10.48315/QGL.2025.494372.1167

فصلنامه «دولت و حقوق»، سال پنجم، شماره چهارم (پیاپی ۱۸)، زمستان ۱۴۰۳، صص. ٤٦-۲۵

الزامات حقوقی جهانیِ حفاظت از امنیتِ زیرساخت‌های‌حیاتی کشورها در قبال جرایم تروریستی فناورانه

پیمان نمامیان*

نوع مقاله: علمی- پژوهشی

چکیده

رشد و قابلیت‌های فضای دیجیتالی، مزایای بسیاری را برای جوامع به همراه داشته است. افراد و کسب‌وکارها از فضای دیجیتالی برای ارتباط آسان بهره گرفته و دولت‌ها برای بهبود عملکرد زیرساخت‌های حیاتی خود از آن استفاده می‌کنند. زیرساخت‌های حیاتی، خدمات حیاتی نظیر سلامت، ایمنی و امنیت مورد نیاز برای عملکرد کارآمد جوامع را فراهم می‌کنند. با این حال، تهدیدها و آسیب‌پذیری‌های موجود در فضای دیجیتال، حمله‌های فناورانه نظیر جرایم تروریستی فناورانه را تسهیل بخشید و ضمن نقض امنیت زیرساخت‌های حیاتی کشورها، موجبات نگرانی جهانی را فراهم آورده است. از این‌رو، ارتکاب جرایم تروریستی فناورانه برای اِعمال تهدید یا ایجاد آسیب بدنی برای به دست آوردن قدرت سیاسی یا عقیدتی از طریق تهدید یا ارعاب است. سرقت داده‌ها، دستکاری داده‌ها و اختلال در خدمات ضروری، می‌توانند در این زمره قرار گیرند. با بحرانی شدن زیرساخت‌های حیاتی و کاهش موانع ورود برای عوامل مخرب، جرایم تروریستی فناورانه به یک نگرانی فزاینده تبدیل شده است. بر این اساس، در چارچوب اسناد جهانی، مقابله با جرایم تروریستی به‌رغم توصیف گونه‌های متعدد جرم تروریستی در برخی از زیرساخت‌های حیاتی، متأسفانه نبود قاعده‌ای الزامی در مقابله با چنین جرایمی، امکان ارتکاب آن را از سوی تروریست‌ها با توجه به تحولات و پیشرفت‌های فناورانه به‌سهولت فراهم کرده است. بنابراین مقالهٔ پیش رو درصدد است ضمن مطالعهٔ نحوهٔ تأمین امنیت زیرساخت‌های حیاتی در مقابله با جرایم تروریستی فناورانه، حفاظت از تهدیدپذیری و آسیب‌پذیری آن‌ها را مورد سنجش قرار دهد.

واژگان کلیدی

فضای دیجیتالی، جرایم تروریستی فناورانه، تهدیدها و آسیب‌ها، امنیت زیرساخت‌های حیاتی، کنوانسیون‌های ضد تروریسم.

---

* دانشیار حقوق کیفری و جرم‌شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران.
p_namamian1512@yahoo.com

تاریخ دریافت: ۱۴۰۳/۰۴/۱۳ تاریخ پذیرش: ۱۴۰۳/۱۰/۰۴

مقدمه

جرایم تروریستی چهره‌های زیادی دارد که آخرین آن‌ها، ارتکاب این نوع از جرایم با استفاده از فناوری‌های نوین است و در این رابطه مدت‌هاست مقامات امنیتی دولت‌ها درخصوص تهدید پیش‌بینی شده ناشی از «جرایم تروریستی فناورانه»[1] هشدارهایی داده‌اند. بنابراین در چارچوب گزارش اعلامی از سوی برخی از گروه کارشناسان ابراز شده است بهره‌گیری از فناوری اطلاعات و ارتباطات برای مقاصد تروریستی، فراتر از استخدام، تأمین مالی، آموزش و تحریک، به‌ویژه برای ارتکاب جرایم تروریستی علیه فناوری اطلاعات و ارتباطات یا زیرساخت‌های وابسته به فناوری اطلاعات و ارتباطات است که در صورت بی‌توجهی به آن، ممکن است به‌نحو فزاینده‌ای صلح و امنیت بین‌المللی را تهدید کند.[2] در سال‌های اخیر، به‌دنبال انبوهی از گزارش‌ها راجع‌به حملات تروریستی فناورانه که به تخریب فیزیکی در دنیای واقعی منجر می‌شوند، مخابره شده است؛ برای نمونه، در سال ۲۰۲۰ بر اثر حملهٔ تروریستی فناورانه به یک بیمارستان در آلمان یک بیمار فوت شد، با وجود اینکه امکان انتقال وی به بیمارستان دیگری فراهم بود.[3]

ممکن است پیشرفت‌های فناورانه نظیر هوش مصنوعی، فناوری زیستی و اینترنت اشیا فرصت‌هایی را برای تروریست‌ها فراهم کند تا با توسعهٔ روش‌های تهاجمی نوین و از راه دور، حملاتی را انجام دهند.[4] این در حالی است که تروریست‌ها به‌طور سنتی فعالیت‌های خود را به مناطق محلی خود محدود می‌کنند و مردم سرزمین خود را هدف قرار می‌دهند، اما به‌علت انفجار فناوری‌های ارتباطی و اطلاعاتی که برای جابه‌جایی کالاها و سرمایه‌های مالی استفاده شده است، تروریست‌ها این امکان را دارند تا افق‌های خود را به‌طور قابل توجهی توسعه دهند.

فناوری برای تروریست‌ها، هم در ابزارهای ترور مانند سلاح‌های کشتارجمعی و بهره‌گیری از اینترنت و هم در اهداف ترور، مانند اهداف زیرساختی فناوری دخالت دارد. فناوری از طریق سامانه‌های شناسایی هوشمند، فناوری‌های پیچیده برای جمع‌آوری و سنجش اطلاعات و

---

1. Technological Terrorist Crimes
2. See https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/227/92/PDF/N1522792.pdf?OpenElement.
3. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

۴. تروریست‌ها ضمن اعتقاد به فناوری‌های نوین، سابقهٔ تاریخی در پذیرش آن‌ها دارند و مورد بهره‌گیری تروریستی قرار می‌دهند؛ به‌تازگی گروه‌های تروریستی در حال استفاده از هواپیماهای بدون سرنشین و فناوری هوش مصنوعی هستند. بنابراین ضرورت تعمیق ادراک از نحوهٔ استفادهٔ تروریست‌ها از پیشرفت‌های فناورانه برای افزایش قدرت خود در حوزه‌های فیزیکی و روانی، امری انکارناپذیر است (Schori Liang, 2023: 1).

بهره‌گیری از اینترنت به‌عنوان کانال ارتباطی برای کاهش تنش‌هایی که می‌تواند به ارتکاب جرایم تروریستی منجر شود، این امکان را دارند تا به‌مثابه ابزار حیاتی در مبارزه با جرایم تروریستی فناورانه باشند.

نه‌تنها در سال‌های اخیر، بلکه در سال‌های آینده، ممکن است توسعهٔ فناوری‌های نوظهور[۱] و مخرب[۲] قابلیت‌های تروریست‌ها را متحول کند و تحقیقات و پاسخ به حملات را پیچیده سازد. همچنین ممکن است تروریست‌ها از فناوری‌های نوظهور استفاده کنند تا ضمن جذب نیرو برای ارتکاب گسترده افراط‌گرایی و رفتارهای خشونت‌آمیز، امکان برنامه‌ریزی و آموزش را افزایش دهد، البته از روش‌های نوین حمله از راه دور نیز بهره می‌گیرد.[۳]

اگرچه برخی از تروریست‌ها هنوز از روش‌های کم‌فناوری حمایت می‌کنند، اما گسترش فناوری‌های نسبتاً ارزان و در دسترس تجاری، به احتمال زیاد بسیاری از تروریست‌ها را قادر می‌کند تا رویکردهای پیچیده و مؤثری را برای تبلیغات، استخدام، مالی، کسب‌وکار، ارتباطات و حملات تروریستی فناورانه اتخاذ کنند. البته گزارش موجود در سند *روندهای جهانی شورای اطلاعات ملی ایالات متحده ۲۰۴۰* که در مارس ۲۰۲۱ منتشر شد، آمده است که اکثر حملات تروریستی در بیست سال آینده احتمالاً به استفاده از سلاح‌هایی شبیه آنچه در حال حاضر در دسترس هستند مانند سلاح‌های کوچک و مواد منفجرهٔ دست‌ساز، ادامه خواهند یافت؛ زیرا این سلاح‌ها معمولاً کافی، در دسترس و قابل اعتماد هستند.[۴] به‌علاوه در سند مزبور مقرر شده است، تروریست‌ها به‌دنبال سلاح‌های کشتارجمعی و سلاح‌های دیگر و رویکردهایی خواهند بود که به آن‌ها امکان ارتکاب حملات تروریستی فناورانه با وسعت بسیار زیاد را می‌دهند. برای نمونه، داعش ضمن استفاده از گاز خردل در ارتکاب حملات، از هواپیماهای بدون سرنشین به‌نحو گسترده بهره برده است.

باوجود اینکه مقابله و سرکوب ارتکاب جرایم تروریستی فناورانه علیه زیرساخت‌های حیاتی،

---

۱. «فناوری‌های نوظهور» به فناوری‌های نوآورانه‌ای اطلاق می‌شوند که به‌تازگی توسعه یافته، در حال توسعه یا احتمالاً در چند سال آینده توسعه خواهند یافت.

۲. «فناوری‌های مخرب» به فناوری‌های نوآورانه‌ای گفته می‌شوند که نحوهٔ عملکرد سازمان‌ها و صنایع را به‌شدت تغییر می‌دهند.

3. https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/134s_-_First_Responders_Toolbox_-_Emerging_Technologies_May_Heighten_Terrorist_Threats.pdf

4. The US National Intelligence Council's Global Trends 2040, The Strategic Futures Group National Intelligence Council, March 2021, https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf

در قلمرو حاکمیتی هر کشور در ساختار حاکمیت حقوقی جهانی قابل ملاحظه است، اما باید اذعان داشت که عدم اقتدار و نقص در استحکام حقوقی اسناد بین‌المللی، الزامات جرم‌انگاری این دسته از جرایم ارتکابی به‌واسطهٔ همکاری میان دولت‌ها قابلیت اصلاح و جبران را خواهد داشت. این در حالی است که نبود یک چارچوب حقوقی جهانی در جرم‌انگاری و الزامات حاکم بر آن در پاسخ‌گذاری به جرایم تروریستی فناورانه علیه زیرساخت‌های حیاتی، به‌عنوان مسئلهٔ مورد اهتمام جهانی قابل ملاحظه است. با مطالعهٔ اسناد حقوقی جهانی و تدقیق در مفاد و موازین قابل اجرا راجع‌به جرایم تروریستی فناورانه که امکان نقض امنیت سامانه‌ها و تأسیسات را در زیرساخت‌های حیاتی فراهم می‌آورند، به‌وضوح موانع و خلأهای حقوقی جهانی در زمینهٔ عدم تعهد حقوقی دولت‌ها و بازیگران غیردولتی غیرقانونی به‌ویژه گروه‌های تروریستی از امکان احراز و انتساب مسئولیت کیفری بین‌المللی به آن‌ها قابل ملاحظه است.

این مقاله با اهدافی مشتمل بر «شناسایی و تحلیل انواع تهدیدات تروریستی فناورانه علیه زیرساخت‌های حیاتی»، «شناخت تهدیدهای موجود و درک بهتر نحوه اجرای حمله‌های تروریستی علیه زیرساخت‌های حیاتی با استفاده از فناوری‌های نوین»، «توسعه راهکارهایی برای تقویت آمادگی و پاسخگویی به جرایم تروریستی فناورانه در زیرساخت‌های حیاتی» و «حفاظت از امنیت زیرساخت‌های حیاتی با ارائه سازوکارهای برای ارتقای هماهنگی بین‌المللی با سنجش نحوه ارتقای همکاری‌های بین‌المللی، تبادل اطلاعات و ایجاد توافق‌نامه‌های بین‌المللی»، درصدد پاسخ به پرسش‌هایی نظیر «آیا تهدیدهای فناورانه‌ای از سوی گروه‌های تروریستی می‌تواند زیرساخت‌های حیاتی را هدف قرار دهد؟» و «چه نقش‌هایی در سطح بین‌المللی باید برای مقابله با جرایم تروریستی فناورانه ایفا شود؟» خواهد بود.

از این‌رو، در این رهگذر، با بهره‌گیری از روش پژوهش توصیفی-تحلیلی و استفادهٔ اسنادی از منابع کتابخانه‌ای ضرورت پاسخ به این پرسش اصلی و اساسی که عبارت است از «آیا الزامات حقوقی جهانی امکان محافظت از زیرساخت‌های حیاتی کشورها در مواجهه با جرایم تروریستی فناورانه را دارند؟»، امری قابل اتکا برای شناسایی رویکردهای حقوقی متخذه در نظام جهانی در این زمینه است؛ هر چند به‌نظر می‌رسد که الزامات جرم‌انگاری‌ها در چارچوب‌های حقوقی جهانی مؤید فقدان مقابلهٔ حداکثری با ارتکاب جرایم تروریستی فناورانه در نقض امنیت زیرساخت‌های حیاتی در قلمرو هر کشور باشد.

۱. مفاهیم و دیدگاه‌ها

در دنیای امروز که کشورها به طور فزاینده‌ای به فناوری‌های دیجیتال و اطلاعات وابسته هستند،

تهدیدهای فناورانه و جرایم تروریستی فناورانه به یک چالش بزرگ تبدیل شده‌اند. این تهدیدها، به‌ویژه حمله‌های فناورانه، می‌توانند به طور مستقیم به زیرساخت‌های حیاتی یک کشور آسیب برسانند و در برخی موارد، حتی می‌توانند موجب نابودی یا اختلالات وسیع در سامانه‌های اقتصادی، اجتماعی و سیاسی کشورها شوند. در این راستا، همکاری‌های بین‌المللی نقش حیاتی دارد. به دلیل آن که تهدیدهای فناورانه مرزهای ملی را در می‌نوردند، نیاز به هم‌افزایی و تبادل اطلاعات بین کشورها برای مقابله با این تهدیدات وجود دارد. همچنین، تدوین استانداردهای امنیتی بین‌المللی و ایجاد چارچوب‌های قانونی منسجم برای حفاظت از زیرساخت‌ها امری ضروری است.

۱-۱. زیرساخت‌های حیاتی

با توجه به نبود دستوری خاص در چارچوب اسناد بین‌المللی، هیچ تعریف جهانی نسبت به «زیرساخت‌های حیاتی» وجود ندارد؛ در مقابل، دولت‌ها به‌طور ذهنی دارایی‌ها، سامانه‌ها یا قابلیت‌هایی را تعیین می‌کنند که برای امنیت ملی آن‌ها حیاتی است. برای نمونه، در ایالات متحدهٔ امریکا، زیرساخت‌های حیاتی به این صورت تعریف می‌شود: «سامانه‌ها و دارایی‌ها، اعم از فیزیکی یا مجازی، به‌حدی برای ایالات متحده حیاتی هستند که ناتوانی یا نابودی چنین سامانه‌ها و دارایی‌هایی تأثیر مخربی بر امنیت، امنیت اقتصاد ملی، سلامت یا ایمنی عمومی ملی یا هر ترکیبی از این موارد خواهد داشت.»[۱] در این رابطه می‌توان به «قانون حفاظت از زیرساخت‌های حیاتی ۲۰۰۱»[۲] اشاره داشت که مقرر می‌دارد: «هرگونه اختلال فیزیکی یا مجازی در عملکرد زیرساخت‌های حیاتی منحصربه‌فرد، مختصر، از نظر جغرافیایی محدود، قابل مدیریت و حداقل برای اقتصاد، خدمات انسانی و دولتی و امنیت ملی ایالات متحده مضر باشد.»[۳] این در حالی است

1. Migration and Home Affairs: Critical Infrastructure, EUR. COMM'N, https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/criticalinfrastructure_en (last visited Dec. 26, 2019) [https://perma.cc/LF9P-DUEZ].

2. Critical Infrastructures Protection Act of 2001, https://www.congress.gov/bill/107th-congress/senate-bill/1407

۳. برای نمونه وزارت امنیت داخلی ایالات متحدهٔ امریکا در حال حاضر شانزده بخش از زیرساخت‌های حیاتی مشتمل بر شیمیایی، تأسیسات تجاری، ارتباطات، تولیدات حیاتی، سدها، پایگاه صنعتی دفاعی، خدمات اضطراری، انرژی، خدمات مالی، غذا و کشاورزی، تأسیسات دولتی، بهداشت‌ودرمان و بهداشت عمومی، فناوری اطلاعات، هسته‌ای، حمل‌ونقل و سامانه‌ها و تأسیسات آب و فاضلاب را شناسایی کرده است؛

- Critical Infrastructure Sectors, U.S. Department of Homeland Security., Supra note 28, https://www.dhs.gov/critical-infrastructure-sectors

که «قانون میهن‌پرستی ایالات متحدهٔ امریکا، مصوب ۲۰۰۱» در رابطه با توصیف زیرساخت‌های حیاتی اشعار می‌دارد «سامانه‌ها و دارایی‌ها، اعم از فیزیکی یا مجازی، برای ایالات متحده آنقدر حیاتی هستند که ناتوانی یا نابودی آن‌ها تأثیر تضعیف‌کننده‌ای بر امنیت، اعم از اقتصاد ملی، سلامت یا ایمنی عمومی ملی یا هر ترکیبی از این موارد را خواهد داشت.»[1] گفتنی است ایالات متحدهٔ امریکا به‌عنوان نخسین دولت در توسعه و ایجاد طرح‌ها و ابتکارات حفاظت از زیرساخت‌های حیاتی، در سال ۱۹۹۸ به انتشار اولین راهبرد در زمینهٔ وفق فرمان اجرایی شمارهٔ ۶۳ سیاست‌های راهبردی ریاست‌جمهوری مبادرت ورزید.[2] این در حالی است که مطابق سند شمارهٔ ۲۱، سیاست راهبردی با هدف تقویت و تاب‌آوری زیرساخت‌های حیاتی در قبال تهدیدهای فیزیکی و فناورانه طی سال ۲۰۱۳ را وضع کرد.[3]

به‌طور کلی، زیرساخت‌های حیاتی به مجموعه ارکان ساختاری درهم‌تنیده‌ای اطلاق می‌شود که یک سامانهٔ وسیع همراه با ابعاد فناوری گسترده و ابعاد فیزیکی غیرعامل حرکت را تشکیل می‌دهد. بنابراین زیرساخت‌های حیاتی مجموعه‌ای از دارایی‌های مهم یک کشور مشتمل بر جمعیت، منابع انرژی(اعم از منابع و تأسیسات آب، برق، گاز، مخابرات و هسته‌ای)، منابع مالی و پولی، منابع ارتباطی و اطلاعاتی، منابع خدماتی و تجاری، پایگاه‌ها و تأسیسات نظامی، اموال و تأسیسات عمومی و دولتی و خصوصی است.

البته «حفاظت از زیرساخت‌های حیاتی» به مجموعه اقدام‌هایی گفته می‌شود که «برای حفاظت زیرساخت‌ها که در هر کشوری بنیان اساسی جامعهٔ آن کشور محسوب می‌شوند و آسیب به آن‌ها

گفتنی است پس از وقوع حملات تروریستی ۱۱ سپتامبر ۲۰۰۱، ایالات متحدهٔ امریکا به‌شدت از چنین حملاتی علیه زیرساخت‌های حیاتی خود آگاه شد. در فوریهٔ ۲۰۰۳، دولت وقت «راهبرد ملی حفاظت فیزیکی از زیرساخت‌های حیاتی و دارایی‌های اساسی» را برای کاهش هزینه‌های ناشی از آسیب‌پذیری در قبال جرایم تروریستی در امریکا منتشر کرد؛

- U.S. Department of Homeland Security, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003), https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf [https://perma.cc/G62A-MY6W].

1. Public Law 107 - 56 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, https://www.govinfo.gov/app/details/PLAW-107publ56

2. White House, "Presidential Decision Directive 63: Protecting America's Critical Infrastructures," Washington, DC, USA, 1998. [Online]. Available: http://www.fas.org/irp/offdocs/pdd-63.htm.

3. White House, "Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience, Washington, DC, USA, 2013. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resi

می‌تواند پیامدهای جبران‌ناپذیری را در کشورها ایجاد کند و آسیب در یک بخش می‌تواند بخش‌های دیگر را نیز تحت تأثیر جدی قرار دهد» (میریوسفی و همکاران، ۱۳۹۹: ۸-۷).

در ایران وفق بند هفتم از مادهٔ نخست «طرح راهبـردی حفاظت از زیرسـاخت‌های کشور، مصوب ۱۴۰۲»[۱]، حفاظت از زیرساخت به مجموعه تدابیر و اقدامات پدافند غیرعاملی توصیف شده است که توانایی و آمادگی عملیاتی زیرساخت و تداوم کارکردهای آن و دستگاه‌های اجرایی مسئول برای پاسخ مؤثر به حوادث و سوانح ناشی از تهدیدهای نظامی، تهدیدهای امنیتی و تروریستی، تهدیدهای سایبری زیرساختی و تهدیدهای از درون دشمن پایه را افزایش می‌دهد، به‌طوری که فعالیت آن حفظ می‌شود و خسارات انسانی و مادی ناشی از آن را به حداقل می‌رساند. افزون بر این، وفق بند (ب-۱) از مادهٔ نخست «نظام فنی و تخصصی حفاظت از زیرساخت‌های کشور، مصوب ۱۴۰۲» حفاظت از زیرساخت به مجموعه تدابیر و اقدامات پدافند غیرعاملی اطلاق می‌شود که توانایی و آمادگی عملیاتی زیرساخت و تداوم کارکرد آن و دستگاه‌های اجرایی مسئول برای پاسخ مؤثر به حوادث و سوانح ناشی از تهدیدات نظامی، امنیتی و تروریستی، سایبری زیرساختی و تهدیدات از درون دشمن پایه را افزایش می‌دهد، به‌طوری‌که فعّالیت آن حفظ می‌شود و خسارات انسانی و مادی ناشی از آن را به حداقل می‌رساند. البته می‌توان اظهار داشت در راستای مقابله با جرایم تروریستی فناورانه علیه زیرساخت‌های حیاتی، «طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری» به‌عنوان یک برنامهٔ جامع برای حفاظت از زیرساخت‌های حساس کشور در برابر تهدیدهای فناورانه توسط مرکز مدیریت راهبردی امنیت فضای تولید و تبادل اطلاعات ریاست‌جمهوری ایران تدوین و در سال ۱۳۹۸ به کلیهٔ سازمان‌ها و دستگاه‌های اجرایی دارای زیرساخت‌های حیاتی کشور ابلاغ شده است.[۲] در چارچوب این طرح، سازمان‌ها تشویق می‌شوند تا تهدیدها و آسیب‌پذیری‌های خود را شناسایی کنند و با اتخاذ اقدامات مناسب، احتمال وقوع حوادث و حمله‌های فناورانه را به حداقل برسانند. وفق طرح مزبور، توجه ویژه‌ای به مدل بلوغ امن‌سازی شده است که به سازمان‌ها امکان می‌دهد سطح آمادگی خود را در قبال تهدیدهای فناورانه بسنجند و براساس آن، برای ارتقای این آمادگی برنامه‌ریزی کنند. البته می‌توان به اسناد دیگری مانند «سیاست‌های کلی نظام در امور»، «امنیت فضای تولید و تبادل اطلاعات و ارتباطات(افتا)، ابلاغی ۱۳۸۹»، «سند راهبردی پدافند سایبری کشور، مصوب ۱۳۹۴»، «آیین‌نامهٔ اجرایی قانون تعیین حریم حفاظتی-امنیتی اماکن و تأسیسات کشور، مصوب ۱۳۹۷» و

۱. طرح راهبـردی حفاظت از زیرسـاخت‌های کشور مشتمل بر بیست مـادّه و سه تبصره که در تاریخ ۱۴۰۲/۰۶/۲۸ در هفتادوهفتمین جلسهٔ کارگروه (کمیته) دائمی پدافند غیرعامل کشور، به تصویب رسید.

2. https://amnafzar-rayka.ir/.pdf

«سند راهبردی جمهوری اسلامی ایران در فضای مجازی، مصوب ۱۴۰۱» اشاره داشت که امکان مقابله با آماج‌های ناشی از جرایم تروریستی فناورانه علیه امنیت زیرساخت‌های حیاتی کشور را فراهم می‌کند (ر.ک: نظری‌نژاد و همکاران، ۱۳۹۹: ۲۹۶؛ تقی‌پور و همکاران، ۱۳۹۸: ۲۱-۱۷).

۱-۲. جرایم تروریستی فناورانه

مفهوم جرایم تروریستی مبتنی فناوری‌های نوین یا به‌تعبیری جرایم تروریستی فناورانه، برای تثبیت در یک تعریف خاص بسیار پیچیده است. یکی از صاحب‌نظران در این ارتباط ضمن اشاره به پیشرفت‌های فناورانه و دشواری تعریف دقیق از این نوع جرم، تأکید دارد یک تعریف باید شامل دانش یا استفاده از جرم رایانه‌ای باشد (Ajetunmobi, 2015: 171). بنابراین جرایم تروریستی فناورانه به‌عنوان یک تهدید فراملی از مرزها و قلمروهای حاکمیتی دولت‌ها عبور می‌کند و موجب می‌شود تا بحرانی‌ترین چالش‌های جامعهٔ اطلاعاتی، امنیت داده‌های دیجیتالی و سیستم‌های اطلاعاتی و پیشگیری از بهره‌گیری مخرب و غیرقانونی از فناوری‌های ارتباطات اطلاعاتی توسط مجرمان فناورانه، گروه‌های تروریستی یا بازیگران دولتی ایجاد کند (Awwad Alkharman and Hassan, 2023, 17-18).

جرایم تروریستی فناورانه به اقداماتی اطلاق می‌شود که از فناوری‌های مدرن، به‌ویژه فناوری اطلاعات و ارتباطات، برای ارتکاب جرایم با اهداف تروریستی استفاده می‌شود. این نوع جرایم معمولاً شامل حمله‌های فناورانه به زیرساخت‌های حیاتی، سوءاستفاده از شبکه‌های اجتماعی برای تبلیغ تروریسم، و استفاده از فناوری‌های نوین مانند پهپادها، هوش مصنوعی و رمزارزها برای اجرای اهداف تروریستی است. این جرایم نه تنها امنیت ملی را تهدید می‌کنند، بلکه موجب ایجاد ترس و بی‌ثباتی در جوامع می‌شوند و به‌طور عمده از ابزارهای دیجیتال برای اعمال فشار سیاسی، اقتصادی یا اجتماعی استفاده می‌کنند (Schmid, 2019: 134-136).

استفادهٔ تروریستی از فناوری‌های نوین، چالش‌های مهمی را برای دولت‌ها در مقابله با جرایم تروریستی ایجاد می‌کند. استفادهٔ تروریست‌ها از فناوری‌های نوین، امکان ناشناس ماندن و توانایی هماهنگی و عملیات از راه دور، و در عین حال، این نوع از فناوری‌ها فرصت‌های قابل‌توجهی را به‌عنوان قابلیت مقابله با جرایم تروریستی فراهم می‌کند. بنابراین مقابله با بهره‌گیری تروریست‌ها از فناوری‌های نوین به درک نحوهٔ استفادهٔ آن‌ها از این نوع فناوری‌ها، توسعهٔ چارچوب قانونی مؤثر و پاسخ‌های سیاستی، و ایجاد ظرفیت عملیاتی برای مقابله با استفادهٔ تروریستی از این فناوری‌ها بستگی دارد.

به این ترتیب تأکید می‌شود جرایم تروریستی فناورانه به آن دسته از جرایمی اطلاق می‌شوند

که «تروریست‌ها با بهره‌گیری از علوم و فناوری‌های نوین در سکوهای مجازی مرتکب می‌شوند که البته غایت آماج‌های تروریست‌ها بیشتر حول محور زیرساخت‌های حیاتی مستقر در قلمرو حاکمیتی کشورهاست.»

۲. تهدیدها و آسیب‌ها

بینش‌ها در ادوار گذشته، مبتنی بر وجود تهدیدها و آسیب‌های اولیه علیه زیرساخت‌های حیاتی در هر کشور ناشی از حوادث و بلایای طبیعی بود، اما امروزه، زیرساخت‌های حیاتی با طیف وسیعی از تهدیدهای نوین مواجه هستند که در این رابطه می‌توان مخاطره‌های ناشی از جرایم تروریستی فناورانه و حتی اقدام‌های دیگر اعم از سیاسی و نظامی را در کانون توجه قرار داد[۱]؛ البته می‌توان تهدیدها و آسیب‌های موجود در نقض امنیت زیرساخت‌های حیاتی را مشتمل بر خطر ژئوپلیتیکی، تهدیدهای فناورانه، بلایای طبیعی و حتی دارایی‌های قدیمی دانست.[۲] البته باید تأکید داشت که در راستای تهدیدها و آسیب‌هایی که به‌واسطهٔ ارتکاب جرایم تروریستی فناورانه علیه زیرساخت‌های حیاتی امکان بروز و ظهور دارند[۳] می‌توان به تقسیم‌بندی شبکه[۴]، حملهٔ انکار سرویس[۵]، حمله‌های برنامه‌های وب[۶]، حمله‌های بدافزار[۷] و فرمان تزریق و دستکاری پارامترها[۸] اشاره داشت (Iaremenko, 2023: 1).

توسعهٔ فناوری اطلاعات و فضای دیجیتالی موجب شده است تا بخش‌های مهمی از کارکرد زیرساخت‌های حیاتی و حساس، به این فضا وابسته شوند. در نتیجهٔ چنین وابستگی‌ای، امنیت زیرساخت‌ها به فضای دیجیتالی گره خورده است(کافی، ۱۳۹۹: ۷۵-۷۴). البته توسعهٔ زیرساخت‌های

---

۱. بردارهای تهدید زیرساخت‌های حیاتی ابزاری هستند که توسط آن یک بازیگر زیرساخت‌های حیاتی را (یا آسیب‌پذیری‌های مرتبط با سن ذاتی در زیرساخت‌های حیاتی که احتمال اختلال یا وقفه در بخش را افزایش می‌دهد) مورد هدف قرار می‌دهد، مانند شناسایی اهداف و عوامل مخرب. زیرساخت شامل سامانه‌ها، دارایی‌ها (اعم از فیزیکی یا مجازی) و بخش‌های جزء مانند افراد، ساختارها، امکانات، اطلاعات، مواد و فرآیندها می‌شود. این چشم‌انداز قابل توجهی از اهداف حساس را نشان می‌دهد که در برابر انواع تهدیدها آسیب‌پذیر هستند که از سوی مدافعان و دشمنان قابل بررسی است. در صورت حمله، ممکن است اهداف بر اساس اهداف اصلی عامل تهدید، آسیب‌پذیری و دسترسی به هدف، و ابزارها و قابلیت‌های مهاجم انتخاب شوند؛

- https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2300/RRA2397-2/RAND_RRA2397-2.pdf

2. https://www.ajg.com/news-and-insights/features/four-threats-to-critical-infrastructure/
3. https://www.anapaya.net/blog/top-5-critical-infrastructure-cyberattacks
4. Network Segmentation
5. Denial-of-service attack
6. Web Application Attacks
7. Malware Attacks
8. Command Injection and Parameters Manipulation

ارتباطی و اتصال شبکه‌های ناهمگون با گسترش هم‌زمان سرویس‌ها و خدمات مفید و متنوع در سطوح سازمانی، بخشی و ملی در کنار ساختار نامتعارف و درهم‌تنیدهٔ آن‌ها به رشد آسیب‌پذیری‌ها و تهدیدهای امنیتی در فضای دیجیتال منجر شده است. تهدیدهای فناورانه با اثرگذاری در سطح ملی علیه برخی از این زیرساخت‌ها به‌عنوان زیرساخت‌های حیاتی، هزینه‌های زیاد و گاه غیرقابل جبرانی را به سازمان‌ها، جوامع و کشورها تحمیل می‌کند(آقایی و همکاران، ۱۳۹۸: ۲۰۲-۲۰۱).

با افزایش سریع مقیاس، پیچیدگی و تأثیر و امکان ارتکاب جرایم تروریستی فناورانه، سامانه‌های حیاتی و داده‌های حساس در معرض خطر قرار می‌گیرند، بنابراین درحالی‌که تحول دیجیتالی از طریق اینترنت اشیا و سامانه‌های کنترل صنعتی موجب افزایش کارایی می‌شود، سطح آماج‌ها را نیز گسترش می‌دهد. از این‌رو، از آنجاکه تهدیدهای فناورانه از وابستگی فزایندهٔ زیرساخت‌های حیاتی به اتصال و دادهٔ دیجیتالی سوءاستفاده می‌کنند، سنجش خطر فعال و تلاش‌های امنیتی در این رابطه ضرورت دارد تا امکان برآورد مخرج‌های احتمالی آینده علیه زیرساخت‌های حیاتی ارزیابی شود.

با این حال، فرکانس فزاینده و تأثیر حمله‌های تروریستی مبتنی بر بهره‌گیری از علوم فناورانه علیه زیرساخت‌های حیاتی، تهدید بزرگی برای امنیت ملی است. از سال ۲۰۱۰، این دسته از حملات گزارش شده چهار برابر شده است و برخی از کارشناسان پیش‌بینی کرده‌اند که هزینه‌های این جرایم تا سال ۲۰۲۵ به بیش از ۱۰ تریلیون دلار خواهد رسید که افزایش قابل توجهی از سه تریلیون دلار در سال ۲۰۱۵ است.[1] این در حالی است که متأسفانه تجاری‌سازی فزایندهٔ هک نیز به حمله‌های مزبور دامن زده است، به‌طوری‌که درآمد جرایم ارتکابی در سال ۲۰۲۰ به ۱٫۵ تریلیون دلار رسیده است. برای مقابله با چنین شرایطی، دولت‌ها دفاع فناورانه را به‌عنوان یک اولویت ملی مطرح و دستورات امنیتی زیرساخت‌های حیاتی را در بخش‌های گوناگون روزآمد کرده‌اند، بنابراین از آنجاکه سامانه‌های دیجیتال زیرساخت‌های حیاتی ممکن است از سوی تروریست‌ها تهدید شوند، مدیریت خطر فعال و همکاری برای تقویت انعطاف‌پذیری آن در این دسته از زیرساخت‌ها امری ضروری است (A.Shaji, T.Baskar, Srikaanth, 2024: 274-275).

نکتهٔ مهم این است که بیشتر دارایی‌ها یا خدمات ضروری برای یک جامعه به هم مرتبط هستند، بنابراین آسیب، تخریب یا اختلال در یک سامانه، به‌طور طبیعی پیامدهای منفی قابل توجهی در سایر سامانه‌های مهم لازم برای عملکرد یک دولت پیشرفته خواهد داشت. با شناخت این خطر پیوستگی، کشورها به‌طور فزاینده‌ای گسترهٔ بسیاری از دارایی‌ها، سامانه‌ها یا قابلیت‌ها را

1. https://www.business-standard.com/finance/personal-finance/cybercrime-costs-to-hit-10-5-trn-by-2025-how-insurance-may-save-your-biz-124072400476_1.html

به‌عنوان زیرساخت‌های حیاتی توصیف می‌کنند. از این‌رو، با چنین رویکردی، دولت‌ها تلاش می‌کنند نه‌تنها از یک دارایی یا خدمات خاص، بلکه از کل قلمرو جغرافیایی(حاکمیتی) که زیربنای امنیت ملی به‌شمار می‌روند، در قبال تهدیدها و چالش‌های امنیتی ناشی از ارتکاب جرایم تروریستی فناورانه محافظت کنند(Schmitt, 2014: 278). بنابراین آنچه موجب می‌شود تا به‌طور فزاینده و بالقوه برای تروریست‌ها امکان ارتکاب جرایم تروریستی فناورانه را در کشورهای پیشرفته جذابیت ایجاد کنند، وجود زیرساخت‌های حیاتی راهبردی همراه با آسیب‌پذیری‌های متعدد موجود در این دارایی‌ها و سامانه‌هاست.[۱]

به این ترتیب عوامل تهدید زیرساخت‌های حیاتی بسیار متنوع هستند و مشتمل بر بازیگران دولتی با قابلیت‌های فناورانهٔ پیشرفته، سازمان‌های جنایی غیردولتی، اغلب با انگیزه‌های مالی و تروریست‌های داخلی یا سایر گروه‌های افراطی می‌شوند. البته عوامل تهدید، جرایم تروریستی فناورانه را به دلایل گوناگونی (نظیر کسب درآمد، جاسوسی یا سرقت اطلاعات، خرابکاری یا مختل کردن هدف، از بین بردن داده‌ها، آزمایش ابزارهای فناورانه یا هدف‌گیری مواضع آسیب‌پذیر و حتی جلب توجه به یک علت یا برای به دست آوردن اهرم فشار در یک موضوع نامربوط) مرتکب می‌شوند.[۲] در ضمن باید اذعان داشت چالش‌های رایج، مانع از پیشگیری و واکنش مؤثر ذی‌نفعان به اختلالات در بخش‌های زیرساختی حیاتی می‌شود؛ برخی از این چالش‌ها نبود سرمایه‌گذاری کافی در زیرساخت‌ها، تعدد ذی‌نفعان، نبود ارتباطات، نبود برنامه‌ریزی و شناسایی و گزارش نادرست تهدیدهای فناورانه است.[۳]

ممکن است تهدیدهای فیزیکی برای زیرساخت‌های حیاتی اشکال گوناگونی داشته باشد. ویژگی مشترک آن‌ها این است که هدفشان از بین بردن زیرساخت، تضعیف یا غیرفعال کردن آن به‌طور کامل یا جزئی از طریق به مخاطره انداختن ساختار فیزیکی، اجزای مکانیکی و ویژگی‌های دیگر آن است.[۴] اگرچه ماهیت تهدیدهای ناشی از ارتکاب جرایم تروریستی فناورانه با تهدیدهای

---

۱. در عصر فناوری‌های امروز، به‌طور فزاینده‌ای غیرقابل تصور است که مقررات موجود در چارچوب جرایم تروریستی فناورانه که به اقدام‌های فناورانه که هنوز در مراحل اولیهٔ فناوری نسبی خود هستند پاسخ می‌دهد، دست‌نخورده باقی بماند. این امر به‌ویژه در شرایطی قابل استناد است که اقدام‌های فناورانه هرچه بیشتر برای عملکرد جوامع مدرن قابلیت سازگاری داشته باشند(Schmitt & Vihul, 2017: 1).

2. https://learn.assetlifecycle.trimble.com/blog/5-cyber-attacks-that-threaten-critical-infrastructure-and-how-to-protect-against-them

3. https://www.gao.gov/products/gao-23-106441

4. McAfee, "In the dark: critical industries confront cyberattack. McAfee's Second Annual Report on Critical Infrastructure", 18 July 2011, p. 6. Available at https://www. publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-gw-en.aspx.

فیزیکی ناشی از جرایم تروریستی متفاوت است، اما ممکن است نتیجهٔ نهایی یکسان باشد، بنابراین ممکن است تهدیدها علیه زیرساخت‌های حیاتی به‌صورت اقدام‌های منفرد و پراکنده صورت پذیرد یا بخشی از یک طرح گسترده برای حمله به زیرساخت‌ها در همان بخش (نظیر انرژی، حمل‌ونقل، مخابرات)، در یک منطقهٔ جغرافیایی باشد؛ البته ممکن است اقدام‌ها با انگیزهٔ تروریستی که زیرساخت‌های حیاتی را هدف قرار می‌دهند مانند موارد جاسوسی صنعتی درک شوند که در آن، حمله‌های مبتنی بر بهره‌گیری از طریق پیشرفت‌های فناورانه، اغلب به‌عنوان حمله‌های گسترده ارتکاب یابند.

تروریست‌ها به دلایلی مانند گسترهٔ اثرگذاری بر هدف و میزان آسیب‌پذیری زیرساخت‌های حیاتی، به ارتکاب جرایم تروریستی فناورانه مبادرت می‌ورزند(نعمت‌پور و همکاران، ۱۴۰۰: ۱۷۳-۱۷۱).[۱] از این‌رو، وجود نقصان در زیرساخت‌های حیاتی اعم از داخلی (تغییرات غیرطبیعی ناشی از درون خود سامانه) یا خارجی (وجود تعاملات خارج از سامانه مانند پدیده‌های طبیعی یا اقدام‌های خرابکارانه) این امکان را به تروریست‌ها می‌دهند تا به‌صورت فناورانه‌ای اقدام به ارتکاب علیه زیرساخت‌های حیاتی نمایند(Alcarz, Zeadally Sherali 2015: 5). بنابراین تروریست‌ها با ادراک و سنجش ظرفیت‌های موجود امکان طراحی و اجرای حمله به زیرساخت‌های حیاتی را به‌عنوان یک هدف مورد آماج خود قرار می‌دهد(مهرگان و همکاران، ۱۳۹۹: ۱۵۸-۱۵۶). افزون بر این، تروریست‌ها در این فرایند، پیش از هرگونه اقدامی، درصدد رصد ظرفیت‌هایی درخصوص زیرساخت حیاتی همچون آسیب‌پذیری، خطر، قابلیت ارتکاب و حتی اثرگذاری و انعکاس آن هستند تا نسبت به اتخاذ تصمیم و برنامه‌ریزی در این رابطه کلیهٔ امکان‌ها را مورد سنجش قرار دهند(Schmid, 2020: 847).

بنابراین تروریست‌ها به‌طور فزاینده‌ای از آسیب‌پذیری‌ها در تأسیسات عمومی، دولتی و خصوصی مانند حمل‌ونقل و انرژی و نیز زیرساخت‌های آب و تأسیسات هسته‌ای استفاده می‌کنند. از این‌رو زیرساخت‌های حیاتی به هدف اصلی تهدیدها و حمله‌های تروریستی فناورانه در سراسر جهان تبدیل شده است. وابستگی‌های متقابل و ماهیت به‌هم پیوستهٔ زیرساخت‌های حیاتی واقع در آن سوی مرزها، نگرانی‌های بیشتری را ایجاد می‌کند و نیاز به پاسخ‌های دوجانبه یا منطقه‌ای دارد.

۳. الزامات حقوقی جهانی در جرم‌انگاری

دولت‌ها در راستای همکاری‌های بین‌المللی در قبال جرایم تروریستی فناورانه به وضع مقرراتی در

---

۱. اردشیر نعمت‌پور، مصطفی تقی‌زادهٔانصاری و سکینه ببری (۱۴۰۰)، مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور در قواعد حقوق بین‌الملل، مطالعات بین‌المللی، ۳(۷۱): ۱۸۵-۱۶۵.

حفاظت از زیرساخت‌های حیاتی مبادرت ورزیده‌اند. این در حالی است که باوجود وضع شمار بسیاری از اسناد جهانی و حتی منطقه‌ای ضد جرایم تروریستی[1] در توصیف و جرم‌انگاری ابعاد و اَشکال گوناگون جرایم تروریستی، متأسفانه نبود مقرره‌ای الزام‌آور در این زمینه قابل ملاحظه است. بنابراین باید تأکید داشت که باوجود خطاب قراردادن زیرساخت‌های حیاتی در چارچوب‌های حقوقی جهانی، امکان حمایت کیفری بین‌المللی در جرم‌انگاری اقدام‌های تروریست‌ها علیه این دسته از زیرساخت‌ها توجه لازم صورت نپذیرفته است. از این‌رو فقدان این امر و ایجاد شکاف در گسترهٔ جامعهٔ جهانی در فرایند مقابله با جرایم تروریستی، موجب شده تا تروریست‌ها با حمایت بازیگران دولتی و حتی غیردولتی، به‌سهولت امکان نقض امنیت زیرساخت‌های حیاتی را داشته باشند؛ هرچند باید اظهار داشت که جامعهٔ جهانی در زمینهٔ رویارویی با جرایم تروریستی فناورانه امکان‌هایی را فراهم آورده است، اما با توجه به تحولات حاکم در حوزهٔ علوم و فناوری‌های نوین، سوءاستفادهٔ تروریست‌ها در این عرصه شرایط و قواعد میدان را با چالش‌هایی مواجه ساخته است که نتیجهٔ آن را باید در سرزمین‌هایی جست‌وجو کرد که تروریست‌ها به‌سهولت به ایجاد اختلال در زیرساخت‌های حیاتی مبادرت می‌ورزند.

با این همه، وفق برخی الزامات جرم‌انگاری جرایم ارتکابی تروریست‌ها در نقض امنیت زیرساخت‌های حیاتی از طریق بهره‌گیری غیرقانونی از پیشرفت‌های فناورانه در چارچوب‌های حقوقی جهانی، سازمان ملل متحد در چارچوب «کارگروه فناوری‌های اطلاعاتی و ارتباطی» و «مؤسسهٔ آموزش و تحقیقات» در سال ۲۰۰۵ کتابچه‌ای با عنوان *عدم امنیت اطلاعات؛ راهنمای بقا در سرزمین‌های ناشناخته تهدیدهای سایبری و امنیت سایبری*[2] منتشر کرد. این کتابچه بر امکان اجرای سازوکارهای احتمالی در پیشگیری و پاسخ‌گذاری به حوادث امنیتی در فرایند چالش‌های ناشی از نبود امنیت اطلاعاتی و توسعهٔ اطلاعات و آگاهی نسبت به جرایم تروریستی فناورانه تأکید دارد.

این در حالی است که نهادهای زیرمجموعهٔ ملل متحد به‌ویژه مجمع عمومی و شورای امنیت سال‌هاست که به این مسئله توجه ویژه‌ای داشته است. البته در راهبرد جهانی مبارزه با تروریسم سازمان ملل متحد، تحت ستون دوم راجع‌به اقدام‌هایی برای مبارزه با جرایم تروریستی و پیشگیری از آن، دولت‌های عضو تصمیم گرفتند که کلیهٔ تلاش‌ها را برای بهبود امنیت و حفاظت از اهداف به‌ویژه آسیب‌پذیر، نظیر زیرساخت‌ها و اماکن عمومی و نیز واکنش به حمله‌های تروریستی و بلایای طبیعی دیگر، به‌ویژه در حوزهٔ حفاظت مدنی، تشدید کنند. از اینرو، برای مقابله با

1. https://treaties.un.org/Pages/DB.aspx?path=DB/studies/page2_en.xml
2. United Nations, Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber Threats and Cyber Security (Ict Task Force Series), July 1, 2005, https://unesdoc.unesco.org/ark:/48223/pf0000143889

تهدیدهای ناشی از جرایم تروریستی فناورانه، همکاری‌های بین‌المللی و تدوین چارچوب‌های حقوقی ضروری است. از جمله مهم‌ترین این چارچوب‌ها می‌توان به کنوانسیون بوداپست (۲۰۰۱) اشاره کرد که اولین معاهده بین‌المللی در زمینه جرایم سایبری است و کشورهای عضو را به همکاری در زمینه مبارزه با جرایم سایبری ملزم می‌کند. همچنین، اتحادیه اروپا با تصویب مقرراتی مانند «دستورالعمل شبکه و سامانه‌های اطلاعاتی»[۱] و «قانون تاب‌آوری سایبری»[۲] به تقویت امنیت سایبری در سطح اتحادیه پرداخته است.

علاوه بر اقدام‌های کلی برای پیشگیری از تهدیدهای ناشی از جرایم تروریستی فناورانه در نقض امنیت زیرساخت‌های حیاتی که در قطعنامه‌های ۱۳۷۳ (۲۰۰۱) و ۱۵۶۶ (۲۰۰۴) مقرر شده بود، شورای امنیت قطعنامهٔ ۲۳۴۱ را در سال ۲۰۱۷ تصویب کرد که به‌عنوان اولین سند جهانی، به‌طور کامل به اهمیت حفاظت از زیرساخت‌های حیاتی اختصاص داشت. در این قطعنامه، شورای امنیت جرایم تروریستی فناورانه را با تأسی از قطعنامهٔ ۱۳۷۳ سال ۲۰۰۱ مورد تأکید قرار داد و از کلیهٔ دولت‌های عضو خواست تا این دسته از جرایم را به‌عنوان جرایم جنایی جدی در قوانین و مقررات داخلی تثبیت کنند و اطمینان حاصل کنند که مسئولیت کیفری این نوع جرایم را با هدف تخریب یا از کار انداختن زیرساخت‌های حیاتی و همچنین برنامه‌ریزی، آموزش، تأمین مالی و پشتیبانی لجستیکی برای چنین جرایمی تعیین کرده‌اند.

گفتنی است یکی از ویژگی‌های متمایز قطعنامهٔ ۲۳۴۱ با سایر اسناد مرتبط فراخوان چارچوب آن از دولت‌های عضو برای جرم‌انگاری خاص اقدام‌های ارتکابی (مانند جرایم تروریستی فناورانه)

---

۱. دستورالعمل شبکه و سامانه‌های اطلاعاتی (Network and Information Systems) مقرراتی در سراسر اتحادیه اروپا است که هدف آن افزایش امنیت شبکه و سامانه‌های اطلاعاتی در سراسر کشورهای عضو است که طی سال ۲۰۱۶ به تصویب رسید و بر ارائه‌دهندگان خدمات ضروری و ارائه‌دهندگان خدمات دیجیتال متمرکز شد. این دستورالعمل از کشورهای عضو می‌خواهد که قابلیت‌های امنیت سایبری خود را افزایش دهند و در عین حال اقدامات مدیریت خطر و الزامات گزارش‌دهی را به نهادهای بخش‌های بیشتری معرفی کنند و قوانینی را برای همکاری، اشتراک‌گذاری اطلاعات، نظارت و اجرای اقدامات امنیت سایبری تنظیم کنند؛

- https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

۲. قانون تاب‌آوری سایبری (Cyber Resilience Act "CRA") برای بهبود امنیت سایبری و انعطاف‌پذیری سایبری در اتحادیه اروپا از طریق استانداردهای امنیت سایبری مشترک برای محصولات دارای عناصر دیجیتال در اتحادیه اروپا است، نظیر گزارش‌های حوادث مورد نیاز و به‌روزرسانی‌های امنیتی خودکار. محصولات با عناصر دیجیتال عمدتاً سخت‌افزار و نرم‌افزاری هستند که استفاده مورد نظر و قابل پیش‌بینی شامل اتصال مستقیم یا غیرمستقیم داده به یک دستگاه یا شبکه است؛

- https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739259

علیه زیرساخت‌های حیاتی است. در انجام این امر، شورای امنیت بر تعدادی از اسناد تصویب شدهٔ قبلی استوار است که الزامات کلی را برای دولت‌های عضو در زمینهٔ محاکمه عاملان جرایم تروریستی فناورانه و تسهیل‌کنندگان آن تعیین می‌کند. بنابراین ابزار شاخص در این زمینه، قطعنامهٔ ۱۳۷۳ است؛ این قطعنامه که اندکی پس از حوادث تروریستی ۱۱ سپتامبر ۲۰۰۱ از سوی شورای امنیت اصدار یافت، در میان اقدام‌های دیگر، مجموعهٔ جامعی از الزامات عدالت کیفری و اسناد راجع‌به پیشگیری، سرکوب و الزامات جرم‌انگاری اقدام‌های تروریستی بین‌المللی علیه زیرساخت‌های حیاتی است که تعهداتی را برای دولت‌های عضو ارائه می‌کند.

به‌علاوه، شورای امنیت در قطعنامهٔ ۲۳۹۶ صادره در سال ۲۰۱۷ اذعان داشت داعش نیز از حامیان و وابستگان خود به‌ویژه جنگجویان تروریستی که مناطق درگیری مسلحانه را ترک می‌کنند، خواست تا حملاتی را به اماکن عمومی و تأسیسات عمومی طراحی و اجرا کنند؛ در این قطعنامه، شورای امنیت بر ضرورت ایجاد یا تقویت مشارکت‌های ملی، منطقه‌ای و بین‌المللی با ذی‌نفعان، اعم از دولتی و خصوصی، برای به اشتراک‌گذاری اطلاعات و تجربیات برای پیشگیری، حفاظت، کاهش، تحقیق، پاسخگویی و بهبودی خسارات ناشی از جرایم تروریستی علیه اهداف نرم (مانند مراکز شهری و اماکن اصلی توریستی، اماکن مذهبی و بهره‌گیری از سامانه‌های هواپیمای بدون سرنشین)[1] تأکید کرد.

در ژوئن ۲۰۲۱، در هفتمین بررسی راهبرد جهانی ضد تروریسم سازمان ملل متحد، دولت‌های عضو با اجماع موافقت کردند که حفاظت از اهداف آسیب‌پذیر باید در اولویت اقدام مشترک آن‌ها علیه جرایم تروریستی باشد.[2] قطعنامهٔ ۲۹۱/۷۵ مجمع عمومی در سال ۲۰۲۱ مشتمل بر دو بند مقدماتی و چهار بند عملیاتی در این زمینه بود که بر لزوم گردهم آوردن همهٔ ذی‌نفعان (اعم از دولت‌های عضو، سازمان‌های بین‌المللی و منطقه‌ای، بخش خصوصی، جامعهٔ مدنی و دانشگاهیان)، برای مقابلهٔ مؤثر با تهدید بی‌سابقه‌ای که جرایم تروریستی فناورانه به زیرساخت‌های حیاتی و اهداف نرم ایجاد می‌کند، تأکید کرد.[3]

برنامهٔ جهانی مقابله با تهدیدهای ناشی از جرایم تروریستی فناورانه علیه اهداف آسیب‌پذیر از جمله زیرساخت‌های حیاتی و اماکن عمومی (یا «اهداف نرم»)، به‌طور مشترک از سوی دفتر مبارزه

1. The protection of critical infrastructures against terrorist attacks: Compendium of good practices, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf
2. https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy
3. United Nations, General Assembly, A/RES/75/291, 2 July 2021, https://documents.un.org/doc/undoc/gen/n21/175/70/pdf/n2117570.pdf

با تروریسم، ادارهٔ اجرایی کمیتهٔ مبارزه با تروریسم[1]، مؤسسهٔ تحقیقات جنایی و عدالت بین منطقه‌ای سازمان ملل متحد[2] و اتحاد تمدن‌های سازمان ملل[3]، با همکاری اینترپل، از سال ۲۰۲۱ از دولت‌های عضو در ایجاد ظرفیت‌های خود، توسعهٔ ارتباطات بین کارشناسان و شناسایی شیوه‌های مطلوب برای حفاظت از زیرساخت‌های حیاتی حمایت می‌کند.

برنامهٔ جهانی دفتر مبارزه با تروریسم سازمان ملل متحد برای مقابله با تهدیدهای ناشی از جرایم تروریستی فناورانه علیه اهداف آسیب‌پذیر به درخواست دولت‌های عضو به‌ویژه از طریق مجمع عمومی (راهبرد جهانی ضد تروریسم و قطعنامه‌های بررسی و قطعنامهٔ ۲۹۸/۷۷[4] مصوب سال ۲۰۲۳) و شورای امنیت (قطعنامه‌های ۲۳۴۱ و۲۳۹۶ در سال ۲۰۱۷ و ۲۶۱۷ در سال ۲۰۲۱) و «اصول راهنمای شورای امنیت راجع‌به جنگجویان تروریست خارجی: اصول راهنمای مادرید[5]، ۲۰۱۵) همراه با الحاقیهٔ ۲۰۱۸، تقویت حمایت سازمان ملل متحد از دولت‌های عضو برای رسیدگی به شکاف‌ها و چالش‌ها در حفاظت از اهداف آسیب‌پذیر که شامل زیرساخت‌های حیاتی و اهداف «نرم» بود را در صدر اولویت قرار داد.[6] هدف این برنامه شناسایی و به اشتراک‌گذاری سیاست‌ها و سازوکارهای عملیاتی برای درک، پیشگیری و مقابله با تهدیدهای احتمالی جرایم تروریستی فناورانه علیه اهداف آسیب‌پذیر بود.[7] البته تقویت ظرفیت دولت‌های عضو برای توسعهٔ راهبردهای جامع و مشترک همچون مشارکت عمومی–خصوصی، ظرفیت‌سازی مناسب برای پیشگیری، حفاظت، کاهش، بررسی، پاسخ و بازیابی جرایم تروریستی فناورانه علیه اهداف آسیب‌پذیر مورد تأکید قرار داشت.[8]

---

1. Office of Counter-Terrorism, the Counter-Terrorism Committee Executive Directorate
2. United Nations Interregional Crime and Justice Research Institute (UNICRI)
3. United Nations Alliance of Civilizations
4. United Nations, General Assembly, A/RES/77/298, 3 July 2023, https://documents.un.org/doc/undoc/gen/n23/189/01/pdf/n2318901.pdf
5. Security Council Guiding Principles on Foreign Terrorist Fighters: The 2015 Madrid Guiding Principles, 2018 Addendum, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/security-council-guiding-principles-on-foreign-terrorist-fig.pdf

۶. در سال ۲۰۲۲ دفتر مبارزه با تروریسم سازمان ملل متحد مجموعه اقدامات سازوکارهای مطلوب سازمان ملل متحد را در مورد حفاظت از زیرساخت‌های حیاتی در قبال جرایم تروریستی روزآمد و منتشر کرد؛

- https://www.un.org/counterterrorism/events/unoct-launches-2022-update-un-compendium-good-practices-protection-critical-infrastructure

7. https://www.un.org/counterterrorism/vulnerable-targets
8. https://www.un.org/counterterrorism/cybersecurity

افزون طرح اقدام‌های فوق‌الاشعار باید اذعان شود که در چارچوب حقوقی مقرر در مادهٔ ۵۶ پروتکل اول الحاقی به کنوانسیون‌های چهارگانهٔ ژنو، برای حفاظت از اشیا به‌ویژه اشیای مهم، سازوکار اجراشدنی‌ای را ارائه می‌دهد.[1] حفاظت‌های ویژه در مادهٔ ۵۶ به‌صراحت سدها، دیواره‌های بتنی و ایستگاه‌های تولید برق هسته‌ای را شامل می‌شود؛ این اشیا زیرمجموعه‌ای از زیرساخت‌های حیاتی هر دولتی به‌شمار می‌روند که به علیت آثار فاجعه‌بار بالقوه ناشی از یک حمله(نظیر جرم تروریستی فناورانه)، از حمایت‌های ویژه برخوردار هستند.[2]

در مخاصمات معاصر، ارتکاب یک جرم تروریستی فناورانه ممکن است به زیرساخت‌های حیاتی از جمله سامانهٔ مراقبت بهداشتی، شبکهٔ برق، یا شبکهٔ حمل‌ونقل آثار مخرب احتمالی را به‌دنبال داشته باشد. بنابراین به‌نظر می‌رسد تدوین مادهٔ قانونی مشابه مادهٔ ۵۶، هرچند با درک وسیع‌تر از موضوع حفاظت‌شده، ضرورتی انکارناپذیر در زمینهٔ مقابله با جرایم تروریستی فناورانه خواهد بود.

با این حال، هر هنجار جدید باید به مادهٔ ۵۶ به‌عنوان الگویی برای سنجش ضرورت نظامی با دستورات اهداف بشردوستانه مورد تصویب قرار گیرد تا امکان نظارت مؤثر در این رابطه فراهم آید. البته دولت‌ها برای الحاق به یک معاهدهٔ ویژهٔ فناورانه که از زیرساخت‌های حیاتی در زمان ارتکاب جرایم تروریستی فناورانه حافظت کند، مقاومت می‌کنند که در قبال چنین رویکردی، باید دولت‌ها در حفاظت از زیرساخت‌های حیاتی خود، منافع حاکمیتی و ملی را در نظر بگیرند. بنابراین با توجه به افزایش توانایی دولت‌ها برای بهره‌گیری تهاجمی از قدرت نبرد فناورانه، آسیب‌پذیری‌ها و تهدیدها علیه زیرساخت‌های حیاتی کشورهای پیشرفته، از توانایی آن‌ها برای دفاع از سامانه‌های فناورانه و شبکه‌ای آن‌ها پیشی گرفته است.[3] گفتنی است اتخاذ توافق‌های بین‌المللی با گسترهٔ محدود برای پیشگیری از پیامدهای فاجعه‌بار بالقوه مخاصمات مسلحانه بی‌سابقه نیست؛ برای نمونه، «کنوانسیون منع استفادهٔ نظامی یا هرگونه بهره‌گیری خصمانهٔ دیگر از فنون اصلاح محیط زیست، مصوب ۱۹۷۶»[4] بهره‌گیری از فنون اصلاح محیطی که اثرات گسترده، طولانی‌مدت یا شدید به‌عنوان ابزاری برای تخریب، آسیب یا صدمه

1. Article 56 - Protection of works and installations containing dangerous forces, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-56
2. Additional Protocol I, supra note 73, at art. 56(2).
3. Sean Watts (2009), Reciprocity and the Law of War, Harvard International Law Journal, 50(4): 365-375.
4. Convention on the Prohibition of the Military or Any Other Hostile Use of Environmental Modification Techniques, New York, 10 December 1976, https://legal.un.org/avl/ha/cpmhuemt/cpmhuemt.html

به هر دولت عضو دیگر دارد[1]، می‌توان اشاره کرد.[2]

با این حال امروزه با توجه به شرایط حاکم در زیرساختهای حیاتی دولت‌ها و امکان وجود چالش‌ها و تهدیدهای ناشی از ارتکاب جرایم تروریستی فناورانه، وجود یک معاهدهٔ ویژهٔ فناورانه نظیر کنوانسیون ۱۹۷۶ که از زیرساخت‌های حیاتی حفاظت کند، مؤید تلاشی معنادار و واقع‌بینانه از سوی دولت‌ها برای تأکید مجدد در شکل‌دهی زیرساخت هنجاری موازین بین‌المللی در پاسخ به فناوری‌های نوظهوری است که در جرایم تروریستی امکان بهره‌گیری از آن وجود دارند و امکان انهدام استحکامات و نقض قواعد آن را فراهم می‌آورد. بنابراین به‌نظر می‌رسد که ضرورت فوری به حفاظت از زیرساخت‌های حیاتی در قبال جرایم تروریستی فناورانه، فرصتی را برای تدوین و تنظیم چنین سندی خاص در چارچوب اقدام‌های فناورانه ایجاد خواهد کرد. سند مزبور که وفق طرح قانونی مقرر در مادهٔ ۵۶ پروتکل اول الحاقی مدنظر واقع شده است، حفاظت‌های ویژه‌ای را از زیرساخت‌های حیاتی در مقابله با ارتکاب جرایم تروریستی فناورانه به‌عمل می‌آورد(Wallace and Reeves, 2020: 1609).

دلیل مهمی که چرا دولت‌های عضو باید رفتارهای شناسایی شده در چارچوب حقوقی جهانی علیه جرایم تروریستی فناورانه را جرم‌انگاری کنند، تسهیل همکاری بین‌المللی در امور کیفری است. مادامی که ارتکاب جرایمی همچون جرایم ترویستی فناورانه علیه زیرساخت‌های حیاتی در مقررات کیفری دولت‌های عضو وضع شود، موانع مهم برای چنین همکاری‌هایی در گسترهٔ بین‌المللی مرتفع خواهد شد. البته دولت‌هایی که به‌دنبال به حداکثر رساندن حمایت از حقوقی و فنی از زیرساخت‌های حیاتی در چارچوب عدالت کیفری هستند، باید نقش چارچوب جهانی علیه جرایم تروریستی فناورانه را در فراهم کردن مبانی حقوقی برای استرداد و مساعدت‌های حقوقی متقابل، اعم از دوجانبه و منطقه‌ای در نظر گیرند.

---

1. See: Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, art. I, Dec. 10, 1976, 1108 U.N.T.S. 151 [hereinafter ENMOD Convention]. The treaty is commonly referred to as the "ENMOD Convention." See, e.g., 1976 Convention on the Prohibition of Military or any Hostile Use of Environmental Modification Techniques, International Committee of the *Red Cross* (ICRC) (Jan. 2003), https://www.icrc.org/en/download/file/1055/1976-enmod-icrc-factsheet.pdf.

۲. کنوانسیون منع استفادهٔ نظامی یا هرگونه بهره‌گیری خصمانهٔ دیگر از فنون اصلاح محیط زیست، «فنون اصلاح محیطی» را به‌عنوان «هر فن برای تغییر از طریق دستکاری عمدی فرآیندهای طبیعی (نظیر دینامیک، ترکیب یا ساختار زمین، همچون بیوتا، لیتوسفر، هیدروسفر و اتمسفر آن، یا فضای بیرونی) تعریف می‌کند؛

- Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, supra note 186, at art. II.

نتیجه‌گیری

امروزه بسیاری از زیرساخت‌های حیاتی در زمینه‌های انرژی، سلامت، حمل‌ونقل (دریایی، هوایی، زمینی و حتی فضای ماورای جو) و مخابرات به سیستم‌های رایانه‌ای و شبکه‌های اینترنتی وابستگی شدید دارند؛ چنین بستری مفاهیم حمله‌های تروریستی را تغییر می‌دهد و امکان ارتکاب را در فضایی غیر حقیقی و در واقع در فضای دیجیتالی مستقر می‌کند. این حملات در برخی موارد زیرساخت‌های یک کشور را هدف قرار می‌دهد و نابود می‌کند.

ارتکاب جرایم تروریستی فناورانه علیه زیرساخت‌های حیاتی در هر کشور به ایجاد اختلال در این زیرساخت‌ها و ورود به زیان‌های جبران‌ناپذیری در زمینه‌های مختلف از قبیل تلفات انسانی، خسارت‌های اقتصادی و از دست‌دادن اعتماد عمومی منجر می‌شود. بنابراین بی‌توجهی متناسب، اثرگذار، مطلوب و حتی روزآمد و بهنگام به مقولهٔ حفاظت در زیرساخت‌های اطلاعاتی حیاتی، علاوه بر ایجاد مخاطرات و تهدیدهای کلان، اقتدار و امنیت ملی در هر کشور را خدشه‌دار خواهد کرد.

ماهیت جرایم تروریستی فناورانه به نحوی است که عاملان متعددی در آن نقش دارند؛ این عوامل مشتمل بر اشخاص و مجموعه‌های دولتی و خصوصی است. وسعت این عوامل به این دلیل است که دسترسی به رایانه و اینترنت بسیار آسان شده است. به تعبیر دیگر، با توجه به اینکه وسایل به کار رفته در جرایم تروریستی فناورانه، کامپیوتر و اینترنت است، به همین علت ارتکاب آن چندان دشوار به‌نظر نمی‌رسد. عوامل (تروریست‌ها) این نوع از جرایم ارتکابی در گسترهٔ فضای دیجیتالی، منحصراً در قلمرو حاکمیتی کشور مورد هدف نیست، بلکه اغلب این عوامل در خارج قلمرو حاکمیتی کشور مورد هدف قرار دارند و مقاصد خود را در کشورهای دیگر دنبال می‌کنند.

در هر حال، باوجود اینکه مقابله و سرکوب ارتکاب جرایم تروریستی فناورانه علیه زیرساخت‌های حیاتی، در قلمرو حاکمیتی هر کشور در ساختار حاکمیت حقوقی جهانی قابل ملاحظه است، اما باید اذعان داشت که عدم اقتدار و نقص در استحکام حقوقی اسناد بین‌المللی، الزامات جرم‌انگاری این دسته از جرایم ارتکابی به‌واسطهٔ همکاری میان دولت‌ها قابلیت اصلاح و جبران را خواهد داشت. این در حالی است که نبود یک چارچوب حقوقی جهانی در جرم‌انگاری و الزامات حاکم بر آن در پاسخ‌گذاری به جرایم تروریستی فناورانه علیه زیرساخت‌های حیاتی، به‌عنوان مسئلهٔ مورد اهتمام جهانی قابل ملاحظه است. با مطالعهٔ اسناد حقوقی جهانی و تدقیق در مفاد و موازین قابل اجرا راجع‌به جرایم تروریستی فناورانه که امکان نقض امنیت سامانه‌ها و تأسیسات را در زیرساخت‌های حیاتی فراهم می‌آورند، به‌وضوح موانع و خلأهای حقوقی جهانی را در زمینهٔ عدم تعهد حقوقی دولت‌ها و بازیگران غیردولتی غیرقانونی به‌ویژه گروه‌های تروریستی از امکان احراز و انتساب مسئولیت کیفری بین‌المللی به آن‌ها قابل ملاحظه است.

پیشنهادهای کاربردی

با توجه به تهدیدهای فزاینده ناشی از جرایم تروریستی فناورانه علیه امنیت زیرساخت‌های حیاتی کشورها، ضرورت دارد تا به‌طور گسترده‌ای امکان مقابله با آنها در کشورها به‌عنوان یک اولویت اساسی، فراهم گردد. از اینرو، سازوکارهای ذیل در این راستا قابلیت اجرایی پیدا می‌کنند:

الف- تقویت سامانه‌های امنیت سایبری داخلی؛ کشورها باید ابتدا سامانه‌های امنیت سایبری داخلی خود را تقویت کنند. این تقویت شامل به‌روز نگه‌داشتن نرم‌افزارها، تجهیز به ابزارهای پیشرفته امنیتی، آموزش نیروهای متخصص و ایجاد زیرساخت‌های مقاوم در برابر حمله‌های فناورانه است. همچنین، ایجاد مراکز فرماندهی و هماهنگی سایبری می‌تواند برای نظارت بر تهدیدها و مدیریت بحران‌های سایبری در زمان حمله اهمیت زیادی داشته باشد.

ب- همکاری‌های بین‌المللی و تبادل اطلاعات؛ تهدیدهای فناورانه به‌طور طبیعی مرزهای جغرافیایی را درنوردیده و جهانی هستند. همکاری‌های بین‌المللی، تبادل اطلاعات، و هماهنگی در پاسخ‌ها، ابزارهایی حیاتی برای مقابله با این نوع جرایم محسوب می‌شوند. کشورهای مختلف باید در سازمان‌ها و توافقات بین‌المللی فعالانه شرکت کنند تا تبادل اطلاعات تهدیدات، شیوه‌های مقابله و راهکارهای امنیتی به‌صورت مؤثر انجام شود.

ج- ایجاد چارچوب‌های قانونی و استانداردهای جهانی؛ در این فرایند، کشورها باید قوانین و مقررات ویژه‌ای برای حفاظت از زیرساخت‌های حیاتی تدوین کنند. ایجاد استانداردهای جهانی برای امنیت سایبری، همان‌طور که در کنوانسیون بوداپست و دیگر اسناد بین‌المللی آمده است، می‌تواند زمینه‌ساز همکاری‌های قانونی میان کشورها شود. در همین راستا، تدوین یک چارچوب جهانی که کشورها را موظف به اجرای آن در راستای مقابله با تهدیدهای فناورانه کند، اهمیت دارد.

د- هم‌افزایی جهانی برای پاسخگویی مؤثر؛ برای مقابله مؤثر با تهدیدهای ناشی از جرایم تروریستی فناورانه، پاسخ‌ها باید هماهنگ و هم‌افزا باشند. کشورها باید با یکدیگر همکاری کنند و یک محیط جهانی امن‌تر برای زیرساخت‌های حیاتی ایجاد کنند. این همکاری‌ها نه تنها باید در زمینه تبادل اطلاعات، بلکه در زمینه توسعه فناوری‌ها، ابزارهای حفاظتی، و مدیریت بحران‌های فناورانه نیز شامل شود.

با این همه، بهره‌گیری از تجربیات کشورهای پیشرفته در حوزه امنیت فناورانه و به‌کارگیری جدیدترین فناوری‌ها و راهبردهای امنیتی می‌تواند به موفقیت بیشتر در ایجاد امنیت در قبال تهدیدهای فناورانه کمک کند. در ضمن، با توجه به سرعت تکامل تهدیدات سایبری و جرایم تروریستی فناورانه، امنیت زیرساخت‌های حیاتی کشورها باید به یک اولویت راهبردی تبدیل شود.

اقدامات پیشگیرانه، همکاری‌های بین‌المللی، استفاده از فناوری‌های نوین و توسعه چارچوب‌های قانونی می‌تواند به کشورها کمک کند تا در برابر تهدیدهای پیچیده و جهانی مقاوم‌تر شوند. این تلاش‌های مشترک در نهایت به ایجاد دنیای دیجیتال امن‌تری برای همه کشورها منجر خواهد شد.

کتابنامه

آقایی، محسن و همکاران (۱۳۹۸) ارائهٔ مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی، امنیت ملی، ۹(۳۲): ۲۰۱-۲۳۱.

تقی‌پور، رضا و همکاران (۱۳۹۸)، الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران، امنیت ملی، ۹(۳۴): ۷-۴۸.

کافی، سعید (۱۳۹۹) شاخص‌های دفاعی ـ امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران مبتنی‌بر رویکردهای پدافند غیرعامل، سیاست دفاعی، ۲۹(۲): ۹۱-۷۱.

مهرگان، امیرحسین و همکاران (۱۳۹۹) ضرورت بازنگری مأموریت کمیتهٔ بین‌المللی صلیب سرخ: از کاهش آلام انسانی تا پیشگیری از خشونت‌های مسلحانه، مطالعات بین‌المللی، ۲(۶۶): ۱۵۱-۱۶۹.

نعمت‌پور، اردشیر و همکاران (۱۴۰۰) مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور در قواعد حقوق بین‌الملل، مطالعات بین‌المللی، ۳(۷۱): ۱۸۵-۱۶۵.

نظری‌نژاد، احمدعلی و همکاران (۱۳۹۹) الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران، مطالعات دفاعی استراتژیک، ۱۸(۸۲): ۳۱۳-۳۳۶.

میریوسفی، سیدمحسن و همکاران (۱۳۹۹) راهبردهای نوین حفاظت از زیرساخت‌های حیاتی، پدافند غیرعامل، ۱۱(۳): ۱-۱۴.

Alcarz, Cristina., Zeadally Sherali. (2015).1 critical infrastructure protection: equirements and challenges for the 21st century, International Jounral of Critical Infrastructure Protection (IJCIP), 8. Elsevier Science, p. 5.

Ajetunmobi, R.L. (2015). Cybercrimes (Prohibition, Prevention, etc. Act 2015: A Review, NIALS Journal of Intellectual Property, 17 p.171.

Iaremenko, Andrey (2023), Five Threats to Critical Infrastructure Security, Hub Cyber Security Ltd, August 2, https://blog.hubsecurity.com/blog/critical-infrastructure-security/5-threats-to-critical-infrastructure-security

Alkharman, Awwad, Jamal and Isyaku Hassan (2023). Cyberterrorism and Self-Defense in the Framework of International Law. Journal of Law and Sustainable Development, 11(8): 1-21.

A.Shaji, George, T.Baskar, P.Balaji Srikaanth (2024), Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors, Partners Universal International Innovation Journal, 2(1): 51-75.

Schori Liang, Christina (2023), Terrorist Digitalis: Preventing Terrorists from Using

Emerging Technologies, 15 March, Geneva Centre for Security Policy, https://www.gcsp.ch/publications/terrorist-digitalis-preventing-terrorists-using-emerging-technologies

Wallace, David A. and Shane R. Reeves (2020), Protecting Critical Infrastructure in Cyber Warfare: Is It Time for States to Reassert Themselves?, University of California-Davis Law Review, 50(2): 1607-1645.

Schmitt, Michael N. (2014), The Law of Cyber Warfare: Quo Vadis?, 25 STAN. Stanford Law & Policy Review, 25(3): 269-281.

Schmitt, Michael & Liis Vihul (2017), International Cyber Law Politicized: The UN Group of Governmental Experts Failure to Advance Cyber Norms, Just Security, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failureadvance-cyber-norms [https://perma.cc/337F-DD8V]

Schmid, A. (2020). Handbook of Terrorism Prevention and Preparedness, ICCT Press, p. 847Schmid, A. P. (2019). The Routledge Handbook of Terrorism Research (2nd ed.). Routledge.