نظام عملیاتی پدافند سایبری کشور

به‌استناد مادهٔ ۸ اساسنامهٔ سازمان پدافند غیرعامل کشور مصوّب مقام‌معظّم رهبری و فرماندهی کلّ قوا(مدظله‌العالی) درتاریخ ۱۳۹۸/۰۲/۳۱ سی‌وچهارمین جلسهٔ کمیتهٔ دائمی (شورای‌عالی) پدافند غیرعامل کشور تشکیل و نظام عملیاتی پدافند سایبری کشور موضوع مادّه نه اساسنامه، پیشنهادی آن سازمان را بررسی و به‌شرح زیر تصویب نمود:

مقدمه:

بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور، در کلیه سطوح، اعم از افراد، موسسات غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور، یا خود بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشور نیز، به این فضا منتقل و یا اساساً در این فضا، شکل گرفته است. به‌عبارت‌دیگر، وجوه مختلف امورکشور به خصوص امور دفاعی و امنیتی و حتی خدمات عمومی و حریم خصوصی افراد به معنای واقعی، با این فضا در آمیخته و هرگونه بی‌ثباتی، ناامنی و چالش در این حوزه، مستقیماً آن‌ها را متاثر خواهد نمود.

مروری بر وقایع و حوادث سال‌های اخیر کشور، مؤید این واقعیت است که بخش عمده‌ای از تهدیدها و حملات سایبری موجود علیه کشور مانند حمله استاکس‌نت به تاسیسات هسته‌ای نطنز در سال ۱۳۸۹، فلیم، دوکو در زیرساخت‌های نفت و گاز و غیره، به‌ویژه در زیرساخت‌های حیاتی و حساس، یا مستقیماً از فضای سایبر نشأت گرفته و یا این فضا را هدف تهدید مستقیم خود قرار می‌دهند.

نظام عملیاتی پدافند سایبری کشور، نمایانگر نحوهٔ تحقّق پدافند سایبری در سطح

عملیاتی، درنتیجهٔ انجام مأموریت‌های عملیاتی توسط نیروهای پدافند سایبری در وضعیت‌های عملیاتی مختلف مواجهه با سناریوهای محتمل تهاجم سایبری دشمن علیه قلمرو سایبری جمهوری اسلامی ایران است. این نظام، تفکّر (اصول، رویکرد، خط‌مشی، اهداف و راهبردهای) عملیاتی پدافند سایبری، تدبیرعملیات پدافند سایبری، نحوهٔ انجام این مأموریت‌ها (طرح اقدام) و تقسیم کار (نگاشت نهادی) بین کنشگران را برای هر یک از وضعیت‌های عملیاتی، نشان می‌دهد.

سند حاضر، به‌منظور ارتقاء آمادگی و پاسخ‌گویی در شرایط اضطراری سایبری در کشور و در راستای هم‌افزایی و اثربخشی کنشگران تهیه و تدوین شده است.

ماده ۱. تعاریف و اختصارات:

اصطلاحات و واژگان به‌کار رفته در این سند، دارای معانی مشروح زیر است؛

۱)**سازمان:** سازمان پدافند غیرعامل کشور

۲)**قرارگاه پدافند سایبری کشور:** 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 عملیاتی پدافندسایبری و دفاع حقوقی در برابر تهدیدات و حملات دشمن را بر عهده دارد.(سند راهبردی پدافند سایبری کشور)

۳)**نظام عملیاتی پدافند سایبری کشور:** بازنمایی‌کنندهٔ نحوهٔ تحقّق مأموریت‌های پدافند سایبری کشور، در سطح عملیاتی است. نظام جامع عملیات پدافند سایبری برای این منظور، ضمن ترسیم «الزامات قانونی و مبانی نظری پدافند سایبری» و تبیین «محیط عملیات پدافند سایبری و ویژگی‌های آن»، «اصول و قواعد اساسی عملیات پدافند سایبری»، «فعالیت‌های اساسی عملیات پدافند سایبری»، «نحوهٔ تحقّق

فعالیت‌های اساسی عملیات پدافند سایبری» و «اختیارات، نقش‌ها و مسؤولیت‌ها» در اجرای عملیات پدافند سایبری را تعیین و تبیین می‌نماید.

۴)قدرت سایبری: مولّفه‌ای از قدرت ملی است که معنی و مفهوم آن حفظ اقتدار کشور در قلمرو و مرزهای سایبری با تاکید بر اعمال حاکمیت ملی، حفظ برتری‌های راهبردی و حفاظت از سرمایه‌های سایبری و وابسته به سایبرکشور در برابر تهدیدات و حملات سایبری و ایجاد بازدارندگی به‌منظور خنثی‌سازی و مقابله با اقدامات دشمن با به‌کارگیری همه ظرفیت‌ها و قابلیت‌های سایبری کشور می‌باشد

۵)اشراف اطلاعاتی: مجموعه فعالیت‌ها و اقداماتی است که در اثر اجرای آن، یک سازمان قابلیت احاطه و تسلط کامل بر روند گذشته، حال و آینده وقایع و حوادث حوزه پیرامونی آن را به‌دست می‌آورد به‌نحوی‌که در جهت پیشگیری و مقابله با تهدیدات و آسیب‌پذیری‌های مترتب بر آن و همچنین تولید فرصت به‌موقع اقدام کند.

۶)فضای سایبری: به شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده (جاگذاری شده)، کنترل‌کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات گفته می‌شود که ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی، در آن تعبیه شده باشد. (سند راهبردی پدافند سایبری کشور)

۷)سرمایه ملی سایبری: بخشی از دارایی‌های کشور اعم از زیرساخت‌ها، سامانه‌ها، تجهیزات، نرم افزارها، اطلاعات و حتی افراد که در فرآیند تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره‌برداری از داده‌های دارای اهمیت حیاتی، حساس و مهم در فضای سایبری کشور نقش مستقیم و تعیین کننده داشته باشند، سرمایه ملی سایبری نامیده می‌شود. سرمایه‌های سایبری در سه دسته فیزیکی، اطلاعاتی و ادراکی شناختی تقسیم‌بندی می‌شوند. (سند راهبردی پدافند سایبری کشور)

۸)زیست‌بوم سایبری: به محیط بومی متشکل از زیرساخت‌های فناوری‌اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، که به‌صورت زنده و پویا با عوامل انسانی در تعامل می‌باشد زیست‌بوم سایبری گفته می‌شود. (سند راهبردی پدافند سایبری کشور)

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

۱۰)تهدید سایبری: هر گونه عاملی که قابلیت وارد نمودن ضربه به ماموریت‌ها، وظایف، تصویر (پنداره) یا اشتهار دستگاه متولی سرمایه ملی سایبری یا افراد مرتبط، به‌واسطه یك سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام (تخریب)، افشاء، تغییر اطلاعات و ایجاد اختلال یا ممانعت از ارائه خدمات را داشته باشد تهدید سایبری گفته می‌شود. انواع تهدید سایبری که نظام پدافند سایبری با آن مواجه است، شامل تهدید ناشی از دولت یک کشور، سازمان‌های غیردولتی (اعم از رسمی و غیررسمی، مشروع و غیرمشروع)، گروه‌های کوچک و افراد حقیقی است. (سند راهبردی پدافند سایبری کشور)

۱۱)تهدیدات ترکیبی: به تهدیداتی که ترکیبی از دو یا چند تهدید از حوزه‌های مختلف شامل تهدیدات نظامی، زیستی، پرتوی، شیمیایی، سایبری و سایر حوزه‌ها به‌صورت هم‌زمان یا مکمل یکدیگر طرح‌ریزی می‌شود، اطلاق می‌گردد.

۱۲)سطوح تاثیر تهدیدات سایبری عبارتند از:

۱. **فراملی:** منافع و سرمایه‌های سایبری کشور در سطح جهانی

۲. **ملی:** بخش گسترده‌ای از فضای سایبری و منافع و سرمایه‌های سایبری کشور

۳. **منطقه‌ای:** فضای سایبری، منافع و سرمایه‌های سایبری یک یا چند استان کشور

۴. **محلی:** فضای سایبری، منافع و سرمایه‌های سایبری یک یا چند شهر کشور

۵. **سرمایه‌ای:** یک یا چند سرمایه ملی سایبری

۶. **سازمانی (دستگاهی):** فضای سایبری یک یا چند دستگاه

۷. فردی: یک یا چند فرد در فضای سایبر

۱۳) آسیب‌پذیری سایبری: به ضعف، نقص و عیب موجود در داخل یک سرمایه ملی سایبری، رویه‌های امنیتی یا کنترل‌های داخلی، یا پیاده‌سازی آن سرمایه ملی سایبری، که قابلیت بهره‌برداری یا فعال‌شدن تهدیدات داخلی و خارجی به‌منظور تهاجم و یا جنگ سایبری را داشته باشد، اطلاق می‌گردد. (سند راهبردی پدافند سایبری کشور)

۱۴) مصون‌سازی: اقداماتی است که سبب می‌شود تاثیر تهدیدات دشمن بر زیرساخت، جامعه و پیکره کشور، کاهش، در حد صفر و یا بی‌اثر شود. این اقدامات شامل اقدامات ایمنی و امنیتی بوده که درصورت وقوع حوادث ناشی از تهدید کمترین آسیب به دارائی‌های سایبری وارد گردد.

۱۵) زیرساخت: به مجموعهٔ از مراکز و بخش‌های فعّال اعم از تجهیزات، امکانات و خدمات در فرایند تولید، تبدیل، انتقال، توزیع و انتشار درحوزه‌های مختلف از قبیل؛ "برق" ، "مخابرات و ارتباطات از راه دور"، "مواد و انرژی هسته‌ای"، "سیستم‌های اطلاعات دولتی و خصوصی" ، "حمل و نقل اعم از راه آهن، بزرگراه، بنادر و راه‌های آبی، فرودگاه‌ها" ، "شبکه‌های بهداشت، درمان و سلامت انسان، دام و محیط‌زیست" ، "سامانه‌های کشاورزی" و موارد مشابه، زیرساخت گفته می‌شود. که به‌صورت ویژه، حیاتی، حساس، مهم و قابل حفاظت دسته‌بندی می‌شوند.

۱۶) زیرساخت‌های حیاتی سایبری: آن دسته از زیرساخت‌های سایبری و وابسته به سایبر هستند که نقش و کارکرد در مقیاس ملی دارند و پیامد توقف کارکرد، حذف و تخریب آن، به امنیت ملی کشور ضربه زده و میزان وابستگی آن به فضای سایبر می‌تواند مخاطره‌آمیز باشد.

۱۷) زیرساخت‌های حساس سایبری: آن دسته از زیرساخت‌های سایبری و وابسته به سایبر هستند که نقش و کارکرد در مقیاس منطقه‌ای دارند و پیامد توقف کارکرد، حذف و تخریب آن، امنیت منطقه‌ای از کشور را مخدوش و میزان وابستگی آن به فضای سایبر مخاطره منطقه‌ای دارد.

۱۸) زیرســـاخت‌های مهم ســـایبری: آن دسته از زیرساخت‌های ســـایبری و وابسته به ســـایبر هستند که نقش و کارکرد در مقیاس محلی دارند و پیامد توقف کارکرد، حذف و تخریب آن، امنیت بخشـــی از کشـــور را مخدوش و میزان وابستگی آن به فضای سایبر مخاطره محلی دارد.

۱۹) دارایی: اطلاعات، خدمات، شبکه‌ها، و سامانه‌های سخت‌افزاری و نرم‌افزاری افراد، سازمان‌ها
و زیرساخت‌های کشور است.

۲۰)شـــرایط اضطرار سایبری: به شـــرایط مخاطره‌آمیزی که در آستانه, حین و یا پس از وقوع یک
حادثه ســـایبری یا مرتبط با ســـایبر، ایجاد و جریان عادی زندگی مـــردم را از تعادل خارج می‌کند،
می‌گویند.

۲۱)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 دســـتیابی به اطلاعات انجام گیرد تهاجم ســـایبری گویند. (ســـند راهبردی پدافند سایبری کشور)

۲۲)جنگ ســـایبری: بالاترین ســـطح و پیچیده ترین نوع از تهاجم ســـایبری که توسط ارتش سایبری کشورهای مهاجم یا گروه‌های سازماندهی شده تحت حمایت دولت‌های متخاصم یا سلاح‌های سایبری، تحت‌کنترل یا رهاشده توسط آن‌ها علیه منافع ملی کشورها انجام می‌شود و سبب تخریب فضای سایبری یا زیرساخت حیاتی ، حساس و مهم کشور و وارد شـــدن آسیب به امنیت ملی، اقتصاد ملی، وجهه کشور در سطح بین‌المللی، روابط سیاسی و اقتصادی کشور، سلامت و ایمنی عمومی، اطمینان عمومی به اداره امور کشور شـــود جنگ سایبری است و مرجع تشخیص وقوع جنگ سایبری علیه جمهوری اسلامی ایران، شورای‌عالی امنیت ملی است.

۲۳)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، کاهش آسیب‌پذیری و حفاظت از سرمایه‌های ملی سایبری و زیست‌بوم سایبری کشور شود و با تولید بازدارندگی امکان تهاجم سایبری را از کلیه متخاصمین سلب نماید.

۲۴)دیپلماســـی پدافند سایبری: به دفاع حقوقی ازمنافع ملی، تعامل و تبادل اطلاعات در قالب پیمان‌های مشترک سایبری بین کشورها دیپلماسی پدافند سایبری گفته می‌شود.

۲۵)ســـامانه پایش، هشـــدار، خنثی‌ســـازی: به‌مجموعه‌ای نظام یافته و منســـجم از ســـخت‌افزار و نرم‌افزارهایی که در یک شـــبکه به‌هم‌پیوســـته و هوشمند ســـازماندهی و ساماندهی شـــده و تهدیدات متصور بر مراکز و زیرساخت‌های حیاتی، حساس و مهم را مراقبت و پایش نموده و احتمال و امکان بروز تهدید را اعلام و خنثی‌ســـازی آن را راهبری می‌نماید، گفته می‌شود.

۲۶)عملیات پدافند ســـایبری: مجموعه اقدامات عملیاتی در فضای ســـایبر اعم از عامـــل و غیرعامل که به‌منظـــور حفظ توانمندی‌ها و قابلیت‌هـــای نیروهای خودی در راستای بهره‌گیری از امکانات فضای سایبر و حفاظت از داده‌ها، شبکه‌ها و قابلیت‌های مبتنی بر شبکه، زیرساخت‌های سایبری و وابسته به سایبر و سایر سامانه‌های تعیین شده صورت می‌گیرد.

۲۷)دســـتگاه اجرایی: کلیه وزارتخانه‌ها، مؤسســـات دولتی، مؤسســـات یا نهادهای عمومی غیردولتی، شـــرکت‌های دولتی و کلیه دســـتگاه‌هایی که شـــمول قانون بر آن‌ها مســـتلزم تصریح و یا ذکر نام است از قبیل شـــرکت ملی نفت ایران، سازمان گسترش و نوســـازی صنایع ایران، بانک مرکزی، بانک‌ها و بیمه‌های دولتی، دســـتگاه‌های اجرایی نامیده می‌شوند.(موضوع ماده۵ قانون مدیریت خدمات کشوری)

۲۸)حادثه: آن دسته از رخدادهایی که موجب نقض اصول و سیاست‌های امنیت فضای سایبری(مورد تأیید قرارگاه پدافند سایبری کشور) شود.

۲۹)پیشگیری: اقداماتی است که برای جلوگیری از استفاده دشمن از آسیب‌پذیری و وقوع و یا بروز حادثه یا ایجاد خسارت انجام می‌شوند.

۳۰)مقابله: اقداماتی است که برای توقف تهدید، حمله یا حادثه و ممانعت از توسعه، رفع یا کاهش خسارات ناشی از آن‌ها انجام می‌شود.

ماده ۲. اسناد بالا دستی:

۱)فرامین، تدابیر و رهنمودهای مقام معظم رهبری(مد ظله العالی)

۲)سیاست‌های کلی نظام در حوزهٔ پدافند غیرعامل

۳)قانون برنامه ششم توسعه کشور (مواد ۱۰۶، ۱۰۷ و ۱۰۹)

۴)اساسنامهٔ سازمان پدافند غیرعامل کشور

۵)تدابیر مقام معظم رهبری(مد ظله العالی) در هیئت عالی سایبری

۶)سند راهبردی پدافند غیرعامل کشور

۷)سند راهبردی پدافند سایبری کشور

ماده ۳.قلمرو :

الف) زیرساخت‌های فضای سایبری کشور

ب) دارایی‌ها و سرمایه‌های ملی سایبری و وابسته به سایبر در زیرساخت‌های ویژه، حیاتی، حساس و مهم

ماده ۴.هدف:

تدوین نظام عملیاتی پدافند سایبری کشور و تعریف عناصر اصلی مشارکت‌کننده در عملیات پدافند سایبری در برابر تهاجم دشمنان و تعیین روابط، نقش‌ها و وظائف آن‌ها درجهت هماهنگی و هم‌افزائی و اثربخشی هرچه بیشتر بین کنشگران در عملیات پدافند سایبری.

ماده ۵. اصول عملیاتی پدافند سایبری کشور:

اصول عملیات پدافند سایبری عبارت است از: صیانت، ممانعت، مانایی، یکپارچگی،

مشـــارکت، دفاع جمعی، آمادگی، انطباق‌پذیری، تاب‌آوری، آگاهی وضعیتی، آینده‌نگری (پیش‌بینی)وپیش‌کنش‌گری

۱)**صیانت:** عالی‌ترین ســـطح محافظت، که موجب تأمین بالاترین ســـطح از امنیت (مصونیت) برای سرمایه ســـایبری در مقابل انواع تهدیدها و حملات سایبری خواهد شد.

۲)**ممانعت:** جلوگیری‌کردن از وقوع تهدید، حمله و حادثه سایبری که میزان خسارت جانبی را محدود و از صرف نیروی غیرضروری جلوگیری خواهد نمود.

۳)**مانایی:** برخورداری فعالیت‌های پدافند سایبری از ماندگاری و استمرار کافی، برای مقابله مؤثر با تهدیدهای پیشرفته پایدار.

۴)**یکپارچگی:** حفظ انســـجام در برنامه‌ریزی و اجرای عملیات پدافند ســـایبری، با عملیات آفند ســـایبری و عملیات غیرسایبری به‌منظور برخورداری از اثربخشی کافی و ایجاد بازدارندگی.

۵)**مشـــارکت و هم‌افزایـــی:** تعمیق همـــکاری، هماهنگی، مشـــارکت حداکثری و هم‌افزایی تمام نیروهای پدافند ســـایبری اعم از متولیان سرمایه‌های حیاتی و حساس سایبری و وابسته به ســـایبر، یگان‌های سایبری نیروهای مســـلح، بخش‌های دولتی و غیردولتی در عملیات پدافند سایبری.

۶)**دفاع جمعی:** عملیات پدافند ســـایبری در مقابل جنگ سایبری و جنگ ترکیبی، با منشأ یک ائتلاف منطقه‌ای یا بین‌المللی، باید با مشارکت جمعی تمام نیروهای پدافند سایبری داخلی اعم از لشکری و کشوری و غیردولتی و آحاد مردم، به‌همراه هم‌پیمانان سایبری کشور انجام گیرد.

۷)**آمادگی:** نیروهای پدافند سایبری و سرمایه‌های حیاتی و حساس سایبری و وابسته به ســـایبر، باید به‌صورت مداوم نســـبت به توســـعه قابلیت‌ها و ارتقاء توانایی، همواره آمادگی مواجههٔ مؤثر با تهدید، آســـیب‌پذیری، حمله، جنگ، حادثه و پیامد سایبری و غیرسایبری ناشی از آن را داشته باشند.

۸)**انطباق‌پذیری:** نیروهای پدافند ســـایبری و ســـرمایه‌های حیاتی و حساس سایبری

و وابسته به ســـایبر، باید قابلیت تطبیق ســـریع وضعیت و اقدام‌های خود، با وضعیت دشمن، حمله سایبری و محیط عملیات را داشته باشند.

۹)تاب‌آوری: توانایی تداوم یا بازگشـــت به عملکرد عادی در صورت وقوع برخی از اختلال‌ها، اعم از طبیعی یا انسانی، و عمدی یا غیرعمدی است.

۱۰) آگاهی وضعیتی: برخورداری نیروهای ســـایبری خـــودی از اطلاعات، تحلیل و ارزیابی دوره‌ای و منظّم وضعیت ســـرمایه‌ها، امکانات، توانایی، نیّت و انگیزهٔ نیروهای سایبری دشمن است.

۱۱) آینده‌نگری (پیش‌بینی) : برخورداری دوره‌ای و منظّم نیروهای ســـایبری خودی از تحلیل روند و وضعیت احتمالی آیندهٔ ســـرمایه‌ها، امکانات، توانایی، نیّت و انگیزه‌ی نیروهای سایبری دشمن است.

۱۲) پیش‌کنش‌گری: تمرکز بر دســـته‌ای از مأموریت‌های پدافند ســـایبری، که زمان اجرای آن‌ها در دوره‌ی زمانی قبل از وقوع جنگ ســـایبری است. به‌عبارت‌دیگر، تمرکز مأموریت‌های پدافند سایبری بر مواجههٔ مؤثر با آسیب‌پذیری‌ها و تهدیدهای سایبری و ممانعت از ایجاد مخاطرات سایبری و وقوع جنگ سایبری است.

ماده ۶. سیاست‌های عملیاتی پدافند سایبری:

سیاست‌های عملیات پدافند سایبری به‌شرح زیر است؛

۱)پرهیز از هرگونه غافلگیری

۲)تناســـب اقدام‌های پدافند ســـایبری، با ویژگی‌های کلیدی اهمیت سرمایه سایبری، تهدید ســـایبری، آسیب‌پذیری ســـایبری، مخاطره ســـایبری، تهاجم سایبری دشمن و پیامدهای سایبری، شناختی و فیزیکی ناشی از جنگ سایبری

۳)اتّکاء به تـــوان داخلی، محصولات بومی و به‌ویژه معمـــاری پدافندی اختصاصی (بومی)

۴)عدم اعتماد به سامانه‌ها و خدمات خارجی

۵)تمرکز بر عملیات پدافند سایبری براساس اولویت پیش‌بینانه، پیش‌گیرانه، پیش‌کنشگرانه، واکنش‌گرایانه و منفعلانه

۶)صیانت از دارایی‌های معنوی و افکار عمومی، دارایی‌های شبکه‌ای-جزیره‌ای، سامانه‌های کنترل صنعتی و دارایی‌های سایبری

۷)تمرکز بر مواجهه با عملیات ترکیبی دشمن از طریق فضای سایبر براساس اولویت مواجهه با عملیات ترکیبی سایبری- اجتماعی، سایبری-فیزیکی و سایبری-سایبری

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

۹)افزایش حداکثری و مداوم زمان دسترسی و دستیابی دشمن به آسیب‌پذیری سایبری، سرعت پیش‌بینی، تداوم کارکردهای ضروری و دقّت پاسخ

ماده ۷. زمان اجرای عملیات پدافند سایبری:

عملیات پدافند سایبری، در چهار محدودهٔ زمانی پیش از جنگ سایبری، در آستانه جنگ سایبری، حین جنگ سایبری و پس از جنگ سایبری اجرا می‌شود و به‌ترتیب معادل عملیات پدافند سایبری پیش‌گیرانه، پیش‌کنشگرانه، واکنش‌گرایانه و منفعلانه است. تمرکز اصلی نظام عملیاتی پدافند سایبری، بر مأموریت‌های پیش‌گیرانه در محدودهٔ زمانی پیش از جنگ سایبری است و عملیات چهارگانه پدافند سایبری براساس اصل آینده‌نگری(پیش‌بینی) باید الزاماً توسط عملیات پیش‌بینانه پشتیبانی شوند.

ماده ۸. سطوح عملیات پدافند سایبری:

عملیات پدافند سایبری، در سه سطح زیرساختی، حوزه‌ای و ملی انجام و تحت عناوین درگیری سایبری، نبرد سایبری، جنگ سایبری، جنگ ترکیبی سایبری-شناختی و جنگ تمام عیار دسته‌بندی می‌شوند.

۱)عملیات پدافند سایبری زیرساختی، در مقابل تهاجم سایبری علیه یک دارایی

حیاتی یا حساس سایبری یا وابسته به سایبر با نقش و کارکرد زیرساختی و قدرت تولید مخاطرات محلی انجام و درگیری سایبری نامیده می‌شود.

۲)عملیات پدافند سایبری حوزه‌ای، در مقابل تهاجم سایبری گسترده علیه یک دارایی حیاتی یا حساس سایبری یا وابسته به سایبر برخوردار از نقش و کارکرد حوزه‌ای و قدرت تولید مخاطرات عمده انجام و نبرد سایبری نامیده می‌شود.

۳)عملیات پدافند سایبری ملی، در مقابل تهاجم سایبری گسترده علیه مجموعه‌ای از چند دارایی حیاتی یا حساس سایبری یا وابسته به سایبر است که مجموعاً نقش و کارکرد ملی و قدرت تولید مخاطرات فاجعه‌بار انجام و جنگ سایبری نامیده می‌شود.

۴)عملیات پدافند سایبری- شناختی ملی در مقابل تهاجم سایبری هم‌زمان با تهاجم شناختی گسترده علیه افکار و باورهای جامعه در یا ازطریق فضای سایبر کشور انجام و جنگ ترکیبی سایبری-شناختی نامیده می‌شود.

۵)عملیات پدافند سایبری تمام عیار که در مقابل جنگ ترکیبی سایبری-شناختی هم‌زمان با جنگ فیزیکی (غیرسایبری) علیه کشور انجام و جنگ تمام عیار نامیده می‌شود.

ماده ۹. لایه‌های عملیات پدافند سایبری:

عملیات پدافند سایبری، در عمق فضای سایبر خودی، در هشت لایه، شامل لایه‌های شبکه، ارتباطات (خطوط ارتباطی) ، سامانه اطلاعاتی، سیستم‌عامل، کاربرد، تجهیزات انتهایی، محتوا (داده) و دسترسی فیزیکی به مورد اجرا گذاشته می‌شود.

ماده ۱۰. وضعیت‌های عملیات پدافند سایبری:

وضعیت سایبری، 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 سایبر یا ازطریق این فضا می‌باشد.

ماده ۱۱. مأموریت‌های عملیاتی پدافند سایبری:

قرارگاه پدافند سایبری در چارچوب تدابیر و سیاست‌های دفاعی و در یک بهم

پیوستگی منسجم با بخش‌های آفندی سایبری انجام اقدامات عملیات پدافند سایبری زیر در دستگاه‌های اجرایی و زیرساخت‌های حیاتی، حساس و مهم کشور را به‌منظور حفاظت و صیانت از فضای سایبری و سرمایه‌های سایبری کشور، با به‌کارگیری ظرفیت‌های عمل کلی دفاع سایبری هدایت، راهبری، پشتیبانی و نظارت می‌نماید:

۱)تهیهٔ برآورد اطلاعاتی از تهدیدات سایبری دشمن و به‌روزرسانی آن

۲)شناسایی و تهیهٔ برآورد از آسیب‌پذیری‌های سایبری، نقاط ضعف قابلیت‌های پدافند سایبری و مخاطرات سایبری، فیزیکی و شناختی ناشی از آن‌ها

۳)صیانت همه‌جانبه، چندلایه و تطبیق‌پذیر از دارایی‌های حیاتی و حساس سایبری و وابسته به سایبر کشور در مقابل تهدیدات سایبری دشمن

۴)آگاهی‌رسانی، هشداردهی، آموزش، تمرین و آزمون هماهنگی و آمادگی قابلیت‌ها و نیروهای پدافند سایبری

۵)ممانعت از انجام، تشخیص، انتساب و دفع تجاوز سایبری و کنترل پیامدهای آن

۶)پاسخ متناسب و/یا تنبیهی به تجاوز سایبری دشمن با هماهنگی نظام آفند سایبری

۷)بازیابی پیامدهای تجاوز سایبری و افزایش آمادگی پدافند سایبری

۸)اقناع افکار عمومی خودی، بی‌طرف و دشمن درخصوص محکومیت جنگ سایبری و ثبت ادله قانونی اثبات تجاوز سایبری و دیپلماسی سایبری

۹)دفاع جمعی باهمکاری کشورهای همسو در برابر تهدیدات ائتلافی سایبری

ماده ۱۲. اهداف عملیاتی پدافند سایبری کشور:

هدف کلان عملیات پدافند سایبری، بازدارندگی پدافندی سایبری یک‌پارچه‌شده با بازدارندگی آفندی سایبری است که تحقّق آن، مستلزم دست‌یابی به اهداف عملیاتی زیر می‌باشد:

(اهداف کمّی وشاخص‌های نظام عملیاتی پدافند سایبری به‌شرح پیوست۱)

۱)اشراف اطلاعاتی بر فضای سایبر و قابلیت‌ها، توانایی و آمادگی عملیات سایبری دشمن و پدافند سایبری خودی

۲)آمادگی عملیاتی قابلیت‌ها و نیروهای پدافند سایبری

۳)مصونیّت دارایی‌های حیاتی و حساس سایبری و وابسته به سایبر در مقابل هر نوع تهدید سایبری

۴)تاب‌آوری و تداوم کارکردهای ضروری دارایی‌های حیاتی و حساس سایبری و وابسته به سایبر در مقابل جنگ سایبری

۵)برتری عملیاتی نیروهای پدافند سایبری خودی بر دشمن

۶)ابقاء (ترمیم) و ارتقاء قدرت پدافندی سایبری

ماده ۱۳. تدبیر عملیاتی (چگونگی اقدام عملیات پدافند سایبری):

قرارگاه عملیاتی پدافند سایبری در چارچوب تکمیل سیاست‌های دفاعی کشور و در دفاع سایبری از فضای ملی سایبری و زیرساخت‌های حیاتی حساس و مهم کشور در برابر انواع تهدیدات سایبری با به‌کارگیری ظرفیت‌های ملی نظامی و غیرنظامی عملیات پدافند سایبری اقدامات زیر توسط دستگاه‌های اجرایی در سطوح ملی، حوزه‌ای و زیرساختی را هدایت، راهبری، پشتیبانی و نظارت می‌نماید.

الف: اشراف اطلاعاتی

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

۲)رصد، پایش، برآورد عملیاتی و اشتراک‌گذاری اطلاعات وضعیت خودی

ب : آمادگی عملیاتی

۳)تعیین وضعیت سایبری و عملیاتی، آگاهی‌رسانی و صدور هشدار سایبری

۴)توسعه تشکیلات، فرآیندها، نیروی انسانی و فناوری‌های پدافند سایبری در سطوح زیرساختی، حوزه‌ای و ملی

۵)ارتقاء مهارت، تخصص و توانایی عملیاتی نیروهای پدافند سایبری

۶)ارتقاء تجارب و آمادگی عملیاتی نیروهای پدافند سایبری با هماهنگی و مشارکت نیروهای آفند سایبری

پ : مصونیّت دارایی‌های حیاتی و حساس در مقابل هر نوع تهدید سایبری

۷)شناخت، احصاء ویژگی‌ها، ارزش‌گذاری و طبقه‌بندی دارایی‌های سایبری و وابسته به سایبر

۸)صیانت همه‌جانبه از دارایی‌های حیاتی و حساس سایبری و وابسته به سایبر در مقابل هر نوع تهدید سایبری

۹)رفع یا کاهش آسیب‌پذیری‌های سایبری، با بهره‌گیری از محصولات بومی، سازوکار اعتبارسنجی و وصله‌زنی آسیب‌پذیری

ت : تاب‌آوری و تداوم کارکردهای ضروری دارایی‌های سایبری و وابسته به سایبر در مقابل جنگ سایبری

۱۰)یک‌پارچه‌سازی، تقویت تعامل و تعمیق همکاری و مشارکت نیروهای پدافند سایبری برای افزایش انسجام و مقاومت در جنگ سایبری

۱۱)بهره‌گیری از سازوکارهای پدافند سایبری همه‌جانبه و لایه‌ای، جهت اجرای مأموریت‌های پدافند سایبری

۱۲)تطبیق‌دادن مکانیزم‌ها و سازوکارهای پدافندی سایبری، در مقابل جنگ سایبری

۱۳)اشتراک‌گذاری اطلاعات و تبادل تجارب برتر جهت تشخیص و واکنش سریع و مؤثر به جنگ سایبری و پیامدهای آن

ث : برتری عملیاتی نیروهای پدافند سایبری خودی بر دشمن

۱۴)کنترل تنش سایبری (کاهش شدّت، احتمال وقوع و اثر مخاطره سایبری) با مدیریت مخاطرات‌سایبری

۱۵)اقناع افکار عمومی خودی در خصوص محکومیت جنگ سایبری قریب‌الوقوع دشمن و مشروعیت پاسخ خودی

۱۶)تأثیرگذاری بر افکار عمومی بی‌طرف و دشمن جهت نفی مشروعیت جنگ سایبری قریب‌الوقوع و مشروعیت پاسخ خودی

۱۷)نمایش قدرت سایبری، بزرگ‌نمایی پیامدهای اقدام‌متقابل و تهدید به‌استفاده از قدرت نظامی در پاسخ به تجاوز سایبری

۱۸)یک‌پارچه‌سازی سلاح‌های پدافندی در مأموریت‌های پدافند سایبری

۱۹)شناسایی متجاوز و منشأ تجاوز سایبری، انتساب تجاوز سایبری به دشمن و مستندسازی ادلّه قانونی تجاوز سایبری

۲۰)ممانعت از تداوم تجاوز سایبری یا مقابله و دفع تجاوز سایبری دشمن ازطریق ریشه‌کنی منشأ جنگ سایبری یا ضدحمله محدود به متجاوز سایبری

۲۱)محدودسازی، قرنطینه، کنترل و پاک‌سازی پیامدهای جنگ سایبری

۲۲)پاسخ محدود تلافی‌جویانه به متجاوز سایبری یا پدافند فعال سایبری

۲۳)هماهنگی پاسخ تهاجمی سایبری و یا غیرسایبری به متجاوز سایبری

ج: ابقاء (ترمیم) و ارتقاء قدرت پدافندی سایبری

۲۴)بازیابی، ترمیم و ریشه‌کنی پیامدهای جنگ سایبری و ابقاء کارکردهای دارایی‌های حیاتی و حساس

۲۵)استیفای حقوق قانونی کشور ازطریق محکومیت سیاسی و حقوقی تجاوز سایبری در مراجع و محاکم بین‌المللی

۲۶)ابقاء و ارتقاء قابلیت‌ها، توانایی و آمادگی عملیاتی غیرعامل و فعّال پدافند سایبری

ماده ۱۴.نقش‌های کنشگران:

کنشگران نظام عملیاتی پدافند سایبری، یکی از چهار نقش راهبر، مجری، پشتیبان و همکار در مأموریت‌های عملیاتی پدافند سایبری را در وضعیت‌های سفید، زرد، نارنجی و قرمز بر عهده دارند.

الف: کنشگران نقش راهبر

دستگاه‌های راهبر مأموریت‌های عملیاتی پدافند سایبری، عبارتند از شورای‌عالی امنیت ملی، شورای‌عالی فضای مجازی، ستاد کل نیروهای مسلح و قرارگاه مرکزی خاتم‌الانبیاء(ص)

ب: کنشگران نقش مجری

دستگاه‌های مجری مأموریت‌های عملیاتی پدافند سایبری، عبارتند از: ستاد کل نیروهای مسلح، قرارگاه مرکزی خاتم‌الانبیاء(ص)، قرارگاه پدافند سایبری، یگان سایبری سپاه پاسداران انقلاب اسلامی، یگان سایبری ارتش جمهوری اسلامی، پلیس فتا، یگان سایبری بسیج، وزارت اطلاعات/ مرکز مدیریت راهبردی افتا، وزارت ارتباطات و فناوری اطلاعات و سایردستگاه‌های اجرایی.

پ : کنشگران نقش پشتیبان

دستگاه‌های پشتیبان مأموریت‌های عملیاتی پدافند سایبری، عبارتند از مجلس شورای اسلامی، قوه قضائیه، سازمان صدا و سیمای جمهوری اسلامی، وزارت دفاع و پشتیبانی نیروهای مسلح ، وزارت امور خارجه، وزارت علوم، تحقیقات و فناوری و قابلیت‌های پدافند سایبری بخش دولتی و غیردولتی ازجمله مراکز آپا و آزمایشگاه‌های ارزیابی و اعتبارسنجی.

ت:کنشگران نقش همکار

دستگاه‌های همکار در اجرای مأموریت‌های عملیاتی پدافند سایبری، عبارتند از: وزارت علوم، تحقیقات و فناوری، سازمان صدا و سیمای جمهوری اسلامی، حوزه‌های علمیه، رسانه‌ها و سایر دستگاه‌های اجرایی حسب مورد.

ماده ۱۵.وظایف کنشگران (پیوست):

۱)شورایعالی امنیت ملی:

اعلام شروع و خاتمه جنگ سایبری، تعیین وضعیت نارنجی و قرمز(جنگ سایبری) به پیشنهاد قرارگاه مرکزی حضرت خاتم الانبیاء(ص) را به عهده دارد.

۲)ستاد کل نیروهای مسلح:

در شرایط سفید و زرد هدایت و راهبری قرارگاه پدافند سایبری کشور را به عهده دارد.

۳)قرارگاه مرکزی حضرت خاتم‌الانبیاء(ص):

در شـــرایط قرمز و نارنجی هدایت و راهبری (کنترل عملیاتی) قرارگاه پدافند سایبری کشور را به عهده دارد.

۴)قرارگاه پدافند سایبری کشور:

- فرماندهی، طرح‌ریزی عملیاتی،هدایت، راهبری و مدیریت سطح ملی پدافند سایبری در وضعیت نارنجی و قرمز
- راهبری و نظارت بر مصون‌سازی زیرساخت‌های حیاتی، حساس، مهم
- پایش، رصد و تشخیص تهدیدات و کشف آسیب‌پذیری‌ها در فضای سایبری
- هدایت، راهبری و نظارت بـــر طرح‌ریزی، آموزش، تمرین، رزمایش و آمادگی سایبری
- طبقه‌بندی و ســـطح بندی زیرســـاخت‌های ســـایبری و وابســـته به ســـایبر به حیاتی،حســـاس و مهم ازمنظر نقش و کارکرد و میزان وابستگی به فضای سایبر و پیامدهای حدف آن
- هدایت و راهبری دفاع جمعی سایبری و دفاع حقوقی سایبری

۵)مرکز ملی فضای مجازی:

هماهنگی دستگاه‌های کشوری برای ایجاد و ارزیابی آمادگی و اجرای عملیات پدافند سایبری

پیگیـــری و نظارت بر اجرای نظامات، دســـتورالعمل‌ها و طرح‌هـــای عملیات پدافند سایبری

۶)سپاه پاسداران انقلاب اسلامی / فرماندهی سایبرالکترونیک و بسیج سپاه:

ظرفیت‌های پشـــتیبانی اطلاعاتی و عملیاتی فرماندهی ســـایبری و سایر ظرفیت‌های ســـایبری ســـپاه برای انجام وظایف زیر بنابه‌دســـتور در کنترل عملیاتی قـــرارگاه پدافند سایبری قرار می‌گیرد؛

تهَیه طرح‌ها و انجام اقدامات عامل، پیش‌کنشانه و پیش دستانه و دفاع فعال

آماده‌سازی و عملیاتی‌سازی ظرفیت‌های لازم برای واکنش سریع به جنگ سایبری

خنثی‌سازی اقدامات ضدامنیتی دشمن و آشوبگران در فضای سایبری

۷)وزارت دفاع و پشتیبانی نیروهای مسلح:

پشـــتیبانی تخصصی از مأموریت‌های عملیاتی پدافند سایبری، از طریق توسعه صنعت بومی پدافند سایبری، ایجاد و سازماندهی ظرفیت عمل کلی زیرساختی پدافند سایبری (ازجمله آزمایشـــگاه‌ها) و پشـــتیبانی تخصصی از مرکز عملیات پدافند سایبری کشور را بر عهده دارد و ظرفیت‌های عملیاتی ســـایبری وزارت دفـــاع برای انجام وظایف زیر بنابه‌دستور در کنترل عملیاتی قرارگاه پدافند سایبری قرارمی‌دهد.

- انجام عملیات امداد و نجات سایبری در زیرساخت‌های حیاتی، حساس و مهم کشور
- جمع‌آوری ادله مثبته و جرم‌شناسی رقومی در زیرساخت‌های حیاتی، حساس و مهم کشور
- رصد تهدیدات دشـــمن و ارســـال گزارش تهدیدات و حملات احتمالی سایبری به زیرساخت‌های
  حیاتی، حساس و مهم کشور
- انجام رزمایش و ارزیابی مستمر آمادگی عملیاتی در زیرساخت‌های کشور
- طراحی، تولید و عملیاتی‌سازی تجهیزات پایه پدافند سایبری مورد نیاز در اسرع وقت.
- پایش و رصد اتحادها و معاهدات دفاعی سایبری و اتخاذ رویکرد مناسب با نیاز قرارگاه پدافند سایبری کشور.
- کمک و پشـــتیبانی در ظرفیت‌سازی و تربیت نیروی انســـانی در قالب اطلاع‌رسانی و مهارت‌آموزی

۸) وزارت اطلاعات / مرکز مدیریت راهبردی افتا:

- پشـــتیبانی اطلاعاتـــی از مأموریت‌های عملیاتـــی پدافند ســـایبری، در چارچوب سیاست‌های پدافند سایبری را با انجام وظایف زیر بر عهده دارد.
- تبادل اطلاعات در مورد تهدیدات سایبری با قرارگاه پدافند سایبری
- تعامل امنیتی-عملیاتی باقرارگاه پدافندسایبری در مورد برنامه‌ها و آسیب‌پذیری‌های سایبری کشور

- کمک به قرارگاه پدافند سایبری در پاسخ‌گویی به شرایط اضطراری سایبری در وضعیت‌های نارنجی و قرمز
- همکاری در مدیریت صحنه رخدادهای سایبری در شرایط دفاع سایبری(وضعیت نارنجی و قرمز) و ارسال گزارش به قرارگاه پدافند سایبری

۹)وزارت امور خارجه:

- پشتیبانی سیاسی-دیپلماتیک از مأموریت‌های عملیاتی پدافند سایبری، در چارچوب سیاست‌های پدافند سایبری را با انجام وظایف زیر بر عهده دارد.
- هماهنگی، همکاری، پشتیبانی و دفاع حقوقی از اقدامات عملیاتی پدافند سایبری در مجامع و مراجع بین‌المللی
- اقناع افکار عمومی کشورهای بی‌طرف و همسو درخصوص محکومیت جنگ سایبری
- ثبت ادله قانونی اثبات تجاوز سایبری، دیپلماسی سایبری، پشتیبانی و دفاع حقوقی از اقدامات عملیاتی پدافند سایبری در مجامع و مراجع بین‌المللی
- هماهنگی و پشتیبانی از دفاع جمعی باهمکاری کشورهای همسو در برابر تهدیدات ائتلافی سایبری

۱۰)نیروی انتظامی-پلیس فتا :

پشتیبانی اطلاعاتی از مأموریت‌های عملیاتی پدافند سایبری، در چارچوب سیاست‌های پدافند سایبری را با انجام وظایف زیر بر عهده دارد.

- اقدام مقابله‌ای به‌موقع با جرائم سازمان یافته سایبری
- ارسال گزارشات رصد و پایش تهدیدات و حملات سایبری احتمالی جرایم سازمان‌یافته در حوزه زیرساخت‌های حیاتی، حساس و مهم و سرمایه‌های ملی سایبری به قرارگاه پدافند سایبری کشور (به‌صورت سیستمی)
- کمک به قرارگاه پدافند سایبری کشور در پاسخ‌گویی به شرایط اضطراری سایبری در وضعیت‌های نارنجی و قرمز

- کمک به دفاع حقوقی و انجام اقدامات فارنزیک

۱۱)وزارت ارتباطات و فناوری اطلاعات:

وزارت ارتباطات و فناوری اطلاعات با هماهنگی کامل قرارگاه پدافند سایبری مسؤولیت انجام وظایف زیر را بر عهده دارد.

- طبقه‌بندی دارایی‌های سایبری کشور
- صیانت و پدافند از مرزهای سایبری کشور با هماهنگی کامل قرارگاه پدافند سایبری(مرزبانی رقومی"سایبر")
- تداوم کارکرد زیرساختی در شبکه ملی و ارتقا پایداری آن
- پایش، رصد و کشف آسیب‌پذیری در زیرساخت‌های ارتباطی در دسترس
- حیطه‌بندی، مدیریت صحنه و فراهم آوردن امکان مدیریت منطقه‌ای و تمرکز بر دفاع در لایه G.W (دروازه ورودی)
- تشخیص، محدودسازی و جلوگیری از انواع حملات سایبری ازجمله حملات منع سرویس توزیع شده
- ایجاد و بهره‌برداری ارتباط ویژه با گروه‌های واکنش سریع(CERT) بین‌المللی
- آماده‌سازی مسیرهای جایگزین مخابراتی، ارتباطی و اینترنت (امکان اتصال و انفصال شبکه‌های خارجی متصل به شبکه ملی اطلاعات)
- انجام عملیات امداد و نجات در زیرساخت‌های ارتباطی کشور (نظیر واکنش سریع به حملات)
- جمع‌آوری ادلّه مثبته و جرم‌شناسی رقومی در زیرساخت‌های تحت کنترل و نظارت.
- در اختیار گذاشتن داشبورد رصد و پایش زیرساخت‌های کشور از طریق برقراری ارتباط اختصاصی مرکز و قرارگاه پدافند سایبری کشور
- ارسال گزارشات تهدیدات و حملات سایبری احتمالی دشمن به زیرساخت‌های حیاتی، حساس و مهم و سرمایه‌های ملی سایبری به قرارگاه پدافند سایبری

- کمک به قرارگاه پدافند سایبری در پاسخ‌گویی به شرایط اضطراری سایبری در وضعیت‌های عملیاتی
- ارزیابی آمادگی‌های عملیاتی در شبکه ملی اطلاعات با انجام رزمایش‌های مستمر

۱۲)دستگاه‌های اجرائی:

دستگاهای اجرایی ملی و استانی در مراحل قبل، در آستانه، حین و بعد از بحران (جنگ) در چارچوب سیاست‌ها و طرح‌های عملیاتی ابلاغی قرارگاه پدافند سایبری کشور به‌شرح زیر اقدام می‌نمایند.

- صیانت همه‌جانبه از دارایی‌های حیاتی و حساس سایبری و وابسته به سایبر ذی‌ربط در مقابل هر نوع تهدید سایبری
- مصون‌سازی، رفع یا کاهش آسیب‌پذیری‌های سایبری، با بهره‌گیری از محصولات بومی، سازوکار اعتبارسنجی و وصله‌زنی آسیب‌پذیری
- تاب‌آوری و تداوم کارکردهای ضروری دارایی‌های سایبری و وابسته به سایبر در زیرساخت‌های ذی‌ربط در مقابل جنگ سایبری
- حیطه‌بندی، مدیریت صحنه و فراهم آوردن امکان مدیریت منطقه‌ای و محلی
- آماده‌سازی مسیرهای جایگزین مخابراتی، ارتباطی و اینترنت
- ارزیابی آمادگی‌های عملیاتی در زیرساخت‌های ذی‌ربط با انجام رزمایش‌های مستمر

۱۳)مشاورین / همکاران (آپا، شرکت‌های مشاور، بخش خصوصی و...):

در تمام وضعیت‌های عملیاتی پدافند سایبری شرکت‌ها، موسسات، و دانشگاه‌ها برای عمل کلی و پشتیبانی‌های عمومی، تخصصی و آموزشی در کنترل عملیاتی قرارگاه پدافند سایبری اقدام می‌نمایند.

۱۴)قوه قضاییه:

سازوکار رسیدگی به‌موقع به جرایم را ایجاد و به تناسب با سطوح، جنبه‌ها، لایه‌ها

محدوده‌های زمان عملیات پدافند سایبری در تمام وضعیت‌ها عملیات پدافند سایبری را از منظر قضایی نظارت، رسیدگی، پشتیبانی و حمایت قضایی می‌نماید.

ماده ۱۶.دستورات هماهنگی:

در وضعیت‌های عملیاتی، بازیگران اصلی با هماهنگی فرماندهی قرارگاه پدافند سایبری، 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 سایبری، ایجاد آمادگی متناسب با وضعیت هشدارها و بازیابی سامانه‌ها را انجام می‌دهند.

۱)مسؤولیت انجام عملیات پدافند سایبری (پایش و رصد، مصون‌سازی، پیشگیری ومقابله با حوادث) مربوط به هر دستگاه با هدایت و راهبری قرارگاه پدافند سایبری کشور بر عهده بالاترین مقام آن دستگاه می‌باشد.

۲)عملیات پدافند سایبری در دارایی‌های حیاتی، حساس و مهم تا پایین‌ترین سطح مورد نیاز با هماهنگی، هدایت و راهبری قرارگاه پدافند سایبری کشور توسط مسؤولین دارایی‌ها تداوم می‌یابد.

۳)ضابطین قضایی و انتظامیِ وضعیت سفید و زرد پلیس فتا، و وضعیت نارنجی و قرمز قرارگاه پدافند سایبری کشور می‌باشند.

۴)قوه قضائیه (دادستانی کل کشور) در وضعیت‌های وضعیت سفید، زرد، نارنجی و قرمز، عملیات پدافند سایبری را پشتیبانی و حمایت قضایی می‌نماید.

ماده ۱۷. قرارگاه پدافند سایبری، اصول و قواعد، سند تفصیلی نظام عملیاتی پدافند سایبری کشور(حاوی جزئیات کافی برای قابل‌درک و قابل‌اجرا نمودن نظام عملیاتی پدافند سایبری، برای هر یک از ارکان این نظام، طرح‌های عملیاتی مربوط به هر یک از مأموریت‌های عملیاتی پدافند سایبری، چارچوب‌ها و قواره‌ها ودستورالعمل‌های عملیاتی و فنی مورد نیاز اجرایی‌نمودن نظام عملیات پدافند سایبری را در چارچوب و مبتنی بر نظام

عملیات پدافند سایبری تهیه، تدوین و به مسؤولین و کنشگران نظام مذکور ابلاغ می‌نماید.

ماده ۱۸. سازمان پدافند غیرعامل کشور با تشکیل کمیتهٔ عالی راهبری و نظارت مرکب از نمایندگان تام‌الاختیار کنشگران نظام عملیات پدافند سایبری، مسؤول هدایت، راهبری و نظارت بر اجرای این نظام است و آمادگی کشور در تمام سطوح، لایه‌ها، جنبه‌ها و زمان اجرای عملیات پدافند سایبری را با انجام رزمایش ارزیابی نموده و به کنشگران راهبر و کمیتهٔ دائمی گزارش می‌نماید.

ماده ۱۹. نظام عملیاتی پدافند سایبری کشور در نوزده مادّه و یکصدو بیست و شش بند در سی‌وچهارمین جلسه کمیتهٔدائمی در تاریخ ۱۳۹۸/۰۲/۳۱ به‌تصویب رسید.

به استناد تبصره یک ماده نه اساسنامه سازمان پدافندغیرعامل کشور مصوّب مقام معظّم رهبری وفرماندهی کل قوا(مدظله العالی) جهت اجرا ابلاغ می‌گردد.

اهداف کمّی نظام عملیاتی پدافند سایبری

اهداف کیفی	اهداف کمّي	ویژگی	مقیاس	پیش‌بینی
اشراف اطلاعاتي	تعداد گزارش برآورد اطلاعاتي	حاوي برآورد کلیه منشأهاي تهدید در سطح عملیاتي	سالیانه	۲
آمادگي عملیاتي	تعداد گزارش برآورد عملیاتي	حاوي برآورد کلیه واحدها و سطوح پدافند سایبري	سالیانه	۲
	رشد متخصصین پدافند سایبري	شاغل در زیرساخت‌هاي حیاتي کشور	سالیانه	۱۰ نفر
	میزان آموزش تخصصي پدافند سایبري	برگزار شده در مرکز عملیات پدافند سایبری کشور و مرکز عملیات پدافند سایبري حوزه‌اي	سالیانه	۵۰۰۰ نفرساعت
	میزان تمرین پدافند سایبري	در محیط آزمایشگاهي	سالیانه	۲۰۰۰ نفر ساعت
	مانور پدافند سایبري	قلمرو برگزاري، حداقل ۱۰٪ از یك زیرساخت حیاتي برگزاري با مشارکت حداقل دو دستگاه متولي زیرساخت‌هاي حیاتي	سالیانه	۱۰ روز
مصونیّت	گزارش طبقه‌بندي و تعیین کارکردهاي ضروري	براي هر یك از دارایي‌هاي سایبري و وابسته به سایر حیاتي و حساس	سالیانه	به تعداد دستگاه‌هاي متولي سطح حوزه‌اي
	حداکثر زمان تشخیص و مستندسازي وجود یك آسیب‌پذیري سایبري شناخته شده در زیرساخت حیاتي	براي آسیب‌پذیري‌هاي برخوردار از CVSS بحراني (۹ تا ۱۰)	روز	۳ روز پس از اعلام رسمي
		براي آسیب‌پذیري‌هاي برخوردار از CVSS زیاد و متوسط (۴ تا ۸,۹)	روز	۷ روز پس از اعلام رسمي
	حداکثر زمان رفع یك آسیب‌پذیري سایبري شناخته شده در زیرساخت حیاتي	براي آسیب‌پذیري‌هاي برخوردار از CVSS بحراني (۹ تا ۱۰)	روز	۵ روز پس از اعلام رسمي
		براي آسیب‌پذیري‌هاي برخوردار از CVSS زیاد و متوسط (۴ تا ۸,۹)	روز	۱۰ روز پس از اعلام رسمي
	گزارش ارزیابي مخاطرات امنیتي	براي هر یك از دارایي‌هاي سایبري و وابسته به سایر حیاتي و حساس	سالیانه	۱
	شناسایي آسیب‌پذیري ناشناخته در سطح حوزه‌اي	براي هر یك از دارایي‌هاي سایبري و وابسته به سایر حیاتي و حساس	سالیانه	۱
	حداقل افزایش سطح امنیت نسبت به دوره قبل، بر اساس گزارش ارزیابي مخاطرات امنیتي دوره‌اي	براي دارایي‌هاي سایبري و وابسته به سایر که ارزیابي میزان امنیت آنها در دوره قبل زیر ۵۰٪ بوده است	سالیانه	۱۵
		براي دارایي‌هاي سایبري و وابسته به سایر که ارزیابي میزان امنیت آنها در دوره قبل بین ۵۰٪ و ۸۰٪ بوده است		۱۰
		براي دارایي‌هاي سایبري و وابسته به سایر که ارزیابي میزان امنیت آنها در دوره قبل بالاي ۸۰٪ بوده است		۵
تاب‌آوري و تداوم کارکردهاي ضروري	متوسط زمان بین دو بهره‌برداري متوالي هر تهدیدي از هر آسیب‌پذیري سایبري (متوسط فاصله بین دو حمله متوالي یا فرکانس تهدید)	براي آسیب‌پذیري‌هاي برخوردار از CVSS بحراني (۹ تا ۱۰)	ماه	حداقل ۱۲ ماه
		براي آسیب‌پذیري‌هاي برخوردار از CVSS زیاد (۷ تا ۸,۹)	ماه	حداقل ۶ ماه
		براي آسیب‌پذیري‌هاي برخوردار از CVSS متوسط (۴ تا ۶,۹)	ماه	حداقل ۳ ماه
	متوسط فاصله بین زمان شروع حمله تا زمان وقوع حادثه (زمان موردنیاز تا شکست امنیت)	براي حملات برخط (مبتني بر ارسال مستقیم ترافیك)	دقیقه	حداقل ۳۰ دقیقه
		براي حملات برون‌خط (مبتني بر گسیل سلاح سایبري)	روز	حداقل ۱۰ روز
برتري عملیاتي	متوسط فاصله زماني بین وقوع حمله و تشخیص حمله	براي حملات برخط (مبتني بر ارسال مستقیم ترافیك)	دقیقه	حداکثر ۵ دقیقه
		براي حملات برون‌خط (مبتني بر گسیل سلاح سایبري)	روز	حداکثر ۷ روز
	متوسط فاصله زماني بین تشخیص حمله و دفع حمله	براي حملات برخط (مبتني بر ارسال مستقیم ترافیك)	دقیقه	حداکثر ۳ دقیقه
		براي حملات برون‌خط (مبتني بر گسیل سلاح سایبري)	روز	حداکثر ۳ روز
	متوسط زمان شناسایي متجاوز، منشا تجاوز سایبری و انتساب تجاوز سایبری به دشمن	براي حملات برخط (مبتني بر ارسال مستقیم ترافیك)	دقیقه	حداکثر ۲ دقیقه
		براي حملات برون‌خط (مبتني بر گسیل سلاح سایبري)	روز	حداکثر ۱۰ روز
	متوسط زمان ارائه گزارش حادثه سایبري و اشتراك‌گذاري اطلاعات حادثه در سامانه	براي حوادث امنیتي فاجعه‌بار	روز	حداکثر ۱ روز
		براي حوادث سایبري بحران‌زا	روز	حداکثر ۲ روز
ابقاء و ترمیم	متوسط فاصله بین دو اختلال گسترده متوالي در کارکردهاي اساسي	براي هر یك از دارایي‌هاي سایبري و وابسته به سایر		حداقل ۱۲ ماه
	متوسط زمان تداوم اختلال گسترده در حداقل یکي از کارکردهاي اساسي (متوسط زمان کنترل و)	براي هر یك از دارایي‌هاي سایبري و وابسته به سایر		حداکثر ۱ روز

مصوّبهٔ مذکور طی شـــمارهٔ ۱۶۰/۱/۲۰۰۷– ۱۳۹۸/۰۶/۱۲ با امضای رئیس ســـتاد کل نیروهای مسلح و رئیس کمیتهٔ دائمی پدافند غیرعامل ــ سرلشکر پاسدار دکتر محمد باقری ــ به دستگاه‌های اجرایی برای اقدام، ابلاغ شده است