فصلنامه سیاست دفاعی
سال چهاردهم، شمارهٔ ٥٤، بهار ١٣٨٥

حفاظت از زیرساخت‌های حیاتی اطلاعاتی

تاریخ دریافت مقاله : ٨٤/١٢/١٠
تاریخ تأیید مقاله : ٨٥/١/٢٥
صفحات مقاله : ١٢٨-٩١

نویسنده : علی عبدالله‌خانی*

چکیده

در این مقاله به منظور نزدیک شدن به طرح ریزی حفاظت از زیرساختهای حیاتی اطلاعاتی، در ج.ا.ایران، ابتدا مفهوم زیرساخت حیاتی را بررسی می‌نماییم. سپس ابعاد، روشها و رویکردهای موجود در حفاظت مورد بررسی قرار می‌گیرد. با این مقدمه چارچوب حفاظت از زیرساختهای حیاتی اطلاعاتی مشخص می‌گردد. بر همین اساس مهم‌ترین فاکتورها در زیرساختهای حیاتی اطلاعاتی در چند کشور مدل مانند آمریکا، استرالیا، انگلستان و سنگاپور مورد بررسی قرار می‌گیرد و به دنبال آن با ایده گرفتن از کشورهای مدل به ارائهٔ ایده‌های خود در خصوص طرح‌ریزی حفاظت از زیرساختهای حیاتی اطلاعاتی در ایران می‌پردازیم.

* * * * *

کلید واژگان

فضا، زیرساخت، زیرساخت حیاتی، زیرساخت حیاتی اطلاعاتی، حفاظت

---

* رئیس مؤسسه مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.
E-mail: Khani@-TISRI.org

مقدمه

همواره کشورها دارایی‌ها و سرمایه‌های مختلفی دارند که در اداره کردن امور کشور مورد استفاده قرار می‌دهند. البته برخی از این سرمایه‌ها و دارایی‌ها نسبت به برخی دیگر دارای اهمیت بیشتری است. تجربه و رویدادهای مختلف نشان داده که آسیب دیدن و یا از بین رفتن و از رده خارج شدن حتی موقت برخی از این دارایی‌ها و زیرساختها لطمات جبران‌ناپذیری را به کشور مربوطه وارد کرده است.

موضوع این تحقیق حفاظت از زیرساختهای حیاتی اطلاعاتی است که حفاظت از بخشی از مجموعه‌های زیرساخت حیاتی را مورد توجه و نظر قرار می‌دهد. در این چارچوب حفاظت از زیرساختهای حیاتی اطلاعاتی و زیرفضاهای اطلاعاتی، محدودهٔ تحقیق را شکل خواهد داد.

در این مقاله ابتدا به تعریف و تشریح حفاظت و زیرساختهای حیاتی در چارچوب محدودهٔ تحقیق یعنی امنیت اطلاعات و زیرساختهای حیاتی اطلاعاتی خواهیم پرداخت که سؤال اصلی، مربوط به چیستی حفاظت از زیرساختهای حیاتی اطلاعاتی می‌باشد.

در بخش دیگری به بررسی نظامها و ساختارهای مربوط به حفاظت از زیرساختهای حیاتی در کشورهای مدل خواهیم پرداخت. در این بخش ما نمونه‌های مناسبی را برای آشنایی با نظامها و ساختارهای درحال اجرا انتخاب و بررسی خواهیم کرد. سؤال اصلی در این بخش چگونگی طراحی و اجرای حفاظت از زیرساختهای حیاتی در کشورهای مدل می‌باشد.

در بخش سوم و پایانی به بررسی مقوله حفاظت از زیرساختهای حیاتی در جمهوری اسلامی پرداخته و تلاش خواهیم کرد تا الگوی اولیه را برای این منظور ارائه دهیم.

کالبدشکافی حفاظت از زیرساختهای حیاتی

مفهوم زیرساخت فضا و زیرفضا

زیرساختها، به‌طور کلی مجموعه‌ای از عناصر ساختاری به هم پیوسته‌ای است

که چارچوبی را برای پشتیبانی کردن از یک ساختار کلی ایجاد می‌کند. از سوی دیگر زیرساختها شبکه‌ای از سرمایه‌های فیزیکی و سیستمهایی است که مبنا، کار پایه، موتور حرکت و یا ظرف فعالیتهای اقتصادی، سیاسی، نظامی، اجتماعی، فرهنگی، صنعتی، علمی و تکنولوژیکِ افراد، گروه‌های اجتماعی، نهادها، سازمانها و دولت قرار می‌گیرد.

به بیان دیگر زیرساخت چارچوب اساسی یا ویژگیهای یک سیستم یا سازمان و تأسیسات و تجهیزات مورد نیاز برای انجامِ درستِ کارهای یک کشور می‌باشد. در مجموع با توجه به تعاریف ارائه شده زیرساخت دارای شاخصه‌هایی همچون؛ یک سیستم بزرگ؛ با ابعاد تکنولوژیک گسترده؛ دارای ابعاد فیزیکی غیرقابل حرکت و ارائه دهندهٔ خدمات پایه‌ای و اساسی می‌باشد.

تعریف زیرساخت به شبکه، خود کمک مؤثری در درک و فهم زیرساخت می‌نماید. شبکه مجموعه‌ای از نقاط اتصال یا گره‌های به هم پیوسته و با ساختار باز است که می‌تواند بدون هیچ محدودیتی گسترش یافته و نقاط شاخص جدیدی را در درون خود پذیرا شود البته تا زمانی که این نقاط توانایی ارتباط در شبکه را داشته باشند. با این تعریف شبکهٔ حمل و نقل، شبکهٔ راه‌ها، شبکهٔ آب، شبکه‌تلفن، شبکهٔ سوخت، شبکهٔ مالی، شبکهٔ اطلاع‌رسانی، شبکهٔ اینترنت، شبکهٔ ارتباط رادیویی، شبکه‌های اطلاعاتی و مواردی از این دست را می‌توان به عنوان زیرساخت معرفی نمود. برخی از این زیرساختها به صورت شبکه نمی‌باشند بلکه به صورت مجموعه هستند یعنی ویژگیهای یک مجموعه را دارند. مانند مجموعهٔ دانشمندان، مجموعهٔ دانشگاه‌ها و مجموعهٔ مراکز تحقیقاتی.

زیرساختهای شبکه‌ای دارای نقاط اتصال و خطوط می‌باشند. به طور مثال در شبکهٔ برق، نیروگاهها، نقاط اتصال و کابلها، خطوط انتقال می‌باشند. مجموعه‌ها نیز دارای اعضا می‌باشند. مانند مجموعهٔدانشگاهها که شامل دانشگاه تهران و دانشگاه صنعتی شریف و دیگر دانشگاهها به عنوان عضو می‌باشد.

در ذیل هر فضا و یا گره و نقاط اتصال نیز زیرفضاها و زیرمجموعه‌ها وجود

دارند که حلقه‌های اصلی و مرکز ثقل فضاها، گره‌ها و نقاط اتصال زیرساخت را تشکیل می‌دهند. به‌طور مثال شبکهٔ مالی یک زیرساخت، بانک ملی مرکزی یک نقطهٔ اتصال و یا گره و مخزن نگهداری اسکناس و شمش‌های طلا یک زیرمجموعه یا حلقه می‌باشد.

حلقه‌ها، زیرمجموعه‌ها و یا زیرفضاها در هر یک از فضاها یا نقاط اتصال متعلق به یک زیرساخت، به پنج دسته اصلی قابل تقسیم است. ما برای توضیح این مرحله از مفهوم زیرفضا ـ که بیشتر استفاده شده است ـ بهره می‌بریم.

اولین زیرفضا، زیرفضای سرمایه‌ای نام دارد. این زیرفضا شامل کلیهٔ سرمایه‌های منقول است که در یک مکان نگهداری می‌شود. این سرمایه‌ها در چرخهٔ کاری نهاد، سازمان، تأسیسات مربوطه به عنوان فضا یا نقاط اتصال نقشی ندارند. بلکه یا خروجی یعنی فراورده‌های تولیدی هستند و یا ورودی یعنی مواد اولیه جهت مصرف که به‌طور موقت نگهداری می‌شوند. و یا اینکه مواد آماده‌ای هستند که صرفاً برای مصرف برای مدتی نگهداری می‌شود. به‌طور مثال شبکهٔ حمل و نقل، یک زیرساخت است و بندر شهیدرجایی یک نقطهٔ اتصال یا گره در شبکه حمل و نقل می‌باشد. در این چارچوب محلهای نگهداری، کانتینرهای حامل کالا یک زیرفضای سرمایه‌ای محسوب می‌شود. آن هم از زیرفضاهای نوع سوم یعنی اینکه نه ماده اولیه است و نه خروجی و فراوردهٔ تولیدی. بلکه کالایی است که صرفاً به منظور انتقال برای مدتی در آنجا نگهداری می‌گردد.

دومین زیرفضا، زیرفضای تأسیسات و تجهیزات می‌باشد. این زیرفضا در چرخهٔ کار، ساختار و یا فرایند یک فضا یا نقطه اتصال و به طریق اولی در یک زیرساخت دارای نقشی اساسی است. به‌طور مثال زیرساخت شبکهٔ آب کشور دارای مجموعه‌ای از ساختها است که یکی از آنها سد کرج می‌باشد. در این ساخت یا نقطه اتصال، توربینها زیرفضای تأسیسات را تشکیل می‌دهد.

سومین زیرفضا، ساختمان و سازه‌های یک ساخت می‌باشند. سازه‌ها و ساختمان در واقع فیزیک یک ساخت را تشکیل می‌دهد. به‌طور مثال شبکهٔ تلفن کشور یک

زیرساخت و برج مخابراتی تهران یکی از حلقه‌های اتصال این شبکه و ساخت بوده و سازه و ساختمان این برج یک زیرفضا یا حلقه‌ای از این ساخت می‌باشد.

چهارمین زیرفضا، عوامل انسانی می‌باشند. در برخی از ساختها، عوامل انسانی از اهمیت به‌سزایی برخوردار بوده و در واقع سرمایه اصلی را تشکیل می‌دهند. این عوامل در چرخهٔ کار، ساختار یا فرایند یک ساخت از اهمیت بالایی برخوردار هستند. به‌طور مثال مجموعهٔ دانشمندان کشور یک زیرساخت، سایت هسته‌ای نطنز یک ساخت یا حلقه اتصال، دانشمندان فعال در این سایت یک زیرفضا می‌باشند.

پنجمین زیرفضا، زیرفضای تبادل اطلاعات می‌باشد. زیرفضای تبادل اطلاعات شامل اطلاعات و ارتباطات است و مواردی مانند رایانه‌ها، نرم‌افزارها، اینترنت، ماهواره‌ها، بانکهای اطلاعاتی، آرشیو اسناد و مدارک را شامل می‌شود.

زیرساخت حیاتی و امنیت ملی

مفهوم زیرساخت به‌طور طبیعی حکایت از نوعی تفکیک میان مجموعه‌ای از زیرساختها می‌کند که در یک تقسیم‌بندی کلی و حداقلی می‌توان به دو نوع زیرساخت حیاتی و غیرحیاتی تقسیم شود. بنابراین با این تقسیم‌بندی، قائل به این هستیم که اهمیت برخی از زیرساختها نسبت به برخی دیگر بیشتر است. با توجه به این تفکیک به نظر می‌رسد زیرساخت‌های حیاتی را می‌توان به زیرساخت‌های مرتبط با امنیت ملی یک کشور مرتبط نمود. تقریباً تمامی امور، مسائل و پدیده‌های حیاتی درون یک کشور مرتبط با امنیت ملی می‌باشد. این ارتباط نیز ناشی از گوهر امنیت است که ما را به مسئلهٔ وجود و یا عدم وجود مدلولهای خود و هر آنچه که وجود آنها را تهدید نماید، ارجاع می‌دهد.

بنابراین می‌توان بر اساس تقسیم سطوح امنیت به: امنیت فردی، امنیت جامعه‌ای[1]، امنیت دولت و امنیت کشور، به مصادیق زیرساخت‌های حیاتی نزدیک

1- Social Security

شد. در این چارچوب چنانچه حادثه امنیتی در یک زیرساخت موجب بروز ترس، دلهره و یا وحشت در تک‌تک افراد یک جامعه از به خطر افتادن جان و مال آنان گردد می‌توان آن زیرساخت را حیاتی نامید.

از سوی دیگر چنانچه جان جمع کثیری از افراد که در یک زمان و مکان مشخص و به صورت نوبه‌ای و مستمر تشکیل یک اجتماع یا جمعیت را می‌دهند بر اثر حادثهٔ امنیتی در یک زیرساخت به خطر افتد و یا حیات و چرخه فعالیت مجموعه‌ای از گروههای اجتماعی و یا سازمانهای (به معنای تخصصی کلمه) حرفه‌ای، صنفی و شغلی بر اثر حمله یا آسیب‌پذیری و در نتیجه حادثه امنیتی در زیرساخت دچار توقف و یا آسیب جدی گردد چنین زیرساختی را نیز می‌توان حیاتی تلقی نمود.

مورد سوم به سطح امنیت دولت برمی‌گردد. در این چارچوب چنانچه حادثهٔ امنیتی در یک زیرساخت منجر به تهدید علیه حیات یا چرخهٔ فعالیت نهادهای اساسی دولت، فیزیک دولت، و جریان ارتباطی دولت با بدنهٔ خود و احاد ملت گردد چنین زیرساختی حیاتی قلمداد می‌گردد. همچنین چنانچه یک زیرساخت خودش یک سرمایهٔ استراتژیک محسوب گردد و یا آسیب دیدن کلی آن منجر به مخاطرهٔ سرمایه‌های استراتژیک دولت گردد، سرمایه‌هایی که ارتباط وثیقی با تعهدات و تکالیف دولت نسبت به مردم کشور داشته و یا برای حیات خود دولت ضروری است، چنین زیرساختی نیز حیاتی تلقی می‌گردد.

در آخر برخی از زیرساخت‌ها، مرتبط با بقای یک کشور می‌باشند. به‌گونه‌ای که حادثهٔ امنیتی بر اثر حمله و یا آسیب‌پذیری چنین زیرساختی تمام سطوح امنیت یک کشور را در هم نوردیده و با تهدید مواجه نماید. چنین زیرساختهایی نیز حیاتی تلقی می‌گردند.

توضیحات ارائه شده تا حدودی می‌تواند مرز میان زیرساختهای حیاتی و غیرحیاتی را روشن کند اما از این تقسیم‌بندی نمی‌توان نتیجه گرفت که هر زیرساخت حیاتی، مربوط به یک سطح به خصوص از امنیت می‌باشد بلکه باید

گفت آسیب‌دیدگی و یا از کارافتادگی زیرساخت‌های حیاتی عمدتاً بر چند سطح از سطوح امنیت تأثیر خواهد گذاشت و کمتر زیرساختی است که تبعات آسیب‌دیدگی آن صرفاً متوجه یکی از سطوح امنیت شود.

تعاریف زیرساخت حیاتی

در اولین گام باید مشخص شود که به چه چیزهایی زیرساخت‌های حیاتی[1] اطلاق می‌شود، در پاسخ به این سؤال ابتدا می‌توان تعاریفی که تاکنون از این مفهوم ارائه شده را مورد بررسی قرار داد.

دیکشنری امریکن هریتیج[2]، در تعریف زیرساخت به تسهیلات، خدمات و تأسیسات مورد نیاز یک جامعهٔ کارآمد از جمله سیستم‌های حمل و نقل و ارتباطات، آب، برق و مؤسسات عمومی، از جمله مدارس، دفاتر پستی و زندان‌ها اشاره می‌کند. (Moteff & Parfomark, 2004, 2)

در دستورالعمل اجرایی حمایت از زیربناهای حیاتی در سال ۲۰۰۱ که توسط رئیس‌جمهور وقت آمریکا منتشر شده است زیرساخت‌های حیاتی به تجهیزات، امکانات و خدمات تولید، تبدیل و توزیع برق، مخابرات و ارتباط از راه دور، تجهیزات و امکانات تولید، استفاده، ذخیره و انهدام مواد و انرژی هسته‌ای؛ سیستم‌های اطلاعاتی دولتی و خصوصی؛ حمل و نقل اعم از راه‌آهن؛ بزرگراه‌ها، بنادر و راه‌های آبی، فرودگاه‌ها و هواپیماها؛ دامداری، کشاورزی و سیستم‌های تهیهٔ آب و غذا برای استفاده و مصرف انسان گفته شده است. (Ibid, p.6)

در یک تعریف دیگر که در سند استراتژی ملی دولت بوش برای حمایت فیزیکی از زیربناهای حیاتی و دارایی‌های کلیدی که در سال ۲۰۰۳ منتشر شده، دارایی‌ها و منابع کلیدی به سه دسته تقسیم گردیده‌اند. در دستهٔ اول، طیف متنوع و گسترده‌ای از بناها، نمادها و مظاهر ملی که نمایانگر میراث، سنن و ارزشهای ملی و قدرت سیاسی می‌باشد آمده است. مانند بناهای تاریخی، نمادهای فرهنگی

1- Cirital Infrastructure
2- The American Heritage Dictionary

و مراکز دولتی و تجاری. در دستهٔ دوم، تسهیلات و ساختارهایی که نمایانگر قدرت اقتصادی و پیشرفت‌های تکنولوژیک است از جمله؛ مراکز تجاری، دفاتر و ساختمانهای اداری و استادیوم‌های ورزشی آورده شده است. در بخش سوم، تمامی مکانهای عمومی که گردآوردندهٔ بخش اعظمی از مردم جهت اجرای فعالیتهای تجاری، بازرگانی و شغلی، خرید یا تفریح می‌باشد، آمده است. (Homeland, 2002, 30)

دولت انگلیس در گزارشی که تحت عنوان: "محافظت از زیرساخت‌های حیاتی در کشور بریتانیا" منتشر کرده است. (www.mio.gov.uk-134) زیرساختهای ملی حیاتی کشور را قسمتی از زیربناهای کشور می‌داند که تداوم صحیح و مداوم آنها برای کشور حیاتی و از کارافتادگی، تأخیر طولانی در خدمات‌رسانی، قطع خدمات و یا خدمات‌رسانی ناصحیح آنها موجب لطمات جدی به بدنهٔ اقتصادی و اجتماعی گردیده و پیامدهای سنگینی برای دولت و جامعه در پی داشته و باعث بروز تهدیدات بالقوه و بالفعل برای کشور می‌شود. دولت انگلستان بر اساس این تعریف بخشهای حیاتی خود را به ۱۰ قسمت اصلی و ۳۹ قسمت فرعی تقسیم می‌نماید که عبارتند از:

- ارتباطات (دیتا، مخابرات و تلفن، پست، اطلاعات ملی و بی‌سیم)
- خدمات اورژانسی (آمبولانس، آتش‌نشانی، پلیس و خدمات دریایی)
- منابع انرژی (الکتریسیته، گاز طبیعی و نفت)
- مالیات (مدیریت دارایی، امکانات مالی، سرمایه‌گذاری بانکی، بازار و بانکداری جزیی)
- غذا (تولید، واردات، فرآیند، توزیع و خرده‌فروشی)
- دولت و خدمات عمومی و ملی (دولت مرکزی، دولت ایالتی، دولت محلی، پارلمان‌ها و مجلس‌های قانونگذاری، دادگستری و امنیت ملی)
- خطر و ایمنی ملی (تروریسم شیمیایی، بیولوژیکی، رادیولوژی و اتمی

(CBRN)[1]: حوادث اجتماعی

- بهداشت (مراقبت بهداشتی و بهداشت عمومی)
- حمل و نقل (هوایی، دریایی، راه‌آهن و جاده)
- آب (آب مرکزی و فاضلاب)

در کشوراسترالیا زیرساختهای حیاتی، بخشهای بحرانی کشور معرفی گردیده و گفته می‌شود که بخشهای بحرانی، بخشهایی هستند که آسیب‌دیدگی آنها تأثیر بسیار شدیدی بر مسائل اجتماعی، اقتصادی و امنیت ملی دارد. بر همین اساس بخشهای بحرانی و به طریقی اولی زیرساختهای حیاتی در استرالیا موارد ذیل تعریف گشته‌اند:

- ارتباطات (تلفن، فاکس، اینترنت، کابل و ماهواره‌ها و ارتباطات الکترونیکی)
- انرژی (گاز، سوخت نفتی، پالایشگاه، لوله‌کشی، تولید الکتریسیته و انتقال آن و راکتورهای هسته‌ای)
- سرمایه (بانکداری، بیمه و تبادلات تجاری)
- غذا (تولید انبوه، ذخیره‌سازی و پخش)
- بخشهای دولتی (سیستم‌های جاسوسی و دفاعی، ساختمانهای مجلس، بخشهای کلیدی دولت، محلهای اقامت مقامات، خدمات اورژانس مانند آمبولانس و آتش‌نشانی)
- سلامتی (بیمارستانها، سلامت عمومی، تحقیق و توسعه لابراتورها)
- صنایع (صنایع سنگین و شیمیایی)
- موارد ملی (ساختمانهای فرهنگی، ورزشی و گردشگری)
- ترابری (کنترل ترافیک هوایی، زمینی، دریایی و راه‌آهن)
- صنایع دفاعی (صنایع دفاع و شیمیایی)

در جمع‌بندی تعریف و تشریح زیرساختهای حیاتی می‌توان گفت: زیرساختهای

1- Chimical, Biological, Radiological, Nuclear Terrorism

حیاتی مجموعه عناصر ساختاری به هم پیوسته‌ای است که یک سیستم بزرگ را تشکیل داده، دارای ابعاد تکنولوژیک گسترده بوده، از ابعاد فیزیکی غیرقابل حرکت برخوردار است و ارائه دهندهٔ خدمات اساسی و چارچوبی برای پشتیبانی از ساختارهای کلان امنیت ملی کشور در سطوح امنیت کشور، امنیت دولت، امنیت جامعه و امنیت افراد و احاد ملت می‌باشد.

زیرساختهای حیاتی اطلاعاتی

همان‌طور که در تعاریف روشن گردید زیرساختهای حیاتی به دسته‌های مختلف تقسیم می‌شود یکی از این مجموعه‌ها زیرساخت‌های حیاتی اطلاعاتی (CII)[1] می‌باشند. این زیرساختها بر پایه و بنیان فضای تبادل اطلاعات قرار دارند و در واقع زیرساختهای مربوط به "فضای تبادل اطلاعات (فتا)" می‌باشند.

منظور از "فضای تبادل اطلاعات" مجموعه عوامل درگیر در تولید، ثبت، بازیابی، پردازش و انتقال اطلاعات شامل؛ تجهیزات پردازشی، تجهیزات راهگزینی و اتصال‌دهی شبکه‌ها، کانال‌های ارتباطی، نرم‌افزارهای سیستمی و کاربری و عوامل انسانی راهبر و کارگزار می‌باشد.

زیرساخت‌های حیاتی اطلاعاتی مانند سایر زیرساختهای حیاتی به فضاها وزیرفضاها تقسیم‌بندی می‌شود. در این چارچوب زیرفضا، تأسیسات و تجهیزات، پایگاه‌های داده‌ها، فضاهای انتقال، عوامل انسانی راهبر و کارگزار و برنامه‌هایی می‌باشد که فضا، عملکرد خود را حول محور آن تنظیم می‌نماید.

برخی از فضاها و زیرفضاهای حیاتی اطلاعاتی مربوط به سایر زیرساخت‌ها است یعنی زیرساخت‌های حیاتی غیراطلاعاتی اما به جهت اهمیت زیرساخت در سطح حیاتی، فضا و زیرفضای اطلاعاتی آن مورد توجه قرار می‌گیرد.

آنچه در این مقاله از این به بعد مورد توجه قرار خواهد گرفت زیرساخت‌های حیاتی اطلاعاتی و فضاها و زیرفضاهای حیاتی اطلاعاتی مربوط به زیرساختهای

1- Critical Information Infrastructure

حیاتی غیراطلاعاتی می‌باشد.

حفاظت از زیرساخت‌های حیاتی اطلاعاتی

حفاظت[1] مترادف با ایمن‌سازی است و ایمن‌سازی مجموعه اقداماتی است که برای تبدیل شرایط موجود به شرایط امن و یا مراقبت از تداوم شرایط امن صورت می‌گیرد.

حفاظت از زیرساخت‌های حیاتی اطلاعاتی و همچنین حفاظت از زیرفضاهای حیاتی اطلاعاتی مربوط به سایر زیرساخت‌های حیاتی‌یی که در این تحقیق موردنظر ما می‌باشد به دو بخش اصلی؛ حفاظت فیزیکی و حفاظت فضای رایانه تقسیم می‌شود.

حفاظت فضای رایانه‌ها به معنای ایمن‌سازی صحت[2] و محرمانگی[3] منابع و داده‌های فضای رایانه‌ای می‌باشد. در حالی که حفاظت فیزیکی بخشی از فرایند خارجی ایمن‌سازی فضای رایانه‌ای است و مربوط به حفاظت بیرونی و خارجی از تجهیزات، سخت‌افزار، اماکن استقرار رایانه‌ها و شبکه‌های اطلاعاتی می‌باشد.

برخی حفاظت فیزیکی از زیرساختهای اطلاعاتی و زیرفضاهای اطلاعاتی مربوط به سایر زیرساختها را در شمول حفاظت از امنیت فضای رایانه‌ای قرار نمی‌دهند. (Denning, 1979, 227-249) در حالی که برخی دیگر آن را بخشی از فرایند ایمن‌سازی یک فضای رایانه‌ای می‌دانند. (Herman, 2008)

پس از روشن شدن محدودهٔ زیرساختهای موردنظر که ما در این مقاله همانا زیرساختهای حیاتی اطلاعاتی و زیرفضاهای حیاتی اطلاعاتی مربوط به سایر زیرساختها می‌باشد. با توضیحات مطروحه در خصوص حفاظت، اکنون روشن است که ما در این مقاله به حفاظت فضای تبادل اطلاعات خواهیم پرداخت. بنابراین حفاظت فیزیکی، زیرساختهای حیاتی اطلاعاتی و زیرفضاهای حیاتی

1- Protection
2- Integrity
3- Confidentiality

اطلاعاتی در این مقاله موردنظر ما نمی‌باشد.

ارکان حفاظت

حفاظت از فضای رایانه‌ای همان‌طور که گفته شد دارای دو رکن اساسی صحت و محرمانگی می‌باشد. قبل از آنکه این دو مفهوم اساسی را توضیح دهیم این سؤال را باید پاسخ داد که صحت و محرمانگی چه چیزهایی در فضای رایانه‌ای باید حفاظت یا ایمن گردد؟ پاسخ این سؤال دو عامل منابع و داده‌ها می‌باشد. منابع، کلیهٔ اجزای فضای رایانه‌ای را شامل می‌شود که در شبکه دارای نقش و وظیفهٔ بخصوصی هستند. و داده‌ها، اجزایی هستند که در سیستم مورد پردازش قرار می‌گیرند. برای منابع مواردی مانند دیسکت سخت، دستگاه کارت‌خوان، پردازنده‌های سیستم عامل، نرم‌افزار سرویس‌دهندهٔ شبکه را می‌توان نام برد و برای داده‌ها محتوای فایلهای اطلاعاتی و پایگاههای اطلاعاتی را می‌توان مثال زد. (http//seclab.cs.edu)

با روشن شدن مرجع صحت و سلامتی که منابع و داده‌ها می‌باشد، می‌توان حفاظت از فضای رایانه‌ای را به حفاظت از صحت و محرمانگی منابع، داده‌ها و اطلاعات ارجاع داد.

منظور از صحت در واقع سلامتی است. یعنی سلامتی منابع و داده‌ها و در یک تعریف دقیق‌تر درخصوص صحت منابع باید گفت که یک منبع هنگامی صحیح شمرده می‌شود که کارکرد آن دقیقاً مطابق با رفتار مورد انتظار باشد، بر این اساس صحت و یا سلامتی منابع از طریق؛ جذب، تغییر و افزودن موارد زائد به آن و یا نقض یکپارچگی آن تهدید می‌شود. (http//cisr.nps.havy.mil)

صحت داده‌ها[1] صرفاً از طریق اطمینان‌پذیری از منشأ اطلاعات، مورد ارزیابی قرار می‌گیرد. بنابراین چنانچه معلوم گردد داده‌های دریافتی دقیقاً همان داده‌هایی است که از منشأ ارسال شده این اطلاعات مهم ارزیابی می‌شود. لذا در اینجا

1- Data integrity

درستی محتوای داده‌ها مطرح نمی‌باشد بلکه انطباق آنچه ارسال شده با آنچه دریافت شده مدنظر است. (Ibid)

رکن دوم حفاظت، محرمانگی است. محرمانگی، در برابر افشا و آشکار شدن قرار دارد و محرمانگی، بیشتر در خصوص داده‌ها مطرح است تا منابع. البته برخی از منابع مانند نصب نرم‌افزار فایروآل جزو منابع پنهان می‌باشد و باید محرمانه بماند.

سیستمهای حفظ و محرمانگی به سه دستهٔ پنهان‌کاری[1]، اختفا[2] و سیستمهای حقیقی محرمانگی[3] تقسیم می‌شود. در سیستم پنهان‌سازی وجود داده‌ها یا منابع از دید حریف مخفی نگه داشته می‌شوند مانند انتقال داده‌ها از طریق نامرئی‌نویسی، در سیستم اختفا، داده یا منبع در پوششهای دیگر قرار می‌گیرد. مانند انتقال صدا اما از طریق تحریف صدا و یا قراردادن یک فایل پنهانی در درون سایر متن‌های عادی. در سیستم‌های حقیقی محرمانگی داده‌ها یا منابع در دسترس است اما آن داده یا منبع به‌صورت رمز درآمده و دسترسی به‌آن منوط به‌شکستن رمز است. (Shamon, 656-715)

ایمن‌سازی

مهم‌ترین سؤال در این بخش آن است که حد ایمن‌سازی در کجا قرار دارد؟ به عبارت دیگر حفاظت و ایمن‌سازی فضای تبادل اطلاعات در چه مرحله‌ای باید صورت گیرد؟

ایمن‌سازی در سه وضعیت قابل برنامه‌ریزی است، وضعیت اول، *ظهور تهدید* است یعنی با تمرکز بر روی تهدیدات صورت گرفته و مواردی مانند شدت، عمق، جهت و هدف آن، برنامه‌ریزی جهت ایمن‌سازی و یا حفاظت در این نقطه انجام خواهد شد. وضعیت دوم، *حمله* نام دارد. یعنی زمانی که تهدید به فعلیت درمی‌آید و مهاجم اقدام به حمله می‌نماید. وضعیت سوم، حادثهٔ امنیتی[4] نامیده

1- Concealment
2- Privacy
3- True Secrecy
4- Security incident

می‌شود. در این وضعیت، تهدید به فعلیت درآمده و بر اثر آن ظرفیت فضای تبادل اطلاعات صدمه دیده است. حادثهٔ امنیتی، رویدادی که نتیجهٔ آن اختلال و آسیب‌دیدن سیستم است.

حادثهٔ امنیتی از دو منبع ناشی می‌شود؛ اول حمله توسط مهاجم و دیگری ناشی از آسیب‌پذیری سیستم. حمله از چهار بخش تشکیل می‌شود: ۱ـ استفاده از مجموعه‌ای از ابزار بر اساس استفاده از آسیب‌پذیریهای سیستم و با روش خاص، به منظور هدف قرار دادن یک یا مجموعه‌ای از عناصر سیستم. چنانچه این اقدام به نتیجه منتج شود؛ حادثهٔ امنیتی رخ داده است. در فضای تبادل اطلاعات حادثهٔ امنیتی وقتی رخ می‌دهد که نفوذ به سیستم اتفاق افتاده باشد.

آسیب‌پذیری، نقص یا ضعف در طراحی، پیاده‌سازی و کارکرد یا مدیریت سیستم نامیده می‌شود که در پاره‌ای موارد این آسیب‌پذیری مورد استفاده حمله‌کننده قرار می‌گیرد و گاهی نیز آسیب‌پذیری بدون فاعل منجر به حادثهٔ امنیتی می‌گردد.

با توجه به این سه وضعیت، دو رویکرد حفاظتی قابل تشخیص است. رویکرد اول *ایمن‌سازی پیشینی* نام دارد که بر طبق آن پیش از وقوع هرگونه خطری باید تمام راه‌های محتمل بر روی آن بسته شود و از تمامی امکانات و ابزارها برای ایجاد مانع و سد به منظور عدم وقوع خطر استفاده گردد. این رویکرد منطبق بر وضعیت ظهور تهدید و حمله می‌باشد. یعنی مبنا را بر دفع تهدید و منصرف کردن حریف از تهدید و یا به بن‌بست کشاندن حمله قرار می‌دهد.

رویکرد دوم، *ایمن‌سازی پسینی* نام دارد. این رویکرد خطرات و تهدیدات را مادام که بالفعل نشده نادیده می‌گیرد و مبنای خود را وقوع حادثهٔ امنیتی قرار می‌دهد. یعنی مشاهدهٔ شواهد یک حادثهٔ امنیتی. وقتی چنین علائمی مشاهده شد، سیستم حفاظتی به‌طور واکنشی دست به کار شده و از صدمه دیدن امنیت فضای تبادل اطلاعاتی جلوگیری می‌کند. بنابراین مبنای این رویکرد، جلوگیری از به فعلیت درآمدن تهدید و حمله نمی‌باشد بلکه پس از آنکه حمله به وقوع پیوست، مبنای خود را به شکست کشاندن آن حمله قرار می‌دهد.

حال با توجه به وضعیتهای سه‌گانه و رویکرد دوگانهٔ ایمن‌سازی، به پاسخ سؤال اصلی این بخش یعنی حد ایمن‌سازی نزدیک می‌شویم، بدیهی است ایمن‌سازی باید معقول، مقرون به صرفه و منتج به موفقیت باشد. لذا ضرورتی ندارد که به ایمن‌سازی مطلق اندیشید. زیرا نبایستی هزینه‌های ایمن‌سازی از اصل آنچه که باید حفاظت شود بیشتر گردد. بنابراین هدف ایمن‌سازی را باید رسیدن به شرایط "اطمینان"[1] تعریف کرد.

در شرایط اطمینان اگرچه احتمال دارد مهاجم در حملهٔ خود موفق گردد و یا مدافع در شکست دادن حمله ناکام بماند اما بر اساس شرایط موجود و به دلیل وجود میزانی از اطمینان، اقدامات انجام شده کافی تلقی می‌شود.

تعیین حد اطمینان و حد ایمن‌سازی بر اساس میزان ریسک محاسبه می‌شود. و هرگاه میزان ریسک در حد قابل قبولی قرار داشته باشد، اقدامات انجام شده برای ایمن‌سازی حد مطلوب ارزیابی خواهد شد. در این چارچوب میزان ریسک را می‌توان به صورت حاصل ضرب احتمال موفقیت یک حمله در مقدار خسارت آن محاسبه نمود. (Blakley, 2001, 97-104)

روشهای ایمن‌سازی: روشهای ایمن‌سازی یا حفاظت، در خصوص صحت و محرمانگی داده‌ها و منابع مطرح می‌گردند. در این میان مثلاً برخی از روشها بیشتر درخصوص صحت‌منابع و برخی‌دیگر درخصوص محرمانگی داده‌ها کاربرد دارند.

اولین روش که بیشترین کاربرد آن در خصوص محرمانگی داده‌ها و منابع می‌باشد، *سیستم تشخیص نفوذ*[2] نام دارد که بیشتر به صورت یک طعمه عمل می‌کند. این سیستم اغلب آسیب‌پذیر و بی‌دفاع می‌باشد و بیشتر برای فریب مهاجم و مشغول داشتن او به یک سیستم انحرافی طراحی می‌گردد.

روش دوم، بیشتر مرتبط با صحت داده‌ها است. این روش، *تصدیق هویت*[3]

1- assurance
2- Intrusion Detection System
3- Authentication

نام دارد. تصدیق هویت به معنای آن است که با استفاده از مکانیسم خاصی، از هویت یک موجود اطمینان حاصل می‌شود. تصدیق هویت روشی برای تشخیص صحت اطلاعات هویتی ارسال‌کنندهٔ اطلاعات می‌باشد.

روش سوم، *کنترل دسترسی*[1] نام دارد. از این روش هنگامی استفاده می‌شود که مدیریت کل فضای تبادل اطلاعات در اختیار ما باشد. این روش به عنوان یک سازوکار مراقبت از دسترسی‌های مستقیم و جلوگیری از دسترسی‌های غیرمجاز به فتا را برعهده دارد. در این سازوکارها، یک مرجع کنترلی. با واسطه شدن و مراقبت از تمامی دسترسی‌های صورت گرفته در یک حوزه، بر اساس مقررات تعیین شده، دسترسی‌ها را پیش از انجام ارزیابی می‌کند و تنها به دسترسیهای مجاز امکان ورود می‌دهد.

روش چهارم، *نهان‌نگاری*[2] نام دارد. این روش بیشتر برای محرمانگی داده‌ها مورد استفاده قرار گرفته و تلاش دارد تا با پنهان کردن داده‌های محرمانه در دل توده‌ای از داده‌های عادی، محرمانگی داده‌های محرمانه را حفظ کند.

روش پنجم، *رمزنگاری*[3] است. در این روش ، ظاهر نمایش داده‌ها به شکل خاصی است که فقط برای افرادی که کلید آن را در اختیار دارند قابل خواندن می‌باشد. این روش یکی از مرسوم‌ترین و مناسب‌ترین روشهای حفظ محرمانگی داده‌ها می‌باشد.

روش ششم، *کنترل جریان اطلاعات*[4] می‌باشد. در این روش به دنبال کنترل نقل مکان اطلاعات در فضا می‌باشد. در حقیقت این روش به دنبال آن است که مستقل از کنترل دسترسی‌ها، از تغییراتی که در اطلاعات منتقل گردیده ایجاد می‌شود، جلوگیری نماید. بنابراین در این روش دسترسی به ظرف نگهداری

1- Access Control
2- Steganography
3- Cryptography
4- Information Flew Control

اطلاعات[1] کنترل می‌گردد.

سیاست‌های امنیتی

سیاست امنیتی دقیقاً بر اساس حد ایمن‌سازی ضروری و لازم می‌آید. در ایمن‌سازی و برآورد ریسک، صرفاً از متغیرهای کمّی استفاده نخواهد شد و بسیاری از متغیرهای کیفی و عناصر نسبی و اعتباری در این زمینه مؤثر و مطرح می‌باشند. در واقع با تعیین مجموع پارامترها و متغیرهاست که می‌توان سطح قابل اطمینان تأمین امنیت و ایمن‌سازی در یک حوزه معین را مشخص کرد. مثلاً اینکه چه دارایی‌هایی با ارزش هستند و امنیت آنها مهم است، کدام دارایی‌ها محرمانه هستند و چه کسانی تا چه حد می‌توانند به آن دسترسی داشته باشند، هزینهٔ ریسک قابل تحمل چه مقدار است. اینها نمونه‌هایی از عناصر قراردادی و اعتباری است که تعیین وضعیت نسبت به هریک از آنها در قالب مجموعه‌ای تحت عنوان سیاستهای امنیتی گنجانده می‌شود.

سیاستهای امنیتی مشخص می‌کند که پارامترهای متغیر و نسبی موجود در ایمن‌سازی، در یک حوزهٔ خاص چگونه هستند و در یک کلام، سیاست امنیتی میان انتظارات و ضوابط امنیتی در یک حوزهٔ خاص چگونه می‌باشد. به‌طور مثال در حوزهٔ زیرساخت‌ها و زیرفضاهای مربوط به تبادل اطلاعات، سیاست امنیتی فایروال به معنای قواعدی است که تعیین می‌کند که کدام بسته‌ها باید از فایروال عبور داده شوند و کدام یک مجاز به عبور نیستند. (Honc, 402-409) این نوع سیاستها در مجموعهٔ سیاستهای کنترل دسترسی قرار می‌گیرند.

سیاست امنیتی در واقع تعیین‌کنندهٔ حدود و معیارهای حفاظت می‌باشد. هدف از تدوین سیاستهای امنیتی آن است که کاربران، کارمندان و مدیران نسبت به حدود و معیارها و ضوابط مربوط به کارها و فعالیتهای ایمن‌سازی دارایی‌های اطلاعاتی آشنا گردند و بدانند انجام فعالیتها، برنامه‌ها و اهداف باید در چه چارچوبی دنبال شود.

1- Information Container

سیاستهای امنیتی در زیرساخت‌ها و فضاهای حیاتی تبادل اطلاعاتی را در سه سطح می‌توان دسته‌بندی نمود: سیاستهای امنیتی برنامه‌ریزی، سیاستهای موضوعات خاص و سیاستهای سیستمی.

سیاستهای امنیتی در سطح برنامه‌ریزی برای ایجاد بازسازی برنامه‌های ایمن‌سازی تدوین می‌گردند. سیاستهای سطح موضوعات خاص آن دسته از سیاستهایی هستند که تنها در یک حوزهٔ خاص که در مقطع زمانی موردنظر مورد توجه قرار گرفته تمرکز می‌یابند. چنین تمرکزی از ظهور فناوریهای جدید در سیاستهای جدید دولت و بروز حوادث جدید در یک حوزهٔ خاص ناشی می‌شود، و در آخر سیاستهای سطح سیستمی سیاستهایی هستند که تنها در حوزهٔ یک سیستم خاص از کل سازمان کاربرد دارند.

حفاظت از زیرساخت‌های حیاتی اطلاعاتی در کشورهای مدل

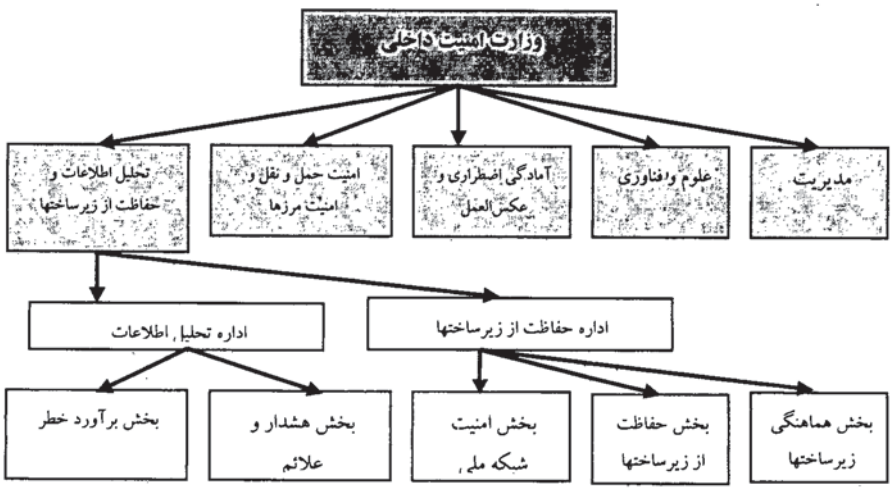
الف) آمریکا

ساختار و سازمان: کشور آمریکا در زمینهٔ فناوری اطلاعات و ارتباطات و به‌ویژه امنیت اطلاعات و ارتباطات، یکی از کشورهای پیشرو محسوب می‌شود که دارای ساختارها، سازمانها و فرایندهای گسترده و پیچیده‌ای در این خصوص می‌باشد و پس از حادثه ۱۱ سپتامبر ۲۰۰۱ نیز آنها را مورد بازنگری جدی و اساسی قرار داد. به‌طوری که تا قبل از این سازمانها و نهادهای متعدد و تقریباً مستقلی در این زمینه‌ها فعالیت می‌کردند اما در حال حاضر بخش عمده‌ای از ساختارها، سازمانها و فرایندهای مربوطه در داخل یک تشکیلات جدید تحت عنوان وزارت اطلاعات امنیت داخلی (DHS)[1] سازماندهی گردیده است.

وزارت امنیت داخلی از پنج بخش اصلی شامل: مدیریت، علوم و تکنولوژی؛ پاسخگویی و آماده‌سازی در موارد اضطراری؛ امنیت مرزها و ترابری؛ تحلیل اطلاعات و محافظت از زیرساختها تشکیل شده که بخش مرتبط با فضای تبادل

1- Department of Homeland Security

اطلاعات و در واقع مهم‌ترین بخش مرتبط با موضوع مقاله یعنی بخش تحلیل اطلاعات و محافظت از زیرساخت‌ها (IAIP) [1] می‌باشد و این بخش از دو اداره تحلیل اطلاعات (IA) و اداره محافظت از زیرساختهای حیاتی (IP) تشکیل گردیده است. در چارچوب IAIP دو برنامهٔ عمده سازماندهی گردید ه که برنامهٔ امنیت اطلاعات [2] و برنامهٔ حفاظت از زیرساختهای اطلاعاتی حیاتی [3] نام دارند. (www.dhs.gov)



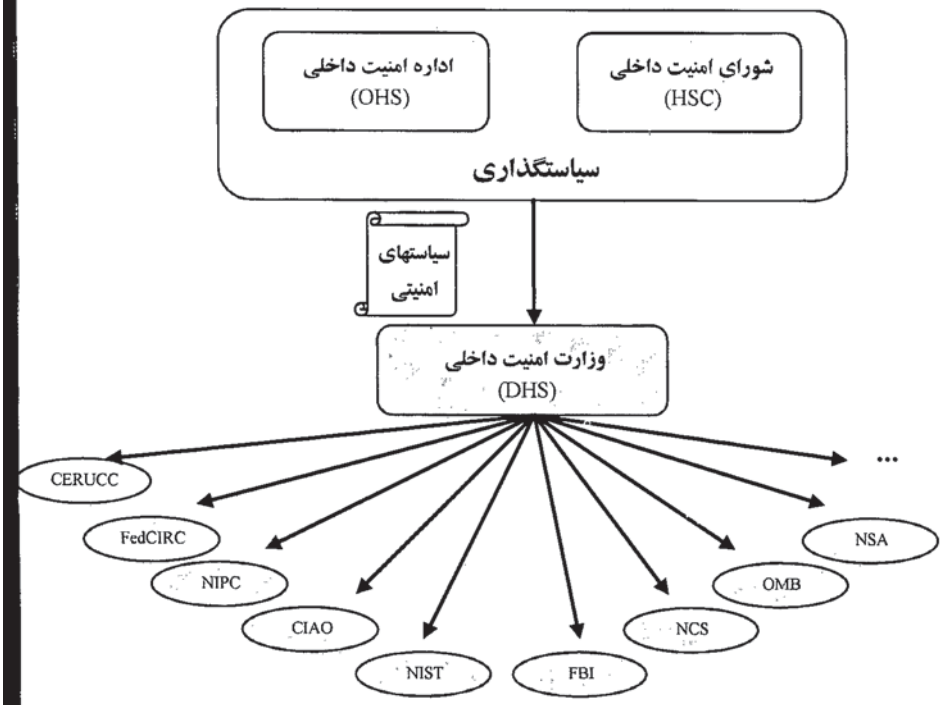
شکل (۲): ساختار وزارت امنیت داخلی آمریکا

۱ـ (Information Analysis and Infrastructure Protection: IAIP) یکی از ۵ بخش دپارتمان امنیت کشور امریکا است. مسئولین این بخش شناسایی و ارزیابی تهدیدات جاری و آینده و نیز آسیب‌پذیری‌های کشور، هشدارهای به موقع و عملکردهای جلوگیری کننده و حفاظتی است. به‌طور خاص می‌توان گفت که بیشترین توجه این بخش بر روی حفاظت ساختارهای حیاتی و امنیت فضای سایبر است. علاوه بر این وظیفهٔ هماهنگی فعالیتها در جهت حفظ ساختارهای ملی و ایجاد ارتباط فعال با بخش خصوصی را نیز دارد. همچنین IAIP وظیفهٔ تحلیل اطلاعات به دست آمده از منابع مختلفی را به عهده دارد که این منابع شامل FBI ، CIA، آژانس جاسوسی دفاع و آژانس امنیت ملی می‌شوند.

2- Information Security (InfoSec)

3- Critical Information Infrastructure Protection (CIIP)

سیاستگذاری برنامه‌های مربوط به InfoSec در بخش IAIP توسط دو نهاد مستقل به نام، ادارهٔ امنیت داخلی (OHS)[1] و شورای امنیت داخلی (HSC)[2] انجام می‌شود. در این چارچوب OHS مسئولیت طراحی و هماهنگی کلیهٔ فعالیتها و سازمانهای دولتی به منظور اجرای استراتژی ملی محافظت از کشور آمریکا را در مقابل تهدیدات و حملات تروریستی برعهده دارد. همچنین HSC مشاور رئیس جمهور در امر سیاستگذاری و هماهنگی سازمانها و آژانسهای دولتی در اجرای سیاستها در کلیهٔ زمینه‌های فعالیت وزارت امنیت داخلی می‌باشد. (Ibid)



شکل (۳) : سازماندهی برنامهٔ امنیت اطلاعات آمریکا

1- Office of Homeland Security (OHS)
2- Homeland Security Council (HSC)

علاوه بر سیاستگذاری مستقل مربوط به InfoSec سیاستگذاری مربوط به CIIP از بخش IAIP نیز به صورت مستقل اما برخلاف مورد قبلی به صورت متمرکز انجام می‌شود. یعنی از همکاری دیگر سازمانهای دولتی برای سیاستگذاری استفاده نمی‌شود. با این وجود اجرای برنامه‌ها توسط دستگاههای متولی زیرساختهای حیاتی انجام خواهد شد ولی تحلیل مدیریت و مخاطرات مربوط به این برنامه توسط IA[1] انجام خواهد گرفت.

با توجه به متمرکز بودن سیاستگذاری، شورایی تحت عنوان، شورای مشورتی زیرساخت ملی (NIAC)[2] مسئولیت سیاستگذاری مربوط به CIIP را برعهده دارد. این شورا زیر نظر رئیس جمهور سیاستگذاری پیرامون زیرساختهای حیاتی در عرصه‌های مختلف را نجام می‌دهد. این شورا ۳۰ عضو دارد که توسط شخص رئیس جمهور و از میان خبرگان بخش خصوصی، دولت مرکزی، دولتهای محلی، دانشگاهها انتخاب می‌گردند.

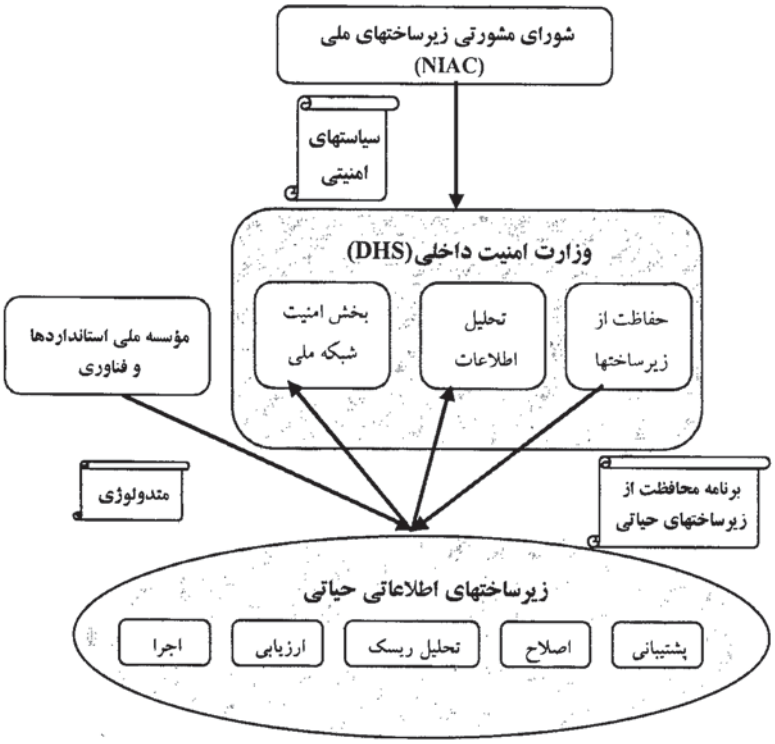
مسئولیتهای این شورا عبارتند از:

- پیشنهاد و توسعه راههایی برای تشویق خصوصی به انجام ارزیابی خطرها به‌طور متناوب ؛
- گسترش و نظارت بر مراکز تحلیل و تسهیم اطلاعات (ISAC)[3] در بخشهای خصوصی[4]؛
- هماهنگ‌کنندهٔ ISAC ها.

زیرساخت‌های حیاتی: آمریکا دارای بخشهای مهم و حساسی می‌باشد. مهمترین بخشها که در چارچوب زیرساخت‌های حیاتی آمریکا گنجانده شده‌اند عبارتند از:

1- Information Analysis
2- National Infrastructure Advisory Council (NIAC)
3- Information Sharing and Analysis Center
۴ـ وظیفهٔ ISAC ها جمع‌آوری و پخش اطلاعات، رویدادها و پاسخ‌دهی به آن از طریق اعضای آن و تسهیل تبادل اطلاعات مابین دولتو بخش خصوصی می‌باشد.

کشاورزی؛ غذا؛ آب؛ سلامتی؛ خدمات اضطراری؛ دولت، بنیانهای صنعتی دفاع؛ ارتباطات و اطلاعات؛ انرژی؛ ترابری؛ سرمایه‌گذاری و بانکداری؛ صنعت شیمیایی؛ پست و حمل و نقل. (Homeland, 2002, 41)



شکل (٤) : سازماندهی برنامه محافظت از زیرساختهای اطلاعاتی حیاتی آمریکا

طرح‌ها و استراتژی‌ها: حفاظت از زیرساخت‌های حیاتی اطلاعاتی که به عنوان یک برنامه در بخش توضیحات آن داده شد، در قالب یک طرح استراتژیک تحت عنوان؛ طرح ملی برای محافظت از سیستم‌های اطلاعاتی به مرحلهٔ اجرا درمی‌آید. (White House, 2003, 13-14)

این طرح دارای سه فصل و ده برنامه به شرح زیر است:

● **آماده سازی و پیشگیری :**

برنامهٔ اول: شناسایی داراییهای زیرساختهای حیاتی، وابستگی‌ها و تشخیص آسیب‌پذیری‌ها.

برنامهٔ دوم: تشخیص حملات و نفوذهای غیرمجاز؛

برنامهٔ سوم: ایجاد و توسعه سیستم‌های اطلاعاتی و مجری قانون؛

برنامهٔ چهارم: به اشتراک‌گذاری سریع هشدارهای حملات؛

برنامهٔ پنجم: تهیهٔ امکانات لازم جهت پاسخ، نوسازی و بازیافت؛

● **تشخیص و مقابله :**

برنامهٔ ششم: توسعهٔ بخش تحقیقات و توسعه؛

برنامهٔ هفتم: آموزش و استخدام متخصصین امنیت ـ اطلاعاتی؛

برنامهٔ هشتم: آگاهی‌رسانی به مردم آمریکا نسبت به نیاز به بهبود امنیت فضای تبادل اطلاعات؛

برنامهٔ نهم: وضع قوانین مقتضی برای پشتیبانی مناسب از برنامه؛

برنامهٔ دهم: در هر بند و مرحله از برنامه، نسبت به حفظ دارایی‌ها، آزادی‌های مدنی و حقوق حریم خصوصی اطمینان حاصل شود.

علاوه بر طرح ملی برای محافظت از سیستم‌های اطلاعاتی، طرح ملی کشور آمریکا در خصوص InfoSec در چارچوب وزارت امنیت داخلی BHS و ذیل بخش IAIP تحت عنوان؛ راهبرد ملی برای امنیت فضای تبادل اطلاعات[1] تدوین و در سال ۲۰۰۳ به تصویب رئیس جمهور آمریکا رسیده است. (Ibid, 9-13) این طرح دارای سه هدف شامل موارد ذیل می‌باشد:

۱ـ جلوگیری از حمله علیه زیرساختهای حیاتی آمریکا؛

۲ـ کاهش آسیب‌پذیریهای ملی در برابر حملات رایانه‌ای؛

۳ـ حداقل کردن خسارت و زمان بازیافت در برابر حملات رایانه‌ای.

1- The National Strategy to Secure Cyber Space

علاوه بر اهداف فوق در راهبرد ملی به برنامه‌ریزی در خصوص پنج اولویت زیر تأکید فراوان شده است:

اولویت اول: سیستم ملی پاسخگویی به امنیت فضای تبادل اطلاعات؛

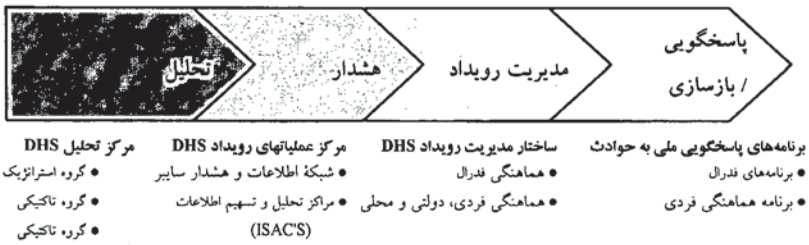
اولویت دوم: برنامه ملی کاهش تهدیدات و آسیب‌پذیریهای فضای تبادل اطلاعات؛

اولویت سوم: برنامه ملی آگاهی‌رسانی و آموزش امنیت فضای تبادل اطلاعات؛

اولویت چهارم: ایمن‌سازی فضای اطلاعات دولت؛

اولویت پنجم: همکاری امنیت ملی و امنیت فضای تبادل اطلاعات بین‌المللی.

متدولوژی تحلیل مخاطرات در آمریکا: سیستم پاسخگویی و متدولوژی تحلیل مخاطرات در آمریکا دارای چهار حلقهٔ تحلیل؛ هشدار؛ مدیریت رویداد؛ و پاسخگویی و بازسازی می‌باشد. (Ibid, 17)



شکل (۵) : سیستم پاسخگویی و تحلیل مخاطرات در آمریکا

روش استاندار تحلیل مخاطرات مربوط به امنیت اطلاعات در سیستم‌های امنیتی آمریکا OCTAVE [1]نام دارد. (Sonsonkin, 2005) این روش به منظور ارزیابی خطرات مربوط به امنیت اطلاعات و تحلیل مخاطرات مربوط به زیرساختهای حیاتی اطلاعات به کار گرفته می‌شود. روش مزبور دارای یک خط‌مشی سه‌مرحله‌ای است و هر مرحله نیز خود دارای چندین زیرمجموعه می‌باشد. این

1- Opertionally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

روش در چارچوب تکنیکهای تحقیقاتی گروهی خصوصاً دلفی انجام می‌شود.

مراحل سه‌گانه و اساسی این روش برای تحلیل مخاطرات به شرح زیر است:

- مرحلهٔ اول: مشخص کردن تمامی تهدیدات علیه سرمایه‌های حیاتی؛
- مرحلهٔ دوم: مشخص کردن آسیب‌پذیریهای مربوط به سرمایه‌های حیاتی؛
- مرحلهٔ سوم: گسترش استراتژی امنیت و طرح‌ها، در این مرحله طرح‌ها، برنامه‌ها و راهبردها برای مواجهه با مخاطرات اتخاذ می‌شود.

علاوه بر این ۵ اصل اساسی در استانداردهای تحلیل مخاطرات مربوط به امنیت اطلاعات در آمریکا و در چارچوب بخش IAIP مورد توجه قرار می‌گیرد.

شکل (٦) : ۵ اصل برای حفاظت از ساختارهای حیاتی

در آمریکا مدیریت تحلیل مخاطرات بر اساس تعیین بخشهای بحرانی و به دنبال آن تعیین فضاهای حائز اهمیت تبادل اطلاعات در بخشهای بحرانی شکل

می‌گیرد. با توجه به این دو اقدام بخشهای تحلیل و بررسی مخاطرات در IA-IP شکل می‌گیرد و در هریک از این دو بخش که زیرمجموعهٔ IAIP می‌باشند تحلیل مخاطرات مربوط به همان مجموعه صورت می‌گیرد. با این وجود تحلیل مخاطرات در دو سطح کلان و بخشهای بحرانی انجام می‌شود. در سطح کلان سیاستگذاری‌ها و تحلیل مجموع مخاطرات در بخشهای مختلف و تأثیرات ان بررسی می‌شود. در سطح بخشهای بحرانی، تحلیل مخاطرات توسط ISAC ها انجام می‌شود.

ب) استرالیا

ساختارها و سازمانها: سه وزارتخانه دفاع، دادگستری و ارتباطات اصلی‌ترین نقش را درخصوص حفاظت از فضاهای حیاتی تبادل اطلاعات در استرالیا برعهده دارند. در این میان نقش اجرایی وزارت دفاع و نقش سیاستگذاری وزارت ارتباطات مشهودتر و مؤثرتر می‌باشد. (Dunn & Wigert, 2004)

در ذیل وزارت دفاع مجموعه‌ای تحت عنوان ادارهٔ سیگنالهای دفاعی (DSD)[1] وجود دارد. این اداره وظیفهٔ حفاظت از شبکه‌های اطلاع‌رسانی، مواجهه با تهدیدات و مخاطرات رایانه‌ای را برعهده دارد و همچنین مسئول دادن هشدار به سازمانها و ادارات ایالتی در خصوص انجام عملیات امنیتی درحوزهٔ IT می‌باشد. DSD مأموریتهای خود را در چارچوب دو بخش امنیت اطلاعات (InfoSec) و اطلاعات سیگنالی انجام می‌دهد. اطلاعات سیگنالی در واقع وظیفهٔ شنودها و ضدشنودها را در سطح ملی برعهده دارد.

DSD همچنین سه برنامهٔ مؤثر را برای انجام وظایف طراحی کرده است. این برنامه‌ها شامل: گزارش حوادث، تیم آسیب‌پذیری شبکه‌های رایانه‌ای (CNVT)[2] و برنامهٔ گواهیهای مدخل[3] می‌باشد.

برنامهٔ گزارش حوادث به شفاف‌سازی و آشکارسازی وقایع موجود در حوزهٔ

1- Defence Signals Directorate
2- The Computer Network Vulnerohility Team
3- Gateway Certification

امنیت و ارائهٔ گزارش و تحلیل پیرامون آن می‌پردازد. گزارشهای این مجموعه کارپایهٔ تعیین تهدیدات و تولیدهای امنیتی می‌گردد. حوادثی که در این مجموعه پیرامون آن گزارش تهیه خواهد شد مواردی مانند؛ ورود غیرمجاز به سیستم IT، وارد نمودن سهوی و عمدی ویروسها به شبکه و تخریب و بهره‌برداریهای غیرمجاز از اطلاعات حفاظت شده می‌باشد.

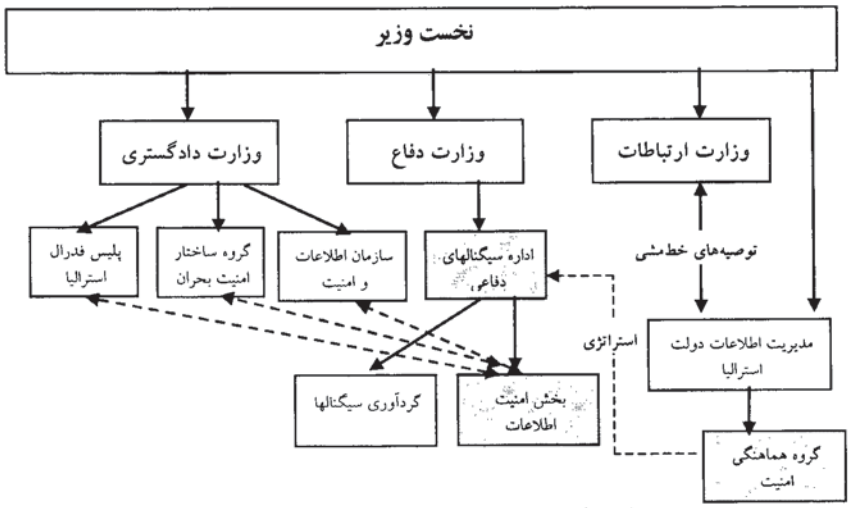
تیم CNVT یکی از برنامه‌های مهم در ذیل سازمان DSD می‌باشد. این تیم مرکب از عناصر بسیار حرفه‌ای کشور استرالیا در زمینهٔ IT هستند که هدف تشخیص بنیانهای آسیب‌پذیری شبکهٔ فتا دولتی را دنبال می‌نمایند.

برنامهٔ سوم که به نام گواهیهای مدخل می‌باشد برای کمک به آن دسته از سازمانهای دولتی که به شبکه اینترنت وصل شده‌اند ایجاد گردیده است. هدف اصلی این مجموعه کاهش خسارت و مخاطرات ورود به شبکه اینترنت توسط کاربران ذکر گردیده می‌باشد.

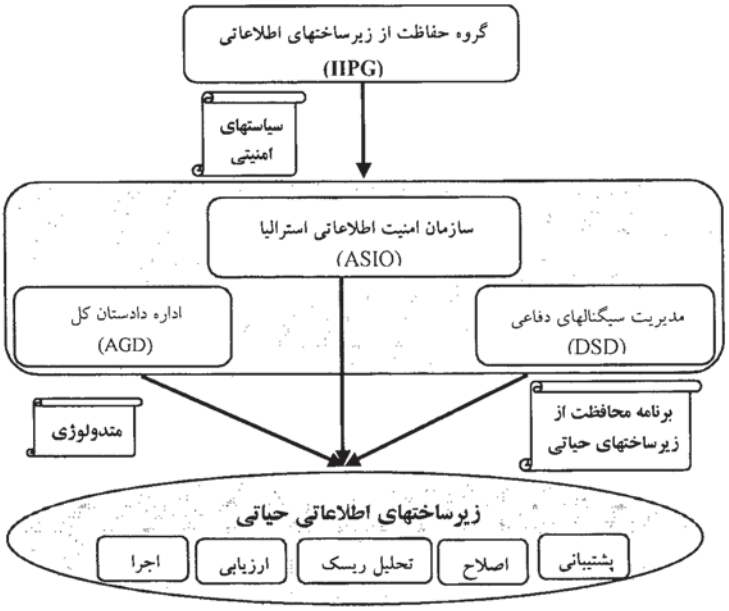
سازمان مدیریت اطلاعات دولت استرالیا (AGIMO)[1] یکی دیگر از تشکیلات درگیر در امنیت فضاهای حیاتی تبادل اطلاعات (افتا) می‌باشد. این سازمان که زیرنظر وزارت ارتباط است، وظیفهٔ کلان تعیین خط‌مشی دولتی در کلیهٔ زمینه‌های مرتبط با افتا را برعهده دارد. در این چارچوب توسعهٔ محیط الکترونیکی امن و قابل اعتماد، افزایش آگاهی در زمینهٔ امنیت الکترونیکی، تهیهٔ گزارش از وقایع از دیگر وظایف این سازمان می‌باشد.

گروه ساختار امنیت بحران (CIPG)[2] که در ذیل وزارت دادگستری قرار دارد نیز یکی دیگر از سازمانهای اصلی درگیر در زمینهٔ افتا می‌باشد. این سازمان وظیفهٔ تشخیص مخاطرات و تعیین و ارزیابی آسیب‌پذیری در بخشهای بحرانی مخابرات، مالی، الکتریسیته و کنترل ترافیک هوایی را برعهده دارد.

1- Australian Government Information Management (AGIMO)
2- Critical Infrastructure Protection Group (CIPG)



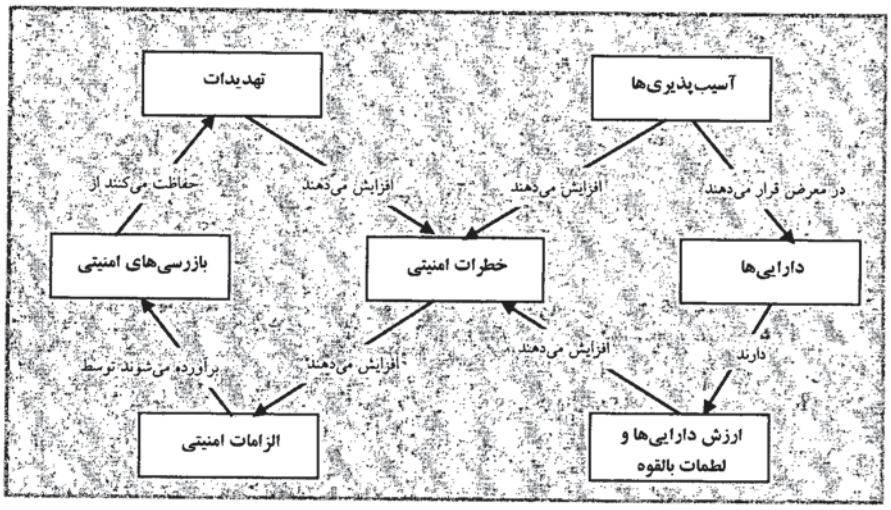
شکل (٧) : ساختار امنیت اطلاعاتی در استرالیا



شکل (٤) : سازماندهی برنامه محافظت از زیرساختهای اطلاعاتی حیاتی استرالیا

متدولوژی تحلیل مخاطرات: استرالیا دارای یک استاندارد مدیریت خطر می‌باشد که در چارچوب آن همهٔ ساختارهای بحرانی به منظور مدیریت خطر برای جلوگیری، آمادگی و پاسخگویی و بازسازی، ارزیابی می‌شوند. نظام‌نامهٔ امنیتی تکنولوژی اطلاعات دولت، استانداردهای استرالیا برای تحلیل مخاطرات در حوزهٔ افتا را شکل داده است. ((Austratian, 2004)

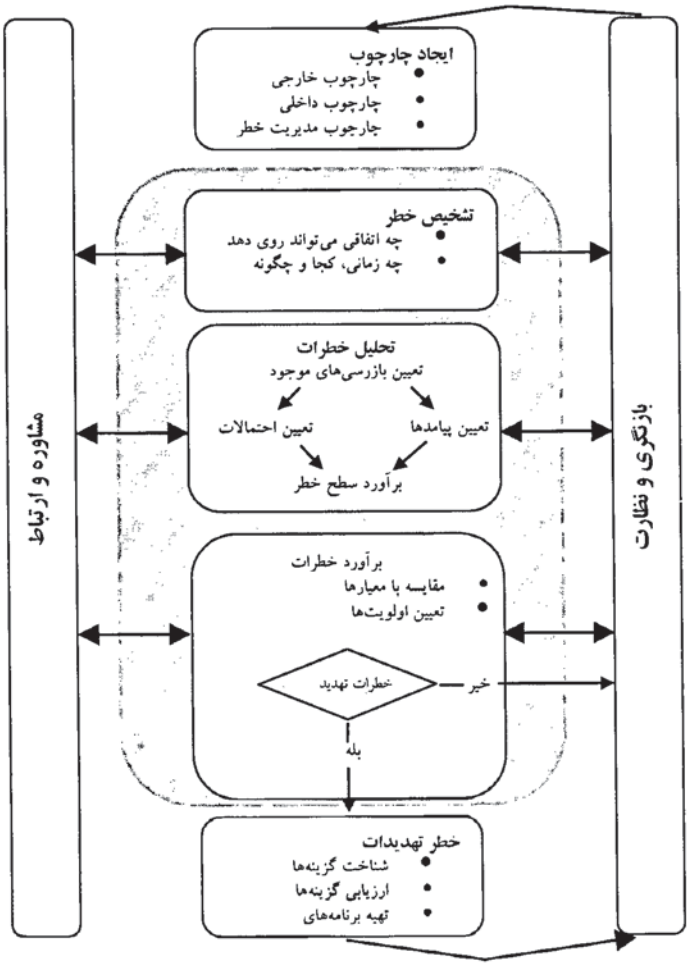
اجزای این نظام‌نامه شامل سرمایه‌ها، ارزش سرمایه‌ها، تهدیدات، آسیب‌پذیریها، خطر امنیتی، نیازهای امنیتی و کنترلهای امنیتی می‌باشد.



شکل (۹) : نمای کلی روابط در مواجهه با خطر در استرالیا

علاوه بر متدولوژی تحلیل مخاطرات که به عنوان صفحه استاندارد تحلیل مخاطرات عمل می‌نماید در استرالیا مدیریت مواجهه با مخاطرات (ERM) توسط ارگانی تحت عنوان مدیریت فوریت‌های استرالیا (EMA) انجام می‌پذیرد. مدیریت مواجهه با مخاطرات در واقع فرایند بررسی، تحلیل و ارزیابی مخاطرات استرالیا در حوزه افتا می‌باشد که بر اساس سند استاندارد متدولوژی تحلیل

مخاطرات این فرایند تحقق می‌یابد. (Handbook, 2003)



شکل (۱۱) : دیاگرام مواجهه با مخاطرات ارائه شده توسط ERM

فرایند برآورد و ارزیابی مخاطرات در استرالیا دارای پنج مرحله شامل؛ ایجاد زمینه، تشخیص مخاطرات، تحلیل مخاطرات، ارزیابی مخاطرات و تهدید

مخاطرات می‌باشد.

این فرایند توسط دو مجموعه که در عرض این فرایند قرار دارد جهت‌دهی و تعدیل می‌گردند. یک مجموعه وظیفهٔ رصد کردن و وارسی وضعیت، در مراحل پنج‌گانه را برعهده دارد. همچنین دریافت بازخورد از مرحله پنجم و تزریق داده‌ها به سیستم جهت آغاز مرحله جدید توسط این مجموعه انجام می‌گیرد. مجموعهٔ دوم ارتباطات و مشاوره می‌باشد. در این مجموعه نیز ارتباط با اعضا و همچنین بخش‌های مختلف فرایند برقرار می‌گردد و ضمن دادن مشاوره به بخشهای مختلف فرایند، نقطه‌نظرهای اعضا را نیز به مجموعه‌های داخلی فرایند منتقل می‌نماید.

ج) انگلستان

دولت انگلیس درحوزهٔ CIIP دو نوع تهدید کلی را شناسایی و تدوین کرده (Assurance, 2004) که عبارتند از:

- حملات تروریستی به تأسیسات و تجهیزات؛
- حملات الکترونیکی به رایانه‌ها و سیستم‌های مخابراتی.

علاوه بر این، این دولت در حوزهٔ InfoSec نیز ٦ نوع تهدید را شناسایی و تدوین نموده که عبارتند از:

- ویروس‌های رایانه‌ای؛
- هک کردن؛
- سیاست و عملکرد ناقص امنیتی؛
- حملات یا حوادث فیزیکی؛
- خطاهای سیستم در حوزهٔ نرم‌افزار و سخت‌افزار؛
- خارج از رده بودن سیستم‌ها و نرم‌افزارها.

دولت بریتانیا در مواجهه با تهدیدات در حوزهٔ فتا برآورد استراتژیک خود را با توجه به محورهای اساسی زیر تهیه می‌نماید:

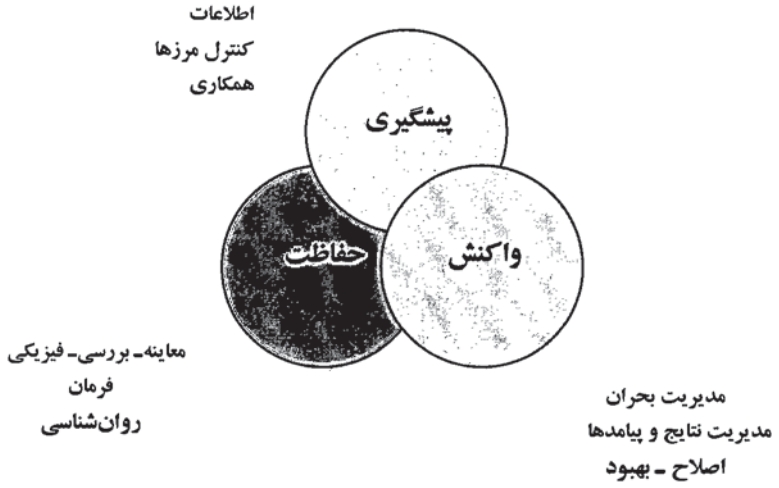
- تحلیل بخش: در این مرحله به تعریف و تبیین بخشهای حیاتی می‌پردازد و مشخص می‌نماید که چه بخش‌ها و فضاهایی، حیاتی می‌باشند.
- تحلیل وابستگی: در این مرحله رابطهٔ میان بخشهای حیاتی با یکدیگر و فضاها و زیرفضاهای هریک از بخشهای حیاتی با یکدیگر و نوع وابستگی‌های میان آنان را تعریف می‌کند.
- تحلیل خطی: در این مرحله روشهای تحلیل خطی و چگونگی سنجش خطرهای مرتبط با CIIP و InfoSec مورد بررسی قرار می‌گیرد.
- ارزیابی تهدیدات: با توجه به روش و معیارهای سنجش خطر، تهدیدات موجود در حوزهٔ فتا برآورد می‌گردد.
- ارزیابی آسیب‌پذیری‌ها: در این مرحله نیز با توجه به روش و معیارهای سنجش خطر، آسیب‌پذیریهای موجود در زیرساختها، فضاها و زیرفضاهای حیاتی برآورد می‌شود.
- تحلیل سیستم: در این مرحله کلیهٔ سیستمهای مرتبط با زیرساختهای حیاتی و نقاط حیاتی و حساس آن مورد بررسی قرار می‌گیرد.
- ارزیابی لطمه[1]: در این مرحله اثر ضربه و نتایج آن مورد بررسی قرار می‌گیرد. در این چارچوب و بر اساس یک روش انتخاب شده برای ارزیابی لطمه، انواع مختلف حملات و لطمات از نظر ناحیه، زمان، دوام، شدت و روش مقابله با آن مورد بررسی قرار می‌گیرد.

د) سنگاپور

بیشتر موارد مربوط به حفاظت از زیرساخت‌های حیاتی در سنگاپور نظیر ساختار و سازمانهای دیگر همانند مدل آمریکا و استرالیا می‌باشد. اما استراتژی سنگاپور در حوزهٔ CIIP دارای جنبه‌های آموزشی مناسبی است.

1- Impact Assessment

استراتژی امنیتی سنگاپور در حوزهٔ فتا یک استراتژی سه حلقه‌ای است که شامل، پیشگیری[1]، حفاظت و واکنش می‌باشد. استراتژی پیشگیری به منظور شناسایی تهدیدات و مقابله با آن قبل از به فعلیت درآمدن متمرکز است. استراتژی حفاظت، برپایهٔ ایمن‌سازی و محافظت از زیرساختهای حیاتی بنا شده است و استراتژی واکنش نیز در برابر حادثهٔ امنیتی و نحوهٔ مقابله با آن طراحی گردیده است. (www.cisco.com.sg)



شکل (۱۲) فضای Cyber در سنگاپور

حفاظت از زیرساختهای حیاتی اطلاعاتی در ایران

موضوعیت زیرساخت‌های حیاتی، اطلاعاتی و زیرفضاهای اطلاعاتی مربوط به سایر زیرساخت‌های حیاتی بستگی به میزان گستردگی، شبکه‌ای بودن، اهمیت آن در قدرت و منافع ملی و به دنبال آن امنیت ملی یک کشور دارد. در برخی از کشورها اصولاً CII موضوعیت‌ندارد زیرا در این کشورها یا چنین زیرساخت‌هایی

1- Prevention

وجود ندارد و یا بسیار ابتدایی است.

از سوی دیگر اهمیت حفاظت از زیرساخت‌ها به اینترنتی یا اینترانتی بودن این زیرساخت‌ها بستگی دارد. چنانچه زیرساخت‌هایی در حوزه‌ی CII، اینترنتی باشد تحقیقاً حفاظت از آن از اهمیت مضاعفی برخوردار خواهد بود. در حالی که اینترانتی بودن CII به مانند گزینه‌ی قبلی، حفاظت آن پیچیده و حساس نمی‌باشد.

کشور جمهوری اسلامی ایران در حال حاضر و در دوره‌ی ۱۰ سال گذشته از رشد چشمگیری در حوزهٔ فتا برخوردار بوده و با توجه به برنامه‌های تدوین شده و نهادهای ایجاد گردیده و چشم‌انداز موجود، این رشد همچنان و با سرعت نسبتاً بالا ادامه خواهد یافت.

در این چارچوب نیز بسیاری از زیرساخت‌های کشور به صورت اجتناب‌ناپذیر به سمت بهره‌برداری هر چه بیشتر از تکنولوژی اطلاعات پش خواهد رفت و همچنین زیرساخت‌های اطلاعاتی نیز توسعه پیدا خواهند کرد. در چنین شرایطی تمهیدات لازم به منظور حفاظت از چنین زیرساخت‌هایی اهمیت زیادی پیدا می‌کند. بدیهی است طراحی، سازمان، ساختار، فرایند، ابزار، نیروی انسانی ماهر و مدیریت در حوزهٔ حفاظت از زیرساخت‌های حیاتی به اندازه‌ی خود زیرساخت‌های حیاتی دارای اهمیت می‌باشد. البته هنوز گستردگی، پیچیدگی، شبکه‌ای شدن و اینترنتی گردیدن زیرساخت‌های حیاتی جمهوری اسلامی در حد برخی کشورهای پیشرو نمی‌باشد لذا ضرورتی به بکارگیری سیستم‌ها، ساختارها، فرایندها و ابزارهای حفاظتی مشابه آنان نیست. بدیهی است چنین رویکردی نه‌تنها مؤثر و کارآمد نخواهد بود بلکه ضمن برجای گذاشتن هزینه‌های گسترده، باعث ایجاد مشکلات جانبی در کار نیز خواهد گردید.

نکتهٔ مهم دیگر این است که، اهمیت، جایگاه و ویژگیهای زیرساخت‌های حیاتی اطلاعاتی و فضاها و زیرفضاهای اطلاعاتی با دیگر زیرساخت‌های غیرحیاتی، همان‌طور که در بخش اول توضیح داده شد متفاوت می‌باشد. بنابراین از جنبه‌های امنیتی جداسازی حفاظت از زیرساخت‌های حیاتی از زیرساخت‌های

غیرحیاتی ضروری به نظر می‌آید.

با توجه به این نکات ایجاد یک شورای عالی امنیت زیرساخت‌های حیاتی در کشور که مأموریت سیاستگذاری و تعیین خط مشی‌ها و بررسی و تصویب طرح‌ها و پروژه‌های ملی امنیت زیرساخت‌های حیاتی را عهده‌دار شود ضروری به نظر می‌رسد. همچنین شناسایی و تعیین زیرساخت‌های حیاتی باید در درون این شورا انجام پذیرد بنابراین افزودن و یا حذف مواردی از فهرست زیرساخت‌های حیاتی کشور در این شورا صورت خواهد گرفت.

نکته‌ی دوم اینکه ایجاد کانون تحلیل مخاطرات مربوط به زیرساخت‌های مطروحه نیز امری ضروری است. بدیهی است با توجه به طبقه‌بندی‌های حفاظتی در هر یک از فضاها و زیرفضاهای مربوط به زیرساخت‌های حیاتی، ایجاد چنین کانون‌هایی در درون هر یک از سازمان‌های متولی چنین فضایی امری ضروری و لازم است. این کانون‌ها مانند دیگر مراکز تحلیل اطلاعات شایسته است که در یک فرایند از پیش تعریف شده شامل تشخیص مخاطرات، تحلیل مخاطرات، برآورد ابعاد، سطوح، عمق و شدت مخاطرات به بررسی مخاطرات مربوط به فتا در حوزه و سازمان مربوطه بپردازد.

نکته سوم ایجاد مرکز فوریت‌های حوادث امنیتی در حوزهٔ فتا آن هم به صورت متمرکز در هر حوزه و سازمان مربوطه امری ضروری و شایسته است. بدیهی است به تناسب حجم و اندازهٔ حوزهٔ فتا در فضا یا زیرفضاهای حیاتی اطلاعاتی، سازمان چنین مرکزی باید گسترده شود. ای‌ن مرکز که در بسیاری از کشورهای دنیا به نام (CERT)[1] شناخته می‌شود، نسبت به حوادث امنیتی در بخش‌های بحرانی مسئولیت خواهد داشت و مأموریت دارد تا پس از وقوع حادثه بلافاصله نسبت به آن واکنش نشان داده و نسبت به خنثی‌سازی حادثه اقدام نماید.

درکنار حوزه‌ها ومراکز وطرحهای اختصاصی مربوط به حفاظت از زیرساختهای

1- Computer Emergency Response Team

حیاتی که به صورت منفصل و توسط سازمان‌های مربوطه انجام می‌شود. بسیاری از نیازمندیهای مربوط به امنیت زیرساخت‌های حیاتی از حوزه‌های خصوصی و عمومی مربوطه در داخل و خارج از کشور قابل تأمین می‌باشند. به طور مثال دیگر نیازی نیست که برای آموزش کادرها و مأموران مرتبط با زیرساخت‌های حیاتی، آموزشکده و یا مرکز جداگانه تأسیس کرد و می‌توان از مراکز موجود در کشور بر اساس آنچه تدارک دیده شده استفاده نمود.

نتیجه‌گیری

نزدیک شدن به شاخص‌های مربوط به زیرساخت‌های حیاتی می‌تواند ما را در تشخیص زیرساخت‌های حیاتی کمک نماید. بدیهی است تعیین و تفکیک دقیق و صحیح زیرساخت‌های حیاتی از زیرساخت‌های غیرحیاتی، به ما در تمرکز بیشتر بر زیرساخت‌های مرتبط با امنیت ملی کمک می‌نماید.

این مقاله نشان می‌دهد که حفاظت از زیرساخت‌های حیاتی اطلاعاتی آن هم حفاظت در حوزه‌ی تبادل اطلاعات، بیش از آنکه براساس استراتژی‌های پیشگیرانه و یا بازدارندگی باشد، بیشتر مبتنی بر استراتژی واکنش است، زیرا در فضای تبادل اطلاعات به علت وجود بازیگران نامحدود با اهداف و مقاصد متفاوت و از سوی دیگر ناممکن بودن تشخیص دقیق مهاجم، استفاده از استراتژی‌های واکنشی مطلوب‌تر است.

نکتهٔ مهم دیگر از موضوع قبلی ناشی می‌شود. با توجه به اینکه حفاظت براساس واکنش، ریسک حفاظتی را افزایش می‌دهد، طراحی و راه‌اندازی مراکز تحلیل مخاطرات به منظور تشخیص دقیق‌تر خطرات و شیوه‌های حمله و چگونگی مدیریت واکنش امری ضروری است. چنین مراکزی می‌تواند توان و دقت مدافع را در دفع تهاجم و یا شکست مهاجم افزایش دهد.

نکتهٔ سوم به تشخیص و تعیین فضاهای حیاتی مربوط است. به نظر می‌رسد مبنا قرار دادن مفهوم زیرساخت نمی‌تواند ما را به سوی تشخیص جامع و مانع

فضاهای حیاتی سوق دهد. به نظر می‌رسد به جای زیرساخت باید بر روی فضا یا بخش‌های بحرانی تأکید کرد و از طریق فهرست کردن کلیه فضاهای قابل بررسی کشور براساس شاخص‌ها و معیارهای از پیش تعیین شده به اولویت‌بندی آنها پرداخت و بر همین اساس فضاهای حیاتی را تعیین نمود.

English References

1. John Moteff and Paul Parfomark, "Critical Infrastructure and Key Assests: Definition and Identification", Science, and Industry Division, (2004), P. 2.
2. U.S. Office of Homeland Security, "The National Strategy for Homeland Security", July 16, 2002, P. 30.
3. http://www.mio.gov.uk/output/page134.html
4. M. Dunu and I. Wigert, Swiss, "International CIIP Handbook", Federal Institute of Technology Zurich, (2004)
5. Dorothy E. Denning, Peter J. Denning", Data Security", ACM Computing Surveys (CSUR), Vol. 11, No. 3 (September 1979), PP. 227-249.
6. Debra S. Herman, "A Practical Guide to Security Engineering and Information Assurance", CRC Press, (2008)
7. James P. Anderson, "Computer Security Technology Planning Study", (http://Seclab.cs.ucdavis.edu/projects/history/paper/)
8. Cynthia E. Irvinc, Timothy E. Levin, "Data Integrity Limitations in Hybrid Security Architecture" (http://cisr.nps.navy.mil/downloods/dataintegrityhybrid.pdf).
9. C. E. Shamon, "Communication Theory of Secrecy Systems", Bell System Technical, Vol. 28, No. 4, pp. 656-715.

10. Bob Blakley, Ellen McDemott, Dan Geer, "Information Security is Information risk management", Workshop on New Security Paradigms, (September 2001), PP. 97-104.
11. K. Honc, J. H. P. Eloff, "Information Security Policy: What do International Security Standard Say?", Computer and Security, Vol. 21, No. 5, PP. 402-409.
12. http://www.dhs.gov.dhspublic/themc_home1.jsp
13. National Strategy for homeland Security, Office of homeland Security, July 2002, P. 41.
14. The White House, "National Plan for Information Systems Protection, Version 10, 2003, PP. 13-14.
15. The White House, "The National Strategy to Secure Cyber Space, 2003, PP. 9-13.
16. Mikhail Sonsonkin, "Operationally Critical threat, Asset and Vulnerability Evaluation", Polytechic University, 2005.
17. M. Dunn and I. Wigert, Swiss, International Handbook 2004, Federal Institute of Technology Zurich, 2004, Part Austraian.
18. Austratian Government Information Technology Security Manual, Defence Signals Directorate, 2004, PP. 1-4.
19. "Critical Infrastructure Emergency Risk Management and Assurance", Handbook, Emergency Management Australia, 2nd Edition, Nov. 2003.
20. Protecting our Information Systems, Central Sponser for Information Assurance, 2004.
21. http://www.cisco.com.sg/service/index.html