مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گزارش سریع
چهل و نهم

استراتژی امنیت ملی سایبری در ژاپن

National Cyber Security Strategy in Japan

بسم الله الرحمن الرحیم

گزارش سریع

گزارش شماره ۴۹
شهریور ۱۴۰۱

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

استراتژی امنیت سایبری ژاپن

گزارش سریع که با عنوان Rapid Report شناخته می‌شود، نوعی گزارش کوتاه است که صرفاً برای اطلاع کلی از موضوع یا پدیده‌ای خاص در بازه زمانی محدود تهیه می‌شود. هدف عمده چنین گزارش‌هایی ایجاد تصویری اجمالی برای آشنایی ابتدایی سیاست‌گذاران و برنامه‌ریزان در موضوعات مورد علاقه آنان است.

تهیه شده در پژوهشگاه فضای مجازی
(گروه مطالعات بین‌الملل)

ترجمه: دکتر آیت حسینی
ناظر: عباس قنبری باغستان

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶غربی، پلاک ۲۰
تلفن: ۸۶۱۵۱۰۶۱-۰۲۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سیدابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

چکیده

چکیده

۱.۱. تغییر پارادایمی ناشی از فضای سایبری

فضـای سـایبری کـه اینترنت بخش مرکزی پلتفرم آن را تشـکیل می‌دهد، از رشـد سـریع تکنولـوژی دیجیتال مبتنی بـر دانش علمی مدرن برخاسـته و به سـبب طرح‌های مسـتقل نهادهای ذی‌نفـع متعدد[۱] که بسـیاری از آن‌ها در بخـش خصوصـی فعالیت می‌کنند، در مقیاس جهانی رشـد و گسـترش یافت.

در نتیجـه رشـد فضـای سـایبری، می‌تـوان اطلاعـات و داده‌هـا را کـه هـم از نظـر مقـدار و هـم از نظـر کیفیـت گوناگونی بالایـی دارند، فراتـر از مرزهای ملـی و فـارغ از تأثیـر زمان و مـکان، آزادانه خلـق کنیم، به‌اشـتراک بگذاریم و تحلیـل کنیـم. در نتیجـه عاملان فضـای سـایبری می‌توانند به طـور بالقوه به واسـطه تعامـل بـا دیگر عامـلان ارزش جدید ایجـاد کنند.

در نتیجـه ایـن خصوصیـات، فضـای سـایبری مکانـی اسـت کـه می‌تـوان در آن مالکیـت معنـوی، از جملـه نوآوری‌های تکنولوژیکـی و الگوهای تجاری جدیـد ایجـاد کـرد و همچنـان پلتفرمـی برای رشـد پایـدار جامعـه اقتصادی باقـی خواهـد مانـد. ایـن فضـا همچنیـن از آزادی‌خواهی، دموکراسـی و رشـد فرهنگـی حمایـت می‌کنـد و عـلاوه بـر این، جایی اسـت کـه مـردم می‌توانند

۱. طبق تعریف در ماده‌ی ۱۶ قانون اساسی امنیت سایبری، این نهادهای ذی‌نفع متعدد شامل «حکومت مرکزی، حکومت‌های محلی، اپراتورهای زیرساخت اطلاعات مهم و نهادهای تجاری مرتبط با فضای سایبری» می‌شوند. ماده ۷ همین قانون نهادهای تجاری مرتبط با فضای سایبری را اینگونه تعریف می‌کند: «نهادهای تجاری مرتبط با فضای سایبری (اشاره به نهادهایی که مشغول تجارت مرتبط با نگهداری از اینترنت و دیگر شبکه‌های اطلاعات و ارتباطات از راه دور پیشرفته و استفاده از تکنولوژی‌های اطلاعات و ارتباطات از راه دور هستند یا در تجارت مرتبط با امنیت سایبری فعالیت می‌کنند؛ همین تعریف در ادامه نیز صادق است).»

از خلق و نوآوری استفاده کنند تا فعالیت‌هایشان را به‌طور چشمگیری گسترش دهند.[1] به عبارت دیگر، فضای سایبری «جبهه‌ای برای ایجاد ارزش بی‌نهایت» است. ژاپن از هر ابزاری که در دسترس داشته باشد استفاده می‌کند تا طرح‌های امنیت سایبری را اجرا کند و از باقی ماندن فضای سایبری در این وضعیت اطمینان حاصل کند.

در آینده نزدیک، انتظار می‌رود رشد بیشتر علوم کامپیوتر که فضای سایبری پیش‌نیاز آن است، مثل هوش مصنوعی (که از این به بعد به آن AI گفته می‌شود) و غیره، به خلق محصولات و خدمات جدید ختم شود. ظهور محصولات و خدمات جدید با تغییر رفتارها و محیط زندگی روزانه افراد آگاهی آن‌ها را تغییر می‌دهد و این مسئله خود منجر به تغییر نظام‌های اجتماعی و زیرساخت‌های صنعتی می‌شود که شامل محصولات، الگوها، سازمان‌ها و غیره فعلی می‌شود. همزمان با اینکه نسل بشر از جامعه شکارچی، جامعه کشاورزی، جامعه‌ی صنعتی و جامعه اطلاعات به «نسخه‌ی ۵.۰ جامعه»[2] تغییر پارادایم را تجربه می‌کند، ضروری است که همزمان با در نظر گرفتن این تغییرات، تصویری از آینده امنیت سایبری ارائه دهیم.

۲.۱. تغییرات شرایط از سال ۲۰۱۵

استراتژی امنیت سایبری (که از این به بعد به آن «استراتژی ۲۰۱۵» گفته می‌شود) در سپتامبر ۲۰۱۵ طبق قانون اساسی امنیت سایبری[3] (که از این به بعد به آن «قانون اساسی» گفته می‌شود) پس از مشورت با مرکز فرماندهی استراتژیک امنیت سایبری (که از این به بعد به آن «مرکز

۱. در گزارش استراتژی امنیت سایبری (سپتامبر ۲۰۱۵)، تأثیرات این خصوصیات روی جامعه با انفجار دانش به سبب اختراع چاپ مسطح گوتنبرگ است.

۲. نسخه‌ی ۵.۰ جامعه مرحله‌ی پنجم تاریخ بشر پس از جامعه شکارچی، جامعه کشاورزی، جامعه صنعتی و جامعه اطلاعات است. نسخه ۵.۰ جامعه، جامعه‌ای است که در آن ارزش جدید و خدمات جدید به طور مداوم ایجاد می‌شود و به مردم جامعه ثروت می‌رساند. (منبع: استراتژی رشد ۲۰۱۷ (تصمیم کابینه در ۹ ژوئن ۲۰۱۷))

۳. این قانون اساسی در تاریخ ۶ نوامبر ۲۰۱۴ به تصویب رسید. این قانون برای مفهوم امنیت سایبری موقعیتی قانونی ایجاد کرد و مسئولیت‌های نهادهای ذی‌نفع متعدد را مشخص کرد.

فرماندهی» گفته می‌شود) توسط کابینه به تصویب رسید و به عنوان سیاستی بنیادی در قبال تمهیدات مرتبط با امنیت سایبری در بازه‌ای سه ساله ایجاد شد.

پس از تنظیم استراتژی ۲۰۱۵، شالوده قانونی برای استفاده از داده‌ها فراهم شد، از جمله قانون اساسی پیشرفت استفاده بخش دولتی و خصوصی از داده‌ها[۱] و قانون متمم حفاظت از اطلاعات شخصی[۲] و غیره. دولت نیز سیاستی مبنی بر حقیقت‌بخشیدن به جامعه‌ای انسان‌محور[۳] را پیش گرفته است که هم به توسعه اقتصادی و هم به حل مشکلات اجتماعی از طریق سطح بالای ادغام فضای سایبری با فضای واقعی دست خواهد یافت. این شرایط، مقادیر عظیمی از داده‌ها که توسط سنسورها و ابزارها در فضای واقعی تولید می‌شوند، در حال حاضر در فضای سایبری جمع‌آوری و آنالیز می‌شوند. به‌علاوه، دیده می‌شود که تهیه محصولات و خدمات جدید در فضای واقعی که از طریق استفاده از داده‌ها تولید ارزش می‌کنند، به صورت دوره‌ای رو به ظهور است و در حوزه‌های مختلف روبه‌رشد است. دیگر فضای سایبری و فضای واقعی دو موجودیت مستقل نیستند، بلکه موجودیت‌هایی با تعامل متقابل‌اند، به طوری که دیگر نمی‌توان آن‌ها را جدا از هم دانست. در نتیجه، این دو فضا را باید یک موجودیت زنده که به طور مداوم در حال تکامل است دانست.

تلفیق فضای سایبری و فضای واقعی به طور چشمگیری پتانسیل حصول فراوانی در جامعه را افزایش می‌دهد. همزمان، فرصت عاملان مخرب برای سوءاستفاده از فضای سایبری را نیز افزایش می‌دهد. انتظار می‌رود خطر ضرر اقتصادی و اجتماعی یا ضربه به فضای واقعی گسترش

۱. این قانون در تاریخ ۷ دسامبر ۲۰۱۶ تصویب شد. این قانون اصول بنیادین تشویق به استفاده بخش خصوصی از داده‌ها را تصریح می‌کند.
۲. این قانون اصلاح‌شده در تاریخ ۳ نوامبر ۲۰۱۵ به تصویب رسید و در تاریخ ۳۰ مه ۲۰۱۷ به طور کامل اجرا شد. این قانون برای تشویق گمنام‌سازی به عنوان پیش‌نیاز برای استفاده از اطلاعات شخصی تنظیم شده است.
۳. محتویات نسخه ۵.۰ جامعه (منبع: استراتژی جامع برای علم، تکنولوژی و نوآوری ۲۰۱۷ (تصمیم کابینه در تاریخ ۲ ژوئن ۲۰۱۷)، سرمایه‌گذاری برای استراتژی آینده (تصمیم کابینه در تاریخ ۹ ژوئن ۲۰۱۷).)

یافته و سریعاً شتاب پیدا کند.

تحت این شرایط، امنیت فضای سایبری که اساس جامعه اقتصادی است، باید تأمین شود و به طور همزمان باید از تکامل و توسعه پایدار و مستقل آن نیز اطمینان حاصل کرد تا به پیشرفت و ثروت پایدار در جامعه دست یابیم. اخیراً در برخی کشورها شایع شده است که در مقابل تهدیدات سایبری روی مدیریت و کنترل حکومت از جایگاه سلطه تأکید می‌کنند اما تقویت مدیریت و کنترل فضای سایبری توسط حکومت منجر به توقف احتمال توسعه مستقل و پایدار می‌شود. از این رو، باید به فضای سایبری امروز که از طریق طرح‌های مستقل تمام نهادهای ذی‌نفع توسعه یافته است، احترام گذاشت و با طرح‌های مبتنی بر همکاری و اتحاد با نهادهای ذی‌نفع امنیت سایبری را تأمین کرد.[1]

بر این اساس، ژاپن با در نظر داشتن موقعیت مورد نظر برای سال ۲۰۲۰ و پس از آن و در نظر گرفتن میزبانی رویدادهای بین‌المللی بزرگی مثل بازی‌های المپیک سی و دو و پارالمپیک ۲۰۲۰ در توکیو (از این به بعد به آن‌ها «بازی‌های ۲۰۲۰ توکیو» گفته می‌شود) از هیچ تلاشی برای تمهیدات مربوط به امنیت سایبری به واسطه شفاف‌سازی طرح اساسی امنیت سایبری، شناسایی مشکلات جدید که نیاز به بررسی دارند و اجرای فوری این تمهیدات مضایقه نخواهد کرد.

این استراتژی موضع اساسی و رویکرد ژاپن در قبال امنیت سایبری مبنی بر حرکت رو به جلو را نشان می‌دهد و به وضوح اهداف و سیاست‌های داخلی و بین‌المللی ژاپن برای پیاده‌سازی تمهیدات مختلف در سه سال آینده را مشخص می‌کند که شالوده‌ای برای درک و اقدامات مشترک ایجاد می‌کند.

۱.«اهداف توسعه پایدار» که در همایش سازمان ملل متحد در سپتامبر ۲۰۱۵ مطرح شد ۱۷ هدف را برای رسیدن به جامعه جهانی پایدار و جامعه‌ای که در آن «هیچ‌کس جا نمی‌ماند» تعیین کرد. نکات متعددی بین سیاست طرح‌های امنیت سایبری در اینجا و اهداف توسعه پایدار مشترک است، از جمله تلاش برای رسیدن به توسعه پایدار و طرح‌هایی مبتنی بر همکاری و اتحاد بین نهادهای ذی‌نفع.

بخش اول

بخش اول

درک فضای سایبری

دانش، تکنولوژی و خدمات فضای سایبری، از جمله AI، اینترنت اشیا[1]، فین‌تک،[2] رباتیک، پرینترهای سه‌بعدی[3] و AR/VR [4] به‌مرور جای خود را در جامعه پیدا کرده‌اند و به نوآوری‌هایی ختم می‌شوند که ساختارهای موجود فعالیت‌های اجتماعی و اقتصادی و زندگی روزمره مردم ژاپن را تغییر می‌دهد. این تغییرات منجر به پیشرفت تلفیق فضای سایبری و فضای واقعی می‌شود. [5]

برای خلق این استراتژی، درکی دقیق از فواید فضای سایبری و وضعیت تهدیدات این فضا باید پیش‌نیاز درنظر گرفته شود. به علاوه برای سود بردن از فواید دانش، تکنولوژی و خدمات فضای سایبری، ضروری است که عدم‌قطعیت‌های نهفته در آن را که همیشه وجود دارد کنترل کنیم. زمانی که چنین کنترلی ممکن نباشد، این امکان وجود دارد،که تهدیدات مرتبط با فضای سایبری به‌سرعت افزایش یابد.

1. IoT: Internet of Things

۲. ترکیبی از دو کلمه امور مالی (finance) و تکنولوژی. این عبارت به نوآوری‌های جدید خدمات مالی با استفاده از تکنولوژی‌های جدید مثل زنجیره بستکی، کلان‌داده و AI اشاره دارد که در ابزارهایی مانند تلفن‌های هوشمند و تبلت‌هایی که به‌سرعت در دسترس عموم قرار گرفته‌اند استفاده می‌شوند (منبع: Information and Communications in ۲۰۱۷ WHITE PAPER Japan).

۳. در مقایسه با پرینترهایی که تصویری مسطح (دوبعدی) را روی کاغذ چاپ می‌کنند، پرینترهای سه‌بعدی با استفاده از داده‌های سه‌بعدی از طراحی سه‌بعدی به کمک رایانه و تصویر سه‌بعدی تشکیل‌شده توسط کامپیوتر اشیا سه‌بعدی چاپ می‌کند (منبع: وبسایت اتحادیه تکنولوژی صنعتی چاپ سه‌بعدی ژاپن).

۴. مخفف واقعیت افزوده (Augmented Reality) و واقعیت مجازی (Virtual Reality)

۵. استراتژی ۲۰۱۵ بیان می‌کند که «اشیا فیزیکی و مردم در فضای واقعی با استفاده از جریان آزاد اطلاعات و ارتباطات دقیق داده‌ها در فضای سایبری به‌صورت چندلایه و بدون محدودیت‌های جسمی به یکدیگر متصل شده‌اند. با توجه به چنین ارتباطی، پدیده "جامعه اطلاعات به هم متصل و همگرا" در حال شکل‌گیری است که در آن فضای واقعی و فضای سایری به‌شدت در هم آمیخته‌اند.»

۱-۱- فواید فضای سایبری

تکنولوژی و خدمات درون فضای سایبری در حوزه‌های مختلف استفاده‌ای روتین پیدا کرده‌اند. انتظار می‌رود توسعه پایدار و مداوم فضای سایبری منجر به وفور نعمت برای انسان‌ها شود.

(۱) پیشرفت خدمات در فضای سایبری و به‌کارگیری آن‌ها در جامعه

تعداد کاربران اینترنت در ژاپن، همچون گسترش خود اینترنت در حال افزایش است.[۱] به‌علاوه از نظر ابزارها نیز نرخ مالکیت تلفن‌های هوشمند شخصی به طور چشمگیری افزایش یافته[۲] و نرخ استفاده از اینترنت نیز بالا رفته است.[۳] نسبت کاربران شبکه‌های اجتماعی نیز در حال افزایش است[۴] که در نتیجه آن حالا محیطی در فضای سایبری وجود دارد که برقراری ارتباط به راحتی ممکن می‌سازد.

افزایش به‌کارگیری خدمات فضای سایبری در جامعه نه فقط جریان آزاد اطلاعات[۵] را، بلکه تشکیل جوامعی گوناگون و به‌اشتراک‌گذاری اطلاعات را هم تشویق کرد.

در زمینه فعالیت‌های مالی نیز پیشرفت وجود داشته است، از جمله خرید اینترنتی، معامله سهام و بانکداری اینترنتی، در حالی که خدمات جدید حوزه فین‌تک و اقتصاد اشتراکی[۶] نیز به طور مرتب ظاهر می‌شوند و به نوآوری ختم می‌شوند. در استفاده از تکنولوژی اطلاعات و ارتباطات در

۱. نرخ نفوذ اینترنت بین عموم مردم (از ۸۲.۸٪ در پایان سال ۲۰۱۴ به ۸۳.۵٪ درصد در پایان سال ۲۰۱۶ رسیده است) (منبع: WHITE PAPER ۲۰۱۷ Information and Communications in Japan)

۲. نرخ مالکیت تلفن هوشمند شخصی (از ۴۴.۷٪ در پایان سال ۲۰۱۴ به ۵۶.۸٪ در پایان سال ۲۰۱۶ رسیده است) (منبع: WHITE PAPER ۲۰۱۷ Information and Communications in Japan)

۳. نرخ استفاده از اینترنت (از ۸۳.۰٪ در پایان سال ۲۰۱۵ به ۸۳.۵٪ در پایان سال ۲۰۱۶ رسیده است) (منبع: WHITE PAPER ۲۰۱۷ Information and Communications in Japan)

۴. نرخ خدمات شبکه‌های اجتماعی محبوب (لاین، فیسبوک، توییتر، میکسی، موبا‌گه، گری) (در مجموع) (از ۶۲.۳٪ در پایان سال...)

۵. ... به ۷۱.۲٪ در پایان سال ۲۰۱۶ رسیده است) (منبع: WHITE PAPER ۲۰۱۷ Information and Communications in Japan)

۶. فعالیت‌های احیای اقتصادی که در آن‌ها دارایی‌های شخصی‌ای که امکان استفاده بالقوه از آن‌ها وجود دارد برای استفاده دیگران از طریق پلتفرم‌های جفت‌سازی اینترنتی در دسترس قرار می‌گیرد. (منبع: WHITE PAPER ۲۰۱۷ Information and Communications in Japan)

زمینـه‌ی درمـان و مراقبـت، بیمه، آموزش و پـرورش و دیگر زمینه‌های مرتبط بـه مشـکلات اجتماعی از جملـه کاهش جمعیت افرادی که در سـن کارکردن قرار دارند و افزایش سـن جوامع محلی نیز پیشـرفت حاصل شـده اسـت.

(۲) تکامل سریع AI

اخیـراً از نظـر AI پیشـرفت زیـادی در علـوم کامپیوتـر و تحقیقات مربوط به یادگیری ماشـین حاصل شـده اسـت کـه نیاز به مقـدار زیـادی داده دارد و بـه رویکـرد جدیـد یادگیـری عمیق ختم می‌شـود. ظهـور یادگیـری عمیق به بهینه‌سـازی و افزایـش کیفیـت عملکردهـای فراوانی از فعالیت‌هـای اجتماعی و اقتصادی از جمله دقت در تشـخیص نقص در محصول، تشـخیص سـرطان، تصمیم‌گیـری در سـرمایه‌گذاری و ترجمـه شـتاب بخشـیده اسـت و کم‌کم از ایـن تکنولـوژی در حوزه‌هـای مختلـف صنعـت اسـتفاده می‌شـود. بـه همین طریـق، در زمینـه امنیـت سـایبری کم‌کـم از ایـن پتانسـیل AI در تمهیدات مختلفـی مانند تشـخیص خـودکار بدافزارها نیز اسـتفاده می‌شـود.

گفتـه می‌شـود تکامـل AI بـر پایـه یادگیـری عمیـق تغییراتـی را به‌وجود خواهد آورد که در دنیای ماشـین‌ها و رباتیک با انفجار کامبرین قابل مقایسـه اسـت.[۱] یادگیـری عمیـق بـه طراحـی اسـتخراج ویژگـی[۲] کـه در تفکیـک و تشـخیص اسـتفاده می‌شـود، یعنی عملکردی که پیش از این باید در یادگیری ماشـین اسـتاندارد توسـط انسـان صورت می‌گرفت، این امکان را بخشـید که بـه صـورت خودکار توسـط کامپیوتر صـورت بگیرد. این موضـوع گامی انقلابی بـرای AI بـه حسـاب می‌آیـد. گامـی کـه منجـر بـه دنیایـی خواهـد شـد که

۱. انفجار کامبرین (Cambrian explosion) پدیده‌ای است که به واسطه‌ی آن بین ۵۴۲ میلیون تا ۵۳۰ میلیون سال قبل راسته‌ی بسیاری از حیوانات امروزی به‌وجود آمدند. اندرو پارکر دیرینه‌شناس این نظریه را مطرح کرده است که ظهور قدرت بینایی باعث این انفجار شده است. یادگیری عمیق معادل همان قدرت بینایی برای AI است.یادگیری عمیق به AI این امکان را می‌دهد که پیش‌بینی کند در مرحله‌ی بعدی چه اتفاقی می‌افتد و طبق آن دست به عمل بزند. از این رو شاهد ظهور ماشین‌هایی با چشم خواهیم بود و احتمالاً معادل انفجار کامبرین در دنیای ماشین‌ها و رباتیک رخ خواهد داد. (منبع: مرکز فرماندهی احیای اقتصادی ژاپن، چهارمین کنفرانس انقلاب صنعتی برای تشویق توسعه‌ی منابع انسانی (همایش دوم) سند اول)

۲. بیان کمّی خصوصیات مهم که هنگام شناسایی یک شیء نیاز به توجه دارند. قبل از ظهور یادگیری عمیق، خصوصیات توسط انسان طراحی می‌شدند. اما یادگیری عمیق به کامپیوترها این امکان را می‌دهد که با استفاده از تشخیص تصویر و صدا، خود به خود استخراج ویژگی را انجام دهند. (منبع: WHITE PAPER ۲۰۱۷ Information and Communications in Japan)

در آن AI می‌تواند به‌صورت مستقل و بدون دخالت خلاقانه انسان، خروجی‌ای تولید کند که نتیجه‌اش آثار خلاقانه مثل موسیقی، نقاشی، رمان و خدمات خودانگیخته باشد (مثلاً نتایجی از تعیین، تصمیم‌گیری و پیشنهاد). به این احتمال نیز اشاره شده است که اگر AI حقی را ضایع کند یا منجر به حادثه‌ای بشود، چه کسی مسئول خواهد بود.[1]

این پیشرفت‌ها در AI به ظهور محصولات و خدماتی کاملاً جدید ختم خواهد شد و رفتار و محیط زندگی روزمره‌ی انسان‌ها را در آینده تغییر خواهد داد. این مسئله درک انسان از جهان را تغییر خواهد داد که انتظار می‌رود نظام‌های اجتماعی و ساختارهای صنعتی موجود را تغییر دهد.

(۳) توسعه اینترنت اشیا

کاهش اندازه، وزن و هزینه سنسورها به گسترش انفجاری اینترنت اشیا امکان بخشیده است. اینترنت اشیا یعنی همه‌چیز به شبکه متصل می‌شود. علاوه بر استفاده از چیزهایی مثل لوازم خانگی، خودروها، ربات‌ها و وسایل اندازه‌گیری هوشمند، کسب‌وکارها و خدمات جدید نیز برای استفاده از داده‌هایی که از ابزارهای دارای اینترنت اشیاء جمع‌آوری می‌شود، ایجاد شده‌اند.

به طور مشخص تلاش می‌شود که بهره‌وری تقویت شده و به ارزش افزودهبالایی در زمینه‌های دولت الکترونیک، شهرهای هوشمند، بخش تولید، خودروهای خودران، امور مالی، سلامتی و درمان و پرستاری دست یابیم[2] و

۱. «در آینده با این مشکل مواجه خواهیم شد که اگر دخالت کاربر (انسان) در خروجی محصولات AI کاهش یابد، آیا باز هم کاربران مسئول خواهند بود یا نه.» مرکز فرماندهی استراتژی مالکیت معنوی «کمیته‌ی بررسی مالکیت معنوی با توجه به دارایی‌های جدید مرتبط با داده (گزارش)» (مارس ۲۰۱۷)

۲. بیانیه تبدیل شدن به پیشرفته‌ترین کشور دیجیتال جهان / طرح ابتدایی برای پیشرفت بخش دولتی و خصوصی استفاده از داده‌ها (تصمیم کابینه در تاریخ ۱۵ ژوئن ۲۰۱۸) هشت زمینه اولویت‌مند تعریف می‌کند (مدیریت الکترونیک؛ سلامت، درمان و مراقبت پرستاری؛ گردشگری؛ امور مالی؛ کشاورزی، جنگل‌داری و ماهی‌گیری؛ تولید؛ زیرساخت‌ها، مدیریت فجایع و کاهش فجایع؛ و حمل‌ونقل) که انتظار می‌رود به حل مشکلاتی مانند (۱) احیاء اقتصادی و بازیابی سلامت مالی، (۲) احیاء منطقه‌ای و (۳) اطمینان از ایمنی و امنیت زندگی مردم از طریق استفاده از داده‌ها در بخش دولتی و خصوصی کمک کند.

انتظار می‌رود که استفاده از داده‌ها در زنجیره‌های تأمین مختلف[1] برای این زمینه‌ها پیشرفت داشته باشد. به‌علاوه، دراصطلاح نوآوری آزاد[2] نیز پیشرفت حاصل شده است که طی آن از طریق فضای سایبری بین چند زمینه همکاری شکل می‌گیرد و انتظار می‌رود سیر ظهور خدمات جدیدی که از طریق به‌اشتراک‌گذاری و تحلیل داده‌ها وفور نعمت بیشتری برای مردم به بار خواهد آورد، ادامه‌دار باشد.

۱-۲- تهدیدهای در حال افزایش در فضای سایبری

اگرچه تکنولوژی و خدمات AI و اینترنت اشیا ممکن است فواید زیادی برای مردم داشته باشند، نمی‌توان از این خطر نهفته چشم‌پوشی کرد که تأمین‌کنندگان چنین تکنولوژی و خدماتی توانایی کنترل آن‌ها را از دست داده و موجب خسارت یا صدمه اقتصادی و اجتماعی بی‌اندازه‌ای بشوند. با ادامه تلفیق فضای سایبری و فضای واقعی، احتمال وقوع چنین صدمه‌شدیدی با سرعت زیادی افزایش می‌یابد. به‌علاوه، فضای سایبری در قید زمان و مکان نیست و هر کسی از جمله عاملان مخرب، می‌تواند به‌راحتی از اطلاعات و تکنولوژی‌های ارتباطی جدید سوءاستفاده کند. علاوه بر اینکه عامل مخرب یا گروه‌های عاملان مخرب می‌توانند به راحتی داده‌ها و اطلاعات را کپی و پخش کنند، از جمله برنامه‌های حمله که در ذات تکنولوژی دیجیتال نهفته است، می‌توانند آزادانه از تکنولوژی‌هایی مانند AI و زنجیره بستکی نیز استفاده کنند.[3] به همین دلیل، مهاجمان از برتری نامتقارنی نسبت به مدافعان برخوردارند، و انتظار

۱. زنجیره تأمین به جریان کالا و اطلاعات در فعالیت‌های تجاری از بالادست به پایین‌دست، از دریافت و تنظیم سفارش بین تأمین‌کنندگان و تدارک مواد اولیه تا مدیریت انبار و تحویل محصولات اشاره دارد.

۲. نوآوری آزاد به استفاده عمدی و پیشگرانه از جریان منابع داخلی مانند تکنولوژی‌ها و ایده‌ها، درون و بیرون سازمان برای تشویق نوآوری داخلی و استفاده از نوآوری‌های داخلی حاصله بیرون از سازمان برای افزایش فرصت‌های بازار اشاره دارد.

۳. اشاره به تکنولوژی زنجیره بستکی (Blockchain). این تکنولوژی از ساختار داده‌ای استفاده می‌کند که در آن می‌توان با استفاده از امضای دیجیتال و نشانگر درهم‌سازی (Hash pointer) تغییرات را تشخیص داد. با ذخیره داده‌های مرتبط در گره‌های چندگانه سرتاسر شبکه، این تکنولوژی به دسترسی و یکپارچگی بالایی در داده‌ها دست پیدا می‌کند. (منبع: Japan Blockchain Association, "Blockchain Definition")

می‌رود این برتری به‌خصوص زمانی افزایش پیدا کند که ترکیب مدافعان به سیاست‌ها و سیستم‌های تکنولوژی موجود وابسته باشد.

با توجه به این شرایط، حمله‌هایی[1] که اینترنت اشیا، فین‌تک از جمله رمزارزها، زیرساخت‌های حیاتی و زنجیره‌های تأمین را هدف قرار می‌دهند، هم داخل ژاپن و هم خارج از ژاپن رخ داده‌اند و علاوه بر درزکردن متداول داده‌ها، موجب خسارت مالی مستقیم و وقفه در تجارت و خدمات نیز شدند و ایمنی و امنیت توسعه پایدار فعالیت‌های اجتماعی و اقتصادی و زندگی مردم را تهدید کردند. برخی از حوادث عظیم نیز مظنون به داشتن پشتیبانیِ دولتی بوده‌اند. این نگرانی نیز وجود دارد که اگر فضایی سایبری توسط کشوری از جایگاه بالاتر کنترل یا مدیریت شود، ممکن است اعتبار زیرساخت‌های اطلاعاتی نیز متزلزل شود.

عقیده عمومی بر این است که با ادامه تلفیق فضای سایبری با فضای واقعی، نگرانی در خصوص تلاش‌های بالقوه برای هدف‌قراردادن نقطه ضعف‌های اینترنت اشیا، زنجیره‌های تأمین و نوآوری آزاد و در خصوص وقوع رفتارهای غیرعمدی در این سیستم‌ها افزایش می‌یابد. انتظار می‌رود آسیب‌هایی جدی نه فقط در انتظار نهادهای دولتی و اپراتورهای زیرساخت‌های حیاتی باشد، بلکه در انتظار کسب‌وکارها و حتی افراد باشد.

(۱) تأثیرات عمده بر جامعه به‌موجب وقفه در کسب‌وکار، عملکردها و خدمات

وقتی در کسب‌وکارها، عملکردها و خدمات متعدد به خاطر وقفه در خدمات زیرساختی مهم یا رفتار غیرعمدی توسط دستگاه‌های اینترنت اشیا وقفه پیش بیاید، جامعه به‌شدت تحت تأثیر قرار می‌گیرد و این

۱. بانک بنگلادش هک شد که به انتقال غیرمجاز حدود ۸۱ میلیون دلار ختم شد. نوع جدیدی از بدافزار (میرای) در سپتامبر ۲۰۱۶ پیدا شد که دستگاه‌های دارای اینترنت اشیا را هدف قرار داد و تبدیل به بزرگترین حمله توزیع‌شده محروم‌سازی از خدمات (DDOS) در تاریخ شد. حمله‌ای سایبری نیز در ایستگاه ترانسفورمرهای شرکت برق ملی اوکراین در دسامبر ۲۰۱۶ رخ داد.

معضلات ممکن است تا جایی پیش بروند که تبدیل به مسئله امنیت ملی شوند. اگر تلفیق فضای سایبری و فضای واقعی حتی بیش از این ادامه داشته باشد، ممکن است احتمالاتی به وجود بیاید که ایمنی و امنیت مردم و ریشه‌های دموکراسی و کشور را تهدید کند، از جمله از کار انداختن عملکردهای جامعه و خطراتی در قبال زندگی و معیشت انسان‌ها و مردم.

(۲) کاهش رقابتی‌بودن به‌موجب از دست دادن یا درزکردن اطلاعات

با گسترش انفجاری اینترنت اشیا و افزایش دسترسی عمومی به داده‌ها، تعداد داده‌هایی که از داده‌ها استفاده می‌کنند افزایش خواهد یافت. استفاده از AI برای تحلیل داده‌ها نیز پیشرفت خواهد کرد. داده‌هایی که برای یادگیری عمیق استفاده می‌شوند، مستقیماً با عملکرد AI ارتباط دارند. با افزایش اهمیت داده‌ها، صدمه‌ای که به اعتبار[۱] یا تمامیت[۲] داده‌ها وارد می‌شود، اعتماد افراد به خدماتی که از داده‌ها استفاده می‌کنند را سلب خواهد کرد.

درزکردن داده‌ها، مانند اطلاعات شخصی، اسرار تجاری و دیگر داده‌های ارزشمند، علاوه بر اینکه مشمول ادعای جبران خسارت یا صدمه می‌شود، ممکن است موجب افول اعتماد جامعه به یک سازمان یا کمپانی نیز شود. چنین داده‌هایی اگر به بیرون درز کنند، دیگر هرگز برنمی‌گردند و ممکن است مستقیماً باعث افت رقابت آن سازمان یا کمپانی شود.

(۳) ضرر به‌موجب کلاهبرداری یا سرقت مالی

تا به حال مواردی پیش آمده که به خاطر ناکافی بودن تمهیدات اساسی برای امنیت سایبری منجر به دسترسی غیرمجاز به اپراتورهای مبادله ارز

۱. خصوصیتی که به ما اطمینان می‌بخشد یک عامل یا منبع با ادعا مطابقت دارد.
۲. اینکه به اطلاعات صدمه وارد نشده، تغییر داده نشده‌اند یا حذف نشده‌اند.

مجازی و خسارت گسترده مالی از طریق دستکاری ایمیل آن کسب‌وکار شده است. همان‌طور که انتظار می‌رود فعالیت‌های اجتماعی و اقتصادی هر چه بیشتر به فضای سایبری وابسته شوند، پیش‌بینی می‌شود که ناکافی بودن تمهیدات امنیت سایبری مستقیماً موجب خسارت و ضرر مالی و افزایش آن خواهد شد.

بخش دوم

بخش دوم

چشم‌اندازها و اهداف این استراتژی

چشم‌اندازها و اهداف این استراتژی در زیر به عنوان ابقای پایدار موضع اساسی ژاپن در خصوص امنیت سایبری و با توجه به چنین موضعی، به عنوان «چشم‌انداز اساسی امنیت سایبری» تحت درک فعلی از فضای سایبری و تصویر آینده آن توضیح داده شده است.

۲-۱- تبعیت از موضع اساسی در خصوص امنیت سایبری

ژاپن از موضع اساسی خود در خصوص امنیت سایبری از جمله «اهداف قانون اساسی امنیت سایبری» و «ایده‌ها و اصول اساسی» ارائه‌شده در استراتژی ۲۰۱۵ تبعیت خواهد کرد. بر این اساس، برای جلوگیری از فعالیت عاملان مخرب و تضمین ایمنی و حقوق مردم، ژاپن ابزارهای سیاسی، اقتصادی، تکنولوژی، قانونی، دیپلماتیک و سایر ابزارهای مناسب و مؤثر را به عنوان گزینه‌های خود حفظ می‌کند.

(۱) اهداف قانون اساسی امنیت سایبری

هدف این قانون اساسی این است که «نشاط اجتماعی و اقتصادی و توسعه پایدار را تقویت کند»، «جامعه‌ای امن و ایمن برای مردم ایجاد

کند» و «به صلح و ثبات جامعه‌یبین‌الملل و امنیت ملی کمک کند»[1] این استراتژی همچنین اهداف سیاسی را در سه زمینه زیر ترتیب می‌دهد تا تمهیدات لازم را بر این اساس ترویج دهد.

(۲) آرمان‌های اساسی

آرمان‌های اساسی‌ای که ژاپن برای رسیدن به اهداف این قانون اساسی به آن‌ها پایبند خواهد بود رسیدن به «فضای سایبری آزاد، عادلانه و ایمن» است. چنین فضای سایبری‌ای به معنای فضای سایبری ایمنی است که در آن آزادی بیان و فعالیت‌های اقتصادی همه‌ی عامل‌هایی که در آن فعالیت می‌کنند، بدون هیچ‌گونه تبعیض و استثناءِ غیرموجه تضمین شده و فعالیت‌های غیرقانونی مانند سرقت اطلاعات یا دارایی مجاز نیست.

(۳) اصول اساسی

پنج اصل مندرج در استراتژی ۲۰۱۵ به عنوان اصول اساسی که تبعیت از آن‌ها برای توسعه و اجرای تمهیدات امنیت سایبری لازم است عبارت‌اند از: (الف) اطمینان از جریان آزاد اطلاعات؛ (ب) حاکمیت قانون؛ (ج) آزادی؛ (د) استقلال و (هـ) همکاری بین چند ذینفع.

(الف) اطمینان از جریان آزاد اطلاعات

برای توسعه پایدار فضای سایبری به‌مثابه مکانی برای خلق و نوآوری، ساخت و نگهداری جهانی که در آن اطلاعات منتقل‌شده بدون سانسور ناعادلانه یا اصلاح غیرقانونی در طول مسیر به گیرنده مورد نظر برسد، ضروری است.[2] توجه به حریم خصوصی نیز باید حفظ شود. طبق اخلاقیات و عرف، به‌عنوان شرطی اساسی برای جریان آزاد اطلاعات

۱. ماده‌ی ۱ این قانون اساسی تصریح می‌کند که «هدف این قانون ترویج سیاست امنیت سایبری به طور جامع و مؤثر است... و در نتیجه، برای تقویت نشاط اقتصادی و اجتماعی، توسعه‌ی پایدار و تحقق شرایطی در اجتماع که در آن مردم بتوانند با حس امنیت و ایمنی زندگی کنند تلاش کرده، به حفاظت از صلح جهانی و همچنین امنیت ملی کمک می‌کند.»
۲. ماده‌ی ۱ این قانون اساسی تصریح می‌کند که «برای اطمینان از جریان آزاد اطلاعات به طور همزمان...»

در فضای سایبری، افراد ملزم‌اند که حقوق و منافع دیگران را خدشه‌دار نکنند.

(ب) حاکمیت قانون

با پیشرفت تلفیق فضای سایبری و فضای واقعی، حاکمیت قانون باید درست مانند فضای واقعی در فضای سایبری نیز حفظ شود. قوانین و ضوابط مختلف داخلی از جمله قوانین و مقررات داخلی در فضای سایبری اعمال می‌شود. به همین ترتیب قوانین بین‌المللی موجود نیز در فضای مجازی اعمال می‌شود. اعمال قوانین بین‌المللی موجود و تدوین هنجارها همچنان برای توسعه پایدار فضای سایبری به‌مثابه فضایی امن و قابل‌اطمینان ضروری است.

(ج) آزادی

برای دستیابی به توسعه پایدار فضای سایبری به‌مثابه فضایی برای تولید ارزش‌های جدید، فضای سایبری باید بدون محدودکردن امکان پیوند ایده‌ها و دانش‌های متنوع برای همه عامل‌ها آزاد باشد. ژاپن از این موضع تبعیت می‌کند که فضای سایبری نباید انحصاراً تحت سلطه برخی گروه‌های خاص قرار بگیرد.[1]

(د) استقلال

فضای سایبری از طریق طرح‌های مستقل چند ذی‌نفع توسعه یافته است. برای یک کشور نامناسب و غیرممکن است که کل، نقش حفظ نظم را برای فضای سایبری ایفا کند تا به عنوان فضایی که در آن نظم و خلاقیت در کنار هم قرار دارند، به‌طور پایدار توسعه یابد. تنها رویکرد برای جلوگیری از و پرداختن به رفتار عاملان مخرب برای حفظ نظم در فضای سایبری این است که سیستم‌های متعدد اجتماعی به طور مستقل به مأموریت‌ها و عملکردهای خود برسند. دولت نیز این رویکرد را تشویق خواهد کرد.[2]

۱. ماده‌ی ۳ قانون اساسی تشکیل جامعه‌ای شبکه‌ای از ارتباطات و اطلاعات پیشرفته این موضوع را تصریح می‌کند.
۲. ماده ۲ بند ۳ قانون اساسی تصریح می‌کند که «ترویج سیاست امنیت سایبری باید با این قصد انجام شود که هر یک از مردم در مورد امنیت سایبری آگاهی پیدا کنند و هر یک از افراد را به اقدامات داوطلبانه تشویق کند.»

(ه) همکاری بین چند ذی‌نفع

فضای سایبری دنیایی چند بُعدی است که از طریق فعالیت چندین نهاد ذی‌نفع، از جمله حکومت، حکومت‌های محلی، اپراتورهای زیرساخت‌های حیاتی، مشاغل مرتبط با فضای سایبری و سایر مشاغل، مؤسسات آموزشی و پژوهشی و افراد ایجاد شده است. برای توسعه پایدار فضای سایبری همه‌ی عامل‌ها ملزم هستند که آگاهانه نقش‌ها و مسئولیت‌های مربوطه خود را انجام دهند. برای انجام این کار، علاوه بر تلاش‌های فردی به هماهنگی و همکاری نیز نیاز است. حکومت‌ها نقش ترویج این هماهنگی و همکاری را بر عهده دارند و تمهیدات لازم برای ایفای چنین نقش‌هایی را ترویج می‌کنند.[1]

۲-۲- چشم‌انداز اساسی امنیت سایبری به‌مثابه هدف

براساس ایده‌های ژاپن که در بالا ذکر شد، در زیر نتیجه مطلوبی ارائه می‌شود که از طرح‌های امنیت سایبری انتظار می‌رود، و همچنین سه رویکرد لازم برای تبلیغ چنین طرح‌هایی به عنوان «چشم‌انداز اساسی امنیت سایبری» مطرح می‌شود.

(۱) هدف

هدف ژاپن محقق کردن جامعه‌ای[2] است که در آن فضای سایبری به عنوان «جبهه تولید ارزش بی‌نهایت» توسعه‌ای پایدار داشته باشد، جایی که ارزش‌ها و خدمات جدید به طور مداوم تولید می‌شوند و برای مردم وفور نعمت به ارمغان می‌آورند.

برای کمک به تحقق چنین جامعه‌ای، فضای سایبری باید از طریق

۱. ماده ۳ بند ۱ قانون اساسی تصریح می‌کند که «(سیاست امنیت سایبری) باید با این قصد انجام شود که از طریق همکاری بین چند ذی‌نفع واکنشی فعال در مقابل تهدیدهای علیه امنیت سایبری ایجاد کند.»

۲. اشاره به نسخه ۵.۰ جامعه (منابع: استراتژی جامع در باب علوم، تکنولوژی و نوآوری (STI) برای سال ۲۰۱۷ (تصمیم کابینه در تاریخ ۲ ژوئن ۲۰۱۷) و استراتژی رشد ۲۰۱۷ (تصمیم کابینه در تاریخ ۹ ژوئن ۲۰۱۷)

مشارکت همه عامل‌ها در تولید ارزش‌های جدید توسعه یابد. برای حمایت از این توسعه پایدار، همه عامل‌ها باید از نقش خود در رابطه با امنیت سایبری آگاه باشند و رویکردهای امنیت سایبری را به صورت مستقل اجرا کنند، درست مانند سیستم ایمنی بدن موجودات زنده.

با چنین چشم‌اندازهایی، دولت طرح‌های زیر را برای تبلیغ طرح‌های امنیت سایبری پیاده خواهد ساخت.

به طور خاص ما طرح‌های بخش دولتی و خصوصی در زمینه امنیت سایبری را با هدف تکامل و توسعه فضای سایبری مستقل و پایدار همزمان با تحقق امنیت و توسعه اقتصادی در فضای سایبری براساس سه رویکرد تبلیغ خواهیم کرد (۱.اطمینان از مأموریت ارائه‌دهندگان خدمات؛ ۲.مدیریت ریسک؛ و ۳.مشارکت، هماهنگی و همکاری.)

تصویر فضای سایبری که به واسطه طرح‌های مستقل همه ذی‌نفعان که متقابلاً بر یکدیگر تأثیر می‌گذارند، به این صورت در حال تکامل است و در مقایسه با نوعی اکوسیستم با توسعه پایدار، «اکوسیستم امنیت سایبری» نامیده می‌شود.

(۲) سه رویکرد

(الف) اطمینان از مأموریت ارائه‌دهندگان خدمات

اجرای قابل اتکای عملیات‌ها و خدمات

«اطمینان از مأموریت» به شرایطی گفته می‌شود که در آن هر سازمانی که نماینده آن کمپانی‌ها، اپراتورهای زیرساخت‌های حیاتی و ارگان‌های دولتی هستند، عملیات یا خدماتی که باید به عنوان «مأموریت» خود انجام دهد را درک می‌کند و از وجود توانایی‌ها و منابع لازم برای اجرای این

«مأموریت‌ها» به صورت قابل‌اتکا اطمینان حاصل می‌کند. از دیدگاه هر سازمانی که عملیات یا خدمات خود را به عنوان «مأموریت» انجام می‌دهد، امری حیاتی است که افراد مسئول در هر سازمان به‌عنوان بخشی از این اطمینان، بدون اتکا به متخصصان در جهت تأمین امنیت سایبری فعالانه تلاش کنند.

به عبارت دیگر، یعنی مدیران ارشد یا مدیران هر سازمان باید عملیات یا خدماتی را شناسایی کنند که نماینده «مأموریت»شان باشد و به‌جای اینکه طرح‌های امنیت سایبری را هدف خود قرار دهند، مسئولیت تأمین امن و پایدار ملزومات را مسئولیت خود بدانند.

(ب) مدیریت ریسک

ارزیابی عدم اطمینان و واکنش مناسب

«مدیریت ریسک» به معنای به حداقل رساندن خطرات در سطح قابل قبول به وسیله شناسایی، تحلیل و ارزیابی ریسک[1] مربوط به «مأموریت‌هایی» است که به سازمان‌ها محول شده است. عدم اطمینان ذاتی فضای سایبری به طور اجتناب ناپذیری به این دیدگاه منجر می‌شود.

ریسک به عنوان «تأثیر عدم اطمینان بر اهداف»[2] تعریف شده است و فقط با در نظر گرفتن اهداف تعیین‌شده قابل اندازه‌گیری است. در نتیجه، ارزیابی یا واکنش به ریسک‌ها بسته به اهداف سازمان متفاوت است. به‌علاوه، مدیریت ریسک[3] به عنوان «مجموعه فعالیت‌ها و روش‌های هماهنگ‌شده برای هدایت یک سازمان و کنترل بسیاری از ریسک‌هایی که ممکن است بر توانایی آن در دستیابی به اهداف تأثیر بگذارد» تعریف شده است و از این رو نمانیده مجموعه کلی فعالیت‌های مقابله با

۱. دقت کنید که این اشاره به عدم اطمینانی دارد که هم جنبه مثبت و هم جنبه منفی دارد.
۲. تعریف ارائه‌شده از سازمان بین‌المللی استانداردسازی (ISO)
۳. تعریف ارائه‌شده از سازمان بین‌المللی استانداردسازی (ISO)

ریسک‌ها از طریق هدایت و کنترل سازمان‌ها و توزیع مناسب منابع محدود سازمان است که محدود به فعالیت‌های فردی شناسایی، تحلیل یا ارزیابی خطرات نیست.

اگر هر سازمانی بدون پذیرش عملیات یا خدماتی که نماینده «مأموریت» آن است ریسک‌ها را دست کم بگیرد و منابع لازم را به امنیت سایبری اختصاص ندهد، ممکن است منجر به موارد غیرمترقبه‌ای شود که می‌تواند بقای سازمان را تهدید کند. از طرف دیگر، اگر خطرات بیشتر از واقعیت تخمین زده شود و منابع اضافی به امنیت سایبری اختصاص یابد، ممکن است مانع اجرای عملیات یا خدمات سازمان و رشد پایدار آن شود.

چنین رویکردی نسبت به مدیریت ریسک برای همه، حتی افراد که از مزایای به‌کارگیری دانش، تکنولوژی یا خدمات فضای سایبری بهره می‌برند، ضروری است.

وقتی از این مزایا بهره می‌بریم، بروز ریسک از دست دادن کنترل تکنولوژی‌ها یا خدمات پیش‌نیاز رایج است. بر این اساس، از آنجایی که پیش‌بینی مکانیکی امکان‌پذیر نیست و از بین بردن ریسک به طور کامل غیرممکن است، لازم است با توجه به ماهیت یا نمود هر ریسک چنین ریسک‌هایی را به‌درستی برطرف کنیم و ریسک‌های مربوط به امنیت سایبری را در سطح قابل قبولی در تعادل با ویژگی‌های خوب خدمات و محصولات ارائه شده در آن به حداقل برسانیم.

(ج) مشارکت، هماهنگی و همکاری

تمهیدات، هماهنگی و همکاری توسط افراد و سازمان‌ها در زمان صلح

«مشارکت، هماهنگی و همکاری» مربوط به طرح‌های اساسی است

کـه توسـط افـراد یـا سـازمان‌ها در زمـان صلـح بـرای جلوگیـری از خسـارت یـا تشـدید آن کـه احتمـالاً از تهدیدات فضای سـایبری نشـأت گرفتـه اعمال می‌شـود. هـر عاملـی کـه در فضـای سـایبری فعالیـت می‌کنـد، ممکن اسـت بـه عنـوان سـود خـود بـه طـور بالقـوه ارزش‌های جدیـد ایجـاد کند، امـا این هـم ممکـن اسـت کـه در معـرض تهدیداتـی قـرار گرفته باشـد که ریشـه در ریسـک‌های ذاتـی فضـای سـایبری دارنـد. از ایـن دیـدگاه لازم اسـت کـه نـه تنهـا سـازمان‌هایی کـه خدمـات ارائـه می‌دهند، بلکه افـراد نیـز در زمان صلح تلاش‌هـای امنیـت سـایبری اساسـی روزمـره را انجـام دهند.

بـه طـور خـاص، ایـن مسـئله شـامل تمهیدات انجام‌شـده بـرای محافظت در برابـر برنامه‌هـای مخـرب، کاهش آسـیب‌پذیری،[1] اطمینان ایمـن مدارک و مدیریـت صحیـح اطلاعات شـخصی و موارد دیگر می‌شـود. ایـن طرح‌ها اغلب بـا فعالیت‌های بهداشـت عمومـی یا کمپین‌هـای ایمنی حمل‌ونقـل در فضای واقعی مقایسـه می‌شود.

بـا ایـن حـال، اگرچه حملات سـایبری ممکن اسـت هر زمـان یا هر جایی اتفـاق بیفتنـد و تهدیدهـا بـه نگرانـی روزمـره تبدیـل شـوند، اما نشـان دادن واکنش تنها با تلاش‌های فردی دشـوار اسـت و بـرای تقویت چنین طرح‌هایی حمایـت فعـال از طـرف دیگـر ذی‌نفعـان از جملـه سـازمان‌ها الزامـی اسـت.

بـه همیـن دلیـل، لازم اسـت کـه همه با هـم در این طرح‌هـا فعالیت کنند کـه یعنـی بایـد بـا یکدیگر همـکاری کننـد. عـلاوه بـر کار بـر روی طرح‌های فـردی، لازم اسـت که هر فرد یا سـازمانی کـه در فضای مجـازی دخالت دارد، اطلاعات را به اشـتراک بگذارد و بدون در نظر گرفتن شـرایط صلح یا شـرایط اضطـراری بـا یکدیگر هماهنگ شـده و همکاری کنند. ایـن تلاش‌های امنیت سـایبری اساسـی باید به‌مثابه بهداشـت جدید سـایبری در نظر گرفته شـوند.

۱. افراد، اشیاء و نقایص خدمات که منجر به تهدید می‌شوند.

بـر همیـن اسـاس، مـا بایـد از طریق مشـارکت دولتـی و خصوصـی از این طرح‌هـا حمایـت کنیـم تا ایـن طرح‌هـای اصولـی را تبلیغ کنیم. بـه خصوص تحـت اصـل «همـکاری بیـن چند نهـاد ذی‌نفـع» کـه در اصول اساسـی ذکر شـده اسـت، ژاپـن بایـد به طـور فعالانه نقـش تبلیـغ همـکاری و هماهنگی را بـه صـورت روزانه انجـام دهد.

بخش سوم

بخش سوم

رویکردهای سیاسی در راستای رسیدن به اهداف

در زیر اهداف و رهنمودهای سیاست‌های برنامه‌ریزی‌شده‌ای آورده شده است که برای ارائه نتایج استراتژی در سه سال آینده اجرا خواهد شد. انتظار می‌رود که هر خط مشی مطابق با سه رویکرد زیر باشد که در ایده ژاپن در باب امنیت سایبری و چشم‌انداز اساسی امنیت سایبری شرح داده شده است.

۳-۱- امکان ایجاد نشاط اجتماعی و اقتصادی و توسعه پایدار

شرکت‌ها با استفاده فعال از ابزارهای دیجیتال مانند رایانه‌های شخصی و تلفن‌های هوشمند و اینترنت در حال بهره‌وری از تجارت خود هستند. از این تکنولوژی‌ها همچنین برای معرفی نوآوری در تجارت، خدمات پیشرفته و سایر ارزش‌های جدید استفاده می‌شود. تمهیدات امنیت سایبری به‌جای «هزینه‌های» ناخواسته باید به‌مثابه «سرمایه‌گذاری» به‌عنوان مبانی پیشبرد این روند تلقی شوند. تمهیدات سازگار امنیت سایبری موجب رشد صنعتی و رقابت جهانی می‌شود و برای نشاط اقتصادی و اجتماعی و توسعه پایدار ژاپن حیاتی است.

۳-۱-۱- پیشرفت امنیت سایبری به عنوان محرک ایجاد ارزش

شرکت‌ها همزمان تلفیق فضای سایبری و فضای واقعی با خطرات امنیت سایبری بیشتری روبرو خواهند شد. آگاهی از امنیت سایبری در بین بخش‌های صنعتی و بنگاه‌های اقتصادی بزرگتر در حال افزایش است. در آینده لازم است درک این نکته در همه بخش‌های صنعتی ضروری است که طرح‌های امنیت سایبری باید برای اطمینان از ادامه تجارت شرکت‌ها و ایجاد ارزش جدید اجرا شوند. تبلیغ این طرح‌ها نیز ضروری است.

در انجام این کار مهم است که بدانیم ریسک‌های مرتبط با امنیت سایبری یکی از انواع ریسک‌هایی است که شرکت‌ها با آن روبرو هستند و تمهیدات مورد نظر باید به عنوان بخشی از مدیریت ریسک انجام شود. علاوه بر این، این تمهیدات باید به طور طبیعی با توجه به وضعیت هر صنعت و تجارت در سازمان‌ها ریشه بدواند.

(۱) افزایش آگاهی اجرایی

به‌نظر می‌رسد هنوز اکثر رهبران تجاری این‌طور فکر می‌کنند که تمهیدات امنیت سایبری هیچ سودی برای کسب‌وکار آن‌ها ندارد. این باور ممکن است ناشی از این فکر باشد که آمادگی برای حمله سایبری چیزی جز «هزینه» ناخواسته نیست، زیرا فضای سیابری باید بدون هیچ‌گونه احتیاطی به صورت رایگان ارائه شود و حملات سایبری برای آسیب‌رساندن به کسب‌وکار آن‌ها تقریباً هرگز اتفاق نمی‌افتد. اگرچه استفاده از فضای سایبری به‌شدت در حال رشد است، شرکت‌ها باید متوجه باشند که تهدیدات دقیقاً به خاطر همین آزادی وجود دارد و آمادگی مقابله با آن‌ها را داشته باشند. ممکن است شرکت ها متوجه شوند که تعیین اهمیت تمهیدات

امنیت سایبری بدون بحث در سطح سازمانی دشوار است. افزایش آگاهی اجرایی ضروری است زیرا انتظار می‌رود مدیران اجرایی نقش مبلّغ این تفکر را بر عهده داشته باشند که تمهیدات امنیت سایبری سرمایه‌گذاری‌ای ضروری برای اطمینان از تداوم تجارت و ایجاد ارزش است، نه هزینه‌ای اجتناب‌ناپذیر.

به‌ویژه از مدیران اجرایی ارشد انتظار می‌رود که از طریق جلسات اجرایی به طور فعال در امنیت سایبری مشارکت داشته باشند و باید سطح مشخصی از دانش و مهارت مدیریت ریسک را در امور امنیت سایبری کسب کنند. اگرچه شاید نیاز به کسب دانش و مهارت فنی عمیق برای مدیران ارشد چندان واقع‌بینانه نباشد. در نتیجه شرکت‌ها باید منابع انسانی (یا «سطح مدیریت استراتژیک») را که توانایی درک ریسک‌های امنیت سایبری در زمینه‌های مدیریت و استراتژی‌های تجاری را دارند، می‌توانند برای تمهیدات امنیت سایبری متناسب با سیاست‌های اجرایی برنامه‌ریزی کنند و هم کسب‌وکارها و هم کارکنان فنی را هدایت کنند، در دسترس داشته باشند. مدیران ارشد باید برای کل زنجیره تأمین طرح‌های مدیریت ریسک مناسب ایجاد کنند که هم سازمان‌های خود و هم سازمان‌های پیمانکار را پوشش دهند. همچنین مدیران ارشد باید در برابر منافع و ریسک‌های کسب‌وکار که به خاطر فضای سایبری به‌وجود آمده است در مقابل نهادهای ذی‌نفع پاسخگو باشند.

با توجه به این وضعیت، دولت با بخش‌های خصوصی همکاری خواهد کرد تا کارکنانی را کشف کنند و آموزش دهند که هنگام برگزاری سمینار برای تغییر تفکر مدیران ارشد، قادر به توضیح و بحث درباره تمهیدات امنیت سایبری برای مدیران ارشد باشند. دولت همچنین سیاست‌هایی را که

بـه اهمیـت تمهیدات امنیت سـایبری بـرای مدیران ارشـد به روشـی قابل‌درک بپردازنـد، تشـویق خواهـد کـرد. این سیاسـت‌ها شـامل تشـویق اظهارنامه‌ها در مـورد طرح‌هـای کمپانـی و توسـعه ابزارهایـی برای تصویرسـازی تمهیـدات به قصـد مقایسـه‌ی آن‌هـا بـا تمهیـدات کمپانی‌هـای مشـابه می‌شـوند. دولـت بـا دانشـگاه‌ها نیـز همـکاری خواهـد داشـت تـا سیسـتم‌های حقوقـی مختلفی را تنظیـم کنـد کـه شـرکت‌ها هنگام اجـرای تمهیـدات امنیت سـایبری خـود به آن‌هـا مراجعـه کنند.

(۲) تقویت سرمایه‌گذاری در امنیت سایبری

مشـوق‌های مدیریتی متناسـب برای اطمینان کمپانی‌ها از اجرای تمهیدات امنیـت سـایبری بـه طور مداوم مهم اسـت. بـه عبارت دیگر بهتر اسـت چرخهٔ مطلوبـی داشـته باشـیم کـه در آن ریسـک‌های امنیـت سـایبری و تمهیـدات مربـوط بـه آن‌هـا از دیدگاه مالی قابل رؤیت باشـند، مدیران ارشـد وضعیت امور را درک کننـد و تمهیـدات لازم دیگـری را مورد بررسـی قـرار داده و اجرا کنند، بـازار ارزیابـی مثبتی از آن تمهیـدات ارائه داده و آن‌ها را تلاش‌هایی نشـان دهد کـه بـه ارزش شـرکتی بیشـتر ختـم می‌شـود، و به همیـن ترتیب مشـوق‌های بیشـتری برای سـرمایه‌گذاری در امنیت سـایبری ایجاد شـود.

بـه همیـن منظـور، انتشـار و افشـای فعالانـه اطلاعات مربوط بـه تمهیدات امنیـت سـایبری توسـط کمپانی‌ها مهم اسـت. دولت هنگام کار بـر روی درک و ارزیابـی مداوم وضعیت انتشـار و افشـای اطلاعـات، اطلاعات مربـوط به بهترین روش‌هـا را بـه اشـتراک گذاشـته و دسـتورالعمل‌هایی ایجاد خواهد کـرد. علاوه بـر ایـن، لازم اسـت که ایجـاد چارچوبی بـرای سـرمایه‌گذاران به‌منظـور ارزیابی طرح‌هـای امنیـت سـایبری از جانب مدیریت شـرکت را پیـش ببریم.

دولت در خصوص تمهیداتی که هدف‌شان تشویق شرکت‌ها به ترویج امنیت سایبری است، استفاده از مشوق‌های سرمایه‌گذاری در امنیت سایبری را پیگیری خواهد کرد تا به طور مؤثر عمل کنند و تمهیدات لازم را ضروری بدانند.

علاوه بر این، استفاده از بیمه به عنوان یک رویکرد مدیریت ریسک برای امنیت سایبری در حال افزایش است. این امر ممکن است باعث شود تشویق به سرمایه‌گذاری آسان شود چون هزینه آمادگی برای ریسک‌ها توسط سیستمی، شفاف‌سازی خواهد شد که در آن حق بیمه با توجه به وضعیت اجرای تمهیدات امنیت سایبری محاسبه خواهد شد. بر اساس این درک، دولت با همکاری بخش خصوصی تدابیری را در خصوص تشویق به استفاده از بیمه امنیت سایبری اتخاذ کرده است.

(۳) تقویت کسب‌وکارهای امنیت سایبری با حمایت از نوآوری‌هایی که از تکنولوژی پیشرفته استفاده می‌کنند

استفاده از تکنولوژی‌های پیشرفته مانند اینترنت اشیا، AI، واقعیت مجازی، زنجیره بستکی و تکنولوژی‌های ارتباط از راه دور نسل بعدی، اغلب برای ایجاد ارزش‌های جدید در شرکت‌ها ضروری است. در عین حال، استفاده از این فناوری‌ها آسیب‌پذیری‌های جدیدی را ایجاد می‌کند که قبلاً وجود نداشته‌اند و استفاده مخرب از چنین تکنولوژی‌هایی نیز ممکن است به ریسک‌های غیرمنتظره منجر شود. به همین دلیل انتظار می‌رود که محصولات یا خدمات به واسطه برآورد خطرات قبلی و به‌کارگیری تمهیدات امنیت سایبری در فرایندهای ایجاد آن محصولات یا خدمات (امنیت از طریق طراحی) در خصوص امنیت سایبری از کیفیت بالایی برخوردار باشند. به‌علاوه، این طرح‌ها نه تنها به افزایش اعتماد به محصولات

یـا خدمـات ژاپـن منجـر خواهد شـد، بلکـه بـه ترویج اسـتقرار زیرسـاخت‌های باکیفیـت در خـارج از کشـور نیـز ختـم خواهد شـد کـه از اهـداف ژاپن اسـت.

در همیـن حـال، بـه دلیـل کمبـود تخصـص در امنیـت سـایبری، شـاید بر خـلاف نیت اولیه‌شـان، پیشـروی بـا چنین طرح‌هایی برای شـرکت‌ها به‌آسـانی ممکـن نباشـد. از طرفـی، از دیـدگاه افزایـش توان رقابتـی بین‌المللـی و پرهیز از اتـکا بـه محصـولات یـا خدمـات امنیتـی کـه به‌سـختی می‌تـوان و صحت و اطمینان‌شـان را تأییـد کـرد، ایـن امـر ضـروری اسـت. بنابرایـن نیاز بـه تقویت کسـب‌وکارهای امنیت سـایبری که راه‌حل‌های مشـخصی در داخل کشـور ارائه می‌دهنـد، وجـود دارد.

بـرای تأمیـن ایـن نیازهـا، دولـت از چالش‌هـای پیش‌روی ایجـاد ارزش‌های جدیـد بـا اسـتفاده از چنین تکنولوژی‌های پیشـرفته‌ای نه فقط در شـرکت‌های بـزرگ بلکـه در شـرکت‌های خطرپذیـر نیـز پشـتیبانی می‌کنـد. دولـت به‌ویژه بـا بخش‌هـای خصوصی همـکاری خواهـد کرد تا ریسـک‌های امنیت سـایبری مرتبـط بـا اسـتفاده از تکنولوژی‌های پیشـرفته را تحلیـل و شفاف‌سـازی کرده و دسـتورالعمل‌های مبتنـی بـر ایـن تحلیـل و شفاف‌سـازی‌ها را ارائـه خواهـد داد. عـلاوه بـر ایـن، دولت تحقیق و توسـعه در حـوزه تحلیل ریسـک و اقدامات متقابـل در برابـر تهدیـدات تکنولوژی‌های پیشـرفته مورد نیاز بـرای این طرح‌ها را تشـویق خواهد کرد. مهم اسـت که مفهوم امنیت از طریق طراحی را اسـاس ایـن طرح‌ها قـرار دهیم. دولت همچنین همـراه با تأمین‌کننـدگان تکنولوژی‌ها یا خدمات امنیت سـایبری که از اسـتفاده این تکنولوژی‌های پیشـرفته حمایت می‌کنـد سیسـتم‌هایی خواهـد سـاخت کـه بـا هـدف شـرکت‌ها بـرای ایجـاد ارزش‌های جدید با اسـتفاده از تکنولوژی‌های پیشـرفته همخوانی داشـته باشـد.

عـلاوه بـر ایـن، به منظور تبلیغ به‌کارگیـری بین‌المللی محصولات یا خدمات

ژاپـن کـه بـه سـطح بالایی از امنیت سـایبری دسـت یافته‌انـد، دولـت از طریق تبلیـغ ایـن محصولات یا خدمات توسـط مقامات ارشـد دولتی و نمایشـگاه‌های تجـاری مزایای آن‌هـا را تبلیغ خواهد کرد. دولت همچنین برای توسـعه فضایی تجـاری تـلاش خواهـد کـرد که به‌کارگیـری بین‌المللـی محصولات یـا خدمات ژاپـن را از طریق اقدامات سـخت‌گیرانه با همـکاری بین‌المللی در برابر تمهیدات مخالف تجارت آزاد به اسـم امنیت سـایبری تسـهیل بخشـد.

۳-۱-۲- رسـیدن به زنجیـره تأمینی که به‌واسـطه ارتباطات گوناگون ایجـاد ارزش می‌کند

بـا سـرعت گرفتـن تلفیـق فضـای سـایبری و فضـای واقعـی، تجـارت بیـن صنایـع و شـرکت‌های مختلـف که پیش از این وجود نداشـته اسـت، همزمان با پیشـروی ما به سـمت نسـخه ۵.۰ جامعه در سـطح جهانی در حال انجام اسـت. عـلاوه بـر ایـن، اشـکال متنـوع و سـیالی فراتـر از دنبالـه عرضه سـنتی در حال ظهـور اسـت، ماننـد اتوماسـیون تجارت. بـا توجه به این اشـکال جدید، مسـائل امنیـت سـایبری کـه در لبـه ایـن ارتباطـات زنجیره‌هـای تأمیـن رخ می‌دهـد، امکان گسـترش گسـترده‌تری نسـبت به قبل دارند و تأثیرات منفی گسـترده‌ای را نـه تنهـا در فضـای واقعـی، بلکـه در تمـام فعالیت‌هـای اقتصـای و اجتماعی ایجـاد خواهنـد کـرد. آگاهـی از ایـن ریسـک‌ها و تشـویق طرح‌هایـی کـه کل زنجیـره‌ی تأمیـن را مـورد توجـه قـرار دهد، ضروری اسـت.

(۱) تدوین چارچوب امنیت سایبری برای ریسک زنجیره تأمین

از آن‌جـا کـه ارتباطـات زنجیـره تأمیـن اشـکال متنـوع و سـیال‌تری دارنـد، بـرای اطمینـان از امنیت سـایبری اجـرای تمهیدات سـازگار بـرای کل زنجیره

تأمین ضروری است. همچنین انتظار می‌رود کیفیت محصولات یا خدمات باعث ایجاد ارزش جدید از طریق اجرای این تمهیدات شود.

به‌ویژه دولت با بخش‌های خصوصی همکاری خواهد کرد تا تهدیدات موجود در زنجیره تأمین را شناسایی کرده و چارچوب‌هایی تدوین و منتشر کند که برای اجرای تمهیدات در سطح عملیاتی در تمام گروه‌های صنعتی کاربرد داشته باشد. برای اینکه اپراتورهای تجاری از جمله شرکت‌های کوچک و متوسط اقدامات را به راحتی انجام دهند، توجه کافی در نظر گرفته می‌شود تا از اینکه محتوای دستورالعمل با توجه به شرایط آن‌ها واقعاً عملی و قابل درک است اطمینان حاصل شود. این نیز مهم است که مطمئن شویم اپراتورهای تجاری از تعادل بین ریسک‌ها و هزینه اقدامات متقابل آگاه باشند.

ارائه تمهیدات ویژه در مورد هر بخش مورد نیاز برای دستگاه‌های اینترنت اشیا یا سازمان‌هایی که از ارتباطات، مناطقی که نیاز به محافظت دارند و تفاوت تهدیدات مربوط به زنجیره تأمین در هر بخش صنعت آگاهی دارند، ضروری است. به‌علاوه، با گسترش زنجیره تأمین در سطح جهان، لازم است گرایش‌های خارجی در توسعه قوانین مربوطه منعکس شود تا تمهیدات امنیت سایبری مبتنی بر چارچوب‌های امنیتی ژاپن در سطح جهانی شناخته شود.

(۲) ساخت یک سیستم برای تأمین امنیت سایبری در زنجیره تأمین

اطمینان از قابل اعتماد بودن عناصر متشکل زنجیره تأمین از جمله دستگاه‌های در حال تولید، داده‌های تولیدشده و توزیع‌شده در دستگاه‌ها و خدماتی که از آن‌ها استفاده می‌کنند برای تأمین امنیت سایبری کل زنجیره تأمین ضروری است. برای این منظور، لازم است که دولت تلاش

کنـد الزامات کار را روشـن سـاخته و سیسـتمی ایجـاد کند که به‌واسـطه تأیید اجـرای ایـن الزامـات اعتمـاد به‌وجـود بیـاورد. در نتیجـه هـر عنصر بـه صورتی سـاخته و توزیـع می‌شـود که الزامـات امنیتی را بـرآورده سـازد. همچنین لازم اسـت کـه دولـت بـا بخـش خصوصی همـکاری کنـد تا سیسـتمی ایجـاد کند کـه لیسـتی از دسـتگاه‌ها و خدماتـی را ایجـاده کـرده و مدیریت کنـد که قابل اعتماد بودن‌شـان تأیید شـده باشـد تا تأمین‌کنندگان در زنجیره تأمین بتوانند هنگام اسـتفاده از دسـتگاه‌ها یا تجهیـزات این قابل اعتماد بـودن را تأیید کنند. دولـت همچنین سیسـتمی بـرای تأیید قابل ردگیـری بودن و سیسـتمی برای تشـخیص و پیشـگیری از حمـلات علیـه خـود اعتمـاد ایجادشـده مدنظـر قرار خواهـد داد تـا ایـن سیسـتم‌ها بـه سیسـتم‌های پیوسـته در ارتباطـات زنجیره تأمین تبدیل شـوند.

(۳) تبلیغ طرح‌ها توسط شرکت‌های کوچک و متوسط

وقتی شـرکت‌های کوچک و متوسـط به خاطر حملات سـایبری با خسـارت مالـی و افـت در اعتمـاد مواجـه می‌شـوند، ضربـه‌ای کـه بـه عملیات‌هـا وارد می‌شـود ممکن اسـت بیشـتر از مورد شـرکت‌های بزرگ باشـد. این نگرانی نیز وجـود دارد کـه شـرکت‌های کوچـک و متوسـط ممکن اسـت به‌عنـوان پایه‌ای بـرای گسـترش ضربـه حملات سـایبری از کمپانی به شـرکای تجاری اسـتفاده شـوند. در ایـن حیـن، تمهیدات امنیت سـایبری باید بـا ایـن درک ترویج یابند کـه شـرکت‌های کوچک و متوسـط الزاماً دارای دانش یا مهـارت بالایی از امنیت سـایبری نیسـتند و ممکن اسـت سـرمایه‌گذاری کافی در امنیت سـایبری برای آن‌ها دشـوار باشد.

بـه همیـن دلیـل، دولـت مطالعـات موردی آسـان‌فهمی از تمهیـدات امنیت

سایبری برای شرکت‌های کوچک و متوسط فراهم خواهد کرد که شامل الگوهایی برای استفاده امن از سیستم‌های اطلاعات خواهد بود و استفاده از بیمه در امنیت سایبری را تبلیغ خواهد کرد. دولت همچنین سیستم مشاوره برای شرکت‌های کوچک و متوسط درباره حوادث امنیت سایبری را تقویت خواهد کرد. به‌علاوه، دولت با همکاری بخش خصوصی طرح‌های پدیداری را برای شرکت‌های کوچک و متوسطی تبلیغ خواهد کرد که روی امنیت سایبری کار می‌کنند تا در طرح‌های خودشان تلاش‌هایشان را به مردم نشان دهند. این طرح‌ها شامل سیستمی خواهد بود که به آن‌ها اجازه می‌دهد تلاش‌های امنیت سایبری خود را به طور مؤثر و هماهنگ با برنامه‌های مشوق اجرا کنند.

۳-۱-۳- ساخت سیستم‌های ایمن اینترنت اشیا[1]

تعداد دستگاه‌های متصل به فضای سایبری به‌سرعت رو به افزایش است و تمهیدات امنیت سایبری برای چیزهای آسیب‌پذیر که ممکن است به عنوان زیرساخت‌های حیاتی برای توسعه فعالیت‌های اجتماعی و اقتصادی تأثیری منفی بر فضای سایبری بگذارند، تبدیل به مسئله‌ای فوری شده است. به‌علاوه، با افزایش اتصال بین اشیای متعدد (اینترنت اشیاء) با استانداردهای امنیتی مختلف، از جمله سطوح امنیتی یا امنیت فیزیکی، امکان ایجاد تهدیدهای جدید برای این اتصالات وجود دارد.

(۱) تقویت چارچوب ساختاری برای سیستم‌های اینترنت اشیا و استاندارد بین‌المللی

تا امروز دولت با همکاری بخش خصوصی از طرح اجرای تمهیدات متعدد

۱. سیستمی که در آن همه‌چیز، از جمله لوازم برقی خانه، خودروها و سنسورهای هوشمند به اینترنت و دیگر شبکه‌ها متصل شده‌اند که باعث می‌شود با استفاده از کلان‌داده‌ها و دیگر تولیدات آن‌ها خدمات جدیدی ارائه دهند.

برای ایجاد سیستم‌های ایمن اینترنت اشیا، از جمله ایجاد خط مشی روی تمهیدات امنیت ملی کار کرده است. از این پس، ضروری است که روی ایجاد ارزش از طریق سیستم‌های ایمن اینترنت اشیا تأکید کرد و به‌طور استراتژیک به صورت پیوسته و پایدار کار کرد.

به همین منظور، با توجه به عناصر پایه[1] امنیت سایبری که برای سیستم‌های ایمن اینترنت اشیا لازم است و تا به حال توسط دولت معرفی شده است، دولت درکی مشترک بین نهادهای ذی‌نفع اصول اساسی، اهداف، روش‌ها و محدودیت‌های زمانی تمهیدات به وجود می‌آورد و نقش‌ها و عملکردهای هر بخش یا نهاد ذی‌نفع را مشخص می‌کند. علاوه بر این، دولت طرح‌هایی را تبلیغ خواهد کرد که طی آن‌ها هر نهاد ذی‌نفع در حین تبلیغ تمهیدات مستقل امنیت سایبری همکاری نیز می‌کند. به علاوه، برای تبلیغ این طرح‌ها، دولت تلاش خواهد کرد تا این مسائل و طرح‌های مشترک هر نهاد ذی‌نفع را در بخش‌های دولتی و خصوصی به‌نحوی تصویرسازی کند که تصویری کلی ارائه داده سیستمی برای اشتراک اطلاعات بسازد. این طرح‌ها فقط شامل مسائل مختص بخش‌ها که بر دوش عوامل بخش‌های دولتی و خصوصی سنگینی می‌کند، نیست بلکه شامل مسائل مشترک مانند مقیاس، تعریف، تمهیدات امنیت فیزیکی، نکات تعیین محدوده مسئولیت‌ها (از جمله مسئولیت‌های قانونی هر عامل مثل مسئولیت در قبال محصول توسط تولیدکنندگان و تعهدات مدیریت ایمنی اپراتور و غیره، برای حوادث مربوط به واکنش نسبت به آسیب‌پذیری‌های شناخته‌شده)، و مسائل حریم شخصی نیز می‌شود. به‌علاوه، دولت با بخش خصوصی همکاری خواهد کرد تا تلاش در جهت استانداردسازی بین‌المللی عناصر اساسی امنیت سایبری را تبلیغ کند که برای به‌واقعیت‌رساندن

۱. چارچوب عمومی اینترنت اشیا (اکتبر ۲۰۱۶، دفتر مرکزی استراتژیک امنیت سایبری)

سیستم‌های ایمن اینترنت اشیا برای توسعه سیستم‌های ایجاد ارزش در سیستم‌های اینترنت اشیا لازم است و آن‌ها را در سطح جهانی به کار بگیرد، در حالی که نقاط قوت ژاپن در ایمنی و امنیت را در جهت مشارکت در توسعه اقتصاد جهانی به واسطه گسترش این سیستم‌های ایمن اینترنت اشیا استفاده خواهد کرد.

(۲) آماده‌سازی تشکیلاتی برای مقابله با آسیب‌پذیری

برای مقابله با جدیت رو به افزایش حملات سایبری علیه دستگاه‌های اینترنت اشیا، به‌کارگیری تمهیدات برای اطمینان از امنیت و قابل‌اعتمادبودن اطلاعات و شبکه‌های ارتباطی تحت هماهنگی و تقسیم وظایف بین صنعت، دانشگاه و بخش‌های دولتی و خصوصی حائز اهمیت است. به همین دلیل، دولت باید با بخش‌های خصوصی همکاری کند تا تشکیلاتی برای تمهیدات امنیت سایبری آماده کند که تمامی چرخه زندگی دستگاه‌های اینترنت اشیا از طراحی و تولید تا به‌کارگیری و دوراندازی را پوشش دهد، و تشکیلاتی برای تمهیدات مرتبط با دستگاه‌های آسیب‌پذیر اینترنت اشیا در شبکه‌های اطلاعات و ارتباطات را آماده کند.

تمهیدات امنیت سایبری برای دستگاه‌های اینترنت اشیا که تمام چرخه زندگی آن‌ها را پوشش دهد باید با درنظرگیری کامل این موضوع به کار گرفته شوند که هر دستگاه چگونه استفاده می‌شود و کدام تهدیدات امنیت سایبری به آن مربوط می‌شود. وضعیت تمایلات و گرایشات و توسعه‌های تکنولوژی نیز باید در نظر گرفته شود. علاوه بر این، این تمهیدات باید با درک و هماهنگی مشترک تمام نهادهای ذی‌نفع مثل تأمین‌کنندگان دستگاه‌های اینترنت اشیا، شرکت‌های مخابراتی و کاربران

به‌کارگرفته شوند. در بخشی از این برنامه، دولت با بخش‌های خصوصی همکاری می‌کند تا نیازمندی‌های امنیت سایبری را برای هر دستگاه اینترنت اشیا بر اساس خصوصیات آن فهرست کرده و استفاده از دستگاه‌های اینترنت اشیائی را تبلیغ کند که این ملزومات را رعایت می‌کنند.

علاوه بر این، در خصوص تمهیدات مرتبط با دستگاه‌های آسیب‌پذیر اینترنت اشیاء در شبکه‌های اطلاعات و ارتباطات، دولت به طور مداوم دستگاه‌های لازم را تقویت خواهد کرد تا دستگاه‌های اینترنت اشیائی را که از رمز عبورهای معیوب استفاده می‌کنند، شناسایی کند و فوراً از طریق شرکت‌های مخابراتی به کاربران اخطار دهد. به‌علاوه، هنگام اجرای تمهیدات، وزارتخانه و آژانس‌های دولتی مرتبط با یکدیگر همکاری می‌کنند و با شرکت‌های مخابرات و تولیدکنندگان دستگاه‌ها هماهنگ خواهند بود.

دولت قصد دارد در آینده به ایجاد محیطی امن از طریق تقویت شبکه‌های اطلاعات و ارتباطات جهانی به واسطه اجرای این تمهیدات ژاپنی به‌مثابه الگو و گسترش آن‌ها در خارج از کشور از طریق همکاری و استانداردسازی بین‌المللی کمک کند.

۳-۲- ساخت جامعه‌ای امن و ایمن برای مردم

برای به واقعیت پیوستن جامعه‌ای که مردم آن زندگی امن و ایمنی داشته باشند، اطمینان از امنیت سایبری چندلایه از طریق هماهنگی چند نهاد ذی‌نفع از جمله نهادهای دولتی، حکومت‌های محلی، شرکت‌های مرتبط با فضای سایبری، اپراتورهای زیرساخت‌های حیاتی مؤسسه‌های آموزشی و تحقیقات و خود همه مردم حائز اهمیت است.

به طور ویژه، عملیات‌ها و خدماتی که نهادهای دولتی، اپراتورهای

زیرساخت‌های حیاتی، سازمان‌های صنعتی و حکومت‌های محلی (که از این پس با عنوان اپراتورهای زیرساخت‌های حیاتی و غیره به آن‌ها اشاره می‌شود) پایه و اساسی را شکل می‌دهند که از فعالیت‌های روان اجتماعی و اقتصادی و زندگی مردم حمایت می‌کند. با توجه به درک این موضوع که حذف کامل ریسک‌های امنیت سایبری غیرممکن است، دولت طرح‌هایی را براساس رویکرد «اطمینان از مأموریت» تبلیغ خواهد کرد که تحت تصویر امنیت سایبری بیان شده تا ریسک‌ها را به سطح قابل‌قبولی کاهش دهد و اطمینان حاصل کند که این عملیات‌ها و خدمات به طور امن و مدام تأمین می‌شوند.

در این حین، ژاپن برای رویدادهای ملی و بین‌المللی ورزشی از جمله جام جهانی راگبی ۲۰۱۹ و بازی‌های ۲۰۲۰ توکیو آماده می‌شود که انتظار می‌رود مورد حمله سایبری شدیدی از جانب عوامل مخرب قرار بگیرند. در نتیجه، ضروری است که هر نهاد ذی‌نفع با اجرای مداوم نقش‌های مرتبط خود و همکاری با یکدیگر برای به واقعیت رساندن اجرای روان بازی‌های ۲۰۲۰ توکیو و دیگر رویدادها با نگاه همزمان به آینده دورتر با هر موقعیت مقابله کند.

۳-۲-۱- تمهیدات حفاظت از مردم و جامعه

با افزایش تهدیدات فضای سایبری، افراد بسیاری نسبت به جرایم سایبری اضطراب پیدا کرده‌اند که موجب افزایش آگاهی درباره امنیت سایبری در تمام جامعه شده است. با توجه به این موقعیت‌ها، ضروری است که همه نهادهای ذی‌نفع به طور مستقل آگاهی امنیتی خودشان را بالا برده و به طور فعال در این زمینه فعالیت کنند، در حالی که همزمان

محیطی فراهم کنند که از وجود امنیت سایبری چند لایه با همکاری دیگر نهادهای ذی‌نفع در آن اطمینان حاصل شده است.

(۱) ایجاد فضای سایبری امن و ایمن برای کاربران

از آنجا که جرایم سایبری و حملات سایبری پیچیده‌تر و بغرنج‌تر می‌شوند و انواع مختلفی از حمله به وجود می‌آید، دیگر نمی‌توان تنها با تمهیدات منفعل سنتی با آن‌ها مقابله کرد و نیاز به اجرای تمهیداتی فعال‌تر از تمهیدات قبلی وجود دارد.

با توجه به این موقعیت، دولت با همکاری شرکت‌های مرتبط به فضای سایبری، سیاست «دفاع فعال سایبری»[۱] را تبلیغ خواهد کرد که اطمینان حاصل می‌کند دولت از تمهیدات پیشگیرانه فعالی برای جلوگیری از تهدیدات استفاده خواهد کرد. به‌ویژه دولت تلاش خواهد کرد که چنین طرح‌هایی را برای جلوگیری از خسارات حاصل از جرایم سایبری یا حملات سایبری تشویق کند، مثل تشویق به اشتراک‌گذاری و استفاده از اطلاعات تهدیدها برای امکان‌بخشیدن به دفاع پیشگیرانه، استفاده از تکنولوژی برای وادار ساختن حمله‌ها به این که از حمله‌کننده اطلاعات جمع کنند و تنظیم تمهیداتی علیه بات‌نت‌ها.[۲]

دولت همچنین توسعه زیرساخت اطلاعاتی قابل اطمینان را ترویج خواهد داد که شامل تقویت کابل‌های زیردریایی بین‌المللی و دیگر زیرساخت‌ها می‌شود که اساس خدمات کلی نهادهای دولتی و اپراتورهای زیرساخت‌های حیاتی و غیره خواهد بود. دولت این مسئله را در نظر خواهد گرفت که چگونه ارزیابی قابل اعتماد بودن را تأیید کند و چگونه عمل تدارکات دولتی را تقویت کند و تمهیدات را پیش ببرد.

۱. طرحی که به طور فعال در مقابل حملات سایبری دفاع می‌کند.

۲. شبکه‌ای که کامپیوترهای شخصی و سایر وسایل را به هم متصل کرده که در نتیجه آلودگی ویروسی (بات‌ها) توسط مهاجم کاملاً قابل کنترل شده‌اند. به طور مخرب برای اعمالی مانند حملات منع سرویس توزیع‌شده و هرزنامه‌ای استفاده می‌شود. (منبع: آژانس تبلیغ تکنولوژی اطلاعات، ژاپن (IPA), Jouhou Sekyuriti Hakusyo ۲۰۱۷ (Information security white paper (2017))

علاوه بر این، دولت با تأمین‌کنندگان خدمات رمزارزها همکاری خواهد کرد تا تمهیداتی در نظر بگیرد که مردم بتوانند به طور ایمن در معامله رمزارزها فعالیت داشته باشند. همچنین در خصوص خودروهای خودران و پهپادها، دولت تمهیداتی در نظر خواهد گرفت که جلوی فعالیت غیرمجاز آن‌ها به خاطر حملات سایبری گرفته شود، چون ممکن است جان مردم را به خطر بیندازد. به‌ویژه در خصوص خودروهای خودران، دولت به پیشتازی خود در مناظرات مداوم در مجامع بین‌المللی در مورد ایجاد استانداردهای بین‌المللی برای امنیت سایبری ادامه خواهد داد.

(۲) تقویت تمهیدات علیه جرایم سایبری

همین طور که فضای سایبری به شکل رو به افزایشی بخشی از زندگی مردم شده است، جرایم سایبری به خاطر ظهور آسیب‌های نفوذ باج‌افزارها[1] در سطح جهانی و مواردی که در آن‌ها انتقال غیرمجاز مقادیر بالای پولی ظاهراً توسط عوامل مخرب علیه اپراتورهای تبادل رمزارزهای داخلی صورت گرفته، تبدیل به مسئله اجتماعی جدی‌ای شده است. در راستای اطمینان از ایمنی و امنیت مردم، دولت به تلاش خود ادامه خواهد داد تا وضعیت حقیقی جرایم سایبری را درک کند و توضیحاتی در خصوص چنین جرایمی ارائه دهد، در حالی که همزمان با مؤسسات و سازمان‌های مرتبط همکاری خواهد کرد تا کمپین‌های آگاهی عمومی برگزار کرده از هر فرد بخواهد تمهیدات مستقلی علیه جرایم سایبری تبلیغ کند. به‌علاوه، توانایی‌های تحقیقاتی و تکنولوژیک نیز برای مقابله با انواع جدید جرایم سایبری ضروری است.

به این منظور، دولت به تبلیغ از طریق فعالیت‌های تحقیقاتی، در نظر گرفتن

۱. نوعی بدافزار که داده‌ها را رمزنگاری کرده و بعد طلب باج می‌کند.

تکنیک‌های بازرسی جدید و کمپین‌های آگاهی عمومی برای جلوگیری از جرایم سایبری ادامه خواهد داد. دولت با هدف مقابله با جرایمی که در آن‌ها از تکنولوژی‌های اطلاعات و ارتباطات پیشرفته استفاده می‌شود، توانایی‌های دیجیتال دادگاهی خود را تقویت کرده، قدرت تکنولوژیک خود را برای تحلیل جدیدترین دستگاه‌های دیجیتال یا بدافزارها تقویت کرده و قدرت تحلیل جامع خود را برای پیش‌بینی تهدیدهای فضای سایبری و برای گره‌گشایی از آن تهدیدها به وسیله تکنولوژی تقویت خواهد کرد. دولت به تبلیغ استفاده مثبت از دانش و تجربه‌ی شرکت‌های خصوصی، تبادل پرسنل بین بخش‌های دولتی و خصوصی، و تمهیداتی برای مقابله با جرایم سایبری که در آن‌ها، تحت شعاع به‌اشتراک‌گذاری اطلاعات، تحلیل اطلاعات، پیشگیری از خسارات جرایم سایبری و توسعه منابع انسانی، بخش‌های دولتی و خصوصی با یکدیگر همکاری خواهند داشت نیز خواهد پرداخت.

و در صورت رخ دادن جرایم سایبری، ضروری است که از قبل ردگیری بودن آن در فضای سایبری برای تحقیقات بیشتر اطمینان حاصل کرد. از آنجا که همکاری با اپراتورهای تجاری مرتبط با همکاری بین‌المللی برای این مسئله ضروری است، دولت هر طرح ضروری برای این مقصود را به کار خواهد بست. دولت به‌ویژه در خصوص حفاظت مناسب از گزارش داده‌های تاریخچه ارتباطات بر اساس راهنماهای مرتبط،[1] از اپراتورهای تجاری مرتبط خواهد خواست که تمهیدات لازم را اجرا کنند.

۳-۲-۲ حفاظت از زیرساخت‌های حیاتی از طریق همکاری بخش‌های دولتی و خصوصی

دولت در خصوص حفاظت از زیرساخت‌های حیاتی طرح‌هایی را براساس

۱. توضیح «راهنمای حفاظت از اطلاعات شخصی در شرکت‌های ارتباط از راه دور»

مجموعه‌ای از پنج گروه سیاست «سیاست‌های امنیت سایبری برای حفاظت از زیرساخت‌های حیاتی (ویرایش چهارم)»[1] که از این پس به آن «سیاست امنیت سایبری» گفته می‌شود) و براساس مفهوم «اطمینان از مأموریت» اجرا کرده است تا به طور ایمن و مداوم خدمات زیرساخت‌های حیاتی را تأمین کند.[2] اگرچه این مشکل باقی می‌ماند که سطح آگاهی درباره امنیت سایبری و پیشرفت در طرح‌ها بین هر بخش زیرساخت‌های حیاتی متفاوت است. به همین دلیل، دولت با بخش‌های خصوصی همکاری خواهد داشت تا همزمان با تلاش هر نهاد ذی‌نفع درخصوص تمهیدات مستقل خود حمایت فعال برای آن‌ها به‌وجود بیاورد. این تلاش‌ها شامل در نظر گرفتن الگوهایی برای تمهیدات امنیت سایبری در مورد اپراتورهای زیرساخت‌های حیاتی با منابع محدود مدیریتی می‌شود که برایشان سرمایه‌گذاری کافی در امنیت سایبری دشوار است.

(۱) طرح‌های اولیه براساس «سیاست امنیت سایبری»

تا امروز، دولت «سیاست امنیت سایبری» را برای حفاظت از زیرساخت‌های حیاتی تنظیم و اصلاح کرده است و به اجرای طرح‌ها براساس «سیاست امنیت سایبری» ادامه خواهد داد. طبق برنامه‌ریزی زمانی، «سیاست امنیت سایبری» پس از بازی‌های ۲۰۲۰ توکیو مورد بررسی دوباره قرار خواهد گرفت. اگرچه اگر نیاز باشد پیش از آن تاریخ هم مورد بررسی قرار خواهد گرفت، یعنی اگر تغییرات بزرگی در جهت حرکت جامعه به وجود بیاید.

بخش‌های زیرساخت‌های حیاتی از این نظر معیّن می‌شوند که به‌ویژه به این دلیل نیاز به محافظت دارند که تا چه حد در زندگی و فعالیت‌های اقتصادی و اجتماعی مردم تأثیر می‌گذارند. از نظر شرایط اجتماعی، دولت

۱. تصمیم مقر استراتژیک امنیت سایبری در ۱۸ آوریل ۲۰۱۷

۲. پنج گروه سیاست: حفظ و ترویج اصول ایمنی، تقویت سیستم به‌اشتراک‌گذاری اطلاعات، تقویت توانایی پاسخگویی به حوادث، مدیریت ریسک و تهیه آمادگی برای بروز حادثه، و تقویت مبانی CIP.

مقیاس اپراتورها و بخش‌های زیرساخت‌های حیاتی را گسترش داده تا هرطور که لازم است مقیاس طرح‌های امنیتی را گسترش داده و «حفاظت به مثابه هواپیما» را تقویت کند. همزمان طرح‌های مبنی بر به‌اشتراک‌گذاری اطلاعات و گسترش و تقویت سیستم‌های به‌اشتراک‌گذاری اطلاعات را ترویج می‌دهد.

علاوه بر این، مشارکت فعال مدیران ارشد در اپراتورهای زیرساخت‌های حیاتی برای ترویج طرح‌های حفاظت از زیرساخت‌های حیاتی ضروری است. به همین دلیل، دولت با مدیران ارشد تماس برقرار خواهد کرد تا آگاهی آن‌ها در زمینه امنیت سایبری را بالا ببرد و همزمان طرح‌های زیر را تبلیغ کند:

(الف) ترویج مدیریت ریسک

تأمین مداوم و ایمن خدمات زیرساخت‌های حیاتی حتی هنگام حملات سایبری ضروری است. به همین دلیل، علاوه بر اجرای تمهیدات امنیتی از قبل، مهم است که اپراتورهای زیرساخت‌های حیاتی مبتنی بر نتایج ارزیابی ریسک با توجه به ریسک‌های پیچیده و بین سازمانی، بر اساس مفهوم اطمینان از مأموریت، طرح ادامه تجارت (BCP)[1] و طرح احتمال وقوع حادثه آماده کرده باشند.

(ب) تقویت و ترویج اصول امنیتی

به منظور ترویج مدیریت صحیح توسط اپراتورهای زیرساخت‌های حیاتی، دولت به ترویج بیشتر خط مشی‌ها برای آمادگی اصول امنیتی ادامه خواهد داد، در حالی که ترویج طرح‌هایی برای تقویت آن اصول امنیتی را هم پیش خواهد برد. این اصول شامل پیشنهاد روش‌هایی برای مدیریت داده‌ها و کاهش ریسک‌های مرتبط با عوامل انسانی برپایه نظرسنجی در خصوص

1. Business Continuity Plan

وضعیت فعلی مدیریت داده‌ها و گرایش‌های بین‌المللی مرتبط، در نظر گرفتن چنین مسائلی به عنوان محتوای تجارت، اندازه سازمان‌ها، طول مدت استفاده از سیستم و تأثیر روی رقابت بین‌المللی می‌شود. به‌علاوه از منظر حفظ ایمنی، دولت به طور مناسب چارچوب‌های سازمانی را با استفاده از ابزارهایی از جمله تنظیم تمهیدات امنیت سایبری به عنوان مقررات ایمنی در قوانین و مقررات مربوط و غیره تقویت می‌کند.

(ج) مقیاس شدت حادثه سایبری NISC برای قطعی برق کشورهای مستقل همسود

با توجه به گرایش‌های اخیر در حملات سایبری، ضروری است که به نهادهای ذی‌نفع، از جمله نهادهای دولتی و اپراتورهای زیرساخت‌های حیاتی این امکان را بدهیم که به‌سرعت درک خود را به‌اشتراک بگذارند و زمانی که حمله‌ای سایبری را تشخیص دادند تعیین کنند که نیاز به واکنش سریع وجود دارد یا نه. به همین منظور، دولت «مقیاس شدت حادثه سایبری NISC برای قطعی برق کشورهای مستقل همسود» را آماده خواهد کرد و شدت حوادث را ارزیابی و منتشر خواهد کرد تا نهادهای ذی‌نفع مختلف را تشویق کند و به آن‌ها این امکان را بدهد که واکنشی منطقی و مناسب داشته باشند و همزمان تأثیر اطلاع‌رسانی کامل به مردم را در نظر داشته باشند. دولت همچنین این مقیاس را در زمان‌های مناسب بررسی خواهد کرد تا آن را تقویت کند.

(د) آموزش و تمرین مشترک بین بخش‌های دولتی و خصوصی

با این فرض که ظهور قطعی خدمات توانایی‌های اپراتورهای زیرساخت‌های

حیاتی را افزایش خواهد داد تا بتوانند واکنشی مناسب به این موقعیت‌ها نشان دهند آموزش و تمرین حائز اهمیت است. دولت و سازمان‌های مرتبط به اجرای آموزش و تمرین بین نهادهای ذی‌نفع در اندازه‌های مختلف و در بخش‌های دولتی و خصوصی ادامه خواهد داد، دامنه طرح‌ها را گسترش داده و در صورت لزوم برای ادامه توسعه، محتوای آن‌ها را بهبود خواهد بخشید.

(ه) تمهیدات امنیتی برای سیستم‌های کنترل صنعتی (ICS)

اپراتورهای زیرساخت‌های حیاتی‌ای مثل برق، گاز و نفت هستند که از سیستم‌های کنترل صنعتی (ICS) استفاده می‌کنند تا خدماتشان را تأمین کنند. در این موارد، وقتی چنین ICSهایی به‌شدت تحت تأثیر حملات سایبری و موارد مشابه قرار بگیرند و تأثیری عظیم بر زندگی مردم بگذارند، احتمال اینکه تأمین عادی خدمات غیرممکن شود، زیاد است. به همین دلیل، بخش‌های دولتی و خصوصی برای ترویج توسعه منابع انسانی با توجه به ICS متحد خواهند شد و در صورت نیاز به جمع‌آوری، تحلیل و به‌کارگیری اطلاعات تهدیدها خواهند پرداخت تا تمهیدات امنیتی مناسب بر اساس خصوصیات ICS برای تأمین ایمن و مداوم خدمات اجرا شوند.

(۲) تقویت و بهبود امنیت در حکومت‌های محلی

خدماتی که حکومت‌های محلی ارائه می‌دهند، ارتباطی نزدیک با زندگی مردم دارد و هر مانعی بر سر راه تأمین این خدمات می‌تواند تأثیری عظیم و فعال بر جامعه داشته باشد. اگرچه محدودیت‌هایی برای راه‌حل‌های فنی‌ای وجود دارد که ممکن است برای تمهیدات امنیت سایبری به طور جداگانه توسط سازمان‌هایی با منابع محدود انجام شود، اما پیش از همه ضروری

است که اقدامات متقابل در برابر نشت اطلاعات از جمله کد ملی، به دلیل قطعی خدمات یا خطای انسانی اجرا شود.

با توجه به این موقعیت و در حالی که مشارکت مستقیم[1] حکومت مرکزی در حکومت‌های محلی به دلیل تقسیم فعلی نقش‌ها بین حکومت مرکزی و حکومت‌های محلی در مقایسه با دیگر سازمان‌ها محدود است، حکومت‌های محلی سراسر کشور مشغول تقویت اساسی تمهیدات شده‌اند و حکومت مرکزی خط مشی خود درباره سیاست امنیت را در صورت لزوم با توجه به الزام رسیدن به سطح بالای امنیت به‌روز خواهد کرد. دولت همچنین تلاش خواهد کرد تا به سطوح لازم امنیت برای شبکه‌های قابل استفاده برسد و طرح‌های مربوطه را ترویج بدهد تا منابع انسانی امنیت سایبری را توسعه دهد و ایمن سازد، سیستم‌ها را تقویت کند و بودجه لازم را تأمین کند، در حالی که به نیاز عملکرد روان حکومت‌های محلی نیز توجه می‌کند.

علاوه بر این، با توجه به اتفاق هویت بین بخش‌های دولتی و خصوصی، دولت تلاش خواهد کرد که محیط را بین دو حالت آسان و ایمن در تعادل نگه داشته و آن را تقویت کند.

۳-۲-۳- تقویت و بهبود امنیت در نهادهای دولتی و موجودیت‌های مرتبط با دولت

تا امروز، از طریق توسعه تمهیدات امنیت اطلاعات براساس استانداردهای یکپارچه، طرح‌هایی برای رسیدگی براساس همان استانداردها و نظارت بر ارتباطات غیرمجاز، در جهت افزایش سطح تمهیدات امنیت اطلاعات برای نهادهای دولتی به طور کلی، تلاش‌هایی صورت گرفته است و دولت موظف

۱. اتحاد و رسیدگی به خصوصیات فنی.

است به تلاش در راستای این طرح‌ها ادامه دهد. چارچوب طرح‌ها در آژانس‌های مدیریتی مشترک و شرکت‌های معین (که از این پس به آن «آژانس‌های مدیریتی مشترک و غیره» گفته می‌شود) همان‌گونه گسترش پیدا کرده که نهادهای دولتی به واسطه بازبینی در قانون اساسی امنیت سایبری[1] گسترش پیدا کردند و این مسئله در حرکت روبه‌جلو به سمت ترویج تمهیدات مؤثر امنیت اطلاعات در آژانس‌های مدیریتی مشترک و غیره با توجه به خصوصیات صورت‌های مختلف تجاری‌شان، حائز اهمیت خواهد بود.

برای واکنش به حملات سایبری پیچیده و بغرنج، باید از تکنولوژی‌های جدید استفاده کنیم تا به وضعیت فعلی که در آن مهاجم‌ها از برتری برخوردارند غلبه کنیم، در حالی که همزمان سیستم دفاعی را عمیقاً تقویت کرده و فرض کنیم که این حملات قطعاً رخ خواهند داد و اقداماتی متقابل برای ریسک‌های زنجیره تأمین در نظر بگیریم.

اجرای روان خدمات دولتی مسئولیتی بسیار مهم برای نهادهای دولتی و آژانس‌های مدیریتی مشترک و غیره (که از این پس به آن‌ها «آژانس‌ها» گفته خواهد شد) است و انجام سرمایه‌گذاری‌های لازم در فناوری اطلاعات و سرمایه‌گذاری‌های مرتبط با امنیت به طور همزمان با سرمایه‌گذاری برای سیستم‌ها از اهمیت بالایی برخوردار است. با توجه به این وضعیت، ضروری است که بودجه‌ی لازم برای تقویت سرمایه‌گذاری‌های مرتبط با امنیت تأمین شود. به این منظور می‌توان برای مثال از بودجه ایجاد شده توسط سرمایه‌گذاری سازمان‌ها در حوزه فناوری اطلاعات به طور مؤثرتری در زمینه امنیت استفاده کرد، و تمهیدات امنیت اطلاعات را که در بالا ذکر شد، تقویت کرد.

۱. مصوب ۱۵ آوریل ۲۰۱۶. دامنه آن طوری گسترش پیدا کرد که نظارت، رسیدگی و بازرسی دلایل یا ارتباطات غیرمجاز توسط دولت را هم پوشش دهد.

(۱) بهبود و تصویرسازی تمهیدات امنیتی برای سیستم‌های اطلاعاتی

آژانس‌ها از تکنولوژی‌های جدید دفاعی برای اجرای طرح‌های مؤثرتر استفاده خواهند کرد، نه تنها با هدف افزایش توانایی پاسخ در برابر تهدید فزاینده حملات سایبری، بلکه همچنین برای جلوگیری از خسارات، و در صورت بروز خسارات جلوگیری از گسترش آن‌ها و به حداقل رساندن خسارت استفاده می‌کنند.

(الف) افزایش توانایی‌های دفاعی و آگاهی شرطی برای سیستم‌های اطلاعاتی

آژانس‌ها با شناسایی رفتار بدافزار در نقطه پایانی (کامپیوتر شخصی و غیره) در جایی که برنامه‌ها اجرا می‌شوند، از قبل تلاش می‌کند جلوی خسارت را بگیرند و از گسترش آن جلوگیری کنند. به واسطه اتوماسیون مدیریت دارایی‌های فناوری اطلاعات، آژانس‌ها وضعیت سیستم‌های اطلاعاتی را به طور زنده کنترل کرده و امکان مدیریت سریع آسیب‌پذیری‌های نرم‌افزار را فراهم می‌کنند. طرح‌های محافظت از داده‌ها نیز برای همه آژانس‌ها انجام می‌شود تا از بروز نشت اطلاعات هنگام وقوع حوادث جلوگیری شود. علاوه بر این، ضروری است که تمهیدات لازم برای شناسایی حملاتی که به‌سختی به‌واسطه تحلیلِ تهدید شناسایی می‌شوند مورد بررسی قرار گرفته، پدیده‌هایی که روی دستگاه‌های مختلف و اطلاعات مدیریت حساب رخ می‌دهند با هم ترکیب شوند. برای به‌کارگیری مؤثر این تمهیدات، باید سیستم‌هایی با هدف اتوماسیون کار مورد نیاز برای تحلیل اطلاعات ایجاد شوند.

(ب) جلوگیری از خسارات و گسترش آن‌ها از طریق همکاری بین‌سازمانی پیشرفته بین سازمان‌ها

با توجه به وضعیت اجرای نظارت بر بدافزار بر روی دستگاه‌ها و اتوماسیون مدیریت دارایی‌های فناوری اطلاعات در همه مراحل از جمله پیشگیری، شناسایی، بازیابی و پاسخگویی، آژانس‌ها با توسعه یک همکاری مؤثر و کارآمد بین سازمان‌ها و GSOC [1] که شامل به‌اشتراک‌گذاری مناسب اطلاعاتی که از این تمهیدات به دست می‌آید با GSOC می‌شود، سعی می‌کنند طرح‌های بین‌سازمانی را توسعه دهند.

(۲) ترویج استفاده از فضای ابری برای تمهیدات امنیتی مؤثر

برای اینکه هر آژانس بتواند با توجه به ویژگی‌های اطلاعات، شکل مناسبی از سیستم اطلاعاتی را انتخاب کند و تمهیدات امنیتی برای تمام دولت به طور مؤثر و کارآمد اجرا شود، دولت استفاده از خدمات ابری از جمله مهاجرت به پلتفرم مشترک دولت به شکل فضای ابری خصوصی دولت را تبلیغ می‌کند که می‌تواند از مزایای تلفیق ساخت و بهره‌برداری از سیستم‌ها و افزایش سطح امنیت بهره ببرد. برای تشویق به استفاده از فضای ابری، دولت تمهیداتی را برای تبلیغ استفاده از خدمات ابری قابل‌اعتمادی که سطح امنیتی مطلوبی مانند ارزیابی ایمنی در آن تأمین شود، در نظر می‌گیرد و اجرا می‌کند.

با توجه به خطوط اتصال اینترنت، دولت همچنین برای یکپارچه‌سازی و تلفیق درگاه اتصال تحت استاندارد مشترک تلاش کرده است. دولت ضمن همکاری با شبکه‌ها و پلتفرم‌های مشترک دولت، ملاحظات لازم از جمله تلفیق نقاط نظارت محیطی را در نظر خواهد گرفت، زیرا ترویج بیشتر

۱. سرواژه Government Security Operation Coordination Team (تیم هماهنگی عملیات‌های امنیتی دولت). این تیم مسئولیت نظارت بین‌سازمانی و واکنش سریع برای امنیت اطلاعات نهادهای دولتی را برعهده دارد.

تلفیق مناسب درگاه‌های اتصال اینترنت برای نهادهای دولتی برای اقدامات و تمهیدات امنیتی بسیار مؤثر است.

(۳) تلاش‌های پیشگیرانه با استفاده از فناوری‌های پیشرفته

برخی از پلتفرم‌های سیستم اطلاعاتی که در سال‌های اخیر مورد استفاده قرار گرفته‌اند، از سطح مقاومت بالایی در برابر حملات سایبری برخوردار هستند. دولت تکنولوژی‌های اطلاعاتی ایجاده شده تحت این فلسفه جدید طراحی را برای آژانس‌ها در نظر می‌گیرد، تلاش می‌کند دانش بهترین روش‌ها را جمع‌آوری کند و سعی می‌کند وضعیت را به نفع مدافع تغییر دهد.

(۴) افزایش سطح امنیت سایبری از طریق رسیدگی

با توجه به قانون اساسی امنیت سایبری، دولت گرایش‌ها و مسائلی را که از طریق تحلیل بین‌سازمانی داده‌ها از رسیدگی به آژانس‌ها شناسایی کرده است، برای ترویج رشد بیشتر سطح امنیت سایبری به عنوان بازخوردی به تمام آژانس‌ها ارائه می‌دهد. علاوه بر این، دولت از اطلاعات مدیریت دارایی‌های فناوری اطلاعات آژانس‌ها استفاده خواهد کرد که مطابق با طرح‌های نظارت مؤثر بر وضعیت آن سیستم‌ها تهیه شده‌اند و تلاش خواهد کرد که به اجرای کارآمد و مؤثر رسیدگی دست پیدا کند.

(۵) تقویت توانایی واکنش سازمانی

دولت در ابتدا از طریق تیمی که حوادث را مدیریت می‌کند،[۱] توانایی واکنش به حوادث و دانش امنیت اطلاعات هر آژانس را افزایش می‌دهد. در صورت بروز حملات سایبری به آژانس‌ها، دولت آموزش و غیره را برای

۱. CSIRT (تیم واکنش به حوادث امنیت کامپیوتری)

ایجاد توانایی مقابله در کارمندان برگزار می‌کند تا تشکیلات کمکِ سیار (تیم کمک اضطراری برای امنیت اطلاعات)[1] را تقویت کند. این تیم از کارمندان دولت با دانش و مهارت کافی از هر آژانس دولتی تشکیل شده است.

۳-۲-۴- ایجاد محیط آموزشی و پژوهشی امن و ایمن در دانشگاه و غیره

دانشگاه‌ها و مؤسسات پژوهشی بین دانشگاهی و غیره (که از این به بعد به آن‌ها «دانشگاه‌ها و غیره» گفته می‌شود) از کارکنانی شامل اعضای مختلف با مجموعه‌ای متنوع از دارایی‌های فناوری اطلاعات و سیستم‌های مورد استفاده تشکیل شده‌اند. با توجه به ماهیت این دانشگاه‌ها و غیره، در کنار اجرای تمهیدات امنیت سایبری مستقل توسط خود دانشگاه‌ها و غیره، مهم است که دولت به طور فعالانه از ایجاد سیستم واکنش و به‌اشتراک‌گذاری اطلاعات و غیره برای مقابله با حملات سایبری از طریق همکاری بین دانشگاه‌ها و غیره به منظور اطمینان از ایجاد یک محیط آموزشی و پژوهشی امن و ایمن حمایت کند.

(۱) ترویج تمهیدات با توجه به تنوع در دانشگاه‌ها و غیره

مدیران ارشد دانشگاه‌ها و غیره باید شخصاً اهمیت تمهیدات امنیت سایبری را درک کنند، تمهیدات امنیت سایبری را موضوعات مهم مدیریتی در نظر بگیرند، و در جایگاه سازمانی مبتنی بر برنامه ترویج تمهیدات امنیت سایبری طرح‌ها را اجرا کنند و در عین حال پیگیر ترویج بیشتر تمهیدات امنیت سایبری باشند.

برای این کار، ضروری است که دارایی‌های فناوری اطلاعات را برای محافظت

۱. CYMAT (تیم کمک سیار به حوادث سایبری)

از آن‌ها شناسایی کنیم، ریسک‌های امنیت سایبری را ارزیابی کنیم، و هنگام اجرای تمهیدات مدیریتی و فنی با توجه به آن ریسک‌ها آن تمهیدات را در اولویت قرار دهیم و در عین حال تنوع افراد در دانشگاه‌ها و غیره را در نظر بگیریم که در حوزه‌های مختلف به آموزش و پژوهش می‌پردازند. علاوه بر این، دانشگاه‌ها و مؤسسات پژوهشی باید طرح‌هایی نیز در نظر بگیرند که توانایی واکنش سریع و مناسب به حوادث را تقویت کند و سیستمی برای اجرای سازمانی و پایدار تمهیدات طراحی کنند.

دولت با ایجاد و انتشار خط مشی‌های مربوط به امنیت سایبری، اجرای روشی برای هر سطح با توجه به مدیریت ریسک و واکنش به حادثه، آموزش و تمرین عملی و حمایت از واکنش اولیه در صورت وقوع حادثه، طرح‌های مستقل و سازمانی دانشگاه‌ها و غیره را ترویج خواهد داد.

(۲) ترویج طرح‌های هماهنگ و مشترک توسط دانشگاه‌ها و غیره

دانشگاه‌ها و غیره از پلتفرم‌های اطلاعاتی رایج استفاده می‌کنند و با معضلات امنیت سایبری مشابه مواجه‌اند.

تقویت تمهیدات امنیت سایبری با توجه به این شرایط واقعی در دانشگاه‌ها و غیره، مهم در نظر گرفته می‌شود و نیاز به ترویج بیشتر طرح‌ها از طریق همکاری متقابل تمام طرفین وجود دارد.

به همین دلیل، سازمان‌هایی که شبکه‌های اطلاعات علمی را مدیریت می‌کنند، با دانشگاه‌های ملی و غیره همکاری می‌کنند تا سیستمی برای نظارت، شناسایی و تحلیل حملات سایبری توسعه بدهند و در مورد آن حملات اطلاعات تهیه کنند، در حالی که همزمان پژوهش‌های مشترک انجام می‌دهند و کارکنان فنی‌ای آموزش می‌دهند تا عملکرد توانایی‌های

نظارتی را حفظ و تقویت کنند و سطح مدیریت استراتژیک به‌وجود بیاورند و برای کارکنان فنی آموزش بگذارند.

برای تقویت تیم‌های واکنش به حوادث در آن دانشگاه‌ها و غیره، دولت از طرح‌هایی نیز حمایت خواهد کرد که طی آن‌ها تیم‌ها مدیریت حادثه چند دانشگاه و سازمان پژوهشی اطلاعاتشان، مشکلات مشترکشان و دانشی که از واکنش به حادثه‌ی مربوط به حملات سایبری کسب کرده‌اند را با هم به‌اشتراک بگذارند.

۳-۲-۵- طرح‌هایی برای بازی‌های ۲۰۲۰ توکیو و پس از آن

ورزشکاران، بزرگان و طرفداران خارجی بی‌شماری از سراسر جهان برای بازی‌های المپیک و پارالمپیک گرد هم می‌آیند و به میزبان این رویداد بالاترین سطح توجه ممکن را می‌دهند و آن را به‌طور بالقوه هدف حملات سایبری قرار می‌دهند.

با نگاهی به بازی‌های المپیک و پارالمپیک گذشته، طبق گزارشات حملات سایبری زیادی در طول بازی‌های ۲۰۱۲ لندن رخ داده است، اگرچه آن‌ها تأثیری در عملکرد این رویداد نداشته‌اند. به همین ترتیب، طبق برخی گزارش‌ها تعداد قابل توجهی حمله سایبری باعث خسارت به بازی‌های ۲۰۱۶ ریو دو ژانیرو و بازی‌های ۲۰۱۸ پیونگ یانگ شدند. همچنین انتظار می‌رود که بازی‌های ۲۰۲۰ توکیو بیش از گذشته مورد حمله سایبری قرار بگیرند و طبیعتاً برخی از حملات چندین بخش خدمات را هدف قرار خواهند داد. به همین دلیل دولت امنیت سایبری بازی‌های ۲۰۲۰ توکیو را تضمین می‌کند و تمهیدات بیشتری برای پس از این رویداد در نظر می‌گیرد.

ایـن تمهیـدات مختلف بعد از بازی‌های ۲۰۲۰ توکیو از نظر دامنه گسـترش یافتـه و ادامـه خواهد یافت و میراث سیسـتم‌های توسـعه‌یافته و تجربه و دانش عملیـات آن‌هـا بـرای تقویـت امنیت سـایبری در ژاپن به طـور مـداوم در آینده مورد اسـتفاده قـرار خواهد گرفت.

(۱) آماده‌بودن برای بازی‌های ۲۰۲۰ توکیو

براسـاس اسـتراتژی اساسـی[۱] کـه در جلسـه هیئـت امنیت سـتاد بازی‌های المپیـک و پارالمپیـک ۲۰۲۰ توکیـو بـه تصویـب رسـید، دولـت به جمـع‌آوری اطلاعـات مرتبـط بـا امنیـت بازی‌هـا و دیگـر تمهیـدات ادامـه خواهـد داد. همچنیـن ارزیابـی منابـع امنیـت سـایبری را نیـز بـا در نظر گرفتـن هماهنگی بـا امنیـت فیزیکی انجـام خواهد داد و ریسـک امنیت سـایبری تأمین‌کنندگان خدمـات حیاتـی را نیز ارزیابی خواهـد کرد که احتمال تأثیرگـذاری در عملکرد بازی‌هـای ۲۰۲۰ توکیـو را دارنـد، از جملـه در نظر گرفتن سـناریوهای ریسـک براسـاس نتایـج ارزیابـی منابع ریسـک امنیـت سـایبری، و به ترویـج تمهیدات بـرای ریسـک‌های مختلف از جمله ریسـک‌های بین‌بخشـی که توسـط ارزیابی ریسـک شناسـایی شـده‌اند، خواهـد پرداخـت. عـلاوه بـر به‌اشـتراک‌گذاری اطلاعـات دربـاره تهدیدات امنیت سـایبری بین سـازمان‌های مرتبط با المپیک، از جملـه وزارت‌هـا و آژانس‌هـای دولتـی مرتبط، کمیته برگزار کننـده بازی‌های المپیـک و پارالمپیـک توکیـو، حکومت کلان‌شـهر توکیـو، حکومت‌های محلی کـه محـل برگـزاری را تأمیـن می‌کننـد، و خدمات‌دهنـدگان مهـم، دولـت توسـعه مرکز هماهنگـی واکنش به حـوادث امنیت سـایبری (CSIRT المپیک و پارالمپیـک دولـت) را تبلیـغ خواهـد کـرد، سـازمانی کـه از طریـق آن دولـت نقـش هماهنگـی سـازمان‌های مرتبـط بـا المپیـک را برعهـده می‌گیـرد تـا

۱. استراتژی اساسی امنیت برای بازی‌های المپیک و پارالمپیک ۲۰۲۰ توکیو (جلسه هیئت امنیت شورای ارتباطی وزارتخانه‌ها و آژانس‌های مرتبط با بازی‌های المپیک و پارالمپیک ۲۰۲۰ توکیو، ۲۱ مارس ۲۰۱۷)

بتوانند در صورت بروز حادثه با یکدیگر به حوادث امنیت سایبری واکنش نشان دهند، یا برای حصول اطمینان از آمادگی برای ارتباط و هماهنگی از نزدیک با یکدیگر همکاری کنند.

(۲) انتقال نتایجی که به آینده ختم می‌شود

دولت در راستای آماده‌سازی برای بازی‌های ۲۰۲۰ توکیو به ترویج تمهیدات مختلف خواهد پرداخت و سیستم توسعه‌یافته و تجربه عملیاتی و دانش این سیستم‌ها به عنوان میراث برای تقویت امنیت سایبری ادامه‌دار ژاپن پس از بازی‌های ۲۰۲۰ توکیو استفاده خواهد شد. به علاوه، مرکز هماهنگی واکنش به حوادث امنیت سایبری (CSIRT ملی) به عنوان سازمانی با هدف هماهنگی بین همه ژاپن برای همکاری در مقابله با حملات سایبری استفاده خواهد شد. روش‌هایی که برای مدیریت ریسک در چشم‌انداز اساسی امنیت سایبری توصیف شده است برای کاربرد گسترده در اپراتورهای تجاری سرتاسر کشور تنظیم و توزیع خواهد شد.

۳-۲-۶- ساخت چارچوب همکاری و به‌اشتراک‌گذاری اطلاعات که از چارچوب‌های سنتی فراتر می‌رود

اساساً ایجاد امنیت سایبری باید طرحی باشد که هر سازمان با توجه به ارزش دارایی داده‌هایش و وضعیت کاربری تکنولوژی ارتباطات و اطلاعاتش به طور مستقل انجام دهد. در همین حال، به دلیل تغییر در حالات حمله، محدودیتی در توانایی ایجاد اقدامات متقابل مؤثر در برابر حملات سایبری در یک سازمان واحد وجود داشته است. به همین دلیل، آگاهی در بخش‌های دولتی و خصوصی به طور پیوسته در حال گسترش است که بر همکاری

با سازمان‌های دیگر تأکید دارد، و نه فقط نهادهای مدیریتی و اپراتورهای زیرساخت‌های حیاتی، بلکه طیف وسیعی از دیگر نهادهای ذی‌نفع نیز در حال کار بر روی به‌اشتراک‌گذاری اطلاعات‌اند.

از آنجا که تعداد بخش‌های نزدیک به فضای سایبری به دلیل افزایش تلفیق فضای سایبری و فضای واقعی بیشتر در حال رشد است، انتظار می‌رود دامنه بخش‌ها و ذی‌نفعانی که نیاز به اشتراک اطلاعات مرتبط با امنیت سایبری دارند همچنان گسترش یابد.

بر همین اساس، از منظر «مشارکت، هماهنگی و همکاری» که به عنوان بخشی از چشم‌انداز اساسی امنیت سایبری مطرح شده است، دولت باید از طریق هماهنگی نزدیک بین نهادهای ذی‌نفع از طرح‌های موجود برای سیستم‌های به‌اشتراک‌گذاری اطلاعات مانند ISAC،[1] حمایت کند، در حالی که نقش‌های جدیدی به‌عهده می‌گیرد.

(۱) ترویج به‌اشتراک‌گذاری اطلاعات و همکاری بین چند نهاد ذی‌نفع

با افزایش تعداد ذی‌نفعانی که در به‌اشتراک‌گذاری اطلاعات مشارکت دارند، اهمیت نقش جمع‌آوری و تحلیل اطلاعات و هماهنگی به‌موقع ذی‌نفعان نیز افزایش می‌یابد. در این میان، از آن‌جا که مدیریت نامناسب اطلاعات به‌اشتراک‌گذاشته‌شده امکان کاهش ارزیابی اجتماعی و اعتماد را به وجود می‌آورد، این مسئله همچنان باقی می‌ماند که ذی‌نفعان تمایلی به به‌اشتراک‌گذاری فعالانه داده‌های خود ندارند.

با توجه به این وضعیت، دولت برای ایجاد یک سیستم جدید تلاش خواهد کرد که به چند نهاد ذی‌نفع در بخش‌های دولتی و خصوصی، از جمله سازمان‌های متخصص با دانش و تجربه کافی در حوزه به‌اشتراک‌گذاری

۱. سرواژه مرکز به‌اشتراک‌گذاری و تحلیل اطلاعات (Information Sharing and Analysis Center). این سازمان اطلاعات مرتبط با امنیت سایبری را برای تحلیل جمع‌آوری می‌کند. داده‌های تحلیل‌شده با اعضای ISAC برای استفاده در تمهیدات امنیتی خودشان به‌اشتراک گذاشته می‌شود. (منبع: امنیت سایبری ۲۰۱۷ (۲۵ آگوست ۲۰۱۷))

اطلاعـات، ایـن امـکان را می‌دهـد کـه بـدون نگرانـی اطلاعاتی را که بـه امنیت سـایبری کمـک می‌کند، به‌اشـتراک بگذارنـد. هنگام انجـام ایـن کار، احترام به اسـتقلال هـر یـک از ذی‌نفعـان مطابق با اصل اسـتقلال کـه در اصول اساسـی مطـرح شـده اسـت حائـز اهمیـت خواهـد بـود. به‌اشـتراک‌گذاری اطلاعـات و هماهنگـی کـه از مرزهـای دولتی-خصوصـی، صنعتـی، ملـی، و دیگـر مرزهای بیـن بخش‌هـای دولتی و خصوصـی، صنایع و مبحث داخلـی و بین‌المللی فراتر بـرود، بـا اجرای ایـن طـرح ترویج خواهـد یافت.

دولـت همچنیـن بـا در نظـر گرفتـن خصوصیـات و نقش‌هـای هـر یـک از سیسـتم‌های موجـود به‌اشـتراک‌گذاری اطلاعـات در بخش‌هـای خصوصـی و دولتـی، همـکاری و اتحـاد بیـن آن‌هـا را نیـز در نظـر می‌گیـرد، بـه طـوری که طرفیـن مربـوط متحمـل بـار اضافـی بـرای سیسـتم جدید نشـوند.

(۲) به‌سوی مرحله‌ای جدید در به‌اشتراک‌گذاری اطلاعات و همکاری

برای توسـعه یک سیسـتم جدید به‌اشـتراک‌گذاری اطلاعات، دولت ساختاری را در نظـر خواهـد گرفـت کـه در آن ذی‌نفعان می‌توانـد روابطی بـر پایه اعتماد ایجـاد کننـد و در آن هـر چـه بیشـتر در تأمیـن اطلاعـات با یکدیگـر همکاری و هماهنگـی داشـته باشـند، بیشـتر از مزایـای سیسـتم بهره‌منـد می‌شـوند.

هـر چـه سـطح همـکاری و هماهنگی بـا طرفین دیگر افزایـش یابد، مزایای مشـارکت در سیسـتم به‌اشـتراک‌گذاری اطلاعـات بیشـتر می‌شـود. بـر همین اسـاس، دولـت بایـد در به‌اشـتراک‌گذاری مناسـب اطلاعاتی که در اختیـار دارد پیشـگام باشـد. دولت همچنین محیطی ایجاد خواهد کرد که در آن ذی‌نفعانی کـه بـه طـور فعالانه اطلاعات خـود را در مورد مسـائلی از جمله حـوادث امنیت سـایبری به‌اشـتراک می‌گذارنـد، مورد توجه مثبـت قرار می‌گیرند. به‌طـور ویژه،

ضروری است که اطلاعات مربوط به امنیت سایبری که باعث فراخوانی برای محافظت از زندگی و رفاه جسمی افراد می‌شود، به‌سرعت و مطمئناً به‌اشتراک گذاشته شود. دولت همچنین تلاش خواهد کرد که به تحلیل و به‌اشتراک‌گذاری مناسب و سریع اطلاعاتی که واقعاً مورد نیاز هر ذی‌نفع است از طریق ترویج پردازش خودکار اطلاعات دریافتی و سایر روش‌ها دست یابد.

از طریق این طرح، درک این نکته که به‌اشتراک‌گذاری متقابل اطلاعات برای افزایش امنیت سایبری ضروری است، در کل جامعه پرورش می‌یابد. علاوه بر این، هدف قرار دادن همکاری استراتژیک با جامعه بین‌الملل نیز ضمن توسعه سیستم به‌اشتراک‌گذاری اطلاعات در ژاپن، ضروری است. دولت همکاری نزدیکی با هر یک از ذی‌نفعان خواهد داشت و به طور فعالانه در جهت بهبود محیط لازم تلاش خواهد کرد تا هر یک از نهادهای ذی‌نفع را قادر به ایجاد روابط همزیستی و توسعه متقابل کند که از مرزهای متعارف بخشیِ مرتبط با صنایع و بخش‌های دولتی و خصوصی فراتر برود. این امر باعث می‌شود که به‌اشتراک‌گذاری اطلاعات و همکاری در زمینه امنیت سایبری به مرحله جدیدی منتقل شود.

۳-۲-۷- تقویت آمادگی برای حوادث در مقابل حملات گسترده سایبری

حملات سایبری در خارج از کشور اتفاق افتاده است و تأثیری چشم‌گیر در زندگی مردم گذاشته، موجب قطع گسترده برق یا خسارات جزئی به عملکرد مؤسسات مالی شده است. با ادامه تلفیق فضای سایبری و فضای واقعی، این احتمال وجود دارد که حملات سایبری در آینده باعث بروز حوادثی در فضای واقعی در کشور ما بشود. علاوه بر این، می‌توان انتظار

داشت که حملات گسترده سایبری باعث خسارت همزمان خدماتی شود که در حالت عادی به یکدیگر ارتباطی ندارند، و کشور باید به‌طور متحد عمل کند تا به مدیریت ریسک تهدیدات فضای سایبری بپردازد و از جامعه و مردم در مقابل آن تهدیدات محافظت کند.

دولت ضمن تقویت آمادگی برای واکنش به حملات سایبری از طریق آموزش و تمرین، آموزش و تمرین واکنش را در سرتاسر فضای سایبری و فضای واقعی انجام خواهد داد تا در زمینه مدیریت ریسک هم برای فضای سایبری و هم برای فضای واقعی تلاش کند. دولت همچنین به‌منظور بهبود قابلیت‌های جمع‌آوری و تحلیل داده‌ها و توانایی واکنش اضطراری در فضای سایبری، آموزش پرسنلی را ترویج خواهد داد که قادر به تحلیل حملات سایبری، به‌اشتراک‌گذاری اطلاعات از طریق چارچوبی برای هماهنگی بخش خصوصی و دولتی و پیشرفت نظارت بر اینترنت هستند.

۳-۳- مشارکت در صلح و ثبات جامعه بین‌المللی و امنیت ملی ژاپن

یک فضای سایبری آزاد، عادلانه و ایمن به صلح و ثبات جامعه بین‌المللی و امنیت ملی ژاپن کمک می‌کند.

یک فضای سایبری که برای همه عاملان آزاد است و در آن از جریان مستقل و آزاد اطلاعات حفاظت می‌شود، نوآوری را تقویت می‌کند و پایه و اساس دموکراسی را تشکیل می‌دهد. فضای سایبری از طریق نوآوری‌های تکنولوژیکی، اختراعات و طرح‌های چند نهاد ذی‌نفع در صنعت، دانشگاه و بخش‌های دولتی و خصوصی توسعه یافته است. کنترل بیش از حد توسط دولت‌ها مانع توسعه مستقل و پایدار فضای سایبری می‌شود. برای توسعه‌ی سالم فضای سایبری، چند نهاد ذی‌نفع باید برای اطمینان از جریان

آزاد اطلاعات و حفظ فضای باز و استقلال فضای سایبری با یکدیگر همکاری کنند.

همان‌طور که استفاده از فضای سایبری در سرتاسر جامعه شتاب گرفته است و موجب پیشرفت تلفیق فضای مجازی و فضای واقعی شده است، مشکلات فضای واقعی از جمله حقوق بشر، حریم شخصی، جنایت و تروریسم و امنیت ملی به قلمرو فضای سایبری وارد شده‌اند و چالش‌آفرین بوده‌اند. بر همین اساس، ضروری است که طرح‌هایی با توجه به این چالش‌ها اجرا شود تا از امنیت و ایمنی فضای سایبری اطمینان حاصل شود. از آن‌جا که ممکن است حملات سایبری به آسانی از مرزهای ملی عبور کند و حوادثی وجود دارد که مشکوک به حمایت مالی دولتی است، ضروری است که حاکمیت قانون تقویت شود، توانایی‌های دفاعی، بازدارندگی و آگاهی موقعیتی در مقابل حملات سایبری افزایش پیدا کند و همکاری و هماهنگی بین‌المللی در جهت اطمینان از امنیت و ثبات فضای سایبری ترویج پیدا کند. با این حال، هنگام انجام این کار لازم است توجه به خرج داد تا از ایجاد مانع در توسعه مستقل و پایدار فضای مجازی جلوگیری شود.

به‌منظور حفاظت از فضای سایبری آزاد، عادلانه و ایمن، ژاپن موضع خود را در مجامع بین‌المللی مطرح خواهد کرد و با استفاده از چارچوب‌های موجود از امنیت ملی خود اطمینان حاصل خواهد کرد و همکاری بین‌المللی را ترویج خواهد کرد.

۳-۳-۱- تعهد به فضای سایبری آزاد، عادلانه و ایمن

برای به واقعیت رساندن فضای سایبری آزاد، عادلانه و ایمن در سطح جهانی، ژاپن ایده‌هایش را در مجامع بین‌المللی مطرح خواهد کرد و نقشی فعال در ترویج حاکمیت قانون در فضای سایبری به عهده خواهد گرفت.

(۱) مطرح کردن ایده‌های فضای سایبری آزاد، عادلانه و ایمن

به‌منظور حفظ اکوسیستم توسعه مستقل و پایدار فضای سایبری، ژاپن سعی می‌کند از امنیت فضای سایبری از طریق هماهنگی و همکاری بین نهادهای ذی‌نفع در تلاش برای اطمینان از امنیت سایبری اطمینان حاصل کند، نه اینکه به سلطه و مقرراتی مثل کنترل جریان اطلاعات توسط دولت‌ها دامن بزند.

ژاپن چنین رویکردهای اساسی‌ای برای رسیدن به امنیت سایبری را در مجامع بین‌المللی مطرح خواهد کرد. علاوه بر این، ژاپن تلاش می‌کند با متحدین و کشورهای هم‌فکرش و همچنین شرکت‌های خصوصی همکاری کند تا جلوی هر تلاشی برای جلوگیری از توسعه فضای سایبری، از جمله تلاش برای تغییر قوانین بین‌المللی را بگیرد.

ضروری است که در این کار بحث درباره چگونگی مدیریت منابع اینترنتی را از بحث درباره مسائلی که به واسطه استفاده از فضای سایبری مطرح می‌شود، مثل حقوق بشر، حریم شخصی، جنایت و تروریسم و امنیت ملی جدا کنیم. با توجه به مسائلی که از استفاده از فضای سایبری نشئت می‌گیرد، بحث‌ها باید در محدوده چارچوب‌های موجود انجام گیرد.

(۲) ترویج حاکمیت قانون در فضای سایبری

ترویج حاکمیت قانون برای صلح و ثبات و جامعه بین‌المللی و امنیت ملی ژاپن حائز اهمیت است.

قوانین بین‌المللی موجود از جمله منشور ملل متحد، در مورد فضای سایبری نیز صدق می‌کند. ژاپن این موضع را اتخاذ می‌کند و به‌طور فعالانه در بحث در مورد کاربردهای خاص و منحصربه‌فرد قوانین بین‌المللی

موجـود و توسـعه و جهانی‌سـازی هنجارهـا مشـارکت می‌کند. همچنیـن ژاپن جهانی‌سـازی هنجارهـای رفتـار دولت‌هـای مسـئولیت‌پذیری را ترویج می‌کند کـه بـه موجب اجـرای مداوم و ممارسـت در چنین هنجارهایی تا امروز[1] آشـکار بوده‌انـد. ژاپـن از طریق جهانی‌سـازی چنیـن هنجارهایی در جامعـه بین‌المللی و جمـع‌آوری روش‌هـای مربوطـه در مقابل هر تلاشـی علیه چنیـن هنجارهایی می‌ایستد.

بـا توجـه بـه تمهیداتـی کـه علیـه جرایـم سـایبری تنظیـم شـده اسـت، آژانـس پلیـس ملـی و سـایر وزارتخانه‌هـا و سـازمان‌های ذی‌ربـط بـرای ترویج بیشـتر مشـارکت بین‌المللـی از طریـق همـکاری تحقیقاتـی بین‌المللـی و به‌اشـتراک‌گذاری اطلاعـات بـا سـازمان‌های بین‌المللـی، سـازمان‌های اجـرای قانـون و آژانس‌هـای امنیـت اطلاعـات در کشـورهای خارجـی بـا اسـتفاده از چارچوب‌هایـی ماننـد کنوانسـیون جرایـم اینترنتـی، معاهـدات کمـک حقوقی متقابـل و ICPO[2] بـا یکدیگـر همـکاری خواهنـد کـرد.

ژاپـن از طریـق ایـن طرح‌هـا حاکمیـت قانون را ترویج خواهـد کرد و صلح و ثبـات در جامعـه بین‌المللی و امنیـت ملی ژاپن را به واقعیت می‌رسـاند.

۳-۳-۲- تقویت توانایی‌های دفاعی، بازدارندگی و آگاهی موقعیتی

فضـای امنیتـی در فضـای مجـازی بـه طـور فزاینـده‌ای شـدیدتر می‌شـود. حملات سـایبری علیـه ارگان‌هـای دولتی، اپراتورهـای زیرسـاخت‌های حیاتی، کمپانی‌هـا و دانشـگاه‌ها و مؤسسـات پژوهشـی دارای فناوری‌هـای پیشـرفته صـورت گرفتـه اسـت. مـواردی بوده کـه ممکن اسـت پایه‌هـای دموکراسـی را تضعیـف کنـد. بـه‌عـلاوه، بعضـی از این حملات مشـکوک بـه حمایـت مالی از طـرف دولت‌ها هسـتند.

۱. این شامل گزارش سال ۲۰۱۵ از چهارمین اجلاس گروه متخصصین دولتی ملل متحد در خصوص توسعه در زمینه اطلاعات و ارتباط از راه دور در حوزه امنیت بین‌المللی (UN GGE)، ابلاغیه رهبران اجلاس آنتالیا G۲۰ سال ۲۰۱۵، و اعلامیه G۷ رفتار کشورهای مسئولیت‌پذیر در فضای سایبری می‌شود.

۲. ICPO سرواژه سازمان پلیس جنایی بین‌الملل (International Criminal Police Organization) می‌شود.

با توجه به این وضعیت، به منظور حفاظت از منافع امنیت ملی ژاپن در برابر حملات سایبری، اطمینان از مقاومت ژاپن در برابر حملات سایبری و افزایش توانایی ژاپن در دفاع از کشور (توانایی دفاعی)، جلوگیری از حملات سایبری (توانایی بازدارندگی) و آگاهی از موقعیت فضای سایبری (توانایی آگاهی موقعیتی) حائز اهمیت است.

کلیه نهادهای ذی‌نفع خصوصی و دولتیِ مرتبط تحت هدایت مرکز ملی آمادگی برای حوادث و استراتژی امنیت سایبری در رابطه با دفاعی، تحت هدایت وزارتخانه‌ها و آژانس‌های مسئول تمهیدات واکنش در رابطه با بازدارندگی، و سازمان‌های جمع‌آوری اطلاعات و تحقیقاتی در رابطه با آگاهی موقعیتی به صورت روزانه با یکدیگر همکاری نزدیک دارند و با هماهنگی کلی دبیرخانه امنیت ملی طرح‌های مربوط به امنیت ملی را اجرا می‌کنند. در صورت لزوم، موضوعات در شورای امنیت ملی به شور گذاشته می‌شوند و تصمیمات لازم اتخاذ می‌شود.

(۱) اطمینان از مقاومت ملی

(الف) اطمینان از مأموریت

این مأموریت ارگان‌های دولتی است که از زندگی مردم و فعالیت‌های اقتصادی و اجتماعی آن‌ها محافظت و پشتیبانی کنند. هر گونه کوتاهی در ایفای نقش آن‌ها نگرانی قابل‌توجهی برای امنیت ملی است. اجرای مأموریت‌های این ارگان‌های دولتی بستگی به خدماتی دارد که اپراتورهای زیرساخت‌های حیاتی و سایر اپراتورهای تجاری تأمین می‌کنند که سیستم اجتماعی را حفظ می‌کنند. این اپراتورها همچنین وظیفه مهمی در ارائه این خدمات ضروری برای مردم و جامعه دارند.

ژاپن ایجاد امنیت سایبری برای ارگان‌های دولتی و اپراتورهای زیرساخت‌های حیاتی را به منظور اطمینان از اجرای مأموریت‌های آن ارگان‌های دولتی مرتبط با امنیت ملی و به منظور ارائه خدمات ضروری برای مردم و جامعه ترویج خواهد کرد. همان‌طور که مقامات دفاعی، به‌ویژه وزارت دفاع و نیروهای دفاع از میهن به تقویت دفاع شبکه‌ها و زیرساخت‌هایی که عملیاتشان به آن‌ها وابسته است ادامه می‌دهند، به طور همزمان توانایی‌های واحدهای دفاع سایبری را در مقابل حملات سایبری تقویت می‌کنند و همکاری با نهادهای ذی‌نفع مشارکت‌کننده در اطمینان از مأموریت نیروهای دفاع از میهن را عمیق‌تر می‌کنند.

(ب) حفاظت از تکنولوژی‌های پیشرفته ژاپن و تکنولوژی‌های مرتبط با دفاع

تکنولوژی‌های پیشرفته نه فقط برای اطمینان از پیشرفت اقتصادی، بلکه برای امنیت ملی نیز دارایی مهمی به‌حساب می‌آید. ژاپن تمهیدات امنیت سایبری‌اش را تقویت خواهد کرد، از جمله کاهش ریسک‌های انسانی که مقابل اپراتورهای تجاری وزارتخانه‌ها و آژانس‌های دولتی مرتبط قرار دارد که تکنولوژی‌های مهم برای امنیت ملی ژاپن را مدیریت می‌کنند، مانند تکنولوژی‌های مرتبط با هوا و فضا، انرژی هسته‌ای، امنیت و تجهیزات دفاعی. به‌ویژه نشت یا افشای غیرقانونی اطلاعات فنی که در اختیار صنایع دفاعی قرار دارد، تأثیر مهمی بر امنیت ملی ژاپن می‌گذارد. به همین دلیل، ژاپن تلاش خواهد کرد که سیستمی اتخاذ کند تا از به‌اشتراک‌گذاری ایمن اطلاعات اطمینان حاصل شود، استانداردهای جدیدی در خصوص امنیت اطلاعات برای پیمانکاران تنظیم کند و در مقررات قراردادی تجدید نظر کند. مسئولین با این فرض که این تمهیدات در تمام زنجیره تأمین صنایع

دفاعی از جمله پیمانکاران فرعی، از طریق همکاری بین بخش‌های دولتی و خصوص با یکدیگر مشورت خواهند کرد.
علاوه بر این، دولت تمهیدات لازم را در سازمان‌های ملی پژوهشی و توسعه و دانشگاه‌ها و مؤسسات پژوهشی دارای تکنولوژی پیشرفته از منظر حفاظت از اطلاعات تکنولوژی‌های پیشرفته ترویج می‌کند.

(ج) تمهیدات علیه استفاده مخرب از فضای سایبری توسط سازمان‌های تروریستی

فضای سایبری مکانی را در اختیار قرار می‌دهد که افراد و سازمان‌ها می‌توانند به تبادل اطلاعات بپردازند و آزادانه عقاید خود را بیان کنند. فضای سایبری در حال حاضر پایه دموکراسی به‌حساب می‌آید. از طرف دیگر، جلوگیری از استفاده مخرب از قضایی سایبری توسط سازمان‌های تروریستی ضروری است. استفاده‌هایی مانند اشاعه و نمایش تعصب خشونت‌آمیز، جذب به سازمان‌ها، جمع‌آوری بودجه برای سازمان‌ها. به همین دلیل، دولت جمع‌آوری و تحلیل اطلاعات درباره فعالیت‌های سازمان‌های تروریستی در فضای سایبری را تقویت می‌کند و تمهیدات لازم دیگر را با همکاری جامعه جهانی اجرا می‌کند، ضمن اینکه حقوق اولیه بشر از جمله آزادی بیان را نیز تضمین می‌کند.

(۲) تقویت توانایی‌های بازدارندگی

(الف) تمهیدات بازدارندگی مؤثر

قوانین بین‌المللی، از جمله منشور ملل متحد، در مورد فضای سایبری نیز صدق می‌کند. همان‌طور که رهبران G7 در اجلاس ایسه‌شیما تأیید

کردند، تحت شرایط خاص، فعالیت‌های سایبری ممکن است معادل استفاده از زور یا حمله مسلحانه به معنای قوانین بین‌المللی باشد.[1] همچنین، همان‌طور که وزرای امور خارجه G7 در لوکا[2] تأیید کردند، یک کشور که قربانی عمل بین‌المللی غیرقانونی‌ای قرار گرفته باشد، در کنار دیگر واکنش‌های قانونی، می‌تواند تحت شرایط خاص به اقدامات متقابل متناسب علیه کشور مسئول آن عمل غیرقانونی روی بیاورد.[3]

براساس تأییدیه بالا، برای جلوگیری از فعالیت‌های مخرب سایبری و محافظت از ایمنی، امنیت و حقوق مردم، با هماهنگی نزدیک با کشورهای متحد و هم‌فکر خود، ژاپن از ابزارها و قابلیت‌های سیاسی، اقتصادی، تکنولوژیک، حقوقی، دیپلماتیک و دیگر ابزارها و قابلیت‌های قابل‌اجرا و مؤثر استفاده می‌کند تا بسته به تهدید، پاسخی قاطعانه در برابر تهدیدات سایبری که امنیت ملی ما را تضعیف می‌کند، از جمله مواردی که احتمالاً تحت حمایت دولت‌ها بوده است، داشته باشد.

دولت برای نشان‌دادن واکنش به‌موقع و مناسب، سیستم هماهنگی بین ارگان‌های دولتی مربوطه را تقویت می‌کند و کابینه وزرا را هسته آن قرار می‌دهد، به صورت قابل‌درکی تلاش‌های بین‌بخشی و بین‌آژانسی خود را ترویج می‌دهد، و همچنین توانایی‌های مقامات مربوطه از جمله مقامات اعمال قانون و نیروهای دفاع از میهن را تقویت می‌کند. در این راستا، ممکن است دستیابی به قابلیت‌هایی برای جلوگیری از عاملین خرابکار سایبری از استفاده از فضای سایبری نیز در نظر گرفته شود.

۱. اصول و اقدامات G7 در مورد فضای سایبری (ماه مه ۲۰۱۶) «ما تأیید می‌کنیم که تحت برخی شرایط، فعالیت‌های سایبری ممکن است معادل استفاده از زور یا حمله مسلحانه به معنای منشور ملل متحد و قوانین عرف بین‌الملل باشد. همچنین می‌پذیریم که کشورها می‌توانند از حق ذاتی دفاع شخصی یا جمعی از خود که در ماده ۵۱ منشور ملل متحد به‌رسمیت شناخته شده و مطابق با قوانین بین‌المللی، از جمله حقوق بشردوستانه بین‌المللی استفاده کنند و در مقابل حمله مسلحانه از طریق فضای سایبری دفاع کنند.»

2. Lucca

۳. اعلامیه G7 در مورد رفتار دولت‌های مسئول در فضای مجازی (آوریل ۲۰۱۷) «ما بیان می‌کنیم که به منظور جلوگیری از درگیری و حل‌وفصل مسالمت‌آمیز اختلافات، قوانین بین‌المللی چارچوبی برای واکنش دولت‌ها به اقدامات غیرقانونی‌ای که معادل حمله مسلحانه قرار نمی‌گیرند نیز در نظر می‌گیرد. این فعالیت‌ها ممکن است شامل فعالیت‌های سایبری نیز بشود. یک دولت که قربانی یک عمل بین‌المللی غیرقانونی قرار گرفته باشد، در کنار دیگر واکنش‌های قانونی، می‌تواند تحت شرایط خاص علیه کشور مسئول آن عمل غیرقانونی به اقدامات متقابل متناسب روی بیاورد، از جمله تمهیداتی از طریق ICTها، تا باعث شود دولت مسئول به تعهدات بین‌المللی خود عمل کند.»

(ب) تمهیدات اعتمادسازی

دولت در راستای ایجاد اعتماد بین کشورها تلاش خواهد کرد تا جلوی رخدادن شرایط غیرمنتظره و وخیم‌تر شدن اوضاع ناشی از حملات سایبری را بگیرد. با توجه به ناشناس‌بودن و مخفی‌بودن حملات سایبری، این خطر وجود دارد که حملات سایبری ناخواسته تنش بین کشورها را بیشتر کرده و وضعیت را بدتر کنند. به‌منظور جلوگیری از چنین حوادث و برخوردهای غیرضروری‌ای، ایجاد کانال‌های ارتباطی بین‌المللی در زمان‌های عادی با هدف آمادگی برای رخدادن حوادثی که از مرزهای ملی عبور می‌کند حائز اهمیت است. همچنین ضروری است که شفافیت به اعتماد بین کشورها از طریق تبادل فعال اطلاعات و گفتمان سیاست در مشاوره‌های دوجانبه و چندجانبه افزایش یابد. دولت همچنین برای در نظر گرفتن سازوکاری برای هماهنگی موضوعات مربوط به فضای سایبری با سایر کشورها همکاری خواهد کرد.

(۳) تقویت آگاهی موقعیتی سایبری

(الف) افزایش توانایی‌های مرتبط با ارگان‌های دولتی

به منظور جلوگیری از حمله سایبری که به‌طور فزاینده‌ای جدی می‌شود، علاوه بر تقویت توانایی‌های واکنش، توانایی کافی برای شناسایی، بررسی و تحلیل حملات سایبری برای پاسخگویی به مهاجمان ضروری است. به همین مظور، دولت از نظر کمی و کیفی توانایی جمع‌آوری و تحلیل اطلاعات ارگان‌های دولتی مربوطه را بهبود می‌بخشد. بر این اساس، دولت با ملاحظات گسترده‌ای در مورد هر ابزار مؤثر از جمله توسعه و ایمن‌سازی منابع انسانی امنیت سایبری با توانایی‌های تحلیلی سطح بالا، و توسعه و استفاده

از تکنولوژی‌های شناسایی، تحقیق و تحلیل حملات سایبری پیش خواهد رفت. دولت همچنین طرح‌هایی را در رابطه با اطلاعات ضد سایبری اجرا خواهد کرد.[1]

(ب) به‌اشتراک‌گذاری اطلاعات تهدید

به‌اشتراک‌گذاری اطلاعات بین وزارتخانه‌ها و آژانس‌های مربوطه در داخل دولت و با کشورهای متحد و هم‌فکر ما برای پاسخگویی دقیق و جلوگیری از تهدیدهای مختلف حملات سایبری، از جمله تهدیدهایی که مظنون به حمایت مالی از طرف دولت‌های دیگر و سازمان‌های غیردولتی هستند، ضروری است. بر همین اساس، دولت به‌اشتراک‌گذاری اطلاعات تهدید با کشورهای متحد و همفکرمان را تشویق می‌کند. دولت همچنین چارچوب‌های به‌اشتراک‌گذاری اطلاعات تهدید و همکاری درون دولت را به رهبری کابینه وزیران تقویت خواهد کرد.

۳-۳-۳- همکاری و هماهنگی بین‌المللی

از آن‌جا که تأثیر حوادث در فضای سایبری ممکن است به راحتی از مرزهای ملی فراتر برود، همیشه ممکن است حوادث سایبری در خارج از کشور روی ژاپن تأثیر بگذارد. ژاپن با دولت‌ها و بخش‌های خصوصی سراسر دنیا همکاری و هماهنگی می‌کند تا از امنیت فضای سایبری اطمینان حاصل کرده، هم در جهت صلح و ثبات جامعه بین‌المللی و هم در جهت امنیت ملی ژاپن تلاش می‌کند.

به همین منظور، دولت به طور فعالانه در بحث‌های مختلف بین‌المللی مشارکت کرده، برای به‌اشتراک‌گذاری اطلاعات و توسعه درک مشترک در

۱. فعالیت دفاع اطلاعاتی در مقابل فعالیت تهاجمی اطلاعاتی توسط کشورهای خارجی با استفاده از تکنولوژی اطلاعات و ارتباطات.

مـورد موضوعـات مرتبـط با فضای سـایبری تلاش خواهد کـرد. دولت همچنین تخصـص خـود را با کشـورهای خارجـی به اشـتراک خواهد گذاشـت، همکاری و هماهنگـی در مسـائل خـاص را ترویـج خواهد داد و دسـت بـه اقدامات واقعی خواهـد زد. بـه‌عـلاوه، مـا در بخش‌هـای دولتـی و خصوصـی کـه قـادر بـه بیان موضـع خـود در مجامـع بین‌الملـل هسـتیم، امنیـت به وجـود خواهیـم آورد و پرسـنل متخصص آموزش خواهیـم داد.

(۱) سیاست به‌اشتراک‌گذاری تخصص و هماهنگی

دولـت از طریـق گفتگوهـای دوجانبـه و کنفرانس‌هـای بین‌المللـی در مورد امنیـت سـایبری تـلاش خواهـد کـه در مـورد سیاسـت‌های امنیـت سـایبری، اسـتراتژی‌ها و سیسـتم پاسـخگویی تبادل اطلاعات داشته باشـد و از این دانش در برنامه‌ریزی سیاسـت امنیت سـایبری ژاپن اسـتفاده کند. همچنین همکاری و هماهنگی کشـور را در زمینه سیاسـت امنیت سـایبری با شـرکای استراتژیک کـه اصول اساسـی مشـترکی با مـا در امنیت سـایبری دارند، تقویـت می‌کنیم.

(۲) همکاری بین‌المللی برای واکنش به حوادث

دولـت اطلاعـات مربـوط بـه حمـلات و تهدیـدات سـایبری را به‌اشـتراک می‌گـذارد و همـکاری بیـن CERTهـا[1] را تقویـت می‌کنـد تـا در صـورت وقوع حادثـه بتواند واکنشـی منسـجم فراهم کند. دولت همچنین تـلاش خواهد کرد تـا از طریـق آمـوزش مشـترک و مشـارکت در تمرین‌هـای سـایبری و آمـوزش مشـترک بین‌المللـی توانایـی واکنـش هماهنـگ را بهبود بخشـد. به‌عـلاوه، در صـورت بـروز حادثـه دولـت از طریـق همـکاری مناسـب بین‌المللـی واکنـش

۱. تیم واکنش اضطراری کامپیوتری (CERT) سازمانی است که به حوادث اضطراری کامپیوتری واکنش نشان می‌دهد.

مناسب نشان خواهد داد.

(۳) همکاری برای ظرفیت‌سازی

امروزه با تعمیق وابستگی متقابل فرامرزی، برای ژاپن ممکن نیست که به‌تنهایی به صلح و ثبات برسد. هماهنگی جهانی برای کاهش آسیب‌پذیری‌های امنیت سایبری و با هدف از بین بردن آن‌ها برای مشارکت در تأمین امنیت ملی ژاپن ضروری است.

از این منظر، کمک به ظرفیت‌سازی در سایر کشورها ثبات زندگی ساکنین ژاپنی و فعالیت کمپانی‌های ژاپنی در سایر کشورها را که به زیرساخت‌های حیاتی در این کشورها و همچنین توسعه صحیح استفاده از فضای سایبری در آن‌جا بستگی دارد، تضمین می‌کند. در عین حال، ارتباط مستقیمی با تأمین امنیت فضای سایبری دارد و به بهبود فضای امنیتی برای کل جهان از جمله ژاپن کمک می‌کند.

طبق استراتژی اساسی درباره ظرفیت‌سازی امنیت سایبری برای کشورهای در حال توسعه[1] که در سال ۲۰۱۶ منتشر شد، دولت به طور فعال ظرفیت‌سازی در کشورهای در حال توسعه را تشویق خواهد کرد.

۳-۴- رویکردهای مقطعی به امنیت سایبری

به منظور دستیابی به سه هدف سیاستی («امکان ایجاد نشاط اجتماعی و اقتصادی و توسعه‌ی پایدار»، «ساخت جامعه‌ای امن و ایمن برای مردم» و «مشارکت در صلح و ثبات جامعه بین‌المللی و امنیت ملی ژاپن») کار بر روی توسعه منابع انسانی و تحقیق و توسعه به‌عنوان پایه‌ای برای اهداف سیاستی هم از منظر مقطعی و هم از منظر میان‌مدت و بلندمدت حائز

اهمیت است. به‌طور همزمان، ایجاد یک رویکرد همکاری که در آن همه در کار بر روی امنیت سایبری به عنوان یک عامل فعال در فضای سایبری نقش داشته باشند، ضروری است.

۳-۴-۱- توسعه و اطمینان از منابع انسانی امنیت سایبری

همان‌طور که ارزش‌های جدیدی در راستای تحقق نسخه ۵.۰ جامعه ایجاد می‌شود، تهدیدات حملات سایبری در حال گسترش است و ضروری است که هر نهاد ذی‌نفع طرح را اجرا کرده و نقش خود را ایفا کند، به‌جای اینکه به تلاش‌های چند متخصص برای اطمینان از امنیت سایبری تکیه کند.

برای آمادگی برای آینده مربوط به این تغییر پارادایم پیش‌رو، نیاز به روشن‌سازی سطح دانش و مهارت موردنیاز پرسنل درگیر در ایجاد امنیت سایبری از نقطه‌نظر حمایت از هر سازمان برای انجام مأموریت خود و استفاده ایمن از فضای سایبری وجود دارد. پس از آن، ایجاد یک چرخه مطلوب ضروری است که در آن عرضه و تقاضا برای پرسنل از این طریق تأمین شود: ارائه کافی دانش لازم و توانایی‌های عملی برای پرسنل، که به واسطه تعیین صلاحیت‌ها و استانداردهای ارزیابی‌ای تأیید شده باشد که از طریق آموزش به‌دست آمده است؛ و بیشتر قادر ساختن آن‌ها تا مهارت‌های خود را از طریق تجربه عملی مکرر تقویت کنند.

برای این منظور، دولت با صنعت، دانشگاه و بخش عمومی همکاری خواهد کرد تا اطلاعات تقاضا برای پرسنل و تمهیدات مربوط به توسعه منابع انسانی را به‌منظور تقویت توسعه و اطمینان از منابع انسانی امنیت سایبری به‌اشتراک بگذارد. در انجام این کار، اطمینان از تنوع پرسنل از نقطه‌نظر تشویق به نوآوری حائز اهمیت است.

(۱) آموزش و پذیرش در سطح مدیریت استراتژیک

به‌منظور پیش‌برد تمهیدات امنیت سایبری به‌عنوان بحثی از مدیریت کمپانی، مناسب نیست که این کار را به متخصصین و کارکنان سطح عملیاتی واگذار کرد، زیرا امنیت سایبری صرفاً یک مسئله فنی نیست.

تحت استراتژی‌های مدیریتی و استراتژی‌های تجاری که مدیران ارشد ارائه می‌دهند، پرسنلی که توانایی مقابله با این چالش را داشته باشند باید:

(الف) ریسک‌های مرتبط با امنیت سایبری را درک کنند که باید در اجرای عملیات و خدمات بخشی از ریسک‌هایی به حساب بیاید که سازمان باید مدیریت کند؛ و

(ب) از متخصصین سطح عملیاتی برای اجرای اقدامات متقابل و پاسخ به حوادث در نقش ارائه پشتیبانی اصلی برای مدیریت ریسک در مورد تداوم تجارت و ایجاد ارزش استفاده کند و آن‌ها را مدیریت کند.

بر همین اساس، دولت پرسنلی را که این نقش‌ها را برعهده دارند به عنوان «سطح مدیریت استراتژیک» تعریف می‌کند و برای پذیرش این مفهوم از طریق همکاری با صنعت تلاش خواهد کرد، از جمله ترویج این درک میان مدیران ارشد.

مواردی نیز وجود دارد که به دلیل تفاوت در فرهنگ یا سنت درون صنایع یا دسته‌های تجاری، ممکن است ادغام و اجرای تمهیدات امنیت سایبری در سیستم‌های مدیریت موجود برای تحقق عملیات و خدمات دشوار باشد. به همین دلیل، دولت ضمن در نظر گرفتن اینکه روش‌های زیادی برای تجارت و مدیریت وجود دارد، اجرای برنامه‌های بازیادگیری را به وسیله توسعه منابع یادگیری عملی برای سطح مدیریت استراتژیک و شناسایی و آموزش مربیان ترویج خواهد داد.

(۲) آموزش برای سطح عملیاتی و متخصص

در مورد سطح عملیاتی و متخصص که تمهیدات مربوط به برنامه‌ریزی، ساخت و بهره‌برداری از سیستم را اجرا می‌کنند، بر اساس دستورالعمل بیناشده توسط سطح مدیریت استراتژیک، برنامه‌های آموزشی متعدد، برنامه‌های صدور گواهینامه و آزمایش و آموزش‌های مختلف از طریق همکاری در بخش‌های خصوصی و دولتی انجام شده است.

ادامه تقویت چنین طرح‌هایی برای افزایش سطح دانش و مهارت ضروری است. کارکنان سطح عملیاتی و متخصص همچنین باید درک خود را از تکنولوژی‌های ارتباطات و اطلاعات، تکنولوژی‌های سیستم کنترل و حملات سایبری که هرروز تکامل می‌یابد، عمیق کنند. علاوه بر این، در واکنش به این حملات مهم است که سیاست‌های مدیران ارشد را درک کنند و بخشی از تیم باشند و با دیگر پرسنل سطح متخصص ارتباط برقرار کنند. برای انجام این کار، استفاده از برنامه‌های توسعه برای سطوح عملیاتی و متخصص در جهت توسعه مهارت‌های لازم برای درک ایده‌های مفهومی و انتزاعی ارائه‌شده توسط سطح مدیریت استراتژیک و تبدیل آن‌ها به تمهیدات عملی در عین ارتباط روان با انواع نهادهای ذی‌نفع، ضروری است.

دولت همچنین به شناسایی، آموزش و اطمینان از پرسنل دارای توانایی‌های استثنایی که توانایی رقابت در سطح جهانی را دارند ادامه خواهد داد. به‌عنوان مثال، دولت به ترویج گسترش فرصت‌ها برای پرسنل ادامه خواهد داد تا خود را وقف تلاش برای دستیابی به توانایی رقابت در سطح جهانی کنند و توانایی خودشان را برای بررسی تمهیدات از طریق تحقیق در مورد موضوعاتی مانند روش‌های واکنش، از جمله روش‌های حمله و روش‌های دفاع علیه

حملات سایبری و سیستم‌سازی روش‌های برای جمع‌آوری، تحلیل و ارزیابی اطلاعات توسعه دهند.

(۳) آماده‌سازی بنیادی برای توسعه منابع انسانی امنیت سایبری

در آماده‌سازی برای تکامل تکنولوژی‌های اطلاعات و ارتباطات در میان‌مدت و بلندمدت، ضروری است که درک از اصول اولیه‌ای را که بنیاد امنیت سایبری را به عنوان بخشی کاربردی تشکیل می‌دهد، ترویج دهیم و طرح‌های توسعه توانایی تفکر منطقی و مفهومی را بهبود ببخشیم. به همین منظور، با توجه به مبانی امنیت سایبری و تکنولوژی‌های اطلاعات و ارتباطات، برای بررسی دانش و سیستم‌های تکنولوژی و برنامه درسی الگو براساس این سیستم‌ها، صنعت، دانشگاه و بخش عمومی با یکدیگر همکاری خواهند کرد.

دولت همچنین به طور پیوسته در زمینه پرورش توانایی استفاده از اطلاعات در برنامه آموزشی مقاطع ابتدایی و متوسطه به‌منظور تقویت آموزش جوانان در ارتباط با امنیت سایبری و مهارت‌های تکنولوژی ارتباطات و اطلاعات تلاش خواهد کرد، از جمله تمهیداتی مثل الزامی‌کردن درس علوم کامپیوتر از مقطع دبستان. همچنین در زمینه پرورش شیوه‌های تفکر منطقی، مثل تفکر برنامه‌نویسانه و در زمینه آموزش درکی از سیستم‌ها و اصول تکنولوژی‌های ارتباطات و اطلاعات با توجه به سطوح رشد بچه‌ها تلاش خواهد کرد. دولت بر گسترش و غنی‌سازی آموزش معلمان تأکید خواهد کرد، ضمن اینکه تلاش خواهد کرد تا موارد درسی راجع به پرورش توانایی استفاده از اطلاعات به‌درستی در دوره‌های آموزش معلم گنجانده شود. هنگام انجام این کار، مهم است که استفاده منعطف

از پرسنل صنعت را الزامی تلقی کرد. علاوه بر این، به دلیل افزایش جرایم اینترنتی توسط جوانان در سال‌های اخیر، آموزش اخلاقِ اطلاعات یکی دیگر از مباحث مهم است.

علاوه بر این، لازم است محیطی فراهم شود که در آن فرصت‌های زیادی برای جوانان فراهم باشد که انتظار می‌رود در آینده مهارت‌های پیشرفته امنیت سایبری را کسب کنند، تا علاقه‌مند شوند و آزادانه استفاده از ابزارها و دستگاه‌های امنیت سایبری را در مکان‌هایی خارج از برنامه درسی مدرسه مانند جامعه، کمپانی‌ها و سازمان ها از طریق استفاده‌ی منعطف از پرسنل صنعت یاد بگیرند. در عین حال، تصور می‌شود که اگر توسعه این محیط برای خودسازی با آموزش اخلاقیات ترکیب شود، در جلوگیری از جرایم سایبری که به دلیل کنجکاوی توسط جوانان انجام می‌شود مؤثر خواهد بود. دولت همچنین به ترویج توسعه منابع انسانی برای تکنولوژی اطلاعات در آموزش عالی مانند دانشگاه‌ها و انستیتوی ملی فناوری از طریق مشارکت‌های صنعت، دانشگاه و دولت ادامه خواهد داد.

(۴) تقویت تضمین و توسعه آژانس‌های منابع انسانی امنیت سایبری

دولت به تلاش خود برای تضمین و توسعه مداوم منابع انسانی امنیت سایبری در آژانس‌هایی تحت مدیریت و کنترل عملکرد معاون وقت وزارت امنیت سایبری و مدیریت تکنولوژی اطلاعات که تمهیدات امنیتی را بر اساس سیاست واحد برای ارگان‌های دولتی اجرا می‌کند، ادامه خواهد داد. دولت همچنین از طریق افزایش کارکنان، آموزش مناسب برای هر سطح با هدف افزایش دانش و توانایی، و روش‌هایی شامل تکنسین‌های امنیتی سطح بالا و اطمینان از جبران خسارت مناسب، به‌طور پیوسته طرح‌هایی را که

بـر اسـاس برنامه‌هـای تضمیـن و توسـعه منابع انسـانی بـرای آژانس‌هـا مطرح شـده اجـرا خواهـد کـرد، ضمن اینکه بـرای بهبود بیشـتر این طرح‌هـا از طریق بررسـی سـالانه برنامه‌هـا تـلاش می‌کنند.

(۵) ترویج شراکت بین‌المللی

بـا توجـه بـه اینکه واکنش به مسـائل مربـوط به امنیت سـایبری در مقیاس جهانـی مـورد نیـاز اسـت، ژاپـن به جـای تأمین ایـن نیازها تنهـا در ژاپـن، باید امـکان کاربـرد جهانـی را تـا جـای ممکـن بـه عنـوان بخشـی از توسـعه منابع انسـانی امنیـت سـایبری فراهم کنـد. به همیـن منظور، دولـت از طریـق اجازه دادن بـه برنامه‌هـای توسـعه منابـع انسـانی در دانشـگاه‌ها و مؤسسـات عمومی به‌عنـوان بخشـی از رعایـت برخـی الزامـات طبـق اسـتانداردهای بین‌المللی، با کشـورهای پیشـرو همـکاری خواهـد کرد تا سیسـتمی بسـازد که همـکاری از طـرق مختلـف بـا سـازمان‌هایی را ترویج کند که در حال توسـعه منابع انسـانی بـه روش‌هـای مختلـف، ماننـد اجـرای برنامه‌هـای آموزشـی مشـترک و مجـاز کـردن انتقـال اعتبار در خارج از کشـور هسـتند.

عـلاوه بـر ایـن، بـا هدف کمک به توسـعه امنیت سـایبری منابع انسـانی در خـارج از کشـور، دولـت از دانـش و تجربـه به‌دسـت‌آمده از طریق توسـعه منابع انسـانی امنیـت سـایبری در ژاپـن برای کمک بـه ایجاد ظرفیـت در میان منابع انسـانی امنیت سـایبری در خارج از کشـور اسـتفاده خواهد کرد.

۳-۴-۲- پیشرفت پژوهش و توسعه

بـا ادامـه تلفیق فضای سـایبری و فضای واقعی، با توجه به پیشـرفت نوآوری در فضای سـایبری و تهدید حملات سـایبری علیه این نوآوری‌ها،

پژوهش و توسعه عملی (R&D)[1] در مورد امنیت سایبری مورد نیاز است. همراه با آن، واکنش با توجه به تکامل ناپایدار تکنولوژی و جامعه در میان‌مدت و بلندمدت نیز لازم است.

(۱) ترویج R&D عملی

انتظار می‌رود محصولات و خدمات جدید مبتکرانه از طریق ترکیبی از تکنولوژی‌های مختلف از جمله اینترنت اشیا و AI ایجاد شود. وقتی هدف رشد صنعت و رقابت پیشرفته بین‌المللی برای ژاپن باشد، ارائه محصولات و خدمات با سطح بالایی از کیفیت امنیتی ضروری است.

در همین حال، استفاده از این تکنولوژی‌ها توانایی ایجاد آسیب‌پذیری‌های جدیدی را دارد که قبلاً وجود نداشته‌اند. به همین منظور، دولت با تمرکز بر تکنولوژی به تلاشش ادامه خواهد داد که از طریق استفاده از تکنولوژی‌های پیشرفته‌ای مانند AI و زنجیره بستکی، تکنولوژی‌های امنیتی‌ای که می‌توان درون سیستم‌های متشکل از محصولات و خدمات جاسازی کرد، و از طریق R&D عملی با توجه به روش‌هایی برای چنین تکنولوژی‌های درونی‌ای از امنیت سایبری اطمینان حاصل شود. به‌طور خاص، دولت به ترویج R&D در زمینه تأیید و ایجاد اعتماد، و اطمینان از قابلیت ردیابی در فرایندهای ایجاد ارزش در زنجیره‌های تأمین و شناسایی و دفاع در مقابل حملات در این مناطق خواهد پرداخت. علاوه بر این، دولت همچنین به توسعه تکنولوژی برای شناسایی مؤثر سخت‌افزار و نرم‌افزار مخرب داخلی داخل دستگاه‌ها و به R&D خواهد پرداخت تا از صحت، در دسترس بودن و محرمانه بودن داده‌ها و اطلاعات در صورت بروز رفتارهای ناخواسته توسط کاربر در پلتفرم اطمینان حاصل کند.

1. Research and Development

دولت همچنین به ترویج R&D خواهد پرداخت که توانایی‌های آگاهی موقعیتی را در فضای سایبری از جمله توانایی شناسایی و تحلیل حملات سایبری افزایش می‌دهد و در تأمین امنیت ملی در فضای سایبری، مانند بهبود قابلیت‌های دفاعی و واکنشی و اطمینان از بازگشت‌پذیری مشارکت می‌کند. به‌طور خاص، دولت به ترویج R&D با هدف درک فعالیت حمله به واسطه جذب مهاجمان به شبکه‌هایی خواهد پرداخت که از سازمان‌هایی مانند ارگان‌های دولتی و کمپانی‌ها تقلید می‌کنند. هدف دیگر دولت کاهش بار جستجو در شبکه‌های گسترده برای بررسی دستگاه‌های آسیب‌پذیر اینترنت اشیا در شبکه است. در اجرای این R&D، تشکیل یک چرخه مطلوب حائز اهمیت است که در آن دانش و تجربه حملات سایبری از محل عملیات امنیت سایبری برای استفاده در R&D در اسرع وقت با محققین به‌اشتراک گذاشته شود، در حالی که نتایج R&D نیز در اسرع وقت برای استفاده در محل عملیات امنیت سایبری به‌اشتراک گذاشته می‌شود. برای دستیابی به این هدف، دولت به ترویج به‌اشتراک‌گذاری اطلاعات به طور زنده بین شرکت‌های عملیاتی امنیتی و مؤسسات پژوهش و توسعه دولتی خواهد پرداخت.

همچنین مهم است که در صورت لزوم از وجود ابزاری برای بررسی اینکه برنامه‌ها و مدارهای مخرب در دستگاه‌ها و نرم‌افزارهایی که در سیستم‌های ارگان‌های دولتی و اپراتورهای زیرساخت‌های حیاتی استفاده می‌شوند اطمینان حاصل کرد. بر همین اساس، دولت نقشی مرکزی در جهت توسعه سیستم برای انجام بازرسی‌های فنی لازم و همچنین کار در زمینه R&D لازم برای این منظور بر عهده خواهد گرفت. دولت در زمینه تکنولوژی‌های اساسی نیز که از نظر امنیت ملی برای کشور ضروری هستند

بـه ترویـج خواهـد پرداخـت. تکنولوژی‌هایی ماننـد تکنولوژی رمزگـذاری که به توسـعه فناوری‌های محاسـباتی (مثل محاسـبات کوانتومـی و AI) می‌پردازد.

عـلاوه بـر ایـن، بجـز ایـن R&D مرتبط با تکنولـوژی، پژوهـش و مطالعه در زمینـه مسـائل مربـوط به سیاسـت‌های تمهیـدات امنیت سـایبری نیـز ترویج داده می‌شـود، ماننـد روشن‌سـازی تفسـیر قوانیـن و مقـررات مربـوط به امنیت سایبری.

بـا توجـه بـه ایـن طرح‌هـای R&D بـرای امنیت سـایبری، دولت بـه ترویج انتشـار و اتخـاذ اجتماعـی نتایـج خواهـد پرداخـت. علاوه بـر ایـن، دولت تلاش خواهـد کـرد تـا همکاری‌هـای بین‌المللـی مربـوط بـه R&D را در بخش‌هـای دولتـی و خصوصـی بـا کشـورهای هم‌فکـر کـه بـا ژاپـن ارزش‌هـای اساسـی مشـترک دارنـد، تقویـت کنـد. ایـن تقویـت از طریـق پژوهش‌های مشـترک و ایجـاد اسـتانداردهای بین‌المللـی بر اسـاس نتایـج تحقیقات، در کنار مشـارکت فعـال در رویدادهـای خارج از کشـور برای انتشـار اطلاعات در سـطح بین‌المللی انجـام خواهد شـد.

(۲) واکنش با نگاه به تکامل میان‌مدت و بلندمدت تکنولوژی و جامعه

با پیشروی تلفیق فضای سایبری و فضای واقعی، پیشرفت در تکنولوژی‌های اطلاعـات و ارتباطـات مانند AI و واقعیت مجازی این امـکان را به‌وجود می‌آورد کـه تجربیـات متنـوع از جمله روندهایی که به واسطه‌شـان این تجربیات شـکل گرفته‌انـد را به‌اشـتراک گذاشـت، در عیـن اینکـه ارزش‌های متفاوت هـر فرد را پذیرفـت. در میـان تغییـرات عمده بشـریت که توسـط این تکنولوژی‌هـا ایجاد شـده اسـت، این احتمـال وجـود دارد که منطق درک‌شـده فعلی سیسـتم‌های اجتماعـی در آینـده بـه طور اساسـی تغییر کند و بـرای کارهایی کـه می‌توان با

رویکردهای موجود R&D امنیت سایبری انجام داد و از ارزیابی تکنولوژی تا امروز فراتر رفته است، محدودیتی وجود دارد. به‌منظور ایجاد ارزش جدید، احتمالاً رویکرد جدیدی لازم خواهد شد که جامعه کلی را از منظر اکوسیستم که انسان هم بخشی از آن است، طراحی کند و از زمان حالی به آینده نگاه کند که تلفیق ادامه‌دار فضای مجازی و فضای واقعی در آن رخ داده باشد. به همین منظور از نظر میان‌مدت و بلندمدت، دولت به‌ترویج پژوهش در مورد هماهنگی و وحدت میان امنیت سایبری در رشته‌های دانشگاهی مختلف، از جمله دیدگاه‌های علوم اجتماعی از رشته‌هایی مانند حقوق و روابط بین‌الملل، امنیت ملی و مدیریت بازرگانی و همچنین دیدگاه‌های انسان‌شناختی و روان‌شناختی رشته‌هایی مانند فلسفه و روان‌شناسی خواهد پرداخت. ناگفته نماند که نتایج R&D از جمله R&D در زمینه‌های علم و تکنولوژی، نباید تأثیر منفی بر جامعه بشری بگذارد.

۳-۴-۳- همکاری توسط همه‌ی کسانی که نقشی اصلی در امنیت سایبری دارند

با گسترش دستگاه‌هایی مانند تلفن‌های هوشمند و شبکه‌های بی‌سیم عمومی، همه افراد به فضای سایبری متصل می‌شوند و از مزایای چشمگیر آن برخوردار می‌شوند. انتظار می‌رود این روند با پیشرفت اینترنت اشیا سرعت بگیرد. در همین حال، برای استفاده امن و ایمن از فضای سایبری به‌طور مداوم و در میان تهدید روبه‌گسترش حملات سایبری، برای تک‌تک افراد به عنوان عاملی فعال در فضای سایبری ضروری است که آگاهی و درک خود از امنیت سایبری را رشد دهند تا بتوانند با انواع مختلف ریسک‌های

فضـای سـایبری مقابله کنند، مانند تمهیدات جلوگیـری از جرایم و عبور و مرور ایمـن در فضـای واقعـی تـا بتواننـد اسـتفاده‌ای امن و ایمـن از فضای سـایبری داشته باشند.

برای رشـد این آگاهی و درک از امنیت سـایبری، محدودیتی برای اثربخشـی طرح‌هـای مبارزاتـی موجـودی کـه فقـط توسـط دولـت اجـرا می‌شـوند وجود دارد. در عـوض، دولـت موظف اسـت سیسـتمی ایجاد کند کـه نهادهای ذی‌نفع را قـادر سـازد بـر اسـاس تقسـیم متقابـل مسـئولیت‌ها بـا یکدیگر همـکاری و هماهنگـی کننـد، در عیـن اینکه به فعالیت‌های مسـتقل جوامـع مختلف مانند مناطـق، کمپانی‌هـا و مـدارس احترام می‌گذارنـد و از طریق رویکـرد حمایتی از چنین سیسـتمی رهبـری خود را اعمـال کنند.

بـر همیـن اسـاس، در حالـی که مرکز ملی آمادگی برای حوادث و اسـتراتژی امنیـت ملـی نقـش اساسـی را ایفـا می‌کننـد، دولـت بـه نهادهـای ذی‌نفـع در صنعـت، دانشـگاه و بخش‌هـای دولتـی و خصوصـی به‌صـورت روان و مؤثـر کار کننـد و به‌طـور طبیعـی همـکاری کنند. بـه طور خـاص، دولت یک اسـتراتژی جامـع و برنامـه عملیاتـی دقیق بـرای آگاهی عمومـی در مورد امنیت سـایبری تهیـه خواهـد کـرد و اطلاعـات لازم را منتشـر کنـد و بـه سـؤالات مردم پاسـخ دهـد. دولـت همچنین با اسـتفاده از کمیته‌هایی که نماینـدگان جوامع مختلف از صنعـت، دانشـگاه و بخش‌هـای دولتـی و خصوصـی در آن شـرکت می‌کنند، نهادهـای ذی‌نفـع را تشـویق بـه اقدامـات عملی خواهـد کرد. دولـت همچنین تـلاش خواهـد کـرد تا آگاهـی از امنیت سـایبری را به عنوان یـک دوره متمرکز بـر ارتقـای درک امنیـت سـایبری توسـط همـه مردم تبلیـغ کنـد. همچنین از طریـق ایجـاد و توزیـع کتاب‌هـای راهنمـای قابـل فهم بـرای مـردم و از طریق پـرورش توانایـی اسـتفاده از اطلاعـات تحـت برنامه‌های درسـی مدارس،

آموزش امنیت سایبری را رواج خواهد داد.

انتظار می‌رود تولیدکنندگان و فروشندگان دستگاه‌هایی مانند تلفن‌های هوشمند و رایانه‌های شخصی و شرکت‌های ارتباط از راه دور مانند شرکت‌های مخابراتی و ارائه‌دهندگان اینترنت، از طریق ارائه محصولات و خدمات سازگار با امنیت و توضیح دادن به کاربران و پاسخگویی به سؤالات آن‌ها کاربران را قادر به اجرای مناسب طرح‌های امنیت سایبری کنند. به همین دلیل، دولت فضایی را ایجاد می‌کند که طرح‌ها توسط این کسب‌وکارها و سازمان‌های مرتبط رواج پیدا کند و توسعه و اجرای مداوم رهنمودهای مفید برای ایجاد امنیت سایبری بر اساس نیازهای کاربر و شکل استفاده او ترویج داده شود.

بخش چهارم

بخش چهارم

ترویج و اجـرای امنیت سـایبری

دولـت مشـغول ترویـج سیاسـت تقویـت تمهیـدات امنیـت سـایبری بوده اسـت تا اسـتفاده و کاربـرد تکنولوژی‌هـای اطلاعـات و ارتباطـات و داده‌ها[1] را بـه عنـوان اسـاس جامعه[2] ایمن سـازد و از امنیـت ملی ژاپـن اطمینان حاصل کند.[3]

بـر اسـاس ایـن سیاسـت، ارگان‌های دولتی مربوطه بایـد نقش فعال خود را در ترویـج تمهیـدات امنیت سـایبری ایفا کنند، در حالی کـه آن‌ها را یکپارچه می‌کننـد. بـه همیـن منظـور، ارگان‌هـای دولتـی مربوطـه بـه تلاش خـود در راسـتای تقویـت توانایی‌هـای امنیـت سـایبری خـود تحت رهبـری مرکز ملی آمادگـی بـرای حـوادث و اسـتراتژی امنیـت سـایبری ادامـه خواهنـد داد تا از اجـرای مـداوم تمهیـدات منـدرج در ایـن اسـتراتژی اطمینـان حاصـل کنـد. مرکـز ملـی آمادگـی بـرای حـوادث و اسـتراتژی امنیت سـایبری نقـش اصلی خـود را به‌عنـوان نقطـه کانونـی در هماهنگـی همـکاری بین دولتـی و ترویج همـکاری بیـن صنعت، دانشـگاه و بخش‌های دولتی و خصوصـی ایفا می‌کنند،

۱. اعلامیه پیشرفته‌ترین ملت فناوری اطلاعات در جهان: برنامه اساسی برای پیشرفت استفاده از داده‌های بخش دولتی و خصوصی (۳۰ مه ۲۰۱۷) بیان می‌کند که «در ترویج کاربرد و استفاده از داده‌ها، ناگفته نماند تمهیدات باید به‌طور همزمان در ارتباط با حفاظت از اطلاعات شخصی و حریم خصوصی، تمهیدات امنیت سایبری، حقوق مالکیت معنوی، کیفیت داده‌ها و تلاش برای اطمینان از اعتمادپذیری و امنیت داده‌ها، وضعیت منطق در دوران AI و ربات‌ها و موارد دیگر اجرا شود.»

۲. استراتژی رشد ۲۰۱۷ (تصمیم کابینه در ۹ ژوئن ۲۰۱۷) بیان می‌کند که «در جامعه فوق هوشمند که مردم می‌توانند در هر موقعیتی راحت و غرق در نعمت زندگی کنند، تأمین فضای سایبری ایمن اساسی مهم برای فعالیت‌های اقتصادی و اجتماعی در جامعه است.»

۳. در استراتژی امنیت ملی (تصمیم کابینه در ۱۷ دسامبر ۲۰۱۳) بیان شده که «فضای سایبری هم برای ترویج رشد اقتصادی و هم برای ترویج نوآوری از طریق جریان آزاد اطلاعات در فضای سایبری ضروری است. محافظت از فضای سایبری در برابر ریسک‌های فوق‌الذکر برای تأمین امنیت ملی امری حیاتی است.»

در حالی که این استراتژی را به اشخاص ذی‌ربط در ژاپن و خارج از ژاپن گسترش می‌دهند. دولت توانایی مدیریت و مقابله با بحران را بیشتر تقویت می‌کند. در رابطه با بازی‌های ۲۰۲۰ توکیو، باید به‌واسطه ایجاد طرح‌هایی برای دخالت، مشارکت و همکاری در بخش‌های صنعتی، دانشگاهی، دولتی و اجتماعی به اجری مداوم تمهیدات امنیت سایبری توجه ویژه‌ای داشت.

ستاد استراتژی امنیت سایبری هنگامی که در زمینه‌های مهم امنیت سایبری فعالیت می‌کند، برای تبلیغ «جامعه شبکه اطلاعات و ارتباط از راه دور پیشرفته» همکاری نزدیکی با ستاد استراتژیک خواهد داشت. این ستاد با ارگان‌های مدیریت بحران، از جمله ستادهای واکنش اضطراری به تروریسم در زمان تشکیل همکاری کرده و اطلاعاتش را به‌اشتراک خواهد گذاشت، و در همکاری نزدیک با شورای امنیت ملی در رابطه با امنیت ملی اقدامات لازم را اتخاذ خواهد کرد.

به‌علاوه، این ستادها در هماهنگی با شورای امنیت ملی به مسائل مربوط به امنیت ملی واکنش نشان خواهند داد. در چنین مواردی، ارگان‌های دولتی مربوطه تحت هماهنگی کلی دبیرخانه امنیت ملی با یکدیگر همکاری خواهند کرد.

ستاد استراتژیک امنیت سایبری سیاست اولویت‌بندی بودجه را تعیین می‌کند و به دنبال تأمین و اجرای بودجه لازم برای دولت است تا تمهیدات آژانس‌های مربوطه طبق اصول مندرج در این استراتژی به طور پیوسته و مؤثر اجرا شود. این ستاد همچنین همکاری بین بخش‌های دولتی و خصوصی برای پیگیری توانایی‌های تحلیلی و اطلاعاتی مؤثر، و همچنین مکانیزم‌هایی برای چرخه بی‌عیب‌ونقص تشخیص زودهنگام،

تحلیل و قضاوت و مدیریت حملات سایبری را تشویق می‌کند.

با گذر زمان، برای اجرای دقیق این استراتژی، ستاد استراتژیک امنیت سایبری برنامه‌های سالانه از جمله لیست پیوست‌شده آژانس‌های متولی در طول دوره اجرای سه‌ساله این استراتژی را مطرح می‌کند و آژانس‌ها بر همین اساس به‌طور پیوسته اقدامات را اجرا می‌کنند. ستاد همچنین وضعیت پیشرفت این اقدامات را بررسی می‌کند، این گزارش را به عنوان گزارش سالانه تنظیم می‌کند و در برنامه سالانه سال بعد منعکس می‌کند. علاوه بر این، از آن‌جا که شرایط و مقدمات فنی در مورد فضای سایبری ممکن است به صورت ناپیوسته تکامل یابد، ممکن است خود استراتژی در زمان لازم، بدون توجه به مدت برنامه‌ریزی، به‌طور منعطفی بررسی شود.

فهرست نهادهای دولتی متولی استراتژی‌های سایبری

مسئولیت	نهاد مربوطه مسئولان اصلی: ◎ سازمان‌های دولتی مربوطه: ○
۱.۴. امکان ایجاد نشاط اجتماعی و اقتصادی و توسعه پایدار	
۱.۱.۴. پیشرفت امنیت سایبری به عنوان محرک ایجاد ارزش	
(۱) افزایش آگاهی اجرایی	◎: NISC[۱]، وزارت اقتصاد و صنعت ○: سازمان امور مالی
(۲) تقویت سرمایه‌گذاری در امنیت سایبری	◎: وزارت کشور، وزارت اقتصاد و صنعت
(۳) تقویت کسب‌وکارهای امنیت سایبری با حمایت از نوآوری‌هایی که از تکنولوژی پیشرفته استفاده می‌کنند	◎: وزارت اقتصاد و صنعت ○:وزارت کشور
۲.۱.۴. رسیدن به زنجیره تأمینی که به‌واسطه ارتباطات گوناگون ایجاد ارزش می‌کند	
(۱) تدوین چارچوب امنیت سایبری برای ریسک زنجیره تأمین	◎:وزارت اقتصاد و صنعت
(۲) ساخت یک سیستم برای تأمین امنیت سایبری در زنجیره‌تأمین	◎: دفتر کابینه ○:وزارت کشور، وزارت اقتصاد و صنعت ○: دفتر کابینه اداره یکپارچه‌سازی سیاست‌ها (مسئولان بخش علم و فناوری و نوآوری)
(۳) تبلیغ طرح‌ها توسط شرکت‌های کوچک و متوسط	◎: NISC، وزارت کشور، وزارت اقتصاد و صنعت
۳.۱.۴. ساخت سیستم‌های ایمن اینترنت اشیا	
۱) تقویت چارچوب ساختاری برای سیستم‌های اینترنت اشیا و استاندارد بین‌المللی	◎: NISC، وزارت کشور، وزارت اقتصاد و صنعت

۱. National Center of Incident Readiness and Strategy for Cybersecurity (مرکز ملی آمادگی برای حوادث و استراتژی فضای سایبری که از سال ۲۰۱۴ زیر نظر کابینه ژاپن تأسیس شد و ریاست آن با دبیر کابینه است و اعضای آن را دبیر شورای امنیت ملی و وزرای مرتبط تشکیل می‌دهند.) آدرس این مرکز:
https://www.nisc.go.jp/eng/

مسئولیت	نهاد مربوطه مسئولان اصلی: ◎ سازمان‌های دولتی مربوطه: ○
(۲) آماده‌سازی تشکیلاتی برای مقابله با آسیب‌پذیری	◎ : NISC، سازمان پلیس، وزارت کشور، وزارت اقتصاد و صنعت
۲.۴. ساخت جامعه‌ای امن و ایمن برای مردم	
۱.۲.۴. تمهیدات حفاظت از مردم و جامعه	
(۱) ایجاد فضای سایبری امن و ایمن برای کاربران	◎ : NISC، دبیرخانه کابینه، دفتر کابینه، سازمان امور مالی، وزارت کشور، وزارت کار، بهداشت و رفاه، وزارت اقتصاد و صنعت و وزارت راه و زیرساخت ○:دبیرخانه کابینه، دفتر کابینه، سازمان امور دربار، سازمان پلیس، سازمان امور مصرف‌کنندگان، وزارت دادگستری، وزارت امور خارجه، وزارت علوم و آموزش، وزارت کشاورزی، جنگل‌داری و شیلات، وزارت محیط زیست، وزارت دفاع
(۲) تقویت تمهیدات علیه جرایم سایبری	◎ : سازمان پلیس، وزارت دادگستری، وزارت کشور، وزارت اقتصاد و صنعت
۲.۲.۴. حفاظت از زیرساخت‌های حیاتی از طریق همکاری بخش‌های دولتی و خصوصی	
(۱) طرح‌های اولیه براساس «سیاست امنیت سایبری»	◎ : NISC، سازمان امور مالی، وزارت کشور، وزارت کار، بهداشت و رفاه، وزارت اقتصاد و صنعت و وزارت راه و زیرساخت ○: دبیرخانه کابینه، سازمان پلیس
(۲) تقویت و بهبود امنیت در حکومت‌های محلی	◎ : NISC، دفتر کابینه، وزارت کشور ○:دبیرخانه کابینه
۳.۲.۴. تقویت و بهبود امنیت در نهادهای دولتی و موجودیت‌های مرتبط با دولت	
(۱) بهبود و تصویرسازی تمهیدات امنیتی برای سیستم‌های اطلاعاتی	◎ : NISC، وزارت کشور، وزارت کار، بهداشت و رفاه، وزارت اقتصاد و صنعت

مسئولیت	نهاد مربوطه مسئولان اصلی: ◎ سازمان‌های دولتی مربوطه: ○
(۲) ترویج استفاده از فضای ابری برای تمهیدات امنیتی مؤثر	◎: NISC، دبیرخانه کابینه، وزارت کشور، وزارت اقتصاد و صنعت
(۳) تلاش‌های پیشگیرانه با استفاده از فناوری‌های پیشرفته	◎: NISC
(۴) افزایش سطح امنیت سایبری از طریق رسیدگی	◎: NISC ○: دفتر کابینه، سازمان امور مصرف‌کنندگان، وزارت کشور، وزارت امور خارجه، وزارت دارایی، وزارت علوم و آموزش، وزارت کار، بهداشت و رفاه، وزارت کشاورزی، جنگل داری و شیلات، وزارت راه و زیرساخت، وزارت محیط زیست، وزارت دفاع
(۵) تقویت توانایی واکنش سازمانی	◎: NISC، وزارت کشور ○: کارگزینی کل کشور
۴.۲.۴. ایجاد محیط آموزشی و پژوهشی امن و ایمن در دانشگاه و غیره	
(۱) ترویج تمهیدات با توجه به تنوع در دانشگاه‌ها و غیره	◎: وزارت علوم و آموزش ○: NISC
(۲) ترویج طرح‌های هماهنگ و مشترک توسط دانشگاه‌ها و غیره	◎: وزارت علوم و آموزش
۵.۲.۴. طرح‌هایی برای بازی‌های ۲۰۲۰ توکیو و پس از آن	
(۱) آماده‌بودن برای بازی‌های ۲۰۲۰ توکیو	◎: NISC، سازمان پلیس
(۲) انتقال نتایجی که به آینده ختم می‌شود	◎: NISC، سازمان پلیس، وزارت کشور، وزارت دادگستری
۶.۲.۴. ساخت چارچوب همکاری و به‌اشتراک‌گذاری اطلاعات که از چارچوب‌های سنتی فراتر می‌رود	◎: NISC، سازمان پلیس، سازمان امور مالی، وزارت کشور، وزارت کار، بهداشت و رفاه ، وزارت اقتصاد و صنعت و وزارت راه و زیرساخت

مسئولیت	نهاد مربوطه مسئولان اصلی: ◎ سازمان‌های دولتی مربوطه: ○
(۱) ترویج به‌اشتراک‌گذاری اطلاعات و همکاری بین چند نهاد ذی‌نفع	◎: NISC
(۲) به‌سوی مرحله‌ای جدید در به‌اشتراک‌گذاری اطلاعات و همکاری	◎: NISC
۷.۲.۴. تقویت آمادگی برای حوادث در مقابل حملات گسترده سایبری	◎: NISC، دبیرخانه کابینه، دفتر کابینه، سازمان پلیس، وزارت اقتصاد و صنعت
۳.۴. مشارکت در صلح و ثبات جامعه بین‌المللی و امنیت ملی ژاپن	
۱.۳.۴. تعهد به فضای سایبری آزاد، عادلانه و ایمن	◎: NISC ○: وزارت امور خارجه
(۱) مطرح کردن ایده‌های فضای سایبری آزاد، عادلانه و ایمن	◎: NISC، وزارت امور خارجه، وزارت اقتصاد و صنعت ○:سازمان پلیس، وزارت کشور، وزارت دفاع
(۲) ترویج حاکمیت قانون در فضای سایبری	◎: NISC، سازمان پلیس، وزارت دادگستری، وزارت امور خارجه ○:وزارت کشور، وزارت اقتصاد و صنعت، وزارت دفاع
۲.۳.۴. تقویت توانایی‌های دفاعی، بازدارندگی و آگاهی موقعیتی	
(۱) اطمینان از مقاومت ملی	◎: NISC، دبیرخانه کابینه، سازمان پلیس، وزارت دادگستری، وزارت علوم و آموزش، وزارت دفاع ○:دفتر کابینه، وزارت کشور، وزارت امور خارجه، بهداشت و رفاه، وزارت کشاورزی، جنگل داری و شیلات، وزارت راه و زیرساخت، وزارت محیط زیست
(۲) تقویت توانایی‌های بازدارندگی	◎: NISC، دبیرخانه کابینه، سازمان پلیس، وزارت امور خارجه، وزارت اقتصاد و صنعت، وزارت دفاع ○:وزارت کشور، وزارت دارایی

مسئولیت	نهاد مربوطه مسئولان اصلی: ◎ سازمان‌های دولتی مربوطه: ○
(۳) تقویت آگاهی موقعیتی سایبری	◎: دبیرخانه کابینه، سازمان پلیس، وزارت دادگستری، وزارت اقتصاد و صنعت، وزارت دفاع ○: NISC ، وزارت کشور، وزارت امور خارجه
۳.۳.۴. همکاری و هماهنگی بین‌المللی	◎: NISC ○: سایر سازمان‌ها و نهادها
(۱) سیاست به‌اشتراک‌گذاری تخصص و هماهنگی	◎: NISC، سازمان پلیس، وزارت کشور، وزارت امور خارجه، وزارت اقتصاد و صنعت، وزارت دفاع ○:وزارت دادگستری
(۲) همکاری بین‌المللی برای واکنش به حوادث	◎: NISC، وزارت اقتصاد و صنعت ○:سازمان پلیس، وزارت امور خارجه
(۳) همکاری برای ظرفیت‌سازی	◎: NISC، سازمان پلیس، وزارت کشور، وزارت امور خارجه، وزارت اقتصاد و صنعت
۴.۴. رویکردهای مقطعی به امنیت سایبری	
۱.۴.۴. توسعه و اطمینان از منابع انسانی امنیت سایبری	◎: NISC ○: وزارت کشور، وزارت علوم و آموزش، وزارت اقتصاد و صنعت
(۱) آموزش و پذیرش در سطح مدیریت استراتژیک	◎: NISC، وزارت علوم و آموزش، وزارت اقتصاد و صنعت
(۲) آموزش برای سطح عملیاتی و متخصص	◎: سازمان پلیس، وزارت کشور، وزارت علوم و آموزش، وزارت کار، بهداشت و رفاه، وزارت اقتصاد و صنعت، وزارت دفاع ○: NISC
(۳) آماده‌سازی بنیادی برای توسعه منابع انسانی امنیت سایبری	◎: وزارت کشور، وزارت علوم و آموزش، وزارت اقتصاد و صنعت

مسئولیت	نهاد مربوطه مسئولان اصلی: ◎ سازمان‌های دولتی مربوطه: ○
(۴) تقویت تضمین و توسعه آژانس‌های منابع انسانی امنیت‌سایبری	◎: NISC، وزارت کشور o:سایر نهادها و سازمان‌های مربوطه
(۵) ترویج شراکت بین‌المللی	◎: NISC، وزارت اقتصاد و صنعت
۲.۴.۴. پیشرفت پژوهش و توسعه	
(۱) ترویج R&D عملی	◎: NISC، دفتر کابینه، وزارت کشور، وزارت علوم و آموزش، وزارت اقتصاد و صنعت o: دفتر کابینه اداره یکپارچه‌سازی سیاست‌ها (مسئولان بخش علم و فناوری و نوآوری)
(۲) واکنش با نگاه به تکامل میان‌مدت و بلندمدت تکنولوژی و جامعه	◎: NISC o: سایر نهادها و سازمان‌های مربوطه
۳.۴.۴. همکاری توسط همه کسانی که نقشی اصلی در امنیت سایبری دارند	◎: وزارت کشور، وزارت علوم و آموزش، وزارت اقتصاد و صنعت o:وزارت دادگستری
۵. ترویج و اجرای امنیت سایبری	◎: NISC، دبیرخانه کابینه o:وزارت کشور

csri.majazi.ir

حوزه فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانه پر از آب و خروشان است که می آید و دائماً هم بر آب آن افزوده و خروشان تر می شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه‌کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می‌شود فرصت. اگر رهایش کنیم و برنامه‌ای برای آن نداشته باشیم می‌شود یک تهدید.

csri.majazi.ir