تعاریف و اصطلاحات پدافند سایبری

فضای سایبری

به شبکه‌های وابسته به یکدیگر از زیر ساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه شده (جاگذاری شده)، کنترل کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور 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.

سرمایه ملی سایبری

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 اهمیّت حیاتی، حساس و مهّم در فضای سایبری کشور نقش مستقیم و تعیین‌کننده داشته باشند، سرمایه ملی سایبری نامیده می‌شود.

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.

تهدید سایبری

احتمال هرگونه رویدادی که قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر (پنداره) یا اشتهار دستگاه متولی سرمایه ملی سایبری یا افراد مرتبط، به واسطه یک 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.

تهاجم سایبری

به هرگونه اقدام غیرمجاز سایبری، که با هدف نقض سیاست امنیتی یک سرمایه سایبری و ایجاد خرابی یا خسارت، ایجاد اختلال در عملکرد یا از کار اندازی خدمات و یا دستیابی به اطلاعات انجام گیرد تهاجم سایبری گویند.

جنگ سایبری

بالاترین سطح و پیچیده‌ترین نوع از تهاجم سایبری که توسط ارتش سایبری کشورهای مهاجم یا گروه‌های سازماندهی شده تحت حمایت دولت‌های متخاصم علیه منافع ملی کشورها انجام می‌شود، جنگ سایبری است.

زیست بوم سایبری

به محیط بومی متشکل از زیر ساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای که به صورت زنده و پویا با عوامل انسانی در تعامل می‌باشد، زیست بوم سایبری گفته می‌شود.

سامانه‌های پایه سایبری

مجموعه‌ای از سخت افزارها و نرم‌افزارهایی که در شکل‌گیری فضای سایبری نقش اساسی داشته و مبنای طراحی و اجراحی سایر سامانه‌ها می‌باشند، سامانه‌های پایه سایبری است.

دیپلماسی پدافند سایبری

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

پدافند سایبری

مجموعه اقدامات سایبری و غیر سایبری 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 آسیب‌پذیری 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.

نظام جامع بومی پدافند سایبری

نظامی است بومی، متشکل از زیر نظام‌های رصد، پایش، تشخیص، مدیریت و کنترل بهنگام، تولید و کنترل آمادگی، مدیریت بحران، دفاع حقوقی، منابع انسانی (آموزش، نیروی انسانی، مدیریت، مهارت، ساختار)، آموزش و فرهنگ‌سازی، صنعت سایبری، هشدار و اطلاع رسانی، حفاظت و امنیت در حوزه پدافند سایبری که برای مأموریت‌های پدافند سایبری کشور ایجاد می‌شود.