مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گزارش سریع
چهل و ششم

استراتژی امنیت ملی سایبری در اسپانیا

National Cyber Security Strategy in Spain

بسم الله الرحمن الرحیم

گزارش سریع

گزارش شماره ۴۶
شهریور ۱۴۰۱

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

استراتژی امنیت سایبری ملی اسپانیا - ۲۰۱۹

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

تهیه شده در پژوهشگاه فضای مجازی
(گروه مطالعات بین‌الملل)

ترجمه: دکتر الهه سوفسطائی
ناظر: عباس قنبری باغستان

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

فهرست

سخن نخست ۵
خلاصه اقدامات ۹
مقدمه ۱۹

بخش اول (فضای مجازی؛ فراتر از یک فضای مشترک جهانی) ۲۵
فضای مجازی: فرصت ها و چالش ها ۲۷
زیرساخت دیجیتال ۲۸
طرح بین الملل: امنیت در فضای مجازی ۲۹
برداشت جدیدی از فضای مجازی ۳۰

بخش دوم (چالش‌ها و تهدیدات در فضای مجازی) ۳۳
تهدیدهای سایبری ۳۵

بخش سوم (پیشنهاد، اصول و اهداف امنیت سایبری) ۴۱
پیشنهاد ۴۳
اصول حاکم ۴۴
هدف کلی ۴۷
هدف اول ۴۷
هدف دوم ۴۸
هدف سوم ۴۹
هدف چهارم ۵۰
هدف پنجم ۵۰
اهداف کلی ۵۳

بخش چهارم (طرح ها و اقدامات) ۵۵
طرح اول ۵۷
طرح دوم ۵۸

طرح سوم ۶۰
طرح چهارم ۶۱
طرح پنجم ۶۲
طرح ششم ۶۴
طرح هفتم ۶۵

بخش پنجم (امنیت سایبری در سیستم امنیت ملی) ۶۷
شورای امنیت ملی ۷۰
کمیته وضعیت ۷۰
شورای امنیت سایبری ملی ۷۰
کمیته دائمی امنیت سایبری ۷۰
مجمع ملی امنیت سایبری ۷۱
مقامات ذی صلاح عمومی و مرجع ملی CSIRT ۷۱
ملاحظات و ارزیابی نهایی ۷۲

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 اقدامات

خلاصه اقدامات

استراتژی امنیت سایبری ملی ۲۰۱۹ توسط شورای امنیت ملی تصویب شده است وارگان‌های زیر در این فرایند شرکت کرده‌اند:

وزارت امور خارجه
اتحادیه اروپا
وزارت دادگستری
وزارت دفاع
وزارت خزانه‌داری
وزارت امور داخلی
وزارت فواید عامه
وزارت آموزش و پرورش و آموزش‌های حرفه ای
وزارت صنعت، تجارت و جهانگردی
وزارت ریاست جمهوری و روابط پارلمانی
وزارت سیاست‌های ارضی و عملکرد عمومی
وزارت اقتصاد و تجارت
وزارت بهداشت، مصرف و رفاه اجتماعی
وزارت علوم، نوآوری و دانشگاه‌ها
مرکز اطلاعات ملی بخش امنیت ملی
کمیته‌ای از متخصصان انجمن‌های حرفه‌ای، شرکت‌ها و دانشگاه‌ها

مقدمه رئیس جمهور

چهارمین انقلاب صنعتی -انقلاب دیجیتال سال‌ها است که در کنار بحران‌های اقتصادی و پیامدهای اجتماعی و سیاسی که هنوز در حال بهبودی از آن هستیم، وجود داشته است. بنابراین با وجود فرصت های انکارناپذیری که دنیای دیجیتال به ما ارائه می‌دهد، بسیاری از شهروندان ما نسبت به بسیاری از اختلالات ایجاد شده در دنیای دیجیتال بدبین هستند و در اینجا، در تلاش برای تغییر این باور، باید تلاش خود را در دولت‌های عمومی متمرکز کنیم. آنچه در معرض خطر است، اعتماد جامعه به نهادهای دموکراتیک و توانایی‌مان برای روبرو شدن با آینده‌ای است که داریم می‌سازیم.

حضور در دوره تحولات و عدم اطمینان، ما را وادار به ارائه افق اخلاقی و مادی محکمی می‌کند و برای این منظور داشتن امنیت سایبری مجهز برای دوره جدید و مطابق با تهدیدهای جدید ضروری است. امنیت سایبری می‌تواند پاسخگوی چالش‌های مختلف باشد و این با همکاری بخش‌های عمومی و خصوصی و حمایت شهروندانی که از واقعیت در حال تغییر آگاه و به راه‌حل‌های این چالش‌ها متعهد هستند، ممکن می‌شود.

استراتژی امنیت سایبری ملی ارائه شده در اینجا مطابق با استراتژی امنیت ملی سال ۲۰۱۷ می‌باشد. این استراتژی در تلاش است تا در این امر سهیم باشد و این کار را با تعیین هدفی مشخص به عنوان راهنمای خود در این مسیر انجام می‌دهد و اطمینان حاصل می‌کند که این دوران تغییر، منشأ نارضایتی‌های فرهنگی و پسرفت‌های اقتصادی و کارگری نیست، بلکه فرصتی برای بهبود فضای رقابتی بین اسپانیا و شرکای

اروپایی است. این کار همچنین وضعیت ژئوپلیتیک فعلی ما را مورد توجه قرار داده است که ساخت و تقویت استقلال استراتژیک اتحادیه اروپا را تبدیل به امری ضروری می کند.

با وجود همه اینها، اسپانیا حرف‌های زیادی برای گفتن و کمک‌رسانی دارد. به هر حال، کشور ما یکی از کشورهای به‌هم‌پیوسته در جهان است. فقط با یک نگاه گذرا به اخبار روزانه می‌توان فهمید که تهدیدات سایبری واقعاً چقدر رایج و خطرناک هستند. از اخبار جعلی در شبکه‌های اجتماعی گرفته تا جاسوسی اینترنتی یا تروریسم در حوزه‌ی دیجیتال که تأثیرشان برروی زندگی روز به روز رو به افزایش است. علاوه بر این، فناوری‌های جدید مانند هوش مصنوعی، رباتیک، داده‌های بزرگ و هوشمند و بلاکچین تبدیل به بخشی از فعالیت‌های روزمره شهروندان، شرکت‌ها و ادارات دولتی شده‌اند. این فناوری های جدید زمینه را برای دستیابی به اطلاعات، دانش و داده‌ها و به اشتراک گذاشتنشان هموار کرده‌اند.

اجرای طرح 5G به عنوان راه جدیدی برای وصل شدن به یکدیگر در این تغییرات خواهد شد. ارتباط بیشتر و در نتیجه وابستگی بیشتر به زیرساخت‌های نام برده شده، به ما این امکان را می‌دهد تا در بسیاری از زمینه‌ها مثل دستیابی به اهداف توسعه پایدار سازمان ملل متحد، تا مبارزه با اثرات تغییرات اقلیمی پیشرفت کنیم.

فضای مجازی همچنین باعث آسیب‌پذیرتر شدن جامعه در برابر اقداماتی شرورانه علیه - و ناشی از - زیرساخت‌های جدید می‌شود. تهدیدها از طریق این فضا پیچیده و پیچیده‌تر می‌شوند و فضای مجازی که منطقه‌ای با نظارت ضعیف، بدون مرزهای قضایی مشخص است، در آن ردیابی و

شناسایی اقدامات مجرمانه دولتی و یا غیر دولتی دشوار است.

ایـن چالشـی بسـیار بزرگ و گسـترده اسـت و متخصصـان ما کـه از اعتبار شایسـته‌ای برخوردار می‌باشـند در حوزه‌های مختلفی درگیر امنیت سـایبری هسـتند. امـا امنیـت سـایبری نیـاز بـه تعهـد همـه مـا دارد. مسـئولیت ما در دولت‌هـای عمومـی ایـن اسـت کـه این تعهـد را هدایـت کنیـم و چارچوبی از اطمینـان را بـه شـرکت‌ها و شـهروندان ارائـه دهیم، آنهـا نیز باید ایـن تعهد را نگـه دارنـد. بـار دیگر، این نه تنها بـرای جلوگیری از خطـرات و تهدیدها، بلکه بـرای اسـتفاده بهینـه از فرصت‌هـا بـه نحـوی که به نفع همه باشـد، اسـت.

امنیـت سـایبری عـلاوه بـر حفاظـت از دارایـی‌هـا، از ارزش‌هـای نهادیـن یـک جامعـه آزاد ماننـد جامعـه مـا نیـز محافظـت می کنـد. ما نمـی خواهیم در ایـن دوره تحـول جهانـی ایـن اصـول را کنـار بگذاریـم. چالـش‌هـای فنی مربـوط بـه امنیت سـایبری متنـوع و پیچیده هسـتند، اما چیز دیگـری نیز در خطـر اسـت، چیـزی که بـه ارزش‌هـای اخلاقی و فرهنگـی مربوط می‌شـود و بـه نحـوه دیـدن و درک مـا از جهـان اشـاره دارد، چیزی کـه ما را بـه بهترین وجـه تعریـف مـی کنـد. آزادی، رفـاه و دموکراسـی مـا در نهایت بـه موفقیت مـا در طراحـی و پیـاده‌سـازی یـک اسـتراتژی امنیت سـایبری بسـتگی دارد. مـن متقاعـد شـده‌ام کـه بـا اسـتفاده از این سـند، ما گامی اساسـی به سـمت موفقیـت طـی سـال‌هایی نامشـخص امـا در عیـن حال جـذاب برداشـته‌ایم.

استراتژی ملی امنیت سایبری منطبق بر پیش‌بینی‌های استراتژی امنیت ملی ۲۰۱۷ با موضوع امنیت سایبری، با در نظر گرفتن اهداف کلی آن و خطوط عملیاتی از پیش تعیین شده برای دستیابی به آن اهداف کار می کند.

فعالیت‌های فضای مجازی برای جامعه کنونی حیاتی هستند. فناوری و زیرساخت‌های فضای مجازی دو عنصر استراتژیکی هستند که در تمام زمینه‌ها نقش دارند و آسیب‌پذیری در فضای مجازی ایجاد می‌کنند که برای توسعه یک کشور می‌تواند خطرآفرین باشد.

به همین دلیل، امنیت فضای مجازی یکی از اهداف با اولویت بالا در دستور کار دولت است که علاوه بر تضمین امنیت ملی، صلاحیت دولت را جهت ایجاد یک جامعه دیجیتال قابل اعتماد نشان می‌دهد.

کمک به ایجاد فضای مجازی امن و قابل اعتماد، از یک منظر چندرشته‌ای ، فراتر از اقدامات صرفاً فنی می‌باشد؛ این هدف با شناخت و درک انواع تهدیدهایی که شاید با آن‌ها روبرو شویم، مثل تهدیدهای جدید و نوظهور ممکن می‌شود.

فصل دوم با عنوان «تهدیدها و چالش‌ها در فضای مجازی» تهدیدات اصلی فضای مجازی را تعیین می‌کند. این تهدیدها و چالش‌ها در دو دسته طبقه‌بندی می‌شوند: از یک طرف، تهدیداتی علیه دارایی‌های فضای مجازی، و از طرف دیگر تهدیدهایی که از فضای مجازی برای انجام انواع فعالیت‌های مخرب و غیرقانونی استفاده می‌کنند.

فصل سوم با عنوان «پیشنهاد، اصول و اهداف امنیت سایبری» اصول حاکم بر استراتژی امنیت سایبری ملی را در سال ۲۰۱۷ (واحد اقدام، پیش‌بینی، کارآیی و تاب‌آوری) به عنوان پنج هدف خاص مشخص می کند. در فصل چهارم ، با عنوان «طرح ها و اقدامات»، هفت طرح و اقدامات لازم برای گسترش هر یک معرفی شده‌اند.

هدف این خطوط عملیاتی شامل:

- تقویت مهارت‌های لازم برای مبارزه علیه تهدیدات فضای مجازی؛
- تضمین امنیت دارایی‌های استراتژیک و افزایش تاب‌آوری اسپانیا؛
- تقویت امنیت سایبری شهروندان و شرکت‌ها؛
- تقویت مهارت‌های لازم برای تحقیق و تعقیب جرایم اینترنتی؛
- تضمین امنیت شهروندان و محافظت از حقوق و آزادی در فضای مجازی؛
- تقویت امنیت سایبری برای شهروندان و شرکت‌ها؛
- تقویت صنعت امنیت سایبری اسپانیا؛
- تشویق و حفظ استعدادها، تقویت استقلال دیجیتال؛
- بهبود امنیت فضای مجازی بین المللی؛
- ایجاد فضای مجازی باز، امن و قابل اعتماد که از منافع ملی حمایت می‌کند و فرهنگ امنیت سایبری را جهت کمک به پیشبرد برنامه جامع فرهنگ امنیت ملی رواج می‌دهد.

فصل پنجم، با عنوان «امنیت سایبری در سیستم امنیت ملی» معماری ارگانیک امنیت سایبری را تعریف می‌کند. به رهبری نخست وزیر اسپانیا، این ساختار به سه مقام تقسیم شده است:

- شورای امنیت ملی به عنوان کمیسیون نمایندگان دولت برای امنیت ملی.

• شورای امنیت سایبری ملی که از شورای امنیت ملی پشتیبانی می‌کند و به نخست وزیر در هماهنگی سیاست امنیت ملی با امنیت سایبری کمک می‌کند و همچنین مدیریتی که هماهنگی و همکاری بین بخش‌های عمومی و خصوصی ایجاد می‌کند.
• کمیته تخصصی که توسط اداره امنیت ملی پشتیبانی می‌شود و در مدیریت وضعیت‌های بحران در هر زمینه‌ای پشتیبانی خواهد کرد زیرا به دلیل چندرشته‌ای بودن و گستردگی، ممکن است توانایی ایجاد پاسخ معمول و اثربخش را نداشته باشد.

این سیستم توسط کمیته دائمی امنیت سایبری تکمیل می‌شود که هماهنگی بین وزارتخانه ها را در سطح عملیاتی برای امنیت سایبری تسهیل می‌کند، و به عنوان مرجعی به شورای ملی امنیت سایبری در زمینه های مربوط به ارزیابی فنی و عملیاتی خطرات و تهدیدات امنیت سایبری کمک خواهد کرد و به مقامات ذی‌صلاح دولتی و CSIRT ملی (تیم پاسخگویی به حوادث امنیت رایانه) در راه‌اندازی یک پروژه مشترک جدید دولتی و خصوصی، کمک می کند.

علاوه بر این، فصل آخر چند نتیجه‌گیری نهایی ارائه می دهد و سازوکارهایی برای به‌روزرسانی و ارزیابی استراتژی‌ها بیان می‌کند.

مقدمه

مقدمه

استراتژی امنیت سایبری ملی ۲۰۱۹ جایگاه اسپانیا را با در نظر گرفتن درک جدیدی که از امنیت سایبری در چارچوب سیاست امنیت ملی بدست آمده است، تعیین می‌کند.

اولین استراتژی ملی امنیت سایبری اسپانیا در سال ۲۰۱۳ به تصویب رسید. این سند دستورالعمل‌ها و اقدامات کلی را برای مقابله با چالش‌های ایجاد شده به دلیل آسیب‌پذیری فضای مجازی نشان می داد. علاوه بر این ، این استراتژی مدل حکومت را برای امنیت سایبری ملی طراحی کرده بود. در این دوره، اسپانیا نیز برای کمک به ایجاد فضای مجازی امن و قابل اعتماد به حرکت رو به جلوی خود ادامه داده است.

یکی از موارد اصلی آن، که به سال ۲۰۱۴ برمی گردد، شورای امنیت سایبری ملی است، مرجعی که از شورای امنیت ملی حمایت می کند. شورای امنیت سایبری ملی از اولین جلسه برگزار شده خود، وظیفه ایجاد هماهنگی بین سازمان‌های دارای صلاحیت ملی در کنار تهیه برنامه ملی امنیت سایبری را برعهده داشت. در نتیجه، امروز اسپانیا می تواند به خاطر سازمان‌های تخصصی امنیت سایبری خود به موقعیت برجسته‌اش نه تنها در اروپا بلکه در سراسر جهان، افتخارکند.

چارچوب قانونی نیز به طور قابل توجهی اصلاح شده است. جهت تضمین امنیت سیستم های بخش عمومی، حفظ تکامل خود و استفاده از تجربیات جمع آوری شده طی این چند سال اخیر، اصلاحیه چارچوب امنیت ملی، در سال ۲۰۱۵ منتشر شد. از سوی دیگر، اجرای قانون فرمان سلطنتی۲۰۱۸/۱۲ در مورد امنیت شبکه اطلاعات و سیستم، در تاریخ ۷ سپتامبر که باعث انتقال بخشنامه (EU) ۱۱۴۸/۲۰۱۶ (معروف به بخشنامه NIS) به نظم حقوقی اسپانیا می‌شود، نقطه عطف مهمی در بهبود امنیت سایبری کشورمان، گسترش دامنه این دستورالعمل برای بهبود امنیت سایبری در بین تمام بخشهای استراتژیک است.

قانون ۲۰۱۵/۳۶، در۲۸ سپتامبر در امنیت ملی تمدید شد تا یکی از پروژه‌هایی که از بزرگترین مسئولیت های دولت را نشان می‌داد، تقویت کند. قانون امنیت ملی امنیت سایبری را به عنوان یک زمینه خاص، مورد توجه قرار داده است.

بدون تردید، امنیت سایبری وجهه مدرن به امنیت ملی داده است، زیرا این حوزه تاکنون بیشترین پیشرفت را داشته است. این پویایی باید در همان مسیر باقی بماند. استراتژی امنیت ملی ۲۰۱۷ نقطه عطفی در تفکر استراتژیک ملی بود و امنیت فضای مجازی را متحول کرد.

یکی از روندهای جهانی شناسایی شده، دیجیتالی شدن و تغییرات ایجاد شده و پیامدهای امنیتی آن می‌باشد. این استراتژی یک چارچوب جدید را با پنج هدف کلی در همه زمینه‌ها تعیین می‌کند. مدیریت بحران، فرهنگ امنیت ملی، فضاهای مشترک جهانی، توسعه فناوری و پیش‌بینی بین المللی برای شبکه ای استراتژیک اسپانیا؛ که در آن‌ها از امنیت سایبری برای بررسی مسیرهای جدید که منتهی به مدل امنیتی

کنونی و آینده اسپانیا شده است، استفاده می‌شود.

مسئله امنیت سایبری جدید فراتر از صرفاً محافظت از میراث فناوری است و در حوزه‌های سیاسی، اقتصادی و اجتماعی نیز قرار می‌گیرد. علاوه بر اقداماتی که بر سیستم‌های دیجیتال تأثیر می گذارند، فضای مجازی باید به عنوان یک رابط استراتژیک در نظر گرفته شود که می‌تواند بر افکار عمومی تأثیر بگذارد و تفکر افراد را با دستکاری اطلاعات، نشر اطلاعات نادرست یا اقدامات ترکیبی تغییر دهد. کاربرد بالقوه آن در شرایط مختلف از جمله روندهای انتخاباتی، آن را بسیار پیچیده می‌کند.

این چشم‌انداز جدید کاربردی گسترش یافته است که در آن همکاری بین بخش‌های عمومی و خصوصی حائز اهمیت است و خواستار یک رویکرد جدید در قالب یک استراتژی ملی امنیت سایبری جدید می‌باشد.

بخش اول

بخش اول

فضای مجـازی؛ فراتر از یک فضـای مشـترک جهانی

ایـن فصـل فرصـت‌هـا و چالـش‌هـای فضـای مجـازی و زیرسـاخت‌هـای دیجیتالـی را ارائـه مـی‌دهـد، جنبه‌هـای بیـن‌المللـی رویکـرد امنیتـی آن را تشـریح می‌کنـد و ابهامات گسـترده در درک اسـپانیا از فضـای مجازی جدید را بیـان مـی‌کند.

فضای مجازی: فرصت‌ها و چالش‌ها

فضـای مجـازی یـک فضـای مشـترک جهانی اسـت که عملکـرد و پویایی از ویژگـی‌هـای بـارز آن می‌باشـد. فقـدان حاکمیـت، صلاحیـت ضعیـف آن، سـهولت دسترسـی و دشواری نسـبت دادن اقدامات در داخل آن، سناریویی را بـا طیـف گسـترده‌ای از فرصت‌ها در آینـده تعریف و همچنیـن تهدید چالش امنیتـی جـدی را ایجـاد می‌کند.

از یـک طـرف، فضـای مجـازی امـکان ارتبـاط جهانـی را فراهـم مـی‌کنـد و جریـان آزاد اطلاعـات، خدمـات و ایـده هـا را تسـهیل مـی‌کنـد. در نتیجـه ایـن حـوزه ای اسـت کـه باعـث افزایـش کارآفرینـی، تقویـت پیشـرفت اقتصـادی- اجتماعـی و ایجـاد فرصـت هـای جدیـد در همـه‌ی بخـش هـای تجاری می شـود. تأثیر دیجیتالی‌شـدن روی فرایندهای تولیدی در سـطح جهانی با

نرخ بی‌سابقه ای مشاهده می‌شوند. هوش مصنوعی، رباتیک، کلان داده، بلاکچین و اینترنت موارد در حال حاضر با ما هستند. گرچه این پایان حضور تکنولوژی با ما نیست و پیامدهای آن فراتر از این می‌باشد و حتی بر سبک‌های جدید زندگی اجتماعی تا روابط شخصی و اخلاقی نیز تأثیر می‌گذارد.

از طرف دیگر، دیجیتالی شدن امنیت را دگرگون می‌کند و چالش‌های بسیار جدی را به وجود می‌آورد. فضای مجازی مثل یک میدان جنگ ساخته شده است که اطلاعات و حریم دارایی با ارزشی در محیطی با رقابت ژئوپلیتیکی هستند. در نتیجه، ارتباط زیاد و وابستگی بیشتر به شبکه‌ها و سیستم‌ها، حتی اجزای دیجیتال، اشیاء و دستگاه‌ها، آسیب‌پذیری بیشتری ایجاد می‌کند و محافظت بهینه از اطلاعات را دشوار می‌کند.

دگرگونی دیجیتال:

هوش مصنوعی، رباتیک، کلان داده، بلاکچین، اینترنت اشیا و امنیت سایبری

زیرساخت دیجیتال

فضای مجازی صرفاً مجازی نیست، بلکه بر عناصر فیزیکی و منطقی نیز پایدار است. دستگاه‌ها، مؤلفه‌ها و سیستم‌های موجود در شبکه‌ها و

سیستم‌های اطلاعاتی و ارتباطی می‌توانند در معرض سوءاستفاده قرار بگیرند و عملکرد صحیحشان متوقف شود. اقدامات عمدی با نیت‌های مخرب علیه آنها می‌تواند عملکرد صحیح زیرساخت‌های مهمی را که به سیستم‌ها و شبکه‌های دیجیتالی وابسته اند را به خطر بیندازد.

این خطر به دلیل بیشتر بودن اهمیت ارزش‌های تجاری از ارزش‌های امنیتی در طراحی محصولات سخت‌افزاری و نرم افزاری، بیشتر نیز می‌شود. لازم به ذکر نیست که سیستم‌ها و خدمات، فرایند صدور گواهینامه را پیچیده می‌کنند و ممکن است زنجیره تامین را به خطر بیندازند. همه این جنبه ها درکنار ارتباط بین سیستم‌ها، می‌توانند اثرات آبشاری‌ایی با نتایج غیرقابل پیش بینی ایجاد کنند.

طرح بین‌الملل: امنیت در فضای مجازی

امنیت در فضای مجازی برای تضمین امنیت ملی و ایجاد یک جامعه دیجیتالی مبتنی بر اعتماد، به یکی از اولویت‌های اصلی دولت تبدیل شده است. در این زمینه، اسپانیا به عنوان یک ملت از چشم‌انداز و منافع خود دفاع می‌کند و با حمایت از فضای مجازی باز، متکثر و ایمن با جامعه جهانی همکاری می‌کند. اسپانیا نقش فعال خود را در تمامی مؤسساتی که امنیت سایبری در آن محوریت مرکزی دارد، به ویژه در اتحادیه اروپا، اتحادیه آتلانتیک و سازمان ملل، حفظ می‌کند و بدین ترتیب پایبندی خود به شرکا و متحدان را ثابت می‌کند. همچنین روابط با کشورهای شخص ثالث از طریق مکانیسم‌های همکاری دو جانبه که درک و اعتماد متقابل مبتنی بر روابط روان در زمینه امنیت سایبری را تسهیل می‌کند، حفظ می‌کند.

با آگاهی از اهمیت یک رویکرد چند جانبه، علاوه بر قوانین بین المللی و استانداردهای موجود برای رفتار مسئولانه در میان کشورها ، بهتر است نقش منشور ملل متحد را به عنوان مرجع برای پیشگیری از تعارض، همکاری و ثبات در فضای مجازی برجسته کنیم. توافق‌نامه‌های قطعی و اقدامات انجام شده برای جلب اعتماد و همچنین معاهدات و توافق نامه‌های بین‌المللی که اسپانیا به آن‌ها پیوسته است، مبنای کاربرد و اجرای آن هستند.

برداشت جدیدی از فضای مجازی

بعد اصلی ثبات شامل دفاع پیوسته از ارزش‌های دموکراتیک و اصول قانون اساسی درکنار حقوق اساسی شهروندان در فضای مجازی، به ویژه از نظر محافظت از اطلاعات و حریم شخصی، آزادی بیان و دسترسی به اطلاعات موثق و با کیفیت است.

درک مناسب این رویکرد نیازمند توجه به صورت چندرشته ای و فراتر از موضوعات صرفاً فنی، استفاده از اصول مدیریت متمرکز و هماهنگی عملکرد آن و اختصاص امنیت سایبری به امنیت ملی به عنوان صلاحیت کشور است.

اولاً، بخش خصوصی به عنوان مدیر و صاحب دارایی‌های دیجیتالی اسپانیا نقش مهمی را ایفا می‌کند، به این معنی که مهارت های لازم برای امنیت سایبری کشور عمدتا در این شرکت‌ها نهفته است. این بدان معنی است که امنیت سایبری برای رقابت بیشتر و تقویت رشد اقتصادی به حمایت، ارتقا و سرمایه‌گذاری نیاز دارد تا یک بستر دیجیتالی امن و مطمئن فراهم کند.

از طرف دیگر، ما باید خودمختاری فناوری خود را با تشویق پایگاه ملی صنعتی برای امنیت سایبری، R + D + i و مدیریت استعدادهای فناوری افزایش دهیم. منابع انسانی همچنان یک عامل حیاتی هستند. شکافی بین مشاغل بسیار تخصصی در فناوری‌های اطلاعاتی به ویژه امنیت سایبری و کارگران با سطح دانش اولیه ایجاد شده است.

ثانیاً، انتقال از یک مدل امنیت سایبری با رویکرد پیشگیرانه و دفاعی به یک حالت بازدارنده‌تر، با یک زمینه جهانی که نشان‌دهنده صلاحیت ژئوپلیتیک بیشتری است، همخوانی دارد. استفاده از فضای مجازی به عنوان زمینه‌ی مقابله، به طور مستقل یا به عنوان بخشی از یک عمل دیگر، به طور گسترده‌ای شناخته شده است. ایجاد اطمینان در امنیت سایبری به عنوان یکی از عناصر اساسی اقدامات دولت، به کسب و تقویت مهارت‌های دفاع سایبری نیاز دارد.

ثالثاً، تحولات سریع تهدیدات سایبری به یک هوش سایبری با رویکرد فعالانه‌تری نیاز دارد. ادغام آن با چارچوب کلی امنیت سایبری برای آگاهی از وضعیت و هشدارهای اولیه لازم که می‌توانند اقدامات مخالفان بالقوه را از طریق دانش مهارت‌ها، فنون، تاکتیک‌ها و اهداف آنها پیش‌بینی کند، کلیدی است. علاوه بر این، افزایش استفاده از مکانیزم‌ها و ابزارهایی که امکان تحقیق مناسب و پیگیری قانونی مرتکبان را ممکن می‌کند، حائز اهمیت می‌باشد.

همه موارد فوق را می‌توان با تشویق فرهنگ امنیت سایبری، افزایش آگاهی نسبت به تعهدات، به این معنی که شهروندان در برابر امنیت سایبری کشور مسئولیتی مشترک دارند، به نیاز پیامدهای بیشتر جامعه اضافه کرد.

بخش دوم

بخش دوم

چالش‌ها و تهدیدات در فضای مجازی

این فصل به بررسی تهدیدات و چالش‌های اصلی اسپانیا در فضای مجازی می‌پردازد.

ایجاد یک محیط امن و قابل اعتماد وظیفه‌ای است که باید با درک دانش، چالش و تهدیدات پیش رو، از جمله مسائل جدید و نوظهور که بر فضای مجازی تأثیر می‌گذارد، همراه باشد. استراتژی امنیت ملی سال ۲۰۱۷ بین آسیب‌های سایبری و اقداماتی که از فضای مجازی به عنوان وسیله‌ای برای فعالیت‌های مخرب یا غیرقانونی استفاده می‌شود، تفاوت قائل می‌شود.

تهدیدهای سایبری

تهدیدهای سایبری اختلالات یا دستکاری‌های مخربی هستند که روی ابزار وابسته به فناوری تأثیرگذار هستند و دامنه اقدامات آنها بسیار گسترده است. تهدیدهای سایبری از نظر ظرفیت و انگیزه انواع مختلفی دارند. آنها عملاً بر تمامی زمینه‌های امنیت ملی مانند دفاع، امنیت اقتصادی و یا حفاظت از زیرساخت‌های مهم تأثیر می‌گذارند و وسعت آنها حد و مرزی ندارد.

این ماهیت به این معنی است که امنیت سایبری یک دیدگاه جامع

است که شامل بخشهای دولتی، خصوصی و جامعه می‌شود. بنابراین ممکن است پیامدهایی همزمان برای مسائل گسترده ای مانند حاکمیت، حقوق اساسی، دفاع، اقتصاد و توسعه فناوری وجود داشته باشد.

در این سناریو، مکانیزم دفاعی همواره می‌تواند تکامل یابد البته تا زمانی که با تهدید جدی پیش روی سازگار شود. به طورهمزمان، مسئله دفاع نیز هر روز در حال پیشرفت و پیچیده تر شدن است.

از این نظر، ایجاد امنیت در شبکه‌ها و سیستم‌های اطلاعاتی مستلزم بهبود پیشگیری، شناسایی، واکنش و همچنین تشویق با توجه به پایبندی به اصول امنیت است. این موضوع باید در هر دو حوزه توسعه محصولات و خدمات فناوری و همچنین به‌روزرسانی و آموزش نحوه استفاده از آن مطرح شود.

اعمالی که در فضای مجازی برای **اهداف شرورانه** استفاده می‌شوند.

فناوری‌های دیجیتالی، فعالیت‌ها و راه‌های جدیدی در حوزه تجارت باز کرده‌اند که باید به طور منظم نظارت شوند، زیرا تهدیدات و چالش‌هایی که برای امنیت ملی ایجاد می‌کنند می‌توانند بر ثبات حقوق و آزادی ما تأثیر بگذارند. به همین ترتیب، همان ویژگی‌هایی که به پیشرفت در فضای مجازی کمک می‌کنند، می‌توانند برای اهداف شرورانه مورد استفاده قرار گیرند، خصوصاً الان که مخفی‌سازی و سرقت هویت اینقدر آسان شده است.

به لطف انقلاب اینترنتی، گروه‌های سازمان یافته، مجموعه‌ها و حتی اشخاص عادی می‌توانند به قدرت بی سابقه‌ای دست پیدا کنند. اتصال دیجیتال به این معنی است که جنبش‌های اجتماعی اهمیت استراتژیکی به خود می‌گیرند که این امر تا قبل از این دست کم گرفته شده بود.

جاسوسی اینترنتی و جرایم اینترنتی شامل اقداماتی در فضای مجازی است که برای اهداف مخرب یا غیرقانونی است.

با توجه به دشوار بودن تثبیت هویت، جاسوسی سایبری روشی نسبتاً ارزان و سریع است که نسبت به جاسوسی سنتی خطرات کمتری دارد. بیشترین توانایی را سازمان‌های اطلاعاتی یا نظامی دارند که اساساً از طریق تهدیدهای مداوم پیشرفته (APT) عمل می‌کنند. این نوع تهدید به این معنی است که حریف دارای دانشی پیچیده همراه با منابع و زیرساخت های مناسب است به طوری که تا پیش از وقوع حملات می‌توانند برای مدت طولانی بر روی اهداف خود تعامل داشته باشند وهم چنین با استراتژی‌های دفاعی سازگار شوند و سطح تعامل را تا لحظه آخر حفظ کنند.

علاوه بر این، در حال حاضر با وجود روند افزایشی تهدیدات (حملاتی هماهنگ و از پیش تعیین شده) دستکاری اطلاعات برای آسیب‌رساندن به سیستم‌های دولتی و نهادهای دموکراتیک از طریق طیف وسیعی از رسانه‌ها انجام می شود. عوامل دولتی و غیردولتی، مستقیماً یا با واسطه، در حال توسعه توانایی های نظامی برای فعالیت در فضای مجازی با بالابردن ظرفیت‌های تهاجمی هستند.

جرایم اینترنتی، به نوبه خود، یک مسئله سطح بالا در حوزه امنیت شهروندان است که یکی از گسترده ترین تهدیدات حال حاضر را نشان می‌دهد؛ این جرایم همه جوره وجود دارند و قربانیانشان هزاران مؤسسه، شرکت و شهروند هستند. اصطلاح جرایم اینترنتی به فعالیت های غیرقانونی در فضای مجازی مانند هدف قرار دادن سیستم‌های رایانه‌ای یا هر دارایی قانونی دیگر با استفاده از ابزارهای تکنولوژیکی اطلاق می‌شود. بسته به ماهیت، نوع یا انگیزه عمل و خسارت وارد شده، این جرایم می‌توانند به تروریسم سایبری، جرایم اینترنتی یا هکتیویسم اشاره داشته باشند. استفاده از روش‌های جدید برای معاملات مالی و اقتصادی، مانند ارز

رمزنگاری شده، یک چالش امنیتی جدی را برای قاچاق و تجارت غیرقانونی کالا و یا اخاذی، کلاهبرداری و سواستفاده از ابزارهای پرداختی غیر پولی، ایجاد می کند. از آنها می توان برای پولشویی و فرار مالیاتی استفاده کرد و منبع درآمدی برای جرایم سازمان یافته هستند. بنابراین، آنها می‌توانند تأمین مالی تروریسم را فراهم کنند و از عدم نظارت بر این ابزار ها، حداکثر سوءاستفاده را می کنند.

مجرمان اینترنتی تحت چارچوب جرایم سازمان یافته فعالیت می‌کنند و بی‌وقفه تکنیک هایی را برای ساخت مدل‌های تجاری کم خطر استفاده می کنند که ردیابی اقدامات آنها دشوار است.

گروه‌های تروریستی سعی دارند با سوءاستفاده از نقاط ضعف فضای مجازی، اقدامات شرورانه خود مانند حملات سایبری، فعالیت‌هایی برای رادیکال سازی گروه‌های دیگر، انتشار تکنیک‌ها و ابزارهای لازم برای یک حمله تروریستی و همچنین جذب نیرو، آموزش و یا تبلیغات را انجام دهند. ارتباط مستقیمی بین این موضوع و تهدید علیه زیرساخت‌های مهم وجود دارد زیرا سرویس‌های اصلی توسط این نقاط ضعف درست مانند یک دومینو فرو می‌ریزند.

گروه‌های هکتیویست به دلایل ایدئولوژیک حملات سایبری را انجام می‌دهند و گاهی اوقات با استفاده از محصولات، خدمات و ابزار رایج در فضای مجازی، به دنبال ایجاد حملاتی با تأثیرات مخرب عمده روی رسانه و اجتماع هستند.

همچنین، علاوه بر تمام تهدیدات و اقدامات ناشی از عدم وجود فرهنگ امنیت سایبری، نمی‌توان تهدیدات به وجود آمده از سازمان‌هایی که با کمک مجرمان اینترنتی می‌خواهند به منابع انسانی و فنی رقبا آسیب برسانند را نادیده بگیریم.

از طرف دیگر، اطلاعات دیجیتال به دارایی با ارزش بالایی تبدیل شده

است. آنالیز داده‌های شخصی در اینترنت برای اهداف گسترده، از مطالعات جامعه‌شناسی گرفته تا کمپین‌های تبلیغاتی، مورد استفاده قرار می‌گیرد. سواستفاده از داده‌های شخصی پتانسیل بالایی برای ایجاد اختلالات در جامعه نیاز دارد. علاوه بر این، سوء استفاده از داده های شخصی نشان دهنده نقض امنیتی این داده ها است که بر حریم خصوصی افراد و محرمانه بودن داده هایشان تأثیر مستقیمی دارد.

تا آنجا که به کمپین‌های اطلاع رسانی جعلی مربوط می‌شود، آنها از عناصری مانند اخبار جعلی برای تأثیرگذاری بر افکار عمومی استفاده می کنند. اینترنت و رسانه های اجتماعی تأثیرگذار، میزان نشر اطلاعات موجود را تقویت می‌کنند که این امر می‌تواند بر علیه اهدافی مانند سازمان‌های بین‌المللی، دولت‌ها، نهادهای سیاسی یا شخصیت‌های عمومی یا حتی انتخابات دموکراتیک مورد استفاده قرار بگیرد.

خرابکاری یا اقدامات شرورانه‌ای که بر عناصر فناوری تأثیر می‌گذارند.
اقداماتی که از فضای مجازی به عنوان یک ابزار برای اعمال غیرقانونی استفاده می کنند.

هکتیویسم	جرایم سایبری	تهدیدات دوگانه	جاسوسی سایبری
حملات سایبری	تروریسم سایبری	اعمال نظامی	تهدیدات پیشرفته مداوم
	جرائم سایبری	حملات سایبری	
		دستکاری در اطلاعات و پروژه‌ها	

بخش سوم

بخش سوم

پیشنهاد، اصول و اهداف امنیت سایبری

در این فصل اهداف و اصول حاکم بر استراتژی به اضافه یک هدف کلی و پنج هدف مشخص دیگر بیان شده است.

پیشنهاد

با توجه به تأسیس استراتژی امنیت ملی در سال ۲۰۱۷، اسپانیا باید توانایی‌اش در پیشگیری، شناسایی و پاسخ به حملات سایبری را تقویت و توسعه دهد و ایجاد برنامه‌های ویژه‌ای جهت ایجاد فضای مجازی امن و قابل اعتماد و نیز استفاده مسئولانه از شبکه و سیستم‌های اطلاعاتی را تضمین کند.

بنابراین، استراتژی امنیت سایبری ملی ۲۰۱۹ به طور کلی بخشنامه‌هایی در حوزه امنیت سایبری جهت دستیابی به اهداف استراتژیک امنیت سال ۲۰۱۷ را توضیح می‌دهد.

برای انجام این کار، اسپانیا باید به تقویت مهارت‌های مقابله با آسیب‌های سایبری و استفاده سوء از فضای مجازی ادامه دهد. بنابراین، در چارچوبی هماهنگ‌تر همراه با ساختارهای بهتر می‌توان تدابیری پیدا کرد که می‌توانند امنیت کشور را با توجه ویژه به بخش دولتی و خدمات تضمین کنند.

از سوی دیگر، ارتقای فرهنگ امنیت سایبری باید یکی از موضوعات اصلی در برنامه های توسعه کشور باشد تا جامعه را از این تهدیدها و چالش ها آگاه سازد. استفاده ایمن از فضای مجازی و کمک به ایجاد این وضعیت حق همه و مسئولیتی مشترک است.

علاوه بر این، امنیت سایبری به معنای پیشرفت است و حمایت و تشویق برای صنعت امنیت سایبری اسپانیا نیاز است تا بتوان محیطی برای پرورش توسعه و نوآوری ایجاد کرد. از طرف دیگر، جامعه ما دستیابی به دانش، مهارت ، تجربه و توانایی‌های فنی و حرفه‌ای را در اولویت خود قرار می‌دهد زیرا برای مقابله با چالش‌های اصلی امنیت سایبری ضروری هستند.

اصول حاکم

استراتژی امنیت سایبری ملی از اصول حاکم بر امنیت ملی الهام گرفته شده است: واحد اقدام، پیش بینی، کارآیی و تاب آوری.

۱) واحد اقدام: در صورت ایجاد هماهنگی و انسجام، واکنش نشان دادن به هر حادثه‌ای در زمینه امنیت سایبری که ممکن است بر عوامل مختلف دولت تاثیر بگذارد، امری پسندیده خواهد بود. این کیفیت‌ها را می توان با تهیه دقیق و سازماندهی مناسب اقدامات دولت به دست آورد. مدیریت بحران فضای مجازی به درک کامل تهدیدات کمک می کند و منابع موجود را با سرعت، کارآیی و انسجام بیشتری بررسی می‌کند.

۲) پیش بینی: ماهیت خاص فضای مجازی و عوامل درگیر در آن به سازوکارهایی در سازمان های تخصصی برای پیش بینی و هدایت اقدامات دولت در شرایط بحرانی نیاز دارد.

اصل پیش‌بینی، اقدامات پیشگیرانه را بر اقدامات واکنش‌ها مقدم می‌داند.

سیستم‌های تأثیر گذار با داشتن جدیدترین اطلاعات به اشتراک گذاشته شده می‌توانند اطلاعات خوبی از وضعیت ارائه می‌دهند. این فاکتور برای به حداقل رساندن زمان واکنش که یک عامل بسیار حیاتی، است بسیار مهم است.

۳) کارآیی: ایجاد امنیت سایبری مستلزم استفاده از سیستم‌های چندمنظوره با سطح بالایی از فناوری است که با نیازهای عظیم و هزینه‌های بسیار زیاد برای توسعه ، خرید و بهره‌برداری همراه است.

علاوه بر این، سناریوهای کنونی و آینده تحت تأثیر شرایط اقتصادی قرار دارند و این بدین معنی است که اسپانیا باید بر روی بهینه‌سازی منابع اختصاص داده شده به امنیت سایبری و داشتن توجه ویژه به واحد اقدام و اشتراک اطلاعات برنامه‌ریزی کند.

۴) تاب‌آوری: تاب‌آوری یک ویژگی اساسی سیستم‌ها و زیرساخت‌های حیاتی آنها است. دولت باید از بهبود عناصر موجود در کشور اطمینان حاصل کند. محافظت از آنها در برابر آسیب‌های مجازی نیاز به تقویت شبکه‌های اطلاعاتی و ارتباطی برای مقابله با اقدامات مخرب سایبری یا استفاده غیرقانونی از فضای مجازی دارد.

واحد اقدام: در صورت ایجاد هماهنگی و انسجام، واکنش نشان دادن به هرحادثه‌ای در زمینه امنیت سایبری که ممکن است بر عوامل مختلف دولت تأثیر بگذارد، امری درست خواهد بود. این کیفیت‌ها را می‌توان با تهیه دقیق و سازماندهی مناسب اقدامات دولت به دست آورد.

پیش‌بینی: ماهیت خاص فضای مجازی و عوامل درگیر در آن، به سازوکارهایی در سازمان‌های تخصصی برای پیش‌بینی و هدایت اقدامات

دولت در شرایط بحرانی نیاز دارد.

کارآیی: ایجاد امنیت سایبری مستلزم استفاده از سیستم‌های چندمنظوره با سطح بالایی از فناوری است که با نیازهای وسیع و هزینه‌های بسیار زیاد لازم برای توسعه، خرید و بهره‌برداری همراه است.

تاب‌آوری: تاب‌آوری یک ویژگی اساسی سیستم‌ها و زیرساخت‌های حیاتی آنها است. دولت باید از بهبود عناصر موجود در کشور اطمینان حاصل کند و از آنها در برابر آسیب‌های مجازی محافظت کند.

هدف کلی

چالش جدید امنیت سایبری به معنای یکپارچه کردن، فراگیرتر کردن و کاهش فنی بودن هدف کلی است.

بر اساس این هدف کلی، یک سری اهداف خاص در زیر توضیح داده شده اند تا اقدامات دولت در این زمینه را هدایت کند.

هدف اول

برای چنین هدفی باید یک چارچوب منسجم و یکپارچه برای تضمین حفاظت از اطلاعات اداره شده توسط بخش عمومی و خدمات ضروری، سیستم ها و خدمات آنها و همچنین شبکه‌هایی که از آنها پشتیبانی می کنند، برپا شود. این چارچوب همچنین توسعه بیشتر امنیت و خدمات کارآمد را فراهم می کند. اقدامات امنیتی باید با تمرکز بر بهبود پیشگیری، کشف و واکنش به حوادث، ایجاد راه‌حل‌های جدید، بهبود هماهنگی و متناسب سازی سیستم حقوقی انجام شود.

اقدامات ضدجاسوسی اینترنتی اهمیت بسیار بالایی دارند، زیرا این امر محافظت از میراث فناوری اسپانیا که به عنوان دارایی‌های مادی یا غیرمادی شناخته می‌شود را تضمین می‌کند و می‌تواند مالکیت معنوی و صنعتی بخش تجارت را حفظ کند.

بخش عمومی و اپراتورهای خدمات ضروری باید به روند بهبود کمک کنند تا از سیستم‌های فناوری اطلاعات و ارتباطات خود با نظارت دائمی بر تهدیدات موجود محافظت کنند. این عوامل باید به عنوان الگوی بهترین شیوه‌های مدیریت امنیت سایبری تعیین شوند.

طبق اصل مسئولیت مشترک، بخش دولتی باید با شرکت‌هایی که

سیستم‌های اطلاعاتی و ارتباطاتی را مدیریت می‌کنند، همکاری نزدیک و تبادل دانش داشته باشد و این امر موجب ایجاد هماهنگی و همکاری مناسب بین این دو در محیط سایبری می‌شود.

تقویت امنیت سایبری مستلزم داشتن روشی نظام‌مند در مورد تأثیرات احتمالی قطع یا تخریب شبکه‌ها و یا سیستم‌های ارائه دهنده خدمات اساسی می‌باشد که به تصمیم‌گیری مناسب با توجه به شرایط موجود کمک می‌کند.

هدف دوم

فضای مجازی می‌تواند در اعمال غیرقانونی و خدشه‌دار کردن اعتماد شهروندان نقش مهمی داشته باشد. تضمین محاکمه مناسب این جرائم امری ضروری است.

مبارزه با جرایم اینترنتی را می‌توان به سه زمینه تقسیم کرد:

(i) فضای مجازی به عنوان هدف مستقیم تهدیدها یا اعمال مجرمانه؛

(ii) فضای مجازی به عنوان رسانه اصلی برای ارتکاب جرم؛

(iii) فضای مجازی به عنوان هدف تحقیق مستقیم برای هر نوع رفتار غیرقانونی.

بر اساس مقررات سنگین که مبارزه با جرایم اینترنتی را تضمین می‌کنند، همکاری‌های حقوقی و پلیسی، چه در سطح ملی و چه در سطح بین‌المللی باید تقویت شوند و منابع کافی در این زمینه به نهادهای ذی‌صلاح اختصاص داده شود و مهارت‌های لازم به افراد متخصص در این زمینه آموزش داده شود.

بـه ایـن ترتیب، همکاری و مشـارکت شـهروندان باید تشـویق شـود؛ مراحل دسترسـی و انتقـال اطلاعاتـی که ممکن اسـت برای پلیس لازم باشـد بایسـتی تسـهیل شـوند و همچنیـن جنبـه‌هایی کـه در نهادهـای پلیس و سـازمان‌های قانونـی نیـاز به بهبود دارند، شناسـایی شـوند.

هدف سوم

حمایت از اکوسیستم تجاری و اجتماعی و شهروندان

همـه افـراد و سـازمان‌هـا حـق اسـتفاده ایمـن از فضـای مجـازی را دارنـد. بنابرایـن مسـئولیت دولت این اسـت کـه اقدامات لازم را برای دسـتیابی و حفظ امنیـت سـایبری، بـه ویژه محافظـت از آسـیب‌پذیرتریـن بخش‌هـای جامعه را تهیـه کـرده و امـکان توسـعه اقتصـاد اسـپانیا را فراهم کند.

امنیـت سـایبری مسـئولیتی اسـت کـه بـا عوامل خصوصی مشـترک اسـت و بـدون مشـارکت آنهـا امکان‌پذیر نیسـت. بنابرایـن، اقدامات لازم بـرای ارتقای همـکاری و تأمیـن امنیـت باید انجام شـود.

دفاع از شـهروندان، مشـاغل مسـتقل و شـرکت‌ها باید امری فراتر از محافظت از خـود دولـت باشـد، بنابراین توصیه می شـود تدابیری برای دفـاع الکترونیکی از آنهـا در فضـای مجـازی اعمـال شـود. همزمان، همـه کاربران فضـای مجازی باید از فناوری در دسـترس خود اسـتفاده مسـئولانه ای داشـته باشند.

اشـتیاق جامعـه بـه فنـاوری‌هـای نوظهـور باعث ایجاد ریسـک‌هایی می‌شـود. در نتیجـه، تبـادل مـداوم دانـش بـا همـه عوامـل و سـازوکارهای نظارتـی برای محافظـت از اکوسیسـتم تجاری و اجتماعـی، ابزاری برای اطلاع‌رسـانی دولت و کمـک در تصمیـم گیـری صحیح و بـه‌روزرسـانی و انطباق اقدامات انجام شـده خواهـد بود.

هدف چهارم

برای مقابله با چالش‌های امنیت سایبری، اسپانیا باید از منابع فنی و انسانی مناسبی برخوردار باشد تا بتواند استقلال فنی و مهارت‌های لازم را برای استفاده ایمن از فضای مجازی به منابع انسانی بدهد و امنیت سایبری را به عنوان یکی از اصلی‌ترین اهداف یک کشور کارآفرین قرار دهد.

برای انجام این کار، امنیت سایبری جمعی و فرهنگ امنیت سایبری باید با کمک سازمان‌های دولتی و خصوصی و همچنین رسانه‌ها گسترش یابد و در این مسیر مکانیسم‌های اطلاعاتی تقویت شوند و به شهروندان کمک شود تا از این طریق ارتباطات بین جامعه مدنی ، ادارات و شرکت‌ها بهبود یابند.

آموزش مهارت‌های مناسب در امنیت سایبری به متخصصان باعث تقویت مهارت‌های ویژه به علاوه تولید دانش و آموزش نحوه استفاده ایمن و مسئولانه از فناوری‌های اطلاعات و ارتباطات میشود. در این بین فعالیت‌های R + D + i در امنیت سایبری توسعه داده می‌شود و استفاده از محصولات و خدمات دارای مجوز تشویق می‌شوند.

علاوه بر این، باید به حفاظت از میراث فناوری و مالکیت صنعتی و معنوی نیز توجه ویژه‌ای شود. برای ارتقای حاکمیت دیجیتال و استفاده حداکثری از فرصت‌های ایجاد شده توسط تحول دیجیتال، صنعت امنیت سایبری اسپانیا باید با توسعه و اجرای سیستم‌های اطلاعاتی و ارتباطی تقویت شود.

هدف پنجم

اسپانیا فضای مجازی آزاد، امن و قابل اعتماد در رابطه دو جانبه خود با سازمان‌های چندجانبه، منطقه‌ای و بین‌المللی و در مجامع و کنفرانس‌ها

را ارتقا خواهد داد.

این طرح حامی ایجاد یک چارچوب بین‌المللی برای پیشگیری از منازعات، ایجاد همکاری و ثبات در فضای مجازی، استفاده از اصول منشور ملل متحد، حقوق بین الملل، حقوق بشر و حقوق بشردوستانه در جنگ می‌باشد.

سازمان ملل متحد که از اهمیت چندجانبه‌گرایی آگاه است، نقش مهمی در پیشبرد جامعه همراه با حفظ رویکرد هایی جهت افزایش اعتماد، همکاری و مشارکت بین همه عوامل درگیر (ایالات، بخش خصوصی، جامعه مدنی، کاربران و دانشگاه) دارد که می‌تواند باعث دستیابی امنیت و ثبات در فضای مجازی بشود.

این هدف که در راستای شرکای اروپایی ما نیز است، می‌تواند اعتماد به اینترنت، تحول دیجیتال و توسعه فناوری های جدید را تقویت می‌کند و به تحکیم یک اکوسیستم سایبرنتیک امن در اروپا کمک کرده تا باعث پیشرفت و گرایش به سمت بازار دیجیتال شود. این کار حامی ایجاد یک اینترنت آزاد است که بازتابی از کثرت فرهنگی و زبانی بین‌المللی می‌باشد و مبتنی بر سیستم حاکمیت دموکراتیک است. علاوه بر این، دسترسی به اینترنت جهانی و امکان نشر اطلاعات را نیز فراهم می‌کند و در نهایت به تحقق اهداف توسعه پایدار نیز کمک می‌کند.

به این ترتیب، متعلق بودن به اتحادیه اروپا (EU) بدان معنی است که ما باید امنیت و استقلال استراتژیک اروپا را نیز با همکاری‌های فنی، عملیاتی و استراتژیک تقویت کنیم. این همکاری به تقویت توانایی ما در پاسخگویی به بحران‌ها و پیشرفت در زمینه‌های مدنی و نظامی به عنوان یکی از هم‌پیمانان اتحادیه اروپا و متحدان سازمان پیمان آتلانتیک شمالی (ناتو) نیز کمک می‌کند.

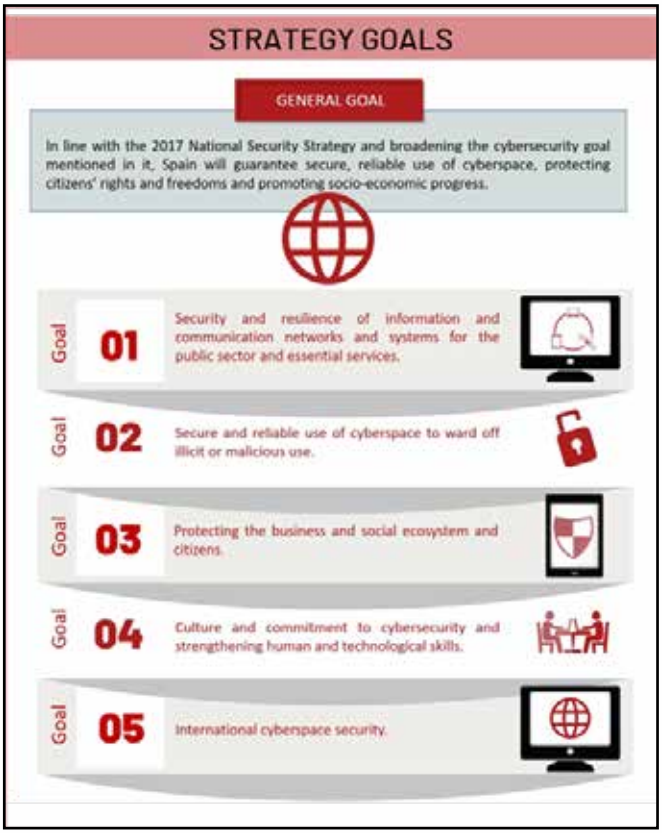
بـر اسـاس مـوارد فـوق، اسـپانیا به نقش فعال خـود در اتحادیه اروپـا و ناتو و سـازمان ملـل و در مجامع غیر اصلـی دیگر مانند :

- مجمـع حاکمیـت اینترنـت (IGF) و سـازمان امنیـت و همـکاری اروپـا (OSCE)؛
- اقداماتـش در توسـعه و ایجـاد اعتمـاد بـا سـازمان کشـورهای آمریکایـی (OAS) و مجمـع جهانـی تخصـص سـایبر (GFCE) ائتـلاف آنلایـن آزادی FOC و
- حضـورش در مرکـز تعالی اروپا برای مقابله با تهدیدهای ترکیبی (Hybrid CoE) مرکز تعالی سایبری دفاع الکترونیکی تعاونی ناتو (CCD CoE)

ادامه خواهد داد.

همچنین می تواند باعث:

- ایجـاد همـکاری هـای دو جانبـه بیـن المللـی در راسـتای ایجـاد امنیـت سـایبری، روابطـی روان و قابـل اعتمـاد ؛
- اقداماتی مشترک برای ایجاد مهارت در کشورهای شخص ثالث؛
- توجه ویژه به زنان و جوانان و
- ایجاد کانال های اطلاعاتی مخصوص برای تبادل تجربیات شود.



اهداف کلی

در راستای استراتژی امنیت ملی ۲۰۱۷ و پیشبرد اهداف امنیت سایبری ذکر شده در آن، اسپانیا استفاده ایمن و قابل اعتماد از فضای مجازی، حفاظت از حقوق و آزادی‌های شهروندان و پیشرفت اقتصادی-اجتماعی را تضمین می‌کند.

هـدف اول: امنیـت و حفـظ اطلاعـات و شـبکه‌هـای ارتباطاتی و سیسـتم‌هایی بـرای بخـش خصوصـی و فعالیت‌هـای‌ضروی

هـدف دوم: اسـتفاده ایمـن و قابـل اعتمـاد از فضای مجـازی بـرای جلوگیری از اسـتفاده‌هـای غیرقانونی و مشـکوک

هدف سوم: حفاظت از اکوسیستم‌های تجاری و اجتماعی و شهروندان

هـدف چهـارم: فرهنگ و تعهد نسـبت به امنیت سـایبری و تقویـت مهارت‌های انسانی و دیجیتالی

هدف پنجم: امنیت فضای سایبری بین‌المللی

بخش چهارم

بخش چهارم

طرح‌ها و اقدامات

این فصل طرح‌های لازم برای دستیابی به اهداف را تعیین می‌کند.

طرح اول

این اقدام با هدف I در استراتژی مطابقت دارد.

۱) گسترش و بهبود مهارت‌های لازم برای تشخیص و آنالیز فضای سایبری تا بتوان روش و منشأ حمله را شناسایی کرد. همچنین تهیه اطلاعات لازم برای حفاظت، انتساب و دفاع مؤثر.

۲) تشویق مراکز تعالی و امکانات تحقیقاتی به ایجاد همکاری بین یکدیگر جهت مقابله مؤثرتر با تهدیدات سایبری.

۳) تقویت شیوه انتشار و استفاده از بهترین استانداردها در امنیت سایبری.

۴) اطمینان از همکاری دیجیتال درعملیات‌ها در سازمان‌ها، شرکت‌ها و گروه‌های دارای مسئولیت امنیت سایبری

۵) تدوین و به‌روزرسانی استانداردها ، رویه‌ها و دستورالعمل ها برای پاسخگویی به حوادث مربوط به امنیت سایبری و مطمئن شدن از قرار دادن آن در سیستم امنیت ملی.

۶) تقویت قابلیت‌های دفاع سایبری و اطلاعات سایبری.

۷) مشارکت شرکت‌ها با هر بخش برای تبادل و تجزیه و تحلیل اطلاعات، و بررسی ریسک های ممکن و اقدامات لازم برای کاهش، مطابق با الزامات قانونی نظارت کننده بر آنها
۸) تقویت و پشتیبانی از تحولات در شبکه CSIRT اسپانیا.
۹) توسعه سیستم‌عامل‌های اطلاع‌رسان، تبادل اطلاعات و هماهنگی برای بهبود امنیت سایبری هر بخش.
۱۰) ایجاد ابزارهایی برای پیشگیری، کشف، واکنش و ارزیابی متمرکز بر مدیریت بحران درحوزه امنیت سایبری و در چارچوب امنیت ملی.
۱۱) تضمین هماهنگی، همکاری و تبادل اطلاعات حوادث سایبری بین بخش‌های دولتی، خصوصی و سازمان‌های بین‌المللی ذی‌صلاح.
۱۲) پیاده سازی اقدامات دفاع سایبری فعال در بخش دولتی جهت تقویت پاسخگویی.

طرح دوم

تضمین امنیت و حفظ دارایی‌های استراتژیک اسپانیا

اقدامات

۱) گسترش و تقویت قابلیت‌های پیشگیری، شناسایی، واکنش، بازیابی و مقاومت در برابر حملات سایبری علیه بخش‌های دولتی، خدمات ضروری و شرکت‌های استراتژیک
۲) تقویت استانداردهای حفاظت از زیرساخت‌های مهم، تقویت امنیت شبکه‌های اطلاعاتی و سیستم‌هایی که آنها را پشتیبانی می‌کنند.
۳) اطمینان از اجرای کامل چارچوب‌های امنیت ملی، سیستم محافظت از زیرساخت‌های حیاتی و انطباق و هماهنگی استاندارد حیاتی

حفاظت از زیرساخت ها و خدمات اساسی با تمرکز بر اولویت مبتنی بر ریسک(risk- based priority).

۴) تقویت پیامدها و اختیارات و نیز ایجاد زیرساخت‌های امنیت سایبری در مناطق خودمختار، شهرهای خودمختار، نهادهای محلی و سازمان‌های وابسته که برای بهبود امنیت سایبری ملی با ساختارهای ملی همکاری و هماهنگی خواهند داشت؛ البته در چارچوب صلاحیت‌شان.

۵) ایجاد مرکز عملیات امنیت سایبری اداره مرکزی اسپانیا که مهارت‌های پیشگیری، ردیابی و واکنش را تقویت کند و مراکز امنیت سایبری را در منطقه و محله توسعه دهد.

۶) تقویت زیرساخت‌ها و خدمات مخابراتی و سیستم‌های اطلاعاتی مشترک که بین دولت های عمومی نیز مشترک است، تقویت مهارت‌های امنیتی و تاب‌آوری آنها.

۷) تقویت سیستم اندازه‌گیری عوامل اصلی امنیت سایبری که به مقامات صالح اجازه می‌دهد تا سطح امنیتی و چگونگی تکامل آنها را تعیین کنند.

۸) متعهد کردن بخش دولتی و خصوصی برای پشتیبانی از زنجیره تأمین، به ویژه هنگامی که بر ارائه خدمات اساسی تأثیرگذار است.

۹) تهیه کاتالوگ محصولات و خدمات دارای مجوز ، جهت استفاده در فرایندهای پیمانکاری بخش دولتی و خدمات ضروری.

۱۰) تقویت ساختارهای امنیتی و ظرفیت‌های نظارتی برای سیستم‌های اطلاعاتی که از اطلاعات طبقه بندی شده استفاده می کنند.

۱۱) محافظت از زیرساخت های علمی - فنی منفرد و مراکز مرجع R + D + i.

طرح سوم

تقویت قابلیت‌های تحقیق و تعقیب جرایم اینترنتی، برای تضمین امنیت شهروندان و محافظت از حقوق و آزادی‌ها در فضای مجازی.

این اقدام با هدف II در استراتژی مطابقت دارد.

اقدامات

۱) تقویت چارچوب قانونی برای پاسخ مؤثر به جرایم اینترنتی در ارتباط با تعریف انواع جرایم و تنظیم اقدامات صحیح تحقیق.

۲) ارتقای همکاری و مشارکت شهروندان، ایجاد روش‌هایی برای تبادل و انتقال اطلاعاتی که ممکن است مورد توجه پلیس باشد و ارتقای فعالیت‌های لازم برای پیشگیری از جرایم اینترنتی با هدف شهروندان و شرکت‌ها.

۳) بهبود سطح تحقیقات و مهارت‌های پیگرد قانونی و در صورت لزوم، اقدام مجرمانه علیه جرایم اینترنتی.

۴) انتقال صلاحیت کیفری اطلاعات مربوط به حوادث امنیتی به سازمان‌های ذی‌صلاح، به ویژه هر کدام که بر خدمات اساسی و زیرساخت‌های مهم تأثیر می‌گذارد.

۵) ایجاد دسترسی به اطلاعات و منابع مادی که برای انجام اقدامات قانونی، استفاده بهتر از چارچوب قانونی و فنی مبارزه را تضمین می‌کند.

۶) دسترسی به اطلاعات و منابع مادی برای اپراتورهای حقوقی که استفاده بهتر از چارچوب حقوقی و فنی مبارزه با جرایم اینترنتی را تضمین می‌کنند و بهبود مهارت‌های آنها در تحقیق و قضاوت در اعمال غیرقانونی.

۷) ارتقای تبادل اطلاعات، تجربه و دانش در بین پرسنل دارای مسئولیت تحقیقات و پیگرد قانونی جرایم اینترنتی.

۸) اطمینـان از دسترسـی متخصصان حقوقی و نیروهـای امنیتی دولتی به منابـع انسـانی و مـادی و ارائه دانش لازم برای اسـتفاده بهینـه از چارچوب حقوقـی و فنـی به آنها.

۹) تقویـت هماهنگـی بیـن ارگان‌هـا و واحدهای مختلـف دارای صلاحیت در تحقیقات علیه جرایم اینترنتی و سایر استفاده‌های غیرقانونی از فضای مجازی.

۱۰) تقویت همکاری‌های حقوقی و پلیس بین‌المللی.

طرح چهارم

تقویت امنیت سایبری برای شهروندان و شرکت ها.

این طرح با هدف III در استراتژی مطابقت دارد.

اقدامات

۱) بـه شـهروندان و بخـش خصوصـی، خدمـات امنیـت سـایبری یکپارچه کـه کیفیـت خـوب و دسترسـی آسـان دارد بدهید تـا تقاضا بـرای خدمات بخـش تجـارت امنیت سـایبری افزایـش یابد.

۲) تقویـت امنیـت سـایبری در microSME ، SME و در میان کارگران با بیـان سیاسـت‌هـای عمومی به ویژه توسـعه تاب‌آوری در امنیت سـایبری.

۳) ارتقـای امنیـت سـایبری بـرای حفـظ حریـم خصوصـی و محافظـت از داده‌هـای شـخصی در چارچـوب حقـوق دیجیتـال شـهروندان و مطابـق با سیسـتم حقوقـی و حمایـت از «هویـت دیجیتال».

۴) ایجـاد راه هایـی بـرای ثبت سـریع و ایمن شـکایات در بخش خصوصی و شهروندان.

۵) افزایـش همـکاری بیـن عوامـل دولتی و خصوصـی ، به ویـژه ارتقای تعهد خدمـات اینترنـت و ارائـه‌دهنـدگان خدمـات دیجیتـال جهت بهبـود امنیت

سایبری. مقررات ملی در این زمینه تقویت خواهند شد و تدابیری برای دفاع آنلاین سایبری شهروندان و SME ها اعمال می‌شود.

۶) ایجاد مکانیزم‌هایی برای اندازه‌گیری و چگونگی مقابله با خطر انباشته شده، هم برای شهروندان و هم برای شرکت‌ها، جهت اولویت‌بندی اقدامات امنیت سایبری و اطلاع رسانی

۷) در بخش تجارت، تقویت و اجرای استانداردهای شناخته شده امنیت سایبری، همکاری با نهادهای استانداردسازی ملی و بین المللی، ایجاد، انتشار و استفاده از بهترین اقدامات امنیت سایبری از جمله چارچوب‌های مختلف صدور گواهینامه.

۸) تقویت سیستم‌های شناسایی الکترونیکی و خدمات الکترونیکی قابل اعتماد.

۹) ترویج ایجاد مجمع ملی امنیت سایبری که شامل نمایندگانی از جامعه مدنی، کارشناسان مستقل، بخش خصوصی، دانشگاه‌ها، انجمن‌ها، سازمان‌های غیرانتفاعی برای تقویت و ایجاد هم‌افزایی‌های عمومی و خصوصی، به ویژه تولید دانش در مورد فرصت و تهدیدها در فضای مجازی.

طرح پنجم

تقویت صنعت امنیت سایبری اسپانیا و ظرفیت آن در پرورش و حفظ استعدادها، برای تقویت استقلال دیجیتال

این طرح با هدف IV در استراتژی مطابقت دارد.

اقدامات

۱. تقویت برنامه‌های R + D + i در زمینه امنیت دیجیتال و امنیت

سایبری در SME ها، مشاغل، دانشگاه‌ها و مراکز تحقیقاتی، تسهیل دسترسی به برنامه‌های تشویقی ملی و بین‌المللی از طریق برنامه‌های نوین.

۲) احیای بخش خدمات صنعتی و امنیت سایبری، حمایت از نوآوری، سرمایه گذاری، بین المللی سازی و انتقال فناوری، به ویژه در microSME و SME.

۳) افزایش فعالیت‌های ملی برای تولید محصولات، خدمات و سیستم های امنیت به ویژه حمایت از هر کدام که منافع ملی را برای تقویت استقلال دیجیتال و مالکیت معنوی و صنعتی حمایت می‌کنند.

۴) ارتقای فعالیت‌های استانداردسازی و الزامات امنیت سایبری در محصولات و خدمات فناوری اطلاعات و ارتباطات، تسهیل دسترسی به محصولات و خدمات آنها ترویج ارزیابی‌ها و صدور گواهینامه و پشتیبانی از تهیه کاتالوگ‌ها.

۵) ایجاد و به روزرسانی چارچوب های شایستگی در امنیت سایبری که نیازهای بازار کار را برآورده می کنند.

۶) شناسایی نیازها و مهارت های حرفه ای لازم در امنیت سایبری و ارتقای همکاری بین مؤسسات آموزشی از طریق تقویت سیستم آموزشی، آموزش اشتغال و تحصیلات دانشگاهی، ارتقای اعتبارنامه‌های حرفه‌ای و سیستم‌های صدور گواهینامه.

۷) قرار دادن معیارهای حرفه‌ای امنیت سایبری در شرح مشاغل بخش دولتی.

۸) شناسایی، تشویق و حفظ استعدادها در حوزه امنیت سایبری.

۹) تقویت برنامه‌های خاص R + D + i در امنیت و دفاع سایبری.

طرح ششم

کمک به امنیت فضای مجازی در سطح بین‌المللی، ترویج فضای مجازی باز، امن و قابل اعتماد که از منافع ملی حمایت بکند

این طرح با هدف V در استراتژی مطابقت دارد.

اقدامات

۱) تقویت حضور اسپانیا در سازمان ها، کنفرانس‌ها و مجامع منطقه‌ای و بین‌المللی که به آنها تعلق دارد و امنیت سایبری بخشی از وظیفه آن ها است؛ در کنار حمایت و مشارکت فعالانه در ابتکارات مختلف، ایجاد هماهنگی بین موقعیت بخش‌های مختلف درگیر.

۲) در حوزه سازمان ملل متحد، ارتقای پیروی از منشور ملل متحد و اعمال و اجرای قوانین بین المللی و قوانین مربوط به رفتارهای مسئولانه. به همین ترتیب، اجرای اقدامات لازم جهت ایجاد اعتماد به نفس در فضای مجازی.

۳) تلاش برای پیدار کردن جنبه‌های مکمل و همکاری بین اتحادیه اروپا و ناتو با توسعه یک اکوسیستم امن اروپایی که پیشرفت و تحکیم بازار واحد و امنیت و استقلال استراتژیک اروپا را تشویق می‌کند.

۴) ارتقای گفتگوی دو جانبه و همکاری سایر کشورها و بهبود سیستم های تبادل اطلاعات و تجربیات و دستگاه‌های هشداردهنده اولیه برای مبارزه با تهدیدهای سایبری.

۵) ارتقاء مهارت های فن آوری و دسترسی به اینترنت در کشورهای شخص ثالث برای کمک به انطباق با اهداف توسعه پایدار.

۶) همکاری با کشورهای اطراف برای افزایش آگاهی در مورد تهدیدهای ترکیبی، کاهش تأثیرشان بر حاکمیت و یکپارچگی کشورمان.

طرح هفتم

ایجاد فرهنگ امنیت سایبری

۱) اقدامات مندرج در این طرح به برنامه فرهنگ امنیت ملی کمک کرده و هدف چهارم استراتژی را برآورده می کند.

اقدامات

۲) افزایش آگاهی شهروندان و شرکت‌ها با ارائه اطلاعات مفید و مناسب به ویژه برای کارگران و شرکت‌های کوچک و متوسط.

حمایت از اقداماتی که موجب افزایش مسئولیت پذیری و ایجاد تعهدات مشترک بین قسمت های مختلف جامعه می‌شوند.

۳) تقویت ابتکارات و برنامه‌های مربوط به سواد دیجیتال در امنیت سایبری

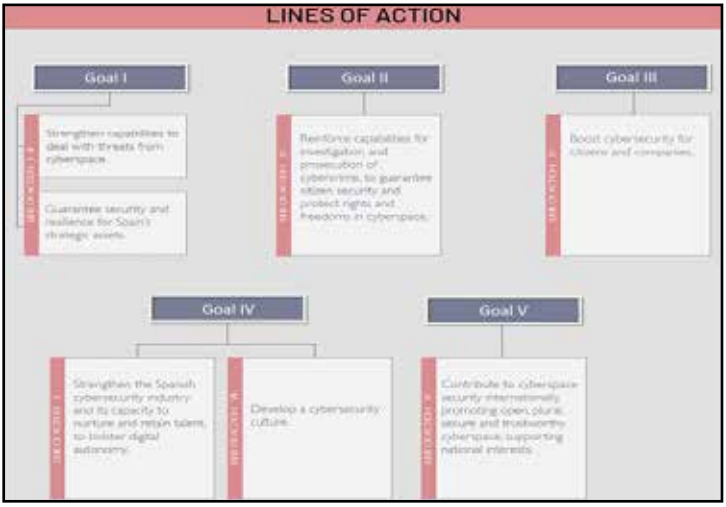
۴) ترویج فرهنگ امنیت سایبری به عنوان بهترین روش تجاری شرکت‌ها برای بهبود امنیت سایبری جمعی.

۵) تقویت روحیه انتقادی به نفع اطلاعات صحیح و کیفیت بالا که به شناسایی دقیق اخبار جعلی و اطلاعات غلط کمک می‌کند.

۶) آگاه کردن مدیران اجرایی سازمان‌ها تا بتوانند منابع لازم را به کار گرفته و پروژه‌های امنیت سایبری را طبق خواسته نهاد خود ارتقا دهند.

۷) ارتقای سطح آگاهی و آموزش در زمینه امنیت سایبری در مدارس، متناسب با سطح آموزشی هر مقطع.

۸) ایجاد همکاری و مشارکت با رسانه‌ها تا فعالیت‌های شهروندان، به ویژه جوانان افزایش یابد.



طرح ها

هدف اول: طرح ۱: تقویت توانایی ها برای مقابله با تهدیدات فضای مجازی
طرح ۲: تضمین امنیت دارایی های استراتژیک اسپانیا

هدف دوم: طرح ۳: تقویت قابلیت‌های تحقیق و تعقیب جرایم اینترنتی، برای‌تضمین امنیت شهروندان و محافظت از حقوق و آزادی‌ها در فضای مجازی.

هدف سوم: طرح ۴: تقویت امنیت سایبری برای شهروندان و شرکت‌ها.

هدف چهارم: طرح ۵: تقویت صنعت امنیت سایبری اسپانیا و ظرفیت آن در پرورش و حفظ استعدادها، برای تقویت استقلال دیجیتال.

هدف پنجم: طرح ۶: کمک به امنیت فضای مجازی در سطح بین المللی، ترویج فضای مجازی باز، امن و قابل اعتماد که از منافع ملی حمایت بکند.

هدف ششم: طرح ۷: ایجاد یک فرهنگ امنیت سایبری

بخش پنجم

بخش پنجم

امنیت سایبری در سیستم امنیت ملی

در این فصل چگونگی ادغام امنیت سایبری در سیستم امنیت ملی فعلی بررسی می‌شود.

استراتژی ملی امنیت سایبری ۲۰۱۳ و پس از آن تصویب قانون امنیت ملی در سال ۲۰۱۵، یک ساختار ارگانیک خاص برای امنیت سایبری ایجاد کرده‌اند. استراتژی ۲۰۱۹ ابتکاراتی را که مکمل پیشرفت بیشتر حاکمیت ملی با سیاست‌های اروپا است را تقویت می‌کند.

در سیستم امنیت ملی، ساختار امنیت سایبری شامل اجزای زیر است:

۱) شورای امنیت ملی

۲) کمیته ویژه تخصصی وضعیت برای کل سیستم امنیت ملی در شرایط بحرانی

۳) شورای امنیت سایبری ملی

۴) کمیته دائمی امنیت سایبری

۵) مجمع ملی امنیت سایبری

۶) مقامات ذی‌صلاح عمومی و CSIRT ملی

شورای امنیت ملی

شورای امنیت ملی، به‌عنوان کمیسیون تفویض شده دولت در موضوع امنیت ملی، ارگانی است که به نخست وزیر اسپانیا در مدیریت سیاست‌های امنیت ملی کمک می‌کند. شورای امنیت ملی از طریق اداره امنیت ملی به عنوان یک رابط ایجاد همکاری مرزی با سایر کشورها در اتحادیه اروپا را تضمین می‌کند.

کمیته وضعیت

فقط یک کمیته وضعیت برای کل شورای امنیت ملی وجود دارد که تحت حمایت وزارت امنیت ملی است و طبق دستورالعمل‌های سیاسی-استراتژیک دیکته شده توسط شورای امنیت ملی در مورد مدیریت بحران فعالیت می‌کند.

شورای امنیت سایبری ملی

شورای امنیت سایبری ملی به شورای امنیت ملی به ویژه به نخست وزیر اسپانیا در مدیریت و هماهنگی سیاست امنیت ملی و همچنین در زمینه امنیت سایبری کمک می‌کند تا وظایف خود را انجام دهد.

کمیته دائمی امنیت سایبری

کمیته دائمی امنیت سایبری برای سهولت هماهنگی بین وزارتخانه‌ها در سطح عملیاتی تشکیل شده است. این نهاد در جنبه های مربوط به ارزیابی فنی و عملیاتی خطرات و تهدیدهای امنیت سایبری به شورای امنیت سایبری ملی کمک می‌کند.

عملکـرد کمیسـیون در رونـد مدیریت بحـران قرار دارد. ایـن روش وظایف خـود را بـا هـدف شناسـایی و ارزیابـی خطـرات و تهدیدها مشـخص مـی‌کند. رونـد تصمیـم‌گیری را تسـهیل می کند و ارائه پاسـخی مناسـب و هماهنگ از طـرف دولـت را تضمین می‌کند. به‌علاوه، این شـامل سـطوح مختلف فعال‌سـازی سیسـتم امنیت ملـی در کنار ارائه دسـتورالعمل‌هایی بـرای مدیریت ارتباطات عمومـی اسـت. ایـن روش بـرای ارائـه یک پاسـخ مناسـب، با توجه به شـرایط موجـود، مهـارت ها و مسـئولیت هایش را بهبود می بخشـد.

مجمع ملی امنیت سایبری

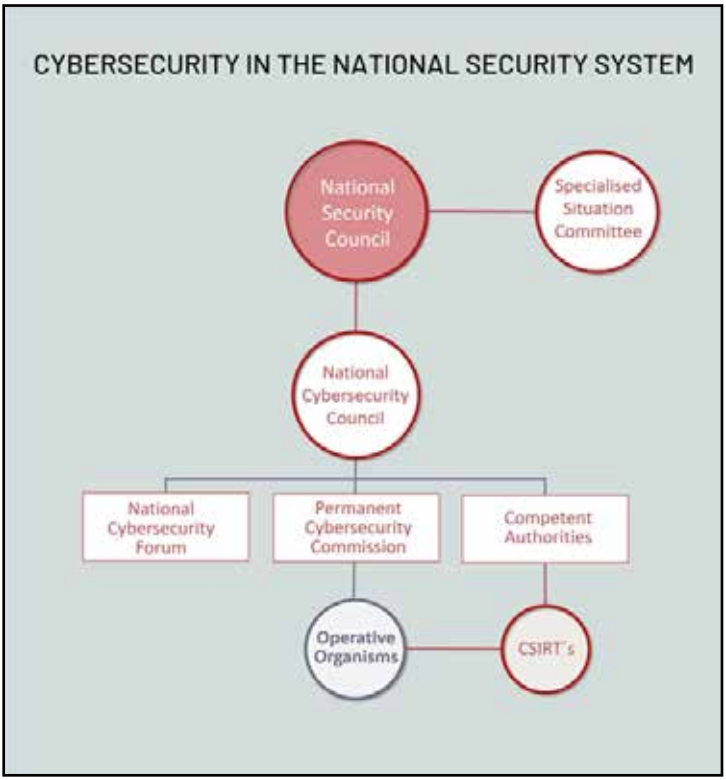
ایـن سـازمان در تقویـت و ایجـاد هـم افزایـی عمومی - خصوصـی، به ویژه تولیـد دانـش مربـوط بـه فرصت‌هـا، چالش‌هـا و تهدیدهای امنیتـی در فضای مجـازی، عمـل خواهد کرد.

ایجـاد مجمـع ملـی امنیت سـایبری و هماهنگی عملکـرد آن با ارگان‌های موجود، مسـتلزم تصویب مقرراتی بر اسـاس اسـتاندارد اسـت، به شـیوه‌ای که ایـن مؤلفـه‌ها مـی‌توانند در سیسـتم امنیت ملی کارا باشـند.

مقامات ذی‌صلاح عمومی و مرجع ملی CSIRT

چارچوب اسـتراتژیک و نهادی امنیت سـایبری توسـط مقامات ذی‌صلاح و CSIRT های ملی که در چارچوب قانونی ملی تدوین شده اند، تکمیل می شود.

عـلاوه بـر ایـن، CSIRT هـا از مناطـق خودمختار و شـهرهای خودمختار، از نهادهـای محلـی و نهادهای وابسـته، از نهادهای خصوصی، CSIRT شـبکه es و سـایر خدمـات امنیت سـایبری مربوطه، بسـته به صلاحیـت هرکدام باید با مـوارد فوق هماهنگ شـوند.



ملاحظات و ارزیابی نهایی

با تشکر از تجربه استراتژی ملی امنیت سایبری ۲۰۱۳، این سند می‌تواند تهدیدها و چالش‌های در حال تغییر را که با آن روبرو هستیم بیان کرده و به روز رسانی کند. برای انطباق با این سناریوی جدید، طرح‌ها به علاوه اقدامات پویاتر ارائه می‌شوند که در صورت لزوم به اکوسیستم امنیت سایبری ملی اجازه می دهد تا به سرعت، و بر اساس یک مدل

حکمرانی کاملاً بالغ که باید شامل مشارکت فعال بخش های خصوصی و بقیه جامعه مدنی باشد، سازگار شود.

از این نظر، این استراتژی به عنوان یک سند زنده است که باید با تغییرات تدریجی در امنیت سایبری سازگار شود، بنابراین باید به طور مداوم، همراه با برنامه‌های خاص به‌روزرسانی شود. گزارش ارزیابی سالانه در مورد استراتژی تهیه خواهد شد که نشان میدهد چه میزان از آن را دنبال کرده و اهداف آن را برآورده کرده است.

از طرف دیگر، با توجه به افزایش تهدیدات و چالش‌های امنیت سایبری که کشورهای پیرامون ما با آن روبرو هستند، داشتن تجهیزات اقتصادی، انسانی و مادی برای مقابله مؤثر با آنها ضروری است. یک اقدام ویژه در اینجا اطمینان حاصل کردن از مجهز کردن مرکز عملیات امنیت سایبری اداره مرکزی اسپانیا به شیوه‌ای مناسب و درخور است.

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