journal iranian political sociology

Vol. 4, No.4, winter2022

Abstract

In this research, using the descriptive-analytical method, we aimed to investigate the cyber attacks of terrorist groups from the perspective of international law and with a view to the performance of the United Nations. Due to the fact that cyber attacks are not mentioned in any of the international law documents, the need to investigate these attacks by terrorist groups as a new means and method of warfare in the current era is strongly felt. The importance of this becomes more apparent when the irreparable effects of these attacks on critical civilian infrastructure are examined. If terrorist groupsUsing the Internet to carry out cyber attacks and these attacks have a minimum level of severity and create effects in the form of injury, death, damage or destruction, it is considered as an armed conflict, so what measures should the United Nations take for Dealing with cyber attacks by terrorist groups? The United Nations, by issuing resolutions and the work of various groups, is trying to create security in the cyber space by not giving the internet to terrorist groups by governments and preventing cyber attacks by these groups.It is raised.

Keywords: cyber attacks, United Nations, armed conflict, terrorism

فصلنامه علمی (مقاله علمی ـ پژوهشی)جامعه شناسی سیاسی ایران، سال چهارم، شماره چهارم (پیاپی ۱۶)زمستان ۱۴۰۰،صص ۹۰۳ -۸۹۱

حملات سایبری گروههای تروریستی از منظر حقوق بین الملل و با نگاهی به عملکرد سازمان ملل متحد

محمدعلی کشور [۱]

دکتر علی مشهدی (نویسنده مسئول) [۲]

تاریخ دریافت :۲۲ /۱۴۰۰/۰۳

تاریخ پذیرش: ۱۴۰۰/۰۵/۲۵

چکیده

در این پژوهش با استفاده از روش توصیفی – تحلیلی در صدد بررسی حملات سایبری گروههای تروریستی از منظر حقوق بین الملل و با نگاهی به عملکرد سازمان ملل متحد برآمدیم. با توجه به اینکه در هیچ یک از اسناد حقوق بین الملل به حملات سایبری اشاره ای نشده است، لزوم بررسی این حملات توسط گروه های تروریستی به عنوان ابزار و شیوه نوین جنگی در دوران حاضر، به شدت احساس می گردد. اهمیت این امر زمانی آشکارتر می شود که آثار جبران ناپذیر این حملات بر زیرساختهای حیاتی غیرنظامی مورد بررسی قرار گیرد. چنانچه گروه های تروریستی با استفاده از اینترنت اقدام به حملات سایبری نمایند و این حملات از حداقل سطحی از شدت برخوردار بوده و آثاری در قالب جراحت، مرگ، خسارت و یا نابودی ایجاد نمایند، به عنوان یک مخاصمه مسلحانه تلقی می گردد، لذا سازمان ملل متحد چه اقداماتی برای مقابله با حملات سایبری گروه های تروریستی انجام داده است؟ سازمان ملل متحد نیز با صدور قطعنامه ها و کار گروه های مختلف درصدد ایجاد امنیت در فضای سایبری از طریق عدم در اختیار گذاردن اینترنت توسط دولت ها به گروه های تروریستی و جلوگیری از حملات سایبری توسط این گروه های برآمده است.

کلمات کلیدی: حملات سایبری، سازمان ملل متحد، مخاصمه مسلحانه، تروریسم

[۱]دانشجوی دکترای تخصصی، گروه حقوق، واحد قم، دانشگاه آزاد اسلامی، قم ایران.

[۲]دانشیار،گروه حقوق، دانشگاه قم، قم، ایران

مقدمه

ماهیت تهدید تروریسم پیش روی جامعه در ۲۰ سال گذشته به طور قابل توجهی تغییر کرده است. با آشکار شدن فناوری‌ها و فرصت‌های جدید برای سازمان‌های تروریستی، نوع تهدید همچنان تغییر خواهد کرد و تروریسم سایبری نمونه‌ای از مرزهای جدید در حال توسعه می باشد. از طرفی هیچ تعریف پذیرفته شده جهانی از تروریسم سایبری وجود ندارد که فقدان آن هم یک مسئله و هم چالش در مقابله با تهدیدات تروریسم سایبری است. زیرساختی حیاتی مانند تاسیسات برق، خدمات تصفیه آب، و سیستم‌های بهداشتی و اضطراری به صورت آنلاین در دسترس هستند. هر روز تهدیدات سایبری پیشرفته تر می شوند.

چنین حملاتی، اگرچه به ندرت علنی می‌شوند، اما بیشتر اتفاق می‌افتند. عاملان بالقوه اقدامات تروریسم سایبری را می توان به پنج دسته تقسیم کرد: جنایات سازمان یافته، هکرها، گروه های تروریستی غیردولتی، گرگ های تنها، و دولت های ملی. اگرچه انگیزه‌ها، توانایی‌ها و اولویت‌ها در گروه‌ها متفاوت است، اما هر کدام می‌توانند در مقیاس جهانی ویران کننده و حملات می توانند فاجعه بارتر شوند.

از آنجایی که تروریسم سایبری شامل استفاده واقعی از خشونت فیزیکی برای آسیب رساندن به افراد بی گناه نیست، بیشتر افراد از معنای آن و میزان خطرناک بودن آن بی اطلاع هستند؛ با تغییر مداوم به سمت خدمات آنلاین برای کاهش هزینه ها و بهبود کارایی و پیشرفت های مستمر در فضای مجازی، راه های روزافزونی برای به خطر افتادن سیستم های فناوری اطلاعات وجود دارد. در حالی که ما به شنیدن حملات سایبری عادت کرده ایم تروریسم سایبری نوع دیگری از نگرانی را القا می کند.

گروه های تروریستی در آینده بیشتر اقداماتشان را در فضای سایبری متمرکز و روندها نشان می‌دهد که توانایی آنها برای انجام حملات مخرب سایبری در آینده افزایش می‌یابد. اگرچه تاکنون به دلیل نداشتن مهارت‌های فنی لازم موفق به انجام حمله سایبری عمده‌ای نشده و در حال حاضر توانایی برای چنین حملاتی محدود است و از فضای سایبر بیشتر توسط تروریست ها برای تامین مالی خود، استخدام تروریست، گسترش محتوای خشونت آمیز افراطی، آموزش تروریست های دیگر، برنامه ریزی و هدایت حملات تروریستی و تبلیغات استفاده می‌شود. مطالعات همچنین نشان داده اند که شهرت گروه های تروریستی بدون اینترنت و دستیابی به اتصال باند پهن ممکن نبوده است.

علاوه بر این، باید توجه داشت که در بسیاری از مواقع، پس پرده حملات سایبری گروه های تروریستی نیز دولت های ملی قرار داشته که به عنوان حامیان این گروه ها، امکانات زیرساختی فضای سایبری را در اختیار این گروه‌ها قرار می دهند. سازمان ملل متحد به عنوان سازمان جهانی که تمامی دولت ها عضوی از آن می باشند، می تواند با صدور قطعنامه های الزام آور و یا توصیه ای و تدوین کنوانسیون های بین المللی و الزام دولت ها در پیوستن به این کنوانسیون ها نقش مهمی در جهت ایجاد امنیت و مقابله با تهدیدات تروریستی در فضای سایبری داشته باشد. لذا سوالی که در این مقاله به آن می پردازیم این است که، سازمان ملل متحد چه اقداماتی برای امنیت فضای سایبری و مقابله با حملات سایبری گروه های تروریستی انجام داده است؟ بنابراین لزوم دخالت سازمان ملل متحد برای حمایت از قربانیان بی گناه در مقابل حملات سایبری و ایجاد امنیت لازم در

فضای سایبری می تواند نقش تعیین کننده ای در توسعه و پیشرفت کشورها و جلوگیری از فقر و مقابله با افراط‌گرایی و پیوستن جوانان به گروه های تروریستی ایفا نماید.

حملات تروریستی سایبری

در گزارش ریسک‌های جهانی که انجمن جهانی اقتصاد در سال ۲۰۱۸ منتشر کرده سومین تهدید بزرگ جهانی، بعد از بلایای طبیعی و تغییرات آب و هوایی، حملات سایبری معرفی شده است؛ در این گزارش آمده، حملات سایبری در جهان در حال افزایش است و احتمال حمله به سیستم‌های ارتباطی صنعتی و زیر ساخت‌های حیاتی یک تهدید جدی است.(فورست[1]، ۲۰۱۸، ص۱)

از جمله حملات سایبری مهم ویروس استاکس‌نت بود که در سال ۲۰۱۰ با هدف تحت تأثیر قرار دادن تاسیسات و تجهیزات غنی سازی اورانیوم ایران به وقوع پیوست؛ اهمیت این ویروس به گونه‌ای بود که برخی از آن به منزله سلاح سایبری که می‌تواند آثاری فیزیکی داشته باشد، نام می‌برند.(رضایی[2]، ۲۰۱۳، ص۱۴۱)

دستورالعمل تالین[3] نخستین تلاش جامع برای تحلیل کاربرد حقوق بین الملل در جنگ سایبری است که توسط یک تیم بین المللی از کارشناسان حقوقی و به درخواست مرکز عالی دفاع سایبری سازمان همکاری ناتو و با همکاری کمیته بین المللی صلیب سرخ در سال ۲۰۱۳ تدوین شده است. اگرچه مقررات این مجموعه الزام آور نیستند، اما می توان گفت درواقع حاصل وفاق عمومی دولتها در این زمینه بوده است و یقیناً در آینده به ایجاد معاهداتی الزام آور در حوزه حقوق بین الملل بشردوستانه و حملات سایبری، کمک شایانی خواهد نمود. در این دستور العمل حمله سایبری، عملیات سایبریِ تهاجمی یا تدافعی است که از آن به‌طور معقول انتظار ایراد صدمه، یا مرگ اشخاص و یا وارد کردن خسارت به اشیا می‌رود.(دستورالعمل تالین، ۲۰۱۳، ص۱۰۶)

گروه داعش یکی از گروه های تروریستی است که از بستر فضای مجازی در راستای تحقق اهداف خود استفاده می‌کند؛ این گروه از شبکه‌های اجتماعی توییتر و یوتیوب به عنوان ابزاری برای عضوگیری و اهداف تبلیغاتی بهره می‌برد؛ چرا که امکان اثرگذاری بر کاربران توئیتر، فیس بوک، یوتیوب و سایر شبکه‌های اجتماعی به دلیل سرعت بالای انتشار فیلم، عکس، تصاویر و پیام از طریق اشتراک گذاری و روش‌های مشابه، فراهم است و این امر برای داعش بسیار مهم است. داعش از طریق اینترنت و شبکه‌های اجتماعی با انتشار عمومی گزارش‌های دوره‌ای و انتشار تصاویری از پیشرفت‌های گروه در عرصه نظامی و میدانی به زبان‌های مختلف از جمله عربی، انگلیسی، آلمانی، فرانسه و روسی دست به تبلیغات می زند.(کلوزن[4]،۲۰۱۵، ص۸) همچنین داعش از طریق رسانه‌های اجتماعی و شبکه‌های اینترنتی، تمام عملیات‌های فیزیکی در عراق و سوریه را کنترل و فرماندهی می کند. مثلاً در طی عملیات داعش برای اِشغال موصل عراق در سال ۲۰۱۴، رهبران داعش از یک حمله گسترده تبلیغاتی شامل ۴۰۰هزار توییت، برای هدایت عملیات وآگاهی از وضعیت منطقه استفاده کردند.(گزارش

[1] - Forrest
[2] - Khalaf Rezaei
[3] - TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE
[4] - Klausen

تاکتیک‌های تهدید[1]، ۲۰۱۴، ص ۲۱) در ژانویه ۲۰۱۵ داعش، حساب توییتر و یوتیوبِ فرماندهی مرکزی آمریکا را هَک و اسنادی که شامل اسامی و آدرس مقامات نظامی ایالات متحده بود، منتشر کرد و در پیام توییتری اظهار داشت که "ما متوقف نخواهیم شد، ما همه چیز را درباره شما، همسر و فرزندان تان می دانیم"(گزارش تاکتیک-های تهدید، ۲۰۱۶، ص۱).

مبحث اول: حملات سایبری و منشور سازمان ملل

بند چهار ماده دو منشور ملل متحد نقش کلیدی و اصلی در قوانین حقوق بین الملل مربوط به توسل به زور ایفا می نماید. طبق این بند:

«کلیه اعضا می بایست در روابط بین المللی خود، از تهدید یا توسل به زور علیه تمامیت ارضی یا استقلال سیاسی دیگر دولتها یا سایر شیوه های ناسازگار با اهداف منشور ملل متحد، خودداری نمایند »یکی از اهداف و مأموریتهای مهم سازمان ملل متحد، حفظ صلح و امنیت جهانی است. این هدف در بند یک ماده یک منشور ملل متحد نیز صریحاً ذکر شده است. بنابراین هرگونه تهدید یا توسل به زوری که ثبات بین المللی را در معرض خطر قرار دهد، تحت شمول بند ۴ ماده ۲ قرار می گیرد.

عبارت «سایر شیوه ها» درواقع هر نوع توسل به زوری که در منشور مجاز دانسته نشده را در بر گرفته و نبایستی قید «تمامیت ارضی یا استقلال سیاسی»را به عنوان محدودیتی بر قلمروی بند چهار ماده دو تلقی کرد. درواقع عبارت «سایر شیوه های ناسازگار با اهداف منشورملل متحد» در بخش آخر جمله یک ممنوعیت همه جانبه نسبت به هرگونه تهدید یا توسل به زور در هر شیوه ای مخالف با اهداف منشور ملل متحد، وضع می نماید. با توجه به این تفاسیر حملات رایانه ای نیز، صرف نظر از ابزار و شیوه به کار گرفته شده، چنانچه تمامیت ارضی یا استقلال سیاسی دولتها را تهدید نمایند، و یا به عنوان توسل به زور محسوب گردند، طبق بند چهار ماده دو غیرقانونی می باشند.(اشمیت، ۱۹۹۹)

از طرفی همانطور که دیوان در قضیه نیکاراگوئه اعلام نمود، ممنوعیت توسل به زور نه تنها یک اصل حقوق بین الملل عرفی است، بلکه یکی از اصول اساسی و زیربنایی قوانین عرفی نیز می باشد. لازم به ذکر است که ممنوعیت توسل به زور طبق بند چهار ماده دو تنها در «روابط بین المللی» بین دولتهای عضو حاکم است و در درگیری های داخلی نمی توان به این اصل استناد نمود.(دیوان بین‌المللی دادگستری، ۱۹۸۶)

در نهایت باید توجه داشت که ممنوعیت توسل به زور حقوق عرفی، به صورت بالقوه، از قلمرو گسترده تری نسبت به بند چهار ماده دو برخوردار است، اما شکل گیری و تکامل آن به روشی دشوار، یعنی از طریق رویه دولتی و اجماع حقوقی صورت می پذیرد. از طرفی متن منشور و سایر قوانین تفسیری آن، مجموعه ای از محدودیتهای خاص را بر بند چهار ماده دو وضع می نمایند، به گونه ای که اعمال آن در حملات رایانه ای را با دشواری هایی روبه رو می سازد. بنابراین این احتمال وجود دارد که در آینده، قواعد حقوق بین الملل عرفی مختص حملات رایانه ای و توسل به زور ایجاد گردد. با این حال، در حال حاضر، شواهد چندانی بر این امر موجود نیست.(دینیس، ۲۰۱۲)

[1]- Threat Tactics Report: Islamic State of Iraq and the Levant

حملات سایبری به مثابه مخاصمه مسلحانه

باراک اوباما، رئیس جمهور سابق ایالات متحده آمریکا، در هفدهم ماه می سال ۲۰۱۱، دستورالعملی را امضا کرد که به موجب آن، اقدامات تخریبی علیه شبکه ها و سامانه های رایانه ایِ نهادهای این کشور از سوی دیگر کشورها یا گروه های غیردولتی، اقدام جنگی[1] محسوب شده، نیروهای آمریکایی مجاز خواهند بود با حمله نظامی و با استفاده از تسلیحات جنگی، به کشور یا گروه حمله کننده پاسخ دهند. بر اساس این راهبرد، که پیش نویس آن را وزارت دفاع آمریکا تهیه کرده، بزرگ ترین دارنده ی نیروهای نظامی و تسلیحات جنگی در جهان مجاز خواهد بود از نیروهای نظامی سنتی و سلاح های جنگی خود برای پاسخگویی به حملات سایبری استفاده کند. این راهبرد را «استراتژی بین المللی برای فضای سایبر» نامیده اند.(www.securitynewsdaily.com) همانطور که بیان شد ایالات متحده آمریکا هر حمله سایبری را به معنای اقدام جنگی در نظر گرفته که با قوای نظامی بدان پاسخ می دهد.

حال این سوال پیش می آید که آیا حمله سایبری از طرف یک دولت یا گروه تروریستی یک حمله مسلحانه تلقی می گردد؟

طبق ماده ۳۵ دستورالعمل تالین:

«عملیات های سایبری که در ضمن یک مخاصمه مسلحانه انجام می شوند تحت شمول قوانین مخاصمات مسلحانه قرار می گیرند؛ صرفنظر از اینکه خود این عملیاتها توسل به نیروهای مسلح تلقی گردند یا خیر». (اشمیت، ۲۰۱۳)

همانطور که می دانیم اصطلاح نیروهای مسلح به شکلی گسترده تفسیر می گردد و گونه های مستقیم و غیرمستقیم اعمال زور را در بر می گیرد. بنابراین چنانچه حملات رایانه ای توسط نیروهای مسلح یا ارگانی دولتی صورت بگیرند و به صورت مستقیم یا غیرمستقیم خسارات فیزیکی در ابعاد وسیعی ایجاد نمایند و یا منجر به آسیب به افراد و یا مرگ ومیر آنها شوند، به گونه ای که این آثار مشابه با آثار ناشی از حملات متداول باشند، می توان گفت یک مخاصمه مسلحانه شکل گرفته است.(والو، ۲۰۱۴)

نکته دیگری که باید به آن توجه داشت این است که در مخاصمات داخلی چنانچه حمله توسط یک گروه مسلح انجام شود، چه حمله رایانه ای باشد و چه نباشد، باید بخشی از یک سلسله حملات بلند مدت و متوالی باشد تا بتوان اطمینان حاصل کرد که حمله مورد نظر، نوعی از اعمال خشونت آمیز پراکنده یا منفرد نبوده است و از حداقل شدت برای ایجاد یک مخاصمه مسلحانه داخلی برخوردار است.(آیالو، ۲۰۱۴)

حقوق بین الملل تمایزی جدی بین اعمال زور مسلحانه و تحمیل سختی یا رنج و عذاب صرف به یک حکومت یا جمعیت قائل می شود. به این معنا که حملات رایانه ای که صرفاً منجر به اذیت و آزار و ایجاد دشواریهای خاص می گردند، در حدی نیستند که با یک مخاصمه مسلحانه برابری نمایند.(دینشتاین، ۲۰۰۴)

---

[1]- act of war

اشمیت معتقد است با توجه به هدف قواعد بشردوستانه، زمانی می توان گفت یک مخاصمه مسلحانه شکل گرفته است که گروهی اقداماتی انجام دهند که منجر به کشته شدن و جراحت افراد و خسارت و نابودی اموال گشته و یا هدف از اقدامات آنها ایجاد چنین نتایجی باشد و یا این نتایج آثار قابل پیشبینی آن اعمال باشند. با توجه به این معیار، به نظر او، یک حمله رایانه ای گسترده علیه سیستم کنترل ترافیک هوایی توسط یک دولت، منجر به اعمال قواعد حقوق بشردوستانه می شود. درحالی که حمله رایانه ای علیه اینترنت یک دانشگاه و از کار انداختن موقت آن و یا دانلود سوابق مالی آن منجر به اعمال این قواعد نمی گردد؛ چراکه نتایج قابل پیشبینی این حمله شامل آسیب، مرگ، خسارت و نابودی نیست.(اشمیت، ۲۰۰۲)

ممکن است یک تکنیک ترکیبی به جهت افزایش تأثیر حملات متداول بسیار مورد توجه گروه های مسلح قرار گرفته شود. بدین نحو که همزمان با یک حمله کوچک متداول به یک شهر، حملات رایانه ای گسترده ای نیز صورت گیرد که منجر به قطع کامل برق همه زیرساخت های حیاتی همچون تأسیسات آبرسانی، بیمارستانها، کنترل ترافیک و غیره گردد، آثار این حمله چند برابر خواهد شد. به نظر می رسد با توجه به آثار و عواقب گسترده این حملات ترکیبی، این نوع حملات، مخاصمه مسلحانه محسوب گردد.(دینیس، ۲۰۱۲)

بنابراین به نظر می رسد که قواعد حقوق مخاصمات مسلحانه، تنها زمانی نسبت به حملات رایانه ای صورت گرفته توسط دولتها و یا در مخاصمات مسلحانه داخلی، توسط گروههای سازمان یافته مسلح و یا گروه های تروریستی اعمال می گردند که آثار و عواقب فیزیکی در قالب مرگ ومیر و جراحت افراد یا نابودی و خسارت به اموال ایجاد نمایند. درواقع، حملات باید از حداقل سطحی از شدت و جدیت برخوردار باشند.

اقدامات سازمان ملل متحد در مبارزه با حملات تروریستی سایبری و امنیت فضای سایبری

توجه بین المللی به امنیت سایبری طی سال های اخیر به طور چشمگیری افزایش یافته است زیرا فضای مجازی به زیر ساخت مرکزی جهان تبدیل شده است. این امر امکان توسعه و رشد را ایجاد اما در عین حال فرصت های گسترده ای را برای منازعات و ارتکاب جرایم فراهم نموده است. کشورها اهمیت فضای سایبر را درک کرده اند و همراه با آن، نیاز به همکاری جهانی برای ایجاد ثبات و امنیت بیشتر دارند. (KriangsakKittichaisaree, Public International Law of Cyberspace, 2017, p209)

امروزه حملات گروه های تروریستی برای خراب کردن زیرساخت های مهم ملی مانند انرژی، سیستم های حمل و نقل، آب، تأسیسات دولتی، مراقبت های بهداشتی یا ارتباطات، باعث نگرانی بیشتر کشورهای عضو سازمان ملل شده است. گروه های تروریستی، توانایی های سایبری تهاجمی را برای ارتکاب، تحریک، استخدام، یا برنامه ریزی اقدامات تروریستی به طرق ۱- حملات سایبری به زیرساخت های مهم ۲- پخش محتوای تروریستی به صورت آنلاین ۳- ارتباطات تروریستی آنلاین ۴- تأمین مالی تروریسم دیجیتال انجام می‌دهند، پس ایجاد امنیت نیازمند همکاری عمل شرکت‌های ارائه‌کننده خدمات اینترنتی می‌باشد؛ پس کنترل مؤثر دولت بر شرکت های ارائه‌کننده خدمات اینترنتی که در حمله سایبری مشارکت دارند بسیار حیاتی می باشد، چرا که

فصلنامه علمی (مقاله علمی – پژوهشی) جامعه شناسی سیاسی ایران، سال چهارم، شماره چهارم (پیاپی ۱۶)، زمستان ۱۴۰۰

منجر به مسئولت دولت ها خواهد گردید. این امر به سازمان ملل نقش اساسی در رسیدگی به مسئله اعتماد و امنیت می بخشد و اهمیت چارچوب سازمان ملل برای رفتار مسئولانه دولت ها در فضای سایبر را برجسته می کند.

اقدامات مجمع عمومی سازمان ملل متحد

قطعنامه ۶۰/۲۸۸ [1] در ۸ سپتامبر ۲۰۰۶ با یک ضمیمه به عنوان استراتژی جهانی مبارزه با تروریسم سازمان ملل، با اجماع به تصویب مجمع عمومی رسید.(https://undocs.org/en/A/60/PV.99) این قطعنامه مهمترین قطعنامه مجمع عمومی در زمینه مبارزه با تروریسم می باشد. پس از تصویب این قطعنامه در مجمع عمومی، در تمامی قطعنامه های شورای امنیت نیز از آن نام برده شده است. این استراتژی به مقابله با استفاده از اینترنت برای مقاصد تروریستی و استفاده از اینترنت به عنوان ابزاری برای مقابله با گسترش تروریسم پرداخت.

دفتر کارگروه اجرای مبارزه با تروریسم (CTITF[2]) یک مکانیسم بین سازمانی سازمان ملل متحد است که توسط دبیر کل برای ترویج اجرای استراتژی ایجاد شد و منجر به گام‌های کوچکی با هدف تعمیق درک مسائل و حمایت از دولت‌ها در تلاش‌هایشان برای مقابله با تهدیدات مرتبط با تروریست‌ها، از جمله از طریق استفاده از فناوری اطلاعات و ارتباطات شد[3]. گروه کاری[4] از آن زمان «مجموعه جنبه‌های حقوقی و فنی مقابله با استفاده از اینترنت برای مقاصد تروریستی» را تدوین کرده است که ابزارها (قوانین و کنوانسیون‌ها)، برنامه‌ها، منابع و ابزارهای فنی مورد استفاده دولت‌ها برای مقابله با استفاده از اینترنت برای مقاصد تروریستی و شناسایی مناطقی که ممکن است در آینده تعامل لازم باشد.

همچنین نگرانی جامعه بین المللی در این زمینه، موجب شد از سال‌های ۱۹۹۸ مجمع عمومی ملل متحد آغاز به تصویب قطعنامه های سالانه نماید و تأکید کند که فناوری اطلاعات بالقوه می تواند برای مقاصدی مغایر حفظ ثبات و امنیت بین المللی به کار گرفته شود. مجمع عمومی در قطعنامه ۵۸/۳۲ [5] از دبیر کل درخواست کرد تا گروهی متشکل از گروه کارشناسان دولتی در توسعه اطلاعات و ارتباطات از راه دور در بستر امنیت بین المللی سازمان ملل متحد(GGE)را تحت نظر کمیته نخست شورای امنیت (کمیته خلع سلاح و امنیت بین المللی) برای پیشبرد رفتار مسئولانه دولتها در فضای سایبری در چارچوب امنیت بین المللی تشکیل دهد. این کار گروه که متشکل از ۲۵ عضو بود، از زمان آغاز به کار در سال ۲۰۰۴ تاکنون ۶ کارگروه تشکیل داده است و آخرین کارگروه، کار خود را در ماه مه ۲۰۲۱ با تصویب یک گزارش به اتفاق آراء به پایان رسانید.

براساس گزارش ۲۴ ژوئن ۲۰۱۳ این گروه، امنیت سایبری می بایست دوشادوش احترام به حقوق بشر و آزادی های بنیادین مندرج در اعلامیه جهانی حقوق بشر و سایر اسناد بین المللی توسعه یابد و دولت ها می بایست بر

---

[1] - A/RES/60/288

[2]- United Nations Counter-Terrorism Implementation Task Force

[3] - دفتر CTITF پس از بررسی دوم استراتژی جهانی در سال ۲۰۰۸ در داخل واحد امور سیاسی (DPA) تأسیس شد. وظیفه آن هماهنگی فعالیت‌های شش ناظر نهادهای عضو آن و تسهیل همکاری و اشتراک اطلاعات بیشتر در مورد فعالیت های ضد تروریسم بین آنها بود. علاوه بر این، دفتر CTITF همچنین به یک نقطه کانونی برای کشورهایی تبدیل شد که درخواست کمک برای اجرای استراتژی داشتند.
See Chowdury Fink, N. (2012), "Meeting the Challenge: A Guide to United Nations Counterterrorism ctivities", International Peace Institute,
https://www.ipinst.org/wpcontent/uploads/publications/ebook_guide_to_un_counterterrorism.pdf.

[4] -اعضای گروه کاری شامل طیف وسیعی از نهادها از جمله کمیته نظارتی قطعنامه ۱۲۶۷، CTED، INTERPOL و UNODC هستند.

[5]- A/RES/58/32 (18 December 2003)

میزان همکاری ها علیه جرایم سایبری و تروریستی در بستر فناوری اطلاعات بیفزایند[۱]. با این گزارش کاربرد حقوق بین الملل در فضای سایبری مورد پذیرش قرار گرفت.

گزارش دوم این گروه در ژوییه ۲۰۱۵ منتشر شد. در بند «ج» و «د» هنجار ۱۳ این گزارش عنوان شد که دولت ها می بایست در زمینه ممانعت از اعمال خرابکارانه همکاری نموده و نباید آگاهانه اجازه استفاده از سرزمین خود برای اعمال خلاف بین المللی با استفاده از فناوری اطلاعات را بدهند؛ تبادل اطلاعات و معاضدت در جهت تعقیب تروریست ها و کاربرد مجرمانه فناوری اطلاعات می بایست در میان دولت ها گسترش یابد[۲].

مذاکرات سال های ۲۰۱۶–۲۰۱۷ این کارگروه به علت اختلاف نظر کارشناسان در مورد مسائل مربوط به کاربرد حقوق بین الملل به ویژه حقوق بشردوستانه، اقدامات متقابل و دفاع مشروع سایبری با شکست مواجه شد و نتیجه ای در پی نداشت.

به دنبال افزایش تنش‌ها میان قدرت‌های سایبری و شکست گروه کارشناسان دولتی در دور پیشین، مجمع عمومی در سال ۲۰۱۸ قطعنامه ۷۳/۲۷ [۳]را با حمایت روسیه به تصویب رساند. در این قطعنامه نیز در بند۱/۳ آمده است، دولت ها نباید آگاهانه اجازه دهند که قلمرو آنها برای اعمال غیرقانونی بین المللی با استفاده از فناوری اطلاعات و ارتباطات استفاده شود. کشورها نباید از نمایندگان برای ارتکاب اعمال غیرقانونی بین المللی با استفاده از فناوری اطلاعات و ارتباطات استفاده کنند و باید به دنبال اطمینان از عدم استفاده از قلمرو آنها توسط بازیگران غیردولتی برای ارتکاب چنین اعمالی باشند. همچنین بر ایجاد کارگروه بازبررسی تحولات در زمینه ارتباطات و اطلاعات در چارچوب امنیت بین المللی(OEWG)[4] تاکید گردید.

نخستین گزارش این کارگروه که در مارس ۲۰۲۱ و به اتفاق آراء توسط کشورهای شرکت کننده تصویب شد، این به دلیل مشارکت مستقیم دولتها در تصویب آن از جایگاه مهم تری نسبت به سایر گزارشها و اقدامات در این زمینه برخوردار می باشد[۵].

در این گزارش، فراوانی، پیچیدگی و تنوع رویدادهای خرابکارانه فناوری اطلاعات و ارتباطات و همینطور افزایش احتمال استفاده از ابزارهای سایبری در مخاصمات آینده توسط تروریستها و گروه های تبهکار و آثار بالقوه ویرانگر آنها را از جمله افزایش تعداد حملات سایبری خصمانه که خدمات عمومی ضروری مثل امکانات پزشکی، خدمات مالی، انرژی، آب، حمل و نقل و بهداشت را به مخاطره می اندازند، شناسایی کرده است.

در کنار این اقدامات مجمع عمومی سازمان ملل در ۱۵ ژوئن ۲۰۱۷ دفتر مبارزه با تروریسم سازمان ملل متحد(**UNOCT**[6]) را تأسیس کرد، همانطور که در گزارش دبیر کل سازمان ملل آمده[۱] ، وظیفه این دفتر کمک به کشورهای عضو در اجرای استراتژی جهانی مبارزه با تروریسم[۲] سازمان ملل می باشد.

---

[1]- 2013 UN GGE Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/68/98)

[2]- 2015 UN GGE – Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/70/174)

[3]- A/RES/73/27 (11 December 2018)
[4]- UN Open-Ended Working Group
[5]- A/AC.290/2021/CRP.2 (10 March 2021)
[6]- United Nations Office of Counter-Terrorism

دفتر مبارزه با تروریسم سازمان ملل متحد ابتکارات متعددی در زمینه فن آوری های جدید از جمله پروژه ای برای استفاده از رسانه های اجتماعی برای جمع آوری اطلاعات آزاد و دیجیتالی برای مقابله با تروریسم و افراط گرایی خشن، ضمن رعایت حقوق بشر دارد. به طور خاص، برنامه سایبر امنیت و فن آوری های جدید با هدف تقویت ظرفیت های کشورهای عضو و سازمان های خصوصی در جلوگیری از حملات سایبری توسط گروه های تروریستی علیه زیرساخت های مهم می باشد تا در صورت بروز حملات سایبری، تأثیرات این حملات را کاهش داده و بازیابی سیستمهای هدفمند را انجام دهد.

(https://www.un.org/counterterrorism/cybersecurity)

در ۲۷ دسامبر ۲۰۱۹ مجمع عمومی سازمان ملل طی قطعنامه ۷۴/۲۴۷ [3](۲۰ ژانویه ۲۰۲۰) خود، تصمیم به ایجاد یک کمیته بین‌دولتی موقت از کارشناسان، نماینده همه مناطق، برای تدوین کنوانسیون جامع بین‌المللی در مورد «مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد مجرمانه» گرفت.

مجمع عمومی در ۲۶ مه ۲۰۲۱ قطعنامه ۷۵/۲۸۲ [4](۱ ژوئن ۲۰۲۱) را با عنوان «مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد مجرمانه» به تصویب رساند.

در بند ۴ این قطعنامه تصمیم می گیرد که کمیته موقت حداقل شش جلسه، هر جلسه ۱۰ روزه، برای شروع در ژانویه ۲۰۲۲ تشکیل دهد و کار خود را به منظور ارائه پیش نویس کنوانسیون به مجمع عمومی در هفتاد و هشتمین جلسه آن، پایان دهد.

اقدامات شورای امنیت سازمان ملل متحد

از آنجاییکه وظیفه حفظ صلح و امنیت بین الملل بر عهده شورای امنیت سازمان ملل می باشد، کمک به درک بهتر خطرات فزاینده ناشی از فعالیت های مخرب در فضای سایبری و تاثیر آنها بر صلح و امنیت بین المللی یک موضوع جدید و وضعیت پیچیده‌ای دارد که مشابه دیگر موضوعات امنیتی بین‌المللی نیست و مثل همیشه، آوردن موضوع جدید در شورای امنیت دشوار است. بنابراین شما باید رویکرد نوآورانه‌تری داشته باشید تا بتوانید آن را به شورای امنیت بیاورید.

تا به امروز عملیات های سایبری توسط دولت ها و یا گروه های تروریستی در حدی نبوده که شورای امنیت سازمان ملل به صورت مستقل ورود ویا قطعنامه ای را تصویب نماید. اما با ظهور گروه های تروریستی القاعده، داعش و گروه های وابسته به آن ها در دهه گذشته و استفاده این گروه ها از فضای سایبری برای تبلیغ، جذب نیرو، خرید سلاح، ایجاد افراط گرایی و یا هدایت عملیات های تروریستی منجر به این گردیده تا در کنار قطعنامه هایی که علیه این گروه ها در شورای امنیت به تصویب رسیده در بندهایی از آن ها به جلوگیری از سوء استفاده تروریست ها از فضای سایبر برای اقدامات تروریستی تأکید گردد.

1- A/71/858
2- A/RES/60/288
3- A/RES/74/247
4- A/RES/75/282

قطعنامه های ۱۲۶۷ (۱۹۹۹) و ۱۳۷۳ (۲۰۰۱) شورای امنیت چارچوبی را برای رژیم گسترده تر ضد تروریسم شورا فراهم می کند که از آن زمان از طریق یک سری قطعنامه های بعدی اصلاح شده است، برخی از آنها به صراحت به استفاده تروریستی از فناوری اطلاعات و ارتباطات می پردازند که در ذیل به برخی از آن ها می پردازیم.

شورای امنیت سازمان ملل نیز در قطعنامه های ۲۱۷۰ (۲۰۱۴) و ۲۲۵۳ (۲۰۱۵) هرگونه ارائه خدمات اینترنتی برای استفاده و حمایت از داعش و القاعده را مورد هدف مقررات تحریمی داده و مصرانه از کشورها درخواست کرده تا از استخدام نیرو برای تروریست ها از طریق اینترنت جلوگیری و با اقدامات تحریک آمیز و تبلیغات افراط گرایی خشونت آمیز این گروه ها در اینترنت و رسانه های گروهی مقابله نمایند.

در قطعنامه ۲۳۷۰ (۲۰۱۷) شورای امنیت کشورهای عضو را ترغیب می کند تا با همکاری و احترام به حقوق بشر و آزادیهای اساسی، مطابق با تعهدات تحت قوانین بین المللی، با یکدیگر همکاری نمایند تا از دستیابی تروریستها به اسلحه، از طریق فناوری اطلاعات و ارتباطات، جلوگیری کنند و بر اهمیت این همکاری با جامعه مدنی و بخش خصوصی تأکید می‌کند.

در قطعنامه ۲۳۹۶ (۲۰۱۷) با ذکر نگرانی از این که تروریست ها و گروه های تروریستی همچنان از اینترنت برای اهداف تروریستی استفاده می کنند بر لزوم فعالیت کشورهای عضو در هنگام انجام اقدامات ملی برای جلوگیری از سوء استفاده تروریست ها از فناوری و ارتباطات برای اقدامات تروریستی تأکید و همچنین ادامه همکاری داوطلبانه با بخش خصوصی و جامعه مدنی برای ایجاد و اجرای ابزارهای مؤثرتر برای مقابله با استفاده از اینترنت برای اهداف تروریستی در سطح جهان، تأکید می کند.

همچنین شورای امنیت در این قطعنامه با نگرانی خاطرنشان می‌کند که تروریست ها با تحریف روایت ها، از آنها برای قطبی شدن جوامع، استخدام حامیان و مبارزان تروریست خارجی، بسیج منابع و حمایت از هواداران به ویژه با سوء استفاده از اطلاعات و ارتباطات و فن آوری ها از طریق اینترنت و رسانه های اجتماعی، استفاده می کنند.

نتیجه گیری

بسیاری از کشورها استفاده تروریستی از اینترنت را به عنوان یک تهدید امنیت ملی و بین المللی با پیوندهای مستقیم یا غیر مستقیم به امنیت سایبری می دانند. در سازمان ملل، تروریسم مدت‌هاست در دستور کار صلح و امنیت بین‌المللی قرار گرفته است. در دهه اخیر، با روی کار آمدن گروه های تروریستی القاعده و داعش ، چنین توجهی را تسریع کرده است. به ویژه اینکه چگونه از فناوری اطلاعات و ارتباطات، اینترنت و پلتفرم های رسانه های اجتماعی، برای رادیکال کردن، جذب حامیان، جمع آوری کمک مالی، به دست آوردن اقلام تحریم شده، و برانگیختن نفرت و خشونت برای اهداف تبلیغاتی استفاده شود.

با توجه به وابستگی روزافزون جامعه جهانی به فناوری اطلاعات و ارتباطات و افزایش همزمان استفاده مخرب از آنها توسط گروه های تروریستی، تعامل سازمان ملل و دولت ها در زمینه فناوری اطلاعات و ارتباطات و صلح و امنیت بین‌المللی باید افزایش یابد. دبیرکل سازمان ملل متحد و نمایندگان دولت ها در بسیاری از سخنرانی ها و تعدادی از بیانیه‌های سیاسی و موضوعات بین‌المللی، امنیت سایبری را مطرح کرده اند که نشان‌دهنده اهمیت روزافزون این موضوع در سازمان است.

گرچه تعدادی معاهدات و کنوانسیون ها با دامنه های مختلف وجود دارد که به موضوع جرایم سایبری می پردازد، اما هیچ کنوانسیون و یا سند قانونی تاکنون در سازمان ملل در مورد جرایم سایبری وجود ندارد.

کار قابل توجهی در سازمان ملل برای مقابله با استفاده از اینترنت برای مقاصد تروریستی در حال انجام است، مسائل پیچیده مربوط به بهترین روش مقابله با تهدیدات فراملی مانند استفاده جنایی و تروریستی از اینترنت و بحث های مربوط به فناوری اطلاعات و ارتباطات و صلح و امنیت بین المللی اغلب به فرآیندهای کمیته اول(خلع سلاح و امنیت بین‌المللی) مربوط می شود. تلاش‌های اولیه همچنین در داخل دبیرخانه برای هماهنگی در مورد موضوعات مرتبط با امنیت سایبری انجام شده است.

تشویق به افزایش آگاهی و گزارش در مورد فرآیندهای هنجاری جاری مربوط به استفاده از اینترنت برای مقاصد تروریستی و جنایی، برجسته کردن پیشرفت در اجرا، محل چالش‌ها و نحوه رسیدگی به آن چالش‌ها؛ و تشویق به ارائه گزارش‌های کارشناسی در کمیته‌های مربوطه مجمع عمومی در مورد موضوعات خاصی که در حوزه‌های مختلف سیاسی از جمله استفاده دولت ها از پتانسیل تروریست‌ها برای انجام حملات سایبری علیه زیرساخت‌های حیاتی و پیامدهای آن برای صلح و امنیت بین‌المللی در حال انجام است.

با این حال، برخی از کشورها نیز خواستار یک سند اصلی، بین المللی و الزام آور قانونی برای تنظیم رفتار دولت در فضای مجازی می باشند. به نظر می‌رسد بایستی با تصویب معاهداتی مستقل، تشکیلات بین المللی جامع و سازمان یافته ای ایجاد شوند که بر عملیات های سایبری کنترل و نظارت داشته باشند.

منابع فارسی

کتاب ها

والو، ژان، (۱۳۹۸)، حملات سایبری و توسل به زور در حقوق بین الملل، مترجم الناز کتانچی، تهران، نشر گلزار ادب.

منابع انگلیسی

Books & Articles:

Ayalew, Y.E. (2014). The impact of cyber warfare under international humanitarian law: A critical legal analysis. Dessie, Ethiopia: School of Law ,Wollo University.

Daintith, J. (2004). A Dictionary of Computing. Oxford: Oxford University Press.

Dinniss, H. (2012). Cyber warfare and the Laws of war. Cambridge: Cambridge University Press.

Forrest, C. (2018). Cyber Attacks Are Third Largest Threat to Global Society over Next 5 Years. www.schinnerer.com.

Khalaf Rezaei, H. (2013). Cyber-Attacks from the perspective of international law (Stuxnet case study), *Majles and Strategic Quarterly*. (in Persian).

Klausen, J. (2015). Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. *https://doi.org.*

KriangsakKittichaisaree, Public International Law of Cyberspace, 2017

Schmitt, Michael (1999). "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", Columbia Journal of Transnational Law, Vol. 37. 50. Schmitt, Michael (2011). "Cyber Operations and the Jus in Bello: Key Issues", Naval War College International Law Studies

Schmitt, Michael N. (2002). "Wired Warfare: Computer Network Attack and Jus in Bello", International Review of the Red Cross, Vol. 84, No. 846.

Schmitt, Michael N. (2013), Tallin Manual on the International Law Applicable to Cyber Warfare, New York, Cambridge University Press

Chowdury Fink, N. (2012), “Meeting the Challenge: A Guide to United Nations Counterterrorism ctivities”, International Peace Institute,

Documents:

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)(1986)

Threat Tactics Report: Islamic State of Iraq and the Levant

TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence(2013)

UN GGE Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/68/98)(2013)

UN GGE Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/70/174)(2015)

Site:

https://www.un.org/counterterrorism/cybersecurity

https://undocs.org/en/A/60/PV.99

https://www.ipinst.org/wpcontent/uploads/publications/ebook_guide_to_un_counterterrorism.pdf.
www.securitynewsdaily.com