مجله سیاست دفاعی

نشریه مرکز مطالعات دفاعی و امنیت ملی، دانشگاه جامع امام حسین(ع)

سال بیستم، شماره‌ی ۳، تابستان ۱۳۹۱، شماره پیاپی ۷۹ **(شماره استاندارد بین‌المللی ۵۰۸۷-۱۰۲۵)**

صاحب امتیاز: دانشگاه جامع امام حسین(ع)، مرکز مطالعات دفاعی و امنیت ملی

مدیر مسئول: علیرضا فرشچی

سردبیر: دکتر سید یحیی صفوی

دبیر تحریریه و مدیر داخلی: علی قنبرزاده

حروف‌چینی و صفحه‌آرایی: محمد حسین سعادت

ناظر چاپ: اندیشگاه علم و صنعت جهان معاصر

لیتوگرافی، چاپ و صحافی: انتشارات شکیب

قیمت: ۵۰,۰۰۰ ریال

قیمت لوح فشرده: ۲۵,۰۰۰

نشانی: دانشگاه جامع امام حسین(ع) ـ مرکز مطالعات دفاعی و امنیت ملی

شماره تماس مستقیم: ۷۷۱۰۵۷۶۵

دورنگار: ۷۷۱۰۵۷۴۷

نشانی پستی: تهران ـ صندوق پستی ۳۴۵۹-۱۶۷۶۵

مرکز فروش: تهران ـ بزرگراه شهید بابایی ـ بعد از پل لشکرک ـ دانشگاه جامع امام حسین(ع) ساختمان شهید بروجردی ـ طبقه دوم ـ مرکز مطالعات دفاعی و امنیت ملی

شماره تماس: ۲ ـ ۷۷۱۰۵۷۴۱

درجه علمی مجله سیاست دفاعی، طبق نامه شماره ۳/۴۴۲۸۶ و مورخ ۱۳۹۱/۰۲/۳۰ کمیسیون بررسی نشریات علمی کشور، به عنوان نشریه علمی ـ پژوهشی، مورد تأیید قرار گرفته است.

هیأت تحریریه، مشاوران علمی و داوران مجله سیاست دفاعی

(به ترتیب حروف الفبا)

هیأت تحریریه

هیأت داوران

مشاوران علمی

شرایط تدوین و ارسال مقاله‌های علمی ـ پژوهشی برای چاپ در مجله سیاست دفاعی

پژوهشگران گرامی لطفاً هنگام ارسال مقالات به نکات زیر توجه فرمایید:

الف) ملاحظات کلی

۱ ـ مقالات فقط مربوط به حوزه‌های دفاعی، امنیت ملی و امنیت بین‌المللی و در سطوح راهبردی و عملیاتی باشند.

۲ ـ مقاله باید تحقیقی و حاصل کار پژوهشی نویسنده یا نویسندگان باشد. مقالات مروری از نویسندگان صاحب‌نظر و حائز اثرات و مقالات پژوهشی در زمینه مورد بحث، به شرطی پذیرفته می‌شود که منابع معتبر و متنابهی، مستند تحقیق قرار گرفته باشد.

۳ ـ مقاله ارسالی نباید قبلاً یا همزمان برای چاپ یا ارائه به نشریات دیگر و یا همایش‌ها ارسال شده باشد.

٤ ـ نام نویسنده یا نویسندگان همراه با رتبه علمی، محل اشتغال و نشانی کامل و تلفن تماس همراه مقاله باشد.

۵ ـ نشانی کامل نویسنده عهده‌دار مکاتبات: شامل نشانی پستی، شماره تلفن، شماره دورنگار و نشانی پیام‌نگار (E-Mail) به فارسی و انگلیسی.

۷ ـ چنانچه مخارج مالی تحقیق یا تهیه مقاله توسط مؤسسه‌ای تأمین شده باشد باید نام مؤسسه در صفحه اول درج شود.

ب) ساختار و شکل ارائه مقاله

۱ ـ رعایت ساختار پیشنهادی الزامی است: عنوان، چکیده (حداکثر ۸ سطر)، کلید واژه (حداکثر ۵ واژه)، مقدمه (دربرگیرنده بیان مسئله و ضرورت، سؤال یا فرضیه و روش تحقیق)، چارچوب نظری (تحلیلی)، داده‌ها و مباحث تفصیلی تحقیق، نتیجه‌گیری، چکیده انگلیسی (حداکثر ۲۵۰ کلمه)، کلید واژه انگلیسی (حداکثر ۵ کلمه)، فهرست منابع (منابع لزوماً باید در متن مقاله استفاده شده باشد).

۲ ـ تیترهای اول، دوم و سوم به ترتیب با فونت‌های B Zar Bold ۱۱، ۱۰، ۹ مشخص شده باشد.

۳ ـ متن مقاله حداکثر در ۲۵ صفحه با نرم‌افزار Word 2003 به بالا و قلم B Lotus و فونت ۱۲ و متن انگلیسی با Calibri 10 آماده و ارسال گردد.

٤ ـ مقاله باید سلیس و روان و بدون هیچ‌گونه غلط املایی نگارش یابد و از آوردن اصطلاحات خارجی که معادل دقیق و ابلاغ شده فارسی دارد، خودداری گردد. معادل خارجی اسامی و اصطلاحات خارجی در پانوشت به صورت اتوماتیک آورده شود و در هر صفحه به طور مستقل شماره‌گذاری گردد.

۵ ـ نمودارها، جداول و اشکال با یکی از نرم‌افزارهای Office به زبان فارسی و در اندازه‌های ۱۲×۸ یا ۱۲×۱٦ طراحی شود و اختصارات آنها در پانوشت توضیح داده شود. نمودارها، جداول و اشکال باید دارای شماره‌های متوالی باشند و بدون نیاز به مراجعه به توضیحات متن گویا باشند.

٦ ـ تیتر عناوین و نوع قلم مربوط مطابق جدول شماره ۱ که در انتهای این راهنما خواهد آمد، می‌باشد.

ج) روش ارجاع به منابع

۱ ـ در متن

۱-۱ ـ مأخذ در متن مقاله داخل کمان به صورت (نام‌خانوادگی، سال انتشار: شماره صفحه)؛ مانند (متقی‌زاده، ۱۳۸۱: ۲۵)؛ (Smith, 1990: 23)

۱-۲ ـ اشاره به منابع دارای چند نویسنده به صورت (نویسنده و همکاران، سال انتشار، شماره صفحه) مانند (متقی‌زاده و همکاران، ۱۳۸۹: ۱۸)؛ (Smith, etal, 2004: 8)

۱-۳ ـ اشاره به آدرس‌های اینترنتی به صورت (نام‌خانوادگی نویسنده / نام مرجع تدوین‌کننده، سال)

۱-۴ ـ در تمامی منابع اگر نویسنده دارای دو یا چند منبع در یک سال باشد، پس از ذکر سال لازم است فصل یا ماه نشر اثر آورده شود، مانند (احمدی، پاییز ۱۳۸۸) و (احمدی، بهار ۱۳۸۸)؛ (Digman, Apr 1999) و (Digman, Jan 1999)

۲ ـ در پایان مقاله

فهرست منابع در پایان مقاله به ترتیب حروف الفبا به صورت زیر آورده شود:

۲-۱ ـ کتاب تألیفی: نام‌خانوادگی، نام (سال انتشار)، عنوان کتاب، محل نشر، نام ناشر.

۲-۲ ـ کتاب ترجمه‌ای: نام‌خانوادگی، نام (سال انتشار)، عنوان کتاب، نام مترجم، محل نشر، نام ناشر.

۲-۳ ـ مقاله: نام‌خانوادگی، نام، «عنوان مقاله»، نام مجله، دوره، شماره، شماره صفحات (ابتدا و انتهای مقاله)، سال نشر.

۲-٤ ـ آدرس اینترنتی: نام‌خانوادگی، نام و نویسنده و نویسندگان / مرجع تدوین‌کننده، عنوان مطلب، آدرس صفحه اینترنتی، تاریخ بارگذاری، تاریخ مشاهده.

د) تذکرات

۱ ـ آرا و دیدگاه‌های ارائه شده در مقالات الزاماً بیانگر نظر و دیدگاه مجله نیست.

۲ ـ مسئولیت ناشی از صحت علمی یا دیدگاه‌ها و ارجاعات مندرج در مقاله به عهده نویسنده یا نویسندگان است.

۳ ـ مجله حق رد یا قبول و نیز ویراستاری مقالات را برای خود محفوظ می‌دارد و از بازگرداندن مقالات رد شده معذور است.

٤ ـ دریافت مقاله از سوی مجله الزاماً به معنای پذیرش قطعی آن برای چاپ نیست.

جدول شماره‌ی ۱

عنوان	نوع قلم	عنوان	نوع قلم
عنوان مقاله با تیتر ۱	B Zar 11 Bold	متن چکیده و کلیدواژگان	B Lotus 10 Italic
عنوان چکیده، کلید واژگان، مقدمه و ...، نتیجه‌گیری (تیتر ۲)	B Zar 10 Bold	متن پانویس فارسی	B Lotus 9
عناوین فرعی زیرمجموعه‌ی تیتر ۲ با تیتر ۳	B Zar 9 Bold	متن پانویس انگلیسی مانند:	Calibri 8
عناوین فرعی زیرمجموعه تیتر ۳ با تیتر ۴	B Lotus 11 Bold	متن مقاله	B Lotus 12
تیتر جدول‌ها، نمودارها و عکس‌ها (تیتر جدول‌ها و نمودارها باید بالای آن‌ها و تیتر شکل‌ها پایین آن‌ها و در وسط ذکر شود.)	B Lotus 10 Bold	ارجاعات منابع داخل متن به فارسی مانند: (متقی‌زاده، ۱۳۸۱: ۲۵)	B Lotus 10
		ارجاعات منابع داخل متن به انگلیسی مانند: (Smith, 1990: 23)	Calibri 9

فهرست مطالب

مجله سیاست دفاعی، سال بیستم، شماره ۷۹، تابستان ۱۳۹۱

عنوان **صفحه**

مقاله‌ها

چکیده انگلیسی

سخن سردبیر

امروزه فناوری اطلاعات در زمره‌ی مهمترین عوامل ایجادکننده‌ی قدرت دفاعی و امنیتی مطرح است و نقش محوری آن در ارتقا و بهبود قابلیت‌های نظامی را نمی‌توان نادیده گرفت. اکثر نیروهای نظامی و شبه‌نظامی به‌دنبال مسلح شدن به این سلاح راهبردی هستند و شناخت و بررسی ابعاد اثرگذاری فناوری اطلاعات بر این فضا در محورهای انسانی، اطلاعاتی و فناورانه، به‌عنوان ضرورتی برای آینده سیاسی و نظامی هر کشور مطرح می‌باشد. به‌واقع، هر فعالیت پیچیده‌ای که در آن نیاز به هماهنگ‌سازی اقدامات و منابع متعدد باشد، مستلزم اطلاعات است و در صحنه‌ی نبرد و اقتدار دفاعی نیز همین شرایط حاکم است؛ اجرای موفق یک عملیات نظامی، نیازمند اطلاع از اهداف عملیات، روش دستیابی به آنها، قابلیت‌ها و فعالیت‌های دشمن، شرایط آب و هوایی و منطقه، میزان محرمانگی عملیات، ظرفیت نیروها و سایر عواملی است که ممکن است هر لحظه تغییر کنند.

تا چندی پیش، نیروهای نظامی برای تقویت قابلیت‌های خود از فناوری اطلاعات بهره می‌گرفتند؛ اما همان‌گونه که فناوری اطلاعات و قابلیت‌های آن موجب تغییر رویه‌ها در سازمان‌های غیرنظامی گردیده، تغییر روش‌های کاری در سازمان‌ها و ساختارهای دفاعی و نظامی را نیز به دنبال داشته و دارد. برای نمونه، رابطه‌ی معکوس فاصله و دقت (و در نتیجه مرگبار بودن) به واسطه‌ی فناوری اطلاعات در حال از میان رفتن است و سلاح‌های قدرتمند با کمک فناوری‌های شناسایی و تعقیب واحدهای دشمن، به تخریب سریع و سیستماتیک نیروهای متخاصم و زیرساخت‌های نظامی آنها منجر می‌شوند. به دنبال انقلاب اطلاعاتی و تأثیر آن روی نحوه‌ی عملیات و نیروهای نظامی، معیارهای ارزیابی قدرت نظامی و امنیتی نیز متحول گردیده است. اندازه و تعدد منابع اهمیت سابق را ندارند و عملکرد نیروها به‌کمک قابلیت‌های فناوری اطلاعات بهبود یافته است، اما باید توجه داشت، این قابلیت، زمانی ارزشمندتر است که به‌صورت هماهنگ با سایر سلاح‌ها عمل کند.

توسعه‌ی فناوری اطلاعات و ارتباطات ما را قادر ساخته است تا نیروها، سلاح‌ها و سیستم‌های فرماندهی را در قالبی یکپارچه درآورده و برآیند کل را به چیزی بیشتر از مجموع عملکرد هر یک از این موارد ارتقا دهیم. استفاده یکپارچه و هماهنگ از کلیه‌ی منابع و امکانات، منجر به تقویت توانمندی نیروهای نظامی در انجام فعالیت‌های کنترل، ارتباطات، پردازش، فرماندهی، دیده‌بانی و شناسایی، در صحنه‌ی نبرد یا عرصه رقابت می‌شود. در همین خصوص، فناوری اطلاعات امکان جنگ مشترک را فراهم می‌کند که می‌تواند مزیت عظیمی به‌شمار می‌رود. به‌جای حمل سلاح‌های مختلف از طریق زمین، هوا و دریا به‌صورت جداگانه، نیروهای دخیل در نبرد مشترک می‌توانند به‌صورت یکپارچه اقدام به اجرای عملیات هماهنگ نمایند و این امکان بالقوه وجود دارد که هریک از قابلیت‌های نیروهای مشترک، بنابر اولویت، با اجزای مختلف ارتش دشمن مقابله نمایند. با تجمیع قابلیت‌های مختلف نظامیان شرکت‌کننده در نبرد مشترک، اقبال رقیب برای دفاع از نیروها و مواضع خود به حداقل می‌رسد.

در مجموع، به‌کارگیری فناوری اطلاعات در عرصه‌های دفاعی و امنیتی، گسترش میدان جنگ ماورای مرزها و حدود سنتی آن را سبب شده است. در گذشته ارتش‌ها، با سلاح‌های نظامی به اهداف نظامی حمله می‌کردند؛ اما امروزه با توجه به قابلیت‌های فناوری اطلاعات، همه‌ی منابع و فرآیندهای اطلاعاتی یک ملت می‌توانند در زمره‌ی سلاح و اهداف بالقوه جنگی به‌شمار روند. از این‌رو؛ شناخت دقیق نحوه و اثرات به‌کارگیری فناوری اطلاعات در فضای رزم جهت مقابله با تهدیدات ناشی از آن، همچنین لزوم به‌کارگیری قابلیت‌های فناوری اطلاعات در حوزه‌ی دفاعی کشور و تجهیز سازمان‌های دفاعی و امنیتی به آخرین نتایج نظری و دستاوردهای فناوری جهانی در این زمینه، جهت بهره‌برداری از فرصت‌ها، می‌بایست در فهرست اولویت‌های مطالعاتی و پژوهشی هر یک از سیاست‌گذاران، صاحب‌نظران، دست‌اندرکاران و دانشجویان این حوزه قرار گیرد و نشریه‌ی سیاست دفاعی در این شماره کوشیده است تا با ارائه‌ی نمونه‌هایی از ابعاد علمی و عملی این مهم، گامی هرچند ناچیز در این مسیر برداشته باشد.

دکتر سیدیحیی صفوی
تابستان ۱۳۹۱
دانشگاه جامع امام حسین (ع)

مجله سیاست دفاعی
سال بیستم، شماره ۷۹، تابستان ۱۳۹۱

محاسبات ابری؛ رویکردی نوین در معماری فضای اطلاعاتی

تاریخ دریافت مقاله: ۱۳۹۰/۱۲/۲۰
تاریخ تأیید مقاله: ۱۳۹۱/۰۲/۲۷
صفحات مقاله: ۳۱ - ۹

امین حکیم [۱]
شهریار محمدی [۲]

چکیده:

محاسبات ابری یا پردازش[۳]، توانایی ارائه‌ی منابع و ظرفیت‌های فناوری اطلاعات از طریق اینترنت می‌باشد و رویکرد جدیدی در معماری است که بر این ایده استوار می‌باشد که منابع مبتنی بر اینترنت سریع‌تر، با هزینه کمتر و تنوع بیشتری می‌توانند در اختیار گرفته شوند. به واقع می‌توان گفت؛ محاسبات ابری یک مدل معماری فضای اطلاعاتی است که امکان دسترسی شبکه‌ای - متناسب و مبتنی بر تقاضا- به انبوهی از منابع محاسباتی (رایانشی) مشترک (مانند شبکه‌ها، سرورها، بانک‌های اطلاعاتی، برنامه‌های کاربردی و سرویس‌ها) را با هزینه‌های بسیار پائین، نوآوری و قابلیت توسعه‌ی بسیار بالا همچنین بدون محدودیت زمانی و مکانی، فراهم می‌کند و بر این اساس، قابلیت‌هایی را ارائه می‌دهد که محاسبات ابری را به رویکردی راهبردی تبدیل کرده است. از این منظر، امنیت و تبادل اطلاعات از یک‌سو با فرصت‌های رشد و از سویی دیگر با چالش‌های جدیدی روبه‌رو می‌شوند. در نتیجه، با توجه به ضرورت و اهمیت موضوع همچنین ویژگی‌های این نوع از معماری (استفاده از ابرها، شبکه‌ها و مراکز مختلف، همچنین ترکیب و تطبیق سرویس‌های گوناگون و تناسب دامنه و سرعت و امنیت دستیابی به اطلاعات)، محور اصلی مطالب مقاله‌ی حاضر پرداختن به این شیوه‌ی نوین معماری از منظر سازمان‌های اطلاعاتی می‌باشد.

* * * * *

۱- پژوهشگر مرکز مطالعات دفاعی و امنیت ملی، گروه مدیریت فناوری اطلاعات (IT)، دانشکده مدیریت، دانشگاه تهران.
۲- استادیار گروه مدیریت فناوری اطلاعات (IT)، دانشکده مهندسی صنایع، دانشگاه صنعتی خواجه نصیرالدین طوسی.
3 – Cloud Computing

واژگان کلیدی

محاسبات ابری، فضای سایبر، فناوری اطلاعات، معماری اطلاعاتی، سازمان‌های اطلاعاتی.

مقدمه

ابر، تصویری است انتزاعی از شبکه‌ای عظیم و توده‌ای که حجم آن مشخص نبوده و نمی‌دانیم از چه میزان منابع پردازشی تشکیل شده است. ابعاد زمانی و مکانی یکایک اجزای آن نیز دانسته نیست؛ به واقع، نمی‌دانیم سخت‌افزارها و نرم‌افزارها در کجای این توده قرار دارند، اما آنچه را که عرضه می‌کند، می‌شناسیم. در محاسبات ابری سازمان‌ها و افراد، برای نرم‌افزار، سخت‌افزار یا شبکه، هزینه‌ای پرداخت نمی‌کنند؛ بلکه توان پردازشی و سرویس‌های[1] نرم‌افزاری مورد نیاز خود را خریداری می‌کنند. سیستم ابری، در ساده‌ترین تعریف؛ ارائه‌ی خدمات رایانه‌ای روی اینترنت است. به جای هزینه کردن در تأسیسات و امکانات فناوری اطلاعات به منظور نگهداری داده‌ها یا تهیه نرم‌افزار، از امکانات سازمان‌های دیگر استفاده کرده و پردازش خود را با استفاده خدمات و بهره‌گیری از امکانات آنها انجام می‌دهند. در واقع برخی از سازمان‌ها، زیرساخت‌های خاصی درست می‌کنند که این امکانات را در اختیار دیگران قرار می‌دهند.

در چند سال آینده، محاسبه‌ی ابری یک مفهوم پیشتاز و فراگیر خواهد بود که فرصت‌های جدیدی برای استفاده بهتر و کارآمدتر از منابع ارائه خواهند کرد. به‌طور مثال، شبکه‌ی ماهواره‌ای «اشلون»[2] که وظیفه‌ی جمع‌آوری و پردازش اطلاعات ماهواره‌ای از

1 - Services

۲ - اشلون (Echelon) نام یک شبکه‌ی اطلاعاتی جهانی می‌باشد که آژانس امنیت ملی امریکا (National Security Agency) آن را طراحی کرده است. البته علاوه بر آژانس امنیت ملی امریکا، سازمان‌هایی همچون؛ ستاد ارتباطات کل انگلیس، مقر امنیتی ارتباطات کانادا، ریاست امنیت دفاعی استرالیا و دایره‌ی امنیت ارتباطات کل نیوزلند، نیز در مدیریت و کنترل این شبکه سهیم می‌باشند که پوشش مناطق جغرافیایی مختلف در سرتاسر دنیا بین این کشورها تقسیم شده است، به‌طوری که امریکا در بخش قاره امریکا، انگلیس در بخش‌های اروپا، افریقا و غرب روسیه، استرالیا در بخش‌های آسیای جنوب شرقی، جنوب غربی اقیانوسیه و مناطق شرقی اقیانوس هند، نیوزلند در بخش شرکت‌های غربی اقیانوس آرام و کانادا نیز در بخش‌های شمال روسیه، اروپای شمالی و همچنین امریکا، فعالیت می‌کنند. این شبکه متشکل از ۱۲۰ ماهواره‌ی ارتباطاتی، اکتشافی و نظارتی می‌باشد که علاوه بر این ماهواره‌ها، تعداد بسیار زیادی گیرنده‌های زمینی نیز در نقاط مختلف دنیا نصب شده است تا نقاط کور ماهواره‌ها را پوشش دهند.

بخش‌های مختلف (مخابرات، اینترنت، بانک‌های اطلاعاتی و ...) به اشکال مختلف (متن، صوت، تصویر و ...) را در سطح جهان برای کشورهای ذی‌نفع به عهده دارد، یا شبکه‌ی اطلاعاتی اتحادیه‌ی اروپا که وظیفه‌ی جمع‌آوری، تحلیل، پردازش، تفکیک و انتشار اطلاعات در سطح کشورهای عضو از طریق به‌کارگیری قابلیت‌ها و کاربردهای مختلف از جمله، به اشتراک گذاشتن اطلاعات شهروندان برای دولت‌های عضو اتحادیه را بر عهده دارد، نمونه‌ای از قابلیت‌های فناوری اطلاعات می‌باشند که اطلاعات مورد اشاره را به وسیله‌ی ابزارهای مختلف (ماهواره‌ها، پایانه‌های سمعی و بصری و ...) و از منابع متعدد (بانک‌های اطلاعاتی فرودگاه‌ها، مراکز خرید و ...) جمع‌آوری نموده و به صورت برخط[1]، با حفظ سطوح دسترسی در قالب‌های مناسب در اختیار متقاضیان قرار می‌دهد (حکیم، ۱۳۸۹).

به‌منظور بررسی این مفاهیم و معرفی قابلیت‌های محاسبات ابری در پوشش نیازهای نیروهای امنیتی، این مقاله در سه بخش تهیه شده است. قسمت اول به بررسی مفهوم، عملکرد و ابعاد محاسبات ابری پرداخته است و سعی دارد تا دیدی مناسب به این مفاهیم را ایجاد نماید. قسمت دوم به بررسی نیازهای سازمان‌های اطلاعاتی و نقش محاسبات ابری در این زمینه می‌پردازد. در این راستا نیازها، حساسیت‌ها و نحوه‌ی نقش‌آفرینی محاسبات ابری مورد بررسی قرار گرفته است. در نهایت، با یک جمع‌بندی و مرور نیازها و دغدغه‌های کنونی این مقاله به پایان می‌رسد.

اهمیت و اهداف تحقیق

استفاده از پیشرفت‌های فناوری، به روز بودن، حفظ یکپارچگی، توزیع منابع و کاهش هزینه‌ها همواره از اولویت‌های مدیران ارشد و برنامه‌ریزان بوده است. در مقابل این خواسته، امنیت اطلاعات و ارتقای سطح امنیتی متناسب با پیشرفت‌های فناوری، چالش اصلی در این

بسترهای این شبکه که در سال‌های جنگ سرد ایجاد شده بود، مخصوص نظارت بر اتحاد جماهیر شوروی، کشورهای عضو پیمان ورشو و دولت‌هایی بود که به اردوگاه سوسیالیستی گرایش داشتند، اما امکانات آن به کسب اطلاعات نظامی و امنیتی منحصر نمی‌باشد، بلکه قابلیت پوشش اطلاعات سیاسی، اقتصادی، صنعتی، سازمان‌ها و افراد را نیز دارا است.

1 - Online

راه بـوده و تعیـین یـک نقطـه‌ی تعـادل بـین ایـن دو خواسـته همـواره یـک پـارادوکس در برنامه‌ریزی‌های توسعه‌ی سیستم‌های اطلاعاتی بوده است. محاسبات ابری نیز از این چالش بـه دور نبوده و همواره محل بحث و اختلاف نظر بوده است.

این مسـأله در مجموعـه‌هـای نظـامی/امنیتـی شـکل مهـم‌تـری بـه خـود گرفتـه اسـت. کوچک‌سازی حجم رایانه‌های همراه نیرو (در زمین و هوا) به کاهش قابلیـت ذخیـره‌سـازی و پردازشی رایانه‌ها منتهی می‌شود. ارتقای یکپارچگی تبادل اطلاعات اولویتی دیگر در صـحنه‌ی نبرد است. هزینه‌های ناشی از محاسبات/تحلیل‌های نادرست و یا بـا تـأخیر، و همچنـین نبـود یکپارچگی در اغلب موارد غیر قابل جبران می‌باشـد. ابرهـای محاسـباتی یـا همـان رایـانش و پردازش، پاسخی نوین به این نکات بوده و از طریق در اختیار گذاشـتن داده و سـرویس‌هـای تحلیلی/محاسباتی می‌توانند ضعف‌های محاسباتی/ ذخیره‌سازی رایانه‌هـای نیروهـا را برطـرف نموده و بر یک بستر اطلاعاتی یکپارچه، انسجام تبادل اطلاعات در بین سطوح مختلف نیروها را بالا ببرند.

از سویی دیگر، حفظ امنیت در تبادل اطلاعات نیازی مبرم و اولـویتی حیـاتی اسـت کـه می‌تواند باعث کم‌رنگ شدن مزایای استفاده از ابرهای اطلاعاتی شود. مزایای اسـتفاده از ابرهـا به قدری بالا است که نیروهای اطلاعاتی و نظامی را وادار سازد تا بـا یـافتن راه‌حلـی مناسـب برای مشکل امنیت، از قابلیت‌های بالای ابرها بهره ببرند. بحث بر روی مشکل و نحوه‌ی بهـره جستن از ابر خواستگاه اصلی این تحقیق بوده و در این پژوهش سعی بر آن است تا به معرفـی این پارادوکس پرداخته و راه‌حلی مناسب برای آن ارائه دهند.

بررسی مفهوم محاسبات ابری

محاسبات ابری مجموعه‌ای است از رایانه‌های مجازی که به یکـدیگر متصـل بـوده و شـامل مواردی مانند پردازش، ذخیره‌سازی، پایگاه داده، توسعه‌ی برنامه و سرویس‌های کاربردی را پوشش می‌دهد. ای فضا در خارج از فایروال[1] سازمان بوده و ارتباط مجموعه‌هـا در آن از طریـق اینترنـت

1 - FireWall

میسر می‌باشد. ایده‌ی اساسی در محاسبات ابری هزینه‌ی سرویس بسیار کم نسبت به زمانی است که سخت‌افزار و نرم‌افزارهایی را خود سازمان در اختیار دارد (Brian, et al., 2010).

محاسبات ابری یک مدل پرداخت هزینه در قبال استفاده از خدمات و امکانات است که امکان دسترسی شبکه‌ای مبتنی بر تقاضا را به انبوهی از منابع محاسباتی و رایانشی مشترک (مثل شبکه‌ها، سرورها، ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) موجب می‌شود. این منابع می‌توانند در حداقل زمان فراهم شده و با کمترین تلاش و تعامل با فراهم‌کننده‌ی سرویس، عملیاتی شوند (Grossman, et al., 2009). این رویکرد در دسترس بودن سرویس را ارتقا داده و شامل ۵ ویژگی کلیدی است:

- خویش خدمتی[1] مبتنی بر تقاضا؛
- دسترسی به شبکه در همه جا؛
- منابع مستقل از مکان؛
- انعطاف‌پذیری بالا؛
- پرداخت در قبال استفاده (Marston, et al., 2011) .

به بیان دیگر، محاسبات ابری توانایی ارائه/استفاده از منابع فناوری اطلاعات به واسطه‌ی اینترنت می‌باشد. خدمات شامل سرویس‌های ذخیره‌سازی، سرویس‌های پایگاه داده، سرویس‌های اطلاعاتی، سرویس‌های تست کردن، سرویس‌های امنیتی، سرویس‌های پلتفرم[2] و هر چیز دیگری که شما می‌توانید در مرکز داده‌های امروزی یافت کنید، می‌باشد که از طریق اینترنت به عنوان سرویس ارسال می‌گردد. از بسیاری جهات، محاسبات ابری با جذب سرویس از نرم‌افزارها و سخت‌افزارهایی که از لحاظ مکانی دور هستند، در ارتباط است. بنابراین، سازمان از سرویس استفاده می‌کند و تقریباً هرگز با نیازمندی‌های مرتبط با پلتفرم مانند نگهداری، کنترل، هزینه‌ی سخت‌افزار و فضای مرکز داده روبه‌رو نمی‌شود. به‌طور ساده، در محاسبات ابری،

1 - Self Service
2 - Platform

سرویس‌ها بر مبنای تقاضای ارائه شده، توسعه می‌یابند و بر مبنای تقاضا قابل کـاهش یا افزایش هستند (Marston, et al., 2011).

معرفی عملکرد و ابعاد محاسبات ابری

ابعاد محاسبات ابری

بسترهای محاسبات ابری در عین این‌که برای استفاده‌کننده طیـف وسـیعی از خـدمات و امکانات را ارائه می‌دهند، به راحتی نیز قابل تغییر هستند. فناوری‌های اصلی ابر محاسـباتی بـه شرح زیر می‌باشند (Linthicum, 2009):

۱) ذخیره‌سازی به عنوان سرویس؛
۲) پایگاه داده به عنوان سرویس؛
۳) اطلاعات به عنوان سرویس؛
٤) فرآیند به عنوان سرویس؛
۵) برنامه‌ی کاربردی و نرم‌افزار به عنوان سرویس؛
٦) پلتفرم به عنوان سرویس؛
۷) یکپارچگی به عنوان سرویس؛
۸) امنیت به عنوان سرویس؛
۹) مدیریت/حکمرانی[1] (حاکمیت) به عنوان سرویس؛
۱۰) آزمایشی به عنوان سرویس؛
۱۱) زیرساخت و شبیه‌سازی به عنوان سرویس.

1 - Governance

شکل شماره‌ی ۱ - اجزای محاسبات ابری

مزایای استفاده از محاسبات ابری

هر نهادی قبل از استفاده از محاسبات ابری قصد دارد بداند که محاسبات ابری چه چیز جدیدی را به مجموعه او ارائه می‌دهند؟ در پاسخ به این سؤال می‌توان به موارد زیر اشاره داشت (Gillam, 2010; Chandra, Mondal, 2011)

اول: توانایی استفاده سرویس‌ها از ابرهای مختلف و ترکیب و تطبیق راه‌کارها با آنچه که می‌خواهید. شما می‌توانید سرویس ذخیره‌سازی را از یک تأمین‌کننده تهیه کنید و سرویس پایگاه داده را از یک تأمین‌کننده‌ی دیگر و حتی پلتفرم توسعه‌ی برنامه را از تأمین‌کننده‌ی سوم گرفت.

دوم: تناسب سرویس با نیاز، این ویژگی موجب می‌شود تا منبع را در زمان مناسب به‌کار ببرید. همانند زمانی که شما آنها را در مرکز داده‌تان دارید.

در نهایت، در دسترس بودن طیف وسیعی از تأمین‌کنندگان (فراهم‌کنندگان) نوآور و به روز یکی دیگر از مزایای محاسبات ابری است. رشد روزافزون محاسبات ابری باعث ارائه‌ی سرویس‌های خلاقانه‌ای می‌شود که به‌طور مستمر در دسترس است.

نکته‌ی دیگر در راستای استفاده از محاسبات ابری نحوه‌ی استفاده از آن است. محاسبات ابری وقتی بیشترین مزیت را برای یک سازمان به همراه می‌آورند که در شرایط زیر مورد استفاده قرار بگیرند: (Grossman, et al.,2009)

- زمانی که فرآیندها، برنامه‌ها، داده‌ها به میزان زیادی مستقل باشند.
- زمانی که نقاط یکپارچگی به خوبی تعریف شده باشند و یا نقاط مشخصی در یک برنامه‌ای که داده، سرویس‌ها و فرآیندها را به اشتراک می‌گذارد، وجود داشته باشد.
- زمانی که سطح پائین‌تری از امنیت مورد نظر است، سیستم‌های محاسبات ابری (عمومی/مشترک) امنیت را در حد کافی فراهم می‌کنند ولی برای اطلاعات محرمانه مناسب نیستند.
- زمانی که وب/اینترنت، بستر مطلوب است یا زمانی که شما واسط کاربر سیستم‌های خود را روی یک جستجوگر اینترنتی راه‌اندازی می‌کنید.
- زمانی که هزینه یک مسأله است و یا زمانی که مزایای آشکاری در استفاده از محاسبات ابری وجود دارد.
- زمانی که گستردگی سازمان شما و نحوه‌ی سرویس‌دهی به اجزای سازمان یک دغدغه‌ی کلیدی است.

درحالی‌که اغلب افراد متخصص فناوری اطلاعات بر این اندیشه‌اند که پردازش ابری کاهش هزینه‌های عملیاتی را مورد توجه قرار می‌دهد، ولی بر حسب نوع سازمان و مسائل آن ممکن است این موضوع در پردازش ابری مورد توجه باشد و یا نباشد (Blokdijk, Menken, 2009). در این مورد چندین بُعد مختلف وجود دارد که باید مورد توجه قرار گیرند ازجمله:

- کاهش مداوم و مستمر هزینه‌های عملیاتی؛
- میزان سرمایه‌ی پشتیبان و سرمایه‌گذاری؛

- میزان بزرگ‌سازی مورد نیاز؛
- میزان توسعه و کوچک‌سازی مورد نیاز؛
- میزان انتقال خطر؛
- میزان چابکی؛
- میزان استفاده‌ی مجدد؛
- میزان محبوبیت.

فعالیت بین ابرها یا قابلیت انتقال بین ابرها

مسأله‌ی کلیدی در محاسبات ابری برای فراهم‌کنندگان ابرها ارائه‌ی قابلیت‌های ارتباطی و انتقالی بین تأمین‌کنندگان (فراهم‌کنندگان) است. هسته کلیدی این مفهوم یک کلمه‌ی مبهم است: بین ابرها!

ارتباط «بین ابرها» مفهومی جدید است که امروزه بسیار مطرح شده و به میزان موضوعیت یافته مطرح شده است. به واقع، به معنای امکان مبادله‌ی اطلاعات و رفتار بین تأمین‌کنندگان گسترده‌ای، برای پشتیبانی از کسانی می‌باشد که از ابر استفاده می‌کنند. همانند اینترنت، که تأمین‌کنندگان مختلف آن تمایل دارند بسیاری سرویس‌های متفاوت را با هم ترکیب کنند و مکانیزم استانداردی برای محقق شدن آن فراهم کنند.

این مسأله به چند دلیل اهمیت دارد. اول، مسئولیت برقراری ارتباط تأمین‌کنندگان را به خود آنها واگذار می‌کند تا کاربران؛ دوم، مبنایی برای «قابلیت انتقال» فراهم کنند. در نهایت هزینه‌ها را کاهش می‌دهد (با درنظر گرفتن دو دلیل قبلی هزینه، مهم‌ترین معیار فروش ابرهاست).

تأمین‌کنندگان ابرها علی‌رغم علاقه‌ی زیادی که به وابسته کردن مشتری به سرویس‌های خود دارند، مزایای زیاد دیگری نیز از بهبود قابلیت انتقال بین ابرها را مشاهده کرده‌اند. به هرحال،

همان‌طور که برنامه‌های «کد باز»[1] بهتر فروش می‌رود تا آنهایی که ویژگی‌های مالکیتی دارند، فروشندگان نیز این امکان را فراهم می‌کنند تا سازمان‌ها در بین ابرها حرکت کنند و شناور باشند.

موفقیت «قابلیت انتقال» در قلمروی تأمین ابرها بستگی دارد به توانایی آنها در توقف ویژگی‌های ساخت مالکانه و شروع ساخت با قابلیت انتقال بین ابرها (Buyya, et al, 2009; Linthicum, 2009).

ارزیابی معماری ابرهای محاسباتی

نحوه‌ی مالکیت ابرهای محاسباتی

ابر خصوصی[2]

ابر خصوصی زیرساخت‌هایی شبیه به محاسبات ابری هستند که از مجازی‌سازی استفاده کرده و در درون مراکز داده‌ای قرار دارند. مفهوم محوری در اینجا این است که محاسبه‌ی ابری رویکرد بسیار خوبی برای بهینه‌سازی استفاده از سخت‌افزار و نرم‌افزار بوده و نحوه‌ی مالکیت و کنترل بر عملکرد آن در اختیار یک مجموعه‌ی خاص است. مزیت اصلی این مدل، سطح بالای امنیت است که ناشی از استقرار یا به‌کارگیری تجهیزات در درون سازمان و عدم ارتباط با دنیای خارج می‌باشد.

ابر گروهی[3]

ابر گروهی هنگامی‌که چند سازمان دارای نیازهای مشابهی بوده و سعی داشته باشند تا با به اشتراک گذاردن یک ابر، از مزایای محاسبات ابری سود ببرند مورد استفاده قرار می‌گیرد. از لحاظ امنیت و هزینه، این مدل بین ابرهای خصوصی و عمومی قرار دارد.

ابر عمومی[4]

منظور از ابر عمومی، محاسبات ابری در معنای اصلی آن می‌باشد. در این حالت، سرویس‌های مورد نیاز از طریق اینترنت و از سوی یک تأمین‌کننده‌ی (ارائه‌دهنده‌ی) ثالث تهیه

1 – Open Source
2 – Private cloud
3 – Community Cloud
4 – Public Cloud

می‌شوند. عرضه‌کننده ابر عمومی، سرویس‌ها را به صورت اشتراکی به کاربران مختلف ارائه می‌دهد (Subashini, Kavitha ,2011; Paquette, et al., 2010).

ارزیابی معماری محاسبات ابری (پردازش یا رایانش بر اساس ابرها)

در این راستا، به منظور ارزیابی معماری آن را به اجزای ترکیب‌کننده‌اش تجزیه کرده (با حرکت از ابتدایی‌ترین به پیچیده‌ترین)، پس از ارزیابی مجزای هر قسمت، برای ارزیابی سیستم به صورت یکپارچه وارد عمل می‌شویم. به دو روش عمده نسبت به ارزیابی معماری اقدام می‌شود:

ارزیابی جعبه‌ی سیاه و جعبه‌ی سفید. ارزیابی جعبه‌ی سیاه؛ فرآیند ارزیابی، وظایفی است که بر آنها دید کامل نداریم. برای مثال، ممکن است از سیستمی بخواهیم که رفتارهای مشخصی را بروز دهد که در این راستا، مشاهده‌ی این‌که سیستم در داخل خود (بر اساس درخواست) چه عملیاتی را بروز می‌دهد تا آن درخواست را اجرا کند برای ما ممکن نخواهد بود (مثلاً بازگردانی اطلاعات به برنامه‌ی واسط کاربردی). استفاده از ارزیابی جعبه‌ی سیاه در استفاده از محاسبات ابری، اهمیت به‌سزایی دارد، چون ما معمولاً مالک و کنترل‌کننده‌ی سیستم‌ها نبوده و از داخل آن خبر نداریم.

در نقطه‌ی مقابل، ارزیابی جعبه‌ی سفید قرار دارد که به ما اجازه می‌دهد سیستمی را که بر آن دید کامل داریم، مورد ارزیابی قرار دهیم. وقتی از سیستمی بروز رفتارهای خاص را می‌خواهیم (مثلاً بازگردانی اطلاعات به میانجی برنامه‌ی کاربردی)، می‌توانیم چگونگی شکل‌گیری درخواست در داخل سیستم را ببینیم. از جمله‌ی این موارد؛ چگونه پایگاه‌های اطلاعاتی بر اساس تقاضای ما شکل می‌گیرند، دستیابی به پایگاه‌های اطلاعاتی چگونه است، فرآیند بازگشت اطلاعات از پایگاه‌های اطلاعاتی چگونه است و غیره می‌باشد (Blokdijk, Menken, 2009;Rochwerger, et al., 2009; Linthicum, 2009).

باید توجه داشت که رویکرد استفاده از ارزیابی جعبه‌ی سفید، به معنی عدم استفاده از ارزیابی جعبه‌ی سیاه نیست. ارزیابی جعبه‌ی سفید نمی‌تواند جایگزین ارزیابی جعبه‌ی سیاه باشد و این خود گامی دیگر خواهد بود که اجزای آن‌را کامل‌تر بررسی نماییم.

گرچه ارزیابی جعبه‌ی سفید معمولاً منجر به بهینه‌سازی می‌شود، اما همیشه مقرون به صرفه نیست. فهم چیستی ارزیابی جعبه‌ی سیاه و جعبه‌ی سفید، و زمان و مکان استفاده از هر یک از این روش‌ها، برای معماری بسیار مهم است. حوزه‌های ارزیابی محاسبات ابری را می‌توان به دسته‌بندی‌های اصلی زیر تقسیم کرد (Linthicum, 2009):

ارزیابی در سطح سرویس‌ها

سرویس‌ها می‌توانند به خودی خود و به‌عنوان بخشی از سیستم یکپارچه، به خوبی عمل کنند و از این منظر همچنین دیدگاه یکپارچه بودن (در تعامل با سایر سیستم‌ها) حتماً باید مورد ارزیابی قرار بگیرند.

بهترین راه برای ارزیابی سرویس‌ها این است که مصارف و هدف استفاده از آنها را فهرست کنیم. بعد، می‌توانیم تست‌هایی به منظور ارزیابی آن سرویس‌ها، مثلاً از لحاظ کارایی، عملکرد یا قابلیت‌ها، طراحی کنیم.

باید توجه شود که سرویس‌ها در درجات بالایی از خودکار[1] بودن و تحت حداکثر بارعملیاتی بارعملیاتی تست و آزمون شوند.

ارزیابی در سطح فرآیند

فرآیندها به تعریف چگونگی همکاری و تعامل سرویس‌های تحت وب با یکدیگر می‌پردازد که شامل منطق کسب و کار، اولویت‌دهی و رفع استثناها، تجزیه‌ی فرآیندها و امکان استفاده مجدد از فرآیندها و سرویس‌ها می‌شود. فرآیندها ممکن است چند سیستم داخلی سازمان، سیستم‌های داخلی بین شرکتی و یا هر دو را پوشش دهند. برخی از این فرآیندها «بلند مدت» و «چند تراکنشی» می‌باشند که همیشه توسط سازمان کنترل می‌شوند و در طبیعت خود ویژگی ناهم‌زمانی و دوباره‌کاری را دارند. به همین دلیل می‌بایست فرآیندهای بین سازمان یا بین ابری کنترل شوند تا از تکرار و دوباره‌کاری فرآیند مشابه جلوگیری شده و توالی زمانی آنها نیز کنترل شده باشد. در حقیقت، فرآیندها در حوزه‌ی معماری، سرویس‌ها اهمیت

1 - Automotion

به‌سزایی دارند. هم‌زمان با تست عملیاتی سرویس‌ها، به ارزیابی عملکردی آنها، (مثلاً در زمینه‌هایی مانند انتزاع، قابلیت استفاده‌ی مجدد و جزئی‌نگری) می‌بایست پرداخته شود. البته باید این نکته را مدنظر قرار داد که این فرآیندها در سرویس‌های کنونی اجرا می‌شوند، و ارزیابی‌ها باید از بالا به پائین یا از پائین به سرویس‌های اولیه و ابتدایی انجام پذیرد.

ارزیابی در سطح مدیریتی

از طریق تطبیق سیاست‌ها و اعمال آنها در ساختار عملکرد سیستم‌ها و اداره کردن سیستم‌ها به‌وسیله‌ی مدیریت و کنترل آنها در سطوح مختلف، به ارزیابی سیستم‌های مدیریتی می‌توان پرداخت. تنها کاری که باید انجام داد، فهرست‌بندی سیاست‌ها و ایجاد موارد ارزیابی برای هریک از آنها است. کار با فناوری‌های مدیریتی، موارد مناسبی را برای ارزیابی کارایی مدیریت در سیستم فراهم می‌آورد.

ارزیابی در سطح اطلاعات

مانند سیستم‌های سنتی ارزیابی یکپارچه، منظور از این نوع ارزیابی درک این مطلب است که آیا تمامی واسطه‌ها (که شامل رفتارها و اشتراک اطلاعات می‌شود)، کار خود را به‌درستی انجام می‌دهند یا نه؟ ارزیابی یکپارچه می‌بایست در سطوح و لایه‌های مختلف ارتباطی کار کند، یعنی کار خود را در سطوح شبکه به پردازشگرهای ارتباطی به سرانجام رساند و قابلیت آن را داشته باشد که نوع ارتباط و تبادل اطلاعات در سطوح و لایه‌های مختلف را ارزیابی کند، در نهایت، به‌علاوه از استفاده‌ی از مکانیسم‌های ارتباطی اطمینان حاصل نماید.

ارزیابی در سطح یکپارچگی

هدف از این کار ارزیابی مستقیم ماندگاری اطلاعات (معمولاً در پایگاه داده‌ها)، بدون مراجعه به سرویس‌ها می‌باشد. به منظور بررسی بازده و ثبات پایگاه داده‌ها موارد زیر می‌بایست مدنظر قرار گیرند:

- ثبات عملکرد؛
- بازدهی واسطه (میانجی)؛

- بازدهی طرح.

عملکرد یعنی اطمینان از این موضوع که آیا پایگاه داده‌ها، در زمان تعیین شده می‌تواند به نیازهای معماری، (و توالی سرویس‌ها) پاسخ بگوید؟ مشکلات عملکردی ممکن است ریشه در واحد پردازش مرکزی[1] و یا مسائل مرتبط با منابع رایانه‌ای داشته باشد، اما در بسیاری از موارد، مشکلات به علت طراحی در پایگاه داده‌ها پدید می‌آیند. این نکته را مدنظر قرار دهید که ارزیابی در سطح اطلاعات، هم پایگاه داده‌ایِ سیستم‌های ابری را در بر می‌گیرد و هم رایانه‌ای و ثبات توانایی داده‌ها مبتنی بر حفظ حالت عملی خود برای مدت طولانی است.

بازده‌ی میانجی یعنی توجه به مواردی همچون: برنامه‌ی کاربردی میانجی[2]،پایگاه اطلاعاتی به‌کار برده شده در زمان درخواست داده، طرح به‌روزسازی و مدیریت پایگاه داده‌ها. این موارد، مسائلِ ویژه پایگاه‌های داده هستند و باید با استفاده از مواردی که ناظر بر چگونگی استفاده از آنها در زمان اجراست، مورد ارزیابی قرار بگیرند.

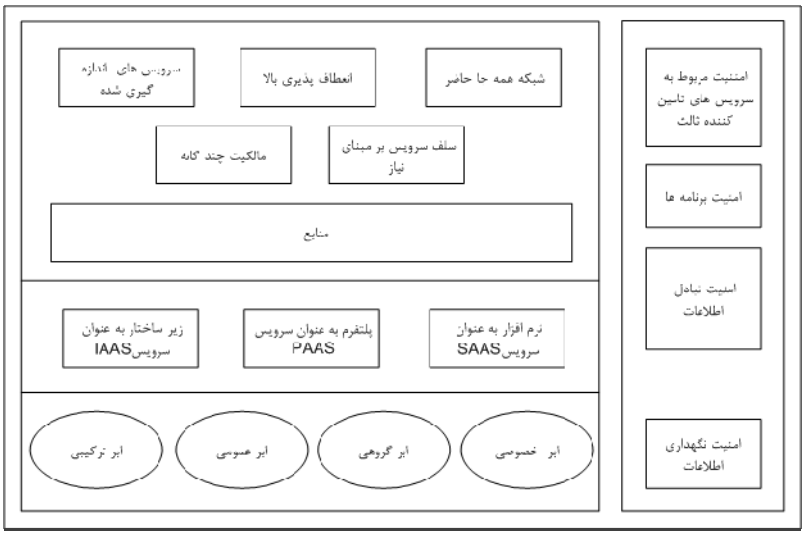
و در آخر، بازدهی طرح ، «به‌هنجار شدگی (نرمال شدگی) پایگاه‌های داده، طراحی و توانایی برای برطرف کردن نیازهای معماری» را مدنظر قرار می‌دهد. پایگاه داده‌ای که به شدت نرمالایز شده باشد، می‌تواند مشکلات اجرایی داشته باشد و پایگاه داده‌ای که به درستی نرمالایز نشده است، نمی‌تواند به درستی به رفع نیازهای کلی سیستم بپردازد.

امنیت اطلاعات در محاسبات ابری

بر اساس تحقیق که توسط «آی دی سی »[3] در سال ۲۰۰۹ صورت پذیرفت، ۷٤ درصد از مدیران ارشد فناوری اطلاعات و راهبران سازمان‌ها بیان داشتند که امنیت به عنوان مهم‌ترین چالش، مانعی اساسی بر سر راه توسعه و به‌کارگیری محاسبات ابری در سازمان‌ها می‌باشد (Clavister, 2009). پیش‌بینی شده است که تا سال ۲۰۱۵ بازار محاسبات ابری رشدی نزدیک به ۹۵ ملیارد دلار داشته باشد و ۱۲٪ نرم‌افزارها بر روی این بستر ارائه شوند (BNA, 2009). با

1 – CPU (Central Process Unit)
2 – API
3 - IDC

توجه به این‌که مهم‌ترین نگرانی در این میان (مخصوصاً برای سازمان‌های نظامی و امنیتی) نحوه‌ی دسترسی به اطلاعات و وجود اطلاعات در ساختاری است که در خارج از آن مجموعه شکل گرفته است، توجه و سرمایه‌گذاری بر نیازمندی‌های امنیتی در محاسبات ابری از اهمیت بالایی برخوردار است. در شکل زیر چارچوب امنیت اطلاعات در پردازش یا محاسبات ابری نمایش داده شده است.



شکل شماره‌ی ۲ - پیچیدگی امنیت اطلاعات در محاسبات ابری

در زمان ارزیابی محاسبات ابری به منظور مسائل امنیتی، اولین گام باید تشخیص نیازمندی‌های امنیتی باشد و سپس، باید نیازمندی‌های برنامه‌ی ارزیابی را ایجاد نموده و نقاط ضعف را مشخص کرد. در دنیای محاسبات ابری، متخصصان فناوری اطلاعات اعتقاد دارند که بهره‌مندی از ارزیابی جعبه‌ی سیاه بهترین روش ارزیابی آزمون سیستم است، که شامل تست‌های نفوذ به سیستم و آسیب‌پذیری،(با استفاده از تکنیک‌ها و روش‌های موجود) می‌شود.

نکته‌ی امنیتی نگران کننده‌ی دیگر در محاسبات ابری این است که معماری آنها امکان استفاده از سرویس‌ها را از خارج از سازمان فراهم می‌سازد که آسیب‌پذیری‌های دیگری را از جمله مسائل امنیت اطلاعات و استفاده‌ی سرویس‌های خارج از دیوار آتش از سرویس‌ها را به‌وجود می‌آورد. این خود،

راه را برای انواع دیگر حملات باز می‌کند که درچنین شرایطی، امنیت نیز باید مورد ارزیابی قرار بگیرد (Subashini, Kavitha, 2011; Santos, et al., 2009).

سازمان‌های اطلاعاتی و پردازش بر مبنای ابرها

نقاط ارزش و مزایای ابر در سیستم‌های اطلاعاتی

استفاده از معماری سرویس‌گرا با رویکرد پردازش ابری برای سازمان‌ها و مجموعه‌های مختلف مزایای کلیدی را ایجاد می‌کند:

- یک مجموعه قادر است از هر مکانی در صورت نیاز از سرویس‌های مورد نیاز خود استفاده کند. چرا که این سرویس‌ها مستقل از مکان و بستر هستند و مکان مورد استفاده برای میزبانی آنها مسأله‌ی مهمی نخواهد بود (Linthicum, 2009).
- سازمان می‌تواند از مجازی‌سازی[1] بهره بگیرد، یعنی از برنامه‌های کاربردی کلیدی به عنوان نمود منطقی سیستم بر روی هر تعداد سرور فیزیکی دلخواه استفاده کنیم و در عین حال، به استفاده بهتر و قابلیت توسعه‌ی منابع برسیم. در واقع، می‌توانیم از طریق رابط سرویس‌ها با برنامه‌های کاربردی ارتباط برقرار کنیم (Gillam, 2010).
- سازمان دارای این توانایی خواهد بود که سرویس‌ها را ترکیب کرده و مطابقت دهد، تا بتواند از آنها در نرم‌افزارها و فرآیند ترکیبی[2] استفاده کرد. این موضوع بیانگر جنبه‌ای از معماری سرویس‌گرا و پردازش ابری است که با مفهوم چابکی سازگاری دارد. علاوه بر این‌که به سرعت قادر خواهیم بود فرآیندهای برنامه‌های کاربردی را برای حل مسائل کسب و کار ایجاد کنید، در صورت نیاز نیز قادر به خلق مجدد آنها می‌باشید و به این ترتیب هسته‌ی اصلی چابکی یک مجموعه محقق خواهد شد (Marston, et al., 2011).

1 – Virtualization
2 – Composite

استفاده از محاسبات ابری دارای نقاط ارزش و مزایای دیگری نیز می‌باشد کـه کـاهش و صرفه‌جویی در منابع سخت و نرم سازمان همچنین کارایی هرچه بیشتر را بـه همـراه خواهنـد داشت. برخی از این موارد در ادامه فهرست شده‌اند:

- کاهش مداوم هزینه‌های عملیاتی؛
- میزان و ارزش سرمایه‌ی پشتیبان؛
- ارزش کاهش/افزایش خدمات مورد درخواست؛
- ارزش انتقال خطر؛
- ارزش چابکی؛
- ارزش استفاده‌ی مجدد؛
- ارزش ابداع؛
- ارزش به‌روزرسانی و برخط بودن.

البته، مزایای دیگری نیز وجود دارند که به سختی در قالب کمیت‌ها قابل بیان می‌باشند با این وجود، نمی‌توان از آنها چشم‌پوشی کرد. برای مثال، ارتقای فرآیند اخذ تصـمیم در سـطوح پخش شده‌ی یک نیرو، پردازش اطلاعات نیروها و مجموعه‌های مختلف که از نظر زمـانی یـا مکانی با هم فاصله دارند، ارزش رضایت بیشتر کاربران و ذی‌نفعان در سطح گسترده‌ای از نیرو (ارزشی که افراد به واسطه‌ی پشتیبانی فناوری اطلاعات از فرآیندهای سرویس‌دهنـده بـه آنهـا درک می‌کنند) و یا ارزش روحیه‌ی بهتر کارکنان و کاربران، از این نوع مزایا هستند.

کاربرد ابرها در سازمان‌های اطلاعاتی

مدیریت و حفظ امنیت و کنترل داده‌ها و اطلاعات غیرمتمرکز همـواره دغدغـه‌ی اصـلی طراحان و کاربران سیستم‌های اطلاعاتی بوده اسـت. در سـازمان‌هـای اطلاعـاتی، سـامانه‌هـای نظامی و صحنه‌ی نبرد (مخصوصاً جنگ‌های مدرن) این امر به اولویتی کلیدی برای فرمانـدهی و کنترل مجموعه‌ها تبدیل شده است. گستردگی نیرو، پراکندگی منابع اطلاعاتی و پایگـاه‌هـای داده، وجود مجموعه و زیرمجموعه‌های مختلف، نحوه‌ی تحلیل صحنه‌ی نبرد و یکپارچه‌سازی

فرآیندها و از همه مهم‌تر، امنیت در دسترسی و تبادل اطلاعات، و وجود ارتباطات بـر بسـتری مطمئن از دیگر متغیرهای حیاتی در تصمیم‌گیری فرماندهی ارشد نیروها می‌باشند.

بنابراین، زمانی که پایگاه داده‌های مختلف را برای پردازش تحلیل می‌کنـیم، موضـوعات مرتبط با یکپارچگی همواره از اولویت‌های بالا خواهند بود. گستردگی سطح عملیـاتی نیـرو و نبود کنترل یکپارچگی در سطح داده‌ها یا اطلاعات (همچنین امکان دور زدن برنامه‌ی کاربردی برای دسترسی مستقیم به داده‌ها در سیستم‌هـای موجـود)، مـی‌توانـد بـه مشـکلات بنیـادین و شکست‌های اطلاعاتی منجر شود. معماران و توسعه‌دهندگان سیستم باید با ایـن مشـکلات بـا دقت و محتاطانه برخورد کرده و اطمینان حاصل کنند که در مسیر حرکت به سـمت پـردازش ابری، اهداف مرتبط با یکپارچگی و امنیت داده‌ها و پایگاه‌های داده به خوبی پوشش داده شـده و محقق شوند.

در این راستا، دو رویکرد را در رابطه با محاسبات ابری باید لحـاظ نمـود. بهتـرین مـدل استفاده از قابلیت‌های محاسبات ابری برای یک مجموعه بهـره‌گیـری از امکانـات «محاسـبات ابری خصوصی» می‌باشد. در این حالت فقط یک مجموعه (فرضاً نیروی اطلاعاتی یـا انتظـامی یک شهر یا یک استان) از یک ابر استفاده کرده و بـا وجـود هزینـه‌ی بـالایی کـه مـی‌پـردازد، دغدغه‌های امنیتی او به پائین‌ترین سطح کاهش پیدا می‌کند. در صـورتی کـه اسـتفاده‌کننـده از محاسبات ابری بیش از یک واحد باشد، به ترتیب ابر گروهی و عمومی (با لحاظ نمودن برخی از ملاحظات) گزینه‌ی مناسب برای استفاده واحدهای نظامی و امنیتی خواهند بود. در هر دوی این گزینه‌ها، استفاده‌کنندگان از ابرها صرفاً و صرفاً نیروهـای نظـامی و امنیتـی مـی‌باشـند. ابـر گروهی، مناسب حالتی می‌باشد که نیروهای نظامی/امنیتی از یک جنس باشند؛ ماننـد نیروهـای انتظامی کل استان‌ها، مانور نیروهای مسلح (هوایی، دریایی و زمینی) در یک منطقه و یا نیـروی زمینی در سطح کشور. ابر عمومی در صورتی می‌تواند به بستری امـن بـرای تبـادل ارتباطـات فراهم شود که به مجموعه‌ای از نیروهای نظامی/امنیتی سرویس بدهـد. در صـورتی کـه قصـد داشته باشیم از بستر یک ابر عمومی استفاده کنیم، مانند شرایط مدیریت بحران یا صحنه‌ی نبرد، متولی این ابر بایست سازمانی معتبر و مورد اعتماد بوده و صرفاً نیروهـای نظـامی و امنیتـی را

تحت پوشش داشته باشد. موارد زیر از جمله‌ی نکات و ویژگی‌هایی می‌باشند که به واسطه‌ی رویکرد یکپارچه محاسبات ابری برای این نیروها فراهم می‌شوند:

- مدیریت و راهبری متمرکز و هدفمند اطلاعات در حداکثر امنیت و سرعت؛
- صرفه‌جویی در منابع (هزینه‌ی پائین، پهنای باند بالا، بهبود مداوم نرم‌افزارها، کاهش هزینه‌ی سرورها و ...)؛
- تأمین فرامکانی و فرازمانی اطلاعات[1] برای مجموعه‌های متقاضی؛
- کاهش تعدد مراکز اطلاعاتی، تمرکز بر یک مجموعه و در نتیجه راندمان و امنیت بالاتر؛
- به‌کارگیری مؤثر ابزارهای همراه[2] و تحقق عامل اطلاعاتی همراه؛
- تأمین اطلاعات به هنگام در صحنه‌ی عملیات (وسایل همراه سبک و قابل حمل و استفاده در زمین و هوا)؛
- استفاده از ابر خصوصی؛ امنیت، یکپارچگی، هویت واحد، شبکه‌ی ارتباطات امن و برخط.

در نظر بگیرید، عامل اطلاعاتی در صحنه‌ی عملیات نیاز به اطلاعات دارد و این اطلاعات را از ابزارهای همراه خود و از طریق ابرها کسب می‌کند. قابلیت پائین محاسباتی و ذخیره‌سازی این ابزارها، از دیگر الزام‌های لحاظ نمودن ابرها در معادلات مختلف دفاعی و امنیتی است. در این صورت، با وجود این‌که سازمان اطلاعاتی و عامل انسانی، اطلاعات به هنگام و در صحنه را تبادل می‌کنند، نگرانی از لو رفتن و آشکارسازی اطلاعات خود ندارند؛ چراکه همه‌ی اطلاعات بر روی ابرها می‌باشد و وسایل همراه افراد فقط نمایش‌دهنده یا تبادل‌کننده اطلاعات با حفظ سطوح نفوذ و دسترسی تعریف شده و امن می‌باشند. در واقع، هنگامی‌که متولی تأمین بسترهای فناورانه اطلاعاتی در کشور متمرکز باشد، امکان مدیریت و یکپارچگی اطلاعات ارتقاءیافته و تمامی توان اطلاعاتی (اعم از منابع نرم و سخت) را می‌توان در این ساختار متمرکز کرد.

---

1 – Intelligence
2 – Mobile Intelligence

نتیجه‌گیری

مزیت ایجاد سیستم‌های جدید در بستر ابرها این است که سازمان و افراد با یک موقعیت بکر روبه‌رو هستند؛ زیرا قادر می‌باشند هر آنچه که می‌خواهند را تعریف کنند و به هیچ عنوان با سیستم‌های فعلی که داده‌ها و فرآیندهای از قبل تعریف‌شده‌ای را به آنها تحمیل می‌کنند، سر و کار ندارند. به واقع، فرآیند ایجاد سیستم‌های جدید بسیار ساده‌تر و کاراتر است، به‌علاوه این‌که در تبادل اطلاعات، مستقل از مکان و بستر هستند و مکان مورد استفاده برای میزبانی و ارائه‌ی آنها مسأله‌ی مهمی نخواهد بود. مضاف بر این‌که اطلاعات برخط و به لحظه را دریافت کرده یا ارائه می‌کنند. اقداماتی که امروزه در زمینه‌ی پردازش ابری صورت می‌گیرد، دارای این توانایی‌اند که بر روی بستر پردازش ابری مزایای راهبردی کلیدی را برای سازمان‌های اطلاعاتی و امنیتی ایجاد کنند.

برای استفاده‌ی نیروهای نظامی و امنیتی، محاسبات ابری، بنابر نیاز عملیاتی، کار ویژه و خواسته‌ی ایشان می‌تواند از هر سه بستر ابر خصوصی، مشترک و عمومی استفاده نموده و نیازهای اطلاعاتی و یکپارچگی را در کمترین زمان و امن‌ترین حالت پوشش داد. از سویی دیگر، نقاط ضعف ابزارها و رایانه‌های همراه نیرو (در زمین و هوا) در نگهداری داده، پردازش و یکپارچه‌سازی نیز به کمک این رویکرد نوین برطرف خواهد شد. تبادل اطلاعات بین ابرها نیز می‌تواند مسائل مربوط به گستردگی سطح عملکرد نیرو، یکپارچگی بین نیروهای عملیاتی مختلف و انسجام صحنه‌های نبرد را پوشش بدهد.

با توجه به مشخصه‌های جنگ‌های نوین، نیازهای اطلاعاتی در صحنه‌ی نبرد، اهمیت غیرقابل انکار امنیت و یکپارچگی پردازش اطلاعات و همچنین ابزارهای موبایل همراه با واحدهای نظامی، می‌توان پیش‌بینی کرد که بیشتر اقداماتی که طی چند سال آینده در مورد پردازش ابری صورت می‌گیرد، عمدتاً به این شکل عمل می‌کنند، زیرا علاوه بر کارایی بالا، هزینه‌ی عملیات کلیدی آنها در زمینه‌ی فناوری اطلاعات به علت

بهره‌گیری از پردازش ابری بسیار پائین است، مطمئناً سازمان‌ها با چنین معماری‌ای دارای توانمندی‌های بیشتری خواهند بود.

منابع

فارسی

۱- حکیم، امین، (۱۳۸۹)، «***برنامه‌ریزی راهبردی و فناوری اطلاعات***»، تهران؛ دانشگاه امام حسین (ع).

انگلیسی

2- Blokdijk G., I. Menken, (2009), ***"Cloud Computing - The Complete Cornerstone Guide to Cloud Computing Best Practices***", Emereo Pty.

3- BNA- Bureau of National Affairs, (2009), "***Privacy& Security Law Report***", http://www.hunton.com/files/ Publication/6acf0d97-7c21-42d1-ab48-315a04601152/ Presentation/ PublicationAttachment/37dc2129-4f0c-45a0-8417-651e05dc423f/CloudComputing_Bruening-Treacy.pdf, Posted at: 10, 03/09/2009, accessed Feb. 2011.

4- Brian J. S. , Jr. Curtis Franklin, Jr. Curtis Franklin, (2010), "***Cloud Computing: Technologies and Strategies of the Ubiquitous Data Center***", CRC Press.

5- Buyya R. (2009), C. ShinYeo, S. Venugopal, J. Broberg, I. Brandic, "***Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility***", Future Generation Computer Systems, No. 25.

6- Clavister, (2007), "***Security in the cloud***" , http://www.it-wire.nu/, Posted at: 2007/06/15, accessed Feb. 2011.

7- Gillam L, (2010), "***Cloud Computing: Principles, Systems and Applications***", Springer.

8- Grossman R. L., Y. Gu, M. Sabala, W. Zhang, (2009), "***Compute and Storage Clouds Using Wide Area High Performance Networks***", Future Generation Computer Systems, Volume 25, Issue 2, February.

9- Linthicum D.S, (2009), "***Cloud Computing and SOA Convergence in Your Enterprise***", Addison-Wesley.

10- Marston S., Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, (2011), "***Cloud Computing - The Business Perspective***", Decision Support Systems, No. 51.

11- Misra S.C. ,A. Mondal, (2011), "***Identification of a Company's Suitability for the Adoption of Cloud Computing and Modeling its Corresponding Return on Investment***", Mathematical and Computer Modeling, No. 53.

12- Paquette S., P.T. Jaeger, S.C. Wilson, (2010), "***Identifying the Security Risks Associated with Governmental Use of Cloud Computing***", Government Information Quarterly, No. 27.

13- Rochwerger B., D. Breitgand, E. Levy, A. Galis, K. Nagin, I. M. Llorente, R. Montero, (2009), "***The Reservoir Model and Architecture for Open Federated cloud Computing***", IBM Journal of Research and Development, 53 (4).

14- Santos N., K.P. Gummadi, R. Rodrigues, (2009), "***Towards Trusted Cloud Computing***", HotCloud'09- Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, CA, USA: USENIX Association Berkeley.

15- Subashini S., V. Kavitha, (2011), "***A Survey on Security Issues in Service Delivery Models of Cloud Computing***", Journal of Network and Computer Applications, No.34.

مجله سیاست دفاعی
سال بیستم، شماره ۷۹، تابستان ۱۳۹۱

تدوین روش توسعه چارچوب‌های معماری سازمان‌های دفاعی

احسان مرآتی [۱]

تاریخ دریافت مقاله: ۱۳۹۱/۰۱/۲۸
تاریخ تأیید مقاله: ۱۳۹۱/۰۳/۱۷
صفحات مقاله: ۶۰ – ۳۳

چکیده:

غالباً حوزه‌ی دفاعی به دلیل برخورداری از اهمیت و حساسیت ویژه، منشأ ابداع روش‌های جدید مدیریتی و مهندسی می‌باشد. مبحث معماری سازمانی نیز یکی از این‌گونه موارد است که ریشه در سازمان‌های دفاعی ایالات متحده دارد. اکنون نیز سازمان‌های دفاعی یکی از بهترین نمونه‌های اجرا کننده‌ی چارچوب‌های معماری سازمانی می‌باشند. اما این سازمان‌ها در زمینه‌ی چگونگی توسعه چارچوب‌های معماری خاص سازمان‌های دفاعی، اطلاعات چندانی را منتشر ننموده‌اند. از این رو، این مقاله به تدوین روشی برای توسعه چارچوب‌های معماری سازمان‌های دفاعی می‌پردازد. برای این منظور، نسخه‌های مختلف چارچوب معماری وزارت دفاع ایالات متحده مورد تحلیل و بررسی قرار گرفته و با به‌کارگیری روش تحقیق نظری زمینه‌ای، با رویکردی استقرائی، روشی برای توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی ارائه شده است. به‌کارگیری این روش می‌تواند مزایایی همچون کاهش زمان توسعه‌ی چارچوب، کاهش ریسک، کاهش هزینه، و مدیریت بهتر فرآیند توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی را به همراه داشته باشد.

* * * * *

واژگان کلیدی

معماری سازمانی، چارچوب معماری، چارچوب معماری وزارت دفاع ایالات متحده، سازمان‌های دفاعی.

---

[۱]– دانشجوی دکتری مدیریت سیستم‌ها، دانشکده مدیریت، دانشگاه تهران.

مقدمه

امروزه معماری سازمانی به یکی از روش‌های مدیریت تغییرات سازمانی مبدل گشته و پیوسته در سازمان‌های بزرگ و متوسط مورد استفاده قرار می‌گیرد. در این راستا، معماری سازمانی مزایایی همچون بهبود روش‌ها و فرآیندهای سازمانی، انعطاف‌پذیری در برابر تغییرات محیطی، تطبیق نیازمندی‌های لایه های مأموریتی و فناوری اطلاعات و ارتباطات، کاهش میزان خطر پروژه‌های فناوری اطلاعات و ارتباطات، کنترل و هدایت مؤثر سازمان، افزایش میزان تعامل‌پذیری میان سیستم‌های اطلاعاتی و افزایش سطح امنیت اطلاعات را برای سازمان‌ها به همراه دارد (Jafari et al., 2009). از طرفی خروجی‌های معماری سازمانی نیز به منظور تهیه‌ی نقشه راه تغییرات سازمانی، تسهیل تصمیم‌گیری، ایجاد دیدگاهی مشترک نسبت به پیچیدگی‌های سازمانی و توسعه‌ی سیستم‌های اطلاعاتی مورد استفاده قرار می‌گیرند. معماری سازمانی به لحاظ تاریخی در سازمان‌های بزرگ دولتی نظیر وزارتخانه‌های دفاع و انرژی ایالات متحده توسعه یافته و این سازمان‌ها در این امر پیشرو بوده‌اند (Allega, 2004). «شِکرمن»[1] یکی از تعاریف جامع از معماری سازمانی را ارائه نموده که به شرح زیر می‌باشد (Schekkerman, 2004):

«معماری سازمانی عبارتست از، شناسایی مجموعه‌ی عناصر شکل دهنده‌ی سازمان و تعیین چگونگی ارتباط بین این عناصر».

تعریف فوق، حول عناصر سازمانی شکل گرفته و بر شناسایی آنها تأکید دارد. برخی از این عناصر عبارتند از: کسب و کار، راهبردها، حوزه‌های کاری، وظایف، فعالیت‌ها، خدمات، افراد، فرآیندها، و فناوری، پیشران‌های کاری، اصول، ذی‌نفعان، واحدها، مکان‌ها، بودجه، اطلاعات، ارتباطات، برنامه‌ها، و زیرساخت‌ها. شناسایی این عناصر و تعیین روابط بین آنها و به عبارتی پیاده‌سازی معماری سازمانی در سازمان نیازمند به‌کارگیری رویه‌ها و اصولی است که در چارچوب‌های معماری تدوین گردیده است. چارچوب‌های معماری سازمانی در طی روند

1 - Schekkerman

تکاملی معماری سازمانی از طرف مؤسسات خصوصی یا بخش‌های دولتی ارائه شده و هر چارچوب، بسته به ماهیت آن متناسب سازمان‌های خاصی می‌باشد. چارچوب‌ها غالباً شامل توصیه‌های اجرایی نظیر نحوه‌ی تشکیل تیم معماری، فرآیند کلی معماری، مشخصات محصولات معماری و توصیه‌های لازم جهت استفاده از تکنیک‌های مدل‌سازی می‌باشد.

در پی گسترش معماری سازمانی و تأیید قابلیت‌های راهبردی آن برای سازمان‌ها، اغلب سازمان‌های بزرگ دفاعی در سطح دنیا (مانند وزارت دفاع ایالات متحده و نیز وزارت دفاع بریتانیا) به توسعه‌ی چارچوب‌های معماری سازمانی بومی پرداخته‌اند تا بتوانند از قابلیت‌های معماری سازمانی در حوزه‌ی دفاعی بهره‌مند گردند. شاید این‌گونه به نظر برسد که سازمان‌های دفاعی کشور ما نیز می‌توانند با به‌کارگیری چارچوب‌هایی نظیر چارچوب معماری وزارت دفاع ایالات متحده[1] که مختص حوزه‌ی دفاعی توسعه یافته‌اند، به نیاز خود در زمینه‌ی معماری سازمانی پاسخ گویند. اما آمار نشان می‌دهد که به دلیل وجود تفاوت‌های عمده میان سازمان‌های مختلفی که در کشورهای گوناگون رشد نموده‌اند، نمی‌توان یک چارچوب معماری حوزه‌ی دفاعی را برای تمامی سازمان‌های دفاعی تجویز نمود و از این رو بخش قابل توجهی از سازمان‌ها یا از چارچوب عمومی «زکمن» که یک چارچوب عام است، استفاده نموده‌اند (۲۵٪) و یا این‌که چارچوب معماری مختص خود (۲۲٪) را توسعه داده‌اند (Institute for Enterprise Architecture Developments, 2005).

چارچوب‌های معماری، نقشی کلیدی را در فرآیند برنامه‌ریزی معماری سازمانی و همچنین در اجرای معماری ایفا می‌نماید. استفاده از چارچوب مناسب برای معماری سازمانی استاندارد بودن و یکپارچگی سیستم‌های اطلاعاتی را در هنگام انتقال از سیستم‌های قدیمی به سیستم جدید تضمین می‌کند (Nagarajan, 2010). کمک به تفکر سازمان‌یافته در خصوص معماری، فراهم آوردن توصیفی از محصولات و ابزارهای معماری، فراهم کردن روشی برای ارتباط میان اجزای معماری و ایجاد زبان مشترک از طریق ایجاد تعاریف و مفاهیم استاندارد و

1 – DoDAF (Department of Defense Architecture Framework)

یکسان در سطح سازمان، از دیگر دلایل به‌کارگیری چارچوب معماری است (Zachman, 2005). در مجموع، انتخاب و تنظیم چارچوب معماری مناسب که در مراحل اولیه‌ی برنامه‌ریزی معماری سازمانی انجام می‌پذیرد، تأثیر بسزایی هم در اجرای معماری سازمانی و هم در محصولات فناوری اطلاعاتی که برای سازمان ایجاد خواهند شد، دارد. تیم معماری سازمانی با در نظر گرفتن این خصوصیات و همچنین تجربیات خود روی چارچوب خاص، محدودیت منابع و زمان برای تولید محصولات، سیاست سازمان و نیاز به سازگاری با سازمان دیگر، چارچوب معماری مورد نظر را ارائه می‌دهد.

با توجه به تجارب جهانی در زمینه‌ی به‌کارگیری چارچوب‌های معماری و همچنین به دلیل حساسیت و اهمیت موضوعات و مسائل دفاعی در کشور، ضروری به نظر می‌رسد که چارچوبی خاص معماری سازمان‌های دفاعی توسعه یابد. مسلماً اولین سؤالی که در این راستا به ذهن می‌رسد، چگونگی توسعه‌ی چارچوب معماری سازمانی حوزه‌ی دفاعی کشور است. از این رو، این مقاله در پی پاسخگویی به این سؤال اساسی، به تدوین روش توسعه‌ی چارچوب معماری سازمان‌های دفاعی می‌پردازد.

روش ارائه شده در این مقاله بایستی به‌گونه‌ای تدوین گردد که خاص حوزه‌ی دفاعی بوده و در عین حال ضروری است تا این روش فاقد هرگونه پیش‌فرض درباره‌ی اجزای چارچوب معماری حوزه‌ی دفاعی باشد. زیرا این روش صرفاً می‌بایست فعالیت‌های مورد نیاز جهت توسعه چارچوب معماری را مشخص نماید و نباید جهت‌گیری و یا پیش زمینه‌ی فکری خاصی را در مورد اجزا و روابط موجود در چارچوب معماری بر کاربران آن تحمیل نماید. در غیر این‌صورت، روش مورد نظر، بخشی از چارچوب را نیز ارائه می‌دهد که این امر بر خلاف ماهیت روش مذکور است.

در واقع، چارچوب‌های معماری سازمان‌های دفاعی، نظیر DoDAF، از طریق روشی که متشکل از مراحل و فعالیت‌های خاصی می‌باشند، توسعه می‌یابند. با این‌که اطلاعات مشروحی درباره‌ی چارچوب‌های معماری در دسترس است، اما با این‌حال مستندات بسیار کمی درباره

روش توسعه‌ی آنها موجود می‌باشد. البته این امر منطقی و قابل قبول است. زیرا قابلیت اصلی[1] سازمان‌های توسعه دهنده‌ی چارچوب‌های معماری، آگاهی و اشراف آنها بر چگونگی توسعه این چارچوب‌ها می‌باشد. نهایتاً آنچه به راحتی در اختیار دیگران قرار داده می‌شود، خروجی کار است و نه روش دستیابی به آن خروجی. یکی از منابعی که مختصراً به تشریح روش توسعه‌ی چارچوب‌های معماری پرداخته است، کتاب «بقا در جنگل چارچوب‌های معماری» (Schekkerman, 2004 b) می‌باشد. «شکرمن» در فصل یازدهم این کتاب مختصراً به روش توسعه‌ی یک چارچوب معماری پرداخته است. وی چند مرحله‌ی عام را برای توسعه‌ی چارچوب معماری پیشنهاد نموده است که به شرح زیر می‌باشد:

۱) ارزیابی و درک دقیق محیط کسب و کار سازمان؛

۲) تعیین اهداف و مقاصدی که چارچوب باید آنها را تأمین نماید؛

۳) شناسایی چارچوب‌هایی که با محیط کسب و کار و اهداف سازمان بیشترین انطباق را دارد؛

٤) بومی‌سازی چارچوب انتخاب شده و تعیین تکنیک‌های مدل‌سازی متناسب؛

۵) اجرای آزمایشی چارچوب توسعه یافته؛

٦) تعیین تجربیات حاصل از اجرا و اصلاح نمودن چارچوب و فرآیندهای مربوط به آن.

در مجموع، با توجه به اهمیت و حساسیت حوزه‌ی نظامی و لزوم بهره‌گیری این حوزه از قابلیت‌های رویکرد معمارانه و نیز به دلیل عدم انتشار شیوه‌ی توسعه‌ی چارچوب‌های معماری حوزه‌ی دفاعی، این مقاله، با تحلیل نسخه‌های گوناگون DoDAF، که چارچوب معماری خاص حوزه‌ی دفاعی ایالات متحده می‌باشد، به ارائه‌ی روشی برای توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی می‌پردازد.

معماری سازمانی

در اوایل دهه‌ی ۹۰ میلادی در پی رشد فناوری‌های اطلاعاتی، سازمان‌های مختلف در کشورهای پیشرفته، به‌ویژه ایالات متحده، با طیف وسیعی از کاربردهای این فناوری‌ها روبه‌رو

1 – Core Competency

شدند که هر یک در جهت خاصی در حال گسترش بود. از طرفی این سازمان‌ها زیر فشارهای محیطی شدیداً به استفاده‌ی مؤثر و ساختار یافته از منابع اطلاعاتی احساس نیاز نمودند. اولین تلاش‌هایی که در این راستا با هدف چارچوب بخشیدن و هماهنگ کردن منابع و فناوری‌های اطلاعاتی صورت گرفت تحقیقات بود که در وزارت دفاع ایالات متحده پایه‌ریزی شد. در سال ۱۹۹۲ وزارت دفاع ایالات متحده پروژه‌ای تحقیقاتی با نام اختصاری TAFIM[1] را با این هدف آغاز نمود. در سال ۱۹۹٤ نیز وزارت دفاع ایالات متحده با انتشار بیانیه‌ای واحدهای تابعه‌ی خود را ملزم به اجرای نتایج TAFIM و انطباق سیستم‌های اطلاعاتی خود با آن نمود. تجربه‌ی وزارت دفاع مورد استقبال سایر وزارتخانه و مؤسسات دولتی فدرال قرار گرفت و روش‌ها و الگوهای به‌کار رفته درآن در سایر سازمان‌ها نیز به‌کار گرفته شد. در سال ۱۹۹٦ نیز قانون «کلینگر- کوهن» در کنگره‌ی ایالات متحده به تصویب رسید که مطابق آن همه‌ی وزارتخانه‌ها و سازمان‌های فدرال ایالات متحده ملزم به تنظیم معماری فناوری اطلاعات خود شدند. در این قانون معماری فناوری اطلاعات (معماری سازمانی) این چنین تعریف شده است (Kang et al., 2010):

«چارچوبی یکپارچه برای ارتقا و یا نگهداری فناوری موجود و کسب فناوری اطلاعاتی جدید برای نیل به اهداف راهبردی سازمان و مدیریت منابع آن»

پس از آن نیز با مورد توجه قرار گرفتن نتایج فعالیت‌های مذکور، سازمان‌های دولتی و خصوصی به انجام تحقیقات در این زمینه و توسعه‌ی چارچوب‌ها و مدل‌های معماری سازمانی پرداختند. معماری سازمانی با استفاده از مدل‌ها و تکنیک‌هایی استاندارد و شناخته شده اقدام به توصیف وضع موجود و وضع مطلوب سازمان می‌نماید. علاوه بر آن معماری سازمانی، حاوی طرح خاصی موسوم به طرح «گذار» می‌باشد که نحوه‌ی رسیدن از وضع موجود به وضع مطلوب یک سازمان را مشخص می‌کند. بنابراین، می‌توان معماری سازمانی را همچون طرحی دانست که بایستی بر اساس تحقیقاتی که برای دستیابی به اهداف کسب و کار و

1 - Technical Architecture Framework for Information Management (TAFIM)

فرآیندهای مورد نیاز سازمان تعریف و اجرا می‌شوند، سازمان را از وضع موجود به وضع مطلوب انتقال دهد (Mamaghani et al., 2012).

لزوم معماری سازمانی را می‌توان در ظهور سازمان‌های بزرگ، نیاز به طراحی و توسعه‌ی سیستم‌های اطلاعاتی پیچیده، ظهور سیستم‌های اطلاعاتی با منظورهای خاص و اهمیت انعطاف‌پذیری سازمان‌ها در برابر فشارهای بیرونی نظیر تغییر کسب و کار، تغییر مأموریت‌ها و ساختارهای سازمانی و تغییرات سریع فناوری ارزیابی کرد. «جان زکمن» انگیزه‌ی اصلی خود از ارائه‌ی معماری سازمانی را «حل مشکل مربوط به پیچیدگی سیستم‌های اطلاعاتی و بهبود مدیریت سازمان» می‌داند. وی پیچیدگی را نه فقط از جنبه‌ی بزرگ شدن سیستم‌ها بلکه مربوط به عوامل متعددی نظیر توزیع شدگی جغرافیایی سیستم‌ها، نیاز به تغییرات سریع سیستم‌ها به دلیل رشد سریع بازار تجارت، نیازمندی‌های خاص و کلیدی شدن جایگاه فناوری اطلاعات در سازمان‌ها می‌داند. به‌طور خلاصه، معماری در صورتی مورد نیاز است که یک یا چند مورد از شرایط ذیل در سیستم مورد نظر وجود داشته باشد: انعطاف‌پذیری، تولید سفارشی، طول عمر زیاد، بزرگ بودن سیستم، و پیچیدگی سیستم. در واقع، معماری سازمانی نگرشی کلان به مأموریت‌ها، وظایف سازمانی، فرآیندهای کاری، موجودیت‌های اطلاعاتی، شبکه‌های ارتباطی، سلسله مراتب و ترتیب انجام کارها در یک سازمان دارد (Zachman, 1997). به طور خلاصه، اهداف کلی در نظر گرفته شده در روش معماری سازمانی عبارتند از (Spewak, 1992):

- **بهبود روش‌ها و فرآیندها در مأموریت‌های سازمانی:** معماری اطلاعات با کشف و حذف فرآیندهای اضافی عملاً به مهندسی مجدد فرآیندها می‌پردازد.
- **کاهش پیچیدگی سیستم‌های اطلاعاتی:** معماری اطلاعات با تعریف معماری اطلاعات و حذف افزونگی در داده‌ها، پیچیدگی سیستم‌های اطلاعاتی را کاهش می‌دهد.
- **یکپارچگی:** معماری اطلاعات، با ایجاد استانداردهایی خاص، قواعدی برای به اشتراک‌گذاری داده‌ها فراهم می‌نماید. این امر امکان تبادل اطلاعات در سطوح مختلف و همچنین امکان انجام تغییرات را برای رسیدن به نتیجه‌ی مطلوب را تأمین می‌نماید.

از این طریق معماری مزایای بسیاری را برای سازمان به دنبال دارد که مهم‌ترین آنها عبارتند از (Kang et al., 2010):

- فراهم‌سازی و انعطاف‌پذیری لازم در برابر تغییرات محیطی؛
- تطبیق نیازمندی‌های لایه‌های مأموریتی و فناوری اطلاعات و ارتباطات؛
- کاهش میزان خطر پروژه‌های فناوری اطلاعات و ارتباطات؛
- فراهم شدن امکان کنترل و هدایت مؤثر سازمان؛
- مدیریت مؤثرتر تغییرات سازمانی؛
- فراهم شدن زمینه‌های ارزیابی تغییرات سازمانی؛
- کاهش هزینه و زمان توسعه‌ی سیستم‌های اطلاعاتی؛
- امکان استفاده از مؤلفه‌های سیستمی مشترک در سطح سازمان؛
- ایجاد زبان مشترک سازمانی؛
- امکان تعریف استانداردهای فناوری اطلاعات و ارتباطات؛
- ارتقا یا تجدید زیرساخت‌های فناوری اطلاعات و ارتباطات.

این اهداف، غالباً با پیاده‌سازی خروجی‌ها یا محصولات معماری سازمانی تأمین می‌گردد. این محصولات مجموعه‌ای از نقشه‌های فنی، نمودارها و مستنداتی هستند که به منظور تعریف مأموریت‌ها، تعیین اطلاعات و فناوری‌های لازم مورد نیاز و فرآیندهای انتقالی مورد نیاز برای راه‌اندازی فناوری‌های جدید مورد استفاده قرار می‌گیرد و از این طریق جنبه‌ها و لایه‌های مختلف معماری سازمانی توصیف می‌گردد. این خروجی‌ها و محصولات، حاصل به‌کارگیری چارچوب‌های معماری سازمانی می‌باشند. چارچوب‌های معماری سازمانی در واقع، قالب‌هایی هستند که در طی روند تکاملی معماری سازمانی از طرف مؤسسات خصوصی یا بخش‌های دولتی ارائه شده و از آنها می‌توان به عنوان راهنمایی جهت پیاده‌سازی معماری سازمانی استفاده نمود. هر چارچوب معماری بسته به ماهیت آن متناسب سازمان‌های خاصی بوده و معمولاً شامل توصیه‌های اجرایی نظیر نحوه‌ی تشکیل تیم معماری، فرآیند کلی معماری،

مشخصات محصولات معماری و توصیه‌های لازم برای استفاده از تکنیک‌های مدل‌سازی می‌باشد (Källgren et al., 2009).

چارچوب معماری وزارت دفاع ایالات متحده (DoDAF)

چارچوب معماری فرماندهی، کنترل، ارتباطات، کامپیوتر، جاسوسی، مراقبت و شناسایی[1] که در سال ۱۹۹۶ توسط وزارت دفاع ایالات متحده ارائه گردید، یکی مهم‌ترین چارچوب‌های معماری سازمان‌های دفاعی می‌باشد (Nimz, 2000; Wilczynski, 2007). از این رو، روش توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی بر مبنای تحلیل این چارچوب ارائه می‌گردد. این چارچوب در ابتدا، برای سیستم‌های ارتباطی، اطلاعاتی در صحنه‌ی عملیات نظامی تدوین شده بود و سپس جای خود را به عنوان یک راه‌حل ممتاز برای پرداختن به معماری در حوزه‌های دیگر باز کرد (Sowell, 2000). در سال ۲۰۰۳ وزارت دفاع ایالات متحده پس از توسعه‌ی دو نسخه از چارچوب معماری C4ISR، چارچوب معماری DoDAF را ارائه نمود. به عبارتی، چارچوب DoDAF نسخه به‌روزشده و تغییر نام یافته‌ی چارچوب C4ISR می‌باشد. حوزه‌ی کاربرد این چارچوب از فرماندهی، کنترل، ارتباطات، کامپیوتر، جاسوسی، مراقبت و شناسایی، به تمامی حوزه‌ها توسعه یافته است. در آوریل ۲۰۰۷ نیز بر اساس تجربیات حاصل از به‌کارگیری DoDAF نسخه‌ی ۱.۵ آن در سه جلد به‌همراه یک کتاب کار ارائه گردید (Department of Defense, 2007). نسخه‌ی ۱.۵ این چارچوب دارای ویژگی‌های زیر می‌باشد:

۱) بهبود و ارتقا در راستای تأکید و توجه به معماری سرویس‌گرا؛
۲) پشتیبانی بیشتر از مدیریت معماری داده – مدار؛
۳) ارائه‌ی رهنمودها و مثال‌های بیشتر جهت تأکید و توجه بیشتر بر توسعه و استفاده از معماری سازمانی هم‌راستا با معماری‌های وزارت دفاع و دولت فدرال؛

1 – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR)

٤) ساده و مؤثر نمودن فرآیند توسعه‌ی معماری برای فراهم ساختن چابکی بیشتر؛

۵) تأکید بر دیگر مباحث معماری نظیر امنیت، مهندسی سیستم، ابزارها، و روش؛

چارچوب معماری DoDAF شامل ۲ لایه می‌باشد: لایه‌ی داده و لایه‌ی ارائه. لایه‌ی داده دربرگیرنده‌ی عناصر داده و ویژگی‌ها و ارتباطات بین آنها است. در لایه‌ی ارائه، محصولات و دیدهایی قرار دارند که ابزارهای بصری را برای تبادل و درک هدف معماری و این‌که معماری چه چیز را تشریح می‌نماید و تحلیل‌های معماری انجام شده را پشتیبانی می‌نمایند. محصولات روشی را برای بصری نمودن داده‌های معماری فراهم می‌نمایند. دیدها نیز توانایی بصری نمودن داده‌های معماری که در محصولات مختلف ریشه دارند را فراهم می‌نمایند. به‌طوری که داده‌ها را به‌طور منطقی از یک دیدگاه کلی و یا دیدگاه خاص سازماندهی می‌نمایند.

چارچوب معماری DoDAF چارچوبی زیربنایی را برای توسعه و ارائه‌ی توصیف‌های معماری فراهم می‌نماید. از این طریق، زبان مشترکی برای درک، مقایسه، و یکپارچه‌سازی معماری‌ها در طول مرزهای سازمانی و بین‌المللی ایجاد می‌گردد. این چارچوب، محصولات معماری را در چهار دید تقسیم‌بندی نموده است. دیدگاه عملیاتی، دیدگاه سیستم‌ها و خدمات، دیدگاه استانداردهای فنی، دیدگاه همه دیدها.

دیدگاه عملیاتی: دیدگاه عملیاتی گره‌های عملیاتی، وظایف و فعالیت‌های انجام شده، و اطلاعاتی که برای انجام مأموریت وزارت دفاع بایستی تبادل شود را گردآوری می‌نماید. این مجموعه انواع اطلاعاتی که باید تبادل شوند، فراوانی تبادلات، وظایف و فعالیت‌هایی که با تبادل اطلاعات پشتیبانی می‌شوند، و ماهیت تبادل اطلاعات را شامل می‌شود.

دیدگاه سیستم‌ها و خدمات: این دیدگاه سیستم‌ها، خدمات، کارکردهای ارتباطی فراهم شده، و فعالیت‌های عملیاتی پشتیبان را در بر می‌گیرد. کارکردهای سیستمی و منابع و اجزای خدمات در این دیدگاه می‌توانند با خروجی‌های معماری دیدگاه عملیاتی مرتبط شوند. کارکردهای سیستمی و منابع خدمات فعالیت‌های عملیاتی را پشتیبانی نموده و تبادل اطلاعات بین گره‌های عملیاتی را تسهیل می‌نمایند.

دیدگاه استانداردهای فنی: این دیدگاه مجموعه‌ی کوچکی از دستورات و قوانین است که بر ترتیب، تعامل، و وابستگی‌های متقابل اجزای سیستم حاکم است و تضمین می‌نماید که مجموعه‌ای خاص از نیازمندی‌های عملیاتی توسط سیستم تأمین گردیده است. دیدگاه استانداردهای فنی رهنمودهای فنی را برای پیاده‌سازی سیستم‌ها ارائه می‌نماید که بر اساس آن، مشخصات مهندسی پایه‌ریزی شده، اجزای تشکیل‌دهنده‌ی اصلی بنا نهاده شده، و خطوط تولید توسعه می‌یابند. همچنین این دیدگاه شامل مجموعه‌ای از استانداردهای فنی، اصول پیاده‌سازی، جایگزین‌های استاندارد، و قوانینی می‌باشد که بر سیستم‌ها و یا اجزای خدمت و سیستم در یک معماری خاص حاکم می‌باشد.

دیدگاه همه‌ی دیدها: در هر معماری برخی جنبه‌های فراگیر وجود دارند که به هر سه دیدگاه مربوط می‌شوند. این موارد در دیدگاه همه‌ی دیدها گردآوری شده‌اند. محصولات این دیدگاه اطلاعات مربوط به کلیت معماری فراهم می‌نمایند و یک دیدگاه معماری مجزا را تشکیل نمی‌دهند. این محصولات، حوزه و زمینه‌ی معماری را مشخص می‌نمایند. حوزه‌ی معماری شامل محدوده‌ی موضوعی و دوره‌ی زمانی معماری می‌باشد. این امر خود متأثر از شرایطی است که بستگی به عواملی نظیر دکترین، تاکتیک، تکنیک، رویه‌ها، اهداف و چشم‌انداز مربوطه، ایده‌ی کلی عملیات، سناریوها و شرایط محیطی دارد.

روش‌شناسی تحقیق

همان‌طور که در مقدمه ذکر گردید، مستندات چندانی در زمینه‌ی روش توسعه‌ی چارچوب‌های معماری وجود ندارد (Kim, et al., 2006). از طرفی اهمیت توسعه‌ی چارچوب‌های معماری برای حوزه‌ی دفاعی موجب گردیده تا این تحقیق در پاسخ به این سؤال اصلی به انجام رسد: چگونه می‌توان به توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی پرداخت؟

در پاسخ به این سؤال، روشی برای توسعه چارچوب‌های معماری سازمان‌های دفاعی تدوین گردیده است. برای این منظور، مراحل زیر در این تحقیق طی شده است:

۱) بررسی ادبیات معماری سازمانی؛
۲) بررسی چارچوب‌های معماری حوزه‌ی دفاعی؛
۳) بررسی ادبیات توسعه‌ی چارچوب‌های معماری سازمانی؛
٤) بررسی چارچوب‌های معماری حوزه‌ی دفاعی از دیدگاه روش توسعه؛
۵) تدوین روش توسعه‌ی چارچوب معماری سازمان‌های دفاعی؛
٦) ارائه‌ی نتایج به خبرگان معماری سازمانی در حوزه‌ی دفاعی کشور برای اعتبارسنجی روش پیشنهادی، دریافت نظرات، انجام اصلاحات و ارائه‌ی روش نهایی توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی.

در انجام این تحقیق، که از نوع تحقیقات کیفی می‌باشد، ابتدا یک‌سری مطالعات بر اساس منابع کتابخانه‌ای و الکترونیکی در حوزه‌های مربوطه صورت می‌گیرد. این حوزه‌ها شامل مباحث مرتبط با معماری سازمانی، چارچوب‌های معماری به‌کارگرفته شده در حوزه‌ی نظامی، نحوه‌ی توسعه این چارچوب‌ها، ذی‌نفعان، کارگروه‌ها، و متخصصین مشارکت‌کننده در توسعه‌ی این چارچوب‌ها می‌باشد. سپس با استفاده از اطلاعات کسب شده به تدوین روش توسعه‌ی چارچوب معماری سازمان‌های دفاعی پرداخته و نهایتاً نتایج حاصله برای اعتبارسنجی به خبرگان این حوزه ارائه گردیده است.

مسأله قابل توجه در این تحقیق، نحوه‌ی دستیابی به شناخت درباره‌ی روش توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی می‌باشد. به دلیل آن‌که سازمان‌های توسعه‌دهنده‌ی چارچوب‌های معماری حوزه‌ی دفاعی از ارائه‌ی اطلاعات در زمینه‌ی روش توسعه‌ی این چارچوب‌ها اجتناب نموده‌اند، این یکی از بهترین راه‌های شناخت درباره‌ی روش توسعه‌ی این چارچوب‌ها، بررسی محتوای چارچوب‌ها و ارائه‌ی استنتاجاتی درباره‌ی نحوه‌ی شکل‌گیری آنها می‌باشد. به عبارتی، تفسیر چارچوب‌های موجود، یکی از بهترین شیوه‌های حصول شناخت درباره‌ی روش توسعه‌ی آنها می‌باشد. از این رو، پارادایم حاکم بر این تحقیق پارادایم تفسیری[1] است. به زعم «بورل» و «مورگان»[2]

1 – Hermeneutic
2 – Burrell and Morgan

(۱۹۷۹) این پارادایم مبتنی بر ذهنی‌گرایی و ثبات (نظم) بوده (شکل شماره‌ی ۱) و نسبت به پارادایم کارکردگرایی سهم کمتری در مطالعات سازمان داشته است.

شکل شماره‌ی ۱ – پارادایم‌های تحقیق (Burrell & Morgan, 1979)

پارادایم تفسیرگرایی بر مبنای نگرشی است که افراد واقعیت‌های اجتماعی را به صورت اجتماعی و نمادین می‌سازند. هدف نظریه‌سازی در پارادایم تفسیرگرایی خلق توصیف‌ها، بینش‌ها و تفسیرهایی از وقایع می‌باشد. بنابراین، سیستمی از تفسیرها و معنی‌دهی در ساختاردهی و سازماندهی فرآیندها منعکس می‌شود. نظریه‌سازی در پارادایم تفسیرگرایی ماهیتاً استقرایی می‌باشد. محققان تفسیرگرا داده‌های مرتبط را گردآوری می‌کنند، تجزیه و تحلیل همراه با گردآوری داده‌ها انجام می‌شود و معمولاً از رویه‌های کدبندی در جهت پی‌بردن به الگوها و روندها استفاده می‌شود. فرآیندهای تحلیل، نظری‌پردازی و گردآوری داده‌های بیشتر، همراه هم انجام می‌شوند. فرآیند نظریه‌پردازی در این پارادایم، یک فرایند تکراری، گردشی و غیرخطی می‌باشد (Myers, 2009). «جیویا» و «پیتره» (۱۹۹۰) به نقل از «بورل» و «مورگان» (۱۹۷۹) روش کلی تحقیق در پارادایم تفسیرگرایی را به صورت نشان داده شده در جدول شماره‌ی ۱ معرفی نموده‌اند.

جدول شماره‌ی ۱- مراحل نظریه‌پردازی در پارادایم تفسیرگرایی

مرحله‌ی آغازین	انتخاب یک موضوع تدوین طرح تحقیق
گردآوری اطلاعات	تعیین یک مورد برای بررسی موضوع در آن گردآوری اطلاعات به کمک ابزارهای مربوطه
تحلیل	کدگذاری فرموله نمودن ارتباطات بین کدهای گوناگون اعتبارسنجی ارزیابی ارتباطات فرموله نمودن نظریه مرور ادبیات جهت تحلیل نظریه شکل گرفته
نظریه‌پردازی	تدوین نظریه نهایی و انتشار آن

در بین روش‌های مختلف تحقیق، روش نظریه‌ی زمینه‌ای[1] بیشترین شباهت را به مراحل ذکر شده در جدول شماره‌ی ۱ دارد. از این رو، روش تحقیق به‌کارگرفته شده در این تحقیق، روش نظریه‌ی زمینه‌ای می‌باشد. روش نظریه‌ی زمینه‌ای ریشه در داده‌هایی مفهومی دارد که به شکلی نظام‌مند گردآوری و تحلیل شده‌اند. برخی محققین، این روش را نوعی نظری استقرایی معرفی نموده‌اند (Glaser and Strauss, 1967). این روش، در مواردی بیشترین کاربرد را دارد که نظریه‌ی قابل توجهی در حوزه‌ی موضوعی مورد نظر موجود نبوده و پژوهشگر در حوزه‌ی موضوعی مورد نظر تقریباً خالی الذهن است. روش‌شناسی این نظریه این اجازه را به پژوهشگر می‌دهد که مبنای نظریه را از ویژگی‌های عمومی یا کلی یک موضوع که هم‌زمان ریشه در مشاهدات یا داده‌های تجربی دارد، ارائه داده و بر مبنای مفاهیم اصلی حاصل از داده به ارائه‌ی نظریه بپردازد. از این رو، این روش در ارائه‌ی توصیف‌ها و تبیین‌های مبنی بر بستر پدیده‌ها

1 – Grounded Theory

بسیار مفید است. در این روش، نظریه از مفهوم‌سازی داده‌ها شکل می‌گیرد و نه از داده‌های عینی (Pandit, 1996). این روش تحقیق متشکل از مراحل زیر می‌باشد:

۱) تدوین پرسش‌های پژوهش؛

۲) گردآوری داده‌ها؛

۳) کدگذاری داده‌ها در سه مرحله‌ی کدگذاری باز، کدگذاری محوری و کدگذاری انتخابی؛

٤) نوشتن یادداشت تحلیلی: ثبت اندیشه‌ها و تفسیر خود از داده‌ها؛

۵) نگارش و تدوین نظری و اعتبارسنجی آن (Strauss and Corbin, 1990).

تحلیل DoDAF برای دستیابی به روش توسعه‌ی آن

همان‌طور که ذکر شد به منظور دستیابی به شناخت در زمینه‌ی روش توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی، چارچوب DoDAF مورد تحلیل و بررسی قرار گرفته است. برای این منظور، چهار نسخه از چارچوب DoDAF تحلیل شده است. لیست نسخه‌های مورد بررسی در جدول شماره‌ی ۲ ذکر گردیده است.

جدول شماره‌ی ۲- نسخه‌های مختلف DoDAF که مورد بررسی و تحلیل قرار گرفته است

C4ISR Architecture Framework v.1.0 (C4ISR ITF Integrated Architectures Panel, 1996)
C4ISR Architecture Framework v.2.0 (C4ISR Architecture Working Group, 1997)
DOD Architecture Framework v.1.0 (Department of Defense, 2004)
DOD Architecture Framework v.1.5 (Department of Defense, 2007)

چارچوب معماری DoDAF که اولین نسخه‌ی آن در سال ۲۰۰۳ ارائه گردید، نسخه توسعه‌یافته از چارچوب C4ISR می‌باشد (Hartt, 2000). از این رو، در این فصل ابتدا نسخه‌ی ۱.۰ و ۲.۰ چارچوب C4ISR از دیدگاه روش توسعه بررسی شده و سپس نسخه‌های موجود از چارچوب DoDAF تحلیل می‌گردد. این تحلیل در ابعاد ذیل به انجام می‌رسد:

- محرک‌های توسعه‌ی چارچوب؛
- هدف و مقصود از توسعه‌ی چارچوب؛
- اصول توسعه‌ی چارچوب؛

- مراحل توسعه‌ی چارچوب.

چارچوب C4ISR v.1.0

محرک‌های توسعه‌ی چارچوب:

- اهداف وزارت دفاع ایالات متحده در راستای توسعه‌ی معماری حوزه‌ی دفاعی ایالات متحده؛
- ایجاد دیدگاه و روشی مشترک جهت توسعه و ارائه‌ی معماری‌ها؛
- تسهیل به‌کارگیری مجدد اطلاعات معماری؛
- سیاست‌ها و دستورالعمل‌های وزارت دفاع ایالات متحده؛

هدف و مقصود از توسعه‌ی چارچوب:

- تعریف یک روش هماهنگ برای توسعه، ارائه، و یکپارچه‌سازی C4ISR؛
- ایجاد پایه و اساس مشترک برای درک، مقایسه و یکپارچه‌سازی معماری‌ها؛
- پشتیبانی از عملیات جنگی؛
- یکپارچه‌سازی و ایجاد تعامل میان معماری‌های بخشی؛
- ایجاد تعامل مؤثر میان نیروهای جنگی و طراحان و توسعه‌دهندگان سیستم؛
- ایجاد هم‌راستایی میان اهداف راهبردی و فرآیندها و اجزای سیستم؛
- ایجاد محیط یکپارچه C4ISR و ایجاد یکپارچگی در بین قابلیت‌های C4ISR؛
- تسهیل توسعه راه‌کارهای مشترک؛
- ارتقای سازگاری و انجام عملیات مشترک؛
- ایجاد دیدگاه و روش مشترک در توسعه‌ی معماری‌های بخش‌های مختلف.

اصول توسعه‌ی چارچوب:

- قابلیت انجام فعالیت اشتراکی و دسته‌جمعی جهت توسعه‌ی چارچوب؛
- توسعه‌ی چارچوب با دیدگاه محصول – مدار؛
- قابلیت توسعه جهت کاربرد در معماری دیگر حوزه‌ها؛
- انعطاف‌پذیری.

مراحل توسعه‌ی چارچوب:

- تحلیل وضع موجود؛
- ایجاد ساختار و مکانیزم‌های حاکمیتی چارچوب متناسب با ابعاد مختلف مسأله؛
- توسعه‌ی تکاملی چارچوب؛
- حصول توافق درباره‌ی مفاهیم زیربنایی؛
- استفاده از تجربیات حاصل از تلاش‌های قبلی.

چارچوب C4ISR v.2.0

محرک‌های توسعه‌ی چارچوب

- تعیین یک چارچوب هماهنگ و منسجم برای توسعه، ارائه، و یکپارچه‌سازی C4ISR؛
- ایجاد ابزار و وسیله‌ای که تضمین‌کننده‌ی سیستم‌های دفاعی تعاملی و مقرون به صرفه باشد؛
- محرک‌های قانونی؛
- سیاست‌ها و راهبردها؛
- لزوم ارزیابی عملکرد سیستم‌های اطلاعاتی سازمان‌های دفاعی.

هدف و مقصود از توسعه‌ی چارچوب:

- تضمین این‌که معماری‌های بخشی در دیدهای مختلف دارای ارتباطات متقابل بوده و در مرزهای سازمانی مشترک و چند ملیتی قابلیت مقایسه و یکپارچه شدن را دارند.
- افزایش قابلیت‌های عملیاتی از طریق ایجاد امکان ترکیب و تفسیر سریع نیازمندی‌ها و مهندسی مؤثر سیستم‌های جنگی

اصول توسعه‌ی چارچوب:

- اصل تکاملی بودن توسعه‌ی چارچوب؛
- استانداردسازی و طبقه‌بندی محصولات معماری؛
- ایجاد تعامل بین معماری‌های بخشی؛
- شروع کار با ارائه‌ی روش‌های محصول – مدار و حرکت به سمت روش‌های داده – مدار.

مراحل توسعه‌ی چارچوب:

- ایجاد ساختار و مکانیزم‌های حاکمیت توسعه‌ی چارچوب معماری.

چارچوب DoDAF v.1.0

محرک‌های توسعه‌ی چارچوب:

- سیاست‌های دولت فدرال؛
- سیاست‌های وزارت دفاع؛
- سیاست‌های ستاد مشترک؛
- الزامات سازمانی.

هدف و مقصود از توسعه‌ی چارچوب:

- تعریف یک روش هماهنگ برای توسعه، ارائه، و یکپارچه‌سازی C4ISR.

اصول توسعه‌ی چارچوب:

- توجه بیشتر به اهداف توسعه‌ی چارچوب و انتظارات از آن؛
- تمرکز بر عناصر داده (دیدگاه داده – مدار)؛
- توسعه‌ی مشارکتی چارچوب و تلاش برای تسهیل این امر.

مراحل توسعه‌ی چارچوب:

در مستندات چارچوب DoDAF v.1.0 اشاره‌ای به مراحل توسعه‌ی چارچوب نشده است.

چارچوب DoDAF v.1.5

محرک‌های توسعه چارچوب:

- لزوم ایجاد سیستم‌های دفاعی با قابلیت انجام تعاملی عملیات؛
- لزوم ایجاد سیستم‌های دفاعی که اثربخشی هزینه‌ای داشته باشند؛
- محرک‌های قانونی؛

- محرک‌های مبتنی بر سیاست‌ها؛
- لزوم مدیریت مؤثر سازمان‌های دفاعی (بزرگ) ایالات متحده؛
- پشتیبانی از فناوری‌های جدید؛
- ایجاد ارتباطات شبکه‌ای بین سازمان‌های دفاعی؛
- امکان‌پذیر نمودن و پشتیبانی از جنگ‌های مبتنی بر اطلاعات و شبکه محور.

هدف و مقصود از توسعه‌ی چارچوب

- متحد نمودن معماری‌های بخشی: این امر یکی از اهداف اساسی در توسعه‌ی DoDAF می‌باشد. به‌دلیل وجود معماری‌های بخشی که در بخش‌های مختلف سازمان‌های دفاعی ایالات متحده و در سطوح مختلف توسعه یافته‌اند، DoDAF به جای ایجاد تحولات پایه‌ای در این معماری‌های بخشی، بر اساس استفاده‌ی بهینه از معماری‌های بخشی موجود و ایجاد تعامل مؤثر میان آنها طراحی گردیده است. از این رو، DoDAF پشتیبانی از هر دو نوع معماری متحد و یکپارچه را در مورد توجه قرار داده است. هر چند که به‌دلیل وجود معماری‌های بخشی تمرکز بیشتری بر معماری متحد شده است.
- پشتیبانی از فرآیند تصمیم‌گیری در سازمان‌های دفاعی به‌ویژه در محیط رزم مبتنی بر شبکه[1].

اصول توسعه چارچوب

- هم‌راستایی چارچوب با چشم‌انداز وزارت دفاع؛
- اتخاذ دیدگاه داده – مدار؛
- انطباق با DoDAF v.1.0؛
- پشتیبانی از معماری متحد و یکپارچه: یکی از اصول مهم در طراحی این چارچوب مفاهیم معماری یکپارچه[2] و توزیع شده[3] می‌باشد. متحد و یا یکپارچه بودن مربوط به معماری سازمان است. اما ملاحظات مربوط به آن بایستی در چارچوب معماری

1 - Net-centric Warfare
2 - Integrated
3 - Federated

دیده شود. چارچوب DoDAF طوری توسعه یافته است که ملاحظات مربوط بـه هـر دو نوع معماری در آن دیده شده است. در نسخه‌ی بعـدی DoDAF پـیش‌بینـی شـده است که چارچوب هر دو نوع معماری را پوشش دهد.

- توجه بیشتر به معماری سرویس‌گرا؛
- ارائه‌ی رهنمودهای بیشتر جهت تشریح تغییرات ایجاد شده در محیط، فرهنگ، دکترین، و فرآیندها؛
- چابکی بیشتر در توسعه‌ی معماری سازمان؛
- انطباق با رزم مبتنی بر شبکه؛
- اثربخشی و انعطاف بیشتر؛

مراحل توسعه‌ی چارچوب

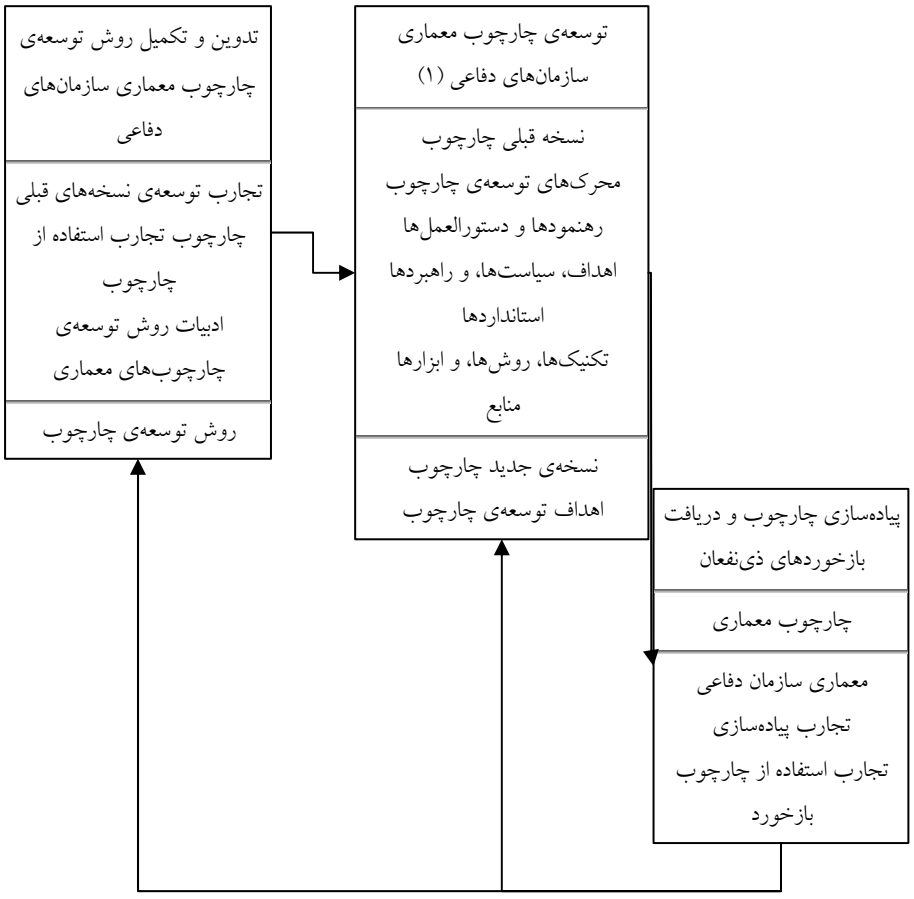
با توجه به توضیحات و تفاسیری که در مستندات DoDAF قید گردیـده اسـت، مـی‌تـوان برخی مراحل و فعالیت‌های انجام شده جهت توسعه‌ی این را شناسایی نمود.

- برای توسعه‌ی DoDAF پانل، هیأت‌ها و کارگروه‌های مختلفی تشکیل گردیـده اسـت. در واقع، در رابطه با هر یک از دیدگاه‌ها، ابعاد و موضوعات کلیدی کـه در حـوزه‌ی معماری مطرح بوده و مورد توجه توسعه‌دهندگان چارچوب بوده است، کـارگروهی خاص جهت بررسی تخصصی موضوعات مورد نظر شکل گرفته است.
- به نظر می‌رسد که این کارگروه‌ها غالباً کارگروه‌های دائمی هستند که در طـی توسـعه‌ی نسخه‌های مختلف DoDAF، بخش‌هایی از چارچوب را که مرتبط بـا موضـوعات کـاری آنان است، در تعامل با دیگر کارگروه‌ها و ذی‌نفعان، بروزرسانی می‌نمایند.
- در راستای توسعه‌ی DoDAF کارگاه‌های اشتراکی متعددی با دو هدف اصلی برپا شده است. یکی از اهداف کسب اطلاعات مورد نیاز از ذی‌نفعان است و دیگری آموزش، جلب توجه و حصول توافق آنان. این امـر تـأثیر بـه‌سـزایی بـر موفقیـت چـارچوب معماری در مرحله‌ی توسعه و همچنین در مرحله‌ی به‌کارگیری دارد.
- تعیین ساختار و مکانیزم‌های حاکمیتی چارچوب معماری و اجزای مختلف آن؛
- تحلیل وضع موجود؛

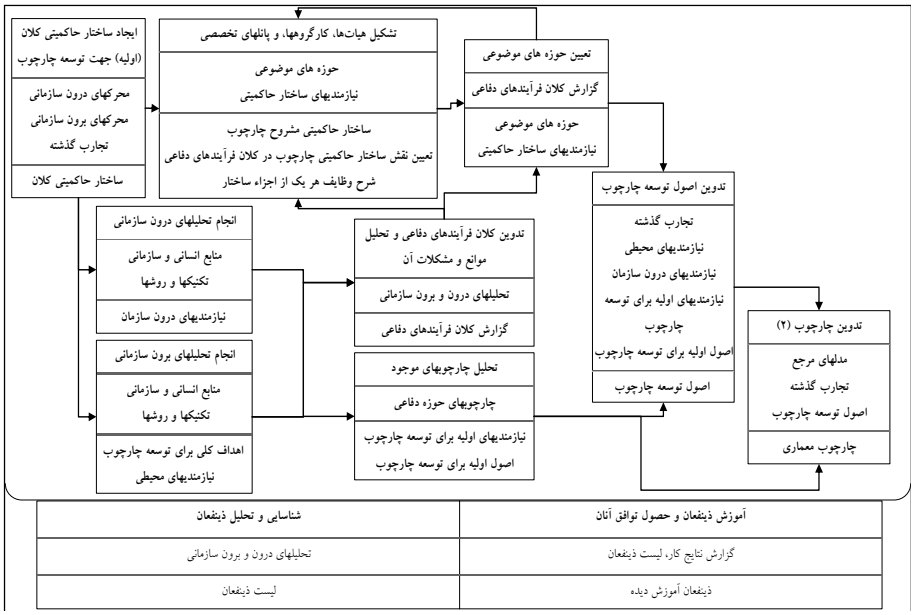
- بهره‌گیری از نظرات ذی‌نفعان و تجربیات حاصل از به‌کارگیری معماری سازمانی در سازمان‌های نظامی ایالات متحده؛
- اتخاذ دیدگاه و رویکرد متناسب برای توسعه‌ی چارچوب با توجه به کاربرد و هدف آن؛
- حصول توافق با ذی‌نفعان درباره اجزا و عناصر چارچوب معماری در راستای دستیابی به اهداف؛
- استقرار فرآیند بازخور گسترده به منظور ارتقا و بروزرسانی چارچوب؛
- تعامل نزدیک، مستمر و بلند مدت با ذی‌نفعان (۱۰ سال)؛
- شناسایی محتوای داده سازمان‌های دفاعی و ایجاد درک مشترک درباره‌ی آن؛
- ایجاد و توافق بر روی فرا – داده ساختاریافته جهت استفاده در اجزای داده چارچوب DoDAF؛
- ایجاد و به‌کارگیری ابزارهای پشتیبان جهت توسعه‌ی چارچوب و یکپارچه‌سازی آنها با دیگر برنامه‌های کاربردی.

روش پیشنهادی برای توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی

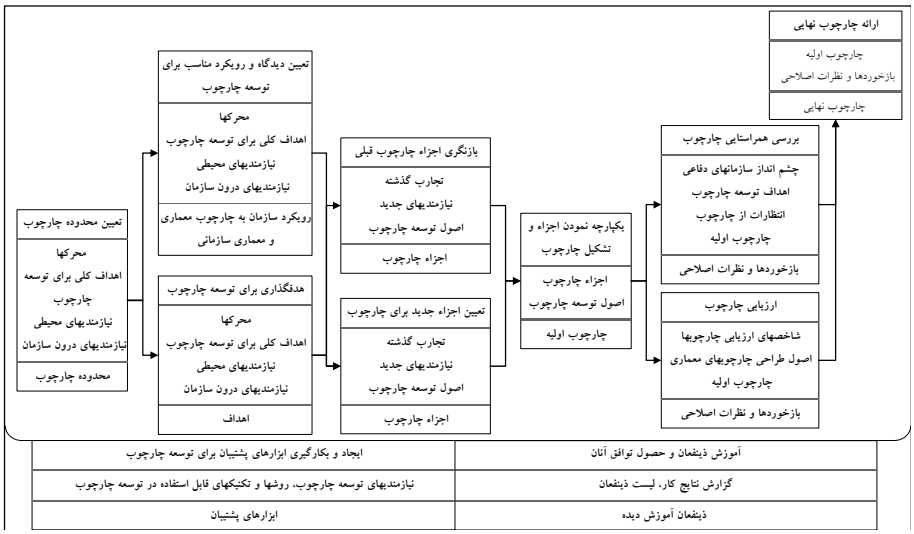
با توجه به مباحث ارائه شده در بخش‌های قبل می‌توان روش توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی را تدوین نمود. این روش در قالب نمودارهای ارائه شده در شکل‌های شماره‌ی ۲، ۳ و ٤ به صورت فرآیندهای توسعه‌ی چارچوب‌های معماری ارائه گردیده است. مدل‌سازی فرآیندهای مربوطه به گونه‌ای انجام شده که در قسمت بالای هر جزء فرآیند (اجزای مستطیل شکل) نام آن فرآیند، در قسمت میانی هر فرآیند ورودی‌ها و در قسمت پائینی، خروجی‌های آن قید شده است.



شکل شماره‌ی ۲ – کلان فرآیند توسعه‌ی چارچوب معماری سازمان‌های دفاعی



شکل **شماره‌ی ۳ – توسعه‌ی چارچوب معماری سازمان‌های دفاعی**



شکل شماره‌ی ٤ – تدوین چارچوب

اعتبارسنجی

همان‌طور که ذکر شد این تحقیق از نوع تحقیقات کیفی است. از طرفی تجارب اندکی در زمینه‌ی روش توسعه‌ی چارچوب‌های معماری سازمانی در سطح کشور وجود دارد و از این رو، تعداد خبرگان این حوزه محدود می‌باشد. بنابراین، برای اعتبارسنجی نتایج تحقیق، روش دلفی مورد استفاده قرار می‌گیرد. «گلاسر» و «استراوس» (Glaser and Strauss, 1967) که طراحان روش تحقیق نظری زمینه‌ای هستند، بیان نموده‌اند که تحقیقاتی که به این روش انجام می‌شود، بایستی با چهار شاخص متناسب بودن[1]، مرتبط بودن[2]، عملی بودن[3]، و تغییرپذیر بودن[4] اعتبارسنجی شوند. مفهوم هر یک از این شاخص‌ها با توجه به این تحقیق به شرح زیر می‌باشد:

۱) **متناسب بودن:** این شاخص بیان می دارد که مفاهیم بیان شده در روش تا چه حد با وقایع و پدیده‌هایی که توسط آن مفاهیم بیان می‌شوند تناسب دارند.

۲) **مرتبط بودن:** هنگامی روش مذکور، مرتبط محسوب می‌گردد که بتواند خواسته‌های مشارکت‌کنندگان و ذی‌نفعان را مورد توجه قرار دهد.

۳) **عملی بودن:** روش مذکور زمانی عملی است که بتواند تشریح کند که چه وقایعی رخ داده، پیش‌بینی کند که چه رخ خواهد داد، و تفسیر کند که چه چیزی در حال وقوع است. روش مذکور بایستی شرایطی را مطرح کند که تحت آن شرایط، روش پیشنهادی به‌کار می‌رود و مبنای معقولی برای اقدام عملی توصیف می‌کند.

٤) **تغییر پذیر بودن:** روش مذکور زمانی تغییرپذیر است که داده‌های مرتبط جدید بتواند باعث تغییر روش مذکور شود. این امر می‌تواند موجب تعمیم روش مذکور گردد.

از این رو، برای اعتبارسنجی نتایج تحقیق پرسشنامه‌ای طراحی گردید و بین خُبرگان حوزه‌ی معماری سازمانی توزیع شد و در نهایت به ۱۱ پرسشنامه پاسخ داده شد. سپس

1 - Fit
2 – Relevance
3 - Workable
4 - Modifiable

امتیازات داده شده به شاخص‌ها توسط نرم‌افزار SPSS تحلیل گردید و نتایج تحلیل در جدول شماره‌ی ۳ مشاهده می‌شود. نتایج حاصله نشان‌دهنده‌ی تأیید شدن شاخص‌ها در سطح ۵٪ (و به‌عبارتی تأیید شدن روش پیشنهادی) می‌باشد.

جدول شماره‌ی ۳ – نتایج تحلیل آماری

		Category	N	Observed Prop.	Test Prop.	Exact Sig. (1-tailed)
Fit	Group 1	<= 3	5	.5	.6	.247[a]
	Group 2	> 3	6	.5		
	Total		11	1.0		
Relevance	Group 1	<= 3	4	.4	.6	.099[a]
	Group 2	> 3	7	.6		
	Total		11	1.0		
Workable	Group 1	<= 3	5	.5	.6	.247[a]
	Group 2	> 3	6	.5		
	Total		11	1.0		
Modifiable	Group 1	<= 3	4	.4	.6	.099[a]
	Group 2	> 3	7	.6		
	Total		11	1.0		

نتیجه‌گیری

تجربیات سازمان‌های دفاعی ایالات متحده و بریتانیا نشان می‌دهد که به دلیل اهمیت و حساسیت حوزه‌ی دفاعی، مبحث معماری سازمانی به طور کاملاً جدی در این حوزه اعمال و پیگیری می‌شود. سازمان‌های دفاعی بزرگ غالباً به توسعه‌ی چارچوب‌های معماری سازمانی خاص خود می‌پردازند و از به‌کارگیری چارچوب‌های رایج اجتناب می‌نمایند. این تحقیق بر اساس تحلیل چارچوب C4ISR/DoDAF به تدوین روشی برای توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی پرداخته است.

بررسی چارچوب C4ISR نشان می‌دهد که نسخه‌ی دوم این چارچوب پیشرفت قابل ملاحظه‌ای نسبت به نسخه قبلی آن داشته است. نسخه‌های بعدی چارچوب C4ISR/DoDAF نیز با تأثیرپذیری از تغییرات محیطی به‌ویژه تغییرات فناورانه، پیوسته ارتقا یافته‌اند. به‌طوری‌که در توسعه‌ی نسخه‌ی ۱.۵ چارچوب DoDAF زیرساخت‌های قابل توجهی فراهم بوده است و توسعه‌دهندگان آن توجه خود را بر روی مسائلی نظیر متحد و یکپارچه بودن معماری،

پشتیبانی چارچوب از قابلیت‌های مبتنی بر شبکه، توسعه‌ی چارچوب داده – مدار، و توسعه‌ی ابزارهای پشتیبان متمرکز نموده‌اند. وجود معماری‌های بخشی که به سطح نسبتاً قابل قبولی از بلوغ رسیده‌اند، باعث گردیده است تا DoDAF فارغ از پرداختن به جزئیات معماری‌های بخشی، بر توزیع شده بودن معماری و استفاده مؤثر از معماری‌های بخشی و همچنین ایجاد تعامل میان آنها متمرکز باشد.

از دیگر زیرساخت‌های قابل توجهی که در توسعه‌ی این چارچوب فراهم بوده است. وجود اسناد مربوط به اهداف، سیاست‌ها، رهنمودها و استانداردها می‌باشد. مسلماً هر نوع سند مربوط به اهداف، سیاست‌ها، رهنمودها و استانداردها نمی‌تواند به‌عنوان یک ورودی معتبر برای توسعه‌ی چارچوب مورد استفاده قرار گیرد. بلکه اسنادی معتبر شمرده می‌شوند که از لحاظ عملی مورد توافق ذی‌نفعان اصلی چارچوب باشد. از این رو، ضروری است در توسعه‌ی چارچوب معماری حوزه‌ی دفاعی کشور در اسناد مربوط به اهداف، سیاست‌ها، رهنمودها و استانداردها بازنگری شود تا از هم‌رأیی و توافق نظر و تعهد ذی‌نفعان اصلی نسبت به آنها اطمینان حاصل گردد. عدم توافق و تعهد ذی‌نفعان اصلی نسبت به زیرساخت‌ها و ورودی‌های توسعه‌ی چارچوب و نسبت به خود چارچوب می‌تواند مقدمات شکست اجرایی چارچوب معماری سازمان‌های دفاعی کشور را فراهم نماید. در مجموع روش ارائه شده در این مقاله می‌تواند از طریق مواردی همچون با کاهش زمان توسعه‌ی چارچوب، کاهش ریسک، کاهش هزینه، مدیریت بهتر توسعه چارچوب، موجبات توسعه موفقیت‌آمیز چارچوب معماری سازمان‌های دفاعی کشور را فراهم آورد.

منابع

انگلیسی

1- Allega P. (2004), "***Yes Virginia, There is Enterprise Architecture***", Meta Group.

2- Burrell, G., and Morgan (1979), "***G. Sociological Paradigms and Organizational Analysis***", Heinemann.

3- C4ISR Architecture Working Group (AWG) (1997), "***C4ISR Architecture Framework Version 2.0***", 18December.

4- C4ISR ITF Integrated Architectures Panel (1996), "***C4ISR Architecture Framework Version 1.0***", Available online at http://fas.org/irp/doddir/dod/c4isr/index.htm.

5- Department of Defense (2004), "***DoD Architecture Framework Version 1.0***".

6- Department of Defense (2007), "***DoDAF 1.5 Volume 1.***" ,Available online at http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_I.pdf, Volume 2. Available online at http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_II.pdf, Volume 3. Available online at http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_III.pdf.

7- Gioia, D.A. and Pitre, E. (1990), "***Multi-paradigm perspectives on theory building. Academy of Management Review***", 15, 584-602.

8- Glaser, B. G., Strauss, A. L. (1967), "***The discovery of grounded theory***", Chicago, Aldine.

9- Hartt, M. B. (2000), "***DOD Architecture Framework Ececutive Seminar***", Air Force Institute of Technology.

10- Institute for Enterprise Architecture Developments, (2005), "***Trends in Enterprise Architecture 2005: How are Organizations Progressing?***"

11- Jafari, M., Akhavan, P. and Nouranipour, E. (2009), "***Developing an architecture model for enterprise knowledge An empirical study based on the Zachman framework in Iran***", Management Decision, Vol. 47 No. 5, pp. 730-759.

12- Källgren, A., Ullberg, J., and Johnson, P. (2009), "***A Method for Constructing a Company Specific Enterprise Architecture Model Framework, 10th ACIS International Conference on Software Engineering, Artificial Intelligences***", Networking and Parallel/Distributed Computing, indexed in IEEE Computer Society.

13- Kang, D., Lee, J., Choi, S., Kim, K. (2010), "***An ontology-based Enterprise Architecture***", Expert Systems with Applications 37.

14- Kim, J., Kwon J., Kim, Y., Kim, H., Baik, D., (2006), "***EAFoC: Enterprise Architecture Framework Based on Commonality***", Journal of Computer Science & technology, Vol. 6.

15- Mamaghani, N., Madani, F., Sharifi, A. (2012), "***Customer oriented enterprise IT architecture framework***", Telematics and Informatics 29 (2012).

16- Myers, M. (2009), "***Qualitative research in business and management***", Sage Publication.

17- Nagarajan, P. (2010). "***Enterprise Architecture Ontology: A Shared Vocabulary for Efficient Decision Making for Software Development Organizations***", The Ohio State University, Thesis for Graduate Program in Computer Science.

18- Nimz, B. (2000), "***The C4ISR Architecture Framework and its Impact on the System Engineering Process***", International Council on System Engineering.

19- Pandit, N. R. (1996), "***The Creation of Theory: A Recent Application of the Grounded Theory Method***", The Qualitative Report 2 (4), December.

20- Schekkerman J. (2004 a), "***Enterprise Architecture Validation***", Revised Version.

21- Schekkerman, J. (2004 b), "***How to survive in the jungle of Enterprise Architecture Frameworks***", Trafford.

22- Sowell, P. (2000), "***The C4ISR Architecture Framework: History, Status, and Plans for Evolution***", The MITRE Corporation, McLean, Virginia.

23- Spewak, S. H. (1992), "***Enterprise Architecture Planning: Developing a Blueprint for Data***", Applications and Technology, John Wiley & Sons, pp. 37-222.

24- Strauss, A., Corbin, J. (1990), "***Basics of qualitative research: Grounded theory procedures and techniques***", Newbury Park, CA: Sage.

25- Wilczynski, B. (2007), "***UML Profile for DoDAF/MODAF Information Session***", Architecture & Interoperability Directorate, Office of the DoD CIO.

26- Zachman J. (1997), "***Enterprise Architecture: The Issue Of Century***", www.zifa.com

27- Zachman J. (2005), "***A Framework for Enterprise Architecture-Cell Definitions***", www.zifa.com.

مجله سیاست دفاعی
سال بیستم، شماره ۷۹، تابستان ۱۳۹۱

معماری سازمانی زمینه‌ساز استقرار و توسعه‌ی معماری اطلاعات در دستگاه‌های دفاعی و اجرایی کشور

تاریخ دریافت مقاله: ۱۳۹۱/۰۱/۱۵
تاریخ تأیید مقاله: ۱۳۹۱/۰۳/۲۳
صفحات مقاله: ۹۶ – ۶۱

علیرضا نادری خورشیدی [۱]
هادی فقیه علی‌آبادی [۲]
رمضان میرعباسی [۳]

چکیده:

تجربه‌ی کشورهای توسعه‌یافته نسبت به معماری اطلاعات در سازمان‌ها، حکایت از آن دارد که معماری اطلاعات نیازمند زیرساخت‌ها و پیش‌زمینه‌هایی است که اگر قبل از تدوین انجام نشود، مانع دستیابی سازمان‌ها به مطلوبیت‌های مورد انتظار و اهداف توسعه‌ی فناوری اطلاعات می‌گردد. در کشور ما علی‌رغم منافع قابل توجه معماری اطلاعات در نظام‌های دفاعی و اجرایی، تلاش‌های صورت گرفته در این زمینه با چالش‌ها و مشکلات بسیار زیادی در مراحل طراحی و اجرایی مواجه شد که نتوانست به نتایج مطلوب و قابل انتظار منجر شود.

این مقاله، به بررسی نمونه‌های واقعی اجرای معماری اطلاعات در سازمان‌های دولتی کشور در مقایسه با نمونه‌های موفق جهانی به عنوان الگوی مبنا پرداخته است. سپس با استفاده از روش رویش نظریه و تحلیل محتوا سعی در شفاف‌سازی علل اصلی و ریشه‌ای عدم موفقیت فعالیت‌های مذکور در دستگاه‌های اجرایی کشور نموده است. در پایان پس از مطالعه‌ی نظام‌مند الگوهای موفق جهانی و تحلیل آنها، با توجه به شرایط بومی کشور به این نتیجه رسیده است در راستای تغییرات و نیازمندی‌های محیط پیرامونی سازمان‌های کشور و هم‌چنین سنتی بودن ساختارها و فرآیندهای انجام کار درونی، آنها باید قبل از انجام هرگونه معماری اطلاعاتی فعالیت‌های معماری سازمانی را به عنوان زیرساخت استقرار توسعه‌ی معماری اطلاعات جهت شفاف‌سازی مأموریت و مهندسی ساختاری سیستم‌ها و فرآیندهای

---

۱ – استاد یار گروه مدیریت دانشگاه جامع امام حسین (ع).
۲ – عضو هیأت علمی دانشگاه جامع امام حسین (ع).
۳ - دانشجوی دکتری مدیریت سیستم دانشگاه جامع امام حسین (ع).

آن انجام دهند، در غیر این‌صورت انجام هرگونه معماری اطلاعات با استقرار دولت الکترونیک از اثربخشی و کارایی لازم برخوردار نخواهد بود.

* * * * *

واژگان کلیدی

معماری اطلاعات، معماری سازمانی، عوامل وحدت‌بخشی، عوامل یکپارچه‌سازی، عوامل رفتاری.

مقدمه

سیاستگذاری، هدایت و رهبری هر جامعه‌ای در حوزه‌های مختلف اجتماعی، اقتصادی، سیاسی و فرهنگی از جمله وظایف نهادها و ارگان‌های دولتی هر کشوری محسوب می‌گردد. در ایران نیز در چند ساله اخیر بر اساس سیاست‌های خصوصی‌سازی، برنامه‌ریزی‌های گسترده‌ای در جهت انتقال بخش‌های اجرایی دولتی به بخش خصوصی و توجه و تمرکز دولت بر فعالیت‌های کلان سیاستگذاری و نظارتی صورت گرفته است. زمانی یک سازمان می‌تواند به هدایت بخش‌های مختلف جامعه بپردازد که دارای زیرساخت‌ها، روش‌های مدیریتی مناسب و سیستم‌های مطلوبی باشد. سازمان‌های امروزی از دیدگاه‌های مختلفی نظیر فرآیندها و ساختارها، بسیار پیچیده شده و از اجزاء و عناصر مختلف و متنوعی تشکیل می‌شوند. صرف‌نظر از ماهیت خاص اجزای سازمان نظیر افراد، دارایی‌ها، تجهیزات، قوانین، روش‌ها و اطلاعات که ماهیتی متغیر دارند، روابط پیچیده بین اجزاء، تحت تأثیر عوامل متغیری چون عادات فردی، آموزش‌های اجتماعی، مذهب، قوانین اجتماعی و فرهنگ سازمانی، سازمان را از سیستمی ساده و ساکن به سیستمی با تغییرات پیوسته مبدل ساخته است. مدیران و رهبران سازمان‌ها از روش‌های نوین برنامه‌ریزی استفاده می‌نمایند تا تغییرات پیش‌رو را در هدایت و کنترل صحیح خود داشته باشند. سازمان‌های دولتی در چند ساله‌ی اخیر فعالیت‌های زیادی را در رابطه با معماری اطلاعات[1] به‌عنوان یکی از روش‌های نوین جهت تسریع در

1 – Information Architecture

روش‌های انجام کار و افزایش کیفیت آن انجام داده‌اند. این روش در حال حاضر، در اغلب کشورهای دنیا به‌عنوان روشی استاندارد در شناخت وضع موجود سازمان، ترسیم وضع مطلوب و گذار از وضع موجود به وضع مطلوب پذیرفته شده است.

این مقاله، به‌دنبال بررسی چگونگی وضعیت معماری اطلاعات در دستگاه‌های اجرایی کشور در مقایسه با نمونه‌های موفق جهانی است. تا ضمن بررسی علل و ریشه‌های توسعه‌نیافتگی، آن ساز و کارهای مناسب جهت برون رفت از وضع موجود را فراهم نماید .

بیان مسأله

علی‌رغم سهم بالای سازمان‌ها و شرکت‌های ایرانی در استفاده از معماری اطلاعات، چالش‌ها و مشکلات بسیاری به‌ویژه در سازمان‌های دولتی وجود دارد که بعضاً منجر به شکست آن شده و سازمان را از دستیابی به منافع و مزایای مورد انتظار محروم کرده است. در پی اقدامات پیشین صورت گرفته در سازمان‌های دولتی، بسیاری از آنها علی‌رغم آشنایی اندک با مفاهیم معماری، به سمت اجرای آن گام برداشته‌اند. شرکت‌های بسیاری در حوزه‌ی تدوین و طراحی معماری اطلاعات ایجاد شد و پروژه‌های متعددی آغاز گردید. از بین ۳۳ سازمان و ۲۱ وزارتخانه، ۲۹ دستگاه دولتی اقدام به انجام معماری اطلاعات در سطح ملی و یا استانی نمودند. حمایت‌های دولتی شامل تخصیص بودجه به سازمان‌های دولتی از مجرای معاونت راهبردی ریاست جمهوری (سازمان مدیریت و برنامه‌ریزی سابق) در قالب طرح تکفا از سال ۱۳۸۲، به عنوان مشوقی مؤثر، روند حرکت سازمان‌های دولتی به سمت معماری اطلاعات مناسب را تسریع بخشید. علی‌رغم حرکت عظیم در مسیر اجرای معماری اطلاعات، موفقیت چندانی حاصل‌نگردید. ۲۲ درصد از پروژه‌ها در مرحله‌ی تدوین RFP و پروپوزال، تعداد ۲۷ درصد در مرحله‌ی طراحی و ۵۱ درصد در مرحله‌ی پیاده‌سازی از کارایی و اثربخشی لازم بهره‌مند نشدند (میرعباسی، ۱۳۸۹: ۷).

تحقیق حاضر در جهت شناسایی علل ریش‌های ناکامی تلاش‌های معماری اطلاعات در سازمان‌های دولتی به دنبال پاسخگویی به سؤالات زیر می‌باشد:

۱) علت اصلی و ریشه‌ای ناکامی‌دستگاه‌های دفاعی و اجرایی کشور برای انجام معماری اطلاعات چیست؟

۲) چه عوامل زمینه‌ای و ساختاری و رفتاری باعث عدم موفقیت معماری اطلاعات در آنها شده است؟

۳) دستگاه‌های دولتی کشور برای برون‌رفت از وضع موجود و کسب کارایی لازم در پاسخگویی سریع، دقیق به مخاطبان چه اقداماتی باید انجام دهند؟

روش تحقیق

اگرچه برای تحقیق، روش‌های متعددی وجود دارد، اما انتخاب روش تحقیق مناسب اغلب اختیاری نبوده و موضوع تحقیق و شرایط آن، روش تحقیق مناسب را مشخص می‌کند. (غفاریان، ۱۳۸۳: ۱۲۹) روش‌های کمی دارای ویژگی جزءنگری بوده که در آنها شناخت خصوصیات سیستم با شناخت خصوصیات اجزای آن امکان‌پذیر خواهد بود. روش‌های کیفی بر نوعی تفسیر کل‌نگر (تمام‌نگر) تأکید می‌کنند. آنها واقعیت‌ها و ارزش‌ها را به صورتی غیرقابل تفکیک و آمیخته با یکدیگر درنظر می‌گیرند.

مقاله‌ی حاضر، با توجه به موضوع تعریف شده و تبعیت از رویکرد سازمان‌گرا در معماری اطلاعات، دارای متغیرهای غیرکمی، منطبق بر نمونه‌های واقعی است که از نگاه کل‌نگری تبعیت کرده و با مشخصات روش‌های کیفی مطابقت دارد. بنابراین، در روش‌شناسی آن از رویکرد رویش نظریه استفاده می‌شود.

رویش نظریه[1]، یکی از پر کاربردترین روش‌های سیستماتیک تجزیه و تحلیل داده‌های کیفی است. این روش قادر است تا مفاهیم نهفته در داده‌ها را استخراج نموده و با کشف روابط بین آنها به نظریه‌هایی که چگونگی و چرایی پدیده‌ها را توضیح می‌دهند، دست یابد.

این روش، یک روش پژوهش عمومی برای تولید نظریه است، نظریه‌هایی که بر اساس گردآوری و تحلیل نظام‌مند داده‌ها پدید می‌آیند. این نظریه در طول تحقیق و

1 - Grounded Theory

بررسی نمونه‌ها رشد می‌کند و از رهگذر تعامل مستمر بین گردآوری و تحلیل داده حاصل می‌گردد(Strauss etal, 1994: 272) . بنابراین، واقعیت‌گرایی یکی از ارکان این روش می‌باشد. واژه‌ی «گراند» به معنای زمینه، بیان‌گر زمینه‌ای مستعد از داده‌های واقعی می‌باشد، که پایه و اساس این روش است (Mansourian, 2006: 391).

این روش، شامل دو فعالیت عمده گردآوری داده‌ها و تجزیه و تحلیل آنها می‌باشد. پس از گردآوری مجموعه‌ی اولیه داده‌ها، تحلیلی بر روی آنها صورت می‌گیرد و بر اساس آن تحلیل، مفاهیم و تعاریف جدیدی شناسایی می‌شوند.

داده‌های واقعی در قالب فرمت‌های گوناگونی شامل متن، صدا، تصویر و یا سایر قالب‌های داده و از روش‌های مختلفی همچون مصاحبه، بررسی اسناد و یا مشاهده حاصل می‌شود. داده‌ها به اجزای کوچکتر تقسیم می‌شوند، تا قابل درک باشند. این تقسیم‌بندی از طریق کدگذاری انجام می‌شود. هر جزء داده، مفهومی را در بر دارد. پس از استخراج مفاهیم، لازم است تا این مفاهیم دسته‌بندی شده و مقایسه شوند.

بنابراین، روش رویش نظریه یک حلقه‌ی تکراری در درون خود دارد و هر چرخش حلقه، شامل بررسی یکی از نمونه‌های واقعی می‌باشد. در اولین تکرار این حلقه، مجموعه‌ی اولیه‌ی داده‌ها گردآوری شده، داده‌ها و اطلاعات حاصل از آنها تحلیل گردیده و مفاهیم و تعاریف جدیدی شناسایی می‌شوند. این مفاهیم و تعاریف در تکرار بعدی مورد استفاده قرار می‌گیرند. به این ترتیب، گردآوری داده‌ها در کنار تحلیل آنها پیوسته تکرار می‌شود. این تکرار تا زمان اشباع ادامه می‌یابد. وضعیت اشباع زمانی رخ می‌دهد که جمع‌آوری داده و تجزیه و تحلیل آن، مفهوم و یا تعریفی را به تحقیق اضافه نکند.

رویش نظریه، شامل ۵ مرحله و ۹ گام زیر است:

۱) مرحله‌ی اول، طرح تحقیق:
- گام ۱: مرور ادبیات؛
- گام ۲: انتخاب مورد.

۲) مرحله‌ی دوم، جمع‌آوری داده‌ها:

- تدوین دقیق روش گردآوری داده‌ها و تشکیل پایگاه داده؛
- ورود به میدان تحقیق.

۳) مرحله‌ی سوم، تنظیم داده‌ها:

- تنظیم داده‌ها بر اساس زمان.

٤) مرحله‌ی چهارم؛ تحلیل داده‌ها:

- تحلیل داده‌ها؛
- نمونه گیری؛
- پایان فرآیند.

۵) مرحله‌ی پنجم، اعتبار سنجی.

مبانی نظری تحقیق

رویکردهای معماری اطلاعات

در ابتدا مدل‌های توسعه‌ی فناوری اطلاعات و ارتباطات تنها بر پایه‌ی داده‌های سازمان استوار بودند. سیر تحول این مدل‌ها منجر به توجه به فرآیندها و نهایتاً درکل سازمان باعث توسعه‌ی مبتنی بر فناوری اطلاعات و ارتباطات گردید. با مراجعه به انواع مدل‌های موجود در زمینه‌ی معماری اطلاعاتی، سه رویکرد عمده شناسایی شد که عبارتند از:

- **رویکرد داده‌گرا:** چارچوب‌ها و مدل‌هایی که در این رویکرد قرار می‌گیرند، تنها به داده‌های سازمان توجه می‌کنند و به‌دنبال مدل‌سازی داده‌ها و طراحی سیستم‌های نرم‌افزاری جهت ذخیره‌سازی و بازیابی آنها می‌باشند. سیستم‌های اطلاعاتی تولید شده در این چارچوب‌ها بندرت می‌توانند از فرآیندهای سازمان پشتیبانی نمایند.
- **رویکرد فرآیندگرا:** این رویکرد، علاوه بر توجه به داده‌های سازمان، تبادل داده‌ها و نیازهای فرآیندهای سازمانی به داده‌ها را نیز مدل‌سازی می‌نمایند. سیستم‌های تولید شده در این رویکرد، فرآیندهای موجود سازمان را پشتیبانی نموده و سیستم‌های پشتیبان تصمیم مورد نیاز سازمان را تأمین می‌نمایند. در این رویکرد، فناوری

اطلاعات و ارتباطات در جهت مدیریت فرآیندها مورد استفاده قرار می‌گیرد. از جمله متدلوژی‌هایی که در این رویکرد مورد تأکید قرار می‌گیرد، می‌توان به متدلوژی برنامه‌ریزی سیستم‌های کسب و کار[1] (BSP) اشاره نمود که در سال ۱۹۶۷ توسط شرکت IBM ارائه شد. این متدلوژی در مدل‌سازی اطلاعاتی سازمان، تأکید عمده‌ای بر شناسایی و تحلیل فرآیندهای کاری دارد.

- **رویکرد سازمان‌گرا:** این رویکرد، به عنوان یک رویکرد جدید در توسعه‌ی فناوری اطلاعات و ارتباطات، به کلیه‌ی ابعاد سازمانی از جمله راهبردها و فرآیندها توجه می‌نماید. در این رویکرد، سازمان سیستمی واحد در نظر گرفته می‌شود که در کلیه‌ی بخش‌ها و لایه‌های آن ارتباطات تنگاتنگی برقرار است. در این رویکرد، نمی‌توان به عنصری از سازمان بدون توجه به سایر عناصر آن توجه نمود و در این‌صورت غفلت بزرگی اتفاق می‌افتد. این رویکرد، یک رویکرد کل‌نگر بوده و بخش‌های مختلف سازمان را وابسته به یکدیگر می‌داند. رویکرد سازمان‌گرا در معماری فناوری اطلاعات و ارتباطات بیان می‌کند که حوزه‌ی اطلاعات در سازمان وابسته به سایر حوزه‌ها بوده و نمی‌تواند به صورت مستقل بررسی گردد. به عبارتی، فناوری‌های اطلاعاتی و ارتباطاتی باید در راستای تحقق چشم‌انداز و راهبردهای سازمان مورد استفاده قرار گیرد. از این‌رو، توجه به حوزه‌ی اطلاعات بدون توجه به لایه‌های راهبردی و مأموریتی سازمان بی‌معنی خواهد بود. معماری سازمانی و مدل‌ها و متدلوژی‌های آن در دسته‌ی رویکرد سازمان‌گرا قرار می‌گیرند. متدلوژی برنامه‌ریزی معماری سازمانی (EAP[2]) یکی از متدلوژی‌های سازمان‌گرا می‌باشد که بر پایه‌ی چارچوب زکمن و در سال ۱۹۹۲ ارائه شد. در این متدلوژی در توسعه‌ی

1 - Business System Planing
2 - Enterprise Architecture Planning

سیستم‌های اطلاعاتی به کلیه ابعاد کسب و کار، اطلاعات، سیستم‌ها و زیرساخت‌ها توجه می‌شود.

جدول شماره‌ی ۱ – تعدادی از متدلوژی‌های توسعه فناوری اطلاعات را به همراه رویکردهای مربوطه نشان می‌دهد (عباسی و همکاران، ۱۳۸٤:٥٤)

متدولوژی	متد ساخت یافته تحلیل و توسعه سیستم SSADM	مهندسی اطلاعات IE	برنامه‌ریزی سیستم‌های کسب و کار BSP	فرآیند یکپارچه منطقی RUP [1]	برنامه‌ریزی معماری سازمانی EAP	معماری فناوری اطلاعات ITA [2]	متدلوژی توسعه‌ی معماری ADM [3]
سال ایجاد	۱۹۸۱	۱۹۸۱	۱۹٦۷	۲۰۰۳	۱۹۹۲	۲۰۰۲	۲۰۰۰
رویکرد	داده‌گرا	داده‌گرا	فرآیندگرا	فرآیندگرا	سازمان‌گرا	سازمان‌گرا	سازمان‌گرا
چارچوب	–	–	–	-	زکمن	ITA	TOGAF

برنامه‌ریزی معماری سازمانی (EAP) به‌عنوان زمینه‌ساز معماری اطلاعات، از یک متدلوژی سازمان‌گرا تبعیت می‌کند. این متدلوژی، تمام سازمان را مورد توجه قرار می‌دهد و تنها بر یک بُعد خاص مانند داده یا فرآیند متمرکز نمی‌شود. این متدلوژی به دلیل سادگی و جامع بودن، به عنوان یکی از متدلوژی‌های رایج در حوزه‌ی معماری اطلاعات شناخته می‌شود و از این‌رو، در تحقیق حاضر، رویکرد سازمان‌گرا به عنوان رویکرد اصلی معماری اطلاعات در نظر گرفته شده است.

رویکرد سازمان‌گرا در معماری فناوری اطلاعات و ارتباطات بیان می‌کند که حوزه‌ی اطلاعات در سازمان وابسته به سایر حوزه‌ها بوده و نمی‌تواند به صورت مستقل بررسی گردد.

1 – Rational Unified Process
2 – Information Technology Architecture
3 – Architecture Development Methodology

به‌عبارتی، فناوری‌های اطلاعاتی و ارتباطاتی باید در راستای تحقق چشم‌انداز و راهبردهای سازمان مورد استفاده قرار گیرد و از این‌رو، توجه به حوزه‌ی اطلاعات بدون توجه به لایه‌های راهبردی و مأموریتی سازمان بی‌معنی خواهد بود. معماری اطلاعات و مدل‌ها و متدلوژی‌های آن در دسته‌ی رویکرد سازمان‌گرا قرار می‌گیرند.

چارچوب‌های معماری اطلاعات در عمل

چارچوب زکمن

«جان زکمن»[1] که به عنوان پدر علم معماری سازمانی شناخته می‌شود، معماری را به معنی ساختن به کار می‌برد و در مباحث سیستم‌های اطلاعاتی آن‌را تشبیهی از ساختن سیستم‌های اطلاعاتی به ساختن ساختمان می‌داند.

وی معماری اطلاعات را به عنوان چارچوبی برای تعیین ضرورت‌های سرمایه‌گذاری بر روی منابع سیستم‌های اطلاعاتی تعریف می‌کند (Sowa et al 1992: 597). به عبارت دیگر، معماری اطلاعاتی یک چارچوب یکپارچه برای ارتقا یا نگهداری فناوری موجود و کسب فناوری اطلاعاتی جدید برای نیل به اهداف راهبردی سازمان و مدیریت منابع آن می‌باشد. (Clinger Cohen, 1996: 132)

طراحی و تولید سیستم‌های اطلاعاتی کوچک و محلی دارای پیشینه و تجربه‌ی زیادی بوده و روش‌های زیادی برای آن ارائه شده است که آخرین آنها طراحی و توسعه بر اساس روش‌های شی‌گرا است که کمک زیادی به انعطاف‌پذیری سیستم‌های اطلاعاتی نمود. رویکردهای اولیه توسعه‌ی سیستم‌های اطلاعاتی تنها بر داده‌های سازمان تکیه داشته و به شناسایی اطلاعات و برقراری ارتباط آنهاپرداخته است. صرف‌نظر از نقاط ضعف، اغلب این متدولوژی‌ها در پاسخگویی به نیازمندی‌های اخیر سازمان‌ها در رابطه با طراحی سیستم‌های توزیع‌شده و سازمانی، متدلوژی‌های فوق در بهترین حالت تنها قادر به مدل‌سازی ابعادی چون اطلاعات، فرآیندها، و مکان‌های سازمان در لایه‌ی فناوری اطلاعات و ارتباطات خواهند بود.

خلاء موجود در زمینه‌ی الگوهایی که بتواند به کلیه‌ی ابعاد سازمانی در توسعه‌ی فناوری اطلاعات و ارتباطات توجه نماید، منجر شد تا در سال ۱۹۸۷ توسط «جان زکمن» و در مقاله‌ای تحت

1 – zachman

عنوان چارچوبی برای معماری سیستم‌های اطلاعاتی، لزوم توجه به ابعاد مأموریتی و راهبردی سازمان مطرح شده و شش بُعد اصلی در پنج لایه برای معماری سیستم‌های اطلاعاتی بیان گـردد. شـش بُعـد چارچوب زکمن شامل داده‌ها، فرآیندها، مکان‌ها، افراد، رویدادها و راهبردها و پنج لایه تعریـف شـده شامل محدوده، کسب و کار، سیستم، زیرساخت و جزئیات می‌باشـد. در ایـن تحقیـق، بـا توجـه بـه رویکرد سازمان‌گرا، چارچوب زکمن به‌دلیل جامعیت به‌عنـوان چـارچوب مـادر مـورد اسـتفاده قـرار می‌گیرد و چارچوب‌های بعدی توسط سایر محققین و بر پایه‌ی آن بنا شده است.

جدول شماره‌ی ۲ – ماتریس زکمن

	اطلاعات چه چیز	فرآیندها چطور	مکان‌ها کجا	افراد چه کسی	رویداد کی	اهداف چرا
دیدگاه برنامه‌ریز توصیف مفهومی	اطلاعات مهم	فرآیندهای کلان	مکان‌های اصلی	بخش‌های مهم	رویدادهای مهم	راهبردها
دیدگاه مالک توصیف سازمانی	موضوعات	فرآیندهای سازمان	مکان‌های سازمان	ساختار سازمانی	رویدادهای سازمان	اهداف
دیدگاه طراح توصیف سیستمی	داده‌ها	کارکردهای برنامه‌ها	وظایف سیستم‌ها	نقش‌ها	رویدادهای سیستمی	احکام ساختاری
دیدگاه سازنده توصیف فناوری	جداول اطلاعاتی	توابع کامپیوتری	سخت افزار و نرم افزار	کاربر	زمان‌های اجرا	قواعد
دیدگاه پیمانکار توصیف فنی)	فیلدها	کدها	پروتکل‌ها	شناسه	واقعه	حالات

در این ماتریس نکات زیر وجود دارد:

- ستون‌ها حق تقدمی نسبت به یکدیگر ندارند.
- ستون یا سطری نباید به آن اضافه نمود. زکمن ادعا می‌کند که این تعداد ستون، کلیه‌ی اطلاعات مورد نیاز سازمان را ارائه می‌کند.
- شش خانه هر سطر مستقل از یکدیگر می‌باشند و در تشریح هر یک از آنها باید مدل‌های مختلفی مورد استفاده قرار گیرد.
- ترکیب مدل‌های ارائه شده در خانه‌های هر سطر بیانگر توصیف کامل سازمان از دیدگاه مورد نظر می‌باشد.

مجموعه‌ی عظیمی از ذی‌نفعان وجود دارند که توجهات، خواسته‌ها و نقطه‌نظرات خود را با یکدیگر به اشتراک می‌گذارند. آنها اطلاعات خود را در قالب شش سؤال پرسشی مطرح می‌کنند. این سؤالات عبارتند از:

- چرا: چرا موضوع مربوطه مهم است؟
- چگونه: چگونه این موضوع محقق می‌شود؟
- چه چیز: به چه چیزهایی برای تحقق این موضوع احتیاج داریم؟
- چه کسی: چه کسی باید فعالیت‌های مربوطه را انجام دهد؟
- چه زمانی: چه زمانی باید این موضوع محقق شود؟
- چه مکانی: مکان‌های اصلی سازمان کجاست؟

چهار سؤال چه چیز، چه زمانی، کجا و چه کسی، پاسخی به پرسش‌های اطلاعاتی می‌باشد. دانش از پردازش اطلاعات به‌دست می‌آید و می‌تواند در قالب رویکردها، روش‌ها، تجربه و راهبرد نمایان شود. دانش سازمان از طریق پاسخ به پرسش چگونه، به‌دست خواهد آمد. در سطحی بالاتر خرد (معرفت)، بیانگر نگاه، هدف، اصول و ارزش‌هایی است که پاسخ به پرسش چرا ،خواهد بود. در صورتی‌که خرد تشخیص داده نشده باشد، دانش پاسخ به پرسش‌های چرا و چگونه خواهد بود.

آنچه مسلم است این است کـه پـیش از بررسـی سـؤالات بـالا و ورود بـه ایـن مرحلـه از معماری، باید مهندسی مجدد کارها، مهندسی ساختارها و شفاف‌سازی نقش‌های زیرسیسـتم‌هـای سازمان در راستای مطلوبیت‌های نهایی سازمان با توجه به تلاطم‌های محیطـی در حـوزه‌ی درون سازمان و بیرون آن به‌طور سیستمی و همه‌جانبه مورد بررسی و تحلیـل قـرار گیـرد. بـه عبـارت دیگر، سازمان با انجام این‌گونه عملیات نرم و سخت، خود را بـرای طراحـی و تـدوین معمـاری اطلاعات آماده می‌کند. بر اساس این چارچوب، تا زمانی‌کـه معمـاری کسـب و کـار در سـازمان انجام نگیرد، زمینه برای معماری اطلاعات از جهت محتلف به‌وجود نخوهد آمد.

روند تکمیل و بهبود مدل‌های معماری اطلاعات منجر به ایجاد چـارچوب‌هـایی نظیر چارچوب معماری فنی برای مدیریت اطلاعات (TAFIM [1]) و برنامه‌ریزی معماری سازمانی(EAP [2]) در سال ۱۹۹۲، چارچوب C4ISR [3] در سال ۱۹۹۶، معماری سـازمانی خزانـه‌داری آمریکـا(TEAF [4]) در سـال ۲۰۰۰ و چـارچوب معمـاری سـازمانی فـدرال (FEAF [5]) در سال ۲۰۰۲ گردید.

چارچوب معماری فدرال

معماری فدرال ورودی‌ها، اقدامات و خروجی‌های معماری را به‌صورت مشخصی تعیـین نموده است. در این معماری، ورودی‌ها شامل تغییـرات مـرتبط در حـوزه‌ی فنـاوری و محـیط کسب و کار، راهبردها ونیازمندی‌های سازمانی به‌عنوان پیش‌نیازهـای اصـلی شـروع معمـاری اطلاعات مطرح می‌باشند. اقدامات مطرح در این چارچوب شامل تدوین معماری وضع موجود و وضع مطلوب و طراحی برنامه‌ی گـذار مـی‌باشـد. ایـن چـارچوب تأکیـد بسـیاری بـر روی خروجی‌های معماری و مطلوبیت‌های آن دارد که شـامل چشـم‌انـداز و برنامـه‌هـای راهبـردی فناوری اطلاعات و استانداردهای لازم برای توسعه فناوری اطلاعات در سازمان می‌شود.

1 - Technical Architecture Framework for Information Management
2 - Enterprise Architecture Planning
3 - Command , Control , Communications , Computers , Intelligence , Surveillance and Reconnaissance
4 - Treasury Enterprise Architecture Framework
5 - Federal Enterprise Architecture Framework

سطح اول چارچوب FEAF شامل هشت جزء اصلی زیر می‌باشد:

- پیشران‌های معماری[1] : معرف یک محرک خارجی است که می‌تواند تغییراتی را به حوزه‌ی فناوری اطلاعات و ارتباطات تحمیل نماید. به عنوان مثال، تغییر در فرآیندها موجب تغییر در سیستم‌های اطلاعات می‌گردد. به کلیه‌ی عواملی که می‌توانند بر وضعیت فناوری اطلاعات و ارتباطات شرکت تأثیر بگذارند، پیشران‌های معماری گفته می‌شود. که قبل از انجام هرگونه برنامه‌ریزی در معماری اطلاعات باید به‌صورت شفاف و روشن مورد بررسی و تحلیل قرار گیرد و ادبیات مشترک نسبت به آن در سازمان به‌وجود آید.
- راهبردها: کلیه‌ی تلاش‌های صورت گرفته در زمینه‌ی معماری اطلاعات باید در راستای تحقق راهبردهای سازمان صورت گیرد. بنابراین، یکی از اجزای چارچوب فوق، راهبردهای سازمان خواهد بود.
- معماری وضع موجود: معماری وضع موجود بیانگر وضعیت فعلی فناوری اطلاعات و ارتباطات در سازمان می‌باشد. این جزء مشخص می‌کند که سازمان در حال حاضر در قالب چه نرم‌افزارهایی و در چه بسترهای سخت‌افزاری اطلاعات خود را نگهداری، بازیابی و پردازش می‌کند. در این مرحله، نقاط ضعف و قوت معماری موجود باید کاملاً شفاف شود تا برای برون‌رفت از آنها نیاز به وضع مطلوب ضرورت پیدا کند.
- معماری وضع مطلوب: وضعیت نهایی و مطلوب سازمان را در حوزه‌ی فناوری اطلاعات و ارتباطات مشخص می‌کند.
- فرآیندهای گذار: این فرآیندها نحوه‌ی حرکت از وضع موجود به وضع مطلوب را در قالب فعالیت‌های برنامه‌ریزی شده‌ای ارائه می‌کنند. این مرحله، یکی از مهم‌ترین گام‌های معماری اطلاعات در سازمان‌ها می‌باشد.

1 - Architecture Drivers

- بخش‌های معماری: شامل بخش‌های متمرکز شده در سازمان شامل اداری، مالی و ... می‌باشد. بخش‌های معماری در واقع، یک سازمان ویژه را در درون معماری ارائـه و توصیف می‌کنند. برای هر بخش معماری با توجه به حوزه‌ی تمرکز بخش، معمـاری وضعیت موجود و مطلوب آن بخش تعریف می‌شود.
- مدل‌های معماری: خروجی‌های مورد انتظار در معماری اطلاعـات شـامل مـدل‌هـای مفهومی، منطقی و فیزیکی را که می‌توانند در قالب گزارش‌ها، نمودارها و ماتریس‌ها ارائه شوند در بر می‌گیرد.
- استانداردها: در برگیرنده‌ی همه‌ی اصول راهبردها و قواعدی است که در توسعه‌های آتی مورد استفاده قرار می‌گیرد.

این چارچوب همان‌طور که ملاحظه می‌شود، قبل از انجام معماری اطلاعات موضـوعاتی تحت عنوان پیش‌ران‌ها را جهت ضرورت معماری اطلاعات در ابعاد ذیل مـورد مطالعـه قـرار می‌دهد: مرحله اول مطالعه‌ی مربوط به زمینه و نیازمندی‌های محیط شامل سازمان است که اگر سازمان به آن توجه نکند بقاء و استمرار آن مورد سؤال قرار می‌گیرد. بر این اساس، سازمان‌هـا قبل از معماری، مطلوبیت‌های خود را از قبیل چشـم‌انـدازها، اهـداف، راهبـردهـا و ... جهـت هم‌سویی با تعاملات محیطی مورد مطالعه و بازمهندسی قرار می‌دهند در مرحله‌ی دوم متناسب با تغییر نیازمندی‌های محیطی شامل تغییر سلیقه‌های مشتریان و ذی‌نفعـان کلیـدی بـه بررسـی ساختارهای درونی سـازمان از قبیـل فرآینـدهای انجـام کـار، مطالعـه و تغییـر شـاخص‌هـا و استانداردها و هم‌چنین توانمندی‌های نیروی انسانی و باورهای آنها بـرای تحـول مـی‌پردازنـد. سپس در مرحله‌ی سوم معماری اطلاعات جهت رفع نیازمندی‌های موجود انجام می‌گیرد.

چارچوب معماری خزانه‌داری آمریکا(TEAF)

از نقاط قابل توجه این چارچوب، توجه به نیازمندی‌های اجرایی معمـاری اطلاعـات در سازمان می‌باشد. این چارچوب فرآیند معماری اطلاعات را به سه بخش رهبری، تفسیر و اجرا تقسیم می‌کند. رهبری معماری که توجه خود را بر تأمین نیازمندی‌ها و ورودی‌های مورد نیـاز قرار داده است، قوانین، سیاست‌ها، برنامه‌های راهبردی، نیازمندی‌های سازمانی، مسـیر حرکـت

سازمان و اصول آن‌را در نظر می‌گیرد. به عبارتی، پیش‌فرض شروع معماری را فراهم آمدن این ورودی‌ها می‌داند. و با استفاده از این ورودی‌ها در بخش تفسیر ،معماری فرآیندها، داده‌ها، زیرساخت‌ها و ساختار و تشکیلات طراحی شده و بر اساس خلاءهای موجود، راهبردهای گذار از وضع موجود به وضع مطلوب به همراه پیش‌بینی‌های مختلفی نظیر زمان، هزینه، خطر و ... تهیه و در بخش اجرای معماری تحقق می‌یابد.

همان‌طور که ملاحظه می‌شود، در این چارچوب قبل از معماری اطلاعات باید مطلوبیت‌های سازمان به‌عنوان سیاست‌های کلان و برنامه‌های راهبردی و هم‌چنین اصول و مبانی ارزشی آن مشخص شود، سپس تغییر تعاملات اجزای درون سازمان به عنوان عوامل یکپارچه‌ساز مشخص و شفاف گردد. به طوری‌که مفاهمه و هم‌سویی در سازمان در راستای آماده شدن برای معماری اطلاعات فراهم شود و بعد از آن، فرآیند معماری اطلاعات و چگونگی تدوین و اجرای آن در سازمان مورد تجزیه و تحلیل و بررسی قرار گیرد.

چارچوب معماری TOGAF [1]

این چارچوب دارای نگرشی فرآیندگرا می‌باشد و برای برنامه‌ریزی معماری اطلاعات مورد استفاده قرار می‌گیرد. گام‌های اصلی در چارچوب TOGAF شامل آماده‌سازی، تعریف معماری، برنامه‌گذار و مدیریت معماری می‌شوند. در مرحله‌ی آماده‌سازی لازم است تا چشم‌اندازها و اهداف سازمان مشخص شده و بر اساس آنها خط سیر معماری اطلاعات مشخص شود. نکته‌ی کلیدی در این چارچوب ارتباط متقابل کلیه‌ی اجزا با یکدیگر و توجه مناسب به موضوع مدیریت تحول است. بدیهی است، در یک سازمان بدون توجه به مفاهیم تحول نمی‌توان یک فرآیند تحولی نظیر معماری اطلاعات را به سرانجام رساند. در واقع، یکی از انتظارات از معماری اطلاعات تحول در سازمان است و این خروجی معماری اطلاعات می‌باشد.

در این مدل قبل از این‌که سازمان را برای معماری اطلاعات آماده کنیم؛ همان‌طور که مدل نشان می‌دهد باید، آن‌را برای ایجاد یک تحول و دگرگونی آماده نماییم. طبیعی است در مدیریت

1 – The Open Group Architecture Frame Work

تحول تمام اجزای سازمان از جهت‌گیری‌ها و اولویت‌های آن به عنوان مطلوبیت نهایی و چشم‌اندازها مورد بررسی قرار می‌گیرد و در راستای آن ساختارهای درونی از قبیل ساختار سازمانی، ساختار منابع انسانی و ... مهندسی می‌شود. بر این اساس، قبل از معماری اطلاعات در این مدل اجزای مختلف سازمان در دو بُعد، اصول و ارزش‌های اساسی به عنوان مطلوبیت‌ها و هم‌چنین ساختارهای درونی به عنوان عوامل یکپارچه‌کننده معماری و بررسی می‌شوند.

چارچوب معماری DODAF[1] (چارچوب معماری بخش دفاعی آمریکا)

این چارچوب با رویکرد مبتنی بر مهندسی سیستم‌ها، نگاه کلانی به فرآیندها، سیستم‌های اطلاعاتی و زیرساخت‌ها دارد. DODAF توجه بسیاری به استانداردها و الگوهای عملی راهنما دارد. استانداردها علاوه بر ایجاد بستری برای جلوگیری از اعمال سلیقه‌ها، خطوط حرکتی سازمان را در توسعه‌ی فناوری اطلاعات و ارتباطات مشخص می‌کنند. در این استاندارد از مدل‌های مرجع به‌خوبی استفاده شده است. مدل‌های مرجع مجموعه‌ای از استانداردها، راهنماها و محدودیت‌هایی برای توسعه‌ی فناوری اطلاعات هستند که در کلیه‌ی مراحل کار مورد استفاده قرار می‌گیرند.

کیفیت و اثربخشی فرآیند معماری اطلاعات اهمیت بسیاری دارد. «مورگان والپ» و همکاران (۲۰۰۳) اهداف پنج‌گانه‌ی معماری اطلاعات در این چارچوب را به شرح ذیل بیان می‌کند (Morgan Walp et al, 2003: 96):

- یکپارچه‌سازی سیستم‌ها: معماری اطلاعات باید منجر به ایجاد سیستم‌هایی گردد که از لحاظ فنی جامع، یکپارچه و انعطاف‌پذیر باشند. به عبارتی، سیستم‌ها باید به یکدیگر متصل باشند. این ارتباط باید در تمامی‌بخش‌ها و کلیه سطوح سیستم‌ها ایجاد گردد.
- اثربخشی واحدهای متقابل[2]: معماری اطلاعات باید منجر به ایجاد سیستم‌هایی گردد که از لحاظ سازمانی جامع، یکپارچه و انعطاف‌پذیر باشند. به عبارتی، سیستم‌ها باید دیدگاه‌ها و نیازهای کلیه‌ی ذی‌نفعان در طول واحدهای سازمانی را برآورده کنند.

1 – Department of Defense Architecture Framework
2 – Cross divisional

- تسهیل ارتباطات: ارتباطات، همکاری‌ها و به اشتراک‌گذاری اطلاعات باید تسهیل گردد.
- توسعه‌ی اقتصادی: سیستم‌های اطلاعاتی باید به‌گونه‌ای اقتصادی توسعه داده شوند. به‌عبارتی، افزایش در استفاده‌ی مجدد از اجزای معماری اطلاعات (از جمله مدل‌های به‌کارگرفته شده) و اجزای دانش سیستم‌های قبلی در سیستم‌های جدید ایجاد شود.
- استفاده‌ی مکرر از فرآیند معماری اطلاعات: استفاده از فرآیند معماری اطلاعات در سازمان به‌صورت یک فرآیند دائم و پیوسته درآید.

به منظور اطلاع از شکست یا موفقیت فرآیند معماری اطلاعات لازم است تا اهداف فوق در قالب معیارها و شاخص‌هایی طراحی گردد. «باچانان» (۲۰۰۱) پیشنهاد نمود تا کیفیت معماری اطلاعات از طریق سه معیار زیر سنجیده شود (Bachanan, 2001: 128).

- کارآیی مالی: صرفه‌جویی هزینه؛
- اثربخشی کسب و کار: ایجاد ارزش‌ها و منافع راهبردی؛
- کیفیت فرآیند معماری: استقرار فرآیند قابل استفاده.

معیار سوم از دیدگاه تعدادی از محققین می‌تواند در داخل دو معیار اول سنجیده شود. بنابراین، کیفیت فرآیند معماری را می‌توان با منافعی که در حالت ایده‌آل توسط دو معیار کارآیی مالی و اثربخشی کسب و کار تأمین می‌شود، ترکیب نمود و تنها دو دسته‌بندی را برای اهداف معماری اطلاعات عنوان کرد.

شاخص‌های زیر برای دو معیار فوق پیشنهاد شده‌اند.

۱) کارآیی مالی:

- استفاده‌ی مجدد از اجزای سخت‌افزاری و نرم‌افزاری و مدل‌ها و متدهای توسعه‌ی معماری؛
- کاهش زمان تدوین و ارائه‌ی خروجی‌های فرآیند معماری اطلاعات؛
- افزایش اثربخشی فرآیند مدیریت برنامه‌ها؛
- کاهش هزینه‌های پشتیبانی؛
- کاهش هزینه‌های تأمین؛
- افزایش سازگاری فنی.

۲) اثربخشی کسب و کار:

- هم‌راستایی بیشتر فناوری اطلاعات و راهبردهای سازمان؛
- پشتیبانی از مدیریت و توسعه‌ی دانش؛
- افزایش مهارت و دانش مدیریت سرمایه‌های شرکت؛
- کاهش هزینه‌های خطر تصمیم؛
- افزایش هم‌راستایی راهبردهای سازمان و شرکا؛
- افزایش سازگاری و توافق اجزای سازمان.

همان‌طور که در قالب شاخص‌های سنجش کارآیی و اثربخشی کسب و کار طرح شد، معماری اطلاعات این دو شاخص کلیدی در سازمان را به‌وجود می‌آورد. اگر اجزای این دو قسمت به صورت فنی مورد ملاحظه قرار گیرد، متوجه می‌شویم آن‌چه که باعث افزایش کارآیی مالی می‌شود اصلاح عوامل ساختاری است و هم‌چنین آن عواملی که باعث افزایش اثربخشی کسب و کار می‌گردد، بیشتر به جهت‌گیری‌ها و مشخص نمودن اولویت‌های سازمان مربوط است. در صورتی که این خروجی‌ها در سازمان به‌وجود آید، معماری اطلاعات کارآیی و اثربخشی لازم را داشته است، در غیر این‌صورت، خاصیت کارکردی مناسب در سازمان به‌وجود نمی‌آید.

ساختار اولیه پژوهش

با استفاده از ادبیات مطرح شده در راستای تجربیات عملی و نظری سازمان‌ها موفق در جهان نسبت معماری اطلاعات موضوعات زیر در رابطه با چگونگی اجرای معماری اطلاعات به صورت موفق منتج می‌شود:

چارچوب زکمن یک تجربه کاملی است که تمام نکات معماری اطلاعات چه قبل از انجام آن و چه بعد از آن را مورد توجه قرار می‌دهد. نکته‌ی مهم در این چارچوب این است که انجام معماری اطلاعات در شرایط محیط متلاطم باعث پیچیدگی‌های بسیار زیادی می‌گردد که چنان‌چه اجزای درون و بیرون سازمان مورد مطالعه قرار نگیرند، بعضاً انجام هرگونه

معماری اطلاعات باعث پیچیدگی بیشتر در سازمان شده و هم‌سوسازی عوامل بیرونی انسجام درونی سازمان را بیشتر با خطر مواجه خواهد کرد. بر این اساس «زکمن»، روی دو رکن اساسی سازمان قبل از معماری اطلاعات تأکید می‌کند. اول، درک پیچیدگی‌های محیطی سازمان است. به عبارتی، متولیان سازمان باید قبل از انجام معماری اطلاعات مطلوبیت‌های سازمان را مشخص نموده و در راستای آن اولویت‌ها و جهت‌گیری آینده آن‌را مشخص کنند. بر این اساس، روی عوامل هم‌سوسازی و وحدت‌بخشی از قبیل تبیین چشم‌انداز، اهداف و راهبردهای توسعه‌ی آینده تأکید می‌کند. رکن دوم همگام با ساماندهی متغیرهای تأثیرگذار خارجی، تأثیرات آنها را در درون سازمان تبیین و مهندسی می‌کند. به‌طوری که، انسجام و یکپارچگی سازمانی به خطر نیافتد. برای این کار، مهندسی مجدد فرآیندها تبیین نقش‌ها و طراحی ساختار سازمانی را مورد توجه قرار می‌دهد.

در چارچوب معماری فدرال بحث پیش‌ران‌های معماری مورد توجه قرار گرفت. سازمان‌ها قبل از انجام معماری اطلاعات از یک طرف باید محرک‌های خارجی و برون‌سازمانی را که تغییراتی را در حوزه‌ی فناوری اطلاعات و ارتباطات تحمیل می‌کنند مورد مطالعه قرار دهند و مطلوبیت‌های هم‌سوساز مثل چشم‌انداز، راهبرد، اهداف و اصول و ارزش‌های خود را بر اساس آنها تنظیم نماید. از طرف دیگر، استانداردها، فرآیندهای سازمان و ساختار سازمانی را با توجه به متغیرهای هم‌سوساز و وحدت‌بخش یکپارچه و منسجم نمایند.

تجربیات عملی و نظری معماری در خزانه‌داری آمریکا نشان می‌دهد که این چارچوب روی نیازمندی‌های زمینه‌ای یا محیطی و ساختاری معماری اطلاعات تأکید دارد. نیازمندی‌های محیطی شامل اصول و مبانی ارزشی سازمان و چشم‌انداز سازمان به عنوان عوامل هم‌سوساز عوامل محیطی و هم‌چنین قوانین و مقررات به عنوان یکپارچه‌ساز درونی را مورد توجه قرار می‌دهد.

در سایر مدل‌ها مانند TOGAF و DODAF هم به فرآیندهای مختلف آماده‌سازی سازمان، معماری سازمانی و سپس مرحله‌ی گذار به عنوان دستیابی به تحول پایدار در سازمان اشاره شده است که در آنها هم عواملی همچون چشم‌انداز، راهبردها، نقش‌ها و فرآیندهای انجام کار مورد تأکید قرار گرفته است.

چنانچه ملاحظه می‌شود، هر یک از چارچوب‌های مطرح شده عناصر و اجزای متنوعی را در یک رویکرد سیستمی و نظام گرا مورد توجه قرار داده‌اند. اما اکثریت آنها قبل از معماری اطلاعات به معماری سازمانی و مفاهیم آن توجه کرده‌اند. با توجه به هدف تحقیق که بررسی علل ناکامی معماری اطلاعات در کشور است، این تحقیق باید عوامل زمینه‌ساز معماری اطلاعات را مورد تأکید قرار دهد؛ در غیر این‌صورت، دلایل ریشه‌یابی نخواهد شد. بر این اساس، آنچه در تمام مدل‌های مطرح شده مورد اتفاق نظر است، انجام معماری سازمانی قبل از اقدام برای معماری اطلاعات می‌باشد. برای این کار باید عوامل هم‌سوساز و وحدت‌بخش در تعامل با محیط و عوامل یکپارچه‌ساز درون‌سازمانی به صورت سیستمی مورد توجه قرار گیرند. جدول شماره‌ی (۳) اتفاق‌نظر اجزای این عوامل را در مدل‌های مختلف قبل از معماری اطلاعات نشان می‌دهد.

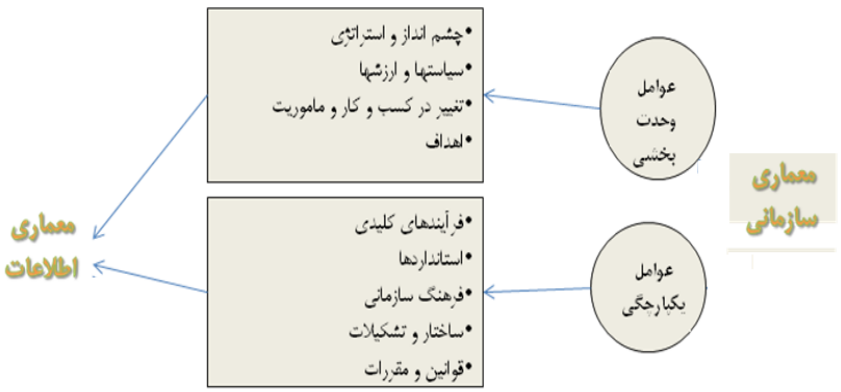
جدول شماره‌ی ۳ – عناصر معماری سازمانی به‌عنوان پیش‌زمینه معماری اطلاعات

	عنوان	زکمن	FEAF	DODAF	TEAF	TOGAF
عوامل هم‌سوساز وحدت‌بخشی	چشم‌انداز و راهبرد سازمانی	*	*		*	*
	سیاست‌ها و اصول و ارزش‌های سازمان	*	*		*	*
	تغییرات حوزه‌ی کسب و کار و مأموریت	*	*			*
	اهداف	*	*		*	
عوامل انسجام‌دهنده یکپارچه‌ساز	فرآیندهای کلیدی سازمان	*	*	*	*	*
	ساختار سازمانی و تشکیلات	*	*	*	*	*
	استانداردها		*	*	*	
	قوانین و مقررات			*	*	
	نیازمندی‌های سازمان	*	*	*	*	*
	فرهنگ و بلوغ سازمانی	*	*	*	*	*

عوامل هم‌سوساز یا وحدت‌بخشی عواملی هستند که تمام اجـزای سـازمان را نسـبت بـه مطلوبیت‌های نهایی سازمان هم‌جهت می‌کنند و هرگونه تردید و ناباوری درون سازمانی را کـه منجر به مقاومت و عدم همکاری با توسعه‌ی فناوری اطلاعات شود را به حـداقل مـی‌رسـاند. بعضی از این عوامل با توجه به تجربیات عملی معماری اطلاعـات در سـازمان‌هـا عبارتنـد از؛ چشم‌انداز مشترک سازمان، راهبردهای سازمان، اصول و مبـانی ارزشـی حـاکم بـر سـازمان و اهداف. عوامل یکپارچه‌ساز، عواملی هستند که باعث تقویت انسجام درون‌سـازمانی در جهـت رسیدن به مطلوبیت‌ها می‌شوند و ساز و کارهای درون سازمان را برای دستیابی به اهداف آماده می‌کنند. این عوامل عبارتند از: ساختار و تشکیلات، استانداردها، قوانین و مقررات، فرآیندهای انجام کار و غیره.

با توجه به رویکرد سازمان‌گرا و جدول شماره‌ی (۳) می‌توان این‌گونه جمع‌بنـدی نمـود که سازمان‌ها قبل از انجام معماری اطلاعات باید معماری سازمانی را انجام دهنـد. بـه عبـارت دیگر، تمام عوامل بیرونی و درونی سازمان باید در یک نگاه سیستمی و نظام‌گـرا مـورد توجـه قرار گیرد و پس از آن معماری اطلاعات با توجه به نیازمندی‌های مشخص شده برای افـزایش سرعت، کیفیت و کاهش هزینه‌ها در آنها انجام گیرد. مطالعه‌ی ادبیات سـازمان‌هـای موفـق در انجام معماری اطلاعات، چارچوب و ساختار اولیه‌ی ذیل را به ما ارائه می‌دهد تا با اسـتفاده از آن با روش رویش نظریه، سازمان‌های کشور را مورد مطالعه قرار دهیم و علل عدم موفقیـت و شکست آنها را در انجام معماری اطلاعات تحلیل و بررسی کنیم.

مطالعه‌ی چارچوب‌های معماری اطلاعات در سازمان‌های مختلف حکایت از آن دارد که تمامی آنها از رویکرد سازمان‌گرایی استفاده می‌کنند و با توجه به این رویکرد قبل از اقـدام بـه هرگونه معماری اطلاعات در سازمان باید به معماری سـازمانی در آن پرداختـه شـود. در ایـن معماری دو مؤلفه‌ی اساسی یعنی عوامل وحدت‌بخشی و عوامل یکپارچه‌سازی مـورد بررسـی قرار می‌گیرد. شکل شـماره‌ی (۱) ارتبـاط بـین معمـاری اطلاعـات و عوامـل اصـلی معمـاری سازمانی را نشان می‌دهد که به عنوان ساختار اولیه‌ی تحقیـق مـورد توجـه بـوده و در بررسـی کیس‌ها مبنای تحقیق و بررسی قرار می‌گیرد.



شکل شماره‌ی ۱ - ساختار اولیه‌ی بررسی اجرای معماری اطلاعات

بررسی نمونه‌های عملی تحقیق

همان‌طور که بیان شد در این تحقیق به منظور شناسایی علل و عوامل شکست معماری اطلاعاتی در سازمان‌های دولتی، از روش رویش نظریه استفاده شده است. در این روش که بر مبنای کیس‌های واقعی به جستجو و شناسایی مفاهیم و نظریه‌ها می‌پردازد، نیاز به انتخاب‌های پی‌درپی و وابسته‌ی نمونه‌های مرتبط با تحقیق می‌باشد. پس از بررسی و شناسایی مفاهیم و علل شکست در هر نمونه، نمونه‌ی بعدی انتخاب شده و با دانش به‌دست آمده در نمونه‌های قبلی به بررسی نمونه‌ی جدید با توجه به ساختار اولیه‌ی تحقیق پرداخته می‌شود.

این انتخاب تا زمانی ادامه می‌یابد که روش بررسی نمونه‌ها به مرحله‌ی اشباع برسد. مرحله‌ی اشباع مرحله‌ای است که در آن مرحله با اضافه شدن نمونه و بررسی آن، به یافته‌های تحقیق مفهومی افزوده نمی‌شود. در این مرحله با تشخیص محقق، کار بررسی به پایان می‌رسد.

بررسی نمونه‌ها با گردآوری داده‌ها از روش‌های مختلفی آغاز می‌گردد که از جمله‌ی این روش‌ها می‌توان به مصاحبه‌ی عمیق، بررسی اسناد و مستندات و تکمیل پرسشنامه اشاره نمود. پس از گردآوری داده‌ها لازم است تا مجموعه‌ی آنها به شکلی در

کنار یکدیگر قرار گیرند تا تقدم و تأخر زمانی در آنها رعایت گردد. رعایت تقدم زمانی مطالب و داده‌ها به شناسایی علل و عوامل ریشه‌ای موضوع کمک بسیاری می‌نماید. نواقص و کاستی‌هایی که در یک بازه‌ی زمانی ایجاد می‌شود، در آینده می‌تواند مشکلات بسیاری را به‌وجود آورد که با ملاحظه‌ی این تفاوت زمانی و با شناسایی پیش‌نیازها و وابستگی‌ها می‌توان به علل ریشه‌ای پی برد.

در این تحقیق سعی گردید تا سازمان‌های دولتی به‌گونه‌ای انتخاب شوند تا فعالیت‌های گوناگونی را پوشش دهند و از توجه و تمرکز بر یک حوزه خودداری شود. در حوزه‌های فوق مجموعه‌ی ۱۲ سازمان و نهاد مورد بررسی قرار گرفت که ۸ مورد اول منجر به شناسایی مفاهیم جدید شده و در ٤ مورد بعدی، مفهومی به مدل اضافه نگردید. این ٤ مورد در مرحله‌ی اشباع قرار گرفته و شناسایی نمونه‌های جدید متوقف گردید.

برای منظم نمودن مفاهیم شناسایی شده و شناسایی مفاهیم مشابه، به هر یک از مفاهیم کدی تحت عنوان کد آزاد تخصیص داده شد. با کمک این کد مفاهیم در نمونه‌ها قابل شناسایی و ردیابی می‌گردند.

مفاهیم شناسایی شده به روش کدگذاری آزاد[1] کد گذاری گردیدند. این مفاهیم پس از دسته‌بندی، در قالب ۲۲ عامل محوری طبقه‌بندی شدند که این عوامل در جدول شماره‌ی (٤) مشخص شده‌اند.

همان‌طور که در جدول شماره‌ی (٤) مشاهده می‌شود، پس از بررسی نمونه‌های واقعی در جامعه‌ی ایران، عواملی که باعث عدم موفقیت سازمان‌های کشور در راستای معماری اطلاعات شده‌اند، در سه دسته‌ی زیر مقوله‌بندی شده‌اند.

1 – Free coding

جدول شماره‌ی ٤ – عوامل محوری شکست معماری اطلاعات

مقوله	عامل	تعداد نمونه‌های مرتبط
عدم آمادگی عوامل وحدت‌بخشی	مشخص نبودن معماری کلان دولت	٦
	مشخص نبودن چشم‌انداز مشترک و راهبرد	٨
	مشخص نبودن ارزش‌ها، اصول و سیاست‌ها	٦
	مشخص نبودن اهداف کلان سازمان	٧
	تغییرات در پیش‌روی مأموریت و کسب و کار	١
عدم آمادگی عوامل یکپارچگی	عدم توجه به مدل‌سازی فرآیندها	٥
	فرهنگ نامناسب و بلوغ سازمانی پائین	٩
	بی‌توجهی به قوانین و مقررات	١
	ساختار و تشکیلات نامناسب و نظام نگهداری	٧
	شناخت نادرست نیازهای اطلاعاتی سازمان	٣
	ضعف در استانداردسازی	٣
عدم آمادگی عوامل رفتاری	عدم باور مدیریت ارشد	١٠
	نبود انگیزه برای کارکنان	١٢
	مقاومت در برابر تغییر	١٢
	نبود آموزش کافی	١١

شبکه‌ی مفهومی مؤثر بر شکست معماری اطلاعات

موضوعات انسانی و به‌ویژه فعالیت‌های تحولی از پیچیدگی‌های بالایی برخوردارند و نمی‌توان به سادگی به دلایل موفقیت یا شکست آنها پرداخت. در شکل‌گیری هر پدیده‌ای می‌تواند عوامل مختلفی دخیل باشد که هر یک از آنها بر روی یکدیگر تأثیر گذاشته و یکدیگر را تقویت یا تضعیف می‌نمایند. در این تحقیق به منظور شناسایی ارتباطات بین عوامل، از شبکه‌ی مفهومی استفاده شده است. در این شبکه‌ی ارتباطات و پیش‌نیازی‌ها و پس‌نیازی‌های عوامل مشخص شده‌اند. دو پارامتر در وزن‌دهی به هر عامل در نظر گرفته شده است که ارتباط مستقیم با شکست و دیگری تعداد ارتباطات غیرمستقیم با سایر عوامل می‌باشد.

همه‌ی عوامل به یک اندازه بر روی شکست تأثیرگذار نیستند. تعدادی از عوامل مستقیماً و تعدادی نیز غیرمستقیم تأثیر می‌گذارند که تعیین تأثیرات از طریق تحلیل شبکه‌ی مفهومی امکان‌پذیر است. بررسی شبکه‌ی مفهومی عوامل شکست منجر به شناسایی عوامل زیر که مستقیماً به شکست معماری منجر می‌شوند، گردید.

عوامل وحدت‌بخشی:

- مشخص نبودن چشم‌انداز؛
- مشخص نبودن اهداف کلان؛
- مشخص نبودن راهبردها.

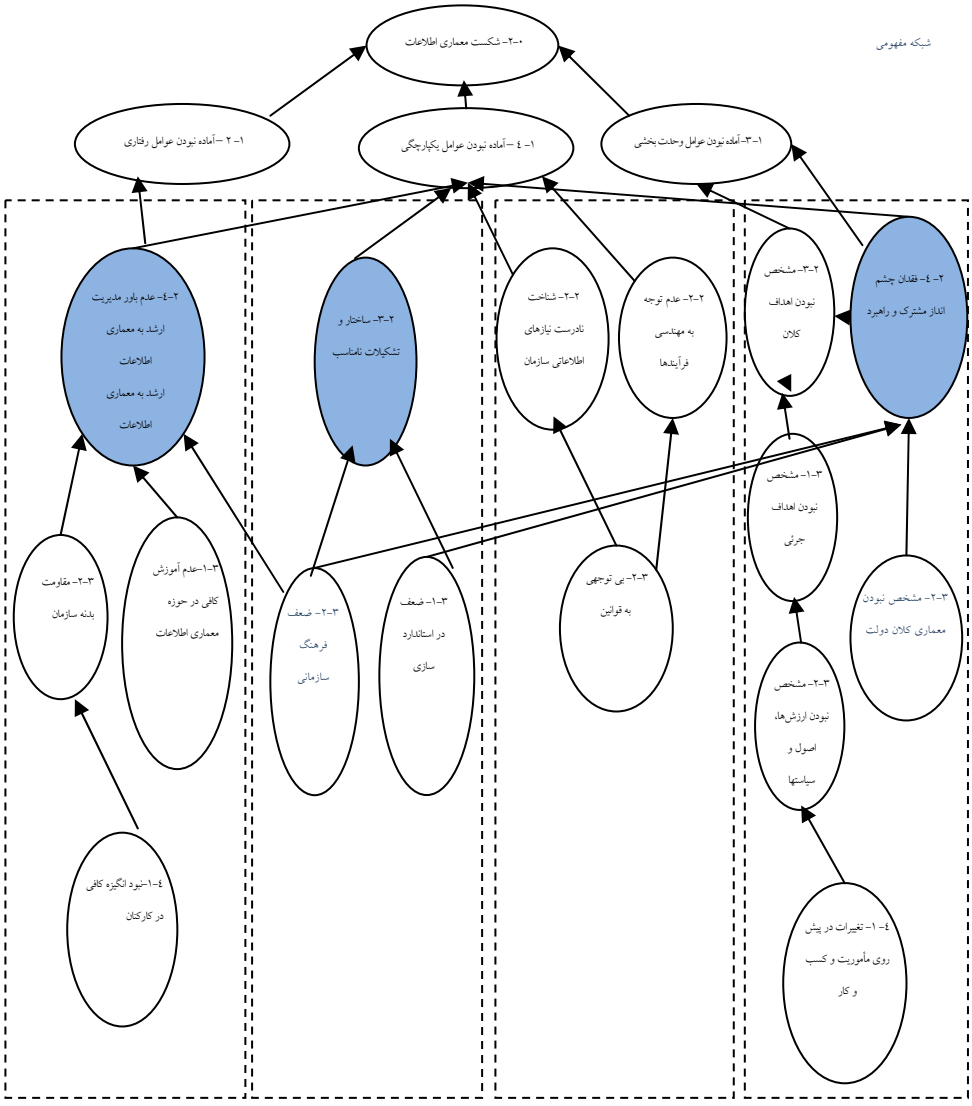
عوامل یکپارچگی:

- بی‌توجهی به قوانین و مقررات؛
- عدم توجه به مهندسی فرآینده؛ا
- شناخت نادرست نیازهای اطلاعاتی سازمان؛
- ساختار و تشکیلات نامناسب.

عوامل رفتاری:

- عدم باور مدیران ارشد به معماری اطلاعات؛
- مقاومت بدنه‌ی سازمان؛
- نبود انگیزه‌ی کافی در کارکنان؛
- نبود مهارت و دانش کافی در کارکنان.

این عوامل مستقیما بر شکست تلاش‌های معماری اطلاعات تأثیرگذار هستند و سایر عوامل از طریق آنها شکست را ایجاد می‌کنند. شبکه‌ی مفهومی عوامل شکست معماری را نشان می‌دهد.



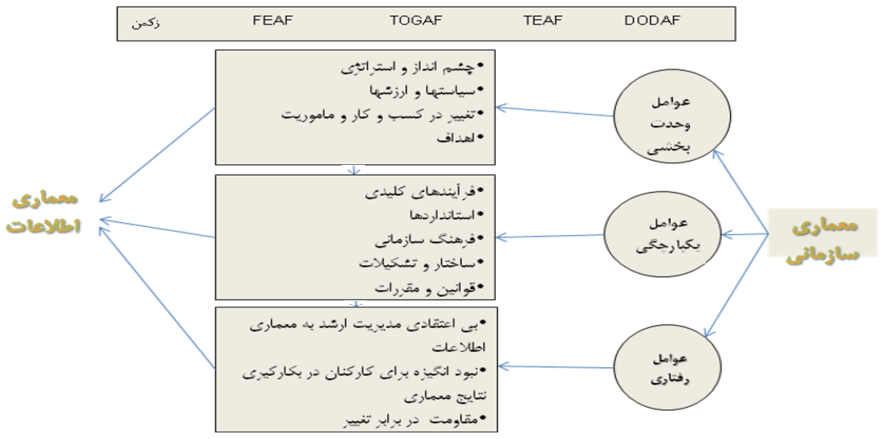
شکل شماره‌ی ۲ – شبکه‌ی مفهومی عوامل شکست معماری اطلاعات

همان‌طور که در شکل مشخص است، عوامل مختلف با تأثیراتی که بر روی یکدیگر می‌گذارند، منجر به شکست معماری اطلاعات می‌شوند. هر چه یک عامل در سطح بالاتری قرار

داشته باشد، نشان‌گر تأثیر مستقیم بر شکست معماری خواهد بود. از طرفی تعداد ارتباطات آن با سایر عوامل بیان‌گر تأثیر آن در شکست است. از مجموع این متغیرها، اهمیت و نقش عوامل مختلف مشخص می‌شود. آن‌چه مشخص است، مهم‌ترین و کلیدی‌ترین دلایل شکست معماری اطلاعات، انجام ندادن معماری سازمانی و آماده‌سازی ساز و کارهای ضروری در سازمان می‌باشد.

الگوی معماری سازمانی به عنوان زمینه‌ساز معماری اطلاعات

نتیجه‌ی بررسی نمونه‌ها مشخص می‌نمایند که عمده‌ی دستگاه‌های دولتی کشور در اجرای معماری اطلاعات، سه زمینه و پیش‌نیاز اصلی که شامل عوامل وحدت‌بخشی و یکپارچگی و رفتاری می‌شود را نادیده می‌گیرند. این سه عامل، شالوده‌ی اصلی معماری سازمانی را تشکیل می‌دهند. معماری سازمانی با بررسی لایه‌های راهبردی و فرآیندهای سازمان سعی در فراهم نمودن بسترهای لازم جهت اجرای صحیح معماری اطلاعات دارد. دستگاه‌های دولتی با توجه به قدمت و کهنگی ساختارها و فرآیندهای انجام کار و تغییرات محیطی بدون انجام معماری سازمانی، اقدام به معماری اطلاعات می‌نمایند و این بی توجهی، به‌عنوان اصلی‌ترین عامل، مقدمه‌ی شکست آنها را فراهم می‌کند.



شکل شماره‌ی ۳ – مدل مفهومی معماری سازمانی به عنوان پیش‌نیاز معماری اطلاعات

عامل وحدت‌بخش یا هم‌سوساز سازمان با استفاده از خط‌مشی روشن ومشخص، دستیابی به اهداف و مأموریت‌های از پیش تعیین شده را محقق می‌سازد. بدیهی است، بدون مشخص بودن مسیر نهایی و جایگاه سازمان در دیدگاه طراحان آن، نمی‌توان نظام واحدی را ایجاد نمود. یکی از عوامل اصلی شناسایی شده‌ی تأثیرگذار بر شکست معماری اطلاعات مشخص نبودن چشم‌اندازها و راهبردها می‌باشد. این عامل تأثیر مستقیمی بر شکست معماری اطلاعات خواهد داشت. معماری اطلاعات فرآیندی است که از طریق آن وحدت بین کلیه‌ی اجزای سازمان ایجاد می‌شود. این وحدت موجب حرکت سازمان به سمت چشم‌اندازها، راهبردها و اهداف آن می‌شود. زمانی که لایه‌های راهبردی سازمان به‌درستی شناخته نشده و یا مورد بی‌توجهی قرار گیرند، وحدت اجزاء بی‌معنی خواهد بود؛ چرا که هدف مشخصی برای ایجاد وحدت وجود ندارد. حتی در صورتی‌که گام‌های مختلف معماری اطلاعات با دقت و تلاش بی‌وقفه تا حصول نتیجه‌ی پیگیری و اجرا شود، معماری ایجاد شده سازمان را به انتظارات نهایی خود نمی‌رساند.

همگام با تغییر در اهداف و چشم‌انداز مشترک سازمان، عوامل و ساختارهای درون‌سازمانی باید مهندسی شود تا یک نوع مفاهمه و ادبیات مشترک در سازمان برای رسیدن به آنها به‌وجود آید. بنابراین، توجه به عوامل یکپارچه‌ساز نظیر مهندسی فرآیندها از مشکلات محوری دوم سازمان‌های دولتی کشور می‌باشد.

پس از مشخص شدن جایگاه سازمان و هدف غایی آن، لازم است تا کلیه‌ی اجزاء در جهت آن هدف به شکلی یکپارچه با یکدیگر تعامل داشته باشند. سازمان را نمی‌توان اجزایی منفصل از هم ترسیم نمود. چرا که هر جزئی از دیگر اجزا جدا نبوده و نیازمند ورودی‌ها و خروجی‌هایی است. یکپارچه‌سازی درونی اجزاء لازمه‌ی شروع معماری اطلاعات می‌باشد که سازمان‌های کشور از تأمین آن قبل از شروع معماری اطلاعات غافل می‌مانند. ایجاد سیستم‌ها و نرم‌افزارها در سازمانی که بستر یکپارچگی در آن به‌وجود نیامده است، راهی به‌سوی شکست خواهد بود.

عوامل رفتاری از جمله‌ی عوامل دیگری است که منجر به شکست معماری در سازمان‌های کشور می‌شود. علت این امر آن است که در کشور ما زیرساخت‌های مدیریتی و انسانی آماده نمی‌باشد. در این وضعیت بدون آموزش، انگیزه‌سازی و ایجاد بسترهای انسانی و مدیریتی لازم به سراغ اجرای پروژه‌های تحولی این چنینی می‌روند.

این عامل نشان می‌دهد که سازمان‌های کشور قبل از انجام معماری اطلاعات باید به یک عزم و اراده‌ی واحد برسند تا در عمل همگام با اهداف سازمان در جهت انجام معماری اطلاعات حرکت کنند.

این مدل نشان می‌دهد که هر سه عامل وحدت‌بخشی و یکپارچگی و رفتاری از ملزومات بسیار حیاتی معماری اطلاعات می‌باشند که خود جزئی از معماری سازمانی هستند. بنابراین، با استفاده از مطالعه‌ی میدانی نمونه‌ها می‌توان در یک جمع‌بندی کلی، معماری سازمانی را زمینه‌ساز اصلی معماری اطلاعات و نقطه‌ی ضعف دستگاه‌های دولتی کشور در این حوزه دانست.

خطاسنجی

به منظور بررسی نظریه‌ها، لازم است تا خطای احتمالی آنها بررسی شود. مبنای خطاسنجی در این تحقیق قانون «رفع مؤلفه»[1] می‌باشد. این قانون توسط «کارل پوپر»[2] اتریشی مطرح شده است و بیان می‌کند که زمانی که دلایل کافی برای رد یک نظریه وجود نداشته باشد، کفایت نظریه تا زمان بروز شواهد رد، وجود خواهد داشت.

«پوپر» در سال ۱۹۸٤ برای این بررسی، سه شرط مقدماتی و یک شرط کفایت پیشنهاد کرده است که چهار گام خطاسنجی را بیان می‌کنند.

گام ۱: بررسی اجزای نظریه به منظور اطمینان از عدم وجود تناقض بین اجزای داخلی نظریه:

- مجموعه‌ی عبارات مستقل نظریه با یکدیگر تناقض نداشته باشند.

1 – Modus Tolens
2 – Karl Poper

- مجموعه‌ی عبارات وابسته نظریه با یکدیگر تناقض نداشته باشند.
- هیچ یک از اصول و یا فرضیه‌های مستقل درون خود دچار تناقض نباشند.

در صورت وجود سه شرط فوق، نظریه دارای سازگاری داخلی بود و استنتاج نتایج از مقدمه آن مجاز می‌باشد.

در این طرح بی‌توجهی به عوامل وحدت‌بخشی و یکپارچگی با این شرط‌ها بررسی شده و شروط فوق در آنها محقق شدند. بنابراین، ادامه‌ی استنتاج مجاز می‌باشد.

گام ۲: تفکیک بخش‌های منطقی و تجربی نظریه:

در این گام، بخش‌های منطقی نظریه بررسی شده و از ارزش منطقی آنها اطمینان حاصل می‌گردد. برای بررسی بخش‌های منطقی از شروط زیر استفاده می‌شود:

- بخش‌های منطقی نظریه می‌بایست عاری از تناقض باشند.
- قضایای منطقی می‌بایست از یکدیگر مستقل باشند.
- استنتاجات قیاسی می‌بایستی به نحو صحیحی صورت گرفته باشد.
- قضایای منطقی می‌بایستی ضرورتاً به کار گرفته شده باشند.

برای بخش تجربی، پوپر شرط آزمون‌پذیری را ذکر می‌کند و بیان می‌کند؛ در صورتی که هیچ پدیده‌ای آن‌را ابطال نکند، این نظریه دارای خصوصیات نظریه علمی است. از طرفی باید بخش‌های تجربی به دنیای واقعی و یا دنیای تجربیات متعلق باشد. برای این منظور سه شرط زیر ذکر می‌شود:

- وقوع پدیده‌ی مورد بحث در نظریه «ممکن» باشد.
- نظریه حاوی مفاهیم ماوراءالطبیعه نباشد، بلکه متعلق به دنیای تجربیات باشد.
- حوزه‌ی نظریه می‌بایستی به نحوی از سایر حوزه‌ها قابل تمیز باشد.

شروط مرتبط با بخش‌های منطقی و تجربی با استفاده از جدول شماره‌ی (۵) بررسی شده و محقق گردیدند.

جدول شماره‌ی ۵ – تفکیک بخش‌های منطقی و تجربی نظریه

بخش منطقی	بخش تجربی
نظریه‌ی عدم آمادگی عوامل وحدت‌بخشی	• مشخص نبودن چشم‌انداز و راهبردها • مشخص نبودن اهداف کلان
نظریه‌ی عدم آمادگی عوامل یکپارچگی	• عدم توجه به مدل‌سازی فرآیندها • شناخت نادرست نیازهای اطلاعاتی سازمان • ساختار و تشکیلات نامناسب
نظریه‌ی عدم آمادگی عوامل رفتاری	• بی‌اعتقادی مدیریت ارشد • بی‌انگیزه بودن کارکنان • نداشتن دانش و مهارت‌های لازم در اجراء

گام ۳: سنجش قدرت پیش‌بینی نظریه:

در این مرحله قدرت پیش‌بینی نظریه بررسی می‌شود. در مواردی که نظریات مطروحه در این زمینه وجود دارد، می‌توان قدرت بهتر و یا ضعیف‌تر نظریه را نسبت به نظریات قبلی مقایسه نمود. اما در ارتباط با تحقیق فوق، به‌دلیل عدم وجود نظریات قبلی، نمی‌توان مقایسه‌ای انجام داد و از این‌رو، صحت پیش‌بینی نظریه‌ی فوق بررسی می‌گردد. به این منظور در پیش‌بینی نمونه‌های بررسی شده قدرت پیش‌بینی نظریه بررسی می‌شود.

با بررسی بی‌توجهی به عوامل وحدت‌بخشی و یکپارچگی و رفتاری در نمونه‌های موجود، مشخص می‌شود که نظریات فوق به‌خوبی پدیده‌های نمونه‌های بررسی شده را پیش‌بینی و تحت پوشش فرار می‌دهد.

گام ٤: بررسی کارکرد تجربی:

در این گام نظریه باید قادر به توضیح نمونه‌های عملی (Case) باشد. به‌دلیل آن‌که نظریات ارائه شده در این تحقیق بر پایه‌ی تجربیات واقعی بنا شده است، این گام نیز مورد تأیید می‌باشد.

بنابراین، بر اساس خطاسنجی صورت گرفته، نظریات مطرح شده قابل ارائه بوده و از کفایت لازم برخوردارند.

نتیجه‌گیری

مقاله‌ی حاضر با توجه به خلاء بررسی جامعی در زمینه‌ی علل ناکامی تلاش‌های معماری اطلاعاتی به بررسی نتایج پروژه‌های صورت گرفته پرداخته و در این مسیر از روش رویش نظریه استفاده نموده است. با بررسی ۱۲ سازمان در حوزه‌های فعالیت مختلف، ۲۲ مفهوم ناکامی معماری اطلاعاتی شناسایی گردید که نتیجه‌ی بررسی و تجزیه و تحلیل این عوامل و روابط بین آنها، شناسایی نظریات عدم موفقیت معماری اطلاعاتی می‌باشد.

یافته‌های مقاله‌ی حاضر به شرح ذیل می‌باشند:

- متدلوژی‌های معماری اطلاعات بر پایه‌ی رویکرد سازمان‌گرا بنا نهاده شده‌اند. این موضوع اهمیت توجه به سازمان و تمامی ابعاد آن در تدوین و اجرای معماری اطلاعات را نشان می‌دهد. در صورتی‌که معماری اطلاعات، تنها به عنوان یک موضوع فناوری اطلاعات و ارتباطات دیده شده و ورودی‌های سازمانی آن تأمین نشوند، نمی‌توانند نتیجه مطلوبی را ایجاد نمایند. از این‌رو، توجه به کلان‌سازمان در انجام معماری اطلاعات از ضروریات است.
- با توجه به رویکرد سازمان‌گرا، توجه به معماری سازمانی قبل از انجام معماری اطلاعات ضروری است. معماری سازمانی رویکردی ارائه می‌دهد تا امکان تأمین پیش‌زمینه‌های معماری اطلاعات فراهم گردد. معماری سازمانی با اتصال لایه‌های بالای سازمان نظیر چشم‌انداز، راهبردها، فرآیندها و ساختارها به موضوعات درون سازمانی نظیر فناوری‌ها و سیستم‌ها، موفقیت آنها را تضمین می‌نماید.
- در معماری سازمانی آماده‌سازی سه مؤلفه‌ی وحدت‌بخشی، یکپارچه‌سازی و رفتاری پیش‌زمینه، آغاز معماری اطلاعات می‌باشد. معماری سازمانی در یک نگاه کلان پیش‌زمینه‌های آغاز معماری اطلاعات را در این سه مقوله می‌داند. وحدت‌بخشی تمامی اجزای سازمان را به سمت و سوی واحدی هدایت می‌نماید.

- دلایل ناکامی شناسایی شده در بررسی نمونه‌های واقعی اجرای معماری اطلاعات در سازمان‌های کشور بیان‌گر این واقعیت هستند که آنها بدون توجه به معماری سازمانی، اقدام به اجرای معماری اطلاعات نموده‌اند.

پیشنهادها

پیشنهادهای زیر در زمینه‌ی رفع خلاءهای موجود و ادامه‌ی روند این تحقیق، ارائه می‌گردند.

۱) بازنگری و شناسایی نقاط ضعف چارچوب معماری ملی ایران با توجه به یافته‌های تحقیق و انجام اصلاحات لازم برای جلوگیری از شکست‌های آتی؛

۲) تشکیل ستاد معماری سازمانی در معاونت نظارت راهبردی ریاست جمهوری با توجه به فرمان ۱۸ ماده‌ای مقام معظم رهبری برای اصلاح نظام اداری؛

۳) تدوین معماری کلان نظام اداری و دفاعی در راستای تحقق دولت الکترونیک و انجام و مهندسی ساختارها و فرآیندهای دستگاه‌های مربوطه برای انجام معماری اطلاعات؛

٤) در راستای معماری سازمانی، جهت شفاف‌سازی عوامل وحدت‌بخش و همسوساز در دستگاه‌های دفاعی و اجرایی کشور، لازم است به شرح ذیل فعالیت‌های مختلفی صورت گیرد:

- مهندسی ساختار کلان و ساختار تشکیلاتی دستگاه‌های مربوطه قبل از معماری اطلاعات؛
- مهندسی قوانین و مقررات و استانداردهای سازمان‌ها و هم‌چنین سایر فرآیندهای پشتیبان؛
- مهندسی فرآیندهای کلیدی و زنجیره‌ی ارزش سازمان جهت شفاف‌سازی مأموریت و رسالت آن.

۵) با توجه به انجام معماری سازمانی، عزم و مفاهمه بین مدیران و کارشناسان به شرح ذیل انجام گیرد:

- ایجاد ادبیات و باورهای مشترک نسبت به معماری اطلاعات در لایه‌های مختلف سازمان؛

- تقویت قابلیت‌ها و مهارت‌های کارکنان و متولیان نسبت بـه توسـعه‌ی فنـاوری اطلاعات و ارتباطات در سازمان.

٦) مشارکت دادن متخصصـین و کارشناسـان در تصـمیم‌سـازی و تصـمیم‌گیـری انجـام معماری اطلاعات.

منابع

فارسی

۱- غفاریان، وفا، (۱۳۸۲)، «***بررسی علل شکست برنامه‌ریزی‌های راهبردی و ارائه یک رویکرد برای بهبود اثربخشی راهبرد در سازمان‌های صنعتی ایران***»، دانشگاه علم و صنعت ایران.

۲- فتح الهی علی، نیکوفر حمیدرضا، شمس فریدون، (۱۳۸٤)، «***چارچوب ملی معماری سازمانی ایران، الگوی تدوین طرح جامع فناوری اطلاعات در سازمان‌ها***»، دبیرخانه شورای عالی اطلاع رسانی.

۳- عباسی، محمدعلی، همکاران، (۱۳۸٤)، «***راهنمای عملی برنامه‌ریزی معماری سازمانی***»، ناشر مؤسسه فرهنگی دیباگران تهران،تهران ،آذر.

٤- میرعباسی ،رمضان ، (۱۳۸۹)، «***بررسی علل شکست معماری اطلاعات در دستگاه‌های دولتی وطراحی و تبیین الگوی مفهومی جهت رفع مشکلات آن***».

انگلیسی

5- Buchanan, R., (2001), "***Assessing Enterprise Architecture Program Value***", Meta Group Report 128, The meta group, 208 Harbor Drive, Stanford, CT 06912-0061.

6- Clinger, Cohen, (1996), "Act of. Available: Cio- nii.defense, gov/docs/ciodesrefvolone . pdfs.

7- Federal Government CIO council, (2001), "***Federal enterprise architecture***", NewYork, Springer INC.

8- IEEE., (1990), "***IEEE standard glossary of software engineering terminology***", as extended in the C4ISR architecture framework v2.0 (IEEE-STD 610.12).

9- Mansourian, Y, (2006), "***Adoption of Grounded Theory in LIS research***". New Library World, Vol. 107 No. 9/10.

10- Morganwalp, Jill. sage, Andrew, (2003), "***A system of system focused enterprise architecture framework and an associated architecture development process***", Information knowledge systems management, vol 3.

11- O'Rourke, Carol and fishman , Neal, (2003), "***Enterprise architecture using the Zachman framework*** , Thomason.

12- Sowa, J. F. and Zachman, J. A., (1992), "***Extending and formalizing the framework for information systems architecture***", IBM systems journal 31, No.3.

13- Strauss, A. and Corbin, J., (1994), "***Grounded theory methodology an overview***", in N.K. Denzin and Y.S. Lincoln, (Eds), Handbook of Qualitative Research, Sage, Thousand Oaks.

14-Zachman, John, (1987), "***A framework for*** Information ***systems architecture***", IBM systems Journal 26, No.3.

مجله سیاست دفاعی
سال بیستم، شماره ۷۹، تابستان ۱۳۹۱

ارائه چارچوبی برای مفهوم‌سازی رزم اطلاعاتی

علیرضا فرشچی [۱]
احسان مرآتی [۲]

تاریخ دریافت مقاله: ۱۳۹۱/۱۲/۱۰
تاریخ تأیید مقاله: ۱۳۹۱/۰۳/۲۰
صفحات مقاله: ۱۲۹ – ۹۷

چکیده:

قابلیت‌های روز افزون فناوری اطلاعات موجب گردیده تا حوزه‌ی دفاعی به‌عنوان یکی از حوزه‌های حساس و مهم، پیوسته به دنبال توسعه و به‌کارگیری قابلیت‌های بروز فناوری اطلاعات باشد. این امر موجب شده تا گاهی حوزه‌ی دفاعی مبدع بروزترین فناوری‌های اطلاعاتی باشد، از طرفی، محققین به‌منظور بسترسازی توسعه‌ی کاربردهای فناوری اطلاعات در حوزه‌ی دفاعی به مفهوم‌سازی کاربردهای مربوطه پرداخته‌اند. از این رو، حضور و ظهور فناوری اطلاعات در حوزه‌ی دفاعی موجب شکل‌گیری مفاهیمی نظیر رزم سایبری [۳]، رزم مبتنی بر شبکه [۴] و رزم الکترونیک [۵] شده است. بر اساس ادبیات، اکثر این اصطلاحات در حوزه‌ی رزم اطلاعاتی [۶] قرار می‌گیرند. با این حال، از لحاظ نظری چگونگی ارتباط بین مفاهیم گوناگون و چگونگی پوشش دان آنها توسط رزم اطلاعاتی به‌خوبی تبیین نشده است. از این رو، پژوهش حاضر به‌واسطه‌ی مطالعه و تحلیل مدل‌ها و مفاهیم موجود در حوزه‌ی رزم اطلاعاتی و مقایسه و مطالعه‌ی تطبیقی آنها به تبیین چارچوبی چند بُعدی برای مفهوم‌سازی رزم اطلاعاتی پرداخته است. این چارچوب تمامی اصطلاحات موجود در حوزه‌ی رزم اطلاعاتی را پوشش داده و به تبیین و تحلیل ابعاد گوناگون و زیربنایی رزم اطلاعات می‌پردازد. این چارچوب، می‌تواند به‌عنوان مبنایی برای نقد پژوهش‌های حوزه‌ی رزم اطلاعاتی مورد استفاده قرار گرفته و به آشفتگی مفاهیم حوزه‌ی رزم اطلاعاتی نظم بخشد که این نظم به نوبه‌ی خود منجر به شکل‌گیری تفکر ساختاریافته در حوزه‌ی رزم اطلاعاتی و پیشرفت آن در ابعاد گوناگون زیربنایی می‌گردد.

---

۱ – رئیس مرکز مطالعات دفاعی و امنیت ملی.
۲ - دانشجوی دکترای مدیریت سیستم، دانشکده مدیریت، دانشگاه تهران.

3 – Cyber Warfare
4 – Net-Centric Warfare
5 – Electronic Warfare
6 – Information Warfare

* * * * *

واژگان کلیدی

فناوری اطلاعات، رزم اطلاعاتی، رزم دانش محور، رزم اطلاعات راهبردی، رزم مبتنی بر شبکه.

مقدمه

فناوری اطلاعات[1] از سال ۱۹۸۰ میلادی تاکنون تغییر و تحولات بسیاری را تجربه نموده که از جمله آنها می‌توان به تغییرات سریع سیستم‌های کامپیوتری و شبکه‌های ارتباطات برخط[2] اشاره نمود. برخی روندهای گذشته در جهت پیشبرد فناوری و آنچه که امروز در اختیار داریم، حرکت کرده‌اند و برخی اثر و حرکت معکوس داشته‌اند و لذا پس از مدت کوتاهی ناپدید شده‌اند (Silberglitt et al., 2006). امروزه، فناوری اطلاعات مفهومی گسترده است که حوزه‌های متنوعی را در خود جای داده است و به‌دلیل برخورداری از قابلیت‌های گوناگون، در حوزه‌های مختلف مورد استفاده قرار گرفته است. از طرفی، به دلیل اهمیت اطلاعات در حوزه‌ی دفاعی، به‌کارگیری فناوری اطلاعات در حوزه‌ی دفاعی توجیه‌پذیر می‌باشد و کشورهای مختلف با وجود صرف هزینه‌های زیاد به به‌کارگیری جدیدترین دستاوردهای فناوری اطلاعاتی در حوزه‌ی دفاعی ترغیب شده‌اند (Janczewski and Colarik, 2008). در فضای رزم، اجرای موفق یک عملیات نظامی مستلزم اطلاع حاضرین در صحنه از اهداف عملیات، روش دستیابی به آنها، قابلیت‌ها و فعالیت‌های دشمن، شرایط آب و هوایی و منطقه، میزان محرمانگی عملیات و سایر عواملی است که ممکن است هر لحظه تغییر کنند. الزام به مدیریت مؤثر اطلاعات و همچنین لزوم مورد هدف قرار دادن سیستم‌ها و منابع اطلاعاتی دشمن موجب شکل‌گیری مفهومی به نام رزم اطلاعاتی گردیده است (Janczewski and Colarik, 2008).

1 – Information Technology (IT)
2 – Online

رزم اطلاعاتی یکی از حوزه‌های مطالعاتی نسبتاً جدید است. دکتر توماس رونا[1] در سال ۱۹۷٦ میلادی به واژه‌ی رزم اطلاعاتی اشاره نمود (Halpin et al., 2006). از آن زمان به بعد، تعاریف مختلفی با تأکید بر جنبه‌های نظامی ارائه شد. امروزه، منظور از جنگ اطلاعاتی یا جنگ سایبر، به تعارضات سیاسی، اقتصادی، حقوقی، امنیتی، مدنی و نظامی است. تعاریف دیگر ارائه شده از رزم اطلاعاتی، آن را اقداماتی با هدف حفاظت، بهره‌گیری، تخریب، تحریف، یا نابود کردن اطلاعات یا منابع اطلاعاتی و کسب مزیت نسبت به دشمن یا حصول به هدفی خاص می‌دانند. کرونین و کراوفورد[2] (۱۹۹۹) چارچوبی را برای رزم‌های اطلاعاتی ارائه نموده‌اند که از حیطه‌ی نظامی فراتر رفته است. آنها بر این باورند که نبردهای این‌چنینی شدت خواهند گرفت و مشکلات اجتماعی و چالش‌های حقوقی جدیدی را به جامعه تحمیل خواهند کرد.

هنوز در مورد نقش و اثربخشی بالقوه‌ی اطلاعات و فناوری‌های اطلاعاتی در فضای نبرد، بحث و اختلاف‌نظر وجود دارد. برخی نقش اطلاعات و سیستم‌های اطلاعاتی را کار کردن روی ذهن افراد (عام و خاص) و قانع ساختن آنها به همراهی می‌دانند تا از این طریق، نیاز به تقابل فیزیکی به حداقل برسد. حامیان این دیدگاه می‌کوشند به «تعالی برتر»[3] و تفوق مورد نظر «سان تزو»[4] که همان «شکستن مقاومت دشمن، بدون جنگیدن» است، دست یابند. زافرانسکی[5] (۱۹۹۵) این دیدگاه را توسعه داده و معتقد است هدف راهبردی می‌تواند به‌جای مواضع فیزیکی دشمن، شناخت‌شناسی[6] (سیستم باورها و عقاید) او باشد و از نیروی نظامی به‌عنوان ابزار ثانویه بهره‌گیری شود.

یکی از اثرات به‌کارگیری فناوری اطلاعات در فضای رزم، گسترش میدان جنگ ماورای مرزهای سنتی آن است. سلاح‌ها و اهداف اطلاعاتی بخش‌مهمی از سرمایه‌های زیرساختی ملت‌ها را

1 – Thomas Rona
2 – Cronin & Crawford
3 – Supreme excellence
4 – Sun Tzu
5 – Richard Szafranski
6 – epistemology

تشکیل می‌دهند. در گذشته ارتش‌ها، با سلاح‌های نظامی به اهداف نظامی حمله می‌کردند؛ اما در نبرد اطلاعاتی همه‌ی منابع و فرآیندهای اطلاعاتی یک ملت می‌توانند سلاح و اهداف بالقوه جنگی به‌شمار روند. برخی دیگر نیز حمله‌ی اطلاعاتی و نشانه رفتن ادراک و باورهای شخصی را اقدامی تکمیلی در عملیات نظامی می‌دانند و آن را جایگزین حمله‌ی نظامی نمی‌دانند، بلکه مکمل آن تلقی می‌کنند. اطلاعات می‌تواند کاربرد یک سلاح را داشته باشد و استراتژیست‌ها باید با دقت و احتیاط از آن بهره گیرند. استراتژیست‌ها باید برای استفاده از اطلاعات به موازات سلاح‌های رایج دیگر برنامه‌ریزی نمایند و پیش از انجام عملیات نظامی و حمله فیزیکی، از آن بهره گیرند (Cronin & Crawford, 1999). در واقع، طیفی از انواع رزم‌ها وجود دارد که هر کدام برای دستیابی به اهداف خود نیازمند ترکیب خاصی از نیروهای فیزیکی و نیروهای اطلاعاتی هستند. جنگ‌های روانی و اقتصادی از جمله نبردهایی هستند که ابزارهای اطلاعاتی و شبکه‌های جهانی، آنها را به بهترین وجه پیاده‌سازی می‌کنند. در مجموع اکثر ادبیات مرتبط با جنگ‌های اطلاعاتی و سایبری به ابعاد نظامی آن پرداخته‌اند. در حالی که، رزم اطلاعاتی خود را به حوزه‌های غیرنظامی نیز توسعه داده است (Cronin & Crawford, 1999).

با همه‌ی این اوصاف، یکی از نکات قابل تأمل در حوزه‌ی رزم اطلاعاتی، مفاهیم متعددی است که برای تبیین چیستی رزم اطلاعاتی و تشریح ابعاد آن ذکر گردیده است. پژوهشگران از اصطلاحاتی نظیر رزم سایبری، رزم مبتنی بر شبکه، رزم مبتنی بر دانش و رزم الکترونیک برای تبیین رزم اطلاعاتی بهره گرفته‌اند. این امر موجب آشفتگی در مفاهیم مطروحه و عدم تبیین دقیق چیستی و ابعاد رزم اطلاعاتی گردیده است. از این رو، این مقاله به ارائه‌ی چارچوبی برای رزم اطلاعاتی می‌پردازد که در آن با تبیین ابعاد زیربنایی رزم اطلاعاتی و پوشش دادن اصطلاحات مطروحه در حوزه‌ی رزم اطلاعاتی، به مفهوم‌سازی بنیادین رزم اطلاعاتی پرداخته شده است.

اطلاعات در فضای رزم

اندیشمند چینی «سان تزو» به اهمیت اطلاعات دقیق و به‌موقع برای فرماندهان نظامی اشاره نموده است. او در این گفتار کوتاه به ابعادی از رزم اشاره نموده که اطلاعات نقش مهمی در تصمیم‌گیری‌های مربوط به آنها دارد؛ اولین آنها شناخت دشمن است (Tzu, 1971).

شناخت دشمن

یک فرمانده‌ی جنگی به مجموعه‌ای از اطلاعات مختلف در مورد دشمنی که در مقابلش صف‌آرایی کرده، نیاز دارد: تعداد نیروهای دشمن، نوع و تعداد تجهیزات جنگی در اختیار دشمن، موقعیت مکانی آنها، آمادگی آنها برای مبارزه، مشخصات پایگاه تدارکات[1] آن، اهداف مدنظر فرمانده‌ی دشمن و موارد این‌چنینی. هرچه تصویر کامل‌تر و دقیق‌تری از دشمن موجود باشد، برنامه‌ریزی برای عملیات و چیدمان نیروها و منابع به نحو بهتری صورت خواهد گرفت و آمادگی نیروها برای مقابله با حوادث و وقایع آتی بیشتر خواهد بود.

ماهیت رزم ایجاب می‌کند که کسب دانش در خصوص دشمن همواره با نقایص فراوان همراه باشد. کلاوزویتس[2] نیز با این باور موافق است. وی بیان می‌دارد که بخش زیادی از اطلاعات گردآوری شده در جریان جنگ‌ها متناقض هستند و بخش قابل‌توجه دیگری غلط بوده و به باقیمانده اطلاعات که بخش اعظم آن نیز می‌باشد، با تردید نگریسته می‌شود. کلاوزویتس این اطلاعات را به دیدن صحنه‌ای از پشت مه یا زیر نور سپیده دم تشبیه می‌کند. او بر این باور است که مشکل بودن گردآوری اطلاعات درست، یکی از منابع اصلی اصطکاک و حساسیت در جنگ‌ها به شمار می‌رود.

برای ارزیابی اعتبار دیدگاه‌های کلاوزویتس نگاهی به کیفیت اطلاعات در دسترس فرماندهان نیروهای چندملیتی متفقین در جنگ خلیج می‌اندازیم. هیچ نیروی نظامی تاکنون اطلاعاتی در این حد کامل و روشن از دشمن خود در اختیار نداشته است: طی پنج ماه پشتیبانی توان رزمی نیروها و شش هفته نبرد، متفقین در مقابله با نیروهای عراقی از حسگرهای هوابرد، گیرنده‌های امواج الکترونیک، و نیروهای اطلاعاتی ویژه‌ای بهره‌مند بودند. با این حال، پس از جنگ مشخص شد، فرماندهان متفقین و تحلیل‌گران کلیدی آنها، تصوری نادرست از دشمن داشته‌اند و در مواردی کلیدی مرتکب اشتباهاتی در ارزیابی شده‌اند. آنها قدرت نیروی زمینی عراق را به نحو درستی برآورد نکرده بودند و توان عراق در تولید

1 – Logistic
2 – Clausewitz

سلاح‌های کشتارجمعی را بسیار دست‌کم گرفته بودند. همچنین در یافتن و هدف‌گیری موشک‌اندازهای متحرک زمین به زمین عراقی که موجب سردرگمی نیروهای آنها شده بود، با مشکل مواجه شدند و توانایی صدام برای حفظ قدرت را دست‌کم گرفته بودند. فرماندهان نظامی در طول تاریخ همواره با عدم قطعیت‌های این‌چنینی و شرایطی بسیار مبهم‌تر از این مواجه بوده‌اند و باید آمادگی مقابله با این ابهامات را داشته باشند.

شناخت خود

به همان میزان که شناخت دشمن مهم است، شناخت دقیق توانایی‌ها، قابلیت‌ها، محدودیت و موقعیت دقیق مکانی نیروهای خودی حایز اهمیت است. دشمن همواره در تلاش برای پنهان کردن اقدامات خود است، اما نیروهای خودی چنین انگیزه‌ای ندارند. با این حال، شرایط ویژه‌ی جنگ ممکن است فرماندهان را در ارزیابی نیروهای خود دچار خطا نماید. فرماندهان عالی‌رتبه اغلب نمی‌توانند تصور دقیقی از رزمی داشته باشند که در فاصله‌ی چند صد مایلی[1] آنها رخ می‌دهد. درک غلط فرماندهان از نیروهای تحت فرمان و شرایط آنها در رده‌های پائین‌تر نیز رخ می‌دهد. یکی از مشکل‌سازترین ابهامات فرماندهان عملیات نظامی، ضعف اطلاعات آنها از محل دیگر واحدهای خودی در منطقه‌ی جنگی است. در شرایطی که تشخیص نیروهای خودی از دشمن مشکل می‌شود، بدون خطر کردن در مورد نیروهای خودی نمی‌توان از آتش پشتیبانی بهره‌گرفت. برای نمونه؛ نیروهای زمینی و هوایی ایالات متحده رویه‌های عملیاتی خاصی برای کنترل آتش در حوالی نیروهای خودی دارند؛ این موارد، تعیین حدود مشخص برای آتش خودی و ثبت علائم مشخصه روی ماشین‌آلات و ادوات نظامی خودی را شامل می‌شوند. علی‌رغم درنظر گرفتن این تمهیدات و موارد دیگری از این دست، هنوز روشی برای حصول اطمینان قطعی از عدم وقوع تلفات خودی وجود ندارد.

1 – Mile

شناخت زمین، شناخت هوا

آشنایی با زمین و جغرافیای منطقه‌ی عملیات، همواره از اولویت‌های برتری نیروهای نظامی بوده است. تهیه‌ی نقشه‌ای مناسب از محل وقوع جنگ همواره از چالش‌های اصلی فرماندهان نظامی و کارکنان آنها بوده‌اند. در اواسط دهه‌ی ٦٠ میلادی هنگامی که نخستین نیروهای نظامی ایالات متحده وارد ویتنام شدند، نقشه‌های راه شرکت‌های نفتی تا مدت‌ها بهترین نقشه‌هایی بودند که واحدهای نظامی در اختیار داشتند. با وجود این‌که نقشه‌های خوبی تهیه شده بودند، گاه فرماندهان نظامی در ویتنام خود را در شرایطی پیش‌بینی نشده و منطقه‌ای ناآشنا می‌یافتند.

کنترل نیروها

کنترل – توانایی هدایت فعالیت‌های نیروها در میدان جنگ–، یکی دیگر از ابعاد فضای رزم است که اطلاعات در آن نقشی کلیدی ایفا می‌کند. غالبا گفته می‌شود که هیچ نقشه جنگی نمی‌تواند از نخستین مواجهه خود با دشمن جان سالم به در ببرد. بنابراین فرماندهان باید قادر باشند در هر لحظه از نبرد با توجه به شرایط تاکتیکی، نیروهای خود را متمرکز کنند، از فرصت‌ها استفاده کنند و از نقاط آسیب‌پذیر خود پشتیبانی و حفاظت کنند.

با توجه به اهمیت چشمگیر اعمال کنترل روی نیروهای تحت فرمان، در گذشته محدودیت‌های کنترلی متغیر اصلی تعیین کننده سازمان نیروهای نظامی و تاکتیک‌های مورد استفاده آنان بود. پیش از توسعه‌ی ابزارهای ارتباطی راه دور، حیطه‌ی کنترل یک فرمانده جنگی به افراد اطرافش که توانایی شنیدن صدای او را داشتند، محدود می‌شد. ارتباطات مدرن امکان گسترش این حیطه را فراهم نموده‌اند. البته در میدان نبردی که همه چیز به سرعت در حال وقوع و تغییر است، تجهیزات ارتباطی مدرن نیز نمی‌توانند متضمن کنترل دقیق حرکات نیروها توسط فرمانده باشند. با وجود توسعه‌ی ارتباطات رادیویی، پیام‌های دیجیتال، نقشه‌های الکترونیک و علائم قراردادی در میان افراد، باید همواره درنظر داشت که فرمانده تاکتیکی یک عملیات تنها یک نفر است و ظرفیت‌های شناختی محدودی دارد.

سرعت و قاطعیت

در اختیار داشتن سیستم‌های کنترلی و اطلاعات مناسب یک مقوله است و بهره‌گیری عملی از آنها مقوله دیگری است. به طور کلی، هرچه فرد به میدان نبرد نزدیک‌تر باشد، زمان برای او حساس‌تر می‌شود. ثانیه‌ها برای نیروهای زمینی درگیر در جنگ آتش یا نیروی هوایی درگیر در یک عملیات هوایی، اهمیت دارد. در یک نبرد یا لشکرکشی، فرماندهان عملیاتی در سطوح میانی تنها چند ساعت برای اتخاذ تصمیمات مهم اعم از نحوه تخصیص نیروها، فرصت دارند. در چنین شرایط حساسی، ارزش اطلاعات کسب شده از دشمن می‌تواند به سرعت دستخوش تغییرات عظیم شود. موفقیت در نبرد تا حد زیادی به سرعت عکس‌العمل در مقابل دشمن وابسته است. این سرعت عمل شامل چهار فعالیت متوالی می‌باشد: مشاهده، درک وضعیت و جهت‌گیری، تصمیم‌گیری، عمل کردن. در جنگ‌ها عموماً طرفی که بتواند این اعمال را بهتر و سریع‌تر به انجام برساند، صرف‌نظر از وضعیت عملیاتی و تاکتیکی خود، برنده میدان خواهد بود.

رزم اطلاعاتی: ظهور فناوری اطلاعات در حوزه دفاعی

بحث در مورد پیشرفت‌های سریع اخیر در مدیریت اطلاعات حوزه دفاعی، اغلب به مباحث پیچیده‌ای وارد می‌شود، عباراتی مانند «فضای نبرد مجازی» و «جنگ سایبر» در ادبیات ناپدید می‌شوند و جای خود را به واژه‌هایی مانند «فضای رزم شبکه محور» می‌دهند. این امر موجب بروز شک و تردید در متخصصین نظامی می‌شود؛ که البته با جدید بودن این مباحث و نبود تجربه در این زمینه، قابل توجیه است و گاهی درک عملکرد سیستم‌های جدید و تأثیر آنها در نحوه‌ی اجرای عملیات نظامی مشکل است. روشن است پیشرفت‌های فناوری اطلاعات نظامی در بسیاری از حوزه‌ها واقعی و کاربردی است و منافع شناخته‌شده‌ای دارد. در حال حاضر، برنامه‌ریزان نظامی با این چالش مواجهند که چگونه فناوری‌های جدید اطلاعاتی و قابلیت‌های آن را در عملیات نظامی پیاده‌سازی نمایند.

امروزه فناوری اطلاعات به مهم‌ترین عامل ایجاد کننده قدرت نظامی تبدیل شده است (Rattray, 2001). تا چندی پیش نظامیان تنها برای تقویت قابلیت‌های موجود خود از فناوری اطلاعات بهره می‌گرفتند؛ اما همان‌گونه که فناوری اطلاعات موجب تغییر همه رویه‌ها در کسب‌وکارهای تجاری گردید، تغییر روش‌های کاری دفاعی را نیز به دنبال داشته است. در نتیجه، انقلاب اطلاعاتی و تأثیر آن بر عملیات و نیروهای نظامی، معیارهای ارزیابی قدرت نظامی متحول گردیده است. اندازه ارتش‌ها و میزان سلاح‌های سنگین مورد استفاده آنها، تعداد هواپیماها و کشتی‌های نظامی دیگر اهمیت سابق را ندارند. عملکرد (شامل دقت، قابلیت اطمینان و میزان مرگبار بودن) سلاح‌های شخصی به‌کمک علم میکروالکترونیک بهبود یافته است، اما زمانی ارزشمند است که به‌صورت هماهنگ با سایر سلاح‌ها عمل کند. توسعه‌ی ارتباطات ما را قادر ساخته است تا حسگرها، سلاح‌ها و سیستم‌های فرماندهی را در قالب سپاهی یکپارچه درآورده و برآیند کل را به چیزی بیشتر از مجموع عملکرد تک‌تک این اجزاء ارتقا دهیم.

استفاده یکپارچه و هماهنگ از سلاح‌ها، حسگرها، و سایر سیستم‌های نظامی به توانمندی نیروهای نظامی در انجام فعالیت‌های کنترل، ارتباطات، محاسبات، فرماندهی، دیده‌بانی و شناسایی، وابسته است. نظامیان با بهره‌گیری از این ابزارها می‌توانند کلیه حرکات دشمن را شناسایی و ردیابی کنند و نیروهای خود را برای نشان دادن عکس‌العمل مناسب هماهنگ کنند تا از این طریق تعیین‌کننده نتیجه جنگ باشند (Ventre, 2011).

رابطه معکوس فاصله و دقت به واسطه‌ی فناوری اطلاعات در حال از بین رفتن است. سلاح‌های مرگبار با کمک فناوری‌های شناسایی و تعقیب واحدهای دشمن، به تخریب سریع و سیستماتیک نیروهای دشمن و زیرساخت‌های نظامی آنها منجر می‌شوند. نیاز به پرواز هواپیماهای دارای سرنشین در محدوده‌ی استقرار دشمن کاهش یافته و سلاح‌های دارای کنترل از راه دور برای شناسایی و تخریب اهداف مورد نظر استفاده می‌شوند.

فناوری اطلاعات امکان جنگ یکپارچه و مشترک را فراهم می‌نماید که می‌تواند مزیت جنگی عظیمی به‌شمار رود. به‌جای حمل سلاح‌های مختلف از طریق زمین، هوا و دریا به صورت جداگانه، نیروهای دخیل در نبرد مشترک می‌توانند به‌صورت یکپارچه اقدام به اجرای عملیات هماهنگ نمایند.

این امکان بالقوه وجود دارد که هریک از قابلیت‌های نیروهای مشترک، بنابر اولویت، با اجزای مختلف ارتش دشمن مقابله نمایند. با تجمیع قابلیت‌های مختلف نظامیان شرکت کننده در نبرد مشترک، شانس دشمن برای دفاع از نیروها و مواضعش به حداقل می‌رسد (Ventre, 2011).

تدارکات دفاعی به واسطه‌ی فناوری اطلاعات بخش خصوصی و روش‌های کاری آن، ناب و سریع‌تر شده‌اند. رهبران ارتش ایالات متحده و منتقدان آن، هنوز در پیچ‌وخم مشکلات بازسازی ساختار و کوچک سازی تأسیسات و انبارهای نظامی عظیمی هستند که در گذشته ایجاد شده است؛ اما تا نیمه راه را طی کرده‌اند. بیشتر ارتش‌های دیگر جهان هنوز فاصله زیادی با این وضعیت دارند و تأسیسات قدیمی آنها بجای پشتیبانی واقعی از عملیات نظامی، موجب اتلاف منابع می‌شوند. فناوری اطلاعات این امکان را فراهم می‌نماید که بهره‌وری تأسیسات دفاعی افزوده شده و تدارکات، مدیریت منابع و آموزش بهبود یابد. در مجموع، فناوری اطلاعات، سیستم‌های نظامی را به‌طور کلی متحول نموده است (Ventre, 2011).

فناوری اطلاعات که به صورت فیزیکی شامل مجموعه‌ای از سخت‌افزارها، نرم‌افزارها و سیستم‌ها و ابزارهاست، تنها دلیل برتری نظامی ابرقدرتها نیست و نباید نقش مزیت‌های ذاتی جامعه را در آن نادیده گرفت. امروزه وجود نیروهای بسیار شایسته اطلاعات محور، به بخشی جدایی‌ناپذیر و کلیدی در موفقیت‌های نظامی کشورها تبدیل شده است و یافتن چنین افرادی در اقتصادهای آزاد و جوامع باز، امکان‌پذیر است. جوامعی که از چنین ویژگی‌هایی برخوردار نباشند تنها می‌توانند سلاح‌ها و سیستم‌های جدید را خریداری نمایند، اما محکوم به استفاده از نیروهای درجه دو و تأسیسات عصر صنعتی هستند که قطعاً توان نظامی آنها را محدود می‌کنند. نظام‌های جامعه‌محور در تأمین همزمان دو جزء «انسان» و «ماشین» برای سیستم‌های اطلاعاتی نظامی خود توفیق بیشتری دارند.

در آینده، سلاح‌های کشتار از راه دور –زمین، دریا و هوا– موفقیت ارتش‌های مجهز به فناوری اطلاعات را تضمین خواهد کرد. اما نقش نبردهای کوچک و پیاده‌نظام‌های پراکنده و پنهان شدن و غافلگیر کردن دشمن را نباید نادیده گرفت؛ که هیچ‌یک نیازی به فناوری اطلاعات ندارند. آیا راهبردهای این‌چنینی با این ایده که ملت‌ها باید در فناوری اطلاعات قوی شوند، در تضاد است؟ پاسخ منفی است. با در نظر داشتن این واقعیت که تحولات مذکور در سیستم‌های نظامی هنوز مراحل اولیه خود را می‌گذرانند، به موازات

توسعه‌ی کاربردهای فناوری اطلاعات، مجموعه‌ای رو به گسترش از راهبردهای مقابله با حملات نظامی بی‌اثر خواهند شد. تأسیسات نظامی، پادگان‌های نظامی و پایگاه‌های استقرار نظامیان از آسان‌ترین اهداف قابل شناسایی و تخریب هستند و از میان بردن آنها با کمک نیروهای مسلط به فناوری اطلاعاتی و ابزارهای دقیق و سریع مورد استفاده آنها، بیش از پیش تسهیل می‌شود (Rattray, 2001).

با وجود همه این موارد، احتمال آن وجود دارد که نیروهای نظامی در عملیات خود از فناوری‌های رایج بهره‌گیری نکنند و همچنان خطرساز و تهدیدکننده باشند. با این حال هر ارتشی که بخواهد در سطح منطقه‌ای یا جهانی قدرت بگیرد یا قصد مقابله با نیروهای قدرت‌های برتر را داشته باشد، باید خود را به فناوری اطلاعات و قابلیت‌های ناشی از آن مجهز کند. برای این کار لازم است فضایی مردمی و اقتصادی آزاد وجود داشته باشد تا فرصت برای رشد فناوری جدید و دانش مرتبط با آن فراهم گردد (Gompert, 1999).

بررسی ادبیات رزم اطلاعاتی، نمایانگر روندهایی (جدول شماره‌ی ۱) است که رزم اطلاعاتی را از حیطه‌ی نظامی خارج نموده و وارد مسائل مدنی نموده است. در ادامه هر یک از این روندها تشریح شده است.

جدول شماره‌ی ۱ – روندهای رزم اطلاعاتی (Janczewski and Colarik, 2008)

ویژگی‌های رزم اطلاعاتی	۱۹۹۰	۲۰۰۵
۱– حوادث مرتبط با کامپیوتر	۲۵۲ حادثه	۱۳۷۵۲۹ حادثه (سال ۲۰۰۳)
۲– موانع ورود در مقابل حمله‌های سایبر	موانع زیاد	موانع کم
۳– انواع سلاح‌های سایبر	انواع محدود، دسترسی کم	متنوع، دسترسی زیاد
٤– کشورهای بهره‌مند از برنامه‌های رزم سایبر	معدود	بیش از ۳۰
۵– وابستگی اقتصادی به زیرساخت‌های اطلاعاتی	بخشی، وابستگی رو به افزایش	وابستگی بسیار زیاد
٦– هدف اصلی در تعارضات اطلاعاتی	نظامی و خصوصی	افزایش اهداف خصوصی
۷– کاربرد فناوری سایبری در مدیریت ادراکات افراد	تلویزیون، رادیو	رسانه‌های متنوع و جهانی
۸– کاربرد فناوری سایبری در جاسوسی تجاری	کم (قابل چشم‌پوشی)	به میزان قابل توجه و رو به افزایش
۹– کاربرد فناوری سایبری در جنایات سازمان‌یافته	کم (قابل چشم‌پوشی)	به میزان قابل توجه و رو به افزایش
۱۰– کاربرد فناوری سایبری در مقابل افراد حقیقی و کسب‌وکارهای کوچک	کم (قابل چشم‌پوشی)	به میزان قابل توجه و رو به افزایش

حوادث مرتبط با کامپیوتر توسعه یافته‌اند: امروزه حوادث امنیتی بسیار رایج هستند، سازمان‌ها و مؤسسات خصوصی هدف بسیاری از حمله‌های سایبری هستند، جامعه و عموم مردم از بسیاری از تهاجمات این‌چنینی بی‌اطلاع می‌مانند. تعداد حوادث گزارش شده از ۷ حادثه در سال ۱۹۸۸ به ۱۳۷۵۲۹ در سال ۲۰۰۳ رسیده است. با وجود این‌که تعداد حوادث گزارش شده زیاد است، این احتمال وجود دارد که بسیاری از حوادث گزارش نشده باشند. پاسخ‌دهندگان به نظرسنجی‌ها بر این باورند که حوادث این بخش بیش از تعداد گزارش شده توسط شرکت‌ها به مشتریان و سهامداران و شرکای تجاری آنهاست. برای مثال، در سال ۲۰۰۵ فقط ۲۰٪ پاسخ‌دهندگان اظهار داشته‌اند که به دلیل نگرانی از ایجاد شهرت و تبلیغات منفی اقدام به گزارش حوادث به مراجع قانونی نموده‌اند (Gordon et al., 2005).

موانع ورود در مقابل حمله‌های سایبری کم هستند: برای استفاده اثربخش از نسل‌های اول سلاح‌های سایبری نیاز به دانش فنی وجود داشت. برای مثال، برخی هکرهای دهه‌ی ٦٠ میلادی از دانشجویان دانشگاه ماساچوست[1] بودند. در دهه‌ی ۷۰ میلادی هکرها افرادی بسیار با انگیزه و باهوش بودند که از دانش فنی بالایی برخوردار بودند و اغلب در مراکز کامپیوتری دانشگاه‌ها مشغول به کار بودند (Jones et al., 2002). در اوایل دهه‌ی ۹۰ میلادی شرایط عوض شد؛ موانع فنی به مرور حذف شدند و تعاملات کاربری از طریق صفحات گرافیکی صورت گرفت. در اواخر دهه‌ی ۹۰ یک اتفاق بزرگ رخ داد. گروهی از نوجوانان هکر تحت سرپرستی جوانی ۱۸ ساله، به تعدادی از کامپیوترهای دولتی و نظامی نفوذ کردند. این اتفاق، هشداری بود که همگان را متوجه خطر موجود از جانب افراد متخصص و نسبتاً غیرمتخصص نمود. در سال ۱۹۹۹ میلادی، مدیر آژانس اطلاعات مرکزی آمریکا[2] در کنگره اذعان داشت تروریست‌ها و سایر افراد دریافته‌اند رزم اطلاعاتی می‌تواند روشی کم‌هزینه برای دستیابی به منافع آنها باشد. تنها تا سال ۲۰۰۲ میلادی متخصصین امنیتی بیش از ٦ هزار سایت هکر را شناسایی کرده بودند که ابزارهای هک و نفوذ را در اختیار داشتند (Jones et al., 2002).

1 – Massachusetts
2 – Central Intelligence Agency (CIA)

ظهور انواع خطرناکی از سلاح‌های سایبری: نخستین جامعه‌ی اینترنتی هکرها در حدود سال ۱۹۸۰ میلادی تشکیل شد و به طرح و انتشار تکنیک‌ها و نرم‌افزارهای آنها کمک کرد. حمله‌ی اینترنتی ۷ فوریه سال ۲۰۰۰ میلادی به‌وسیله‌ی همین نرم‌افزار انجام شد و منجر به از کار افتادن تعداد زیادی از سایت‌های اینترنتی شد. سازمان تحقیقات دفاعی انگلستان اعلام نمود که تروریسم سایبری در این کشور میلیون‌ها پوند خسارت به کامپیوترها وارد ساخته است (Rhem, 2005).

دسترسی بسیاری از کشورها به فناوری رزم اطلاعاتی: در اوایل دهه‌ی ۹۰ میلادی تنها تعداد محدودی از کشورها از قابلیت رزم اطلاعاتی بهره‌مند بودند. در سال ۲۰۰۱ میلادی تعداد آنها به بیش از ۳۰ کشور رسید که از جمله آنها می‌توان به هند، چین، تایوان، ایران، رژیم اشغالگر قدس، فرانسه، روسیه و برزیل اشاره نمود. نتایج بررسی‌های میدانی حاکی از این است که ۲۸٪ پاسخ‌دهندگان، این احتمال را می‌دهند که از سوی دولت‌های دیگر حمله‌های سایبری به سیستم‌های آنها انجام شود. چین یکی از کشورهایی است که قابلیت‌های خود را در حیطه‌ی رزم اطلاعاتی گسترش داده است (Gordon et al., 2005).

افزایش وابستگی اقتصادی به زیرساخت‌های اطلاعاتی: جامعه امروز مراحل کشاورزی و صنعتی را پشت سر گذاشته است و در حال حاضر فرهنگ مبتنی بر اطلاعات بر آن حاکم است. اشاره‌هایی که به اقتصاد دیجیتال[1] یا موج سوم شده است، نشان‌دهنده افزایش وابستگی به فناوری اطلاعات است. با افزایش نگرانی‌ها نسبت به تهدیدهای احتمالی، دولت ایالات متحده در گزارش هیات تحقیقات ملی[2] در سال ۱۹۹۱ میلادی با عنوان «کامپیوترها در معرض خطر وابستگی شدید اقتصاد ملی» به کامپیوترها اشاره کرده است. این گزارش به نگرانی‌های موجود در زمینه‌ی وابستگی به کامپیوترها در حوزه‌ی انرژی، ارتباطات، حمل و نقل هوایی و خدمات مالی اشاره نموده است. کامپیوترها برای ذخیره اطلاعات حیاتی اعم از سوابق پزشکی و برنامه‌های کسب‌وکار و سوابق جنایی مورد استفاده قرار گرفته‌اند (Gordon et al., 2005). این

1 – Digital Economy
2 – National Research Council

وابستگی تا جایی ادامه یافته است که ایالات متحده راهبرد ملی امنیت فضای سایبری در سال ۲۰۰۳ میلادی آورده است: «تا سال ۲۰۰۳ میلادی اقتصاد و امنیت ملی ما کاملاً به زیرساخت‌های اطلاعاتی وابسته خواهد بود. شبکه‌ای از شبکه‌ها، پشتیبانی مستقیم عملیات همه‌ی بخش‌های اقتصاد، انرژی، حمل‌ونقل، مالی و بانکی، اطلاعاتی و ارتباطی، بهداشت و سلامت عمومی، خدمات اضطراری، آب، پزشکی، تأسیسات دفاعی، تغذیه، کشاورزی و حمل و نقل و پست را برعهده خواهد گرفت».

بخش خصوصی هدف اصلی جنگ‌های اطلاعاتی: حمله‌های سایبری، نخست اهداف نظامی را مدنظر داشتند. با افزایش وابستگی اقتصادی به فناوری اطلاعات، زیرساخت‌های شهری بیش از پیش به اهداف مورد نظر حملات سایبری تبدیل شده‌اند. عناوین خبری به حملاتی اشاره نموده‌اند که سایت‌ها و محصولات تجاری را مورد حمله وسیع قرار داده‌اند. در همین خصوص به‌عنوان نمونه: این حمله‌ها، کنگره ایالات متحده را بر آن داشت قوانین جدیدی برای تضمین ایمنی فضای سایبری در نظر بگیرند تا از این طریق ۱۰۳ راکتور اتمی موجود در ایالات متحده را مورد حمایت و محافظت قرار دهند (Gordon et al., 2005).

گسترش به‌کارگیری فناوری سایبری برای مدیریت ادراکات افراد: مدیریت ادراکات[1] فرآیندی است شامل مجموعه اقداماتی که برای تأثیرگذاری روی دیدگاه‌های عمومی و فرهنگ، انجام می‌شوند و در حوزه‌های سیاسی، مدنی، فرهنگی، سازمانی و نظامی کاربرد دارند. در روش‌های مدرن مدیریت ادراکات، فناوری‌های نوین و سریع نقشی کلیدی در متأثر نمودن افکار و ایده‌های افراد دارند. توسعه‌ی فناوری‌های اینترنتی و شبکه‌های جهانی، مدیریت ادراکات را به جنبه‌ای کلیدی در بسیاری از مبارزات و تعارض‌ها تبدیل کرده است. در جنگ‌های اعتقادی، ادراکات عموم مردم هدف قرار داده می‌شود (Rhem, 2005).

افزایش کاربرد فناوری سایبری در جاسوسی: در مارس سال ۲۰۰۱ ویلیام کوهن[2]، وزیر دفاع سابق ایالات متحده، اعلام نمود که رئیس سابق سرویس اطلاعاتی فرانسه تأیید کرده که این سازمان

1 – Perception management
2 – William Cohen

اقدام به گردآوری اطلاعات کلیدی شرکت‌های ایالات متحده و سایر شرکت‌هایی می‌کند که رقیب سازمان‌های فرانسوی هستند و این اطلاعات را به فرانسه ارسال می‌کند. او به چند نمونه جاسوسی فرانسوی‌ها علیه سازمان‌های ایالات متحده اشاره نمود. یکی از این موارد به سرقت اطلاعات فنی از کامپیوترهای ایالات متحده مربوط می‌شود که توسط سرویس اطلاعاتی فرانسه به یکی از شرکت‌های فرانسوی ارسال گردید. متوسط زیان ناشی از حمله یک هکر به یک کامپیوتر ۱۵۰ هزار دلار است که این هزینه در جاسوسی بسیار بیشتر است. جاسوسی ممکن است از طریق ایمیل‌های رد و بدل شده میان کارکنان یک سازمان با سازمان‌های رقیب انجام شود. نتایج یکی از مطالعات میدانی انجام شده در میان ٤٩٨ نفر از کارکنان سازمان‌های مختلف آشکار ساخت که ٤٠٪ آنها دریافت اطلاعات محرمانه در مورد سازمان‌های دیگر از طریق اینترنت را تایید کرده‌اند و این رقم از سال ۱۹۹۹ میلادی در حدود ۳٥٦٪ رشد داشته است. دستگاه قضایی ایالات متحده در سال ۲۰۰٤ میلادی اعلام کرد فعالیت‌های غیرقانونی اینترنتی زیادی را اعم از کلاهبرداری با کارت اعتباری و جاسوسی شناسایی کرده است. در این کشور، مأموران تحقیق و تفحص بیش از ۱۵۰ هزار قربانی حملات سایبری را شناسایی کردند که خسارات وارد بر آنها از مرز ۲۱۵ میلیون دلار می‌گذشت. لازم به ذکر است که با گسترش شبکه‌های داخلی سازمان‌ها و قرار دادن اطلاعات بیشتر در اختیار کارکنان و تأمین‌کنندگان، احتمال وقوع جاسوسی افزایش می‌یابد (Rhem, 2005).

افزایش کاربرد فناوری در جرایم سازمان‌یافته: انفجار اینترنتی منجر به ظهور و بروز جرایم نوینی در فضای سایبری گردید. در همین خصوص دستگاه قضایی ایالات متحده مدعی است کلاهبرداری‌های اینترنتی و سایر جرم‌های آنلاین، جزء جرایمی هستند که در حال افزایش با بالاترین نرخ هستند. یکی از روش‌های مورد استفاده این مجرمین، استفاده از سایت‌های تقلبی با ظاهری مشابه سایت اصلی است. متخصصین در زمینه ویروس‌کش‌ها فعالیت‌های بسیاری را در حوزه‌ی تولید ویروس و کرم نرم‌افزاری گزارش کرده‌اند و رشد سریع این نوع جرم را شناسایی کرده‌اند. فعالیت‌های زیرزمینی و غیر قانونی این‌چنینی در راستای تقویت اقتصاد موسوم به زیرزمینی می‌شود که تمرکز آن بر روی کلاهبرداری است (Rhem, 2005).

گسترش استفاده از فناوری سایبری بر علیه اشخاص و کسب‌وکارهای کوچک: امروزه نرم‌افزارهای موسوم به جاسوس‌افزارها[1] افراد و کسب‌وکارهای کوچک را تهدید می‌کنند. آنها برنامه‌های کاربردی معمولی هستند که مورد استفاده یا موافقت کاربران قرار می‌گیرند و عمل پایش مداوم را انجام می‌دهند. تاکنون وجود ۷۰۰۰ جاسوس افزار شناسایی شده است که بنابر گزارش شرکت مایکروسافت[2]، مسوول خرابی نیمی از کامپیوترها هستند. نتایج یک مطالعه نشان داده است ۹۱٪ کامپیوترهای خانگی تحت تأثیر جاسوس افزارها قرار دارند.

یکی دیگر از مشکلات رو به افزایش، سرقت هویت است که نوع جدیدی از تروریسم سایبری بر علیه اشخاص تلقی می‌شود که اغلب برای انجام اعمال غیرقانونی و مجرمانه با نام فردی دیگر، انجام می‌شود. چنین اقدامی هم افراد و هم کسب‌وکارها را با مشکل مواجه می‌کند. در گزارش کمیسیون تجارت فدرال[3] آمده است طی سال ۲۰۰۳ حدود ۹/۹ میلیون نفر در ایالات متحده قربانی این جرم شدند. اغلب این موارد توسط سارقان سایبری انجام شده که هویت افراد را برای بازکردن حسابی جدید سرقت می‌کردند و خسارت هریک از این موارد به طور متوسط ۱۲۰۰ دلار برآورد شده است. حساب‌های تقلبی تاکنون ۳۲/۹ میلیارد دلار خسارت به کسب‌وکارها و ۳/۸ میلیارد دلار خسارت به مصرف‌کنندگان تحمیل کرده‌اند (Rhem, 2005).

روش‌شناسی تحقیق

این پژوهش که از نوع پژوهش‌های کیفی می‌باشد، به‌دنبال پاسخ به سؤالات ذیل به انجام رسیده است که عبارتند از:

- رزم اطلاعات چیست و چه ابعادی دارد؟
- از طرفی مباحث متنوع ذکر شده در ادبیات در حوزه‌ی رزم اطلاعاتی را چگونه می‌توان در کنار هم قرار دادو مدل تحلیل آن چیست؟

1 – Spyware
2 – Microsoft Corporation
3 – Federal Trade Commission

در واقع، این پژوهش به دنبال تبیین مفاهیم، رفع ابهامات و مدیریت دیدگاه‌های گوناگون در حوزه‌ی رزم اطلاعات است. در نهایت این پژوهش سعی دارد تا به جای بررسی عوامل تأثیرگذار بر (و یا مؤثر از) رزم اطلاعات، به تبیین و تشریح ماهیت درونی و چیستی رزم اطلاعات بپردازد.

سؤالی که از منظر روش شناسی مطرح می‌شود آن است که چه نوع خروجی نظری می‌تواند قالب مناسبی برای پاسخ ارائه شده این پژوهش به سؤالات آن باشد. به عبارتی باید تعیین نمود که کدام یک از انواع خروجی‌های نظری و یا ترکیبی از آنها مانند مدل‌ها، روش‌ها، سازه‌ها، چارچوب‌ها می‌تواند بهترین گزینه برای خروجی پژوهش حاضر باشد. برای پاسخ به این سوال بایستی به گونه‌شناسی[1] نظریه‌ها پرداخت. یکی از بهترین تحقیقات در این زمینه، توسط شرلی گرگور[2] به انجام رسیده است. گرگور پنج نوع نظریه در حوزه فناوری اطلاعات را شناسایی نموده است که به شرح جدول شماره‌ی (۲) می‌باشد.

جدول شماره‌ی ۲ – انواع نظریه‌های حوزه فناوری اطلاعات (Gregor, 2006)

نوع نظریه	ویژگی‌های نظریه
نظریه برای تحلیل	به سؤال «چه چیزی» پاسخ می‌گوید. هیچ روابط علی بین پدیده‌ها و متغیرها در این نوع نظریه مطرح نمی‌شود و هیچ‌گونه پیش‌بینی صورت نمی‌گیرد.
نظریه برای تبیین	به سؤال «چه چیزی، چگونه، چرا، چه زمانی و کجا» پاسخ می‌گوید. این نوع نظریه به تبیین پدیده‌ها می‌پردازد اما به دنبال پیش‌بینی نیست. هیچ فرضیه آزمون‌پذیری ارائه نمی‌گردد.
نظریه برای پیش‌بینی	به سؤال «چه چیزی است و چه خواهد بود» پاسخ می‌گوید. این نوع نظریه به ارائه پیش‌بینی پرداخته و شامل فرضیات آزمون‌پذیر می‌باشد.
نظریه برای تبیین و پیش‌بینی	به سؤال «چه چیزی، چگونه، چرا، چه زمانی، کجا و چه خواهد بود» پاسخ می‌گوید. این نوع نظریه به ارائه پیش‌بینی می‌پردازد و هم شامل فرضیات آزمون‌پذیر و هم روابط علی می‌باشد.
نظریه برای طراحی و اجرا	به سؤال «چگونه کاری را انجام دهیم» پاسخ می‌گوید. این نظریه تجویزات صریحی (مانند روش‌ها و تکنیک‌ها) را برای ساخت مصنوعات ارائه می‌نماید.

1 – Ontology
2 – Shirley Gregor

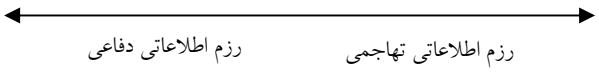
هر یک از انواع نظریه‌های فوق‌الذکر در قالب‌های گوناگونی ارائه می‌شوند که گرگور به قالب‌های معمول اشاره نموده است. وی معتقد است «نظریه برای تحلیل» غالباً به‌صورت طبقه‌بندی‌ها و چارچوب‌ها ارائه می‌شوند. به عقیده گرگور، این نوع نظریه بیشتر در مواقعی کاربرد دارد که شناخت و درک نسبتاً کمی درباره پدیده‌ی تحت بررسی وجود داشته و چیستی پدیده‌ی مورد نظر به‌خوبی تبیین نشده است (Gregor, 2009). از آنجا که پژوهش حاضر نیز به دنبال مفهوم‌سازی رزم اطلاعاتی و تبیین چیستی آن است، از این رو این پژوهش بایستی به ارائه چارچوبی برای این منظور بپردازد.

به‌طور کلی چارچوب عبارتند از یک ساختار مفهومی بنیادین که برای بررسی و حل مسائل پیچیده مورد استفاده استقرار می‌گیرد. چارچوب‌ها یک ساختار زیربنایی برای پشتیبانی از چیزی و یا دربر گرفتن برخی مفاهیم مرتبط به هم فراهم می‌نمایند. چارچوب‌های مربوط به حوزه‌ی فناوری اطلاعات و کاربردهای آن در بخش‌های گوناگون، به درک حوزه‌ها و ابعاد مختلف آنها کمک می‌نماید و از این رو، از دیدگاه مفهومی، چارچوب‌ها به پیچیدگی حوزه‌های مرتبط با فناوری اطلاعات نظم بخشیده و منجر به مدیریت بهتر پیچیدگی‌های درونی این حوزه‌ها می‌شوند. چارچوب‌های یک حوزه، تعیین کننده دستگاه مفهمومی است که هنگام فعالیت در یک حوزه به کار می‌بریم و یا بر آن دستگاه مفهومی تأثیرگذار است (Basden, 2008). این چارچوب‌ها تعیین می‌کنند که چگونه پدیده‌ها را طبقه بندی می‌کنیم، چه نظریه‌هایی را اتخاذ می‌نماییم و چه نوع متدلوژی‌ها و قوانینی را برای هدایت تحقیق و یا پژوهش فرموله می‌کنیم، چه موارد و موضوعات با اهمیتی را در آن حوزه تشخیص می‌دهیم، چه سؤالاتی از خودمان خواهیم پرسید، چه مواردی را به عنوان مشکلات و چه راه‌حل‌هایی برای حل این مشکلات بر می‌گزینیم. درستی یا نادرستی یک چارچوب به‌وسیله‌ی مفاهیم نظری قابل اثبات نیست. چرا که یک چارچوب به عنوان یک پیش‌نظریه از مجموعه‌ای از باورها و مفروضات درباره حوزه‌ای که به‌وسیله کسانی که در آن حوزه کار می‌کنند شکل گرفته است (Basden, 2008).

چارچوب رزم اطلاعاتی

چارچوبی که برای رزم اطلاعاتی در این مقاله ارائه گردیده است بر سه محور بنا نهاده شده است. اولین محور بر «جهت رزم اطلاعاتی» اشاره دارد، این محور شامل دو بعد است (شکل شماره‌ی ۱ را ببینید):

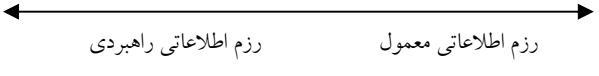
- رزم اطلاعاتی دفاعی: رزم اطلاعاتی دفاعی زمانی رخ می‌دهد که رزم اطلاعاتی با هدف دفاع از سیستم‌ها و سرمایه‌های اطلاعاتی صورت می‌پذیرد. این امر ممکن است از طریق عملیات فیزیکی و یا عملیات نرم افزاری و سایبری و سایر شیوه‌های دفاعی صورت پذیرد.
- رزم اطلاعاتی تهاجمی: در رزم اطلاعاتی تهاجمی، سیستم‌ها و سرمایه‌های اطلاعاتی دشمن از طریق عملیات فیزیکی و یا عملیات نرم‌افزاری و سایبری و سایر شیوه‌های رزم، مورد تهاجم و تخریب قرار می‌گیرد.



شکل شماره‌ی ۱ – ابعاد محور «جهت رزم اطلاعاتی»

دومین محور چارچوب، بر «عمق رزم اطلاعاتی» تأکید دارد. این محور دارای دو بعد می‌باشد (شکل شماره‌ی ۲ را ببینید):

- رزم‌های اطلاعاتی راهبردی: در برخی از رزم‌های اطلاعاتی، با بهره‌گیری از ابزارها و روش‌های حاصل از انقلاب اطلاعاتی، دارایی‌های راهبردی کلیدی کشورها اعم از زیرساخت‌های بخش‌های انرژی، ارتباطات، حمل‌ونقل، مالی تهدید می‌گردد.
- رزم‌های اطلاعاتی معمول: در این‌گونه رزم‌های اطلاعاتی، هدف‌های رزم اطلاعاتی جنبه راهبردی ندارد.

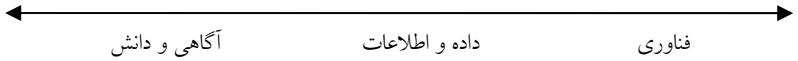


شکل شماره‌ی ۲ – ابعاد محور «عمق رزم اطلاعاتی»

سومین محور بر «عناصر رزم اطلاعاتی» تأکید دارد. همان‌طور که در پیش‌تر ذکر شد، ظهور و به‌کارگیری فناوری‌های اطلاعاتی در حوزه‌ی دفاعی عاملی بنیادی در راستای شکل‌گیری مفهوم رزم اطلاعاتی بوده است. به‌عبارتی، یکی از ریشه‌های رزم اطلاعاتی را بایستی در فناوری اطلاعات جستجو کرد. بررسی ادبیات نشان می‌دهد که مباحث حوزه‌ی رزم اطلاعاتی با تأکید بر عناصر و اجزای مختلف فناوری‌های اطلاعاتی، به تبیین مفهوم رزم اطلاعاتی و تشریح آن پرداخته‌اند.

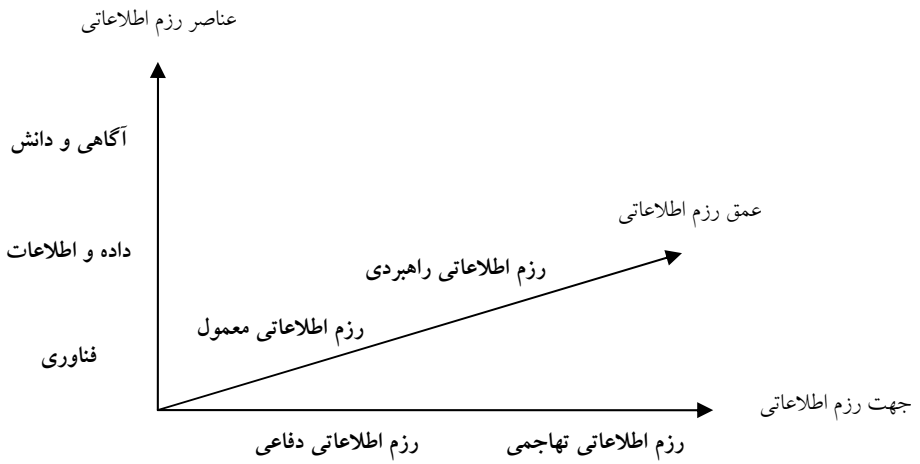
ادبیات مربوطه را می‌توان در دو بخش عمده تقسیم بندی نمود (شکل شماره‌ی ۳ را ببینید):

- تأکید بر اطلاعات: دسته اول بر اطلاعات تأکید دارند. منظور از تأکید بر اطلاعات در رزم اطلاعاتی آن است که رزم چه در حالت دفاع و چه در حالت تهاجم با تکیه بر قابلیت‌های اطلاعاتی به انجام می‌رسد. در رویکرد رزم اطلاعاتی دفاعی، از قابلیت‌های اطلاعاتی برای دفاع در برابر شیوه‌های گوناگون حمله، بهره گرفته می‌شود. در رویکرد رزم اطلاعاتی تهاجمی، از قابلیت‌های اطلاعاتی برای حمله همه‌جانبه به دشمن استفاده می‌شود. تأکید بر اطلاعات نیز به نوبه‌ی خود در دو شاخه قابل بررسی است. برخی از ادبیات بر سطوح انتزاع بالای اطلاعات که شامل آگاهی و دانش می‌باشد تأکید داشته و برخی نیز بر سطوح انتزاع پائین‌تر اطلاعات که شامل داده و اطلاعات (در معنای عام) است، تمرکز داشته‌اند.
- تأکید بر فناوری: دسته دوم بر فناوری تأکید دارند که در رزم‌های اطلاعاتی مبتنی بر فناوری، در رویکرد دفاعی، از قابلیت‌های فناوری (که پشتیبانی کننده عملیات مربوط به جمع‌آوری، پردازش، ذخیره و انتشار اطلاعات است) برای مقابله با شیوه‌های گوناگون حمله، بهره گرفته می‌شود و در رزم‌های اطلاعاتی مبتنی بر فناوری، در رویکرد تهاجمی نیز از قابلیت‌های فناوری برای حمله همه‌جانبه به دشمن استفاده می‌شود.



شکل شماره‌ی ۳ - ابعاد محور «عناصر رزم اطلاعاتی»

محورهای تشکیل‌دهنده‌ی چارچوب رزم اطلاعاتی در شکل شماره‌ی ٤ نشان داده شده است.



شکل شماره‌ی ٤ – محورهای تشکیل‌دهنده‌ی چارچوب رزم اطلاعاتی

به‌منظور تشریح محورهای چارچوب رزم اطلاعاتی، محورهای نشان داده شده در شکل شماره‌ی ٤، در قالب ماتریس دوبعدی (جدول شماره‌ی ۳) ارائه گردیده است. این ماتریس نشان‌دهنده‌ی چارچوب رزم اطلاعاتی می‌باشد.

جدول شماره‌ی۳ – چارچوب رزم اطلاعاتی

			جهت رزم اطلاعاتی	
		عمق رزم اطلاعاتی	رزم اطلاعاتی دفاعی	رزم اطلاعاتی تهاجمی
عناصر رزم اطلاعات	آگاهی و دانش	رزم اطلاعاتی معمول	۱. رزم اطلاعاتی دفاعی مبتنی بر آگاهی و دانش	۲. رزم اطلاعاتی تهاجمی مبتنی بر آگاهی و دانش
		رزم اطلاعاتی راهبردی	۳. رزم اطلاعاتی راهبردی دفاعی مبتنی بر آگاهی و دانش	٤. رزم اطلاعاتی راهبردی تهاجمی مبتنی بر آگاهی و دانش
	داده و اطلاعات	رزم اطلاعاتی معمول	٥. رزم اطلاعاتی دفاعی مبتنی بر داده و اطلاعات	٦. رزم اطلاعاتی تهاجمی مبتنی بر داده و اطلاعات
		رزم اطلاعاتی راهبردی	۷. رزم اطلاعاتی راهبردی دفاعی مبتنی بر داده و اطلاعات	۸ رزم اطلاعاتی راهبردی تهاجمی مبتنی بر داده و اطلاعات

ادامه‌ی جدول شماره‌ی ۳			
فناوری	رزم اطلاعاتی معمول	۹. رزم اطلاعاتی دفاعی مبتنی بر فناوری	۱۰. رزم اطلاعاتی تهاجمی مبتنی بر فناوری
	رزم اطلاعاتی راهبردی	۱۱. رزم اطلاعاتی راهبردی دفاعی مبتنی بر فناوری	۱۲. رزم اطلاعاتی راهبردی تهاجمی مبتنی بر فناوری

چارچوب فوق آنچه را که در ادبیات رزم اطلاعاتی مطرح شده است، در خود جای می‌دهد. مباحثی نظیر رزم مبتنی بر شبکه، رزم مبتنی بر دانش، رزم اطلاعاتی راهبردی و رزم سایبری اصطلاحاتی هستند که تحت عنوان رزم اطلاعاتی در ادبیات ذکر شده‌اند و هر یک بر بعدی خاص از رزم اطلاعاتی اشاره دارند. چارچوب ارائه شده با مورد توجه قرار دادن ابعاد زیر بنایی رزم اطلاعاتی، مبنایی را برای تبیین جایگاه هر یک از اصطلاحات و برداشت‌ها از رزم اطلاعاتی و تبیین تمایزات بین آنها فراهم نموده است.

در بخش بعد برخی از این اصطلاحات و ادبیات مربوطه بر سلول‌های مختلف چارچوب پیشنهادی نگاشت می‌شود. بررسی‌ها نشان می‌دهد که در ادبیات موجود رزم اطلاعاتی، ادبیات حوزه‌ی رزم اطلاعاتی مبتنی بر آگاهی و دانش و نیز رزم اطلاعاتی مبتنی بر فناوری بیشتر جنبه تهاجمی و ادبیات حوزه‌ی رزم اطلاعاتی مبتنی بر داده و اطلاعات بیشتر جنبه دفاعی دارد. پیشنهاد می‌شود در پژوهش‌های آتی به تبیین محتوای سایر سلول‌های چارچوب بر اساس ادبیات پرداخته شود. چه بسا این امر منجر به شکل‌گیری مفاهیم و روش‌های نوینی در رزم اطلاعاتی گردد.

کاربرد نظری چارچوب پیشنهادی در فضای رزم

در این بخش سه مفهوم پر کاربرد در حوزه رزم اطلاعاتی به سلول‌های مربوطه در چارچوب رزم اطلاعاتی اختصاص یافته و تشریح گردیده است. این مفاهیم عبارتند از: رزم دانش‌محور[1]، رزم اطلاعاتی راهبردی[2]، رزم مبتنی بر شبکه[3]. رزم دانش‌محور یکی از گونه‌های

1 – Knowledge-based Warfare (KBW)
2 – Strategic Information Warfare (SIW)
3 – Net-Centric Warfare

رزم اطلاعاتی مبتنی بر آگـاهی و دانـش اسـت کـه در ایـن بخـش از رویکـرد رزم اطلاعـاتی تهاجمی مورد بررسی قرار می‌گیرد. رزم اطلاعاتی راهبردی در طبقه‌ی راهبـردی از رزم مبتنـی بر آگاهی و دانش قرار دارد که در این بخش از رویکرد تهاجمی بررسی می‌شود. رزم مبتنی بر شبکه نیز در گروه رزم اطلاعاتی مبتنی بر فناوری قرار می‌گیرد که از دیـدگاه تهـاجمی و غیـر راهبردی مورد بررسی قرار می‌گیرد.

رزم دانش محور: رزم اطلاعاتی تهاجمی مبتنی بر آگاهی و دانش (سلول ۲)

با پیشرفت فناوری اطلاعات، مباحثی در زمینه نحـوه‌ی بـه‌کـارگیری قابلیـت‌هـای آن در تغییرات سازمانی و فرآیندی و ایجاد زیرساخت دگرگونی جنگ‌ها، موسـوم بـه انقـلاب امـور نظامی[1]، طرح گردید. به‌واقع، در صورت تلفیق فنـاوری اطلاعـات و فرآینـدهـا بـا عملیـات و مفاهیم جدید سازمانی، فرصت‌هایی برای تغییرات غیرمسـتمر و حرکـت از عصـر صـنعتی بـه عصر اطلاعاتی فراهم می‌شود. مشکل امنیت را می‌توان در کوتاه‌مـدت بـه کمـک فرآینـدهـا و فناوری عصر اطلاعات و در نهایت از طریق شکل‌دهی نیروهایی حل نمود. اما دستیابی به ایـن هدف، مستلزم برخورداری از چشم‌انداز راهبردی مشترک دولت و صنایع، به‌ویـژه بخـش‌هـای خدماتی است. لازم است بخش‌های خدماتی، فلسـفه و دیـدگاه‌هـای مشـترکی را در حـوزه‌ی مبارزه و نبرد توسعه دهند که مبنای تغییرات سازمانی و فرآیندی مورد نیاز برای توانمند و کارا نمودن نیروها قرار گیرند. همچنین لازم است این مفهوم، زیربنای سـرمایه‌گـذاری خـدمات در تحقیق، توسعه و اکتساب تلقی شود. بدین ترتیب زیربنایی منسجم و همسان برای برنامه‌ریـزی هزینه‌های دفاعی و اقدامات توسعه و خرید ایجاد می‌شود. چنین چشم‌اندازی، رزم دانش‌محور نامیده می‌شود (Casper and Halter, 1996).

رزم دانش‌محور انقلابی منطقی است از راهبردهای تهدیدمحور عصر صنعت به راهبـردهـای مبتنی بر قابلیت‌ها در عصر اطلاعات. رزم دانش‌محور، فرآیندی است که برتری آگاهی نیـروهـا در میدان جنگ را تضمین می‌کند و امکان اتخاذ سریع‌تر تصمیمات، در مقایسـه بـا دشـمن، را فـراهم

1 – Revolution in military affairs (RMA)

می‌کند. این نوع رزم، موجب کسب برتری اطلاعـاتی در جنـگ و توفیـق در رسـیدن بـه اهـداف، به‌واسطه‌ی استفاده دقیق و درست از قدرت و توان نظامی می‌شود. تفاوت رزم دانش‌محور با انـواع دیگر رزم، هم‌افزایی ابزارهای مختلف اعم از حسگرهای پیشـرفته، فنـاوری اطلاعـات و ابزارهـای تحلیلی پردازشگر اطلاعات است؛ که اطلاعات متنوعی را در مورد میدان نبرد در اختیار فرمانـدهان قرار می‌دهد و آنها خواهند توانست به کمک این اطلاعات، از تجربه‌ی نظـامی و قـدرت قضـاوت خود حداکثر استفاده را بکنند. توانایی گردآوری اطلاعات، تحلیل و پردازش و بهره‌گیـری از آن در فضای نبرد، همان برتری اطلاعاتی است. فرمانـدهان و تصـمیم‌گیرنـدگان همـواره در جسـتجوی اطلاعاتی بوده‌اند که بتوانند سرعت و قدرت عمل خود را بیشتر نموده و پیوسـته بـرای مقابلـه بـا دشمنان خود آماده باشند. امروزه، این کار امکان‌پذیر شده است. برخـورداری از مزیـت اطلاعـاتی می‌تواند به چرخه تصمیم‌گیری دشمن، ضربه سنگینی وارد کنـد. فرمانـدهان مـی‌تواننـد از طریـق کانال‌های ارتباطی به اهداف مورد نظر خود دست یابند و از نبردهای سـنگین و خسـارت‌هـای آن حتی‌الامکان اجتناب کنند. این راهبرد، موجب تقویـت برتـری اطلاعـاتی و کسـب مزیـت پایـدار راهبردی می‌شود (Lambe, 2003).

رزم دانش‌محور، به گردآوری و تحلیل اطلاعات وابسـته اسـت. یـک سیسـتم یکپارچـه فرماندهی، کنترل، محاسبه، اطلاعات عملیات، دیده‌بانی و شناسایی، به انجام یک برنامـه‌ریـزی پویا و پشتیبانی از تصمیم‌گیری‌هـا و برنامـه‌هـا کمـک مـی‌کنـد. چنـد نکتـه‌ی جدیـد در رزم دانش‌محور وجود دارد. در رزم دانش‌محـور، اولویـت بـا توسـعه‌ی سیسـتم‌هـای یکپارچـه‌ی فرماندهی و کنترل است و پس از آن به سیستم‌های مسلح طراحی شده برای کار در چارچوب فرماندهی و کنترل پرداخته می‌شود. این امر منجر به تغییر روند تولیـد سـلاح‌هـای پیشـرفته و اتکای آن به نیازهای فرماندهی و کنترل می‌شـود. در رزم دانـش‌محـور بـه‌جـای تـلاش بـرای فرسایش نیروهای دشمن در نبردی خطی، به تخریب فیزیکی اهداف مورد نظـر بـا رویکـردی غیرخطی، در داخل و خارج میدان نبرد توجه می‌شود. بنابراین، فرآیندی ترسـیم مـی‌شـود کـه تعیین‌کننده و پیش‌بینی‌کننده تأثیر اقدامات و سیستم‌های دشمن و میـزان تـأثیرات مرگبـار آنهـا است (Connery, 2003).

شبکه‌ها، اطلاعاتی را منتشر می‌کنند که می‌توانند با کمک به تصمیم‌گیری‌های افراد، آنها را در سطوح راهبردی، عملیاتی و تاکتیکی توانمند نمایند. سربازان، در صورتی که از برتری آگاهی و دانش کافی در مورد اهداف مورد نظر برخوردار باشند، می‌توانند خروجی‌های راهبردی مورد نظر را محقق نمایند. اطلاعات کاربردی در فرآیند تصمیم‌گیری منجر به افزایش سرعت ایجاد فرصت، اتخاذ تصمیمات در مورد خط مشی مبارزه، تسریع برنامه‌ریزی و پیاده‌سازی آن، و تطبیق سریع با فرآیندهای امنیتی می‌شود. تطبیق به‌موقع، نتیجه منطقی فرآیند پایش همزمان، ارائه بازخورد و تحلیل معیارهاست که نتیجه‌ی آن تسریع کل فرآیندهای امنیتی از نقطه پایش پیش از بحران تا اجرای تصمیمات اتخاذ شده برای رفع بحران را شامل می‌شود (Lambe, 2003).

در رزم دانش‌محور بر کنترل سرعت مبارزه تأکید می‌شود که نتیجه‌ی آن ایجاد برتری اطلاعاتی فرماندهان در مورد زمان، مکان و تحرکات مورد نظر آنها است. در این صورت زمان به یکی از معیارهای اثربخشی فرآیندهای امنیتی تبدیل می‌شود که جنگ‌های موازی، نقطه غایی چنین رویکردی است. ترکیب دانش میدان جنگ با توانایی حمله‌ی دقیق و هم‌راستا با اهداف کلیدی، با سرعت و کشندگی زیاد، قابلیت‌های چشمگیری را برای به زانو درآوردن سریع یک ارتش یا جامعه‌ی پیشرفته و صنعتی در اختیار قرار می‌دهد. به واقع رزم دانش‌محور، دیدگاه‌های ذهنی جدیدی در مورد برنامه‌ریزی و اشتراک اطلاعات دارد.

این رویکرد، از برنامه‌ریزی پویا، تعاملی و هماهنگ استقبال می‌کند و بر هدف‌گیری سیستماتیک و نتیجه‌محور اهداف و نتایج راهبردی مورد انتظار، تأکید دارد. توزیع موازی اطلاعات میان رده‌های مختلف اعم از سربازان تا تصمیم‌گیران و بهره‌گیری از عامل‌های هوشمند برای مرتب نمودن اطلاعات قابل‌استفاده در تصمیم‌گیری، از ویژگی‌های دیگر آن است. تأکید اصلی آن روی تحلیل داده، ایجاد اطلاعات قابل استفاده در تصمیم‌گیری و در نهایت دانش است. رزم دانش‌محور فرصت‌هایی را فراهم می‌کند که اثرات چشمگیری بر راهبرد امنیت ملی دارند؛ نه تنها قابلیت‌های آن را بهبود می‌بخشند، بلکه موجب افزایش گزینه‌های تصمیم‌گیرانی می‌شود که از دانش تولید شده در یک حوزه مشترک بهره می‌گیرند و

با اقدامات سیاسی، دیپلماتیک و نظامی خود می‌کوشند مانع از بروز جنگ و درگیری شوند. آنها می‌توانند با تسهیل دوران گذار به سوی نیروهای کارآمدتر و توانمندتر، از بروز تعارضات عظیم و وسیع پیشگیری کرده و ابزاری را در اختیار تدوین‌کنندگان خط‌مشی قرار دهند تا بتوانند در آینده محیط امنی را فراهم نمایند (Evans, 2012).

رزم اطلاعاتی راهبردی: رزم اطلاعاتی راهبردی تهاجمی مبتنی بر داده و اطلاعات (سلول ۸)

این احتمال وجود دارد که در آینده نیروهای نظامی با بهره‌گیری از ابزارها و روش‌های حاصل از انقلاب اطلاعاتی، دارایی‌های راهبردی کلیدی ملت‌ها اعم از زیرساخت‌های بخش‌های انرژی، ارتباطات، حمل‌ونقل، مالی و... دشمنان خود را تهدید نمایند. این خطر بالقوه، از ویژگی‌های ماهوی محیط رزم اطلاعاتی راهبردی به شمار می‌رود. دشمنان و رقبای اقتصادی ممکن است از ابزارها و تکنیک‌های رزم اطلاعاتی راهبردی برای به چالش کشیدن کشورها، منافع و متحدان آنها، بهره‌گیری نمایند. در آینده‌ی نزدیک سلاح‌های رزم اطلاعاتی راهبردی می‌توانند مورد استفاده دشمنان باشند که در صورت ضعف در مقابله فیزیکی، به استفاده از راهبردهای نامتقارن[1] روی می‌آورند. این راهبرد ترکیب ابزارهای رزم اطلاعاتی راهبردی با سلاح‌های هسته‌ای، شیمیایی، بیولوژیک و جنگ‌افزارهای معمولی را می‌طلبند (Molander et al., 1996).

در رزم اطلاعاتی راهبردی، میدان نبرد همان زیرساخت اطلاعاتی جوامع مدرن است که وابستگی جامعه به آن در سیستم‌های تأمین انرژی، مالی، کنترل ترافیک و سایر سیستم‌های کامپیوتری نمود پیدا می‌کند. رزم اطلاعاتی راهبردی برخاسته از اینترنت است و در آن از اینترنت استفاده زیادی می‌شود. ارتباط تعداد زیادی از کامپیوترها با یکدیگر، آنها را مستعد آسیب‌پذیری در مقابل وقفه‌ها و ضعف‌های سیستماتیک می‌کند. این امکان وجود دارد از خارج از کشور حمله‌هایی به کامپیوترها شود که ردیابی آنها امکان‌پذیر نباشد. در اکثر موارد این کار به قدری زیرکانه و ماهرانه صورت می‌گیرد که تا پایان حمله، کسی متوجه آن نمی‌شود

1 - Asymmetric Strategies

و بعد از اتمام آن دیگر دیر شده و فرصتی برای مقابله وجود ندارد. ایالات متحده اصولاً آسیب‌پذیری خاصی در مقابل چنین حمله‌هایی دارد، چرا که از پیشرفته‌ترین سیستم‌های کامپیوتر برخوردار است و وابستگی نسبی بیشتری به آنها دارد (Molander et al., 1996).

با وجود این‌که زیرساخت‌های اطلاعاتی مورد نیاز برای رزم راهبردی اطلاعاتی به اینترنت محدود نمی‌شوند، شبکه‌ها به‌قدری با اینترنت عجین شده‌اند که این دو، یک موجودیت به نظر می‌رسند. در نتیجه، خطرات و نقاط ضعف اینترنت، جدی‌ترین تهدیدها برای زیرساخت‌های اطلاعاتی به شمار می‌روند. گزارش‌های منتشر شده در مورد حمله‌های کامپیوتری، جرائم الکترونیک و تروریسم اطلاعاتی، باعث شده این تصور در عموم مردم حاکم شود که اتصال به شبکه و دسترسی از راه دور، فقدان سیستم کنترل‌کننده مرکزی و ارتباطات متقابل و چند جانبه موجب شده اینترنت و به طور کلی کامپیوترها فاقد امنیت باشند. بسیاری از این گزارش‌ها غلط و احساسی هستند، اما ضعف دانش فنی عمومی نسبت به کامپیوترها و شبکه مرتباً به شایعات و نگرانی‌ها دامن می‌زند (Molander et al., 1998).

در تاریخ رزم‌های راهبردی، یافتن نبردی که در آن از اطلاعات مهم و حساس به‌عنوان یکی از حربه‌های اصلی مبارزه استفاده نشده باشد، مشکل است. در همین راستا، سان تزو استفاده از اطلاعات را برای دستیابی به اهداف راهبردی، به موازات اجتناب از تعارض فیزیکی پیشنهاد می‌کند. بدون شک می‌توان فهرستی از وقایع تاریخی تهیه نمود که در آنها تغییرات بنیادین فناوری منجر به تغییر نقش و جایگاه اطلاعات در نبردهای راهبردی شده است.

هنوز تأثیر بالقوه انقلاب اطلاعات روی رزم‌های راهبردی به‌خوبی روشن نیست. رزم اطلاعاتی راهبردی در گذشته نقش زیرمجموعه را در رزم‌های راهبردی ایفا نموده است، در حالی که ممکن است در اوج انقلاب اطلاعاتی نقشی بسیار مهم‌تر را ایفا کند. تأثیر بالقوه انقلاب اطلاعات روی آسیب‌پذیری زیرساخت‌های ملی و سایر دارایی‌های راهبردی ممکن است در گذر زمان تغییر کرده و منجر به بروز نوع کاملاً جدیدی از رزم‌های راهبردی مبتنی بر اطلاعات شود. به‌طور کلی می‌توان دو نسل را برای رزم اطلاعاتی راهبردی متصور شد (Molander et al., 1998).

۱) رزم اطلاعاتی راهبردی نسل اول: رزم اطلاعاتی راهبردی به‌عنوان یکی از اشکال یا اجزای رزم‌های راهبردی در آینده است، که مفهوم آن حرکت به جلو از طریق هماهنگی تعدادی از ابزارهای مختلف رزم راهبردی می‌باشد.

۲) رزم اطلاعاتی راهبردی نسل دوم: رزم اطلاعاتی راهبردی به‌عنوان نوعی مستقل و جدید از رزم راهبردی شناخته می‌شود که در نتیجه‌ی انقلاب اطلاعاتی ظهور کرد. در حیطه‌های نوظهوری از رزم راهبردی (مانند اقتصاد) و در طول زمان (مثلاً سال در مقابل روز، هفته و ماه) کاربرد دارد و زمان مورد نیاز برای آن عموماً طولانی‌تر از رزم‌های راهبردی است.

صاحب‌نظران بر این باورند که ابر قدرت‌ها و قدرت‌های نوظهور منطقه‌ای، به احتمال زیاد از رزم اطلاعاتی راهبردی نسل اول بهره خواهند گرفت. البته این دیدگاه قابل بحث و بررسی است. برای مثال ممکن است قدرت‌های برتر در آینده نزدیک با شرایطی مواجه شود که ترجیح دهد از مزیت‌های فناوری اطلاعات خود بهره‌برداری نموده و رزم اطلاعاتی راهبردی نسل دوم را به‌کار گیرد تا از بروز شرایطی که در نهایت منجر به نبرد فیزیکی وسیع و خسارات فراوان می‌شود، پیشگیری کند (Molander et al., 1998).

رزم اطلاعاتی مبتنی بر شبکه: رزم اطلاعاتی تهاجمی مبتنی بر فناوری (سلول ۱۲)

با ورود به هزاره سوم، مسائل نظامی پا به عرصه جدیدی گذاشته‌اند؛ دورانی که در آن رزم متأثر از محیط متغیر راهبردی و تغییرات سریع فناوری است. کشورهای مختلف در حال تجربه گذار از عصر صنعتی به عصر اطلاعاتی هستند. این تغییرات، به موازات تجربه‌های کسب شده در عملیات نظامی گذشته، موجب ظهور رویکرد جدیدی شده که جنگ مبتنی بر شبکه[1] و عملیات مبتنی بر شبکه‌ی هسته مرکزی آن را تشکیل می‌دهد. برای درک بهتر، اهمیت تجهیز نیروهای مسلح به ابزارهای جنگ مبتنی بر شبکه، بایستی به سؤالات اساسی مطرح در زمینه‌ی ظهور رزم مبتنی بر شبکه به‌عنوان یک نظریه‌ی نظامی در عصر اطلاعات پاسخ گفت.

1 – Network-Centric Warfare

همچنین تشریح می‌شود چگونه اصول در توسعه مفاهیم، سازمان‌ها و فرآیندهای جدید جنگی کاربرد پیدا می‌کند که تأمین‌کننده مزیت رقابتی نیروهای نظامی در مقابل دشمنان احتمالی فعلی و آتی است (Office of Force Transformation, 2003).

رزم مبتنی بر شبکه، نظریه نوظهوری است که در عصر اطلاعات شکل گرفت. واژه‌ی رزم مبتنی بر شبکه، ترکیبی از راهبرد، تاکتیک‌های نوظهور، سازمان، تکنیک‌ها و رویه‌هایی است که نیروهای مجهز به شبکه می‌توانند از آن به طور کلی یا بخشی در جهت تقویت مزیت دفاعی خود بهره‌گیری کنند. نخستین عاملی که باید در پیاده‌سازی رزم مبتنی بر شبکه مورد توجه قرار گیرد، رفتار انسان‌ها در مواجهه با فناوری اطلاعات است. لذا هنگام ارزیابی میزان بهره‌برداری یک واحد یا بخش یا سازمان نظامی از رزم مبتنی بر شبکه، بر رفتار انسان‌ها در محیط شبکه‌ای تمرکز می‌شود. نیروهای نظامی در چنین فضایی چگونه رفتار می‌کنند، چه عملکردی دارند و چطور سازماندهی می‌شوند؟ تجربه نشان داده تجهیز سربازان، ملوانان، خلبانان، تفنگداران دریایی و سایر نیروهای رده‌های تاکتیکی و عملیاتی به ابزارهای مبتنی بر شبکه، موجب افزایش میزان آگاهی آنها از وضعیت و شرایط موجود شده و در مقابل دشمن مزیتی چشمگیر به آنها می‌دهد. نظریه‌ی رزم مبتنی بر شبکه قابل تعمیم و کاربرد در هر سه رده راهبردی، عملیاتی و تاکتیکی نبردها می‌باشد (Edward and Smith, 2002).

دیدگاه رزم مبتنی بر شبکه نه تنها ماهیت سازمان‌ها را متحول ساخته، بلکه عملکرد نیروهای نظامی را نیز تغییر داده و خواهد داد. به موازات توسعه‌ی زیربنای اطلاعاتی رزم مبتنی بر شبکه در عصر اطلاعات، وزارت دفاع ایالات متحده در قالب برنامه تحقیقاتی کنترل و فرماندهی مجموعه کتبی را منتشر نموده است. در اولین کتاب این مجموعه با عنوان رزم مبتنی بر شبکه: توسعه و تقویت برتری اطلاعاتی، مطالبی در زمینه‌ی ارتباط قدرت نظامی با شبکه‌های پایدار، تشریح و مکتوب شده است. در این کتاب، تأثیر و کارکرد اطلاعات در فرماندهی و کنترل و نتیجه آن در تغییر ساختارهای نظامی، تشریح شده است. در این مجموعه سه جلدی، دو عنوان دیگر نیز وجود دارد: درک مفهوم رزم در عصر اطلاعات، و تحولات عصر اطلاعات. برنامه تحقیقاتی کنترل و فرماندهی همچنین اقدام به انتشار کتاب کاربرد رزم مبتنی بر شبکه در زمان صلح، جنگ و بحران

نموده است که در آن به ارتباط متقابل میان سازمان‌ها، فرآیندها و ماموریت‌های مبتنی بر شبکه پرداخته شده است (US Office of the force transformation, 2010).

برای اجرای عملیات نتیجه‌محور[1]، برخورداری از نیروهای مجهز به ابزارهای شبکه‌محور که قابلیت اجرای عملیات مبتنی بر شبکه را دارا باشند، ضروری است. عملیات نتیجه‌محور به مجموعه اقداماتی اطلاق می‌شود که برای شکل‌دهی و هدایت رفتار حامیان، بی‌طرفان و دشمنان، در شرایط صلح، جنگ یا بحران، انجام می‌شوند. عملیات نتیجه‌محور نوع جدیدی از مبارزه به شمار نمی‌رود و تصمیم‌گیرندگان همواره در طول تاریخ به دنبال ایجاد شرایط و وضعیتی بوده‌اند که دستیابی آنها به اهداف موردنظرشان را امکان‌پذیر نماید. فرماندهان و برنامه‌ریزان نظامی همواره کوشیده‌اند با طرح‌ریزی سلسه اقدامات و مبارزات، چنین شرایطی را به‌وجود آورند که این اقدام در ادبیات نظامی امروزی، عملیات نتیجه‌محور نامیده می‌شود. این مفهوم که در قرن ۲۱ توسط نیروهای مجهز به شبکه توسعه‌یافته، به متدلوژی برنامه‌ریزی، پیاده‌سازی و اجرا، و ارزیابی عملیات نظامی اشاره دارد که با هدف به‌جا گذاشتن تأثیری خاص انجام می‌شود که منجر به حصول نتایج مورد نظر در حوزه‌ی امنیت ملی می‌شود. نیروهای مسلح ابرقدرت‌ها به سرعت در حال توسعه‌ی رزم مبتنی بر شبکه و قابلیت‌های نظامی خود در این حیطه هستند تا بتوانند اقدام به پیاده‌سازی عملیات نتیجه‌محور نمایند. این کشورها انتظار دارند در نبردهای مشترک آتی بتواند با کمک قدرت حاصل از رزم مبتنی بر شبکه به مزیت رقابتی دست یابند (Cebrowski and Garstka, 1998).

رزم مبتنی بر شبکه به کمک شبکه‌ای از حسگرها، تصمیم‌گیرندگان و تفنگداران، میزان آگاهی، و سرعت انتقال فرامین و همزمانی را در درگیری‌های تن به تن افزایش داده و توانایی کشتار دشمن و شانس نجات نیروهای خودی را ارتقا می‌دهد این سیستم‌ها با برقراری ارتباط مؤثر میان نیروهای حاضر در میدان جنگ، آگاهی آنها را به شدت بهبود می‌بخشند و اتخاذ تصمیمات در همه‌ی رده‌های نظامی را تسهیل و تسریع می‌کنند، و در نهایت منجر به افزایش سرعت پیاده‌سازی عملیات و ایجاد مزیت در نبرد می‌شوند (Garstka, 2003).

1 – Effect-based Operation

نتیجه‌گیری

استفاده از چارچوب‌ها (که نظریه‌هایی برای تحلیل هستند) از الزامات نظری آن‌دسته از حوزه های علمی به شمار می رود که شناخت و درک نسبتاً کمی درباره پدیده‌های تحت بررسی آنها وجود داشته و چیستی پدیده‌های مورد نظر به خوبی تبیین نشده است. در واقع چارچوب‌ها به جای توجه بر روابط بیرونی یک پدیده با سایر پدیده‌ها و نحوه تأثیر و تأثر آنها، بر چیستی آن پدیده و تبیین روابط درونی آن تأکید دارند. رزم اطلاعاتی از جمله مفاهیمی است که در حوزه‌ی علوم دفاعی و امنیتی تعابیر گوناگونی درباره چیستی آن ارائه شده و وجه تمایز مشخصی بین تعابیر و کارکردهای گوناگون آن وجود ندارد. بنابراین این مفهوم نیازمند پشتیبانی با چارچوب‌های نظری است که به تبیین چیستی و روابط درونی آن بپردازد.

در واقع، پیچیدگی‌های حوزه رزم و حوزه فناوری اطلاعات موجب پیچیدگی مضاعف رزم اطلاعاتی و مفاهیم مرتبط با آن، که حاصل به‌کارگیری فناوری‌های اطلاعاتی در حوزه‌ی دفاعی می‌باشد، گردیده است. این امر موجب شده تا مفاهیم متعددی در حوزه‌ی رزم اطلاعاتی شکل گیرد که برخی از این مفاهیم با سایر موارد هم‌پوشانی داشته و مرزبندی مشخصی بین آنها وجود ندارد. از این رو، به‌منظور مفهوم‌سازی رزم اطلاعاتی و ساختاردهی به مفاهیم مربوطه، چارچوب رزم اطلاعاتی ارائه گردید. این چارچوب، از سه محور «جهت رزم اطلاعاتی»، «عمق رزم اطلاعاتی» و «عناصر رزم اطلاعاتی» تشکیل شده است. از تقاطع این سه محور، ۱۲ سلول شکل می‌گیرد که هر سلول بخشی از مفاهیم مرتبط با رزم اطلاعاتی را در خود جای می‌دهد. بر اساس این چارچوب، رزم دانش‌محور در سلول رزم اطلاعاتی تهاجمی مبتنی بر آگاهی و دانش (سلول ۲)، رزم اطلاعاتی راهبردی در سلول رزم اطلاعاتی راهبردی تهاجمی مبتنی بر داده و اطلاعات (سلول ۸) و رزم اطلاعاتی مبتنی بر شبکه در سلول رزم اطلاعاتی تهاجمی مبتنی بر فناوری (سلول ۱۲) قابل تقسیم بندی می‌باشد. به‌کارگیری این چارچوب موجب شکل‌گیری تفکر ساختاریافته درباره مفاهیم مرتبط با رزم اطلاعاتی شده و محققان را در راستای شناسایی و تحلیل شکاف‌های موجود در این حوزه پشتیبانی می‌نماید.

منابع

انگلیسی

1- Basden, A. (2008), "***Philosophical Frameworks for Understanding Information Systems, IGI Publishing***", Hershey, New York.

2- Casper, L., Halter, I. (1996), "***Knowledge-Based Warfare: A Security Strategy for the Next Century***", JFQ.

3- Cebrowski, A. K. and Garstka, J. (1998), "***Network-Centric Warfare: Its Origin and Future***", U.S. Naval Institute Proceedings. Annapolis, Maryland: January.

4- Connery, D. (2003), "***Trash or Treasure? Knowledge Warfare and The Shape Of Future War***", National Library Of Australia, Strategic and Defence Studies Centre.

5- Cronin, B., & Crawford, H. (1999), "***Information warfare: Its applications in military and civilian contexts. Information Society***", 15(4), 257264.

6- Edward A. Smith, Jr., (2002), "***Effects-Based Operations: Applying Network-Centric Warfare in Peace, Crisis, and War***", Washington, DC: DoD CCRP.

7- Evans, M. (2012), "***Knowledge Management and Warfare in the Information Age***", Land Warfare Studies Centre.

8- Garstka, J. (2003), "***Network-Centric Warfare Offers Warfighting Advantage***", Signal.

9- Gompert D. (1999), "***Right Makes Might: Freedom And Power In The Information Age***". Rand Research.

10- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005), "***Tenth Annual, 2005 CSI/FBI Computer Crime and Security Survey***", San Francisco: Computer Security Institute (www.gocsi.com).

11- Gregor, S. (2006), "***The nature of theory in information systems***", MIS Quarterly, Volume: 30, Issue: 3, Publisher: Citeseer, Pages: 611-642.

12- Gregor, S. (2009), "***Building Theory in the Sciences of the Artificial***", Academy of Management Review.

13- Halpin, E., Trevorrow, P., Webb, D. and Wright, S. (2006), "***Cyberwar, Netwar and the Revolution in Military Affairs***", Palgrave, Macmillan.

14- Janczewski, Le., Colarik, A. (2008), "***Cyber warfare and cyber terrorism***", Idea Group Inc (IGI).

15- Jones, A., Kovacich, G. L., & Luzwick, P. G. (2002), "***Global information warfare: How businesses, governments, and others achieve objectives and attain competitive advantages***". New York: Auerbach Publications.

16- Lambe, P. (2003), "***The Perils of Knowledge-Based Warfare' in Knowledge Management***", http://www.destinationkm.com/articles/default.asp?ArticleID=1043.

17- Molander, C., Riddile, S. and Wilson P. (1996), "***Strategic Information Warfare: A New Face of War***", Santa Monica, Calif.: RAND, MR-661-AF.

18- Molander, R., P. Wilson, D. Mussington, and R. Mesic (1998), "***Strategic Information Warfare Rising***", Santa Monica, Calif.: RAND, MR-964- OSD.

19- Office of Force Transformation, (2003), "***Network Centric Operations Conceptual Framework***", Version 2.0, See also Network Centric Operations Conceptual Framework, Version 1.0, November.

20- Rattray, G. (2001), "***Strategic Warfare in Cyberspace***", MIT Press.

21- Rhem, K. T. (2005), "***China investing in information warfare technology***", doctrine. American Forces Press Service.

22- Richard Szafranski, (1995), "***A Theory of Information Warfare***", Airpower Journal.

23- Silberglitt, R., Antón, P., Howell, D. (2006), "***The Global Technology Revolution 2020***", In Depth Analyses.

24- Tzu S. (1971), "***The Art of War***". Translated by Ralph D. Sawyer. Boulder, CO: Westview Press, 1994.

25- US Office of the force transformation, (2010), "***The Implementation of Network-Centric Warfare***", Office of the Secretary of Defense.

26- Ventre, D. (2009), "***Information Warfare***", Wiley – ISTE.

27- Ventre, D. (2011), "***Cyberwar and Information Warfare***", Wiley – ISTE.

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» (۲۰۰٦: 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

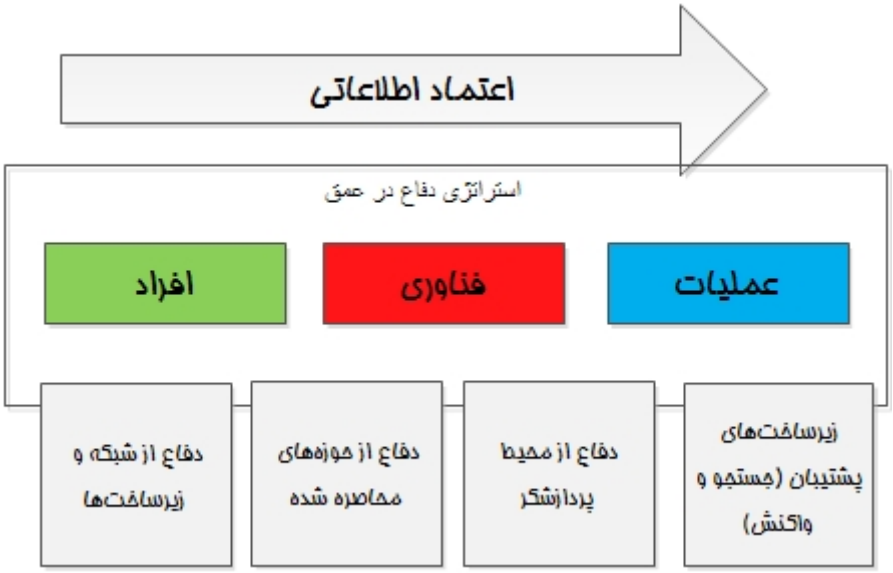
1 - Information Assurance
2 - Protection, Detection and Reaction

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.

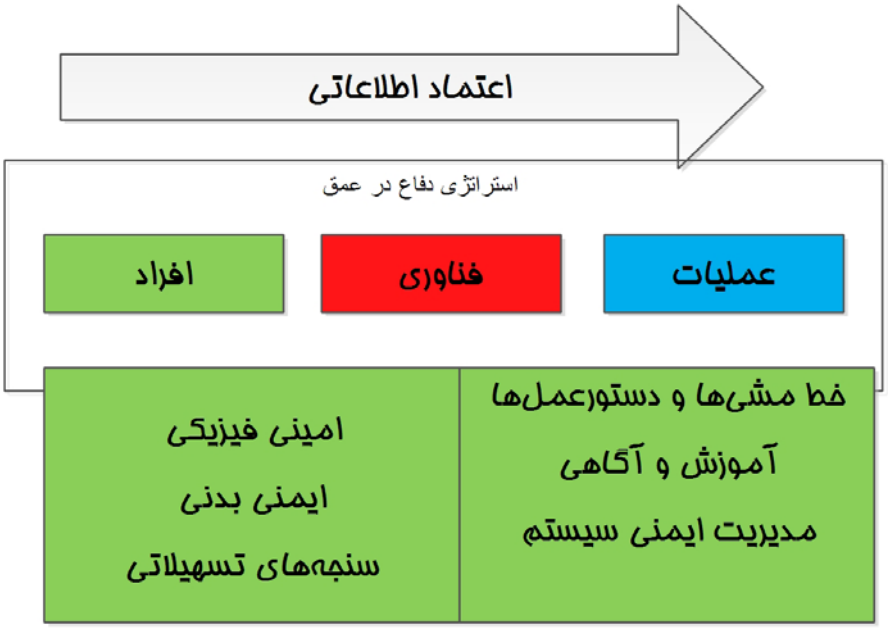


شکل شماره‌ی ۱ - اجزای راهبرد دفاع از عمق و حوزه‌های تمرکز آن

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)؛

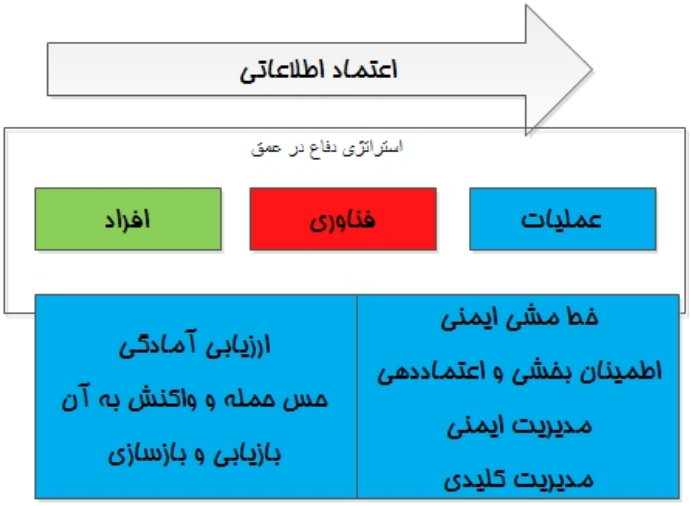
٤) فراهم کردن خدمات مدیریت کلیدی و حفاظت از این زیرساخت سودمند؛

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

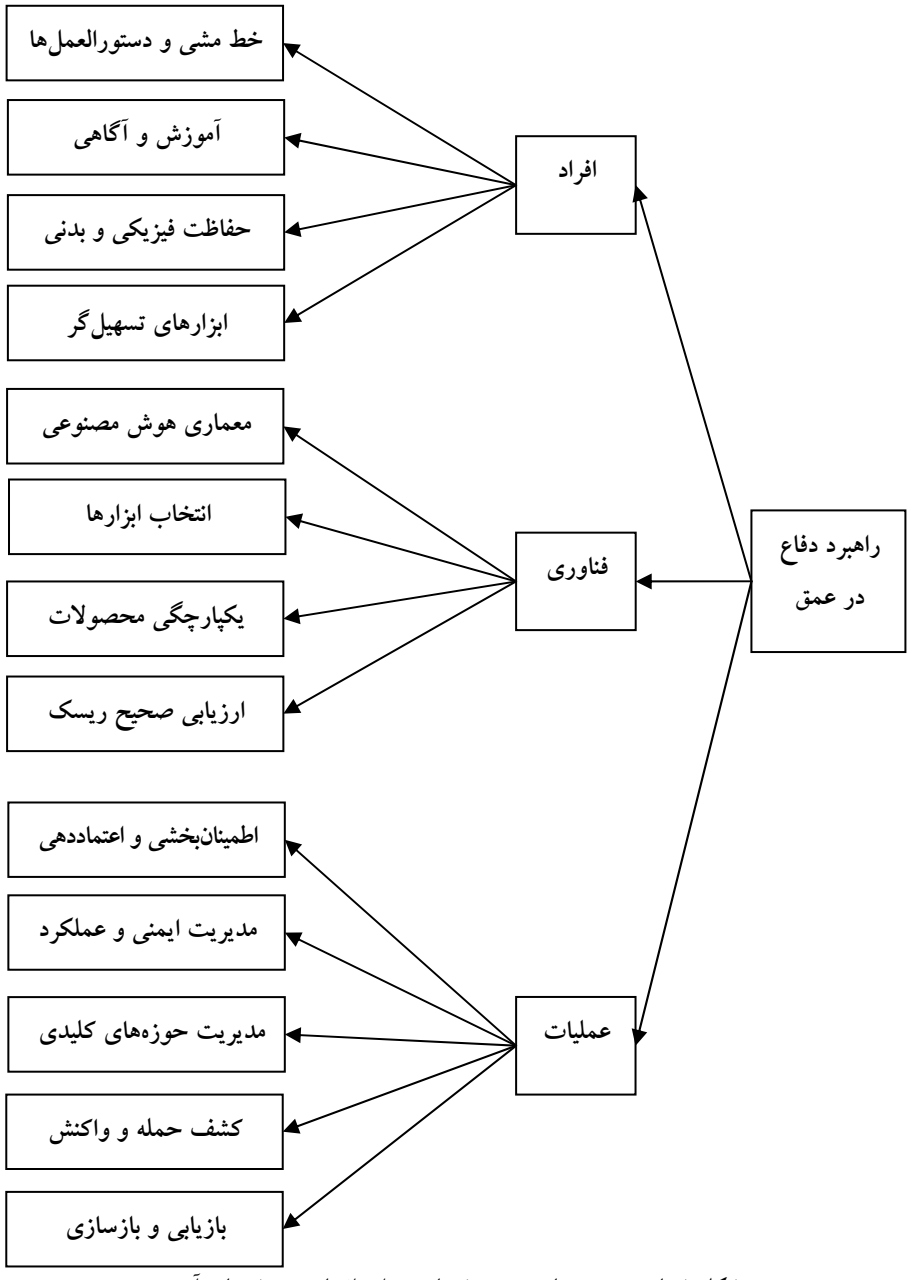
برای مثال، معمولاً اثربخش و به‌طور عملیاتی سودمند است که سازوکار قوی‌تری را در شبکه‌ها نسبت به رایانه‌های شخصی به‌کار گیریم.

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.

مجله سیاست دفاعی
سال بیستم، شماره ۷۹، تابستان ۱۳۹۱

ابعاد ژئوپلیتیک فضای مجازی در عصر فناوری اطلاعات

تاریخ دریافت مقاله: ۱۳۹۱/۰۲/۰۲
تاریخ تأیید مقاله: ۱۳۹۱/۰۳/۲٤
صفحات مقاله: ۱۸۲ – ۱٤۹

زهرا احمدی پور [۱]
رضا جنیدی [۲]
عبدالوهاب خوجم لی [۳]
اسماعیل پارسایی [٤]

چکیده:

ژئوپلیتیک در فرایند توسعه‌ی خود همگام با انقلاب اطلاعات به‌ویژه ظهور اینترنت با حوزه‌ی جدیدی مواجه شد که تحت عنوان ژئوپلیتیک فضای مجازی شناخته می‌شود. با خلق فضای مجازی ناشی از پدیده‌ی اینترنت به عنوان عرصه‌ی جدید فعالیت انسانی که در آن بازیگران، توانایی کنش و واکنش را نسبت به همدیگر می‌یابند، بخشی از مطالعات ژئوپلیتیک نیز به این عرصه وارد شده است. با عنایت به این تحول مهم، مقاله‌ی حاضر در صدد است، ابعاد ژئوپلیتیکی فضای مجازی و تحولات ژئوپلیتیکی ناشی از انقلاب اطلاعات را مورد بررسی و تحلیل قرار دهد.

استدلال مقاله‌ی حاضر بر این اصل استوار است که مهم‌ترین ابعاد ژئوپلیتیکی فضای مجازی و تحولات ژئوپلیتیکی ناشی از انقلاب اطلاعات عبارتند از: تحول در فضای مورد رقابت در ژئوپلیتیک، همگرایی و همکاری، تحول در ماهیت قدرت در ژئوپلیتیک، افزایش شکاف دیجیتالی، بُعد مدیریتی و کنترل فضای مجازی، تحول در روابط میان حکومت و شهروندان، هویت ملی و فروملی، تروریسم سایبری، جنگ نرم سایبری و جنگ مجازی.

* * * * *

واژگان کلیدی

ژئوپلیتیک فضای مجازی، قدرت، انقلاب اطلاعات، فناوری اطلاعات.

---

۱ – دانشیار جغرافیای سیاسی دانشگاه تربیت مدرس.
۲ – دانشجوی دکتری جغرافیای سیاسی دانشگاه تربیت مدرس.
۳ - کارشناس ارشد جغرافیای سیاسی دانشگاه تربیت مدرس.
٤ – دانشجوی دکتری جغرافیای سیاسی دانشگاه تربیت مدرس.

مقدمه

فناوری اطلاعات و فضای مجازی که محصول قابلیت‌های آن است، نماد پیشرفت علم و فناوری است که کشورهای قدرتمند به‌ویژه آمریکا در تولید و معماری آن نقش اصلی را به عهده داشته و دارند. فضای مجازی عرصه‌ی جدیدی برای حیات بشری است که قابلیت پذیرش و انجام بخش عمده‌ای از نیازها، فعالیت‌ها و شئونات زندگی بشر و اجتماعات انسانی و حکومت‌ها را دارد و به‌عنوان سایه‌ی فضای واقعی، و از طریق تمرکز، پردازش و جابه‌جایی اطلاعات، توانایی شبیه‌سازی فعالیت‌ها و ساختارهای فضای واقعی را داشته و این شبیه‌سازی را با اثربخشی در فضای واقعی انجام می‌دهد (حافظ‌نیا، ۱۳۹۰).

امروزه پدیده‌ی انقلاب اطلاعات و ارتباطات در حال ایجاد تغییرات اساسی و وسیعی در ماهیت و اشکال و ساختارهای قدرت در جوامع مختلف اعم از پیشرفته و در حال توسعه است (میناوند، ۱۳۸۵: ۱۲۱) و مفهوم قدرت و عناصر تشکیل‌دهنده‌ی ساختارهای آن، به‌عنوان ابزار و هدف اساسی در عملکردهای سیاسی جوامع و کشورها در عرصه‌ی نظام بین‌الملل، به نسبت بسیار زیادی در ارتباط با میزان توسعه و پیشرفت کشورها در زمینه‌ی فناوری ارتباطات و اطلاعات و فناوری‌های الکترونیکی مورد ارزیابی قرار می‌گیرد. از این رو، کشورهایی که عرصه‌ی بازی قدرت جهانی را در دست گرفته‌اند از پیشگامان توسعه‌ی این فناوری‌ها قلمداد می‌گردند؛ به‌ویژه این‌که اطلاعات خون حیات‌بخش نظام بین‌الملل است.

در واقع، شبکه‌ی اینترنت و فضای مجازی شاخص و انعکاس قدرت برتر کشورهایی است که آن را به‌وجود آورده و معماری کرده‌اند. زیرا بدون داشتن سطح بالایی از دانش، علم و فناوری و نیز توان اقتصادی امکان خلق آن وجود نداشت. کشوری که به این واقعیت یعنی اینترنت و فضای مجازی جامه‌ی عمل پوشانده است، آمریکا است که قدرت برتر جهان شناخته می‌شود. طراحی و ساخت شبکه‌ی مجازی مانند اینترنت نیاز به قابلیت‌هایی در زمینه‌ی فناوری اطلاعات، مخابرات، ارتباط اطلاعاتی، فناوری فضایی، سرمایه‌گذاری و غیره داشت که همه‌ی اینها در دست آمریکا موجود بود. آمریکا با سرمایه‌گذاری خود پس از جنگ جهانی دوم در پروژه‌ی معروف «آرپانت»، و طی چند دهه توانست اینترنت را در سال ۱۹۸۳ متولد

نماید. این شبکه بدون وجود زیرساخت‌های مخابراتی و ارتباطی نظیر ماهواره‌های فضایی، شبکه و کابل‌های نوری و غیره نمی‌توانست تحقق یابد. فناوری‌های فضایی و توانایی ساخت و در مدار قرار دادن ماهواره‌های مخابراتی محصول رقابت‌های دوره‌ی جنگ سرد است، که آمریکا در این زمینه قابلیت‌های چشم‌گیر و خوبی داشته و دارد (نامی و شامی، ۱۳۸۹: ۱۲۳).

بنابراین، همانند گذشته که تسلط بر دریاها و خشکی‌ها اهمیت فوق‌العاده‌ای داشت، امروزه، تسلط بر امواج، کنترل شبکه‌های اینترنتی، جاسوسی از کانال‌های اجاره‌ای، ماهواره‌ای و غیر آن می‌تواند علاوه بر تسلط سیاسی و اقتصادی به نوعی تسلط فرهنگی نیز منجر شود. به‌طوری که گفتمان‌های جهانی درباره‌ی مسائل و رویدادها و نیز ارزش‌های آمریکایی را شکل داده و بر طرز تلقی، باورها، نگرش‌ها و رفتارهای ملل دیگر تأثیر بگذارد و باعث قرار گرفتن آمریکا در موقعیت الگویی برای دیگران بشود. این امکان برای آمریکا، باعث واکنش قدرت‌های درجه‌ی دوم جهانی نظیر فرانسه، روسیه و چین شده است (حافظ‌نیا، ۱۳۹۰).

از منظر ژئوپلیتیک سنتی، مفهوم فضا شامل سرزمین‌هایی است که انسان توانسته در آنجا سکونت گزیند یا به گونه‌ای در آن دخل و تصرف کند. فضا صحنه‌ی نمایش پدیده‌های گوناگونی است که در آن ترکیب و تلفیق این پدیده‌ها به شکل‌های گوناگون، آثار متنوعی از خود بر جای می‌گذارد (عزتی، ۱۳۸۰: ۸٤). فضا یک تولید اجتماعی است و تولید فضا مانند تولید کالای تجاری است و نظام‌های مختلف سیاسی – اقتصادی، فضاهای مختلفی تولید می‌کنند. بسیاری از تحقیقاتی که اخیرا بر روی تحرکات فضایی – اجتماعی صورت گرفته است، آشکارکننده‌ی نقش جریان‌ها و شبکه‌ها در هماهنگ کردن فعالیت‌های اساسی است. در واقع جریان‌ها تداعی‌کننده‌ی حضور چشمگیر سیاست و ایدئولوژی در شکل بخشی به فضای جغرافیایی می‌باشد. از ربط دادن سیاست و فضا و همه‌ی متغیرهای مربوط به آنها جغرافیای سیاسی و ژئوپلیتیک شکل می‌گیرد (حافظ‌نیا و دیگران، ۱۳۸۹: ۱۱٤). با خلق فضای مجازی ناشی از پدیده‌ی اینترنت به‌عنوان عرصه‌ی جدید فعالیت انسانی که در آن بازیگران توانایی کنش و واکنش را نسبت به همدیگر می‌یابند، بخشی از مطالعات ژئوپلیتیک نیز به این عرصه وارد شده است. با عنایت به این تحول مهم، مقاله‌ی حاضر در صدد است، ابعاد ژئوپلیتیکی فضای مجازی و تحولات ژئوپلیتیکی ناشی از انقلاب اطلاعات را مورد بررسی و تحلیل قرار دهد.

مبانی نظری

ژئوپلیتیک فضای مجازی

ژئوپلیتیک به‌عنوان علمی که روابط متقابل جغرافیا، قدرت و سیاست و کنش‌های ناشی از ترکیب آنها را با یکدیگر مطالعه می‌کند (حافظ‌نیا، ۱۳۸۵)، پس از ظهور فناوری‌های اطلاعاتی ارتباطاتی متحول شده است. ظهور شبکه‌ی اینترنت و ایجاد فضای مجازی باعث شده است که بخشی از محیط جغرافیای عملکردی علم ژئوپلیتیک به فضای مجازی منتقل شود.

ژئوپلیتیک فضای مجازی عمدتاً بر پایه‌ی مفهوم فضا استوار گردیده است. چرا که مفهوم مجاز به عنوان پسوند متمایزکننده‌ی آن از دیگر موضوعات مطرح در ژئوپلیتیک، کاملاً بر پایه‌ی عنصر جریانات فضایی استوار گردیده است؛ جریانات فضایی که ناشی از ارتباط کاربران اینترنت در نقاط مختلف کره زمین می‌باشد. در واقع ابعاد و گستره‌ی وسیع کارکردی و موضوعی ارتباطات در اینترنت و جایگزینی آن به جای جریان ارتباطات فیزیکی رایج، باعث شکل‌گیری مفهوم فضای مجازی شده است. با استناد به همین واقعیت، امروزه بسیاری از اندیشمندان در پدیده‌ی انقلاب اطلاعات از فضای مجازی، با عنوان سرزمین مجازی یاد می‌کنند. همین ویژگی باعث گردیده است، اصطلاحات و مفاهیم مورد استفاده در فضای جغرافیایی واقعی به نوعی با افزودن پسوند «مجازی» در این جنبه از فضای زندگی و عملکرد انسانی مورد بحث قرار بگیرد.

از دیگر سو، تغییر در عناصر و عوامل مولد مفهوم قدرت در عصر انقلاب اطلاعات و فناوری ارتباطات، مفهوم قدرت را به عنوان محور اصلی در مباحث علم ژئوپلیتیک وارد ابعاد و فضاهای ایجاد شده توسط این نوع از فناوری‌ها از جمله شبکه‌ی اینترنت، کانال‌های ماهواره‌ایی، دستگاه‌های ارتباطی همگانی و ... نموده است. اما در الگوهایی که برای سنجش قدرت ملی کشورها طراحی شده‌اند، این فناوری‌ها تنها به عنوان یک معیار از چندین معیار رایج در اندازه‌گیری قدرت ملی کشورها مورد اشاره بوده است. در واقع، مفهوم قدرت در

ژئوپلیتیکِ واقعیت‌محور از برآیند قوای ترکیب شده عناصر و عوامل تشکیل کالبد یک بازیگر سیاسی نشأت می‌گیرد که فناوری اطلاعات تنها یک جنبه از آن را شامل می‌شود.

عامل سیاست به عنوان دیگر عنصر تشکیل‌دهنده‌ی مفهوم ژئوپلیتیک در فضای جغرافیایی واقعی اشاره به تدابیر، مکانسیم‌ها و معیارهایی دارد که بازیگران عرصه‌ی سیاست بین‌المللی شامل کشورها، شرکت‌های چند ملیتی و احزاب و گروه‌های حامی حقوق بشر و محیط زیست با استفاده از آنها در فضای جغرافیایی سطح زمین به ایفای نقش و بازیگری می‌پردازند. با توجه به این چارچوب مفهوم سیاست در اصطلاح ژئوپلیتیک فضای مجازی دارای بیشترین نزدیکی با مفهوم سیاست در علم ژئوپلیتیک در مقایسه با دو مفهوم دیگر بوده و تنها تفاوت آنها در ابزارها و ترفندهای پیش‌بَری سیاست در دو فضای واقعی و مجازی می‌باشد.

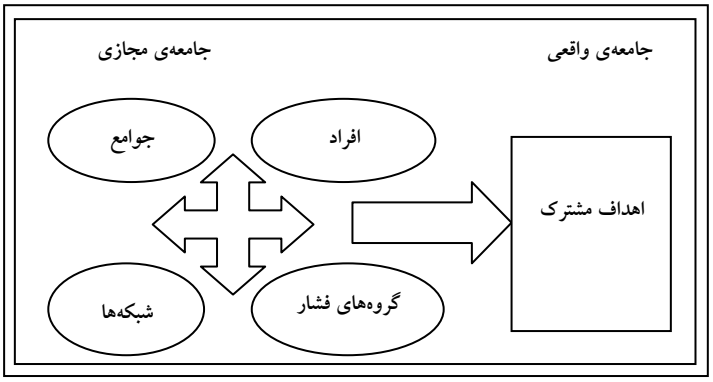
این نوع از مقایسه و تبیین در اصول و مفاهیم اصلی تشکیل‌دهنده‌ی دو مفهوم ژئوپلیتیک و ژئوپلیتیک فضای مجازی ناشی از الزامات پیشرفت و توسعه در به‌کارگیری فناوری‌های اطلاعاتی و ارتباطی جدید بوده و در راستای شناخت و ارائه‌ی راه‌حل برای مسائل و مشکلات ناشی از به‌کارگیری این پدیده‌ها و نیز استفاده کارآمد و صحیح از این ابزار برای پیشبرد منافع و اهداف گوناگون می‌باشد. در واقع، این فرآیند علاوه بر افزودن گزاره‌ها و نظریه‌های علمی نو در تبیین‌ها و تحلیل‌های ژئوپلیتیک، بُعد جدیدی از مباحث ژئوپلیتیک با عنوان ژئوپلیتیک فضای مجازی را در این علم مطرح نموده است که در راستای تحلیل، تبیین، گزاره‌سازی و پاسخگوی مسائل و مشکلات به وجود آمده ناشی از به‌کارگیری فناوری اینترنت و فناوری اطلاعات توسط سازمان‌ها و واحدهای سیاسی – سرزمینی رسمی عرصه‌ی نظام بین‌الملل یعنی کشورها یا شرکت‌های چند ملیتی و احزاب و گروه‌های با حیطه‌ی عملکرد فراملی در حوزه‌ی حقوق بشر، محیط زیست و اخیراً فعالیت‌های تروریستی می‌باشد.

فضای مجازی

فضای سایبر یا فضای مجازی[1] در تعریف برخی نویسندگان عبارت است از: «مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی

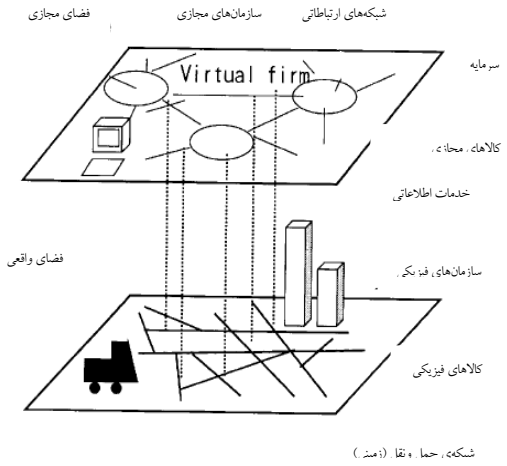
1 – Cyber Space

است. «آدامز» از سه استعاره‌ی عمده‌ی «مرز الکترونیک»، «فضـای مجـازی» و «شـاه‌راه اطلاعـات» استفاده می‌کند تا توجیه کند که شبکه‌های کامپیوتر همان فضای مجازی می‌باشد. به عبارتی فضـای مجازی مفهومی درباره‌ی جدا شدگی از جسم می‌باشد. یک سیستم فعل و انفعـال درونـی (کـنش متقابل) که گره‌گاه‌های یک نوع از فضا می‌باشد و به خاطر داشتن کنش متقابل معین مـی‌شـوند. در یک فضای معین شده بر اساس کنش متقابل، بالا و پـائین، داخـل و بیـرون، اینجـا و آنجـا معـانی ویژه‌ای را می دهد. حرکت از یک فضای یک یا دو بُعدی به یک فضای چند بُعـدی تغییـر جهـت می‌دهد و عناصر و پدیده‌ها در مکان‌های دور به صورت مکرر و در لحظـه‌ی آنـی بـه هـم وصـل می‌شوند (Adams, 1997: 164). از دید کلان عملکـردی، فضـای مجـازی کنتـرل و مـدیریت نـوع ویژه‌ای از اطلاعات را برآورده کرده است که برای نوع جدیدی از اقتصاد اجتماعی که اغلب اقتصاد اجتماعی اطلاعات نامیده می‌شود، ضروری می‌باشد. در واقع، این فضا منابع حیاتی زندگی خارج از فضای مجازی را از فضای مجازی فراهم می‌کند (Jordan, 2003: 142). از دید اجتماعی نیـز شـکل شماره‌ی (۱) نشانگر آن است که فضای مجازی توانایی آن را دارد که قابلیت‌های بـالقوه‌ی نیـروی انسانی و اطلاعات را برای غلبه بر مرزهای جغرافیایی، موانع سیاسی و تشریفات اداری به‌کار گیرد و منابع انسانی و اطلاعاتی را در انجام کارهای جمعی مدنظر قرار دهد. علاوه بر این، به عنوان یک بازوی مجازی، کمک مؤثری برای بسیاری از فعالیت‌هایی است کـه توسـط سـازمان‌هـا در دنیـای واقعی انجام می‌شود (فیضی و مقدسی، ۱۳۸٤: ٦٨).



شکل شماره‌ی ۱ – مدل حمایت الکترونیک (فیضی و مقدسی، ۱۳۸٤: ٦٩).

انقلاب در فناوری اطلاعات و شبکه‌ی اینترنت شبیه انقلاب صنعتی، در حال شکل دادن دوباره به جهان و ایجاد الگوهای جدید در قلمروهای اجتماعی، فرهنگی، اقتصادی و سیاسی (شکل شماره‌ی ۲) می‌باشد. مردمی که در حال حاضر از کامپیوترها استفاده می‌کنند، می‌توانند در آن واحد با همدیگر در سرتاسر جهان ارتباط برقرار کنند و کالاها و خدمات را بدون محدودیت در فضا یا زمان و با کمترین مداخله در این انتقالات نسبت به دوران قبلی مبادله کنند (Racicot & others, 1998: 96).



شکل شماره‌ی ۲ – فضای مجازی و فضای واقعی (Shibusawa, 2000: 255)

فضای مجازی شکل گرفته در عصر جهانی شدن الگوهای فضایی مطرح در جغرافیا را نیز تغییر داده است؛ چه به گفته‌ی «مانوئل کاستلر» فشرده‌سازی زمان و مکان در فضای جریان‌ها چنان رخ داده که فضایی مجازی و تقریباً بدون زمان و مکان به وجود آورده است. این فضای مجازی همان فضای الکترونیک و دیجیتال است که اقتصاد جهانی جدیدی پدید آورده است و این اقتصاد را بی‌وزن و بی‌مرز نامیده‌اند (هاگت، ۱۳۷۳).

از نظر حافظ‌نیا (۱۳۹۰) فضای مجازی و شبکه‌ی اینترنت دارای ویژگی‌هایی است که از منظر ژئوپلیتیک نیز دارای معنی بوده و می‌تواند در فرآیند رقابت بازیگران سیاسی و

حکومت‌ها و نیز نقش‌آفرینی در تولید قدرت و مناسبات آن در سیستم‌های جهانی و منطقه‌ای به‌کار گرفته شود. این ویژگی‌ها عمدتاً عبارتند از:

۱) امکان دسترسی کروی و جهانی و جابه‌جایی اطلاعات در مقیاس وسیع، سریع و ارزان بین مکان‌ها و فضاهای جغرافیایی؛

۲) امکان مبادله پیام، ایده، ارزش بین ملت‌ها، دولت‌ها، شرکت‌ها و بازیگران عرصه‌های مختلف؛

۳) امکان پیوند تمامی انسان‌ها، گروه‌ها، اجتماعات، سازمان‌ها، شرکت‌ها، دولت‌ها در سطح جهان و شکل‌گیری ائتلاف‌ها و همکاری‌ها؛

٤) امکان ابراز وجود و نمایش هویت‌های میکرو و ماکرو در سراسر جهان؛

۵) امکان بهره‌گیری از فضای مجازی برای ستیز، جنگ، رقابت و تهاجم نظامی، تروریستی و امنیتی علیه رقبا و دشمنان؛

٦) امکان تولید قدرت و تسریع روند توسعه‌ی ملی کشورها و تغییر موقعیت و منزلت ژئوپلیتیکی در سیستم‌های منطقه‌ای وجهانی؛

۷) امکان تولید رفاه، آسایش، سرعت عمل و ارائه‌ی خدمات به شهروندان در کشورهای مختلف؛

۸) امکان توسعه‌ی تعامل‌های اجتماعی و تفاهم فرهنگی بین شهروندان و گروه‌های اجتماعی کشورها و ملل مختلف و کمک به توسعه صلح و ثبات بین‌المللی و جهانی؛

۹) امکان بهره‌گیری ابزاری از فناوری اطلاعات و قابلیت‌های شبکه جهانی اینترنت برای سلطه و نفوذ بر سایر کشورها و ملت‌ها؛

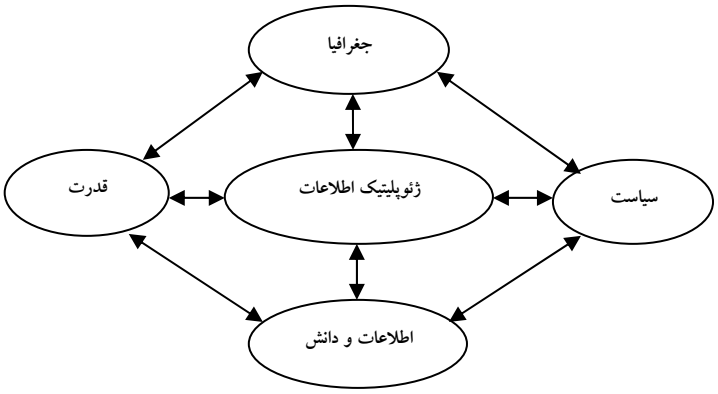
۱۰)امکان بهره‌گیری از فضای مجازی و شبکه‌ی اینترنت در توسعه‌ی مبادلات و تجارت بین‌الملل و گسترش فعالیت مالی و اقتصادی و نیز تولید درآمد و منابع اقتصادی برای کشورها، شرکت‌ها، مؤسسات و افراد؛

۱۱)امکان دسترسی به اطلاعات، پیام‌ها، نظرات و اندیشه‌های موجود در سراسر جهان به‌عنوان میراث فرهنگی و معرفتی مشترک بشری و نیز امکان انتشار نظرات، صداها، تظلمات و فریادها در مقیاس جهانی و رساندن آن به گوش هم‌نوعان و ابنای بشر. البته مشروط بر اینکه حکومت‌ها، شهروندان خود را از این حق طبیعی محروم نکنند.

ویژگی‌های مزبور در کنار سایر ویژگی‌های دیگر در فضای مجازی و شبکه‌ی اینترنت، آن را از نظر ژئوپلیتیک معنی‌دار می‌نماید که کالبدشکافی و تبیین آن می‌تواند به گسترش دانش ژئوپلیتیک در فضای مجازی منجر شود.

ژئوپلیتیک اطلاعات

همان‌گونه که «قدرت» موضوع و مبنای ژئوپلیتیک است و تمامی برداشت‌ها، رویکردها، مصادیق و مؤلفه‌های ژئوپلیتیک حول مدار و محور قدرت می‌چرخند و عنصر قدرت، به صورت نهان و آشکار، خود را در ژئوپلیتیک نشان می‌دهد و ژئوپلیتیک بدون قدرت مفهوم و معنایی ندارد، در ژئوپلیتیک اطلاعات و ارتباطات نیز موضوع کلیدی، برتری اطلاعاتی[1]، تفوق اطلاعاتی[2]، مزیت اطلاعاتی[3]، تمایز اطلاعاتی[4]، و در یک کلام قدرت است (شامحمدی، ۱۳۸۵). بر این اساس، ژئوپلیتیک اطلاعات به مطالعه‌ی نقش دانش، اطلاعات، فناوری و هنر در ابعاد مختلف تولید، گردآوری، تمرکز و انتشار آن بر تولید قدرت و تأثیر این قدرت بر روابط بازیگران و مناقشات آنها برای توسعه‌ی حوزه‌ی نفوذ خود در فضاهای جغرافیای و گروه‌های انسانی در مقیاس‌های محلی، ملی و جهانی می‌پردازد (حافظ‌نیا و دیگران، ۱۳۸۷: ۷۹).



شکل شماره‌ی ۳ - رابطه‌ی بین قدرت سیاسی و ژئوپلیتیک اطلاعات (حافظ‌نیا و دیگران، ۱۳۸۷: ۳۸۱)

1 – Information Superiority
2 – Information Dominance
3 – Information advantage
4 - Information Differential

یافته‌های تحقیق

ژئوپلیتیک فضای مجازی بـه عنـوان یکـی از عرصـه‌هـای نوظهـور ژئوپلیتیـک، ابعـاد و کارکردهای دوگانه‌ی مختلفی دارد. فضای مجازی، هم‌زمان که فرآیند جهانی شـدن را تسـریع می‌بخشد، محلی‌گرایی را نیز تشدید می‌کند. همچنین، همان‌طور که فضای مجازی ایـن امکـان را به بسیاری از افراد در پر اختناق‌ترین کشورها می‌دهد که از تحولات دیگر مناطق جهـان بـا خبر شوند، خود به عنصر سلطه بر افکار عمومی جهانی به‌ویژه توسط کشورهای کنترل‌کننده‌ی فضای مجازی نیز تبدیل می‌شود؛ به نحوی که با قدری تأمل می‌توان به این نتیجـه رسـید کـه امروزه رسانه‌ها به‌ویژه رسانه‌های دیجیتال، در خانه‌های مـا نیسـتند، بلکـه مـا درون رسـانه‌هـا زندگی می‌کنیم و همانند زندانی‌هایی که از غل و زنجیر فیزیکی رها و البته گرفتـار پایبنـدهای ذهنی قدرتمندتری شده‌اند، هیچ‌گونه مفری از امواج مسحورکننده‌ی آنها نداریم.

با این مقدمه‌ی کوتاه می‌توان گفت کـه مهـم‌تـرین ابعـاد ژئـوپلیتیکی فضـای مجـازی و تحولات ژئوپلیتیکی ناشی از انقلاب اطلاعات عبارتند از: تحـول در فضـای مـورد رقابـت در ژئوپلیتیک، همگرایی و همکاری، تحـول در ماهیـت قـدرت در ژئوپلیتیـک، افـزایش شـکاف دیجیتالی، بُعد مدیریتی و کنترل فضای مجازی، تحول در روابط میـان حکومـت و شـهروندان، هویت ملی و فروملی، تروریسم سایبری، جنگ نرم سایبری و جنگ مجازی.

تحول در فضای مورد رقابت در ژئوپلیتیک

از زمان ظهور ژئوپلیتیک در اوایل قرن بیستم، منابع قدرت از نظر ژئوپلیتیسین‌ها دائماً در حال تغییر بوده است. زمانی سلطه بر دریاها (نظریه‌ی قدرت دریـایی ماهـان) و زمـانی کنتـرل مناطق خشکی بزرگ دنیا (نظریه‌ی هارتلند مکیندر) عامل اصلی در به دسـت گـرفتن سـلطه‌ی جهانی قلمداد می‌گردید.

با آغاز جنگ سرد، عامل و منبع قدرت‌زا بـرای دو قـدرت مسـلط در ایـن دوره، توسـعه‌ی صنایع و تجارت جهانی و رشد اقتصادی برای کشورهای عضو دو بلوک و ارتقای صنایع سنگین در درون کشورها و به‌خصوص، توسعه در صنایع هوایی و فضایی و رقابـت تسـلیحاتی و اتمـی

همراه با کشش و جذبه‌ی ایدئولوژیک، ایدئولوژی‌های تحت رهبری دو ابرقدرت یعنی سرمایه‌داری لیبرال و کمونیسم بود. با اختراع کامپیوتر و توسعه‌ی ریزتراشه و انقلاب در فناوری اطلاعات و صنایع الکترونیک که از دهه‌ی ۱۹۶۰ و ۱۹۷۰ شروع و به تدریج در دهه‌های ۱۹۹۰ و ۲۰۰۰.م به اوج خود رسید به صورت ملموسی مزایا و نواقص دو مکتب مسلط نیمه‌ی دوم قرن بیستم آشکار گردید. انقلاب اطلاعاتی بر ویژگی شاخص اتحاد جماهیر شوروی یعنی قدرت نظامی اثر گذاشت. در عرصه‌ی تجاری نیز مسابقه‌ی تجاری عظیمی به راه افتاد و رقابت در عرصه‌های رایانه، ارتباطات دوربُرد و تراشه‌ها بین شرکت‌های آمریکایی و ژاپنی در گرفت که حاصل آن پشت سر گذاشتن دنیای کمونیست بود (آلبرتس و پاپ، ۱۳۸۵: ۲۴۹).

امروزه، داشتن قدرت اطلاعاتی یعنی تسلط برگردش اطلاعات الکترونیک در جهان دارای اعتبار و ارزش است. این‌گونه اطلاعات از طریق کاربری داده‌های انفورماتیک و تصاویر ماهواره‌ای و ابرشبکه‌های بزرگ اطلاعاتی به‌دست می‌آید.

درحال‌حاضر، ایالات متحده امریکا با اتخاذ راهبردهای پیچیده‌ی الکترونیک، با قدرت همه‌جانبه‌ی خود درصدد تسلط برجهان است (رفیعی، ۱۳۸۷ و کلاه‌مال همدانی،۱۳۸۱). آمریکا به‌عنوان مؤسس و متولی اولیه‌ی اینترنت کماکان کنترل و نفوذ محسوس و نامحسوس خود را بر این شبکه و فضا اعمال می‌نماید و از مزایای اقتصادی آن در فضای جغرافیایی خود بهره‌مند می‌شود. به‌عنوان مثال، مدیریت فنی و فناوری شبکه‌ی جهانی اینترنت در قالب شرکت آیکان[1]، هرچند خصوصی ولی با هویت آمریکایی در کالیفرنیا وجود دارد. قلب فناوری و تخصصی شبکه‌ی جهانی اینترنت و شرکت‌های بزرگ و برجسته‌ی اینترنتی و کامپیوتری در فضای جغرافیایی دره‌ی سیلیکون[2] در ایالت کالیفرنیا قرار دارد. سرورهای ریشه و بنیادین شبکه‌ی اینترنت و مدیریت بخش عمده‌ی سرورهای حافظه‌ی این شبکه در آمریکا قرار داشته و یا اینکه مدیریت و کنترل آنها در دستان شرکت‌های اصلی مستقر در آمریکا نظیر یاهو[3]،

1 - Internet Corporation for Assigned Names and Numbers (ICANN)
2 - Silicon Valley
3 – Yahoo

گوگل[1]، مایکروسافت[2]، فیس‌بوک[3]، یوتیوب[4]، تویتر[5] و غیره قرار دارد. تمرکز نهادهای ساختاری شبکه‌ی جهانی اینترنت و فضای مجازی و شرکت‌های اصلی آنها در خاک آمریکا، عملاً آن را در موقعیت مرجعیت اطلاعاتی قرار داده و به تمرکز فوق‌العاده‌ی اطلاعات و داده‌ها در قلمرو جغرافیایی آمریکا منجر می‌شود. تمرکز و ذخیره‌سازی اطلاعات ریز و درشت بخش‌های مختلف جهان اعم از خصوصی، عمومی، شرکت‌ها، حکومت‌ها و غیره به افزایش قدرت اطلاعاتی و سپس سلطه‌ی اطلاعاتی آمریکا بر دیگران می‌انجامد. اندیشه‌ی جریان آزاد اطلاعات در شبکه‌ی جهانی اینترنت که به سیاست رسمی و طبیعی ایالات‌متحده آمریکا تبدیل شده است، عملاً منجر به جهت‌گیری جریان خروشان اطلاعات و داده‌ها از سراسر جهان به سوی سرزمین ایالات‌متحده آمریکا و تمرکز و ذخیره‌سازی اطلاعات فراوان و گسترده‌ی جهان، و به‌دنبال آن توسعه‌ی فناوری اطلاعات در آن کشور می‌گردد که سلطه‌ی اطلاعاتی آمریکا بر جهان را در پی خواهد داشت. تسلط اطلاعاتی، به دارنده‌ی آن قدرت فزاینده‌ای نسبت به دیگران را اعطاء می‌نماید. احتمالاً بر همین اساس، برخی صاحب‌نظران در مسیر روند تحول قدرت در جهان، عصر جدید قدرت جهانی را مبتنی بر فناوری اطلاعات دانسته که از نظر آنها زیبنده‌ی ایالات‌متحده آمریکا می‌باشد.

از این رو، یکی از ابعاد ژئوپلیتیک فضای مجازی کنترل و بهره‌گیری از آن توسط قدرت سیاسی برتر است که این امر از طرق زیر انجام می‌شود:

- کنترل بر ابزار تولید اطلاعات نظیر نرم‌افزارهای پردازش‌کننده؛
- کنترل دسترسی برفضای مجازی به‌عنوان فضای جریان اطلاعات و شاه‌راه‌های اطلاعاتی؛
- کسب اطلاع و بهره‌گیری از محتوای پیام‌ها و داده‌های اطلاعاتی؛
- تمرکز و ذخیره‌سازی اطلاعات کاربران در مقیاس وسیع و از کشورهای مختلف؛

1 – Google
2 – Microsoft
3 – Facebook
4 – YouTube
5 – Twitter

- کنترل مدیریت فنی و تخصصی شبکه‌ی جهانی اینترنت از طریق مؤسساتی نظیر آیکان[1].
- آمریکا تنها قدرت و کشوری در جهان است که موارد مزبور را با فضای جغرافیایی قلمرو خود پیوند زده و قادر به کنترل شبکه‌ی جهانی اینترنت و فضای مجازی می‌باشد (حافظ‌نیا، ۱۳۹۰).

همگرایی و همکاری

فضای مجازی و شبکه‌ی جهانی اینترنت بسترهایی را برای همگرایی و همکاری در سطوح مختلف شهروندی و حکومتی بین کشورها نیز فراهم می‌کند که می‌تواند به صلح و امنیت جهانی کمک نماید. همگرایی و همکاری حکومت‌ها و کشورها در رابطه با فضای مجازی به‌دلیل سرشت و ماهیت جهانی آن، بر پایه‌ی ضرورت‌ها و الزامات زیر انجام می‌پذیرد:

الف) ضرورت‌های فنی و تخصصی برای تأمین نیازها و زیرساخت‌های شبکه‌ی اینترنت در مقیاس‌های ملی و فراملی؛

ب) ضرورت‌های ناشی از مدیریت یکپارچه و جهانی شبکه‌ی اینترنت و در قالب یک نهاد یا سازمان بین‌المللی؛

ج) ضرورت‌های حاکمیتی و حقوقی برای تعریف و استقرار یک نظام حقوقی بین‌المللی که امر کنترل و نظارت بر اینترنت را امکان‌پذیر نموده و امنیت شبکه را تضمین نماید؛

د) ضرورت‌های امنیتی و مقابله با تهدیدات در فضای مجازی به‌عنوان یک ارزش و نیاز مشترک برای همه‌ی شهروندان، کشورها و حکومت‌ها نظیر مقابله با جرایم سازمان‌یافته، شبکه‌های تبهکار و جنایتکار، مهاجمان به شبکه نظیر ویروس‌ها، هکرها، کراکرها و کرم‌های جاسوسی و بالاخره مبارزه با تروریسم در فضای مجازی؛

ه) ضرورت ائتلاف‌های سیاسی – نظامی، برای مقابله با تهدیدات نظامی و جنگ‌های مجازی دولت‌ها علیه یکدیگر (حافظ‌نیا، ۱۳۹۰).

1 – ICANN

بنابراین، ضرورت‌های پنجگانه‌ی مزبور، به‌ویژه تهدیدات امنیتی آن می‌تواند مبنا و اساس محکمی برای همگرایی و همکاری کشورها و دولت‌ها برای اتخاذ سیاست‌ها و روش‌های هماهنگ جهت مقابله با آن و نیز تدوین معاهدات سیاسی، امنیتی و کنوانسیون‌های حقوقی مورد نیاز باشد.

تحول در ماهیت قدرت

«رابرت کوهین» و «جوزف نای» معتقدند که انقلاب اطلاعاتی و ارتباطی به عنوان پدیده‌ای ملموس، فراگیر و اثرگذار، تأثیر بسزایی بر منابع قدرت می‌گذارد؛ چنان‌که در قرن ۲۱، احتمالاً فناوری‌های اطلاعاتی – ارتباطی مهم‌ترین منبع قدرت شناخته خواهند شد. قدرت نرم‌افزاری به‌گونه‌ای محسوس در اقناع فرهنگ از طریق برنامه‌های تلویزیونی اثرگذار است و تردیدی نیست که سازوکارهای فناوری‌های ارتباطی – اطلاعاتی همچون ماهواره و پرتاب امواج نامرئی شبکه‌های الکترونیکی جهانی، تار و پودهای قدرت تمدن‌های آینده را تشکیل خواهند داد (سوری، ۱۳۸۵: ۷۵). به اعتقاد «نای» (۱۳۸۷: ۱۳۱) قدرت در حال حرکت کردن از کشور «غنی از سرمایه» به کشور «غنی از اطلاعات» است. امروزه قدرت در گستره‌ی جهانی شدن بر تولید دانش مبتنی است. در این گستره کشورهایی قدرتمند محسوب می‌شوند که در دو محور اقتصاد و فناوری اطلاعات و ارتباطات پیشگام باشند (حافظ‌نیا و دیگران، ۱۳۸۵: ۵). بر این اساس، مفهوم قدرت وارد فضای مجازی و شبکه‌ی ارتباطات مالی و اقتصادی جهانی گردیده است و طیف جدید و گسترده‌ای از امکانات و قابلیت‌ها را همراه با مسائل و مشکلات مرتبط برای بازیگران آن به وجود می‌آورد.

«نای» (۱۳۸۷: ۱٦۷) معتقد است قدرت در عصر اطلاعات جهانی، بر اساس الگویی در میان کشورها توزیع شده است که به یک بازی شطرنج پیچیده و سه بعدی شباهت دارد. در رأس این صفحه‌ی شطرنج قدرت نظامی واقع شده است که عمدتاً خصلتی تک قطبی دارد. در صفحه‌ی میانی شطرنج، قدرت اقتصادی قرار گرفته است که خصلتی چند قطبی دارد و پائین‌ترین صفحه‌ی شطرنج نیز به عرصه‌ی روابط فراملی اختصاص دارد که خارج از کنترل

حکومت، از مرزهای سیاسی عبور می‌کند. این حوزه، بازیگران متنوعی دارد؛ بانکداری، راهزنی اینترنتی که عملیات اینترنتی دیگران را مختل می‌کنند و ... در این صفحه‌ی پایینی، قدرت به میزان گسترده‌ای پراکنده شده است. در اینجا، اساساً سخن گفتن از وضعیت تک قطبی، چند قطبی یا برتری معنایی ندارد ... اگر کشوری که در یک بازی شطرنج سه بعدی وارد شده است، تنها به بالای شطرنج نگاه کند و به صفحات دیگر و پیوندهای عمودی میان صفحات توجه نکند، در این بازی شکست خواهد خورد. در این ارتباط «کاستلز»[1] معتقد است: «فناوری اطلاعات و توانایی کاربرد و سازگار کردن آن، عامل حیاتی در تولید و دسترسی به ثروت، قدرت و دانش در دوران ماست» (کاستلز، ۱۳۸۵: ۱۱۲-۱۱۳).

«تافلر» نیز استدلال می‌کند که در عصر اطلاعات، آن دسته از دولت‌هایی که از فناوری‌های عصر اطلاعات استفاده می‌کنند و بیشترین منافع را از آنها به دست می‌آورند، در قله‌ی ساختار قدرت جهانی سه گانه قرار خواهند گرفت که تحت سیطره‌ی دانش و امور نامحسوس مرتبط با دانش است. توانمندی‌های این‌گونه دولت‌ها، برتر از کشورهایی خواهد بود که وابستگی خویش به اقتصاد صنعتی یا کشاورزی را حفظ کنند (آلبرتس و پاپ، ۱۳۸۵: ۵۱). «جوزف نای» در رابطه با قدرت در عصر اطلاعات خاطر نشان می‌کند:

«قدرت در عصر جهانی اطلاعات، بیش از هر زمان دیگری، یک بخش نرم جاذبه را در بر می‌گیرد و از یک بخش سخت تهدید و تطمیع نیز برخوردار است. تنها یکی از آنها را شامل نمی‌شود، بلکه هر دو را در بر می‌گیرد. منظور من از قدرت هوشمند همین است. در گذشته، کشورهای آتلانتیک قدرت هوشمند را از طریق جنگ سرد و با به‌کار گرفتن هر دو قدرت سخت و نرم اعمال می‌کردند. قدرت سخت ما تهاجم شوروی را متنفی ساخت، اما این قدرت نرم ما بود که اصول کمونیسم را در پس پرده‌ی آهنین نگاه داشت. فروریختن دیوار برلین بر اثر آتش توپخانه نبود، بلکه بر اثر ضربه چکش‌ها و بلدوزرها بود. این حادثه مثال بسیار حائز اهمیتی است» (نای، ۲۰۱۰).

1 – Castells

از این رو، نبردهای فرهنگی نبردهای قدرت در عصر اطلاعات هستند. در این ارتباط کاستلز معتقد است: «ارتباطات رایانه‌ای به نحو فزاینده‌ای در شکل‌دهی فرهنگ آینده، نقش مهمی ایفا خواهد کرد و نخبگانی که ساخت آن را شکل می‌دهند به نحو روزافزونی در جامعه‌ای که در حال ظهور است، دارای امتیاز ساختاری خواهند بود. بنابراین، ارتباط رایانه‌ای به راستی انقلابی در فرآیند ارتباطات و به واسطه‌ی آن در فرهنگ ایجاد خواهد کرد» (کاستلز، ۱۳۸۰: ٤١٨).

افزایش شکاف دیجیتالی

در طبقه‌بندی قدرت بین کشورها از جهت قابلیت‌های مختلف سیاسی، اقتصادی، فرهنگی، اجتماعی، نظامی و ... تفاوت‌هایی وجود دارد. این تفاوت‌ها در حوزه‌ی فناوری اطلاعات، تعبیر به شکاف دیجیتالی[1] می‌شود (شامحمدی، ۱۳۸۵). شکاف دیجیتالی نمایانگر شکل تازه‌ای از طبقه‌بندی اجتماعی در سطح جهان است که واجدان و فاقدان توانایی مشارکت در انقلاب اطلاعات را مشخص می‌سازد (گریفیتس، ۱۳۹۰: ١٤٠). برای نمونه، اگر چه در سال ۱۹۹۵ آمریکای شمالی و اروپای غربی به ترتیب ٤٣/٥ و ٢٨/٣ درصد بازار جهانی فناوری اطلاعات را در دست داشتند. ارقام مشابه برای آمریکای لاتین از یک‌سو و اروپای شرقی، خاورمیانه و آفریقا از سوی دیگر به ترتیب ۲ و ۲/٦ درصد بود (روزنا، ۱۳۹۰: ۳۲۱).

ضریب نفوذ اینترنت در جهان متفاوت است و فاصله آن بین کاربران کشورهای پیشرفته و عقب‌مانده زیاد است. این فاصله گاهی از یک تا هفت می‌باشد. مثلاً برابر با آمار تابستان سال ۲۰۱۰ ضریب نفوذ اینترنت در قاره‌ی آفریقا ۱۰/۹ درصد (آخرین رتبه در جهان) و درآمریکای شمالی برابر با ٧٧/٤ درصد (اولین رتبه در جهان) بوده است (حافظ‌نیا، ۱۳۹۰). شکل شماره‌ی ٤ به وضوح اختلاف سطح برخورداری کشورهای غربی با سایر کشورها را نشان می‌دهد.

1 – Digital Gap

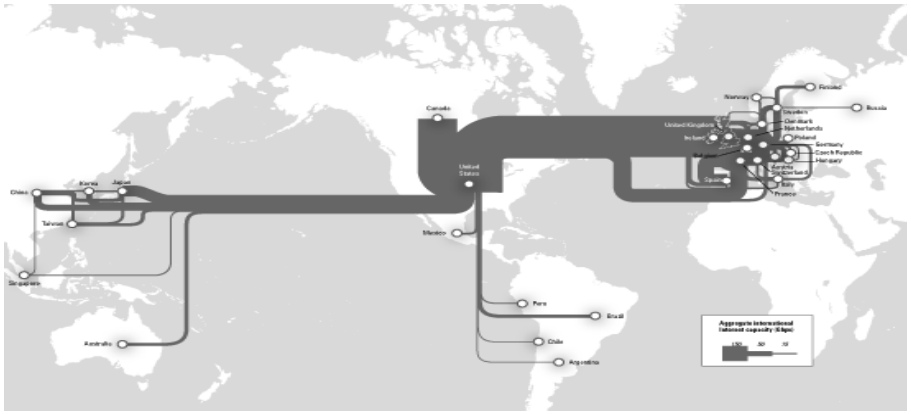
بر این اساس می‌توان گفت که امروزه، واقعیت‌های جهـان بـر اسـاس منـافع کشـورهای شمال تعریف و تفسیر می‌شوند. بر اساس آنچه «گالتونگ» به درستی ترسـیم مـی‌کنـد جریـان بین‌المللی اخبار بر اساس چهار محور مشخص می‌گردد:

۱) رویدادهای جزئی «مرکز» [غـرب] کـه در سیسـتم‌هـای مطبوعـاتی جهـان گـزارش می‌شود، از ثقل بیشتری برخوردار است؛

۲) میزان تبادل خبرها میان ملل «مرکز» و «پیرامون» و میزان تبادل خبرها بین خـود ملـل «مرکز»، با یکدیگر تفاوت بسیار زیادی دارد؛

۳) خبرهای ملل «مرکز» سهم بیشـتری از رویـدادهای خـارجی را در رسـانه‌هـای ملـل «پیرامون» به خود اختصاص می‌دهد، حـال آن کـه سـهم رویـدادهای «پیرامـون» در رسانه‌های «مرکز» کمتر است؛

تقریباً «جریان خبر» در میان ملل «پیرامون» بسیار ناچیز است و یا اصلاً وجود ندارد. این امـر به ویژه در طول مرزهای به وجود آمده توسط استعمار بیشتر صادق است (خان‌محمدی، ۱۳۸۵).



شکل شماره‌ی ٤ – نقشه مسیرهای اصلی اینترنت بین‌المللی (Saunders, 2009: 20).

بدیهی است تداوم شکاف فناورانه و دیجیتالی و شـکاف فنـاوری اطلاعـات و کـامپیوتر منجر به تداوم شکاف توسعه، و تقسیم جهان به دو بخش توسعه‌یافته و عقب‌مانـده مـی‌گـردد. تداوم آن همچنین به توسعه و پایداری شکاف فقـر و غنـی و شـکل‌گیـری رابطـه‌ی سـلطه و

زیرسلطه منجر می‌شود. از این رو، شکاف دیجیتالی را می‌توان ناشی از عدم توازن[1] ژئوپلیتیکی در قلمرو فناوری‌های اطلاعاتی و ارتباطی دانست که از ساختار و نظام سیاسی، اقتصادی، اجتماعی، فرهنگی حاکم بر کشورهای ضعیف و قوی یا محروم و برخوردار متأثر می‌شود. به عبارت بهتر، شکاف دیجیتالی معضلی سیاسی – اجتماعی است و بر فاصله اجتماعی – اقتصادی بین جوامع دلالت می‌کند که بر اثر تفاوت سطح دسترسی آنان به فناوری اطلاعات و ارتباطات ایجاد شده است. شکاف دیجیتالی در واقع تداوم همان راه فقر و غنا است، منتهی با تعابیر، ادبیات و ابزاری دیگر.

بُعد مدیریتی و کنترل فضای مجازی

مدیریت و کنترل بر شبکه‌ی جهانی اینترنت و فضای مجازی یکی از موضوعات رقابتی بین بازیگران است. این امر به یکی از چالش‌های ایالات‌متحده آمریکا به‌عنوان کشوری که به‌طور تاریخی و سنتی و به شکل محسوس و غیرمحسوس این شبکه را کنترل و مدیریت می‌نماید، درآمده است. کشورها و دولت‌های دیگر به این امر علاقه‌ای ندارند و سعی می‌کنند یا مدیریت و کنترل اینترنت را از دست آمریکا خارج نمایند و یا اینکه در مدیریت جهانی آن مشارکت داشته باشند. پس از تصمیم «بیل کلینتون» رئیس‌جمهور آمریکا در سال ۱۹۹۸، دولت آمریکا خود را از مدیریت روزمره‌ی شبکه جهانی اینترنت کنار کشید و اداره‌ی امور فنی و تخصصی آن را در قالب یادداشت تفاهمی که به امضای وزارت بازرگانی آمریکا و شرکت آیکان رسید، به آن شرکت محول نمود. این یادداشت تفاهم تاکنون چند بار تمدید شده است. آیکان شرکتی غیرانتفاعی و خصوصی است که در خاک آمریکا بوده و مطابق نظام حقوق خصوصی ایالت کالیفرنیا تأسیس شده است و اداره‌ی چهار امر اساسی در رابطه با شبکه‌ی اینترنت را به‌عهده دارد، شامل: مدیریت سیزده سرور بنیادی شبکه‌ی اینترنت، تخصیص «آی پی» یا پروتکل اینترنت به‌کاربران، تخصیص نام‌های دامنه‌ی تراز اول عمومی و جغرافیایی، هماهنگی پارامترها و پروتکل‌های فنی شبکه‌ی اینترنت. با توجه به نقش مدیریتی و کنترلی

1 – Imbalance

آیکان از حیث فنی و تخصصی بر شبکه‌ی اینترنت، پرواضح است که موقعیت و منزلت ژئوپلیتیکی آمریکا نسبت به سایر کشورها حالت فرادستی دارد و این موضوع مورد اعتراض دولت‌ها و کشورهای دیگر قرار گرفته است (حافظ‌نیا، ۱۳۹۰).

تحول در روابط میان حکومت و شهروندان

فناوری‌های اطلاعاتی و ارتباطی رابطه‌ی میان حکومت‌ها با شهروندانشان را نیز تا حدود زیادی تحت تأثیر قرار داده است. تأثیر اینترنت بر حوزه‌ی عمومی سیاسی تأثیری دیالکتیکی است یعنی از یک‌سو وابستگی افراد را به مراجع سنتی قدرت کاهش داده و قدرت شهروندان را در اتخاذ موضعی آگاهانه‌تر در برابر این مراجع افزایش می‌دهد و از سوی دیگر، این روند در چارچوب همان الگوهای سیستم فرهنگی حاکم و نابرابری قدرت جریان می‌یابد (میناوند، ۱۳۸۵: ۱٤۱). بیشتر مردم تصور می‌کنند که زیرساخت عظیم اینترنت، شبکه‌ای باز و غیرمتمرکز است و اطلاعات آزادانه به اشتراک گذاشته می‌شود. در حالی که گره[1] مجزایی که ارتباطات اینترنتی را شکل می‌دهد وجود ندارد و در نتیجه هیچ شکلی از کنترل متمرکز به چشم نمی‌خورد، اما هزاران گره وجود دارد که ضمن تجزیه و تحلیل و فیلتر اطلاعات، به عنوان دروازه[2] عمل می کنند (Deibert,2009: 324).

از طرف دیگر، امروزه امور زندگی اجتماعی – سیاسی بیش از پیش از حد و مرزهای ملی فراتر رفته و توانایی‌های دولت ملی برای اداره و ساماندهی این‌گونه امور کمتر شده است. فرآیند جهانی شدن توانایی‌های دولت در امر نظارت، کنترل و سانسور را به میزان چشم‌گیری کاهش داده است. بازسازی شدن فضا در زمان و فضامند شدن زندگی اجتماعی، هرگونه مرز و بستر، به ویژه اجتماعی- فرهنگی، را نفوذپذیر کرده، سانسور و کنترل و انحصار را بسیار دشوار و حتی ناممکن نموده است (گل‌محمدی، ۱۳۸٤: ۷٤-۷۵).

1 – Node
2 – Gateway

فضای مجازی و شبکه‌ی جهانی اینترنت بـه‌دلیـل ماهیـت عملکـردی فراکشـوری و نیـز قابلیـت برقراری ارتباط و جابه‌جایی اطلاعات و داده در مقیاس جهانی و اتصال کاربران و ابنـای بشـر از سراسـر جهان، صرف‌نظر از ملیت، قومیت، مذهب، نژاد، زبان و غیره، عملاً در تعارض بـا منـافع حکومـت‌هـا و کشورها و دولت‌های ملی قرار می‌گیرد. به عبارتی، فضای مجازی و شبکه‌ی اینترنت، قدرت حکومت‌ها و دولت‌های ملی و نیز حاکمیت آنها بر فضای ملی را به چالش می‌کشد. این خاصـیت فضـای مجـازی می‌تواند به تولد و رشد نیروهای ضد حکومتی، کاهش مقبولیت حکومـت‌هـا نـزد شـهروندان، افـزایش قدرت مانور نیروهای ضد حکومتی چه در مقیاس شهروندی و فضای ملی و چه در مقیاس فراکشـوری و جهانی و به‌طور کلی امکان تهدید، تضعیف، سـقوط و جابجـایی دولـت‌هـا و حکومـت‌هـای ملـی و ارزش‌های مورد نظر آنها و جایگزینی نیروهای رقیب و نیز کاهش اقتدار حاکمیتی آنان منجر گردد.

از این‌رو، حکومت‌ها و دولت‌های ملی به تکاپو افتاده‌اند تا از پس این چـالش برآینـد و تهدیدات بر علیه خود را کاهش داده و یا از بین ببرند. آنها گاهی اوقات تهدیدات علیه خود را به تهدیدات علیه امنیت ملی تعبیر، تفسیر و معنی می‌کنند و از آن بر علیـه نیـروهـای رقیـب و ضد خود استفاده می‌نمایند. بنابراین، حکومت‌ها و دولت‌ها و نیروهای ضد آنها (چه با مبـدأ و مقیاس ملی و چه با مبدأ و مقیاس فراکشوری و جهانی) در فضای مجازی و بر سر فرصت‌هـا و قابلیت‌های آن با یکدیگر به رقابت و نبرد می‌پردازند و همدیگر را به چالش می‌کشند.

نیروهای ضد حکومتی، حکومت‌ها را به دیکتاتوری، سانسور اخبار و اطلاعات، ستم بـه شهروندان و نقض حقوق شهروندی و حق دسترسی آزاد به اطلاعات متهم کـرده و از تمـامی ظرفیت‌های فضای مجازی نظیر سایت‌ها، موبایل‌ها، پیـام‌هـای کوتـاه، وبـلاگ‌هـا، ای‌میـل‌هـا، شبکه‌های اجتماعی و غیره برای تبلیغات و رساندن پیام‌ها و نظرات خود بـه گـوش هموطنـان خود و نیز جهانیان و کسب هواداری استفاده می‌کنند (حافظ‌نیا، ۱۳۹۰).

هویت ملی و فروملی

مسأله‌ی هویت در فضای مجازی از موضوعات بحث‌برانگیز شده اسـت. زیـرا بـرخلاف انتظار عده‌ای، خرافه‌ی یکپارچه‌سازی مردم جهان در پرتو شـبکه‌ی جهـانی ارتباطـات، تحقـق

نیافت و در نقطه مقابل باعث ظهور و بروز هویت‌های ریشه‌ای جهان واقعی نظیر قومیت، سرزمین ملی، مکان و فضا، دین و مذهب، نژاد و زبان، طبقه اجتماعی و غیره گردید. به‌طوری که بر پایه‌ی آنها سایت‌های اینترنتی و وبلاگ‌های فراوانی تأسیس شده و فعالیت می‌نمایند که بر این اساس رقابت شدیدی را برای ابراز وجود در برابر دیگران سبب شده است.

در این رابطه، «کوهن» روند سریع جهانی شدن اقتصاد جهانی و تبدیل شبکه‌های ارتباطی به سیستم‌های اطلاعات جهان‌گستر، مرزها و هویت‌های ملی را از میان نخواهد برد. به رغم برخی ادعاها، جهانی شدن به حیات جغرافیا و ژئوپلیتیک پایان نخواهد داد، بلکه نظام ژئوپلیتیکی به مراتب پیچیده‌تری را پدید خواهد آورد (Cohen, 2009).

علاوه بر آن، تشکل‌ها و شبکه‌های اجتماعی فراوانی مبتنی بر هویت‌های ریشه‌ای نیز پدید آمده‌اند که عامل همگرایی آنها احساس تعلق به شناسه‌ی هویتی فضای واقعی و تعریف خود در چارچوب یک هویت مشخص و متمایز از سایر شناسه‌های هویتی می‌باشد.

این فرآیند گردانندگان و هواداران این‌گونه تشکل‌ها و سایت‌های هویت‌پایه را به وادی نوعی رقابت در فضای مجازی می‌کشاند. آنها احساسات، عواطف و علایق هویتی خود که متعلق به دنیای واقعی است را به فضای مجازی منتقل می‌کنند و سعی می‌نمایند ارزش‌های هویتی خود را در فضای مجازی انتشار دهند تا بر رقبای خود پیشی بگیرند و به درخشندگی و تثبیت موقعیت برای ارزش‌های هویتی خود در برابر دیگران کمک کنند. نمونه‌ی مشخص این رقابتها، رقابت زبانی است. بر همین اساس گروه‌ها و کاربران کشورهای مختلف سعی دارند زبان خود را در اینترنت جاری کنند، تا اولاً به معرفی و درخشندگی زبان خود به‌عنوان یکی از شاخصه‌های بنیادین هویت در مقیاس جهانی کمک نمایند، ثانیاً با ایجاد فضای چند صدایی و تکثرگرا از سلطه‌ی تک‌زبانی بر فضای مجازی و به‌طور مشخص زبان انگلیسی جلوگیری نمایند، ثالثاً مانع از انتقال ارزش‌های فرهنگی تهدیدکننده می‌شوند که از طریق زبان انگلیسی، ارزش‌های هویتی آنها را به چالش می‌کشد. همین امر سبب شده است که ساختارهای فضای مجازی نظیر مرورگرها، موتورهای جستجو، سایت‌های بزرگ شبکه‌های اجتماعی، دایره‌المعارف‌های فضای مجازی مانند «ویکی‌پدیا» تنوع زبانی را در برنامه کار خود بپذیرند و

حتی زبان‌های محلی و غیرمشهور را نیز در فرآیند فعالیت و کارکردهای خـود مـورد پـذیرش قرار دهند. البته این سیاست یک پیامد مثبـت بـرای آنهـا نیـز دارد و آن اینکـه حـوزه‌ی نفـوذ جغرافیایی و دایره‌ی کاربران خود را نیز گسترش می‌دهنـد و از ایـن طریـق اعضـا و کـاربران متعامل با آنها افزایش پیدا می‌کند (حافظ‌نیا، ۱۳۹۰).

همچنین باید توجه نمود که دولت – ملت‌ها به رغم مشکلاتی کـه بـرای آنهـا در عصـر انقلاب اطلاعات به وجود می‌آید، همچنان بـه حیـات خـود ادامـه خواهنـد داد؛ چـه، گیـدنز[1] (۱۳۷۹) در پاسخ به این سؤال که آیا در حالت جهانی شدن، ملت‌ها اهمیت خـود را از دسـت می‌دهند می‌گوید: «کسانی که معتقدند دوران دولت ـ ملت سپری شده، اشتباه می‌کنند. دولت ـ ملت‌ها هنوز قدرت زنده و پویایی هستند. حتی به جهاتی می‌توان گفت که دولت ـ ملت‌ها نـه تنها تضعیف نشده‌اند بلکه اهمیت بیشتری یافته‌اند. تا چند سال پیش پدیده‌هـایی دیگـر ماننـد امپراتوری‌ها در مقابل دولت ـ ملت‌ها قرار داشتند. شوروی یک نوع امپراتـوری بـود. در قـرن بیستم امپراتوری‌های مختلفی وجود داشت، امـا اکنـون همـه‌ی اشـکال امپراتـوری بـه غیـر از امپراطوری امریکا از بین رفته‌اند. همه‌ی کشورها دولت ـ ملت شده‌انـد و ایـن تحـولی بـزرگ است.»

تروریسم سایبری

تروریسم سایبری یا تروریسم مجازی واژه‌ی جدیدی می باشـد کـه بـه ادبیـات سیاسـی جهان وارد شده است. این نوع عملیات تروریستی به هرگونـه اقـدامات خرابکارانـه‌ای اطـلاق می‌شود که نفوذگران و اخلال‌گران رایانه‌ای علیه شبکه‌های رایانه‌ای و اینترنتی یک کشور انجام می‌دهند (ضیائی‌پرور، ۱۳۸٦: ۲٤ و کانوی، ۱۳۹۰). در تروریسـم مجـازی گـروه‌هـای سیاسـی معترض حکومت‌ها، زیرساخت‌ها، منافع و توانـایی‌هـای حکومـت مقابـل خـود را در فضـای مجازی مورد تهاجم قرار داده و احتمالاً به جان شهروندان کشور مربوطه نیز تعرض می‌نمایند.

1 – Giddens

در دهه‌ی ۱۹۸۰ «باری کولین»، پژوهشگر ارشد مؤسسه‌ی اطلاعات و امنیت درکالیفرنیا، واژه‌ی «سایبر تروریسم» را جعل کرد. این واژه جعل شده توسط او، سایبر – فضا و تروریسم را دربر می‌گرفت. «سایبر تروریسم، حمله‌ی از پیش طراحی شده و دارای انگیزه‌های سیاسی به سیستم‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده‌ها است که به خشونت علیه اهداف غیر متخاصم توسط گروه‌های زیر ملی یا عوامل پنهان، منجر می‌شود» (جعفرپور، ۱۳۸۷: ۳۵۵). با این حال، متخصصان معتقدند که تعریف تروریسم همانند تعریف سایبر تروریسم محل مناقشه و مباحثه می‌باشد. سایبر تروریسم در رابطه با حمله‌های غیرقانونی علیه کامپیوترها و اطلاعات، انگیزه‌های سیاسی و تأثیرات یک حمله‌ی سایبری مورد تعریف بوده است (goodman, 2007: 195).

جنگ نرم سایبری

قابلیت‌های فضای مجازی همراه با تماس مستقیم میلیاردها کاربر باعث شده تا بازیگران سیاسی اعم ازدولت‌ها، احزاب و اشخاص حقیقی، فضای مزبور را به عرصه‌ی رقابت و عمل سیاسی تبدیل نمایند و فرصت‌ها و تهدیدها این فضا را در راستای کسب قدرت به نفع خود و یا علیه رقیب به‌کار گیرند. مهم‌ترین عرصه‌های عمل سیاسی در فضای مجازی فرآیندهای دموکراتیک نظیر انتخابات و دموکراسی الکترونیکی، فرآیندهای تصمیم‌گیری، تبلیغات و تأثیرگذاری به افکار عمومی و کاربران اینترنت برای کسب مقبولیت سیاسی و نیز تضعیف موقعیت و مقبولیت سیاسی حکومت‌ها و بازیگران رقیب نزد شهروندان می‌باشد. به همین خاطر هم‌زمان با افزایش ضریب نفوذ در کشورها، در سال‌های اخیر، فضای مجازی و شبکه‌ی اینترنت به نحو قابل توجهی در انتخابات کشورها نظیر آمریکا و ایران و نیز فعالیت‌های تبلیغاتی بازیگران سیاسی، و همچنین بسیج سیاسی از طریق شبکه‌های اجتماعی مجازی نظیر تونس و مصر در فرآیند سرنگونی دولت‌های «بن علی» و «مبارک» و نیز «اردن»، «یمن»، «بحرین» و غیره در ژانویه ۲۰۱۱ و پس از آن مورد بهره‌برداری قرار گرفته است (حافظ‌نیا، ۱۳۹۰).

جنگ نرم نوعی جدید از جنگ است که درآن به جای استفاده از زور و سلاح و قدرت نظامی از ابزارها و تکنیک‌های غیرخشونت‌آمیز در تقابل با رقیب یا دشمن برای برتری‌جویی و یا

کسب منافع ملی استفاده می‌شود. جنگ‌های رسانه‌ای، جنگ‌های رایانه‌ای، جنگ الکترونیک، جنگ روانی، جنگ اطلاعاتی و سرانجام جنگ سایبری از جمله مصادیق جنگ نرم هستند. بر این اساس، جنگ نرم سایبری به نوعی از جنگ اطلاق می‌شود که با استفاده از فناوری‌های مبتنی بر اینترنت مانند ایمیل، وبلاگ، وب سایت و شبکه‌های اجتماعی و با تکنیک‌هایی مانند هک و نفوذ، خرابکاری و اختلال در پایگاه‌های اطلاع‌رسانی، سعی در برتری‌جویی نسبت به دشمن یا رقیب دارند و هدف از آن تغییر مواضع کشور هدف، استحاله و فروپاشی و یا تغییر حکومت در کشور مورد نظر است (دفتر مطالعات و توسعه‌ی رسانه‌ها، ۱۳۸۸).

در رابطه با مصادیق اصطلاح جنگ سایبری «رالف فوربس» نویسنده و کارشناس مسائل سیاسی طی مقاله‌ای با عنوان «نخبگان جهانی، سیا در پشت جنگ کثیف علیه ایران» که در هفته‌نامه‌ی «آمریکن فری پرس» منتشر شد در رابطه با مسائل انتخاباتی ایران در سال ۱۳۸۸ نوشته است:

«یک جنگ پیچیده در فضای سایبر علیه ایران جریان داشت که طی آن رایانه‌ها و ابزارهای ارتباطی یا خاموش می‌شدند و یا اینکه با انواع هک شده یا بدلی جایگزین می‌شدند؛ به‌طوری‌که وب سایت‌های متعلق به خبرگزاری‌های ایران، ریاست جمهوری و برخی دیگر از مقامات ایرانی از فضای آنلاین خارج شدند. همچنین وب سایت‌های خبری ایرانی طی اعلام نتایج انتخابات یا غیر فعال شده بودند و یا اینکه با سایت‌های بدلی جایگزین شده بودند. در حقیقت این آشفتگی به‌طور مخفیانه و سری توسط سازمان سیا و به منظور گسترش آشفتگی، هماهنگ شده بود. آنها، ایرانیان را غرق در اطلاعات غلط، پیامک‌های متضاد، عکس‌ها و ویدئوهای تقلبی کردند. مرتکبین این حملات سپس قطع کانال‌های ارتباطی را که خود در راستای نقشه‌ی براندازی دولت ایران انجام داده بودند، به این دولت نسبت داده و آن را محکوم کردند. در میان این آشفتگی سایبری، یکی از مقامات وزارت امور خارجه‌ی آمریکا از پایگاه اینترنتی «توئیتر» خواست تا برنامه‌ی تعمیراتی خود را به تعویق بیاندازد؛ زیرا بر اساس این برنامه سرویس‌های توئیتر طی زمانی که در ایران جزء ساعات روز و اوج التهابات سیاسی

است، قطع می‌شوند. این در حالی است که اگرچه دولت اوباما در ابتدا اعلام نفوذ بر تـوئیتر را تکذیب کرد اما در نهایت این اقدام خود را پذیرفت» (بابک، ۱۳۸۸: ۱۸٦).

جنگ مجازی (پست مدرن):

فضای مجازی قابلیت‌های وسیعی برای تبدیل شـدن بـه عرصـه‌ی کـارزار و سـتیز بـین دولت‌ها، بازیگران و طرف‌های درگیر می‌باشد. درگیری‌ها در فضای مجازی، شبیه‌سـازی شـده درگیری‌های در فضای واقعی می‌باشد. در عرصه‌ی جنگ مجازی طرفین منازعه، حکومت‌ها و کشورها هستند که علیه یکدیگر می‌جنگند. در جنگ مجازی طرفین درگیر هـم مـی‌تواننـد بـه سازماندهی ارتش‌های مجازی و دست زدن به یک نبرد و جنگ مجازی اقدام کنند و هم این‌که ظرفیت‌های فضای مجازی و شبکه اینترنت را برای انجـام عملیـات نظـامی در فضـای واقعـی به‌کار گیرند (حافظ‌نیا، ۱۳۹۰).

در جنگ‌های آینده، کشمکش بر سر اطلاعات، نقشی محـوری خواهـد داشـت و شـاید جای کشمکشی را بگیرد که در جنگ‌های گذشته بر سـر دسـتیابی بـه مواضـع جغرافیـایی در می‌گرفت. برتری اطلاعاتی آرام آرام به صورت عرصه‌ی رقابتی نـو و بسـیار شـدیدتر پدیـدار می‌شود (دیویس، ۱۳۹۰: ٤٤٨)

جنگ اطلاعات، جنگ روز است. مجله‌ی تایم روی جلد یکی از شماره‌هایش را به ایـن نوع جنگ اختصاص داده، «نیوت گینگریچ»[1] در مورد آن به ایراد سخنرانی پرداخته، «جکسـون براون»[2] آهنگی با نام «جنگ‌های اطلاعات» خوانده، «تام‌کلنسـی»[3] رمـانی بـا همـین درون‌مایـه نوشته و مؤسسه‌ی پژوهشی «رَند» پروژه‌ی تحقیقاتی وسیع و گسترده‌ای را در همین زمینـه در دسـت اجـرا دارد. «جنـگ سـیبرنتیک، جنگـی قریـب‌الوقـوع»[4] عنـوان مقالـه‌ای اثرگـذار از «جان‌آرکوییلا» و «دیوید راندفلت»[5] است که در سال ۱۹۹۳ منتشر گردید. مقاله‌ی مزبـور از آن

1 - NewtGingrich
2 - Browne Jackson
3 - Tom Clancy
4 - Coming is CyberWar
5 - Rondfeld David and Arquilla John

دست هشدارهای خشک و بی‌روحی نبود کـه معمـولاً از تحلیـل‌گـران دایـره‌ی سیاسـت‌هـای بین‌الملل مؤسسه‌ی رَند یا نشریات سیاسی انتظار می‌رود. البته محتوای مقاله پیش از آن بارها و بارها از سوی دانشگاهیان غیر وابسته به این موسسه، نویسندگان داستان‌های علمی ـ تخیلـی و افسران نه چندان عالی‌رتبه‌ی آمریکا که از اوایل دهه‌ی ۱۹۸۰ به طور مکرر نگرانـی خـود را از تأثیر انقلاب اطلاعات بر جنگ ابراز داشته‌اند مورد اشاره قرار گرفته بود و حتی نمی‌شد بین آن با پاره‌ای جریانات فکری نظامی رایج در طول تاریخ جنگ، از زمان چاپ کتـاب هنـر جنـگ «سون تزو» تا به امروز تفاوت محسوسی سراغ گرفت. اما آنچه هست، فعلاً اسم این مقالـه بـر سر زبان‌ها افتاده و شهرتش موجب انتشار ده‌ها مقالـه‌ی مشـابه در مطبوعـات و نشـریات روز گردیده است (Gray, 1997).

جنگ سیبرنتیک دارای سه مؤلفه‌ی متمایز است که بـه عقیـده‌ی طرفـدارانش حسـاس و مهم‌اند. نخست این تصور که، جنگ را می‌توان با شیوه‌های علمی اداره کرد. این تصور بـاوری است بسیار کهن که قدمت‌اش دست‌کم به دهه‌ی نخست ۱۵۰۰ میلادی باز می‌گردد. دوم ایـن اعتقاد که، عمده‌ی فرآیند جنگ به عنصر اطلاعات و تفسیر آن، به‌خصوص در قالب سیاسـت، متکی است و در همین حیطه است که فراقواعد جنگ برای تعیین برنده تدوین می‌شـوند. ایـن هم مفهوم تازه‌ای نیست و آن را در کتاب هنر جنگ نیز می‌توان یافت. شالوده‌ی تفکر انـواع و اقسام جنـگ‌هـای چریکـی (کوچـک)، اعـم از ناهماهنگ،مسـتعمراتی، نـامنظم، ضدشـورش، جنگ‌های سرد کم‌شدت و طیف وسیع عملیات‌های نظـامی غیررزمـی (موسـوم بـه OOTW)[1] همین مفهوم است. سوم، تأکید برنقش و جایگاه رایانه و نیز قابلیت آن در پشت سـر گذاشـتن مرزهای مرسوم زمانی و مکانی (Gray, 1997).

حوزه‌ی اخیر حقیقتاً حوزه‌ای جدید و قابل توجـه اسـت، گرچـه نظریـه‌پـردازان نظـامی معاصر نیز همان رؤیاهای شـیرینی را در سـر مـی‌پرورانـند کـه نظریـه‌پـردازان جنـگ ویتنـام

1 - Snoitarepo rehto Naht Raw

درخصوص ایجاد میدان‌های نبرد الکترونیکی در سر داشتند، با این تفاوت که اینان در نظریات‌شان، خودِ عرصه‌ی سیبرنتیک را در حکم میدان نبرد می‌گیرند.

بعضی اندیشمندان با توجه به ماهیت تنش‌ها و جنگ‌هایی که در عصر اطلاعات و در فضای مجازی روی می‌دهد توصیه می‌کنند اگر تهدیدهای جنگ اطلاعاتی واقعیت پیدا کند، آمریکا نباید راهبرد جنگ اطلاعاتی در برابر جنگ اطلاعاتی را در پیش بگیرد؛ زیرا ممکن است مهاجمان به مقدار بسیار کم به زیر ساختار اطلاعاتی وابسته باشند و در نتیجه از تهدید خطرهای جنگ اطلاعاتی تلافی‌جویانه تأثیر نگیرند (آلبرتس و پاپ، ۱۳۸۵: ۲۷۱). دکترین‌های پنتاگون و بازی‌های جنگی مخصوص جنگ‌های سیبرنتیک جلوه‌ای روشن و شفاف به این تصویر تیره و کدر می‌بخشند. طبق‌آماری که از سوی روزنامه‌ی «واشنگتن پست» ارائه شده بیش از ۹۵ درصد حجم ارتباطات نیروهای نظامی آمریکا ازطریق شبکه‌های غیرنظامی انجام‌می‌پذیرد و دست‌کم ۱۵۰ هزار دستگاه رایانه‌ی نظامی مستقیماً به شبکه‌ی اینترنت وصلند. در سال ۱۹۹٤ سازمان سیستم‌های اطلاعات دفاعی[1] گروهی از نفوذگران داخلی را مأمور دستبرد به رایانه‌های نظامی کرد. این عده موفق شدند به ۸۸ درصد از قریب به ۹۰۰۰ دستگاه رایانه‌ای که مورد حمله قرار گرفت رخنه کنند و جالب آن‌که تنها ٤ درصد از موارد رخنه، لو رفت. بنابراین، با توجه به ثبت ۳۵۰ فقره دستبرد واقعی در سال ۱۹۹٤ و با فرض این‌که تنها ٤ درصد از دستبردها افشا شده، رایانه‌های نظامی آمریکا در این سال به‌طور تخمینی مورد ۳۰۰ هزار فقره دستبرد قرار گرفته‌اند (Gray, 1997).

در بازی‌های جنگی مخصوص جنگ‌های سیبرنتیک که در سال ۱۹۹۵ طراحی گردید هدف دشمن فرضی (بنیادگرایان مسلمانی که تعدادی نفوذگر اروپایی را به خدمت گرفته‌اند) آن بود که با کمک ویروس‌ها و کرم‌واره‌ها[2] وعوامل نفوذی نرم‌افزاری در کار قطارها و هواپیماها و بانک‌ها بی‌نظمی ایجاد کند و سپس با ایجاد اختلال در خطوط تلفن آمریکا، این کشور را به زانو در آورد. به گفته‌ی یکی از افراد بازی‌کننده: «این را دیگر نمی‌شد با بمباران

1 - Agency Systems Information Defence

۲ – worm ـ ویروسی که نحوه‌ی گسترش آن از طریق شبکه و به‌صورت رایانه به رایانه است.

منطقه‌ای رفع و رجوع کرد». البته گفتنی است کـه بمبـاران منطقـه‌ای هـیچ‌گـاه در برخـورد بـا مشکلات ژئوپولیتیک چاره‌ساز نبوده، اما این تفکر اسطوره‌ای که فناوری قادر به حـل و فصـل مسائل و مشکلات سیاسی است تفکر قدرتمندی است. به همین خاطر است که شور و شـوق جنـگ سـیبرنتیک هنـوز فـروکش نکـرده و آمریکـا بـا شـتاب در حـال بسـط و گسـترش زیرساخت‌های نظری و دیوان‌سالارانه‌ی مرسومی است که بتواننـد هرگونـه انقـلاب جدیـد و پرهزینه درعرصه‌ی امور نظامی را جوابگو باشند (Gray, 1997).

نتیجه‌گیری و جمع‌بندی

یافته‌های تحقیق در مجموع نشان می‌دهد که:

۱) فناوری اینترنت مسائل ژئوپلیتیک از جمله ژئوپلیتیک اطلاعات، ژئوپلیتیک تروریسم، جنگ پست مدرن و ... را تحت تأثیر قرار داده است و فضاها و مباحـث ژئـوپلیتیکی نو در حیطه‌ی نظام قدرت جهانی، روابط قدرت بین جناحی درون کشوری را مطرح کرده است که تحت عنوان ژئوپلیتیک فضای مجازی شناخته می‌شوند.

۲) با توجه به مباحث مطرح، مفهوم ژئوپلیتیک فضـای مجـازی منـتج از فرآینـدهای کـنش متقابل در فضای مجازی ناشی از شبکه‌ی اینترنت می‌باشد کـه کشـورها و سـازمان‌هـای موجود در صحنه‌ی رقابت‌های نظام قدرت جهانی برای نیل به اهداف خود به عنوان یک ضرورت عملکردی در عصر اطلاعات از آن بهره می‌برند. نوع رابطـه و سلسـله مراتـب نظام قدرت میان بازیگران در آن با توجه به میزان برتری فناوری و اطلاعاتی و نیز میـزان تسلط و نفوذ در فضای مجازی همراه با میزان قابلیت مانور در پیشبرد اهداف مورد نظر و سطح موفقیت در نهادینه کردن پارادایم و فضای فکری دلخواه می‌باشد.

۳) مسائل ژئوپلیتیک فضای مجازی بـر گرفتـه از محـیط واقعـی مـورد مطالعـه‌ی علـم ژئوپلیتیک همراه با ابعاد پیچیده و گسترده‌تر ناشی از کاربرد ابزار اینترنـت در محـیط عملکردی انسان می‌باشد.

٤) امروزه کشورها به عنوان عناصر تشکیل‌دهنده‌ی نظام قدرت جهانی و روابط بین‌الملل، علاوه بر عوامل و فضاهای سنتی رقابت همچون مسائل اقتصادی، نظامی و نیز رقابت بر سر کنترل بر فضای جریان‌های ارتباطی و انتقالی همچون لوله‌های انتقال انرژی نفت و گاز، خطوط زمینی ترانزیت کالا، خطوط کشتیرانی بین‌المللی و تسلط ماهواره‌ای بر تمام مناطق کره زمین ناگزیر به رقابت و سرمایه‌گذاری در فضاهای جدید ارتباطی و انتقالی همراه با خصوصیات کاملاً متمایز فضایی از لحاظ فرهنگی، اقتصادی، نظامی و پارادایم‌های فکری می‌باشند. فضای مجازی با توجه به خصوصیات ارتباطات در آن در کنترل کشورهایی خواهد بود که از لحاظ فناوری اطلاعاتی و ارتباطاتی، مسائل فرهنگی و ژئوپلیتیک اطلاعات از دیگران برتر باشند. کشور ایالات متحده آمریکا به رغم در اختیار داشتن سرورهای اینترنت در قلمرو سرزمینی خود در دره‌ی سیلیکون به عنوان یکی از نقاط راهبردی جهان تاکنون در معرض بیشترین حملات سایبری از طریق اینترنت به ارگان‌های مختلف اقتصادی و نظامی‌اش بوده است و هنوز در جستجوی ایجاد مکانیسم کارآمد برای مقابله با آن می‌باشد.

٥) با پیشرفت فناوری‌های اطلاعاتی – ارتباطی، میزان توان تأثیرگذاری یک کشور در تولید و پردازش هدفمند اطلاعات به گونه‌ای که به تولید قدرت بیانجامد، می‌تواند یک کشور را در دنیای ژئوپلیتیک اطلاعات و ارتباطات در انزوای ژئوپلیتیکی[1]، چالش ژئوپلیتیکی[2] و یا تحول ژئوپلیتیکی[3] قرار دهد.

٦) تداوم شکاف فناورانه و دیجیتالی و شکاف فناوری اطلاعات و کامپیوتر منجر به تداوم شکاف توسعه، و تقسیم جهان به دو بخش توسعه‌یافته و عقب‌مانده از این جهات می‌گردد. تداوم آن همچنین به توسعه و پایداری شکاف فقر و غنی و شکل‌گیری رابطه‌ی سلطه و زیرسلطه منجر می‌شود.

1 – geopolitical Isolation
2 – geopolitical Challenge
3 – geopolitical Evolution

۷) در جنگ‌های آینده، کشمکش بر سر اطلاعات، نقشی محوری خواهد داشت و شاید جای کشمکشی را بگیرد که در جنگ‌های گذشته بر سر دستیابی به مواضع جغرافیایی در می‌گرفت. برتری اطلاعاتی آرام آرام به صورت عرصه‌ی رقابتی نو و بسیار شدیدتر پدیدار می‌شود.

۸) موضوع و مفهوم اصلی در ژئوپلیتیک، قدرت است و همه چیز حول محور آن دور می‌زند. این قدرت در گذشته، برآمده از لوله‌ی تفنگ بود اما با ظهور پدیده‌ی افکار عمومی و ورود جهان به عصر اطلاعات و ارتباطات عمدتاً متأثر از میزان اثرگذاری بر افکار عمومی است؛ چرا که با ظهور این پدیده، دیگر سران حکومت‌ها بدون جلب نظر افکار عمومی نمی‌توانند اهداف ژئوپلیتیکی خود را به پیش ببرند (قالیباف و جنیدی، ۱۳۸۷). به عبارتی، رشد فزاینده و غیر قابل تصور فناوری و اهمیت یافتن بیش از اندازه‌ی ارزش اقتصادی و اطلاعات با تمرکز مکان‌های جغرافیایی و فشرده شدن مکان و زمان، بنیان ژئوپلیتیک اطلاعات و رسانه‌ها را ایجاد کرده است. این تحول پارادایمی نظام جدیدی از ژئوپلیتیک را ایجاد نموده که هدف آن خلاف نظام سنتی ژئوپلیتیک با گرایش تسخیر هارتلند، این بار با تسخیر فضاهای مجازی چالش اصلی قدرت‌ها در نظام نوین جهانی شده است (بای، ۱۳۸۳). بنابراین، در این نظام ژئوپلیتیکی جدید، میزان توان تسخیر فضای ذهنی انسان‌ها به عنوان اصلی‌ترین بازیگران ژئوپلیتیک، نقش ویژه‌ای در تعیین جایگاه و منزلت ژئوپلیتیکی کشورها ایفا می‌نماید و با توجه به رشد فزاینده‌ی شکاف دیجیتالی و اطلاعاتی (آن‌گونه که گالتونگ و والرشتاین اشاره می کنند) به نظر می‌رسد باید همچنان شاهد شکل فرانوینی از سلطه‌ی کشورهای شمال بر جنوب باشیم (قالیباف و جنیدی، ۱۳۸۷).

۹) کشورها در عصر فناوری اطلاعات در جنگ نرم سایبری با استفاده از فناوری‌های مبتنی بر اینترنت مانند ایمیل، وبلاگ، وب سایت و شبکه‌های اجتماعی و با تکنیک‌هایی مانند هک و نفوذ، خرابکاری و اختلال در پایگاه‌های اطلاع‌رسانی، سعی در

برتری‌جویی نسبت به دشمن یا رقیب دارند؛ موضوعی که به قلمرو مطالعاتی جدیدی در علم ژئوپلیتیک به عنوان علم رقابت قدرت‌ها تبدیل شده است.

۱۰)و در نهایت، روند سریع جهانی شدن اقتصاد جهانی و تبدیل شبکه‌های ارتباطی به سیستم‌های اطلاعات جهان‌گستر، مرزها و هویت‌های ملی را از میان نخواهد برد. به رغم برخی ادعاها، جهانی شدن به حیات جغرافیا و ژئوپلیتیک پایان نخواهد داد، بلکه نظام ژئوپلیتیکی به مراتب پیچیده‌تری را پدید خواهد آورد. درون این نظام، دولت‌های ملی با نیروها و فشارهای داخلی و خارجی ـ شامل تروریسم سایبری ـ بسیار بیشتری مواجه خواهند بود؛ بسیار بیشتر از مشکلاتِ فرا روی کشورها در پنج قرن گذشته؛ زمانی‌که لویی چهاردهم (۸۳ ـ ۱٤٦۱ میلادی) آخرین بقایای قدرت فئودالی را از بین برد و فرانسه را به عنوان نخستین نمونه‌ی یک کشور مدرن بنا نهاد.

منابع

فارسی

۱- آلبرتس، دیوید. س و دانیل. س .پاپ، (۱۳۸۵)، «***گزیده‌ای از عصر اطلاعات؛ الزامات امنیت ملی در عصر اطلاعات***»؛ ترجمه: علی علی‌آبادی و رضا نخجوانی، تهران، پژوهشکده مطالعات راهبردی.

۲- بابک، اسماعیل، (۱۳۸۸)، «***سراب نبرد نرم در بستر دموکراسی؛ واکاوی و بررسی چگونگی و چرایی کودتای ناکام مخملی در ایران***»، چاپ سوم، تهران، درک نو.

۳- بای، یار محمد، (۱۳۸۳)، «***خاورمیانه در نظریات ژئوپلیتیکی خیر و شر***»، فصلنامه جغرافیای نظامی و امنیتی، سال دوم، شماره ۱.

٤- جعفرپور، محمود، (۱۳۸۷)، «***قدرت نرم: درآمدی بر جنگ‌های رسانه‌ای و رایانه‌ای***»، مقالات برگزیده همایش بسیج و قدرت نرم، تهران، جلد یک، پژوهشکده مطالعات و تحقیقات بسیج- دانشگاه امام صادق (ع).

۵- حافظ‌نیا، محمدرضا و دیگران، (۱۳۸۵)، «***تأثیر جهانی شدن بر هویت ملی (مطالعه موردی: دانشجویان دانشگاه‌های دولتی شهر تهران)***»، فصلنامه ژئوپلیتیک، سال دوم، شماره سوم و چهارم.

٦- حافظ‌نیا، محمدرضا، (۱۳۸۵)، «***اصول و مفاهیم ژئوپلیتیک***»، مشهد، انتشارات پاپلی.

۷- حافظ‌نیا، محمدرضا و دیگران، (۱۳۸۷)، «***بسیج و ژئوپلیتیک اطلاعات***»، مقالات برگزیده همایش بسیج و قدرت نرم، تهران، جلد سوم، پژوهشکده مطالعات و تحقیقات بسیج- دانشگاه امام صادق (ع).

۸- حافظ‌نیا، محمدرضا، زهرا احمدی‌پور و مصطفی قادری حاجت، (۱۳۸۹)، «***سیاست و فضا***»، مشهد، انتشارات پاپلی.

۹- حافظ‌نیا، محمدرضا، (۱۳۹۰)، «***مفهوم‌سازی ژئوپلیتیک اینترنت و فضای مجازی***»، فصلنامه ژئوپلیتیک، سال هفتم، شماره اول.

۱۰-خان محمدی، کریم، (۱۳۸۵)، «***اسلام، غرب و رسانه‌ها***»، مجله علوم سیاسی، شماره ۳٦.

۱۱-دفتر مطالعات و توسعه رسانه‌ها، (۱۳۸۸)، «***جنگ سایبری***»، دفتر مطالعات و برنامه‌ریزی رسانه‌ها.

۱۲-دیویس، نورمن، (۱۳۹۰)، «***انقلاب اطلاعات در آیینه امور نظامی***»، ترجمه: علیرضا طیب، مجموعه مقالات انقلاب اطلاعات، امنیت و فناوری‌های جدید، پژوهشکده مطالعات راهبردی.

۱۳-رفیع، حسین، (۱۳۸۷)، «***دانشواژه ژئوپولیتیک و ژئواستراتژی در دنیای اطلاعات (با تأکید بر مورد ایران)***»، فصلنامه علوم سیاسی، شماره ۷.

۱٤-روزنا، جیمز، (۱۳۹۰)، «***فناوری‌های اطلاعات و مهارت‌ها، شبکه‌ها، و ساختارهای قوام بخش امور جهان***»، ترجمه: علیرضا طیب، مجموعه مقالات انقلاب اطلاعات، امنیت و فناوری‌های جدید، پژوهشکده مطالعات راهبردی.

۱۵-سوری جواد، (۱۳۸۵)، «***نقش فناوری‌های نوین ارتباطی در عملیات روانی***»، فصلنامه عملیات روانی، سال سوم، شماره ۱۲، تهران.

۱٦-شامحمدی، محمد، (۱۳۸۵)، «***ژئوپلیتیک اطلاعات و ارتباطات***»، فصلنامه عملیات روانی، سال چهارم، شماره چهاردهم.

۱۷-ضیایی‌پرور، حمید، (۱۳۸٦)، «***جنگ نرم ۱: ویژه جنگ رایانه‌ای***»، تهران، انتشارات ابرار معاصر.

۱۸-ضیایی‌پرور، حمید، (۱۳۸۸)، «***جنگ نرم سایبری در فضای شبکه‌های اجتماعی***»، فصلنامه وسایل ارتباط جمعی، سال بیستم، شماره ۲، شماره پیاپی ۷۷ .

۱۹-عزتی، عزت الله، (۱۳۸۰)، «***ژئوپلیتیک***»، تهران، سمت.

۲۰-فیضی، کامران و علیرضا مقدسی، (۱۳۸٤)، «***دولت الکترونیک؛ بازآفرینی دولت در عصر اطلاعات***»، تهران، انتشارات ترمه.

۲۱-قالیباف، محمدباقر و جنیدی، رضا، (۱۳۸۷)، «***ژئوپلیتیک بر بال رسانه؛ نقش عملیات روانی در بازنمایی‌های ژئوپلیتیکی***»، مجموعه مقالات برتر همایش عملیات روانی و مهندسی آینده‌پژوهی، انتشارات معاونت فرهنگی و تبلیغات دفاعی ستاد کل نیروهای مسلح.

۲۲-کاستلز، مانوئل، (۱۳۸۰)، «***اقتصاد، جامعه و فرهنگ عصر اطلاعات***»؛ پایان هزاره، ترجمه: احد عقیلیان، افشین خاکباز و حسن چاوشیان، جلد اول، تهران، طرح نو.

۲۳-کاستلز، مانوئل، (۱۳۸۵)، «***اقتصاد، جامعه و فرهنگ عصر اطلاعات***»؛ پایان هزاره، ترجمه: احد عقیلیان، افشین خاکباز و حسن چاوشیان، چاپ پنجم، جلد سوم، تهران، طرح نو.

۲٤-کانوی، مائورا، (۱۳۹۰)، «***بهره‌برداری تروریست‌ها از اینترنت و چالش‌های مدیریت فضای اطلاعات***»، ترجمه: علیرضا طیب، مجموعه مقالات انقلاب اطلاعات، امنیت و فناوری‌های جدید، پژوهشکده مطالعات راهبردی.

۲۵- کلاه مال همدانی، احمد، (۱۳۸۱)، «***مرزهای جغرافیایی تغییر می‌کنند***»، روزنامه ابرار، شماره ٤۰۳۸/ مورخ ۱۳ آبان.

۲٦-گریفیتس، مارتین، (۱۳۹۰)، «***دانشنامه روابط بین‌الملل و سیاست جهان***»، تهران، نشر نی.

۲۷-گل محمدی، احمد، (۱۳۸٤)، «***گفتمان‌های هویت‌ساز در عصر جهانی شدن (رابطه قدرت - مقاومت در بازسازی هویت ملی)***»، مجموعه مقالات همایش؛ هویت ملی و جهانی شدن، مؤسسه تحقیقات و توسعه علوم انسانی دانشگاه تهران.

۲۸-گیدنز، آنتونی، (۱۳۷۹)، «***گفتاری در باب فرایند فروریختن مرزهای ملی و بومی در جهان***»، ترجمه: ملیحه مغازه‌ای. روزنامه‌ی بهار، ۱۳۷۹/۵/۲.

۲۹-میناوند، محمد قلی، (۱۳۸۵)، «***اینترنت و توسعه سیاسی: حوزه عمومی در فضای سایبرنتیک***»، مجله پژوهش علوم سیاسی، شماره دوم، بهار و تابستان ۱۳۸۵.

۳۰-نامی، محمدحسن و شامی، ابوالفضل، (۱۳۸۹)، «***فضا بُعد چهارم قدرت***». تهران: زیتون سبز.

۳۱-نای، جوزف، (۱۳۸۷)، «***قدرت در عصر اطلاعات؛ از واقع‌گرایی تا جهانی شدن***»، ترجمه: سعید میرترابی، تهران، پژوهشکده مطالعات راهبردی.

۳۲-نای، جوزف، سخنرانی «***قدرت نرم و دیپلماسی عمومی در قرن ۲۱***»، سخنرانی جلسه آغازین پارلمانی شورای انگلستان، ۲۰ ژوئن ۲۰۱۰، سایت www.strategicreview.org.

۳۳-هاگت، پتر، (۱۳۷۳)، «***جغرافیا: ترکیبی نو***». ترجمه: دکتر شاهپور گودرزی‌نژاد. انتشارات سمت.

انگلیسی

34- Adams. C Paul (1997), "***Cyber Space and Virtual Places***", New York, The Geographical Review, 87 (2).

35- Cohen, Bernard, (2009), "***Geopolitics; The Geography of International Relations***", second edition, Rowman & Littlefield Publisher.

36- Deibert. J Ronald, (2009), "***The Geopolitics of Internet Control***", The Routledge Handbook of Internet Politics, Edited by Andrew Chadwick and Philip N. Howard, Routledge.

37- Goodman E. Seymour and jessica C. Kirk, Megan H. Kirk (2007), "***Cyberspace as a medium for terrorist***", Science Direct, Tecnological Forecasting & Sosial change, 74.

38- Gray, Chris Hables, (1997), "***War Postmodern The New Politics of Conflict***", Routledge.

39- Jordan, Tim (2003), "***Cyberpower: The culther and Political of Cyberspace and the internet***", london and Newyork, Tylore & Francis e-Library.

40- Racicot, Macheal and Marek S. Hayes, Alec R. Szibbo, Pierre trudel (1998), "***The cyberspace is not a " no law land" a study of liability for content circulating on the internet***", Computer law & securits Report Vol.14 no. 2.

41- Saunders. A, Rabert (2009), "***Wiring the Second World: The Geopolitics of Information and Communications Technology in Post-Totalitarian Eurasia***", USA, Farmingdale State College, www.russian-cyberspace.org, papers 1-٦

42- Shibusawa, Hiroyuki (2000), "***Cyberspace And Physical in an Urban Economy***", Japan, Toyohoshy University of Tecnology, Regional Science.

مجله سیاست دفاعی
سال بیستم، شماره ۷۹، تابستان ۱۳۹۱

پروتکلی دفاعی جهت امن‌سازی پیام‌های کوتاه در مناطق عملیاتی

شهریار محمدی [۱]
فرزاد توکلی [۲]

تاریخ دریافت مقاله: ۱۳۹۱/۰۱/۲۸
تاریخ تأیید مقاله: ۱۳۹۱/۰۳/۰۹
صفحات مقاله: ۲۱۱ – ۱۸۳

چکیده:

یکی از مشکلات عمده امنیتی، تبادل پیام در مناطق عملیات نظامی، دسترسی و رمزگشایی پیام توسط گیرنده مورد نظر و همچنین جلوگیری از دسترسی‌های غیر مجاز توسط مهاجمین در مسیر کانال تبادلی می‌باشد. روش‌های معمول رمز نگاری پیام‌های نظامی عمدتاً از امکان دستیابی دشمن به پیام حین ارسال، مصون نمی‌باشند. واژه رمزنگاری مبتنی بر موقعیت مکانی[۳]، در یک تعریف ساده به مفهوم روشی از رمزنگاری است که متن رمز شده فقط در یک محل خاص قابل رمزگشایی است. این الگوریتم‌ها جایگزین روش‌های سنتی رمزنگاری نیستند بلکه یک لایه امنیتی اضافی فراتر از آنچه رمزنگاری‌های سنتی فراهم می‌کنند، ایجاد می‌کنند. در این مقاله، یک پروتکل جدید رمزنگاری مبتنی بر موقعیت مکانی پیشنهاد شده است که امکان تبادل اطلاعات رمز شده را به صورت کاملاً امن، مناسب مناطق عملیاتی در اختیار کاربران قرار می‌دهد. گرچه تمرکز مدل رمزنگاری بر روی پیام کوتاه تبیین شده اما مدل پیشنهادی برای رمزنگاری هر نوع داده مانند صدا و تصویر و ... قابل تعمیم می‌باشد. یکی از چالش‌های پیش روی صنایع با فناوری بالا علی‌الخصوص در صنایع نظامی، تضمین استفاده از ادوات نظامی در یک منطقه خاص مثلاً در سطح یک کشور می‌باشد. در این مدل پیشنهادی می‌توان کلید مجوز راه اندازی یک سیستم نظامی و یا کلید رمزگشایی یک پیام محرمانه مانند دستورالعمل‌های دفاعی و یا نظامی را با موقعیت مکانی استخراج شده از سیستم موقعیت یاب جهانی[۴] تلفیق کرده و یک لایه امنیتی دیگر به سطوح امنیتی پیش بینی شده برای سیستم اضافه نمود. به طور کلی ویژگی مدل پیشنهادی در سه موضوع قابل طرح است:

۱- استادیار گروه مدیریت فناوری اطلاعات (IT)، دانشکده مهندسی صنایع، دانشگاه صنعتی خواجه نصیرالدین طوسی.
۲- پژوهشگر مرکز مطالعات دفاعی و امنیت ملی، گروه مدیریت فناوری اطلاعات (IT)، دانشکده مدیریت، دانشگاه تهران.
3 – Geo-encryption
4 – GPS

۱- استفاده از الگوریتم‌های سبک رمزنگاری و درهم سازی منتج از پروژه eSTREAM-Profile (software) *۲- عدم استفاده از الگوریتم رمزنگاری نامتقارن به دلیل ردپا و اثر[1] بالا و نیاز به مدیریت کلید ۳- استفاده از الگوریتم بهینه شده دفی هلمن[2] به منظور تولید کلید نشست با استفاده از یک رمز عبور کوتاه.*

* * * * *

واژگان کلیدی

رمزنگاری، پیام کوتاه، موقعیت مکانی، رمز دنباله‌ای، توابع درهم ساز، سرویس‌های مبتنی بر موقعیت.

مقدمه

رمزنگاری مبتنی بر موقعیت، امنیت را مناسب با مناطق عملیات نظامی از طریق اختلاط موقعیت مکانی، زمان و حتی سرعت با استفاده از فرآیندهای رمزنگاری و رمزگشایی ارتقا می‌بخشد. اما از منظر رمز نگاری این امر به سادگی محقق نمی‌شود و با مسائلی همچون تولید و انتقال کلید درگیر است.

خط مشی رمزنگاری مبتنی بر موقعیت، بر اساس الگوریتم‌های رمزنگاری و پروتکل‌هایی بنا نهاده شده است به نحوی که یک لایه امنیتی اضافی فراتر از آن‌چه رمزنگاری مرسوم فراهم می‌کند، ایجاد می‌کند. این خط مشی اجازه می‌دهد داده‌ها در مکان(ها) یا محدوده (ها) ی مشخصی رمزگذاری و رمزگشایی شوند مثلاً در محدوده یک منطقه نظامی. مضافاً به این‌که می‌توان محدودیت زمانی را نیز همانند محدودیت مکانی به سیستم اعمال نمود یعنی پیام‌ها در محدوده زمانی و مکانی خاص رمزگشایی شوند. این فناوری هم در ادوات ثابت و هم در ادوات همراه مانند موبایل کاربرد داشته و طیف وسیعی از داده‌های به اشتراک گذاشته شده و راهبردهای انتشار و توزیع داده را پشتیبانی می‌کند(Scott & Denning, 2003).

1 – Footprint
2 – Diffe-Hellman

نکته مهمی که در این نوع رمزنگاری باید همواره مورد توجه باشد تمهیداتی است که جلوی عملیات ضد امنیتی مهاجم را در خصوص میانبر زدن ویژگی‌های مبتنی بر موقعیت بگیرد.

از سوی دیگر طی این سال‌ها الگوریتم‌های متعددی برای امنیت تبادل اطلاعات مطرح شده است، از الگوریتم‌های رمزنگاری کلید متقارن و نامتقارن گرفته تا رمزنگاری دنباله‌ای و بلاکی. اما این روش‌ها مستقل از مکان می‌باشند یعنی فرستنده پیام رمز شده قادر به محدود کردن مکان گیرنده برای رمزگشایی پیام نمی‌باشد. اگر الگوریتم و یا پروتکلی طراحی شود که این قابلیت را فراهم آورد برای افزایش امنیت داده در فضای انتقال بی سیم که به صورت عمده‌ای در مناطق عملیات نظامی مورد استفاده‌اند، بسیار کارآمد خواهد بود.

این لایه امنیتی در مواردی که لازم است پیامی فقط در محدوده خاص جغرافیایی قابل رمزگشایی باشد، بسیار کارا خواهد بود. مثلاً در صنایع نظامی برای حفظ امنیت پیام‌ها در جریان عملیات نظامی علیه دشمن، با استفاده از این طرح اول نیاز به افشای پیام قبل از موعد مقرر نبوده و دوم در مکانی خارج از محدوده عملیات پیام قابل رمزگشایی نیست. علاوه بر این، با استفاده از این طرح می‌توان بر دغدغه استفاده از ادوات نظامی علی‌الخصوص با فناوری بالا در خارج از منطقه مورد توافق فروشنده و خریدار فائق آمد.

در مدل پیشنهادی از پارامترهای موقعیت مکانی (طول/عرض جغرافیایی) به عنوان کلید رمزگذاری داده استفاده شده است. البته دستگاه‌های موقعیت یاب جهانی علاوه بر این دو پارامتر، مقادیر دیگری مانند سرعت، زمان و ارتفاع را نیز در اختیار می‌گذارند که می‌توان از آن‌ها برای محدود کردن شرایط رمزگشایی استفاده نمود مثلاً رمزگشایی در موقعیت منطقه‌ای خاص و در محدوده زمانی مشخص.

پارامترهای رمزگشایی (طول/ عرض جغرافیایی) توسط دستگاه موقعیت یاب جهانی استخراج شده و پیام رمز شده فقط در همان مکان مورد انتظار قابل رمزگشایی خواهد بود. اما از آنجایی‌که دقت این دستگاه‌ها یکسان نبوده و علاوه بر آن در شرایط جوی مختلف، دقت آنها متفاوت می‌باشد، نمی‌توان انتظار داشت که دقیقاً در یک نقطه مشخص برای رمزگشایی

قرار گرفت. از اینرو مسافتی را به عنوان بازه قابل اغماض در نظر گرفته تا پیام در آن محـدوده قابل رمزگشایی باشد.

رمزنگاری مبتنی بر موقعیت[1]

در یک تعریف ساده به روشی از رمزنگاری است که متن رمز شده فقـط در یـک محـل خاص قابل رمزگشایی است. اگر تلاشی برای رمزگشایی داده‌های رمز شـده در مکـانی دیگـر صورت پذیرد فرایند رمزگشایی با شکست مواجه شـده و اطلاعـاتی را در خصـوص پیـام بـر نمی‌گرداند. تجهیزاتی که برای رمزگشایی استفاده مـی‌شـود موقعیـت مکـانی را بـا اسـتفاده از حسگرهای موقعیت یاب مانند یک سیستم موقعیت یاب جهانی و یا دیگر سیستم‌های موقعیت یاب مبتنی بر فرکانس رادیویی تعیین می‌کنند(Scott & Denning, 2003) .

سیستم موقعیت یاب جهانی یک سیستم ناوبری مبتنی بر ماهواره بوده کـه از شـبکه‌ای از ۲٤ ماهواره در مدار زمین که متعلق به وزارت دفاع آمریکاست، تشکیل شده است. این سیستم در اصل برای کاربردهای نظامی بوده است اما در سال ۱۹۸۰ توسط دولت امریکا برای استفاده غیرنظامی در اختیار قرار گرفت. البته به دلیل سیاسـت وزارت دفـاع آمریکـا در خصـوص «در دسترس بودن انتخابی»[2] که از طریق تضعیف توان سیگنال‌های ماهواره‌ای به منظـور مقابلـه بـا دشمن در استفاده از سیگنال‌های پرقدرت دستگاه‌های موقعیت یاب جهانی، تـا مـاه مـی سـال ۲۰۰۰ به انجام می‌رسید، عملاً این دستگاه‌ها برای کاربردهای عمومی به‌کار نمی‌رفت. اما پـس از این تاریخ استفاده از دستگاه‌های موقعیت یاب جهانی دستی، برای ناوبری در فواصـل چنـد متر امکان پذیر گردید.

با ظهور فناوری سیستم موقعیت یاب مکانی جهانی تفاضـلی[3]، دسترسـی بـه دقـت‌هـای کمتر از یک متر نیز محقق گردیده است. امروزه گیرنده‌های موقعیت یـاب مکـانی در زنـدگی روزمره ما عمومیت پیدا کرده‌اند مثلاً در سیستم ناوبری خـودرو، هوانـوردی و در کاربردهـای

1 – Geo-encryption
2 – Selective Availability (SA)
3 – Differential GPS (DGPS)

متعدد ورزشی مانند کوه‌نوردی، شکار و غیره. اگرچه در گذشته این سیستم به عنوان یک دستگاه جانبی از طریق کابل و یا بلوتوث به دستگاه‌های تلفن همراه متصل می‌شد اما امروزه به جزئی لاینفک از آن بدل شده است.

مروری بر فعالیت‌های انجام شده

فراگیری ادوات مکان یاب باعث اهمیت‌بخشی به سرویس‌های مبتنی بر موقعیت گردیده است. در سال‌های اخیر این سرویس به عنوان فیلدی از محاسبات همراه گسترش یافته است. تعریف ساده‌ای از سرویس‌های مبتنی بر موقعیت توسط انجمن GSM که کنسرسیومی از ۶۰۰ اپراتور می‌باشد به شرح ذیل ارائه شده است: »سرویس‌های مبتنی بر موقعیت، سرویس‌هایی هستند که از موقعیت هدف برای ارزش افزوده به سرویس استفاده می‌شود« در اینجا منظور از هدف همان موجودیتی است که تعیین موقعیت می‌شود و لزوماً استفاده کننده از سرویس نمی‌باشد (Kupper, 2005).

سرویس‌های مبتنی بر موقعیت به چهار دسته قابل تقسیم می‌باشند: سرویس‌های اورژانسی مانند هشدارهای امنیتی، امنیت اجتماعی و سرویس‌های اطلاعاتی مانند اخبار، آب و هوا، خرید و ...، سرویس‌های ردگیری مانند ردگیری نظامی، ره گیری کالا و ... و در نهایت سرویس‌های سرگرمی مانند بازی، موزیک و غیره (Liao & Chao, 2008).

یکی از کاربردهای اولیه رمزنگاری مبتنی بر موقعیت در خصوص مسئله حق نشر[1] فیلم‌های دیجیتال مطرح شده است. این ایده توسط دنینگ و اسکات[2] مطرح شد و به عبارتی می‌توان گفت مفهوم رمزنگاری مبتنی بر موقعیت اولین بار توسط این دو نفر ارائه گردید. در این طرح با استفاده از کلید رمزنگاری مبتنی بر موقعیت، امکان نمایش فیلم در سالن‌های سینمای مجاز در محدوده مکانی خاص امکان پذیر گردید. البته لازمه این کار به‌کارگیری

1 – Copyright
2 – L. Scott, D. Denning

ویدئو پروژکتورهای دیجیتال بوده که قابلیت اتصال به شبکه‌های ارتباطی را در خود دارند (Scott & Denning, 2003).

بر اساس این ایده اولیه کاربردهای مختلفی برای این تکنیک مطرح گردید. لیائو و چائو[1] مدلی برای رمزنگاری پیام مبتنی بر موقعیت کاربران تلفن همراه ارائه کردند. الگوریتم ارائه شده توسط آن‌ها LDEA[2] نامیده شده و بر اساس رمزنگاری هیبرید عمل می‌کرده است یعنی برای رمزنگاری پیام از الگوریتم کلید متقارن و برای تبادل کلید آن از رمزنگاری کلید نامتقارن استفاده شد (Liao & Chao, 2008).

ژانگ[3] برای تصدیق هویت و تحقق امنیت تبادل اطلاعات بین گره‌های شبکه‌های حسگر استفاده از موقعیت مکانی گره‌های مجاور را مطرح کرد. در طرح دیگری یک مدل به نام LEDS[4] برای امنیت تبادل اطلاعات در گره‌های شبکه‌های حسگر مبتنی بر موقعیت جغرافیایی گره ارائه گردید (Ren et al., 2008).

در شبکه اختصاصی حمل و نقل[5] یان و الاریو[6] مدلی برای تحقق محرمانگی تبادل اطلاعات و تصدیق هویت ارائه کردند که در آن اطلاعات موقعیت مکانی شامل مکان، سرعت و زمان به عنوان کلید رمزنگاری پیام استفاده می‌شد. در این مدل نیز از دو مرحله رمزنگاری/رمزگشایی استفاده شده است یکی برای پیام و دیگری برای انتقال کلید در کانال غیر امن (Yan & Olariu, 2009).

کیاو[7] از دانشگاه استنفورد یک پروتکل امنیتی مبتنی بر سیگنال Loran ارائه کرد. Loran یک سیستم ناوبری فرکانس پایین می‌باشد که در مقابل دخل و تصرف و استفاده غیر مجاز

1 – H.C. Liao, Y.H. Chao
2 – Location-dependent data encryption algorithm
3 – Y. Zhang
4 – Location-aware End-to-end Data Security
5 – Vehicular adhoc network (VANET)
6 – G. Yan, S. Olariu
7 – D. Qiu

مقاوم می‌باشد. این پروتکل به عنوانTESLA [1] ارائه و پیاده سازی شد. نتایج این تحقیق نشان داد که پروتکل مذکور در مقابل حملات جعل هویت[2] موقعیت مکانی بسیار مستحکم و قوی عمل می‌کند (Qiu, 2007).

مدل پیشنهادی برای رمزنگاری مناسب در مناطق عملیاتی

پروتکل پیشنهادی در این نوشتار برای تحقق رمزنگاری پیام کوتاه تبیین می‌شود اما با توجه به ساختار مدل قادر به تعمیم به انواع مختلف انتقال داده می‌باشد مثلاً به‌جای انتقال پیام کوتاه می‌توان رمزنگاری را بر روی یک فایل حاوی پیام انجام داد. پروتکل رمزنگاری پیام کوتاه مبتنی بر موقعیت مکانی از چهار ماژول اصلی به شرح ذیل تشکیل شده است:

- ماژول استخراج پارامترهای موقعیت مکانی؛
- ماژول تولید کلید؛
- ماژول رمزنگاری/رمزگشایی؛
- ماژول مولد پیام کوتاه رمز شده.

ماژول استخراج پارامترهای موقعیت مکانی

بر اساس تعریف NMEA [3] فرمت مختصات بدست آمده از گیرنده‌های موقعیت یاب جهانی بر اساس استاندارد WGS84 [4] به‌جای درجه، دقیقه، ثانیه به صورت درجه، دقیقه با اعشار می‌باشد. فرمت نمایش اطلاعات در این استاندارد به شکل HDD(D)MM.MMMM است که در آن H نمایانگر نیمکره و D زاویه بر حسب درجه و M زاویه بر حسب دقیقه می‌باشد. یعنی مقدار ثانیه با تبدیل به دقیقه در قالب یک عدد با ممیز شناور نمایش داده می‌شود. واضح است که محدوده قابل قبول برای عرض جغرافیایی [90.0,90.0-] بوده که در عرض‌های شمالی مثبت و در عرض جنوبی منفی است. این محدوده برای طول جغرافیایی [180.0,180.0-]

1 – Timed Efficient Stream Loss-tolerant Authentication
2 – Spoofing attacks
3 – National Marine Electronics Association
4 – World geodetic system 1984

می‌باشد کـه بـرای شـرق مثبـت و بـرای غـرب منفـی مـی‌باشـد. مـثلاً در اسـتاندارد مـذکور E12012.5638 به معنی 121 درجه و 12.5638 دقیقه طول جغرافیایی شـرقی و N1202.3452 به معنی 12 درجه و 2.3452 دقیقه عرض جغرافیایی شمالی می‌باشد.

خوشبختانه برای استفاده از این پارامترها به عنوان کلید، واسط برنامه نویسـی کـاربردی[1] لازم تحـت عنـوان JSR 179 در محـیط J2ME وجـود دارد(Mahmoud, 2004) و از طریـق آن علاوه بر استخراج پارامترهای مکانی امکاناتی برای تبدیل انواع مختصات به یکدیگر در اختیار برنامه نویس قرار دارد. برای اسـتفاده از پارامترهـای موقعیـت مکـانی بـه منظـور تولیـد کلیـد رمزنگاری/ رمزگشایی ابتدا مقادیر طول و عرض جغرافیایی بدست آمـده از گیرنـده موقعیـت یاب جهانی که به فرمت WGS84 می‌باشد به فرمت درجه تبدیل می‌گردند. البته برای رهایی از مقادیر اعشاری دو اقدام به شرح ذیل صورت می‌گیرد:

- تبدیل به ثانیه

$$lat_s = lat_d * 3600 + lat_m * 60 + lat_s \quad (۱)$$

- استفاده از دو رقم اعشار در ثانیه و تبدیل آن به عدد صحیح

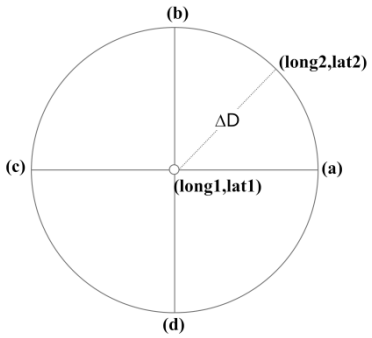
$$lat_s = lat_s * 100 \quad (۲)$$

عملیات مذکور برای طول جغرافیایی نیز محاسبه می‌شود. مقادیر مختصات بدست آمـده از روابط فوق بر حسب درجه می‌باشد اما محدوده رمزگشایی ΔD بازه قابل قبول بـرای تعیـین محدوده رمزگشایی) بر حسب متر در نظر گرفته شده اسـت. بـرای تبـدیل ایـن دو واحـد بـه یکدیگر می‌توان از رابطه فاصله دو نقطه بر روی کره زمین (Spherical law of cosines) استفاده نمود. با توجه به اینکه در این رابطه مقدار فاصله مشخص است می‌توان مختصات دوم که در فاصله ΔD از نقطه اولیه رمزنگاری را محاسبه نمود.

$$\Delta D = \text{acos}(\sin(lat1) * \sin(lat2) + \cos(lat1) * \cos(lat2) * \cos(long2 - long1)) * R \quad (۳)$$

1 – API (Application Programming Interface)

که در آن R=6371Km و شعاع متوسط زمین است. با توجه به شکل شماره‌ی (۱) نقـاطی که به فاصله ΔD از نقطه اصلی مورد هدف رمزگذاری قرار دارنـد بـر روی دایـره‌ای بـه مرکـز (long1,lat1) و شعاع ΔD قرار دارند.



شکل شماره‌ی ۱ – مختصات نقاط در محدوده‌ی نقطه هدف

نکته‌ی مهم در خصوص استفاده از پارامترهای موقعیت مکانی در تولید کلیـد اینجاسـت که اگر این مقادیر به طور مستقیم در فرآیند تولید کلید مورد استفاده قرار گیرند در آن صـورت احتمال تولید کلید یکسان بسیار پایین می‌آید چرا که مثلاً بـا ۰.۰۱ ثانیـه انحـراف از موقعیـت اصلی کلید جدیدی تولید می‌شود که امکان رمزگشایی را نمی‌دهد. از اینرو با اسـتفاده از ΔD و روابط ٤ و ٥ ، مقادیر را نرمالیزه کرده و بـه عنـوان پـارامتر تولیـد کلیـد مـورد اسـتفاده قـرار می‌دهیم. در هنگام رمزگشایی کافی ست علاوه بر نقطه مرکزی یک واحـد قبـل و بعـد از هـر مختصات را نیز وارد الگوریتم رمزگشایی کنیم یعنی اگر در محدوده نقطه مرکزی قرار داشـته باشیم در بدترین شرایط حداکثر با اعمال ۵ رمزگشایی به کلید صحیح دسترسی خواهیم یافـت و پیام رمزگشایی خواهد شد. نحوه محاسبه این ۵ نقطه به شرح ذیل می‌باشد:

$$\P lat_{k0} = \left\lfloor \frac{lat_{s0}}{\Delta D} \right\rfloor , long_{k0} = \left\lfloor \frac{long_{s0}}{\Delta D} \right\rfloor .$$

$$\P a \left| \begin{matrix} long_{k0}+1 \\ lat_{k0} \end{matrix} , b \right| \begin{matrix} long_{k0} \\ lat_{k0}+1 \end{matrix} , c \left| \begin{matrix} long_{k0}-1 \\ lat_{k0} \end{matrix} , d \right| \begin{matrix} long_{k0} \\ lat_{k0}-1 \end{matrix} .$$

اگر به‌جز طول و عرض جغرافیایی عوامل محدودکننده‌ی دیگری مانند زمـان و محـدوده زمانی رمزگشایی پیام نیز مورد نظر باشد باید عملیاتی مشابه برای نرمـالیزه کـردن پارامترهـا و آماده سازی برای استفاده به عنوان پارامتر تولید کلید انجام پذیرد. مثلاً اگـر بخـواهیم پیـام در محدوده زمان (تاریخ و ساعت) خاصی قابل رمزگشایی باشد باید با اسـتفاده از بـازه‌ی زمـانی پارامترهای ساعت و تاریخ را نرمالیزه کرد و سپس به عنوان پارامتر تولید کلید استفاده نمود.

تولید کلید

اگر طول و عرض جغرافیایی به تنهایی به عنوان پارامترهای تولید کلید رمزنگاری انتخاب شوند تعداد کلیدهای ممکن به اندازه کل مساحت زمین یعنی $5.11 * 10^{14} m^2$ خواهـد بـود. اگـر بـر اسـاس محدوده مساحت محدوده مکانی احتمال شکستن کلید را محاسبه کنیم این مقدار برابر خواهد بود با

$$P = \frac{\pi * \Delta D^2}{5.11 * 10^{14}}. \qquad (٤$$

مثلاً اگر $\Delta D = 25m$ فرض شود احتمال شکستن کلید برابر است با :

$$P = \frac{\pi * 25^2}{5.11 * 10^{14}} = \frac{1}{2.6 * 10^{11}}. \qquad (٥$$

بدتر از همه این‌که اگر بخواهیم رمزنگاری را در محیط واقعی انجام دهیم این احتمال بیشـتر هم خواهد شد چرا که حدود ۸۰٪ مردم بر روی ۳٪ خاک زمین زندگی می‌کنند بنابراین :

$$P = \frac{\pi * 25^2}{5.11 * 10^{14} * 0.03} = \frac{1}{7.8 * 10^{9}} \qquad (٦$$

که نشانگر این است که کلید خیلی مستحکمی نیست. از اینرو نیاز بـه یـک کلیـد اضـافی است که در هر نشست به صورت اتفاقی تولید شده و به همراه بقیه پارامترها در فرآیند تولیـد کلید نهایی شرکت کند.

تولید کلید نشست

یکی از روش‌های تولید کلید نشست، تولید یک کلید تصادفی (Kc) در سمت رمز کننده پیـام و ارسال به صورت امن به سمت گیرنده پیام می‌باشد. با توجه به فقدان کانال امـن جهـت انتقـال

کلید نشست، اغلب از الگوریتم‌های کلید نامتقارن بـرای حفـظ محرمـانگی کلیـد مـذکور اسـتفاده می‌شود(Liao & Chao, 2008) . این مدل که اغلب به عنوان مدل هیبریـد(Scott & Denning, 2003) از آن یاد می‌شود برای رمزنگاری پیام از الگوریتم رمزنگاری متقارن و برای انتقال کلیـد از رمزنگـاری نامتقارن استفاده می‌کند. اما دو اشکال عمده بر این مدل وجود دارد که عبارتند از:

- سرعت نسبتاً پایین در مقایسه با الگوریتم‌های رمزنگاری کلید متقارن و همچنین نیاز به توان محاسباتی بالا در برنامه‌های کـاربردی کـه از ایـن نـوع رمزنگـاری اسـتفاده می‌کنند (Lisonik & Drahansky, 2008).
- مشکل مدیریت کلید خصوصی. در عمل اکثر حملات انجام شده بـر روی سیسـتم‌هـای رمزنگاری با کلید عمومی، به جای تمرکز بر روی الگوریتم‌هـای رمزنگـاری ، بـا هـدف نفوذ به سیستم مدیریت کلید انجام می‌شود (RSA Laboratories, 2000) . کلید خصوصـی باید در سمت دارنده کلید مثلاً در گوشی تلفن همراه ذخیره شود و هیچ تضمینی وجـود ندارد که ذخیره کلید بر روی دستگاه موبایل امن باشد؛ چرا که ممکن اسـت بـه راحتـی دزدیده شده یا از طریق بلوتوث هک شود. کلید خصوصی در دستگاه همراه می‌توانـد از طریق تکنیک ذخیره سازی فایل در JAR [1] و یا ذخیره سازی رکورد[2] در RMS [3] نگهداری شود (Rice & Zhu, 2009) . ذخیره سـازی فایـل در JAR اشـاره بـه ذخیـره سـازی کلیـد خصوصی در فایل برنامه کاربردی JAR در کنار فایل‌های کـلاس بسـته برنامـه کـاربردی دارد. ذخیره سازی رکورد در RMS اشاره به استفاده از زیر سیستم MIDP [4] در اسـتاندارد J2ME [5] دارد (Giguere, 2004) . متأسفانه ابزارهای مجانی زیادی وجود دارند که قادر بـه استخراج کد منبع[6] فایل‌های JAR و ویرایش فایل‌های کلاس می‌باشـند؛ ضـمناً ابزارهـای ویرایش HEX بسیاری وجود دارند که قادر بـه اسـتخراج کلیـد از فایـل JAR مـی‌باشـند.

1 – Java ARchive
2 – Record Stored
3 – Record Management System
4 – Mobile Information Device Profile
5 – Java 2 Mobile Edition
6 – Decompile

به‌علاوه داده‌های دودویی به راحتی از RMS قابل استخراج می‌باشند. برای تحقق امنیت بیشتر می‌توان از امکانات MIDP 2.0 استفاده کرد که به دستگاه تلفن همراه اجازه تصدیق امضای دیجیتال نصب شده بر روی فایل‌های JAR را می‌دهد. در این روش گواهی کپسوله شده با فایل JAR قادر به تصدیق محتویات فایل بوده و از این طریق می‌توان از حملات مرد میانی[1] جلوگیری به عمل آورد(Lo et al., 2008).

- از این رو، برای اضافه کردن فاکتور ثانویه‌ای برای تصدیق هویت و مقابله با لو رفتن کلید خصوصی در هنگام دزدیده شدن گوشی می‌توان از یک رمز (PIN) استفاده کرد. Pin رمزی است که در صورت مراجعه فیزیکی کاربر به رمز کننده پیام مبتنی بر موقعیت، برای نصب برنامه کاربردی رمزگشا انتخاب کرده و فقط خود او و رمز کننده پیام از آن اطلاع دارند و به هیچ عنوان بر روی دستگاه گوشی همراه کاربر ذخیره نمی‌شود. در صورتیکه مراجعه فیزیکی در کار نباشد قبل از ارسال اولین پیام رمز شده مبتنی بر موقعیت، از طریق یک کانال امن مانند ارسال پستی و یا مکالمه تلفنی این رمز بین طرفین تبادل می‌شود. اما همان‌طور که گفته شد این رمز بر روی دستگاه گوشی همراه کاربر ذخیره نمی‌شود و باید به ذهن کاربر سپرده شود. از این‌رو، نمی‌تواند از پیچیدگی زیاد و یا طول زیاد برخوردار باشد و این چالشی در خصوص استفاده از *Pin* به عنوان کلید رمزگذاری می‌باشد.
- در مدل پیشنهادی در این نوشتار برای غلبه بر این مشکل از نسخه‌ای تغییر یافته از روش SPEKE[2] که توسط جابلون[3] ارائه شد(Jablon, 1996)، استفاده شده است. این روش برای تصدیق هویت و برپایی کلید نشست از طریق یک کانال نا امن با استفاده از یک

1 – Man-in-the-middle
2 – Simple password exponential key exchange method
3 – D.P. Jablon

رمز کوتاه و بدون نگرانی از ریسک حمله مبتنی بر واژه نامه[1] بنا نهاده شده است. پایه و اساس این روش همان مدل تبادل کلید دفی هلمن[2] است با دو تفاوت :

- الگوریتم دفی هلمن به خودی خود تصدیق هویت را تأمین نمی‌کند از اینرو نسبت به حمله مردمیانی آسیب پذیر است اما مدل SPEKE به صورت انتخابی قادر به انجام این کار می‌باشد.
- در SPEKE بجای استفاده از مقدار پایه ثابت (g) دفی هلمن ، از یک تابع (*f*) که مقدار رمز (Pin) را به یک پایه برای توان رسانی آماده می‌کند، استفاده می‌شود.

همان‌طور که تشریح شد اگر مرحله تصدیق هویت را از SPEKE حذف کنیم مرحله اول تولید کلید تقریباً شبیه الگوریتم دفی هلمن می‌باشد. پارامترهای تولید کلید نشست در این الگوریتم به شرح ذیل است :

جدول شماره‌ی ۲ – پارامترهای الگوریتم دفی هلمن

pin	رمز توافق شده اولیه بین طرفین
p	یک عدد اول بزرگ
f(pin)	تابعی که Pin را به مقدار مناسب پایه دفی هلمن تبدیل می‌کند
R_A,R_B	اعداد تصادفی انتخاب شده توسط طرفین
Q_A,Q_B	مقادیر نمایی محاسبه و ارسال شده توسط طرفین
H(m)	تابع درهم ساز (Hash)
K_C	کلید نشست تولید شده

همان‌طور که در شکل شماره‌ی (۲) نشان داده شده است در طرح ساده این الگوریتم (بدون تصدیق هویت)، فقط به تبادل دو پیام برای تولید کلید نشست نیاز است. با انتخاب تابع مناسب f مثلاً به شکل زیر می‌توان از حمله مرد میانی به شکل موثری جلوگیری کرد (Hallsteinsen et al., 2007):

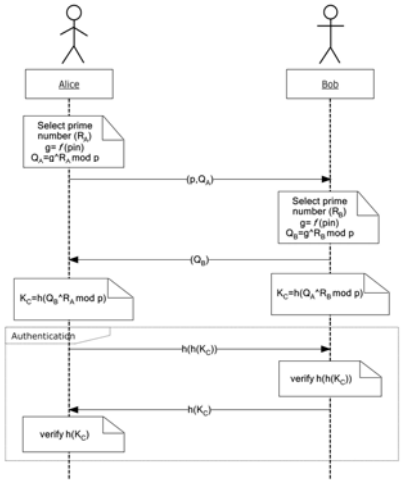
$$g = f(pin) = hash(pin)^2 \cdot \qquad (۷$$

1 – Dictionary attack
2 – Diffie-Hellman

ترکیب و درهم سازی

پس از آماده شدن پارامترهای تولید کلید و خروج از مرحله قبل، کلیه پارامترهـای مولـد کلید شامل مقادیر نرمالیزه شده طول/عرض جغرافیایی، محدوده فاصله (ΔD و کلید نشسـت (K_C) به یکدیگر الحاق شده و نتیجه آن به یک تابع درهم ساز سبک داده می‌شود تا عـلاوه بـر تولید کلید با طول یکسان، استخراج مختصات مکانی از کلید لو رفته امکان پذیر نباشد.

در سال‌های اخیر، به دنبال پیشرفت‌های حاصل شده در تجزیه و تحلیـل توابـع چکیـده ساز، نیاز به توابعی جدید و امن‌تر افزایش یافته است. یکی از نتـایج ایـن نیـاز مسـابقه SHA-3 می‌باشد که توسط NIST [1] بنیان گذاری شده است. ٦٤ پیشنهاد در مسابقه به ثبت رسـید کـه از بین آن‌ها ۵۱ عدد برای ارزیابی در دور اول مسابقه پذیرش شـدند. بعـد از حـدود یـک سـال لیست کاندیدها در مرحله دوم به ١٤ عدد کاهش یافـت و در دسـامبر ۲۰۱۰، ۵ عـدد[2] از ایـن توابع به عنوان فینالیست انتخاب شدند.



شکل شماره‌ی ۲ – Sequence Diagram **تولید کلید نشست در** SPEKE

1 – National Institutes for Standards and Technology
2 – Blake,Grostl, JH,Keccak and Skein

در میان فینالیست‌ها، خانواده توابع چکیده ساز BLAKE یکی از توابعی است که امید به انتخاب دارد. در طراحی خانواده این تابع از طراحی ساده ARX استفاده شده یعنی از ترکیبی از XOR ها، چرخش‌های بیتی با مقادیر ثابت و جمع پیمانه‌ای $(\mathrm{mod}\ 2^n)$ محاسباتی ساده می‌باشند، استفاده شده است(Dunkelman & Khovratovich, 2011) .

BLAKE خانواده‌ای از چهار تابع چکیده‌ساز می‌باشد : BLAKE-224, BLAKE-256, BLAKE-384 و BLAKE-512. جدول شماره‌ی (۲) مشخصات کلی این توابع را نمایش می‌دهد. در مرحله دوم مسابقه SHA-2 این خانواده شامل دو مدل ۳۲ بیتی (BLAKE-256) و ٦٤ بیتی (BLAKE-512) بود که تفاوت آنها در مقادیر اولیه، گوناگونی دنباله زنی[1] و برش خروجی[2] می‌باشد.

جدول شماره‌ی ۲ – ویژگی‌های توابع چکیده ساز BLAKE (اندازه‌ها به بیت)(Aumasson et al., 2010)

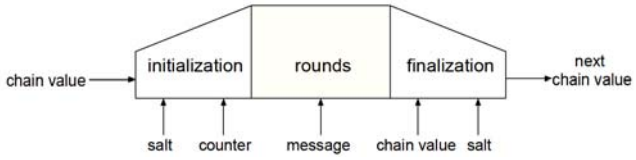
Algorithm	Word	Message	Block	Digest	Salt
BLAKE-224	32	$<2^{64}$	512	224	128
BLAKE-256	32	$<2^{64}$	512	256	128
BLAKE-384	64	$<2^{128}$	1024	384	256
BLAKE-512	64	$<2^{128}$	1024	512	256

تابع چکیده‌ساز BLAKE از روش تکرار[3] به‌کار گرفته شده در الگوریتم HAIFA تبعیت می‌کند (Biham & Dunkelman, 2006): برای فشرده سازی هر بلاک پیام با یک تابع مشخص، تابع چکیده ساز وابسته است به نمک[4] و یک شمارنده، که مشخص کننده تعداد بیت‌های چکیده شده در هر مرحله می‌باشد.

ساختار تابع فشرده ساز BLAKE از تابع LAKE به ارث برده شده است و همان‌طور که در جدول شماره‌ی (۲) نمایش داده شده است یک وضعیت داخلی بزرگ از مقدار اولیه، نمک و شمارنده، مقداردهی اولیه می‌شود. سپس این مقدار در هر مرحله (راند[5]) با مقدار پیام ترکیب

1 - Padding
2 - Truncated output
3 - Iteration mode
4 - Salt: A value that parametrizes the function, and can be either public or secret.
5 - Round

می‌شود و در آخـر فشرده شده تا به زنجیـره بعـدی وارد شـود. ایـن راهبـرد local wide-pipe نامیده می‌شود (Aumasson et al., 2010).



شکل شماره‌ی ۳ – ساختار local wide-pipe در تابع فشرده ساز BLAKE (Aumasson et al., 2010)

یک دور از تابع BLAKE-256 یک جفت راند تغییر یافته از رمز دنباله‌ای ChaCha [۱] کـه خـود گونه‌ای از رمزنگاری SalSa است، می‌باشد. این تابع دارای مزیت‌هایی به شرح ذیل است :

- طراحی:
  - سادگی الگوریتم؛
  - انجام عمل چکیده سازی با نمک .
- کارایی:
  - سرعت عمل هم در پیاده سازی نرم‌افزاری و هم سخت‌افزاری؛
  - قابلیت پـردازش مـوازی و سـبک سـنگینی بـین حافظـه و تـوان عملیـاتی در پیاده‌سازی سخت‌افزاری؛
  - سادگی سبک سنگینی بین سرعت و محرمانگی از طریق تعداد دورهای قابل تنظیم؛
- امنیت:
  - مبتنی بر اجزای تجزیه و تحلیل شده پرقدرت (ChaCha)؛
  - مقاوم در مقابل حملات عمومی پیش تصویر دوم؛
  - مقاوم در مقابل حملات کانال جانبی.

۱ – گونه‌ای از الگوریتم رمزنگاری SalSa که برای تحقق پراکنش سریع‌تر (Faster Diffusion) طراحی و ارائه شد (Bernstein, 2008).

با توجه به مزایای مذکور به‌ویژه سادگی پیاده سازی و سرعت اجرای الگوریتم، تابع BLAKE-256 به عنوان تابع چکیده ساز در مدل پیشنهادی در نظر گرفته شده است. همان‌طور که در ابتدای بخش نیز تشریح شد، این تابع یک چکیده پیام ۲۵٦ بیتی را تولید می‌کند. نتایج حاصل از پیاده سازی این الگوریتم بر روی دستگاه‌های همراه مختلف گویای کارایی این الگوریتم بوده که در بخش نتایج به تفسیر مورد بررسی قرار خواهد گرفت.

ماژول رمزنگاری/ رمزگشایی

الگوریتم رمزنگاری در مدل پیشنهادی باید به گونه‌ای باشد که با توجه به محدودیت منابع (پردازنده، حافظه و انرژی) بالاترین کارایی را ارائه کند. رمزنگاری دنباله‌ای به عنوان یکی از روش‌های رمزنگاری کلید متقارن همواره به دلیل کارایی در پیاده‌سازی نرم‌افزاری و سرعت اجرا عملیات مشهور بوده است. این نوع رمزنگاری از ابتدای شروع پروژه eSTREAM در سال ۲۰۰٤ بسیار مورد توجه قرار گرفتند. در ۱۵ آوریل ۲۰۰۸ مسابقات eSTREAM به پایان رسید و بر اساس گزارش نهایی (S. Babbage, C. Cannière, A. Canteaut, C. Cid, H. Gilbert, T. Johansson, M. Parker, B. Preneel, V. Rijmen, and M. Robshaw, 2008) HC-128 (Wu, 2005)، Rabbit (Boesgaard et al., 2005)، Salsa20/12 (Bernstein, 2005)، SOSEMANUK (Berbain et al., 2005) به عنوان لیست نهایی پروژه‌ی مذکور اعلام شدند.

Salasa20 یک رمز دنباله‌ای است که توسط دانیل برنشتاین[1] در سال ۲۰۰۵ به عنوان یکی از کاندیدهای پروژه eSTREAM مطرح شد. برنشتاین در ضمن انواع ۸ و ۱۲ دوری از این الگوریتم به نام‌های Salsa20/12, Salsa20/8 را برای ارزیابی عمومی به ثبت رسانید (Bernstein, 2005)، اگرچه آن‌ها به عنوان کاندیدهای رسمی در پروژه‌ی eSTREAM نبودند.

رمز دنباله‌ای Salsa20 بر روی کلمات ۳۲ بیتی[2] عمل می‌کند، به‌طوری‌که به عنوان ورودی یک کلید ۲۵٦ بیتی $k = (k_0, k_1, \ldots, k_7)$ و یک مقدار ٦٤ بیتی به عنوان عدد یکبار

1 – Daniel Bernstein
2 – 32-bit words

مصرف[1] به‌صورت $v = (v_0, v_1)$ می‌باشد و یک‌سری از کلیدهای بلاک ۵۱۲ بیتی تولید می‌کند. i_{th}- بلاک خروجی تابع Salsa20 می‌باشد که به عنوان کلید، عدد تک‌شمار(یک‌بار مصرف) و یک شمارنده ٦٤ بیتی $t = (t_0, t_1)$ طابق با عدد صحیح i می‌باشد. این تابع بر روی یک ماتریس 4×4 کلمات ۳۲ بیتی که به شکل زیر نوشته شده‌اند عمل می‌نماید:

$$x = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{pmatrix} = \begin{pmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ t_0 & t_1 & c_2 & k_4 \\ k_5 & k_6 & k_7 & c_3 \end{pmatrix} \quad (۸)$$

مقادیر c_i، مقادیر ثابتی مطابق جدول (۲) می‌باشند. موارد تشریح شده در بالا همگی در مورد کلید با طول ۲٥٦ بیت می‌باشند. اگر کلید k، ۱۲۸ بیتی باشد بیت‌های کلید ۲٥٦ بیتی در ماتریس با مقدار $k = k||k'$ خواهند شد.

جدول شماره‌ی ۳ – مقادیر ثابت SalSa20

	Round	F_0	F_1	F_2	F_3
C_0	61707865	73726966	6f636573	72696874	72756f66
C_1	3320646E	6d755274	7552646e	6d755264	75526874
C_2	79622D32	30326162	3261626d	30326162	3261626d
C_3	6B206574	636f6c62	6f6c6230	636f6c62	6f6c6230

اگر طول کلید ذکر نشود ۲٥٦ بیت به عنوان طول کلید در نظر گرفته می‌شود. بلاک از جریانی از کلیدها Z به صورت زیر تعریف می‌شود:

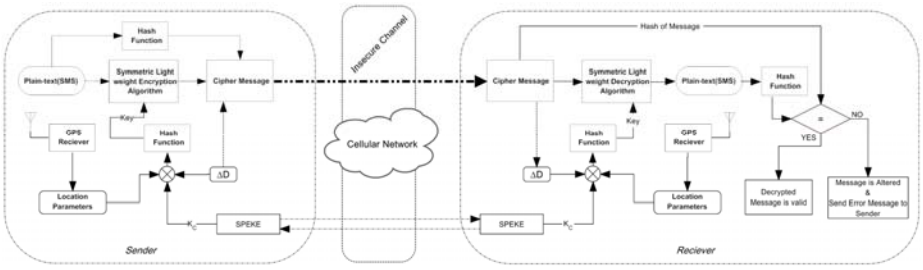
$$Z = X + X^{20} \quad (۹)$$

در این رابطه علامت + نمایانگر جمع عدد صحیح به صورت کلمه‌ای (۸ بیتی) $X^r = Round^r(X)$، در آن تابع Round بر اساس تکرار الگوریتم Salsa می‌باشد. تابع Round بر اساس روابط غیرخطی زیر که Quarterround function نیز نامیده می‌شوند به‌دست می‌آید. این تابع از انتقال بردار (X_0, X_1, X_2, X_3) به (Z_0, Z_1, Z_2, Z_3) طریق محاسبات پی‌درپی حاصل می‌شود.

$$z_1 = x_1 \oplus [(x_3 + x_0) <<< 7]$$

1 – Nonce

$$z_2 = x_2 \oplus [(x_0 + z_1) <<< 9]$$
$$z_3 = x_3 \oplus [(z_1 + z_2) <<< 13$$
$$z_0 = x_0 \oplus [(z_2 + z_3) <<< 18$$



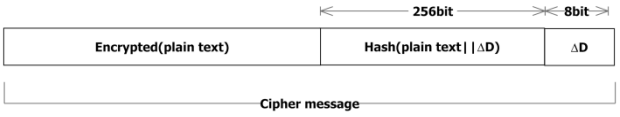
ماژول پیام کوتاه رمز شده

پس از رمزگشایی پیام در سمت فرستنده، به منظور تحقق تمامیت و جامعیت پیام[1]، چکیده پیام با استفاده از همان تابع درهم ساز استفاده شده برای تولید کلید، محاسبه شده و به انتهای پیام رمز شده الحاق می‌گردد. علاوه بر این، چون در سمت گیرنده پیام برای تولید کلید مناسب رمزگشایی داشتن مقدار ΔD ضروری است این مقدار نیز بدون رمزنگاری به پیام ارسالی الصاق می‌گردد. با در نظر گرفتن ۸ بیت برای این مقدار، قادر به تعیین محدوده رمزگشایی بین ۱ تا ۲۵۶ متر خواهیم بود. اگر محدوده بیشتری مورد نظر باشد باید ۱۶ بیت برای آن در نظر گرفته شود. از این‌رو، ۸ بیت آخر پیام را به این مقدار و ۲۵۶ بیت بعدی را به مقدار Hash و باقی‌مانده، پیام رمز شده خواهد بود.

در سمت گیرنده با جدا سازی مقادیر انتهایی پیام دریافت شده از شبکه و استخراج کلید ΔD مناسب رمزگشایی تولید شده و پیام رمزگشایی می‌شود و در مرحله بعد برای تعیین جامعیت پیام مجدداً چکیده پیام رمزگشایی شده محاسبه شده با مقدار استخراج شده از انتهای پیام دریافتی مقایسه می‌شود. اگر مقادیر یکسان باشد پیام مورد قبول بوده و در غیر این صورت

1 – Message integrity

پیغام خطایی به فرستنده پیام ارسال می‌گردد. شکل شماره‌ی (۵) ساختار پیام کوتاه ارسالی را نمایش می‌دهد.



شکل شماره‌ی ۵ – ساختار پیام کوتاه رمز شده

پیاده سازی

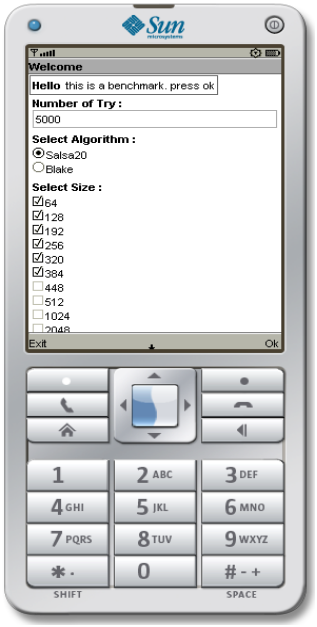
به منظور اثبات مدل پیشنهادی دو ماژول مهم رمزنگاری و درهم ریزی (چکیده سازی) که در میان ماژول‌های سیستم بیشترین مصرف کننده منابع سیستم از نظر پردازنده و حافظه می‌باشند، پیاده سازی شده و زمان اجرای الگوریتم‌های مذکور در سیستم‌های مختلف همراه با قابلیت‌های پردازشی و حافظه کم، متوسط و بالا مورد آزمایش و محک قرار گرفته است.

در طراحی و پیاده‌سازی برنامه‌ی تست کارایی الگوریتم‌های رمزنگاری/ رمزگشایی و همچنین الگوریتم درهم‌سازی از سه کلاس جاوا به شرح ذیل استفاده شده است:

- Benchmark: حاوی رابط کاربری به منظور انجام تست‌های مورد نظر بر روی الگوریتم‌ها با قابلیت انتخاب طول پیام و همچنین محاسبه زمان اجرای الگوریتم بر روی انواع دستگاه‌های همراه میزبان.
- Salsa: حاوی توابع رمزنگاری/ رمزگشایی الگوریتم Salsa20 با طول کلید ۲۵٦ بیتی می‌باشد.
- Blake: حاوی تابع چکیده ساز BLAKE-256 بوده که ورودی آن پیام با طول دلخواه و خروجی آن چکیده پیام به طول ۲۵٦ بیت می‌باشد.

رابط کاربری تهیه شده امکان اجرای تعداد دفعات تست را برای هر یک از طول‌های پیام مختلف فراهم می‌آورد. مقدار پیش فرض قرار داده شده در برنامه، ۱۰ می‌باشد اما با توجه به تست‌های مکرر به عمل آمده مشخص شد که به دلیل عدم دسترسی MIDlet به دستوراتی به منظور بالا بردن اولویت اجرای برنامه‌ی تست و به

دست گیری کامل توان پردازشی دستگاه همراه، اگر تعداد تست‌های اجرا شده پایین باشد به مراتب نتایج حاصله خطای بیشتری دارند. این مورد در دستگاه‌های همراه دارای سیستم‌های عامل با قابلیت اجرای چند برنامه به طور هم‌زمان بیشتر دیده می‌شود؛ به‌طوری‌که اگر در زمان اجرای تست وظایف دیگری نیز بر دوش پردازنده باشد زمان‌های بدست آمده بسیار بالا و دور از ذهن خواهد بود



شکل شماره‌ی ٦ – محیط واسط کاربری برنامه تولید شده برای تست کارایی الگوریتم‌های مدل

در ضمن برنامه کاربردی تهیه شده امکان انتخاب تست بر روی الگوریتم رمزنگاری و الگوریتم درهم سازی را در یک رابط کاربری ارائه می‌کند. طول پیام‌های کوتاه مورد آزمایش به صورت انتخابی بوده و کاربر می‌تواند آزمایش را بر روی پیام‌های کوتاه از ٦٤ بایت تا ١٢٨٠٠ بایت انجام دهد.

نرم‌افزار تهیه شده به منظور تست کارایی و سرعت الگوریتم‌های رمزنگاری و درهم سازی، بر روی ١٥ دستگاه گوشی همراه با ویژگی‌های سخت‌افزاری و سیستم

عامل مختلف تست گردید. دستگاه‌های انتخاب شده طیف وسیعی از دستگاه‌های همراه را شامل می‌شدند از دستگاه‌های گران قیمت با پردازنده پیشرفته و حافظه بالا، تا نمونه‌های بسیار ارزان قیمت و با حداقل امکانات سخت افزاری.

اما در همه آن‌ها مشترک بود، قابلیت اجرای برنامه‌های Java بر روی این دستگاه‌ها بود که شرط اولیه برای استفاده کاربر از سیستم بانکداری مبتنی بر پیام کوتاه است.

نتایج نشان داد که عملیات رمزنگاری/ رمزگشایی و درهم سازی که بیشترین حافظه و زمان پردازش را به خود مشغول می‌کنند در زمان‌هایی بسیار کمتر از ثانیه قابل اجرا می‌باشند. ضمناً دستگاه‌های با حداقل حافظه نیز توانستند تست انجام شده را اجرا کرده و این عملیات را انجام دهند.

این نتایج، گویای انتخاب صحیح الگوریتم‌های رمزنگاری و درهم سازی سبک می‌باشد. اکثر مدل‌های رمزنگاری پیام کوتاه از الگوریتم‌های مانند AES و SHA-1 استفاده می‌کنند که کد برنامه آن‌ها در J2ME در اینترنت یافت می‌شود. اما کدهای استفاده شده در الگوریتم SalSa20 و BLAKE-256 برای اجرا در محیط مذکور بهینه سازی شده و حتی در برخی موارد مجدداً کد نویسی شده است.

جدول شماره‌ی ٤ – دستگاه‌های همراه مورد تست را به همراه مشخصات آن‌ها نشان می‌دهد.

Row(ID)	Brand	Model	Memory[1]	Os	Announce
1	Nokia	N73	64MB	Symbian OS 9.1, S60 3rd edition	2006
2	Sony Ericsson	C905	160MB	Java MIDP 2.0	2008
3	Sony Ericsson	K800	64MB	Java MIDP 2.0	2006
4	Nokia	6670	8MB	Symbian OS v7.0s, Series 60 v2.0	2004
5	Nokia	6710N	50MB	Symbian OS 9.3, S60 rel. 3.2	2009
6	HTC	Touch cruise	128MB	Microsoft Windows Mobile 6.0 Professional	2007

1 – Internal memory-RAM

7	Sony Ericsson	W350	14MB	Java MIDP 2.0	2008
8	Sony Ericsson	W810	20MB	Java MIDP 2.0	2006
9	Nokia	2710N	64MB	Java MIDP 2.1	2009
10	Sony Ericsson	Vivaz	75MB	Symbian Series 60, 5th edition	2010
11	Sony Ericsson	Z610i	16MB	Java MIDP 2.0	2006
12	Samsung	8910	150MB	Java MIDP 2.0	2009
13	Sony Ericsson	Aino	55MB	Java MIDP 2.0	2009
14	Nokia	N70	22MB	Symbian OS 8.1a , Series 60 UI	2005
15	Nokia	N76	96MB	Symbian OS 9.2, S60 rel. 3.1	2007

جدول شماره‌ی ۵ – نتایج حاصل از تست الگوریتم SalSa20 بر روی دستگاه‌های همراه

Headset ID	64B	128B	196B	256B	320B	384B	Average
1	142.6	187.6	239.2	277	318	373.6	219.8571
2	207.8	230.5	423.8	554.8	668.6	802.6	412.8714
3	144	221.4	353.2	483.8	812	852.6	410
4	362.2	429.8	594.4	715.6	887.8	1309.2	614.7143
5	67.2	92.2	119.2	149.4	177	214.4	117.7714
6	88.2	136	179.4	242.2	280	299.2	175.8571
7	274.2	954	972	1069.2	1146.4	1195.4	802.6
8	324.8	935	1025.4	1135	1290.2	1326	863.4857
9	445	553.8	655.6	759	850.4	948	602.9714
10	70.2	91	113.6	138.6	163.2	200.8	112.4857
11	145.6	239	375.4	619.8	728.8	756.4	410.8571
12	16.4	64.4	81.2	97.2	114.8	129.8	73.68571
13	157.6	182.6	293.6	358.4	433	528.6	280.9714
14	193.6	237	325.8	343.8	440.8	481.2	290.8857
15	86.4	114.2	134.4	177.6	207.6	236.6	138.8286

جدول شماره‌ی ٦ – نتایج حاصل از تست الگوریتم BLAKE-256 بر روی دستگاه‌های همراه

Headset ID	64B	128B	196B	256B	320B	384B	Average
1	764.6	1198	3279.8	3895.8	4371	4754.2	3043.9
2	901.4	1273	2094.2	2507	2855.2	3244.2	2145.833
3	1524.8	1817.4	2165.2	2431.6	2766.4	3076.2	2296.933
4	1339.8	2136.4	4616	5319.2	5956.4	6522.6	4315.067
5	272.6	276.4	357.2	444.2	523.6	612.8	414.4667
6	437.6	606.2	777.4	970	1105.4	1280.4	862.8333
7	2126.8	2646.6	3134.4	3631	4069.2	4627.4	3372.567
8	2376	2985.2	3577.2	4281	4965	5665.4	3974.967
9	1022.2	1507.6	1989.6	2474.2	2964.4	3449.2	2234.533
10	174.6	236	307.6	380	448.2	531.2	346.2667
11	1352	1635.8	1976	2301	2669.6	2994.6	2154.833
12	237.4	342	447.2	554.8	660.4	767.6	501.5667
13	844.6	1325.8	1758.8	2211.6	2595	2930.6	1944.4
14	1000.2	1421.8	1696.4	2163	2535	3002.4	1969.8
15	495	732.2	969.6	1491.6	4390.8	4834	2152.2

نتایج حاصل از تست الگوریتم‌ها (SalSa, BLAKE) بر روی دستگاه‌های جدول شماره‌ی (٤)، در جداول شماره‌ی (٥) و (٦) نمایش داده شده است. مقادیر نشانگر زمان متوسط اجرای عملیات بوده و برای راحتی نمایش به میکرو ثانیه تبدیل شده‌اند. ضمناً تعداد دور تست برابر با ٥٠٠٠ در نظر گرفته شده است.

همان‌طور که از نتایج آزمایش مشخص است الگوریتم SalSa20 که به منظور الگوریتم رمزنگاری و رمزگشایی در مدل پیشنهادی مطرح شده است کارایی بسیار مطلوبی از خود نمایش می‌دهد. حتی در دستگاه‌های قدیمی با حداقل حافظه و توان پردازشی (ردیف ٤)، در زمان حدود ١.٣ میلی ثانیه قادر به رمزگذاری یک پیام به طول ٣٨٤ کاراکتر می‌باشد.

این زمان در مورد یک دستگاه همراه جدید با توان پردازشی مناسب و حافظه بالا، به حدود ٠.١٢٩ میلی ثانیه می‌رسد که عملاً می‌توان آن‌را به عنوان بلادرنگ فرض نمود.

مقدار متوسط زمان رمزگذاری این الگوریتم نشانگر اجرای عملیات رمزگذاری در کمتر از یک میلی ثانیه به طور متوسط است.

در خصوص الگوریتم BLAKE-256 نیز می‌توان به نتایجی مشابه دست یافت. هرچند زمان اجرای عملیات این الگوریتم بالاتر است اما در بدترین شرایط این زمان از ٦.٥ میلی ثانیه تجاوز نمی‌کند.

نتایج حاصل از هر دو الگوریتم گویای کارایی بالای هر دو در دستگاه‌های همراه با حداقل امکانات می‌باشد. هرچند امروزه با پیشرفت فناوری در حوزه حافظه‌ها و پردازنده‌ها محدودیتی در این خصوص احساس نمی‌شود اما هدف از اجرای این تست اثبات کارایی و سازگاری الگوریتم‌های انتخابی در مدل پیشنهادی بوده است که نتایج بدست آمده به خوبی آن‌را اثبات می‌کنند.

نتیجه

تکنیک‌های رمزنگاری معمول قادر به محدودسازی کاربران ادوات همراه به رمزگشایی داده‌ها در محدوده مکانی مشخصی نیستند. برای تحقق این امر در این مقاله مدلی ارائه شده است که با استفاده از پارامترهای مختصات مکانی

قادر به محدودسازی رمزگشایی پیام در منطقه خاص عملیاتی خواهیم بود. پروتکل پیشنهادی با به‌کارگیری الگوریتم‌های سبک از نوع رمز دنباله‌ای و توابع درهم ساز سبک با حداقل منابع، محرمانگی، تمامیت و جامعیت داده و تصدیق هویت و عدم انکار را فراهم می‌آورد. هرچند مدل بیانگر رمزنگاری پیام کوتاه مبتنی بر موقعیت است اما طراحی پروتکل به گونه‌ای است که قادر به رمزنگاری انواع مختلف داده اعم از فایل داده، صدا و تصویر قابل استفاده در مناطق عملیاتی می‌باشد.

نوآوری‌های این مقاله را می‌توان به شرح ذیل بیان نمود:

- بررسی فعالیت‌های انجام شده در این حوزه تحقیقاتی و تبیین اهمیت موضوع و کاربردهای آن علی‌الخصوص در مسائل نظامی و دفاعی.
- ارائه مدل امن رمزگذاری.
- طراحی و ترسیم نمودار توالی عملیات جهت سهولت درک فرآیند عملیات تولید کلید.
- ارائه الگویی جدید جهت تبادل کلید در محیط ناامن مبتنی بر الگوریتمی تغییر یافته از الگوریتم دفی هلمن.
- استفاده از الگوریتم‌های جدید و سبک رمزنگاری و درهم‌سازی.

- اثبات سازگاری و کارایی الگوریتم‌های انتخابی بر روی دستگاه‌های مختلف همراه با استفاده از نرم افزار طراحی شده.

در ضمن، در مدل پیشنهادی فقط از مختصات جغرافیایی برای محدود سازی رمزگشایی استفاده شده اما با اعمال پارامترهای دیگر مانند سرعت، زمان و ارتفاع از سطح زمین می‌توان رمزنگاری را مستحکم‌تر نمود. این مسئله می‌تواند زمینه‌ای برای فعالیت‌های آتی باشد. ضمن اینکه پیاده سازی کل مدل نیز می‌تواند به عنوان فعالیت‌های آتی در جهت اثبات هر چه بیشتر مدل مورد نظر محققان باشد. علاوه بر موارد مذکور، پیاده سازی بقیه الگوریتم‌های رمزنگاری و درهم سازی از دو مسابقه معتبر ذکر شده خود زمینه تحقیقی بسیار مناسبی است برای انتخاب بهینه الگوریتم‌ها.

منابع

انگلیسی

1- Aumasson, J.P., Henzen, L., Meier, W. & Phan, R.C.-W., (2010). "***SHA-3 proposal BLAKE***". [Document] Available at: http://www.131002.net/blake/blake.pdf [Accessed July 2011].

2- Berbain, C. et al., (2005). "***SOSEMANUK, a fast software-oriented stream cipher***". [Online]. eSTREAM project website.

3- Bernstein, D.J., (2005). "***Salsa20/8 and Salsa20/12***". Technical Report 2006/007. ECRYPT Stream Cipher Project.

4- Bernstein, D.J., (2008). "***ChaCha, a variant of Salsa20***". [Online] eSTREAM Project Available at: http://cr.yp.to/chacha.html.

5- Biham, E. & Dunkelman, O., (2006). "***framework for iterative hash functions - HAIFA. In In Proceedings of Second NIST Cryptographic Hash Workshop***"., 2006.

6- Boesgaard, M., Vesterager, M., Christensen, T. & Zenner, E., (2005). "***The stream cipher Rabbit***". [Online]. eSTREAM project website.

7- Dunkelman, O. & Khovratovich, D., (2011). "***Iterative Differentials, Symmetries, and Message Modification in BLAKE-256. In ECRYPT II Hash Workshop***". Tallinn, Estonia, 2011.

8- Giguere, E., (2004). "**Databases and MIDP, Part 1: Understanding the Record Management System.** [Online] Available at: http://developers.sun.com/mobility/midp/articles/databaserms/.

9- Hallsteinsen, S., Jorstad, I. & Thanh, V., (2007). "***Using the mobile phone as a security token for unified authentication***". In *ICSNC '07 Proceedings of the Second*

International Conference on Systems and Networks Communications., 2007. IEEE Computer Society Washington, DC, USA.

10- Jablon, D.P., (1996). "***Strong Password-Only Authenticated Key Exchange***". *ACM SIGCOMM Computer Communication Review*, 26(5).

11- Kupper, A., (2005). "***Location-based services : fundamentals and operation***. West Sussex, England: John Wiley & Sons.

12- Liao, H.C. & Chao, Y.H., (2008). "***A New Data Encryption Algorithm Based on the Location of Mobile Users***". *Information Technology Journal*, 7(1).

13- Lisonik, D. & Drahansky, M., (2008). "***SMS Encryption for Mobile Communication***". In International Conference on Security., 2008.

14- Lo, L.C., Bishop, J. & Eloff, J.H.P., (2008). "***SMSSec: An end-to-end protocol for secure SMS***". *Computers & Security*, 27.

15- Mahmoud, Q.H., (2004). "***J2ME and Location-Based Services***". [Online] Available at: http://developers.sun.com/mobility/apis/articles/location.

16- Qiu, D., 2007. (2007) "***Security Analysis of Geoencryption: A Case Study Using Loran***". In *ION GPS/GNSS*.,.

17- Ren, K., Lou, W. & Zhang, Y., (2008). "***LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks***". *IEEE TRANSACTIONS ON MOBILE COMPUTING,* 7(5).

18- Rice, J.E. & Zhu, Y., (2009). "***A proposed architecture for secure two-party mobile payment***". In IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, PacRim'09., 2009.

19- RSA Laboratories, (2000). [Online] "***RSA Security Inc***". Available at: http://www.rsa.com/rsalabs/node.asp?id=2152.

20- S. Babbage, C. Cannière, A. Canteaut, C. Cid, H. Gilbert, T. Johansson, M. Parker, B. Preneel, V. Rijmen, and M. Robshaw, (2008). [Online] Available at: http://***www.ecrypt.eu.org***/stream/portfolio.pdf [Accessed May 2011].

21- Scott, L. & Denning, D.E., (2003). "***A Location Based Encryption Technique and Some of Its Applications***". In Proceedings of the 2003 National Technical Meeting of The Institute of Navigation. Anaheim, CA, 2003.

22- Scott, L. & Denning, L., (2003). "***Location Based Encryption & Its Role In Digital Cinema Distribution***". In *Proceedings of ION GPS/GNSS*., 2003.

23- Wu, H., (2005). "***The Stream Cipher HC-128***". [Online]. eSTREAM project website.

24- Yan, Y. & Olariu, S., (2009). "***An efficient geographic location-based security mechanism for vehicular adhoc networks***". In *IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, 2009. MASS* '09. Macau, 2009

A Defense Protocol for Securing Short Messages in Military Operation Regions

Shahryar Mohammadi and Farzad Tavakkoli

ABSTRACT

Tone of the major security problems in exchanging messages in military operation regions is how to access and decrypt the message by the intended receiver, as well as to prevent the illegal access by those waiting in the communication channel. Primarily, the usual methods for decrypting military messages are not immune from the probable efforts made by the enemy trying the catch the message. By simple definition, the concept of geo-encryption is a method of cryptography in which the encrypted text can be encrypted in a specific place. These algorithms are not substitutes for the traditional methods of cryptography. Instead, they create an additional security layer more that what the traditional cryptographies. This article proposes a new cryptography protocol based on a spatial situation which enables users to exchange the encrypted information in a completely secure manner, in proportion to the operation regions. Although the cryptographic model has been explained to focus on short message, the proposed model can be generalized for encrypting any kind of data like sound, image and etc.… One of the challenges facing high-technology industries especially in military industries is to secure the use of military devices and ammunitions in a specified region like that of a country. In this proposed model, the key authorizing the initiation of a military system or that for decrypting confidential messages like defense or military directives can be integrated with the spatial position extracted from the GPS system, hence adding an additional security layer to the security levels expected for the system. Generally, the features of this proposed model can be argued at three levels: 1) using crypto algorithms and merging resulted by the project eSTREAM_Profile (software); 2) not using asymmetric crypto algorithm due to strong footprint and the need to key management; 3) using Diffe-Hellman's optimized algorithm in order to generate key exchange using a short password.

KeyWords: *cryptography; short message; spatial position; stream cipher; Hashing Function; Location Based Services*

The Geopolitical Dimensions of the Cyberspace in the Age of Information Technology

Zahra AhmadiPur, Reza Joneydi, AbdolVah'hab Khoja Lee and Esmaeil Parsaei

ABSTRACT

In its process of development in line with the information revolution, especially the advent of Internet, geopolitics faced with a new area which is referred to as the geopolitics of cyberspace. With the arrival of cyberspace due to the coming of internet as a new area of human activity where actors acquire the ability to act and react as to each other, part of the geopolitical studies has entered the same area. Considering this very important development, the present article seeks to analyze the geopolitical dimensions of cyberspace and the geopolitical developments that come as a result of the information technology.

The present article argues that the most important dimensions of cyberspace and the geopolitical developments arising from the information technology include: a change in the contested space in geopolitics, convergence and cooperation, a change in the nature of power in geopolitics, the increasing digital gap, the managerial aspect and the controlled cyberspace, the developed relationship between the government and the citizens, national and sub0national identity, cyber terrorism, cyber soft war and cyber war.

KeyWords: *the geopolitics of cyberspace; power; cyberspace; information revolution; information technology.*

The Place of Information Reliability in the Horizon of the I.R.I. Defense Policy; a Research Framework for Studying Defense in Depth Strategy to Counter the Computer Threats

Abbas HadaviNia, Rahim Mohtaram Ghalatee

ABSTRACT

In the recent years, the change in cyber attacks has transformed into a security-defense challenge throughout the world. Under the circumstances where the military wars have been replaced by soft and cyber wars, the defense systems of countries have no alternative but to pay more attention to strategies of protecting against such attacks. The defense-in-depth, which is addressed in this research, is one of the strategies of defending against such attacks. Considering the fact that no example of paying heed to this strategy has been observed in studying the research record, the present research has aimed at presenting a theoretical framework for giving direction to future researches. Therefore, information reliability has been theoretically explored as a fundamental concept of defense-in-depth strategy in the area of cyber security, which resulted in the representation of three components- people, technology, and operations- as the constituents of information reliability that play a major role in defense-in-depth strategy. It ends by coming up with a framework for considering the strategy intended in the country's defense policy, which has covered the above-mentioned components along with the elements suggested to have formed them. Considering the theoretical nature of this research, the method of carrying it out has been the documentary literature analysis as evidenced by the documents published in defense organizations, which has culminated in a framework proposed through results orientation on the part of the researchers.

KeyWords: *information reliability; defense-in-depth strategy; computer security; cyber attacks.*

I A Framework for Conceptualizing Information Warfare

AliReza Farsh'chee, Ehsan Mer'atee

ABSTRACT

The increasing capabilities of information technology have caused the defense area as an important and sensitive domain, to be constantly seeking to develop and employ up-to-date capabilities of information technology. This has caused the concerned agents in defense area to sometimes invent the most up-to-date information technologies. On the one hand, scholars have started to conceptualize the uses of related applications in the area of defense in order to pave the way for developing the information technology applications. It follows that the advent of information technology in defense area has led to the formation of concepts like cyber warfare, net-centric warfare, and electronic warfare. According to the related literature, most of the terminology lies in the area of electronic warfare. However, from a theoretical point of view, the way the relationship between different concepts has been established, and how information warfare has covered them, has not been explained well. So, the present research has set about conceptualizing information warfare by studying and analyzing the existing models and concepts in information warfare, and making a comparative study of them. This framework has covered the entire concepts and terminology in the area of information warfare, explaining and analyzing the fundamental dimensions of information warfare. This framework can be used as a basis for criticizing the researches made in the area of information warfare. Furthermore, it has the capability of mitigating the disorder in the area of information warfare, where the resulted order can lead to the formation of a structural way of thinking in the area of information warfare, and to the furthering of this way of thinking in different fundamental dimensions.

KeyWords: *information technology; information warfare; knowledge-based warfare; strategic information warfare; net0centric warfare*

Organizational Architecture Setting the Ground for Establishing and Developing Information Architecture in I.R.I Administrative and Defense Organizations

AliReza Naderi Khorshidi, Hadi Faghih AliAbadi, Ramezan MirAbbasi

ABSTRACT

The experiences gained in developed countries in information architecture in organizations indicate that information architecture requires infrastructures and backgrounds that, if not met prior to being built, will prevent organizations from achieving the expected utilities as well as the objectives sought in developing information technology. Despite the remarkable benefits that information architecture may encompass in administrative and defense systems, the efforts and energy put to this area in our country came across many challenges in the stages of designing and implementing, which couldn't lead to desirable and expected results.

This article has examined real examples of implementing information architecture in government organizations in our country compared with international successful examples introduced as a basic model. Then, using grounded theory and content analysis, it has sought to clarify the main reasons why the mentioned activities in the administrative organizations in our country have been unsuccessful. Finally, having studied international successful models and analyzed them, and further due to natural circumstances in the country, the article has concluded that – in accordance with the changes and needs of the environment surrounding the organizations in the country, as well as the traditional structures and the process in which work is done inside them- they must establish organizational architecture activities as an infrastructure for developing information architecture in order to make the mission and architectural engineering of systems and its processes transparent. Otherwise, it will not be effective- as expected- to do any information architecture by establishing electronic government.

KeyWords: *information architecture; organizational architecture; integrating factors; behavioral factors.*

Building a Methodology for Developing Architecture Frameworks for Defense Organizations

Ehsan Mer'atee

ABSTRACT

It is often the case that the defense area is a starting point where new managerial and engineering methods are invented due to the fact that it has acquired a peculiar importance and sensitivity. The issue of organizational architecture is one like such cases taking its origin from the U.S. defense organizations. Although defense organizations are the best examples of those that implement enterprise architecture frameworks, these organizations have in no way published any information on how to develop specific architecture frameworks for defense organizations. So, this article sets out to build a methodology for developing architecture frameworks for defense organizations. In so doing, it analyses different versions of the architecture frameworks designed for the United States Department of Defense, and presents a methodology for developing architecture frameworks for defense organizations by using grounded theory research method. Drawing on such method, one can bring in advantages like decreased time in developing frameworks, risk mitigation, cost reduction, and better management of developing architecture frameworks for defense organizations.

KeyWords: *organizational architecture; architecture framework; the architecture framework designed for the United States Department of Defense.*

Cloud Computing; a Modern Approach in the Architecture of Information Space

Amin Hakim, Shahryar Mohammadi

ABSTRACT

Cloud computing is the ability to provide information technology resources and capacities via internet. It is a new approach in architecture relying on the fact that internet-based resources can be employed fast with less cost and more variety. In fact, it can be argued that cloud computing is an information space architecture model that enables an appropriate and demand-based network to access a mass of common computing resources- like networks, servers, information database, applied programs and services) with much less cost, and high-level development capability and innovation as well as without any spatial and time limitation, and provides capacities that have transformed cloud computing into a strategic approach. From such perspective, information exchange and security face growth opportunities on the one hand, and new challenges on the other. As a result, and with regard to how it important the issue is, as well as the features of this kind of architecture (the use of clouds, different centers and networks, as well as the combination of differing services and the balance between the range, speed and security of information access), the present article considers this kind of addressing this modern kind of architecture as the central axis around which its discussions revolve.

KeyWords: *cloud computing; cyberspace, information technology; information architecture; information organizations.*

Table of Contents

The Journal of Defense Policy, Vol. 20, Serial No. 79, Summer 2012

In the Name of God, the Compassionate, the Merciful

The Journal of Defense Policy

The Scientific Journal
of Center for Defense Studies and National Security,
affiliated to Imam Hossein (P.B.U.H) University

Vol. 20, No. 3, Summer 2012, Serial No. 79 (ISSN-1025-5087)

Proprietor: Imam Hossein Comprehensive University, Defence & National Security Studies Center

Chairman Manager: Ali Reza Farshchi

Editor: Dr. Seyyed Yahya Safavi

Managing Editor: Ali Ghanbarzadeh

Typesetter and Typographer: mohammad hossain saadat

Observer of Publication: Andishgah-e Elmo-San'ate Jahan-e Moaser

Lithograph, Publication and Bookbinding: Shakib Publications

Address: Defence & National Security Studies Center; Imam Hossein(PBUH) Comprehensive University

Tel: +9821-77105765

Fax: +9821-77105747

P. O. Box: 16765-3459 Tehran, Iran

Book Store: Defence & National Security Studies Center; Imam Hossein(PBUH) Comprehensive University; Shahid Babaie Exp way, Tehran, Iran.

Tel: +9821-77105741 & 42