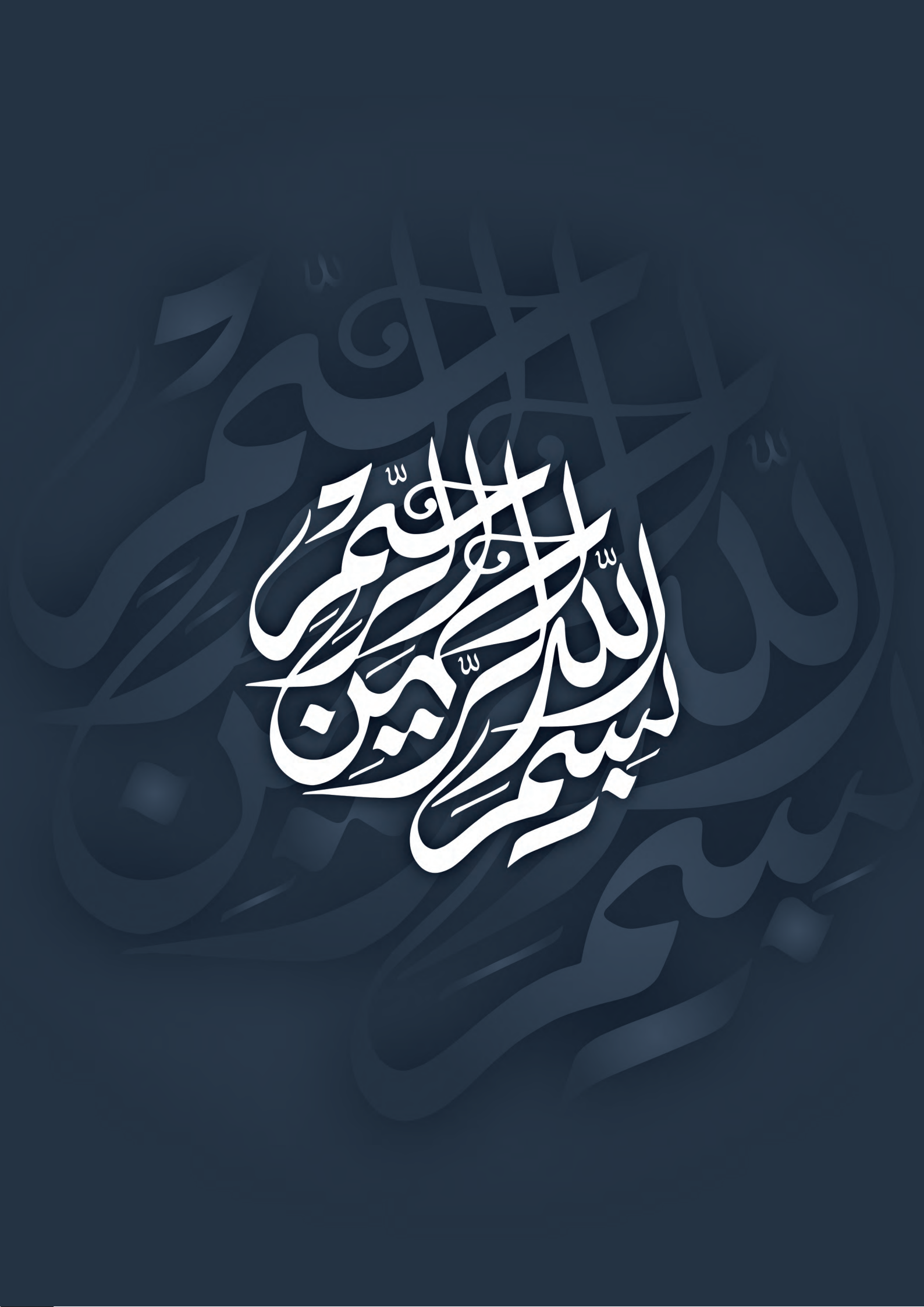
آژانس امنیت ملی آمریکا در سال ۲۰۲۳

گزارش فعالیت‌های NSA در حوزه امنیت سایبری


بسم الله الرحمن الرحيم

یادداشت

کارنامه آژانس امنیت ملی آمریکا در سالی که گذشت

آژانس امنیت ملی آمریکا (NSA) اصلی‌ترین نهاد حوزه امنیت سایبری در ساختار دولت آمریکا است. این نهاد که یکی از اعضای اصلی جامعه اطلاعاتی آمریکا محسوب می‌شود از نظر ساختاری ویژگی‌های منحصر به فردی را در بین سایر سازمان‌های اطلاعاتی آمریکا دارد. مدیر NSA که به طور سنتی از بین ژنرال‌های ارشد ارتش آمریکا انتخاب می‌شود به طور همزمان ریاست یکی از قرارگاه‌های فرماندهی ارتش آمریکا یعنی «فرماندهی سایبری ایالات متحده» را نیز بر عهده دارد.

ازاین‌رو به لحاظ ساختاری اهمیت NSA تنها به عنوان یک سرویس جاسوسی و اطلاعاتی نیست، بلکه به عنوان یک سازمان نظامی نیز مطرح است. این ساختار دوگانه با هدف اعطای حداکثر اختیارات قانونی لازم به آژانس برای ایفای نقش خود در مجموعه نظامی-امنیتی آمریکا است. یکی از وظایف NSA اشراف اطلاعاتی بر وضعیت امنیت سایبری و ارائه راهنمایی‌های لازم برای مقابله با حملات سایبری است.

از دیگر وظایف NSA را می‌توان نقش انحصاری در مقابله با حملات سایبری علیه سامانه‌های نظامی و امنیتی آمریکا دانست. این سامانه‌ها علاوه بر سیستم‌های تسلیحاتی و سامانه‌های فناوری اطلاعات دستگاه‌های حساس دولتی، شامل تمامی شرکت‌هایی نیز می‌شود که به نحوی در صنایع نظامی این کشور سهیم بوده و در زنجیره تأمین تجهیزات نظامی پنتاگون حضور دارند.

این گستردگی حوزه مأموریت‌ها نشان دهنده‌ی حساسیت حوزه امنیت سایبری و همچنین پیچیدگی حوزه دفاع سایبری در برابر تهدیدات خارجی است. آژانس‌های جاسوسی سایبری کشورهای غربی و متحدان آمریکا نیز با آژانس امنیت ملی همکاری‌های گسترده‌ای دارند.

یکی از دیگر نکات جالب توجه در این گزارش ورود و دخالت آژانس در طراحی استانداردهای دولتی در حوزه‌های مربوط به امنیت سایبری است.

ازایـن‌رو و با توجه به نقـش و جایگاه خاص آژانس امنیت ملی آمریکا در فضای سایبری و برنامه‌های گسترده تجسس سیگنال‌های ارتبـاطی (SIGINT) کـه ایـن نهـاد بـر عهـده دارد، مدیـران این مجموعـه تلاش می‌کننـد که با ارائه گزارش‌هایـی از فعالیت‌های خـود تلاش بـر برندسـازی و ارتقای تصویر خـود در افکار عمومی آمریکا داشته باشند.

متـنی کـه در ادامـه می‌آیـد ترجمه کامـل گزارش سـال ۲۰۲۳ آژانـس امنیـت ملی اسـت که با هـدف معـرفی جهت‌گیری‌ها و مأموریت‌های متنوع این نهاد در ساختار نظامی-اطلاعاتی آمریکا به صورت عمومی منتشـر شده است. در این گزارش خلاصه‌ای از برخی اقدامات و محورهای فعالیت‌های آژانس در سـال گذشـته میلادی آمده است.

مقدمه

از زمان جنگ جهانی دوم، آژانس امنیت ملی (National Security Agency) و سازمان‌های پیش از آن، از حساس‌ترین اطلاعات ایالات متحده محافظت کرده‌اند. امروزه که پیشرفت های فناوری، جهانی به‌هم‌پیوسته‌تر ایجاد کرده و تهدیدات را افزایش داده، مأموریت آژانس نیز گسترش یافته است. آژانس مسئولیت‌ها و اختیارات عملیاتی جدیدی را برای اطمینان از امنیت شبکه‌های ما بر عهده گرفته است.

امروزه، NSA در اجرای مأموریت امنیت سایبری، تخصص رمزنگاری، جاسوسی سیگنال‌های خارجی، تحلیل آسیب‌پذیری‌ها، عملیات دفاعی و عناصر دیگری را با یکدیگر یکپارچه کرده است تا از تهدیدت سایبری را از این سه حوزه کلیدی بزداید.

این سه حوزه عبارت‌اند از:

- سامانه‌های امنیت ملی (National Security Systems): شبکه‌هایی که حاوی اطلاعات طبقه‌بندی شده هستند یا به نحوی برای فعالیت‌های نظامی و اطلاعاتی ایالات متحده حیاتی می‌باشند. حفظ امنیت این شبکه‌ها برای حفظ آمادگی جنگی قابلیت‌های نظامیِ ایالات متحده و همچنین حفاظت از حساس ترین اطلاعات کشور ضروری است.
- وزارت دفاع (Department of Defense): نیروهای نظامی ایالات متحده و قرارگاه‌های فرماندهی رزمی و همچنین سازمان‌ها و وزارت‌خانه‌های دولت آمریکا که به حوزه امنیت ملی مربوط می‌شوند.
- مجموعه صنایع دفاعی (Defense Industrial Base): گروه بزرگ شرکت‌هایی که سامانه‌ها، پلتفرم‌ها و فناوری‌های لازم برای دفاع از کشور را برای وزارت دفاع طراحی، توسعه، بهره‌برداری و پشتیبانی می‌کنند. محصولات، خدمات و توانمندی‌های آن‌ها برای امنیت ایالات متحده و متحدان ما حیاتی است.

آژانس به منظور ارتقای شفافیت، یک گزارش سالانه منتشر می‌کند که در آن اطلاعاتی در خصوص تلاش‌هایش در حوزه امنیت سایبری که باعث تقویت توان دفاع ایالات متحده در برابر تهدیدات سایبری با اولویت بالا شده است را به اشتراک می‌گذارد. تلاش‌های NSA برای ایمن‌سازی حساس‌ترین سیستم های کشور به امنیت سایبری شما نیز کمک می‌کند، زیرا NSA این راه‌حل‌ها را از طریق راهنمایی‌های عمومی به اشتراک می‌گذارد و در همکاری با مهم‌ترین ارائه دهندگان خدمات فناوری، به ارتقای امنیت محصولات و خدمات آن‌ها کمک می‌کند.

> **امنیت سایبری همان امنیت ملی است.**
>
> **ژنرال پاول ام. ناکاسونی**
> فرمانده سایبری ایالات متحده،
> مدیر آژانس امنیت ملی (NSA)
> و رئیس سرویس امنیتی مرکزی (CSS)

یادداشت مدیر آژانس امنیت ملی

به عنوان مدیر آژانس امنیت ملی (NSA)، این افتخار و امتیاز را دارم که وظیفه رهبری نیرویی را بر عهده داشته باشم که از طریق مأموریت‌های امنیت سایبری و تجسس سیگنال (Signal Intelligence) از تمام اجزای جامعه اطلاعاتی و وزارت دفاع پشتیبانی می‌کند.

آژانس در رمزنگاری و رمزشکنی نیروی پیشتاز جهان است. افراد مستعد در آژانس بی‌وقفه کار می‌کنند تا از کشورمان در برابر دشمنان خارجی محافظت کنند.

کمک‌های NSA در رقابت استراتژیک کنونی، که در آن قدرت‌های جهانی از نظر اقتصادی، نظامی، فناوری و دیپلماتیک رقابت می‌کنند، حیاتی است.

جمهوری خلق چین به عنوان چالشی در حال رشد برای ایالات متحده ظهور پیدا کرده و خود را رقیبی نشان می‌دهد که هم قصد و هم توانایی تغییر شکل نظم بین‌المللی را طبق طراحی خود دارد. جمهوری خلق چین حریفی است که تهدیدِ به وجود آمده از سوی آن از نظر دامنه، مقیاس و پیچیدگی منحصر به فرد بوده و همچنین تمایل خود را برای تبدیل شدن به یکی از قدرت‌های برتر جهان اعلام کرده است.

روسیه همچنان یک تهدید جدی است و همچنان به دلیل بی‌توجهی به هنجارهای بین‌المللی و تمایل به استفاده از سلاح‌های خود برای هدف قرار دادن غیرنظامیان و زیرساخت‌های حیاتی، تهدیدی برای امنیت منطقه‌ای و ثبات جهانی است. ما شاهد نمونه‌ای گویا از این موضوع طی تجاوز غیرقانونی روسیه به اوکراین بودیم. روسیه همچنین با هدف ضعیف کردن نهادهای دموکراتیک در سراسر جهان عملیات‌های اطلاعاتی ترتیب داده است.

ما باید بتوانیم به تهدیدات ناشی از جمهوری خلق چین، روسیه و سایر حریفان جهانی هم در شرایط فعلی و هم در آینده پاسخ دهیم. ما باید همواره از رقبای جهانی خود که به شکل مداوم به دنبال تغییر در محیط اطلاعاتی جهان و نظم کنونی جهانی هستند پیشی بگیریم.

اختیاراتی مانند ماده ۷۰۲ قانون نظارت و جاسوسی خارجی (Foreign Intelligence Surveillance Act) به ما این امکان را می‌دهند. ماده ۷۰۲ این قانون یک مجوز کلیدی برای فعالیت‌های اطلاعاتی خارجی است که به حفظ امنیت ایالات متحده و متحدانش کمک به‌سزایی می‌کند. از اطلاعات حاصل از ماده ۷۰۲ به شکل روزانه برای محافظت از کشور در برابر تهدیدات حیاتی، آگاه کردن استراتژی دولت ایالات متحده، و حفظ جان آمریکایی‌ها استفاده می‌شود. از آنجا که هر گونه وقفه در اجرای این قانون تأثیر کورکننده‌ای بر نظارت ما نسبت به فعالیت‌های دشمنان خارجی فراتر از مرزهای ما دارد، ما از کنگره درخواست تجدید مجوز ماده ۷۰۲ را داریم.

مجوزهایی که به NSA اعطا شده است به آژانس اجازه می‌دهد که به مهم‌ترین دغدغه‌های امنیت ملی ما از جمله امنیت سایبری رسیدگی کند. ما اخیراً شاهد تغییر ماهیت منازعات بوده‌ایم: فضای سایبری یک فضای رقابتی است. این امر به وضوح مشخص شده است که تغییر وضعیت از رقابت به بحران و از بحران به درگیری می‌تواند اکنون در چند هفته، چند روز یا حتی چند دقیقه صورت گیرد. ما هر روز در NSA برای مقابله با تهدیدات سایبری علیه سامانه‌های امنیت ملی ایالات متحده، وزارت دفاع و مجموعه صنایع دفاعی و حذف آن‌ها تلاش می‌کنیم.

استراتژی ملی جدید امنیت سایبری، تمرکزی واضح و جدی بر بهره‌گیری از ظرفیت شراکت‌های بین‌المللی برای دنبال کردن اهداف مشترک در تأمین امنیت نرم‌افزارها، زیرساخت‌های حیاتی و شبکه‌های جهانی، از بین بردن و شکست دادن سازندگان باج‌افزارها، ارتقای همکاری‌های عملیاتی در فضای سایبری و ایجاد ظرفیت‌های تشخیص و واکنش به حوادث سایبری را نشان می‌دهد.

روابط ما با متحدان و شرکایمان در حوزه‌های اطلاعاتی و امنیت سایبری برای ما یک دارایی استراتژیک به شمار می‌رود که بیش از پیش بر رقابت ما با رقبایمان، به ویژه در حوزه فناوری، اثرگذار خواهد بود.

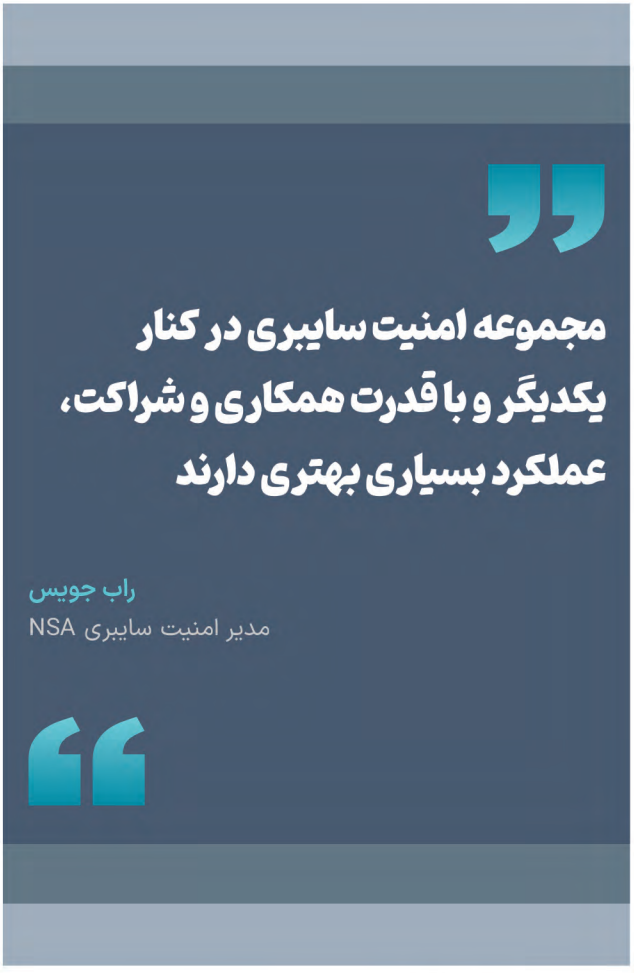
همزمان با پیشرفت فناوری‌هایی که در فضای سایبری استفاده می‌کنیم، چشم‌انداز جهانی پیچیده‌تر می‌شود. یکی از این مثال‌ها هوش مصنوعی است که توانایی برهم زدن چندین بخش از جامعه به طور همزمان را دارد. ما باید در رقابت جهانی برای درک پدیده هوش مصنوعی و به کار گرفتن قابلیت‌های آن پیشتاز باشیم و همچنین باید خود را در مقابل استفاده حریفان از این فناوری ایمن کنیم. ما در NSA با در کنار هم قرار دادنِ تخصص فنی عمیق خود، شناخت نسبت به تهدیدات و همچنین اختیارات قانونی لازم، موقعیت منحصر به فردی برای پشتیبانی از تلاش‌ها در جهت رسیدن به این هدف داریم.

من به تازگی اعلام کردم که NSA در حال متمرکز کردن تمام فعالیت‌های مرتبط با امنیت هوش مصنوعی در یک مجموعه جدید با نام مرکز امنیت هوش مصنوعی (NSA Artificial Intelligence Security Center) است. مرکز امنیت هوش مصنوعی، که در درون مرکز همکاری امنیت سایبری (Cybersecurity Collaboration Center) قرار دارد، به ما امکان می‌دهد تا همکاری نزدیکی با جامعه اطلاعاتی، وزارت دفاع، مجموعه صنایع دفاعی، آزمایشگاه‌های ملی، دانشگاه‌ها و شرکای خارجی منتخب داشته باشیم تا اطمینان حاصل کنیم که ایالات متحده برتریِ پایدار خود در حوزه هوش مصنوعی را حفظ می‌کند.

اصول و ارزش‌های NSA در کنار فرهنگ قانون مداری و تعهد به حفظ حریم خصوصی و آزادی‌های مدنی، پایه و اساس موفقیت‌های آژانس در حوزه امنیت سایبری هستند که در این گزارش شرح داده شده است و همچنین در آینده نیز مبنای خدشه‌ناپذیر خدمات NSA خواهد بود.

در NSA ایـن افـراد و شـراکت‌های ماسـت کـه پیشـرفت‌ها را رقـم می‌زننـد. کارکنـان آژانـس بـه اهمیت اعتمادی که به خاطر سوگندی که خورده‌اند بـه وجـود آمده، بـاور اسـتواری دارند. شـراکت‌های عمیق و پایدار ما، این امکان را به ما می‌دهد که در مقابـل تهدیـدات بایستیـم و راه حل‌هایـی را برای ایمن‌تر شـدن کشـورمان و متحدانمان بیاندیشیم. من از طرف آژانس امنیت ملی از تمام شرکایمان در این حوزه به خاطر تلاش‌هایشـان تشکر صمیمانه‌ای دارم، زیرا تاب‌آوری سایبریِ مشترک‌مان و واکنش‌های به‌موقـع، زمانی که بـا یکدیگر همکاری می‌کنیم بهتر محقق می‌شود.

ژنرال پاول ام. ناکاسونی
فرمانده سایبری آمریکا
مدیر آژانس امنیت ملی
رئیس سرویس امنیتی مرکزی



یادداشت مدیر امنیت سایبری NSA

اداره امنیت سایبری NSA با هدف برقراری ارتباط با صنعت و سایر شرکا تأسیس شده است. این روند در سـال گذشـته ادامه یافت و ما بیش از همیشـه به شـراکت‌ها تکیه کردیم. ما بر روی تبدیل دانش خود به اقداماتی متمرکز هستیم که شبکه‌ها را ایمن سازند و از طریـق روش‌هـای جدید در اقدامـات قدرت‌های مخالـف ما اخلال ایجاد کنند. شـراکت‌های داخلی و بین‌المللی به ما کمک می‌کنند تا با تهدیدات مقابله کنیم، راهکارهای امنیت سـایبری را گسترش دهیم و تأثیرات بلندمدت بیشتری ایجاد کنیم.

دانسـته‌ها و اطلاعـات ما تنها زمانی ارزش پیـدا می‌کنند که مدافعان شـبکه بتواننـد با بهره‌گیری از آن، اقدامـات واقعی انجام دهند. ما با به اشـتراک گذاشـتن دوطرفـه اطلاعـات بـا شـرکای خـود در محیطی طبقه‌بندی نشده، به ارتقای امنیت سایبری و امنیت ملی کمک می‌کنیم.

ترکیب اسـتعدادهای موجود در مجموعه شـرکای مـا، بزرگترین مزیت رقابتی اسـت که برای مقابله با تهدیـدات پیچیده‌تری که امروزه مشـاهده می‌کنیم در اختیار داریم.

در سـال گذشـته، مـا تعـداد زیـادی از تهدیدات امنیت سایبری را آشکار کردیم. با همکاری صنعت و شـرکای بین‌المللی، مـا نشـان‌گرهای نفـوذ (Indicators of Compromise) را شناسایی کردیم کـه مرتبط با یک عامل سـایبری پشتیبانی شـده از سـوی دولت جمهوری خلق چین بود. این عامل از تکنیک‌های «کسـب روزی از زمین» (Living off the Land) بـرای هدف قـرار دادن شـبکه‌های مرتبط با زیرساخت‌های حیاتی آمریکا استفاده می‌کرد. در این نوع حملات سـایبری از ابزارهای درونی شـبکه برای دور زدن لایه‌هـای دفـاعی بـدون بـه جـا گذاشـتن هرگونه ردی استفاده می‌شود. ما از کـــــمک‌های

چندین مجموعه بخش خصوصی برای شناخت بهتر این تهدید بهره بردیم و راهنمایی‌های لازم را منتشر کردیم تا مدافعان شبکه بتوانند این نوع فعالیت‌های مخرب در سیستم‌ها و شبکه‌های حیاتی را شناسایی و با آن مقابله کنند.

همکاری با سازمان‌های شریک به ما این امکان را داد تا یک بدافزار پیشرفته جاسوسی سایبری روسی به نام Snake را شناسایی کنیم که در بیش از ۵۰ کشور در سراسر جهان مورد استفاده بود. با همکاری یکدیگر، ما اجرا و مدیریت این بدافزار را به واحدی شناخته شده از مرکز ۱۶ سرویس امنیت فدرال روسیه منتسب کردیم. جزئیات فنی که با همکاری شرکایمان منتشر کردیم به عملیات‌های سازمان تحقیقات فدرال (FBI) کمک کرد و به بسیاری از سازمان‌های دیگر کمک کرد تا این بدافزار را در سراسر جهان شناسایی و حذف کنند.

همچنین در یک اقدام جداگانه، همکاری ما با شرکای صنعتی منجر به کشف یک آسیب‌پذیری در سرورهای Citrix شد که می‌توانست منجر به سرقت اطلاعات مجموعه صنایع دفاعی شود. به خاطر این همکاری‌ها بود که این آسیب‌پذیری روز صفر آشکار و ترمیم شد و در نتیجه تعداد سرورهای آسیب‌پذیر در سراسر کشور به طور قابل توجهی کاهش یافت.

مرکز همکاری امنیت سایبری (Cybersecurity Collaboration Center) به ما امکان می‌دهد تا ائتلاف‌هایی برای به اشتراک گذاری اطلاعات و مقابله با تهدیدهایی مانند این ایجاد کنیم. در این سال، این مرکز تعداد شرکای خود را سه برابر کرد و ما اکنون با بیش از ۷۵۰ مجموعه صنعتی و دولتی همکاری مستحکمی داریم. این امر به ما امکان می‌دهد تا بتوانیم بهره‌گیری از تکنیک‌های پیشگیری، تشخیص و مقابله را در گستره‌ای به وسعت میلیاردها دستگاه متصل به شبکه در جهان گسترش دهیم.

مرکز همکاری امنیت سایبری سطح شمول برنامه خدمات امنیت سایبری خود را گسترده‌تر کرد تا کسب وکارهای کوچک و متوسطی که در زنجیره تأمین مجموعه صنایع دفاعی حضور دارند را نیز در بر گیرد. افزایش ۴۰۰ درصدی ثبت‌نام‌ها برای دریافت خدمات امنیت سایبری به ما کمک می‌کند تا بیش از پیش اطمینان حاصل کنیم که شرکای بسیار مهم ما در بخش دفاعی (و از جمله کسب‌وکارهای کوچک و متوسط) در امر دفاع از شبکه‌های خود تنها نیستند. این شراکت‌ها به ما اجازه می‌دهد با رویکردی رو به جلو و به صورت پیشگیرانه دیدگاه‌هایمان را به اشتراک بگذاریم و به وظایف محوله‌مان عمل کنیم:حفظ امنیت بخش دفاعی، حساس‌ترین شبکه‌های کشور و مجموعه صنایع دفاعی.

هوش مصنوعی یک تهدید (و یک فرصت) رو به رشد است. فناوری‌های هوش مصنوعی و یادگیری ماشین سریع‌تر از آن توسعه پیدا کرده و اشاعه پیدا می‌کنند که شرکت‌ها و دولت‌ها بتوانند هنجارها و استانداردهای مربوطه را شکل داده و تضمین کنند که نتایج مثبتی به وقوع می‌پیوندد. این ابزارهای جدید می‌توانند منجر به خلق قابلیت‌های دفاعی شگفت‌انگیزی شوند اما در عین حال می‌توانند قدرت مهاجمان را نیز افزایش دهند. مرکز امنیت هوش مصنوعی (Artificial Intelligence Security Center) که به تازگی به عنوان زیرمجموعه مرکز همکاری امنیت سایبری تأسیس شده نقطه تمرکز جدید آژانس برای کاربردی کردنِ اشراف اطلاعاتیِ منحصر به فردی است که NSA از طریق جاسوسی سیگنال و تخصص در امور فناوری به دست می‌آورد. این مرکز همچنین به صنایع کمک می‌کند که تهدیدات را در اکوسیستم هوش مصنوعی درک و از آن‌ها پیشگیری کرده و بتوانند با آن‌ها مقابله صورت دهند. این مرکز در قالب تلاش ما برای ترویج ایمن‌سازیِ ظرفیت‌های به وجود آمده از

هـوش مصنـوعی، یـک نقطـه کانـونی برای توسـعه تکنیک‌های مناسب، روش‌های ارزیابی و چارچوب‌های ریسک خواهد بود.

مـا همچنیـن در رقابـتِ دستیابـی بـه «رمزنگاری مقـاوم در برابـر کوانتـوم» (Quantum-Resistant Cryptography) بـا هـدف محافظـت از شـبکه‌ها، فناوری‌هـا و تسـلیحات مـوردِ اتکایمان، پیشرفـت کرده‌ایـم. ما برای هر یک از شـرکای خـارجیِ ائتلاف فرمانـدهی رزمی آمریکا نقشـه راه حوزه رمزنگاری را تکمیل کردیم تا بتوانند تشـخیص دهند که در چه بخش‌هایی نیاز به سرمایه‌گذاری بیشتر برای تأمین امنیت در برابر تهدیدات سایبری پیشرفته دارند و به شکل کامـل قابلیـت همـکاری و هماهنـگی را بـا نیروهای ایالات متحده و متحدان پیدا کنند.

در نهایت، این نتایج قابل توجه توسـط نیروهای NSA و سـازمان‌های شـریک رقـم خورده اسـت که نـوآوری و ایده‌پردازی‌هـای برجسـته‌ای می‌کنند و با کنش‌های فوری که بر اساس آن‌ها صورت می‌دهند، امنیتِ امروز و فردای کشـور و شـرکای ما را تأمیـن می‌کنند.

هوشیاری در خصوص اولویت‌ها و تهدیدات ملی

مقابله با تهدیدات جهانی

آژانس با همکاری شرکای داخلی و بین‌المللی به گسترش تأثیرگذاری خود در مقابله با تهدیدات رو به رشد جهانی و دشمنان کارآزموده ادامه می‌دهد.

همزمان که دولت ایالات متحده به اشراف اطلاعاتیِ منحصر به فردِ NSA در حوزه جاسوسی سیگنال خارجی برای اتخاذ تصمیمات کلیدی وابسته است، همکاری بخش عمومی و خصوصی این زمینه را ایجاد می‌کند تا درک چیستی تهدیدات و چگونگی مقابله با آن‌ها بهبود پیدا کند.

هر سازمان دارای توانایی‌ها، اختیارات و دیدگاه‌های منحصر به فرد خود است که به ترسیم تصویری گسترده‌تر کمک می‌کند که در نهایت توانایی NSA را برای پیشگیری و ریشه‌کنی برخی از نگران کننده‌ترین تهدیدات سایبری جهان ارتقا می‌بخشد.

آشکارسازی و رسیدگی به فعالیت‌های مخرب جمهوری خلق چین

آژانس با همکاری شرکای کلیدی از بخش صنعت، یک عامل سایبری پشتیبانی شده از سوی دولت جمهوری خلق چین را شناسایی کرد. این عامل از ابزارهای درونی شبکه برای هدف قرار دادنِ زیرساخت‌های حیاتی آمریکا استفاده می‌کرد. با هدف کمک به مدافعان شبکه برای شناسایی و شکار این نوع بدافزارِ چینی در سیستم‌های خود، NSA در هماهنگی با شرکای آمریکایی و بین‌المللی خود یک توصیه‌نامه مشترک را منتشر کرد. این توصیه‌نامه شامل راهنمایی برای مقابله و توصیه‌های مرتبط بود و مثال‌هایی از دستوردهی مهاجم و نشان‌گرهای شناسایی را در بر می‌گرفت.

در یک مورد دیگر، هنگامی که یکی از شرکای بخش صنعت تشخیص داد که عاملان مرتبط با جمهوری خلق چین تعدادی از اعضای مهم مجموعه صنایع دفاعی را با استفاده از یک آسیب‌پذیری روز صفر هدف قرار می‌دهند، آژانس بلافاصله نشان‌گرهای فنی را با شرکای مجموعه صنایع دفاعی به اشتراک گذاشت تا بتوانند تهدید را در شبکه‌های خود کشف کنند.

به شکل دقیق‌تر، این آسیب‌پذیری دستگاه‌هایی را که به طور گسترده در مجموعه صنایع دفاعی استفاده می‌شدند را هدف قرار داده بود. بنابراین تعاملات روزانه NSA با صنعت طی یک دوره دو ماهه به قطع و کاهش این حملات کمک کرد.

شکار بدافزار Snake سازمان اطلاعات روسیه

در هماهنگی با شرکا، آژانس یک بدافزار پیچیده جاسوسی سایبری روسی با نام Snake را شناسایی کرد که در بیش از ۵۰ کشور در سراسر جهان استفاده می‌شد. آژانس با همکاری نیروی ملی مأموریت سایبری (Cyber National Mission Force) از زیرمجموعه‌های فرماندهی سایبری ایالات متحده (USCYBERCOM)، اف‌بی‌آی، آژانس امنیت سایبری و زیرساخت‌ها (CISA)، مرکز امنیت سایبری کانادا، مرکز امنیت سایبری استرالیا (ACSC)، اداره امنیت ارتباطات دولتی نیوزیلند و مرکز امنیت سایبری ملی بریتانیا (NCSC)، راه‌اندازی و مدیریت بدافزار Snake را به یک واحد شناخته شده از مرکز ۱۶ سرویس امنیت فدرال روسیه منتسب کرد. این زیرساخت در سراسر آمریکای شمالی، آمریکای جنوبی، اروپا، آفریقا، آسیا و استرالیا شناسایی شد، از جمله در ایالات متحده و حتی روسیه. جزئیات فنی که همراه با شرکا منتشر شد به عملیات اف‌بی‌آی کمک کرد تا بتواند با کمک بسیاری از سازمان‌های شریک، این بدافزار را در سطح جهان یافته و حذف کنند.

همکاری بین‌المللی برای انتشار گزارش‌های راهنما

آژانس امنیت ملی با همکاری دولت آمریکا و طرف‌های همکار بین‌المللی، به اشتراک گذاری اطلاعات را از طریق توصیه‌های امنیت سایبری (Cybersecurity Advisory) در خصوص تهدیدات دولتی را امکان‌پذیر کرده است.

ما برای اولین بار با سازمان ملی پلیس ژاپن و مرکز استراتژی و آمادگی در برابر حوادث سایبری ژاپن همکاری نمودیم و با مشارکت آژانس‌های دیگر یعنی اف‌بی‌آی و CISA یک توصیه‌نامه مشترک منتشر کردیم تا جزئیات فعالیت یک عامل سایبری به نام BlackTech را افشا کنیم. این عامل سایبری که با جمهوری خلق چین مرتبط است نشان داده است که توانایی دستکاری ثابت‌افزارهای مسیریاب‌ها را بدون شناسایی شدن دارد و می‌تواند از روابط دامنه-اعتماد (Domain Trust) برای نفوذ به شرکت‌های آمریکایی و ژاپنی از طریق زیرمجموعه هایشان سوءاستفاده کند.

در یک ابتکار عمل دیگر، NSA با سرویس ملی اطلاعات، سازمان ملی پلیس و وزارت امور خارجه جمهوری کره، به همراه شرکای خود در اف‌بی‌آی و وزارت امور خارجه آمریکا، به صورت مشترک یک توصیه‌نامه امنیت سایبری منتشر کردند. این گزارش تأکید داشت که عاملان سایبری تحت حمایت جمهوری خلق کره از تکنیک‌های مهندسی اجتماعی استفاده می‌کنند تا توانمندی لازم برای نفوذ به شبکه‌ها و هدف قرار دادنِ کارکنان مراکز تحقیقاتی، اندیشکده‌ها، دانشگاه‌ها و خبرگزاری‌ها را پیدا کنند.

همکاری با بخش صنعت و دفاع از مجموعه صنایع دفاعی

حفاظت از مجموعه صنایع دفاعی

اگرچه بسیاری از مردم مجموعه صنایع دفاعی را با پیمانکاران بزرگ حوزه دفاعی مرتبط می‌دانند، اما بیش از ۷۰ درصد از این مجموعه متشکل از شرکت‌های کوچک است. پس از انعقاد قرارداد با وزارت دفاع، این شرکت‌ها اغلب به هدف بازیگران دولت‌های بیگانه تبدیل می‌شوند. کسب‌وکارهای کوچک معمولاً فاقد منابع لازم برای دفاع از خود در برابر نیروهای سایبری دولت‌ها هستند. آژانس امنیت ملی با شرکت‌های بزرگ و کوچک حوزه دفاعی -که شرکای مهم آژانس در این حوزه هستند- همکاری می‌کند و پیشروترین سازمان فعال در حوزه رمزنگاری و رمزشکنی در جهان را به یاری آن‌ها گماشته است.

همکاران حوزه صنعت آژانس امنیت ملی چه می‌گویند؟

«به عنوان یک کسب‌وکار کوچک، ما فاقد منابع نامحدودی هستیم که بازیگران بزرگ در اختیار دارند، بنابراین از هر چیزی که به ما برتری دهد، قدردانی به عمل می‌آوریم. این کمک‌ها سبب می‌شود که یک مسئله کمتر برای فکر کردن داشته باشیم، و یک مسئله کمتر برای هزینه کردن، و یک مسئله کمتر برای نگران شدن.»

آژانس امنیت ملی با پشتوانه چندین دهه تجربه و تخصص در رمزنگاری و رمزشکنی، خدمات امنیت سایبری را بدون هرگونه هزینه‌ای به پیمانکاران وزارت دفاع ارائه می‌دهد. این خدمات به نوعی طراحی شده‌اند که برای دفاع در برابر روش‌های اصلی حملات از سوی دشمنان به مجموعه صنایع دفاعی که آژانس مشاهده کرده مناسب باشند. این تجربیات با اشراف و تحلیل‌های منحصر به فرد آژانس نیز درهم‌آمیخته شده است. در سال ۲۰۲۳، به لطف تلاش‌ها در راستای توسعه و ارتقای راهکارها، آژانس امنیت ملی میزان ثبت‌نام‌ها برای دریافت خدمات امنیت سایبری را حدود ۴۰۰ درصد افزایش داد.

آژانس امنیت ملی در حال حاضر به بیش از ۶۰۰ شرکت حاضر در زنجیره تأمین وزارت دفاع، از جمله تأمین کنندگانی که ممکن است فاقد منابع کافی در زمینه امنیت سایبری باشند، کمک می‌کند. هر شرکتی که قرارداد جاری اصلی یا فرعی با وزارت دفاع داشته باشد می‌تواند از این خدمات استفاده کند، با این حال آژانس امنیت ملی چندین کارزار جدید را در سال ۲۰۲۳ ترتیب داد تا به شرکت‌هایی که در این حوزه‌ها فعالیت دارند اولویت دهد:

۱.منطقه مسئولیت فرماندهی اقیانوس هند و آرام ایالات متحده

۲.مناقشه روسیه و اوکراین

۳.سامانه‌های تسلیحاتی اولویت‌دار در وزارت دفاع

علاوه بر این، آژانس امنیت ملی با اداره کسب وکارهای کوچک وزارت دفاع همکاری کرده تا اطمینان حاصل شود که کسب‌وکارهای کوچک متعلق به اقلیت‌ها از این خدمات آگاهی داشته و فرصت استفاده از آن‌ها را برای صرفه‌جویی در هزینه‌ها و بهره‌گیری از امنیت شبکه بهتر دارند.

چهارچوب امنیت پایدار (Enduring Security Framework) از طریق همکاری با ۱۷ حکومت و ۶۲ شریک صنعتی، ۶ محصول امنیتی منتشر کرد که تهدیدات را در بخش‌های زیرساخت حیاتی ارتباطات، مجموعه صنایع دفاعی و فناوری اطلاعات برطرف می‌کند. به طور خاص، محصولات چهارچوب امنیت پایدار، به تهدیدات مرتبط با اینترنت نسل پنجم (5G)، هویت و مدیریت دسترسی و زنجیره تأمین نرم‌افزار پرداخته‌اند. این محصولات توصیه‌های مؤثری را ارائه کرده و برای بخش صنعت، بهترین شیوه‌ها برای کاهش تهدیدهای شناسایی شده را پدید آوردند.

گسترش خدمات امنیت سایبری برای مجموعه صنایع دفاعی

امسال آژانس امنیت ملی با بهره‌گیری از اشراف منحصر به فرد خود در مورد فعالیت‌های سایبری دولت‌ها، پیشنهادهایش را بهبود بخشید. خدمت دی‌ان‌اس حفاظتی (Protective Domain Name System) آژانس که مانع از اتصال کاربران به وب‌سایت‌های مخرب و یا مشکوک می‌شود، نمونه بارز بهبود خدمات است. آژانس یک ورودی سفارشی برای به‌روز کردن تهدیدات طراحی کرده که از طریق آن در هر هفته صدها نشان‌گر نفوذ (IoC) را به شرکت عامل فیلتر دی‌ان‌اس خود ارائه می‌دهد تا آن‌ها بتوانند لیست مسدودسازی خود را به‌روز کنند. این نشان‌گرهای نفوذ از سه منبع به دست آمده‌اند:

۱.اشراف به دست آمده از جاسوسی سیگنال

۲.تجزیه و تحلیل‌های آژانس

۳.داده‌های به‌دست آمده از شرکای بین سازمانی، بخش صنعت و یا شرکای بین‌المللی

تا به امروز، خدمت دی‌ان‌اس حفاظتی آژانس امنیت ملی حدود ۱۰ میلیارد درخواست غیرمجاز را مسدود کرده است. از این تعداد، حدود ۲۰ میلیون درخواست به دلیل تطابق با نشان‌گرهای گزارش شده از سوی آژانس مسدود شده‌اند؛ این یعنی آژانس در حال خنثی کردن فعالیت‌های مخرب سایبری است که در غیر این صورت شناسایی نشده و با آن‌ها مقابله صورت نمی‌گیرد. همچنین این نشان‌گرهای نفوذ با بخش‌های مختلف دولت آمریکا و شرکای بین‌المللی به اشتراک گذاشته می‌شوند تا اقدامات دفاعی را امکان‌پذیر کنند.

همچنین امسال NSA برنامه اسکن آسیب‌پذیری خود را برای ارائه پشتیبانی جامع مدیریت سطح حمله بهبود داد. این برنامه دو مزیت قابل توجه برای کسب‌وکارهای مجموعه صنایع دفاعی ارائه می‌کند؛ اول، از ابزارهای متن‌باز استفاده می‌کند تا فهرست کاملی از دارایی‌های مرتبط با اینترنت

شرکت‌ها را به آن‌ها ارائه دهد، زیرا نمی‌توان از چیزی که در خصوص آن اطلاعی نداریم محافظت کنیم. سپس این برنامه تمامی این دارایی‌ها را به قصد شناسایی آسیب‌پذیری‌ها بررسی می‌کند و گزارشی متناسب با آسیب‌پذیری‌های دارای اولویت ارائه می‌کند. این ابزار از اشراف اطلاعاتی آژانس در خصوص روش‌هایی که عاملان سایبری دولتی در حال بهره‌برداری از آن‌ها هستند، استفاده می‌کند.

در سال جاری، آژانس امنیت ملی همچنین از قابلیت «رصد مستمر» رونمایی کرد. هر روز، آژانس منابع مختلف را مورد رصد قرار می‌دهد تا ببیند عاملان وابسته به دولت‌های دیگر چه زمانی شروع به بهره‌برداری از آسیب‌پذیری‌های شناخته‌شده عمومی می‌کنند. وقتی یک آسیب‌پذیری از وضعیت «شناخته شده» به وضعیت «مورد سوءاستفاده» منتقل می‌شود، آژانس فوراً فهرست دارایی‌های کشف شده خود را جست‌وجو می‌کند تا شناسایی کند که کدام یک از مشتریان مجموعه صنایع دفاعی ممکن است آن آسیب‌پذیری را در محیط خود داشته باشند و این اخطار را برای آن‌ها صادر می‌کند که یک آسیب‌پذیری فعال در دستگاهی حاضر در آن محیط وجود دارد. این هشدارها نرخ پاسخگویی ۸۰ درصدی دارند و نتیجتاً ثابت می‌کنند که شرکت‌ها در حال یافتن و رفع مشکلات خود پیش از به خطر افتادن داده‌ها و استخراج‌شان هستند.

امسال به کمک برنامه مدیریت سطح حمله، یک کارزار بزرگ مرتبط با جمهوری خلق چین که چندین شرکت از مجموعه صنایع دفاعی را با استفاده از یک آسیب‌پذیری در محیط‌های Citrix هدف قرار می‌داد، کشف شد. در نتیجه همکاری آژانس امنیت ملی با شرکت‌های بزرگ و کوچک صنایع دفاعی و Citrix، آژانس همزمان با افشای این کارزار، وصله (patch) امنیتی مربوطه را نیز منتشر کرد. محققان مستقل در وبلاگ‌های خود نوشتند که طی چند روز پس از انتشار این توصیه، تعداد سرورهای آسیب پذیر در آمریکا و کشورهای متحد تقریباً ۲۵ درصد کاهش یافت.

سرویس همکاری اطلاعات تهدید (Threat Intelligence) آژانس امنیت ملی در سال جاری به بلوغ خود رسید. از طریق این خدمت، شرکت‌ها می‌توانند اطلاعات تهدیدِ غیرعمومی و مخصوص مجموعه صنایع دفاعی آژانس را از طریق یک مسیر همکاری امن و طبقه‌بندی نشده دریافت کنند. این روش به شرکت‌ها امکان دسترسی به ظرفیت تحلیلی آژانس را به سادگی از طریق باز کردن یک برنامه در گوشی همراه خود می‌دهد و به آن‌ها کمک می‌کند توانمندی‌های خود برای اقدام و محافظت بهتر از شبکه‌ها را توسعه دهند.

افزایش طرح‌های آزمایشی ابتکاری

سرمایه‌گذاری در زمینه خدمات امنیت سایبری مربوط به مجموعه صنایع دفاعی، به همین‌جا ختم نمی‌شود. آژانس امنیت ملی امسال چهار طرح آزمایشی جدید را راه‌اندازی کرد که به مدت ۱۲ ماه اجرا می‌شوند. ارزیابی‌هایی که به وسیله این طرح‌ها صورت خواهد گرفت نشان خواهد داد که آیا این خدمات در کاهش فعالیت‌های سایبری دولت‌ها تأثیرگذار بوده است یا نه و آیا می‌توانند به شکلی کم هزینه، قابل گسترش و بدون سربارهای اضافی به شرکت‌های حاضر در این طرح‌ها کمک کنند یا خیر. طرح‌های آزمایشی جدید عبارت‌اند از:

امنیت ابری: از آنجایی که رایانش ابری به سرعت در حال تبدیل شدن به یک هنجار برای امنیت سایبری است، آژانس امنیت ملی تلاش‌ها را بر کشف و رسیدگی به آسیب‌پذیری‌ها و پیکربندی‌های نادرستی متمرکز می‌کند که شبکه‌های مجموعه صنایع دفاعی

و حقوق مالکیت فکری آن‌ها را آسیب‌پذیر می‌سازد. این طرح آزمایشی همچنین داده‌های لازم برای درک سطح حمله ابری به این صنایع را در اختیار مرکز همکاری امنیت سایبری آژانس قرار می‌دهد که برای تهیه و انتشار راهنمایی امنیتی ابری ویژه مجموعه صنایع دفاعی استفاده خواهد شد.

شکار تهدید: شناسایی و رسیدگی به تهدیدات پیش از ضربه زدن، به شکل فعال نیازمند بستری برای ارائه اطلاعات سیستم‌ها و مدیریت رویداد از سوی شرکای مجموعه صنایع دفاعی است. این بستر شناسایی و رسیدگی به فعالیت‌های مخرب و مشکوک در شبکه را تسهیل می‌کند. تحلیلگران آژانس در کنار شرکا در صنایع دفاعی مترصد تهدیدات خواهند بود و راهنمایی‌ها و تحلیل‌های لازم برای مقابله با آن‌ها را برای تمامی مجموعه صنایع دفاعی ارسال خواهند کرد.

حفاظت در برابر فیشینگ: فیشینگ از جمله حملات فراگیر محسوب می‌شود. این طرح آزمایشی به مشتریان ما از صنایع دفاعی یک دروازه ایمیل امن برای فیلتر کردن حملات فیشینگ می‌دهد و برای آن‌ها دسترسی مناسبی به جعبه شنی (sandbox) برای بهتر پیدا کردن بدافزارها و پیوست‌های مخرب می‌دهد تا فرصت مناسب برای رسیدگی و مقابله با این حملات ایجاد شود.

تست نفوذ خودکار: این طرح ابتکاری از ابزارهای خودکار، الگوریتم‌ها و هوش مصنوعی برای شناسایی آسیب‌پذیری‌های دیجیتالی بهره می‌گیرد و نسبت به نیروهای انسانی توان انجام تست‌ها به صورت مداوم‌تری را دارد. در این طرح ابتکاری با تقلید از اقدامات هکرها، ارزیابی تهدید به صورت لحظه‌ای (real-time) به مشتریان عرضه می‌شود تا مداخله انسانی کاهش و کارآمدی افزایش یابد و دیدگاه روشن‌تری نسبت به شیوه تفکر دشمنان به دست آید.

به روایت اعداد

۷۵۰ مجموعه همکار

۲۰ میلیون مسدودسازی که از سوی نشانگرهای نفوذ آژانس امنیت ملی صورت گرفته است

بیش از ۵۵۰ هشدار آسیب‌پذیری به شرکا ارسال شده، با نرخ پاسخگویی ۸۰ درصد

۱۰ میلیارد دامنه مخرب/ مشکوک پردازش و/یا مسدود شدند، از جمله فعالیت باج‌افزار و بدافزارهای وابسته به دولت‌ها، فیشینگ هدف‌دار و بات‌نت‌ها

۳۱۲ هزار دارایی بر روی اینترنت متعلق به شرکت‌های مجموعه صنایع دفاعی شناسایی و فهرست‌بندی شد

۷۰ خوشه منحصر به فرد از فعالیت‌های شناخته‌شده از سوی دولت‌ها به طور پیوسته توسط آژانس امنیت ملی و بخش صنعت ردیابی می‌شوند

صدها نشانگر نفوذ منحصر به فرد و جدید که به صورت هفتگی در فهرست مسدودسازی آژانس امنیت ملی قرار می‌گیرند

۱/۳ میلیون آسیب‌پذیری کشف و برای اصلاح نشان‌گذاری شدند

چندین کارزار متعلق به دولت‌های بیگانه که مجموعه صنایع دفاعی را هدف قرار می‌دادند افشا شدند. برخی از آن‌ها از آسیب‌پذیری‌های روز صفر بهره می‌گرفتند

ایمن‌سازی هوش مصنوعی

مرکـز جدیـدی که در آژانس امنیت ملی با نام مرکز امنیت هوش مصنوعی و در زیرمجموعه مرکز همکاری امنیـت سـایبری تأسـیس شـد، ایمن‌سـازی فرآینـد توسـعه، یکپارچه‌سـازی و بهره‌بـرداری از قابلیت‌های هـوش مصنـوعی را در سـامانه‌های امنیـت مـلی و مجموعـه صنایـع دفـاعی ترویـج می‌کند. ایـن مرکز همچنین از اشراف اطلاعاتی منحصر به فرد آژانس که برآمده از جاسوسی سیگنال‌های خارجی است استفاده می‌کند تا به صنعت در فهم این موضوع که دشمنان چگونـه از هـوش مصنـوعی بهره برده و سـامانه‌های هوش مصنوعی را هدف قرار می‌دهند کمک کند. مرکز امنیـت هـوش مصنوعی با مشـارکت رهبـران بخش صنعـت آمریکا، آزمایشـگاه‌های ملی و دانشـگاه‌ها و همچنین در هماهنگی با جامعه اطلاعاتی، وزارت دفاع و شـرکای خارجی، در توسـعه شیوه‌هـا و توصیه‌های امنیتی در حوزه هوش مصنوعی مشارکت می‌نماید.

مشارکت برای مقابله با تهدیدات و ایجاد استاندارد

مرکـز اسـتانداردهای امنیـت سـایبری (Center for Cyber Security Standards) در زمینـه تنظیم، ارتقا و مدیریتِ اِعمال استانداردهای مخابراتی فعالیت می کند. این مرکز بر ایمن‌سازی اینترنت نسل پنجم (5G) و آماده‌سـازی پروتکل‌هایـی برای رمزنـگاری مقاوم در برابر محاسبات کوانتومی تمرکز دارد. تا به امروز، مرکز استانداردهای امنیت سایبری بیش از ۹۵ استاندارد را برای اینترنت نسل پنج، شبکه‌های ابری و پروتکل‌های اینترنـتی تدوین و منتشـر کرده اسـت. ایـن اقدامات تضمیـن می‌کنـد کـه امنیـت برقـرار شـده و توانایی دشـمنانمان برای سـرقت دارایی‌های معنـوی آمریکا کاهـش پیـدا کند. آژانس امنیت مـلی در بیش از ۱۵ سـازمان توسـعه اسـتاندارد و بیـش از ۴۰ کارگـروه مشارکت دارد. آژانس با ارائه نظرات تخصصی فنی در مجامع مختلف از دولت ایالات متحده پشتیبانی به عمل آورد. در مجمع بخش مخابـرات اتحادیـه بین‌المللی مخابرات (ITU)، مرکز استانداردهای امنیت سایبری با همکاری نزدیک وزارت امور خارجه به عنوان هیئـت نمایندگی ایالات متحده به خدمت مشـغول بـود. ایـن مرکـز چندیـن پیش‌نویـس را بـرای اسـتانداردهای پـروتکل ایمن را در کارگـروه مهندسی اینترنـت (IETF)، بـرای اطمینـان از مقـاوم بـودن پروتکل‌ها و هم‌کنش‌پذیری در دوران پساکوانتوم ارائه کرد.

مرکز اسـتانداردهای امنیت سـایبریِ آژانس امنیت ملی، اکنون عضوی از ائتلاف شبکه دسترسی رادیویی بـاز (O-RAN) اسـت؛ یـک کنسـرسیوم بین‌المللی که استانداردهای شبکه دسترسی رادیویی را برای اینترنت نسل پنجم توسعه می‌دهد. از نظر تاریخی این ائتلاف بـا دولـت آمریکا ارتباطی برقرار نمی‌کرد و پیش از این بیشـتر بـر انگیزه‌هـای بـازاری متمرکز بود تـا الزامات امنیـتی. از آنجا که فناوری شـبکه دسـترسی رادیویی جزئی کلیدی از زیرسـاخت اینترنت نسل پنجم است، مشـارکت در این ائتلاف که با اجماع اعضا امکان‌پذیر اسـت راهی برای ایالات متحده جهت تقویت اهداف امنیتی برای اینترنت نسل پنجم به شمار می‌رود.

مرکز استانداردهای امنیت سایبری از طریق چهارچوب امنیت پایدار، مطالعه‌ای را با هدف افزایش مجدد سرمایه گـذاری آمریـکا و متحدانـش در سـازمان‌های توسـعه اسـتاندارد (SDOs) تدوین کرد که امنیت فناوری‌های حیـاتی را در بلندمـدت تضمیـن می‌کنـد. ایـن گروه مطالعـاتی تهدیدهـای فنی و ژئوپلیتیـکی که متوجه سـازمان‌های توسـعه اسـتاندارد بین‌المللی هستند را ارزیابـی کرده و اسـتراتژی‌هایی را بـرای مقابله با این تهدیدها پیشـنهاد کـرد. آگاهی آژانـس امنیت ملی، دولـت آمریـکا، بخش صنعـت و شـرکای بین‌المللی نسبت به تهدیدات علیه استانداردها افزایش پیدا کرد و بـرای مبـارزه با ایـن تهدیـدات، راهبردهایی اتخاذ کردند. بهترین راه برای مقابله با نفوذ دشمنان خارجی در سازمان‌های توسعه استاندارد بین‌المللی این است

که کشورهایی که در زمینه امنیت، حریم خصوصی و رقابت در بازار جهانی ارزش‌های مشترکی دارند، مشارکت خود را از طریق ارائه پیشنهادهای فنی صحیح نشان دهند.

محصولات تجاری به طور فزاینده‌ای جهت ایمن‌سازی سامانه‌های امنیت ملی مورد استفاده قرار می‌گیرند. از طریق برنامه ملی اطمینان اطلاعات (NIAP)، مرکز همکاری‌های امنیت سایبری ۵۷ قطعه تجاری را به منظور استفاده جهت حافظت از سامانه‌های امنیت ملی مورد تائید قرار داد. علاوه بر این، برنامه ملی اطمینان اطلاعات سه نمایه حفاظتی (Protection Profile) را به منظور افزایش امنیت در محصولات مذکور منتشر کرد. نمایه‌های حفاظتی دستورالعمل‌هایی هستند که فارغ از تولیدکننده و نوع محصول تجاری، امنیت آن‌ها را از طریق تعریف حداقل‌هایی از الزامات امنیتی افزایش می‌دهند. همچنین برنامه ملی اطمینان اطلاعات، روند به‌روزرسانی نمایه‌های حفاظتی را بیش از پیش تسریع می‌کند تا با دستورالعمل الگوریتم‌های تجاری امنیت ملی، احراز هویت چندعاملی و اصول اعتماد صفر (Zero Trust) مطابقت داشته باشد.

برنامه ملی اطمینان اطلاعات از طریق مشارکت پیوسته با ۳۱ کشور در چارچوب توافق‌نامه ترتیبات تشخیص معیارهای مشترک (CCRA) به تقویت امنیت جهانی فناوری اطلاعات ادامه داد. توافق‌نامه CCRA ارزیابی‌های مستمر بین اعضا و شناخت متقابل را تضمین می‌کند تا این امکان را برای تولیدکنندگان فراهم کند که پیش از فروش تجهیزات در چندین کشور، آن‌ها را مورد آزمایش قرار دهند.

این توافق‌نامه از دو جهت ایالات متحده را در جایگاه رهبری جامعه جهانی قرار داده است؛ اول از طریق استفاده بیشتر از استانداردهای ایالات متحده و دوم از طریق صدور بیشترین تعداد گواهینامه برای محصولات تولیدشده در بین کشورهای عضو CCRA.

برنامه ملی اطمینان اطلاعات به ریاست بر کمیته مدیریت CCRA ادامه داد و موجب گسترش همکاری‌ها در جهت شناخت متقابل شد. برنامه ملی همچنین میزبان کنفرانس بین‌المللی CCRA و نشست CCRA در واشنگتن دی‌سی با حضور ۲۶ کشور بود که در آن‌ها بر ارزش مشارکت‌های بین‌المللی برای نسل بعدی فناوری‌های تجاری تأکید صورت گرفت.

آژانس امنیت ملی میزبان یک کارگروه عملیات‌های فریب همراه با شرکای بخش صنعت بود. این کارگروه پس از موفقیت شرکای بخش صنعت در برابر تهدید هانی‌پات‌ها (Honeypots) و تمایل آن‌ها برای به اشتراک گذاشتن ابزارها و تکنیک‌های مرتبط با عملیات‌های فریب به وجود آمد. در این کارگروه کارشناسان آژانس دیدگاه‌های فنی خود را ارائه کردند و شرکای بخش صنعت نیز تجربیات خود را به اشتراک گذاشتند و رویکردهای مختلف را در عملیات‌های فریب توضیح دادند. این کارگروه، ارتباطی ادامه‌دار را بین بخش صنعت و آژانس برای همکاری‌های آتی پدید آورد. این ارتباط شیوه‌های جدیدی را به وجود می‌آورد که نه تنها برای دفاع از شبکه‌ها در برابر دشمنان خارجی توسعه دهد بلکه همچنین آگاهی بیشتری در خصوص روش‌هایی که عاملان تخریب‌گر برای هدف قرار دادن مجموعه صنایع دفاعی، وزارت دفاع و سایر زیرساخت‌های حیاتی آمریکا استفاده می‌کنند، به وجود آورد.

آژانس امنیت ملی همچنین در راستای تعامل با شرکای خود در جهت ایجاد استانداردهای امنیت سایبری، میزبان نخستین اجلاس «تهدید علیه استانداردها» بود و کارشناسان حوزه استاندارد را از تمامی بخش‌های دولت ایالات متحده، شرکای خارجی، صنعت و دانشگاه‌ها را گرد هم آورد تا چالش‌ها و خطرات رو به رشد مرتبط با استانداردهای امنیت سایبری را بررسی کنند.

تسلیح مدافعان شبکه با ارائه اسناد راهنما

ارائه راهنمایی‌های عملی و به موقع

مدافعان شبکه در محیط پیچیده تهدیدات امروزی با مسائل بسیاری مواجه هستند و برای کاهش آسیب‌پذیری‌های جدی و محافظت از شبکه‌های خود در برابر جرائم سایبری و تهدیدات دشمنان، به اطلاعات به موقع نیازمندند.

گزارش‌های عمومی آژانس امنیت ملی که اغلب با افزایش بیش از پیش تعداد طرف‌های همکار تهیه و منتشر می‌شود، به تسلیح مدافعان شبکه از طریق ارائه راهنمایی‌ها و مشورت‌های مورد نیاز آن‌ها در خصوص مسائل حساس و حیاتی امنیت سایبری کمک می‌کند.

در هماهنگی با همکاران، آژانس امنیت ملی به صورت عمومی ۲۷ مورد توصیه‌نامه و اطلاعیه در حوزه امنیت سایبری منتشر کرده که بر روی وب‌سایت NSA.gov قابل دسترسی هستند.

این‌گونه گزارش‌ها طیف گسترده‌ای از موضوعات مختلف را پوشش می‌دهد؛ از بهترین روش‌ها برای حفظ امنیت شبکه‌های خانگی تا استفاده دولت کره شمالی از روش‌های مهندسی اجتماعی برای هک کردن اندیشکده‌ها، دانشگاه‌ها و رسانه‌ها.

مثالی دیگر در این زمینه، کمک به مجموعه‌های مختلف برای مقابله با تهدید جعل عمیق (دیپ‌فیک) است. جعل عمیق به معنای ساختن محتوای مصنوعی اما بسیار واقع‌گرایانه توسط هوش مصنوعی است. جعل عمیق می‌تواند در راستای تهدید برند یک سازمان، جعل هویت رهبران و ایجاد دسترسی به شبکه ها، ارتباطات و اطلاعات حساس مورد سوءاستفاده قرار گیرد. آژانس امنیت ملی با همکاری اف‌بی‌آی و آژانس امنیت سایبری و امنیت زیرساخت (CISA) اقدام به انتشار اطلاعیه امنیت سایبری با عنوان «تبیین تهدیدات جعل عمیق برای سازمان‌ها» کرده است.

این سند شامل یک مرور کلی بر تهدیدات ناشی از محتوای مصنوعی و شگردها و روندهای این حوزه است. همچنین در این اطلاعیه توصیه‌ها، راهنمایی‌ها و راهبردهایی برای کاهش خسارات جعل عمیق با تمرکز بر محافظت از سازمان‌ها در برابر این تهدید رو به رشد ارائه می‌کند.

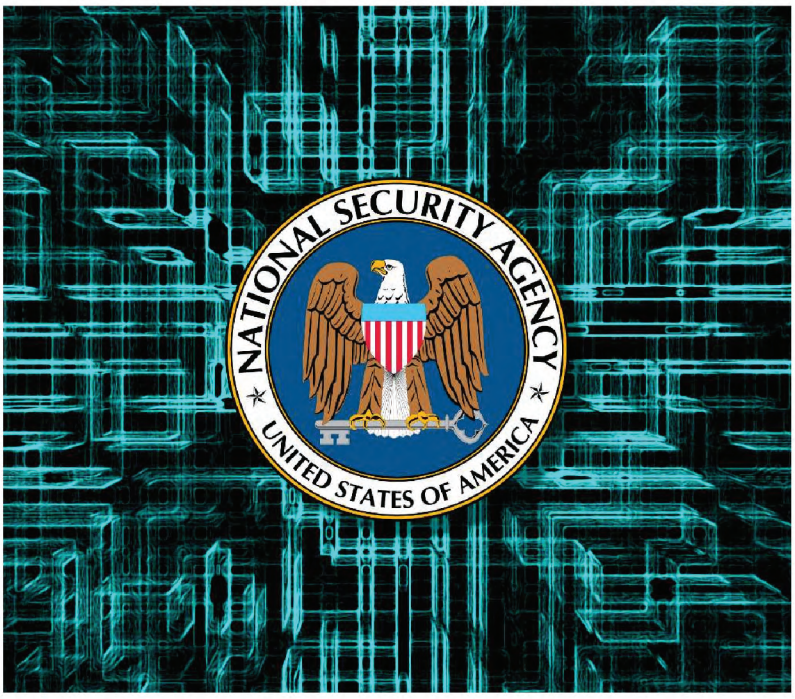
آژانس امنیت ملی و آژانس‌های همکار از طریق انتشار این اسناد می‌توانند اقدامات ضروری برای کاستن از خسارات این‌گونه تهدیدات را ارائه کرده و از این رهگذر به حفاظت از طیف گسترده‌ای از سیستم‌ها کمک کنند.

آژانس امنیت ملی با راه‌اندازی شبکه هشدارهای دفاعی شبکه (Network Defense Notice) توانست ارائه نشان‌گرهای نفوذ (IoC) را که به شناسایی انواع بدافزارها کمک می‌کردند را تسهیل کند. هشدارهای دفاعی شبکه برای سایر سازمان همکار در جامعه اطلاعاتی به‌روزرسانی‌های سریعی در مورد بدافزارهای مشاهده شده در فضای سایبری فراهم می‌کند که در نتیجه آن‌ها می‌توانند از این هشدارها برای مقابله با تهدیدهای احتمالی این بدافزارها برای سیستم‌هایشان ترتیبات لازم را اتخاذ نمایند.

دفاع از حساس‌ترین شبکه‌های کشور

دفاع از شبکه‌های بسیار حیاتی

آژانس امنیت ملی همچنان از اجرای «یادداشت بهبود وضعیت امنیت سایبری در سامانه‌های امنیت ملی، وزارت دفاع و جامعه اطلاعاتی» معروف به یادداشت شماره ۸ امنیت ملی (NSM-8) حمایت می‌کند. این یادداشت اختیارات جدیدی به رئیس آژانس امنیت ملی به عنوان مدیر سامانه‌های امنیت ملی (NSS) داد. این اختیارات باعث شد که میزان دسترسی‌های بخش امنیت سایبری در آژانس به شبکه‌های حساس افزایش یابد؛ شبکه‌هایی که حاوی اطلاعات طبقه‌بندی شده هستند و یا به هر نحو برای فعالیت‌های نظامی و اطلاعاتی در تمامی بخش های دولت حیاتی محسوب می‌شوند. از زمان امضای یادداشت شماره ۸، آژانس امنیت ملی روابط نزدیک‌تری با بیش از ۵۰ وزارت‌خانه و سازمان دولتی که مالک سامانه‌های امنیت ملی هستند یا از آن‌ها بهره‌برداری می‌کنند، برقرار کرده است. آژانس امنیت ملی به افزایش سطح امنیت سیستم‌های حساس دولت ایالات متحده ادامه می‌دهد تا از داده‌های حساس نظامی و اطلاعاتی در برابر دشمنانمان محافظت کنیم.



محافظت از اسرار کشور

آژانس امنیت ملی در بطن فرآیند طراحی و ساخت سامانه‌های امنیت ملی و سامانه‌های تسلیحاتی وزارت دفاع و رمزنگاری‌های آن‌ها قرار دارد. آژانس همچنان وظیفه حفظ ایمنی میلیون‌ها دستگاه و تجهیز را در سراسر جهان به عهده دارد و زیرساخت‌های لازم برای رمزگذاری آن دستگاه‌ها را با ظرفیت‌های خود مدیریت می‌کند. این امر شامل تولید و توزیع کلیدها، کدها و ابزارهای رمزنگاری می‌شود که دولت و ارتش ایالات متحده را قادر می‌سازد تا از تسلیحات، ماهواره‌ها، ارتباطات و بسیاری دیگر از سیستم‌هایی که امنیت ملی شدیداً به آن‌ها وابسته است، محافظت کند.

آژانس امنیت ملی مسئول حفاظت از حساس ترین اسرار کشور در برابر قوی‌ترین دشمنانمان است: کشورها و افراد توانمند در حوزه سایبری که قصد ورود به شبکه‌هایمان را دارند و یا رمزنگاری‌ما را مورد حمله قرار دهند، مسئول می‌داند.

کلیدهای رمزنگاری آژانس همه‌چیز را ایمن نگه می‌دارند؛ از دستگاه‌های ارتباط رادیویی تاکتیکی و هر ابزار رمزنگاری شده در دست سربازان، ملوانان، خلبانان، نگهبانان و تفنگداران آمریکایی تا پلتفرم‌های تسلیحاتی حساس مانند سیستم کنترل و فرماندهی اتمی. آژانس امنیت ملی بر ایمن بودن سیستم‌های مورد استفاده نظامیان ما در برابر حملات سایبری نظارت دارد و از مزیت راهبردی آمریکا در درگیری‌های نظامی محافظت می‌کند.

در سال گذشته تحلیل‌های آژانس زیرساخت‌های ابهام‌سازی (Obfuscation) جمهوری خلق چین که به صورت عمومی نیز منتشر شد، عملکرد دفاع از سامانه‌های امنیت ملی را بهبود بخشید.

مرکز همکاری امنیت سایبری توانست از رهگذر شگردهای تحلیلی و با استفاده از گزارش‌های شناسایی که شرکت‌های تجاری منتشر کرده بودند فعالیت‌های مخرب جمهوری خلق چین را شناسایی کند. تشخیص خودکار شاخصه‌های این نوع حملات توانست شناسایی اقدامات جمهوری خلق چین علیه شبکه سامانه‌های امنیت ملی را تسهیل کند.

ایمن‌سازی فناوری عملیاتی

گروه‌های عامل در حوزه سایبری تمایل دارند فعالیت‌های مخرب سایبری علیه زیرساخت‌های حیاتی را از طریق بهره‌برداری از دارایی‌ها و زیرساخت‌هایی انجام دهند که از اینترنت قابل دسترسی هستند. آژانس تعدادی از پایگاه‌های وزارت دفاع را مورد ارزیابی قرار داد، چندین توصیه امنیت سایبری و هشدار دفاعی برای حفظ ایمنی فناوری های عملیاتی (Operational Technologies) منتشر کرد. آژانس به تأمین امنیت زیرساخت‌های فناوری عملیاتی و سامانه‌های امنیت ملی ادامه می‌دهد. به همین منظور، آژانس امنیت ملی مجموعه‌ای از نشان‌گرهای تشخیص نفوذ به سیستم‌های OT را در حساب CyberGitHub آژانس منتشر کرد. این ظرفیت، که به عنوان الیت‌ولف (ELITEWOLF) شناخته می‌شود، می‌تواند مدافعان شبکه را در حفاظت از زیرساخت‌های حیاتی، مجموعه صنایع دفاعی و سامانه‌های امنیت ملی یاری کرده و آن‌ها را قادر به شناسایی و تشخیص فعالیت‌های سایبریِ بالقوه مخرب در محیط OT خود سازد.

نوسازی روش‌های رمزنگاری برای محافظت از داده‌ها و ارتباطات

حرکت به سوی رمزنگاری مقاوم در برابر کوانتوم

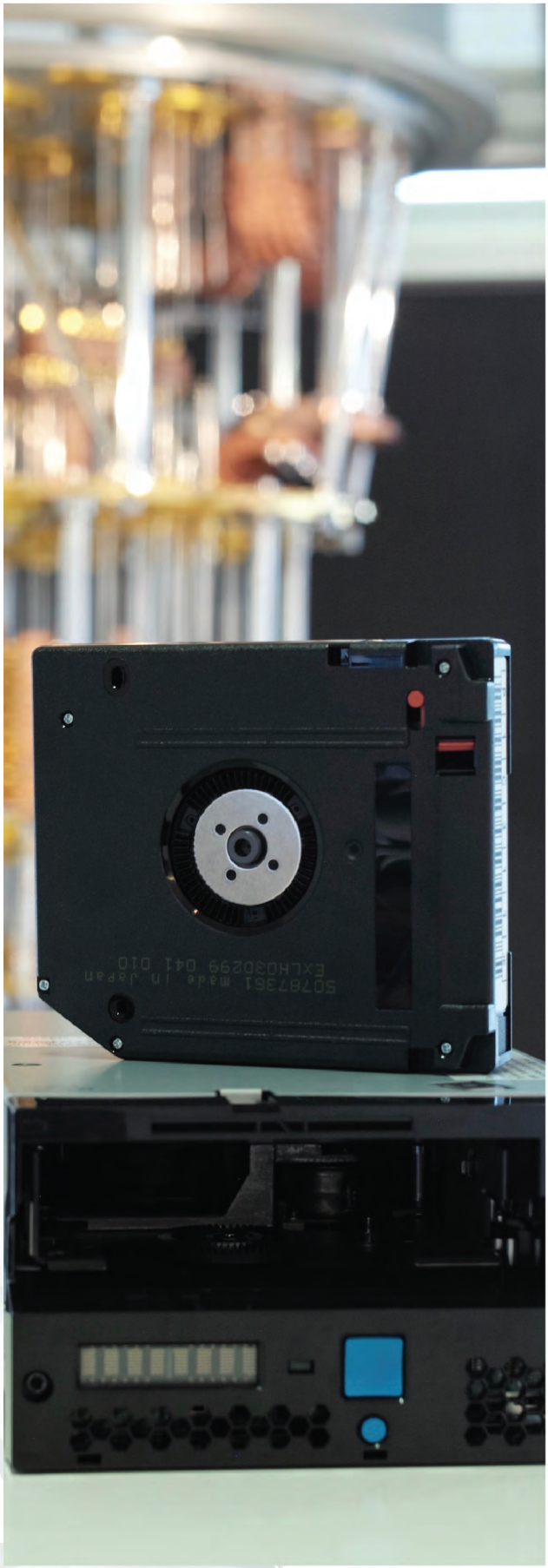
هنگامی که کامپیوتر کوانتومی مرتبط با رمزنگاری اختراع شود، وضعیت به کلی دگرگون خواهد شد. این امر تهدیدهای بسیاری علیه سیستم‌های اطلاعاتی کشورمان به وجود خواهد آورد و سیستم‌های رمزنگاری که امنیت اینترنت و سیستم‌های اطلاعاتی را در سراسر جهان حفظ می‌کنند، خواهد شکست.

رمزنگاری مقاوم در برابر کوانتوم همچنان بهترین دفاع در برابر این تهدید بزرگ است.

آژانس امنیت ملی به اجرای یادداشت استراتژیک شماره ۱۰ امنیت ملی با عنوان «ارتقای رهبری ایالات متحده در محاسبات کوانتومی و کاهش خطرات علیه سیستم‌های رمزنگاری آسیب پذیر» ادامه می‌دهد. این یادداشت به سازمان‌های حکومتی ایالات متحده دستور می‌دهد تا در یک برنامه چندساله سیستم‌های رمزنگاری آسیب‌پذیر را به رمزنگاری مقاوم در برابر کوانتوم ارتقا دهند.

مدیر آژانس امنیت ملی به عنوان مدیر سامانه‌های امنیت ملی (NSS) بر فرآیند ارتقا به رمزنگاری مقاوم در برابر کوانتوم در بیش از ۵۰ سازمان و نهاد حکومتی که از سامانه‌های امنیت ملی استفاده می‌کنند، نظارت می‌نماید.

تداوم بخشیدن به مشارکت و همکاری با شرکای دولتی و خصوصی، کلید مبارزه با این چالش حوزه امنیت سایبری است. آژانس امنیت ملی در این زمینه با موسسه ملی استاندارد و فناوری (NIST)، آژانس امنیت سایبری و زیرساخت (CISA)، بخش دانش و فناوری در دفتر مدیر اطلاعات ملی (ODNI S&T) و همچنین وزارت دفاع و سازمان‌های استاندارد خارجی مشارکت و همکاری می‌کند.



جامعه امنیت سایبری -که متشکل از بخش صنعت، دولت و دانشگاه‌ها است- بایستی از هم‌اکنون برای نوسازی رمزنگاری، برنامه‌ریزی کند. محاسبات کوانتومی ممکن است یک تهدید قریب‌الوقوع به نظر نرسد، اما تهدیدی است که اکنون باید برای مقابله با آن اقدام کرد.

در سال گذشته، آژانس امنیت ملی بر اساس اعلامیه شماره ۲ الگوریتم‌های تجاری (Commercial National Suite2.0) که پیش‌تر منتشر شده بود، دستورالعملی تهیه و تنظیم کرد که تمامی مالکان، عملگرها و تأمین‌کنندگان سامانه‌های امنیت ملی را از الزامات آینده الگوریتم‌های مقاوم در برابر کوانتوم برای استفاده در تمامی بخش‌های سامانه های امنیت ملی، مطلع کرد. در ماه مارس و ژوئن، آژانس امنیت ملی دستورالعملی را با هدف کمک به دولت آمریکا جهت شناسایی و فهرست‌بندی رمزنگاری‌های آسیب‌پذیر در برابر کوانتوم، تقویت مجموعه فعلی رمزنگاری و برنامه‌ریزی برای ارتقا به رمزنگاری مقاوم در برابر کوانتوم منتشر کرد. این برنامه نوسازی شامل فهرست‌بندی رمزنگاری، اولویت‌بندی، زمان‌بندی و استفاده مناسب از منابع و نیز برنامه‌ریزی برای بهره‌گیری از مجموعه الگوریتم‌های مقاوم در برابر کوانتومِ آژانس و استانداردهای مصوب از سوی مؤسسه ملی استانداردها و فناوری (NIST) برای سامانه‌های امنیت ملی می‌شود.

گذار به رمزنگاری مقاوم در برابر محاسبات کوانتومی تنها مثالی از این واقعیت است که چگونه آژانس برای محافظت از حساس‌ترین داده‌های کشور همواره یک گام جلوتر از دشمنانمان قرار دارد. آژانس امنیت ملی به طور مداوم روش‌های امنیت سایبری خود را به گونه‌ای نوسازی می‌کند که چابک، سازگار با تهدید و مقیاس‌پذیر در عملیات چنددامنه‌ای باشد.

محافظت از نیروهای جنگی و پشتیبانی از قرارگاه های فرماندهی رزمی

پشتیبانی از ارتش

آژانس امنیت ملی به عنوان بخشی از وزارت دفاع، یک سازمان پشتیبانی رزمی است و از رهگذر انجام دو وظیفه کلیدی از آن پشتیبانی به عمل می‌آورد: تجسس سیگنال‌های خارجی و امنیت سایبری. در حالی که کارشناسان ما در حوزه جاسوسی سیگنال خارجی نقش پشتیبانی اطلاعاتی را در عملیات نظامی بر عهده دارند، کارشناسان امنیت سایبری آژانس نیز به ایمن ماندن ارتباطات و داده‌های نظامی کمک می‌کنند.

آژانس امنیت ملی شراکت گسترده و پویای خود را با فرماندهی سایبری ایالات متحده برای ارائه پشتیبانی برای عملیات‌های شکار رو به جلو (Hunt Forward) تحکیم بخشید. در این عملیات‌ها تیم‌هایی به درخواست شرکای ما در سراسر جهان در کشورهای میزبان مستقر شده و به آن‌ها در برابر گروه‌ها و عوامل سایبری مخرب کمک می‌کنند.

جنگجویان ما می‌بایست نسبت به عملیات خود اطمینان داشته باشند. کمک‌های آژانس امنیت ملی به تحقق این هدف کمک می‌نماید، به نحوی که ارتش ایالات متحده توانایی ایمن سازی ارتباطات برای عملیات‌هایی نظیر کنترل و فرماندهی هسته‌ای و همچنین توان تمایز بین دوست و دشمن را داشته باشد. آژانس همراه با شرکای خود در دولت آمریکا تلاش می‌کند تا از ایمن بودن عملکردهای اصلی مدیریتی، شبکه‌ها، سامانه‌ها و دستگاه‌های ارتباطی مورد استفاده وزارت دفاع اطمینان حاصل شود. آژانس همچنین بهترین شیوه‌های تأمین امنیت ارتباطات را عرضه می‌دارد تا محتوای رمزنگاری که در این سامانه‌ها و دستگاه‌ها مورد استفاده قرار می‌گیرند ایمن باقی بمانند.

آژانس امنیت ملی همچنین محصولات امنیتی در حوزه رمزنگاری را برای رسیدگی به حوادث برنامه ریزی نشده و پشتیبانی از مأموریت‌های فوری عرضه می‌کند. در سال گذشته، آژانس امنیت ملی برای پشتیبانی مأموریت‌های عملیاتی در وضعیت‌های بحرانی جهانی، در حدود ۵۵۰ دستگاه امنیت ارتباطی (COMSEC) را به سرعت مستقر کرد. همچنین آژانس در سال ۲۰۲۳، بیش از ۲۳۴ هزار محصول آشکارساز دستکاری (Tamper-indicationg) را در سراسر جهان ارائه کرد. محصولات آشکارساز دستکاری جهت جلوگیری از دستکاری شدنِ تجهیزات رمزنگاری و محتوای طبقه‌بندی شده در زمان حمل و نقل و انتقال در نقاط مختلف جهان استفاده می‌شود. همچنین این محصولات می‌توانند به شناسایی پسینیِ دستکاری‌ها کمک کنند.

در سال گذشته، آژانس امنیت ملی به پشتیبانی از ۶۱ مشتری مختلف برای عملیات‌های حساس ادامه داد. این مشتری‌ها شامل فرماندهی هند و اقیانوس آرام ایالات متحده، فرماندهی اروپای ایالات متحده، ستاد مشترک ارتش، فرماندهی ترابری ایالات متحده، سازمان ملی هوانوردی و فضا (ناسا)، آژانس فدرال مدیریت اضطراری و بسیاری دیگر از نهادها و سازمان‌ها هستند.

آژانس در بیش از ۲۰ تمرین سایبری و جلسات تبادل فنی شرکت کرد که منجر به تهیه ۷ گزارش ارزیابی آسیب‌پذیری همراه با طرح‌های رسیدگی و توصیه‌های امنیتی مهندسی شد. آژانس به ارائه راهنمایی جهت توسعه راهبردهای نظارت دفاعی برای کمک به بهبود آگاهی محیطیِ (Situational Awareness) پلتفرم‌های تسلیحاتی کمک می‌کند.

آژانس امنیت ملی همچنین با آژانس توسعه فضایی (SDA) در توسعه سند معماری فضایی خود همکاری کرد که به این آژانس کمک کرد تا ده ماهواره اول خود را با موفقیت پرتاب کند و فصل جدیدی را در تاریخ دفاع ملی رقم بزند.

علاوه بر این، آژانس امنیت ملی در سال گذشته در جلسات توجیهی و گفت‌وگوهای متعددی با رهبری و کارکنان فرماندهی فضایی ایالات متحده شرکت کرد. آژانس نظرات خود را در رابطه با ارائه خدمات امنیت سایبری و شیوه‌های تجاری مورد استفاده توسط مرکز همکاری امنیت سایبری را به اعضای ستاد فرماندهی فضایی جهت شروع و توسعه روابط با شرکای صنعتی ارائه کرد. فرماندهی فضایی نیز گزارشی از روند توسعه روابط تجاری این فرماندهی ارائه کردند. این امر به گسترش بیشتر مشارکت‌های مرکز همکاری امنیت سایبری با شرکای اصلی فرماندهی فضایی ایالات متحده کمک می‌نماید.

همانگونه که پیش از این توضیح داده شد، تمامی اعضای جامعه امنیت سایبری می‌بایست از هم‌اکنون برای نوسازی رمزنگاری‌ها و جلوگیری از تهدیدات کوانتومی برنامه‌ریزی کنند. در سال گذشته، آژانس امنیت ملی به تلاش‌های خود برای نوسازی رمزنگاری در تمامی قرارگاه‌های فرماندهی رزمی ایالات متحده ادامه داد. آژانس با همکاری بخش شبکه‌های اطلاعات دفاعیِ فرماندهی سایبری (JFHQ-DODIN) احتمال دسترسی دشمنان آمریکا به ارتباطات نیروهای جنگی و داده‌های حساس را کاهش می‌دهد.

برنامه نظارت مشترک بر امنیت ارتباطات (JCMA) به فعالیت‌های خود برای شناسایی نشت‌های اطلاعاتی که جزئیات عملیات‌های نظامی حساس و همچنین اطلاعات تردد‌های افراد مهم را که در ارتباطات طبقه‌بندی نشده یافت شده است ادامه داد. این نشت‌ها می‌تواند سطح خطرات را برای مأموریت ها و کارکنان افزایش دهد برنامه JCMA گزارش‌هایی را به قرارگاه‌های فرماندهی رزمی برای اقدام و انجام اصلاحات مربوط به این یافته‌ها ارسال کرد.

ارزیابی سامانه‌ها و ایجاد نقشه راه

انجام ارزیابی‌های امنیت سایبری بر روی برخی از مهم‌ترین سامانه‌های تسلیحاتی و فضایی کشور در تمام دامنه‌های جنگی به ما کمک می‌کند اطمینان حاصل کنیم که آن‌ها در برابر دشمنان سایبری آسیب‌پذیر نیستند. در سال گذشته آژانس امنیت ملی انجام این امر مهم را ادامه داد.

در سال ۲۰۲۳، آژانس نقشه راه رمزنگاری را برای تمام قرارگاه‌های فرماندهی رزمی ایالات متحده تکمیل کرد. آژانس امنیت ملی با حضور در جلسات هیأت هم‌کنش‌پذیری فرماندهی و کنترل بین فرماندهی‌های جنگی ایالات متحده، توانست مأموریت‌های حساسی را که در آن‌ها از روش‌های رمزنگاری منسوخ شده استفاده می‌شد را شناسایی کرده و با رویکردی عملیات‌محور نوسازی را صورت دهد. این رویکرد جدید با مبنا قرار دادن وضعیت هر یک از شرکای آژانس در زمینه رمزنگاری، مشخص می‌کند که رمزنگاری در سامانه‌های تسلیحاتی خاص چگونه باشد و سکوهای پشتیبانی عملیات چگونه عمل کنند. این اقدامات به دقت مشخص می‌کند که منابع چگونه بایستی برای رسیدن به این دو هدف به کار گرفته شوند: اول اطمینان پیدا کردن از ایمنی شرکای آژانس در برابر تهدیدات سایبری پیشرفته در تمام دامنه‌های جنگی و دوم هم‌کنش‌پذیریِ کامل با نیروهای نظامی ایالات متحده و سایر متحدان.

از رهگذر برنامه راهبردی امنیت سایبری وزارت دفاع، آژانس امنیت ملی در هماهنگی با فرماندهان ارشد وزارت دفاع و نیروهای نظامی ایالات متحده، فعالیت‌هایی را برای ارزیابی سیستم‌های آن‌ها، ارائه طرح‌هایی برای کاهش آسیب‌پذیری‌ها، نوسازی روش‌های رمزنگاری و رصد سامانه‌های آن‌ها صورت داد.

در آینده، آژانس قصد دارد از طریق همکاری مستمر با نیروهای نظامی برای انجام ارزیابی‌های بیشتر بر روی سیستم‌های اولویت‌دار، این فعالیت‌های خود را ارتقا دهد. آژانس همچنین از رزمایش‌های نظامی و جلسات طرح‌ریزی، پشتیبانی عملیاتی به عمل آورد.

آژانس امنیت ملی به کار خود در زمینه سازماندهی و اجرای ارزیابی ریسک‌های امنیت سایبری درباره حیاتی ترین سیستم‌های وزارت دفاع ادامه می‌دهد و این نهاد را در افزایش آمادگی‌ها و توانمندی‌ها برای مواجهه با تهدیدات سایبری چالش‌برانگیز یاری می‌دهد. در سال گذشته، آژانس امنیت ملی بررسی‌های اعتماد صفر (Zero Trust) و نقشه‌های راه پیاده‌سازی دو سامانه حساس را برای نیروی دریایی و نیروی هوایی عرضه کرد. این محصولات در حقیقت حاصل همکاری پایدار با نیروی دریایی و نیروی هوایی در طول سال گذشته بود.

کمک به هم‌کنش‌پذیری مأموریت‌ها

آژانس در سال گذشته نیز نماینده آمریکا در گروه ایمنی اطلاعات و دفاع سایبری ناتو بود. آژانس در این گروه به تقویت روابط با کشورهای شریک ادامه داد و تمرکز خود را بر نوسازی پلتفرم‌ها و تجهیزات با هدف کمک به هم‌کنش‌پذیری (Interoperability) مأموریت‌ها قرار داده بود. هم‌زمان با اقدام ایالات متحده برای نوسازی روش‌های رمزنگاری، آژانس با به اشتراک گذاشتن منطق رمزنگاری پیشرفته به شرکای توانمند عضو ناتو به نوسازی مجموعه پیمان ناتو کمک کرد. در سال گذشته آژانس بر اقدام سازمان ملی استاندارد (NIST) برای توسعه رمزنگاری مقاوم در برابر کوانتوم تأکید داشت. گروه دفاع سایبری ناتو راهنمایی‌های فنی لازم را برای به اشتراک گذاشتن اطلاعات بین کشورهای عضو ناتو فراهم کرد تا ایمنی شبکه‌های حساس را در برابر تهدیدات سایبری پیشرفته ارتقا بخشد.

ارتقای امنیت سایبری در حوزه فرماندهی، کنترل و ارتباطات هسته‌ای

در سال ۲۰۲۳ آژانس با همکاری سایر سازمان‌های زیرمجموعه وزارت دفاع در جهت پیشگیری و پاکسازی تهدیدات سایبری که متوجه سامانه‌های کنترل و فرماندهی هسته‌ای هستند اقداماتی انجام داد. این اقدامات با هدف تقویت همکاری‌ها صورت گرفت؛ همکاری‌هایی که به گسترش امنیت سایبری و بهره‌گیری از رویکردهای خلاقانه کمک خواهد کرد.

آژانس در پی همکاری‌های فرماندهی استراتژیک ایالات متحده (STRATCOM) نمونه‌ای از ابزاری را توسعه داد که امکان اشراف دقیق را بر سامانه‌های فرماندهی، کنترل و ارتباطات هسته‌ای (NC3) می‌دهد. این ابزار از حسگرها، ابزارهای رصد و تصویرسازی‌ها برای این هدف بهره می‌برد. آژانس به جمع‌آوری کلان داده‌ها (Big Data) که از آن‌ها برای شکل‌گیری تصمیمات و مقاوم‌سازی سیستم‌ها و حذف تهدیدات استفاده می‌شود، ادامه خواهد داد.

همچنین آژانس با برقراری روابط همکارانه جدید و تقویت روابط موجود خود ارزیابی‌های خود از برنامه امنیت سایبری راهبردی NC3 را ارائه کرد. این ارزیابی‌ها با هدف شناسایی مخاطرات امنیت سایبری، ارائه برنامه‌های مقابله‌ای و ارائه توصیه‌های دفاعی برای سامانه‌های در حال استفاده صورت گرفت. در سال گذشته امنیت پشتیبانی عملیاتی از رزمایش‌های انجام شده توانست نمونه‌هایی واقعی از شیوه پیشگیری و پاکسازی تهدیدات علیه سامانه‌های تسلیحاتی و فضایی را برای سازمان‌های همکار در زیرمجموعه وزارت دفاع فراهم آورد.

ایمن‌سازی سامانه‌های امنیت ملی با ابزارهای تجاری

برنامه آژانس امنیت ملی با عنوان برنامه ابزارهای تجاری برای سامانه‌های طبقه‌بندی شده (Commercial Solutions for Classified) یا به اختصار CSfC مشتریان را قادر می‌سازد را ابزارهای تجاری را برای محافظت از اطلاعات طبقه‌بندی شده لایه‌بندی کنند. بسته‌های پیشنهادی CSfC رویکردی چابک را برای نیروهای نظامی ایالات متحده، فرماندهی‌های رزمی و سایر نهادهای فدرال فراهم می‌سازد تا از سامانه‌های امنیت ملی خود دفاع کنند.

برنامه CSfC به مشتریان این امکان را می‌دهد که با استفاده از ابزارهای تجاری تائید شده از سوی آژانس، به سرعت از راه‌حل‌های امن برای طیف گسترده‌ای از کاربردها استفاده کنند. این کاربردهای عملی نه‌تنها در داخل و بین مجموعه‌های ایمن بلکه همچنین برای شرایطی است که بنا به اقتضای مأموریت‌ها نیاز به کارهایی خارج از محیط‌های کاری استاندارد است. در سال ۲۰۲۳ CSfC کار بهبود و ارتقای بسته ابزارهای عمومی و تجاری خود را ادامه داد.

همچنین آژانس امنیت ملی برای مشتریانی نظیر اف‌بی‌آی و سایر سیستم‌های حساس، ارزیابی‌های ایمنی را در خصوص ابزارهای عملیاتی شده ارائه می‌دهد. برنامه CSfC برای چهار مشتری گواهی‌های CSfC یک ارزیابی میدانی انجام داد که در آن ابزارهای عملیاتی شده با ابزارهای تائید شده آژانس مورد مقایسه قرار گرفته و ایمنی آن‌ها مورد بررسی قرار گرفت. آژانس اطمینان حاصل کرد که ویژگی‌های فنی، رصد و مدیریت در راستای ملزومات CSfC باشد. این کار فرصتی را برای اشتراک دوجانبه اطلاعات و فناوری فراهم می‌کند. آژانس برنامه‌ریزی می‌کند که چنین ارزیابی‌هایی را در آینده نیز ادامه دهد.

پژوهش در زمینه راهکارهای امنیت سایبری

آزمایشـگاه تحقیقات پیشرفته امنیت سایبری NSA از طریق مشارکت جدی و موفقیت‌آمیز با دانشگاه‌ها، آزمایشگاه‌های تحقیقاتی وابسته به دولت فدرال و بخش خصوصی، همچنان در خط مقدم حفاظت و ایمن سـازی اکوسیسـتم سایبری مشـغول فعالیت اسـت. آژانس امنیت ملی جایگاهی منحصر به فرد در ارائه دیدگاه‌های کارشـناسی تخصصی در تراز جهانی قرار دارد تا از این رهگذر از تلاش‌های تمامی بخش‌های دولت در راسـتای تضمین مزیت پایدار ایالات متحده در زمینه هوش مصنوعی و یادگیری ماشینی حفاظت نماید. دانشمندان، مهندسان و رهبران فکری آژانس امنیت ملی سال‌ها تحقیقات، مهارت‌ها و توانمندی‌های خود را در حوزه علوم داده (Data Science) به پیش برده‌اند و تخصص ما در این موضوع باعث می‌شـود آژانس در توسـعه، یکپارچه‌سـازی و بهره‌گیری از ظرفیت‌های هوش مصنوعی در سامانه‌های امنیت ملی و مجموعه صنایع دفاعی مورد مراجعه و استفاده شرکا قرار گیرد.

دیگـر پیشـرفت‌های اخیر در زمینـه تحقیقات حوزه امنیت سـایبری عبارت‌اند از:

- تقویت استانداردهای امنیت سایبری در فناوری‌های آتی که برای کشـور نقشی حیاتی دارند، مانند پروژه مشـارکت نسل سوم که به عنوان نهاد اصلی تعیین استاندارد 5G عمل می‌کند.
- ارائه راهنمایی‌های اساسی در زمینه زنجیره تأمین برای مدافعان شـبکه‌های سـامانه‌های امنیت ملی و مجموعه صنایـع دفاعی، تضمین یکپارچگی دسـتگاه‌هایی مانند رایانه‌های رومیزی، سـرورها و لپ‌تاپ‌های دخیل در تمام فعالیت‌های تدارکاتی مرتبط با تشکیلات مذکور.
- به سرانجام رساندن آخرین نسخه از برنامه علوم امنیت NSA که از تحقیقات بنیادین در حوزه امنیت سایبری در دانشگاه‌ها حمایت می‌کنـد. ایـن برنامه تحقیقات در زمینه علوم روز و فناوری‌های نوظهور را ترویج می‌کند. نسخه بعدی این برنامه نیز که شامل حمایت از پروژه‌های جدید در هفت دانشگاه مختلف می‌شود آغاز شد. برنامه علوم امنیت از همکاری دانشگاه‌ها، صنعت و دولت برای ارتقای امنیت سایبری از رهگذر دیدگاه‌های علمی استقبال می‌کند.
- توسـعه دوره‌های آموزشی نیروی سـایبری که برای توانمندسـازی نسـل آتی متخصصان حوزه سایبری با مهارت‌های پیشرفته برای ارزیابی آسیب‌پذیری‌های نرم‌افزار و حفاظت از دارایی‌های سایبری ملی ما طراحی شده است.

پرورش نسل فعلی و آتی متخصصان سایبری

توانمندسازی نیروی انسانی حوزه سایبری

آژانس امنیت ملی با پشتیبانی دفتر مدیر ملی سایبری (National Cyber Director) و در همکاری با سایر سازمان‌های دولت فدرال، پیش‌نویس و انتشار نخستین استراتژی ملی تربیت نیروی انسانی سایبری را تهیه کرد که توسط دولت کنونی در ماه جولای به تصویب رسید. این استراتژی با دیدگاهی متمرکز بر افراد تهیه شد تا پشتیبان سند استراتژی ملی امنیت سایبری باشد که رئیس جمهور بایدن در ماه مارس امضا کرد. این استراتژی دارای چهار رکن کلیدی است:

- آموزش مهارت‌های اساسی سایبری به تمام مردم آمریکا
- ایجاد تحول در حوزه آموزش سایبری
- گسترش و توانمندسازی نیروی انسانی حوزه سایبری
- توانمندسازی نیروی انسانی سایبری فعال در دولت فدرال

این سند پس از مشورت با بخش صنعت، دانشگاه‌ها، سازمان‌های غیرانتفاعی [اندیشکده‌ها] و شرکای دولتی تدوین شده است. آژانس امنیت ملی در تهیه این استراتژی همکاری کرده و در کارگروه‌های کاخ سفید با تمرکز بر تلاش‌ها در زمینه آموزش سایبری و نیروی انسانی حوزه سایبریِ دولت فدرال مشارکت نمود. تعهدات آژانس امنیت ملی شامل یک پروژه آزمایشی برای کمک به توسعه «کلینیک‌های سایبری» در سراسر کشور است که از شهرها و دولت‌های محلی که راه دیگری برای دسترسی به کمک در زمینه برنامه‌ریزی و ارزیابی خطرات حوزه سایبری ندارند حمایت کند. این کلینیک‌ها همچنین فرصتی را برای بیش از ۲۰۰ دانش‌آموز فراهم می‌کنند تا در یک محیط آموزشی تحت نظارت، قابلیت‌های خود را توسعه‌دهند.

توجه به استخدام زنان در حوزه امنیت سایبری

مرکز همکاری امنیت سایبری آژانس امنیت ملی، ائتلافی را با شرکای دانشگاهی، صنعتی و دولتی رهبری می‌کند تا زنان بیشتری را به اشتغال در حوزه امنیت سایبری تشویق کنند. به دنبال آزمایش موفق سال گذشته زنان مشغول در حوزه امنیت سایبری، پنج مدرسه جدید و بیست دانشجوی مشتاق در رویداد زنان مشغول در امنیت سایبری ۲۰۲۳ که به میزبانی مرکز همکاری امنیت سایبری برگزار شد، شرکت کردند. برنامه مذکور، رویدادی یک هفته‌ای برای تجربه یادگیری همه‌جانبه است که به دانشجویان اجازه می‌دهد با برخی از متخصصان برتر حوزه امنیت سایبری آژانس و فرماندهی سایبری ایالات متحده همکاری کنند و آموزش ببینند. شرکت‌کنندگان در این رویداد توسط اساتید مربوطه خود نامزد شدند که از آموزشگاه‌هایی نظیر یک کالج اجتماعی با دوره‌های دوساله، یک کالج و دانشگاه با پیش‌زمینه تاریخی سیاه‌پوست، یک مؤسسه خدمات اجتماعی مربوط به لاتین‌تبارها و یک دانشگاه دولتی با دوره‌های ۴ ساله، در این رویداد شرکت کردند. دانشجویان با مأموریت آژانس امنیت ملی در زمینه امنیت سایبری آشنا شدند و بسیاری از آن‌ها به عنوان «سفیران» آژانس امنیت ملی که در سطح پردیس‌های دانشگاهی‌شان از خدمات دولتی دفاع می‌کنند، به آموزشگاه‌های خود بازگشتند.

همکاری با دانشگاه‌ها

آژانس امنیت ملی به اجرای راهبرد دانشگاهی امنیت سایبری خود برای الهام بخشیدن به جنگجویان سایبری آتی خود از رهگذر ابتکاراتی مانند موارد ذیل ادامه می‌دهد:

چالش رمزگشایی آژانس (Codebreaker Challenge) به دانشجویانی که در دانشگاه‌های آمریکا تحصیل می‌کنند، این فرصت را ارائه می‌دهد تا مهارت‌های سایبری خود را تقویت کرده و در سناریوهای واقعی مأموریت‌محورِ آژانس امنیت ملی کسب تجربه کنند. تا ۲۱ دسامبر، دانشجویان در حال کار بر روی تفسیر و کشف یک سیگنال ناشناخته بودند که توسط گارد ساحلی ایالات متحده شناسایی شده است. به دانشجویان مجموعه‌ای از ۹ کار پیچیده‌تر نیز ارائه می‌شود تا آنچه که سیگنال را تولید می‌کند، مکان‌یابی کرده و به تجزیه و تحلیل آن بپردازند، یک عملیات جمع‌آوری فعال که توسط یک سرور متخاصم انجام می‌شود، را کشف کنند و سرور متخاصم را با هدف متوقف کردن دستگاه جمع‌آوری کننده، مورد حمله قرار دهند.

برنامه نسل سایبری (GenCyber Program) آموزش‌های مربوط به امنیت سایبری را در تمام طول سال به دانش‌آموزان و معلمان پایه متوسطه ارائه می‌کند. این برنامه رقابتی یک رویداد سالانه است که از طریق یک موسسه دانشگاهی در مؤسسات آموزشی و مؤسسات عام‌المنفعه و غیرانتفاعی برگزار می‌شود. متقاضیان می‌توانند برای چهار نوع برنامه درخواست ارائه کنند: ویژه دانش‌آموز، ویژه معلم، ترکیبی و زبان دانش‌آموز. در سال ۲۰۲۳، ۱۶۰ برنامه در ۴۷ ایالت به علاوه منطقه کلمبیا (دی‌سی) و پورتوریکو تأمین مالی شد که در آن‌ها حدود ۵ هزار و ۳۰۰ دانش‌آموز و معلم تحت آموزش قرار گرفتند. آژانس امنیت ملی و بنیاد ملی علوم (NSF) این امکان را برای دانش‌آموزان و معلمان فراهم کردند.

رزمایش سایبری آژانس امنیت ملی (NSA Cyber Exercise) جنگجویان و رهبران آینده‌ی سایبری در بخش‌های نظامی و غیرنظامی را با آزمودن مهارت‌های امنیت سایبری، کار تیمی،برنامه‌ریزی،

ارتباطات و تصمیم‌گیری‌شان، پرورش می‌دهد. برنامه مذکور، یک رویداد سالانه رقابتی در حوزه سایبری است که به طور ویژه برای دانشکده‌های نظامی هر یک از نیروها و کالج‌های نظامی اصلی ایالات متحده و شرکت‌کنندگان حرفه‌ای برنامه توانمندسازی آژانس طراحی شده است.

جایزه رویداد تمرین‌های حوزه سایبری آژانس امنیت ملی در سال ۲۰۲۳ به نیروی هوایی ایالات متحده اعطا شد.

برنامه تور تجربی آژانس امنیت ملی امکان برگزاری تورهای چهار تا شش هفته‌ای فرماندهی سایبری را برای نزدیک به ۲۰۰ نفر از اعضای دانشکده‌های نظامی، کالج‌های نظامی اصلی و اعضای منتخب سپاه آموزش افسران ذخیره (ROTC) فراهم می‌کند.

در این تورها هم تجربیات طبقه‌بندی شده و هم طبقه‌بندی نشده به شرکت‌کنندگان ارائه می‌شود. از آنجایی که شرکت‌کنندگان می‌بایست برای بر عهده گرفتن نقش‌های رهبری آماده شوند، برای آن‌ها این امکان فراهم می‌شود تا به مأموریتشان شکل دهند.

توانمندسازی نیروی انسانی حوزه سایبری

آژانس امنیت ملی با هدف ارتقای مشاغل حوزه امنیت سایبری در تمامی سطوح آموزشی سرمایه گذاری کرده است. دانشگاه ملی رمزنگاری (مستقر در آژانس) مراکز ملی تعالی آکادمیک در حوزه امنیت سایبری (NCAE-C) را اداره می‌کند. این اقدام به دنبال طراحی و مدیریت یک برنامه آموزشی در زمینه امنیت سایبری با همکاری کالج های محلی، کالج‌ها و دانشگاه‌ها است و:

- استانداردهایی را برای برنامه درسی امنیت سایبری و تعالی آکادمیک ایجاد می‌کند.
- شامل توسعه شایستگی دانشجویان و اساتید می‌شود.
- برای فعالیت‌های اطلاع‌رسانی و رهبری جامعه در زمینه توسعه حرفه‌ای، ارزش قائل می‌شود.
- اقدامات امنیت سایبری را در هر موسسه و در سراسر رشته‌های دانشگاهی یکپارچه می‌سازد.
- فعالانه در ارائه راه‌حل‌ها برای چالش‌های پیش روی آموزش امنیت سایبری مشارکت می‌کند.

بیش از ۴۰۰ مرکز آموزشی نشان برنامه NCAE-C را در حوزه‌های سایبری، دفاع سایبری و پژوهش های سایبری دریافت کرده‌اند.