جنگ و دفاع سایبری

استان سیستان وبلوچستان
آذر ۱۴۰۱


بسم الله الرحمن الرحيم

1 در یک نگاه

تهدیدات فناوری پایه	تهدید سایبری	سرمایه های سایبری	فضای سایبری	لایه های فضای سایبری

ویژگی های کلیدی	تعاریف تهدید سایبری	بازتعریف تهدید سایبری	مثال هایی از تهدیدات سایبری	طیف کلی تهدیدات	ویژگی های تهدیدات
چالش های عمده	جنگ سایبری	شاخص های جنگ	ویژگی های جنگ	سناریوهای تهدیدات	زمینه سازان جنگ
پیامدهای جنگ	ویژگی های سلاح سایبری	مقایسه سلاح سایبری و دیجیتالی	ویژگی های سربازان سایبری	اشتباهات متداول	آسیب پذیری
تهدیدات سایبری	تهاجم سایبری	سلاح سایبری	جنگ سایبری	منشاء جنگ	پیامدهای جنگ
سناریوهای جنگ	پدافندهای سایبری	زیست بوم سایبری			

2 مقدمه

همهٔ ما شاهد توسعهٔ روز افزون فناوری اطلاعات و ارتباطات هستیم و به اهمیت و نقش اساسی آن در بافت اجتماعی آینده پی‌برده‌ایم. محاسن بسیاری چون سرعت، دقت، کیفیت، ایجاد شفافیت، ایجاد دسترسی و ... در فناوری اطلاعات نهفته است. شواهد و قراین حاکی ازآن است که کشورها ناگزیر از توسعهٔ فناوری اطلاعات و ارتباطات هستند. امروزه فناوری اطلاعات و ارتباطات به یک زیر ساختار حیاتی برای کشورها در کنار انرژی، سوخت، غذا، حمل و نقل و ... تبدیل شده است و شرایط جدیدی را به وجود آورده که به آن فضای سایبر گویند.

3 مقدمه

این فناوری روش ارتباط و تعامل انسان ها را به صورتی بنیادین دگرگون نموده است که به عنوان نمونه می توان به کار از راه دور، تجارت الکترونیک و دانشگاه مجازی و بسیاری موارد دیگر اشاره نمود. سرعت، کارایی و بهره وری این فناوری در انقلاب دیجیتال علاوه بر مزیت های بسیاری که به ارمغان آورده ، چالش های جدیدی را نیز برای امنیت و محرمانگی اطلاعات وارتباطات درشبکه های جهانی اطلاع رسانی و اینترنت ایجاد نموده است . عدم توجه کافی به این چالش‌ها و به عبارتی تمرکز بر توسعهٔ انفعالی فناوری اطلاعات و ارتباطات بدون توجه به همهٔ ابعاد آن ،می تواند در دراز مدت زیان های جبران ناپذیری را بر کشور تحمیل کند. پدیده هایی مثل جنگ سایبر که ماهیتًا با جنگ های واقعی تفاوت دارد و همچنین وابستگی اطلاعاتی و تکنولوژیکی ناشی از توسعهٔ فناوری اطلاعات به کشورهای دیگر می تواند ما را با مشکل روبرو نماید.

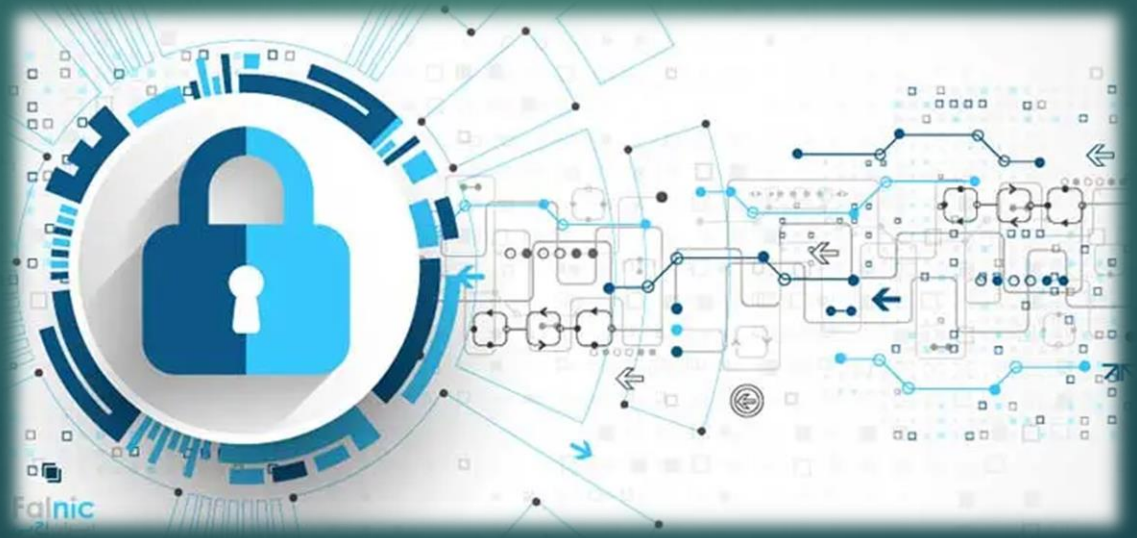
4 تهدیدات فناوری پایه

- تهدید سایبری
- تهدید پرتویی
- تهدید الکترومغناطیس
- تهدید زیستی
- تهدید شیمیایی
- تهدید سیگنالی
- تهدید الکترونیک

5

تهدید سایبری

تهدید سایبری پدیده‌ای جدید است که در دهه‌های اخیر، همزمان با تحول فناوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت، در سراسر جهان ظهور پیدا کرده است؛ به گونه ای که امروزه چالش تهدیدهای سایبری، هم مهم و هم پیچیده به نظر می‌رسد.



6 سرمایه های سایبری

این سرمایه ها عبارت اند از زیرساخت های فناوری اطلاعات و شبکه های ارتباطی و سامانه های اطلاعاتی و کنترلرهای صنعتی که به منظور تولید، پردازش، ذخیره سازی، ارسال، دریافت، امحاء، بازیابی و بهره برداری از اطلاعات مرتبط با زیرساخت‌های حیاتی، حساس و مهم کشور تعبیه شده اند.

7 فضای سایبری

- IT : فناوری اطلاعات و پروتکل
- CT : فناوری ارتباطات
- EW : جنگ الکترونیک
- IW : جنگ اطلاعات
- EMP :پالس‌های الکترومغناطیسی

8

لایه های فضای سایبری

براساس مدل ارائه شده در مقالهٔ «توصیف فضای سایبر»، فضای سایبر براساس یک مدل چهارلایه ای به شرح زیر توصیف شده است:

الف. لایهٔ فیزیکی: این لایه به منظور پشتیبانی از المان‌های منطقیِ فضای سایبر پیش بینی شده است.

ب. لایهٔ منطقی: در فضای سایبر، تمامی تصمیمات در لایهٔ منطقی اتخاذ می‌گردد.

ج. لایهٔ اطلاعات: لایهٔ اطلاعات در دو لایهٔ قبلی جاگذاری می‌شود و می‌تواند شکل های مختلفی داشته باشد.

د. لایهٔ جمعیت: این لایه متشکل از افراد و ویژگی های آن‌ها، اعم از ویژگی های هویتی، موقعیت جغرافیایی، علایق و سایر ویژگی های افراد است

9 ویژگی های کلیدی فضای سایبری

الف. مجازی بودن، دسترسی توأمان با ایجاد، داشتنِ اتصال متقابل، داشتن تعارض امنیت و آزادی با حریم خصوصی، غیرمستقیم بودن، غیرجنبشی بودن، بی‌قاعده بودن و داشتن عدم قطعیت؛

ب. تضمین مأموریت، فشرده بودن چرخهٔ تصمیم، تعارض گمنامی و داشتن اِسناد؛

ج. آسیب پذیربودن، وجود عدم تقارن، وجود گمنامی و عدم کفایت دفاع؛

د. داشتن تغییر سریع، داشتن ساختار پروتکل، گسترده بودن استانداردها، داشتن پیچیدگی زیاد، داشتن عدم تقارن و ابهام؛

هـ دیجیتالی بودن، وجود حافظهٔ مجازی، تعاملی بودن، فرامتن بودن، داشتن واقعیت مجازی، داشتن عدالت اطلاعاتی/ داشتن دسترسی برابر و گسترده، نامحسوس بودن فاصله (فرازمانی بودن)، داشتن سیالیت، اطلاعات محوربودن، حذف سلسله مراتب تصمیم گیری، نامرئی بودن، جهانی بودن (بی مرزبودن) و گمنام بودن؛ و عامل انتشار قدرت بودن

تعریف تهدید سایبری

احتمال هرگونه رویدادی که قابلیت واردنمودن ضربه به مأموریت ها، وظایف، تصویر (پنداره) یا اشتهار دستگاه متولی سرمایه ملی سایبری یا افراد مرتبط، به واسطه یک سامانه اطلاعاتی از طریق دسترسی غیرمجاز، انهدام (تخریب)، افشا، تغییر اطلاعات و ایجاد اختلال یا ممانعت از ارائهٔ خدمات را داشته باشد، **تهدید سایبری** گفته می‌شود .

بازتعریف تهدید سایبری

- قابلیت، نیت یا اقدام احتمالی متخاصمان بالقوه و بالفعل جمهوری اسلامی ایران.

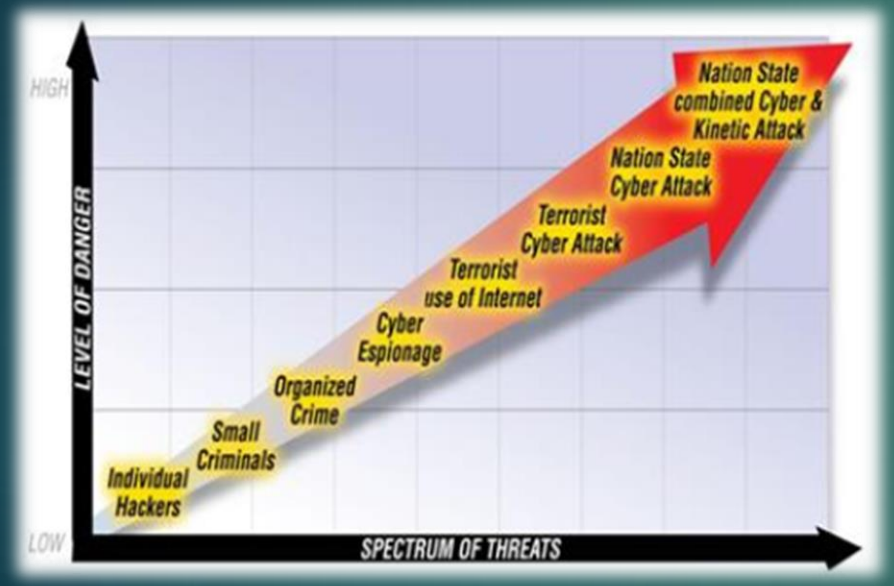
- از لایهٔ منطقی (اطلاعاتی یا سایبری) فضای سایبر، علیه سرمایه های ملی سایبری، به ویژه لایهٔ فیزیکی این سرمایه ها.

- با قابلیت تأثیرگذاری بر امنیت، منافع و اقتصاد ملی، وجهه و روابط بین المللی، سلامت، ایمنی و اطمینان عمومی، باورهای دینی و ملی یا ادارهٔ امور کشور.

مثال هایی از تهدید سایبری

- اختلال در شبکه های مخابراتی کشور اعم از شبکه تلفن ثابت ، موبایل و ... (شنود ، اختلال و انهدام)
- اختلال در شبکه حمل و نقل و ترافیک کشور(شبکه های مترو ، بین شهری ، زمینی ، هوایی و راه آهن)
- اختلال در شبکه برق کشور
- اختلال در شبکه گاز
- اختلال و سرقت در شبکه بانکی و مالی کشور
- اختلال در شبکه های صداوسیما

طیف کلی تهدیدات سایبری و سطوح رو به افزایش خطر



۱. پایین ترین سطح تهدید، هکر فردی است.

۲. دومین سطح، مجرمان کوچک قرار دارند؛ مثلاً گروهی که در فضای سایبری به بانک حمله می‌کنند.

۳. در سومین سطح، گروه های سازماندهی شده هستند. در این سطح ممکن است حتی ده گروه از کشورهای مختلف کنار هم قرار بگیرند؛ چون در فضای سایبر لازم نیست همگی از یک کشور باشند.

۴. درسطح بعدی، جاسوسی سایبری قرار دارد.

۵. در سطح بعد از آن، تروریست های اینترنتی قرار دارند.

۶. در سطح بالاتر، حملات سایبری با محوریت یک کشور قرار می‌گیرد و بالاتر از آن، حملات چند کشور علیه یک کشور. بدیهی است که در این طیف هرچه به سمت بالاتر می‌رویم، خطر بیشتر می‌شود و هرچه پایین‌تر می‌رویم، خطر کمتر

14 ویژگی های تهدیدات سایبری

- تاثیر حملات سایبری در زیرساخت های حیاتی و حساس
- تاثیر مستقیم بر امنیت ملی کشورها
- انتخاب مراکز و گره های ضعیف زنجیره

چالش‌های عمده تهدیدات سایبری

- سخت بودن اثبات منشأ تجاوز؛
- استفاده از پوشش لازم برای تهاجم؛
- امکان استفادهٔ غیرارادی از سایر منشأها؛
- توزیع تخصص‌های ذیربط در بخش‌های مختلف سایبری شامل سامانه‌های اسکادا،
- نظام جامع بانکی، سیستم عامل و...؛
- آسیب پذیری‌های عمده در اثر توسعهٔ زیرساخت‌ها؛
- ضعف عمده در معماری پدافند سایبری؛
- سازماندهی واحدهای تخصصی تجاوز سایبری در حوزه‌های عمده

16 جنگ سایبری

بالاترین سطح و پیچیده ترین نوع از تهاجم سایبری که توسط ارتش سایبری کشورهای مهاجم یا گروه‌های سازماندهی شدهٔ تحت حمایت دولت‌های متخاصم، علیه منافع ملی کشورها انجام می‌شود، جنگ سایبری است.

17 جنگ سایبری

جنگ سایبر عبارت است از انجام یا آماده شدن برای انجام عملیات های نظامی، مطابق با اصول مربوط به اطلاعات.
جنگ سایبر یعنی ایجاد اختلال {اگر نگوییم نابودی کامل}در سیستم های اطلاعاتی و ارتباطی که دشمن برای "دانستنِ"خود به آن‌ها تکیه می‌کند.
کشورهای درگیر جنگ سایبری تلاش می‌کنند همه چیز را دربارهٔ دشمن بدانند و در عین حال، نگذارند او هیچ چیز دربارهٔ آن‌ها بداند. به بیان دیگر، هدف اصلی در جنگ سایبر برهم زدن "موازنهٔ اطلاعات و دانش" به نفع نیروهای خودی است؛ به ویژه اگر"موازنهٔ توان رزمی" وجود نداشته باشد. بنابراین در این جنگ می توان با بهره گیری از دانش برتر، ضعف سرمایه و نفرات کمتر را جبران کرد و به پیروزی قاطع دست یافت.

شاخص های جنگ سایبری

منشأ تهاجم سایبری، یک کشور متجاوز سایبری است؛
- به جای ویروس معمولی، سلاح سایبری به کار گرفته می‌شود (سلاح سایبری دارای پیچیدگی، فرمان پذیری و هوشمندی بسیار زیاد است)؛
- سطح تهاجم سایبری و خسارت ناشی از آن، در سطح تهدید امنیت ملی است؛
- شدت تهاجم سایبری، بسیار زیاد و همراه با اختلال و تخریب فاجعه‌بار است؛
- پیامد تهاجم سایبری، اختلال گسترده در عملکرد سرمایه‌های ملی سایبری است.

19 ویژگی های جنگ سایبری

- منشأ تهدیدات، یک دولت متخاصم است؛
- از سلاح سایبری استفاده می‌شود؛
- سطح تولید خطر در سطح امنیت ملی است؛
- حوزۀ تهدیدات در سطح خطر شدید قرار دارد؛
- پیامد تهدید در سطح امنیت ملی است

20 سناریوهای تهدیدات جنگ های سایبری

- جنگ محدود به یک حوزه، با خطر در یک بخش، با هدف خسارت به یک بخش؛
- جنگ محدود به چند حوزه، با خطر در چند بخش، با هدف تهدید در امنیت کشور؛
- جنگ محدود به کل حوزه های حیاتی، با خطر در سطح ملی، با هدف خسارت عمده بر کشور؛
- جنگ کامل همزمان با چند سناریوی عمده، با هدف براندازی

21 زمینه سازان جنگ های سایبری

- وابسته شدن زیرساخت‌های حیاتی به فناوری آسیب پذیر؛
- اتکای زیاد به فناوری غیربومی؛
- اعتماد به ابزار و تجهیزات غیرخودی؛
- وابسته شدن خدمات حیاتی به بستر اینترنت؛
- عدم رعایت ملاحظات و توصیه های امنیتی و پدافندی در استفاده از فناوری

پیامد های جنگ های سایبری

- براندازی نظام حاکمیتی یا تهدید فاجعه‌بار امنیت ملی؛
- آغاز همزمان جنگ فیزیکی یا زمینه سازی و تسهیل شروع جنگ فیزیکی در آیندهٔ نزدیک؛
- تخریب یا صدمهٔ فاجعه‌بار به وجههٔ کشور در سطح بین‌المللی؛
- تخریب یا صدمهٔ فاجعه‌بار به روابط سیاسی و اقتصادی کشور؛
- ایجاد تلفات انسانی یا مخاطرهٔ گسترده برای سلامت و ایمنی عمومی از طریق آلودگی هسته‌ای، شیمیایی یا بیولوژیک؛
- هرج‌ومرج و شورش داخلی؛
- اختلال گسترده در ادارهٔ امور کشور؛
- تخریب یا زدن صدمهٔ گسترده به اطمینان عمومی یا باورهای دینی، ملی و قومی؛
- زدن خسارت شدید به اقتصاد ملی یا ایجاد اختلال گسترده در آن؛
- تخریب یا اختلال گسترده در عملکرد سرمایه های ملی سایبری

ویژگی های عمده سلاح سایبری

- هوشمندی در شناخت محیط؛
- قدرت پنهان شوندگی؛
- فرمان پذیری؛
- هدایت از راه دور؛
- استفاده از نهفتگی عامل تهدید؛
- وجود فضای نفوذی پیش نهفته

مقایسه سلاح های سایبری و دیجیتالی از نظر اقتصادی

با مقایسهٔ اسلحه های سایبری و اسلحه های دیجیتالی از نظر قیمت، مشاهده می‌شود که اسلحه های سایبری به شدت مقرون به صرفه هستند.

25 ویژگی های سربازان سایبری

- با چابکی و سرعت حمله می‌کنند؛
- حمله کنندگان از دید هدف مخفی هستند؛
- با صراحت و روانی حمله می‌کنند؛
- امکان تغییر حجم عملیات را دارند؛
- چندین تأثیر از یک حمله به دست می‌آورند؛
- هدف را در موقعیت واکنش قرار می‌دهند؛

اشتباهات متداول کاربران

کاربران، به افرادی اطلاق می گردد که طی روز با داده ها ی حساس در یک سازمان سروکار داشته وتصمیمات و فعالیت های آنان، داده ها ی حساس و مقوله امنیت و حفاظت ازاطلاعات را تحت تاثیرمستقیم قرار خواهد داد . در ادامه با برخی از اشتباهات متداولی که این نوع استفاده کنندگان از سیستم وشبکه مرتکب می شوند، اشاره می‌گردد.

27 آسیب پذیری سایبری

آسیب پذیری، به ضعف موجود در داخل یک سرمایه، رویه های امنیتی یا کنترل های داخلی، یا پیاده سازی آن سرمایه ملی سایبری، که قابلیت بهره برداری یا فعال شدن توسط تهدیدات داخلی و خارجی به منظور انجام جنگ سایبری را داشته باشد، اطلاق می گردد.

28

تهدیدات سایبری

هررویداد یا واقعه با قابلیت واردنمودن ضربه به مأموریت ها، وظـایف، تصویر (پنداره) یا اشتهار دستگاه متولی، سرمایه ملـی سـایبری یـا پرسنل دستگاه به واسطه یک سامانه اطلاعـاتی، ازطریـق دسترسـی غیرمجاز، انهدام (تخریب ،) افشاء، تغییراطلاعـات و / یـا ممانعـت از (ایجاداختلال در) ارائه خدمت

29 تهاجم سایبری

به هرگونه اقدام غیرمجاز سایبری، که با هدف نقض سیاست امنیتی یک سرمایه سایبری و ایجاد خرابی یا خسارت، ایجاد اختلال در عملکرد یا از کار اندازی خدمات و یا دستیابی به اطلاعات سرمایه ملی سایبری مذکور انجام گیرد، تهاجم سایبری اطلاق می گردد.

30 سلاح سایبری

سامانه‌ی سایبری که برای وارد نمودن خسارت (تخریب) به ساختار یا عملیات سامانه های سایبری دیگر، طراحی و تولید شده باشد. این سامانه ها، شامل شبکه ربات‌ها، بمب‌های منطقی، افزارهای بهره‌برداری از آسیب‌پذیری سایبری، انواع بدافزارها و سامانه‌های تولید ترافیک حملات ممانعت از سرویس و ممانعت از سرویس توزیع شده می‌باشند که برای انجام تهاجم‌های سایبری، مورد استفاده قرار می‌گیرند.

31

جنگ سایبری

بالاترین سطح و پیچیده ترین نوع از تهاجم سایبری(عملیات سایبری) است که علیه منافع ملی سایبری کشورها انجام شده و شدیدترین پیامدها را به همراه خواهد داشت. ویژگی های این نوع از تهاجم های سایبری، برای آن که دولت ها آنها را جنگ علیه منافع ملی خود تلقی نمایند.

32 منشاء جنگ سایبری

نیروی سایبری کشور مهاجم یا گروه های سازمان دهی شـده تحـت دولت های متخاصم، سلاح های سایبری تحت کنتـرل یـا رهـا شـده توسط این نیروها

33 پیامد جنگ سایبری

- براندازی نظام حاکمیتی یا تهدید فاجعه بار امنیت ملی
- آغاز همزمان جنگ فیزیکی یـا زمینـه سـازی و تسـهیل شـروع جنگ فیزیکی در آینده نزدیک
- تخریب یا صدمه فاجعه بار به وجهه کشور در سطح بین المللی
- تخریب یا صدمه فاجعه بار به روابط سیاسی و اقتصادی کشور
- تلفات انسانی یا مخاطره گسترده برای سلامت و ایمنی عمـومی)از طریق ایجاد آلودگی هسته ای، 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

نهضت سوادرسانه ای انقلاب اسلامی
استان سیستـــان وبلوچستـــان

34 سناریوهای جنگ سایبری

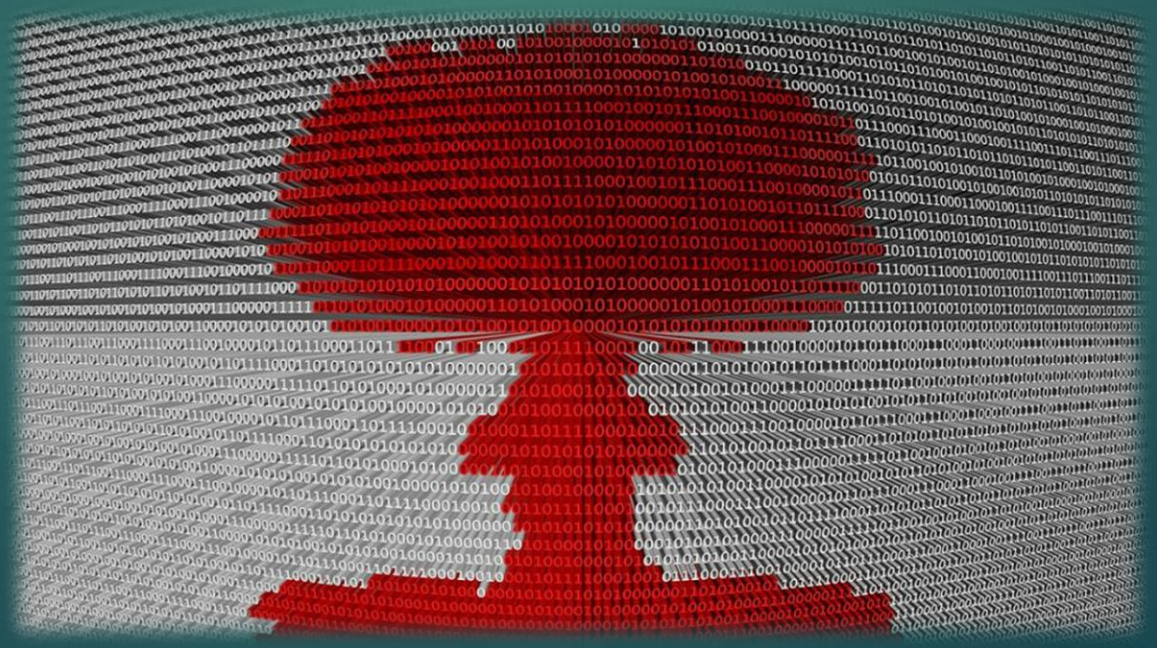
سناریو (۱) : جاسوسی سایبری با حمایت دولت‌ها با هدف جمع آوری اطلاعات برای برنامه ریزی تهاجم‌های سایبری بعدی

سناریو (۲) : یورش سایبری با هدف بسترسازی برای هرج‌ومرج و شورش مردمی

سناریو (۳) : یورش (تهاجم) سایبری با هدف از کار اندازی تجهیزات و تسهیل تهاجم فیزیکی

سناریو (۴) : یورش (تهاجم) سایبری به عنوان مکمل تهاجم فیزیکی

سناریو (۵) : یورش (تهاجم) سایبری با هدف تخریب یا اختلال گسترده به عنوان هدف نهایی – جنگ سایبری



35 پدافند سایبری

بهره‌گیری از کلیه امکانات غیر مسلحانه سایبری و غیرسایبری کشور، به منظور ایجاد بازدارندگی، پیشگیری، ممانعت از انجام، تشخیص به موقع، مقابله موثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری جمهوری اسلامی ایران، توسط متخاصمین سایبری، اعم از نیروی نظامی(ارتش سایبری) کشورهای متخاصم و گروه های تحت حمایت پنهان دولت های متخاصم به نحوی که امکان تهاجم سایبری را از کلیه متخاصمین سلب نماید.

زیست بوم سایبری

زیست بوم به ارتباط متقابل بین موجود زنده و محیط آن اطلاق می‌شود.

زیست بوم سایبری به شکل گیری محیطی بومی، پویا و زنده سایبری اشاره دارد که برای کشور در عرصه های مختلف حمایتگر و پشتیبانی کننده خواهد بود.

37 منابع

۱. مقاله حملات سایبری، ۱۳۸۸،شرکت ایزایران- مرکز پدافند غیرعامل- شماره/۸۲شبکه و امنیت/ مهر۱۳۸۸

۲. ملکیان، احسان، ۱۳۸۸،نفوذگری در شبکه و روشهای مقابله، تهران، نص، ۱۳۸۸

۳. تدابیر عملیات های سایبری آمریکا برای ۲۰۱۶_۲۰۲۸، سایت باشگاه افسران جوان جنگ نرم (club.revayat.ir)، شهریور ۱۳۹۰

۴. جنگ و دفاع سایبر،۱۳۸۴، اندیشگاه شریف و اندیشکده کاوشگران آینده، دی ماه ۱۳۸۴

۵. صدرزاده، حبیب، ۱۳۹۰، بعد هفتم: فضای سایبر، مجموعه مقالات نخستین همایش ملی دفاع سایبری، تهران، بهمن ماه ۱۳۹۰