Scientific Journal of Political Law Approaches

Scientific J. Pol. L. App., 2(1) (2024) 15-27
DOI: 10.22084/qjpla.2025.30336.1008

Bu-Ali Sina University

Cyber-Technological Terrorism and Extremism: Legal and Security Challenges for the International Legal System

Mohammadmehdi Seyed Nasseri[1*], Leila Mirbod [2]

[1] Ph.D. in International Law, Department of Law, Faculty of Humanities, Islamic Azad University, Dubai, UAE.
[2] Ph.D. Graduated in Public International Law, Islamic Azad University, Science and Research Branch, Tehran, Iran.

ABSTRACT: Recent developments in the realm of cybercrime and cyber-technological terrorism—particularly the exploitation of cyberspace by terrorist organizations—have given rise to extensive legal challenges in areas such as human rights violations, jurisdictional competence, crime detection, punishment of offenders, and international cooperation. Cyberterrorism, which emerges from the intersection of terrorism and cyberspace, conceptually differs from cyber-extremism, which is more closely associated with cybercrime.This study, employing a descriptive-analytical approach, demonstrates that the utilization of emerging technologies has rendered counterterrorism efforts increasingly complex and has necessitated the regulatory structuring of cyberspace in response to evolving security threats. Fundamentalist groups, leveraging concepts such as “electronic jihad,” exploit cyberspace for recruitment and propaganda. A precise distinction between cyberterrorism and cyber-extremism facilitates the formulation of effective and coordinated responses; namely, the eradication of cyberterrorism within the framework of international law, while countering cyber-extremism remains within the domain of domestic legal systems.

Review History:

Received: Apr. 28, 2024
Revised: Jul. 05, 2024
Accepted: Sep. 06, 2024
Available Online: Sep. 21, 2024

Keywords:

Cyber Terrorism
Extremism
Cyberspace
Peace
International Security

*Corresponding author’s email: sm.snaseri@gmail.com

نشریه علمی رویکردهای حقوق سیاسی

نشریه علمی رویکردهای حقوق سیاسی، دوره ۲، شماره ۱، بهار و تابستان ۱۴۰۳، صفحات ۱۵ تا ۲۷
(مقاله پژوهشی)
DOI: 10.22084/qjpla.2025.30336.1008

تروریسم و افراطی‌گری سایبر-تکنولوژیک؛ چالش‌های حقوقی و امنیتی برای نظام حقوق بین‌الملل

محمدمهدی سیدناصری[۱*]، لیلا میربد[۲]

۱. دکترای تخصصی حقوق بین‌الملل، گروه حقوق، دانشکده علوم انسانی، دانشگاه آزاد اسلامی، دبی، امارات.
۲. دانش آموخته دکتری حقوق بین‌الملل عمومی، واحد علوم و تحقیقات تهران، دانشگاه آزاد اسلامی، ایران.

خلاصه: تحولاتِ اخیر در حوزه جرایم سایبری و تروریسم سایبر-تکنولوژیک، به‌ویژه بهره‌برداری سازمان‌های تروریستی از فضای مجازی، چالش‌های حقوقی گسترده‌ای در زمینه‌هایی چون نقض حقوق بشر، صلاحیت قضایی، کشف جرم، مجازات مرتکبان و همکاری‌های بین‌المللی ایجاد کرده است. تروریسم سایبری که از هم‌پوشانی تروریسم و فضای سایبری ناشی می‌شود، با افراطی‌گری سایبری که بیشتر مرتبط با جرایم سایبری است، تفاوت‌های مفهومی دارد. این پژوهش با روش توصیفی-تحلیلی نشان می‌دهد که بهره‌گیری از فناوری‌های نوین، مبارزه با تروریسم را پیچیده‌تر کرده و تحولات امنیتی، قاعده‌مندسازی فضای سایبر را ضروری ساخته است. بنیادگرایان نیز با استفاده از مفاهیمی چون "جهاد الکترونیک"، از فضای سایبر برای عضوگیری و تبلیغات بهره‌برداری می‌نمایند. تفکیک دقیق میان تروریسم و افراطی‌گری سایبری، تدوین واکنش‌های مؤثر و هماهنگ در این زمینه را تسهیل می‌کند؛ به‌گونه‌ای که ریشه‌کنی تروریسم سایبری در چهارچوب حقوق بین‌الملل و مقابله با افراطی‌گری سایبری در حقوق داخلی امکان‌پذیر است.

تاریخچه داوری:
دریافت: ۱۴۰۳/۰۲/۰۹
بازنگری: ۱۴۰۳/۰۴/۱۵
پذیرش: ۱۴۰۳/۰۶/۱۶
ارائه آنلاین: ۱۴۰۳/۰۶/۳۱

کلمات کلیدی:
تروریسم سایبری
افراطی‌گری
فضای سایبر
صلح
امنیت بین‌المللی

۱- مقدمه

باظهور استفاده از تکنولوژی اطلاعات و دسترسی و به اشتراک‌گذاری اطلاعات، خطرات استفاده از آن نیز بیش از پیش نمودارگردید و حوزه‌های گوناگونی ازجمله حقوق بین‌الملل را با چالش‌های نوینی مواجه نموده است. حفظ صلح و امنیت بین‌المللی که دلیل وجودی سازمان ملل متحد است به حوزه‌های نوینی همچون فضای سایبری وارد گردیده است. تروریسم سایبری با اختلال در داده‌ها به ویژه هنگامی که زیرساخت‌های حیاتی مانند سدها، کنترل ترافیک هوایی، تأسیساتِ زیرساختی یا انتقال برق را مورد حمله قرار می‌دهد، می‌تواند از نظر شدت تلفات و خسارت به سطح حملات مسلحانه برسد. افراد ممکن است قربانی مخاصمات میان دولت‌ها باشند؛ اما در آن، اهداف و مناطق نظامی اغلب جزو اهداف اصلی حملات هستند، در مقابل، در تروریسم، ممکن است هیچ تفاوتی میان نظامی و غیرنظامی قائل نشود و قربانیانش از میان مردم عادی باشند(اتان شاو، ۱۳۹۴، ص۳۲). این ویژگی تروریسم از دیدگاه مرتکبان یا حامیان و همچنین عموم مردم و دولت، بعد از تحول مفهوم امنیت پس از جنگ سرد[۱]، قابل رؤیت شده است. علاوه‌بر آن، تأکید بیشتر بر روی امنیت اقتصادی، زیست‌محیطی و امنیت اطلاعات که در طول جنگ سرد در اهمیت دوم قرار داشتند، در حال حاضر بسیار مورد توجه بوده و عامل نگرانی در امنیت انسانی و آنچه هویت امنیت[۲] نامیده می‌شود، به‌شمار می‌آیند. به جز بحث تروریسم سایبری، تروریست‌ها می‌توانند به جای انجام عملیات ترور فیزیکی، از اینترنت برای اهداف سازمانی خود در جهت توسعه و گسترش افراطی‌گری سایبری استفاده نمایند (Clarke, C. P., 2018, p 13). تروریست‌ها این امکان را دارند از رایانه جهت انجام جرم و جنایت‌های مختلفی نظیر سرقت هویت، ویروس‌های رایانه‌ای، هک کردن، استفاده از بدافزارها، تخریب یا دستکاری داده‌ها برای اهداف مختلف استفاده نمایند: تبلیغات، جمع‌آوری اطلاعات، آماده‌سازی حملات دنیای واقعی، انتشار موارد آموزشی، ارتباطات،

۱. جنگ سرد به دوره‌ای از رقابت، تنش و کشمکش ژئوپلیتیکی بین اتحاد جماهیر شوروی و متحدانش (بلوک شرق) و ایالات متحده آمریکا و متحدانش (بلوک غرب) بعد از جنگ جهانی دوم گفته می‌شود.

2. Security identity

* نویسنده عهده‌دار مکاتبات: sm.snaseri@gmail.com

سرمایه‌گذاری تروریستی[۱]. این بدین معناست که سازمان‌ها یا دولت‌هایی که وابسته به عملیات رایانه‌ای و شبکه‌های کامپیوتری هستند که می‌توانند به سادگی موردحمله قرارگیرند[۲].

جهان آنلاین (اینترنت) این مزیت را برای عملیات تروریستی دارد که در آن فرایندها می‌توانند نسبت به رسانه‌های سنتی، سریع، پویا، عمقی، ناشناخته، غیرقابل ویرایش، ارزان و با دسترسی از راه دور باشد. بنابراین آن‌چه در این پژوهش به‌عنوان چالش‌های نوین فضای سایبر مورد واکاوی و بررسی قرارخواهد گرفت، مسئله‌ی «تروریسم سایبری و افراطی‌گری در فضای مجازی[۳]» است. پرسش اصلی این است که کدام حوزه‌های حقوق بین‌الملل در رویارویی با این دو مسئله قرار می‌گیرند و آیا حوزه‌های کلاسیکی چون حقوق بشردوستانه بین‌المللی[۴] یا امنیت بین‌الملل[۵]، قواعدی را در مسیر مبارزه با این پدیده‌ها ارائه می‌نمایند؟ به نظر می‌رسد باتوجه به عدم تعریف جامعی از تروریسم و عدم قاعده‌مندی فضای سایبر، راه‌های مبارزه با آن، از شاهراه همکاری‌های بین‌المللی در تعهد دولت‌ها به مبارزه با انواع تروریسم بگذرد؛ اما باتوجه به اقدامات تبلیغاتی و عضوگیری از افراطیون در فضای سایبر دولت‌ها تمایل بیشتری دارند تا به این مسئله در چهارچوب صلاحیت داخلی‌شان رسیدگی نمایند. پس از واکاوی عملکرد دولت‌ها و سازمان‌های بین‌المللی، راهکارهایی جهت مبارزه با افراطی‌گری و تروریسم سایبری ارائه می‌شود. تفاوت استفاده تروریست‌ها از فضای سایبر یا افراطی‌گری سایبری و تروریسم سایبری و قواعد مبارزه با هرکدام در این پژوهش مورد بررسی قرارمی‌گیرد (Williams, 2007, p 11). این پژوهش بر آن است با روش توصیفی- تحلیلی و با بررسی اسناد، کتب و مرور مقالات منتشر شده به زبان انگلیسی و فارسی که در خلال سال‌های ۲۰۰۲-۲۰۲۲ ، و از طریق مرور ادبیات گسترده، تجزیه و تحلیل، تحقیقات علمی و نظرات متخصصین و پژوهشگران و حقوقدانان پیشرو در این حوزه به دنبال درک ماهیت تروریسم سایبر-تکنولوژیک است.

۲- وجود یا عدم وجود تروریسم سایبر-تکنولوژیک[۶] در عصر انقلاب صنعتی چهارم

میان وجود یا عدم وجود مفهوم تروریسم سایبری، میان حقوقدانان اختلاف‌نظر شدید وجود دارد. منبع این اختلاف نبود تعریف جامع و فراگیر از دو واژه تروریسم و فضای سایبر[۷] است. تعاریف بسیاری برای تروریسم سایبری ارائه شده است که ماحصل همه آن‌ها می‌تواند در این تعریف خلاصه شود: اعمال خشونت یا تهدید به آن، توسط عوامل غیردولتی یا سازمان‌های مجرمانه با انگیزه‌ی سیاسی یا ایدئولوژیک که از طریق سیستم‌ها و سامانه‌های ارتباطی و رایانه‌ای، علیه داده‌ها با ایجاد اختلال شدید در سیستم‌های رایانه‌ای صورت می‌گیرد و منجر به رعب و وحشت در میان جمعیت غیرنظامی و ورود خسارت فیزیکی یا دیجیتالی شده و زیرساخت‌های حیاتی دولت را تهدید نماید، هدف از ارتکاب چنین اعمالی اجبار دولت به تغییر ساختار سیاسی یا شیوه عمل خاصی است؛ اما بسیاری از متخصصان فن، میان تروریسم سایبری و استفاده تروریست‌ها از اینترنت برای تبلیغات، عضوگیری و استخراج اطلاعات یا برقراری ارتباط تفاوت قایل شده‌اند. تروریسم سایبری در واقع زیرمجموعه‌ی حملات سایبری است که با انگیزه‌ی سیاسی و ایدئولوژیک و علیه اهداف غیر نظامی صورت می‌گیرد؛ اما جنگ سایبری با هدف نائل آمدن به برتری اطلاعاتی از طریق اثرگذاری بر اطلاعات و سیستم‌های اطلاعاتی دشمن و دفاع از داده‌ها و اطلاعات خود صورت می‌گیرد (پاکزاد، ۱۳۸۹، ص ۱۰۱).

۲- ۱- فضای سایبر به مثابه یک انتخاب در تسهیل تروریسم

ادله‌ی متعددی وجود دارد که چرایی حملات سایبری به عنوان یک انتخاب جذاب برای تروریست‌ها را تبیین می‌نماید، از آنجایی‌که تروریست‌ها

---

۱. شبکه‌های اجتماعی همچون فیس‌بوک، یوتیوب، مای اسپیس و توییتر اعضای جهانی یادی دارند که روز به روز نیز در حال افزایش است. فیس‌بوک به تنهایی یک میلیارد عضو دارد که بیشتر آن را جوانان تشکیل می‌دهند. اکثر برآوردهای انجام شده نشان می‌دهد تقریبا ۹٪ از فعالیت‌های تروریستی آنلاین با استفاده از ابزارهای شبکه اجتماعی اتفاق می‌افتد. سرویس‌های شبکه اجتماعی همگی خصوصیات وب‌سایت‌های استاندارد را دارند و بیشتر به تروریست‌ها اجازه می‌دهند تا از آن‌ها برای تبلیغات، آموزش، استخدام، افزایش درآمد، ارتباط مرموز و استخراج داده‌ها استفاده کنند. از تصویر ماهواره‌ای و ابزارهای موقعیت یاب برای برنامه‌ریزی حملات‌شان استفاده می‌کنند.

۲. کرم کامپیوتری استاکس نت در سال ۲۰۱۰ آسیب‌پذیری زیرساخت‌های حیاتی را نشان داده است. حملات شناخته شده، علیه سیستم‌های رایانه‌ای در استونی (۲۰۰۷) و گرجستان (۲۰۰۸) نیز اهمیت توجه به قانون‌گذاری و مبارزه با تروریسم سایبری را بیش از پیش نشان داد.

۳. باوجود توسعه فراگیر کاربرد و آثار فضای مجازی در سطوح مختلف زندگی بشری در عصر حاضر، تاکنون تعریف واحد و اتفاق نظری از این عبارت ارائه نشده است. با این حال می‌توان گفت فضای مجازی حوزه دیجیتال جهانی از شبکه‌های وابسته به هم و همچنین شبکه‌های تعاملی ازجمله اینترنت و سایر شبکه‌های مخابراتی و پردازنده‌هایی است که جهت انتقال، تولید یا حفظ و حذف اطلاعات گوناگون از آن استفاده می‌شود.

۴. که منظور از آن «قواعد ایجادکننده حق و تکلیفی است که در طول مناقشه و در هر مکانی که دایره‌ی تخاصم وجود داشته باشد، مجری خواهد بود».

5. International Security

۶. Cyber Technology فناوری های نوین، فضایی را به وجود آورده است به نام فضای سایبر. این فضا مجازی نیست بلکه کاملاً واقعی است و انسان همه پدیده‌های فضای واقعی زندگی خود را در این فضا شبیه‌سازی کرده است. این فضا افراد و بازیگران بین‌المللی را با یکدیگر همراه می‌کند و ساختارهای سیاسی و اقتصادی را با ماهیت سایبری و بدون هیچ فاصله جغرافیایی در کنار یکدیگر قرار می‌دهد به‌طوری‌که کشورها، سازمان‌های بین‌دولتی و چندملیتی بدون هیچ واسطه، مرز، با یکدیگر تعامل می‌کنند. در واقع به نوعی شاهد هژمونی فضای سایبر بر همه ابعاد زندگی بشر هستیم.

7. Cyber Space

سرمایه‌های محدودی دارند و حملات سایبری نیاز به منابع و افراد کمتری دارد، استفاده از فضای سایبر بسیار اغواکننده است. به عبارت دیگر آن‌ها می‌توانند افراد و اهداف زیادی را با همان مقدار امکانات محدود متأثرکنند. فضای سایبر به تروریست‌ها کمک می‌کند تا گمنام بمانند، درحالی‌که آن‌ها می‌توانند از منطقه فیزیکی که اعمال تروریستی در آن صورت می‌پذیرد، دور باشند و متحمل خسارات جانی نیز نگردند. هیچ قانون و مانع فیزیکی خاصی وجود ندارد که آن‌ها ملزم به رعایت آن باشند. سرعت و شکل حمله متکی بر سرعت ارتباطات مهاجمین است. ترکیبی از تروریسم فیزیکی و تروریسم سایبری پرکاربردترین استفاده از تروریسم سایبری را دارد[1](حاتمی و رضایی، ۱۳۸۹، ص ۹۶).

حمله به زیرساخت‌های حیاتی یک دولت که از فاکتورهای مهم شناسایی تروریسم سایبر-تکنولوژیک است، توسط حمله به سیستم‌های کنترل نظارتی و کسب داده[2] انجام می‌شود، که عملیات بسیاری از بخش‌های زیرساخت‌های مهم و حیاتی مثل ژنراتورهای تولید برق و آبرسانی را کنترل و تنظیم می‌کنند. این سیستم‌ها به صورت خودکار فرایندهای کنترل، تولید و تعویض را بر اساس بازخوردهای عددی دریافت شده از حسگرها رصد و تنظیم می‌کنند و یا اعمال فیزیکی همچون سطح فشار در لوله‌ها را انجام داده یا این‌که یک سد باز یا بسته است را کنترل می‌کنند[3]. رایانه‌ای که از القاعده[4] در افغانستان مصادره شد حاوی نمونه‌هایی از یک سد بود که با سبک معماری و نرم‌افزار مهندسی طراحی شده بود و طراحان آن‌را قادر می‌ساخت که سطح آسیب‌پذیری و تخریب سد را تخمین بزنند. دفتر تحقیقات فدرال از موارد زیادی از نمونه‌های طراحی شده توسط القاعده که برای اهداف آنلاین و نظارت بر سیستم‌های تلفن اضطراری، ژنراتورها و دستگاه‌های مخابراتی، مخازن آب و سیستم توزیع، نیروگاه‌های اتمی و شبکه‌های مخازن سوخت برنامه‌ریزی شده بودند، پرده برداشت. بنابراین به‌طور خلاصه می‌توان ویژگی‌های فضای سایبر را برای اعمال تروریسم سایبری این‌گونه بر شمرد: ۱. امکان انجام اقدامات تروریستی با کمترین هزینه، تلفات و خسارت؛ ۲. گم‌نامی و مخفی بودن عملیات تروریستی که بسیار برای تروریست‌ها اهمیت دارد؛ ۳. کنترل‌ناپذیر بودن فضای سایبر و کم بودن احتمال کشف عملیات و دستگیری؛ ۴. جهانی بودن و امکان انجام عملیات در کسری از ثانیه با ایجاد خسارات شدید.

۲- ۲- چالش نظام بین‌الملل حقوق بشر و تروریسمِ سایبر-تکنولوژیک

اعمال کنترل بر فضای سایبر در جهات مبارزه با تروریسم و افراطی‌گری، چالش دیگری را در حوزه حقوق بشر به دنبال خواهد داشت. اهمیت تعادل بین جلوگیری و بررسی جرایم مربوط به استفاده تروریست‌ها از اینترنت با نیاز بهحمایت از آزادی بیان پوشیده نیست (UNODC, 2012, p19). روش‌های قانونی برای جرم انگاری انتشار تبلیغات نباید مانع حق آزادی بیان شود. طرفداران آزادی ارتباطات اینترنتی معتقدند که اقدامات دولت‌ها برای تدوین مقرراتی به منظور مجاز دانستن و دسترسی دولت‌ها به ارتباطات الکترونیک: اولاً. به حق حفظ اسرار محرمانه لطمه می‌زند و نیز توسعه ارتباطات اینترنتی را محدود می‌کند؛ ثانیاً. مانع ارتکاب جرم نمی‌شود. طرفداران آزادی ارتباطات الکترونیکی براین باورند که چون محرمانه بودن ارتباطات را قوانین اساسی دولت‌های مختلف و مقررات بسیاری از معاهدات سیاسی و کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی[5] به رسمیت می‌شناسند؛ لذا سازوکارهای محدودکننده، خلاف حق شناخته شده شهروندان و مغایر روح حقوق بین‌الملل و معیارهایی است که حفظ اسرار محرمانه را درخصوص افراد را از اصول سیاسی حقوق بشر می‌شناسد. (حاتمی، رضایی، ۱۳۹۸، ص ۱۳). در مقابل طرفداران محدودیت این‌گونه استدلال می‌کنند که استفاده از توانایی‌های نوین رایانه‌ای و اینترنتی دست جنایتکاران را در ارتکاب جرم باز می‌گذارد، مدافعان آزادی ارتباطات بر این باورند که ایجاد محدودیت نه تنها باعث کاهش و یا مانع ارتکاب جرم نمی‌شود؛ بلکه فرصت‌های مجرمین را برای ارتکاب اعمال مجرمانه افزایش می‌دهد. از سوی دیگر محدودیت ارتباطات به معنای محروم کردن بخش اقتصادی و تجاری کشورها از فرصت‌هایی است که ممکن است آن‌ها را از سودهای سرشار و فرصت‌های تجاری محروم نماید (میربد، ۱۳۸۸، ص ۴۳).

۱. یکی از نمونه‌های در رابطه با استفاده از وب سایت‌ها توسط تروریست‌ها است، وب سایت سازمان تروریستی پ.ک.ک است. ۳۷ وب سایت وجود دارد که وابسته به همین سازمان است.

2. SCADA

۳. به‌عنوان مثال در سال ۱۹۹۷ یک هکر اینترنتی توانست به سیستم ارتباطی فرودگاهی در ورچستر در ماساچوست آمریکا دستیابی پیدا کند که باعث مختل شدن خط تلفنی شد که به برج مراقبت فرودگاه متصل بود و همچنین توانایی روشن کردن چراغ‌های باند فرود را توسط هواپیماهایی که در حال نزدیک شدن به باند بودند را غیرممکن ساخت. در نمونه‌ای دیگر یک کارمند سابق صنایع مدیریت پسماند استرالیا به سیستم‌های رایانه ای آن جا دستیابی پیدا کرد و باعث شد که هزاران لیتر فاضلاب در کوئینزلند جاری شود و به گیاهان و جانوران صدمه وارد شده و مردم نیز آنجا را تخلیه کنند.

۴. القاعده که به صورت رسمی با عنوان قاعدة الجهاد نیز شناخته می‌شود، سازمان افراط‌گرای اسلامی از شبه‌نظامیان سنی چندملیتی است که از جهادگرایان سلفی تشکیل شده است. این شبکه در ۱۹۸۸ میلادی توسط اسامه بن لادن، عبدالله عزام، و چندین داوطلب عرب دیگر طی جنگ شوروی در افغانستان تأسیس شد. القاعده، توسط اعضای دائم شورای امنیت سازمان ملل(شامل چین، روسیه، فرانسه، بریتانیا و آمریکا)، ناتو، اتحادیه اروپا، هند و چندین کشور دیگر به‌عنوان گروهی تروریستی در نظر گرفته شده است. القاعده حملاتی را علیه اهداف غیرنظامی و نظامی در کشورهای مختلف انجام داده، که شامل بمب‌گذاری ۱۹۹۸ سفارت ایالات متحده، حملات ۱۱ سپتامبر و بمب‌گذاری‌های ۲۰۰۲ بالی می‌شود.

5. European Convention on Human Rights and Fundamental Freedom 1950.

۲- ۳- مبارزه با تروریسم سایبری و نظام حقوق بشردوستانه بین‌المللی

دومین چالش در خصوص مفهوم تروریسم سایبر-تکنولوژیک این است که کدام دسته از قوانین مربوط به مخاصمات مسلحانه مربوط به حوزه جنگ اطلاعاتی و تروریسم سایبری می‌شوند؟ آیا حمله سایبری آنچنان که در ماده (۴)۲ منشور ملل متحد تعریف شده می‌تواند مصداق «استفاده از زور» باشد؟ اگر پاسخ این سوال مثبت است آیا چنین حمله‌ای طبق ماده ۵۱ منشور حق «دفاع مشروع » را در برمی‌گیرد؟ به‌عنوان مثال، حتی اگر اِستونی می‌توانست اثبات کند که روسیه عامل حملات آوریل ۲۰۰۷ میلادی بوده است باز هم نامشخص بود که آیا می‌تواند از پاسخ‌های قانونی نظیر استفاده از دفاع مشروع، حملات سایبری یا دیگر اقدامات متقابل یاد شده در ماده (۴)۲ استفاده نماید. معیارهای حقوق بشردوستانه بین‌المللی در محدوده زمانی و مکانی یک نزاع مسلحانه بین‌المللی که میان دو یا چند دولت اتفاق می‌افتد عمل می‌نمایند. بنابراین حتی با دریافت این مسئله که حمله از خاک چه کشوری صورت گرفته، احراز این‌که آیا حمله سایبری به سطح حمله مسلحانه رسیده یا خیر، دشوار است؛ اگرچه میزان خسارات یا تلفات یک حمله تروریستی از طریق فضای سایبر ممکن است بسیار شدیدتر از حملات انجام شده با سلاح‌های کلاسیک باشد.در اعمال اصول حقوق بشردوستانه بین‌المللی، اصل تمایز میان نظامیان و غیرنظامیان در مورد مهاجمین سایبری نیز دشوار است و علی‌القاعده حملات تروریستی علیه غیرنظامیان صورت می‌گیرد. هکرها یا اخلال‌گران در سیستم‌های اطلاعاتی در تروریسم امتیاز نظامی بودن را از دست می‌دهند؛ چرا که آن‌ها خود را به‌عنوان نظامی معرفی نمی‌کنند(Doman, 2013, p 1).

بنابراین نظر غالب آن است که این افراد در صورتی که بتوان حمله تروریستی را حمله مسلحانه قلمداد نمود، تنها از برخی حمایت‌های حقوق بشردوستانه بین‌المللی که مندرج در ماده ۷۵ پروتکل اول الحاقی ۱۹۷۷ میلادی است و در صورت غیربین‌المللی بودن مخاصمه، از مندرجات ماده‌ی ۳ مشترک کنوانسیون‌های چهارگانه ژنو برخوردارند؛ اما کماکان تحت حمایت‌های حقوق بین‌الملل بشر هستند. (ضیایی بیگدلی، ۱۳۹۲، ص ۶۱). غیرقابل هدف‌گیری بودن اماکن غیرنظامی نیز طبق پروتکل الحاقی اول کنوانسیون ژنو[1] از اصول حقوق حاکم بر مخاصمات مسلحانه است. در مورد استونی، بانک خدمات دولتی، برنامه‌های تلویزیونی و رادیویی، کنترل رفت و آمد هوایی از این حملات آسیب دیدند؛ چرا که اینترنت و ارتباطات مجازی برای جامعه استونی ضروری بود (Shackelford, 2008, p 56).

اصل منع حملات نامتناسب (که ریسک خسارت متوازی و تلفات غیرنظامی را افزایش دهند)، نیز به نظر نمی‌رسد که در سیاق تروریسم سایبری جایی داشته باشد. نکته دیگر در این خصوص، ماده‌ی ۵۱ منشور سازمان ملل متحد است. گستره دفاع مشروع[2] شامل پاسخ به یک تهدید اقتصادی یا سیاسی نمی‌باشد. بنابراین حملات سایبر که تهدید کمتری نسبت به مفهوم یک حمله مسلحانه مطرح می‌کنند از گستره ماده پیش‌بینی شده مورد بحث، خارج می‌شوند. آنچنان که انتظار می‌رود واژه‌ای که ما باید توجه خود را روی آن متمرکز نماییم «حمله مسلحانه» است؛ نه متوسل شدن به زور. در صورتی که در عملکرد دولت‌ها در مبارزه با تروریسم سایبری دولت ایالات متحده آمریکا در قبال حملات سایبری برای خود حق دفاع مشروع نظامی را قائل شده است (Cassim, 2012, p 14). برخی معتقدند براساس پروتکل الحاقی اول گسترش یا پذیرفتن یک سلاح جدید یا روشی جدید در میدان جنگ می‌بایست مورد مداقه قرار گیرد تا مشخص شود که آیا می‌تواند مورد استفاده قرار گیرد یا خیر؟ در برخی تفاسیر، از منظر قوانین بین‌المللی، استفاده از هر نوع سلاح و روش جدیدی در جنگ ممنوع اعلام شده است. بنابراین می‌توان گفت مسلّم است که وضع قوانین در پروتکل الحاقی اول در مورد مخاصمه مسلحانه، ترجیحاً به صورت یک عبارت کلی و عمومی است که بنابر قواعد حقوق بین‌الملل قابل تسری به سلاح‌های جدید است (Lee, 2013, p 99).

۲- ۴- جایگاهِ مبارزه و بازدارندگی سایبری و ایجاد سیستم‌های دفاعی

تروریسمِ سایبری تهدیدی جهانی است که به واکنش یکپارچه جهانی نیاز دارد. وجود قانون به تنهایی کافی نیست. قانون باید با تنفیذ و استراتژی‌های حفاظت مؤثری پشتیبانی شود. بنابراین، ایجاد سیستم‌های دفاعی علیه جرائمِ سایبری و تروریست‌های سایبری مهم است. تلاش جامعه بین‌المللی برای توسعه سازوکارهای جهانی جهت مبارزه با جنایات سازمان یافته بین‌المللی، ریشه در این حقیقت دارد که این جنایات جدی‌تر شده‌اند. جنایات فراملی و اشکال مختلف آن، تهدیدی فراروی صلح و امنیت بین‌المللی است که آرمان‌های بشریت را تحلیل برده و هزینه‌های سنگینی را بر دوش دولت‌ها و بزه‌دیدگان تحمیل می‌کنند (زارعی، ۱۳۹۴، ص ۲). در مناسب‌ترین روش با انعقاد کنوانسیون‌های بین‌المللی، این اتحاد جلوه‌گر خواهد شد؛ اما این روش با مانع تعارض منافع دولت‌ها روبه‌رو است؛ یعنی دولت‌هایی که از نظر فناوری پیشرفته‌تر بوده و تأمین‌کننده خدمات

۱. اهداف نظامی به اهدافی محدود می شود که مشارکت موثر در اقدام نظامی دارند و تخریب آن‌ها یک منفعت نظامی را در پی دارد.

2. Self-defence

اینترنتی هستند روش قانون‌گذاری ملی یا فراملی را ترجیح می‌دهند. از سوی دیگر از آنجاکه به علت برابری حاکمیت‌ها، دادگاه داخلی یک دولت اصولاً نمی‌تواند علیه جرایم ارتکابی کشوری دیگر حکم صادرکند و به دلیل فرامرزی و بین‌المللی بودن فضای سایبر و همچنین جرایم سایبر-تکنولوژیک، بهترین روش برای مبارزه با سایبر تروریسم و جرایم سایبری رجوع به محاکم بین‌المللی و ایجاد همکاری‌های پلیسی و حقوقی در سطح بین‌المللی است (زارعی، ۱۳۹۳، ص ۳). بنابراین می‌توان سه گرایش کلیدی واکنش‌های قانونی به این پدیده را مشخص نمود: ۱. برخی از کشورها قوانین جرائم رایانه‌ای موجود را برای استفاده تروریستی از اینترنت به‌کار می‌برند، ۲. برخی از کشورها قوانین ضدتروریستی را برای اقدامات اینترنتی آن به‌کار می‌برند، ۳. برخی از کشورها قوانین ویژه‌ای برای سوءاستفاده تروریستی از اینترنت تصویب کرده‌اند. حفظ صلح و امنیت بین‌المللی که دلیل وجودی سازمان ملل متحد است، از مفهوم حاکمیت وستفالیایی[1] آن دچار تحول شده[2] و به حوزه‌های نوینی چون فضای سایبری آن ورود کرده است. مسئله تروریسم سایبری که با مداخله مستقیم و غیرمستقیم دولت‌ها یا از طریق بازیگران غیر دولتی انجام می‌پذیرد، حوزه امنیت بین‌الملل را با چالش‌های جدید مواجه نموده است(ضیایی بیگدلی و همکاران، ۱۳۸۷، ص ۳۹). بنابراین به جز دولت‌ها، سازمان‌های بین‌المللی و ارکان سازمان ملل، قطعنامه‌های ضدتروریسم شورای امنیت و اداره مبارزه با مواد مخدر و جرم سازمان ملل متحد[3] نیز در راه مبارزه با تروریسم سایبری وارد شده‌اند. امروزه ناتو[4] توانسته است با تحقیقات و جلب همکاری اعضاء، گام‌های مؤثری در مبارزه با این شکل تروریسم بردارد[5].

۳- افراطی‌گری سایبری جریان‌های تکفیری در جهان آنلاین

برخلاف تروریسم سایبری، افراطی‌گری سایبری، ناظر بر استفاده از فضای سایبر توسط تروریست‌ها، برای عضوگیری، تبلیغات و یا افزایش بودجه است. جریان‌های تکفیری و سلفی‌گری، داعش، سپاه صحابه و القاعده امروزه از اینترنت جهت گسترش فعالیت‌های تروریستی خود بهره می‌گیرند. بنیادگرایی اسلامی یا نژادپرستی به عنوان یک نظریه در روابط بین‌الملل ممکن است در حوزه سایبر برای درک انگیزه، ایدئولوژی و اقدامات پشت پرده حملات تروریستی در فضای سایبر و نیز واکنش به آن‌ها قابل اجرا باشد. برخی همچون فهدبن‌سعدالجهانی سعودی[6] بیان کرده که آیات قران و سنت در مورد جهاد در حوزه سایبر و جنگ سایبری نیز جاری است (Stalinksky, 2012 , p 7). متأسفانه بیاناتی از این دست نه تنها به گسترش اسلام هراسی و نمایش چهره‌ای خشونت طلب از اسلام منجر خواهدشد؛ بلکه بسیاری از اندیشمندان معتقدند استفاده غلط و نابجا در شرایط یا زمان و مکان اشتباه می‌تواند منجر به خشونت گسترده‌ای گردد. عقیده‌ای چون «جهاد محدود به سلاح نیست و تا زمانی که در راستای اهداف تروریستی باشد با هر وسیله‌ای مجاز است». (Geller, 2012, p 20) امروزه نیز از جهاد الکترونیکی سخن به میان آمده است که تنها شامل موعظه‌ها و آموزه‌های اسلامی از طریق اینترنت یا هک سایت‌ها نیست؛ بلکه اقدامات گسترده‌ای است که از جرایم سایبری تا خرابکاری و حملات سایبری و حتی جنگ سایبری تنوع دارد. بنابر گزارش پنتاگون[7] حدود بیش از پنج هزار وب سایت با محتوای جهادی وجود دارد که هر روز بر تعداد این وب‌سایت‌ها افزوده می‌گردد.

۳- ۱- دلایل افراطی‌گری و جهاد الکترونیکی

اقدامات تروریستی هنگامی بوجود می‌آید که طرف‌های ضعیف‌تر نمی‌توانند یک دشمن را مستقیماً به چالش بکشانند و درنتیجه به روش‌های غیرمعمول متوسل می‌شوند هنگامی که هدف وارد کردن خسارت است و گروه تروریستی هیچ علاقه‌ای به کسب اعتبار ندارد، نیاز به گسترده بودن کاهش می‌یابد و هدف به سمت ایجاد خسارت بیشتر خواهد رفت؛ بنابراین در این صورت، استفاده از

---

1. Westphalian Sovereignty

۲. حاکمیت وستفالی این اصل در حقوق بین‌الملل است که، بر پایه اصل عدم مداخله در امور داخلی کشور دیگر، هر دولت ملی بر قلمرو و امور داخلیش دارای حاکمیت است، و این که هر دولت (فارغ از این که چقدر بزرگ یا کوچک باشد) در حقوق بین‌الملل برابر است.

3. UNODC

۴. سازمان پیمان آتلانتیک شمالی در ۴ آوریل ۱۹۴۹ میلادی (۱۵ فروردین ۱۳۲۸) با هدف دفاع جمعی در واشینگتن، دی.سی. پایه‌گذاری شد. این سازمان، بزرگ‌ترین پیمان نظامی در جهان است که ۳۲ کشور در آن عضویت دارند. این پیمان در حال حاضر بزرگ‌ترین پیمان نظامی در جهان است و با پیوستن مونته‌نگرو در سال ۲۰۱۷ میلادی، مقدونیه شمالی در ۲۷ مارس ۲۰۲۰، فنلاند در ۴ آوریل ۲۰۲۳، و سوئد در ۷ مارس ۲۰۲۴ میلادی شمار اعضای آن به ۳۲ عضو رسید.

۵. مرکز دفاع سایبری در تالین، استونی است. حمله ی سایبری در دستور کار ناتو سال‌هاست که قرار گرفته و پس از حمله‌ی سایبری در مقابل استونی در می ۲۰۰۷ ارائه شده است. حمله‌های متوالی در سیستم‌های مالی آنلاین برای چند ساعت است و استونی را از کمک از ناتو بزداشت. مدیران دفاعی یک سیاست دفاعی سایبری برای ناتو در اکتبر ۲۰۰۷ ارائه دادند. که موجب ایجاد مرکز دفاعی سایبری شد. این مرکز به ناتو کمک می‌کند تا تهدیدهای این زمینه را دفع کند. مرکز جدید دفاعی سایبری در ۲۰۰۹ آغاز به کار کرد.

۶. ملک فهد بن عبدالعزیز بن عبدالرحمن بن فیصل بن ترکی بن عبدالله بن محمد بن سعود بن محمد بن مقرن آل سعود زاده ۱۶ مارس ۱۹۲۱ – درگذشته ۱ اوت ۲۰۰۵) فرزند نهم ملک عبدالعزیز، بنیان‌گذار پادشاهی عربستان سعودی، و پنجمین پادشاه این کشور از خاندان آل سعود در سال‌های ۱۹۸۲ – ۲۰۰۵ بود. او با ۳ پادشاه پیش از خود (ملک سعود، ملک فیصل و ملک خالد) و ۲ پادشاه پس از خود (ملک عبدالله و ملک سلمان) برادر می‌باشد. وی در ۱ اوت ۲۰۰۵ در سن ۸۴ سالگی درگذشت.

۷. پِنتاگون مرکز و مقر فرماندهی وزارت دفاع ایالات متحده آمریکا و نیروهای مسلح ایالات متحده آمریکا است.

سلاح کشتار جمعی قابل تصورتر است (Jenkins, 1999, p 68) به‌عنوان مثال می‌توان گفت: بن لادن[1] به‌صورت علنی علیه ایالات متحده آمریکا، خصوصاً علیه نیروهای نظامی مستقر در عربستان سعودی اعلان جنگ کرد. در مقابل، بیانیه هیلاری کلینتون[2] که انتقام آمریکا برای بمب‌گذاری در سفارت‌هایش در شرق آفریقا، اولین نشانه‌های یک جنگ طولانی علیه تروریسم را نشان داد بیان می‌کند که باور اتخاذ الگوی جنگی برای مبارزه با ترور رواج پیدا کرده است. طبق نظر هانگتینتون، منبع دیگر تروریسم ممکن است از ارزیابی ارتباطات بین‌المللی در راستای خطوط ستیزه‌گری و انسانیت بروز کند. در حالت بسیار خشن، این شکست‌های انسانی می‌تواند، هم در بین جوامع و هم در میان دولت‌ها یا گروه‌هایی از دولت‌ها به ویژه وقتی قدرت نظامی، زمین‌گیر یا از کار افتاده هستند، به تروریسم تبدیل شوند. (Jenkins, 1999, p 70) از دیدگاه شبکه‌ای، یکی از ویژگی‌های مهم استفاده از فضای سایبر جهت چنین اقداماتی، توانایی برای تغییر سریع مکان عملیات‌ها از یک نقطه به نقطه دیگر در پاسخ به نیازها و شرایط متغیر است. عملیات‌های انجام شده در مصر، سومالی، استان سیکیانگ در غرب چین، سفارت‌های ایالات متحده آمریکا در کنیا و تانزانیا، این ادعا که اعضای این شبکه می‌توانند با سرعت و چابکی خاص در فواصل طولانی فعالیت کنند را تأیید می‌کند. سازوکارهای سازمانی در این گروه‌ها با گروه‌های سنتی در تضاد هستند. یکی دیگر از ویژگی‌هایی که نسل جدیدتر گروه‌های تروریستی را متمایز می‌کند، استفاده آن‌ها از فناوری اطلاعات است.

۳- ۲- انگیزه در افراطی‌گری سایبری در قرن وحشت

در قرنِ بیست و یکم میلادی اشکال نوینی از سازمان‌های تروریستی در کنار سازمان‌های تروریستی کلاسیک شکل گرفتند. با ظهور سازمان‌های شبکه‌ای با سیستم رهبری افقی، اینترنت به‌عنوان ابزاری پیشرفته در زمینه هدایت و ارتباط استفاده می‌گردد. یک ایمیل نمونه‌ای از اَشکال ارتباط است که به راحتی قابل رمزگذاری است. پیامی که به ظاهر عادی است می‌تواند حاوی پیامی تروریستی باشد[3]. هرچه میزان ارتباط به صورت شبکه سازمانی در یک گروه تروریستی بیشتر باشد، احتمال این که از فناوری اطلاعات برای تصمیم‌گیری شبکه‌ای استفاده گردد، بیشتر می‌شود. پیشرفت‌های اخیر در فناوری اطلاعات سازمان‌های تروریستی شبکه‌ای را تسهیل می‌کند؛ زیرا جریان اطلاعات سریع‌تر و ارزان‌تر و امن‌تر می‌گردد. همانطورکه گروه‌های تروریستی فرا می‌گیرند تا از فناوری اطلاعات جهت تصمیم‌گیری و دیگر اهداف سازمانی استفاده کنند، احتمال این‌که از همان فناوری به‌عنوان یک سلاح تهاجمی برای نابودی و یا اغتشاش استفاده‌نمایند، بیش‌تر می‌شود.

(CTITF, 2011, p31) تروریست‌ها به‌طور کلی دارای چهار انگیزه کلاسیک می‌باشند:

۱. آن‌هایی که به دنبال هدفی خاص هستند و از خشونت برای نشان دادن پیام یا مخالفت خود با موضوعی استفاده می‌کنند، همچون مخالفان سقط جنین. در این مورد، ممکن است به تروریسم به‌عنوان ابزاری جهت رسیدن به اهدافی خاص نگاه شود و سطح خشونت طبق هدف مورد نظر ممکن است محدود و یا بسیار زیاد باشد. مطابق این الگو، روزگای فرض می‌شد که تروریسم نیازی به سلاح‌های کشتار جمعی ندارد؛ چون که چنین ابزارهایی، وسایلی را فراهم می‌کنند که با اهداف ترور بسیار در تضاد هستند. این دیدگاه در ابتدا در بیست سال پیش به‌وسیله برایان جنکینز[4] تشریح گردید[5].

۲. تروریست‌هایی که از خشونت برای ارتقای ایدئولوژی خود استفاده می‌کنند و معمولاً چپ یا راست گرایان افراطی هستند. جناح راست افراطی در راستای گروه‌های چپ‌گرا در دهه ۱۹۷۰میلادی، و اوایل ۱۹۸۰ میلادی مسئول حملات مخرب در ایتالیا و ترکیه بود. در دهه ۱۹۹۰میلادی، جناح راست افراطی‌گر به‌عنوان یک نیروی مروج خشونت در آلمان، استرالیا و سایر مناطق اروپایی پدیدار شد. حملات علیه مهاجران و خارجیان در قلب این اتفاقات بودند[6] (Jenkins, 1999, p 98).

۳. ترویست‌هایی که انگیزه‌های ملی‌گرایانه داشته و به علل نارضایتی‌های جغرافیایی یا نژادی به دنبال استقلال از یک کشور و یا پیوستن به خاک کشور دیگری هستند. در دولت‌هایی همچون ایرلند، مکزیک، ترکیه، مصر و اندونزی، فاصله طبقاتی و اقتصادی باعث نارضایتی‌های قومی و نژادی گردید. (Matsson, 2022, p 43)

---

۱. اُسامه بن محمد بن عوض بن لادِن (۱۰ مارس ۱۹۵۷ – ۲ مه ۲۰۱۱) یکی از اعضای خاندان بن لادن و بنیان‌گذار و رهبر شبکه القاعده بود.

۲. وزیر وقت امور خارجه ایالات متحده امریکا

۳. برای مثال رمزی یوسف که متهم به شرکت در اولین بمب‌گذاری مرکز تجارت جهانی در ۱۹۹۳ شد از رمزگذاری استفاده کرد تا جزئیات یک نقشه برای انهدام خطوط هوایی ایالات متحده آمریکا را پنهان کند پلیس فایل های رمزگذاری شده را در یک کامپیوتر در آپارتمان او در سال ۱۹۹۵ کشف کرد. تروریست دیگری وادی الحجاج که متهم به بمب‌گذاری‌های در سفارت ایالات متحده در شرق آفریقا در سال ۱۹۹۸ شد به همتایان القاعده بر اساس اسناد دادگاه ایمیل های رمزی فرستاد. پرونده یوسف بیشتر از یک سال وقت مقامات اعمال کننده قانون را گرفت تا الگوریتم رمزی سازی استفاده شده توسط تروریست شکسته شود.

4. Brrian Michael Jenkins

۵. برایان مایکل جنکینز (متولد ۱۹۴۲) یک متخصص آمریکایی در زمینه تروریسم و امنیت حمل و نقل است. جنکینز در طول بیش از پنج دهه تحلیل خود به دولت‌ها، شرکت‌های خصوصی، کلیسای کاتولیک و کلیسای انگلستان در مورد تهدیدات تروریستی مشاوره داده است.

۶. چپگراهای اصولگرا (مثل جنبش‌های مارکسیستی، لنینی، ماورماتیسم، استالین) سازمان‌هایی همچون ارتش سرخ ژاپن و ارتش سرخ در آلمان و فرماندهان سرخ در ایتالیا.

۴. تروریست‌هایی که انگیزه‌های مذهبی و سیاسی دارند. این گروه گرایش بیشتری به کشتار دارند، زیرا معتقدند اقداماتشان در جهت دستورات الهی است و اغلب از مذهب و یا آیین خاصی استفاده نامشروع می‌کنند. جنون مذهبی، یا تمایل برای کنترل مستبدانه و یا تلاشی برای هرج و مرج، عامل برخی اقدامات تروریستی است. اوم شینریکیو[1] نمونه اخیر این نوع باور است[2]. این الگو که پس از اعتراضات اجتماعی در ژاپن شکل گرفت و گروه‌های کوچک را ترغیب کرد تا با دنبال کردن یک هرج و مرج بزرگ و نهایی به رستگاری دست یابند. این الگو به‌دنبال برهم ریختن نظم سیاسی، اجتماعی و اقتصادی است. تحقق این هدف ممکن است شامل استفاده از سلاح کشتار جمعی و ایجاد ویرانی مرگبار باشد. ممکن است تروریست‌های مذهبی به خاطر خودویرانی و یا نوعی «پاکسازی» به دنبال آن باشند[3]. تروریسم مذهبی به هیچ عنوان به افراطی‌های اسلامی محدود نمی‌شود. کشمیر، یوگسلاوی سابق، سیک‌ها، مصر یا سودان، بوسنی‌ها، چچنی‌ها و سایر موارد دیگر نشان می‌دهند که تحرکات مذهبی، نقش کلیدی در خشونت سیاسی داشته‌اند و به‌عنوان نیروی ژئوپلتیک مطرح شده‌اند. افراط‌گرایانی که در این دسته‌ها قرار می‌گیرند، با برانگیختن احساسات مذهبی، ملی‌گرایانه و یا ایدئولوژیک طرفداران خود از خشونت در جهت نیل به اهدافشان استفاده می‌کنند. به هرحال درک روان شناختی از تروریست‌ها و انگیزه‌های آنان در چگونگی مبارزه و دفاع در برابر آن‌ها دارای اهمیت است. تروریست‌ها دارای سطوح مختلفی از تحصیلات، رفاه و اشتغال هستند و از لحاظ روحی بسیار ناپایدار می‌باشند. در تمام یا بخشی از ضرورت‌های مذهبی انگیزه اغلب اعمال خشونت بیش‌تر است چنین حوادثی، در مقایسه با حوادثی که توسط سازمان‌های تروریستی- سکولار صورت گرفته است، به میزان قابل توجهی منجر به مرگ‌ومیر و خسارت بیش‌تری می‌شود، گرایش به تروریسم مذهبی از تروریسم- سکولار به دلیل سیستم ارزش اساساً متفاوت است.

1. Aum Shinrikyo

۲. اوم‌شینریکیو یک فرقه ژاپنی است که در چندین کشور به‌عنوان گروه تروریستی شناخته شده‌است، این گروه در سال ۱۹۸۴ توسط شوکو آساهارا به وجود آمد. در سال ۱۹۹۵ میلادی اعضای این فرقه مبادرت به پخش گاز سارین در متروی توکیو کردند در این حملات سیزده نفر کشته و بیش از پنجاه نفر مجروح شدند و هزاران نفر دیگر برای مدتی با عوارض جسمی از این حملات دست به گریبان بودند. اوم‌شینریکیو، که معنی آن «حقیقت عالی» است در دهه ۱۹۸۰ میلادی به عنوان یک گروه معنوی که بر پایه تلفیق باورهای هندوها و بوداییان بود، به‌وجود آمد اما به تدریج به فرقه‌ای تبدیل شد که موجودیت خود را بر اساس پیشگویی‌های مسیحیت درباره آخرالزمان، قرار داد.

۳. در این زمینه، قابل ذکر است که تا ۱۹۹۵ میلادی این فرقه که مسئول حمله گازی کشنده ی سارین در مترو توکیو بود، اعضای زیادی در روسیه نسبت به ژاپن داشت. گروه‌هایی که از طریق انگیزه‌های اخرالزمانی برانگیخته شدند همراه با بلوغ تحرکات تروریستی سابق باعث افزایش پدیده‌ای می‌شوند که والتر لاکیور آنرا تروریسم پست‌مدرن می‌نامد.

۳- ۳- افراطی‌گری و مزایای فضای سایبر

مهم‌ترین امکانات بالقوه‌ای که فضای سایبر در اختیار سازمان‌های تروریستی قرار می‌دهد عبارت است از: عضوگیری، افراطی‌گری، تبلیغات و افزایش بودجه با امکان فرماندهی و کنترل ساده و سریع (Charvat, 2013, p 8). اینترنت برای تروریست‌ها یک ابزار حمله است که حوزه وسیعی را جهت ارتباطات به شکل سریع در اختیار تروریست‌ها قرار می‌دهد. تروریست‌ها به‌ویژه آن‌هایی که با انگیزه سیاسی فعالیت می‌کنند نیاز به تبلیغ و استفاده از رسانه‌ها و مجاری ارتباطی دارند. بنابراین می‌توان چهار مزیت را در استفاده از فضای سایبری جهت اقدامات افراطی‌گرایانه ذکر نمود: تبلیغات، عضوگیری، افزایش بودجه و درآمدزایی و آموزش. که در ذیل به هر کدام خواهیم پرداخت.

۳- ۳- ۱- تبلیغات با ماهیت تروریستی

تبلیغات تروریستی پخش شده از طریق اینترنت طیف گسترده‌ای از مخاطبان را در بر می‌گیرد. این مخاطبان از هواداران واقعی یا بالقوه و یا حامیان یک سازمان یا عقاید افراطی گرفته تا قربانیان مستقیم و یا غیرمستقیم فعالیت‌های تروریستی یا جوامع بین‌المللی و یا حتی زیرمجموعه آن‌ها در نوسان هستند. تبلیغاتی که حامیان واقعی و یا بالقوه را تحت شعاع قرار می‌دهند، بر استخدام، افراط‌گرایی و یا تحریک به تروریسم تمرکز داشته و این کار را از طریق پیام‌هایی انجام می‌دهند که ناقل حس افتخار، موفقیت و تعهد نسبت به هدف هستند. همچنین ممکن است جهت نشان دادن اجرای حملات تروریستی مؤثر به حامیان مالی به‌کار برده‌شود. از دیگر اهداف تبلیغ تروریستی استفاده از دستکاری‌های روانی برای تضعیف اعتقاد افراد در برخی از ارزش‌های اجتماعی خاص و یا انتشار یک حس اضطراب، ترس یا وحشت در جامعه و یا زیر مجموعه‌ای از جامعه است که این‌ها می‌توانند از طریق انتشار اطلاعات گمراه‌کننده، شایعات، تهدیدات خشونت آمیز و یا تصاویر مربوط به اعمال تحریک‌آمیز خشونت صورت گیرند. مخاطبان در نظر گرفته شده ممکن است بینندگان مستقیم مطالب و یا همچنین افرادی باشند که از طریق این موارد تحت تأثیر تبلیغات بالقوه تولید شده قرار گرفته‌اند. باتوجه به جامعه بین‌المللی گسترده‌تر، هدف انتقال، تمایل برای دستیابی به اهداف سیاسی اصیل می‌باشد. (UNODC, 2012, p 4). یونس تسولی[4] تروریستی بود[5] که اگرچه امکان اقدامات فیزیکی داشت؛ اما به القاعده پیوست و وب‌سایتی برای ترویج پیام

4. Younes Tsouli

۵. این فرد به همراه دو همکار خود متهم است که با راه اندازی یک سایت اینترنتی گروه‌های تندرو را به عملیات تروریستی تشویق می‌کردند. مقامات انگلیسی که نام این گروه را "سایبر جهاد" (جهاد الکترونیکی) گذاشته‌اند می‌گویند اعضای این گروه با شبکه القاعده در عراق و پاکستان رابطه گسترده‌ای داشته‌اند.

القاعده راه‌اندازی نمود. در لندن تروریست دیگری که هرگز یکدیگر را ندیده بود امور حمایت مالی را برعهده گرفت. تسولی با استفاده از ۱۲۰۰ کارت اعتباری توانست ۱/۶ میلیون پوند برای مقاصد تروریستی القاعده جمع‌آوری کند؛ اما نهایتاً با صدها فایل و ویدئو که تبلیغات القاعده را نشان می‌داد دستگیر شد (CTITF, 2011, p 31). اینترنت اجازه می‌دهد فرد یا یک گروه کوچک تروریستی بسیار ساده و ارزان با میلیون‌ها مخاطب در ارتباط باشد. تبلیغات یک عنصر ضروری برای تروریسم است. تروریست‌ها از طریق اینترنت بویژه شبکه‌های اجتماعی پیام خود را منتشر نموده و اقدامات خود را توجیه می‌کنند. (International Telecommunication Union, 2008, p 51) داعش[1] برخلاف بسیاری از گروه های تکفیری دیگر، در شبکه‌های اجتماعی همچون توئیتر و فیس‌بوک و اینستاگرام فعال است، اعضا و طرافداران داعش صدها حساب در شبکه توئیتر دارند، آن‌ها در این حساب‌ها به‌صورت شبانه‌روزی، اخبار و تصاویر پیشروی‌ها و عملیات داعش را منتشر می‌کنند. داعش هفت بازوی رسانه‌ای دارد که با استفاده از آن‌ها خشونت و ترور را در جهان ترویج می‌کند، این بازوها عبارتند از شبکه‌های اجناد، الفرقان، الاعتصام، الحیات، مکاتب الولایات، رادیو البیان و پایگاه اینترنتی دابق. این گروه همچنین ۹۰ هزار صفحه از شبکه اجتماعی به ویژه صفحاتی در فیسبوک و توئیتر[2] را به خود اختصاص داده است. داعش وزارت رسانه و اطلاع‌رسانی دارد که محمد العدنانی وزیر آن است. مهم‌ترین هدف بازاریابی اندیشه‌های داعش در جهان است. آنان می‌خواهند با موفقیت در این زمینه نیروهای انسانی بیشتری را به خود جذب کنند. در این زمینه جوانان تندرو بیش از دیگر گروه‌ها مدنظر هستند، ضمن این‌که تأکید بر دولت خلافت اسلامی و تبلیغ حمله به ایالات متحده آمریکا و اروپا در آینده با شعار تسلط کامل بر جهان از اهداف دیگر بازوهای رسانه‌ای داعش است. در ویدیوهای منتسب به داعش نیز درباره این اهداف سخن به میان آمده است[3]. باتوجه به این‌که شبکه‌های اجتماعی همچون توئیتر و فیس‌بوک[4] و اینستاگرام[5] و تیک‌تاک در دولت‌های عربی و میان مسلمانان غرب‌نشین محبوب هستند، خوراک‌های تبلیغاتی داعش به بسیاری از افراد می‌رسد و برخی از آن‌ها جذب این تبلیغات می‌شوند[6]. اگرچه در بسیاری از مناطق، داعش عقب‌نشینی فیزیکی کرده است، این خطر همواره وجود دارد که از جای دیگری و نیز شبکه‌های اجتماعی به‌طور گسترده‌تر، سر بر آورد. (Maloney, 2021, p 16)

۳- ۳- ۲- عضوگیری و استخدام

سازمان‌های تروریستی به‌طور فزاینده‌ای از تبلیغات برای استخدام استفاده می‌کنند که این کار از طریق وب‌سایت‌های محافظت شده با گذرواژه‌ها یا گروه‌های چت اینترنتی با دسترسی محدود صورت می‌گیرد. در دسترس بودن اینترنت، پتانسیل استخدامی جهانی زیادی را در اختیار سازمان‌های تروریستی و هواداران آن قرار می‌دهد. استفاده از موانع تکنولوژیکی برای ورود به سیستم عامل استخدام باعث افزایش پیچیدگی ردیابی فعالیت‌های مرتبط با تروریسم می‌شود که این کار توسط پرسنل اجرایی قانون و اطلاعات صورت می‌گیرد. تبلیغات تروریستی اغلب برای جذب گروه‌های آسیب‌پذیر و منزوی جامعه تهیه می‌شوند. روند استخدام در افراط‌گرایی معمولاً از باورهای فرد در زمینه بی‌عدالتی، طرد و یا تحقیر بهره‌گیری می‌کند. تبلیغات معمولاً از عواملی ازجمله سن، جنسیت، و یا شرایط اجتماعی، اقتصادی سوء استفاده می‌کنند. رشد افراط‌گرایی به شدت با مبحث قابلیت اینترنت

---

1. ISIS
2. Twitter

۳. هریک از کانال‌های هفتگانه‌ای که نام برده شد ماموریت مشخصی دارند اما اهداف سیاسی این کانال ها را می‌توان به‌طور خلاصه این‌گونه تشریح کرد. استودیو «اجناد» اصلی‌ترین بازوی رسانه‌ای داعش است. در این استودیو سرودهای حماسی اعم از دینی و جهادی تهیه می‌شود. داعش برای راه اندازی این استودیو حدود یک میلیارد دلار هزینه کرده است. داعش برای شبکه «الفرقان»، به‌عنوان دومین بازوی رسانه‌ای خود حدود ۲۰۰ میلیون دلار هزینه کرده است، این شبکه سال‌ها قبل و با کمک القاعده راه‌اندازی شده بود اما پس از اعلام موجودیت دولت اسلامی عراق و شام، تحت مالکیت این گروه درآمد.کانال الاعتصام سومین بازوی رسانه ای داعش، با ۵۰۰ میلیون دلار بودجه ایجاد شده است. این شبکه تلویزیونی خبرنگاران متعددی در عراق و سوریه دارد که ماموریتشان تهیه اخبار صوتی و تصویری از درگیری‌های میدانی است. شبکه الحیات چهارمین بازوی رسانه‌ای داعش است که با بودجه‌ای بیش از ۵۰۰ میلیون دلار راه‌اندازی شده است. شبکه الحیات مرکز اصلی مونتاژ ویدیوهایی است که از جنایات داعش تهیه می‌شود. ویدیوهایی که در این شبکه تهیه می‌شود عالی‌ترین کیفیت صدا و تصویر را دارد و در آن‌ها از سرودهای حماسی و تأثیر گذار استفاده شده است. روند فعالیت شبکه الحیات را مجموعه‌ای از روانپزشکان، جامعه شناسان، فقها و متشرعین عضو داعش نظارت می‌کنند. مکاتب الولایات پنجمین بازوی رسانه‌ای داعش است که با بودجه‌ای ۲۰۰ میلیون دلاری ایجاد شده است. این شبکه مجموعه برنامه‌هایی را منتشر می‌کند که مخاطب آنها ولایات (تعبیری از استان‌ها در دولت اسلامی مورد ادعای داعش) تحت امر داعش است. رادیوی «البیان» ششمین بازوی تبلیغاتی داعش است که در موصل و الانبار در عراق، رقه در سوریه و همچنین در اینترنت پخش می‌شود. برای راه‌اندازی این شبکه رادیویی ۱۰۰ میلیون دلار هزینه شده است. این رادیو به پخش قرآن و سرودهای حماسی- جهادی می‌پردازد؛ اما لابلای پخش قرآن و سرود خبرهایی نیز منتشر می‌کند تا بیش‌تر با احساسات مخاطبان بازی کند. به نظر می‌رسد مخاطب اصلی این رادیو ستیزه جویان داعش در میادین نبرد عراق و شام و ماموریت اصلی رادیو البیان روحیه دادن به این افراد است. هفتمین و آخرین بازوی رسانه‌ای داعش پایگاه اینترنتی «دابق» است. این پایگاه اینترنتی به منزله هفته نامه اینترنتی و همزمان پایگاه الکترونیکی روزانه عمل می‌کند. داعش برای پیشبرد اهدافش ۵۰۰ میلیون دلار هزینه برای دابق اختصاص داده است به نقل از: http://www.entekhab.ir/fa/news/194015.

4. Facebook
5. Instagram

۶. داعش تلاش کرده است که عملیات‌های نظامی‌اش را به صورت کامل فیلم‌برداری کند، داعش این فیلم ها را با یک تدوین حرفه‌ای در اینترنت منتشر کند، انتشار فیلم‌های عملیات های بزرگ و موفق داعش در عراق و سوریه که با سرودهای جهادی همراه است، باعث جذب افراد بسیاری به داعش شده است. در تبلیغات ویدیویی‌اش بر نیروهای غیر سوری تاکید زیادی می‌شود و واحد تبلیغاتی داعش، مصاحبه‌های بسیاری را با اعضای غیرسوری گروه داعش می‌کند تا آن‌ها، مسلمانان دیگر را به پیوستن به داعش تشویق کنند.

به عنوان یک وسیله جهت استخدام و انتشار تبلیغات در ارتباط است. انجمن‌های مجازی فاصله‌های جغرافیایی را از بین می‌برند و شبکه‌های اجتماعی همچون توییتر، فیس‌بوک، یوتیوب و ...رادیکال‌های غیرمرتبط را با یکدیگر آشنا می‌کند. پیام‌های بین اعضا از طریق تصاویر یا هرزنامه‌ها یا ایمیل‌هایی که ارسال نشده در حساب کاربری ذخیره می‌شوند، رد و بدل می‌شوند (UNODC, 2012, p 5). عضوگیری و توسعه افراطی‌گری از عناصر ضروری یک سازمان تروریستی است. سازمان‌های تروریستی در حوزه اقدامات سایبری‌شان در پی افرادی هستند: قابل اعتماد، متخصص و باهوش که دارای مهارت‌های فناوری اطلاعات باشند. در اتاق‌های گفتگو و وب سایت‌ها، توانایی تروریست‌ها در به دست آوردن توجه مخاطبان افزایش می‌یابد. ممکن است موضوع یک اتاق گفتگو یا گروه، حقوق حیوانات باشد؛ اما تروریست‌ها با کنترل و نظارت بر آن‌ها، افراد هم فکر با خود را پیدا می‌کنند. این شکل تماس می‌تواند به‌طور مؤثر چند نفر را به‌طور هم‌زمان در برگیرد. فردی که اداره‌کننده گروه است می‌تواند از افرادی که گمان می‌کند در یک جریان فکری با او هستند، بخواهد به‌طور فعال‌تری در گروه مشارکت کند و با دانشی که خود در مورد مسایل تبلیغاتی دارد گفتگو را به‌سمت مسائل سیاسی و جدی می‌کشاند. در مرحله بعد فردی را که نشانه هایی از تمایل به عضویت در یک سازمان تروریستی را از خود نشان داده به فرد بالاتر گروه معرفی می‌شود تا طبق برنامه‌ریزی آموزش ببینید و مهارت‌هایش سنجیده شود. این افراد از هویت اصلی راهنما یا کنترل کننده خود هرگز مطلع نمی‌شوند. ایمیل یکی از ساده‌ترین اشکال ارتباط است که به راحتی قابل کدگذاری است و با ارسال پیامی که در ظاهر عادی است می‌توان پیامی حاوی دستور به اقدامات تروریستی ارسال نمود. گاهی حتی این ایمیل‌ها ارسال هم نمی‌شوند و در قسمت پیش‌نویس[1] ذخیره شده و دیگر عضو با داشتن رمز عبور به آن دسترسی پیدا می‌کند. که این امکان رهگیری ایمیل‌ها را غیرممکن می‌گرداند (Charvat, 2013, p 5-7). نکته شگفت‌آور این که در پی یک نظرسنجی که در صفحه‌های اجتماعی صورت گرفته برخی از کسانی که جذب گروه‌های جهادی می‌شوند با هدف گردشگری و توریسم و ورود به مناطق تحت کنترل گروه‌های جهادی اقدام به همکاری با آن‌ها می‌کنند. فیگارو این جهادی ها را «دشمنان از داخل» لقب داده که شناسنامه فرانسوی دارند و با همکاری با گروه‌های جهادی علیه امنیت ملی فرانسه فعالیت می‌کنند[2].

۳- ۳- ۳- افزایش بودجه و درآمدزایی سازمان‌های تروریستی

افزایش منابع مالی بعد دیگری از فعالیت‌های سازمان‌های تروریستی است که اینترنت آن را تسهیل می‌کند. در جهان مدرن، بانکداری الکترونیک به‌صورت مستقیم یا غیرمستقیم و ابزارهای قانونی و غیرقانونی در دسترس است. اینترنت و فضای سایبر فرصت‌های زیادی را برای کسب و کار و امور شبه خیریه، جهت درآمدزایی ایجاد می‌کند. حمل‌ونقل بین‌المللی پول از این طریق امکان ردیابی و مسدودسازی را مشکل می‌کند. از سوی دیگر بسیاری از سازمان‌های تروریستی، فعالیت‌های خود را از طریق اشکال سنتی جرایم آنلاین انجام می‌دهند. جرم‌هایی از قبیل جعل کارت اعتباری و سرقت مالکیت فکری. تروریست‌ها و حامیانشان از اینترنت به چهار شیوه برای کسب درآمد و افزایش بودجه استفاده می‌کنند درخواست مستقیم از طرفداران، استفاده از مزایای تجارت الکترونیک، بهره‌مندی از روش‌های پرداخت آنلاین و نهادهای خیریه. در این شیوه‌ها، ترویست‌ها یا به‌طور مستقیم از طرفدارانشان از طریق وب سایت‌ها، اتاق های گفتگو و شبکه‌های اجتماعی می‌خواهند تا به آن‌ها کمک مالی کنند. این کمک‌های مالی از طریق پرداخت آنلاین از طریق کارت‌های اعتباری و هویت‌های جعلی صورت می‌گیرد. گاهی نیز تروریست‌ها برای انجام مقاصد مالی شان از طریق تاسیس نهادهای به ظاهر قانونی همچون خیریه‌ها اقدام می‌کنند. این خیریه‌ها اغلب ادعای کمک‌های بشردوستانه دارند اما در حقیقت برای کلاهبرداری از افراد در جهت کسب منافع مالی برای مقاصد شوم خود هستند[3] (UNODC, 2012, p 7).

۳- ۳- ۴- آموزش، تحقیقات و توسعه جهت انجام حمله تروریستی

مرحله نهایی آموزش، تحقیقات و توسعه است که در یک حمله تروریستی ضروری است. اینترنت حوزه وسیعی را در اختیار سازمان‌های تروریستی قرار

1. Draft

۲. پژوهشی که توسط مرکز بین‌المللی مطالعات افراط‌گرایی در دانشکده سلطنتی لندن در آوریل ۲۰۱۴ صورت گرفته است، اعلام می‌کند که یکی از گروه‌های جهادی در یکی از صفحات اجتماعی اقدام به تبلیغ برای جذب نیرو کرده که توانسته است از قبل آن ۱۱ هزار نیرو جذب کند که ۱۹۰۰ نفر آن‌ها از کشورهای اروپایی بوده‌اند. در این میان اتباع فرانسوی با ۴۲۱ سرباز در راس هستند و بعد از آن‌ها بریتانیایی ها با ۳۶۶ و بلژیکی‌ها با ۲۶۹ و آلمانی‌ها با ۲۴۹ به ترتیب در رده‌های بعدی قرار دارند. بنا به این گزارش جنگ سوریه نخستین نبرد در نوع خود در تاریخ است که در آن اینترنت و صفحات اجتماعی جایگاه ویژه‌ای دارند. این پژوهش همچنین تاکید می‌کند که ۱۹۰ مبارز غربی فعال در سوریه نقشی محوری برای تبلیغ در ایالات متحده امریکا، استرالیا و بریتانیا در ترویج افکار جهادی دارند. در تفکیک سایت‌های جذب نیرو برای این نیروها نیز ۶۱/۵ درصد وابسته به دولت اسلامی در عراق و شام، موسوم به داعش و ۱۷،۵ درصد وابسته به جبهه النصره است و این در حالی است که سایت‌های متعلق به ارتش آزاد سوریه و احرار الشام بیش از دو درصد نیستند به نقل از http://www.irdiplomacy.ir/fa/page/1932761.

۳. در خاورمیانه خیریه‌هایی با عناوین زیر در خدمت فعالیت های تروریستی بوده‌اند:
Benevolence International Foundation, Global Relief Foundation and the Holy Land Foundation for Relief and Developmen

می‌دهد تا به راحتی و سرعت اطلاعات را به اشتراک گذارند و از قابلیت‌های جستجو استفاده کنند. نمونه‌های بسیاری از جزوات و دستورالعمل‌های تروریستی در اینترنت وجود دارد که در آن شیوه‌های تهیه بمب با مواد در دسترس آموزش داده می‌شود. در سال ۱۹۹۱ میلادی دیوید کوپلند[1] در لندن ۳ نفر را در یک حمله تروریستی کشت و ۱۳۹ نفر را مجروح کرد. اقدام وی در سه مرحله بمب گذاری صورت گرفت و بعدها در جریان محاکمه گفت شیوه ساخت بمب را از دفترچه راهنمای تروریست‌ها که از اینترنت به دست آورده بود، آموخته است. (بوگانسکی و پترسکی، ۱۳۹۴، ص ۲۵۴) این قابلیت برای سازمان‌های تروریستی که شبکه سلسله مراتبی افقی دارند دارای جذابیت بیشتری است. آن‌ها از این طریق می‌توانند بدون تماس رسمی، عملیات خود را انجام دهند. فلسفه آن‌ها حمایت آنلاین از طرفداران است که بدون حضور فیزیکی بتوانند آموزش‌های لازم را ببینند (Charvat, 2012, p 9). تروریست‌ها امروزه از اینترنت برای آموزش اعضا نیز استفاده می‌کنند. این آموزه‌ها شامل چگونگی پیوستن به گروه تروریستی، ساخت مواد انفجاری و خطرناک، شیوه سازماندهی حملات، استفاده از ویروس‌ها، هک و نیز ساخت شبکه‌های ارتباطی میان اعضا برای تبادل اطلاعات است. این دستورالعمل‌ها همچون یک نقشه واقعی عمل می‌کنند[2].

۴- نتیجه‌گیری

تروریسم، در مقام یک پدیده پیچیده و چندوجهی، نه صرفاً ابزاری برای جلب توجه بلکه روشی برای تثبیت هویت مرتکبان تلقی می‌شود. در این راستا، می‌توان گفت که تروریسم در پی القای این پیام است: «من مرتکب عمل تروریستی شدم، پس هستم.» چنین اقداماتی به مرتکبان امکان می‌دهد تا از طریق اعمال خشونت‌آمیز و ایجاد وحشت، هویتی متمایز برای خود بسازند. این نوع رفتار به وضوح فراتر از استفاده ابزاری از خشونت است و گاه در قالب ابزاری برای بازتعریف نظم موجود و برهم زدن وضعیت کنونی جهت نیل به نظم جدیدی در آینده مطرح می‌شود. این رویکرد در ایدئولوژی برخی گروه‌های تندرو مذهبی و همچنین در آموزه‌های گروه‌های هزاره‌گرا و آخرالزمانی مشاهده می‌شود. ویژگی اصلی و ممتاز تروریسم، توانایی آن در حمله مستقیم به امنیت فردی افراد است. با تحول مفهوم امنیت بین‌المللی و تفسیرهای متنوع از توسل به زور در قالب تروریسم، به‌ویژه طبق تعریف تجاوز در قطعنامه‌های بین‌المللی، تروریسم سایبری نیز به منزله نقض اصل عدم مداخله در امور داخلی دولت‌ها شناخته می‌شود. این نوع تروریسم با بهره‌گیری از فناوری اطلاعات و ابزارهای سایبری، نه‌تنها به دسترسی آزاد به اطلاعات آسیب می‌رساند، بلکه از منظر حقوقی، به دلیل استفاده از بدافزارهایی[3] نظیر استاکس‌نت، می‌تواند به‌عنوان شکلی از حمله نظامی تلقی گردد. قابلیت‌های فضای مجازی به گروه‌های تروریستی این امکان را می‌دهد که با حملات سایبری علیه زیرساخت‌های حیاتی، رعب و وحشت را به شکلی مؤثرتر ترویج کنند. افزون بر این، توسعه افراط‌گرایی از طریق ابزارهای دیجیتال به سهولت بیشتری انجام می‌پذیرد. برای نمونه، اسناد آموزشی گروه القاعده که در افغانستان کشف شده است، حاکی از آن است که تروریست‌ها می‌توانند از منابع آزاد برای جمع‌آوری اطلاعات استفاده کنند، به‌گونه‌ای که تا ۸۰ درصد اطلاعات لازم درباره اهداف خود را بدون نیاز به ابزارهای غیرقانونی به دست آورند. همچنین، حوادثی نظیر افشاگری‌های ویکی‌لیکس در سال ۲۰۱۱ میلادی نشان‌دهنده گستره وسیع اطلاعاتی است که از طریق اینترنت قابل دسترسی است. باتوجه به تازگی حملات سایبری، تاکنون هیچ نظام حقوقی بین‌المللی نتوانسته است به‌طور صریح این نوع حملات را محکوم کند. آشکار است که چنین حملاتی از منظر حقوقی و اجرایی نه به‌آسانی قابل کنترل هستند و نه می‌توانند در چهارچوب قوانین موجود محدود شوند. خطر گسترش افراط‌گرایی خشن که قلب خاورمیانه را درگیر کرده و به سمت اروپا در حال پیشروی است، نیازمند اقدامات فوری و هماهنگ بین‌المللی است. این تهدیدات، بربریتی را به نمایش می‌گذارند که هیچ مرزی نمی‌شناسد و جان انسان‌ها را بی‌حرمت می‌کند. جهت مقابله با این چالش‌ها، ضرورت اتخاذ رویکردهای نوین و تقویت همکاری‌های بین‌المللی در مبارزه با این معضل جهانی بیش از پیش احساس می‌شود.

پیشنهادات برای مقابله با تروریسم سایبری در سه سطح حقوقی، سازمانی و فنی:

۱. راه‌حل‌های حقوقی:

- جرم‌انگاری حملات سایبری در قوانین داخلی.
- همکاری بین‌المللی برای کشف جرم و مجازات مرتکبان.
- استرداد مجرمان و ایجاد قوانین دادرسی ویژه.

1. David Copeland

۲. به طور مثال مجله ای به نام INSPIRE که القاعده به شکل اینترنتی منتشر می‌کرد، حاوی بیانیه‌های منتسب به بن لادن و ایمن الظواهری، شیوه‌های آمادگی برای جهاد، آموزه‌های ایدئولوژیک و تشویق طرفداران به فعالیت‌های تروریستی بود. این نشریه در پاییز ۲۰۱۰، شیوه استفاده از وسیله‌نقلیه با تمام جزییات آن را برای انجام حمله و بمب‌گذاری آموزش می‌داد. (UNODC, 2012, p 7)

۳. بدافزار (malware) هر نوع نرم‌افزاری است که از روی عمد برای آسیب‌زدن به رایانه، سرور، کارخواه، یا شبکه رایانه‌ای طراحی شده است (در مقایسه با اشکال (باگ) نرم‌افزاری که نوعی نرم‌افزار است که منجر به آسیب غیرعمدی، مثلاً به علت یک عیب و ایراد می‌شود).

۲. راه‌حل‌های سازمانی:

- پیوستن به کنوانسیون‌های منطقه‌ای و بین‌المللی.
- تقویت سیستم‌های گزارش‌دهی و ارائه اسناد معتبر.
- آموزش نیروهای متخصص، به‌ویژه پلیس سایبری.

۳. راه‌حل‌های فنی:

- تقویت همکاری‌های فنی در سطح دوجانبه و چندجانبه.
- استفاده از فناوری برای مقابله با تروریسم، با در نظر گرفتن چارچوب‌های قانونی و سیاست‌های عمومی شفاف.
- تحلیل آسیب‌پذیری‌های گروه‌های تروریستی از طریق فناوری‌های پیشرفته.
- ضرورت تضمین حقوق بشر در اقدامات ضدتروریستی، از جمله حفاظت از آزادی بیان و حق دسترسی به اطلاعات.
- مسئولیت دولت‌ها در قبال حملات سایبری و ضرورت تطبیق استانداردهای بین‌المللی با ماهیت این تهدیدات.
- ایجاد همکاری گسترده میان بخش‌های خصوصی و دولتی، به‌ویژه در مدیریت زیرساخت‌های حیاتی و به اشتراک‌گذاری اطلاعات. در مجموع، مقابله با تروریسم سایبری مستلزم رویکردی جامع و چندبعدی است که ابعاد حقوقی، فنی و سازمانی آن با یکدیگر هماهنگ شده و در چارچوب‌های قانونی روشن تعریف گردد.

منابع

[۱] بوگانسکی، میتکو و پترسکی، دریژ. (۱۳۹۴). تروریسم سایبری، تهدید علیه امنیت جهانی، ترجمه ندا نیازمند، مجموعه مقالات تروریسم شناسی، نگاه بینه.

[۲] پاکزاد، بتول. (۱۳۸۹). تروریسم سایبری؛ تهدید نوین علیه امنیت ملی، دفتر گسترش تولید علم معاونت پژوهشی دانشگاه آزاد اسلامی، تهران.

[۳] ضیایی بیگدلی، محمدرضا. (۱۳۹۲). حقوق بین‌الملل بشردوستانه، انتشارات گنج دانش، تهران.

[۴] میربد، لیلا. (۱۳۸۸). بررسی جرایم علیه کودکان در اینترنت با توجه به اسناد بین‌المللی. پایان نامه کارشناسی ارشد. حقوق بین‌الملل. دانشکده حقوق. دانشگاه ازاد اسلامی واحد تهران مرکزی.

[۵] ضیایی بیگدلی، محمدرضا و همکاران. (۱۳۸۷). ترجمه‌ی آراء و نظریات مشورتی دیوان بین‌المللی دادگستری، جلد اول، انتشارات دانشگاه علامه طباطبایی، تهران.

[۶] بیگ‌زاده، ابراهیم. (۱۳۹۴). حقوق سازمان‌های بین‌المللی، جلد دوم، انتشارات مجد، تهران.

[۷] اتان شاو، مالکوم. (۱۳۹۴). روش‌های حل و فصل مسالمت آمیز اختلافات بین‌المللی، مترجمان: حسینی، لطیفه و حسینی، نرگس، انتشارات خرسندی، تهران.

[۸] حاتمی، عباس و رضایی، فاطمه. (۱۳۹۸). تحلیل تطبیقی شیوه‌های تأمین منابع مالی القاعده و داعش: رهیافتی در اقتصاد سیاسی تروریسم. مطالعات اقتصاد سیاسی بین‌الملل.

[9] Ambos, K. (2016). Individual Criminal Responsibility for Cyber Aggression. Journal of Conflict & Security Law, 21(3), 495-504.

[10] Cassim, F. (2012). Addressing the specter of cyber terrorism, vol 15. No2,avalable at: www.dx.doi.org

[11] Charvat, J. (2012). Cyber Terrorism: A New Dimension in Battle space , available at: https://ccdcoe.org/sites/defaul

[12] Clarke, C. P. (2018). An Overview of Current Trends in Terrorism and Illicit Finance: Lessons from the Islamic State in Iraq and Syria and Other Emerging Threats, Santa Monica: Rand Corporation.

[13] Coleman, Kevin. (2012). Cyber Terrorism Computer Crime, Research Centre, available at: Counter-Terrorism Implementation Task Force (CTITF),(2009), Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes

[14] Darcy, S. (2021). Accident And Design: Recognising Victims Of Aggression In International Law. International & Comparative Law Quarterly, 70(1), pp 103-132.

[15] Denning, Dorothy. (2002). The Future of Terror, Crime, and Militancy, RAND Corporation.

[16] Dormonn, Knut. (2013). Applicability of the Additional Protocols to Computer Network Attack, available at: https://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

[17] Geller, Pamela. (2012). Islamic scholars approve e-jihad and cyber warfare, available at: http://atlasshrugs2000.typepad.com/atlas_shrugs/2012/01/islamic-scholars-approve-e-jihad-and-cyber-warfare.html

[18] Gray, David and Head, Albon. (2009). The importance of the internet to the post-modern terrorist and its role as a form of safe haven, European Journal of Scientific Research 25(3).

available at: http://www.nato.int/cps/en/natolive/official_texts_63654.htm

[33] Roshanaei, M. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. Journal of Computer and Communications, 9 (8), 80-102

[34] Ruys, T. (2018). Criminalizing Aggression: How the Future of the Law on the Use of Force Rests in the Hands of the ICC. European Journal of International Law, 29(3), , 887–917.

[35] Shackelford, Scott. (2010). state responsibility for cyber-attacks, conference of cyber conflict, Tallinn, Estonia. available at: https://ccdcoe.org

[36] Stalinsky, Steven. (2012). Muslim Brotherhood restoration of caliphate and new era of cyber jihad, available at: http://www.rightsidenews.com/2012061916452/world/terrorism/muslim-brotherhood-restoration-of-caliphate-and-new-era-of-cyber-jihad.html

[37] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. (2013). Cambridge University Press

[38] United Nations Office on Drugs and Crime .(2012). The use of internet for terrorist purposes, United Nations.

[39] Williams, R. (2007). "The psychosocial consequences for children of mass violence, terrorism and disasters". International Review of Psychiatry, 19(3), 263-277.

[40] www.hamshahrionline.ir

[41] Yunos, Z., and Sulaman, S. (2017). Understanding Cyber Terrorism from Motivational Perspectives. Journal of Information Warfare, 16(4), 1–13. https://www.jstor.org/stable/26504114

[19] Heller, kj. (2020). Who Is Afraid of the Crime of Aggression?. Journal of International Criminal Justice,. 18(1), 2019-2031.

[20] Horowitz, J. (2020). Cyber Operations under International Humanitarian Law: Perspectives from the ICRC. ASIL Insights.

[21] http://www.crime research.org/library/Cyber-terrorism

[22] http://www.irdiplomacy.ir/fa/page/1932761

[23] http://www.jonoubnews.ir/showpage.aspx?id=149246

[24] International Telecommunication Union High level expert group. (2008). GLOBAL STRATEGIC REPORT, Geneva, Switzerland.

[25] Jenkins, brain. (1999). countering the new terrorism, available at: www.rand.org/content/dam/rand/pubs.

[26] Lee, Newton. (2013). countering terrorism and cyber security, spring, New York.

[27] Lee, Robert. (2012). Stuxnet and cyber deterrence, available at: http://www. infosecisland. comblogview/22168-Stuxnet-and-Cyber-Deterrence.html.

[28] Madubuike-Ekwe, J. N. (2021). Cyberattack and the Use of Force in International Law. Beijing Law Review, 12, 631-649.

[29] Maloney D. (2021). A youthful metaverse: towards designing safe, equitable, and emotionally fulfilling social virtual reality spaces for younger users.

[30] Matsson D. (2022). GDPR, Blockchain & Personal data- The rights of the individual v. the integrity of Blockchain.

[31] McDougall, C. (2021). The Crime of Aggression under the Rome Statute of the International Criminal Court. 2nd edition, Cambridge University Press.

[32] NATO. (2010). assured security; dynamic engagement,