جنگ مجازی

رایاجنگ، **نبرد مجازی**، یا **جنگ سایبری** (به انگلیسی: cyberwar یا cyberwarfare) به نوعی از نبرد گفته می‌شود که طرفین جنگ در آن از رایانه و شبکه‌های رایانه‌ای (به خصوص شبکه اینترنت) به عنوان ابزار استفاده کرده و نبرد را در فضای مجازی[۱] جاری می‌سازند.

تعریف

جنگ اطلاعاتی با انقلاب اطلاعات ظهور پیدا کرده‌است. این انقلاب به دلیل دامنه وسیع و تأثیرات گسترده آن می‌تواند سبک نوینی از جنگ را ارائه بدهد.
مارتین لیبیکی، از پژوهشگران برجسته مؤسسه 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 گوناگون یک فیل بگویند که این موجود چیست. جنگ اطلاعاتی نیز شامل بخش‌های گوناگون و متعددی می‌شود.» تلاش برای داشتن نگرش جامعه نگرانه در تعریف جنگ اطلاعات نکته‌ای است که باید حتماً به آن توجه شود.
مگان برنز در سال ۱۹۹۹، با نگرشی کلی تعریف زیر را ارئه می‌دهد: «جنگ اطلاعاتی طبقه یا مجموعه‌هایی از تکنیک‌ها شامل جمع‌آوری، 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 وفادار ماندن به تعریف کاملاً نظامی از جنگ اطلاعاتی هفت شکل گوناگون 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 بر پایه اطلاعات که متشکل از طراحی، حفاظت و ممانعت از دسترسی به سیستم‌هایی 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 طرز فکر دوستان، بی‌طرف‌ها 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 سایبری ترکیبی از همه موارد شش‌گانه بالا.

حمله‌های سایبری بین کشورها نخستین‌بار در سال ۲۰۰۸، با حمله اسرائیل و آمریکا به تأسیسات هسته ای ایران شروع شده که دردسرها و تنش‌های سایبری بعدی در ادامه آن ایجاد شده. در حمله سایبری، کشورها همدیگر را مورد حمله قرار می‌دهند و بدون اینکه به مرزهای هم حمله کنند، نتایج دلخواه خود را می‌گیرند. ضمن اینکه هزینه کمی دارد؛ چون فقط به تعدادی برنامه‌نویس نیاز دارد. این تنش‌ها همیشه در مقیاس‌های بزرگ نیست و اتفاقاً باید از حمله‌هایی ترسید که خیلی جزئی هستند و به راحتی قابل فهمیدن و شناسایی نیستند؛ مثلاً عوض کردن اطلاعات بانک خونی ارتش یک کشور.[۲]

نقاط ضعف اصلی در دفاع سایبر

- بررسی هویت و مکان مهاجم
- شناسائی نیت مهاجم
- تشخیص حمله‌های از قبل طراحی شده
- بررسی و ارزیابی تلفات پس از جنگ

اقدامات دیگر کشورها

پریزم یکی از عملیات سری آژانس امنیت ملی ایالات متحده آمریکا است که با آن، داده‌های کاربران شرکت‌های مخابراتی یا فناوری اطلاعات، مانند گوگل، فیس‌بوک، مایکروسافت، اپل، و ای‌تی‌اندتی، گردآوری می‌کند.

روسیه

سران روسیه اهمیت ویژه‌ای برای جنگ سایبر قائل هستند؛ به گونه‌ای که در رتبه‌بندی از نظر اهمیت جنگ سایبر را دقیقاً پس از جنگ هسته‌ای قرار می‌دهند. در سال ۱۹۹۵، یکی از فرماندهان روسی در کنفرانس مشترک روسیه – آمریکا دربارهٔ امنیت ملی در دوران پس از جنگ سرد اظهار داشت: «از دیدگاه نظامی، ما استفاده دشمنان از جنگ اطلاعاتی علیه کشور یا نیروهای مسلح روسیه را، به عنوان یک مرحله غیرنظامی درگیری تلقی نمی‌کنیم. با توجه به ابعاد و عواقب فاجعه‌آمیز استفاده از جنگ اطلاعاتی استراتژیک علیه نظام اقتصادی ملی، نظام فرماندهی و کنترل و به‌طور کلی علیه توانمندی‌های دفاعی و رزمی روسیه، ما این حق را برای خود محفوظ می‌دانیم که در برابر ابزارها و نیروهای مهاجم اطلاعاتی و در مرحله بعد علیه خود کشور مهاجم از سلاح هسته‌ای استفاده کنیم.»

چین

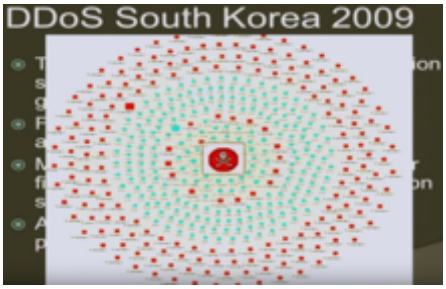
امروزه چین تعاریف و مفاهیم جدیدی را در واژگان نظامی وارد کرده‌است. در سال‌های اخیر، چین در زمینه استفاده از فناوری نوین و نیز تغییرات فراوان در آموزش، یک انقلاب نظامی واقعی در فضای سایبر را تجربه کرده‌است. فعالیت‌های چین به قدری پیشرفت کرده‌است که موجب نگرانی مقامات آمریکایی شده‌است.
علی‌رغم اینکه فعالیت‌های چین محدود به ترجمه اسناد و مدارک تهیه شده توسط آمریکایی‌ها است، اما برخی دیدگاه‌های چینی را می‌توان در سیاست‌های ارتش چین مشاهده کرد. پایه رویکرد چین به جنگ بر پایه فریب جنگ به سبک دانش و سبک مزیت‌های نامتقارن بر دشمن استوار است.

سایبر (به انگلیسی: Cyber) واژه‌ای است بر گرفته از واژه «kybernetes» به معنای سکاندار یا راهنما. نخستین کسی که واژه فضای سایبر را به کار برد، ویلیام گیبسون نویسنده داستان‌های علمی- تخیلی، در کتاب نورومنسر (به انگلیسی: Neuromancer) بود.

فضای سایبر یا فضای مجازی (Cyber Space) در تعریف برخی نویسندگان عبارت است از: «مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی است.»

البته شاید بهتر باشد آن را چنین تعریف کنیم: «محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص خود؛ در آن زنده و مستقیم روی می‌دهد». قید «واقعی»، مانع از این است که تصور شود مجازی بودن این فضا به معنای غیرواقعی بودن آن است؛ چرا که در این فضا نیز همان ویژگی‌های تعاملات انسانی در دنیای خارج، همچون مسئولیت وجود دارد. ضمن این که فضای سایبر در واقع یک «محیط» است که ارتباطات در آن انجام می‌شود؛ نه صرف مجموعه‌ای از ارتباطات. از سوی دیگر، این ارتباطات گرچه ممکن است در همه حال برخط نباشند، ولی زنده و واقعی و مستقیم هستند. از این رو، تأثیر و تأثر بالایی در این روابط رخ می‌دهد.

اصطلاح فضای سایبر: این اصطلاح به هر اتاق و هر فضایی گفته می‌شود که به وسیلهٔ نرم‌افزار در رایانه ایجاد می‌شود. اتاق فرمان را در دنیای مجازی، رایانه به دست می‌گیرد. به جرئت می‌توان گفت: بزرگترین فضای سایبر را که میلیون‌ها کاربر را به یکدیگر متصل می‌کند، فضای مجازی اینترنت است.



شبیه‌سازی دیداری هجوم‌ها به کره جنوبی

آمار

شرکت آمریکایی امنیت اینترنتی Trend Micro اعلام کرد در سه‌ماهه دوم سال ۲۰۱۵ میلادی، کشورهای هند، مصر و ایران هدف بیشترین حمله بدافزارهای اینترنتی قرار گرفته‌اند. بر این اساس مصر با ۱۶ درصد و هند و ایران با ۱۱ درصد در این مدت هدف بیشترین حملات سایبری قرار گرفته‌اند.

اکنون این حملات با پیچیدگی و دقت بیشتری صورت می‌گیرند و به هک کردن برنامه هواپیماها، خودروهای هوشمند و ایستگاه‌های تلویزیونی گسترش یافته‌است. منطقه آسیا و اقیانوسیه، بیش از ۱۱۸ میلیون بدافزار و ۳۹۶ پیام اسپم بوده‌است. علاوه بر این کاربران ۲۱۴ میلیون بار به آدرس‌های مخرب برخورده‌اند که ۵۰ میلیون آن‌ها از منطقه آسیا و اقیانوسیه صورت گرفته‌است.[۳] از بین کشورها، روسیه، چین و آمریکا از بهترین‌ها در حمله سایبری هستند که از آن برای رسیدن به اهداف سیاسی استفاده می‌کنند. آمریکا ۶۳۰۰ نیرو (سرباز) برای حملات سایبری دارد.[۲]

پانویس

1. *Cyberspace*

2. *«نیویورک تایمز» (https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html?te=1&nl=morning-briefing&emc=edit_NN_p_20190829&section=topNews?campaign_id=9&instance_id=11987&segment_id=16563&user_id=9b155a9916c5b39f548ec581bfff1f13&regi_id=90207508tion=topNews)* .

3. *هند، مصر و ایران هدف بیشترین حملات سایبری (/http://www.irna.ir/fa/News/81755231)* . *[خبرگزاری جمهوری اسلامی(ایرنا) http://www.irna.ir]*

منابع

- فرهنگستان زبان و ادب فارسی، دفتر هفتم واژگان مصوب
- مؤسسه آموزشی و تحقیقاتی صنایع دفاعی

آخرین ویرایش ۲ ماه پیش **توسط Shayan2020x انجام شده**