Scientific Journal of Military Sciences Research

11

Vol. 6
Spring-Summer
2025

Research Paper

Received:
2024/07/19
Revised:
2025/03/04
Accepted:
2025/05/08
p.p:61-91

ISSN:2717-3682
E-ISSN:2717-3690

An Analysis of Terrorist Crimes in the Age of Digitalization and Countermeasures

Hassan, Nouri Pashaie [1] | Ezzati, Mohammad [2]

Abstract

The digital age has today become an inseparable part of the life of all humanity, acting in many cases like a double-edged sword. Just as it has had a significant impact on the development and dissemination of science, it also has a considerable effect on the expansion of terrorist crimes. This article analyzes the forms of such criminal activities committed by terrorist groups in the digital space using digital technologies, including the dissemination of violent ideology and propaganda of terrorist activities, recruitment and training of new members, the use of digital technologies in the process of preparatory and direct terrorist activities, and financing. It can be observed that the development of the digital space and digital technologies greatly facilitates terrorism and also leads to changes in the mechanism of committing terrorist crimes. It is concluded that in order to ensure the effectiveness of measures to counter terrorist crimes in the digital space and the use of digital technologies, a clear strategy and an appropriate legal framework are required.

Keywords: Recruitment; Crime; Propaganda; Terrorist Financing; Digital Technologie

1. Command and Staff University (DAFOOS), Faculty of War, Tehran ✉ hassan.nouri.pashaie80@gmail.com
2. Imam Ali Officer University, Tehran, Iran

«تحلیلی بر انجام جنایات تروریستی در عصر دیجیتالی شدن و اقدامات متقابل»

پاشایی و ...

نشریه علمی پژوهش‌های علوم نظامی

۱۱

سال ششم
بهار و تابستان ۱۴۰۴

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۴/۲۹
تاریخ بازنگری:
۱۴۰۳/۱۲/۱۴
تاریخ پذیرش:
۱۴۰۴/۰۲/۱۸

صص: ۹۰-۶۱

شاپا چاپی: ۳۶۸۲-۲۷۱۷
الکترونیکی: ۳۶۹۰-۲۷۱۷

تحلیلی بر انجام جنایات تروریستی در عصر دیجیتال شدن و اقدامات متقابل

نوری پاشایی، حسن [۱] ✉ | عزتی، محمد [۲]

چکیده:

عصر دیجیتال امروزه بخش جدایی‌ناپذیر زندگی تمامی بشریت است که در بسیاری از موارد مانند شمشیر دو لبه عمل کرده و همان‌گونه که در توسعه و انتشار علم تأثیری بسزا داشته است، در گسترش انجام جنایات تروریستی نیز تأثیر بسزایی دارد. این مقاله به تجزیه و تحلیل اشکال چنین فعالیت‌های جنایی گروه‌های تروریستی متعهد در فضای دیجیتال با استفاده از فناوری‌های دیجیتال، مانند گسترش ایدئولوژی خشونت و تبلیغات فعالیت‌های تروریستی، استخدام اعضای جدید و آموزش آن‌ها، استفاده از فناوری‌های دیجیتال در روند فعالیت‌های مقدماتی و مستقیم تروریستی، تأمین مالی پرداخته است. می‌توان دریافت که توسعه فضای دیجیتال و فناوری‌های دیجیتال به شدت تروریسم کمک می‌کند و همچنین منجر به تغییر در مکانیسم ارتکاب جرایم تروریستی می‌شود. نتیجه‌گیری می‌شود که به منظور اطمینان از اثربخشی اقدامات برای مقابله با جنایات تروریستی در فضای دیجیتال و استفاده از فناوری‌های دیجیتال، یک استراتژی روشن و یک چارچوب قانونی مناسب مورد نیاز است.

واژگان کلیدی: کلمات کلیدی: استخدام، جرم، تبلیغات، تروریسم مالی، فناوری‌های دیجیتال

۱. دانشگاه فرماندهی و ستاد، دانشکده جنگ، تهران hassan.nouri.pashaie80@gmail.com ✉
۲. دانشگاه افسری امام علی ﷺ نزاجا

بیان مسئله

انسان برای رسیدن به موفقیت و دستیابی به اهداف والای انسانی خود بعد از برآوردن نیازهای فیزیولوژیکی که اساس موجودیتش را تشکیل می‌دهد، نیاز به وجود امنیت دارد. فرایند اجتماعی بنیادین با امنیت را می‌توان نوعی ویژگی‌های خودجوش دانست که هدف آن به وجود آوردن فضاهای اجتماعی سیاسی، اقتصادی نسبتاً امن است. جوامع امن به افراد امکان می‌دهند تا زندگی کنند، تحرک داشته باشند و به فرهنگ، زبان و هویت‌شان بدون هراس از تهدیدهای خشونت‌آمیز مستقیم و غیر مستقیم وفادار بمانند. بدین ترتیب امنیت یکی از اساسی‌ترین نیازهای اجتماعی است که افراد جامعه باید از آن برخوردار باشند. آیا فضای دیجیتال باعث گسترش جنایات تروریستی می‌شود و بدین ترتیب یکی از اساسی‌ترین نیازهای اجتماعی بشر یعنی امنیت را به خطر می‌اندازد؟ آیا راهکارهایی برای جلوگیری از گسترش انجام اقدامات تروریستی در بستر فضای دیجیتالی وجود دارد؟

سؤال و هدف

یکی از عوامل اثرگذار در حوزه احساس امنیت عمومی کشورها، تروریسم است که همواره و از گذشته-های دور به عنوان یک عامل تهدیدکننده برای امنیت کشورها مطرح بوده است. امروزه این پدیده به یکی از مهم‌ترین دغدغه‌های امنیتی ملت‌ها و دولت‌ها در سراسر جهان تبدیل شده است. رواج پدیده تروریسم منحصر به منطقه و یا دولت خاصی نیست، بلکه از کشورهای کوچک کمتر توسعه یافته تا بزرگ‌ترین قدرت‌های دنیا به نحوی با این معضل امنیتی مواجه هستند. کشور ایران به دلیل واقع شدن در منطقه حساس خاورمیانه با تهدیدها، مخاطره‌ها، چالش‌ها و تحولات عمده‌ای در محیط امنیتی خود روبه‌رو است. واقعیت این است که محیط راهبردی ایران از جمله امنیت ملی در معرض تهدیدهای تروریستی قرار دارد. بعضی از نقاط کشور، خصوصاً مناطق مرزی دستخوش حوادث و ناامنی‌های متعددی از سوی گروه‌های تروریستی بوده و باعث واردشدن آسیب به نیروها و امکانات کشور گردیده است (مهدی قنبری، ۱۳۹۸).

حال سؤال این است که آیا اقدامات تروریستی در بستر فضای دیجیتالی در کشور ما قابلیت گسترش را دارد؟ این مقاله به تجزیه و تحلیل چنین اشکال فعالیت‌های جنایی گروه‌های تروریستی متعهد در فضای دیجیتال با استفاده از فناوری‌های دیجیتال، مانند گسترش ایدئولوژی خشونت و تبلیغات

فعالیت‌های تروریستی، استخدام اعضای جدید و آموزش آن‌ها، استفاده از فناوری‌های دیجیتال در روند فعالیت‌های مقدماتی و مستقیم تروریستی، تأمین مالی پرداخته است.

مبانی نظری و ادبیات

برپایه نوشته دانشنامه بریتانیکا، تروریسم به معنی کاربرد نظام‌مند ارعاب خشونت پیش‌بینی‌ناپذیر برضد حکومت‌ها، مردم یا افراد برای دستیابی به یک هدف سیاسی است.

فضای سایبر

واژه «سایبر» از لغت یونانی کایبرنتس[1] به معنی سکان‌دار یا راهنما مشتق شده است. سایبر پیشوندی است برای توصیف یک شخص، یک شیء، یک ایده یا یک فضاکه مربوط به دنیای رایانه و اطلاعات است. درفرایند توسعه اینترنت واژه‌های ترکیبی بسیاری ازکلمه سایبر به وجود آمده است که به تعدادی از آن‌ها اشاره می‌کنیم.

فضای سایبری، محیط یا فضای خلق‌شده فنّاورانه است که به جهان مجازی معروف است.

مزایای استفاده ازفضای دیجیتال و یا فناوری‌های دیجیتال درروند ارتکاب جنایات تروریستی آشکار می‌شود. تغییرات در مکانیسم ارتکاب جرایم تروریستی در ارتباط با استفاده از فناوری‌های دیجیتال باید درفرایند جرم (تغییرشدت مجازات) اعمال خطرناک اجتماعی درنظرگرفته شود. زمینه‌های مهم سیاست دولت در زمینه مقابله با این جنایات شامل فعالیت‌های آموزشی، آموزش مأموران اجرای قانون،گسترش قدرت خود برای اطمینان ازکنترل روشن و مؤثر محتوای دیجیتال است.

جرایم درفضای دیجیتال با استفاده از فناوری‌ها، سیستم‌ها و برنامه‌های دیجیتال نشان‌دهنده تکامل طبیعی جرم و جنایت به دلیل پیشرفت علمی و فنّاورانه و تحولات جدید و از جمله مشکلات جدی دنیای مدرن است (راهداری، ۱۳۹۲: ۲۳).

جنایات تروریستی نیزازاین قاعده مستثنی نیستند. لازم به ذکراست که سطح تروریسم همچنان در حال رشد است و همچنین پیشرفت‌های فنّاورانه[2] که به جلب توجه و تأثیرعاطفی تروریست‌ها کمک می‌کند. (Orehek, 2014 :33).

1. Kybernetes
2. Technological advances

عصر تروریسم دیجیتال در حال آمدن است که از نظر مقیاس عواقب احتمالی می‌تواند قابل مقایسه با سلاح‌های کشتار جمعی باشد. حدود ۳۰ هزار وبسایت تروریستی و افراطی در اینترنت وجود دارد. این شرایط نیاز به کار جدی برای مقابله با جنایات تروریستی انجام شده در فضای دیجیتال با استفاده از فناوری‌های دیجیتال، سیستم‌ها و برنامه‌ها دارد.

افراد درگیر در فعالیت‌های تروریستی به طور فعال از فناوری‌های دیجیتال مدرن هم در روند ارتکاب جرم و هم در زندگی روزمره استفاده می‌کنند. چنین فناوری‌هایی در جوامع و سازمان‌های تروریستی به عنوان یک ابزار ارتباطی، از جمله در فرایند سازمان‌دهی و هدایت فعالیت‌های تروریستی و همچنین در استخدام اعضای جدید گروه‌های تروریستی، گسترش ایدئولوژی[1] خشونت، تبلیغات فعالیت‌های تروریستی و درخواست برای ارتکاب اقدامات تروریستی خاص استفاده می‌شود. اعضای گروه‌های تروریستی به دنبال انتقال چنین پیام‌هایی و همچنین نشان‌دادن اقدامات غیرقانونی خود به گسترده‌ترین مخاطبان ممکن هستند، زیرا هدف اصلی آن‌ها بی‌ثبات کردن جامعه و بی‌ثباتی اخلاقی و سیاسی آن است.

رادیکال‌سازی آنلاین و توهین غیرخشونت‌آمیز (آنلاین) همچنان به احتمال زیاد خشونت را تشویق و تأیید می‌کند و به تداوم فرهنگ آنلاین باورهای افراطی کمک می‌کند و جو مبتنی بر شکایت را تثبیت می‌کند که پتانسیل مداوم تشویق اعمال خشونت‌آمیز را در جهان دارد. با توجه به گسترش جهانی اینترنت، این ممکن است یکی از قوی‌ترین استدلال‌ها برای جدی گرفتن تأثیرات آنلاین باشد. شیوع سخنان مشوق عداوت و تنفر و مطالب مرتبط آنلاین را می‌توان بالا در نظر گرفت و مطالعات اخیر در این زمینه نشان داده است که ۴۰ تا ۵۰ درصد از افراد جوان، گاه به گاه با چنین محتوای آنلاین مواجه می‌شوند. به این ترتیب فرصت‌های ثابتی برای آغاز فرآیندهای رادیکال‌سازی بیشتر در جمعیت‌های بزرگ وجود دارد (ساها و همکاران، ۲۰۱۴: ۲۴).

۱. Ideology (به معنای ساده طرز فکر)

پیشینه تحقیق

نقش انکارناپذیر توسعه بشری در عرصه‌های فناوری‌های اطلاعاتی و ارتباطی را درکره زمین در عصر حاضر به هیچ عنوان نمی‌توان نادیده گرفت. فناوری‌های معرف به نرم‌افزارها امروزه تمام ابعاد زندگی بشری را درکلیه حوزه‌های جغرافیایی تحت تاثیرقرارداده است.

تأثیر این روند جدید بر جغرافیای سیاسی نیزکاملاً مشهود بوده و جا برای تحقیقات و پژوهش‌های گسترده در این حوزه را فراهم کرده است و این بدین معنی است که محیط تهدید آفرین علیه امنیت ملی دولت‌ها دیگر محدود به جهان واقعی نیست بلکه در جهت مجازی نیز هم پای جهان واقعی محیطی تهدید زا برای دولت‌هاست. یکی از مهم‌ترین تهدیدات نوظهور، سایبر تروریسم است و با توجه به تراکم گروه‌های تروریستی معاند نظام در محیط پیرامونی جمهوری اسلامی ایران و افزایش نقش کنشگران غیر دولتی در تهدید آفرینی با بهره‌گیری از ظرفیت فضای مجازی این نوشته بر آن است که اهمیت این نقش را بیان و راه‌کارهایی جهت مقابله با آن ارائه دهد. (یزدان پناه،۱۳۹۴:۱۳)

یافته‌ها

ایدئولوژی خشونت نقش مهمی در ارتکاب جنایات تروریستی دارد. (Antonova, E. Yu. 2018:41).

تروریسم یک ابزار سیاسی است که نیاز به انگیزه و توانایی‌هایی دارد که دامنه، ریشه‌ها، ایدئولوژی و ضد استراتژی‌های آن را تعیین می‌کند. (Orehek, E, 2014:22)

موفقیت داعش به این واقعیت بستگی دارد که این گروه به عنوان یک سازمان آموزش‌دیده، با انگیزه ایدئولوژیک و بی‌رحمانه کار می‌کند.

اینترنت به یک فضای دیجیتال بدون کنترل تبدیل شده است که در میان چیزهای دیگر برای گسترش و پرورش ایدئولوژی تروریسم استفاده می‌شود.

به عنوان مثال، بازیگران گروه‌های راست افراطی[1] از اینترنت برای تبلیغ، ترویج جنایات تروریستی و به حداکثر رساندن افشای خود با پخش زنده حملات خود استفاده می‌کنند. از ۲۲ توطئه تروریستی کشف شده در انگلستان بین مارس ۲۰۱۷ و سپتامبر ۲۰۱۹، هفت مورد از ایدئولوژی بازیگران گروه‌های راست افراطی الهام گرفته شده است. در همان دوره، افرادی که از ایدئولوژی بازیگران گروه‌های راست

۱. XRW جنبش‌هایی است که ایده‌های برتری نژادی را به اشتراک می‌گذارند.

افراطی الهام گرفته بودند، سه اقدام تروریستی مرگبار انجام دادند؛ بنابراین، در عصر دیجیتال، ممکن است احساس ارتباط بسیار نزدیکی با گروه‌های آنلاین و مخاطبین آنلاین داشته باشیم که ممکن است منافع و ایدئولوژی‌های خشونت‌آمیز مشابه داشته باشند. اگرچه عضو این گروه‌ها نباشند، به تنهایی عمل می‌کنند، از جمله برای اهداف تروریستی.

تبلیغات دیجیتال مقیاس‌پذیرترین، همه‌کاره‌ترین، مقرون به‌صرفه‌ترین و ایمن‌ترین روشی است که می‌توانید در هر زمان و مکانی پیدا کنید؛ اما حتی بدتر از آن است - فرار مالیاتی بین‌المللی، جنایات سازمان‌یافته، تأمین مالی تروریست‌ها و گروه‌های نفرت‌انگیز و مفهوم آدم‌های بد ادغام شده را اضافه کنید و نگاهی اجمالی به دنیای تبلیغات دیجیتال امروزی خواهید داشت. همیشه این‌قدر بد نبوده است و هنوز هم برخی از بازاریابی دیجیتال واقعی در جریان است؛ اما در سال‌های پس از ظهور فناوری تبلیغات برنامه‌ای (حدود ۱۳-۲۰۱۲)، میزان کلاه‌برداری و سایر جرایم نیز افزایش یافته است. (Makinda,2016:36)

در روزهای اولیه تبلیغات دیجیتال، تبلیغ‌کنندگان (خریداران تبلیغات) مستقیماً از ناشران (فروشندگان فضای تبلیغاتی) خرید می‌کردند؛ اما با مبادلات تبلیغاتی برنامه‌ای، تبلیغات در میلیون‌ها وب‌سایت و اپلیکیشن موبایل قرار می‌گیرد که هیچ‌کس تا به حال نام آن‌ها را نشنیده است. تبلیغ‌کنندگان با هیچ یک از میلیون‌ها سایت و برنامه تعامل ندارند. آن‌ها فقط تبلیغات را از طریق یک مکان خریداری می‌کنند. با قطع ارتباط خریدار از فروشنده، مبادلات تبلیغاتی برنامه‌ای باعث ایجاد عدم شفافیت در اکوسیستم تبلیغات دیجیتال شد. این به طور مستقیم منجر به فرصت بسیار بیشتری برای کلاه‌برداری و سایر جرایم شد.

گیل و همکاران در مطالعه برجسته خود در سال ۲۰۱۵. گزارش مفصلی از فعالیت‌های آنلاین ۲۲۷ بازیگر تروریستی مستقر در بریتانیا ارائه کرد که دوره ۱۹۹۸ تا ۲۰۱۳ را پوشش می‌داد. به طورکلی، شواهدی مبنی بر برخی فعالیت‌های آنلاین مرتبط با یک حمله یا جرم تروریستی مرتبط در ۶۱ درصد از موارد وجود داشت. با نگاهی به فعالیت‌های خاص، ۵۴ درصد از همه موارد از اینترنت برای یادگیری، ۴۴ درصد برای گسترش رسانه‌های آنلاین افراطی، ۳۲ درصد برای آماده‌سازی حمله استفاده کردند (Gill P,2015:54).

گروه‌های تروریستی از این واقعیت استفاده می‌کنند که فضای دیجیتال (سایبری) به شما اجازه می‌دهد تا اطلاعات را فوراً در عرض چند ثانیه در یک منطقه نامحدود گسترده انتقال دهید. محتوای

ویدئویی بسیار هیجان‌انگیز و بالقوه نگران‌کننده رویدادها به سرعت از طریق اینترنت، دستگاه‌های تلفن همراه و سیستم عامل‌های رسانه‌های اجتماعی، از جمله حملات تروریستی بین‌المللی زنده همراه با بمب‌گذاری و تیراندازی گسترش می‌یابد(Huddy, L,2021:47).

علاوه بر این، از طریق کانال‌های شبکه‌های اجتماعی، مقامات رسمی و عموم مردم به شرایط خطرناک واکنش نشان می‌دهند. استفاده روزافزون از توییتر[1] و فیسبوک[2] در مواقع اضطراری نشانه روشنی است که مردم اطلاعات منتشرشده یا ارسال‌شده در فضای دیجیتال (سایبر) را به عنوان «حقیقت» می‌پذیرند. با وجود آنچه که در حال حاضر به عنوان عصر اخبار جعلی یا اطلاعات غلط نامیده می‌شود، مردم هنوز هم به طورکلی به اطلاعاتی که به صورت آنلاین یا در رسانه‌های اجتماعی دریافت می‌کنند اعتماد می‌کنند. (Grobbelaar,2022:56)

با انتشار اطلاعات از طریق فضای دیجیتال (سایبری) که همیشه با واقعیت مطابقت ندارد (می‌تواند اطلاعات غلط، شایعات، تهدید به خشونت یا تصاویر اعمال خشونت‌آمیز باشد)، گروه‌های تروریستی نه تنها بر حامیان احتمالی یا واقعی دیدگاه‌های تروریستی، ایدئولوژی خشونت (که در درجه اول برای جذب اعضای جدید، افراط‌گرایی، تحریک به تروریسم، تضعیف ایمان به اجتماعی استفاده می‌شود) تأثیر می‌گذارد.

این نیز به این دلیل است که تروریسم نیز به عنوان استفاده عمدی یا تهدید به خشونت توسط افراد یا گروه‌های زیرملیتی برای دستیابی به یک هدف سیاسی یا اجتماعی با ارعاب مخاطبان بزرگ به غیر از قربانی مستقیم درک می‌شود. (Sandler, 2013:41).

این نیز به این دلیل است که تروریسم نیز به عنوان استفاده عمدی یا تهدید به خشونت توسط افراد یا گروه‌های زیرملیتی برای دستیابی به یک هدف سیاسی یا اجتماعی با ارعاب مخاطبان بزرگ به غیر از قربانی مستقیم درک می‌شود. (Sandler, 2013:41).

به عنوان مثال، بین سال‌های ۲۰۱۴ و ۲۰۱۷، داعش ۲۹۶ نفر را گردن زد و فیلم‌هایی از گروگان‌های غربی، از جمله روزنامه‌نگاران آمریکایی جیمز فولی[3] و استیون ساتلوف[4] و همچنین چند امدادگر

1. Twitter
2. Facebook
3. James wright foley
4. Steven joel sotloff

بریتانیایی منتشرکرد. همه گروگان‌ها در سال ۲۰۱۴ اعدام شدند و در نظرسنجی یک شرکت مطالعاتی[1] در نوامبر ۲۰۱۴، ۳۲ درصد از آمریکایی‌ها گفتند که حداقل چند ویدیو ازگردن زدن داعش دیده‌اند و ۹ درصد گفتند که شاهد گردن‌زدن واقعی بوده‌اند. بر اساس داده‌های به دست آمده در سطح ملی از یک گروه آنلاین نماینده که حدود شش تا نه ماه پس از معروف‌ترین اعدام‌ها در ایالات متحده مورد بررسی قرارگرفت، ۲۰،۱۴ درصد از آمریکایی‌ها گفتند که برخی یا همه فیلم‌های گردن‌زدن را دیده‌اند. چنین اقداماتی در درجه اول با هدف ارعاب مردم وگسترش احساس اضطراب و ترس شدید است که می‌تواند منجر به وحشت در میان جمعیت شود(Huddy,2021:14).

مطالعه‌ای در مورد نابرابری در پوشش رویدادهای تروریستی، حملاتی را در بازه زمانی ۱۰ ساله ۲۰۰۵-۲۰۱۵ انجام داد و نشان داد که ۱۳۶ قسمت از تروریسم در ایالات متحده رخ داده است. LexisNexis Academic و CNN پلتفرم‌هایی بودند که برای اندازه‌گیری پوشش رسانه‌ای مورد استفاده قرارگرفتند. مشخص شد که از سایر حملات تروریستی که در اخبار نشان داده شده است، حملات تروریستی با عاملان مسلمان بیش از ۳۵۷ درصد پوشش داده شده است. علاوه بر این نابرابری، حملات همچنین زمانی که دولت را هدف قرار می‌دادند پوشش بیشتری دریافت می‌کردند؛ نرخ مرگ و میر بالایی داشتند و نشان می‌داد که بازداشت‌هایی صورت گرفته است. این یافته‌ها با تمایل آمریکا به دسته‌بندی مسلمانان به عنوان تهدیدی برای امنیت ملی همسو بود؛ بنابراین، پوشش رسانه‌های جمعی درباره تروریسم باعث ایجاد روایت‌های جعلی و عدم پوشش مرتبط می‌شود. به عنوان مثال، عموم مردم آمریکا بر این باورند که نرخ جرم و جنایت در حال افزایش بوده و درواقع به پایین‌ترین حد خود رسیده است. با توجه به اینکه رسانه‌ها اغلب جرم را تقریباً بلافاصله و مکرر پوشش می‌دهند، پیشنهاد می‌شود که مردم استنباط کنند که همیشه آن اتفاق می‌افتد. با توجه به تفاوت در حملات تروریستی، سه حمله کمترین پوشش رسانه‌ای را در بین ۱۳۶ مورد داشتند. کشتار معبد سیک در ویسکانسین که ۲،۶ درصد پوشش داشت، کشتار کنیسه کانزاس با ۲،۲ درصد و مرگ و میر کلیسای چارلستون؛ که تنها ۵،۱ درصد پوشش داشته است. این سه رویداد مشترکاتی داشتند که قابل ذکر است، زیرا همه آن‌ها دارای عاملان سفیدپوست بودند و متوجه شهودات حکومتی نبودند (درواقع همه اقلیت‌ها را هدف قرار می‌دادند). وسواس رسانه‌ها نسبت به ترور باعث می‌شود مردم از چیزهای نادرست بترسند و به مسائلی که اساساً دیده نمی‌شوند توجه کافی نداشته باشند (Kearns,2018:11).

1. HuffPost-YouGov

علاوه بر این، اقدامات تروریستی اغلب با هدف تحریک پاسخ‌های دولت، مانند امتیازات ارضی یا اصلاحات سیاسی از طریق اعمال ارعاب است که عزم دولت مخالف را تخلیه می‌کند یا ناکارآمدی آن را برجسته می‌کند؛ به همین دلیل است که گروه‌های تروریستی به دنبال تطبیق ابزارهای ارتباطی افراطی برای جلب توجه و دید در محیط رسانه‌های جهانی هستند. خشونت تروریستی، بسیار با میانجیگری و تماشایی، باعث تبدیل حملات به رویدادهای رسانه‌ای می‌شود که در یک فضای ترکیبی آشکار می‌شوند و ریشه در قابلیت‌ها و فناوری‌های موجود دارند (Uusitalo, 2021:54)

گروه‌های تروریستی از طیف گسترده‌ای از ابزارهای فنی برای انجام فعالیت‌های تبلیغاتی استفاده می‌کنند: وب‌سایت‌ها، گروه‌های چت و انجمن‌های چت، مجلات آنلاین، سیستم عامل‌های رسانه‌های اجتماعی مانند توییتر و فیس بوک، وب‌سایت‌های محبوب به اشتراک‌گذاری ویدئو و فایل مانند یوتیوب[1] و موتورهای جستجو در اینترنت پیداکردن محتوای تروریستی را آسان‌تر می‌کنند.

در جلسات کمیته فرعی اطلاعات و مبارزه با تروریسم کمیته امنیت ملی مجلس نمایندگان دولت ایالات متحده، نمونه‌هایی از استفاده از سیستم‌های هوش مصنوعی که به عنوان AI[2] نامیده می‌شود، توسط تروریست‌ها ارائه شد. به عنوان مثال، یک نژادپرست سفیدپوست به دو مسجد در کریستچرچ نیوزیلند آتش گشود و ۵۱ نفر را کشت و ۴۹ نفر دیگر را زخمی کرد، این تروریست توانست این حمله را به صورت زنده در فیس‌بوک پخش کند، زیرا هوش مصنوعی شبکه فکر نمی‌کرد که این فیلم به اندازه کافی وحشتناک باشد. این ویدئو با موفقیت ۳۰۰ هزار بار توسط کاربران دیگر در فیس بوک آپلود شد. این ثابت می‌کند که فناوری‌های AI طراحی شده برای مسدودکردن چنین فیلم‌هایی هنوز به این کار نرسیده‌اند. علاوه بر این، شواهدی وجود دارد که هوش مصنوعی فیس‌بوک در حال فیلم‌برداری فیلم‌ها و ترویج محتوای تروریستی است که باید حذف شود . (Huddy, 2021:41)

اما حتی اگر عاملان حمله را به صورت زنده پخش نکنند، شاهدان به صورت بصری وقایع را ضبط می‌کنند و این فیلم‌ها در بخش‌های خبری که اغلب در سایت‌های آنلاین مانند یوتیوب و همچنین سایر سیستم عامل‌های رسانه‌های اجتماعی آپلود می‌شوند، گنجانده می‌شوند. این محتوای ویدئویی گرافیکی خام به راحتی قابل دسترسی است (گاهی اوقات با یک هشدار بی‌دلیل همراه است) و می‌تواند

1. youtube
2. Artificial intelligence

احساسات قوی را در بینندگان ایجاد کند و به طور بالقوه پاسخ عمومی به یک عمل تروریستی را تقویت کند .(Huddy, 2021:42)

استخدام و آموزش اعضای جدید گروه‌های تروریستی

استخدام اعضای جدید نقش مهمی در فعالیت‌های گروه‌های تروریستی ایفا می‌کند، زیرا ناتوانی در جذب تعداد کافی عضو و انجام حملات موفق نشان‌دهنده ضعف گروه است(Polo S,2020:62).

توسعه فناوری‌های اطلاعاتی و مخابراتی، به ویژه اینترنت و ابزارهای آن، پلت فرمی را فراهم می‌کند که توسط گروه‌های تروریستی برای جذب اعضای جدید و انتشار تبلیغات آن‌ها و همچنین برای آموزش آنلاین و برنامه‌ریزی حملات تروریستی استفاده می‌شود (Dingji Maza,2020:74).

به عنوان مثال، استفاده گروهک الشباب از فیلم‌ها و پیام‌ها از طریق اینترنت، این سازمان تروریستی را در سراسر جهان به سازمانی شناخته شده تبدیل کرده است. تا سال ۲۰۰۹، الشباب منحصراً سومالیایی‌ها را به صفوف خود جذب می‌کرد. با این حال، از زمانی که ارتباط آن‌ها با القاعده آغاز شد، جنگجویان خارجی که از نظر ایدئولوژیک خود را با جهاد جهانی معرفی کردند، استخدام شده‌اند. یکی از برجسته‌ترین مبارزان بین‌المللی آن‌ها، عمر حمامی که همچنین به عنوان ابومنصور امریکی شناخته می‌شود، از سال ۲۰۰۹ به طور منظم به صورت آنلاین فعالیت می‌کند و آن‌ها را به عنوان استخدام الشباب منتشر می‌کند . (Polo S, 2020:36)

ایجاد شبکه‌های محلی گروه‌های تروریستی یا پیوستن به آن‌ها انتقال دانش و آموزش را تسهیل می‌کند. برای آموزش مشترک و برنامه‌ریزی حمله؛ افزایش دسترسی، عرضه و تبادل سلاح، پرسنل و سایر سرمایه‌های مرتبط با تروریسم؛ شبکه‌های محلی حتی به گروه‌ها اجازه می‌دهند تا اتحاد تشکیل دهند، با هم متحد شوند و کمپین‌های هماهنگ علیه دولت را انجام دهند؛ بنابراین شبکه‌های تروریستی به عنوان یک عامل تعیین‌کننده عمل می‌کنند که قدرت را افزایش می‌دهد، ظرفیت گروه‌ها، توانایی‌ها و اثربخشی آن‌ها را حفظ می‌کند. (Polo S, 2020:37).

علاوه بر این، سایت‌های تخصصی تروریستی به عنوان کتابخانه‌های آنلاین متون ایدئولوژیک، سیستم عامل برای استخدام و انجمن‌ها برای تبادل اطلاعات عمل می‌کنند. عکس و مواد ویدئویی، بازی‌ها (شبیه‌سازی حملات تروریستی و تشویق کاربران به نقش بازی با عمل به عنوان یک تروریست مجازی)،

آموزش‌ها و دستورالعمل‌های فنی تهیه شده توسط گروه‌های تروریستی به افراط‌گرایی حامیان آن‌ها کمک می‌کند (Khokhlov, 2022:79).

مواد تبلیغاتی ممکن است حاوی راهنمایی‌های ایدئولوژیک یا عملی، توضیحات، توجیهات یا تبلیغات برای فعالیت‌های تروریستی باشد. در طول بازرسی توسط دفتر دادستانی شهر شاخونیا روسیه[1] از منابع اینترنتی، انجام شده با استفاده از برنامه مرورگر گوگل کروم، در منبع جستجوی یاندکس[2] هنگام وارد کردن کلمات کلیدی: «سلاح گرم خانگی مناسب»، فهرستی زیادی از سایت‌های اینترنتی نمایش داده شد.

اطلاعات گرفته‌شده در این صفحات اینترنتی اطلاعات دقیقی در مورد روش‌های سلاح دست‌ساز وجود دارد. دسترسی به مواد برای همه کاربران رایگان است، سایت و صفحات اینترنت حاوی محدودیت در دسترسی به آن توسط افراد نیست، پیش ثبت‌نام و رمز عبور موردنیاز نیست، هر کاربر می‌تواند خود را با محتوای این صفحه وب آشنا و به صورت الکترونیکی، هیچ محدودیتی در انتقال، کپی و توزیع وجود دارد.

به‌گفته کارشناسان، تأثیر بر اطلاعات کامپیوتری به مجرم اجازه می‌دهد تا احساسات و آگاهی قربانی را دستکاری کند و باعث عواقب جدی روانی فیزیولوژیکی شود. اثر روانی-عاطفی از نظر قدرت قابل مقایسه با تأثیر وقایع در دنیای واقعی است، در عین حال با تغییر اطلاعات کامپیوتری مدل‌سازی می‌شود (Dremlyuga R, 2022:71).

تحقیقات نشان می‌دهد که جنبش‌های اجتماعی اغلب از فضای رسانه‌های دیجیتال برای کار با هویت استفاده می‌کنند، با استفاده از پیام‌های دیجیتال برای توسعه حس مشترک استفاده می‌کنند (Gaudette t, 2020:47). شواهد قابل‌توجهی جمع‌آوری شده است که رسانه‌های اجتماعی به مکانی برای شکل‌گیری هویت تبدیل شده‌اند و به تشکیل جوامع با حس قوی همبستگی گروهی کمک می‌کنند(Tornberg P, Tornberg, A, 2022:51).

گروه‌های تروریستی در فرایند جذب اعضای جدید و ترویج ایدئولوژی خود به چنین فنون روان‌شناختی متوسل می‌شوند.

1. shakhunya
2. yandex

استفاده از فناوری‌های دیجیتال در روند فعالیت‌های تروریستی آماده‌سازی و مستقیم

در علم، موفقیت‌های فوق‌العاده‌ای از سیستم‌های هوش مصنوعی نه تنها در زمینه سیستم عامل‌های دیجیتال، بلکه در محیط مادی و فوری نیز وجود دارد. این به طور مستقیم در مثال معرفی فناوری‌های دیجیتال (رباتیک مدرن) به سیستم کنترل بدون سرنشین وسایل نقلیه دیده می‌شود که انجام اقدامات تروریستی را تسهیل می‌کند. در حال حاضر در عمل، موارد استفاده از فناوری‌های دیجیتال، از جمله هواپیماهای بدون سرنشین، در روند فعالیت‌های تروریستی مقدماتی و مستقیم، به ویژه برای تحویل مواد مخدر، مواد روانگردان و سایر موارد ممنوعه، سلاح، مواد منفجره، دستگاه‌های انفجاری و غیره وجود دارد.

بنابراین، گروه‌های تروریستی به طور فزاینده‌ای از هواپیماهای بدون سرنشین برای نظارت، انفجار و سایر اقدامات خطرناک اجتماعی استفاده می‌کنند؛ هم در مرحله آماده‌سازی و هم در مرحله مستقیم اقدامات تروریستی. گزارش شده است که داعش شروع به استفاده از هواپیماهای بدون سرنشین جنگی در عراق کرد و چندین بمباران را هم برای اهداف غیرنظامی و هم نظامی و حتی تلاش برای حمله به سران کشورها با استفاده از هواپیماهای بدون سرنشین را انجام داد.

بین سال‌های ۱۹۹۴ تا ۲۰۱۸، بیش از ۱۴ حمله تروریستی برنامه‌ریزی شده یا تلاش‌شده با استفاده از پهپادهای هوایی انجام شد. برخی از این موارد عبارت بودند از:

- در سال ۱۹۹۴، Aum Shinrikyo سعی کرد از یک هلیکوپتر (بالگرد) کنترل از راه دور برای پاشش گاز سارین استفاده کند، اما آزمایش‌ها با سقوط هلیکوپتر (بالگرد) ناموفق بود.
- در سال ۲۰۱۳، یک حمله برنامه‌ریزی‌شده توسط القاعده در پاکستان با استفاده از هواپیماهای بدون سرنشین متعدد توسط مجریان قانون محلی متوقف شد.
- در آگوست ۲۰۱۸، دو پهپاد هدایت شونده با GPS، مملو از مواد منفجره، در تلاشی ناموفق برای ترور رئیس جمهور ونزوئلا «مادورو» استفاده شد.
- در ژانویه ۲۰۱۸، گروهی متشکل از ۱۳ هواپیمای بدون سرنشین دست‌ساز به دو پایگاه نظامی روسیه در سوریه حمله کردند(The Role of Drones in Future Terrorist Attacks by Thomas G. Pledger).

با افزایش تولید این ابزارها و کاهش هزینه‌ها، این نوآوری‌ها برای تروریست‌ها و گروه‌های تروریستی جذاب‌تر و مفیدتر خواهد شد. چاقو و کامیون ممکن است هنوز گزینه‌های ساده‌تر و ارزان‌تر باشند، اما روش‌های جدید حمله تروریستی شروع به تحقق خواهد کرد.

چاپگرهای سه‌بعدی همچنین می‌توانند فنّاوری پیچیده و گران‌قیمت را برای تروریست‌ها در دسترس قرار دهند. به عنوان مثال، مهاجم آلمانی در یوم کیپور[1] در اوایل اکتبر ۲۰۱۹ با استفاده از چاپ سه‌بعدی برای تهیه سلاح‌های خانگی استفاده کرد. وی تنها ۳ دلار برای قطعات چاپ سه‌بعدی برای سلاح‌های مورد استفاده در حمله هزینه کرد.

فضای دیجیتال (سایبری) همچنین به عنوان وسیله‌ای برای ارتکاب حملات سایبری طراحی شده برای مختل‌کردن عملکرد عادی سیستم‌های کامپیوتری، سرورها با کمک ویروس‌های کامپیوتری، بدافزارها و نرم‌افزارهای جاسوسی یا سایر ابزارهای دسترسی غیر مجاز به اطلاعات کامپیوتری استفاده می‌شود. این اقدامات با ویژگی‌های یک عمل تروریستی به عنوان تمایل به بی‌ثبات‌کردن فعالیت‌های نهادهای دولتی یا سازمان‌های بین‌المللی با ارعاب مردم، نفوذ در تصمیم‌گیری آن‌ها و در نتیجه دستیابی به اهداف سیاسی یا سایر اهداف اجتماعی مشخص می‌شود.

کانال‌های تأمین مالی دیجیتال تروریسم

گروه‌های تروریستی برای دستیابی به اهداف و فعالیت‌های مؤثر خود، منابع مادی (مالی) قابل‌توجهی را جذب می‌کنند. فضای دیجیتال (سایبری) و فناوری‌های دیجیتال جدید تنها به تولید سریع درآمد کمک می‌کند که متعاقباً برای نیازهای تروریست‌ها استفاده می‌شود.

مطالعات مختلف نشان می‌دهد که گروه‌های تروریستی مانند القاعده و داعش از طریق پرداخت‌های دیجیتالی از گروه‌ها و افراد دلسوز به آرمان خود کمک مالی و حمایت می‌کنند. نمونه‌هایی از این پرداخت‌های دیجیتال شامل بانکداری اینترنتی، انتقال وجوه تلفن همراه، تجارت آنلاین و افزایش استفاده از ارزهای رمزنگاری شده مانند بیت کوین است (Dingji Maza, 2020:75).

یک تحول دیجیتالی در مکانیسم‌ها و کانال‌های تأمین مالی تروریسم وجود دارد. تروریست‌ها از کازینوهای[2] آنلاین به عنوان منابع درآمد استفاده می‌کنند، از طریق فروشگاه‌های آنلاین ساختگی و

---

۱. روز بخشایش گناهان یهودیان
۲. یا قمارخانه محلی برای انجام انواع بازی‌ها و شرط‌بندی کردن بر سر آن‌ها

سایت‌های همزاد به اختلاس وجوه متوسل می‌شوند، از حملات فیشینگ، دسترسی غیرمجاز به منابع بانکی و مبادلات رمزنگاری استفاده می‌کنند.

علاوه بر این، از طریق فضای دیجیتال (سایبری)، گروه‌های تروریستی درخواست مستقیم برای کمک‌های مالی می‌کنند. برای این منظور، وب‌سایت‌ها، گروه‌های چت، پیام‌های جمعی با درخواست کمک‌های مالی استفاده می‌شود.

هیچ‌کس به‌طور قطع نمی‌داند چقدر ارز دیجیتال در تأمین مالی تروریست استفاده می‌شود. گروه‌های شبه‌نظامی از روش‌های مختلفی برای جابه‌جایی پول استفاده می‌کنند، از جمله پول نقد، بانک‌ها، شرکت‌های پوسته‌ای و مؤسسات خیریه و شبکه‌های مالی غیررسمی. کارشناسان می‌گویند کریپتو بخش کوچکی است.

بلومبرگ گزارش داد که یکی از مقامات سازمان ملل در سال ۲۰۲۲ گفت که چند سال پیش ۵ درصد از حملات تروریستی توسط رمزارزها تأمین مالی می‌شد، اما این میزان ممکن است به ۲۰ درصد برسد. FATF امسال اعلام کرد که کریپتو «خطرات فزاینده تأمین مالی تروریسم» را ارائه می‌دهد، اما «اکثریت قریب به اتفاق» تأمین مالی تروریسم همچنان از پول معمولی استفاده می‌کند.

Chainalysis، محققین کریپتو، در وبلاگی می‌گویند: وقتی جریان‌های مالی غیرقانونی در یک شرکت رمزنگاری شناسایی می‌شود، لزوماً به این معنی نیست که تمام جریان‌های آن شرکت آلوده است. Chainalysis گفت که تأمین مالی تروریسم «بخش کوچکی از کمتر از ۱٪ کل بازار ارزهای دیجیتال اشغال شده توسط فعالیت‌های غیرقانونی را نشان می‌دهد.»

وب‌سایت‌ها همچنین به عنوان فروشگاه‌های آنلاین ارائه کتاب، صدا، ضبط ویدئو و سایر مواد با محتوای مربوطه استفاده می‌شود. فروش چنین کالاهایی نه تنها اجازه می‌دهد تا درآمد اضافی دریافت کنید، بلکه به گسترش ایدئولوژی تروریسم کمک می‌کند.

مزایای استفاده از فضای دیجیتال و یا فناوری‌های دیجیتال در روند ارتکاب جرایم تروریستی

مزایای استفاده از فضای دیجیتال و یا فناوری‌های دیجیتال، اولاً به دلیل سرعت انتقال داده‌ها و انتشار اطلاعات و همچنین پردازش مجموعه بزرگی از اطلاعات، به عنوان مثال، اجازه می‌دهد تا به

سرعت پیدا کردن حامیان، استخدام اعضای جدید گروه‌های تروریستی و غیره افزود؛ ثانیاً، رسیدن به مخاطبان نامحدود گسترده و گسترش جغرافیای گسترش ایدئولوژی مخرب خشونت در شرایط ناشناس بودن نسبی؛ ثالثاً، دشواری کنترل محتوای اطلاعات منتشرشده؛ رابعاً، ساده‌سازی هماهنگی اقدامات اعضای گروه‌های تروریستی (Antonova, E. Yu. 2022).

این عوامل و عوامل دیگر در بسیاری از موارد میزان خطر عمومی اعمال انجام شده را افزایش می‌دهد که باید در هنجارهای قانون کیفری منعکس شود.

در این راستا، مخاطبان زیر سن قانونی به ویژه برای گروه‌های تروریستی جذاب هستند، زیرا تجربه زندگی لازم، جهت‌گیری‌های مثبت پایدار را ندارند و کاربر فعال فضای دیجیتال (سایبری) هستند. علاوه بر این، همان‌طور که در ادبیات علمی اشاره شده است، «نوجوانان مستعد شکل‌گیری نگرش نسبت به رفتار پرخاشگرانه هستند». مؤثرترین آن‌ها فناوری‌های تحریک پرخاشگری از طریق شعارهای افراطی، سیاسی‌کردن مشکلات اجتماعی و اقتصادی، رمانتیک‌کردن تصاویر «قهرمانان منفی»، تحمیل ایده‌هایی است که خشونت را به عنوان یک هنجار اجتماعی ترویج می‌کند و آن‌ها را در جوامع آنلاین مخرب غوطه‌ور می‌کند.

موزیک ویدیوهای محبوب، بازی‌های رایانه‌ای، فیلم‌های پویانمایی، داستان‌هایی که اقدامات تروریست‌ها، مأموریت‌های انتحاری و غیره را تشویق و ستایش می‌کنند، برای استخدام افراد زیر سن قانونی استفاده می‌شود.

بنابراین، سه نوجوان ۱۵ ساله از اکتبر ۲۰۱۹ تا ژوئن ۲۰۲۰ با برقراری ارتباط در یکی از شبکه‌های اجتماعی و پیام‌رسانان، برای پیوستن به ایده‌های انارشیسم[1] در یک گروه برای اجرای مشترک فعالیت‌های تروریستی در قلمرو شهرکانسک متحد شدند. با اختصاص نقش بین خود، نوجوانان به طور مستقل با خواندن ادبیات افراطی ممنوع و تماشای فیلم در رابطه با تولید مواد منفجره و دستگاه‌های انفجاری به منظور انجام فعالیت‌های تروریستی مورد آموزش قرار گرفتند. آن‌ها به طور مستقل مواد منفجره و دستگاه‌های انفجاری تولید می‌کردند و استفاده از آن‌ها را در یک خانه متروکه، در زمین‌های خالی و سایت‌های ساخت و ساز به منظور آماده شدن برای انجام یک اقدام تروریستی یا منفجرکردن

۱. Anachism یک فلسفه و جنبش سیاسی که نسبت به انحصارطلبی در قدرت ضدیت دارد و همه شکل‌های اجبار سلسله‌مراتب را رد می‌کند

ساختمان پلیس تمرین می‌کردند. این پرونده شامل تصاویری از مکاتبات در شبکه‌های اجتماعی بود که در آن متهمان در مورد مکان و نحوه خرید اجزای مواد منفجره بحث می‌کردند.

اسکرین شات تریلر بازی ویدیویی که توسط کاربر «عشاق ابوبکر البغدادی» بارگذاری شده است و نظرات آن در مقاله احمد الروی بررسی شده است.

در مورد نظرات، در مجموع ۳۹۷ نظر و پاسخ در مورد ویدیوهای ارسال شده وجود دارد. به دلیل ماهیت بسیار شخصی پاسخ‌ها، آن‌ها به همراه هر پست نامربوط و مبهم از مطالعه کنار گذاشته شدند. در مجموع، ۱۹۹ نظر شناسایی شد. ۵۷٫۲٪ (n = 114) نظرات نسبت به بازی و داعش منفی، ۳۳٫۶٪ (n = 67) نظرات مثبت و ۹٪ (n = 18) بدون حمایت از هیچ طرفی خنثی بودند. با توجه به نظرات منفی، آن‌ها معمولاً حاوی ستایش از هر کسی بود که از داعش و بازی آن انتقاد می‌کرد که معمولاً به دلیل این ادعا که به طور مستقل از Grand Theft Auto ساخته شده است مورد تمسخر قرار می‌گرفت. به عنوان مثال، یوتیوبر «Hadji M» اشاره کرد که «این یک بازی ویدیویی معروف آمریکایی است و هر شخصی که تجربه‌ای در برنامه‌نویسی داشته باشد می‌تواند شکل شخصیت‌ها و حتی جلوه‌های صوتی آن را تغییر دهد.» علاوه بر این، بیشتر انتقادها بر این بود که نشان دهد داعش نماینده اسلام نیست و یا اینکه شبه نظامیان شیعه که با داعش می‌جنگند پیروز شدند. در مورد نظرات مثبتی که بازی و داعش را تحسین می‌کردند، ۳۳٫۶ درصد از کل نظرات را تشکیل می‌دادند. این نتایج دقیقاً با تعداد دفعات پسندیدن ویدیو (۶۸٫۳٪) از بازی و پسندیدن آن‌ها (۳۱٫۵٪) مطابقت دارد. علی‌رغم غلبه نظرات منفی علیه داعش، هنوز گروهی فعال از هواداران و پیروان وجود داشتند که عمدتاً معتقد بودند حمایت آنلاین از داعش بیانگر ارادت آن‌ها به اسلام سنی است که گفته می‌شود مورد حمله شیعیان قرار گرفته است.

همه موارد فوق توسط کارشناسان در زمینه مبارزه با تروریسم تأیید شده است. به عنوان مثال، مدیر دفتر مبارزه با تروریسم سازمان ملل متحد[1]، اشاره می‌کند که تروریست‌ها به طور فعال از دستاوردهای مختلف فنّاورانه استفاده می‌کنند. با استفاده از شبکه‌های اجتماعی و پیام‌های رمزگذاری شده آن‌ها ایدئولوژی انسان‌گریزانه خود را گسترش می‌دهند، جمع‌آوری و انتقال پول، رادیکالیزه[2] کردن جوانان و استخدام حامیان جدید، هماهنگی حملات تروریستی. علاوه بر این، آن‌ها از الگوریتم‌های شبکه‌های اجتماعی به گونه‌ای استفاده می‌کنند که محتوای خود را در اسرع وقت و به طور گسترده‌ای توزیع

۱. V. Voronkov

۲. Radicalize تندرو و افراطی کردن

کنند. شواهدی از تلاش‌های تروریست‌های زیرزمینی برای استفاده از مواد مخدر برای ایجاد سلاح‌های بیولوژیکی وجود دارد. تروریست‌ها می‌توانند از هواپیماهای بدون سرنشین، از جمله هواپیماهای خودکار، برای تحویل مواد شیمیایی، بیولوژیکی یا رادیولوژیکی استفاده کنند.

مقابله با جرایم تروریستی در فضای دیجیتال (سایبری) و یا با استفاده از فناوری‌های دیجیتال

پیچیدگی مقابله با جرایم دیجیتال در درجه اول به دلیل این واقعیت است که نمی‌توان آن را به وضوح اندازه‌گیری کرد. توضیح این پیچیده است: تناقضات چارچوب نظارتی فعلی، نقص اجرای قانون و مکانیسم‌های حسابداری آماری، ماهیت بی‌شماری و ... همیشه در حال تغییر جرم دیجیتال هستند (Russkevich, E, 2022:54) .

برای مقابله با جرایم تروریستی انجام شده در فضای دیجیتال (سایبری) و یا با استفاده از فناوری‌های دیجیتال، لازم است مکانیسم‌های مؤثر، از جمله نفوذ قانون کیفری که اجازه پاسخ به موقع به تهدیدات تروریستی را در محیط دیجیتال می‌دهد تقویت شود.

لازم به ذکر است که پیچیدگی مقابله با اقدامات خطرناک اجتماعی، از جمله اقدامات تروریستی که در فضای دیجیتال انجام می‌شود، به عنوان یک قاعده، منجر به تغییر در چارچوب قانونی دولت‌ها می‌شود. اغلب، چنین تغییراتی با افزایش مسئولیت قانونی برای ارتکاب چنین اعمالی همراه است.

قوانین کیفری تمامی کشورها در حال اصلاح است: هنجارها با شرایط جدید و با استفاده از رسانه‌ها یا الکترونیکی یا اطلاعات و شبکه‌های مخابراتی، از جمله اینترنت تکمیل می‌شوند و هنجارهای جدید در مورد جرایم در زمینه اطلاعات کامپیوتری اصلاح می‌شوند و هنجارهای جدید در حال ظهور هستند. با وجود تمام نوآوری‌های قانونی، هنوز نمی‌توان وجود یک سیستم مناسب و مؤثر از اقدامات قانون کیفری را بر افرادی که مرتکب اعمال مورد نظر در فضای دیجیتال (سایبری) و یا استفاده از فناوری‌های دیجیتال می‌شوند، بیان کرد. تجزیه و تحلیل مقررات قانون کیفری نشان می‌دهد که تا به امروز، قانون‌گذارها تنها مسئولیت درخواست‌های عمومی برای فعالیت‌های تروریستی، توجیه عمومی تروریسم یا تبلیغات تروریسم را تقویت کرده‌اند. در عین حال، عمل نشان می‌دهد که فضای دیجیتال (سایبری) نه تنها برای انتشار اطلاعات تبلیغاتی برای اهداف تروریستی، بلکه برای ترویج فعالیت‌های

تروریستی، از جمله استخدام اعضای جدید گروه‌های تروریستی، تأمین مالی، آموزش عاملان، تحریک به ارتکاب اقدامات تروریستی و غیره استفاده می‌شود.

باید در نظر داشت که مقابله با جنایات تروریستی انجام شده در فضای دیجیتال (سایبری) و یا با استفاده از فناوری‌های دیجیتال، تنها با جرم انگاری اقدامات جدید خطرناک اجتماعی یا افزایش شدت مجازات غیرممکن است. درک روشنی از مکانیسمی که چنین جنایاتی انجام می‌شود ضروری است. از این رو، با وظایف جدید توسط سازمان‌های اجرای قانون مواجه هستیم که باید قادر به شناسایی سریع منبع تهدید تروریستی و مسدود کردن و از بین بردن آن باشد.

علاوه بر این، همان‌طور که در ادبیات علمی اشاره شده است، توسعه سریع فناوری‌های دیجیتال، دستگاه‌های هوشمند و شبکه‌های اجتماعی توانایی کارکنان امنیت عمومی را برای مدیریت پاسخ عمومی به یک حمله تروریستی بدتر کرده است. از آنجاکه مردم و سازمان‌های اطلاعاتی به طور فزاینده‌ای به فناوری‌های دیجیتال تکیه می‌کنند، مشخص نیست که در صورت شکست امنیتی، سیستم سایبری چگونه عمل خواهند کرد. در این راستا، احتمال یک خرابی آبشاری[1] و ظهور آسیب‌پذیری سایبری افزایش می‌یابد. (Keenan, P,2019:14)

همه این‌ها می‌تواند توسط گروه‌های تروریستی مورد استفاده قرارگیرد و باید در هنگام توسعه اقدامات برای مقابله با چنین جنایاتی در نظر گرفته شود.

تجزیه‌وتحلیل

داده‌ها و روش‌شناسی تجربی

ما با توصیف منابع داده خود برای تروریسم و جریان‌های اطلاعاتی به عنوان متغیرهای کلیدی در تحلیل تجربی ما، شروع می‌کنیم. هدف ما این است که به دقت فرضیه‌های نظری خود را با تحلیل‌های تجربی موجود که بر مفاهیم مرتبط تمرکز می‌کنند، مرتبط کنیم. سپس به توضیح مجموعه متغیرهای کنترلی خود، همان‌طور که توسط ادبیات موجود پیشنهاد شده است، می‌رویم. تمامی متغیرهای موجود در مطالعه ما به همراه منابع و تعاریف مربوطه در جدول ۱ خلاصه شده است. در نهایت استراتژی اقتصادسنجی خود را معرفی می‌کنیم.

۱. Cascading failure فرایندی در یک سیستم که در آن خرابی یک عضو می‌تواند باعث خرابی اعضا دیگر شود.

داده‌های مربوط به تروریسم

ما به داده‌های مربوط به حملات تروریستی از آنچه به منبع استاندارد تحقیقات تجربی در مورد تروریسم تبدیل شده است دسترسی داریم (START 2016).

ما از آخرین نسخه GTD استفاده می‌کنیم که بیش از ۱۷۰،۰۰۰ حادثه از سال ۱۹۷۰ تا ۲۰۱۴ را پوشش می‌دهد. GTD را می‌توان به عنوان تروریسم داخلی یا فراملی طبقه‌بندی کرد.

متغیر نتیجه اصلی ما تعداد حملات تروریستی را در یک کشور و سال معین اندازه‌گیری می‌کند. توجه داشته باشید که ما حملات موفق و ناموفق را در اینجا گنجانده‌ایم. ما با تجزیه و تحلیل همه حملات شروع می‌کنیم، اما سپس نمونه را به مواردی تقسیم می‌کنیم که توسط GTD و اندرز، سندلر و گایبولوف (۲۰۱۱) به عنوان داخلی یا فراملی طبقه‌بندی شده‌اند.

یک نکته نگران‌کننده این است که GTD، مانند بسیاری دیگر از پایگاه‌های داده در دسترس عموم، اطلاعات را از منابع داده باز جمع‌آوری می‌کند؛ بنابراین، این امکان وجود دارد که برخی از حملات در صورتی که هرگز در جایی گزارش یا مستند نشده باشند، یعنی زمانی که جریان اطلاعات برای شروع محدود باشد، شناسایی نشده باقی بمانند. برای مثال، دراکوس و گوفاس (۲۰۰۶a، ۲۰۰۷) در کشورهایی که رسانه‌ها آزاد نیستند، سوگیری گزارش کمتری را پیشنهاد می‌کنند.

طیف وسیعی از مطالعات استدلال می‌کنند که احتمال سوگیری سیستماتیک در داده‌های شمارش رویدادهای مبتنی بر رسانه بسیار کوچک‌تر می‌شود، اگر داده‌ها (۱) حقایق سخت را پوشش دهند (فرانزوسی ۱۹۸۷:۱۴)، (۲) مربوط به رویدادهای خشونت‌آمیز مهم (شرودت ۱۹۹۴)، یا (۳) از تعداد زیادی منابع جمع‌آوری شده‌اند (Woolley, 2000:54) . دو معیار اول به طور شهودی در رابطه با حملات تروریستی برآورده می‌شوند.

داده‌ها در مورد جریان اطلاعات

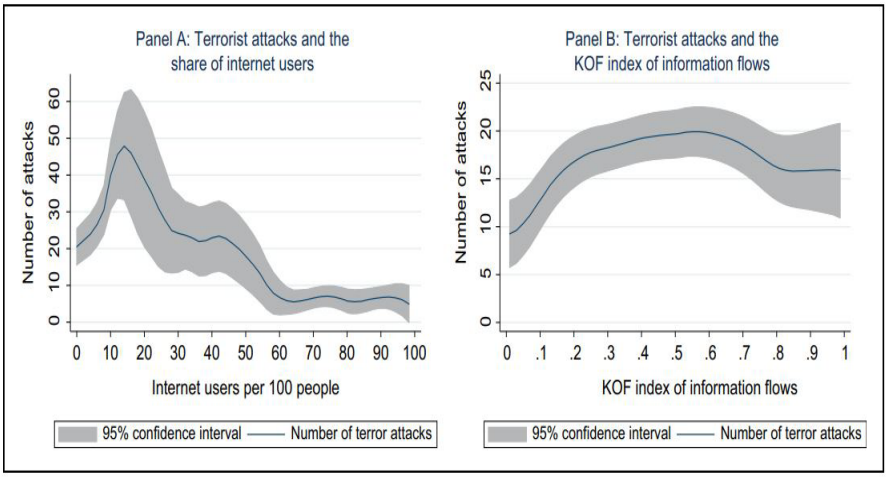
برای اندازه‌گیری درجه جریان اطلاعات و CT (فناوری ارتباطات) موجود در یک کشور و سال معین، از شاخص KOF جریان اطلاعات استفاده می‌کنیم. این شاخص یکی از زیر شاخص‌های شاخص جهانی‌شدن KOF است که سالانه برای ۲۰۷ کشور از سال ۱۹۷۰ تا ۲۰۱۴ توسعه می‌یابد (درهر ۲۰۰۶؛ درهر، گاستون و مارتنز ۲۰۰۸). این شاخص که توسط مؤسسه اقتصادی KOF سوئیس

منتشرشده است، از ۰ تا ۱۰۰ متغیر است و شامل سه متغیر است: تعداد کاربران اینترنت، سهم خانوارهای دارای تلویزیون و تجارت روزنامه به عنوان درصدی از تولید ناخالص داخلی(GDP) ؛ بنابراین، این شاخص مفهوم t را از چارچوب نظری ما به خوبی دریافت می‌کند و درجه CT را در جامعه‌ای که جریان اطلاعات را تسهیل می‌کند، ارزیابی می‌کند. برای تسهیل مقایسه بزرگی‌ها در تحلیل رگرسیون آتی، شاخص را بر ۱۰۰ تقسیم می‌کنیم تا بین ۰ و ۱ باشد.

در این مرحله، در نظرگرفتن نزدیک‌ترین مطالعات مرتبط هنگام تحلیل «برهان عمومی» در رابطه با تروریسم مفید است. چندین مطالعه از شاخص‌های دوتایی آزادی مطبوعات استفاده کرده‌اند تا بفهمند که آیا و چگونه محیط رسانه‌ای موجود در یک کشور می‌تواند به تروریست‌ها کمک کند تا تبلیغات عمومی پیدا کنند (لی ۲۰۰۵؛ ساویر ۲۰۰۵؛ چنووت ۲۰۱۰؛ عسل و هافمن ۲۰۱۶). این استدلال بر محیط نظارتی یک کشور متمرکز است؛ به طور شهودی، اگر مطبوعات آزاد نباشند در مورد حملات تروریستی احتمالی گزارش دهند، ممکن است تروریست‌ها به همان دلایلی که فرضیه خود را بر اساس آن‌ها می‌سازیم، از حمله منصرف شوند. با این حال، مفهوم ما از این نظرگسترده‌تر است که درجه عمومی جریان اطلاعات در جامعه ممکن است بتواند بر تصمیم تروریست‌ها تأثیر بگذارد. به این ترتیب، محیط نظارتی ممکن است به خوبی بر جریان اطلاعات تأثیر بگذارد، اما تمام درجه جریان اطلاعات به طور کامل توسط آزادی مطبوعات به تنهایی در نظرگرفته نمی‌شود. معیارهای مربوط به آزادی مطبوعات در این رشته از تحقیقات از داده‌های آزادی مطبوعات (Freedom House,2011:59) یا از مجموعه داده‌های آزادی رسانه جهانی ون بل (Van Belle,2017:15) گرفته شده است. در واقع، این مجموعه داده‌ها یا کانال‌های ارتباطی مدرن مانند استفاده از اینترنت را در نظر نمی‌گیرند (معیار ون بل) یا کمتر (داده‌های آزادی مطبوعات) را نشان می‌دهند.

با در نظرگرفتن فرضیه ما، ادبیات گسترده در مورد مطالعات ارتباطی ثابت کرده است که در دسترس بودن کانال‌های رسانه‌ای مدرن نه تنها ارتباطات و جریان اطلاعات را بهبود می‌بخشد، بلکه ممکن است آگاهی و مشارکت سیاسی را به طور مؤثرتری نسبت به کانال‌های سنتی هدایت کند. به عنوان مثال، به رسمیت شناختن رسانه‌های اجتماعی به عنوان جایگزینی برای رسانه‌های سنتی برای درک میزان بسیج جمعی ضروری است، به ویژه به این دلیل که رسانه‌های اجتماعی گروه‌های سنی مختلف و طبقات اجتماعی- اقتصادی را هدف قرار می‌دهند.

با توجه به تروریسم، وایمن (۲۰۰۶) مستند می‌کند که تروریست‌ها از اینترنت برای جمع‌آوری سرمایه، جلب حمایت و جذب پیروان و همچنین برنامه‌ریزی و اجرای حملات استفاده می‌کنند. به طور خلاصه، فرضیه‌های ما در اینجا وضعیت جامع یک کشور را در مورد جریان اطلاعات از طریق CT به جای تمرکز بر محیط نظارتی تنها در بر می‌گیرد. برای به دست آوردن یک ایده اولیه از رابطه تجربی بین CT و تروریسم، شکل ۱ دو رابطه توصیفی اساسی را به تصویر می‌کشد. پانل A سهم کاربران اینترنت را در برابر تعداد حملات تروریستی در مشاهدات سالیانه کشور ترسیم می‌کند، در حالی که پانل B تعداد حملات تروریستی را در برابر شاخص KOF جریان اطلاعات نشان می‌دهد. همان‌طورکه توسط چارچوب نظری ما پیشنهاد شده است، در هر دو نمودار یک رابطه زنگ‌شکل مشاهده می‌کنیم. اگرچه فقط ماهیت توصیفی دارد، اما این مقایسه‌های ساده نشان‌دهنده رابطه سیستماتیک بین جریان‌های اطلاعات و تروریسم است و انگیزه تحلیل اقتصادسنجی ما است.



شکل ۱: جریان اطلاعات و تروریسم هر دو نمودار از یک هموارسازی چندجمله‌ای محلی با وزن هسته از مشاهدات سال کشور استفاده می‌کنند که فاصله اطمینان ۹۵ درصدی مربوطه را نشان می‌دهد.

متغیرهای کنترل

برای اطمینان از اینکه سایر عوامل بالقوه مخدوش‌کننده برآوردهای ما را هدایت نمی‌کنند، مجموعه‌ای جامع از متغیرهای کنترلی را بر اساس ادبیات موجود گنجانده‌ایم. ابتدا، ما ویژگی‌های مرتبط با رژیم سیاسی را به دنبال لی (۲۰۰۵)، پیاتزا (۲۰۰۸)، چنووت (۲۰۱۲، ۲۰۱۳) وگایبولوف، پیازا و سندلر (۲۰۱۷) بررسی می‌کنیم. به طور خاص، ما متغیر polity۲ را از مجموعه داده‌های Polity IV برای اندازه‌گیری درجه دموکراسی وارد می‌کنیم.

این شاخص از ۱۰- تا ۱۰+ با مقادیر پایین‌تر نشان‌دهنده رژیم‌های خودکامه و مقادیر بالاتر به دموکراسی است. از آنجایی که ادبیات رابطه غیرخطی بین نوع رژیم و تروریسم را پیشنهاد می‌کند، ما مربع سیاست ۲ را نیز در نظر می‌گیریم.

بنابراین، برای ایجاد مناسب رابطه مربع، ابتدا شاخص polity۲ را در محدوده ۰ تا ۲۰ تغییر می‌دهیم. سپس، معیاری را برای دوام رژیم از طریق امتیاز بادوام از مجموعه داده Polity IV ترکیب می‌کنیم، زیرا کشورهایی که در حال تغییر رژیم هستند پیشنهاد شده است، در برابر تروریسم آسیب‌پذیرتر باشند (واینبرگ و یوبانک، ۱۹۹۸). دوم، ما تولید ناخالص داخلی سرانه و اندازه جمعیت را با دسترسی به شاخص‌های توسعه جهانی کنترل می‌کنیم (به بانک جهانی ۲۰۱۶ مراجعه کنید). مطابق با ادبیات موجود، ما لگاریتم طبیعی را برای هر دو متغیر اعمال می‌کنیم. به طور شهودی، در حالی که توسعه اقتصادی می‌تواند نارضایتی یک گروه مخالف را کاهش دهد، منابع قابل توجه تر نیز «جایزه» تروریسم را افزایش می‌دهد. با توجه به تروریسم فراملی، توسعه اقتصادی بالاتر نیز می‌تواند نماد اهداف جذاب‌تر باشد. از این رو، پیش از این، ادبیات شواهدی در مورد چگونگی ارتباط سطح درآمد با تروریسم ارائه کرده است. علاوه بر این، جمعیت بزرگ‌تر ممکن است به دلیل مشکلات مرتبط با پلیس یا استدلال‌های مقیاس ساده، با حملات تروریستی بیشتری همراه باشد (به عنوان مثال، لی ۲۰۰۵ را ببینید).

سوم، با استفاده از داده‌های Melander، Pettersson و Themn´r (۲۰۱۶) و برنامه داده‌های درگیری اوپسالا و مؤسسه تحقیقات صلح بین‌المللی، اسلو (۲۰۱۷)، دخالت یک کشور در درگیری‌ها را با گنجاندن داده‌های درگیری‌های مسلحانه بین‌دولتی و داخلی کنترل می‌کنیم. انتظار می‌رود درگیری مسلحانه داخلی، تروریسم را افزایش دهد؛ زیرا دسترسی به سلاح‌ها آسان‌تر است و یک موقعیت امنیتی بالقوه آسیب‌پذیر است، درگیری مسلحانه بین ایالتی با افزایش امنیت در داخل کشور همراه است و بنابراین،

ممکن است تروریسم را با افزایش هزینه‌های آن کاهش دهد (لی ۲۰۰۵). علاوه بر این، به دنبال Piazza (۲۰۰۷)، (۲۰۰۸)، Kis-Katos، Liebert و Schulze (۲۰۱۱) و M. C. Wilson و Piazza (۲۰۱۳)، متغیری را شامل می‌شود که نشان‌دهنده شکست دولت است که ازگروه ویژه بی‌ثباتی سیاسی مشتق شده است (به مارشال مراجعه کنید، گور و هارف ۲۰۱۷). در راستای پژوهش پیاتزا (۲۰۰۸b، (این متغیر به عنوان مجموعه‌ای از چهار نوع شکست دولت ساخته شده است: تغییرات رژیم نامطلوب، جنگ‌های قومی، نسل‌کشی/سیاست‌کشی و جنگ‌های انقلابی. علاوه بر این، ما شاخص ترکیبی توانایی ملی (به سینگر، برمر و استاکی ۱۹۷۲؛ سینگر ۱۹۸۸ را ببینید) برای به دست آوردن ظرفیت یک ایالت برای مبارزه با تروریسم، به دنبال پیشنهادهای لی (۲۰۰۵) وگایبولوف، پیازا و سندلر (۲۰۱۷) ترکیب می‌کنیم.

در نهایت، برای در نظرگرفتن ویژگی‌های مشاهده نشده در طول بُعد کشور و زمان، از اثرات ثابت کشور و اثرات ثابت سال استفاده می‌کنیم. به طور خاص، تعدادی از محرک‌های تروریسم خاص کشوری با زمان ثابت پیشنهاد شده‌اند که همه آن‌ها را می‌توان در یک تنظیم اثرات ثابت در هنگام استفاده از داده‌های تابلویی در نظرگرفت. به عنوان مثال، عبادی (۲۰۰۶) مساحت کشور، ارتفاع وکسری از مناطق گرمسیری را به عنوان پیش‌بینی کننده‌های مرتبط تروریسم پیشنهاد می‌کند. کولیر و هوفلر (۲۰۰۴) پیشنهاد می‌کنند که زمین‌های کوهستانی و جنگل‌ها می‌توانند پناهگاه‌های امنی برای شورشیان فراهم کنند و احتمال گرفتار شدن آن‌ها راکاهش دهند، در حالی که Fearon و Laitin (۲۰۰۳) پیشنهاد کردند که مناطق غیرهمجوار به نفع شورشیان بالقوه است. علاوه بر این، با توجه به اثرات ثابت زمانی، ممکن است که تحولات جهانی در مقیاس بزرگ بتواند هم تروریسم و هم بر میزان جریان اطلاعات به طور هم‌زمان تأثیر بگذارد. به عنوان مثال، دوران جنگ سرد یا دوره پس از۱۱ سپتامبر حاکی از شوک‌های جهانی است که می‌تواند به خوبی تروریسم و شاید جریان اطلاعات را به طور هم‌زمان تحت تأثیر قرار دهد (لی ۲۰۰۵؛گایبولوف، پیازا و سندلر ۲۰۱۷ را ببینید). اثرات ثابت چنین تحولاتی را نشان می‌دهد.

جدول ۱: آمار خلاصه همه متغیرها

متغیر	تعریف متغیر	مشاهدات	میانگین	انحراف معیار	حداقل	حداکثر	منبع اطلاعات
حملات	تعداد کل حملات در یک کشور در سال	۸۰۴۶	۱۷,۲۷	۱۰۰,۲۸	۰	۳۹۲۵	پایگاه جهانی تروریسم
حملات داخلی	تعداد کل حملات داخلی یک کشور در سال	۶۲۳۹	۷,۳۲	۳۹,۹۶	۰	۸۸۱	پایگاه جهانی تروریسم
حملات فراملی	تعداد کل حملات فراملی یک کشور در سال	۷۰,۵۵	۳,۶۱	۱۷,۱۳	۰	۴۵۳	پایگاه جهانی تروریسم
KOF شاخص جریان اطلاعات	شاخصی از جریان اطلاعات از ۰ تا ۱ با مقادیر بالاتر مرتبط با جریان بزرگ اطلاعات	۸۰۴۶	۰,۵۱	۰,۲۳	۰,۰۱	۰,۹۹	درهر (۲۰۰۶)، درهر و همکاران. (۲۰۰۸)
سیاست ۲	۲۰/(۱۰ + score Polity۲)	۶۳۵۶	۱۱,۲۱	۷,۳۷	۰	۲۰	مجموعه داده Polity IV مارشال و همکاران (۲۰۱۷)
مدت زمان رژیم	(نمره دوام رژیم)Log	۵۷۹۳	۲,۲۶	۱,۱۷	۰	۵,۳۲	مجموعه داده Polity IV مارشال و همکاران (۲۰۱۷)
درگیری مسلحانه بین ایالتی (بله/خیر)	درگیری مسلحانه بین ایالتی	۸۰۴۶	۰,۰۱۸	۰,۱۳	۰	۱	برنامه داده‌های درگیری اوپسالا و موسسه تحقیقات صلح بین‌المللی، اسلو (۲۰۱۷) مجموعه داده‌های درگیری مسلحانه

متغیر	تعریف متغیر	مشاهدات	میانگین	انحراف معیار	حداقل	حداکثر	منبع اطلاعات
درگیری مسلحانه داخلی (بله/خیر)	درگیری مسلحانه داخلی	۸۰،۴۶	۰،۱۲	۰،۳۲	۰	۱	برنامه داده‌های درگیری اوپسالا و موسسه تحقیقات صلح بین‌المللی، اسلو (۲۰۱۷) مجموعه داده‌های درگیری مسلحانه
شاخص بی‌ثباتی سیاسی	شاخص شکست دولت	۸۰۴۶	۰،۴۸	۱،۴۸	۰	۱۴	PITF
Ln(GDP/ سرانه)	لگاریتم تولید ناخالص داخلی سرانه به قیمت ثابت سال ۲۰۰۵ به دلار آمریکا	۶۷۷۷	۸،۲۵	۱،۵۳	۴،۷۵	۱۱،۸۹	آمار UN
Ln(اندازه جمعیت)	لگاریتم کل جمعیت	۸۰۰۱	۱۵،۱۶	۲،۲۲	۹،۱۲	۲۱،۰۳	شاخص‌های توسعه جهانی
شاخص ترکیبی توانمندی ملی	شاخص ترکیبی توانمندی ملی	۶۸۹۷	۰،۰۰۵	۰،۰۲	۰	۰،۲۲	قابلیت‌های مواد ملی (نسخه ۵،۰؛ سینگر و همکاران ۱۹۷۲؛ سینگر ۱۹۸۸)

توجه: GDP = تولید ناخالص داخلی. PITF =گروه ویژه بی‌ثباتی سیاسی. UN = سازمان ملل متحد؛

KOF =Konjunkturforschu gsstelle.d

نتیجه

تجزیه‌وتحلیل اشکال مختلف فعالیت‌های مجرمانه گروه‌های تروریستی که در فضای دیجیتال و یا با استفاده از فناوری‌های دیجیتال انجام می‌شود، به ما اجازه می‌دهد تا بیان کنیم که:

۱. توسعه فضای دیجیتال (شبکه‌های اجتماعی، رسانه‌های الکترونیکی و سایر منابع اینترنتی)، افزایش تعداد کاربران چنین فضاها و فناوری‌های دیجیتال، سیستم‌ها و برنامه‌ها به گسترش ایدئولوژی خشونت به دلیل فعالیت‌های تبلیغاتی فعال گروه‌های تروریستی و در نتیجه شدت تروریسم کمک می‌کند.

۲. استفاده از فناوری‌های دیجیتال توسط گروه‌های تروریستی، در واقع منجر به تغییر در مکانیسم ارتکاب جنایات تروریستی از مرحله آماده‌سازی به جرم و پنهان کردن آثار آن است.

این شرایط همچنین باید در هنگام توسعه اقدامات سازنده و مؤثر برای مقابله با جرایم تروریستی در نظرگرفته شود. فناوری‌های دیجیتال مدرن باید به طور فعال در فرایند شناسایی، افشا و تحقیق در مورد جرایم تروریستی مورد استفاده قرارگیرند؛ به ویژه هنگامی که آن‌ها در فضای دیجیتال (سایبری) و همچنین با استفاده از فناوری‌ها انجام می‌شوند. یک جنبه مهم در این زمینه امکان استفاده از هوش مصنوعی توسط واحدهای عملیاتی- تحقیقاتی (به عنوان مثال، یک سیستم تشخیص چهره، شناسایی افراد، شماره خودرو، نظارت بر شبکه‌های اجتماعی و غیره) است.

فضای دیجیتال می‌تواند به طور مؤثر برای انجام اقدامات عملیاتی و اطلاعاتی، جمع‌آوری اطلاعات استخراج‌شده از پیام‌ها در وب‌سایت‌ها، اتاق‌های چت و سایر منابع دیجیتال که به پیشگیری و سرکوب به موقع اقدامات تروریستی کمک می‌کند، تأثیر بگذارد.

یکی دیگر از اقدامات متقابل ایجاد وب‌سایت‌ها، گروه‌های چت، انجمن‌های چت و سایر سیستم عامل‌های اینترنتی برای بحث‌های آنلاین، تظاهرات ضد تروریسم و سایر مواد آموزشی بر اساس حقایق مشخص، ارائه روش‌های جایگزین غیر خشونت‌آمیز برای حل مشکلات سیاسی و سایر مشکلات اجتماعی است.

برای شناسایی مؤثر، افشا و تحقیق در مورد جرایم تروریستی انجام شده در فضای دیجیتال (سایبری) و یا با استفاده از فناوری‌های دیجیتال، مأموران اجرای قانون باید نه تنها دانش قانونی، بلکه

دانش فنی ویژه‌ای در مورد مکانیسم ارتکاب این جنایات داشته باشند. آن‌ها باید فناوری‌ها، سیستم‌ها و برنامه‌های دیجیتال مدرن (کامپیوتر، اطلاعات و ارتباطات)، مکانیسم و روش عملیات خود را بدانند.

بنابراین، به منظور اطمینان از اثربخشی اقدامات برای مقابله با جرایم تروریستی انجام‌شده در فضای دیجیتال (سایبری) و یا استفاده از فناوری‌های دیجیتال، یک استراتژی روشن و یک چارچوب نظارتی مناسب مورد نیاز است که باید هدف قرارگیرد:

۳. تغییر در شدت مجازات جرم اقدامات اجتماعی خطرناک (از جمله اقدامات تروریستی) در فضای دیجیتال و یا با استفاده از فناوری‌های دیجیتال است. برای انجام این کار، لازم است که قانون کیفری و سایر اقدامات قانونی نظارتی در زمینه فناوری‌های دیجیتال به منظور شناسایی شکاف در حفاظت قانونی از اشیاء از تهدیدات تروریستی و تعیین نیاز به تقویت مسئولیت در موارد خاص، تجدید نظر شود. ما اعتراف می‌کنیم که ارتکاب جرایم در فضای دیجیتال (سایبری) و یا با استفاده از فناوری‌های دیجیتال ممکن است در همه موارد میزان خطر عمومی اقدامات ممنوعه را افزایش دهد.

۴. تقویت نیروها و ابزارها برای فعالیت‌های آموزشی، از جمله در فضای دیجیتال (سایبری)، با هدف ترویج همزیستی مسالمت‌آمیز همه مردم، صرف نظر از نژاد، ملیت و زبان در مقابل اطلاعات منفی و تأثیر ایدئولوژیک بر فرد از خارج، از جمله تبلیغات ایدئولوژی تروریسم (Ishchuk Ya,2021:47). آموزش مأموران اجرای قانون شناسایی، تحقیق در مورد جرایم، از جمله جرایم تروریستی در فضای دیجیتال (سایبری) و یا با استفاده از فناوری‌های دیجیتال.

۵. توانمندسازی مأموران اجرای قانون برای اطمینان از کنترل روشن و مؤثر محتوای دیجیتال.

۶. توسعه توافقنامه‌های همکاری بین‌المللی در زمینه مبارزه با جرایم، از جمله جرایم تروریستی، در فضای دیجیتال (سایبری) و یا با استفاده از فناوری‌های دیجیتال.

فهرست منابع:

الف- فارسی

۱. راهداری، علیرضا (۱۳۹۲). **سایبر تروریسم در هفت گام**. انتشارات نظری.

۲. قنبری، محمد (۱۳۹۸). **امنیت عمومی و تهدیدهای تروریستی**. انتشارات دانشگاه و پژوهشگاه عالی

ب- انگلیسی

3. Antonova, E. Yu. (2018). **Terrorism as the ideology of violence**. Vestnik Dalnevostochnogo yuridicheskogo instituta

4. T. Scrivens, R. & Venkatesh, V. (2020). **The role of the internet in facilitating violent extremism: insights criminal infringements**. *doctrine, law, and law enforcement*. Moscow: Yurlitinform. (In Russ). Gaudette,

5. Kraidy, M. (2018). **Terror, territoriality, temporality: Hypermedia events in the age of Islamic state**. *Cultural Research*, 56(4), 385-418. https://doi.org/10.1177/10693971221085343

6. Grobbelaar, A. (2022). **Media and Terrorism in Africa**. Al-Shabaab's Evolution from Militant Group to Media.

7. Kearns, Erin; Betus, Allison; Lemieux, Anthony (2018). **Why Do Some Terrorist Attacks Receive More Media Attention Than Others?**. *SSRN Electronic Journal*. doi:10.2139/ssrn.2928138. ISSN 1556-5068.

8. Huddy, L. Smirnov, O. Snider, K. L. G. & Perliger, A. (2021). **Anger, Anxiety, and Selective Exposure to Terrorist Violence**. Journal of Conflict Resolution, 65(10), 1764-1790. Mogul. Insight on Africa, 75(1), 7-22. https://doi.org/10.1177/09750878221114375

9. Ishchuk, Ya. G. Pinkevich, T. V. & Smolyaninov, E. S. (2021). **Digital criminology**. tutorial. Moscow: Akademiya. https://doi.org/10.1177/00220027211014937

10. Antonova, E. Yu. (2022). **Technologies of artificial intelligence - a subject or a tool/means of crime?**. Yuridicheskiy vestnik Kubanskogo gosudarstvennogo universiteta, 1, 31 -39. MVD Rossii, 2(43), 69-74. (In Russ).

11. Dingji Maza, K. Kolda§, U. & Aksit, S. (2020). **Challenges of Combating Terrorist Financing in the Lake Chad Region: A Case of Boko Haram**. SAGEOpen, 70(2), 215824402093449. https://doi.org/10.31429/20785836-14-1 -31-39

12. Dremlyuga, R. I. (2022). **Criminal-legal protection of digital economy and informational society against cyber**. https://doi.org/10.1177/2158244020934494

13. Kydd, Andrew H. Walter, & Barbara F. (2006). **The Strategies of Terrorism**. International Security, 31(1), 49-80. New Media, 79(2), 170-176.

14. Liem, M. van Buuren, J. de Roy van Zuijdewijn, J. Schönberger, H. & Bakker, E. (2018). **European Lone Actor Terrorists Versus "Common" Homicide Offenders: An Empirical Analysis**. *Homicide Studies*, 22(1), 45-69.

15. Makinda, S. (2016). **Terrorism in International Society: An Eclectic Perspective**. https://doi.org/10.1177/1088767917736797

16. Nossek, H. (2008). **'News media'-media events: Terrorist acts as media events**. Communications, 33(3), 313-330.

17. Orehek, E. & Vazeou-Nieuwenhuis, A. (2014). **Understanding the Terrorist Threat: Policy Implications of a Motivational Account of Terrorism: Policy Implications of a Motivational Account of Terrorism**. *Policy Insights From the Behavioral and Brain Sciences*, 7 (1), 248-255. https://doi.org/10.1177/2372732214549747 Polo, S. M. T. (2020). **How Terrorism Spreads: Emulation and the Diffusion of Ethnic and Ethnoreligious Terrorism**.

18. Rafat Mahmood, and Michael Jetter (2019). **Communications Technology and Terrorism**.

19. Russkevich, E. A. Dmitrenko, A. P. & Kadnikov, N. G. (2022). **Crisis and palingenesis (rebirth) of criminal law under digitalization**. Vestnik Sankt-Peterburgskogo universiteta. Pravo, 13(3), 585-598. (In Russ).

20. Sandler, T. (2013). **The analytical study of terrorism**. *Journal of Peace Research*, 57 (2), 257-271. https://doi.org/10.21638/spbu14.2022.301

21. Saha K. Chandrasekharan E. De Choudhury M. (2019). **Prevalence and psychological effects of hateful speech in online college communities**. *In Proceedings of the 10th ACM conference on web science* (pp. 255–264). [PMC free article] [PubMed]

22. Schwartz, Carly. (2014). **Majority of Americans Think Watching ISIS Beheadings Is Disrespectful**.

23. Shchetinina, E. V. (2018). **Problems of development of the culture of violence in the Internet space**. Innovatsionnoe

24. Tornberg, P. & Tornberg, A. (2022). **Inside a White Power echo chamber: Why fringe digital spaces are polarizing**.

25. Uusitalo, N. Valaskivi, K. & Sumiala, J. (2021). **Epistemic modes in news production: How journalists manage ways of knowing in hybrid media events involving terrorist violence**. *Journalism*, 23(9), 1811-1827.

26. Keenan, P. K. (2019). **Creating spaces of public insecurity in times of terror: The implications of code/space for urban vulnerability analyses**. Environment and Planning C: Politics and Space, 37(1), 81 -101. Upravleniya MVD Rossii. (In Russ).

27. Khokhlov, N. & Korotayev, A. (2022). **Internet, Political Regime and Terrorism: A Quantitative Analysis**. https://doi. org/10.1177/2399654418776660

28. Zedner, L. (2021). **Countering terrorism or criminalizing curiosity? The troubled history of UK responses to right-wing and other extremism**. *Common Law World Review*, 50(1), 57-7