را مقدور می‌سازد، به این منظور برنامه‌ریزی شده است که ارتش و سایرین را، به برآوردن این نیاز، از طریق شبیه‌سازی و آزمودن ظرفیت‌ها و تکنولوژی‌های جدید قادر سازد.

وزارت دفاع، برای تشویق مشارکت بخش خصوصی در توسعه توانایی‌های قوی فضای مجازی، سازمان‌ها را تقویت خواهد کرد تا به‌عنوان اتاق‌های پایاپای برای تکنولوژی‌ها و مفاهیم نوآور عمل کنند و به شرکت‌هایی که تکنولوژی‌های نوآور و سودمند را توسعه می‌دهند، پاداش دهند. وزارت دفاع، گذشته از همکاری‌اش با مراکز تثبیت شده برتری تکنولوژیکی، نوآوری و چابکی مقاطعه‌کاران و شرکت‌های کوچک را از طریق ابتکاراتی مثل بررسی نوآوری شرکت‌های کوچک (SBIR)، ریسک‌های مشترک مولد و اعطاها و سرمایه‌گذاری‌های هدفمند در زمینه مفاهیم درحال ظهور و آزمایش نشده، بالا خواهد برد.

دینامیسم، تکنولوژی و نیروی انسانی کشور، بنیان نیرومندی را برای وزارت دفاع فراهم می‌آورد که بر پایه آن نیروی نظامی و غیرنظامی‌اش را تهیه کند و توانایی‌های تکنولوژیکی‌اش را بالا ببرد. وزارت دفاع به توسعه توانایی‌های قوی فضای مجازی ادامه خواهد داد و از تلاش‌های درون‌سازمانی که در جهت درگیر کردن نهادهای خصوصی و دولتی برای تشویق نوآوری در زمینه امنیت فضای

مجازی صورت می‌گیرد، پشتیبانی خواهد کرد.

وزارت دفاع در زمینه توانایی‌ها و پرسنل آینده، به‌منظور پیشبرد اهداف خود در زمینه فضای مجازی و پشتیبانی از امنیت ملی آمریکا سرمایه‌گذاری خواهد کرد.

نتیجه‌گیری

«یک شکست ازسوی وزارت دفاع در تأمین امنیت سیستم‌هایش در فضای مجازی خطر بزرگی را بر توانایی ما در اجرای مأموریت‌های دفاعی درحال حاضر و آینده وارد خواهد کرد».

بررسی چهار سالیانه دفاعی، ۲۰۱۰

امنیت ملی با فضای مجازی بازتعریف می‌شود. وزارت دفاع، علاوه‌بر فرصت‌ها، با چالش‌های مهمی در حوزه فضای مجازی روبرو است. همه عملیات‌های تجاری، اطلاعاتی و نظامی وزارت دفاع، برای موفقیت در مأموریت به فضای مجازی وابسته هستند.

«استراتژی وزارت دفاع برای عمل کردن در فضای مجازی» این چالش‌ها و فرصت‌ها را ارزیابی می‌کند و رویکردی استراتژیک برای مأموریت مجازی وزارت دفاع تدوین می‌کند.

پنج ابتکار استراتژیک وزارت دفاع نقشه راهی را برای وزارت دفاع عرضه می‌کند تا به‌طور کارآمد در فضای مجازی عمل کند، از منافع ملی دفاع نماید و اهداف امنیت ملی را پیش ببرد. هر ابتکاری از بقیه ابتکارها متمایز است و در عین حال ضرورتاً با بقیه ابتکارها ارتباط دارد. در سرتاسر استراتژی، فعالیت‌های اتخاذ شده در یک ابتکار

با تفکر استراتژیک وزارت دفاع هماهنگ خواهد بود و منجر به راهکارهای جدیدی در بقیه ابتکارها خواهد بود.

با دنبال کردن فعالیت‌های گفته شده در این استراتژی، وزارت دفاع در فرصت‌های ناشی از فضای مجازی سرمایه‌گذاری خواهد کرد، از سیستم و شبکه‌های خود در مقابل ورود غیرمجاز و فعالیت‌های بداندیشانه دفاع خواهد کرد، از تلاش‌هایی که برای تقویت امنیت فضای مجازی برای شرکای صنعتی، بین‌المللی و درون‌سازمانی انجام می‌شود پشتیبانی خواهد کرد و مشارکت و توانایی‌های قوی فضای مجازی را توسعه خواهد داد.

این استراتژی، دفاع وزارت دفاع از منافع آمریکا در فضای مجازی را هدایت خواهد کرد به نحوی که آمریکا و شرکا و متحدانش از مزایای نوآوری‌های عصر اطلاعات منتفع شوند.

شناسنامه گزارش

مرکز پژوهش‌های مجلس شورای اسلامی

شماره مسلسل: ۱۱۰۴۹

عنوان گزارش: استراتژی وزارت دفاع آمریکا در فضای مجازی

نام دفتر: مطالعات سیاسی (گروه سیاست خارجی)

تهیه و تدوین: خیراله خیری

ناظر علمی: محمد جمشیدی

متقاضی: معاونت پژوهشی

ویراستار تخصصی: مهدی جاودانی‌مقدم

سرویراستار: حسین صدری‌نیا

واژه‌های کلیدی: ـــــ

تاریخ انتشار: ۱۳۹۰/۷/۳