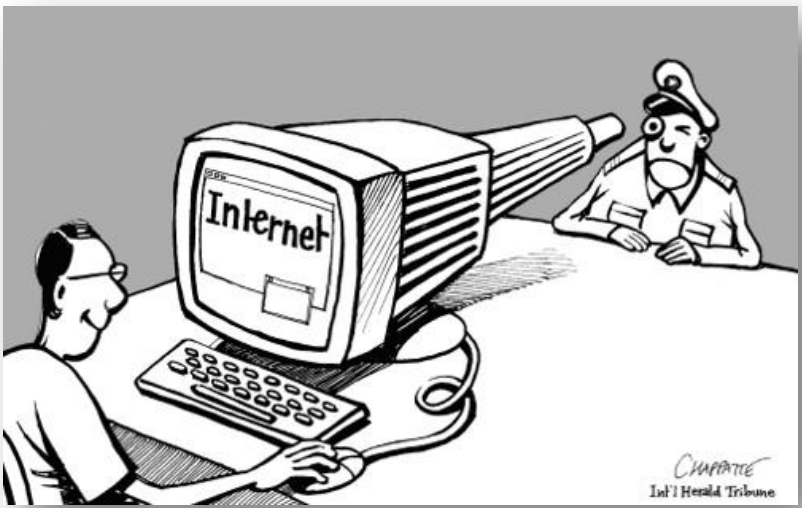
امنیت در فضای تبادل اطلاعات



فهرست

در عصر کنونی که عصر اطلاعات نام گرفته است با وجود تمامی امکانات و تسهیلاتی که فناوری اطلاعات برای بشر امروز به ارمغان آورده‌است، عرصه‌ای برای سوء استفاده از این فناوری و حتی اعمال مجرمانه نیز فراهم گردیده‌است. هر ساله سازمان‌های بسیاری در سطح دنیا هدف جرائم مرتبط با امنیت -از حملات ویروسی گرفته تا کلاهبرداری های تجاری- قرار می گیرند.

برای در امان ماندن از کلیه تهدیدات فضای سایبری اعم از تهدیدات داخلی و خارجی باید یک برنامه جامع امنیت سایبری تدوین نمود. برای دستیابی به چنین هدفی باید ابتدا انواع جرائم و جنگ‌های سایبری را شناخته و راهکارهای مقابله با آن‌ها را اتخاذ نمود. در این کتابچه سعی بر این است که ضمن تشریح مقوله امنیت، انواع جنگ‌ها و جنگ‌افزارهای اطلاعاتی، بررسی و تأثیر آن در ابعاد گوناگون بیان شود.

جنگ‌افزارهای اطلاعاتی شامل جنگ‌افزارهای فرمان و کنترل، مبتنی بر جاسوسی، الکترونیکی، روانی، اطلاعات در فضای مجازی، نفوذگران رایانه‌ای و اطلاعات اقتصادی هستند.

آغاز

منظور از امنیت چیست؟

شما می‌خواهید مهندسی را برای بخش امنیت شبکه استخدام کنید. سه نفر درخواست کار در شرکت شما را داده‌اند؛ از هر کدام می‌پرسید: «چقدر امنیت می توانید ایجاد کنید؟!»

نفر اول پاسخ می‌دهد: «*من می‌توانم فضای تبادل اطلاعات شما را در مقابل هر تهدیدی امن سازم*» مسلماً با شنیدن این پاسخ به این نتیجه می‌رسید که شخص مذکور فرد مورد نظر شما برای ایجاد امنیت فضای سایبری نیست! نفر دوم در پاسخ می گوید: «*من فضای تبادل اطلاعات شما را تا حد امکان امن می‌سازم*» بدیهی است او نیز فرد منتخب شما نخواهد بود. نفر سوم پاسخ می‌دهد: «*منظور شما از امنیت چیست؟*»[1] این دقیقاً همان پاسخ درستی است که شما باید بشنوید.

[1] پدافند غیرعامل، سه جنبه زیر در حفاظت از زیرساخت‌های فناوری اطلاعات را شامل می‌شود:امنیت، مربوط به امنیت محتوای زیرساخت‌های فناوری اطلاعات؛ ایمنی، مربوط به ایمنی و حفاظت‌های فیزیکی از زیرساخت‌های فناوری اطلاعات؛ پایداری، مربوط به ایجاد پایداری و استمرار در عملکرد زیرساخت‌های فناوری اطلاعات.

در چه مرحله ای باید به مقوله امنیت پرداخت؟

چنانچه امنیت از ابتدا در طراحی سامانه‌ها منظور نشود ممکن است سرعت در مرحله طراحی و تولید بیشتر شود اما در این حالت حتی اگر سامانه دچار شکست قطعی نشود باید منتظر هزینه های بسیار هنگفت در آینده بود!

مثال جالب در این زمینه تجربه اختراع هواپیما است. برادران رایت سال‌های سال با دقت فراوان به طراحی سامانه هواپیما پرداختند و در نهایت هم موفق شدند این اختراع را به نام خود ثبت کنند. اما در سال‌های قبل از فعالیت آن‌ها برادران مونتگوفایر با ایده‌ای مشابه به ساخت هواپیما پرداختند و به سرعت وسیله‌ای را طراحی و به ساخت آن اقدام نمودند اما در همان استفاده آزمایشی اول با شکست روبرو شدند! ایده آن‌ها شروعی برای مخترعین بعدی شد و با احتساب و جدی گرفتن مقوله امنیت منجر به اختراع هواپیما شد.

در عمل بسیاری از مهندسین و طراحان نیز همین سیاست را پی می‌گیرند یعنی «تولید سریع یک نمونه». در حالیکه با این سیاست عملاً امنیت قربانی سرعت شده و نتیجه ایده‌آل به دست نمی آید.

جرایم فضای تبادل اطلاعات چیست؟

جرم فضای تبادل اطلاعات (سایبر) به فعالیت مجرمانه‌ای گفته می‌شود که با استفاده از فضای رقومی و رایانه و اینترنت انجام شده باشد. جرم سایبر در واقع مفهوم وسیعی است که گستره‌ای از انواع متفاوت جرایمی که به کمک فناوری اطلاعات می‌تواند انجام شود را در بر می‌گیرد. این جرایم می‌تواند شامل مواردی از قبیل جعل، استتار سایبری، آزار و اذیت، افترا و حتی تروریسم سایبری باشد.

در حال حاضر تعریف جرایم سایبری در هر کشور متفاوت است ولی بطور کلی آنچه مشخص است ابزارهای بازدارنده و سیاست‌های صریح و محکم در دنیای امنیت داده‌های رقومی نیاز روز در این حوزه است. به‌علاوه دولت‌ها نیز برای مبارزه مؤثر با جرایم سازمان‌یافته در عصر دیجیتال باید تلاش گروهی داشته‌باشند. همچنین لازم است مجازات‌های محکم، متناسب و جدی به‌منظور ریشه‌کن کردن آنچه که به یک مشکل جهانی و گسترده مبتنی بر فناوری تبدیل شده در نظر گرفته شود.

قانون جرایم رایانه ای در جمهوری اسلامی ایران

در کشور جمهوری اسلامی ایران قانون جرایم رایانه‌ای در خردادماه ۱۳۸۸ به تصویب مجلس شورای اسلامی رسیده‌است. این قانون در سه بخش تشریح شده‌است که عناوین آن در زیر آورده شده است:

- بخش اول: جرایم و مجازات‌ها
  - فصل اول: جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی (شامل دسترسی غیرمجاز، شنود غیرمجاز و جاسوسی رایانه‌ای)

- فصل دوم: جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی (شامل جعل رایانه‌ای و تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی)
- فصل سوم: سرقت و کلاهبرداری مرتبط با رایانه
- فصل چهارم: جرایم علیه اخلاق و عفت عمومی
- فصل پنجم: هتک حیثیت و نشر اکاذیب
- فصل ششم: مسئولیت کیفری اشخاص
- فصل هفتم: سایر جرایم
- فصل هشتم: تشدید مجازات‌ها

بخش دوم: آیین دادرسی

- فصل اول: صلاحیت‌ها
- فصل دوم: جمع‌آوری ادله الکترونیکی (شامل نگهداری اطلاعات، حفظ فوری داده‌های رایانه‌ای ذخیره‌شده، ارائه داده‌ها، تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی و شنود محتوای ارتباطات رایانه‌ای)
- فصل سوم: استنادپذیری ادله الکترونیکی

بخش سوم: سایر مقررات

ماهیت جنگ اطلاعات

برای جنگ اطلاعاتی، تعریف‌های مختلفی ارایه شده‌است که هر یک از منظر خاصی به رویارویی اطلاعاتی می‌نگرد، ولی تمام این تعریف‌ها رویکرد مشخصی را دنبال می‌کنند. به‌عنوان نمونه به ذکر چند مورد زیر می‌پردازیم.

- توانایی شنیدن، دیدن، داشتن درک صحیح از سامانه فرمان و کنترل، شناسایی منابع اطلاعاتی و حسگرهای دشمن و در مجموع دست‌یابی به درک بهتر از استعدادهای دشمن به گونه‌ای که به برتری اطلاعاتی بیانجامد.
- کلیه اقداماتی که از طریق اثرگذاری بر اطلاعات و سامانه‌های اطلاعاتی دشمن و به منظور دستیابی به برتری اطلاعاتی، در راستای راهبرد نظامی یک کشور صورت پذیرد.
- عملیات‌های نظامی به غیر از جنگ‌های فیزیکی
- ایده‌ها و نظریه‌های مرتبط با اثرگذاری و روش تفکر انسان‌ها و از آن مهم‌تر روش بهره گیری از اطلاعات برای دست‌یابی به اهداف ملی یک کشور. این اهداف ممکن است در زمینه‌های سیاسی، اقتصادی یا نظامی باشند.

سابقه جنگ اطلاعات

واژه «جنگ اطلاعات» در جنگ جهانی دوم توسط چرچیل مورد استفاده قرار گرفت. زمانی که مهندسین پیام‌های رمزشده آلمانی‌ها را شنود و کشف می‌کردند مصداق‌هایی از جنگ اطلاعات در حال شکل گرفتن بود. این واژه در سال ۱۹۷۶ میلادی در یکی از گزارش‌های داخلی شرکت بویینگ بکار

رفت ولی تا سال ۱۹۹۶ که یکی از مدیران CIA از آن در سنای آمریکا استفاده کرد ناشناخته ماند.

در سال ۱۹۹۸ میلادی مرکز ملی حفاظت از زیرساخت‌ها در آمریکا تأسیس شد. هدف این مرکز تشخیص، جلوگیری، ارزیابی، هشدار، واکنش و بررسی نفوذهای رایانه‌ای و فعالیت‌های خلاف قانون در این رابطه ذکر شده‌است.

انواع جنگ افزار اطلاعاتی

جنگ افزار اطلاعاتی به کلیه امکانات و انواع جنگ‌افزارهایی اطلاق می‌گردد که روی اطلاعات دشمن تأثیر می‌گذارد. هفت نوع از جنگ‌افزارهای اطلاعاتی در زیر شرح داده شده اند.

۱. جنگ افزار فرمان و کنترل

استفاده یکپارچه و هماهنگ از روش‌های جنگ روانی، فریب نظامی، امنیت در عملیات، جنگ الکترونیک و تخریب فیزیکی که به وسیله اطلاعات پشتیبانی شده باشند در گستره دامنه جنگ فرمان و کنترل قابل دست‌یابی است و قابلیت پیشگیری از دسترسی دشمن به اطلاعات خودی، اثرگذاری بر فرآیند گردآوری اطلاعات و کاهش کیفیت اطلاعات دشمن، از بین بردن سامانه‌های فرمان و کنترل حریف و دفاع از سامانه‌های خودی را دارد. جنگ فرمان و کنترل شامل هر نوع عملیات در تمامی سطوح رویارویی نظامی است. بنابراین جنگ فرمان و کنترل می تواند ماهیت تدافعی و تهاجمی داشته باشد.

رمز تهیه یک طرح موفق برای جنگ فرمان و کنترل، تا حد زیادی بستگی به موفقیت فرماندهی در ایجاد یکپارچگی و درهم‌تنیدگی مناسب بین اجزای تشکیل‌دهنده جنگ دارد. جزییات روش طرح‌ریزی و سازماندهی، تحت عنوان سامانه طراحی و اجرای عملیات مشترک، به طور معمول توسط ستاد مشترک هر کشور منتشر می‌شود.

۲. جنگ افزار مبتنی بر جاسوسی

عامل هوش مستقیماً در عملیات (به ویژه برای هدف‌گیری و ارزیابی خسارت یک نبرد) به کار گرفته می‌شود، نه اینکه از آن به عنوان یک ورودی برای کل سامانه فرمان و کنترل استفاده شود. بر خلاف شکل‌های دیگر رویارویی، این روش به طور مستقیم در اصابت گلوله به هدف (به جای تخریب اطلاعات) مؤثر است. با پیشرفت دقت و قابلیت اعتماد به حسگرها، گسترش تنوع و نیز با افزایش توانایی آنها در تغذیه سامانه‌های کنترل آتش در سریع‌ترین زمان ممکن، به تدریج وظیفه نگهداری، بکارگیری سامانه ناظر بر فضای نبرد و توسعه آن‌ها، ارزیابی ترکیب سامانه‌ها در میدان نبرد و ارسال نتایج بدست آمده به سامانه‌های آتش‌بار، به سامانه حسگرها محول شده‌اند.

۳. جنگ افزار الکترونیکی

کلیه جنگ‌افزارهایی که علیه حسگرها و رادارهای دشمن عمل می‌کنند تلاش می‌کنند تا امکانات مخابراتی آن‌ها را هدف بگیرند. مدیریت صحیح امواج الکترومغناطیسی موجب پیشگیری از صدمه‌زدن دشمن به سامانه‌های مخابراتی و غیرمخابراتی شده و از

تولید الگوی ارتباطی محسوس که سبب شناسایی امکانات خواهد شد، پیشگیری می‌شود.

پشتیبانی الکترونیکی با بهره‌گیری از روش‌های تجسس و گردآوری اطلاعات مفید از وضعیت دشمن، می‌تواند تهاجم‌های احتمالی علیه گلوگاه‌های کلیدی فرمان و کنترل خودی را شناسایی و اعلام نماید. همچنین در بعد امنیت اطلاعات، این عنصر می‌تواند روزنه‌های نفوذ و گردآوری اطلاعات از نیروهای خودی توسط دشمن را شناسایی و آشکار کند.

۴. جنگ افزار روانی

بکارگیری اطلاعات برای مقابله با قدرت تفکر انسان‌ها است. جنگ روانی به چهار گروه متمایز به شرح زیر تقسیم می‌شود:

- اقدام علیه اراده یک ملت
- اقدام علیه یک نیروی نظامی
- اقدام علیه فرماندهان ارشد (به ویژه فرماندهان مخالف با یک راهبرد خاص)
- رویارویی فرهنگی

۵. جنگ افزار فضای مجازی

در بین جنگ‌های اطلاعاتی، این نوع رویارویی (در فضای مجازی) طیف بسیار وسیعی را در بر می‌گیرد که شامل تروریسم اطلاعاتی[۱]، تهاجم از طریق اختلال در منطق حاکم بر یک نرم‌افزار[۲]، شبیه‌سازی تمام عیار یک نبرد[۳] و جنگ گیبسون[۴] است. جنگ اطلاعات به دلیل مجازی بودن آن در فضای مجازی، کمتر از انواع پیش‌گفته دارای مستندات و منابع قابل تعقیب است. در تهاجم از طریق تغییر در مفهوم یا منطق حاکم بر یک نرم‌افزار، سعی می‌شود مأموریت یک نرم‌افزار بگونه‌ای تغییر داده شود تا نتایج نهایی، بر خلاف انتظار سامانه باشد. به عنوان مثال، با تزریق ویروس در سامانه ناوبری یک هواپیما می‌توان زمینه نمایش اطلاعات غلط (ولو به ظاهر طبیعی) مانند ارتفاع هواپیما از سطح دریا یا فاصله واقعی باند پرواز تا هواپیما را فراهم نمود.

- تروریسم اطلاعاتی زیر مجموعه‌ای از نفوذهای رایانه‌ای، نه با هدف تخریب سامانه‌ها، بلکه با هدف بهره‌برداری از اطلاعات موجود در سامانه‌ها برای حمله به افراد و اعمال نفوذ به آن‌ها است.
- حملات معنایی به منظور تغییر عملکرد سامانه اطلاعاتی هدف انجام می‌گیرند. برخلاف جنگ نفوذگری که در سامانه‌ها خرابی ایجاد می‌کند و عمل آن‌ها را متوقف می‌سازد، در این

---

[۱] Information Terrorism

[۲] Semantic Attack

[۳] Simula-Warfare

[۴] Gibson Warfare

حملات یک سامانه تحت حمله معینی کار می‌کند و به‌نظر می‌رسد که بطور صحیح عمل می‌کند، اما پاسخ‌دهی مغایر با واقعیت تولید می‌کند.

- جنگ شبیه‌سازی برخلاف جنگ واقعی، پرآشوب و خطرناک نیست. اگر دقت شبیه‌سازی به حد کافی خوب باشد، نتایج بدست آمده تقریب معقولی از جنگ واقعی است و چنانچه بتوان با نتایج حاصل از یک جنگ شبیه‌سازی شده به دشمن ثابت کرد که شکست خورده است و باید تسلیم شود، نیازی به شروع یک جنگ واقعی نیست. جنبه بازدارندگی جنگ شبیه‌سازی رو به گسترش است.

- جنگ گیبسون محدوده‌ای را شامل می‌شود که به سختی با واقعیت محدود می‌شود. در این نوع جنگ فرد تمایل دارد شبکه‌ای بسازد که به او اجازه دهد در هر جایی که بطور واقعی شفاف نیست جنگ را شروع کند. اینترنت و کاربران آن معادل مجازی دنیای واقعی را تولید می‌کنند و با استفاده از فناوری عامل[1]، کاربر یک شبح یا تمثال را برای انجام خواسته‌هایش – از رزرو هتل و خرید کالا تا شاید شروع درگیری و جنگ روانی در شبکه– ایجاد می نماید. نام این جنگ برگرفته از نام نویسنده معروف داستان‌های علمی–تخیلی، ویلیام گیبسون است.

[1] Agent

۶. جنگ افزار نفوذگران رایانه ای

معمولاً هدف این نوع جنگ افزار اطلاعاتی، روش‌های تهاجم به بخش غیرنظامی یک کشور است. چراکه تهاجم به بخش‌های نظامی در قالب روش‌های جنگ فرمان و کنترل صورت می‌پذیرد. در این نوع جنگ، سارقین اطلاعات یا نفوذگران رایانه‌ای اقدام به شناخت نقاط آسیب‌پذیر ساختار یک سامانه نموده و از آن نقاط، تهاجم خود را آغاز می‌کنند. زمینه‌های این تهاجم می‌تواند بسیار متنوع باشد. برای نمونه هدف از تهاجم ممکن است ساقط کردن یک سامانه، تعطیلی و توقف مکرر یک سامانه، ایجاد خطاهای اتفاقی در داده‌ها، سرقت خدمات (انجام مکالمات تلفنی رایگان، ورود و بهره‌برداری از اطلاعات پایگاه‌ها بدون پرداخت هزینه)، جعل هویت (استفاده از امضای رقومی و یا کارت اعتباری دیگران)، گردآوری اطلاعات برای سرویس‌های امنیتی (رمزشکنی و دستیابی به رمز ورود به پایگاه‌های نظامی و فروش این رمزها به سرویس‌های اطلاعاتی)، ارسال پیام‌های ساختگی غیرمجاز و دستیابی به اطلاعات شخصی افراد به منظور اخاذی از آن‌ها باشد. در این رابطه از نرم‌افزارهای متعددی نیز بهره گرفته می‌شود.

۷. جنگ افزار اطلاعات اقتصادی

جنگ‌افزارهای اطلاعاتی جهت حمله به زیربناهای حیاتی اقتصادی است. کسب اطلاعات به منظور محاصره اقتصادی، تولید کالای رقابتی، بی‌ارزش کردن پول ملی و جاسوسی صنعتی از انواع کاربردهای آن است.

تأثیر جنگ افزار های اطلاعاتی از ابعاد گوناگون

جنگ‌افزارهای اطلاعاتی را به طور کلی از سه منظر ماهیت تقابل آن، زمینه فعالیت و سطح تأثیرگذاری آن می توان بررسی نمود.

از منظر زمینه های فعالیت موارد زیر قابل توجه است:

- ارتشی و نظامی
- فناورانه
- اقتصادی
- سیاسی
- اجتماعی
- ایدئولوژی و مذهبی

در خصوص سطح تأثیرگذاری، جنگ‌افزارهای اطلاعاتی می‌توانند سطوح زیر را درگیر نمایند:

- راهبردی و بین المللی
- عمومی و گسترده
- ملی
- سازمانی
- فردی

زمان‌های مورد استفاده این جنگ‌افزارها بین کشورها می‌توانند به شکل زیر باشند:

- همکاری
- رقابت
- تعارض
- جنگ