بررسی تأثیر سیاست BYOD در سازمان ها بر امنیت ملی

پرویز حسینی [۱]
حقی مهدیار [۲]

تاریخ دریافت: ۱۳۹۶/۰۵/۰۹ تاریخ پذیرش: ۱۳۹۶/۰۷/۲۷

چکیده

با افزایش استفاده از دستگاه‌های همراه در زندگی روزمره، میل افراد به استفاده از این ابزارها در هنگام یا به منظور انجام کارهای روزانه نیز افزایش می یابد. BYOD [۳] سیاستی است که به کارکنان اجازه می‌دهد از دستگاه‌های شخصی مانند گوشی هوشمند، تبلت و لپتاپ برای وظایف سازمانی استفاده کنند. با توجه به آن که تهدید سایبری به عنوان مولفه ای جدید در ابعاد تهدید امنیت ملی محسوب می شود و اقدامات پدافند غیرعامل به دنبال پیشگیری از وقوع این گونه اتفاقات است، مقاله پیش رو در پی پاسخ به این پرسش است که آیا پذیرش BYOD در سازمان ها منجربه یک تهدید امنیت ملی است یا خیر؟ پس از انجام مطالعات کتابخانه ای و اخذ نظر خبرگان حوزه امنیت فاوا با روش تحلیل سلسله مراتبی نسبت به اولویت‌بندی مولفه های مستخرج از مفاهیم به دست آمده اقدام و با استفاده از روش داده بنیاد با ارائه یک مدل ارتباط بین مولفه های تأثیرگذار بر پذیرش این سیاست بر امنیت سایبری و به تبع آن امنیت ملی تبیین گردید.

کلیدواژه : *BYOD، امنیت ملی، تهدید سایبری، داده بنیاد، تحلیل سلسله مراتبی، پدافندغیرعامل*

۱دکتری امنیت ملی دانشگاه عالی دفاع ملی(par.hos@iran.ir)

۲دانشجوی کارشناسی ارشد پدافندغیرعامل گرایش امنیت ملی دانشگاه علوم و فنون فارابی(dore۱۲farab@chmail.ir)

۳ Bring Your Own Device

مقدمه

افزایش دستگاه‌ها و فناوری‌های رایانه‌ای در دهه‌های هشتاد و نود میلادی، سازمان‌ها را بر آن داشت که به سرعت برای انطباق با روند استفادهٔ کارکنان از دستگاه‌های شخصی در محل کار، تلاش کنند با این‌که در آن زمان، بسیاری از سازمان‌ها از فواید فناوری‌هایی چون رایانه‌های قابل حمل به دلیل مسائل کنترل و امنیت داده‌ها آگاهی داشتند، از این فناوری‌ها استقبال زیادی نکردند (سنتوش ردی،۲۰۱۲،ص ۷) همزمان با رشد روزافزون فناوری اطلاعات در سده بیست ویکم، سازمان ها به دنبال کم هزینه ترین راه افزایش دسترسی و مبادله داده ها برای کارکنان هستند. (آستانی، ردی و تسما،۲۰۱۳،ص ۱۵)

یکی از سیاست‌هایی که سازمان‌ها برای این هدف به کار می‌برند BYOD نامیده می‌شود. بر این اساس BYOD یا "دستگاه خودت را بیاور"، سیاستی است که کارکنان از دستگاه‌های شخصی مانند گوشی‌های هوشمند، تبلت و لپتاپ برای کارها و مسئولیت های اداری خود استفاده می کنند(هنسما،۲۰۱۳،ص۲۱) در واقعBYOD به معنای استفاده از دستگاه‌های شخصی برای انجام کارهای رسمی سازمان است (ویگنش و آشا،۲۰۱۵، ۳۶) مزیت‌ها و چالش‌های بهره‌مندی از BYOD در سطح بخشی را می‌توان در سه جایگاه مصرف کننده، سازمان و واحد فناوری اطلاعات سازمان، بررسی کرد. در نگاه بخشی و در مورد یک سازمان خاص، استفاده از دستگاه برای کار و زندگی شخصی سبب افزایش رضایت شغلی، کاهش پیچیدگی در استفاده از دستگاه و بهبود تجربه‌ی کاری می‌شود و سازمان نیزبه سودهایی دست می‌یابد. با به کاربردن سیاست BYOD کارکنان زمان بیشتری را برای کارها به ویژه در تعطیلات اختصاص می‌دهند. در کنار فرصت‌های یادشده، سازمان با چالش‌هایی مانند نیاز به پشتیبانی از دستگاه‌های گوناگون، ایمنی در دسترسی به شبکه‌ی سازمان (برادلی، لوکاس، مکوآلی، مدکالف و بوکالیو، ۲۰۱۲ ،صص ۶۵-۶۱) به روزرسانی پیوندهای نو برای دستگاه‌های جدید، تدوین و اجرای سیاست‌های استفاده ازدستگاه‌ها برای اتصال به شبکهٔ سازمان، حفاظت از داده‌ها و پیشگیری از نشر آن‌ها و لغو دسترسی به شبکه (آندرسن،۲۰۱۲، ص۵۶) نیز روبه رو می‌شود. به عنوان مثال ۸۵٪ از مالزیایی‌ها از BYOD استفاده می‌کنند که تنها ۲۶٪ از آن ها از حمایت امنیتی کافی برخوردارند(طایی زاده و دیگران،۱۳۹۵،ص ۲)

بیان مساله:

امروزه با رشد روز افزون فضای کسب و کار، تنوع در فرایند های تجاری، استفاده از تکنولوژی های فناوری اطلاعات و ارتباطات در سازمان ها و شرکت ها به امری مهم تبدیل شده است که در بستر این موضوع، مفهوم جدیدی به نام BYOD (دستگاه شخصی خودت را بیاور پدید آمده است) .درواقع این ابتکار جدید به این معنی است که کارمندان از دستگاه شخصی خود (مانند گوشی هوشمند، تبلت ،لپ تاپ) در محیط کسب و کار و برای دسترسی به منابع کاری استفاده می‌کنند .بر طبق نتایج ارائه شده توسطeMarketer در حال حاضربیش از ۲ میلیارد از مردم در سراسر جهان از گوشی های هوشمند استفاده می‌کنند، که انتظار می‌رود تا پایان سال ۲۰۱۸ میزان نفوذ آن در جمعیت جهان از۶۱ به ۷۱ درصد افزایش یابد. از آنجایی که قدرت پردازش، ذخیره سازی و اتصال به اینترنت روز به روز در حال افزایش است، انتظار می‌رود که در بیشتر کسب و کارها و جوامع حرفه ای، کارکنان از دستگاه شخصی خود برای برای مدیریت فعالیت‌های شرکتی استفاده کنند. طبق نظرسنجی ارائه شده توسط Cisco، از بین ۶۰۰ کارفرما، نزدیک به ۹۵ درصد از آنها به کارمندان خود اجازه داده‌اند که برای انجام فعالیت‌های کاری، وسیله‌ی شخصی خود را به محل کار بیاورند .با توجه به روند رو به رشد این مسئله، مهمترین موضوعی که سازمان‌ها و شرکت‌ها را در استفاده ازBYOD نگران کرده است، امنیت و حفظ حریم خصوصی منابع ذخیره شده‌ی شرکت، بر روی دستگاه مدیریت نشده ی کارمندان است. با توجه به حقایق پیش رو پژوهشگر بر آن شد تا ضمن بررسی نقاط قوت و ضعف این پدیده در تمامی ابعاد، به ارائه مدلی همه جانبه نگر در تبیین مخاطرات متناظر این پدیده با تهدیدات سایبری و به تبع آن تهدید احتمالی این پدیده علیه امنیت ملی به عنوان عنصری تأثیرگذار در موضوع پدافند غیرعامل بپردازد.

اهمیت پژوهش

یک کارمند برای هدف کاری اش بشدت وابسته به استفاده از هر یک از دستگاه‌های قابل حمل مثل لپ تاپ، تلفن هوشمندو نوت بوک است، چرا که آن‌ها ابزارها و دستگاه‌های خود را بسیار سهل‌تر از ابزارهایی می‌یابند که در اتاق یا میز کارشان در سازمان فراهم است. لذا متوجه می‌شویم که بمنظور رقابتی شدن در بازار، سازمان‌ها به تسهیل هر چه بیشتر هر نوع پیشرفت

فناوری در سمت کاربر نهایی که کارمندانشان هستند نیاز دارند، اما نه با به خطر انداختن امنیت اطلاعات شرکت و حریم خصوصی کاربر نهایی (Johnson et al, ۲۰۱۲،۷۵) بنابر این پیشبرد اهداف سازمان ها و به تناسب تسهیل در دسترسی کارکنان می بایست همراه با سیاست های امنیتی متناسب باشد تا با شناخت دقیق پدیده، تهدیدات و مواهب آن در کنار یکدیگر دیده شود. با توجه به نوظهور بودن این سیاست، بررسی دقیق نقش و تأثیر آن بر امنیت سایبری نیز از اهمیت بسزایی برخوردار است. از آن جایی که در ادبیات جدید امنیت ملی مولفه ی امنیت سایبری نیز بعنوان یک مولفه تأثیرگذار پذیرفته شده است بنابر این ترسیم یک الگوی شناختی در موضوع مورد اشاره می‌تواند به تبیین دقیق ملاحظات پدافند غیر عامل در ابعاد امنیت ملی کمک شایانی نماید. همچنین تشریح وتبیین ابعاد مختلف این پدیده می‌تواند ابزاری مناسب جهت تصمیم‌گیری مدیریت کلان کشور به منظور پیش بینی ملاحظات لازم دربکارگیری این پدیده باشد.

ضرورت پژوهش.

برای کارکنان BYOD فی نفسه ضرری ندارد .استفاده از دستگاه‌های شخصی برای کارهای روزمره، برای مثال تعادل زندگی وکار را تهدید می‌کند و کارکنان را در معرض مسئولیت تخریب شبکه شرکت با بدافزارها قرار می‌دهد (Niehavesetal,۲۰۱۲،۴۴) این مورد آخر نتایجی را می‌تواند به بار آورد که نه برای سازمان و نه برای فرد مطلوب نیستند. با توجه به تجربیات کشور در مواجهه با پدیده‌های نوظهور بخصوص در عرصه فناوری اطلاعات و ارتباطات، عدم شناسایی تمامی ابعاد این پدیده‌ها و آسیب‌ها و تهدیدات احتمالی آن می‌تواند تبعات گسترده فرهنگی، اجتماعی، اقتصادی و امنیتی به دنبال داشته باشد. عدم شناسایی پدیده‌های نوین در حوزه سایبری و تبیین روابط این پدیده‌ها با ابعاد مختلف تهدیدات سایبری، سیاست‌گذاران و تصمیم‌گیران این حوزه را در انجام وظایف و اقدامات بایسته دچار مشکلات فراوان خواهد نمود. به ویژه آن‌که درسال‌های اخیر، بسیاری از پدیده های غیرامنیتی دربستر سایبر، به دلیل عدم شناخت و یا عدم مواجهه صحیح تبدیل به پدیده های ضدامنیتی حتی در سطح تهدید علیه امنیت ملی شده است.لذا بررسی همه جانبه این پدیده ها به منظور حفظ امنیت ملی کشور امری ضروری است.

پیشینه پژوهش

در پرداخت به موضوع سیاست BYOD دو نوع رویکرد پژوهشی وجود دارد که برخی به معرفی و توصیه به کاربرد و حصول نتایج مثبت بهره وری ناشی از بهره‌گیری از این سیاست پرداخته می شود و در برخی نیز ابزارهای امنیتی و نگرانی های حاصل از این پدیده معرفی شده است. نقطه مشترک تمامی این پژوهش‌ها به نگرانی‌هایی از کاربرد این پدیده و تبعات ناامنی، نفوذ، سوء استفاده و به طور کلی به عنوان تهدید پرداخته شده است شده است. جان دیلن در نشریه Network security اشاره می کند که استیو جابز و تیم امنیتی اپل تا زمان حیات وی این موضوع که درصورت پیاده شدن سیاست BYOD در سطح امریکای شمالی و کشورهای مشترک المنافع با امریکا خلاءهای امنیتی ابزارهای ساخته شده در این شرکت به دلیل استفاده گسترده در سطح ایالات متحده و کانادا می تواند موجب بروز تهدید علیه امنیت ملی باشد را پنهان می نمودند. همچنین در این مقاله اشاره شده که شرکت اپل از سوی آژانس امنیت ملی جهت بکارگیری برخی افزونه‌ها در ابزارهای خود تحت فشار بوده است که به ادعای نویسنده مقاله تن به این کار نداده است. چارچوب‌های امنیت دستگاه‌هایی که به عنوان رابط در این سیاست بکار برده می شوند نیز در این مقاله تشریح شده است. (Network security, volume ۲۰۱۷, issue ۷). بیل مارو در مقاله ای ضمن پرداختن به چالش ها و فرصت های این سیاست معتقد است این سیاست اطلاعات حیاتی کشور را تهدید خواهد نمود (Bill Morrow, Networking security, Volume ۲۰۱۶, Issue ۱۲, page۵-۸) . کوین تیسر محقق ارشد امنیت شبکه ماکروسافت بیان می دارد که بر خلاف نظر عامه که کمپانی های بزرگ هدف عمده ای برای تهدید از سوی سیاست BYOD هستنند بنگاه‌های کوچک[1] اهداف سهل الوصول تری به عنوان قربانیان بکارگیری این سیاست بدون در نظر گرفتن ملاحظات امنیتی خواهند بود. همچنین از نظر این متخصص امنیت، بنگاه های کوچک بیشتر از کمپانی های بزرگ مورد هجمه انواع تهدیدات سایبری ناشی از اجرای این سیاست بدون ملاحظات امنیتی قرار گرفته اند. با توجه به توسعه و نقش بنگاه های کوچک در سیاست های

1 SME

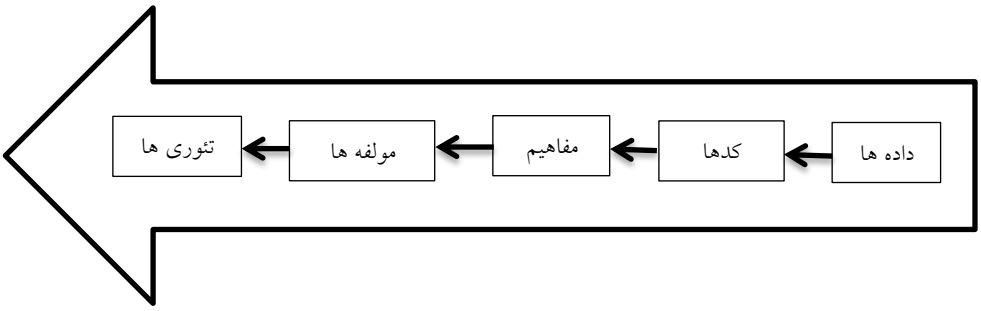
اقتصادی جمهوری اسلامی ایران و نقش احتمالی تهدید این بنگاه ها در تهدید امنیت ملی ج.ا.ا موضوع مقاله این محقق قابل توجه می باشد (John Thelens,Computer fread & security, volume ۲۰۱۷, issue ۷).هومن درخشانیان و سایرین ضمن معرفی پدیده BYOD و سطح بندی چالش های امنیتی آن مطالعه ای بر روی هزینه های ناشی از حوادث امنیتی داشته اند و گریزی هم بر هزینه های این پدیده بر امنیت ملی زده اند (درخشانیان هومن و عسگری آتنا،۱۳۹۴) طایی زاده و همکاران در نقد و بررسی این پدیده ضمن معرفی ابزارهای امنیتی مورد استفاده در محافظت از نهادهایی که از سیاست BYOD استفاده می‌کنند به معرفی دلایل شکست امنیتی این پدیده پرداخته شده است(طایی زاده و سایرین، ۱۳۹۵) حامد معصومی و همکاران به مطالعه موردی تأثیر پذیرش این سیاست بر کارکنان شهرداری تهران پرداخته و ضمن بررسی عوامل غیر امنیتی بر پذیرش آن، چالش‌های متنوع سازمان‌ها پس از پرداختن به این پدیده را تشریح نموده است.(معصومی و دیگران، ۱۳۹۵)

روش تحقیق:

در این مقاله با در نظر گرفتن شاخص های متعدد اثر گذار بر پذیرش پدیده BYOD و برقراری ارتباط بین شاخص‌های کیفی و استنباط کمی از آن می‌توان از روش داده بنیاد استفاده نمود.

نظریه داده بنیاد، روشی است که نظریه‌ها، مفاهیم، فرضیه‌ها و قضایا را طی یک فرایند منظم، به جای استنتاج از پیش فرض‌های قبلی، سایر پژوهش ها یا چارچوب های نظری موجود، به طور مستقیم از داده ها کشف می کند. (پاول ۱۹۹۹، ص ۶۷) هدف اصلی مبتکرین این روش یافتن روشی برای تولید نظریه در حین یک فعالیت تحقیقاتی بود. بسیاری از محققین علوم انسانی و اجتماعی ناگزیر به مفهوم سازی در این حوزه هستند. نظریه داده بنیاد، با ارائه یک روش سیستماتیک دقیق برای مفهوم سازی می‌تواند این محققان را یاری دهد. تئوری‌های استخراج شده از روش نظریه داده بنیاد، به صورت استقرایی از پدیده مورد مطالعه، منشعب می‌گردد. این تئوری ها، از طریق جمع آوری سیستماتیک داده های تجربی و تجزیه و تحلیل آن ها کشف و توسعه داده می شوند. جمع آوری اطلاعات و بسط نظریه، ارتباط تنگاتنگی با یکدیگر دارند. (کربین و استراوس، ۱۹۹۰، ص ۵۰) در واقع نظریه داده بنیاد روشی است کیفی برای ساخت نظریه ای که مبتنی بر واقعیت و داده ها باشد.

در روش شناسی داده بنیاد، کشف یا تولید نظریه بر مبنای حقایق و واقعیات موجود و از طریق جمع آوری نظام مند داده ها و با مدنظر قرار دادن کلیه جوانب مرتبط با موضوع تحقیق صورت می گیرد. داده های جمع آوری شده سیر تکاملی خود را تا رسیدن به تئوری مراحل را طی می‌کنند. تحلیل داده هایی که به منظور تکوین نظریه گرد آوری می شوند، با استفاده از "رمز نگاری نظری[1]" انجام می شود. در این شیوه ابتدا رمزهای مناسب به بخش های مختلف داده ها اختصاص می یابد. این رمزها در قالب مفهوم تعیین می شوند که آن ها را "رمزگذاری باز[2]" می نامند. سپس پژوهشگر با اندیشیدن در مورد ابعاد متفاوت این مقوله ها و یافتن پیوندهای میان آن ها به "رمزگذاری محوری[3]" اقدام می کند



شکل ۱: مدل فرایند اجرای گراندد تئوری استراوس(۱۹۹۰) دانایی فرد (۱۳۸۴)

سوال تحقیق:

آیا سیاست BYOD موجب بروز تهدیدات سایبری در سطح سازمان ها و در نهایت موجب تهدید امنیت ملی خواهد شد؟

ادبیات تحقیق

۱. پدافندغیرعامل

مجموعه اقدامات غیرمسلحانه ای که موجب افزایش بازدارندگی، کاهش آسیب پذیری، تداوم فعالیت های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران درمقابل تهدیدات و

1 Theoretical Coding
2 Open Coding
3 Axial Coding

اقدامات نظامی دشمن می گردد. (بازنگری سند راهبردی پدافند غیرعامل کشور،۱۳۹۶،ص ۱۴)

۲. امنیت ملی

تعاریف مندرج در فرهنگ های لغت درباره مفهوم کلی امنیت، بر روی احساس آزادی از ترس یا احساس ایمنی که ناظر بر امنیت مادی و روانی است، تأکید دارند (مندل،۱۳۹۵،۴۴) چندبعدی بودن مفهوم امنیت ملی سبب شده است دیدگاه های بسیار متنوعی راجع به آن وجود داشته باشد و هر کسی از زاویه دید خود به تعریف آن بپردازد .در همین راستا، برخی از نظریه پردازان، امنیت ملی را معادل با ارزش‌های حیاتی کشور می‌دانند، بدانگونه که آرنولد ولفرز آن را برابر با نبود تهدید برای ارزش‌های اکتسابی می‌داند (Wolfers,۱۹۶۲،۱۵۰).بری بوزان نیز امنیت را رهایی از تهدید و توانایی دولت و جوامع برای حفظ هویت مستقل و یکپارچگی کارکردی در مقابل نیروی تغییردهنده تعریف می کند (Buzan,,۱۹۹۱،۴۳۲) در عین حال، یکی از کامل ترین تعاریف را ریچارد اولمن ارائه کرده است:

تهدید امنیت ملی اقدام یا سلسله رویدادهایی است که نخست، به شکلی مؤثر و در دوره زمانی کوتاه خطر افت کیفیت زندگی را برای ساکنان کشور پیش آورد و دوم، با خطر جدی کاهش طیف خط مشی‌هایی که حکومت یا واحدهای غیرحکومتی خصوصی موجود در داخل کشور، اشخاص، گروه‌ها و شرکت‌ها می‌توانند از میان آن‌ها دست به انتخاب زنند، همراه باشد(تریف،۱۳۹۳،۴۹) مسلماً با این تعریف تصور ما از عوامل تهدیدزا دامنه بیشتری می‌یابد در مورد خصوصیات و ویژگی های امنیت ملی نیز تحلیل گران به طور عمده بر روی سه ویژگی تحول پذیری، نسبی بودن و ذهنی بودن مفهوم امنیت ملی تأکید می کنند .در مورد ویژگی اول، یعنی تحول پذیری مفهوم امنیت ملی باید گفت به دلیل نیاز حکومت به تعریف مشخصی از امنیت ملی، صاحب نظران کوشیده‌اند به این مهم دست یابند، اما تا کنون هیچ‌یک از آنان تعریف جامعی از این مفهوم ارائه نداده‌اند. در مورد ویژگی دوم یعنی نسبی بودن نیز باید افزود که ادعای دست‌یابی به امنیت مطلق، قابل تصور نیست .کشوری که ممکن است از لحاظ نظامی و اقتصادی دچار ناامنی نباشد، تهدیدهایی با ماهیت فرهنگی و اجتماعی، امنیت آن را در معرض خطر قرار دهد. جنبه دیگر نسبی بودن امنیت، توانایی‌های نسبی دولت ها برای مقابله با تهدیدهاست

(درویشی سه تلانی،۲۳،۱۳۷۱) ویژگی آخر یعنی ذهنی بودن امنیت به برداشت‌ها از احساس امنیت یا عدم امنیت مربوط می‌شود و ممکن است افراد و گروه‌های مختلف نسبت به آن نظر واحدی نداشته باشند.

۳. ارتباط امنیت ملی با امنیت سایبری

چندبعدی بودن مفهوم امنیت ملی سبب شده است دیدگاه های بسیار متنوعی راجع به آن وجود داشته باشد و هر کسی از زاویه دید خود به تعریف آن بپردازد .در همین راستا، برخی از نظریه پردازان، امنیت ملی را معادل با ارزش های حیاتی کشور می‌دانند، بدان‌گونه که آرنولدولفرز آن را برابر با "نبود تهدید برای ارزش های اکتسابی می داند (Wolfers, ۱۹۶۲،۴۴). امنیت ملی امروزه با تهدیدهای بیشماری مواجه است، اما در این میان، تهدیدهای سایبری پدیده جدیدی است که همراه با فناوری اطلاعات و گسترش ارتباطات گریبان‌گیر دولت‌ها شده است. این پدیده آنقدر جدید است که بررسی پیامدهای آن برای امنیت ملی دولت‌ها تا حد زیادی مورد غفلت واقع شده است. در دو دهه اخیر یک طیف، گرایش به زیر سؤال بردن رویکرد رایجی که درباره امنیت در چارچوب مطالعات راهبردی در طول دوره جنگ سرد توسعه داده شده است، دارند. این گرایش تأکید بر ضرورت فرارفتن از آنچه در بسیاری از نگرش‌ها به عنوان تفسیر بیش از حد نظامی شده از امنیت در نظر گرفته شده است(کلارک،۱۳۸۶:۲۳۶)

بحث درباره تهدیدهای سایبری تأثیر گرفته از انقلاب مداوم اطلاعات می‌باشد که ناشی از پویایی انتشار اطلاعات و تکنولوژی‌های ارتباطات در همه جنبه‌های زندگی انسان است (Cavetly and Brunner, ۲۰۰۷ :۱۵) در طول دهه گذشته، شماری از ویژگی‌های عمومی حملاتی که به وسیله کامپیوتر شکل گرفته و به تهدیدهای سایبری معروف شده‌اند، به عنوان یکی از بدترین تهدیدهای منافع ملی امروز شناسایی شده است (Cavetly, ۲۰۱۰:۱۸۰) با توجه به آنچه گفته شد، می‌توان امنیت سایبری را به طور کلی به عنوان حفاظت از زیرساخت‌های اطلاعاتی مهم و فرایندها و محتوای آن تعریف کرد (Theoharyand and Rollins،۲۰۰۹) بنابراین همانطور که یکی از مهمترین بخش‌های قدرت ملی امروز از قدرت اطلاعات بر می‌خیزد، یکی از مهمترین بخش‌های امنیت ملی نیز از امنیت و حفاظت از اطلاعات بر می‌آید.

انواع تهدیدات سایبری امنیت ملی را ازابعاد مفهوم امنیت، دولت محوری در امنیت، بعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، شیوه مقابله با تهدیدها و تعدد بازیگران در این عرصه، تحت تأثیر قرار داده و به تبع آن موجب تهدید امنیت ملی خواهد شد (خلیلی پور و نورعلی وند، ۱۳۹۱)

۴. مزایای استفاده از BYOD

کارکنان کار با دستگاه خود را به جای استفاده از دستگاه‌های شرکت را ترجیح می‌دهند. آنها احساس راحتی کار با .دستگاه‌های خود را دارند که این امر موجب افزایش بهره‌وری می‌شود BYOD افزایش تحرک با دستگاه و انجام کار از هر نقطه جغرافیایی را ممکن می سازد. BYOD سازمان را قادر می‌سازد که از کارمندان خود بدون در نظر گرفتن مکان مشخصی در سازمان استفاده کنند.

پدیده BYOD زیر ساخت ساده ای دارد و از شبکه‌های بی سیم استفاده می‌کند که صرفه جویی در هزینه برای سازمان را به دنبال دارد. در حال حاضر یکی از آسان‌ترین روش های محیط کار استفاده از سیاست BYOD است. سازمان می‌تواند با استفاده از این سیستم هزینه ارائه ماشین آلات، مدیریت IT و پشتیبانی و عیب‌یابی را کاهش می‌دهد. بررسی‌های شرکت اینکل منافع استفاده از BYOD را به شرح زیر اعلام می کند:

۲۸ ٪ بهبود کارایی و بهره وری

۲۲ ٪تحرک بهبود یافته کارمندان

۱۷ ٪صرفه جویی در خرید ماشین آلات جدید

۶٪ افزایش مدیریت و کاهش بروز عیب

۹ ٪رضایت شغلی (طایی زاده و سایرین، ۱۳۹۵)

۵. چالش های امنیتی BYOD

دستگاه‌های حاوی اطلاعات حساس سازمان ممکن است گم یا دزدیده شود که یک مسأله جدی به حساب می آید. زمانی که اطلاعات سازمان بر روی دستگاه های تلفن همراه ذخیره می‌شود مساله مالکیت داده پیش می‌آید. کارکنان ممکن است از محصولات مختلف با سیستم عامل‌های مختلف استفاده کنند. کاربران از این دستگاه‌ها در شبکه‌های خانگی و دیگر شبکه‌ها استفاده

می‌کنند این امکان وجود دارد که با حملات به این شبکه ها اطلاعات افشا و یا مخدوش شوند. مشکل بعدی در روت کردن دستگاه‌ها توسط کاربران برای افزایش دسترسی و نصب نرم‌افزارهای غیر مجاز است که ممکن استBYOD اسپم و یا ارسال اطلاعات ناشناس در شبکه باعث اختلال در سیستم شود. البته گستردگی این نوع دستگاه ها کمتر از۲٪ است، اما باید به طور جدی با این دستگاه‌ها مقابله کرد. برای مثال برای مسائل امنیتی BYOD، کلمات عبور قوی برای قفل کردن دستگاه توصیه می‌گردد؛ همچنین دسکتاپ مجازی[1] جایگزین برای جلوگیری از ذخیره سازی اطلاعات بر روی دستگاه است؛ این کار باعث می‌شود که کارکنان فقط در حالت آنلاین بتوانند به اطلاعات دسترسی داشته باشند و اطلاعات بر روی دستگاه شخصی ذخیره نمی‌شود تهدیدات دستگاه‌های همراه را می‌توان در کلاس‌های مختلفی دسته بندی کرد:

۱. نرم افزار های مخرب
۲. نرم افزار جاسوسی
۳. Mobots (محرومیت از خدمات)
۴. Botmaster (یکی از خطرناک ترین جرائم سایبری شناخته شده)

قابلیت پیشرفته دستگاه های مدرن همراه با قدرت ذخیره سازی بالا و سرعت بالای اینترنت باعث شده تا گزارش ESET انگیزه بیشتری برای تغییر مسیر فعایت خود از کامپیوتر به دستگاه های همراه را داشته باشند.آزمایشگاه این شرکت رشد نرم‌افزارهای مخرب اندروید را منتشر کرده است که در آن ۶۰ ٪ از خانواده بات نت ها هستند. (مشوش و سرمدی، ۱۳۹۶، ص۲)

۵. سیاست های امنیتیBYOD

۵،۱. سطح سازمانی:

سازمان باید قراردادی را با کارمندان برای اجرای سیاست هایBYOD منعقد کند. توافق باید دارای فهرست وظایف باشد که در آن مسئولیت برای پشتیبان‌گیری از دستگاه تعمیر و نگهداری و هزینه‌ها در آن بیان شده باشد. باید اطمینان حاصل کرد که کاربران مسئول پشتیبان‌گیری از اطلاعات شخصی خود هستند.کارکنان باید برنامه‌هایی را به دستور سازمان از دستگاه خود حذف کنند. کارمندان نباید از دستگاه‌های روت شده استفاده کنند و توضیح عواقب هرگونه تخلف از

1 VID

سیاست‌های امنیتی به آن‌ها داده شود. کنترل دسترسی باید بر اساس درجه و شرح شغل محدود شده باشد. از مکانیزم اثر انگشت برای ثبت دستگاه‌ها استفاده شود و برای دستگاه‌هایی که نمی‌خواهیم به شبکه شرکت دسترسی داشته باشند برای سیستم تعریف نماییم، تمام کارکنان نیازی به استفاده از دستگاه‌های شخصی برای کار ندارند.

در این بخش چند سطح دسترسی و طبقه بندی برای کاربران را معرفی می کنیم:

- کاربر معمولی:

کارمند معمولی ممکن است با سازمان برای مدت محدود و یا به صورت آموزشی در شرکت مشغول به کار باشد. این سطح دسترسی به کارمند اجازه می‌دهد با دستگاه خود در شبکه شرکت به اطلاعات مورد نیاز خود دسترسی داشته باشد .اما در خارج از شرکت دسترسی فقط از طریق برخی از شبکه ها و به صورت محدود دسترسی به اطلاعات سازمان را دارد.

- کاربر پیشرفته :

کاربر پیشرفته یک کارمند مورد اطمینان است که نیاز به استفاده از دستگاه خود در محل کار و منزل را دارد. کارمند می‌تواند اطلاعات را از طریق شبکه‌های عمومی در اختیار داشته باشد ولی از دسترسی به اطلاعات حساس جلوگیری می‌شود.

- کاربر حرفه‌ای :

کاربر حرفه ای از دانش امنیتی بالایی برخوردار است و کارمندی قابل اطمینان است این کاربر می‌تواند یک مدیر و یا رئیس شرکت باشد. آن‌ها امتیاز دسترسی به هر گونه اطلاعات سازمان را از شبکه‌های خانگی و حتی شبکه های غیر قابل اطمینان را دارند. برای دسترسی به اطلاعات حساس شرکت از VPN[1] و خدمات ابری استفاده می‌شود.

- کاربر میهمان :

کاربر میهمان یک کاربر جدید در شبکه است. تا زمانی که دستگاه کاربر در سیستم ثبت نشده باشد از هر گونه دسترسی به اطلاعات شرکت جلوگیری می‌شود (طایی زاده و سایرین، ۱۳۹۵).

۵،۲. سطح نرم افزار

1 Virtual Private Network

این سطح امنیت در قالب برنامه‌های کابردی دستگاه تلفن همراه می‌باشند. گوشی‌های تلفن همراه دارای نرم افزارهای کمکی برای تأمین امنیت هستند .چنین برنامه‌هایی در دستگاه‌های تلفن همراه با نام مدیریت دستگاه تلفن همراه شناخته می‌شوند. رویکرد امنیتی MDM[1] در ۳ اقدام اولیه و بر اساس کنترل، نظارت و محافظت عمل می‌کند. مدیریت دستگاه تلفن همراه پشتیبانی کامل از کنترل دستگاه شامل قفل کردن، کنترل اتصال SSL[2] به سرور، حذف کردن از راه دور، اعلان خطر، پشتیبان‌گیری از اطلاعات شخصی و اجرای سیاست‌های مدیریتی را انجام می‌دهد. نرم افزار مدیریت موبایل MAM[3] برای مدیریت دستگاه تلفن همراه است که برای کنترل برنامه‌های خاص در دستگاه استفاده می‌شود .نرم‌افزارهای مدیریتی موبایل قابل اعتماد نیست چون از دستگاه‌های همراه بطورکامل حفاظت نمی‌کند. در دستگاه‌های همراه سیستم مدیریت محتوا استفاده شده است که برای حفظ داده‌های گوشی‌های هوشمند، تبلت و PDA[4] ها به کار می‌روند و داده‌ها را می‌توان رمزنگاری و در دستگاه تعبیه نمود و درصورتی که دستگاه به سرقت برود اطلاعات قابل بازیابی نباشد. سازمان می‌تواند دسترسی به اطلاعات را بر اساس محل تعیین نماید که با استفاده از GPS[5] اعمال می‌شود.

تایید اطلاعات دستگاه در ۲ مرحله انجام می‌پذیرد. مرحله ۱ استفاده از رمزعبور و مرحله دوم ارسال تعدادی نشانه برای شماره تلفن همراه متعلق به کاربر ارسال می‌شود. نیاز به یک نرم افزار رمزنگاری خارجی برای به رمز درآوردن کارت حافظه خارجی است. هر زمان که کاربر اقدام به نصب نرم افزار از بازار یا فروشگاه اینترنتی نماید اجازه نرم افزار برای دسترسی به برخی از ویژگی‌های تلفن همراه مانند:

- جزئیات حساب کاربری
- اطلاعات نرم افزار
- تماس تلفنی
- شبکه‌های ارتباطی
- تنظیمات همگام‌سازی
- ابزارهای سیستمی

1 Mobile Device Management
2 Secure Socket System
3 Mobile Access Management
4 Personal Digital Assistant
5 Global Positioning System

- دسترسی به محل
- دوربین
- نشانه‌ها و سابقه وب
- ذخیره‌سازی

باعث می‌شود دستگاه و اطلاعات داخل آن در برابر حملات و درز اطلاعات کاربر به شدت آسیب‌پذیر خواهد بود.

۵,۳. سطح دستگاه

در این سطح دستگاه گواهینامه‌ها، رمزنگاری داده، چندکاربره بودن و سیستم‌های روت شده را چک می‌کند .در سیاست سطح دستگاه می‌توان برای یک گواهی کار برای کاربرانی که غیر قابل اطمینان هستند استفاده کرد. اگر گواهینامه کاربر هک شود احتمال دارد هکر بتواند به اطلاعات سرور دست پیدا کند، بنابراین دستگاه باید به اعتبار گواهینامه‌ها نظارت داشته باشد. متاسفانه دستگاه‌های روت شده در سازمان چندان مورد توجه قرار نمی‌گیرند کاربرانی که از دستگاه‌های روت شده استفاده می‌کنند قابلیت تغییر سیستم عامل و نصب هرگونه نرم افزاری در سیستم را دارند که ممکن است آسیب‌های جبران ناپذیری به سیستم وارد کنند. (Souppaya and Scarfone, ۲۰۱۳،۱۲۴-۴۲۰)

۶. متداول‌ترین مدل‌های امنیتی BYOD

مدل‌های امنیتی موجود:

- MDM مدیریت دستگاه سیار
- MAM برنامه مدیریت موبایل
- MIM[1] مدیریت اطلاعات موبایل
- مدل دسترسی مبتنی برVPN
- مدل چند لایه
- مدل کنترل دسترسی به شبکه[2] NAC

در ادامه به تشریح هر کدام از این مدل ها پرداخته می شود:

۶,۱. MDM مدیریت دستگاه سیار

1 Mobile Information System
2 Network Admition Center

وظیفه نظارت و کنترل از راه دور بر وضعیت دستگاه‌های همراه و کنترل عملکرد را برعهده دارند همان طور که در شکل زیر مشاهده می‌کنید MDM از یک عامل MDM.و یک سرور تشکیل شده است. عامل MDMیک برنامه است که بر روی دستگاه همراه نصب می‌شود و وضعیت داده های آن را برای سرور ارسال می‌کند. سرور MDMمدیریت داده‌های دریافت شده را انجام می‌دهد و براین اساس باعث می‌شود دستورات بر روی تلفن همراه ثبت شود و برای قفل کردن، کنترل رمزنگاری و سیاست‌های سازمانی را اعمال کند.

۶,۲. MAM برنامه مدیریت موبایل

سیستمMAM یک راه حل ارائه شده توسط مدیران IT[1] است که از راه دور نصب، به‌روزرسانی، حذف، حسابرسی و نظارت بر برنامه‌های سازمان را برعهده دارد.ویژگی‌های MAM را می‌توان به شرح زیر خلاصه کرد:

- مدیریت مقررات برنامه از راه دور
- حذف برنامه و پیکره‌بندی از راه دور
- به‌روز رسانی و پشتیبان‌گیری از راه دور
- نرم افزار لیست سفید و لیست سیاه

۶,۳. مدیریت اطلاعات موبایل MIM

هدف اصلی از MIM حفظ اطلاعات سازمانی برروی یک ابر خصوصی به صورت ایمن برای به اشتراک گذاری آن‌ها بین نقاط مختلف و سیستم عامل‌های مختلف است. MIM تنها اجازه می‌دهد تا تعداد محدودی از برنامه‌های کاربردی قابل اطمینان که برای کنترل و مدیریت اطلاعات شرکت رمز نگاری شده است در دسترس باشد.

راه حل‌هایی که در مدل‌هایی امنیتی مانند MIM , MDM , MAM قرار دارند را می‌توان از ۴ دیدگاه بررسی کرد

- شناسایی و کنترل ورودی
- حفاظت از داده
- امنیت نرم افزار
- موافقت/پذیرش

1 Information Thecnology

- .مدل امنیتی ارائه شده

۶,۴ مدل دسترسی مبتنی برVPN

این مدل با محافظت از کانال ارتباطات، امنیت محدودی را به وجود می‌آورد. داده‌ها در حالت ساکن، امن هستند در حالی که داده‌های در حالت استراحت خارج از دامنه این مدل است. دسترسی کارکنان به داده‌های شرکت، با استفاده از سرور از طریق کانال امن از طریق خود دستگاه خواهد بود.

۶,۵ مدل کنترل دسترسی به شبکه NAC

امنیت دستگاه‌ها را می‌توان توسط فن‌آوری‌های بالا و شبکه‌ها را می‌توان با استفاده از دسترسی به کنترل دسترسی شبکه(NAC) محافظت کرد. با استفاده از NAC می‌توان کاربران مجاز، دستگاه و برنامه‌های کاربردی را شناسایی کرد یک راه حل NAC، بررسی حالت فعلی و ویژگی‌های امنیتی دستگاه تلفن همراه قبل از اتصال به شبکه BYOD است. هردستگاهی ویژگی‌های امنیتی سازمان را برآورده نمی‌کند. بعد از حل مشکلات، دستگاه به شبکه BYODو منابع متصل می‌شود هدف از استفاده از NAC اجرای خط مشی امنیتی و محدود کردن ممنوعیت ترافیک، شناسایی کاربرانی که قوانین را می‌شکنند و یا غیرسازگار با سیاست هستند و توقف و کاهش نرم‌افزارهای مخرب می‌باشد. ویژگی‌های بسیاری در دستگاه تلفن همراه وجود دارد که باعث می‌شود NAC را به عنوان یک محیط برای BYOD انتخاب کرد که از جمله آن می‌توان به تنظیمات امنیتی نرم افزار آنتی ویروس، سیستم عامل و نرم افزار و فعال کردن نرم افزار فایروال اشاره نمود.

راه حل‌های امنیتی مختلفی برای BYODدر سازمان‌های مختلف وجود دارد که معمولاً از موارد مختلف مبهم و سازماندهی نشده تشکیل شده است. سیاست قابل اطمینان برای BYOD یک سیاست چند سطحی است و امنیت در چند سطح برقرار می‌شود. مدل طراحی شده به گونه ای عمل می‌کند که بدون در خطر قرار دادن بهره‌وری امنیت را برقرار می‌کند.

۷. دلایل شکست‌های امنیتی در BYOD

با بررسی دلایل شکست امنیتی BYOD، لیستی از این تهدیدات شناسایی شده است. شکست‌ها و دلایل آن به صورت مختصر به شرح ذیل می‌باشند:

۷,۱. سیاست های ناهماهنگ امنیتی

شکاف‌های وقفه، پایه و اساس بسیاری از شکست‌های امنیتی هستند، امنیت BYOD هم از این قاعده مستثنی نیست. برای مثال در کامپیوترهای رومیزی از کلمات عبور پیچیده استفاده می‌شود اما در سیستم های BYODبه یک کلمه عبور ۴ حرفی اکتفا می‌شود .افشای اطلاعات در رسانه‌های به اشتراک گذاری شده می‌توان از شایع‌ترین موارد به USB فلش‌ها و فلش مموری‌ها اشاره کرد .این دستگاه ها باعث می‌شوند تا فایل‌های حساس به دستگاه‌های عمومی راه پیدا کنند و زمینه افشای اطلاعات فراهم شود.

۷,۲. مدیریت حداقلی در دستگاه

دسترسی نامحدود و آسان در BYOD که این قابلیت به ندرت در لب تاب‌ها بوده است .دستگاه‌های BYOD غالباً مجاز به اتصال به شبکه‌های سازمان و دسترسی به ایمیل و دسترسی و دستکاری اطلاعات دارند.

۷,۳. اطلاعات باقی مانده در دستگاه‌ها قابل استفاده هستند

بسیاری از اطلاعات حساسی که بر روی گوشی‌های هوشمند و تبلت‌ها قرار می‌گیرند حتی پس از پاک شدن هم قابل سؤاستفاده هستند و بسیاری از آن‌ها قابل بازیافت و به فروش می‌رسند .بسیاری از کاربران آگاه هستند که زمانی آنها اطلاعات را از روی سیستم خود پاک می‌کنند سیستم عامل به سادگی آدرس آن محل را به عنوان پاک شده نشان می‌دهد ولی باز هم اطلاعات می‌توانند بازیابی شوند .این فقط شامل اطلاعاتی است که از روی سیستم حذف شده‌اند و اطلاعاتی که هنوز روی سیستم باقی می‌مانند و حذف نشده‌اند به مراتب در وضعیت بدتری قرار دارند.

۷,۴. افشای اطلاعات از داخل برنامه

گوشی های هوشمند و تبلت‌ها گیگابایت‌ها از داده‌ها را به راحتی فایل‌های ضمیمه شده به ایمیل‌ها، تصاویر و اسناد ذخیره شده را بین برنامه‌های کاربردی و یا مکان ناامن و از طریق ابزارهای همگام‌سازی، ابزار ابری، یا سیستم پشتیبان‌گیری خودکار نسخه‌ای از اطلاعات را برای

خود کپی کنند. احراز هویت، اطلاعات از دست داده یا به سرقت رفته، دسترسی به تلفن همراه، عدم درک سیاست‌های امنیتی عدم آموزش کارکنان سازمان، شرکت‌های تلفن همراه، اسناد، نرم‌افزارهای تلفن را کاهش می‌دهد.

۸.چالش‌های انسانی BYOD

تعلیم و آموزش کارکنان در مورد امنیتBYOD، راه حل‌های استقرا و اجرای سیاست های امنیتی، بسیار مهم هستند. این چالش‌ها هنگامی که همه کارکنان نیاز به درک سیاست های امنیتی BYOD دارند افزایش می‌یابد. حال کارکنانی که با اطلاعات حساس‌تری سروکار دارند، روش‌های امنیتی بیشتری را دنبال می‌کنند. هدف اصلی ازآموزش، انتقال انتظارات قابل قبول از دستگاه‌های مورد استفاده، حصول اطمینان از آگاهی از خطرات و چگونگی حفظ شیوه های امنیتی خوب است. واکنش‌های کارمندان، احساسات و رعایت سیاست‌های امنیتی BYOD یک چالش مداوم برای نظارت و نگهداری درکسب و کارها است. سیاست‌ها باید شامل دستورالعمل‌ها برای شرایطی باشد که در آن کارکنان مخالفت نشان می‌دهند، از دستگاه‌های تلفن همراه برای فعالیت‌های غیر قانونی استفاده می‌کنند، یا از لحاظ سخت افزاری به مشکل برخورد می‌کنند. با این حال نیاز به آموزش مداوم وجود دارد، چرا که با گذشت زمان کارمندان تمایل به فراموش کردن دستور العمل‌های امنیتی دارند و یا ممکن است که از تغییرات آگاهی نداشته باشند. برخی از کارمندان به طور جدی به دنبال بهره‌وری از نقاط ضعف امنیتی در BYOD هستند، به همین دلیل با محدودیت‌هایی که در اجرای سیاست های امنیتی وجود دارد به شدت مخالفت می‌کنند. (DownerandBhattacharya,۱۱۳۰،۲۰۱۵-۱۱۲۸)

۹. چالش قوانین و مقررات

قوانین و مقررات، مربوط به اطلاعات شرکت‌ها با استفاده از سیاست امنیتی BYOD یک شرکت تعیین می‌شود. قوانین ممکن است محدود به سطوح کنترل شرکت در اجرای دستگاه‌های کارکنان باشد. با گسترش شرکت‌ها در سطح جهانی نیاز به تنظیم سیستم‌های BYOD برای هر کشوری وجوددارد، که بر اساس آن‌ها، هماهنگی با قوانین محلی انجام شود، که باعث می‌شود.

قرارداد کارکنان و نظارت بر تغییر قوانین دشوار، ساده شود. به عنوان مثال، قوانین موثر بر طرح‌های BYOD در استرالیا شامل حفظ حریم شخصی کاربران قانون (۱۹۸۸) و قانون آزادی اطلاعات می‌باشد(۱۹۸۲) مسائل اخلاقی و حفظ حریم خصوصی همزمان با پیامدهای قانونی فوق می‌باشد. هنگامی که کارمندان دستگاه ها را برای استفاده در محل کار ارائه می‌کنند، شرکت‌ها باید چگونگی دور زدن اقدامات امنیتی، چگونه پیروی کردن از آئین‌نامه‌ها و رعایت حقوق و حریم خصوصی داده‌ها را در نظر بگیرند. اطلاعات حساس، به تحت نظارت قرار دادن به منظور جلوگیری از نشت اطلاعات که منجر به پرونده‌های حقوقی می‌شود نیاز دارد .اکثر قوانین حفظ حریم خصوصی داده‌ها در سراسر جهان بیان می‌کنند، قبل از اینکه شرکت‌ها برای حفظ داده‌ها و یا دسترسی به داده‌ها دردستگاه شخصی اقدامات امنیتی انجام دهند، اعلام رضایت کارکنان لازم است و در عوض شرکت‌ها و سازمان‌ها باید سطح امنیتی و حفاظتی خود را بهبود بخشند (DownerandBhattacharya,۲۰۱۵, ۱۱۳۳-۱۱۳۰)

۱۰. مخاطرات غیر امنیتی سیاست BYOD

خطر را به عنوان مقداری تعریف می‌کنند)یعنی مقداری که مشروط است(، که اگر نتایج عمل مورد نظر مطلوب نباشند خسارت وارد می‌شود و احساس فرد از این نتایج نامطلوب خواهند بود (Cunningham,۲۰۰۶،۲۲) در نتیجه خطر را به عنوان باورهای فرد درباره نتایج منفی نامعلوم بالقوه ناشی از مشارکت در برنامه BYOD در نظر می‌گیریم. درادامه به تشریح این مخاطرات می پردازیم:

۱۰،۱. مخاطرات فردی

میزان احتمال از دست رفتن کنترل فرد در اطلاعات شخصی‌اش در نظر گرفته می‌شود ،خطر فردی همچنین پتانسیل از دست خطر رفتن داده‌های خصوصی را شامل می‌شود. (Featherman and Pavlou,۲۰۰۳،۵-۸)

۱۰،۲. مخاطرات مالی

خطرات مالی به عنوان پتانسیل از دست رفتن هزینه سرمایه گذاری شده مربوط به خرید اولیه دستگاه و هزینه های نگهداری متعاقب آن تعریف می‌شود (Featherman and Pavlou,۲۰۰۳،۱۲)

۱۰،۳. مخاطرات روانی- اجتماعی

دارای ابعاد روانشناختی و اجتماعی است که به پتانسیلی اشاره می‌کند که تصمیم یک فرد می‌تواند آثار منفی در ذهن یا اعتماد به نفس فرد و یا محیط اطراف فرد داشته باشد مثلا دوستان، خانواده و همکاران (Cunningham,۱۹۶۷،۹)

۱۰،۴. خطر ادراکی

مجموعه خطاهای پیشنهاد شده در نظریه خطای درک شده ، بعنوان مخاطرات ادراکی در نظر گرفته می‌شود.

۱۰،۵. مخاطرات ایمنی

خطر ایمنی یعنی آثاری که سلامتی یک فرد را تهدید می‌کنند (Jacoby and Kaplan,۱۹۷۲;۲۳, Lu et al,۲۰۰۰،۵) در دسترس بودن در ساعات غیرکاری (مثلا به خاطر استفاده از گوشی‌های همراه هوشمند برای مصارف خصوصی و کاری) باعث می‌شود که بسیاری از ساعات غیرکاریشان صرف کار شود و در مقابل، بار کاری و اضطراب آن‌ها افزایش می‌یابد.

۱۰،۶. مخاطرات زیر ساختی

الزامات و زیر ساخت شامل زیرساخت فناوری، زیرساخت انسانی، زیرساخت فرهنگی، زیرساخت مدیریتی، زیرساخت پشتیبانی می‌باشد (Clark,۱۹۹۴; Keller and Suzuki,۲۰۰۴) هر پدیده‌ای که ظرفیت به خطر انداختن این زیرساخت‌ها را داشته باشد به عنوان یک مخاطره زیر ساختی شناخته می‌شود.

۱۱. انواع تهدیدهای سایبری

بازیگران دولتی و غیردولتی از قدرت سایبری استفاده می‌کنند تا به اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مالی خود در فضای سایبری و دنیای واقعی دست یابند. این اهداف در فضای مجازی از شیوه‌های متفاوتی حاصل می‌شوند که مهمترین آن‌ها عبارتند از: جنگ سایبری، تروریسم سایبری، جرایم سایبری، جاسوسی سایبری و آشفتگی سایبری (خلیلی پور و نورعلی وند، ۱۳۹۱،۷،-۶)

۱۱،۱. جنگ سایبری

به منظور درک اینکه آیا عمل خصمانه در فضای مجازی جنگ قلمداد می‌شود یا نه، لازم است قصد بازیگر را درک کنیم. به عنوان مثال، اگر هدف از یک حمله اینترنتی سود مالی یا شخصی از طریق روش‌های مجرمانه مانند سرقت، تقلب و اخاذی باشد، باید با آن به عنوان عمل مجرمانه برخورد شود، اما اگر هدف مهاجم با جاه طلبی‌های به مراتب بزرگتر همچون وارد کردن آسیب جدی به دولت یا شهروندان آن همچون تخریب، تضعیف و غیرفعال کردن زیرساخت های نظامی و غیرنظامی باشد، چنین رفتاری در واقع چیزی نزدیک به اقدام جنگی در مفهوم سنتی است (Cornish and Et al,۲۰۱۰: ۱۲۱۳-)

۱۱,۲. تروریسم سایبری

آژانس مدیریت فوق العاده فدرال[1]، تروریسم سایبری را اینگونه تعریف می کند: تهدید و حمله غیرقانونی علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آن، زمانی که برای ترساندن یا مجبورکردن حکومت یا مردم آن در پیشبرد اهداف سیاسی یا اجتماعی صورت می‌گیرد.(Congressional Research Service, ۲۰۰۸،۱۴)

۱۱,۳. حمله های سایبری

حمله سایبری چیزی متفاوت از جنگ سایبری است. حمله سایبری اختلال در صحت یا درستی داده‌هاست که معمولاً از طریق کدهای مخرب و تغییر در منطق برنامه و کنترل داده‌ها که منجر به خروجی‌های اشتباه می‌شود، صورت می‌گیرد. (Rodriguez,۲۰۰۶: ۹-۱۰) حمله‌های سایبری شامل چهار حوزه می‌شود:

۳-۱ از دست دادن تمامیت

۳-۲از دست دادن قابلیت

۳-۳ از دست دادن اطلاعات محرمانه

۳-۴ تخریب فیزیکی

آب، برق، بانکداری و حمل و نقل هوایی، تنها چند نمونه از خدماتی است که توسط زیرساخت های اطلاعات و ارتباطات در حال اجراست. این زیرساخت ها به طور فزاینده ای به یکدیگر

1 Federal Emergency Management Agency

وابسته هستند و هر حمله اینترنتی می تواند همانند بازی دومینو در آن‌ها اختلال ایجاد کند. اختلال در یک سیستم مساوی با اختلال در دیگر سیستم هاست و ادامه این روند از تأثیرات بالقوه حملات اینترنتی است (Islan and Et al, ۲۰۱۱: ۵-۶).

۱۱,۴. جرایم سایبری

جرایم اینترنتی می تواند نقض حق مالکیت معنوی، نقض حق اختراع، ربودن اسرار تجاری و غیره باشد. این جرایم، همچنین شامل حمله عمدی به رایانه ها به منظور مختل کردن آن‌ها و یا تحلیل گران هزینه کپی از اطلاعات طبقه بندی شده می‌شود

(Nagre and Warade, ۲۰۰۰, ۶)

۱۱,۵. جاسوسی سایبری

جاسوسی سایبری از رایانه ها و سیستم های مربوط به آن استفاده می کند تا اطلاعات محرمانه را جمع آوری کند. برخلاف جرایم سایبری که مسائل مالی و اقتصادی محرک اصلی مجرمان است، جاسوسی سایبری بیشتر تأثیرات سیاسی داشته و جامعه را تهدید می‌کند. محرک های اصلی جاسوسی سایبری متفاوت است، اما شامل کسب منافع نظامی، صنعتی،سیاسی و فنی است. جاسوسان سایبری اطلاعات دزدیده شده را با اهداف مختلف مورد استفاده قرار می دهند که برخی از آنها عبارتند از تهدید، اخاذی و مختل کردن اقدامات رقبای سیاسی.(Lord and Sharp, ۲۰۱۱, ۱۷)

۱۱,۶. آشفتگی سایبری

آشفتگی سایبری از رایانه‌ها و سیستم های مربوط به آن استفاده می کند تا هدف مورد نظر خود را ناقص کرده، تحت تأثیر قرار داده و یا آن را آزار دهد. اهداف سیاسی و ایدئولوژیکی در پشت این اقدامات وجود دارد و افراد از ابزاری استفاده می‌کنند که غیرقانونی هستند. گروه های هکری آنارشیستی و نیهیلیست‌ها از آشفتگی سایبری استفاده می‌کنند. به عنوان مثال، در واکنش به دستگیری جولیان آسانژ، مدیر سایت جنجالی "ناشناخته‌ها" گروهی تحت عنوان

ویکی لیکس، حمله‌های سایبری گسترده‌ای انجام دادند. برخلاف جرایم سایبری و جاسوسی سایبری که هدف شأن دزدی یا تغییر اطلاعات است، آشفتگی سایبری سعی در مجازات یا تأثیرگذاری بر عقاید و رفتار هدف‌های خود دارد. ممکن است طی این مرحله، اطلاعات زیادی دزدیده شده و یا تغییر یابد و یا هزینه‌های مادی فراوانی به شبکه‌های هدف وارد شود، اما قصد و نیت اصلی آشفتگی سایبری، آسیب رساندن است. بازیگران دولتی و غیردولتی می‌توانند از این ابزار استفاده کنند، ولی تاکنون آشفتگی سایبری توسط افرادی انجام شده که با نام فعالان عرصه هک شناخته شده‌اند (Lord and Sharp,۱۷،۲۰۱۱).

ویژگی‌های تهدیدهای سایبری:

۱. تعدد بازیگران در فضای سایبری
۲. هزینه کم ورود، صرف زمان کم و سرعت بالای اقدام
۳. ناشناس ماندن بازیگران و عدم قابلیت ردیابی
۴. تأثیرگذاری بسیار وسیع
۵. کمرنگ شدن نقش جغرافیا
۶. ساختار فضای اینترنت

مراحل انجام تحقیق

جهت انجام این پژوهش ضمن انجام مطالعات کتابخانه ای در مقالات و کتب چاپ شده در خصوص پدیده BYOD مفاهیم مد نظر در ارائه الگوی شناختی این پدیده استخراج شد. همچنین ۱۸ نفر از متخصصین و نخبگان عرصه امنیت فاوای سازمانی جهت انتخاب مفاهیم مختلف تأثیر گذار بر پدیده BYOD انتخاب و ابتدا مفاهیم جهت صحه گذاری در اختیار ایشان قرار گرفت. همچنین مقرر شد سایر مفاهیمی که از دیدگاه محقق احتمالاً مغفول مانده توسط ایشان بیان گردد در نهایت۳۶ عنوان از مفاهیم مرتبط با پذیرش سیاست BYOD در سازمان شناسایی و به شرح جدول یک کد گذاری شدند.

جدول شماره ۱ کد گذاری باز مفاهیم مرتبط با ابعاد مختلف پذیرش و بکارگیری BYOD در سازمان ها

ردیف	مفهوم	شناسه
۱.	مخاطرات عملکردی	T۱

۲.	مخاطرات روانی	T۲
۳.	مخاطرات فردی	T۳
۴.	الزامات زیرساختی	T۴
۵.	استفاده و انتخاب رمزعبورها	T۵
۶.	انتقال اطلاعات از طریق USB فلش ها و فلش مموری ها	T۶
۷.	اتصال همزمان به شبکه سازمان و شبکه جهانی	T۷
۸.	امکان دستکاری اطلاعات	T۸
۹.	امکان ردیابی	T۹
۱۰.	امکان قفل کردن دستگاه از راه دور	T۱۰
۱۱.	امکان پاک کردن اطلاعات از راه دور	T۱۱
۱۲.	امکان استفاده از روش های بیومتریک جهت احراز هویت	T۱۲
۱۳.	امکان استفاده از توکن جهت احراز هویت	T۱۳
۱۴.	امکان مجازی سازی میز کار (VID)	T۱۴
۱۵.	وجود نرم افزارهای مخرب	T۱۵
۱۶.	وجود نرم افزارهای جاسوسی	T۱۶
۱۷.	اقدامات محرومیت از خدمات	T۱۷
۱۸.	اقدامات BOT شدن یا کردن دستگاه	T۱۸
۱۹.	امکان ذخیره اطلاعات به صورت رمزگذاری شده	T۱۹
۲۰.	جاسوسی از اطلاعات شخصی	T۲۰
۲۱.	مدیریت تلفن همراه MDM	T۲۱
۲۲.	VPN	T۲۲
۲۳.	میزان آموزش کارکنانی که عضو این سیاست هستند	T۲۳
۲۴.	قوانین محلی	T۲۴
۲۵.	قوانین دولتی و ملی	T۲۵
۲۶.	مسائل اخلاقی و حفظ حریم شخصی	T۲۶
۲۷.	مدیریت اطلاعات دستگاه همراه MIM	T۲۷
۲۸.	حملات تشدید کننده امتیاز	T۲۸
۲۹.	کنترل دسترسی شبکه	T۲۹

.۳۰	میزان رضایت یا نارضایتی کارکنانی که این سیاست در سازمان آن ها اجرا می شود	T۳۰
.۳۱	مدیریت نرم افزارهای کاربردی MAM	T۳۱
.۳۲	اقدامات چند لایه حفاظتی	T۳۲
.۳۳	میزان اثرگذاری	T۳۳
.۳۴	بازدهی استفاده از پدیده	T۳۴
.۳۵	محل هایی که این پدیده می‌تواند مفید باشد	T۳۵
.۳۶	NAC	T۳۶

جدول شماره ۲ کدگذاری های محوری

ردیف	شناسه	مولفه ها
.۱	**T۲۳+T۳۰+T۳**	جنبه انسانی BYOD
.۲	**T۲۴+T۲۵+T۲۶**	سیاستها و قانون گذاریBYOD
.۳	**T۷+T۱۰+T۱۴+T۱۹+T۲۹**	جنبه فنی کاربری BYOD
.۴	**T۳۵+T۳۴+T۳۳**	میزان گسترش پدبده BYOD
.۵	**T۲۲+T۲۷+T۱۱**	اقدامات تأمینی سطح سازمانی BYOD
.۶	**T۸+T۱۵+T۱۶+T۱۸+T۲۰+T۲۸**	مخاطرات امنیتی BYOD
.۷	**T۱**	مخاطرات عملکردی
.۸	**T۲**	مخاطرات روانی
.۹	**T۳**	مخاطرات فردی
.۱۰	**T۳۳**	مخاطرات اجتماعی BYOD
.۱۱	**T۶+T۹**	مخاطرات زیرساختی BYOD
.۱۲	**T۲۱**	**MDM**
.۱۳	**T۲۷**	**MAM**
.۱۴	**T۳۱**	**MIM**
.۱۵	**T۲۲**	**VPN**

.۱۶	**T۳۶**	**NAC**
.۱۷	**T۳۲**	**مدل حفاظت چند لایه**
.۱۸	**T۱۲+T۱۳+T۱۷+T۵**	دسترسی غیرمجاز در BYOD
.۱۹	**T۸+T۲۰**	جاسوسی از طریق BYOD

جدول شماره ۳ کدگذاری انتخابی و ابعاد متناظر تهدیدسایبری

مولفه	بعد		ابعاد متناظر تهدید سایبری
جاسوسی	تهدید امنیتی (متغیرهای زمینه ساز ناامنی سیاست BYOD)	تهدید سایبری	جنگ سایبری
حملات تشدید کننده امتیاز			
دسترسی غیر مجاز فیزیکی یا مجازی			حمله سایبری
عوامل روانی کاربران			
جنبه انسانی	چالش امنیتی (عوامل موثر بر پذیرش سیاست BYOD)		تروریسم سایبری
سیاست گذاری و قانون گذاری			
ابعاد فنی			جرایم سایبری
ابعاد گسترش پدیده			
مخاطرات امنیتی	ابعاد شناختی مخاطرات BYOD		جاسوسی سایبری
مخاطرات اجتماعی			
مخاطرات ادراکی			
مخاطرات سیاسی			
مخاطرات مالی			
مخاطرات فردی			

مخاطرات زیرساختی			
MDM	مدل های امنیتی (متغیرهای بازدارنده عدم استفاده از سیاست (BYOD		آشفتگی سایبری
MAM			
MIM			
VPN			
NAC			
مدل حفاظت چند لایه			

به طور معمول نمونه گیری برای مسائل تخصصی که ارزیابی آنها با فنون تصمیم گیری چندمعیاره صورت می‌گیرد،از نوع هدفمند یا در دسترس است و جامعهٔ پژوهش این نوع مطالعات تنها شامل متخصصان می‌شود که اغلب شمار آنها محدود است(آذر و فرجی ، (۱۳۸۷ این پژوهش نیز با شمار محدود نیروی در دسترس در حوزهٔ فناوری اطلاعات و ارتباطات به تعداد ۱۸ نفر روبه رو بود که به عنوان گروه تصمیم گیرنده انتخاب شدند.

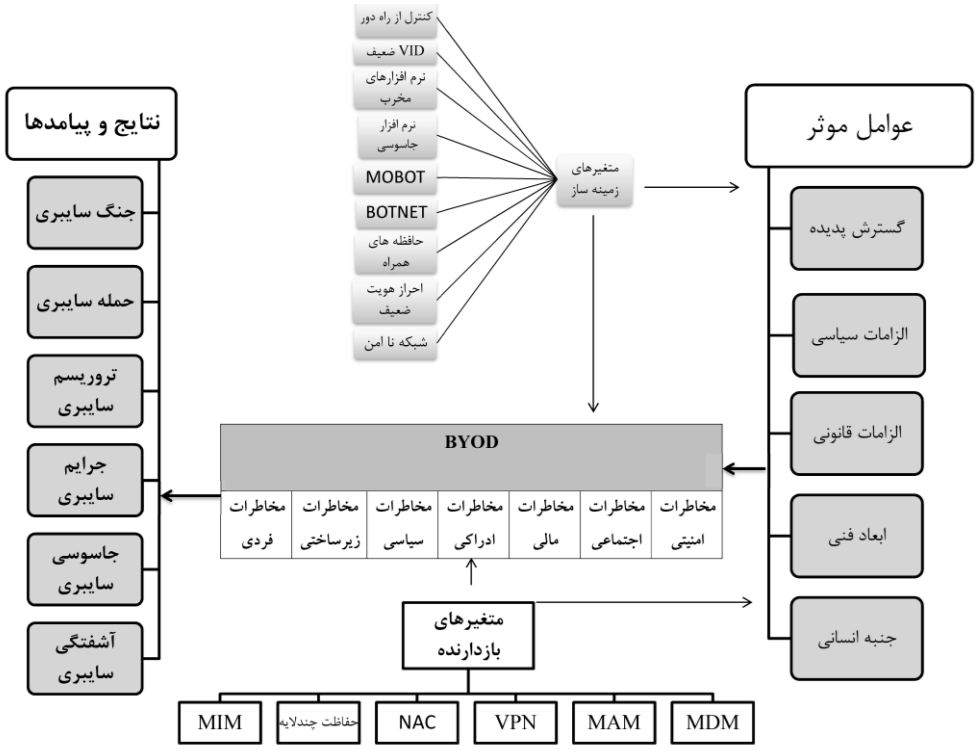
جامعه آماری مورد استفاده شامل ۱۸ نفر از مدیران، کارشناسان و خبرگان عرصه امنیت فاوا بوده اند. این افراد ۲۰ درصد در مقطع تحصیلی دکتری، ۵۵درصد کارشناسی ارشد و ۲۵ درصد کارشناسی بوده اند. ۴۵ درصد از این جامعه آماری شامل مدیران ارشد، ۲۵ درصد مدیران میانی و ۳۰ درصد از میان کارشناسان خبره عرصه امنیت فناوری اطلاعات بودند. همچنین ۹۰ رصد از افراد مورد مصاحبه مرد و ۱۰ درصد از ایشان زن بودند. ۸۵ درصد متاهل و ۱۵ درصد مجرد مورد مطالعه قرار گرفته اند.

پس از جمع بندی مولفه های قابل شناسایی در مرحله کدگذاری محوری، این بار نیز نتایج حاصل شده در اختیار گروه متخصصین قرار گرفت تا ضمن معرفی عوامل (ابعاد) موثر بر پذیرش این سیاست در سطح سازمان ها و در نظر گرفتن متغیرهای زمینه ساز و بازدارنده مخاطرات BYOD در سطح سازمان ها با عناوین تهدیدات، سیاست‌ها،چالش ها و مدل های امنیتی استخراج گردید. برای مرحله انتخاب نهایی ابعاد مدل ارتباطی پذیرش سیاست BYOD با تهدیدات سایبری و امنیت ملی از روش تحلیل سلسله مراتبی استفاده شد.روش تحلیل سلسله مراتبی بر پایهٔ الگوریتم ویژه و قضاوت های خبرگان اجرا می‌شود (اصغرپور،(۱۳۸۸،

فنون تصمیم‌گیری چندمعیاره، گروهی از خبرگان با شمار اندک و در دسترس، دربارهٔ مسئله‌ای که بر آن تسلط و شناخت دارند، نظر می‌دهند.

در نظر سنجی صورت گرفته مخاطبین که از متخصصین حوزه امنیت فناوری اطلاعات بودند بر مخاطرات غیر امنیتی این پدیده تأکید داشتند. به طور کلی پدیده های نوظهور در عرصه فناوری اطلاعات و ارتباطات بیش از آن که دارای پیچیدگی های فنی باشند دارای پیچیدگی های فرهنگی و اجتماعی هستند.

با در نظر گرفتن تمامی ابعاد و مولفه های مرتبط با پدیده BYOD، عوامل موثر، متغیرهای اثرگذار و بازدارنده مدل پیشنهادی جهت تشریح ارتباط ابعاد مختلف این پدیده و ارتباط آن با تهدیدات سایبری به شکل زیر استخراج شد:



تشریح مدل تدوین شده:

در این مدل با در نظر گرفتن عوامل موثری مانند گسترش پدیده BYOD، الزامات سیاسی، قانونی و در در نظر گرفتن ابعاد فنی و انسانی ظهور و گسترش سیاست BYOD در سازمان ها می‌بایست مخاطرات مختلف امنیتی، اجتماعی، مالی، ادراکی، سیاسی، زیرساختی و فردی را در نظر داشت. به منظور جلوگیری از مخاطرات امنیتی پدیده BYOD که عوامل مختلف زمینه ساز نا امنی سایبری مانند نرم افزارهای جاسوسی، خطرات محتمل در موضوعاتی مانند احراز هویت، تفکیک شبکه های ارتباطی عدم امکان کنترل از راه دور در همه بخشها و ....متغیرهای بازدارنده ای در سطوح فرد، دستگاه تلفن همراه و سازمانی مانند MDM,MAM,VPN,MIM,NAC و مدل های چند لایه بکار برده می‌شود اما مخاطرات ۷ گانه مورد اشاره در مدل، به دلیل گستردگی و فرا امنیتی بودن این مخاطرات و ابعاد، می‌تواند موجب بروز تهدیدات سایبری متناظر با تهدیدات BYOD مانند جاسوسی سایبری، ترویسم سایبری، جرایم سایبری و درصورتی که این پدیده بدون ملاحظات و ایجاد زیرساخت های مستحکم و چندلایه امنیتی در سطح جامعه گسترش یابد حتی جنگ و یا آشفتگی سایبری در سطح سازمان، جامعه و در نهایت موجب تهدید علیه امنیت ملی خواهد بود. در واقع این مدل بیان می دارد که تهدیدات مترتب و منشعب از بکارگیری سیاست BYOD در صورت عدم برنامه ریزی و مواجهه صحیح قطعا می‌تواند منجر به بروز مولفه های تهدید سایبری و در نتیجه تهدید علیه امنیت ملی شود.

به طور خلاصه با توجه به مخاطرات امنیتی و غیر امنیتی مترتب با سیاست BYOD در صورتی که از متغیرهای بازدارنده در مقابل متغیرهای زمینه ساز به خوبی استفاده نشود و زیرساخت های لازم در این خصوص فراهم نشود، مخاطرات مرتبت با این پدیده می‌تواند موجب بروز تهدیدات سایبری شود و با توجه به آن که تهدید سایبری به طور پیش فرض تهدید علیه امنیت ملی است بنابر این BYOD تبدیل به تهدید علیه امنیت ملی خواهد شد. این امر بر خلاف بند ۲ اهداف کلان در افق چشم انداز پدافند غیرعامل می‌باشد. (مصوبات سند راهبردی پدافندغیرعامل کشور ، ۱۳۹۲،ص۳۵)

نتیجه گیری و پیشنهاد

با توجه به الزامات پدافند غیرعامل به منظور جلوگیری از وقوع تلفات و تبعات اقدامات هوشمند علیه منافع ملی، مدل ارائه شده و در نظر گرفتن سیاست‌ها، تهدیدات و چالش های امنیتی سیاست BYOD در سازمان ها و اینکه تمامی چالش ها و تهدیدات سایبری سیاست BYOD به نحوی با عناصر تهدید سایبری در ارتباط است و پذیرش این حقیقت که تهدیدات سایبری موجب تهدید امنیت ملی خواهد شد بنابر این رشد و گسترش این سیاست در سازمان ها و نهاد های مختلف بدون در نظر گرفتن تمامی ابعاد مدیریت تهدیدات و چالش های امنیتی این پدیده می‌تواند موجب تهدید علیه امنیت ملی شود. در این تحقیق این حقیقت که سیاست BYOD می‌تواند موجب تهدید سایبری شود پرداخته شد؛ با توجه به آن که تهدید سایبری تهدید علیه امنیت ملی است بنابر این BYOD می‌تواند موجب تهدید علیه امنیت ملی شود. استفاده موثر و صحیح از متغیرهای بازدارنده فنی ارائه شده در این مقاله به همراه تبیین دقیق نقش عوامل موثر بر این پدیده می‌تواند از بروز ابعاد متناظر با تهدیدات سایبری جلوگیری بعمل آورد و در نتیجه امنیت ملی نیز از مخاطرات ناشی از این پدیده مصون گردد. همچنین ذکر این نکته ضروری است که آن چه به عنوان ویژگی های تهدید سایبری مرور شد دقیقا با تهدیدات متصور پدیده BYOD متناظر بوده و این موضوع خطر انطباق این دو مولفه با یکدیگر را تشدید می‌نماید.

با عنایت به این حقیقت که قبل از توصیه به گسترش پدیده های نوظهور به خصوص در بخش سایبری لازم است ابتدا در بخش کلان سیاست گذاری کشور ابزارهای قانونی در خصوص ایجاد بستر سیاست های امنیتی چه در بعد سخت افزاری و چه در بعد نرم افزاری فراهم شود، پیشنهاد می شود پژوهشگران در خصوص چگونگی ایجاد زیر ساخت های محلی امنیت سایبری و نحوه به وجود آمدن چالش‌های امنیتی که خود مستوجب ایجاد چالش های منجر به تهدید امنیت ملی است در ابعاد فرهنگی،اقتصادی، اجتماعی و سیاسی تحقیقات تکمیلی انجام دهند.

در پایان از دیدگاه پژوهشگر لازم به یاد آوری است، ساختار اجتماعی کشور ما در مواجهه با پدیده های نوظهور در عرصه‌های فناوری اطلاعات و ارتباطات بیش از آن که تحت تأثیر

جنبه‌های فنی و فناورانه آن پدیده قرار گیرد، با مخاطرات فردی، اجتماعی و فرهنگی آن پدیده مواجه است. مطالعه و بررسی عمیق و همه جانبه این گونه پدیده‌ها پیش از فراگیر شدن آن می‌تواند از بروز ناهنجاری‌های فردی، سازمانی، اجتماعی و به تبع آن امنیت ملی جلوگیری بعمل آورد.

منابع:

۱. بوزان، بری (۱۳۷۸)؛ **مردم، دولتها و هراس،** ترجمه پژوهشکده مطالعات راهبردی، تهران: پژوهشکده

۲. روزنا، جیمز و دیگران (۱۳۹۰)؛ "انقلاب اطلاعات، امنیت و فناوریهای جدید "، مترجم علیرضا طیب، تهران: پژوهشکده مطالعات راهبردی

۳. کلودزیچ،ادوارد، (۱۳۹۵) ،امنیت وروابط بین الملل،ترجمه:نادرپورآخوندی،چاپ دوم، تهران، پژوهشکده مطالعات راهبردی.

۴. یزدانفام، محمود (۱۳۸۶)؛ "دگرگونی در نظری ههها و مفهوم امنیت بین المللی"، فصلنامه مطالعات راهبردی،.شماره ۳۸ ،صص ۷۵۰-۷۲۵

۵. دانایی فرد. حسن (۱۳۸۴)، تئوری پردازی با استفاده از روی کرد استقرایی، استراتژی مفهوم سازی تئوری بنیاد، دانشور رفتار، شماره ۱۱

۶. سلیمی فرد خداکرم ، عباسی زاده عباس ، یاوشیرضا س (۱۳۹۴) شناسایی و اولویت بندی عوامل موثر بر پذیرش BYOD در سازمان با رویکرد فازی، مدیریت فناوری اطلاعات، دوره ۷، شماره ۴، صص ۷۸۸-۷۶۹

۷. خلیلی پور رکن آبادی علی ، نورعلی وند یاسر (۱۳۹۱)، تهدیدات سایبری و ـدثیر آن بر امنیت ملی، فصلنامه مطالعات راهبردی، شماره دوم سال پانزدهم

۸. مشوش منیژه ، سرمدی سعیده (۱۳۹۶)، بررسی مدل های ایجاد امنیت در BYOD،دومین کنفرانس مهندسی کامپیوتر و فناوری اطلاعات، تهران، ایران

۹. طایی زاده علی ، حسینی سید شهاب الدین (۱۳۹۵)، نصیری پریا ، امنیت سیستم های BYOD و ارائه چارچوب امنیتی، سومین کنفرانس بین المللی نوآوری های مهندسی برق و کامپیوتر

۱۰. Buzan, Barry (۱۹۹۱); “New Paern of Global Securiy in he firs-weny Cenury”, Internaional Affairs

۱۱. CACI International Inc. and U.S Naval Institute (July ۲۰۱۱); “Cyber Threats o National Security, Symposium One: Countering Challenges o he Global Supply Chain”, www.caci.com,۲۰/۰۵/۲۰۱۱

۱۲. Lewis, James A. (۲۰۱۵); “Cyber Security Two Years Later”, Center for Strategic &

۱۳. International Studies (CSIS)

۱۴. Carney, Scot (۲۰۱۷); “Rethinking he Cyber Threat A Framework and Path Forward”, Microsoft Corp. One Microsoft Way • Redmond, WA ۹۸۰۵۲-۶۳۹۹ • USA.

۱۵. Corniest, Paul & Livingstone, David & Clement ،Dave & Yorker, Claire (November ۲۰۱۵)

۱۶. Dunn Cavalry M. & Brunner E. (۲۰۱۷); “Information Power and Security: An Outline of

۱۷. Debates and Implications” in Dunn Cavalry M. & Mauler V. & Krishna-Hansel

۱۸. Haller, John & Merrell, Samuel A. & Bucolic, Mathew J. & Willkie, Bradford J. (۲۰۱۳);

۱۹. Politics and Methods”, Merton International Studies Review.

۲۰. Lord, Kristin M. & Sharp, ravis (۲۰۱۱); “America’s Cyber future Security and Prosperity in the Information Age”, Center for a New American Security, Volume I.

۲۱. Nye, Joseph s. (۲۰۱۴); “Cyber Power”, Belfour Center for Science and International Affairs.

۲۲. Perez, Akin & Sechris, Michael (۲۰۱۵); “Protecting Cyberspace and The U.S. National

۲۳. Rodriguez, Carlos A.; “Cyber Terrorism”, Inner-American Defense College as a University, Center for technology and National Security Policy

A. Drury and R. Absalom. (۲۰۱۶) BYOD: an emerging market trend in more ways than one.

۲۴. B. Morrow, "BYOD security challenges: control and protect your most sensitive data," Network Security, (vol ۴،۲۰۱۷)

۲۵. M. Eslahi, R. Salleh, and N. B. Anuar, "MoBots: A new generation of bonnets on mobile devices and networks," in Proceedings of the Computer Applications and Industrial Electronics (ISCAIE), ۲۰۱۴

۲۶. J. Lee, Y. Lee, and S.-C. Kim, "A White-List Based Security Architecture (WLSA) for the Safe Mobile Office in the BYOD Era," in Grid and Pervasive Computing. vol. ۷۸۶۱, end: Springer Berlin Heidelberg, Tajfar, A.H., Mimand, M.M., R. Soltani, F. & R. Soltani, P. (۲۰۱۶)

۲۷. Un Jan, A. & Contreras, V. (۲۰۱۵). Technology acceptance model for the use of information technology in universities. Computers in Human Behavior

۲۸. Vignette, U. & Asha, S. (۲۰۱۵). Modifying security policies towards BYOD. ۲nd International Symposium on Big Data and Cloud Computing (ISBCC'۱۵)

۲۹. The BYOD Opportunity. Retrieved ۲۰۱۶, from VMware, Inc

۳۰. K. Downer and M. Bhattacharya, "BYOD Security: A New Business Challenge," ۲۰۱۵ IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), Chengdu, ۲۰۱۵