سند راهبردی پدافند سایبری کشور

کمیتـــهٔ دائمـــی (شـــورای‌عالی) پدافنـــد غیرعامل کشـــور در جلســـه مورخ ۲۹ /۰۲/ ۱۳۹۴ به استناد ماده (۸) اساسنامه سازمان پدافند غیرعامل کشور مصوّب مقـــام معظم رهبری و فرماندهی کل قوا (مدظله‌العالی)، « ســـند راهبردی پدافند سایبری کشور» پیشنهادی ســـازمان پدافند غیرعامل کشور، موضوع بند ۱ ماده ۹ اساسنامه مذکور را بررسی و به شرح زیر تصویب نمود:

ماده۱: تعاریف و اصطلاحات:

۱)**فضای سایبری:** به شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده (جاگذاری شده)، کنترل کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انســـان به‌منظور تولید، پردازش، ذخیره‌ســـازی، مبادله، بازیابـــی و بهره‌برداری از اطلاعات گفته می‌شـــود که ممکن اســـت در ارتباط مستقیم و مداوم با ســـامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی، در آن تعبیه شده باشد.

۲) **ســـرمایه ملی سایبری:** بخشی از دارایی‌های کشور اعم از زیرساخت‌ها، سامانه‌ها، تجهیزات، نرم‌افزارها، اطلاعات و حتی افراد که در فرآیند تولید، پردازش، ذخیره‌ســـازی، مبادله، بازیابی و بهره‌برداری از داده‌های دارای اهمیت حیاتی، حســـاس و مهم در فضای سایبری کشـــور نقش مســـتقیم و تعیین‌کننده داشته باشند، ســـرمایه ملی سایبری نامیده می‌شود.

۳)**آســـیب‌پذیری ســـایبری:** به ضعف، نقص و عیب موجود در داخل یک سرمایه ملی ســـایبری، رویه‌های امنیتی یا کنترل‌های داخلی، یا پیاده‌سازی آن سرمایه ملی سایبری، که قابلیت بهره‌برداری یا فعال شـــدن تهدیدات داخلی و خارجـــی به‌منظور تهاجم و یا جنگ سایبری را داشته باشد، اطلاق می‌گردد.

۴) تهدید سایبری: احتمال هرگونه رویدادی که قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر (پنداره) یا اشـــتهار دستگاه متولی ســـرمایه ملی سایبری یا افراد مرتبط، به‌واسطه یك سامانه اطلاعاتی، از طریق دسترســـی غیرمجاز، انهدام (تخریب)، افشاء، تغییراطلاعات و ایجاد اختلال یا ممانعت از ارائه خدمات را داشـــته باشد تهدید سایبری گفته می‌شود.

۵)تهاجم سایبری: به هرگونه اقدام غیرمجاز سایبری، که با هدف نقض سیاست امنیتی یك سرمایه سایبری و ایجاد خرابی یا خسارت، ایجاد اختلال در عملکرد یا از کاراندازی خدمات و یا دستیابی به اطلاعات انجام گیرد تهاجم سایبری گویند.

۶)جنگ ســـایبری: بالاترین سطح و پیچیده ترین نوع از تهاجم سایبری که توسط ارتش ســـایبری کشـــورهای مهاجم یا گروه‌های ســـازماندهی شـــده تحت حمایت دولت‌های متخاصم علیه منافع ملی کشورها انجام می‌شود جنگ سایبری است.

۷) زیســـت‌بوم سایبری: به محیط بومی متشـــکل از زیرساخت‌های فناوری‌اطلاعات، شـــبکه‌های ارتباطی، ســـامانه‌های رایانه‌ای که به‌صورت زنده و پویا با عوامل انسانی در تعامل می‌باشد زیست‌بوم سایبری گفته می‌شود.

۸)سامانه‌های پایه سایبری: مجموعه‌ای از سخت افزارها و نرم‌افزارهایی که در شکل‌گیری فضای سایبری نقش اساسی داشته و مبنای طراحی و اجرای سایر سامانه‌ها می‌باشند سامانه‌های پایه سایبری است.

۹) دیپلماسی پدافند ســـایبری: به دفاع حقوقی از منافع ملی، تعامل و تبادل اطلاعات در قالب پیمان‌های مشترک سایبری بین کشورها دیپلماسی پدافند سایبری گفته می‌شود.

۱۰)پدافند سایبری: مجموعه اقدامات سایبری و غیرسایبری است که توانمندی رصد، پایش، تشـــخیص تهدید، استخراج آســـیب‌پذیری، تجزیه و تحلیل میزان خطر، مدیریت و کنترل تهاجم ســـایبری، بازیابی اطلاعات و تولید قدرت پاسخ‌گویی به تهدید سایبری دشمن را ایجاد کند و موجب مصون‌سازی، کاهش‌آسیب‌پذیری و حفاظت از سرمایه‌های

ملی سایبری و زیست‌بوم سایبری کشور شود و با تولید بازدارندگی امکان تهاجم سایبری را از کلیه متخاصمین سلب نماید.

۱۱)نظام جامع بومی پدافند سایبری: نظامی است بومی، متشکل از زیر نظام‌های رصد، پایش، تشخیص، مدیریت و کنترل بهنگام، تولید و کنترل آمادگی، مدیریت بحران، دفاع حقوقی، منابع انسانی (آموزش، نیروی انسانی، مدیریت، مهارت، ساختار)، آموزش و فرهنگ‌سازی، صنعت سایبری، هشدار و اطلاع‌رسانی، حفاظت و امنیت درحوزهٔ پدافند سایبری که برای انجام مأموریت‌های پدافند سایبری کشور ایجاد می‌شود.

ماده ۲: چشم‌انداز پدافند سایبری کشور:

با یاری خداوند قادر متعال، جمهوری اسلامی ایران در افق ۱۴۰۴، کشوری است؛ دست یافته به زیست‌بوم ملی سایبری امن، مصون، پایدار در برابر تهدیدات و حملات سایبری دشمن و قدرت برتر پدافند سایبری و دارای جایگاهی ممتاز در بین کشورهای منطقه و برخوردار از:

۱)نظام جامع بومی پدافند سایبری هوشمند، پایدار و مقاوم، انحصاری، ابتکاری، لایه به لایه، شبکه‌ای، چابک و منعطف در سطوح ملی، دستگاهی و استانی

۲) نظام مدیریت و کنترل جامع و هوشمند با قابلیت رصد، پایش، تشخیص، هشدار و مدیریت و کنترل بهنگام صحنه عملیات پدافند سایبری

۳) مصونیت در زیرساخت‌های حیاتی، استحکام و پایداری در زیرساخت‌های حساس و امنیت و ایمنی در زیرساخت‌های مهم

۴) سرمایه‌های انسانی مؤمن، متعهد مجرب، آموزش دیده و متخصص در حوزهٔ پدافند سایبری و دارای تفکر بسیجی و روحیه جهادی

۵) نظام دیپلماسی پدافند سایبری فعال، متعامل، مشارکت‌جو و مدافع منافع ملی سایبری

۶) صنعت بومی پدافند سایبری روزآمد، رقابتی و پاسخ‌گو به تهدید، خوداتکا و اقتصادی در تولید سامانه‌های پایه پدافند سایبری با بهره‌گیری از ظرفیت‌های کشور

۷)استانداردها و الگوهای پدافند سایبری بومی، امن، پویا و روزآمد

۸)جایگاه ممتاز علمی و فناورانه در حوزهٔ پدافند سایبری منطقه

۹)توانمندی مدیریت بحران سایبری در راستای تداوم خدمات‌رسانی ضروری

۱۰) نظام نهادینه شـــده آموزش و فرهنگ‌ســـازی پدافند سایبری در متن فرهنگ عمومی و نظام آموزشی کشور

۱۱) مشارکت ظرفیت بخش‌های دولتی، غیردولتی، مردم نهاد و بسیج در پدافند سایبری

۱۲) نظام تولید، حفظ و ارتقاء آمادگی‌های پدافند سایبری در برابر تهدیدات

ماده ۳: ارزش‌های اساسی حاکم بر حوزهٔ پدافند سایبری کشور:

۱) خودباوری و خوداتکایی

۲) اعتمادسازی، اطمینان‌بخشی

۳) نوآوری و خلاقیت

۴) اخلاق اسلامی

۵) نفی سلطه دشمن

۶) فرهنگ و ارزش‌های اسلامی

۷) مدیریت جهادی

۸) تفکر و عمل بسیجی

ماده ۴: اصول حاکم بر حوزهٔ پدافند سایبری کشور:

۱) مصون‌سازی و پایداری

۲) وحدت مدیریت

۳) بازدارندگی

۴) حفظ آمادگی

۵) پیش‌بینی در تهدیدشناسی

۶) اقتصادی‌سازی (رعایت صرفه و صلاح)

۷) اشراف اطلاعاتی

۸) دیپلماسی فعال

۹) اقتدار درون‌زا

ماده ۵: رسالت پدافند سایبری کشور:

"پدافند سایبری از سرمایه‌های ملی سایبری و فضای سایبری کشور در برابر تهدیدات و حملات سایبری دشمن"قرارگاه پدافند سایبری کشور رسالت مصون‌سازی و پایدارسازی سامانه‌های سایبری کشور از طریق رصد، پایش و تشخیص تهدیدات، کشف، مدیریت و کنترل آسیب‌پذیری‌ها، اعلام هشدارهای لازم، اطمینان از پدافند سایبری، تدوین و انتشار نظامات (ملاحظات، مقررات، الزامات و اصول) پدافندی، آموزش و نهادینه‌سازی پدافند سایبری، مدیریت عملیات پدافند سایبری و دفاع حقوقی در برابر تهدیدات و حملات دشمن را بر عهده دارد.

ماده ۶: مأموریت‌های عمده قرارگاه پدافند سایبری کشور

۱) هدایت، راهبری، نظارت و هماهنگی فرماندهی عملیاتی پدافند سایبری از زیرساخت‌های اساسی کشور متناسب با سطح اهمیت آن‌ها (مصون‌سازی زیرساخت‌های حیاتی سایبری، مستحکم و پایدارسازی زیرساخت‌های حساس سایبری و ایمن‌سازی و کاهش آسیب‌پذیری زیرساخت‌های مهم سایبری کشور)

۲) رصد، پایش و تشخیص تهدیدات سایبری دشمن و هشدار و تعیین وضعیت آن

۳) هدایت و راهبری ایجاد توانمندی‌ها و ظرفیت‌های احتیاط راهبردی برترساز در حوزهٔ پدافند سایبری

۴) هدایت و راهبری پدافند سایبری هوشمند، چندلایه و اثربخش از سرمایه‌های سایبری کشور

۵) هدایت و راهبری کنترل عملیاتی پدافند سایبری در سطوح ملی، منطقه‌ای و دستگاهی

۶) هدایت و راهبری ایجاد و ارتقاء نظام جامع پدافند سایبری کشور

۷) هدایت و راهبری ایجاد و ارتقاء آمادگی پدافند سایبری در دستگاه‌های اجرایی ملی و استانی، بخش غیردولتی و آحاد جامعه

۸) هدایت و راهبری مصون‌سازی، پایدارسازی و استحکام زیست‌بوم سایبری و سرمایه‌های ملی سایبری کشور

۹) نظارت و حصول اطمینان از تولید و به‌کارگیری سامانه‌های پایه و اساسی پدافند سایبری کشور

۱۰) هدایت و راهبری جلب مشارکت ظرفیت‌های بخش‌های دولتی، غیردولتی، مردم و به ویژه بسیج در پدافند سایبری

۱۱) هدایت و راهبری ایجاد و ارتقاء ظرفیت‌های صنعت بومی دفاع سایبری کشور (دولتی و غیردولتی)

۱۲) نهادینه‌سازی اصول، الزامات و ملاحظات فنی پدافند سایبری در متن برنامه‌ها و طرح‌های توسعه سایبری کشور

۱۳) هدایت و راهبری توسعه و پایدارسازی معماری پدافند سایبری در زیرساخت‌های دارای اهمیت

۱۴) نهادینه‌سازی آموزه‌های پدافند سایبری در متن برنامه‌های آموزشی و فرهنگ‌سازی کشور در سطوح‌مختلف

۱۵) هدایت و راهبری ایجاد و ارتقاء نظام اطلاع‌رسانی و عملیات روانی در فضای سایبری در برابر دشمن

۱۶) هدایت و راهبری آموزش‌های تخصصی تربیت نیروی انسانی متخصص در حوزهٔ پدافند سایبری

۱۷) هدایت و راهبری تولید و مدیریت دانش در حوزهٔ پدافند سایبری

۱۸) هدایت و راهبری دیپلماسی پدافند سایبری

تبصره: قرارگاه پدافند سایبری مسؤولیت هر یک از دستگاه‌های اجرایی کشور مرتبط با اجرای مأموریت‌های مندرج در این ماده را حداکثر یک سال پس از ابلاغ سند با مشارکت و هماهنگی دستگاه مربوط تهیه و جهت تصویب به دبیرخانه کمیتهٔ دائمی ارائه نماید.

ماده ۷: اهداف کلان در افق چشم‌انداز پدافند سایبری کشور

۱) دستیابی به نظام جامع بومی پدافند سایبری

۲) دستیابی به زیرساخت‌ها و سرمایه‌های ملی مصون سایبری

۳) دستیابی به زیست‌بوم سایبری امن، مصون و پایدار

۴) دستیابی به منابع انسانی توانمند و کارآمد پدافند سایبری

۵) دستیابی به جایگاه ممتاز علمی و فناوری پدافند سایبری منطقه

۶) دستیابی به صنعت بومی خوداتکا و پیشرفته پدافند سایبری

۷) دستیابی به استانداردها و الگوهای پدافند سایبری بومی، امن، پویا و روزآمد

۸) دستیابی به دیپلماسی فعال پدافند سایبری

۹) دستیابی به ظرفیت مناسب فرماندهی و کنترل پدافند سایبری

۱۰) نهادینه‌سازی فرهنگ، ادبیات و آموزه‌های پدافند سایبری

۱۱) دستیابی به مشارکت ظرفیت‌های بخش‌های دولتی و غیردولتی در حوزهٔ پدافند سایبری

۱۲) حفظ و ارتقاء آمادگی‌های پدافندی سایبری در برابر تهدیدات

ماده ۸: راهبردهای پدافند سایبری کشور

۱) طراحی، پیاده‌سازی و راهبری نظام جامع بومی پدافند سایبری هوشمند، پایدار و مقاوم، انحصاری، ابتکاری، لایه به لایه، پیش‌گیرانه، شبکه‌ای، چابک و منعطف در سطوح ملی، دستگاهی و استانی

۲) طراحی، پیاده‌سازی و راهبری طرح‌ها و برنامه‌های پدافند سایبری از زیرساخت‌های کشور برای مصون‌سازی زیست‌بوم سایبری دربرابر تهدیدات و تهاجم سایبری متناسب با سطح اهمیت آن‌ها.

۳) الزام و همراه سازی سازمان‌های متولی زیرساخت‌های حیاتی و حساس کشور در استفاده از محصولات سایبری امن بومی.

۴) به‌کارگیری منابع انسانی متخصص و امین با ساماندهی و ارتقای کمی و کیفی درحوزهٔ پدافندسایبری.

۵) تولید و مدیریت دانش و فناوری پدافند سایبری متناسب با تهدیدات.

۶) بومی و امن سازی سامانه‌های سایبری مورد استفاده در زیرساخت‌های حیاتی و حساس کشور با تأکید بر ممنوعیت کاربرد سامانه‌های خارجی در آن‌ها (در جهت کاهش وابستگی به فناوری‌ها و محصولات غیربومی).

۷) ساماندهی و تقویت صنعت پدافند سایبری بومی و حمایت از سازمان‌ها و شرکت‌های تولیدکننده دولتی و غیردولتی و محصولات بومی و روزآمد.

۸) سازماندهی، حمایت و صیانت از تولید امن داخلی سامانه‌های پایه و اساسی پدافند سایبری کشور.

۹) بومی‌سازی فرآیندها، نظام‌ها و استانداردها، پروتکل‌های فنی، رویه‌ها و روال‌های پدافند سایبری.

۱۰) طراحی، پیاده‌سازی و راهبری نظام دیپلماسی پدافند سایبری کشور.

۱۱) طراحی، پیاده‌سازی و راهبری سامانه فرماندهی و کنترل پدافند سایبری.

۱۲) فرهنگ‌سازی و آموزش تخصصی و عمومی مسؤولین و نخبگان و آحاد جامعه در حوزهٔ پدافند سایبری.

۱۳) نهادینه‌سازی آموزه‌های پدافند سایبری در نظام آموزشی(ابتدایی، متوسطه و دانشگاهی) و نظام آموزش دفاعی کشور.

۱۴) بهره‌گیری از قابلیت‌های سازمان بسیج مستضعفین و سازمان‌های مردم نهاد و ظرفیت‌های بخش غیردولتی در پدافند سایبری.

۱۵) مدیریت بر ارتقاء ضریب پایداری، مصون‌سازی، ارتقاء توان بازدارندگی زیرساخت‌های حیاتی و حساس کشور در برابر تهدیدات و حملات سایبری.

۱۶) حفاظت و تأمین امنیت هوشمندانه سایبری از زیرساخت‌ها و طرح‌ها متناسب با سطح اهمیت آن‌ها.

۱۷) استفاده هوشمندانه (توجه به فرصت‌ها و تهدیدات فناوری‌ها) از سامانه‌های جدید سایبری در زیرساخت‌های دارای اهمیت.

۱۸) مشارکت در تدوین راهبردها علیه تهدیدات مشترک نظامی و سایبری .

۱۹) راهبـــری، هدایت، ایجـــاد هماهنگی و هم‌افزایی راهبرد محور پدافند ســـایبری در کلیه دستگاه‌های اجرایی.

۲۰) طراحی و پیاده‌سازی و راهبری نظام جامع رصد، پایش، تشخیص و هشدار در مقابل تهدیدات سایبری دشمن.

این ســـند که در هشـــت ماده و نود بند و یک تبصره درجلسه مورخ ۱۳۹۴/۰۲/۲۹ کمیتهٔ دائمی بررســـی و به تصویب رسیده به اســـتناد تبصره ۱ ماده ۹ اساسنامه سازمان پدافند غیرعامل کشـــور مصوب مقام معظم رهبـــری و فرماندهی کل قوا (مدظله‌العالی) جهت اجرا ابلاغ می‌گردد.

*** مصوّبهٔ مذکور طی شمارهٔ ۱۶۰/۱/۵۸۵ مورخ ۱۳۹۴/۰۳/۲۱ با امضای رئیس ستاد کل نیروهای مســـــلح و رئیس کمیتهٔ دائمی پدافند غیرعامل (سرلشکر بسیجی دکتر سید حسن فیروزآبادی) به دستگاه‌های اجرایی برای اقدام، ابلاغ شده است.**