نوع مقاله: پژوهشی
تاریخ دریافت: ۱۴۰۲/۱۲/۱۹
تاریخ پذیرش: ۱۴۰۳/۰۵/۰۱
صفحه: ۱۵ الی ۳۴

Applied Criminology Research
پژوهش های جرم شناسی کاربردی

Volume 3, Issue 7, Spring 2025
Received: 2024/03/09
Accepted: 2024/07/22
Pages: 15-34

System: qacr.ir
doi: 10.22034/AQCR.2024.2045159.1036
Article Type: **Research**

دوره ۳ / شماره ۷/ بهار ۱۴۰۴

Legal Approaches to Preventing Digital Terrorist Crimes Against Nuclear Facilities

Peyman Namamian[1]

Abstract

Field and Aims: One of the most important emerging threats is digital terrorist crimes, especially digital terrorist crimes against nuclear facilities that can be committed. Today, terrorist groups can expand the dimensions of their terrifying operations by using new communication technologies. These groups, using various media, especially the Internet, expose their hateful and violent messages to everyone. Therefore, to prevent threats arising from anomalies arising from the digital space, numerous documents have been approved so far, but despite the diversity of these documents in national and international systems, unfortunately, none of them has provided the opportunity to achieve a desirable situation in facing the emerging threats.

Method: This research, using library resources and websites and using a descriptive-analytical method, seeks to study how to confront nuclear digital terrorist crimes, as well as to assess the achievements and legal approaches governing it.

Findings and Conclusions: Reducing vulnerabilities and strengthening security and peace in the face of emerging threats and new actors and getting rid of digital terrorist crimes requires addressing future studies on the impact of the information revolution on national security, threats from the digital space, improving technical capabilities and public awareness of these threats, as well as utilizing knowledge and information in this regard. However, it seems that adopting global strategies against terrorist crimes by covering the diverse dimensions of digital terrorist crimes will create a new arena of interaction and consensus among elites to create international peace and security.

Keyword: Digital Space, Digital Terrorist Crimes, Nuclear Digital Terrorist Crimes, Nuclear Facility Security, International Security.

Citation (APA): Namamian, P. (2025). Legal Approaches to Preventing Digital Terrorist Crimes Against Nuclear Facilities. *Applied criminology research*, 3(7), 15-34.
https://qacr.ir/article_718709.html?lang=en

1. Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran. Email: p-namamian@araku.ac.ir

Volume 3, Issue 7, Spring 2025

Received: 2024/03/09
Accepted: 2024/07/22
Pages: 15-34

پژوهش های جرم شناسی کاربردی
Applied Criminology Research

نوع مقاله: پژوهشی

تاریخ دریافت: ۱۴۰۲/۱۲/۱۹
تاریخ پذیرش: ۱۴۰۳/۰۵/۰۱
صفحه: ۱۵ الی ۳۴

Article Type: **Research**
doi: 10.22034/AQCR.2024.2045159.1036
سامانه: qacr.ir

دوره ۳ / شماره ۷/ بهار ۱۴۰۴

رویکردهای حقوقی ناظر بر پیشگیری از جرایم تروریستی دیجیتالی علیه تأسیسات هسته‌ای

پیمان نمامیان[۱]

چکیده

زمینه و هدف: یکی از مهم‌ترین تهدیدهای نوظهور، جرایم تروریستی دیجیتالی به ویژه جرایم تروریستی دیجیتالی علیه تأسیسات هسته‌ای است که امکان ارتکاب پیدا می‌نمایند. امروزه، گروه‌های تروریستی با استفاده از فناوری‌های نوین ارتباطی می‌توانند به ابعاد عملکرد هراس‌انگیز خود وسعت بیشتری بخشند. این گروه‌ها با بهره‌گیری از رسانه‌های مختلف و به‌ویژه اینترنت، پیام‌های نفرت‌انگیز و خشونت‌آمیز خود را در معرض دید همگان قرار می‌دهند. از این رو، برای پیشگیری از تهدیدهای ناشی از ناهنجاری‌های برآمده از فضای دیجیتالی، تاکنون اسناد متعددی به تصویب رسیده است؛ اما با وجود تنوع این اسناد در نظام‌های ملی و بین‌المللی، متأسفانه هیچ یک از آنها موجبات تحقق وضعیتی مطلوب در مواجهه با تهدیدهای پیش‌روی را فراهم نکرده است.

روش: این پژوهش با بهره‌گیری از منابع کتابخانه‌ای و وب‌گاه‌ها و استفاده از روش توصیفی- تحلیلی، درصدد است تا ضمن مطالعه نحوه رویارویی با جرایم تروریستی دیجیتالی هسته‌ای، دستاوردها و رویکردهای حقوقی حاکم بر آن را مورد سنجش قرار دهد.

یافته‌ها و نتایج: کاهش آسیب‌پذیری‌ها و تقویت امنیت و صلح در مواجهه با تهدیدهای نوظهور و بازیگران جدید و رهایی از جرایم تروریستی دیجیتالی مستلزم پرداختن به مطالعات آینده‌پژوهی درباره تأثیر انقلاب اطلاعاتی بر امنیت ملی، تهدیدهای فضای دیجیتالی، ارتقای قابلیت‌های فنی و اگاهی عمومی از این تهدیدها و همچنین، بهره‌گیری از دانش و اطلاعات در این خصوص است. با این حال، به نظر می‌رسد که اتخاذ راهبردهای جهانی علیه جرایم تروریستی با پوشش‌دادن به ابعاد متنوع جرایم تروریستی دیجیتالی، به ایجاد عرصه‌ای نوین از تعامل و همفکری نخبگان برای ایجاد صلح و امنیت بین‌المللی خواهد شد.

کلیدواژه‌ها: فضای دیجیتالی، جرایم تروریستی دیجیتالی، جرایم تروریستی دیجیتالی هسته‌ای، امنیت تأسیسات هسته‌ای، امنیت بین‌المللی.

استناددهی (APA): نمامیان، پیمان. (۱٤۰٤). رویکردهای حقوقی ناظر بر پیشگیری از جرایم تروریستی دیجیتالی علیه تأسیسات هسته‌ای. *پژوهش‌های جرم‌شناسی کاربردی*، ۳(۷)، ۳٤-۱۵.

https://qacr.ir/article_718709.html

۱. دانشیار گروه حقوق دانشکده علوم اداری و اقتصاد دانشگاه اراک، اراک، ایران. رایانامه: p-namamian@araku.ac.ir

مقدمه

با محیط امنیتی جهانی که به طور مداوم در حال تحول است، جلوتربودن از تهدیدات بالقوه برای دارایی‌های هسته‌ای بسیار مهم است. در عصری که با پیشرفت‌های سریع فناوری و چالش‌های امنیتی در حال تکامل مشخص می‌شود، حفاظت از دارایی‌های هسته‌ای به یک نگرانی جهانی تبدیل شده است (لاورینگ و همکاران[1]، ۲۰۲۰: ۵؛ اوندرکو و زوت[2]، ۲۰۲۱: ۲۹۱-۲۸۹).[3]

اساس امنیت هسته‌ای موثر در هم‌افزایی حفاظت فیزیکی قوی، نظارت پیشرفته، امنیت دیجیتالی و همکاری بین‌المللی نهفته است (تاوارس و گیوزا[4]، ۲۰۲۲: ۱). از لحاظ تاریخی، صنعت هسته‌ای توانایی چشمگیری برای انطباق با چالش‌ها و امکانات فناوری نوین از خود نشان داده است.[5] ادغام فناوری‌های پیشرفته با پروتکل‌های امنیتی تثبیت‌شده این پتانسیل را دارد که پارادایم جدیدی از انعطاف‌پذیری را در برابر تهدیدات مرسوم و غیرمتعارف معرفی کند (هاویلا و چیرایت[6]، ۲۰۱۸: ۱۵٤). با افزایش تهدیدات ناشی از تروریسم هسته‌ای و سوءاستفاده احتمالی از مواد رادیواکتیو، امنیت هسته‌ای در دستور کار جهانی قرار گرفته است. اطمینان از ایمنی و حفاظت از تاسیسات و مواد هسته‌ای به یک نگرانی اساسی برای امنیت ملی و ثبات بین‌المللی تبدیل شده است.[7] برای مقابله با این چالش، سیستم‌های نظارتی و نظارتی پیشرفته در حال توسعه و استقرار هستند تا ردیابی، شناسایی و پیشگیری از دسترسی غیرمجاز و فعالیت‌های مخرب در تأسیسات هسته‌ای را افزایش دهند. این سیستم‌ها از فناوری‌های پیشرفته‌ای نظیر هوش مصنوعی، سنجش از راه دور، تجزیه‌وتحلیل داده‌ها در زمان واقعی و

---

1. Lovering et al
2. Onderco & Zutt

۳. تحول دیجیتالی تأسیسات هسته‌ای می‌تواند بهبود تصاعدی عملکرد و رقابت هزینه تأسیسات را باز کند. با این حال، کنترل دیجیتال و ابزار دقیق در تاسیسات هسته‌ای نیز می‌تواند آسیب‌پذیری‌های بالقوه‌ای داشته باشد که چالش‌های امنیت دیجیتالی را ایجاد می‌کند. بهره‌برداری از آسیب‌پذیری‌ها توسط یک عامل تهدید پیچیده ممکن است منجر به انتشار مواد رادیواکتیو در محیط شود.

4. R. L. TavaresR.D, & Giozza

۵. در سال‌های اخیر، پیشرفت فن‌آوری موجب تحول در قابلیت‌های نظارت و نظارت شده است. هوش مصنوعی و فناوری‌های سنجش از راه دور، امکان تجزیه‌وتحلیل بی‌درنگ حجم وسیعی از داده‌ها را فراهم کرده‌اند و تشخیص سریع دسترسی‌های غیرمجاز یا فعالیت‌های مشکوک را تسهیل می‌کنند. امنیت دیجیتالی، یک ستون اساسی امنیت هسته‌ای در عصر دیجیتال، با چالش‌های مستمری از سوی دشمنان دیجیتالی که به دنبال بهره‌برداری از آسیب‌پذیری‌ها در سیستم‌های حیاتی هستند، مواجه است (Hellman, 2017: 56; Jang et al., 2022: 608). در نتیجه، درک آخرین پیشرفت‌ها در سازوکارهای حفاظت دیجیتال برای محافظت در برابر تهدیدات دیجیتالی بالقوه امری انکارناپذیر قلمداد می‌شود.

6. Hawila & Chirayath

۷. جرایم تروریستی دیجیتالی به نهادهای دولتی، سیستم‌های دفاعی یا زیرساخت‌های حیاتی نظیر تأسیسات هسته‌ای، تهدیدی جدی برای امنیت ملی به شمار می‌رود که به‌طور بالقوه توانایی یک کشور برای دفاع از خود را به خطر می‌اندازد.

یادگیری عمیق استفاده می‌کنند تا پوشش جامع و قابلیت‌های تشخیص زودهنگام را ارائه دهند.[1]

امنیت هسته‌ای فراتر از تهدیدهای خارجی است و تهدیدات داخلی ناشی از افراد دارای دانش، دسترسی و اختیار در تاسیسات هسته‌ای را دربرمی‌گیرد. برای مقابله با این خطرات، یک رویکرد چندوجهی مورد نیاز است؛ از جمله توسعه سیاست‌های امنیتی قوی، ابزارهای نظارتی مؤثر و فرهنگ امنیتی قوی.[2]

علاوه بر این، تهدیدهای مرتبط با جرایم تروریستی هسته‌ای نیز از منابع بسیاری مانند سازمان‌های تروریستی پیچیده و سازمان‌یافته، قاچاقچیان هسته‌ای یا هکرهایی که می‌توانند جرایم تروریستی دیجیتالی ویرانگری را علیه اطلاعات و سیستم‌های رایانه‌ای در تأسیسات هسته‌ای انجام دهند، سرچشمه می‌گیرند. همه این چالش‌ها بر نحوه مدیریت این تهدیدها توسط اپراتورهای تاسیسات، آژانس‌های نظارتی هسته‌ای و سازمان‌های مسئول برنامه‌ریزی و واکنش اضطراری اثرگذار است (کور[3]، ۲۰۲۳: ۲۴۱-۲۳۹).

به هر روی، این پژوهش درصدد بررسی تلاقی جرایم دیجیتالی و امنیت در تأسیسات هسته‌ای بوده و بر اهمیت پرداختن به تهدیدهای نوظهور علیه تأسیسات هسته‌ای ناشی از چنین جرایمی تأکید می‌کند. افزون بر این، با توجه به فقدان رژیم بین‌المللی برای امنیت دیجیتالی هسته‌ای، این وضعیت موجب شده تا چارچوب رژیم معاهده منع گسترش سلاح‌های هسته‌ای با چالش‌های جدی مواجه شده و صلح و ثبات جهانی را با تضعیف اهداف معاهده و افزایش خطر اشاعه و سوءاستفاده هسته‌ای تهدید کند. از این رو، این پژوهش ضمن ایجاد گفتمان جدید راجع به امنیت بین‌المللی تأسیسات هسته‌ای، از یک واکنش جهانی هماهنگ برای محافظت در قبال پیامدهای فاجعه‌بار تهدیدهای ناشی از ارتکاب جرایم دیجیتالی علیه تأسیسات هسته‌ای حمایت می‌کند. بنابراین، نگارنده درصدد خواهد بود تا با بهره‌گیری از منابع

---

۱. از آنجایی که تأسیسات هسته‌ای از فناوری‌های دیجیتال برای افزایش کارایی و عملیات استفاده می‌کنند، در برابر تهدیدات دیجیتالی نیز آسیب‌پذیر می‌شوند که می‌توانند از آسیب‌پذیری‌ها در نرم‌افزار، شبکه‌ها و سیستم‌های کنترل سوءاستفاده کنند. این هم‌گرایی نیازمند یک رویکرد کل‌نگر است که ملاحظات امنیت دیجیتالی را در چارچوب امنیت هسته‌ای موجود ادغام می‌کند (Shubayr, 2024: 5-6).

۲.به‌عنوان نمونه، می‌توان اظهار داشت که نمونه‌های دیگری از جرایم تروریستی دیجیتالی با هدف قراردادن زیرساخت‌های حیاتی در جریان مداخله روسیه در اوکراین، مشاهده شد که در سال ۲۰۱٤ آغاز شد. استفاده از تلفن‌های همراه در کریمه در اولین روزهای نبرد نزدیک در مارس ۲۰۱٤ با تخریب زیرساخت‌های شرکت تلفن انحصاری اوکراین، مقام رسمی اوکراین، پیشگیری شد. شرکت تلفن همراه حمله دیجیتالی دیگری در ۲۳ دسامبر ۲۰۱۵ علیه یک نیروگاه برق در اوکراین انجام داد که باعث قطع برق در آنجا شد. بر اساس ادعاهای اوکراین، این جرایم تروریستی دیجیتالی توسط سرویس‌های اطلاعاتی روسیه و گروه‌های هکر وابسته صورت پذیرفت (Case, 2016: 18-19).

3. Kur

کتابخانه‌ای و وب‌گاه‌ها و استفاده از روش توصیفی- تحلیلی، نحوه رویارویی با جرایم تروریستی دیجیتالی هسته‌ای را مورد مطالعه قرار داده و دستاوردها و رویکردهای حقوقی حاکم بر آن را مورد سنجش قرار دهد.

۱. تأثیر فناوری‌ها بر نحوه ارتکاب جرایم تروریستی

چارچوب حقوق بین‌المللی راجع به جرایم تروریستی پیش از حوادث تروریستی ۱۱ سپتامبر ۲۰۰۱ وجود داشت. از میان هجده سند بین‌المللی[1] که از سال ۱۹۶۳ به تصویب رسیده است، سیزده سند پیش از سال ۲۰۰۱ مصوب شده بود؛ اگرچه بدیهی به‌نظر می‌رسد که حمله به مرکز تجارت جهانی و سایر رویدادهای داخل ایالات‌متحده به‌عنوان جایگزین برای توسعه اسناد جدی بین‌المللی عمل کرده است؛ به عنوان نمونه، کنوانسیون سال ۲۰۰۵ برای سرکوب اقدام‌های تروریسم هسته‌ای و راهبرد جهانی ضدتروریستی سازمان ملل متحد طی سال ۲۰۰۶، وفق مبانی قانونی پیشین به تصویب رسیده‌اند.

دولت‌ها مدت‌هاست که نگران استفاده تروریست‌ها از اینترنت برای انجام جرایم تروریستی دیجیتال، گسترش تبلیغات، استخدام و افراط‌گرایی افراد و جمع‌آوری سرمایه هستند. حقوق بین‌الملل برای حمایت از پاسخ به جرایم تروریستی دیجیتال موقعیت مناسبی ندارد، اما فقدان چنین حملاتی تا به امروز انگیزه دولت‌ها را برای توسعه حقوق بین‌المللی در برابر این تهدید تضعیف می کند. در مورد استفاده تروریست‌ها 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 برجسته حقوق بین‌المللی در قبال جرایم تروریستی دیجیتال ایجاد نکرده است (فیدلر[2]، ۲۰۱۶: ٤٧٥).

ارتکاب جرایم تروریستی دیجیتالی مشتمل بر استفاده از اینترنت و سایر اشکال فناوری اطلاعات و ارتباطات برای تهدید یا ایجاد آسیب بدنی برای به‌دست‌آوردن قدرت سیاسی یا عقیدتی از طریق تهدید یا ارعاب است.[3] سرقت داده‌ها، دستکاری داده‌ها و اختلال در خدمات

1. International Legal Instruments to Counterterrorism, U.N. Action to Counter Terrorism. http://www.un.org/terrorism/ instruments.shtml
2. Fidler
۳. بزرگترین تهدید برخط که توسط یک گروه تروریستی غیردولتی ایجاد می‌شود، از ظرفیت آن‌ها برای بهره‌گیری از اینترنت برای مقاصدی غیر از جرایم تروریستی دیجیتالی، نظیر جمع‌آوری سرمایه، تحقیقات هدف و جذب حامیان ناشی می‌شود؛ اگرچه جرایم تروریستی دیجیتالی ممکن است در آینده به وجود بیاید، جرایم برخط و جنگ دیجیتالی تهدیدهای فوری‌تری را ایجاد می‌کنند. البته، جنگ دیجیتالی برای توصیف زمانی استفاده می‌شود که یک کشور از حملات دیجیتالی مانند ویروس‌های رایانه‌ای و هک برای آسیب‌رساندن، کشتن و تخریب سیستم‌های رایانه‌ای حیاتی کشور دیگر استفاده می‌کند. در آینده، هکرها در کنار تسلیحات سنتی نظیر اسلحه و موشک می‌جنگند و با استفاده از کد رایانه‌ای به زیرساخت‌های دشمن حمله می‌کنند. جنگ دیجیتالی به‌عنوان یک جنبه منظم و مرگبار از درگیری بین‌المللی در دنیایی که

ضروری، همه انواع حملات دیجیتالی هستند. به‌دیگر تعبیر، جرایم تروریستی دیجیتالی به‌مثابه رفتارهایی برای هک، انسداد و آلودگی رایانه به منظور محدودیت افراد دارای مجوز قانونی برای دسترسی به منابع رایانه‌ای و کسب و تحصیل غیرمجاز به هرگونه اطلاعاتی است که به منظور امنیت کشور، اطلاعات محدودشده یا روابط خارجی است (راج و یاداو[1]، ۲۰۲۲: ۱۳۸- ۱۳۷).

با بحرانی‌شدن زیرساخت‌های دیجیتالی و کاهش موانع ورود برای عوامل مخرب، جرایم تروریستی 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 حمل‌ونقل نیز می‌توانند مختل شوند که منجر به اختلالات و پریشانی گسترده شود.

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

الف- بدافزار: نرم‌افزارهای مخرب نظیر ویروس‌ها، کرم‌ها، باج‌افزارها می‌توانند برای به‌مخاطره‌افکندن سیستم‌های رایانه‌ای و سرقت اطلاعات حساس، اخلال زیرساخت‌های حیاتی یا ایجاد هرج‌ومرج مورد استفاده قرار گیرند. تروریست‌های دیجیتالی ممکن است بدافزار را برای دسترسی به اهداف خود توسعه دهند یا مستقر کنند.

ب- فیشینگ: حملات فیشینگ مشتمل بر بهره‌گیری از آدرس‌های الکترونیک، وب‌گاه‌ها یا پیام‌های فریبنده برای فریب‌دادن افراد به افشای اطلاعات حساس مانند اعتبار ورود، جزئیات مالی یا داده‌های شخصی است. از این فنون می‌توان برای جمع‌آوری اطلاعات یا دسترسی به سیستم‌های حیاتی استفاده کرد.

ج- مهندسی اجتماعی: فنون مهندسی اجتماعی شامل دستکاری افراد برای افشای اطلاعات محرمانه یا انجام اقداماتی است که ممکن است امنیت را به خطر بیندازند. تروریست‌های دیجیتالی ممکن است برای دسترسی به داده‌ها یا سیستم‌های حساس، هویت افراد یا نهادهای مورد اعتماد را جعل کنند.

هنوز مملو از جاسوسان، هکرها و برنامه‌های تسلیحات دیجیتالی فوق‌سری است، ظاهر شده است. با این حال، اکنون به دلیل رقابت مداوم تسلیحاتی در جنگ دیجیتالی و فقدان دستورالعمل‌های تعریف‌شده حاکم بر مبارزه برخط، خطر واقعی خارج‌شدن سریع موقعیت‌ها از کنترل وجود دارد (Ranger, 2018: 195-197).

1. Raj & Yadav

د- باج‌افزار: باج‌افزار نوعی بدافزار است که داده‌های قربانی را رمزگذاری می‌کند و تا زمان پرداخت باج، غیرقابل‌دسترسی است. تروریست‌های دیجیتالی ممکن است باج‌افزاری را برای مختل‌کردن سیستم‌های حیاتی یا اخاذی از سازمان‌های هدف مستقر کنند.

ه- تهدیدهای داخلی: تهدیدهای داخلی شامل افرادی در یک سازمان می‌شود که به‌نحو عمدی یا غیرعمدی به تروریست‌های دیجیتالی در فعالیت‌های خود کمک می‌کنند. این افراد ممکن است به اطلاعات یا سیستم‌های حیاتی دسترسی داشته باشند.

ر- حمله‌های مشابه استاکس‌نت: استاکس‌نت نمونه معروفی از حملات دیجیتالی هدفمند است که به‌طور خاص با هدف ایجاد اختلال در سیستم‌های کنترل صنعتی، نظیر مواردی که در تأسیسات هسته‌ای استفاده می‌شود، انجام می‌شود. تروریست‌های دیجیتالی ممکن است سیستم‌های زیرساختی حیاتی را هدف قرار دهند تا آسیب فیزیکی یا تخریب ایجاد کنند.[1]

با این همه، تروریست‌های دیجیتالی اغلب از ترکیبی از این روش‌ها برای دستیابی به اهداف خود استفاده می‌کنند و انگیزه‌های آنها می‌تواند بسیار متفاوت باشد؛ از جمله سیاسی، عقیدتی، مالی یا صرفاً ایجاد هرج‌ومرج و اختلال. برای افراد، سازمان‌ها و دولت‌ها بسیار مهم است که اقدامات امنیتی دیجیتالی قوی برای دفاع در برابر جرایم تروریستی دیجیتالی و فنون مختلف آن اجرا کنند (یونگ[2]، ۲۰۲٤: ۱۹۳).

۲. قابلیت‌های جرایم تروریستی دیجیتالی بر نقض امنیت تأسیسات هسته‌ای

بیش از سه دهه است که مشکل جرایم تروریستی دیجیتالی به اشکال مختلف وجود داشته است. از آنجایی که فناوری به طور گسترده‌تری مورد استفاده قرار گرفته است و پتانسیل مجرمانه آن به طور گسترده‌تر شناخته شده است، به نظر می‌رسد برخی از گونه‌های حملات دیجیتالی گزارش‌شده توسط صنعت در مقیاس و وسعت افزایش یافته است (لیو[3] و همکاران، ۲۰۲۳: ۱۲٦-۱۲۵).

---

۱. در صورتی که جرایم دیجیتالی به زیرساخت‌های حیاتی یک کشور نفوذ کرده و ظرفیت ایجاد تخریب در حد یک حمله مسلحانه را داشته باشند، مسلحانه اطلاق می‌شود و دولت بزه‌دیده از حق دفاع مشروع برخوردار خواهد بود. راجع به حمله کرم رایانه‌ای استاکس‌نت در سال ۲۰۱۰ به تأسیسات هسته‌ای ایران، صرف‌نظر از مسأله انتساب آن به عنوان یک امر موضوعی، حق دفاع مشروع قابل‌اثبات است. از این رو، از منظر حقوق بین‌الملل و به استناد مقررات الزام‌آور پیرامون ایمنی تأسیسات هسته‌ای و قطعنامه‌های آژانس بین‌المللی انرژی اتمی، اقدامات خرابکارانه و حمله‌های دیجیتالی در تأسیسات هسته‌ای کشورها ممنوع است. به دیگر تعبیر، وفق چارچوب کلی معاهدات بین‌المللی، هرگونه اقدام خرابکارانه در تأسیسات هسته‌ای که زیر نظر آژانس بین‌المللی انرژی اتمی در حال فعالیت است، نقض اصول حاکم در منشور ملل متحد، اساسنامه آژانس بین‌المللی انرژی اتمی و مغایر با اسناد بین‌المللی الزام‌آور در حوزه ایمنی هسته‌ای اطلاق می‌شود.

2. Jung
3. Leu

جرایم تروریستی دیجیتالی شامل بهره‌گیری از اینترنت و سایر اشکال فناوری اطلاعات و ارتباطات برای تهدید یا ایجاد آسیب بدنی در اخذ قدرت سیاسی یا عقیدتی از طریق تهدید یا ارعاب است.[1] سرقت داده‌ها، دستکاری داده‌ها و اختلال در خدمات ضروری، همه انواع این نوع از جرایم تروریستی دیجیتالی هستند. با بحرانی‌شدن زیرساخت‌های دیجیتال و کاهش موانع ورود برای عوامل مخرب، جرایم تروریستی 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. این نوع از جرایم می‌تواند اثرات مخربی بر طیف وسیعی از افراد و سازمان ها 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 جرایم تروریستی دیجیتالی، زیرساخت‌های حیاتی مانند شبکه‌های برق، بیمارستان‌ها و سیستم‌های حمل‌ونقل نیز می‌توانند مختل شوند که منجر به اختلالات و پریشانی گسترده شود (افتخار[2]، ۲۰۲٤: ۱).

بنابراین، در کنار فناوری در حال توسعه، روش‌های تروریستی نیز پوسته خود را به موازات این فناوری‌های در حال توسعه تغییر می‌دهند و همه کشورهای جهان را با نوع جدیدی از جرم تروریستی، یعنی جرایم تروریستی دیجیتالی، تهدید می‌کنند. اخیراً، فضای دیجیتالی به منطقه‌ای تبدیل شده است که به شدت توسط گروه‌های هکری تحت حمایت دولت و همچنین، گروه‌های تهاجمی مستقل مورد استفاده قرار می‌گیرد (آنانند، کریشنان و دوندرا[3]، ۲۰۱٤: ۱۲۸).[4] این در حالی است که جرایم تروریستی دیجیتالی به دلیل اتکای فزاینده به فناوری اطلاعات در بسیاری از جنبه‌های جامعه و احتمال ایجاد اختلال یا آسیب قابل‌توجه ناشی از جرایم تروریستی دیجیتالی، یک نگرانی فزاینده است که تأثیر قابل‌توجهی در سطح جهانی داشت و هم‌چنان ابعاد گوناگون ثبات یک کشور را مورد تهدید قرار می‌دهد.

---

۱. در بیشتر مواقع، جرایم تروریستی دیجیتالی می‌تواند منجر به مرگ یا آسیب فیزیکی، انفجار، تصادف هواپیما، آلودگی آب یا ضرر اقتصادی یا سیاسی شود. البته، جرایم تروریستی دیجیتالی به‌طور معمول شامل حملاتی با انگیزه سیاسی، عقیدتی یا اجتماعی است که زیرساخت‌های حیاتی را هدف قرار می‌دهد، آسیب قابل‌توجهی به بار می‌آورد یا تهدیدی جدی برای امنیت ملی است. آنچه جرایم تروریستی دیجیتالی را از سایر حملات دیجیتالی متمایز می‌کند، مانند جرایم دیجیتالی، قصد صریح برای تحریک ترور یا بی‌ثبات‌کردن جوامع است که اغلب در تعقیب اهداف سیاسی یا عقیدتی است، نه صرفاً منافع مالی یا تعقیب اهداف اجتماعی یا اخلاقی. جرایم تروریستی دیجیتالی به‌دنبال ایجاد ترس، هرج‌ومرج و بی‌اعتمادی در مقیاس بزرگ‌تر است که اغلب با پتانسیل آسیب یا تخریب در دنیای واقعی همراه است.

2. Iftikhar

3. Anand, Krishnan, & Devendra

٤. به‌عنوان نمونه، می‌توان اذعان داشت گروه تروریستی داعش از جمله فرقه‌هایی است که با مجهزشدن به فناوری‌های پیشرفته دیجیتالی، اقدام به پیشبرد اهداف، تبلیغ ایدئولوژی، جذب مخاطبان و انجام عملیات تروریستی نموده است (هلیلی و سلطانپور، ۱۳۹۹: ٦٨).

جرایم تروریستی دیجیتالی به‌عنوان چهره جدید جرایم تروریستی در قرن جدید قابل‌پیش‌بینی است؛ جایی که تروریست‌ها می‌توانند دروازه‌های یک سد را با حمله الکترونیکی باز کنند، وارد ارتباطات ارتش شوند و اطلاعات گمراه‌کننده را از خود به جا بگذارند، تمام چراغ‌های راهنمایی شهر را متوقف کنند، سیستم را فلج کنند و موجب قطع تلفن‌ها، برق و گاز طبیعی، پیچیدگی سیستم‌های رایانه‌ای و سیستم‌های آب، فروپاشی بخش بانکی و مالی، اختلال در عملکرد امدادرسانی‌های اورژانس، پلیس، بیمارستان‌ها، آتش‌نشانی‌ها و غیره شوند (اوزکیسلالی[1]، ۲۰۰۸: ٥٤).

طی سال‌های اخیر، امنیت دیجیتالی افزایش یافته است و این امر ایمنی نیروگاه‌های هسته‌ای را مجدد در دستور کار قرار داده است. از این رو، در قبال چالش‌ها و تهدیدهای ناشی از ارتکاب جرایم تروریستی دیجیتالی علیه نیروگاه‌ها و تأسیسات هسته‌ای باید سازوکارهای امنیتی مستحکمی اتخاذ شود تا امکان اجرای اینگونه جرایم را به حداقل رساند. لازم به ذکر است برای ایجاد یک دفاع دیجیتالی قوی نسبت به دارایی‌های دیجیتالی حیاتی در تأسیسات هسته‌ای، تجزیه‌وتحلیل گسترده تهدیدها و آسیب‌پذیری‌ها در سیستم‌ها، شبکه‌ها و دستگاه‌ها ضرورتی انکارناپذیر است (ر.ک: نعمت‌پور، تقی‌زاده‌انصاری و ببری‌گنبد، ۱٤۰۰: ۱۷۳-۱٦۹).

با این همه، اتکا به فناوری‌های دیجیتال در سیستم‌های تسلیحاتی مدرن، به ویژه در سیستم‌های تسلیحات هسته‌ای، به نگرانی‌های فزاینده‌ای منجر شده است که جرایم تروریستی دیجیتالی ممکن است خطرات بیشتری را در زمان تشدید درگیری ایجاد کند که می‌تواند اعتماد لازم برای تصمیم‌گیری قابل‌اعتماد را تضعیف کند. البته، آسیب‌پذیری‌های دیجیتالی در سیستم‌ها و ساختارهای تسلیحات هسته‌ای مجموعه‌ای از خطرات را به همراه دارد. در بهترین حالت، ناامنی دیجیتالی در سیستم‌های تسلیحات هسته‌ای احتمالاً اعتماد و اطمینان به قابلیت‌های نظامی و زیرساخت سلاح‌های هسته‌ای را تضعیف می‌کند. در بدترین حالت، حملات دیجیتالی می تواند منجر به اطلاعات اشتباه عمدی و پرتاب سهوی سلاح‌های هسته‌ای شود.

۳. از فرایندهای کُنشی تا دستاوردهای فنی

برای محافظت از داده‌ها، سیستم‌ها و شبکه‌های سیستم های کنترل صنعتی دیجیتال سیمی و بی‌سیم[2] در برابر نفوذ مخرب، درک کامل ظرفیت و انگیزه مهاجم ضروری است. چنین حمله‌هایی می‌تواند برای سرقت فناوری، جاسوسی تجاری، فعالیت دیجیتالی، توسط کارکنان ناراضی یا گروه تروریستی صورت پذیرد. یکی از مهم‌ترین چالش‌هایی که سیستم‌های کنترل

1. Özkışlalı
2. Digital Industrial Control Systems (ICS)

صنعتی و دیجیتالی نوین با آن مواجه هستند، بهره‌برداری‌های سیستمی توسط مهاجمان باانگیزه از منابع خوب و پیچیده است. تأثیر حمله‌های دیجیتالی در سیستم‌های کنترل صنعتی و دیجیتالی هسته‌ای نیز در پیچیدگی حمله منعکس می‌شود، زیرا راه‌اندازی یک حمله دیجیتالی فاجعه‌بار به یک دشمن پیچیده نیاز دارد. از این رو، تجزیه‌وتحلیل تهدید جامع و ابزارهای ارزیابی امنیت سیستم‌های کنترل صنعتی دیجیتال هسته‌ای برای ارزیابی و حفاظت خطر، مناسب و ضروری هستند (آیودجی[1] و همکاران، ۲۰۲۳: ۲۵۸-۲۵۷).

لازم به ذکر است در تأسیسات صنعتی حیاتی، حمله‌های دیجیتالی به‌طور طبیعی به تأثیرات فیزیکی منجر می‌شوند. فضای دیجیتالی یک کانال مناسب و قابل‌تکرار فراهم می‌کند که از طریق آن مهاجم می‌تواند به سیستم فیزیکی دسترسی داشته باشد و به آن آسیب برساند. مسیرهای انتشار حمله به‌عنوان مسیر بالقوه‌ای تعریف می‌شوند که یک عامل تهدید می‌تواند برای دستیابی به اهداف خود از آن استفاده کند.

با توجه به تعامل سیستم در سطوح مختلف در تأسیسات هسته‌ای، نگرانی‌های امنیت دیجیتالی به بهترین وجه توسط یک استاندارد امنیت ملی و بین‌المللی جامع با یک رویه پیاده‌سازی واضح، که توسط سیستم ارزیابی امنیتی دقیق سیستم‌های کنترل صنعتی دیجیتال مدرن اطلاع‌رسانی شده است، مورد توجه قرار می‌گیرد.

٤. شناسایی رویکردهای قانونی

جرایم تروریستی دیجیتالی یکی از روزآمدترین مصادیق جرایم تروریستی است که به سبب بهره‌گیری غیرقانونی از فناوری و ابزارهای الکترونیکی و رایانه‌ای در فضای مجازی، به طور عمده از سوی بازیگرانی که به این علوم نوین دسترسی دارند و آنها را در راه اهداف راهبردی علیه ملت‌های جهان سوم به کار می‌گیرند، موجبات تهدیدهای فزاینده‌ای را در عرصه بین‌المللی فراهم کرده است. از این رو، اسنادی بین‌المللی به منظور پیشگیری و سرکوب کلیه اشکال جرایم تروریستی، به ویژه جرایم تروریستی دیجیتالی، تدوین و تصویب شده است.

٤-١. فرایندهای رویارویی

نظام‌های حقوقی جهانی به‌طور قابل‌توجهی تحت تأثیر جرایم تروریستی دیجیتالی قرار گرفته‌اند. بهره‌برداری از فناوری‌های اطلاعات و ارتباطات توسط تروریست‌ها، به‌ویژه اینترنت و فناوری‌های نوینی که امکان ارتباطات ناشناس را فراهم می‌کند، یک نگرانی فزاینده است. یک راهبرد جامع امنیت دیجیتالی توسط دفتر مبارزه با تروریسم سازمان ملل متحد در حال

1. Ayodeji

توسعه است. دفتر مبارزه با تروریسم سازمان ملل متحد ابتکارات متعددی را در زمینه امنیت دیجیتالی و فناوری‌های نوین راه‌اندازی کرد.

برنامه امنیت دیجیتالی و فناوری‌های نوین با هدف افزایش ظرفیت‌های کشورهای عضو و سازمان‌های خصوصی برای پیشگیری از ارتکاب جرایم دیجیتالی توسط بازیگران تروریست علیه زیرساخت‌های حیاتی نظیر تأسیسات هسته‌ای انجام می‌شود؛ این برنامه به دنبال کاهش تأثیر جرایم دیجیتالی و بازیابی سیستم‌های هدفمند در صورت وقوع چنین حملاتی است. در سال ۲۰۲۲، دفتر مبارزه با تروریسم سازمان ملل متحد و اینترپل ابتکاری را با هدف تقویت ظرفیت‌های مجری قانون و مقامات قضایی کیفری در کشورهای منتخب شریک برای مقابله با بهره‌برداری از فناوری‌های نوین و نوظهور برای اهداف تروریستی و همچنین، حمایت از کشورهای عضو در استفاده از اهرم‌ها راه‌اندازی کردند.[1]

طرح‌های دفتر مبارزه با تروریسم سازمان ملل متحد گذشته بر استفاده از رسانه‌های اجتماعی برای جمع‌آوری اطلاعات منبع باز و شواهد دیجیتالی برای مقابله با جرایم تروریستی و افراط‌گرایی خشونت‌آمیز با رعایت حقوق بشر متمرکز شده‌اند. در طول هشتمین بررسی راهبرد جهانی مبارزه با جرایم تروریستی، مجمع عمومی از دفتر مبارزه با تروریسم و سایر نهادهای مرتبط با پیمان هماهنگی جهانی مبارزه با جرایم تروریستی درخواست کرد تا به طور مشترک از اقدامات و رویکردهای نوآورانه برای ایجاد ظرفیت کشورهای عضو، بر اساس آنها حمایت کنند؛[2] درخواست چالش‌ها و فرصت‌هایی که فناوری‌های نوین از جمله جنبه‌های حقوق بشر در پیشگیری و مقابله با جرایم تروریستی فراهم می‌کند.[3]

نگرانی فزاینده‌ای در مورد سوءاستفاده تروریست‌ها از فناوری‌های اطلاعات و ارتباطات، به‌ویژه اینترنت و فناوری‌های دیجیتالی نوین برای ارتکاب، تحریک، عضوگیری، تأمین مالی یا برنامه‌ریزی ارتکاب جرایم تروریستی وجود دارد. کشورهای عضو در قطعنامه ۲۳۴۱ شورای امنیت (۲۰۱۷)[4] و راهبرد جهانی مبارزه با تروریسم سازمان ملل متحد بر اهمیت همکاری چندجانبه در قبال این تهدید، از جمله در میان سازمان‌های بین‌المللی- منطقه‌ای بخش خصوصی و جامعه مدنی تأکید کرده‌اند.[5]

1. https://www.un.org/counterterrorism/cybersecurity
2. https://documents.un.org/doc/undoc/gen/n23/189/01/pdf/n2318901.pdf
3. https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity
٤. شورای امنیت ملل متحد از طریق قطعنامه ۲۳٤۱ کمیته مبارزه با تروریسم را با حمایت اداره اجرایی کمیته مبارزه با تروریسم هدایت کرد تا تلاش‌های کشورهای عضو برای محافظت از زیرساخت‌های حیاتی نظیر تأسیسات هسته‌ای در قبال جرایم تروریستی را مورد بررسی قرار دهد؛ https://www.un.org/securitycouncil/ctc/tags/%C2%A02341
5. https://documents.un.org/doc/undoc/gen/n17/038/57/pdf/n1703857.pdf

۲-٤. موازین و معیارهای حقوقی

ملاحظات حقوقی و اخلاقی پیرامون جرایم تروریستی در پرداختن به چالش‌های پیچیده ناشی از ارتکاب چنین جرایمی علیه تأسیسات حیاتی و هسته‌ای است. چارچوب حقوقی بین‌المللی و قوانین و مقررات ملی نقش اساسی در تعریف، تعقیب و پیشگیری از جرایم تروریستی دیجیتالی دارند (ر.ک: قدیر و کاظمی‌فروشانی، ۱۳۹۸: ۲٤۳-۲۳۹)؛ به‌عنوان نمونه، سازمان ملل متحد (سازمان ملل متحد) در خط مقدم رسیدگی به دیجیتالی از طریق قطعنامه‌های مجمع عمومی خود بوده است که کشورهای عضو را به همکاری و توسعه هنجارهایی برای رفتار مسئولانه دولت در فضای دیجیتالی تشویق می‌کند (هندرسون[1]، ۲۰۲۱: ٤۷۵).

در چارچوب برخی اسناد بین‌المللی می‌توان نکاتی را در مواجهه با جرایم تروریستی دیجیتالی استنتاج کرد که در این رابطه می‌توان به ماده نخست کنوانسیون مونترال (کنوانسیون در مورد سرکوب اعمال غیرقانونی علیه ایمنی هواپیمایی کشوری) که جرایم را در چارچوب اجرای کنوانسیون تعریف کرده است، اشاره داشت. هرچند شاید از حیث حقوقی و فنی فاصله‌ای قابل‌ملاحظه با این نوع از جرم در متن ماده وجود داشته باشد، اما در هر حال، کنوانسیون در این رابطه مراتبی را تقریر و نوع نگاه خود را معطوف به شناخت جرم و نحوه کیفرگذاری کرده است.[2]

در ضمن، باید اذعان داشت ماده ۲ کنوانسیون بین‌المللی، بمب‌گذاری‌های تروریستی جرایم را در چارچوب اجرای کنوانسیون تعریف کرده است. این ماده شامل سه دسته از جرایم می‌شود: جرایم ارتکابی از سوی مرتکب اصلی، مبادرت به ارتکاب جرم و هر نوع معاونت در جرم‌بندهای زیر به ارزیابی کاربردپذیری کنوانسیون بین‌المللی بمب‌گذاری‌های تروریستی در مورد جرایم تروریستی دیجیتالی پرداخته‌اند. جرایم مندرج در ماده (۱) ۲ کنوانسیون بین‌المللی منع بمب‌گذاری‌های تروریستی، عناصر متعددی را در برمی‌گیرند؛ چرا که جرایم تروریستی دیجیتالی و جرم تروریستی فیزیکی تنها از نظر عمل انجام‌شده با یکدیگر تفاوت دارند و از نظر حالت ذهنی تروریست مجری آن عمل، فرقی بین آنها نیست. دو گزینه مرتبط با نیت مجرم تحلیل نخواهند شد. تروریست شبکه‌ای همان مقاصد یک تروریست عادی را دارد و از این رو، هیچ تفاوت حقوقی در اطلاق قصد به آن وجود ندارد.[3]

---

1. Henderson
2. ICAO, International Conference on Air Law: Minutes and Documents, ICAO Doc. 9801, p. 21, Delegates of France and Japan (hereinafter: "ICAO Documents").
۳. طبق تعریف مقررشده در ماده (۳) ۱ کنوانسیون بین‌المللی منع بمب‌گذاری‌های تروریستی مواد منفجره یا ادوات مرگبار دیگر، یکی از دو تفسیر احتمالی را بیان می‌کند؛ نخست، می‌تواند به این معنا باشد: ماده منفجره یا سلاح و ادوات آتش‌زا که برای تسبیب مرگ، جراحات بدنی جدی یا ضرر مالی اساسی طراحی شده یا قابلیت آن را داشته باشد. یک زیرساخت رایانه‌ای‌شده احتمالاً واجد شرایط این تفسیر نیست. می‌توان از رایانه برای چکاندن بمب استفاده کرد، اما رایانه

بر اساس پیش‌نویس کنوانسیون جامع مقابله با تروریسم بین‌المللی، هر کشور عضو می‌پذیرد جرایم مندرج در ماده ۲ را به موجب حقوق داخلی خود، جرم کیفری قلمداد کند. پیش‌نویس کنوانسیون به مسائل صلاحیت قضایی، همکاری بین کشورها، محاکمه و اجرای معیارها و مانند آن نیز پرداخته است.[1] ماده (ب) (۱) ۲ تصریح می‌کند: «هر شخص در حیطه معنایی این کنوانسیون، در صورتی مرتکب جرم شده که به هر طریق و وسیله، به طور غیرقانونی و عمدی، باعث صدمات جدی به اموال دولتی یا شخصی، ازجمله اماکن عمومی، تأسیسات کشوری یا دولتی، سیستم حمل‌ونقل عمومی و تأسیسات زیرساختی یا محیط‌زیست شود تا از طریق مرعوب‌ساختن مردم، یک دولت یا سازمان بین‌المللی را به انجام یا خودداری از انجام هر عملی وادار کند.»

اشاره ماده (ب) (۱) ۲ پیش‌نویس کنوانسیون جامع مقابله با تروریسم بین‌المللی به «هر طریق و وسیله» در کنار تعریف «تأسیسات زیرساختی» ازجمله ارتباطات، مخابرات و شبکه‌های اطلاعاتی، کاربرد جرم مندرج در پیش‌نویس کنوانسیون را برای ارتکاب جرایم تروریستی دیجیتالی امکان‌پذیر می‌سازد؛ زبانِ آن به قدری گسترده و واضح است که می‌تواند به طور مستقیم به جرایم تروریستی دیجیتالیِ رسیدگی کند؛ مزیت اصلی آن نیز این است که نیازی به تکیه‌کردن بر روش‌های تفسیری ندارد تا مورد مخالفت نمایندگان یک مکتب فکری یا حقوقی متفاوت قرار بگیرد.

در سال ۲۰۰۱، شورای اروپا «کنوانسیون جرم سایبری» را تصویب کرد.[2] کنوانسیون جرم سایبری دستاورد چهار سال تلاش کارشناسان شورای اروپا، ایالات متحده، کانادا، ژاپن و کشورهای دیگر است که در انتظار امضای تمامی کشورهاست. همان گونه که در پیش‌گفتار مقرر شده است، هدف اصلی کنوانسیون جرم سایبری، پیگیری یک سیاست کیفری هماهنگ و مشترک با هدف حفاظت از جامعه در برابر جرم دیجیتال، به ویژه با به‌کارگیری قانون‌گذاری مناسب و تقویت همکاری بین‌المللی است؛ هرچند اصطلاح «جرم دیجیتال» به مضمون جرمی است که در اینترنت یا از طریق اینترنت واقع می‌شود، چارچوب عمل کنوانسیون جرم سایبری فراتر از این حد و شامل جرایمی است که با استفاده از رایانه واقع می‌شوند یا جرایمی که در کل، رایانه‌ها را دخالت می‌دهند.

به‌خودی‌خود نمی‌تواند مانند یک بمب عمل کند.

1. Draft Convention, Report of the Ad-Hoc Committee established by General Assembly resolution 51/210 of December 1996, General Assembley Official Records, fifty-seven session, Supplement no. 37 UN Doc
2. Council of Europe Convention on Cybercrime, Nov. 8, 2001, E.T.S. 185. (hereinafter “Convention on Cybercrime”).

در اگوست ۲۰۰۰، کارشناسان «دانشگاه استانفورد» طرحی پیشنهادی را برای کنوانسیون بین‌المللی جرم و جرم تروریستی ارائه کردند. این پیش‌نویس که مبتنی بر کنوانسیون جرم سایبری شورای اروپاست، جرم‌انگاری رفتارهای متعدد از قبیل استفاده از سیستم‌های دیجیتالی برای اجرای جرایم تعیین‌شده در سایر معاهدات خاص[1] و هدف‌گیری زیرساخت‌های بحرانی را پیشنهاد داده است.[2] از طرفی، پیش‌نویس یادشده تأسیس یک آژانس بین‌المللی را نیز برای حفاظت از زیرساخت اطلاعاتی پیشنهاد داده که جایگاهی برای کنکاش در خصوص وضع استانداردها و شیوه‌های مرتبط با امنیت دیجیتالی است.[3]

پیش‌نویس استانفورد، برخلاف کنوانسیون جرم سایبری شورای اروپا، به‌طور اختصاصی به تطابق بین زیرساخت مبتنی بر ارتباطات رایانه‌ای و جرم تروریستی می‌پردازد. پیش‌نویس استانفورد برخلاف پیش‌نویس کنوانسیون جامع، به وضوح تصریح کرده است که برای فعالیت‌های مربوط به درگیری مسلحانه جاری کاربردی ندارد.[4]

کنوانسیون بوداپست در مورد جرایم دیجیتالی، همچنین معروف به کنوانسیون شورای اروپا در مورد جرایم دیجیتالی، یک معاهده چندجانبه با هدف هماهنگ‌کردن قوانین و تقویت همکاری بین‌المللی در مبارزه با جرایم دیجیتالی است که شامل مقررات مربوط به جرایم تروریستی دیجیتالی است (ویکی بیرچلر[5]، ۲۰۲۰: ۶۹-۶۸).

با این حال، اقدامات اتخاذشده در قبال جرایم تروریستی دیجیتالی که موجبات نقض امنیت تأسیسات هسته‌ای را موجب می‌شود، باید متناسب و با رعایت حقوق فردی باشد. تعقیب تروریست‌های دیجیتالی شامل فرآیندهای قانونی است که باید مدارک دیجیتالی، زنجیره بازداشت و همکاری بین‌المللی را در نظر بگیرد. تضمین پاسخگویی برای جرایم تروریستی دیجیتالی تحت حمایت دولت می‌تواند پیچیده باشد؛ زیرا ممکن است شامل مذاکرات دیپلماتیک، حقوق بین‌المللی و ملاحظات سیاسی باشد. پیشگیری از جرایم تروریستی دیجیتالی شامل رسیدگی به علل و آسیب‌پذیری‌های ریشه‌ای، مانند بهبود امنیت دیجیتالی، مقابله با رادیکال‌سازی و ترویج همکاری بین‌المللی برای بازدارندگی عوامل مخرب است. حمایت از حقوق بشر در زمینه امنیت دیجیتالی و مقابله با جرایم تروریستی دیجیتالی ضروری است، زیرا اقدامات بیش از حد گسترده یا تهاجمی می‌تواند آزادی‌های فردی را نقض کند.

1. Article 3 refers to the following: Tokyo Convention, supra note 14; Hague Convention, supra note 14; Montreal Convention, supra note 14; Hostage Convention, supra note 14; Terrorist Bombings Convention, supra note 14.
2. Convention on Cybercrime, supra note 123, E.T.S. 185 at Art. 3.
3. Id. at Art. 12.
4. Id. at Art. 20.
5. Wicki-Birchler

به‌طور کلی، ملاحظات حقوقی و اخلاقی پیرامون جرایم تروریستی دیجیتالی شامل تعامل پیچیده‌ای از چارچوب‌های حقوقی بین‌المللی، مقررات ملی و معضلات اخلاقی است.

۳-٤. سازوکارهای عملیاتی

با توجه به اینکه جرایم دیجیتالی اغلب از خارج از مرزهای ملی انجام می‌شود، همکاری بین‌المللی نیز در مبارزه با چنین جرایمی ضروری است. برای تشویق تبادل داده‌ها و تحقیقات مشترک، بسیاری از کشورها اتحادها و موافقت‌نامه‌هایی را تشکیل داده‌اند؛ البته، اقدامات حقوقی بین‌المللی متنوعی برای مبارزه با جرایم تروریستی دیجیتالی صورت گرفته است که از آن جمله می‌توان به ایجاد چارچوب‌های حقوقی بین‌المللی، تدوین قوانین و مقررات ملی، ایجاد واحدهای تخصصی برای مبارزه با جرایم دیجیتالی و تشویق همکاری‌ها و مشارکت‌های جهانی اشاره کرد (ر.ک: جان‌پرور، صالح‌آبادی و احمدی، ۱۳۹۷: ۱۲۲-۱۲۱). انتظار می‌رود با توسعه جرایم تروریستی دیجیتالی، به‌ویژه ارتکاب جرایم موصوف علیه تأسیسات هسته‌ای، کشورها به توسعه و تطبیق اقدامات و سیاست‌های قانونی برای مدیریت این تهدید در حال گسترش ادامه دهند.

در هر حال، یک دولت باید برای رویارویی با چالش جرایم تروریستی دیجیتالی بتواند با اتخاذ راهبردهایی در قبال چنین جرایمی، امکان حفاظت در مقابل تهدیدهای ناشی از آن را فراهم نماید که مشتمل بر موارد ذیل است (باستوق[1] و همکاران، ۲۰۲۳: ۳٦-۳٤):

الف- آموزش و آگاهی: ترویج آموزش امنیت دیجیتالی و آگاهی در میان مردم، کارکنان دولت و اپراتورهای زیرساخت حیاتی برای اطمینان از آگاهی افراد و سازمان‌ها از تهدیدات بالقوه و نحوه کاهش آنها ضروری است.

ب- دفاع دیجیتالی ایمن: توسعه و حفظ اقدامات امنیتی دیجیتالی قوی، از جمله سیستم‌های تشخیص نفوذ و نرم‌افزار آنتی‌ویروس، برای پیشگیری و پاسخگویی موثر به حملات دیجیتالی بسیار مهم است.

ج- همکاری بین‌المللی: همکاری با سایر کشورها و سازمان‌های بین‌المللی برای به‌اشتراک‌گذاشتن اطلاعات تهدید، تحقیق در مورد حوادث دیجیتالی و ایجاد یک پاسخ جهانی هماهنگ به جرایم تروریستی دیجیتالی ضروری است.

1. Bastug

د- تحقیق و توسعه: سرمایه‌گذاری در تحقیق و توسعه امنیت دیجیتالی برای پیشی‌گرفتن از تهدیدهای نوظهور و توسعه فناوری‌ها و راهبردهای نوآورانه برای محافظت در قبال جرایم تروریستی دیجیتالی ضرورت دارد.

ه- پاسخ به حوادث دیجیتالی: ایجاد یک طرح واکنش به حادثه به‌خوبی‌تعریف‌شده به مدیریت مؤثر و کاهش تأثیر حوادث دیجیتالی در هنگام وقوع کمک می‌کند.

ر- چارچوب قانونی قابل‌اتکاء: اجرای قوانین و مقررات امنیت دیجیتالی مبنای قانونی را برای تعقیب مجرمان دیجیتالی و بازدارندگی عوامل مخرب فراهم می‌کند.

ز- قراردادها و هنجارهای بین‌المللی: مشارکت و ترویج موافقت‌نامه‌ها، هنجارها و معاهدات بین‌المللی مرتبط با فضای دیجیتالی می‌تواند به ایجاد قواعد رفتار و همکاری در حوزه دیجیتال کمک کند.

ژ- نظارت و اطلاعات مستمر: نظارت مستمر بر شبکه‌ها و سیستم‌ها، همراه با جمع‌آوری و تجزیه‌وتحلیل اطلاعات، امکان شناسایی زودهنگام تهدیدات دیجیتالی و تصمیم‌گیری بهتر در پاسخ به آن تهدیدات را فراهم می‌کند.

ح- همکاری با بخش خصوصی: همکاری با سازمان‌های بخش خصوصی که اغلب زیرساخت‌های حیاتی را در اختیار دارند و اداره می‌کنند، حیاتی است. مشارکت‌های عمومی و خصوصی می‌تواند اشتراک‌گذاری اطلاعات را بهبود بخشد و اقدامات امنیت دیجیتالی را افزایش دهد.

با اجرای این اقدامات متقابل، دولت‌ها می‌توانند به طور قابل‌توجهی مقاومت خود را در برابر جرایم تروریستی دیجیتالی و سایر تهدیدهای دیجیتالی بهبود بخشند. تطبیق و تکامل این اقدامات برای رسیدگی به ماهیت در حال تحول تهدیدات دیجیتالی و فعال‌ماندن در حفاظت از امنیت ملی و زیرساخت‌های حیاتی مهم است.

۵. چشم‌انداز و آینده‌انگاری

خطرات امنیت دیجیتالی در سال‌های اخیر افزایش یافته است و این امر ایمنی نیروگاه‌های هسته‌ای را دوباره در دستور کار قرار داده است. کشورها در جغرافیای خود با بسیاری از سازمان‌های تروریستی در حال مقابله هستند. اکثر این سازمان‌ها ظرفیت حمله به نیروگاه‌های هسته‌ای را دارند. در برابر چنین حملاتی اعم از این‌که در محیط دیجیتالی و یا فیزیکی باشند، باید تدابیر امنیتی لازم اتخاذ شود (راج و یاداو[1]، ۲۰۲۲: ۱۴۲-۱۴۱).

1. Raj & Yadav

سیاست‌های امنیت دیجتالی باید به‌طور مداوم با رویکردی نوآورانه روزآمد شوند. تغییرات و تحولات در فضای مجازی به قدری سریع رخ می‌دهد که ضمن توسعه همه این اقدامات، باید تعادل خوبی بین همه حوزه‌ها مانند امنیت ملی، حقوق و آزادی‌های شخصی، دموکراسی، هزینه‌ها و منافع سرمایه‌گذاری برقرار شود. اقدامات احتیاطی برای حفاظت از زیرساخت‌های حیاتی بسیار مهم است. نباید فراموش کرد که زمانی می‌توان امنیت را تضمین کرد که تمامی عناصر موجود در سیستم‌ها به‌طور کامل وظایف خود را انجام دهند. با این حال، علی‌رغم تمام اقدامات احتیاطی، در صورت حمله در مقیاس بزرگ، سیستم‌ها و گروه‌های واکنش اضطراری نقش مهمی در غلبه بر اثرات منفی به طور موثر ایفا خواهند کرد. به منظور افزایش سطح بازدارندگی دیجیتالی باید تمهیدات قانونی لازم تکمیل و تلاش برای همکاری مؤثر بین‌المللی تسریع شود (بائ جانگ[1] و همکاران، ۲۰۲۰: ۱۳۳۶-۱۳۳٤).

علاوه بر این، آموزش‌ها و شیوه‌های امنیت دیجیتالی در تمام مراحل و در تمام سطوح که باعث افزایش آگاهی می‌شود، باید مورد حمایت قرار گیرد. با توجه به اینکه مطالعات فردی در حفاظت از زیرساخت‌های حیاتی ناکافی خواهد بود، اتخاذ رویکرد اشتراک اطلاعات و همکاری بین بخش‌ها و نهادها به منظور ایجاد وحدت ضروری است.

بحث و نتیجه‌گیری

با توجه به رشد فزاینده استفاده از اینترنت و حرکت شتابان کشورها به سوی الکترونیکی‌کردن خدمات اجتماعی، اقتصادی و تأثیر انقلاب اطلاعاتی بر بهبود فناوری‌های نظامی، امنیت بین‌المللی در سال‌های آتی با تهدیدها و چالش‌های نوینی مواجه خواهد شد. بدیهی است که کاهش آسیب‌پذیری‌ها و تقویت امنیت و صلح در مقابل تهدیدات نوظهور و بازیگران جدید و رهایی از جرایم تروریستی و به‌ویژه ارتکاب چنین جرایمی علیه تأسیسات هسته‌ای، مستلزم پرداختن به مطالعات آینده‌پژوهی در زمینه تأثیر انقلاب اطلاعاتی بر امنیت ملی، تهدیدهای فضای دیجیتالی و ارتقای قابلیت‌های فنی و آگاهی عمومی از این تهدیدها و همچنین، در بهره‌گیری در خصوص دانش و اطلاعات مرتبط است.

جرایم تروریستی دیجیتالی مادام که علیه تأسیسات هسته‌ای ارتکاب یابد، مشتمل بر بهره‌برداری از فناوری‌های رایانه‌ای و مبتنی بر اینترنت برای ارتکاب رفتارهای خشونت‌آمیز است. تلاش‌های جهانی برای افزایش امنیت دیجیتالی و تقویت انعطاف‌پذیری سیستم‌های حیاتی در برابر این حملات که نگرانی فزاینده‌ای برای دولت‌ها و کسب‌وکارها است، در حال انجام است. با این حال، علی‌رغم این تلاش‌ها، جرایم تروریستی دیجیتالی هم‌چنان یک تهدید

1. Bae Jang

مهم است. این امر به دلیل ماهیت دائمی در حال تغییر اینترنت و همچنین، اتکای روزافزون به فناوری در کلیه ابعاد جامعه به علت استفاده روزافزون از فناوری است. برای محافظت از خود در برابر این تهدید، افراد و سازمان‌ها باید هوشیار باشند و تدابیر امنیتی خود را به طور مرتب به‌روز کنند تا در برابر آن محافظت شوند.

آسیب‌های اقتصادی و اعتباری واردشده توسط سازمان‌ها و دولت‌ها، نیاز به راهبردهای امنیت دیجیتالی قوی را نشان می‌دهد. با این حال، محدودیت‌هایی شامل چالش‌هایی در دستیابی به داده‌های جامع به دلیل گزارش‌دهی کم، ماهیت پویای تهدیدات دیجیتالی است که به سرعت در حال تکامل هستند. علاوه بر این، اندازه‌گیری اثربخشی اقدامات متقابل همچنان یک تلاش پیچیده است و انطباق آنها با محدودیت‌های منابع و فنون مهاجم در حال تکامل مانع می‌شود. از آنجایی که جرایم تروریستی دیجیتالی و به‌ویژه این نوع از جرایم که موجبات نقض تأسیسات هسته‌ای را فراهم می‌آورند، یک موضوع همیشه در حال تحول است، تحقیقات آینده می‌تواند بر روی یافتن تأثیر سیاست‌های خاصی که توسط برخی کشورها ایجاد شده است، بر جرایم تروریستی دیجیتالی هسته‌ای تمرکز کند.

منابع

– قدیر، محسن و کاظمی‌فروشانی، حسین. (۱۳۹۸). بررسی تطبیقی حقوق کیفری ایران با اسناد بین‌المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری. *حقوقی بین‌المللی*، ۶۰(۳۶)، ۲۶۷–۲۳۸.

https://www.cilamag.ir/article_35084.html

–جان‌پرور، محسن؛ صالح‌آبادی، ریحانه و احمدی، سیروس. (۱۳۹۷). کنترل تروریسم سایبری با مدیریت مرزهای فضای سایبر راهبردی. *مطالعات قدرت نرم*، ۸(۱۹)، ۱۲۵–۹۹.

https://www.spba.ir/article_99339.html

–نعمت‌پور، اردشیر؛ تقی‌زاده‌انصاری، مصطفی و ببری‌گنبد، سکینه. (۱۴۰۰). مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور در قواعد حقوق بین‌الملل. *مطالعات بین‌المللی*، ۳(۷۱)، ۱۶۵–۱۸۵.

https://www.isjq.ir/article_165395.html

–هلیلی، خداد؛ سلطانپور، محمدرضا. (۱۳۹۹). تهدیدات تروریسم سایبری و واکاوی تحرکات گروه تروریستی داعش در فضای سایبر. *مطالعات جنگ*، ۲(۷)، ۸۳–۶۸.

https://www.qjws.ir/article_249183.html

- Ayodeji, Abiodun, Mokhtar Mohamed, Li Li, Antonio Di Buono, Iestyn Pierce, Hafiz Ahmed (2023). *"Cyber Security in the Nuclear Industry: A Closer Look at Digital Control Systems, Networks and Human Factors",* Progress in Nuclear Energy, 161: 243-284.
https://www.sciencedirect.com/science/article/pii/S0149197023001737

-Anand, K., Krishnan, P., & Devendra, K. P. (2014). "Facing the Reality of Cyber Threats in the Power Sector", *Energy Policy*, 65: 126-133.
https://dergipark.org.tr/tr/pub/joltida/article/1198842

-Bastug MF, Onat I, Guler A (2023). "Threat Construction and Framing of Cyberterrorism in the U.S. News Media", *International Journal of Cybersecurity Intelligence & Cybercrime*, 6(1):29–44.
https://vc.bridgew.edu/ijcic/vol6/iss1/3/

-Bae Jang, Kyung, Chang Hyun Baek & Tae Ho Woo (2020). "Protocol Construction for Preventing the Cyber Nuclear Terrorism in the Nuclear Power Plants (NPPs) Using the Nonlinear Algorithm", *Journal of Nuclear Science and Technology*, 57(12): 1331-1338.
https://www.tandfonline.com/doi/full/10.1080/00223131.2020.1789007

-Case, D. U. (2016). "*Analysis of the cyber-attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC)*", 388: 1-29.
https://dergipark.org.tr/en/pub/jep/issue/81893/1399365

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

https://peerj.com/articles/cs-1772/
-Fidler, David P (2016). "Cyber Space, Terrorism and International Law Get Access Arrow", *Journal of Conflict and Security Law*, 21(3): 475-493.
https://www.researchgate.net/publication/308339234_Cyberspace_Terrorism_and_International_Law
-Jung, Yujin J. (2024). "Cyber Shadows over Nuclear Peace: Understanding and Mitigating Digital Threats to Global Security", *Journal of Asian Security and International Affairs*, 11(2): 281-204.
https://ideas.repec.org/a/sae/asseca/v11y2024i2p233-253.html
-Kur, Hüseyin (2023). "Cyber Terror Threats Against Nuclear Power Plants", *Journal of Learning and Teaching in Digital Age*, 8(2), 237-244.
https://dergipark.org.tr/en/pub/joltida/issue/78765/1198772
-Leu DM, Udroiu C, Raicu GM, Gârban HN, Şcheau MC (2023). "Analysis of Some Case Studies on Cyberattacks and Proposed Methods for Preventing Them", *Romanian Journal of Information Technology & Automatic Control*/Revista Română de Informatică şi Automatică, 33(2):119–134.
https://www.researchgate.net/publication/371947489_Analysis_of_some_case_studies_on_cyberattacks_and_proposed_methods_for_preventing_them
-Özkışlalı, G. (2008). Globalization, the Internet and the Changing Face of Terrorism; Cyber Terrorism. *Published Master's Thesis*, Hacettepe SBE, Ankara, 71.
-Jang, K.B., C.H. Baek, T.H. Woo (2022). "Assessment for Nuclear Security Using Analytic Hierarchy Process (AHP) incorporated with Neural Networking Method in Nuclear Power Plants (NPPs)", *Kerntechnik*, 87: 607-614.
https://www.semanticscholar.org/paper/Assessment-for-nuclear-security-using-Analytic-with-Jang-Baek/e75f679b38f96d58ef69b5071c3b4916ebeeca60
-Onderco, M., M. Zutt (2022). "Emerging Technology and Nuclear Security: What Does the Wisdom of the Crowd Tell Us?", *Contemporary Security Policy*, 42: 286-311.
https://www.tandfonline.com/doi/full/10.1080/13523260.2021.1928963
-Hawila, M.A., S.S. Chirayath (2018). "*Combined Nuclear Safety-Security Risk Analysis Methodology Development and Demonstration Through a Case Study*", Progress in Nuclear Energy, 105: 153-159.
https://www.researchgate.net/publication/324867583_Combined_nuclear_safety-security_risk_analysis_methodology_development_and_demonstration_through_a_case_study
-Hellman, M.E. (2017). "*Cybersecurity, Nuclear Security, Alan Turing, and Illogical Logic*", Communications of the ACM, 60: 52-59.
https://cacm.acm.org/research/cybersecurity-nuclear-security-alan-turing-and-illogical-logic/
-Henderson C. çinde Nicholas Tsagourias ve Russell Buchan (2021). "International law and cyberspace", *Research handbooks in international law*, (Edward Elgar, 2015); 2021. The United Nations and the regulation of cybersecurity, pp. 474–475.
https://sussex.figshare.com/articles/chapter/The_United_Nations_and_the_regulation_of_cybersecurity/23448347?file=41157845
-Lovering, J.R., A. Abdulla, G. Morgan (2020). "Expert Assessments of Strategies to Enhance Global Nuclear Security", *Energy Policy*, 139: 1-9.
https://www.tandfonline.com/doi/abs/10.1080/10736500.2022.2130457
-Raj, P., & Yadav S. (2022). "*Cyber Terrorism: A Threat to Cyber World. Emerging Trends in Technology & its Impact on Law*", 1.
https://dergipark.org.tr/en/download/article-file/2348831
-Ranger, S (2018). "What is Cyberwar? Everything you Need to Know About the Frightening Future of Digital Conflict", *ZDNET*.
https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/
-Shubayr, Nasser (2024). "Nuclear Security Measures: A Review of Selected Emerging Technologies and Strategies", *Journal of Radiation Research and Applied Sciences*, 17(1): 1-11.
https://www.researchgate.net/publication/378640887_Nuclear_security_measures_A_review_of_selected_emerging_technologies_and_strategies

-Tavares, R.L., O.A. Robson de, W. Giozza (2022). “Effectiveness Evaluation of a Nuclear Facility Security System Under a Cyber-Physical Attack Scenario”, *17th Iberian Conference on Information Systems and Technologies (CISTI),* 22-25 June. https://ieeexplore.ieee.org/document/9820179.
-Wicki-Birchler D (2020). “The Budapest Convention and the General Data Protection Regulation: Acting in Concert to Curb Cybercrime?”, *International Cybersecurity Law Review*,1:63–72.
https://www.researchgate.net/publication/346246542_The_Budapest_Convention_and_the_General_Data_Protection_Regulation_acting_in_concert_to_curb_cybercrime