فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال دوم، شماره‌ی ۵ (بهار ۱۳۹۲): صص ۴۱ – ۶۸

مطالعه تطبیقی ساختار دفاع سایبری کشورها

پرویز حسینی[۱]
حسین ظریف‌منش[۲]

تاریخ دریافت: ۱۳۹۲/۰۷/۰۶
تاریخ پذیرش: ۱۳۹۲/۰۸/۲۰

چکیده

امروزه توجه به مخاطرات امنیتی فضای سایبر، یعنی واقع شدن در وضعیتی که بتوان از حساسیت و آسیب‌پذیری ارکان نظام در مواجهه با تهدیدات داخلی و خارجی حوزه سایبر فروکاست، از عنایت ویژه‌ای برخودار است. دلیل این توجه از یک سو متأثر از رشد روز افزون وابستگی جوامع به فضای سایبر به عنوان بستر اصلی اطلاعات و از سوی دیگر گوناگونی تهدیدات در حوزه مذکور است.

یکی از مهم ترین مسائلی که به دنبال پیشرفت روز افزون فناوری دستخوش تغییرات شگرفی در سازمان‌ها گردیده است ساختار سازمان می‌باشد. لذا با توجه به تهدیدات حوزه سایبر، کشورها سازمان دفاعی خود را خاص این حوزه، جهت مقابله با تهدیدات مذکور ایجاد نموده، در حال بهینه کردن آن می‌باشند. تحقیق مذکور ضمن برشماری ویژگی‌های فضای سایبر و تبیین مفهوم دفاع و حمله در حوزه سایبر، ساختار دفاع سایبری برخی از کشورها را مورد مطالعه قرار داده، با جمع‌آوری اطلاعات به روش کتابخانه‌ای و میدانی و مصاحبه با خبرگان، با رویکرد کاربردی، داده‌ها را با اتکاء بر موضوعات نظری و مطالعات تطبیقی، تحلیل نموده، با تبیین ساختار دفاع سایبری ج.ا.ا، و براساس اطلاعات به دست آمده، ایجاد سازمان دفاع سایبری جمهوری اسلامی ایران، ذیل شورای عالی فضای مجازی را امری ضروری و لازم می‌داند.

کلید واژه‌ها: *امنیت سایبری، تهدیدات سایبری، دفاع سایبری، ساختار سایبری، فضای سایبر*

۱- دانشجوی دکتری تهدیدات امنیت ملی دانشگاه عالی دفاع ملی
۲- دکتری امنیت ملی دانشگاه عالی دفاع ملی

۱- مقدمه

شالوده و بنیاد هر کشوری براساس مجموعه‌ای از زیرساختارهای حیاتی آن کشور در بخش‌های ارتباطات، دفاع، انرژی، حمل‌ونقل، کشاورزی، بهداشت و امور اقتصادی است که فضای سایبر به مثابه یک سامانه عصبی، آنها را به‌هم مرتبط می‌سازد. (افتخاری،۱۳۸۲: ۵)

فضای سایبر مجموعه‌ای متشکل از زیرساخت‌ها، شبکه‌ها، نرم‌افزارها، سخت‌افزارها، پروتکل‌ها، محتوی و سیاست‌های حاکم براین حوزه است. همچنین این فضا، مجموعه‌ای از مفاهیم را در قالب محتوای فرهنگی، محتوای سیاسی یا حتی منابع مادی و مالی و منابع حقوقی و معنوی را در برمی‌گیرد.

استفاده از فنآوری‌های فضای سایبر با توجه به رویکردهای جدید در دنیای کنونی امری اجتناب ناپذیر می‌باشد. با نگرش به در اینکه قواعد و ابزار فضای سایبر در اختیار دیگران می باشد، بازیگر یا کشوری که می‌خواهد وارد این عرصه شود باید تلاش کند که از همه ظرفیت‌ها، نقاط مثبت و فرصت‌های آن استفاده کند و با تهدیدات موجود در فضای مذکور مبارزه نموده و حداکثر بهره‌برداری لازم را از این فضا داشته باشد و این مهم بدون داشتن ساختار مناسب جهت مقابله با تهدیدات این حوزه امکان‌پذیر نمی‌باشد . استفاده از فضای سایبر که دستاورد فناوری‌های نوین اطلاعات است، اگرچه برای کشورهای در حال توسعه به عنوان یک فرصت برای جبران عقب‌ماندگی‌های فناورانه نسبت به جوامع پیشرفته است، اما باید دقت نمود که همین فناوری که ساخته دست این جوامع است، اگر درست مورد بهره‌برداری قرار نگیرد و حساسیت‌های امنیتی آن مورد توجه واقع نشود، خود می‌تواند به عنوان یک تهدید مهم به حساب آید.

نبردهای سایبری به عنوان جدیدترین و پیچیده‌ترین نبردها در جنگ پست مدرن به شمار می‌آید. حملات سایبری به دلیل بکر بودن، درصد هزینه و فایده بالا، عدم توانایی کشور هدف در مشخص و اثبات نمودن منشأ تهدید و عدم توانایی در تعیین میزان و دامنه‌ی خسارات شده در مراحل اولیه شروع حمله، مورد توجه کشورهای متخاصم به ویژه در جنگ‌های پنهان قرار گرفته است.

امروزه اقدامات و حملات تروریستی فراوانی در فضای سایبر متوجه دولت‌هاست که از ویژگی‌های این حملات می‌توان به ناشناخته بودن و سرعت حملات مذکور اشاره نمود، و معمولاً این‌گونه حملات پس از وقوع مورد شناسایی قرار می‌گیرد.بنابراین با ایجاد یک راهبرد ملی در استقرار حداکثر امنیت در فضای سایبر می‌توان به کاهش آسیب‌پذیری کشور درمقابل حملات پرداخته ، از بروز خسارت به زیرساخت‌های اطلاعاتی پایه و حیاتی و همچنین دارایی‌های ملی جلوگیری نمود.

بر مبنای رشد روزافزون دانش سایبری و همپایی سازمان‌ها با آن، تحولات سازمانی و تحولات علم و فناوری، سازمان‌ها را با تحولات محیطی جدیدی مواجه ساخته‌است که این سازمان‌ها ناگزیر باید در اندیشه راهکارهای مقابله با چالش‌های محیط جدید و انعطاف‌پذیرکردن ساختار فرآیندها و منابع انسانی خود باشند.

ساختار سازمانی، راه یا شیوه‌ای است که به وسیله آن فعالیت‌های سازمانی تقسیم، سازماندهی و هماهنگ می‌شود. سازمان‌ها ساختارهایی را به وجود می‌آورند تا فعالیت‌های عوامل انجام کار را هماهنگ کرده و اعمال اعضاء را کنترل کنند. (اعرابی، ۱۳۸۵: ۳۶)

تمام سازمان‌ها دارای ساختارهای مشخص و معینی می‌باشند که به وسیله این ساختارها به اهداف و راهبردهای خود دست پیدا می‌کنند. ساختار سازمان سه وظیفهٔ اصلی به عهده دارد: ابتداء و مهم ترین آن‌ها این است که ساختار سازمان باید در خروجی یا بـازده سازمان و در نیل سازمان به اهدافش نقش داشته باشد. سپس در ایجاد هماهنگی نقش افراد مختلف در سازمان مؤثّر باشد. به عبارت دیگر، ساختار موجب می‌شود تا هر فرد براساس نظر و سلیقهٔ شخصی اقدام نکنـد، بلکه در چارچوب اهـداف سازمانی گام بردارد. درنهایت ساختار سازمانی سبب می‌گردد تا کارکنان بـا شرایط تدوین شدهٔ سازمان خود را مُنطبق سازنـد. (نجف‌بیگی، ۱۳۷۶: ۱۳۵)

در نگاهی به سوابق تحرکات دفاعی– امنیتی در سطوح کلان، بر اساس آمار تاکنون ۳۲ کشور در دنیا، ساختار دفاع سایبری خود را تشکیل داده‌اند و ۱۴۰ کشور در حال مطالعه روی توسعه دفاع ملی در کشور خود هستند. (سازمان پدافند غیرعامل، ۱۳۹۱/۳/۱۶) لذا غفلت از این موضوع می‌تواند خسارت‌های جبران‌ناپذیری را متوجه نظام نماید. مسئله اصلی این است که عدم کارائی و اثربخشی ساختارهای موجود حوزه دفاع سایبری در ج.ا.ا امکان حملات سایبری بر علیه کشور اسلامی‌مان را به حداکثر رسانده ، دائماً دشمن را متوجه نقاط ضعف ساختاری این حوزه می‌نماید. لذا چه ساختاری می‌تواند جهت مقابله با تهدیدات این حوزه موثر باشد و امر دفاع در فضای سایبر را روشمند و هدفمند نماید تا در برخورد با حملات سایبری علاوه بر کنترل تهدیدات، آسیب‌پذیری‌ها را به حداقل رسانده، با توجه به فرمایش مقام معظم رهبری بتوان در صورت حمله سایبری دشمن علاوه بر دفاع مناسب از زیرساخت‌های موجود در فضای سایبر، در همان سطح دشمن را مورد تهدید قرار داد. ساختار دفاع سایبری مهم ترین محور و برنامه‌ای است که می‌توان با آن به دفاع سایبری مناسب دست پیدا کرد.

۲- تعاریف و مفاهیم

فضای سایبری[۱]

منظور از فضای سایبر یا فضای مجازی ترکیبی از ده‌ها هزار رایانه به‌هم پیوسته، سرویس‌دهنده‌ها، شبکه‌های ارتباطی، سویچ‌ها و کابل‌های فیبرنوری است که امکان ایجاد ارتباطات را در یک سامانه جامع فراهم می‌آورد. (افتخاری،۱۳۸۲: ۵)

۱. Cyber Space

فضای سایبری استعاره‌ای برای تشریح سرزمین غیرفیزیکی، تشکیل شده توسط سامانه های رایانه ای می‌باشد. بر خلاف فضای حقیقی، سیر و گشت در این سرزمین بدون هیچ گونه حرکت فیزیکی مقدور است، تنها با حرکت موشواره یا فشردن کلیدی در صفحه کلید. (سیدمفیدی، ۱۳۸۳: ۶)

ویلیام گیبسون در رمان علمی‌تخیلی نورومنسر (۱۹۸۴) اصطلاح فضای سایبر را ابداع نمود. (Gibson،۱۹۸۴ :۶۹) گیبسون در شرایطی که شبکه‌ها و سامانه‌های رایانه ای جهانی امروزی نبود فضای سایبری را این گونه معرفی کرد:«فضای سایبر یک توهم مورد وفاق است که روزانه میلیاردها اپراتور و کودکانی که مفاهیم ریاضی به آن‌ها داده می‌شود آن را تجربه می‌کنند. فضای سایبر نوعی بازنمایی گرافیکی از داده‌هایی است که از بانک‌های تمامی رایانه ها در سامانه انسانی تصویر سازی شده است. پیچیدگی‌ای که قابل تصور نیست». (بل، ۲۰۰۱: ۴۶)

در بعد چیستی فضای سایبر از دیدگاه سخت‌افزاری، شبکه‌ای جهانی از رایانه های به هم پیوسته است که از طریق مسیر ارتباطی پرسرعت تارعنکبوتی را شکل داده که سریع تر از مصنوعات دیگر انسان در حال گسترش است. اینترنت که نمایشی از فضای مجازی است، بستری هیجان انگیزی را ایجاد نموده که قابلیت ارائه خدمات متنوع، سریع و جذاب را دارد.

ارتباطات سریع قابلیت ارسال پیام؛ ارائه سرویس‌های ارتباطی؛ تبادل اطلاعات با فرمت‌های مختلف از خدمات متنوع این ابر شبکه است. اینترنت قابلیت‌های ویژه‌ای را برای تجارت الکترونیکی، بازاریابی، تبلیغات و بانکداری الکترونیکی پدید آورده است. (Mutula،۲۰۰۷:۱۵)

در سطح معنایی فضای سایبر، فضایی خیالی بین شبکه‌های رایانه ای است. فضای مجازی افراد و کاربران در شبکه‌های اجتماعی، محیط‌های گفتگو، فروشگاه و... با یکدیگر ارتباط برقرار نموده، به گشت و گذار، خرید فروش، بحث و تبادل نظر می‌پردازند بدون اینکه هیچ گونه حرکتی داشته باشند. فضای سایبر برای توصیف هر مفهومی‌که در ارتباط با شبکه‌های رایانه‌ای، فناوری اطلاعات، اینترنت و جامعه اطلاعاتی،کار برده شده است و افراد و کاربران در این فضا به تجربه اجتماعی از تعامل، تبادل و اشتراک گذاری اطلاعات، کسب و کار، بازی و تفریح، بحث‌های گروهی که به صورت غیر فیزیکی است، دست پیدا می‌نمایند. این جذابیت هیجان انگیز انسان را به مفهوم ذهنی پیوند داده که با خیال و وهم گره خورده است و واقعیت را به درون ذهن برده ، در آنجا به هر شکل که بخواهد تغییر داده ، یا از نو می‌سازد بدون اینکه محدودیت مادی برآن اثر گذارد. فضای سایبر چیزی فراتر از اینترنت است که اینترنت این مفهوم را در حال گسترش دادن است. با شکل گیری فضای سایبر و رشد سریع آن مفاهیم عرصه زندگی نیز به سمت تغییر ماهوی گام بر می‌دارد. همه چیز از هویت، فرهنگ، حکمرانی، روابط و تعاملات خصوصی و گروهی در حال

تغییر است. فضای سایبری یکی از ویژگی‌های زندگی امروزی است که در آن افراد و جوامع در سراسر جهان با هم مرتبط شده، معاشرت و همکاری می‌نمایند. (DOD،۲۰۱۱:۱)

تهدید سایبری[۱]

مخاطرات موجود در فضای سایبری را تهدید سایبری گویند. تهدید سایبری یک عامل بالقوه (پتانسیل) برای نقض امنیت در فضای سایبری است. تهدید سایبری در صورتی وجود خواهد داشت که یک پیشامد، قابلیت، کنش، یا رخداد که می‌تواند در امنیت سایبری رخنه ایجاد نموده ، منجر به صدمه شود به وجود بیاید. این بدان معنی است که یک تهدید سایبری، یک خطر بالقوه است که ممکن است منجر به بهره‌برداری از یک آسیب‌پذیری امنیتی[۲] شود. (سازمان فناوری اطلاعات، ۱۳۹۰: فصل ۶)

جنگ سایبر[۳]

استفاده از رایانه ها به عنوان یک اسلحه یا به عنوان ابزاری برای انجام کارهای خشونت بار جهت ترساندن یا تغییر عقیده یک گروه یا کشور است. جنگ سایبر به قصد کارهای سیاسی وآرمانی انجام می‌گیرد و مکان‌ها و تأسیسات حیاتی، مانند انرژی، حمل‌ونقل، ارتباطات، سرویس‌های ضروری (مانند پلیس و خدمات پزشکی) را هدف قرار می‌دهد و از شبکه‌های رایانه ای به عنوان بسترهایی جهت انجام این اعمال خرابکارانه استفاده می‌کند. (سازمان پدافند، بی‌تا: ۵)

جرائم سایبر[۴]

هرگونه دخل و تصرف غیرمجاز از طریق ورود یا خروج، ضبط و ذخیره، پردازش و کنترل داده‌ها و نرم‌افزارهای رایانه‌ای و ایجاد یا وارد کردن انواع ویروس‌های رایانه‌ای و امثال آن جرم محسوب می‌شود. (سازمان پدافند، بی‌تا: ۵)

همزمان با توسعه و کاربردپذیری رایانه و سامانه های رایانه‌ای، جرایم رایانه‌ای هم به وجود آمده است. اگرچه دامنه و حوزه‌ی وقوع جرم در هر حوزه با توجّه به ویژگی‌ها و وسعت کاربرد و استفاده متفاوت بوده‌است. از سال ۱۹۶۰ میلادی تا کنون سه نسل از جرایم رایانه‌ای برشماری شده است. نسل اوّل که مقارن سال‌های دهه‌ی هشتاد، هفتاد و اوایل دهه‌ی هشتاد میلادی است و چون استفاده از اینترنت در آن زمان شیوع نداشت، عمده‌ی جرایم مرتبط با رایانه‌ها بود و از این رو این دسته از جرایم صرفاً به «جرایم

۱. Cyber Threat
۲. security vulnerability
۳. Cyber warfare
۴. Cyber crime

رایانه‌ای» یاد می‌شود. نسل دوّم جرایم رایانه‌ای از اوایل دهه‌ی هشتاد تا اوایل دهه‌ی نود به وقوع پیوست که به «جرایم علیه داده‌ها» تعبیر می‌شود. در این نسل، «داده» صرف‌نظر از این‌که در رایانه قرار داشته باشد یا در واسطها و ابزارهای انتقال، مورد توجّه قرار گرفت و دیگر تأکیدی بر رایانه نبود. نسل سوّم رایانه‌ای نیز هم‌زمان با فراگیر شدن اینترنت از اوایل دهه‌ی ۱۹۹۰ میلادی به وجود آمد. این جرایم که با گسترش کاربرد شبکه و اینترنت به وجود آمد نام «جرایم سایبری» را به خود گرفت. (syberpolice.ir)

۳- ساختار سازمانی

ساختار سازمانی، راه یا شیوه‌ای است که به وسیله آن فعالیت‌های سازمانی تقسیم، سازماندهی و هماهنگ می‌شود. سازمان‌ها ساختارهایی را به وجود می‌آورندتا فعالیت‌های عوامل انجام کار را هماهنگ کرده ، اعمال اعضاء را کنترل کنند. ساختار سازمانی در نمودار سازمانی نمایان می‌شود. نمودار سازمانی نیز یک نماد قابل رویت از کل فعالیت‌ها و فرایندهای سازمان است. (اعرابی، ۱۳۸۵: ۲۶)

شکل ساختار

ساختار سازمانی دارای شکل‌های گوناگون است. اساس و پایهٔ کارهایی که بر روی ساختار انجام شد، براساس کارهای وبـر، در سال ۱۹۴۷ قرار دارد. به گفتهٔ او دیوانسالاری (بروکراسی) دارای یک سلسله مراتب اختیارات، اختیارات محدود، تقسیم کار، افراد با صلاحیّت، رویـه یا شیوهٔ انجام کار، قوانین و مقرّرات الزامی و پاداش‌های متفاوت است. اگر همهٔ این ارکان و عوامل به میزان بالائی وجود داشته باشد به یک ساختار دیوانسالار (بروکرات) مطلوب و آرمانی دسـت می‌یـابیم. در طراحی ساختار سازمانی باید به سه نکتهٔ اساسی توجّه کرد. (پارسائیان واعرابی، ۱۳۸۲: ۵۸)

- تعیین کارهایی که باید انجام شود.
- زنجیرهٔ فرماندهی یا تعیین خطوط سلسله مراتب سازمانی
- طبقه‌بندی دوایـر

ابعاد ساختار سازمانی

در ساختار سازمانی آگـاهی از اَبعاد سازمان، نـقش و اهمیّت آنها ضروری اسـت. اَبـعاد سازمانی به دو دستهٔ ساختاری و محتوائی تقسیم شده است، که هر دو از ویژگی‌های درونی یـک سازمان محسوب می‌شوند. (نجف‌بیگی، ۱۳۷۶: ۱۲۸)

ساختاری	محتوائی
رسمی‌بودن	اندازه
تخصّصی‌بودن	محیط
فناوری سازمانی	هدف‌ها و راهبرد
داشتن استاندارد	فرهنگ
سلسله‌مراتب اختیارات	
پیچیدگی	
مُتمرکزبودن	
حرفه‌ای‌بودن	
نسبت پرسنلی (کارکنان)	

طراحی ساختار سازمانی

در طراحی ساختار سازمانی، مشاغل باید با توجّه به نوع، طبیعت و فعالیّت سازمان شناخته ، سپس در دسته‌ها یا واحدها گروه‌بندی شود. به این ترتیب همهٔ وظایفی که باید انجام شود، مُشخّص و روشن گردد.

صاحب‌نظران سازمان، ساختارهای سازمانی را مُتـعدّد می‌داننـد که مُتداول‌ترین آنها ساختار وظیفه‌ای، ساختار مُبتنی برمحصول،ساختارهای ماتریسی،ساخـتارهای بُلـنـد وساخـتارهای پَـهـن هستنـد. (پارسائیان واعرابی، ۱۳۸۲: ۶۲)

٤- حمله سایبری

حمله سایبری یا حمله شبکه رایانه ای[۱] به‌صورت زیر تعریف می‌شود:

«حمله سایبری، مجموعه اعمالی است که برای ایجاد اختلال، قطعی، کاهش کیفیت یا نابودی اطلاعات مقیم در رایانه های موجود در فضای سایبری انجام می‌شود.» (Andress and Winterfeld،۲۰۱۱:۲۵)

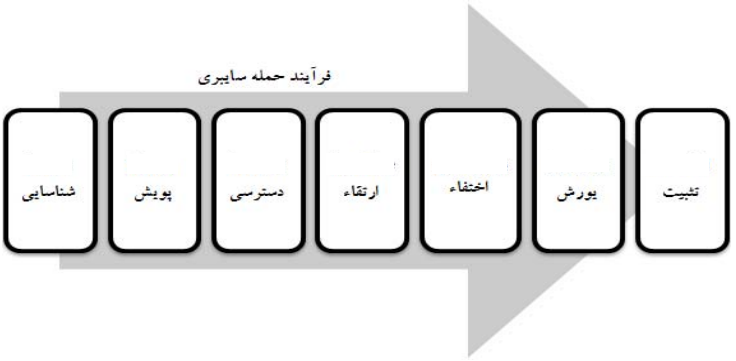
فرآیند حمله سایبری

فرآیند حمله معمولاً بر روی یک سامانه یا مجموعه از سامانه های هدف متمرکز می‌شود. دراین فرآیند همان طور که در شکل زیر نشان داده شده است، معمولاً عملیات **شناسایی** و **پویش**[۲] زیادی به منظور

۱. computer network attack (CNA)
۲. scanning

استخراج اطلاعات لازم از سامانه هدف انجام می‌شود. در این مرحله می‌توانیم عملیات شناسایی را با عمق بیشتری انجام دهیم، زیرا معمولاً در این مرحله شاید نیاز به محرمانگی و مخفی‌کاری نسبت به مرحله اصلی حمله به مراتب کمتر باشد. سپس سعی خواهیم کرد که به سامانه هدف **دسترسی**[۲] پیدا کنیم. برای این کار یا می‌توانیم از یک حمله جدید استفاده کرده یا از اطلاعاتی که طی مرحله کشف یا از روش‌های مهندسی اجتماعی به دست آورده‌ایم، استفاده کنیم.

هنگامی که دارای یک حساب کاربری درسامانه هدف شدیم، شاید نیازمند **ارتقاء**[۳]حقوق دسترسی خود در سامانه هدف به منظور دست یافتن به اهدافمان باشیم. هدف در این مرحله معمولاً به دست آوردن حقوق دسترسی حساب کاربری مدیر سامانه یا «ریشه»[۱] است. هنگامی‌که حقوق دسترسی مناسب در سامانه را به دست آوردیم می‌توانیم هر صدمه‌ای که دوست داریم به آن زده یا هر اطلاعات لازمی را استخراج کنیم. حتی می‌توانیم هر ابزار لازمی را برای نگهداشتن دسترسی خود به سامانه در آینده را بر روی آن نصب نماییم.



در طول فرآیند حمله، ما به دنبال **مخفی‌کردن**[۲] آثار حمله و ردپای خود هستیم. به عنوان مثال شاید نیازمند این باشیم که به این صورت به نظر برسد که حمله از منطقه فیزیکی دیگری در حال انجام است یا اقداماتی را انجام دهیم تا مطمئن شویم که نمی‌توان از آثار حمله به مشخصات ما دست یافت. همچنین در اغلب مواقع نیازمند آن هستیم که ردپا و آثار تمامی فعالیت‌هایی که بر روی سامانه هدف انجام داده‌ایم را هنگام ترک آن از بین ببریم. آنگاه، موقع **یورش**[۳] به سامانه فرا می‌رسد. در نهایت، هم باید به **تثبیت مواضع**[۴] خود در سامانه بپردازیم. (Andress and Winterfeld، ۲۰۱۱: ۲۷)

۱. root
۲. exfiltrate
۳. assault
۴. sustain

۵- دفاع سایبری

دفاع سایبری عبارت است از: قابلیت‌های سازمان‌یافته برای محافظت در مقابل، یا کاهش و بازیابی سریع اثرات حمله سایبری است. (Rauscher and Yaschenko،۲۰۱۱:۵۸)

دفاع سایبری اعمالی است که به وسیله یک طرف ارتباطی انجام می‌شود که دارایی‌هایش را در مقابل وقوع حمله محافظت می‌کند. دفاع مؤثر در سامانه های الکترونیکی نوعاً مبتنی است بر شناسایی، مجزاسازی[۱]، گزارش، بازیابی و خنثی‌سازی[۲]. (سازمان فناوری اطلاعات، ۱۳۹۰: فصل ۶)

مراحل دفاع سایبری

الف- جلوگیری[۳]

عبارت است از شناسایی راه‌های نفوذ وحمله و مقابله با آن جهت افزایش ضریب امنیت، ایمنی و پایداری. از جمله روش های جلوگیری می‌توان به موارد زیر اشاره نمود:

طراحی امن و ایمن و پایدار سامانه‌ها[۴]

در صورتی که امنیت جزو معیارها و اصول طراحی سامانه ها، قرار بگیرد، سامانه ها بسیار امن تر و ایمن تر و پایدارتر از قبل خواهد بود.

متوقف نمودن حملات[۵]

از دیگر راه های جلوگیری از حملات، متوقف نمودن آن می‌باشد این روش از طریق استفاده از تجهیزات پیشرفته امنیتی و وضع قوانین لازم، میسر است.

ب- مدیریت حادثه[۶]، محدود کردن خرابی‌ها[۷]

روش های مدیریت حوادث و محدود نمودن اثرات زیانبار حوادث، راه هایی است که با استفاده از آن می‌توانیم اثر حملات صورت گرفته را در کمترین زمان کاهش دهیم.

۱. isolation
۲. neutralization
۳. Prevention
۴. Embed Security into design
۵. Ban attacks
۶. Incident management
۷. damage limitation

تعیین آثار، نشانه‌ها و هشدارها

بدین معنی که وقتی حمله ای اتفاق می‌افتد، ابتدا در گام اول باید آثار و خطراتی که این حمله می‌تواند داشته باشد را شناسایی کنیم، زیرا با شناسایی آثار یک حمله می‌توانیم از پیامدهای حملات دیگر و خطراتی که ممکن است ایجاد شود، جلوگیری کنیم.

امن، ایمن و پایدار کردن سامانه‌ها[۱]

جهت جلوگیری از نفوذهای بیرونی، ضروری است تا موانعی ایجاد کنیم. از قدیمی‌ترین موانع نفوذ ، استفاده از کلمه عبور است که البته روش های جدیدتر، استفاده از تکنیک هایی ،مانند دیوار آتش یا پروکسی سرور ها[۲] است. البته همان طور که شیوه های رمزنگاری شکست خورده است، شیوه های جدید نیز می‌تواند منجر به شکست شود. در مورد حملات فیزیکی نیز لازم است که ابتدا تمام حملات و نفوذهایی که می‌تواند انجام شود را، شناسایی کنیم. مثلاً در مورد یک شبکه اطلاعاتی، باید راهبرد های فیزیکی مناسب جهت امن، ایمن و پایدار نمودن مراکز داده آن اتخاذ نمود.

خاموشی و تخصیص مجدد[۳]

یک راه حل دیگر این است که سامانه به طور کامل یا به طور جزئی خاموش شود و دوباره تخصیص مجدد شود. سامانه ای که متوجه شود تحت یک حمله قرار دارد، باید موانع و دفاع هایی از خود را بنا نهد که شاید در مواقع عادی از آن استفاده نمی‌کند و سعی کند قسمت هایی از سامانه را که مواجه با حمله شده‌ا، جدا کند. البته مراحل خاموش کردن و تخصیص دهی مجدد باید به صورت بلادرنگ[۴] و به سرعت انجام گیرد.

پ- پشتیبانی[۵]

نکتهٔ قابل توجه این است که باید همواره از اطلاعات جمع‌آوری شده، قبل از هر حمله‌ای پشتیبانی کنیم. این تاکتیک از طریق تهیه نسخه پشتیبان اطلاعاتی که ذخیره شده، به‌دست می‌آید. بسیاری از روش‌های دفاع، نیاز به این دارد که حالت صحیح سامانه قبل از حمله را، جهت تسهیل در بازیابی و طراحی مجدد بدانند. این روش برای مواقعی است که حملات براساس نقطهٔ شروع دقیق و مشخصی انجام می‌شود و پشتیبان‌ها به‌طور منظم ذخیره می‌شود. بسیاری از حملات موذیانه به کندی و به طور محرمانه، مشکلات

۱. harden the system
۲. proxy servers
۳. Shutdown and reallocation
۴. real time
۵. Backup

زیادی را نسبت به زمانی که اطلاعات سالم بود، ایجاد می‌کند (یعنی در اینگونه از حملات ما زمان دقیق سالم‌بودن اطلاعات را نداریم و تاثیر حملات هنوز ایجاد نشده است). در این حالت، جهت ایجاد فضای سالم، سامانه‌های سازمان باید خودشان برنامه‌هایی برای تهیه نسخه پشتیبان داشته باشد. (سازمان پدافند، بی‌تا: ۱۷)

٦- نگاهی به سوابق تهدیدات سایبری

«ال گور» معاون رئیس جمهور آمریکا در سال ۱۹۹۴ اعلام داشت: «ساختار اطلاع رسانی جهانی به پیشبرد دموکراسی کمک می‌کند» و «این زیر ساخت اطلاع رسانی برای اقتصاد دهه ۱۹۹۰ آمریکا ، مانند زیر ساخت حمل و نقل است برای اقتصاد اواسط قرن بیستم کشور» و «دستیابی بدون اعمال هیچ گونه محدویت به این شبکه یکی دیگر از اصول و مهم است.» (کلانتری، بی‌تا: ۱۶)

چند سال بعد در اوایل سال ۱۹۹۶ میلادی شاهد آن هستیم که کنگره آمریکا لایحه‌ای را تصویب می‌کندکه در آن موارد خلاف اخلاق شبکه ارتباطی رو به توسعه اینترنت تحریم می‌گردد. این مصوبه که به لایحه (محجوبیت) یا پاکسازی ارتباطات موسوم گردید به بهانه مغایرت با اولین اصلاحیه پیشنهادی، توسط اتحادیه آزادی‌های مدنی آمریکا در دادگاه فیلادلفیا مورد اعتراض قرار گرفت. (نیوزویک، ۱۹۹۶).

یک نهاد تروریستی اعلام می‌کند که شبکه برق شمال‌غربی اقیانوس آرام را به مدت ۶ ساعت از ساعت ۴ بعدازظهر قطع خواهد کرد و همین تهدید را هم اجرا می کند، سپس همان گروه اعلام می‌کند مدارهای اصلی مخابرات بین شرق و غرب ایالات متحده را به مدت نصف روز از کار خواهد انداخت و همین کار را هم علیرغم کوشش‌های متخصصان جهت مبارزه علیه آنها انجام می‌دهد؛ سپس این گروه تهدید می‌کند سامانه کنترل ترافیک هوایی شهر نیویورک را از کار انداخته، مانع پروازها شده ، مسیر پروازهای داخلی را منحرف می‌سازد و این کار را نیز انجام می دهد. تهدیدها به‌طور پیاپی ادامه یافته، با موفقیت اجرا می‌شود که این نمایانگر توانایی دشمن برای حمله به زیرساخت‌های حیاتی یک کشور در فضای سایبر است. نهایتاً تهدید می‌کند که اگر فهرست خواسته‌هایشان برآورده نشود تجارت الکترونیک و سرویس کارت اعتباری را به وسیله چند صدهزار هویت ربوده شده در میلیون‌ها معامله تقلبی، از کار خواهد انداخت. حال هراس و آشوب و اغتشاش عمومی را پس از این تهدید تجسم کنید. (موحدی‌صفت، ۱۳۸۶: ۲۵۲)

در اکتبر سال ۲۰۰۰ هکرهای رژیم صهیونیستی به سایت‌های حماس و حزب الله حمله کردند و در سامانه‌های آنها مشکلاتی را پدید آوردند و در مقابل نیز هکرهای ضد رژیم صهیونیستی به سایت‌های اسرائیلی حمله کرده ، آن‌ها را با ترافیک قلابی درگیر کردند. آنها سایت کنست (پارلمان اسرائیل)، بانک‌ها، وزرات خارجه و وزارت دفاع اسرائیل را مورد هدف قرار دادند. حملات سایبری علیه جمهوری استونی در سال ۲۰۰۷ میلادی که به مدت ۲۲ روز به طول انجامید نمونه دیگری از این دست حملات بود. طی این

حملات که توسط دولت روسیه صورت پذیرفت بسیاری از اطلاعات دولتی و خصوصی استونی مورد هجوم قرار گرفت. این حملات در واکنش به تصمیم دولت استونی برای تبدیل بنای یادبود جنگ جهانی دوم دولت شوروی به گورستان نظامی انجام گرفت. این تصمیم با انتقاد جمع کثیری از سران روسی و همچنین اقلیتی از روس‌های مقیم در استونی مواجه شد؛ این اقدام نهایتاً منجر به حملات سایبری از سوی روس‌ها شد. در ۲۶ سپتامبر سال ۲۰۰۹ میلادی مسئولان نیروگاه اتمی بوشهر از ویروسی شدن سامانه‌های این نیروگاه به ویروس استاکس‌نت خبر دادند.

ریچارد پرل معاون پیشین وزارت دفاع آمریکا به تولید ویروس استاکس‌نت توسط رژیم صهیونیستی و شکست این برنامه در توقف کار تأسیسات هسته‌ای ایران اعتراف کرد. بعدها لیام مارچو مدیر عملیاتی شرکت سیمنتک با تجزیه و تحلیل برنامه نویسی استاکس‌نت و رمزگشایی کد آن دریافت که به احتمال زیاد متهم پشت پرده حمله به ایران، اسرائیل است. هرچند رایانه‌های نیروگاه اتمی بوشهر از این ویروس پاکسازی شدند، اما این حمله به نیروگاه اتمی بوشهر خود گواهی بر امکان حملاتی از این دست بود. نمونه دیگری از این دست حملات حمله آئورا بود. در سال ۲۰۰۹ میلادی، گوگل و چند شرکت دیگر مورد هجوم حملات سایبری قرار گرفتند که در این سری حملات، هکرها به اطلاعات حیاتی و خصوصی این شرکت‌ها دست پیدا کردند. (Ottis،۲۰۰۸: ۱۶۳-۱۶۸)

۷- ساختار دفاع سایبری در برخی کشورهای جهان

آلمان

دولت آلمان همانند دیگر دولت‌های اروپایی و به طور هماهنگ با آنها درپی چاره اندیشی به مسائل و چالش‌های رو به رشد در زمینه امنیت فضای سایبری می‌باشد و به‌این موضوع به صورت یک موضوع راهبردی می‌نگرد و برای روبرو شدن با مسائل و چالش‌های مذکور اهداف و راهبردهای مختلفی را در سطح داخلی و بین المللی در قالب یک سند راهبرد امنیت سایبری در سال ۲۰۱۱ ترسیم نموده است.

سند راهبرد امنیت سایبری آلمان بر روی چند محور اساسی تمرکز دارد نظیر: محافظت از زیرساخت اطلاعات حیاتی،ایمن سازی و تقویت سامانه‌های فناوری اطلاعات و ارتباطات، شورای ملی امنیت سایبری و مرکز ملی پاسخ سایبری، بهبود اجرای قوانین، افزایش تعاملات بین المللی، اطمینان حاصل نمودن از فناوری اطلاعات قابل اعتماد و آموزش نیروی سایبری.

از جمله موارد مهم دراین سند، ایجاد شورای ملی امنیت سایبر، مرکز ملی پاسخ سایبری و مرکز دفاع سایبری و تقویت ساختارها و تعاملات سازمان‌ها با یکدیگر است.

شورای امنیت سایبری ملی: در کمیساریای فناوری اطلاعات دولت فدرال تاسیس خواهد شد و مسئول اجرای راهبرد امنیت سایبر دولت آلمان خواهد بود.این شورا برای هماهنگ کردن ابزارهای پیشگیرانه و رویکردهای میان رشته‌ای امنیت سایبری بخش عمومی‌و خصوصی عمل خواهد کرد. شورای مذکور، مدیریت فناوری اطلاعات را در سطح فدرال و کار شورای برنامه ریزی فناوری اطلاعات در زمینه امنیت سایبری را در سطح سیاسی و راهبردی تکمیل و به هم پیوند خواهد زد. این شورا متشکل از صدراعظم فدرال و وزارت امور خارجه، و تعدادی از وزارتخانه‌های کلیدی، از جمله وزارت فدرال امور داخله، وزارت دفاع فدرال، وزارت فدرال اقتصاد و فناوری، وزارت فدرال دادگستری، وزارت دارایی و امور مالی، وزارت فدرال آموزش و پرورش و تحقیقات و نمایندگانی از دولت‌های ایالتی خواهد بود و در موارد و مناسبت‌های خاص، وزارتخانه‌های دیگری نیز بدان اضافه خواهد شد. ضمنا نمایندگانی از صنوف مختلف کسب و کار به عنوان اعضای مرتبط و در صورت لزوم نمایندگانی از دانشگاه‌ها در جلسات شورا دعوت خواهند شد.

مرکز ملی پاسخ‌گوئی سایبری: برای بهینه سازی همکاری عملیاتی بین تمام مقامات دولتی و بهبود هماهنگی محافظت وپاسخ گوئی به حوادث فناوری اطلاعات، راه‌اندازی خواهد شد این مرکز به اداره فدرال امنیت اطلاعات[۱] گزارش داده، همکاری مستقیم با اداره فدرال حفاظت از قانون اساسی[۲] و دفتر فدرال حفاظت مدنی و کمک به سوانح[۳] دارد. اداره پلیس جنایی فدرال[۴]، پلیس فدرال[۵]، دفتر جرم‌شناسی گمرکات[۶]، گمرکات[۶]، سرویس اطلاعاتی فدرال[۷]، نیروی دفاع فدرال[۸] و جایگاه‌های نظارت‌کننده بر گردانندگان زیرساخت حیاتی، همه در این مرکز در چارچوب وظایف و اختیارات قانونی خود مشارکت دارند. به اشتراک‌گذاری سریع و نزدیک اطلاعات از ضعف محصولات فناوری اطلاعات، آسیب‌پذیری، شکل‌های حمله و نمایی از مرتکبین این گونه اعمال، مرکز ملی پاسخ‌گوئی سایبری را قادر می‌سازد که حوادث فناوری اطلاعات را تجزیه و تحلیل‌کرده، توصیه‌های تثبیت شده‌ای را برای اقدام فراهم آورد. این مرکز با آمادگی‌های امنیتی از طریق هشدار دهندگی زود هنگام و پیشگیری توصیه‌هایی را به شورای امنیت سایبر ملی به دو صورت منظم یا در شرایط حوادث خاص عرضه می‌دارد. اگر وضعیت امنیت سایبری به سطح یک بحران قریب‌الوقوع یا درحال رخداد رسیده باشد، مرکز ملی پاسخ‌گوئی سایبری به طور مستقیم، کارکنان مدیریت بحران به ریاست مسئول امور برون‌سازمانی در وزارت امور داخله فدرال را مطلع می‌نماید.

۱. BSI: Federal Office for Information Security
۲. BfV: Federal Office for the Protection of the Constitution
۳. BBK: Federal Office of Civil Protection and Disaster Assistance
۴. BKA: Federal Criminal Police Office
۵. BPOL: Federal Police
۶. ZKA: Customs Criminological Office
۷. BND: Federal Intelligence Service
۸. Bundeswehr

مرکز دفاع سایبر ملی آلمان: در آوریل ۲۰۱۱ تحت نظارت و اختیار اداره فدرال امنیت اطلاعات و دخالت مستقیم اداره فدرال حفاظت از قانون اساسی و دفتر فدرال حفاظت مدنی و کمک به سوانح راه اندازی شد. در حال حاضر علاوه بر این سه جایگاه، پلیس جنایی فدرال آلمان، پلیس فدرال، اداره جنایی گمرک، اداره اطلاعات فدرال و نیروهای مسلح فدرال نیز به‌عنوان مقامات مرتبط در این امر مشارکت دارند.

در ۲۶ ماه ژوئن ۲۰۱۱ وزارت کشور فدرال آلمان رسماً مرکز دفاع سایبر ملی را به عنوان بخشی از راهبرد امنیت سایبر جامع خود که توسط دولت فدرال آلمان در تاریخ ۲۳ فوریه ۲۰۱۱ به تصویب رسیده بود در شهر بن افتتاح کرد. این مرکز برای خدمت رسانی به عنوان یک پلت فرم مشترک برای تبادل اطلاعات سریع و هماهنگی بهتر از اقدامات حفاظتی و دفاعی در برابر حوادث امنیتی فناوری اطلاعات در نظر گرفته شده است. ماموریت مرکز دفاع سایبر ملی ، بررسی و ارزیابی سریع حوادث امنیتی فناوری اطلاعات است و به صورت جامع به منظور توسعه توصیه‌هایی برای یک پاسخ ، هماهنگ شده است. برای رسیدن به این هدف، سازمان‌ها اطلاعات آسیب‌پذیری‌های امنیتی در محصولات فناوری اطلاعات را به اشتراک گذاشته ، حوادث امنیتی و حملات فناوری اطلاعات را تجزیه و تحلیل می‌کنند. تمام سازمان‌های درگیر با مرکز بر، اساس اختیارات قانونی موجود می‌باشد. (huntonprivacyblog.com)

سازمان BSI یا دفتر فدرال امنیت فناوری اطلاعات: در تاریخ ۱ اوت ۲۰۰۱ بنا بر اقدام وزیر فدرال داخله آلمان ایجاد شد، این سازمان اغلب به عنوان آژانس امنیت اطلاعات آلمان[۱] نامیده می‌شود و یک سازمان دولتی و مسئول مدیریت امنیت رایانه و ارتباطات برای دولت آلمان می‌باشد. حوزه تخصص و مسئولیت این سازمان عبارت است از: امنیت برنامه‌های کاربردی رایانه، حفاظت از زیرساخت‌های حیاتی، امنیت اینترنت، رمزنگاری، مقابله با استراق سمع، صدور گواهینامه محصولات امنیتی و اعتباربخشی آزمایشگاه‌های امنیتی. این سازمان در بن مسقر است و بالغ بر ۴۰۰ کارمند دارد و رئیس فعلی آن، از ۱۶ اکتبر ۲۰۰۹، ریاضیدان مایکل هنگ[۲] می‌باشد. این سازمان تقریبا نقشی مشابه نقش بخش امنیت رایانه آزمایشگاه فناوری اطلاعات از موسسه بین‌المللی استاندارد و فناوری[۳] ایالات متحده امریکا را داراست. (en.wikipedia.org)

واحدهای نظامی‌آلمان و سازمان‌های اطلاعاتی مولفه‌های سایبری دارند. سازمان امنیتی آلمان در حوزهٔ تحقیقات و توسعهٔ توانایی‌های سایبری در حال سرمایه گذاری است. بخش عملیات شبکه رایانه ای و اطلاعات، درون واحد شناسایی راهبردی، به وسیلهٔ یک ژنرال[۴] از نیروی هوایی و با ۷۶ عضو نظامی از بخش‌های علوم رایانه ای رهبری می‌شود و هر دو توانایی دفاعی و تهاجمی‌را توسعه خواهد داد.

۱. GISA
۲. Michael Hange
۳. NIST: National Institute of Standards and Technology
۴. Brigadier

از آنجا که بیشتر حملات در حال حاضر جنبه اقتصادی دارد همچنین یک نیروی کاری جدید تحت عنوان «امنیت فناوری اطلاعات در کسب و کار« در دولت آلمان آغاز به کار کرده است. (سازمان فناوری اطلاعات، ۱۳۹۰: فصل ۶)

آمریکا

کشور آمریکا از سال‌ها پیش با توجه به تعریف فضای سایبری و تهدیدات آن اقدام به تشکیل واحدهای مختلفی برای دفاع در برابر حملات سایبری نموده است. طی تحقیقات به عمل آمده، در کشور آمریکا مسوولیت دفاع سایبری در بخش نظامی بر عهده سازمان فرماندهی سایبری‌ایالات متحده[۱] می‌باشد. ماموریت این سازمان برقراری امنیت فضای سایبر برای ارتش آمریکا، وزارت دفاع و همچنین برقراری امنیت و آزادی ایالات متحده و هم‌پیمانانش در فضای سایبر می‌باشد.(U.S. Cyber Command Fact Sheet, ۲۰۰۵)

علاوه براین سازمان دو سازمان از جامعه‌ی اطلاعاتی آمریکا (آژانس امنیت ملی[۲] و پلیس فدرال[۳]) و یک اداره از وزارت امنیت داخلی[۴] نیزدر زمینه‌ی دفاع و امنیت فضای سایبر فعالیت دارند. همچنین رییس فرماندهی اطلاعات ملی به عنوان هماهنگ کننده و مشاور رییس جمهور در حوزه دفاع سایبری ایفاء نقش می‌نماید. از نظر ساختار سازمانی، فرماندهی سایبری یکی از زیر مجموعه‌های فرماندهی راهبردی ایالات متحده[۵] می‌باشد. فرماندهی راهبردی یکی از ده فرماندهی اصلی وزارت دفاع آمریکا می‌باشد. فرماندهی سایبری شامل فرماندهی سایبری نیروی زمینی، فرماندهی سایبری نیروی دریایی، فرماندهی سایبری نیروی هوایی و فرماندهی سایبری تفنگداران دریایی می‌باشد.

بر مبنای قانون ایالات متحده‌ی آمریکا، ریاست فرماندهی سایبری ارتش و فرماندهی آژانس امنیت ملی و سرویس امنیت مرکزی[۶] درایالت متحده باید به صورت مشترک به یک نظامی با حداقل درجه‌ی سرلشگری[۷] سپرده شود.(STRATEGIC AND INTERNATIONAL STUDIES, ۲۰۱۰)

۱. United State Cyber Command

۲- NSA-National Security Agency آژانس امنیت ملی (مسوولیت شنود سیگنال و حفاظت از سیگنال را در کشور ایالات متحده‌ی آمریکا بر عهده دارد.)

۳- FBI-Federal Bareau of investigation پلیس فدرال آمریکا، مسوولیت مبارزه با جرائم سازمان یافته و تروریسم را برعهده دارد.

۴. DHS-Department of Homeland Security

۵. United State Strategic Command

۶. CSS-Central Security Service

۷- ژنرال سه ستاره که به آن (Lieutenant General) می‌گویند و معادل درجه‌ی سرلشگری در ایران است.

بنابراین شخص فوق دارای مقام بالایی در سازمان‌های اطلاعاتی بوده ، با توجه به در اختیار داشتن سمت ریاست سرویس امنیت مرکزی که مرکز اطلاعاتی وزارت دفاع آمریکا است، می‌توان گفت مرکزیت اطلاعات ارتش آمریکا را بر عهده دارد و یکی از عناصر مهم در ساختار اطلاعاتی ایالات متحده می‌باشد.

بخش‌های فعال در حوزهٔ امنیت و دفاع سایبر در آمریکا

ایالات متحده‌ی آمریکا وظایف مرتبط با دفاع سایبری را در وزارت دفاع، مرکز امنیت سایبری ملی از وزارت امنیت داخلی[۱] و وزارت دادگستری تقسیم کرده است. در بخش وزارت دفاع، فرماندهی سایبری نیروهای مسلح وظیفه‌ی حفاظت از اطلاعات و شبکه‌های ارتباطی نیروهای مسلح از میادین جنگ تا ستاد فرماندهی را بر عهده دارد و همچنین در صورت لزوم و با دستور ریاست جمهوری این فرماندهی باید توانایی حمله‌ی سایبری به کشور(های) مورد نظر را داشته باشد. به علاوه، آژانس امنیت ملی نیز در وزارت دفاع آمریکا وظیفه‌ی شنود سیگنال و حفاظت سیگنال را بر عهده دارد که شامل برقراری امنیت شبکه‌های رایانه‌ای نیز می‌باشد. این سازمان وظیفه‌ی تحقیق و توسعه در زمینه‌ی امنیت و رمزگذاری و همچنین ابلاغ استانداردهای امنیتی، نظارت و بررسی سطح امنیتی تمامی سازمان‌های فدرال را بر عهده دارد. تمامی سازمان‌های فعال در زمینه‌ی دفاع سایبری ارتباط نزدیکی با آژانس امنیت ملی دارند. وزارت امنیت داخلی مسوولیت اجرایی امنیت غیرنظامی سایبری کشور را بر عهده دارد که در بخش امنیت سایبری ملی به انجام می‌رسد. این وظیفه شامل مرکز امداد و نجات رایانه‌ای[۲] ملی، سامانه‌های تشخیص نفوذ و مقابله با نفوذ و همچنین سامانه‌های آگاهی موقعیتی می‌باشد. پلیس فدرال از وزارت دادگستری نیز در موارد جرائم مرتبط با فضای سایبر و همچنین جرائم سایبری و پیگیری مجرمین با وزارت امنیت داخلی همکاری می‌نماید. هماهنگی تمامی این سازمان‌ها در زمینه‌ی امنیت سایبری توسط هماهنگ‌کننده‌ی ستاد عملیاتی فضای سایبری انجام می‌گیرد که به عنوان معاون رییس جمهور در زمینه‌ی امنیت سایبری می‌باشد. (سازمان فناوری اطلاعات، ۱۳۹۰: فصل ۶)

انگلیس

برابر بررسی‌های به آمده در انگلستان، دو نهاد اصلی جدید برای مسائل سایبری در سال ۲۰۱۰ ایجاد شد، دفتر امنیت سایبر[۳] و مرکز عملیات امنیت سایبری[۴]. دفتر امنیت سایبری در دفتر کابینه مستقر است و متولی امنیت سایبری راهبردی بریتانیا است و رهبری راهبردی امنیت سایبری در کل دولت و سراسر ادارات

۱. National Cyber Security Center of DHS
۲. CERT-Computer Emergency Response Team مرکز امداد و نجات رایانه‌ای
۳. OCS: Office of Cyber Security
۴. CSOC: Cyber Security of operation Centre

آن را به عهده دارد، و مرکز عملیات امنیت سایبری پایش و هماهنگی[۱] پاسخ به حادثه را فراهم می‌کند[۲]. وظایف اصلی این مرکز نظارت بر تحولات در فضای سایبر، (نهایتاً سطح آگاهی موقعیتی[۳] جمعی را فراهم می‌آورد.) تجزیه و تحلیل روندها، و بهبود هماهنگی پاسخ‌های فنی به حوادث سایبری می‌باشد.

علاوه بر این، تعدادی از سازمان‌ها در حال حاضر برای محافظت از تهدیدات سایبری انگلستان در حال فعالیت می‌باشند، از جمله گروه امنیت ارتباطات و الکترونیک[۴]، مرکز حفاظت از زیر ساخت های ملی[۵] و دیگر سازمان‌های مرتبط نظیر دفتر کابینه، اداره رسیدگی به جرایم سازمان یافته[۶]، پلیس و....

گروه امنیت ارتباطات و الکترونیک قدرت و تصدی ملی امور فنی در تضمین اطلاعات را فراهم می‌آورد و تیم واکنش اضطراری رایانه‌ای[۷] را اداره می‌کند، و هشدارها، اعلام خطر و کمک رسانی در حل و فصل جدی حوادث فناوری اطلاعات برای بخش عمومی‌فراهم می‌آورد.

سازمان مرکز حفاظت از زیر ساخت‌های ملی است که بر روی توصیه‌های امنیتی حفاظتی برای سازمان‌ها و کسب و کارهای مرتبط با زیرساخت‌های حیاتی ملی فعالیت می‌نماید و همکاری نزدیکی با گروه امنیت ارتباطات و الکترونیک دارد و نقش هماهنگی درپاسخ گوئی به حوادث امنیتی را برای حرفه ها و سازمان‌هایی که زیرساخت‌های حیاتی ملی بریتانیا را تشکیل می‌دهند ایفا می‌نماید. این سازمان در ۱ فوریه ۲۰۰۷، از ادغام مرکز هماهنگی زیرساخت‌های امنیت ملی[۸] و بخشی از سرویس امنیتی بریتانیا[۹]، و مرکز مشاوره امنیت ملی[۱۰] ایجاد گردید. واحد مرکز هماهنگی زیرساخت‌های امنیت ملی مسئولیت ارائه مشاوره و اطلاعات مربوط به شبکه‌های رایانه ای دفاعی و مسائل مربوط به تضمین اطلاعات غیر رایانه‌ای را عهده دار بود و مرکز مشاوره امنیت ملی مسئولیت ارائه مشاوره در مورد امنیت فیزیکی و مسائل امنیتی کارکنان را به عهده داشت. سازمان حفاظت از زیر ساخت های ملی از نظر ساختاری یک سازمان بین اداره‌ای، با منابعی از تعدادی از ادارات و سازمان‌های دولتی، مانند سرویس امنیتی بریتانیا، گروه امنیت ارتباطات و الکترونیک و دیگر سازمان‌های مسئول زیر ساخت‌های حیاتی است. این سازمان به مدیر کل سرویس امنیتی بریتانیا پاسخ گو است و تحت قانون سرویس امنیتی ۱۹۸۹عمل می‌نماید.

۱. Monitoring and Coordinating
۲. Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space published by TSO
۳. situational awareness
۴. CESG -Communications-Electronics Security Group(سازمان فنی ملی برای تضمین اطلاعات (زیرمجموعه می‌باشد.
۵. CPNI -Centre for the Protection of National Infrastructure مرکز حفاظت از زیر ساخت های ملی
۶. SOCA: Serious Organised Crime Agency
۷. Gov Cert UK
۸. NISCC
۹. MI۵
۱۰. NSAC

در موضوع دفاع سایبری، انگلستان تصمیم به تشکیل یک گروه عملیات دفاع سایبری جدید در وزارت دفاع گرفته است. این گروه با عنوان فرماندهی نیروهای مشترک و تحت رهبری یک افسر نظامی چهار ستاره در آوریل ۲۰۱۲ شروع به کار خواهد کرد، و تاکتیک‌های جدید، تکنیک‌ها و طرح‌هایی را برای ارائه قابلیت‌های سایبری نظامی‌توسعه خواهد داد و هدایت توسعه و یکپارچه‌سازی قابلیت‌های دفاع سایبری رابه عهده خواهد گرفت. (cabinetoffice.gov.uk)

فرانسه

راهبرد جدید دفاع و امنیت ملی فرانسه[۱] در سال ۲۰۰۸ منتشر گردید. دراین سند تهاجمات سایبر یکی از تهدیدات اصلی قلمرو ملی قلمداد گردیده ، ممانعت و عکس العمل فناوری های ارتباطات و اطلاعات در مقابل تهاجمات سایبر به عنوان یکی از اولویت‌های اصلی نهاد امنیت ملی تعیین شده است.

جهت اجرائی شدن اهداف ترسیم شده در سند ر اهبرد، سازوکارهای جدیدی و از جمله سازماندهی مجدد دفاع امنیت ملی طراحی و ابلاغ گردیده است. بر اساس تدابیر اخذ شده، شورای دفاع امنیت ملی[۲] ایجاد گردیده است.

ساختار سیاست‌گذاری و اجرایی امنیت سایبر فرانسه

آژانس امنیت اطلاعات و شبکه فرانسه[۳]، زیر نظر نخست وزیر و دبیر خانه عمومی‌دفاع و امنیت ملی[۴] سازماندهی شده است. این آژانس در سال۲۰۰۹ با مسئولیت امنیت فناوری اطلاعات فرانسه تشکیل گردید.اختیارات و مسئولیت‌های آژانس امنیت اطلاعات و شبکه فرانسه از سال ۲۰۱۱ با حکمی‌که در خصوص مسئولیت دفاع ملی از ریاست جمهور دریافت نموده است بسیار گسترده‌تر شده ، هم اکنون این نهاد با مسئولیت کامل امنیت فضای سایبر، متولی ملی در دفاع سامانه‌های اطلاعاتی، مسئولیت محافظت از زیر ساخت حیاتی[۵] مهم ترین نهاد امنیت فضای سایبر فرانسه محسوب می‌گردد. این آژانس علاوه بر وظائف کلان ستادی نظیر سیاست گذاری ، تدوین خطوط راهنمای ملی، امور اجرائی مرتبط با مخاطرات سایبر سطح ملی را نیز به عهده دارد.این آژانس در حال تجهیز، به عنوان یک اطاق عملیات و منطبق با چالش‌های پیش روی فرانسه است. یکی از اساسی‌ترین ماموریت‌های این آژانس، پاسخ‌گوئی به بحران‌های اصلی تاثیرگذار، یا تهدید آمیز امنیت سامانه‌های اطلاعاتی، مدیران یا مجریان زیر ساخت‌های حیاتی کشور

۱. NSD: national security directive
۲. CDSN
۳. ANSSI: Agence Nationale de la Sécurité des Systèmes dInformation- French Network and Information Security Agency
۴. SGDSN: Secrétariat Général de la Défense et de la Sécurité Nationale
۵. CIP: Critical Infrastructure Protection

است. تشکیل مرکز عملیات امنیت سامانه اطلاعات[۱] که معادل مرکز عملیاتی امنیت سایبر[۲] در سایر کشورها می‌باشد اصلی‌ترین ابزار اجرائی آژانس امنیت اطلاعات و شبکه فرانسه می‌باشد. گروه پاسخ‌گوئی به فوریت‌های رایانه‌ای دولتی فرانسه در داخل مرکز عملیات امنیت سامانه اطلاعات سازماندهی شده است.

اخیراً آژانس دفاع سایبر با ماموریت سازماندهی و اجرای جنگ سایبر در تابعیت وزارت دفاع تشکیل شده است. گرچه اطلاعات بسیار ناچیزی از ماهیت واقعی، ابعاد و سازماندهی آژانس دفاع ملی و حد فصل آن با آژانس امنیت اطلاعات و شبکه فرانسه منتشرشده است اما به نظر می‌رسد که وظائف دفاع سایبر ملی به مفهوم دفاع از منافع غیرنظامی ملی و زیرساخت‌های حیاتی در وحله اول به عهده آژانس امنیت اطلاعات و شبکه فرانسه قرار گرفته است و در صورتی که ابعاد تهاجمات سایبر از حد معینی تجاوز نموده ، یا آژانس امنیت اطلاعات و شبکه فرانسه جهت مواجهه با تهدیدات به کمک و مساعدت نیازداشته باشد از ظرفیت‌های اژانس دفاع سایبر نیز بهره مند خواهد شد. گرچه درحال حاضر به نظر نمی‌رسد که آژانس دفاع سایبر با توجه به جدید التاسیس بودن آن، ظرفیت مازادی بر آژانس امنیت اطلاعات و شبکه فرانسه داشته باشد. درصورتی که به هر دلیل آژانس دفاع ملی بخواهد از ظرفیت‌های غیرنظامی و از جمله آژانس امنیت اطلاعات و شبکه فرانسه استفاده نماید موارد را از طریق دبیر خانه عمومی دفاع و امنیت ملی هماهنگ می‌نماید. مباحث مرتبط با آفند سایبر تنها در وزارت دفاع (ستادمشترک ونیروها) مدیریت شده، آژانس امنیت اطلاعات و شبکه فرانسه نقشی در آن ندارد.

ساختار دفاع سایبر ملی فرانسه

علاوه بر نهادهای مذکور سایر نقش آفرینان اصلی حوزه دفاع سایبر فرانسه عبارتند از: متولی محافظت داده فرانسه[۳]، دفتر مرکزی برای مبارزه با جرم مرتبط با فناوری اطلاعات و مخابرات[۴]، نمایندگی کاربرد اینترنت، شبکه امن اینترنت[۵]، مرکز امنیت اطلاعات فرانسه[۶]، یک شبکه تحقیقاتی مخابرات راه دور ملی، رصد خانه امنیت شبکه و سامانه‌های اطلاعاتی[۷] و پروژه امنیت برنامه‌های کاربردی تحت وب متن باز[۸]. (Renater.Fr)

۱. COSSI: Centre Opérationnel de la Sécurité des Systèmes d'Information
۲. CSOC: Syber security operational center
۳. CNIL: Commission Nationale de l'Informatique et des Libertés– French Data Protection Authority
۴. OCLCTIC: Office Central de Lutte contre la Criminalité liée aux Technologies de l Information et de la Communication– Central Office for the Fight against Crime Related to Information Technology and Communication
۵. INTERNET SAFE
۶. CLUSIF: Club de la Sécurité de l'Information Français– French Information Security Club
۷. OSSIR: Observatoire de la Sécurité des Systèmes d'Information et des Réseaux–Observatory of Information Systems and Network Security
۸. OWASP: Open Web Application Security Project

۸- ساختار دفاع سایبری در ایران

مرکز بررسی تهدیدات سایبری

مرکز بررسی تهدیدات سایبری سپاه پاسداران انقلاب اسلامی به منظور شناسایی و انهدام جرایم سازمان‌یافته اجتماعی، اقتصادی، جاسوسی، فرهنگی و تروریستی در فضای مجازی و ساماندهی و هدایت فعالیت‌ها در اینترنت جهت مقابله با تهدیدات فضای مجازی، تمام فعالیت‌های معاند را رصد و با توجه به ماهیت تهدید، اقدامات لازم را انجام می‌دهد. مانند نابودی سرورها، عملیات نفوذ و هک سایت‌های غیر اخلاقی و مورد حمایت غرب و ناامن کردن فضا برای معاندان و شناسایی و دستگیری مجرمان در داخل و خارج از کشور. (شریعت‌پناه، ۱۳۸۹: ۱۶)

پلیس فتا

ایجاد امنیت و کاهش مخاطرات برای فعّالیّت‌های علمی، اقتصادی، اجتماعی در جامعه‌ی اطّلاعاتی، حفاظت و صیانت از هویت دینی و ملّی، مراقبت و پایش از فضای تولید و تبادل اطّلاعات برای پیش‌گیری از تبدیل شدن این فضا به بستری برای انجام هماهنگی‌ها و عملیات برای انجام و تحقّق فعّالیّت‌های غیرقانونی و ممانعت از تعرّض به ارزش‌ها و هنجارهای جامعه در فتا از جمله‌ی وظایف و مأموریت‌های پلیس فضای تولید و تبادل اطّلاعات ناجاست. (syberpolice.ir)

دادسرای جرایم رایانه‌ای

جرایمی که دادسرای جرایم رایانه‌ای به آن رسیدگی می‌کند، پیش از این به صورت پراکنده در دادسراهای مختلف مانند دادسرای انقلاب، دادسرای ویژه امنیت، دادسرای ارشاد و برخی دیگر از دادسراها مورد رسیدگی قرار می گرفت. شرح وظایف و احکامی که برای مجتمع قضایی رسیدگی به جرائم رایانه‌یی متشکل از سه عضو اصلی و سه عضو علی‌البدل در نظر گرفته شده این است که می‌تواند برای افراد و اشخاص حکم قضایی صادر کند و نیروی انتظامی به عنوان بازوی اجرایی در این زمینه فعالیت می‌کند. (ilaw.ir)

معاونت رسانه و فضای مجازی صدا وسیما

با ابلاغ مقام معظم رهبری صدا و سیما یک معاونت به نام معاونت رسانه‌های مجازی در سال ۱۳۸۹ با هدف جبران عقب‌ماندگی‌های تولید محتوا در حوزه رسانه ایجاد نمود. در راستای ماموریت سازمان صدا و

سیما مصرح در سند افق رسانه و هم سو با چشم‌انداز سازمان در افق ده ساله آینده مندرج در همان سند و برای تحقق راهبردهای پنج ساله دوم «معاونت رسانه های مجازی» تشکیل گردیده است.

ایجاد رسانه کارآمد و موثر مبتنی بر فناوری‌های نوین در محیط‌های مجازی و اینترنت و تأمین و تولید محتوای ارزشمند و مورد نیاز اقشار مختلف جامعه به شیوه مشارکتی با مخاطبان از جمله ماموریت‌های معاونت رسانه و فضای مجازی می‌باشد. (eirib.ir)

سازمان پدافند غیرعامل در حوزه فناوری اطلاعات

سیاست‌گذاری، هدایت، نظارت راهبردی و توسعه امنیت، ایمنی و پایداری فضای تبادل اطلاعات کشور و پشتیبانی از برنامه دستگاه‌ها و بخش‌های زیرساختی در جهت کاهش آسیب در برابر تهدیدات و جنگ از طریق ساماندهی و به کارگیری منابع و ظرفیت‌های ملی از وظایف سازمان پدافند غیر عامل است. (سازمان پدافند غیرعامل، بی‌تا: ۱۰)

قرارگاه دفاع سایبری

تشکیل این قرارگاه در راستای سیاست‌های کلی در بخش امنیت فضای تولید و تبادل اطلاعات است که توسط مقام معظم رهبری ابلاغ شده است و از جمله ماموریت‌های آن عبارت است از: رصد تهدیدات سایبری علیه زیرساخت‌های امنیت ملی کشور، اجرایی شدن سیاست‌های نظام در بخش فتا، اعلام هشدارهای ملی در برابر تهدیدات امنیتی کشور، ایمن سازی زیرساخت‌های کشور نسبت به تهدیدات سایبری و ایجاد توان بازدارندگی در حوزه سایبری، تدوین سند دفاع غیرعامل و تهیه برنامه جامع دفاع سایبری. (ماهنامه دنیای مخابرات و ارتباطات،۱۳۸۹: ۴۱)

شورای عالی فضای مجازی

حضرت آیت‌الله خامنه‌ای رهبر معظم انقلاب در تاریخ ۱۳۹۰/۱۲/۱۷ دستور تشکیل شورای عالی فضای مجازی به ریاست رئیس‌جمهور، صادر نمودند. در این دستور آمده است: «گسترش فزاینده فناوری‌های اطلاعاتی و ارتباطاتی شبکه‌ی جهانی اینترنت و آثار چشمگیر آن در ابعاد زندگی فردی و اجتماعی، و لزوم سرمایه گذاری وسیع و هدفمند در جهت بهره گیری حداکثری از فرصت‌های ناشی از آن در جهت پیشرفت همه جانبه کشور و ارائه خدمات گسترده و مفید به اقشار گوناگون مردم و همچنین ضرورت برنامه‌ریزی و هماهنگی مستمر به منظور صیانت از آسیب‌های ناشی از آن اقتضا می‌کند که نقطه‌ی کانونی متمرکزی برای سیاست‌گذاری، تصمیم‌گیری و هماهنگی در فضای مجازی کشور به‌وجود آید. به این مناسبت شورای

عالی فضای مجازی کشور با اختیارات کافی به ریاستِ رئیس جمهور تشکیل می‌گردد و لازم است به کلیه‌ی مصوبات آن ترتیب اثر قانونی داده شود.»

۹- تجزیه و تحلیل

کشورها به کمک ساختار دفاعی منسجم اشراف اطلاعاتی لازم را در فضای سایبر فراهم می‌آورند. در کشور ما با ایجاد مراکزی، مانند مرکز بررسی تهدیدات سایبری (سپاه پاسداران)، پلیس فتا(ناجا)، دادسرای جرایم رایانه‌ای (قوه قضائیه)، معاونت رسانه و فضای مجازی (صدا و سیما)، سازمان پدافند غیرعامل (ستاد کل)، کمیته پدافند غیرعامل (دولت)، قرارگاه دفاع سایبری (ستاد کل) و شورای عالی فضای مجازی، گام‌های موثری در کاهش تهدیدات سایبری برداشته شده است، اما به نظر می رسد که در این میان یگانی که حوزه ماموریتی آن مشخصاً فضای سایبر بوده، تا امور حمله و دفاع سایبری را در سطح کشور بین سازمان‌های اجرائی، هماهنگ نموده ، مدیریت نماید به چشم نمی‌خورد. تا علاوه بر دفاع در برابر حملات سایبری، حمله به زیرساخت‌های سایر کشورها را طراحی و نظارت نماید.

همچنین ضرورت دارد نیروهای مسلح جمهوری اسلامی ایران متناسب با رویکرد کشورهای فرا منطقه‌ای، خود را با یک ساختار منطقی مجهز به علوم دفاع و حمله در حوزه سایبر نمایند و در این زمینه بایستی از کلیه ظرفیت‌های کشور در این زمینه استفاده نموده تا به قدرت بازدارندگی سایبری نایل گردیم.

در جدول زیر اقدامات اساسی کشورها در حوزه سایبر نشان داده شده است. با بررسی اجمالی مشخص می‌گردد که در تمام کشورها، مرکزی وجود دارد که کلیه امور سایبری (اعم از حمله و دفاع سایبری) را هماهنگ و هدایت می‌نماید و تحت نظر بالاترین شخص مملکت اداره می‌شود.

جدول۱- اقدامات اساسی کشورها در حوزه سایبر

کشور	اقدامات اساسی حوزه سایبر
آلمان	۱- ترسیم سند راهبرد امنیت سایبری در سال ۲۰۱۱ ۲- ایجاد شورای ملی امنیت سایبر(زیر نظر صدر اعظم آلمان) ۳- ایجاد مرکز ملی پاسخ سایبری ۴- ایجاد مرکز دفاع سایبری ۵- ایجاد آژانس امنیت اطلاعات آلمان ۶- ایجاد ساختار سایبری در واحدهای نظامی‌آلمان و سازمان‌های اطلاعاتی
آمریکا	۱- هماهنگ‌کننده‌ی ستاد عملیاتی فضای سایبری(زیر نظر رئیس جمهور) ۲- سازمان فرماندهی سایبری‌ایالات متحده (فرماندهی سایبری نیروی زمینی، فرماندهی سایبری نیروی دریایی، فرماندهی سایبری نیروی هوایی و فرماندهی سایبری تفنگداران دریایی) ۳- آژانس امنیت ملی(مسوولیت شنود سیگنال و حفاظت از سیگنال را در کشور ایالات متحده‌ی آمریکا بر عهده دارد.) ۴- پلیس فدرال آمریکا (مسوولیت مبارزه با جرائم سازمان یافته و ترورسیم را بر عهده دارد). ۵- اداره ارتباطات و امنیت سایبری ۶- بخش امنیت سایبری ملی
فرانسه	۱- ترسیم سند دفاع و امنیت ملی فرانسه(رویکرد تهدیدات سایبری) ۲- شورای دفاع و امنیت ملی سایبری(زیر نظر رئیس جمهور) ۳- آژانس امنیت اطلاعات و شبکه فرانسه ۴- مرکز عملیات امنیت سامانه اطلاعات ۵- آژانس دفاع سایبر ۶- دفتر مرکزی برای مبارزه با جرم مرتبط با فناوری اطلاعات و مخابرات ۷- مرکز امنیت اطلاعات فرانسه
انگلیس	۱- دفتر امنیت سایبر(در دفتر کابینه) ۲- مرکز عملیات امنیت سایبری.(یکی از سه سازمان اطلاعاتی بریتانیا و بخشی از ماشین اطلاعاتی ملی بریتانیا است) ۳- گروه امنیت الکترونیک وارتباطات ۴- مرکز حفاظت از زیر ساخت‌ها ۵- اداره رسیدگی به جرایم سازمان یافته ۶- گروه عملیات دفاع سایبری

۱۰- یافته‌های تحقیق

در زمینه ساختار دفاع سایبری علاوه بر تحقیقات کتابخانه‌ای و مطالعات تطبیقی، با ۸ نفر از کسانی که می‌توانستند ما را در مورد ساختار دفاع سایبری یاری نمایند، مصاحبه گردید که همگی به نامناسب بودن ساختار کنونی اذعان داشته ، ضمن برشمردن ایرادت ساختار فعلی، پیشنهاداتی را جهت برطرف نمودن آن ارائه نمودند، که در زیر نظرات آنان به صورت جمع‌بندی شده و بر اساس فراوانی موضوعات مطرح شده و اهمیت آن‌ها، آورده می‌شود.

الف: ایرادات ساختار فعلی

۱- عدم هماهنگی لازم بین بخش‌های مختلف فعال در حوزه سایبر.
۲- موازی کاری در اجرای مسئولیت‌های دفاع سایبری.
۳- عدم اجرای برخی از ماموریت‌ها به علت روشن نبودن مسئولیت‌ها در این حوزه.
۴- پاسخ‌گو نبودن سازمان‌های مرتبط در مواقع لزوم.
۵- نبود نظام مناسب جهت شناسائی تهدیدات، آسیب‌پذیری‌ها و خطرات حوزه سایبر.
۶- هدر دادن منابع و امکانات سایبری.
۷- مشخص نبودن سیاست‌ها و راهبردهای حوزه سایبر.
۸- عدم استفاده سازمان‌ها از تجربیات همدیگر.
۹- عدم وجود وحدت فرماندهی.

ب: پیشنهادات جهت بهینه نمودن ساختار فعلی

۱- ایجاد سازمان دفاع سایبری تحت نظر بالاترین مرجع اجرائی و مدیریتی کشور.
۲- ایجاد مرکز آموزش دفاع سایبری در کشور.
۳- ایجاد قسمتی در کشور به منظور تعامل بخش خصوصی با بخش دولتی در راستای دفاع سایبری.
۴- ایجاد مرکز نظارت و سیاستگذاری در حوزه سایبر.
۵- ایجاد مرکز مطالعات سایبری.

۱۱- نتیجه‌گیری

بی‌شک فضای سایبر در حال تبدیل شدن به یک میدان جدید به منظور پیگیری عملیات‌های نظامی است و به اعتراف کارشناسان نظامی فضای سایبر به عنوان پنجمین عرصه نبردهای نظامی در حال ظهور

است. از آنجا که بخش اعظم چنین حملاتی از طریق بستر اینترنت و شبکه‌های به هم پیوسته رایانه‌ای صورت می‌پذیرد لذا رصد فعالیت کاربران در این فضا از اهمیت زیادی برخوردار است.

لذا ساختار زیر جهت دفاع سایبری پیشنهاد می‌گردد:

با توجه اینکه مقام معظم رهبری(مدظله‌العلی) شورای عالی فضای مجازی را به ریاست بالاترین مقام اجرائی کشور یعنی رئیس جمهور تشکیل داده‌اند و مسئولین و متخصصین مرتبط با حوزه سایبر در آن عضو می‌باشند، یک سازمان دفاع سایبری زیر نظر این شورا تشکیل گردیده تا بر کلیه امور دفاع سایبری اعم از هماهنگی، سیاست‌گذاری ،نظارت، ارزیابی و ....احاطه کامل داشته تا حفاظت مناسب در برابر تهدیدات حوزه سایبر، در کشور به وجود آید. یادآوری این نکته لازم است که این شورا در تعامل کامل با سیاست‌های شورای عالی امنیت ملی باید باشد و مواردی که به امنیت ملی کشور برمی‌گردد با این شورا هماهنگ بوده تا مشکلی از این لحاظ متوجه کشور نگردد. البته چون ریاست هر دو شورا با رئیس جمهور می‌باشد این هماهنگی به خودی خود اتفاق خواهد افتاد ولی در عین حال باید اعضای شورای عالی مجازی متوجه این موضوع باشند.

پس از جمع‌بندی تحقیقات ومصاحبه‌های انجام شده با صاحب‌نظران،ساختاراولیه برای سیاست گذاری، هماهنگی و نظارت بر سازمان‌هائی که در حوزه سایبر هر کدام بخشی از دفاع سایبری را انجام می‌دهند، ترسیم و مجدداً در معرض خبرگی گذاشته شد و در نهایت نتیجه گرفته شد که این سازمان باید دارای قسمت‌های زیر باشد تا ساختار بهینه و مناسبی در حوزه دفاع سایبری داشته باشیم:

۱- مرکز سیاست گذاری حوزه سایبر: این مرکز مسئولیت هماهنگی، سیاست‌گذاری، تدوین آیین‌نامه‌ها، صدور بخشنامه‌ها، مشخص‌کردن مسئولیت‌های بخش‌های مختلف حوزه سایبر، تعیین وظایف، برنامه‌ریزی، و.... را بر عهده خواهد داشت.

۲- مرکز نظارت بر دفاع سایبری: این مرکز مسئولیت نظارت و ارزیابی فعالیت‌ها و اقدامات دفاع سایبری در کل کشور را به منظور هر چه بهتر انجام شدن عملیات‌های سایبری بر عهده خواهد داشت.

۳- مرکز آموزش عالی دفاع سایبری: این مرکز مسئولیت آموزش کلیه دست‌اندرکاران حوزه سایبر را که به نحوی در این حوزه مشغول فعالیت می‌باشند را عهده دار خواهد بود.

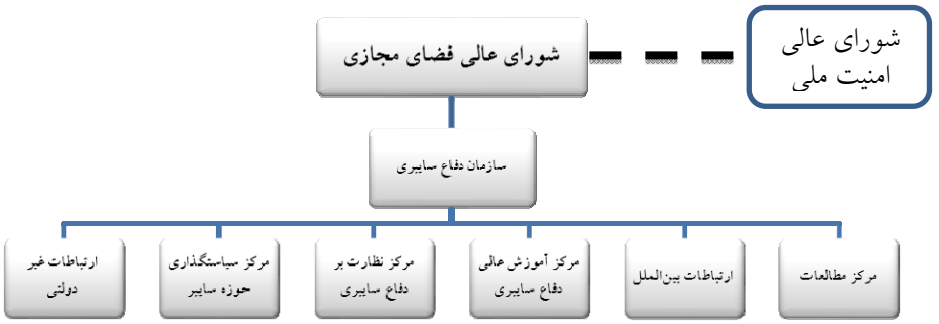
۴- مرکز مطالعات: این مرکز مسئولیت مطالعات سایبری را دارا بوده تا با توجه به پیشرفت علوم سایبری در جهان و بروز تهدیدات جدید در این حوزه، آگاهی کامل از نحوه اقدامات دشمنان را پیدا نموده ، راه‌کارهای اقدام بر علیه این تهدیدات را ارائه می‌نماید.

۵- ارتباطات بین‌الملل: این قسمت با توجه به سه رویکرد دوست، دشمن و رقیب اقدامات خود را در این حوزه طرح ریزی و به انجام می‌رساند و با تعاملات حداکثری با کشورهای دوست، اقدامات سیاسی

مناسب را در نظام بین‌الملل بر علیه کشورهای دشمن اتخاذ و کلیه حرکات رقیب را تحت نظر داشته ، دنبال می‌نماید.

۶- ارتباطات غیردولتی: این قسمت مسئول ارتباط با بخش‌های غیر دولتی در داخل کشور است تا از اقدامات بخش خصوصی آگاهی داشته، همچنین در صورت لزوم آنها را با اقدامات سازمان هماهنگ نماید.

ساختار پیشنهادی زیر یک ساختار وظیفه‌ای و پهن بوده، برگرفته از نظرات صاحب‌نظران این حوزه است و همچنین نگاهی ویژه به تجربیات کشورهائی که سابقه فعالیت در حوزه سایبر را دارند، داشته لذا بهتر از وضع موجود می‌تواند پاسخ گوی دغدغه‌ها و تهدیدات سایبری باشد و از موازی کاری و مغفول ماندن بعضی از وظایف جلوگیری نموده ، هماهنگی مناسبی را بین حوزه‌های عمل کننده در فضای سایبر ایجاد نماید.



کتابنامه

اعرابی، سید محمد،(۱۳۸۵)، *طراحی ساختار سازمانی*، دفتر پژوهشهای فرهنگی، چاپ پنجم،

افتخاری، اصغر، (۱۳۸۲)، *استراتژی ملی برای تأمین امنیت در فضای مجازی*، پژوهشکده مطالعات راهبردی،

افتخاری،اصغر،(۱۳۸۳)، *ارکان پنج‌گانه استراتژی تأمین امنیت در فضای مجازی*، پژوهشکده مطالعات راهبردی،

آلبرتس دیوید، پاپ دانیل، (۱۳۸۵)، *الزامات امنیت ملی در عصر اطلاعات*، پژوهشکده مطالعات راهبردی

بل دیوید، (۲۰۰۱)، *درآمدی بر فرهنگ سایبر* ترجمه مسعود کوثری، حسین حسنی، چاپ اول انتشارات جامعه شناسان

پارسائیان و اعرابی، (۱۳۸۲)، *سازمان، دفتر پژوهشهای فرهنگی*، فصل سوّم.

رشاد ، علی اکبر،(۱۳۸۸)، *معنا منهای معنا*، تهران: انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی

سازمان پدافند غیر عامل، *پدافند غیر عامل در حوزه جنگ سایبر*

سازمان پدافندغیرعامل،(۱۳۹۱/۳/۱۶)، *آیا جنگ سایبری متمدنانه است؟*، قابل دسترسی در http://۹۱.۲۲۵.۵۲.۷۵/article/

سازمان فناوری اطلاعات، (۱۳۹۰)، *نظام دفاع سایبری*، فصل ششم

سید مفیدی، کاوه، (۱۳۸۳)، *جنگ سایبری*

شریعت پناه، (۱۳۸۹)، *نشریه پیام انقلاب*، شماره ۳۶، تیر ماه

کیان خواه احسان، (۱۳۸۹)، *مدیریت امنیت اطلاعات* ، انتشارات ناقوس

کلانتری، «*ال گور، ارتباط با دانش جهانی*»، بولتن بررسی مطبوعات جهان ویژه ارتباطات، شماره۱۷۴، وزارت فرهنگ و ارشاد اسلامی اداره کل مطبوعات و رسانه‌های خارجی.

ماهنامه دنیای مخابرات و ارتباطات، (۱۳۸۹)، سال هفتم، شماره ۷۲، تیر ماه

موحدی صفت، محمدرضا، (۱۳۸۶)، *امنیت ملی در فضای سایبر*، فرصت‌ها و تهدیدها با تأکید بر استقرار دولت الکترونیکی، فصلنامه مطالعات دفاعی استراتژیک، سال هشتم، شماره ۳۰

نجف‌بیگی، رضا، (۱۳۷۶)، *سازمان و مدیریت*، تهران، مرکز انتشارات علمی دانشگاه آزاد اسلامی.

نشریه نیوزویک،۲۲ آوریل ۱۹۹۶.

Defense, US Department of. U.S. Cyber Command Fact Sheet. (۲۰۰۵), available at: http://www.defense.gov

Dod, (۲۰۱۱) ,Department Of Defence Strategy For Operatingin Cyberspace, http://www.defence.gov

GibsonWilliam,۱۹۸۴ , Neuromancer , US : Ace Books
Http://en.wikipedia.org/wiki/Federal_Office_for_Information_Security
Http://www.cabinetoffice.gov.uk/news/protecting-and-promoting-uk-digital-world
Http://www.eirib.ir
Http://www.huntonprivacyblog.com/۲۰۱۱/۰۷/articles/germany-launches-national-cyber-defense-center/
Http://www.ilaw.ir
Http://www.Renater.Fr
Http://www.syberpolice.ir
J. Andress and S. Winterfeld, (۲۰۱۱), Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Elsevier Syngress,
K.F. Rauscher and V. Yaschenko (Eds.), Russia# U.S. Bilateral on Cybersecurity Critical Terminology Foundations, EastWest Institute and the Information Security Institute of Moscow State University, ۲۰۱۱.
Mutula,Stephen M.,۲۰۰۷,Web Information Management, UK : Cahndos Publication
Ottis, R.: (۲۰۱۰), Analysis of the ۲۰۰۷ Cyber Attacks Against Estonia From the Information Warfare Perspective In: Proceedings of the ۷th European Conference on Information Warfare and Security.
STRATEGIC AND INTERNATIONAL STUDIES (CSIS), (۲۰۱۰), available at: http://csis.org/files/attachments/۱۰۰۶۰۳csis-alexander.pdf.