

چالش آفرینی اینترنت اشیاء بر ارکان امنیت ملی کشور

محمد رضا کریمی قهرودی^۱

احسان کیان خواه^۲

تاریخ پذیرش: ۹۴/۰۴/۲۵

تاریخ دریافت: ۹۴/۰۳/۱۵

چکیده

اینترنت اشیاء به سرعت در حال گسترش است. اشیاء متنوعی از پوشیدنی، ثابت و متحرک با قابلیت عمل فیزیکی با فرمان سایبری در حال گسترش است. اینترنت آینده با نفوذ در همه شئون زندگی انسان از حالات شخصی و فردی تا تعاملات جمعی اجتماعی، اقتصادی، سیاسی و فرهنگی در حال خلق دنیایی جدید برای انسان است. در عصر سایبر با درهم تنیده شدن گسترده زندگی و تکنولوژی‌های غیر بومی تهدیدات نوینی متوجه امنیت ملی شده است. از آنجایی که این تکنولوژی‌ها عموماً بومی نبوده و متعلق به کشورهای متخاصم و یا هم‌پیمانان آن‌ها است، چالش‌هایی را متوجه امنیت ملی خواهد کرد. تحقیق با شکل‌دهی به پرسشنامه محقق ساخته براساس اثرات اینترنت اشیاء و تکنولوژی‌های مرتبط آن با امنیت ملی نظرات متخصصان این حوزه را مورد پرسش قرار داده است. سپس با تکنیک معادلات ساختاری و نرم‌افزار SmartPLS مورد تحلیل قرار گرفته است. مردم و سبک زندگی، حاکمیت و قلمرو و جغرافیا متحمل چالش‌هایی نو خواهد شد. ماشینی شدن زندگی انسان، غفلت انسان از مسئولیت دنیوی و اخروی، تغییر سبک زندگی جامعه به سبک زندگی غربی، اشراف اطلاعاتی دشمن بر تعاملات اجتماعی، اقتصادی، سیاسی، دانش راهبردی و کاهش حفاظت از سرمایه‌های ملی از اثرات گسترش اینترنت اشیاء در کشور خواهد بود. باید با درک صحیح چالش‌های آینده، راهبردهایی را در شکل‌دهی به قدرت درون‌زای سایبری اتخاذ نمود.

واژه‌های کلیدی:

اینترنت اشیاء، چالش‌های امنیت ملی، مردم، حاکمیت، قلمرو

^۱ دکتری آینده پژوهی - موسسه آموزشی و تحقیقاتی صنایع دفاعی

^۲ دانشجوی دکتری مدیریت راهبردی فضای سایبر دانشگاه عالی دفاع ملی و پژوهشگر پژوهشگاه فرهنگ و اندیشه

مقدمه و بیان مسئله

در عصر سایبر با درهم تنیده شدن گسترده زندگی و فناوری‌های غیربومی تهدیدات نوینی متوجه امنیت ملی شده است. فضای سایبر در حال ساخت محیط جدیدی در فضای فرهنگی و هویتی است. تا قبل از عصر سایبر هویت انسان به نژاد، قبیله و عرصه جغرافیایی استوار بود و زیست جهان مشهود و نامشهود در مکان و زمان خاص جغرافیایی فرهنگ را تشکیل می‌داد. اما با شکل‌گیری و رشد سریع فضای سایبر مفاهیم عرصه زندگی نیز به سمت تغییر ماهوی گام برداشت. همه چیز از هویت، فرهنگ، حکمرانی، روابط و تعاملات خصوصی و گروهی در حال تغییر است. فناوری به علت ماهیت جذاب و نوآورانه‌ی خود بدون توجه به تهدیدهای آشکار و پنهان این فضا، مورد پذیرش عمومی قرار می‌گیرد. این پذیرش عمومی و گسترده موجب بروز چالش‌های هویتی، فرهنگی، سیاسی، اقتصادی در سطح ملی خواهد شد. در این دوران، رابطه بین امنیت ملی و فضای سایبر پیچیده، وابسته به زمان و غیرخطی شده است.

یکی از ابعاد گسترش و توسعه فضای سایبر در دهه‌های آینده، اینترنت اشیا است. اینترنت اشیا بیانگر تعداد و تنوع اشیا فیزیکی متصل به هم در بستر اینترنت است. اینترنت اشیا، انسان‌ها، وسایل و مکان‌ها را به هم گره می‌زند. پیش‌بینی می‌شود، بیش از ۵۰ میلیارد شیء تا سال ۲۰۲۰ به اینترنت متصل خواهد شد (ایوانس^۱، ۲۰۱۱). این اشیا شبکه شده، تور قدرتمندی را شکل خواهد داد که سلامتی و بیماری، رفتار فیزیکی و سایبری انسان‌ها، آمایش سرزمینی تجهیزات فنی و صنعتی، مدیریت زنجیره تأمین و نظارت بر جریان تأمین مواد غذایی، تجهیزات صنعتی و خطوط انرژی را رصد و کنترل می‌نماید. اینترنت اشیا و تکنولوژی‌های مرتبط در حقیقت قابلیت کنترل افکار و برنامه‌های فردی، اجتماعی و حاکمیتی را در مکان‌های متنوع از نظامی و سیاسی تا فرهنگی تفریحی دارد. جریان داده و اطلاعات حاصل از این اشیا و تحلیل و داده‌کاوی آن‌ها قدرت تأثیرگذاری نوینی را شکل خواهد داد. قدرت سایبری شکل گرفته با گسترش اینترنت اشیا حضور پررنگ‌تری در تعاملات سیاسی، اقتصادی و فرهنگی درون و بین کشورها خواهد داشت. این قدرت هم توانمندی تغییر سبک زندگی و رفتار فردی و جمعی جوامع را دارد و هم قدرت تأثیرگذاری اقتصادی، سیاسی و نظامی بر جوامع را دارد. قدرت سایبری شاید به‌ظاهر در اختیار بهره‌بردار باشد اما به علت ذات تکنولوژی دیجیتال و ارتباطات جهانی پرسرعت و فناوری‌های

¹ Evans

مرتبط با اینترنت اشیاء، صاحبان تکنولوژی‌های فضای سایبر، این قدرت را در اختیار داشته و مدیریت و برنامه‌ریزی می‌کنند.

مسئله و دغدغه اصلی این تحقیق بررسی فناوری اینترنت اشیاء و تکنولوژی‌های مرتبط با آن و تأثیر این فناوری بر امنیت ملی و شناسایی چالش‌های نوپدید بر ارکان امنیت ملی جمهوری اسلامی است. در ضرورت تحقیق می‌توان بیان داشت که از آنجایی که ماهیت اصلی انقلاب اسلامی در تقابل با فرهنگ، اقتصاد و سیاست تمدن غربی و سبک زندگی شکل یافته از این تمدن است و چالش‌هایی را متوجه امنیت ملی جمهوری اسلامی می‌کند لذا بررسی چالش‌های امنیت ملی با گسترش اینترنت اشیاء که با سرعت بالایی درون جامعه ما در حال نفوذ است، لازمه حذف آسیب پذیری هاست.

هدف اصلی این تحقیق «شناسایی چالش‌های اینترنت اشیاء بر ارکان امنیت ملی جمهوری اسلامی» است. از این رو، سؤال اصلی این تحقیق عبارت است از: «چالش‌های نوین امنیت ملی جمهوری اسلامی ایران متأثر از گسترش اینترنت اشیاء و فناوری‌های مرتبط با آن کدام است؟». همچنین سؤالات فرعی این پژوهش عبارت است از: (۱) مفهوم اینترنت اشیاء و فناوری‌های مرتبط و خدمات شکل گرفته از آن چیست؟ و (۲) چالش‌های گسترش اینترنت اشیاء و فناوری‌های مرتبط بر ارکان امنیت ملی چیست؟

روش تحقیق

روش پژوهش حاضر کاربردی و آینده‌نگر است و از آنجایی که تحقیق مشابهی وجود ندارد، پژوهش از نوع توسعه ای است. اطلاعات مورد نیاز برای این پژوهش از طریق بررسی منابع کتب و مقاله‌های پژوهشی و نتایج تحقیقات و پروژه‌های بین‌المللی، جمع‌آوری شده سپس مورد مذاقه و تحلیل قرار گرفته و مفهوم و اینترنت اشیاء، تکنولوژی‌های مرتبط و سرویس‌های شکل یافته از آن در دهه آینده ترسیم شده است. از طرفی امنیت ملی مورد بررسی قرار گرفته و براساس چالش‌های حاصل از گسترش اینترنت اشیاء پرسشنامه‌ای از ابعاد چالش‌ها طراحی شده و از محققان حوزه امنیت ملی و فضای سایبر مورد پرسش قرار گرفته است. نتایج با مدل‌سازی معادلات ساختاری و با نرم‌افزار SmartPLS تحلیل شده است. برای حداقل نمونه لازم در روش PLS، بارکلای و همکاران (۱۹۹۵) ارائه شده است (داوری و رضازاده، ۱۳۹۲). این نویسندگان اظهار می‌دارند که حداقل حجم نمونه لازم برای استفاده از روش PLS برابر است با بزرگ‌ترین مقدار حاصل از دو

قاعده؛ (۱) ۱۰ ضرب در تعداد شاخص‌های مدل اندازه‌گیری که دارای بیشترین شاخص در میان مدل‌های اندازه‌گیری مدل اصلی پژوهشی است؛ (۲) ۱۰ ضرب در بیشترین روابط موجود در بخش ساختاری مدل اصلی پژوهش که به یک متغیر مربوط می‌شوند (همان). با این فرض حجم نمونه برای این مدل تحقیق، براساس این دو الگو برابر با ۴۰ و ۳۰ است. در این تحقیق حجم نمونه ۴۰ نفر از بین متخصصان حوزه سایبر و امنیت ملی انتخاب شده است که دارای مدرک کارشناسی ارشد و دکتری هستند و نتایج براساس این حجم نمونه مورد ارزیابی قرار گرفته است.

مبانی نظری

پیشینه تحقیق

در پیشینه این تحقیق، به‌رغم اهمیت موضوع، پژوهش یا تحقیقات مناسب و علمی در تبیین چالش‌های امنیت ملی با گسترش اینترنت اشیاء مشاهده نشد که انگیزه ای مضاعف در محقق ایجاد نمود. اگرچه از بین محدود کارهای پژوهشی و تحقیقات مرتبط با این حوزه می‌توان به «تهدیدات سایبری و تأثیر آن بر امنیت ملی» (خلیلی پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱) و «تأثیر فضای مجازی بر امنیت ملی جمهوری اسلامی و ایران و ارائه راهبرد» (قدسی، ۱۳۹۲) اشاره نمود. خلیلی و نورعلی‌وند در تحقیق خود معتقد هستند که فضای سایبر مفهوم امنیت را تغییر داده است و امنیت ملی دیگر صرفاً در ارتباط با مرزهای جغرافیایی نیست بلکه افت کیفیت شهروندان نوعی تهدید امنیت ملی است. از میان رفتن بعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، تغییر ماهیت تهدید و گستردگی آسیب‌پذیران از تأثیرات فضای سایبر بر امنیت ملی است. در پژوهش دیگر، قدسی، به بررسی تأثیر فضای مجازی بر امنیت ملی در حوزه‌های اجتماعی - فرهنگی، سیاسی، امنیت و روان‌شناختی پرداخته است. دو تحقیق فوق تأثیر فضای سایبر بر امنیت ملی را از دو نگاه مختلف بررسی نموده‌اند، اما پژوهش حاضر بر آن است با توجه به ویژگی‌های اینترنت اشیاء و فناوری‌های مرتبط که پرچم‌دار حضور گسترده و متنوع فضای سایبر در دهه‌ی آینده است، چالش‌های امنیت ملی کشور را شناسایی نماید.

۱- اینترنت اشیاء

۲- توسعه پرشتاب فناوری اینترنت، زندگی فیزیکی را به سمت دنیای مجازی^۱ سوق می‌دهد. انسان‌ها توانمندی گفتگو، تجارت، انجام فعالیت‌های کاری، خرید در دنیای مجازی را دارند.

^۱ Virtual world

باین‌حال، انسان‌ها در دنیای واقعی زندگی می‌کنند و هنوز فعالیت‌های انسانی به‌طور کامل از طریق فضای خیالی قابل انجام نبوده است. برای حذف این محدودیت، فناوری جدیدی مورد نیاز است که به ادغام فضای خیالی و دنیای واقعی در قالب پردازد. این فناوری اینترنت اشیا^۱ است که از تعداد زیادی حسگر^۲ ارزان‌قیمت و ارتباطات بی‌سیم تشکیل شده است. این تغییرات بزرگ آینده جامعه و شیوه زندگی و مدل کسب‌وکار را تغییر خواهد داد (کومار و پاتل^۳، ۲۰۱۴). اینترنت اشیا قابلیت اتصال هرچیز در هر مکان و هر زمان با هر وسیله ای را به کاربران می‌دهد (شکل ۱).



شکل ۱. ویژگی اینترنت اشیا (پروا و همکاران، ۲۰۱۳)

واژه اینترنت اشیا اولین بار در سال ۱۹۹۹ توسط کوین اشتون در مدیریت زنجیره تأمین بکار گرفته شد (اشتون^۴، ۲۰۰۹). اشیا بیان شده بیانگر برداشت و جمع‌آوری اطلاعات بدون کمک انسان است (گابی^۵ و همکاران، ۲۰۱۳). امروزه اینترنت انسان‌ها را به اطلاعات متصل می‌کند. اما اینترنت اشیا محصولات و خدمات جدیدی را با قابلیت اتصال انسان‌ها و سازمان‌ها به وسایل نقلیه، مراکز درمانی، وضعیت آب و هوا، وضعیت ترافیک، سامانه‌های کنترل انرژی و کنترل‌های محیطی متنوعی را در دسترس قرار داده و هوشمندی نوینی را مبتنی بر تعاملات انسان و اشیا پدید می‌آورد. این انقلاب در شبکه اینترنت، صرفاً جمع‌آوری اطلاعات توسط حسگرها نیست

¹ Internet of Things (IoT)

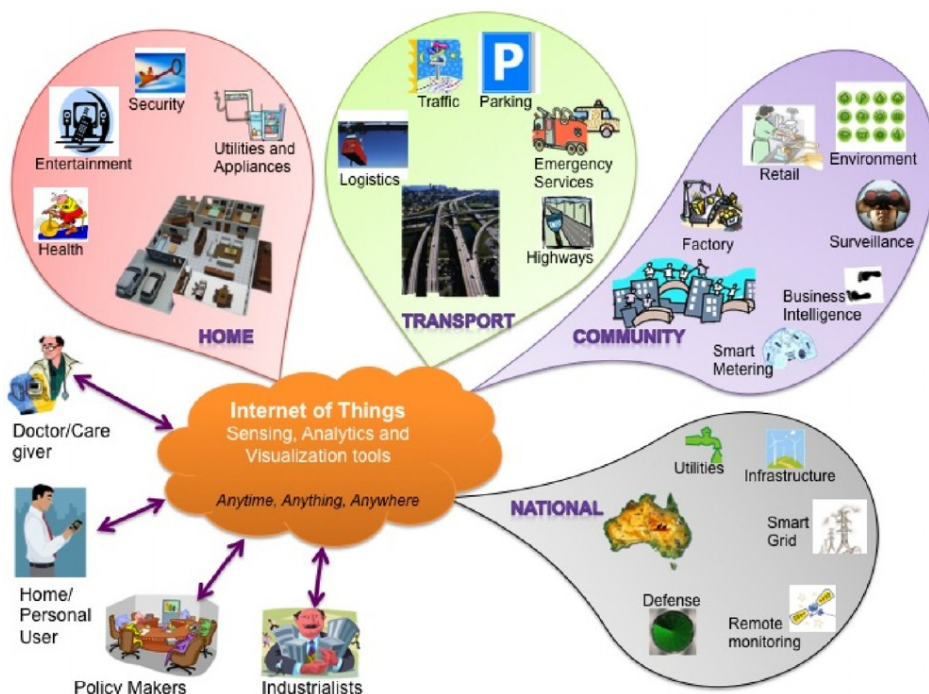
² Sensors

³ Kumar and Patel

⁴ Ashton

⁵ Gubbi

بلکه تعامل با محیط فیزیکی، کنترل، فرمان و عمل از طریق فضای سایبر در محیط فیزیکی خواهد بود، اما در حال حاضر اینترنت و بگردی، تحلیل و به‌کارگیری اطلاعات است. اینترنت اشیاء نمایشی از یکپارچگی کامل در اینترنت آینده است (باکلی^۱، ۲۰۰۶). پیشرفت ریزسامانه‌های الکترومکانیکی^۲، ارتباطات به یسیم، الکترونیک دیجیتال موجب توسعه حسگرهای مینیاتوری، پردازش اطلاعات، و ارتباطات به یسیم در مسافت‌های کوتاه شده است. در شکل ۲ بیان شده است که، اینترنت اشیاء ابزاری برای حسگری، تحلیل و مجازی‌سازی است و هر زمان، هر مکان و هر در شی وجود دارد، به ترتیب از چپ به راست در خانه (حوزه‌های سلامت، سرگرمی، امنیت و مدیریت بهینه)، در حمل‌ونقل (پشتیبانی و لجستیک، ترافیک، پارکینگ، خدمات فوریتی و مدیریت بزرگ‌راه‌ها)، در اجتماع (کارخانه‌ها، خرده‌فروشی، محیط، ردیابی، هوش تجاری و جلسات هوشمند) و در سطح ملی (دفاع، مدیریت منابع آبی، زیرساخت‌ها، شبکه‌های توزیع برق و نظارت از راه دور) کاربرد وسیعی خواهد داشت.



شکل ۲. نمایشی از کاربردهای اینترنت اشیاء برای کاربران نهایی (گالی و همکاران، ۲۰۱۳)

¹ Buckley

² micro-electro-mechanical systems (MEMS)

در سال ۲۰۰۳، ساکنین زمین ۶.۳ میلیارد نفر زندگی بودند و ۵۰۰ میلیون دستگاه به اینترنت متصل بود. این وضعیت تا سال ۲۰۲۰ که جمعیت کره زمین به ۷.۶ میلیارد نفر خواهد رسید و به ۵۰ میلیارد دستگاه افزایش خواهد یافت (ایوانس، ۲۰۱۱). سه عامل کلیدی موجب توسعه سریع اینترنت اشیا شده است: (۱) کوچک‌سازی^۱: دستگاه‌های الکترونیکی در حال کوچک‌تر شدن، قوی‌تر شدن با مصرف انرژی کارا تر هستند؛ (۲) کاهش هزینه^۲: هزینه‌های عناصر الکترونیکی و شبکه‌ها در حال کاهش است؛ (۳) به یسیم شدن^۳: پیش‌ازپیش همه‌چیز در حال بیسیمی شدن است و آخرین کابلی که ناپدید خواهد شد، کابل برق است (کلمریت و ابدوفسکی^۴، ۲۰۱۱). پیشرفت فناوری اینترنت اشیا (IOT) در بسیاری از زمینه‌ها، موازی و اغلب متداخل با سایر تکنولوژی‌ها از جمله سیستم‌های توکار^۵، رایانش فراگیر و همه جا^۶، تلفن همراه، دورسنجی و ارتباطات ماشین به ماشین^۷، شبکه حسگرهای بی‌سیم^۸، محاسبات موبایلی^۹ و شبکه‌های کامپیوتری است. اینترنت اشیا چیزهای متفاوت برای افراد مختلف است. عناصر تشکیل‌دهنده اینترنت اشیا (۱) شیء فیزیکی^{۱۰}، (۲) کنترل‌کننده‌ها، حسگرها و عملگرها^{۱۱} و (۳) اینترنت است (مک ایون^{۱۲} و ۲۰۱۳). این عناصر در کنار هم هوشمندی سایبری را برای اشیا فیزیکی به ارمغان خواهد آورد (شکل ۳).

¹ Miniaturization

² Affordability

³ De-wireization

⁴ Kellmerein and Obodovski

⁵ Embedded systems

⁶ Ubiquitous and pervasive computing

⁷ Telemetry and machine-to-machine communication

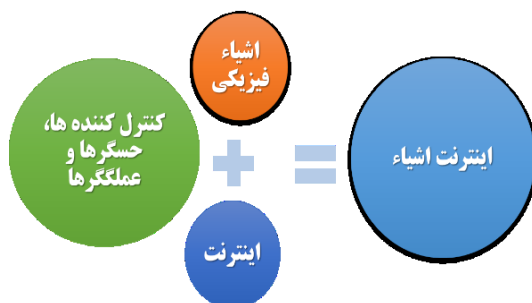
⁸ Wireless sensor networks (WSN)

⁹ Mobile computing

¹⁰ Physical Object

¹¹ Controller, Sensors, and Actuators

¹² McEwen



شکل ۳. عناصر تشکیل دهنده اینترنت اشیاء

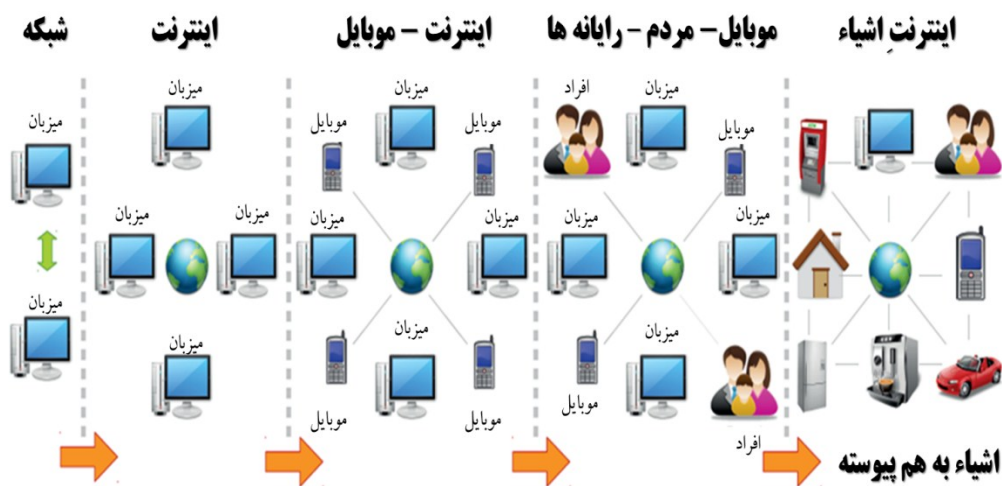
اینترنت اشیاء تکامل یافته، دنیای ساخته شده توسط اینترنت است. در اواخر دهه ۱۹۶۰ میلادی دو کامپیوتر با شکل گیری مفهوم شبکه های کامپیوتری و سویچینگ بسته ها به یکدیگر متصل شدند. در اوایل دهه ۱۹۸۰ میلادی پروتکل^۱ TCP/IP برای اتصال کامپیوترها و شبکه های متنوع کامپیوتری کامپیوتری معرفی شد. در سال ۱۹۹۱ مفهوم وب پا به عرصه اینترنت گذاشت. اتصال تلفن های همراه به اینترنت و ظهور شبکه های اجتماعی بر حجم و گستردگی اینترنت شتاب مضاعفی وارد شد و کاربر به جزئی از شبکه تبدیل شد. در اینترنت اشیاء، اشیاء در کنار دستگاه های مرسوم به اینترنت متصل و در تعامل باهم قرار می گیرند. اینترنت اشیاء (IOT) وعده ایجاد جهانی را می دهد که در آن تمام اشیاء اطراف ما به اینترنت متصل شده و با یکدیگر با حداقل دخالت انسان در ارتباط هستند. هدف نهایی، فضای جدید ایجاد «یک دنیای بهتر برای انسان»، با به خدمت گیری اشیاء براساس نیاز و خواست انسان ها است. اشیاء اطراف ما می دانند در چه زمان و مکان و شرایطی ما چه می خواهیم، چه چیزی دوست داریم و به چه چیزی نیاز خواهیم داشت (پرِرا^۲ و همکاران، ۲۰۱۳). عمومی شدن IPV6 و قابلیت افزوده شدن حدود (۲^{۱۲۸})^۳ دستگاه به طور هم زمان هم زمان به شبکه اینترنت در مقابل IPV4 که (۲^{۳۲})^۴، اهداف اینترنت اشیاء برای اتصال همه اشیاء اطراف ما به اینترنت را عملی خواهد کرد. در شکل ۴، پرِرا (۲۰۱۳) سیر تکامل اینترنت تا شکل گیری اینترنت اشیاء را به تصویر کشیده است. اینترنت از ارتباط دو رایانه، تا اتصال میلیون ها رایانه، دستگاه های همراه و اجتماع های انسانی به سمت اتصال اشیاء فیزیکی پیش رفته است.

¹ Transmission Control Protocol (TCP) and the Internet Protocol (IP)

² Perera

³ 340,282,366,920,938,000,000,000,000,000,000,000

⁴ 4.29 billion



شکل ۴. سیر تکامل اینترنت تا شکل گیری اینترنت اشیا (پهرا و همکاران، ۲۰۱۳)

داده‌های عظیم

هم‌پایه رشد اینترنت اشیا، اطلاعات جمع‌آوری شده از اشیاء سایبری شده که با موقعیت‌های جغرافیایی، وضعیت‌های محیطی، انسان و رفتارهای متنوعی که از حالات و زمان‌های مختلف او حکایت دارد^۱، در حال رشد و افزایش است. با تجزیه و تحلیل این داده‌های عظیم^۲، می‌توان «الگوهای پنهان»، «همبستگی‌های ناشناخته» و «مدل‌های رفتاری فرد یا جامعه» را استخراج کرد.

داده‌های عظیم اشاره به داده‌های بزرگ و پیچیده دارد که نیازمند تکنیک‌های جدیدی برای پردازش و کشف الگوهای پنهان داده‌ها دارد. این داده‌ها به قدری بزرگ و حجیم هستند که با ابزارهای مدیریتی و پایگاه‌های داده سنتی و معمولی قابل مدیریت نیستند. اما این تجزیه و تحلیل‌ها موجب تشخیص روند کسب‌وکار، پیشگیری از بیماری، جرم و موارد متنوع دیگر باشد (اکونومیست^۳، ۲۰۱۲). رشد و افزایش داده‌های عظیم به انقلاب داده‌های اجتماعی مرتبط شده است، این دو انگیزه‌ای برای توسعه خدمات در مقیاس وسیع، توسعه زیرساخت‌های جهانی و توسعه ابزار تحلیل با کارایی بالا شده است؛ شبکه‌های اجتماعی به‌طور گسترده‌ای به دسته‌بندی اطلاعات شخصی و رفتاری کاربران پرداخته و ارائه خدمات و تبلیغات بهتر، مفیدتر و دقیق‌تر را ساده کرده

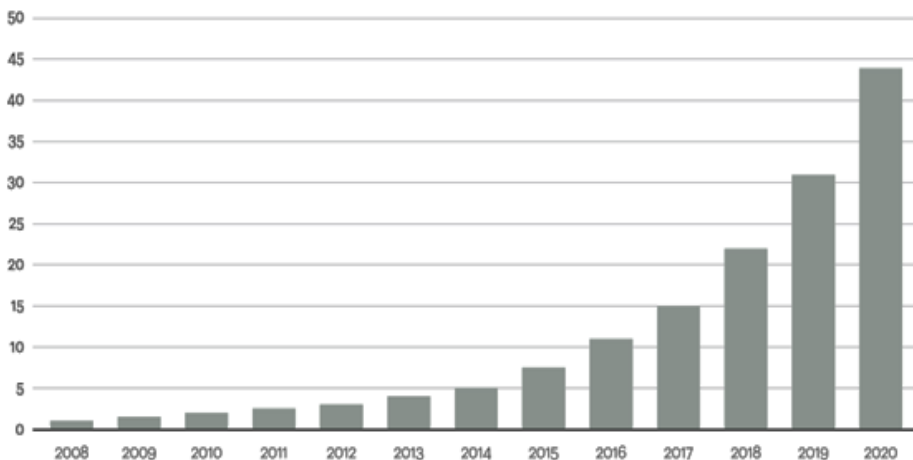
^۱ رفتارهای انسان تابع زمان و موقعیت‌های مختلف است. رفتار در منزل، محل کار، در زمان تفریح و... متفاوت است.

^۲ Big data

^۳ Economist

است (دم چن کو^۱ و همکاران، ۲۰۱۴). شکل ۵، روند ترسیم‌شده‌ی رشد داده‌های دیجیتال را به تصویر کشیده است.

Data in zettabytes (ZB)



Source: Oracle, 2012

شکل ۵، روند رشد داده‌های دیجیتالی تا سال ۲۰۲۰ (اوراکل، ۲۰۱۲). هر زتا بایت یک میلیارد ترا بایت است. شکل ۶، داده‌های عظیم را در پنج ویژگی ۲ حجم، تنوع، سرعت، ارزش و صحت ترسیم کرده است (دم چن کو و همکاران، ۲۰۱۴). (۱) حجم داده زیاد از ویژگی‌های اصلی داده‌های عظیم است. اندازه داده تعیین‌کننده‌ی ارزش و پتانسیل داده‌های برای اطلاق داده بزرگ است. داده‌های تولیدشده توسط ماشین‌آلات، شبکه‌ها و تعاملات انسانی در سامانه‌هایی مانند رسانه‌های اجتماعی، حجم اطلاعات قابل تجزیه و تحلیل گسترده و پرحجمی را تولید کرده است. (۲) تنوع داده، اشاره به انواع داده ساختاریافته و ساختارنیافته از منابع متنوع دارد. داده‌ها از صفحات گسترده و پایگاه‌های داده به تنوع داده‌ای در قالب‌های ایمیل، عکس، فیلم و صوت، سیستم‌های نظارتی، فایل‌های متنی و انواع دیگر است. لازمه تجزیه و تحلیل موردنیاز برای کشف الگوهای پنهان توسط تحلیلگران وجود داده‌های متنوع است. (۳) سرعت، اشاره به رشد روزافزون تولید داده‌ها توسط وسایل متنوع دارد. (۴) ارزش و (۵) صحت، به نتیجه طبقه‌بندی، خوشه‌بندی و پردازش در شکل‌دهی به فرایند یا مدل ویژه‌ی استخراج‌شده، اشاره دارد.

¹ Demchenko

² Volume, Variety, Velocity, Value and Veracity (5Vs)



شکل ۶: پنج ویژگی داده‌های عظیم (دم چن کو و همکاران، ۲۰۱۴)

رایانش ابری

رایانش ابری^۱ از مسائل مرتبط با اینترنت اشیاء است. رایانش ابری مدلی است برای فراهم کردن دسترسی آسان کاربر از طریق شبکه به مجموعه‌ای از منابع رایانشی قابل تغییر و پیکربندی است. رایانش ابری، قدرت نامحدود مجازی را با منابع رایانشی از قبیل زیرساخت، شبکه، سرور با قدرت پردازش و حافظه براساس نیاز و متغیر، فضای ذخیره‌سازی، رایانه‌های شخصی، تجهیزات امنیتی، برنامه‌های کاربردی و سرویس‌ها مهیا می‌سازد (ویکی‌پدیا، ۲۰۱۵).

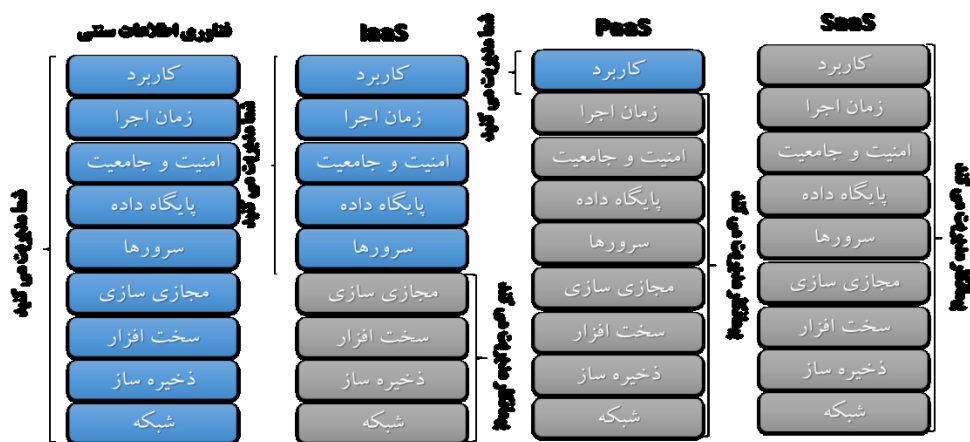
دسته‌بندی سرویس‌ها در فضای ابری به سه گونه کلان است: خدمات زیرساخت (IaaS)^۲: فراهم آوردن امکاناتی شامل توان پردازشی، فضای ذخیره‌سازی، شبکه‌ها و دیگر منابع پایه ای محاسباتی است. به گونه‌ای که مشتری می‌تواند زیرساخت دلخواه خود که می‌تواند شامل سیستم‌های عامل و برنامه کاربردی، شبکه‌های ارتباطی و دستگاه‌های امنیتی است را طراحی و اجرا نماید. خدمات بستراجرای (PaaS)^۳: بسترهای برخطی برای ایجاد، آزمایش و راه‌اندازی برنامه‌های تحت وب فراهم می‌کند که می‌توانند با بهره‌مندی از ابزارهای برنامه‌نویسی و گسترش نرم‌افزار مبتنی بر مرورگر مورد استفاده قرار گیرند. ایجاد یک برنامه با استفاده از این خدمات نسبت به رویکرد سنتی در برنامه‌نویسی و گسترش نرم‌افزار با کار کمتر و در زمان کوتاه‌تری انجام می‌شود و دیگر نیازی به نصب و پیکربندی بسترها و ابزارها و برنامه‌های گسترش نرم‌افزار نیست. خدمات نرم افزاری

¹ Cloud Computing

² Infrastructure-as-a-Service

³ Platform-as-a-Service

(SaaS) ۱: معمول‌ترین نوع خدمات در این دسته، استفاده از برنامه‌ها و نرم افزارهایی است که بر روی فضای ابری قرار دارند. پست الکترونیکی از رایج‌ترین این نوع از خدمات است. شکل ۷، نمایشی از دسته‌بندی سرویس‌ها در رایانش ابری است. این تصویر مقایسه ای از فناوری اطلاعات سنتی و خدمات ابری را به تصویر کشیده است. هرچه از خدمات سنتی فناوری اطلاعات به خدمات نرم افزاری ابری حرکت می‌شود، از مقدار تمرکز بخش‌های فناوری اطلاعات سازمان کاسته شده و به آنچه توسط مراکز داده بزرگ سپرده می‌شود، بیشتر می‌شود.



شکل ۷. سطوح خدمات در فضای ابری و غیر ابری، مقایسه ای از فناوری اطلاعات سنتی تا فناوری اطلاعات ابری کامل

رایانش ابری، موجب انعطاف‌پذیری و توانمندسازی اینترنت اشیا در قدرت، فضای ذخیره‌سازی و شبکه خواهد شد. داده‌های حجیم تولیدشده توسط اشیا متصل به شبکه، قابلیت تحلیل و استخراج رفتارهای انسان‌ها و ماشین‌ها را در فضای ابری به علت وجود منابع رایانشی متنوع و متمرکز خواهد داشت. در حقیقت فضای ابری در حال تمرکز بخشی به داده‌ها و ارائه سرویس‌های موردنیاز کاربران بر اساس شرایط زمانی و مکانی مختلف است. فضای ابری در حال حرکت به سمت هر چیز موردنیاز در هر نقطه مورد درخواست است. تلفیق رایانش ابری و اینترنت اشیا، پارادایم جدیدی را در خلق اینترنت آینده به دنبال خواهد داشت (باتا و همکاران، ۲۰۱۴). این تلفیق و شکل‌گیری پارادایم جدید، موجب شکل‌گیری مفاهیم نوینی شده است. اینترنت اشیا

¹ Software-as-a-Service

ابری، با جمع‌آوری اطلاعات زندگی فردی و اجتماعی در سطح منطقه‌ای، کشوری و جهانی و با تحلیل این اطلاعات و داده‌های عظیم سرویس‌های متنوعی را شکل خواهد داد که زندگی فیزیکی را تماماً در محیط سایر شکل خواهد داد. شهر هوشمند^۱، خانه هوشمند^۲ و اندازه‌گیری هوشمند انرژی مصرفی^۳، نظارت تصویری^۴، خودروهای هوشمند و بدون راننده^۵، شبکه هوشمند انرژی^۶، تدارکات و لجستیک هوشمند^۷، رصد محیطی^۸ و مراقبت از سلامتی^۹ از نتایج این تلفیق است (شکل ۸). این تلفیق و همگرایی اینترنت اشیا، رایانش ابری و داده‌های عظیم، پرچم‌دار تحول آینده جوامع با فضای سایر خواهد بود (بورت^{۱۰} و همکاران، ۲۰۱۴).



شکل ۸. کاربردهای اینترنت اشیا ابری (باتا^{۱۱} و همکاران، ۲۰۱۴)

¹ Smart City

² Smart Home

³ Smart Metering

⁴ Video Surveillance

⁵ Automotive and Smart Mobility

⁶ Smart Energy and Smart Grid

⁷ Smart Logistics

⁸ Environmental monitoring

⁹ Healthcare

¹⁰ Burt

¹¹ Botta

۳- امنیت ملی جمهوری اسلامی ایران

امنیت به مفهوم مصون بودن از تعرض و تهدید است. امنیت به معانی؛ درامان بودن، ایمنی، آرامش و آسودگی آمده است (عمید، ۱۳۶۳، ۲۳۳). به لانی^۱ امنیت را آزادی نسبی از جنگ دانسته و بوزان^۲ امنیت را آزادی از تهدید و توان دولت‌ها و جوامع برای حفظ هویت مستقل خود معرفی کرده است (سیف، ۱۳۸۹، ۸).

امنیت مضاف به ملی، بیانگر عدم وقوع سختی و رخدادی ناراحت‌کننده در سطح ملی در آینده است. در فرهنگ علوم سیاسی در تعریف امنیت ملی چنین آمده است: «امنیت ملی عبارت از احساس آزادی کشور در تعقیب هدف‌های اساسی و فقدان ترس و خطر جدی از خارج نسبت به منافع سیاسی، اساسی و حیاتی کشور است» (بهزادی، ۱۳۵۳، ۱۰۰) در فرهنگ اصطلاحات روابط بین‌الملل این مفهوم بدین صورت تعریف شده است: «حالتی که ملتی فارغ از تهدید از دست دادن تمام یا بخشی از جمعیت، دارایی یا خاک خود به سر می‌برد» (آشوری، ۱۳۶۶، ۲۹). نقیب زاده معتقد است: «امنیت ملی؛ یعنی دستیابی به شرایطی که به یک کشور امکان می‌دهد تا از تهدیدهای بالقوه یا بالفعل خارجی و نفوذ سیاسی و اقتصادی بیگانه در امان باشد و در راه پیشبرد امر توسعه اقتصادی، اجتماعی و انسانی و تأمین وحدت و موجودیت کشور و رفاه عامه فارغ از مداخله بیگانه گام بردارد» (نقیب زاده، ۱۳۷۷، ۹۲). برکوینز و باک می‌گویند: «توانایی یک ملت برای حفاظت از ارزش‌های داخلی در مقابل تهدیدات خارجی یا به عبارت دیگر، امنیت ملی عبارت است از این که کشورها چگونه سیاست‌ها و تصمیمات لازم برای حمایت از ارزش‌های داخلی در مقابل تهدیدات خارجی را اتخاذ می‌کنند» (برکوینز و باک، ۱۳۷۸، ۱۰۳).

امنیت ملی در جمهوری اسلامی ایران مصون بودن منافع ملی جامعه اسلامی ایران از هرگونه تهدید و آسیب‌پذیری است. منافع ملی آن چیزی است که برای بقا کشور و جامعه ارزشمند و حیاتی است. منافع ملی را می‌توان هدف سیاست خارجی هر کشور در رابطه با حفظ سیستم سیاسی، فرهنگی و تمامیت ارضی کشور در مقابل تجاوز سایرین دانست؛ منافع ملی به هدف‌های اولیه و همیشگی مردم یعنی حفظ تمامیت ارضی، حفظ جان مردم و حفظ سیستم‌های اجتماعی و حاکمیت کشور اشاره دارد (بهزادی، ۱۳۶۸، ۸۲). با توجه به مطالب بیان‌شده، به صورت کلی امنیت

¹ Bellany

² Buzan

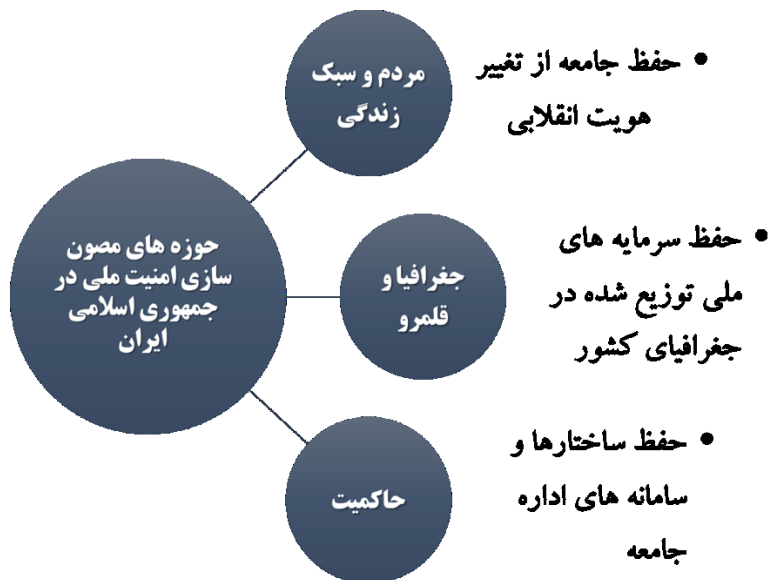
ملی حفظ قلمرو و جغرافیا (تمامیت ارضی)، حاکمیت ملی و مردم به عنوان عناصر تشکیل دهنده کشور است.

براساس این نگاه، امنیت ملی جمهوری اسلامی در سه حوزه بدین شکل تعریف می شود (شکل ۹): (۱) مردم و سبک زندگی، در ایران اسلامی، مردم حافظان اصلی انقلاب هستند. حفاظت از انقلاب به داشتن صرفاً تعداد و نفرات نیست، بلکه کیفیت باید همراه کمیت قرار گیرد. یعنی حافظ انقلاب انسان‌هایی هستند که از لحاظ فکری و عملی اعتقاد قلبی به اسلام و انقلاب داشته باشند. به عبارت دیگر مردم و سبک زندگی^۱ عنصر جمعیت را در امنیت ملی نظام اسلامی تشکیل می دهند. سبک زندگی بیانگر رفتار نشئت گرفته از باورها و انگیزه‌هاست و تغییر سبک زندگی، تغییر همراهی و یا عدم همراهی با انقلاب است. در حکومت اسلامی باید قلب انسان‌ها طاهر و پاک باشد تا جامعه و حکومت اسلامی به سمت تمدن نوین اسلامی و زمینه‌سازی بیداری جهانی و شکل‌گیری دولت کریمه حرکت کند. مسئله اصلی این حوزه مصون‌سازی انسان از غفلت در مقابل مبدأ آفرینش و پایداری قلب و رفتار در حفظ انقلاب اسلامی است.

عنصر دوم جغرافیا یا تمامیت ارضی است. محیط جغرافیا تبلور فیزیکی، عینی، ملموس و مشهود هویت ملی به حساب می آید و برای شکل‌گیری هویت واحد ملی، تعیین محدوده و قلمرو یک سرزمین مشخص، ضرورت تام دارد؛ سرزمین با اقتصاد و سیاست پیوند نزدیک دارد (زارعی و ذکی، ۱۳۹۰). قلمرو باید به عنوان وسیله ای برای رسیدن به هدف مشخصی مانند ادامه بقاء، سلطه سیاسی و بیگانه‌ستیزی شناخته شود (مویر، ۱۳۷۹). جغرافیای کشور در بردارنده سرمایه‌های انسانی، فیزیکی، اقتصادی و سایبری است. این سرمایه‌ها در بستر جغرافیای کشور پراکنده شده و براساس طبقه‌بندی آشکار یا مخفی هستند. حفظ سرمایه‌ها در سطح ملی بر اساس اولویت حیاتی، حساس و یا مهم تعیین می شود. در پدافند غیرعامل سرمایه‌های قابل حفاظت به ۴ گروه سرمایه انسانی، سرمایه فیزیکی، سرمایه سایبری و سرمایه‌های معنوی و ملی دسته‌بندی شده است (جلالی، ۱۳۹۱). قلمرو جغرافیای کشور در بردارنده سرمایه‌های انسانی، فیزیکی و سایبری است که در گستره‌ی جغرافیای کشور پراکنده شده است. مراکز نظامی، مراکز تجمع سرمایه‌های انسانی مختلف، محل قرارگیری زیرساخت‌های فنی و سایبری از جمله‌ی این سرمایه‌ها در بستر جغرافیا است.

^۱افزوده شدن سبک زندگی به مردم برگرفته از فرمایشات سرلشکر بسیجی دکتر فیروزآبادی در سال ۱۳۹۳ در دانشگاه عالی دفاع ملی است.

عنصر سوم حاکمیت ملی است. حاکمیت به معنای قدرت برتر و عالی صلاحیت برای اتخاذ تصمیم نهایی تلقی شده که در رأس همه قدرت‌ها قرار دارد (عالم، ۱۳۷۳، ۲۵). حاکمیت حق انحصاری حکومت و دولت برای نظارت بر یک قلمروی ارضی معین است (گیدنز، ۱۳۸۴، ۸۱۱). به راین اساس حاکمیت مجموعه‌ی ساختار و تدابیری است که اداره‌کننده کشور برای رسیدن به اهداف است. این تدابیر دربردارنده ساختارهای اقتصادی، سیاسی، فرهنگی و نظامی است.



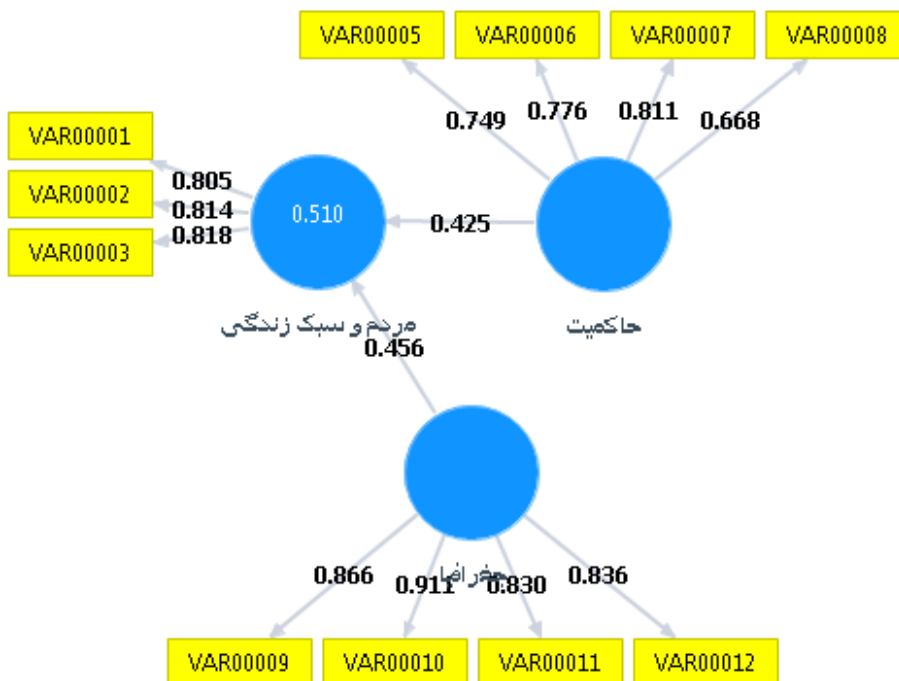
شکل ۹. حوزه‌های مصون‌سازی امنیت ملی و حفاظت از منافع ملی کشور

تجزیه و تحلیل داده‌ها

داده‌های حاصل از اخذ پرسشنامه از ۴۰ نفر از متخصصین امنیت ملی و فضای سایبر جمع‌آوری شده و در نرم‌افزار SmartPLS، مدل تحلیل اولیه برای محاسبه بارهای عاملی با ۵۰۰ نمونه اجرا شده است. بارهای عاملی شاخص‌های بیش از ۰.۴ است و در نتیجه شاخص‌های مورد تأیید است (شکل ۱۱ و جدول ۱).

کد	مؤلفه ها	ابعاد
Var00001	ماشینی شدن زندگی انسان	مردم و سبک زندگی
Var00002	غفلت انسان از مسئولیت دنیوی و اخروی	
Var00003	تغییر سبک زندگی جامعه به سبک زندگی غربی	
Var00005	اشراف صاحبان تکنولوژی بر روابط و تعاملات اقتصادی	حاکمیت
Var00006	اشراف صاحبان تکنولوژی بر روابط و تعاملات فرهنگی	
Var00007	اشراف صاحبان تکنولوژی بر روابط و تعاملات سیاسی	
Var00008	اشراف اطلاعاتی صاحبان تکنولوژی بر اطلاعات و دانش راهبردی	
Var00009	کاهش حفاظت از سرمایه های فیزیکی حیاتی، حساس و مهم	جغرافیا
Var00010	کاهش حفاظت از سرمایه های اقتصادی حیاتی، حساس و مهم	
Var00011	کاهش حفاظت از سرمایه های انسانی حیاتی، حساس و مهم	
Var00012	کاهش حفاظت از سرمایه های سایبری حیاتی، حساس و مهم	

جدول ۱. ابعاد و مؤلفه های چالش آفرینی اینترنت اشیا و کد هر کدام



شکل ۱۰. مدل تحقیق

در جدول زیر گزارش روایی و پایایی مدل قرار گرفته است.

آلفای کرونباخ	معیار پایایی ترکیبی	AVE	
۰.۷۴۴	۰.۸۵۳	۰.۶۶۰	مردم و سبک زندگی
۰.۷۴۳	۰.۸۳۹	۰.۵۶۷	حاکمیت
۰.۸۸۴	۰.۹۲۰	۰.۷۴۲	جغرافیا

جدول ۱. گزارش روایی و پایایی

همانگونه که در جدول ۱ مشاهده می‌شود، ضریب آلفای کرونباخ همه ابعاد بالاتر از ۰/۷ و قابل قبول است و معیار پایایی ترکیبی^۱ بالای ۰/۷ که از پایایی مدل روایت می‌کند. برای روایی مدل فورنل و لدرکر (۱۹۸۱) مقدار مناسب برای AVE^۲ را ۰/۵ به بالا معرفی کرده‌اند که بر اساس نتایج تمامی مقادیر عددی بالاتر از ۰/۵ است که روایی همگرایی مناسب مدل را نشان می‌دهد. با توجه به نتایج (شکل ۱۲) مدل نهایی و مورد تأیید قرار گرفته است.

یافته‌های پژوهش

چالش‌های امنیت ملی با گسترش اینترنت اشیاء

با گسترش اینترنت اشیاء در کشور و اتصال اشیاء اطراف ما و تجاری‌سازی اشیاء پوشیدنی هوشمند همانند عینک، گوشی‌های هوشمند، تلویزیون، یخچال، خودرو، تجهیزات اداری سیلی از اطلاعات به سمت سرورهای صاحبان تکنولوژی به حرکت درمی‌آید. ارتباط و همگرایی اطلاعات با اشیاء، مکان‌های جغرافیایی و انسان‌ها موجب کشف الگوهای پنهان موجود در این اطلاعات شده و چالش‌هایی را متوجه امنیت ملی کشور می‌کند.

- **مردم و سبک زندگی:** اصلی‌ترین سرمایه انقلاب اسلامی مردم ایران هستند. اگر مردم درصحنه باشند انقلاب از آفت‌های درونی و برونی حفظ خواهد شد. مقام معظم رهبری حضرت امام خامنه‌ای (مدظله‌العالی) می‌فرمایند: «هیچ حادثه‌ای در تاریخ ایران همانند انقلاب اسلامی وجود ندارد که مردم در پیروزی و ادامه آن نقش مستقیم و اساسی داشته باشند» (امام خامنه‌ای،

¹ Composite Reliability

² Average variance extracted (AVE)

۱۳۹۰/۷/۲۰). دور شدن مردم از اسلام حقیقی و گرایش عملی یا فکری به مظاهر تمدن غرب چالش اصلی امنیت ملی است. مقام معظم رهبری حضرت امام خامنه‌ای (مدظله‌العالی) در جمع اعضای مجلس خبرگان رهبری فرموده‌اند: «شما ببینید امروز وسائلی که برای اغوای دل جوان‌ها هست، چقدر است؛ قابل مقایسه‌ی با گذشته نیست. این ماهواره‌ها، این اینترنت‌ها، این انواع و اقسام وسایل ارتباطات، این‌ها دل‌ها را اغوا می‌کند، جذب می‌کند، از راه به در می‌برد، انگیزه‌های معنوی را در انسان سست می‌کند، شهوات را در انسان بیدار می‌کند» (امام خامنه‌ای، ۱۳۹۰/۶/۱۷). با تسلط اینترنت و اتصال گسترده اشیای اطراف ما به آن، چگالی حضور تکنولوژی در زندگی آدمی بشدت بالا خواهد رفت. به‌گونه‌ای که دیگر انسان توانایی فرار از رصد و پایش شدن تکنولوژی‌های متنوع را نخواهد داشت و این تکنولوژی است که انسان را مدیریت می‌کند.

در جامعه پیش از مدرن، بنیان شخصیت آدمی بر دو ساحت تن و جان استوار بود، روح تفکر بر اعتبار شخصیت انسان می‌افزود، اینک روزگاری فرارسیده که واقعیت ذاتی و ماهوی انسان در قبال شیئیت و سودمندی اقتصادی او از یادرفته و تکنولوژی انسان را به بردگی سوق داده است (لاکوست، ۱۳۷۵، ۸۳). این عقلانیت‌بیزاری که تجسم عینی آن تکنولوژی است، در برهه‌ای از زمان به آزادی انسان از سیطره کار سخت و طاقت‌فرسا و چیرگی بر طبیعت انجامید ولی امروزه باعث گونگی انسان شده و به ناظری بر عملکرد آدمی بدل گشته است و آفریده در مقابل آفریننده قدعلم کرده است (رحیم‌پور، ۱۳۸۳، ۶۳). ایجاد انگیزه‌ی کاذب برای ادامه زندگی و بی‌هدفی که ثمره دوری از خدا که هدف اصلی خلقت انسان است^۱ و خالی نمودن زندگی از مخلوق بودن چه به‌صورت نمایان و یا چه به‌صورت پنهان‌شده در توهمات و خیالات باطلی که ظاهری قدسی دارد و از حقیقت به دور است، موجب سوق دادن انسان به نهیلیسم و پوچ‌گرایی شده است. این انسان مدرن هویتش را از تمایلات غریزی و لذت‌جویانه که غیرقابل مقاومت و اجتناب‌ناپذیر است اخذ نموده و از هویت آخرت‌گرای خود غافل شده است. انسان دیگر به خالق و مسئولیت خود در مقابل او توجه ندارد و به بی‌هویتی و فراموشی خود دچار می‌شود، «وَأَلَّا تَكُونُوا كَالَّذِينَ نَسُوا اللَّهَ فَأَنْسَاهُمْ أَنْفُسَهُمْ أُولَئِكَ هُمُ الْفَاسِقُونَ، و همچون کسانی نباشید که خدا را فراموش کردند و خدا نیز آن‌ها را به خود فراموشی گرفتار کرد، آن‌ها فاسقان‌اند (حشر/ ۱۹)».

ماشینی شدن زندگی انسان، غفلت انسان از مسئولیت دنیوی و اخروی و تغییر سبک زندگی جامعه

^۱ وَمَا خَلَقْتُ الْجِنَّ وَالْإِنْسَ إِلَّا لِيَعْبُدُونِ (ذاریات/ ۵۶)

به سبک زندگی غربی ثمره حضور گسترده و بدون برنامه اینترنت اشیاء در زندگی خواهد بود و انسان انقلابی را تحت برنامه خود به سمت سبک زندگی غربی سوق خواهد داد.

• **حاکمیت:** حاکمیت در واقع، قدرت برتری است که در حیطه‌ی دولت کشور، اراده ای فراتر از آن وجود ندارد، به گونه‌ای که در مقابل اعمال اراده و اجرای اقتدارش مانعی نمی‌پذیرد و از هیچ قدرت دیگری تبعیت نمی‌کند. حاکمیت با ساختارهای اقتصادی، فرهنگی و سیاسی اعمال قدرت پیدا می‌کند. درون‌داد و برونداد ساختارهای اداره کشور، جریان اطلاعات و دانش راهبردی است. با گسترش بسترهای سخت و نرم اینترنت اشیاء صاحبان تکنولوژی حاکمان بلامنازع این فضا خواهند شد. این اشراف تکنولوژیکی فراتر از مرزهای جغرافیایی و حاکمیت دولت‌ها است. صاحبان تکنولوژی از دارندگان تکنولوژی‌های خرد همانند تولیدکنندگان برنامه‌های کاربردی (Apps) تا تولیدکنندگان دستگاه‌های ارتباطی، دستگاه‌های توکار، سیستم عامل‌ها، مسیریاها، مراکز انتقال و... براساس سطح و گستردگی نفوذ خود به بهره‌کشی و برده‌داری مدرن با مدیریت افکار می‌پردازد.

سامسونگ یکی از بزرگ‌ترین شرکت‌های تولید لوازم‌خانگی از کاربران و مصرف‌کنندگان خودخواسته تا در برابر تلویزیون‌های هوشمندی که از قابلیت اتصال به اینترنت برخوردارند در رابطه با مسائل خصوصی زندگی‌شان صحبت نکنند زیرا امکان انتقال و شنود آنها وجود دارد (خبرگزاری مهر، ۱۳۹۳). در آمریکا در مورد عینک گوگل گفته می‌شود: «این عینک ابزار جاسوسی است. زمانی که شما به من نگاه می‌کنید، من نیز به شما نگاه می‌کنم و هر جا که شما با این عینک بروید، شمار بسیار اندکی از آمریکایی‌ها که با شما روبه‌رو می‌شوند خواهند دانست که شما از آنها فیلم‌برداری می‌کنید» (خبرگزاری آریا، ۱۳۹۳). اشراف صاحبان تکنولوژی بر رفتار و تعاملات اقتصادی، فرهنگی، سیاسی و اطلاعات و دانش راهبردی اداره و مدیریت کشور، عملاً کشورهای متخاصم را بر برنامه‌ریزی و تعاملات کشور مسلط خواهد کرد و امکان جهت‌دهی به رفتارها را با توجه به قدرت نرمی که برای خود ایجاد کرده‌اند، ممکن خواهد ساخت.

• **قلمرو و جغرافیا:** قلمرو هر کشور دربردارنده سرمایه‌های متنوع و توانمندساز است هر کشور برای حفظ امنیت ملی و سرزمینی خود به حفاظت از منابع حیاتی و حساس خود در قلمرو جغرافیایی می‌پردازد. سرمایه‌ها براساس طبقه‌بندی و حساسیت خود در تداوم حیات کشور به انواع گوناگونی حفاظت می‌شود. سرمایه‌ها ممکن است در مکان‌های جغرافیایی ناشناخته در دل

جنگل‌ها، کوه‌ها و یا دشت‌ها قرار گرفته باشد. سرمایه‌های انسانی، فیزیکی و اقتصادی و سایبری حیاتی، حساس و مهم، حفاظت برنامه‌ریزی شده‌ای را می‌طلبد.

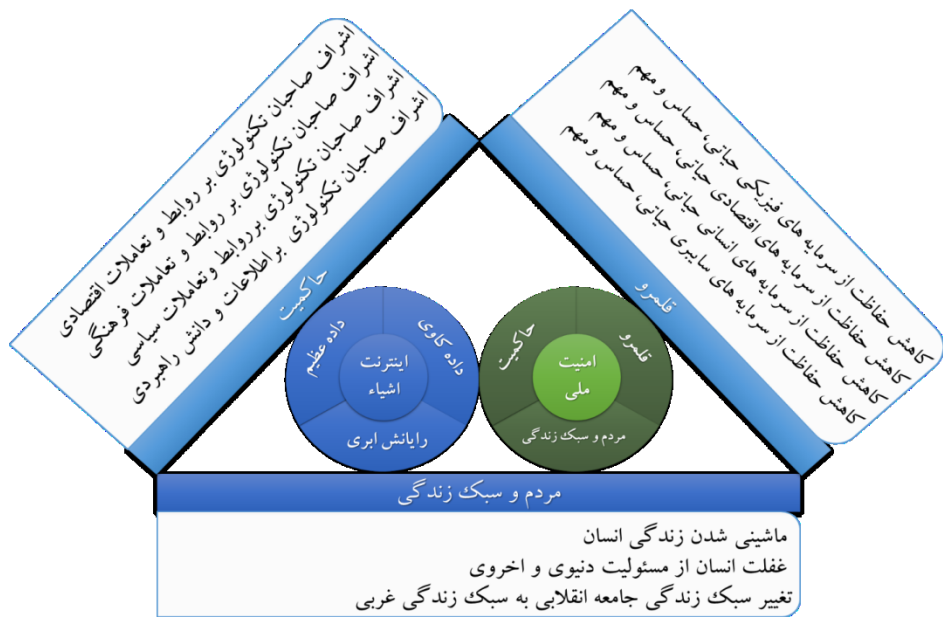
با گسترش اینترنت اشیاء، حفاظت از سرمایه‌های ملی برای دولت‌های در معرض تهدید پیچیده‌تر خواهد شد. سرمایه‌های ملی که به صورت پنهان و نیمه پنهان موردحفاظت قرار می‌گیرند، در معرض تهدید مضاعفی قرار خواهند گرفت. شناسایی، ره‌گیری و انهدام سرمایه‌های ملی در این عصر برای کشورهای مسلط بر فضای تکنولوژیکی ساده تر خواهد شد. گسترش اینترنت اشیاء موجب کاهش حفاظت از سرمایه‌های ملی خواهد شد، این کاهش در چند جنبه مختلف خواهد بود، (۱) شناسایی نقاط حیاتی و حساس کشور با رصد و پایش سرمایه‌های انسانی، سرمایه‌های فیزیکی سایبری شده؛ (۲) شناسایی سرمایه‌های انسانی حیاتی و حساس بر اساس میزان مراجعه به نقاط حیاتی و حساس؛ (۳) شناسایی زیرساخت‌های حیاتی و حساس سایبری و غیر سایبری؛ (۴) در معرض تهدید قرار گرفتن سرمایه‌های ملی با دست‌کاری اشیاء سایبری برای آسیب رساندن و انفجار. گسترش موجب کاهش حفاظت از سرمایه‌های انسانی، کاهش حفاظت از سرمایه‌های فیزیکی و اقتصادی و کاهش حفاظت از سرمایه‌های سایبری خواهد شد. دیگر نیازی به به‌کارگیری تیم‌های ویژه‌ای برای عملیات تروریستی نیست، بلکه تکنولوژی هم قابلیت رصد و نظارت را پدید می‌آورد و هم قابلیت تخریب و انفجار را به‌صورت بالقوه خواهند داشت.



شکل ۱۱. گسترش اینترنت اشیاء و چالش‌های پیش روی امنیت ملی (محقق ساخته)

نتیجه‌گیری و پیشنهاد

اینترنت اشیاء به سرعت در حال گسترش است. اشیاء متنوعی از پوشیدنی، ثابت و متحرک با قابلیت عمل فیزیکی با فرمان سایبری در حال گسترش است. اینترنت آینده با نفوذ در همه شئون زندگی انسان از حالات شخصی و فردی تا تعاملات جمعی اجتماعی، اقتصادی، سیاسی و فرهنگی در حال خلق دنیایی جدید برای انسان است. اینترنت اشیاء، داده‌های عظیم، رایانش ابری و داده‌کاوی در کنار مزایای زیادی که دارد، از آن‌جهت که طراحان و تولیدکنندگان آن متعلق به کشورهای دارای فرهنگ و ایدئولوژی متفاوت با فرهنگ انقلاب اسلامی است، چالش‌های جدیدی را متوجه امنیت ملی جمهوری اسلامی ایران خواهد کرد. این چالش‌ها در ابعاد مردم و سبک زندگی، حاکمیت و قلمرو جغرافیایی از تغییر نگرش به زندگی و تحول سبک زندگی دینی به سمت سبک زندگی غربی تا اشراف کشورهای متخاصم بر رفتار و تعاملات فردی و کاهش حفاظت از سرمایه‌های ملی خواهد بود. لزوم آمادگی در مقابل تهدیدهای نوپدید لازم و ضروری است. پیشنهاد می‌شود محققین حوزه‌های راهبردی و امنیت ملی به تأمل در فرصت‌ها و تهدیدهای فضای سایبر آینده پردازند و راهبردهای مناسبی را برای برون‌رفت از این چالش‌ها طراحی نمایند. این راهبردها باید به منجر به اقتدار درون‌زای کشور در فضای سایبر شود. این اقتدار باید متکی کردن بر عناصر قدرت آفرین به توانمندی‌های کشور با برون‌نگری و حضور فعالانه در عرصه‌های جهانی است. برای شکل‌دهی به قدرت درون‌زای سایبری باید حصار بندگی علمی و برده‌داری مدرن دنیای پیشرفته را کنار زد و به حیات دنیوی و اخروی، گسترش منافع علم برای آحاد بشریت، توجه به تعالی انسان و جامعه و شناخت رفتار دشمن توجه نمود. باید توانست تکنولوژی مدرن را با حذف آسیب‌های آن که انسان را مصرف‌زده کرده و برده‌داری مدرن را شکل داده است، در اختیار گرفت و به فراتر از آن را با راه‌های جدید و میانبر دست‌یافت.



شکل ۱۲. اینترنت اشیاء و چالش‌های پیش روی امنیت ملی (مدل نهایی تحقیق)

منابع

- قرآن کریم، ترجمه آیت الله مکارم شیرازی.
- بیانات مقام معظم رهبری حضرت امام خامنه‌ای (مدظله‌العالی). قابل دسترس در: Khamenei.ir
- قانون اساسی جمهوری اسلامی ایران.
- آشوری، داریوش (۱۳۶۶). دانشنامه سیاسی، تهران: انتشارات سهروردی و مروارید، چاپ اول.
- الجرجانی، السید الشریف علی بن محمد (۱۳۶۸). کتاب التعریفات، جمالیه مصر، المطبعه الخیریه، الطبعه الاولى. افست تهران: انتشارات ناصر خسرو.
- برکوویتز، مورتون و باک، پی. سی. (۱۳۷۸). مقاله امنیت ملی. انتشارات پژوهشکده مطالعات راهبردی، چاپ دوم.
- بندر ریگی، محمد (۱۳۶۱). فرهنگ عربی به فارسی: ترجمه منجد الطلاب (چاپ سوم). تهران: انتشارات اسلامی.
- بهزادی، حمید (۱۳۵۲). اصول روابط بین الملل و سیاست خارجی، تهران انتشارات کتابفروشی دهخدا.
- خبرگزاری مهر (۱۳۹۳). جاسوسی سامسونگ با تلویزیون‌های هوشمند
- <http://www.mehrnews.com/print/2492007>-جاسوسی-سامسونگ-با-تلویزیون-های-هوشمند
- جلالی، غلامرضا (۱۳۹۱). دسته‌بندی سرمایه‌ها. خبرگزاری فارس ارائه شده در تاریخ ۱۳۹۱/۰۸/۰۱
- <http://www.farsnews.com/newstext.php?nn=13910801000771>
- خبرگزاری آریا (۱۳۹۳). عینک گوگل ابزار جاسوسی یا نشانه پیشرفت.
- <http://aryanews.com/News.aspx?code=20140417105245706&svc=63>
- سیف، الله مراد (۱۳۸۹). مفهوم شناسی امنیت اقتصادی. آفاق امنیت، سال سوم، زمستان ۱۳۸۹، ص ۳۵-۷.
- داوری، علی، رضازاده، آرش، (۱۳۹۲)، مدل‌سازی معادلات ساختاری با نرم‌افزار PLS، انتشارات جهاد دانشگاهی، تهران
- عمید، حسن (۱۳۶۳). فرهنگ عمید. تهران: انتشارات امیرکبیر.

- قدسی، امیر (۱۳۹۲). تأثیر فضای مجازی بر امنیت ملی ج. ا. ایران و ارائه راهبرد (با تأکید بر ایفای نقش سرمایه اجتماعی). مجله راهبرد دفاعی، زمستان ۱۳۹۲، دوره ۱۱، شماره ۴۴.
- گیدنز (۱۳۸۴). جامعه‌شناسی، ترجمه: منوچهر صبوری. نشر نی.
- لاکوست، ژان (۱۳۷۵)، فلسفه در قرن بیستم، ترجمه رضا داوری اردکانی، تهران: انتشارات سمت. دیده‌شده در کتاب «نقدی بر مبانی معرفت‌شناسی اومانیستی» نوشته مریم صانع پور (۱۳۸۸)، تهران: انتشارات کانون اندیشه جوان.
- نقیب زاده، احمد (۱۳۷۷). نظریه‌های کلان و روابط بین‌الملل. تهران: نشر قومس.
- Ashton, K. (2009). "Internet of Things", RFID Journal.
- Botta, Alessio and de Donato, Walter and Persico, Valerio and Pescape, Antonio (2014). On the Integration of Cloud Computing and Internet of Things. Proceedings of the 2nd International Conference on Future Internet of Things and Cloud (FiCloud-2014).P27—29.
- Buckley J. Ed. (2006). The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems. Auerbach Publications, New York, 2006.
- Burt, David and Kleiner, Aaron and Nicholas, J. Paul and Sullivan, Kevin (2014). CyberSpace 2025, today's Decisions,
- Tomorrow's Terrain Navigating the Future of Cybersecurity Policy. Microsoft.
- Demchenko, Yuri and de Laat, Cees and Membrey, Peter (2014). Defining Architecture Components of the Big Data Ecosystem. Collaboration Technologies and Systems (CTS), 2014 International Conference on.p104-112.
- Economist (2012). "Data, data everywhere". The Economist. 25 February 2010. Retrieved 9 December 2012.
- Evans Dave (2011). The Internet of Things: How the Next Evolution of the Internet Is Changing Everything Cisco, April 2011,
- http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
- Fornell, C. and Larcker, D. (1981); "Evaluating Structural Equation Modeling with Unobserved Variables and Measurement Error"; Journal of Marketing Research, Vol.18, No.1, pp.39-50.
- Gubbi, Jayavardhana and Buyya, Rajkumar and Marusic, Slaven and Palaniswami, Marimuthu (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Elsevier. Future Generation Computer Systems, volume 29, number 7. P1645-1660.
- Kellmerein, Daniel and Obodovski, Daniel (2013). The Silent Intelligence: The Internet of Things. DND Ventures LLC; 1 edition (September 20, 2013).
- Kumar, J. Sathish and Patel, Dhiren R. (2014). A Survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications (0975 – 8887) Volume 90 – No 11, March 2014
- Oracle (2012). <http://www.oracle.com/>. Visited in "https://www.atkearney.com/strategic-it/ideas-insights/article/-

/asset_publisher/LCcgOeS4t85g/content/big-data-and-the-creative-destruction-of-today-s-business-models/10192”.

- Perera, Charith and Zaslavsky, Arkady and Christen, Peter and Georgakopoulos, Dimitrios (2013). Context aware computing for the internet of things: A survey. Communications Surveys \& Tutorials, IEEE volume 16, number 1, P414-454.
- McEwen, Adrian and Cassimally, Hakim (2013). Designing the internet of things. P11. John Wiley & Sons.
- Voorsluys, William and Broberg, James and Buyya, Rajkumar (2011). Introduction to cloud computing. Cloud computing: Principles and paradigms journal 3-37. John Wiley \& Sons Inc.
- Wikipedia (2015). Cloud computing. https://en.wikipedia.org/wiki/Cloud_computing. Visited on 2 August 2015.