
بسم الله الرحمن الرحیم

جنگ سایبری

شکل گیری و توسعه

ارائه دهنده:

محسن آقایی

نبرد در عرصه پنجم یا ؟

تقدیم به تمامی آزادمردان و شیرزنانی که حسرت

تسخیر حتی ذره ای از خاک میهن عزیزمان را بر دل دشمنان گذاشتند

تا آیندگان بدانند که وارثان

بابایی ها

دوران ها

صیاد شیرازی ها

سلیمانی ها

و

فخری زاده ها

هستند.

یادشان گرامی و راهشان پر رهرو باد.

۱۳۸۴/۰۲/۱۱
بیانات در دیدار با جمعی از روحانیون استان کرمان

امروز اینترنت و ماهواره و وسایل ارتباطیِ بسیار متنوع وجود دارد و حرف، آسان به همه جای دنیا می‌رسد.

امروز ما در یک میدان جنگ و کارزار حقیقیِ فکری قرار داریم این کارزار فکری **به هیچ وجه به زیان ما نیست؛ به سود ماست** اگر وارد این میدان بشویم .

جنگ

جنگ

- درگیری شدید مسلحانه میان دولت‌ها، حکومت‌ها، جوامع یا گروه‌های شبه‌نظامی مانند مزدورها، شورشگران و شبه‌نظامیان است. از آن‌جا که جنگ یک درگیری مسلحانه واقعی، ارادی و گسترده بین جوامع سیاسی است می‌توان آن را نوعی خشونت سیاسی تلقی کرد. (ویکی پدیا)

- در سال ۱۸۳۲ ژنرال کارل فون کلاوزویتس، فرمانده و نظریه‌پرداز نظامی پروسی در رساله‌ای به نام «پیرامون جنگ» چنین تعریفی از جنگ ارائه داد: «جنگ عملی مبتنی بر زور است تا دشمنان را مجبور به انجام خواسته های خودمان کنیم.»

مهارت نظامی

مهار کردن دشمن بدون رویارویی فیزیکی !

سان تزو

تغییر ماهیت جنگ ها

از جنگ در فضای سخت و نظامی

به

جنگ در فضای فناوری

دلایل اصلی تغییر ماهیت جنگ ها

- کاهش تلفات انسانی(پیروزی بدون خونریزی)
- کاهش هزینه های جنگی
- کاهش زمان عملیات ها
- اثر بخشی بیشتر
- ابعاد گسترده تر(نظامی، اقتصادی، اجتماعی، سیاسی، صنعتی و....)
- امکان بکارگیری از همه مولفه های قدرت
- ریسک کم
- قدرت زیاد در کنترل احساسات

مقایسه اقتصادی در انواع سلاح ها

هزینه یک فروند بمب افکن Stealth: $1.5 to $2 billion

هزینه یک فروند جنگنده Stealth: $80 to $120 million

هزینه یک فروند موشک Cruise: $1 to $2 million

هزینه یک سلاح سایبری: $400 to $50,000

مقایسه اقتصادی در انواع سلاح ها

هزینه یک فروند بمب افکن Stealth :

$1.5 to $2 billion

هزینه یک فروند جنگنده Stealth:

$80 to $120 million

هزینه یک فروند موشک Cruise:

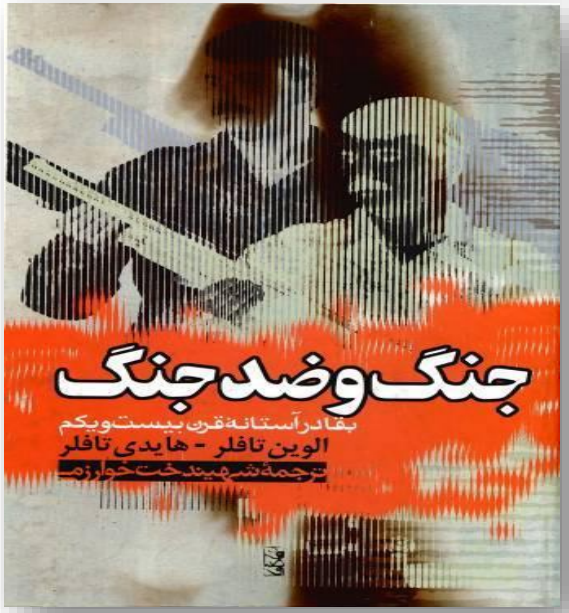
$1 to $2 million

هزینه یک سلاح سایبری:

$400 to $50,000

تغییر در شیوه رزم :شیوه جنگ متناسب با شیوه تولید ثروت !

- آلوین تافلر در سال ۱۹۹۳ و در کتاب « جنگ و ضد جنگ» می گوید :



شیوه جنگ در هر کشوری متناسب با شیوه تولید ثروت در آن جامعه است و همان عواملی که باعث دگرگونی اقتصاد کشورها می شوند منشا دگرگونی های نظامی و جنگ نیز می باشند.

ظهور تهدیدات جدید و از جنس فناوری اطلاعات

به موازات افزایش رفاه عمومی ناشی از قابلیت های فناوری اطلاعات، ظهور تهدیدات جدید و از جنس فناوری اطلاعات و در بستر فناوری در حوزه های مختلف:

- تهدیدات فردی
- تهدیدات اجتماعی و مردمی
- تهدیدات شرکت ها و سازمان ها
- تهدیدات زیر ساخت های کشور(حیاتی ، حساس ،مهم)
- تهدیدات در حوزه امنیت ملی

جنگ سایبری

چرا ؟ جنگ سایبری

دیدگاه ایجابی

- آشنایی با مفهوم جنگ سایبری و ویژگی‌های آن
- شناخت فرصت‌ها و تهدیدهای جنگ سایبری
- اطلاع از خلاءهای حقوقی و قانونی حوزه جنگ سایبری در عرصه بین‌المللی و بهره‌گیری از فرصت‌های مثبت و بر حذرماندن از چالش‌ها و تهدیدهای آن
- اتخاذ تمهیدات و سازوکار مناسب برای پیگیری اقدامات سایبری خصمانه دشمنان در عرصه بین‌الملل
- ایجاد بازدارندگی حقوقی لازم در برابر اقدامات خصمانه دشمنان، بروز جنگ سایبری و ایجاد خسارت به زیرساخت‌های کشور
- کسب آمادگی برای مواجهه حقوقی لازم با جنگ سایبری و جلوگیری از غافلگیری در این مواجهه

چرا ؟ جنگ سایبری

دیدگاه سلبی

- ضعف در شناخت و اطلاق جنگ سایبری
- عدم اطلاع از پیامدها و نتایج عملیات سایبری علیه دشمنان در جامعه بین‌الملل
- عدم نقش‌آفرینی مناسب در عرصه حقوق فضای سایبر در سطح بین‌الملل
- ضعف در پیگیری حقوقی مخاصمات و حملات سایبری و نیز تهدید جنگ سایبری از سوی دشمنان در سطح بین‌الملل
- ضعف در بهره‌گیری از فرصت‌های موجود در عرصه جنگ سایبری و عدم توجه به این عرصه مهم و موثر در سطح جهانی
- ضعف در ایجاد بازدارندگی حقوقی لازم در مقابل اقدامات خصمانه دشمنان در عرصه جنگ سایبری
- نداشتن تمهید مناسب برای مواجهه با جنگ سایبری در عرصه حقوق بین‌الملل
- در معرض تهدید قرارگرفتن زیرساخت‌های کشور در مقابل حمله و جنگ سایبری

تهدیدات (حملات) سایبری سال‌های اخیر در جهان

- اقدامات سایبری سال ۲۰۰۱ ایالات‌متحده علیه ارتش عراق
- تهاجم سایبری علیه کشور استونی در آوریل ۲۰۰۷
- حملات مستمر سایبری به وزارت دفاع ایالات‌متحده در سال ۲۰۰۷
- حملات سایبری روسیه در سال ۲۰۰۸ به کشور گرجستان
- حملات سایبری علیه زیرساخت‌های ارتباطی اسراییل در سال ۲۰۰۹
- حملات سایبری در اکتبر ۲۰۱۰ به کشورهای اندونزی و جمهوری اسلامی ایران با سلاح سایبری استاکس نت
- حملات سایبری به مراکز داده چندین کشور در فروردین‌ماه ۱۳۹۷ ازجمله جمهوری اسلامی ایران
- شبکه برق ونزوئلا در سال ۲۰۱۹
- حملات سایبری به شبکه حمل و نقل جمهوری اسلامی ایران در سال ۲۰۲۱
- حمله سایبری به شبکه توزیع سوخت هوشمند جمهوری اسلامی ایران در سال ۲۰۲۱

ماهیت

- پدیده ای پویا و دینامیک
- پدیده ای فناناپذیر و همیشگی
- پدیده ای در شکل های مختلف
- پدیده ای با بکارگیری فناوری های نوین
- استفاده کننده از هوش مصنوعی
- دارای هویت پنهان
- دارای قدرت یادگیرندگی

مواجهه

- با قدرت تحلیل
- با قدرت بازیابی
- با قدرت یادگیرندگی
- دارای سیکل همیشگی
- با قدرت کنترل
- دارای قدرت تصمیم سازی و تصمیم گیری

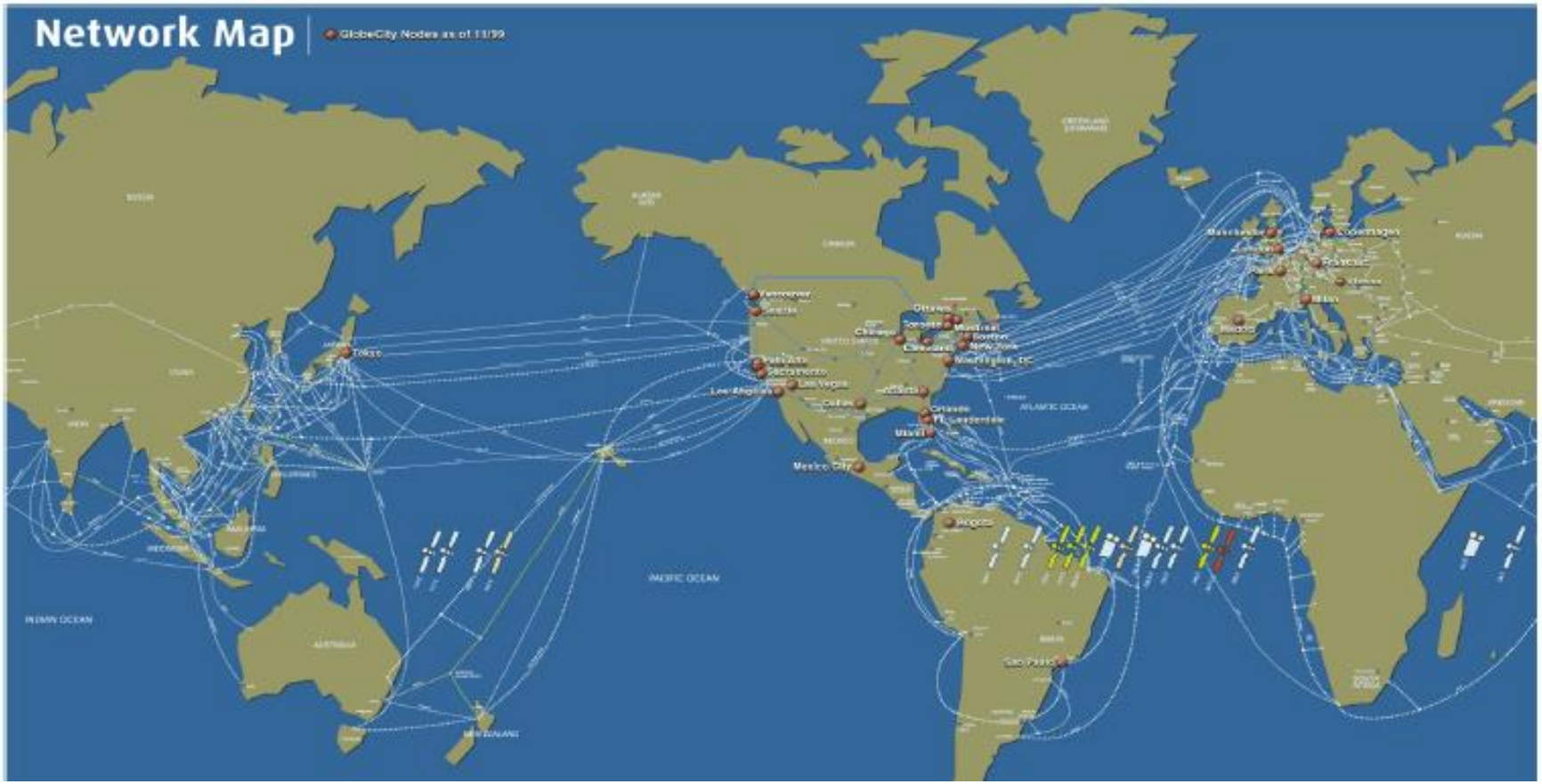
فضای سایبر

شناختی

اطلاعاتی

فیزیکی

بر اساس تعریف مشترک ارائه شده در واژه‌نامه دوجانبه اصطلاحات حیاتی امنیت فضای سایبر (انستیتو شرق-غرب آمریکا و انستیتو امنیت اطلاعات دانشگاه دولتی مسکو، ۲۰۱۱)، **"فضاي سايبر، محيط الكترونيكي است كه اطلاعات در آن توليد، ارسال، دريافت، ذخيره‌سازي، پردازش و حذف مي‌گردد."**



فضای سایبر

- **فضای سایبری یک دامنه سراسری در محیط اطلاعاتی است که شامل شبکه های مرتبط به هم از زیرساخت های فناوری اطلاعات، شامل اینترنت، شبکه های مخابراتی، سیستم های کامپیوتری، پردازنده ها و کنترلرهای توکار است.** (تعریف وزارت دفاع آمریکا از فضای سایبر)

- **رسانه الکترونیکی که از طریق آن اطلاعات تولید، منتقل، دریافت، ذخیره، پردازش یا حذف می شوند.** (تعریف مشترکی از آمریکا و روسیه)

- **فضای سایبری، رسانه الکترونیکی شبکه های کامپیوتری است که ارتباطات برخط در آن انجام می شود.**

خصوصیات فضای سایبر

- اطلاعات از یک محیط به محیط دیگر، گردش دارند.
- درآن محیط پردازش، کپی و ذخیره می شوند.
- این فضا شامل سیستم‌های ارتباطات، رایانه‌ها، شبکه‌ها، ماهواره‌ها و زیرساخت ارتباطات است.
- در آن همه چیز مبهم و نامشخص است.
- در این فضا ارتباطات، جنگ سایبری و الکترونیکی به شدت گسترش پیدا کرده است.
- از امور نظامی تا امور فرهنگی و اجتماعی همگی رایانه محور شده است.
- رقبا برای افزایش توانمندی خود و نیز ضربه به دشمن در این فضا سرمایه‌گذاری می کنند.

خصوصیات فضای سایبر

- معاهده حقوقی مشخص و جامعی که تمام جنبه‌های مختلف را دربرگیرد، به‌وجود نیامده است و حق و تکلیف دولت‌ها مبهم است.

- عرصه جدیدی برای زندگی بشر فراهم کرده و فرصت‌ها و تهدیدهای فراوانی را با خود به همراه داشته است.

- اغلب حوزه‌ها و مفاهیم آنها را دستخوش تغییر و تحول نموده است.

- از جمله موضوعات مهمی که با پدیدارشدن فضای سایبر با تحول مواجه شده، جنگ است.

- هم اکنون عرصه جدیدی از جنگ و نبرد شکل گرفته که از آن با نام عرصه پنجم نبرد یا همان فضای سایبری یاد می‌شود.

شکل گیری فضای جنگی

- ورود مناقشات و جنگ‌ها به فضای سایبری، جنگ سایبری

- سایبر در سایر عرصه‌های جنگ و نبرد (زمینی، دریایی، هوایی و فضایی) نیز ورود پیدا کرده و مفهومی با عنوان سایبر در رزم

- دیگر عرصه‌های نبرد، به شدت به فضای سایبر وابسته شده است .

- بهره‌گیری از قابلیت‌های سایبری می‌تواند منجر به موفقیت در سایر عرصه‌های نبرد نیز گردد.

زمینه سازان جنگ سایبری

- اتکاء زیاد به فناوری غیر بومی
- اعتماد به ابزار و تجهیزات غیر خودی
- وابسته شدن زیرساختهای حیاتی به فناوری آسیب پذیر
- وابسته شدن خدمات حیاتی به بستر اینترنت
- عدم رعایت ملاحظات و توصیه های امنیتی و پدافندی در استفاده از فناوری

مفاهیم

- **تهدیدات سایبری**
- **آسیب پذیری های سایبری**
- **حملات سایبری (اگر در یک حمله سایبری، آسیب‌ها به حدی شدید بوده باشند که قابل مقایسه با آسیب‌های معمول در جنگ‌ها باشند، در این صورت، حمله سایبری درحکم جنگ سایبری خواهد بود)**
- **جنگ سایبری «نفوذ غیرمجاز به وسیله، از طرف، یا در حمایت از یک دولت به شبکه‌ها یا رایانه‌های ملی دیگری، یا هر فعالیت متأثرکننده سیستم‌های رایانه‌ای، که هدف در آن جمع‌کردن، تغییردادن یا دستکاری اطلاعات، یا باعث مختل شدن یا صدمه زدن به رایانه، طرح شبکه، یا اهداف کنترل سیستم رایانه است»**
- **رزم سایبری**
- **نبرد سایبری (نبرد سایبری در اصل به معنای روش جنگ ، نبرد سایبری بیشتر معطوف و ناظر به شیوه، فنون و روش جنگ سایبری است در حالیکه جنگ سایبری بیشتر به یک درگیری مسلحانه خاص اشاره دارد.)**
- **عملیات سایبری**

تعاریف

- تاکنون تعریف پذیرفته‌شده‌ای از جنگ سایبری ارائه نشده است.
- بطور کلی می‌توان گفت جنگ سایبری به جنگی اطلاق می‌شود که در فضای سایبر و با استفاده از روش‌ها و ابزارهای سایبری انجام می‌شود.
- جنگ سایبری به عنوان وسیله‌ای برای اجرای عملیات‌های نظامی، طبق اصول مرتبط با اطلاعات است.
- فضای جنگ سایبری فضای اطلاعات است که هنگام جنگ مورد توجه قرار می‌گیرد .
- فضای جنگ سایبری شامل هر چیزی می‌باشد که در محیط فیزیکی و نیز محیط فضای سایبری روی می‌دهد.

نظرات در مورد جنگ سایبری

- برخی صاحبنظران، حملات سایبری در قرن بیست و یکم را معادل با سلاح‌های هسته‌ای در قرن بیستم دانسته‌اند که این موضوع حاکی از اهمیت و حساسیت بالای فضای سایبر و لزوم نقش‌آفرینی حاکمیت‌ها در آن است.

- به همین دلیل تعداد کشورهایی که در عملیات‌های سایبری نقش دارند، هر روز در حال افزایش است.

- از طرفی حقوق بین‌الملل در عرصه جنگ سایبری تقریبا سکوت کرده و قاعده و قانون مورد توافق جامعه بین‌الملل در حوزه جنگ سایبری وجود ندارد که این موضوع، فرصت‌ها و تهدیدهای بی‌شماری را برای جوامع و دولت‌ها داشته است

نظرات در مورد جنگ سایبری

- **جنگ سایبری از منظر حقوق بین‌الملل :**

- جنگ سایبری، بکارگیری هدفمند قوای سایبری یک کشور، شامل مجموعه اقدامات پیوسته رایانه‌ای، در جهت تخریب، ضربه یا تصرف کشور هدف است که می‌تواند از طریق کنترل و تخریب زیرساخت‌های اطلاعاتی و امنیتی یک کشور انجام گیرد. (صلاحی و کشفی، ۱۳۹۵)

- آنچه در این تعریف، جنگ سایبری را از کنش و واکنش‌های آنی و کوتاه مدت دیگر اقدامات سایبری مجزا می‌کند دو موضوع «هدفمندی» و «پیوستگی» است.

نظرات در مورد جنگ سایبری

- جنگ سایبری شامل حملات دیجیتالی به شبکه‌ها، سامانه‌ها اطلاعات کشور دیگری با هدف صدمه زدن به آنهاست. این حملات ممکن است حاوی تخریب، تغییر یا به سرقت بردن اطلاعات یا از دسترس‌خارج‌کردن خدمات برخط باشد که جامعه نظامی و یا جامعه‌های بزرگتر از آنها استفاده می‌کنند. (جعفری و اسدی، ۱۳۹۷)

- برخی افراد، در تعریف «حمله سایبری»، به اشتباه آن را، جنگ سایبری یا مخاصمه مسلحانه می‌دانند. این در حالی است که فقط آن دسته از حملات سایبری که پیامدهایی برابر با پیامدهای حملات مسلحانه دارند یا در بستر مناقشه‌ای مسلحانه رخ می‌دهند، در سطح جنگ سایبری قرار می‌گیرند. به بیانی دیگر اگر در یک حمله سایبری، آسیب‌ها به حدی شدید بوده باشند که قابل مقایسه با آسیب‌های معمول در جنگ‌ها باشند، در این صورت، حمله سایبری درحکم جنگ سایبری خواهد بود(جعفری و توتونچیان، ۱۳۹۸).

نظرات در مورد جنگ سایبری

- سازمان همکاری منطقه‌ای شانگهای تعریف نسبتا جامعی از جنگ سایبری ارائه کرده است. تعریف این سازمان از جنگ سایبری عبارت است از: مقابله میان دولت‌ها، در عرصه اطلاعاتی با هدف صدمه‌زدن به سیستم‌های اطلاعاتی، روندها و منابع، ساختارهای حیاتی و مهم، تضعیف سیستم‌های سیاسی، اقتصادی و اجتماعی، عملیات‌های روانی گسترده برای بی ثبات‌سازی جامعه و دولت، همچنین مجبورکردن دولت برای اتخاذ تصمیماتی در راستای منافع مخالفین تعریف کرده است (عباسی و مرادی، ۱۳۹۴).

نظرات در مورد جنگ سایبری

اگر **حمله سایبری** واجد شرایط ذیل باشد می‌توان گفت که جنگ سایبری روی داده است:

- منبع و منشاء حمله از جانب یک یا چند کشور باشد.
- عواقب و نتایج حملات، مخرب و جبران‌ناپذیر باشد.
- برخوردار از انگیزه و اهداف سیاسی باشد.
- نیاز به طرح‌ریزی پیچیده و روش‌های سفارشی برای اجرا داشته باشد.

ویژگی‌های جنگ سایبری

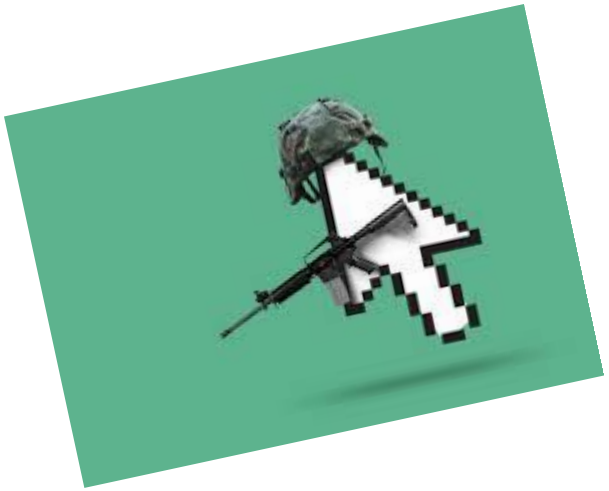
- حمله از راه دور
- دشواری در شناسایی و ردیابی
- محدودیت در انتقال
- تهدید متوجه هر سه جنبه امنیت
- اندازه هدف

ویژگی‌های جنگ سایبری

- انتشار حمله
- هزینه پایین
- مسئولیت‌پذیری
- راهبری ساده
- شروع و پایان
- از بین رفتن مرزهای شناخته‌شده فیزیکی

ویژگی های جنگ سایبر

1. **بدون مرز بودن فضای سایبر**
2. **کاهش هزینه جرم و یا حمله**
3. **امکان وارد آوردن خسارات مالی ، بدون آسیب های جسمی**
4. **تامین راحت امکانات و عوامل مورد نیاز برای اقدامات تروریستی**
5. **انعکاس جهانی موفقیت، مکتوم ماندن شکست ها**
6. **امکان هماهنگی لحظه ای در سراسر جهان با ضریب اطمینان بالا**
7. **امکان یارگیری و جذب حامیان از سراسر جهان**



خصوصیات جنگ سایبری

- جدیدترین و پیچیده‌ترین نبردها در جنگ پست مدرن
- بکر بودن، درصد هزینه کم و فایده بالا
- عدم توانایی کشور هدف در مشخص و اثبات نمودن منشأ تهدید
- عدم توانایی در تعیین میزان و دامنه خسارات وارد شده در مراحل اولیه شروع حمله
- مورد توجه کشورهای متخاصم به ویژه در جنگ‌های پنهان

تعریف جنگ سایبری

- جنگ سایبر در ساده‌ترین تعریف به عنوان «استفاده از رایانه و اینترنت برای جنگیدن در فضای سایبر تعریف شده است»

- در سند راهبردی پدافند سایبری کشور، جنگ سایبری بدین صورت تعریف شده است: بالاترین سطح و پیچیده‌ترین نوع از تهاجم سایبری که توسط ارتش سایبری کشورهای مهاجم یا گروه‌های سازماندهی‌شده تحت حمایت دولت‌های متخاصم علیه منافع ملی کشورها انجام می‌شود.

- جنگ سایبری به نوعی از نبرد اطلاق می‌شود 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 می‌اندازند.

سایبر در رزم

رزم سایبری


جنگ سایبری
هکرهای کلاه سفید یا هکر خوب
هکرهای کلاه خاکستری
هکرهای کلاه سیاه
هکرهای کلاه سبز
پلیس فتای تولید و تبادل اطلاعات
وقفه
اختلال در شبکه و توقف اطلاعات
تغییر اطلاعات

جنگ طب سوزنی در دکترین سایبر چین

- جنگ طب سوزنی(Acupuncture Warfare) یا جنگ فلج کننده یک نوع جنگ نامتقارن بر گرفته از تعالیم سان تزو است.

- نحوه عمل در این نوع جنگ به مانند ضربه زدن به نقاط حساس انسان در هنرهای رزمی بوده که باعث فلج کردن مبارز و از میدان به در شدن او می شود . در این نوع جنگ ابتدا نقاط بحرانی شبکه دشمن شناسایی و بررسی شده سپس با حمله به پیوند های ضعیف در فرماندهی ، کنترل ، ارتباطات و اطلاعات دشمن ، باعث فلج شدن سیستم آن گشته و بدین ترتیب کل سیستم دشمن از کار می افتد . هدف اصلی این گونه رزم این است که اولین نبرد آخرین نبرد باشد .

- چینی ها به چگونگی وابستگی غرب به زیر ساخت های فناری اطلاعات پی برده اند و می خواهند به مراکز ثقل آنها حمله کنند . آنها به یکپارچگی سیستم ها حمله کرده و باعث می شوند دشمنانشان نتوانند به سیستم های فرماندهی و کنترلشان اعتماد نمایند .

جنگ سایبری

- مفهوم جنگ سایبری
- انواع نفوذگران درجنگ سایبری
- انواع حملات نفوذگران
- محدودیت های جنگ سایبری
- اهداف جنگ سایبری

علائم جنگ سایبری

- منبع و منشاء حمله از جانب یک یا چند کشور باشد.
- عواقب و نتایج حملات، مخرب و جبران‌ناپذیر باشد.
- برخوردار از انگیزه و اهداف سیاسی باشد.
- نیاز به طرح‌ریزی پیچیده و روش‌های سفارشی برای اجرا داشته باشد.

تحلیل برخی حملات سایبری

حملات سایبری علیه زیرساخت‌های حیاتی جمهوری اسلامی ایران

- **اختلال سراسری در ایستگاه‌های قطار کشوری / احتمال حمله سایبری؟ (۱۴۰۰/۴/۱۸) ساعت ۱۹:۲۰**

به‌دنبال اختلال سراسری در ساعات اخیر در سیستم‌های کامپیوتری شرکت راه‌آهن که احتمالا بدلیل حمله سایبری است، فعالیت صدها خطوط قطار به تعویق افتاده و حتی لغو شد، ورودی‌ها و خروجی‌ها، مراکز خرید بلیط، خدمات الکترونیک باری و مسافری، و سایت شرکت راه آهن نیز دچار اختلال شدند.

این واقعه منجر به هرج و مرج بی‌سابقه‌ای در ایستگاه‌های قطار سراسر کشور شده است.

اختلال در سیستم‌های کامپیوتری، معطل شدن هزاران مسافر، آن هم بدون هیچ گونه پاسخگویی از طرف مقامات مسئول یا هیچ‌گونه پیش‌بینی در تجدید کار خطوط را با خود به همراه آورده است.

در این لحظات مسافرینی که در این ایستگاه‌ها حضور دارند پست‌های فراوانی را در صفحات اجتماعی خود به اشتراک می‌گذارند.

طبق گزارش به دست رسیده، صفحات اعلان ساعات ورود و خروج قطار، لغو فعالیت تمامی خطوط قطار را اعلان کرده و پیام «تاخیر زیاد به‌دنبال حملات سایبری» بر روی آنها قید شده است.

تحلیل و علت یابی حملات سایبری موفق به وزارت راه و راه آهن ؟

- **کم توجهی به الزامات امنیتی ابلاغ شده** از قبیل طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری و هشدارهای مرکز مدیریت راهبردی افتا، علت اصلی بروز حملات سایبری جمعه و شنبه گذشته به وزارت راه و شهرسازی و شرکت راه‌آهن بوده است.

- مرکز مرکز مدیریت راهبردی امنیت فضای تولید و تبادل اطلاعات ریاست جمهوری (افتا) در پی حملات سایبری هفته گذشته، **کم توجهی و ساده‌انگاری را دلیل اصلی وقوع این حملات** اعلام کرده است.

- **عملکرد ضعیف برخی دستگاه‌های دارای زیرساخت‌های حیاتی در اجرای الزامات امنیتی ابلاغ شده**

- برخی سازمان‌ها، **اینترنت و اینترانت را همچنان با هم و در یک سیستم استفاده می کنند،** بر دسترسی‌های از راه دور خود کنترل مناسبی ندارند و آسیب پذیری‌های اعلام شده را به موقع بروزرسانی نمی کنند.

- **مهاجمان توانسته‌اند به برخی از مدیریت سیستم‌ها، دسترسی یافته** و موجب اختلال در عملکرد عادی آنها شوند.

حملات سایبری به وزارت راه و راه آهن ؟

- **حمله یک ماه قبل رخ داده است**

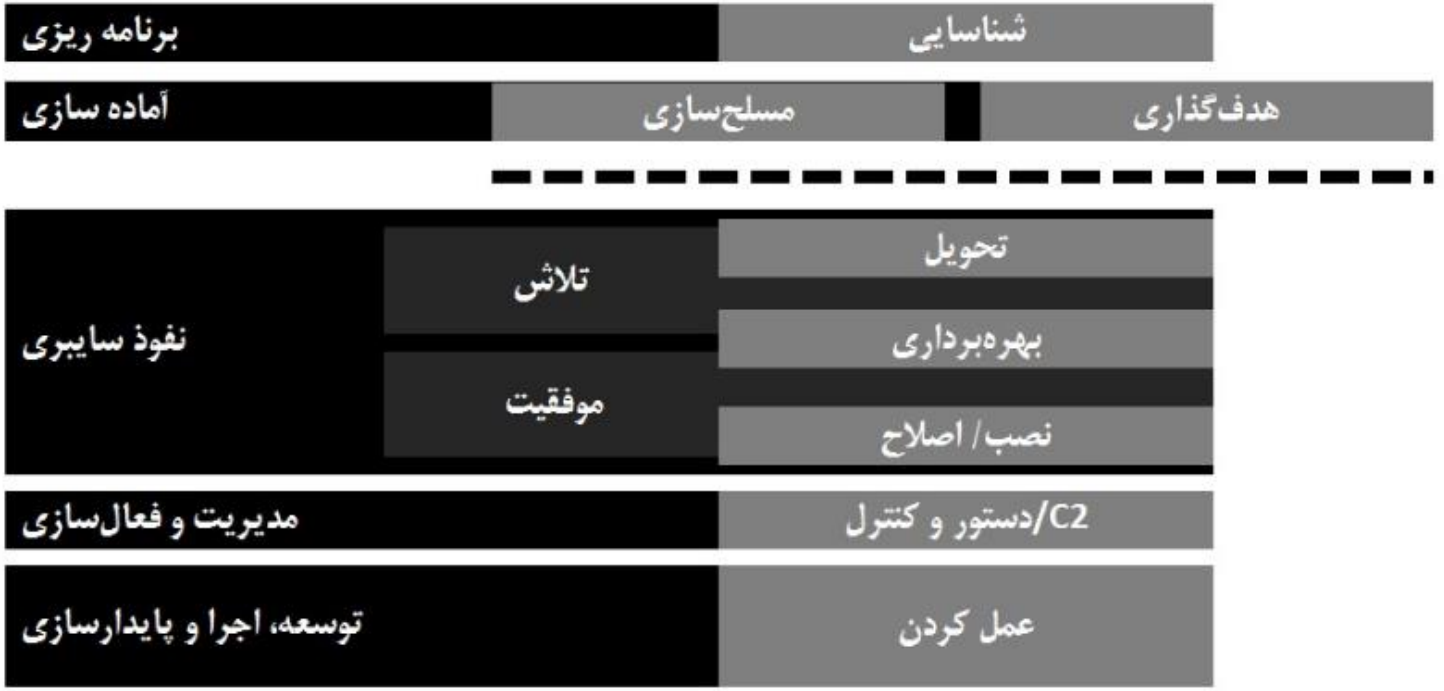
- نفوذ به سامانه‌های وزارت راه و شهرسازی و شرکت راه‌آهن، حداقل یک ماه قبل از مشخص شدن حمله سایبری، رخ داده است و مهاجمان از هفته دوم تیرماه برنامه حمله سایبری و ابزارهای خود را کاملا آماده کرده بودند و اطلاعات خارج شده از اعلامیه حمله سایبری، گواه آن است که هکران آن را، حدود ۷ روز قبل از حادثه سایبری آماده کرده‌اند.

- مهاجمان سایبری در هر دو حمله سایبری، تنظیمات لود شدن سیستم‌ها و کلمات عبور کاربران را یا حذف و یا تغییر داده بودند، سیستم قربانی را قفل، برای خود دسترسی مدیرسیستم (Admin) ایجاد و حالت بازیابی را در برخی سیستم‌ها غیرفعال کرده بودند.

- بدلیل زمان بر بودن تخریب دیتاها، مهاجمان به تخریب برخی از ساختارهای دیتا بسنده کرده‌اند.

- مهاجم یا مهاجمان سایبری در صورتیکه در حمله سایبری خود، کنترل سیستم را بدست گیرند، همه زیرساخت‌های IPرا تخریب می کنند و بیشترین ضربه را وارد می‌کنند.

مراحل حمله سایبری



مدل حمله به سرویس دهنده های اسکادا در سناریو زنجیره مرگ (شرکت Lockheed Martin**)**

سیستم های موجود در تاسیسات هسته ای نطنز (هدف حمله سلاح سایبری استاکس نت)

حملات نرم افزاری

حملات نرم افزاری

حملات نرم افزاری با اجرای یک قطعه کد به نام بدافزار توسط CPU بر روی سیستم انجام می شود. این بدافزار برای کنترل دستگاه به منظور دسترسی به هر گونه منابع سیستم (مانند ID، RAM و محتوای حافظه فلش یا رجیسترهای جانبی) یا اصلاح عملکرد آن در نظر گرفته شده است.

این نوع حمله بیشتر تهدیدات دستگاه را به دلایل زیر نشان می دهد:

- هزینه حمله کم است زیرا به تجهیزات خاصی نیاز ندارد بلکه به رایانه شخصی نیاز دارد.
- بسیاری از هکرها می‌تواند تلاشهای خود را کنار هم بگذارند، تخصص و ترفندهای خود را به اشتراک بگذارند، به طوری که در صورت وجود یک نقض امنیتی، احتمال وقوع یک حمله موفقیت‌آمیز وجود دارد. علاوه بر این، در صورت موفقیت، پروتکل حمله ممکن است خیلی سریع از طریق وب پخش شود

بدافزار را می‌توان به دستگاه تزریق کرد یا می‌تواند از قبل (تهدید داخلی) در firmware برنامه اصلی از طریق یک کتابخانه غیرقابل اعتماد یا تأیید نشده وجود داشته باشد.

بدافزارها انواع مختلفی دارند و می توانند بسیار کوچک باشند و به راحتی پنهان شوند. کارهایی که یک بدافزار می تواند انجام دهد:

- پیکربندی دستگاه را تغییر دهد (مانند option bytes یا ویژگی های حافظه).
- محافظت ها را غیرفعال کند
- حافظه را بخواند و محتوای آن را برای firmware دامپ و داده‌ها را کلون کند.
- ردیابی یا ثبت اطلاعات دستگاه
- دسترسی به موارد رمزنگاری
- کانال/رابط ارتباطی را باز کند.
- عملکرد دستگاه را تغییر دهد یا مسدود کند.

حتی زمانی که برنامه کاربر کاملاً قابل اعتماد، بدون اشکال و ایزوله باشد، بدون هیچ وسیله ای برای برقراری ارتباط با دنیای خارجی بازهم حملات نرم افزاری باید در نظر گرفته شوند.

حملات سخت افزاری

حملات سخت افزاری نیاز به دسترسی فیزیکی به دستگاه یا اغلب به چندین دستگاه به صورت موازی دارند.
این حملات به دو نوع حمله که از نظر هزینه، زمان و تخصص لازم تفاوت دارند تقسیم می‌شود:

- حملات غیرتهاجمی فقط دسترسی خارجی به دستگاه دارند
- حملات تهاجمی دسترسی مستقیم

گزارش تحلیلی از

حمله سایبری به

سامانه هوشمند توزیع سوخت

حمله سایبری اخیر علیه جمهوری اسلامی ایران(بحران سوخت– بنزین)

در تاریخ ۱۴۰۰/۰۸/۰۴ تمام پمپ بنزین های کشور به دلیل حمله سایبری از کار افتادند. سازمانهای مسئول، وقوع حمله سایبری را تایید کردند. این حمله سایبری، کشور را در آستانه یک بحران جدید قرار داده بود که با اقدامات مناسب شرکت ملی پخش و پوشش خبری مناسب رسانه ها این بحران مهار شد.

مقامات مسئول گمانه زنی هایی را مطرح کردند مبنی بر اینکه این حمله از خارج کشور انجام شده است. همچنین وعده دادند در روزهای آینده جزئیات بیشتری از این حمله سایبری را منتشر خواهند کرد.

- **سامانه هوشمند توزیع سوخت**

این پروژه، از پروژه های ملی و شاخص فناوری اطلاعات در کشور بوده است که در آن بخشهای نرم افزاری و سخت افزاری و تجهیزات الکترونیکی و زیرساختهای ارتباطی متنوعی استفاده شده است. گروهی که این حمله سایبری را انجام داده اند قطعا اشراف کاملی به معماری و تجهیزات بکار گرفته شده در آن داشته اند.

معماری و تجهیزات بکاررفته در شبکه هوشمند توزیع سوخت

تحلیل و بررسی (اهداف حملات)

- بررسی ها نشان از برنامه‌ریزی منسجم از سوی برخی دولت‌ها و ارتش‌ها در تهاجم سایبری دو دهه اخیر علیه دولت‌ها و ملت‌های دیگر دارد.

- بررسی تهدیدها و تهاجم‌های سایبری
چندساله اخیر علیه زیرساخت‌های حیاتی نشان دهنده گونه‌ای از تهدیدات برنامه‌ریزی‌شده و در بیشتر مواقع با تصمیم‌سازی از سوی دولت‌ها و ارتش‌ها است.

- به دلیل دخالت دولت‌ها و ارتش‌ها، لازم است در تدابیر مربوط به امنیت زیرساخت‌های حیاتی، ملاحظات پدافند غیرعامل برای شناخت تهدیدات امنیتی سایبری به‌عنوان اقدامی اساسی در حفظ، توسعه و ارتقاء امنیت سایبری در نظر گرفته شود.

آناتومی تهدیدات سایبری

آسیب‌پذیری سایبری

آسیب‌پذیری، به ضعف موجود در داخل یک سرمایه، رویه‌های امنیتی یا کنترل‌های داخلی یا پیاده‌سازی آن سرمایه، که قابلیت بهره‌برداری یا فعال‌شدن توسط یک تهدید خارجی را داشته باشد، اطلاق می‌گردد.

تهدیدسایبری

هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به ماموریت‌ها، وظایف، سامانه های سایبری یا پرسنل دستگاه به واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، تخریب، افشاء، تغییر اطلاعات، ممانعت یا اختلال در ارائه خدمت.

اهداف جنگ های سایبر

مراکز نظامی، خدمات اجتماعی، سامانه های نقل و انتقال، مخابرات، نیرو انرژی، سرویس های خدماتی ضروری و هر زیرساخت حیاتی می تواند قربانی این جنگ ها بوده و امنیت، ایمنی و پایداری آن به خطر افتد.

طبقه‌بندی تهدیدهای سایبری در سند افتا

هدف تهدیدات	شرح
افشاء	عبارت است از تهدیدی که در صورت عملی شدن آن، اطلاعات و داده‌ها در اختیار افراد غیرمجاز قرارگیرد.
جعل	عبارت است از تهدیدی که در صورت عملی شدن آن اطلاعات و داده‌های غیرواقعی در محیط زیر فضا تزریق شود و مورداستفاده قرار گیرد.
تغییر	عبارت است از تهدیدی که در صورت عملی شدن آن، اطلاعات و داده‌های غیرواقعی (تغییریافته (در محیط زیر فضا جایگزین اطلاعات و داده‌های واقعی گردد.
انکار	عبارت است از تهدیدی که در صورت عملی شدن آن، از ارائه خدمات و اطلاعات در محیط زیر فضا به دلایل ناموجه جلوگیری شود.
از کار اندازی	عبارت است از تهدیدی که در صورت عملی شدن، به اختلال یا ازکارافتادن خدمات خاصی در محیط زیر فضا منجر شود.

دسته‌بندی تهدیدهای سایبری درگزارش کنگره ایالات‌متحده امریکا

منشأ تهدیدات	شرح
عملگرهای شبکه‌های بات	شبکه‌هایی از سیستم‌ها که با کنترل از راه دور برای حملات قربانی شده‌اند.
گروه‌های بزهکار (جنایتکاران)	گروه‌هایی با نیات پلید و با قصد نابودی سیستم‌ها و اطلاعات
هکرها	افراد با قصد و نیت خرابکارانه
نفوذ گران داخلی	افراد ناراضی و کارکنان غیرحرفه‌ای
دولت‌ها	تهدیدکنندگانی در سطح دولت‌ها با قصد حمله، پاسخ و یا کسب اطلاعات است.
فیشرها	هکرهایی که با استفاده از تکنیک مهندسی اجتماعی برای سرقت اطلاعات حساس -نظیر نام کاربری، رمز عبور و رمز کارت‌های اعتباری- اقدام می‌کنند.
منتشرکنندگان هرزنامه‌ها	افرادی که پیام یا پست الکترونیکی بدون درخواست گیرنده و برای افراد بی‌شماری ارسال می‌کنند و به‌عنوان ابزار اصلی برای انتقال بدافزارها و آدرس‌های مخرب استفاده می‌کنند.
طراحان جاسوس‌افزار و بدافزار	افرادی که برای کسب اطلاعات با بدافزارها اقدام به جاسوسی در فضای سایبر می‌کنند.
تروریست‌ها	افرادی که با استفاده از ابزارها و تکنیک‌ها در فضای سایبر اقدام به زمینه‌سازی برای ترور
منع سرویس	هدف جلوگیری از ارائه سرویس با اقداماتی مثل استفاده از بدافزار و ....
منع سرویس توزیع‌شده	جلوگیری از ارائه سرویس به شکلی گسترده با استفاده از شبکه سیستم‌های قربانی

دسته‌بندی تهدیدهای سایبری
AVOIDIT

معیار دسته‌بندی	شرح
روش حمله	روش حمله به‌عنوان مسیر حمله است که از طریق آن مهاجم می‌تواند با استفاده از آسیب‌پذیری‌ها به سیستم دسترسی پیدا کند. آسیب‌پذیری‌هایی مثل: پیکربندي نادرست، عیوب هسته، خطاهاي طراحی، سرریز بافر، اعتبارسنجی ناکافی ورودي، پیوندهاي نمادین، حمله توصیفگر فایل و ...
هدف حمله	حملات سایبری به سیستم‌ها و مؤلفه‌های نرم‌افزاری و سخت‌افزاری مختلف یک شبکه حمله می‌کنند و بنابراین مدافعان را در یک وضعیت مبهم نسبت به شناسایی هدف بعدی حملات آینده قرار می‌دهند. اهداف عبارت‌اند از: سیستم‌عامل، شبکه، کاربر و...
تأثیر عملیاتی	امکان دستیابی به منابع و داده‌های حساس برای مهاجمان و فراهم شدن اطلاعات سطح بالاي کارشناسان و کاربران سیستم برای آنها. مثل: سوءاستفاده از منابع، مسلط شدن بر کاربر و ...
تأثیر اطلاعاتی	یک حمله علیه یک سیستم هدف می‌تواند به طرق مختلف روی اطلاعات حساس تأثیر گذارد. آثار مختلف حملات سایبری روی اطلاعات عبارت‌اند از: دست‌کاری، وقفه، تخریب و ...
شیوه دفاع	در نظر گرفتن مکانیزم‌ها و راهبردهای دفاعی از طریق: کاهش تأثیر، حذف از شبکه، توصیه مراجع و ...

دسته‌بندی بر اساس ریسک‌های امنیتی سایبری (دانشگاه کارنگی ملون– آپا)

ریسک‌های امنیتی	شرح
اعمال انسان‌ها	اقدامات مخاطره‌آمیز انجام‌شده انسانی
خرابی سیستم‌ها و فناوری	اشکالات فنی در سیستم‌ها و مشکلات به‌کارگیری و استفاده از فناوری
پردازه‌های داخلی خراب‌شده	فرایندهای داخلی که دارای اشکال هستند.
وقایع خارجی	انفاقات خارج از کنترل که در محدوده سیستم نیست.

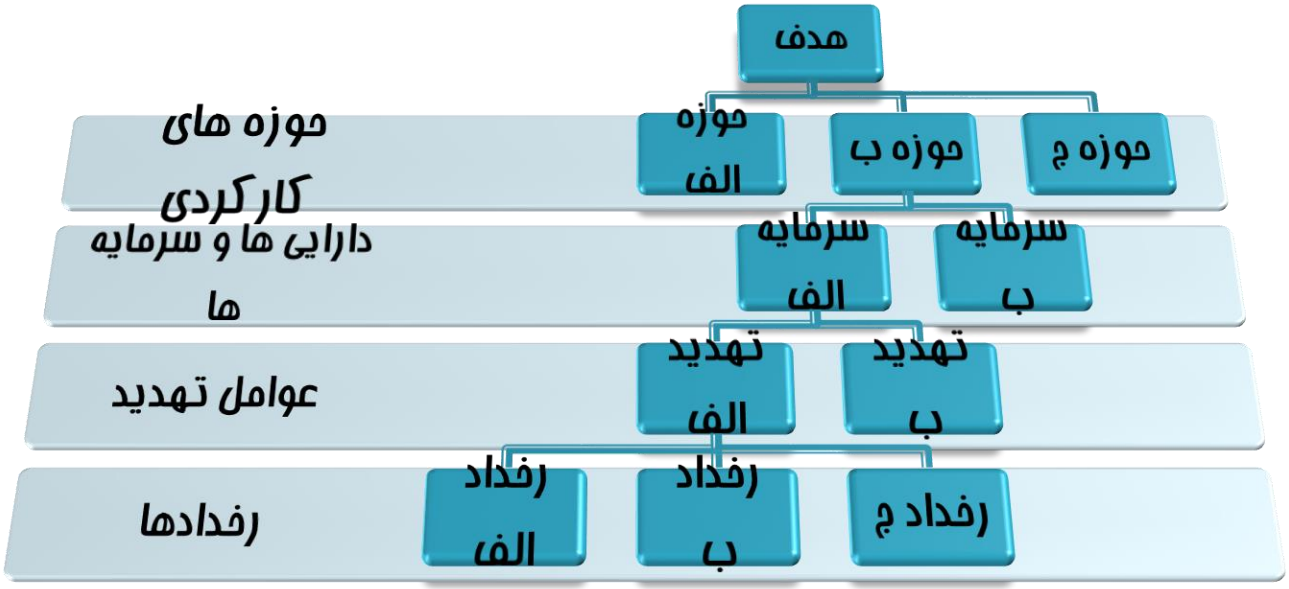
دسته‌بندی بر اساس شدت تهدید
F-Secure

دسته تهدیدات	شرح
نرم افزار های مخرب	برنامه های این دسته شامل ویروس ها، کرم ها و تروجان‌ها هستند. عملکرد این برنامه های مخرب در محدوده سرقت اطلاعات محرمانه کاربر، آلوده کردن کامپیوتر و از بین بردن اطلاعات کاربر می باشد.
نرم افزار های جاسوسی	جاسوس افزارها بدافزارهایی هستند که بر روی رایانه کاربر نصب می‌شوند و بدون اطلاع وی، اطلاعات مختلف درمورد او را جمع‌آوری می‌کنند .اکثر جاسوس‌افزارها از دید کاربرها مخفی می‌مانند و تشخیص و پیدا کردن آنها در اغلب موارد مشکل است.
نرم افزار های دارای ریسک	برنامه هایی هستند که در صورت استفاده از آنها امکان ریسک وجود دارد و در صورت سوء استفاده توسط حمله کننده باعث تخریب اطلاعات می شود.

تعریف مایکروسافت برای تقسیم‌بندی تهدیدات

تقسیم‌بندی تهدیدات	شرح
فریب دادن	ارائه هویت جعلی برای فریب ارسال کننده یا دریافت‌کننده (Spoofing identity)
دست‌کاری داده	تغییر داده به‌نحوی‌که صحت و درستی اصل داده خدشه‌دار شود (Tampering with data).
انکار	اعلام ناصحیح از وضعیت داده ارسال‌شده (Repudiation)
افشای اطلاعات	ارائه اطلاعات به افراد غیرمجاز (Information disclosure)
منع سرویس	جلوگیری از ارائه سرویس (Denial of service)
افزایش سطح دسترسی	افزایش سطح دسترسی بدون مجوز برای افراد غیرمجاز (Elevation of privilege)

درخت تهدید


هدف
حوزه الف
حوزه ب
حوزه ج
سرمایه الف
سرمایه ب
تهدید الف
تهدید ب
رخداد الف
رخداد ب
رخداد ج
حوزه های کارکردی
دارایی ها و سرمایه ها
عوامل تهدید
رخدادها

برخی اهداف مهم تهدیدات سایبری : انواع زیرساخت های حیاتی

- به‌طورکلی می‌توان زیرساخت‌های حیاتی را به ۱۶ بخش، با سیستم‌ها، شبکه‌ها، اجزای فیزیکی و مجازی مجزا تقسیم کرد. بروز اختلال در هر یک از این ۱۶ زیرساخت حیاتی، امنیت، اقتصاد ملی و بهداشت را با نارسایی شدید مواجه می‌کند:

- **صنایع شیمیایی**
- **بخش خدمات تجاری**
- **بخش‌های تولیدی شاخص**
- **بخش صنایع دفاعی**
- **بخش انرژی**
- **صنایع غذایی و کشاورزی**
- **بخش فناوری اطلاعات**
- **زیرساخت‌های انرژی هسته‌ای و دفع پسماندهای اتمی**
- **سیستم حمل‌ونقل**
- **بخش آب و فاضلاب**
- **بخش خدمات دولتی**
- **بخش ارتباطات**
- **بخش سدها**
- **بخش خدمات اضطراری**
- **بخش خدمات مالی**
- **بخش بهداشت و درمان عمومی**

«انواع حملات سایبری»

- استراق سمع به‌صورت عام (مکالمات، دیتا، تصویر) به روش‌های مختلف و از راه دور
- جاسوسی از راه دور و از طریق بستر شبکه
- اختلال یا قطع شبکه‌های اطلاع رسانی مانند قطع سیگنال رسانی به صدا و سیما
- قطع کامل یا اختلال در شبکه‌های ارتباطات تلفنی داخل و یا خارج از کشور (شهری، بین شهری، بین‌الملل، موبایل)
- 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...
- انهدام و یا آسیب‌رسانی به تاسیسات صنعتی کشور از قبیل پالایشگاه‌ها، نیروگاه‌ها و... با استفاده از نفوذ در سیستم های کنترلی این تاسیسات

«انواع حملات سایبری»

- 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
- ممانعت از استفاده برخی سرویس‌های شبکه جهانی اینترنت به بهانه تحریم‌ها
- قطع ارتباط با سامانه میزبانیHosting(مراکز داده در مواقع حساس)
- حمله سایبری به مراکز نگهداری داده اعم از بومی و غیر بومی
- دسترسی غیر مجاز به بانک‌های اطلاعاتی مختلف از قبیل دسترسی غیر قانونی به بانک اطلاعاتی سازمان ثبت احوال کشور
- ورود غیر قانونی به حریم خصوصی افراد و امکان ایجاد مشکلات مختلف برای زندگی مردم
- حمله به وب سایت‌های متعلق به سازمان ها ، نهادها به منظور جلوگیری از ارائه خدمات به مردم

انواع حملات

حملات خاموش:

این حملات شامل فعالیت هایی می شوند که در آنها بدون انجام هرگونه فعالیت ظاهری یا ایجاد تغییرات در سیستم های آسیب پذیر، به آنها نفوذ شده و منجر به سوء استفاده از منابع سیستم می گردد.

حملات فعال:

این حملات، حملاتی هستند که به سیستم های رایانه ای زیرساخت های حیاتی نفوذ می کنند و میتوانند اطلاعات حساس را دستکاری کنند و باعث بروز حوادث و فجایع ملی و جبران ناپذیر گردند .از اهداف آنها می توان، از کار انداختن شبکه های خدماتی عمومی مثل شبکه برق، گاز و ... و همچنین ایجاد وحشت و ترس در جامعه و کاهش میزان اعتماد به دولت و نظام را برشمرد.

روش های حملات سایبری

نوع حمله	توصیف
انکار خدمات	در این روش دسترسی سامانه به کاربران مجاز 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 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 کند 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.

روش های حملات سایبری

نوع حمله	توصیف
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 ای بی سیم	روشی برای امکان ورود به شبکه های رایانه ای بی سیم با استفاده از لپ تاپ، آنتن و کارت شبکه بی سیم که شامل گشت زنی در موقعیت های خاص برای دسترسی غیر مجاز می باشد.

روش های حملات سایبری

نوع حمله	توصیف
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 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.

برخی ابزارها در حملات سایبری

بدافزارها: (malicious software)

ابزارهای بد نیتی هستند که به صورت مخفیانه وارد سیستم کاربر میشوند و اعمال خاص بدافزارها خود را روی داده های قربانی انجام میدهند که ممکن است خساراتی به بار آورند و به علت آنکه معمولاً کاربر را آزار می دهند یا خسارتی به وجود می آورند، به این نام مشهورند. Malware واژه ای عمومی برای معرفی انواع ویروس ها، کرم ها، ابزارهای جاسوسی، تروآ و ... است

ویروس:

ویروس برنامه یا کد(اسکریپت) بسیار کوچکی است که بر روی برنامه های بزرگتر سوار می شود .یعنی در بین کد های اصلی یا فایل های اصلی بک برنامه دیگر که معمولا پر کاربرد می باشد قرار می گیرد و به محض نصب برنامه اصلی خود را وارد سیستم رایانه ای شخص قربانی می کند و هنگام اجرای برنامه به طور خود کار اجرا می شود و شروع به تخریب (کارهایی که نویسنده ویروس از آن خواسته) می کنند .

کرم اینترنتی (Worm)

یک کرم در واقع کد خرابکاری است که خود را انتشار می دهد و قادر است به صورت خودکار در شبکه ها گسترش پیدا کند.

یک کرم می تواند دست به اعمال مضری مانند مصرف پهنای باند شبکه یا مصرف منابع محلی سیستم بزند و منجر به حملات انکار سرویس شود .برخی از کرم ها می توانند بدون مداخله کاربر اجرا شده و گسترش پیدا کنند در حالی که برخی از کرم ها نیاز دارند کاربر آنها را مستقیماً اجرا کرده تا بتوانند گسترش پیدا کنند .کرم ها علاوه بر تکرار خود قادرند یک عملیات خرابکارانه را نیز بر سیستم قربانی اعمال کنند.

اسب تروا (Trojan)

گونه دیگر از برنامه های مخرب اسب تروا یا همان تروجان است .این نوع از برنامه ها در ظاهر برنامه هایی مفید و بی ضرر هستند ولی در اصل کار این برنامه ها تخریب و دزدی اطلاعات است. تروجان می تواند از طریق ایمیل و یا سایت های گول زننده انتقال یابد از این نوع مخرب بیشتر برای دزیدن کلمه عبور ایمیل ها استفاده می شود که برای فرد قربانی به صورت عکس و یا برنامه های گول زننده مانند کرک نرم افزار فرستاده می شود.

SYSTEM MONITOR.1:

سیستم مانیتور برنامه ای خاص است که برای کنترل فعالیت کاربران استفاده می شود این گونه برنامه ها می توانند اطلاعاتی از قبیل آدرس ایمیل و کلمات عبور و کلماتی که توسط صفحه کلید تایپ شده را جمع آوری کنند .این نوع از برنامه ها حتی می توانند از فعالیت های کاربران عکس برداری کنند و به یک ایمیل خاص ارسال کنند.

BACK DOOR.1:

به زبان ساده تر از در پشتی وارد شدن .این نوع از برنامــه ها که یک هکر بر روی یک سیستم اجرا کرده و راه را برای نفوذ مجدد باز می کند.

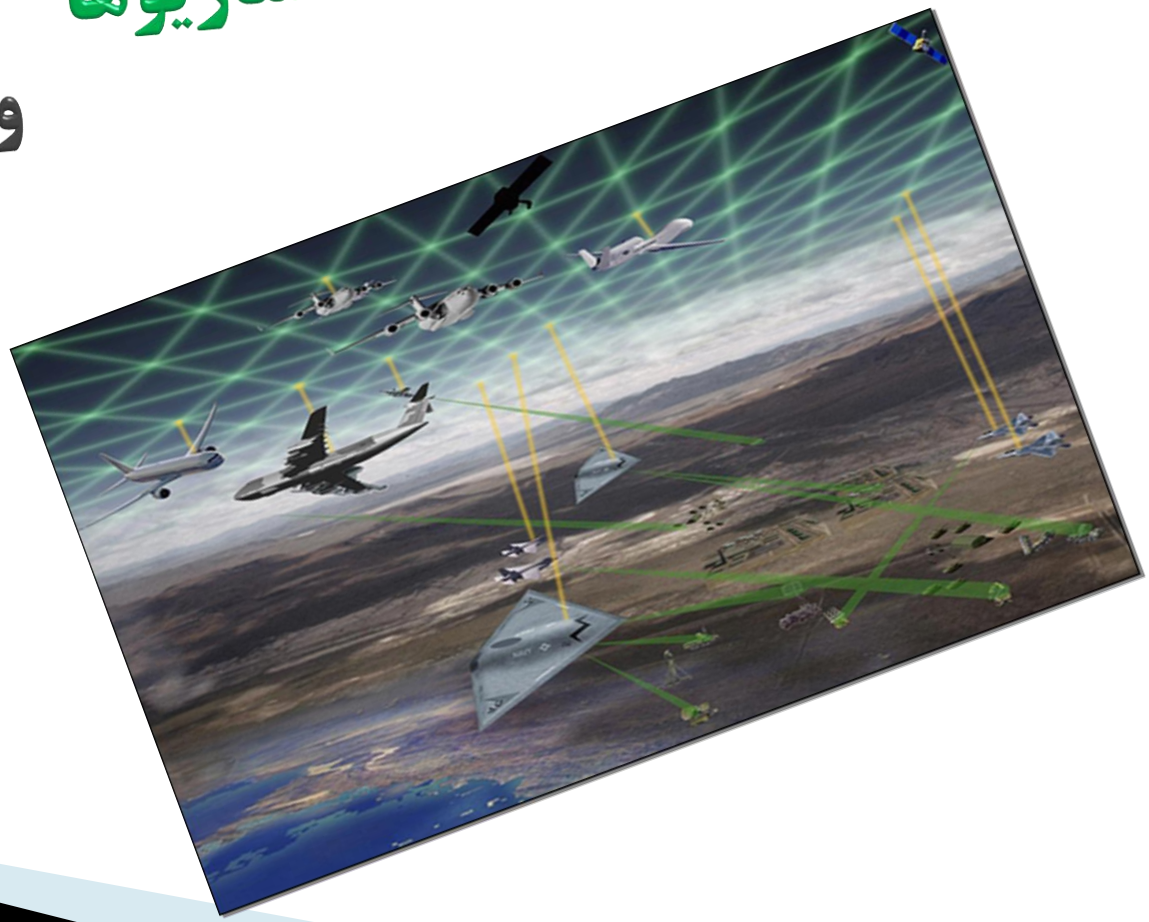
:TRACE.1

یک نوع دیگر از برنامه ها تریس می باشند این گونه از برنامه ها می توانند به صورت های مختلف اعمال تخریب را انجام دهند به صورتی که می توانند وارد محیط ریجستری شده و یا در حافظه رم و یا درون دیسکت ها مقیم شوند و حتی خود را با یک برنامه ترکیب کرده و اعمال تخریب را انجام دهند.

SPY.1 :

هر برنامه ای که بصورت مخفیانه وارد سیستم شود اسپای نامیـده مـی شود که این نوع از مخرب ها کلمه عبور ایمیـل و آی دی و حتـی کـارت های اعتباری را برای فرد هکر ارسال می کنند.

منشاء جنگ سایبری،
اهداف،
سناریوها
و
پیامدهای آن



منشاء جنگ سایبری

- به طور کلی منشاء جنگ سایبری را می‌توان در نیروی سایبری کشور مهاجم یا گروه‌های سازمان‌دهی‌شده تحت دولت‌های متخاصم، سلاح‌های سایبری تحت کنترل یا رهاشده توسط این نیروها دانست.

- **نفوذگران سایبری نظامی**

- **نفوذگران سایبری عضو تشکیلات حکومتی یا اشخاص شبه‌حکومتی**

- **نفوذگران سایبری اجیرشده توسط دولت‌ها**

- **نفوذگران سایبری تحت تحریک عوامل دولتی**

- **حملات سایبری که از رایانه‌های موجود در کشوری خاص بدون دخالت هیچ دولتی، سرچشمه گرفته‌اند.**

اهداف ؟

- هدف راهبردی :

سطله‌طلبی

براندازی در سطح حاکمیت و دولت

عملیاتی

مراکز نظامی، خدمات اجتماعی، سامانه های نقل و انتقال، مخابرات، نیرو انرژی، سرویس های خدماتی ضروری و هر زیرساخت حیاتی می تواند قربانی این جنگ ها بوده و امنیت، ایمنی و پایداری آن به خطر افتد.

(سازمان پدافند غیرعامل کشور، ۱۳۹۴)

سناریوها؟

- **سناریو۱):** جاسوسی سایبری با حمایت دولت‌ها با هدف جمع‌آوری اطلاعات برای برنامه‌ریزی تهاجم‌های سایبری بعدی
- **سناریو۲):** یورش سایبری با هدف بسترسازی برای هرج و مرج و شورش مردمی
- **سناریو۳):** یورش (تهاجم) سایبری با هدف از کاراندازی تجهیزات و تسهیل تهاجم فیزیکی
- **سناریو٤):** یورش (تهاجم) سایبری به عنوان مکمل تهاجم فیزیکی
- **سناریو٥):** یورش (تهاجم) سایبری با هدف تخریب یا اختلال گسترده به عنوان هدف نهایی جنگ سایبری

پیامدهای جنگ سایبری؟

- براندازی نظام حاکمیتی یا تهدید فاجعه‌بار امنیت ملی
- آغاز همزمان جنگ فیزیکی یـا زمینـه‌سـازی و تسـهیل شـروع
- 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 عمـومی (از طریق ایجاد آلودگی هسته‌ای، شیمیایی یا بیولوژیک)
- هرج ومرج و شورش داخلی
- اختلال گسترده در اداره امور کشور
- تخریب (یا صدمه گسترده بـه) اطمینـان عمـومی یـا باورهـای دینی، ملی و قومی
- خسارت شدید به (یا اختلال گسترده در) اقتصاد ملی
- تخریب یا اختلال گسترده در عملکرد سرمایه‌های ملی سایبری

سربازان جنگ سایبری

- **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 چاله‌های 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.

چالش های جنگ سایبری در جهان (دیدگاه حقوقی)

۱

- نبود یک قانون جهانی مورد قبول همه کشورها در حوزه جنگ سایبری
- نبود درک مشترک در خصوص قواعد حقوق بین‌الملل قابل اعمال بر رفتار دولت‌ها در حوزه فضای سایبر
- عدم تمایل دولت‌ها به ایجاد معاهدات و اسناد حقوقی الزام‌آور در حوزه جنگ‌ها و مناقشات سایبری
- مشکل در انتساب حملات سایبری به دولت متخاصم و نبود قطعیت در این حوزه
- تردید در چگونگی و سطح برخورد حقوقی با حملات سایبری در حقوق بین‌الملل به علت ویژگی‌های خاص حملات در عرصه سایبر
- نبود اشتراک نظر بین‌المللی در خصوص نحوه پاسخگویی به حملات سایبری
- مشکل در انطباق اصل عدم مداخله در مورد حملات سایبری که به آستانه لازم برای ایجاد حمله مسلحانه نرسیده اند.

۲

- عدم بازدارندگی قوانین فعلی درحوزه جنگ سایبری و عدم مواجهه مهاجم با هزینه‌های بالا و پیامدهای سنگین در این عرصه از جنگ
- نبود تدابیر اعتمادساز و به تبع آن عدم اعتماد کشورها به قواعد حقوق بین‌الملل فعلی در حوزه جنگ سایبری
- عدم امکان تعمیم حقوق مخاصمات مسلحانه به حملات از سوی عوامل غیردولتی
- مشکل در اثبات کنترل یک دولت بر بازیگران غیردولتی درگیر در مخاصمات علیه دولت دیگر
- نبود اجماع بین‌المللی در خصوص تعریف جنگ سایبری
- همگام‌نبودن رشد نظام‌های حقوقی با رشد سریع فناوری‌های حوزه فضای سایبر و بروز مشکلات و چالش‌های جدید حقوقی در خصوص فناوری‌های جدید فضای سایبر

رفع چالش های جنگ سایبری در عرصه حقوق بین الملل؟ – ۱

- شکل‌گیری یک رژیم حقوقی مشترک جهانی مورد توافق اکثر کشورهای جهان ذیل سازمان ملل

- بازبینی نحوه اجرا و یا تفسیر قوانین فعلی موجود در حوزه منازعات و مناقشات و تطبیق آنها با وضعیت منازعه و جنگ در فضای سایبر و یا به عبارتی تعمیم قوانین موجود در حوزه حقوق بین‌الملل نظیر حقوق بشردوستانه به جنگ سایبری

- همکاری نزدیک و مساعدت دولت‌ها و سازمان‌ها و نهادهای بین‌المللی برای مقابله با حملات سایبری و شکل‌گیری پیمان‌ها و معاهدات حقوق الزام‌آور در عرصه جنگ سایبری

رفع چالش های جنگ سایبری در عرصه حقوق بین الملل؟–۲

- تدوین ساختار، سازوکار و امکانات لازم برای شناسایی و انتساب حملات سایبری
- تعیین نوع و شکل مناسب و سطح بازدارنده واکنش و پاسخگویی به حملات سایبری در نظام حقوق بین‌الملل، با درنظرگرفتن ضمانت اجرای لازم
- داشتن یک راهبرد یا خطمشی حقوقی باثبات و به هم پیوسته کشوری برای پاسخگویی به حملات سایبری و اعلام رسمی آن از سوی حاکمیت
- بررسی موردی حملات سایبری ناقض اصل عدم مداخله در دادگاه صالحه بین‌المللی

رفع چالش های جنگ سایبری در عرصه حقوق بین الملل؟–۳

- بالابردن هزینه‌های جنگ و مناقشه سایبری در جامعه بین‌الملل
- اتخاذ تدابیر اعتمادساز در معاهدات، توافقنامه‌ها یا بیانیه‌های مرتبط با جنگ سایبر
- مسئولیت‌پذیر و متعهدنمودن کشورها به کنترل عوامل غیردولتی در حملات سایبری و لزوم پاسخگویی آنها به حملات این عوامل به زیرساخت‌ها و منافع کشورهای دیگر
- تعریف روشن و دقیق جنگ سایبری در یک اجماع یا از سوی یک نهاد صالحه بین‌المللی و تعیین مصادیق و شاخص‌های آن
- همکاری و تعامل نزدیک متخصصان حقوق و فضای سایبری در عرصه بین‌الملل به منظور تسریع در تنظیم قواعد حقوقی حوزه فضای سایبر


محمد صلی اللہ علیہ وسلم