The Journal of Iranian Health System Law
فصلنامه حقوق نظام سلامت ایران

Vol 1, No 3, Pages: 23-33 **Original Article**

Response to Threats from Terrorist Crimes on Digital Platforms to Violations of Public Health Rights

Peyman Namamian[*1]

1. Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran. (Corresponding Author) Email: p_namamian@araku.ac.ir

Received: 09 Jan 2024 **Revised:** 05 Apr 2024 **Accepted:** 10 May 2024 **Available Online:** 22 Sep 2025

Abstract: The harms in digital platforms are considered a new health risk in the digital age. The digital space has created new security challenges for governments. The threats posed by terrorist crimes in digital platforms for the healthcare and public health sectors are expanding. Therefore, the main threats in the digital space include external threats, internal threats, threats in the supply chain of goods and services and threats arising from the operational inability of local forces. The consequences of terrorist crimes in digital platforms can include a catastrophic threat to national security, the beginning of internal insecurity and the creation of widespread national destruction at the international level, catastrophic destruction or damage to national political and economic relations, widespread human losses or risks to public health and safety, widespread disruption of the governance of the country, the destruction of public trust or religious, national and ethnic beliefs and widespread destruction or disruption in the functioning of national digital assets. To counter the growing risk of terrorist crimes on digital platforms, which pose challenges to the protection of public health, it is necessary to adopt mechanisms in line with healthcare. Of course, improving digital security is an undeniable step towards the level of preparedness of governments to defend themselves and their digital assets against terrorist crimes on digital platforms.

Keywords: Digital Space, Digital Crimes, Terrorist Crimes, Public Health, Health Rights.

Please Cite This Article As: Namamian, P (2025). "Response to Threats from Terrorist Crimes on Digital Platforms to Violations of Public Health Rights". *Iranian Health System Law*, 1(3): 23-33.

مقاله پژوهشی

(صفحات ۲۳-۳۳)

پاسخ به تهدیدهای ناشی از جرایم تروریستی در سکوهای دیجیتالی در قبال نقض حقوق سلامت عمومی

پیمان نمامیان*[۱]

۱. دانشیار حقوق کیفری و جرم‌شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران. (نویسنده مسؤول)
Email: p_namamian@araku.ac.ir

تاریخ دریافت: ۱۴۰۲/۱۰/۱۹ **تاریخ ویرایش:** ۱۴۰۳/۰۱/۱۷ **تاریخ پذیرش:** ۱۴۰۳/۰۲/۲۱ **تاریخ انتشار:** ۱۴۰۴/۰۷/۰۱

چکیده:

آسیب‌های موجود در سکوهای دیجیتالی به‌عنوان یک خطر جدید برای سلامتی در عصر دیجیتال قابل ملاحظه است. فضای دیجیتالی چالش‌های امنیتی جدیدی را برای دولت‌ها ایجاد کرده است. تهدیدهای ناشی از جرایم تروریستی در سکوهای دیجیتالی برای بخش‌های بهداشت و درمان و سلامت عمومی در حال گسترش است. ازاین‌رو تهدیدهای اساسی در فضای دیجیتالی مشتمل بر تهدیدهای خارجی، تهدیدات داخلی، تهدیدات در زنجیره تأمین کالا و خدمات و تهدیدات ناشی از ناتوانی عملیاتی نیروهای بومی است. پیامدهای جرایم تروریستی در سکوهای دیجیتالی می‌تواند مشتمل بر تهدید فاجعه‌بار امنیت ملی، سرآغاز ناامنی‌های داخلی و ایجاد تخریب گسترده ملی در سطح بین‌المللی، تخریب یا آسیب فاجعه‌آمیز به روابط سیاسی و اقتصادی ملی، تلفات انسانی گسترده یا خطر برای سلامت و ایمنی عمومی، اختلال گسترده در اداره کشور، از بین‌بردن اعتماد عمومی یا باورهای مذهبی، ملی و قومی و تخریب یا اختلال گسترده در عملکرد دارایی‌های دیجیتالی ملی باشد. برای مقابله با خطر فزاینده جرایم تروریستی در سکوهای دیجیتالی که امکان محافظت از سلامت عمومی را با مشکلاتی مواجه است که باید نسبت به اتخاذ سازوکارهایی در راستای مراقبت‌های بهداشتی، اقدام کرد، البته ارتقای امنیت دیجیتالی سطح آمادگی دولت‌ها برای دفاع از خود و دارایی‌های دیجیتالی خود در قبال جرایم تروریستی در سکوهای دیجیتالی امری انکارناپذیر است.

کلمات کلیدی: سکوی دیجیتالی، جرایم دیجیتالی، جرایم تروریستی، سلامت عمومی، حقوق سلامت.

مقدمه

در حال حاضر بیشتر فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و در تمامی سطوح اعم از افراد، سازمان‌های مردم‌نهاد و نهادهای دولتی در فضای مجازی انجام می‌شود. دنیای امروز به‌شدت به فناوری الکترونیک وابسته است و حفاظت از این داده‌ها در قبال جرایم تروریستی در سکوهای دیجیتالی یک مسأله چالش‌برانگیز است. ازاین‌رو مقامات امنیتی مدت‌هاست که نسبت به تهدید پیش‌بینی‌شده ناشی از جرایم تروریستی در سکوهای دیجیتالی هشدار داده‌اند (Shandler *et al*, 2022: 853).

چالش‌های امنیتی جدیدی در فضای دیجیتالی برای دولت‌ها ایجاد شده است.[۱] این امر تهدیدهای ناشی از جرایم تروریستی در سکوهای دیجیتالی را از تهدیدهای سنتی امنیت ملی متمایز می‌کند که به‌طور عمده ماهیت شفافی دارند و بازیگران آن دولت‌ها و ملت‌هایی هستند که در یک منطقه جغرافیایی خاص قابل شناسایی هستند و باعث شده است که امنیت ملی به‌معنای سنتی آن در این زمینه به چالش کشیده و ناکارآمد باشد.[۲]

تهدیدهای ناشی از جرایم تروریستی در سکوهای دیجیتالی برای بخش‌های بهداشت و درمان و سلامت عمومی در حال گسترش است[۳]، البته می‌توان اشاره کرد که در دسامبر ۲۰۲۱، یک جرم دیجیتالی با رویکرد تروریستی موجب شد تا وزارت بهداشت مریلند وب‌گاه خود را برای مدتی غیربرخط نموده و کنترل شیوع کووید-۱۹ و سایر خدمات معمول بهداشت عمومی را قطع نماید.[۴]

جرایم تروریستی در سکوهای دیجیتالی شامل استفاده از اینترنت و سایر اشکال فناوری اطلاعات و ارتباطات برای تهدید یا ایجاد آسیب بدنی برای به‌دست‌آوردن قدرت سیاسی یا ایدئولوژیکی از طریق تهدید یا ارعاب است. سرقت و دستکاری داده‌ها و اختلال در خدمات ضروری، همه انواع جرایم دیجیتالی با رویکرد تروریستی هستند. با کاهش موانع ورود برای عوامل مخرب، جرایم تروریستی در سکوهای 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 در سکوهای 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، درنتیجه جرایم دیجیتالی، زیرساخت‌های حیاتی مانند شبکه‌های برق، بیمارستان‌ها و سیستم‌های حمل و نقل نیز می‌توانند مختل شوند که منجر به اختلالات و پریشانی گسترده شود (Iftikhar, 2024: 1).

با این همه، نگارنده در این مقاله بر آن است تا با استفاده از اطلاعات و منابع کتابخانه‌ای و وب‌گاه‌ها و بهره‌گیری از روش پژوهش توصیفی ـ تحلیلی و پاسخ به این پرسش‌هایی که «با چه سازوکارهای فنی و حقوقی می‌توان نسبت به تهدیدهای ناشی از جرایم تروریستی ارتکابی در سکوهای دیجیتالی از چهارچوب حقوق سلامت عمومی حمایت کرد؟» و «با چه ابزارهایی دولت‌ها امکان

---

[۱]- تهدیدهای ناشی از جرایم تروریستی در سکوهای دیجیتالی می‌توانند بر دارایی‌های دیجیتالی ملی در سطوح فراملی، ملی، نهادی، استانی، حیاتی و حیاتی زیرساخت تأثیر بگذارند، درضمن تهدیدهای اساسی موجود در فضای دیجیتالی مشتمل بر تهدیدهای خارجی، تهدیدات داخلی، تهدیدات در زنجیره تأمین کالا و خدمات و تهدیدات ناشی از ناتوانی عملیاتی نیروهای بومی است، البته تروریست‌ها منبع دیگری از تهدید هستند که به‌دنبال تخریب، از کارانداختن یا سوءاستفاده از زیرساخت‌های حیاتی برای تهدید امنیت ملی، واردکردن خسارات سنگین، تضعیف اقتصاد کشور و تضعیف ذهنیت و اعتماد عمومی هستند (Saxena and Gayathri, 2021: 82).

[۲]- پیامدهای جرایم تروریستی در سکوهای دیجیتالی می‌تواند مشتمل بر تهدید فاجعه‌بار امنیت ملی، سرآغاز ناامنی‌های داخلی و ایجاد تخریب گسترده ملی در سطح بین‌المللی، تخریب یا آسیب فاجعه‌آمیز به روابط سیاسی و اقتصادی ملی، تلفات انسانی گسترده یا خطر برای سلامت و ایمنی عمومی، اختلال گسترده در اداره کشور، از بین‌بردن اعتماد عمومی یا باورهای مذهبی، ملی و قومی و تخریب یا اختلال گسترده در عملکرد دارایی‌های دیجیتالی ملی باشد. علاوه‌بر این، مسائل قابل ملاحظه و چالش‌برانگیزی را می‌توان برای را جنگ دیجیتالی در نظر گرفت: ۱- جاسوسی دیجیتالی تحت حمایت دولت برای جمع‌آوری اطلاعات برای برنامه‌ریزی جرم دیجیتالی با رویکرد تروریستی آینده؛ ۲- یک جرم دیجیتالی با رویکرد تروریستی با هدف ایجاد زمینه برای هرگونه ناآرامی و خیزش مردمی؛ ۳- جرم دیجیتالی با رویکرد تروریستی با هدف از کارانداختن تجهیزات و تسهیل تهاجم فیزیکی؛ ۴- جرم دیجیتالی با رویکرد تروریستی به‌عنوان مکمل تهاجم فیزیکی؛ ۵- جرم دیجیتالی با رویکرد تروریستی با هدف تخریب یا اختلال گسترده به‌عنوان هدف نهایی (جنگ دیجیتالی).

[3]- https://www.naccho.org/blog/articles/cyber-threats-public-health-risk.

[4]- Maryland health workers, lawmakers want answers as problems persist a month after cyberattack. Washington Post. (January 8, 2022). https://www.washingtonpost.com/dc-md-va/2022/01/08/cyberattack-still-disrupting-maryland-department-of-health/.

حمایت از حقوق سلامت عمومی در قبال جریم تروریستی و تهدیدهای ناشی از آن در سکوهای دیجیتالی را دارند؟» نسبت به تهدیدهای ناشی از جرایم تروریستی را در سکوهای دیجیتالی و تجربیات حقوقی و قانون‌گذاری برخی از کشورها را مورد سنجش قرار دهد.

۱- جرایم تروریستی در سکوهای دیجیتالی؛ شناخت مفهوم و توصیف آن

استفاده روزافزون از فناوری‌های دیجیتال مخاطره‌هایی را برای سیستم‌های حیاتی به‌دلیل بهره‌برداری توسط تروریست‌ها ایجاد می‌کند. امنیت فضای دیجیتال مستلزم اقدامات پیشگیرانه و واکنشی است که برای محافظت از نرم‌افزار و دستگاه‌های الکترونیکی در قبال هرگونه تهدید طراحی شده است (Shaweorcid & McAndrew, 2023: 548). ورود این فناوری به روش‌های ارتکاب جرایم نیز امکان‌پذیر شده است و یکی از مهم‌ترین آن‌ها جرایم مدرن نظیر جرایم تروریستی در سکوهای دیجیتالی است.

برخلاف جرایم سنتی، جرایم دیجیتال دارای ویژگی‌های منحصربه‌فردی است. ازاین‌رو مجرمان مرتکب انواع مختلف جرایم دیجیتال شده‌اند که در ذیل قابل ملاحظه است:

۱- حمله با تهدید: تهدید جان دیگران یا تلاش برای بدنام‌کردن افراد دیگر با استفاده از رایانه، شبکه یا تلفن.

۲- هرزه‌نگاری کودکان: استفاده از رایانه، شبکه و سایر وسایل دیجیتال در بهره‌کشی جنسی از کودکان.

۳- پول‌شویی دیجیتالی: انتقال الکترونیکی پول غیرقانونی برای پنهان‌کردن منبع یا مقصد.

۴- سرقت دیجیتالی استفاده از رایانه برای سرقت است: از رایانه در فعالیت‌های مجرمانه استفاده می‌شود. به‌عنوان مثال می‌توان به جاسوسی، سرقت هویت، کلاه‌برداری، هک مخرب و سرقت ادبی اشاره کرد (Nabat Arfi, 2013: 3). شواهد دیجیتالی به عنوان هر داده‌ای است که با استفاده از رایانه ذخیره یا منتقل می‌شود که نظریه‌ای در مورد چگونگی وقوع جرم را تأیید یا رد می کند یا ارکان جرم را مورد توجه قرار می‌دهد. داده‌ها در اینجا به انواع مختلفی از اطلاعات مانند متن، شماره صوتی یا تصویری اشاره دارند.

اصطلاحات جدید در زبان جرم مانند جرایم دیجیتالی نوع جدیدی از تحقیقات جنایی را ایجاد می‌کند که مستقیماً به جرایم دیجیتال مربوط می‌شود. تحقیقات دیجیتالی جرم مانند سایر انواع تحقیقات سعی در پاسخگویی به سؤالات رایجی، مانند چه کسی، چه چیزی، چه زمانی، کجا، چرا و چگونه دارد (Computer Crime Investigation & Computer Forensic, 1997: 28). محقق ابتدا این سؤالات را می‌پرسد و سعی در حل آن‌ها دارد. در پایان، هدف نهایی در پشت تحقیقات، کشف حقیقت و مجرمان واقعی با ردیابی آن‌چه آن‌ها پشت سر خود به‌جا می‌گذارند، است، اما در اینجا صحنه جنایی که مورد بررسی قرار خواهد گرفت، یک صحنه سنتی نیست، بلکه یک صحنه دیجیتال است. یک بازپرس در حوزه جرایم دیجیتال باید بتواند شواهد قابل توجهی را از صحنه جرم جمع‌آوری کند. منظور از شواهد به‌ویژه شواهد دیجیتالی است که مجرم می‌تواند آن‌ها را در رایانه‌ها، شبکه‌ها یا هر وسیله دیجیتالی به‌جا بگذارد. یک محقق باید بتواند این شواهد را کشف کند و با آن‌ها به شیوه‌ای مناسب برخورد کند، زیرا شواهد دیجیتالی نسبت به هرگونه تغییر حساس هستند. همچنین او باید مسائل حقوقی مربوط به تحقیقات جرایم دیجیتال را به‌خوبی درک کند و از طریق کار خود در برابر هرگونه خطری آماده باشد (Aaron, 2010: 89).

۲- ارتکاب جرایم تروریستی در سکوهای دیجیتالی علیه نظام مراقبت سلامت عمومی

در چهارچوب حقوق بین‌الملل، دولت‌ها باید برای مقابله با جرایم تروریستی در سکوهای دیجیتالی علیه امکانات و قابلیت‌های بهداشتی در طول همه‌گیری کووید-۱۹ سازوکارهای عملیاتی فنی و حقوقی را اتخاذ نمایند، بنابراین قانونی‌بودن ارتکاب جرایم دیجیتالی با رویکرد تروریستی توسط بازیگران غیردولتی، مانند جنایتکاران، هکرها، یا گروه‌های تروریستی، عموماً با استناد به موازین حقوق بین‌المللی ارزیابی نمی‌شود (Ruvic, 2020: 1).

برای تعیین این‌که آیا یک دولت مسؤول نقض حقوق بین‌المللی در رابطه با جرایم تروریستی در سکوهای دیجیتالی علیه یک مرکز بهداشتی یا توانایی یا فعالیت بهداشت عمومی است، این عملیات باید از نظر قانونی قابل انتساب به آن دولت باشد. در اصطلاح قانون مسؤولیت دولت، «دولت مسؤول» درصورت تلاقی این دو شرط، مرتکب «عمل متخلف بین‌المللی» علیه «دولت آسیب‌دیده» شده است.[1] انتساب زمانی واضح‌تر است که جرایم تروریستی در سکوهای دیجیتالی توسط نهادها و دولت‌ها صورت پذیرد. با این حال، دولت‌ها اغلب برای انجام جرایم تروریستی در سکوهای دیجیتالی خود به گروه‌های غیردولتی مانند هکرهای سیاسی، گروه‌های تروریستی یا بخش خصوصی روی می‌آورند، درحالی‌که چندین موقعیت وجود دارد که در آن ممکن است اقدامات یک بازیگر غیردولتی به‌عنوان یک موضوع قانونی به یک دولت نسبت داده شود.

۳- حفاظت از بخش مراقبت‌های بهداشتی در قبال جرایم تروریستی در سکوهای دیجیتالی

مقررات راجع به بخش مراقبت‌های بهداشتی در قبال جرایم تروریستی در سکوهای دیجیتالی با جرم‌انگاری رفتار مربوطه، امکان محافظت را فراهم می‌کند. این امر عمدتاً در رژیم‌های حقوق کیفری داخلی اتخاذ می‌شود که اغلب رفتارهایی را که سلامت و ایمنی عمومی را به خطر می‌اندازد، صرف نظر از ابزار مورد استفاده، جرم‌انگاری می‌کنند، اما حقوق بین‌الملل نیز ممکن است نقش داشته باشد. وفق کنوانسیون ۲۰۰۱ بوداپست دولت‌های عضو ملزم به جرم‌انگاری فعالیت‌های دیجیتالی مشخص، مانند دسترسی غیرقانونی (ماده ۲)، تداخل داده‌ها (ماده ۴) و تداخل در سیستم (ماده ۵) هستند. دولت‌های عضو نیز موظفند در تحقیق و تعقیب اعمالی که توسط کنوانسیون جرم‌انگاری شده است، با یکدیگر همکاری کنند.

در دنیای امروزی که به دیجیتال وابسته است، جرایم تروریستی در سکوهای دیجیتالی تهدیدات واقعی برای زیرساخت‌های حیاتی و عملکرد جوامع است. کمیته بین‌المللی صلیب سرخ به‌ویژه نگران آسیب‌پذیری بیمارستان‌ها در برابر جرایم دیجیتالی است، خطری که همیشه حاد است، اما در مواقع درگیری یا بیماری‌های همه‌گیر، مانند بحران فعلی کووید-۱۹، حتی خطرناک‌تر است. دبیرکل سازمان ملل متحد ابراز نگرانی کرده است که اگر امروز یک درگیری بزرگ آغاز شود، «با یک حمله دیجیتالی گسترده نه‌تنها به تأسیسات نظامی، بلکه برخی از زیرساخت‌های غیرنظامی آغاز می‌شود.»[2]

در سال ۲۰۱۳، کشورهای عضو کنوانسیون به‌صراحت موافقت کردند که حملات به سیستم‌های رایانه‌ای ضروری برای حفظ سلامت و ایمنی عمومی تحت پوشش مقررات موجود کنوانسیون قرار می‌گیرد، به‌علاوه به شرط رعایت الزامات خاص این جنایات، جرایم تروریستی خاص در سکوهای دیجیتالی به‌ویژه علیه تأسیسات پزشکی می‌تواند به‌عنوان جنایات بین‌المللی، مانند جنایات جنگی یا جنایات علیه بشریت واجد شرایط باشد (Durham, 2020: 1).

در طول درگیری‌های مسلحانه، حقوق بشردوستانه بین‌المللی حمایت‌های قوی برای خدمات و امکانات پزشکی ارائه می‌کند. این به این دلیل است که یکی از الزامات اساسی حقوق بشردوستانه بین‌المللی کاهش تا آنجا که ممکن است از رنج‌های جدانشدنی از جنگ است. در جنگ، رزمندگان و غیرنظامیان ممکن است دچار جراحات و بیماری شوند و باید از آن‌ها مراقبت کرد.

مادامی‌که درگیری‌ها و بیماری‌های همه‌گیر تلاقی می‌کنند، این محافظت‌ها مهم‌تر از همیشه هستند: جایی که افرادی که خانه هایشان ویران شده یا در اثر درگیری آواره شده‌اند، در پناهگاه‌ها و بدون امکانات بهداشتی مناسب زندگی می‌کنند، ویروس سریع تر و گسترده‌تر پخش می‌شود، اما اگر بیمارستان‌ها دیگر کار نکنند، درمان نجات‌بخش در دسترس نخواهد بود. بر این اساس،

[1]- Report of the International Law Commission to the General Assembly, art. 2, U.N. GAOR, 56th Sess., Supp. No. 10, at 32, U.N. Doc. A/56/10 (2001) [hereinafter Articles on State Responsibility].
[2]- https://www.wired.com/story/un-secretary-general-antonio-guterres-internet-risks/.

حقوق بشردوستانه بین‌المللی ایجاب می‌کند که واحدهای پزشکی، حمل‌ونقل و پرسنل باید همیشه توسط طرفین درگیری مورد احترام و محافظت قرار گیرند.[۱]

مقررات اساسی حقوق بشردوستانه بین‌المللی مانند این موارد نیز «در فضای مجازی اعمال می‌شود و باید رعایت شوند»، بنابراین متخاصمان نباید از طریق جرایم تروریستی در سکوهای دیجیتالی به زیرساخت‌های پزشکی آسیب برسانند و باید احتیاط زیادی برای پیشگیری از آسیب‌های اتفاقی ناشی از این عملیات‌ها داشته باشند. از نظر کمیته بین‌المللی صلیب سرخ، این حمایت قانونی شامل داده‌های مربوط به واحدهای پزشکی و پرسنل آن‌ها نیز می‌شود.

بنابراین جرایم تروریستی در سکوهای دیجیتالی که عملکرد تأسیسات مراقبت‌های بهداشتی را در طول درگیری‌های مسلحانه مختل کند، توسط حقوق بشردوستانه بین‌المللی ممنوع است. درنهایت همان‌طور که در بالا ذکر شد، جرایم تروریستی در سکوهای دیجیتالی ممکن است به‌عنوان یک جنایت جنگی واجد شرایط باشد، مشروط بر این‌که شرایط خاص برآورده شود.[۲]

هیچ قانون حقوقی بین‌المللی مستقلی وجود ندارد که به‌طور جامع از امکانات پزشکی محافظت کند. سه حوزه از حقوق بین‌الملل ممکن است تعهدات مربوطه را در رابطه با حملات یک دولت یا نیروهای نیابتی آن علیه زیرساخت‌های بهداشتی یک کشور دیگر ارائه دهد: قانون استفاده از زور، اصل عدم مداخله و اصل حاکمیت اولاً حقوق بین‌الملل ممنوعیت کلی استفاده از زور را در بند ۴ ماده ۲ منشور ملل متحد پیش‌بینی کرده است. در میان مفسران دانشگاهی اتفاق نظر وجود دارد که جرایم تروریستی در سکوهای دیجیتالی تحت حمایت دولت که مستقیماً منجر به کشتن افراد در خارج از کشور می‌شود، مشمول این ممنوعیت می‌شود.

درحالی‌که این ممنوعیت همه جرایم تروریستی در سکوهای دیجیتالی علیه تأسیسات پزشکی را پوشش نمی‌دهد، اما بسیار مهم است، زیرا حملاتی را که ممکن است انتظار می‌رود شدیدترین عواقب را داشته باشند، ممنوع می‌کند؛ ثانیاً حقوق بین‌الملل همه کشورها را از مداخله در امور داخلی سایر کشورها منع می‌کند. به‌عنوان مثال، بریتانیا به‌صراحت اعلام کرده است که این ممنوعیت ممکن است اعمالی مانند هدف قراردادن خدمات ضروری پزشکی را نیز دربر گیرد.

به‌نظر می‌رسد جرایم تروریستی در سکوهای دیجیتالی که ارائه مراقبت‌های بهداشتی را در قلمرو کشوری دیگر تضعیف می‌کند، با این حق تداخل دارد. با این حال، این تحلیل به‌دلیل اختلاف مداوم در مورد این‌که آیا واقعاً یک تعهد حقوقی مستقل بین‌المللی برای احترام به حاکمیت سایر کشورها در فضای دیجیتال وجود دارد یا خیر یا این‌که آیا حاکمیت «صرفاً» یک اصل است که تعاملات دولت‌ها را هدایت می‌کند، پیچیده است، اما خود نمی‌تواند باشد، نقض شده است.

همچنین ممکن است این سؤال مطرح شود که آیا جرایم تروریستی در سکوهای دیجیتالی تحت حمایت دولت علیه بخش مراقبت های بهداشتی یک کشور دیگر می‌تواند حقوق بین‌المللی حقوق بشر را نقض کند. از آنجایی که «همان حقوقی که افراد آفلاین دارند، باید به‌صورت آنلاین نیز محافظت شوند»، دولت‌ها عموماً ملزم به تعهدات مرتبط هستند، مانند تعهدات ناشی از حق سلامت مندرج در ماده ۱۲ میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی (ICESCR) یا حق حیات مندرج در ماده ۶ میثاق بین‌المللی حقوق مدنی و سیاسی (ICCPR). باتوجه به عملیات فراسرزمینی، طبق نظر عمومی ۳۱ کمیته حقوق بشر سازمان ملل متحد، دولت‌ها تعهدات مربوطه را نسبت به همه افراد تحت «قدرت یا کنترل مؤثر» خود دارند. با این حال، دیدگاه‌های متفاوتی

---

[۱]- براساس حقوق بین‌الملل بشردوستانه و در چهارچوب بند چهارم از ماده ۵۱ پروتکل اول الحاقی به کنوانسیون‌های چهارگانه ژنو، حملاتی که از ابزارها یا روش‌های جنگی استفاده می‌کنند که نمی‌توانند علیه یک هدف نظامی خاص هدایت شوند یا اثرات آن را نمی‌توان به شیوه‌ای قانونی محدود کرد، ممنوع است. درواقع، تأیید محدودیت‌هایی که حقوق بشردوستانه بین‌المللی بر جرایم تروریستی در سکوهای دیجیتالی در جریان درگیری‌های مسلحانه اعمال می‌کند، امروز بیش از هر زمان دیگری اهمیت دارد. جرایم تروریستی در سکوهای دیجیتالی به واقعیت درگیری مسلحانه تبدیل شده است و بسیاری از کشورها در حال توسعه قابلیت‌های تهاجمی دیجیتالی هستند. دولت‌ها موظفند اطمینان حاصل کنند که این ابزارها و روش‌های جدید جنگ بدون محدودیت نیستند، حتی در زمان صلح، برخی از موازین حقوق بشردوستانه بین‌المللی، انواع سلاح‌ها، وسایل و روش‌هایی را که ممکن است ایجاد شود، محدود می‌کند.

[۲]- جنایت جنگی هدایت حمله به یک مرکز پزشکی تحت اساسنامه رم دادگاه کیفری بین‌المللی که در ماده ۸ (xxiv) (b) (2) و (ii) (e) پیش‌بینی شده است.

در مورد این‌که آیا کسانی که تحت تأثیر جرایم تروریستی در سکوهای دیجیتالی در قلمرو کشور دیگری قرار می‌گیرند، در محدوده قدرت یا کنترل مؤثر آن دولت هستند، وجود دارد (Gisel & Rodenhauser, 2019: 1).

باتوجه به حق زندگی، کمیته حقوق بشر اخیراً اظهار داشت که تعهدات یک دولت برای احترام و تضمین این حق شامل افراد واقع در خارج از هر سرزمینی که به‌طور مؤثر توسط دولت کنترل می‌شود که حق زندگی آن‌ها با این وجود تحت تأثیر ارتش یا دولت قرار دارد، گسترش می‌یابد. سایر فعالیت‌ها به‌صورت مستقیم و قابل پیش‌بینی منطقی. به‌طور گسترده‌تر، کمیته حقوق اقتصادی، اجتماعی و فرهنگی سازمان ملل استدلال کرده است که «دولت‌های عضو باید به برخورداری از حق سلامت در سایر کشورها احترام بگذارند. به‌عبارت دیگر، دیدگاه‌های متفاوتی در مورد دامنه کاربرد حقوق بین‌المللی حقوق بشر به‌طور کلی و بر این اساس، در مورد میزان حفاظتی که حقوق بین‌المللی حقوق بشر به‌طور خاص از تأسیسات پزشکی در قبال جرایم تروریستی در سکوهای دیجیتالی می‌کند، وجود دارد» (Marelli, 2020: 1).

در هر حال، نهادهای مختلف حقوق بین‌الملل از تأسیسات پزشکی در برابر جرایم تروریستی در سکوهای دیجیتالی حمایت قوی می‌کنند. بسته به‌نحوه تفسیر حقوق بین‌الملل، می‌توان تصور کرد که هرگونه جرایم تروریستی در سکوهای دیجیتالی خصمانه علیه خدمات پزشکی را ممنوع می‌کند، هرچند برخی از تفاسیر ممکن است خلأهایی ایجاد کنند. این موضوع باتوجه به اهمیت خدمات پزشکی برای هریک از ما نگران‌کننده است. در این راستا، کمیته بین‌المللی صلیب سرخ اخیراً پیشنهاد کرده است که کشورهای شرکت‌کننده در کارگروه باز سازمان ملل متحد در مورد تحولات در زمینه اطلاعات و مخابرات در زمینه امنیت بین‌المللی، هنجار جدیدی از رفتار مسؤولانه دولت در فضای دیجیتال را مورد بررسی قرار دهند. این هنجار ایجاب می‌کند که «دولت‌ها نباید فعالیت‌های [دیجیتال] را که به خدمات پزشکی یا امکانات پزشکی آسیب می‌رساند، انجام دهند یا آگاهانه از آن‌ها حمایت نکنند و باید اقداماتی را برای محافظت از خدمات پزشکی در برابر آسیب انجام دهند.»

باتوجه به حقوق بین‌الملل بشردوستانه، هدف این مجموعه مقررات محدودیت استفاده از ابزار و روش‌های جنگ برای محافظت از غیرنظامیان و اشیای غیرنظامی در برابر اثرات خصمانه است. کمیته بین‌المللی صلیب سرخ از کشورها می‌خواهد که مواضع روشنی در مورد نحوه اعمال حقوق بشردوستانه بین‌المللی در فضای دیجیتال اتخاذ کنند، ازجمله در مورد این‌که چگونه از زیرساخت‌های غیرنظامی در برابر غیرفعال‌شدن از طریق ابزارهای دیجیتال محافظت می‌کند و چگونه از داده‌های غیرنظامی محافظت می‌کند. چنین مواضعی میزان حمایتی را که حقوق بشردوستانه بین‌المللی از غیرنظامیان و زیرساخت‌های غیرنظامی ارائه می‌کند را تعیین می‌کند و بر این اساس بر ارزیابی کافی و کافی‌بودن مقررات موجود یا نیاز به مقررات جدید برای تنظیم جرایم تروریستی در سکوهای دیجیتالی در طول درگیری‌های مسلحانه تأثیر می‌گذارد.[1]

۴- آثار و تبعات ناشی از جرایم تروریستی در سکوهای دیجیتالی بر سلامت عمومی

جرایم تروریستی در سکوهای دیجیتالی، حتی زمانی که کشنده نباشد، به طرق مختلف بر جمعیت غیرنظامی تأثیر می‌گذارد. نخست، جرایم تروریستی در سکوهای دیجیتالی اضطراب و ناامنی شخصی را تشدید می‌کند؛ دوم، جرایم تروریستی کشنده و غیرکشنده، تصور تهدید و ناامنی شخصی را تشدید می‌کند؛ سوم، بسیاری از مردم، به‌ویژه آن‌هایی که سطح بالایی از درک تهدید دارند، مایل به حمایت از سیاست‌های قوی دولت هستند. این سیاست‌ها در دو خط تقسیم می‌شوند و شامل سیاست خارجی (مانند پاسخ‌های دیجیتالی و/یا واکنش‌های نظامی جنبشی به جرایم دیجیتالی با رویکرد تروریستی) و سیاست داخلی (مانند تحمل نظارت دولت و کنترل اینترنت) می‌شوند. با افزایش درک تهدید، افراد دیدگاه‌های سیاسی سختگیرانه‌تری دارند. مانند جرم تروریستی متعارف، جرایم تروریستی در سکوهای دیجیتالی نگرش‌های سیاسی را سخت‌تر می‌کند، زیرا افراد مایلند آزادی‌های مدنی و حریم

[1]- https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/?.

خصوصی را برای امنیت مبادله کنند و از نظارت دولتی، مقررات بیشتر اینترنت و پاسخ‌های نظامی قاطع در پاسخ به جرایم تروریستی در سکوهای دیجیتالی حمایت کنند (Gross *et al*, 2016: 288).

سازمان بهداشت جهانی که علی‌رغم ادعاهای سیاسی برخلاف آن، نقشی حیاتی در واکنش جهانی به این بیماری همه‌گیر ایفا می کند، در معرض جرایم تروریستی در سکوهای دیجیتالی مخربی قرار گرفت که سعی در ایمن‌سازی رمز عبور پرسنل خود داشت (Satter *et al*, 2020: 1).

با این وجود، جرایم تروریستی در سکوهای دیجیتالی به اندازه جرم تروریستی کلاسیک اعتماد به دولت ملی یا نهادهای آن را تضعیف نمی‌کند. این از اقدامات اطمینان ما در مقایسه یک گروه کنترل با گروه‌هایی که در معرض تصاویر جرایم تروریستی متعارف و دیجیتالی قرار داشتند، مشهود بود، البته چنین معیارهای گسترده اعتماد همیشه تحت تأثیر جرایم تروریستی یا سایر رویدادهای آسیب‌زا قرار نمی‌گیرند.

درک تهدید و نه‌تنها رویدادهای واقعی دیجیتالی، تأثیرات شناختی جرایم تروریستی در سکوهای دیجیتالی را هدایت می‌کند. به عبارت دیگر، برای برانگیختن اضطراب، قرارگرفتن در معرض رویدادهای واقعی لازم نیست، بلکه تنها درک تهدید لازم است. این نتایج با مطالعاتی مطابقت دارد که نشان می‌دهد چگونه به سادگی افزایش و کاهش هشدارهای تهدید تروریستی می‌تواند اضطراب و افسردگی را افزایش دهد و تمایل به پذیرش محدودیت‌های آزادی‌های شخصی و اعمال خشونت‌آمیز علیه دیگران را تقویت کند (McDermott & Zimbardo, 2007: 359).

۵- حفاظت از سلامت عمومی و پاسخ به جرایم تروریستی در سکوهای دیجیتالی

جرایم تروریستی در سکوهای دیجیتالی علیه مراقبت‌های بهداشتی همچنان در حال افزایش است. روش‌های اولیه مورد استفاده در این حملات شامل فیشینگ و به خطرانداختن ایمیل (به‌عنوان مثال، باج‌افزار و سایر بدافزارها)، کلاه‌برداری، نقض سرور شبکه، دسترسی نامناسب به سوابق پزشکی، تهدیدات داخلی و سرقت استاندارد است.[1]

این نوع از جرایم تروریستی استرس و اضطراب را تشدید می‌کند، احساس آسیب‌پذیری را تشدید می‌کند و نگرش‌های سیاسی را سخت‌تر می‌کند. به این روش‌ها، ما نشان می‌دهیم که جرایم تروریستی در سکوهای دیجیتالی واکنش‌هایی مشابه جرایم تروریستی متعارف ایجاد می‌کند. این پاسخ‌ها بعد انسانی جرایم تروریستی در سکوهای دیجیتالی را برجسته می‌کنند که اغلب به‌دلیل تمرکز سیاست‌گذاران بر منافع امنیت ملی و حفاظت از مرزها، زیرساخت‌های حیاتی و قابلیت‌های نظامی نادیده گرفته می‌شود. هر دو مهم هستند و با افزایش تهدید جرایم تروریستی در سکوهای دیجیتالی، سیاست‌گذاران باید توجه خود را به ناراحتی عاطفی که جرایم تروریستی در سکوهای دیجیتالی ایجاد می‌کند، معطوف کنند، همان‌طور که برای تقویت قابلیت‌های دیجیتالی بازدارنده و تهاجمی تلاش می‌کنند.

درحالی‌که ابزارهای دیجیتال فرصت‌های جدیدی را برای افزایش سلامت و رفاه به ارمغان آورده‌اند، اما خطرات امنیتی جدیدی مانند جرایم تروریستی در سکوهای دیجیتالی علیه مراقبت‌های بهداشتی و اطلاعات نادرست نیز ایجاد کرده‌اند. برای ارائه درک واضح‌تر از این خطرات و کاهش احتمال و شدت آن‌ها، سازمان جهانی بهداشت دو گزارش را با همکاری اینترپل، دفتر مبارزه با مواد مخدر و جرم سازمان ملل متحد، دفتر مبارزه با تروریسم سازمان ملل متحد، مرکز محاسبات بین‌المللی سازمان ملل متحد[2]، مؤسسه تحقیقات جنایت و عدالت بین منطقه‌ای سازمان ملل متحد[3] و مؤسسه صلح سایبری[4] تهیه کرد.

---

[1]- https://domesticpreparedness.com/articles/cybersecurity-in-hospitals-and-the-public-health-sector.

[2]- UN International Computing Centre (UNICC)

[3]- UN Interregional Crime and Justice Research Institute

[4]- Cyber Peace Institute

وفق گزارش ارائه‌شده در ۲۶ ژانویه ۲۰۲۴ از سوی سازمان جهانی بهداشت ضمن ارائه سازوکارهایی برای امنیت سلامت عمومی، اذعان تأکید کرد در طول همه‌گیری کووید-۱۹، زیرساخت‌های فناوری اطلاعات سلامت به‌طور فزاینده‌ای مورد هدف جرایم تروریستی در سکوهای دیجیتالی قرار گرفت و در مواقعی بیمارستان‌ها را از ارائه مراقبت‌های به‌موقع در مواقعی که بیشتر مورد نیاز بود، بازداشت. برای بازیابی سیستم‌های فناوری اطلاعات و بازیابی داده‌های دزدیده‌شده، مراکز درمانی باج‌های قابل توجهی پرداخت کردند. این حملات سازمان‌های مجری قانون را بر آن داشت تا هشدارهایی در مورد تهدید جرایم تروریستی در سکوهای دیجیتالی به بخش بهداشت صادر کنند (Abed *et al*, 2024: 25).

جرایم تروریستی در سکوهای دیجیتالی در همه اشکال آن در حال تکامل و رشد بوده و گزارش مزبور حاکی از آن است که ایمنی بیماران تا چه حد در برابر جرایم تروریستی در سکوهای دیجیتالی آسیب‌پذیر است و همه ما چقدر کار برای تأمین امنیت زندگی در پیش داریم. سیستم‌های بهداشتی در سطح جهانی به راه حل‌های دیجیتالی روی آورده‌اند تا کیفیت بالینی و کارایی خدمات خود را افزایش دهند. این امر وابستگی دیجیتالی را ایجاد کرده است که گاهی اوقات بدون در نظرگرفتن دقیق خطرات جدید و سرمایه‌گذاری مناسب در امنیت دیجیتالی پیشرفت کرده است. اطلاعات حساسی که توسط خدمات بهداشتی نگهداری می‌شود، همراه با امنیت ناکافی، زیرساخت‌های مراقبت‌های بهداشتی را به یک هدف اصلی برای مجرمان دیجیتالی تبدیل می‌کند.[1]

برای مقابله با خطر رو به رشد دیجیتالی برای مراقبت‌های بهداشتی، افزایش ارتقای دیجیتالی مهم است. ارتقای امنیت دیجیتالی سطح آمادگی سازمان برای دفاع از خود و دارایی‌های دیجیتالش در برابر جرایم تروریستی در سکوهای دیجیتالی است. این شامل سرمایه‌گذاری بر روی افراد، فرآیندها و فناوری، ازجمله از طریق آموزش آگاهی دیجیتالی و توسعه طرح‌های واکنش به حادثه است که توسط کارکنان در پیش‌بینی جرایم دیجیتالی با رویکرد تروریستی تمرین می‌شود. افزایش ارتباطات و همکاری با آژانس‌های مجری قانون (مانند پلیس، اینترپل)، سازمان‌های دولتی (مانند آژانس امنیت دیجیتالی، مؤسسه بهداشت عمومی، آژانس ملی ایمنی داروها و محصولات بهداشتی، آژانس ایمنی هسته‌ای) ضروری است. بخش خصوصی و سازمان‌های غیردولتی، این نهادها می توانند هشدارها و هشدارهایی را در مورد جرایم تروریستی در سکوهای دیجیتالی در حال انجام ارائه دهند.

نتیجه‌گیری

تهدیدهای روزافزون برای امنیت دیجیتالی چالش‌های جدی برای سلامت جمعیت ایجاد می‌کند. با این حال، تقاطع مستقیم بین امنیت دیجیتالی و سلامت عمومی می‌تواند از بررسی از طریق لنزهای چهارچوب‌های عملیاتی سیستم سلامت عمومی بهره‌مند شود.

دولت‌ها براساس موازین حقوق بشر وظیفه دارند تا در قبال جرایم تروریستی در سکوهای دیجیتالی، ازجمله اطلاعات نادرست توسط دولت‌ها و بازیگران غیردولتی، به‌منظور حمایت از حقوق بشر در مورد زندگی و سلامتی کسانی که در قلمرو خود هستند، مبارزه کنند. مسلماً زمانی که جرایم تروریستی در سکوهای دیجیتالی که بر حقوق بشر افراد در خارج از مرزهایشان تأثیر می‌گذارد، از قلمرو آن‌ها یا از طریق آن‌ها راه‌اندازی می‌شود، آن‌ها همان تعهد را برعهده دارند. با این حال، دولت‌ها نباید با انجام این کار، سایر حقوق بشر، مانند آزادی بیان را بی‌رویه نقض کنند.

اگرچه به‌ندرت براساس حقوق بین‌المللی، به‌عنوان متمایز از هنجارهای سیاسی رفتار مسؤولانه دولت‌ها، اما همه دولت‌ها، دادگاه‌های حقوق بشر، نهادهای نظارت بر حقوق بشر، آکادمی، بخش خصوصی و سازمان‌های غیردولتی باید چالشی را که این همه‌گیری غم‌انگیز ایجاد می‌کند، بپذیرند تا قانون حاکم بر فضای دیجیتالی را در مسیر درست حرکت دهند.

---

[1]- https://www.who.int/news/item/06-02-2024-who-reports-outline-responses-to-cyber-attacks-on-health-care-and-the-rise-of-disinformation-in-public-health-emergencies.

در هر حال، وفق یافته‌های پژوهشی این مطالعه، آثار عملیاتی این دسته از جرایم که برای سیاست‌های خارجی و دیجیتالی دولت ها به‌دنبال دارد را می‌توان در ذیل ابراز داشت:

۱- غیرنظامیان به جرایم تروریستی در سکوهای دیجیتالی مانند جرم تروریستی جنبشی متعارف از نظر سیاسی پاسخ می‌دهند، اما تنها زمانی که جرایم تروریستی در سکوهای دیجیتالی به عواقب مرگبار منجر شود. به‌نظر می‌رسد تمایز کشنده/ غیرکشنده آستانه شروع تأثیرات سیاسی قوی باشد. از جرم تروریستی به‌عنوان مثال، حملات تروریستی غیرمرگبار دیجیتالی که زیرساخت‌های حیاتی، مانند ایستگاه‌های برق یا شبکه‌های مالی را هدف قرار می‌دهند، می‌توانند پیامدهای بسیار مخربی داشته باشند، اما برای برانگیختن درخواست‌های عمومی برای حملات تلافی‌جویانه به همان شیوه‌ای که یک حمله متعارف انجام می‌دهد، کافی نیستند.

۲- حملات تروریستی سایبری و متعارف از طریق سازوکار روانی مشابه، با خشم به‌عنوان یک متغیر مداخله‌گر عمل می‌کنند، البته اذعان می‌گردد جرایم تروریستی در سکوهای دیجیتالی واقعاً می‌تواند باعث حمایت عمومی قوی از اقدام نظامی تلافی‌جویانه شود، اما تنها زمانی که منجر به تلفات شود.

ملاحظات اخلاقی: ملاحظات اخلاقی مربوط به انجام پژوهش رعایت شده است.

تعارض منافع: تدوین این مقاله، فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان: نگارش مقاله منفرداً انجام گرفته است.

تشکر و قدردانی: از همه کسانی که در بازخوانی و ویرایش اثر همیاری و راهنمایی داشتند، قدردانی و تشکر می‌گردد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین مالی انجام گرفته است.

منابع و مآخذ

- Abed, S. F; A Sophie, A. I & Nahoko, S (2024). *Examining the Threat of Cyber-Attacks on Health Care During the COVID-19 Pandemic*. Weekly Epidemiological Record Press.

- Aaron, P; Cowen, D & Chris, D (2010). *Hacking Exposed Computer Forensics*. 2nd ed., McGraw-Hill.

- Computer Crime Investigation & Computer Forensic (1997). "Information Systems Security". 6(2): 25-56.

- Durham, H (2020). "Cyber operations During Armed Conflict: 7 Essential Law and Policy Questions". March 26, via: https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/?

- Nabat, A & Agarwal, S (2013). "Assessment of Types of Cyber Crime Faced by Elderly Across Residence". *The International Journal of Engineering and Science*, 2(6): 1-18.

- McDermott, R & Zimbardo, PG (2007). "The Psychological Consequences of Terrorist Alerts". in: Bongar, B; Brown, LM; Beutler, LE *et al*. (eds), *Psychology of Terrorism*, Oxford: Oxford University Press.

- Marelli, M (2020). "Hacking Humanitarians: Moving Towards a Humanitarian Cybersecurity Strategy". January 16, via: https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/

- Gross, ML; Canetti, D & Vashdi, DR (2016). "The Psychological Effects of Cyber Terrorism". *Bulletin of the Atomic Scientists*, 72: 284-291.

- Iftikhar, S (2024). "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures". *PeerJ Computer Science*, 10: 1-32.

- Gisel, L & Tilman, R (2019). "Cyber Operations and International Humanitarian Law: Five Key Points". November 28, via: https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/

- Wright, J (2018). "Attorney General of the UK, Address at Chatham House, Cyber and International Law in the 21st Century". Via: https://perma.cc/DWZ3-WNX9.

- Ruvic, D (2020). "U.S., UK Cyber Officials Say State-backed Hackers Taking Advantage of Outbreak". *Reuters*, via: https://perma.cc/RCU7-UPYR.

- Satter, R; Stubbs J & Bing, C (2020). "Elite Hackers Target WHO as Coronavirus Cyberattacks Spike". *Reuters*, via: https://perma.cc/D7NP-9THA.

- Saxena, R & Gayathri, E (2021). "Cyber Threat Intelligence Challenges: Leveraging Blockchain Intelligence with Possible Solution". *Mater Today*, 5(6): 81-83.

- Shandler, R; Michael L; Gross, S.B & Canetti, D (2022). "Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment". *British Journal of Political Science*, 52(2): 850 – 868.

- Shaweorcid, R & McAndrew, I. R (2023). "Cybersecurity and Domestic Terrorism: Purpose and Future". *Journal of Software Engineering and Applications*, 16(10): 548-560.