امنیت فضای مجازی و دفاع الکترونیکی

جلسه پنجاه و دو

فصل سوم: احکام امنیت فضای مجازی

۹۶/۱۱/۲۶

- امنیت
- امنیت فضای مجازی
- تهدیدهای امنیت ملی

اول: جنگ

۱- جنگ الکترونیکی

۲- جنگ سایبری

۳- جنگ رسانه‌ای

دوم: تروریسم

سوم: جاسوسی

جـنگ الکـترونیکی را می‌توان به سه بـخش کلی تقسیم کرد:

- بخش اول رصد سیگنال (SIGINT)
  - رصد الکترونیکی
  - رصد مخابراتی
- بخش دوم اقدام‌های ضدّ الکترونیکی (ECM) (حمله الکترونیکی (EA))

  جلوگیری یا کاهش اسـتفاده مـؤثر دشمن از راه اختلال یا فریب
- بخش سوم اقدامات ضدّ ضدّ الکترونیکی (ECCM)

  مقابله با بخش دوم

خلاصه:

ابزار اصلی در جنگ الکترونیک رادار است و رادار دارای پنج کارکرد اصلی است:

- شناسایی حضور اجسام
- شناسایی ماهیت اجسام
- شناسایی فاصله اشیاء
- شناسایی حرکت و سرعت اجسام متحرک
- ردگیری اجسام

- بنابر این مبنای اصلی جنگ الکترونیک بر شناسایی و ردگیری است و همان طور که توضیح آن گذشت این عمل با روشهایی چون اختلال، اختفا، فریب و مانند آن همراه است.

جـنگ سایبری:

- در تعریفی معمول از جنگ سایبری چنین می‌گویند:
- اقدام یک دولت-ملت علیه رایانه‌ها یا شبکه‌های ارتباطاتی یا بانکهای اطلاعاتی یا سامانه‌های نرم‌افزاری و سخت‌افزاری ملتی دیگر با هدف اخلال، تخریب یا انهدام آنها.

(Clarke, Richard A. *Cyber War*, HarperCollins (2010))

- این اقدام می‌تواند اقدامی ابتدائی برای شروع جنگ یا اقدامی تدافعی برای دفاع باشد. همچنین این اقدام ممکن است به صورتی علنی یا مخفیانه شکل گیرد.
-
- گاهی در این جنگ تخریب یا نابودی بخشهایی از نظامهای اطلاعاتی و ارتباطاتی طرف مقابل روی می‌دهد.
- این نظامها ممکن است در یک سامانه اطلاعات ملی مثل سامانه هویت ملی روی دهد و
- گاهی نیز حمله علیه نظامهای خدماتی یک کشور رخ می‌دهد مثل حملات رد خدمات که نظامهای بانکی یک کشور را از کار می‌اندازد یا
- ویروسی کردن سامانه خدماتی یک دستگاه خدماتی مثل سازمان ثبت یا سامانه تولیدی در یک کارخانه تولیدی مثل کارخانه فولاد.

جـنگ سایبری:

- برای رفع ابهام از این تعریف سه نوع کاربرد واژه جنگ سایبری را از هم تفکیک می‌کنیم:

- اول: جنگ واقعی + سامانه‌های سایبری

- جنگ واقعی نوعاً همراه تسخیر زمین، هوا و دریا یا بخشهایی از آنها و معمولاً همراه با کشتن و مجروح کردن افرادی است که در برابر آن مقاومت می‌کنند. بنابر این آسیبی که در این جنگ حاصل می‌آید در سطح امنیت ملی است و حاکمیت یک سرزمین را مخدوش می‌کند طوری که آن سرزمین یا بخشی از آن را به تسخیر خود در می‌آورد و تصاحب می‌کند.

- معمولاً این کار همراه با حمله نظامی و قتل، جراحت و اسارت مقاومت کنندگان است.

جـنگ سایبری:

- گاهی که چنین جنگی روی می‌دهد، علاوه بر آن، از سامانه‌ای اطلاعاتی و ارتباطاتی به عنوان تسلیحات جنگی استفاده می‌کنند. مثل ابزارهای هوشمند جنگی از قبیل
  - رباتهای هوشمند برای حمله به اهداف تعیین شده،
  - موشکهای هوشمند،
  - بمبهای نصب شده بر روی پهبادها،
  - هواپیماها و تانکهای دارای ابزارهای اطلاعاتی نقطه زن و مانند آن.
- این جنگ جنگی واقعی است که در آن از ابزارهای فناورانه نیز استفاده می‌شود. در این نوع جنگ ابزارها توسعه یافته و گستره‌ای از امور فناورانه را شامل می‌شود.
- گاهی با تصرف در دستورات رایانه‌ای امکان دستکاری در زمان و مکان شلیک موشکهای دوربرد یا هسته‌ای فراهم می‌آید. (ضد حمله سایبری)
- روشن است که این نوع جنگ یا دفاع هیچ تفاوتی با مفهوم سنتی آن ندارد فقط ابزارهای قتل، تخریب و تسخیر پیشرفته شده است.

جـنگ سایبر:

- سه نوع کاربرد را در جنگ سایبری از هم تفکیک می‌کنیم:
- دوم: بهره‌مندی از سامانه سایبری بدون جنگ واقعی
- گاهی حمله اصلاً به صورت فیزیکی روی نمی‌دهد بلکه صرفاً به صورت سایبری است و در آن هکرهای یک کشور یا سازمان به سامانه‌های رایانه‌ای یک کشور حمله‌ور می‌کنند و از کار انداختن یا تخریب رایانه‌ها و شبکه‌ها یا اخلال در کارکرد آنها را هدف قرار می‌دهند.
- در این حال، حمله نه از طریق بمب و موشک بلکه از طریق ارسال یک ویروس به رایانه یک زیرساخت حیاتی مثل سدّها یا نیروگاه‌های برق یا سایتهای هسته‌ای صورت می‌گیرد و موجب انهدام یا اختلال آنها می‌شود.
- اگر حمله کننده یک فرد باشد این کار جنگ تلقی نمی‌شود ولی اگر سازمان‌یافته و از سوی دولت متخاصم باشد آنگاه آن را جنگ سایبری گویند.
- اما آنچه واقعاً رخ می‌دهد تهدید علیه امنیت ملی به صورت حمله سرزمینی نیست بلکه تهدید علیه زیرساختهای حیاتی یک کشور مثل شبکه برق یا سایت انرژی هسته‌ای یک کشور است.

جـنگ سایبری:

- برخی از دولتها راهبردهای جنگ سایبری را بخشی از راهبردهای جنگی-دفاعی خود می‌دانند و حملات سایبری را به مثابه حملات زمینی و هوایی تلقی کرده‌اند. در بخشی از راهبردهای امنیتی امریکا در باب جنگ سایبری امور ذیل به عنوان راهبرد تلقی شده است:
  - جلوگیری از حملات علیه زیرساختهای حیاتی
  - کاهش آسیب‌پذیری ملی در برابر حملات سایبری
  - کاهش آسیب‌ها و زمان ترمیم حملات سایبری
- مشهورترین مثال این نوع از تخریب ویروس استاکس‌نت است:

نمونه عینی: ویروس استاکس‌نت: افشا و کشف و اثرات

- ویروس استاکس‌نت در ژوئن ۲۰۱۰ به وسیله شرکت کسپرسکی افشا شد و معلوم شد که لااقل از سال ۲۰۰۵ فعال بوده است.
- همه دنیا متوجه شدند که اسرائیل با کمک امریکا با استفاده از سلاح سایبری قصد تخریب زیرساختهای حیاتی کشور ما را داشت و ویروس استاکس‌نت را برای این کار طراحی کرد تا در کار سانتریفویژهای مستقر در نطنز اخلال ایجاد کرده و آنها را از دور خارج کند
- برخی از تحلیل‌گران خارجی گمانه زنی کرده‌اند که در نیمه اول سال ۲۰۰۹ غنی سازی اورانیوم در نطنز تا ۳۰ درصد کاهش یافته که ناشی از اختلال در کارکرد سانتریفیوژهایی بود که از چرخه خارج شده‌اند. در آن موقع به دلائل نامشخصی طبق آمار منتشره توسط فدراسیون دانشمندان امریکایی تعداد سانتریفیوژها از ۴۷۰۰ عدد به ۳۹۰۰ عدد کاهش یافته است. اطلاعات منتشره از ویکی لیکس نیز این امر را تأیید می‌کرد.
- گمانه‌زنی شده که استعفای آقازاده در آن سال در این راستا بوده است.

نمونه عینی: ویروس استاکس‌نت: گستره شمول

- مشاهدات نشان می‌دهدکه یک ویروس آمده و ۷۰ درصد فعالیتش در کشور ایران بوده و این برای شرکتهای ضد ویروس عجیب بود. این ویروس خود را در رایانه قربانی مخفی می‌کرد و از طریق شبکه حرکت کرده تا به هدفش می‌رسد.

نمونه عینی: ویروس استاکس‌نت: اهداف و نتایج

- مصاحبه کننده تلویزیونی از رئیس وقت سازمان سیا (ژنرال مایکل هایدن) می‌پرسد: وقتی به دو امر نگاه می‌کنیم یکی فناوری پیچیده بکار رفته در این ویروس و دیگری علل انگیزشی به این نتیجه می‌رسیم که ساخت این ویروس کار امریکا یا اسرائیل بوده است. نظر شما چیست؟

وی در پاسخ به این احتمال می‌گوید: با کسی که دارای سوابق بنده است اصلاً خوب نیست که حتی به این سؤال فکر کند (چه رسد به این که بدان پاسخ دهد)

باید خاطر نشان کرد که طبق اظهارات مقامات وقت این ویروس نتوانست اختلال جدی در فعالیت سایت نطنز ایجاد کند و پس از یک دوره موقت و کوتاه سرعت کار در نطنز بیشتر شد و در نهایت اسرائیل تصمیم گرفت با ترور دانشمندان هسته‌ای ما توقف جدیدی در کار ما ایجاد کند که نشان از آن دارد که عملیات استاکس‌نت دارای موفقیت کاملی نبوده است.

والحمد لله رب العالمين