



شماره مستقر رهبری و فرماندهی کل قوا امام خمینی (مد ظله العالی): ۱۳۹۸/۰۶/۱۲

«آرایش دشمن آرایش جنگی است؛ از لحاظ اقتصادی آرایش جنگی گرفته؛ از لحاظ سیاسی آرایش جنگی گرفته؛ از لحاظ نظامی علی‌القاعده آرایش جنگی ندارد که آن هم البته شواهد نظامی مبین است؛ جهان طور که عرض کردم از لحاظ فضای مجازی آرایش جنگی گرفته؛ در مقابل این دشمنی که آرایش جنگی در مقابل ملت ایران گرفته ملت ایران باید آرایش مناسب بگیرد؛ باید خودش را آماده کند و رهبری شناسایی مختلف»

تصویب‌نامه

وزیر محترم کشور

وزیر محترم دفاع و پشتیبانی نیروهای مسلح

معاون محترم رئیس جمهور و رئیس سازمان برنامه و بودجه کشور

رئیس محترم کمیسیون امنیت ملی و سیاست خارجی مجلس شورای اسلامی

سردار معاون محترم هماهنگ کننده ستاد کل نیروهای مسلح

سردار رئیس محترم سازمان پدافند غیرعامل کشور

سلام علیکم

با صلوات بر محمد و آل محمد و احترام؛ به استناد ماده ۸ اساسنامه سازمان پدافند غیرعامل کشور مصوب مقام معظم رهبری و فرماندهی کل قوا (مد ظله العالی) در تاریخ ۱۳۹۸/۰۲/۳۱ سی و چهارمین جلسه کمیته دائمی (شورای عالی) پدافند غیرعامل کشور تشکیل و نظام عملیاتی پدافند سایبری کشور موضوع ماده نه اساسنامه، پیشنهادی آن سازمان را بررسی و به شرح زیر تصویب نمود:

نظام عملیاتی پدافند سایبری کشور

مقدمه:

بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور، در کلیه سطوح، اهم 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. به عبارت دیگر، وجوه مختلف امور کشور 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، فلیپ، دوکو در زیرساخت‌های نفت و گاز و غیره، بویژه 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 نحوه‌ی تحقق پدافند سایبری در سطح عملیاتی، در نتیجه‌ی 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، تفکر (اصول، رویکرد، خط‌مشی، اهداف و راهبردهای) عملیاتی پدافند سایبری، تدبیر عملیات پدافند سایبری، نحوه‌ی انجام این مأموریت‌ها (طرح اقدام) و تقسیم کار (نگاشت نهادی) بین کشورهای هم‌افزایی برای یک وضعیت‌های عملیاتی، نشان می‌دهد.

سند حاضر، بمنظور ارتقاء آمادگی و پاسخگویی در شرایط اضطراری سایبری در کشور و در راستای هم‌افزایی و همکاری کشوران تهیه و تدوین شده است.





ماده ۱. تعاریف و اختصارات:

اصطلاحات و واژگان بکار 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 مصون سازی 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:** بازنمایی‌کننده‌ی نحوه‌ی تحقق مأموریت‌های پدافند سایبری کشور، در سطح عملیاتی است. نظام جامع عملیات پدافند سایبری برای این منظور، ضمن ترسیم «الزامات قانونی و مبنای نظری پدافند سایبری» و تبیین «محیط عملیات پدافند سایبری و ویژگی‌های آن»، «اصول و قواعد اساسی عملیات پدافند سایبری»، «فعالیت‌های اساسی عملیات پدافند سایبری»، «نحوه‌ی تحقق فعالیت‌های اساسی عملیات پدافند سایبری» و «اختیارات، نقش‌ها و مسئولیت‌ها» در اجرای عملیات پدافند سایبری را تعیین و تبیین می‌نماید.

(۴) **قدرت سایبری:** مولفه‌ای 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 سایبر کشور در برابر تهدیدات و حملات سایبری و ایجاد بازدارندگی به منظور 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 بدست می‌آورد به نحوی که 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، ذخیره‌سازی، 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 تقسیمه بندی می‌شوند. (سند راهبردی پدافند سایبری کشور)

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

(۹) **سامانه‌های پایه سایبری:** مجموعه‌ای از سخت افزارها و نرم افزارهایی 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 مأموریت‌ها، وظایف، تصویر (پنداره) یا شهرت دستگاه متولی سرمایه ملی سایبری یا افراد مرتبط، به‌واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام (تخریب) یا افشاء/تعمیر 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 به صورت همزمان یا مکمل یکدیگر طرح‌ریزی می‌شود، اطلاق می‌گردد.
- ۱۲) **سطوح تاثیر تهدیدات سایبری عبارتند از:**
۱. **فرمانی:** 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. **محل:** فضای سایبری، منافع و سرمایه‌های سایبری یک یا چند شهر کشور
 ۵. **سرمایه‌ای:** یک یا چند سرمایه ملی سایبری
 ۶. **سازمانی (سنگاه):** 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 فعال شدن تهدیدات داخلی و خارجی به منظور تهاجم و یا جنگ سایبری را داشته باشد، اطلاق می‌گردد. (سند راهبردی پدافند سایبری کشور)
- ۱۴) **مصون سازی:** اقداماتی است که سبب می‌شود تاثیر تهدیدات دشمن بر زیرساخت، جامعه و بیکره کشور، کاهش، در حد صفر و یا بی‌اثر شود. این اقدامات شامل اقدامات ایمنی و امنیتی بوده که در صورت وقوع حوادث ناشی از تهدید کمترین آسیب به دارائی‌های سایبری وارد گردد.
- ۱۵) **زیرساخت:** به مجموعه‌ای از مراکز و بخش‌های فعال 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 محیط زیست"، "سامانه‌های کشاورزی" و موارد مشابه، زیرساخت گفته می‌شود. که به صورت ویژه، حیاتی، حساس، مهم و قابل حفاظت دسته بندی 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 مخاطره آمیز 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) **زیرساخت‌های مهم سایبری:** آن دسته از زیرساخت‌های سایبری و وابسته به سایبر هستند که نقش و کارکرد در مقیاس محلی دارند و پیامد توقف کارکرد، حذف و تخریب آن، امنیت بخشی از کشور را مخدوش و میزان وابستگی آن به فضای سایبر مخاطره محلی دارد.
- ۱۹) **دارائی:** اطلاعات، خدمات، شبکه‌ها، و سامانه‌های سخت‌افزاری و نرم‌افزاری افراد، سازمان‌ها و زیرساخت‌های کشور است.
- ۲۰) **شرایط اضطرار سایبری:** به شرایط مخاطره آمیزی که در آستانه، حین و یا پس از وقوع یک حادثه سایبری با مرئی یا هایب، ایجاد و جریان عادی زندگی مردم را از تعادل خارج می‌کند، می‌گویند.





- (۲۱) **تهاجم سایبری:** به هرگونه اقدام غیرمجاز سایبری، که باهدف نقض سیاست امنیتی یک 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. (سند راهبردی پدافند سایبری کشور)
- (۲۲) **جنگ سایبری:** بالاترین سطح و پیچیده ترین نوع از تهاجم سایبری که توسط ارتش سایبری کشورهای مهاجم یا گروه‌های سازماندهی شده تحت حمایت دولت‌های متخاصم یا سلاح‌های سایبری، تحت کنترل یا ره‌اشده توسط آنها علیه منافع ملی کشورها انجام می‌شود و سبب تخریب فضای سایبری یا زیرساخت حیاتی، حساس و مهم کشور و وارد شدن 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 شود جنگ سایبری است و مرجع تشخیص وقوع جنگ سایبری علیه جمهوری اسلامی ایران شورای عالی امنیت ملی است.
- (۲۳) **پدافند سایبری:** مجموعه اقدامات سایبری و غیرسایبری است که توانمندی رصد، پایش، تشخیص تهدید، استخراج آسیب پذیری، تجزیه و تحلیل میزان خطر، مدیریت و کنترل تهاجم سایبری، بازیابی اطلاعات و تولید قدرت پاسخگویی به تهدید سایبری دشمن را ایجاد کند و موجب مصون‌سازی، کاهش آسیب پذیری و حفاظت از سرمایه‌های ملی سایبری و زیست بوم سایبری کشور شود و با تولید بازدارندگی امکان تهاجم سایبری را از کلیه متخاصمین سلب نماید.
- (۲۴) **دیپلماسی پدافند سایبری:** به دفاع حقوقی ازمنافع ملی، تعامل و تبادل اطلاعات در قالب پیمان‌های مشترک سایبری بین کشورها دیپلماسی پدافند سایبری گفته می‌شود.
- (۲۵) **سامانه پایش، هشدار، خنثی‌سازی:** به مجموعه‌ای نظام یافته و منسجم از سخت‌افزار و نرم افزارهایی که در یک شبکه به هم پیوسته و هوشمند سازماندهی و ساماندهی شده 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 خنثی‌سازی آن را راهبری می‌نماید، گفته می‌شود.
- (۲۶) **عملیات پدافند سایبری:** مجموعه اقدامات عملیاتی در فضای سایبر اعم از عامل و غیرعامل که به منظور حفظ توانمندی‌ها و قابلیت‌های 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) **دستگاه اجرایی:** کلیه وزارتخانه‌ها، مؤسسات دولتی، مؤسسات یا نهادهای عمومی غیردولتی، شرکتهای دولتی و کلیه دستگاه‌هایی که شمول قانون بر آنها مستلزم تصریح و یا ذکر نام است از قبیل شرکت ملی نفت ایران، سازمان گسترش و نوسازی صنایع ایران، بانک مرکزی، بانک‌ها و بیمه‌های دولتی، دستگاه‌های اجرایی نامیده می‌توند. (موضوع ماده ۵ 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 می‌شود.

ماده ۲. اسناد بالادستی

- (۱) فرامین، تدابیر و رهنمودهای مقام معظم رهبری (مدظله‌العی)
- (۲) سیاست‌های کلی نظام در حوزه پدافند غیرعامل
- (۳) قانون برنامه ششم توسعه کشور (مواد ۱۰۶، ۱۰۷ و ۱۰۹)
- (۴) اساسنامه سازمان پدافند غیرعامل کشور
- (۵) تدابیر مقام معظم رهبری (مدظله‌العی) 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 (شورای عالی پدافند غیرعامل کشور)





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 در جهت هماهنگی و هم‌افزایی 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، مشارکت، دفاع جمعی، آمادگی، انطباق‌پذیری و تاب‌آوری، *استمرار (پیش‌بینی و پیشگیری)* و *بازدارندگی*.

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

۲) **ممانعت:** جلوگیری کردن 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 انسجام در برنامه‌ریزی و اجرای عملیات پدافند سایبری، با عملیات آفند سایبری و عملیات غیرسایبری به منظور برخورداری از اثربخشی کافی و ایجاد بازدارندگی.

۵) **مشارکت و هم‌افزایی:** تعمیق همکاری، هماهنگی، مشارکت حداکثری و هم‌افزایی تمام نیروهای پدافند سایبری اعم از متولیان سرمایه‌های حیاتی و حساس سایبری و وابسته به سایر، بگان‌های سایبری نیروهای مسلح، بخش‌های دولتی و غیردولتی در عملیات پدافند سایبری.

۶) **دفاع جمعی:** عملیات پدافند سایبری 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 سایر، باید به‌صورت مداوم نسبت به توسعه قابلیت‌ها و ارتقاء توانایی، همواره آمادگی مواجهه مؤثر با تهدید، آسیب‌پذیری، حمله، جنگ، حادثه و پیامد سایبری و غیرسایبری ناشی از آن را داشته باشند.

۸) **انطباق‌پذیری:** نیروهای پدافند سایبری و سرمایه‌های حیاتی و حساس سایبری و وابسته به سایر، باید قابلیت تطبیق سریع وضعیت و اقدام‌های خود، با وضعیت دشمن، حمله سایبری و محیط عملیات را داشته باشند.

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

۱۰) **آگاهی وضعیتی:** برخورداری نیروهای سایبری خودی از اطلاعات، تحلیل و ارزیابی دوره‌ای و منظم وضعیت سرمایه‌ها، امکانات، توانایی، نیت و انگیزه‌ی نیروهای سایبری دشمن است.

۱۱) **آینده‌نگری (پیش‌بینی):** برخورداری دوره‌ای و منظم نیروهای سایبری خودی از تحلیل روند و وضعیت احتمالی آینده‌ی سرمایه‌ها، امکانات، توانایی، نیت و انگیزه‌ی نیروهای سایبری دشمن است.

۱۲) **پیش‌کنش‌گری:** تمرکز بر دسته‌ای از مأموریت‌های پدافند سایبری، که زمان اجرای آن‌ها در دوره‌ی زمانی *مفصل قبل از وقوع* جنگ سایبری است. به عبارت دیگر، تمرکز مأموریت‌های پدافند سایبری بر مواجهه 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) برهیز از هر گونه غافلگیری

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

۳) اتکاء به توان داخلی، محصولات بومی و به ویژه معماری پدافندی اختصاصی (بومی)

۴) عدم اعتماد به سامانه ها و خدمات خارجی

۵) تمرکز بر عملیات پدافند سایبری بر اساس اولویت پیش بینانه، پیش گیرانه، پیش کنش گرانه، واکنش گرایانه 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 بر اساس 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 دقت پاسخ

ماده ۷. زمان اجرای عملیات پدافند سایبری

عملیات پدافند سایبری، در چهار محدوده‌ی زمانی پیش از جنگ سایبری، در آستانه جنگ سایبری، حین جنگ سایبری و پس از جنگ سایبری اجرا می‌شود و به ترتیب معادل عملیات پدافند سایبری پیش گیرانه، پیش کنش گرانه، واکنش گرایانه و منفعلانه است. تمرکز اصلی نظام عملیاتی پدافند سایبری، بر مأموریت‌های پیش گیرانه در محدوده‌ی زمانی پیش از جنگ سایبری است و عملیات چهارگانه پدافند سایبری بر اساس 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 فرگیری 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 فرگیری 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 از طریق 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 (غیر سایبری) 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 انتقال)، اطلاعاتی، سیستم عامل، 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 به ترتیب معادل احساس امنیت، احساس احتیاط، احساس خطر و احساس تهدید، احساس جنگ قریب‌الوقوع و وقوع جنگ در فضای سایبر یا از طریق 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 به منظور حفاظت و صیانت از فضای سایبری و سرمایه‌های سایبری کشور، با به‌کارگیری ظرفیت‌های عمل کلی دفاع سایبری هدایت، راهبری، پشتیبانی و نظارت می‌نماید:

- ۱) تهیهی برآورد اطلاعاتی از تهدیدات سایبری دشمن و به‌روزرسانی آن
- ۲) شناسایی و تهیهی 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) اقتناع 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 تحقق آن، مستلزم دستیابی به اهداف عملیاتی زیر می‌باشد: (اهداف کمی و شاخص‌های نظام عملیاتی پدافند سایبری به شرح پیوست ۱)
- 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) مصونیت 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 بکارگیری 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

ب: مصونیت دارایی‌های حیاتی و حساس در مقابل هر نوع تهدید سایبری

۷) شناخت، احصاء و 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) تطبیق دادن 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 شدت، احتمال وقوع و اثر مخاطره سایبری) با مدیریت مخاطرات سایبری

۱۵) افشای 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 اقدام متقابل و تهدید به استفاده 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 ادله قانونی تجاوز سایبری

۲۰) ممانعت از تداوم تجاوز سایبری یا مقابله و دفع تجاوز سایبری دشمن از طریق 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 با غیرسایبری به متجاوز سایبری

ج: ابقاء (ترمیم) و ارتقاء قدرت پدافندی سایبری

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

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

۲۶) ابقاء و ارتقاء قابلیت‌ها، توانایی و آمادگی عملیاتی غیرعامل و فعال 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 شورای عالی امنیت ملی، شورای عالی فضای مجازی،

ستاد کل نیروهای مسلح و قرارگاه مرکزی خاتم‌الانبیاء (ع)

ب: کنش‌گران نقش مجری

دستگاه‌های مجری مأموریت‌های عملیاتی پدافند سایبری، عبارتند از ستاد کل نیروهای مسلح و قرارگاه مرکزی خاتم‌الانبیاء (ع)،

قرارگاه پدافند سایبری، یگان سایبری سپاه پاسداران انقلاب اسلامی، یگان سایبری ارتش جمهوری اسلامی ایران، یگان

فتا، یگان سایبری بسیج، وزارت اطلاعات/ مرکز مدیریت راهبردی افتا، وزارت ارتباطات و فناوری اطلاعات و سایر دستگاه‌های

اجرائی.





ب: نقش گران نقش پشتیبان

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

ت: نقش گران نقش همکار

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

ماده ۱۵. وظایف کنشگران (پوست)

۱) **شورای عالی 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 خاتم الانبیاء (ص):** در شرایط قرمز و نارنجی هدایت و راهبری (کنترل عملیاتی) قرارگاه پدافند سایبری کشور را به عهده دارد.

۴) قرارگاه پدافند سایبری کشور:

« فرماندهی، طرح ریزی عملیاتی، هدایت، راهبری و مدیریت سطح ملی پدافند سایبری در وضعیت نارنجی و قرمز

« راهبری و نظارت بر مصون سازی زیرساخت‌های حیاتی، حساس، مهم

« پایش، رصد و تشخیص تهدیدات و کشف آسیب‌پذیری‌ها در فضای سایبری

« هدایت، راهبری و نظارت بر طرح ریزی، آموزش، تمرین، رزمایش و آمادگی سایبری

« طبقه بندی و سطح بندی زیرساخت‌های سایبری و وابسته به سایبر به حیاتی، حساس و مهم از منظر نقش و کارکرد و میزان وابستگی به فضای سایبر و پیامدهای حذف 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

« پیگیری و نظارت بر اجرای نظامات، دستورالعمل‌ها و طرح‌های عملیات پدافند سایبری

۶) **سپاه پاسداران انقلاب اسلامی / فرماندهی سایبر الکترونیک و سیخ سپاه:** ظرفیت‌های پشتیبانی اطلاعاتی و عملیاتی فرماندهی سایبری و سایر ظرفیت‌های سایبری سپاه برای انجام وظایف زیر بنا به دستور در کنترل عملیاتی قرارگاه پدافند سایبری قرار می‌گیرد؛

« تهیه طرح‌ها و انجام اقدامات عامل، پیش‌کنشانه و پیش‌دستانه و دفاع فعال

« آماده‌سازی و عملیاتی سازی ظرفیت‌های لازم برای واکنش سریع به جنگ سایبری

« خنثی سازی اقدامات ضد امنیتی دشمن و آشوبگران در فضای سایبری

۷) **وزارت دفاع و پشتیبانی نیروهای مسلح:** پشتیبانی تخصصی از مأموریت‌های عملیاتی پدافند سایبری، از طریق توسعه صنعت بومی پدافند سایبری، ایجاد و سازماندهی ظرفیت عمل کلی زیرساختی پدافند سایبری (از جمله آزمایشگاه‌ها) و پشتیبانی تخصصی

از مرکز عملیات پدافند سایبری کشور را بر عهده دارد و ظرفیت‌های عملیاتی سایبری وزارت دفاع برای انجام وظایف زیر بنا به دستور در کنترل عملیاتی قرارگاه پدافند سایبری قرار می‌دهد.

« انجام عملیات امداد و نجات سایبری در زیرساخت‌های حیاتی، حساس و مهم کشور

« جمع‌آوری ادله مثبت و جرم‌شناسی رقومی در زیرساخت‌های حیاتی، حساس و مهم کشور

« رصد تهدیدات دشمن و ارسال 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.
- ◀ پیش و رصد اتحادها و معاهدات دفاعی سایبری و اتخاذ رویکرد مناسب با نیاز قرارگاه پدافند سایبری کشور.
- ◀ کمک و پشتیبانی در ظرفیت‌سازی و تربیت نیروی انسانی در قالب اطلاع‌رسانی و مهارت‌آموزی

۸) وزارت اطلاعات / مرکز مدیریت راهبردی افتا:

پشتیبانی اطلاعاتی از مأموریت‌های عملیاتی پدافند سایبری، 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 با قرارگاه پدافند سایبری 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
- ◀ افشاح افکار عمومی کشورهای بیطرف و همسو در خصوص 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 با همکاری 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 پیش‌تهدیدات 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 فارتزیک

۱۱) وزارت ارتباطات و فناوری اطلاعات

وزارت ارتباطات و فناوری اطلاعات با هماهنگی کامل قرارگاه پدافند سایبری مسئولیت 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 "سایبری")
- ◀ تداوم کارکرد زیرساختی در شبکه ملی و ارتقا پایداری آن
- ◀ پیش، رصد و کشف آسیب‌پذیری در زیرساخت‌های ارتباطی در دسترس
- ◀ حیثه‌بندی، مدیریت صحنه و فراهم آوردن امکان مدیریت منطقه‌ای و تمرکز بر دفاع در لایه (C.W) (در حوزه و روم) جمهوری اسلامی ایران
- ◀ تشخیص، محدودسازی و جلوگیری از انواع حملات سایبری از جمله حملات منع سرویس توزیع مقیده
- ◀ 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 ادله مثبت 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 اجرایی:

- « دستگاه‌های 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 به شرح 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 به موقع به جرایم را ایجاد و به تناسیب با سطوح، جنبه‌ها، لایه‌ها و محدوده‌های زمان عملیات پدافند سایبری در تمام وضعیت‌ها عملیات پدافند سایبری را از منظر قضایی نظارت، رسیدگی، پشتیبانی و حمایت قضایی می‌نماید.

ماده ۱۶. دستورالعمل هماهنگی:

- « در وضعیت‌های عملیاتی، بازیگران اصلی یا 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 (در صورت وجود فرصت لازم)، اعمال و کنترل الزام و ملاحظات پدافند سایبری، ایجاد آمادگی متناسب با وضعیت هشدارها و بازیابی سامانه‌ها را انجام می‌دهند.
- ۱) مسئولیت انجام عملیات پدافند سایبری (پایش و رصد، مصون‌سازی، پیشگیری و مقابله 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 و پشتیبانی قرارگاه پدافند سایبری کشور توسط مسئولین دارایی‌ها تداوم می‌یابد.
- ۳) ضابطین قضایی و انتظامی وضعیت سفید و زرد پلیس فتا، و وضعیت نارنجی و قرمز قرارگاه پدافند سایبری کشور را پایش و نظارت می‌کنند.





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 قابل درک و قابل اجرا 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 قوازه‌ها و دستورالعمل‌های عملیاتی و فنی مورد نیاز اجرایی نمودن نظام عملیات پدافند سایبری را در چارچوب و مبنای بر نظام عملیات پدافند سایبری تهیه، تدوین و به مسئولین و کنش‌گران نظام مذکور ابلاغ می‌نماید.

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

ماده ۱۹. نظام عملیاتی پدافند سایبری کشور در **نوزده ماده و یکصد و بیست و شش بند** در سی و چهارمین جلسه کمیته دائمی به تصویب رسید.

نظام عملیاتی پدافند سایبری کشور مشتمل بر **نوزده ماده و یکصد و بیست و شش بند** که در تاریخ ۱۳۹۸/۰۲/۳۱ در سی و چهارمین جلسه کمیته دائمی (شورای عالی) پدافند غیرعامل کشور به تصویب رسید، به استناد تبصره یک ماده نه اساسنامه سازمان پدافند غیرعامل کشور مصوب مقام معظم رهبری و فرماندهی کل قوا ابلاغ می‌گردد.

رئیس ستاد کل نیروهای مسلح و کمیته دائمی پدافند غیرعامل کشور

سرلشکر پاسدار محمدباقری





گیرندگان:

۱. سردار رئیس محترم دفتر فرماندهی معظم کل قوا جهت استحضار معظّمه .
۲. دفتر رئیس محترم جمهوری اسلامی ایران جهت استحضار.
۳. دفتر رئیس محترم قوه قضایه جهت استحضار.
۴. دفتر رئیس محترم مجلس شورای اسلامی جهت استحضار.
۵. وزیر محترم امور خارجه - جناب آقای دکتر محمدجواد ظریف .
۶. سرپرست محترم وزارت آموزش و پرورش - جناب آقای دکتر سید جواد حسینی.
۷. وزیر محترم ارتباطات و فناوری اطلاعات - جناب آقای مهندس محمدجواد آذری جهرمی.
۸. وزیر محترم اطلاعات - حجت الاسلام والمسلمین سید محمود علوی .
۹. وزیر محترم اقتصاد و دارایی - جناب آقای دکتر فرهاد دزئید .
۱۰. وزیر محترم بهداشت، درمان و آموزش پزشکی - جناب آقای دکتر سعید نمکی.
۱۱. وزیر محترم تعاون، کار و رفاه اجتماعی - جناب آقای دکتر محمد شریعتمداری.
۱۲. وزیر محترم جهاد کشاورزی - جناب آقای مهندس محمود حجینی .
۱۳. وزیر محترم دادگستری - جناب آقای دکتر سید علیرضا آوازی.
۱۴. وزیر محترم راه و شهرسازی - جناب آقای مهندس محمد اسلامی .
۱۵. وزیر محترم صنعت و معدن و تجارت - جناب آقای دکتر رضا رحمانی.
۱۶. وزیر محترم علوم، تحقیقات و فناوری - جناب آقای دکتر منصور غلامی.
۱۷. وزیر محترم فرهنگ و ارشاد اسلامی - جناب آقای سید عباس صالحی.
۱۸. وزیر محترم نفت - جناب آقای مهندس بیژن نامدار زنگنه .
۱۹. وزیر محترم نیرو - جناب آقای دکتر رضا اردکانیان.
۲۰. وزیر محترم ورزش و امور جوانان - جناب آقای دکتر مسعود سلطانی فر.
۲۱. امیر فرمانده محترم کل ارتش جمهوری اسلامی ایران جهت استحضار.
۲۲. سردار فرمانده محترم کل مپنا یاسداوان انقلاب اسلامی جهت استحضار.
۲۳. سردار فرمانده محترم نیروی انتظامی جمهوری اسلامی ایران جهت استحضار.
۲۴. سردار رئیس محترم سازمان بسیج مستضعفین جهت استحضار.
۲۵. رئیس محترم سازمان صدا و سیما جمهوری اسلامی ایران - جناب آقای دکتر علی عسکری جهت استحضار.
۲۶. رئیس محترم سازمان انرژی اتمی ایران - جناب آقای دکتر علی اکبر صالحی جهت استحضار.
۲۷. رئیس محترم سازمان محیط زیست کشور - جناب آقای مهندس عیسی کلانتری جهت استحضار.
۲۸. رئیس محترم کل بانک مرکزی جمهوری اسلامی ایران - جناب آقای دکتر عبدالناصر همتی جهت استحضار.
۲۹. رئیس محترم سازمان تبلیغات اسلامی - حجت الاسلام والمسلمین محمد قمی جهت استحضار.
۳۰. رئیس محترم مرکز ملی فضای مجازی و دبیر شورای عالی فضای مجازی کشور - جناب آقای دکتر سید ابوالحسن فیروزآبادی جهت استحضار.





(پیوست ۱)

اهداف کمی نظام عملیاتی پدافند سایبری

اهداف کیفی	اهداف کمی	ویژگی	مقیاس	پیش‌بینی	
اشراف اطلاعاتی	تعداد گزارش برآورد اطلاعاتی	حاوی برآورد کلیه منشأهای تهدید در سطح عملیاتی	سلیانه	۲	
	تعداد گزارش برآورد عملیاتی	حاوی برآورد کلیه واحدها و سطوح پدافند سایبری	سلیانه	۲	
	رشد متخصصین پدافند سایبری	شاغل در زیرساخت‌های حیاتی کشور	سلیانه	۱۰ نفر	
	میزان آموزش تخصصی پدافند سایبری	برگزار شده در مرکز عضیات پدافند سایبری کشور و مرکز عملیات پدافند سایبری حوزه‌ای	سلیانه	۵۰۰۰ نفر ساعت	
آمادگی عملیاتی	میزان تمرین پدافند سایبری	در محیط آزمایشگاهی	سلیانه	۲۰۰۰ نفر ساعت	
	مانور پدافند سایبری	قلمرو برگزاری: حداقل ۱۰٪ از یک زیرساخت حیاتی برگزاری با مشارکت حداقل دو دستگاه متولی زیرساخت‌های حیاتی	سلیانه	۱۰ روز	
مصونیت	گزارش طبقه‌بندی و تعیین کارکردهای ضروری	برای هر یک از دارایی‌های سایبری و وابسته به سایبر حیاتی و حساس	سلیانه	به تعداد دستگاه‌های متولی سطح حوزه‌ی	
	حداکثر زمان تشخیص و مستعدسازی وجود یک آسیب‌پذیری سایبری شناخته شده در زیرساخت حیاتی	برای آسیب‌پذیری‌های برخوردار از CVSS بحرانی (۹ تا ۱۰)	روز	۴ روز پس از اعلام رسمی	
	حداکثر زمان رفع یک آسیب‌پذیری سایبری شناخته شده در زیرساخت حیاتی	برای آسیب‌پذیری‌های برخوردار از CVSS زیاد و متوسط (۴ تا ۸٫۹)	روز	۷ روز پس از اعلام رسمی	
		برای آسیب‌پذیری‌های برخوردار از CVSS بحرانی (۹ تا ۱۰)	روز	۵ روز پس از اعلام رسمی	
		برای آسیب‌پذیری‌های برخوردار از CVSS زیاد و متوسط (۴ تا ۸٫۹)	روز	۱۰ روز پس از اعلام رسمی	
	گزارش ارزیابی مخاطرات امنیتی	برای هر یک از دارایی‌های سایبری و وابسته به سایبر حیاتی و حساس	سالانه	۱	
	شناسایی آسیب‌پذیری ناشناخته در سطح حوزه‌ای	برای هر یک از دارایی‌های سایبری و وابسته به سایبر حیاتی و حساس	سالانه	۱	
		برای دارایی‌های سایبری و وابسته به سایبر که ارزیابی میزان امنیت آنها در دوره قبل زیر ۵۰٪ بوده است	سالانه	۱۵	
		برای دارایی‌های سایبری و وابسته به سایبر که ارزیابی میزان امنیت آنها در دوره قبل بین ۵۰٪ و ۸۰٪ بوده است		۱۰	
		برای دارایی‌های سایبری و وابسته به سایبر که ارزیابی میزان امنیت آنها در دوره قبل بالای ۸۰٪ بوده است		۵	
تاب‌آوری و تداوم کارکردهای ضروری	متوسط زمان بین دو پیرودباری متوالی هر تهدیدی که هر آسیب‌پذیری سایبری (متوسط فاصله بین دو حمله متوالی یا فرکانس تهدید)	برای آسیب‌پذیری‌های برخوردار از CVSS بحرانی (۹ تا ۱۰)	ماه	حداقل ۱۲ ماه	
		برای آسیب‌پذیری‌های برخوردار از CVSS زیاد (۷ تا ۸٫۹)	ماه	حداقل ۶ ماه	
		برای آسیب‌پذیری‌های برخوردار از CVSS متوسط (۴ تا ۶٫۹)	ماه	حداقل ۳ ماه	
	متوسط فاصله بین زمان شروع حمله تا زمان وقوع حادثه (زمان مورخه تا شکست امنیت)	برای حملات برخط (امنیتی بر ارسال مستقیم ترافیک)	دقیقه	حداقل ۳۰ دقیقه	
برتری عملیاتی	متوسط فاصله زمانی بین وقوع حمله و تشخیص حمله	برای حملات برون‌خط (امنیتی بر گسیل سلاح سایبری)	روز	حداقل ۱۰ روز	
		برای حملات برخط (امنیتی بر ارسال مستقیم ترافیک)	دقیقه	حداکثر ۵ دقیقه	
	متوسط فاصله زمانی بین تشخیص حمله و دفع حمله	برای حملات برون‌خط (امنیتی بر گسیل سلاح سایبری)	روز	حداکثر ۷ روز	
		برای حملات برخط (امنیتی بر ارسال مستقیم ترافیک)	دقیقه	حداکثر ۳ دقیقه	
	متوسط زمان شناسایی متجاوز، منبأ تجاوز سایبری و محاسب تجاوز سایبری به دشمن	برای حملات برون‌خط (امنیتی بر ارسال مستقیم ترافیک)	دقیقه	حداکثر ۲ دقیقه	
		برای حملات برون‌خط (امنیتی بر گسیل سلاح سایبری)	روز	حداکثر ۲ روز	
	متوسط زمان ارائه گزارش حادثه سایبری و اشتراک‌گذاری اطلاعات حادثه در سامانه	برای حوادث امنیتی فاجعه‌بار	روز	حداکثر ۱ روز	
		برای حوادث سایبری بحرانی	روز	حداکثر ۱ روز	
	ایفاء و ترمیم	متوسط فاصله بین دو اختلال گسترده متوالی در کارکردهای اساسی	برای هر یک از دارایی‌های سایبری و وابسته به سایبر	سالانه	حداقل ۳۰ روز
		متوسط زمان تداوم اختلال گسترده در حداقل یکی از کارکردهای اساسی (متوسط زمان کنترل و)	برای هر یک از دارایی‌های سایبری و وابسته به سایبر	سالانه	حداکثر ۱ روز

