تاریخ دریافت: ۱۴۰۲/۱۲/۲۰ تاریخ پذیرش: ۱۴۰۳/۴/۱۵ صفحه ۷۳ تا ۹۱

محافظت از امنیت سکوهای دیجیتالی در قبال جرایم تروریستی؛ راهبردی در ارتقای امنیت دیجیتالی دولت‌ها

پیمان نمامیان[۱]، مهدی شهبازی[۲]

چکیده

امنیت سکوهای دیجیتالی بعد اقتصادی و اجتماعی امنیت دیجیتالی است. حفظ اعتماد در اقتصادهای به طور فزاینده وابسته به دیجیتال و افزایش انعطاف‌پذیری در جهانی که در معرض درگیری‌های ژئوپلیتیک فزاینده و جرایم دیجیتالی بوده که امری ضروری است. روند افزایش روزافزون هنجارهای حکمرانی سکوهای دیجیتالی به طور بالقوه باعث می‌شود که حقوق بین المللی آینده در مورد فضای دیجیتال به سختی به طور مؤثر بر بازیگران دولتی تحمیل شود. این در حالی است که با ظهور جامعه مبتنی بر اطلاعات، خطراتی که تروریست‌های دیجیتال بتوانند با حملات رایانه‌ای به داده‌ها آسیب برسانند، به وجود آمد. در صورتی که حقوق بین‌المللی آینده در مورد فضای دیجیتال توسط حکمرانی سکوهای دیجیتال به بهای منافع بازیگران غیردولتی آنها تغییر می‌کند. علی‌رغم عدم امکان تصویب یک سند حقوقی راجع به حاکمیت بر اینترنت و فضای دیجیتالی از سوی جامعه بین‌المللی به جهت نبود اجماع جهانی، اما این امکان برای هماهنگی در اِعمال واکنش بین‌المللی موفقیت‌آمیز به تحرکات تروریست‌ها در فضای دیجیتالی راهبردی است که می‌تواند در مقابله با این‌گونه اقدامات مؤثر واقع گردد.

واژگان کلیدی: رسانه‌های اجتماعی، فضای دیجیتال، جرایم دیجیتالی، جرایم تروریستی، امنیت دیجیتالی.

۱. دانشیار حقوق کیفری و جرم‌شناسی دانشکده علوم اداری و اقتصاد دانشگاه اراک، اراک، ایران.(نویسنده مسئول)
p_namamian1512@yahoo.com

۲ پژوهشگر دکتری حقوق بین الملل عمومی. m.shahbazi618@gmail.com

مقدمه

چالش‌های جدیدی برای حقوق فردی و انسجام اجتماعی پدیدار شده است. قانون به‌عنوان ابزاری برای تضمین حقوق، توزیع تعهدات و فراهم کردن جوامع باثبات، باید مطابق با فناوری تغییر کند. پس از اختراع اینترنت، روندهای نوینی نظیر دیجیتالی شدن، سرمایه‌داری نظارتی و افزایش عملیات مخرب دیجیتال، همگی اعمال حقوق بین‌المللی موجود در فضای دیجیتالی را به چالش کشیده‌اند.[۱]

در فرآیند ساخت هنجارهای بین‌المللی امنیت سکوهای دیجیتالی و عملیات دیجیتالی، لازم است اهمیت جدید آنها توسعه یابد؛ نخست، حکمرانی فضای دیجیتالی گسترش حکمرانی دولت در فضای را رقم خواهد زد. بنابراین، حکمرانی دیجیتالی باید متقابلاً محترم شمرده شود. دوم، هر دولتی باید متعهد شود که به فضای دیجیتالی یک کشور دیگر تعرض، حمله یا تخریب نکند، در حالی که هر دولتی مسئولیت دارد و از حق محافظت از فضای دیجیتالی خود در برابر تهدید، مداخله و تخریب برخوردار است. سوم، نباید از فضای دیجیتالی برای مداخله در امور داخلی یا بی‌ثبات کردن نظم سیاسی، اقتصادی و اجتماعی سایر کشورها استفاده کرد و باید به تنوع سیاست‌های فضای دیجیتالی در کشورهای مختلف احترام گذاشت. چهارم، همه دولت‌ها باید تکالیف خود را در زمینه حکمرانی فضای دیجیتالی بین‌المللی انجام دهند. از اینرو، فضای دیجیتالی باید فضایی صلح‌آمیز، ایمن و باز باشد که در آن چین به تقویت همکاری با سایر دولت‌ها، حفظ امنیت دیجیتالی در کنار هم و ساختن آینده‌ای مشترک برای نوع بشر اختصاص دارد(Zhu and Chen, 2022: 187).

امنیت سکوهای دیجتالی اکنون یک موضوع مهم برای کلیه دولت‌ها است.[۲] دولت‌ها باید از خود در قبال این تهدیدهای ناشی از جرایم تروریستی ارتکابی در سکوهای دیجیتالی در حال

---

۱. در دهه‌های اخیر شاهد توسعه فناوری دیجیتالی و گسترش فضای مجازی بوده ایم که جامعه بشری را به شدت تحت تأثیر قرار داده است. فضای مجازی به اندازه زمین، دریا، هوا و فضا در حال تبدیل شدن به یک حوزه مهم است، اما ساختار سنتی سیاسی، اقتصادی و اجتماعی جامعه بین‌المللی را به چالش می‌کشد؛ اگرچه هیچ تعریف مورد توافق جهانی از حاکمیت وجود ندارد، اما به رسمیت شناختن حق دولت برای اعمال کنترل انحصاری بر قلمرو خود اجماع اساسی در مورد این موضوع است. برای فضای مجازی که مجازی است، مفهوم حاکمیت یک توهم به نظر می‌رسد، اما از اهمیت زیادی برخوردار است و هم‌چنان از بسیاری جهات مرتبط است.

2. https://www.finance-ni.gov.uk/publications/cyber-security-government-cyber-security-strategy-2022-2030

توسعه محافظت کنند. از اینرو، سیاست‌گذاری امنیت دیجیتالی یک حوزه چند وجهی است که نیازمند یک رویکرد راهبردی مبتنی بر یک چشم‌انداز روشن است تا اطمینان حاصل شود که همه ذینفعان، از سازمان‌های دولتی گرفته تا سازمان‌های بخش دولتی و خصوصی و افراد، به شیوه‌ای منسجم، اثربخش و قابل اتکاء ملحق شوند.[1]

فضای دیجیتالی در نظام بین‌الملل از اهمیت بالایی برخوردار شده است، زیرا ماهیت آن سیستم را پس از اتکای فزاینده به فناوری تحت تأثیر قرار می‌دهد. علاوه بر این، از طریق ظهور نوع جدیدی از قدرت، که قدرت الکترونیکی یا دیجیتالی است، به پایان دادن به انحصار قدرت به معنای سنتی قدرت سخت کمک کرد. علاوه بر این، این قدرت برای هر کسی که دانش فناورانه را در اختیار دارد و توانایی استفاده از آن را برای دستیابی به اهداف خود دارد، قابل دسترس شد. با این حال، نه تنها به صورت مسالمت آمیز، بلکه توسط گروه‌های تروریستی برای انجام حملات خود استفاده می‌شود.

بشر به عنوان یک پدیده اجتماعی در حال ظهور در عصر اطلاعات، جرایم دیجیتالی (به‌مثابه یکی از مصادیق «جرایم فناورانه»[2]) به دلیل تخریب زیاد و تأثیر گسترده، نگرانی‌های فزاینده‌ای را در سراسر جهان برانگیخته است. در کنار توسعه سریع فناوری اطلاعات و ارتباطات و شیوع فزاینده اینترنت، این فعالیت‌های جنایی به‌طور قابل توجهی اقتصاد جهانی، امنیت ملی، ثبات اجتماعی و علایق فردی را مختل می‌کند؛ اگرچه تخمین هزینه دقیق مالی جرایم دیجیتالی دشوار است. شواهد آماری از دولت‌ها و صنایع نشان می‌دهد که خسارات اقتصادی ناشی از جرایم دیجیتالی بسیار عظیم بوده و در حال حاضر به سرعت در حال افزایش است (McAfee, 2021).

در عصر دیجیتال نوین، اطلاعات می‌توانند در کسری از ثانیه در سراسر جهان به صورت ویروسی انتشار یابند. جرایم دیجیتال اغلب به عنوان جرایم رایانه‌ای یا جرایم با فناوری پیشرفته تعریف می‌شوند. آنها به قصد آسیب رساندن به اموال دیگران، تمامیت شخصی، جان دیگران و سرقت اقلام و اطلاعات ارزشمند از افراد دیگر متعهد شده‌اند. نمونه‌هایی از جرایم دیجیتالی شامل ویروس‌های رایانه‌ای، توزیع محتوای غیرقانونی و غیراخلاقی، هک یا دسترسی غیرمجاز، تغییر غیرمجاز داده‌های رایانه‌ای، مخدوش کردن گسترده برخط، سرقت هویت یا فیشینگ، اسکوات دیجیتال، تعقیب دیجیتال و بسیاری موارد دیگر است (Mohamed, 2012).

1. https://www.oecd.org/en/topics/policy-issues/digital-security.html
2. Technological Crimes

فن‌آوری‌های دیجیتال ابزار جدیدی برای دفاع و اجرای حقوق بشـــر فراهم می‌کنند. استفاده از فناوری‌های نوین اطلاعات و ارتباطات حتی توسط افراد و نهادهای غیردولتی ممکن است تهدیدی برای صلح و امنیت بین‌المللی باشد. دیجیتالی شدن، سرمایه‌داری نظارتی و افزایش عملیات مخرب دیجیتالی، همگی اعمال حقوق بین‌المللی موجود در فضای دیجیتال را به چالش کشـــیده‌اند. در حال حاضر هیچ ابزار هنجاری خاصی وجود ندارد که به طور جامع حقوق بشـــر قابل اجرا در عصر دیجیتال را تعیین کند.

فناوری‌های دیجیتالی در حال حاضر زندگی ما را به شـــدت تغییر داده است. به‌طور تقریبی هر حوزه از روابط اجتماعی در حال حاضر هم در ســـطوح ملی و بین‌المللی در حال دیجیتالی شـــدن است. شورای امنیت سازمان ملل متحد در قطعنامه‌های ۲۴۱۹ (۲۰۱۸)، ۲۴۶۲ (۲۰۱۹) و ۲۴۹۰ (۲۰۱۹) اذعان می‌دارد فعالیت افراد و نهادهای غیردولتی در حوزه دیجیتال ممکن است تهدیدی برای صلح بین‌المللی و نیز موجبات نقض امنیت را در حملات دیجیتالی به زیرساخت‌های حیاتی؛ عدم امکان استفاده از سیستم‌های پرداخت برخط، انسداد دسترسی به اینترنت، حساب‌های توییتر و اینستاگرام (ر.ک: شاهیده، ۱۴۰۲: ۲۷۳-۲۷۰) فراهم نماید.

بـــا توجه به شکســـت اقدام‌های کنترلی و نظارت مؤثـــر بر اینترنت و فضای مجازی به دلیل عـــدم همـــکاری دولت‌ها، بهره‌گیری گروه‌های تروریســـتی از فضای مجـــازی، چالش نوینی برای ســـازوکارهای ضد تروریســـتی قلمداد می‌شـــود. در ضمن، برای توسعه فضای مجازی در چارچوب راهبرد دولت‌ها به‌ویژه دولت‌های دارنده زیرســـاخت اینترنت پیشـــرفته، باید در راســـتای پیشگیری و ســـرکوب بهره‌گیری تروریستی از رسانه‌ها صورت پذیرد. افزون بر این، با توجه به فقد یک ســـند حقوقی جامع در حاکمیت بر اینترنت و فضای مجازی به علت عدم اجماع جهانی، ضرورت دارد تا نســـبت به هماهنگی در اِعمال واکنش بین‌المللی موفقیت‌آمیز به تحرکات تروریســـت‌ها در فضای مجازی دولت‌ها با اتخاذ راهبردهایی متناســـب و اثرگذار، در این زمینه اقدام کنند.

با این همه، این پژوهش درصدد آن است که با استفاده از منابع مطالعاتی کتابخانه‌ای و بهره‌گیری از روش پژوهش توصیفی تحلیلی نحوه حفاظت از سکوهای دیجیتالی را در قبال جرایم تروریستی مورد ســـنجش قرار داده و ضمن بررســـی تهدیدها و چالش‌ها، رویکردهای فنی و حقوقی حکم بر آن را مورد سنجش قرار دهد.

۱. تحولات بین‌المللی

گسترش فزاینده فناوری اطلاعات و ارتباطات منجر به تحوّل و دگرگونی جوامع در ابعاد مختلف سیاسی، امنیتی، اقتصادی و اجتماعی شده است. در چنین فضایی که با عنوان فضای مجازی توصیف می‌شود، تهدیدهای نوینی نظیر جنگ مجازی، جنگ اطلاعاتی، جرایم دیجیتالی، پدیده هکرها و سرقت اطلاعات محرمانه نهادهای امنیتی و اطلاعاتی، ظهور کرده‌اند تا امنیت ملی کشورها را با چالش جدی مواجه سازند.

توسعه فناوری‌های دیجیتال کلیه ابعاد زندگی بشر و حقوق بین الملل از جمله گستره، مسائل، ابزار و روش‌های تحریم‌های بین‌المللی و یک‌جانبه را تغییر داده و هم‌چنان در حال تغییر است. فهرست زیر نمونه‌هایی را ارائه می‌دهد اما کامل نیست: پاسخ به حملات مسلحانه و تهدیدات علیه صلح و امنیت بین المللی. استفاده از ابزارهای دیجیتالی برای تأمین مالی جرایم تروریستی؛ فعالیت‌های دیجیتال مخرب، از جمله حملات به زیرساخت‌های حیاتی که به سطح یک حمله مسلحانه نمی رسند. انسداد تجارت برخط کشورهای هدف، شرکت‌ها و افراد و همچنین سایر اتباع. پیشگیری از دسترسی به سیستم عامل‌های برخط عمومی؛ انسداد تجارت با نرم افزار یا تجهیزات ارتباطی اطلاعاتی؛ انسداد حساب‌های کاربری مجازی؛ فهرست ارزهای دیجیتال(Douhan, 2022: 129).

جرایم تروریستی دیجیتالی جنایتی است که به خاطر خطراتش شناخته می‌شود و تأثیرات آن بر جامعه و زندگی مردم در طول تاریخ ظاهر شده است، زیرا جان میلیون‌ها انسان بی‌گناه را گرفت، جوامع را ویران کرد، و این جنایت مرزی نمی‌شناسد. در عرصه‌های گوناگون، مرتکبان جرایم مختلف از فناوری روز ابزارهای جدیدی برای ارتکاب جرایم خود گرفته اند، به‌طوری که بسیاری از جرایم از طریق اینترنت یا وسایل الکترونیکی مرتکب می‌شوند؛ آنچه جرایم تروریستی دیجیتالی نامیده می‌شود، ظهور کرده است.

پیشرفت در فناوری اطلاعات و ارتباطات نه تنها طیف وسیعی از مشکلات جدید جرم را ایجاد کرده است، بلکه پیشگیری، کشف، تحقیق، تعقیب و مجازات جرم را نیز تسهیل کرده است؛ اگرچه این فناوری به آژانس‌های عدالت کیفری کمک کرده و حمایت‌های زیادی را برای مظنونان و مجرمان ارائه کرده است، اما خطرات نقض حقوق بشر از نحوه واکنش قانون به جرایم رایانه‌ای را فراهم کرده است.

تروریست‌ها به‌طور روزافزون از فضای مجازی به‌عنوان ابزاری برای جذب نیرو و شناساندن

خود به مردم اســـتفاده می‌کنند. رســـانه اجتماعی یک نوآوری جدید اســـت که به افراد اجازه می‌دهد اطلاعات، ایده‌ها، پیامهای شـــخصی و محتویات دیگر (مانند فیلم) را در سراســـر دنیا با یکدیگر به اشـــتراک بگذارند.[1] رســـانه اجتماعی موجود در فضای مجازی ویژگی‌های مفیدی برای انتشـــار محتوا، دسترســـی آزاد به کاربران، توانایی بازآفرینی و انتقال فوری اطلاعات دارد، اما همین مزیت‌ها موجب شـــده اســـت تا این‌گونه رسانه‌ها ابزار ســـودمندی برای تروریست‌ها باشند(Weimann, 2014: 1).

با این همه، رویارویی با جرایم تروریســـتی به یک مســـأله مهم بین‌المللی مبدل گشـــته است. گروه‌های تروریســـتی اکنون از فرصت‌های ارائه شده توسط اینترنت و فضای مجازی بهره می‌برند و از منابع برخط برای فرماندهی، کنترل و برقراری ارتباط با شـــبکه‌های خود اســـتفاده می‌کنند و روایت‌های خود را به گونه‌ای شـــکل می‌دهند که نگرانی‌های عمومی را بیان می‌کنند و نیروهای جدید جذب می‌کنند(Yüksel, 2020: 1089).

۲. رویکردهای شناختی و توصیف مفاهیم

فناوری دیجیتال به‌عنوان ابزاری بسیار پویا برای ارتباطات دارای کاربرد قابل ملاحظه‌ای است. به‌نحوی که این فناوری هم‌چنین نیروی محرکه‌ای برای سازمان‌های تروریستی و حامیان آنها برای طیف وسیعی از اهداف است. اینترنت به‌دلیل مزایای بسیاری که ارائه می‌کند، به ابزار مورد علاقه تروریست‌ها تبدیل شده است از جمله دسترسی آسان، مقررات اندک یا بدون محدودیت، سانسور ضعیف یا بدون آن یا ســـایر اشـــکال کنترل دولتی، مخاطبان بالقوه عظیمی که در سراســـر جهان منتشر می‌شوند(Sander, 2022: 295). ناشناس بودن ارتباطات، جریان سریع اطلاعات، تعامل، توسعه و نگهداری ارزان یک حضور وب، یک محیط چندرسانه‌ای، و توانایی تأثیرگذاری بر پوشش در رســـانه‌های جمعی ســـنتی. بنابراین، عصر دیجیتال و گســـترش پلتفرم‌های موجود در فضای مجازی، ظهور تروریسم سایبری را تسهیل کرد(Odhiambo, Ochara and Kadymatimba, 2018: 149-151).

گسترش فناوری اطلاعات و ارتباطات نظیر اینترنت عرصه شکل‌گیری مجموعه‌ای از ارتباطات میان گروه‌های اجتماعی متفاوت از فاصله‌های بســـیار دور در دنیای واقعی اســـت که فرصت‌ها و

1. 15. Social Media, Merriam-Webster, http://www.merriam-webster.com/dictionary/social / 20media.

تهدیدهـــای نوینی را فراروی جامعه بین‌المللی قرار داده اســـت؛ به‌طور نمونه جرایم تروریســـتی از جملـــه تهدیدهای نوینی اســـت که فضـــای مجازی و دیجیتالی موجبات آن را فراهم ســـاخته است(یزدان‌پناه‌درو و جعفری، ۱۳۹۷: ۲۲۱).

حمله‌های دیجیتالی در مقیاس بزرگ با ســـرعت هشـــدار دهنده‌ای در سراســـر جهان در حال افزایش اســـت. این حمله‌ها اغلب با تهدیدهای تروریســـتی دیجیتالی که به‌طور گســـترده تبلیغ و عمومی شده است، مرتبط هستند. با این حال، «تروریسم دیجیتالی» یک زمینه تحقیقاتی نسبتاً جوان اســـت و اصطلاحات آن، نظیر اصطلاح اصلی آن، یعنی «تروریســـم»، تاکنون به‌نحو قابل پذیرشـــی مورد تعریف قرار نگرفته اســـت(Taylor, 2014: 48-50). البته تعریف جدید از تجزیه و تحلیل دقیق تعاریف موجود در ادبیات قابل دســـترس عموم قابل ملاحظه اســـت، که مشتمل بر کلیه اشـــتراکات کلیدی شناسایی شـــده وفق طبقه‌بندی جدید پیشنهادی (یعنی بازیگر، انگیزه، قصد، وسیله، اثر و هدف) است. این رویکرد نوین برای تعریف تروریسم دیجیتالی درک مشترکی از تهدید گسترده‌تر برای استانداردسازی سیاست، همکاری جهانی و تحقیقات ارائه می‌کند، در حالی که اجازه می‌دهد زیرمجموعه‌های منحصربه‌فردی از این شاخه از جرایم ترویستی برای کاربردهای قانونی یا تخصصی خاص تعریف شود(Plotnek and Slay, 2021: 136-137).

در هـــر حال، جرایم دیجیتالی جرایمی اســـت که مولود جامعه فنـــآور و مدرن بوده و به همین دلیل، ابهامات زیادی در باب ماهیّت و پیشـــینه اینگونه جرایم از یک ســـو و ویژگی‌های این جرایم و مرتکبـــان آنها از ســـوی دیگر وجود دارد. با عنایت به این ابهامـــات و نیز تفاوت‌های موجود بین جرایم دیجیتالی و سایر جرایم، پیشگیری و مقابله با جرایم دیجیتالی اقدامات تهاجمی خاصّی را می‌طلبد(موسوی، روحانی‌مقدم و آقائی‌بجستانی، ۱۴۰۱: ۳۲۳).

جرایم تروریستی دیجیتالی را می‌توان اینگونه تعریف کرد: «فعالیت یا حمله عمدی با انگیزه‌های سیاسی که به دنبال تأثیرگذاری بر تصمیمات دولتی و افکار عمومی جهانی است و از فضا، همانطور که می‌خواهد، در فرآیند انجام جرم تروریســـتی و به عنوان یک ابزار الکترونیکی کمکی اســـتفاده می‌کند. رسانه به عنوان عاملی برای ایجاد تأثیر اخلاقی و روانی از طریق تحریک به نفرت پراکنی این اثر به صورت دیجیتالی از طریق اســـتفاده از ســـازوکارهای جدید ســـلاح‌های الکترونیکی در نبردهایی است که در فضای مجازی رخ می‌دهد.

با این حال، ارتکاب جنایات تروریستی ممکن است از راه‌هایی غیر از رایانه‌ها مانند تلفن همراه، دستگاه‌های بلک‌بری، تبلت‌ها و آی‌پدها اتفاق بیفتد که در آن فرد می‌تواند از طریق این دستگاه‌ها

به اینترنت رفته و از رسانه‌های اجتماعی استفاده کند. جرایم تروریستی را از طریق ترویج و تأمین مالی جرایم تروریستی و استخدام افراد برای این عملیات تروریستی انجام دهد(Corliss, 2023: 98).[1]

۳. تهدیدها و چالش‌ها

گسترش فزاینده فناوری اطلاعات و ارتباطات منجر به تحوّل و دگرگونی جوامع در ابعاد مختلف سیاسی، امنیتی، اقتصادی و اجتماعی شده است. در چنین فضایی که با عنوان فضای مجازی توصیف می‌شود، تهدیدهای نوینی نظیر جنگ مجازی، جنگ اطلاعاتی، جرایم دیجیتالی، پدیده هکرها و سرقت اطلاعات محرمانه نهادهای امنیتی و اطلاعاتی، ظهور کرده‌اند تا امنیت ملی کشورها را با چالش جدی مواجه سازند.

توسعه فناوری‌های دیجیتال همه جنبه‌های زندگی بشر و حقوق بین الملل از جمله دامنه، موضوعات، ابزار و روش‌های تحریم‌های بین‌المللی و یکجانبه را تغییر داده و همچنان در حال تغییر است. از اینرو، جرایم دیجیتالی به ویژه طی یک دهه اخیر، به‌مثابه یک راز اطلاق نمی‌شود. مردم برای انجام کارهای خود هر روز به رایانه یا دستگاه‌های تلفن همراه وابسته هستند، همچنین از آنها در شبکه‌های اجتماعی برای برقراری ارتباط با دوستان و خانواده خود استفاده می‌کنند، همه این فعالیت‌ها حجم عظیمی از داده‌ها و اطلاعات را بر روی رایانه / دستگاه‌های تلفن همراه تولید می‌کنند یا از طریق مختلف عبور می‌کنند. جرم دیجیتالی زمانی شروع می‌شود که فعالیت

---

۱. این ظرفیت وجود دارد که دولت‌ها می‌توانند از قابلیت‌های دیجیتالی برای دستیابی به اهدافی استفاده کنند که صلح و امنیت بین‌المللی و منطقه‌ای را با مخاطره‌هایی موجه سازند. به این ترتیب، نگرانی‌های فزاینده‌ای وجود دارد که عملیات دیجیتالی تحت حمایت دولت می‌تواند به زیرساخت‌های حیاتی و سیستم‌های اطلاعاتی سایر کشورها آسیب برساند(Moynihan, 2021: 399-401). به‌دیگر تعبیر، عملیات دیجیتالی تحت حمایت دولت به جرایم دیجیتالی اطلاق می‌شود که از سوی یک دولت برای ایجاد اختلال یا سوءاستفاده از سیستم‌های رایانه‌ای یک کشور هدف یا آسیب رساندن به سیستم‌های رایانه‌ای و زیرساخت‌های حیاتی کشور هدف با هدف کسب مزیت انجام می‌شود. کشور مورد نظر چنین حملاتی ممکن است به‌طور مستقیم توسط یک دولت از طریق مؤسسات آن یا از طریق نمایندگی غیردولتی با حمایت یک دولت انجام شود. اهداف عملیات دیجیتالی تحت حمایت دولت به‌طور معمول زیرساخت‌های حیاتی هستند. با این حال، کلیه اشکال دستگاه‌های محاسباتی متصل به شبکه‌های اطلاعاتی نیز اهداف بالقوه عملیات دیجیتالی تحت حمایت دولت هستند. عملیات دیجیتالی تحت حمایت دولت را می‌توان از طریق فعالیت‌های دیجیتالی مخرب نظیر استقرار ویروس‌ها، کرم‌های رایانه‌ای و بدافزارهایی که می‌توانند زیرساخت‌های حیاتی را مختل کرده و به آن‌ها آسیب برساند، اجرا کرد(Jerome Orji, 2022: 236).

غیرقانونی روی داده‌ها یا اطلاعات موجود در رایانه‌ها یا شبکه‌ها انجام شود. در روزهای اولیه جرایم دیجیتالی، جرم به‌طور معمول در زمینه مالی انجام می‌شد، اما جرایم دیجیتالی اکنون به شکل‌های دیگری تکامل یافته است، به عنوان مثال سیستم‌های اطلاعاتی به دلایلی می‌توانند توسط برخی از شرکت‌ها به سرقت رفته یا آسیب ببینند. رایانه یا دستگاه‌های تلفن همراه می‌توانند به عنوان ابزاری برای مقابله با جرم مورد استفاده قرار گیرند و به طور کلی میزان جرایم دیجیتالی به وضوح پس از ظهور اینترنت افزایش می‌یابد. شبکه‌ها نیز نقش بسزایی در افزایش میزان جرایم دیجیتالی دارند.

البته با ظهور اینترنت بخش قابل توجهی از دغدغه‌های امنیت بین المللی معطوف این فضا شده است. فضایی که با ساختار فنی پیچیده خود چالش‌های مهمی را برای دولت‌ها که از سوی شرکت‌های فناوری به‌عنوان بازیگران فعال به گوشه‌ای رانده شده اند، فراهم آورده است. یکی از بزرگترین خطراتی که این فضا برای تمامی کشورها اعم از کشورهای پیشرفته در فناوری و کشورهای توسعه نیافته ایجاد نموده آن است که ضعف فناورانه حتی یک کشور می‌تواند بستری برای تهدیدهای جدی علیه کلیه کشورها فراهم آورد. دلیل این امر آن است که امروزه سوءاستفاده از زیرساخت‌های اینترنتی کشورهایی که امکان نظارت و پیشگیری جدی برای فضای دیجیتال خود ندارند برای انجام اقدامات خرابکانه و حتی جنگ مجازی علیه کشورهای دیگر به امری معمول بدل شده است.[1]

با این همه، آنچه جرایم دیجیتالی با رویکرد تروریستی را متمایز می کند، توانایی پنهان کردن و مخفی کردن منابع اطلاعاتی است: یکی از آنها دشواری ردیابی عامل حادثه جرایم دیجیتالی با رویکرد تروریستی است؛ زیرا مشکلات زیادی وجود دارد که مانع از دستیابی به شواهد فیزیکی مرتبط با مرتکب می‌شود. واقعه علاوه بر این، اثبات جرایم دیجیتالی با رویکرد تروریستی دشوار است؛ زیرا هیچ مدرک فیزیکی واضح و همچنین مورد حملات سنتی وجود ندارد. با این حال، دشواری اثبات آنها به دلایل بسیاری است؛ ارتکاب آنها توسط فردی با صلاحیت بالا، فریب و اطلاعات نادرست، علاوه بر تفاوت زمان، مکان و قانون قابل اجرا در کشوری که در آن وجود دارد، دارد.

۴. مصادیق و اَشکال بروز

دولت‌ها مدت‌هاست که نگران استفاده تروریست‌ها از اینترنت برای انجام جرایم تروریستی دیجیتال، گسترش تبلیغات، استخدام و افراط گرایی افراد و جمع‌آوری سرمایه هستند. حقوق

1. https://unstudies.ir/iauns-forum/

بین‌الملل برای حمایت از پاســخ به جرایم تروریســتی دیجیتال موقعیت مناسبی ندارد، اما فقدان چنیــن حملاتی تا به امروز انگیزه دولت‌ها را برای توســعه حقــوق بین المللی در برابر این تهدید تضعیف می‌کند. در مورد اســتفاده تروریســت‌ها از اینترنت و رسانه‌های اجتماعی برای تبلیغات، رادیکال‌سازی، جذب نیرو و جمع‌آوری کمک مالی، بحران ناشی از فعالیت‌های برخط، اجماع کافی برای حمایت از نقش برجســته حقوق بین‌المللی در قبال جرایم تروریستی دیجیتال ایجاد نکرده است(Fidler, 2016: 475).

ارتکاب جرایم تروریستی دیجیتالی مشتمل بر استفاده از اینترنت و سایر اشکال فناوری اطلاعات و ارتباطات برای تهدید یا ایجاد آســیب بدنی برای به دســت آوردن قدرت سیاســی یا عقیدتی از طریق تهدید یا ارعاب اســت. سرقت داده‌ها، دستکاری داده‌ها و اختلال در خدمات ضروری، همه انواع حملات دیجیتالی هســتند. با بحرانی شدن زیرســاخت‌های دیجیتالی و کاهش موانع ورود برای عوامل مخرب، جرایم تروریســتی دیجیتالی به یک نگرانی فزاینده تبدیل شده است. کشف، واکنش و پیشگیری از این جنایت چالش‌های منحصربه‌فردی را برای مجریان قانون و دولت‌ها ایجاد می‌کند که نیازمند رویکردی چندوجهی است. جرایم تروریستی دیجیتالی می‌تواند اثرات مخربی بر طیف وسیعی از افراد و سازمان‌ها داشته باشد. اعتبار و ثبات یک کشور ممکن است آسیب ببیند، خسارات مالی رخ دهد و در برخی موارد حتی ممکن است جان افراد از دست برود؛ در نتیجه این نوع از جرایم، زیرساخت‌های حیاتی نظیر شبکه‌های برق، بیمارستان‌ها و سیستم‌های حمل و نقل نیز می‌توانند مختل شوند که منجر به اختلالات و پریشانی گسترده شود.

به‌هر روی، برخی از روش‌های رایجی که از طریق آن جرایم تروریستی دیجیتالی انجام می‌شود، عبارت است از:

الف- بدافزار؛ نرم افزارهای مخرب نظیر ویروس‌ها، کرم‌ها، باج افزارها می‌توانند برای به مخاطره افکندن سیســتم‌های رایانه‌ای و ســرقت اطلاعات حساس، اخلال زیرساخت‌های حیاتی یا ایجاد هرج و مرج مورد استفاده قرار گیرند. تروریست‌های دیجیتالی ممکن است بدافزار را برای دسترسی به اهداف خود توسعه دهند یا مستقر کنند.

ب- فیشــینگ؛ حملات فیشــینگ مشــتمل بر بهره‌گیری از آدرس‌های الکترونیک، وب‌گاه‌ها یا پیام‌های فریبنده برای فریب دادن افراد به افشــای اطلاعات حســاس مانند اعتبار ورود، جزئیات مالی یا داده‌های شــخصی اســت. از این فنون می‌توان برای جمع‌آوری اطلاعات یا دسترسی به سیستم‌های حیاتی استفاده کرد.

پ- مهندســی اجتماعی؛ فنون مهندسی اجتماعی شامل دستکاری افراد برای افشای اطلاعات محرمانه یا انجام اقداماتی اســت که ممکن اســت امنیت را به خطر بیندازند. تروریست‌های دیجیتالی ممکن اســت برای دسترســی به داده‌ها یا سیســتم‌های حساس، هویت افراد یا نهادهای مورد اعتماد را جعل کنند.

ت- باج‌افــزار؛ باج‌افزار نوعی بدافزار اســت که داده‌های قربانــی را رمزگذاری می‌کند و تا زمان پرداخت باج غیرقابل دسترســی است. تروریســت‌های دیجیتالی ممکن است باج‌افزاری را برای مختل کردن سیستم‌های حیاتی یا اخاذی از سازمان‌های هدف مستقر کنند.

ث- تهدیدهای داخلی؛ تهدیدهای داخلی شامل افرادی در یک سازمان می‌شود که به‌نحو عمدی یــا غیرعمدی به تروریســت‌های دیجیتالی در فعالیت‌های خــود کمک می‌کنند. این افراد ممکن است به اطلاعات یا سیستم‌های حیاتی دسترسی داشته باشند.

ج- حمله‌های مشابه استاکس‌نت: استاکس نت نمونه معروفی از حملات دیجیتالی هدفمند است که به‌طور خاص با هدف ایجاد اختلال در سیستم‌های کنترل صنعتی، نظیر مواردی که در تأسیســات هسته‌ای استفاده می‌شود، انجام می‌شود. تروریست‌های دیجیتالی ممکن است سیستم‌های زیرساختی حیاتی را هدف قرار دهند تا آسیب فیزیکی یا تخریب ایجاد کنند.

با این همه، تروریست‌های دیجیتالی اغلب از ترکیبی از این روش‌ها برای دستیابی به اهداف خود اســتفاده می‌کنند و انگیزه‌های آنها می‌تواند بسیار متفاوت باشد، از جمله سیاسی، عقیدتی، مالی یا صرفاً ایجاد هرج و مرج و اختلال. برای افراد، ســازمان‌ها و دولت‌ها بســیار مهم است که اقدامات امنیتی دیجیتالی قوی برای دفاع در برابر جرایم تروریستی دیجیتالی و فنون مختلف آن اجرا کنند.

۵. چالش‌ها و رویکردهای پیش‌روی

در مدت کمی بیش از دو دهه، رشد سریع اینترنت و فناوری‌های اطلاعاتی و ارتباطی باعث رشد اقتصادی و گسترش دسترسی به خدمات حیاتی شده است. با این حال، فرصت‌های جدیدی برای فعالیت‌های مجرمانه نیز ایجاد کرد. از آنجایی که مجرمان به ذینفعان ناخواســته فناوری جدید و جهانی شدن تبدیل شده اند، زیرا این تحولات آنها را قادر می‌سازد تا با بهره‌برداری از فعالیت‌های فراملی مرتکب جنایات شده و از آن سود ببرند و همچنین فعالیت‌ها و اقدامات غیرقانونی خود را از طریق پلتفرم‌های دیجیتال به گونه‌ای گســترش دهند که خطرات به ویژه کاهش یابد. از سوی دیگــر، فناوری‌های کنونی فرصت‌های جدیدی را برای اجــرای قانون، تحقیقات جنایی و تعقیب

کیفری و مبارزه با جرایم دیجیتالی از جمله جرایم دیجیتالی با رویکرد تروریستی ارائه می‌کند تا امنیت عمومی را بهبود بخشـــد و آژانس‌های مجری قانون و عدالت کیفری را قادر به پیشـــگیری و مبارزه با جرایم از طریق فن‌آوری کنند(Kumar Saini, 2023: 28-29).

نگرانی فزاینده‌ای در مورد سوءاستفاده تروریست‌ها از فناوری‌های اطلاعات و ارتباطات به ویژه اینترنت و فناوری‌های دیجیتال جدید برای ارتکاب، تحریک، عضوگیری، تأمین مالی یا برنامه‌ریزی جرایم تروریستی وجود دارد. از اینرو، سازمان ملل متحد به خطرات استفاده تروریستی از اینترنت پی برده اســـت. در دهه ۱۹۹۰ ســـازمان از دولت‌های عضو خواســـت خطر اســـتفاده تروریستی از سیســـتم‌ها و شـــبکه‌های الکترونیکی یا مخابراتی با سیم جهت انجام اعمال جنایتکارانه را متذکر شوند و سازوکاری برای پیشگیری از چنین جرم و جنایتی و برای ترویج همکاری به تناسب حال پیدا کنند.[1] پس از آن شورای امنیت از دولت‌های عضو خواست با تبادل اطلاعات مربوط به استفاده گروه‌های تروریستی از فناوری ارتباطات و مخابراتی همکاری بین‌المللی را افزایش دهند.[2] دستیابی به این همکاری به‌طور عملی دشوارتر از آن بود که تصور می‌شد(Archick, 2014: 8 - 9).

با این حال ســـازمان در ســـال ۲۰۰۵ مشکل خاص تروریست‌هایی که به‌ویژه در عصر رسانه‌های پرطرفدار شبکه‌ســـازی اجتماعی هم‌چون فیس‌بوک، تلگرام، توییتر، یوتوب، فلیکر، و ســـکوهای وبلاگ‌سازی از اینترنت سوءاستفاده می‌شد و افرادی که خواسته یا ناخواسته مقدار بی‌سابقه‌ای از اطلاعات حساس را از طریق اینترنت انتشار دادند را اعلام کرد.

اینترنـــت و فضای مجازی علاوه بر تأثیرات بنیادین بر حوزه‌های فرهنگی، اجتماعی و اقتصادی جوامع مختلف ابعاد تهدیدآمیزی را نیز آشکار ساخته و زمینه انتقال منابع ناامنی از فضای واقعی به مجازی را فراهم کرده اســـت. امروزه محیط‌های تهدیدآمیز علیه منافع ملت‌ها و دولت‌ها صرفا به ســـرزمین محدود نمی‌شود و جهان مجازی نیز محیطی تهدیدزا به‌شمار می‌آید. ارتکاب جرایم تروریســـتی در بســـتر فضای مجازی یکی از مهم‌ترین تهدیدهای نوظهور اســـت که با استفاده از قابلیت‌های اینترنت به فعالیت‌های خود بُعد بین‌المللی داده است. از اینرو، ماهواره، اینترنت، فضای مجازی و روزنامه‌نگاری ســـایبر، عامل فضای مجازی در ظهور و گســـترش و گروه‌های تروریستی به‌عنوان بازیگران جدید در عرصه بین‌الملل بیشترین نقش را ایفاء کرده است(برجعلی‌زاده، جعفری و کردی، ۱۳۹۸: ۱۳۹).

1. G.A. Res. 51 /210
2. S.C. Res. 1373, para. 3, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

فضای بی‌مرز دیجیتال، جهانی موازی با جهان فیزیکی را به‌وجود آورده است که در واقع کنترل و ادارهٔ حقوقی آن از حیطهٔ اعمال قدرت یک حاکمیت برنمی‌آید. بنابراین، برای حاکمیت بر این فضا و مقابله با جرایم روزافزون و پیچیدهٔ ارتکابی در فضای دیجیتال همکاری و معاضدت جامعهٔ بین‌المللی برای قاعده‌مندی نیاز است، به‌گونه‌ای که هیچ مجرمی بدون مجازات نماند و این مهم به‌دست نمی‌آید، مگر با تدوین مقررات هماهنگ و متحدالشکل؛ زیرا جرایم ارتکابی در فضای دیجیتال مرزهای جغرافیایی و سنتی را پشت سر می‌گذارند[1] و به‌سبب ویژگی‌هایی که دارند، می‌توان برخی از این‌گونه جرایم را در زمرهٔ آن دسته جرایمی به‌شمار آورد که برای مقابله با آنها اعمال صلاحیت جهانی ضرورت دارد(جلالی و توسلی‌اردکانی، ۱۳۹۸: ۱۳۵۱).

۶. سیاست‌گذاری‌های فنی و حقوقی در نظام بین‌المللی

با توجه به پیچیدگی روزافزون تهدیدهای دیجیتالی در سطح جهانی، رعایت این مقررات بسیار مهم است. برنامه جهانی مبارزه با جرایم دیجیتالی با رویکرد تروریستی و فناوری‌های نوین در آوریل ۲۰۲۰ تصویب شد و پشتیبانی ظرفیت‌سازی را برای کشورهای عضو، سازمان‌های بین‌المللی و منطقه‌ای برای توسعه و اجرای پاسخ‌های مؤثر به چالش‌ها و فرصت‌هایی که اینترنت و سایر فناوری‌های اطلاعات و ارتباطات در ارائه می‌دهند، ارائه می‌کند. از اینرو، برنامه جهانی از تعهد راهبردی سازمان ملل متحد به جهانی بدون جرایم تروریستی از طریق، «توسعه دانش و افزایش آگاهی از چالش‌ها و فرصت‌های مرتبط با فناوری‌های جدید در جرایم تروریستی»،

---

۱. مطابق الگوهای سنتی ارتکاب جرم، مرتکبان جرایم تروریستی پیش از ارتکاب، مکان‌های خاصی را انتخاب می‌کنند که بر این اساس توزیع و پراکندگی جغرافیایی جرایم تروریستی متناسب با مکان‌های خاص مدنظر تروریست‌ها تعریف می‌شود. گستردگی آثار تروریستی، موجبات تسهیل انتقال پیان تروریست‌ها به دولت‌ها را فراهم می‌آورد. بر این اساس، آن‌ها مکان‌هایی را انتخاب می‌کنند که ضمن دارای ارزش نمادین و جلب توجه افکار عمومی و رسانه‌ها، موجب ارعاب بیشتر و خسارت بیشتر شود. یافته‌های پژوهشی حاکی از آن است که مراکز تردد شهری نظیر ایستگاه‌های راه‌آهن، مترو و حتی فرودگاه‌ها امکان چنین اهدافی را برای تروریست‌ها به‌سهولت فراهم می‌آورد(شاهیده، ۱۴۰۲: ۲۶۵-۲۶۴). این در حالی است که امروز با توجه به گستره بسیار عمیقی که فناوری‌های دیجیتالی در حیات بشری به‌نحو فزاینده‌ای رسوخ پیدا کرده است، امکان ارتکاب جرایم در گستره جغرافیایی و سنتی جای خود را به فضای دیجیتال داده و امکان تخریب، محو و نقض امنیت را در کلیه ابعاد آن ایجاد نموده است؛ به‌ویژه آن‌که جرایم سازمان‌یافته نظیر جرایم تروریستی و حتی جرایم فناورانه هم‌چون جرایم دیجیتالی با رویکرد تروریستی، مادام که در بستر فضای دیجیتال ارتکاب می‌یابند، نه‌تنها از حیث پدیداری آثار قابل ملاحظه‌ای از جغرافیای حیات بشری ندارند، بلکه نحوه کشف، تعقیب، و حتی مقابله با آن‌ها نیز متفاوت خواهد بود.

«تقویت مهارت‌ها و ظرفیت‌های مورد نیاز برای توسعه و اجرای پاسخ‌های مؤثر سیاست ملی ضد جرایم تروریستی به چالش‌ها و فرصت‌های فناوری‌های جدید»، «تقویت مهارت‌ها و ظرفیت‌های مورد نیاز برای حفاظت از زیرساخت‌های حیاتی در برابر جرایم دیجیتالی با رویکرد تروریستی» و «افزایش ظرفیت‌های عدالت کیفری برای مقابله و بررسی استفاده تروریستی از فناوری‌های نوین»، قابل اجراست.[1]

قطعنامه‌های ۲۱۷۸ (۲۰۱۴) و ۲۳۹۶ (۲۰۱۷) شورای امنیت از کشورهای عضو می‌خواهد هنگام اتخاذ تدابیر ملی برای پیشگیری نسبت به بهره‌گیری تروریست‌ها از فناوری و ارتباطات برای ارتکاب جرایم دیجیتالی با رویکرد تروریستی، همکاری کنند.[2] قطعنامه ۲۳۹۶ (۲۰۱۷) همچنین کشورهای عضو را تشویق می‌کند تا همکاری با بخش خصوصی، به‌ویژه با شرکت‌های فناوری ارتباطات اطلاعات، در جمع‌آوری داده‌های دیجیتال و شواهد در پرونده‌های مربوط به جرایم تروریستی را افزایش دهند.[3]

«برنامه جهانی مبارزه با تروریسم راجع‌به امنیت سایبری و فناوری‌های نوین»[4] در آوریل ۲۰۲۰ با هدف ارتقای ظرفیت‌های کشورهای عضو، سازمان‌های بین‌المللی و منطقه‌ای و نهادهای سازمان ملل متحد برای افزایش آگاهی در مورد تهدید ناشی از جرایم دیجیتالی با رویکردهای تروریستی و ارتقای ظرفیت‌های فنی مورد نیاز برای پیشگیری به تصویب رسید. کاهش و پاسخگویی به گروه‌های تروریستی و تندرو خشونت آمیز که از فناوری‌های نوین نظیر اینترنت سوء استفاده می‌کنند.

سنجش قلمرو حقوق بین‌المللی در حوزه رسانه‌ها به‌ویژه در مسأله فضای مجازی و البته بررسی کارکرد آن‌ها در بستر فضای مجازی به شکل ساختاری واقعی، به‌مثابه چالشی اطلاق می‌شود که به دلیل نقش استثنایی رسانه‌ها به‌طور کلی و تأثیر مستمر و اساسی آن بر فرآیندهای دموکراتیک در حال وقوع در جهان، نیاز به اثبات علمی دارد. در این راستا، توجه ویژه‌ای به تأثیر رسانه‌ها بر روندهای معاصر مربوط به روند ادغام اتحادیه اروپا، توسعه دموکراسی و حاکمیت قانون شده است.

---

1. https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity
2. https://main.un.org/securitycouncil/en/s/res/2178-%282014%29
3. https://main.un.org/securitycouncil/en/content/sres23962017
4. Global Counter Terrorism Programme on Cybersecurity and New Technologies; https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/mya_project_itemid_27.pdf

این امر به‌ویژه بر آزادی بیان، احترام به ارزش‌ها و اصول استانداردها، حقوق و آزادی‌های بشر تأکید دارد(Ronkova, 2016: 58).

جامعه بین‌المللی تاکنون اسناد حقوقی بین‌المللی ویژه‌ای را برای مواجه با بهره‌گیری از اینترنت توسط گروه‌های تروریستی تصویب کرده که توسط سازمان ملل متحد، شورای اروپا و اتحادیه اروپا رهبری می‌شود. با این حال، توسعه مقررات قانونی به دلیل ویژگی‌های بدیع اینترنت با چالش‌هایی مواجه است؛ هر چند که سازمان ملل متحد در چارچوب مجمع عمومی طی سال ۲۰۲۱، برای تدوین کنوانسیون بین المللی جامع مبارزه با بهره‌گیری از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه اولین جلسه سازمانی خود را برگزار کرد. هدف از تهیه پیش‌نویس مزبور «تقویت همکاری‌های بین المللی برای مبارزه با برخی جرایم ارتکابی از طریق سیستم‌های فناوری اطلاعات و ارتباطات و به اشتراک گذاری مدارک به صورت الکترونیکی جرایم جدی» و با هدف نهایی تهیه «پیش‌نویس کنوانسیون سازمان ملل متحد علیه جرایم سایبری»[1] بود که در نهایت به‌دلایل فنی و حقوقی تاکنون سند مزبور به‌لحظ تقریر متن نهایی و تصویب نشده است. در ضمن، «کنوانسیون بوداپست راجع‌به جرایم سایبری» یک معاهده بین‌المللی است که به جرایم جنایی ارتکابی از طریق فضای دیجیتالی نظیر هک، سرقت داده‌ها و کلاهبرداری برخط می‌پردازد.[2] این همکاری بین‌المللی را در تحقیق و تعقیب جرایم دیجیتالی ترویج می‌کند(Reveron and Savage, 2023: 237-239).

نتیجه‌گیری

جرایم تروریستی دیجیتالی یکی از انواع جرایم اطلاعاتی در نظر گرفته می‌شود، زیرا به شکل میدان یا دامنه‌ای است که یک عمل تروریستی در آن انجام می‌شود یا ابزاری است که می‌توان از آن برای انجام یک جرم تروریستی استفاده کرد. جرایم دیجیتالی یک جرم هزار ساله جدید است که چالش‌های جدیدی را به ویژه برای نیروی کار در محکومیت جرایم دیجیتالی ایجاد می‌کند. جامعه بین‌المللی باید نقش‌های مربوطه خود را ایفا کرده و با برای مهار گسترش این جرایم دیجیتالی و تهدید دیجیتالی تشریک مساعی کنند.

1. “Draft United Nations Convention against Cybercrime”, UN General Assembly, A/AC.291/L.16, New York, 29 July–9 August 2024, 7 August 2024, https://documents.un.org/doc/undoc/gen/v24/055/48/pdf/v2405548.pdf

2. Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series - No. 185, https://rm.coe.int/1680081561

از آنجایی که جرایم دیجیتال یک تهدید بزرگ برای همه کشـــورهای جهان است، باید اقدامات خاصی در سطح بین المللی برای پیشگیری از جرایم دیجیتال انجام شود. باید عدالت کامل برای بزه‌دیدگان جرایم دیجیتال از طریق جبران خسارت و برخورد قاطع با متخلفان برقرار شود تا بتواند مجرمان جرایم اینترنتی را پیش‌بینی کند.

به‌هر روی، با توجه به یافته‌های پژوهشی در این مطالعه می‌توان پیشنهادهای ذیل را در جهت ارتقای ســـطح محافظت از ســـکوهای دیجیتالی در قبال جرایم تروریستی ارتکابی ابراز داشت که امکانی برای ارتقای امنیت دیجیتالی دولت‌ها فراهم آید:

الف- ارتقاء سطح آگاهی، مهارت‌ها و توانمندسازی در سراسر جامعه برای مدیریت خطر امنیت دیجیتالی از طریق ابتکارات بی طرفانه از حیث فناوری متناسب با نیازهای خاص گونه‌های مختلف ذینفعان؛

ب- پشـــتیبانی از توســـعه و حفظ نیروی کار ماهر که امکان مدیریت خطر امنیت دیجیتالی را فراهم آورد، به ویژه با پرداختن به مدیریت خطر امنیت دیجیتالی نظیر جرایم تروریســـتی در راهبردهای مهارتی گسترده؛

پ- تشـــویق به اســـتفاده از استانداردهای بین المللی و بهترین شیوه‌ها در مدیریت خطر امنیت دیجیتالی، و ارتقاء توسعه و بازنگری آنها از طریق فرآیندهای باز، شفاف و چند ذینفع؛

ت- هماهنگـــی و ترویج تحقیق و توســـعه عمومی در مورد مدیریـــت خطر امنیت دیجیتالی با هـــدف تقویت و ارتقای امنیت ســـکوهای دیجیتالی در قبال تهدیدهای ناشـــی از ارتکاب جرایم تروریستی؛

ث- پیش‌بینـــی چالش‌های امنیت دیجیتالی مرتبط با تحـــول دیجیتالی مخرب در بخش‌های گوناگون و ویژه؛

ج- تبـــادل اطلاعـــات راجع‌بـــه مدیریت خطر امنیـــت دیجیتالی و بهبود شناســـایی و اصلاح آسیب‌پذیری‌ها و تهدیدها، و همچنین کاهش خطر امنیت دیجیتالی؛

چ- تلاش برای بهبود پاســـخ‌ها اعم از حقوقی و فنی به تهدیدهای داخلی و بین‌المللی از ســـوی دولت‌ها در قبال ارتکاب جرایم تروریستی در سکوهای دیجیتالی؛

ح- ایجاد ســـازوکارهای هماهنگی میان جامعه بین‌المللی برای اطمینان از ســـازگاری مدیریت خطر امنیت دیجیتالی.

منابع

برجعلی زاده، محمد، جعفری، علی و کردی، ناهید (۱۳۹۷). بررسی نقش رسانه‌های مدرن در گسترش تروریسم در عرصه بین المللی، مطالعات قدرت نرم، ۱(۹).

شاهیده، فرهاد (۱۴۰۲). سیاست‌گذاری جنایی در برابر تروریسم، تهران: بنیاد حقوقی میزان، چاپ اول.

جلالی، محمود و توسلی اردکانی، سعیده (۱۳۹۷). ضرورت ایجاد نظام حقوقی هماهنگ بین‌المللی در برخورد با جرایم در فضای سایبری، مطالعات حقوق عمومی، ۴(۴۹).

موسوی، سیدجمال، روحانی‌مقدم، محمد و آقایی‌بجستانی، مریم (۱۳۹۱). اقدامات پیشگیری از جرایم سایبری با تأکید بر اقدامات پلیسی با رویکرد فقهی، مطالعات فقه و حقوق اسلامی، ۱۴(۲۶).

یزدان‌پناه‌درو، کیومرث و مهتاب جعفری (۱۳۹۷). تحلیل ژئوپلیتیک اثرگذاری اینترنت در افزایش فعالیت تروریسم: با تأکید بر داعش. پژوهش‌های راهبردی سیاست، ۲۶(۵۶): ۲۴۴-۲۲۱.

Kristin, Archick (2014), "U.S.-E.U. Cooperation Against Terrorism", CRS (Dec. 1).

Barrie, Sander, "International Law in the Age of Digital Media: Reflections on History, the Neoliberal Communication Sphere, and Race", London Review of International Law, 2022, (10)2, 295.

Corliss, Cody (2023), "Digital Terror Crimes", Columbia Journal of Transnational Law, 62(13): 58-112.

Douhan, Alena, "The Changing Nature of Sanctions in the Digital Age", in: Digital Transformations in Public International Law, Angelo Jr. Golia | Matthias C. Kettemann Raffaela Kunz [Eds.], Published by Nomos, 2022, p. 129.

McAfee (2021) McAfee and the Center for Strategic and International Studies (CSIS). The Hidden Costs of Cybercrime. https://www.csis.org/analysis/hidden-costs-cybercrime

Moynihan, Harriet (2021), "The Vital Role of International Law in the Frame-

work for Responsible State Behaviour in Cyberspace", Journal of Cyber Policy, 6(3): 394-410.

Fidler, David P (2016), "Cyber Space, Terrorism and International Law Get Access Arrow", Journal of Conflict and Security Law, 21(3): 475-493.

Mohamed, D. (2012). Investigating Cybercrimes Under the Malaysian Cyber Laws and the Criminal Procedure Code: Issues and Challenges. Malaysian Law Journal, 6: 1–10.

Odhiambo, N. A., Ochara, N. M., and Kadymatimba, A. (2018), "Structuring of the Terrorism Problem in the Digital Age: A Systems Perspective", in: Open Innovations Conference, OI (Johannesburg: IEEE), pp. 148-154.

Jerome Orji, Uchenna (2022), "Interrogating African Positions on State Sponsored Cyber Operations: A Review of Regional and National Policies and Legal Responses", Baltic Yearbook of International Law Online, 20(1): 236–267.

Kumar Saini, Hemant (2023), Artificial Intelligence and Internet of Things: A Boon for the Crime Prevention, International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), 23-24 Nov, 1-43.

Yüksel, Cüneyt (2020), "Combating Terrorist Use of the Internet and Social Media: Recommended Solutions within the Scope of International Law", Public and Private International Law Bulletin, 40(2), p. 1092.

Plotnek, Jordan J and Jill Slay (2021), "Cyber Terrorism: A Homogenized Taxonomy and Definition", Computers & Security, 102: 102-145.

Reveron, Derek S. and John E. Savage (2023), "International Law and Norms in Cyberspace", in: Security in the Cyber Age An Introduction to Policy and Technology, Cambridge University Press, pp. 226 - 252.

Ronkova, Nevenka, "International Legal Framework for Media", Journal of Process Management New Technologies, 2016, 4(2), p. 58.

Weimann, Gabriel (2014), “New Terrorism and New Media”, Wilson Center Commons Lab, 1, available at http://www.wilsoncenter.org/publication/new-terrorism-and-new-media.

Taylor, Robert W., Eric J. Fritsch, John Liederbach (2014), Digital Crime and Digital Terrorism, Prentice Hall Press.

Zhu, Lixin and Wei Chen (2022), “Chinese Approach to International Law with Regard to Cyberspace Governance and Cyber Operation: From the Perspective of the Five Principles of Peaceful Co-existence”, Baltic Yearbook of International Law Online, 20(1): 187–208.