فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال سوم | شماره سوم | پاییز ۱۴۰۲ | شماره پیاپی ۱۱
وبگاه مجله: https://cyberlaw.maragheh.iau.ir
ISSN: 2821-126X

The Strategy of International and Regional Organizations in Encountering Cyber Attacks

Tajmohammad Sadeghi
Ph.D. Student in International Law, Najafabad branch, Islamic Azad University, Najafabad.
Leila Raisi
Associate professor, Department of Law, Esfahan Branch, Islamic Azad University, Esfahan, Iran.
(Corresponding Author) Email: raisi.Leila.@Gmail.com.
Alireza Ansari Mahyari
Assistant Professor, Department of Law, Najafabad Branch, Islamic Azad University, Najafabad, Iran.

Keywords:
Cyber-attacks, Regional Organizations, International Organizations, Cyber Wars

Abstract

Cyber space is a space similar to other competitive areas such as sea, land, air, but with the difference that it is fabricated and intangible. With its expansion, it has challenged human life and threatens global and regional security. In this context, the reaction of international and regional organizations is significant and they have been able to take steps to reduce and minimize the resulting damages. Therefore, this article examines the role of international and regional organizations in facing cyber-attacks using descriptive-analytical method. Since governments have increasingly focused on unilateral policies and initiatives to deal with cyber threats, international and 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 and results of the research show that international and regional organizations such as the United Nations, the International Telecommunication Organization, NATO, the European Union, Shanghai, ASEAN, ECOWAS, the Organization of American States and the Organization for Security and Cooperation in Europe have taken measures that have reduced the damages caused by cybercrimes and countered cyber-attacks, including increasing knowledge and establishing cyber laws, regional cooperation, sharing information, strengthening infrastructure and building trust.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال سوم | شماره سوم | پاییز ۱۴۰۲ | شماره پیاپی ۱۱
صفحات مقاله ۵۰ الی ۶۵

راهبرد سازمان‌های بین‌المللی و منطقه‌ای در مواجهه با حملات سایبری

تاج محمد صادقی

دانشجوی دکتری حقوق بین‌الملل، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

پست الکترونیک: ttn.tina@yahoo.com

لیلا رئیسی

دانشیار، گروه حقوق، واحد اصفهان (خوراسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران.(نویسنده مسئول)

علیرضا انصاری مهیاری

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

تاریخ دریافت : ۱۳ شهریور ۱۴۰۲ تاریخ پذیرش: ۲۴ خرداد ماه ۱۴۰۳

چکیده

فضای سایبری در اصل، فضایی شبیه سایر سطوح رقابتی مانند دریا، زمین، هوا است اما با این تفاوت که این محیط دست‌ساخته انسان و ناملموس است. با گسترش آن، زندگی انسان را به چالش کشیده است و امنیت جهانی و منطقه‌ای را تهدید می‌کند. در این زمینه، واکنش سازمان‌های بین‌المللی و منطقه‌ای، قابل‌توجه است و توانسته‌اند راحل‌هایی را برای کاهش و به حداقل رساندن خسارات ناشی از آن انجام دهند. ازاین‌رو مقاله حاضر با استفاده از روش توصیفی –تحلیلی به بررسی نقش سازمان‌های بین‌المللی و منطقه‌ای در مواجهه با حملات سایبری می‌پردازد. ازآنجایی‌که دولت‌ها به‌طور فزاینده‌ای به سیاست‌ها و ابتکارات یک‌جانبه برای مقابله با تهدیدات سایبری متمرکزشده‌اند سازمان‌های بین‌المللی و منطقه‌ای باید نقش فعالی در شکل دادن به همکاری میان اعضا در قالب رویکردهای متمرکز بر همکاری بین‌المللی و منطقه‌ای در زمینه امنیت سایبری و پیشگیری از تهدیدات سایبری و توسعه سیستم امنیت سایبری جهانی ایفا کنند. یافته‌های و نتایج تحقیق نشان می‌دهد که سازمان‌های بین‌المللی و منطقه‌ای نظیر سازمان ملل متحد، سازمان بین‌المللی مخابرات، ناتو، اتحادیه اروپا، شانگهای، آ سه آن، اکوواس، سازمان کشورهای آمریکایی و سازمان امنیت و همکاری اروپا اقداماتی مانند دانش‌افزایی و وضع قوانین سایبری، همکاری منطقه‌ای، اشتراک گزاری اطلاعات، تقویت زیرساخت‌ها و اعتمادسازی در راستای مقابله و کاهش خطرات ناشی از حملات سایبری انجام داده‌اند.

واژگان کلیدی: حملات سایبری، سازمان‌های منطقه‌ای، سازمان‌های بین‌المللی، جنگ‌های سایبری

مقدمه

جنگ‌های سایبری عبارت‌اند از حمله به زیرساخت‌های کامپیوتری، دزدی اطلاعات یا تخریب داده‌ها گفته می‌شود. این اقدامات ممکن است به یکی از چهار اهداف زیر هدفمند شوند: تخریب، سرقت، نفوذ و نفوذ برای ارتقا یا تغییر داده‌ها به‌نحوی‌که سازمان‌ها یا افراد نتوانند به آن‌ها اعتماد کنند یا اطلاعات آن‌ها را به‌عنوان دانه‌ای درخطر ببینند. این تهدیدات گریبان سازمان‌ها و نهاده‌ای منطقه‌ای را گرفته است بطوری که با افزایش حملات سایبری، سازمان‌های بین‌المللی به شیوه‌ای مختلف اقدام به مقابله با آن گرفته‌اند. مقیاس و ماهیت فرامرزی تهدیدات سایبری به‌گونه‌ای است که همکاری بین‌المللی را می‌طلبد، سازمان ملل متحد گروهی از کارشناسان دولتی و دفتر امور آزادسازی سلاح‌های کشورهای متحد را برای برخورد با مسائل امنیت سایبری و جلوگیری از استفاده صحیح از فناوری‌های اطلاعات و ارتباطات تأسیس نموده است. سازمان ملل متحد همچنین همکاری بین‌المللی و افزایش ظرفیت در زمینه امنیت سایبری را از طریق ابتکارهایی مانند «انجمن جهانی تخصص سایبر» و «برنامه افزایش ظرفیت امنیت سایبری سازمان ملل» ترویج می‌کند. سازمان بین‌المللی ارتباطات منطقه‌ای منابع و فرصت‌های افزایش ظرفیت را برای بهبود امنیت سایبری فراهم می‌آورد. همچنین جامعه اقتصادی کشورهای غرب آفریقا بر تأکید بر ایجاد یک مکانیزم نظارتی منطقه‌ای و پایه قانونی برای مسئولیت کشورهای عضو در صورت عدم انطباق با راهنماها تأکید دارد. سازمان‌های بین‌المللی و منطقه‌ای سیاست‌ها و استراتژی‌های مشترک در این زمینه را تعیین می‌کنند و در تبادل اطلاعات و همکاری بین‌المللی برای جلوگیری از حملات سایبری مشغول به فعالیت هستند. با توجه به اهمیت این موضوع سؤال اصلی مقاله این است که سازمان‌های بین‌المللی و منطقه‌ای برای پیشگیری و مقابله با تهدیدات سایبری به چه راهکارهایی می‌پردازند؟ در پاسخ به این سؤال، فرضیه تحقیق این‌گونه مطرح می‌شود که ازآنجایی‌که دولت‌ها به‌طور فزاینده‌ای بر سیاست‌ها و منابع یک‌جانبه برای تضمین حفاظت سایبری تکیه می‌کنند، سازمان‌های بین‌المللی و منطقه‌ای نقش بهتری در شکل دادن به همکاری بین اعضای خود در قالب رویکردهای متمرکز بین‌المللی مبتنی بر همکاری در زمینه امنیت سایبری و پیشگیری از تهدیدات سایبری و همچنین توسعه یک سیستم امنیت سایبری جهانی و منطقه‌ای ایفا کنند. در کنار این سؤال اصلی، برای فهم بهتر و کامل‌تر موضوع موردبحث، سؤالات فرعی زیر مطرح می‌شوند:

منظور از حملات سایبری چیست و سازمان‌های بین‌المللی و منطقه‌ای چگونه با تهدیدات سایبری مقابله می‌کنند؟ و چالش‌های پیش رو سازمان‌های بین‌المللی و منطقه‌ای در پیشگیری از حملات سایبری چیست؟ در این مقاله با روش توصیفی –تحلیلی و استفاده از منابع کتابخانه‌ای و اینترنتی، ابتدا تحلیلی از مفاهیم تهدیدات و حملات سایبری و ابعاد رویکردهای نسبت به آن را بررسی می‌شود، تمرکز روی اقدامات سازمان‌های بین‌المللی و منطقه‌ای ازجمله وضع هنجارها و اقدامات تأمینی مجازی و فیزیکی در مقابل حملات سایبری ارائه می‌شود و چالش‌های پیش رو سازمان‌های بین‌المللی و منطقه‌ای را مطرح می‌شود. قبل از اینکه به اقدامات و مکانیسم‌های سازمان‌های بین‌المللی منطقه‌ای در پیشگیری از حملات سایبری پرداخته شود لازم است مفاهیم کلیدی زیر اصطلاح حملات سایبری تبیین شود سپس به اقدامات سازمان‌های بین‌المللی و منطقه‌ای پرداخته شود.

۱. حملات سایبری

یکی از ابعاد گسترده جرایم سایبری، حملات سایبری است. حملات سایبری در زمینه وسیع‌تری نسبت به آنچه به‌طور سنتی عملیات اطلاعاتی نامیده می‌شود قرار می‌گیرند. عملیات اطلاعاتی عبارت‌اند از استفاده یکپارچه از قابلیت‌های 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 تصمیم‌گیری ملی است. عملیات شبکه کامپیوتری شامل حمله، دفاع و توانمندسازی به‌کارگیری و استفاده از آن‌هاست.

– جاسوسی سایبری تحت حمایت دولت باهدف جمع‌آوری اطلاعات برای حملات سایبری آینده؛

– یک حمله سایبری باهدف ایجاد زمینه‌سازی هرگونه ناآرامی و آشوب مردمی؛

– حمله سایبری باهدف از کار انداختن تجهیزات و تسهیل آشوب‌های فیزیکی مردم؛

– حمله سایبری به‌عنوان مکمل تهاجم فیزیکی؛

– حمله سایبری باهدف تخریب یا اختلال گسترده به‌عنوان هدف نهایی (جنگ سایبری) حملات سایبری محدود به موارد خاص نیستند و می‌توانند شامل حملات مختلف و گسترده‌ای مانند مختل کردن شبکه‌های رادیو و تلویزیون، آشفتگی بازار و سهام... و هدف قرار دادن زیرساخت‌های حیاتی باشند. هدف قراردادن زیرساخت‌های حیاتی مهم‌ترین نوع حملات سایبری است.(انصاری مهیا ری و سادات حسینی،۱۴۰۱: ۲۱-۲۲)

۱-۱-تعریف جنگ‌های سایبری

تعریف جنگ‌های سایبری از دیدگاه فنی و حقوقی که از طرف متخصصان و صاحب‌نظران مطرح‌شده به شرح زیر می‌آید می‌توان به یک تعریف جامع و کاملی از حملات سایبری رسید.

ریچارد کلارک: معتقد است که حملات سایبری مجموعه از اقدامات هستند که توسط کشورها برای نفوذ به رایانه‌ها یا شبکه‌های رایانه‌ای یک کشور یا سازمان برای ایجاد آسیب یا اختلال انجام می‌شود.

مایکل هایدن: حملات سایبری را هرگونه کوشش عمدی جهت ایجاد اختلال یا تخریب شبکه‌های کامپیوتری یک کشور به کشور یا سازمان دیگر.

مارتین لی بیکی: اعتقاد دارد که حملات دیجیتالی به سیستم‌های رایانه‌ای موجب می‌شود سیستم‌های رایانه‌ای موردحمله قرار گیرند تا عادی به نظر برسند اما درواقع پاسخ‌های غیرواقعی تولید و صادر می‌کند.

گروه راهنما: معتقدند حمله سایبری به‌عنوان یک عملیات سایبری تهاجمی یا تدافعی است که می‌تواند موجب جراحت یا مرگ افراد و یا آسیب و تخریب اموال گردد (Li and Liu, 2021: 8179). موسسه «رند» جنگ سایبری را این‌گونه تعریف می‌کند. جنگ سایبری جنگی با محوریت دولت‌ها و سازمان‌های بین‌المللی علیه سایر دولت‌ها باهدف ایجاد تخریب در شبکه اطلاعات و کامپیوتر است. این حملات با ویروس‌ها، تروجان‌ها و سایر بدافزارها صورت می‌گیرد. شورای ملی تحقیقات ایالات‌متحده، حمله سایبری را به‌عنوان «اقدامات عمدی برای تغییر، اخلال، فریب، تخریب، یا تخریب سیستم‌ها یا شبکه‌های رایانه‌ای یا اطلاعات و/یا برنامه‌های ساکن در این سیستم‌ها یا شبکه‌ها یا در حال انتقال آن‌ها» تعریف می‌کند. رویکرد تعاریف مبتنی بر هدف اتخاذ شده توسط ایالات‌متحده ترجیح داده می‌شود(Hathaway, 2011: 9) . در یک سطح عمیق‌تر جنگ سایبری درواقع یک جنگ دانش است و جنگی مبتنی بر رایانه و اطلاعات، جنگ سایبری جدیدترین شکل جنگ اطلاعاتی است و می‌توان شامل موارد زیر باشد: خراب‌کاری اینترنتی، اخلال در سرویس‌دهی، اخلال در تجهیزات.(انصاری مهیا ری و محمودی،۱۴۰۱:۲۵-۲۶)

۲-۱-حملات سایبری، جنایات سایبری و جنگ سایبری

جرایم سایبری مفهومی، گسترده است که ازلحاظ تحلیلی از حمله سایبری متمایز است. درحالی‌که مانند مفهوم حمله سایبری، هیچ تعریف شناخته شده جهانی از جرایم سایبری وجود ندارد جنبه‌هایی از جرایم سایبری وجود دارد که به‌طور گسترده به رسمیت شناخته‌شده‌اند. به‌این‌ترتیب، جرایم سایبری طیف گسترده‌ای از فعالیت‌های غیرقانونی را در برمی‌گیرد. ازجمله اولویت‌های وزارت دادگستری و واحدهای FBI برای رسیدگی به جرایم سایبری، روش‌های متقلّبانه در اینترنت، دزدی دریایی آنلاین، ذخیره و به اشتراک‌گذاری پورنو گرافی کودکان در رایانه و نفوذهای رایانه‌ای است. شبکه‌های کامپیوتری هدف را تضعیف می‌کنند بیشتر جرایم سایبری، حمله سایبری یا جنگ سایبری نیز محسوب نمی‌شوند. یک عمل فقط زمانی جرم سایبری است که یک بازیگر غیردولتی مرتکب عملی شود که طبق قوانین دولتی یا بین‌المللی جرم انگاری شده است. سه سناریو وجود دارد: اول، یک بازیگر غیردولتی برای اهداف سیاسی یا امنیت ملی و از طریق یک شبکه کامپیوتری مرتکب یک عمل غیرقانونی می‌شود اما آن شبکه را تضعیف نمی‌کند. به‌عنوان‌مثال، ممکن است فردی با ابراز مخالفت سیاسی از طریق اینترنت مرتکب جنایت سایبری شود، جایی که این مخالفت طبق قوانین ایالتی غیرقانونی است. به‌طور مشابه، یک فرد ممکن است با هک کردن سوابق یک بانک بزرگ باهدف امنیتی ملی یا سیاسی، اما بدون تضعیف سیستم بانک در این فرآیند، مرتکب جرم سایبری شود. دوم، یک بازیگر غیردولتی از طریق یک شبکه کامپیوتری مرتکب یک عمل غیرقانونی می‌شود و یک شبکه کامپیوتری را تضعیف می‌کند اما نه برای اهداف سیاسی یا امنیت ملی. دوباره هکر داده‌های بانکی را در نظر بگیرید که اکنون موفق شده است سیستم حساب آنلاین بانک را تضعیف کند اما تنها هدفش سود اقتصادی است. این نیز یک جنایت سایبری است، اما نه یک حمله سایبری یا جنگ سایبری. ثالثاً، یک بازیگر غیردولتی با استفاده از رایانه یا شبکه به فعالیت غیرقانونی می‌پردازد اما عملکرد شبکه رایانه‌ای را تضعیف نمی‌کند و باهدف سیاسی یا امنیت ملی عمل نمی‌کند. به‌عنوان‌مثال، شخصی که پورنو گرافی کودکان را انتقال می‌دهد، مرتکب جنایت سایبری می‌شود اما حمله سایبری انجام نمی‌دهد، هم به این دلیل که اقدامات او عملکرد یک شبکه رایانه‌ای را تضعیف نمی‌کند و هم به دلیل اینکه انگیزه او یک هدف سیاسی یا امنیت ملی نیست. (Hathaway, 2012: 19) همان‌طور که برخی از جرایم سایبری نه حمله سایبری هستند و نه جنگ سایبری، برخی از حملات سایبری نیز نه جرایم سایبری هستند و نه جنگ سایبری. دو سناریو در این مورد است که فقط در حملات سایبری قرار می‌گیرند. سناریوی اول شامل حملاتی است که توسط یک بازیگر دولتی خارج از چارچوب یک درگیری مسلحانه انجام می‌شود، مشروط بر اینکه اثرات آن به سطح یک حمله مسلحانه نرسد. نمونه‌ای از این، حمله دولت چین به وب‌سایت فالون گونگ در سال ۲۰۱۱ است. بااین‌حال، هر اقدامی توسط یک بازیگر دولتی به‌طور خودکار الزامات هدف سیاسی یا امنیت ملی را برآورده می‌کند. سناریوی دوم فقط حمله سایبری شامل حملاتی از سوی بازیگران غیردولتی است که به سطح یک حمله مسلحانه نمی‌رسد و جرم سایبری محسوب نمی‌شود، چه به این دلیل که طبق قوانین ملی یا بین‌المللی جرم انگاری نشده است. آن‌ها از وسایل کامپیوتری استفاده نمی‌کنند. ازنظر عملی، بعید است که یک بازیگر خصوصی به‌طور هدفمند عملکرد یک شبکه رایانه‌ای را بدون نقض قانون تضعیف کند، اما چنین شکاف‌هایی در قوانین کیفری ازنظر مفهومی امکان‌پذیر است. درحالی‌که فعالیت‌های سایبری ممکن است فقط جنایت سایبری یا فقط حمله سایبری باشد، بخش قابل‌توجهی از جرایم سایبری نیز حملات سایبری هستند. حوزه همپوشانی بین جرایم سایبری و حمله سایبری زمانی رخ می‌دهد که یک بازیگر غیردولتی با استفاده از یک شبکه رایانه‌ای مرتکب عمل غیرقانونی شود، یک شبکه رایانه‌ای را تضعیف کند و یک هدف سیاسی یا امنیت ملی داشته باشد. پیامدهای این عمل به سطح یک حمله مسلحانه نمی‌رسد و یا این فعالیت به‌منزله جنگ سایبری خواهد بود. همچنین توجه داشته باشید که دولتی که مرتکب همین عمل می‌شود، در این همپوشانی قرار نمی‌گیرد، زیرا فقط یک بازیگر غیردولتی می‌تواند مرتکب جرم سایبری شود. (Hathaway, 2012: 20) جنگ سایبری در میان سه مقوله سایبری در نظر گرفته‌شده در اینجا متمایز است، زیرا

جنگ سایبری باید یک حمله سایبری نیز باشد. منطقه همپوشانی بین حمله سایبری و جنگ سایبری (اما نه جنایات سایبری) دو نوع حمله است. نوع اول شامل حملاتی است که توسط هر بازیگری در چارچوب یک درگیری مسلحانه انجام می‌شود، مشروط بر اینکه آن اقدامات را نتوان جنایات سایبری تلقی کرد، چه به این دلیل که جنایات جنگی محسوب نمی‌شوند، یا از ابزارهای رایانه‌ای استفاده نمی‌کنند، یا هر دو. نوع دوم شامل حملاتی است که توسط یک بازیگر دولتی انجام می‌شود که اثراتی معادل حملات مسلحانه معمولی ایجاد می‌کند. توجه داشته باشید که این استفاده از زور ممکن است قانونی یا غیرقانونی باشد. ازآنجایی‌که بازیگر یک کنش گر دولتی است، حتی اقدامات غیرقانونی نیز «جرم سایبری» محسوب نمی‌شود. یک حمله سایبری ممکن است توسط بازیگران دولتی یا غیردولتی انجام شود، باید شامل رفتار فعال باشد، باید هدف آن تضعیف عملکرد یک شبکه کامپیوتری باشد و باید هدف سیاسی یا امنیت ملی داشته باشد. برخی از حملات سایبری نیز جرایم سایبری هستند، اما همه جرایم سایبری، حملات سایبری نیستند. از سوی دیگر، جنگ سایبری همیشه شرایط یک حمله سایبری را دارد. (Hathaway, 2012:22) اما همه حملات سایبری جنگ سایبری نیستند. فقط حملات سایبری با اثراتی معادل حملات «حمله مسلحانه» متعارف، یا در چارچوب درگیری‌های مسلحانه، به سطح جنگ سایبری می‌رسند.

۳-۱-انواع جنگ‌های سایبری

در تقسیم‌بندی اول بر اساس مقیاس حملات که به جنگ‌های سایبری خرد و جنگ‌های سایبری کلان و در تقسیم‌بندی دوم بر اساس ماهیت حملات سایبری که می‌تواند انواع مختلفی از تجاوز را شامل شود طبقه‌بندی‌شده‌اند. در زیر به شرح آن‌ها پرداخته می‌شود؛

الف)جنگ‌های سایبری خرد: به حملاتی سایبری با اهداف فردی و محدود گفته می‌شود که شامل حمله به‌حساب‌های ایمیل اتومبیل‌ها اشاره دارد؛

ب) جنگ‌های سایبری کلان: به حملاتی گسترده و همه‌جانبه‌ای که به زیرساخت‌های حیاتی و مهمی مانند دستگاه‌های بیمارستانی و کنترل ترافیک هوایی در این مورد می‌توان به حملات گسترده‌ای که به تأسیسات دولتی کشور استونی اشاره کرد.

طبقه‌بندی حملات سایبری بر اساس ماهیت که می‌توان یک جنگ سایبری گسترده و کیفیتی است نظیر هک کردن اطلاعات، غیرقابل استفاده نمودن سیستم‌های کامپیوتری، تبلیغات، جاسوسی، خرابکار و اختلال در ادارات دولتی از طریق انکار حملات سرویس؛ علاوه بر این جنگ سایبری می‌تواند منجر به تروریسم سایبری هم شود که یک جنگ مجازی است و باعث تخریب مشابه جنگ فیزیکی می‌شود.

۴-۱-پیامدهای جنگ‌های سایبری

در قرن بیست یکم جنگ‌های سایبری بیشتر از جنگ‌های فیزیکی معمول و متعارف شده است و هرروز کشورها و سازمان‌های مختلفی موردحمله سایبری قرار می‌گیرند وسعت آسیب‌پذیری ناشی از این حملات بسیار گسترده است. این حملات پیامدهای زیادی برای کشورها و سازمان به بار می‌آورد که در زیر به برخی از عواقب آن اشاره می‌شود:

سرنگونی نظام حکومتی یا تهدیدات فاجعه‌بار امنیت ملی، شروع هم‌زمان جنگ فیزیکی یا مهیاکردن شرایط برای جنگ فیزیکی در آینده، تخریب یا آسیب فاجعه‌بار 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 باورهای مذهبی –ملی قومی،

آسیب شدید به اقتصاد ملی، اختلال گسترده در عملکرد دارایی‌های سایبری ملی، ایجاد زمینه‌سازی ناآرامی و آشوب مردمی، حمله سایبری به‌عنوان مکمل تهاجم فیزیکی، تخریب یا اختلال گسترده به‌عنوان هدف نهایی (جنگ سایبری) (Li and Liu, 2021: 8177).

۲. اقدامات سازمان‌های بین‌المللی در برابر حملات سایبری

از دیدگاه نهادگرایان لیبرال نیز معمولاً دیدگاه خوش‌بینانه‌ای نسبت به کارکرد سازمان‌های بین‌المللی در ایجاد و گسترش همکاری‌های بین‌المللی و درنتیجه امنیت دارند و معتقدند که از سازمان‌های بین‌المللی و توانایی آن‌ها می‌توان برای افزایش یا تثبیت مزایای صلح مانند وابستگی متقابل اقتصادی و کاهش هزینه‌های 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 و کشورها، مؤسسات دولتی و غیردولتی، نهاد بین‌المللی با حملات پیاپی به مراکز مهم صنعتی و نظامی، ورود ویروس‌های مختلف سیستم‌های اینترنتی نظم جهانی اخلال ایجادشده است. شبکه جهانی وب اکنون به عرصه‌ای برای درگیری‌های مربوط به جاسوسی، ورود غیرمجاز و کنترل پایگاه‌های داده تبدیل‌شده است که ممکن است امنیت ملی برخی از کشورها را تحت تأثیر قرار دهد. با توجه به این تحولات، اکثر دولت‌ها و سازمان‌های بین‌المللی موضوع فضای مجازی را در اولویت قرار داده‌اند و بر توسعه مکانیسم‌های اقدام پیشگیرانه تمرکز کرده‌اند و نیازمند یک اقدام جمعی برای مقابله با این حملات می‌باشد. سازمان‌های منطقه‌ای باید ظرفیت‌سازی، تقویت گفتگو و افزایش اعتماد را در برنامه پیشگیری خود داشته باشند. جدای از تلاش‌های ملی، اقدامات بین‌المللی در سطح سازمان‌ها و نهادهای بین‌المللی در راستای پرداختن به تهدیدات سایبری صورت گرفته است. درواقع اکثر سازمان‌های بین‌المللی فعال در حوزه سایبری، مبتنی بر معاهدات چندجانبه و تحت تأثیر دولت‌های تأسیس کننده آنان می‌باشند. در این زمینه، به اقداماتی برخی سازمان‌های بین‌المللی در مقابل حملات سایبری اشاره می‌شود:

۱-۲- سازمان ملل متحد[1]

سازمان ملل متحد اقدامات مختلفی را برای مقابله با حملات سایبری و افزایش امنیت سایبری انجام می‌دهد. سازمان ملل متحد گروهی از کارشناسان دولتی (GGE) را در زمینه تحولات در زمینه اطلاعات و ارتباطات از راه دور در زمینه امنیت بین‌المللی برای بحث و تبادل‌نظر، در مورد موضوعات مرتبط با فضای سایبری ایجاد کرده است. مجمع عمومی سازمان ملل در قطعنامه ۲۰۰۴۱۲۵ بر ایجاد فرهنگ جهانی امنیت سایبری و بررسی تلاش‌های ملی برای حفاظت از زیرساخت‌های اطلاعات حیاتی تأکید می‌کند و مشخص می‌کند که یک حمله سایبری، تهدید یا نقض صلح و امنیت بین‌المللی بر اساس ماده ۴۲ منشور قلمداد می‌شود و باید اقدامات لازم صورت گیرد (Aphrodite, 2010: 34). کمیته مبارزه با تروریسم سازمان ملل متحد در بیانیه دهلی در ۲۹ اکتبر ۲۰۲۲ با نگرانی به افزایش استفاده تروریست و حامیان آن‌ها از اینترنت و سایر فناوری‌های ارتباطی و حمله به زیر ساخته‌های حیاتی و مکان‌های عمومی کشورها، اشاره می‌کند و از همه کشورهای عضو می‌خواهد از طریق اجرای کامل قطعنامه ۱۳۷۳(۲۰۰۱)۱۶۲۲(۲۰۰۵)،۲۱۷۸(۲۰۱۴)،۲۳۹۱(۲۰۱۷) اقدام فوری را برای جلوگیری و مقابله با تروریسم در همه اشکال آن صورت گیرد (The counter Committee, 2022: 1-2). علاوه بر این، سازمان ملل دفتر امور خلع سلاح سازمان ملل متحد (UNODA) را ایجاد کرده است که در راستای جلوگیری از استفاده از فناوری اطلاعات و ارتباطات برای اهداف مخرب کار می‌کند. سازمان ملل همچنین همکاری بین‌المللی و ظرفیت‌سازی در امنیت سایبری را از طریق طرح‌هایی مانند مجمع جهانی تخصص

[1] Unite Nation

سایبری (GFCE) و برنامه ظرفیت‌سازی امنیت سایبری سازمان ملل ترویج می‌کند. هدف این تلاش‌ها تقویت امنیت سایبری، حفاظت از زیرساخت‌های حیاتی و تضمین استفاده صلح‌آمیز و ایمن از فضای سایبری است. مجمع عمومی سازمان ملل چندین قطعنامه مرتبط را تصویب کرده است. در آگوست ۱۹۹۹، سازمان ملل متحد از یک نشست بین‌المللی کارشناسان در ژنو حمایت کرد تا مفاهیم امنیتی فناوری‌های اطلاعاتی در حال ظهور را بهتر درک کنند. این قطعنامه همچنین خواستار مطالعه جدیدی در مورد مسائل امنیت اطلاعات بین‌المللی شد، اما اقدام اندکی حاصل شد (Hathaway, 2012: 48-49) شورای امنیت سازمان ملل سلسله نشست‌های مختلفی در مورد حملات سایبری تشکیل داد در ژانویه ۲۰۲۱ اولین نشست رسمی شورا در مورد تهدیدات سایبری برگزار نمود که اعضا توافق کردند که اجرای هنجارهای موجود، رفتار مسئولانه دولت‌ها در فضای سایبری و اقدامات اعتماد ساز و ظرفیت‌سازی باعث به حداقل رساندن بی‌اعتمادی بین کشورهای عضو و کمک به ثبات سایبری می‌شود. در مارس ۲۰۲۰ شورا درباره حملات سایبری علیه کشور گرجستان تشکیل جلسه داد و در این نشست انگلیس، امریکا و استونی این حملات را متوجه روسیه نمودند که روسیه رد نمود. در ۲۲ مه ۲۰۲۰ شورا دو نشست غیررسمی با موضوع ثبات سایبری، پیشگیری از درگیری و ایجاد ظرفیت‌سازی و اعتمادسازی در فضای سایبری تشکیل داد در این جلسه اوکراین کشور روسیه را به ارتکاب تجاوز ترکیبی متهم نمود و از مکانیسم پاسخگویی برای محاکمه کسانی که عمداً حملات سایبری را سازمان‌دهی و انجام می‌دهند حمایت کرد. در ۲۶ اکتبر ۲۰۲۰ جلسه شورا به ابتکار اندونزی در مورد حملات سایبری علیه زیرساخت‌های حیاتی ترتیب داده شد تا از این طریق آگاهی را در مورد آسیب‌پذیری و نیاز به حفاظت از زیرساخت‌های حیاتی در برابر حملات سایبری افزایش دهد. اعضای شورا سه نشست در ۱۷ مه ۲۰۲۱ با عنوان تأثیر فناوری نوظهور بر صلح و امنیت بین‌المللی تشکیل دادند که در آن به تلاش‌ها برای کاهش خطرات احتمالی ناشی از استفاده از فناوری نوین موردبررسی قرار گرفت، کشور کنیا در ۲۸ اکتبر ۲۰۲۱ یک جلسه شورا را با موضوع بررسی و مقابله با سخنان نفرت‌انگیز و جلوگیری از تحریک به تبعیض، خصومت، خشونت در رسانه‌های اجتماعی را سازمان‌دهی نمود، در ۲۰ دسامبر ۲۰۲۱ جلسه شورا به ابتکار استونی و انگلیس در مورد فعالیت‌های مخرب سایبری تشکیل شد و نماینده عالی خلع سلاح، شورای امنیت را به دلیل مشارکت فزاینده آن در زمینه صلح و جنبه‌های امنیتی فضای سایبری تحسین نمود (Www-securitycouncilreport-org). انبوه جلسات شورا در مورد تهدیدات سایبری به افزایش آگاهی بین اعضای شورا کمک می‌کند.

۲-۲-سازمان پلیس بین‌الملل[۱]

مأموریت اصلی اینترپل این است که آژانس‌های مجری قانون در ۱۹۰ کشور عضو را قادر سازد تا برای جنایات علیه کودکان، مبارزه با جرایم فراملی ازجمله جرایم سایبری با یکدیگر همکاری کنند و به‌عنوان مرکزی برای تبادل اطلاعات و اشتراک‌گذاری اطلاعات، تخصص فنی، آموزش و ظرفیت‌سازی را به‌عنوان خدمتی نیز ارئه دهد. به‌عبارتی‌دیگر این سازمان با همکاری کشورهای عضو، تلاش می‌کند تا با جرائم سایبری مبارزه کند و امنیت سایبری را تقویت کند. اقدامات این سازمان شامل ایجاد تیم‌های تحقیق و پیگیری در زمینه جرائم سایبری، ایجاد پایگاه داده‌ها و اشتراک اطلاعات، برگزاری دوره‌های آموزشی و آماده‌سازی نیروهای پلیس در زمینه سایبری، همکاری با سازمان‌های دیگر و تشکیل اجلاس‌ها و نشست‌های مربوط به امنیت سایبری است. این سازمان همچنین برنامه‌های همکاری بین‌المللی را برای مبارزه با جرائم سایبری ترویج می‌دهد. (تقی زاد و دوستان،۱۳۹۶: ۱۲۰) از دیدگاه نگارنده کشورها می‌توانند از دانش و تجربیات اینترپل در زمینه مقابله با حملات سایبری استفاده نمایند که پیش‌زمینه کاهش آسیب‌های جرایم سایبری است.

[۱] International Criminal Police Organization

۳-۲-سازمان بین‌المللی مخابرات[1]

یک آژانس تخصصی سازمان ملل متحد است که هماهنگ‌سازی استانداردهای فنی برای فناوری‌های ITU و مخابراتی را ترویج می‌کند و همکاری‌های بین‌المللی را برای بهبود امنیت سایبری از طریق دستور کار جهانی در مورد مواد مخدر، مشارکت خود با دفتر سازمان ملل و امنیت سایبری تقویت می‌کند و با یونیسف برای انتشار راهنماهایی در موردحمایت آنلاین از کودکان مشارکت دارند. برای مواجهه با حملات سایبری، سازمان بین‌المللی مخابرات (ITU) اقدامات متعددی را انجام می‌دهد. این سازمان باهدف اعتمادسازی و امنیت در استفاده از فناوری اطلاعات و ارتباطات، توسعه و پیاده‌سازی استانداردها در امنیت سایبری فعالیت می‌کند همچنین، ITU تلاش می‌کند تا همکاری بین کشورها را در جهت مبارزه با جرایم سایبری و تروریسم در حوزه فناوری اطلاعات تقویت کند. از طریق برگزاری کنفرانس‌ها، کارگاه‌ها و برنامه‌های آموزشی، ITU امکانات و ظرفیت‌سازی لازم را برای بهبود امنیت سایبری در دسترس کشورها و سازمان‌های مختلف قرار می‌دهد. (کتان چی و قهرمانی،۱۴۰۰: ۲۴۸) علاوه بر اقدامات فوق در سال‌های اخیر با شدت گرفتن حملات سایبری، این اتحادیه قطعنامه‌هایی در خصوص مبارزه با جرایم سایبری به تصویب رسانده است که نشان از جدیت اتحادیه بین‌المللی ارتباطات با کشورهای عضو در راستای کاهش جرایم سایبری و قانونمند کردن مقررات در بهره‌مندی از فضای امن سایبری است.

۳. اقدامات سازمان‌های منطقه‌ای در برابر حملات سایبری

در دهه اخیر با تشدید حملات سایبری، سازمان‌های منطقه‌ای اقدامات مؤثری در مواجهه با این حملات انجام داده‌اند که ذیل به پاره‌ای از آن‌ها اشاره می‌شود.

۱-۳- اتحادیه اروپا[2]

اتحادیه اروپا در یک رویکرد جدی به ایجاد اسناد الزام‌آور روی آورده است؛ و در این زمینه یک مرکز اروپایی جرایم سایبری تأسیس نموده است. اولویت‌های استراتژیک اتحادیه اروپا در مقابل تهدیدات سایبری عبارت‌اند از:

دستیابی به تاب‌آوری سایبری، کاهش شدید جرایم سایبری، توسعه و تقویت سیاست دفاع سایبری و قابلیت‌های مرتبط با آن، تقویت سیاست مشترک دفاعی و امنیتی، توسعه منابع صنعتی و فناوری برای امنیت سایبری، ایجاد یک سیاست منسجم بین‌المللی فضای مجازی برای اتحادیه اروپا و ترویج ارزش‌های اصلی اتحادیه و ظرفیت‌سازی، سازش سایبری اتحادیه ازجمله اولویت‌های برنامه سایبری اتحادیه اروپا هستند. یکی از بخش‌های مهم برنامه مقابله با تهدیدات سایبری اتحادیه اروپایی، همکاری بیشتر با سازمان‌ها و کشورهای خاص و فعال در مقابل با حملات سایبری است به همین منظور اتحادیه با سازمان نظامی ناتو، آ سه آن، اتحادیه افریقا، سازمان کشورهای آمریکایی روابط نزدیکی دارد و با کشور امریکا اقدام به ایجاد موافقت‌نامه‌های دوجانبه در زمینه مقابله با تهدیدات سایبری و توسعه روابط با این‌گونه کشورها و سازمان‌ها نموده است. در زمینه تدوین مقررات سایبری اولین اقدام آن تدوین اجلاس «بوداپست» 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 پرونده‌های سایبری مورد اعمال قرار می‌گیرد و دولت‌های ثالث می‌توانند به آن ملحق شوند.)Cyber security Strategy of the European Union, 2013:91-94. در زمینه حفاظت از اطلاعات و امنیت شخصی سایبری، کمیسیون اروپا در سال ۲۰۱۳ اصول و اولویت‌هایی را برای تضمین فضای باز، امن و

[1] International Telecommunication Union
[2] European Union

ایمن‌سازی در اتحادیه شناسایی نمود و وظایف و مسئولیت‌هایی را برای نهادها، آژانس‌ها، کشورها و صنعت دانشگاه در اروپا مشخص نمود. در این چارچوب پنج هدف اصلی را طراحی نمود که عبارت‌اند از: انعطاف‌پذیری سایبری که این هدف با توسعه ظرفیت‌سازی و افزایش آگاهی و ایجاد همکاری بین دولتی و بخش خصوصی تحقق می‌یابد و نقطه عطف آن تصویب دستورالعمل امنیت شبکه اطلاعات در سال ۲۰۱۶ انجام گرفت و علاوه بر آن قانون امنیت سایبری خود را در سال ۲۰۱۹ برای تقویت مأموریت آژانس امنیت سایبری که مسئول واکنش به حوادث سایبری در مقیاس بزرگ به تصویب رساند. این آژانس با توجه به مسئولیت آگاهی بخشی که بر عهده داشته، کارگاه‌ها و مشاوره‌های عمومی و خصوصی را خصوص آی سی تی ارائه نمود. کاهش جرایم سایبری یکدیگر از اهداف امنیت سایبری اتحادیه اروپاست که با استفاده از قوانین قوی و مؤثر قابلیت عملیاتی و بهبود هماهنگی در سطح منطقه است که از کشورهای عضو خواسته‌شده کنوانسیون بوداپست را تصویب نمایند و مقدرات آن را با قواعد داخلی هماهنگ نمایند (Bennincasa,2020: 5). شورای اروپا اولین معاهده بین‌المللی در مورد جرایم سایبری با عنوان کنوانسیون جرایم سایبری در سال ۲۰۰۱ تصویب نمود در این کنوانسیون یک سیاست مشترک باهدف حمایت از آحاد جامعه بین‌المللی در برابر جرایم سایبری از طریق وضع قوانین و همکاری بین‌المللی ارائه نمود. حملات سایبری شامل جرایم ذیل کنوانسیون جرایم سایبری مربوط به محرمانه بودن، یکپارچگی دسترسی غیرقانونی به داده‌ها و سیستم‌های رایانه‌ای و اخلال در این‌گونه داده‌ها و سیستم‌ها است. به‌عنوان‌مثال ماده ۲ کنوانسیون از دولت‌های عضو می‌خواهد که هرگونه دسترسی عمدی و غیرقانونی به داده‌ها و سیستم‌های رایانه‌ای را به‌عنوان جرم سایبر در قوانین داخلی خود لحاظ نمایند و هرگونه تهدید سایبری حق دفاع را برای دولت‌ها ضرورت می‌داند. علاوه بر اقدامات فوق، شورای اروپا در سال ۲۰۱۷ چارچوبی به نام جعبه‌ابزار دیپلماسی سایبری را ارائه کرد که بر بهبود همکاری، جلوگیری از درگیری، کاهش تهدیدات احتمالی سایبری و تأثیرگذاری رفتار متجاوزان احتمالی تأکید داشت (Hathaway and others, 2012: 864). اتحادیه اروپا در راستای مقابله با حملات سایبری از همه شرکای خودخواسته تا همکاری بین‌المللی را برای ارتقای امنیت و ثبات در فضای سایبری تقویت کنند. به‌طورکلی اتحادیه اروپا همه ظرفیت‌ها خود و نهادهای تابع را بکار گرفته است.

۲-۳- ناتو[۱]

ناتو اولین سازمان منطقه‌ای است که در زمینه حملات سایبری فعالیت‌های خود را شروع کرد. این سازمان ابتدا در سال ۲۰۰۸ تالین استونی را به‌عنوان مرکز عالی همکاری جهت دفاع سایبری ایجاد نمود و در سال ۲۰۰۹ از گروه کارشناسان مستقل جهت نگارش دستورالعملی در خصوص ایجاد هنجارهای حقوقی حاکم بر جنگ‌های نوین به‌ویژه جنگ‌های سایبری دعوت به عمل آورد. این پروژه حقوقی به دستورالعمل تالین معروف شد و به‌عنوان مهم‌ترین سند حقوقی سازمان ناتو دربرگیرنده حقوق بر جنگ و حقوق در جنگ سایبری است.(Schmitt,2013: 16-19) از مهم‌ترین عواملی که زمینه توجه سران ناتو در باب حوزه سایبر قرار گیرد، آسیب‌پذیری کشورهای عضو ناتو در برابر تهدیدات سایبری و دیگری حملات سایبری روسیه و چین علیه برخی از کشورهای اروپایی ازجمله، حمله سایبری روسیه به مراکز حیاتی کشور استونی و گرجستان، یک سال پس از حمله سایبری به استونی در سال ۲۰۰۸ در نشست ناتو در بوداپست مجارستان پیشنهاد تدوین سند راهبرد سیاست دفاع سایبری ناتو توسط سران مطرح شد و سران ناتو خواهان آن شدند که امنیت سایبری جزء وظایف ناتو قرار گیرد و سپس سند راهبرد دفاع سایبری تهیه و به تصویب سران قرار گرفت. (ترابی،۱۳۹۴: ۱۴۶) چنانچه یکی از کشورهای عضو ناتو در معرض حمله سایبری قرار بگیرد که منجر به خسارات جبران‌ناپذیر شود، ماده ۵ دفاع جمعی پیمان آتلانتیک شمالی فعال می‌شود. بر اساس بند ۵[۲]، ناتو می‌تواند حمله به هر یک از اعضای عضو پیمان آتلانتیک شمالی را حمله به همه اعضا تلقی کند. در سند «ناتو ۲۰۳۰» که چشم‌انداز ۱۰ ساله اهداف و

[۱] North Atlantic Treaty Organization

[۲] – که در آن کشورهای امضاکننده توافق کرده‌اند حمله نظامی علیه یک یا چند کشور عضو را به‌عنوان حمله به‌تمامی کشورهای عضو تلقی کنند و به مقابله آن برخیزند.

رویکردهای پیمان آتلانتیک شمالی را ارائه می‌کند، حملات سایبری هم مشمول بند ۵ شد. مهم‌ترین تغییر در این زمینه پذیرش حمله سایبری در سطح حمله نظامی می‌باشد. در اجلاس سران ناتو در سال ۲۰۱۱، کشورها عضو حملات سایبری را در حکم حمله نظامی ارزیابی کردند و درنتیجه مجوز دفاع سایبری و نظامی، شامل استفاده از نیروهای هوایی، دریایی و زمینی را برای خود محفوظ داشتند. ناتو تغییرات ساختاری، رویه‌ای و فنی در مقابل حملات سایبری ایجاد کرده که سازمان و کشورهای عضو در برابر این تهاجمات انعطاف‌پذیرتر باشند. با توجه به رشد تعداد و شدت حملات، اتحادیه باید توانایی‌ها و تخصص‌های سایبری خود را تطبیق و گسترش دهد (Dims, 2019: 71). به نظر می‌رسد استراتژی قرن بیست یکم ناتو، روی دفاع مشترک در مقابل حملات سایبری و همکاری بیشتر با کشور روسیه است و حتی در اظهارات دبیر کل این سازمان، تأکید فراوانی بر این موضوع شده است.

۳-۳- اکوواس[۱]

سازمان اکوواس در حوزه مبارزه با حملات سایبری اقداماتی را به عمل می‌آورد. اکوواس با اتخاذ قوانین و آیین‌نامه‌های مربوط به محافظت از داده‌های شخصی و مبارزه با جرم سایبری، سعی در آدرس دادن به نگرانی‌های امنیت سایبری دارد. در این راستا، شورای وزیران اکوواس دستورالعملی با عنوان C/DIR.1/08/11 درباره مبارزه با جرم سایبری را تصویب نموده است. دستورالعمل به‌منظور کیفری کردن جرم سایبری و ایجاد اقداماتی برای مقابله با آن در منطقه تعیین می‌کند. در این سند همچنین، نیاز به ایجاد یک مکانیزم پیگیری منطقه‌ای در چارچوب اکوواس را تأکید می‌کند و بر این اساس، برای مسئولیت کشورهای عضو در صورت عدم اجرای این دستورالعمل تأکید می‌کند. همچنین بر طبق اساسنامه ارتقای توسعه اقتصادی هماهنگ بین کشورهای عضو، مستلزم همکاری و یکپارچگی اقتصادی منطقه‌ای مؤثر است. سیاست‌های ملی و ارتقای برنامه‌های ادغام در زمینه‌هایی ازجمله ارتباطات، فناوری و حقوقی. بند یک ماده ۳۵ دستورالعمل جرایم سایبری مقرر می‌دارد که کشورهای عضو اقدامات قانونی، نظارتی و اداری لازم را به‌منظور انطباق با این دستورالعمل حداکثر تا اول ژانویه ۲۰۱۴ اتخاذ خواهند کرد. ماده فوق مشابه ماده ۱۶(۱) دستورالعمل اتحادیه اروپا در سال ۲۰۱۳ است که از کشورهای عضو می‌خواهد با وضع قوانین از این دستورالعمل را به کشورها منتقل کنند (Jerome Orji,2019).

۴-۳- سازمان کشورهای آمریکایی[۲]

سازمان کشورهای آمریکایی در دهه‌های گذشته به‌طور فعال به موضوع حملات سایبری در منطقه پرداخته است. این سازمان جلسات متعددی را در محدوده وظایف وزیران دادگستری یا دادستان‌های کل قاره امریکا برگزار نموده است قبلاً 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 موضوع جرایم سایبری پرداخته‌اند و بر روی تعدادی از توصیه‌ها به توافق رسیدند این کارگروه تاکنون 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، گروه‌های پاسخگویی به حوادث امنیتی رایانه‌ای (CSIRT) در اکثر کشورهای عضو آن، ازجمله شیلی، کاستاریکا و غیره ایجادشده است. همچنین به کشورهایی مانند جامائیکا، ترینیداد کمک کرده است (Neethu, 2020: 12). در نشست ۲۰۰۶ کارگروه سازمان کشورهای آمریکایی توصیه نمود که کشورهای عضو باید همکاری را با شورای اروپا تقویت نمایند بطوری که بتوانند اصول کنوانسیون حملات سایبری شورای اروپا را اجرا نمایند و مکانیسم‌های تبادل اطلاعات همچنان ادامه داشته باشد و علاوه بر آن شورای اروپا با سایر سازمان‌ها و آژانس‌های بین‌المللی همچون سازمان ملل متحد، اتحادیه اروپا، مجمع همکاری اقتصادی آسیا اقیانوسیه و جی هشت در زمینه

[۱] Economic Community Of West African States

[۲] Organization of American States

جرایم سایبری همکاری داشته باشند. در سال ۲۰۰۸ کارگروه (REMJA) سازمان کشورهای آمریکایی خواهان الحاق اعضا به کنوانسیون شورای اروپا در مورد حملات سایبری شد (Sanou, 2012: 23). این همکاری می‌تواند با استفاده از تجربیات دیگر آژانس‌های بین‌المللی سطح دفاعی سازمان را نسبت به حملات سایبری تقویت نماید.

۵-۳- سازمان همکاری شانگهای[۱]

اعضای شانگهای سندی تحت عنوان برنامه اقدام کشورهای عضو در سال ۲۰۰۷ جهت حفاظت از امنیت اطلاعات بین‌المللی امضا نمودند که در این سند مقرر کردند که کشورهای عضو در مواجهه با چالش‌ها و تهدیدات جدید در زمینه امنیت اطلاعات با یکدیگر همکاری نمایند تا به‌طور مشترک و دسته‌جمعی با تهدیدات رو به رشد سایبری مقابله کنند. در اوت ۲۰۰۸ سران کشورهای عضو در شهر دوشنبه تاجیکستان یک بیانیه دیگر به‌منظور 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 تأکید نمودند. در بیانیه «یکاترینبورگ» روسیه، سران کشورهای عضو سازمان همکاری شانگهای امنیت اطلاعات را به‌عنوان یک عنصر کلیدی در امنیت دسته‌جمعی قلمداد نمودند و بر آن تأکید کردند. سازمان در جهت تقویت سیستم سایبری کشورهای عضو در نشست سال ۲۰۰۹ در چین، یک تفاهم‌نامه‌ای 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 چالش‌های سایبری ایمن شوند. در تمام نشست‌های اعضای سازمان بر مبارزه با تهدیدات سایبری تأکید شده است. در برنامه آینده سازمان که به دستور کار ۲۰۳۰ سازمان معروف است که در آن به اهداف توسعه فناوری دیجیتالی، بهبود زیرساخت‌های اطمینان بخشی فضای دیجیتالی پرداخته است در آن به امنیت فضای مجازی و مبارزه با چالش‌های سایبری تأکید ویژه‌ای شده است. سازمان گام‌های زیادی در جهت مقابله با تهدیدات سایبری برداشته است در نشست تاشکند ازبکستان در سال ۲۰۱۵ برای مبارزه با تروریسم سایبری «برنامه مانور مبارزه با تروریسم سایبری» را تصمیم‌گیری نمودند (Hathaway and others, 2012: 865-6).

۶-۳- اتحادیه جنوب شرق آسیا[۲]

اتحادیه جنوب شرق آسیا برنامه‌های مختلفی در راستای مقابله با تهدیدات سایبری در پیش رو داشته است. در چند سال گذشته شاهد پیشرفت‌های پایدار و قابل‌توجهی بوده چراکه سیاست امنیت سایبری را شتاب داده و منجر به ایجاد نهاده‌ای جدید در رابطه با امنیت سایبری شده است (Benincasa, 2020:5). در اولین نشست خود با موضوع تهدیدات سایبری در ۸ ژانویه 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 فراملی اعلام نمودند. «آسه آن» یک طرح اقدام مشترک با کشور چین برای صلح و رفاه به امضا رساند که در آن طرح، بهروش‌های همکاری و واکنش اضطراری، حفظ و افزایش امنیت سایبری و همچنین پیشگیری و مبارزه با حملات سایبری تأکید شده است. علاوه بر آن، آسه آن به همکاری بیشتر از طریق به اشتراک گذاشتن سریع اطلاعات تهدیدی می‌تواند به‌موقع به حملات سایبری واکنش نشان دهد و تأثیر یا گسترش بالقوه یک حمله سایبری را کاهش دهد. در بیانیه مجمع آ سه آن در ژوئیه ۲۰۰۶ به همکاری همه‌جانبه در تمام اشکال در مبارزه با تهدیدات سایبری با سرعت و عملکرد مناسب تأکید نمودند و از دولت‌های عضو خواسته شد قوانین و مقررات بین‌المللی بخصوص توصیه‌های مجمع عمومی سازمان ملل متحد وفق قطعنامه ۶۶/۵۵ در مورد حملات سایبری را با قوانین ملی هماهنگ کنند و از آن‌ها پیروی نمایند و یک قطعنامه روسای پلیس کشورهای عضو آ سه آن در

[۱] Shanghai Cooperation Organization
[۲] Association of Southeast Asian Nation (ASEAN)

سال ۲۰۰۸ در مورد جرایم سایبری تصویب نمودند. آسه آن باوجود پیشرفت‌های حاصل‌شده 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 سازمان‌های منطقه‌ای دیگری نظیر اتحادیه اروپا و ناتو با اتخاذ که یک استراتژیک منسجم و کارآمد منطقه‌ای، توانسته‌اند زمینه‌های دستیابی به اهداف مهم برای افزایش تاب‌آوری سایبری خود را فراهم نموده‌اند و گام‌های مهمی را برداشته‌اند.

۷-۳- سازمان امنیت و همکاری اروپا[۱]

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. بر اساس این تصمیم سازمان از اعضا خواسته است که یک نوع شفافیت در اطلاعات نظامی و یا فعالیت‌های مربوط به کنترل سلاح‌های سبک و سنگین داشته باشند و هرگونه تحرک و مانور نظامی را به اطلاع دیگر اعضا رسانده شود. سازمان امنیت و همکاری اروپا اقدامات اعتمادسازی در فضای مجازی را در فرانسه و سایر کشورهای عضو اجرا نموده است این سازمان با تهدیدات سایبری مختلف ازجمله جرایم سایبری و استفاده از اینترنت برای اهداف تروریستی مقابله می‌کند و تمرکز خود را بر توسعه اقدامات اعتمادسازی برای کاهش خطرات سوءبرداشت و تشدید تهدیدات سایبری با تبادل اطلاعات و ارتباطات بین دولت‌های عضو می‌تواند به خنثی کردن تنش‌های احتمالی و توقف یا کند کردن پیوسته یک درگیری غیرعمدی را متوقف کند (https://www-osce-org). اقدامات اعتماد ساز سازمان امنیت و همکاری اروپا توسط دبیرخانه خود انجام می‌دهد و به‌منظور تقویت ثبات و امنیت در فضای سایبری کشورهای عضو از طریق گفتگو مستمر میان کشورها تأکید می‌کند.

نتیجه‌گیری

این مقاله به نقش سازمان‌های بین‌المللی و منطقه‌ای در مواجهه با حملات سایبری متمرکزشده است. سازمان‌های بین‌المللی و منطقه‌ای نقش بسیار مهمی در ایجاد ثبات در روابط دولت‌ها در فضای مجازی ایفا می‌کنند. سازمان‌های بین‌المللی و منطقه‌ای به‌عنوان یکی از کنش گران عرصه جهانی و منطقه‌ای در جهت موضوع صلح با تهدیدات سایبری مواجهه بوده و در مقابل حملات سایبری توانسته‌اند اقدامات پیشگیرانه‌ای اتخاذ نمایند از این طریق بتوانند تاب‌آوری و توانمندی سازمان و اعضا را تقویت نمایند. اقدامات و تدابیر پیشگیرانه سازمان‌های بین‌المللی و منطقه‌ای در مقابل تهدیدات سایبری متفاوت بوده برخی سازمان‌ها به‌طور ویژه اقداماتی عملی همه‌جانبه و با ایجاد معاهدات بین‌المللی اقدام به وضع قوانین بازدارندگی و تنبیهی در مقابل تهدیدات سایبری نموده‌اند مثلاً سازمان ملل متحد، همکاری بین‌المللی و ظرفیت‌سازی در امنیت سایبری را از طریق طرح‌هایی مانند مجمع جهانی تخصص سایبری (GFCE) و برنامه ظرفیت‌سازی امنیت سایبری سازمان ملل ترویج می‌کند و اتحادیه بین‌المللی ارتباطات باهدف اعتمادسازی و امنیت در استفاده از فناوری اطلاعات و ارتباطات، توسعه و پیاده‌سازی استانداردها در امنیت سایبری فعالیت می‌کند و همچنین سازمان نظامی ناتو که به‌عنوان اولین سازمان منطقه‌ای، با توجه به ماهیت ذاتی نظامیش اقدامات خاصی در مقابل تهدیدات سایبری انجام داده است و جنگ سایبری را هم‌سطح جنگ نظامی ارزیابی نموده است و بر اساس 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 تاکنون در برابر تهدیدات سایبری تدوین نکرده است. سازمان امنیت و همکاری اروپا به

[۱] Organization for Security and Co-operation in Europe

استراتژی اعتمادسازی برای جلوگیری از درگیری‌های سایبری تأکید نموده است. اکوواس با اتخاذ قوانین و آیین‌نامه‌های مربوط به محافظت از داده‌های شخصی و مبارزه با جرم سایبری، سعی در آدرس دادن به نگرانی‌های امنیت سایبری، سازمان کشورهای امریکای هم اقداماتی مانند از طریق مداخله، گروه‌های پاسخگویی به حوادث امنیتی رایانه‌ای جهت جلوگیری و کاهش خطرات حملات سایبری انجام دادند. با اجرای اقدامات مناسب و همکاری‌های منطقه‌ای می‌توان فضای سایبری را برای میلیاردها انسان فضایی امن و قابل‌اعتماد تبدیل کرد.

منابع

۱. انصاری مهیاری، علیرضا، سادات حسینی، زهرا. (۱۴۰۱). حملات سایبری در پرتوی توسل به‌زور از نگاه حقوق بین‌الملل فصلنامه مطالعات حقوقی فضای مجازی، سال اول، شماره،۱۸.

۲. مشیر زاده، حمیرا. (۱۳۸۸). حول در نظریه‌های روابط بین‌الملل، تهران، نشر سمت.

۳. انصاری مهیاری، علیرضا، محمودی، هادی. (۱۴۰۱). «بررسی راه‌کاری‌های تقلیل حملات سایبری از منظر حقوق بین‌الملل بشردوستانه»، فصلنامه مطالعات حقوقی فضای مجازی، سال اول، شماره ۳.

۴. ترابی، قاسم. (۱۳۹۴). «تکامل ناتو در قبال جنگ سایبری؛ دلایل؛ ابعاد و مؤلفه‌ها»، فصلنامه مطالعات راهبردی، سال هیجدهم، شماره اول، مسلسل ۱۳۳.

۵. تقی زاد، مهرداد، زمرد، کیوان، حاجیان، مهدی. (۱۳۹۶). «نقش اتحادیه اروپا در قاعده‌مند سازی جرائم سایبری»، فصلنامه مطالعات بین‌المللی پلیس، سال هفتم، شماره،۱۰۴.

۶. دزیانی، زهرا. (۱۳۸۳). «مقدمه‌ای بر ماهیت و تقسیم‌بندی تئوریک جرایم سایبری» خبرنامه انفورماتیک، شماره ۸۷

۷. ضیایی، محسن. (۱۳۹۷). «نقش و عملکرد سازمان‌های بین‌المللی در تأمین صلح جهانی»، مجله بین‌المللی پژوهش ملل، دوره سوم: شماره،۷۵.

8. Abhishek Kumar Singh. (2016). Jurisdictional Issues in Cybercrime: An Analytical Study
9. University of Luck now,
10. Abase Mohammad. (2021). Security in cyber space in the field of international Relations" Journal of Archives in Military medicine: Vole, 8, issue 4.
11. Benincasa Eugenio. (2020). The rile of regional organizations in building cyber resilience:
12. ASEAN and EU, Issues insights, working paper, vole, 20.wp3.
13. 11. Beidleman Scott w. (2009). Defining and Deterring cyber war" USAWC strategy Research
14. Project, PA17013-5050.www.indianstrategicknow ledgeonline.com.
15. 12. Dismal Carlo. (2019). The evolving cyber warfare landscape" www.jstor.org.
16. 13. Finkelstehn, Claire, Govern, Kevin H. (2015). "Cyber and the changing Face of war" Faculty scholarship at Penn Carey Law.
17. 14. Jerome Orji, Uchenna. (2019). An inquiry into the legal status of the Ecowas cybercrime directive and the plication's of its obligations for member states" Computer Law & Security Review, Volume 35, issue 6, https://doi.otg/10.1016/j.clsr. 2019.06.0
18. 15. Hathaway Oona, others. (2012). The Law of cyber-Attack" Vole 100, No,4. https://www.jstor.org/stable/232498823.
19. 16. Levinson, Paul. (2020). "Micro cyber war VS. Macro-cyber war: towards the beginning of afaxonomy" Digital war 1.
20. 17. 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,
21. http://creativecohmons.org.
22. 18. Lilli Eugenio. (2023). How can we know what we Think we Know about cyber operation?
23. 'Journal of Global security studies, Volume, 8, issue, 2.
24. 19. K Lukas, Timothy j Elves, frank j, Evans, cilluffo, Alec a Neadeau. (2016). European Union and Nato Global cyber security challenge: A Way Forward" Vole, 6, No 2, www.jator.org/stable/26470452
25. 20. Kavanagh Stephen. (2021)."African cyber Herat Easement Report" www.interpol.int.
26. 21. Marie Louise, Deveanny Joe. (2023). Raising the Political of cyber security in Latin America" www-cfr-org.
27. 22. Mawgoud Ahmed A. (2020)."Cyber Security Rests in Mena Region: Threats, challenges and counter measures" A. E. Hassanienet al. AISC, 1058,
28. 23. Meltzer Nils. (2011). "Cyber warfare and international law" ideas for peace and security.
29. 24. 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.
30. 25. Molyakov, Andrei. (2021). "The information and PSY wars of the future: Chinese cyber troops" Journal of scientific-Technical Research, volume 33, issue, Dole: 10.26717/bestir.
31. 26. Neethu N. (2020). Role of international organization in prevention of cybercrimes an
32. Analysis" https://www.researchgate.net/publication/350525198.
33. 27. Oakley, John T. (2013). cyber warfare: china's strategy to Dominate in cyber space"www.jstor.org
34. 28. Obi, Festus C, Oludere, Alaba M.(2022). Taming the shrew of rising cyber warfare" Open Access Library journal,

35. Volume 9. https://doi.org/104236/oalib.1109003
36. 29. Papanastasiou Aphrodite. (2010). Application of international law in cyber warfare operations"https://ssrn.com
37. 30. Rohith, cheerala, Singh bath, ranbir. (2019). "cyber warfare: Nations cyber conflict cyber cold war between nations and its repercussion"
31. Saroha Rashmi. (2014). Proflingacyber criminal" international journal of in formal and computation Technology, Issn0974-2239, Velum 4, Number3.
38. 32. Sanou Brahma. (2012). Cybercrimes/e-crimes: Assessment Report" HIPCAR, www.itu.int.
39. 33. Schmitt, Michael N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare, New York, Cambridge University Press,
40. 34. WA lid Mahmoud Khalid. (2013). Cyber-attacks: The Electronic Battlefield" www.dohainstitute.org.
41. 35. Walter Dom A, Webb Stewart. (2019). "New Ways to prevent and manage cyber-attacks" International journal of cyber warfare and Terrorism, Volume 9, issue 1.
42. 36. "The Role of Regional organizations in strengthening cyber security and stability". (2022). www.diplomacy-edu.\
37. "Cyber war: the challenge to National security" Global security studies, winter (2013), Vole 4, issue 1.
43. 38. United Nations Office on Drugs and Crime, *Cybercrime Trends* (Nov. 27, 2020, 06:15 PM), 39. United nationals institute for Disarmament research 8. (2019). The center for strategic and international states"
44. 40. ASEAN cyber security cooperation strategy, 2021-2025(draft), www.asean.org