مجله علمی پژوهش در حقوق، فقه، فلسفه و الهیات ، شماره ۱۶ ، تابستان ۱۳۹۸جلد۲، ص ۱۵-۸
http://www.jrse.ir

انقلاب سایبری و امنیت منطقه‌ای

مجله علمی پژوهش در حقوق، فقه، فلسفه و الهیات (سال پنجم)
شماره ۱۶ / تابستان ۱۳۹۸ / ص ۱۵-۸

لیلا باجلان[۱]
[۱]دانش آموخته کارشناسی ارشد حقوق بین الملل دانشگاه مفید قم.

نویسنده مسئول:
لیلا باجلان

چکیده
امنیت یکی از دغدغه‌های اصلی بشر از ابتدای زندگی تاکنون بوده است. امروزه با گسترش اینترنت و کاربرد آن و خدمات متعدد و عمدتاً رایگان آن در میان کشورها، مؤسسات و افراد، گرایش‌های روزافزون مردم به استفاده از این خدمات را در زندگی پررنگ‌تر کرده است. به‌طوری‌که بخش گسترده‌ای از کشورهای خاورمیانه بر فناوری اطلاعات‌پایه‌گذاری شده‌اند و تمامی بخش‌های مالی، دولتی، مدارس، بیمارستان‌ها، به‌صورت برگشت‌ناپذیر وابسته به اینترنت شده‌اند. بنابراین لزوم امنیت در فعالیت‌های مجازی در این منطقه بیش‌ازپیش احساس می‌شود. اما ایجاد ترس و اختلال و تخریب شبکه و نداشتن امنیت روانی و فرهنگی و هجوم اطلاعات آلوده و مخرب از طریق اینترنت و فضاهای مجازی با واکنشی‌هایی روبرو است. و هر نوع اطلاعات مخرب سلامت و امنیت کشورها را به خطر می‌اندازد. ازاین‌رو به‌کارگیری ابزارها و روش‌های مختلف فنی و حقوقی جهت پیشگیری از نفوذ اطلاعات مخرب و گزینش اطلاعات سالم رو به افزایش است. در مقاله حاضر با عناوینی چون چالش‌های امنیت سایبری در خاورمیانه، همکاری و تعهدات دولت‌های منطقه در مدیریت این بحران آشنا خواهیم شد و به این سوالات پاسخ خواهیم داد که آیا همکاری‌های ملی و منطقه‌ای در جهت مقابله با آن انجام‌شده است؟ در پاسخ به سؤالات فوق، این فرضیه مطرح می‌شود که فضای سایبری تأثیر انقلابی و بنیادین در امنیت کشورهای خاورمیانه داشته است به‌طوری‌که استفاده از جاسوسی سایبری، نشان‌گر تأثیر درمیان کشورهای خاورمیانه است. از سوی دیگر تهدیدات سایبری در منطقه رو به افزایش است و دلیل آن این است که خاورمیانه نظام پیشرفته و دانش فنی و حقوقی در مبارزه با آن را ندارد . از سویی دیگر با رایگان شدن خدمات اینترنت هیچ‌گونه قانونی وجود ندارد که سرویس‌دهندگان را ملزم به کنترل محتوا نماید، بنابراین نیاز به همکاری بیشتر بازیگران دولتی برای مبارزه با این چالش‌ها در منطقه احساس می‌شود.

کلمات کلیدی: انقلاب سایبری، امنیت خاورمیانه،چالش‌های امنیت، همکاری‌های بین‌المللی

مقدمه

امنیت، نبود تهدید روانی و جسمی برای جامعه است. که خواست همسان انسان‌ها و حیوانات در همه زمان‌ها و مکان‌ها بوده است. در معنای امروزی از امنیت اشیا و موجودات بی‌جان مانند امنیت شبکه، امنیت فضای سایبری، سخن به میان می‌آید. ازآنجایی‌که تمامی بخش‌های دولتی و خصوصی خاورمیانه به اینترنت وابسته است. امنیت فضای سایبری در این منطقه بیش از پیش احساس می‌شود. . فضای سایبری تأثیر بنیادینی را در امنیت کشورهای خاورمیانه داشته است به‌طوری‌که استفاده از جاسوسی سایبری، جرائم سایبری نشان‌گر تأثیر درمیان کشورهای خاورمیانه است. از سوی دیگر تهدیدات سایبری در منطقه رو به افزایش است و دلیل آن این است که خاورمیانه نظام پیشرفته و دانش فنی و حقوقی در مبارزه با آن را ندارد . از سویی دیگر با رایگان شدن خدمات اینترنت هیچ‌گونه قانونی وجود ندارد که سرویس‌دهندگان را ملزم به کنترل محتوا نماید، بنابراین نیاز به همکاری بیشتر کشورهای خاورمیانه احساس می‌شود. درجهیت ایجاد و افزایش امنیت سایبری تاکنون همکاری‌هایی میان کشورهای خاورمیانه مانند ایران و قطر ،ایران و تایلند ، ایران و آذربایجان در زمینه امنیت فضای سایبری منعقدشده است. تا به همکاری یکدیگر امنیت فضای سایبری را توسعه دهند.

مبحث اول: چالش‌های امنیت سایبری در خاورمیانه

فضای سایبری تأثیر انقلابی و بنیادین در امنیت کشورهای خاورمیانه داشته است که موجب ایجاد چالش هایی در این منطقه شده است. به برخی از مهمترین چالش ها در ادامه خواهیم پرداخت.

گفتار اول: آسیب‌های اقتصادی

ارتقای امنیت سایبر در بخش اقتصادی و حفظ تجارت دیجیتال از گزند حوادث سایبری، از مسائلی هستند که دولت‌های خاورمیانه سعی می‌کنند در راهبردهای سایبری خود به آن‌ها توجه کنند.

بند اول: بانک‌ها و نهادهای پولی

فضای سایبری امکانات و ظرفیت های بالایی را به صورت های مختلف در اختیار افراد، شرکت های دولتی و خصوصی و سازمان ها قرار داده است تا بتوانند از آن ها در جهت دستیابی به مقاصد اقتصادی خود بهرهمند شوند . اما در کنار جنبه های مثبت جنبه های منفی برای افراد در زمینه های اقتصادی ایجاد کرده است از جمله این که گزارشی که در سال ۲۰۱۴ تهیه شده است حاکی از آن است که جرائم اقتصادی حدود ۴۰۰ میلیارد دلار در سال هزینه در بر داشته است. (Intel Security and Centre for Strategic and International Studies, 2016) علاوه بر این گزارش‌های اخیر حمله به بانک‌ها در منطقه حملات سایبری را در هر دو طرف اقتصاد منطقه‌ای و جهانی اثبات کرده است.در ماه دسامبر ۲۰۱۲ و فوریه ۲۰۱۳ بانک RAKدر امارات متحده عربی و بانک BMI در عمان توسط باند بین‌المللی سایبری مورد هدف قرارگرفته است. جنایات کاران توانستند سیستم‌های پردازش را هک کنند و محدودیت‌های موجود و را افزاش دهند. آن‌ها هم‌چنین کارت‌ها را مسدود کردند و توانستند حدود ۴۵ میلیون دلار از ۲۷ کشور خارج سازند.(A. Blom et al,2013) و گروه‌های باند را در سراسر جهان افزایش دادند.بانک‌های خاورمیانه در پیاده‌سازی امنیت اطلاعات فناوری و اقدامات تأخیر داشته‌اند و مؤسسات مالی برای بهبود سیاست‌ها و تکنیک‌ها برای اجرای استانداردهای بین‌المللی این اقدامات امنیتی را افزایش داده اند. (El-Guindy, Middle East Cyber Security Threat Report 2014)

بند دوم: لوکس گرایی

فضای سایبر دارای شرایطی است که می‌توان در آن‌ها کالاها و چیزهای لوکس نگران قیمت را به‌صورت مختلف به نمایش و عرضه به دیگران قرارداد و از این امکان در راستای توسعه فرهنگ تجمل‌گرایی در جوامع مختلف در بین جوانان و نوجوانان به‌ویژه در جوامع جهان سوم بهره برد و آن را به‌صورت فرهنگ در بین افراد تبدیل و از این طریق به منافع اقتصادی گسترده‌ای دست یابد .وجود این نگرش‌ها و استفاده‌های اقتصادی از فضای سایبر سبب آسیب‌های اقتصادی متعددی در جوامع می‌شود و ضرر و زیان‌های متعددی را به اقتصاد خانواده و جامعه وارد می‌کند و امنیت اجتماعی را دچار چالش می‌کند.

بند سوم: مسئولیت فردی و آگاهی و دسترسی به اینترنت

امنیت سایبری امنیت ملیتی نیست. بلکه مسئله شخصی است و به‌منظور بهبود آن اولین گام این است که افراد برای بهبود و مسئولیت‌پذیری آن تشویق شوند. شهروندان نیز در صورت نیاز باید قابلیت‌های سایبری و فعالان اجتماعی را افزایش دهند . این مسائل را می‌توان به‌طور مؤثر

با ایجاد برنامه‌های آموزشی برای کمک شهروندانِ کشورهای درحال‌توسعه، جهت غلبه بر شکاف دیجیتالی دانست و افزایش امنیت اطلاعات رادر برنامه‌های درسی همه سیستم‌های آموزشی در تمام سطوح منطقه‌ای گنجاند. کشورها برای کمک به مقابله با مشکل عدم دسترسی به اینترنت باید سرمایه‌گذاری کنند و به عموم مردم اجازه دهند تا به اینترنت دسترسی داشته باشند. دسترسی به اینترنت باید در مدارس، کتابخانه‌ها، و سایر ادارات دولتی فراگیر شود. (Ibid.)

بند سوم: توان بخشی و آموزش و اشتراک دانش

چندین کمپین در کشورهای عمان ، عربستان سعودی، قطر و امارات متحده عربی وجود دارد که مسئول آموزش در مقابله با تهدیدات جرائم اینترنتی هستند(M.N. El-Guindy) زمانی که بحث امنیت اطلاعات می‌شود کارمندان اولین خط دفاعی هستند. بنابراین آموزش امنیت فناوری اطلاعات بخشی از فرایند آموزش کارکنان جدید خواهد بود که این آموزش باید به صورت مرتب انجام پذیرد. هم‌چنین کارمندان می‌بایست ، با تکنیک‌های مهندسی اجتماعی آگاهی داشته باشند . ایمیل های کلاهبرداری به راحتی کاربران اجتماعی را فریب می دهند تا فایل های ضمیمه را باز کنند که ظاهراً بی خطر هستندو از سوی کاربران شناخته شده ارسال شده اند. خسارات ناشی از این حملات می‌تواند ویران کننده باشد . بنابراین جهت در امان ماندن از این گونه خطرات آموزش لازم است.

بند چهارم : جاسوسی سایبری

جاسوسی سایبری یا هنر یا تکنیک کسب اطلاعاتِ سری بدون مجوز گرفتن از نگهدارنده اطلاعات (شخصی ، حساس، طبقه بندی شده) است. جاسوسی مانند پولشویی فرایندی است که به صورت گام به گام به وجود می آیند. در واقع جاسوسی سایبری در سه مرحله اتفاق می افتد. مرحله اول دسترسی به مکانی است که اطلاعات طبقه بندی شده درآن جای گرفته اند. مرحله دوم دست یابی به اطلاعات. و مرحله سوم افشا اطلاعات طبقه بندی شده برای دشمن یا دولتی که صلاحیت دسترسی به آن اطلاعات را ندارند. افشا اطلاعات چهره همگانی دارد و مرتکب محتوای اطلاعات را نسبت به همه بازگو می کند و چون دولت ها یا گروه های بیگانه بیش از هر شخص دیگری در پی اطلاعات هستند ، افشا اطلاعات به آن ها خطرناک است. (عالی پور، حسن، صص۱۵-۳۴۹)

گفتار دوم: عملیات امنیت سایبری در خاورمیانه

هر کشوری در خاورمیانه تلاش می‌کند که خود را برای حملات سایبری آماده کند و حتی برخی از کشورها ابزارهای پیشگیرانه دفاعی را برای حملات سایبری ایجادِ کرده‌اند.

بند اول: نظارت بازی گران غیردولتی بر سایبر

بسیاری از کشورهای خاورمیانه دارای برنامه‌هایی برای نظارت بر سایبر هستند که در مراحل اولیه توسعه آن هستند مثلاً گزارش یک گروه سایبری از مصر ادعا می‌کند که، به تبلیغات آنلاین تروریست‌ها حمله کرده و هدف از آن دفاع از زیرساخت‌های بحرانی مصر بوده است [11] . (J. Vaentino-Deveries and D. Yadron.October 2015,) یکی دیگر از راه‌های سایبری که برای دفاع از دولت ایجادشده است ارتش الکترونیکی سوریه می‌باشد. SEA پس‌ازآن که را جنگ داخلی در سوریه آغازشده این گروه دارای هکرهای اینترنتی بودند که از رژیم پشتیبانی می‌کردند آن‌ها به‌طور خاص گروه‌های مخالف را مورد هدف قراردادند و با استفاده از حملات مانند انکار و اطلاعات و همچنین سیاست‌ها و تغیر محتوا این گروه هر دو هدف را با موفقیت مورد هدف قرار دارند. و با استفاده از حملاتی مانند انکار خدمات و اطلاعات و هم‌چنین قطع وب‌سایت‌ها و تغییرمحتوا.

این گروه‌ها هر دو هدف گروه‌های مخالف سوریه و وب‌سایت‌های جهانی را مورد هدف قراردادند. این سازمان توانست بیش از ۱۲۰ وب‌سایت را هک نماید وب‌سایت‌هایی که از تایمز [۲] "تلگراف" و "واشنگتن‌پست" و" العربیه " استفاده می‌کنند.(Sibioni et al)

شاید مؤثرترین حمله زمانی بود که SEA از حملات کاربری [۳]شکست خورد و نوشت که کاخ سفید بمباران‌شده است و ایالات‌متحده نوشت که رئیس‌جمهور در این حمله مجروح شده است و این موجب افت شدید بازارهای مالی ایالات‌متحده شد. (P. Foster, 23 April 2013)

هم‌چنین در سال ۲۰۱۰ اسرائیل برای دفاع از امنیت سایبری، دفتر ملی سایبری را تأسیس کرده است که مسئول جمع‌آوری اطلاعات و رمزگشایی کدها می باشد. (UN Institute for Disarmament Research, 2013-en-463.pdf)علاوه بر اسرائیل ، ارتش در سال ۲۰۱۳ برنامه ملی امنیت

[2] . FINANCIAL TIMES
[3] . ASSOICATED PRESS

سایبری را برای تحقیقات خلع سلاح مورد تجزیه‌وتحلیل قرارداد و در سراسر جهان متوجه شدیم که ۱۱۴ برنامه وجود دارد که ۴۷ مورد آن مربوط به ارتش است. کشور ایران نیز (UNIDIR, "UNIDIR Cyber Stability Seminar 2015) برنامه‌ریزی سایبری خود را از طریق سپاه پاسداران تأسیس کرده که حدود یک میلیارد دلار هزینه در برداشته است. این برنامه توسط سپاه پاسداران اداره می‌شود و یک هسته اینترنت دارد که کاربران اینترنت را استخدام می‌کند. ایران تحت‌فشار است تا برنامه سایبری قوی‌تری را ایجاد نماید. هرچند که تحت تأثیر تحریم‌های بین‌المللی قرارگرفته است در مقابل برنامه سایبر آمریکا، اسرائیل، چین، روسیه، بریتانیا، در حال پیشرفت است.

بنددوم: قانون‌گذاری سایبری[۴]

قانون‌گذاری بخش درست و صحیح در مقابله با تهدید جهانی سایبری است. مقنن در کشورهای خاورمیانه در زمان انعقاد قانون با معیارهایی که شامل قوانین جنایی، قضایی و مدنی هستند روبرو می‌شوند .که با تنظیم قوانین جهت مبارزه با جرائم سایبری مفید هستند. قانون‌گذاری در خاورمیانه اغلب در مراحل اولیه و یا درحال‌توسعه می‌باشد. اردن ، عمان، عربستان امارات متحده عربی با معرفی نظام‌های خاص از قانون جرائم سایبری انتقاداتی نموده‌اند.(El-Guindy, Cybercrime Challenges in the Middle East) ایالات‌متحده عربی در سال ۲۰۱۲در مبارزه با جرائم سایبری لایحه حکم فدرال شماره ۵[۵] را تصویب کرد طبق این قانون «اگر فردی از شبکه‌های اجتماعی یا سیستم الکترونیکی به مقام با شأن شخص دیگر توهین نماید به شش ماه حبس یا جریمه نقد محکوم خواهد شد.»،(UAE (United Arab Emirates, 2012)) عربستان صعودی نیز در سال ۲۰۰۷ توسط حکم سلطنتی به تصویب رساند. هدف آن مبارزه با جرائم سایبری از طریق شناسایی جرائم و تعیین مجازات برای محافظت از اطلاعات امنیتی و حفاظت از اطلاعات رایانه ا و شبکه‌ای ، حفاظت از منافع عمومی ، حفاظت از اقتصاد ملی است(M.A. Saeed,2015)

علاوه بر این وزارت امور خارجه و کمیسیون فناوری و اطلاعات می‌توانند تشدید مجازات را در جرائمی مانند سرقت هویت[۶]، افترا، سرقت الکتریکی، و دیگر اعمال غیرقانونی تعیین کنند. هم‌چنین عمال در سال ۲۰۱۱ قانون مبارزه با جرائم سایبری را تصویب کرده است. این قانون جرائم سایبری را شناسایی کرده و مجازات‌هایی ازجمله جرائم نقدی و یا در صورت تشدید زندان را تعیین کرده است. (Oman,2011)

مبحث دوم: راحل های چند جانبه در امنیت سایبری

گفتار اول: توسعه ظرفیت[۷]

برنامه امنیت سایبری باید قابلیت‌های پیشگیرانه را داشته باشد. دولت‌ها باید توانایی‌های بالایی را برای حل این تهدید داشته باشند. برای مثال استانداردهای تضمین اطلاعات را افزایش داده و ریسک‌های مربوط به سایبر را کاهش دهند. به طوری که ترویج امنیت سایبری به‌عنوان جزئی از فعالیت‌ها و تصمیم‌گیری‌های دولت‌ها در بخش خصوصی و عمومی‌باشد. [۸] یکی از راه‌حل‌های ارتقا توسعه ظرفیت یا ظرفیت‌سازی استفاده از برنامه‌های آموزشی است این مهم است که در خاورمیانه وکلا، قضات با اجرای قوانین مربوط به فضای مجازی ، فناوری اطلاعات و ارتباطات و جنایات سایبری زمینه پیشرفت بین‌المللی را افزایش دهند(S. Aboul-Enein,2015)

گسترش مسئله امنیت سایبری پیش‌شرط انعطاف‌پذیری است که می‌تواند با تهدید جهانی سایبری روبرو شود. آموزش امنیت سایبری می‌تواند از طریق دوره‌های آموزشی در سطح اجرایی از طریق دانشگاه‌ها صورت بگیرد. علاوه بر این کنفرانس‌های سازمان تجارت و سازمان ملل می‌تواند در بهبود این وضعیت سهیم باشند.

---

[4] . legislation

[5] . The UAE's Federal Decree Law no. 5,

[۶] . **سرقت هویت**(Identity theft) در حالی که استفاده از یک نام مستعار لزوماً غیرقانونی نیست، سرقت هویت استفادهٔ عمدی از هویت شخص دیگری‌است، و معمولاً به عنوان روشی برای به دست آوردن سود مالی و یا برخورداری از اعتبار و مزایای دیگر، به نام شخصی دیگر صورت می‌گیرد،

[7] . Capacity-building

[8] . Tohme et al., Cyber Security in the Middle East.

گفتار دوم: قانون‌گذاری

استفاده از اجبار در زمینه امنیت فناوری اطلاعات و ارتباطات[۹] به تمام لایه‌های ایالتی چه فیزیکی و چه دیجیتالی آسیب وارد می‌کند. [۱۰] برای مقابله با این تهدید چارچوب قانونی برای تقویت پروتکل‌های امنیت سایبری در سطح ملی در کشورهای خاورمیانه درحال‌توسعه است که باید با قوانین بین‌المللی بشردوستانه منطبق باشند. به‌خصوص در زمان درگیری(S. Aboul-Enein, 2016)منشور سازمان ملل متحد، قوانین مربوط به مخاصمات مسلحانه که در کنوانسیون ژنو گردآوری‌شده است. و کنوانسیون شورای اروپایی چارچوبی کلی برای کمک به ملت‌ها در توسعه قوانین مربوط به امنیت سایبری هستند. کشورهای خاورمیانه باید در استفاده از فناوری اطلاعات تعهدات خود را طبق ماده ۲ منشور سازمان ملل متحد عمل نمایند و اختلافات بین‌المللی خود را طبق ماده دو برطرف نمایند و از تهدید یا زور و اجبار جلوگیری نمایند.

گفتار سوم:مقررات انتقال اطلاعات

چگونگی انتقال اطلاعات بین‌المللی را بیان می‌کند که مربوط به دسترسی، ذخیره و پردازش حجم زیادی از اطلاعات از جهان است (GCIC (Global Commission on Internet Governance)2016), ازآنجایی‌که انتقال این اطلاعات از اهمیت بالایی برخوردار است، بنابراین انتقال آن به مقصد می‌بایست صورت خصوصی صورت بگیرد .زیرا بیشترین نقض امنیت شهروندان در آشکارسازی اطلاعات شخصی آنان است. بنابراین هرگونه خطا و اشتباه درروند انتقال داده‌ها تأثیر منفی بر امنیت آن‌ها خواهد گذاشت.(A. Ünver and G. Kim, 2016) بااین‌حال شهروندان عادی می‌دانند که می‌بایست از اطلاعات شخصی محافظت گردد. به گفته شریف هاشم معاون امنیت سایبری در شرکت National Telecom " مقامات نظارتی در مصر به افراد، اقداماتی را جهت آموزش حفاظت از اطلاعات را ارائه می‌دهند و هم‌چنین چگونگی دسترسی به اطلاعات را به آن‌ها آموزش می‌دهند تا هر کس به این اطلاعات دسترسی پیدا نکند حتی اگر نقش تعدیل‌کننده و امنیت اشخاص را داشته باشد ". هم‌چنین وی تأکید می‌کند که آشکارسازی اطلاعات نه‌تنها امنیت افراد را در معرض خطر قرار می‌دهد بلکه دارای پیامدهای اقتصادی و مالی فراوانی است. و ممکن است ماه طول بکشد تا به مقابله آن پرداخت(S. Hashem, International Telecommunications Union, 2016)

بنابراین اقدامات احتمالی برای تقویت امنیت شامل اعتماد از رمزگذاری و استفاده از رمزهای چند منظور برای اطمینان از امنیت اطلاعات شخصی و حساس است. علاوه بر این‌ها بر عملکرد اقتصاد ملی نیز اشکالاتی را در این زمینه ایجاد کرده است. (Intel Security and Centre for Strategic and International Studies, Net Losses).

اکثر کشورهای خاورمیانه و شمال آفریقا در رتبه‌بندی جنایات مالی بین‌المللی قرار دارند آمار نشان می‌دهد که حدود ۲۶ درصد از تجارت منطقه، قربانیِ جرائم اقتصادی شده‌اند. ۳۰ درصد آمار اعتقاددارند که جرائم سایبری دومین جرم اقتصادی است که به عملکرد سازمان‌ها تأثیر می‌گذارد. و ۶۳ درصد آمار نشان می‌دهد که جنایت‌کاران اصلی جنایت‌کاران اصلی جرائم سایبری اقتصادی را از شرکت‌های منطقه‌ای آغاز کرده پس به نقص شبکه‌های اینترنتی پرداخته‌اند. اما مجرمان سایبری تاکتیک‌های حملات را تغییر داده‌اند تا از شناسایی آن‌ها خودداری شود. و هم چنان به سرقت اطلاعات بپردازند. تحقیق انجام‌شده توسط pwC در سال ۲۰۱۶ نشان داده است که $\frac{1}{4}$ کسانی که مورد حملات سایبری قرارگرفته‌اند معتقد بوده‌اند که هیچ‌گونه زیان و ضرر مالی نداشته‌اند. بااین‌حال که ۴۲ درصد از این افراد معتقد بوده‌اند که حملات سایبری خسارات فراوانی به شهرت آن‌ها وارد کرده است. استفاده از ابزارهای پیشگیری و تشخیص جرائم می‌تواند تا حدودی فرصت‌های جرائم اقتصادی را کاهش دهد (www.pwc.com/m1/en/publications/documents/economic-crime-in-the-arabworld-2016.pdf)سازمان‌هایی که مبنی بر فرهنگ و ارزش‌های مشترک هستند از طریق ایجاد برنامه اخلاقی و انطباق آن با تصمیم‌گیری‌های روزمره می‌توانند جرائم اقتصادی را کاهش دهند.

گفتار چهارم: طرح‌های نظارتی بر حملات سایبری

درنتیجه افزایش حملات سایبری، کشورهای خاورمیانه روش‌ها و رویه‌هایی را جهت ایجاد امنیت سایبری به‌کاربرده‌اند. نگرانی عمده‌ای که در میان سازمان‌های منطقه‌ای و شرکت‌های نفت و گاز وجود دارد تعیین و به‌کارگیری تکنیک‌ها سیاست‌ها و شیوه‌هایی جهت افزایش توانایی‌های امنیت سایبری است که آن‌ها را تقویت نمایند. بسیاری از کشورهای خاورمیانه قابلیت امنیت سایبری را برای اطمینان از امنیت

---

[9] . Information and Communications Technology (ICT).
[10] . Aboul-Enein, “Input Paper”.

ملی خود بهبود ، و اطلاعات درخواست امنیت در منطقه را افزایش داده‌اند.عواملی مانند حفاظت از اطلاعات، یکپارچه‌سازی اطلاعات ازجمله عوامل تقاضا جهت افزایش امنیت سایبری در خاورمیانه هستند.

برخی از کشورها ازجمله امارات، مراکش، عمان، قوانین جدیدی در جهت حمایت از حملات الکترونیک و جرائم سایبری ایجاد کرده‌اند هم‌چنین در سازمان‌ها و در ادارات سیاست‌های حمایت از زیرساخت‌های اطلاعاتی و برنامه‌های امنیتی تأسیس‌شده است. علاوه بر این کشورهای دیگر مانند اردن، الجزیره، عربستان، رویه‌ها و شیوه‌هایی جهت افزایش آگاهی و توانایی در امنیت سایبری ایجادشده است.

گفتار پنجم: همکاری‌های دوجانبه کشورهای خاورمیانه بر امنیت سایبری

همکاری‌های دوجانبه به پیمان‌های همکاری کشورهای خاورمیانه در زمینه برنامه‌های گوناگون ازجمله پیکار با انقلاب سایبری اشاره دارد. به جهت چهره جهانی بزه‌های سایبری ، کشورهای خاورمیانه برای رسیدن به امنیت سایبری می‌بایست با یکدیگر پیمان‌نامه‌های دوجانبه برای همکاری‌های امنیتی و حقوقی پدیدآورند تا سیاست‌های هم سویی برای امنیت سایبری را افزایش دهند. برای نمونه همکاری‌های دوجانبه کشورهای خاورمیانه در زمینه امنیت سایبری می‌توان به همکاری امنیتی میان دولت ایران و دولت قطر مصوب ۱۳۸۹/۱۰/۱ اشاره کرد. هم‌چنین به همکاری‌های ایران و کشور آذربایجان در زمینه حفاظت از شبکه‌ها و زیرساخت‌های اطلاعاتی و تبادل دیتا و اطلاعات در مقابل حمله‌ها و خطرات سایبری با یکدیگر اشاره کرد.

نتیجه‌گیری

یافته‌های تحقیق حاضر نشان می دهد که یکی از تهدیدهای اصلی این کشورها نبود امنیت در فضای سایبری است که موجب به خطر افتادن امنیت کشورهای خاورمیانه شده است. امنیت سایبری یکی از دسته‌بندی‌های امنیت بر فضای سایبری است که بر امنیت اطلاعات اشاره دارد و تا زمانی که امنیت اطلاعات تهدید نشوند ، امنیت ملی تهدید نمی‌شود. بنابراین برای جلوگیری از تهدید اطلاعات پیشنهاد می‌شود که نهادهای دولتی دسترسی به وب‌سایت‌های مستهجن را مسدود یا کنترل نمایند. هم‌چنین برای جلوگیری از این کار همکاری‌هایی در سطح ملی و منطقه‌ای میان کشورهای خاورمیانه رخداده است در سطح ملی می‌توان به همکاری‌های تمامی دستگاه‌های ملی و دولتی جهت ایجاد امنیت فضای سایبری اشاره کرد، هم‌چنین توسعه آموزش و اطلاعات آموزش دادن به کارمندان و دانشجویان در جهت مقابله با جرائم سایبری را می‌تواند اشاره کرد. در سطح منطقه‌ای نیز تاکنون کشورهای خاورمیانه موافقت‌نامه‌های همکاری میان خود جهت توسعه امنیت سایبری منعقد کرده‌اند تا سیاست‌ها و تکنیک‌های افزایش امنیت فضای سایبری را در منطقه گسترش دهند.

منابع

۱. علی پور، حسن، امنیت سایبری در چشم انداز۱۴۰۴ ، چالش ها و راهکارهای حقوقی رویارویی با بزه های امنیتی سایبری، مجموعه مقالات نخستین همایش ملی دفاع سایبری،

2. A. Blom et al., Cyber Security and Data Protection in the Middle East, Financier Worldwide, November 2013, https://www.financierworldwide.com/cyber-security-and-data-protection-in-the-middle-east/
3. A. Ünver and G. Kim, “Cross-border Data Transfers and Data Localization”, EDAM Cyber Policy Paper Series no. 2016/3, 2016, http://www.edam.org.tr/en/File?id=3192.
4. El-Guindy, Cybercrime Challenges in the Middle East.
5. El-Guindy, Middle East Cyber Security Threat Report 2014
6. GCIC (Global Commission on Internet Governance), One Internet, Centre for International Governance Innovation and Chatham House, 2016, https://www. chathamhouse.org/sites/files/chathamhouse/publications/research/2016-06-21-global-commission-internet-governance.pdf
7. Intel Security and Centre for Strategic and International Studies, Net Losses.
8. Intel Security and Centre for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime, 2014, https://www.mcafee.com/us/resources/reports/ rp-economic-impact-cybercrime2.pdf
9. J. Tebbs, Adjusting the Lens on the Economic Crime in the Arab World, PwC, 2016, http://www.pwc.com/m1/en/publications/documents/economic-crime-in-the-arab-world-2016.pdf
10. J. Vaentino-Deveries and D. Yadron, “Cataloging the World’s Cyberforces”, Wall Street Journal, 11 October 2015, https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710.
11. M.A. Saeed, “Cyber Security and Data Privacy Law in Saudi Arabia”, Financier Worldwide, April 2015, http://www.financierworldwide.com/cyber-security-and-data-privacy-law-in-saudi-arabia/#.V2buhed950s
12. M.N. El-Guindy, Cybercrime Challenges in the Middle East, 13 October 2012, http:// www.issa-eg.org/res/Cyber-Sec-Energy-Cybercrime-elguindy.pdf
13. M.N. El-Guindy, Middle East Cyber Security Threat Report 2014, December 2013, http://www.academia.edu/5522905/Middle_East_Cyber_Security_Threat_Report_2014
14. Oman, Issuing the Cybercrime Law, Royal Decree no. 12, 2011.
15. P. Foster, “‘Bogus’ AP Tweet about Explosion at the White House Wipes Billions off US Markets”, The Telegraph, 23 April 2013, http://www.telegraph.co.uk/finance/ markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.
16. S. Aboul-Enein, “Input Paper for the Work of the Group of Governmental Experts”, Proceedings of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 26 July 2015, http://www.gcsp.ch/News-Knowledge/Experts/Fellows/Aboul-Enein-Amb.-Dr- Sameh-Aboul-Enein/Selected-publications.
17. S. Hashem, International Telecommunications Union (ITU) Interviews at the Global Symposium for Regulators 2016 (GSR16), 2016, https://www.youtube.com/ watch?v=eftNdYsa0iE.
18. S. Hashem, International Telecommunications Union (ITU) Interviews at the Global Symposium for Regulators 2016 (GSR16), 2016, https://www.youtube.com/ watch?v=eftNdYsa0iE.
19. Sibioni et al., “The Threat of Terrorist Organizations in Cyber Space”.
20. UAE (United Arab Emirates), On Combating Cybercrimes: Federal Decree-Law no. 5 of 2012.
21. UNIDIR (UN Institute for Disarmament Research), “The Cyber Index: International Security Trends and Realities”, 2013, http://www.unidir.org/files/publications/pdfs/ cyber-index-2013-en-463.pdf
22. UNIDIR, “UNIDIR Cyber Stability Seminar 2015: Regime Coherence”, http://www.unidir. org/programmes/emerging-security-issues/annual-cyber-stability-conference/cyber-stability-seminar-2015-regime-coherence.