فصلنامه مطالعات راهبردی فضای سایبر
سال دوم، شماره چهارم، پائیز ۱۴۰۲
مقاله دوم از صفحات ۶۲-۳۷

ارائۀ ساختار مفهومی ضد بدافزاری نیروهای مسلح در جهت افزایش امنیت ملی سایبری در جمهوری اسلامی ایران

علی بزرگمهر[۱]، روزبه رمضانی[۲]

تاریخ دریافت: ۱۴۰۰/۱۰/۳۰ تاریخ پذیرش: ۱۴۰۱/۰۴/۱۰

چکیده

زیست‌بوم انسان همیشه دارای انواع تهدیدات بوده است که با توجه به شکل‌گیری مفهوم سایبر در آن عنوان‌هایی همچون نبرد سایبری، تهدید سایبری، مافیای سایبری و اسامی گروه‌های فعال در این حوزه امروزه بسیار به گوش می‌خورند به‌طوری‌که این اسامی و فعالیت‌های آن‌ها قسمتی از زندگی انسان شده است. تهدیدات سایبری امروزه بعد مهمی از زیست واژه جهانی را شکل می‌دهد. تهدیدات سایبری می‌تواند سبب از بین رفتن تجهیزات، تغییر در طراحی محصول یا فرایندهای تولیدی یا نظامی شود. نوع تحقیق در این مقاله را می‌توان در زمره تحقیقات کاربردی به شمار آورد. قلمرو تحقیق ازلحاظ زمانی گذشته‌نگر و حال نگر، ازنظر مکانی عرصه جهانی بوده و ازنظر موضوعی فضای سایبری و ساختارهای سایبری کشورهای مختلف به‌خصوص در حوزۀ مقابله با بدافزارها می‌باشد. در این مقاله ضمن بررسی ضرورت ایفای نقش ارکان نظامی حاکمیت در حوزۀ سایبری و تحلیل اقدامات کشورهای مختلف در برخورد با واژه جنگ سایبری و راهبرد آن‌ها در برابر حملات بدافزارها، به ارائه ساختار مفهومی موردنیاز نیروهای مسلح برای مقابله با بدافزارها و فائق آمدن بر مشکلات ناشی از آن‌ها به‌عنوان گونه‌ای از سلاح‌های سایبری پرداخته می‌شود و به‌منظور دفاع و مقابله با این‌گونه تهدیدات، ساختاری مفهومی در جهت اشراف و فرماندهی سایبری پیشنهاد می‌گردد.

کلیدواژه‌ها: فضای سایبری، راهبرد امنیت ملی، تهدیدات سایبری، معماری، ساختار مفهومی.

۱. دکترای تخصصی، نویسنده مسئول a.bozorgmehr@chmail.ir

۲. دانشجوی دکترای مهندسی کامپیوتر گرایش فناوری اطلاعات دانشگاه. اصفهان، rozbeh.ramezani@gmail.com

۱. مقدمه و بیان مسئله

با توجه به پیچیدگی‌های زندگی بشری در دنیای معاصر و درهم‌تنیدگی ابعاد مختلف جامعه که از پیامدهای ناگریز زندگی در عصر جدید است، مطالعه در حوزهٔ امنیت ملی در کشور به نگاهی کلان نگر و جامع نیاز دارد تا کشور را از معرض تهدیدات سخت و نرم پیشرو عبور دهد. نگاه‌های تنگ‌نظرانه نسبت به مطالعات امنیت ملی قطعاً جوابگوی نیازهای کنونی کشور نبوده، به سردرگمی و عدم موفقیت در مبارزه و مقابله با تهدیدات پیرامونی منجر خواهد شد. یکی از مهم‌ترین مسائل موردتوجه کشورهای قدرتمند جهان، در شرایط کنونی، حرکت به‌سوی اولویت‌بندی تهدیدات امنیت ملی است (زابلی زاده و وهاب پور، ۱۳۹۷). درواقع لازم است این اولویت‌بندی با نگاهی سازمان‌یافته و فراگیر و مبتنی بر روش‌شناسی علمی انجام پذیرد تا بتواند در تخصیص بهینهٔ منابع مؤثر واقع شود. دفاع سایبری پویا و کارآمد همواره جزو دغدغه مسئولان و کارشناسان فنی در حوزهٔ امنیت زیرساخت‌های فناوری اطلاعات بوده ازاین‌رو ایجاد یک مرکز فرماندهی سایبری به‌منظور مقابله با بدافزارها و تهدیدات سایبری ازجمله ضرورت در جهت مدیریت حوادث سایبری می‌باشد (صالح نیا و بختیاری، ۱۳۹۷).

روش انجام این تحقیق، روش توصیفی - تحلیلی و سناریونویسی خواهد بود و روش گردآوری اطلاعات به روش کتابخانه‌ای، بررسی اسناد بالادستی، روش‌های میدانی و ... بوده و ابزار گردآوری اطلاعات، فیش‌برداری‌های موردنیاز از روش اسنادی و کتابخانه‌ای می‌باشد. در این مقاله به‌منظور درک خطرات ناشی از بدافزارها و تهدیدات نوین سایبری، بارزترین ویژگی‌های جنگ سایبری و اقدامات کشورهای مختلف در برابر این حملات موردبررسی قرار می‌گیرد و سپس روشی را برای محافظت از این دارایی‌ها در جنگ سایبری و خاصه مقابله با بدافزارها در برابر دشمنان اتخاذ و پیشنهاد می‌شود.

۲. ادبیات و مبانی نظری

۲-۱. ضرورت مدیریت نیروهای مسلح بر فضای سایبری به‌منظور مقابله با بدافزارها و افزایش امنیت ملی در جمهوری اسلامی ایران

هر آنچه، به‌صورت عینی یا ذهنی، ارزش‌ها و منافع ملی یک کشور را تهدید کند یا مانعی برای رسیدن کشور به اهدافش باشد تهدید امنیت ملی محسوب می‌شود. عملیات مشترک در جنگ‌های نوین از تمامی عرصه‌های نبرد در هوا، فضا، دریا، زمین و سایبر بهره می‌برند (لرستانی، ۱۳۹۷). در این عملیات عنصر سایبری در کنار سایر عناصر رزم قرارگرفته و در تصمیم سازی و تصمیم‌گیری به فرمانده کمک می‌کند. عناصر سایبری می‌تواند با طرح‌ریزی حملات سایبری قبل، حین و بعد از جنگ حقیقی کمک شایانی به فرمانده عملیات نماید (اسماعیل زاده و رجب پور، ۱۳۹۰). بدافزارها به‌عنوان یکی از مهم‌ترین خطرات فضای سایبر در اشکال و اهداف مختلف و با ماهیت‌های ساختاری متنوع روزبه‌روز در حال گسترش و رشد می‌باشند ازاین‌رو می‌توانیم با تحلیل درست شرایط کنونی کشور و هماهنگی بین مراکز پژوهشی فعال در بخش‌های مختلف نیروهای مسلح، از این پتانسیل برای مدیریت صحیح و ایجاد سازوکار یکپارچه برای مقابله با تهدیدات فضای سایبر ازجمله بدافزارها مقابله کرده و زیرساخت‌های حیاتی کشور ازجمله زیرساخت‌های صنعتی، خدماتی و نظامی را مصون نگه‌داریم (صالح نیا و بختیاری، ۱۳۹۷). امنیت سایبری محافظت از سامانه‌ها و ساختارهای اطلاعاتی یک کشور می‌باشد که جهت مهار و مقابله با این‌گونه تهدیدات نیاز به همکاری مؤثر بین دولت‌ها و افراد به وجود می‌آید (رحیمی، احمدی سربرزه، و علی پور، ۱۳۹۸).

۲-۲. بارزترین ویژگی‌های جنگ سایبر

جنگ سایبر به بازیگران این امکان را می‌دهد که بدون توسل به جنگ مسلحانه، به اهداف سیاسی و راهبردی خود دست یابند. فضای مجازی قدرت غیرواقعی به بازیگران کوچک و کم‌اهمیت می‌دهد (آقایی، معینی، عرب سرخی، محمدیان، و زارعی، ۱۳۹۸). در فضای مجازی، مرز بین نظامی و غیرنظامی و نیز فیزیکی و مجازی چندان روشن و شفاف نیست، ازاین‌رو قدرت یا از طریق دولت‌ها، بازیگران غیردولتی اعمال می‌شود یا از طریق پروکسی در کنار سایر میدان‌های سنتی نبرد. مثل زمین، هوا، دریا و فضا، باید فضای

مجازی را پنجمین میدان نبرد دانست (کلفام و حسینی، ۱۳۹۷). ازآنجاکه اینترنت و ارتباطات به‌طور روزافزون در حال گسترش می‌باشد، یک حمله‌کننده سایبری قادر است ۲٤ ساعته در حال ارتباط باهدف خود باشد (Linke & Al-Mohanndi, 2016). از دیگر ویژگی و مؤلفه‌های این فضا می‌توان از توجه رسانه‌ای، تأثیرگذاری بر میزان نیرو، تأثیرات فیزیکی، هوشمندی و سادگی نام برد (Laura, 2016).

۳-۲. ساختار دفاع سایبری در ایران

پیرو رویکرد فعالانه نظامی جمهوری اسلامی در سال‌های بعد از انقلاب و دکترین تعریف‌شده توسط رهبری به‌منظور حضور فعال در عرضه دفاع، ساختارهای پیش‌رونده‌ای در بخش‌های نظامی و غیرنظامی به‌منظور مقابله با این نگاه طراحی و شکل گرفت. 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 ارتباطی شبکۀ جهانی اینترنت و آثار چشمگیر آن در ابعاد زندگی فردی و اجتماعی و لزوم سرمایه‌گذاری وسیع و هدفمند در جهت بهره‌گیری حداکثری از فرصت‌های ناشی از آن در جهت پیشرفت همه‌جانبه کشور و ارائه خدمات گسترده و مفید به اقشار گوناگون مردم و همچنین ضرورت برنامه‌ریزی و هماهنگی مستمر به‌منظور صیانت از آسیب‌های ناشی از آن اقتضا می‌کند که نقطۀ کانونی متمرکزی برای سیاست‌گذاری، تصمیم‌گیری و هماهنگی در فضای مجازی کشور به وجود آید .به این مناسبت شورای عالی فضای مجازی کشور با اختیارات کافی به ریاست رئیس‌جمهور تشکیل می‌گردد و لازم است به کلیۀ مصوبات آن ترتیب اثر قانونی داده شود.» (خامنه ای، ۱۳۹۰). 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) (آقایی، معینی، عرب سرخی، محمدیان، و زارعی، ۱۳۹۸)، پلیس فتا (ناجا) (ذبیح الله نژاد، ۱۳۹٦)، دادسرای جرائم رایانه‌ای (قوه قضائیه) (محمدی، فرهنگ پور، و موسوی هاشمی، ۱۳۹٤)، معاونت رسانه و فضای مجازی (صداوسیما) (رضائیان، ۱۳۹۰)، سازمان پدافند غیرعامل (ستاد کل) (حیدرآزادزاده، بیاتی، واحدیان، و سوکی، ۱۳۹۲)، کمیته پدافند غیرعامل (دولت)، قرارگاه دفاع سایبری (ستاد

کل) (حسینی امینی و محسن زادگان، ۱۳۹۵) و شورای عالی فضای مجازی، گام‌های مؤثری در کاهش تهدیدات سایبری برداشته‌شده است؛ اما به نظر می‌رسد که در این میان یگانی که حوزه مأموریتی 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. جدول ۱ به‌طور خلاصه اقدامات اساسی حوزه سایبری در کشورهای مختلف را گردآوری نموده است (Rajoy Brey, 2013).

جدول شماره ۱: اقدامات اساسی حوزه امنیت ملی سایبری در کشورهای مختلف

کشور	اقدامات اساسی حوزه امنیت ملی سایبری و مقابله با بدافزارها
آلمان	• ترسیم سند راهبرد امنیت سایبری در سال ۲۰۱۱ • ایجاد شورای ملی امنیت سایبر (زیر نظر صدراعظم آلمان) • ایجاد مرکز ملی پاسخ سایبری • ایجاد مرکز دفاع سایبری • ایجاد آژانس امنیت اطلاعات آلمان • ایجاد ساختار سایبری در واحدهای نظامی آلمان و سازمان‌های اطلاعاتی
آمریکا	• هماهنگ‌کنندهٔ ستاد عملیاتی فضای سایبری (زیر نظر رئیس‌جمهور) • سازمان فرماندهی سایبری ایالات‌متحده (فرماندهی سایبری نیروی زمینی، فرماندهی سایبری نیروی دریایی، فرماندهی سایبری نیروی هوایی و فرماندهی سایبری تفنگداران دریایی) • آژانس امنیت ملی (مسئولیت شنود سیگنال و حفاظت از سیگنال را در کشور ایالات‌متحدهٔ آمریکا بر عهده دارد.) • پلیس فدرال آمریکا (مسئولیت مبارزه با جرائم سازمان‌یافته و تروریسم را بر عهده دارد.) • ادارهٔ ارتباطات و امنیت سایبری • بخش امنیت سایبری ملی
فرانسه	• ترسیم سند دفاع و امنیت ملی فرانسه رویکرد تهدیدات سایبری • شورای دفاع و امنیت ملی سایبری (زیر نظر رئیس‌جمهور) • آژانس امنیت اطلاعات و شبکه فرانسه • مرکز عملیات امنیت سامانه اطلاعات • آژانس دفاع سایبر • دفتر مرکزی برای مبارزه با جرم مرتبط با فناوری اطلاعات و مخابرات • مرکز امنیت اطلاعات فرانسه
انگلیس	• دفتر امنیت سایبر در دفتر کابینه • مرکز عملیات امنیت سایبری. (یکی از سه سازمان اطلاعاتی بریتانیا و بخشی از ماشین اطلاعاتی ملی بریتانیا است) • گروه امنیت الکترونیک و ارتباطات • مرکز حفاظت از زیرساخت‌ها • ادارهٔ رسیدگی به جرائم سازمان‌یافته

کشور	اقدامات اساسی حوزه امنیت ملی سایبری و مقابله با بدافزارها
	• گروه عملیات دفاع سایبری

٤-٢. ضرورت ایجاد مرکز فرماندهی سایبری در جمهوری اسلامی ایران جهت مقابله با بدافزارها

حاکمیت سایبری برای یک ملت به دلیل داشتن یک منبع راهبردی از اولویت بالا برخوردار است. حملات بدافزاری، مخابرات، صنعت، اقتصاد، دولت و ارتش را مختل خواهد کرد. امنیت سایبری برای یک ملت مهم است تا امنیت را برای زیرساخت‌های حیاتی کشور فراهم کند و اطمینان حاصل شود که فرآیندهای مبتنی بر اطلاعات سازگار نیستند (گلپرور و خراسانی، ١٣٩٥). این بخش به بررسی ساختار عمومی پیشنهاد شده برای سایبر در نهاد نظامی جهت دفاع از حاکمیت سایبری و ارائه دیدگاه پیشنهادی درباره نحوه ارتقاء ارتش سایبری در نیروی نظامی می‌پردازد. علاوه بر این، مزایای راهبردی را به ارتش نشان می‌دهد و دیدگاه نظامی در اجرای ارتش سایبری را به‌عنوان یک مدل پیشنهادی ارائه می‌دهد.

٥-٢. ارتباط ارتش سایبری با ارتش نظامی

نیروهای نظامی برای محافظت از حاکمیت و یکپارچگی یک ملت ازجمله جامعه مدنی آن در برابر یک کشور متخاصم که هدف آن‌ها خشونت است، به وجود آمده‌اند (محمدی الموتی، ١٣٨٤). ارتش سایبری یک گروه فن‌آوری اطلاعاتی بسیار ماهر از سربازان است یعنی «جنگجویان سایبری» که درک گسترده‌ای از مهارت‌های سایبری دارند قادر به دفاع از زیرساخت‌های حیاتی دولت نظامی و راهبردی می‌باشند و می‌توانند حملات سایبری و حملات از نوع بدافزارها را نیز راه‌اندازی کنند.

٦-٢. قانونی بودن ارتش سایبری

امروزه این نگرانی برای دولت‌ها ایجادشده که حملات مبتنی بر فضای مجازی، می‌توانند سرویس‌های ارتباطی، اقتصادی و حیاتی کشورها را مختل نموده و موجب خسارات شدید گردند (برقعی، ١٣٩٣). مشروعیت دولت‌ها برای داشتن یک ارتش سایبری در ارتش خود، به دلیل تهدید انفجار جهانی فضای اینترنتی توجیه شده است. یک کشور

حق دارد از خود محافظت کند و اگر از طریق حمله سایبری موردحمله قرار گیرد، از خـود دفاع می‌کند.

۲-۷. عملیات ارتش سایبری

انقلاب اطلاعات و فناوری ارتباطات، توان رزمی و تاکتیکی ارتش‌ها را تغییر داده و میـزان موفقیت آن‌ها در میدان نبرد را تعیین خواهد کرد (نـاظمی اردکـانی، نجـات پـور، و احمـدی، ۱۳۹۵). هنگامی‌که حمله تشخیص داده شود، برنامه‌ریزی و توسعه یک اقدام جایگزین یا یـک درخت هدف دفاعی، موردبررسی قرار می‌گیرد یا به یک مورد احتمالی بازمی‌گردد، پـس‌ازآن، عملیات سایبر کامل است.

۲-۸. ارتش سایبری غیردولتی

حامیان غیردولتی (هکرهای مستقل) راه‌اندازی جرائم اینترنتی و اقدامات دفاعی را آغـاز می‌کنند. آن‌ها توسط دولت‌ها، نیروهای نظامی یا بخـش خصوصـی بـرای چنـین اقـداماتی استخدام می‌شوند و هزینه مالی دریافت می‌کنند. حامیان غیردولتی برای اعتقادات خود و یا سود مالی مبارزه می‌کنند و به‌طور مستقل علیه ملت‌ها یا سازمان‌هـای خصوصـی بـه‌عنـوان ارتش سایبری خارج از قدرت نظامی یا حکومت می‌جنگند (Green, 2015).

۲-۹. مقایسه جامع بین ارتش سایبری نظامی در جهان

۲-۹-۱. فرماندهی سایبری ایالات‌متحده آمریکا

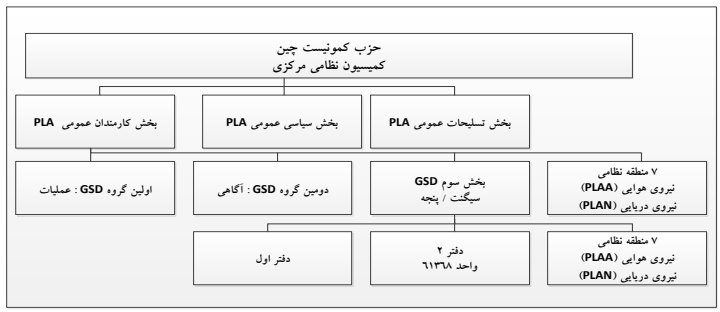
مأموریت تنهـا فرمانـدهی سـایبری آمریکـا، دفـاع از فضـای مجـازی اسـت، خـارج از میدان‌های جنگی سنتی زمین، دریایی، هوا و فضا. آن‌ها سعی در پیـدا کـردن و در صـورت لزوم، حملات سایبری را برای دفاع از شبکه‌های کامپیوتری نظامی خنثی می‌کنند. ایـن امـر با استفاده از روش دفاعی توسط گروه تضمین اطلاعات[1] و در ارتش ایالات‌متحده بـه‌عنـوان یک عملیات اطلاعاتی محسوب می‌شود و از طریق اطمینان از دسترسی، یکپارچگی، احراز هویت، محرمانه بودن با روش‌های حفاظت و دفاع از سـامانه‌هـای اطلاعـاتی، تشـخیص و واکنش موردنظر در رابطه با آن واقعه انجام می‌شود (Grobman, 2018).

1 Information Assurance (IA)

فرماندهی سایبری ایالات‌متحده از چندین بخش خدماتی و همچنین واحدهای خدمات نظامی تشکیل‌شده که خدمات مشترک را به فرماندهی سایبری ارائه می‌دهند. فرماندهی سایبری تحت فرمان راهبردی مستقیم فرماندهان ستادهای مشترک است. نیروهای مأموریت سایبری شامل سه نوع تیم هستند: تیم مأموریت‌های ملی، تیم‌های مأموران مبارز و گروه‌های محافظت از سایبر. علاوه بر این، دولت ایالات‌متحده همچنین از عوامل غیردولتی استفاده می‌کند، مانند شرکت‌های اندگیم[1] اکسدس[2] ووپن[3] و آزمایشگاه ان.اس.اس[4] که اطلاعات مربوط به آسیب‌پذیری را ارائه می‌دهند (Vuuren, Leenen, Aschmann, 2017).

۲-۹-۲. چین

رویکرد چین در دهه ۱۹۹۰ کنترل جریان اطلاعات در فضای سایبری بود (که تا زمان حاضر تغییر قابل‌توجهی نداشته است) و متفاوت از رویکرد آمریکا و غرب است که به حمله و تخریب کمک می‌کند؛ که منجر به «فایروال بزرگ چین» (نام دیگر پروژه گلدن شیلد[5]ست) که جهت نظارت و فیلتر کردن هر بسته داده، فیلتر کردن آدرس اینترنتی و غیره، ورود و خروج از زیرساخت‌های سایبری ملی چین است (Vuuren, Leenen, Aschmann, 2017). عملیات شبکه کامپیوتری چین که بر اساس ساختار واحدهای ارتش آزادی‌بخش مردم می‌باشد در شکل۱ آمده است.

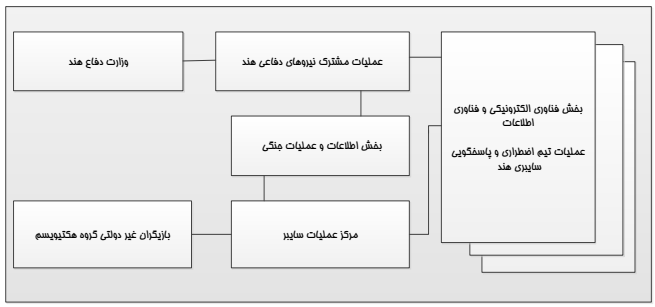


شکل۱ عملیات شبکه کامپیوتری چین که براساس ساختار واحدهای ارتش آزادی‌بخش مردم می‌باشد

1 Endgame
2 Exodus
3 Vupen
4 NSS
5 Project Golden Shield

۳-۹-۲. هند

رویکرد هند به جنگ سایبری برای استفاده از یک ثبت ملی است؛ بـه نـام پایگـاه ملـی امنیت[1]که بر ضبط و ثبت متخصصان آموزش‌دیده فنـاوری اطلاعـات و امنیـت سـایبری در هند تمرکز دارد. این دفتر ثبت برای «هکرهای سفید» ثبت‌نام می‌کند که می‌تواند در صورت نیاز توسط ارتش هند، استخدام شوند و برای اجرای عملیات اینترنتی با یـک جـزء نظـامی کوچک سایبری که مدیریت و برنامه‌های سـایبری بـرای ارتـش را برنامـه‌ریـزی مـی‌کنـد، مورداستفاده قرار گیرد. رویکرد هند به‌عنوان یک کشور، یک شبکه کامپیوتری دفـاعی قـوی است و تعدادی از گروه‌های پاسخ اضطراری سایبری[2]را برای جلوگیری از هکرهـا، عوامـل غیردولتی و یا دیگر ارتش‌های سایبری از نفوذ بـه فضـای سـایبری هنـد دارد. ارتـش هنـد دستور داده است که در رابطه با عملیات سایبری مشارکت داشته باشد. بااین‌حـال، در برابـر حملات سایبری واکنش بیشتری نسبت به داشتن یـک رویکـرد پیشـگیرانه بـرای عملیـات اینترنتی دارد. نویسندگان یک ساختار احتمالی را کـه در شـکل ۲ نشـان داده‌شـده طراحـی کرده‌اند.



شکل ۲–ساختار استراتژی سایبری هند (Vuuren, Leenen, Aschmann, 2017)

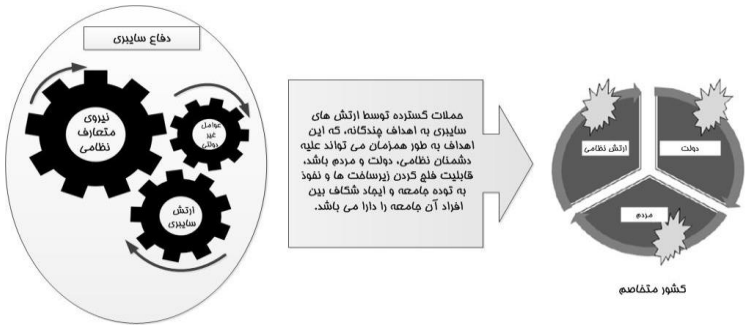
٤. تجزیه و تحلیل یافته‌ها

٤-١. ساختار پیشنهادی برای مرکز فرماندهی سایبری ایران در جهت مقابلـه بـا بدافزارها

تهدیدات دفاعی و امنیتی در سطح ملی نیازمند سامانه‌هایی است که فرماندهی و کنتـرل بحران‌ها و تهدیدات سایبری را ممکن سازد (محمودزاده، نیک نفس، و قوچانی، ١٣٩٦). بر

1 National Security Database (NSD)
2 Cyber Emergency response teams (CERTs)

همین اساس رویکرد یکپارچه در داشتن یک مرکز فرماندهی سایبری در جهت مقابله با بدافزارها در ستاد نیروهای مسلح جمهوری اسلامی ایران این است که به‌عنوان یک دارایی راهبردی در یک ملت به آن دیده شود. ادغام نیروهای نظامی با مرکز فرماندهی سایبری، به توانایی‌های دفاعی و تهاجمی سایبری نیروهای نظامی می‌افزاید. علاوه بر این، ارتش سایبری به‌وسیله جمع‌آوری اطلاعات و آگاهی موقعیت‌ها، اطلاعات تصمیم‌گیرندگان در میدان جنگ، را بالا می‌برد. زیرساخت‌های اطلاعاتی نظامی و دولتی می‌تواند از حملات محافظت شود و در صورت لزوم، زیرساخت‌های انتقالی و پروسه‌های مبتنی بر اطلاعات می‌تواند توسط مرکز فرماندهی سایبری حمله‌کننده سایبری موردحمله قرار گیرند. تمرینات انجام‌شده توسط گروه‌های قرمز و آبی سایبری (قرمز: گروه نفوذ یا گروه حمله و آبی: گروه دفاعی) نیز تأثیر مثبتی در یک کشور خواهد داشت، زیرا این امر اطمینان حاصل خواهد کرد که شبکه‌های کامپیوتری سالم هستند. اگر گروه‌های قرمز و آبی کشور قادر به نفوذ به سامانه‌های خود باشند، احتمال وجود دارد که یک کشور دشمن نیز بتواند این کار را انجام دهد. یک رویکرد یکپارچه برای ایجاد یک مرکز فرماندهی سایبری برای ایران در شکل ۳ نشان داده‌شده است.



شکل ۳ مفهوم یکپارچه برای مرکز فرماندهی سایبری ایران

٤-۲. ملاحظات برای تشکیل یک مرکز فرماندهی سایبری در ایران به‌منظور مقابله با بدافزارها

شاید می‌توان فضای سایبر را به‌مثابه اسلحه‌ای دانست که می‌تواند در صورت برخورد انفعالی در برابر آن اثرات به‌مراتب بیشتر و خطرناک‌تر از سلاح‌های اتمی و شیمیایی داشته باشد. تأکیدات مکرر شخص اول کشور بر شناخت درست فضای سایبر و تحلیل و

تحقیقات ما نشان داده است کشورهای توسعه‌یافته با سرمایه‌گذاری بی‌اندازه در این بخش و استفاده از ژنرال‌های نظامی در مدیریت تمامی سطوح فضای سایبری از این محیط به‌عنوان بستری مطمئن برای شروع و امتداد جنگ استفاده کنند. با توجه به رویکرد دکترین جمهوری اسلامی ایران در بعد دفاعی و تأکید مقام عالی فرماندهی کل قوا، بر تجمیع و تمرکز کشور در این بخش، لزوم ایجاد یک مرکز فرماندهی سایبری و لزوم مدیریت یکپارچه آن با سایر بخش‌های نظامی احساس می‌شود. ازاین‌رو سعی شده است با توجه به پیشینه تحقیقات دلایل زیر را برای تشکیل یک مرکز یا قرارگاه فرماندهی سایبری باهدف شناخت تهدیدات از نقطه آغازین و ایجاد رویکرد دفاعی پیش فعال در برابر خطرات سایبری نام برد:

ـ تغییر ماهیت تهدیدات: مهم‌ترین عامل نیاز کشور به شکل‌گیری و سازمان‌دهی مرکز فرماندهی سایبری، تغییر ماهیت تهدیدات در ادبیات نظامی از جنگ سخت به جنگ نرم می‌باشد. این تغییر ماهیت هم در شکل و هم در فرم قابل‌بررسی است. با شکل‌گیری زیرساخت‌های مبتنی بر ارتباطات و ارزشمند شدن داده‌ها در بخش‌های دولتی و غیردولتی و استفاده از تمامی بخش‌ها ازجمله صنعت، آموزش، کشاورزی و حمل‌ونقل از فنّاوری‌های شبکه‌ای، گسیل تهدیدات به این سمت امری اجتناب‌ناپذیر است.

ـ کم‌هزینه بودن جنگ‌های نامتقارن: شاید می‌توان به کمترین فضای لازم برای پاسخ‌گویی در هر سطح از تهدیدات را فضای سایبری دانست. مدیریت منابع درست و استفاده از نیروهای کارآمد با بهره‌وری بالا مفهومی است که در جنگ‌های نامتقارن به‌عنوان کلیدواژه پیروزی یافت می‌گردد. به دلیل بهینه بودن این مفهوم در ساختار نیروهای نظامی ما و وجود مدیران و فرماندهان ارشد در این حوزه که باتجربه جنگ تحمیلی شناخت کافی از این نوع جنگ را دارا می‌باشند، ترکیب این دیدگاه با رویکرد دفاعی در فضای سایبری امکان مواجهه به‌موقع و آنی را با تهدیدات این بخش فراهم می‌سازد.

ـ گستردگی و تنوع: به‌جرئت می‌توان فضای سایبر را برای دشمنان به‌عنوان جذاب‌ترین بخش معرفی نمود. تنوع و گستردگی روزافزون تهدیدات و نبود زیرساخت‌های مناسب و عدم خودکفایی هم در حوزهٔ تجهیزات هم در حوزهٔ فرایندها، لزوم مدیریت یکپارچه این

محیط را با کمک تجربیات به‌دست‌آمده در حوزهٔ نظامی ترکیب و بـه یـک مـدل مسـتقل و البته کارا دست‌یافت.

در هنگام تشکیل یک مرکز فرماندهی سایبری در زیرمجموعه ستاد کل نیروهای مسـلح به‌منظور مقابله با بدافزارها و دفاع از زیرساخت‌هـای حیـاتی و حسـاس اطلاعـاتی کشـور می‌بایست ملاحظات و وظایف زیر باید موردتوجه قرار گیرد:

- تجزیه‌وتحلیل آسیب‌پذیری و تهدید سایبری؛
- سیاست، استراتژی و قوانین دفاعی و تهاجمی سایبری
- ارتقای آمادگی سایبری در دولت، سازمان‌ها و بخش‌های خصوصی در خصـوص حملاتی چون بدافزارها؛
- قابلیت اتصال فضای سایبر به‌صورت یکپارچه و متمرکز در دولت؛
- سطوح مهارت سایبر و محققان سایبری؛
- توسعه و تأمین مالی سلاح‌های سایبری؛
- همکاری بین گروه‌های امنیتی وادارات قضایی؛
- ایجاد کنسرسیوم دفاعی نظامی در حوزهٔ سایبر.

٤-٣. استراتژی و برنامه‌های عملیاتی پیشنهادی جهت مقابله با حملات سایبری و مقابله با بدافزارها در جمهوری اسلامی ایران

با توجه به پیامدهای بسیار زیان‌بار حملات بـدافزاری اتخـاذ تـدابیری بـرای تـدوین و انتخاب استراتژی ملی برای آماده‌سازی در برابر جنگ سایبری، ضروری است. در ادامه این بخش پیشنهادی به جهت تدوین اسـتراتژی سـایبری بـه‌طـور خـاص بـه‌منظـور مقابلـه بـا بدافزارها در کشور جمهوری اسلامی ایران می‌پردازیم.

٤-٤. پیشنهاد یک مرکز فرماندهی سایبری به‌منظور مقابله با بدافزارها

توسعه سامانه‌های الکترونیک، با چالش‌ها و مشکلات زیادی ازجمله، قابلیت همکاری، یکپارچگی، پیچیدگی و عدم وجود استانداردها مواجه است. معماری سازمانی یک ابزار کارآمد برای غلبه بر این چالش‌ها در نظر گرفته می‌شود. تا به امروز چارچوب‌های معماری

سازمانی زیادی ارائه‌شده است ازجمله آن‌ها چارچوب معماری سازمانی زکمن[1]نام برد. در این پژوهش سعی شده است تا معماری پیشنهادی با معماری سازمانی زکمن به‌عنوان یک چارچوب مادر منطبق گردد.

مدل پیشنهادی، متشکل از چهار بخش کلان که به ترتیب پاسخی برای جنبه محتوایی از چارچوب معماری زکمن (موجودیت، وظیفه، مکان، افراد و زمان) می‌باشد، تشکیل‌شده است. دلیل، انگیزه، چرایی و نقش مرکز فرماندهی سایبری در جمهوری اسلامی ایران را می‌توان حفاظت از حاکمیت ملی قلمداد کرد، ازاین‌رو برای حفاظت از اطلاعات، فعالیت‌ها و هویت مردم، دولت و زیرساخت‌های سایبری غیرنظامی می‌توان نقش‌های زیر را به‌صورت خاص برای تشکیل یک‌نهاد سایبری زیر نظر ستاد کل نیروهای مسلح و به‌منظور دفاع و مقابله با تهدیدات ازجمله بدافزارها مهم دانست:

- ایدئولوژی، سیاست، استراتژی، دکترین و حکمرانی مرکز فرماندهی سایبری؛
- ایجاد یک سیستم فرماندهی سایبری متمرکز؛
- توانایی تحقیق و توسعه در محیط سایبری؛
- ایجاد توانایی‌های سایبری تهاجمی و دفاعی؛
- انجام رمزنگاری و تجزیه‌وتحلیل رمزنگاری؛
- حفظ توانایی‌های فرماندهی سایبری، برنامه‌ریزی، هماهنگی و اجرای عملیات سایبری (تهاجمی و دفاعی)؛
- ارتباط بین عوامل امنیت سایبری؛
- جمع‌آوری و تجزیه‌وتحلیل اطلاعات در حوزهٔ سایبری؛
- استخدام رزمندگان سایبری؛
- آموزش و ارتقای ظرفیت رزمندگان سایبری؛
- همکاری با متخصصان سایبری خارجی؛

1 Zachman Enterprise Architecture Framework

دستیابی به این وظایف برای یک مرکز فرماندهی سایبری اجازه می‌دهد تا یک سازمان نظامی جهت و هدف داشته باشد. ساختار پیشنهادشده برای مرکز فرماندهی سایبری ایران در شکل ٤ نشان داده‌شده است.[1]

۱. تدوین راهبردی سایبری: این واحد با شناخت نقاط قوت و ضعف داخلی و همچنین بررسی و مطالعه تهدیدات و فرصت‌های موجود درزمینهٔ جنگ سایبری به تدوین راهبردهای مقابله‌ای در سطوح مختلف می‌پردازد. یکپارچه‌سازی و کلاسترینگ استراتژی‌های امنیتی ازجمله اهداف این بخش می‌باشد که به ارائه فهرستی ازآنچه برای سازمان دارای اهمیت است و شناخت موجودیت‌ها و برنامه‌ریزی جامع و راهبردی در جهت نیل به اهداف و تعیین خطوط کلی فعالیت‌ها و مأموریت‌های سازمان در درازمدت می‌پردازد. از مهم‌ترین مأموریت‌های این بخش می‌توان به موارد ذیل اشاره کرد:

• تعیین و تدوین اهداف آینده مرکز	• شناخت اهداف و استراتژی‌های موجود
• تجزیه‌وتحلیل شرایط محیطی مرکز	• تجزیه‌وتحلیل منابع و امکانات
• شناخت وضع موجود	• تعیین تغییرات مورد لزوم در استراتژی‌ها
• تصمیم‌گیری در مورد استراتژی مطلوب	• اجرای استراتژی جدید
• کنترل و سنجش استراتژی جدید در عمل	•

۲. واحد بازنگری راهبردی سایبری: مطابق با چارچوب معماری زکمن، این بخش فهرست فرآیندهایی که توسط مرکز فرماندهی سایبری انجام می‌گردد جمع‌آوری و راهبردهای سایبری بروزرسانی می‌گردد و قابلیت‌های رمزگذاری و نگهداری اطلاعات و دیتاهای حساس را توسعه می‌بخشد. در این واحد علاوه بر تحقیق و توسعه اقدامات جدید در حوزهٔ دفاع سایبری، به مطالعه و پیاده‌سازی روش‌های مختلف رمزنگاری و پنهان‌سازی اطلاعات می‌پردازد. از مهم‌ترین مأموریت‌های این بخش می‌توان به موارد ذیل اشاره کرد:

- به‌روزرسانی راهبردهای دفاع سایبری با رصد مستمر تهدیدات جنگ سایبری؛
- ® مطالعه و شناخت فنّاوری‌های روز در حوزهٔ رمزنگاری و پنهان‌سازی؛
- اجرا و پیاده‌سازی روش‌ها و الگوریتم‌های بومی در این حوزه؛

[1] جهت اطلاع بیشتر به دفتر فصلنامه مراجعه شود.

- امن سازی بسترهای حساس و تصمیم‌ساز اطلاعاتی با استفاده از فنّاوری‌های بومی.

۳. مرکز عملیات سایبری: از سه زیرمجموعه تشکیل‌شده است: بخش اول، برنامه‌ریزی، تجزیه‌وتحلیل و رمزنگاری که کلیه عملیات و اقدامات در حفظ، نگهداری و ذخیره‌سازی امن اطلاعات و داده‌های مراکز مختلف برنامه‌ریزی و نگهداری می‌شود. ازجمله وظایف این بخش می‌توان به طراحی و استقرار سامانه‌های رمزنگاری، مدیریت کلید و پنهان‌سازی بومی، پیاده‌سازی و استقرار استانداردهای داخلی به‌منظور حفظ و نگهداری اطلاعات مهم و حساس اشاره کرد. بخش دوم، دفاع سایبری است که تضمین‌کننده برنامه‌ها و تعهدات عملیات امنیتی در حوزهٔ مقابله با بدافزارها و ردیابی و مقابله با تهدیدات سایبری محسوب می‌شود.

مرکز عملیات امنیتی شامل یک گروه مقابله با تهدیدات و تیمی جهت ردیابی و ره‌گیری تهدیدات و حملات بدافزاری می‌باشد که در این بخش می‌بایست با رویکرد فعالانه دفاعی به طراحی ابزارها و راه‌حل‌هایی برای تحلیل آنلاین بدافزارها، مشاهده رفتارهای آن‌ها و پیش‌بینی اثرات آن‌ها در بخش‌های مختلف خدمات و صنعت پرداخته شود. بخش سوم حمله سایبری است که تمامی برنامه‌ریزی‌ها و کنترل عملیات در مرکز فرماندهی سایبری شامل نیروهای سایبری زمینی، دریایی و هوایی و نیروهای ویژه از این بخش پشتیبانی می‌نمایند.

در این بخش با تمرکز بر شناخت و رصد دقیق حملات، می‌بایست راهبردهای پاسخ فعالانه و تقابلی در برابر رخنه‌ها و آسیب‌پذیری کشورهای متخاصم اتخاذ شود. این موضوع شامل تشکیل گروه‌های تخصصی، تشکیل ساختار متمرکز، مطالعه و تحقیق درباره زیرساخت‌های کشورهای مختلف در حوزهٔ امنیت سایبری و تحلیل رفتار کاربران مهم آن‌ها در بازه زمانی مشخص می‌باشد و با طراحی اطلس دفاع سایبری راه‌کارهایی برای جبران و پاسخ مناسب به این جملات در سطوح مختلف ایجاد می‌گردد که مکان‌های اصلی سازمان را تشکیل می‌دهد و به دیدگاه مکانی از چارچوب معماری زکمن پاسخ می‌دهد. همچنین همان‌گونه که قبلاً بیان داشتیم، قدرت امنیت سایبری کشورها صرفاً

باقابلیت حمله سایبری و توانایی‌های دفاعی آن کشور قابل‌سنجش باشد. افـراد در معمـاری زکمن بخش مهمی از سازمان را تشکیل می‌دهند، در طرح پیشـنهادی یگـان‌هـای سـایبری (زمینی، هوایی، دریایی و نیروهای ویژه) با همراهی نیروی ارتش نظـامی بـه تحلیـل رفتـار بازیگران غیردولتی (گروه‌های تروریستی، جاسوسان و مجرمان سازمان‌یافتـه، هکرهـا و...) می‌پردازند و از رفتار آن‌ها الگـوبرداری مـی‌کننـد و در جهـت تعلـیم و برنامـه‌ریـزی‌هـای استراتژیک بهره می‌جویند.

٤. هوشمندی تهدیدات سایبری[1]: هوشمندی تهدیدات فرایند دسـتیابی بـه اطلاعـات از منابع متعدد می‌باشد و مفهومی برای به‌دست آوردن دانش در مورد تهدیدات در یک محیط خاص دارد. هوشمندی تهدیدات به‌عنوان دانش مبتنی بر شواهد، شامل مفـاد[2] مکانیسـم‌هـا، شاخص‌ها[3] پیامدهای و توصیه‌های عملی در مورد یک تهدید موجود یا در حـال ظهـور یـا دارای خطر، توضیح داد که می‌تواند تصمیم‌گیری در مورد پاسخ به آن خطـر یـا مخـاطرات ارائه دهد. ازآنجایی‌که هدف و چارچوب امنیت سنتی، محافظت از دارایی‌هـا و دسـتگاه‌هـا است، در نظر گرفتن شناسایی تهدید[4] به‌عنوان تکامـل فراینـدها و رویـه‌هـای امنیـت سـنتی یک‌قدم طبیعی محسوب می‌شود تا بتوان با توجه به هدف اصلی هوش تهدیـد، حـوادث را زودتر شناسایی نمود و نهایتاً زمینه‌ای برای جلوگیری از تهدیدات ایجاد کرد. مدیران به‌طور فزاینده‌ای هوشمندی تهدیدات را ابزاری باارزش می‌دانند و اکنون درک و به‌کـارگیری ایـن ابزار به یک ضرورت برای تجارت تبدیل‌شده است. متخصصان امنیتی همچنین می‌دانند کـه مهاجمان معمولاً درک بهتری از شبکه سازمانی نسبت به آنچه آن‌ها برای امنیت سـازمان در نظر گرفته‌اند، در دست دارند. یکی از برنامه‌های موفـق شناسـایی تهدیـد در یـک محـیط، هنگام تعامل با برنامه امنیتی سازمان است. وضعیت امنیتـی[5] فراینـدی اسـت کـه نقشـه بـین تجارت و دارایی‌های شناسایی تهدید را توصیف می‌کند. نتیجه ایـن تجزیـه‌وتحلیـل تعیـین دارایی‌های مهم است که باید محافظت شود. هوشمندی تهدیدات سایبری تلاش دارد تا بـا

1 Cyber Threat Intelligence (CTI)
2 context
3 indicators
4 Threat Identification (TI)
5 Security Posture

فراهم نمودن فهرست رویدادهای مهم سازمانی و به اشتراک‌گذاری بهنگام دانشی که بر پایهٔ شواهد تهدید به دست می‌آید، سازمان‌ها را در محافظت، تشخیص و پاسخگویی به این تهدیدهای روزافزون یاری کند که به دودسته راهبردی و فنی تقسیم می‌شوند. «هوش تهدید راهبردی» بیشتر انسان‌محور است اعضای این گروه می‌توانند جزو رزمندگان سایبری نیروهای مسلح و ارتش نظامی سایبری و یا از عوامل غیردولتی و دانشجویان و راهبران در حوزهٔ امنیت اطلاعات باشند و گزارش‌هایی که در تصمیم‌گیری‌های ذاتاً بلندمدت کاربرد دارد را تدوین نمایند. گروه اطلاعاتی تهدید و پاسخگویی به حوادث در یک سازمان معمولاً از مدیران، تحلیلگران و مهندسان که دانش عمیقی در مورد فرآیندهای سازمان دارند تشکیل‌شده است که می‌توانند برای تشخیص سریع‌تر فعالیت‌های مشکوک به شناسایی تهدید اعتماد کنند.

«هوش تهدید فنی» از ابزارهای هوشمندی تهدید اطلاعات برای جلوگیری از حملات، در عملیات روزمره و عادی استفاده می‌کند تا با تحلیل شرایط عادی، تغییرات و روند حملات توسط یک بازیگر تهدیدکننده را شناسایی کند. این ابزار ناظر است بر اطلاعات فنی از قبیل لیست IP های بدخواه که معمولاً در سامانه‌های اطلاعاتی استفاده می‌شوند.

مرکز فرماندهی سایبری متمرکز باید فهرستی از اهداف و راهبردها، نتایج و عوامل حیاتی موفقیت را دارا بوده و تحت فرماندهی نظامی راهبردی باشد تا بتواند با ترکیب اساسی و عناصر ارتش سایبری منطبق شود و جهت استراتژیک را تضمین کند. با توجه به‌ضرورت توسعه فن‌آوری‌های دفاعی و سلاح‌های تهاجمی سایبری، دفاع سایبری، سرمایه‌گذاری عظیمی برای کشور خواهد بود. مرکز فرماندهی سایبری ایرانی، جزء مرکز عملیات سایبر باید عناصر زیر را نیز دارا باشد:

مؤلفه دفاعی که در مواجه با حملات بدافزارها، دفاع سایبری را در داخل مرکز فرماندهی سایبری و حکومت اجرا کند و به یک سیاست امنیتی سایبری و زیرساخت‌های ملی امنیت سایبری مرتبط باشد؛

رمزنگاری و تجزیه‌وتحلیل برای اطمینان از اطلاعات طبقه‌بندی‌شده ورودی و خروجی دولتی و نظامی، ضروری است؛

ارزیابی تهدیدات سایبری و آسیب‌پذیری‌های بدافزاری به‌صورت منظم؛

جهت پیش‌بینی آسیب‌پذیری بالقوه، نوآوری‌های فنّاورانه در سامانه‌های ICT در حوزه‌های راهبردی و زیرساخت‌های بحرانی مورد نظارت قرار گیرند؛

تجزیه‌وتحلیل مربوطه را با اپراتورهای خدمات ضروری و زیرساخت‌های بحرانی از طریق پلتفرم‌های نهادی اختصاصی اشتراک گذاشته شود؛

همکاری با دانشگاه‌ها و مراکز تحقیقاتی به‌منظور توسعه روش‌ها و فن‌آوری‌های جدید برای شناسایی/تجزیه‌وتحلیل آسیب‌پذیری‌ها و تهدیدات؛

بهبود قابلیت‌های جمع‌آوری، تجزیه‌وتحلیل و انتشار در تهدیدات اینترنتی؛

بهبود تشخیص تهدید از طریق توسعه نظارت بر ترافیک و قابلیت‌های تجزیه‌وتحلیل؛

اجرای رویه‌های هشدار زودهنگام؛

ایجاد قابلیت‌های یکپارچه اطلاعات (بین سازمان و چند منبع)؛

به جهت تسهیل، اطلاعات بین مقامات دولتی و بخش خصوصی به اشتراک گذاشته شود؛

در جهت بهبود قابلیت‌های یکپارچگی در پاسخ‌دهی از اپراتورها در زیرساخت‌های حیاتی در حوزهٔ سایبری استفاده شود تا با توجه به پروتکل‌های از پیش تعیین‌شده و به‌منظور ایجاد طرح‌های جدید قانونی و ایجاد گروه‌های مداخله فنی بتوان پشتیبانی از ادارات مرکزی را تسریع بخشید؛

قابلیت برنامه‌ریزی و اجرای عملیات نظامی به ساختارهای فرماندهی و کنترل سایبری داده شود؛

ایجاد رویه‌ها و ابزارهای مناسب برای پردازش تجربه‌های آموخته‌شده و مدیریت رویدادهای سایبری؛

فعالیت‌های پشتیبانی شده توسط جلسات نهادی، گروه‌های فنی و سازمان‌های صالح مربوط به زیرساخت‌های بحرانی و اپراتورهای خدمات ضروری و همچنین سایر عوامل راهبردی ICT به‌صورت دوره‌ای برگزار گردد؛

به‌منظور مدیریت مؤثر خطرات بدافزاری، همکاری میان مقامات صالح، مؤسسات، سازمان‌های خصوصی و نهادهای مشارکتی را در میان مسئولیت‌های بحرانی ایجاد گردد؛

تعیین استانداردهای ارزیابی خاص و توسعه فرمت‌های ارتباطی برای ارزیابی آسیب‌پذیری زیرساخت‌ها؛

تعلیم و آموزش‌وپرورش فرهنگ امنیت فناوری اطلاعات و ارتباطات و توسعه تعالیم؛
آگاهی امنیتی در حوزهٔ بدافزارها به شهروندان، دانشجویان، شرکت‌ها وادارات دولتی در جهت سازمان‌دهی ابتکارات؛
شرکت در دوره‌ها و برنامه‌های سازمان‌های بین‌المللی درزمینهٔ امنیت سایبری و مقابله با بدافزارها؛
بالا بردن سطح آگاهی در میان تصمیم‌گیرندگان در آخرین تحولات تهدیدات بدافزاری؛
سازمان‌دهی تمرینات آموزشی برای اپراتورها و مدیران امنیت سایبری و همچنین مدیران سامانه‌های IT و شبکه‌ها؛
توسعه، آزمون و اعتبارسنجی فعالیت‌های سایبری از طریق ابزار شبیه‌سازی، تمرینات مشترک و آموزش در حین کار.
تمرکز بر توانایی‌های آموزشی سایبر در مراکز آموزش عالی، ادغام مراکز موجود و تسهیل درگیری مستقیم سازمان‌های خصوصی و سایر سازمان‌های سهیم؛
ایجاد همکاری با دانشگاه‌ها و مراکز تحقیقاتی برای ایجاد دوره‌های آموزشی و دوره‌های خاص برای مدیریت عمومی و کارکنان شرکت‌های خصوصی؛
تقویت روابط با کشورهای اسلامی و سایر شرکای راهبردی درزمینهٔ تقویت بنیه دفاعی سایبری و مقابله هوشمند با تهدیدات بدافزارها و نرم‌افزارهای مخرب؛
قابلیت همکاری در برنامه‌ریزی و اجرای عملیات امنیتی سایبری در حوزهٔ بدافزار از طریق ارتقا فعالیت‌های مشترک در دفاع، وزارت کشور و سطوح چندملیتی؛
شرکت در جلسات بین‌المللی برای نظارت بر آخرین تحولات و حفظ سطح ملی؛
ایجاد یک گروه واکنش به حادثه امنیتی کامپیوتر[1] که مسئولیت حمایت فعالانه اپراتورهای دولتی و خصوصی در مورد حملات بدافزاری و اختلالات را داشته باشد، ضروری است تا در جریان انتقال این دستورالعمل، گروه‌های واکنش اضطراری رایانه‌ای، ابزار و روش‌های خود را در یک اقدام مدیریت هماهنگ شده در برابر حوادث سایبری ابراز و اعلام دارند؛

1 Computer Emergency Response Teams (CERT)

یک نقطه تماس و یک یا چند گروه پاسخگویی به حوادث کامپیوتری را باقابلیت پاسخگویی کامل ایجاد کنید (طبق دستورالعمل موسسه ملی فناوری و اطلاعات[1])؛

هماهنگی ظرفیت‌های فعلی عوامل ملی امنیت سایبری، (مرکز ملی رایانه‌های ضد جرم و جنایت برای حفاظت از زیرساخت‌های بحرانی، اطلاعات) با الزامات NIST؛ و شناسایی مکانیسم‌های همکاری در میان آن‌ها؛

ایجاد مدل مدیریت خودکار و استاندارد حوادث سایبری با تمرکز خاص بر بدافزارها؛

به حداقل رساندن تأثیر حوادث سایبری فناوری اطلاعات به‌ویژه بدافزارها و آن حوادث که باعث از دست دادن اطلاعات و یا اختلال در سامانهٔ IT می‌گردد؛

در نظر گرفتن قوانین ملی زیرساخت‌های حیاتی و تحت پوشش قرار دادن بخش‌هایی از این قوانین؛

تطبیق تعهدات ملی به اپراتورهای دولتی و خصوصی و ساده‌سازی فرایندهای اطلاع‌رسانی حادثه‌ای برای به حداکثر رساندن اثربخشی سیاست‌های امنیت سایبری؛

به‌روزرسانی قوانین در مورد امنیت سایبری، ازجمله فعالیت‌های مربوط به بدافزارها، مطابق با قوانین روز دنیا؛

ایجاد مقررات قانونی برای استقرار ابزارهایی جهت شناسایی و مقابله با تهدیدات اینترنتی؛

ایجاد یک چارچوب قانونی برای شناسایی نقض‌های امنیتی (و تحریم‌های مرتبط) توسط مدیران شبکه و کاربران؛

شناسایی و به‌روزرسانی اقدامات امنیتی پایه‌ای برای شبکه‌های دولتی و شبکه‌های اطلاعاتی بحرانی؛

یک سامانهٔ حسابرسی برای سازمان‌های مسئول صدور گواهینامه‌های امنیتی دیجیتال و IT ایجاد شود؛

مدیریت چارچوب ملی برای صدور گواهینامه ICT از محصولات و خدمات طبقه‌بندی نشده؛

طرح ملی صدور گواهینامه سامانه‌های اطلاعاتی به‌روز نگه‌داشته شود؛

---

1 National Institute of Standards and Technology (NIST)

ارتقاء قابلیت عملیاتی مرکز ارزیابی و تأسیس آزمایشگاه جهت ارزیابی فنی محصولات و سامانه‌های ICT؛

شرکت در فعالیت‌های سازمان‌های بین‌المللی که مدیریت متوازن‌سازی استانداردهای صدور گواهینامه را اداره می‌کنند؛

به‌طور منظم از طریق چک‌های فنی و رویه‌ای، سامانه‌های حفاظت آزموده شوند؛

ایجاد یک سیستم کنترل مستقل (نظیر ممیزی خارجی)؛

امنیت قطعات سخت‌افزاری و نرم‌افزاری، به‌ویژه آن‌هایی که توسط زیرساخت‌های بحرانی و اپراتورهای استراتژی ملی تصویب‌شده است؛

تحریک ایجاد یک زنجیره تأمین ایمن و انعطاف‌پذیر برای اجزای ICT، توسط اعتبارسنجی و ارزیابی انعطاف‌پذیر و کارآمد و درنهایت صدور گواهینامه، پشتیبانی می‌شود؛

ارتقاء نوآوری فناوری اطلاعات و ارتباطات، همچنین از طریق یک بسته محرک بالقوه، برای ایجاد یک پایگاه صنعتی رقابتی در سطح ملی و بین‌المللی و تسهیل ایجاد یک زنجیره عرضه عمودی بر اساس طراحی امنیتی؛

بهبود برنامه‌های همکاری دوجانبه و چندجانبه برای بهبود تحقیقات و توسعه ملی در سطح ارتش سایبری و ارتش نظامی؛

تسهیل ایجاد یک آزمایشگاه دولتی برای تجزیه‌وتحلیل تطبیقی سامانه‌های ICT که توسط ادارات دولتی و زیرساخت‌های بحرانی اتخاذ می‌شود؛

به‌منظور افزایش بهره‌وری ارتباطات ظرفیت هماهنگی در مورد آگاهی موقعیتی ایجاد شود تا واکنش و اقدامات اصلاحی تسهیل یابد و ارزیابی زمان انتشار برای عموم و شناسایی کانال‌های ارتباطی مناسب ایجاد گردد؛

شناسایی اولویت‌ها و بودجه مربوط به امنیت سایبری و زیرساخت‌های بحرانی و نیز هزینه‌های مربوط به توسعه ظرفیت اساسی ازنظر منابع مالی و سرمایه انسانی؛

شناسایی معیارهای مرتبط برای ارزیابی تأثیرات اقتصادی رویدادهای سایبر (تشخیص، اصلاح، آسیب‌شناسی، از دست دادن مشتریان و رقابت و غیره)؛

تجزیه‌وتحلیل ساختارهای بحرانی در حوزهٔ بدافزار و وابستگی متقابل به‌منظور بهبود ارزیابی اثرات اقتصادی رویدادهای سایبری که «تأثیراتی مشابه دومینو» دارند؛

نقشه حوادث و سناریوهای بالقوه ازنظر اقتصادی؛
اجرای مقررات هزینه‌های حفاظت از امنیت سایبری در سطح ملی و بین‌المللی (از طریق برنامه‌های همکاری)؛
با پیگیری بهترین شیوه‌های بین‌المللی، همکاری‌های استخدامی هماهنگ شده بین منابع تخصصی تسهیل شود؛
اقدامات ارزیابی ریسک را در سطح ملی پذیرش کنید؛
شناسایی یک روش منحصربه‌فرد و توافق شده برای مدیریت ریسک سایبری و خدمات ضروری، در زیرساخت‌های حیاتی و دیگر عوامل راهبردی ملی؛
بخش تحقیقاتی و دانشگاهی را در توسعه ابزارهای مدیریت ریسک دخیل کنید.

۵. نتیجه‌گیری و پیشنهاد

ارتش سایبری (فرمان سایبری) برای یک کشور، گسترش قدرت نظامی کشور برای بستن شکاف در حوزهٔ اطلاعات است. این امر دفاع و حفاظت از قلمرو فنّاورانه و فضای سایبر کشور را تقویت خواهد کرد و می‌تواند به‌طور اتفاقی یک حملهٔ سایبری (حملات از نوع بدافزاری و ...) از یک کشور دشمن را متوقف کند. از مزایای این راهبرد، حفاظت از حاکمیت ملی سایبری و توانایی تلافی علیه حملات سایبری خواهد بود؛ که به افزایش اقتصادی ملت کمک خواهد کرد و به دلیل یک فضای سایبر ملی امن، رشد فنّاوری در کشور و دفاع از سایبر و سلاح‌های سایبری در برابر تهاجم‌ها ایمن خواهد شد. متناسب با پیچیده‌تر شدن روابط و شبکه‌های اجتماعی در عصر پست‌مدرنیته و خارج شدن این روابط از حالت‌های ساده اولیه که جنبه فیزیکی و محسوس داشت، بر اهمیت افزایش امنیت فضای مجازی و بررسی فرصت‌ها و آسیب‌های احتمالی آن بر ابعاد مختلف اقتصادی، فرهنگی و سیاسی افزوده‌شده که این خود ضرورت تبیین نظام جامع مدیریتی برای تهدیدات امنیتی در فضای سایبری را دوچندان کرده است.

در این مقاله تعاریف و مفاهیم در رابطه با تهدیدات، جنگ، حمله و امنیت فضای سایبری مطرح شد و اهداف و استراتژی‌های امنیتی در سطح ملی و بین‌المللی موردبررسی قرار داده شد. همچنین اقدامات قابل‌توجه در حوزهٔ امنیت اطلاعات و مقابله با بدافزارها و

دستورالعمل‌های راهبردی و ساختار دفاعی ایران و دیگر کشورهای جهان بررسی شد. درنهایت ارتش سایبری ایران موردبررسی قرار گرفت و یک ساختار پیشنهادی در جهت ادغام ارتش نظامی و نیروهای مسلح با ارتش سایبری در جهت مقابله با بدافزارها داده شد که از حملات گسترده توسط ارتش سایبری ممانعت به عمل‌آورده و سبب حفاظت اطلاعات، فعالیت‌ها و هویت مردم، دولت و زیرساخت‌های سایبری می‌گردد. در آینده به جهت دستیابی به ارزش‌های اساسی حاکم بر حوزه پدافند سایبری کشور و نهادینه‌سازی فرهنگ، ادبیات و آموزه‌های پدافند سایبری به ارائه طرحی در جهت پیاده‌سازی و مصون‌سازی زیست‌بوم سایبری در برابر تهدیدات و تهاجم سایبری پرداخته خواهد شد تا متناسب با تهدیدات بتوان دانش و فناوری پدافند سایبری را تولید و مدیریت نمود.

فهرست منابع و مآخذ

الف. منابع فارسی

- اسماعیل‌زاده، م. و رجب پور، م. (١٣٩٠)، «**بررسی نقش جنگ سایبری در عملیات مشترک و مرکب**»، فصلنامه علمی علوم و فنون نظامی، ٦٧-٨٧.
- برقعی، س. (١٣٩٣)، «**مروری بر امنیت سایبری؛ درس‌هایی برای جمهوری اسلامی ایران**»، شمارهٔ ٣٨ علمی-پژوهشی (وزارت علوم)/ISC، ١٠٤-٨٥.
- حسینی امینی، ح. و محسن زادگان، ا. (١٣٩٥)، «**فضای سایبر، قدرت هوشمند با رویکرد پدافند غیرعامل**»، مجموعه مقالات همایش ملی پدافند غیرعامل و علوم انسانی، ٥٤٣-٥٦٨.
- حیدرآزادزاده، م. بیاتی، ن. واحدیان، ع. و سوکی، م. (١٣٩٢)، «**مبانی پدافند غیرعامل در حوزهٔ امنیت فناوری اطلاعات**»، ششمین کنگره انجمن ژئوپلیتیک ایران پدافند غیرعامل.
- خامنه‌ای، س. (١٣٩٠، ١٢ ١٧)، «**تشکیل شورای عالی فضای مجازی**»، بازیابی از پایگاه اطلاع‌رسانی دفتر مقام معظم رهبری: https://www.leader.ir/fa/content/9213
- درویشی، ع. و صادقی، ر. (١٣٩٤)، «**ارتش سایبری و پیش‌بینی بعد از حملهٔ سایبری**»، نخستین اجلاس بین‌المللی فناوری اطلاعات. دولت‌آباد: نخستین اجلاس بین‌المللی فناوری اطلاعات.
- ذبیح‌الله نژاد و. (١٣٩٦)، «**نقش پلیس فتا در پیشگیری وضعی و پیشگیری اجتماعی از جرائم سایبری**»، فصلنامه دانش انتظامی البرز، ٦٧-٨٩.
- رحیمی، پ. احمدی سربرزه، م. و علی پور، ه. (١٣٩٨)، «**مطالعه تأثیر متغیرهای نوین آینده‌پژوهی و کارآفرینی بر مدیریت راهبردی امنیت سایبری کشور**»، دومین اجلاس ملی پدافند سایبری.

- رضائیان، س. (۱۳۹۰)، «**مورد کاوی طراحی مدل ساختاری معاونت رسانه‌های مجازی سازمان صداوسیما با بهره‌گیری از معماری سازمانی و رویکردهای نوین مدیریتی**»، نهمین اجلاس بین‌المللی مدیریت.
- زابلی زاده، ا. و وهاب پور، پ. (۱۳۹۷)، «**قدرت بازدارندگی در فضای سایبر**»، مطالعات میان‌رشته‌ای در رسانه و فرهنگ سال هشتم بهار و تابستان، ۱-۱۵.
- صالح نیا، ع. و بختیاری، ح. (۱۳۹۷)، «**اولویت‌بندی تهدیدات امنیت ملی جمهوری اسلامی ایران با روش تحلیل سلسله مراتبی** (AHP)»، فصلنامه مطالعات راهبردی سیاست‌گذاری عمومی، ۲۵۵-۲۷۷.
- علیرضا لرستانی. (۱۳۹۷)، «**مروری بر روش‌های مقابله با بدافزارها و نرم‌افزارهای جاسوسی (موردمطالعه بدافزار استاکس‌نت)**»، فصلنامه مطالعات حفاظت و امنیت انتظامی، (۱۲۵-۱۵۲).
- کلفام، ع. و حسینی، س. (۱۳۹۷)، «**بررسی سایبر تروریسم آمریکا علیه ایران**»، تحقیقات جدید در علوم انسانی، (ص. ۷۷-۹٤).
- گلپرور، م. و خراسانی، پ. (۱۳۹۵)، «**بررسی مقایسه‌ای نقش سیاست دو ستونی آمریکا در سیاست خارجی ایران و عربستان در دوره پهلوی دوم**»، فصلنامه مطالعات سیاسی، (ص. ۱٦۱-۱۸۰).
- محسن آقایی، علی معینی، ابوذر عرب سرخی، ایوب محمدیان و علی‌اصغر زارعی (۱۳۹۸)، «**ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی**»، فصلنامه علمی امنیت ملی، ۲۰۱-۲۳۱.
- محمدی الموتی، م. (۱۳۸٤)، «**جنگ و سیاست در اندیشه کلاوزویتس**»، مرکز تحقیقات کامپیوتری علوم اسلامی، ۷۳-۱۰٤.
- محمدی، م. فرهنگ پور، ش. و موسوی هاشمی، س. (۱۳۹٤)، «**دادرسی جرائم رایانه‌ای**»، همایش ملی قانون آیین دادرسی کیفری سال ۱۳۹۲ در بوته نقد.
- محمودزاده، ۱. نیک‌نفس، ع. و قوچانی، م. (۱۳۹٦)، «**اولویت‌بندی راهبردهای توسعهٔ سامانهٔ فرماندهی و کنترل (C4I) فضای سایبر کشور با رویکرد مطالعهٔ تطبیقی**»، فصلنامه علمی مطالعات بین‌رشته‌ای دانش راهبردی، ۱۹۹-۲۲۸.
- محمود زاده، ا. نیک‌نفس، ع. و قوچانی، م. (۱۳۹٦)، «**اولویت‌بندی راهبردهای توسعهٔ سامانهٔ فرماندهی و کنترل (C4I) فضای سایبر کشور**»، شمارهٔ ۲۷ علمی-پژوهشی (وزارت علوم)، ۲۲۹ - ۲٤۸.
- ناظمی اردکانی، م. نجات پور، م. و احمدی، م. (۱۳۹۵)، «**انقلاب اطلاعات و تأثیر آن بر جنگ نرم**»، فصلنامه پژوهش‌های راهبردی سیاست، دوره: ٤، شمارهٔ: ۱٦، ۱-۲۸.

ب. منابع انگلیسی

- Daniel Gibert .(2016) .Convolutional Neural Networks forMalware Classification .Barcelona: A thesis presented for the degree of Master in Artificial Intelligence.
- DeNardis Laura .(2016) .Global Commission on Internet Governance . Canada Waterloo، Ontario.
- Dhabia M Al-Mohannadi و Patrick Linke .(2016) .On the systematic carbon integration of industrial parks for climate footprint reduction . Journal of cleaner production, 4053-4064.
- eGovernment inAustria .(2013) .Federal Chancellery of the Republic of Austria .Vienna: Federal Chancellery of the Republic of Austria.
- Gaute Wangen .(2015) The Role of Malware in Reported Cyber Espionage: A Review ofthe Impact and Mechanism .Information (Switzerland, 183-211.
- Hisham Shehata Galal ،Yousef Bassyouni Mahdy و Mohammed Ali Atiea . (2016) .Behavior-based features model for malware detection .Springer Nature Switzerland, 59-67.
- James A. Green, (2015), Cyber Warfare: A Multidisciplinary Analysis . Political Science.
- Jannie Zaaiman و Louise Leenan . (2015)The Proceedings of the 10th International Conference on Cyber Warfare and Security .ACPIL.
- Mariano Rajoy Brey .(2013).NATIONALCYBER SECURITY STRATEGY .PRESIDENCY OF THE GOVERNMENT.
- McAfee .(2017) .McAfee Labs Threats Report.
- McAfee Security Group .(2014) .Net Losses: Estimating the Global Cost of Cybercrime .Santa Clara: McAfee، Inc.
- Michael Aschmann ،Louise Leenen و J.C. Jansen van Vuuren .(2017) . Conference: International Conference on Cyber Warfare and Security . Conference: International Conference on Cyber Warfare and Security.
- Monirul Sharif ،Andrea Lanzi ،Jonathon Giffin و Wenke Lee .(2008) . Impeding Malware Analysis Using Conditional Code Obfuscation . Proceedings of the Network and Distributed System Security Symposium . San Diego، California، USA: DBLP.
- Nolen، Scaife ،Henry، Carter ،Patrick، Traynor و Kevin R. B. Butler . (2016) .CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data٣٦ .th International Conference on Distributed Computing Systems (ICDCS).
- Osvaldo Gervasi ،Beniamino Murgante و Sanjay Misra .(2015) . Computational Science and Its Applications .Canada: Springer.
- Radu S. Pirscoveanu ،Steven Hansen ،Thor M. T. Larsen ،Matija Stevanovic ، Jens Myrup Pedersen و Alexandre Czech .(2015) .Analysis of Malware behavior: Type classification using machine learning .2015 International

Conference on Cyber Situational Awareness، Data Analytics and Assessment (CyberSA .(London، UK: IEEE.

- Savita Mohurle و Manisha Patil .(2017) .A brief study of Wannacry Threat: Ransomware Attack 2017 .International Journal of Advanced Research in Computer Science, 1938-1940.
- Steve Grobman .(2018) .Economic Impact of Cybercrime: Why Cyber Espionage isn't Just the Military's Problem .McAfee.
- Symantec Corporation .(2017) Internet Security threat Report .Symantec Security Center.
- Van Nguyen ،Marwan Omar و Mohammed Derek. (2017). A Security Framework for Enhancing User Experience. International Journal of Hyperconnectivity and the Internet of Thing.