فصلنامه دستاوردهای نوین در حقوق عمومی، سال سوم، شماره نهم، بهار ۱۴۰۳

کارکرد سازمان های منطقه ای در جنگ های سایبری

تاج محمد صادقی[۱]، لیلا رئیسی[۲]، علی رضا انصاری مهیاری[۳]

تاریخ دریافت: ۱۴۰۲/۰۸/۱۵ تاریخ پذیرش: ۱۴۰۲/۰۷/۱۰

چکیده

با گسترش فضای سایبری، عرصه جدیدی از تهدیدات برای دولت ها در قالب تهدیدات سایبری ایجاد شده است و جنبه های مختلف امنیت ملی از جمله امنیت اجتماعی، اقتصادی، نظامی و سیاسی را تحت تأثیر خود قرارداده است. امنیت بین المللی و منطقه ای را تحت تاثیر قرارداده که راه حل های لازم را برای حداقل رساندن خسارات ناشی از این نوع تهدیدات و حفظ امنیت بین المللی می طلبد. مقاله حاضر با استفاده از روش توصیفی –تحلیلی به بررسی نقش سازمان های منطقه ای در پیشگیری از حملات سایبری می پردازد. فرضیه مطرح شده در این پژوهش آن است که از آنجاییکه دولت ها به طور فزاینده ای به سیاست ها و ابتکارات یکجانبه برای مقابله با تهدیدات سایبری متمرکز شده اند سازمان های منطقه ای باید نقش فعالی در شکل دادن به همکاری میان اعضا در قالب رویکردهای متمرکز بر همکاری بین المللی و منطقه ای در زمینه امنیت سایبری و پیشگیری از تهدیدات سایبری و توسعه سیستم امنیت سایبری جهانی ایفا کنند. یافته های تحقیق نشان می دهد که سازمان های منطقه ای نظیر ناتو، اتحادیه اروپا، شانگهای، آسه آن، سازمان امنیت و همکاری اروپا و سازمان کشورهای امریکایی اقداماتی در کاهش خسارات ناشی از جرایم سایبری و مقابله با حملات سایبری انجام داده اند از جمله به دانش افزایی و وضع قوانین سایبری، همکاری منطقه ای، اشتراک گزاری اطلاعات، تقویت زیرساخت ها و اعتماد سازی مبادرت نموده اند.

واژگان کلیدی: حملات سایبری، چالشها، سازمان های منطقه ای ،فرصتها

[۱] . دانشجو دکتری حقوق بین الملل، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

[۲]. دانشیار، گروه حقوق، واحد اصفهان(خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران(نویسنده مسئول)
raisi.Leila.@Gmail.com

[۳]. استادیار، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

۱- مقدمه

موضوع تهدیدات سایبری نه تنها در سطوح کشورها بلکه گریبان سازمان ها و نهاد های منطقه ای را هم گرفته است بطوریکه با افزایش حملات سایبری، سازمان های بین المللی به شیوه ای مختلفی اقدام به مقابله با آن گرفته اند. مقیاس و ماهیت فرامرزی تهدیدات سایبری به گونه‌ای است که همکاری بین‌المللی را می طلبد، زیرا تهدیدات عمده اغلب بر چندین حوزه قضایی به طور همزمان تأثیر میگذارند و به سرعت در شبکه ها و سیستم های رایانه‌ای منتشر می‌شوند. به عنوان مثال، حمله باج افزار WannaCry در سال ۲۰۱۷ که تنها در چند روز در ۱۵۰ کشور گسترش یافت و ۲۳۰۰۰۰ رایانه را تحت تأثیر قرار داد و حدود ۴ میلیارد دلار خسارت در سرا سر جهان ایجاد کرد. این پیچیدگی ها با مشکلات مربوط به انتساب و دسترسی قضایی تشدید می شوند. امنیت سایبری یک چالش مشترک اجتماعی است که نیازمند مشارکت همه لایه های دولت، اقتصاد و جامعه به ویژه بخش خصوصی است این لایه ها شامل سازمان های منطقه ای که به عنوان انجمن های بین المللی که به لحاظ جغرافیایی و ایدئولوژیکی به هم مرتبط هستند، تعریف می شوند. با این حال، امروزه سازمان های بین المللی مختلف (در جلوگیری از تهدید جرایم سایبری دخالت دارند. این سازمان ها شامل سازمانهای منطقه‌ای مانند اتحادیه اروپا، ناتو، سازمان کشورهای امریکایی، اتحادیه افریقا برای ارتقای آگاهی امنیتی، همکاری بین المللی در اجرای قانون، هماهنگ سازی قوانین غیره فعالیت می کنند و نقش بسزایی در کنترل گسترش جرایم سایبری در سطح جهان ایفا می کنند. با توجه به اهمیت این موضوع سوال اصلی مقاله این است که سازمان های منطقه ای برای پیشگیری و مقابله با تهدیدات سایبری به چه راهکارهایی می پردازند؟ در پاسخ به این سوال، فرضیه تحقیق اینگونه مطرح می شود که از آنجایی که دولت ها به طور فزاینده ای بر سیاست ها و منابع یکجانبه برای تضمین حفاظت سایبری تکیه می کنند، سازمان های منطقه ای با داشتن اشتراکات فرهنگی جغرافیایی و منافع مشترک، نقش بهتری در شکل دادن به همکاری بین اعضای خود در قالب رویکردهای متمرکز بین المللی مبتنی بر همکاری در زمینه امنیت سایبری و پیشگیری از تهدیدات سایبری و همچنین توسعه یک سیستم امنیت سایبری جهانی و منطقه ای ایفا کنند. در کنار این سوال اصلی، برای فهم بهتر و کاملتر موضوع مورد بحث، سوالات فرعی زیر مطرح می شوند:

«حمله سایبری چیست و چه ویژگیهایی دارد و کدام سازمان های منطقه ای در مبارزه با جرایم و حملات سایبری نقش برجسته ای دارند و عمده اقدامات آنها چیست؟ و چالش های پیش رو سازمان های منطقه ای در پیشگیری از حملات سایبری چیست ؟در این مقاله با روش توصیفی –تحلیلی و استفاده از منابع کتابخانه ای و اینترنتی، ابتدا تحلیلی از مفاهیم پایه فضای مجازی و تهدیدات سایبری و ابعاد رویکردهای نسبت به آن را بررسی می شود، تمرکز روی اقدامات سازمان های منطقه ای ازجمله وضع هنجارها و اقدامات تأمینی مجازی و فیزیکی در مقابل حملات سایبری ارائه می شود و چالش های پیش رو سازمان های منطقه ای را مطرح می شود.

۲-پیشینه پژوهش

با توجه به مطالعه ی منابع مختلفی و بررسی هایی که توسط نگارنده صورت گرفته است، پژوهش های مربوط به عملکرد سازمانهای منطقه‌ای در جنگ سایبری نسبتاً محدود هستند اما در سالهای اخیر رو به رشد بوده است و تعداد پژوهش های منتشر شده در مقایسه با سایر موضوعات بویژه در زبان فارسی در این زمینه بسیار اندک است، این پژوهش ها عمداً بر مطالعات موردی سازمان های منطقه ای خاص و تلاش های آنها برای مقابله با تهدیدات سایبری متمرکز است. این مطالعات اغلب بینش های ارزشمندی در مورد استراتژی ها و قابلیت های سازمان های منطقه ای در پاسخ به جنگ های سایبری ارئه می دهد. در ذیل به مهمترین پژوهش ها اشاره می شود:

کتاب « جنگ برای فضای مجازی»[۱] اثر کلیمبورگ،آ[۲] (۲۰۰۷) به بررسی چشم انداز در حال تحول فضای مجازی و چالش هایی که برای سازمان های منطقه ای ایجاد می کند می پردازد. او ابعاد مختلف جنگ سایبری و تهدیدهای فزاینده ای که ملت ها و سازمان ها با آن مواجه هستند را بررسی می کند. این کتاب به نقش سازمان های منطقه ای در مقابله با تهدیدات سایبری و تقویت همکاری های بین المللی می پردازد. این تحلیل جامعی از پویایی های ژئوپلیتیک در فضای سایبری و پیامدهای آن برای امنیت منطقه ای ارائه می دهد. بر اهمیت توسعه استراتژی های جامع برای مقابله با تهدیدات سایبری و ارتقای امنیت سایبری تاکید می کند. این کتاب همچنین بر اهمیت همکاری بین المللی و به اشتراک گذاری اطلاعات بین سازمان های منطقه ای برای مبارزه موثر با جنگ سایبری تاکید می کند.

کتاب« کتابچه راهنمای تالین»[۳] نوشته اشمیت، ام ان[۴] (۲۰۱۷) این کتابچه راهنمای تاثیرگذار تجزیه و تحلیل جامعی از قوانین بین‌المللی قابل اجرا در عملیات سایبری ارائه می‌کند. این چارچوب قانونی حاکم بر جنگ سایبری و عملیات سایبری، از جمله نقش سازمان های منطقه ای در اجرای قوانین بین المللی را بررسی می کند و نقش سازمان های منطقه ای را در ارتقای انطباق با هنجارهای قانونی و تضمین مسئولیت پذیری برای عملیات سایبری برجسته می کند. مقاله «نقش سازمان های منطقه ای در جنگ سایبری»[۵] جانسون، آر و براون، ک.[۶] (۲۰۱۷) این تحلیل تطبیقی نقش سازمان های منطقه ای را در جنگ سایبری بررسی می کند. نویسندگان مطالعات موردی سازمانهای منطقه‌ای مختلف را تجزیه و تحلیل کرده و اثربخشی آنها را در مقابله با تهدیدات سایبری ارزیابی می‌کنند. نتایج اصلی این مقاله این است که سازمانهای منطقه‌ای با تسهیل همکاری و هماهنگی بین کشورهای عضو، نقش مهمی در جنگ سایبری ایفا می‌کنند. مقاله «امنیت سایبری در اتحادیه اروپا»[۷] نوشته آندراس دال[۸] این مقاله به درک تهدیدات و حملات سایبری در زمینه سازمان های بین المللی و دولت ها پرداخته است و در بخشی دیگر حملات سایبری علیه کشورهای عضو ناتو را بررسی نموده و همچنین به تاثیر هوش مصنوعی در تهدیدات سایبری تاکید نموده است. این مقاله به نقش سازمان های منطقه ای را در پاسخگویی و مدیریت جنگ سایبری بررسی می کند. و تلاش های سازمان های منطقه ای در توسعه چارچوب ها، استراتژی ها و سیاست ها برای مقابله با تهدیدات سایبری را بررسی می کند. این ادبیات فرصت ها چالشهای پیش روی سازمانهای منطقه‌ای را از نظر همکاری، اشتراک گذاری اطلاعات، ظرفیت سازی و مکانیسم‌هایی واکنش در فضای سایبری برجسته می‌کند که در هیچ کدام از پژوهش های فوق دیده نشده است. قبل از اینکه به اقدامات و مکانیسم های سازمان های بین المللی منطقه ای در پیشگیری از حملات سایبری پرداخته شود لازم است مفاهیم کلیدی ذیل اصطلاح فضای مجازی تعریف و تبیین شود سپس به اقدامات سازمان های بین المللی منطقه ای پرداخته شود.

۳-تعاریف،مفاهیم فضای مجازی

در ذیل تعاریف و مفاهیم اساسی در مورد فضای مجازی مورد بررسی و ارزیابی قرار خواهد گرفت.

۳-۱-تعریف و مفاهیم

[۱] The war for cyberspace
[۲] Limburg, A .
[۳] Tallinn manual on the international law applicable to cyber operations
[۴] Schmitt, M. N
[۵] The role of regional organizations in cyber warfare
[۶] Johnson, R., & Brown, K
[۷] Cyber security in the European union,
[۸] Andreas Dull

درمورد تعریف و مفهوم فضـای سـایبری یا فضـای مجازی تعاریف و مفاهیم زیادی ارائه شـده اسـت که هر کدام از زوایای متفاوت به آن نگریسـته اند. برخی معتقدند که منظور از فضـای مجازی یا سـایبری ترکیبی از ده ها هزار رایانه به هم پیوسـته، سرویس دهنده، شبکه های ارتباطی و کابل های فیبر نوری است که امکان خلق ارتباط را در یک سامانه جامع را فراهم می کند. برخی دیگر اعتقاد دارند که فضای سایبری، استعاره ای برای تشریح سرزمین غیر مادی و غیر فیزیکی تشکیل شده توسط سامانه های رایانه ای می دانند که بر خلاف فضـای واقعی، گشـت و گذار در این فضـا بدون هیچگونه حرکت فیزیکی و مادی و تنها با حرکت موشـواره وبا فشـردن کلیدی در صـفحه کلید امکانپذیر اسـت. همچنین گروهی دیگر فضـای سـایبری را نوعی بازنمایی گرافیکی از داده هایی که بانک های تمامی رایانه ها در سـامانه انسـانی تصـویر سـازی شـده اسـت تشـریح می نمایند.(تقی زاد و همکاران، ۱۳۹۶: ۱۰۶) اولین بار اصطلاح فضای مجازی توسط« ویلیام گیبسون» در رمان علمی تخیلی نورو منسر در سال۱۹۸۴ ارائه شد که برای نخستین بار از این واژه استفاده می شد. گیبسون در شرایطی که شبکه ها و رایانه های جهانی امروزه نبود فضای سـایبری را این گونه معرفی نمود: فضـای مجازی یک توهم مورد وفاق اسـت که روزانه میلیاردها اپرا تور و کودکانی که مفاهیم ریاضـی به آنها داده می شـود آن را تجربه می کنند. در واقع فضـای سـایبری مثل هر فضـای دیگری دارای موقعیت جغرافیایی، فیزیکی یا محدوده سـرزمینی خاصـی نیسـت ولی با این وجود نوعی واقعیت مهم در دنیای معاصـر اسـت چرا که ما کنش گران انسانی هر روزه در آن دست به اقدام می زنیم و با آن در تعامل هستیم (همان :۱۰۷)و تمام بخش های زندگی انسان را در بر گرفته است و وابستگی با آن در حدی شده که ادامه زندگی بدون آن بسیار سخت است. از این رو می توان فضای سایبر را بعنوان دنیای جدید و موازی با دنیای واقعی و مخلوق رایانه های جهان و ارتباط های بین آنها تعریف نمود.(دزیانی،۱۳۸۳: ۶۳) یکی از مصادیق تابع فضای سایبری، جرم سایبری است. به زبان ساده، جرم سایبری ممکن است به عنوان یک فعالیت مجرمانه شامل یک رایانه و یک شبکه شکل بگیرد که این ابزارها یک وسیله یا یک هدف را مورد توجه دارند. تاکنون یک تعریف جامع و قابل قبولی برای جرایم سـایبری صـورت نگرفته اسـت. با توجه به گسـتردگی جنایاتی که می تواند توسـط یک مجرم سـایبری که در پشـت یک صفحه پنهان شده است مرتکب شود. با این حال، تعریف قبلی از جرایم سایبری به عنوان «عملی که قانون را نقض می کند، که با استفاده از فناوری اطلاعات و ارتباطات (ICT) به منظور هدف قرار دادن شبکه‌ها، سیستم‌ها، داده ها، وب سایت‌ها و/یا فناوری یا تسهیل جرم انجام می‌شود، شامل می‌شود. تقریباً تمام ویژگی ها در اکثر تعاریف پوشش داده شده است. (Neethu, 2020: 7) پس جرایم سایبری عبارتند از هرگونه فعالیت غیر مجاز که شامل یک سیستم، تجهیزات یا شبکه ارتباطی یک کشور یا سازمان می شـود می گویند. به دو نوع تقسـیم می شـود :-جنایاتی که از یک سـیسـتم به عنوان هدف اسـتفاده می کند -جنایاتی که یک سیستم ناآگاهانه در ایجاد آن نقش دارد.(Li and Liu, 2021:8183)

۳-۲-ویژگی های جرایم سایبری

افزایش میزان وقوع فعالیتهای مجرمانه و ظهور احتمالی انواع جدید فعالیتهای مجرمانه، چالشـهایی را برای نظامهای حقوقی و همچنین برای اجرای قانون ایجاد میکند. در ذیل برخی از اصـلی ترین ویژگی های جرایم سـایبری آورده می شـود:

- فناوری دیجیتال : جرایم سایبری به ناچار نوعی فناوری دیجیتال را شامل می شود، از تلفن هو شمند یا رایانه رومیزی گرفته تا داده هـای رمز گـذاری شـده یـا شـبکـه هـای امن؛(Neethu,2020: 7)

-دانش تخصصی : جرایم سایبری تنها از طریق فن آوری قابل ارتکاب است، بنابراین برای ارتکاب این نوع جرایم باید در اینترنت و رایانه و اینترنت مهارت زیادی داشته باشند

-آثار شدید: جرایم سایبری به طور فزاینده ای فراگیر و پیچیده می شوند و اثرات اقتصادی شدیدتری نسبت به بسیاری از جرایم متعارف دارند.

- ساختار ویژه :جرایم سایبری از نظر ساختاری از سه طریق اصلی منحصر به فرد هستند آنها از نظر فناوری و مهارت فشرده هستند. آنها نسبت به جرایم متعارف درجه جهانی شدن بالاتری دارند و جدید؛

-فقدان اطلاع رسانی: جرایم سایبری نیز از جمله گزارش نشده ترین اشکال جرم و جنایت هستند. بسیاری از قربانیان تمایلی به گزارش جنایات سایبری ندارند زیرا فکر می کنند مراجعه به مجریان قانون مانع از حمله نمی شود.

-فرا مرزی بودن و میزان پایین دستگیری مجرمان: جرایم سایبری با هیچ مرزی محدود نمی شود، آنها فراملی اند و مهاجم ممکن است قربانی ناآگاهی را در همسایگی یا در قاره ای دیگر هدف قرار دهد.

- نبود علائم و نشانه های ظاهری : برخلاف جرایم سنتی، جرایم سایبری صحنه معمول جرم را دربر نمی گیرد و ممکن است تا مدت ها جنایت کشف نشود؛

- تأثیرات منفی گسترده: یک جرم سایبری در یک زمان محدود می تواند آسیب ها و مشکلات طولانی مدت و گسترده ای را به جامعه و کشور تحمیل نماید؛(Neethu,2020: 7)

۳-۳-طبقه بندی جرایم سایبری

جرایم سایبری شایع ترین جرمی هستند که نقش مخربی در جهان مدرن ایفا می کنند، در اینگونه جرایم مجرمان نه تنها خسارت های زیادی به جامعه و دولت ها وارد می کنند بلکه می توانند هویت خود را تا زمان زیادی مخفی نگه دارند و حتی ممکن است هیچ وقت هویت اینگونه مجرمان مشخص نشود. مفهوم جرم سایبری با جرم سنتی بسیار متفاوت است همچنین به دلیل رشد فن آوری اینترنت، این جرم در قیاس با جرائم سنتی مورد توجه جدی قرار گرفته است، بنابراین بررسی ویژگیهای خاص جرم سایبری ضرورت دارد که در ادامه به برخی از جرایم سایبری رایج پرداخته می شود: تعقیب سایبری، ،هرزه نگاری سایبری، هک کردن،،ویروس ها و آلایندهای رایانه ای، جرایم سایبری مالی، «فیشینگ» و «ویشینگ»: یک نوع جرم سایبری است که به شیوه های مختلفی اطلاعات حساس افراد کلاهبرداری می شود.. (Kavanagh, ۲۰۲۱: ۹-۱۰)-حمله انکار سرویس، سرقت اطلاعات، انجام داده ها، حملات سالامی، بمباران ایمیل، جعل ایمیل، بمب منطقی، سرقت زمان اینترنت، جرایم مربوط به فناوری موبایل و بی سیم، جرایم سایبری مربوط به حقوق مالکیت معنوی. (Neethu, ۲۰۲۰: ۸)

۳-۴-حملات سایبری

یکی از ابعاد گسترده جرایم سایبری، حملات سایبری است. حملات سایبری در زمینه وسیع تری نسبت به آنچه که بطور سنتی عملیات اطلاعاتی نامیده می شود قرار می گیرند. عملیات اطلاعاتی عبارتند از استفاده یکپارچه از قابلیت های اصلی جنگ الکترونیک، روانی، شبکه کامپیوتری، ترفند نظامی و امنیتی، عملیات در هماهنگی یا پشتیبانی ویژه و مربوط به توانایی و نفوذ،

توقف، تخریب یا ربودن تصمیمات انسانی و یکی از فرآیندهای تصمیم گیری ملی است. عملیات شبکه کامپیوتری شامل حمله، دفاع و توانمند سازی بکارگیری و استفاده از آنهاست.

-جاسوسی سایبری تحت حمایت دولت با هدف جمع آوری اطلاعات برای حملات سایبری آینده؛
-یک حمله سایبری با هدف ایجاد زمینه سازی هرگونه ناآرامی و آشوب مردمی؛
-حمله سایبری با هدف از کار انداختن تجهیزات و تسهیل آشوب های فیزیکی مردم؛
-حمله سایبری به عنوان مکمل تهاجم فیزیکی؛
-حمله سایبری با هدف تخریب یا اختلال گسترده به عنوان هدف نهایی(جنگ سایبری)؛(Li and Liu, 2021:8177)

۳-۴-۱-تعریف جنگ های سایبری

تعاریف مختلفی از حملات سایبری از دیدگاه فنی و حقوقی از طرف متخصصان و صاحبنظران مطرح شده به شرح زیر می آید: ریچارد کلارک: معتقد است که حملات سایبری مجموعه از اقدامات هستند که توسط کشورها برای نفوذ به رایانه ها یا شبکه های رایانه ای یک کشور یا سازمان برای ایجاد آسیب یا اختلال انجام می شود. مایکل هایدن: حملات سایبری را هرگونه کوشش عمدی جهت ایجاد اختلال یا تخریب شبکه های کامپیوتری یک کشور به کشور یا سازمان دیگر.

مارتین لی بیکی: اعتقاد دارد که حملات دیجیتالی به سیستم های رایانه ای موجب می شود سیستم های رایانه ای مورد حمله قرار گیرند تا عادی بنظر برسند اما در واقع پاسخ های غیر واقعی تولید و صادر می کند. گروه راهنما تالین: معتقدند حمله سایبری به عنوان یک عملیات سایبری تهاجمی یا تدافعی است که می تواند موجب جراحت یا مرگ افراد و یا آسیب و تخریب اموال گردد. (Li and Liu, 2021: 8179)بنابراین حملات سایبری مجموعه از اقدامات دیجیتالی از طرف یک کشور یا شخص بصورت عمدی به زیرساخت ها حیاتی برای تخریب و آسیب رساندن و اخلال به سیستم رایانه ای یک کشور یا سازمان و ممکن است بطور غیر مستقیم منجر مرگ انسانها شود.

۳-۴-۲-انواع جنگ های سایبری

جنگ های سایبری را می توان به انواع مختلفی طبقه بندی کرد، در تقسیم بندی اول براساس مقیاس حملات ، که به جنگ های سایبری خرد و جنگ های سایبری کلان و در تقسیم بندی دوم براساس ماهیت حملات سایبری که می تواند انواع مختلفی از تجاوز را شامل شود طبقه بندی شده اند. در زیر به شرح آنها پرداخته می شود؛
الف)جنگ های سایبری خرد: به حملاتی سایبری با اهداف فردی و محدود گفته می شود که شامل حمله به حساب های ایمیل اتومبیل ها اشاره دارد؛

ب) جنگ های سایبری کلان: به حملاتی گسترده و همه جانبه ای که به زیرساخت ها ی حیاتی و مهمی مانند سیستم های بیمارستانی و کنترل ترافیک هوایی در این مورد می توان به حملات گسترده ای که به تأسیسات دولتی کشور استونی وارد آمد اشاره کرد. طبقه بندی بر اساس ماهیت که می توان یک جنگ سایبری گسترده و کیفیتی است نظیر هک کردن اطلاعات، غیر قابل استفاده نمودن سیستم های کامپیوتری، تبلیغات، جاسوسی، خراب کاری و اختلال در ادارات دولتی از طریق انکار حملات

سرویس؛ علاوه بر این جنگ سایبری می تواند منجر به تروریسم سایبری هم شود که یک جنگ مجازی است و باعث تخریب مشابه جنگ فیزیکی می شود. (Levinson, 2020)

۳-۴-۳-پیامدهای جنگ های سایبری

در قرن بیست یکم جنگ های سایبری بیشتر از جنگ های فیزیکی معمول و متعارف شده است و هر روز کشورها و سازمان های مختلفی مورد حمله سایبری قرار می گیرند وسعت آسیب پذیری ناشی از این حملات، بسیار گسترده است. این حملات، پیامدها های زیادی برای کشورها و سازمان به بار می آورد که در ذیل به برخی از آنها اشاره می شود: سرنگونی نظام حکومتی یا تهدیدات فاجعه بار امنیت ملی، شروع همزمان جنگ فیزیکی یا مهیا کردن شرایط برای جنگ فیزیکی در آینده، تخریب یا آسیب فاجعه بار وجه کشور در سطح بین المللی و منطقه ای و حتی داخلی، تخریب یا آسیب فاجعه بار به روابط سیاسی و اقتصادی کشور، تلفات گسترده انسانی یا تهدیدات برای سلامت و بهداشت عمومی جامعه، هرج مرج داخلی، اختلال گسترده در اداره امور کشور، از بین بردن اعتماد عمومی یا باور های مذهبی –ملی قومی، آسیب شدید به اقتصاد ملی، اختلال گسترده در عملکرد دارایی های سایبری ملی، ایجاد زمینه سازی ناآرامی و آشوب مردمی، حمله سایبری به عنوان مکمل تهاجم فیزیکی، تخریب یا اختلال گسترده به عنوان هدف نهایی(جنگ سایبری)(Li and Liu, 2021: 8177)

۴-اقدامات سازمان های منطقه ای در مواجه با حملات سایبری

امروزه کنش گری سازمان های بین المللی در نظام بین الملل نه تنها در حوزه های فنی، تجاری و صنعتی، بلکه در زمینه های صلح و امنیت بین المللی نقش مهم و برجسته ای بویژه بعد از جنگ جهانی اول ایفا نموده اند. از دیدگاه نهاد گرایان لیبرال نیز معمولا دیدگاه خوش بینانه ای نسبت به کارکرد سازمان های بین المللی در ایجاد و گسترش همکاری های بین المللی و در نتیجه امنیت دارند و معتقدند که از سازمان های بین المللی و توانایی آنها می توان برای افزایش یا تثبیت مزایای صلح مانند وابستگی متقابل اقتصادی و کاهش هزینه های جنگ از طریق تنبیه متجاوز استفاده کرد.(مشیرزاده،۱۳۸۸: ۵۹) در اوایل قرن بیست یکم با ظهور اینترنت و توسعه فضای مجازی میان کشورها و گسترش آن به سراسر جهان میدان نبرد پنجمی به نبردهای سنتی (جنگ هوایی، زمینی، دریایی، فضا سایبری) اضافه شد که کشورها و نهاد بین المللی با حملات پیاپی به مراکز مهم صنعتی و نظامی، ورود ویروس های مختلف سیستم های اینترنتی نظم جهانی اخلال ایجاد شده است. با توجه به این تحولات، اکثر دولت ها و سازمان های بین المللی موضوع فضای مجازی را در اولویت قرار داده اند و بر توسعه مکانیسم های اقدام پیشگیرانه تمرکز کرده اند و نیازمند یک اقدام جمعی برای مقابله با این حملات می باشد. سازمان های منطقه ای باید ظرفیت سازی، تقویت گفتگو و افزایش اعتماد را در برنامه پیشگیری خود داشته باشند. جدای از تلاش های ملی، اقدامات بین المللی در سطح سازمان ها و نهاد های بین المللی در راستای پرداختن به تهدیدات سایبری صورت گرفته است. در واقع اکثر سازمان های بین المللی فعال در حوزه سایبری، مبتنی بر معاهدات چند جانبه و تحت تأثیر دولت های تاسیس کننده آنان می باشند. بطور مثال می توان در سطح منطقه ای به اتحادیه اروپا، سازمان منطقه ای شانگهای، اتحادیه افریقا، آسه آن، ناتو، سازمان کشورهای امریکایی و شورای اروپا اشاره کرد. در حالیکه اغلب امور در حوزه حملات

سایبری بوسیله دولت ها برنامه ریزی و انجام می گیرند، سازمان های بین المللی به بهبود وضع و ارتقای راهبرد های جهانی، ایجاد ساختارها، نهاد و سازمان های منطقه ای و بین المللی در راستای پیشگیری از سوء استفاده از فناوری ها، تقویت سازوکارهای مقابله تهدیدات سایبری و اجرای حقوق مخاصمات مسلحانه می پردازند. (تقی زاد و دوستان ،۱۳۹۶: ۱۲۰)در دهه اخیر با تشدید حملات سایبری سازمان های منطقه ای اقدامات موثری در مبارزه و مواجهه با حملات سایبری انجام داده اند که به پاره ای از آنها اشاره می شود.

۴-۱-اقدامات اتحادیه اروپا برای جلوگیری از حملات سایبری

در برنامه جامع اتحادیه اروپا، تدابیر قانونی و حقوقی اقدامات عملیاتی و اجرایی دیده شده و یک رویکرد جدی به ایجاد اسناد الزام آور روی آورده است. در این زمینه یک مرکز اروپایی جرایم سایبری تاسیس نموده است. اولویت های استراتژیک اتحادیه اروپا در مقابل تهدیدات سایبری عبارتند از : دستیابی به تاب آوری سایبری، کاهش شدید جرایم سایبری، توسعه و تقویت سیاست دفاع سایبری و قابلیت های مرتبط با آن، تقویت سیاست مشترک دفاعی و امنیتی، توسعه منابع صنعتی و فناوری برای امنیت سایبری، ایجاد یک سیاست منسجم بین المللی فضای مجازی برای اتحادیه اروپا و ترویج ارزش های اصلی اتحادیه و ظرفیت سازی سازش سایبری اتحادیه از جمله اولویت های برنامه سایبری اتحادیه اروپا هستند. یکی از بخش های مهم برنامه مقابله با تهدیدات سایبری اتحادیه اروپایی، همکاری بیشتر با سازمان ها و کشورهای خاص و فعال در مقابل با حملات سایبری است به همین منظور اتحادیه با سازمان نظامی ناتو، آسه آن، اتحادیه افریقا، سازمان کشورهای امریکایی روابط نزدیکی دارد و با کشورهای امریکایی اقدام به ایجاد موافقت نامه های دوجانبه در زمینه مقابله با تهدیدات سایبری و توسعه روابط با اینگونه کشورها و سازمان ها نموده است. در زمینه تدوین مقررات سایبری اولین اقدام آن تدوین کنفرانس« بودا پست» است که یک سند مهم و یک الگویی برای تدوین قانون ملی جرایم سایبری و مبنایی برای حقوق بشردوستانه و در صورت اقتضا قانون حقوق بشر خواهد بود و در مورد پرونده های سایبری مورد اعمال قرار می گیرد و دولت های ثالث می توانند به آن ملحق شوند. (Poli and Sommario, 2023: 533-534)در زمینه حفاظت از اطلاعات و امنیت شخصی سایبری، کمیسیون اروپا[1]در راستای استراتژیک سایبری خود در سال ۲۰۱۳ اصول و اولویت هایی را برای تضمین فضای باز، امن و ایمن سازی در اتحادیه شناسایی نمود و وظایف و مسئولیت هایی را برای نهادها، آژانس ها ، کشورها و صنعت دانشگاه در اروپا مشخص نمود. اتحادیه قانون امنیت سایبری خود را در سال۲۰۱۹برای تقویت ماموریت آژانس امنیت سایبری[2]که مسئول واکنش به حوادث سایبری در مقیاس بزرگ به تصویب رساند. (Benincasa, 2020: 5)توسعه سیاست و توانمندی های دفاع سایبری، که سند چارچوب آن در سال۲۰۱۸ به تصویب اتحادیه رسیده، شش حوزه فعالیت را در اولویت قرارداد که تمرکز اولیه بر توسعه قابلیت های دفاع سایبری و حفاظت از شبکه های ارتباطی و اطلاعات اتحادیه است. اولویت های بعدی آموزش و تمرین، تحقیق و فناوری، همکاری نظامی و بین المللی ، در این زمینه اتحادیه نهادها و موسسات خاصی را ماموریت داده که در این زمینه انجام وظیفه نمایند: می توان به کالج امنیت و دفاع اروپا[3]آژانس دفاع اروپا[4]سرویس اقدام خارجی اروپا[5]کنش گران اصلی اتحادیه اروپایی در این زمینه باشند. توسعه منابع و فناوری برای امنیت سایبری هدف بعدی امنیت سایبری ، که اتحادیه برای تحقق این هدف بدنبال ترویج بازار واحد برای محصولات امنیت سایبری و ایجاد انگیزه سرمایه گذاری تحقیق و توسعه، نو آوری برای پرکردن

[1] EC
[2] ENISA
[3] ESDC
[4] EDA
[5] EEAS

شکاف در بازار امنیت فناوری اطلاعات و ارتباطات است. ایجاد یک سیستم منسجم بین المللی فضای سایبری برای اتحادیه اروپا و ترویج ارزش های اصـــلی اتحادیه، در این زمینه اتحادیه با اعمال قوانین موجود بین المللی در تلاش برای ایجاد ظرفیت ســـازی امنیت ســـایبری اســـت واز پذیرش کنوانســـیون «بودا پســـت» به عنوان بهترین راه برای رســـیدگی به جرایم ســـایبری حمایت می کند.(Benincasa, 2020: 6-7)

۴-۲-اقدامات شورای اروپا در برابر حملات سایبری

شـــورای اروپا در میان ســـازمان ها و نهاد های بین المللی، ملموس ترین رویکرد را برای تنظیم مجموعه ای از مشـــکلات امنیت سایبری بویژه جرایم سایبری تا به امروز اتخاذ نموده ا ست. اولین معاهده بین المللی در مورد جرایم سایبری با عنوان کنوانسیون جرایم سایبری در سال ۲۰۰۱ تصویب نمود در این کنوانسیون یک سیاست مشترک با هدف حمایت از آحاد جامعه بین المللی در برابر جرایم سایبری از طریق وضع قوانین و همکاری بین المللی ارائه نمود. حملات سایبری شامل جرایم ذیل کنوانسیون جرایم سایبری مربوط به محرمانه بودن، یکپارچگی و دسترسی غیر قانونی به داده ها و سیستم های رایانه ای و اخلال در اینگونه داده ها و سیستم ها ا ست. به عنوان مثال ماده ۲ کنوانسیون از دولت های عضو می خواهد که هرگونه د ستر سی عمدی و غیر قانونی به داده ها و سیستم های رایانه ای را به عنوان جرم سایبر در قوانین داخلی خود لحاظ نمایند و هرگونه تهدید سایبری حق دفاع را برای دولت ها ضرورت می داند. براساس کنوانسیون دولت ها توافق نمودند که در زمینه تحقیقات و رسیدگی به جرایم و حملات سایبری با همدیگر همکاری های لازم را داشته ارزنده علاوه بر اقدامات فوق شورای اروپا در سال ۲۰۱۷ چارچوبی به نام جعبه ابزار دیپلماسی سایبری را ارائه کرد که بر بهبود همکاری، جلوگیری از درگیری، کاهش تهدیدات احتمالی سایبری و تأثیرگذاری رفتار متجاوزان احتمالی تأکید داشت. در این بسته مجموعه‌ای از ابزارها از جمله اِعمال تحریم‌ها، توسعه ظرفیت‌های پیام‌رسانی و واکنش در سطح اتحادیه اروپا و کشورهای عضو با هدف تأثیر گذاری بر رفتار متجاوزان احتمالی، با در نظر گرفتن ضرورت و تناســـب پاســـخ، عنوان شـــده اســـت. این چارچوب ســـایبری در ماه مه ۲۰۱۹ به تصـــویب نهایی رســـید و ســـالانه توســـط شـــورای اروپا۲۰۱۹/۷۹۶ مورد بررسی قرار می گیرد.(Hathaway and others, 2012: 864)

۴-۳-راهبرد ناتو در برابر حملات سایبری

سازمان پیمان آتلانتیک شمالی(ناتو) اولین سازمان منطقه ای که در زمینه حملات سایبری فعالیت های خود را شروع کرد. این سازمان از سال۲۰۰۷ به طور رسمی اقدام علیه تهدیدات سایبری را در دستور کار خود قرارداد. از مهمترین عواملی که زمینه توجه سران ناتو در باب حوزه سایبر قرار گیرد، آسیب پذیری کشورهای عضو ناتو در برابر تهدیدات سایبری و دیگری حملات سایبری روسیه و چین علیه برخی از کشورهای اروپایی از جمله، حمله سایبری روسیه به مراکز حیاتی کشور استونی و گرجستان، یکسال پس از حمله سایبری به ا ستونی در سال ۲۰۰۸ در نشست ناتو در بودا پست مجار ستان پیشنهاد تدوین سند راهبرد سیا ست دفاع سایبری ناتو تو سط سران مطرح شد و سران ناتو خواهان آن شدند که امنیت سایبری جزء وظایف ناتو قرار گیرد و سپس سند راهبرد دفاع ســایبری تهیه و به تصـویب ســران قرار گرفت.(ترابی،۱۳۹۴: ۱۴۶) چنانچه یکی از کشـور های عضـو ناتو در معرض حمله سایبری قرار بگیرد که منجر به خسارات جبران ناپذیر شود، ماده ۵ دفاع جمعی پیمان آتلانتیک شمالی فعال می شود. در توضیح بند۵ باید گفت ، ناتو میتواند حمله به هر یک از اعضای عضو پیمان آتلانتیک شمالی را حمله به همه اعضا تلقی کند. در ســند «ناتو ۲۰۳۰» که چشــم انداز ۱۰ ســاله اهداف و رویکردهای پیمان آتلانتیک شــمالی را ارائه می کند، حملات ســایبری هم مشمول بند ۵ شد. مهمترین تغییر در این زمینه پذیرش حمله سایبری در سطح حمله نظامی می باشد. در اجلاس سران ناتو در سال ۲۰۱۱، کشـورها عضـو حملات سـایبری را در حکم حمله نظامی ارزیابی کردند و در نتیجه مجوز دفاع سـایبری و نظامی، شـامل

استفاده از نیروهای هوایی، دریایی و زمینی را برای خود محفوظ داشتند. ناتو تغییرات ساختاری، رویه ای و فنی در مقابل حملات سایبری ایجاد کرده که سازمان و کشورهای عضو در برابر این تهاجمات انعطاف پذیر تر با شند. با توجه به ر شد تعداد و شدت حملات ، ناتو باید توانایی ها و تخصص های سایبری خود را تطبیق و گسترش دهد. (Dism, 2019: 71)

۴-۴-اقدامات سازمان امنیت و همکاری اروپا در برابر حملات سایبری

به گفته «زانیر» دبیرکل ، سازمان امنیت و همکاری اروپا در حال انجام اقداماتی جهت استقرار و به کارگیری سیستم های حفاظتی بهتر و پیشرفته، جهت جلوگیری از تهدیدات سایبری است. شورای دائمی سازمان امنیت و همکاری اروپا در تصمیم شماره ۱۲۰۲ خود تدابیری را در مورد اقدامات اعتماد ساز سازمان برای کاهش خطرات درگیری ناشی از استفاده از فناوری اطلاعات و ارتباطات اتخاذ نمود. براساس این تصمیم سازمان از اعضا خواسته است که یک نوع شفافیت در اطلاعات نظامی ویا فعالیت های مربوط به کنترل سلاح های سبک و سنگین دا شته با شند و هرگونه تحرک و مانور نظامی را به اطلاع دیگر اعضا ر سانده شود. سازمان امنیت و همکاری اروپا اقدامات اعتماد سازی در فضای مجازی را در فرانسه و سایر کشورهای عضو اجرا نموده است این سازمان با تهدیدات سایبری مختلف از جمله جرایم سایبری و ا ستفاده از اینترنت برای اهداف تروریستی مقابله می کند و تمرکز خود را بر توسعه اقدامات اعتماد سازی برای کاهش خطرات سوء برداشت و تشدید تهدیدات سایبری با تبادل اطلاعات و ارتباطات بین دولت های عضو می تواند به خنثی کردن تنش های احتمالی و توقف یا کند کردن پیوسته یک درگیری غیر عمدی را متوقف کند. اقدامات اعتماد ساز سازمان امنیت و همکاری اروپا توسط دبیرخانه خود انجام می دهد و به منظور تقویت ثبات در فضای سایبری از طریق گفتگو مستمر میان کشورها تاکید می کند. (Kert staubyn, 2016)

۴-۵-اقدامات پیشگیرانه سایبری سازمان کشورهای امریکایی

سازمان کشورهای امریکایی در دهه های گذ شته به طور فعال به مو ضوع حملات سایبری در منطقه پرداخته ا ست. این سازمان جلسات متعددی را در محدوده وظایف وزیران دادگستری یا دادستان های کل قاره امریکا برگزار نموده است قبلا وزیران دادگستری قاره(REMJA) توصیه به تشکیل یک کار گروهی از کارشناسان بین دولتی در زمینه حملات سایبری نمودند و همچنین در سال ۲۰۰۰ وزرای دادگستری کل قاره امریکا به مو ضوع جرایم سایبری پرداخته اند و برروی تعدادی از تو صیه ها به توافق رسیدند این کار گروه تا کنون ۷ جلسه با موضوع حملات سایبری برگزار نموده است. (Sanou, 2012:22) برنامه امنیت سایبری OAS در انجام اقداماتی برای جلوگیری از جرایم سایبری از اوایل دهه ۲۰۰۰ بسیار مؤثر بوده است. از طریق مداخله، تیم های پاسخگویی به حوادث امنیتی رایانه ای (CSIRT) در اکثر کشورهای عضو آن، از جمله شیلی، کاستاریکا و غیره ایجاد شده ا ست. همچنین به کشورهایی مانند جامائیکا، ترینیداد کمک کرده ا ست.(Neethu, 2020: 12) در نشست۲۰۰۶ کار گروه سازمان کشورهای امریکایی توصیه نمود که کشورهای عضو باید همکاری را با شورای اروپا تقویت نمایند بطوریکه بتوانند اصول کنوانسیون حملات سایبری شورای اروپا را اجرا نمایند و مکانیسم های تبادل اطلاعات همچنان ادامه داشته باشد و علاوه بر آن، شورای اروپا با سایر سازمان ها و آژانس های بین المللی همچون سازمان ملل متحد، اتحادیه اروپا، مجمع همکاری اقتصادی آسیا اقیانوسیه و جی هشت در زمینه جرایم سایبری همکاری داشته باشند. در سال۲۰۰۸ کار گروه(REMJA) سازمان کشورهای امریکایی خواهان الحاق اعضا به کنوانسیون شورای اروپا در مورد حملات سایبری شد.(Sanou, 2012: 23) این همکاری می تواند با ا ستفاده از تجربیات دیگر آژانس های بین المللی سطح دفاعی سازمان را نسبت به حملات سایبری تقویت نماید.

۴-۶-اقدامات سازمان همکاری شانگهای در برابر حملات سایبری

سنگ بنای اقدامات سازمان همکاری شانگهای در مقابله با تهدیدات سایبری به نشست هفتم سران کشورهای عضو در سال۲۰۰۷ بر می گردد که سندی تحت عنوان برنامه اقدام کشورهای عضو جهت حفاظت از امنیت اطلاعات بین المللی امضا نمودند که در این سند مقرر کردند که کشورهای عضو در مواجهه با چالش ها و تهدیدات جدید در زمینه امنیت اطلاعات با یکدیگر همکاری نمایند تا به طور مشترک و دسته جمعی با تهدیدات رو به رشد سایبری مقابله کنند. در اوت۲۰۰۸ سران کشورهای عضو در شهر دوشنبه تاجیکستان یک بیانیه دیگر به منظور ایجاد یک چارچوب قانونی برای همکاری در زمینه امنیت اطلاعات کشورهای عضو صادر نمودند که در این بیانیه به اصل حاکمیت ملی در فضای سایبری تاکید نمودند. در بیانیه «یکاترینبورگ» روسیه، سران کشورهای عضو سازمان همکاری شانگهای امنیت اطلاعات را به عنوان یک عنصر کلیدی در امنیت دسته جمعی قلمداد نمودند و بر آن تاکید کردند. سازمان در جهت تقویت سیستم سایبری کشورهای عضو در نشست سال۲۰۰۹ در چین، یک تفاهم نامه ای را به امضا سران رساندند که اعضا را مکلف نمودند همکاری علمی و فناوری با یکدیگر داشته و در راستای تقویت سیستم امنیت اطلاعات به یکدیگر کمک و مساعدت نمایند تا در مقابل تهدیدات و چالش های سایبری ایمن شوند. در تمام نشست های اعضای سازمان بر مبارزه با تهدیدات سایبری تاکید شده است. در برنامه آینده سازمان که به دستور کار ۲۰۳۰ سازمان معروف است که در آن به اهداف توسعه فناوری دیجیتالی، بهبود زیرساخت های اطمینان بخشی فضای دیجیتالی پرداخته است در آن به امنیت فضای مجازی و مبارزه با چالش های سایبری تاکید ویژه ای شده است. سازمان گام های زیادی در جهت مقابله با تهدیدات سایبری برداشته است در نشست تاشکند ازبکستان در سال۲۰۱۵برای مبارزه با تروریسم سایبری «برنامه مانور مبارزه با تروریسم سایبری» را تصمیم گیری نمودند. (Hathaway and others, 2012: 865-6)

۴-۷-اقدامات اتحادیه جنوب شرق آسیا(ASEAN)در برابر حملات سایبری

اتحادیه جنوب شرق آسیا برنامه های مختلفی در راستای مقابله با تهدیدات سایبری در پیش رو داشته است. در چند سال گذشته شاهد پیشرفت های پایدار و قابل توجهی بوده چرا که سیاست امنیت سایبری را شتاب داده و منجر به ایجاد نهاده ای جدید در رابطه با امنیت سایبری شده است.(Benincasa, 2020:5)-در اولین نشست خود با موضوع تهدیدات سایبری در ۸ژانویه ۲۰۰۴ در بانکوک بیانیه را منتشر نمودند که در آن همکاری نزدیک اعضا را مهمترین عامل در مقابله با تهدیدات سایبری و افزایش مبارزه علیه جرایم فرا ملی اعلام نمودند. «آسه آن» یک طرح اقدام مشترک با کشور چین برای صلح و رفاه به امضا رساند که در آن طرح ، به روش های همکاری و واکنش اضطراری، حفظ و افزایش امنیت سایبری و همچنین پیشگیری و مبارزه با حملات سایبری تاکید شده است. علاوه بر آن، آسه آن به همکاری بیشتر از طریق به اشتراک گذاشتن سریع اطلاعات تهدیدی می تواند به موقع به حملات سایبری واکنش نشان دهد و تاثیر یا گسترش بالقوه یک حمله سایبری را کاهش دهد. در بیانیه مجمع آسه آن در ژوئیه۲۰۰۶ به همکاری همه جانبه در تمام اشکال در مبارزه با تهدیدات سایبری با سرعت و عملکرد مناسب تاکید نمودند و از دولتهای عضو خواسته شد قوانین و مقررات بین المللی بخصوص توصیه های مجمع عمومی سازمان ملل متحد وفق قطعنامه۶۶/۵۵در مورد حملات سایبری را با قوانین ملی هماهنگ کنند و از آنها پیروی نمایند ویک قطعنامه روسای پلیس کشورهای عضو آسه آن در سال ۲۰۰۸ در مورد جرایم سایبری تصویب نمودند. آسه آن با وجود پیشرفت های حاصل شده در تدوین قوانین مبارزه با حملات سایبری و اقدامات عملیاتی، در چند سال اخیر هنوز مسیر و استراتژیک مشخصی ندارد و منجر به یک ساختار امنیت سایبری معیوب شده است.(Benincasa, 2020: 34) برخلاف سازمان های منطقه ای دیگری نظیر اتحادیه

اروپا و ناتو با اتخاذ که یک ا ستراتژیک منسجم و کارآمد منطقه ای، توانسته اند زمینه های د ستیابی به اهداف مهم برای افزایش تاب آوری سایبری خود را فراهم نموده اند و گام های مهمی را برداشته اند.

۵-چالش ها و فرصت ها

اگرچه نهاد ها و سازمان های بین المللی متعددی در سراسر جهان به طور گسترده و اختصاصی جهت کنترل آسیب ها و عواقب حملات سایبری در تلاش هستند و مقابله با حملات سایبری را در دستور کار دارند اما هنوز در نقاط مختلف جهان به طور غیر قابل مهاری در حال رشد است و کشورها و سازمان های زیادی مورد حملات سایبری قرار می گیرند. بنابراین تحلیل چالش های مختلف که سازمان های بین المللی در هنگام انجام اقدامات مقتضی جهت مقابله با حملات سایبری با آن مواجه می شوند ضروری است.

۵-۱-چالش ها

در زیر برخی از چالش های مقابله با حملات سایبری آورده می شود؛

۵-۱-۱- چالش های فنی و تخصصی

-حجم بالای کاربران اینترنتی و متخلفان در میان آنها اجرای قانون را بسیار دشوار می کند بطوریکه تا سال۲۰۲۲ نزدیک به ۵میلیار کاربر اینترنتی فعال هستند.

- ابزار و اطلاعات دیجیتالی برای ارتکاب به جرایم و حملات سایبری بسیار ارزان و به راحتی در دسترس قرار دارد و نیازی به دانش پیچیده ندارد لذا محدود کردن استفاده از این ابزارها کار بسیار دشواری است.

-به دلیل دسترس بودن تعداد زیادی از شبکه های بی سیم عمومی و ابزارهای دیگر جهت دستیابی به ناشناس بودن، ردیابی مجرمان و تبهکاران سایبری دشوار است.

- امروزه تعداد زیادی از وب سایت ها ،نرم افزارها و برنامه ها در برابر تهدیدات سایبری آسیب پذیرند واین فقدان امنیت کافی ارتکاب به جرم سایبری را آسانتر می کند.

- امروزه اکثر فعالیت های مجازی بصورت آنلاین و خودکار انجام می شوند. پیام ها و حملات سایبری از طریق ربات ها انجام می شود بطوری که اقدام یک مجرم سایبری می تواند به اطلاعات میلیون ها کاربر آسیب وارد کند. برای جلوگیری از چنین فعالیت های گسترده ای برای همه سازمان ها سخت و طاقت فرساست.

- علاوه بر ناشناس بودن، کد گزاری یک شیوه فنی است که بصورت یک چاقو دو لبه عمل می کند. مهاجمان با کد گزاری چند لایه از سیستم های خود محافظت می کنند، به همین دلیل، سازمان ها ممکن است در مواقعی تشخیص تهدیدات را غیر ممکن بدانند. در این مواقع مدارک و اسناد تا شکسته شدن کد گزاری از بین بروند و پاک شوند.

- اگر چه تعدادی از سازمان های بین المللی و منطقه ای اقدامات قابل ستودنی در مقابله با حملات سایبری انجام داده اند اما همچنان کمبودهای جدی در زیر ساخت ها و منابع به طور گسترده بویژه در کشورهای در حال تو سعه وجود دارد. (Neethu, ۲۰۲۰: ۱۴)

۵-۱-۲-چالش های حقوقی

جرایم سایبری یک جنایت فرا ملی و فرا مرزی است که مرتکبین و قربانیان آن با اتصال به اینترنت می توان در هر نقطه ای جهان باشند پیدا نمود به همین خاطر تبادل اطلاعات و اشتراک گزاری داده ها در این زمینه لازم است. بنابراین چالش های حقوقی برای تعقیب مجرمان سایبری عبارتند از:

-سیستم های حقوقی متفاوت کشورها؛

-تغییرات در قوانین ملی جرایم سایبری؛

-تفاوت در شواهد و قوانین آیین دادرسی کیفری؛

-تغییرات در دامنه و قابلیت کاربرد جغرافیایی معاهدات منطقه ای و چند جانبه ای جرایم سایبری؛

- تفاوت در رویکردهای حفاظت از اطلاعات و احترام به حقوق بشر(Sanou,2012: 12)

۵-۱-۳-چالش های اخلاقی

فراتر از اجرای قانون، چالش های اخلاقی در استفاده انسانها، شرکت ها ، سازمان ها ، گروه ها و دولتها از فضای مجازی و ارتباطات (ICT) وجود دارد. در زیر تعدادی از این چالش ها آورده می شود:

- پرهیز از آسیب رساندن به دیگران و سیستم ها و داده های آنها؛

-احترام به حاکمیت قانون و حقوق بشر در حوزه صلاحیت قضایی آن؛

-حریم خصوصی افراد در فضای سایبری حفظ شود واز افشا اطلاعات کاربران خودداری شود؛(Neethu, 2020: 15)

۵-۱-۴-چالش های عملیاتی

یکی از چالش های کلیدی عملیاتی در مبارزه با جرایم سایبری مربوط به همکاری با کشورها دیگر است. مبارزه با جرایم سایبری نیازمند همکاری بین المللی و هماهنگی بین قوانین کشورها است، هرچند معاهدات حقوقی می توانند کمک متقابل به آنها بکند اما این فرآیند می تواند وقت گیر باشد و ممکن است نتایج قابل قبول و مدنظر سازمان ها در پی نداشته باشد. سازمان های منطقه ای می توانند با استفاده از راهبردهای مختلفی چالش های پیش رو مقابله با حملات سایبری را به فرصت هایی جهت ارتقا و توانمند سازی سازمان های منطقه ای تبدیل نموده و از این طریق تاب آوری سازمان ها را در تقابل با تهدیدات مختلف تقویت کرده و تهدیدات را به فرصت ها تبدیل نمایند.(Sanou, 2012: 40)

۵-۲-فرصت ها

در زیر به برخی فرصت های سازمان های منطقه ای در مقابله با تهدیدات سایبری اشاره می شود:

- کاربران باید نسبت به تهدیدات احتمالی فضای مجازی هوشیار باشند. سازمان های بین المللی با اعضای خود در این زمینه همکاری و مساعدت داشته باشند تا آگاهی را در سطوح پایه و ریشه ای گسترش دهند و این کار با برگزاری کارگاه ها ، سمینارها در مدارس و دانشگاه ها و ادارات صورت گیرد؛

- سازمان های بین المللی می توانند نرم افزارها و اپلیکیشن هایی که در برابر حملات سایبری آسیب پذیرند رصد و در صورت نقص اصلاح نمایند. برنامه هایی که حریم خصوصی را نقض می کنند بوسیله مراجعه قضایی ملی متوقف شوند.

-جهت مبارزه با جنایات سایبری کشورها بویژه کشورهای در حال توسعه نیازمند منابع و نیروی انسانی هستند که در این زمینه سازمانهای بین المللی برای ایجاد و توسعه با آنها همکاری و مساعدت نمایند.

- با توجه به ماهیت فرا ملی جرم، سیاست های ملی در مقابله با آن ناکافی است. در چنین شرایطی سازمان های بزرگ و مهم بین المللی از جمله سازمان ملل و سازمان های منطقه ای می توانند به طور فعال در جهت هماهنگ سازی سیاست های مقابله اقدام نمایند. ممکن است یک دادگاه بین المللی کیفری جرایم سایبری و دادستانی برای فضای سایبری ایجاد شود.

-سازمان ملل متحد بعنوان یک سازمان جامع و بالا دستی یک کد اخلاقی جهانی برای سازمان های منطقه ای که مجری علیه تهدیدات سایبری را مشخص نماید تا بطور موثر اقدامات مقتضی علیه حملات سایبری انجام دهد. (Kumar sing, 2016: ۲۴۱-۲۵۴)

۶- نتیجه گیری

این مقاله به نقش سازمان های منطقه ای در پیشگیری از حملات سایبری متمرکز شده است. سازمان های منطقه ای نقش بسیار مهمی در ایجاد ثبات در روابط دولت ها در فضای مجازی ایفا می کنند. با مروری به عملکرد سازمان های منطقه ای در مقابل حملات سایبری، توانسته اند اقدامات پیشگیرانه ای اتخاذ نمایند از این طریق بتوانند تاب آوری و توانمندی سازمان و اعضا را تقویت نمایند. این اقدامات، متفاوت بوده برخی سازمان ها بطور ویژه اقداماتی عملی همه جانبه و با ایجاد معاهدات بین المللی اقدام به وضع قوانین بازدارندگی و تنبیهی در مقابل تهدیدات سایبری نموده اند مثلا سازمان نظامی ناتو که به عنوان اولین سازمان منطقه ای، با توجه به ماهیت ذاتی نظامیش اقدامات خاصی در مقابل تهدیدات سایبری انجام داده است و جنگ سایبری را هم سطح جنگ نظامی ارزیابی نموده است و براساس ماده ۵ اساسنامه خود حق دفاع سایبری را برای خود قائل شده است. اتحادیه اروپایی هم اقدام به ایجاد منشور حقوقی در قابل تهدیدات سایبری کرده است و یک استراتژیک منسجمی در برابر تهدیدات سایبری اتخاذ نموده است. آسه آن هرچند اقدامات زیادی در رابطه با تهدیدات سایبری داشته اما همچنان برنامه منسجمی تا کنون در برابر تهدیدات سایبری تدوین نکرده است. سازمان امنیت و همکاری اروپا به استراتژی اعتماد سازی برای جلوگیری از درگیری های سایبری تاکید نموده است. این اقدامات با چالش ها و فرصت هایی روبرو شدند. از چالشها می توان به تعارض در سیاست های ملی و کمبود زیر ساخت ها و فرصت ها به ایجاد دادگاه بین المللی برای تهدیدات سایبری، آگاهی بخشی مردم و تغییرات در قوانین بین المللی فعلی اشاره کرد. با اجرای اقدامات مناسب و همکاری های منطقه ای می توان فضای سایبری را برای میلیاردها انسان فضایی امن و قابل اعتماد تبدیل کرد.

منابع:

-ترابی، قاسم(۱۳۹۴)«تکامل ناتو در قبال جنگ سایبری؛ دلایل؛ ابعاد و مؤلفه ها» فصلنامه مطالعات راهبردی، سال هیجدهم، شماره اول، مسلسل۶۷،۱۳۳-۱۵۸

-تقی زاد، مهرداد، زمرد ، کیوان و حاجیان، مهدی(۱۳۹۶)« نقش اتحادیه اروپا در قاعده مند سازی جرائم سایبری» فصلنامه مطالعات بین المللی پلیس، سال هفتم، شماره۲۹،۱۰۴-۱۴۳.

-دزیانی، زهرا(۱۳۸۳)« مقدمه ای بر ماهیت و تقسیم بندی تئوریک جرایم سایبری» خبرنامه انفورماتیک، شماره۸۷

-ضیایی، محسن(۱۳۹۷)«نقش و عملکرد سازمان های بین المللی در تامین صلح جهانی» مجله بین المللی پژوهش ملل، دوره سوم: ماره۷۵، ۳۰-۸۹.

-مشیر زاده، حمیرا(۱۳۸۸)« تحول در نظریه های روابط بین الملل» تهران، نشر سمت.

-Abhishek Kumar Singh, (2016)" Jurisdictional Issues in Cybercrime: An Analytical Study (University of Luck now,

-Abase Mohammad, (2021)" Security in cyber space in the field of international Relations" Journal of Archives in Military medicine: Vole, 8, issue four, 44-85, DoI: https://doi.org/10,5812.

-Benincasa Eugenio (2020)"the rile of regional organizations in building cyber resilience: SEAN and EU, Issues insights, working paper, vole, and 20.wp3.1-41

-Beidleman Scott w (2009)" Defining and Deterring cyber war" USAWC strategy Research Project, PA17013-5050.www.indianstrategicknow ledgeonline.com.

-Dismal Carlo (2019)"The evolving cyber warfare landscape" www.jstor.org.

-Finkelstehn, Claire and Govern, Kevin H, (2015) "Cyber and the changing Face of war" Faculty scholarship at Penn Carey law.

-Hathaway Oona, and others (2012)" The Law of cyber-Attack" Vole 100, No 4, pp. 717-885, https://www.jstor.org/stable/232498823.

-Levinson, Paul (2020) "Micro cyber war VS. Macro-cyber war: towards the beginning of afaxonomy" Digital war 1, pp.: 171-173, open access.

-Li Yu Chong and Liu Qinghai, (2021)" A comprehensive review study of cyber- attacks and cyber security: Emerging trends and recent developments "Energy Reports7, 8176-8186, http://creativecohmons.org.

-Lilli Eugenio (2023)" How can we know what we Think we Know about cyber operation? 'Journal of Global security studies, Volume, 8, issue, 2, p1-18, https://doi.org/10.1093/jogss/ogad 11.

- K Lukas, Timothy j Elves, frank j, Evans, cilluffo, and Alec a Neadeau, (2016)" European Union and Nato Global cyber security challenge: A Way Forward" Vole, 6, No 2,126-141, www.jator.org/stable/26470452

-Kert-staubyn, Mari (2016)" Osce confidence building measures for cyberspace" www.ccdcoe.org

-Marie Louise and Deveanny Joe (2023)" Raising the Political of cyber security in Latin America" www-cfr-org.

-Mawgoud Ahmed A. (2020)"Cyber Security Rests in Mena Region: Threats, challenges and counter measures" A. E. Hassanienet al. AISC, 1058, pp912-921.

-Meltzer Nils (2011) "Cyber warfare and international law" ideas for peace and security.

-Madubuike ekwe Joseph n (2021)" cyber-attack and the use of force in international law" Scientific Research an academic publisher, Beijing Law Review, Vole 12, No 2, pp. 631-649 DoI: 10.4236/bar. Www-scrip-org.

-Molyakov, Andrei (2021) "The information and PSY wars of the future: Chinese cyber troops" Journal of scientific-Technical Research, volume 33, issue, 2 pp.: 25603-25608, Dole: 10.26717/bestir.
-Neethu N, (2020)' Role of international organization in prevention of cybercrimes an Analysis" https://www.researchgate.net/publication/350525198.
-Oakley, John T (2013)" cyber warfare: china's strategy to Dominate in cyber space"www.jstor.org
-Obi, Festus C. and Oludere, Alaba M. (2022)" Taming the shrew of rising cyber warfare" Open Access Library journal, Volume 9, https://doi.org/104236/oalib.1109003
-Poli, Sara and Sommario Emanuel (2023)" The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions, German Law Journal, pp. 522–536 doi:10.1017/glj.2023.25
-Kavanagh Stephen (2021)"African cyber Herat Easement Report" www.interpol.int.
-Rohith, cheerala and Singh bath, ranbir (2019) "cyber warfare: Nations cyber conflict cyber cold war between nations and its repercussion"
-Saroha Rashmi (2014)" Proflingacyber criminal" international journal of in formal and computation Technology, Issn0974-2239, Velum 4, Number3, pp253-258.
-Sanou Brahma (2012)" Cybercrimes/e-crimes: Assessment Report" HIPCAR, www.itu.int.
-WA lid Mahmoud Khalid (2013)" cyber-attacks: The Electronic Battlefield" www.dohainstitute.org.
-Walter Dom A, and Webb Stewart, (2019) "New Ways to prevent and manage cyber-attacks" International journal of cyber warfare and Terrorism, Volume 9, issue 1, DoI: 10, 40181ijcwt-2019010102.
-"The Role of Regional organizations in strengthening cyber security and stability" (2022), www.diplomacy-edu.
-"Cyber war: the challenge to National security" Global security studies, winter (2013), Vole 4, issue 1, pp. 93-115,
https://www-cybercrimelaw.net.translate.goog/International_organizations.htm-
-United Nations Office on Drugs and Crime, *Cybercrime Trends* (Nov. 27, 2020, 06:15 PM),
-United nationals institute for Disarmament research 8, (2019)" The center for strategic and international states"
-https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-trends.html.
-ASEAN cyber security cooperation strategy, 2021-2025(draft), www.asean.org
-https://www.tasnimnews.com/fa/news/1400/09/20/2623648
-Www-f-marc-Gov.-cu.

The function of regional organizations in cyber wars

Abstract

With the expansion of the cyber space, a new arena of threats has been created for governments in the form of cyber threats, and it has affected various aspects of national security, including social, economic, military and political security. It has affected international and regional security, which requires the necessary solutions to minimize the damage caused by this type of threats and maintain international security, Therefore, this article examines the role of regional organizations in preventing cyber-attacks by using the descriptive-analytical method,The hypothesis proposed in this research is that since governments are increasingly focused on unilateral policies and initiatives to deal with cyber threats,regional organizations should play an active role in shaping cooperation among members in the form of approaches focused on International and regional cooperation in the field of cyber security and prevention of cyber threats and the development of the global cyber security system The findings of the research show that regional organizations such as NATO, the European Union, Shanghai, ASEAN, the Organization for Security and Cooperation in Europe and the Organization of American States have taken measures to reduce damages caused by cybercrimes and counter cyber-attacks, including They have started to increase knowledge and establish cyber laws, regional cooperation, information sharing, infrastructure strengthening and trust building.

Keywords: Cyber-attacks, challenges, regional organizations, opportunities