نوع مقاله: پژوهشی
تاریخ دریافت: ۱۴۰۳/۱۲/۲۵
تاریخ پذیرش: ۱۴۰۴/۰۳/۱۵
صفحه: ۳۵ الی ۵۷

Applied Criminology Research
پژوهش های جرم شناسی کاربردی

Volume 3, Issue 7, Spring 2025
Received: 2025/03/15
Accepted: 2025/06/05
Pages: 35-57

System: qacr.ir
doi: 10.22034/AQCR.2024.2042435.1030
Article Type: **Research**

دوره ۳ / شماره ۷/ بهار ۱۴۰۴

Situational Prevention of Modern Terrorism in INTERPOL's Actions

Sadegh Salimi[1]

Abstract

Field and Aims: The threats posed by terrorism and the challenges surrounding its concept have led to complexities in the methods of combating this criminal phenomenon in terms of prevention and investigation. Since no country is immune to terrorism, nor can any country combat it alone, international cooperation in this field is of vital importance, with INTERPOL playing a prominent role.

Method: This article is written using a descriptive-analytical approach.

Findings and Conclusions: There are two approaches to defining terrorism, inductive and deductive. The inductive approach is primarily based on specific instances of terrorism, while the deductive approach begins with a general definition of terrorism and applies it to specific cases. Regarding INTERPOL's preventive measures against terrorism, key actions include identifying suspects and criminals through biometric data, preventing terrorist travel, tracking terrorist financial resources, and preventing bioterrorism, radiological terrorism, and nuclear terrorism.

Keyword: INTERPOL, Terrorism, Crime Prevention, Terrorism Financing, Terrorist Activities.

Citation (APA): Salimi, S. (2025). Situational Prevention of Modern Terrorism in INTERPOL's Actions. *Applied criminology research*, 3(7), 35-57.
https://qacr.ir/article_719194.html?lang=en

1. Associate Professor, Department of Public International Law, Faculty of Law, Central Tehran Branch, Islamic Azad University, Tehran, Iran. Email: sadegsalimi@yahoo.com

Volume 3, Issue 7, Spring 2025

Received: 2025/03/15
Accepted: 2025/06/05
Pages: 35-57

پژوهش های جرم شناسی کاربردی
Applied Criminology Research

نوع مقاله: پژوهشی

تاریخ دریافت: ۱۴۰۳/۱۲/۲۵
تاریخ پذیرش: ۱۴۰۴/۰۳/۱۵
صفحه: ۳۵ الی ۵۷

Article Type: **Research**
doi: 10.22034/AQCR.2024.2042435.1030
سامانه: qacr.ir

دوره ۳ / شماره ۷/ بهار ۱۴۰۴

پیشگیری وضعی از تروریسم مدرن در اقدامات اینترپل

صادق سلیمی[۱]

چکیده

زمینه و هدف: تهدیدات ناشی از تروریسم و چالش‌های موجود پیرامون مفهوم آن، موجب پیچیدگی در شیوه‌های مقابله با این پدیده مجرمانه در پیشگیری و پیگیری آن شده است. از آنجایی‌که هیچ کشوری از تروریسم در امان نیست و همچنین نمی‌تواند به‌تنهایی با تروریسم مقابله نماید، لذا همکاری‌های بین‌المللی در این زمینه اهمیت حیاتی دارد که نقش اینترپل در این زمینه برجسته است.

روش: این مقاله به شیوه توصیفی- تحلیلی نگارش یافته است.

یافته‌ها و نتایج: پیرامون تعریف تروریسم دو رویکرد استقرایی و قیاسی وجود دارد که رویکرد استقرایی بیشتر مبتنی بر مصادیق تروریسم است. ولی رویکرد قیاسی با یک تعریف کلی از تروریسم شروع می‌شود و آن را بر مصادیق اعمال و تطبیق می‌کند. پیرامون اقدامات پیشگیرانه از تروریسم توسط اینترپل می‌توان به مواردی چون شناسایی متهمین و مجرمین از طریق داده‌های بیومتریک، پیشگیری از مسافرت تروریست‌ها، پیشگیری از طریق ردیابی منابع مالی تروریست‌ها، پیشگیری از بیوتروریسم، تروریسم رادیولوژیکی و هسته‌ای، اشاره نمود.

کلیدواژه‌ها: اینترپل، تروریسم، پیشگیری از جرم، تأمین مالی تروریسم، اقدامات تروریستی.

استناددهی (APA): سلیمی، صادق. (۱٤۰٤). پیشگیری وضعی از تروریسم مدرن در اقدامات اینترپل. *پژوهش‌های جرم‌شناسی کاربردی*، ۳(۷)، ۵۷-۳۵.

https://qacr.ir/article_719194.html

۱. دانشیار گروه حقوق بین‌الملل عمومی دانشکده حقوق، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران.
رایانامه: sadegsalimi@yahoo.com

مقدمه

هر زمان که دنیا به یک جهش فناوری دست می‌یابد، مجرمین و تروریست‌هایی وجود دارند که از آن استفاده می‌کنند. تا سال ۲۰۰۰ تمام گروه‌های تروریستی حضور خود را در فضای اینترنت تثبیت کردند. به‌عبارت دیگر ما شاهد به خدمت گرفتن فناوری سایبر توسط گروه تروریستی هستیم و این شروع تروریسم مدرن بود. با افزایش تهدید تروریسم بین‌المللی برای صلح و امنیت جهانی، جامعه بین‌المللی باید به دنبال راه‌هایی برای تقویت پیوندهای همکاری میان اعضای خود در مبارزه با تروریسم باشد. همچنین امروزه تسلیحات تروریستی غیرمتعارف نگرانی خاصی را برای جامعه جهانی به همراه دارند.

ویلکینسون چهار نوع تروریسم را تعریف کرده است: جنایی، روانی، جنگی و سیاسی. یکی از اهداف تروریسم تحریک مقامات به استفاده از اقدامات غیرقانونی، خلاف قانون اساسی و سرکوبگرانه و درنتیجه از دست دادن حمایت عمومی است (سن[1]، ۱۹۹۳: ۳۷). در خصوص جرم بین‌المللی بودن تروریسم آنتونیو کاسسه می‌گوید: «به نظر من می‌توان ادعا نمود که از این گذشته دست‌کم تروریسم بین‌المللی، تروریسم مورد حمایت دولت یا تروریسمی که دولت بر آن چشم می‌پوشد، جنایتی بین‌المللی است و هم‌اکنون به‌موجب حقوق بین‌الملل عرفی به عنوان نوع مجزایی از این‌گونه جرایم در نظر گرفته شده و ممنوع است.»(کاسسه، ۱۳۸۰: ۳۸۵). در خصوص ضرورت مقابله با تروریسم باید گفت عملکرد گروه‌های تروریستی، ضمن آنکه امنیت داخلی کشورها را به مخاطره می‌اندازد، موجب بر هم خوردن نظم و امنیت بین‌المللی نیز می‌گردد. امروزه و با گسترش مفهومی بنام جهانی‌شدن، منافع اعضای جامعه بین‌المللی بیش از پیش به هم گره خورده است. بر این اساس آثار بر هم‌خوردن نظم و امنیت در یک کشور در پی ایجاد و فعالیت گروه‌های تروریستی تنها محدود به خاک آن کشور نیست و ابعاد جهانی خواهد یافت (بندک[2]، ۲۰۱۰: ۷)؛ لذا پیشگیری از تروریسم با همکاری بین‌المللی به عنوان نوعی اقدام بازدارنده دارای اهمیت می‌باشد.

مبارزه با تروریسم به اقداماتی تدافعی گفته می‌شود که برای کاهش آسیب‌پذیری‌های فردی و اجتماعی از اعمال تروریستی با استفاده از نیروهای نظامی محلی و مدنی انجام می‌شود (دود[3]، ۲۰۰۹: ۳۹). در واقع مقابله با تروریسم به معنای آن است که در حالی‌که به معلول (اقدامات تروریستی) پاسخ می‌دهد به علت‌ها و ریشه‌های تروریسم هم توجه دارد، از منظری دیگر، به اقدامات، تکنیک‌ها، تاکتیک‌ها و استراتژی‌هایی گفته می‌شود که دولت‌ها، نیروهای نظامی و پلیس به‌منظور جلوگیری و پاسخ دادن به اقدامات و یا تهدیدات انجام می‌دهند

1. Sen
2. Benedek
3. Dod

(ناکووس[1]، ۲۰۰۸: ۱۶۹–۲۱۸). پیشگیری همواره بهتر از پیگیری هست و هرچه جرم خطرناک‌تر باشد اهمیت این امر نیز بیشتر می‌شود؛ بنابراین پیشگیری از تروریسم اهمیت مضاعفی دارد. در خصوص پیشگیری از تروریسم اقدامات و سیاست‌هایی در دستور کار اینترپل قرار دارد که مطالعه آن هدف اصلی این مقاله می‌باشد. لیکن ابتدا باید معنی و مفهوم تروریسم را روشن کرد.

۱. مفهوم تروریسم و جرایم مشابه

تروریسم درگذر زمان از نظر معنا دچار نوسان شده و تعاریف مختلف، منعکس‌کننده ایده‌هایی هستند که به دوره زمانی و مکانی خاصی مربوط می‌شوند. بسیاری از مطالعات ریشه‌شناسی درباره ریشه‌های تروریسم، خاستگاه اولیه این واژه را به دستاوردهای انقلاب فرانسه و «حکومت وحشت» ماکسیمیلیان روبسپیر بین سال‌های ۱۷۹۲ و ۱۷۹٤ بازمی‌گردانند (هافمن[2]، ۲۰۰٦: ۲). در اواخر قرن نوزدهم و اوایل قرن بیستم، به‌ویژه پس از ترور رئیس‌جمهور ایالات متحده ویلیام مک کینلی[3] در سال ۱۹۰۱ توسط لئون چولگوس[4] یک آنارشیست که به این امر اعتراف کرده بود، تروریسم اغلب برای اشاره به آنارشیست‌ها مورد استفاده قرار می‌گرفت. ارتباط این موضوع با «مبارزان آزادی» درنتیجه مبارزات مجدد برای استقلال ایرلند از بریتانیا با استفاده از تاکتیک‌هایی مانند بمب‌گذاری، تکنیک‌های ترور و جنگ چریکی برقرار شد.[5]

با این حال، این تحول مفهومی تروریسم مورد حمایت دولت‌ها نبود. در دهه ۱۹۳۰، به دلیل ظهور رژیم‌های خشونت‌طلب و مستبد در ایتالیا، اسپانیا و آلمان نازی، تروریسم دوباره با خشونت‌هادولتی مرتبط شد (هافمن، ۲۰۰٦: ۹–۷). پس از پایان جنگ جهانی دوم و افول امپراطوری‌های اروپایی، تروریسم دوباره با مبارزان آزادی و روش‌های خشونت‌آمیز مورد استفاده گروه‌های مختلف ضد استعماری که به دنبال تعیین سرنوشت خود بودند، پیوند خورد (گرینه[6]، ۲۰۱۷: ٤١٤). امروزه این دو موضوع که آیا دولت‌ها می‌توانند مرتکب تروریسم شوند و اینکه آیا می‌توان تروریست‌ها را از مبارزان آزادی‌خواه در حال مبارزه با یک رژیم سرکوبگر

1. Nacos
2. Hoffmann
3. William McKinley
4. Leon Czolgosz

۵. بریتانیا در گذشته اصرار داشت که به دلیل مبارزاتش با ارتش جمهوری ایرلند (IRA) هیچ تفاوتی بین تروریست‌ها و مبارزان آزادی قائل نمی‌شود.

6. Greene

متمایز کرد یا خیر، مشکلات اساسی است که تلاش‌ها برای ارائه تعریفی از تروریسم را با چالش[1] مواجه ساخته است.

یک پژوهش معروف در سال ۱۹۸۸ بیش از ۱۰۰ تعریف مورد استفاده توسط محققان تروریسم را جمع‌آوری کرده است که این پژوهش خود به‌عنوان یک وضعیت انحرافی توصیف شده است؛ زیرا در آن تعداد زیادی از محققان در حال مطالعه یک پدیده هستند که اساساً با هم توافق دارند که مخالف هم نظر دهند و اتفاق نظری وجود ندارد. در حالی‌که قانون صرفاً جنبه توصیفی و تبیینی ندارد، بلکه قدرت آمره یا نهی‌کننده دارد. عوامل هنجاری که یک قانون آمره باید واجد آن باشند شاید یک جامعه‌شناس خود را ملتزم به رعایت آن نداند. مطالعات مرتبط با تروریست که ساختارهای قدرت را در برچسب زدن یک رویداد یا فرد به‌عنوان «تروریست» بررسی می‌کنند، نشان می‌دهد که تروریسم یک اصطلاح تحقیرآمیز همراه با محکومیت اجتماعی هست که از انگیزه سیاسی اصلی این اعمال مشروعیت زدایی می‌کند (گرینه، ۲۰۱۷: ٤١٧). به‌منظور تعریف تروریسم دو رویکرد وجود دارد که شامل رویکرد استقرایی و قیاسی می‌باشد. رویکرد استقرایی بیشتر مبتنی بر مصادیق تروریسم است و لذا شاهد شکل‌گیری کنوانسیون‌های مختلف مانند کنوانسیون‌های مربوط به هواپیماربایی هستیم.[2] برخلاف رویکرد استقرایی، رویکرد قیاسی با یک تعریف کلی از تروریسم شروع می‌شود و آن را در بسیاری از شرایط مختلف اعمال می‌کند. برای اینکه استدلال قیاسی به‌طور مؤثر عمل کند، فرضیه اولیه باید درست باشد و درواقع باید در مورد آن توافق شود و این مانعی است که حقوق بین‌الملل هنوز نتوانسته از آن عبور کند (کر[3]، ۲۰۰۷: ٤٩)؛ به‌عبارت دیگر مانع اصلی در رسیدن به اجماع در ارائه تعریف مشخص از تروریسم استفاده از این اصطلاح برای اهداف سیاسی است. اگرچه در محافل آکادمیک تعریف‌هایی در این باره ارائه شده، اما در اسناد بین‌المللی شاهد ارائه تعریفی واضح و مشخص از این پدیده نیستیم (گیل و کرنر[4]، ۲۰۱۷: ۳). اما دو عامل مهم منجر به آن گردیده است که تروریسم از منظر بین‌المللی حائز اهمیت باشد، نخست اینکه هدف اصلی تروریست‌ها وادار کردن دولت‌ها به پذیرش خواسته‌های آنان است و دوم اینکه سطح عملیات تروریستی در ابعاد بین‌المللی می‌باشد. لذا مقابله با آن نیازمند اقدامات و همکاری‌های بین‌المللی است، اما برای رسیدن به مطلوب لازم است تا پیشتر، اجماعی بین‌المللی در زمینه تعریف تروریسم ارائه شود.

---

۱. لازم به ذکر است که تلاش‌ها برای درک تروریسم طیف وسیعی از روش‌شناسی‌ها، پارادایم‌ها و شاخه‌های مختلف دانش را به وجود آورده است.

۲. مهم‌ترین اسناد بین‌المللی عبارت‌اند از: کنوانسیون‌های ۱۹٤٤ شیکاگو، ۱۹٦۳ توکیو، ۱۹۷۰ لاهه، ۱۹۷۱ مونترال.

3 .Carr

4. Gill & Corner

۱-۱. تسلیحات مدرن و تروریسم سایبری

تروریست‌ها همگام با پیشرفت فناوری و فضای مجازی خود را با سلاح‌های نو، وسایل حمل‌ونقل مدرن و جدیدترین سخت‌افزار و نرم‌افزار رایانه‌ای تجهیز کرده‌اند. نوآوری‌ها در فناوری تسلیحات، سلاح‌های کشنده را کوچک‌تر و قابل حمل‌تر و در عین‌حال شناسایی آنها را دشوارتر نموده است. صنعت حمل‌ونقل مدرن نه‌تنها تروریست‌ها را قادر می‌سازد تا با عبور از مرزها ویرانی را به سراسر جهان منتقل کنند، بلکه اهداف آسیب‌پذیرتری را در دسترس مرتکبین حملات تروریستی قرار می‌دهند. مهم‌تر از همه، تروریسم مدرن از توسعه و گسترش رسانه‌های جمعی و ارتباطات الکترونیکی مدرن بهره برده است که ابزارهای مفیدی را برای هماهنگی حملات در مکان‌های مختلف در اختیار تروریست‌ها قرار داده است (گانور[1]، ۲۰۰۳: ۹). برای این منظور حداقل دانش شیمی همراه با یک آزمایشگاه ابتدایی و چند ماده اولیه که بیشتر آنها را می‌توان به‌راحتی خریداری کرد، برای انجام یک عملیات تروریستی که می‌تواند توده‌های مردم را بکشد کافی است.

گروه‌های تروریستی مدرن از سلاح‌های قابل حمل استفاده می‌کنند، در گروه‌های غیرمتمرکز کوچک فعالیت می‌کنند، اغلب از قاچاق مواد مخدر کسب سرمایه می‌کنند، بر انعطاف‌پذیری در عملیات خود تأکید دارند و به‌طور فزاینده‌ای شهری هستند (سن، ۱۹۹۳: ۳۷). برای اینکه تروریست‌ها بتوانند تأثیر عملیات مرگبار خود را به حداکثر برسانند نیازمند تأثیر بر افکار عمومی از طریق افزایش ترس و اضطراب در بین مردم هستند. کشوری که با تروریسم گسترده مواجه است باید تلاش‌های فکری و فیزیکی خود را بر حفظ روحیه مثبت در میان شهروندان خود متمرکز کند و در عین‌حال توانایی دولت را برای مقابله با تهدید تروریسم تقویت کند.

«تروریسم سایبری» اصطلاح نسبتاً جدیدی هست که گاهی در مفهوم کلی و مصداقی از «جرم سایبری» به کار می‌رود و گاهی برای اینکه از یک جرم ساده سایبری متمایز شود و اهمیت و گستردگی عمل را نشان دهد، «حمله سایبری» نامیده می‌شود، ولی این دو را نیز نباید یک مفهوم پنداشت. حمله سایبری[2] می‌تواند حوزه گسترده‌ای از یک جرم سایبری که از ناحیه یک فرد با قصد و انگیزه شخصی صورت می‌گیرد تا تروریسم سایبری و حتی جنگ سایبری را در برگیرد. از دیدگاه نوشته‌هایی که تروریسم سایبری را از بعد امنیتی بررسی کرده‌اند، تفاوتی اندک میان تروریسم سایبری و جرم سایبری وجود دارد؛ اما باید گفت، جرم سایبری یک حمله انفرادی است و با قصد رعب و وحشت و پیشینه ایدئولوژیک یا قصد فشار بر دولت انجام نمی‌شود. اگر اطلاعات کارت بانکی فردی سرقت شود جرم به حساب می‌آید، اما

1. Ganor
2. Cyber attack

قطع برق یک شهر مسلماً چیزی بیش از یک جرم است؛ بنابراین جرم سایبری در مفهوم خاص خود و نه در ذیل حمله سایبری طبقه‌بندی می‌شود (ترشچنکو[1]، ۲۰۱۳: ٤).

برخی از به کار بردن واژه تروریسم سایبری خودداری نموده و از عنوان کلی‌تری به نام حملات سایبری استفاده می‌کنند. به نظر می‌رسد عنوان تروریسم سایبری از یک‌سو به حوزه حملات سایبری و با تجمیع شرایط و رسیدن به آستانه حملات مسلحانه، به جنگ سایبری نیز ارتباط می‌یابد. لذا عملکرد تابعان حقوق بین‌الملل در این حوزه به دریافت آن‌ها از مفهوم تروریسم سایبری بازمی‌گردد که آن را صرفاً حمله سایبری تلقی نموده یا واجد ویژگی‌های جنگ سایبری بدانند. صرف نظر از صاحب‌نظران حوزه تروریسم سایبری، دولت‌ها نیز هنگامی‌که بحث بررسی تهدیدهای تروریستی اینترنتی پیش می‌آید اغلب با هم اختلاف نظر دارند (میربد، ۱٤۰۳: ۱۸-۱۷).

سازمان‌های تروریستی سیستم‌های پویایی هستند که در طول زمان خود را با شرایط تطبیق می‌دهند و تکامل می‌یابند. به‌طور سنتی تصور می‌شد که سازمان‌های تروریستی ساختاری متمرکز و سلسله مراتبی دارند که در آن رهبران در رأس عملیات کل سازمان را کنترل می‌کنند. این امر کمک می‌کند تا زنجیره فرامین از سوی بالاترین فرماندهان به اعضاء انتقال یابد (کوچ[2]، ۲۰۱۸: ۲۷)؛ لذا آنچه تروریسم مدرن را از تروریسم سنتی متفاوت می‌نماید نه ساختار، بلکه شیوه‌های اقدامات تروریستی می‌باشد که در تروریسم مدرن شاهد بهره‌گیری از فناوری توسط این گروه‌ها می‌باشیم.

۲-۱. وصف فراملی اقدامات تروریستی

استفاده از فناوری‌های جدید و امکانات فضای مجازی موجب شده است مرزها بی‌معنا شود و به‌راحتی توسط تروریست‌ها پشت سر گذاشته شود. گسترش فزاینده گروه‌های تروریستی به‌طور فراملی و به‌عبارت‌دیگر «فراملی» شدن فعالیت‌های تروریستی چالش دنیای امروز ماست. با توجه به این واقعیت که ما در دنیایی جهانی شده زندگی می‌کنیم، سازمان‌های تروریستی فعالانه به سرزمین‌های خارجی گسترش می‌یابند و فعالیت‌هایی را خارج از منطقه عملیاتی خود انجام می‌دهند. در خصوص مفهوم جرم فراملی کنوانسیون ملل متحد علیه جنایات سازمان‌یافته فراملی سال ۲۰۰۰ موسوم به کنوانسیون پالرمو آن را تعریف کرده و برخی مطالعات جرم‌شناسی گسترش فراملی را عمدتاً در رابطه با جرایم سازمان‌یافته مورد مطالعه قرار داده‌اند. مفهوم «فراملی» در بند ۲ ماده ۳ کنوانسیون پالرمو در چهار بند بیان شده است: الف) در صورتی که جرم در قلمرو بیش از یک دولت ارتکاب یابد؛ ب) در سرزمین یک دولت ارتکاب یابد؛

1. Tereshchenko
2. Koch

ولی بخش مهمی از مقدمات، طرح‌ریزی، هدایت یا کنترل آن در دولت دیگری صورت پذیرد؛ ج) جرم در سرزمین یک دولت ارتکاب یابد؛ ولی توسط یک گروه جنایی سازمان‌یافته ارتکاب یابد که در سرزمین بیش از یک دولت به فعالیت اشتغال دارد؛ د) جرم در سرزمین یک دولت ارتکاب یابد؛ ولی آثار اساسی آن در سرزمین دولت دیگری بروز کند (سلیمی، ۱۳۹۱: ٦٨).

البته برخی پژوهشگران مانند کوترن و همکاران بر نزدیکی محل اقامت تروریست‌ها و فعالیت‌های عملیاتی آنها تأکید کرده‌اند. تحقیقات آن‌ها نشان می‌دهد که تروریست‌ها تمایل دارند در مناطق نزدیک به محل زندگی‌شان یا محل فعالیتشان حملاتی انجام دهند. آنها دریافتند که حدود نیمی از تروریست‌ها در شعاع ۳۰ مایلی از مکان‌های مورد نظر خود ساکن هستند و برای عملیات خود آماده می‌شوند. این نزدیکی ممکن است باعث راحتی لجستیکی، امنیت عملیاتی بیشتر و آشنایی عمیق‌تر با محیط هدف شود که می‌تواند برای اجرای مؤثر حملات مورد سوءاستفاده قرار گیرد (روزمو و هریس[1]، ۲۰۱۱: ۲۲٤). این افزایش دسترسی ممکن است منجر به فراوانی بیشتر حوادث تروریستی فراملی شود که نشان‌دهنده استفاده استراتژیک از مناطق مرزی است.

در پژوهشی دیگر که توسط ساویچ انجام شده است، محیط‌های شهری بسترهای منحصربه‌فردی را در زمینه تروریسم فراهم می‌کنند. تروریسم شهری با حملات در مناطق پرجمعیت، هدف قرار دادن غیرنظامیان و زیرساخت‌های کلیدی مشخص می‌شود. پیچیدگی محیط‌های شهری فرصت‌هایی را برای تروریست‌ها فراهم می‌کند تا با جمعیت غیرنظامی ترکیب شوند و از ناشناس بودن در شهرها سوءاستفاده کنند (ساویچ[2]، ۲۰۰۵: ۳٦۳).

نمث و همکاران بر شناسایی عوامل جغرافیایی و اجتماعی- اقتصادی که با بروز تروریسم داخلی مرتبط است، تمرکز نموده و اقدامات آنها نشان می‌دهد که چگونه شرایط خاص، مانند مناطق کوهستانی بودن مناطق، نزدیکی به مراکز ایالتی، جمعیت زیاد و تراکم بالای جمعیت و همچنین شرایط بد اقتصادی، می‌تواند زمینه‌های مناسبی برای فعالیت‌های تروریستی ایجاد کند (نمث و همکاران[3]، ۲۰۱٤: ۳۰۸).

بوفا و همکاران از مدل‌سازی چندعاملی برای شبیه‌سازی توزیع‌های اجتماعی و فضایی شبکه‌های تروریستی استفاده می‌کنند. هدف روش‌شناسی آن‌ها کشف رهبران، آسیب‌پذیری‌های سازمانی و نقاط حساس است. مطالعه دیگری که با هدف شناسایی رهبران و نقاط حساس و آسیب‌پذیر سازمان‌های تروریستی انجام گرفت نتیجه‌گیری شد که ماهیت ایدئولوژیک گروه‌های

1. Rossmo & Harries
2. Savitch
3. Nemeth et al

تروریستی می‌تواند بر انتخاب مکان آنها تأثیر بگذارد و بر محل برنامه‌ریزی و اجرای حملات تأثیرگذار باشد (بوفا و همکاران[1]، ۲۰۲۲: ۱۱).

درنهایت، در مورد مفهوم نقاط حساس تروریستی، «بریثویت» و «لی» به بررسی شناسایی و اثرات نقاط حساس تروریسم فراملی می‌پردازند. یافته‌های آنها نشان می‌دهد که کشورهایی که در این نقاط قرار دارند، بیشتر شاهد افزایش فعالیت‌های تروریستی هستند (بریثویت و همکاران[2]، ۲۰۰۷: ۲۸۷). تمامی این تحقیقات به‌طور صریح یا ضمنی این واقعیت را تأیید می‌کنند که فعالیت‌های تروریستی به سرزمین یا چارچوب مرزی خاصی محدود نیستند؛ همواره عوامل فراملی از قبیل محل تأمین بودجه، تابعیت مرتکبین، آثار جرم و نظایر آن آنها را ذاتاً فراملی کرده است.

۳-۱. وجوه تشابه و افتراق تروریسم و جنایت سازمان‌یافته فراملی

با توجه به اینکه جرایم تروریستی اغلب واجد اوصاف «سازمان‌یافته» و «فراملی» هستند لذا گاهی این جرایم مصداقی از جرایم سازمان‌یافته فراملی به نظر می‌رسند. بین مفهوم جنایات سازمان‌یافته فراملی و تروریسم مشابهت‌هایی وجود دارد. تروریسم جنایتی تلقی می‌شود که غالباً توسط گروه واجد تشکیلات و سازمان‌دهی خاص ارتکاب می‌یابد و نیز دامنه فعالیت و تأثیرگذاری آن از مرزهای یک دولت فراتر می‌رود. اگرچه معنای لغوی این دو دسته جنایت مشابهت‌هایی دارند، اما اگر به معنی فنی و اصطلاحی جنایت سازمان‌یافته فراملی آن‌گونه که در کنوانسیون پالرمو مورد تائید واقع شده، بنگریم، تروریسم از شمول جنایت سازمان‌یافته خارج خواهد شد (سلیمی، ۱۳۹۱: ٤٧).

در مورد وجوه تشابه و افتراق تروریسم و جنایت سازمان‌یافته فراملی می‌توان، وجود تشابه را در امکان ارتکاب فراملی تروریسم، سازمان‌دهی شده عمل کردن تروریست‌ها و مجنی علیه واقع شدن جامعه در هر دو جنایت اشاره نمود. در بعد اختلافات این دو دسته جرم آنچه اهمیت وافر دارد انگیزه ارتکاب جرم است که در تروریسم سایبری ایجاد رعب و وحشت و اجبار دولت یا سازمان به پذیرش خواسته‌های تروریست‌هاست درصورتی‌که در جنایت سازمان‌یافته انگیزه مالی در درجه اول اهمیت است. اگرچه تروریسم سایبری ممکن است توسط یک یا دو نفر و به شیوه غیر فراملی نیز رخ دهد و نیز سازمان‌دهی گروه‌های تروریستی که اغلب حملاتشان را برای جلب توجه انجام می‌دهند با سازمان‌دهی جنایات سازمان‌یافته که در خفا انجام می‌شوند، متفاوت است؛ اما به هر حال ارتباط متقابلی میان تروریسم سایبری و جنایات سازمان‌یافته فراملی ممکن است وجود داشته باشد (سلیمی، ۱۳۹۱: ۵۱-۵۰).

1. Buffa et al
2. Braithwaite et al

جرایم تروریستی اغلب محدود به سرزمین کشوری خاص نیستند و اغلب فرامرزی و فراملی عمل می‌کنند با این حال حتی در مواردی که عملیات تروریستی در قلمرو یک دولت واقع شده باشد، همواره احتمال فرار متهمین به خارج، تأمین مالی یا تأمین تسلیحاتی از خارج و اثرات فرامرزی اقدامات وجود دارد. برای پیشگیری و مقابله با این اقدامات که با وحدت فرماندهی و با سرعت انجام می‌گیرد، روش‌های سنتی همکاری دولت‌ها پاسخگو نیست و در نبود یک پلیس جهانی با وحدت فرماندهی و اختیارات کافی، سازمان اینترپل به نوبه خود تلاش کرده است این خلأ را از طریق فراهم نمودن همکاری و هماهنگی بین پلیس ملی دولت‌ها و ارتقای توان مبارزه آنان پر کند.

۲. شیوه‌های پیشگیری اینترپل از عملیات تروریستی

سازمان جنایی پلیس بین‌الملل یا همان اینترپل علاوه بر بانک‌های اطلاعات و اعلان‌های رنگی که اطلاعات و همکاری‌های ارزشمندی را میان دول عضو مهیا می‌کند و علاوه بر پروژه‌های موردی، در خصوص سه دسته جرایم برنامه‌های قابل توجهی دارد:

برنامه ضد تروریسم: که به منظور پیشگیری و سرکوب فعالیت‌های تروریستی از طریق شناسایی اعضای شبکه‌های تروریستی و وابستگی‌های آنها و شناسایی عوامل اصلی که می‌توانند فعالیت‌های آنها را عملی کنند ردیابی سفر و تحرک آنها، حضور آنلاین، تسلیحات و وسایل و بودجه مورد استفاده آنها انجام می‌گیرد.

برنامه مقابله با جرائم سایبری: در این خصوص هدف اصلی جرائم خاص سایبری یعنی جرائم علیه رایانه‌ها و سامانه‌های اطلاعاتی می‌باشد. در این مورد همچنین به جرائمی که از طریق سایبر تسهیل می‌شوند از قبیل استفاده از فناوری جهت تسهیل جرائمی مانند کلاهبرداری مالی و استفاده تروریست‌ها از رسانه‌های اجتماعی پرداخته می‌شود.

برنامه مقابله با جرائم سازمان‌یافته و جرایم در حال پیدایش: در این برنامه هدف سرکوب شبکه‌های مجرمانه سازمان‌یافته فراملی و شناسایی، تحلیل و پاسخ به تهدیدات در حال شکل‌گیری می‌باشد.[1]

همان‌طور که در مباحث پیشین بحث شد خود جرایم تروریستی با جرایم سایبری و سازمان‌یافته ارتباط و بلکه اشتراک دارند و لذا می‌توان ادعا کرد همه برنامه‌های سه‌گانه اینترپل به جرایم تروریستی و پیشگیری از آن مرتبط هستند.

گروه‌های تروریستی افراد، اغلب جوانان را تحریک می‌کنند تا جوامع خود را در سراسر جهان ترک کنند و به مناطق درگیری سفر کنند، در درجه اول در عراق و سوریه و به‌طور فزاینده‌ای

1. COM/FS/2020-01/GI-01

در لیبی. نحوه هدف‌گیری و رادیکالیزه شدن افراد استخدام شده با تمرکز بیشتر بر رسانه‌های اجتماعی و سایر کانال‌های دیجیتال تغییر کرده است.

امروزه مطالعات جرم‌شناسی در حوزه جرایم تروریستی در جرم‌شناسی فراملی یا جهانی یا جرم‌شناسی جرائم جهانی شده، شکل‌گرفته است. البته در کنار این جرم‌شناسی‌های خاص، به فراخور جرم توجه ویژه‌ای به جرم‌شناسی پیشگیری به‌عنوان یک جرم‌شناسی خاص از منظر دیگر نیز توجه شده چه موضوع مطالعه آن بحث پیشگیری از جرم به‌طور کلی و پیشگیری از انواع جرائم به طور خاص از جمله جرائم جهانی شده و تروریسم است. (مرادی و کاظمی، ۱۳۹۶: ۳۷)

تروریسم بنابه مخاطرات جدی که دارد مستلزم تدابیر ویژه‌ای هم هست. جرم‌انگاری پیش‌دستانه اعمال تروریستی یکی از جلوه‌های افزایش مداخله حقوق کیفری است که استفاده از اصل حداقلی و کمینه حقوق جزا را نقض می‌کند. ماهیت خطرناک و خشونت‌آمیز جرائم تروریستی و حالت خطرناک مجرمان آن نقش مؤثری در شکل‌گیری جرم‌انگاری پیش‌دستانه داشته است. راهبرد ضد تروریسم جرم‌انگاری پیش‌دستانه که نمونه‌ای از حقوق کیفری پیشا جرم است، گستره وسیع‌تری از رفتارها و افراد را نسبت به حقوق کیفری پساجرم شامل می‌شود. جرم‌انگاری پیش‌دستانه با پیشگیری سرکوبگرانه، قلمرو و فضای مداخله در سیاست جنایی را توسعه می‌دهد.[۱] جرم‌انگاری پیش‌دستانه در حوزه تروریسم، رویکرد پساجرم حقوق کیفری را به رویکرد پیشاجرم تغییر می‌دهد و به دنبال ادغام مفهوم امنیت در عدالت کیفری است.[۲]

از جمله مهم‌ترین اقداماتی که پلیس در مواجهه با مجرمان تروریستی در دستور کار خود قرار داده است، ارتقاء توان اطلاعاتی- عملیاتی و به‌کارگیری اشراف اطلاعاتی در شناسایی و دستگیری تروریست‌ها است. از این‌رو، خبرگان و صاحب‌نظران معتقدند که اشراف اطلاعاتی بر نحوه فعالیت‌ها و اقدامات به‌ویژه تأمین مالی تروریسم مقاصد گروه‌های تروریستی و افراطی، از الزامات اساسی در کنترل و پایش این جرم است. (نمامیان، امیری، نجات و شعبانلی، ۱۴۰۱: ۹)

در حقوق بین‌الملل دولت‌ها متعهدند که از اقدامات تروریستی حمایت نکنند و اقدامات مؤثری را در جهت پیشگیری و مبارزه با تروریسم انجام دهند؛ اما متأسفانه دولت‌ها به‌صورت ارتکاب مستقیم اعمال تروریستی یا تحریک به ارتکاب این اعمال، عدم پایبندی خود به مفاد

---

۱. رک: شاهیده فرهاد و نیاز پور امیرحسن، جرم‌انگاری پیش‌دستانه اعمال تروریستی، آموزه‌های حقوق کیفری، دانشگاه علوم اسلامی رضوی، دوره هفدهم، شماره ۱۹ بهار تابستان ۱۳۹۹، ص ۱۲۶-۱۲۵.
۱۲۳-۱۶۰.
۲. همان، ص ۱۲۶.

این تعهد را نشان می‌دهند.[1] اف ای تی اف یکی از نهادهای مؤثر بین‌المللی است که به‌عنوان یک سیاست‌گذار با ایجاد استانداردهای بین‌المللی سیاست‌ها و روش‌های مبارزه با پول‌شویی و تأمین مالی اقدامات تروریستی را تعیین می‌کند، سیاست جنایی ایران در مسیر تعامل خود با اف ای تی اف مواجه با تعارضاتی می‌باشد. جهت مطالعه تفصیلی این موارد می‌توان به منابع موجود مراجعه کرد.[2] گروه ویژه اقدام مالی یا همان اف ای تی اف برای بانک‌ها و مؤسسات مالی نیز الزامات سخت‌گیرانه‌ای جهت احراز هویت مشتری و معاملات وی و حتی هدف از معاملات ایجاد نموده است تا هم کسانی که تبادل مالی می‌کنند و هم اهداف این معاملات روشن باشد و از تأمین مالی تروریسم نیز پیشگیری شود.[3]

در خصوص مفهوم پیشگیری غیر کیفری و خصوصیات آن تعاریف متعددی ارائه گردیده است. در یک تعریف، موریس کوسن جرم‌شناس کانادایی پیشگیری غیر کیفری را چنین تعریف کرده است:«مجموعه اقدام‌ها و تدابیر غیر قهرآمیز که با هدف خاص مهار بزهکاری، کاهش احتمال جرم و کاهش وخامت جرم پیرامون علل جرایم اتخاذ می‌شود.»(ابراهیمی، ۱۳۹۰،۳۸). از میان تقسیم‌بندی‌های مختلفی که در خصوص تدابیر پیشگیرانه صورت گرفته است دو نوع پیشگیری اجتماعی و پیشگیری وضعی بیشترین مقبولیت را دارد.

۱-۲. شناسایی مظنونین یا تروریست‌ها از طریق داده‌های بیومتریک

داده‌های بیومتریک مانند تصاویر چهره و اثر انگشت می‌تواند منجر به شناسایی دقیق افرادی شود که از هویت جعلی استفاده می‌کنند و در نتیجه تلاش‌ها برای شناسایی تروریست‌ها و انجام تحقیقات و پیگردهای موفق را بهبود می‌بخشد.

توانایی اندازه‌گیری و تجزیه و تحلیل ویژگی‌های رفتاری (امضا، صدا، راه رفتن) و ویژگی‌های بیولوژیکی (فیزیولوژیکی و تشریحی) (اثر انگشت، هندسه کف دست، الگوی عنبیه، شبکیه چشم) بیومتریک را تشکیل می‌دهد. فناوری‌های بیومتریک از این ویژگی‌ها به‌عنوان وسیله‌ای برای شناسایی افراد استفاده می‌کنند (ارشاد، حیات و خان[4]، ۲۰۱۵: ۱۲).

اهمیت این موضوع در این است که اعتبار شناسایی و تأیید هویت مانند رمزهای عبور و نشانه‌ها معمولاً فراموش می‌شوند و به سرقت می‌روند، اما شناسایی بیومتریک شخصی است و

---

۱. کارگری، نوروز، درون‌مایه‌های تروریست، تهران، انتشارات میزان، ۱۳۹۱، ص. ۱۱۰.

۲. رک: طالع، غلامرضا و میرزاجانی، حمیدرضا، سیاست جنایی ایران در قبال تامین مالی تروریسم در مواجهه با توصیه‌ها و برنامه اقدام اف ای تی اف، نشریه علمی پژوهش‌نامه حقوق کیفری، سال سیزدهم، شماره دوم پاییز و زمستان ۱۴۰۱، شماره پیاپی ۲۶ ۰ صص ۲۴۱ الی ۲۶۹.

۳. برای مطالعه بیشتر رجوع کنید به: علیزاده، غزاله، شامبیاتی، هوشنگ و سلیمی، صادق، پیشگیری از تامین مالی تروریسم و پول‌شویی با بهره‌گیری از شناسایی ریسک مشتری، مجله پژوهش‌های حقوقی، دوره ۲۱، شماره ۵۰، تابستان ۱۴۰۱، صفحه ۱۶۴ و ۱۶۵ صفحه ۱۵۷ الی ۱۸۵.

4. Arshad, Hayat & Khan

نمی‌توان آن را گم یا فراموش کرد (گوپتا، ۲۰۱۵: ۳). چشم‌انداز آینده دستگاه‌های بیومتریک و فناوری مرتبط با آن و همچنین استراتژی‌هایی که می‌توانند برای کنترل خطر و تهدید امنیتی امروزی تقویت شوند، یک ابزار حیاتی مبارزه با تروریسم است که باید آن را ارتقاء داد (کالدول[1]، ۲۰۱۵: ۷). خدمات کنترل مهاجرت و امنیت چندین دهه است که از سیستم‌های بیومتریک نظارت شده در مرزهای کشورهای مختلف استفاده می‌کنند. از زمان حمله تروریستی ۱۱ سپتامبر در ایالات متحده، اکثر کنترل‌های مرزی به‌تدریج از سیستم‌های بیومتریک برای گرفتن داده‌های زیستی هر کسی که از مرزهای آنها عبور می‌کند استفاده کرده‌اند (بوئر، ۲۰۱۵: ٤٠٤٠). امروزه از فناوری بیومتریک در تلفن‌های همراه نیز استفاده می‌شود و پیش‌بینی می‌شود که برنامه‌های کاربردی بیومتریک قابل حمل در دستگاه‌های تلفن همراه تا سال ۲۰۳۰ به حدود ٦ میلیارد افزایش یابد (کوپر و پرکینز[2]، ۲۰۱٤: ١٤). یکی از اقدامات اینترپل در این راستا ایجاد «پروژه اول»[3] است که شامل چهره، تصویربرداری، تشخیص، جستجو و ردیابی می‌باشد و این امر کمک می‌کند تا اطلاعات مظنونان تروریستی را به اشتراک بگذارند. داده‌های بیومتریک مانند تصاویر چهره و اثر انگشت می‌تواند منجر به شناسایی دقیق افرادی شود که از هویت جعلی استفاده می‌کنند و درنتیجه تلاش‌ها برای شناسایی تروریست‌ها و انجام تحقیقات و پیگردهای موفق را بهبود می‌بخشد.[4] برای این منظور ضرورت دارد تا افسران پلیس برای ثبت داده‌های مجرمان تروریستی آموزش ببینند تا این اطلاعات در پایگاه داده‌های اینترپل ذخیره شود. این اطلاعات در پایگاه‌های سیستم تشخیص چهره و پایگاه داده اثر انگشت نیز ذخیره می‌گردد تا شناسایی به‌طور دقیق صورت پذیرد.

در این راستا اینترپل مدلی را توسعه و اجرا نمود تحت عنوان «مدل تبادل اطلاعات نظامی به پلیس[5]» که این اطلاعات از مناطق درگیری را در اختیار افسران مجری قانون قرار می‌دهد تا از تحقیقات پلیس و روند پیگرد قانونی حمایت کند. اولین واکنش‌دهنده‌های نظامی می‌توانند اطلاعات طبقه‌بندی‌شده جمع‌آوری‌شده از میدان جنگ را با دفاتر مرکزی ملی اینترپل مربوطه به اشتراک بگذارند که اطلاعات را طبق قوانین اینترپل پردازش می‌کنند و آن را در پایگاه‌های اطلاعاتی و فایل‌های تحلیلی وارد می‌کنند. کاربران مجاز خط مقدم در کشورهای عضو می‌توانند از طریق شبکه آی- ٧/٢٤[6] به اطلاعات دسترسی داشته باشند.[7]

1. Caldwell
2. Cooper & Perkins
3. Project First
4. https://www.interpol.int/en/Crimes/Terrorism/Identifying-terrorist-suspects
5. Military-to-police information exchange model (Mi-Lex)
6. I-۷/۲۴ Network
7. https://www.interpol.int/en/Crimes/Terrorism/Identifying-terrorist-suspects

۲-۲. جلوگیری از مسافرت تروریست‌ها

یکی از شیوه‌های مقابله با تروریسم ممانعت از مسافرت تروریست‌ها می‌باشد و هدف آن کاهش آسیب‌پذیری مردم در سرتاسر جهان در برابر تروریسم با بسیج تخصص و منابع برای پیشگیری، مبارزه و تعقیب اقدامات تروریستی و مقابله با تحریک و استخدام برای گروه‌های تروریستی است. همچنین تلاش تروریست‌ها برای استفاده از اسناد جعلی موضوع مهم دیگری است که برای جلوگیری از سفر آنها باید مد نظر قرار گیرد.

پایگاه داده اس-ال-تی-دی[1] اینترپل حاوی اطلاعاتی درباره اسناد مسافرتی و هویتی است که به‌عنوان دزدیده شده، گم شده، باطل، نامعتبر یا بدون متن (سفید) به سرقت رفته، گزارش شده باشند. این پایگاه داده به پلیس کمک می‌کند تا تروریست‌ها و جنایتکارانی را که اغلب از اسناد مسافرتی جعلی برای عبور از مرزها استفاده می‌کنند، دستگیر کند.[2]

پایگاه‌های اطلاعاتی اینترپل حاوی جزئیات حدود ۱۳۵۰۰۰ جنگجوی تروریست خارجی است. این امر اینترپل را به بزرگ‌ترین مخزن چنین اطلاعاتی در جهان تبدیل می‌کند که می‌تواند در شناسایی تروریست‌ها حیاتی باشد. داده‌ها از تعدادی از نقاط حساس از جمله مرزها، میدان‌های جنگ و زندان‌ها جمع‌آوری‌شده است. برای تحقق اهداف مذکور این امر برای مقامات مرزی ضروری است که اطلاعات هویتی و گذرنامه مسافران را با پایگاه داده اسناد مسافرتی دزدیده و مفقود اینترپل بررسی کنند.[3] سیستم اسناد کتابخانه الکترونیکی فرانتکس اینترپل[4] کنترل موثر اسناد مسافرتی و هویتی سنگ بنای امنیت مرزها و مدیریت موفق مهاجرت است. دسترسی بی‌درنگ به فایلدز[5] و کیو- سی -سی‌های[6] موجود در آن - در طول بررسی‌های مرزی، احراز صحت اسناد مسافرتی و هویتی را سریع‌تر و آسان‌تر می‌کند و نتایج دقیق‌تری دارد. با پوشش دادن جعل و تزویر، سیستم فایلدز پایگاه داده اس- ال- تی- دی موجود اینترپل را تکمیل می‌کند که حاوی سوابق مربوط به اسناد خالی دزدیده شده، گم شده، باطل، نامعتبر و مسروقه است. این سیستم همچنین از طریق یک پلتفرم وب در دسترس است که در آن افسران خط دوم و پزشکی قانونی می‌توانند زمان بیشتری را برای بررسی کامل کیو- سی- سی‌ها و هشدارهایی که فایلدز در اختیار دارد صرف کنند. هشدارها حاوی عکس‌ها

1. SLTD database
۲. این پایگاه داده ۳.٦ میلیارد بار در سال ۲۰۲۳ توسط مقامات در سراسر جهان جستجو شد که منجر به ۲۳۲٤۲۳ تطابق مثبت شد.
3. https://www.interpol.int/en/Crimes/Terrorism/Preventing-terrorist-travel
4. Frontex
5. Fields
6. QCC

و سایر اطلاعات مهم درباره اشکال تازه کشف شده اسناد جعلی هستند و برای اطلاع سایر کشورها از روند تقلب استفاده می‌شوند.

۳-۲. پیشگیری از طریق ردیابی منابع مالی تروریست‌ها

از آنجاکه هر اقدام تروریستی مستلزم صرف هزینه است، درنتیجه پول را باید به‌مثابه خونی دانست که در رگ‌های سازمان‌های تروریستی جریان دارد، به‌گونه‌ای که بدون آن، این سازمان‌ها قادر به ادامه حیات یا انجام فعالیت‌های خود نخواهند بود (کارگری، ۱۳۹۱: ۱۱۶- ۱۱۵)؛ لذا جامعه بین‌المللی، دریافت تا زمانی که منابع مالی تروریسم خشکانده نشود، تروریسم سرکوب نخواهد شد (الهویی نظری، ۱۳۹۶: ۷۲۶). این ضرورت هم در بعد ملی و هم بعد بین‌المللی مورد توجه دولت‌ها بوده و البته این ضرورت منجر به ایجاد استانداردهایی در این زمینه گردیده است. این استانداردها می‌تواند موجب شکل‌گیری یک اقدام متحدالشکل در زمینه مقابله با گروه‌های تروریستی گردد. لذا امروزه موضوع مقابله و پیشگیری از تأمین مالی تروریسم به یک بحث جدی تبدیل شده است.

مبارزه با تأمین مالی تروریسم ازآن جهت به بحثی ویژه تبدیل گردیده که در آن موضوعات اقتصادی، حقوقی، دیپلماتیک و پلیسی آمیخته است (امیسل[1]، ۲۰۰۸: ۱۶۹). واقعیت آن است که تروریست‌ها برای جذب و حمایت از اعضا، حفظ مراکز لجستیکی و انجام عملیات خود خصوصاً در خارج از مرزهایی که حضور دارند، به بودجه نیاز دارند؛ بنابراین، جلوگیری از دسترسی تروریست‌ها به منابع مالی برای مقابله با موفقیت تروریسم بسیار مهم است.

در واقع تروریست‌ها برای رسیدن به اهداف تروریستی خود نیازمند تأمین مالی هستند و برای تأمین این نیاز حیاتی خود به راه‌های گوناگون متوسل می‌شوند. لذا به‌منظور مبارزه با تروریسم یکی از مهم‌ترین و ضروری‌ترین راه‌ها مبارزه با تأمین مالی آن است (نورمحمدی و خالقی، ۱۳۹۸: ۲). در اینجا لازم است تا میان دو مفهوم تأمین مالی تروریسم و حمایت مالی تروریسم قائل به تفکیک شد. تأمین مالی تروریسم از طرق مختلفی ممکن است انجام گیرد که یکی از آنها کمک ثروتمندان و دولت‌هاست و حمایت مالی از تروریسم اغلب متوجه این شیوه است. از این‌رو اشخاصی که بدون اغراض حمایتی و صرفاً با انگیزه‌های سودجویانه با گروه‌های تروریستی یا اشخاصی که با گروه‌های تروریستی در ارتباط هستند، دادوستد و تعامل مالی دارند، بهتر است مشارکت‌کنندگان در تأمین مالی تروریسم بدانیم نه حامیان مالی تروریسم (شمس ناتری و اسلامی، ۱۳۹٤: ۲٦۱). لذا ایجاد اختلال در جریان کمک‌های مالی تروریست‌ها برای محدود کردن فعالیت‌های آنها ضروری است. هر جنایتی که منجر به سود و

1. Amicelle

منافع شود می‌تواند برای تأمین مالی تروریسم استفاده شود. این بدان معناست که یک کشور ممکن است با خطرات مالی تروریسم مواجه شود، حتی اگر خطر یک حمله تروریستی کم باشد. در این راستا اینترپل روابط خود را با تعدادی از نهادها حفظ می‌کند تا به اجرای سیاست‌های سطح بالا و همکاری برای مقابله با تأمین مالی تروریسم کمک نماید. از جمله گروه ویژه اقدام مالی[1] که یک نهاد بین‌دولتی که استانداردهای بین‌المللی را برای مبارزه با پول‌شویی و تأمین مالی تروریسم تدوین می‌کند. همچنین گروه اگمونت[2] که شبکه‌ای متشکل از ۱۵۹ واحد اطلاعات مالی از سراسر جهان است. به‌علاوه در سطح عملی، اینترپل به دنبال تشویق همکاری بهتر بین واحدهای اطلاعات مالی[3] و پلیس در کشورهای عضو هستند تا به اشتراک‌گذاری اطلاعات و تجزیه‌وتحلیل را تشویق نماید.[4]

٤-٢. پیشگیری از طریق تجزیه‌وتحلیل فضای مجازی

با توجه به ماهیت در حال تحول و تنوع گسترده پلتفرم‌های آنلاین و همچنین گستردگی تکنیک‌های مورد استفاده توسط گروه‌های تروریستی آنالیز این پلتفرم‌ها در شناسایی رویکرد و روش‌های گروه‌های تروریستی دارای اهمیت می‌باشد.

در سال‌های اخیر، رسانه‌های اجتماعی و اینترنت، پیچیدگی و کاهش هزینه اشتراک‌گذاری اطلاعات را افزایش داده‌اند. این به نوبه خود از روند بسیاری از سازمان‌های تروریستی برای سازمان‌دهی مجدد خود در ساختار شبکه‌ای حمایت کرده و ظرفیت هر فرد را برای فعالیت مستقل‌تر، به‌ویژه برای انتشار پیام‌های سازمان، افزایش داده است (ژو و همکارن[5]، ۲۰۰۹: ۱۱).

این سازمان‌دهی مجدد انعطاف‌پذیری و گسترش بیشتری را برای آنها فراهم کرده است. درنتیجه، شبکه‌های تروریستی می‌توانند گسترده‌تر باقی بمانند، حتی اگر یک یا چند هسته به‌شدت آسیب‌دیده یا از بین بروند. برای مثال، پس از ۱۱ سپتامبر، القاعده از افزایش فشارها رنج می‌برد، اردوگاه‌های آموزشی را در افغانستان از دست داد و بسیاری از رهبران ارشد قبل از ۱۱ سپتامبر کشته یا اسیر شده بودند؛ بنابراین، برای اینکه القاعده فعال باقی بماند، آنها باید رویکرد خود را به سمت الهام بخشیدن و هدایت سایر گروه‌ها تغییر می‌دادند، حتی اگر فقط از طریق ارتباطات فضای مجازی امکان‌پذیر بود.[6]

---

1. Financial Action Taskforce (FATF)
2. Egmont Group
3. Financial intelligence units (FIUs)
4. https://www.interpol.int/en/Crimes/Terrorism/Tracing-terrorist-finances
5. Xu et al

٦. ابو مصعب السوری یکی از محرکان اصلی این تغییر در ساختار و استراتژی بود و اینترنت به‌عنوان وسیله‌ای برای تسهیل این تغییر مورد بهره‌برداری قرار گرفت. این تغییر رویکرد منجر به تأثیرات جهانی قابل‌توجهی شد، به‌نحوی که با تشکیل گروه‌های وابسته محلی که حملات تروریستی را در بالی، لندن و مادرید انجام دادند.

در این راستا مهم‌ترین راهبرد برای جلوگیری از رادیکال‌سازی و فعالیت گروه‌های تروریستی در رسانه‌های اجتماعی و اینترنت شامل جلوگیری و ممنوعیت انتشار محتوا و تبلیغات تروریستی در فضای آنلاین با استفاده از مکانیزم‌ها و ابزارهای دیجیتال است.

لازم به ذکر است که جلوگیری از انتشار محتوای تروریستی آنلاین مستلزم استفاده از فناوری و پلتفرم‌هایی است که معمولاً متعلق به بخش خصوصی است، بنابراین مشارکت و همکاری عمومی و خصوصی در این استراتژی خاص بسیار مهم است. یکی از نمونه‌های این نوع مشارکت، فناوری در برابر تروریسم است، ابتکاری که در حمایت از قطعنامه شورای امنیت سازمان ملل متحد برای مقابله با روایت‌های تروریستی آنلاین توسعه یافته است.[1]

اینترپل استفاده گروه‌های تروریستی از پلتفرم‌های رسانه‌های اجتماعی را به‌منظور تقویت شناسایی و کشف در تحقیقات ملی ضد تروریسم تجزیه و تحلیل می‌نماید. به عنوان مثال، اینترپل پلتفرم‌های رسانه‌های اجتماعی را جستجو می‌کند تا شاهدان احتمالی را شناسایی نموده، همان‌طور که پس از حمله به پل لندن در بریتانیا در سال ۲۰۱۷ و حمله به مجموعه هتلی در نایروبی، کنیا، در ژانویه ۲۰۱۹ اتفاق افتاد. برای این منظور به عنوان بخشی از اولین پروژه مشترک، اینترپل با مرکز مبارزه با تروریسم سازمان ملل متحد، کارگاه‌هایی را برای بازرسان در چهار حوزه اصلی شامل الف) شناسایی فعالیت‌های مرتبط با تروریست‌ها به‌صورت آنلاین؛ ب) جمع‌آوری سوابق الکترونیکی؛ پ) درخواست مدارک الکترونیکی در سراسر مرزها از طریق همکاری پلیس با پلیس و ت) تعامل با بخش خصوصی برای پیشبرد تحقیقات توسط سازمان‌های مجری قانون [2] برگزار کرده است. این پروژه توسط دولت‌های ژاپن، عربستان سعودی و امارات متحده عربی تأمین مالی شده است.[3]

۳. تمهیدات پیشگیرانه اینترپل در مورد بیوتروریسم، تروریسم رادیولوژیکی و هسته‌ای

بیوتروریسم انتشار عمدی ویروس‌ها، باکتری‌ها، سموم یا سایر عوامل مضر برای ایجاد بیماری یا مرگ در افراد، حیوانات یا گیاهان است. تهدید بیوتروریسم واقعی است، با گزارش‌های فعلی که نشان می‌دهد افراد، گروه‌های تروریستی و جنایتکاران هم توانایی و هم قصد استفاده از عوامل بیولوژیکی را برای آسیب رساندن به جامعه دارند. دسترسی به دانش و داده‌ها نیز به‌طور

1. Security Council Resolution 2354 (2017)

۲. تکمیل‌کننده این کارگاه‌ها یک کتاب راهنما است که به‌طور مشترک توسط INTERPOL و UNCCT منتشر شده است، با عنوان «استفاده از اینترنت و رسانه‌های اجتماعی برای تحقیقات ضد تروریسم». این به بازرسان راهنمایی‌های عملی در مورد بهترین روش یافتن سرنخ‌های تحقیقاتی آنلاین و جمع‌آوری و حفظ سوابق الکترونیکی اغلب در سراسر مرزهای بین‌المللی برای کمک به تحقیقات و پیگردهای قانونی موفق ارائه می‌دهد.

3. https://www.interpol.int/en/Crimes/Terrorism/Analysing-social-media

فزاینده‌ای از طریق اینترنت در دسترس است و مجرمان از جریان‌های مخفی و ناشناس ارتباطی مانند Darknet برای خرید، فروش و به اشتراک‌گذاری داده‌ها و برقراری ارتباط با یکدیگر استفاده می‌کنند. خسارات ناشی از چنین رویدادی می‌تواند به حجم بی‌حد و حصری برسد و باعث بیماری و مرگ گسترده شود و ترس و وحشت را در مقیاس جهانی ایجاد کند.
بیوتروریسم به انتشار عمدی عوامل بیولوژیکی یا سموم به‌منظور آسیب رساندن یا کشتن انسان‌ها، حیوانات یا گیاهان به‌قصد ارعاب یا اجبار یک دولت یا جمعیت غیرنظامی برای پیشبرد اهداف سیاسی یا اجتماعی اشاره دارد. انتشار یک عامل بیولوژیکی عفونی یا سمی می‌تواند بدون هشدار اتفاق بیفتد، درحالی‌که واکنش به یک رویداد بیولوژیکی، خواه به‌طور طبیعی، تصادفی یا عمدی، متکی به هماهنگی در بخش‌های مختلف است. بدیهی است که نیاز به راهبردهای پیشگیری، آمادگی و واکنش ساختاریافته حیاتی است.

بیوتروریسم انواع مختلفی دارد و می‌تواند از طریق محیط زیست و امنیت جسمی افراد و امنیت زنجیر غذایی و کشاورزی و اقتصادی و دارویی و پزشکی به جامعه لطمه وارد کند. زمینه‌های پزشکی و کشاورزی امروزه از اهداف عمده بیوتروریسم محسوب می‌شوند (ضرابی، ۱۳۹۵: ۱). در حال حاضر انتشار یا تهدید به انتشار عمدی عوامل بیولوژیک (ویروس‌ها، باکتری‌ها، قارچ‌ها یا سموم آنها) به‌منظور ایجاد بیماری یا مرگ در میان جمعیت انسانی یا محصولات غذایی و دام برای ایجاد وحشت در جمعیت غیرنظامی یا دستکاری دولت در سناریوی کنونی افزایش فعالیت‌های تروریستی به یک احتمال واقعی تبدیل شده است.

۱-۳. پیشگیری از بیوتروریسم

پنج مرحله فعالیت در مقابله با حمله بیوتروریستی عبارتند از: مرحله آمادگی، مرحله هشدار اولیه، مرحله اطلاع‌رسانی، مرحله واکنش و مرحله بازیابی (داس و کاتاریا[1]، ۲۰۱۱: ۲۵۵). با آنکه تاکنون چند سند بین‌المللی در زمینهٔ تروریسم و بیوتروریسم به تصویب رسیده، اما این اسناد نتوانسته‌اند مانع از اقدامات بیوتروریستی این گروه‌ها شوند. همچنین بسیاری از دولت‌ها در نظام‌های حقوقی داخلی خود، سازوکارهای قانونی مناسبی برای مقابله با اقدامات بیوتروریستی گروه‌های غیردولتی نداشته یا آنکه به دلایل اقتصادی و سیاسی تمایل چندانی به مقابله با اقدامات بیوتروریستی این گروه‌ها ندارند (ابراهیمی و همکاران، ۱۴۰۳: ۱۸۰۴).

رویکرد و سیاست کلی اینترپل این است که مدیریت موفقیت‌آمیز یک حادثه شامل انتشار باکتری‌ها، ویروس‌ها یا سموم بیولوژیکی، خواه منشأ طبیعی، تصادفی یا عمدی باشد، متکی به

1. Das & Kataria

همکاری بین‌المللی است. این امر شامل همکاری ذی‌نفعان ملی درگیر در آماده‌سازی، پیشگیری و واکنش به حوادث بیولوژیکی در سطح عملیاتی، تاکتیکی و استراتژیک است.

هدف واحد پیشگیری از بیوتروریسم اینترپل این است که آژانس‌های مجری قانون را قادر سازد تا از استفاده عمدی از باکتری‌ها، ویروس‌ها یا سموم بیولوژیکی که انسان‌ها، حیوانات یا کشاورزی را تهدید می‌کنند یا به آنها آسیب می‌رسانند، پیشگیری کرده و به آن پاسخ مناسب دهند. سازمان علاوه بر همکاری در سطوح بین‌المللی و منطقه‌ای، همچنین با سازمان‌های مجری قانون، بهداشت، دانشگاه و صنعت ملی برای مقابله با این جنایت چالش‌برانگیز همکاری می‌کند و در تعدادی از پروژه‌ها و فعالیت‌های طراحی‌شده برای کاهش خطر بیوتروریسم مشغول هست.

واحد پیشگیری از بیوتروریسم اینترپل، اسناد بسیاری ازجمله دستورالعمل‌ها، فیلم‌های آموزشی و رویه‌های عملیاتی استاندارد را آماده می‌کند و در نوشتن آن مشارکت می‌کند.
به‌منظور کمک به افسران مجری قانون برای شناسایی محرک‌ها و شاخص‌های فعالیت مجرمانه بالقوه مرتبط با دسترسی و تجارت مواد بیولوژیکی و شیمیایی با استفاده از تاریک‌نت، «راهنمای عملیاتی اینترپل برای بررسی تروریسم بیولوژیکی و شیمیایی در شبکه تاریک» توسط تیمی از کارشناسان CBRNE و جوامع سایبری تهیه و تدوین شده است. افسرانی که در زمینه‌های اطلاعاتی، تحقیقات ضد تروریسم و جرایم سایبری کار می‌کنند، می‌توانند از این راهنما به‌عنوان یک سند مرجع استفاده کنند که مفاهیم اساسی، بهترین شیوه‌های بین‌المللی و همچنین تکنیک‌ها و روش‌های مفید برای مقامات تحقیق و تحلیلگران را هنگام انجام تحقیقات Darknet مرتبط با دستیابی به عوامل بیولوژیکی و شیمیایی بیان می‌کند.[1]

برنامه اختصاصی اینترپل از کشورهای عضو حمایت می‌کند تا توانایی‌های خود را برای پیشگیری از تهدیدات و حوادث بیولوژیکی افزایش دهند. اینترپل این پیشگیری را با افزایش آگاهی جهانی از چشم‌انداز تهدید بیولوژیکی، تقویت همکاری بین بازیگران مربوطه، افزایش اشتراک‌گذاری اطلاعات، ارائه طیف گسترده‌ای از آموزش و با ارائه پشتیبانی تحقیقاتی انجام می‌دهد.[2]

۲-۳. تروریسم رادیولوژیکی و هسته‌ای

مواد هسته‌ای و سایر مواد رادیولوژیکی در زمینه‌های پزشکی، کشاورزی، صنعت و تأمین انرژی برای جامعه مفید بوده است. با این حال، این خطر وجود دارد که مواد هسته‌ای یا سایر مواد رادیولوژیکی در تروریسم یا سایر اعمال جنایی مورد استفاده قرار گیرند.

1. https://www.interpol.int/Crimes/Terrorism/Bioterrorism
2. https://www.interpol.int/en/Crimes/Terrorism/Bioterrorism

اگر عمل تروریستی شامل یک وسیله انفجاری رادیولوژیکی یا هسته‌ای باشد، احتمالاً بزرگترین چالش‌ها برای جامعه ایجاد می‌شود. حملات شیمیایی و بیولوژیکی و هسته‌ای را می‌توان به طیف وسیعی از اهداف هدایت کرد. تروریست‌ها ممکن است بر مناطق وسیع جمعیت یا مناطق کشاورزی روستایی تمرکز کنند و عوامل شیمیایی و بیولوژیکی را می‌توان با استفاده از ابزارهای مختلف پخش کرد. همچنین هواپیماها و قایق‌ها روش‌های مرسوم برای رهاسازی عوامل بیولوژیکی و شیمیایی هستند، اگرچه روش‌های غیرمتعارف زیادی نیز وجود دارد (آرل ون[1]، ۲۰۰٤: ٥٤-٥٦). همچنین دستیابی یا تلاش در مسیر دستیابی به مواد و وسایل هسته‌ای جهت انجام اعمال تروریستی مهم‌ترین کابوس جامعه جهانی را در سده جاری تشکیل می‌دهد. در این زمینه، کنشگران نظام حقوق بین‌الملل درجهت مقابله با تروریسم هسته‌ای طی انشای کنوانسیون سرکوب اعمال تروریسم هسته‌ای در سال ۲۰۰۵، جرم‌انگاری اعمال تروریستی یادشده را در دستور کار قرار دادند؛ اعمال تروریسم هسته‌ای از تهدید تا استفاده از مواد و وسایل انفجاری هسته‌ای را در ذیل قلمروی خود قرار می‌دهد (مشکات، ۱٤۰۰: ۱۲۷)، لذا ضرورت دارد تا مجریان قانون به حملات به تأسیسات رادیولوژیکی و هسته‌ای، جستجو برای یافتن منابع رادیواکتیو، یا هدایت عملیات پیچیده برای متوقف کردن تلاش‌ها برای خرید مواد رادیواکتیو از طریق بازارهای سیاه، پاسخ دهند. بنابراین، مقامات مجری قانون باید از تهدیدی که می‌تواند برای امنیت عمومی ایجاد شود آگاه باشند و توانایی پاسخگویی موثر به جرایم مربوط به مواد رادیواکتیو را داشته باشند.

در این خصوص کار اینترپل به منظور پیشگیری از تروریسم رادیولوژیکی و هسته‌ای مبتنی بر تهدید است و توسط اطلاعات جنایی هدایت می‌شود. بدین نحو که اینترپل از طریق برنامه حمایت از اجرای قانون، اطمینان حاصل می‌کند که کار این سازمان با کشورهای عضو قابل اندازه‌گیری، پایدار و بر اساس نیازهای شناسایی شده از طریق همکاری با کشورهای ذی‌نفع است. بر این اساس برنامه اینترپل بر حوزه‌های زیر تمرکز دارد: الف) تجزیه و تحلیل تخصص؛ ب) مشارکت‌های جهانی و پ) فراگیری جنسیتی. همچنین پروژه‌هایی[2] را در دستور کار خود قرار داده است تا از این طریق با تروریسم رادیولوژیکی و هسته ای مقابله و ارتکاب آنها پیشگیری نماید.[3]

1. Arl Van
2. INTERPOL and UN launch initiative on CBRNE terror threats (2020) & Chemical terrorism: developing a global security network (2018)
3. https://www.interpol.int/en/Crimes/Terrorism/Radiological-and-Nuclear-terrorism

بحث و نتیجه‌گیری

همگام با رشد فناوری، ساختار، ابزار و شیوه اقدامات تروریستی هرروز در حال تحول و روزآمد شدن است. این امر نه‌تنها بزه‌دیدگان مستقیم اعم از اشخاص حقیقی و کشورهای قربانی تروریسم، بلکه صلح و امنیت بین‌المللی را در خطر قرار داده است. در حقیقت نه‌تنها شیوه ارتکاب جرائم آنها خلاقانه‌تر و مبتنی بر تکنولوژی نوین است، بلکه از ابزار رسانه نیز در ایجاد رعب و وحشت استفاده می‌کنند. موضوع دیگری که در خصوص اقدامات تروریستی اهمیت دارد استفاده از فضای سایبر و فراملی بودن جنایات تروریستی است. در حقیقت توانایی و حمایت یک گروه جنایت‌کار سازمان‌یافته فراملی برای کنترل یک مرکز در یک دوره طولانی قدرت خاص جهت فعالیت و حتی جذب و تربیت نیرو به گروه‌های تروریستی می‌دهد. پیرامون اقدامات پیشگیرانه، شناسایی گروه‌های تروریستی، شناسایی هویت متهمین یا محکومین به اقدامات تروریستی، اطلاع یافتن از نحوه عملکرد تروریست‌ها و شگردهای مجرمانه آنان می‌تواند کشورهای دیگر را که مقصد بالقوه تروریست‌ها هستند؛ در پیشگیری از ارتکاب جرم کمک کند. اینترپل در بانک‌های اطلاعاتی خود و تمهیدات مفصل خویش تلاش کرده است به تسهیل شناسایی متهمان و مجرمان از طریق داده‌های بیومتریک، پیشگیری از مسافرت تروریست‌ها، پیشگیری از طریق ردیابی منابع مالی تروریست‌ها، پیشگیری از بیوتروریسم، تروریسم رادیولوژیکی و هسته‌ای به پیشگیری از تروریسم بپردازد. در کنار این موارد اقدامات و پروژه‌های دیگری نیز در دستور کار اینترپل می‌باشد که با همکاری اعضاء در حال انجام است. با توجه به اینکه تروریسم امری است که در حال تحول می‌باشد و تأثیر فناوری بر آن تأثیر بسیار دارد، لذا ضرورت دارد تا ماهیت اقدامات پیشگیرانه و مقابله‌ای اینترپل نیز با توجه به این تحولات به‌روز شود.

منابع

- سلیمی، صادق. (۱۳۹۱). *جنایات سازمان‌یافته فراملی*. چاپ دوم. جنگل جاودانه.
- سلیمی، صادق. (۱٤۰۲). *اینترپل؛ از تعقیب تا تضمین حقوق منهمین و مجرمین*. چاپ اول. انتشارات شهر دانش.
- میربد، لیلا. (۱٤۰۳). عملکرد بین‌المللی تابعان حقوق بین‌الملل در مبارزه با تروریسم سایبری. [رساله دکتری حقوق بین‌الملل دانشگاه آزاد اسلامی واحد علوم و تحقیقات].
- ضرابی، مینا. (۱۳۹۵). خطر تولارمی در بیوتروریسم، همایش ملی بیماریهای مشترک بین انسان و دام.
- ابراهیمی، محمود؛ چهکندی نژاد، علی و طاهری بجد، محمدعلی. (۱٤۰۳). ابعاد حقوقی استفادهٔ گروه‌های غیردولتی از سلاح زیستی. *مطالعات حقوق عمومی*، ٥٤ (۳)، ۱۸۲۳-۱۸۰۳.
https://jplsq.ut.ac.ir/article_96514.html
- مشکات، مصطفی. (۱٤۰۰). جستاری بر هم‌پوشانی محاربه و افساد فی‌الارض در مواجهه با اعمال تروریسم هسته‌ای. *پژوهش‌های حقوقی*، ۲۰(٤٥)، ۱٤۷-۱۲٥.
https://jlr.sdil.ac.ir/article_129109.html
- ابراهیمی، شهرام. (۱۳۹۰). *جرم‌شناسی پیشگیری*. جلد اول. تهران: انتشارات میزان.
- الهویی نظری، حمید و فامیل زوار جلالی، امیر. (۱۳۹٦). مسئولیت بین‌المللی دولت‌های تأمین‌کننده‌ی مالی تروریسم. *مطالعات حقوق عمومی*، ٤۷(۳)، ۷٤٦-۷۲٥.
https://jplsq.ut.ac.ir/article_63757.html
- شمس ناتری، محمد ابراهیم؛ اسلامی، داوود. (۱۳۹٤). ماهیت کیفری تأمین مالی تروریسم. *مطالعات حقوق کیفری و جرم‌شناسی*، ۲(٥ و ٤)، ۲٥۷-۲۸٦.
https://jplsq.ut.ac.ir/article_63757.html
- کارگری، نوروز. (۱۳۹۱). *درونمایه‌های تروریسم*. تهران: نشر میزان.
- کاسسه، آنتونیو. (۱۳۸۰). حمله تروریستی به مرکز تجارت جهانی و بر هم خوردن برخی مقوله‌های تعیین‌کننده حقوق بین‌الملل. ترجمه زهرا کسمتی. *اطلاعات سیاسی – اقتصادی*، ۱۷۳ و ۱۷٤.
- نورمحمدی، فوزیه و خالقی، ابوالفتح. (۱۳۹۸). *سیاست کیفری ایران در قبال تامین مالی تروریسم*، پنجمین همایش بین‌المللی مدیریت، روانشناسی و علوم انسانی با رویکرد توسعه پایدار، تهران، مرکز راهکارهای دستیابی به توسعه پایدار.

- Rossmo, D. K., & Harries, K. (2011). The geospatial structure of terrorist cells. *Justice Quarterly*, 28 (2).
- Savitch, H. V. (2005). An anatomy of urban terror: Lessons from Jerusalem and elsewhere. *Urban Studies*, 42(3), 361-395.
https://ideas.repec.org/a/sae/urbstu/v42y2005i3p361-395.html
- Nemeth, S. C., Mauslein, J. A., & Stapley, C. (2014). The primacy of the local: Identifying terrorist hot spots using geographic information systems. *The Journal of Politics*, 76(2).
https://www.journals.uchicago.edu/doi/abs/10.1017/S0022381613001333?journalCode=jop

- Braithwaite, A., & Li, Q. (2007). Transnational terrorism hot spots: Identification and impact evaluation. *Conflict Management and Peace Science*, 24 (4), 281-296.
https://www.jstor.org/stable/26275247
- Ganor, Boaz. (2003). *Strategy of Modern Terrorism, Innovation Exchange*, 10.
- Sen, S. (1993). Features of Modern Terrorism, *Police Journal*, 66(1), 37-42.
https://www.ojp.gov/ncjrs/virtual-library/abstracts/features-modern-terrorism
- Caldwell, T. (2015). Market report: border biometrics. *Biometric Technology Today,* 2015(5).
- Arshad, I., Hayat, H., & Khan, A. A. (2015). *Biometric Security through Multimodal Systems.*
- Gupta, M. (2015). Biometric Another Way of User Authentication. *International Journal of Emerging Trends in Science and Technology*, 2(3), 2130-2133.
https://journals.indexcopernicus.com/api/file/viewByFileId/151075
- Boer, M. D. (2015). Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis. *Intelligence and National Security*, 30(2-3).
https://www.taylorfrancis.com/chapters/edit/10.4324/9781315674360-16/counter-terrorism-security-intelligence-eu-governance-challenges-collection-exchange-analysis-monica-den-boer
- Cooper, A., & Perkins, C. (2014). 2 Mobile borders/bordering mobilities. In *Governing Borders and Security: The Politics of Connectivity and Dispersal*.
- Hoffmann, B. (2006). *Inside Terrorism: Revised and Expanded Edition*, Columbia University Press.
- Greene, A. (2017). Defining Terrorism: one size fits all*? International & Comparative Law Quarterly*, 66(2), 411-440.
https://primoa.library.unsw.edu.au/discovery/fulldisplay/cdi_cambridge_journals_10_1017_S0020589317000070/61UNSW_INST:UNSWS
- Carr, C. (2007). "Terrorism": Why the Definition Must be Broad, *World Policy Journal*, 24 (1), 47-50.
https://www.jstor.org/stable/40210071
- Koch, Ariel. (2018). Jihadi Beheading Videos and their Non-Jihadi Echoes, *Perspectives on Terrorism*, 12(3), 24-34.
https://www.jstor.org/stable/26453133
- Xu, Jie, Daning, Hu, & Hsinchun, Chen. (2009).'The Dynamics of Terrorist Networks: Understanding the Survival Mechanisms of Global Salafi Jihad,' *Journal of Homeland Security and Emergency Management*, 6(1).
- Das, S, Kataria, VK. (2011). Bioterrorism: A Public Health Perspective, *Med J Armed Forces Indi*a, 66(3), 255-260.
https://pmc.ncbi.nlm.nih.gov/articles/PMC4921253/
- Arl Van, Moore Jr .(2004). Radiological and nuclear terrorism: are you prepared? *J Am Coll Radiol*. 1(1).
- Tereshchenko, N. (2013). US foreign policy challenges: cyber terrorism and critical infrastructure, e. *International Relations*, 12.