مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گزارش سریع
پنجاهم

استراتژی امنیت ملی سایبری در ایرلند

National Cyber Security Strategy
in Ireland

بسم الله الرحمن الرحیم

گزارش سریع

گزارش شماره ۵۰
شهریور ۱۴۰۱

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

راهبرد ملی امنیت سایبری
ایرلند

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: اسماعیل یزدان پور
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

خلاصه مدیریتی

خلاصه مدیریتی

ایرلنـد از نظـر جـذب و اسـتفاده از فناوری‌هـای دیجیتـال رتبـه بالایـی را در میـان کشـورهای عضـو اتحادیـه اروپـا بـه خـود اختصـاص داده اسـت. ایـن فناوری‌هـا در ایرلنـد هـم ماننـد سـایر کشـورهای توسـعه‌یافته، نقشـی اساسـی در پشـتیبانی و تسـهیل زندگـی اقتصـادی و اجتماعـی ایفـا کرده‌اند. ایرلنـد بـا توسـعه زیسـت‌بوم جهانـی داده توانسـته اسـت بـه سـود اقتصادی بسـیار چشـمگیری دسـت یابد. موقعیـت جغرافیایی، اقتصاد بـاز و عضویت در اتحادیـه اروپـا، از جمله عواملی اسـت که توانسـته اسـت این تضمیـن را برای ایرلنـد فراهـم آورد تـا حجـم قابل‌توجهـی از داده و فعالیت‌هـای اقتصـادی را میزبانـی کنـد. بااین‌وجود، توسـعه و به‌کارگیری روزافـزون اینترنت و مجموعه عظیمـی از ابزارهـا و دسـتگاه‌های مرتبـط بـا یکدیگر، باعث وابسـتگی شـدید بـه این سـامانه‌ها شـده اسـت. ایـن وابسـتگی، به مجموعـه پیچیده و سـیالی از مخاطراتـی انجامیـده اسـت کـه برخـی از آن‌ها ناشـی از اشـتباه در طراحی یـا عملکـرد سـامانه‌ها بـوده و منجـر بـه اتـلاف نامنتظـره خدمـات می‌شـود. مخاطـرات دیگـری هـم در اثر فعالیت‌های عمـدی گروه‌های سازماندهی‌شـده و از جملـه دولت‌هـا بـه وجـود می‌آیـد، آن‌هـا کـه بـرای مقاصد خـاص تلاش می‌کننـد ایـن سـامانه‌ها را از کار انداختـه یـا در آن نفـوذ کننـد تـا بـه اهداف

خاصی برسند. این نفوذ می‌تواند به‌صورت دزدی یا تخریب اطلاعات یا پول بوده و از راه متلاشی کردن یا تخریب خدمات یا زیرساخت‌ها صورت گیرد. درنتیجه، این مخاطرات مجموعه‌ای از پیامدهای پیچیده و به‌هم‌پیوسته برای دولت‌ها دارد که طیف گسترده‌ای از صیانت اطلاعات شهروندان تا حفاظت از زیرساخت‌ها و خدمات اصلی را در برمی‌گیرد.

امنیت سایبری اغلب به‌عنوان مجموعه فعالیت‌هایی برای تضمین محرمانه بودن، انسجام کلی، اصالت، دسترس‌پذیری شبکه‌ها، ابزارها و اطلاعات تعریف می‌شود. اما ازآنجاکه سامانه‌های اطلاعاتی و شبکه‌ها پیچیده‌تر شده و در همه ابزارها به کار گرفته می‌شوند، تضمین امنیت آن‌ها اهمیت بیشتری پیداکرده و دشوارتر می‌شود. با آن‌که این مجموعه پاسخ‌ها در تلاش با همراهی با تحولات فنی و بازاری، با سرعت بالایی توسعه یافته است، ماهیت به‌شدت پویا و پرانرژی این تحولات هم از نظر فناوری‌ها و هم از نظر شرایط راهبردی جهانی، باعث چالش‌های بیشتری در کل این فرایند می‌شود.

نخستین راهبرد ملی امنیت سایبری ایرلند در جولای سال ۲۰۱۵ به تصویب حاکمیت رسیده و منتشر شد. این سند، نقشه راهی را برای توسعه «مرکز ملی امنیت سایبری» و مجموعه‌ای از اقدامات برای حفاظت بهتر از شبکه‌ها و داده‌های حاکمیتی و زیرساخت‌های حساس ملی مشخص کرد. از زمان تأسیس «مرکز ملی امنیت سایبری» تاکنون، این مرکز از نظر گستره و ظرفیت رشد چشمگیری داشته است و در جریان اجرای بخشنامه امنیت اطلاعات و شبکه اتحادیه اروپا به شماره ۱۱۴۸ سال ۲۰۱۶، مجموعه‌ای از اقدامات قابل‌توجه را برای پشتیبانی سازمان‌ها و دستگاه‌های دولتی به‌منظور مدیریت سامانه‌ها به انجام رسانده است.

افـزون بـر ایـن، حـدود ۷۰ اپراتـور زیرسـاخت‌های حسـاس ملـی جایـگاه حقوقـی تعریف‌شـده‌ای پیـدا کرده‌انـد و الزامات امنیتی آن‌ها مشـخص شـده و وظایـف آن‌هـا در شـرایط اعـلان حادثه تعریف شـده اسـت. وقتـی همه این مـوارد در کنـار یکدیگر قـرار می‌گیرد، معلوم می‌شـود که دولـت و اپراتورهای زیرسـاخت‌های حسـاس ملـی آمادگـی بسـیار بیشـتری بـرای مواجهـه بـا مخاطـرات امنیـت سـایبری نسـبت به گذشـته دارند.

البتـه یکـی از ویژگی‌هـای اصلـی بخش فناوری، پویایی شـدید آن اسـت و بـه نظـر می‌رسـد که مـوج جدیـدی از تحولات فنی در راه اسـت کـه در مرکز آن شـبکه‌های مجازی قـرار دارد و از پروتکل‌های پیشـرفته ارتباطی (همچون نسـل پنجـم تلفن همـراه)، هوش مصنوعی و اینترنت اشـیاء اسـتفاده می‌کند. این پیشـرفت‌های مرتبط بـا یکدیگر، به احتمال زیاد کاربردهای وسـیعی پیدا خواهنـد کـرد و ایـن بدان معناسـت که نفوذ بیشـتری بـه زندگی شـهروندان پیـدا خواهنـد کـرد و بـر زیرسـاخت‌های وابسـته اثـر خواهند گذاشـت. افزون بـر ایـن، ماهیت مبتنی بـر نرم‌افـزار این فناوری به‌گونه‌ای اسـت کـه ابزارهای رگلاتـوری و حاکمیتـی ویـژه‌ای لازم خواهنـد آمد تا امنیت و سـلامت داده‌ها و خدمات تضمین شـود.

ایـن پیشـرفت‌ها همـراه بـا رشـد سـریع صنعـت جهانـی بـوده اسـت کـه خدمـات و محصولاتـی بـرای تأمیـن امنیـت زیرسـاخت‌ها و سـامانه‌های دیجیتـال را هـدف قـرار داده‌انـد. در ایرلنـد کـه بیـش از ۶۵۰۰ نفـر در بخش امنیـت دیجیتـال مشـغول بـه کار هسـتند، ایـن صنعـت یکـی از مهم‌تریـن بخش‌هـای بخـش فنـاوری شـده اسـت کـه اسـتقلال خـودش را هـم دارد و توانمندسـازی سـرمایه‌ها در بخش‌هـای وابسـته را هـم به‌پیـش می‌بـرد. صیانـت از ایـن موفقیـت و مبنـا قـرار دادن آن‌هـا نقـش مهمـی در تضمیـن

اشتغال کیفی و رشد اقتصادی آینده دارد و همچنین حضور و فعالیت زیست‌بوم گسترده امنیت سایبری با نفوذ همه‌جانبه را تأمین می‌کند.

جذب و به‌کارگیری ظرفیت‌های فناوری‌های دیجیتال در سطحی ملی همچنان یکی از فرایندهای جاری و مهم هست، کاری که در همه بخش‌های حاکمیتی پیگیری می‌شود. «راهبرد خدمات عمومی ۲۰۱۵» توسط «خدمات عمومی ما، ۲۰۲۰» بازآفرینی شده است، چارچوب سیاستی جدیدی که مبتنی بر اقدامات اصلاحی پیشین است و درعین‌حال دامنه اصلاحات را چنان بسط می‌دهد تا تمرکز بهتری بر همکاری، نوآوری و ارزیابی ایجاد شود. در سطحی ملی، «برنامه پهنای باند ملی» به دنبال فراهم آوردن این تضمین است که برای نخستین بار، بیش از نیم میلیون نفر دسترسی به پهنای باند با سرعت بالا داشته باشند و «راهبرد دیجیتال ملی» آینده مشخص خواهد کرد که چگونه حاکمیت تلاش دارد منافع دیجیتالی شدن را در اختیار همگان قرار دهد. همه این موارد در کنار یکدیگر، آثار مثبت و ایجابی بر رشد اقتصادی، تعادل منطقه‌ای و فرصت‌های فردی خواهند داشت؛ هرچند این دیجیتالی شدن درجاتی از خطر را هم به همراه دارد.

این سند راهبردی شیوه مواجهه ایرلند با این چالش‌ها را مشخص خواهد کرد و نشان خواهد داد که برای استفاده از فرصت‌های حاصل از این تحولات تکنولوژیک جهانی برای ایجاد اشتغال باید چگونه برنامه‌ریزی کنیم. این سند راهبردی مجموعه‌ای از اقدامات را مشخص می‌کند که برای مواجهه با برخی از چالش‌های پیچیده ناشی از اشتغال تعداد روزافزونی از مردم شاغل در این حوزه مناسب خواهد بود.

دست‌آخر، توسعه شبکه و امنیت اطلاعات به‌مثابه مضمون اصلی

سیاست‌ها، ابعاد بین‌المللی قابل‌توجهی هم دارد که هم علاوه بر بحث مهم حاکمیت اینترنت، در مسائل بسیار حساس روابط بین‌الملل نمود پیدا می‌کند. امنیت سایبری یکی از موضوعات ردیف اول در مسائل روابط بین‌الملل است. این سند راهبردی مشخص می‌کند که ایرلند چگونه می‌تواند نقشی در شکل دادن به این فضا در سطح بین‌المللی داشته باشد.

اقدامات

اقدامات

در طول دوره سال‌های ۲۰۲۴-۲۰۱۹ هم زمان با توسعه اینترنت، حاکمیت اقدامات نظام‌مند ذیل را به‌منظور صیانت از ملت، توسعه بخش امنیت سایبری و تعمیق روابط بین‌المللی به اجرا خواهد گذاشت.

۱) «مرکز ملی امنیت سایبری»، به‌خصوص با توجه به گسترش توانایی برای نظارت و پاسخگویی در برابر حوادث امنیت سایبری و تهدیدهای فزاینده در برابر دولت، توسعه بیشتری خواهد یافت.

۲) اطلاعات و تحلیل‌های تهیه شده پیرامون تهدید توسط «مرکز ملی امنیت سایبری» در کارهای مرکز بررسی‌های امنیت ملی ادغام خواهد شد.

۳) سامانه کنونی حفاظت از زیرساخت‌های حساس ملی که بر اساس شیوه‌نامه امنیت شبکه و اطلاعات ملی راه‌اندازی شده است، با تمرکز ویژه بر برنامه‌های همگرایی و ممیزی مستمر در جهت کاهش خطرات خدمات اصلی همچنان به کار گرفته شده و توسعه می‌یابد.

۴) «مرکز ملی امنیت سایبری» با همکاری نیروهای نظامی و انتظامی، یک ارزیابی دقیق و به‌روز از آسیب‌پذیری‌های ممکن در همه خدمات و زیرساخت‌های حساس در برابر حملات سایبری انجام خواهد داد.

۵) سامانه پشتیبانی از زیرساخت‌های حساس ملی در طول اجرای سند راهبردی، گسترش و تعمیق خواهد یافت تا دامنه وسیع‌تری از زیرساخت‌های حساس ملی و ازجمله ابعادی از سامانه‌های انتخاباتی را شامل شود.

۶) گروه‌های اشتراک اطلاعات فعلی که توسط «مرکز ملی امنیت سایبری» اداره می‌شوند، توسعه بیشتری خواهند یافت و گروه‌های اشتراک تهدید فعلی چنان توسعه خواهند یافت تا طیف وسیع‌تری از زیرساخت‌های حساس ملی را شامل شوند.

۷) حاکمیت، مجموعه جدیدی از استانداردهای همگرایی را معرفی خواهد کرد تا امنیت سایبری زیرساخت‌های مخابراتی کشور را پشتیبانی کند.

۸) «مرکز ملی امنیت سایبری» یک استاندارد امنیتی پایه را تعیین خواهد کرد تا توسط همه دستگاه‌های دولتی و سازمان‌های اصلی به کار گرفته شود.

۹) طرح «حسگر» فعلی گسترش خواهد یافت تا تمام وزارتخانه‌های دولتی را در برگیرد، و یک ارزیابی جامع انجام خواهد شد تا میزان امکان‌پذیری توسعه «حسگر» برای پوشش تمامی شبکه‌های دولتی بررسی شود.

۱۰) به‌منظور سهولت در اشتراک اطلاعات، اقدامات برتر و نیز فراهم آوردن امکاناتی برای «مرکز ملی امنیت سایبری» در راه پشتیبانی از به‌کارگیری استانداردهای امنیتی پایه، مجمع حاکمیتی امنیت فناوری‌های اطلاعاتی ایجاد خواهد شد و تمامی مدیران امنیت فناوری‌های اطلاعات در سراسر حاکمیت می‌توانند عضو آن شوند.

۱۱) «مرکز ملی امنیت سایبری» از طرف حاکمیت موظف به انتشار توصیه‌هایی در رابطه با استفاده از نرم‌افزارها و سخت‌افزارهای خاص در زیرساخت‌های مخابراتی و فناوری‌های اطلاعاتی دولت خواهد شد.

۱۲) حاکمیت توسعهٔ و استفاده از آموزش سطح دوم و سوم در علوم رایانه و امنیت سایبری را همچنان تضمین خواهد کرد و این کار را از جمله از راه پشتیبانی از شبکه‌های آموزش مهارت در ایرلند در توسعه برنامه‌های آموزشی برای همه سطوح و همچنین پشتیبانی از ابتکارات مراکز آموزشی پیشرفته «سولاس» (طرح آموزش مهارت‌های تکمیلی ایرلند) برای برنامه‌های کارآموزی فناوری‌های اطلاعاتی و ارتباطی و امنیت سایبری پیگیری خواهد کرد.

۱۳) بنیاد علوم ایرلند در چارچوب «برنامه آینده‌های هوشمند»، به ترویج امنیت سایبری به‌عنوان یک گزینه شغلی در مدارس و دانشگاه‌های ایرلند خواهد پرداخت.

۱۴) بنیاد علوم ایرلند با همکاری وزارت سرمایه، تجارت و اشتغال و نیز وزارت محیط‌زیست، آب‌وهوا و ارتباطات، از طریق برنامه آینده‌های هوشمند، مراکز آموزشی بنیاد و دیگر بنگاه‌ها، کار امکان‌سنجی تأمین بودجه برای پژوهش در حوزه امنیت سایبری را انجام خواهند داد.

۱۵) حاکمیت به پشتیبانی و همکاری کامل خود با برنامه ایرلند سایبری با بودجه سازمان جذب سرمایه‌های خارجی ادامه خواهد داد و سازوکارهای جدیدی را برای حمایت از همکاری‌های صنعت / دانشگاه / دولت در زمینه امنیت سایبری بررسی خواهد کرد.

۱۶) سازمان توسعه بنگاه‌های ایرلند در جهت تسهیل پیوندهای مشترک بین نهادهای پژوهشی و سازمان‌ها، یک برنامه اختصاصی در زمینه امنیت

سایبری را طراحی و اجرا خواهد کرد که به کاربرد عملی پژوهش در تجارت خواهد انجامید.

۱۷) تعهدات دیپلماتیک ایرلند در زمینه امنیت سایبری را تقویت خواهیم کرد و برای این کار از جمله به استقرار وابستگان سایبری در مأموریت‌های اصلی دیپلماتیک و ایجاد ظرفیت پایدار در کشورهای سوم خواهیم پرداخت.

۱۸) به‌منظور هماهنگی مواضع ملی در سراسر دستگاه‌های حاکمیتی، یک گروه میان‌بخشی در زمینه حاکمیت اینترنت و سیاست بین‌المللی فضاهای سایبری ایجاد خواهیم کرد.

۱۹) همکاری‌های فعلی خود با سازمان‌های بین‌المللی را گسترش خواهیم داد و برای این کار از جمله به مرکز برتر امنیت سایبری در تالین، استونی خواهیم پیوست.

۲۰) دولت یک پویش سراسری اطلاعات امنیت سایبری در سطح ملی ایجاد خواهد کرد تا از اطلاعات ارائه‌شده توسط «مرکز ملی امنیت سایبری» و اداره ملی جرائم سایبری پلیس استفاده کرده و اطلاعاتی را در اختیار دستگاه‌هایی قرار دهد که به‌صورت مستقیم مشغول تدارک اطلاعات هستند.

برنامه اجرایی دقیق اقدامات مربوط به این حوزه، از جمله جدول زمانی و سازمان‌های مسئول، در پیوست آمده است.

مقدمه

مقدمه

ایرلنـد از نظـر جـذب و اسـتفاده از فن‌آوری‌هـای دیجیتـال در میـان رتبه‌هـای برتـر کشـورهای عضـو اتحادیـه اروپـا قـرار دارد (هفتمین کشـور از ۲۸ کشـور عضـو اتحادیـه اروپا بر اسـاس شـاخص اقتصـاد و جامعـه دیجیتال کمیسـیون اروپـا، ۲۰۱۹). از نظـر کاربـردی، ایـن بدان معناسـت کـه اینترنت و مجموعـه وسـیعی از فناوری‌هـا و دسـتگاه‌های متصـل بـه آن نقـش مهمی را در توانمندسـازی و تحقـق موفقیـت اقتصـادی مـا داشـته‌اند. به‌عـلاوه، این فناوری‌هـا همچنیـن امـکان پیشـرفت قابل‌توجهـی در بهـره‌وری و کیفیـت زندگـی را فراهـم آورده و کارایـی و پایـداری بیشـتری در اسـتفاده از منابـع را ممکـن کرده‌انـد. درعین‌حـال همیـن فناوری‌هـا، مجموعـه‌ای از مخاطـرات و تهدیدهـا را هـم بـه همـراه دارند. با مسـئله‌ای پرتحرک و پویا مواجه هسـتیم؛ بـا هـر دسـتگاه جدیـدی کـه بـه اینترنـت وصـل می‌شـود، بـر پیچیدگی‌ها و چالش‌هـای ایـن مسـئله افـزوده می‌شـود و بـا تمامی ابعـاد زندگی مـا ارتباط پیـدا می‌کند.

مواجهه با این چالش، هم از نظر مقاومت زیرساخت‌ها و خدمات اصلی و هم توانایی دولت در مدیریت و پاسـخگویی به حوادث، یکی از مهم‌ترین فعالیت‌ها بـرای تأمیـن رفـاه اقتصـادی و اجتماعـی دولـت و مردم شـده اسـت. این کار

ساده‌ای نیست. امنیت سایبری شبکه پیچیده‌ای از موضوعات را برای حل‌وفصل به همراه دارد. فناوری‌های فعال و متصل به مدد اینترنت، پیش‌ازاین در همه ابعاد و حوزه‌های زندگی ما نفوذ پیدا کرده است و خدمات قابل‌اتکای و غیرقابل‌اجتنابی را هم در سطح فردی و هم در سطح اجتماعی ارائه می‌دهد. ماهیت متنوع این بخش‌های مختلف با الگوهای متنوعی که برای مالکیت دارند، در عمل به این معنی است که هیچ الگو یا راه‌حل واحدی، از نوع فنی یا غیرفنی وجود ندارد که متناسب با همه بخش‌ها باشد. برای تدوین راهبردی ملی به‌منظور پاسخ، نیاز به رویکردی پویا و انعطاف‌پذیر هست؛ رویکردی که راه‌حل‌های مختلف را بر اساس ماهیت بخش موردنظر و خطرهای نمایان شده در برابر جامعه، زندگی انسان و اقتصاد به کار می‌گیرد.

ماهیت جهانی اینترنت پیامدهای ژئوپلیتیکی قابل‌توجهی نیز دارد هر نوعی از زیرساخت متصل به اینترنت در معرض تهدید از سراسر زمین قرار دارد. به‌این‌ترتیب، جغرافیای امنیت ملی تغییر یافته است و پرسش‌های عمیقی در برابر سیاست امنیت ملی ایرلند قرار داده است. در وهله نخست، مدیریت جهانی اینترنت، نحوه اداره آن و نحوه رفتار و عملکرد کشورها و دیگران، تبدیل به نگرانی اصلی در سطح ملی شده است. دوم آن‌که امنیت هر فرایند، خدمات و زیرساخت در ایرلند، از روند انتخابات تا زیرساخت‌های نظامی و امنیت داده‌های بخش‌های حاکمیتی باید به روش‌های متفاوتی مورد بررسی قرار گیرد، چرا که همه این‌ها تا حدی، به ابزارهای متصل به اینترنت وابسته هستند و اکنون ممکن است از هر جای کره زمین هدف مورد حمله مستقیم واقع شوند.

دست‌آخر این‌که ماهیت اقتصاد ما هم تغییری اساسی یافته است. بر اساس

برخی تخمین‌ها، ایرلند بیش از ۳۰ درصد از کل داده‌های اتحادیه اروپا را میزبانی کرده و مقر اصلی چند شرکت بزرگ فناوری جهان را در مرکز اروپا قرار داده است. بنابراین موفقیت اقتصادی ما وابستگی زیادی با توانایی پیوسته ما برای ایجاد فضایی امن برای فعالیت این شرکت‌ها دارد. بنابراین، امنیت شبکه و سامانه‌های اطلاعاتی ما نقشی بنیادی در رشد اقتصادی و اجتماعی جامعه ایرلند دارد. اولین سند راهبرد ملی امنیت سایبری که در سال ۲۰۱۵ منتشر شد، به تأسیس عمل‌گرا و کاربردی «مرکز ملی امنیت سایبری» انجامید و مجموعه‌ای از اقدامات جامع به‌منظور صیانت از زیرساخت‌های مهم و حساس ملی و امنیت داده‌ها و سامانه‌های حاکمیتی را ایجاد کرد. خود همین اقدامات، مجموعه گسترده‌تری از موضوعات را نسبت به گذشته در برمی‌گیرد؛ چالش‌هایی پیرامون مهارت‌ها، توسعه شرکت‌ها، و پژوهش وجود دارد که نیاز به اقدامات مستقل دارند.

فرایند تدوین این سند راهبردی توسط شورای عالی راهبردی مدیریت می‌شد که مدیریت آن بر عهده وزارت ارتباطات، کنش اقلیمی و محیط‌زیست بود و نمایندگانی از وزارت امور داخله، وزارت امور خارجه و تجارت، وزارت کار و تأمین اجتماعی، وزارت دفاع، دفتر واحد اطلاعات حاکمیتی، وزارت دادگستری و برابری و وزارت سرمایه، تجارت و اشتغال در این شورا حضور دارند.

کل این فرایند توسط مجموعه‌ای از سازوکارهای مشورتی هدایت می‌شد. در مرحله نخست، مجموعه‌ای از پنج گروه درگیر با مسئله شامل سهام‌داران بخش‌های دولتی و خصوصی در کنار هم قرار گرفتند. این گروه‌ها، به مسئله نظم و امنیت ملی، توسعه بنگاه‌ها، مهارت و پژوهش،

امنیت فناوری‌های اطلاعاتی و ارتباطی بخش دولتی و حفاظت از زیرساخت‌های حساس ملی پرداختند و مأمور به تضمین جامعیت سند راهبردی و پرداختن سند به طیف وسیعی از مسائل و موضوعات بودند. هر یک از این گروه‌ها دو بار تشکیل شدند، یک‌بار پیش از مشاوره‌های عمومی و برای تضمین این‌که پرسش‌ها و اسناد مشورتی متناسب هستند و نیز برای تشخیص دغدغه‌هایی که بر هر بخش اثر می‌گذارند. جلسه دوم پس از پایان مشاوره‌های عمومی انجام می‌گرفت و نتایج آن در اختیار اعضای گروه قرار می‌گرفت که به همراه نتایج پیشنهادی سند راهبردی بود. این گروه‌ها مجمعی را تشکیل دادند که در آن، همه افراد با آزادی نظرها، دغدغه‌ها و ایده‌های خود را مطرح می‌کردند و ارزش زیادی برای تعیین چارچوب و بستر سند راهبردی داشته و به کار شناسایی راه‌حل‌هایی برای چالش‌های موجود می‌آمدند.

یک مجمع مشورتی عمومی بین ماه‌های مارس و مه سال ۲۰۱۹ برگزار شد که در آن خلاصه‌ای از پیش‌نویس سند راهبردی به‌عنوان بخشی از فرایند مشورتی عمومی منتشر شد تا نظر عمومی و گستره وسیعی از صنایع اخذ شود. اعضای عمومی ۳۰ روز کاری مهلت داشتند تا خلاصه پیش‌نویس سند راهبردی را ارسال کنند و درمجموع ۴۷ نظر مکتوب دریافت شد. این نظرات دریافت شده توسط گروه راهبری و پنج گروه همکار از هر بخش ارزیابی شد و اقدامات پیشنهادی هر بسته استخراج شده و برای تجزیه‌وتحلیل بیشتر مقوله‌بندی شد. این تحلیل همچنین شامل ارزیابی بیش از ۳۰ استراتژی ملی از سراسر اروپا و خارج از اروپا شد و همچنین اسناد، نمونه‌های موفقی از «سازمان همکاری اقتصادی و توسعه» و «آژانس امنیت سایبری اتحادیه اروپا» بود.

بخش اول

بخش اول

چشم‌انداز

در چشم‌انداز ما، ایرلند جامعه‌ای است که می‌تواند با خیال راحت از فرصت‌های انقلاب دیجیتال بهره‌مند شود و می‌تواند سهم عمده‌ای در شکل دادن به آینده اینترنت داشته باشد. برای نیل به این هدف باید اقدامات زیر را انجام داد:

حفاظت از دولت، مردم و زیرساخت‌های حساس ملی در برابر مسائل امنیت سایبری به صورتی پویا و منعطف، به شکلی که حقوق افراد را به تمامی رعایت کرده و متناسب با آن، تعادلی میان مخاطرات و هزینه‌ها ایجاد کند.

توسعه ظرفیت‌های دولت، نهادهای پژوهشی، بخش تجاری، بخش عمومی و عموم مردم در راه فهم بهتر ماهیت و مدیریت چالش‌هایی که با آن در این عرصه مواجه می‌شویم و نیز برای اطمینان از این‌که افراد و سازمان‌ها می‌توانند از مزایای اقتصادی و شغلی فناوری اطلاعات و به‌خصوص امنیت سایبری بهره گیرند.

مشارکت در سطح ملی و بین‌المللی با اصولی راهبردی، پشتیبانی از فضای سایبری آزاد، گشوده، صلح‌آمیز و ایمن و نیز اطمینان از این‌که امنیت سایبری یکی از مؤلفه‌های اصلی مواضع دیپلماتیک ما در سراسر همکاری‌ها است.

بخش دوم

بخش دوم

اهداف

- بهبود مستمر میزان توانایی دولت در پاسخگویی و مدیریت حوادث امنیت سایبری، از جمله مواردی که مؤلفه‌های امنیت ملی دارند؛
- شناسایی و حفاظت از زیرساخت‌های حساس ملی از طریق افزایش مقاومت آن‌ها در برابر حمله‌های سایبری و اطمینان از این‌که اپراتورهای خدمات اساسی، برنامه‌های مناسبی برای مقابله در نظر دارند و می‌توانند هرگونه اختلال در خدمات را کاهش داده و مدیریت کنند ؛
- تقویت مقاومت و امنیت سامانه‌های بخش عمومی فناوری‌های اطلاعاتی به‌منظور حفاظت بهتر از داده‌ها و خدماتی که مورداتکای مردم است؛
- سرمایه‌گذاری در طرح‌های آموزشی به‌منظور آماده‌سازی نیروی کار برای پذیرش شغل‌های فناوری‌های پیشرفته اطلاعاتی و امنیت سایبری؛
- ارتقای آگاهی‌ها پیرامون مسئولیت‌های سازمان‌ها در خصوص ایمن‌سازی شبکه‌ها، ابزارها و اطلاعات و تأمین و هدایت تحقیق و توسعه در امنیت سایبری در ایرلند، از جمله از راه تسهیل در سرمایه‌گذاری

برای فناوری‌های جدید؛

- ادامه همکاری‌های با شرکای بین‌المللی و سازمان‌های بین‌المللی به‌منظور اطمینان از این‌که فضاهای سایبری همچنان گشوده، ایمن، یکپارچه، آزاد و توانا در جهت تسهیل توسعه اقتصادی و اجتماعی باقی می‌ماند؛

- افزایش سطح عمومی مهارت‌ها و آگاهی‌ها در میان افراد در حوزه اصول بهداشتی سایبری و پشتیبانی از آنان از طریق ارائه اطلاعات و آموزش.

بخش سوم

بخش سوم

مخاطـرات و جامعـه اطلاعاتی

از همـان ابتـدای طـرح «آرپانت» در دهه ۱۹۶۰ میلادی در امریـکا، بنابراین بـود کـه اینترنـت سـامانه گشـوده‌ای باشـد کـه هـر نقطـه در شـبکه امـکان دریافـت پیـام از نقطه‌هـای دیگـر را داشـته و بـرای حرکـت اطلاعـات از یـک نقطه‌به‌نقطـه دیگـر مسـیرهای مختلفـی در پیـش داشـته باشـد. به‌رغـم این واقعیـت کـه هم‌اکنـون میلیاردها دسـتگاه‌های متصل به شـبکه‌ای در سراسـر جهـان وجـود دارد، همـان اصول بنیادین هنـوز پابرجا اسـت و درواقع، یکی از پایه‌هـای اصلـی رشـد سـریع اینترنـت و کاربـرد آن بـرای جوامع بشـری بوده است.

البتـه ایـن گشـودگی و سـادگی در ارتبـاط، امکان اسـتفاده از شـبکه برای فعالیت‌هـای بدخواهانـه را هم تسـهیل کرده اسـت. در طول زمـان و با اهمیت یافتـن روزافـزون اینترنـت، دامنـه بالقـوه و اثر چنیـن اقداماتی افزایـش یافته و طیـف وسـیعی از خطـرات جدیـد را در برابـر جامعـه و اقتصـاد ایجـاد کرده اسـت. این بخـش مخاطرات اصلی پیـش روی ایرلند را به‌طـور خلاصه معرفی می کند.

۳ - ۱- مخاطرات راهبردی

توسعه امنیت سایبری دو چالش بنیادین را در سطحی بسیار بالا برای ایرلند ایجاد می‌کند. نخست آن‌که ماهیت غیرمکانی اینترنت، دولت را در برابر چالش‌های روزافزون جهانی و از جمله تهدیدهای ایجادشده و به کار گرفته شده توسط گروه‌های خطرناک با قدرت و منابع قوی قرار می‌دهد. این خطرها خود را در سطح ملی و به شکل‌های مختلفی نشان می‌دهند و امکان شناسایی و مواجهه با پیامدهای آن بسیار دشوار است. این واقعیت که فضاهای امنیتی جهانی در مرحله گذرا و پرجنب‌وجوشی قرار دارد هم اهمیت دارد؛ بازگشت آشکار سیاست «قدرت بزرگ» در روابط بین‌الملل در کنار تنش‌های پیرامون تجارت و فروش فناوری، چالش‌های خاصی را بر سر راه اقتصادهای کوچک و گشوده‌ای همچون ایرلند ایجاد می‌کند.

دوم آن‌که پایه فناوری اقتصاد ایرلند در سال‌های اخیر توسعه قابل‌توجهی یافته است؛ دولت حالا محل استقرار بخش مهمی از اطلاعات اروپا شده است (بر اساس برخی ارزیابی‌های بخش صنعت، بالاتر از ۳۰ درصد) و دفتر مرکزی برخی از بزرگترین شرکت‌های فناوری جهان در ایرلند قرار دارد. این نکته هم بسیار مهم است که تکامل مفهومی رایانش ابری پیامدهای عمیقی برای ایرلند به همراه داشته است. در بسیاری از موارد، این مراکز ذخیره اطلاعات، انبارهای منفعل و غیرفعال داده و اطلاعات نیستند بلکه پایگاه‌های مهم عملیات امروزی هستند؛ هر حادثه یا قطعی در یکی از این پایگاه‌ها، می‌تواند اثرات فوری و مخربی بر زیرساخت‌ها یا تجارت در سطح اتحادیه اروپا یا جهان به همراه داشته باشد. این بدان معناست که زیرساخت‌های پشتیبان این مراکز، اعم از دولتی و خصوصی، اکنون ابعاد امنیتی و اقتصادی گسترده‌تری دارند.

در سال‌های اخیر، شاهد توسعه و استفاده منظم از ابزارهای بسیار پیشرفته مجهز به ابزارهای سایبری برای حمله و جاسوسی بوده‌ایم و شاید اولین بار باشد که ابزارهای سایبری توانسته باشند زیرساخت‌های حساس ملی را تخریب کنند. به همین خاطر، یکی از ویژگی‌های اصلی حوزه امنیت سایبری، جریان مداوم و پرخطر مسابقه تسلیحاتی فناوری در دو شکل تهاجمی و تدافعی شده است.

ماهیت پیوندهای شبکه‌ای زیرساخت‌ها پیچیدگی‌های بیشتری را سبب می‌شود. نخست آن‌که به‌هرحال همه این فرایندها و رویدادها در نظام جهانی رخ می‌دهد، هم از نظر زنجیره عرضه دستگاه‌ها و نرم‌افزارها و هم از نظر شبکه‌ای که این‌ها را به هم وصل می‌کند؛ این بدان معناست که هر کشور حتی در قلمرو خود، فقط حد محدودی از کنترل عملکرد این شبکه را در دست دارد. همچنین و مهم آن‌که، این دستگاه‌ها و سامانه‌ها متعلق به طیف گسترده‌ای از انواع مشاغل و سازمان‌ها هستند. درواقع، اکنون بسیاری از خانه‌های شخصی چندین دستگاه متصل به اینترنت دارند، امری که با ظهور و نفوذ پیوسته اینترنت اشیا شیوع بیشتری خواهد یافت. این بدان معناست که هماهنگی اقدامات حفاظتی یا پاسخ به حوادث یا حملات در طیف وسیعی از اهداف بالقوه، خود تبدیل به چالش بسیار پیچیده‌ای شده است.

علاوه بر این، تا زمانی که دولت‌ها بر نظام نظارتی سرزده تأکید دارند، برای پیشگویی و پیشگیری حملات یا رخدادها علیه حوزه کاری خودشان، شهروندان یا زیرساخت‌ها، گزینه‌های محدودی را در اختیار دارند. در این حوزه، چالش‌های بسیار بنیادینی پدید می‌آید؛ ماهیت حمله‌های سایبری تاکنون چنان بوده است که در ساختارهای سنتی دیده یا گزارش نشده‌اند و

مسئله فهم و پاسخ به چالش‌ها را تبدیل به یکی از مسائل اساسی و بنیادی حاکمیت کرده است.

پیچیدگی و پویایی روزافزون چالش‌های امنیتی در برابر دولت، پیش از این در سطح کلی حاکمیتی و از راه استقرار کمیته ویژه دولتی برای بررسی موضوعات امنیت ملی موردتوجه قرار گرفته است. افزون بر این، حاکمیت پیش از این «مرکز ملی بررسی‌های امنیتی» را هم تأسیس کرده است که همه بخش‌های دولتی را شامل شده و تلاش دارد با رویکردی منسجم به ارزیابی، فهم و مقابله با چالش‌های امنیت ملی بپردازد، کاری که به شناخت راهبردی پیشرفته‌ای برای کل حاکمیت انجامیده است.

۳ - ۲- تهدیدهای ترکیبی

یکی از مسائل چالش‌برانگیز پدید آمده در سال‌های اخیر، استفاده از تهدیدهای چندرگه و پیچیده‌ای بوده است. اتحادیه اروپا این تهدیدها را به‌مثابه مجموعه اقدامات «چندوجهی، ترکیبی از کارهای خصمانه و خرابکارانه، با استفاده از ابزارها و فنون متعارف و غیرمتعارف (دیپلماتیک، نظامی، اقتصادی و فنی) برای ایجاد بی‌ثباتی در میدان مخالف» تعریف کرده است که در چند سال گذشته در تعدادی از اتحادیه اروپا رخ داده است. بسیاری از این تهدیدها عنصری سایبری داشته‌اند که متداول‌ترین آن‌ها استفاده از ابزارهای سایبری برای سرقت اطلاعات برای استفاده در کمپین‌های اطلاعات جعلی بوده است (که به‌عنوان «هک و نشت» شناخته می‌شود). این کمپین‌ها اهداف سیاسی دارند و چنان طراحی می‌شوند که به سادگی قابل شناسایی نیستند و حتی مسئولان رسمی هم نمی‌توانند برای مقابله با آن‌ها اقدام کنند.

ایرلند به‌عنوان کشوری با نظام دموکراسی گشوده، درست مثل دیگر کشورهای عضو اتحادیه اروپا، در معرض این نوع از تهدیدها قرار دارد. در دسامبر سال ۲۰۱۷، حاکمیت اولین «گروه میان‌بخشی امنیت فرایند انتخابات و اطلاعات جعلی» را با محوریت وزارت امور داخله برپا کرد.

این گروه با در نظر گرفتن موضوعات اساسی ناشی از تجربیات اخیر در سایر کشورهای دموکراتیک در خصوص استفاده از طرف‌های خارجی و ناشناس از رسانه‌های اجتماعی، ارزیابی مخاطرات روند انتخابات ایرلند را بر عهده دارد. این گروه اولین گزارش خود را در ژوئیه ۲۰۱۸ منتشر کرد که به‌طورکلی مبتنی بر این دریافت بود که به‌رغم مخاطرات به نسبت کمی که انتخابات در ایرلند با آن مواجه است، به دلیل گسترش اطلاعات جعلی در اینترنت و تهدید حملات سایبری به سامانه‌های انتخاباتی، احتمال می‌رود در آینده مخاطراتی در این عرصه ایجاد شود. این گروه مجموعه اقدامات مختلفی را برای محافظت در برابر این مخاطرات پیشنهاد داده است، از جمله، ایجاد کمیسیون انتخابات، نوسازی سامانه ثبت‌نام رأی‌دهندگان، قانون‌گذاری برای تبلیغات سیاسی اینترنتی و حمایت از تلاش‌های اتحادیه اروپا برای مقابله با اطلاعات جعلی. در سطح اروپا نیز کارهای قابل‌توجهی همچون ساخت «سلول ائتلاف ترکیبی»[1] در «اداره خدمات بیرونی اروپایی» انجام شده است، کاری که برای اشتراک فوری اطلاعات مرتبط با کنش‌های نوع ترکیبی اثرگذار بر کشورهای عضو اتحادیه اروپا طراحی شده است.

۳ - ۳- مخاطرات در برابر زیرساخت‌های حساس ملی و داده‌ها و سامانه‌های دولتی

پیامدهای ناخواسته تحولات در حوزه سایبری به مخاطرات عمومی

1. Hybrid Fusion Cell

در جامعه می‌انجامد اما برخی بخش‌ها هستند که می‌توانند پیامدهای شدیدتری را تجربه کنند. به بیانی کلی، این بخش‌ها همان زیرساخت‌هایی هستند که در عملکرد اجتماعی و اقتصادی نقش حساس و مهمی را بر عهده دارند و اغلب به نام «زیرساخت‌های حساس ملی» و «داده‌ها و سامانه‌های دولتی» شناسایی و معرفی می‌شوند.

مفهوم‌پردازی سنتی«زیرساخت‌های حساس ملی» شامل بخش‌های انرژی و حمل‌ونقل، بخش خدمات مالی، بهداشت و درمان و نیز سامانه‌های مخابراتی است. سامانه‌های فناوری اطلاعات حاکمیتی هم نقش محوری در بسیاری از عملکردها ضروری هستند و نقش مهمی در کارکرد جامعه مدرن دارند که شامل خدمات اجتماعی و سامانه‌های خدماتی، جمع‌آوری مالیات و کارکردهای دموکراسی هستند.

در دهه‌های اخیر، توسعه و استفاده از ابزارهایی برای نفوذ، اختلال و حتی تخریب این سامانه‌ها مشاهده شده است. این تهدیدها از طیف وسیعی از کنشگران برمی‌خیزد که از نظر منابع و توانایی‌ها تنوع زیادی دارند. این موارد طیف وسیعی را شامل می‌شوند و از افرادی که به‌تنهایی یا در گروه‌های کوچک در کار حملات و مزاحمت از نوع تخریب وب‌سایت‌ها و حمله‌های کوچک به درگاه‌های خدماتی تا «هکتیویست‌ها»، مجرمان بزرگتر مختلف و حتی دولت‌ها را در برمی‌گیرد. در میان تهدیدهای سطح بالاتر، باندهای تبهکار سازمان‌یافته اغلب از دولت‌ها قابل‌تشخیص نیستند؛ چرا که آن‌ها گاهی فنون و روش‌های بسیار پیشرفته‌ای را برای آلوده‌سازی و نفوذ به شبکه‌ها و داده‌ها به کار می‌گیرند.

دست‌آخر، در رأس این هرم، آن نهادهای موردحمایت دولت قرار دارند که بیشتر سازمان‌های نظامی یا امنیتی هستند و به دنبال آن هستند که از

سامانه‌های اطلاعاتی و شبکه‌ای برای انجام طیف گسترده‌ای از عملیات، از استخراج اطلاعات تا تخریب زیرساخت‌های فیزیکی بهره می‌گیرند. آشکار شده است که این عوامل تهدید که اغلب با عنوان «تهدیدهای پیوسته و پیشرفته» معرفی می‌شوند، در طیف وسیعی از بخش‌ها به کار گرفته شده‌اند و بیشتر بر شرکت‌های فناوری، شبکه‌های مخابراتی، خدمات مالی و سامانه‌های فناوری اطلاعات حکومتی تمرکز دارند. این واحدها با منابعی که در اختیار داشته، و نیز سماجت و تخصصی که دارند، چالش‌های بسیار خاصی را ایجاد می‌کنند؛ خیلی دشوار است که بتوان آن‌ها را شناسایی کرد، خیلی دشوار است که بتوان آن‌ها را رفع کرد و به همین خاطر چالش امنیتی مستمر و جدی برای شبکه‌ها و سامانه‌های اطلاعاتی ایجاد می‌کنند.

در طول تاریخ همه دولت‌ها دوست داشته‌اند زیرساخت‌های حساس ملی و نیز داده‌ها و سامانه‌های بخش عمومی را از راه ایمن‌سازی تعداد خیلی کمی از تأسیسات ایمن کنند. آن‌ها می‌توانستند قوانینی وضع کنند که طرف‌های مختلفی که به سرزمین آن‌ها دسترسی دارند را از استفاده در جهت اهداف یا فعالیت‌های غیرقانونی منع کنند، و می‌توانستند مرزهای فیزیکی مشخصی را برای دفاع در برابر تهدیدهای خارجی تعیین کنند. هیچ‌یک از این اقدامات در عصر دیجیتال کارآیی ندارد. افزون بر این، به دلایل عملی و قانونی، دولت‌ها حتی در قلمرو خودشان به طیف وسیعی از دستگاه‌ها و ترافیک ورودی و خروجی از این دستگاه‌ها دسترسی و اشراف اطلاعاتی ندارند یا نمی‌توانند امنیت آن‌ها را تضمین کنند. این بدان خاطر است که شبکه‌ها مالکیت شخصی دارند، درست به همان شکل که دستگاه‌های متصل به اینترنت و بخش عظیمی از زیرساخت‌های حساس ملی خصوصی هستند.

تا سال ۲۰۱۶ میلادی، رویکرد بسیاری از دولت‌های ملی، مبتنی بر پشتیبانی از سازمان‌ها از طریق ارائه اطلاعات در مورد تهدیدها، اقدام در جهت کاهش خطرات، و واکنش به حوادث بوده است. در ایرلند، امضای «قانون امنیت شبکه و اطلاعات ۲۰۱۸» منجر به رویکردی بسیار پیشگیرانه برای حفاظت از زیرساخت‌های حساس ملی شده است که از جمله شامل شناسایی رسمی اپراتورها و آغاز طرحی برای اجرای اقدامات امنیتی بوده که به ارزیابی و نظارت بر میزان انطباق با قوانین می‌پردازد و در راستای اقدامات انجام شده در سراسر اروپا قرار دارد. بااین‌وجود هم در بخش‌هایی که تحت مقررات امنیت اطلاعات و شبکه‌ها قرار دارند و هم خارج از این بخش‌ها، مخاطرات همچنان وجود دارند.

در وهله نخست، پایبندی به اقدامات امنیتی در مقررات امنیت اطلاعات و شبکه‌ها تضمین امنیت مطلق نیست و فقط یک روش برای کاهش خطر است. دوم آن‌که «شیوه‌نامه امنیت شبکه و اطلاعات ملی» آشکارا فقط به سه بخش محدود شده است. ارزیابی زیرساخت‌های حساس ملی که توسط «مرکز ملی امنیت سایبری» و در طی مراحل ثبت انجام می‌شود و نیز اجرای اقدامات امنیتی پس از ثبت، هر دو نشان داده است که برخی از زیرساخت‌های فعال دولت در خارج از حیطه امنیت اطلاعات و شبکه‌ها، هم درواقع حساس و حیاتی هستند و همچنین، برخی از بخش‌های زیرساخت‌های حساس ملی با هم وابستگی‌های متقابلی دارند که می‌توانند باعث مخاطرات خاصی شوند.

با آن‌که امنیت فناوری‌های اطلاعاتی و ارتباطی بخش دولتی، توجه و سرمایه‌های هنگفتی را دریافت کرده است، این مهم نه به دلیل وضع قانون عمومی حفاظت از داده‌ها، بلکه به خاطر ماهیت این بخش است

کـه چالش‌هـای خاصـی را ایجـاد کرده اسـت. برخی از سـازمان‌ها و دسـتگاه‌ها می‌تواننـد به‌خوبـی بـا روش‌های برتر جهانـی (و اسـتانداردهای جهانی همچون ایـزو ۲۷۰۰۱) انطبـاق دارنـد امـا بازهـم چالش همگرایـی با معیارهـای امنیتی سـازمان‌ها و دسـتگاه‌های دولتـی باقـی می‌ماند. در هر دو سـطح کلی و سـطح اطلاعـات طبقه‌بندی‌شـده ملی و نیز اطلاعات طبقه‌بندی‌شـده سـایر کشـورها و نهادهـای بین‌المللـی، مسـائل خاصی پیرامـون حاکمیت امنیـت فناوری‌های اطلاعاتـی و ارتباطـی باقی می‌ماند. در خصوص شـرکت‌هایی کـه برای مدیریت و ذخیـره اطلاعـات محرمانـه درخواسـت مجوز امنیتـی دارند، وضعیـت و موارد مشـابهی وجـود دارد. برخـی از اقدامـات بـرای پاسـخ بـه این چالش‌هـا طراحی و اجـرا شـده اسـت، از جملـه اسـتفاده روزافـزون (و برنامـه بـرای اسـتفاده) از زیرسـاخت‌های اشـتراکی فنـاوری اطلاعات میان دسـتگاه‌های مختلـف دولتی، امـا بازهـم بسـیاری از چالش‌های پیشـین همچنـان بر جای خود هسـتند.

نکتـه بسـیار مهم آن‌که پیشـرفت‌های پیوسـته در فنـاوری، از جمله انقلاب در ارتباطـات از راه دور، ممکـن اسـت این وضعیت را پیچیده‌تر کند. به‌کارگیری فناوری‌هـای نسـل پنجـم تلفـن همـراه کـه امـکان انتقال بـا تأخیر بسـیار کم و پهنـای بانـد بسـیار بـالا بـرای انتقـال اطلاعـات را فراهـم می‌کنـد، می‌توانـد زیرسـاخت‌های توانمندسـاز و مهمـی را بـرای مجموعـه دیگـری از فناوری‌هـا و کاربردهـا فراهـم آورد. خدمـات تشـخیص چهره مشـتری، خودروهـای بدون راننده و خدمات بهداشـت الکترونیک، سـرگرمی‌های جدیـد و خدمات معطوف بـه صنایـع می‌تواننـد از جمله این فناوری‌ها باشـند. بر این اسـاس، این احتمال وجـود دارد کـه شـبکه‌های نسـل پنجـم تلفن همـراه زیرسـاخت‌های مجموعه جدیـدی از خدمـات بـرای عملکردهای حسـاس و حیاتی اجتماعـی و اقتصادی فراهـم آورنـد. ماهیـت ایـن شـبکه‌ها و فناوری‌هـا هـم در اینجـا مهـم اسـت،

این‌که نرم‌افزار هستند و مجازی هستند بدین معناست که شاید انواع جدیدی از اقدامات امنیتی در این بخش مورد نیاز باشد تا امنیت شبکه نسل پنجم ارتباطات همراه و خدمات وابسته به آن را تأمین کند.

۳ - ۴- شهروندان و کسب‌وکارها

از نظر شهروندان در تمامی دوره‌های سنی، بسیاری از موضوعات مرتبط با امنیت سایبری، رابطه تنگاتنگی با ایمنی آنلاین و پیشگیری از جرائم اینترنتی دارند. این موارد بیشتر به رفتار افراد در فضاهای اینترنتی یا شیوه آن‌ها در نگهداری یا استفاده از وسایل شخصی یا خانگی اشاره دارد. این مخاطرات شامل از دست دادن احتمالی داده‌ها در اثر حملات رمزنگاری، یا از دست دادن یا سرقت اطلاعات شخصی از جمله اسناد هویتی و بانکی است. برای کسب‌وکارها، یکی از نتایج رایج و مخرب ناشی از افزایش فعالیت‌های مخرب آنلاین به‌صورت به کسب‌وکار، به‌منظور کسب سود مالی است. به‌رغم افزایش سطح آگاهی‌ها، حوادث جرائم سایبری در ایرلند در حال افزایش است؛ ۶۱٪ از سازمان‌های ایرلندی گزارش داده‌اند که در دو سال گذشته با صورت‌هایی از جرم‌های سایبری همچون کلاهبرداری مواجه بوده‌اند و تخمین زده می‌شود که به‌طور متوسط ۱/۳ میلیون یورو زیان دیده باشند.

بخش چهارم

بخش چهارم

توسعه ظرفیت های ملی

۴ - ۱- وضعیت میدان

تا سال ۲۰۱۱، مسئولیت دولت در حوزه امنیت سایبری در ایرلند در تعدادی از سازمان‌های مختلف نظامی و غیرنظامی پراکنده بود. در ژوئیه ۲۰۱۱، دولت تصمیم گرفت «مرکز ملی امنیت سایبری» را تأسیس کند؛ همین‌جایی که در حال حاظر وزارت ارتباطات، کنش‌های اقلیمی و محیط‌زیست است و تمامی موارد امنیت سایبری به یک واحد عملیاتی انتقال داده شد. این تصمیم مبتنی بر تجزیه‌وتحلیل دقیق تهدیدات در حال رشد در حوزه امنیت، ارزیابی بهترین نوع سازمان در جهت پاسخگویی به مسائل و نیز ارتقای فعال میزان تاب‌آوری خدمات و زیرساخت‌های اصلی بود. این مفهوم‌پردازی سازمانی از همان زمان به‌عنوان یکی از اقدامات برتر در کل اروپا شناسایی شد، امری که در درجه نخست به خاطر ایجاد یک مرکز ذخیره تجربه‌های حساس و تخصص‌های عملیاتی و نیز امکان مدیریت همه‌جانبه هر نوعی از حادثه بود.

اولین سند راهبردی امنیت ملی که در سال ۲۰۱۵ به تصویب دولت رسید، مجموعه‌ای از اقدامات را برای تأسیس و توانمندسازی «مرکز ملی امنیت سایبری» و دستیابی به سطح بالایی از امنیت برای شبکه‌های

رایانه‌ای و زیرساخت‌های حساس ملی در سطح دولت تعریف کرد. این اقدامات با تمرکز بر توسعه ظرفیت‌ها در «مرکز ملی امنیت سایبری» در «گروه پاسخگویی به حوادث امنیت رایانه» (CSIRT) و مجموعه‌ای از اقدامات همگرا با هدف ارتقای امنیت اطلاعات و شبکه ارگان‌های دولتی همراه بوده است. این سند راهبردی همچنین چگونگی ارتقای تاب‌آوری زیرساخت‌های حساس ملی بر اساس «شیوه‌نامه امنیت شبکه و اطلاعات ملی» را توصیف کرده و چگونگی توسعه ملی فرایند واکنش به حوادث از طریق مشارکت مستمر در «سامانه مدیریت اضطراری ملی» را تبیین می‌کند.

تمرکز اولیه «مرکز ملی امنیت سایبری» بر ایجاد «گروه واکنش به حوادث امنیتی رایانه‌ای» در سطح داخلی سازمان بود. «گروه‌های واکنش به حوادث امنیتی رایانه‌ای» نوعی سازمان است که در سطح بین‌المللی به‌رسمیت شناخته شده و وظیفه رسمی آن، واکنش به رخدادهای امنیت سایبری و اشتراک اطلاعات است. در پایه‌ای‌ترین سطح، این گروه‌ها طراحی شده‌اند تا به‌عنوان نقاط کانونی اطلاعات عمل کنند. این گروه‌ها از راه گردآوری و ناشناس‌سازی گزارش‌های حوادث از قربانیان و بعد به اشتراک‌گذاری جزئیات فنی حوادث و راهبردهای کاهش پیامدهای آن با اعضا (ارگان‌هایی که مأمور به کمک شده‌اند)، می‌توانند این تضمین را برای گروه‌های بزرگتر فراهم آورند که به آگاهی‌های موقعیتی دقیق‌تری پیرامون رخدادها دست خواهند یافت.

به‌این‌ترتیب، «گروه پاسخگویی به حوادث امنیت رایانه» آشکارا به‌منظور رفع برخی از چالش‌های ساختاری ناشی از مالکیت غیرمتمرکز سامانه‌های فناوری اطلاعات طراحی شده‌اند.

«گروه پاسخگویی به حوادث امنیت رایانه» در «مرکز ملی امنیت سایبری»، فرآیند طولانی ظرفیت‌سازی و ارتقای مهارت را پشت سر گذاشت. در مراحل اولیه، تمرکز بر وظایف اصلی توانایی مدیریت و رصد رخدادها و اشتراک اطلاعات با اعضا به‌صورت ایمن و حرفه‌ای بود. برای انجام این کار، نیاز به مجموعه‌ای از نیروهای آموزش دیده و باتجربه و نیز زیرساخت‌های مستقل و ایمن برای فناوری اطلاعات است. این موارد از سال ۲۰۱۵ به این‌سو توسعه قابل‌توجهی پیدا کرده و به ایجاد واحدی تخصصی با توانایی و ظرفیت قابل‌توجه در طیف گسترده‌ای از واکنش به حوادث امنیت سایبری انجامیده است. همکاری‌های نیروهای دفاعی و انتظامی نقش مهمی در مراحل نخستین این فرایند داشتند و نیروی اعزامی و تخصصی در زمینه امنیت، توسعه فرایندها و ارزیابی اطلاعاتی تهدید تدارک می‌دیدند. همچنین، مرکز تحقیقات جرائم اینترنتی دانشگاه دوبلین نقش مهمی در توسعه مهارت‌های امنیت سایبری بر عهده داشته است؛ بخش عمده‌ای از دانشی که باعث تشکیل «مرکز ملی امنیت سایبری» شد، حاصل فعالیت‌های انجام شده در دانشگاه دوبلین بوده است.

توسعه ظرفیت عملیاتی «گروه پاسخگویی به حوادث امنیت رایانه» چنان طراحی شده بود تا گروه را به آگاهی موقعیتی سطح بالایی نسبت به فعالیت‌های امنیت سایبری در دولت برساند و اعضایی داشته باشد که بتواند جزئیات فنی و اطلاعات با اطمینان خاطر و البته به‌صورت ناشناس با آن‌ها به اشتراک بگذارد و برای آن‌ها این فرصت را فراهم آورد که اقدامات لازم برای محافظت از دستگاه‌ها و خدمات خود را اتخاذ کنند. این اعضا شامل دستگاه‌ها و سازمانی‌های دولتی، اپراتورهای زیرساخت‌های حساس ملی و بیش از ۱۳۰ مرتبط هستند. به‌هرحال، «مرکز ملی امنیت

سایبری» در تعدادی از رخدادهای جدی امنیت سایبری در سال‌های ۲۰۱۶ و ۲۰۱۷ ورود پیدا کرد و در هر مورد با مسائلی مواجه شد که در سند راهبردی شناسایی نشده بودند. تجزیه‌وتحلیل این رخدادها، لزوم توسعه برخی از روش‌ها و ابزارهای «مرکز ملی امنیت سایبری» برای پاسخ بهتر به رخدادهای آینده را آشکار کرد. به‌این‌ترتیب، «مرکز ملی امنیت سایبری» طی این دوره اقداماتی را برای پشتیبانی از اپراتورهای مهم زیرساخت حساس ملی و نیز سهامداران حاکمیتی به انجام رسانید. از جمله مثال‌هایی که می‌توان به این موارد اشاره کرد: (الف) تأسیس و تقویت سامانه مشورتی و هشداری (که از آموزه‌های حاصل از فرایند مدیریت حادثه در دو حمله بدافزاری به نام‌های WannaCry2 و NotPetya سرچشمه می‌گیرد)، و (ب) تشکیل گروه اشتراک تهدیدها در سال ۲۰۱۷ که علاوه بر آن‌که به‌عنوان پایگاهی برای اپراتورهای زیرساخت حساس ملی عمل می‌کند، ابزاری در دست کنشگران دولتی (و از جمله نیروهای نظامی و انتظامی) هم هست تا بتوانند اطلاعات لازم را در اختیار این اپراتورها قرار داده و با افراد متخصص در زمینه امنیت سایبری در ارتباط باشند. همین رخدادها بودند که اهمیت امنیت سایبری به‌عنوان چالش‌های امنیتی اصلی پیش روی دولت و نیز نیاز به همکاری مداوم و نزدیک با سرویس‌های امنیتی دولتی در امور عملیاتی را تقویت کردند.

«مرکز ملی امنیت سایبری» از نظر ظرفیت و منابع توسعهٔ قابل‌توجهی یافته است و نقش‌های آن، از جمله مسئولیت‌های مربوط به حفاظت از زیرساخت‌های حساس ملی و همچنین رسیدگی به الزامات اتحادیه اروپا در مورد امنیت برخی از ارائه‌دهندگان خدمات دیجیتال، در قوانین رسمی مشخص شده است. مسئولیت‌های «گروه‌های پاسخگویی به حوادث

امنیتی رایانه» هم در رابطه با مخاطرات ریسک و رسیدگی به حوادث، در قالب الزام‌های زیر تعریف قانونی شده است:

(الف) نظارت بر رخدادهای داخلی دولت؛

(ب) ارائه اخطار، هشدار، اطلاعیه و انتشار به‌موقع اطلاعات مربوط به خطر و حوادث به ذی‌نفعان مربوطه؛

(ج) واکنش به رخدادهایی که توسط سامانه به حوادثی که تحت قوانین ۱۸ یا ۲۲ «شیوه‌نامه امنیت شبکه و اطلاعات ملی» ؛

(د) ارائه تحلیل پویا از مخاطرات، حوادث و اطلاعات نسبت به موقعیت‌ها؛

(ه) مشارکت و همکاری در شبکه «گروه پاسخگویی به حوادث امنیت رایانه»؛

(و) ایجاد روابط با افراد در بخش خصوصی برای تسهیل همکاری با آن بخش.

«گروه پاسخگویی به حوادث امنیت رایانه» اولین اعتبارنامه بین‌المللی خود را در اواخر سال ۲۰۱۷ دریافت کرد (سطح اعتبار معرف معتمد) که نشان می‌دهد این گروه به سطح برتری از عملکرد و بلوغ رسیده است. «مرکز ملی امنیت سایبری» پایگاهی از داده اطلاعات مربوط به تهدیدات را ایجاد کرده است که برای کمک به دستگاه‌ها و سازمان‌ها، در جهت محافظت از شبکه‌های اطلاعاتی مورد استفاده قرار می‌گیرد. همچنین پایگاه سازنده «مرکز ملی امنیت سایبری» به بیش از ۱۳۰ عضو گسترش یافته است. این پایگاه اکنون شامل دستگاه‌ها و نمایندگی‌های دولتی و نهادهای اصلی در بخش مالی، تأمین‌کنندگان زیرساخت‌های حساس ملی و سایر اپراتورهای خدمات ضروری می‌شود.

از آن دوره، «گروه پاسخگویی به حوادث امنیت رایانه» ظرفیت پاسخگویی به حوادث خود را با استفاده از سامانه پاسخگویی یکپارچه و تحلیلی، و نیز سامانه شبیه‌سازی و پیشرفته مشاوره برای اعضا در زیرساخت‌های دولتی و بحرانی ملی بیشتر توسعه داده است. افزون بر این، «گروه پاسخگویی به حوادث امنیتی رایانه» از موضعی واکنشی به موضعی فعال‌تر تغییر راهبرد داده است. این شامل کار استقرار و استفاده از سکوهای اشتراک اطلاعات بدافزارها برای اشتراک مستقیم اطلاعات مرتبط با تهدیدها در میان تأمین‌کنندگان زیرساخت‌های ملی مهم و توسعه و استفاده از مجموعه‌ای از ابزارها برای شناسایی، تجزیه و تحلیل اطلاعات منبع باز است. همچنین «گروه پاسخگویی به حوادث امنیت رایانه» برای شناسایی و هشدار نسبت به انواع خاصی از تهدیدها، سکوی «حسگر» (سنسور) را طراحی و نصب کرده است، سکویی که اکنون در زیرساخت تعدادی از دستگاه‌های دولتی در حال فعالیت است.

رشد و توسعه «مرکز ملی امنیت سایبری» با تحولاتی در حوزه‌های مرتبط همراه بوده است. گزارش راهبرد دفاعی سال ۲۰۱۵ بیان می‌دارد که «وزارت ارتباطات، انرژی و منابع طبیعی مسئولیت اصلی امور مربوط به امنیت سایبری را بر عهده دارد» و در توضیح ادامه می‌دهد که «تمرکز اصلی وزارت دفاع و نیروهای دفاعی، حفظ شبکه‌های دفاع خواهد بود» و درعین‌حال «همچون همه شرایط اضطراری یا بحرانی، اگر از سامانه‌های دفاعی پشتیبانی شود، وزارت دفاع و نیروهای دفاعی از «گروه پاسخگویی به حوادث امنیتی رایانه» در حد منابع و امکان و منابع پشتیبانی خواهد کرد.» به‌این‌ترتیب، نیروهای دفاعی در خصوص امنیت سایبری، به‌صراحت و آشکارا نقشی پشتیبان است و مسئولیت اصلی آن‌ها در این حوزه،

حفاظت از سامانه‌های خودشان است. این نقش پشتیبان در طول زمان توسعه پیدا کرده است و نیروهای دفاعی همچنان نقش اصلی را در تسهیل عملیات «مرکز ملی امنیت سایبری» بر عهده دارند. «مرکز ملی امنیت سایبری» همکاری‌های نزدیکی با نیروهای نظامی و انتظامی در زمینه مسائل امنیت ملی دارند و با هر دو نهاد توافق‌نامهٔ اعزام نیرو دارد.

نیروی انتظامی و پلیس هم در این بخش، در پیشگیری، تحقیق و پیگرد قانونی جرائم اینترنتی و نیز در سطح امنیت ملی، مجموعه‌ای از مسئولیت‌ها را بر عهده دارد. ظرفیت و ساختار سازمانی نیروهای انتظامی در سال‌های اخیر تحول زیادی پیدا کرده است؛ واحد پیگیری جرائم رایانه‌ای (تأسیس در سال ۱۹۹۱) در قالب «اداره ملی جرائم سایبری پلیس» (GNCCB) در سال ۲۰۱۷ بازتأسیس شد. دفتر این واحد ملی وظیفه انجام آزمایش‌های پزشکی قانونی رسانه‌های رایانه‌ای را در جریان هر تحقیقات جنایی بر عهده دارد. به‌علاوه این اداره، تحقیقات لازم در زمینه جرائم سایبری از جمله نفوذ به شبکه، تداخل داده‌ها و حمله به وب‌سایت‌های دستگاه‌های دولتی و سازمان‌ها و مؤسسات را انجام می‌دهد، سازمان پلیس ایرلند در این حوزه سرمایه‌گذاری هنگفتی کرده و بیشترین تمرکز را بر توسعه ظرفیت‌های در مناطق حاشیه‌ای داشته است. «مرکز ملی امنیت سایبری» و «اداره ملی جرائم سایبری گاردا» از طریق همکاری‌ها مشترک و مستمر و ایجاد فرصت‌های تبادل نیروهای متخصص، به چارچوب‌های ایجابی برای همکاری دوجانبه رسیده‌اند.

مهم‌ترین پیشرفت‌ها

۱) «گروه پاسخگویی به حوادث امنیت رایانه» ساختاری عملیاتی پیدا

کرده و از اعتبار بین‌المللی برخوردار شده است.

۲) برنامه‌های خبررسانی و اشتراک اطلاعات که توسط «مرکز امنیت امنیتی سایبری» اجرا می‌شود، به‌خصوص پس از استقرار «سامانه‌های اشتراک اطلاعات بدافزارها» (MISPs) توسعه چشمگیری یافته است.

۳) سامانه «حسگر» یکی از مهم‌ترین برنامه‌هایی است که توسط «گروه پاسخگویی به حوادث امنیت رایانه» آن توسعه، آزمایش و استقرار یافته است.

۴) اداره ملی جرائم سایبری گاردا تأسیس شده و ظرفیت این سازمان توسعه قابل‌توجهی یافته است.

۵) مرکز ارزیابی امنیت ملی در وزارت امور داخله ایجاد شده است.

۴ - ۲- اهداف

به منظور ادامه ارتقای توانایی های دولت در واکنش به حوادث امنیت سایبری و مدیریت آن ها، از جمله مواردی که حوادث امنیت سایبری و مولفه های امنیت ملی دارد.

۴ - ۳- اقدامات

«مرکز ملی امنیت سایبری» به‌عنوان مرجع اصلی امنیت سایبری در دولت خواهد بود و ظرفیت‌های خود را در دو نقش اصلی همچنان بیشتر توسعه خواهد داد؛ راهبری واکنش‌های ملی به حوادث امنیت سایبری و توسعه تاب‌آوری شبکه‌ها و دستگاه‌های اصلی در سراسر بدنه دولت. محور اصلی واکنش «مرکز ملی امنیت سایبری» همچنان توسعه خواهد یافت و مبنای آن از واکنش‌گرایی ساده به‌سوی پاسخ‌های فعال حرکت خواهد

کرد و در این راه از روش‌های جدید تشخیص تهدیدها پیش از اثرگذاری بر خدمات و شهروندان استفاده خواهد کرد. همچنین تا پایان سال ۲۰۲۲، «مرکز ملی امنیت سایبری» چند نقش جدید و مهم در محافظت از شبکه‌ها و داده‌های دولت بر عهده خواهد داشت و به همکاری با دفتر مدیر اخبار و اطلاعات دولت در جهت توسعه و اجرای سیاست‌ها و شیوه‌های مربوط به خدمات حاکمیتی و عمومی ادامه خواهد داد.

۱) «مرکز ملی امنیت سایبری»، به‌خصوص در رابطه با توانایی نظارت و واکنش به حوادث امنیت سایبری و تهدیدهای درحال‌توسعه در دولت، توسعه بیشتری خواهد یافت.

«گروه پاسخگویی به حوادث امنیت رایانه» در «مرکز ملی امنیت سایبری» تا پایان سال ۲۰۲۰ به «مرکز عملیات مشترک امنیتی» (یا JSOC) تبدیل خواهد شد تا بهتر بتواند امنیت فناوری‌های اطلاعاتی و ارتباطی دولت و نیز زیرساخت‌های حساس ملی را تأمین کند. گروه‌های تخصصی دیگری هم در «مرکز عملیات مشترک امنیتی» تأسیس خواهند شد که از جمله می‌توان به گروه اطلاعات تهدید، واکنش به رویداد و نظارت بر شبکه اشاره کرد. این امر هم توسعه پیوسته گروه واکنش را تسهیل خواهد کرد و هم شرایط لازم برای حفاظت و پیشرفت تدریجی«مرکز ملی امنیت سایبری» در جهت نظارت بر فعالیت شبکه در تمامی زیرساخت‌های حساس ملی و دولتی را فراهم خواهد آورد. این واحد به‌عنوان پایگاه مشترک ملی برای همه حوادث امنیت سایبری به کار خود ادامه خواهد داد و همچنان به حوادث امنیت سایبری در هر اندازه و مقیاسی خواهد پرداخت.

۲) اطلاعات و تحلیل‌های مربوط به تهدیدهای تهیه شده توسط «مرکز ملی امنیت سایبری»، با کارهای «مرکز ملی بررسی‌های امنیتی» ادغام خواهد شد.

مرکز ملی بررسی‌های امنیتی که در وزارت امور داخله مستقر است، نقش مهمی در این هماهنگی تحلیل‌های راهبردی از تهدیدهای امنیت ملی و در ارائه آگاهی‌های موقعیتی ارتقا یافته به حاکمیت خواهد داشت. «مرکز ملی امنیت سایبری» به کسب این اطمینان کمک می‌کند که چالش‌های جدید و نوظهور امنیت سایبری که آثار فراگیری بر امنیت ملی دارند، در کارهای مرکز ملی بررسی‌های امنیتی و از جمله در تدوین استراتژی جدید امنیت ملی نمایان می‌شوند.

اقدام ۱ – «مرکز ملی امنیت سایبری»، به‌خصوص با توجه به گسترش توانایی نظارت و پاسخگویی به حوادث امنیتی سایبری و تهدیدهای فزاینده در برابر دولت، توسعه بیشتری خواهد یافت.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	تهیه برنامه دقیق فنی و سازمانی برای «مرکز عملیات مشترک امنیتی»	فصل چهارم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	وزارت محیط‌زیست، آب‌وهوا و ارتباطات
۲	دریافت ضمانت قانونی برای توسعه «مرکز ملی امنیت سایبری»	فصل دوم سال ۲۰۲۱	«مرکز ملی امنیت سایبری»	وزارت محیط‌زیست، آب‌وهوا و ارتباط، وزارت هزینه‌های عمومی و اصلاح
۳	ساخت نمونه اولیه مرکز عملیات مشترک امنیتی با استفاده از امکانات موقت	فصل چهارم سال ۲۰۲۱	«مرکز ملی امنیت سایبری»	اداره امور عمومی، وزارت محیط‌زیست، آب‌وهوا و ارتباطات
۴	کمیسیون نهایی تسهیلات مرکز عملیات مشترک امنیتی در پایگاه اصلی «مرکز ملی امنیت سایبری»	فصل دوم سال ۲۰۲۳	«مرکز ملی امنیت سایبری»	اداره امور عمومی، وزارت محیط‌زیست، آب‌وهوا و ارتباطات

اقدام ۲ – اطلاعات و تحلیل‌های تهیه شده پیرامون تهدید توسط «مرکز ملی امنیت سایبری» در کارهای مرکز بررسی‌های امنیت ملی ادغام خواهد شد.				
	اقدامات برای ارائه	**جدول زمانی فصلی**	**راهبری**	**همکاران اصلی**
۱	ایجاد زیرساخت‌های گزارش‌دهی و اشتراک اطلاعات مرکز ملی بررسی‌های امنیتی	فصل اول ۲۰۲۰	«مرکز ملی امنیت سایبری»	مرکز ملی بررسی‌های امنیتی

بخش پنجم

بخش پنجم

حفاظت از زیرساخت های حساس ملی

۵ - ۱- وضعیت میدان

تا همین اواخر، روش‌های برتر پذیرفته‌شده در اروپا در جهت حفاظت از خدمات و زیرساخت‌های حساس ملی در برابر نوع حمله سایبری شامل دو نوع از کنش است: ۱) ایجاد یک بدنه واکنش به رخداد همچون مرکز ملی بررسی‌های امنیتی و ۲) نهادینه‌سازی واحدهای رسمی اشتراک اطلاعات که بتواند اطلاعات مربوط به تهدیدهای خاص و از جمله اطلاعات ضروری درباره تهدیدهای فوری را در میان مالکان و اپراتورها به اشتراک گذارد. در مرکز ملی امنیت سایبری» ارائه همین خدمات را راه‌اندازی کرده و با کمک اپراتورهای خدماتی و سایر دستگاه‌ها در دیگر حوزه‌های قضایی، در جهت مدیریت مخاطرات موجود در برابر زیرساخت‌های حساس ملی در ایرلند و نیز مدیریت فعال رخدادهای جاری، همچنان به‌صورت مستمر پیگیری می‌کند.

باوجوداین، تجربه‌های تاریخی در اروپا و دیگر کشورها آشکار کرده است که میان مخاطرات منافع عمومی و مخاطرات بسیاری از اپراتورهای این‌گونه زیرساخت‌ها، تقارنی وجود ندارد. علی‌رغم تلاش‌های گسترده حاکمیت برای ارائه اطلاعات و پشتیبانی از اپراتورها در بسیاری از موارد،

خدمات حساس و ضروری آسیب‌پذیری زیادی دارند. ازاین‌رو و با ادامه کار در برخی از کشورهای عضو اتحادیه اروپا و بر اساس شیوه‌نامه‌های پیشین برای مخابرات، کمیسیون اروپا پیش‌نویس «دستورالعمل امنیت شبکه و اطلاعات» را در سال ۲۰۱۳ منتشر کرد. این «شیوه‌نامه امنیت شبکه و اطلاعات ملی» که در سال ۲۰۱۶ مورد تأیید رسمی قرار گرفت، شامل مجموعه‌ای از اقدامات در جهت ارتقای تاب‌آوری زیرساخت‌های حساس ملی در ۷ بخش مختلف بود (شامل انرژی، حمل‌ونقل، آب آشامیدنی، بازارهای مالی، مراقبت‌های بهداشتی و زیرساخت‌های دیجیتال). این اقدامات شامل الزام کشورهای عضو برای بازبینی و ارزیابی رسمی زیرساخت‌های خود و تعیین قانونی «اپراتورهای خدمات ضروری» است - آن دسته از دستگاه‌هایی که برای ارائه این خدمات در هر کشور ضروری و حیاتی هستند. علاوه بر این، این دستگاه‌ها باید تحت مجموعه‌ای از الزامات امنیتی رسمی، ملزم به ارائه گزارش رخدادها باشند. به‌این‌ترتیب، «شیوه‌نامه امنیت شبکه و اطلاعات ملی» با هدف (الف) الزام ارتقای زیرساخت‌های حساس ملی در امنیت و تاب‌آوری، و (ب) ارتقای آگاهی دولت از رخدادهای امنیت سایبری در سراسر اروپا، و (ج) ایجاد سازگاری بیشتر و هماهنگی برای واکنش به رخدادها در سطح اتحادیه اروپا.

سند راهبردی ۲۰۱۵ در استقبال از «شیوه‌نامه امنیت شبکه و اطلاعات ملی» نگاشته شد و پیش از آن‌که سند راهبردی کامل شود، کارهای دقیقی برای ارزیابی «زیرساخت‌های حساس ملی» در ایرلند کامل شده بود که شامل مطالعه وابستگی زیرساخت‌ها با انگلیس بود (کاری که اواسط سال ۲۰۱۷ کامل شد). سپس از این ارزیابی‌ها برای تهیه فهرست ملی «اپراتورهای خدمات ضروری» به کار گرفته شد، که پس از ابلاغ

رسمی «شیوه‌نامه امنیت شبکه و اطلاعات ملی» ایرلند در سپتامبر ۲۰۱۸ اجرایی شد. اختیارات اجرایی تحت مقررات امنیت شبکه و اطلاعات ملی به مدیران ذی‌ربط «مرکز ملی امنیت سایبری» این اختیار را داد تا ارزیابی‌ها و ممیزی‌های امنیتی را در ۵ بخش از ۷ بخش انجام داده (بانک مرکزی ایرلند مسئولیت اعمال تدابیر امنیتی در بخش‌های خدمات مالی را حفظ می‌کند)، و ملزم به تهیه اطلاعات و صدور شیوه‌نامه‌های الزام‌آور برای رفع کاستی‌های احتمالی می‌کند. «مرکز ملی امنیت سایبری» همچنین اسناد راهنمای جزئیات مربوط به اقدامات امنیتی، انطباق و گزارش حادثه را برای پشتیبانی بیشتر از اپراتورهای خدمات ضروری تهیه کرده است که در ژانویه ۲۰۱۹ در جهت اخذ مشاوره‌های عمومی انتشار یافت.

برای اهداف این سند، زیرساخت‌های حساس ملی چنین تعریف شده است: «... هر دارایی، سامانه یا بخشی از آن‌که در کشورهای عضو قرار دارد، برای حفظ عملکردهای حیاتی جامعه، بهداشت، ایمنی، امنیت، رفاه اقتصادی یا اجتماعی مردم ضروری است، و اختلال یا تخریب آن در یک کشور عضو، بر این عملکردها تأثیر قابل‌توجهی خواهد داشت.» هدف حاکمیت، صیانت از زیرساخت‌های حساس ملی است و این کار را از راه الزام اپراتورها به توجه به مدیریت مخاطرات این زیرساخت‌ها، و از جمله از طریق الزام به داشتن برنامه‌های مناسب برای مقابله با حوادث و هرگونه اختلال در خدمات انجام می‌دهد.

وابستگی تدریجی خدمات و زیرساخت‌های حساس ملی به ابزارها و دستگاه‌های متصل به شبکه باعث شده است که دولت برای اطمینان از انعطاف‌پذیری مجموعه‌های خاصی از زیرساخت‌های حساس ملی، اقداماتی را انجام دهد. باوجوداین، با توجه به ماهیت و میزان خطر و نیز

بـه دلیـل توسـعه فن‌آوری‌هـا، خود همین سـامانه نیاز به توسـعه و گسـترش بیشـتری دارد. بـرای ایـن منظور، دولـت اقدامات زیر را برای محافظت بیشـتر از زیرسـاخت‌ها و خدمـات مهـم ملی انجـام خواهد داد.

مهم‌ترین پیشرفت

۱) روش حفاظـت از زیرسـاخت‌های حسـاس کـه در «شـیوه‌نامه امنیـت شـبکه و اطلاعات ملی» اتحادیه اروپا مشـخص شـده بود، به اجرا گذاشـته شـده است.

۲) ایـن امـر منجـر بـه تعییـن اپراتورهـای خدمـات ضـروری در ۷ بخـش اصلـی و شـروع مجموعـه‌ای از ارزیابی‌هـای رسـمی برای سـنجش آمادگی توسـط اپراتورها شـده اسـت.

۳) معرفـی سـازوکارهای اشـتراک اطلاعـات اختصاصی در زمینه اشـتراک اطلاعات حسـاس بـا اپراتورهـای اصلی.

۵ - ۲ - اهداف

به‌منظـور شناسـایی و نیـز حفاظـت از زیرسـاخت‌های حسـاس ملـی از طریـق افزایـش تاب‌آوری آن‌هـا در برابر حملات سـایبری و اطمینان از این‌که اپراتورهـای خدمـات ضـروری برنامه‌های مناسـبی بـرای مقابله با حـوادث در جهـت مدیریـت و کاهـش هرگونه اختـلال در خدمـات دارند.

۵ - ۳ - اقدامات

«مرکـز ملـی امنیـت سـایبری» همچنیـن بـه اجـرای برنامـه محافظت از زیرسـاخت حسـاس ملـی خـود ادامـه خواهـد داد که بر اسـاس دسـتورالعمل

«امنیت شبکه و اطلاعات ملی» تاکنون اجرا شده است و درعین‌حال، بر اساس مطالعات و تحلیل‌های در دست اجرا، به توسعه گسترده این برنامه خواهد پرداخت. این کار مورد پشتیبانی ویژه نیروهای نظامی و انتظامی قرار خواهد گرفت و همه اجزای حاکمیتی را در جهت اطمینان از یکپارچه‌سازی امنیت سایبری در تمامی موضوعات و سیاست‌های مرتبط به مشارکت فرا خواهد خواند.

۳) سامانه کنونی حفاظت از زیرساخت‌های حساس ملی که بر اساس شیوه‌نامه امنیت شبکه و اطلاعات ملی راه‌اندازی شده است، با تمرکز ویژه بر برنامه‌های همگرایی و ممیزی مستمر در جهت کاهش خطرات خدمات اصلی، همچنان به کار گرفته شده و توسعه می‌یابد.

هدف اصلی شیوه‌نامه امنیت شبکه و اطلاعات ملی اطمینان از وجود سطح یکسان و بالایی از امنیت سایبری در کشورهای عضو است. «مرکز ملی امنیت سایبری» مرجع معتبر در سطح ملی است که متعهد به ارائه راهنمایی در مورد امنیت زیرساخت‌های حساس ملی و نظارت بر کاربرد کنترل‌های امنیتی در بسیاری از این بخش‌ها است. «مرکز ملی امنیت سایبری» به‌منظور اطمینان از اجرای کامل شیوه‌نامه امنیت شبکه و اطلاعات ملی در ایرلند و همچنین همگرایی آن با تغییرات در فناوری‌ها و پیروی از الگوهای برتر، به توسعه و اجرای این اقدامات ادامه خواهد داد.

۴) «مرکز ملی امنیت سایبری» با همکاری نیروهای نظامی و انتظامی، یک ارزیابی دقیق و به‌روز از آسیب‌پذیری‌های ممکن در همه خدمات و زیرساخت‌های حساس در برابر حملات سایبری انجام خواهد داد.

«مرکز ملی امنیت سایبری» با اتکای به ارزیابی‌های موجود انجام شده تحت شیوه‌نامه امنیت شبکه و اطلاعات ملی، ارزیابی دقیقی از

مخاطرات و آسیب‌پذیری‌های خدمات و زیرساخت‌های حساس ملی در برابر حمله سایبری را انجام می‌دهد. این فرایند شامل ارزیابی حساسیت طیف گسترده‌ای از خدمات و تهیه نمودارهایی از وابستگی‌های متقابل بین این خدمات است. نتیجه حاصل از این فرایند، اخبار و اطلاعات تازه را وارد روند حفاظت و امنیت سایبری زیرساخت‌های حساس ملی موجود می‌کند.

۵) سامانه پشتیبانی از زیرساخت‌های حساس ملی در طول اجرای سند راهبردی، گسترش و تعمیق خواهد یافت تا دامنه وسیع‌تری از زیرساخت‌های حساس ملی و ازجمله ابعادی از سامانه‌های انتخاباتی را شامل شود.

سیستم نظارتی موجود برای امنیت سایبری زیرساخت‌های حساس ملی، گسترش و تعمیق خواهند یافت تا طیف وسیعی از اپراتورها را در مجموعه وسیع‌تری از بخش‌ها شامل شود و امکان نظارت دقیق بر همگرایی را ایجاد کند. این سامانه توسعه یافته می‌تواند جنبه‌هایی از آموزش عالی و نیز سامانه‌های انتخاباتی را در برگیرد و همان اموری را پیگیری خواهد کرد که بر اساس «شیوه‌نامه امنیت شبکه و اطلاعات ملی» در حال اجرا است.

۶) گروه‌های اشتراک اطلاعات فعلی که توسط «مرکز ملی امنیت سایبری» اداره می‌شوند، توسعه بیشتری خواهند یافت و گروه‌های اشتراک تهدید فعلی چنان توسعه خواهند یافت تا طیف وسیع‌تری از زیرساخت‌های حساس ملی را شامل شوند.

مجامع اشتراک اطلاعات امنیت سایبری موجود، همچون «گروه اشتراک اطلاعات تهدیدها» (TSG) و «مرکز تبادل اطلاعات سراسر جزیره» (AIIE)

توسعه بنیادین خواهند یافت.

۷) حاکمیت مجموعه جدیدی از استانداردهای همگرایی را معرفی خواهد کرد تا امنیت سایبری زیرساخت‌های مخابراتی کشور را پشتیبانی کند.

مجموعه ویژه و تازه‌ای از الزامات امنیتی برای بخش ارتباطات از راه دور را معرفی خواهیم کرد که همراه با اقدامات دقیق کاهش خطرات خواهد بود و «مرکز ملی امنیت سایبری» به کار گرفته خواهد تا به نظام رگلاتوری ارتباطات در انجام وظایف قانونی خود، تحت مقررات امنیتی موجود در اتحادیه اروپا و نیز برنامه آتی مخابرات اتحادیه اروپا (بخشنامه ۱۹۷۲/۲۰۱۸) کمک کند.

اقدام ۳ – سامانه کنونی حفاظت از زیرساخت‌های حساس ملی که بر اساس شیوه‌نامه امنیت شبکه و اطلاعات ملی راه‌اندازی شده است، با تمرکز ویژه بر برنامه‌های همگرایی و ممیزی مستمر در جهت کاهش خطرات خدمات اصلی، همچنان به کار گرفته شده و توسعه می‌یابد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	تکمیل مرحله اول خودارزیابی اپراتورهای خدمات ضروری (OES) بر اساس چارچوب کنترل امنیت	فصل اول سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	اپراتور خدمات ضروری تعیین‌شده
۲	آغاز آزمایش کنترل امنیت اپراتورهای خدمات ضروری	فصل سوم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	اپراتور خدمات ضروری تعیین‌شده
۳	بازبینی ثبت اپراتورهای خدمات ضروری و دستورالعمل‌های امنیتی	فصل سوم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	اپراتور خدمات ضروری تعیین‌شده
۴	کنترل امنیت پس از حوادث و بررسی‌های مستمر همگرایی اپراتورهای خدمات ضروری	در حال اجرا	«مرکز ملی امنیت سایبری»	اپراتور خدمات ضروری تعیین‌شده

اقدام ۴ – «مرکز ملی امنیت سایبری» با همکاری نیروهای نظامی و انتظامی، یک ارزیابی دقیق و به‌روز از آسیب‌پذیری‌های ممکن در همه خدمات و زیرساخت‌های حساس در برابر حملات سایبری انجام خواهد داد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	گروه راهبری تشکیل‌شده و اصول مرجع برای بررسی مورد توافق قرار گیرد	فصل اول سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی، بانک مرکزی ایرلند، کمیسیون تنظیم مقررات ارتباطات، کمیسیون مقررات صنایع عمومی، سازمان هواپیمایی
۲	تکمیل مرحله جمع‌آوری اطلاعات و توافق پیرامون روش اجرایی	فصل سوم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی، بانک مرکزی ایرلند، کمیسیون تنظیم مقررات ارتباطات، کمیسیون مقررات صنایع عمومی، سازمان هواپیمایی
۳	فرایند ارزیابی کامل شامل مشاوره بین‌المللی و ارزیابی دقیق روابط متقابل میان‌بخشی.	فصل دوم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی، بانک مرکزی ایرلند، کمیسیون تنظیم مقررات ارتباطات، کمیسیون مقررات صنایع عمومی، سازمان هواپیمایی
۴	تکمیل گزارش نهایی و توصیه‌ها	فصل چهارم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی، بانک مرکزی ایرلند، کمیسیون تنظیم مقررات ارتباطات، کمیسیون مقررات صنایع عمومی، سازمان هواپیمایی

اقدام ۵ – سامانه پشتیبانی از زیرساخت‌های حساس ملی در طول اجرای سند راهبردی به‌گونه‌ای گسترش و تعمیق خواهد یافت تا دامنه وسیع‌تری از زیرساخت‌های حساس ملی و ازجمله ابعادی از سامانه‌های انتخاباتی را شامل شود.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	پیش‌نویس رئوس لایحه برای موافقت دولت	فصل چهارم سال ۲۰۲۱	وزارت محیط‌زیست، آب‌وهوا و ارتباطات	دفتر دادستان کل کشور
۲	تهیه پیش‌نویس با دفتر دادستان کل کشور	فصل اول سال ۲۰۲۲	وزارت محیط‌زیست، آب‌وهوا و ارتباطات	دفتر دادستان کل کشور
۳	فرایند قانون‌گذاری	فصل دوم سال ۲۰۲۲	وزارت محیط‌زیست، آب‌وهوا و ارتباطات	دفتر دادستان کل کشور، قوه مقننه

اقدام ۶ – گروه‌های اشتراک اطلاعات فعلی که توسط «مرکز ملی امنیت سایبری» اداره می‌شوند، توسعه بیشتری خواهند یافت و گروه‌های اشتراک تهدید فعلی چنان توسعه خواهند یافت تا طیف وسیع‌تری از زیرساخت‌های حساس ملی را شامل شوند.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	گسترش نمایندگان فعلی گروه اشتراک تهدید تا حد گنجاندن زیرساخت‌های حساس ملی و تدوین اصول مرجع جدید	فصل دوم سال ۲۰۲۰	مرکز ملی امنیت سایبری	نیروی پلیس، نیروی دفاعی، زیرساخت‌های حساس ملی
۲	اصلاح توافق‌های موجود با انگلیس در مورد به‌اشتراک‌گذاری اطلاعات و واکنش به حوادث، با ارجاع خاص به حفاظت از زیرساخت‌های حساس حیاتی شمال - جنوب	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر برنامه‌ریزی اضطراری، مرکز پشتیبانی از زیرساخت‌های ملی، انگلیس

اقدام ۷ – حاکمیت مجموعه جدیدی از استانداردهای همگرایی را معرفی خواهد کرد تا امنیت سایبری زیرساخت‌های مخابراتی کشور را پشتیبانی کند.				
	اقدامات برای ارائه	**جدول زمانی فصلی**	**راهبری**	**همکاران اصلی**
۱	تصویب اقدامات اجرایی برای بخش‌نامه ۱۹۷۲/۲۰۱۸	فصل چهارم سال ۲۰۲۰	وزارت محیط‌زیست، آب‌وهوا، و ارتباطات	مرکز ملی امنیت سایبری، کمیسیون تنظیم مقررات ارتباطات
۲	ارائه پشتیبانی فنی به کمیسیون تنظیم مقررات ارتباطات	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	کمیسیون تنظیم مقررات ارتباطات
۳	اجرای اقدامات امنیتی بازبینی‌شده	فصل اول سال ۲۰۲۱	کمیسیون تنظیم مقررات ارتباطات	وزارت محیط‌زیست، آب‌وهوا، و ارتباطات،

بخش ششم

بخش ششم

داده‌ها و شبکه‌های بخش دولتی

۶ - ۱- وضعیت میدان

مسئولیت عملکرد و امنیت سامانه‌های فناوری اطلاعات بخش عمومی با همان دستگاه‌ها و ادارات است و در این میان دفتر مدیر ارشد اطلاعات دولت نقش اساسی در رهبری اجرای استراتژی فناوری‌های اطلاعاتی و ارتباطی بخش عمومی و مدیریت شبکه‌ای دارد که دستگاه‌ها و ادارات از آن در جهت برقراری ارتباط با یکدیگر و با فضاهای وسیع‌تر اینترنت استفاده می‌کنند. نقش اصلی «گروه پاسخگویی به حوادث امنیت رایانه» در «مرکز ملی امنیت سایبری» در سال‌های اولیه، واکنش به حوادث در جهت پشتیبانی از این بخش‌ها و سازمان‌ها هنگام گزارش حوادث به «مرکز ملی امنیت سایبری» بود و نیز می‌خواستند که سامانه مشورتی بسازند تا امکان انتشار سریع اطلاعات خاص مربوط به تهدیدها و رخدادها را فراهم آورند و بهترین روش‌ها در مواجهه با رخدادهای امنیت سایبری را به اشتراک بگذارند. البته «مرکز ملی امنیت سایبری» هیچ نظارت مستقیمی بر فعالیت‌های شبکه‌های دولتی ندارد و به همین خاطر هیچ طرح دقیقی برای تعیین اقدامات امنیتی در دستگاه‌ها و سازمان‌های مختلف ندارد. بر این اساس و هم‌زمان با توسعه پیوسته «گروه پاسخگویی

بـه حـوادث امنیت رایانه» و مجموعـه ابزارهایی که در دسـترس همه بخش‌ها قـرار دارد، «مرکـز ملـی امنیت سـایبری» پـروژه‌ای با عنوان حسـگر را معرفی کـرد؛ حسـگر لایه دیگـری از حفاظت مـرزی برای دسـتگاه‌های دولتی اسـت کـه هنـگام مشـاهده هـر نـوع از نقـض حریـم شـبکه‌های دولتـی، بـه «مرکز ملـی امنیـت سـایبری» هشـدارهای لازم را ارائـه می‌دهـد. همچنیـن، «مرکز ملـی امنیت سـایبری» در اواخر سـال ۲۰۱۸ سـند «۵ نکتـه در راهنمایی» را برای اسـتفاده دسـتگاه‌های دولتی منتشـر کـرد که مبانی امنیتی پیشـنهادی را بـرای اسـتفاده سـازمان‌ها و دسـتگاه‌های دولتی برشـمرده بود. ایـن راهنما مبتنـی بـر حوادثی اسـت کـه «گـروه پاسـخگویی بـه حـوادث» در دوره‌های گذشـته تجربه کـرده بود.

مهم‌ترین پیشرفت‌ها

۱) نظـام مشـورتی بـه اجـرا گذاشـته شـده توسـط «مرکـز ملـی امنیت سـایبری»، تـا انـدازه زیادی تقویت شـده اسـت و امکانات پیشـرفته‌تری برای انتشـار سـریع اطلاعـات را فراهم کرده اسـت.

۲) «مرکز ملی امنیت سـایبری» توانسـته اسـت برنامه عملیاتی «حسگر» را طراحـی و آزمایـش کـرده و در تعـدادی از ادارات و دسـتگاه‌های دولتـی مسـتقر کنـد و بـا ایـن کار بـه ارتقـای امنیـت سـامانه‌ها و داده‌هـای فنـاوری اطلاعـات در برابـر تهدیـدات سـطح بـالا کمک کرده اسـت.

۳) سـازمان‌ها و دسـتگاه‌های دولتـی بـا راهنمایـی «مرکـز ملـی امنیـت سـایبری»، سـرمایه‌گذاری‌های زیـادی در زمینـه امنیـت انجـام داده‌اند.

۶ - ۲- هدف

به‌منظور ارتقای تاب‌آوری و امنیت سامانه‌های فناوری اطلاعات بخش دولتی در جهت محافظت بهتر از خدماتی که مردم به آن‌ها اتکا دارند و داده‌های آن‌ها.

۶ - ۳- اقدامات

بخش دولتی به فناوری اطلاعات اتکای زیادی دارد تا در عمل بتواند خدماتی که لازم است را ارائه دهد؛ به همین خاطر، این خدمات باید ایمن و تاب‌آور بوده و بتواند محرمانه ماندن اطلاعات خصوصی را تضمین کند. به این منظور، دولت اقدامات خاص ذیل را به اجرا می‌گذارد.

۸) «مرکز ملی امنیت سایبری» یک استاندارد امنیتی پایه را تعیین خواهد کرد تا توسط همه دستگاه‌های دولتی و سازمان‌های اصلی به کار گرفته شود.

«مرکز ملی امنیت سایبری» در همکاری با دفتر مدیر ارشد اطلاعات دولت، مجموعه استانداردهای پایه امنیت سایبری را برای فناوری‌های اطلاعاتی و ارتباطی دولت تدوین می‌کند. این مجموعه با استانداردهای بین‌المللی مطابقت خواهد داشت، از ادارات دولتی آغاز خواهد شد و به‌تدریج در تمام ارگان‌های دولتی به کار گرفته خواهد شد. این استانداردها بیشتر شامل اقدامات و نظارت‌هایی در رابطه با آموزش کارکنان، هویت و مدیریت دسترسی هستند. بر اساس تمهیدات، این استانداردها در سطح داخلی دستگاه‌های دولتی و با پشتیبانی‌ها و راهنمایی‌های ارائه‌شده توسط «مرکز ملی امنیت سایبری» ارزیابی می‌شوند.

۹) طرح «حسگر» فعلی گسترش خواهد یافت تا تمام وزارتخانه‌های دولتی را در برگیرد، و یک ارزیابی جامع انجام خواهد شد تا میزان امکان‌پذیری توسعه «حسگر» برای پوشش تمامی شبکه‌های دولتی بررسی شود.

برنامه حسگر «مرکز ملی امنیت سایبری» در تمامی سازمان‌ها و دستگاه‌های دولتی و ارتقای سامانه تشخیص و رفع زودهنگام تهدیدها پیگیری خواهد کرد. «مرکز ملی امنیت سایبری» از برنامه خود در همه واحدهای دولتی پشتیبانی می‌کند و «مرکز عملیات مشترک امنیتی» به‌منظور پشتیبانی و بهره‌برداری از این سامانه توسعه خواهد یافت. بر اساس تمهیدات، هر سازمان و دستگاه حاکمیتی بزرگ، تحت مدیریت «مرکز ملی امنیت سایبری» مورد نظارت «مرکز عملیات مشترک امنیتی» قرار خواهد داشت.

۱۰) به‌منظور سهولت در اشتراک اطلاعات و اقدامات برتر و نیز فراهم آوردن امکاناتی برای «مرکز ملی امنیت سایبری» در راه پشتیبانی از به‌کارگیری استانداردهای امنیتی پایه، مجمع حاکمیتی امنیت فناوری‌های اطلاعاتی ایجاد خواهد شد و تمامی مدیران امنیت فناوری‌های اطلاعات در سراسر حاکمیت می‌توانند عضو آن شوند.

«مرکز ملی امنیت سایبری» ایجاد، مدیریت و اجرای مجمع جدید امنیت فناوری اطلاعات بخش دولتی با حضور مدیران امنیت فناوری اطلاعات سراسر دستگاه‌ها و سازمان‌های دولتی را رهبری خواهد کرد. این مجمع هر سه ماه یک‌بار تشکیل خواهد شد و اطلاعات پیرامون روش‌های برتر، فرایندهای میان‌سازمانی، تهدیدهای امنیت سایبری، اقداماتی برای همگرایی با استانداردهای جدید امنیت سایبری را در میان

خواهند گذاشت.

۱۱) «مرکـز ملـی امنیـت سـایبری» از طـرف حاکمیت موظف به انتشـار توصیه‌هایـی در رابطـه بـا اسـتفاده از نرم‌افزارهـا و سـخت‌افزارهای خـاص در زیرسـاخت‌های مخابراتـی و فناوری‌هـای اطلاعاتـی دولـت خواهد شـد.

«مرکـز ملـی امنیـت سـایبری» موظـف اسـت در مـورد تهیه و اسـتفاده از انـواع خاصی از زیرسـاخت‌ها و نرم‌افزارهای فناوری اطلاعـات در تأمین امنیت داده‌هـا و خدمـات دولـت، توصیه‌هایـی ارائه کنـد و برخی از زیرسـاخت‌ها که بـه تشـخیص ایـن مرکـز خطـری غیـر قابـل پذیـرش بـرای امنیـت داده‌های دولـت اسـت را معرفـی کند تـا از شـبکه‌های دولتـی فناوری اطلاعـات حذف شـده یـا به‌کارگیـری آن‌ها ممنوع شـود.

اقدام ۸ – «مرکز ملی امنیت سایبری» یک استاندارد امنیتی پایه را تعیین خواهد کرد تا توسط همه دستگاه‌های دولتی و سازمان‌های اصلی به کار گرفته شود.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	طراحی استانداردهای حداقلی مناسب برای فناوری اطلاعات دولت، در هماهنگی با مجمع امنیت فناوری‌های اطلاعات دولت	فصل چهارم سال ۲۰۲۱	مرکز ملی امنیت سایبری /دفتر مدیر ارشد اطلاعات دولت / مجمع فناوری اطلاعات دولت	دستگاه‌های دولتی و سازمان‌های اصلی
۲	تدوین تدابیر، نظارت‌ها و روش‌های اجرایی دقیق	فصل اول سال ۲۰۲۲	مرکز ملی امنیت سایبری /دفتر مدیر ارشد اطلاعات دولت/ مجمع فناوری اطلاعات حاکمیت	دستگاه‌های دولتی و سازمان‌های اصلی
۳	تهیه پیش‌نویس راهنماها و مطالب پشتیبان برای گروه‌های فناوری اطلاعات و واحدهای ارزیابی داخلی پیرامون قواعد همگرایی	فصل دوم سال ۲۰۲۲	مرکز ملی امنیت سایبری /دفتر مدیر ارشد اطلاعات دولت/ مجمع فناوری اطلاعات حاکمیت	دستگاه‌های دولتی و سازمان‌های اصلی

اقدام ۸ – «مرکز ملی امنیت سایبری» یک استاندارد امنیتی پایه را تعیین خواهد کرد تا توسط همه دستگاه‌های دولتی و سازمان‌های اصلی به کار گرفته شود.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۴	پشتیبانی از دستگاه‌ها و ادارات دولتی و سازمان‌های اصلی در اجرای استانداردهای مبنایی	در حال اجرا	مرکز ملی امنیت سایبری /دفتر مدیر ارشد اطلاعات دولت/ مجمع فناوری اطلاعات حاکمیت	دستگاه‌های دولتی و سازمان‌های اصلی
۵	ارزیابی روش و فرایند اجرای استانداردمبنایی	فصل چهارم سال ۲۰۲۳	مرکز ملی امنیت سایبری /دفتر مدیر ارشد اطلاعات دولت/ مجمع فناوری اطلاعات حاکمیت	دستگاه‌های دولتی و سازمان‌های اصلی

اقدام ۹ – طرح «حسگر» فعلی گسترش خواهد یافت تا تمام وزارتخانه‌های دولتی را در برگیرد، و یک ارزیابی جامع انجام خواهد شد تا میزان امکان‌پذیری توسعه «حسگر» برای پوشش تمامی شبکه‌های دولتی بررسی شود.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	به‌کارگیری «حسگر» در زیرساخت‌های همه ۱۵ وزارتخانه دولتی	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	تمامی دستگاه‌های دولتی، مجمع امنیت اطلاعات حاکمیت
۲	بررسی هزینه‌ها و مسائل حقوقی مرتبط با استفاده از «حسگر» در شبکه‌های حاکمیتی، پوشش تمامی دستگاه‌های فناوری اطلاعات و ارتباطات بخش دولتی، و ارائه نتیجه به دولت برای تصمیم	فصل چهارم سال ۲۰۲۱	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، دفتر دادستان کل کشور، وزارت هزینه‌های عمومی و اصلاحات

اقدام ۱۰ – به‌منظور سهولت در اشتراک اطلاعات اقدامات برتر و نیز فراهم آوردن امکاناتی برای «مرکز ملی امنیت سایبری» در راه پشتیبانی از به‌کارگیری استانداردهای امنیتی پایه، «مجمع حاکمیتی امنیت فناوری‌های اطلاعاتی» ایجاد خواهد شد و تمامی مدیران امنیت فناوری‌های اطلاعات در سراسر حاکمیت می‌توانند عضو آن شوند.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	پشتیبانی از ایجاد گروه فناوری اطلاعات بخش‌های دولتی در «مرکز ملی امنیت سایبری» و تدوین اصول مرجع برای مجمع	فصل اول سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، تمام ادارات دولتی
۲	طراحی جلسه توجیهی برای همه رؤسای امنیت فناوری‌های اطلاعات به‌منظور تشریح هدف مجمع امنیت سایبری	فصل اول سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، تمام ادارات دولتی
۳	برگزاری جلسات سه‌ماهه مجمع و تعیین رئیس و دبیر جلسات	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، تمام ادارات دولتی

اقدام ۱۱ – «مرکز ملی امنیت سایبری» از طرف حاکمیت موظف به انتشار توصیه‌هایی در رابطه با استفاده از نرم‌افزارها و سخت‌افزارهای خاص در زیرساخت‌های مخابراتی و فناوری‌های اطلاعاتی دولت خواهد شد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	تهیه توجیه و اصول مرجع و ارائه به دولت برای تصویب	فصل سوم سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی
۲	شروع به کار فرایند پیشنهادی «مرکز ملی امنیت سایبری»	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی

بخش هفتم

بخش هفتم

مهارت‌ها

۷ - ۱- وضعیت میدان

بیشتر در اثر رشد سریع امنیت سایبری به‌مثابه چالشی اجتماعی، در تعدادی از مهارت‌های مهم در این حوزه، شکاف‌های مهارتی قابل‌توجهی ایجاد شده است. این شکاف مهارتی مسئله‌ای جهانی است و بیش از ۲ میلیون پست خالی امنیت سایبری در سراسر جهان در سال ۲۰۱۹ وجود دارد. در سطح ملی، اطمینان از تأمین نیروی انسانی آماده برای حفظ توانایی‌ها در پشتیبانی از زیرساخت‌ها و همچنین برای ادامه جذب و حفظ سرمایه سنگین داده‌ها بسیار ضروری است. در جای خود، تأمین این تقاضا علاوه بر آموزش تازه‌واردان، به ترویج الگوهای آموزش چندسطحی و ارتقای مهارت‌ها با مشارکت متخصصان فناوری‌های اطلاعاتی و ارتباطی و سایر بخش‌های مربوطه نیاز دارد. ایرلند در سال‌های اخیر در راستای ارتقای مهارت‌ها، توسعه توانایی‌های پژوهشی و افزایش آگاهی‌های پیرامون امنیت سایبری به‌مثابه یک شغل، گام‌های بزرگی برداشته است. بااین‌وجود هنوز در چنین بخش‌هایی که با سرعت حرکت می‌کنند، نوعی فاصله زمانی وجود دارد و باید این تضمین وجود داشته باشد که دانش‌آموختگان، مؤسسات آموزشی را با مهارت‌های لازم برای نیازهای

شغلی بخش صنعت ترک می‌کنند.

دولت به دنبال آن است تا از طریق اجرای برنامه ارتقای مهارت‌های فناوری ۲۰۲۲، سومین برنامه اجرایی ارتقای مهارت‌های فناوری‌های اطلاعاتی و ارتباطی، به تقاضاهای روزافزون برای مهارت‌های امنیت سایبری توجه داشته باشد. این طرح، توسط گروه متخصص در زمینه نیازهای مهارت‌های آینده اجرا شد و امنیت سایبری در پژوهش‌های اولیه مربوط به آن، به‌مثابه یکی از مهم‌ترین زمینه‌های نوظهوری معرفی شد که در سال‌های آینده برای مهارت‌های پیشرفته فناوری اطلاعات و ارتباطات در ایرلند تقاضا ایجاد خواهد کرد. برنامه مهارت‌های امنیت سایبری به‌عنوان بخشی از برنامه مهارت‌های فناوری ۲۰۲۲ و از طریق چندین مسیر، از جمله برنامه «شبکه مهارت‌های ایرلند»، گسترش خدمات در آموزش عالی و ترویج کارآموزی فناوری‌های اطلاعاتی و ارتباطی از طریق پروژه سولاس (طرح آموزش مهارت‌های تکمیلی ایرلند) و مرجع ملی آموزش‌های تکمیلی به کار خود ادامه می‌دهد.

در اکتبر سال ۲۰۱۸، شبکه مهارت‌های ایرلند طرح جدید مهارت‌های امنیت سایبری را با همکاری مرکز ملی امنیت سایبری، اداره ملی جرائم سایبری پلیس و سایر آژانس‌ها و مؤسسات سطح سوم آغاز کرد. اهداف اصلی این طرح ارتقای آگاهی‌ها، پر کردن شکاف مهارت‌ها و تعیین استانداردهایی برای پذیرش مهارت‌ها و شایستگی‌ها در جهت پذیرش مسئولیت‌های امنیت سایبری تعریف شده است. طرح سه‌ساله این برنامه بر ایجاد آموزش و تأیید اعتبار در جهت رفع شکاف مهارت‌ها، جذب جوانان و به‌ویژه زنان به این بخش و ارتقا و توسعه مداوم حرفه‌ای تمرکز دارد. بر اساس برآورد شبکه مهارت‌های ایرلند، این طرح طی سه سال

آینده آموزش امنیت سایبری را به بیش از ۵۰۰۰ نفر ارائه خواهد داد. همچنین، بخش سطح سوم در ایرلند نیز تعداد قابل‌توجهی دوره را در زمینه امنیت سایبری آغاز کرده است که اکنون حداقل ۸ دوره در سطح ارشد ارائه می‌شود.

دوره‌های کارآموزی توسط کنسرسیوم‌هایی توسعه یافته است که با همین صنعت هدایت می‌شوند، این دوره‌ها آموزش‌های ضمن اشتغال و خارج از کار را ترکیب می‌کنند. دوره‌های کارآموزی که مصوب شورای عالی کارآموزی هستند و از صندوق ملی کارآموزی بودجه می‌گیرند، راه‌های تازه‌ای در برابر افراد ترک تحصیل کرده، جویای کار و افراد خواهان تغییر شغل قرار می‌دهد. در فوریه سال ۲۰۱۹ یک دوره کاردانی حرفه‌ای ۲ ساله در مهارت‌های امنیت سایبری در سطح ۶ با محوریت مؤسسه تربیت نیروی انسانی «سَپ» به‌عنوان شاخص این صنعت و شرکت «خط سرعت فناوری اطلاعات» به‌عنوان همکار راه‌اندازی شد.

همچنین، مؤسسات سطح سوم هم تعداد زیادی از دوره‌ها در حوزه امنیت سایبری را ارائه می‌دهند که در حال حاضر حداقل ۸ دوره در سطح ارشد در حال اجرا است. همچنین برنامه‌های امنیت سایبری به‌عنوان بخشی از طرح اسپرینگ‌بورد+ در حال اجرا است، طرحی که تسهیلات روزافزونی را برای افراد شاغل و آماده‌سازی آن‌ها برای پذیرش نقش‌ها یا شغل‌های دیگر ارائه می‌دهد. با افزایش تقاضا برای مجموعه مهارت‌های امنیت سایبری، اهمیت این مراکز و مؤسسات بیشتر هم خواهند شد.

وزارت کسب‌وکار و نوآوری با همکاری وزارت شوراها، در مارس ۲۰۱۹ طرح «مشاغل آینده ایرلند» را راه‌اندازی کرد که تلاش دارد بسترهایی

فراهم کند تا افراد و سازمان‌ها بهتر بتوانند در برابر فرصت‌ها و چالش‌های آینده تاب‌آوری و آمادگی داشته باشند. «مشاغل آینده ایرلند» همچنین تلاش دارد اطمینان حاصل کند که بنگاه‌ها و کارکنان موقعیت مناسبی دارند چنان‌که خودشان می‌توانند با تغییرات فناورانه و سایر تحولات آینده مواجه شوند. با آن‌که «مشاغل آینده ایرلند» دامنه وسیعی دارد، یکی از پنج محور اصلی آن «پذیرش نوآوری و تغییر فناورانه» است. این چارچوب نیاز به مهارت‌های جدید و متنوع را برای مواجهه با اقتصاد در حال تغییر متغیر به رسمیت می‌شناسد و «بهره‌برداری از حوزه‌های پیشرفته فناوری مانند هوش مصنوعی، تجزیه‌وتحلیل داده‌های کلان، اینترنت اشیا و ارز رمز، به‌منظور تسهیل امور و کمک به شرکت‌ها در زمینه نوآوری و توسعه راه‌حل‌ها» ضروری می‌داند.

برای دستیابی به این اهداف، مجموعه‌ای از اهداف آرمانی قابل‌دسترس هم مشخص شده است، از جمله افزایش ظرفیت شرکت‌های متوسط و کوچک برای اجرای برنامه‌های تحقیق و توسعه، ارائه آموزش با کیفیت بالا، تشویق یادگیری مادام‌العمر و افزایش مشارکت در برنامه‌های کارآموزی. تعدادی از طرح‌های اجرایی پیش‌ازاین تحت عناوین برنامه‌های میان‌مدت «مشاغل آینده ایرلند» در سال ۲۰۱۹ آغاز شده است. «مشاغل آینده ایرلند» هر ساله گام‌های جدیدی را برای تحقق این آرمان‌ها برمی‌دارد.

مهم‌ترین پیشرفت‌ها

۱) سند راهبردی مهارت‌های فناوری ۲۰۲۲ منتشر و اجرایی شده است.

۲) «شبکه مهارت‌های ایرلند» برنامه «مهارت‌های امنیت سایبری» خود را در جهت ارائه طیف وسیعی از برنامه‌ها در این زمینه آغاز کرد.

۳) شرکت «خط سرعت فناوری اطلاعات» یک برنامه امنیت سایبری برای کارآموزان راه‌اندازی کرده است.
۴) دولت برنامه «مشاغل آینده ایرلند» را راه‌اندازی کرده است، بستری چندساله برای توسعه بنگاه‌ها و مهارت‌ها، به‌ویژه در بخش فناوری.

۷ - ۲- هدف

سرمایه‌گذاری در طرح‌های ابتکاری آموزشی برای آماده‌سازی نیروی انسانی در جهت استفاده از فناوری‌های اطلاعاتی پیشرفته و مشاغل امنیتی سایبری.

۷ - ۳- اقدامات

دولت با اجرای طرح «آینده شغلی ایرلند»، «مهارت‌های فناوری ۲۰۲۲» و اجرای این سند راهبردی، قصد دارد این اطمینان را حاصل کند که بازار کار نیروی انسانی ماهر و آموزش دیده کافی در جهت پاسخگویی به خواسته‌های کارفرمایان دارد.

۱۲) حاکمیت، توسعه و استفاده از آموزش سطح دوم و سوم در علوم رایانه و امنیت سایبری را همچنان تضمین خواهد کرد و این کار را از جمله از راه پشتیبانی از شبکه‌های آموزش مهارت در ایرلند در توسعه برنامه‌های آموزشی برای همه سطوح و همچنین پشتیبانی از ابتکارات مراکز آموزشی پیشرفته «سولاس» (طرح آموزش مهارت‌های تکمیلی ایرلند) برای برنامه‌های کارآموزی فناوری‌های اطلاعاتی و ارتباطی و امنیت سایبری پیگیری خواهد کرد.

دولت به پشتیبانی خود از «شبکه مهارت‌های ایرلند» در توسعه و ارائه آموزش مهارت‌ها به صنایع خصوصی در جهت ارتقای مشارکت نیروی کار سایبری، توسعه مهارت‌ها و پیشرفت شغلی ادامه خواهد داد. «مرکز ملی امنیت سایبری» از طرح‌هایی پشتیبانی خواهد کرد که زنان را به فعالیت در حوزه امنیت سایبری ترغیب کرده و مشارکت‌کنندگان سایر حوزه‌ها را هم دعوت به ارائه آموزش‌های ترکیبی خواهد کرد.

۱۳) بنیاد علوم ایرلند، در چارچوب «برنامه آینده‌های هوشمند»، به ترویج امنیت سایبری به‌عنوان یک گزینه شغلی در مدارس و دانشگاه‌های ایرلند خواهد پرداخت.

«آینده هوشمند» یک برنامه آموزشی مشترک است که توسط بنیاد علوم ایرلند اجرا می‌شود و اطلاعاتی در مورد مشاغل مرتبط با علوم، فناوری، مهندسی و ریاضیات (STEM) برای دانشجویان سطح دوم در ایرلند ارائه می‌دهد. بنیاد علوم ایرلند با استفاده از متخصصان تازه‌وارد به این صنعت و برای شمول در طرح «آینده هوشمند»، طرح درس امنیت سایبری را خواهد افزود تا دانشجویان از طیف گسترده‌ای از فرصت‌های شغلی موجود در این زمینه آگاه شوند.

۱۴) بنیاد علوم ایرلند با همکاری وزارت سرمایه، تجارت و اشتغال و نیز وزارت محیط‌زیست، آب‌وهوا و ارتباطات، از طریق برنامه آینده‌های هوشمند، مراکز آموزشی بنیاد و دیگر بنگاه‌ها، کار امکان‌سنجی تأمین بودجه برای پژوهش در حوزه امنیت سایبری را انجام خواهند داد.
این مرکز پژوهشی، دانشمندان و مهندسان را از دانشگاه تا صنایع دور هم جمع خواهد کرد تا به پرسش‌های اساسی پژوهش بپردازند.

اقدام ۱۲ – حاکمیت توسعه و استفاده از آموزش سطح دوم و سوم در علوم رایانه و امنیت سایبری را همچنان تضمین خواهد کرد و این کار را از جمله از راه پشتیبانی از شبکه‌های آموزش مهارت در ایرلند در توسعه برنامه‌های آموزشی برای همه سطوح و همچنین پشتیبانی از ابتکارات مراکز آموزشی پیشرفته «سولاس» (طرح آموزش مهارت‌های تکمیلی ایرلند) برای برنامه‌های کارآموزی فناوری‌های اطلاعاتی و ارتباطی و امنیت سایبری پیگیری خواهد کرد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	پشتیبانی از ابتکارات تحت مهارت‌های فناوری ۲۰۲۲ از جمله توسعه مهارت‌های شبکه‌های مهارت‌آموزی و فناوری‌های اطلاعاتی و ارتباطی برای کارآموزی	در حال اجرا	وزارت محیط‌زیست، آب‌وهوا، و ارتباطات	شبکه‌های مهارت، سولاس (طرح آموزش مهارت‌های تکمیلی ایرلند)
۲	افزودن آموزش و مهارت‌افزایی به‌عنوان موضوعی ثابت در دستور کار مجمع امنیت فناوری‌های اطلاعاتی حاکمیت	فصل دوم سال ۲۰۲۰	مرکز ملی امنیت سایبری	مجمع امنیت فناوری‌های اطلاعاتی دولت
۳	پشتیبانی از توسعه دوره کوتاه‌مدت امنیت سایبری که پیش‌نیاز گنجاندن آموزش امنیت سایبری در سطح دوم خواهد بود	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	شورای ملی برنامه‌ریزی و ارزیابی درسی
۴	پشتیبانی از طرح‌های ابتکاری که زنان را در زمینه امنیت سایبری تشویق می‌کنند	در حال اجرا	مرکز ملی امنیت سایبری، وزارت آموزش و مهارت‌ها	صنعت

اقدام ۱۳ – بنیاد علوم ایرلند، در چارچوب «برنامه آینده‌های هوشمند»، به ترویج امنیت سایبری به‌عنوان یک گزینه شغلی در مدارس و دانشگاه‌های ایرلند خواهد پرداخت.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	مرکز ملی امنیت سایبری به دنبال شرکایی در بخش صنعت برای مشارکت در «آینده‌های هوشمند» است	فصل اول سال ۲۰۲۰	مرکز ملی امنیت سایبری	بنیاد علوم ایرلند، صنعت
۲	مرکز ملی امنیت سایبری با «آینده‌های هوشمند» همکاری خواهد کرد تا طرح‌های ابتکاری را موردحمایت قرار دهد که دانشجویان دختر را به حوزه امنیت سایبری تشویق می‌کنند	فصل اول سال ۲۰۲۰	مرکز ملی امنیت سایبری	بنیاد علوم ایرلند

اقدام ۱۴ – بنیاد علوم ایرلند با همکاری وزارت سرمایه، تجارت و اشتغال و نیز وزارت محیط‌زیست، آب‌وهوا و ارتباطات، از طریق برنامه آینده‌های هوشمند، مراکز آموزشی بنیاد و دیگر بنگاه‌ها، کار امکان‌سنجی تأمین بودجه برای پژوهش در حوزه امنیت سایبری را انجام خواهند داد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	صدور فراخوان برای مشارکت جامعه امنیت سایبری و مبتنی بر نظام بررسی آزاد جامعه مستقل بین‌الملل	فصل چهارم سال ۲۰۲۰	بنیاد علوم ایرلند	مرکز ملی امنیت سایبری، وزارت سرمایه، تجارت و اشتغال، بنیاد علوم
۲	صدور فراخوان برای مشارکت جامعه امنیت سایبری و مبتنی بر نظام بررسی آزاد جامعه مستقل بین‌الملل	فصل اول سال ۲۰۲۱ ۲۰۲۱	بنیاد علوم ایرلند	مرکز ملی امنیت سایبری، وزارت سرمایه، تجارت و اشتغال، بنیاد علوم

بخش هشتم

بخش هشتم

توسعه بنگاه‌ها

۸ - ۱- وضعیت میدان

«سازمان جذب سرمایه‌های خارجی» ایرلند از طرح «سایبر ایرلند» توسط «موسسه فناوری کورک» به‌منظور رشد و توسعه «خوشه امنیت سایبری ایرلند» حمایت کرده است. سایبر ایرلند در ۲۰ مه سال ۲۰۱۹ به‌صورت رسمی راه‌اندازی شد و به میزبانی مؤسسه فناوری کورک شروع به کار کرد. این خوشه ملی تلاش دارد نیازهای این بخش را در ایرلند نمایندگی کند و مشارکت‌کنندگانی را از بخش‌های صنعت، دانشگاه و دولت به همراه دارد. «مؤسسه فناوری کورک» ۲ سال بودجه را از «سازمان جذب سرمایه‌های خارجی» به‌منظور توسعه خوشه تأمین کرده و برای دستیابی به این هدف یک برنامه با ساختاری ۷ مرحله‌ای تدوین کرده است. توسعه «سایبر ایرلند» یکی از موارد گنجانده شده در طرح «مشاغل آینده ایرلند، ۲۰۱۹» است و تعهد دولت به توسعه این بخش را نشان می‌دهد.

مهم‌ترین پیشرفت‌ها

۱) برنامه سایبر ایرلند، ابتکار سایبر ایرلند با کمک مالی سازمان جذب سرمایه‌های خارجی و برای کمک به توسعه این بخش در ایرلند راه‌اندازی شده است.

۸ - ۲- اهداف

برای ارتقای سطح آگاهی‌ها از مسئولیت‌های کسب‌وکارهای پیرامون ایمنی شبکه‌ها، ابزارها، و اطلاعات و نیز در جهت هدایت تحقیق و توسعه در زمینه امنیت سایبری در ایرلند، از جمله از راه تسهیل سرمایه‌گذاری در حوزه فناوری جدید.

۸ - ۳- اقدامات

۱۵) حاکمیت به پشتیبانی و همکاری کامل خود با برنامه ایرلند سایبری با بودجه سازمان جذب سرمایه‌های خارجی ادامه خواهد داد و سازوکارهای جدیدی را برای حمایت از همکاری‌های صنعت / دانشگاه / دولت در زمینه امنیت سایبری بررسی خواهد کرد.

مرکز ملی امنیت سایبری به همراه سازمان جذب سرمایه‌های خارجی و مؤسسه ایرلند، به‌عنوان اعضای هیئت فعال راه‌اندازی «سایبر ایرلند» مشارکت خواهند داشت و از طرح‌های ابتکاری آن‌ها در دور هم آوردن صنعت، دانشگاه و دولت در جهت تقویت فضای امنیت سایبری در ایرلند حمایت خواهند کرد. سایبر ایرلند به‌طور فعال در ارتقای آموزش و مهارت‌ها، مجامع ارتباطی، جذب سرمایه‌های مستقیم خارجی و تحقیق و توسعه نقش خواهد داشت.

۱۶) سازمان توسعه بنگاه‌های ایرلند در جهت تسهیل پیوندهای مشترک بین نهادهای پژوهشی و سازمان‌ها، یک برنامه اختصاصی در زمینه امنیت سایبری را طراحی و اجرا خواهد کرد که به کاربرد عملی پژوهش در تجارت خواهد انجامید.

همخوان با مأموریت «مؤسسه ایرلند»، این مؤسسه دانش و تجربه بخشی خود

در زمینـه برنامه‌هـای ابتکاری مشـترک صنعتی و دانشـگاهی را بـه کار گرفته و از طریـق همـکاری بـا «مرکـز ملی امنیت سـایبری» به بررسـی فرصت‌های حمایـت اقتصـادی از امنیت سـایبری در طرح‌های دارای سـود اقتصادی میان مؤسسـه و گروه‌هـای پژوهشـی می‌پردازد.

اقدام ۱۵ – حاکمیت به پشتیبانی و همکاری کامل خود با برنامه ایرلند سایبری با بودجه سازمان جذب سرمایه‌های خارجی ادامه خواهد داد و سازوکارهای جدیدی را برای حمایت از همکاری‌های صنعت / دانشگاه / دولت در زمینه امنیت سایبری بررسی خواهد کرد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	ارائه پشتیبانی به سایبر ایرلند برای توسعه خوشه امنیت سایبری صنعت، دانشگاه و دولت	در حال اجرا	سازمان جذب سرمایه‌های خارجی	سایبر ایرلند، مؤسسه ایرلند، مرکز ملی امنیت سایبری، وزارت سرمایه، تجارت و اشتغال

اقدام ۱۶ – سازمان توسعه بنگاه‌های ایرلند در جهت تسهیل پیوندهای مشترک بین نهادهای پژوهشی و سازمان‌ها، یک برنامه اختصاصی در زمینه امنیت سایبری را طراحی و اجرا خواهد کرد که به کاربرد عملی پژوهش در تجارت خواهد انجامید.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	تأسیس یک مرکز صلاحیت امنیت سایبری ملی	فصل اول سال ۲۰۲۱	مرکز ملی امنیت سایبری	مرکز ملی امنیت سایبری، مؤسسه ایرلند، وزارت سرمایه، تجارت و اشتغال

بخش نهم

بخش نهم

مشارکت و همکاری

۹ - ۱- وضعیت میدان

امنیت سایبری در ذات و اساس خود امری بین‌المللی است و برای بسیاری از ابعاد ارتباطات بین‌المللی دولت پیامدهای پیچیده و متعددی دارد. ما امنیت سایبری را به‌عنوان یک اولویت سیاست خارجی مهم می‌دانیم. از چندی پیش تحولات در این زمینه بخشی جدایی‌ناپذیر از سیاست‌گذاری خارجی ایرلند بوده است، اما در هر دو معنای خاص و عام، اتحادیه اروپا نیاز به تکامل و توسعه این نوع از مشارکت و همکاری وجود دارد.

در سطح جهانی، ۱۰ سال گذشته با حملات و حوادث فزاینده‌ای از جمله حملات به زیرساخت‌های برق در اوکراین در سال ۲۰۱۵ و حوادث مرتبط با دو بدافزار «Wannacry2» و «NotPetya» در سال ۲۰۱۷ همراه بوده است. این حوادث، بحث‌های جدیدی را در مورد نقش دولت‌ها و جامعه بین‌المللی در بازاندیشی نگرش و رفتار دولت در مورد اینترنت و همچنین بررسی مجموعه اقدامات مناسب برای استفاده کشورها در حوزه حاکمیتی خود به‌منظور تضمین یکپارچگی و تاب‌آوری سامانه‌های اصلی برانگیخته است.

تعدادی از سازمان‌های بین‌المللی برنامه‌هایی را برای آزمودن و طرح این موضوعات در چارچوب روابط موجود بین‌المللی ارائه داده‌اند. برجسته‌ترین آن‌ها «گروه متخصصان حاکمیت سازمان ملل» (GGE) بوده است. این گروه در سال ۲۰۰۴ و بر اساس بحث‌هایی تأسیس شد که از سال ۱۹۹۸ بر اساس قطعنامه ۷۰/۵۳ در جریان بود. از سال ۲۰۰۴، این گروه پنج نشست داشته است که در سه مورد درباره گزارش‌ها به توافق رسیده و در دو مورد، از جمله آخرین مورد در سال ۲۰۱۷، نتوانست که به توافقی برسد.

در اواخر سال ۲۰۱۸، سازمان ملل دو قطعنامه جدید در مورد مسائل مربوط به امنیت سایبری را تصویب کرد. اولین قطعنامه کارگروه گشوده‌ای را تأسیس کرد که در ابتدا در ژوئن ۲۰۱۹ تشکیل جلسه داد و بر ارتقای آگاهی‌ها، ایجاد فهم مشترک و پیگیری اجرای اصول و قواعد رفتار دولت پاسخگو تمرکز خواهد داشت. قطعنامه دوم سه گزارش موفق «گروه متخصصان حاکمیت سازمان ملل» را مورد تأکید قرار داده و خواستار ایجاد «گروه متخصصان حاکمیت سازمان ملل» دیگری با تمرکز بر کاربرد قوانین بین‌المللی در فضاهای مجازی و پیگیری ایجاد اجماع درباره رفتار دولت پاسخگو در فضای مجازی شده است.

در سطح منطقه‌ای، هر دو سازمان امنیت و همکاری در اروپا و اتحادیه اروپا نیز نقش پیشروی را در حوزه امنیت سایبری بر عهده داشته‌اند. سازمان امنیت و همکاری اروپا در سال‌های ۲۰۱۳ و ۲۰۱۶، دو مجموعه پیش‌نویس «اقدامات اعتمادسازی» به‌منظور «ارتقای همکاری میان‌دولتی، شفافیت، پیش‌بینی‌پذیری و ثبات،کاهش خطرات سوءتفاهم، تشدید تعارض، و درگیری» را تهیه کرده‌اند که «ممکن است

در اثر فناوری‌های اطلاعاتی و ارتباطی ایجاد شود».

مهم‌ترین پیشرفت‌ها

۱) سازمان ملل دو قطعنامه جدید با تمرکز بر همکاری و ایجاد آگاهی در مورد مسائل امنیت سایبری تصویب کرد.

۲) سازمان امنیت و همکاری اروپا دو مجموعه اقدامات اعتمادسازی را برای افزایش همکاری و ثبات ارائه داد.

۹ - ۲- هدف

ادامه همکاری با شرکای بین‌المللی و سازمان‌های بین‌المللی برای اطمینان از گشودگی، امنیت، یگانگی و آزادی فضاهای سایبری و توانایی آن در تسهیل توسعه اقتصادی و اجتماعی.

۹ - ۳- اقدامات

۱۷) تعهدات دیپلماتیک ایرلند در زمینه امنیت سایبری را تقویت خواهیم کرد و برای این کار از جمله به استقرار وابستگان سایبری در مأموریت‌های اصلی دیپلماتیک و ایجاد ظرفیت پایدار در کشورهای سوم خواهیم پرداخت.

ایرلند از راه تعیین وابستگان سایبری تعیین شده در مأموریت‌های اصلی دیپلماتیک، تعهد دیپلماتیک خود در زمینه امنیت سایبری را به‌عنوان بخشی از طرح «ایرلند جهانی» تقویت می‌کند. بر اساس برنامه خود برای پشتیبانی از فضای مجازی آزاد، گشوده، صلح‌آمیز و ایمن، در تعامل بین‌المللی خود طرفدار دیپلماسی پیشگیرانه خواهیم بود. ما از

همکاری‌های بین‌المللی برای مقابله با جرائم اینترنتی و ارتقای سطح همکاری‌های رسمی و غیررسمی در فضاهای مجازی پشتیبانی خواهیم کرد و برای این کار، از جمله به ایجاد ظرفیت پایدار در کشورهای طرف سوم خواهیم پرداخت. به‌عنوان بخشی از تعهد خود در مبارزه با جرائم اینترنتی، کنوانسیون بوداپست را به‌زودی تصویب خواهیم کرد. کاربرد قوانین بین‌الملل، از جمله حقوق بشردوستانه بین‌المللی و احترام به حقوق بشر، تعهدات بین‌المللی ما در زمینه امنیت سایبری را هدایت می‌کند. ما کشورهای درحال‌توسعه و بازیگران جامعه مدنی را پشتیبانی و توانمند خواهیم کرد و خوب می‌دانیم که نقض احتمالی حقوق بشر حمله به مدافعان حقوق بشر، و ردیابی و کنترل اقلیت‌های قومی با استفاده از فناوری هم انجام می‌شود.

۱۸) به‌منظور هماهنگی مواضع ملی در سراسر دستگاه‌های حاکمیتی، یک گروه میان‌بخشی در زمینه حاکمیت اینترنت و سیاست بین‌المللی فضاهای سایبری ایجاد خواهیم کرد.

یک گروه میان‌بخشی بین‌المللی در زمینه سیاست‌های بین‌المللی سایبری ایجاد خواهیم کرد تا همکاری‌هایی که ابعاد ژئوپلیتیک دارند را هماهنگ کنیم و در زمینه حاکمیت اینترنت و امنیت سایبری به موضع هماهنگی در سطح بین‌المللی برسیم.

۱۹) همکاری‌های فعلی خود با سازمان‌های بین‌المللی را گسترش خواهیم داد و برای این کار از جمله به مرکز برتر امنیت سایبری در تالین، استونی خواهیم پیوست.

ما همکاری و تعامل خود با سازمان‌های بین‌المللی در برخورد با طیف وسیعی از موضوعات ناشی از این سند راهبردی را تعمیق خواهیم بخشید.

به‌این‌ترتیب، ایرلند به «مرکز تعالی امنیت سایبری» در تالین، استونی ملحق می‌شود و در این عرصه مشارکتی فعال خواهد داشت. این کار شامل اعزام یکی از اعضای نیروهای دفاعی به آن مرکز در زمان مناسب خواهد بود.[1] ما همچنین از فرایندهای سازمان ملل متحد در تلاش برای ایجاد و اجرای چارچوبی برای ثبات در فضای مجازی پشتیبانی کامل خواهیم کرد.

اقدام ۱۷ – تعهدات دیپلماتیک ایرلند در زمینه امنیت سایبری را تقویت خواهیم کرد و برای این کار از جمله به استقرار وابستگان سایبری در مأموریت‌های اصلی دیپلماتیک و ایجاد ظرفیت پایدار در کشورهای طرف سوم خواهیم پرداخت.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	استقرار وابسته سایبری برای مأموریت‌های دیپلماتیک مهم	فصل سوم سال ۲۰۲۰	وزارت امور خارجی	مرکز ملی امنیت سایبری
۲	تصویب کنوانسیون بوداپست	فصل دوم سال ۲۰۲۱	وزارت دادگستری	مرکز ملی امنیت سایبری، وزارت پارلمان
۳	تدوین و توسعه یک برنامه ظرفیت‌سازی پایدار برای کشورهای درحال‌توسعه	فصل دوم سال ۲۰۲۱	وزارت امور خارجی، مرکز ملی امنیت سایبری	مرکز ملی امنیت سایبری

اقدام ۱۸ – به‌منظور هماهنگی مواضع ملی در سراسر دستگاه‌های حاکمیتی، یک گروه میان‌بخشی در زمینه حاکمیت اینترنت و سیاست بین‌المللی فضاهای سایبری ایجاد خواهیم کرد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	تأسیس یک گروه میان‌بخشی برای هماهنگی در زمینه سیاست‌های سایبری	فصل دوم سال ۲۰۲۰	وزارت امور خارجی	مرکز ملی امنیت سایبری، تمامی وزارتخانه‌ها

۱. اعزام اولیه به مرکز تعالی امنیت سایبری از نیروهای دفاعی خواهد بود، پس از تصویب آن در دولت ممکن است افراد اعزامی غیرنظامی یا نظامی باشند.

اقدام ۱۹ – همکاری‌های فعلی خود با سازمان‌های بین‌المللی را گسترش خواهیم داد و برای این کار از جمله به مرکز برتر امنیت سایبری در تالین، استونی خواهیم پیوست.				
	اقدامات برای ارائه	**جدول زمانی فصلی**	**راهبری**	**همکاران اصلی**
۱	اعزام عضو وزارت دفاع به «مرکز تعالی امنیت سایبری»	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	نیروی دفاعی، وزارت دفاع، وزارت امور خارجی

بخش دهم

بخش دهم

شهروندان

۱۰ - ۱- وضعیت میدان

از نظر آگاهی از امنیت سایبری طی چند سال اخیر، به‌ویژه در نظام آموزشی، اقدامات ملی مهمی انجام شده است. به‌عنوان یک نمونه، وب وایز، یک ابتکار امنیت اینترنتی است که بخشی از بودجه آن توسط وزارت آموزش و مهارت‌ها تأمین می‌شود و طرح «توسعه حرفه‌ای معلمان» و « فناوری در آموزش» استفاده مستقل، مؤثر و ایمن از اینترنت جوانان را ترویج می‌دهد، کاری که از طریق برنامه راهبردی توسعه مستمر اطلاعات و آگاهی والدین، معلمان و خود کودکان و با ارسال پیام‌های به‌روز، مرتبط و منظم و از جمله معرفی شیوه‌های خوب استفاده از اینترنت در مدارس انجام می‌شود.

برای این کار طیفی از ابزارها و منابع آماده شده است که شامل «UP2US»، «سلفی من و جهان وسیع‌تر»، «Lockers» می‌شود، مرکز والدین آنلاین با عنوان وب وایز، و «در کنترل باش» هم برای معلمان طراحی شده است که به موضوع اجبار و اخاذی جنسی آنلاین و شیوه‌های مقابله با آن می‌پردازد. در اواسط سال، طرح مرجع «قهرمانان HTML» راه‌اندازی شد، که هدف آن کمک و پشتیبانی از مربیان کودکان ۷ تا

۱۰ ساله در مورد استفاده ایمن و مسئولانه از اینترنت، از جمله رسانه‌های اجتماعی است.

طرح آینده هوشمند توسط بنیاد علوم ایرلند و با مشارکت سازمان‌ها و دانشگاه‌ها به اجرا گذاشته می‌شود. این برنامه اطلاعاتی در خصوص مشاغل مرتبط با علوم، فناوری، مهندسی و ریاضیات (STEM) برای دانش‌آموزان سطح دوم مدارس در ایرلند فراهم می‌کند. طرح آینده هوشمند با همکاری مشاوران، معلمان و صنعت، به اجرا گذاشته شده است تا منابع و فعالیت‌هایی را برای تشویق دانش‌آموزان به کار علمی ایجاد کند. وب‌سایت آینده‌های هوشمند اطلاعاتی را در مورد طیف گسترده‌ای از فرصت‌های موجود مانند دوره‌های آموزشی، کارآموزی، جشنواره و رویدادها ارائه می‌دهد. در فوریه ۲۰۱۹، طرح آینده‌های هوشمند با مشارکت وزارت آموزش و مهارت، پویش ملی جدیدی را با عنوان «من برای این کار دستمزد می‌گیرم» راه‌اندازی کرد. پویش این کمپین پیرامون منبعی آنلاین از پروفایل افراد متخصص در صنایع مرتبط با علوم، فناوری، مهندسی، و ریاضیات کار می‌کند تا دانش‌آموزان به شناختی از زندگی در رابطه با این رشته‌ها و فرصت‌های متنوع پیش روی آن‌ها برسند.

این برنامه در حال حاضر توسط یک گروه حامی مالی و با ریاست وزارت آموزش و مهارت‌ها در حال اجرا است. تصویب قانون ایمنی آنلاین که به چگونگی تضمین ایمنی بیشتر کودکان در فضاهای آنلاین می‌پردازد هم به‌زودی انجام می‌شود. این تصویب برای اولین بار، این خواسته را نزد ارائه‌دهندگان خدمات اینترنتی مطرح می‌کند که باید برای اطمینان از ایمنی کاربران از خدمات خود اقدامات ویژه‌ای را به انجام برسانند.

مهم‌ترین پیشرفت‌ها

۱) طرح وب‌وایز، از طریق یک برنامه پایدار ارتقای اطلاعات و آگاهی به والدین، معلمان و کودکان راهنمایی‌های لازم در مورد استفاده ایمن از اینترنت را ارائه داده است.

۲) طرح آینده‌های هوشمند، در جهت ارائه اطلاعات در مورد مشاغل در رشته‌های مرتبط با علوم، فناوری، مهندسی و ریاضیات به دانش‌آموزان سطح دوم راه‌اندازی شده است.

۱۰ - ۲- هدف

به‌منظور افزایش سطح عمومی مهارت‌ها و آگاهی‌های افراد در مورد اقدامات اساسی سلامت سایبری و پشتیبانی از آن‌ها از راه ارائه اطلاعات و آموزش.

۱۰ - ۳- اقدامات

با توسعه مراقبت‌های سلامتی سایبری مناسب در جمعیت‌های بیشتر، می‌توان جامعه ایمن‌تری را فراهم کرد. آگاهی از تهدیدات سایبری در بخش‌های آسیب‌پذیر، اهمیت ویژه‌ای دارد.

۲۰) دولت یک پویش سراسری اطلاعات امنیت سایبری در سطح ملی ایجاد خواهد کرد تا از اطلاعات ارائه‌شده توسط «مرکز ملی امنیت سایبری» و اداره ملی جرائم سایبری پلیس استفاده کرده و اطلاعاتی را در اختیار دستگاه‌هایی قرار دهد که به‌صورت مستقیم مشغول تدارک اطلاعات هستند.

پویش ملی آگاهی سایبری طراحی و برای مردم به اجرا گذاشته خواهد

شد. این برنامه تجربه «مرکز ملی امنیت سایبری» و اداره ملی جرائم سایبری پلیس را استخراج خواهد کرد و با همکاری «خدمات توسعه حرفه‌ای معلمان» و «کمیسیون ایمنی آنلاین» به‌عنوان یک نمونه تلاش مشترک میان‌بخشی توسعه خواهد یافت. هدف از این پویش، ارتقای آگاهی‌های جامعه در مورد تهدیدهای رایج سایبری مانند سلامت مبنایی فضاهای سایبری و مهندسی اجتماعی خواهد بود. این برنامه همچنین فعالیت‌های آگاهی‌بخشی را با هدف قرار دادن گروه‌های آسیب‌پذیر مانند کودکان و افراد مسن، از جمله با ارائه اطلاعات به طرح وب‌وایز تسهیل می‌کند.

اقدام ۲۰ – دولت یک پویش سراسری اطلاعات امنیت سایبری در سطح ملی ایجاد خواهد کرد تا از اطلاعات ارائه‌شده توسط «مرکز ملی امنیت سایبری» و اداره ملی جرائم سایبری پلیس استفاده کرده و اطلاعاتی را در اختیار دستگاه‌هایی قرار دهد که به‌صورت مستقیم مشغول تدارک اطلاعات هستند.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	پشتیبانی از ادامه افزودن عناصر امنیت سایبری در برنامه‌های طرح وب‌وایز	فصل چهارم سال ۲۰۲۰	وزارت محیط‌زیست، آب‌وهوا و ارتباطات	نیروی پلیس، وزارت آموزش و مهارت‌ها
۲	طراحی و اجرای یک پویش به‌منظور ارتقای آگاهی‌های عمومی شامل انتشار اطلاعات مربوط به امنیت سایبری و پیشگیری از جرائم اینترنتی	فصل اول سال ۲۰۲۱	مرکز ملی امنیت سایبری، کمیسیون ایمنی آنلاین	وزارت محیط‌زیست، آب‌وهوا و ارتباطات، نیروی پلیس، وزارت آموزش و مهارت‌ها، وزارت دادگستری

بخش یازدهم

بخش یازدهم

مسئولیت‌ها و چارچوب‌های حکمرانی

۱۱ - ۱- ساختار حکمرانی

اجرای سند راهبرد ملی در امنیت سایبری به یک چارچوب و ساختار حاکمیتی نیاز دارد، هم از نظر پاسخ عملیاتی و هم از اجزای اصلی خود اجرای چارچوب راهبردی.

۱۱ - ۲- اجرای راهبرد ملی امنیت سایبری

کمیته امنیت کابینه مسیر اصلی هماهنگی پاسخ‌ها به موضوعات امنیت ملی خواهد بود. بااین‌حال، یک کمیته بلندمرتبه میان‌بخشی ایجاد می‌شود که سالی دو بار تشکیل جلسه داده و وظیفه ارزیابی و گزارش پیشرفت از دستیابی به اقدامات برشمرده در این سند راهبردی را بر عهده دارد و نیز می‌تواند متمم‌هایی بر اقدامات برنامه‌ریزی شده را پیشنهاد دهد.

پیوست

پیوست

فهرست اقدامات

توسعه ظرفیت‌های ملی

اقدام ۱ – «مرکز ملی امنیت سایبری»، به‌خصوص با توجه به گسترش توانایی نظارت و پاسخگویی به حوادث امنیتی سایبری و تهدیدهای فزاینده در برابر دولت، توسعه بیشتری خواهد یافت.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	تهیه برنامه دقیق فنی و سازمانی برای «مرکز عملیات مشترک امنیتی»	فصل چهارم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	وزارت محیط‌زیست، آب‌وهوا و ارتباطات
۲	دریافت ضمانت قانونی برای توسعه «مرکز ملی امنیت سایبری»	فصل دوم سال ۲۰۲۱	«مرکز ملی امنیت سایبری»	وزارت محیط‌زیست، آب‌وهوا و ارتباطات، وزارت هزینه‌های عمومی و اصلاح
۳	ساخت نمونه اولیه مرکز عملیات مشترک امنیتی با استفاده از امکانات موقت	فصل چهارم سال ۲۰۲۱	«مرکز ملی امنیت سایبری»	اداره امور عمومی، وزارت محیط‌زیست، آب‌وهوا و ارتباطات
۴	کمیسیون نهایی تسهیلات مرکز عملیات مشترک امنیتی در پایگاه اصلی «مرکز ملی امنیت سایبری»	فصل دوم سال ۲۰۲۳	«مرکز ملی امنیت سایبری»	اداره امور عمومی، وزارت محیط‌زیست، آب‌وهوا و ارتباطات

اقدام ۲ – اطلاعات و تحلیل‌های تهیه شده پیرامون تهدید توسط «مرکز ملی امنیت سایبری» در کارهای مرکز بررسی‌های امنیت ملی ادغام خواهد شد.				
	اقدامات برای ارائه	**جدول زمانی فصلی**	**راهبری**	**همکاران اصلی**
۱	ایجاد زیرساخت‌های گزارش‌دهی و اشتراک اطلاعات مرکز ملی بررسی‌های امنیتی	فصل اول ۲۰۲۰	«مرکز ملی امنیت سایبری»	مرکز ملی بررسی‌های امنیتی

حفاظت از زیرساخت‌های حساس ملی

اقدام ۳ – سامانه کنونی حفاظت از زیرساخت‌های حساس ملی که بر اساس شیوه‌نامه امنیت شبکه و اطلاعات ملی راه‌اندازی شده است، با تمرکز ویژه بر برنامه‌های همگرایی و ممیزی مستمر در جهت کاهش خطرات خدمات اصلی، همچنان به کار گرفته شده و توسعه می‌یابد.				
	اقدامات برای ارائه	**جدول زمانی فصلی**	**راهبری**	**همکاران اصلی**
۱	تکمیل مرحله اول خودارزیابی اپراتورهای خدمات ضروری (OES) بر اساس چارچوب کنترل امنیت	فصل اول سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	اپراتور خدمات ضروری تعیین شده
۲	آغاز آزمایش کنترل امنیت اپراتورهای خدمات ضروری	فصل سوم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	اپراتور خدمات ضروری تعیین شده
۳	بازبینی ثبت اپراتورهای خدمات ضروری و دستورالعمل‌های امنیتی	فصل سوم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	اپراتور خدمات ضروری تعیین شده
۴	کنترل امنیت پس از حوادث و بررسی‌های مستمر همگرایی اپراتورهای خدمات ضروری	در حال اجرا	«مرکز ملی امنیت سایبری»	اپراتور خدمات ضروری تعیین شده

اقدام ۴ – سامانه کنونی حفاظت از زیرساخت‌های حساس ملی که بر اساس شیوه‌نامه امنیت شبکه و اطلاعات ملی راه‌اندازی شده است، با تمرکز ویژه بر برنامه‌های همگرایی و ممیزی مستمر در جهت کاهش خطرات خدمات اصلی، همچنان به کار گرفته شده و توسعه می‌یابد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	گروه راهبری تشکیل شده و اصول مرجع برای بررسی مورد توافق قرار گیرد	فصل اول سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی، بانک مرکزی ایرلند، کمیسیون تنظیم مقررات ارتباطات، کمیسیون مقررات صنایع عمومی، سازمان هواپیمایی
۲	تکمیل مرحله جمع آوری اطلاعات و توافق پیرامون روش اجرایی	فصل سوم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی، بانک مرکزی ایرلند، کمیسیون تنظیم مقررات ارتباطات، کمیسیون مقررات صنایع عمومی، سازمان هواپیمایی
۳	فرایند ارزیابی کامل شامل مشاوره بین‌المللی و ارزیابی دقیق روابط متقابل میان‌بخشی.	فصل دوم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی، بانک مرکزی ایرلند، کمیسیون تنظیم مقررات ارتباطات، کمیسیون مقررات صنایع عمومی، سازمان هواپیمایی
۴	تکمیل گزارش نهایی و توصیه‌ها	فصل چهارم سال ۲۰۲۰	«مرکز ملی امنیت سایبری»	نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی، بانک مرکزی ایرلند، کمیسیون تنظیم مقررات ارتباطات، کمیسیون مقررات صنایع عمومی، سازمان هواپیمایی

اقدام ۵ – سامانه پشتیبانی از زیرساخت‌های حساس ملی در طول اجرای سند راهبردی به‌گونه‌ای گسترش و تعمیق خواهد یافت تا دامنه وسیع‌تری از زیرساخت‌های حساس ملی و ازجمله ابعادی از سامانه‌های انتخاباتی را شامل شود.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	پیش‌نویس رئوس لایحه برای موافقت دولت	فصل چهارم سال ۲۰۲۱	وزارت محیط‌زیست، آب‌وهوا و ارتباطات	دفتر دادستان کل کشور
۲	تهیه پیش‌نویس با دفتر دادستان کل کشور	فصل اول سال ۲۰۲۲	وزارت محیط‌زیست، آب‌وهوا و ارتباطات	دفتر دادستان کل کشور
۳	فرایند قانون‌گذاری	فصل دوم سال ۲۰۲۲	وزارت محیط‌زیست، آب‌وهوا، و ارتباطات	دفتر دادستان کل کشور، قوه مقننه

اقدام ۶ – گروه‌های اشتراک اطلاعات فعلی که توسط «مرکز ملی امنیت سایبری» اداره می‌شوند، توسعه بیشتری خواهند یافت و گروه‌های اشتراک تهدید فعلی چنان توسعه خواهند یافت تا طیف وسیع‌تری از زیرساخت‌های حساس ملی را شامل شوند.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	گسترش نمایندگان فعلی گروه اشتراک تهدید تا حد گنجاندن زیرساخت‌های حساس ملی و تدوین اصول مرجع جدید	فصل دوم سال ۲۰۲۰	مرکز ملی امنیت سایبری	نیروی پلیس، نیروی دفاعی، زیرساخت‌های حساس ملی
۲	اصلاح توافق‌های موجود با انگلیس در مورد به اشتراک‌گذاری اطلاعات و واکنش به حوادث، با ارجاع خاص به حفاظت از زیرساخت‌های حساس حیاتی شمال - جنوب	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر برنامه‌ریزی اضطراری، مرکز پشتیبانی از زیرساخت‌های ملی، انگلیس

اقدام ۷ – حاکمیت مجموعه جدیدی از استانداردهای همگرایی را معرفی خواهد کرد تا امنیت سایبری زیرساخت‌های مخابراتی کشور را پشتیبانی کند.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	تصویب اقدامات اجرایی برای بخش‌نامه ۱۹۷۲/۲۰۱۸	فصل چهارم سال ۲۰۲۰	وزارت محیط‌زیست، آب‌وهوا و ارتباطات	مرکز ملی امنیت سایبری، کمیسیون تنظیم مقررات ارتباطات
۲	ارائه پشتیبانی فنی به کمیسیون تنظیم مقررات ارتباطات	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	کمیسیون تنظیم مقررات ارتباطات
۳	اجرای اقدامات امنیتی بازبینی شده	فصل اول سال ۲۰۲۱	کمیسیون تنظیم مقررات ارتباطات	وزارت محیط‌زیست، آب‌وهوا و ارتباطات، مرکز ملی امنیت سایبری، اپراتورهای مخابرات

داده‌ها و شبکه‌های بخش دولتی

اقدام ۸ – «مرکز ملی امنیت سایبری» یک استاندارد امنیتی پایه را تعیین خواهد کرد تا توسط همه دستگاه‌های دولتی و سازمان‌های اصلی به کار گرفته شود.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	طراحی استانداردهای حداقلی مناسب برای فناوری اطلاعات دولت، در هماهنگی با مجمع امنیت فناوری‌های اطلاعات دولت	فصل چهارم سال ۲۰۲۱	مرکز ملی امنیت سایبری /دفتر مدیر ارشد اطلاعات دولت / مجمع فناوری اطلاعات دولت	دستگاه‌های دولتی و سازمان‌های اصلی
۲	تدوین تدابیر، نظارت‌ها و روش‌های اجرایی دقیق	فصل اول سال ۲۰۲۲	مرکز ملی امنیت سایبری /دفتر مدیر ارشد اطلاعات دولت/ مجمع فناوری اطلاعات حاکمیت	دستگاه‌های دولتی و سازمان‌های اصلی

اقدام ۸ – «مرکز ملی امنیت سایبری» یک استاندارد امنیتی پایه را تعیین خواهد کرد تا توسط همه دستگاه‌های دولتی و سازمان‌های اصلی به کار گرفته شود.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۳	تهیه پیش‌نویس راهنماها و مطالب پشتیبان برای گروه‌های فناوری اطلاعات و واحدهای ارزیابی داخلی پیرامون قواعد همگرایی	فصل دوم سال ۲۰۲۲	مرکز ملی امنیت سایبری /دفتر مدیر ارشد اطلاعات دولت/ مجمع فناوری اطلاعات حاکمیت	دستگاه‌های دولتی و سازمان‌های اصلی
۴	پشتیبانی از دستگاه‌ها و ادارات دولتی و سازمان‌های اصلی در اجرای استانداردهای مبنایی	در حال اجرا	مرکز ملی امنیت سایبری /دفتر مدیر ارشد اطلاعات دولت/ مجمع فناوری اطلاعات حاکمیت	دستگاه‌های دولتی و سازمان‌های اصلی
۵	ارزیابی روش و فرایند اجرای استاندارد مبنایی	فصل چهارم سال ۲۰۲۳	مرکز ملی امنیت سایبری /دفتر مدیر ارشد اطلاعات دولت/ مجمع فناوری اطلاعات حاکمیت	دستگاه‌های دولتی و سازمان‌های اصلی

اقدام ۹ – طرح «حسگر» فعلی گسترش خواهد یافت تا تمام وزارتخانه‌های دولتی را در برگیرد، و یک ارزیابی جامع انجام خواهد شد تا میزان امکان‌پذیری توسعه «حسگر» برای پوشش تمامی شبکه‌های دولتی بررسی شود.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	به‌کارگیری «حسگر» در زیرساخت‌های همه ۱۵ وزارتخانه دولتی	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	تمامی دستگاه‌های دولتی، مجمع امنیت اطلاعات حاکمیت
۲	بررسی هزینه‌ها و مسائل حقوقی مرتبط با استفاده از «حسگر» در شبکه‌های حاکمیتی، پوشش تمامی دستگاه‌های فناوری اطلاعات و ارتباطات بخش دولتی و ارائه نتیجه به دولت برای تصمیم	فصل چهارم سال ۲۰۲۱	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، دفتر دادستان کل کشور، وزارت هزینه‌های عمومی و اصلاحات

اقدام ۱۰ – به‌منظور سهولت در اشتراک اطلاعات اقدامات برتر و نیز فراهم آوردن امکاناتی برای «مرکز ملی امنیت سایبری» در راه پشتیبانی از به‌کارگیری استانداردهای امنیتی پایه، «مجمع حاکمیتی امنیت فناوری‌های اطلاعاتی» ایجاد خواهد شد و تمامی مدیران امنیت فناوری‌های اطلاعات در سراسر حاکمیت می‌توانند عضو آن شوند.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	پشتیبانی از ایجاد گروه فناوری اطلاعات بخش‌های دولتی در « مرکز ملی امنیت سایبری» و تدوین اصول مرجع برای مجمع	فصل اول سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، تمام ادارات دولتی
۲	طراحی جلسه توجیهی برای همه رؤسای امنیت فناوری‌های اطلاعات به‌منظور تشریح هدف مجمع امنیت سایبری	فصل اول سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، تمام ادارات دولتی
۳	برگزاری جلسات سه‌ماهه مجمع و تعیین رئیس و دبیر جلسات	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، تمام ادارات دولتی

اقدام ۱۱ – «مرکز ملی امنیت سایبری» از طرف حاکمیت موظف به انتشار توصیه‌هایی در رابطه با استفاده از نرم‌افزارها و سخت‌افزارهای خاص در زیرساخت‌های مخابراتی و فناوری‌های اطلاعاتی دولت خواهد شد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	تهیه توجیه و اصول مرجع و ارائه به دولت برای تصویب	فصل سوم سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی
۲	شروع به کار فرایند پیشنهادی «مرکز ملی امنیت سایبری»	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	دفتر مدیر ارشد اطلاعات دولت، نیروی پلیس، نیروی دفاعی، کمیته مشورتی غربالگری ملی

مهارت‌ها

اقدام ۱۲ – حاکمیت توسعه و استفاده از آموزش سطح دوم و سوم در علوم رایانه و امنیت سایبری را همچنان تضمین خواهد کرد و این کار را از جمله از راه پشتیبانی از شبکه‌های آموزش مهارت در ایرلند در توسعه برنامه‌های آموزشی برای همه سطوح و همچنین پشتیبانی از ابتکارات مراکز آموزشی پیشرفته «سولاس» (طرح آموزش مهارت‌های تکمیلی ایرلند) برای برنامه‌های کارآموزی فناوری‌های اطلاعاتی و ارتباطی و امنیت سایبری پیگیری خواهد کرد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	پشتیبانی از ابتکارات تحت مهارت‌های فناوری ۲۰۲۲ از جمله توسعه مهارت‌های شبکه‌های مهارت‌آموزی و فناوری‌های اطلاعاتی و ارتباطی برای کارآموزی	در حال اجرا	وزارت محیط‌زیست، آب‌وهوا، و ارتباطات	شبکه‌های مهارت، سولاس (طرح آموزش مهارت‌های تکمیلی ایرلند)
۲	افزودن آموزش و مهارت‌افزایی به‌عنوان موضوعی ثابت در دستور کار مجمع امنیت فناوری‌های اطلاعاتی حاکمیت	فصل دوم سال ۲۰۲۰	مرکز ملی امنیت سایبری	مجمع امنیت فناوری‌های اطلاعاتی دولت
۳	پشتیبانی از توسعه دوره کوتاه‌مدت امنیت سایبری که پیش‌نیاز گنجاندن آموزش امنیت سایبری در سطح دوم خواهد بود	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	شورای ملی برنامه‌ریزی و ارزیابی درسی
۴	پشتیبانی از طرح‌های ابتکاری که زنان را در زمینه امنیت سایبری تشویق می‌کنند	در حال اجرا	مرکز ملی امنیت سایبری، وزارت آموزش و مهارت‌ها	صنعت

اقدام ۱۳ – بنیاد علوم ایرلند، در چارچوب «برنامه آینده‌های هوشمند»، به ترویج امنیت سایبری به‌عنوان یک گزینه شغلی در مدارس و دانشگاه‌های ایرلند خواهد پرداخت.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	مرکز ملی امنیت سایبری به دنبال شرکایی در بخش صنعت برای مشارکت در «آینده‌های هوشمند» است	فصل اول سال ۲۰۲۰	مرکز ملی امنیت سایبری	بنیاد علوم ایرلند، صنعت
۲	مرکز ملی امنیت سایبری با «آینده‌های هوشمند» همکاری خواهد کرد تا طرح‌های ابتکاری را موردحمایت قرار دهد که دانشجویان دختر را به حوزه امنیت سایبری تشویق می‌کنند	فصل اول سال ۲۰۲۰	مرکز ملی امنیت سایبری	بنیاد علوم ایرلند

اقدام ۱۴ – بنیاد علوم ایرلند با همکاری وزارت سرمایه، تجارت و اشتغال و نیز وزارت محیط‌زیست، آب‌وهوا و ارتباطات، از طریق برنامه آینده‌های هوشمند، مراکز آموزشی بنیاد و دیگر بنگاه‌ها، کار امکان‌سنجی تأمین بودجه برای پژوهش در حوزه امنیت سایبری را انجام خواهند داد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	صدور فراخوان برای مشارکت جامعه امنیت سایبری و مبتنی بر نظام بررسی آزاد جامعه مستقل‌بین‌الملل	فصل چهارم سال ۲۰۲۰	بنیاد علوم ایرلند	مرکز ملی امنیت سایبری، وزارت سرمایه، تجارت و اشتغال، بنیاد علوم
۲	صدور فراخوان برای مشارکت جامعه امنیت سایبری و مبتنی بر نظام بررسی آزاد جامعه مستقل بین‌الملل	فصل اول سال ۲۰۲۱	بنیاد علوم ایرلند	مرکز ملی امنیت سایبری، وزارت سرمایه، تجارت و اشتغال، بنیاد علوم

توسعه بنگاه‌ها

اقدام ۱۵ – حاکمیت به پشتیبانی و همکاری کامل خود با برنامه ایرلند سایبری با بودجه سازمان جذب سرمایه‌های خارجی ادامه خواهد داد و سازوکارهای جدیدی را برای حمایت از همکاری‌های صنعت / دانشگاه / دولت در زمینه امنیت سایبری بررسی خواهد کرد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	ارائه پشتیبانی به سایبر ایرلند برای توسعه خوشه امنیت سایبری صنعت، دانشگاه و دولت	در حال اجرا	سازمان جذب سرمایه‌های خارجی	سایبر ایرلند، مؤسسه ایرلند، مرکز ملی امنیت سایبری، وزارت سرمایه، تجارت و اشتغال

اقدام ۱۶ – سازمان توسعه بنگاه‌های ایرلند در جهت تسهیل پیوندهای مشترک بین نهادهای پژوهشی و سازمان‌ها، یک برنامه اختصاصی در زمینه امنیت سایبری را طراحی و اجرا خواهد کرد که به کاربرد عملی پژوهش در تجارت خواهد انجامید.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	تأسیس یک مرکز صلاحیت امنیت سایبری ملی	فصل اول سال ۲۰۲۱	مرکز ملی امنیت سایبری	مرکز ملی امنیت سایبری، مؤسسه ایرلند، وزارت سرمایه، تجارت و اشتغال

مشارکت و همکاری

اقدام ۱۷ – تعهدات دیپلماتیک ایرلند در زمینه امنیت سایبری را تقویت خواهیم کرد و برای این کار از جمله به استقرار وابستگان سایبری در مأموریت‌های اصلی دیپلماتیک و ایجاد ظرفیت پایدار در کشورهای طرف سوم خواهیم پرداخت.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	استقرار وابسته سایبری برای مأموریت‌های دیپلماتیک مهم	فصل سوم سال ۲۰۲۰	وزارت امور خارجی	مرکز ملی امنیت سایبری
۲	تصویب کنوانسیون بوداپست	فصل دوم سال ۲۰۲۱	وزارت دادگستری	مرکز ملی امنیت سایبری، وزارت مجلس
۳	تدوین و توسعه یک برنامه ظرفیت‌سازی پایدار برای کشورهای درحال‌توسعه	فصل دوم سال ۲۰۲۱	وزارت امور خارجی، مرکز ملی امنیت سایبری	مرکز ملی امنیت سایبری

اقدام ۱۸ – به‌منظور هماهنگی مواضع ملی در سراسر دستگاه‌های حاکمیتی، یک گروه میان‌بخشی در زمینه حاکمیت اینترنت و سیاست بین‌المللی فضاهای سایبری ایجاد خواهیم کرد.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	تأسیس یک گروه میان‌بخشی برای هماهنگی در زمینه سیاست‌های سایبری	فصل دوم سال ۲۰۲۰	وزارت امور خارجی	مرکز ملی امنیت سایبری، تمامی وزارتخانه‌ها

اقدام ۱۹ – همکاری‌های فعلی خود با سازمان‌های بین‌المللی را گسترش خواهیم داد و برای این کار از جمله به مرکز برتر امنیت سایبری در تالین، استونی خواهیم پیوست.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	اعزام عضو وزارت دفاع به «مرکز تعالی امنیت سایبری»	فصل چهارم سال ۲۰۲۰	مرکز ملی امنیت سایبری	نیروی دفاعی، وزارت دفاع، وزارت امور خارجی

شهروندان

اقدام ۲۰ – دولت یک پویش سراسری اطلاعات امنیت سایبری در سطح ملی ایجاد خواهد کرد تا از اطلاعات ارائه‌شده توسط «مرکز ملی امنیت سایبری» و اداره ملی جرائم سایبری پلیس استفاده کرده و اطلاعاتی را در اختیار دستگاه‌هایی قرار دهد که به‌صورت مستقیم مشغول تدارک اطلاعات هستند.

	اقدامات برای ارائه	جدول زمانی فصلی	راهبری	همکاران اصلی
۱	پشتیبانی از ادامه افزودن عناصر امنیت سایبری در برنامه‌های طرح وب‌وایز	فصل چهارم سال ۲۰۲۰	وزارت محیط‌زیست، آب‌وهوا و ارتباطات	نیروی پلیس، وزارت آموزش و مهارت‌ها
۲	طراحی و اجرای یک پویش به‌منظور ارتقای آگاهی‌های عمومی شامل انتشار اطلاعات مربوط به امنیت سایبری و پیشگیری از جرائم اینترنتی	فصل اول سال ۲۰۲۱	مرکز ملی امنیت سایبری، کمیسیون ایمنی آنلاین	وزارت محیط‌زیست، آب‌وهوا و ارتباطات، نیروی پلیس، وزارت آموزش و مهارت‌ها، وزارت دادگستری

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