مجله سیاست دفاعی
سال بیستم، شماره ۷۹، تابستان ۱۳۹۱

# جایگاه اعتماد اطلاعاتی در سپهر خط‌مشی دفاعی کشور

## (ارائه چارچوب پژوهشی برای مطالعه‌ی راهبرد دفاع در عمق برای مقابله با تهدیدهای رایانه‌ای)

تاریخ دریافت مقاله: ۱۳۹۱/۰۱/۲۲
تاریخ تأیید مقاله: ۱۳۹۱/۰۳/۱۶
صفحات مقاله: ۱۴۸ - ۱۳۱

عباس هادوی نیا [۱]
رحیم محترم‌قلانی [۲]

**چکیده:**

*افزایش حمله‌های سایبری در سالیان اخیر تبدیل به یک چالش دفاعی - امنیتی در سراسر جهان شده است. در شرایطی که جنگ‌های نظامی جای خود را به جنگ‌های سایبری و نرم داده‌اند، نظام‌های دفاعی کشورها نیز ناگزیرند توجه بیشتری به سوی راهبردهای دفاع در برابر چنین حمله‌هایی معطوف کنند. راهبرد دفاع در عمق، یکی از راهبردهای دفاع در برابر چنین حملاتی است و در این پژوهش نیز مورد توجه قرار گرفته است. با توجه به این‌که در بررسی پیشینه پژوهش‌ها در کشور موردی از توجه به این راهبرد دیده نشد، این تحقیق ارائه‌ی چارچوبی نظری برای جهت‌گیری پژوهش‌های آتی در این زمینه را هدف خود قرار داد. از این رو، اعتماد اطلاعاتی به عنوان مفهوم بنیادین راهبرد دفاع در عمق مورد کاوش نظری در حوزه‌ی امنیت سایبری بررسی گردید و در نتیجه سه بخش افراد، فناوری و عملیات به عنوان بخش‌های تشکیل‌دهنده‌ی اعتماد اطلاعاتی مطرح نمود که در راهبرد دفاع در عمق نقش کلیدی ایفا می‌کند. در پایان چارچوبی برای بررسی راهبرد مورد نظر در سیاست دفاعی کشور ارائه گردید که این سه بخش را همراه با عناصر پیشنهادی تشکیل‌دهنده‌ی آنها در بر داشته است. با توجه به ماهیت نظری این پژوهش، روش انجام آن تحلیل ادبیات اسنادی، در سطح اسناد منتشر شده سازمان‌های دفاعی بوده است که با جهت‌دهی یافته‌ها توسط پژوهشگران به یک چارچوب پیشنهادی منجر شده است.*

* * * * *

۱- دانشجوی دکترای مدیریت رسانه، دانشکده مدیریت دانشگاه تهران.
۲- دانشجوی دکترای مدیریت بازاریابی، دانشگاه تهران.

**واژگان کلیدی**

*اعتماد اطلاعاتی، راهبرد دفاع در عمق، امنیت رایانه‌ای، حملات سایبری.*

**مقدمه**

حملات سایبری به عنوان شکل غالب جنگ نرم در سالیان اخیر بخش عمده‌ای از توجه محافل خبری و اطلاعاتی کشور را به خود معطوف نموده است. تلاش‌های گسترده برای نفوذ در سیستم‌های اطلاعاتی کشور و سرقت اطلاعات حیاتی یک رویکرد متعارف جنگ نرم است که از طریق آن تلاش می‌شود تا به بنیه‌ی امنیت اطلاعاتی آسیب زده شود و از این رهگذر به عدم توازن در جنگ نرم دست یافته شود. هک کردن سایت‌ها، نفوذ به شبکه‌های تبادل اطلاعات، ارسال ویروس‌های مخرب، در اختیار گرفتن هدایت سیستم‌های اطلاعاتی و امثال آنها، نمونه‌هایی از تهدیدهایی هستند که سیستم‌های اطلاعاتی کشور همواره با آنها مواجه هستند. گسترش یافتن این حملات نیاز کشور به ارتقای سیاست دفاعی سایبری خود و به‌کارگیری راهبردهای قابل اعتمادتر دفاعی را مشخص‌تر می‌کند. جهت‌گیری پژوهش‌های کاربردی و نظری به سمت عناصر تقویت‌کننده‌ی سیاست دفاعی کشور در حوزه‌ی فناوری اطلاعات و دفاع سایبری یکی از مهم‌ترین نیازهای تحقیقاتی کشور است که جامعه‌ی علمی باید با توجه به آن، به ارتقای بنیه‌ی دفاعی کشور در زمینه‌ی جنگ نرم و پدافند اطلاعاتی بپردازد. در مطالعه‌ی پیش رو، پژوهشگران با تمرکز توجه تحقیقاتی خود به سازه‌ی اعتماد اطلاعاتی، کاربرد آن را در سیاست دفاعی از طریق مطالعه راهبرد دفاع در عمق مورد بررسی قرار داده‌اند.

**بیان مسأله**

در دهه‌ی اخیر الکترونیکی کردن امور کشور به‌عنوان یک رویکرد غالب در نظام اداری و اطلاعاتی کشور پذیرفته شده است و ایجاد دولت الکترونیک به‌عنوان مفهومی برای ایجاد یک نظام حاکمیتی کارآمد و انعطاف‌پذیر مورد توجه قرار گرفته است. مطابق با این رویکرد، سیستم‌های اطلاعاتی و ارتباطی دیجیتال و شبکه‌پایه به عنوان زیربنای مهم پیاده‌سازی فضای

حاکمیتی دیجیتال نقش مهمی ایفا می‌کنند. بدیهی است که اتکا بر چنین شبکه‌هایی در کنار مزایای فوق‌العاده خود، تهدیداتی را نیز به همراه داشته باشد. حملات سایبری یکی از مهم‌ترین این تهدیدات است. این حملات با اهداف گوناگون، از سرقت اطلاعات گرفته تا خرابکاری طیف وسیعی از مشکلات را به همراه دارد و می‌تواند منجر به از کار افتادن سیستم‌های حاکمیتی شود. از این رو، بخش بزرگی از سیستم‌های دفاعی هر کشوری به سیستم‌های دفاعی رایانه‌ای و شبکه‌ای اختصاص یافته است. حتی می‌توان ادعا کرد در شرایطی که به دلیل اهمیت فزاینده‌ی نهادهای بین‌المللی و فشارهای بین‌المللی، جنگ‌های فیزیکی و لشکرکشی‌های نظامی در دنیا کاهش یافته‌اند، حملات سایبری شکل اصلی تهاجم در برابر کشور دیگر و نهادهای آن را را یافته‌اند و مهم‌ترین نوع جنگ را می‌توان نه در جنگ‌های نظامی، که در جنگ نرم مشاهده کرد و از این رو، سامانه‌های دفاع الکترونیکی و مقابله با تهاجمات سایبری حتی مهم‌تر از سامانه‌های دفاعی نظامی کشورها تلقی می‌شوند. با توجه به این‌که کشور ما به دلیل موقعیت ممتاز خود در جهان یکی از اهداف مهم این حملات می‌باشد، نظام‌های دفاعی دیجیتال بخش مهمی از نظام دفاعی کشور را شکل می‌دهند. تحقیق حاضر با توجه به اهمیت دفاع در برابر تهاجمات سایبری، راهبرد دفاع در عمق را به عنوان یکی از راهبردهای مهم در انجام دفاع الکترونیکی مورد توجه قرار داده است و با توجه به نیاز فزاینده‌ی کشور در زمینه‌ی پژوهش در عرصه‌ی نظام‌های دفاعی، ارائه‌ی چارچوب برای انجام مطالعات در آینده را به عنوان مسأله‌ی پژوهش در نظر گرفته است. بنابراین، به‌طور مشخص مسأله‌ی پژوهش عبارت است از «ارائه‌ی چارچوبی برای بررسی اجرای راهبرد دفاع در عمق در سیاست‌های دفاعی کشور که پژوهش‌های آتی بر این چارچوب انجام شوند».

**اهداف تحقیق**

هدف اصلی این پژوهش ارائه‌ی چارچوبی برای پژوهش در زمینه‌ی بررسی اجرای راهبرد دفاع در عمق در سیاست‌های دفاعی کشور است.

در کنار این هدف اصلی، اهداف فرعی دیگری نیز مورد نظر پژوهشگران قرار داشته‌اند که عبارتند از:

۱) شناسایی نقش اعتماد اطلاعاتی در راهبرد دفاع در عمق؛

۲) شناسایی عناصر تشکیل‌دهنده‌ی اعتماد اطلاعاتی؛

۳) شناسایی عوامل تشکیل‌دهنده‌ی هر یک از عناصر اعتماد اطلاعاتی.

**سؤالات تحقیق**

سؤال اصلی این پژوهش عبارتست از:

اجرای راهبرد دفاع در عمق در عرصه سیستم‌های فناوری کشور با چه عناصری ممکن است؟

برای پاسخ دادن به پرسش اصلی باید ابتدا چند سؤال فرعی پاسخ داده شوند که عبارتند از:

۱) اعتماد اطلاعاتی چه نقشی در اجرای راهبرد دفاع در عمق دارد؟

۲) چه عناصری اعتماد اطلاعاتی را تشکیل می‌دهند؟

۳) چگونه می‌توان از این عناصر در تقویت خط‌مشی دفاعی کشور استفاده کرد؟

**روش انجام تحقیق**

اهداف پژوهش نشان‌دهنده‌ی این است که ماهیت این تحقیق نظری و ایجاد یک درک بنیادی برای پژوهش‌های آینده است. با توجه به چنین ماهیتی، و نظر به عدم وجود بدنه‌ی پژوهشی در این زمینه، از روش تحلیل ادبیات اسنادی توسط محققان استفاده گردید. عمده‌ی توجه بر مطالعه اسناد منتشر شده و در دسترس سازمان‌های دفاعی خارجی بوده است که با جهت‌دهی یافته‌ها توسط پژوهشگران به یک چارچوب پیشنهادی منجر شده است. با توجه به این‌که ارائه چارچوب هدف تحقیق بوده است؛ از این رو، از روش‌های میدانی استفاده نشد.

**راهبرد دفاع در عمق**

در برابر تهاجم‌های سایبری راه‌کارهای دفاعی متعددی ارائه شده است. در حقیقت همواره شکل‌های جدید حمله‌ی سایبری، راه‌کارها و راهبردهای نوینی را نیز برای بی‌اثر

گذاشتن به همراه داشته است. سیاست‌های دفاعی در برابر این حمله‌ها در سطوح مختلف، راهبردها، تکنیک‌ها، و راه‌کارهای گوناگون بوده‌اند. با توجه به این‌که راهبرد در دفاع نقش بالاتری را داشته است و تعیین‌کننده‌ی تکنیک‌ها و راه‌کارها می‌باشد؛ از این رو، توجه به راهبردها، تفکر راهبردی دفاعی را تشکیل می‌دهد و سبب می‌شود که ابزارها و راه‌کارهای مناسب با آن مورد توجه قرار گیرند. در میان راهبردهای متعددی که در برابر حملات سایبری مطرح شده است، راهبرد دفاع در عمق یکی از راهبردهای مهم و قابل توجه است.

«دفاع در عمق»[1] یک راهبرد عمل‌گرایانه برای دستیابی به ایمنی اطلاعات در محیط شبکه‌ای شده امروز است. این راهبرد، نوعی الگوبرداری است که عمیقاً بر کاربرد هوشمندانه‌ی فنون و فناوری‌هایی تکیه دارد که امروز در دسترس هستند. این راهبرد، میان توجه به ظرفیت حفاظت از اطلاعات با توجه به هزینه، عملکرد و ملاحظات عملیاتی توازن برقرار می‌کند. مقاله‌ی حاضر، مروری بر عناصر اصلی این راهبرد ارائه می‌دهد و به منابعی که بصیرتی را درباره‌ی آن فراهم می‌کند ارتباط می‌دهد (آژانس امنیت ملی آمریکا، ۲۰۰۲).

یکی از اصول پایه‌ای طراحی راهبرد دفاعی شناسایی اهداف، انگیزه‌ها و طبقه‌بندی انواع حملات به یک سیستم است. در حقیقت برای مقاومت مؤثر در برابر اطلاعات و سیستم‌های اطلاعاتی، هر سازمانی نیاز دارد تا دشمنان خود را بشناسد و به درستی تعریف کند، انگیزه‌های آنان را دریابد و دسته‌های مختلف هجوم آنها را شناسایی کند. به‌طور بالقوه، دشمنان می‌توانند گروه‌های مختلفی باشند، همچون دولت‌ها، تروریست‌ها، دسته‌های جنایتکار، هکرهای کامپیوتری یا رقبای شرکتی. انگیزه‌های آنها می‌تواند بسیار گوناگون باشد، همچون جمع‌آوری اطلاعات، سرقت مالکیت معنوی، از کار انداختن خدمات، رسواسازی، یا گاهی صرفاً کسب اعتبار و شهرت ناشی از موفقیت در یک حمله. انواع حملات می‌تواند در گروه‌های مختلفی دسته‌بندی شوند؛ همچون رصد کردن انفعالی ارتباطات، حملات فعال شبکه‌ای، حمله‌های نزدیک، استخراج اطلاعات درونی، و سرانجام حملاتی از طریق ارائه‌کنندگان منابع فناوری

1- Defense In Depth

اطلاعات در یک صنعت. علاوه بر این موارد کـه در برابـر دشـمنان هوشـمند و تحـت کنتـرل انسانی لازمند، مقاومت در برابر اثرات تعیین‌کننده‌ی حوادث غیر تخریبی همچون آتش، سـیل، کمبود قدرت و اشتباهات کاربران نیز از جمله توانایی‌های بسیار مهم سیستم دفاعی در فناوری اطلاعات است که باید در آنها تعبیه شود (نقشه راه وزارت دفاع آمریکا، ۲۰۱۱).

**اعتماد اطلاعاتی**

آژانس امنیت ملی آمریکا، راهبـرد دفـاع در عمـق را ابـزاری بـرای دسـتیابی بـه اعتمـاد اطلاعاتی[1] تعریف کرده است و بیان نموده که ایجاد اعتماد اطلاعاتی هـدف اصـلی از اجـرای راهبرد دفاع در عمق است که در نتیجه‌ی آن به یک ابزار دفاعی قابل اطمینان در برابر حملات سایبری دست یافته می‌شود. «بلیت» و «کوواچیچ» اعتماد اطلاعاتی را بـه سـادگی شـامل ایـن دانسته‌اند که: «اعتماد اطلاعاتی به شما اطمینان می‌دهد که اطلاعات شـما در همـان جـایی کـه می‌خواهید، در زمانی که می‌خواهید، در شرایطی که به آن نیازمندیـد در اختیـار صـرفاً شـما و کسانی است که می‌خواهید به آن دسترسی داشته باشند» (۲۰۰۶: ۳). این دو، اعتمـاد اطلاعـاتی را به عنوان مفهومی برای حفاظت از دارایـی‌هـای اطلاعـاتی در برابـر تخریـب، دسـتکاری و استخراج توسط دشمن مطرح نمودند. وزارت دفاع آمریکا (۲۰۱۲) اعتماد اطلاعاتی را به شرح زیر تعریف نموده است: «اقداماتی که برای حفاظت و دفاع از اطلاعات و سیستم‌های اطلاعاتی انجام می‌شود تا از در دسترس بودن، یکپارچگی، مجاز بودن دستیابی، محرمانـه بـودن و عـدم کپی‌برداری از آنها اطمینان حاصل شود. این امر شامل بازیابی سیسـتم‌هـای اطلاعـاتی توسـط یکپارچه نمودن حفاظت، جستجو و ظرفیت‌های واکنشی نیز می‌شـود». از دیـد آژانـس امنیـت ملی آمریکا (۲۰۰۲) اعتماد اطلاعاتی زمانی بـه دسـت مـی‌آیـد کـه اطلاعـات و سیسـتم‌هـای اطلاعاتی توسط نرم‌افزارهای ایمنی دربرابر حملات سایبری حفاظت شـده باشـند. اسـتفاده از این نرم‌افزارها باید بر اساس پارادایم‌های حفاظت، جستجو و واکنش[2] صورت پذیرد. این امـر

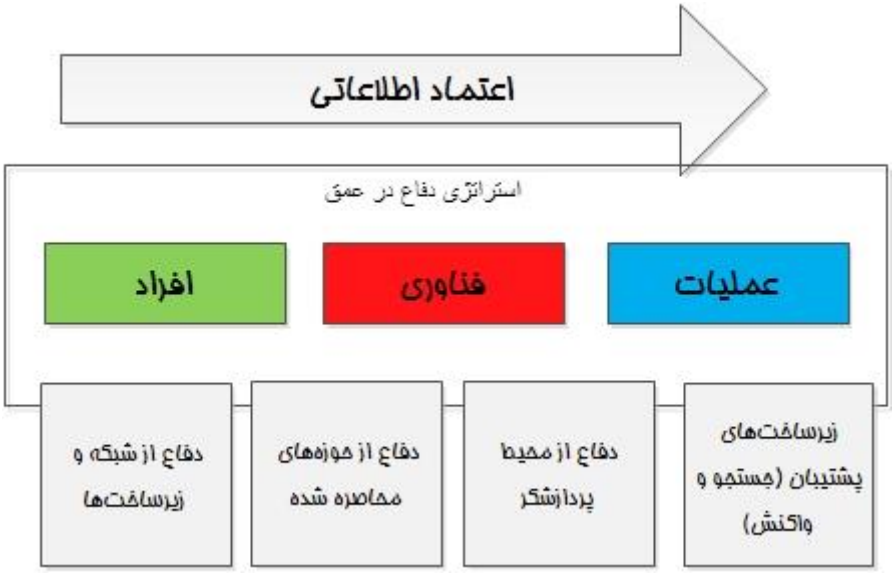
1 - Information Assurance
2 - Protection, Detection and Reaction

بدین معناست که علاوه بر سازوکارهای حفاظت، سازمان‌ها باید همیشه در انتظار وقوع حمله باشند و از این رو، ابزارهای جستجوی حمله و دستورالعمل‌هایی را شامل می‌شود که سبب واکنش به حملات و جلوگیری و بازیابی خسارت‌ها شوند. «مکوناچی» و همکاران (۲۰۰۱) در تلاشی برای طراحی یک مدل یکپارچه برای اعتماد اطلاعاتی، با استفاده از مدل «مک چمبر» سه بعد اساسی را برای آن در نظر گرفتند: بُعد ویژگی‌های اطلاعات؛ که شامل در دسترس بودن، انسجام اطلاعاتی و محرمانه بودن اطلاعات می‌شود؛ بُعد اقدامات اطلاعاتی که شامل آموزش، سیاست‌گذاری و استفاده از فناوری می‌شود؛ و سرانجام بُعد وضعیت اطلاعات که شامل تبادل، ذخیره کردن و پردازش اطلاعات می‌شود.

**اجزای راهبرد دفاع در عمق**

راهبرد دفاع در عمق، همان‌گونه که از نام آن نیز بر می‌آید، یک پدیده‌ی راهبردی است و دارای اجزایی است که برهم کنش این اجزا این راهبرد را شکل می‌دهد. این اجزا عبارتند از: افراد، فناوری و عملیات. غفلت از هر یک از این اجزا سبب می‌شود که طراحی و اجرای راهبرد با ناکارآمدی مواجه شود. با توجه به این‌که هدف از راهبرد دفاع در عمق دستیابی به اعتماد اطلاعاتی عنوان شده است، در نتیجه، در بررسی هر یک از این اجزا، به نقش آنها در ایجاد اعتماد اطلاعاتی توجه خواهیم کرد تا هدف اصلی انجام پژوهش مد نظر قرار داشته باشد.

علاوه بر اجزای تشکیل‌دهنده‌ی راهبرد دفاع در عمق، توجه به حوزه‌های عملکرد آن نیز عامل مهمی در شناسایی تأثیرگذاری آن در دستیابی به اعتماد اطلاعاتی است. همان‌طور که در شکل شماره‌ی (۱) دیده می‌شود، حوزه‌های تمرکز این راهبرد عبارتست از: دفاع از شبکه‌ها و زیرساخت‌ها، دفاع از حوزه‌های محاصره شده توسط عناصر مهاجم، دفاع از محیط پردازشگر و سرانجام ایجاد زیرساخت‌های پشتیبان که از طریق جستجوی تهدید و انجام عملیات پشتیبانی نسبت به رفع تهدید اقدام می‌کند. توجه به این حوزه‌ها در شناسایی عناصر تشکیل‌دهنده‌ی اجزای راهبرد کمک می‌کند. هر یک از اجزای تشکیل‌دهنده‌ی راهبرد دفاع در عمق را همراه با عناصر آنها را به ترتیب بررسی خواهیم کرد.

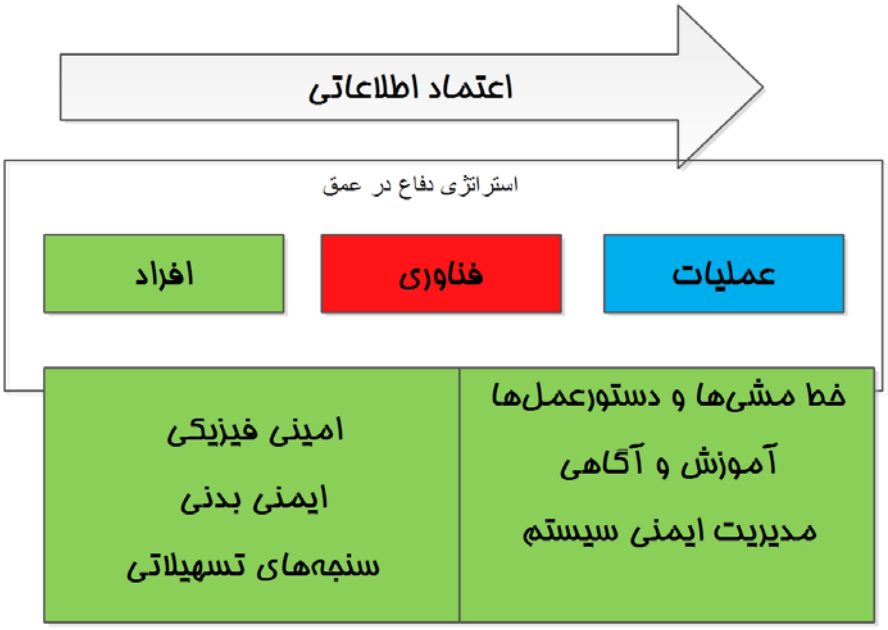



**شکل شماره‌ی ۱ - اجزای راهبرد دفاع از عمق و حوزه‌های تمرکز آن**

**افراد:** در هر سیستم دفاعی افراد مهم‌ترین عامل هستند. استفاده از پرسنل ماهر و آزموده که نه تنها به دانش پیشینی مسلط باشد، بلکه بتواند با خلاقیت و ارائه‌ی مهارت در برابر تهدیدهای تازه مقاومت کند، یک جزء بسیار مهم و حیاتی در موفقیت یک نظام دفاعی است. دستیابی به اعتماد اطلاعاتی در نخستین گام نیازمند تعهد مدیریت سطح ارشد سازمان است، نسبت به سرمایه‌گذاری و توجه مداوم به امنیت اطلاعاتی است. چنین امری جز با یک درک صحیح از تهدیدات احتمالی حال و آینده میسر نمی‌شود. معمولاً مدیر ارشد اطلاعات مسئول ایجاد چنین درکی و انتقال آن به سایر اعضای سازمان است.

تعهد مدیریت باید با عناصر دیگری همراه شود تا به اعتماد اطلاعاتی منجر شود. این تعهد باید به طراحی سیاست‌ها و ارائه‌ی دستورالعمل‌هایی منجر شود که در نتیجه‌ی آنها وظایف و مسئولیت افراد در زمینه‌ی ایجاد اعتماد اطلاعاتی به درستی مشخص شود، منابع موجود جهت ایجاد چنین سطح بالایی از اطمینان تخصیص داده شوند، افراد کلیدی همچون کاربران و مدیران سیستم‌ها و سایر افراد دارای تعامل آموزش داده شوند و افراد در برابر کلیه

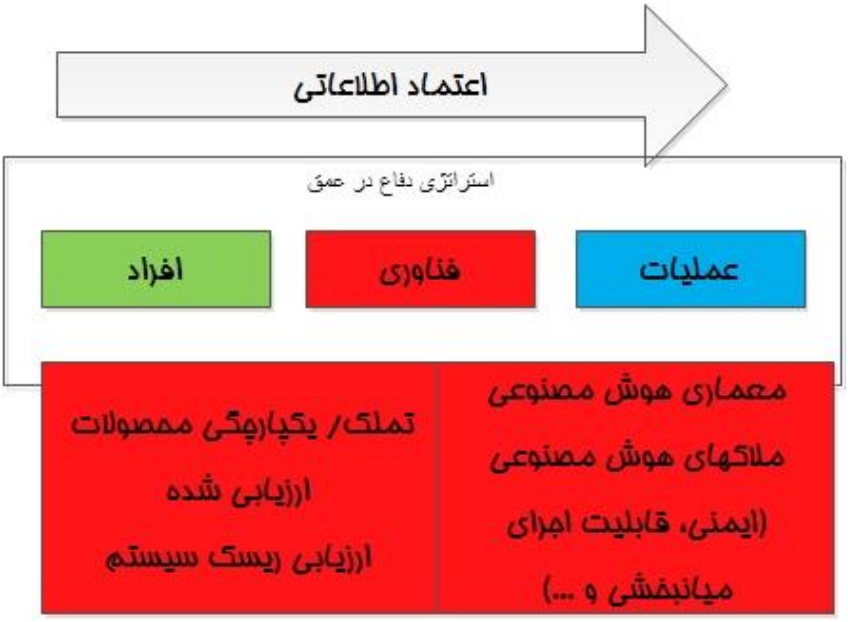
اقدامات خود ملزم به پاسخگویی شوند. این امر همچنین شامل ایجاد سنجه‌های ایمنی فیزیکی و ایمنی بدنی جهت کنترل و رصد دستیابی به تسهیلات و عناصر حیاتی در محیط فناوری اطلاعات نیز می‌شود. شکل شماره‌ی (۲) این عناصر را که با پرسنل در ارتباط است ترسیم نموده است.




**شکل شماره‌ی ۲ - عناصر شکل‌دهنده‌ی بخش افراد**

**فناوری:** ماهیت حملات سایبری یک ماهیت فناورانه است و طبیعتاً در این عرصه فناوری مهم‌ترین عامل تعیین‌کننده‌ی موفقیت و شکست، چه در تهاجم و چه در دفاع برابر تهاجم است. بخش مهمی از این فناوری را دانش ضمنی افراد حاضر در سازمان تشکیل می‌دهند که در بخش پیشین به‌طور خلاصه به آن پرداخته شد. علاوه بر این دانش ضمنی، مجموعه‌ی وسیعی از ابزارهای فناورانه نیز در دسترس قرار دارند که با هدف دفاع در برابر انواع تهاجم‌های پیشرفته طراحی و ساخته می‌شوند. معمولاً سازمان‌ها از ترکیبی از این

ابزارها و دانش افراد استفاده می‌کنند که البته به‌طور معمول سهم ابزارها بسیار بیشتر است و وظیفه‌ی افراد بیشتر کنترل صحت کار ابزارها است. برای اطمینان از این‌که فناوری‌های درستی خریداری شده و استفاده می‌شوند، یک سازمان باید خط‌مشی‌ها و فرآیندهای مؤثری را برای تملک فناوری ایجاد کند. چنین امری شامل این موارد می‌شود: خط‌مشی ایمنی، اصول اعتماد اطلاعاتی، استاندارد و معماری برای اعتماد اطلاعاتی در سطح سیستم، وضع معیارهایی برای محصولات مورد نیاز اعتماد اطلاعاتی، تملک محصولاتی که توسط اشخاص ثالث و بنگاه‌های ارزیابی معتبر تأیید شده‌اند، راهنمای پیکربندی، فرآیندهایی برای ارزیابی ریسک سیستم‌های یکپارچه.




**شکل شماره‌ی ۳ - عناصر شکل‌دهنده‌ی بخش فناوری**

**عملیات:** آخرین جزء اصلی از عناصر تشکیل‌دهنده‌ی راهبرد دفاع در عمق، عملیات است. عملیات در حقیقت اجرای مهارت‌های افراد با استفاده از فناوری برای دستیابی به نتایج مورد انتظار است (زاپریانوف، ۲۰۰۱). در راهبرد دفاع در عمق، کلیه‌ی عملیات‌ها باید کاملاً با

دقت و متکی بر نتایج مشخص و ملموس و قابل سنجش طراحی شوند و باید بر تمام فعالیت‌های مورد نیاز برای حفظ ایمنی سازمان در فعالیت‌های روزمره تمرکز داشته باشند. هدف از عملیات شامل موارد زیر می‌شود:

۱) حفظ خط‌مشی ایمنی سیستم و به روز نگهداشتن آن؛

۲) انجام تغییرات اطمینان‌بخش و اعتبارده بر اساس فناوری اطلاعات. این فرآیندها (که به اختصار فرآیندهای C&A خوانده می‌شوند)، باید داده‌هایی را برای حمایت از مدیریت خطر بر پایه‌ی تصمیمات فراهم کند. این فرآیندها همچنین باید متوجه این باشند که در محیط به هم مرتبط ارتباطی، خطری که توسط یک نفر پذیرفته می‌شود، بین سایرین نیز تسهیم می‌شود.

۳) مدیریت وضعیت ایمنی فناوری اعتماد اطلاعات (برای مثال، نصب وصله‌های امنیتی و به‌روزرسانی اطلاعات ویروس‌ها، حفظ لیست‌های کنترل دسترسی)؛

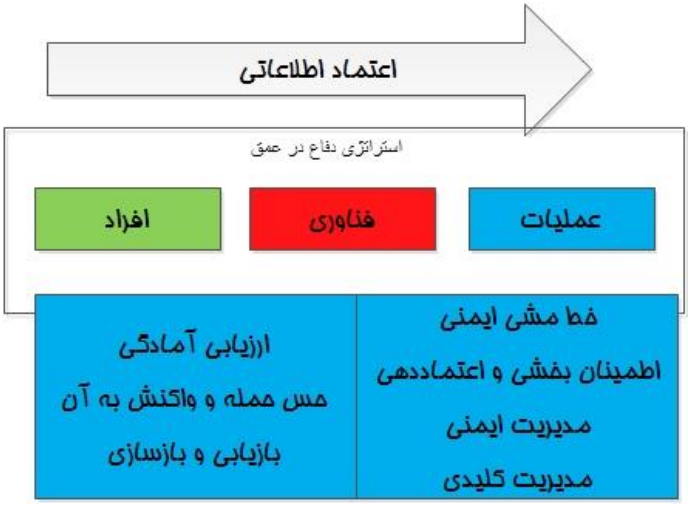
٤) فراهم کردن خدمات مدیریت کلیدی و حفاظت از این زیرساخت سودمند؛

۵) اعمال ارزیابی‌های امنیت سیستم (مثلاً اسکن‌های داوطلبانه) برآورد مستمر میزان آمادگی ایمنی؛

٦) پایش دائمی تهدیدهای کنونی و واکنش نشان دادن به آنها؛

۷) پیش‌بینی حمله‌ها، اخطاردهی و واکنش؛

۸) بازیابی و بازسازی.




**شکل شماره‌ی ٤ - عناصر تشکیل‌دهنده‌ی بخش عملیات**

### اصول راهبرد دفاع در عمق

راهبرد دفاع در عمق اصول چندگانه اعتماد اطلاعاتی را توصیه می‌کند. این اصول عبارتند از:

الف) **دفاع در مکان‌های چندگانه:** با فرض این‌که دشمن می‌تواند چه با استفاده از نفوذی‌های درونی و چه با استفاده از نفوذی‌های بیرونی به یک هدف از نقاط چندگانه حمله کند، یک سازمان نیازمند به‌کارگیری سازوکار حفاظت در مکان‌های چندگانه است، تا بتواند در مقابل همه‌ی طبقه‌های حمله‌ها مقاومت کند. در حداقل شرایط، نواحی تمرکز چندگانه‌ی دفاعی، باید شرایط زیر را داشته باشند:

- دفاع از شبکه‌ها و زیرساخت‌های آن، که خود شامل حفاظت از شبکه‌های ارتباطی محلی و گسترده از یک‌سو و فراهم کردن شرایط امنیت و حفاظت مطمئن و یکپارچه برای انتقال داده‌ها از طریق این شبکه‌ها از سوی دیگر می‌شود.
- دفاع از مرزهای محاصره شده (مثلاً از طریق استفاده از دیواره‌های آتش و جستجوی نفوذهای غیرقانونی برای مقاومت در برابر حمله‌های شبکه‌ای).

- دفاع از محیط پردازش (برای مثال ارائه‌ی کنترل‌های دسترسی بر میزبان‌ها و سِرورها برای مقاومت در برابر نفوذها و حمله‌های مداخله‌گرانه).

ب) **دفاع لایه‌بندی شده:** حتی بهترین محصولات مطمئن اطلاعاتی نیز دارای ضعف‌هایی هستند. از این رو، صرفاً موضوع زمان مورد نیاز برای نفوذ به سیستم توسط دشمن موردی است که باید مورد توجه قرار گیرد. یک ضد سنجه‌ی مؤثر استفاده از سازوکارهای دفاع چندگانه میان دشمن و اهداف آن است. هر یک از این سازوکارها باید موانع منحصر به فردی را در برابر دشمن قرار دهند. علاوه بر این، هر یک از آنها باید شامل هر دو سنجه‌ی «حفاظت» و «جستجو» نیز باشند. این امر خطر کشف شدن را برای دشمن افزایش می‌دهد و هم‌زمان شانس موفقیت آن را برای نفوذ کاهش می‌دهد. استفاده از «دیواره‌های آتش تودرتو»[1] در مرزهای درونی و بیرونی شبکه که هر یک با یک ابزار جستجوی نفوذ توأم شده باشند، نمونه‌ای از دفاع لایه‌بندی شده است. دیواره‌های آتش داخلی می‌تواند کنترل و غربال داده‌ها را به‌طور ریزتر و دقیق‌تری انجام دهد.

**جدول شماره‌ی ۱ - نمونه‌هایی از دفاع لایه‌ای**

| طبقه حمله | خط اول دفاعی | خط دوم دفاعی |
|---|---|---|
| انفعالی | رمزگذاری لایه‌های شبکه و اتصال‌ها و ایمنی در ایمنی گردش اطلاعات | نرم‌افزارهای ایمنی‌بخش |
| فعال | دفاع از مرزهای محاصره شده | دفاع از محیط پردازش |
| حمله به عامل درونی | ایمنی فیزیکی و افراد | محدودسازی دسترسی‌ها، کنترل و نظارت |
| تقارب | ایمنی فیزیکی و افراد | سنجه‌های تجسس فنی |
| ایجاد مداخله | توسعه و توزیع نرم‌افزارهای امن | اجرای کنترل یکپارچگی زمانی |

ج) مشخص نمودن میزان نیرومندی ایمنی (قوت و اطمینان از آن) برای هر عنصر دخیل در امر اعتماد اطلاعاتی به عنوان عملکرد ارزشمند از آن‌چه از آن محافظت می‌شود.

1- Nested Firewalls

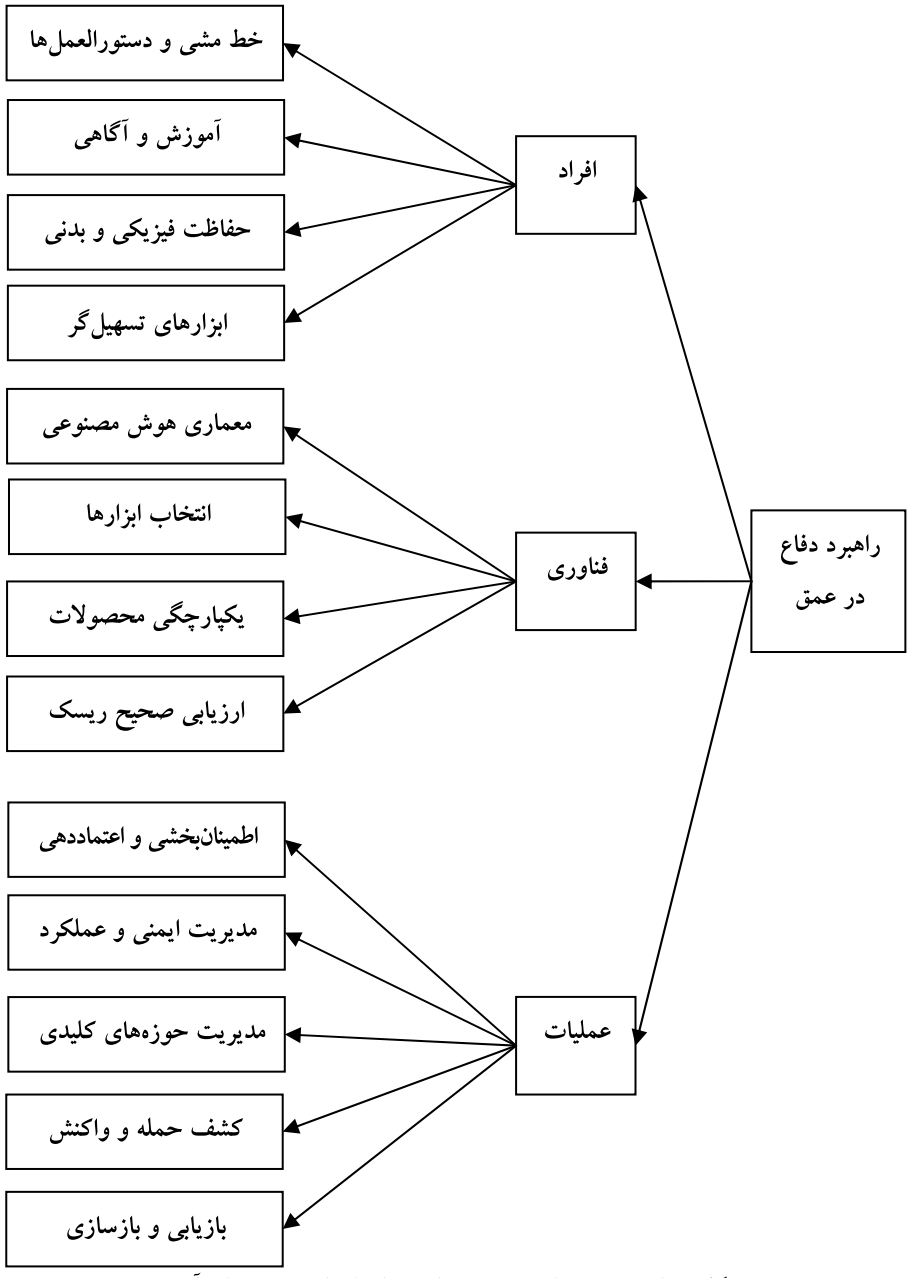
برای مثال، معمولاً اثربخش و به‌طور عملیاتی سودمند است که سازوکار قوی‌تری را در شبکه‌ها نسبت به رایانه‌های شخصی به‌کار گیریم.

د) استفاده از تقویت مدیریت کلیدی و زیرساخت‌های عمومی کلیدی که تمام فناوری‌های یکپارچه شده اعتماد اطلاعاتی را پشتیبانی کند و به شدت در برابر حملات مقاوم باشند. این نکته‌ی پایانی تشخیص می‌دهد که این زیرساخت‌ها می‌توانند اهداف سودمندی باشند یا نه.

ه) استفاده از زیربناها برای جستجوی نفوذ و تحلیل کردن و همبستگی نتایج و واکنش متناسب. این زیربناها باید به کارکنان بخش «عملیات» کمک کنند تا به پرسش‌هایی پاسخ دهند؛ همچون: آیا تحت حمله قرار گرفته‌ام؟ چه کسی منبع حمله است؟ هدف چیست؟ چه کس دیگری در خطر حمله است؟ چه گزینه‌هایی در دسترس است؟ و ....

**نتیجه‌گیری و ارائه‌ی چارچوب**

همان‌طور که بیان گردید هدف از انجام این پژوهش ارائه‌ی چارچوبی برای پژوهش‌های آینده در زمینه‌ی امنیت سایبری و دفاع در برابر تهاجم‌های سایبری به سیستم‌های اطلاعاتی کشور می‌باشد. این چارچوب به عنوان دستاورد این پژوهش به پژوهشگران آتی ارائه می‌گردد تا در شناسایی، توصیف و اندازه‌گیری عوامل مؤثر در افزایش ایمنی سیستم‌های دفاعی از آن استفاده نمایند و پژوهش‌های کاربردی خود را حول آن متمرکز کنند. در نتیجه انجام این پژوهش نظری، چارچوبی معرفی گردید که در آن سه مؤلفه‌ی اساسی افراد، فناوری و عملیات را تشکیل شده از اجزا وعوامل دیگری ارائه نمودیم:




شکل شماره‌ی ۵ - چارچوب پیشنهادی برای انجام پژوهش‌های آتی

امید است کـه ایـن چـارچوب، در پـژوهش‌هـای آتـی مـورد توجـه محققـان حـوزه‌ی سیاست‌های دفاعی قرار گیرد و با اسـتفاده از آن بـه‌عنـوان چـارچوب مفهـومی پـژوهش، بـه اندازه‌گیری عملکرد و تأثیر کنونی و نیز سطح ایده‌آل هر یک از این عوامل و عناصر در سـپهر دفاعی کشور اقدام کنند. آنچه در این پژوهش ارائه شد بسترسازی برای انجام دانش‌افزایی‌های آینده در زمینه‌ی حوزه‌ی مطالعه بوده است و نه ارائه یافته‌های کاربردی. این وظیفـه بـر عهـده پژوهشگران آینده قرار می‌گیرد که با انجام مطالعات کـاربردی و توسـعه‌ای نسـبت بـه ارائـه‌ی نتایج کاربردی اقدام نمایند.

آن‌چه شایان توجه است، اهمیت داشتن نگاه متوازن به عناصر گوناگون دخیل در طراحی سامانه‌های دفاعی در قالب راهبرد است. راهبرد دفاع در عمق اگر چه ماهیتاً یک پدیده‌ی فنـی است که عمدتاً در حوزه‌ی معماری شبکه و اطلاعـات قـرار دارد، امـا عـدم توجـه در سـطح مدیریت ارشد و در قبال سازمان، سبب تنزل آن به صرفاً سطح فنـاوری مـی‌شـود و در نتیجـه سبب می‌شود که اعتماد اطلاعاتی که هدف اصلی از طراحی و اجرای این راهبرد است حاصل نشود. بی‌شک توجه متوازن به افراد، فناوری و عملیات در چارچوب نگاه منسجم برای کسـب اعتماد اطلاعاتی، زیربنایی قابل اعتماد برای انجام به‌روزرسانی‌ها و نوسازی‌های فنـی در برابـر حملات سایبری آینده ایجاد خواهد کرد که یقیناً در آینده تعداد آنهـا در سـطح جهـان فزونـی خواهد یافت. طراحی سیستم دفاعی کشور، بی‌نیاز از سیاست‌های دفاعی در عرصه‌ی فنـاوری نیست و از این رو، انجام پژوهش‌های بنیادین در حوزه‌ی هم‌پوشانی سیاست‌ها بـا سیسـتم‌هـا می‌تواند نقش مهمی در امنیت اطلاعاتی و دفاعی کشور داشته باشد.

## منابع

### انگلیسی


1- Armistead, Edwin L. (2004), "***Information Operations: Warfare and the Hard Reality of Soft Power***" (Issues in Twenty-First Century Warfare), Potomac Books Inc.

2- Blyth, Andrew and Kovacich, Gerald (2006), "***Information Assurance; security in the information environment***", Second Edition, Springer.

3- Department of Defense Information Technology (2011), "***Enterprise Strategy and Roadmap***", Version 1.0 – 06 September.

4- Fornäs, Johan, Becker, Karin, Bjurström, Erling, Ganetz, Hillevi (2007), "***Consuming Media;Communication,Shopping and Everyday Life***", Berg Publications, Oxford.

5- Hazlewood, Victor (2006), "***Defense-In-Depth; An Information Assurance Strategy for the Enterprise***", San Diego Supercomputer Center, Security Technologies.

6- Li, C., & Bernoff, J. (2008). "***Groundswell: Winning in a world transformed by social technologies***", Boston: Harvard Business Press.

7- Maconachy, W. Victor, Schou, Corey D., Ragsdale, Daniel and Welch, Don (2001), "***A Model for Information Assurance: An Integrated Approach***", Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, NY.

8- National Security Agency (2002), "***Defense in Depth; a practical strategy for achieving Information Assurance in today's highly networked environments***".

9- U.S Departement of Defense (2012), "***Information Assurance Workforce Improvement Program***", Incorporating Change 3, January 24, 2012. The document

by Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer.

10- Rothwell, J. Dan (2010). "***In the company of others : an introduction to communication***" (3rd ed. ed.). New York: Oxford University Press.

11- Sun, Wanning (2010), "***Mission Impossible? Soft Power, Communication Capacity, and the Globalization of Chinese Media***", International Journal of Communication 4.

12- Zaprianov, Atanas (2001), "***IT-related Challenges Facing the Bulgarian Armed Forces and Their Performance Related Impact***", Information & Security. Volume 6.