فصلنامه مطالعات راهبردی فضای سایبر
سال دوم، شماره چهارم، پائیز ۱۴۰۱
مقاله ششم از صفحات ۱۷۸-۱۴۹

ابعاد معماری کلان گروه پاسخ‌گویی فوریتی رایانه‌ای مراکز دفاعی

محمدرضا کریمی قهرودی [۱]، رضا کشاورز [۲]، محمدرضا موحدی صفت [۳] و محمود صالح اصفهانی [٤]

تاریخ دریافت: ۱۴۰۰/۰۶/۲۲ تاریخ پذیرش: ۱۴۰۱/۰۴/۱۵

چکیده

گسترش روز افزون به‌کارگیری فناوری اطلاعات در سازمان‌های دفاعی، موجب شده است که دارایی‌ها و اطلاعات با ارزشی در این بستر قرار گیرد؛ ولیکن درصورت وقوع رخداد رایانه‌ای و نیز عدم آمادگی لازم برای پاسخ‌گویی، عواقب جبران ناپذیری به همراه خواهد داشت؛ از این‌رو، ضرورت تشکیل گروهی منسجم که بتواند به فوریت‌های رایانه‌ای در مراکز دفاعی پاسخ‌گو باشد، احساس می‌گردد؛ قبل از راه‌اندازی چنین امر مهمی، باید ابعاد معماری کلان احصاء شود؛ این تحقیق، درپی شناسایی ابعاد معماری کلان گروه پاسخ‌گویی مراکز دفاعی است. با اتکا به روش کتابخانه‌ای، داده‌های مورد نیاز استخراج و با نظر خبرگان حوزه دفاع سایبری، سوالاتی تنظیم و در بین ٦٥ نفر از خبرگان جامعه هدف توزیع گردید. سپس با تحلیل نتایج آماری از طریق نرم‌افزار اس‌پی‌اس‌اس، ابعاد معماری کلان گروه پاسخ‌گویی فوریتی مراکز دفاعی به‌صورت زیر احصاء شد: ۱.مدیریت و فرماندهی، ۲. امنیت، ۳. مأموریت، ٤. اهداف و کارکردها، ۵. فرآیندها، ٦. ساختار و سازمان، ۷. فناوری، ۸. تنظیم مقررات و حقوقی به‌دست آمد.

کلیدواژه‌ها: ابعاد، معماری کلان، گروه پاسخ‌گویی فوریتی رایانه‌ای، مراکز دفاعی، فوریت‌های رایانه‌ای.

[۱] استادیار و عضو هیات علمی دانشگاه مالک اشتر، نویسنده مسئول، رایانامه: favad110@gmail.ir
[۲] دکترای دانشگاه عالی دفاع ملی، رایانامه: Rezakeshavarz@sndu.ac.ir
[۳] دانشیار و عضو هیات علمی دانشگاه عالی دفاع ملی، رایانامه: movahedi@sndu.ac.ir
[٤] استادیار و عضو هیات علمی دانشگاه امام حسین (ع)، m_saleh@ihu.ac.ir

۱- مقدمه و بیان مساله

عصر حاضر شاهد رشد روزافزون فناوری اطلاعات و ارتباطات در مراکز دفاعی بوده و این امر موجب شده است که دارایی‌های سازمان‌ها بر مبنای سامانه‌های بر پایه فناوری اطلاعات قرار گیرد؛ اما از آن‌جایی که این دارایی‌ها ارزش بسیار زیادی برای سازمان دارد، بایستی درصورت بروز یک رخداد امنیتی، فرآیند یا سازوکاری وجود داشته باشد که بتواند با سرعت در تشخیص تهدید، تحلیل و پاسخ‌گویی به یک مشکل امنیتی، میزان خطر و هزینه ترمیم را کاهش دهد؛ از طرفی در عصر حاضر با گسترش فناوری اطلاعات، دانش سازمان‌های مهاجم و هکرها روند افزایشی به خود گرفته و با گسترش دانش و ترفندها، تهدیدات پیچیده‌تر و جنگ‌ها به‌صورت شبکه‌ای شده‌اند؛ از طرفی با توجه به نرخ گسترش تهدیدات، معماری جامعی که بتواند با همکاری سازمان‌های تابعه و نهادهای ذی‌ربط، پاسخ‌گویی مناسبی به این‌گونه تهدیدات باشد، احساس می‌گردد؛ اما بر اساس مطالعات انجام شده، بیشتر سازمان‌ها دارای مرجع مناسب و شیوه‌نامه منسجمی برای پاسخ‌گویی کارآمد به تهدیدات و رخدادهای رایانه‌ای نیستند.

تیم پاسخ‌گویی فوریتی به حوادث رایانه‌ای[1]، یک سازمان خدماتی مسئول دریافت، مرور و پاسخ‌گویی به گزارشات ارسالی و فعالیت‌های مربوط به مشکلات و رویدادهای رایانه‌ای است (پندو[2]، ۲۰۱۸ : ۱۳). درواقع گروه پاسخ‌گویی یک نقطه مرکزی برای گزارشات مرتبط با مشکلات امنیتی است که پس از بررسی اطلاعات وارده، الگو و هدف فعالیت مخرب در آن شناسایی و عکس العمل مناسب نشان داده می‌شود. گروه پاسخ‌گویی می‌تواند با سایر تیم‌های پاسخ‌گویی به حوادث رایانه‌ای در خارج سازمان همکاری داشته باشد. این همکاری به اشتراک راهبردها در پاسخ‌گویی به حملات مشابه می‌انجامد و می‌توان به عنوان یک هشداردهنده برای مشکلات بالقوه برشمرد (براون لی[3]، ۲۰۱۸: ۲۱). این گروه یک نقطه مرکزی برای گزارش مشکلات امنیتی است که پس از بررسی اطلاعات وارد شده، هدف و الگوی فعالیت مخرب را شناسایی کرده و بر اساس آن عکس‌العمل مناسب نشان داده می‌شود. گروه پاسخ‌گویی می‌تواند با بقیه تیم‌های پاسخ‌گویی به حوادث

1- Computer Emergency Response Team (CERT).
2- Penedo.
3- Brownlee.

رایانه‌ای در خارج سازمان همکاری داشته باشد؛ این همکاری منجر به اشتراک راهبردها در پاسخ‌گویی به حملات مشابه شده و به عنوان یک هشداردهنده برای مشکلات بالقوه در نظر گرفته می‌شود (پندو و دیوید، ۲۰۱۸). زمانی می‌توان از فضای سایبر به‌عنوان پیوند دهنده زیرساخت‌های حیاتی کشور استفاده نمود که مسئله امنیت آن به‌طور کامل حل شده باشد، وجود هرگونه شکاف امنیتی در این فضا و در اجزایی که در این فضا عمل می‌نمایند، ضربات جبران ناپذیری را به کشور وارد خواهد کرد (صیاد و همکاران، ۱۳۹۹: ۱۲).

تدوین، تصویب و ابلاغ سند راهبردی امنیت فضای تبادل اطلاعات کشور (افتا)، ابلاغ سیاست‌های کلان نظام درخصوص افتا و تشکیل شورای عالی فضای مجازی طی این سال‌ها، شروع مناسبی را برای پیشرفت دانش در حوزه‌های مختلف و خصوصاً حوزه امنیت در کشور ایجاد کرده است؛ همچنین در طرح‌های امنیتی و دیگر اسناد بالادستی، برای این مباحث و مقابله با تهدیدات و پاسخ‌گویی به تهدیدات رایانه‌ای گروه‌های امنیتی ایجاد شده‌اند، اما با توجه به کارکرد و ساختار گروه پاسخ‌گویی، این تیم‌ها قادر به ارایه خدمات مورد نیاز برای سازمان‌های وابسته به مراکز دفاعی نیستند. درصورتی‌که این امر با دقت لازم و همت و اراده‌ای قوی دنبال نگردد و نیز به علت کمبود شیوه مناسب و منسجم و نیز عدم وجود مرجع واحد در پاسخ‌گویی به تهدیدات رایانه‌ای در سطح مراکز دفاعی، منجر به افزایش آسیب‌پذیری در برابر تهدیدات و ایجاد خسارات جبران ناپذیر خواهد شد. در فرآیند مطالعات پیشین، روش‌شناسی به عنوان قسمتی از یک چارچوب مدیریتی مناسب برای شناسایی و ارزیابی فرآیند مورد نیاز است؛ به‌همین منظور کشاورز در مقاله‌ای با عنوان "ارایه الگوی استقرار گروه پاسخ‌گویی فوریتی رایانه‌ای مراکز دفاعی"، روش پاسخ‌گویی به حوادث از دیدگاه‌های موسسه ملی استاندارد و فناوری[1] و موسسه فوریت امنیتی[2] و مرکز فوریت رایانه‌ای ژاپن[3] را مورد بررسی قرار داده است؛ همچنین تطبیق الگوهای گروه پاسخ‌گویی در پاسخ‌گویی به حوادث، خدمات و ساختارهای پیشنهادی مراکز دفاعی، الگوی فرآیند نحوه مقابله گروه پاسخ‌گویی در مراکز دفاعی با یک رخداد و ارتباط بین مولفه‌ها در این مقاله بررسی شده و در نهایت الگوی استقرار گروه پاسخ‌گویی مراکز دفاعی ارایه گردیده است (کشاورز، ۱۳۹۳: ۹۷). همچنین طیرانی(۱۳۹۵) در نشریه‌ای از آپای

1- NIST (National Institute of standard and technology).
2 - SEI (Security Emergency Institute).
3- Japanizes CERT (JPCERT).

دانشگاه فردوسی مشهد، به بررسی انواع تیم‌های پاسخ‌گویی پرداخته و روش‌های مقابله با رخدادهای رایانه‌ای و بررسی نقاط قوت و ضعف انواع گروه پاسخ‌گویی را مورد بررسی قرار داده است. این موارد از نقاط اشتراک این مقاله با موضوع مورد تحقیق می‌باشد (طیرانی، ۱۳۹۵: ۲۳). پرداختن به خدمات گروه پاسخ‌گویی، خدمات مدیریت کیفیت امنیت و اندازه گروه و تعداد نفرات از دیگر موارد مورد نیاز در مطالعه گروه پاسخ‌گویی می‌باشند که رشتی(۱۳۸۸) با عنوان ایجاد یک گروه پاسخ‌گویی به رخدادهای رایانه‌ای به این مسأله پرداخته است (رشتی، ۱۳۸۸: ۱۲۳). مدیریت مخاطرات و تحلیل موقعیتی و مکانی از دیگر موارد مورد تفحص شده نشریه سایبری طرح پاسخ‌گویی به فوریت‌های رایانه‌ای[1] همچنین معماری و اجزای لایه معماری گروه پاسخ‌گویی نیز به عنوان یکی از مهم‌ترین مؤلفه‌ها در بررسی یک گروه پاسخ‌گویی از سند سایبر ملی مورد استفاده قرار گرفته است (طرحی برای آینده ایمن سایبری[2]، ۲۰۱۷).

با عنایت به مواردی که اشاره گردید، علت بیان مساله موردنظر ناشی از کاستی‌های موجود در خلق و ایجاد گروهی است که بتواند در مراکز دفاعی به تهدیدات رایانه‌ای پاسخ‌گویی فوری داشته باشد. برای این امر باید گروهی منسجم متشکل از خبرگان و متخصصان امنیت فناوری اطلاعات تشکیل گردد؛ از طرفی با توجه به ضرورت تشکیل این گروه، در ابتدای امر باید معماری این گروه فوریتی رایانه‌ای تهیه شود و گام مهم و نخست در معماری این گروه، شناسایی ابعاد آن است؛ لذا عدم شناسایی ابعاد در معماری کلان گروه پاسخ‌گویی فوریتی رایانه‌ای مراکز دفاعی، دغدغه اصلی این پژوهش و بدیهی است که با شناسایی ابعاد معماری، شناسایی مولفه‌ها و دیگر اجزای معماری کلان گروه پاسخ‌گویی فوریتی رایانه‌ای مراکز دفاعی، امکان‌پذیر خواهد شد.

هدف تحقیق

با توجه به اینکه تهدیدات رایانه‌ای به سرعت در حال گسترش و پیچیدگی بالا می‌باشند و نظر به اهمیت بسترهای موجود در زیرساخت‌های مراکز دفاعی و لزوم حراست از این زیرساخت‌ها و پاسخ‌گویی به تهدیدات مورد نظر، نیاز است تاگروهی منسجم از خبرگان و متخصصان حوزه امنیت فناوری اطلاعات، برای پاسخ‌گویی به تهدیدات رایانه‌ای مراکز

1- National Cyber Incident Response Plan.
2- Blueprint for a Secure Cyber Future.

دفاعی ایجاد گردد و برای این مهم، ابتدا لازم است تا یک معماری کلان برای گروه پاسخ-گویی مراکز دفاعی تهیه شود و گام مهم و نخست برای ارایه معماری کلان، شناخت و احصاء ابعاد آن است؛ لذا هدف اصلی تحقیق عبارتست از: ارایه ابعاد معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای برای مراکز دفاعی. در رسیدن به هدف اصلی، اهداف فرعی مانند: ۱. شناخت معماری‌های موجود و مقایسه بین آنها، ۲. شناسایی انواع تیم‌های پاسخ‌گویی فوریتی رایانه‌ای، ۳. شناخت چارچوب‌های موجود در معماری مراکز دفاعی از مهمترین اهداف فرعی در انجام این پژوهش می‌باشند.

۲-مبانی نظری تحقیق

۲-۱- رویدادها[1] و رخدادهای رایانه‌ای[2]

برای سازماندهی قابلیت پاسخ‌گویی به حوادث رایانه‌ای چند جنبه مهم باید تعریف گردد: یکی از آن‌ها تعریف واژه حادثه است. هر اتفاق قابل مشاهده در یک سامانه یا شبکه یک رویداد است. یک رویداد مثلاً اتصال کاربر به پرونده‌های مشترک و یا ارسال یک رایانامه است. یک رویداد مضر[3] دارای پیامد منفی است مثل طغیان بسته‌های شبکه، منگ شدن سامانه، استفاده غیرمجاز از داده‌های حساس و غیره. رخداد امنیتی رایانه‌ی[4] شامل تهدید حتمی به خط‌مشی امنیتی رایانه‌ای است. یک حادثه به‌دلایل فراوانی ممکن است اتفاق بیفتد (اسکارفن[5] و همکاران، ۲۰۱۸: ۲۰۹).

۲-۲- ماموریت‌ها و خدمات قابل ارائه گروه پاسخ‌گویی

خدماتی که عموماً توسط گروه پاسخ‌گویی به رخدادهای رایانه‌ای ارائه می‌شود را می‌توان در سه گروه رده‌بندی کرد: خدمات واکنشی، خدمات پیشگیرانه و خدمات مدیریت کیفیت امنیت (کیلکرس و همکاران[6]، ۲۰۱۶ : ۷۳).

خدمات انفعالی (واکنشی): این خدمات در پاسخ به یک درخواست یا اتفاق مانند گزارش از آسیب‌پذیری یک نرم‌افزار، تشخیص نفوذ در یک سامانه یا تشخیص رمزینه‌های مخرب انجام می‌شوند (همان).

1- Events.
2- Computer incident.
3- Adverse events.
4- Computer security incident.
5- Scarfone.
6- Killcrece.

خدمات غیرانفعالی (پیش‌گیرانه): این خدمات، راهنمایی‌ها و اطلاعات لازم برای کمک به آماده‌سازی، حفاظت و ایمن‌سازی سامانه‌های تحت پوشش رافراهم می‌کنند (همان: ۷٤).
خدمات مدیریت کیفیت امنیت: این خدمات، خدمات موجود و از قبل تعیین شده‌ای را تکمیل می‌نمایند، که مستقل از رسیدگی به رخدادها هستند و به صورت سنتی توسط دیگر بخش‌های سازمان همانند بخش‌های فناوری اطلاعات، بازرسی یا آموزشی ارائه می‌شوند (همان: ۷٦).

۳-۲- جرم‌شناسی دیجیتال و واکنش به حوادث[1]

یکی از اقداماتی‌که معمولاً توسط گروه پاسخ‌گویی به فوریت‌های رایانه‌ای انجام می‌شود و به‌عنوان یکی از خدمات آنها قابل تعریف است، بحث مربوط به جرم‌شناسی است؛ در این حوزه موارد مربوط به این امر، به دسته‌بندی‌های زیر تقسیم می‌گردد:
۱. جرم‌شناسی ویندوز[2]، ۲. جرم‌شناسی لینوکس[3]، ۳. جرم‌شناسی موبایل[4]، ٤. جرم‌شناسی حافظه[5]، ۵. تحلیل بدافزار[6].

در موارد فوق برای مثال در بحث ویندوز سوابق[7] رخداد ویندوز برای تشخیص حمله استفاده می‌شود؛ مهمترین نکته در خصوص جرم‌شناسی حافظه است. در این حالت، رفتار دودویی پرونده اجرایی بررسی می‌گردد به این دلیل که بعضی از برنامه‌ها بدون پرونده بوده و حتی یک بایت از آن برروی حافظه سخت نوشته نمی‌شود و با راه‌اندازی مجدد سامانه عامل، خودش را از طریق پردازش‌های سامانه عامل دوباره تولید می‌کند در خصوص تحلیل بدافزار، گروه تحلیل بدافزار، زبان‌های برنامه‌نویسی سامانه سطح پایین مانند زبان C را مسلط است و بدافزارها را شناسایی می‌کند (دپارتمان ای‌سی‌کانسیل[8]، ۲۰۱۷: ٤۸).

٤-۲- سازماندهی یک گروه پاسخ‌گویی کارآمد

شکل (۱) چهار عنصر اساسی یک گروه موثر و کارا را نشان می‌دهد و عبارتند از:

1- Digital Forensics and Incident Response (DFIR).
2- Windows forensic.
3- Linux forensic.
4- Mobile forensic.
5- Memory forensic.
6- Malware Analysis.
7 - Log.
8- Departmant of EC-COUNCIL.

۱) چارچوب عملیاتی: شامل ماموریت واضح و مشخص، محدوده عملکرد تعریف شده، ارتباط رسمی با دیگر تیم‌های سازمانی است. ۲) چارچوب سیاست‌گذاری و خدمت: شامل خدمات تعریف شده، اطلاعات واضح و مشخص، فرآیندهای مشخص برای جمع‌آوری، ثبت، پیگیری و بایگانی اطلاعات، خط‌مشی سازمانی فراگیر و واضح است. ۳) اطمینان کیفیت: شامل تعریف کیفیت سامانه، کنترل و اندازه‌گیری خاص مولفه‌های کیفی، گزارش و بررسی فرآیندها، فرآیندهای متوازن برای اطمینان از سطوح کیفیت، بازخوردهای مشتری و محدوده عملکرد گروه است. ٤) انعطاف پذیری و سازگاری: توانایی تطبیق با تهدیدات زمان واقعی[1] و آنهایی که در آینده اتفاق می‌افتد، پشتیبانی و تخصص حقوقی (استلویو[2] ، ۲۰۱۷ : ۱٤۷).

شکل (۱): عناصر یک گروه پاسخ‌گویی کارآمد (کیلکرس[3] و همکاران: ۲۰۱٦)

اجزای گروه‌های پاسخ‌گویی بر روی یکدیگر و طراحی آن تاثیر می‌گذارند. برای مثال، ماموریت گروه‌های پاسخ‌گویی با محدوده عملکرد و نیازمندی‌های آنها متاثر می‌گردد. منابع و چگونگی پراکندگی آنها، روی الگوی سازمانی مورد نیاز، خدمات فراهم شده و چگونگی اجرای ماموریت گروه تاثیر می‌گذارد (استلویو، ۲۰۱۷ : ۱٤۸).

۵-۲- تعریف معماری

در استاندارد IEEE STD ٦۱۰ ،۱۲ معماری این‌گونه تعریف شده است: ارائه توصیفی فنی از یک سامانه که نشان‌دهنده ساختار اجزا آن، ارتباط بین آنها و اصول و قواعد حاکم بر طراحی و تکامل آنها در گذر زمان باشد.

می‌توان گفت عواملی مانند ابعاد بزرگ، پیچیدگی زیادی نیازمندی خاص، طول عمر زیاد و انعطاف‌پذیری در برابر تغییرات می‌توانند منجر به لزوم معماری در یک سامانه

1- Real-time.
2- Stelvio.
6- Killcrece.

گردند و از معماران برای طراحی و ساخت کمک بگیرند. معماران افرادی مدبر، مدیر، هنرمند، کلان نگر، آینده‌نگر و باتجربه هستند که قادرند ضمن تشخیص نیازهای مشتریان -که عموماً به‌صورتی غیرفنی بیان می‌شوند - آنها را به زبانی علمی و استاندارد تبدیل کرده و زمینه‌های آفرینش واقعی تفکرات و خواسته‌های آنان را فراهم سازند؛ لذا می‌توان خصوصیات یک معمار را به‌صورت زیر بیان نمود:

- نگرش معمار، کلان و جامع بوده و از توجه زیاد به جزئیات خودداری می‌کند.
-برای بیان ایده‌ها و طرح‌ها از الگوها استفاده می‌کند.
-خصوصیات، رفتار و نحوه ارتباط اجزا سامانه را به‌خوبی می‌شناسد.
-با ترکیب مناسب اجزا موفق به طراحی سامانه مورد نظر می‌شود (شمس، ۱۳۸۳: ۱۱).

۳- روش تحقیق

این تحقیق کاربردی و توسعه‌ای است. نظربه لزوم وجود یک الگوی مناسب برای ارایه معماری گروه پاسخ‌گویی فوریتی رایانه‌ای و باتوجه به این‌که نتایج حاصله از پژوهش در حوزه دفاعی قابل بهره‌برداری است، در زمره تحقیقات کاربردی محسوب می‌شود. همچنین نظربه اهمیت تحقیق حاضر در پاسخ‌گویی به تهدیدات، این تحقیق قابلیت توسعه داشته که در نتیجه تحقیق حاضر توسعه‌ای می‌باشد.

روش تحقیق نیز آمیخته و ترکیبی از روش‌های توصیفی-تحلیلی و پیمایشی (مصاحبه و نخبگی) است.

جامعه آماری پژوهش حاضر شامل کلیه خبرگان، صاحب‌نظران و متولیان کشور و مراکز دفاعی که واجد ویژگی‌های زیر بوده‌اند:

۱- دارا بودن حداقل مدرک تحصیلی کارشناسی ارشد، ۲- دارا بودن جایگاه شغلی راهبردی فناوری اطلاعات و ۳- صاحب‌نظر و مجرب در مباحث راهبردی فناوری اطلاعات

در بررسی مقدماتی و طی مشورت با چند تن از خبرگان، حجم جامعه آماری از ٦٥ نفر تشکیل شده و با توجه به محدود بودن حجم جامعه آماری، نمونه آماری به جامعه آماری منطبق و روش نمونه‌گیری تمام شمار است.

نظر به این‌که محققین درپی تبیین راهکارهایی برای ایجاد امنیت و مقابله با تهدیدات رایانه‌ای بوده‌اند، پس از مطالعه مبانی نظری، تحلیل اسناد مربوطه، مصاحبه عمیق و هدفمند

با خبرگان و صاحب‌نظران در حوزه علوم رایانه‌ای دفاعی امنیتی کشور جمهوری اسلامی ایران و واکاوی پیشینه‌های موجود با تأکید بر چارچوب نظری تحقیق به الگوی مفهومی اولیه و سپس با استفاده از داده‌های گردآوری شده، به پرسش‌نامه محقق ساخته دست یافتند. سپس در یک جمع خبرگی ده نفره به تعیین شاخص‌های رواسنجی (روایی و پایایی) پرداختند و پس از تعیین شاخص‌ها جهت ممیزی طرح موردنظر به روش پیمایش عمل نمودند.

٤- مرور چارچوب‌های معماری سازمانی

١-٤- انواع معماری

معماری را می‌توان از جنبه‌های مختلف مورد بررسی قرار داد. یک طراح پایگاه داده، همیشه از معماری داده صحبت می‌کند، طراح نرم‌افزار، از معماری نرم‌افزار و مدیر ارشد فناوری اطلاعات سازمان از معماری اطلاعات و غیره. لذا معماری‌های مختلفی وجود دارد که در اینجا تنها اشاره‌ای کوتاه به آنها خواهد شد (درویش روحانی، ۱۳۹۰: ۷).

-معماری سامانه[1]: بالاترین مفهوم در دسته‌بندی‌های معماری، معماری سامانه می‌باشد. مفهوم معماری و معماری سامانه تقریبا یکسان است، زیرا برای بیان تعریف معماری در واقع معماری یک سامانه را تعریف کردیم که این سامانه هر چیزی می‌تواند باشد. لذا برای تعریف معماری یک سامانه خاص کافی است در تعریف معماری به‌جای اجزا، اجزا و موجودیت‌های سطح بالای سامانه مورد نظر را قرار دهیم؛ زیرا همان‌طور که گفتیم معماری، ساختارهای سطح بالای یک سامانه را شامل می‌شود (مهجوریان، ١٣٨٦: ٣٢).

-معماری نرم‌افزار[2]: جامعه مهندسی فناوری اطلاعات و ارتباطات نیز در مواجهه با پیچیدگی‌های روزافزون سامانه‌های اطلاعاتی، ناگزیر از حرکت به سمت معماری بوده است. این امر، هر چند با اندکی تأخیر، ولی با قوت و سرعت شروع شده و مباحث مربوط به آن به مرحله کاربردی رسیده‌اند. مفهوم معماری سامانه را می‌توان برای معماری سامانه-های نرم‌افزاری نیز گسترش داد؛ یعنی ساختار سطح بالای نرم‌افزار را به عنوان مفهوم معماری نرم‌افزار بیان کرد و برای غلبه بر پیچیدگی سامانه‌های نرم افزاری و طراحی آنها از معماری نرم‌افزار استفاده کرد (همان: ٣٤).

[1]- System Architecture.
[2]- Software Architecture.

-معماری سازمان[1]: سازمان‌های امروزی موجودات پیچیده‌ای هستند که توصیف فنی جنبه-های مختلف سامانه‌های اطلاعاتی آنها نیازمند به کارگیری معماری خاصی است که معماری سازمانی خوانده می‌شود. اگر بخواهیم تعریف معماری سازمان را از ٦١٠، ٢٠١٢ IEEE STD داشته باشیم باید گفت: معماری سازمانی عبارت است از تنظیم قوانین و مقرراتی برای تعریف یک ساختار واحد و منسجم که شامل اجزا، روابط بین آنها و چگونگی تعامل اجزا فوق با یکدیگر می‌باشد (همان: ۳۵).

بسته به این‌که معماری، در چه حوزه یا موضوعی از سازمان انجام شود، می‌توانیم معماری‌های مختلفی داشته باشیم، لذا انواع معماری سازمانی که به آنها لایه‌های معماری نیز اطلاق می‌شوند عبارتند از:

-معماری کسب و کار[2]: بالاترین سطح معماری سازمانی به حساب می‌آید و هدف این معماری شناسایی و توصیف حوزه‌های مأموریتی، خطوط مأموریتی و وظایف سازمانی است (همان: ۳۷).

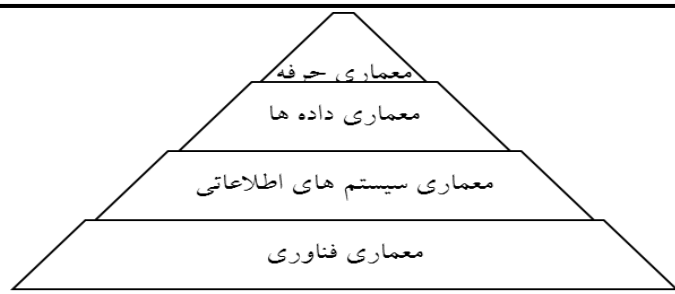
-معماری داده‌ها[3]: دومین سطح از معماری سازمانی محسوب می‌شود که به‌منظور توصیف سرفصل‌های اطلاعاتی، الگوهای منطقی داده‌ها و الگوهای فیزیکی داده‌ها به کار می‌رود (همان: ۳۹).

-معماری سامانه‌های اطلاعاتی[4]: سومین سطح معماری محسوب شده و به منظور توصیف فرآیندهای کاری، سامانه‌های اطلاعاتی، برنامه‌های کاربردی و روش‌های تعامل سامانه‌ها به کار می‌رود (همان: ٤٠).

-معماری فناوری[5]: آخرین سطح از معماری محسوب شده و شامل الگوهای مرجع فنی و استانداردهای فنی است که باید در سطح سازمان رعایت شوند (همان: ٤٢).

ارتباط میان این چهار نوع معماری به صورت هرمی است که معماری کسب و کار در نوک هرم، پایه‌ای است برای معماری داده‌ها و معماری داده‌ها پایه‌ای برای معماری سامانه‌های اطلاعاتی و معماری سامانه‌های اطلاعاتی پایه‌ای برای معماری فناوری می‌باشند (درویش روحانی، ۱۳۹۰: ۹-۷).

1- Enterprise Architecture.
2- Business Architecture.
3- Data Architecture.
4- Applications Architecture.
5- Technology Architecture.



شکل (۲): لایه‌های معماری سازمانی (درویش روحانی، ۱۳۹۰)

چه داده‌هایی برای حمایت از فرآیندهای سازمان لازم هست؟ چه سامانه‌هایی برای مدیریت داده‌های فوق لازم هستند؟ چه فناوری‌هایی برای حمایت از سامانه‌های فوق لازم است؟

سازمان[1]: یک سازمان شامل کارکنان، اهداف، فرآیندها، اطلاعات و فناوری‌ها است؛ وظایف کاری را انجام می‌دهد؛ دارای یک ساختار سازمانی تعریف شده است که معمولاً در جاهای مختلف توزیع شده است؛ به رخدادهای داخلی و خارجی پاسخ می‌دهد؛ دارای یک راهبرد برای فعالیت‌هایش است؛ محصولات یا خدماتی را برای مشتریان با مخاطبانش فراهم می‌کند (شمس و یادآور نیک‌روش، ۱۳۸٦: ۳۸).

۲-٤- چارچوب‌های معماری سایبری کشورها

در بررسی مقدماتی، ابتدا تمامی الگوهای مرتبط با معماری فضای سایبر، شناسایی شده و در ادامه، مطابق آنچه در جدول (۱) نمایش داده شده است.

جدول (۱): لیست الگوهای معماری (موسسه توسعه معماری سازمانی[2]، ۲۰۱۷)

	عنوان الگوی معماری و تحلیل امنیت	ارائه‌دهنده	حوزه قلمرو
۱	راهنمای چارچوب امنیت فضای سایبر ملی	مرکز مشارکتی نخبگان دفاع سایبری ناتو	امنیت فضای سایبر ملی
۲	الگوی برآورد تهدید سایبری	قرارگاه پدافند سایبری ج.ا.ایران	
۳	الگوی معماری TOGAF	مؤسسه بین‌المللی استاندارد (ISO)	امنیت فضای سایبر سازمانی
۴	الگوی معماری FEAF	مؤسسه بین‌المللی استاندارد (ISO)	
۵	الگوی معماری Zachman	مؤسسه بین‌المللی استاندارد (ISO)	
۶	الگوی معماری Gartner	مؤسسه بین‌المللی استاندارد (ISO)	

1- Enterprise.
2- Institute for Enterprise Architecture Developments.

۷	الگوی معماری SABSA	مؤسسه بین‌المللی استاندارد (ISO)	
۸	سیستم مدیریت امنیت اطلاعات	مؤسسه بین‌المللی استاندارد (ISO)	
۹	سنجش مدیریت امنیت اطلاعات	مؤسسه بین‌المللی استاندارد (ISO)	
۱۰	مدیریت مخاطرات امنیت اطلاعات	مؤسسه بین‌المللی استاندارد (ISO)	
۱۱	الگوی معماری برای ارتباطات انتها-به-انتها	اتحادیه بین‌المللی مخابرات (ITU)	امنیت شبکه‌های ارتباطی
۱۲	چارچوب بهبود امنیت سایبری زیرساخت‌های حیاتی	مؤسسه استاندارد و فناوری آمریکا (NIST)	

۳-٤- مقایسه کلی چارچوب‌های مهم معماری

در مقایسه سه چارچوب مهم معماری که در موارد زیادی مورد استفاده قرار گرفته‌اند می‌توان موارد زیر را که از مقایسه نقطه نظرات و دیدگاه‌ها و میزان پوشش جنبه‌های مختلف کاری به دست آمده‌اند را که در جدول (۲) آمده است مهم دانست (همان).

-چارچوب FEAF مسأله را از سه جنبه داده، عملکرد و شبکه، از دیدگاه‌های مختلف بررسی می‌کند.

-چارچوب TEAF مسأله را از چهار جنبه داده، عملکرد، شبکه و کنش‌گر و از پنج دیدگاه بررسی می‌کند.

- چارچوب C4ISR با پیشینه نظامی خود مسأله را از سه جنبه داده، عملکرد و شبکه و از پنج دیدگاه مورد بررسی قرار می‌دهد و در بعضی موارد با توجه به نیازی که نسبت به نگرش‌ها دارد، بعضی از آنها را حذف می‌کند.

جدول (۲): مقایسه چارچوب‌های کاری (موسسه توسعه معماری سازمانی[1]، ۲۰۱۷)

FEAF	DODAF	TEAF	TOGAF	ZACHMAN
ماتریس بر مبنای چارچوب زکمن شامل ۳ ستون داده نرم-افزارهای کاربردی و فناوری	سه دیدگاه عملیاتی، سامانه‌ای و فنی	ماتریس شبیه زکمن شامل چهار ستون وظیفه ای، اطلاعاتی، ساختاری و زیرساختارها	چهار لایه اصلی کسب و اجاره داده، نرم‌افزارهای کاربردی و فناوری	دیدهای پایه معماری
توضیح بسیار خلاصه در خصوص محصولات معماری	توضیحات کامل برای تمام محصولات	توضیحات کامل بر محصولات دودف[2] همچنین تشریح برنامه-	توضیح مفیدی موجود نمی-باشد	مشخصات کامل و مشروح محصولات

[1]- Institute for Enterprise Architecture Developments.
[2]- DODAF.

		ریزی و طرح انتقال		
تبیین رابطه معماری سازمانی با دیدگاه راهبردی و اهداف ماموریت	راهبردهای کسب و کار به عنوان ورودی فاز دیدگاه معماری در نظر گرفته شده است.	به عنوان یک محصول مجزا (نقشه راه) در نظر گرفته شده است.	به بعضی محصولات نیز اشاره شده ولی محصول مجزائی برای آنها در نظر گرفته نشده است.	به‌طور کامل تبیین شده است
تهیه قوانین معماری	وجود دارد.	فقط لیست قوانین وزارت خزانه داری و مسئولیت ادارات آورده شده است.	قوانین به عنوان جزئی از توصیف محصولات معماری دیده شده	برای صفات خود چارچوب معماری فدرال تهیه شده است.
محصولات برای تعیین استانداردها	در قالب الگوی مرجع فناوری (TRM)	تحت عنوان نمایه استانداردها	وجود دارد (TV-1)	وجود ندارد.
بحث در خصوص ملاحظات امنیتی	موضوع امنیت مورد بحث قرار گرفته است	دیده شده است	به‌طور خلاصه در انتخاب محصولات	خیر
بحث پیرامون راهبرد گذار و تعریف محصولات برنامه‌گذار	در قالب فاز برنامه‌ریزی گذار (مهاجرت)	در قالب یک محصول مشخص	مقداری بحث شده	بررسی شده ولی نه به‌طور کامل و مشخص
بحث در خصوص مخزن معماری	راهنمایی‌هایی وجود دارد	مسئولیت‌های مربوط به آن تعیین شده است	بحث شده	نیاز به مخزن گفته شده
روش شناسی یا راهنمای اجرای معماری سازمانی	دارای روش توسعه معماریADM است	در قالب موضوعاتی چون راهبرد معماری سازمانی	٦ گام کلان بدون ورود به جزئیات ارائه شده	به روش‌شناسی و برنامه‌ریزی معماری سازمانی

٤-٤- چارچوب معماری بخش دفاع

درپی گسترش معماری سازمانی و تأیید قابلیت‌های راهبردی آن برای اغلب سازمان‌های بزرگ دفاعی در سطح دنیا (مانند وزارت دفاع ایالات متحده و نیز وزارت دفاع بریتانیا) به توسعه چارچوب‌های معماری سازمانی بومی پرداخته‌اند تا بتوانند از قابلیت‌های معماری سازمانی در حوزه‌ی دفاعی بهره‌مند گردند. شاید این‌گونه به‌نظر برسد که سازمان‌های دفاعی کشور ما نیز می‌توانند با به کارگیری چارچوب‌هایی نظیر چارچوب معماری وزارت دفاع ایالات متحده که مختص حوزه دفاعی توسعه یافته‌اند، پاسخگوی نیاز خود در زمینه معماری سازمانی باشند، اما بنابر آمار؛ به‌دلیل وجود تفاوت‌های عمده میان سازمان‌های مختلف رشد یافته در کشورهای گوناگون، نمی‌توان یک چارچوب معماری حوزه‌ی دفاعی را برای تمامی سازمان‌های دفاعی تجویز نمود. ازاین‌رو بخش قابل توجهی از سازمان‌ها از

چارچوب عمومی زکمن که یک چارچوب عام است، استفاده نموده و چارچوب معماری مختص خود را توسعه داده‌اند (پژوهشکده توسعه معماری سازمانی[1]، ۲۰۱۷ : ۲۱۷).

چارچوب‌های معماری سازمان‌های دفاعی، نظیر دودف، از طریق روشی که متشکل از مراحل و فعالیت‌های خاصی می‌باشند، توسعه می‌یابند. بااین‌که اطلاعات مشروحی درباره چارچوب‌های معماری در دسترس است، اما با این حال مستندات بسیار کمی درباره روش توسعه‌ی آنها وجود دارد. البته این امر منطقی و قابل قبول است، زیرا قابلیت اصلی سازمان‌های توسعه دهنده‌ی چارچوب‌های معماری، آگاهی و اشراف آنها بر چگونگی توسعه این چارچوب‌ها می‌باشد. نهایتاً آنچه به‌راحتی در اختیار دیگران قرار داده می‌شود، خروجی کار است و نه روش دست‌یابی به آن خروجی، یکی از منابعی که مختصر به تشریح روش توسعه‌ی چارچوب‌های معماری پرداخته است، کتاب «بقا در جنگل چارچوب‌های معماری» می‌باشد (شکرمن[2]، ۲۰۱۷ : ۱۲۳). شکرمن، در فصل یازدهم این کتاب مختصراً به روش توسعه‌ی یک چارچوب معماری پرداخته است. وی چند مرحله 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 فنون الگوسازی متناسب؛ ٥) اجرای آزمایشی چارچوب توسعه یافته؛ ٦) تعیین تجربیات حاصل از اجرا و اصلاح نمودن چارچوب و فرآیندهای مربوط به آن.

٥-٤- چارچوب معماری سازمانی فدرال

چارچوب معماری سازمانی فدرال توسط شورای مدیران ارشد اطلاعاتی دولت فدرال ایالات متحده آمریکا تهیه و تنظیم شد (شمس و یادآور نیک‌روش، ١٣٨٦: ٣٥). این معماری شامل رهنمودهایی برای معماران سامانه‌های اطلاعاتی در توصیف مأموریت‌های چند سازمانی در دولت فدرال و چارچوب یک ساز و کار سازمان‌دهی برای مدیریت، توسعه و نگهداری توصیفات معماری است. همچنین ساختاری را برای سازمان‌دهی منابع اطلاعاتی و تشریح و مدیریت فعالیت‌های معماری سازمانی فدرال ارائه می‌دهد. فرآیند

1- Institute for Enterprise Architecture Developments.
2- Schekkerman.

معماری سازمانی فدرال هشت مؤلفه اساسی دارد و عبارتند از: پیشران‌های معماری، جهت‌گیری راهبردی، معماری فعلی فناوری اطلاعات سازمان، معماری مطلوب فناوری اطلاعات سازمان، الگوی معماری، فرآیند گذار، بخش‌های معماری و استانداردهای فناوری اطلاعات.

٦-٤- چارچوب فرماندهی،کنترل، ارتباطات،کامپیوتر، هوشمندی ، نظارت و اکتشاف[1]

در فوریه ۲۰۰٤ وزارت دفاع نسخه کامل این چارچوب را ارائه نمود. هدف از تدوین این چارچوب این بود که چون سازمان‌های وزارت دفاع آمریکا در سطح دنیا معماری‌های مختلفی را جهت نمایش عملیات نظامی خویش تولید و استفاده می‌نمودند و این معماری-ها از لحاظ محتوایی و قالب مستندات با هم متفاوت بوده و به روش‌های مختلفی معماری را توصیف می‌کردند، برای این‌که بتوان این معماری‌ها را با هم مقایسه کرده و آنها را با هم تجمیع نمود، باید یک چارچوب معماری تدوین و سازمان‌های تابعه را ملزم به استفاده از این چارچوب برای توصیف معماری نمود. این چارچوب برخلاف زکمن که شامل شش دیدگاه می‌شد از سه دیدگاه تشکیل شده که با هم تفاوت عمده دارند. این سه دیدگاه عبارتند از: دیدگاه عملیاتی، دیدگاه سامانه ای و دیدگاه تکنیکی (همان: ۳۷).

۷-٤- چارچوب معماری وزارت دفاع ایالات متحده[2]

چارچوب معماری فرماندهی، کنترل، ارتباطات، کامپیوتر، جاسوسی، مراقبت و شناسایی که در سال ۱۹۹۹ توسط وزارت دفاع ایالات متحده ارائه گردید، از مهم‌ترین چارچوب‌های معماری سازمان های دفاعی است (ویلزینسکی[3]، ۲۰۱۷: ۷۹). از این رو، روش توسعه‌ی چارچوب‌های معماری سازمان‌های دفاعی بر مبنای تحلیل این چارچوب ارائه می‌گردد. این چارچوب در ابتدا، برای سامانه‌های ارتباطی، اطلاعاتی در صحنه‌ی عملیات نظامی تدوین شده بود و سپس جای خود را به عنوان یک راه حل ممتاز برای پرداختن به معماری در حوزه‌های دیگر باز کرد، (سوول[4]، ۲۰۱۷ : ۱۱٤) در سال ۲۰۰۳ وزارت دفاع ایالات متحده پس از توسعه‌ی دو نسخه از چارچوب معماری کنترل و فرماندهی هوشمند، چارچوب معماری دودف را ارائه نمود. به عبارتی، چارچوب دودف نسخه به روز شده و

1- Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance(C4ISR)
2- DoDAF.
3- Wilczynski.
4- Sowell.

تغییر نام‌یافته چارچوب کنترل و فرماندهی می‌باشد. حوزه‌ی کاربرد این چارچوب از فرماندهی، کنترل، ارتباطات، رایانه، جاسوسی، مراقبت و شناسایی، به تمامی هدف دودف تعریف مفاهیم و الگوهای قابل استفاده در شش فرآیند اصلی وزارت دفاع است:

۱- ادغام و توسعه قابلیت‌های مشترک[1] ۲- برنامه‌ریزی، بودجه‌بندی و اجرا[2] ۳- سامانه اکتساب دفاع[3] ٤- مهندسی سامانه[4] ٥- برنامه‌ریزی عملیاتی[5] ٦- مدیریت نمونه کارها قابلیت[6] در حوزه‌های مختلف توسعه یافته است (دپارتمان دفاعی[7]، ۲۰۱۷: ۱۱).

نسخه‌ی ۲.۲ این چارچوب دارای ویژگی‌های زیر است:

۱) دیدگاه کلی، نمای کلی از کل معماری است که خلاصه‌ای اجرایی از معماری را شامل می‌شود و هم نتیجه‌گیری، توصیه‌ها و تعاریف مفصلی را برای تمام اصطلاحات استفاده شده در معماری ارائه می‌دهد. این دیدگاه توسط همه ذی‌نفعان معماری استفاده می‌شود؛

۲) دیدگاه قابلیت‌ها، مربوط به جنبه‌های راهبردی سازمان است، از جمله چشم‌انداز سازمان و اهداف آن، توانایی‌های لازم برای دست‌یابی به اهداف، روابط بین توانایی‌ها و تغییر آنها در طول زمان و این‌که چه سازمان‌هایی از این قابلیت‌ها استفاده می‌کنند. این دیدگاه مورد توجه اصلی مدیریت اجرایی است؛

۳) دیدگاه اطلاعات و اطلاعات مربوط به توصیف داده‌های سازمانی مشترک و ساختار یافته است. دیدگاه‌ها در این دیدگاه، نمایانگر الگوهای مفهومی، منطقی یا فیزیکی داده‌های مشترک هستند. این دیدگاه، بسته به سطح جزئیات موجود، مورد توجه هر یک از مدیران تجاری، پرسنل عملیاتی و پرسنل فناوری اطلاعات است؛

٤) از نظر عملیاتی اطلاعات مربوط به عملیات سازمان، شامل مفهوم عملیات یا مأموریت عملیاتی، فرآیندهای تجاری یا مأموریت، مجریان، جریان اطلاعات بین مجریان و فعالیت‌های فرآیندها و سازمان‌های درگیر ارائه می‌شود. دیدگاه عملیاتی اطلاعاتی راجع به رفتارهای عملیاتی شرکت ارائه می‌دهد: عناصر عملیاتی رفتار دولت، سناریوهای اصلی

1- Integration and development of common capabilities (I&DCC).
2 -Joint Capabilities Integration and Development (JCIDS).
3- Planning, Programming, Budgeting, and Execution (PPBE)
4- Defense Acquisition System (DAS).
5- Systems Engineering (SE).
6- Capability Portfolio Management(CPM)
7 -Department of Defense.

عملیاتی و قوانین تجاری یا عملیاتی را شامل می‌شوند. این دیدگاه مورد توجه اصلی مدیر تجارت و پرسنل عملیاتی است؛

۵) دیدگاه پروژه مربوط به پروژه‌های مختلف توسعه‌ای است که در حال حاضر یا برای شرکت برنامه‌ریزی شده است. دیدگاه‌های موجود در این دیدگاه مشخص می‌کند که سازمان‌ها چه پروژه‌هایی را مدیریت می‌کنند، زمان‌بندی تحویل مجموعه پروژه‌ها و وابستگی بین تحویل‌ها چیست و چه پروژه‌هایی اجزای کدام قابلیت را ارائه می‌دهند. این دیدگاه مورد توجه مدیران و مدیران تجاری است؛

٦) دیدگاه سرویس و خدمات، اطلاعاتی را در مورد کسب و کار یا خدمات فناوری اطلاعات شرکت ارائه می‌دهد. این اطلاعات می‌تواند شامل موارد زیر باشد: عملکردهای سرویس، رابط‌های سرویس و توافقنامه‌های سطح خدمات[1] چیست. نحوه اتصال خدمات به یکدیگر؛ منابع مبادله شده؛ و زمان دسترسی به خدمات جنبه‌های رفتاری خدمات نیز قابل توصیف است. این دیدگاه مورد توجه مدیران تجاری (برای خدمات کسب و کار) و پرسنل فناوری اطلاعات (برای خدمات فناوری اطلاعات) است؛

۷) دیدگاه استانداردها مربوط به استانداردهای فنی و سامانه‌ها یا خدماتی است که این استانداردها در مورد آنها اعمال می‌شود. استانداردهای فنی بر اساس الگوی مرجع فنی[2] تنظیم می‌شوند. استانداردها ممکن است تاریخ‌های مرتبط با خود را داشته باشند: چه زمانی استاندارد باید برآورده شود و چه زمانی استاندارد دیگر اعمال نخواهد شد و چه استاندارد نوظهوری جایگزین آن می‌شود. این دیدگاه برای پرسنل فناوری اطلاعات و مدیران تجاری درگیر مناسب است؛

۸) دیدگاه سامانه‌ای، اطلاعاتی در مورد سامانه‌های شرکت ارائه می‌دهد. اطلاعات شامل سامانه‌ها و چگونگی ارتباط آنها با یکدیگر است، چه منابعی بین آنها جریان می‌یابد، چه زمانی در دسترس قرار می‌گیرند و چه فعالیت‌هایی پشتیبانی می‌شوند. پرسنل فناوری اطلاعات به این دیدگاه توجه دارند (بلمن[3]، ۲۰۱۸ : ۲۰).

به دلیل وجود معماری‌های بخشی که در بخش‌های مختلف سازمان‌های دفاعی ایالات متحده و در سطوح مختلف توسعه یافته‌اند، دودف به جای ایجاد تحولات پایه‌ای در این

1- SLA.
2– TRM.
3- Bellman.

معماری‌های بخشی، بر اساس استفاده‌ی بهینه از معماری‌های بخشی موجود و ایجاد تعامل مؤثر میان آنها طراحی گردیده است. از این رو، دودف پشتیبانی از هر دو نوع معماری متحد و یکپارچه را مورد توجه قرار داده است. هرچند که به دلیل وجود معماری‌های بخشی تمرکز بیشتری بر معماری متحد شده است و دارای ویژگی‌های زیر است:

۱- پشتیبانی از فرآیند تصمیم‌گیری در سازمان‌های دفاعی به ویژه در محیط رزم مبتنی بر شبکه؛ ۲- هم‌راستایی چارچوب با چشم انداز وزارت دفاع؛ ۳- انطباق با دودف نسخه ۱.۰ ٤- پشتیبانی از معماری متحد و یکپارچه؛ ۵- توجه بیشتر به معماری سرویس‌گرا؛ ٦- ارائه رهنمودهای بیشتر جهت تشریح تغییرات ایجاد شده در محیط، فرهنگ، دکترین و فرآیندها؛ ۷- چابکی بیشتر در توسعه‌ی معماری سازمان؛ ۸- انطباق با رزم مبتنی بر شبکه؛ ۹- اثربخشی و انعطاف بیشتر (همان: ۲۵).

مراحل توسعه‌ی چارچوب: با توجه به توضیحات و تفاسیری که در مستندات دودف قید گردیده است، می‌توان برخی مراحل و فعالیت‌های انجام شده جهت توسعه‌ی این را شناسایی نمود که در شکل (۳) ترسیم شده است:

شکل (۳): توسعه چارچوب معماری درون سازمانی‌های دفاعی (برلی برمن، ۲۰۱۸)

۸-٤- معماری خدمات‌پایه جاکوبز

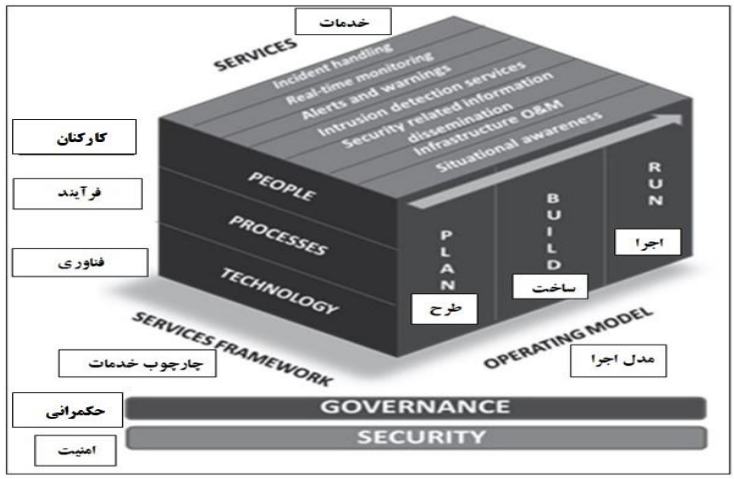
در معماری پییرجاکوبز (جاکوبز و همکاران، ۲۰۱۹: ٦۷) الگوی خدمات‌پایه که در سازمان‌های دفاعی کاربرد داشته، سرویس‌ها و خدماتی که محوریت دارند، در جدول (۳) آمده است:

جدول (۳): خدمات گروه پاسخ‌گویی در الگوی جاکوبز (جاکوبز و همکاران، ۲۰۱۹)

ردیف	خدمات گروه پاسخ‌گویی
۱	رسیدگی به رخداد
۲	پایش بلادرنگ
۳	هشدار و اخطار
٤	خدمات کشف نفوذ
٥	انتشار اخبار مرتبط با امنیت اطلاعات
٦	نگهداری و عملیات زیرساخت
۷	آگاهی وضعیتی

در الگوی ارایه شده توسط جاکوبز، الگوی اجرایی براساس طرح[1]، ساخت[2]، اجرا[3] آمده است و در یال دیگر مکعب، به فناوری، فرآیند و کارکنان اشاره دارد. این معماری، تفکیک مناسبی ازخدمات و لایه‌ها دارد و ارتباط بین مولفه‌ها و ابعاد به خوبی تبیین شده است. از نظر جاکوبز دولت و حاکمیت و امنیت، مانند چتری بر همه ابعاد پوشا هستند و به‌همین دلیل این دو را مجزا از سایر مولفه‌های مکعب در نظر می‌گیرد. این الگو براساس خدمت پایه طراحی شده و به‌صورت شکل (٤) است (پییرجاکوبز و همکاران، ۲۰۱۹: ٦۷).

[1]- PLAN.
[2]- BUILD.
[3]- RUN.



شکل (٤): لایه‌های معماری سرویس پایه جاکوبز (جاکوبز و همکاران، ۲۰۱۹)

۵- معماری پیشنهادی گروه پاسخ‌گویی فوریتی رایانه‌ای مراکز دفاعی

باتوجه به معماری‌های پیشین و مقایسه هر یک و نیز کارکرد آنها، برای اینکه معماری ارایه شده، جامع‌نگر بوده و ظرفی برای تمامی مولفه‌ها باشد از همان معماری مرجع که در شکل زیر آمده است بهره می‌بریم. این معماری که یک معماری محقق یافته و کلان‌نگر است. در معماری همه جوانب امر در نظر گرفته خواهد شد و به ماموریت‌ها، اهداف و کارکرد، فرآیندها، ساختار و سازمان و فناوری‌ها و تجهیزات می‌پردازد و بر اساس همین معماری که همانند ظرفی عمل می‌نماید، همگی مولفه‌ها و شاخص‌های مربوط به معماری قابل احصاء خواهد بود (شکل۵).

در این معماری، همه لایه‌ها و ابعاد به‌صورت کلان پرداخته می‌شود و با عنایت به این موضوع، همه این موارد مورد بررسی قرار خواهد گرفت و در جدول‌های صفحات بعد همه این ابعاد مورد بررسی قرار خواهند گرفت.

۱-۵ تعیین ارکان اصلی الگوی پیشنهادی

مواردی که می‌تواند به‌عنوان ارکان اصلی در معماری مورد نظر سازمان‌های کشور قرار گیرد در نمای شکل زیر ترسیم شده است. پس از تعیین عومل موثر حاصل از کار تحقیقاتی، در یافتن ابعاد معماری برای پاسخ‌گویی رخدادهای رایانه‌ای، می‌توان آن‌ها را به‌صورت منظمی دسته‌بندی و مرتب نمود که در زیر به آن پرداخته می‌شود:

۱.ماموریت و خدمات: اصولا قبل از انجام هر اقدامی باید ماموریت محوله و کارکردی که یک سازمان یا یک گروه باید نقش خود را در آن ایفا نماید مشخص گردد؛

۲. اهداف و کارکرد: نقش گروه، با هدف پاسخ‌گویی به رخدادها، محافظت از منابع و جلوگیری از ورود غیرمجاز به شبکه، بهبود شبکه پس از مرتفع نمودن رخداد به‌وجود آمده و شناسایی و پایش مجرمان شکل خواهد گرفت؛

۳. فرآیندها: از برنامه‌ریزی، کنترل و اجرا تا مدیریت مخاطرات و تحلیل و رصد و پایش به منظور انسجام‌بخشی در تصمیمات کلان در گروه فرآیندها قرار می‌گیرند؛

٤. فناوری: اجزای خدمات و سامانه‌ها و نیز تجهیزات سخت‌افزاری و نرم‌افزاری با توجه به سنخیت در یک گروه قرار می‌گیرند؛

۵. ساختار و سازمان: مباحث منابع انسانی که شامل نیروی انسانی، آموزش، اطلاع‌رسانی ظرفیت‌سازی، مدیریت دارایی‌ها و تعیین الگوی استقرار سازمانی و کنترل دسترسی‌ها تجمیع و در یک گروه قرار گیرد؛

٦. تنظیم مقررات و حقوقی نیز بهتر است به عنوان رکنی مستقل قرار گیرد تا بتواند به – عنوان بازوی اجرایی در کنار بخش‌های مختلف قرار گیرد؛

۷. بخش امنیت که بخش مستقلی است و باید در همه ارکان گروه حضور داشته باشد؛

۸.. بخش مدیریت و فرماندهی نیز به‌عنوان پوش همه ارکان خواهد بود.

٦- تجزیه و تحلیل داده‌ها

پس از پیشنهاد این ابعاد به عنوان ابعاد معماری کلان گروه پاسخ‌گویی فوریتی مراکز دفاعی، در قالب یک پرسش‌نامه، نظر خبرگان دفاعی در حوزه سایبری اخذ و با تحلیل نتایج آماری پرسش‌نامه، بااستفاده از نرم‌افزار اس‌پی‌اس‌اس، نتایج سوال اصلی حاصل گردید.

٦-١ بررسی ابعاد در معماری کلان گروه پاسخ‌گویی

سوال مطرح شده از خبرگان دفاعی این است: آیا ابعاد زیر در حوزه "معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای" جای می‌گیرند؟

جدول (٤)-ابعاد معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای

ردیف	بعد	جای نمی‌گیرد	بسیار کم	کم	متوسط	زیاد	بسیار زیاد	نمره از ۱۰۰
۱	ماموریت	1.5	0	0	6.2	32.3	60	89.6
۲	اهداف و کارکردها	0	1.5	0	6.2	40	52.3	88.4
۳	فرآیندها	0	0	1.5	12.3	33.8	52.3	87.4
٤	ساختار و سازمان	0	0	0	12.3	24.6	63.1	90.2
٥	فناوری	0	0	1.5	7.7	27.7	63.1	90.4
٦	مدیریت و فرماندهی	1.5	0	0	3.1	26.2	69.2	92
۷	امنیت	0	0	0	4.6	26.2	69.2	93
۸	تنظیم مقررات و حقوقی	0	1.5	0	7.7	33.8	56.9	89

بر اساس جدول فوق نتایج زیر قابل استخراج است:

- حدود ٦۰ درصد از پاسخ‌گویان، ماموریت را در سطح بسیار زیاد و حدود ۳۲ درصد آن را در سطح زیاد از ابعاد معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای دانسته‌اند به‌طوری‌که میانگین نمره این گویه ۸۹/٦ از ۱۰۰ می‌باشد.

–حدود ۵۲ درصد از پاسخ‌گویان، اهداف و کارکردها را در سطح بسیار زیاد و حدود ۴۰ درصد آن را در سطح زیاد از ابعاد معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای دانسته‌اند به‌طوری‌که میانگین نمره این گویه ۸۸/٤ از ۱۰۰ می‌باشد.

–حدود۵۲ درصد از پاسخ‌گویان، فرآیندها را در سطح بسیار زیاد و حدود۳٤ درصد آن را در سطح زیاد از ابعاد معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای دانسته‌اند به‌طوری‌که میانگین نمره این گویه ۸۷/٤ از ۱۰۰ می‌باشد.

– حدود ٦۳ درصد از پاسخ‌گویان، ساختار و سازمان را در سطح بسیار زیاد و حدود ۲۵ درصد آن را در سطح زیاد از ابعاد معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای دانسته‌اند به‌طوری‌که میانگین نمره این گویه ۹۰/۲ از ۱۰۰ می‌باشد.

– حدود ٦۳ درصد از پاسخ‌گویان، فناوری را در سطح بسیار زیاد و حدود ۲۸ درصد آن را در سطح زیاد از ابعاد معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای دانسته‌اند به‌طوری‌که میانگین نمره این گویه ۹۰/٤ از ۱۰۰ می‌باشد.

– حدود ٦۹ درصد از پاسخ‌گویان، مدیریت و فرماندهی را در سطح بسیار زیاد و حدود ۲٦ درصد آن را در سطح زیاد از ابعاد معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای دانسته‌اند به‌طوری‌که میانگین نمره این گویه ۹۲ از ۱۰۰ می‌باشد.

–حدود ٦۹ درصد از پاسخ‌گویان، امنیت را در سطح بسیار زیاد و حدود ۲٦ درصد آن را در سطح زیاد از ابعاد معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای دانسته‌اند به‌طوری‌که میانگین نمره این گویه ۹۳ از۱۰۰ می‌باشد.

– حدود ۵۷ درصد از پاسخ‌گویان، تنظیم مقررات و حقوقی را در سطح بسیار زیاد و حدود ۳٤ درصد آن را در سطح زیاد از ابعاد معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای دانسته‌اند به‌طوری‌که میانگین نمره این گویه ۸۹ از ۱۰۰ می‌باشد.

در مجموع از نظر پاسخ‌گویان هر ۸ بعد با میانگین نمره بیش از ۸۸ از ۱۰۰ در حوزه "معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای" بیان شده به‌نحوی‌که بیشترین نمره را مربوط به فناوری و ساختار و سازمان دانسته‌اند.

همان‌طور که ملاحظه می‌شود بیشترین میانگین نمره مربوط به بعد اهداف و کارکردها با میانگین ۸٦/۸ از ۱۰۰ بوده، به‌نحوی‌که مقدار میانه آن برابر ۸۸/۰ گزارش شده که این موضوع بیانگر آن است که نیمی از پاسخ‌گویان نمره بیشتر از ۸۸/۰ را به این بعد داده و نیمی دیگر کمتر از این نمره را اظهار داشته‌اند.

٦-۲ شاخص‌های مرکزی و پراکندگی ابعاد

شاخص‌های مرکزی و پراکندگی ابعاد هشت‌گانه ماموریت، اهداف و کارکردها، فرآیندها، ساختار و سازمان، فناوری، تنظیم مقررات و حقوقی، امنیت و مدیریت و فرماندهی بر اساس گویه‌های آنان به شرح جدول (۵) می‌باشد:

جدول (۵)- شاخص‌های مرکزی و پراکندگی ابعاد معماری کلان گروه پاسخ‌گویی به فوریت‌های رایانه‌ای مراکز دفاعی

ابعاد	میانگین	میانه	انحراف معیار	چولگی	کشیدگی	کمینه	بیشینه
اهداف و کارکردهای تیم پاسخگوی فوریت‌های رایانه‌ای	86.8	88.0	11.3	-1.5	3.7	40.0	100
ساختار و سازمان تیم پاسخگوی فوریت‌های رایانه‌ای	85.9	86.7	10.7	-1.0	1.3	50.0	100
فناوری تیم پاسخگوی فوریت‌های رایانه‌ای	85.7	88.6	11.8	-0.9	0.9	45.7	100
ماموریت پاسخگوی فوریت‌های رایانه‌ای	85.4	88.0	10.5	-1.3	2.2	52.0	100
فرآیندهای پاسخگوی فوریت‌های رایانه‌ای	84.1	85.0	12.2	-0.9	0.9	42.5	100
تنظیم مقررات و حقوقی تیم پاسخگوی فوریت‌های رایانه‌ای	۸۳,۷	۸٤	۱۰,٥	-1.0	1.3	50.0	100
امنیت تیم پاسخگوی فوریت‌های رایانه‌ای	85.7	88.6	11.8	-0.8	0.9	45.7	100
مدیریت و فرماندهی تیم پاسخگوی فوریت‌های رایانه‌ای	85.4	88.0	10.5	-1.1	2.2	52.0	100

انحراف معیار این بعد برابر ۱۱/۳ گزارش شده و این موضوع بیانگر آن است که اکثر مشاهدات حدود ۱۱/۳ نمره از میانگین بعد اهداف و کارکردها که برابر ۸۶/۸ است فاصله دارند. چولگی بیانگر چگونگی انحراف از نرمال بودن توزیع دارد به این صورت که اگر مقدار آن منفی باشد یعنی توزیع مشاهدات چوله به چپ و اگر مقدار آن مثبت باشد یعنی توزیع مشاهدات چوله به راست است. چوله به چپ یعنی بیشتر داده‌ها از میانگین بیشتر هستن و چوله به راست یعنی بیشتر داده‌ها از میانگین کمتر هستند. این بعد چوله به چپ بوده (۱/۵-) که این موضوع بیانگر آن است بیشتر پاسخ‌گویان نمره بیشتر از .میانگین را به این بعد داده‌اند. کشیدگی بیانگر میزان تمرکز و پراکندگی مشاهدات را نشان می‌دهد. به این‌صورت که مقدار مثبت آن بیانگر تمرکز زیاد داده‌ها حول میانگین و مقدار منفی آن بیانگر پراکندگی داده‌ها و مقدار صفر یا نزدیک به صفر آن بیانگر نرمال بودن شرایط است. باتوجه به مثبت بودن کشیدگی این بعد (۳/۷)، نتیجه حاکی از متمرکز بودن داده‌ها حول میانگین ۸۶/۸ می‌باشد. کمینه بیانگر کمترین نمره و بیشینه بیانگر بیشترین نمره می‌باشد که همانظور ملاحظه می‌شود برای این بعد کمترین نمره برابر ۴۰ و بیشترین نمره برابر ۱۰۰ گزارش شده و در مقابل کمترین میانگین مربوط به بعد فرآیندها با میانگین ۸۴/۱ می‌باشد.

۳-۶ بررسی برازش الگوی اندازه‌گیری

این برازش به‌منظور بررسی روابط متغیرهای آشکار یا قابل‌اندازه‌گیری (مستطیل‌ها- زیرمؤلفه‌ها) با متغیرهای پنهان مرتبط (دایره‌های متصل به آن‌ها-مؤلفه‌ها)، در راستای تعیین روایی و پایایی پرسش‌نامه با استفاده از معیارهای کیفیت الگو صورت می‌گیرد (Error! Unknown switch argument.).

جدول (۶): معیارهای کیفیت الگو

ابعاد	آلفای کرونباخ	پایایی ترکیبی	متوسط واریانس استخراج‌شده
اهداف و کارکردها	۰.۶۴۳	۰.۷۷۵	۰.۴۱۲

ساختار و سازمان	۰.۷۲۱	۰.۸۰۹	۰.٤۱۹
فرآیندها	۰.۷۷۹	۰.۸٤۱	۰.٤٤
فناوری	۰.۸٤۳	۰.۸۸	۰.۵۱۵
ماموریت	۰.٦۳۱	۰.۷۵۱	۰.۲۷٦
تنظیم مقررات و حقوقی	۰.۷۱۱	۰.۸۰۹	۰.٤۰۹
امنیت	۰.۷۷۹	۰.۸٦۱	۰.٤۵
مدیریت و فرماندهی	۰.۸٤۳	۰.۸۸	۰.۵۱۵
معماری کلان پاسخگوی فوریت‌های رایانه‌ای مراکز دفاعی	۰.۸۱۷	۰.۸۷۵	۰.۵۸٦

۷- ابعاد کلان معماری گروه پاسخ‌گویی به فوریت‌های رایانه‌ای

باتوجه به نتایج به‌دست آمده از خبرگان دفاعی و تصدیق ابعاد مطرح شده، ابعاد شکل ٦، به‌عنوان ابعاد معماری کلان گروه پاسخ‌گویی فوریتی رایانه‌ای مراکز دفاعی شناخته شد.

شکل (٦): ابعاد معماری کلان گروه پاسخ‌گویی فوریتی رایانه‌ای مراکز دفاعی

۸- نتیجه‌گیری و پیشنهاد

در این مقاله پس از تبیین مفاهیم گروه پاسخ‌گویی، خدمات گروه پاسخ‌گویی و دیگر مولفه‌ها و موارد اثرگذار در گروه پاسخ‌گویی بررسی شد. سپس معماری‌های ملی و دفاعی برخی از کشورها مورد بررسی قرار گرفت. در پیشینه تحقیق با توجه به ضرورت تخلیص،

امکان معرفی فعالیت سایر کشورها در این حوزه وجود نداشت. در نهایت، پس از اجماع نظر خبرگان دفاعی در حوزه سایبری و تحلیل آماری، ابعاد معماری کلان گروه پاسخ‌گویی فوریتی رایانه‌ای مراکز دفاعی شامل: مدیریت و فرماندهی، امنیت، مأموریت، اهداف و کارکرد، فرآیند، ساختار، فناوری و زیرساخت و تنظیم مقررات و حقوقی پیشنهاد گردید که به‌عنوان یک نوآوری، می‌تواند امکان گسترش و پیاده‌سازی تیم پاسخ‌گویی را تسهیل نماید. مرحله بعدی در این حوزه، تبیین ارتباط و مولفه‌ها در معماری گروه پاسخ‌گویی است و سپس پیاده‌سازی گروه پاسخ‌گویی فوریتی رایانه‌ای در سطح مراکز دفاعی است که پیشنهاد می‌گردد به‌عنوان مطالعات و تحقیقات آتی انجام شود. تمامی موارد ذکر شده، نتایج بررسی یک تحقیق علمی است، اما نکته مهمی که در اکثر مقالات به‌صورت مغفول باقی می‌ماند، جلب نظر مدیران و مسئولان راهبردی و تصمیم‌گیر است و بدون همراهی آنها این مهم میسر نخواهد شد؛ لذا امید است با مطالعه این تحقیق، مدیران و مسئولان تصمیم‌گیر مراکز دفاعی ج.ا.ا در سطح راهبردی به ضرورت و اهمیت راه‌اندازی گروه پاسخ‌گویی بالاخص در مراکز دفاعی پی برده و آن را از اولویت‌های اصلی سازمان قرار دهند.

از پیشنهادهایی که مکمل این پژوهش بوده و به نظر محقق می‌تواند در مراکز تحقیقاتی و پژوهشی نیز به یاری ایجاد و تشکیل این گروه بشتابد، می‌توان به:۱. شناسایی مولفه‌ها و اجزای معماری کلان گروه پاسخ‌گویی مراکز دفاعی، ۲. نحوه استقرار و پیاده‌سازی گروه پاسخ‌گویی فوریتی رایانه‌ای، ۳. تعمیق ابعاد احصاء شده معماری کلان گروه پاسخ‌گویی فوریتی رایانه‌ای نام برد؛ همچنین ارتباط این گروه با فناوری‌های نوین مانند هوش مصنوعی[1] در مراکز دفاعی اشاره کرد.

1 -Artificial intelligence(AI)

فهرست منابع و مآخذ

الف- منابع فارسی

- درویش روحانی، بابک. (۱۳۹۰). مهندسی اطلاعات. تهران: دانشگاه پیام نور واحد هشتگرد.
- رشتی، سید محمدرضا. (۱۳۸۸). راهنمای ایجاد یک گروه پاسخ‌گویی به رخدادهای امنیتی رایانه‌ایCSIRT. تهران: رویش جوانه‌های فردا.
- -شمس، فریدون. (۱۳۸۳). «مفاهیم پایه معماری سازمانی»، مجله تکفا، سال دوم، شماره ۳.
- -شمس، فریدون و یادآور نیک‌روش، سیدعلی. (۱۳۸٦). «بررسی تلفیق چارچوب FEAF و معماری سرویس‌گرا»، دانشکده مهندسی برق و کامپیوتر. تهران: دانشگاه شهید بهشتی.
- صیاد، محمدکاظم و امینی، آرمین و طاهری، ابوالقاسم. (۱۳۹۹) «تهدیدات سایبری و اقدامات امنیتی در فضای مجازی». فصلنامه علمی امنیت ملی، سال دهم، شماره سی و هشتم.
- طیرانی، احسان. (۱۳۹۵). «مدیریت رخدادهای امنیت رایانه‌ای و تشکیل تیم‌های CERT سازمانی». آپای مشهد.
- کشاورز، رضا. (۱۳۹۳). «ارایه الگوی استقرار CERT مراکز نظامی». مجله علمی پژوهش‌های حفاظتی.
- مهجوریان، امیررضا. (۱۳۸٦). «تدوین روش برنامه‌ریزی معماری سازمانی سرویس‌گرا در جهت پوشش کامل به چارچوب زکمن». پایان نامه کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار، دانشگاه شهید بهشتی.

ب- منابع لاتین

- Beryl Bellman, Principal Instructor, (2018).
- Brownlee, N. (۲۰۱۸). "Expectations for Computer Security Incident Respons". U.S: Software Engineering Institute, Carnegie Mellon University.
- Department of EC- COUNCIL. (۲۰۱۷). "Ethical Hacking and countermeasure v11.0".
- Blueprint for a Secure Cyber Future: (2017), The Cybersecurity Strategy forthe Homeland Security Enterprise NIST Incident Response , 2021, The step bysetp guide for incident response reporting.
- Department of Defense. (2017). "DoD Architecture Framework Version 1.0". Available online at http://fas.org/irp/doddir/dod/chisr/index.htm.

- Institute for Enterprise Architecture Developments (2017).
- Killcrece, Georgia. Kossakowski, Klaus-Peter. Ruefle, Robin. Zajicek, Mark. . (2016) "State of the Practice of Computer Security Incident Response Teams (CSIRTs)". US: Carnegie Mellon University.
- Penedo, David. (2018)."Technical Infrastructure of a CSIRT". Cote d'Azur: Internet Surveillance and Protection, ICISP '06. International Conference, : 27 – 27.
- Pierre Jacobs, Sebastiaan von Solms and Marthie Grobler,(2019), E-CMIRC: Towards a Model for the Integration of Services Between SOCs and CSIRTs(2017).
- Scarfone, Karen. Grance, Tim and Masone, Kell. (March 201۸). "Computer Security Incident Handling Guide". U.S: Department of Commerce, National Institute of Standards and Technology.
- Stelvio bv. (2017). "CSIRT Services".U.S: Software Engineering Institute, Carnegie Mellon University.
- Schekkerman, J. (۲۰۱۷)."How to Survive in the Jungle of Enterprise Architecture Frameworks: Creating or Choosing an Enterprise Architecture Framework Paperback". New York: Trafford Publishing.
- Sowell, P. (۲۰۱۷), "The C4ISR Architecture Framework: History, Status, and Plans". Version 2.0, developed by the U.S. Department of Defense (DoD).
- Wilczynski, B. (2017). " Unified Profile for DODAF/MODAF (UPDM). http://www.updmgroup.org/index.htm

Sowell, P. (۲۰۱۷), "The C4ISR Architecture Framework: History, Status, and Plans". Version 2.0, developed by the U.S. Department of Defense (DoD)