فصلنامه علمی امنیت ملی
سال دهم، شماره سی‌وهفتم، پاییز ۱۳۹۹
مقاله پانزدهم از صفحات ۵۱۲-۴۷۳

مقاله پژوهشی: ارائه مدل بومی رصد، پایش و هشداردهی سایبری بر اساس چرخه اودا

مهدی صحرایی[۱]، محمدرضا ولوی[۲]، بهرام بیات[۳]، عبدالرضا ترقی[۴]

تاریخ دریافت:۱۳۹۸/۰۴/۲۳ **تاریخ پذیرش:۱۳۹۸/۱۲/۱۷**

چکیده

بهره‌گیری از فضای سایبر موجب بروز چالش‌های نو در قلمرو امنیت ملی شده است، به‌نحوی‌که اساساً مفاهیم امنیتی در همه ارکان قدرت ملی را متحول نموده است. این موارد امنیتی گاهی در قالب تهدیدات و حملات سایبری با خدشه‌دار نمودن ابعاد امنیت سایبری، لطمات جبران‌ناپذیری به سیستم‌ها و زیرساخت‌های حیاتی وارد نموده است که تأثیر مستقیم بر امنیت ملی کشورها داشته است. نظر به اهمیت جلوگیری از این آسیب‌ها و لطمات، ضرورت دارد تا با تدابیری در خصوص اقدامات پیشگیرانه نسبت به مخاطرات مورد بحث اقدام نمود. به همین منظور و به دلیل خلأ جدی در مورد به‌کارگیری سیستم‌هایی که بتوانند در زمان مناسب اقدامات مربوط به شناسایی و هشداردهی در فضای سایبر را به انجام برسانند، سعی شده مدلی جهت رصد، پایش و هشداردهی سایبری بر اساس مطالعه تطبیقی ساختارهای موجود در کشورهای منتخب، مطابق با سیاست‌ها و ضوابط بومی ارائه گردد. با توجه به موضوع و هدف پژوهش، نوع تحقیق کاربردی- توسعه‌ای است. روش تحقیق به‌کارگیری‌شده روش ترکیبی؛ شامل مطالعات کتابخانه‌ای جهت گردآوری تجربیات موفق کشورهای منتخب و مقایسه آن و سپس مصاحبه باز، از طریق پانل خبرگان در بخش کیفی و سپس توزیع پرسشنامه جهت ارزیابی مؤلفه‌های به‌دست‌آمده مدل ارائه‌شده است. جامعه آماری پژوهش حاضر، تعداد ۲۰ نفر از خبرگان عرصه فناوری اطلاعات و ارتباطات و حوزه امنیتی کشور بوده است. در این مقاله بر اساس جمع‌بندی نتایج مطالعه تطبیقی کشورهای منتخب، یک مدل رصد، پایش و هشداردهی سایبری بر اساس چرخه اودا ارائه گردیده است و مؤلفه‌های مدل مذکور بر اساس نظر خبرگان اولویت‌بندی شده است که بر اساس نظر ایشان، اولویت مراحل چهارگانه به ترتیب شامل مشاهده، تحلیل، اقدام و تصمیم‌گیری می‌باشد و بیشترین اهمیت مؤلفه‌های ابعاد سایبری نیز بر این اساس به ترتیب شامل فرهنگی، دفاعی-امنیتی، دیپلماسی، اجتماعی، اقتصادی، علم و فناوری و سیاسی می‌باشد.

کلیدواژه‌ها: مدل رصد پایش و هشداردهی سایبری، چرخه OODA، مطالعه تطبیقی

۱. دانشجوی دکتری مدیریت امنیت سایبر (نویسنده مسئول) ایمیل:m.sahraei@sndu.ac.ir
۲. دانشیار دانشگاه مالک اشتر
۳. هیئت‌علمی و استادتمام دانشگاه عالی دفاع ملی
۴. داشنجوی دکتری مدیریت امنیت سایبر

۱. مقدمه

با رشد و پیشرفت فناوری سایبری، روز به روز این فضا توسعه یافته و متناسب با آن تهدیدات و آسیب‌های نوینی در همه ابعاد زندگی بشر ازجمله رقابت‌های بین‌المللی و مخاصمات و درگیری‌های سیاسی-امنیتی به وجود آمده است. با افزایش نقش فضای سایبر، در مخاصمات و درگیری‌ها، کشورهای مختلف نیز اقدام به راه‌اندازی واحدها و مراکز مسئول در جهت رصد و پایش فضای سایبری و به دست آوردن توانایی در ارتقاء امنیت و دفاع سایبری کرده‌اند؛ ازجمله این کشورها می‌توان به آمریکا، انگلیس، کره جنوبی، چین و روسیه اشاره کرد.

با توجه به اهمیت فناوری اطلاعات و رشد سریع و در عین حال نامتوازن آن، این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک و در عین حال فرصت‌آفرین مبدل شده است؛ درنتیجه ضرورت توجه و پرداخت سریع و در عین حال نظام‌مند، به‌منظور مصون‌سازی این بستر از تهدیدات موجود در جهت حفظ امنیت ملی و حریم شخصی شهروندان در فضای مخاصمات امروز بین‌المللی را می‌طلبد.

اکنون بدافزارهای پیچیده‌ای تولید شده که یک بدافزار، به چند بدافزار تبدیل می‌شود و این سلاح سایبری به جنگ سایبری می‌انجامد و درنتیجه موجب تخریب سرمایه‌های سایبری، اختلال در امور کشور، تخریب روابط سیاسی و آغاز جنگ فیزیکی هم‌زمان با جنگ سایبری مثل جنگ روس و گرجستان می‌شود که مشکل بزرگ آن هم این است که امکان انتساب در جنگ سایبری وجود ندارد. ارتش روسیه در سال ۲۰۰۷ میلادی، مخفیانه از این تکنولوژی برای فلج کردن اقتصاد «استونی» استفاده کرد و یک سال پس از آن نیز علیه دولت و بانک‌های گرجستان از آن بهره جست (تقی‌پور، ۱۳۹۵).

صیانت، مقاوم‌سازی و امن‌سازی کشور و نظام مقدس جمهوری اسلامی در ابعاد مختلف امنیت ملی در برابر تهدیدات و مخاطرات ناشی از فضای سایبر با توجه به چالش‌های پیش‌رو در این فضا از موضوعات مهمی است که باید مورد توجه قرار گیرد. به‌منظور ارتقاء قدرت تصمیم‌سازی و تصمیم‌گیری در روند شناسایی و آشکارسازی

تهدیدات و مخاطرات فضای سایبر و با هدف افزایش امنیت سایبری و امنیت ملی؛ ضرورت دارد بررسی‌های علمی در مورد گونه‌های مختلف کسب آگاهی از وضعیت تهدیدات و مخاطرات سایبری انجام شود.

بر این اساس ضمن بررسی سازمان‌دهی مدل‌های نظارت و هشداردهی سایبری در کشورهای منتخب، یک مدل رصد و پایش سایبری بومی مبتنی بر سیاست‌ها و راهبردهای ملی ارائه گردیده است. تا ضمن شناسایی و تبیین مسئله، به الزامات مدل یکپارچه، منسجم و هدفمند رصد، پایش و هشداردهی مبتنی بر مطالعه تطبیقی چند کشور منتخب بپردازد و یک مدل بومی ارائه نماید.

۲. بیان مسئله

با توسعه فضای سایبر، مرزهای عرفی ملی و بین‌المللی بسیار کم‌رنگ می‌شود، به‌طوری‌که کنترل دولت‌ها بر بخش‌های حاکمیتی مانند جریان اطلاعات، مدیریت امور سیاسی، اقتصادی، فرهنگی، اجتماعی و امنیتی دگرگون می‌گردد و بخش قابل توجهی از فعالیت‌ها توسط کنشگران در فضای سایبر و با بهره‌گیری از امکانات فناوری‌های اطلاعات و ارتباطات انجام می‌گیرد. در این چارچوب تهدیداتی که در زیست‌بوم فضای سایبر ظهور کرده‌اند، افراد، سازمان‌ها و کشورها را متأثر ساخته است. طبیعی است که در چنین فضایی مفهوم امنیت ملی، چالش‌ها و تهدیدات متحول شده و تغییر ماهیت داده است. به‌علاوه رشد فزاینده استفاده از فضای سایبر و حرکت شتابان دولت به سمت الکترونیکی کردن خدمات اجتماعی و اقتصادی و تأثیر انقلاب اطلاعاتی بر عرصه‌های مختلف مذکور، امنیت ملی جمهوری اسلامی ایران را در سال‌های آتی با تهدیدات و چالش‌های نوینی مواجه خواهد ساخت.

صیانت، مقاوم‌سازی و امن‌سازی کشور در ابعاد مختلف امنیت ملی در برابر تهدیدات و مخاطرات ناشی از فضای سایبر با توجه به چالش‌های پیش‌رو در این فضا از موضوعات مهمی است که باید از هم‌اکنون مورد توجه قرار گیرد و زمینه و بستر لازم بدین منظور فراهم گردد.

رصد تحولات فضای سایبری به‌صورت مقطعی توسط برخی از دستگاه‌ها در کشور صورت می‌پذیرد که به دلیل فقدان مدلی جامع، این امر منتج به بروز موازی‌کاری در برخی از حوزه‌ها گردیده است و برخی از ابعاد فضای سایبری مغفول مانده است که فقدان مدلی جامع جهت رصد و پایش سایبری سبب بروز غافلگیری در ابعاد مختلف فضای سایبری می‌گردد.

بر این اساس، دغدغه اصلی این مقاله فقدان مدل جامع و مدون رصد، پایش و هشداردهی سایبری است که برای حفظ منافع و پایداری امنیت ملی ضروری است. این رصد و پایش و هشداردهی چندبعدی است و علاوه بر زیرساخت‌ها می‌بایست به موضوعاتی همانند محتوا، راهبردها، اقدامات دشمن و فناوری‌های نو و تأثیرات آینده آن‌ها نیز بپردازد تا به‌صورت جامع پاسخگوی نیاز بوده و پیش‌دستی در اقدام، استفاده از فرصت‌ها و ممانعت از غافلگیری را فراهم سازد. در حال حاضر با خلأ جدی مطالعات و کار تحقیقاتی در این زمینه در سطح کشور مواجه هستیم.

۳. اهمیت و ضرورت تحقیق

تحولات سریع و عمیق در ابعاد مختلف اجتماعی، فرهنگی، اقتصادی، سیاسی، فناورانه، امنیتی و نظامی–دفاعی ناشی از توسعه فضای سایبر نیازمند نگاهی جامع، ساختاریافته و منسجم به‌منظور حفاظت و صیانت از منافع ملی و تحکیم و توسعه امنیت ملی در زمینه رصد و پایش شرایط، رویدادها، روندها، تغییرات و تحولات در حال و آینده است تا امکان تصمیم‌گیری، برنامه‌ریزی و مدیریت آن را فراهم سازد. لذا اهمیت و ضرورت وجود مدلی جامع به‌منظور رصد، پایش و هشداردهی سایبری در سطح ملی روشن و به شرح زیر است.

۱–۳. اهمیت تحقیق

اهمیت این مقاله و دستاوردها و مزایای عمده حاصل از اجرای آن را می‌توان به‌صورت خلاصه در موارد زیر دانست:

۱) فراهم نمودن مبانی نظری و شناخت نسبت به تحولات و تغییرات عمده پیش‌رو در حوزه سایبر با تأثیرگذاری سطح امنیت ملی
۲) تبیین مدل جامع و فراگیر به‌منظور رصد، پایش و هشداردهی با هدف جلوگیری از غافلگیری در عرصه سایبر.
۳) بهبود نسبی سطح امنیت ملی از طریق ایجاد اشراف بر ابعاد مختلف و تهدیدات متنوع حوزه‌های مختلف فضای سایبر و واکنش مناسب و به‌موقع به آن‌ها.
۴) ایجاد شرایط مدیریتی، تصمیم‌سازی و تصمیم‌گیری مناسب و مبتنی بر اطلاعات کافی و درنتیجه ثبات در عمل در حوزه سایبر کشور.

۲-۳. ضرورت تحقیق

ضرورت انجام این تحقیق و معایب و نواقص موجود در کشور که در صورت انجام نشدن این پژوهش مغفول مانده و همچنان آسیب‌زا خواهند بود عبارت‌اند از:

۱) کمبود پیش‌آگاهی و آمادگی در زمینه مقابله با تهدیدات حوزه سایبر.
۲) احتمال خدشه به امنیت ملی ناشی از غافلگیری در فضای سایبر.
۳) فقدان هم‌گرایی و هم‌افزایی بین ذینفعان همسو و تشتت مدیریتی و درنتیجه هدررفت شدید منابع ناشی از آن.
۴) فرصت‌سازی و فراهم کردن امکان پیش‌دستی برای حریف

موارد مذکور گویای این اهمیت و ضرورت است که باید یک مدل جامع و فراگیر رصد، پایش و هشداردهی سایبری با رویکرد امنیت ملی و مناسب کشور جمهوری اسلامی ایران، در تمامی عرصه‌های فضای سایبر، اعم از سیاسی، نظامی، اقتصادی، فرهنگی، فناوری و ... طراحی شود.

٤. اهداف تحقیق

هدف اصلی: تبیین مدل جامع رصد، پایش و هشداردهی سایبری مبتنی بر مطالعه تطبیقی مدل‌های پنج کشور هدف.

اهداف فرعی

۱. آسیب‌شناسی و تحلیل وضعیت رصد، پایش و هشداردهی فضای سایبر و تعیین ویژگی‌های مدل مطلوب.
۲. ارائه ابعاد، مؤلفه‌ها و شاخص‌های مدل رصد، پایش و هشداردهی سایبری.
۳. تعیین ارتباط بین ابعاد، مؤلفه‌ها و شاخص‌های مدل مورد نظر

۵. سؤالات تحقیق

سؤال اصلی: مدل رصد، پایش و هشداردهی مبتنی بر مطالعه تطبیقی کشورهای هدف در جمهوری اسلامی ایران کدام است؟

سؤالات فرعی

۱. آسیب‌های وضعیت موجود در خصوص سیستم‌های رصد، پایش و هشداردهی موجود به چه میزان است؟
۲. ابعاد، مؤلفه‌ها و شاخص‌های مدل رصد، پایش و هشداردهی سایبری کدامند؟
۳. ارتباط بین ابعاد، مؤلفه‌ها و شاخص‌های استخراج‌شده چگونه است؟

٦. مبانی نظری تحقیق

۱-۶. اصطلاحات و متغیرها

فضای سایبر: مجموعه‌ای است از سامانه‌های الکترونیکی و شبکه‌های رایانه‌ای، شامل نیروی انسانی، زیرساخت‌ها، تجهیزات سخت‌افزاری و نرم‌افزاری، سامانه‌های ارتباطی و کنترلی و مدیریتی، به‌منظور تولید، ذخیره‌سازی، پردازش، تبادل، بازیابی، حذف و بهره‌برداری از داده‌ها (United States Department of Defense, 2015). در این پژوهش با اغماض، فضای سایبر و فضای مجازی معادل یکدیگر تلقی شده است و این دو مفهوم به یک معنا به کار گرفته شده‌اند.

رصد (دیده‌بانی): به‌مثابه راداری است که رویدادهای جدید، غیرمنتظره و بزرگ و کوچک محیطی و داخلی اثرگذار را به‌گونه‌ای نظام‌مند و وظیفه‌گرا نشان می‌دهد. اگویلار، رصد یا دیده‌بانی را گردآوری نظام‌یافته اطلاعات محیطی می‌داند که به‌منظور کاهش تصادفی اطلاعات ورودی و فراهم ساختن سامانه هشدار اولیه در محیط سرشار از تغییر و ناپایداری برای مدیران طراحی می‌شود (Aguilar, 1967: 34).

پایش: به معنی نظارت است و منظور از آن هشیاری از وضعیت یک سامانه یا پدیده از راه مشاهده دگرگونی‌هایی است که ممکن است با گذر زمان در آن سامانه یا پدیده رخ دهد. امروزه پایش در بسیاری از زمینه‌ها کاربرد دارد، به‌ویژه در شبکه‌های همگانی، صنعتی و جغرافیایی(Glossary of Environment Statistics,1997) .

هشداردهی: عبارت است از «آگاه‌سازی نسبت به رخدادهایی که منافع فرد، سازمان یا نظام ملی و بین‌المللی را در سطوح مختلف به مخاطره اندازد». در خاص کردن این مفهوم به هشدار اطلاعاتی می‌توان گفت: «آگاه‌سازی نسبت به رخدادهایی که امنیت ملی را در سطوح مختلف به مخاطره کشاند». همچنین در علوم نظامی هشدار عبارت است از: «نشانه تصویری یا شنیداری یا حسی که بر خطری قریب‌الوقوع دلالت دارد» (فکوری، ۱۳۹۳).

۲-۶. مطالعه تطبیقی

محورهای مورد مطالعه در این بخش شامل مؤلفه‌های مطلوبیت‌های راهبردی (مبانی، چشم‌انداز، مأموریت و...)، راهبردها و اجزاء معماری است. با توجه به اینکه نیازمندی‌های مطالعه تطبیقی در حوزه امنیت و رصد فضای سایبر و در سطوح راهبردی، عملیاتی و تاکتیکی تعیین گردیده است لذا باید کشورهایی برای مطالعه انتخاب گردند که اول اینکه، در سطح راهبردی رصد و پایش سایبری فعالیت نموده ودوم اینکه، اسناد مرتبط را منتشر نموده و در دسترس قرار داده باشند. از آنجایی که کشورهای محدودی در جهان موفق به برنامه‌ریزی درخور و سازمان‌دهی مناسب گردیده‌اند، این امر محدودیت بسیاری را در دامنه انتخاب کشورها باعث شده است. در انتخاب کشورها، علاوه بر پیشرفته بودن آن‌ها در موضوع مورد

مطالعه، تلاش گردید که حتی‌المقدور کشورهای هدف، از میان کشورهایی که منطقاً از سازگاری بیشتری با ما برخوردار هستند شناسایی گردند. همچنین به انتخاب حداقل یک کشور قدرتمند در حوزه سایبری نیز به‌طور ویژه توجه گردید. با توجه به اینکه هم‌زمان با رشد و توسعه فضای سایبر، انواع تهدیدات سایبر ظهور و بروز یافته و به یک مخاطره ملی مبدل گردیده‌اند، لذا این کشورها قبل از سایر کشورهای کمترتوسعه‌یافته، در معرض تهدیدات مختلف بوده و در مقام مقابله مؤثر به فکر ایجاد سیستم رصد و پایش نظام‌یافته بوده‌اند. کشورهای مورد بحث در این بخش شامل آمریکا، کره جنوبی، انگلیس می‌شوند. پنج مؤلفه ارزیابی کشورهای منتخب اقدامات قانونی، اقدامات فنی، اقدامات سازمانی، ارتقاء ظرفیت، تعاملات و همکاری، سیاست‌ها و راهبردها بوده است (Global Cyber Security Index, 2018).

– آمریکا: (پیشروترین کشور جهان در امنیت و دفاع سایبر است که دارای اسناد راهبردی امنیت و دفاع سایبری است).

–کره جنوبی: (به‌عنوان یک کشور نسبتاً مستقل پیشرو در حوزه فناوری‌های نوین و سایبر است).

– انگلیس: (کشوری پیشرو در امنیت و دفاع سایبر که دارای اسناد راهبردی امنیت و دفاع سایبری است).

رویکرد اصلی مطالعه تطبیقی، بررسی و شناخت در حوزه معماری سامانه رصد، پایش و هشداردهی سایبری در کشورهای منتخب است که دارای ویژگی‌های زیر است:

ـ در سطح راهبردی دارای سازمان و مستندات قابل اعتبار در دسترس باشند.

ـ در حوزه‌های سایبری پیشرو و دارای سابقه باشند.

ـ تجارب آن کشورها متناسب با شرایط توسعه ج.ا.ا قابل بهره‌برداری باشد.

با توجه به ویژگی‌های فوق، کشور آمریکا، کره جنوبی و انگلستان انتخاب و مورد مطالعه قرار گرفت. این کشورها اقدام مناسبی در سازمان‌دهی حوزه رصد و پایش انجام داده و مستندات مناسبی را ارائه نموده‌اند. متأسفانه مستندات مناسب در کشورهای چین و روسیه مشاهده نگردید.

۶-۳. آمریکا

کشور آمریکا از سال‌ها پیش با توجه به ویژگی‌های فضای سایبری و تهدیدات آن، اقدام به تشکیل واحدهای مختلفی برای دفاع در برابر تهدیدات و آسیب‌های سایبری نموده است. طی تحقیقات به‌عمل‌آمده، در کشور آمریکا مسئولیت دفاع سایبری در بخش نظامی بر عهده سازمان فرماندهی سایبری ایالات‌متحده[1] می‌باشد. مأموریت این سازمان برقراری امنیت فضای سایبر برای ارتش آمریکا، وزارت دفاع و همچنین برقراری امنیت ایالات‌متحده و هم‌پیمانانش در فضای سایبر می‌باشد (U. S. Cyber Command Fact Sheet, ۲۰۱۴) (سند فرماندهی سایبری ایالات‌متحده، ۲۰۱۴).

علاوه بر این سازمان، دو سازمان از جامعه اطلاعاتی آمریکا، آژانس امنیت ملی[2] و پلیس فدرال[3] و یک اداره از وزارت امنیت داخلی[4] نیز، در زمینه دفاع و امنیت فضای سایبر مسئولیت دارند (حسینی، ظریفی‌منش، ۱۳۹۲:۱۲).

۶-۳-۱. بخش‌های فعال در حوزه امنیت و دفاع سایبر در آمریکا

ایالات‌متحده آمریکا وظایف مرتبط با دفاع و امنیت سایبری را در وزارت دفاع، مرکز امنیت سایبری ملی از وزارت امنیت داخلی[5] و وزارت دادگستری تقسیم کرده است. در بخش وزارت دفاع، فرماندهی سایبری نیروهای مسلح وظیفه 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 حمله سایبری به کشورهای مورد نظر را داشته باشد. به‌علاوه، آژانس امنیت ملی نیز در وزارت

---

1. United State Cyber Command

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

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

4. DHS-Department of Homeland Security
5. National Cyber Security Center of DHS

دفاع آمریکا وظیفه شنود سیگنال و حفاظت سیگنال را بر عهده دارد که شامل برقراری امنیت شبکه‌های رایانه‌ای نیز می‌باشد. این سازمان وظیفه تحقیق و توسعه در زمینه امنیت و رمزگذاری و همچنین ابلاغ استانداردهای امنیتی، نظارت و بررسی سطح امنیتی تمامی سازمان‌های فدرال را بر عهده دارد. تمامی سازمان‌های فعال در زمینه دفاع سایبری ارتباط نزدیکی با آژانس امنیت ملی دارند. وزارت امنیت داخلی مسئولیت 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[1] 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.

۲-۳-۶. امنیت سایبر ملی

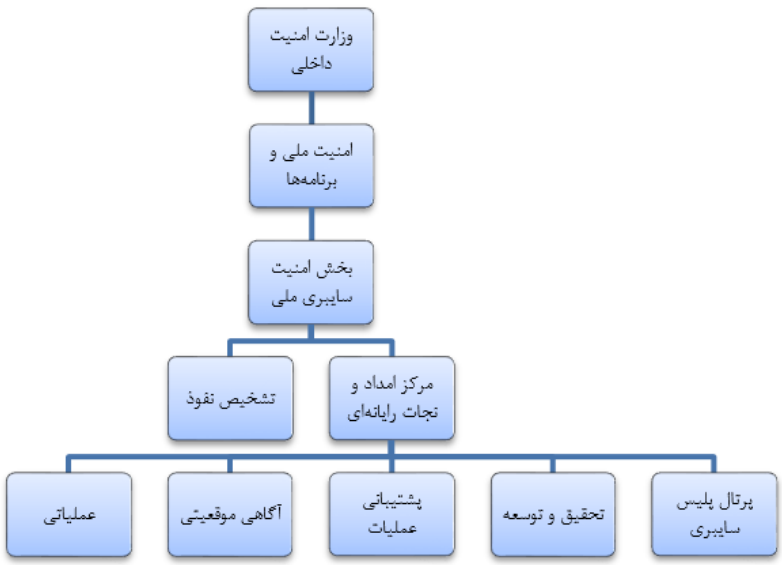
مأموریت بخش امنیت سایبری ملی، همکاری مستمر با نهادهای دولتی، خصوصی و بین‌المللی جهت برقراری امنیت فضای سایبری آمریکا می‌باشد. (U.S. DEPARTMENT OF HOMELAND SECURITY, 2018)

مأموریت بخش امنیت سایبری ملی، ایجاد و نگهداری بستری مؤثر جهت پاسخگویی به نیازهای امنیتی فضای سایبر و پیاده‌سازی سیستم مدیریت ریسک فضای سایبری جهت محافظت از زیرساخت‌های سایبری کشور است. بخش امنیت سایبری ملی زیرمجموعه اداره برنامه‌ها و محافظت ملی از وزارت امنیت داخلی آمریکا می‌باشد. این بخش باید امنیت ساختارهای سایبری کشور آمریکا را به‌صورت مداوم برقرار کند. به این منظور زیربخش‌های مختلفی ایجاد شده است. زیرشاخه‌های مربوط به این سازمان و فعالیت‌های آن‌ها به شرح زیر است (شکل ۱):

مرکز امداد و نجات رایانه‌ای (تیم پاسخگویی به حوادث امنیتی و رایانه‌ای)[2]

1 .CERT-Computer Emergency Response Team
2.Computer Emergency Response Team

تشخیص نفوذ: پیاده‌سازی و به‌کارگیری روش‌های تشخیص نفوذ و راه‌اندازی و به‌کارگیری آن در سایر سازمان‌های فدرال، محلی و خصوصی بر عهده این بخش است.



شکل ۱. نمودار سازمانی بخش امنیت سایبری ملی در وزارت امنیت داخلی

همچنین وزارت امنیت داخلی آمریکا غیر از وظیفه حفاظت از زیرساخت‌ها این قدرت را دارد تا هدایت و هماهنگی تمامی عملیات‌های پیشگیری از آسیب، حفاظت، ترمیم کامپیوترها و زیرساخت‌های ارتباطی را بر عهده گیرد. همچنین سیستم محافظت از نفوذ سازمان به نام انیشتین[1] در حال پیاده‌سازی است تا به این وظایف کمک کند.

۳-۳-۶. سیستم تشخیص نفوذ

تمام سازمان‌های دولتی غیرنظامی موظف به استفاده از سیستم تشخیص نفوذ انیشتین ۲ هستند. این سیستم فقط ترافیک شبکه و اینترنت که یک طرف آن، شبکه‌های غیرنظامی دولتی می‌باشد را بررسی می‌کند. همان‌طور که در توافقنامه این سیستم ذکر شده، ترافیک به

1. EINSTEIN

مقاصد و از مبدأهای تجاری یا خصوصی بررسی نمی‌شود. این امر مستلزم این است که سازمان مربوطه با ISP[1] خود همکاری کند تا فقط اتصالات به شبکه‌های دولتی از انیشتین عبور کند.

برای رسیدن به اهداف این مأموریت، وزارت امنیت داخلی آمریکا باید از فناوری‌های نوظهور و جدید کمک بگیرد. این سازمان از انیشتین با رویکرد سیستم سیستم‌ها[2] پیاده شده است که نیروی انسانی و فناوری‌های مورد نیاز برای پاسخگویی به تهدیدات را در برمی‌گیرد. اولین نسخه از این سیستم در سال ۲۰۰۳ توسعه یافته که تنها یک سیستم مانیتور جریان ترافیک شبکه است که از طریق تغییر روند ترافیک شبکه، فعالیت مخرب را تشخیص می‌دهد. در سال ۲۰۰۸، قابلیت‌های تشخیص نفوذ به این سیستم اضافه شد و تحت عنوان انیشتین ۲ ارائه شد.

۴-۳-۶. مروری بر برنامه اینشتین

سیستم اینشتین برای حفاظت از سیستم‌ها و شبکه‌های مؤسسات اجرایی عمومی فدرال مورد استفاده قرار می‌گیرد.

اینشتین اطلاعات خلاصه ترافیک شبکه را از درگاه‌های مؤسسات دولتی دریافت کرده و دید سطح بالایی از اتصالات شبکه دولت فدرال را فراهم می‌کند.

تحلیلگران شبکه اینشتین شامل اجزای زیر می‌باشد:

- خروجی‌های سنسورهای شبکه را بررسی می‌کنند.
- رکوردهای جریان شبکه را ذخیره می‌کنند.
- داده‌های تحلیلی به US-CERT ارسال می‌شوند تا هشدارها صادر شود
- تحلیلگران US-CERT از داده‌های اینشتین برای ایجاد همبستگی بین رخدادهای شبکه‌های سازمانی مختلف استفاده می‌کنند.

1. Internet Service Provider
2. System Of Systems Approach

- داده‌های مؤسسات دولتی از طریق یک پورتال امن برای بهبود قابلیت CSIRT[1] در اختیار US-CERT قرار می‌گیرند.

که نتایج این تحلیل شامل موارد زیر می‌شود:

- ایجاد پروفایلی از رفتار شبکه
- مدل‌سازی رفتار
- شناسایی ناهنجاری‌های ناشی از تهدیدات خارجی و نقض سیاست‌ها
- ارائه راهکارهای اصلاحی با استفاده از تحلیل‌های کوتاه‌مدت و بلندمدت

اینشتین برای دفاع از مرزهای شبکه سازمان‌های اجرایی فدرال ایجاد شده است.

برای امنیت بیشتر، از تکنیک دفاع در عمق[2] (استفاده از چندین ابزار در ترکیب با یکدیگر) استفاده می‌شود.

۵-۳-۶. مراحل برنامه اینشتین

- اینشتین ۱ (E1): جمع‌آوری جریان اطلاعات
  - قابلیت تحلیل اولیه و به‌اشتراک‌گذاری اطلاعات
  - ثبت و تحلیل رکوردهای جریان داده
- اینشتین ۲ (E2): تشخیص مزاحمت
  - استفاده از سنسورهای مناسب برای شناسایی فعالیت‌های بدخواهانه
  - تحلیل و نظارت بر ترافیک عبوری از زیرساخت
- اینشتین ۳ (E3): پیشگیری از مزاحمت
  - بهبود حفاظت شبکه برای جلوگیری از بروز فعالیت‌های بدخواهانه
  - زیرساختی برای تجمیع ترافیک سازمان‌های اجرایی فدرال
  - افزودن حفاظت‌های امنیتی به مکان‌های محدود شبکه

1. Computer security incident response Team
2. Defense-in-depth

NCPS[1]: سیستم حفاظت امنیت سایبری ملی

در سال ۲۰۰۸ برای حفاظت از شبکه دولتی سازمان‌های غیرنظامی و پیشگیری از تهدیدات سایبری ایجاد شده است که وظیفه پیشگیری، تشخیص، پاسخ‌دهی و مقابله مناسب با تهدیدات سایبری مشکوک یا شناخته‌شده در ترافیک شبکه فدرال را بر عهده دارد. شبکه تحت پوشش آن ترافیک اینترنت ورودی یا خروجی سازمان‌ها و مؤسسات دولتی غیرنظامی (در اصطلاح کل ترافیک.gov) می‌باشد.

جدول ۱- چارچوب امنیت سایبری آمریکا

(National Institute of Standards and Technology: ۲۰۱۴)

دسته	عملکرد	مرحله
مدیریت دارایی‌ها	شناسایی	مرحله اول
محیط کسب‌وکار		
حکومت		
ارزیابی ریسک		
استراتژی مدیریت ریسک		
کنترل دسترسی	محافظت	مرحله دوم
آموزش و آگاهی		
امنیت داده		
فرایندهای حفاظت از اطلاعات		
نگهداری		
فناوری‌های حفاظتی		
ناهنجاری‌ها و رویدادها	کشف	مرحله سوم
نظارت مستمر امنیت		
فرایندهای تشخیص		
برنامه‌ریزی پاسخ	پاسخ	مرحله چهارم
ارتباطات		
تجزیه‌وتحلیل		
کاهش		
بهبود		
برنامه‌ریزی بازیابی	بازیابی	مرحله پنجم
ارتقا		
ارتباطات		

1. National Cyber security Protection System

۶-۳-۶. معرفی یکی از چارچوب‌های رصد و پایش سایبری در آمریکا

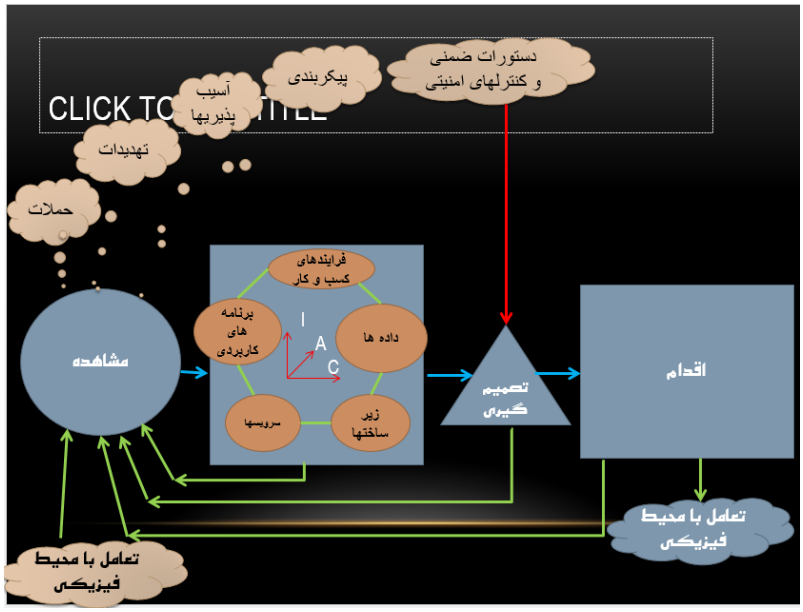
در این بخش یکی از ساختارهای پایش و هشداردهی سایبری مبتنی بر مدل اودا[۱] مربوط به وزارت امنیت داخلی آمریکا معرفی می‌گردد.

- سیستم هشداردهی شامل سه مرحله است:
  - **مشاهده:** جمع‌آوری از عناصر در زمان و فضا
    - در این مرحله چالش جمع‌آوری داده‌ها با فرمت‌های گوناگون است؛ ازاین‌رو اطلاعات سنسورها باید نرمال، تمیز و ترجمه شود.
  - **جهت‌دهی و طبقه‌بندی موضوعی و یکنواخت‌سازی:** سنتز عناصر بی‌ربط که نیاز است در این مرحله درک شود.
    - یافتن وابستگی میان داده‌ها و به نظم درآوردن آن‌ها
  - **طرح‌ریزی:** تحلیل مبتنی بر نگاه به آینده و پیش‌بینی نتایج این عناصر در وضعیت فعلی تصمیم‌گیری نماید.
    - تحلیل و هشداردهی سایبری بر اساس الگوریتم‌های از پیش تعریف‌شده مبتنی بر رفتارشناسی
- حلقه OODA یک مدل کلاسیک جهت مدل پشتیبان تصمیم‌گیری (DSS[۲]) می‌باشد.
- هدف از این چرخه دستیابی به امکان مشاهده سریع و واکنش به وقایع سایبری سریع‌تر از حریف می‌باشد (مبتنی بر مدل سایبر اودا (سورنسن، ۲۰۱۰): چارچوب مفهومی فضای مجازی).
- نکته حائز اهمیت در مورد این ساختار حلقه بودن ساختار اودا به معنای فعالیت مستمر در حوزه زمان می‌باشد (ولوی، ۱۳۹۵).

---

۱. Observation Orientation Decision, Action؛ این مدل مربوط به نیروی هوایی آمریکاست که اولین بار در سال ۲۰۱۰ برای استفاده در فضای سایبری طرح گردید.

2.Decision Support System



شکل ۲- ساختار Cyber OODA (Lenders، ۲۰۱۵)

شرح وظایف هرکدام از مراحل مذکور در شکل ۳ به شرح زیر می‌باشد:

مشاهده:

- پیکربندی
- فعالیت کاربران
- دستورات و کنترل‌های امنیتی ضمنی
- نرم‌افزار و خدمات آسیب‌پذیری
- تهدیدات فعلی
- حملات مداوم
- تعامل آشکار با محیط فیزیکی
- اطلاعات جمع‌آوری‌شده توسط سنسورها به لحاظ معنایی و حجم داده‌های بزرگ می‌توانند دسته‌بندی و نمایش داده شوند. پالایش، دسته‌بندی و همسان‌سازی این داده‌ها جهت به‌کارگیری در مرحله بعد بسیار مهم می‌باشند.

جهت‌دهی (همسوسازی)

- در این مرحله هدف همسوسازی اطلاعات جمع‌آوری‌شده توسط سنسورها با هدف دستیابی به سه ویژگی محرمانگی، دسترس‌پذیری و جامعیت می‌باشد.

تصمیم‌گیری

- فرایند شناسایی و انتخاب یک راه‌حل برای یک مشکل خاص
- در حلقه اودا تصمیم‌گیری عموماً منطبق بر مشاهدات وضعیت جاری و نیز نحوه دسته‌بندی مشکلات صورت می‌گیرد و الگوهای استخراج‌شده به‌صورت دانش در این مرحله به کار می‌روند که این الگوها به‌مرور، پایگاه دانش را تکمیل می‌نمایند، به عبارت ساده‌تر پایگاه دانش مبتنی بر الگوهای استخراجی پرتکرار در گذشته جهت تحلیل‌های آتی شکل می‌گیرد.
- عموماً فرایند تصمیم‌گیری به جهت یافتن یک نقطه میانی با رویکرد اولویت‌بندی اهداف محرمانگی، یکپارچگی و دسترس‌پذیری پیچیده می‌باشد.

اقدام

اقدام به دو صورت ممکن است رخ دهد:

- گزارش‌دهی یا اطلاع‌رسانی
- واکنش در راستای حل مشکل و یا اقدام متقابل

۴-۶. کره جنوبی

آژانس امنیت اینترنت کره جنوبی (**KISA**[1])، زیرمجموعه‌ای از وزارت علوم، اطلاعات و ارتباطات و برنامه‌ریزی است که با مدیریت و تخصیص منابع اینترنتی سروکار دارد. این

1. KISA; Korean Internet Security Agency

سازمان همچنین وظیفه ایجاد امنیت در فضای سایبری کره جنوبی را عهده‌دار است. ازجمله این موارد می‌توان به تشخیص و جلوگیری از بدافزارها و ویروس‌ها در سطح وب اشاره کرد. علاوه بر این آموزش درباره اینترنت و امنیت سایبری و انواع دیگر مشکلات این حوزه از وظایف این سازمان است. شایان ذکر است در جولای سال ۲۰۰۹ دو سازمان به نام‌های آژانس توسعه ملی اینترنت کره جنوبی[1] و آژانس همکاری بین‌المللی فناوری اطلاعات کره جنوبی[2] با این سازمان تلفیق شدند.[3]

این آژانس به‌واسطه نیاز موجود در رابطه با مدیریت قوانین و سیاست‌گذاری‌ها جهت محافظت از توسعه امن اطلاعات بنا نهاده شد. آژانس امنیت اینترنت کره جنوبی، همچنین مسئول مقابله با نفوذ و خرابکاری‌های اینترنتی است. آنالیز نقاط ضعف و ارزیابی امنیت تأسیسات کلیدی مرتبط با فناوری اطلاعات، جلوگیری از بدافزارها و ارتقاء امنیت، امضای دیجیتال و محافظت از اطلاعات مهم صنعتی از دیگر اقدامات این سازمان است (ADNDRC).[4]

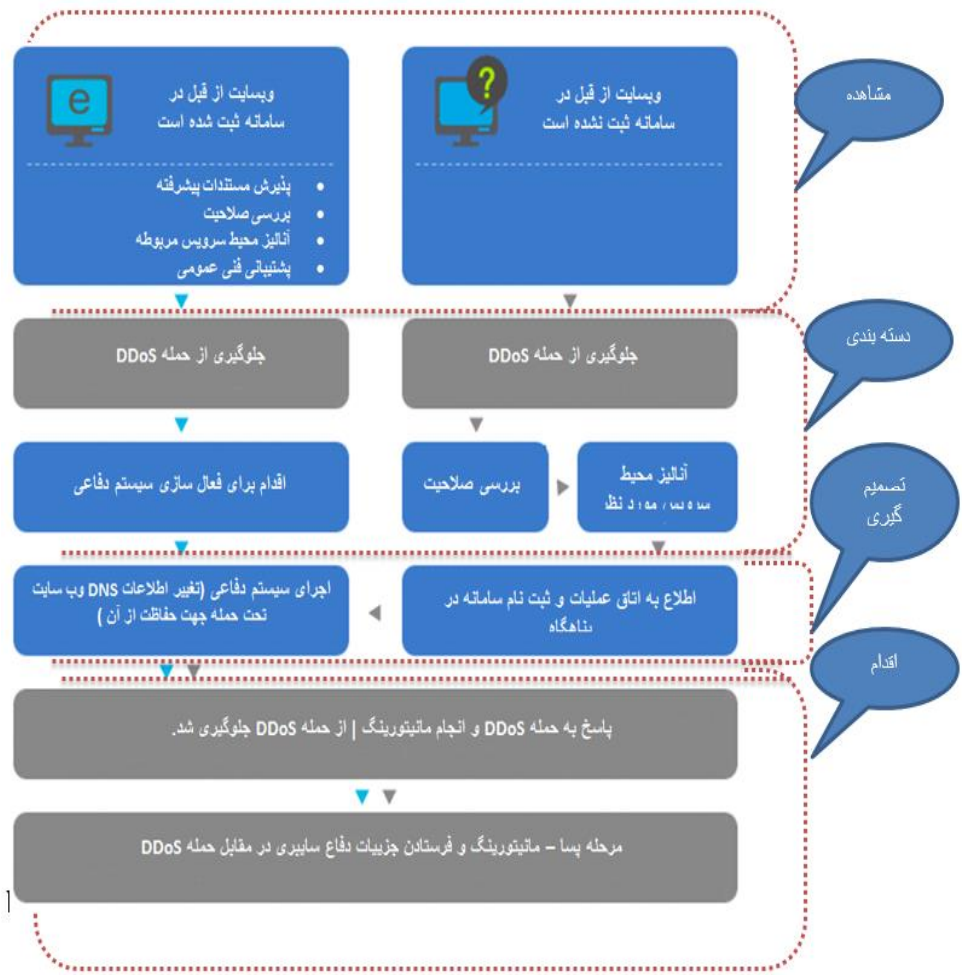
۱-۴-۶. مسئولیت‌ها

به‌عنوان بانی امور اینترنت در کره، این آژانس مسئولیت‌های ذیل را عهده‌دار است:

۱. تهیه قوانین مربوط به اینترنت.
۲. ایجاد و توسعه محیط جوامع اینترنتی.
۳. تبیین و تبلیغ استفاده از اینترنت در کشور.
۴. محافظت از ساختار اینترنت ملی در مقابل ترور مجازی، بدافزارها و دیگر فعالیت‌های مشکوک.
۵. هدایت طرح تیم واکنش سریع کامپیوتری[5] به‌منظور ارتقاء امنیت اینترنت در کره.

1. NIDA
2. KIICA
3. (Asia Pacific Internet Research Aliance, 2008)
4.Asian Domain Name Dispute Resolution Centre
5. krCERT CC

۶. پشتیبانی از سازمان‌های بین‌المللی، مانند انجمن بین‌المللی ارتباطات[1] و همچنین یاری‌رسانی به شرکت‌های کره‌ای در حوزه امنیت سایبری.

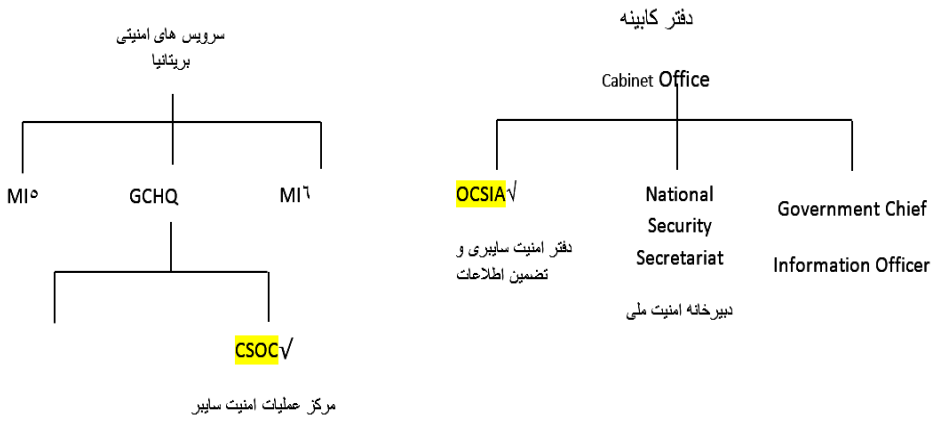


شکل ۳ – سامانه واکنش به حملات کره جنوبی ((KISA,2015

1. International Communication Union

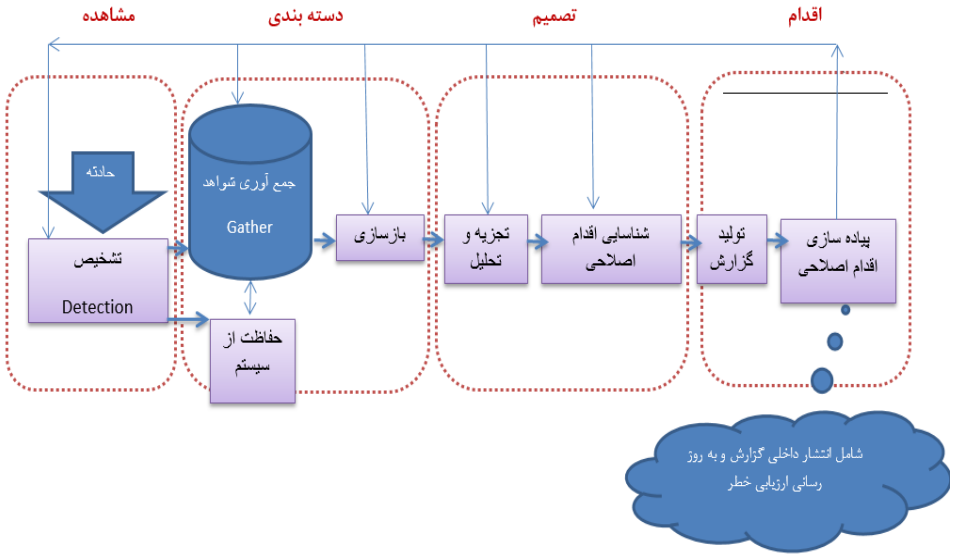
۵-۶. انگلیس

برابر بررسی‌های به‌عمل‌آمده در انگلستان، دو نهاد اصلی جدید برای مدیریت امور سایبری در سال ۲۰۱۰ ایجاد شده است: دفتر امنیت سایبر (OCS) و مرکز عملیات امنیت سایبری (CSOC). دفتر امنیت سایبری در دفتر کابینه مستقر بوده و متولی امنیت سایبری راهبردی بریتانیا است و رهبری استراتژیک امنیت سایبری در کل دولت و سراسر ادارات آن را به عهده دارد و مرکز عملیات امنیت سایبری در GCHQ که یکی از سازمان‌های امنیتی است مستقر بوده و پایش و هماهنگی[1] پاسخ به حادثه را فراهم می‌کند[2]. وظایف اصلی این مرکز نظارت بر تحولات در فضای سایبر، (درنهایت سطح آگاهی وضعیتی[3] جمعی را فراهم می‌آورد)، تجزیه‌وتحلیل روندها و بهبود هماهنگی پاسخ‌های فنی به حوادث سایبری می‌باشد (حسینی، ظریفی‌منش، ۱۳۹۲:۱۲).



در شکل زیر به یکی از سامانه‌های پایش سایبری انگلیس که به‌منظور پیشگیری و هشداردهی سایبری مورد استفاده قرار می‌گیرد، ارائه شده است. معماری سامانه گزارش حادثه داخلی (Chris W. Johnson, 2015) به‌صورت زیر می‌باشد:

1. Monitoring and Coordinating
2. Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space published by TSO
3. Situational awareness



شکل ۴- معماری سامانه گزارش حادثه سایبری انگلیس

۶-۶. خلاصه مطالعه تطبیقی

در اسناد راهبردی امنیت سایبری بر روی چند محور اساسی؛ نظیر تغییر ساختارهای کلان سازمانی و افزودن مجموعه‌های امنیت سایبر در عالی‌ترین سطوح ستادی نظیر شورای ملی امنیت سایبری، مرکز تحقیقاتی دفاع سایبر، متمرکزسازی فعالیت‌های امنیت سایبر کشورها در قالب واحد ستادی و در مواردی اجرایی، تقویت محافظت از زیرساخت اطلاعات حیاتی، ایمن سازی و تقویت سیستم‌های IT، بهبود اجرای قوانین، افزایش تعاملات بین المللی، اطمینان حاصل نمودن از فناوری اطلاعات قابل اعتماد و آموزش نیروی سایبری و به ویژه مرکز ملی مقابله سایبری تمرکز دارند (ولوی، ۱۳۹۵).

جدول ۲- مقایسه ساختارهای کشورهای منتخب

کشورهای منتخب	ساختار منسجم رصد، پایش و هشداردهی سایبری	ساختار متمرکز/ توزیع‌شده	متولی امنیت سایبری	سطح راهبردی	سطح تاکتیکی	سطح عملیاتی
آمریکا	دارد	توزیع‌شده	**DHS/DOD**	✓	✓	✓
کره جنوبی	دارد	متمرکز	**KISA**	✓	✓	✓
انگلیس	دارد	متمرکز	**OCS/CSOC**	✓	✓	✓

ازجمله موارد مهم در اسناد راهبردی مورد مطالعه عبارت‌اند از:

- بازنگری در راهبرد امنیت ملی کشورها و گنجاندن بحث امنیت سایبر در آن‌ها
- ایجاد شورای ملی امنیت سایبر و (یا) مرکز ملی مقابله سایبری
- استفاده از دو بازوی عمده عملیاتی و اجرایی Cert[1], CSOC[2] تیم پاسخگویی به حوادث امنیتی و رایانه‌ای جهت مقابله با تهدیدات سایبری
- متمرکزسازی موارد مهم مرتبط با امنیت سایبر؛ نظیر محافظت از زیرساخت حیاتی، رمزشناسی، امنیت فناوری اطلاعات
- تقویت ساختارها و تعاملات سازمان‌ها با یکدیگر

سامانه‌های پایه و اساسی پدافند سایبری بر اساس جمع‌بندی مطالعات تطبیقی به‌صورت جدول ۲ می‌باشد.

1. Computer Emergency Response Team
2. Cyber Security Operation Center

جدول ۳- سامانه‌های پایه و اساسی پدافند سایبری

واژه انگلیسی	معادل فارسی	تعریف
SOC[1]	**مرکز عملیات امنیت**	سیستم مدیریت امنیت شبکه، دارای مکانیزم‌های بررسی تجهیزات شبکه به‌صورت خودکار در جهت جلوگیری از نفوذ هکرها و تهدید حملات از طریق منابع داخلی و منابع خارجی
CSIRT[2]	**گروه‌های واکنش هماهنگ رخداد (گوهر)**	گروهی که وظیفه پاسخگویی به کلیه رخدادهای صورت‌گرفته در فضای تولید و تبادل اطلاعات در حوزه فعالیت خود را بر عهده دارد.
تیم پاسخگویی به حوادث امنیتی و رایانه‌ای[3]	**مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر)**	مرکزی که وظیفه اقدام متقابل با رخدادهای فضای تبادل اطلاعات را بر عهده دارد.
ISAC[4]	**مرکز تحلیل و به‌اشتراک‌گذاری اطلاعات**	سازمانی است که منابع اصلی و مرکزی برای جمع‌آوری اطلاعات مرتبط با تهدیدات سایبری زیرساخت‌های حیاتی را فراهم می‌کند و امکان به‌اشتراک‌گذاری دوطرفه اطلاعات بین بخش‌های عمومی و خصوصی را ایجاد می‌کند.
ISAS[5]	**سیستم هشدار امنیت اطلاعات**	آسیب‌پذیری‌ها، تهدیدات و مسائل امنیتی موجود در سیستم را در هر زمان نشان می‌دهد.

آنچه در این بخش استنباط می‌شود، این است که آمریکا به‌عنوان یک نمونه جامع در حوزه پایش فضای سایبری که موفق به پیاده‌سازی مدل رصد، پایش و هشداردهی سایبری به‌صورت توزیع‌شده گردیده است، الگوی بسیاری از کشورها نیز قرار گرفته است. مدل چرخه مشاهده، جهت‌دهی، تصمیم‌گیری و اقدام در الگوی کشورهای کره جنوبی و انگلیس نیز به وضوح دیده می‌شود و بر اساس مطالعه تطبیقی، تنها در اجزا

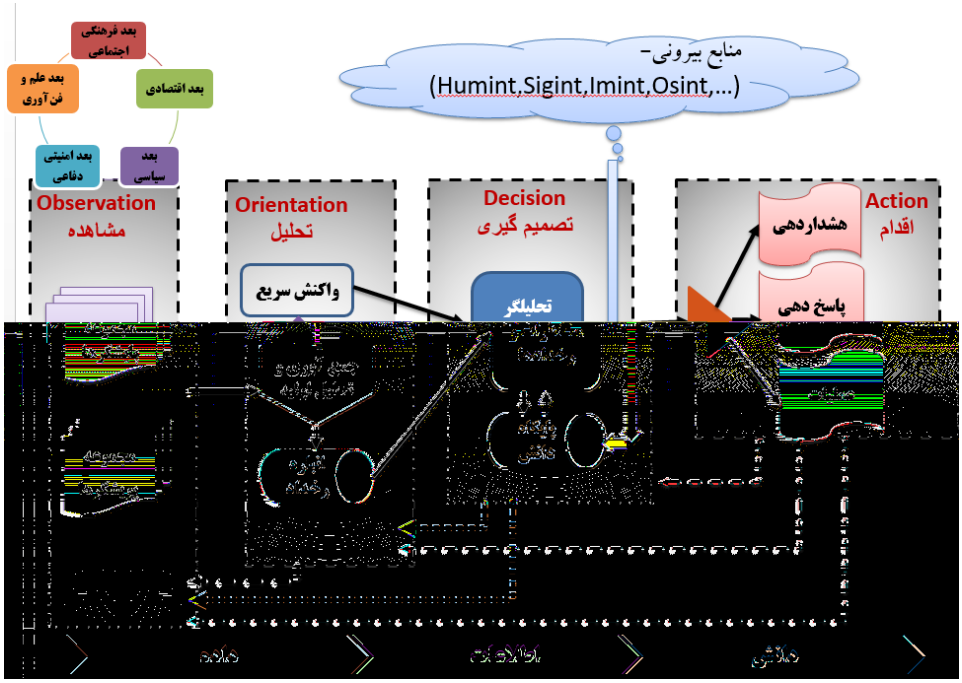
1.Security Operation Center
2.Computer Security Incident Response Team
3.Computer Emergency Response Team
4.Information Sharing and Analysis Center
5.Information Security Alert System

می‌توان تفاوت‌هایی را مشاهده نمود؛ مانند آنکه در الگوی دروازه‌بان سایبری انگلیس اقدام سریع در مواجهه با مشکلات می‌تواند قبل از مرحله تصمیم‌گیری به وقوع بپیوندد که امری، ضروری است. درنهایت آنچه در اسناد مشاهده گردید به‌رغم وجود دیدگاه راهبردی به این مدل در کشورهای منتخب، مبتنی بر اسناد در دسترس، به مقوله پایش فضای سایبری بیشتر در بُعد فنی پرداخته شده است و به عمده تهدیدات این فضا که می‌تواند تبعات گسترده‌ای را در ابعاد دیگر نیز شامل شود، بیشتر از لحاظ فنی توجه گردیده است و به پایش روند حاکم بر این فضا و آنچه که با نام جنگ نرم از آن یاد می‌شود کمتر پرداخته شده است.

ارائه مدل بومی رصد، پایش و هشداردهی سایبری بر اساس چرخه فرماندهی کنترل اودا

همان‌گونه که ذکر گردید مدل پیشنهادی بر اساس چارچوب چرخه اودا[1] و نیز نتیجه مطالعات تطبیقی و احصای نظرات نخبگان با استفاده از مصاحبه به دست آمده است. نخبگان این بخش شامل ۱۰ نفر از کارشناسان و مدیران حوزه فناوری اطلاعات و ارتباطات با مدرک دکتری تخصصی و ۱۵ سال تجربه کاری انتخاب گردیدند. این مدل ضمن تشخیص ناهنجاری و تحلیل شرایط موجود به روندهای آینده نیز توجه دارد، به‌طوری‌که در هر مرحله فیدبک به مراحل قبل با هدف تدقیق روال‌ها و فرایندها توجه دارد و نیز در مرحله دوم (تحلیل) قابلیت واکنش سریع بر اساس مدل دروازه‌بان سایبری انگلیس و نیز توصیه نخبگان گنجانده شده است که این بخش می‌بایست بر اساس فهم اتوماتیک و یادگیری ماشین به برخی از اقدامات اولویت‌دار در صورت بروز رخداد سایبری بپردازد. وظایف هرکدام از بخش‌های این مدل به‌صورت زیر می‌باشد:

1. OODA



شکل ۵- مدل بومی رصد و پایش و هشداردهی سایبری

همان‌گونه که در شکل ۵ بیان شده است شاخص‌ها و مؤلفه‌های بومی بودن مدل عبارت‌اند از:

همان‌گونه که در مدل مفهومی فضای سایبری شورای عالی فضای مجازی در شکل ۶ نمایش داده شده است، امنیت مشتمل بر کلیه لایه‌های کاربر، محتوا، خدمات و زیرساخت می‌شود؛ لذا جهت رصد، پایش و هشداردهی سایبری در کشور جمهوری اسلامی ایران می‌بایست به کلیه ابعاد قدرت سایبری توجه نمود، زیرا مخاطرات این فضا در کلیه ابعاد وجود دارد. وجود تحریم‌های اقتصادی و انعکاس آن در فضای مجازی، جریان‌سازی جریانات سیاسی معارض نظام و انتشار محتوای فراخوانی اعتراضات مانند دی‌ماه ۹۶، جنگ نرم و هجمه شدید فرهنگی با انتشار محتوای خلاف فرهنگ ایرانی، همه گواه وجود مخاطرات جدی در سایر ابعاد فضای مجازی علاوه بر زیرساخت‌های فنی کشور ایران می‌باشد. لذا تعمیم مرحله مشاهده از بُعد فنی به پنج بُعد اقتصادی، فرهنگی اجتماعی، سیاسی، امنیتی دفاعی، علم و فناوری در مدل بومی صورت پذیرفته است.

شکل ۶. مدل مفهومی فضای سایبری (شورای عالی فضای مجازی، ۱۳۹۲)

گنجاندن مرحله واکنش سریع در مرحله تحلیل به‌منظور رسیدگی به حملات آنی و صدور اقدامات اولیه عاجل مستقل از اتمام چرخه اودا.

لحاظ نمودن پایگاه دانش به‌عنوان بازوی کمکی لایه تصمیم‌گیری که به‌صورت خودکار در حال به‌روزرسانی و نیز یادگیری ماشین بر اساس رفتارهای گذشته می‌تواند عمل نماید؛ به‌عنوان نمونه تقویم امنیتی ایران یکی از مثال‌های پایگاه دانش می‌باشد که خود می‌تواند منشأ مخاطرات امنیتی را در کلیه ابعاد فضای مجازی در لایه تصمیم‌گیری نمایان سازد و به عبارت ساده‌تر پایگاه دانش خودیادگیر از رفتارهای پرتکرار می‌باشد و نیز گذشته فهم است تا از بروز مخاطرات تکراری جلوگیری نماید.

۶-۷. تشریح حلقه اودا

شکل ۵ بیانگر حلقه بسته تصمیم‌گیری می‌باشد که مجموعه فعالیت‌ها به نحوی هدایت می‌شوند که تشکیل یک حلقه بسته داده و همه به یک نقطه بازمی‌گردند و آن نقطه مرکز تصمیم‌گیرنده یا فرماندهی می‌باشد. در حال حاضر حلقه اودا فراتر از یک حلقه مورد توجه فرماندهان قرار گرفته است. هر مرحله‌ای از حلقه، خود یک فرایندی است که به شرح فرایندهای زیر ساخته می‌شود:

شکل ۷- مشاهده، تحلیل، تصمیم، اقدام (Benaskeur, 1998)

۶-۷-۱. فرایند مشاهده

فرایند مشاهده هم شامل تصمیم بر مشاهده فعالیت‌های خاص و اقدامات فیزیکی مورد نیاز برای دریافت داده مربوط به اطلاعات مراقبت و هدف‌گیری بوده و آنچه در مدل بومی سایبری می‌بایست به آن توجه گردد جمع‌آوری حسگرها به‌صورت جامع و در ابعاد گوناگون می‌باشد؛ به‌عبارت‌دیگر این مدل تنها در بُعد فنی به پایش فضای سایبری نمی‌پردازد بلکه در کلیه ابعاد فناوری، سیاسی، امنیتی، دفاعی، فرهنگی و اجتماعی و ... به رصد و پایش فضای سایبری به‌منظور دستیابی به یک نمای ۳۶۰ درجه از این فضا می‌پردازد و انتخاب حسگرها در این مرحله می‌بایست به‌صورت جامع صورت پذیرد. نکته دیگر در این بخش توجه به پوشش تمامی سطوح تکنیکی، تاکتیکی و راهبردی می‌باشد، به‌نحوی‌که علاوه بر لایه عملیاتی، تصمیمات در کلیه سطوح به‌صورت سلسله‌مراتبی، بر اساس درجه اهمیت و دامنه اثربخشی تا سطح تاکتیکی و راهبردی نیز خواهد رفت (ولوی، ۱۳۹۵).

۶-۷-۲. فرایند جهت‌دهی و تطبیق‌دهی

شامل داده‌کاوی جهت کشف یا یادگیری مشخصات ناشناخته قبلی در داده است که می‌توان از آن به‌عنوان قالب‌هایی جهت آشکارسازی و پیشگویی بعدی در فرایندهای ادغام

اطلاعات استفاده کرد. نکته قابل توجه در این لایه در نظر گرفتن بخش واکنش سریع است که می‌تواند بر اساس روش‌های یادگیری ماشین به انجام برخی واکنش‌های ضروری و آنی اولیه منتج گردد. این واکنش می‌تواند بر اساس آستانه‌های قابل تعریف به‌عنوان ابزار هشدار[1] سریع در مواجهه با رویدادهای سریع جهت اتخاذ تصمیم در مراحل بعد بپردازد(ترخان، ۱۳۹۵).

۳-۷-۶. فرایند تصمیم‌گیری

شامل فرایندهای اتوماتیک و دستی (توسط انسان) است. پاسخ‌های ساده و سریع را می‌توان بر مبنای آشکارسازی شرایط از پیش تعیین‌شده به‌صورت خودکار تنظیم نمود. درحالی‌که قضاوت فرماندهان برای تصمیم‌گیری‌های پیچیده‌تر و حیاتی نیاز بوده و شرایط را جهت دخالت به وجود می‌آورد.

با توجه به حجم بالای اطلاعات و پیشگیری از سردرگمی فرماندهان در تصمیم‌گیری لازم است تا سرعت پردازش اطلاعات در داده‌کاوی و تلفیق اطلاعات افزایش یابد. تلفیق اطلاعات یک فرایند تطبیقی تولید دانش است که در آن عناصر گوناگون مشاهدات مشابه و غیرمشابه (داده را مرتب، هم‌بسته و ترکیب کرده) را به‌صورت مجموعه سازمان‌یافته و دارای فهرست تبدیل می‌کند. در نظر گرفتن پایگاه دانش در این بخش به‌منظور افزودن امکان تقاطع اطلاعات و دانش از منابع دیگر به محیط پایش سایبری لحاظ گردیده است. در بسیاری از مواقع جهت ارتقاء دقت رصد و پایش فضای سایبری به اطلاعات دیگری در فضاهای دیگر نیاز است که به دلیل همپوشانی و یا اثرگذاری این فضا بر فضاهای دیگر، این بخش بسیار مهم می‌باشد. پایگاه دانش مذکور دائماً در حال به‌روزرسانی توسط فضای پایش سایبری و نیز محیط بیرونی می‌باشد (ترخان، ۱۳۹۵).

1. Early Warning

۴-۷-۶. فرایند اقدام

مجموعه مراحل طی‌شده از زمان ابلاغ تا اجرای آن فرایند را اقدام گویند که در سه بخش هشدار، پاسخ‌دهی و عملیات صورت می‌پذیرد (ولوی، ۱۳۹۵).

۷. روش تحقیق

در این پژوهش از روش ترکیبی استفاده شده است؛ یعنی با استفاده از آماره‌های توصیفی و نیز تحلیل-کیفی مستند بر آراء و دیدگاه صاحب‌نظران مطلع به موضوع مورد مطالعه، انجام شده و درنهایت نظام رصد، پایش و هشداردهی با رویکرد امنیتی تبیین گردیده که برای دولتمردان و مدیران امنیتی کاربرد دارد.

روش مورد استفاده در این تحقیق روش ترکیبی اکتشافی و به‌صورت دومرحله‌ای است که ابتدا با مصاحبه باز و گردآوری و مطالعه مستندات به شناسایی مؤلفه‌ها و ابعاد طرح به‌صورت کیفی پرداخته شده است و سپس با استفاده از ابزار پرسش‌نامه و توزیع در میان خبرگان به مدل بومی با رویکرد امنیت ملی دست یافته‌ایم و مدل تحقیق به‌صورت زیر می‌باشد:

شکل ۸. روش پژوهش ترکیبی (حافظ‌نیا، ۱۳۸۳)

جهت انجام این پژوهش در گام اول مدل استنتاجی بر اساس مبانی نظری و مطالعات تطبیقی با نخبگان حوزه فناوری اطلاعات به‌صورت مصاحبه باز طرح گردید و سپس تعریف نظام و نیز مؤلفه‌ها و شاخص‌های نظام جهت روایی تعریف نظام طی یک پرسشنامه بسته توسط نخبگان مورد بررسی و پاسخ قرار گرفت و در مرحله سوم مدل دستیابی‌شده متأثر از مرحله اول و دوم مصاحبه و پرسشنامه در قالب پرسشنامه بسته و از طریق روش کمی مورد سنجش قرار گرفت.

۸. نتایج تحلیل

در این بخش مبتنی بر روش تحقیق ترکیبی، مدل مفهومی احصاءشده در شکل ۵ طی سه مرحله مورد ارزیابی جامعه نخبگان سایبری کشور قرار گرفته است که خلاصه‌های پژوهش در ادامه ارائه گشته است. به این منظور در مرحله اول ضمن تبیین چارچوب نظری پژوهش برای حدود ۱۰ نفر از مدیران سایبری کشور، مدل مفهومی مدل رصد، پایش و هشداردهی سایبری به‌صورت مصاحبه باز ارائه گردید. انتخاب جامعه آماری به نحوی صورت گرفت که در تمامی ابعاد فضای سایبر که در پژوهش حاضر مورد توجه قرار گرفته است نماینده‌ای انتخاب گردد و سپس نتایج ارزیابی ایشان در جلسات مطالعات گروهی به بحث گذاشته شد و نکات جمع‌بندی در مدل مفهومی اصلاح گردید و سپس دو پنل خبرگان برگزار گردید و در انتها سؤالات پژوهش به‌منظور ارزیابی پایایی و روایی تحقیق پس از جمع‌بندی طی دو مرحله اصلاح گردید و درنهایت در میان ۵۰ تن از صاحب‌نظران و نخبگان حوزه سایبری توزیع گردید که در فصل حاضر به جمع‌بندی نتایج تحقیق میدانی پرداخته شده است. در بخش تبیین و مستندسازی، تجربیات خبرگان، کارشناسان و متخصصان خبره و مدیران حوزه امنیت سایبری نظام جمهوری اسلامی ایران می‌باشند که بر اساس شرط انتخابی به‌صورت تمام‌شمار و با حجم ۷۰ نفر به‌صورت ترکیبی از نخبگان و صاحب‌نظران علمی کشور و نیز مدیران باسابقه اجرایی بالا انتخاب گردیده است.

۸-۱. تحلیل جمعیت‌شناسی

از بین ۵۷ پرسشنامه تکمیل‌شده نتایج تحلیل جمعیت‌شناسی به‌صورت زیر بوده است.

جدول ۴. نتایج تحلیل توصیفی جمعیت‌شناختی

	N	حداقل	حداکثر	میانگین	انحراف معیار
سن	54	33	59	46.17	5.142
سابقه	53	5	30	12.81	4.962
مدرک تحصیلی	55	1	3	2.25	.844
تعداد صحیح	50				

از نظر سنی حداقل سن پاسخگویان ۳۳ و حداکثر آن ۵۹ سال بوده و میانگین سنی پاسخگویان نیز ۴۶,۱۷ سال با انحراف معیار ۵,۱۴ است. به‌علاوه تعداد بیست‌ویک نفر از پاسخگویان در رنج سنی ۴۱ تا ۴۵ و همین تعداد نیز در رنج سنی ۴۶ تا ۵۰ سال قرار داشته‌اند که بخش عمده‌ای از پاسخگویان را شامل می‌شود. همچنین تعداد شش نفر نیز در رنج سنی ۵۱ تا ۵۵ سال قرار داشتند. سابقه فعالیت پاسخگویان در حوزه‌های تخصصی فضای سایبر نیز بین ۵ تا ۳۰ سال با میانگین ۱۲,۸۱ و انحراف معیار ۴,۹۶ بوده است. در این بین تعداد ۲۷ نفر بین ۱۱ تا ۱۵ سال سابقه فعالیت تخصصی داشته‌اند.

از نظر مدارک تحصیلی نیز تعداد ۲۷ نفر از پاسخگویان مدرک تحصیلی دکتری، ۱۳ نفر کارشناسی ارشد و ۱۵ نفر مدارک تحصیلی کارشناسی داشته‌اند.

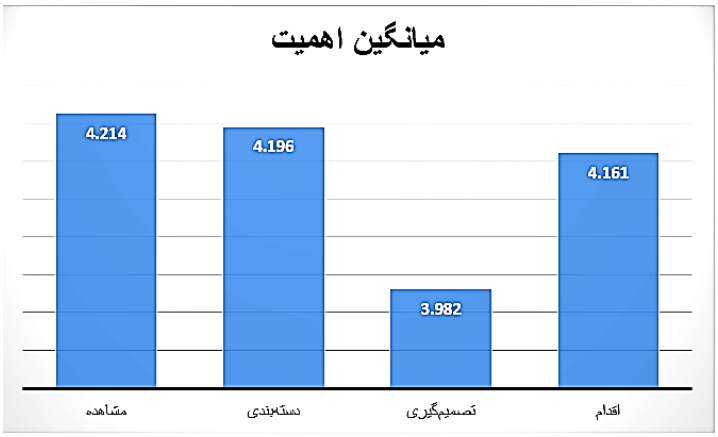
بررسی و ارزیابی مدل از منظر چرخه رصد (مشاهده، دسته‌بندی، تصمیم، اقدام)

جدول ۵- تحلیل کمی اهمیت مراحل چرخه اودا از نگاه خبرگان

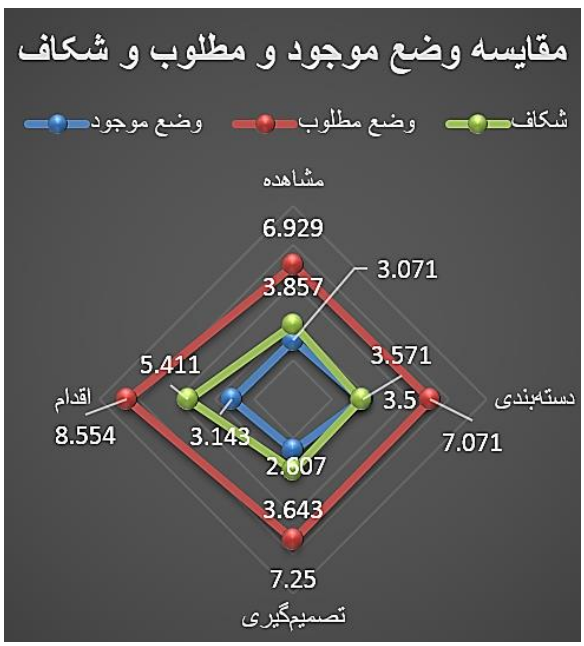
رتبه	مرحله	میانگین اهمیت	وضع موجود	وضع مطلوب	شکاف	شکاف موزون
۳	مشاهده	4/214	3/071	6/929	3/857	16/255
۴	دسته‌بندی	4/196	3/571	7/071	3/500	14/688
۲	تصمیم‌گیری	3/982	2/607	7/250	4/643	18/489
۱	اقدام	4/161	3/143	8/554	5/411	22/512

مشاهده، از این جهت که به‌عنوان اولین گام در مدل مفهومی پژوهش حاضر زیربنای چرخه مدل رصد و پایش تلقی می‌گردد از نظر خبرگان بیشترین اهمیت را داشته است. پس از آن تصمیم‌گیری بر اساس معیارها و اصول مدون و مشخص استقرار یافته است. لذا ضرورت دارد در مدل پیشنهادی مبانی تصمیم‌گیری به‌عنوان ورودی مرحله اقدام تعیین گردد. از نظر خبرگان به دلیل تصمیم‌گیری‌های سلیقه‌ای و غیرمنطقی در شرایط جاری، شکاف وضع موجود و مطلوب بالاترین گزارش شده است و همین موضوع مقدار شکاف موزون آن را در صدر نشانده است. در یک واحد مدل ارائه‌شده، تشخیص یک رویداد و

نوع آن پس از مشاهده تظاهرات و رفتارهای غیرمعمول در فضای سایبر در مرحله دوم چرخه مدل قرار دارد که این موضوع نیز می‌بایست مبتنی بر شاخص‌ها و معیارهای مشخص باشد تا حداقل مخاطرات را به دنبال داشته باشد، چراکه این مرحله پیش‌درآمد مرحله اقدام خواهد بود.



شکل ۹. نمودار میانگین اهمیت مراحل چهارگانه چرخه اودا



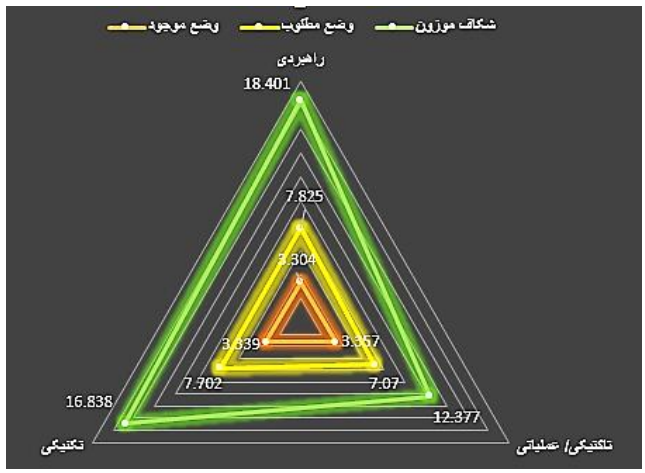
شکل ۱۰. نمودار راداری مقایسه وضع موجود، مطلوب و شکاف موزون مراحل چهارگانه چرخه اودا

بررسی اهمیت سطوح سه‌گانه راهبردی، عملیاتی و تکنیکی در مدل پایش

بر اساس نتایج آمار توصیفی و پس از محاسبه شکاف که حاصل تفاوت بین وضع مطلوب و وضع موجود است و همچنین شکاف موزون که حاصل‌ضرب شکاف در اهمیت مؤلفه است (محمدی‌پور، ۱۳۹۰) نتایج نهایی به شرح جدول زیر به دست آمده است. درنتیجه بر اساس نظرات خبرگان، بیشترین توجه مدل رصد باید معطوف به سطح راهبردی و در وهله دوم سطح تکنیکی و فنی و سپس سطح تاکتیکی/عملیاتی باشد.

جدول ۶. نتایج آمار توصیفی و تحلیل شکاف

رتبه		اهمیت	وضع موجود	وضع مطلوب	شکاف	شکاف موزون
۱	راهبردی	4/070	3/304	7/825	4/521	18/401
۲	تاکتیکی/ عملیاتی	3/333	3/357	7/070	3/713	12/377
۳	تکنیکی	3/860	3/339	7/702	4/362	16/838



شکل ۱۱. نمودار راداری مقایسه وضع موجود، مطلوب و شکاف موزون از منظر سطوح سه‌گانه راهبردی، تاکتیکی/عملیاتی و تکنیکی

با توجه به اینکه هرگونه اقدام تاکتیکی و تکنیکی، راهبرد معینی لازم دارد و حوزه سایبر نیز از این قاعده مستثنا نیست لذا با توجه به فقدان سیاست و راهبرد مشخص در حوزه رصد و پایش فضای سایبر کشور جنبه راهبردی از نظر نخبگان اهمیت بالاتری پیدا کرده است؛ اما با

توجه به اینکه هر روز با بروز و ظهور فناوری‌های نوین مواجه هستیم لذا طبیعی است که وجه فنی و تکنیکی در اولویت بالاتری نسبت به تاکتیک و عملیات قرار گیرد؛ چراکه این موضوع در واکنش به وجه قبلی نمود خواهد یافت. لذا از نظر خبرگان ابتدا راهبردها تدوین و پس از پرداختن به موضوعات تکنیکی، وجه تاکتیک و عملیات می‌بایست مدنظر قرار گیرد.

بررسی مدل از منظر ابعاد قدرت ملی

جدول ۷- نتایج آمار توصیفی و تحلیل شکاف مؤلفه‌های بخش مشاهده

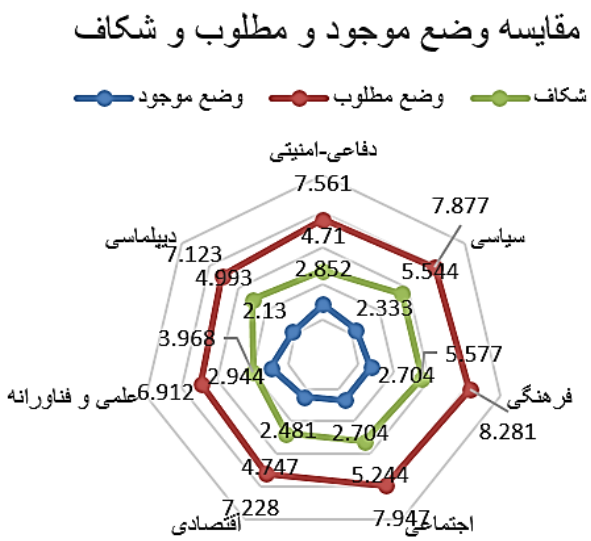
رتبه		میانگین اهمیت	وضع موجود	وضع مطلوب	شکاف	شکاف موزون
۱	فرهنگی	4/316	2/704	8/281	5/577	24/069
۲	اجتماعی	4/070	2/704	7/947	5/244	21/343
۳	دیپلماسی	4/211	2/130	7/123	4/993	21/024
۴	دفاعی-امنیتی	4/281	2/852	7/561	4/710	20/160
۵	اقتصادی	3/930	2/481	7/228	4/747	18/653
۷	علمی و فناورانه	3/456	2/944	6/912	3/968	13/713
۶	سیاسی	3/263	2/333	7/877	5/544	18/090

از نظر خبرگان با توجه به رشد کسب‌وکارهای اینترنتی در فضای سایبر کشور، ضرورت رصد و پایش این فضا به‌منظور تأمین امنیت اقتصاد تجارت در این حوزه از اهمیت نسبتاً بالایی برخوردار شده است. همچنین با توجه به شکاف بالای وضع موجود که بر مبنای نظر خبرگان احصاء شده، مقدار آن را در صدر اولویت قرار داده است.

حسب نظر خبرگان، از آنجا که تفکیک فضای سایبر به داخل و خارج و ایجاد حدومرز فیزیکی به سبک حدود جغرافیایی متصور نیست لذا دیپلماسی سایبری به معنی ایجاد همکاری‌های منطقه‌ای و فرامنطقه‌ای بین‌المللی، یک ضرورت انکارناپذیر در تکمیل فرایند رصد و پایش است. ازاین‌رو دیپلماسی در جایگاه دوم قرار گرفته است. درحالی‌که شکاف

احصاءشده در حوزه فرهنگی در مقایسه با سایر ابعاد، مقدار قابل توجهی را به خود اختصاص نداده است، لیکن اهمیت پرداختن به این حوزه از نظر نخبگان بالاترین بوده است که شکاف موزون آن را در جایگاه سوم قرار داده است. سایر ابعاد دفاعی–امنیتی و اجتماعی هم از منظر اهمیت و هم از نظر میزان شکاف حدوداً هم‌تراز بوده‌اند و در جایگاه‌های پایین‌تر واقع شده‌اند.

شکل ۱۲. نمودار میانگین اهمیت ابعاد قدرت سایبری در مرحله مشاهده



شکل ۱۳. نمودار راداری مقایسه وضع موجود، مطلوب و شکاف موزون ابعاد قدرت سایبری در مرحله مشاهده

بر اساس نتایج تحلیلی به‌دست‌آمده، توجه به بُعد فرهنگی از اولویت بالاتری در وضعیت مطلوب برخوردار می‌باشد. همچنین در وضعیت موجود، بیشترین اهمیت به بُعد علمی و فناوری سایبری معطوف می‌باشد و بیشترین شکاف از وضع موجود تا مطلوب مربوط به بُعد فرهنگی سایبر می‌باشد و این امر لزوم توجه بیش‌ازحد این مدل به پرداختن به مقوله فرهنگی فضای سایبری می‌باشد.

۹. خلاصه و نتیجه‌گیری

در پژوهش حاضر ضمن مرور ساختارهای نظارت سایبری در سه کشور آمریکا، انگلیس و کره جنوبی به ارائه یک مدل بومی رصد، پایش و هشداردهی سایبری بر اساس چرخه فرماندهی کنترل اودا پرداخته شد. اصلی‌ترین تفاوت مدل ارائه‌شده نسبت به نتایج مطالعات تطبیقی، توجه به همه ابعاد فضای سایبری؛ شامل اقتصادی، فرهنگی اجتماعی، علم و فناوری، امنیتی دفاعی و سیاسی می‌باشد که در سطوح عملیاتی، تاکتیکی و راهبردی به پایش فضای سایبری کشور می‌پردازد.

ویژگی‌های مدل بومی رصد، پایش و هشداردهی سایبری

۱. این مدل از سرعت اقدام فرماندهی در تبدیل یک موقعیت اطلاعاتی برتر به یک اقدام عملیاتی، پشتیبانی می‌کند و رعایت ترتیب و توالی تمامی فرایندهای حلقه بسته تصمیم‌گیری، موجبات یک هم‌افزایی ناشی از تعامل بین فرایندها را به وجود خواهد آورد.
۲. با اجرای دقیق مدل، آگاهی وضعیتی مناسب‌تری برای مسئولین ایجاد شده و آن‌ها را در شناسایی و رصد به‌موقع فضای سایبری توانمندتر می‌سازد.
۳. با اجرای دقیق حلقه پیشنهادی در مدل، فرایندها و دستیابی به سرعت، دقت و خودهم‌زمانی است که منجر به بهبود آگاهی وضعیتی فرمانده شده و درنتیجه طی دوره زمانی مشخص، عملیات بیشتری انجام گرفته و فرماندهان قادر خواهند بود

بر اقدامات خودی و دشمن متمرکز شوند و هدف مورد نظر را در زمان مناسب نشانه گرفته و در زمان مناسب انهدام نمایند.

۴. دید جامع نسبت به کل فضا و ابعاد فضای سایبری ایجاد می‌شود.

۵. توجه به سطوح اثربخشی مدل رصد و پایش سایبری متشکل از سطح عملیاتی، تاکتیکی و راهبردی که می‌تواند در اتخاذ تصمیم و نیز سطح آن مؤثر باشد.

۶. وجود بازخورد در تمامی مراحل این چرخه با هدف پویایی و سرعت بیشتر و هوشمندسازی حداکثری جهت خودیادگیری مدل، متناسب با سرعت روند تغییرات فضای سایبری در تمامی ابعاد و مؤلفه‌های قدرت سایبری.

همان‌گونه این حلقه به‌عنوان سریع‌ترین و دقیق‌ترین حلقه در جنگ فرماندهی و کنترل شناخته شده است، در تشخیص، پیشگیری و هشداردهی فضای سایبری به دلیل پویایی و سرعت تغییرات بالا، بسیار مؤثر خواهد بود.

۱۰. پیشنهادات

با عنایت به پژوهش صورت‌پذیرفته و دامنه آن که معطوف به دستیابی به چارچوب نظام رصد، پایش و هشداردهی سایبری بوده است، موارد زیر جهت تکمیل این حوزه و در ادامه این پژوهش پیشنهاد می‌گردد:

- تدوین طرح راهبردی رصد، پایش و هشداردهی سایبری
- معماری سازمانی بومی جهت پیاده‌سازی نظام رصد، پایش و هشداردهی سایبری

در ادامه این پژوهش می‌توان ضمن مطالعه وضع موجود از حیث مدل‌های رصد پایش و هشداردهی سایبری کشور پرداخت و با ترسیم وضع مطلوب، راهبردهای دستیابی به آن‌ها را تحلیل نمود.

فهرست منابع ومآخذ

الف. منابع فارسی

- 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.
- ترخان، محمدرضا و فتوح‌آبادی، وحید (۱۳۹۵)، ارائه یک الگوی مفهومی مبتنی بر آگاهی موقعیتی با هدف بهبود امنیت سایبری، دومین کنفرانس بین‌المللی یافته‌های نوین پژوهشی در مهندسی برق و علوم کامپیوتر، رامسر، مؤسسه آموزش عالی غیرانتفاعی کسری رامسر، https://www.civilica.com/Paper-COMCONF02-COMCONF02_040.html
- تقی‌پور، رضا (۱۳۹۲)، کارگروه مطالعات گروهی دانشجویان دوره اول امنیت سایبری، دانشگاه عالی دفاع ملی، تهران: دانشگاه عالی دفاع ملی.
- حاجیانی، ابراهیم (۱۳۹۰)، هشداردهی: کارکرد تحلیل اطلاعاتی در پیشگیری از غافلگیری، فصلنامه پژوهشی مطالعات راهبردی ۵۳ (سوم)، سال چهاردهم، ۱۵۱–۱۲۷.
- حسینی، پرویز و ظریفی‌منش، حسین (۱۳۹۲)، مطالعه تطبیقی ساختار دفاع سایبری کشورها، فصلنامه پژوهش‌های حفاظتی امنیتی دانشگاه جامع امام حسین (علیه‌السلام)، سال دوم، شماره ۵، ۶۸–۴۱.
- دوپویی، ترورنویت (۱۳۷۹)، اطلاعات نظامی، پیروز ایزدی، تهران: انتشارات دافوس (سپاه پاسداران انقلاب اسلامی).
- دیویس، جک (۱۳۸۶)، هشدار استراتژیک: اگر شگفتی غیر قابل اجتناب است، تحلیل چه نقشی را ایفا می‌کند؟، معاونت پژوهشی، دانشکده اطلاعات، فصلنامه دانش اطلاعاتی (شماره چهارم)، دانشکده اطلاعات، ۸۳–۶۱.
- زندی، ابراهیم (۱۳۷۹)، مفهوم و جایگاه پیش‌بینی در بررسی اطلاعاتی، فصلنامه پژوهش اطلاعاتی–امنیتی سال اول دوره جدید، (شماره اول)، دانشکده اطلاعات.
- صالحی، محمود (۱۳۷۹)، مدل چهارلایه‌ای مدیریت بحران: الگویی برای خروج از بحران‌های سیاسی اجتماعی، فصلنامه پژوهش اطلاعاتی–امنیتی (اول)، سال اول دوره جدید.
- علیخانی، علی (۱۳۹۳)، هشدارشناسی، تهران: دانشکده اطلاعات، چاپ اول.

- غیاث‌آبادی، عباس؛ فعلی، صابر و انصاری، محمد (۱۳۹۲)، ارزیابی حلقه OODA در DBA, DBK با رویکرد فرماندهی و کنترل، هفتمین کنفرانس علمی فرماندهی و کنترل ایران، تهران: دانشگاه امام حسین.
- فکوری، هشداردهی والاترین مأموریت اطلاعات (۱۳۹۳)، دانشکده اطلاعات، ۱۵۹–۱۵۷.
- محمدی‌پور، ا (۱۳۹۰)، روش تحقیق کیفی، ضد روش ۲، تهران: جامعه‌شناسان.
- نورآذر، علی؛ نوآذر، منصور و غیاث‌آبادی، عباس (۱۳۹۳)، پیاده‌سازی جنگ الکترونیک در حلقه فرماندهی و کنترلOODA ، هشتمین کنفرانس ملی فرماندهی و کنترل ایران(C4I) ، تهران: دانشگاه هوایی شهید ستاری،

http://www.civilica.com/Paper-CCCI08-CCCI08_119.html

- ولوی، محمدرضا و صحرایی، مهدی (۱۳۹۵)، ارائه مدل رصد، پایش و هشداردهی سایبری بر اساس چرخه فرماندهی کنترل OODA مبتنی بر مطالعه تطبیقی کشورهای هدف، نهمین کنفرانس ملی فرماندهی و کنترل ایران، تهران: دانشگاه خوارزمی – انجمن علمی فرماندهی و کنترل ایران،

https://www.civilica.com/Paper-CCCI09-CCCI09_051.html https://www.civilica.com/Paper-CCCI09-CCCI09_051.html

ب. منابع لاتین

- Global cybersecurity index & cyberwellness profiles. (2015), ITU & ABI research Comp.
- Lenders,Vincent. (2015), Gaining an Edge in cyberspace with Advanced situational Awareness. IEEE. April 2015
- "Cyber Command Fact Sheet". U.S. Department of Defense. 21 May 2010. Archived from the original on 16 April 2014. Retrieved 16 April 2014. DOD, (2011),Department Of Defence Strategy For Operatingin Cyberspace,
- Mutula,Stephen M., 2007, Web Information Management, UK: Cahndos Publication
- Ottis, R.: (2010), Analysis of the 2007 Cyber Attacks Against Estonia From the Information Warfare Perspective In: Proceedings of the ۷th European Conference on Information Warfare and Security.
- KISA. (n.d.). Retrieved 05 08, 2015, from
- http://isis.kisa.or.kr/eng/ebook/ebook.html
- White Paper, Best Practices for Building a Security Operations Center, August 2006
- http://ca. com/Files/WhitePapers/best_practices_snoc_white_paper. pdf