فصلنامه مطالعات جنگ
سال سوم، شماره یازدهم، زمستان ۱۴۰۰
مقالهٔ پنجم از صفحه ۹۷ تا ۱۲۱

فناوری‌های نوظهور سایبری و تهدیدات ناشی از بکارگیری آنها در سازمان‌های دفاعی– نظامی

خداداد هلیلی[۱]

دریافت مقاله: ۱۴۰۰/۱۰/۱۲ پذیرش مقاله:۱۴۰۰/۱۲/۰۱

چکیده

در عصر فناوری اطلاعات و ارتباطات، توسعه روزافزون فناوری‌های نوین سایبری، تمامی عرصه‌های زندگی بشر، از جمله حوزه‌های دفاعی و نظامی را دستخوش تغییرات اساسی نموده است. شناخت چالش‌ها و تهدیدات این فناوری‌های نوظهور و آمادگی برای مواجهه هوشمندانه با کلان‌روندهای فناورانه، از دغدغه‌های همیشگی سیاست‌گذاران و ذینفعان فضای سایبر است. ازاین‌رو، آینده‌پژوهی، مطالعه اکتشافی عمیق و بررسی و تحلیل اسناد و گزارش‌های معتبر جهانی در این حوزه، امری ضروری است. در این تحقیق، پس از بررسی فناوری‌های اینترنت اشیاء، رایانش ابری، کلان داده، و سامانه‌های فیزیکی سایبری، نمونه‌ای از کاربردهای آنها در سازمان‌های نظامی و دفاعی و نیز تهدیدات سایبری هر کدام، موردتوجه قرار گرفته است. این تحقیق، از نظر هدف، کاربردی– توسعه‌ای و از نظر شیوه گردآوری داده‌ها توصیفی– موردی است. به‌منظور گردآوری داده‌ها، از منابع کتابخانه‌ای، سایت‌های معتبر علمی، اسناد و گزارش‌های داخلی و خارجی استفاده شده و رویکرد مورد استفاده برای تجزیه‌وتحلیل داده‌ها نیز از نوع کیفی است. نتایج حاصل از این تحقیق نشان می‌دهد، با اینکه بکارگیری این فناوری‌ها می‌تواند موجب بهبود کیفیت و کارایی در محیط‌های عملیاتی سازمان‌های دفاعی شود؛ اما بهره‌گیری مناسب از مزایا و قابلیت‌های آنها، به خاطر تهدیدات سایبری نیازمند زیرساخت‌های ارتباطی و شبکه‌های اختصاصی است. بنابراین برای پیشگیری از غفلت راهبردی، در پذیرش و استفاده از این فناوری‌ها، باید میان نگرانی‌های ناشی از دستیابی به اطلاعات حساس، تضمین امنیت داده‌ها و کارایی‌های جذاب و وسوسه‌انگیز آنها، مصالحه برقرار نمود.

واژگان کلیدی: رایانش ابری، کلان داده، سامانه‌های فیزیکی سایبری، تهدیدات سایبری

۱ - عضو هیأت علمی دانشکده برق، دانشگاه شهید ستاری، دانشجوی دکترای امنیت سایبر halili@chmail.ir

مقدمه

روند شکل‌گیری و توسعه فناوری‌های پیشرفته، برهم زن[1] و بعضاً غیرقابل‌پیش‌بینی مرتبط با فضای سایبر، نشان می‌دهد؛ این فناوری‌ها، زمینه‌ساز یک انقلاب صنعتی نوین و جهش تاریخی خواهد بود. که پیامدهای آن، همه ارکان زندگی بشر را تحت تأثیر قرار خواهد داد. وابستگی به فضای سایبر در جهان آینده یک تصویر خیالی نیست بلکه واقعیتی انکارناپذیر و اجتناب‌ناپذیر است. در کشورهای پیشرفته در زمینه فناوری اطلاعات و ارتباطات، بخش عمده‌ای از فعالیت‌های اقتصادی، اجتماعی و زیست‌محیطی مبتنی بر فضای سایبر است. در این کشورها، سازمان‌های نظامی و دفاعی نیز به تجهیزات نوین سایبری مجهز شده‌اند. ازآنجاکه در این سامانه‌ها، منابع اطلاعاتی حساس و حیاتی هستند؛ نگرانی از امنیت اطلاعات مبادله شده از موانع توسعه این فناوری‌ها و برخورد محتاطانه با آن شده است. در این تحقیق هدف اصلی، بررسی فناوری‌های نوظهور سایبری و تهدیدات ناشی از بکارگیری آنها در سازمان‌های دفاعی و نظامی است. بدین منظور، پس از بررسی کاربردهای نظامی چهار فناوری مهم اینترنت اشیاء، رایانش ابری، کلان داده و سامانه‌های فیزیکی و سایبری، تهدیدات سایبری ناشی از بکارگیری آنها تبیین شده است.

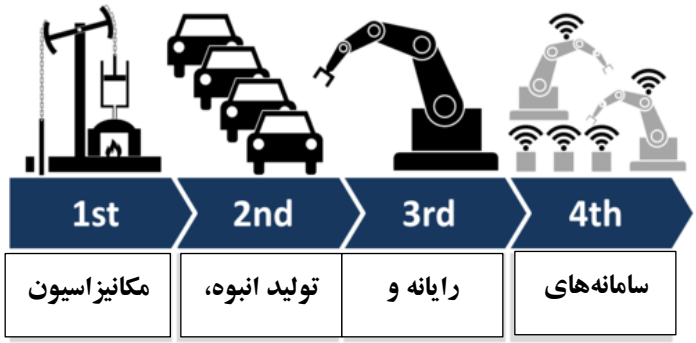
انجام تحقیقات علمی، آینده‌پژوهی، مطالعات اکتشافی عمیق و بررسی و رصد و دیدمبانی گزارش‌های معتبر جهانی در این حوزه، از اهمیت بالایی برخوردار است چراکه می‌تولند موجب شکل‌گیری یک درک مشترک میان تولیدکنندگان، ذینفعان، سیاست‌گذاران و تصمیم گیران در این زمینه شود. همچنین مواجهه هوشمندانه با این کلان‌روندهای فناورانه، مستلزم شناخت چالش‌ها و تهدیدات نوین این فناوری‌ها است. از طرفی، فقدان تحقیقات علمی در این زمینه، موجب می‌شود پاسخگویی به دغدغه‌های بومی کشور و نحوه مقابله با چالش‌ها و تهدیدات این حوزه همچنان باقی بماند.

[1] Disruptive

مبانی نظری

انقلاب صنعتی چهارم و فناوری‌های نوظهور سایبری

از اواسط قرن هیجدهم میلادی دگرگونی‌های بزرگی در صنایع کشاورزی، تولید و حمل‌ونقل آغاز شد و با توسعه کارخانجات صنعتی، فعالیت‌های تولیدی و خدماتی توسط ماشین و با نظارت انسان و در ادامه با ظهور رایانه‌ها با کاهش دخالت انسان صورت گرفت. تحولات صنعتی، متأثر از اختراعات خاصی است که از آن تحت عنوان انقلاب صنعتی یاد می‌شود. انقلاب صنعتی اول، با تکمیل و اختراع ماشین بخار در سال ۱۷۶۹ توسط جیمز وات[1] آغاز شد. با اختراع موتور الکتریکی توسط مایکل فارادی[2] در سال ۱۸۲۱ و در ادامه تلاش‌های علمی بزرگانی چون ادیسون، گراهام بل، نیکولا تسلا و ورنر زیمنس در اوایل قرن بیستم؛ الکتریسیته به ابزاری مهم در انقلاب صنعتی



شکل(۱) روند تکاملی انقلاب صنعتی تا صنایع نسل چهارم

دوم تبدیل شد که تولید انبوه محصولات را در پی داشت. انقلاب صنعتی سوم با ورود رایانه به صنعت تحت عنوان انقلاب دیجیتال شکل گرفت. رایانه‌های خانگی و ظهور اینترنت در سال ۱۹۶۹ و خودکارسازی از پیامدهای این انقلاب صنعتی بود. در انقلاب صنعتی چهارم[3] ترکیبی از فناوری‌های حوزه‌های فیزیک، فضای سایبر و زیست‌شناسی تحت عنوان سامانه‌های سایبر فیزیکی (CPS) دوران جدیدی را در زندگی بشر به ارمغان خواهد آورد. دورانی که هنوز در آغاز راه آن هستیم. در شکل (۱) روند تکامل چهار انقلاب صنعتی آمده است[4].

---

[1] James Watt
[2] Michael Faraday
[3] Industry 4.0
[4] http://www.allaboutlean.com

کلاوس شواب[1] بنیان‌گذار مجمع جهانی اقتصاد[2] در مقاله‌ای به توصیف این انقلاب صنعتی پرداخته است (Schwab,2015). از دیدگاه وی، انقلاب صنعتی چهارم نه تنها آنچه انجام می‌دهیم بلکه آنچه هستیم را تغییر خواهد داد. اینترنت اشیا، کلان داده، رایانش ابری، امنیت سایبری، شبیه‌سازی، روبات‌های خودکار، واقعیت افزوده، یکپارچه‌سازی سامانه‌ها و دیجیتالی شدن تولید انبوه ، ۹ فناوری کلیدی و مهم‌ترین ارکان تشکیل‌دهنده انقلاب صنعتی چهارم هستند.

این انقلاب، بر پایه ایده هوشمند سازی محصولات و شبکه‌سازی آنها صورت خواهد گرفت و نسل‌های جدید اینترنت مانند اینترنت اشیاء و اینترنت سرویس زیرساخت‌های اصلی آن محسوب می‌شوند. بسیاری از کارخانجات جدید با دیجیتالی کردن محصولات خود و مجهز کردن آنها به حس‌گرهای متصل به اینترنت خدمات بهتری را در اختیار مشتریان خود قرار می‌دهند. همکاری میان این فناوری‌ها، سامانه‌های سایبر فیزیکی (CPS) را به وجود می‌آورد که با یکدیگر و انسان‌ها در تعامل قرار می‌گیرند. جمع‌آوری و تحلیل داده‌ها چرخه عمر و زنجیره تولید و توزیع محصولات را بهبود می‌بخشد. در ادامه ویژگی‌های چهار فناوری مهم مرتبط با انقلاب صنعتی چهارم بررسی شده است. ازآنجاکه این فناوری‌ها، هنوز در آغاز راه است بسیاری از قابلیت‌های آنها پدیدار نشده و تهدیدات ناشی از وابستگی مفرط به آن قابل پیش‌بینی نیست

اینترنت اشیاء

افزایش روزافزون کاربران اینترنت به بیش از سه میلیارد نفر در سطح جهان و دگرگونی‌های ایجادشده متأثر از نفوذ آن در تمامی لایه‌های زندگی، نشان‌دهنده این است که در آینده، اینترنت کارکردی مشابه برق در زندگی روزمره پیدا خواهد کرد و به بخشی جدایی‌ناپذیر از زندگی تبدیل خواهد شد به‌طوری‌که تصور زندگی بدون آن دشوار خواهد بود (Galis, 2013). استفاده از رایانش ابری، هوش مصنوعی، واقعیت افزوده، شبکه‌های اجتماعی فرامرزی، تبدیل اینترنت به شبکه‌های مجزا و ملی، آموزش مجازی از پیامدهای اینترنت است. به‌منظور پیش‌بینی و مواجهه با تهدیدات و چالش‌های پیش رو، نیازمند شناخت روندهای فناورانه در مورد آینده اینترنت هستیم. هدف اصلی اینترنت آینده[3]، ایجاد زیرساخت قدرتمندی است که بتواند از خدمات و کاربردهای

[1] Klaus Schwab
[2] World Economic Forum
[3] future internet

نوظهور پشتیبانی کند در یک تقسیم‌بندی کلی، ابعاد و خدمات مرتبط با اینترنت شامل موارد زیر است (موزونی، ۱۳۹۵).

- **اینترنت افراد**[1] **(IoP)**: اتصال کاربران به همدیگر به‌منظور افزایش سطح ارتباط آنها بین آنهاست بطوریکه برای فعالیت‌های برخط محدودیتی نداشته باشند. اینترنت افراد، تغییرات نوآورانه و هوشمندانه بسیاری در فعالیت‌های اجتماعی و اقتصادی به همراه دارد.
- **اینترنت خدمات**[2] **(IoS)** : در اینترنت خدمات، خدمات مبتنی بر وب ارائه می‌شود. این خدمات باید از طریق اینترنت و به‌صورت خودکار قابل پیاده‌سازی شده و در پیوند با هم قرار گیرد مانند خدمات تراکنشی تجاری در کسب‌وکار و تجارت.
- **اینترنت انرژی**[3] **(IoE)**: زیرساخت شبکه‌ای پویا که شبکه انرژی را از طریق اینترنت به هم متصل می‌کند و واحدهای انرژی (که به‌صورت محلی ایجاد، ذخیره و ارسال شده‌اند) بتوانند در هر زمان و هر مکان که نیاز است مخابره شوند. داده‌های مرتبط، جریان‌های انرژی را دنبال می‌کنند و اطلاعات ضروری با انتقال انرژی مبادله می‌کنند. در شهرهای هوشمند، اینترنت انرژی کاربردها مختلفی دارد مانند هوشمند سازی ساختمان‌ها و تأسیسات ، تنظیم تهویه ساختمان و...
- **اینترنت رسانه**[4] **(IoM)**: ارتباط بین انسان‌ها و ماشین‌ها رابطه مستقیمی با فناوری‌های صوتی و تصویری و اینترنت رسانه دارد که مباحثی مانند پردازش تصویر، دوربین دیجیتال و برنامه‌های کاربردی چندرسانه‌ای تلفن همراه را در بر می‌گیرد.
- **اینترنت اشیاء**[5] **(IoT)**: اینترنت اشیاء در هوشمند سازی مدیریت شهری، حمل‌ونقل، کشاورزی، صنایع دفاعی، صنعت بیمه، صنایع مربوط به نفت، گاز و معدن، مدیریت انرژی، پایش و امنیت اماکن عمومی و خصوصی، خرده‌فروشی، لجستیک، بانک‌ها،

[1] Internet of People
[2] Internet of Service
[3] Internet of Energy
[4] Internet of Media
[5] Internet of Things

بهداشت و درمان، هتلداری و .... استفاده می‌شود. استفاده از اینترنت اشیاء و رایانش ابری موجب هوشمندتر شدن دولت الکترونیک می‌شود

در اینترنت آینده، کلیه موجودات و اشیاء به عضوی فعال تبدیل شده و در بستر، اینترنت افراد، اینترنت خدمات، اینترنت انرژی و اینترنت رسانه به تعامل با محیط اطراف خود می‌پردازند. برخی، ابعاد اینترنت آینده را در قالب اینترنت (همه) اشیاء[1] (IoE) یا به طور خلاصه اینترنت اشیاء تعریف می‌کنند. در اینترنت همه اشیاء، صحبت از هر شخص، هر چیز، هر سرویس، هر شبکه، هر مسیر، هر کسب‌وکار، هر قطعه، هر مکان، هر زمان و هر زمینه مطرح است (پارادایم هر[2] در اینترنت اشیاء) بر این اساس، در حالت کلی می‌توان گفت؛ فناوری اینترنت اشیاء با ترکیب ابعاد مختلف اینترنت شکل نوینی از تکامل اینترنت در فضای سایبر را به منصه ظهور و بروز خواهد رساند.

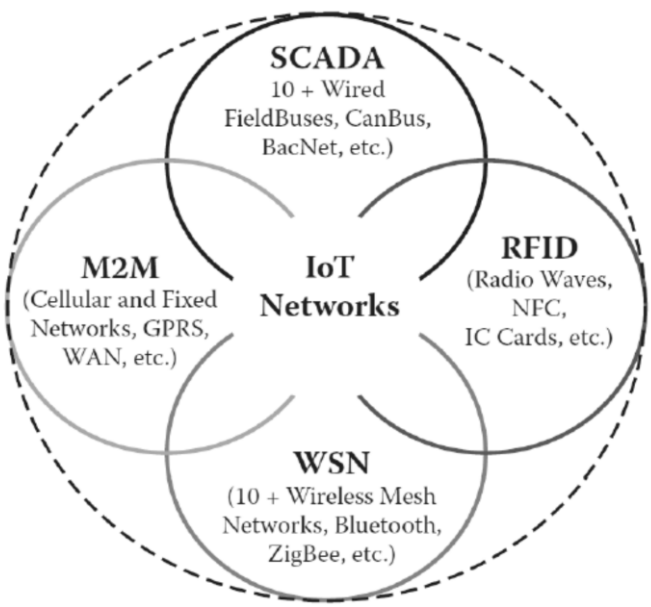
اینترنت اشیاء، فناوری مدرنی است که در آن برای هر موجودی (انسان، حیوان و یا اشیاء) قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت، فراهم می‌شود. در این فناوری، اشیا پیرامون ما قادرند از محیط اطراف خود داده‌های مفیدی را از طریق حسگرهای مختلف جمع‌آوری کرده و آن‌ها را برای پردازش و اتخاذ تصمیمات لازم به یک سیستم مرکزی منتقل کنند موسسه گارتنر، پیش‌بینی می‌کند تا سال ۲۰۱۸ بیش از ۱۸ میلیارد وسیله به اینترنت متصل خواهند شد که ۹ میلیارد از این اتصالات به شبکه، ناشی از اتصال اشیاء می‌باشد. همچنین تا ۲۰۲۰ حدود ۲۶ میلیارد وسیله مبتنی بر اینترنت اشیاء وجود خواهد داشت [3]. در واقع اینترنت اشیاء، روند تکامل اینترنت را نشان می‌دهد که در آن دریافت، ذخیره‌سازی و ارسال اطلاعات از محیط، به‌منظور خدمات بهتر و هوشمندتر به کاربر نهایی ارائه می‌شود.

طبق برآورد موسسه سیسکو ۹۹.۴ در صد از اجسام فیزیکی هنوز به اینترنت متصل نیست یعنی از میان ۱.۵ تریلیون عینیت فیزیکی در سطح جهان تنها ۱۰ میلیارد به اینترنت متصل هستند. به‌عبارت‌دیگر به ازای هر نفر ۲۰۰ شیء مختلف قابل اتصال به اینترنت وجود دارد. طبق پیش‌بینی این موسسه تا سال ۲۰۲۰ بیش از ۵۰ میلیارد دستگاه متصل به اینترنت خواهیم داشت. برآوردهای آماری نشان می‌دهد، تا سال ۲۰۲۰ به میزان ۴۰ درصد از همه داده‌های تولید شده از حس‌گرهای

[1] Internet of Everything
[2] Any Paradigm
[3] http://www.gartner.com

متصل شده به اینترنت دریافت خواهد شد؛ این مسئله موجب افزایش ترافیک داده‌ها به چهار برابر می‌شود (Tan and Koo, 2014).

در اینترنت اشیاء، فناوری‌هایی مانند شبکه حسگرهای بی‌سیم[1] (WSN)، ارتباطات ماشین به ماشین[2] (M2M)، روباتیک، تگ‌های بازشناسی با امواج رادیویی[3] (RFID)، هوش مصنوعی،



شکل (۲): چهار فناوری مهم در اینترنت اشیاء

سامانه‌های سرپرستی و اکتساب داده (SCADA) سامانه موقعیت‌یاب جهانی (GPS) و هوش مصنوعی برای تحلیل و مدیریت داده‌ها استفاده می‌شود در شکل(۲) این فناوری‌ها نشان داده شده است (Zhou, 2013).

بررسی روندهای فناورانه و توجه به توسعه اینترنت اشیاء در بسیاری از کشورها نشان از ورود به عصری جدید دارد که در آن، جامعه شبکه‌ای مبتنی بر زیرساخت اینترنت اشیاء در حال شکل‌گیری است. یک ضرب‌المثل آمریکایی می‌گوید: اگر چیزی روی اینترنت نیست پس حتماً وجود خارجی

[1] Wireless Sensor Network
[2] Machine to Machine
[3] Radio Frequency Identification

ندارد. در آمریکا، اینترنت اشـــیاء به‌منظور ابزاری برای شـــنود اطلاعات در خارج از آمریکا برای مبارزه با تروریسم توسط سازمان امنیت ملی آمریکا مورد توجه قرار گرفته است. در مقاله قرشی و شبرو، نحوه بکارگیری اینترنت اشیاء در شبکه هوشمند صنعت برق کشور بررسی شده است (قرشی و شبرو، ۱۳۹۳). قاسمی و دیگران نیز با بررسی کاربرد اینترنت اشیاء در بخش بهداشت و درمان کشور به اولویت بندی شاخص‌های مهم فناورانه در این حوزه پرداخته‌اند (قاسمی و دیگران، ۱۳۹۵). استفاده از اینترنت اشیاء در حوزه نظامی هم در صحنه نبرد و هم در مسائل پشتیبانی کاربرد دارد. استفاده از حسگرهای محیطی برای شناخت آگاهی وضعیتی، در سامانه‌های ارتباطی و فرماندهی و کنترل، و شناسایی فرکانس‌های رادیویی، برچسب‌های ردیابی محموله‌ها در مسائل لجستیک دفاعی کاربرد دارد.

رایانش ابری

دستیابی همه‌جایی و همه مکانی به اطلاعات از طریق اینترنت، بدون نیاز به حافظه سخت و برنامه‌های کاربردی و لزوم تمرکز منابع اطلاعاتی و محاسباتی، موجب شکل‌گیری ایده رایانش ابری در اوایل قرن اخیر شد. رایانش ابری مشابه استفاده از ژنراتورهای برق و شبکه توزیع آن است که می‌تواند سازگاری میان سامانه‌ها و کاربردهای ناهمگون را فراهم سازد. واژه ابر اشاره به پنهان بودن جزئیات فنی و پیچیده از دید کاربر و ویژگی منفعت همگانی از رایانش ابری (مانند بارش باران از ابر) دارد. این مسئله کارایی سامانه‌های اطلاعاتی را بالا برده و صرفه‌جویی زیادی نیز در هزینه‌ها هم برای ارائه دهنده سرویس و هم سرویس‌گیرنده در بر خواهد داشت.

طبق تعریف موسسه استاندارد و فناوری آمریکا (NIST)[1] رایانش ابری مدلی برای فراهم نمودن دسترسی آسان و مبتنی بر تقاضای کاربر به منابع محاسباتی قابل پیکربندی مانند شبکه‌ها، سرورها، منابع ذخیره‌سازی، برنامه‌های کاربردی و خدماتی است به‌طوری‌که با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم ارائه‌دهنده سرویس این دسترسی به سرعت فراهم گردد[2]. در جدول(۱) مهم‌ترین ویژگی‌های این فناوری به‌طور خلاصه آمده است.

جدول (۱): ویژگی‌های رایانش ابری

سرویس مبتنی بر تقاضا[3]	**ذخیره‌سازی و دسترسی به منابع محاسباتی بدون دخالت انسانی بر اساس تقاضای بهره‌بردار**
استخری از منابع[4]	دسترسی به منابع محاسباتی مجازی و فیزیکی نامحدود با استفاده از مدل‌های چند اجاره‌ای
انعطاف‌پذیری سریع[5]	انتخاب میزان بهره‌برداری از سرویس‌های موردنظر در هر مکان و زمان
دسترسی به شبکه پهن‌باند[6]	دسترسی به قابلیت‌های محاسباتی از طریق انواع پلتفرم‌ها، گوشی‌های موبایل، تبلت و لپ‌تاپ‌ها در یک شبکه پهن باند
سرویس قابل‌اندازه‌گیری[7]	اندازه‌گیری سرویس (ذخیره، پردازش و...) با مانیتور و کنترل کردن منابع به طور شفاف برای مصرف‌کننده و ارائه‌دهنده

روند توسعه فناوری رایانش ابری از رایانش خوشه‌ای[8] شروع شد و پس از رایانش توری[9] به رایانش ابری رسید. در رایانش خوشه‌ای با اتصال گروهی از کامپیوترها به هم، امکان افزایش توان

---

1 National Institute of Standards and Technology
2 National Institute of Standards and Technology. (http://www.nist.gov)
3 On-Demand Self Service
4 Resources Pooling
5 Rapid Elasticity
6 Broad Network Access
7 Measured Service
8 Cluster Computing
9 Grid Computing

و قابلیت اطمینان ایجاد می‌شـــود. در رایانش توری اشـــتراک منابع بین کامپیوترهای ناهمگن و در فواصل جغرافیایی مختلف صورت می‌گیرد و کنترل مرکزی روی آنها وجود ندارد. در رایانش ابری دسـترسـی به منابع از طریق شـبکه، بویژه اینترنت به‌صـورت متمرکز انجام می‌شـود. در جدول (۲) مدل‌های پیاده‌سازی و سرویس‌های ارائه‌شده رایانش ابری، در حالت کلی نشان داده شده است[1].

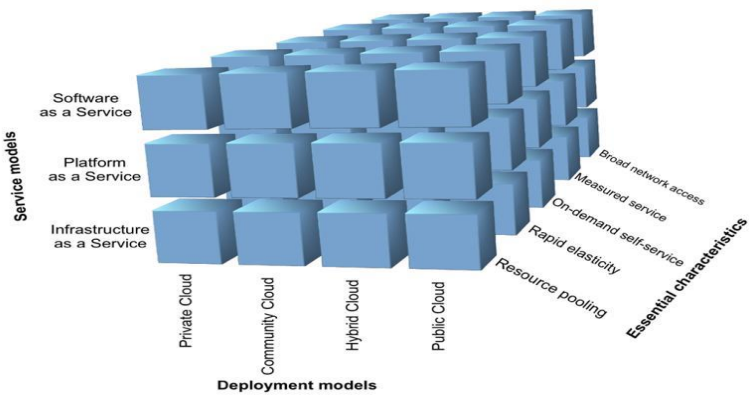
جدول(۲): مدل‌های پیاده‌سازی و سرویس‌های ارائه‌شده در رایانش ابری

مدل‌های پیاده‌سازی	
ابر خصوصی[2]	اسـتفاده یک سـازمان از زیرسـاخت رایانش ابری و امکان کنترل بر تمام سطوح پیاده‌سازی (سخت‌افزار، شبکه، سیستم‌عامل، نرم‌افزار)، این حالت برای سازمان‌های خاص با برنامه‌ها و اطلاعات حساس مناسب است
ابر عمومی[3]	اسـتفاده از اینترنت برای بهره‌گیری از سـرویس‌ها (مشـابه صـنعت برق و تلفن)، این مـدل توسـط سـرویس‌دهنـدگـان بزرگ مـانـنـد آمـازون و مایکروسافت و گوگل استفاده می‌شود
ابر ترکیبی[4]	اتصـــال کاربران از طریق ابر خصـــوصـــی به ابر عمومی، این مدل برای شرکت‌های تجاری برای بهره‌برداری از مزایایی مانند هزینه پایین‌تر مناسب است.
ابر انجمنی(اشتراکی)[5]	در این حالت زیرساخت بین چند سازمان به اشتراک گذاشته می‌شود.
انواع سرویس‌ها	
نـرم‌افـزار بـه‌عـنـوان سرویس[6] (SaaS)	در این حـالـت برنـامـه‌هـا و نرم‌افزارهـای کـاربردی روی ســـرور مرکزی نصب‌شده و کاربر می‌تواند از طریق موبایل، لپ‌تاپ و یا مرورگرهای وب به آنها دســـترســـی پیدا کند. کاربر، کنترلی روی عناصـــر زیرســـاخت (ذخیره‌سازی، قابلیت پردازشی یا سیستم‌های عملیاتی ندارد و تنها امکان برخی تنظیمات و پیکربندی‌ها وجود دارد. منابع پردازشـی، ذخیره‌سـازی، شبکه و سایر منابع رایانشی به‌صورت چند اجاره‌ای ارائه می‌شود.

[1] http://www.it-solutions.siemens.com
2. Private
3. Public
4. Hybrid
5. Communality
6. Software as a Service

پلتفرم به‌عنوان سرویس[1] (PaaS)	در این حالت، امکان استفاده از سرویس‌های مختلف روی زیرساخت فراهم‌شده و کاربر کنترلی روی منابع محاسباتی و شبکه ندارد. امکان ایجاد برنامه‌های کاربردی توسط کاربر در محیط ابری وجود دارد.
زیرساخت به‌عنوان سرویس[2] (IaaS)	در این حالت بااینکه کاربر امکان کنترل روی منابع مانند نصب نرم‌افزار یا برنامه‌های کاربردی را دارد اما هیچ‌گونه دسترسی یا مدیریتی بر زیرساخت‌های ابری ندارد.

در شکل (۳) یک مدل مفهومی برای نشان دادن ویژگی‌ها، مدل‌های پیاده‌سازی و انواع سرویس‌های بکار رفته در رایانش ابری که در جداول ... و.... موردبررسی قرار گرفت نشان داده شده است



شکل(۳): ویژگی‌ها، مدل‌ها و سرویس‌ها در رایانش ابری

(Klems ،2009).

رایانش ابری دارای مزایایی از جمله کاهش هزینه، انعطاف‌پذیری در کاربرد، سرعت بهره‌گیری و تعمیر و نگهداری پایین است شرکت‌های بزرگ مانند مایکروسافت، گوگل و آمازون امروزه در توسعه سریع و تسلط در عرصه با هم رقابت دارند در بسیاری از کشورها مانند سنگاپور، آمریکا، سوئد، انگلیس، ژاپن، کره جنوبی، کلنادا، آلمان و ... سرمایه‌گذاری زیادی در زمینه بکارگیری رایانش ابری در دولت الکترونیک، انجام شده است (Bhisikar, 2011). بهره‌گیری از رایانش ابری، به خاطر استفاده حداکثری از منابع، کاهش هزینه‌ها و یکپارچگی زیرساخت‌ها در حوزه نظامی موجب افزایش کارایی می‌شود اما مهاجرت این سازمان‌ها باید با در نظر گرفتن شاخص‌های

1. Platform as a Service
2. Infrastructure as a Service

امنیتی مانند احراز هویت، دسترس‌پذیری، محرمانگی و حریم خصوصی انجام شود (ولوی و همکاران، ۱۳۹۶).

پذیرش رایانش ابری در سازمان‌های دفاعی که داده‌های آنها از طبقه‌بندی و حساسیت خاصی برخوردار است همواره مورد تردید است. امروزه، برخی از سازمان‌های نظامی مانند موسسه سامانه‌های اطلاعات دفاعی[1] (DISA) با استفاده از مکانیسم‌های امنیتی پیشرفته از این روش استفاده می‌کنند و این مسئله افق جدیدی در به‌کارگیری این فناوری ایجاد نموده است. به‌هرحال در بسیاری از موارد نمی‌توان مصالحه‌ای بین نگرانی‌های امنیتی ناشی از دستیابی به اطلاعات حساس و کارایی‌های جذاب و وسوسه‌انگیز این فناوری برقرار نمود (هلیلی و همکاران، ۱۳۹۴).

کلان داده

یکی از پیامدهای توسعه روزافزون فناوری‌های فضای سایبر، تولید خیره‌کننده، تصاعدی و انفجارگونه اطلاعات از منابع مختلف است که مفهومی به نام کلان داده[2] را به وجود آورده است. مدیریت، کنترل و پردازش این اطلاعات حجیم، فراتر از توانایی ابزارهای نرم‌افزاری و پایگاه‌های داده سنتی است. ازآنجاکه داده و اطلاعات، از مهم‌ترین دارایی‌های نامشهود، و محرک نوآوری محسوب می‌شود؛ داده‌کاوی و استخراج دانش از اطلاعات، امروزه جذابیت و اهمیت زیادی پیداکرده است. ارزش بالقوه نهفته در کلان‌داده برای شرکت‌های مختلف تجاری، صنعتی، علمی و سازمان‌های دولتی به حدی است؛ که برخی آن را نفت دوران جدید نامیده‌اند. کریستوفر لینچ[3] که یکی از سرمایه‌گذاران در پروژه‌های مرتبط با کلان‌داده است، از این فناوری به‌عنوان اولین فناوری پس از شکل‌گیری اینترنت نام می‌برد که می‌تواند جهان را تغییر دهد. مؤسسه تحقیقات بین‌المللی گارتنر[4] کلان‌داده را در میان ۱۰ روند برتر فناوری در سال ۲۰۱۳ و یکی از ۱۰ روند حیاتی فناوری در ۵ سال آینده معرفی نموده است.

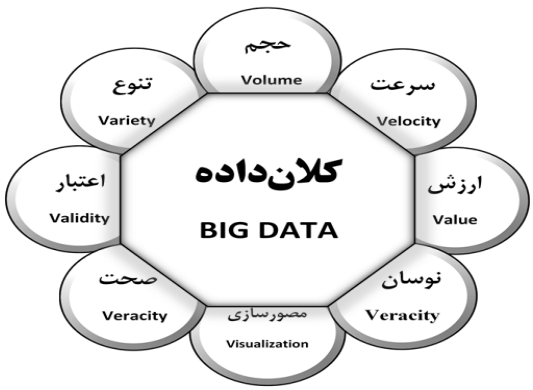
تعریف کلان‌داده اولین بار در سال ۲۰۰۱ توسط داگ لنی[5] در موسسه گارتنر مطرح شد. طبق تعریف وی، کلان‌داده عبارت است از اطلاعات با حجم بالا، سرعت‌بالا و تنوع زیاد که همانند سرمایه اطلاعاتی با روش‌های نوین پردازشی، ذخیره‌سازی برای درک بهتر از دنیا و روند

---

[1].Defence Information Systems Agency
[2] Big Data
[3] Christopher Lynch
[4] www.gartner.com
[5] Doug Laney

تصـمیم‌گیری مورداسـتفاده قرار می‌گیرد[1]. وی این سـه ویژگی (حجم، سـرعت و تنوع) را تحت عنوان 3V مطرح کرد. در سال‌های اخیر به این تعریف پنج V دیگر نیز اضـافه شـد که با 8Vs بیان می‌شوند (Mills، 2012). در شکل (۴) ویژگی‌های هشتگانه کلان‌داده نشان داده‌شده است. علاوه بر حجم، سرعت و تنوع داده ویژگی‌های دیگر کلان‌داده عبارت‌اند از:

- اعتبار: مناسب بودن داده برای کاربرد خاص
- صحت: قابلیت اعتماد به داده‌ها
- نوسان: زمان و دوره لازم برای نگهداری داده‌ها
- ارزش: ارزش هزینه کردن برای پردازش و نگهداری داده



شکل (۴): ویژگی‌های هشتگانه کلان‌داده

- مصوّرسازی: استفاده از گرافیک و تصویرسازی برای فهم بهتر داده‌ها

کلان‌داده از مهم‌ترین مباحث روز دنیا و پژوهش‌های آینده اسـت که مزایایی مانند بهبود بهره‌وری، ارتقای شـفافیت سـازمانی و گسـترش مرزهای دانش، شـناخت الگوهای رفتاری در شـبکه‌های اجتماعی برای کاربردهای اجتماعی، امنیتی و فرهنگی را دارد. با اینحال بهره‌گیری از مزایا و کاربردهای آن، مسـتلزم فراهم نمودن زیرسـاخت‌های لازم سـخت‌افزاری، نرم‌افزاری و بسـتر محاسباتی است. بومی‌سازی صنایع و فناوری‌های مربوط به کلان‌داده در افزایش بهره‌وری و توسعه خدمات نقش سـازنده‌ای دارد و توانمندی، خودکفایی، عدم وابسـتگی و تأمین امنیت ملی، را به همراه خواهد داشـت. تولید داده‌هایی که مدیریت و کنترل آنها در دسـت ما نیسـت؛ در واقع تبدیل نقاط ضعف به تهدید است (هلیلی و ولوی، ۱۳۹۶).

[4] http://blogs.gartner.com/doug-laney

در سازمان‌های دفاعی و امنیتی در زمان صلح و جنگ با دریافت اطلاعات و تجزیه‌وتحلیل مناسب آنها، سعی در شناسایی و واکنش مناسب به این اطلاعات هستند. به‌عنوان‌مثال آژانس‌های امنیتی در پیش‌بینی فعالیت‌های تبهکارانه و شناسایی و ردگیری تروریست‌های سایبری از داده‌کاوی استفاده می‌کنند. همچنین، در محیط‌های عملیات نظامی حسگرهای محیطی مبتنی بر اینترنت اشیاء مانند شبکه‌های حسگر بیسیم جهت شناسایی تجهیزات و نیروهای دشمن و یا تعیین مسیر حرکت نیروهای خودی به طور پیوسته در حال تولید و تبادل داده هستند. ازآنجاکه در جنگ‌های آینده، اطلاعات، از ارزش‌ها و سرمایه‌های حیاتی محسوب می‌شود و ناگزیر از جایگزینی تجهیزات پردازش و مبادله داده با تجهیزات سنتی هستیم؛ مدیران و فرماندهان عالی باید شناخت کافی از سامانه‌های موردنیاز داشته باشند تا با برنامه‌ریزی راهبردی، ضمن شناخت تهدیدات و آسیب‌پذیری‌های این فناوری‌ها، از مزایا و فرصت‌های استفاده از آن بهره لازم را ببرند (هلیلی و همکاران، ۱۳۹۴).

سامانه‌های فیزیکی، سایبری

سامانه‌های فیزیکی سایبری[1] (CPS) شبکه‌ای از سامانه‌های سایبری (محاسباتی و ارتباطی) و اجزای فیزیکی (حسگرها و راه‌اندازها) هستند که در یک حلقه بازخورد شامل مداخله انسانی در تعامل و ارتباط با هم قرار می‌گیرند. این سامانه ارتباط تنگاتنگی با شبکه‌های حسگر، هوش محاسباتی و مکانیسم‌های هوشمند سازی دارد. اجزای این سامانه شامل سه لایه حسگرهای محیطی، فناوری‌های انتقال داده و جمع‌آوری و تحلیل داده برای تصمیم‌گیری است که در شکل (۵) نشان داده شده است (Ashibani, 2017)

شکل (۵): سه لایه کلی سامانه فیزیکی سایبری

[1] Cyber Physical Systems

این سامانه، در مخابرات، انرژی، سلامت، ، نظامی، رباتیک، حمل‌ونقل، خلبان خودکار و... کاربرد دارد. استفاده از فناوری‌های نوین برای هوشمند سازی تجهیزات مورد استفاده در منازل، خودروها، تلفن همراه و... با بکارگیری دوربین‌های دیجیتال، مجهز شدن آنها به سامانه موقعیت‌یاب جهانی (GPS)، اتصال آنها به اینترنت از طریق فناوری‌های مختلف بیسیم، امکان جمع‌آوری و پردازش اطلاعات از آنها را فراهم نموده است. نمونه‌ای از این هوشمند سازی در گوگل مپ برای تعیین مسیر با ترافیک کمتر دیده می‌شود. همچنین در کاربردهایی از جمله جراحی رباتیک، عملیات در محیط‌های خطرناک و غیرقابل‌دسترس مانند جستجو در اعماق دریا و تقویت نظارت در بهداشت و درمان از این فناوری استفاده می‌شود (Berger, 2016).

در محیط‌های عملیاتی پیچیده و پویا، که ترکیبی از فناوری‌های پیچیده و متنوع، وجود دارد؛ کسب نتایج مطلوب و انجام به موقع مأموریت‌ها، در سایه خودکارسازی فرایندها و سازگاری میان عوامل ذهنی و شناختی فرماندهان، امکان‌پذیر است. استفاده از سامانه فیزیکی سایبری، با لحاظ کردن جنبه‌های شناختی، فیزیکی و سایبری در بهبود کیفیت عملکرد، میزان تأثیرگذاری و پویایی سامانه از اهمیت بالایی برخوردار است و می‌تواند در سامانه‌های دفاعی مورد استفاده قرار گیرد (هلیلی و همکاران،۱۳۹۶)

تهدیدات سایبری

توسعه فضای سایبر در کنار فرصت‌ها و مزایای بی‌بدیل خود، تهدیدات فزاینده‌ای را نیز به همراه داشته است. به خاطر وابستگی مستقیم یا غیرمستقیم زیرساخت‌های حیاتی کشورها به فضای سایبر، این تهدیدات امکان ایجاد خسارات زیان‌بار و خدشه به امنیت و منافع ملی را فراهم نموده است. ازاین‌رو تهدیدات سایبری در راهبردهای اکثر کشورها، مورد توجه قرار گرفته است. در این بخش، ویژگی‌های مهم تهدیدات سایبری بررسی شده است.

واژه تهدید از نظر لغوی به معنای ترساندن، بیم دادن است (لغت‌نامه دهخدا). در لغت‌نامه آکسفورد[1] تهدید[2] به معنای شخص یا چیزی است که بتواند صدمه، خطر یا اقدام خصمانه علیه کسی یا چیزی انجام دهد. در فرهنگ لغت لانگمن[3] نیز، تهدید به معنای احتمال وقوع فاجعه و حادثه و ایجاد خطر است. از نظر مفهومی تهدید به معنای هر گونه نیت، حادثه، قابلیت و اقدام

[1] https://www.oxforddictionaries.com
[2] Threat
[3] https://www.ldoceonline.com

بالفعل و بالقوه برای مداخله یا جلوگیری از نیل به منافع و اهداف است. بنابراین تهدید سایبری را می‌توان به‌صورت زیر تعریف نمود:

هرگونه عامل بالقوه، رویداد یا واقعه با قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، سرمایه‌های ملی سایبری یا کارکنان سازمان به واسطه یک سامانه اطلاعاتی و از طریق دسترسی غیرمجاز، انهدام (تخریب)، افشاء، تغییر اطلاعات و یا ممانعت از ارائه خدمت (ایجاد اختلال).

ماهیت فراگیر و گستره جهانی فضای سایبر، زمینه‌ای برای ایجاد تهدیدات سایبری در ابعاد سیاسی، اقتصادی، اجتماعی، فرهنگی، زیست‌محیطی، و دفاعی–نظامی فراهم نموده است. تهدیدات سایبری در حوزه نظامی و دفاعی بر خلاف سایر ابعاد آن، رویکردی سخت و چهره‌ای خشن دارد. بسیاری از این تهدیدات، به خاطر محدودیت‌های بین‌المللی به صورت بالقوه وجود دارد و تنها جنبه بازدارندگی دارد. در صورت افزایش تنش و تخاصم میان کشورها این تهدیدات به مرحله عملیاتی و جنگ منجر می‌شود. در یک دسته‌بندی کلی ویژگی‌های تهدیدات سایبری را می‌توان شامل موارد زیر در نظر گرفت:

- **منشأ تهدید:** مزدوران سایبری یا گروه‌های تحت حمایت پنهان دولت‌ها، دولت‌های متخاصم، تروریست‌های سایبری، جاسوسان سایبری، مجرمین سازمان‌یافته سایبری، هکرهای دارای انگیزه سیاسی
- **پیامد تهدید:** مخاطره سایبری (احتمال بهره‌برداری یک تهدید سایبری، از آسیب‌پذیری سایبری موجود در یک سرمایه سایبری) و تهاجم سایبری(اقدام عملی تهدید برای بهره‌برداری از آسیب‌پذیری سایبری)
- **سطح تهدید:** زیرساختی، سازمانی، ملی و فراملی
- **احتمال وقوع تهدید:** احتمال بهره‌برداری تهدید از آسیب‌پذیری ایجاد مخاطره سایبری شامل: خیلی کم (مخاطره سایبری غیر محتمل)، کم (مخاطره سایبری غیر محتمل)، متوسط (مخاطره سایبری ممکن) و زیاد (مخاطره سایبری محتمل)
- **شدت تهدید:** شدت خیلی کم (تهدید منجر به خسارات محدود و قابل کنترل)، کم (تهدید سایبری حادثه‌آفرین)، متوسط (تهدید منجر به حادثه امنیتی)، شدت زیاد (بحران و خسارات گسترده سایبری مانند اختلال در شبکه بانکی)، خیلی زیاد (تهدیدات فاجعه‌بار مانند از کار افتادن شبکه برق سراسری)

همچنین برخی از مهم‌ترین انواع تهدیدات سایبری در حوزه نظامی عبارتند از:

۱) **جاسوسی سایبری:** در این نوع از تهدید امکان سرقت اطلاعات، برنامه‌ها و عملیات نظامی و فناوری‌های مرتبط با صنایع دفاعی وجود دارد. به‌عنوان‌مثال وزارت دفاع ایالات‌متحده اعلام نموده که جاسوسان سایبری اطلاعات شرکت سازنده جنگنده اف ۳۵ را که شامل میلیون‌ها کد نرم‌افزاری و گران‌قیمت‌ترین برنامه تسلیحاتی در تاریخ آمریکاست، سرقت کرده‌اند.

۲) **تروریسم سایبری**: تهدیدات تروریسم سایبری، با هدف ترساندن، و مجبور نمودن دولت‌ها برای پیشبرد اهداف سیاسی یا اجتماعی گروه‌های مخالف صورت می‌گیرد. این کار با استفاده از ابزارهای سایبری و ایجاد رعب و وحشت در جامعه انجام می‌شود. از کار انداختن سامانه‌های اضطراری، انفجار، سقوط هواپیما و .... از طریق حملات سایبری توسط تروریست‌ها قابل انجام است.

۳) **تسلیحات سایبری:** سلاح سایبری به حملات پیچیده کامپیوتر به کامپیوتر گفته می‌شود که از طریق شناسایی و بهره‌برداری آسیب‌پذیری در یک بخش از نرم‌افزار مورد استفاده توسط طرف مقابل موجب ایجاد اختلال و نابودی یک سامانه فناوری اطلاعات یا یک شبکه می‌شود (Herr, 2014). سلاح سایبری یک سلاح ناشناس و دقیق، بدون نیاز به حضور سرباز (هکر) است. این سلاح وابسته به شناسایی و بهره‌برداری از آسیب‌پذیری‌های فناوری اطلاعات است اما تنها زمانی می‌تواند کارآمد و مؤثر باشد که مخفی و محرمانه باشد و در صورت افشا شدن، کارایی خود را از دست می‌دهد. جذابیت این سلاح‌ها، عمدتاً به خاطر توانایی آنها در ایجاد عدم اطمینان نسبت به اعتبار و کارایی سامانه‌های مبتنی بر اطلاعات از جمله سامانه فرماندهی و کنترل نظامی است که در آن، محرمانگی و امنیت اطلاعات امری حیاتی است.

۴) **حمله سایبری**: عبارت است از هجوم با استفاده از سلاح سایبری به منظور صدمه زدن به اهداف مشخص. حمله سایبری با توجه به نوع سلاح سایبری مورد استفاده تعریف می‌شود نه طبیعت هدف. بنابراین یک حمله سایبری می‌تواند از یک جنگ‌افزار سایبری علیه یک دارایی غیر سایبری یا علیه یک دارایی سایبری استفاده کند اما حمله سایبری به

استفاده از یک جنگ‌افزار غیر سایبری علیه یک دارایی سایبری یا غیر سایبری اطلاق نمی‌شود.

۵) **جنگ سایبری**: در این نوع از جنگ، زیرساخت‌های حیاتی و حساس مانند اهداف نظامی، خدمات اجتماعی، سامانه‌های حمل‌ونقل، انرژی، مخابرات و... هدف قرار می‌گیرد. این نوع از جنگ به خاطر حمله از راه دور، دشواری در شناسایی و ردیابی منبع حمله از جنگ‌های سنتی متفاوت است. در جنگ سایبری به شبکه‌های رایانه‌ای نظامی دشمن نفوذ کرده و موجب تخریب آنها می‌شود.

روش‌شناسی

در این تحقیق به مفهوم‌سازی و توصیف جنبه‌های مختلف فناوری‌های نوین سایبری و تهدیدات سایبری پرداخته شده است. بنابراین این تحقیق از نظر هدف، از نوع کاربردی- توسعه‌ای است. این تحقیق از نظر ماهیت و روش گردآوری داده‌ها از نوع توصیفی موردی است. در تحقیقات توصیفی موردی محقق به دنبال مطالعه عمیق در چیستی و چگونگی یک موضوع و توصیف ویژگی‌ها و تجزیه‌وتحلیل یک پدیده است. به‌منظور گردآوری داده‌ها، از منابع کتابخانه‌ای، سایت‌های معتبر علمی، اسناد و گزارش‌های داخلی و خارجی استفاده شده است. این تحقیق ازنظر رویکرد مورداستفاده برای تجزیه‌وتحلیل داده‌ها از نوع کیفی است. در این تحقیق، روایی و پایایی بر مبنای معیارهای کرسول محقق شده است (Creswell,2014) در این روش، معیارهای روایی و پایایی شامل تماس طولانی با فضای پژوهش، مشاهده مستمر، بررسی از زوایای مختلف، گردآوری از منابع اطلاعاتی متنوع، تبادل‌نظر با همتایان است.

تجزیه و تحلیل

چالش‌ها و تهدیدات فناوری‌های نوظهور سایبری در حوزه دفاعی و نظامی

در فضای سایبر، ظهور فناوری‌های برهم زن مانند رایانش ابری، اینترنت اشیاء، کلان داده، رایانش کوانتومی، علوم شناختی و سامانه‌های فیزیکی سایبری، زمینه‌ساز ایجاد یک تحول اساسی در قالب انقلاب صنعتی چهارم است. حوزه‌های دفاعی و نظامی نیز متأثر از این فناوری‌های نوین دچار تحولات اساسی شده و ناگزیر از انطباق خود با این پدیده هستند. تغییر در ماهیت جنگ و روی آوردن به تجهیزات و تسلیحات سایبری، جایگزینی برای تسلیحات هسته‌ای شده و این مسئله، نقشی حائز اهمیت در امنیت ملی و تعاملات بین‌المللی ایفا می‌کند. بااین‌حال، توسعه فناوری‌های

نوین فضای سایبر تهدیدات و مخاطرات متنوعی را به همراه دارد که هرچه وابستگی به این فضا بیشتر باشد عمق و میزان تأثیر مخاطرات ناشی از این تهدیدات نیز بیشتر خواهد بود. در حوزه‌های دفاعی و نظامی، هرکدام از کلان‌روندهای فناورانه فضای سایبر، چالش‌ها و تهدیداتی به همراه دارد که لزوم مواجهه فعال و هوشمندانه با آنها امری ضروری و اجتناب‌ناپذیر است. در این بخش، برخی از کاربردها و تهدیدات سایبری این فناوری‌های در جدول (۳) به‌صورت خلاصه ارائه شده است.

جدول (۳): کاربردها و تهدیدات فناوری‌های نوظهور سایبری در سامانه‌های نظامی و دفاعی

	کاربردهای نظامی	تهدیدات سایبری
اینترنت اشیاء	در حوزه نظامی برای هدایت و مدیریت تجهیزات، تدارکات، فعالیت‌های نظامی، سربازان و... در میدان نبرد، مأموریت‌ها و آموزش‌ها مثلاً اطلاع فرماندهان از وضعیت سلامت جسمانی نیروها در هر زمان و تسهیل در تصمیم‌گیری در لحظات دشوار از اینترنت اشیاء استفاده می‌شود. در صنعت هوانوردی استفاده از حسگرهای فشار، دما، لرزش و غیره و ارسال آنها برای خلبان و برج مراقبت کاربرد دارد.	استفاده از اینترنت اشیاء در تجهیزات نظامی، امکان جاسوسی، نفوذ و سرقت اطلاعات را افزایش می‌دهد. همچنین در صورت عدم بکارگیری مکانیسمهای امنیت سایبری، امکان استفاده از سلاح‌های سایبری برای وارد نمودن صدمه به تجهیزات و نیروها، افزایش می‌یابد.
رایانش ابری	در سازمان‌های دفاعی، فناوری اطلاعات و ارتباطات به‌منظور ایجاد قابلیت اطمینان، انعطاف‌پذیری، توانمندسازی، اقتصادی بودن، سهولت و سرعت در ارائه خدمات، کاهش هزینه عملیات پشتیبانی و یکپارچه‌سازی ارتباطات، موردتوجه قرار گرفته است. علاوه بر آن، در این سازمان‌ها کارایی، اثربخشی و چابک‌سازی فرایند اجرای مأموریت، از خواسته‌های مهمی	در سامانه‌های دفاعی، حتی در صورت استفاده از بستر فیزیکی ابر خصوصی، ارسال، دریافت و ذخیره‌سازی داده در زیرساختی که خارج از محدوده و کنترل است؛ با چالش‌های امنیتی مانند محرمانگی، احراز هویت و کنترل دسترسی مواجه است. علاوه بر آن، در سامانه‌های دفاعی، اشتراک اطلاعات، برای انطباق با زیرساخت ابری نیازمند

	است که این سازمان‌ها را به استفاده از رایانش ابری ترغیب می‌نماید.	واسط‌هایی است که امنیت این واسط‌ها نیز چالش‌برانگیز است.
کلان داده	در سازمان‌های دفاعی و امنیتی، به‌منظور آگاهی از وضعیت سازمان و نیروها، تصمیم‌گیری راهبردی و انجام عملیات نظامی با کلان داده‌ها مواجه هستیم. این حجم انبوه از داده‌ها، ممکن است ماشینی باشد و از تجهیزات مختلفی مانند کشتی‌ها، هواپیماها و وسایل حمل‌ونقل، ماهواره‌ها، پهپادها و رادارهای مراقبت، هواپیماهای ردگیری، حسگرهای هوشمند بیسیم در میدان نبرد، به دست آید؛ یا دارای منشأ انسانی باشد و از رسانه‌های اجتماعی، سایت‌ها، شبکه‌های اجتماعی، تراکنش‌های مالی و .... تولید شود. در سامانه‌های دفاعی، داده‌ها از حسگرهای محیطی، ماهواره، سامانه‌های جنگ الکترونیک الینت، کامینت، سیگینت، رسانه‌های اجتماعی و غیره به دست می‌آید. این اطلاعات به‌منظور، غنی‌سازی، کشف همبستگی، اشتراک و به‌روزرسانی در یک هاب داده سازمانی[1] (EDH) جمع‌آوری‌شده و پس از تحلیل‌های پیشرفته و بلادرنگ برای ایجاد اخطار و آگاه‌سازی و یا ارزیابی میدان نبرد مورداستفاده قرار می‌گیرند.	در سازمان‌های دفاعی و امنیتی با توجه به توسعه و گسترش سامانه‌های مختلف ارتباطی، منابع داده و حجم داده به‌صورت نمایی در حال افزایش است. جمع‌آوری و استخراج اطلاعات از این داده‌های حجیم، نیازمند استفاده از فناوری‌های نوین کلان داده است. اما در صورت وابستگی فناورانه، تهدیدات سایبری را ایجاد خواهد نمود. در کلان‌داده به خاطر حجم ذخیره‌سازی بالا و توان پردازشی زیاد، استخراج دانش از داده‌ها مراحل مختلفی مانند دریافت، ذخیره، انتقال، مدیریت، تجزیه‌وتحلیل و مصورسازی داده انجام می‌شود. انباشت و نگهداری این داده‌ها، تهدیداتی همچون نشت اطلاعاتی و جاسوسی سایبری را به همراه خواهد داشت. تصمیم‌گیری در مورد نحوه مدیریت صحنه نبرد و برتری در میدان جنگ در آینده مستلزم بکارگیری کلان‌داده و فناوری‌های وابسته به آن است. بااین‌حال امکان تحریف و تغییر اطلاعات و اخذ تصمیم نادرست، یا

1. Enterprise Data Hub

	تنوع داده‌های جمع‌آوری‌شده و لزوم سرعت پردازش و تحلیل ضرورت استفاده از فناوری‌های کلان‌داده را در سامانه‌های نوین مشخص می‌سازد.	دریافت دستورات جعلی همواره وجود دارد. حساسیت و اهمیت اطلاعات در سامانه‌های دفاعی مستلزم دستیابی به فناوری‌های رمزنگاری پیشرفته است و در صورت عدم تضمین و تأمین امنیت سایبری مراکز داده در معرض حملات و تهدیدات سایبری قرار دارند.
سامانه‌های فیزیکی، سایبری	یک سازمان نظامی کارآمد باید دارای انعطاف‌پذیری لازم، قابلیت پاسخگویی، نوآورانه، تاب آور و سازگار در جنگ‌های شبکه محور امروزی را داشته باشد. این ویژگی‌ها توسط سامانه‌های هم‌زمان و خودکار انجام می‌شود. چالش اصلی، این سامانه‌ها، یکپارچه‌سازی حوزه‌های مختلفی فیزیکی سایبری، اطلاعاتی و شناختی است. راه حل این مسئله استفاده از سامانه فیزیکی، سایبری است. در سامانه‌های فیزیکی سایبری، تعامل میان عناصر ذهنی با عناصر فیزیکی در یک زنجیره کنترل مؤثر ایجاد می‌شود. یکپارچه‌سازی سامانه‌های فیزیکی، اشتراک اطلاعات، فرایندهای تصمیم‌گیری و فرایند هم‌زمان‌سازی عملیات در چنین سازمان‌هایی موجب پویایی آنها نسبت به سامانه‌های سنتی خواهد شد.	ایجاد یک تصویر مطلوب از عملیات مشترک و شفاف‌سازی مأموریت‌ها، بر اساس معماری سامانه‌های فیزیکی سایبری نیازمند یکپارچه‌سازی میان منابع حوزه‌های فیزیکی و انسانی است. که چالش‌های امنیت سایبری در صورت عدم درک و شناخت عوامل انسانی و بومی نبودن تجهیزات می‌تواند تهدید زا باشد. در سامانه‌های فیزیکی سایبری اشتراک اطلاعات، و تطابق حوزه اطلاعاتی با شناختی از طریق زیرساخت‌های فضای سایبر انجام می‌شود. این مسئله نیازمند اختصاص زیرساخت مستقل و امن برای پیشگیری از حملات سایبری مجرمان سایبری و گروه‌های متخاصم است.

	استفاده از سامانه‌های فیزیکی سایبری در سازمان‌های دفاعی موجب می‌شود، به‌جای کنترل اقدامات فردی، هم‌زمان‌سازی اطلاعات از طریق شناخت و تصمیم‌گیری یکپارچه در هدایت رفتار سازمانی انجام می‌شود و به‌جای یک سازمان فردی یا منطقه‌ای یک سازمان چندجانبه و همه‌منظوره ایجاد شود.	همگام‌سازی و هم‌زمان‌سازی مأموریت، میان واحدهای عملیاتی از چالش‌های مهمی است که در سامانه‌های فیزیکی سایبری مبتنی بر شبکه جهانی اینترنت منشأ بسیاری از تهدیدات خواهد بود.

نتیجه

در سال‌های اخیر، سرمایه‌گذاری وسیعی توسط کشورهای پیشتاز و پیشرفته صنعتی در حوزه فناوری‌های کلیدی فضای سایبر انجام شده است. این فناوری‌ها زمینه‌ساز وقوع انقلاب صنعتی چهارم هستند و اکثر کشورها به استفاده از آنها در حوزه‌های مختلف ترغیب شده‌اند. حمایت از توسعه فناوری‌های نوین، یکی از مهم‌ترین وظایف و دغدغه دولت‌هاست و امروزه پروژه‌های مرتبط با استفاده از فناوری‌های سایبری در حوزه‌های مختلف ازجمله نظامی و دفاعی در کشورهای پیشرو در حال اجراست. در این حوزه، به خاطر حساس بودن اطلاعات مورداستفاده در سامانه‌های اطلاعاتی، پذیرش و توسعه تجهیزات نیازمند تأمل و تمهیدات بیشتری است. تهدیدات سایبری در حوزه دفاعی و نظامی در سطوح راهبردی می‌تواند امنیت و منافع ملی کشورها را خدشه‌دار کند. بنابراین تولنایی یک کشور برای دفاع از زیرساخت‌های کلیدی نظامی و ملی در برابر حملات سایبری و قدرت بازدارندگی و تهاجم، توانایی یک کشور در محافظت از اطلاعات محرمانه و سری مرتبط با صنایع دفاعی، از اهمیت بالایی برخوردار است.

در این مقاله پس از مروری بر مهم‌ترین فناوری‌های فضای سایبر به بررسی تهدیدات سایبری مرتبط با آنها در حوزه دفاعی و نظامی پرداخته شده است. نتایج این تحقیق نشان می‌دهد در استفاده از این فناوری‌ها، باید میان نگرانی‌های امنیتی ناشی از دستیابی به اطلاعات حساس و کارایی‌های جذاب و وسوسه‌انگیز آنها، مصالحه برقرار نمود. استفاده از رایانش ابری در سازمان‌های دفاعی می‌تواند موجب افزایش و تسهیل در حملات سایبری شود. بنابراین استفاده از آن مستلزم غلبه بر چالش‌های امنیت اطلاعات است. فناوری‌های مرتبط با کلان‌داده، به‌صورت مستقیم و غیرمستقیم در سازمان‌های دفاعی کاربرد دارد. توسعه دانش، مدیریت سامانه‌های اطلاعاتی و

جغرافیایی، شبیه‌سازی و تصویرسازی صحنه نبرد، مدیریت یکپارچه و مرکزی سامانه‌های فرماندهی و کنترل از کاربردهای مستقیم این فناوری و استفاده از کلان‌داده در جنگ‌های نامتقارن، ترکیبی، شبکه‌ای، عملیات ضد تروریستی در فضای سایبر، از جمله کاربردهای غیرمستقیم این فناوری است. بااین‌حال حساسیت و اهمیت اطلاعات در سامانه‌های دفاعی، مستلزم دستیابی به فناوری‌های رمزنگاری پیشرفته است و در صورت عدم تضمین و تأمین امنیت سایبری مراکز داده در معرض حملات و تهدیدات سایبری قرار دارند. معماری مورداستفاده در سامانه‌های فیزیکی سایبری و ایجاد سازگاری و تعامل میان فرایندهای ذهنی و شناختی فرماندهان با اینکه سامانه‌های فیزیکی در محیط‌های پیچیده و پویای عملیاتی می‌تواند موجب بهبود کیفیت و کارایی سازمان‌های دفاعی شود اما بهره‌برداری مناسب از این فناوری نیز به خاطر تهدیدات سایبری نیازمند زیرساخت‌های ارتباطی و شبکه‌های اختصاصی است.

در جمهوری اسلامی ایران، توسعه فناوری‌های نوین سایبری در صنایع نظامی می‌تواند از طریق شرکت‌های دانش‌بنیان صورت گیرد و دولت بهتر است در این حوزه نقش رگولاتوری و نظارتی داشته باشد و با توجه به همگرایی این فناوری‌ها، راهبردهایی برای تضمین امنیت اطلاعات در سامانه‌های دفاعی داشته باشد. همچنین پیشنهاد می‌شود نحوه به‌کارگیری هرکدام از فناوری‌های مطرح‌شده در کاربردهای نظامی و نیز راهکارهای امنیتی برای غلبه بر چالش‌ها و تهدیدات سایبری مرتبط با آن در پژوهش‌های آتی موردتوجه قرار گیرد.

مراجع و منابع

۱. قاسمی، روح ا... و دیگران (۱۳۹۵). اولویت‌بندی کاربردهای فناوری اینترنت اشیا در بخش بهداشت و درمان ایران :محرکی برای توسعه پایدار، نشریه مدیریت فناوری اطلاعات، شماره ۱، ۱۵۵-۱۷۶

۲. قرشی، سید علی، شبرو، مریم (۱۳۹۳). مقدمه ای بر نحوه بکارگیری فن آوری اینترنت اشیاء در شبکه هوشمند صنعت برق کشور، بیست و نهمین کنفرانس بین‌المللی برق، تهران، ایران

موزونی، عباس (۱۳۹۵). سمینار رسانه در آستانه اینترنت اشیاء، صدا و سیما

۳. ولوی، محمدرضا. موحدی صفت، محمدرضا و باقری ایمان. (۱۳۹۶). ارائه الگوی راهبردی مهاجرت سازمان‌های دفاعی به محیط رایانش ابری. فصلنامه مدیریت نظامی، سال هفدهم، شماره ۱. صص:۱۰۶-۱۳۰

۴. هلیلی خداداد. کاظمی، سید محسن و دهقانی، مهدی. (۱۳۹۴). بررسی الزامات و مکانیسم‌های امنیتی در سامانه‌های فرماندهی و کنترل مبتنی بر رایانش ابری (CBC4I). نهمین کنفرانس ملی فرماندهی و کنترل ایران. دانشگاه خوارزمی.

۵. هلیلی، خداداد. ولوی، محمدرضا. (۱۳۹۶). فناوری کلان داده، فرصت‌ها، چالش‌ها و راهبردها. فصلنامه علمی پژوهشی مطالعات بین‌رشته‌ای دانش راهبردی. سال هفتم شماره ۲۸. صص: ۷-۲۸

۶. هلیلی، خداداد. مظلوم، جلیل و هادیان، بهرنگ. (۱۳۹۴). بررسی کاربردهای نظامی فناوری کلان داده و نقش آن در مدیریت صحنه نبرد. فصلنامه علوم و فنون نظامی، سال یازدهم شماره ۳۳. صص ۴۷-۶۲

۷. هلیلی، خداداد. سلطانپور، محمدرضا و موسوی، فاطمه سادات. (۱۳۹۴). لزوم بکارگیری فناوری کلان‌داده در سامانه‌های C4I و بررسی چالش‌های آن. نهمین کنفرانس ملی فرماندهی و کنترل ایران. دانشگاه خوارزمی

۸. هلیلی، خداداد. ولوی، محمدرضا و موحدی صفت، محمدرضا. (۱۳۹۶). مدلسازی فرایندهای C4I توسط سامانه‌های فیزیکی- سایبری- اجتماعی (CPSS). دهمین کنفرانس ملی فرماندهی و کنترل ایران. دانشگاه خاتم‌الانبیاء (ص)

1. Ashibani, Y. Mahmoud, Q. H. (2017). Cyber physical systems security: analysis, challenges and solutions, Computers & Security Volume 68, PP 81-97
2. Berger, Ch. M. R. Mousavi, R. Wisniewski (Eds.) (2016). Cyber Physical Systems, Design, Modeling, and Evaluation, 6th International Workshop, CyPhy, Pittsburgh, PA, USA
3. Creswell J. W. (2014). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). Thousand Oaks, CA: Sage
4. Galis, Alex, Gavras, Anastasius (Eds.) (2013). the Future Internet: Future Internet Assembly Validated Results and New Horizons. Lecture Notes in Computer Science, springer.
5. Herr, T. Prep, (2014). A framework for malware & cyber weapons, The Journal of Information Warfare, 13(1), 87–106.
6. Tan, J. Simon, Koo, G. M. (2014). A Survey of Technologies in Internet of Things, IEEE International Conference on Distributed Computing in Sensor Systems
7. Zhou, H. (2013). Internet of Thing in the Cloud, a Middleware Perspective, CRC Press
8. Klems, M., Lenk, A., Nimis J. et.al. (2009). what's Inside the Cloud? An Architectural Map of the Cloud Landscape. IEEE Xplore, pp 23-31
9. Bhisikar, A. (2011). G-Cloud: New Paradigm Shift for Online Public Services. International Journal of Computer Applications, vol. 22.
10. Mills, S. (2012). Demystifying Big Data: A practical guide to transforming the business of Government ،Technical report. Washington ،D.C: Tech America Foundation
11. Schwab, K. (2015). The Fourth Industrial Revolution: what it means and how to respond, World Economic Forum, https://agenda.weforum.org/2015/12/the-fourth-industrial-revolution-what-it-means-and-how-to-respond.