بسمـــــه تعالی

آشنایی با پدافند غیر عامل

پدافند در مفهوم کلی، دفع، خنثی کردن و یا کاهش تاثیرات اقدامات آفندی دشمن و ممانعت از دستیابی به اهداف خودی است.

پدافند به دو بخش تقسیم می‌شود ۱- پدافند عامل ۲- پدافند غیرعامل

پس از وقوع انقلاب صنعتی در قرن هجدهم در اروپا و توسعه بیشتر، (پژوهش و توسعه) پیشرفت‌های شگرفی در همه سطوح فناوری پدید آمد. به طوری که دوران کنونی به ویژه دو دهه اخیر را (عصر انقلاب سوم فناوری) یا (دوران انقلاب در میکروالکترونیک) نامیده‌اند، تحولات مذکور لزوما فناوری تسلیحاتی را به شدت تحت تاثیر قرار داد به طوری که همه ابعاد و سطوح این فناوری بسیار پیچیده شده و در خصوص طرح‌های نظامی جنبه راهبردی یافته است. پیشرفت سریع علوم و فناوری نظامی در زمینه تولید انواع سلاح‌های آفندی توسط کشورهای پیشرفته و توان همپائی سایر کشورها موجب گردیده است تا بحث پدافند به ویژه دفاع غیر عامل توسط کشورهای اخیرالذکر مورد توجه جدی قرار گیرد.

اقدامات دفاع غیر عامل شامل اصول اساسی و ملاحظاتی است که در اغلب کشورهایی جهان، این اصول و ملاحظات با کمی اختلاف پذیرفته شده اند ولی شیوه به کارگیری آنها ابتکاری، هنرمندانه و خردمندانه است نه اینکه کلیشه‌ای باشد به همین دلیل وسعت هر اصل به خلاقیت‌های فکری بشر و شرایط زمان و مکان بستگی دارد و بعضا حد و مرزی برای این اصول نمی‌توان تعیین کرد و لذا در حد غیر قابل تصوری در نحوه بکارگیری اصول دفاع غیر عامل تنوع وجود دارد. در این مقاله سعی گردیده است پس از تبیین اصول و ملاحظات دفاع غیر عامل و موضوعات ذیربط، توصیه‌هایی چند در خصوص اقدامات دفاع غیر عامل ارائه گردیده است.

اصول پدافند عامل:

مجموعه اقدامات بنیادی و زیر بنایی است که در صورت بکار گیری می‌توان به اهداف پدافند غیر عامل از قبیل تقلیل خسارات و صدمات، کاهش قابلیت و توانایی سامانه شناسائی، هدف یابی و دقت هدف گیری تسلیحات آفندی دشمن و تحمیل هزینه بیشتر به وی نائل گردید.

در اکثر منابع علمی و نظامی دنیا اصول پدافند غیر عامل شامل ۶ الی ۷ اقدام مشروحه ذیل می‌باشد که در طراحی و برنامه ریزی‌های و اقدامات اجرایی دقیقا می‌بایست مورد توجه قرار گیرد.

۱- استتار Camouflage

۲- اختفا Concealment

۳- پوشش Cover

۴- فریب Deception

۵- تفرقه و پراکندگی Separation And Dispersion

۶- مقاوم سازی و استحکامات Hardening

۷- اعلام خبر Early warning

تعاریف و اصلاحات

* پدافند (Active Defense)

عبارتست از بکارگیری مستقیم جنگ افزار، به منظور خنثی نمودن و یا کاهش اثرات عملیات خصمانه هوایی، زمینی، دریایی، نفوذی و خرابکارانه بر روی اهداف مورد نظر.

**** پدافند غیر عامل (Passive Defense)***

به مجموعه اقداماتی اطلاق می گردد که مستلزم بکارگیری جنگ افراز نبوده و با اجرای آن می‌توان از وارد شدن خسارات مالی به تجهیزات و تاسیسات حیاتی و حساس نظامی و غیر نظامی و تلفات انسانی جلوگیری نموده و یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد.

* دفاع غیر نظامی (Civil Defsnse)

دفاع غیرنظامی تقلیل خسارات مالی و صدمات جانی وارده بر غیر نظامیان در جنگ یا در اثر حوادث طبیعی نظیر سیل، زلزله، طوفان، آتش‌فشان، آتش‌سوزی و خشکسالی می‌باشد، در منابع خارجی، وظایف دفاع غیر نظامی شامل چهار عنوان ذیل می‌باشد:

۱- اقدامات پیشگیرانه و کاهش دهنده (Mitigation)

۲- آماده سازی و امداد رسانی (Preparation)

۳- هشدار و اخطار (Response)

۴- باز سازی مجدد (Recovery)

* مراکز حیاتی و مراکز ثقل (Vital and Gravity Centers)

مراکز و تاسیسات حیاتی و پر اهمیت کشور می‌باشند که در صورت حمله و بمباران و انهدام آنها صدمات جدی به نظام

اجتماعی، سیاسی و نظامی کشور وارد شده، آنها را در یک مخاطره و بحران جدی قرار می‌دهد.

* مراکز حیاتی (Vita Centers)

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تاثیرگذاری در سراسر کشور گردد.

*مراکز حساس (Critical Centers)

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل‌توجهی در نظام سیاسی، هدایت، کنترل و فرماندهی تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تاثیر گذاری منطقه‌ای در کشور گردد.

* مراکز مهم (Important Centers)

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز آسیب و صدمات محدود در نظام سیاسی، اجتماعی، دفاعی با سطح تاثیر گذاری محلی در کشور گردد.

* استتار و اختفاء (Concealment & Camouflage)

فن و هنری است که با استفاده از وسائل طبیعی یا مصنوعی، امکان کشف و شناسائی نیروها، تجهیزات و تاسیسات را از دیده بانی، تجسس و عکسبرداری دشمن تقلیل داده و یا مخفی داشته و حفاظت نماید.

مفهوم کلی استتار، همرنگ و هم‌شکل کردن تاسیسات، تجهیزات و نیروها با محیط اطراف می‌باشد.

اختفا، حفاظت در برابر دید دشمن را تامین می‌نماید و استتار امکان کشف یا شناسایی نیروها، تجهیزات و تاسیسات و فعالیتهای را تقلیل می‌دهد.

* پراکندگی(Dispersion)

گسترش باز و پخش نمودن و تمرکز زدایی نیروها، تجهیزات، تاسیسات یا فعالیت‌های خودی، به منظور تقلیل آسیب پذیری آنها در مقابل عملیات دشمن به طوری که مجموعه‌ای از آنها هدف واحدی را برای دشمن تشکیل ندهند.

* تفرقه و جابجایی (Separation and Movement)

جداسازی، گسترش افراد، تجهیزات و فعالیت‌های خودی از محل استقرار اصلی به محلی دیگر به منظور تقلیل آسیب پذیری، کاهش خسارات و تلفات می‌باشد، مانند: انتقال هواپیماهای مسافرتی به فرودگاه‌های دورتر از برد سلاح‌های دشمن و یا انتقال تجهیزات حساس قابل حمل از محل اصلی به محل موقت که به علت عدم شناسایی و حساسیت مکانی، دارای امنیت و حفاظت بیشتری می‌باشد.

*استتار، اختفاء و ماکت فریبنده D &CC

استفاده و بهره برداری از اقدامات تجهیزات و روش‌هایی برای پنهان نمودن، همگون سازی، تغییر شکل، شبیه سازی، ایجاد طعمه فریبنده و حذف شکل منظم هندسی اهداف در جهت ممانعت از کشف و شناسائی نیروها، تجهیزات، تاسیسات و فعالیت‌های خودی توسط سامانه‌های آشکار ساز و حساسه دشمن.

* فریب (Deception)

کلیه اقدامات طراحی شده حیله‌گرانه‌ای که موجب گمراهی دشمن در نیل به اطلاعات و محاسبه و برآورد صحیح از توان کمی و کیفی طرف مقابل گردیده و او را در تشخیص هدف و هدف گیری با شک و تردید مواجه نماید.

* مقاوم سازی و استحکامات (Fortification)

ایجاد هر گونه حفاظتی که در مقابل اصابت مستقیم بمب، راکت، موشک، گلوله توپخانه، خمپاره و یا ترکش آنها مقاومت نموده و مانع صدمه رسیدن به نفرات، تجهیزات یا تاسیسات گردیده و اثرات ترکش و موج انفجار را به طور نسبی خنثی نماید. پناهگاه، جان پناه، سازه‌های امن و مقاوم‌سازی تاسیسات، ایجاد استحکامات صحرایی و سازه‌های موقتی، دال بتنی، کیسه شن، خاک‌ریز، بشکه شن و یا استوانه بتنی و... جزء استحکامات محسوب می‌شوند.

* اعلام خبر (Early warning)

آگاهی و هشدار به نیروهای خودی مبنی بر نزدیک بودن عملیات تعرضی دشمن.

این هشدار که برای آماده شدن می‌باشد، ممکن است چند ساعت، چند روز و یا زمانی طولانی‌تر از آغاز مخاصمات اعلام گردد.

دستگاه‌ها و وسایل اعلام خبر شامل رادار، دیده‌بانی بصری، آژیر، بلندگو، پیامها و آگاهی های هشدار دهند می‌باشد.

* مکان یابی (Site selection)

یکی از اقدامات اساسی و عمده پدافند غیر عامل، انتخاب مکان مناسب می‌باشد تا آنجا که ممکن است باید از ایجاد تاسیسات حیاتی و حساس در دشت‌های مسطح یا نسبتا هموار اجتناب کرد. زیرا تاسیسات احداث شده در چنین محل‌هایی را نمی‌توان از دید دشمن مخفی نگاهداشت.

ایجاد تاسیسات حیاتی و حساس در کنار بزرگراه‌ها، جاده‌های اصلی، کنار سواحل دریا، رودخانه‌ها و نزدیکی مرزها موجب سهولت شناسایی و هدف یابی آسان آنها توسط دشمن می‌گردد.

توضیح اینکه سه موضوع عمده که می‌بایست در مکان یابی به آن توجه خاص مبذول گردد به شرح ذیل می‌باشد:

۱- ماموریت (Mission)

امکان اجرای ماموریت در مکان تعیین شده موجود باشد.

۲- پراکندگی (Dispersion)

وسعت مکان انتخابی به صورتی باشد که امکان پراکندگی مناسب تاسیسات و تجهیزات را فراهم نماید.

۳- شکل عوارض و محیط (Terrain Pattern)

چشم انداز پدافند غیر عامل

- دارای عزم ملی و باور عمومی در مسئولین و مردم نسبت به رعایت اصول پدافند غیر عامل
- برخوردار از اصول پدافند غیر عامل جامع ، توسعه یافته و نهادینه شده
- توانمند در تأمین حداکثر ایمنی و پایداری و به حداقل رسانیدن آسیب پذیری زیر ساخت های مرتبط در مقابل تهدیدات دشمن
- قادر به ایفای نقش اساسی در حراست و حفظ استقلال ، تمامیت ارضی و سرمایه های ملی در چرخه نظام دفاعی امنیتی کشور
- برخوردار از آمایش سرزمینی مناسب و متکی به ویژگیهای جغرافیایی ، جمعیتی وفرهنگی و اصول دفاع غیر عامل در حوزه مختلف با رعایت توزیع و پراکندگی موزون سرمایه ها و فعالیت ها در عرصه ایمن جغرافیا
- توانمند در تولید دانش فنی و برخوردار از پشتوانه تحقیقاتی و پژوهشی در زمینه پدافند غیر عامل با تأثیر باز دارندگی بالا و با موفقیت ممتاز در سطح منطقه
- دارای پشتوانه فرهنگی و حقوقی و قانونی جامع در سطح کشور با قابلیت تأمین و اجرای الزامات و ضوابط مربوطه
- برخوردار از نظام یکپارچه ، هماهنگ و کارآمد پدافند غیر عامل کشور با قابلیت تعامل سازنده و پیشبرنده با دولت در زمینه اعمال تدابیر دفاعی امنیتی در بخش های مختلف

راهبردهای پدافند غیرعامل

- تعامل گسترده و فراگیر با سازمان ها و ایجاد سازو کارهای مناسب در جهت ایمن سازی و حفاظت از تاسیسات زیربنایی
- ساماندهی آمایش سرزمین ملی و آمایش دفاعی از منظر پدافند غیرعامل به منظور استفاده حداکثری از پهنه جغرافیایی کشور

- ایفای نقش هدایتی و نظارتی بر سازمان ها و نهادهای کشوری و لشکری در زمینه مطالعات و طراحی فنی طرح های پدافند غیرعامل
- بکارگیری و بسیج امکانات در جهت ارزان سازی، تنوع و ابتکار عمل در سامانه ها و شیوه های پدافند غیرعامل
- استفاده حداکثرسازی از پهناوری و عمق سرزمینی و عوارض طبیعی کشور و به کاهش مخاطرات و خسارات
- ساماندهی مناسب استفاده از فناوری های نوین به منظور کاهش آسیب پذیری ناشی از وابستگی و امکان جمع آوری اطلاعات توسط دشمن
- توسعه و تعامل موثر و سازنده با نهادهای سیاست گذار، قانون گذار و اجرایی کشور
- توسعه علمی و تولید دانش فنی و ارتقاء فناوری و برنامه جامع آموزشی و همچنین ، بهینه سازی تولید صنعتی با استفاده از تمامی ظرفیت ها
- نهادینه نمودن نظام جامع و استفاده از اصول و ضوابط در طرح های توسعه کشور
-

قابلیت‌های پدافند غیرعامل

- پدافند غیر عامل، بستر مناسب توسعه پایدار توان ملی کشور
- پدافند غیر عامل، هم راستا با سیاست های تنش زدایی
- پدافند غیر عامل، پایدارترین، ارزان ترین وصلح آمیزترین روش دفاع
- پدافند غیر عامل، بهترین راهکار افزایش آستانه مقاومت ملی
- پدافند غیر عامل، پشتوانه اقتدار ملی
- پدافند غیر عامل، یکی از مهمترین ابزارهای بازدارندگی
- پدافند غیر عامل، بهترین و مناسب ترین شیوه کاهش مخاطرات و کاهش آسیب پذیری
- کشورهایی که توسعه پدافند غیر عامل را به عنوان یک سیاست دفاعی مستمر در دستور کار خود قرار می دهند، هیچ گاه در مظان اتهام تهدید بر علیه کشورهای دیگر قرار نمی گیرند
- کشورهایی که پدافند غیر عامل را به عنوان یک راهکار اصلی بر می گزینند، به شرایطی از نظر کاهش آسیب پذیری دست می یابند که مطامع کشورهای تهدید کننده بر علیه آنها کاهش می یابد
- در جهان امروز کشورهایی که نقاط آسیب پذیری آنها فراوان است، و دشمن می تواند با ضربات سریع، حیاتی ترین منابع آنان را منهدم نماید، عوامل تهدید از بیرون را درون خود ایجاد می نماید
- پدافند غیر عامل، می تواند به یک فرهنگ عمومی در کشور تبدیل شود

- پدافند غیر عامل، عنصری است پویا و متحرک؛ لذا باید همواره در صدر تلاش های علمی و پژوهشی قرار گیرد

دفاع اقتصادی

یکی از واقعیت های حال حاضر در فضای اقتصاد بین الملل، تقابل و درگیری اقتصادی است؛ امری که در فضای ادبیات علمی اقتصاد کمتر بدان پرداخته میشود چون فرض بنیادین در علم اقتصاد، آزادی تجارت و دادوستد است. تقابل اقتصادی در برخی از موارد، ازجمله مقابلهٔ برخی قدر تهای غربی با جمهوری اسلامی ایران، از حد متعارف آن خارج شده و به جنگ تمام معیار اقتصادی تبدیل شده است.

اگر چه میتوان استفاده از ابزارهای اقتصادی در مقابلهٔ کشورها را در دوران پس از جنگ جهانی دوم یعنی دوران به اصطلاح جنگ سرد جستجو کرد ولی جنگ اقتصادی علیه جمهوری اسلامی ایران هم به لحاظ مدت زمانی که بیش از سه دهه از آغاز آن می گذرد و هم به لحاظ ابعاد گستردهٔ آن خصوصاً از زمستان سال ۱۳۹۰ و هم از نظر صف بندی بین المللی، نمونه ای کم نظیر در این نوع جنگ هاست.

نکته درخور تأمل دربارهٔ جنگ تمام عیار اقتصادی این است که متأسفانه با وجود اینکه سابقه تحریم و محدودیت اقتصادی در جهان به بیش از یک قرن م یرسد، جنگ اقتصادی واژ های ناشناخته برای مجامع علمی محسوب میشود و محتوای منسجمی در این حوزه وجود ندارد. این درحالی است که کشورهای متخاصم با تحمیل ادبیات اقتصادی متعارف به کشورهای مختلف و نگنجاندن راهکارهای مقابله و برون رفت از جنگ اقتصادی، نظریات جنگ اقتصادی را برای به چالش کشیدن زیرساختهای حیاتی اقتصادی کشورهای هدف طراحی کرده و با آمادگی کامل وارد این وادی شده است. نمونه ای از این تلاش ها را میتوان در گزارش ۱۴ آوریل ۲۰۱۴ دربارهٔ شکل گیری اتاق جنگ مدرن اقتصادی آمریکا در وزارت خزانه داری این کشور ملاحظه کرد. این اتاق جنگ در حکم خط مقدم جبههٔ اقتصادی ایالات متحده و شرکای بین المللی آن محسوب می شود. تیم ۱۷۰ نفرهٔ جنگ اقتصادی شامل مجموع های از وکلا، استراتژیست ها و تحلیلگران اطلاعاتی است که قدرت فوق العاده ای در قطع و مسدودکردن تبادلات ارزی دلاری در سراسر جهان دارد .

در تمامی جنگ های اقتصادی آمریکا علیه کشورهای مختلف، به واسطه سیطرهٔ نظریات لیبرال سرمایه داری در کشورهای هدف و فقدان ایدئولوژی قوی و ساختار حکومتی منسجم در آن کشورها، آمریکا توانسته بود به بسیاری

از اهداف ازپیش تعیین شدهٔ خود نائل شود اما دربارهٔ ایران با پدیدهٔ پیچیده ای مواجه شده است که عبارت است از مقاومت مکتبی که در متن رفتارهای مردم و حاکمان اثرات عمیق و خدشه ناپذیری دارد. این روحیهٔ مقاومت باعث شده است که پس از وضع تحریم های گسترده و ایجاد ممنوعیت ها و موانع مختلف در مسیر حرکت اقتصاد ایران خصوصاً تحریمهای سالهای اخیر که به «تحریمهای فلج کننده » معروف شده است، اقتصاد ایران نه تنها پابرجا بماند بلکه بتواند همچنان نیازهای مردم را تأمین و معیشت آنها را اداره کند. این روحیهٔ مقاومت مردمی ریشه در اندیشهٔ اسلامی و نظام حاکمیتی ایران دارد که پس از پیروزی انقلاب اسلامی در قالب جمهوری اسلامی و حکومت ولی فقیه متبلور شده است. رهبران انقلابی ایران، از همان ابتدای استقرار نظام اسلامی، با توجه به خصومتهای دشمنان در عرصه های مختلف، از تهاجم اقتصادی قدرتهای جهانی غافل نبودند و در برهه های مختلف آن را متذکر شده اند. حضرت امام خمینی (ره) در همان سال های ابتدایی پیروزی انقلاب اسامی (۹/ ۳/ ۶۱) دربارهٔ جنگ اقتصادی فرمودند: «شما درحال جنگید الان. یک جنگی که جنگ اقتصادی است. یک محاربه الان مابین اسلام و کفر است که محاربهٔ اقتصادی یکیش است » (صحیفه امام، ج ۱۱، ص: ۴۲۵) و در حالی که دشمن متخاصم نقشهٔ تحریم فروش نفت را کلید زد حضرت امام خمینی ره این تحریم ها و جنگ اقتصادی علیه ایران اسلامی را یک تحفه الهی نامیدند (صحیفه امام خمینی .ج ۱۱.ص ۴۲۴)

در چند سال اخیر نیز مقام معظم رهبری نیز با الهام از مفاهیم ارزشمند الهی و دینی و همچنین احاطه به نقش ههای دشمن، با اعلام وضعیت جنگی در حوزهٔ اقتصاد، توجه مردم و مسئولان کشور را به این خطر بزرگ و تهاجم گسترده جلب کرده اند و لزوم ایجاد آمادگی ها و تدارکات لازم برای مقابله با این جنگ تمام عیار را در مناسبت های مختلف متذکر شده اند. ایشان در جلسهٔ تبیین سیاستهای اقتصاد مقاومتی فرمودند: «تحریم ها از قبل بود منتها این تحریم ها از حدود زمستان سال ۹۰ تا امروز، تبدیل شده به جنگ اقتصادی. دیگر اسم آن تحریم هدفمند نیست، یک جنگ تمام عیار اقتصادی است که متوجه ملت ما است.

براساس بند ۵ اصل ۱۱۰ قانون اساسی، اعلام جنگ و صلح کشور برعهده رهبری می باشد و در این وضعیت، مقام معظم رهبری در تاریخ بیستم بهمن ۱۳۹۲ ، کشور را درگیر جنگ تمام عیار اقتصادی ترسیم کردند. از همین رو، سازمان پدافند غیرعامل کشور در راستای دفاع از ساختارهای حیاتی اقتصادی کشور و خنثی کردن تهدید دشمن، وارد عرصهٔ پدافند اقتصادی کشور شد. قرارگاه پدافند اقتصادی با هدف کاهش آسیب پذیری اقتصادی، مقاوم سازی اقتصاد، تداوم چرخهٔ تولید، ذخیره سازی و نگهداری و تسهیل مدیریت بحران در وضعیت تحقق تهدیدها، افزایش بازدارندگی اقتصادی و درنهایت مصون سازی اقتصادی در برابر تهدیدها و اقدامات خصمانه و مخرب دشمن، به تدوین سیاستهای مختلف و برنامه ریزی، هدایت و راهبری، طراحی و پیاده سازی راهبردهای جامع دفاع اقتصادی و نیز فرهنگ سازی با رویکرد اقتصاد مقاومتی اقدام کرده است. ا گرچه ابلاغ سیاستهای اقتصاد مقاومتی با

توجه به فشار و تهدید دشمن، خود از امور پدافند غیرعامل محسوب می شود، سازمان پدافندغیرعامل کشور در حوزههایی که مرتبط با دفاع اقتصادی است به صورتی فعال وارد شده است تا در رفع تهدیدات دشمن و کمک به ادارهٔ بهتر مردم از طریق تدوین برنامه های راهبردی و راهکارهای عملیاتی به همهٔ ارکان نظام و خصوصاً قوای سه گانه همیاری رساند و وظیفهٔ ذاتی و سازمانی خود را به انجام رساند.

پدافند غیر عامل زیستی

پدافند غیرعامل زیستی چیست؟

هرگونه آلودگی از نوع ویروسی یا میکروبی که به وسیله آذوقه یا هر نوع نیازمندی‌های طبیعی توسط دشمنان به کشور وارد شود، تهدید زیستی به شمار می‌رود و مجموعه اقداماتی که در جهت کاهش آسیب‌پذیری جامعه و حفظ سرمایه انسانی انجام می‌شود، پدافند غیرعامل است.

وقتی صحبت از تهدیدات زیستی می‌شود، منظور تهدیدات طبیعی از جمله زلزله و سیل نیست، بلکه منظور تهدیدات انسان ساز است که توسط دشمن، عوامل دست نشانده دشمن در داخل و عوامل انسانی به طور ناخواسته پیش می‌آید، چون اولویت نخست پدافند غیرعامل زیستی حفظ جان انسان‌ها و به عبارتی حفظ سرمایه انسانی کشور است، لذا حتی اگر عوامل زیستی ناخواسته ایجاد شود و جان انسان را تهدید کند، به نظر پدافند غیرعامل نوعی تهدید تلقی می‌شود. دشمن از این طریق جمعیت را دچار مشکل می‌کند و به موجب آن هزینه‌های کشور مورد حمله را افزایش میدهد.

دفاع سایبری

حملات پیشرفته‌ی سایبری، خطرهای جدی را برای اقتصاد و امنیت ملی کشورها پدید آورده است. امروزه کشورها استفاده از پدافند غیرعامل را به‌تنهایی برای مقابله با حملات سایبری کافی نمی‌دانند. پدافند عامل سایبری، شامل اقداماتی در جریان حمله یا قبل از حمله‌ی دشمن است که می‌تواند موجب بهبود تشخیص، جلوگیری و پاسخگویی به حملات سایبری دشمن می‌شود.

در این نوع پدافند که به «Proactive Cyber Defense» شهرت دارد، مدافع از سلاح‌های سایبری برای پاسخگویی به دشمن استفاده می‌کند، درحالی‌که هدف، در پدافند غیرعامل سایبری، کاهش ضرر و زیان خسارات ناشی از حملات سایبری است. درمجموع می‌توان در تعریف پدافند عامل سایبری، به تعریف پنتاگون در راهبرد امنیت سایبر سال ۲۰۱۱، اشاره کرد.

«دفاع سایبری فعال و عامل یعنی توانایی تشخیص، کشف، تحلیل و کاهش تهدیدات و آسیب‌پذیری‌ها. در واقع این نوع دفاع مجموعه اقداماتی برای دفاع از سامانه‌ها و شبکه‌ها است. اقداماتی برای تکمیل رزمایش‌ها با رویکردهای جدید. در دفاع غیرعامل سایبری، از نرم‌افزارها، حس‌گرها و جمع‌آوری اطلاعات برای تشخیص و توقف بدافزارها – قبل از وقوع حمله–استفاده می‌شود.»

امروزه حملات سایبری، فقط یک حادثه مجزا و تک‌مرحله‌ای نیستند. به همین دلیل دفاع در برابر آن‌ها، احتیاج به مهارت‌های سایبری دارد. حملات سایبری دارای مراحلی است که آن‌ها را به ۷ دسته، تقسیم می‌کنند و در هر مرحله باید دفاع متناسب با آن صورت بگیرد تا بتوانیم دفاع فعال سایبری را انجام داده باشیم.

- بازشناسی: در این مرحله دشمن، اهداف خود را تشخیص می‌دهد. معمولاً در این مرحله، هکرها به دنبال یافتن آسیب‌پذیری‌ها هستند.
- مسلح شدن: در این مرحله، دشمن ابزار حمله‌ی خود را انتخاب می‌کند.
- ارسال: دشمن در این مرحله، بدافزار یا هرگونه ابزار دیگر را به هدف موردنظر، انتقال می‌دهد.
- به کار انداختن: در این مرحله، ابزار موردنظر هکر، در کمین قربانی است تا به‌محض انجام هرگونه اقدامی، به هدف هجوم آورد.
- استقرار: بدافزار یا هر ابزار دیگری، در این مرحله، خود را از در سیستم وی، مخفی می‌کند.
- کنترل و فرماندهی: زیرساخت‌های کنترل و فرماندهی شامل سرورها و سایر زیرساخت‌های فنی است که برای کنترل بدافزار به کار می‌رود.
- انجام مأموریت: در نهایت ابزار موردنظر هکر، به اهداف وی، جامه‌ی عمل می‌پوشاند و انتظارات هکر را برآورده می‌کند.

دفاع الکترونیک(جنگ الکترونیک)

جنگ الکترونیک یا جنگال (کوتاه‌شده *جنگ الکترونیک*) اصطلاحی نظامی و بیانگر کاربرد الکترونیک و امواج الکترومغناطیس در نبردهاست و شامل ارتباطات رادیویی، ایجاد اختلال در ارتباطات رادیویی دشمن و شنود (استراق سمع) گفتگوهای دشمن است.

امروزه کاربردهای نوین دیگری مانند هدایت نفرات و موشک‌ها با دستگاه‌های الکترونیکی به جنگ الکترونیک افزوده شده‌است. دستگاه پارازیت‌انداز شعاع اصلی از این جمله دستگاه‌هاست که با ایجاد چگالی از انرژی در مسیر سیگنال فرستاده می‌شود و با افزودن نوفه (نویز) به آن، رادار را مختل می‌کند. البته می‌توان آن را شناسایی کرد.

افراد یگان جنگال می‌کوشند تحرک هر فرستنده‌ای را کشف، صدای هر گوینده‌ای را ضبط و هرگونه سامانه الکترونیکی تهدیدآمیز را نابود کنند.

بکارگیری سایت‌های شنود متحرک مجهز به سامانه‌های رهگیری مراقب، استراق سمع، ضبط و ثبت فرستنده‌های فعال دشمن، پخش پارازیت شنود و فریب الکترونیکی اهمیت ویژه‌ای در این گونه عملیات دارد. تجهیزات شنود، سامانه‌های اختلالگر، جهت‌یاب‌های مختلف، رادارها و سامانه‌های کشف و رهگیری و رمزشکن از لوازم یگان جنگال است.

دفاع اطلاعاتی(جنگ اطلاعات)

مقصود از «جنگ اطلاعاتی»، عملیات‌های تهاجمی و تدافعی است که توسط سازمان‌های تشکیلاتی یا فردی با سیاست‌های خاص و اهداف راهبردی برای بهره‌برداری و یا تخریب اطلاعات موجود در رایانه‌ها یا شبکه اینترنت و دیگر سیستم‌های اطلاعات شبکه‌ای به کار گرفته می‌شود.

جنگ اطلاعاتی یک ویژگی درگیری‌های نظامی است که سامانه‌های اطلاعاتی به طور مستقیم یا غیرمستقیم مورد تهاجم واقع شده یا از آنها دفاع می‌شود تا بدین ترتیب داده‌ها، دانش، باورها یا پتانسیل جنگ‌جوئی دشمن افت کرده یا کاملا نابود شود و در عین حال داده‌ها،دانش، باورها و میل جنگ‌جوئی نیروهای خودی حفظ شود.

- پدافند غیرعامل / جنگ نرم / روش‌های جنگ نرم / تکنیک‌های جنگ روانی / پدافند روانی

دایره المعارف "ویکی پدیا" پس از معرفی جنگ فرماندهی و کنترل جامع ترین تعریف ممکن را برای جنگ اطلاعات ارائه می دهد:"جنگ فرماندهی و کنترل عبارت است از کاربرد یکپارچه امنیت عملیات، فریب نظامی، عملیات روانی، جنگ الکترونیک و تخریب فیزیکی برای تاثیرگذاری، افت کیفیت، یا تخریب توانمندی‌های

فرماندهی و کنترل دشمن و در عین حال حفاظت از توانمندی‌های فرماندهی و کنترل خودی در برابر اقدامات مشابه دشمن. زمانی که هدف اصلی چنین جنگی چیزی بیش از فرماندهی و کنترل و ارتباطات دشمن باشد از اصطلاح عمومی تر جنگ اطلاعاتی استفاده می‌شود که در سطوح غیرنظامی همچون جنگ دیپلماسی و سیاسی و دیگر اشکال ارتباطات نیز کاربرد دارد.

امنیت اطلاعاتی: امنیت اطلاعاتی عبارت است از فرایند شناسایی و تحلیل اطلاعاتی که برای عملیات های نیروهای خودی حیاتی می باشد و شامل موارد زیر است:

- شناسایی اطلاعاتی که سامانه های اطلاعاتی دشمن می توانند آن را مشاهده نمایند.
- تعیین شاخص‌هایی که نشان می‌دهد سامانه‌های اطلاعاتی مهاجم چگونه اطلاعات حیاتی را در زمان مناسب برای بهره‌برداری نیروهای دشمن استخراج می کنند.

گزینش و اجرای اقداماتی که آسیب پذیری برای اقدامات نیروهای خودی را در برابر سوء استفاده نیروهای دشمن از بین برده یا کاهش می‌دهند.

اصطلاح جنگ اطلاعاتی برای نخستین‌بار در سال ۱۹۷۵ میلادی مورد استفاده قرار گرفت و کشور های پیشرفته در زمینه تکنولوژی به اهمیت آن پی بردند و تلاش کردند در زمینه‌های سیاسی، اقتصادی، نظامی و فرهنگی آن را بکار ببرند.

در اواخر دهه ۹۰ اصطلاح جنگ اطلاعاتی دامنه وسیع تری یافت و به عملیات اطلاعاتی معروف گشت و منظور از آن هر گونه عملیات نظامی یا غیر نظامی با هدف سلطه بر تفکر دشمن بود به گونه ای که به دلخواه ما فکر کند و اجرای تصمیم‌هایش منافع مارا تامین کند و از طرف دیگر ممانعت از اینکه دشمن همانند این عملیات را بر علیه ما بکار ببرد.

تکوین جنگ اطلاعاتی مستقیماً با پیشرفت های سریع در تکنولوژی های اطلاعاتی جدید مثل شبکه های الکترونیک در طی دو دهه اخیر مرتبط است.

- مفهوم شناسی:

اطلاعات: اطلاعات در اینجا به معنای محتوا یا معنی یک پیام است هدف از جنگ‌ها همیشه تاثیر گذاری بر سیستم های اطلاعاتی دشمن بوده است. در معنای گسترده تر، سیستم های اطلاعاتی دربردارنده نوعی وسیله یا شیوه ای هستند که بدان طریق بتوان به آگاهی یا اعتقادات خاصی دست پیدا کرد در معنای محدود آنکه سیستم های

اطلاعاتی مجموعه‌ای کامل از دانش، اعتقادات و فرایندهای تصمیم گیری دشمن هستند نتیجه مطلوب نیز آن خواهد بود که دشمن پیام هایی را دریافت کند که او را به توقف جنگ متقاعد سازد.

نبرد Warfare: نبرد مجموعه‌ای از تمام فعالیت‌های مهلک و غیر مهلک است که برای غلبه بر اراده حریف یا دشمن انجام می‌شود. در این معنا Warfare مترادف (War) و نیازمند اعلام جنگ نیست و در عین حال با شرایطی که وضعیت جنگی نامیده می‌شود همراه نمی‌گردد نبرد می‌تواند از سوی گروههای دولتی، گروههای مورد حمایت دولتی یا [گروه های] غیر دولتی، یا بر ضد آنها صورت گیرد. هدف از نبرد لزوماً کشتن دشمنان نیست بلکه فقط مهم تحت کنترل درآوردن آنان است.

- جنگ اطلاعاتی

جنگ اطلاعاتی عبارتست از استفاده از شبکه‌های الکترونیکی برای تخریب یا از کار انداختن و غیر عملیاتی کردن زیر ساخت های اطلاعاتی دشمن که هم می‌تواند علیه یک جامعه (اهداف غیر نظامی) و هم علیه ارتش یا نیروی نظامی آن جهت گیری شود. جنگ اطلاعاتی علیه ارتش یا نیروی نظامی می‌تواند مرکب از جنگ کنترل و فرماندهی (W۲C) جنگ جاسوسی محور و جنگ الکترونیکی باشد و علیه جامعه و نیروهای غیر نظامی می‌تواند مرکب از جنگ اطلاعاتی/ اقتصادی و جنگ روانی، سرقت یا تخریب اطلاعات کامپیوتری باشد.

- فرق جنگ اطلاعاتی با جنگ با تکنولوژی و تسلیحات پیشرفته

استفاده از شبکه های الکترونیکی برای اهداف مزیت اطلاعاتی بخش عظیمی از جنگ اطلاعاتی را تشکیل می‌دهند اصطلاح جنگ اطلاعاتی که روز به روز استفاده از آن گسترده تر می‌شود اغلب به اشتباه جنگ با تکنولوژی و تسلیحات پیشرفته که ارتش های بزرگ و پیشرفته از ان استفاده می‌کنند اشتباه گرفته می‌شود. در حالی که باید توجه داشت از تکنولوژی اطلاعاتی پیشرفته در زمینه بالا بردن دقت، افزایش برد و تقویت قدرت کشندگی سلاح های متعارف استفاده می‌شود، اما در جنگ اطلاعاتی هیچ کدام از این عناصر کاربرد ندارند. جنگ اطلاعاتی صرفاً به اطلاعات و داده‌ها که در قالب ذرات الکترونیک شناخته می‌شوند محدود نمی‌گردد. حتی تخریب فیزیکی مبادلات مخابرات نیز جنگ اطلاعاتی محسوب نمی‌شود، اما از کارانداختن سیستم سوئیچینگ تلفن‌ها با ویروس، جنگ اطلاعاتی نامیده می‌شود.

اصولاً، جنگ اطلاعاتی نتیجه ظهور جامعه اطلاعاتی است که هنوز در بسیاری از کشورها معمول نشده است در جوامع اطلاعاتی تمامی مبادلات اجتماعی، اقتصادی، سیاسی و فرهنگی ماهیتاً دیجیتال شده اند و البته وابسته به کامپیوتر. یعنی در جامعه اطلاعاتی بیشتر اتفاقات معنادار بین افراد و سازمان‌ها با واسطه کامپیوترها و شبکه های

کامپیوتری صورت می‌پذیرد. وضعیت در این جوامع به گونه‌ای است که مقادیر زیادی از اطلاعات سیستم های پیچیده شامل شهرها، بازارهای مالی، بهداشت، ثروت و ذخایر، تولید و حتی توزیع را در داخل خود جای داده اند.

- سطوح جنگ اطلاعاتی

جنگ اطلاعاتی را باید در دو سطح مورد توجه قرار داد: در سطح تاکتیکی و در سطح استراتژیک.

سطح تاکتیکی: شکل های سنتی حملات اطلاعاتی مانند اقدامات ضد رادار در حوزه فرماندهی، نظارت، ارتباطات، نیز رخنه کامپیوتری و عملیات روانی است که از ویژگی های زیر برخوردار می‌باشد:

- روش های اقدام و ضد اقدام
- اهداف، منطقه‌ای هستند و دورنمای محدودی دارند وصرفاً در یک عملیات رزمی خاص قابلیت هماهنگی وجود دارد
- از فعالیت های نظامی پشتیبانی می کند.

این شکل از حملات در سطح تاکتیکی انجام می‌شود و نیاز به دانستن مشخصات تکنیکی و روش های عملیاتی دارد و می تواند در قالب چند عملیات همزمان و پی در پی انجام شود. در اینجا، صحنه نبرد گسترش می‌یابد و از محدوده مرزهای جغرافیایی و زمانی در زمان صلح، بحران و یا صحنه نبرد گسترش می‌یابد.

سطح استراتژیک: جنگ افزارهای استراتژیک جنگ اطلاعاتی به طور گسترده‌ای باعث کاهش اهمیت فاصله و مسافت می‌شوند، به طوری که آسیب پذیری‌های I۳C در میدان جنگ اهمیت کمتری از آسیب پذیری های زیر ساخت های غیر نظامی ملی پیدا می کند.

- اهداف

اصولاً هدف نهایی این رویارویی، روند تصمیم گیری رقیب و دشمن است در تعریف گسترده مشترک از جنگ اطلاعاتی، اهداف واقعی جنگ اطلاعاتی صرفاً بر روی سیستم های تهاجمی دشمن متمرکز نمی‌باشند بلکه بر روی روندهای تصمیم گیری دشمن طراحی می‌شود. به همین دلیل باید گفت که طراحی حملات جنگ اطلاعاتی بر اساس مشخصات سیستم های تهاجم نیست بلکه، بر پایه تاثیر گذاری در سطوح بالای فرماندهی است مثلاً در یک عملیات جنگ الکترونیک، حملات اختلالی علیه حس گرها بر اساس دانستن مشخصات تکنیکی و عملیاتی حس گرها می‌باشد، در حالی که در جریان حمله جنگ اطلاعات، طراحی و هدایت آن علیه اطلاعاتی که حس گرها از وضعیت منطقه برای نیروهای تهاجم بدست می‌آورند، مد نظر می‌باشد.

اهداف جنگ اطلاعاتی را می‌توان در سه سطح یا لایه از هم متمایز کرد که در هر سطحی یک پیامد خاص ایجاد می‌شود:

- لایه سیستم اطلاعاتی: این سطح شامل عناصر مادی، تولید، انتقال و ذخیره می‌باشد و حملات علیه سیستم های اطلاعاتی باعث ایجاد پیامدهای تکنیکی می‌شود
- لایه مدیریت اطلاعاتی در این سطح روندهای پردازش اطلاعات و مدیریت آن مورد حمله قرار می‌گیرد و باعث ایجاد پیامدهای کارکردی می‌شود
- لایه تصمیم گیری این سطح مربوط به تصمیم گیری و استفاده از اطلاعات در امر تدوین و تنظیم سیاست و تصمیمات است. حملات در این سطح، می‌تواند پیامدهای عملیاتی ایجاد کند.

ویژگی جنگ اطلاعاتی دارای یکسری ویژگی های خاص خود است که بررسی آن‌ها به درک بیشتر آن کمک می‌کند. مهمترین ویژگی هایی که برای این جنگ برشمرده اند عبارتند از:

- کم هزینه بودن ورود به جنگ اطلاعاتی: داشتن تخصص در سیستم های اطلاعاتی و شبکه های الکترونیکی یا داشتن متخصص در این زمینه و دسترسی به شبکه های الکترونیکی از شرایط لازم مهم برای ورود به این قسم از جنگ می‌باشد.ساز و برگ جنگ اطلاعاتی برای پیشبرد از جنگ با بسیج شهروندان نیاز دارد و نه به بسیج منابع ، به جای آن فقط به جذب لبه های پیشرو نوآوری های صنعتی برای مقاصد تکیه می‌کند مثل مهندسی الکترونیک، کامپیوتر، مخابرات، هوافضا و... .
- فناوری فوق العاده پیچیده : ساز و برگ جنگ اطلاعاتی با استفاده از فناوری های فوق العاده پیچیده هدایت می‌شود.
- انعطاف پذیری : به دلایل گوناگون، ساز و برگ جنگ اطلاعاتی به برنامه ریزی نیاز دارد، اما این برنامه ریزی برای پاسخی انعطاف پذیر است برای جنگی که تحرک، انعطاف پذیر و واکنش سریع را در اولویت قرار می‌دهد. برنامه ریزی ازقبل: به خاطر چنین پیچیدگی در برنامه ریزی برای انعطاف پذیری است که بسیاری از جنبه های ساز و برگ جنگ اطلاعاتی را از پیش برنامه ریزی می‌کنند، و از آن طریق دست جنگ جویان واقعی را کوتاه می‌سازند.
- خدشه در مرزبندی های سنتی: متعدد بودن مخالفان و دشمنان احتمالی، تنوع در جنگ افزارها و گوناگونی استراتژی‌ها موجب می‌شود که شناسایی منابع تهدید در این جنگ به طور فزاینده‌ای با مشکلات فراوانی رو به رو شود، به طوری که اغلب اوقات با دشواری می‌توان بین منابع داخلی و خارجی تهدیدهای جنگ اطلاعاتی تفاوت و

تمایز قایل شد. حتی نمی‌توان به راحتی دریافت که چه کسی مورد حمله قرار گرفته و چه کسی متهم به حمله کردن است مرز بین زمان صلح و جنگ به طور فزاینده‌ای کدر می‌شود.

- افزایش اهمیت و نقش دستکاری: در جنگ اطلاعاتی این امکان وجود دارد تا با تکیه بر تکنیک های اطلاعاتی، توانایی فریب و دستکاری را افزایش داد.
- مشکلات سخت هشدار تاکتیکی و ارزیابی حمله: در حال حاضر هیچ گونه سیستم هشدا دهنده تاکتیکی با کفایتی که قادر باشد بین حملات استراتژیک جنگ اطلاعاتی و دیگر انواع فعالیت های ارتباطات کامپیوتری نظیر جمع آوری اطلاعات یا حوادث اتفاقی تمایز ایجاد می کند وجود ندارد. نتیجه آنکه نمی‌توان تشخیص داد که دقیقاً چه زمانی حمله می‌شود، از کجا حمله می‌شود، چه کسی حمله می کند و تهاجم چگونه هدایت می‌شود.
- چالش جدید جاسوسی: در جهان سایبر سپس جایی برای پنهان شدن وجود ندارد. با افزایش ماهواره‌ای متصل به شبکه های الکترونیکی توان مراقبت الکترونیکی بی نهایت افزایش می‌یابد.
- دشواری ایجاد و نگهداری ائتلاف: متعدد بودن مخالفان و دشمنان احتمالی که می‌توانند به صورت فردی نیز ظاهر شوند و تنوع در جنگ افزارها و استراتژی‌ها و کاهش توانایی پیش بینی متحدان و دشمنان، ایجاد ائتلاف و نگهداری آن را با مشکل فزاینده روبرو می کند.

انواع و اشکال جنگ اطلاعاتی:

جنگ فرماندهی و کنترل (Command and control warfare): هدفش قطع ارتباط بین ساختار و فرماندهی دشمن از بدنه زیر فرمانش است.

از این نوع جنگ با نام (I۴C) نیز نام برده شده که مخففand communication Command, control است که از چهار C پدید آمده است فرماندهی، نظارت و کنترل، رایانه و ارتباطات. که خود به دو صورت انجام می‌شود.

- هدف قراردادن سرفرمانده (Antihead) در گذشته همواره این نوع عملیات بر حذف فیزیکی فرماندهی عالی جنگ متمرکز بوده و به طور کلی حذف آنها تاثیرات قابل توجهی بر نتایج جنگ داشته است امروزه علاوه بر اهمیت نقش فرماندهان مراکز فرماندهی به عنوان مولفه‌ای بسیار مهم این نوع عملیات ایفای نقش می کند حمله به

یک مرکز فرماندهی بویژه اگر به موقع انجام گیرد، م یتواند حتی بدون زدن یک فرمانده عالی رتبه دشمن، عملیات را مختل کند.

- هدف قراردادن گردن فرمانده (Antineck) : این عملیات علیه خطوط ارتباطی و اطلاعاتی فرماندهی و بخش های مختلف صحنه‌ی عملیات صورت می گیرد. قطع این ارتباط الکترونیکی منجر به ضعف و شکست می‌شود.

جنگ اطلاعات – محور [یا جنگ مبتنی بر اطلاعات – عملیات] (Intelligence Based Warfare [IBW])

این نوع جنگ زمانی رخ می‌دهد که اطلاعاتی به گونه‌ای مستقیم عملیات‌ها را دارد (به خصوص در تعیین هدف و ارزیابی خسارت های جنگی) هدایت کند، به جای اینکه اطلاعات به عنوان یک داده به فرماندهی و کنترل منتقل و مورد استفاده قرار گیرد این جنگ منجر به کاربرد مستقیم فولاد (بمب) علیه دشمن می‌شود (به جای اینکه بایت‌ها را خراب کند). این جنگ در دو محور انجام می‌شود.

- جنگ اطلاعات- محور آفندی (جنگ تهاجمی) (Offensive IBW) : افزایش سریع قدرت در مقایسه با قیمت فناوری های اطلاعاتی (بویژه فناوریهای سیستم های پخش متمرکز) طرح های جدیدی را برای جمع آوری و پخش اطلاعات عرضه می کند محیط جنگ های آینده دارای حس گرهای گوناگونی خواهد بود که به طور کامل میدان جنگ را نشان می‌دهند بدین ترتیب فرمانده می‌تواند طرح‌ها و برنامه های نبرد را اجرا کند.
- جنگ اطلاعات- محور پدافندی (جنگ تدافعی) (Defensive IBW)

در اینجا آنچه مهم است ایجاد روش دفاعی به منظور افزایش شکاف میان تصویر و واقعیت در میدان جنگ است . [یعنی کاری کنیم که حس گرهای دستگاه های جمع آوری اطلاعات دشمن، یا به اطلاعاتی نرسند یا اگر رسیدند منطبق با واقعیت نباشد].

جنگ الکترونیکی (Electronic Warfare): جنگ الکترونیکی برای کاهش دادن ارتباطات، چه در سطح فیزیکی (از طریق پارازیت در رادارها یا مخابرات) و چه در سطح ترکیبی (بوسیله رهگیری یا حقه زدن) انجام می‌شود.

انواع جنگ الکترونیکی:

- ضد رادار (Antiradar): از طریق ایجاد پارازیت ها، کارایی رادار را مختل می کند.
- ضد مخابرات (Anti communications) یا هدف قراردادن ارتباطات
- رمزنگاری (cryptography): مخابره پیام‌ها به صورت رمز در بین نیروهای خودی

- جنگ روانی (Psychological Warfare): استفاده از اطلاعات بر علیه ذهن و فکر افراد و انسان‌ها.

اشکالات آن عبارتند از:

- عملیات علیه اراده ملی (counter-will)
- عملیات علیه فرماندهی دشمن
- عملیات علیه نیروهای نظامی
- جنگ فرهنگی (kulturkampf)

جنگ نفوذگر (مزاحم رایانه‌ای هکرها) (Hacke warfare): حمله هکرها به سیستم های اطلاعاتی نظامی و امنیتی

جنگ اطلاعاتی اقتصادی (Economic Information warfare) از راه تحریم اطلاعاتی حاصل می‌شود به طوری که بتوان با تحریم اطلاعات، موانعی را در تجارت و اقتصاد آن کشور هدف ایجاد کرد البته امکان فیزیکی تجارت، از بین نمی‌رود.

جنگ سایبر یا اینترنتی (cyber warfare): استفاده از کامپیوتر و اینترنت برای جنگیدن در فضای سایبر.

شیوه‌های حمله در این نوع جنگ:

- خرابکاریهای اینترنتی (Web Vandalism): حملاتی جهت تغییر محتوا و مشکل صفحات وب یا اخلال در سرویس دهی
- گردآوری داده ها: دسترسی به اطلاعات طبقه بندی شده برای جاسوسی
- حملات گسترده اخلالی در سرویس دهی
- اخلال در تجهیزات (equipment Disrupation) مهاجمان می‌توانند فرمان‌ها و ارتباطات را در فعالیت های نظامی که در آنها از رایانه و ماهواره برای هماهنگی استفاده می‌شود. رهگیری کرده یا تغییر دهند.
- حمله به زیرساخت های حیاتی: نیروگاههای برق، تاسیسات آبرسانی و سوخت رسانی، ارتباطات، حمل و نقل و ... .

جنگ ادراکی: عملیات هایی که به منظور تاثیرگذاری بر عقاید و رفتار مردم، از رسانه‌ها جمعی در دسترس آنها سوء استفاده می کنند. جنگ ادراکی هدفی مشابه عملیات روانی دارد اما حوزه عمل آن از حوزه عملی عملیات روانی گسترده است.

ابزارهای جنگ اطلاعاتی:

- ویروس ها: ویروس‌ها برنامه هایی می‌باشند که قادر به تکثیر خود برنامه های بزرگتر هستند. برنامه های ویروس وقتی فعال می‌شوند که برنامه میزبان شروع به فعالیت کند و دنبال آن ویروس خود را تکثیر می‌کنند و برنامه های دیگر را آلوده می‌نمایند ویروس‌ها در هر محیط کامپیوتری ساخته می‌شوند. پس تعجب آور نیست که به مثابه جنگ افزار اطلاعاتی مورد استفاده قرار بگیرند . وقتی یک عامل ویروس های کامپیوتری را به داخل شبکه های کامپیوتری رخنه داده باشد، در آن حالت شبکه هدف از کار می‌افتد و یا حداقل نارسایی های وسیعی در آن‌ها ایجاد می‌شود.

- کرم ها: کرمها یک برنامه مستقل است که به طور شعله ور خودش را تکثیر می‌کند و از یک کامپیوتر به کامپیوتری دیگر و اغلب بر روی شبکه‌ها می‌ورد و برخلاف ویروس ها، برنامه های دیگر را تغییر نمی‌دهد. پیامدهای مخرب این جنگ افزار دو زمینه قابل بررسی است: یکی نابودی منابع موجودی اطلاعاتی در شبکه و دیگری تغییر شکل و انتشار در شبکه.

- اسب ترویا: اسب های ترویا برنامه هایی هستند که در داخل سایر برنامه‌ها پنهان می‌گردند و برنامه خود را به اجرار در می‌آورند. اسب ترویا می‌تواند خود را استتار کند و حتی در برنامه های ایمنی شبکه مانند SATAN قرار بگیرند.

- بمب منطقی: بمب منطقی یک نوع اسب ترویاست که برای آزاد کردن ویروس‌ها و یا سیستم های تهاجمی دیگری استفاده می‌شوند و می‌تواند به صورت یک برنامه مستقل که توسط برنامه نویس و طراح در سیستم جاسازی می‌شود عمل کند. نظر به این که تعداد زیادی نرم افزار از امریکا صادر می‌شود، پیشنهاد شده است که در هر نرم افزار صادراتی اسب ترویا نصب شود. این عامل مخفی می‌تواند در شرایطی که آن کشور علیه امریکا وارد جنگ شد، از راه دور فعال شده و اثرات مخرب آن می‌تواند شامل فرمت کردن دسک سخت و ارسال اسناد به سازمان سیا باشد.

- درهای پشتی یا دامی: این شامل سازوکارهایی است که طراح نرم افزار در زمان ساخت نرم افزار تعبیه می‌کند تا در زمانی که سیستم حفاظت کامپیوتر به طور طبیعی کار می‌کند به طراح امکان می‌دهد تا به طور مخفیانه وارد سیستم شود. این مکانیزم در زمان جنگ اطلاعاتی قادر است سیستم‌ها و اطلاعات ذخیره شده در کشورهای خارجی را مورد کاوش و جستجو قرار دهد این مهمترین مسئله و برنامه ریزی در استراتژی نظامی و منبعی برای فراهم آوردن اطلاعات حیاتی برای بخش جاسوسی است.

- تخریب چیپس ها: همانطور که نرم افزار می‌تواند کارهای غیر منتظره انجام دهد، می‌توان همان کارکرد را درون سخت افزار تعبیه کرد. چیپس های امروزی شامل میلیون‌ها مدار مجتمع می‌بانشد که سازنده آن به راحتی می‌تواند

در آن‌ها تغییر شکل دهد و همچنین قادر است کارهای غیرمنتظره انجام دهند. چیپس‌ها می توانند بعد از زمان خاصی از کار بیافتند یا بعد از رسیدن علائمی منفجر شوند و یا امواج رادیویی از خود صادر کنند که باعث تعیین دقیق محل آن‌ها شود.

- میکروب ها: این‌ها می‌توانند باعث تخریب های شدید در سیستم‌ها بشوند و برخلاف ویروس‌ها می‌توانند بر روی سخت افزار و نه نرم افزار موثر واقع شوند.با توجه به این که میکروبهایی وجود دارند که نفت می‌خورند این پرسش‌ها وجود دارد که آیا می‌توان آن‌ها را برای خوردن ماده سلسیم پرورش داد؟ در صورت عملی بودن، می‌توان پیش بینی کرد که بتوان کلیه مدارهای مجتمع را تخریب کرد.
- اختلالات الکترونیکی: استفاده از اختلالات کامپیوتری برای سد کردن ارتباطات و در مرحله پیشرفته دادن اطلاعات غلط و بیش از حد.
- بمب های EMP و تفنگ های HERF : HERF امواج رادیویی با قدرت زیاد است که می‌تواند امواج رادیوییی پر قدرت را به اهداف الکترونیکی شلیک کند و آنها را از بین ببرد. تخریب این وسیله می‌تواند کم شدت باشد و فقط موجب خاموش شدن و روشن شدن مجدد آن گردد و باعث صدمه به سیستم سخت افزاری(به طور فیزیکی) شود.اهداف آن می تواند یک مین فریم در داخل یک ساختمان و یا کل یک شبکه در داخل ساختمان باشد. حتی هدف می‌تواند یک وسیله متحرک باشد که به تجهیزات الکترونیک مجهز است.
- پالس های الکترومگنتیک: که منبع آن می‌تواند انفجارات هسته‌ای و یا غیر هسته‌ای باشد و می‌تواند توسط نیروهای ویژه‌ای که داخل منطقه دشمن نفوذ کرده اند در نزدیک مراکز الکترونیک منفجر شود و باعث تخریب قسمت های الکترونیک تمام کامپیوترها و سیستم های مخابراتی در منطقه کاملاً وسیع شود.

این پدیده که در آغاز به عنوان اثر جنبی آزمایش های هسته‌ای کشف شد. اکنون به مولد های غیر هسته‌ای گسترش یافته است این مولدها می‌توانند یک EMP ایجاد نمایند که سیستم های الکترونیکی حافظ را ناتوان سازد این بمب‌ها خساراتی را بوجود می‌آورند که دائمی است.

کاربردهای جنگ اطلاعاتی:

کاربردهای جنگ اطلاعاتی را در عرصه نظامی می‌توان به صورت زیر خلاصه کرد:

آمادگی

- در صحنه نبرد؛ ۲- مدیریت یکپارچه در صحنه نبرد (آمادگی درگیری شدید در صحنه نبرد، حمله در زمان مناسب و تدارک به موقع)

پدافند

- جلوگیری از قطع ارتباطات کامپیوتری در صحنه نبرد.

آفند

- سعی در قطع ارتباطات کامپیوتری در حوزه فرمتندهی ، نظارت ، ارتباطات کامپیوتری و جمع آوری اطلاعات و مراقبت و شناسایی .

جنگ اطلاعاتی با انقلاب اطلاعات ظهور پیدا کرده‌است. این انقلاب به دلیل دامنه وسیع و تاثیرات گسترده آن می‌تواند سبک نوینی از جنگ را ارائه بدهد.
مارتین لیبیکی، از محققان برجسته موسسه مطالعات استراتژیک در دانشگاه دفاع ملی، در کتاب «جنگ اطلاعاتی چیست؟» می‌نویسد «تلاش برای درک مفهوم جنگ اطلاعاتی مانند این است که چند نفر نابینا بخواهند با لمس کردن بخش‌های مختلف یک فیل بگویند که این موجود چیست. جنگ اطلاعاتی نیز شامل بخش‌های مختلف و متعددی م یشود.» تلاش برایداشن نگرش جامعه نگرانه در تعریف جنگ اطلاعات نکته ایست که باید حتماً به آن توجه شود.
مگان برنز در سال ۱۹۹۹ با نگرشی کلی تریف زیر را ارئه می‌دهد «جنگ اطلاعاتی طبقه یا مجموع‌های از تکنیک‌ها شامل جمع آوری، انتقال، حفاظت، ممانعت از دسترسی، ایجاد اغتشاش و افت کیفیت در اطلاعات است که از طریق آن یکی از طرفین درگیر بر دشمنان خود به مزیتی چشمگیر دست یافته و آن را حفظ می‌کند.»
مارتین لیبیکی ضمن وفادارماندن به تعریف کاملاً نظامی از جنگ اطلاعاتی هفت شکل مختلف جنگ اطلاعاتی را به شرح زیر نام می‌برد

- جنگ فرماندهی و کنترل که هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن، است.
- جنگ برپایه اطلاعات که متشکل از طراحی، حفاظت و ممانعت از دسترسی به سیستم هائی است که برای برتری بر فضای نبرد در جستجوی دانش کافی هستند.
- جنگ الکترونیک تکنیک‌های رادیوئی، الکترونیک، یا رمزنگاری.
- جنگ روانی که در آن از اطلاعات برای تغییر ذهنیت و طرزفکر دوستان، بی طرف‌ها، و دشمنان استفاده می‌شود.

- جنگ هکرها که در آن به سیستم‌های رایانه‌ای حمله می‌شود.
- جنگ اطلاعاتی اقتصادی ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات با هدف کسب برتری اقتصادی.
- جنگ سایبر ترکیبی از همه موارد شش گانه بالا.