بسمه تعالی

جمهوری اسلامی ایران

سند راهبردی پدافند سایبری کشور

فهرست مطالب:

عنوان **شماره صفحه**

مقدمه ۲
اسناد بالادستی ۳
قلمرو سند ۳
تعاریف و مفاهیم اساسی ۴
ارزش های اساسی حاکم بر حوزه پدافند سایبری کشور ۸
اصول حاکم بر حوزه پدافند سایبری کشور ۹
بیانیه رسالت و ماموریت قرارگاه پدافند سایبری کشور ۱۲
ماموریت های پدافند سایبری کشور ۱۳
چشم انداز پدافند سایبری کشور ۱۴
اهداف کلان در افق چشم انداز پدافند سایبری کشور ۱۵
موضوعات اساسی راهبردی پدافند سایبری کشور ۱۷
عوامل محیطی پدافند سایبری کشور ۱۸
راهبردهای نظام پدافند سایبری کشور ۲۰
پیوست ها :
اسناد بالادستی ۲۲
تهدیدات فضای سایبری ۲۴

وظیفه‌ی همه‌ی ما این است که سعی کنیم کشور را مستحکم، غیرقابل نفوذ، غیرقابل تأثیر از سوی دشمن، حفظ کنیم و نگه داریم؛

مقام معظم فرماندهی کل قوا حضرت امام خامنه ای(۹۲/۱/۱)

مقدمه

در حال حاضر، 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. عمده فعالیت‌های رسانه‌ای به این فضا منتقل شده، بیشتر مبادلات مالی از طریق این فضا انجام می‌گیرد و نسبت قابل توجهی از وقت و فعالیت‌های شهروندان، صرف تعامل در این حوزه می‌گردد. سهم درآمد حاصل از کسب وکارهای فضای سایبر در تولید ناخالص ملی افزایش چشم‌گیر یافته و از میان شاخص-های تعیین شده برای سنجش میزان توسعه‌یافتگی کشور، شاخص‌های حوزه سایبر، سهم عمده‌ای را به خود اختصاص داده‌اند. بخش قابل توجهی از سرمایه‌های مادی و معنوی کشور، صرف این حوزه شده و بخش قابل توجهی از درآمدهای مادی و اکتسابات معنوی شهروندان نیز از این حوزه کسب شده و یا تاثیر عمده می‌پذیرد. به عبارت دیگر، وجوه مختلف زندگی شهروندان، به معنای واقعی، با این فضا در آمیخته و هرگونه بی‌ثباتی، ناامنی و چالش در این حوزه، مستقیماً وجوه مختلف زندگی شهروندان را متاثر خواهد نمود.

بررسی سوابق جنگ‌ها و انقلاب‌های مخملی شکل گرفته طی دو دهه اخیر، در کشورهای مختلف، که منجر به براندازی حکومت‌ها و نابودی منابع و زیرساخت‌های آنها شده است، بیانگر این واقعیت است که عمده این جنگ‌ها و انقلاب‌ها، با یک جنگ سایبری شروع و یا حمایت شده است.

مروری بر وقایع و حوادث سال‌های اخیر کشور، مؤید این واقعیت است که بخش عمده‌ای از تهدیدهای موجود علیه کشور، بویژه در زیرساخت‌های حیاتی، یا مستقیماً از فضای سایبر نشأت می‌گیرند و یا این فضا را هدف تهدید مستقیم خود قرار می‌دهند. بنابراین:

- با توجه به آسیب پذیری های ذاتی موجود در فضای سایبری و روند رو به رشد مهاجرت از دنیای سنتی به این فضا، ریسک سامانه های مبتنی بر فناوری اطلاعات، که برای اقتصاد کشور حیاتی می باشند، را افزایش می دهد.
- پیچیدگی روزافزون و رو به ازدیاد سامانه ها و شبکه های مبتنی بر فناوری اطلاعات چالش های امنیتی را برای کشور در بر دارد.

بر این اساس ارتقاءپایداری عملیاتی و امنیت و مصون سازی زیرساخت ها به ویژه مراکز حیاتی وحساس برای کشور بسیار حائز اهمیت تلقی می شود. سازمان پدافند غیرعامل کشور به منظور تحقق تدابیر مقام معظم رهبری و سند چشم انداز ۲۰ ساله جمهوری اسلامی ایران و با عنایت به سیاست های کلی نظام در عرصه پدافند غیرعامل، افتا و خودکفایی دفاعی – امنیتی که از سوی معظم له ابلاغ گردیده است، سند راهبردی پدافند سایبری کشور را تهیه و تدوین نموده است.

اسناد بالا دستی

۱. **چشم انداز جمهوری اسلامی ایران در افق ۱۴۰۴**
۲. **حکم مقام معظم رهبری در تشکیل شورای عالی فضای مجازی کشور**
۳. **سیاست‌های کلی نظام درامورامنیت فضای تولیدوتبادل اطلاعات و ارتباطات(افتا)**
۴. **سیاست های کلی نظام در حوزه پدافند غیرعامل**
۵. **سیاست های کلی ابلاغی مقام معظم رهبری در حوزه خودکفایی دفاعی و امنیتی**
۶. **سند راهبردی پدافند غیرعامل کشور**

قلمرو سند

کلیه دستگاه های اجرایی کشور اعم از وزارت خانه ها، سازمان ها و نهادهای سیاسی، فرهنگی و اقتصادی، امنیتی در مرکز، مراکز استان ها و شهرهای کشور که در عرصه پدافند سایبری دارای ماموریت، مسئولیت و وظیفه اند.

نکته: قلمرو این سند شامل نیروهای مسلح جمهوری اسلامی ایران نمی باشد.

تعاریف و مفاهیم اساسی

ردیف	عنوان	تعریف
۱	**فضای سایبری**	شبکه‌های وابسته به یکدیگر، از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده های تعبیه شده(جاگذاری شده)، کنترل‌گرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط وانسان به منظورتولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات می باشد. این فضا، 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.
۲	**سرمایه ملی سایبری**	یک زیرساخت حیاتی (یا حساس) کشور، یک سامانه حیاتی (یا کلیدی) سایبری و یا اطلاعات حیاتی (یا کلیدی) یا افراد متعلق به کشور و برخوردار از شرایط ذیل: ✓ دارای سطح اهمیت حیاتی یا حساس ✓ دارای کارکرد ملی(فرا استانی) ✓ برخوردار از اداره متمرکز(اداره زیرساخت، از مرکز کشور انجام می گیرد) ✓ برخوردار از حوزه عملکرد تخصصی ✓ برخوردار از قابلیت تاثیرگذاری بر امنیت ملی، اقتصاد ملی، سلامت و ایمنی عمومی، اطمینان عمومی و باورهای دینی و ملی
۳	**آسیب‌پذیری سایبری**	آسیب‌پذیری، به ضعف موجود در داخل یک سرمایه، رویه‌های امنیتی یا کنترل‌های داخلی، یا پیاده‌سازی آن سرمایه ملی سایبری، که قابلیت بهره‌برداری یا فعال‌شدن توسط تهدیدات داخلی و خارجی به منظور انجام جنگ سایبری را داشته باشد، اطلاق می‌گردد.
۴	**تهدیدات سایبری**	هررویداد یا واقعه با قابلیت واردنمودن ضربه به مأموریت‌ها، وظایف، تصویر (پنداره) یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا پرسنل دستگاه به واسطه یک سامانه اطلاعاتی، ازطریق دسترسی غیرمجاز، انهدام (تخریب)، افشاء، تغییراطلاعات و / یا ممانعت از

		(ایجاداختلال در) ارائه خدمت.
۵	**سطح تهدیدات سایبری**	تهدیدات سایبری، قادر به تاثیر گذاری بر سرمایه های ملی سایبری، در سطوح فراملی، ملی، دستگاهی، استانی، منطقه حیاتی و حساس و زیرساختی می باشند.
۶	**احتمال وقوع تهدیدات سایبری**	قابل طبقه بندی در سطوح: خیلی زیاد(قریب الوقوع)، زیاد(محتمل)، کم(غیرمحتمل) و خیلی کم(خیلی غیرمحتمل) می باشند.
۷	**شدت تهدید سایبری**	تهدیدات سایبری علیه سرمایه های ملی سایبری، در پنج سطح: خیلی زیاد(فاجعه)، زیاد(بحران)، متوسط(حادثه امنیتی عمده)، کم(حادثه امنیتی) و خیلی کم(رویداد امنیتی) طبقه بندی می گردند.
۸	**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 سرمایه ملی سایبری مذکور انجام گیرد، تهاجم سایبری اطلاق می‌گردد. همچنین"استفاده عمدی از یک سلاح سایبری علیه یک سامانه اطلاعاتی، به شکلی که موجب بروز یک حادثه سایبری شود" نیز تهاجم سایبری تلقی می شود. تهاجم های سایبری شاخص عبارت هستند از جرایم سایبری سازمان یافته، عملیات شناسایی برای تهاجم سایبری، مبارزه(ستیز/نزاع) سایبری و جنگ سایبری.
۹	**سلاح سایبری**	سامانه ی سایبری است که برای وارد نمودن خسارت(تخریب) به ساختار یا عملیات سامانه های سایبری دیگر، طراحی و تولید شده باشد. این سامانه ها، شامل شبکه بات ها، بمب های منطقی، افزارهای بهره برداری از آسیب پذیری سایبری، انواع بدافزارها و سامانه های تولید ترافیک حملات ممانعت از سرویس و ممانعت از سرویس توزیع شده می باشند که برای انجام تهاجم های سایبری، مورد استفاده قرار می گیرند. سلاح های سایبری به دو دسته ی اصلی سلاح های رها شده در شبکه و سلاح های سایبری برخوردار از کنترل آتش انسانی طبقه بندی می شوند.
۱۰	**جنگ سایبری**	بالاترین سطح و پیچیده ترین نوع از تهاجم سایبری(عملیات سایبری) است که علیه منافع ملی سایبری کشورها انجام شده و شدیدترین پیامدها را به همراه خواهد داشت. ویژگی های این نوع از تهاجم های سایبری، برای آن که دولت ها آنها را جنگ علیه منافع

		ملی خود تلقی نمایند.
۱۱	**منشاء جنگ سایبری**	نیروی سایبری کشور مهاجم یا گروه های سازمان دهی شده تحت دولت های متخاصم، سلاح های سایبری تحت کنترل یا رها شده توسط این نیروها
۱۲	**پیامدهای جنگ سایبری**	✓ براندازی نظام حاکمیتی یا تهدید فاجعه‌بار امنیت ملی ✓ آغاز همزمان جنگ فیزیکی یا زمینه‌سازی و تسهیل شروع جنگ فیزیکی در آینده نزدیک ✓ تخریب یا صدمه فاجعه‌بار به وجهه کشور در سطح بین‌المللی ✓ تخریب یا صدمه فاجعه‌بار به روابط سیاسی و اقتصادی کشور ✓ تلفات انسانی یا مخاطره گسترده برای سلامت و ایمنی عمومی (از طریق ایجاد آلودگی هسته‌ای، شیمیایی یا بیولوژیک) ✓ هرج‌ومرج و شورش داخلی ✓ اختلال گسترده در اداره امور کشور ✓ تخریب (یا صدمه گسترده به) اطمینان عمومی یا باورهای دینی، ملی و قومی ✓ خسارت شدید به (یا اختلال گسترده در) اقتصاد ملی ✓ تخریب یا اختلال گسترده در عملکرد سرمایه‌های ملی سایبری
۱۳	**سناریوهای جنگ سایبری**	✓ سناریو (۱) : جاسوسی سایبری با حمایت دولت‌ها با هدف جمع‌آوری اطلاعات برای برنامه‌ریزی تهاجم‌های سایبری بعدی ✓ سناریو (۲) : یورش سایبری با هدف بسترسازی برای هرج‌ومرج و شورش مردمی ✓ سناریو (۳) : یورش (تهاجم) سایبری با هدف از کار اندازی تجهیزات و تسهیل تهاجم فیزیکی ✓ سناریو (۴) : یورش (تهاجم) سایبری به عنوان مکمّل تهاجم فیزیکی ✓ سناریو (۵) : یورش (تهاجم) سایبری با هدف تخریب یا اختلال گسترده به عنوان هدف نهایی – جنگ سایبری
۱۴	**پدافند سایبری**	بهره‌گیری از کلیه امکانات غیر مسلحانه سایبری و غیرسایبری کشور، به منظور ایجاد بازدارندگی، پیش‌گیری، ممانعت از انجام، تشخیص به موقع، مقابله موثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری جمهوری اسلامی ایران، توسط متخاصمین سایبری،اعم از نیروی نظامی(ارتش سایبری) کشورهای متخاصم و گروه‌های تحت حمایت پنهان

		دولت‌های متخاصم به نحوی که امکان تهاجم سایبری را از کلیه متخاصمین سلب نماید.
۱۵	**زیست بوم سایبری**	زیست بوم به ارتباط متقابل بین موجود زنده و محیط آن اطلاق می‌شود. زیست بوم سایبری به شکل گیری محیطی بومی، پویا و زنده سایبری اشاره دارد که برای کشور در عرصه های مختلف حمایتگر و پشتیبانی کننده خواهد بود.
۱۶	**موقعیت تدافعی خفیف**	سازمان‌هایی که در موقعیت تدافعی خفیف هستند برخی از ویژگی‌های سازمان‌های تدافعی را در مراتب پایین‌تر دارند. ویژگی‌هایاین سازمان‌ها در حوزه نیروی انسانی، تکنیکی بودن ، مأمور و معذور بودن است. افراد متکی به اهداف فردی هستند. در مدیریت وبرنامه ریزی مبنای کار بودجه بندی است. این سازمان‌ها نامنسجم(غیریکپارچه) و الگوی کنترل در آن ها پس کنترلی است. این سازمان‌ها درسیطره عوامل محیط می‌باشند و تصمیم سازی در آن‌ها مبتنی بر اخبار است.
۱۷	**موقعیت تهاجمی خفیف**	سازمان‌هایی که در موقعیت تهاجمی خفیف هستند برخی از ویژگی‌های سازمان‌های تهاجمی را در مراتب پایین‌تر دارند. این سازمان‌ها بهره‌ور(کاردرست را درست انجام دادن) و نتیجه گرا هستند. هماهنگی در سطوح تکنیکی، تاکتیکی وعملیاتی وجود دارد. الگوی عمومی مدیریت و برنامه ریزی مدیریت استراتژیک است. این سازمان‌ها انسجام سیستمی دارند. همراستایی اهداف اعضا، سازمان وجامعه را داریم. مدیریت محیط در این سازمان‌ها مدیریت محیط زمینه ای است. این سازمان‌ها درگیر مسائل و مشکلات هستند.

ارزش‌های اساسی حاکم بر حوزه پدافند سایبری کشور

۱) خودباوری و خوداتکایی

بر اساس تعالیم عالیه اسلام و فرمایشات حضرات معصومین(علیهم السلام)، همچنین با توجه به تدابیر رهبرکبیرانقلاب اسلامی ایران و خلف صالح ایشان، مقام معظم رهبری، ملت ایران می تواند با توکل به ذات لایزال الهی و با شناخت، باور و تکیه بر توانمندی های ارزنده خود، در بسیاری از موارد به خوداتکایی دست یابد تا به سرعت وابستگی خود را به بیگانگان به حداقل برساند.

۲) اعتماد سازی، اطمینان بخشی

اقدامات کشور در حوزه پدافند سایبری باید در راستای جلب اعتماد عمومی و ایجاد اطمینان خاطر در قلوب مردم باشد. این دو عامل نقشی کلیدی در توفیق مجموعه فعالیت های این حوزه دارند. جلب اعتماد عمومی و ایجاد اطمینان قلبی از نتایج حاصل از اقدامات پدافند سایبری امری ضروری و اجتناب ناپذیر است.

۳) نوآوری و خلاقیت

با توجه به بهره گیری فضای سایبری از دانش ها و فناوری های نوین و پیچیده ترشدن امکانات سخت افزاری و نرم افزاری این فضا، لازمه مصون سازی و امنیت بخشی به زیرساخت های حیاتی و حساس کشور، برخورداری از توان نوآوری، ابتکار و خلاقیت در تمامی سطوح نیروی انسانی این حوزه می باشد.

۴) ارزش های والای انسانی- اسلامی

لازمه کار در حوزه پیچیده و گسترده سایبری، که معمولاً با برتری نسبی کشورهای متخاصم همراه است، برخورداری نیروی انسانی در سطوح مختلف از ارزش های والای انسانی-اسلامی از قبیل ایمان، صداقت، سلامت، تعهد، امانت، آگاهی، مهارت، ابتکار، پویایی، انگیزه داشتن، دشمن شناسی، تهدید شناسی، رازداری، سلحشوری، التزام به مبانی اعتقادی اسلام ناب محمدی و تفکر بسیجی می باشد

۵) نفی سلطه دشمن بر فضای سایبری

به مصداق آیه شریفه ای که متضمن مفهوم نفی سبیل برای کفار علیه مومنین است، تمامی سیاست گذاری ها، طراحی ها و برنامه ریزی ها باید در جهت نفی سلطه دشمن بر فضای سایبری باشد. بدیهی است هرگونه اقدامی که نتیجه تبعی آن ایجاد روزنه نفوذ برای دشمن در این فضا باشد گامی در جهت کمک به اوست و در تعالیم آسمانی ما به شدت نکوهیده و ممنوع است.

اصول حاکم بر حوزه پدافند سایبری کشور

۱) مصون سازی وپایداری فضای سایبر کشور

«پدافند غیرعامل مانند مصونیت سازی بدن انسان است. از درون ما را مصون می کند. ولو دشمن تهاجمی هم بکند اثری نخواهد کرد. بسیار مهم است که ما این حالت را در کل پیکره کشور و جامعه در دستگاه های مختلف بوجود بیاوریم. همت ما فقط مصروف به منصرف کردن دشمن و یا کسب آمادگی برای مقابله نباشد. کاری کنیم که مصونیت در خودمان بوجود بیاوریم. این با پدافند غیرعامل تحقق پیدا می کند.» بر اساس این تدابیر حکیمانه که از سوی مقام معظم رهبری در آبان ۱۳۹۲ بیان گردید، فضای سایبری کشور هم که بخش مهمی از سرمایه های حیاتی و حساس کشور را در بردارد باید مصون و پایدار بماند.

۲) وحدت فرماندهی پدافند سایبری کشور

برای ایجاد یکپارچگی و وحدت رویه در مصون سازی و پایدارسازی فضای سایبری کشور و همراهی و همگامی همه دستگاه های مرتبط با این فضا، لازم است پدافند سایبری کشور از فرماندهی واحدی برخوردار باشد تا تهدیدات و حملات دشمن به نتیجه دلخواه وی نرسد.

۳) دفاع بومی، همه جانبه و بازدارنده

دفاع به شیوه دشمن نتیجه ای برای ما در بر نخواهد داشت؛ فلذا باید از روش های بومی و خودی در دفاع بهره جست. همچنین دفاع باید تمام جوانب مربوط به فضای به هم پیوسته و شبکه ای شده سایبری را در بر گیرد به گونه ای که هیچ حلقه ضعیفی در زنجیره سرمایه های کشور وجود نداشته باشد. چنین دفاعی دشمن را با در بسته مواجه نموده و انگیزه های وی را برای تهدید و حمله کاهش خواهد داد و در صورت اقدام هزینه های سنگینی را بر وی تحمیل خواهد کرد.

۴) هوشمندی در دفاع

با توجه به محیط پیچیده و ناشناخته سایبری و تحولات و پیشرفت های روز به روز دانش و فناوری این عرصه، پدافند سایبری باید از عنصر هوشمندی و کیاست به خوبی بهره ببرد تا کشور دچار غافلگیری نشده و بالعکس دشمن در موضع انفعال و سردرگمی قرار گیرد.

۵) روز آمدی و آینده‌نگری

علوم و فنون مربوط به فضای سایبری با سرعت سرسام آوری رشد می کنند و عرصه های نوینی را شکل می دهند. این امر ضرورت روزآمدی و تسلط بر آخرین دستاوردها در این عرصه را دوچندان نموده و در عین حال نگاه مستمر به آینده این حوزه از دانش و فناوری بشری را می طلبد تا کشور در رقابت نفس گیر در این عرصه دچار عقب افتادگی نگردد.

۶) کاهش آسیب پذیری سایبری

یکی از کارکردهای اساسی پدافند غیرعامل، کاهش آسیب پذیری زیرساخت های حیاتی و حساس کشور در برابر تهدیدات و حملات دشمن می باشد. این اقدام یکی از مجموعه اقداماتی است که در نهایت منجر به مصونیت سازی و پایداری می شود. قدم اول در این عرصه، شناخت دقیق تمامی آسیب پذیری ها و ضعف های نهفته در سامانه های سخت افزاری و نرم افزاری است.

۷) حفظ تداوم کارکرد سامانه های سایبری

در شرایط ویژه، اعم از بحران و جنگ سایبری، روند عملکردی سامانه های سایبری کشور نباید با وقفه روبرو شود، زیرا این سامانه ها عملیات زیرساخت های حیاتی و حساس کشور را واپایی و مدیریت می کنند. هرگونه اختلال و تخریب در این سامانه ها می تواند منجر به ایجاد چالش های مهمی برای امنیت ملی کشور بشود. بنابراین حفظ تداوم کار آنها به عنوان یکی از کارکردهای پدافند غیرعامل مورد تاکید است.

۸) آمادگی و پایداری

همانند هر عرصه دیگر، پدافند سایبری کشور باید آمادگی کامل خود را به منظور مصون سازی و نیز مقابله با تهدیدات و حملات دشمن در حد عالی حفظ کند. این آمادگی در همه سطوح کاری باید همراه با استقامت و پایداری و حفظ روحیه بسیجی باشد.

۹) حفظ و صیانت از سرمایه‌های سایبری

سرمایه های سایبری شامل امکانات، اماکن، تجهیزات، اطلاعات و افرادی است که در فضای سایبری کشور از اهمیت خاصی برخوردارند. از مهم ترین وظایف پدافند سایبری کشور اتخاذ سیاست ها و تدابیر لازم برای حفظ و صیانت از این سرمایه ها در راستای مصونیت سازی و پایداری آنها می باشد.

۱۰) پیش دستی در شناخت تهدیدات

از جمله تدابیر ارزشمند مقام معظم رهبری، پیش دستی در کار علمی باشد. این مهم با کار علمی و کار فنی انجام می شود و همه کارها باید در این جهت باشد؛ به فرموده ایشان، مدیران دولتی، مدیران دانشگاه‌ها، مدیران علمی، آحاد ملت باید در این جهت حرکت کنند. شناخت تهدیدات دشمن و اقدام به موقع برای مصونیت سازی و پایدارسازی کشور در برابر آنها از جمله این امور است.

۱۱) اقتصادی سازی

فعالیت های این حوزه باید برای دستگاه های اجرایی کشور، مشاورین و پیمانکاران در بخشهای دولتی و خصوصی دارای صرفه اقتصادی بوده و تحلیل هزینه/فایده آنها به درستی انجام شود. در صورتی که همه از بکاربردن الزامات و ملاحظات پدافند سایبری علاوه بر امنیت و افزایش قابلیت دفاعی متوجه نفع اقتصادی آن هم بشوند طبعاً با اقبال بیشتری به این موضوعات می پردازند

۱۲) اشراف اطلاعاتی در فضای سایبری کشور

مبادرت به اعمال دفاعی و پدافندی در فضای سایبری کشور به شدت نیازمند تسلط بر داده ها، اطلاعات و دانش این فضا می باشد. اساساً بدون برخورداری از اطلاعات دقیق و صحیح از وضعیت خودی و دشمن در این فضا، امکان طراحی پدافندی و عملیاتی تقریباً وجود ندارد. با اتخاذ شیوه های متنوع جمع آوری و تحلیل اطلاعات، می توان بنیه اطلاعاتی خودی را تقویت نموده و از سوی دیگر با اشراف اطلاعاتی بر این فضا می توان از دست یابی دشمن به اطلاعات خودی ممانعت نمود. همچنین امکان فریب دشمن با ارائه اطلاعات غیرواقعی وجود خواهد داشت.

۱۳) دانش و فناوری بومی و مدیریت آن

پر واضح است که دشمن تمام تلاش خود را برای ممانعت از دست یابی متخصصین کشور ما به دانش و فناوری پیشرفته فضای سایبری به عمل می آورد و با سنگ اندازی در این مسیر، جلو پیشرفت کشور را در این عرصه می گیرد. لکن با اتکا بر توانمندی و هوشمندی نیروهای خودی می توان نسخه بومی این دانش ها و فناوری ها را توسعه داد و با اعمال مدیریت صحیح بر آن کاستی ها را جبران نمود.

۱۴) نفوذ ناپذیری و اقتدار

ایجاد سد محکم و پولادین در برابر نفوذ دشمن به فضای سایبری کشور همان مفهوم مصونیت سازی است که در تدابیر عالمانه مقام معظم رهبری دیده می شود. متخصصین کشور اثبات کرده اند که توان این کار را دارند و می توانند با استفاده از قوه ابتکار و خلاقیت خود باعث تولید اقتدار و بازدارندگی برای کشور بشوند.

۱۵) بهداشت سایبری

فضای سایبری کشور باید پاک و بی آلایش باشد به نحوی که همه بتواند با آرامش خاطر از آن بهره ببرند و از آسیب ها و آفات آن متضرر نشوند. وظیفه نظام پدافند سایبری کشور آن است که با اتخاذ تمهیدات صحیح و دقیق از آلودگی این فضا جلوگیری نموده و با رصد و پایش مستمر آن، پاک بودن آن را تضمین کنند.

۱۶) رعایت قوانین بین المللی

از آنجا که فضای سایبری کشورها دارای قلمرو تعریف شده ای نمی باشد، در بهره برداری از آن کشورها باید موارد مشترک و مفترق بین خود را تعریف نموده و با تلاش برای طراحی و اجماع بر روی مقررات و قوانین بین المللی این عرصه از احتمال بروز درگیری بین خود جلوگیری کنند. همچنان که در موضوع جرایم سایبری بین پلیس سایبری کشورها پروتکل های همکاری وجود دارد، در موضوع پدافندسایبری و جلوگیری از بروز جنگ های گسترده بین کشورهای دنیا باید اقدامات لازم به عمل آید.

۱۷) بی اعتمادی به محصولات خارجی

در بسیاری از موارد معلوم گردیده است که محصولات سخت افزاری و نرم افزاری خارجی مورد استفاده در سامانه ها و شبکه های رایانه ای و ارتباطی و نیز سامانه های کنترل صنعتی کشور، امکاناتی تعبیه شده تا دشمن بتواند در موارد خاص با بهره گیری از آنها به کشور ما ضربه بزند. بنابراین نباید به تولیدات خارجی اعتماد نمود و حتی الامکان باید از محصولات بومی بهره جست. در مواردی که به ناچار از محصولات خارجی استفاده می شود، باید با ارزیابی دقیق امنیتی و دفاعی آنها راه های نفوذ تعبیه شده در آنها را مسدود نمود.

بیانیه رسالت پدافند سایبری کشور

رسالت قرارگاه پدافند سایبری کشور، مصون سازی و پایدار سازی سرمایه های سایبری کشور از طریق پایش و تشخیص تهدیدات، کشف، مدیریت و کنترل آسیب پذیری ها، اعلام هشدارهای لازم، امن سازی، تدوین و انتشار نظامات(ملاحظات، مقررات، الزامات و اصول) پدافندی، آموزش و نهادینه سازی پدافند سایبری، مدیریت صحنه پدافندسایبری و دفاع حقوقی در برابر تهدیدات و حملات دشمن می باشد.

بیانیه ماموریت پدافند سایبری کشور

قرارگاه پدافند سایبری تشکیلاتی است نظام مند و منحصر بفرد در تعامل با سایر نهادهای کشوری، امنیتی و دفاعی کشور با ماموریت های: رصد، پایش، مراقبت، کنترل،تشخیص و هشدار تهدیدات سایبری، ایجاد و ارتقاء نظام جامع پدافند سایبری کشور، فرماندهی و مدیریت بحران سایبری حوزه کشوری، مدیریت بحران های سایبری کشور از آغاز تا بازیابی شرایط عادی، ایجاد توانمندی های برترساز در پدافند سایبری، دفاع هوشمندانه چند لایه و اثربخش از سرمایه های سایبری کشور، ایجاد، حفظ و ارتقاء توان پایداری و بازدارندگی در فضای سایبر، تولید و ارتقاء آمادگی دفاع سایبری در دستگاه اجرایی، بخش خصوصی و مردم، ایجاد، حفظ و ارتقاء توان کاهش آسیب پذیری، امن سازی، استحکام، پایداری، مصون سازی و بازدارندگی در فضای سایبر، تامین پایداری و استحکام زیرساخت های زیست بوم سایبری کشور، ایجاد، حمایت و ارتقاء ظرفیت‌های خود اتکا صنعت دفاع سایبری کشور(دولتی و غیردولتی)، آموزش و تربیت سرمایه‌های انسانی در حوزه سایبری، تولید، مدیریت و بومی سازی دانش، آرامش بخشی و هدایت افکار عمومی در برابر تهدیدات، دفاع حقوقی و قانونی از منافع ملی کشور در حوزه سایبری، تعامل با کشورها و نهادهای بین‌المللی و منطقه ای درحوزه پدافند سایبری وفرهنگ سازی در راستای حفظ، صیانت و دفاع هوشمندانه از سرمایه های سایبری کشور، تداوم خدمات ضروری، افزایش توان بازدارندگی و ارتقا پایداری به منظور مأیوس سازی دشمنان از حمله به سرمایه ها و منافع ملی.

مأموریت پدافند سایبری کشور

۱) ایجاد توانمندی های برتر ساز در پدافند سایبری

۲) دفاع هوشمندانه چند لایه و اثربخش از سرمایه های سایبری کشور

۳) فرماندهی، هدایت و کنترل صحنه پدافند سایبری در سطوح ملی، منطقه ای و دستگاهی

۴) ایجاد، ارتقا و راهبری نظام جامع پدافند سایبری کشور

۵) ایجاد، حفظ و ارتقاء توان کاهش آسیب پذیری، امن سازی، استحکام، پایداری، مصون سازی و بازدارندگی در فضای سایبر

۶) تولید و ارتقاء آمادگی پدافند سایبری در دستگاه های اجرایی، بخش خصوصی و آحاد جامعه

۷) افزایش توان برگشت پذیری سامانه های ملی سایبری به وضع عادی

۸) تأمین پایداری و استحکام زیرساخت های زیست بوم سایبری کشور

۹) ایجاد، حمایت و ارتقاء ظرفیت‌های خوداتکا صنعت بومی دفاع سایبری کشور(دولتی و غیردولتی)

۱۰) آموزش و تربیت سرمایه‌های انسانی در حوزه سایبری

۱۱) تولید و مدیریت دانش و فناوری پدافند سایبری

۱۲) فرهنگ سازی پدافند سایبری (نیازسنجی، طراحی، تدوین محتوا، اجرا، نظارت و راهبری، آگاهی و تغییر رفتار

۱۳) افزایش اعتماد عمومی و ارتقاء سطح مشارکت مردمی

۱۴) اطلاع رسانی به منظور آرامش بخشی و کاهش تأثیرات مخرب عملیات روانی دشمن

۱۵) دفاع حقوقی و قانونی از منافع ملی کشور در حوزه سایبری

۱۶) تعامل با کشورها و نهادهای بین‌المللی و منطقه ای درحوزه پدافند سایبری

چشم اندازپدافند سایبری کشور

با استعانت از قادر متعال "جمهوری اسلامی ایران در افق ۱۴۰۴" با قدرت بازدارندگی موثر در برابر تهدیدات سایبری دشمن مبتنی برنظام پدافند سایبری هوشمندانه، انحصاری، ابتکاری، عمیق، لایه به لایه، بومی و پیشگیرانه، شبکه ای، گسترش یافته و سلسله مراتبی، چابک و منعطف، نظام دفاع حقوقی و قانونی جامع ملی در حوزه پدافند سایبری، دانش و فناوری و صنعت پیشرفته بومی، منابع انسانی نخبه، خبره، توانمند، متعهد و مبتکر، فرماندهی و کنترل جامع، مقتدر و هوشمند ، دارای جایگاه ممتاز جهانی در پدافند سایبری است.

پدافند سایبری کشور در راستای این چشم انداز دارای ویژگی‌های زیر است:

(۱) برخوردار ازنظام جامع پدافند سایبری هوشمندانه، انحصاری، ابتکاری، عمیق، لایه به لایه، بومی، پیشگیرانه، شبکه ای، گسترش یافته و سلسله مراتبی ، چابک و منعطف در سطح ملی، منطقه ایو استانی

(۲) دست‌یافته به زیست بوم ملی سایبری امن، مصون و پایدار در برابر تهدیدات سایبری

(۳) برخوردار از نظام فرماندهی، هدایت، راهبری و کنترل پدافند سایبری

(۴) برخوردار از سامانه های رصد، پایش، مراقبت، کنترل، تشخیص، هشدار و پیشگیری و دفاع در مقابل انواع تهدید

(۵) برخوردار از سرمایه‌های ملی سایبری امن ، مصون و پایدار در سطح ملی

(۶) برخوردار از سرمایه های انسانی آموزش دیده، مومن، متعهد، متخصص، کارآمد، بصیر، امین و رازدار و دارای روحیه بسیجی

(۷) بهره‌مند از زیرساخت‌های حیاتی آسیب ناپذیر راهبردی سایبری

(۸) بهره بردار از صنعت دفاع سایبری بومی، توانا، پاسخگو و قادر به تولید بومی زیرساخت ها و سامانه های اساسی سایبری (ساماندهی شده از بخش خصوصی و ظرفیت های دانش بنیان و دانشگاهی و نخبگان متخصص) به عنوان پشتیبان نظام جامع پدافند سایبری کشور

(۹) خود اتکا در تولید سامانه‌های پایه پدافند سایبری

(۱۰)برخوردار از استانداردها، نظامات و الگو های پدافند سایبری بومی و روزآمد و امن

(۱۱)برخوردار از مشارکت و بهره مند از ظرفیت‌های بخش‌های دولتی، خصوصی و مردم در پدافند سایبری

(۱۲)توانمند در مدیریت بحران سایبری و تضمین تداوم خدمات رسانی ضروری به مردم

(۱۳)برخوردار از جامعه ای آگاه و آموزش دیده ، سازماندهی شده، بصیر و آماده در برابر انواع تهدیدات و حملات سایبری

(۱۴)دارای تعامل و همکاری هوشمندانه با مجامع و نهادهای بین‌المللی و منطقه ای

(۱۵)قادر به بهره برداری هوشمندانه، خلاقانه و هدفمند از مزایا و فرصت‌های فضای سایبر

(۱۶)برخوردار از نظام دفاع حقوقی قانونی سایبری در راستای دفاع از منافع ملی در مجامع بین المللی

اهداف کلان در افق چشم انداز پدافند سایبری کشور

۱) طراحی، پیاده سازی و اجرای نظام پدافند سایبری هوشمندانه، انحصاری، ابتکاری، عمیق، لایه به لایه، بومی، پیشگیرانه، شبکه ای، گسترش یافته و سلسله مراتبی ، چابک و منعطف در سطح ملی، منطقه ای و استانی

۲) ارتقای آمادگی دفاعی و بازدارندگی کشور درمقابل تهدیدات وحملات سایبری کشورهای متخاصم

۳) طراحی، پیاده سازی و اجرای سامانه جامع رصد، پایش، مراقبت، کنترل و تشخیص و هشدار تهدیدات سایبری

۴) طراحی، پیاده سازی و اجرای نظام جامع فرماندهی وکنترل یکپارچه و هوشمند پدافند سایبری

۵) حفاظت، صیانت و پایدارسازی سرمایه‌های سایبری کشور درمقابل تهدیدات و حملات سایبری دشمنان

۶) ارتقاء توانمندی فرماندهی و کنترل و مدیریت بحران سایبری در راستای تضمین تداوم خدمت رسانی ضروری به مردم و دستگاه های حیاتی و بازیابی وضعیت عادی

۷) آموزش، تربیت و توانمندسازی سرمایه های انسانی کارآمد متناسب با اقتضائات حال و آینده پدافند سایبری

۸) تولید، مدیریت و بومی سازی دانش پدافند سایبری با بکارگیری ظرفیت های ملی

۹) ایجاد زیست بوم سایبری ملی، بومی،امن و پایدار با اولویت زیرساخت های حیاتی و حساس سایبری

۱۰) مشارکت دستگاه های دولتی، بخش خصوصی و نهاد های مردمی در پدافند سایبری

۱۱) ارتقاء فرهنگ پدافند سایبری (نیازسنجی، طراحی، تدوین محتوا، اجرا، نظارت و راهبری، آگاهی و تغییر رفتار)

۱۲) سازماندهی، آموزش، هدایت، کنترل و ارزیابی مداوم دستگاه های کشور در راستای ارتقای کارآیی دفاعی و نیل به بازدارندگی پدافندی از طریق فعال سازی قرارگاه پدافند سایبری

۱۳) آرامش بخشی و هدایت افکار عمومی در برابر تهدیدات و ارائه اقتدار پدافند ملی سایبری

۱۴) تعامل بین المللی در حوزه پدافند سایبری در چارچوب سیاست ها، مقررات و قوانین ابلاغی

۱۵) ایجاد، حمایت و ارتقاء ظرفیت‌های خوداتکا و توسعه یافته صنعت بومی پدافند سایبری(دولتی و غیردولتی) در تولید سامانه های اساسی پدافند سایبری

۱۶) طراحی پیاده سازی و راهبری نظام پدافند سایبری با ویژگی بومی سازی استانداردها،رویه ها و روال های پدافند سایبری کشور

۱۷) ایجاد، استقرار، پیاده سازی و راهبری نظام دفاع حقوقی و قانونی از منافع ملی کشور در حوزه سایبری

۱۸) فرهنگ سازی، آموزش عمومی، سازماندهی، تمرین و رزمایش و تولید آمادگی پدافند سایبری در دستگاه های اجرایی

۱۹) طراحی، پیاده سازی و اجرای سامانه امن و پایدار خدمات سایبری به زیرساخت های حیاتی و حساس کشور در راستای مصونیت بخشی کامل به آنها

۲۰) طبقه بندی و سطح بندی سایبری زیرساخت ها، آسیب شناسی در برابر تهدیدات، ایمن سازی، پایدارسازی و مصونیت بخشی به زیرساخت های سایبری کشور و ارتقای بازدارندگی آنها

۲۱) نهادینه سازی اصول، الزامات و ملاحظات پدافند غیرعامل و پدافند سایبری در ذات طرحهای توسعه ای بخش سایبری کشور و سایر زیرساخت های دارای اهمیت بالا.

موضوعات اساسی راهبردی پدافند سایبری کشور

۱) توسعه آمادگی دفاعی و بازدارندگی درمقابل تهدیدات وحملات سایبری

۲) دستیابی به نظام جامع فرماندهی وکنترل مقتدر و هوشمند دفاع سایبری

۳) رصد، پایش، مراقبت و تشخیص و هشدار تهدیدات وحملات سایبری

۴) حفظ و پایدارسازی زیرساختهای حیاتی وحساس کشور درمقابل تهدیدات و حملات سایبری

۵) توسعه زیست بوم سایبری بومی، امن و پایدار داخلی زیرساخت های کشور

۶) توسعه صنعت بومی و خوداتکا در دفاع سایبری

۷) ایجاد تناسب وکفایت سرمایه های انسانی

۸) فرهنگ سازی وتوسعه مفاهیم دفاع سایبری

۹) تامین علم وفناوری بومی، آینده پژوهی و نوآوری درفضای دفاع سایبری

۱۰) توسعه نظام حقوقی وتعاملات بین المللی درحوزه دفاع سایبری

۱۱) تدوین قوانین ومقررات، دستورالعمل‌ها و استانداردهای بومی درحوزه دفاع سایبری

۱۲) توسعه قابلیت های صیانت از اطلاعات، افراد و سرمایه‌های سایبری

۱۳) درک هوشمندانه و پیش دستانه تهدیدات

۱۴) نفوذناپذیری و استحکام و ایمنی زیرساخت های حیاتی و حساس

۱۵) عدم بکارگیری غیرهوشمندانه سامانه های خارجی در مراکز دارای اهمیت بالا

ارزیابی عوامل محیطی پدافند سایبری کشور

عوامل محیطی چهارگانه قوت ها، ضعف ها، فرصت ها و تهدیدات پدافند سایبری کشور عبارتند از:

قوت ها:

[۱] توجه جدی و حمایت های مؤثر مسئولین عالی نظام به فضای سایبری، ظرفیت ها و مخاطرات آن

[۲] درک نسبی مسئولین از تبعات تهدیدات و حملات سایبری قبلی دشمن به زیرساخت‌های کشور

[۳] وجود ساختار پدافند غیرعامل سایبری برای دفاع از فضای سایبری کشور

[۴] وجود ظرفیت‌های مناسب در اسناد بالادستی و حمایتی

[۵] وجود سند افتا و ابلاغیات دولت در این حوزه

[۶] وجود قوانین جزایی مربوط به جرایم رایانه ای

[۷] وجود تجربیات مفید از تهدیدات فضای سایبر درسازمان‌های نظامی، دولتی و خصوصی

[۸] شکل گیری نسبی ساختارهای مصوب در عرصه امنیت سایبری کشور

[۹] وجود ظرفیت‌های علمی، پژوهشی و صنعتی حوزه سایبری و افتا در بخش‌های دولتی و خصوصی کشور

[۱۰] وجود رشته‌های دفاع سایبری در دانشگاه‌های کشور

[۱۱] برخورداری نسبی از نیروی انسانی متعهد و متخصص در حوزه سایبری

[۱۲] توانایی نسبی طراحی، تولید بومی و مهندسی معکوس نرم افزارها و سخت‌افزارهای پدافند سایبری

[۱۳] توانایی طراحی و تولید الگوریتم‌های رمزنگاری بومی

[۱۴] توانایی کشف و تحلیل آسیب پذیری های شناخته شده و ناشناخته در زیرساخت های سایبری کشور

[۱۵] توانایی نسبی مقابله و پاسخگویی به تهدیدات سایبری

[۱۶] وجود ظرفیت های ارتباطی پشتیبان برای پدافند سایبری از سرمایه های کشور

ضعف ها:

[۱] تنوع دیدگاه‌های فرهیختگان نسبت به تهدیدات فضای سایبری

[۲] کم توجهی به استفاده از ظرفیت های بخش خصوصی در حوزه سایبری

[۳] کمبود رشته ها، دروس و پایان نامه های دانشگاهی در حوزه تهدیدات سایبری

[۴] کُندی رشد صنعت پدافند سایبری

[۵] بهره برداری از تجهیزات غیر بومی در حوزه سایبری

[۶] پایین بودن سرعت رشد تجهیزات سخت افزاری و نرم افزاری بومی در فضای سایبری کشور

[۷] کندی سرعت رشد دانش، فناوری، استانداردها و محصولات بومی حوزه سایبری

[۸] قطع نشدن وابستگی به دانش، فناوری‌ها و استانداردهای غیربومی در حوزه سایبری

[۹] کمبود آزمایشگاه‌های مرجع سایبری

[۱۰] فقدان نظام جامع حقوقی و قانونی در حوزه سایبری به منظور دفاع از منافع ملی در مجامع بین المللی

تهدیدات

[۱] انگیزه دشمن برای تسلط بر فضای سایبری

[۲] وجود راهبردهای تهاجمی دشمن در فضای سایبری

[۳] وجود سازمان رزم سایبری در کشورهای متخاصم

[۴] ساختارمند شدن تهدیدات استکبار جهانی بر علیه ج.ا.ا. در فضای سایبری

[۵] مخاطرات ناشی از بکارگیری بدافزارها و سلاح‌های سایبری توسط حریف

[۶] تأثیرات شبکه‌های اجتماعی و فناوری‌های نوظهور دشمن در تضعیف امنیت ملی

[۷] وجود شبکه ها و گروه های جاسوسی و نفوذی وابسته به دشمن در فضای سایبری

[۸] توافقات و تفاهمات کشورهای متخاصم علیه ج.ا.ا

[۹] فقدان حقوق بین‌المللی عادلانه در حوزه دفاع سایبری

[۱۰] بهره گیری دشمن از بلاتکلیفی قلمرو سایبری کشور

[۱۱] تقدم راهبردهای جنگ سایبری نسبت به جنگ فیزیکی

فرصت ها

[۱] امکان استفاده از ویژگی بی مرزی و گستردگی جهانی فضای سایبری در امر پدافند سایبری

[۲] اتکای شدید دشمن به زیر ساخت‌های اطلاعاتی، ارتباطی و پردازشی و خدمات عمومی

[۳] فعال شدن ظرفیت‌های دفاع سایبری به واسطه وجود تحریم ها و تهدیدات

[۴] امکان بهره گیری از دانش و فناوری‌های نو ظهور

[۵] امکان ارتقاء سطح همکاری‌های بین‌المللی و منطقه‌ای در زمینه پدافند سایبری

[۶] رقابت کشورها، دولت‌ها و شرکت‌های چند ملیتی صاحب دانش و فناوری

[۷] امکان همکاری‌های بین‌المللی در زمینه حقوق بین‌الملل و پیمان‌های همکاری و دفاعی سایبری همسو(اسلامی، نم، منطقه و ...)

راهبردهای نظام پدافند سایبری کشور

۱) طراحی، پیاده سازی و اجرای نظریه‌ها و الگوهای پدافند سایبری بومی، دانش محور و پاسخگو به تهدید

۲) کاهش آسیب پذیری، پایدارسازی، مصون سازی، ارتقاءتوان بازدارندگی زیرساخت‌های حیاتی وحساس کشور در برابر تهدیدات و حملات سایبری

۳) طراحی، پیاده سازی و اجرای نظام پدافند سایبری درمقابل تهدیدات و حملات سایبری با ویژگی بومی سازی فرآیندها، نظامات و استانداردها، پروتکلها، رویه ها و روال ها

۴) بهره گیری از قابلیت های بسیج و سازمان‌های مردم نهاد و ظرفیت های بخش خصوصی در پدافند سایبری

۵) آموزش، فرهنگ سازی و برگزاری رزمایش به منظور نیل به آمادگی آرمانی پدافند سایبری

۶) ساماندهی و ارتقا دانشی و بکارگیری منابع انسانی متخصص درحوزه پدافند سایبری

۷) رصد، پایش، مراقبت، تشخیص و هشدار هوشمندانه و دست یابی به اشراف اطلاعاتی در برابر تهدیدات فضای سایبری از طریق سازماندهی مراکز رصد و پدافند سایبری با رویکرد شناخت پیش دستانه تهدید

۸) مدیریت و کنترل پیامدهای تهدیدات و حملات سایبری

۹) طراحی، پیاده سازی و اجرای مراکز رصد، پایش و کنترل زیرساخت‌های حیاتی به صورت بومی

۱۰) نهادینه سازی اصول، راهبردها، ملاحظات و الزامات پدافند غیر عامل و پدافند سایبری در طرح های توسعه ملی و استانی پدافند سایبری کشور

۱۱) بومی و ایمن سازی تجهیزات مورد استفاده در زیرساخت‌های حیاتی وحساس کشور در جهت کاهش وابستگی به فناوری‌ها و محصولات غیربومی و ممنوعیت کاربرد سامانه های خارجی در آنها

۱۲) تقویت صنعت پدافند سایبری بومی و حمایت از سازمان‌ها و شرکت‌های تولیدکننده سامانه‌ها و محصولات بومی

۱۳) الزام و همراه سازی سازمان‌های متولی زیرساخت‌های حیاتی وحساس کشور در ایجاد زیست بوم سایبری و استفاده از محصولات امن داخلی

۱۴) تولید و مدیریت دانش و طراحی و اجرای آموزش‌های پدافند سایبری درسطوح مختلف

۱۵) طراحی و پیاده سازی زیرساخت سایبری امن و مصون برای زیرساخت های حیاتی و حساس کشور

۱۶) طراحی، پیاده سازی و اجرای راهبردهای اطلاع رسانی و عملیات روانی در جهت آرامش بخشی داخلی و پاسخ به تهدیدات خارجی و تولید بازدارندگی پدافند سایبری

۱۷) فرهنگ سازی و آموزش مسئولین و نخبگان و آحاد جامعه در حوزه پدافند سایبری

۱۸) نهادینه سازی مفاهیم پدافند سایبری در نظام آموزشی(ابتدایی، متوسطه و دانشگاهی)کشور و نظام آموزش دفاعی کشور

۱۹) بکارگیری ظرفیت های مراکز تحقیقات بنیادی و کاربردی در حوزه پدافند سایبری در جهت تولید سامانه های اساسی سایبری در داخل کشور

۲۰) طراحی، پیاده سازی و اجرای نظام دفاع حقوقی و قانونی پدافند سایبری کشور در جهت دفاع از منافع ملی در مجامع بین المللی

۲۱) تعامل با نهادها و سازمان های بین المللی سایبری در جهت مشارکت و ایفای نقش در تدوین قوانین و مقررات بین‌المللی دفاع سایبری و احقاق حقوق کشور

۲۲) بومی سازی و گسترش فرهنگ حفاظت و امنیت درحوزه پدافند سایبری

۲۳) طبقه بندی و سطح بندی مراکز و زیرساخت های کشور از نظر تهدیدات جنگ سایبری و اولویت دهی نسبت به زیرساخت های حیاتی و حساس سایبری کشور

۲۴) ارزیابی مداوم، بازرسی، ممنوعیت و برخورد با بکارگیری سامانه های خارجی در زیرساخت های حیاتی و حساس کشور

۲۵) فعال سازی قرارگاه پدافند سایبری و اجرایی کردن نظامات پدافند سایبری کشور با رویکرد مصون سازی (ایمن سازی و پایداری) فرهنگ سازی، آموزش و نظارت

پیوست ۱ : اسناد بالا دستی

۱. چشم انداز جمهوری اسلامی ایران در افق ۱۴۰۴

جامعه ایرانی در افق چشم انداز.....امن، مستقل، ومقتدر با سامان دفاعی مبتنی بر بازدارندگی همه جانبه و پیوستگی مردم و حکومت ....

۲. حکم مقام معظم رهبری در تشکیل شورای عالی فضای مجازی کشور

گسترش فزاینده فناوری‌های اطلاعاتی و ارتباطاتی به ویژه شبکه‌ی جهانی اینترنت و آثارچشمگیر آن در ابعاد زندگی فردی و اجتماعی، و لزوم سرمایه‌گذاری وسیع و هدفمند درجهت بهره‌گیری حداکثری از فرصت‌های ناشی از آن در جهت پیشرفت همه جانبه کشور وارائه خدمات گسترده و مفید به اقشار گوناگون مردم و همچنین ضرورت برنامه‌ریزی وهماهنگی مستمر به منظور صیانت از آسیب‌های ناشی از آن اقتضا می‌کند که نقطه‌ی کانونی متمرکزی برای سیاست‌گذاری، تصمیم‌گیری و هماهنگی درفضای مجازی کشور به وجود آید.

۳. سیاست‌های کلی نظام در امور «امنیت فضای تولید و تبادل اطلاعات و ارتباطات(افتا)

ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای امن سازی ساختارهای حیاتی و حساس و مهم درحوزه فناوری اطلاعات و ارتباطات، وارتقاء مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی درکشور به منظور:

- ✓ استمرارخدمات عمومی.
- ✓ پایداری زیرساخت‌های ملی.
- ✓ صیانت از اسرارکشور.
- ✓ حفظ فرهنگ و هویت اسلامی- ایرانی و ارزش‌های اخلاقی.
- ✓ حراست از حریم خصوصی و آزادی‌های مشروع و سرمایه‌های مادی و معنوی.

۴. سیاست های کلی ابلاغی مقام معظم فرماندهی کل قوا در حوزه خودکفایی دفاعی و امنیتی

۱- توسعه و تعمق فرهنگ خودباوری، خودکفایی، نوآوری و خلاقیت در تمام سطوح و ابعاد دفاعی و امنیتی

۲- ترویج نهضت نرم افزاری، تولید توسعه علوم و فناوری و تحقیقات دفاعی و امنیتی حرکت در مرزهای دانش با تأکید بر بومی سازی

۳- دستیابی به فناوری برتر مورد نیاز دفاعی و امنیتی حال و آینده با تأکید بر نوآوری و پشتیبانی از توسعه آنها

۴- تأکید بر خودکفایی کشور در سامانه ها، کالاها و خدمات اولویت دار دفاعی و امنیتی توأم با بهسازی تجهیزات موجود و افزایش قابلیت و کارایی آن.

۵- ممنوعیت نأمین نیاز دفاعی و امنیتی از خارج کشور مگر در حد ضرورت و حتی الامکان با رعایت ملاحظات زیر :

- با اولویت انتقال فناوری
- تأمین آموزش و پشتیبانی
- تأمین از منابع متنوع

۶- برون سپاری و جلب مشارکت سایر بخش ها اعم از دولتی و غیر دولتی درتأمین نیازهای نیروهای مسلح با رعایت ملاحظات امنیتی و حفاظتی.

۷- جذب، توانمندسازی و به کارگیری نیروهای مستعد و نخبه با فراهم نمودن زمینه های رشد و تقویت آنها برای ارتقاء قابلیت های توسعه فناوری های نیازهای دفاعی و امنیتی کشور.

۸- برقراری ارتباط و همکاری با دیگر کشورها در زمینه علمی، تولید و تجاری کالاها و خدمات دفاعی و امنیتی برای دستیابی به اهداف سیاست های کلی خودکفایی دفاعی و امنیتی

۹- مقرون به صرفه سازی مسیر توسعه صنایع و فناوری دفاعی و امنیتی کشور و ایجاد هم افزایی در فناوری مورد نیاز

پیوست ۲ : « تهدیدات فضای سایبری»

«جنگ سایبری» (Cyberwarfare) به نوعی از نبرد اطلاق می شود که طرفین جنگ در آن از رایانه و شبکه‌های رایانه‌ای (به خصوص شبکه اینترنت) به عنوان ابزار تهاجم استفاده کرده و نبرد را در فضای سایبری به راه می اندازند.

فضای سایبر در این نوع جنگ به هر فضائی اطلاق می‌شود که به وسیله نرم افزار در رایانه ایجاد می شود و به عبارتی می توان گفت که در دنیای مجازی، اتاق فرمان جنگ را مدیران شبکه های رایانه ای به دست می گیرند. با این تعریف می توان اعلام کرد که «بزرگ‌ترین فضای سایبری که میلیون‌ها کاربر را به یکدیگر متصل می کند، فضای مجازی اینترنت است.»

با پیشرفت فناوری اطلاعات و ارتباطات، دستگاه های اجرایی برای انجام عملیات خود و به منظور تولید، ذخیره سازی، پردازش، نگهداری، بازیابی و ارائه گزارش اطلاعات خود، به سامانه های اطلاعاتی رایانه ای وابسته شده اند. در برنامه پنج ساله پنجم توسعه کشور قرار بر آن است که در آینده نزدیک بیش از هفتاد درصد خدمات دولتی با بهره گیری از سامانه های خودکار و داده های الکترونیکی انجام شود. بدین ترتیب اجرای ماموریت ها و ارائه خدمات به عموم مردم بدون استفاده از این سامانه ها ممکن نخواهد بود. بنابر این امنیت اطلاعات در دستگاه های اجرایی از اهمیت ویژه ای برخوردار خواهند بود تا اطمینان از حفظ محرمانگی، یکپارچگی و دسترس پذیری اطلاعات و سامانه های اطلاعاتی حاصل شود. از سوی دیگر، کنترل های امنیت اطلاعات اگر به صورت ناکار آمد صورت گیرد می تواند منجر به مخاطرات مهمی در انجام ارائه خدمات دولتی و چرخه ارائه خدمات شود.

نمونه های مخاطراتی که عملیات حوزه سایبری را تحت تاثیر قرار می دهد عبارتند از:

- تخریب و سرقت منابع مالی در روند پرداخت های عمومی و جمع آوری مبالغ پرداختی
- استفاده از امکانات رایانه ای برای رسیدن به مقاصد غیرمجاز و یا برای حمله به سایر سامانه ها
- افشاء، مرور و نسخه برداری از اطلاعات حساس، همانند داده های مودیان مالیاتی، سوابق امنیت اجتماعی، سوابق پزشکی، مدارک مالکیت معنوی و اطلاعات تجاری خصوصی به منظور سرقت هویت، جاسوسی و یا سایر انواع جرایم.
- ایجاد اخلال در عملیات اساسی، همانند عملیاتی که زیرساخت های حیاتی را پشتیبانی می کنند و دفاع ملی و خدمات اضطراری را حمایت می نمایند.
- افزودن، تغییر دادن و یا حذف داده ها به منظور فریب، اختفا یا قطع جریان اطلاعات

- ایجاد حوادث گیج کننده در زیرساخت های حیاتی که منجر به کاهش اعتماد عمومی به توانمندی دستگاه های اجرایی برای انجام عملیات و ایفای مسئولیت هایشان می شود.

تهدیدات سایبری که دستگاه های اجرایی را در خطر قرار می دهند، عمدتا با هدف دست یابی به سامانه های اطلاعاتی آنها و زیرساخت های اساسی مبتنی بر سایبر عمل می کنند.

تهدیدات سایبری به هر دو شکل غیر عمدی و عمدی می توانند وجود داشته باشند. همچنین این تهدیدات می توانند هدفمند یا بدون هدف گذاری خاصی صورت پذیرند و نکته مهم دیگر آن است که این تهدیدات از منابع متعددی بر می خیزند.

تهدیدات غیر عمدی ناشی از کارکنان (آموزش ندیده) یا بی توجه، ارتقاء و به روز آوری نرم افزاها، رویه های نگهداری و نقایص و عیوب تجهیزاتی می باشد که به صورت غیر عمدی موجب اخلال در عملکرد سامانه ها و یا تخریب داده ها می شوند.

تهدیدات عمدی می تواند از نوع هدفمند و بدون هدف باشد. حمله هدفمند هنگامی رخ می دهد که فرد یا گروهی به سامانه خاصی یا زیرساخت حیاتی مبتنی بر سایبر حمله نماید. حمله بدون هدف هنگامی صورت می گیرد که هدف مورد نظر حمله، نامعین می باشد. مانند وقتی که ویروس، کرم یا سایر بد افزارها بدون هدف مشخصی در اینترنت رها می گردند.

نگرانی های عمده ای در خصوص توانمندی های بالقوه برای انجام حمله سایبری وجود دارد. اینترنت و سایر زیرساخت های ارتباطی فرصت هایی را برای مهاجمین بوجود می آورند تا بتوانند اقدام به قطع ارتباطات، قطع شبکه برق رسانی و سایر زیرساخت های حیاتی بنمایند. از آنجا که دولت، بخش خصوصی و عموم مردم رویکرد سریع و پرحجمی به عملیات شبکه ای دارند و استفاده از سامانه های دیجیتال و بی سیم همه گیر شده است و طراحی، ساخت و بهره برداری از محصولات و خدمات مبتنی بر فناوری اطلاعات، مرزها را در نوردیده است، تهدیدات نیز به تبع این تحولات، رشد فزاینده ای خواهند داشت.

با توجه به شکل گیری قرارگاه پدافند سایبری و مراکز پدافند سایبری در دستگاه های اجرایی کشور، می بایست هنگامی که حوادث سایبری رخ می دهد، بلافاصله دستگاههای اجرایی کشور باید مرکز پدافند سایبری خود و سپس از طریق آن مرکز پدافند سایبری کشور را در جریان امر قرار دهند.

«ماهیت فضای سایبری»

تهدیدات ناشی از فعالیت ها در فضای سایبری حداقل سه مشخصه دارند:

۱–گسترده :

طبیعت تهدید راهبردی در فضای سایبری همانند خود فضای سایبری گسترده است. هر بخشی از جهان که وابسته به فضای (حوزه) سایبر باشد حداقل به صورت بالقوه در معرض خطر قرار دارد. بنابراین کشورها با فعالیت های خصمانه ای روبرو هستند که می تواند تهدید کننده یکپارچگی زیرساخت های حیاتی آنها باشدبه طوری که می تواند و سامانه های مالی را از پایداری خارج سازد و یا به سارقان مالکیت معنوی امکان سرقت بدهد و یا به هر روش مهم دیگر توانایی کشورها برای اتکاء بر فناوری در جهت نیل به اهداف مهم امنیت ملی آنها را کاهش دهد.

۲– نهفته:

تهدیدات مربوط به یکپارچگی اطلاعات و امنیت در فضای سایبری عمیقاً در حوزه سایبر نهفته می باشند. این تهدیدات ناشی از آسیب پذیری های بالقوه موجود یا قرار داده شده در سیستم های عامل نرم افزاری پیچیده و همچنین ناشی از سخت افزارهای بالقوه معیوب یا ناقص می باشند. لفظ نهفته به این دلیل به کار می رود که تهدید بالقوه، ویژگی ذاتی فضای سایبری بوده و لذا هرگز نمی توان آن را بطور کامل کشف و آشکار نمود. این تهدیدات گاهی در زمان عبور کالاها از زنجیره تأمین در آنها تعبیه می گردند.

۳– متنوع:

تهدیدات در فضای سایبری متنوع می باشند. گروه های جنایتکار و خرابکار با سازماندهی مناسب، سازمانهای مستقل مدیریتی و هکری از هر عنوانی، در صحنه حضور دارند. هر یک از این عاملان خرابکاری، نوع مجزایی از تهدید را تحمیل می نمایند.

دلایل و عوامل تفاوت تهدیدات فضای سایبری از تهدیدات دنیای واقعی:

- طبیعتاً گستره فضای سایبری جهانی است، که حوزه های کنترلی متداخل و هم پوشانی را برای فعالان عرصه کشوری همراه با رویکردهای حقوقی و فرهنگی مختلف و منافع راهبردی گوناگون ایجاد می نماید.
- کشورهای دنیا به اندازه کافی در امور ارتباطات و کنترل دنیای فیزیکی وابسته به حوزه سایبر شده اند؛ به نحوی که جدا شدن از آن قطعاً غیر ممکن است. از این رو وظایف و کارکردهای امنیت ملی تحت تأثیر روز افزون فضای سایبری می باشد.

- با توجه به تولید محصولات نرم افزاری و سخت افزاری در سطح جهانی (مثلا در چین، هند و مکزیک)، فراهم کردن تضمین در فرایند زنجیره تامین محصول، غیر ممکن می باشد.
- مقیاس پذیری حوزه سایبری آن را از نظر کیفی متفاوت می سازد. یک بمب در شدیدترین شرایط محدوده فیزیکی محدودی دارد؛ اما تهدیدات سایبری گستره تاثیر بسیار وسیعی از خود به جای می گذارد بنابراین با ساز و کاری مواجه هستیم که می تواند عملیات واقعی را در مقیاس جهانی کنترل نماید.
- همانند بسیاری از دیگر زمینه های تخصصی دانش، عملیات در درون حوزه سایبری، توسط تعداد نسبتاً کمی از افراد کنترل می شود. کاربران قابلیت عملی برای اصلاح یا کنترل نرم افزار و سخت افزار مورد استفاده خود را ندارند. پوشیده نیست تعداد قلیلی از افراد به طور موثر جنگ سایبری را کنترل نموده و یا می توانند اداره نمایند.
- علیرغم تمرکز و دانش تخصصی مورد نیاز، طبیعت توزیع شده حوزه سایبری مانع شخص یا گروهی از اشخاص می شود که بخواهند کنترل کامل را در دست بگیرند.
- تغییرات در حوزه سایبری به سرعت رخ می دهد و مبنای آن پیشرفت مرتب فناوری های محاسباتی و ارتباطی است. به هم پیوستگی حوزه سایبری این شتاب را افزایش می دهد. هر تغییر دوره جدیدی از آسیب پذیری و پاسخ را بوجود می آورد. فضای سایبری فاصله زیادی از حالت ایستا داشته و تقریبا سرتاسر آن پویاست.
- توزیع دارایی های سایبری در همه انواع سازمان ها گسترده است، از سامانه های بسته و تحت کنترل دولتی تا سامانه های در مالکیت و مدیریت بخش های غیر انتفاعی جامعه، هر یک با منابع و امکانات مختلف و ظرفیت ها و نگرانی های متفاوت در صحنه حضور دارند.
- و در نهایت طبیعت فضای سایبری به گونه ای است که، در حال حاضر توانایی فنی برای انتساب فعالیت ها به افراد یا گروه ها یا سازمان ها، با درجه بالایی از اطمینان وجود ندارد.

تهدیدات مبنا در فضای سایبری عبارتند از:

۱. تهدیدگران خارجی
۲. تهدیدگران داخلی
۳. تهدیدات موجود در زنجیره تأمین کالا
۴. تهدیدات ناشی از عدم کفایت توانمندی عملیاتی نیروهای خودی

جدول۲: منابع تهدیدات سایبری

منبع تهدید	توصیف
کشورهای خارجی	سرویس های اطلاعاتی کشورهای خارجی برای انجام بخشی از فعالیت های جمع آوری اطلاعات و جاسوسی خود از ابزار سایبری استفاده می کنند. در سطح جهان موارد متعددی از این دست برای سوء استفاده و تخریب زیرساخت های اطلاعاتی کشورها شامل اینترنت، شبکه های اطلاعاتی، سامانه های رایانه ای و پردازشگرها و کنترل کننده های نهفته در صنایع حیاتی مشاهده شده است.
گروه های خرابکار	گروه هایی از افراد که به منظور کسب درآمد، به سامانه های سایبری حمله می برند که به طور روزافزون تهاجمات این گروه ها رو به افزایش است.
هکرها	هکرها گاهی اوقات برای اظهار وجود خود وارد شبکه می شوند. در شرایط فعلی نفوذ به شبکه ها با حداقل دانش و مهارت امکان پذیر است به این طریق که آنها برنامه ها و پروتکل های لازم را از اینترنت دریافت نموده و همان ها را بر علیه سایت های دیگر بکار می برند.
هکرهای سازمان یافته	افراد دارای انگیزه سیاسی که به صفحات وب مورد نیاز عموم مردم یا میزبان های پست الکترونیک حمله می کنند، هکتیویسم نام دارند. این افراد معمولاً میزبان های پست الکترونیک را با افزایش بار مواجه نموده و با نفوذ به سایت های شبکه وب پیام های سیاسی خود را اعلام می نمایند.
عوامل ناراضی داخلی	عوامل ناراضی داخلی که در درون سازمان فعالیت می کنند منبع اصلی جرایم رایانه ای هستند و این دسته از عوامل لازم نیست دانش قابل توجهی در خصوص تهاجمات رایانه ای داشته باشند زیرا اطلاع آنها از سیستم مورد هدف غالباً امکان دسترسی نامحدود برای وارد کردن ضربه به سامانه و یا سرقت اطلاعات سازمان را فراهم می سازد. تهدید عوامل داخلی شامل کارکنان پیمان کاران نیز می شود.
تروریستها	تروریست ها به دنبال تخریب، ناتوان سازی و یا بهره برداری بدخواهانه از زیرساخت های حیاتی به منظور تهدید کردن امنیت ملی، وارد آوردن خسارات سنگین، تضعیف اقتصاد کشور و تخریب روحیه و اعتماد عمومی می باشند.

جدول۳: انواع و روش های حملات سایبری

نوع حمله	توصیف
انکار خدمات	در این روش دسترسی کاربران مجاز به سامانه و بالعکس از دست می رود. در واقع حمله کننده از یک نقطه شروع به غوطه ور کردن کامپیوترهای هدف در پیام های مختلف و انسداد آمد و شد قانونی داده ها می نماید. این امر باعث می شود که هیچ سامانه ای نتواند از اینترنت استفاده و یا با سامانه های دیگر ارتباط برقرار کند.
انکار گسترده خدمات	در این روش به جای شروع حمله از یک منبع، همزمان از تعداد زیادی سامانه توزیع شده اقدام به حمله می کنند. غالباً این کار با استفاده از کرم ها و تکثیر آنها در رایانه های متعدد برای حمله به هدف صورت می گیرد.
ابزارهای سوء استفاده	این ابزار ها در دسترس عموم قرار دارد که می توانند با برخورداری از سطوح مهارتی مختلف آسیب پذیری های موجود در شبکه ها را کشف و از آن طریق وارد شوند.
بمب منطقی	نوعی خرابکاری که در آن برنامه نویس کدی وارد برنامه می نماید که در صورت بروز اتفاقی خاص، برنامه خود به خود یک فعالیت تخریبی را صورت می دهد.
اسنیفر	برنامه ای است که داده های مسیریابی شده را شنود نموده و با بررسی هر بسته در جریان داده ها به دنبال اطلاعات خاصی مانند کلمه های عبور می گردد.
اسب تروا	برنامه ای رایانه ای که کدی خطرناک را مخفی می کند. معمولاً اسب تراوا دارای ظاهری مشابه برنامه های مفیدی است که کاربر تمایل به اجرای آنها دارد.
ویروس	برنامه ای است که فایل های رایانه ای که معمولاً برنامه های اجرایی هستند را با وارد کردن نسخه ای از خود در آن فایلها آلوده می سازد با بارگذاری فایل های آلوده در حافظه، این نسخه ها اجرا و به ویروس امکان آلوده کردن سایر فایل ها را می دهد. بر خلاف کرم ها ویروس برای انتشار نیازمند دخالت انسانی است.
کرم	برنامه ای رایانه ای مستقل که با نسخه برداری از خود از یک سامانه به سامانه دیگر در شبکه تکثیر می شود. بر خلاف ویروس های رایانه ای، کرم ها نیازی به دخالت انسان برای انتشار ندارند.
جاسوس افزار	بدافزار نصب شده بدون اطلاع کاربر برای ردیابی و یا ارسال داده ها به طرف سوم غیر مجاز به صورت پنهانی
شماره گیری مکرر	برنامه ساده ای که شماره تلفن های متوالی را شماره گیری می کند تا مودمی را پیدا کند.
جنگ شبکه های	روشی برای امکان ورود به شبکه های رایانه ای بی سیم با استفاده از یک لپ تاپ،

بی سیم	آنتن و کارت شبکه بی سیم که شامل گشت زنی در موقعیت های خاص برای دسترسی غیر مجاز می باشد.
ارسال هرزنامه	ارسال نامه های پست الکترونیک تجاری ناخواسته که می تواند حاوی سازوکار تحویل نرم افزار های مخرب و سایر تهدیدات سایبری باشد.
سرقت کلمه های عبور و اطلاعات مالی	با استفاده از هرزنامه افراد را فریب می دهد تا اطلاعات حساس خود را افشا نمایند.
ساخت وب سایت جعلی	ایجاد یک وب سایت فریب برای تقلید از یک سایت واقعی و مشروع و معمولاً در مورد پست الکترونیک این عمل هنگامی رخ می دهد که آدرس فرستنده و دیگر بخش های مشخصات نامه الکترونیک تغییر داده می شود به طوری که گیرنده تصور می کند نامه از مبدأ معتبری ارسال شده است.
فریب	روشی که دزدان کلمه عبور برای فریب کاربران و متقاعد کردن آنها از ارتباط با وب سایت معتبر بکار می برند.
بات نت	شبکه ای از سامانه های کنترل از راه دور آلوده، که برای هماهنگی حملات، توزیع بدافزار و هرزنامه و پیام های سرقت اطلاعات بکار برده می شود. بات ها معمولاً به صورت مخفیانه در سامانه هدف نصب می شوند و امکان کنترل از راه دور رایانه مورد هدف را به کاربر غیر مجاز می دهند تا اهداف خرابکارانه خود را محقق کنند. از بات نت ها به عنوان سربازان الکترونیکی نیز نام برده می شود.

ویژگی های حملات سایبری:

۱. نیازی به نزدیکی فیزیکی مهاجمین به اهداف خود برای انجام حملات سایبری وجود ندارد.
۲. فناوری امکان عبور از مرزهای ملی و بین المللی را به راحتی برقرار می کند.
۳. حملات را می توان به صورت خودکار و با سرعت بسیار زیاد و با حمله همزمان به اهداف بی شماری صورت داد.
۴. مهاجمین به راحتی می توانند گمنام باقی بمانند.

«انواع حملات سایبری»

۱. استراق سمع به‌صورت عام (مکالمات، دیتا، تصویر) به روش‌های مختلف و از راه دور
۲. جاسوسی از راه دور و از طریق بستر شبکه
۳. اختلال یا قطع شبکه‌های اطلاع رسانی مانند قطع سیگنال رسانی به صدا و سیما
۴. قطع کامل یا اختلال در شبکه‌های ارتباطات تلفنی داخل و یا خارج از کشور (شهری، بین شهری، بین‌الملل، موبایل)
۵. اختلال در شبکه‌های مراکز مختلف خدماتی از قبیل: بانک‌ها، پالایشگاه‌ها، نیروگاه‌ها، سدها، مراکز صنعتی، مراکز کنترلی، شبکه‌های حمل و نقل و ترافیک، شبکه‌های توزیع برق و آب و...
۶. انهدام و یا آسیب‌رسانی به تاسیسات صنعتی کشور از قبیل پالایشگاه‌ها، نیروگاه‌ها و... با استفاده از نفوذ در سیستم های کنترلی این تاسیسات
۷. عضویت غیرارادی سرورها و رایانه های کشور در گروه‌های هکری و سربازگیری الکترونیکی موسوم به بات نت جهت سازماندهی و مشارکت غیرارادی در حملات سایبری
۸. ممانعت از استفاده برخی سرویس‌های شبکه جهانی اینترنت به بهانه تحریم‌ها
۹. قطع ارتباط با سامانه میزبانیHosting (مراکز داده در مواقع حساس)
۱۰. حمله سایبری به مراکز نگهداری داده اعم از بومی و غیر بومی
۱۱. دسترسی غیر مجاز به بانک‌های اطلاعاتی مختلف از قبیل دسترسی غیر قانونی به بانک اطلاعاتی سازمان ثبت احوال کشور
۱۲. ورود غیر قانونی به حریم خصوصی افراد و امکان ایجاد مشکلات مختلف برای زندگی مردم
۱۳. حمله به وب سایت‌های متعلق به سازمان ها ، نهادها به منظور جلوگیری از ارائه خدمات به مردم
۱۴. تهدیدات فرهنگی جامعه از قبیل رواج بی بندوباری، ایجاد بی اعتقادی، سست کردن باورهای مذهبی، تهاجم فرهنگی
۱۵. تهدیدات اجتماعی جامعه از قبیل بسیج و سازماندهی اغتشاشات و ناآرامی های مختلف در کشور و یا تشکیل و هدایت گروههای منحرف و .....
۱۶. تهدیدات سیاسی از قبیل انجام اقدامات هماهنگ علیه یک کشور
۱۷. تهدیدات اقتصادی و مالی از قبیل اعمال تحریم های اقتصادی از طریق فضای مجازی از قبیل ممانعت از خرید و فروش اینترنتی کالا و خدمات یا جلوگیری از نقل و انتقالات پولی و بانکی
۱۸. تهدیدات امنیتی از قبیل تروریسم سایبری

۱۹. دستکاری و مخدوش نمودن اطلاعات موجود در فضای سایبر

۲۰. جعل هویت در شبکه های ارتباطی و رایانه ای

سربازان جنگ سایبری **"نفوذگران"** در عرصه اطلاعات دیگران هستند که کارشناسان این حوزه، آنها را به چند گروه تقسیم کرده‌اند:

- **گروه نفوذگران کلاه سفید:** هر کسی که بتواند از سد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه‌ای انجام ندهد را یک هکر کلاه سفید می‌خوانند که در حقیقت متخصصین شبکه‌ای هستند که حفره های امنیتی شبکه را پیدا کرده و به مسئولان گزارش می‌دهند.
- **گروه نفوذگران کلاه سیاه:** اشخاصی هستند که وارد رایانه قربانی خود شده و به دستبرد اطلاعات و یا جاسوسی کردن و یا پخش کردن بدافزار و غیره می‌پردازند.
- **گروه نفوذگران کلاه خاکستری:** اشخاصی هستند که حد وسط دو تعریف بالا می‌شوند.
- **گروه نفوذگران کلاه صورتی:** این افراد آدم‌های کم سوادی هستند که با چند نرم‌افزار خرابکارانه به آزار و اذیت بقیه اقدام می‌کنند.

اصلی ترین **حملات نفوذگران** عبارت است از:

* **شنود:** در این روش نفوذ گر می‌تواند به شکل مخفیانه از اطلاعات نسخه برداری کند.
* **تغییر اطلاعات:** در این روش نفوذگر به دستکاری و تغییر اطلاعات می‌پردازد.
* **افزودن اطلاعات:** در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می‌کند.
* **وقفه:** در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود.

بر اساس آنچه کارشناسان مبارزه با جنگ سایبری اعلام می کنند، بررسی هویت و مکان مهاجم، شناسائی نیت مهاجم، تشخیص حمله‌های از قبل طراحی شده و بررسی و ارزیابی تلفات بعد از جنگ، از مهم ترین نقاط ضعف اصلی در دفاع سایبری است.