DOI: 10.22034/ISJ.2021.252695.1237

International Studies Journal (ISJ)
Vol. 18, No. 1 (69), Summer 2021
Reseived Date: 2020/10/13
Accept Date: 2021/2/18
Article Type: Original Research
PP: 139-156

فصلنامه مطالعات بین‌المللی
سال ۱۸، شماره ۱ (٦٩)، تابستان ۱٤۰۰
تاریخ دریافت: ۱۳۹۹/۷/۲۲
تاریخ پذیرش: ۱۳۹۹/۱۱/۳۰
نوع مقاله: علمی- پژوهشی
صفحات: ۱٥٦-۱۳۹

چالش‌های امنیتِ سایبری در کشورهای «آسه‌آن»*

الناز کتانچی**- دکتر بابک پورقهرمانی***

چکیده

تبدیل امنیت سایبری به یک مشکل اساسی در جهان، باعث شده «آسه‌آن» نسبت به رفع مشکل امنیت سایبری با احساس فوریت اقدام کند. انجام اقدامات حفاظتی و سایر تلاش‌های صورت گرفته برای مقابله با حوادث سایبری در سطح منطقه‌ای و ملی نشان دهنده آگاهی «آسه‌آن» از اهمیت وجود یک روش مقاوم سایبری است که دستیابی به آن از طریق بررسی شاخص‌های مربوط به امنیت سایبری با موضوعات دفاع در برابر حملات سایبری نوآورانه، راهبردهایی در برابر تهدیدات امنیت سایبری، سیاست‌های دولت و محافظت در برابر حریم خصوصی، حمایت از زیرساخت‌های رایانه‌ای در دولت و مسائل حقوقی و اخلاقی در فضای سایبری به عنوان هدف این پژوهش با رویکرد توصیفی- تحلیلی میسر می‌باشد و سوالی که به ذهن متبادر می‌شود این است که کشورهای «آسه‌آن» برای دستیابی به روش مقاوم سایبری، محورهای مطالعاتی امنیت سایبری را بر کدام یک از شاخص‌ها استوار ساخته و تاکنون چه تعداد تحقیق در این شاخص‌ها انجام داده‌اند؟ یافته‌های پژوهش نشان می‌دهد که در مورد شاخص‌های مطالعاتی امنیت سایبری به خصوص در زمینه سیاست‌های دولت و محافظت در برابر حریم خصوصی در برخی کشورهای «آسه‌آن» تحقیقات محدود صورت گرفته است که این موضوع ارتباط مستقیم با افزایش جرایم سایبری دارد.

کلیدواژگان

آسه‌آن، چالش‌ها، امنیت سایبری، حملات سایبری، جرایم سایبری، سیاست دولت‌های عضو.

---

* این مقاله برگرفته از رساله دکتری الناز کتانچی با موضوع «نقش نهادها و سازمان‌های بین‌المللی در مبارزه با جرایم سایبری» و راهنمایی دکتر بابک پورقهرمانی است.

** دانشجوی دکتری تخصصی حقوق بین‌الملل عمومی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.

*** نویسنده مسئول، دانشیار گروه حقوق جزا و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران / ایمیل: pourghahramani@iau-maragheh.ac.ir

Article Link: https://www.isjq.ir/article_126626.html

مقدمه

حرکت کشورها به سمت نو گرایی باعث ایجاد انقلاب صنعتی چهارم[1]است، این نشان می‌دهد که امنیت سایبری به دلیل رشد سریع فناوری دیجیتال در کشورهای مدرن در سطح جهان، به عنوان موضوع تحقیقاتی انتخاب می‌شود. «آسه‌آن»[2]مخفف، انجمن ملل جنوب شرقی آسیا است. آغاز به کار «آسه‌آن» در ۸ آگوست ۱۹۶۷ توسط ۵ کشور اندونزی، مالزی، فیلیپین، سنگاپور و تایلند بوده، برونئی داروسلام در ۱۹۸۴ به «آسه‌آن» پیوسته است و کامبوج، جمهوری دموکراتیک خلق لائوس، میانمار و ویتنام در ۱۹۹۵ به «آسه‌آن» پیوستند. «از سال ۱۹۹۹ ده کشور عضو، عمدتاً به مسائل مربوط به صلح و امنیت منطقه‌ای پرداخته‌اند» (E.B.a.B.W, 2018).

وزیر خارجه پیشین تایلند[3]به عنوان یکی از بنیان‌گذاران «آسه‌آن» اعلام کرد که «هدف ترویج ثبات و صلح منطقه‌ای از طریق پیروی از قوانین مقرر و همچنین پیروی از اصول منشور سازمان ملل متحد است»(Jayabalan and et.al., 2014: 111). «فناوری اطلاعات و ارتباطات اکنون بخشی از زندگی روزمره است. این را می‌توان با رشد سریع تحول در فناوری دیجیتال اثبات کرد» (Staples and Niazi, 2007). بنابراین فناوری اطلاعات و ارتباطات به دلیل راحتی که در اختیار شما قرار می‌دهد به یک عامل اساسی در تجارت و دولت تبدیل شده است. با کمک رایانه‌های پیشرفته و اینترنت، دولت‌ها اکنون قادر به ارائه خدمات فوری به شهروندان خود با سطح کارایی بالاتر هستند. ارتباطات روزانه در حال حاضر در رسانه‌ها و کانال‌های مختلف گسترش یافته است. «توسعه داده‌های غیر متمرکز بر تمدن تأثیر مثبت گذاشته است. اما بدون نظارت، داده‌های دولتی شامل اطلاعات طبقه‌بندی شده به دلیل جرایم سایبری می‌توانند به سرقت بروند» (Dai, 2015: 10318). «این می‌تواند تهدیدی برای کشورهایی باشد که از طریق حملات سایبری و با هدف حملات تروریستی دچار جنگ می‌شوند»(Kazeruni, 2016: 179). «از زمان شروع این فناوری در انقلاب صنعتی چهارم، لزوم داشتن دانش امنیتی در هنگام استفاده از اینترنت اطلاع‌رسانی شده و برای تقویت دانش بحث شده است. برای دستیابی به این هدف، کار قابل توجهی برای حل مشکل ادغام دیجیتال در سراسر منطقه «آسه‌آن» انجام شده است» (Wardana and et.al., 2018: 18).

تاکنون، «تلاش‌های منطقه‌ای برای اتخاذ یک استراتژی جامع در خصوص امنیت سایبری کُند بوده است»(Katanchi & Pourghahramani, 2019: 41). «برای کشف فناوری سریع و پویای انقلاب صنعتی چهارم باید یک تحقیق از طریق یک آزمایش تجربی انجام شود، که این امر

---

[1]. Industrial Revolution (IR4.0)

[2]. Association of Southeast Asian Nations

[3]. Thanat Khoman

دولت‌ها را برای پذیرش شتاب انقلاب صنعتی چهارم دشوار کرده است» (Supayah and Ibrahim, 2017: 17-18). «اصلاحات در تجارت، آموزش، تجارت الکترونیک، تولید و مراقبت‌های بهداشتی باید با یک سیستم مدرن‌تر در ساختار سازمانی یا شرکت انجام شود که این ممکن است نیاز به تلاش گسترده داشته باشد» (Supayah and Ibrahim, 2017: 18 & Ong and Chong, 2014). مسئله این است که نوآوری نیاز به یک سرمایه‌گذاری بزرگ دارد. این امر منجر شده است به این که سرمایه‌گذاری‌های مالی، در آینده‌ای نزدیک به بخش سودآوردتر متمرکز شود، بدون اطلاع از اینکه امنیت سایبری می‌تواند به دلیل رشد سریع در فضای مجازی در طولانی مدت، سودآوری بیشتری داشته باشد. مطالعات قبلی در درجه اول به موضوعات خاصی در زمینه امنیت سایبری که در یافته‌ها مشاهده می‌شود، تمرکز دارد.

بنابراین، این پژوهش در صدد پاسخ به این پرسش است که کشورهای «آسه‌آن» برای دستیابی به یک روش مقاوم سایبری، محورهای مطالعاتی امنیت سایبری را بر کدام یک از شاخص‌ها استوار ساخته و تاکنون چه تعداد تحقیق در این شاخص‌ها انجام داده‌اند؟ پاسخ به این پرسش برای مطرح کردن نام این کشورها و بیان مشکل، بررسی اقدامات و تقویت سیستم موجود فعلی از طریق مطالعه شاخص‌های مربوط به امنیت سایبری با عناوین دفاع در برابر حملات سایبری نوآورانه، راهبردهایی در برابر تهدیدات امنیت سایبری، سیاست‌های دولت و محافظت در برابر حریم خصوصی، حمایت از زیرساخت‌های رایانه‌ای در دولت و مسائل حقوقی و اخلاقی در فضای سایبری می‌باشد. نتایج این تحقیق از طریق شاخص‌های بیان شده نشان می‌دهد که برخی از کشورهای «آسه‌آن» تحقیقات کافی در زمینه امنیت سایبری در داخل کشور انجام نمی‌دهند و به تمام شاخص‌ها توجهی ندارند و این‌ها با افزایش جرایم سایبری، کلاهبرداری‌ها و تجاوزهایی که می‌تواند به امنیت شهروندان آسیب برساند و روند اجرای آن را مختل می‌کند، مرتبط است.

۱- پیشینه

مطالعات زیادی در زمینه این موضوع صورت گرفته است که از امنیت سایبری در کشورهای «آسه‌آن» خبر می‌دهد. همانطور که قبلاً گفته شد، این مطالعات عمدتاً به موضوعات و چالش‌های مربوط به امنیت سایبری پرداخته است. ابتکارات مختلفی برای رسیدگی به این قبیل موضوعات از قبیل اجرای برنامه‌ریزی استراتژیک فناوری اطلاعات و ارتباطات که در مالزی اجرا شده است، صورت گرفته است. در ژوئیه سال ۲۰۱۱، واحد نوسازی و برنامه‌ریزی مدیریتی مالزی[1] با عنوان «برنامه استراتژیک بخش فناوری اطلاعات و ارتباطات ۲۰۱۱-۲۰۱۵» و در مارس ۲۰۱۶ «برنامه استراتژیک فناوری اطلاعات و ارتباطات[2] در بخش عمومی ۲۰۱۶-۲۰۲۰» را منتشر کرد. واحد

[1]. Modernization and Management Planning Unit (MAMPU)

[2]. Information and Communications Technology (ICT)

نوسازی و برنامه‌ریزی مدیریتی مالزی با شناخت اهمیت آن، در آگوست ۲۰۰۳ سندی با عنوان «برنامه استراتژیک بخش فناوری اطلاعات و ارتباطات بخش ۲۰۰۳-۲۰۰۸» صادر کرد. «این برنامه شامل راهنمایی‌های لازم برای توسعه برنامه‌ریزی استراتژیک فناوری اطلاعات و ارتباطات، به ویژه در بخش دولتی است»(Faradilla and et.al., 2017: 3). حجم گسترده‌ای از مطالعات منتشر شده وجود دارد که کشورها تحقیقات مرتبطی را انجام داده‌اند، همانطور که در قسمت‌های بعدی توضیح داده خواهد است.

اخیراً حوادث مرتبط با سایبر در کشورهای «آسه‌آن» در ژانویه سال ۲۰۱۷ تا ماه مه ۲۰۱۹ رخ داده است. در ژوئیه سال ۲۰۱۸، سنگاپور بدترین حملات سایبری خود را متحمل شده است. نخست وزیر «لی هسیین لوون»[1]در مقاله‌ی منتشر شده توسط TODAY اظهار داشت که هکرها برای سرقت اطلاعات ۱,۵ میلیون بیمار سرپایی و سوابق دارویی آنها وارد سیستم‌های فناوری SingHealth شدند. همچنین، طبق مرکز ریسک آسیا و اقیانوسیه، داده‌های شخصی ۸۵۰ شخص در سال ۲۰۱۷ از درگاه پایگاه داده آنلاین وزارت دفاع سنگاپور به سرقت رفت. از اکتبر سال ۲۰۱۸، در مجموع ۴۵ واقعه باج افزار با هدف؛ هدف قرار دادن بخش‌های مختلف در مالزی گزارش شده است، که تعداد زیادی سرور و رایانه در سازمان‌ها را تحت تأثیر قرار داده است. در طول حادثه نقض شدید مالزی، گزارش شد که اطلاعات بیش از ۴۶ میلیون مشترک تلفن همراه به سرقت رفته و در محیط وب منتشر شده است. به نوبه خود، مالزیایی‌ها، ممکن است در برابر اصطلاحات مهندسی اجتماعی آسیب‌پذیر باشند و در بدترین حالت ممکن است طبق گزارش TheStar در اکتبر ۲۰۱۷ تلفن‌ها شنود شوند.

همچنین «تیم واکنش اضطراری رایانه برونئی»[2]سال گذشته ۲/۱۴۳ حمله به امنیت سایبری در برونئی را ثبت کرد که از این تعداد ۳۸ درصد ناشی از نرم افزارهای مخرب بود که توسط «بورنئو بولتن» در نوامبر سال ۲۰۱۸ منتشر شد. در وب سایت تایلند، شرکت تویوتا موتور قربانی نقض داده‌ها شده است. در حمله سایبری به تایلند ممکن است به اطلاعات برخی از مشتریان آن دسترسی بالقوه وجود داشته باشد. اما بدترین حمله در مارس ۲۰۱۹ رخ داد، هنگامی که اطلاعات شخصی متعلق به ۳/۱ میلیون مشتری در نتیجه نقض داده‌ها در دفاتر فروش خودشان در ژاپن در معرض دید قرار گرفت. دولت مالزی راه حل اصلی این مشکلات را در این می‌داند که برای هماهنگی با سایر کشورها در جهت کاهش حمله‌های سایبری و افزایش میزان دفاع موفق باید کنترل ایجاد کند»(Dai, 2015: 131-132).

---

[1]. Lee Hsien Loong

[2]. Brunei Computer Emergency response team (BruCert)

به گفته عبدل ماناپ[1] (S. Chia, 2013)، «در عصر دیجیتال، هویت را می‌توان صرفاً در گستردگی دسترسی به اطلاعات دانست، نه در «روابط». مجرمان به اشکال جدید سرقت هویت در فضای مجازی متوسل می‌شوند. این امر باعث قرار گرفتن بیشتر افراد در معرض خطر و ایجاد یک چالش واقعی برای مقامات اجرای قانون و قانونگذاران است. هنگامی که توسط پلیس به دلیل جرم دستگیر شود، این جنایتکار به دروغ ادعا می‌کند که قربانی شده است» (Kadis and Abdullah, 2017). پیشتر سیستم تشخیص نفوذ را بررسی کرده بود، که می‌تواند نقش مهمی در مهار و متوقف کردن سوء استفاده‌ای که توسط اشخاص غیرمسئول در شبکه اتفاق افتاده مانند کاربران مخرب داشته باشد. این سیستم دارای دو روش برای تشخیص سوء استفاده از شبکه است، یعنی تشخیص مبتنی بر ناهنجاری و امضا.

برای رقابت با کشورهای توسعه یافته باید رویکردی منظم از اجرای امنیت سایبری در کشورهای «آسه‌آن» توسعه یابد. طبق گفته سالامزادا[2] (Ghazi-tehrani, 2015: 25)، «برخی از آثار قبلی از رویکرد کیفی استفاده کرده‌اند، از جمله انجام مصاحبه برای تهیه چارچوب امنیت سایبری یا ارائه پیشنهادهایی برای بهبود چارچوب موجود در امنیت سایبری. به عنوان مثال: برای فناوری VPN، هنگامی که کاربر با اتصال یک رایانه دیگر با استفاده از پلت فرم VPN، داده یا اطلاعات را کنترل می‌کند، از تمامیت داده‌ها محافظت می‌شود. معماری شبکه برای بازیابی سایت با احراز هویت از طریق فناوری‌های VPN فراهم شده است. یکپارچگی داده‌ها یکی از تکنیک‌های امنیتی است که می‌تواند تغییر داده‌های دیگر را هنگام انتقال تشخیص دهد» (Kargar and et.al., 2016: 27).

۲- مبانی نظری امنیت سایبری

امنیت در فضای سایبری، «امنیت در قسمت زیرساخت و شریان‌های اطلاعاتی می‌باشد. ایجاد فرصت جدید برای شغل‌ها و ممالک در محیط خودکارسازی، تجارت الکترونیکی، تبادل و همکاری منجر به تولید هدفمند، ذخیره سازی و بهره برداری از اطلاعات حساس و حیاتی شده است. وابسته بودن به شبکه‌های پر سرعت و قدرتمند شدن پردازشگرها روز به روز در حال افزایش است که باعث قرار گرفتن سیستم‌ها در معرض خطرات طبیعی و حتی بزهکاری و تروریسم سایبری شده، که نیازمند نظارت و مدیریت می‌باشد» (Kiankhah, 2010: 35).

در عصر حاضر، «اهم‌ترین اثر توانایی و قدرت، محافظت از اطلاعات در برابر تهدیدات دشمنان، مبادله و به اشتراک گذاشتن اطلاعات امن در جهت افزایش قدرت است. جنگ

[1]. Abdul Manap

[2]. Salamzada

نفوذگرها، جنگ اطلاعاتی و تروریسم سایبری، از تهدیدات به شمار می‌آیند، چرا که این تکنولوژی بومی نبوده و عمل به دستورهای صاحبان تکنولوژی باعث افزایش تاثیرگذاری تهدیدها بر زیر ساخت‌ها و شاهرگ‌های اطلاعاتی شده است»(Kiankhah and Alavi, 2011: 7).

می‌توان گفت که امنیت در حوزه ملی و حاکمیتی در مفهوم امنیت در فضای سایبری گنجانده می‌شود. «به گونه‌ای که تهدیدها، امنیت در حوزه ملی و حاکمیتی حیاتی‌ترین منافع ملی و حاکمیتی یک نظام را با تغییر مواجه می‌سازد. این قسمت از تهدیدها در بخش زیرساخت و شاهرگ‌های اطلاعاتی قرار دارد و قسمتی از آن در حوزه امنیت اقتصادی و سیاسی مطرح است. برای تعامل افراد و جوامع فضای سایبری به عنوان ابزاری به شمار می‌آید که فضایی را برای جنگ روانی ایجاد می‌نماید. در این جنگ روانی، اطلاعات حاصل علیه تفکرات انسانی مورد استفاده قرار می‌گیرد و سبب بروز عملیات علیه اراده ملی و عناصر نظامی شده و باعث به وجود آمدن تضاد در فرهنگ و آنارشی می‌گردد»(Alberts, 2006: 104).

همچنین «می‌توان امنیت را به صورت سلبی، عدم تهدید، به ویژه تهدید خارجی در حوزه‌های سیاسی، اجتماعی، اقتصادی، غذایی، فرهنگی و... دانست» (Adkanian and Khosravi, 2018: 140). «در دفع تهدیداتی که یک کشور با آن روبه‌رو بوده و از طریق این دفع می‌تواند به صورت ایجابی امنیت خود را تأمین نماید، سطح قدرت یک کشور دارای اهمیت فراوان می‌باشد» (Soheili Najaf Abadi and et.al., 2019: 158). بنابراین «امنیت سایبری را می‌توان به عنوان راه حل‌های پیشنهادی (شامل قوانین، دستورالعمل‌ها، حراست‌های فناوری و غیره) برای تهدیدات ناشی از هک و به خطر انداختن سیستم‌های رایانه‌ای تعریف کرد»(Botnet, 2018: 3).

بیان مطالب اجمالی در خصوص امنیت سایبری و اینکه چه مفاهیمی در خصوص امنیت سایبری بیان شده و با توجه به موضوع بایستی به این نکات نیز اشاره گردد که کشورهای «آسه‌آن» چارچوبی برای همکاری در زمینه امنیت سایبری ایجاد کرده‌اند. «اعضای «آسه‌آن» در مورد لزوم ایجاد یک چارچوب رسمی برای هماهنگی تلاش‌های امنیت سایبری در منطقه و تشریح دیپلماسی سایبری، سیاست‌ها و مسائل عملیاتی توافق کرده‌اند و توصیه شده است که این مکانیزم انعطاف‌پذیر باشد و عوامل مختلفی مانند شرایط اقتصادی را در نظر بگیرد. اعضا همچنین بر اهمیت «فضای مجازی مبتنی بر قوانین» برای پیشبرد پیشرفت اقتصادی و بهبود سطح زندگی تأکید دارند. همچنین توافق دارند که اصولاً قوانین داخلی، هنجارهای داوطلبانه و غیر الزام آور رفتار دولت و همچنین اقدامات عملی «ایجاد اعتماد به نفس» برای اطمینان از ثبات فضای مجازی ضروری است»(Khanisa, 2013: 45).

اما با این وجود کشورهای «آسه‌آن» نیز مورد حملات سایبری قرار گرفته‌اند، یا به این دلیل که زیرساخت‌های ناامنی دارند که می‌توانند مورد بهره برداری قرار بگیرند، یا مراکز اتصال خوبی

برای شروع حملات هستند. برخی از حوادث قابل توجه عبارتند از: «در ژوئیه ۲۰۱۶، ویتنام توسط گروه هک چینی «CN1937» مورد حمله سایبری قرار گرفت که صفحات اطلاعات پرواز و سیستم‌های صوتی را در فرودگاه‌های Noi Bai و Tan Son Nhat ربود و منجر به از دست دادن کنترل محلی و پخش ضد ویتنامی و فیلیپین شد. گزارشات نشان می‌داد که گروه هک «APT32»، معروف به OceanLotus، که پیشتر با دولت ویتنام در ارتباط بود، قبل از اجلاس سران منطقه‌ای در مانیل، پایتخت فیلیپین، کامپیوترهای «آسه‌آن» را شکسته است. آنها همچنین وب سایت‌های وزارتخانه‌ها یا سازمان‌های دولتی در لائوس، کامبوج و فیلیپین را به خطر انداختند، بنابراین کدهای مخرب را بر روی کامپیوترهای قربانیان هدف قرار می‌دهند. این اهداف شامل وزارتخانه‌های امور خارجه کامبوج، محیط زیست، خدمات ملکی و امور اجتماعی و پلیس ملی بود. وب سایت‌های نیروهای مسلح فیلیپین و دفتر رئیس جمهور؛ وب سایت ده‌ها گروه غیر دولتی ویتنامی، افراد و رسانه‌ها؛ و وب سایت‌های متعلق به چندین شرکت نفت چینی» (Raska, 2018: 2). بنابراین می‌توان گفت که این خطرات سایبری می‌تواند مانع اعتماد به اقتصاد دیجیتال شود و از تحقق کامل ظرفیت دیجیتالی منطقه جلوگیری کند.

در سال ۲۰۱۸، «آسه‌آن» اولین گروه منطقه‌ای بوده و همچنان تنها گروهی است که اصولاً در ۱۱ استاندارد داوطلبانه و غیر الزام آور در گزارش سال ۲۰۱۵ کارشناسان دولتی سازمان ملل متحد عضو شده است. «به دنبال اولین بیانیه رهبران «آسه‌آن» در مورد همکاری امنیت سایبری که در همان سال صادر شد، «آسه‌آن» پیشرفت قابل توجهی در زمینه ایجاد ظرفیت سایبری منطقه‌ای داشته است تا به اعضای خود در مدیریت موثر خطرات و تهدیدهای سایبری کمک کند. برنامه ظرفیت سایبری «آسه‌آن»، مرکز تعالی امنیت سایبری سنگاپور «آسه‌آن – سنگاپور» و مرکز ظرفیت سازی امنیت سایبری «آسه‌آن – ژاپن» همه در تلاش برای دستیابی به این هدف هستند» (Koh, 2020).

مداقه در موارد مطرح شده نشان می‌دهد که کشورهای «آسه‌آن» در جهت تقویت همکاری در جنبه‌های گوناگون آموزشی، فرهنگی، اقتصادی و اجتماعی، تکنولوژیکی و غیره که ارتباط مستقیمی با ایجاد امنیت سایبری به دلیل بهره‌مندی از فضای سایبری در جنبه‌های گوناگون ذکر شده دارد، گام برداشته و علاوه بر این، هدف ترویج ثبات و صلح منطقه‌ای بالاخص صلح و ایجاد امنیت اقتصادی، سیاسی و تکنولوژیکی را از طریق پیروی از قوانین مقرر و همچنین پیروی از اصول منشور سازمان ملل متحد را به عنوان مهم‌ترین موضوعات مورد توجه قرار داده‌اند. با این وجود باز هم کشورهای «آسه‌آن» با چالش‌های برقراری امنیت سایبری روبرو هستند که در مطالب آتی به آن‌ها اشاره خواهد شد.

۳- تاریخچه امنیت سایبری

در کنار چندین ویروس مخرب و انواع مختلف بدافزارها در سناریوی امروز، فکر اینکه «فقط چند دهه پیش، هنگام به وجود آمدن شبکه‌ها و شبکه‌های جهانی گسترده، امنیت همیشه مهمترین نگرانی نبوده» غیرمنطقی به نظر می‌رسد. حتی، در مراحل اولیه به «آژانس پروژه‌های تحقیقاتی پیشرفته»[1] و «شبکه‌های مبتنی بر پکت سوئیچ که توسط پنتاگون حمایت مالی می‌شود»، حملات زیادی توسط دانش‌آموزان دبیرستان انجام شد. به همین ترتیب، «می‌توان به سناریوهای مربوط به (TalkTalk)[2] نگاه کرد، که در اوایل، امنیت نداشتند»(Iranian Students Newsletter, 2018: 2/8) و در یک حمله طولانی، اولین محققان رایانه‌ای در جهان به اجرای روش‌های امنیتی پرداختند.

روند هک کردن خطوط تلفن برای ایجاد تماس‌های رایگان[3] تکنیکی معروف بود که در دهه ۷۰ و روزهای آغازین کار شبکه‌ها به کار گرفته شد. یکی از مشهورترین فریدرها، جان دراپر، که قبلاً فعالیت می‌کرد و سپس به دلیل حملات مکرر مجازات و دستگیر شد. در سال ۱۹۸۹، «رابرت موریس اولین کرم رایانه‌ای را در اینترنت راه اندازی کرد، که توانست بسیاری از موارد آنلاین را در آن زمان از بین ببرد». اما در اواخر دهه ۸۰، اینترنت به عنوان قسمت حیاتی زندگی روزمره ما نبود و عواقب آن به اندازه امروز کارآمد نبود. ویروس «کرم» اولین جرمی شد که تحت «قانون تقلب و سوء استفاده رایانه‌ای در سال ۱۹۸۶» محکوم شد. «این کرم پس از اینکه چندین ویروس اولیه در اوایل دهه ۱۹۸۰ در معرض خطر قرار گرفت، مانند ویروس «مغز» در سال ۱۹۸۶، مورد تبلیغ قرار گرفت» (Gupta and et.al., 2018: 178).

٤- روش‌شناسی

در این تحقیق از رویکرد مقاله مروری استفاده شده است، که روشی مؤثر برای انجام بررسی تحقیقات انجام شده است(ASEAN: Conception and Evolution, 2018). «به گفته مارک استپلز[4] یک بررسی منظم روشی است که می‌تواند تعیین، ارزیابی و تجزیه و تحلیل کند. مروری بر پیشینه تحقیق با استفاده از بانک‌های اطلاعاتی آنلاین، استفاده از کلمات کلیدی که در ظرف شش سال انتشار یافته‌اند. همچنین این تحقیق به بررسی و تحلیل مسئله امنیت سایبری و چالش‌های مربوط به «آسه‌آن» از سال ۲۰۱۴ تا ۲۰۱۹ می‌پردازد. این کمک می‌کند تا مشخص شود که کدام کشورها به طور فعال در زمینه تحقیق در مورد امنیت سایبری خود فعالیت می‌کنند و منبع مکرر تحقیقات

---

[1]. Advanced Research Projects Agency Net (ARPANET)

[2]. شرکتی است که در زمینه ارائه سرویس‌های شبکه همراه، مخابرات و دسترسی به اینترنت فعالیت می‌کند.

[3]. Phreaking

[4]. Mark Staples

امنیت سایبری بوده‌اند»(Rahmawati, 2019). «با استفاده از کلمات کلیدی مانند «امنیت سایبر و آسیا»، «حمله سایبر»، «تهدید»، «انتشار سایبر» و «چالش‌های آسه‌آن» برای بدست آوردن نتیجه، روش‌های جستجو از طریق یافتن اطلاعات در پایگاه داده‌های آنلاین انجام می‌شود. اطلاعات مربوطه از مقالات بازیابی شده استخراج می‌گردد و متعاقباً به سؤالات تحقیق پاسخ می‌دهند» (Abd and et.al., 2015).

مقاله شامل داده‌های دانشگاه‌های محلی به عنوان داده‌های ثانویه برای ارائه شواهد بیشتر است. برای تجسم تصویر بزرگتر، داده‌هایی که از منابع آنلاین مانند ژورنال‌ها، مقالات، کار کنفرانس و فصل‌های کتاب جمع آوری شده و تجزیه و تحلیل شدند. در این تجزیه و تحلیل، از روش ردیابی فرآیند استفاده خواهد شد که به وسیله آن داده‌های جمع آوری شده با استفاده از روش دو رویکرد تفسیر می‌شوند، یعنی از لحاظ زمانی و موضوعی. مجموعه تحقیقات از سال‌های ۲۰۱۴ تا ۲۰۱۹ انجام شده است. که در جدول شماره ۱ و ۲ توضیحات موضوع تحقیق و شاخص‌های اختصاری و ژورنال/ مقاله کشور مبدا مشخص شده است (Mizan and et.al., 2019: 115).

توضیحات موضوع تحقیق	شاخص
دفاع در برابر حملات سایبری نوآورانه	Defense against innovative cyber attacks (DCA)
راهبردهایی در برابر تهدیدات امنیت سایبری	Strategies against cybersecurity threats (SCS)
سیاست‌های دولت و محافظت در برابر حریم خصوصی	Government policies and protection against privacy (GPP)
حفاظت از زیرساخت‌های رایانه ای در دولت	Protection of computer infrastructures in the government (PCG)
مسائل حقوقی و اخلاقی در فضای سایبری	Legal and ethical issues on cyberspace (LEC)

جدول- ۱: توضیحات موضوع تحقیق و شاخص‌های اختصاری آن

Table 1: Description of the Research Topic and Its Brief Characteristics

Source: (Authors, 2021)

ژورنال/ مقاله کشور مبدا	نام اختصاری	ژورنال/ مقاله کشور مبدا	نام اختصاری
سنگاپور	SG	تایلند	TH
کامبوج	CB	فیلیپین	PH
میانمار	MY	اندونزی	IN
ویتنام	VT	بروئنی داروسلام	BD
لائوس	LO	مالزی	MA

جدول- ۲: ژورنال مقاله کشور مبدا و نام اختصاری آن‌ها

Table 2- Journal of the Country of Origin and Their Acronym

Source: (Authors, 2021)

۵- یافته‌ها

نویسندگان در ۲۷ ژورنال، مقالاتی را شناسایی کرده و موضوعات و چالش‌های امنیت سایبری در کشورهای «آسه‌آن» را که در جدول شماره ۳ (مجموعه داده‌ها با استفاده از موضوع تحقیق)

مشخص شده، برجسته می‌کنند. این یافته‌ها در جدول شماره ۳ نشان داده شده است. همه ۲۷ ژورنال / مقاله‌ها و مقالات مربوط به کنفرانس از پایگاه داده مندلی، گوگل اسکولار و سایر پایگاه‌های داده ژورنال‌ها در موضوع تحقیق در امنیت سایبری جمع آوری شده است. جدول ۳ مجلات بارگیری شده از منبع پایگاه داده باز و مجلات اختصاصی را به خوبی نشان می‌دهد (Mizan and et.al., 2019: 119). این جدول همچنین موضوع تحقیق را با شاخصی که در جدول شماره ۱ توضیح داده شده است ساده می‌کند(LEC, PCG, DCA SCS GPP).

شماره	نویسندگان	تعداد	کشور	سال	شاخص تحقیق				
					DCA	SCS	GPP	PCG	LEC
1	Lowell A Quisumbing	15	PH	2017		*			
2	Candice Tran Dai	16	VT	2015				*	
3	Nazura Abdul Manap, Anita Abdul Rahim, Hossein Taji	9	MA	2015				*	
4	Chooi Shi Teoh, Ahmad Kamil, Mahmood Suhazimah Dzazali	17	MA	2018		*			
5	Hashim/ Masrek, Mohd Shamir, Mohamad Noorman, Yunos Zahri	18	MA	2016			*		
6	M S Razana, W. Shafiuddin	40	MA	2016				*	
7	Zahri Yunos, Rabiah Ahmad, Nor Amalina, Mohd Sabri	19	MA	2015	*				
8	Lean Ping Ong, Chien Fatt Chong	20	MA	2014		*			
9	Ganesan A/L Supayah, Jamaludin Ibrahim	21	MA	2017					*
10	Maslina Daud, Rajah Rasiah, Mary George, David, Asirvatham, Govindamal Thangiah	35	MA	2018		*			
11	Nazli Ismail Nawang	39	MA	2014					*
12	Harry Hung	22	SG	2016	*				
13	Ching Yuen Luk	42	SG	2019				*	
14	Aufar Muhammad Rizki	23	SG	2018		*			
15	Elina Noor	24	SG	2014				*	
16	Elina Noor	41	SG	2015				*	
17	Goryan Ella, Vladimirovna	25	BD	2018					*
18	Sahidan Abdulmana, Burhan Saleh	26	TH	2015		*			
19	Adam ghazi Tehrani	27	TH	2015			*		
20	Ineu Rahmawati	28	IN	2019				*	
21	Elsa Faradilla Anak, Agung Banyu Perwita	29	IN	2017				*	
23	Muhmad Rizal Yanyan M. Yani	30	IN	2017			*		
24	Tin Maung Maung, Mie Mie Su Thwin	31	MY	2017					*
25	Tin Maung Maung, Mie Mie Su Thwin	32	MY	2017	*				
	Lars Gjesvik, Niels Nagelhus Schia	33	MY	2018		*			
26	Rainer Einzenberger	43	MY	2016		*			
27	Aroy C.K Wardana, Rodon Pedrason, Triyoga Budi Prasetyo	34	MY	2018	*				
28	-	-	CB	-					
29	-	-	LO	-					

جدول-۳: مجموعه داده‌ها با استفاده از موضوع تحقیق

Table 3: Data Set Using the Research Topic/ Source: (Authors, 2021)

شماره	کشور	درصد تحقیقات	شماره	کشور	درصد تحقیقات
1	ویتنام	4%	6	کامبوج	0%
2	مالزی	33%	7	اندونزی	11%
3	فیلیپین	4%	8	لائوس	0%
4	برونئی	4%	9	تایلند	7%
5	سنگاپور	18%	10	میانمار	19%

جدول-۴: درصد تحقیقات منتشر شده در زمینه امنیت سایبری توسط کشورهای «آسه‌آن» در ۲۰۱۹-۲۰۱۴

Table 4: Percentage of Research Published in the Field of Cyber Security by ASEAN Countries in 2019-2014

Source: (Authors, 2021)

شماره	موضوع تحقیق	درصد
1	DCA	15%
2	SCS	29%
3	GPP	11%
4	PCG	30%
5	LEC	15%

جدول-۵: درصد موضوع تحقیق امنیت سایبری در کشورهای «آسه‌آن» در ۲۰۱۹-۲۰۱۴

Table 5: Percentage of Cyber Security Research in ASEAN Countries in 2019-2014

Source: (Authors, 2021)

رویکرد مشاهده امنیت سایبری در کشورهای «آسه‌آن» را می‌توان با تعداد تحقیقات انجام شده در جدول ۴ را بررسی کرد. یافته‌ها نشان می‌دهد که لائوس و کامبوج به عنوان اعضای «آسه‌آن» از اهمیت مبارزه با جرایم سایبری در فضای سایبری در کشورهای خود اطلاع ندارند. از داده‌های جدول ۴ می‌توان دریافت که از سال ۲۰۱۴ تا سال ۲۰۱۹ هیچ تحقیقی درباره مسائل مربوط به امنیت سایبری در هر دو کشور انجام نشده است. با این حال؛ مالزی، سنگاپور و میانمار رویه توجیهی و بازدارندگی را در مورد اشکال قانونگذاری و سیاست اجرا کرده‌اند. در جدول ۴ نشان داده شده است که ۹ تحقیق در مالزی و همچنین ۵ مورد در سنگاپور و میانمار بین سال‌های ۲۰۱۴ تا ۲۰۱۹ انجام شده است. کشورهای دیگر مانند فیلیپین، ویتنام، برونئی، تایلند و اندونزی تحقیق در مورد چالش‌ها و موضوعات پیش رو در زمینه امنیت سایبری را آغاز کرده‌اند.

طبق گفته Sunkpho، فقط اندونزی قانون امنیت سایبری خاصی ندارد، اما آنها به اطلاعات الکترونیکی و عمل معاملات متکی هستند. در رابطه با موضوع حمایت از داده‌ها، به کشورهایی مانند تایلند و اندونزی استثنا داده شده است که قانون کلی حمایت از داده‌ها را در دست داشته باشند. تایلند و اندونزی در مورد حریم خصوصی قانونی یکپارچه ندارند، درعوض این قانون از طریق قوانین و مصوبات مختلفی اجرا می‌شود. با این حال، تایلند و اندونزی در حال تهیه یک قانون کلی برای محافظت از داده‌ها هستند. ویتنام تنها کشوری است که قانون کاملی دارد که با

یک قانون واحد، یعنی قانون امنیت اطلاعات سایبری[1] که هم ایجاد امنیت نموده و هم از داده محافظت می‌کند. نکته جالب توجه این است که «مالزی فقط قانون حمایت از داده‌های شخصی را در معاملات تجاری به استثنای داده‌های پردازش شده توسط دولت اعمال می‌کند» (Rizal and Yani, 2017).

نتایج تحقیق حاضر همچنین زمینه‌های امنیت سایبری را از جمله دفاع در برابر حملات سایبری نوآورانه، راهبردهایی در برابر تهدیدات سایبری، سیاست‌های دولت و محافظت در برابر حریم خصوصی، محافظت از زیرساخت‌های رایانه‌ای در دولت و مسائل حقوقی و اخلاقی در فضای سایبری را در جدول ۵ نشان داده است. جدول ۵ نشان می‌دهد که محافظت از زیرساخت‌های رایانه‌ای در دولت و راهبردهایی در برابر تهدیدات سایبری از مضامین تحقیقاتیِ محبوب در بین کشورهای «آسه‌آن» هستند که با تعداد ۸ تحقیق در هر دو موضوع در رتبه اول قرار دارند. مسائل حقوقی و اخلاقی در فضای مجازی و دفاع در برابر حملات سایبری نوآورانه با تعداد چهار نوع تحقیق در هر دو موضوع تحقیق در رتبه دوم قرار دارند. از این رقم مشخص می‌شود که تعداد بسیار کمی از تحقیقات در مورد سیاست‌های دولت و محافظت در برابر حریم خصوصی در بین کشورهای «آسه‌آن» انجام شده است که تنها سه تحقیق در طول سال ۲۰۱۴ تا ۲۰۱۹ است.

نتیجه گیری

در این مقاله نتایج تحقیقات انجام شده در خصوص امنیت سایبری در کشورهای «آسه‌آن» در سال ۲۰۱۴ تا ۲۰۱۹ ارائه شده است. این مطالعه نتیجه گرفته است که برای غلبه بر موانع در امنیت سایبری، «آسه‌آن» نیاز به همکاری کامل از سوی همه اعضای آن دارد. این مسائل و چالش‌ها را نمی‌توان به درستی مدیریت کرد و به طور مستقل توسط کشورهای خاص اداره می‌شود. بنابراین، «آسه‌آن» برای دستیابی به هدف ثبات سایبری برای منطقه باید از فرصت‌ها استفاده کند و همکاری را بهبود بخشد. این مطالعه نشان داده است که به طور کلی، در تحقیقات راجع به موضوع امنیت سایبری تنها به برخی از شاخص‌ها توجه می‌شود. بنابراین، برای گسترش سیاست‌های محافظت از بخش خصوصی و زیرساخت‌های حفاظت از جامعه عمومی، باید به دامنه گسترده‌تری گسترش یابد.

جمع آوری شواهد در این مطالعه نشان می‌دهد که تحقیقات در زمینه امنیت سایبری باید بهبود یابد، با توجه به اینکه این چالش بزرگ است و موضوعاتی که ناشی از تهدیدات سایبری است همچنان ادامه می‌یابد و یافته‌های این مطالعه تأثیرگذار بر تحقیقات فعلی است. در مرحله

[1]. Law of Cyber – Information Security (LCIS)

اول، این مطالعه می‌تواند به عنوان منبع تحقیق برای مطالعه از سال ۲۰۱۴ تا اوایل سال ۲۰۱۹ در بین کشورهای عضو «آسه‌آن» استفاده شود. ثانیاً، تحقیقات بیشتر می‌تواند در مورد دو کشور، یعنی کامبوج و لائوس، که هنوز مقالات نمایه شده‌ای منتشر نکرده‌اند، متمرکز شود. با این حال؛ مالزی، سنگاپور و میانمار رویه توجیهی و بازدارندگی را در مورد اشکال قانونگذاری و سیاست اجرا کرده‌اند. کشورهای دیگر مانند فیلیپین، ویتنام، برونئی، تایلند و اندونزی تحقیق در مورد چالش‌ها و موضوعات پیش رو در زمینه امنیت سایبری را آغاز کرده‌اند.

اما با این وجود چالش‌های زیادی برای بهبود امنیت سایبری در کشورهای آسه‌آن وجود دارد. این کشورها فاقد ذهنیت استراتژیک، آمادگی در سیاست و نظارت نهادی بر امنیت سایبری هستند. مسئولیت ممکن است با هماهنگی کم یا بدون هماهنگی بین پلیس ملی (برای جرایم اینترنتی)، وزارت کشور (برای زیرساخت‌های حیاتی)، وزارت ارتباطات از راه دور (برای نقض موارد) و ارتش (برای درگیری‌های سایبری) تقسیم شود. عدم وجود یک چارچوب متحد اغلب منجر به کمبود سرمایه قابل توجه می‌شود. در بخش خصوصی، خطر سایبری هنوز به جای یک مشکل تجاری، یک فناوری ارتباطات و اطلاعات تلقی می‌شود، بنابراین مشاغل منطقه‌ای رویکرد جامعی به امنیت سایبری ندارند. صنعت امنیت سایبری منطقه آسه‌آن برای تأمین تقاضا تلاش می‌کند زیرا فاقد توانایی و تخصص است. کشورهای آسه‌آن دارای اطلاعات محدودی از تهدید هستند که اغلب به دلیل بی اعتمادی و عدم شفافیت است. تکامل سریع فناوری، نظارت و پاسخگویی به تهدیدها را دشوارتر می‌کند، به ویژه با رمزگذاری قوی تر، رایانش ابری و رشد گسترده اینترنت اشیا. در نهایت مفید خواهد بود که اثرات امنیت سایبری در فعالیت‌های تجاری و سازمانی در «آسه‌آن» یا سایر کشورها نیز مورد ارزیابی قرار گیرد.

Reference

1. Abd, R, N. H., Hamid, S., Kiah, L. M., Shamshirband, S., Furnell. S. (2015). A Systematic Review of Approaches to Assessing Cybersecurity Awareness. Kybernetes 44(4):606–22. at: https://doi.org/10.1108/K-12-2014-0283
2. Abdul Manap, N., Abdul Rahim, A., Taji, H. (2015). Cyberspace Identity Theft: The Conceptual Framework. Mediter. r. *J. Soc. Sci*., 6(4), 595–605. at: https://doi.org/10.5901/mjss.2015.v6n4s3p595
3. Abdulmana, S., Saleh, B. (2015). Coordinate Negative Content Filtering and Threat Detection in Thailand on the Internet Infrastructure. 5th Int. *Conf. Inf. Commun. Technol. Muslim World*, at: https://doi.org/10.1109/ICT4M.2014.7020647, 6–10
4. Adkanian, A., Khosravi, M. (2018), the Position of Food Security from the Perspective

of Transitional Justice. *International Studies Journal (ISJ)*, 16(2), 155-139. **(In Persian)**

5. Alberts, D. (2006). National Security Requirements in the Information Age. *Research Institute for Strategic Studies*. **(In Persian)**
6. ASEAN. (2018). Conception and Evolution. In The 3rd ASEAN Reader. *ISEAS –Yusof Ishak Institute Singapore*, xiii–xviii.
7. Brunot, R. (2018). United Nations Security Council Background Guide, at: http://www.ccwa.org/wp-content/uploads/2018/09/UNSC-Final.pdf: 1-11
8. Chia, S. (2013). The ASEAN Economic Community: Progress, Challenges, and Prospects. at: https://doi.org/10.2139/ssrn.2346058
9. Dai, C. T. (2015). Cybersecurity in Vietnam: Formulation and Implementation of a New Strategy. @ *La cybersécurité au VIêt Nam: Formulation et mise en oeuvre d'une nouvelle stratégie. Herodote*, no. 157, 126–140. at: https://doi.org/10.3917/her.157.0126
10. Daud, M., George, M., Asirvatham, D. (2018). Bridging the Gap between Organisational Practices and Cyber Security Compliance: Can Cooperation Promote Compliance in Organisations?. *Int. J. Bus. Soc*, 19(1), 161–180.
11. E. B. a B. W. World. (2018), Cybersecurity for Industry 4.0 Cyber Security Implications for Government, Industry and Homeland Security.
12. Einzenberger, R. (2016). If It's on the Internet It Must Be Right: An Interview with Myanmar ICT for Development Organisation on the Use of the Internet and Social Media in Myanmar. *Austrian Journal of South-East Asian Studies*, 9(2), 301-310.
13. Faradilla, E., Agung, A., Perwita, B. (2017), Indonesia Cyber Security Development: The Analysis of Infrastructure, Regulation and Institutional Building (2007-2015). *Information System Application Journal*, 2(1), pp. 1–5.
14. Ghazi-Tehrani, A. (2015). The Current State of Cybercrime in Thailand: Legal, Technological, and Economic Barriers to Effective Law Enforcement. *J. Thai Justice Syst. Spec. Ed*, 1–28.
15. Gjesvik, L., Schia, N. N. (2018). *Paper and Gjesvik. Managing a Digital Revolution Cyber Security Capacity Building in Myanmar.* Norway: Published by the Norwegian Institute of International Affairs.
16. Gorian, E. V. (2018). Singapore's Leadership on Cyber security in ASEAN:

Intermediate Results and Future Prospects.

17. Gupta, R., Khari, M., Shirivastava, G. (2018). Role of Cyber Security in Today`s Scenario, Available at: www.igi-global.com/chapter/role-of-cyber-security-in-todaysscenario/
18. Haddon, L. (2004). *Information and Communication Technologies in Everyday Life*. Berg Publishers, First Edition.
19. Hashim, M. S., Masrek, M. N., Yunos, Z. (2016). Elements in the Cyber Security Framework for Protecting the Critical Information Infrastructure against Cyber Threats. *International Information Institute (Tokyo). Information; Koganei*, 19(7), 2989-2994.
20. Hung, H. (2016). Confronting Cybersecurity Challenges through US- Singapore Partnership.
21. Iranian Students Newsletter. (2018). "Things to do after the Account is Hacked". IT News Service, At: https://iusnews.ir/fa/print/295896/ **(In Persian)**
22. Ismail, N. N. (2014). Greater Freedom in the Cyberspace? An Analysis of the Regulatory Regime of the Internet in Malaysia. South East Asia. *J. Contemp. Business, Econ. Law*, 5(4), 40–44.
23. Jayabalan, P., Ibrahim, R., Manaf, A. A. (2014). Understanding Cybercrime in Malaysia: An Overview. *Sains Humanika J*, 2(2), 109-115.
24. Kadis, M. R., Abdullah, A. (2017). A. Global and Local Clustering Soft Assignment for Intrusion Detection System: A Comparative Study. *Asia-Pacific J. Inf. Technol. Multimed,* 6(1), 30-38.
25. Kargar, A., Sistani, R., Patel, A. (2016). A. M. Design and Evaluation of a Virtual Private Network Architecture for Collaborating Specialist Users. *Asia-Pacific Journal of Information Technology and Multimedia,* 5(1): 15–30.
26. Katanchi, E., Pourgharmani, B. (2019). Symbolic Policies Council of Europe Cybercrime Treaty. *International Studies Journal (ISJ)*, 62(2), 31- 47. **(In Persian)**
27. Kazeruni, M. (2016). The Challenge of Implementing the Right to Freedom of Expression with the Prohibition of the Use of Cyberspace by Terrorism. *International Studies Journal (ISJ)*, 61 (4), 167-198. **(In Persian)**
28. Khanisa, -. (2013), a Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation. *Journal of ASEAN Studies*, 1(1), 41–53.

29. Kiankhah, E. (2010). *Information Security Management*, Tehran: Naghos Publications, First Edition. **(In Persian)**
30. Kiankhah, E., Alavi Vafa, S. (2011). The Concept of Cyber Security. *Proceedings of the First National Conference on Cyber Defense*, 1-8. **(In Persian)**
31. Koh, D. (2020). The Geopolitics of Cyber Security. At: https://thediplomat.com/2020/12/the-geopolitics-of-cybersecurity/
32. Malaysian Administrative Modernisation and Management Planning Unit. (2016). the Malaysian Public Sector ICT Strategic Plan. Malaysian Public Sect. ICT Strateg. Plan 2016-2020, August, 23.
33. Maung, T. M., Thwin, M. M. S. (2017). Proposed Applicable CCFIM Framework for Cybercrime Forensics Investigation in Myanmar. *15th Int. Conf. Computer*.
34. Maung, T. M., Thwin, M. M. S. (2017). Proposed Effective Solution for Cybercrime Investigation in Myanmar. *Int. J. Eng. Sci.,* 6(1), 01–07.
35. Mizan, N., Ma'arif, M., Mohd Satar, N., Shahar, S. (2019). CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries. *International Journal of Advanced Trends in Computer Science and Engineering,* 8(1), 113-119.
36. Noor, E. (2014). Securing ASEAN's Cyber Domain: Need for Partnership in Strategic Cyber Security. ***S. Rajaratnam Sch. Int. Stud. Singapore***, no. 236, 01–03.
37. Noor, E. (2015). Strategic Governance of Cyber Security: Implications for East Asia. Navigating Change: ASEAN-Japan Strategic Partnership in East Asia and in Global Governance*, Tokyo: Japan Center for International Exchange*.
38. Omar, S. A., Hasbolah, F. (2018). Awareness and Perception of Accounting Students towards Industrial Revolution 4.0. *in Proceedings of the 5th International Conference on Accounting Studies* (ICAS 2018) 16-17 October 2018, Penang, Malaysia.
39. Omar, S. A., Hasbolah, F., Zainudin, U. M. (2017). The Diffusion of Artificial Intelligence in Governance of Public Listed Companies in Malaysia. *Int. J. Business, Econ. Law*, 14(2), 1–9.
40. Ong, L., Chong, C. (2014). Information Security Awareness: An Application of Psychological Factors A Study in Malaysia. 2014 International Conference on Computer, Communications and Information Technology (CCIT 2014).
41. Quisumbing, L. A. (2017). Global Perspectives on Cyber Security Using Latent Dirichlet Allocation Algorithm. *Int. J. Appl. Eng. Res*., 12(20), 10310–10323.

42. Rahmawati, I. (2019). The Analysis Ofcyber Crime Threat Risk Management to Increase Cyber Defense. *J. Pertahanan Bela Negara*.
43. Razana, W. S. M. (2016). Cybersecurity: Towards Becoming A National Certification Body For Information Security Management Systems Internal Auditors. *Int. Sch. Sci. Res. Innov,* 10(8), 2907–2910.
44. Rizal, M., Yani, Y. (2017). Cyber Security Policy and Its Implementation in Indonesia. *Journal of ASEAN Studies,* 4(1), 61-78.
45. Rizki, A. M. (2018). Langkah Singapura Dalam Meningkatkan Kesadaran Negara Anggota Asean Untuk Meningkatan Keamanan Siber, Pros. Senas POLHI ke-1 Tahun 2018.
46. Salamzada, K., Shukur, Z., Abu Bakar, M. (2016). A Framework for Cybersecurity Strategy for Developing Countries: Case Study of Afghanistan. *Asia-Pacific J. Inf. Technol. Multimed*. 4, 1-10.
47. Soheili Najafabadi, S., Priests of Sir Ki, G., Qaedi, M., Simber, R. (2019). Study of Military Policies on the Security of the Persian Gulf Regions. *International Studies Journal (ISJ)*, 61 (1), 155- 182. **(In Persian)**
48. Staples, M., Niazi, M. (2007). Experiences Using Systematic Review Guidelines. *J. Syst. Softw*, at: https://doi.org/10.1016/j.jss.2006.09.046
49. Suhaiza S., Zawiyah M. Y. (2017). Public Sector ICT Strategic Planning: Framework of Monitoring and Evaluating Process. *Asia-Pacific J. Inf. Technol. Multimed*, 6(1), 85–99.
50. Sunkpho, J., Ramjan, S., Ottamakorn, C. (2018). Cybersecurity Policy in the ASEAN Countries. *Inf. Inst. Conf*, March.
51. Supayah, G., Ibrahim, J. (2017). An Overview of Cyber Security in Malaysia. *Kuwait Chapter Arab. J. Bus. Manag.* Rev, 6(4), 12–20. At: https://doi.org/10.12816/0036698
52. Teoh, C. S., Kamil Mahmood, A., Dzazali, S. (2018). Cyber Security Challenges in Organisations: A Case Study in Malaysia. 2018 4th Int. *Conf. Comput. Inf. Sci. Revolutionising Digit. Landsc. Sustain. Smart Soc. ICCOINS 2018 - Proc*., 1–6.
53. Wardana, A., Pedrason, R., Prasetyo, T. B., and Pertahanan, U. (2018), Implementasi Digital Forensik Brunei Darussalam Dalam Membangun Keamanan Siber Implementation of Digital Forensic Brunei Darussalam in Building Cyber Security. *Jurnal Prodi Perang Asimetris*, 4, 1–22.

54. Yuen, L. C. (2019). Strengthening Cybersecurity in Singapore: Challenges, Responses, and the Way Forward. *In Security Frame works in Contemporary Electronic Government*, 96-128. IGI Global, 2019. At: https://doi.org/10.4018/978-1-5225-5984-9.ch005
55. Yunos, Z., Ahmad, R., Mohd Sabri, N. A. (2015). a Qualitative Analysis for Evaluating a Cyber Terrorism Frame work in Malaysia Inf. *Security Journal*, 24(1–3), 15–23. At: https://doi.org/10.1080/19393555.2014.998844
56. Raska, M. (2018). Cyber Security in Southeast Asia. Note d'introduction à la table ronde du 22 Mai, 1-9.