تحلیلی بر مؤلفه‌های دکترین سایبری کشورها

(مطالعه موردی: جمهوری اسلامی ایران)

سجاد کریمی پاشاکی*

روح‌الله منعم**

علی کاظمی‌پور***

چکیده

امروزه اکثر نظریه‌پردازان ژئوپلتیک جهان اعتقاد دارند که مرزهای سیاسی دچار تغییرکاربرد شده و نمی‌توانند جلوی بسیاری از تهدیدات بگیرند. تروریسم نیز از دیگر سو به جنگی همطراز علیه جامعه جهانی بدل شده و امنیت دولت‌ها را با چالش‌های بسیاری مواجه می‌کنند. به این لحاظ، توجه به عوامل ضدّتروریستی و گزینه‌های کاهش‌دهنده تبعات آن مورد توجه سیاستگذاران دولتی و خصوصی قرار می‌گیرد. بهبود در الگوهای امنیتی شهر به منظورکاهش اثرات و تبعات حملات نظامی، نقش به سزایی در برنامه‌ریزی‌های دفاعی دارد و تروریسم نیز

---

*. دکتری جغرافیای سیاسی، واحد صومعه سرا، دانشگاه آزاد اسلامی، صومعه سرا، ایران(نویسنده مسئول: sajadkarimipashaki@gmail.com).

**. دانشجوی دکتری روابط بین الملل دانشگاه گیلان.

***. کارشناسی ارشد جغرافیای سیاسی، دانشگاه آزاد اسلامی واحد رشت.

تاریخ دریافت: ۱۳۹۱/۷/۹ **تاریخ پذیرش: ۱۳۹۲/۶/۶**

فصلنـــامه پژوهش‌های روابط بین‌الملل، دوره نخست، شماره پانزدهم، صص ۲۲۰ - ۱۹۳.

به عنوان شکل بالقوه عملیات نامتعارف، سیاست‌گذاری‌هایی متناسب با نوع و شکل بروز خود را می‌طلبد. دامنه در برگیرنده تهدیدهای سایبری بسیار وسیع است. این موضوع را می‌توان از یک هک کردن ساده تا مباحث مربوط به تروریسم سایبری ارزیابی نمود. تروریسم سایبری هدف قرار دهنده سایت‌ها و مختل کننده تأسیسات متصل به شبکه های مجازی است که می‌تواند امنیت ساختارهای حاکمیتی، دولتی و نیز خصوصی را مختل و به شکل مستقیم و غیرمستقیم امنیت شهروندان را بنا به نوع حمله و میزان تخریب با تهدید مواجه سازد. از آنجائی‌که با ظهور فن‌آوری‌های جدید، ایران پس از انقلاب اسلامی با تهدیدهای نرم‌افزاری و سخت‌افزاری بالقوه و بالفعلی روبرو شده است، از این رو در سال‌های اخیر هدف قرار دادن سایت‌ها و تأسیسات شبکه‌ای همچون مراکز انرژی هسته‌ای و مراکز دولتی نشان‌دهنده ظهور تهدیدهای سایبری در این عرصه است.

این مقاله با روش تحلیلی-توصیفی و با هدف کاربردی در نظر دارد ضمن بررسی عملکرد تهدیدهای سایبری بر ساختارهای شبکه‌ای محیط های شهری و تأسیسات حیاتی کشورها، تأثیر اجرای پدافند سایبری بر جلوگیری و کاهش تبعات عملیات‌هایی از این دست را در ایران بررسی نماید.

واژه‌های کلیدی: *فضای مجازی، تهدیدهای سایبری ، تحولات ژئوپلتیک، پدافند سایبری.*

مقدمه

رشد روز افزون علم و تکنولوژی، برخی ایده‌هایی را که غالباً در گذشته به صورت داستان بیان می‌شدند، محقق کرد. فضای سایبر اولین بار توسط گیبسون[1] در رمان نیورومنسر[2] در سال ۱۹۸۴ مطرح شد. وی در تصویری از آینده کاربران کامپیوتری را که بوسیله اتصال‌شان، به‌طور مستقیم و آگاهانه به شبکه جهانی کامپیوتری دسترسی پیدا می‌کنند(Bell,2009:468)، ترسیم کرد، ولی دیری نپایید که این ایده داستانی، شکلی واقعی به خود گرفت. به‌طوری‌که زندگی بشر را در حوزه‌های مختلف علمی، اقتصادی و اجتماعی به خود وابسته نمود. تحولات گسترده در فضای سایبر، تهدیدهایی جدید را رقم زده که در واقع امنیت را در این شبکه‌ها با تهدید و چالش مواجه می‌سازد. فراتر از اینکه تهدیدهای فضای سایبر تنها در حوزه‌های فنی خلاصه شود، تأثیر و بازخورد آن بر زندگی واقعی انسآن‌ها حائز اهمیت است. تحولات گسترده در فضای سایبر می‌تواند دامنه وسیعی از اقدامات تهدیدآمیز علیه امنیت کشورها را به موجب شود. این اقدامات می‌تواند به‌نحوی از یک تلاش ساده برای مختل‌کردن کارایی یک سیستم رایانه‌ای تا تلاش برای اخلال در یک سایت هسته‌ای دامنه‌دار باشد. این موضوع زمانی سیاسی قلمداد می‌شود که سازمان‌های جنایی و یا تروریستی به عنوان عاملان حملات شناسایی شوند. تروریسم سایبری جزو اشکال جدید تروریسم است که تلاش می‌کند با هدف یا اهداف سیاسی، روندهای یک مجموعه دولتی یا خصوصی و یا عامه مردم را با تهدید مواجه سازد. از آن‌جائی‌که تعریف تروریسم خود مقوله‌ای چالش‌برانگیز است لذا تعریف سایبرتروریسم نیز خارج از این موضوع نیست. بنابراین عموماً این مفهوم از طریق مصادیق و گروه‌های

1. Gibson
2. neuromancer

به‌کارگیرنده تعریف می‌شود. نفوذ به سایت‌های دولتی کشورها به منظور اخلال و یا سرقت اطلاعات از طریق گروه‌های تروریستی می‌تواند ضربات غیرقابل جبرانی را به روند خدمات‌رسانی یک مجموعه وارد آورد که عمق آسیب‌پذیری آن را بنا به میزان اتکای آن مجموعه به فضای مجازی و گستردگی شبکه‌ای آن می‌توان به‌صورت تقریبی برآورد کرد.

از آن‌جاکه جمهوری اسلامی ایران پس از انقلاب اسلامی، همواره دچار تهدیدهای سخت و نرم بوده است و با توجه به اینکه با پیشرفت تکنولوژی، میزان وابستگی تأسیسات به فن‌آوری‌های نوین همچون اینترنت، شبکه‌های مجازی و... بیش از پیش شده است، لذا تلاش‌های صورت‌گرفته علیه ایران در سال‌های اخیر به منظور نفوذ به تأسیسات شبکه‌ای همچون سایت‌های هسته‌ای ایران با ارسال بدافزار استاکس نت[1]، استارس[2] و کرم‌های اینترنتی[3] و همچنین هک‌کردن سایت‌های دولتی از جمله سایت وزارت نفت و... نشان می‌دهد که تأسیسات وابسته به فضای شبکه‌ای و سایبری ایران همواره دچار تهدیدهایی از این دست می‌باشد. از این رو، ضروری می نماید تا تهدیدهای ناشی از این بخش تحلیل و تأثیر آن بر تأسیسات حیاتی و زیربنایی ایران ارزیابی شود و در این راستا به نقش و کارکرد پدافند غیرعامل در جلوگیری و یا به حداقل رساندن تبعات چنین حملاتی اشاره شود.

۱. رهیافت نظری

۱-۱. فضای مجازی و تکنولوژی شبکه‌ای

اطلاعات نیروی حیات بخش سیستم‌های بین‌المللی می‌باشد. سیاست امروز جهان فراتر از روابط ساده بین‌المللی بوده و بسیاری از تغییرات صورت‌پذیرفته‌شده در نتیجه گسترش زیرساخت‌های اطلاعاتی می‌باشد(Conway, 2007:95). فضای سایبر بخشی از فضای گسترده‌تر مجازی و در برگیرنده مجموعه‌ای وسیع از داده‌ها و اطلاعات است که امروزه بستر فعالیت را برای دسته‌های مختلف بازیگران در این عرصه مهیا ساخته است. ظهور انقلاب تکنولوژیکی، نویدبخش پدیدآمدن فن‌آوری‌های پیچیده‌ای بود که توسعه آن باعث تحت تأثیر قرارگرفتن سایر علوم شد، به‌گونه‌ای که فضای جدیدی را در دنیای واقعی به خود اختصاص داد. پیوند میان کامپیوتر و ارتباطات راه دور و ادغام

1. Stuxnet
2. Stars
3. Worm

این فن‌آوری‌ها در سیستم‌های چند رسآن‌های، منجر به دسترسی به شبکه جهانی شد که از نظر هزینه ارزان و در عین حال تحولی اساسی در زندگی بشر ایجاد کرد. (Cavelty,2008:19) فضای مجازی شکل گرفته از پیوند این فن‌آوری‌های اطلاعاتی و در واقع محیط شبیه‌سازی‌شده جهان واقعی است که در آن شبکه‌های ارتباطاتی و تکنولوژی‌های اطلاعاتی بر دیجیتالیزه[1] کردن تعاملات تأکید می‌کنند(کریمی پاشاکی،۱۳۹۱: ۴۰۹). به فراخور کارکرد و توسعه فضای مجازی و نیز سایبری که با پیدایش اینترنت رشد چشمگیری پیدا کرد، همان‌گونه که در جغرافیای واقعی، تهدیدها، فرصت‌ها و چالش‌هایی برای گروه‌های مختلف انسانی و در مجموع محیطی وجود دارد در فضای سایبر نیز عرصه این دسته از فعالیت‌ها منابع سخت‌افزاری و نرم‌افزاری را تحت‌الشعاع قرار می‌دهد. با توجه به‌اینکه در عصر نانو کسب اطلاعات منجر به افزایش قدرت و لذا دارای اهمیت شده، بنابراین حفاظت از اطلاعات و منابع اطلاعاتی از اهمیت بسیار برخوردار می‌شود. با این حال بررسی تهدیدها و چالش‌ها در فضای سایبر علاوه بر ابعاد تکنولوژیکی و اطلاعاتی، برای دولت‌ها، سازمان‌ها، گروه‌ها و نیز افراد در حوزه اجتماعی نیز حائز اهمیت قلمداد می‌شود.

۲-۱. امنیت، تهدید و آسیب‌پذیری‌ها در فضای سایبر

مفهوم امنیت هر روز بیش از گذشته، نه تنها در جهان سیاست، بلکه در اقتصاد، فرهنگ و اجتماع به کار می‌رود و آرام آرام به واژه و مفهومی پرقدرت تبدیل شده است. این مفهوم باعث شده است که محورهای مطالعاتی در حوزه‌های مختلف علمی بدان بپردازند(ربیعی،:۱۲۴۱۳۸۲). امنیت، زمانی به خطر می‌افتد که تهدید یا تهدیداتی علیه آن به وجود آید و یا این‌که بیم شکل‌گیری مخاطرات برای امنیت چالش‌هایی را به وجود آورد. در واقع در رابطه با کشورها و دولت‌ها تهدید در برابر مفهوم امنیت ملی قرار می‌گیرد و از آن به تجاوز به حق حاکمیت دولت‌ها در امور داخلی و خارجی آن‌ها تعبیر می‌شود (Alagappa, 1987: 2). عده‌ای از نظریه‌پردازان امنیت ملی بر این باورند که در جوامع مدرن، امنیت سخت‌افزاری نیست (روحانی،:۸۱۳۸۷). دشمنان امروز از طریق تکنولوژی ارتباطاتی قصد نفوذ بر افکار را دارند. بنابراین، طرفینِ ارتباط، مفاهیم خود را از طریق ایجاد

1. Digitalizing

ارتباط به یک‌دیگر انتقال می‌دهند و قرابت فکر و اندیشه ایجاد می‌کنند(احمدی دهکاء و پیشگاهی فرد،۳۹۱۳۹۱). واژه امنیت فصل مشترکی میان زندگی واقعی و مجازی است. همانگونه که در زندگی طبیعی و فیزیکی افراد، تهدیدهای سخت و نرم وجود دارد، این تهدیدها به فراخور ساختارهای محیطی و فضایی در فضای مجازی و سایبر نیز امنیت را تحت‌الشعاع قرار می‌دهد.

جدول ۱- ماتریس زیرساخت‌های تهدید

قصد/ ابزار	فیزیکی	سایبری
فیزیکی	- قطع ارتباط راه دور کابلی - آسیب‌رسانی فیزکی به سرور - بمب‌گذاری در شبکه برق	- استفاده از پالس‌های الکترومغناطیسی و فرکانس رادیویی به عنوان سلاح - بی‌ثباتی قطعات الکترونیکی
سایبری	- هک‌کردن یک سیستم SCADA[1] و کنترل سیستم فاضلاب شهری - نفوذ در سیستم کنترل ترافیک هوایی جهت سرنگون کردن هواپیماها	- هک‌کردن شبکه مهم دولتی - به‌کارگیری اسب‌های تروا در سوئیچ‌های یک شبکه عمومی

Cavelty,2008:23

با بررسی تهدیدها و آسیب‌پذیری‌ها در فضای سایبر در بخش حملات سایبری، پنج سطح تقسیم‌بندی وجود دارد که عبارتند از:

۱. کاربران خانگی و تجارت‌های کوچک
۲. تشکیلات اقتصادی بزرگ
۳. نواحی بحرانی/ تأسیسات زیربنایی
۴. آسیب‌پذیری در حوزه ملی
۵. تهدیدات جهانی

۱-۲-۱. کاربران خانگی/تجارت های کوچک

عموماً کامپیوترهای خانگی و شبکه‌های تجارت کوچک که در قالبِ تجارت محلی سازمان‌دهی می شوند، جزو بی‌دفاع‌ترین و آسیب‌پذیرترین سطوح فعالان سایبر به حساب می‌آیند. در واقع مشترکان از طریق اتصال به خط اشتراک دیجیتال[1] و یا اتصالات کابلی

1. Digital subscriber line(DSL)

می‌توانند از مزایای آن بهره‌گیرند و حمله‌کنندگان کسانی هستند که بدون آگاهیِ کاربران اصلی از اطلاعات آنان استفاده می‌کنند. نفوذگران با ورود به شبکه‌های کاربران شخصی یا حوزه تجارت‌های کوچک از داده‌ها و بانک اطلاعاتی آنان برای منافع شخصی خود استفاده می‌کنند.

۲-۲-۱. تشکیلات اقتصادی بزرگ

تشکیلات اقتصادی بزرگ(مانند: شرکت‌ها، کنندگی‌های دولتی و دانشگاه‌ها) عموماً اهداف متداولی برای حملات سایبری محسوب می‌شوند. بسیاری از تشکیلات اقتصادی بخش مهمی از زیر ساخت‌های مهم کشور می‌باشند. از این رو، لازم است این تشکیلات، سیاست‌ها و برنامه‌های امنیت اطلاعاتی خود را برای رسیدن به امنیت لازم در حوزه سایبر برنامه‌ریزی کنند (The white house,2003:7). حمله‌کنندگان به چنین مراکزی یا دارای اهداف اقتصادی برای جمع‌آوری اطلاعات مالی مربوطه می‌باشند و یا دارای اهداف سیاسی به‌منظور ضربه‌زدن به زیرساخت‌های اقتصادی هستند.

۲-۲-۱. بخش‌های بحرانی- تأسیسات زیربنایی

وقتی سازمان‌ها در بخش‌های اقتصادی، دولتی یا واحدهای آکادمیک دارای مشکلات امنیتی سایبر می‌باشند که حمله‌کنندگان اهداف خود را به سوی آنان معطوف می‌دارند. ضربه‌زدن به ساختار اقتصادی، سرقت اطلاعات و بانک‌های اطلاعاتی و تخریب فعالیت‌های جاری این دسته از بخش‌ها و تأسیسات از اهدافی است که حمله‌کنندگان دارا می‌باشند. هزینه تأمین امنیت سایبری در چنین بخش‌هایی بسیارگزاف است و باید سیستم امنیتی آن همواره به روز بوده تا در مقابل حملات نفوذگران از آسیب‌پذیری کمتری برخوردار باشد.

۲-۲-۱. موضوعات ملی و قابلیت آسیب‌پذیری

برخی از مشکلات امنیتی سایبر، دلالت بر ملی بودن آن دارد که نمی‌تواند به وسیله شرکت‌های خصوصی یا بخش‌های زیربنایی به تنهایی مرتفع شود. همه بخش‌ها به طور مشترک در اینترنت حضور دارند و از آن بهره‌می‌گیرند. بنابراین، همه آن‌ها در ریسک

ساختاری آن (مانند: پروتکل‌ها[1] و روترها[2]) ایمن نیستند. به‌کارگیری نرم‌افزار و سخت‌افزار ضعیف، در بسیاری از موارد می‌تواند مشکلاتی را در سطح ملی ایجادکند که مستلزم فعالیت‌های هماهنگ برای تحقیق و توسعه بهبود تکنولوژی‌ها است. علاوه بر آن فقدان آموزش و تأیید حرفه‌ای امنیتی سایبر در سطح ملی دارای مزیت و اهمیت است.

۵-۲-۱. تهدیدات جهانی

استانداردهای مشترک جهانی، همکاری‌های میان سیستم‌های کامپیوتری جهانی را امکان‌پذیر می‌سازد. به‌هم‌پیوستگی و درهم‌تنیدگی شبکه‌های کامپیوتری در جهان، این فرصت را به وجود آورده است که حمله‌کنندگان علیه چارچوب‌های ساختارمند جهانی اقدام و باعث وارد آمدن ضربات شدیدی به نظام شبکه‌ای شوند که می‌توان از حملات سایبری گروه‌های تروریستی در این خصوص یاد کرد.

۳-۱. شکل‌ها و بازیگران تهدید در فضای سایبر

برای تبیین اَشکال فیزیکی تهدیدات و چالش‌های فضای سایبرکه همواره توسط نفوذگران در حال تهدید است، جدول شماره ۲ به بیان مشروحی از منابع تهدیدات- انگیزه و اقدامات تهدیدآمیز اشاره می‌کند. سطوح دربرگیرنده تهدیدات سایبری بازگوکننده توانایی نفوذ در عرصه جغرافیای سایبر را مطرح می‌کند که تبعات خسارتی آن می‌تواند چالش‌های جدی برای افراد- سازمان‌ها و دولت ها به ثمر آورد. این دسته از حملات چنان‌چه بستر فضای شبکه‌ای در جوامع مهیا باشد، می‌توانند در صورت عدم تدبیر به‌موقع و ارتقاء امنیت شبکه، خساراتی به‌مراتب سنگین‌تر از یک جنگ در واقعیت را سبب شود. به‌صورت کلی حملات سایبری به دو طریق انجام می‌شوند. این حملات یا از طریق بیرونی صورت گرفته و یا از داخل انجام می پذیرد.

حملات سایبری که از خارج از یک شبکه انجام می‌شود، قاعدتاً از طریق هک‌کردن سیستم یا شبکه صورت می‌پذیرد درحالی‌که در شکل داخلی این حمله به واسطه وجود یک عامل یا عنصر خرابکار داخلی انجام می‌شود(Libicki,2009:13).

1.Protocols
2.Routers

جدول ۲- تهدیدات انسانی- منابع تهدیدات- انگیزش و اقدامات تهدیدآمیز

منابع تهدید	انگیزه	اقدامات تهدیدآمیز
هکر[2]- کراکر[3]	علایق شخصی	هک‌کردن مهندسی اجتماعی نفوذ سیستمی ورود با اجبار دسترسی غیر مجاز سیستمی
جنایت‌کار کامپیوتری[4]	خرابی اطلاعات افشای غیرقانونی اطلاعات منافع مالی تغییر غیرمجاز داده‌ها	جنایت(بزه‌کاری) کامپیوتری(مانند کمین سایبری) فعالیتَ کلاه‌برداری(مانند برگرداندن جعل هویت، ره‌گیری) ارتشاء اطلاعاتی حقه بازی تجاوز سیستمی
تروریست	نامه‌های الکترونیکی سیاه[5] تخریب بهره‌برداری انتقام	بمباران {اطلاعاتی} /تروریسم جنگ اطلاعاتی حملات سیستمی(مانند:DDos[6]) نفوذ سیستمی مداخله سیستمی
جاسوسی صنعتی (کمپانی‌ها، مؤسسه‌های دولتی و دیگر منافع دولتی)	مزایای رقابتی جاسوسی اقتصادی	بهره‌برداری اقتصادی سرقت اطلاعاتی تجاوز به حریم خصوصی مهندسی اجتماعی نفوذ سیستمی دسترسی غیرمجاز سیستمی(دسترسی به مطالب طبقه‌بندی‌شده اختصاصی یا تکنولوژی- روابط اطلاعاتی)

کارمندان داخلی(نارضایتی،آموزش ضعیف، ناخوشنودی، بداندیشی، بی‌دقتی، پایان کار یک کارمند	کنج‌کاوی نفس زیرکی منافع مالی کینه جویی اشتباه‌های غیرعمدی و ازقلم‌افتادگی(مانند: اشتباه در ورود اطلاعات، اشتباه در برنامه‌نویسی	حمله یک کارمند نامه الکترونیکی سیاه بازکردن اطلاعات خصوصی سوءاستفاده کامپیوتری فریب و سرقت ارتشاء اطلاعاتی واردکردن دیتای دست‌کاری‌شده، دیتای خراب جاسوسی کدهای خراب‌کاری(مانند: ویروس‌ها، بمب‌های هوشمند، اسب تروا) فروش اطلاعاتی شخصی اشکالات سیستمی تجاوز سیستمی خراب‌کاری سیستمی دسترسی غیرمجاز به اطلاعات

US Army Training and Doctrine Command & other, 2005: II-7, II-8))

تجزیه و تحلیل اهداف حملات سایبری می‌تواند برجسته‌کننده چهار حوزه کلی متأثر از این حملات باشد، سه حوزه اول، تأثیر حملات بر سیستم‌های فنآوری اطلاعات می‌باشد و چهارمین حوزه تخریب فیزیکی سیستم‌های فنآوری اطلاعات را بیان می‌کنند:

- از دست رفتن اعتماد به سالم بودن سیستم[1]
- خارج شدن از دسترس[2]
- از دست رفتن طبقه‌بندی محرمانه[3]
- تخریب فیزیکی[4]

1. Loss of Integrity
2. Loss of Availability
3. Loss of Confidentiality
4. Physical Destruction

۴-۱. بازیگران تهدیدهای سایبری

هر فرد یا گروهی که با استفاده از فناوری اطلاعات برای پیشبرد اهداف خود به مخالفان خود حمله می‌کند، تهدیدی سایبری قلمداد می‌شود. با این حال، اغلب، تعیین این‌که این اقدامات از سوی یک گروه سازمان‌یافته انجام پذیرفته یا افراد حقیقی، دشوار است. عموماً تصور غالب در خصوص تهدیدهای سایبری، هک‌کردن است. درحالی‌که هک، تنها گوشه‌ای از فعالیت گسترده در این بخش محسوب می‌شود. بنابراین، مشخص‌شدن گروه‌هایی که با فعالیت‌های خود بسترهای تهدیدهای سایبری را فراهم می‌آورند، امری حائز اهمیت است.

● **هکرها:** هکر به فردی گفته می‌شود که بدون مجوز به سیستم کامپیوتری برای خراب‌کاری و یا برای نشان‌دادن شعف سیستم نفوذ می‌کند(Downing& others,2004:223). فعالیت هکرها در واقع بیان‌گر نقاط ضعف سایبری مخاطبان است. دردهه ۱۹۷۰ واژه هکر به شخصی اطلاق می‌شد که در برنامه‌نویسی بسیار ماهر و باهوش بود. بعدها دردهه ۱۹۸۰ این واژه به معنی شخصی بود که در نفوذ به سیستم‌های جدید به‌صورت ناشناس تبحر داشته باشد. امروزه رسانه‌ها ومقامات مسئول مانند آژانس‌های دولتی و ادارات پلیس بیشتر با هدف ترساندن هکرها، این واژه را به هرشخصی که مرتکب یک جرم مرتبط با فناوری شود، اطلاق می‌کنند. این درست است که هکرهای کنجکاو می‌توانند سهواً باعث زیان‌های قابل توجهی شوند، اما جستجو برای یافتن اطلاعات وآموزش، نه انتقام‌گیری یا صدمه‌زدن به دیگران، عاملی است که باعث می‌شود اکثر هکرها سرگرمی خود را به‌نحوی بی‌رحمانه دنبال‌کنند. هکرها افرادی هستند که به‌طور غیرقانونی به کامپیوترهای هدف نفوذ پیدا می‌کنند و اقدام به آسیب‌رسانی به داده‌های سیستمی و نیز سرقت اطلاعات می‌کنند. فعالیت آن‌ها باعث اخلال در شبکه‌ها و با انگیزه‌هایی چون تأمین مالی صورت می پذیرد.

● **نفوذگر**[1]: این دسته از افراد ترکیبی از هکرها و فعالان اجتماعی هستند که دارای انگیزه سیاسی برای فعالیت‌های خود می‌باشند. در واقع افرادی که برای ایجاد یک تغییر اجتماعی دست به هک‌کردن می‌زنند. این افراد دولت‌ها، سازمان‌ها و شرکت‌ها را هدف قرار می‌دهند تا دیدگاه‌های اجتماعی، ایدئولوژیک، مذهبی یا سیاسی خود را به گوش آنان برسانند. در واقع فردی که برنامه‌های سیاسی یا اجتماعی را از طریق فعالیت نفوذی به پیش می‌برد. این افراد ممکن است در سیستم‌های کامپیوتری نفوذ کنند تا ترافیک را

1. Hacktivists

برهم بزنند، یا موجب آشفتگی شوند و ممکن است صفحات وب یا ایمیل را تغییر دهند تا هم‌دردی خود را به علت خاصی نمایش‌دهند. (مایکروسافت،۱۳۸۳: ۲۶۶). هکرهایی که بین کشورها فعالیت می‌کنند نیز از این دسته اند.

● **جنایت‌کاران کامپیوتری:** مجرمان دانسته‌اند که می‌توانند با استفاده از سیستم‌های کامپیوتری برای خود کسب منافع مالی کنند. کاربرد غیرقانونی کامپیوتر توسط فردی غیرمجاز، برای سرگرمی یا سوءاستفاده را نیز جرم کامپیوتری تعریف کرده‌اند (مایکروسافت،۱۳۸۳: ۱۳۰). اخاذی کامپیوتری یک نوع از جرائم است.

● **جاسوسی صنعتی**[1]: جاسوسی صنعتی سابقه‌ای طولانی در جوامع، به‌خصوص جوامع صنعتی، دارد که درواقع با پیشرفت تکنولوژی و به‌کارگیری کامپیوترها و شبکه‌ها در محیط‌های صنعتی، این دسته از افراد یا گروه‌ها فعالیت‌های خود را گسترش داده و روش‌های جدیدی برای به‌دست‌آوردن اطلاعات صنعتی به‌کار می‌گیرند. این‌گونه از فعالیت جاسوسی ممکن است با حمایت مستقیم یا غیرمستقیم دولت همراه باشد و هدف از آن ممکن است کشف اطلاعات اختصاصی مربوط به مسائل مالی و قراردادها و همچنین اطلاعات طبقه‌بندی‌شده در موسسات، سازمان‌ها و کارخانجات باشد. جاسوسی صنعتی عبارت است از به‌کارگیری روش‌هایی به‌صورت برنامه‌ریزی‌شده و هدفمند برای دسترسی به اطلاعات مهم و سرّی یک شرکت. اگر چه این نوع حمله معمولاً از جانب موسسات خاصی با پشتوانه مالی خوب صورت می‌گیرد، اما تحقیقات نشان داده است که جلوگیری از این حملات بسیار ساده و با تمرکز بر نقاط آسیب‌پذیر به راحتی قابل پیشگیری است (صادقی،۱۳۹۰:mahdisadeghi.com).

● **خودی‌ها**[2]: اگرچه متخصصان فناوری اطلاعات تلاش خود را برای تأمین امنیت سیستم‌ها در مقابل هجوم‌های خارجی به کار می‌گیرند، اما تهدیدهای درون‌سازمانی با توجه به دسترسی مجاز می‌تواند زمینه‌ساز یک نفوذ غیرمجاز باشد. این نفوذ می‌تواند توسط کارکنان ناراضی به تنهایی و یا در ارتباط با یک گروه تروریستی صورت پذیرد.

مشاوران و پیمان‌کاران[3]: نگرانی دیگر برای توسعه فناوری‌های اطلاعاتی نیاز به مشاوران و پیمان‌کاران خارج سازمانی برای توسعه سیستم‌های نرم‌افزاری و سخت‌افزاری

1. Industrial Espionage
2. Insiders
3. Consultants/contractors

است. اغلب این دسته از پیمان‌کاران می‌توانند در دسترس یا نفوذ سایبر تروریست ها قرارگیرند.

تروریست‌ها: تروریسم همواره با ارتباطات پیوند خورده است. در واقع، دانشمندان بر این باور هستند که تروریسم بدون وجود ارتباطات نمی‌تواند فعالیت داشته باشد (Conway,2006:94). اگرچه حملات سایبری عمده، از فعالیت‌های گروه‌های تروریستی ناشی می‌شود، اما این لزوماً بدین معنا نیست که تخریب شدید فیزیکی در دستور کار آن‌ها قرار ندارد. برخی از کارشناسان بر این باروند که تروریست‌ها در نقطه‌ای که قادر به استفاده از اینترنت هستند، می‌توانند از آن به‌عنوان ابزار مستقیم ایجاد تلفات و یا در ارتباط با یک حمله فیزیکی بهره بگیرند. از جمله گروه‌های تروریستی نوین، تهدیدکنندگان امنیت ملی کشورها در فضای سایبر هستند. این گروه‌ها با هدف دستیابی به مقاصد خود به زیرساخت‌های فناوری اطلاعات حمله می‌کنند. گسترش تعداد این گروه‌ها و بهره‌برداری از شرایط جدید، زمینه‌های تهدید آن‌ها را بیشتر کرده است. ماهیت شبکه‌ای و به‌هم‌پیوسته دنیا و امکان خراب‌کاری از طریق این شبکه که بیشتر مبتنی بر دانش است، باعث کوچک‌تر اما کاراترشدن این گروه‌ها می‌شود؛ این درحالی‌است که استفاده از سلاح‌های پیشرفته، هم گران و هم خطرناک است و این خود، درگذشته مانع توسعه این گروه‌ها بود (حسن بیگی،۱۵۷۱۳۸۴).

از سوی دیگر، شکل تهدیدات سایبری به‌خصوص برای حاکمیت، تشکیل و تأثیرات جوامع اجتماعی شبکه‌ای و کارکردهای ناشی از آن در جغرافیای سایبر می‌باشد. فضای سایبر مبیّن آزادی مطلق بیان است، لذا افراد و گروه‌های موافق و مخالف سیاست‌های دولت می‌توانند از آن برای نیل به اهداف خود استفاده کنند. به‌وجودآمدن جوامع اجتماعی شبکه‌ای همانند Face book و Twitter و... و عضویت بسیاری از مردم در آن و نیز شکل‌گرفتن گروه‌های مختلف اجتماعی، که اهداف سیاسی یا فرهنگی را دنبال می‌کنند، می‌تواند سیاست‌های دولت‌ها به‌خصوص کشورهای عقب‌مانده و یا درحال‌توسعه را دچار چالش کنند. این مسائل به‌خصوص در کشورهایی که از تکثر اقوام برخوردار و یا به لحاظ دموکراسی دچار ضعف هستند، تشدید می‌شود. شبکه‌های اجتماعی، این امکان را فراهم می‌آورد تا دوستان، هم‌فکران، هم‌حزب‌ها و کسانی‌که دارای عقاید و دیدگاه‌های مشترک هستند، به‌سرعت هم‌دیگر را یافته و تبادل‌نظر و برنامه کنند. امری که شاید در

جغرافیای واقعی با محدودیت‌ها و موانعی روبرو می‌باشد. در واقع، حاکمیت درصورتی‌که دریابد فعالیت‌هایی از این دست مشروعیت آن را دچار چالش می‌کند، اقدام به محدودیت دسترسی و نیز مسدود کردن چنین دامنه‌هایی می‌کند که آن نیز با توجه به پیشرفت تکنولوژی و یا حمایت‌های خارجی اثر زیادی نخواهد داشت. لاجرم، حاکمیت برای کاهش ابعاد تهدیدات اجتماعی می‌بایست به رقابت در چنین محیطی اقدام نماید؛ چراکه به‌کاربردن ابزارهای محدودکننده و بازدارنده تنها بازخورد منفی دربرخواهد داشت. نمونه این گونه از اقدامات را می‌توان در چین و ایران ملاحظه کرد.

ابزارهای بسیاری وجود دارد که می‌تواند شکل‌دهنده تهدیدهای سایبری قلمداد شده و افراد و گروه‌ها برای حملات خود از آن‌ها استفاده کنند. موسسه ملی استاندارد و فن‌آوری[1] وزارت بازرگانی و نیز وزارت دفاع ایالات متحده اقسام حملات کامپیوتری را به شرح ذیل طبقه‌بندی کرده است:

- درِپشتی[2]
- حملات عدم اجرای خدمات[3]
- ایمیل‌های جعلی[4]
- آی پی های جعلی[5]
- کی‌لاگر[6]
- بمب منطقی[7]
- حملات فیزیکی
- ردیاب[8]
- اسب‌های تروا
- ویروس‌ها

1. National Institute of Standards and Technology(NIST)
2. Back door
3. Denial of Service Attacks
4. Email Spoofing
5. IP Spoofing
6. Key logger
7. Logical Bomb
8. Sniffer

- کرم‌ها
- زامبی [1] (Gustin,2004)

۲. ادبیات پژوهش

این تحقیق با روش توصیفی-تحلیلی، به تجزیه و تحلیل تهدیدهای بالقوه و بالفعل سایبری در موضوع امنیت در فضای سایبر پرداخته و در این رابطه حملات گروه‌های خرابکار و یا تروریستی را به شبکه‌های مجازی و ساختارهای وابسته به آن را ارزیابی می‌کند. از این رو، در این تحقیق تلاش می‌شود تا به این سوال پاسخ داده شود که«ساختارهای پدافند غیرعامل چگونه می‌توانند از حملات سایبری به شبکه‌های مراکز و تأسیسات مهم ایران جلوگیری نماید؟ و یا تبعات آن را به حداقل کاهش دهد؟»

با توجه به فراگیر شدن به‌کارگیری ابزارهای تکنولوژیک و سایبری توسط ملت‌ها و دولت‌ها و بروز تهدیدها، چالش‌ها و فرصت‌های مختص فضای سایبر، سیاست‌گذاری جهت تأمین امنیت اطلاعات نرم‌افزاری و سخت‌افزاری جزو وظایف سیاست‌گزاران این حوزه قرارگرفته است. هر مقدار که به‌کارگیری فضای سایبر در جوامع رونق داشته باشد، به‌همان مقدار تأمین امنیت آن نیز حائز اهمیت است. تجارب کشورهای مختلف پیرامون تدوین استراتژی فضای سایبر و یا تأسیس مراکزی برای پایش تهدیدات و دفاع از حملات سایبری خود بازگوکننده اهمیت این موضوع است.

ایالات متحده امریکا از سال‌های پیش با توجه به تعریف فضای سایبر و تهدیدات آن، واحدهای مختلفی برای دفاع در برابر حملات سایبری تشکیل داده است. در این کشور، مسئولیت دفاع سایبری در بخش نظامی بر عهده سازمان فرماندهی سایبری ایالات متحده است. مأموریت این سازمان، برقراری امنیت فضای سایبر برای ارتش امریکا، وزارت دفاع و همچنین برقراری امنیت و آزادی ایالات متحده و هم پیمانانش در فضای سایبر است (U.S. Cyber Command Fact Sheet, 2005). علاوه بر اینسازمان، دو سازمان از جامعه اطلاعاتی امریکا (آژانس امنیت ملی و پلیس فدرال) و یک اداره از وزارت امنیت داخلی نیز در زمینه دفاع و امنیت فضای سایبر فعالیت دارند (حسینی و ظریف منش،۱۳۹۳: ۵۵).

انگلستان نیر در سال ۲۰۱۰ دو نهاد اصلی جدید برای مسائل سایبری ایجاد کرده

1. Zombie

است. این دو دفتر امنیت سایبر و مرکز عملیات امنیت سایبری هستند. دفتر امنیت سایبری در دفتر کابینه مستقر است و متولی امنیت سایبری راهبردی بریتانیا است و رهبری راهبردی امنیت سایبر در کل دولت و سراسر ادارات آن را بر عهده دارد. و مرکز عملیات امنیت سایبری پایش و هماهنگی پاسخ به حادثه را فراهم می‌کند (حسینی و ظریف منش،:۵۷۱۳۹۳). 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 شروع به کار کرده و تاکتیک‌های جدید، تکنیک‌ها و طرح‌هایی را برای ارایه قابلیت‌های سایبری نظامی توسعه خواهد داد و هدایت توسعه و یکپارچه‌سازی قابلیت‌های دفاع سایبری را به عهده خواهد گرفت (Cabinetoffice.gov.uk).

۳. یافته‌های تحقیق

۳-۱. تهدیدهای بالقوه سایبری در ایران

پویایی فن‌آوری‌های مرتبط با حوزه سایبر به‌حدی است که نمی‌توان دامنه‌ای برای تهدیدها و فرصت‌های برآمده از آن تعیین‌کرد. زیرا با پیشرفت تکنولوژی و توسعه شبکه‌های اطلاعاتی و ارتباطاتی، همواره شیوه‌های جدیدی برای به چالش‌کشیدن فضاهای مرتبط با فضای مجازی به وجود می‌آید که در واقع خلاء پای امنیتی محسوب می‌شود. به فراخور رشد تکنولوژی و وابستگی جهانی به شبکه‌های مجازی، ضریب رشد دسترسی به اینترنت نیز در ایران رشدی چشمگیر داشته به‌نحوی که ضریب اینترنت از ۲۱/۸ در سال ۱۳۸۷ به ۵۹/۵۰ در شش ماه اول ۱۳۹۱ رشد یافت (متما،۱۳۹۱). این رشد به همراه رشد تجارت الکترونیک، خدمات الکترونیک، بانک‌داری الکترونیک، آموزش الکترونیک و.... نشان‌دهنده گُذار ساختارهای سنتی به مدرن می‌باشد که امروزه در ایران به شدت به‌علت تقاضا و سهولت دسترسی در حال توسعه است. اما از سوی دیگر، رشد فزاینده جرایم اینترنتی و نفوذهای غیرمجاز با اهداف مختلف باعث شده که امنیت در این فضا نیز امری نسبی و وابسته به الزامات خاصی تعریف شود. برای شناخت مجموعه تهدیدات سایبری در ایران می‌بایست به تهدیدات موجود در سه حوزه «حملات سایبری، جنگ سایبری و تروریسم سایبری» اشاره و نمونه‌هایی از آن‌ها ذکرشود.

● **حملات سایبری:** این دسته از حملات به سایت‌های دولتی و خصوصی با هدف‌های مختلف چون سرقت و کلاه‌برداری، نفوذ و جاسوسی، از دسترس خارج ساختن و اعلام پیام‌های سیاسی، اجتماعی و فرهنگی و یا تلفیقی از موارد ذکر شده سازمان‌دهی می‌شوند.

جنگ سایبری: جنگ سایبری عبارت است از انجام یا آماده‌شدن برای انجام عملیات نظامی مطابق با اصول مربوط به اطلاعات (صدوقی،۱۳۸۲: ۱۳۳)، اما گسترده‌تر از این تعریف می‌توان گفت که جنگ سایبری، به‌کارگیری ابزارهای سایبری جهت نفوذ و ضربه زدن به ساختارهای اطلاعاتی کشور هدف، از طریق کشوری است که به‌صورت بالقوه یا بالفعل متخاصم محسوب می‌شود. به‌طور مثال، همواره دو کشور ایالات متحده امریکا و ایران هم‌دیگر را به دست داشتن در انجام عملیات‌های سایبری علیه یک‌دیگر متهم می‌کنند.

● **تروریسم سایبری:** این نوع از تروریسم، فناوری اطلاعات را برای حمله به افراد غیرنظامی و جلب نظر به سمت عامل تروریستی به کار می‌گیرد. این می‌تواند به این معنا باشد که آن‌ها با استفاده ابزاری از تجهیزات فناوری اطلاعات چون سیستم‌های رایانه‌ای با وسایل ارتباط راه دور به سازمان‌دهی حمله‌ای می‌پردازند که بارها با شیوه‌ای سنتی شکل گرفته است(سازمان پدافند غیر عامل کشور ۱،۱۳۹۱: ۲۲). درواقع، می‌توان به‌طور خلاصه تروریسم سایبری را به‌کارگیری ابزارهای سایبری برای حمله به ساختارهای اطلاعاتی و ارتباطی یک کشور، حزب، گروه یا.... توسط گروه‌های تروریستی به‌منظور خربکاری یا نفوذ تعریف کرد.

با توجه به تهدیدات سایبری ساختارهای اطلاعاتی و ارتباطی، در ایران دو گروه حملات سایبری و نیز جنگ سایبری دارای سابقه بوده و تهدیدهای آن در جریان است. اما در مبحث تروریسم سایبری این موضوع کم‌رنگ‌تر است؛ اما با توجه به فعالیت‌های تروریستی برخی از گروه‌های معاند جمهوری اسلامی ایران، نمی‌توان ریسک آن را برای بلندمدت نادیده گرفت؛ هرچند که برخی از منابع از نقش‌آفرینی سازمان تروریستی مجاهدین خلق ایران در ورود آلودگی استاکس نت به رایانه‌های نیروگاه اتمی کشور خبر داده‌اند(تابناک،۱۳۹۱).

۲-۳. ساختار تهدیدهای سایبری در ایران

هم‌سو با جنگ سخت و نرم، تلاش‌هایی برای به چالش‌کشیدن امنیت تأسیسات و

ساختارهای شبکه‌ای در جمهوری اسلامی ایران توسط اشخاص و گروه‌هایی که غالباً با هدف مشخص سیاسی اقدام به حملات سایبری می‌کنند، شکل گرفته است. این اقدامات عموماً از مقطع زمانی که در آن وابستگی سیستم‌های زیربنایی و خدماتی کشور به کامپیوتر و شبکه‌های محلی و بین‌المللی افزایش پیدا کرد، آغاز شد که در آن تلاش برای آلوده‌کردن این دسته از سیستم‌ها به‌منظور خراب‌کاری و یا سرقت اطلاعات، هدف قرار گرفت. این دسته از اقدامات به دو گروه عمده «با منبع مشخص و محدود» و «بدون منبع مشخص و متکثر» تقسیم‌بندی شده که در غالب حملات و جنگ سایبری از یک‌دیگر تفکیک می‌شود.

در بررسی تاریخچه حملات سایبری علیه سایت‌های ایران، می‌توان به مهم‌ترین آن‌ها که بازتاب خبری جهانی یافت، یعنی بدافزار استاکس نت اشاره کرد. این بدافزار در سال ۲۰۱۰، مراکز هسته‌ای ایران از جمله نطنز و بوشهر را هدف قرارداد. استاکس‌نت، با استفاده از نقص امنیتی موجود در میان‌برهای ویندوز، با آلوده‌کردن رایانه‌های کاربران صنعتی، فایل‌های با قالب اسکادا را، که مربوط به نرم‌افزارهای وین سی سی[1] و پی سی اس۷[2] شرکت زیمنس است، جمع‌آوری کرده و به یک سرور خاص ارسال می‌کند. این بدافزار به دنبال خراب‌کاری در تأسیسات غنی‌سازی اورانیوم نطنز بوده و در حقیقت هدف اصلی از طراحی آن، ایجاد خلل در فعالیت‌های غنی‌سازی اورانیوم در کشور به‌ویژه در این سایت هسته‌ای بوده است. هرچند که روزنامه نیویورک تایمز در تاریخ ۱۶ ژانویه ۲۰۱۱، در مقاله‌ای صراحتاً اعلام کرد که اسرائیل استاکس‌نت را در مرکز اتمی دیمونا و بر روی سانتریفیوژهای مشابهی که ایران از آن‌ها در تأسیسات غنی‌سازی اورانیوم نطنز استفاده می‌کند، یا موفقیت آزمایش کرده بود (آل‌طاهر،۱۳۹۰: ۷). استاکس نت، جولای همان سال در جغرافیایی وسیع، از برزیل تا مصر انتشار یافت، ولی بیش‌ترین میزان آلودگی با ۶۰ درصد در ایران گزارش شد (زهره‌ای،۱۳۹۱). همچنین ویروس استارس نیز که از خانواده استاکس‌نت محسوب می‌شود، در سال ۲۰۱۱، در ایران شناسایی شد. علاوه بر استارس و استاکس‌نت، ویروس‌ها و بدافزارهای دیگری همچون؛ دوکو و فلیم نیز علیه تأسیسات هسته‌ای ایران استفاده شده است. همچنین فعالیت‌های افراد و گروه‌هایی با هویت‌های

1. winCC
2. PCS7

معلوم و یا مجهول در شکل‌دهی به حملات سایبری علیه سایت‌های اینترنتی ایران با هدف از کارانداختن و یا تبلیغ عقاید و اعلان اعتراضات سیاسی و اجتماعی جزو دیگر حملات عمده سایبری محسوب می‌شوند. حمله به سایت‌های دولتی و حاکمیتی از جمله این دسته حملات می‌باشند که نمونه اخیر و برجسته آن حمله به سایت وزارت نفت ایران است. همچنین پس از انتخابات ریاست جمهوری دوره دهم در ایران و اعتراضات پس از آن، یکی از اشکال اعتراض استفاده از دی داس[1] علیه وب سایت‌های دولتی ایران بود که با استفاده از زیرساخت شبکه اجتماعی توییتر صورت گرفت(Carr,2010:37). این حملات باعث مختل‌شدن و یا در برخی از اوقات خارج شدن از دسترس برخی از این سایت‌ها شد.

۳-۳. پدافند غیرعامل در حوزه فضای سایبر

پدافند در واقع به روش‌های جلوگیری از حملات و کسب پیروزی دشمن گفته می‌شود و خود به اقسام گوناگونی تقسیم می شود. «استفاده از استتار، پوشش، اختفاء، پراکندگی، فریب و کنترل حرکت در روشنایی را پدافند غیرعامل می‌گویند (روشن-فرهادیان،:۴۲۱۳۸۵). از این رو، می‌توان پدافند غیرعامل را مجموعه‌ای از فعالیت‌ها عنوان کرد که درصورت اقدامات نظامی دشمن، خسارات احتمالی را کاهش می‌دهد. هدف از اجرای این طرح، حفظ آسیب‌پذیری افراد، تأسیسات نظامی، حیاتی، روبنایی و زیربنایی است که بتوانند در شرایط بحرانی به فعالیت خود ادامه دهند. تفاوت عمده پدافند عامل و غیرعامل در آن است که در پدافند عامل با استفاده از ابزار و آلات نظامی مناطق مهم پوشش داده می‌شوند، اما در پدافند غیرعامل، نیروهای نظامی، اداری و حتی کلیه مردم باید ایفای نقش بکنند.

جمع‌آوری اطلاعات سایبری رابطه مستقیم با پیشرفت تکنولوژی ارتباطی دارد و اساساً جمع‌آوری سایبری فرزند و یا نتیجه پیشرفت تکنولوژی‌های ارتباطی و به ویژه رایانه‌ای است. هم از این رو کشورها و یا گروه‌های دارنده فناوری سطح برتر همواره یک قدم جلوتر از دیگران هستند(خوش عمل،۱۳۹۱: ۱۲۲). این موضوع با توجه به وابستگی هر چه بیشتر ساختارها به فضای سایبر بیشتر نقش‌آفرینی می‌کند. به این معنی که هر اندازه که ساختارها متکی به فضای مجازی شود، از سوی دیگر آسیب‌شناسی تهدیدات

1. DDos

بالقوه و بالفعل می بایست مد نظر قرارگیرد. این به معنای آن است که رشد و پیشرفت تکنولوژی اگرچه می‌تواند کارکرد بسیاری از ساختارهای سنتی را تسریع و بهبود ببخشد، اما تهدیدات داخلی و خارجی علیه آن نیز گستردگی خود را پیدا می‌کند. از این رو، پدافند غیرعامل در حوزه سایبر در واقع شناسایی ریسک‌ها و مدیریت حملات سایبری به ساختارهای مجازی(سایبری و شبکه‌ای) به جهت مقابله یا کاهش تبعات آن و از چرخه خارج نشدن و حفاظت از اطلاعات است که بالتبع نتیجه‌ای جز کاهش میزان نفوذ عامل یا عوامل بیگانه و جلوگیری از سوء استفاده و خراب‌کاری آن را ندارد. از این رو، توجه به ساختارهای سایبری به لحاظ جایگاه فیزیکی و مجازی مستلزم طبقه‌بندی در چارچوب‌های ذیل است:

- **مراکز حیاتی**[1]: مراکزی هستند که درصورت انهدام کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری در سراسر کشور شود.
- **مراکز حساس**[2]: مراکزی هستند که درصورت انهدام کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات قابل توجهی در نظام سیاسی، هدایت، کنترل و فرماندهی تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری منطقه‌ای در بخشی از کشور شود.
- **مراکز مهم**[3]: مراکزی هستند که درصورت انهدام کل یا قسمتی از آن‌ها، آسیب و صدمات محدودی در نظام سیاسی، اجتماعی، دفاعی با سطح تأثیرگذاری محلی در کشور وارد می‌شود (ایزایران، بی تا: ۸-۷).

اگرچه سطح‌بندی مورد اشاره در خصوص ساختارهای فیزیکی و بناهای طبقه‌بندی شده لحاظ می‌شود، ولی همین سطح‌بندی می‌تواند جایگاه فضای سایبر را در هر یک از سطوح مذکور مشخص کند. این بدان معنا است که میزان پوشش حفاظتی سایبری بنابر سطوح ذکر شده می‌بایست در برگیرنده پوشش و پشتیبانی به‌منظور به‌حداقل رساندن ریسک‌های تهدیدات سایبری باشد.

1. Vital Centers
2. Critical Centers
3. Important Centers

۴-۳. مستندات و الزامات قانونی در پدافند غیر عامل سایبری

به‌منظور توسعه و تأمین امنیت، پایداری و ایمنی در فضای تبادل اطلاعات کشور، سیاست‌گذاری و نظارت راهبری به منظور توسعه امنیت و ایمنی و پایداری در فضای تبادل اطلاعات باید مدّ نظر قرارگیرد. این موضوع به همراه پشتیبانی از برنامه دستگاه‌های دولتی و خصوصی در بخش‌های زیرساختی به جهت کاهش آسیب‌پذیری در برابر تهدیدات و جنگ‌های سایبری از طریق به‌کارگیری منابع و ظرفیت‌های تکنولوژیک داخلی امکان‌پذیر می‌شود. باتوجه به سند راهبردی ابلاغی از سوی رهبری، در زمینه پدافند غیرعامل و اهتمام ویژه آن بر روی فضای تبادل اطلاعات و ارتباطات، در بند ۱۱ سیاست‌های کلی نظام در خصوص پدافند غیرعامل چنین تصریح شده است: اصول و ضوابط مقابله با تهدیدات نرم‌افزاری و الکترونیکی و سایر تهدیدات جدید دشمن به منظور حفظ و صیانت شبکه‌های اطلاع رسانی، مخابراتی و رایانه‌ای (مجمع تشخیص مصلحت نظام،۱۳۸۶).

بر اساس سند راهبردی اشاره شده، اهداف کلان پدافند غیرعامل در حوزه سایبر عبارتند از:

۱. تأمین امنیت و حصول اطمینان از عدم دسترسی‌های غیرمجاز به اسرار و اطلاعات کشور(ملی و بخشی).

۲. ایمن‌سازی و حصول اطمینان از پایداری و خلل‌ناپذیری در فعالیت شبکه‌های الکترونیکی مدیریت و کنترل کشور(ملی و بخشی).

۳. حفظ و تأمین آرامش اجتماعی و عمومی از طریق توسعه اطمینان و اعتماد آحاد جامعه.

۴. نسبت به صحت و تداوم کارکرد شبکه و سامانه‌های الکترونیکی سرویس و خدمات عمومی.

۵. توسعه ظرفیت دفاع الکترونیکی در برابر تهاجم فرهنگی و نرم ازطریق شبکه‌های بین‌المللی و ملی اینترنت.

۶. تقویت ضریب امنیت و پایداری در حوزه زیرساخت‌های ملی و حیاتی(ایز ایران، بی تا: ۹).

بر اساس این اهداف کلان، اهداف راهبردی و اجرایی این سیاست‌ها نیز به شرح گزینه های ذیل می‌باشند:

۱. نهادینه‌سازی فرامین و قانونمندسازی تدابیر رهبری درخصوص پدافند غیرعامل در سازمان‌ها و دستگاه‌های ذیربط.

۲. ساماندهی، انسجام‌بخشی و هدایت راهبردی مجموعه‌های علمی، پژوهشی، آموزشی و صنعتی مرتبط با حوزه تخصصی فاوا در راستای تولید و توسعه دانش و فن‌آوری‌های بومی و ملی مورد نیاز پدافند غیرعامل.

۳. توسعه امنیت، ایمنی و پایداری در شبکه‌های ارتباطی و الکترونیکی موجود با تأکید بر فن‌آوری‌های بومی.

۴. نهادینه‌کردن اصول و ملاحظات پدافند غیرعامل در طرح‌های توسعه شبکه‌های ارتباطی و الکترونیکی.

۵. توسعه فرهنگ پدافند غیرعامل و ارتقاء دانش و شناخت مسئولین و کارشناسان حوزه ارتباطات و الکترونیک از پدافند غیرعامل.

۶. خوداتکایی از دستگاه‌های پشتیبان آسیب‌پذیر و خودکفایی از منابع خارجی فن‌آوری‌ها.

۷. حمایت از برنامه ایجاد شبکه ملی اینترنت مبتنی بر مولفه‌های امنیت، ایمنی، پایداری و متکی بر فن‌آوری‌های بومی.

۸. توسعه و تقویت سیستم پست کشور (بهره‌مندی از پست بسیار سریع و امین).

۹. بهره‌مندی از شبکه ارتباطی ویژه مدیریت کشور در شرایط بحران جنگ (با مولفه‌های امنیتی و پایداری و ایمنی بسیار بالا و دسترسی سریع).

۱۰. توسعه توان کنترل و مدیریت بحران و برنامه‌های حراست، حفاظت و ضد جاسوسی.

۱۱. نهادینه‌کردن ملاحظات دفاع غیرعامل و امنیت ملی در تعاملات و همکاری با کشورها و شرکت‌های خارجی در حوزه فن‌آوری اطلاعاتی و ارتباطاتی (ایز ایران، بی تا: ۱۰ تا ۱۲).

۵-۳. مراکز پدافند غیرعامل سایبری و امنیت شبکه‌ای

به‌منظور پیشگیری و مقابله با تهدیدات متصوّر سایبری، ایجاد مراکز پایش و رصد سایبری در دستگاه‌ها و ادارات بنا به اهمیت کارکرد آن‌ها ضروری می‌نماید. از آن‌جاکه سه سطح حیاتی، حساس و مهم برای اماکن، دستگاه‌ها، ادارات و... در نظر گرفته شده، لذا بنا به

سطح اهمیت هر کدام، می‌توان زیرساخت‌های پدافند غیرعامل سایبری را در آن‌ها لحاظ کرد. بنابراین، شرط اول اجرایی‌شدن موضوع تقسیم‌بندی و طبقه‌بندی اماکن و... در این سه طبقه می‌باشد. همچنین با توجه تشکیل سازمان پدافند غیرعامل کشور و نیز ادارات کل پدافند غیرعامل در برخی از سازمان‌ها و دستگاه‌ها، اهتمام ویژه به موضوعات: «رصد، پایش و تشخیص تهدید»، «استخراج آسیب‌پذیری»، «تجزیه و تحلیل تهدیدات»، «مدیریت صحنه جنگ‌های سایبری»، «بازیابی اطلاعات»، «ایمن‌سازی، پایدارسازی و ارتقاء آمادگی دفاع سایبری» و «تولید قدرت پاسخگویی به تهدید» می‌بایست مورد توجه قرار گیرد.

۱. رصد، پایش و تشخیص تهدید

- رصد، پایش و تشخیص تهاجم سایبری در سطح دستگاه.
- رصد پایش و تشخیص حادثه و خسارت سایبری در سطح دستگاه.

۲. استخراج آسیب‌پذیری

- جمع‌آوری، تنظیم و ارایه اطلاعات وضعیت دفاع سایبری در حوزه دستگاه و استخراج آسیب‌پذیری‌ها(نقاط ضعف) اساسی در این حوزه.
- استخراج آسیب‌پذیری‌های کیفی زیرساخت‌های حوزه دستگاه، بر اساس مقایسه نتایج ارزیابی‌های مرکز پدافند سایبری و زیرساخت ها.

۳. تجزیه و تحلیل تهدیدها

- تحلیل تهدیدهای بالقوه و قریب‌الوقوع و آسیب‌پذیری‌های وضعیت و عملیاتی دفاع سایبری دستگاه و ارزیابی و برآورد مخاطرات ناشی از این تهدیدها.
- تحلیل تهاجم‌های سایبری و آسیب‌پذیری‌های وضعیت و عملیاتی دفاع سایبری دستگاه و ارزیابی و برآورد حوادث و خسارات ناشی از این تهاجم.
- تحلیل حوادث و خسارات سایبری و آسیب‌پذیری‌های وضعیت و عملیاتی دفاع سایبری دستگاه و ارزیابی و برآورد پیامد های فاجعه‌بار ناشی از این حوادث.

۴. مدیریت صحنه جنگ سایبری

- مقابله و دفع تهاجم سایبری در سطح دستگاه.
- هدایت عملیاتی(برنامه‌ریزی، هدایت و نظارت) پاکسازی پیامدها و ریشه‌کنی منشاء تهاجم سایبری در سطح زیر ساخت‌های دستگاه.
- مستند سازی مقابله قانونی با منشاء تهاجم سایبری در حوزه دستگاه.

۵. بازیابی اطلاعات

- هدایت عملیاتی، بازیابی مبتنی بر نسخه پشتیبان در سطح زیر ساخت‌های دستگاه.
- بازیابی مبتنی بر نسخه اصلی در زیر ساخت‌های خود دستگاه.

۶. ایمن سازی، پایدارسازی و ارتقاء آمادگی دفاع سایبری

- مدیریت عملیات امن سازی در حوزه دستگاه.
- توسعه مرکز عملیات دفاع سایری و تیم مقابله با تهاجم سایبری دستگاه.
- توسعه توان‌مندی بازیابی اطلاعات زیر ساخت های حوزه دستگاه.

۷. تولید قدرت پاسخگویی به تهدید

- مقابله قانونی با منشاء تهاجم سایبری در حوزه دستگاه(سازمان پدافند غیرعامل کشور۲،۱۳۹۱: ۲۶ تا ۲۸) .

نتیجه‌گیری

با توجه به تحولات سریع در حوزه فناوری اطلاعات و از آن‌جاکه افراد، گروه‌ها، سازمان‌های خصوصی و دولتی و... از این فناوری‌ها به‌منظور پیشبرد اهداف خود بهره می‌گیرند، لذا گروه‌های خرابکار و سازمان‌های تروریستی و حتی خود دولت‌ها نیز به‌منظور ضربه‌زدن به منافع و امنیت کشوری دیگر تلاش می‌کنند تا با به‌کارگیری توانمندی‌های سایبری به مقاصد خود دست پیدا کنند. دامنه این مقاصد، طیف انعطاف پذیری از نفوذ و استخراج اطلاعات تا خراب‌کاری و از دور خارج کردن سیستم‌ها است. بنابراین، با توجه به ظهور تهدیدات جدید در عرصه فناوری اطلاعات ضروری است که تهدیدات جدید نیز پایش و رصد شود.

بهره‌مندی از پدافند سایبری در حوزه فناوری اطلاعات و ارتباطات در جهت پیشگیری و دفاع می‌تواند زمینه‌ساز کاهش ریسک‌های سایبری شود. اگرچه این امر مستلزم ارائه طبقه‌بندی صحیح از مراکز حیاتی، حساس و مهم است، اما با توجه به استفاده از فناوری اطلاعات و ارتباطات در فرایندهای سازمانی و چرخش مجازی اطلاعات در سازمان‌ها و همچنین وابسته بودن برخی از سیستم‌های کنترلی، پایش و حتی اجرایی به سخت‌افزارها و نرم‌افزارهای تحت شبکه، توجه به ارتقای امنیت شبکه به خصوص در مراکزی که می‌تواند امنیت شهروندان را تحت‌الشعاع قرار بدهد، ضروری است. پدافند غیرعامل سایبری در واقع بسترساز شناخت ظرفیت‌های سایبری و تهدیدها و نیز چگونگی مواجهه و مقابله با آن با در نظر گرفتن رفع تهدید و یا کاهش تبعات آن است. از این رو، عمومیت‌بخشی به موضوع پدافند غیرعامل سایبری به همراه آمایش سرزمینی نقاط آلوده و یا در معرض آلودگی می‌تواند ساز وکارهای لازم برای پوشش پدافند غیرعامل سایبری را مشخص سازد.

این تحقیق به دنبال پاسخگویی به این سوال بود که «ساختارهای پدافند غیرعامل چگونه می‌تواند از حملات سایبری به شبکه‌های مراکز و تأسیسات مهم ایران جلوگیری کند؟ و یا تبعات آن را به حداقل کاهش دهد؟»

به‌منظور پاسخ‌گویی به این سوال می‌بایست در ابتدا انواع تهدیدهای متصور سایبری احصاء و به عبارتی منابع تهدید مشخص شود. سپس با تحلیل سازوکارهای پدافند غیرعامل و به‌ویژه راهبردهای آن در بخش سایبری این امکان مهیا شود تا تعمیم پدافند غیرعامل در تهدیدهای سایبری تعریف و تبیین شود. با توجه به توضیحات داده شده در این خصوص، پدافند غیرعامل سایبری از طریق گسترش ساختاری آن در سازمان‌ها و مراکز طبقه‌بندی شده و یا دارای درجه اهمیت می‌تواند منجر به ایجاد بسترهای شناخت و پایش تهدیدها و نیز ارائه الگوهای مقابله آن شود. از این رو، با توجه به مستندات قانونی موجود در حوزه پدافند غیرعامل به‌ویژه پدافند سایبری تأکید بر استقرار قرارگاه‌ها و ساختارهای مربوطه و نیز تبیین اهداف آن به شکلی عمومی و به عبارتی آگاهی‌بخشی سازمانی و مردمی می‌تواند زمینه‌ساز رشد کارکرد پدافندغیرعامل سایبری در مراکز و سازمان‌هایی چون نیروگاه‌های اتمی، نیروگاه‌های مولد، مراکز اطلاعاتی و عملیاتی، وزارت‌خانه‌ها، مراکز مولد علمی و... شده و بالتبع نسبت به دانش‌افزایی عمومی کارکردی منجسم داشته باشد.

کتابنامه

منابع فارسی

احمدی‌دهکاء، فریبرز و پیشگاهی‌فرد، زهرا.(۱۳۹۱) **مقدمه‌ای بر روش‌های شناخت تهدیدات امنیت ملی در ایران**، تهران: انتشارات سازمان جغرافیایی نیروهای مسلح.

ایز ایران.(بی تا) **پدافند غیرعامل در حوزه جنگ سایبر**، جزوه آموزشی، شرکت ایز ایران

آل طاهر، احمدرضا (۱۳۹۰) «ایران و تهدیدات سایبری»، روزنامه رسالت، شماره ۷۴۲۹، ۹۰/۹/۲۰

تابناک.(۱۳۹۱). عامل انتقال ویروس استاکس نت به تجهیزات نطنز مشخص شد، کد خبر ۲۳۸۴۸۹، ۲۸ فروردین ۱۳۹۱: www.tabnak.ir

حسن بیگی، ابراهیم.(۱۳۸۶) **حقوق و امنیت در فضای سایبر**، تهران: انتشارات ابرار معاصر

حسینی، پرویز و حسین ظریف منش.(۱۳۹۲) «مطالعه تطبیقی ساختار دفاع سایبری کشورها»، **فصلنامه علمی پژوهشی پژوهش‌های حفاظتی و امنیتی**، ۲(۵).

خوش عمل، حسین.(۱۳۹۱) پدافند غیرعامل در حوزه سایبر، تهران: انتشارات مرکز آموزشی و پژوهشی سپهبد صیاد شیرازی.

ربیعی، علی.(۱۳۸۲) «امنیت ملی، مفهومی در حال تکوین»، **دو ماهنامه علمی-ترویجی اطلاعات سیاسی و اقتصادی**، شماره ۱۹۷-۱۹۸، بهمن و اسفند ۱۳۸۲.

روحانی، حسن.(۱۳۸۷) «رسانه‌های گروهی و امنیت ملی»، **نشریه راهبرد**، شماره ۴۶، بهار ۱۳۸۷، تهران: انتشارات مرکز تحقیقات استراتژیک.

روشن، علی‌اصغر و نورالله فرهادیان.(۱۳۸۶) **فرهنگ اصطلاحات جغرافیای سیاسی – نظامی**، تهران: انتشارات دانشگاه امام حسین(ع).

زهره‌ای، محمدعلی.(۱۳۹۱). نبرد سایبری علیه برنامه هسته‌ای، www.irancdc.ir/paper/1339

سازمان پدافند غیرعامل کشور[۱]. (۱۳۹۱) **معرفی تهدیدات و نحوه بررسی و ارزیابی آن‌ها،** (کتابچه) تهران: سازمان پدافند غیرعامل کشور.

سازمان پدافند غیرعامل کشور[۲].(۱۳۹۱) **دستورالعمل آمادگی دستگاه‌ها، استان‌ها و مناطق ویژه به منظور مقابله با تهدیدات سایبری دشمن،** تهران: سازمان پدافند غیرعامل کشور.

صادقی، مهدی.(۱۳۹۰). جاسوسی صنعتی، www.mahdisadeghi.com/fa/?m139012

صدوقی، مرادعلی.(۱۳۸۲) **تکنولوژی اطلاعاتی و حاکمیت ملی،** تهران: انتشارات وزارت امور خارجه.

کریمی‌پاشاکی، سجاد.(۱۳۹۱) **چشم‌اندازهای سیاسی در تحلیل جغرافیای مجازی،** مجموعه مقالات پنجمین کنگره انجمن ژئوپلیتیک ایران، جلد دوم، تهران: انتشارات سازمان جغرافیایی نیروهای مسلح.

مایکروسافت.(۱۳۸۳) **فرهنگ تشریحی مایکروسافت ۲۰۰۴**، ویرایش پنجم، تهران: چاپ دانشیار.

متما.(۱۳۹۱). **آمار ظریب نفوذ کاربران اینترنت،**

www.matma.ir/matma/mnu-internet-penetration.html

مجمع تشخیص مصلحت نظام(۱۳۸۶) **سند راهبردی پدافند غیر عامل کشور،** سند ابلاغی.

منابع انگلیسی

Alagappa, Muthiah. (1987)***The National Security Of Developing States*** (Malaysia: ISIS).

Carr, Jeffrey. (2010) ***Inside Cyber Warfare***, Published by: O'Reilly Media

Cavelty, Myriam Duun.(2008)***Cyber security and threat politics: Us Efforts to secure the information Age***, Routledge published.

Conway, Maura. (2006) ***The internet and Politics***, ed by: Sarah Oates & others, article: Cybercortical Warfare: Hizbollahs Internet Strategy, Published by Routledge.

Conway, Maura.(2007) ***Power and Security in the Information Age***, ed by: Myriam Dunn and others, article: Terrorist use of the internet and the Challenges of Governing Cyberspace, Ashgate Published.

Downing, Douglas A. & other. (2009) ***Dictionary of computer and Internet terms***, 10th ed, Published by Barron's.

Gustin, Joseph F.(2004) ***Cyber Terrorism: a Guide for facility managers***, India: The Fairmont press.

Libicki, Martin C.(2009) ***Cyberdeterrence and cyberwar*** ,Rand published

Schell, Bernadette and Clemens. (2006) ***Webster's New World Hacker Dictionary***, Published by Wiley.

US Army Training and Doctrine Command. (2005) ***Cyber operation Defense***, US Department of. U.S. Cyber Command Fact Sheet, available at: http://www.defense.gov

White House. (2003) ***The national Strategy for security cyberspace***, Published by: White House.

www.cabinetoffice.gov.uk/news/protecting-and-promoting-uk-digitalworld

پی نوشت

1 .Supervisory control and data acquisition
2 . Hacker
3 . Cracker
4 . Computer criminal
5 . Black email

۶. یک حمله سایبری که در آن کراکر یک هدف کامپیوتری را با هزاران (یا بیشتر) از سیگنال‌های جعلی اطلاعاتی که موجب خروج کامپیوتر از صحنه می شود، بمباران می‌کند (Schell&Martin,2006:102).