جمهوری اسلامی ایران

فرماندهی کل قوا

کمیته دائمی پدافند غیرعامل کشور

شماره: ۱/۳۱۸۱/ک ۱۶۰
تاریخ: ۱۴۰۴/۱۱/۲۷
پیوست: ندارد

بسم الله الرحمن الرحیم

مقام معظم رهبری و فرمانده کل قوا (مدظله العالی):

« در مقابل شیوه‌های پیچیده دشمنان، پدافند غیرعامل باید کامل هوشیار و جدی باشد و به صورت علمی، دقیق، به روز و همه جانبه عمل و با هرگونه نفوذ مقابله کند. »

« کارگروه (کمیته) دائمی پدافند غیرعامل کشور به ریاست رئیس ستاد کل نیروهای مسلح بالاترین مرجع تصمیم گیری در حوزه پدافند غیرعامل کشور است که تصمیمات آن با ابلاغ رئیس کارگروه مزبور، برای همه دستگاه‌های لشکری، کشوری، بخش دولتی و عمومی غیردولتی لازم الاجراست. . . . » قانون تشکیل سازمان پدافند غیرعامل کشور (۱۴۰۲/۰۶/۱۲)

تصویب‌نامه

"با صلوات بر محمد و آل محمد و احترام"

کلیه دستگاه‌های اجرایی
(موضوع ماده ۵ قانون مدیریت خدمات کشوری و موضوع ماده۲۹ قانون برنامه پنج‌ساله ششم توسعه کشور)
ستاد کل نیروهای مسلح- ارتش ج.ا. ایران- سپاه پاسداران انقلاب اسلامی- فرماندهی انتظامی ج.ا. ایران
سازمان پدافند غیرعامل کشور

به استناد تبصره۱ قانون تشکیل سازمان پدافند غیرعامل کشور- مصوب مجلس شورای اسلامی- یکصدویکمین جلسه کارگروه دائمی پدافند غیرعامل کشور در تاریخ ۱۴۰۴/۰۸/۲۵ تشکیل گردید و در اجرای ماده۵ مصوبه ۸۴۶ کمیته دائمی[1]، پیشنهاد سازمان پدافند غیرعامل کشور در بازنگری سند راهبردی پدافند غیرعامل الکترونیک کشور را بررسی و به‌شرح زیر تصویب نمود:

سند راهبردی پدافند غیرعامل الکترونیک کشور
(ملاحظات عملیاتی، اقدامات اساسی، وظایف دستگاه‌های اجرایی)

مقدمه

امروزه درصد چشمگیری از زیرساخت‌های کشور وابسته به حوزه الکترونیک، مشتمل بر سخت‌افزارهای الکترونیک و همچنین طیف الکترومغناطیس و تجهیزات مرتبط به آن است. تجهیزات الکترونیک شامل تراشه‌های میکروالکترونیک، الکترونیک صنعتی، مکاترونیک و روبات‌ها، ماهواره‌ها، حسگرهای الکترونیکی حساس به مواد شیمیایی، پرتویی، بیولوژیکی، زیستی و متالوژی و حساس به پالس‌های الکترومغناطیسی مانند پالس‌های راداری و امواج حاصل از انواع فرستنده‌های مخابراتی و سیگنال‌های انتشاری در جنگ الکترونیک و در عرصه‌های جغرافیایی زمینی، دریایی، هوایی و فضایی، نقش بسزایی ایفاء می‌کند. حوزه الکترومغناطیس در جنگ الکترونیک باعث ایجاد فرصت در طراحی و ساخت سامانه‌های تشخیص و مقابله با تهدیدات الکترونیکی مانند ریزپرنده‌ها و ایجاد تهدیداتی مانند بمب‌های الکترومغناطیس، HPM[2] و حملات EMP[3] توسط دشمن علیه سرمایه‌های الکترونیک کشور می‌شود.

[1] ماده۵- مصوبه ۸۴۶ کمیته دائمی: این سند تا زمانی که سند دیگری جایگزین آن نشده، معتبر بوده و هر سه سال یک بار، بازنگری یا تمدید خواهد شد.
[2] Hight power Microwave [3] Electro Magnetic Pulse

وقوع این تهدیدات در اکثر صنایع الکترونیک و وابسته به آن در جنگ ۱۲روزه با رژیم صهیونیستی نشان داد که امروزه این‌گونه حملات و تهدیدها با هدف اثرگذاری مستقیم بر مردم قابلیت تبدیل به یک جنگ عمده زیرساختی را داشته و می‌تواند ضمن ایجاد خسارات مالی و جانی، پیامدهای گسترده‌ای را نیز به همراه داشته باشد. بنابراین آمادگی دستگاه‌های اجرایی و زیرساخت‌های با اهمیت بالای کشور در مقابله با تهدیدات احتمالی و به حداقل رساندن پیامدهای آن، امری اجتناب ناپذیر می‌باشد.

ماده ۱ – تعاریف و اختصارات

۱) **کارگروه دائمی:** کارگروه(کمیته) دائمی پدافند غیرعامل کشور،

۲) **سازمان:** سازمان پدافند غیرعامل کشور،

۳) **قانون تشکیل:** قانون تشکیل سازمان پدافند غیرعامل کشور مصوب شهریورماه ۱۴۰۲،

۴) **اساسنامه:** اساسنامه سازمان پدافند غیرعامل کشور،مصوب مقام معظم رهبری(مدظله‌العالی) موضوع ابلاغیه شماره ۲۶۱۲/۱/۱۲۷/۹۵ مورخ ۱۴۰۳/۱۰/۱۹ رئیس ستاد کل نیروهای مسلح،

۵) **دستگاه اجرایی:** کلیه دستگاه‌های اجرایی موضوع مادهٔ ۵ قانون مدیریت خدمات کشوری و مادهٔ ۲۹ قانون برنامهٔ پنج ساله ششم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران،

۶) **قرارگاه:** قرارگاه پدافند غیرعامل الکترونیک کشور،

۷) **حوزه الکترونیک:** مجموعه‌ای است از تجهیزات و امکانات الکتریکی و الکترونیکی که به صورت مجزا یا ترکیبی، یکپارچه و منسجم در زیرساخت‌های کشور مورد استفاده قرار می‌گیرند و می‌توانند تولید طیف الکترومغناطیس و همچنین قابلیت ارسال و دریافت اطلاعات در فضای الکترومغناطیس را نیز داشته باشند.

حوزه اصلی الکترونیک شامل ۱۰ حوزه تخصصی زیر است:

۷-۱- **حوزه الکترومغناطیس:** مجموعه‌ای است از امواج در کلیه باندهای فرکانسی مشتمل بر امواج رادیویی (سلولی، ماهواره‌ای، نوری و سایر) و پالس‌های راداری با فازها و دامنه‌های مختلف اطلاق می‌شود که به صورت مجزا یا ترکیبی به صورت یکپارچه و منسجم در زیرساخت‌های کشور مورد استفاده قرار می‌گیرند.

۷-۲- **حوزه سایبرالکترومغناطیس:** به مجموعه‌ای از تجهیزات و امکانات الکترونیکی سخت‌افزاری و نرم‌افزاری اطلاق می‌شود که به‌صورت ترکیبی، یکپارچه و منسجم در زیرساخت‌های کشور مبتنی بر طیف الکترومغناطیس در کلیه باندهای فرکانسی مورد استفاده قرار می‌گیرد که برای آلوده‌سازی تجهیزات الکترونیک از طریق امواج نیز استفاده می‌شود.

۷-۳- **حوزه مکاترونیک:** ترکیبی از مکانیک و الکترونیک است و مشتمل بر روبات‌های هوایی (پهپادها و ریزپرنده‌ها)، زمینی (خپهادها)، دریایی (شهپادها) و زیرسطحی (زهپادها) و همچنین حوزه اتوماسیون صنعتی، میکروالکترومکانیک، نانوالکترومکانیک، بیومکاترونیک (استفاده از تراشه‌ها در بدن)، حسگرها و سنجنده‌های الکترونیک اینترنت اشیاء و انواع سنجنده‌های شیمیایی، بیولوژیکی، هسته‌ای، گرمایی، رطوبتی و سنجنده‌های حوزه سلامت و محیط زیست که از تراشه‌های الکترونیک استفاده می‌کنند، می‌باشد.

۷-۴- **حوزه میکروالکترونیک:** مجموعه‌ای است از فن‌آوری‌های تولید تراشه‌های الکترونیک مشتمل بر سخت‌افزار و نرم‌افزار که به‌صورت مجزا و یا ترکیبی، یکپارچه و منسجم در تجهیزات حوزه الکترونیک مورد استفاده قرار گیرد، حوزه نانوالکترونیک نیز در راستای این موضوع تعریف می‌شود.

CPU[۲]، GPU، TPU و QPU از جمله تراشه‌های مهم هستند که به عنوان بستر پردازشی هوش‌مصنوعی استفاده می‌شوند.

۷-۵- **حوزه بیوالکترومغناطیس:** مجموعه‌ای از تجهیزات و امکانات الکترونیکی سخت‌افزاری و نرم‌افزاری هستند که به‌صورت ترکیبی، یکپارچه و منسجم در زیرساخت‌ها با محوریت طیف الکترومغناطیس و اثر آن بر بافت‌های بدن انسان و کلیه موجودات زنده، در زیرساخت‌های حوزه سلامت، بیولوژیک و پزشکی مورد توجه می‌باشند.

۷-۶- **حوزه ژئوالکترومغناطیس:** مجموعه‌ای از تجهیزات و امکانات الکترونیکی سخت‌افزاری و نرم‌افزاری هستند که به‌صورت ترکیبی، یکپارچه و منسجم در زیرساخت‌ها با محوریت طیف الکترومغناطیس بر اقلیم و فضای مرتبط با آن، تأثیرگذار است.

۷-۷- **حوزه سایبرالکترونیک:** مجموعه‌ای از تجهیزات و امکانات الکترونیکی سخت‌افزاری و نرم‌افزاری هستند که به صورت ترکیبی، یکپارچه و منسجم مبتنی بر فن‌آوری میکروالکترونیک و نانوالکترونیک است و می‌تواند در آلوده‌سازی تراشه‌ها و سخت‌افزارهای الکترونیک در زمان تولید تراشه یا خرابکاری الکترونیک در زمان توزیع آن، تهدیدی علیه زیرساخت‌های کشور تأثیرگذار باشد.

۷-۸- **حوزه اپتیک و لیزر:** مجموعه‌ای است از تجهیزات و امکانات نوری و اپتیکی، مادون قرمز، لیزری، فوتونیک متشکل از سخت‌افزار و نرم‌افزار که به صورت ترکیبی، یکپارچه و منسجم با هدف تصویربرداری، ارتباطات نوری، فعالیت‌های لیزری و انرژی مستقیم با کاربرد جنگ الکترونیک مورد استفاده قرار می‌گیرند.

۷-۹- **حوزه آکوستیک:** مجموعه‌ای است از امواج مکانیکی با بسامدهای مختلف در محیط گازها، مایعات و جامدات اطلاق می‌شود که در باندهای فروصوت و فراصوت با توجه به اثر آن بر روی جانداران و انسان‌ها، تجهیزات الکترونیک و اقلیم به صورت مجزا و یا ترکیبی به صورت یکپارچه و منسجم به صورت فرصت و تهدید مورد توجه قرار می‌گیرند.

۷-۱۰- **ماهواره:** سازه‌ای فضا پایه متشکل از تجهیزات و امکانات الکترونیکی سخت‌افزاری و نرم‌افزاری است که حول محور یک ستاره یا سیاره در مدارات مختلف گردش می‌کند و به صورت منفرد یا منظومه با هدف سنجش از راه دور، ارتباطات مخابراتی و تصویری، ارتباطات اینترنتی، ناوبری و موقعیت‌یابی، جاسوسی، عملیات جنگ الکترونیک و سایر فعالیت می‌کند.

۸) **پدافند غیرعامل الکترونیک:** به مجموعه اقدامات پیشگیرانه در حوزه‌های ۱۰گانه الکترونیک اطلاق می‌گردد که هدف آن‌ها مصونیت، استفاده پایدار و مداوم از سرمایه‌های الکترونیک کشور و تسهیل مدیریت بحران و هدایت عملیات تخصصی این حوزه در برابر تهدیدات دشمن می‌باشد.

۹) **تهدیدات الکترونیکی:** هر گونه عاملی که قابلیت وارد نمودن ضربه به سرمایه‌های ملی الکترونیکی (انسانی یا تجهیزات) به واسطه سامانه‌ها، تجهیزات و امکانات الکتریکی و الکترونیکی به صورت مجزا یا ترکیبی، از طریق تخریب(انهدام)، فریب یا افشاء و ایجاد اختلال یا ممانعت از ارائه خدمات را داشته باشد، تهدید الکترونیکی

[۲] Central Processing Unit, Graphic Processing Unit, Tensor Processing Unit, Quantum Processing Unit

گفته می‌شود. تهدیدات الکترونیکی می‌تواند از طرف دولت یک کشور، سازمان‌های غیردولتی اعم از رسمی و غیررسمی، مشروع و غیرمشروع، گروه‌های کوچک و افراد حقیقی انجام شود.

۱۰)**مخاطرات الکترونیکی:** به اندرکنش تهدیدات با آسیب‌پذیری‌ها و احتمال وقوع و شدت پیامد آنها با منشاء دشمن در حوزه الکترونیک یا ترکیبی با سایر حوزه‌ها که با هدف ضربه‌زدن به امنیت ملی کشور باشد، اطلاق می‌گردد.

۱۱)**سرمایه الکترونیکی:** بخشی از دارایی‌های کشور اعم از زیرساخت‌ها، سامانه‌ها، تجهیزات، نرم‌افزارها، اطلاعات و حتی افراد که در فرآیند تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از داده‌های دارای اهمیت حیاتی، حساس و مهم در حوزه الکترونیک نقش مستقیم و تعیین کننده داشته باشند، سرمایه الکترونیکی نامیده می‌شود.

۱۲)**جنگ الکترونیک:** مجموعه اقدامات پدافند الکترونیک، پشتیبانی الکترونیک و آفند الکترونیک می‌باشد که باعث افزایش توانمندی‌های دفاعی کشور در نیل به اهداف نظامی در سطوح تاکتیکی، عملیاتی و راهبردی شده و درصدد مقابله با تهدیدات الکترونیکی در پشتیبانی از انواع عملیات با رویکرد تسلط عملیاتی علیه دارایی‌های دشمن از قبیل تأسیسات، تجهیزات، جنگ‌افزارها، سکوها و افراد می‌شود.

۱۳)**زیرساخت الکترونیکی:** به مجموعه‌ای از مراکز و بخش‌های فعال اعم از تجهیزات، امکانات و دارایی‌ها در بخش‌های مختلف از قبیل مخابرات و ارتباطات، ماهواره‌ها، برق و سایر صنایع مانند آن اطلاق می‌شود که علاوه بر وابستگی کارکردی آنها به حوزه الکترونیک، کالا یا خدمات در حوزه‌های ۱۰گانه را ارائه می‌کنند.

۱۴)**خرابکاری الکترونیک:** به اقدامات خرابکاری از قبیل قراردادن کاشته‌های انفجاری قابل کنترل از طریق داده و سیگنال، تبدیل دارایی به سلاح از طریق اقدامات الکترونیک و الکترومغناطیس، قرار دادن کاشته‌های سخت‌افزاری آلوده‌شده، قراردادن کاشته‌های سخت‌افزاری در سطح میکروالکترونیک و نانوالکترونیک، تروجان‌های سخت‌افزاری و درب‌های پشتی تعبیه شده در تراشه‌های الکترونیک در زنجیره تولید، تأمین و توزیع گفته می‌شود.

۱۵)**مرکز عملیات پدافند غیرعامل الکترونیک**(EDOC[۴]): مرکز رصد، پایش و تشخیص تهدیدات الکترونیک حوزه کشوری وابسته به سازمان و در تابعیت رئیس ستاد کل نیروهای مسلح است که با راهبری قرارگاه پدافند غیرعامل الکترونیک کشور ایفای نقش می‌کند.

ماده ۲ – هدف

هدف از تدوین سند عبارت است از تدوین چارچوب معین برای فعالیت‌های پدافند غیرعامل الکترونیک در برابر تهدیدات الکترونیک دشمن و تعیین اهداف، راهبردها، اقدامات اساسی و تقسیم کار بین دستگاهی در حوزه دستگاه‌های اجرایی موضوع قانون تشکیل سازمان.

ماده ۳ – منظورها

۱)آسیب‌شناسی وضع موجود دستگاه‌ها و زیرساخت‌های با اهمیت بالای حوزه الکترونیک کشور و کاهش آنها؛

۲)شناخت تهدیدات، راهبردها، راهکنش‌ها(تاکتیک‌ها)، فناوری‌های تهدیدزای دشمن در حوزه الکترونیک؛

۳)ارتقاء آمادگی‌های عملیاتی پدافند غیرعامل الکترونیک در زیرساخت‌های مرتبط با آموزش و رزمایش؛

۴)تعیین و الویت‌بندی اهداف و راهبردهای پدافندی در حوزه الکترونیک کشور و هدایت و راهبری اجرای آنها؛

---

۴ Electronic "Passive" Defense Operatoin Center

۵)تدوین طرح‌های اقدام، دستورالعمل‌ها، آیین‌نامه‌ها و استانداردهای عملیاتی و فنی حوزه پدافند غیرعامل الکترونیک؛

۶)تعیین نظامات و رویکردهای عملیاتی پدافند غیرعامل الکترونیک در برابر تهدیدات الکترونیک دشمن؛

۷)ایجاد همسویی و هم افزایی اقدامات در حوزه پدافند غیرعامل الکترونیک با حوزه پدافند عامل الکترونیک در برابر تهدیدات الکترونیک.

مـاده ۴ - اسناد بالادستی

۱) سیاست‌های کلی نظام ابلاغی مقام معظم رهبری در حوزه پدافند غیرعامل و حوزه خودکفایی دفاعی و امنیتی؛

۲) قانون تشکیل سازمان پدافند غیرعامل کشور - مصوب ۱۴۰۲/۰۵/۳۰؛

۳) قانون برنامه پنج‌ساله هفتم توسعه جمهوری اسلامی ایران و سیاست‌های کلان مرتبط با آن؛

۴) اساسنامه سازمان پدافند غیرعامل کشور؛

۵) مصوبات کمیته دائمی شامل اسناد مصوب، نظامات عملیاتی و دستورالعمل‌های مرتبط؛

۶) مصوبات مرتبط از شورای عالی فضای مجازی.

ماده ۵- حوزه شمول

حوزه شمول این سند، دستگاه‌ها و مراکز دارای زیرساخت‌های با اهمیت بالای حوزه الکترونیک در همه دستگاه‌های اجرایی مشمول قانون تشکیل سازمان پدافند غیرعامل کشور می‌باشد.

قلمرو کاربردی این سند عبارت است از:

الف) دارایی‌ها و سرمایه‌های ملی حوزه الکترونیک و وابسته به آن و ترکیبی آنها با حوزه سایبری در زیرساخت‌های حیاتی، حساس، مهم و قابل‌حفاظت کشور؛

ب) زیرساخت‌های مبتنی بر فناوری‌های ۱۰گانه (الکترومغناطیس، بیوالکترومغناطیس، ژئوالکترومغناطیس، میکروالکترونیک، اپتیک و لیزر، سایبرالکترومغناطیس، سایبرالکترونیک، مکاترونیک(روبات‌ها و ریزپرنده‌ها)، الکتروآکوستیک و ماهواره)؛

تبصرهٔ۱- تمشیت و راهبری اجرای این سند در نیروهای مسلح، بر عهدهٔ شورای راهبردی پدافند غیرعامل نیروهای مسلح می‌باشد.

تبصرهٔ۲- اعتبار این سند به مدت ۱۰ سال پیش‌بینی شده است و هر سه سال یکبار قابل بازنگری یا تمدید می‌باشد.

ماده ۶- اصول و ارزش‌ها

۱) تعامل‌پذیری و هماهنگی بین دستگاهی؛
۲) تاب آوری و انطباق‌پذیری؛
۳) هوشمندی و بهره‌گیری از هوش مصنوعی؛
۴) آگاهی وضعیتی و آمادگی دائمی؛
۵) آینده‌نگری و آینده‌پژوهی فن‌آورانه؛
۶) پایداری و تداوم کارکردی؛

۷) عدم اعتماد به محصولات خارجی (پنهان کاری دشمن در ذات تجهیزات الکترونیک)؛

۸) بومی‌سازی روزآمد زیست بوم الکترونیک (ترجیح محصولات بومی بر غیربومی)؛

۹) صیانت از سرمایه‌های الکترونیک و انسانی متخصص کشور و وابسته به آن؛

۱۰)پیش‌بینی، پیشگیری، خنثی‌سازی و پیش‌تهی‌سازی تهدیدات الکترونیک؛

۱۱)دفاع جمعی در جنگ ترکیبی؛

۱۲)مدیریت جهادی، تفکر و عمل بسیجی.

ماده ۷- رسالت

صیانت، تضمین تداوم عملکرد، افزایش پایداری، رصد و کاهش آسیب‌پذیری و مخاطرات و مصون‌سازی و ارتقاء آمادگی‌های عملیاتی و پدافندی دارایی‌ها و زیرساخت‌های حوزه الکترونیک کشور مبتنی بر ظرفیت‌ها، قابلیت‌ها و فن‌آوری بومی و روزآمد در برابر تهدیدات حوزه الکترونیک دشمن و مصونیت زنجیره تولیدات و خدمات راهبردی الکترونیک کشور.

مـاده ۸ - مأموریت

سازمان/ قرارگاه با هماهنگی و تعامل و راهبری دستگاه‌های مسئول و ذی‌نقش، سیاستگذاری، هدایت، راهبری و نظارت و حصول اطمینان از اقدامات در زمینه افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء آموزش و پایداری ملی، مقاوم‌سازی زیرساخت‌های حیاتی، حساس، مهم و قابل حفاظت کشور، تسهیل مدیریت بحران در برابر انواع تهدیدات الکترونیک دشمن و سلاح‌های نامتعارف این حوزه و مدیریت پیشگیرانه در مقابل تهدیدات جدید حوزه الکترونیک و حصول اطمینان از آمادگی دستگاه‌های اجرایی را برعهده دارد.

بیانیه مأموریت:

۱) اشراف اطلاعاتی بر تهدیدات حوزه الکترونیک و ترکیبی دشمن در حوزه‌های ۱۰گانه الکترونیک؛

۲) رصد، پایش، تشخیص، واپایش، ارزیابی و هشداردهی پیش‌دستانه تهدیدات، هدایت و هماهنگی عملیاتی در حوزه الکترونیک از طریق مرکز عملیات پدافند غیرعامل الکترونیک کشور (EDOC)؛

۳) مصون‌سازی و کاهش دائمی آسیب‌پذیری‌های زیرساخت‌های الکترونیکی و الکترومغناطیسی کشور در برابر تهدیدات حوزه الکترونیک؛

۴) صیانت از دسترسی و بهره‌برداری دشمن از طیف الکترومغناطیس و مراقبت از شبکه مخابراتی و الکترونیکی کشور در برابر حملات الکترومغناطیس، اختلالات فرکانسی(ارتباطی و ناوبری)، بیوالکترومغناطیس، ژئوالکترومغناطیس و سایبرالکترومغناطیس در زیرساخت‌های با اهمیت بالای کشور؛

۵) ایجاد تعامل و هماهنگی بین دستگاهی در حوزه پدافند غیرعامل الکترونیک در حوزه‌های زیرساختی و عملیاتی در جهت ارتقاء هماهنگی و هم افزایی بین دستگاهی؛

۶) مقابله با تهدیدات حوزه الکترونیک با اقدامات عملیاتی پدافند غیرعامل الکترونیک در زیرساخت‌های حیاتی و حساس کشور با تمرکز بر طراحی عملیاتی و راهبری و نظارت آن، آموزش، فرهنگ‌سازی و رزمایش؛

۷) طبقه‌بندی و سطح‌بندی زیرساخت‌ها، دارایی‌ها و سامانه‌های الکترونیک کشور بر اساس اهمیت و ماهیت آنها و تعیین نقاط کلیدی و عناصر دارایی؛

۸) تهیه، تدوین، تنظیم و ابلاغ نظامات، مقررات، ضوابط، شیوه‌نامه‌ها و استانداردهای بومی پدافند غیرعامل الکترونیک و نظارت بر حسن اجرای آنها؛

۹) ساماندهی و توسعه ظرفیت آزمایشگاه‌ها و تعیین آزمایشگاه مرجع تخصصی الکترونیک با قدرت تشخیص مخاطرات و آسیب‌پذیری‌ها، خرابکاری‌های صنعتی، تهدیدات پنهان در ذات فناوری پدافند غیرعامل الکترونیک در کشور؛

۱۰) فرهنگ‌سازی، اطلاع‌رسانی و آگاهی‌بخشی در جامعه مخاطب نسبت به پدافند غیرعامل الکترونیک و تهدیدات الکترونیک دشمن براساس الگوی پدافند رسانه‌ای؛

۱۱) توسعه دانش تخصصی پدافند غیرعامل الکترونیک و حمایت از تحقیق، توسعه و مدیریت دانش و توانمندسازی علمی نیروی انسانی مبتکر، متخصص و متعهد پدافند غیرعامل الکترونیک کشور؛

۱۲)طرح‌ریزی، آموزش، تجهیز، تمرین، رزمایش و ارزیابی عملیاتی و ارتقاء آمادگی‌ها در حوزه پدافند غیرعامل الکترونیک؛
۱۳)حمایت از صنعت بومی پدافند غیرعامل الکترونیک با تأکید بر همکاری و مشارکت شرکت‌های دانش بنیان و فن-آور در جهت خودکفایی و کاهش جدی وابستگی به فناوری‌ها و محصولات خارجی؛
۱۴)تعامل با کشورها و نهادهای بین المللی و منطقه‌ای در حوزه پدافند غیرعامل الکترونیک با همکاری و هماهنگی وزارت امورخارجه در چارچوب دیپلماسی دفاعی کشور.

ماده۹– چشم انداز

با استعانت از پروردگار متعال و تدابیر مقام معظم رهبری مدظله‌العالی در افق ۱۴۱۴، جمهوری اسلامی ایران با ابتناء به ساختارهای نوآور و انسان‌های فداکار به عنوان الگو و اُسوه منطقه و جهان اسلام در پاسداری از سرمایه‌های الکترونیکی و زیرساخت‌های حیاتی، حساس و مهم کشور در برابر هرگونه تهاجم دشمنان به حوزه الکترونیک به‌صورت پایدار، تاب‌آور، مصون با قابلیت حفظ تداوم کارکردهای اساسی و پاسخگو به تهدیدات این حوزه دشمنان منطقه‌ای و **دارای جایگاهی اطمینان بخش در سطح جهانی و در شمار قدرت‌های برتر منطقه** است.

ویژگی‌های این چشم‌انداز عبارتند از:

۱)بهره‌مند از سرمایه‌های الکترونیک پایدار، تاب آور و مصون با قابلیت حفظ تداوم کارکردهای اساسی، حداقل آسیب‌پذیری و پاسخگو به تهدیدات؛
۲)توانمند در رصد، پایش، تشخیص، هشدار پیش‌دستانه تهدیدات الکترونیک دشمنان و ارزیابی و تحلیل هوشمند و به‌موقع مخاطرات و واپایش و آسیب‌پذیری حوزه الکترونیک با استفاده از هوش مصنوعی؛
۳)برخوردار از سرمایه‌های انسانی مبتکر، ماهر، متخصص، متعهد، کارآمد، امین، خلاق، بصیر و دارای روحیه بسیجی متناسب با تهدیدات؛
۴)دارای نظام پدافند غیرعامل الکترونیک هوشمندانه، اختصاصی، ابتکاری، عمیق، لایه‌به‌لایه، بومی، پیشگیرانه، شبکه‌ای، توزیع‌شده، سلسله مراتبی، چابک و منعطف در سطح ملی، استانی و دستگاهی؛
۵)برخوردار از نظام عملیاتی پدافند غیرعامل الکترونیک، هماهنگ، یکپارچه، کارا و اثربخش فرماندهی واپایش و مدیریت رصد و پایش مخاطرات و برنامه و طرح‌ها و دستورالعمل‌های عملیاتی پدافند غیرعامل الکترونیک؛
۶)بهره‌مند از نظام نهادینه و نهادمند آموزش و فرهنگ‌سازی، تمرین، رزمایش، آمادگی، اطلاع‌رسانی و آرامش‌بخش؛
۷)برخوردار از اسناد هادی راهبردی، استانداردها، مقررآت و دکترین پدافندی نهادینه شده درحوزه پدافند غیرعامل الکترونیک.

ماده ۱۰– اهداف کلان

۱) مصون‌سازی، افزایش تاب‌آوری و کاهش آسیب‌پذیری زیرساخت‌های کشور در برابر تهدیدات حوزه الکترونیک؛
۲) طراحی، راهبری و نهادینه‌سازی نظام جامع پدافند غیرعامل الکترونیک متناسب با سطح تهدیدات این حوزه؛
۳) تعیین متولی و ساختار پدافند غیرعامل الکترونیک کشور و تعیین نقش‌ها، وظایف و جایگاه دستگاه‌ها و نهادهای ذی‌ربط در آن؛
۴) دستیابی به ظرفیت و توانمندی لازم برای مصون‌سازیِ خوداتکا و بومی در حوزه پدافند غیرعامل الکترونیک.

ماده ۱۱– راهبردهای حوزه پدافند غیرعامل الکترونیک

۱) مصون‌سازی زیرساخت‌های الکترونیک و وابسته به آن در حوزه‌های ۱۰گانه الکترونیک:
۱-۱- در برابر تهدیدات سایبر الکترونیک و سایبر الکترومغناطیس مبتنی بر غربالگری الکترونیک و واپایش زنجیره تأمین؛

۱-۲- در برابر تهدیدات مکاترونیک، روبات‌ها، ریزپرنده‌ها با استفاده از سامانه‌های تشخیص‌گر و سلاح‌های غیرعامل الکترونیک برای مقابله با آنها؛

۱-۳- مصون‌سازی تجهیزات الکترواپتیک (اپتیک، مادون قرمز، لیزر) مورد استفاده در زیرساخت های کشور برای ممانعت از دسترسی و نفوذ دشمن؛

۱-۴- صیانت از اقلیم و تغییر زیست بوم کشور در برابر تهدیدات حوزه ژئوالکترومغناطیس از قبیل جلوگیری از باران زدایی و ابرزدایی؛

۱-۵- صیانت از حوزه سلامت کشور در برابر تهدیدات حوزه بیوالکترومغناطیس جلوگیری از آسیب‌های ناشی از طیف الکترومغناطیس ناهنجار در کشور؛

۱-۶- مصون‌سازی زیرساخت‌های وابسته به حوزه الکترومغناطیس (مخابراتی، راداری، ناوبری) در کشور در برابر اختلالات فرکانسی با بومی سازی تجهیزات این حوزه و هماهنگی در تنظیم مقررات رادیویی بخش لشکری و کشوری؛

۱-۷- در برابر تهدیدات حوزه جاسوسی تصویری ماهواره‌های سنجش از راه دور دشمن؛

۱-۸- در برابر حملات تروریستی و خرابکارانه مبتنی بر میکرو ماهواره‌ها با استفاده از ابزار **GETSAT**، اینترنت اشیاء و هوش مصنوعی؛

۲) سازماندهی نظام جامع رصد، پایش، مراقبت، تشخیص و هشداردهی با بهره‌گیری از ظرفیت‌های موجود در بخش کشوری به صورت شبکه محور با سامانه مدیریت، فرماندهی، واپایش و نظارت الکترونیک در قالب مرکز عملیات پدافند غیرعامل الکترونیک کشور (**EDOC**)؛

۳) طراحی و استقرار نظام فرماندهی و کنترل عملیات پدافند غیرعامل الکترونیک به صورت هوشمند، هم افزا، منسجم و مجهز به هوش مصنوعی برای تصمیم‌یاری و افزایش دقت و سرعت در عملیات پدافندی در مقابله با تهدیدات حوزه الکترونیک در کشور؛

۴) طراحی و استقرار نظام رصد، پایش، تشخیص، شبیه سازی، هشدار تهدیدات و مخاطرات الکترونیک و اشراف اطلاعاتی بر دشمن با بهره‌گیری از هوش مصنوعی و سایر فناوری‌های پیشرفته اطلاعاتی موردنیاز؛

۵) طبقه‌بندی، سطح‌بندی و اولویت‌دهی مراکز و زیرساخت‌های الکترونیک و وابسته به آن از منظر تهدیدات حوزه الکترونیک؛

۶) ساماندهی نظام غربالگری الکترونیک برای ورود فناوری تا بهره‌برداری در لایه‌های طراحی، ساخت، تعمیر و نگهداری، به‌روزرسانی و ارتقاء در زیرساخت‌های کشور با استفاده از ظرفیت‌های نظارتی گمرکی و ظرفیت‌های آزمایشگاه‌های مرجع پدافند غیرعامل الکترونیک به‌صورت شبکه محور با ارزیابی روزآمد و قطب در کشور و برای تشخیص و کشف خرابکاری‌های صنعتی در تجهیزات الکترونیک؛

۷) طراحی و استقرار نظام ارزیابی محصولات بومی با هدف افزایش امنیت و اعتمادبخشی و تقویت صنعت الکترونیک کشور با بهره‌گیری از ظرفیت‌های آزمایشگاهی حوزه کشوری و لشکری؛

۸) طراحی زیرساخت بومی خودکفا و کاهش وابستگی در حوزه خدمات ناوبری به منظومه‌های ماهواره‌ای کشورهای بیگانه (GNSS[۵]) جهت مقابله با تهدیدات و کاهش مخاطرات حوزه ناوبری؛

[۵] Global Navigation Satellite System

۹) صیانت از فضای فرکانسی کشور با ممانعت ورود دشمن از بستر طیف الکترومغناطیس ماهواره‌های اینترنتی با هدف جلوگیری از تضعیف حاکمیت فضای مجازی کشور؛

۱۰) ارتقاء تاب‌آوری و ضریب امنیت تدوام عملکرد زیرساخت‌های الکترونیک و وابسته به آن با عملیات تخصصی پدافند غیرعامل الکترونیک با پیش بینی جایگزین‌های قابل اطمینان برای آنها؛

۱۱) ارتقاء آمادگی پدافندی از طریق برگزاری رزمایش‌های مستمر در داخل کشور و مشترک متناسب با سناریوهای تهاجمی احتمالی دشمن و افزایش آمادگی‌های پدافند غیرعاملی در برخورد با تهدیدات حوزه الکترونیک؛

۱۲) تدوین قوانین و مقررات، تنظیم آیین‌نامه‌های اجرایی و نظارت بر اجرا برای پیاده‌سازی قانون سازمان در این حوزه؛

۱۳) هماهنگی و هم‌افزایی حداکثری بین زیرساخت‌های الکترونیک و وابسته با آن بین دستگاه‌های اجرایی بخش لشکری و کشوری برای تسریع اجرای مأموریت، نظارت، بازرسی، هماهنگی و هم افزایی در کشور؛

۱۴) توسعه علمی و دانشی و آموزشی و فرهنگ‌سازی و نهادینه‌سازی مفاهیم پدافند غیرعامل الکترونیک در نظام آموزشی و پژوهشی کشور و بخش‌های مرتبط با حوزه الکترونیک؛

۱۵) طراحی و راهبری نظام تحقیق، توسعه و مدیریت دانش کارآمد، هوشمندانه، نافذ و به‌روز شونده در حوزه پدافند غیرعامل الکترونیک با بهره‌گیری از دانش و فناوری‌های روزآمد و به‌کارگیری نخبگان و متخصصان حوزه الکترونیک کشور با هدف دستیابی به فناوری‌های شالوده شکن با افزایش ظرفیت ایده‌پردازی، پژوهش، تحقیقات، طراحی، تولید بومی و مهندسی معکوس در داخل کشور؛

۱۶) حمایت و پشتیبانی از صنعت تولید تراشه در کشور برای خودکفایی حوزه میکروالکترونیک و کاهش وابستگی در حوزه نانوالکترونیک کشور؛

۱۷) توسعه صنعت الکترونیک و الکترومغناطیس بومی روزآمد، خوداتکا با حمایت مادی و معنوی از شرکت‌های دانش‌بنیان و سایر فعالان این حوزه در بخش‌های غیردولتی و خصوصی برای افزایش رونق کسب‌وکار پدافند غیرعامل الکترونیک؛

۱۸) دستیابی به نظام دفاع حقوقی و جمعی با تعاملات بین‌المللی در حوزه‌های مختلف پدافند غیرعامل الکترونیک در راستای دفاع از منافع ملی و دیپلماسی فعال و حضور مؤثر در مجامع تصمیم‌گیری بین‌المللی و منطقه‌ای؛

۱۹) تعامل سازنده با کشورهای پیشرفته همسو، دوست و همسایه به‌منظور توسعه تعاملات و انتقال تجارب و فناوری‌های نوین و حمایت از صادرات تجهیزات الکترونیک بومی؛

۲۰) سازماندهی قرارگاه پدافند غیرعامل الکترونیک در دستگاه‌های اجرایی برای رصد و پایش و تشخیص و هشدار تهدیدات الکترونیک و امن‌سازی و مصون‌سازی زیرساخت‌های الکترونیک و حصول اطمینان از آمادگی‌های عملیاتی و زیرساختی پدافند غیرعامل الکترونیک؛

ماده ۱۲ - سیاست‌های عملیاتی پدافند غیرعامل الکترونیک

۱) پرهیز از هرگونه غافلگیری؛

۲) اتّکاء به توان داخلی، محصولات بومی به‌ویژه معماری پدافندی اختصاصی (بومی)؛

۳) عدم اعتماد به سامانه‌ها و خدمات خارجی؛

۴) واپایش مضاعف محصولات الکترونیک وارداتی از منظر تهدیدات درون‌زای مبتنی بر فناوری‌های نوین و انسانی پنهان و نهادینه شده در ذات فناوری؛

۵) کاهش حداکثری و مداوم آسیب‌پذیری، تهدید، خطای پیش‌بینی، زمان تشخیص و واکنش؛

۶) تناسب اقدام‌های پدافند غیرعامل الکترونیک با ویژگی‌های کلیدی اهمیت سرمایه الکترونیک، تهدید الکترونیک، آسیب‌پذیری و مخاطره حوزه الکترونیک، تهاجم الکترونیک دشمن و پیامدهای الکترونیکی و فیزیکی ناشی از جنگ الکترونیک؛

۷) تمرکز بر عملیات پدافند غیرعامل الکترونیک با اولویت در رویکردهای پیش‌بینانه، پیش‌گیرانه، پیش‌کنشگرانه، واکنش‌گرایانه و منفعلانه؛

۸) سرعت پیش‌بینی، تداوم کارکردهای ضروری و دقّت و سرعت پاسخ و مقابله؛

۹) تمرکز بر مواجهه با عملیات ترکیبی دشمن در حوزه الکترونیک بر اساس اولویت مواجهه با عملیات ترکیبی الکترونیکی و الکترومغناطیسی - سایبری- اجتماعی، الکترونیکی- فیزیکی و سایر.

ماده ۱۳– طرح‌های عملیات تخصصی پدافند غیرعامل الکترونیک

۱) **طرح پاسخ اضطراری حوزه الکترونیک** (EERP: Electronic Emergency Response Plan)

به مجموعه فرایند و اقدامات حوزه پدافند غیرعامل الکترونیک در شرایط اضطراری با هدف پاسخ به حملات الکترونیک در حوزه های ۱۰گانه اطلاق می‌گردد.

۲) **طرح حفظ و تداوم کارکردهای اساسی حوزه الکترونیک** (EBCP: Electronic Business Countinuty Plan)

به مجموعه فرایند و اقدامات حوزه پدافند غیرعامل الکترونیک اطلاق می گردد که هدف آن تداوم ارائه خدمات اساسی در دستگاه‌ها و زیرساخت‌ها بااهمیت بالای کشور اطلاق می‌گردد.

۳) **طرح بازیابی و برگشت پذیری بعد از حادثه حوزه الکترونیک** (EDRP: Electronic Disaster Recovery Plan)

به مجموعه اقدامات حوزه پدافند غیرعامل الکترونیک در واکنش به رویداد فاجعه بار در جهت نجات افراد، تجهیزات و دارایی‌های حوزه الکترونیک با هدف تثبیت وضعیت و بازیابی سریع خدمات و عملیاتی حیاتی اطلاق می‌گردد.

۴) **طرح بهینه سازی وابستگی متقابل حوزه الکترونیک** (EOIP: Electronic Optimizing Interdependency Plan)

به مجموعه اقدامات حوزه پدافند غیرعامل الکترونیک با هدف مدیریت فعالانه، هماهنگ‌سازی و بهبود کارایی ارتباطات و تأثیرات متقابل بین بخش‌ها، فرایندها تیم‌ها و یا منابع هستند اطلاق می شود.

۵) **طرح کاهش و مدیریت مخاطرات حوزه الکترونیک** (EHMP: Electronic Hazard Management Plan)

به مجموعه اقدامات حوزه پدافند غیرعامل الکترونیک برای ارزیابی ریسک، احتمال وقوع و شدت پیامدها و تجزیه و تحلیل آنها با هدف پیش‌بینی و مدیریت مخاطرات در زمان وقوع حادثه اطلاق می‌گردد.

۶) **طرح مصون‌سازی زیرساخت‌های با اهمیت بالا حوزه‌الکترونیک**(ECIP:Electronic Critical Infrastructure Protection)

به مجموعه اقدامات پدافند غیرعامل الکترونیک برای پیشگیری، کاهش ریسک و امن‌سازی و مصون‌سازی در برابر تهدیدات حوزه الکترونیک اطلاق می‌گردد.

۷) **طرح آمادگی حوزه پدافند غیرعامل الکترونیک** (EPP: Electronic Preparedness Plan)

به مجموعه اقدامات شامل طرح‌ریزی، آموزش، تمرین و رزمایش های برنامه ریزی شده با هدف حصول اطمینان از آمادگی‌ها در برابر تهدیدات حوزه الکترونیک اطلاق می‌گردد.

۸) **طرح کاهش دائمی آسیب‌پذیری‌های عمده حوزه الکترونیک** (EVRP: Electronic Vulnerability Reduction Plan)

مجموعه اقدامات حوزه پدافند غیرعامل الکترونیک برای کاهش آسیب‌پذیری حوزه الکترونیک در دستگاه‌ها و زیرساخت‌های الکترونیک و وابسته به آن با انجام فرایند شناسایی، ارزیابی، الویت‌بندی و رفع آسیب‌پذیری‌ها یا کاهش آنها اطلاق می‌گردد.

ماده ۱۴- سطوح عملیات پدافند غیرعامل الکترونیک

عملیات پدافند غیرعامل الکترونیک در سه سطح ملی، منطقه‌ای و محلی انجام می‌شوند.

۱) **عملیات پدافند غیرعامل الکترونیک محلی**، در مقابل تهاجم الکترونیک و الکترومغناطیس علیه یک دارایی حیاتی یا حساس با نقش و کارکرد زیرساختی و قدرت تولید مخاطرات محلی انجام و درگیری الکترونیک و الکترومغناطیس نامیده می‌شود.

۲) **عملیات پدافند غیرعامل الکترونیک منطقه‌ای**، در مقابل تهاجم الکترونیکی و الکترومغناطیسی گسترده علیه یک دارایی حیاتی یا حساس برخوردار از نقش و کارکرد منطقه‌ای یا حوزه‌ای و قدرت تولید مخاطرات عمده انجام می‌شود.

۳) **عملیات پدافند غیرعامل الکترونیک ملی**، در مقابل تهاجم الکترونیکی و الکترومغناطیسی گسترده علیه مجموعه‌ای از دارایی‌های حیاتی یا حساس کشور با نقش و کارکرد ملی و قدرت تولید مخاطرات فاجعه‌بار انجام می‌شود. اختلالات مسیریابی در حوزه کشتیرانی، هواپیمایی و فضایی که باعث توقف و تغییر در مسیرها و حوادث دیگر مانند آن نیز در این سطح قرار می‌گیرند.

ماده ۱۵- وضعیت‌های عملیات پدافند غیرعامل الکترونیک

وضعیت عملیات پدافند غیرعامل الکترونیک، شامل چهار وضعیت با عناوین سفید، زرد، نارنجی و قرمز است که به‌ترتیب معادل احساس امنیت، احساس تهدید، احساس جنگ قریب‌الوقوع و وقوع جنگ در فضای الکترونیک و الکترومغناطیسی یا ازطریق این فضا می‌باشد.

تعاریف، شاخص‌ها و اقدامات اجرایی لازم برای هریک از وضعیت‌های فوق، در دستورالعمل آماده‌باش دستگاه‌های بخش کشوری در برابر تهدیدات نظامی دشمن مصوبه شماره ۳۰۸۱ مورخ ۱۴۰۳/۱۱/۲۸ به کلیه دستگاه‌های اجرایی ابلاغ شده است.

ماده ۱۶- رویکردهای عملیاتی پدافند غیرعامل الکترونیک

الف) **رویکرد عملیاتی پیش‌بینانه:** رویکرد عملیات پیش‌بینانه شامل اقداماتی از قبیل رصد و پایش، مراقبت و تشخیص زودهنگام (قبل از وقوع) تهدیدات و اقدامات دشمن به منظور عدم غافلگیری و ایجاد آمادگی برای رویارویی.

ب) **رویکرد عملیاتی پیش‌گیرانه:** رویکرد عملیات پیش‌گیرانه اقداماتی شامل برطرف‌کردن آسیب‌پذیری‌ها و نقاط ضعف، کنترل و ارتقاء آمادگی‌ها به‌منظورکاهش‌غافلگیری و برطرف‌کردن آسیب‌پذیری‌های عمده و ارتقاء آمادگی‌های مقابله‌ای می‌باشد.

ج) **رویکرد عملیاتی پیش‌دستانه/پیش‌کنشگرایانه:** مجموعه‌ای از اقدامات عملیاتی است که با هدف برهم زدن تمرکز و انصراف دشمن از اقدام و تحمیل اراده خودی بر آن و دستیابی به شرایط و موقعیت‌های بهتر برای نیروهای خودی انجام می‌گیرد.

هـ) **رویکرد عملیاتی مقابله:** به مجموعه اقدامات و عملیاتی که در زمان وقوع حادثه و حمله انجام می‌شود و شامل پاسخ به حمله و کنترل حادثه و پیامدهای آن می‌باشد. در این وضعیت احتمالاً غافلگیری حادث شده یا بر اساس طرح‌ریزی از قبل اقدام می‌شود و واحدهای خودی مجبور به واکنش مقابله‌ای هستند.

و) **رویکرد عملیاتی عکس‌العملی:** این رویکرد پس از غافلگیر شدن، حین یا پس از حادثه به صورت عکس‌العملی اتفاق می‌افتد این رویکرد منجر به اقداماتی عکس‌العملی و انفعالی با اثر کم و با محوریت برگشت‌پذیری به شرایط اولیه و کاهش پیامدها و ضایعات و خسارات انجام می‌گیرد.

ماده ۱۷- تدبیر عملیاتی (چگونگی اقدام عملیات پدافند غیرعامل الکترونیک)

قرارگاه در چارچوب و تکمیل سیاست‌های دفاعی کشور با پدافند غیرعامل الکترونیک از فضای ملی الکترونیک و الکترومغناطیس و زیرساخت‌های حیاتی،حساس، مهم و قابل حفاظت الکترونیک و وابسته به آن در برابر انواع تهدیدات الکترونیکی با بسیج منابع ملی در این حوزه، اقدامات پدافند غیرعامل الکترونیکی در ۶ گام عملیاتی زیر توسط دستگاه‌های اجرایی در سطوح ملی، منطقه‌ای و محلی را هدایت، راهبری، پشتیبانی و نظارت می‌کند.

گام اول- اشراف اطلاعاتی

۱) رصد، پایش، برآورد اطلاعاتی و اشتراک‌گذاری اطلاعات وضعیت تهدید الکترونیک و مخاطرات احتمالی ناشی از آن؛

۲) رصد، پایش، برآورد عملیاتی و بررسی نقاط ضعف و قوت خودی و پایش آمادگی‌ها؛

گام دوم - آمادگی عملیاتی

۱) تعیین وضعیت پدافند غیرعامل الکترونیک و عملیاتی، آگاهی‌رسانی؛

۲) توسعه آموزش‌ها و تمرین‌های عملیاتی و سازماندهی واحدهای عملیاتی الکترونیک؛

۳) ارتقاء مهارت، تخصص و توانایی عملیاتی نیروهای پدافند غیرعامل الکترونیک؛

۴) ارتقاء تجارب و آمادگی عملیاتی نیروهای پدافند غیرعامل الکترونیک و هماهنگی و مشارکت نیروهای آفند الکترونیک؛

گام سوم - مصونیّت دارایی‌های حیاتی و حساس در مقابل هر نوع تهدید الکترونیک

۱) شناخت، احصاء ویژگی‌ها، ارزش‌گذاری و طبقه‌بندی دارایی‌های حوزه االکترونیک؛

۲) آمن‌سازی اضطراری و کاهش آسیب‌پذیری‌های حوزه الکترونیک؛

۳) صیانت و مصون‌سازی الکترونیک دارایی‌های حیاتی و حساس و مهم در مقابل هر نوع تهدید الکترونیک؛

گام چهارم - تاب‌آوری و تداوم کارکردهای ضروری دارایی‌های الکترونیکی

۱) یکپارچه‌سازی، تقویت تعامل و تعمیق همکاری و مشارکت نیروهای پدافند غیرعامل الکترونیک برای افزایش انسجام و مقاومت در جنگ الکترونیک؛

۲) بهره‌گیری از سازوکارهای پدافند غیرعامل الکترونیک برای اجرای مأموریت‌های پدافند غیرعامل الکترونیک؛

۳) اشتراک‌گذاری اطلاعات و تبادل تجارب و تشخیص و واکنش سریع و مؤثر به جنگ الکترونیک و پیامدهای آن؛

گام پنجم - برتری عملیاتی نیروهای پدافند غیرعامل الکترونیک خودی بر دشمن

۱) کنترل تنش الکترونیکی و الکترومغناطیسی (کاهش شدّت، احتمال‌وقوع و اثر مخاطره) با مدیریت مخاطرات آنها؛

۲) اقناع افکار عمومی خودی درخصوص محکومیت جنگ الکترونیک قریب‌الوقوع دشمن و مشروعیت پاسخ خودی؛

۳) نمایش قدرت الکترونیک، بزرگ‌نمایی پیامدهای اقدام‌متقابل و تهدید به‌استفاده از قدرت نظامی در پاسخ به تجاوز در حوزه‌های االکترونیک؛

۴) یکپارچه‌سازی تجهیزات پدافند غیرعامل الکترونیک در مأموریت‌های پدافند غیرعامل الکترونیک؛

۵) شناسایی متجاوز و منشأ تجاوز و انتساب تجاوز الکترونیکی به دشمن و مستندسازی ادلّه قانونی تجاوز الکترونیک و الکترومغناطیسی؛

۶) ممانعت از تداوم تجاوز الکترونیک یا مقابله و دفع تجاوز دشمن ازطریق ریشه‌کنی منشأ جنگ الکترونیک؛

گام ششم- ابقاء (ترمیم) و ارتقاء قدرت پدافندی الکترونیک

۱) بازیابی، ترمیم و اصلاح پیامدهای جنگ الکترونیک و ابقاء کارکردهای دارایی‌های حیاتی و حساس؛
۲) استیفای حقوق قانونی کشور ازطریق محکومیت سیاسی و حقوقی تجاوز الکترونیک و الکترومغناطیسی در مراجع و محاکم بین‌المللی؛
۳) ابقاء و ارتقاء قابلیت‌ها، توانایی و آمادگی عملیاتی غیرعامل و فعّال پدافند غیرعامل الکترونیک.

ماده ۱۸- اقدامات اساسی در حوزه پدافند غیرعامل الکترونیک

۱) راه اندازی و فعال سازی مرکز رصد و پایش عملیاتی الکترومغناطیس (EDOC) در حوزه کشوری؛
۲) ساماندهی مراکز آزمایشگاهی و تعیین آزمایشگاه مرجع پدافند غیرعامل الکترونیک در کشور؛
۳) تنظیم و تولید سند نظام عملیاتی هماهنگ و هم افزای پدافند غیرعامل الکترونیک در برابر تهدیدات دشمن و تعیین وظایف دستگاه‌های دارای نقش اساسی در حوزه پدافند غیرعامل الکترونیک؛
۴) ایجاد مرکز تنظیم مقررات پدافند غیرعامل الکترونیک برای تهیه مقررات، ضوابط و الزامات و ملاحظات پدافند غیرعامل الکترونیک و تدوین دستورالعمل‌های عملیاتی پدافند غیرعامل الکترونیک در حوزه‌های ۱۰گانه؛
۵) برقراری و تداوم ارتباط بین بخش کشوری و لشکری و هماهنگی حداکثری عملیاتی در حوزه الکترونیک به ویژه در حوزه رصد و پایش اختلالات فرکانسی کشوری با عضویت در شورای تنظیم مقررات رادیویی؛
۶) نهادینه‌سازی نظام عملیاتی پدافند غیرعامل الکترونیک و ارتقاء آمادگی زیرساخت‌های الکترونیک کشور در برابر دشمن؛
۷) سازماندهی رصدخانه علمی فناوری‌های نوین در حوزه الکترونیک و پایش راهبردها و راهکنش(تاکتیک)های ترکیبی دشمن به‌منظور شناخت و اشراف بر دشمن و توانایی‌های آن با استفاده از ظرفیت‌های علمی کشور؛
۸) سازماندهی و فعالسازی قرارگاه با رویکرد هم افزایی و هماهنگی حداکثری با دفاع الکترونیک یکپارچه کشوری و لشکری و راه‌اندازی یگان‌های عملیاتی فاتح در قرارگاه و سایر دستگاه‌های اجرایی؛
۹) مصون‌سازی زیرساختی و کالبدی الکترونیک برای مراکز حیاتی و مراکز داده راهبردی حیاتی کشور؛
۱۰) تدوین و ابلاغ سیاست‌ها و دستورالعمل‌های عملیاتی پدافند غیرعامل الکترونیک ذیل این سند.

ماده ۱۹- وظایف دستگاه های اجرایی

الف) وزارت دفاع و پشتیبانی نیروهای مسلح

پشتیبانی تخصصی از مأموریت‌های عملیاتی پدافند غیرعامل الکترونیک، از طریق توسعه صنعت بومی پدافند غیرعامل الکترونیک، ایجاد و سازماندهی ظرفیت عمل کلی زیرساختی پدافند غیرعامل الکترونیک مانند آزمایشگاه‌های تشخیصی و پشتیبانی تخصصی از مرکز عملیات پدافند غیرعامل الکترونیک کشور را بر عهده دارد و ظرفیت‌های عملیاتی الکترونیک وزارت دفاع برای انجام وظایف زیر، بنا به دستور در کنترل عملیاتی قرارگاه قرار می‌گیرند.

۱) تولید و تأمین سامانه‌های الکترواپتیک با هدف شناسایی تهدیدات حوزه الکترونیک؛
۲) تولید و تأمین سامانه‌های ارتباطی آمن با هدف ایجاد ارتباطات ایمن در زیرساخت‌ها؛
۳) تولید و تأمین سامانه‌های ژئوالکترومغناطیس با هدف شناسایی و مقابله با تهدیدات این حوزه؛
۴) تولید و تأمین سامانه‌های سایبرالکترومغناطیس با هدف شناسایی و مقابله با تهدیدات این حوزه؛
۵) تولید و تأمین تراشه‌های بومی با هدف کاهش وابستگی به غرب؛
۶) طراحی، تولید و عملیاتی‌سازی تجهیزات پایه پدافند غیرعامل الکترونیک موردنیاز؛

۷) ارائه خدمات آزمایشگاه غربالگری الکترونیک در حوزه سایبرالکترونیک؛
۸) تولید و تأمین سامانه‌های مقابله با تهدیدات حوزه جنگ الکترونیک؛
۹) کمک به انجام عملیات امداد و نجات الکترونیک در زیرساخت‌های حیاتی، حساس، مهم و قابل حفاظت؛
۱۰) کمک به جمع‌آوری ادلّه و جرم‌شناسی رقومی در زیرساخت‌های حیاتی، حساس، مهم و قابل حفاظت.

ب) وزارت ارتباطات و فناوری اطلاعات

وزارت ارتباطات و فناوری اطلاعات با هماهنگی قرارگاه مسئولیت انجام وظایف زیر را بر عهده دارد.
۱) امن‌سازی و مصون‌سازی زیرساخت‌های الکترونیک و وابسته به آن در برابر تهدیدات الکترونیک با تأکید بر زیرساخت‌های ارتباطاتی (با سیم و بی‌سیم، ارتباطات فضا پایه، شبکه زیرساختی کشور، ماهواره‌ای)؛
۲) صیانت و پدافند از مرزهای الکترونیک کشور با هماهنگی قرارگاه پدافند غیرعامل الکترونیک؛
۳) حفظ و ارتقاء تداوم کارکرد زیرساختی در شبکه دارایی‌ها و سرمایه‌های الکترونیک و ارتقاء پایداری آن؛
۴) پایش، رصد و کشف آسیب‌پذیری در زیرساخت‌های ارتباطی در دسترس؛
۵) دفاع از منافع ملی کشور در حوزه الکترونیک در مجامع بین‌المللی ارتباطات و مخابرات و فضا پایه با بهره‌گیری از دیپلماسی پدافندی؛
۶) تشخیص تهدیدات الکترونیک در لایه شبکه ارتباطی و مقابله و محدودسازی حملات الکترونیک؛
۷) ایجاد و بهره‌برداری ارتباط ویژه با گروه‌های واکنش سریع (EERT[۴]) بین‌المللی؛
۸) آماده‌سازی مسیرهای جایگزین مخابراتی، ارتباطی و اینترنت (امکان اتصال و انفصال شبکه‌های خارجی متصل به شبکه ملی اطلاعات)؛
۹) رصد و پایش زیرساخت‌های الکترونیک کشور و تهیه گزارش‌های نوبه‌ای و ارسال به قرارگاه.

ج) وزارت اطلاعات / سازمان اطلاعات سپاه / سازمان اطلاعات فراجا

پشتیبانی اطلاعاتی از مأموریت‌های قرارگاه در چارچوب سیاست‌های پدافند غیرعامل الکترونیک با انجام وظایف زیر، برعهده دارند:
۱) تبادل اطلاعات در مورد تهدیدات الکترونیک با قرارگاه؛
۲) تعامل امنیتی-عملیاتی با قرارگاه در مورد برنامه‌ها و آسیب‌پذیری‌های الکترونیک کشور؛
۳) کمک به قرارگاه در پاسخگویی به شرایط اضطراری الکترونیک در وضعیت‌های نارنجی و قرمز؛
۴) همکاری در مدیریت صحنه بحران‌ها و رخدادهای الکترونیک در شرایط دفاع الکترونیک در وضعیت‌های عملیاتی نارنجی و قرمز؛

د) سازمان پدافند غیرعامل کشور

۱) سازماندهی و فعالسازی قرارگاه پدافند غیرعامل الکترونیک کشور و هدایت و راهبری یگان‌های تخصصی عملیاتی فاتح در قرارگاه و سایر دستگاه‌های اجرایی؛
۲) راه اندازی و فعالسازی مرکز فرماندهی کنترل و پایش فضای الکترونیک کشور(EDOC)؛
۳) پایش، رصد و تشخیص تهدیدات و کشف آسیب‌پذیری‌ها، وابستگی‌های متقابل، مخاطرات و پیامدهای ناشی از اثر تهدیدات در حوزه‌های ۱۰گانه الکترونیک؛

فرماندهی کل قوا

[۴] Electronic Emegency Response Team

۴) راهبری و نظارت بر مصون‌سازی زیرساخت‌های حیاتی، حساس، مهم و قابل‌حفاظت الکترونیکی و وابسته به آن در برابر تهدیدات الکترونیک؛

۵) طرح‌ریزی عملیاتی، هدایت، راهبری و مدیریت سطح ملی پدافند غیرعامل الکترونیک در وضعیت‌های مختلف عملیاتی؛

۶) هدایت، راهبری و نظارت بر طرح‌ریزی، آموزش، تمرین، رزمایش و آمادگی عملیاتی پدافند غیرعامل الکترونیک در حوزه‌های ۱۰گانه الکترونیک؛

۷) طبقه‌بندی و سطح‌بندی زیرساخت‌های الکترونیک و دارایی‌های وابسته به آن در مراکز حیاتی، حساس، مهم و قابل حفاظت ازمنظر نقش و کارکرد و میزان وابستگی به فضای الکترونیک و پیامدهای حذف آن؛

۸) عضویت در کمیسیون تنظیم مقررات ارتباطات موضوع آیین‌نامه شماره ۷۶۲۰۰ ت ۳۰۵۸۲هـ مورخ ۱۳۸۳/۱۲/۲۴ هیئت وزیران به‌منظور حصول اطمینان از اجرای مصوبات کمیته دائمی و احتمال استفاده دشمن از شبکه‌های ارتباطی، مخابراتی و الکترونیکی کشور(موضوعات اصلی پدافند الکترونیک کشور)؛

۹) هدایت و راهبری دفاع جمعی الکترونیک و دفاع حقوقی الکترونیک؛

۱۰) هماهنگی عملیات مشترک پدافند غیرعامل الکترونیک کشوری و دفاع الکترونیک لشکری.

تبصره- قرارگاه، اقدامات عملیاتی پدافند غیرعامل الکترونیک را در چارچوب سیاست‌های دفاعی و عملیاتی ستاد کل نیروهای مسلح انجام می‌دهد.

۵) سپاه پاسداران انقلاب اسلامی/ فرماندهی سایبرالکترونیک

ظرفیت‌های پشتیبانی اطلاعاتی و عملیاتی فرماندهی سایبرالکترونیک و سایر ظرفیت‌های سایبرالکترونیک سپاه برای انجام وظایف زیر، بنا به دستور در کنترل عملیاتی قرارگاه قرار می‌گیرد؛

۱) ایفاء نقش عمل‌کلی و احتیاط دفاع الکترونیک کشوری؛

۲) کمک به قرارگاه در شرایط عملیاتی و انجام رزمایش‌های مشترک؛

۳) مشارکت در تولید تجهیزات الکترونیک پدافند غیرعاملی؛

۴) مشارکت در اجرای آزمایش‌های تخصصی الکترونیک، آزمون‌های نفوذ و پایداری و اختلالات داخلی الکترونیک.

و) وزارت علوم، تحقیقات و فناوری

۱) توسعه علمی رشته‌های علمی موردنیاز در عرصه‌های پدافند غیرعامل الکترونیک؛

۲) اختصاص حداقل یک دانشکده برای توسعه و آموزش رشته‌های مرتبط با پدافند غیرعامل الکترونیک؛

۳) مساعدت و حمایت از انجمن‌های علمی حوزه پدافند غیرعامل الکترونیک و سایبری؛

۴) توسعه آزمایشگاه‌های مرجع تشخیص تهدیدات، مخاطرات و آسیب‌پذیری‌های پنهان در ذات فناوری.

ز) وزارت صنعت، معدن و تجارت

۱) حمایت از صنعت پدافند غیرعامل الکترونیک بومی کشور؛

۲) حمایت و پشتیبانی از راهبردهای عملیاتی و زیرساختی قرارگاه.

ح) وزارت اقتصاد و دارایی- گمرک ج.ا.ایران

۱) کنترل ورود تجهیزات الکترونیک از منظر تهدیدات و مخاطرات و آسیب‌پذیری‌های در ذات فناوری و پنهان با راهبری قرارگاه و با همکاری مبادی ذی‌ربط.

تبصره- مفاد این سند، نافی مسئولیت‌ها و وظایف ذاتی دستگاه‌های اجرایی در حوزه‌های ۱۰گانه الکترونیک نبوده و هریک از دستگاه‌های متولی موظف به اجرای تکالیف و مأموریت‌های قانونی خود می باشند.

ماده ۲۰– دستورات هماهنگی

در وضعیت‌های عملیاتی، بازیگران اصلی با هماهنگی قرارگاه، اقدامات پایش، رصد و تشخیص تهدیدات و آسیب‌ها، هشدار و تعیین وضعیت و کشف آسیب‌پذیری، امن‌سازی اضطراری (برطرف‌سازی سریع آسیب‌های کشف شده)، مصون‌سازی جامع (درصورت وجود فرصت لازم)، اعمال و کنترل الزام و ملاحظات پدافند غیرعامل الکترونیک، ایجاد آمادگی متناسب با وضعیت هشدارها و بازیابی سامانه‌ها را انجام می‌دهند.

۱) مسئولیت انجام عملیات پدافند غیرعامل الکترونیک (پایش و رصد، مصون‌سازی، پیشگیری و مقابله با حوادث) مربوط به هر دستگاه با هدایت و راهبری قرارگاه بر عهده بالاترین مقام آن دستگاه می‌باشد.

۲) عملیات پدافند غیرعامل الکترونیک در زیرساخت‌های با اهمیت بالا تا پایین‌ترین سطح موردنیاز با هماهنگی، هدایت و راهبری قرارگاه توسط مسئولان دستگاه‌های اجرایی و زیرساخت‌ها تداوم می‌یابد.

۳) قوه قضائیه/دادستانی کل کشور در وضعیت‌های وضعیت سفید، زرد، نارنجی و قرمز، عملیات پدافند غیرعامل الکترونیک را پشتیبانی و حمایت قضایی می‌نماید.

ماده ۲۱– دستگاه‌های اجرایی دارای زیرساخت‌های الکترونیکی و وابسته به آن موظفند منطبق با سازوکار اختصاصی و داخلی خود، پیش‌نویس برنامهٔ سالیانهٔ در حوزه پدافند غیرعامل الکترونیک خود را تهیه و ظرف یک ماه، در قالب توافقنامه به سازمان پیشنهاد و ارسال کنند.

ماده ۲۲ – اعتبارات و منابع مالی موردنیاز برای اجرای تکالیف مقرر در این دستورالعمل، حسب مورد باید در بودجه سالانه دستگاه اجرایی مربوط منظور شود. اشخاص بخش غیردولتی مکلفند منابع مالی موردنیاز برای اجرای ضوابط و الزامات پدافند غیرعامل را در حوزه خود منظور کنند.

ماده ۲۳ – سازمان موظف است ضمن نظارت بر حسن اجرای این سند، هرگونه قصور و کوتاهی در اجرای این مصوبه را به مراجع ذی‌ربط گزارش کنند تا برابر مقررات با فرد متخلّف برخورد شود. با مستنکفان از اجرای این سند، براساس آیین‌نامه شماره ۱/۳۱۰۱/ک۱۶۰ مورخ ۱۴۰۴/۰۲/۰۸ مصوب کارگروه دائمی، برخورد می‌شود.

ماده ۲۴ – سازمان بر حسن اجرای این مصوبه، نظارت و اجرای آن را به‌صورت سالانه به کارگروه دائمی گزارش کند.

ماده ۲۵ – این آیین‌نامه مشتمل بر بیست‌وپنج ماده و چهار تبصره در یکصدویکمین جلسه کارگروه دائمی به تاریخ بیست و پنجم آبان‌ماه سال یک‌هزار و چهارصد و چهار هجری شمسی به‌تصویب رسید و از تاریخ ابلاغ، لازم‌الاجراست.

سند راهبردی پدافند غیرعامل الکترونیک کشور، مشتمل بر بیست‌وپنج ماده و چهار تبصره که در تاریخ ۱۴۰۴/۰۸/۲۵ در یکصد و یکمین جلسه کارگروه(کمیته) دائمی پدافند غیرعامل کشور به‌تصویب رسید، به استناد تبصره۱ قانون تشکیل سازمان پدافند غیرعامل کشور برای اجرا ابلاغ می‌گردد./

رئیس ستاد کل نیروهای مسلح
و کمیته دائمی پدافند غیرعامل کشور
سرلشکر سید عبدالرحیم موسوی

فرماندهی کل قوا
کمیته دائمی پدافند غیرعامل کشور

رونوشت:

دفتر فرماندهی معظم کل قوا – دفتر رئیس جمهوری اسلامی ایران – دفتر رئیس قوه قضاییه– دفتر رئیس مجلس شورای اسلامی – دفتر معاون اول رئیس‌جمهور– دفتر رئیس ستاد کل نیروهای مسلح – دبیرخانه شورای‌عالی امنیت ملی ج.ا.ایران– دبیرخانه شورای امنیت کشور– کلیه وزارتخانه‌ها، سازمان‌ها، مؤسسات دولتی، نهادهای انقلاب اسلامی و سازمان‌های نیروهای مسلح – سازمان بازرسی کل کشور – دیوان محاسبات کشور– دیوان عدالت اداری– معاونت قوانین مجلس شورای اسلامی – امور تدوین، تنقیح و انتشار قوانین و مقررات – دفتر هیئت دولت– روزنامه رسمی جمهوری اسلامی ایران