

The role of Interpol surveillance networks in curbing transnational terrorism

Azar Alinezhad¹

Abstract

Field and Aims: The spread of terrorism outside the borders of countries led to the formation of a type of terrorism, known as transnational terrorism. Today, the development and advancement of communication and information technologies and the use of them by terrorist organizations and individuals has created a situation where dealing with this form of terrorism has become a new challenge at the international level, and numerous international organizations and institutions have also involved the international community in this confrontation and providing effective solutions. Interpol is one of the organizations that, by having supervisory institutions at the international level, can take effective measures in the field of curbing this form of terrorism, and the purpose of this article is to examine the role of Interpol's supervisory networks in this regard.

Method: This article is written in a descriptive-analytical way.

Finding and Conclusion: The findings indicate that terrorist groups with goals, activities and organizational forms that are beyond their origin can be called "transnational". Therefore, terrorists can be transnational in three ways: goals, actions and organizational form. In dealing with the transnational terrorism network, Interpol has adopted methods that include: a- Identifying suspected terrorists; b- Preventing the travel of people suspected of terrorist activities; C- tracing the financial resources of terrorists; T- The use of two monitoring networks including the mobile network database and the fixed network database. Interpol member states that have adopted the connection to mobile and fixed networks and have also used it to screen people and documents at border crossings and other key points, compared to member states that have not joined or installed this connection. But they have not activated, they have suffered less transnational terrorist incidents. Of course, it is clear that the aforementioned networks cannot identify the traffic of potential terrorists whose information is not in Interpol or national data banks as suspected terrorists.

Keywords: Interpol, terrorism, transnational terrorism, counter terrorism, international organizations, surveillance networks.

*Citation (APA): Alinezhad, A. (2023). The role of Interpol surveillance networks in curbing transnational terrorism. *International Legal Research*, 16(62), 69-94.

1. Assistant Professor, Department of Islamic Studies and Law, Faculty of Literature and Humanities, Vali Asr University (AJ) Rafsanjan, Kerman, Iran. Email: a.alinezhad@vru.ac.ir



Introduction

The scenario of strengthening the solidarity and cohesion of the international community in dealing with terrorism, with features such as a more serious leadership of the United Nations, a commitment to respect human rights in the fight against terrorism, the formation of a coherent operational strategy, accepting the jurisdiction of the International Criminal Court to punish the perpetrators of terrorist acts and strengthening equality and Economic justice is one of the most likely and most desirable prospects for countering terrorism in the international arena. This can be seen from the historical campaign of countering terrorism in the international arena, when efforts to curb terrorist acts were put on the agenda of the United Nations.

Two important factors have led to the fact that terrorism is important from an international point of view, firstly, the main goal of terrorists is to force governments to accept their demands, and secondly, the level of terrorist acts is reflected in international dimensions. Accordingly, in 1972, the United Nations General Assembly established a special committee with the agenda of defining terrorism, which, after seven years of efforts, submitted its report to the General Assembly in 1979 without providing a definition of terrorism, in which it explained the reason for not defining terrorism. He had declared the existence of differences of opinion between the developing and developed countries regarding the nature of the activities of the liberation movements. However, the actions at the level of international organizations did not stop and international organizations, considering the importance of the issue of transnational terrorism, especially after the September 11 incident, tried to use the maximum power of the governments and international players in dealing with it. They did it with me. The use of the capacities of the International Criminal Police Organization (Interpol) and the cooperation of the governments as much as possible with this organization took place in this direction.

Thus, Interpol's surveillance methods, which cost millions of euros per year, are valuable given their effectiveness in curbing transnational terrorism, as our analysis will show. In principle, Interpol helps member countries to deal with terrorist organizations by coordinating police activities. Besides that, it offers many services including police training, communication links, coordinating the pursuit of fugitives, etc. to the member countries. This article focuses on one of these services, which is the control of transnational terrorism through Interpol surveillance networks.

Conclusion

The historical campaign of countering terrorism in the international arena shows that countering terrorism is an international challenge. Terrorism is the premeditated use or threat of violence by individuals or groups to achieve a political or social goal by intimidating a large audience beyond the immediate victims. In the description of transnational terrorism, it should be said that just as transnational companies originate from one place and develop operations that expand locally and internationally, terrorist groups with goals, activities and organizational forms that go beyond their origin can also be "transnational". called Two important factors are involved in the recognition of transnational terrorism, which include the different nationality of terrorist perpetrators and the spread of terrorist actions and operations outside the borders of the country where the terrorists are present. Also, distinguishing the nationality of the victims is another criterion for identifying transnational terrorism. In distinguishing transnational



terrorism from civil war, it should be said that civil wars are considered as intra-state violent conflicts that pit a state against non-state rivals, whether these rivals are separatists motivated by ethnic nationalist grievances or minorities or revolutionaries whose goal is to displace the ruling elite. to be Civil wars often take the form of insurgencies aimed at mobilizing the population against the government rather than conventional wars in which armies engage each other. One of the institutions that plays an important role in dealing with transnational terrorism is the Interpol organization, which performs this role in different ways. INTERPOL links law enforcement agencies, national headquarters and the General Secretariat of INTERPOL in the fight against transnational crime and terrorism. Specifically, INTERPOL addresses six major criminal concerns: first - corruption, second - drugs and organized crime, third - financial and high-tech crimes, fourth - fugitives, fifth - human trafficking, and sixth - transnational terrorism.

In order to deal with the transnational terrorism network, Interpol uses methods that include the use of tools to identify suspected terrorists. This method is to use the biometric system and enter information in the network 24/7. Another method is to prevent suspected people from traveling. Another way is to trace the financial resources of terrorists, which is done by limiting these resources by the member states. What we specifically considered in this article was Interpol's surveillance networks and their effectiveness in dealing with transnational terrorism. In 2005, Interpol introduced two surveillance networks, a mobile network database and a fixed network database that facilitate the search of persons, motor vehicles and documents in international transit or elsewhere. The main difference between these networks is that in the fixed network it provides access to an online database that is constantly updated, while in the mobile network database it also provides access to an offline database. It is downloaded periodically and updated every 24 to 48 hours. The fact is that global security depends on the level of security in the least secure country. Therefore, the adoption of both networks created by Interpol by a country may divert some transnational terrorist incidents to countries that do not use this technology, thereby reducing transnational terrorism in the monitored and connected countries. Increases in non-connected countries. Analyzes show that INTERPOL member states that have adopted mobile and fixed network connectivity and used it to screen people and documents at border crossings and other key points than those that have not. They did not connect or installed it but did not activate it, they have less transnational terrorist incidents. Of course, these networks cannot identify the transit of potential terrorists whose information is not in Interpol or national data banks as suspected terrorists. What has been said leads us to the conclusion that dealing with transnational terrorism requires serious determination at the international level, and if the governments have serious determination in this regard, it will be very useful to use methods such as the Interpol surveillance network, but if this determination is not serious for various reasons, the international community will not be able to act effectively in dealing with transnational terrorism. It may be said that the non-joining or non-cooperation of some governments with this network is for the same reasons that the international community has not been able to reach a single definition of "terrorism", and this is something that we will always be involved with. However, it is necessary to note that some actions clearly have the characteristics of a terrorist act, and the identification of groups that engage in this type of actions, and the commitment of governments to cooperate with organizations such as Interpol, as well as a serious determination in using the method new methods in dealing with



this type of measures, in addition to reducing many internal costs, will help to realize global security as much as possible.

نقش شبکه‌های نظارتی اینترنتی در مهار تروریسم فراملی

آذر علی‌نژاد^۱

چکیده

زمینه و هدف: گسترش تروریسم به خارج از مرزهای کشورها منجر به شکل‌گیری نوعی از تروریسم، موسوم به تروریسم فراملی گردید. امروزه گسترش و پیشرفت فناوری‌های ارتباطاتی و اطلاعاتی و استفاده افراد و سازمان‌های تروریستی از آن، وضعیتی را ایجاد کرده است که مقابله با این شکل از تروریسم با چالش‌های جدید در سطح بین‌المللی بدل شده و سازمان‌ها و نهادهای متعدد بین‌المللی را نیز درگیر این مقابله و ارائه راهکارهای کارآمد نموده است. اینترنتی از جمله سازمان‌هایی است که با داشتن نهادهای نظارتی در سطح بین‌المللی می‌تواند در زمینه مهار این شکل از تروریسم اقدامات مؤثری داشته باشد و هدف از این مقاله بررسی نقش شبکه‌های نظارتی اینترنتی در این خصوص است.

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

یافته‌ها و نتایج: یافته‌ها بیانگر آن است که گروه‌های تروریستی با اهداف، فعالیت‌ها و اشکال سازمانی که فراتر از مبدأ خود هستند را می‌توان «فراملی» نامید؛ بنابراین تروریست‌ها از سه طریق اهداف، اقدامات و شکل سازمانی می‌توانند فراملیتی باشند. اینترنتی در مقابله با شبکه تروریسم فراملی شیوه‌هایی اتخاذ نموده است که عبارت‌اند از: الف) شناسایی تروریست‌های مظنون؛ ب) جلوگیری از سفر افراد مظنون به فعالیت‌های تروریستی؛ پ) ردیابی منابع مالی تروریست‌ها؛ ت) استفاده از دو شبکه نظارتی شامل پایگاه داده شبکه سیار و پایگاه داده شبکه ثابت. کشورهای عضو اینترنتی که اتصال به شبکه‌های موبایل و ثابت را پذیرفته‌اند و همچنین از آن برای غربال افراد و اسناد در گذرگاه‌های مرزی و سایر نقاط کلیدی استفاده کرده‌اند، نسبت به کشورهای عضو که به این اتصال نپیوستند و یا آن را نصب کرده، اما فعال نکرده‌اند، کمتر دچار حوادث تروریستی فراملی شده‌اند. البته واضح است که شبکه‌های مذکور نمی‌توانند عبور و مرور تروریست‌های بالقوه را که اطلاعات آنها در اینترنتی یا بانک‌های داده ملی به عنوان تروریست‌های مظنون نیست، شناسایی کنند.

کلیدواژه‌ها: اینترنتی، تروریسم، تروریسم فراملی، مقابله با تروریسم، سازمان‌های بین‌المللی، شبکه‌های نظارتی.

* استناددهی (APA): علی‌نژاد، آذر. (۱۴۰۲). نقش شبکه‌های نظارتی اینترنتی در مهار تروریسم فراملی. *تحقیقات حقوقی بین‌المللی*، ۱۶(۶۲)، ۶۹-۹۴.

۱. استادیار، گروه معارف اسلامی و حقوق، دانشکده ادبیات و علوم انسانی، دانشگاه ولی عصر (عج) رفسنجان، کرمان، ایران.

ایمیل: a.alinezhad@vru.ac.ir

مقدمه

سناریوی تقویت همبستگی و انسجام جامعه بین‌المللی در مقابله با تروریسم، با ویژگی‌هایی چون رهبری جدی تر سازمان ملل متحد، تعهد به رعایت حقوق بشر در مبارزه با تروریسم، شکل‌گیری راهبرد عملیاتی منسجم، پذیرش صلاحیت دیوان کیفری بین‌المللی برای مجازات عاملان اقدامات تروریستی و تقویت برابری و عدالت اقتصادی، از محتمل‌ترین و مطلوب‌ترین چشم‌اندازهای روندهای مقابله با تروریسم در عرصه بین‌المللی است. این امر را می‌توان از پویای تاریخی مقابله با تروریسم در عرصه بین‌المللی ملاحظه نمود که تلاش برای مهار اقدامات تروریستی در دستور کار سازمان ملل متحد قرار گرفت.

دو عامل مهم منجر به آن گردیده است که تروریسم از منظر بین‌المللی حائز اهمیت باشد، نخست اینکه هدف اصلی تروریست‌ها و ادار کردن دولت‌ها به پذیرش خواسته‌های آنان است و دوم اینکه سطح اقدامات تروریستی در ابعاد بین‌المللی نمود پیدا کرد. بر این اساس در سال ۱۹۷۲ مجمع عمومی سازمان ملل متحد کمیته‌ای ویژه را با دستور کار تعریف تروریسم تأسیس نمود که پس از هفت سال تلاش گزارش خود را در سال ۱۹۷۹ بدون ارائه تعریفی از تروریسم تقدیم مجمع عمومی کرد که در آن علت عدم تعریف تروریسم را وجود اختلاف نظر میان کشورهای در حال توسعه و توسعه یافته در خصوص چیستی فعالیت نهضت‌های رهایی‌بخش اعلام نموده بود. با این حال اقدامات در سطح نهادهای بین‌المللی متوقف نگردید و سازمان‌های بین‌المللی با توجه به اهمیت یافتن موضوع تروریسم فراملی خصوصاً بعد از حادثه یازده سپتامبر سعی در به کار گرفتن حداکثر توان دولت‌ها و بازیگران عرصه‌های بین‌المللی در مقابله با تروریسم نمودند. استفاده از ظرفیت‌های سازمان پلیس جنایی بین‌المللی (اینترپل) و همکاری هر چه بیشتر دولت‌ها با این سازمان در همین راستا صورت گرفت.

بنابراین، روش‌های نظارتی اینترپل که میلیون‌ها یورو در سال هزینه می‌کنند، با توجه به اثربخشی آنها در مهار تروریسم فراملی، همان‌طور که تحلیل ما نشان خواهد داد، دارای ارزش است. سازمان اینترپل در اصل با هماهنگی کردن فعالیت‌های پلیسی به کشورهای عضو در مقابله با سازمان‌های تروریستی یاری می‌رساند. در کنار آن خدمات متعددی شامل آموزش پلیس، پیوندهای ارتباطی، هماهنگی تعقیب فراریان و ... را به کشورهای عضو ارائه می‌دهد. این مقاله بر یکی از این خدمات یعنی کنترل تروریسم فراملی از طریق شبکه‌های نظارتی اینترپل تمرکز دارد.

۱. ماهیت تروریسم فراملی

تروریسم به هر شکلی ظهور یابد، هدف اصلی آن ایجاد رعب و وحشت جهت نیل به هدف است. این در حالی است که همه افراد بشر، از حق امنیت و حیات برخوردارند و همه دولت‌ها در احترام، تضمین و تحقق این حقوق مسئولیت دارند که این امر می‌طلبد جامعه بین‌المللی سیاست‌های

مؤثری را در جهت پیشگیری از بروز رفتارهای مجرمانه؛ به خصوص رفتارهای توأم با خشونت و سلب امنیت مردم؛ از جمله تروریسم و مجازات مرتکبان اقدامات تروریستی به کار بندد (لوتز^۱، ۲۰۱۳: ۱۰۳). قبلاً اشاره کردیم که کمیته ویژه سازمان ملل متحد بر اساس وجود برخی مشکلات که مهم‌ترین آن ناظر بر یک مسئله ایدئولوژیک است از ارائه تعریفی واحد از تروریسم خودداری نمود. به نظر می‌رسد همین مسئله ایدئولوژیک محور حقوقدانان و سیاست‌گذاران و سایر اندیشمندان حوزه علوم انسانی را نیز در ارائه تعریف واحد از تروریسم ناتوان ساخته است (رهامی، علی نژاد، ۱۳۹۰: ۱۳۳)، اما در بحث از تروریسم با توجه به نوع اقدامات و هدف غایی تروریست‌ها و با در نظر گرفتن نقطه اشتراک تمامی تعارف و خصوصیات ارائه شده در خصوص مفهوم تروریسم، می‌توان گفت که تروریسم استفاده از پیش برنامه‌ریزی شده یا تهدید به استفاده از خشونت توسط افراد یا گروه‌های محلی برای دستیابی به یک هدف سیاسی یا اجتماعی از طریق ارباب مخاطبان بزرگ فراتر از قربانیان فوری است.

ماهیت به هم پیوسته سیستم جهانی نه تنها فرصت‌ها و پیشرفت‌های بی‌سابقه‌ای را در توسعه انسانی به همراه داشته است، بلکه خطرات بیشتری را نیز به همراه داشته است. جنبه سایه جهانی شدن به گروه‌های جنایتکار و خشن این توانایی را می‌دهد که پیام خود را منتشر کنند و عملیات خود را گسترش دهند. تأثیر این امر نه تنها سازمان، منابع و روش‌های این گروه‌ها، بلکه استدلال و انگیزه‌های آنها را نیز تغییر می‌دهد. در این شرایط، ما شاهد تکثیر گروه‌های تروریستی با برنامه‌ها و عملیات‌هایی بوده‌ایم که فراتر از کشورهای است که این گروه‌ها در آنجا منشأ گرفته‌اند و اساساً در آن فعالیت می‌کنند. روابط بین‌الملل نگران تروریسم فراملی است؛ زیرا خطرات و سؤالاتی را به همراه دارد که به راحتی از طریق راه‌حل‌های نظم و قانون داخلی حل نمی‌شوند. در دهه‌های اخیر، تروریسم فراملی پس از یازده سپتامبر و متعاقب آن جنگ علیه تروریسم به رهبری ایالات متحده، بحث‌های داغی را هم در حوزه‌های علمی و هم در حوزه‌های عمومی و سیاسی ایجاد کرده است (آبراهامز^۲، ۲۰۰۶: ۴).

در یک جمع‌بندی در خصوص تروریسم فراملی می‌توان گفت که در صورت تحقق شرایط در سه جنبه می‌توان از تروریسم فراملی صحبت کرد. از نظر هدف، از منظر نوع اقدامات صورت گرفته و از نظر شکل سازمانی، یک گروه تروریستی و اقدامات صورت گرفته از سوی اعضا آن می‌تواند فراملی خوانده شود. این موضوع تمایز مهمی را از گروه‌های تروریستی غیرملیتی مانند بیره‌های تامیل^۳ در سریلانکا و یوسکادی تا آسکاتاسونا^۴ در اسپانیا ایجاد می‌کند که اهداف، عضویت و فعالیت‌های آنها بر سیاست دولتی متمرکز است، حتی اگر از حمایت بین‌المللی

1. Lutz
2. Abrahams
3. Tamil Tigers (LTTE)
4. Euskadi Ta Askatasuna (ETA)

برخوردار شوند. در حالی که تعریف تروریسم فراملی نسبتاً ساده است همان‌طور که نشان می‌دهد زمانی که موضوع مورد توجه روابط بین‌الملل است، تعریف تروریسم خود موضوع بحث‌های زیادی است (هورگان^۱، ۲۰۱۴: ۷).

۲. تمایز تروریسم داخلی، جنگ داخلی و تروریسم فراملی

شاید هیچ گروه تروریستی فراملی به اندازه دولت اسلامی شام و عراق (که به آنها داعش گفته می‌شود) توجه و بدنمایی برای فعالیت‌های خود جلب نکرده باشد. در حالی که این القاعده بود که پس از حملات ۱۱ سپتامبر، تروریسم فراملی را به مرکز روابط بین‌الملل رساند، اما دولت اسلامی به دلیل تمایل آنها برای ایجاد یک «خلافت» (امپراتوری اسلامی) در درازمدت مورد توجه قرار گرفت. دولت اسلامی با بهره‌گیری از هرج و مرج جنگ داخلی سوریه و بی‌ثباتی مداوم در عراق پس از سال ۲۰۱۱، کنترل مناطق وسیعی از قلمرو را به دست گرفت. زمانی تقریباً ۳۰ درصد سوریه و ۴۰ درصد عراق را در اختیار داشت. تا سال ۲۰۱۸، اقدامات هماهنگ بین‌المللی آنها را از بیشتر این قلمرو بیرون راند.

این امر مفهومی بنام تروریسم داخلی را بیشتر روشن کرد. تروریسم داخلی در داخل یک دولت ایجاد و رشد می‌کند و هیچ‌گونه تبعات خارجی بین‌المللی برای سایر دولت‌ها ندارد. در تروریسم داخلی، عاملان، قربانیان و اهداف همه از کشور محل وقوع حمله هستند. بمب‌گذاری اوکلاهاما سیتی توسط تیموتی مک وی در ۱۹ آوریل ۱۹۹۵ یک حادثه تروریستی داخلی منظور گردید؛ زیرا عامل و قربانیان آن آمریکایی‌هایی از کشور محل وقوع حمله بودند (دافی^۲، ۲۰۱۵: ۲).

در واقع عامل مهم در شناخت تروریسم داخلی شامل یکسان بودن تابعیت عاملان تروریستی و وقوع حمله تروریستی در کشوری که عاملان تابعیت آن را دارند، است. عدم تسری اقدامات و عملیات‌های تروریستی به خارج از مرزهای این کشور نیز معیار دیگری برای شناسایی و تمایز تروریسم داخلی از فراملی است.

در مقابل، تروریسم فراملی شامل عاملان، قربانیان یا اهدافی از دو یا چند کشور متفاوت است. اگر تروریست‌ها در کشور دیگری اقدام به حمله تروریستی نمایند، آن حادثه تروریسم فراملی است. هنگامی که یک حمله تروریستی در انگلستان، مثلاً یک آمریکایی را می‌کشد یا مجروح می‌کند، این حمله یک رویداد تروریستی فراملی است. بمب‌گذاری ماراتن بوستون توسط برادران تسارنایف در ۱۵ آوریل ۲۰۱۳ یک حادثه تروریستی فراملی تعریف شد؛ زیرا یکی از عاملان آن غیرآمریکایی بود، همچنین یکی از قربانیان نیز دانشجویی از چین بود (بریج^۳، ۲۰۰۹: ۵).

1. Horgan
2. Duffy
3. Bridge

در این خصوص نیز باید گفت دو عامل مهم در شناخت تروریسم فراملی دخالت دارد که شامل متفاوت بودن تابعیت عاملان تروریستی و تسری اقدامات و عملیات‌های تروریستی به خارج از مرزهای کشوری است که تروریست‌ها در آن حضور دارند. همچنین تمایز تابعیت قربانیان نیز معیار دیگری برای شناسایی تروریسم فراملی می‌باشد.

قبلاً بیان کردیم که تروریست‌ها از سه طریق می‌توانند فراملیتی باشند: از طریق اهداف، اقدامات و شکل سازمانی خود که هر کدام جنبه تاریک جهانی شدن را آشکار می‌کند. علاوه بر این، در حالی که نمونه‌هایی از تروریسم فراملی از سال ۲۰۰۱ ممکن است به نظر عمدتاً الهام گرفته از دین باشد، نمی‌توان نتیجه گرفت که چیزی اجتناب‌ناپذیر در این مورد وجود دارد، یا اینکه دین به‌طور خاص عامل مهمی است، اما افراط‌گرایی به عنوان یک عامل مورد توجه بوده است (اشمید^۱، ۲۰۰۴: ۳۷۵).

در اینجا ضرورت دارد تا بین تروریسم فراملی و جنگ داخلی نیز تمایز قائل شویم. جنگ‌های داخلی به‌عنوان درگیری‌های خشونت‌آمیز درون‌دولتی در نظر گرفته می‌شوند که یک دولت را در برابر رقبای غیردولتی قرار می‌دهند، خواه این رقبا جدایی‌طلبان با انگیزه نارضایتی‌های ملی‌گرایانه قومی یا اقلیت‌ها یا انقلابیونی که هدفشان جابه‌جایی نخبگان حاکم است، باشند. جنگ‌های داخلی اغلب به شکل شورش‌هایی است که هدف آنها بسیج کردن جمعیت علیه دولت است نه جنگ‌های متعارف که در آن ارتش‌ها با یکدیگر درگیر می‌شوند.

تروریسم در حملات علیه غیرنظامیان و اهداف بسیار نمادین و دارای طنین عاطفی مانند مسجد، راه‌آهن یا ساختمان‌های دولتی ظاهر می‌شود. چنین حملاتی برای به حداکثر رساندن شوک در نظر گرفته شده است. تروریسم فراملی شامل اقداماتی است که در آن قربانیان، مرتکبین و مکان‌های خشونت‌ناپذیر دولت‌ها و ملیت‌های مختلف هستند. حملات تروریستی فراملی در عین حال ممکن است توسط بازیگران محلی علیه اهداف خارجی در فضای درگیری جغرافیایی یا توسط ساکنان محلی افراطی یا شبکه‌های فراملی علیه اهداف خارجی آغاز شود. این ویژگی‌های بازیگر و مکان، تروریسم فراملی را از تروریسمی که توسط احزاب محلی در جنگ‌های داخلی انجام می‌شود متمایز می‌کند (کرنشاو^۲، ۲۰۲۰: ۴).

این دسته‌بندی‌های مختلف جنگ داخلی و تروریسم منحصر به فرد نیستند: شورشیان جنگ داخلی می‌توانند هم‌زمان تروریست‌های فراملی باشند. مداخله نظامی توسط دولت‌های خارجی یا نهادهای بین‌المللی مانند اتحادیه آفریقا، اتحادیه اروپا، ناتو، یا سازمان ملل از ارائه کمک‌های امنیتی و اطلاعاتی محدود به دولت‌های محلی درگیر تا استقرار نظامی در مقیاس کامل و اشغال

1. Schmid
2. Crenshaw



توسط نیروهای زمینی را شامل می‌شود. در این بین حملات هوایی، عملیات ویژه و تهیه سلاح و تجهیزات، آموزش و سایر اشکال کمک‌های زمینی توسط نیروهای خارجی وجود دارد. در خصوص تروریسم مدرن می‌توان گفت که تروریسم مدرن همگام با توسعه سلاح‌های نوآورانه و وسایل حمل و نقل مدرن رشد کرده است. نوآوری‌ها در فناوری تسلیحات، سلاح‌های کشنده را کوچک‌تر و قابل حمل‌تر کرده است، در حالی که شناسایی آنها دشوارتر شده است. صنعت حمل و نقل مدرن نه تنها تروریست‌ها را قادر می‌سازد تا ویرانی را به سراسر جهان منتقل کنند، بلکه اهداف آسیب‌پذیری را برای حملات تروریستی ایجاد می‌نمایند. 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^۱، ۲۰۰۵: ۹).

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. تسلیحات تروریستی غیرمتعارف نگرانی خاصی را ایجاد نموده؛ زیرا منابع، امکانات، یا ظرفیت‌های تکنولوژیکی یک دولت را برای تولید مقادیر کشنده گازهای شیمیایی سمی نمی‌طلبد. در واقع فقط به‌طور حداقل دانش شیمی-همراه با یک آزمایشگاه ابتدایی و چند ماده اولیه که بیشتر آنها را می‌توان به راحتی خریداری کرد- برای ایجاد یک سازمان تروریستی با توانایی انجام جنگ‌های غیرمتعارف که می‌تواند توده‌های مردم را از میان ببرد کافی است. بر این مبنا تنها توافق گسترده بین‌المللی در مورد ماهیت پدیده، ماهیت و مقیاس تهدید و اقدامات لازم برای مقابله با آن، کشورهای جهان را قادر می‌سازد تا به‌طور مؤثر با تروریسم مبارزه کنند و نفوذ آن را به حداقل برسانند.

۳. اقدامات اینترپل علیه تروریسم فراملی

علی‌رغم وجود تعاریف متعدد و غیرواحدی از مفهوم تروریسم و تروریست بیان شده است که به‌طور کلی بیانگر دیدگاه ارائه‌دهنده آن است، اجماعی بر دسته‌بندی تروریسم بر اساس نوع (مانند دولتی، مذهبی، پاتولوژیک، سایبری، نارکوتروریسم و بیوتروریسم)، مقیاس (داخلی و بین‌المللی)، انگیزه‌ها و اهداف آن وجود دارد. همچنین، ریشه‌ها و علل تروریسم می‌تواند منشأ داخلی (مانند شاخص‌های اجتماعی، اقتصادی، سیاسی و فرهنگی) و خارجی (مانند استعمار و پسااستعمار، درگیری‌های منطقه‌ای و دشمنی‌های تاریخی، دولت در مانده و مناطق بی‌قانون و نفوذ فرهنگ و سبک زندگی بیگانه) داشته باشد. چنین زمینه‌هایی می‌تواند به عنوان علل اشتراکی در نظر گرفته

1. Ganor



شوند و صرفاً بیانگر دلایل احتمالی تبدیل یک فرد به یک عضو بالقوه سازمان‌های تروریستی است (صالحی نژاد، ۱۳۹۸: ۲).

در خصوص جرم بودن تروریسم آنتونیو کاسسه می‌گوید «به نظر من می‌توان ادعا نمود که از این گذشته دست کم تروریسم بین‌المللی، تروریسم مورد حمایت دولت یا تروریسمی که دولت بر آن چشم می‌پوشد، جنایتی بین‌المللی است و هم اکنون به موجب حقوق بین‌الملل عرفی به عنوان نوع مجزایی از اینگونه جرائم در نظر گرفته و ممنوع است» (کاسسه، ۱۳۸۰: ۳۸۵).

سندلر، آرس و اندرز (۲۰۱۱) تخمین زدند که به ازای هر دلار سرمایه گذاری شده در فعالیت‌های ضد تروریستی اینترنتی، کشورهای عضو به طور متوسط ۲۰۰ دلار بازده دریافت می‌کنند. این بازده بزرگ را می‌توان با بازده ناامیدکننده مخارج امنیت داخلی ایالات متحده که توسط سندلر، آرس و اندرز (۲۰۰۹) در مطالعه اجماع کپنهاگ به صورت چهار تاده سنت بر دلار محاسبه شد، مقایسه کرد. (سندلر و همکاران^۱، ۲۰۱۱: ۳۱۹)، مولر و استوارت (۲۰۱۴) نیز در تحقیقات خود نشان دادند که امنیت داخلی ایالات متحده به توجیه ده‌ها میلیارد دلاری که هر سال خرج می‌شود، نزدیک نیست (مولر و استوارت^۲، ۲۰۱۴: ۲۳۷).

تسهیل نقل و انتقالات و مسافرت به نقاط مختلف جهان سبب شده مجرمین بتوانند برای فرار از مجازات به خارج از کشور متواری شوند. با توجه به سرزمینی بودن حاکمیت دولت‌ها، تعامل مثبت بین‌دولتی، بالاخص بین کشورهای عضو سازمان اینترنتی می‌تواند در جهت استقرار یک نظام عادلانه کیفری موثر واقع شده به طوری که هیچ کشوری مامن مجرمین متواری نشود (گودرزی و رزمی، ۱۳۹۷: ۵۰). آنچه می‌تواند از تهدیدات ناشی از جرایم سازمان یافته در هر دو عرصه داخلی و فراملی بکاهد اتخاذ سیاست‌ها و راهبردهایی اجرایی و کارا است که ضمن توانمندسازی سازمان‌های مسئولی چون اینترنتی، منجر به کاهش فعالیت‌های مجرمانه سازمان‌های جنایتکار نیز گردد. نتایج مطالعات حاکی از آن است که بهبود، تقویت و تجهیز کارآمد دستگاه‌های قضایی و پلیسی از طریق گسترش ارتباطات و همکاری‌های بین‌المللی به ویژه با کشورهای همسایه و عقد قراردادهای منطقه‌ای و بین‌المللی جهت همکاری با سایر کشورها، از مهم‌ترین تدابیر مطلوب در راستای مقابله با جرایم سازمان یافته فراملی می‌باشند (سیادت و پیرعلی، ۱۳۹۵: ۵۴). در ادامه سازوکارهای اتخاذی از سوی سازمان اینترنتی در راستای مقابله با تروریسم فراملی مورد بررسی قرار می‌گیرد.

1. Sandler et al
2. Mueller & Stewart

۳-۱. شناسایی تروریست‌های مظنون

اینترپل پل ارتباطی میان تمامی پلیس‌های ملی ۱۹۵ کشور عضو است. علاوه بر آشنایی با تدابیر عمومی این سازمان برای پیشگیری و برخورد با کلیه جرایم از قبیل اعلان‌ها و پایگاه‌های اطلاعاتی، اینترپل پروژه‌ها و تدابیر ویژه‌ای برای تعداد کثیری از جرایم مهم دارد (سلیمی، ۱۴۰۲)، اینترپل در سال ۱۹۲۳ به عنوان یک سازمان بین‌المللی مستقل با مأموریت ارتقای همکاری بین‌المللی در مبارزه با جرایم بین‌المللی تأسیس شد. در حال حاضر، اینترپل دارای ۱۹۵ کشور عضو است که حق عضویت تعیین شده عمدتاً برای کارکنان، زیرساخت‌ها و عملیات سازمان تأمین می‌شود و باقیمانده بودجه اینترپل از کمک‌های داوطلبانه تأمین می‌شود.

اینترپل آژانس‌های مجری قانون، دفاتر مرکزی ملی^۱ و دبیرخانه عمومی اینترپل^۲ را در مبارزه با جرایم و تروریسم فراملی مرتبط می‌کند. به‌طور خاص، اینترپل به شش نگرانی اصلی جنایی می‌پردازد: نخست) فساد؛ دوم) مواد مخدر و جرایم سازمان‌یافته؛ سوم) جرایم مالی و فناوری پیشرفته؛ چهارم) فراریان؛ پنجم) قاچاق انسان و ششم) تروریسم فراملی (مک کرو، ۲۰۲۳: ۴).

پس از چهار حمله از طریق آسمان در ۱۱ سپتامبر ۲۰۰۱ (از این پس ۱۱ سپتامبر)، اینترپل ۲۰ تا ۲۵ درصد از منابع سالانه مبارزه با جرم و جنایت خود را برای هماهنگ کردن تلاش‌های اجرای قانون بین‌المللی برای مقابله با تروریسم فراملی هزینه نمود. اینترپل شبکه‌های ارتباطی، امکانات آموزشی، بهترین شیوه‌ها، پایگاه‌های داده اطلاعات و سایر ظرفیت‌های خود را در اختیار کشورهای عضو قرار می‌دهد تا در دستگیری تروریست‌های مظنون به آنها کمک کند. بسیاری از این دستگیری‌ها زمانی اتفاق می‌افتد که تروریست‌ها هنگام تلاش برای عبور از مرزهای کشورها شناسایی می‌شوند (همان منبع: ۶).

ایجاد یک شبکه جهانی جهت تبادل اطلاعات میان پلیس کشورهای عضو، نقطه آغاز مهمی برای همکاری مؤثر میان کشورها می‌باشد. در این راستا اینترپل اقدام به طراحی و ایجاد یک سیستم ارتباط جهانی با نام I/24/7^۳ نموده است. این سیستم ابزاری است پیشرفته برای تسهیل فعالیت‌های پلیس بین‌المللی جنایی که دسترسی سریع و آسان اعضای این سازمان را به اطلاعات مهم پلیسی فراهم می‌سازد. این سیستم دارای مکانیزم‌های کلیدی جهت ارتقای همکاری، تشریک مساعی و ارتباطات میان اینترپل‌های سراسر جهان می‌باشد.

اعضای اینترپل و مأموران اجرای قانون در کشورهای عضو آنها می‌توانند از طریق پیوند ارتباطی امن شبکه، I/24/7 که یک پورتال اینترنتی با دسترسی محدود است، ارتباط برقرار کنند. هنگام اتصال به I/24/7 مأموران اجرای قانون در کشورهای عضو، اعضا می‌توانند اطلاعات را به

1. Members' National Central Bureaus (NCBs)
 2. INTERPOL General Secretariat (IPGS)
 3. McAndrew

اشتراک بگذارند و به پایگاه‌های اطلاعاتی و منابع آنلاین اینترپل دسترسی داشته باشند. شبکه I/24/7 همچنین توسط اینترپل برای صدور اعلان‌های دستگیری (قرمز) و پخش اخبار منتشر شده توسط کشور برای هشدار به کشورهای عضو برای بازداشت مجرمان یا تروریست‌های مظنون استفاده می‌شود. در میان بسیاری از موارد دیگر، پایگاه‌های اطلاعاتی اینترپل حاوی اطلاعات مربوط به تروریست‌های مظنون و اسناد مسافرتی دزدیده شده و گم شده^۱ است. چنین اسنادی توسط تروریست‌ها و جنایتکاران برای عبور از مرزهای بین‌المللی استفاده شده است که بررسی اقدامات تروریستی گذشته نشان می‌دهد که این امر در مورد برخی از هواپیماربایان ۱۱ سپتامبر نیز صادق بوده است (هوک^۲، ۲۰۲۲: ۳۸۳).

امروزه استفاده از طریق سیستم بیومتریک موجب شناسایی دقیق‌تر افراد مظنون شده است. 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. اینترپل در این راستا اقدام به ایجاد پروژه‌ای نمود که از طریق (چهره، تصویربرداری، تشخیص، جستجو و ردیابی)^۳ به کشورهای عضو کمک می‌کند تا داده‌های بیومتریک جنگجویان تروریست خارجی و دیگر مظنونان تروریستی را به اشتراک بگذارند.^۴

افسران مجری قانون محلی با استفاده از تجهیزات سیار به ثبت داده‌های بیومتریک زندانیان محکوم به جرایم مرتبط با تروریسم می‌پردازند. این داده‌ها سپس در پایگاه‌های اطلاعاتی اینترپل ذخیره می‌شوند، برای مثال به‌عنوان هشدار آبی^۵ که هشدارهای بین‌المللی برای جمع‌آوری اطلاعات اضافی درباره هویت، مکان یا فعالیت‌های یک شخص در رابطه با جرائم هستند.

۳-۲. جلوگیری از سفر افراد مظنون به تروریسم

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 همچنین به‌طور فزاینده‌ای در لیبی. نحوه هدف‌گیری و رادیکالیزه شدن افراد استخدام شده با تمرکز بیشتر بر رسانه‌های اجتماعی و سایر کانال‌های دیجیتال تغییر کرده است. در این خصوص داده‌های بیومتریک در شناسایی جنگجویان تروریست خارجی و جلوگیری از عبور آنها از مرزها اهمیت فزاینده‌ای دارد. از طریق اینترپل، این امکان وجود دارد که اطلاعات و هشدارها را در مورد

1. Suspected terrorists and stolen and lost travel documents (SLTD)
2. Houck
3. Facial, Imaging, Recognition, Searching and Tracking
4. <https://www.interpol.int/en/Crimes/Terrorism>
5. Blue Notices



شبکه‌های تروریستی فراملی به اشتراک گذاشت تا روش‌ها، انگیزه‌ها و تأمین مالی آنها را بهتر درک کند و در نهایت مظنونان را شناسایی و دستگیر کنند.

در حال حاضر پایگاه‌های اطلاعاتی اینترنتی حاوی جزئیات حدود ۱۳۵۰۰۰ جنگجوی تروریست خارجی است.^۱ این امر اینترنت را به بزرگ‌ترین مخزن چنین اطلاعاتی در جهان تبدیل نموده که می‌تواند در شناسایی این افراد به هنگام مسافرت حیاتی باشد. این داده‌ها از تعدادی از نقاط حساس از جمله مرزها، میدان‌های جنگ و زندان‌ها جمع‌آوری شده است. اسناد مسافرتی دزدیده شده دارای کلیدی برای تحرک تروریست‌ها، به ویژه برای جنگجویان تروریست خارجی است. این امر برای مقامات مرزی ضروری است که اطلاعات هویتی و گذرنامه مسافران را با پایگاه داده اسناد مسافرتی دزدیده و مفقود اینترنتی بررسی کنند.

پایگاه‌های اطلاعاتی دیگر برای مدیریت قوی مرزها، پایگاه‌های اطلاعاتی اسمی اینترنتی که حاوی جزئیات اطلاعات شخصی و سابقه جنایی افراد مشمول درخواست همکاری بین‌المللی است و پایگاه داده اسناد مسافرتی مرتبط با اعلامیه‌ها هستند (دفلم^۲، ۲۰۲۲: ۹). هنگامی که اطلاعات تروریستی در سطح جهانی به اشتراک گذاشته می‌شود، هر بررسی ترافیکی، کنترل گذرنامه یا جستجوی تصادفی احتمال شکست در عملیات تروریسم را دارد.

۳-۳. ردیابی منابع مالی تروریست‌ها

از آنجا که هر اقدام تروریستی مستلزم صرف هزینه است، در نتیجه پول را باید به مثابه خونی دانست که در رگ‌های سازمان‌های تروریستی جریان دارد، به گونه‌ای 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 (الهوپی نظری، ۱۳۹۶: ۷۲۶). 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 این رو اشخاصی که بدون اغراض حمایتی و صرفاً با انگیزه‌های سودجویانه با گروه‌های تروریستی یا اشخاصی که با گروه‌های تروریستی در ارتباط هستند، داد و ستد و تعامل مالی دارند، بهتر است مشارکت کنندگان در تأمین مالی تروریسم بدانیم نه حامیان مالی تروریسم (شمس ناتری و اسلامی، ۱۳۹۴: ۲۶۱).

در ماده (۱۸) کنوانسیون سرکوب تأمین مالی تروریسم، بر این امر تأکید شده که به منظور پیشگیری از تأمین مالی تروریسم دولت‌ها باید اقدامات تقنینی را اتخاذ نمایند. این اقدامات باید از انجام فعالیت‌های غیرقانونی مندرج در ماده (۲) افراد و سازمان‌ها در داخل قلمروهایشان جلوگیری

1. <https://www.interpol.int/en/Crimes/Terrorism/Identifying-terrorist-suspects>
2. Deflem

نماید. بر این اساس ایجاد اختلال در جریان کمک‌های مالی تروریست‌ها برای محدود کردن فعالیت‌های آنها ضروری است. واقعیت آن است که هر جنایتی که منجر به سود شود می‌تواند برای تأمین مالی تروریسم مورد استفاده قرار گیرد. این بدان معنی است که یک کشور ممکن است با خطرات مالی تروریسم مواجه شود، حتی اگر خطر یک حمله تروریستی کم باشد.

منابع تأمین مالی تروریسم شامل، کلاهبرداری سطح پایین، آدم‌ربایی برای باج، سوء استفاده از سازمان‌های غیرانتفاعی، تجارت غیرقانونی کالاها (مانند نفت، زغال‌سنگ، الماس، طلا و مواد مخدر «کاپتاگون»^۱) و ارزهای دیجیتال می‌باشد، اما محدود به این موارد نمی‌گردد. بر این اساس با ایجاد اختلال در جریان تأمین مالی تروریست‌ها و با درک بودجه حملات قبلی، می‌توان به جلوگیری از حملات در آینده کمک نمود (دفلم^۲، ۲۰۰۵: ۱۷۷).

بر این مبنای اینترپل روابط خود را با تعدادی از نهادها حفظ نموده تا به اجرای سیاست‌های سطح بالا و همکاری برای مقابله با تأمین مالی تروریسم کمک نماید. این نهادها عبارتند از: الف) گروه ویژه اقدام مالی^۳ که یک نهاد بین دولتی است که استانداردهای بین‌المللی را برای مبارزه با پولشویی و تأمین مالی تروریسم تدوین می‌کند؛ ب) نهادهای منطقه‌ای به سبک اف.ای.تی.اف^۴ که بهترین شیوه‌ها را در منطقه مربوطه خود منتشر می‌کنند؛ پ) گروه اگمونت^۵، شبکه‌ای متشکل از ۱۵۹ واحد اطلاعات مالی از سراسر جهان.

در سطح عملی، اینترپل به دنبال تشویق همکاری بهتر بین واحدهای اطلاعات مالی (اف. آی. یو)^۶ و پلیس در کشورهای عضو می‌باشد تا اشتراک‌گذاری اطلاعات و تجزیه و تحلیل اطلاعات را تشویق نماید.^۷ بخش کلیدی این امر ترویج گسترش فعالیت شبکه I/24/7 سیستم ارتباطات پلیس جهانی امن اینترپل، به اف. آی. یوها در سراسر جهان است.^۸

در سایت اینترپل در این خصوص نمونه‌ای بیان شده است که می‌تواند شیوه عملکرد این سیستم را نشان دهد. بر این مبنای یکی از کشورهای عضو اینترپل در اروپا درخواست کمک برای تحقیقات تأمین مالی تروریسم می‌نماید که در آن مظنون، سفر اعضای خانواده و دیگران را به مناطق درگیری با انتقال وجوهی به ارزش حدود ۱۸۰۰۰ یورو تأمین مالی کرده بود. افسران متخصص اینترپل به منظور ساده کردن تحقیقات مشاوره ارائه کردند و با چهار کشور عضو دیگر از آفریقا، آمریکا و خاورمیانه که وجوه انتقال داده شده بود، ارتباط برقرار کردند. به درخواست

1. captagon

2. Dflem

3. Financial Action Taskforce (FATF)

4. Financial Action Task Force (FATF)

5. Egmont Group

6. Financial intelligence units (FIUs)

۷. واحد اطلاعات مالی یک مجموعه تشکیلات ملی مرکزی در کشورهاست که از طریق ارتباط با سیستم بانکی، بیمه‌ای، مالیاتی، گمرکی و ... اطلاعات و گزارش‌های مالی مشکوک را دریافت و مورد تجزیه و تحلیل قرار می‌دهد.

8. <https://www.interpol.int/en/Crimes/Terrorism/Preventing-terrorist-travel>

کشوری که درخواست تحقیق داده بود، اینترپل اعلان قرمزی برای مظنون منتشر کرد که متعاقباً در کشور عضو دیگری که قبلاً نامرتبط بود دستگیر و برای پیگرد قانونی تحویل داده شد.^۱

۴. شبکه‌های نظارتی اینترپل در مقابله با تروریسم

در سال ۲۰۰۵، اینترپل دو شبکه نظارتی را معرفی نمود که شامل پایگاه داده شبکه سیار^۲ و پایگاه داده شبکه ثابت^۳ که جستجوی افراد، وسایل نقلیه موتوری و اسناد را در ترانزیت بین‌المللی یا سایر نقاط تسهیل می‌کند. تفاوت اصلی بین این شبکه‌ها این است که در شبکه ثابت امکان دسترسی به یک پایگاه داده آنلاین را فراهم می‌کند که به‌طور مداوم به‌روز می‌شود، در حالی که در پایگاه داده شبکه موبایل دسترسی به یک پایگاه داده آفلاین را نیز فراهم می‌کند که به صورت دوره‌ای و به روز شده هر ۲۴ تا ۴۸ ساعت دانلود می‌شود (انگریست^۴، ۲۰۰۹: ۲۳).

این فناوری‌ها در عملکرد اینترپل نشان‌دهنده آن است که می‌تواند در مهار جنایات بین‌المللی و تروریسم فراملی مؤثر باشند. با این حال تا دسامبر ۲۰۰۸، تنها ۴۷ کشور از ۱۸۸ کشور عضو اینترپل، این فناوری‌ها را پذیرفته بودند که بیانگر آن است که اثرات خارجی فراملی مبارزه با جرم و جنایت ناشی از دو پایگاه فوق به‌طور کامل توسط کشورهای عضو پیاده‌سازی داخلی نشده است.

سندلر به منظور درک دلایل این مزایای بهره‌برداری نشده، بررسی کردند که چرا برخی کشورها پیوستن به شبکه‌های سیار و ثابت را انتخاب کردند و برخی دیگر از اعضاء از پذیرش آن خودداری کردند. آنها دریافتند که درآمد سرانه، جمعیت و آزادی‌های دموکراتیک عوامل اصلی تعیین‌کننده برای نصب فناوری‌های فوق در کشورهای عضو اینترپل هستند. تا اوت ۲۰۱۲، بیش از صد عضو به شبکه‌های موبایل یا ثابت یا هر دو متصل بودند. این افزایش عضویت زمانی اتفاق افتاد که اینترپل برای آموزش کشورهای عضو خود در مورد مزایای این دو پایگاه داده در مبارزه با جنایات بین‌المللی و تروریسم فراملی فعالیت بیشتری کرد، با این حال، همه کشورهای عضو باز از این شبکه‌ها استفاده نکردند (سندلر^۵، ۲۰۱۱: ۳۲۱).

کشورهای عضو البته باید به خاطر داشته باشند که جلوگیری از تردد آزادانه تروریست‌های فراملی از کشوری به کشور دیگر، ضعیف‌ترین مشکل عمومی است، زیرا تروریست‌ها به دنبال عبور از مرزهای با حداقل هوشیاری هستند. علاوه بر این مبنای، اگر دو پایگاه اینترپل حملات

1. <https://www.interpol.int/en/Crimes/Terrorism/Tracing-terrorist-finances>

2. Mobile INTERPOL Network Database (MIND)

3. Fixed INTERPOL Network Database (FIND)

4. Angrist

5. Sandler

تروریستی فراملی را در کشورهای پذیرنده محدود کنند، حملات برنامه‌ریزی شده احتمالاً به کشورهای دیگر منتقل می‌شوند، جایی که فناوری‌های مشابه در آنجا به کار نمی‌روند. در واقع باید گفت که اگرچه تروریسم فراملی برای بسیاری از کشورها نگران‌کننده است، شبکه‌های طراحی شده توسط اینترپل اساساً تنها برای مهار تروریسم فراملی نیست، بلکه به منظور کاهش جرایم بین‌المللی (مثلاً قاچاق انسان) نیز می‌باشد توسط دو پایگاه اینترپل همچنین مجرمان غیر از تروریست‌ها را از عبور از مرزهای بین‌المللی منصرف می‌کند و این امر در ایجاد محدودیت برای فعالیت‌های تروریستها بسیار موثر است (ایندرز^۱، ۲۰۱۱: ۲۶۴).

توانایی کشورهای عضو برای دستگیری جنایتکاران و تروریست‌ها در مرزهایشان در پایان سال ۲۰۰۵ زمانی که اینترپل پیشنهاد پایگاه داده شبکه سیار و پایگاه داده شبکه ثابت (هر دو) را به اعضای علاقه‌مند ارائه کرد، بسیار افزایش یافت. هر دو شبکه‌های مذکور یک ابزار سیستماتیک کارآمد برای بررسی افراد، وسایل نقلیه موتوری و اسناد سفر در برابر پایگاه‌های اطلاعاتی جهانی اینترپل فراهم می‌کند. از طریق این دو شبکه، کشورها می‌توانند تمام گذرنامه‌ها و وسایل نقلیه موتوری را در گذرگاه‌های مرزی و سایر نقاط بررسی کنند. در عرض چند ثانیه، گذرنامه‌های اسکن شده یا اسناد خودرو توسط این دو شبکه - نسبت به بانک‌های اطلاعات ملی - بررسی می‌شوند. در غیاب این دو پایگاه، این جستجوها به دلیل رفتار مشکوک انجام می‌شود که دارای در واقع یک امر تصادفی است و لذا نمی‌توان به عنوان یک روش کارآمد در نظر گرفت. علاوه بر این، مأموران مرزی باید پست وظیفه خود را ترک کند و شماره پاسپورت یا سایر اسناد را در پورتال I/24/7 کلید بزند که چنین اقدامی اشتباه و خطرناک است (گاسبندر^۲، ۲۰۱۱: ۲۴۰).

کشورها بسته به زیرساخت‌هایشان ممکن است به پایگاه داده شبکه سیار و پایگاه داده شبکه ثابت یا هر دو متکی باشند. یکی از تفاوت‌های کلیدی میان این دو پایگاه تازگی و به‌روز بودن اطلاعات قابل دسترسی است. شبکه اطلاعات ثابت دسترسی آنلاین بلادرنگ به پایگاه‌های اطلاعاتی اینترپل را امکان‌پذیر می‌سازد، در حالی که پایگاه اطلاعات موبایل حاوی یک کپی از این پایگاه‌های اطلاعاتی است. این نسخه آفلاین به صورت دوره‌ای، ظرف ۴۸ ساعت یا کمتر به روز می‌شود.

بنابراین، پایگاه داده شبکه ثابت تا حدودی داده‌های به‌روزتری را ارائه می‌دهد. با این حال، این مزیت احتمالاً با گذشت زمان از بین می‌رود؛ زیرا پایگاه اطلاعات موبایل به‌طور منظم به‌روز می‌شود. در عمل، این تأخیر کوتاه نباید هیچ تفاوت مؤثری بین این دو پایگاه ایجاد کند. این دو پایگاه امکان دسترسی به پایگاه‌های اطلاعاتی عظیم حاوی میلیون‌ها رکورد را نیز فراهم می‌کند

1. Enders
2. Gassebner



که توسط همه کشورهای عضو اینترپل قابل دسترس است و این پایگاه‌های داده اطلاعات به‌طور مداوم به‌روز می‌شوند.

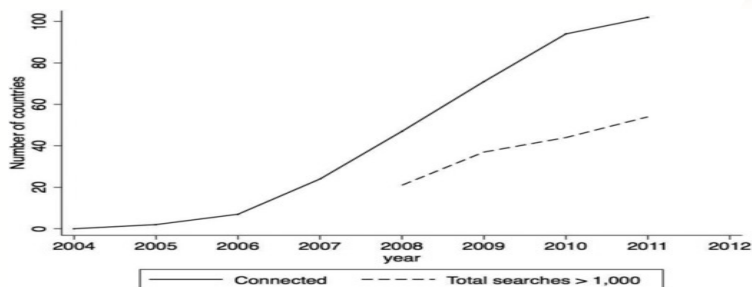
با این حال، بزرگی جریان سوابق در مقایسه با اندازه رکوردهای موجود در پایگاه‌های داده اطلاعات بسیار ناچیز است؛ بنابراین، جستجو در پایگاه‌های اطلاعاتی اینترپل از طریق شبکه داده موبایل، جریان سوابق را از آخرین به‌روزرسانی از دست می‌دهد. برای مثال، اگر از زمان آخرین به‌روزرسانی، مظنون تروریستی جدیدی ظاهر شود، این می‌تواند بین اطلاعات پایگاه داده شبکه سیار و پایگاه داده شبکه ثابت تفاوت ایجاد کند، اما پس از آن اعلان قرمز این تطابق ایجاد می‌گردد. البته پیش‌بینی می‌شود که تروریست‌ها از اسناد مسافرتی دزدیده شده یا گم شده از قبل^۱، استفاده کنند.^۲ کشورها همچنان می‌توانند بدون امکان استفاده از این دو پایگاه داده اطلاعات نسبت به دستگیری تروریست‌ها اقدام نمایند، زمانی که رفتار یک فرد مشکوک ایجاب می‌کند و یا فردی خود را تسلیم می‌کند.^۳

بررسی داده‌های سالانه کشورهای عضو اینترپل، از سال ۲۰۰۵ تا ۲۰۱۱ می‌تواند میزان استفاده از این فناوری‌ها را به‌وسیله کشورهای عضو نشان دهد. شکل ۱ تعداد کشورهای متصل به پایگاه داده شبکه سیار و پایگاه داده شبکه ثابت را از سال ۲۰۰۴ تا ۲۰۱۱ نشان می‌دهد. در طول سال ۲۰۰۵، سوئیس و لیختن اشتاین اولین کشورهایی بودند که به این شبکه‌ها پیوستند. تا پایان سال ۲۰۰۶، بلژیک، لیتوانی، اسپانیا، سنت کیتس و نویس و ترکیه نیز به این شبکه پیوستند. تعداد کشورهای متصل به شبکه موبایل و ثابت در سال ۲۰۰۷ به ۲۴ کشور، در سال ۲۰۰۸ به ۴۷ کشور، در سال ۲۰۰۹ به ۷۱، در سال ۲۰۱۰ به ۹۴ کشور و در سال ۲۰۱۱ به ۱۰۲ کشور رسید.

1. INTERPOL's SLTD database

۲. در این خصوص می‌توان به بانک اطلاعاتی گذرنامه‌های مفقوده و مسروقه اینترپل اشاره نمود. این پایگاه داده به پلیس کمک می‌کند تا تروریست‌ها و جنایتکارانی را که اغلب از اسناد مسافرتی جعلی برای عبور از مرزها استفاده می‌کنند، شناسایی و دستگیر کنند. پایگاه داده مذکور حاوی اطلاعاتی درباره اسناد مسافرتی و هویتی است که به‌عنوان دزدیده، گم شده، باطل، نامعتبر یا به سرقت رفته گزارش شده است. افسران مجری قانون در سراسر جهان می‌توانند اعتبار یک سند مسافرتی یا هویتی را در چند ثانیه با استفاده از پایگاه داده SLTD بررسی کنند. پایگاه داده SLTD حاوی اطلاعاتی درباره اسناد مسافرتی و هویتی است که به‌عنوان خالی، مفقود، باطل، نامعتبر یا دزدیده شده گزارش شده‌اند.

۳. البته همه کشورهای مرتبط با این دو پایگاه از این فناوری برای جستجو استفاده نمی‌کنند. در مارس ۲۰۱۴، زمانی که دو مسافر با گذرنامه‌های دزدیده شده سوار بر پرواز ۳۷۰ خطوط هوایی مالزی شدند و توسط مالزی، یک کشور دارای پایگاه داده ثابت از ژوئن ۲۰۰۷، غربالگری نشدند، این موضوع کاملاً مشخص شد.



نمودار ۱- کشورهای متصل به پایگاه داده شبکه سیار و پایگاه داده شبکه ثابت

علاوه بر تاریخ دقیق اتصال هر کشور، اطلاعات بخش تجزیه و تحلیل اینترنت تعداد جستجوهای هر کشور عضو را برای سال‌های ۲۰۰۸ تا ۲۰۱۱ را نیز ارائه نمود. تعداد کل جستجوهای دو پایگاه داده موبایل و ثابت توسط کشورهای عضو نشان داد که برخی از کشورهای متصل واقعاً از این شبکه‌ها استفاده نمی‌کنند و همچنین برخی از کشورهایی که به‌طور رسمی نامرتب هستند، زمانی که رفتارهای مشکوک یا رویدادهای بین‌المللی برانگیخته می‌شوند، از طریق پورتال I/24/7 اطلاعات خود را جستجو می‌کنند. چنین آستانه ملایمی از نظر تعداد کشورهایی که واقعاً از این دو پایگاه استفاده کرده‌اند تفاوت ایجاد می‌کند و بنابراین می‌توان آن‌ها را به عنوان یک عرف رفتاری در دولت‌ها در نظر گرفت. جدول زیر تعداد موارد سالانه کشور و میانگین تعداد جستجوها را گزارش می‌کند که بر اساس اینکه کشورها به‌طور رسمی به هر دو شبکه متصل بوده‌اند و اینکه آیا تعداد جستجوها بالاتر یا کمتر از آستانه ۱۰۰۰ بوده، طبقه‌بندی شده است. جدول زیر همچنین نشان می‌دهد که در ۱۲۴ مورد در سال، کشورها به‌طور رسمی به هر دو پایگاه متصل بودند، اما کمتر از ۱۰۰۰ جستجو در شبکه انجام دادند (به‌طور متوسط ۸۱.۱ جستجو در سال). این ارقام نشان می‌دهد که آن کشورها، اگرچه به‌طور رسمی به این پایگاه‌ها متصل هستند، اما به‌طور سیستماتیک از شبکه استفاده نکرده‌اند. علاوه بر این، نمونه ما شامل مواردی است که در آن کشورهایی که به‌طور رسمی به شبکه متصل نیستند، بیش از ۱۰۰۰ جستجو در شبکه از طریق پورتال I/24/7 خود انجام دادند (به‌طور متوسط ۸۹۷۹۷۴.۹ جستجو). اگرچه این کشورها کشورهای متصل به پایگاه‌های موبایل و ثابت نبودند، اما حجم جستجوهای آنها به اندازه کافی زیاد است که نشان‌دهنده استفاده بیش از حد معمول از شبکه است. به‌طور خلاصه، جدول زیر نشان می‌دهد که آستانه ۱۰۰۰ جستجو، استفاده سیستماتیک تری از شبکه را نسبت به وضعیت اتصال مشخص می‌کند. از این پس زمانی که کشوری واقعاً از شبکه موبایل و ثابت I/24/7 برای انجام حداقل هزار جستجو در سال استفاده می‌کند، در تجزیه و تحلیل و آمار در نظر گرفته می‌شود (گاردیازبال^۱، ۲۰۱۵: ۷).

1. Gardeazabal



Table 1

Number of searches and MIND/FIND connection status

Number of searches	Connected		Not connected	
	Average searches	Country-year cases	Average searches	Country-year cases
≥1,000	11,005,625.0	135	897,974.9	7
<1,000	81.1	124	3.0	298

[Open in a separate window](#)

Notes: This table shows the average number of searches and the number of country-year cases classified according to MIND/FIND connection status and whether countries performed at least 1,000 searches or not.

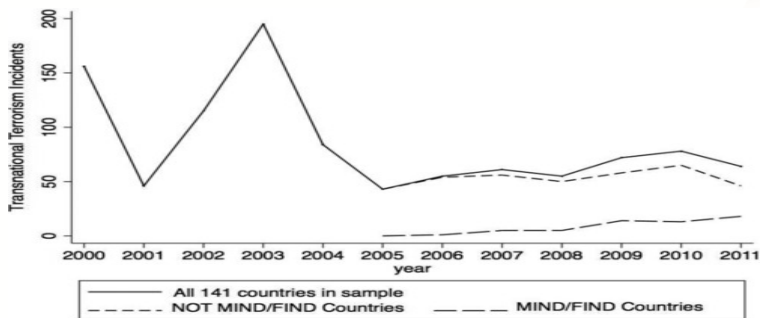
نمودار ۲- تعداد موارد سالانه کشور و میانگین تعداد جستجوها

بنابراین، کشوری در یک سال خاص اگر تعداد کل جستجوها (در هر دو شبکه) بیش از ۱۰۰۰ باشد، تحت بررسی قرار می‌گیرد. با این حال، دامنه زمانی تجزیه و تحلیل ما از سال ۲۰۰۵ تا ۲۰۱۱ است. این دامنه نه تنها شامل دوره ۲۰۰۸ تا ۲۰۱۱ است که تعداد جستجوهای آن در دسترس است، بلکه دوره ۲۰۰۵ تا ۲۰۰۷ را نیز شامل می‌شود که فقط اطلاعاتی در مورد وضعیت اتصال پایگاه داده شبکه سیار و پایگاه داده شبکه ثابت دارد، اما هیچ اطلاعاتی دیگری قابل دسترسی نیست.

متغیر نتیجه، تعداد حوادث تروریستی فراملی است که در یک کشور به انجام می‌رسد که از طریق پروژه «تروریسم بین‌المللی: ویژگی‌های رویدادهای تروریستی»^۱ در دسترس است. این پروژه اطلاعات زیادی را برای کسانی که می‌خواهند تروریسم بین‌المللی را فراتر از ارجاعات گزینشی یا حکایتی تجزیه و تحلیل کنند، ارائه می‌کند. این پروژه داده‌های مربوط به ویژگی‌های گروه‌های تروریستی فراملی، فعالیت‌های آن‌ها که تأثیرات بین‌المللی دارند و محیطی که در آن فعالیت می‌کنند را ارزیابی می‌کند. مجموعه داده پروژه، جامع‌ترین و پر استنادترین مجموعه داده عمومی در مورد تروریسم فراملی است (میکولوس و همکاران^۲، ۲۰۱۶: ۲).

پروژه «تروریسم بین‌المللی: ویژگی‌های رویدادهای تروریستی» از رسانه‌های خبری برای شناسایی حوادث تروریستی فراملی و محل وقوع آنها در کشور استفاده می‌کند. شکل زیر نمودار زمانی تعداد حوادث تروریسم فراملی را در نمونه ما برای دوره ۲۰۰۰ تا ۲۰۱۱ نشان می‌دهد. در طول دوره فرعی ۲۰۰۵ تا ۲۰۱۱، تعداد کل حوادث به گروه کشورهای تحت بررسی (دارای هر دو شبکه) و کشورهایی که دارای این دو شبکه نیستند. البته لازم به ذکر است که برخی کشورهایی که ابتدا به شبکه‌های موبایل و ثابت ملحق شدند، قبل از پیوستن به شبکه یا پس از آن فقط چند حادثه داشتند، به عنوان مثال، سوئیس در کل دوره نمونه، قبل یا بعد از پیوستن به شبکه‌ها هیچ حادثه‌ای را تجربه نکرد (همان منبع: ۴).

1. The International Terrorism: Attributes of Terrorist Events (ITERATE)
2. Mickolus et al.



نمودار ۳- حوادث تروریسم فراملی را در نمونه برای دوره ۲۰۰۰ تا ۲۰۱۱

واقعیت آن است که امنیت جهانی به سطح امنیت در کشوری که کمترین امنیت را داراست بستگی دارد؛ بنابراین، پذیرش هر دو شبکه ایجاد شده توسط اینترنتل به وسیله یک کشور ممکن است برخی از حوادث تروریستی فراملی را به کشورهایی که از این فناوری استفاده نمی‌کنند منحرف نماید، در نتیجه تروریسم فراملی را در کشورهای تحت نظارت و متصل کاهش داده و آن را در کشورهای متصل نشده افزایش می‌دهد (گاردیازبال، ۲۰۱۵: ۹).

تجزیه و تحلیل‌ها نشان می‌دهد که کشورهای عضو اینترنتل که اتصال به شبکه‌های موبایل و ثابت را پذیرفته‌اند و همچنین از آن برای غربال افراد و اسناد در گذرگاه‌های مرزی و سایر نقاط کلیدی استفاده کرده‌اند، نسبت به کشورهای عضو که به این اتصال نپیوستند و یا آن را نصب کرده، اما فعال نکرده‌اند، کمتر دچار حوادث تروریستی فراملی شده‌اند. برآوردها نشان می‌دهد که کشوری با ۶۴ میلیون نفر، مانند فرانسه در سال ۲۰۰۸، به طور متوسط هر سال ۰.۳۲ کمتر از حوادث تروریستی فراملی را در نتیجه استفاده از هر دو شبکه اینترنتل تجربه می‌کند. این کاهش حملات تروریستی ممکن است زیاد به نظر نرسد، اما برای اکثر کشورها کاهش قابل توجهی در حوادث تروریستی فراملی حدود ۳۰ درصد است و در سطح جهانی، این می‌تواند به کاهش حملات بسیار منجر شود (همان: ۱۰).

اگرچه هر حادثه تروریستی فراملی به طور متوسط یک نفر را می‌کشد و دو نفر را مجروح می‌کند، اما کاهش این حوادث از طریق دو شبکه اینترنتل به معنای دستگیری احتمالی تروریست‌ها و ایجاد اختلال در اقدامات گروه‌های تروریستی است. علاوه بر این، ممکن است در مواقعی یک رویداد مهم تروریستی، مانند ۱۱ سپتامبر یا بمب‌گذاری در قطار شهری مادرید در سال ۲۰۰۴، متوقف شود، جایی که نتیجه آن عملیات، کشتار و خرابی وسیعی در پی داشت. در واقع این استدلال وجود دارد که بازده حتی برای حوادث کوچک نیز زیاد است؛ زیرا مهار چنین حوادثی پوشش رسانه‌ای حملات را کاهش می‌دهد، جذب تروریست را محدود می‌کند و اضطراب جامعه

را کاهش می‌دهد. علاوه بر این، کاهش حوادث تروریستی فراملی در سرتاسر جهان به کشورها اجازه می‌دهد که تا حدودی هزینه‌های امنیت داخلی را کاهش دهند (سن^۱، ۲۰۲۲: ۶).

نکته قابل توجه عبارت است از تأثیر بررسی شبکه‌های موبایل و ثابت اینترنت بر تروریسم فراملی که ممکن است تحت تأثیر مداخله در کشورها باشد. این مداخله ممکن شامل فرآیندی باشد که آن را ضعیف‌ترین پیوند می‌نامیم. ضعیف‌ترین اثر پیوند مربوط به جابجایی احتمالی حوادث تروریستی فراملی از کشورهای متصل به شبکه‌ها به کشورهایی است که از این فناوری استفاده نمی‌کنند. ضعیف‌ترین اثر پیوندی می‌تواند بر تخمین‌ها نقش داشته باشد؛ زیرا بخشی از اثر بررسی با افزایش تعداد حوادث تروریستی فراملی در کشورهای غیر متصل به شبکه‌ها مطابقت دارد. نوع دوم تداخل بین واحدها، اثرات هم‌تا است که به موجب آن کشورهای متصل یا غیرمتصل به شبکه‌های اینترنت از استفاده کلی فناوری‌ها بهره می‌برند. اثر هم‌تا ممکن است تا حدی با سیستم هاب اسپیک^۲ سفر هوایی مرتبط باشد، جایی که مسافران باید از مراکز اصلی (مانند هیتر و در لندن، شارل دوگل در پاریس، یا فرودگاه فرانکفورت در آلمان) سفر کنند. به مقصد نهایی خود برسند. اگر فرودگاه‌های اصلی در کشورهای دارای سیستم متصل به شبکه‌ها باشند، اثرات هم‌تایان بیشتر خواهد بود (گاردیازبال، ۲۰۱۵: ۱۰).

البته شبکه‌های موبایل و ثابت اینترنت نمی‌توانند حوادث تروریستی فراملی را که در آن یک عامل به دارایی‌های خارجی (افراد یا اموال) برای اهداف سیاسی حمله می‌کند را حذف کنند. علاوه بر این، شبکه‌های مذکور نمی‌توانند ترانزیت تروریست‌های بالقوه را که اطلاعات آنها در اینترنت یا بانک‌های داده ملی به عنوان تروریست‌های مظنون نیستند، شناسایی کنند؛ بنابراین، شبکه‌های اینترنت می‌توانند مقابله با تروریسم فراملی را بهبود بخشند، اما نمی‌توانند آن را از بین ببرند. یک نقطه ضعف بالقوه این شبکه‌ها ممکن است مربوط به افزایش تروریسم داخلی باشد، به طوری که مقامات باید مراقب این انتقال با گسترش استفاده از این شبکه‌ها باشند. برای حملات تروریستی داخلی، کشورها انگیزه‌های مناسبی برای اتخاذ اقدامات پیشگیرانه دارند؛ زیرا هرگونه منافع حاصله به طور کامل توسط کشور عامل به دست می‌آید و هیچ تبعات خارجی فراملی وجود ندارد.

البته اگر بخواهیم هزینه‌های اینترنت را در نظر بگیریم، کل بودجه عملیاتی اینترنت در سال (۲۰۱۱) ۶۰ میلیون یورو اعلام گردیده است. بر اساس درصدهای گذشته محاسبه شده توسط سندلر، آرس و اندرز (۲۰۱۱) برای سال‌های ۲۰۰۶ و ۲۰۰۷، حدود ۲۳ درصد از بودجه اینترنت صرف هماهنگی مبارزه با تروریسم می‌شود. برای مثال، آنها تمام هزینه‌های I-۷/۲۴ را در تلاش‌های اینترنت برای مقابله با تروریسم لحاظ کردند. اگر از درصد آنها استفاده کنیم، کمتر از

1. San

2. hub-spoke system

۱۳۸ میلیون یورو توسط اینترپل در سال ۲۰۱۱ برای کمک به فعالیت‌های ضد تروریسم کشورهای عضو هزینه شده است (سندلر و همکاران، ۲۰۱۱: ۳۲۵). کشورهای عضوی که از شبکه‌های متصل استفاده می‌کنند، قبل از اینکه مقامات مرزی‌شان بتوانند از فناوری و پایگاه‌های اطلاعاتی برای جستجو استفاده کنند، هزینه‌های راه‌اندازی اولیه را دارند. لذا پیرامون امنیت داخلی می‌توان گفت که هزینه‌های کوچک اینترپل در خنثی کردن تروریسم فراملی با ایمن‌تر شدن مرزهای کشورها، بازپرداخت بیشتری دارد.

بحث و نتیجه‌گیری

پوشش تاریخی مقابله با تروریسم در عرصه بین‌المللی بیانگر آن است که مقابله با تروریسم یک چالش بین‌المللی است. تروریسم در ماهیت استفاده‌ی از پیش برنامه‌ریزی شده یا تهدید به استفاده از خشونت توسط افراد یا گروه‌ها برای دستیابی به یک هدف سیاسی یا اجتماعی از طریق ارباب مخاطبان بزرگ فراتر از قربانیان فوری است. در توصیف تروریسم فراملی باید گفت همان‌طور که شرکت‌های فراملیتی از یک مکان سرچشمه می‌گیرند و عملیات‌هایی را توسعه می‌دهند که در سطح محلی و بین‌المللی گسترش می‌یابد، گروه‌های تروریستی با اهداف، فعالیت‌ها و اشکال سازمانی که فراتر از مبدأ خود هستند را می‌توان «فراملی» نیز نامید. دو عامل مهم در شناخت تروریسم فراملی دخالت دارد که شامل متفاوت بودن تابعیت عاملان تروریستی و تسری اقدامات و عملیات‌های تروریستی به خارج از مرزهای کشوری است که تروریست‌ها در آن حضور دارند. همچنین تمایز تابعیت قربانیان نیز معیار دیگری برای شناسایی تروریسم فراملی می‌باشد. در تمایز تروریسم فراملی از جنگ داخلی باید گفت جنگ‌های داخلی به عنوان درگیری‌های خشونت‌آمیز درون‌دولتی در نظر گرفته می‌شوند که یک دولت را در برابر رقبای غیردولتی قرار می‌دهند، خواه این رقبای جدایی‌طلبان با انگیزه نارضایتی‌های ملی‌گرایانه قومی یا اقلیت‌ها یا انقلابیونی که هدفشان جابه‌جایی نخبگان حاکم است، باشند. جنگ‌های داخلی اغلب به شکل شورش‌هایی است که هدف آنها بسیج کردن جمعیت علیه دولت است نه جنگ‌های متعارف که در آن ارتش‌ها با یکدیگر درگیر می‌شوند. یکی از نهادهایی که در مقابله با تروریسم فراملی نقش مهمی ایفاء می‌نماید سازمان اینترپل می‌باشد که این نقش را از طرق مختلف اعمال می‌نماید. اینترپل آژانس‌های مجری قانون، دفاتر مرکزی ملی و دبیرخانه عمومی اینترپل را در مبارزه با جرایم و تروریسم فراملی مرتبط می‌کند. به طور خاص، اینترپل به شش نگرانی اصلی جنایی می‌پردازد: نخست) فساد؛ دوم) مواد مخدر و جرایم سازمان‌یافته؛ سوم) جرایم مالی و فناوری پیشرفته؛ چهارم) فراریان؛ پنجم) قاچاق انسان و ششم) تروریسم فراملی. اینترپل در راستای مقابله با شبکه تروریسم فراملی از روش‌هایی استفاده می‌کند که به کارگیری ابزارهایی برای شناسایی تروریست‌های مظنون از جمله این روش‌ها می‌باشد. این روش استفاده از سیستم بایومتریک و وارد نمودن اطلاعات در

شبکه ۲۴/۷ می‌باشد. روش دیگر جلوگیری کردن از مسافرت افراد مظنون است. شیوه دیگر ردیابی منابع مالی تروریست‌ها است که این امر با محدود نمودن این منابع توسط کشورهای عضو انجام می‌شود. آنچه در این مقاله مد نظر ما به صورت خاص قرار گرفت شبکه‌های نظارتی اینترنتی و کارآیی آن‌ها در مقابله با تروریسم فراملی بود. در سال ۲۰۰۵، اینترنتی دو شبکه نظارتی را معرفی نمود که شامل پایگاه داده شبکه موبایل و پایگاه داده شبکه ثابت که جستجوی افراد، وسایل نقلیه موتوری و اسناد را در ترانزیت بین‌المللی یا سایر نقاط تسهیل می‌کند. تفاوت اصلی بین این شبکه‌ها این است که در شبکه ثابت امکان دسترسی به یک پایگاه داده آنلاین را فراهم می‌کند که به طور مداوم به‌روز می‌شود، در حالی که در پایگاه داده شبکه موبایل دسترسی به یک پایگاه داده آنلاین را نیز فراهم می‌کند که به صورت دوره‌ای و به‌روز شده هر ۲۴ تا ۴۸ ساعت داندولد می‌شود. واقعیت آن است که امنیت جهانی به سطح امنیت در کشوری که کمترین امنیت را داراست بستگی دارد؛ بنابراین، پذیرش هر دو شبکه ایجاد شده توسط اینترنتی به وسیله یک کشور ممکن است برخی از حوادث تروریستی فراملی را به کشورهای دیگر که از این فناوری استفاده نمی‌کنند منحرف نماید، در نتیجه تروریسم فراملی را در کشورهای تحت نظارت و متصل کاهش داده و آن را در کشورهای متصل نشده افزایش می‌دهد. تجزیه و تحلیل‌ها نشان می‌دهد که کشورهای عضو اینترنتی که اتصال به شبکه‌های موبایل و ثابت را پذیرفته‌اند و همچنین از آن برای غربال افراد و اسناد در گذرگاه‌های مرزی و سایر نقاط کلیدی استفاده کرده‌اند، نسبت به کشورهای عضو که به این اتصال نپیوستند و یا آن را نصب کرده، اما فعال نکرده‌اند، کمتر دچار حوادث تروریستی فراملی شده‌اند. البته این شبکه‌های مذکور نمی‌توانند ترانزیت تروریست‌های بالقوه را که اطلاعات آنها در اینترنتی یا بانک‌های داده ملی به عنوان تروریست‌های مظنون نیستند، شناسایی کنند. آنچه بیان گردید ما را به این نتیجه می‌رساند که مقابله با تروریسم فراملی نیازمند عزم جدی در سطح بین‌المللی است و اگر دولت‌ها در این خصوص عزم جدی داشته باشند بهره‌گیری از روش‌هایی همچون شبکه نظارتی اینترنتی بسیار مفید خواهد بود، اما اگر این عزم به دلایل مختلفی جدی نباشد جامعه جهانی قادر نخواهد بود در مقابله با تروریسم فراملی مؤثر عمل نماید. شاید بتوان گفت که نپیوستن و یا همکاری نکردن برخی دولت‌ها با این شبکه به همان دلایلی باشد که هنوز جامعه جهانی نتوانسته است به تعریف واحدی از «تروریسم» دست یابد و این امری است که ما همواره با آن درگیر خواهیم بود؛ اما لازم است توجه شود که برخی از اقدامات به وضوح دارای ویژگی‌های یک اقدام تروریستی هستند و شناسایی گروه‌هایی که به این نوع اقدامات دست می‌زنند و تهدید دولت‌ها به همکاری با سازمان‌هایی همچون اینترنتی و همچنین عزم جدی در استفاده از روش‌های نوین در مقابله با این نوع اقدامات، علاوه بر اینکه از بسیاری از هزینه‌های دخالی خواهد کاست به تحقق هر چه بیشتر امنیت جهانی کمک خواهد نمود.

منابع

- الهویی نظری، حمید؛ میل زوار جلالی، امیر. (۱۳۹۶). مسئولیت بین‌المللی دولت‌های تأمین‌کننده مالی تروریسم. *مطالعات حقوق عمومی*، ۴۷.
- بصیری، علی؛ آقا محمدی، زهرا. (۱۳۹۶). آینده پژوهی خاورمیانه طی سه دهه آینده؛ تحلیل روندهای مقابله با تروریسم در سطح بین‌الملل. *تحقیقات سیاسی و بین‌المللی*، ۹ (۳۱).
- رهامی، محسن؛ نژاد، آذر. (۱۳۹۰). ریشه‌های ایدئولوژیک تروریسم. *سیاست*، ۳ (۴۱)، ۱۳۱-۱۵۱.
- سلیمی، صادق. (۱۴۰۲). *اینترپل: از تعقیب تا تضمین حقوق متهمین و مجرمین*. چاپ اول. تهران: موسسه مطالعات و پژوهش‌های حقوق شهر دانش.
- سیادت، سعیده؛ پیرعلی، علی رضا. (۱۳۹۵). جرایم سازمان‌یافته فراملی و نقش اینترپل در مقابله با آن. *مطالعات بین‌المللی پلیس*، ۲۵.
- شمس‌ناتری، محمد ابراهیم؛ اسلامی، داوود. (۱۳۹۴). ماهیت کیفری تأمین مالی تروریسم. *مطالعات حقوق کیفری و جرم‌شناسی*، ۲ (۴).
- کارگری، نوروز. (۱۳۹۱). *درون‌مایه‌های تروریسم*. تهران: نشر میزان.
- گودرزی، مسعود؛ رزمی، سمیرا. (۱۳۹۷). نقش پلیس اینترپل در ناامن سازی جهان برای مجرمین. *امنیت انتظامی دریایی*، ۳۵، ۶۶-۵۰.
- کاسسه، آنتونیو. (۱۳۸۰). حمله تروریستی به مرکز تجارت جهانی و برهم خوردن برخی مقوله‌های تعیین‌کننده حقوق بین‌الملل. *اطلاعات سیاسی اقتصادی*، (۷۳ و ۱۷۴)، ۶۱-۵۴.
- صالحی نژاد، علیرضا. (۱۳۹۸). *ضرورت رویکردی اجتماعی روان‌شناختی برای مقابله با تروریسم: چرا افراد به گروه‌های تروریستی ملحق می‌شوند*. سومین همایش سالانه انجمن علمی مطالعات صلح ایران علوم انسانی و اجتماعی و صلح، تهران، انجمن علمی مطالعات صلح ایران.
- Abrahms, M. (2006). *Why Terrorism Does Not Work*, International Security, 31(2).
- Angrist, J. D., & Pishke, J.-S. (2009). *Mostly harmless econometrics: An empiricist's campaign*. Princeton, NJ: Princeton University Press.
- Bridge, S. T. (2009). *Russia's New Counteracting Terrorism Law: The Legal Implications of Pursuing Terrorists Beyond the Borders of the Russian Federation*, 3, Columbia Journal of East European Law.
- Crenshaw, M. (2020). *Rethinking Transnational Terrorism AN INTEGRATED APPROACH*, United States Institute of Peace, 158.
- Deflem M., Maybin L. C. (2005). *Interpol and the policing of international terrorism: Developments and dynamics since September 11*. In Snowden L. L., Whitsel B. (Eds.). *Terrorism: Research, readings, and realities*.
- Deflem, M. (2022). *The Declining Significance of Interpol: Policing International Terrorism After 9/11*, Sag Journals, First published.
- Duffy, H. (2015). *Terrorism' in international law*, Published online by Cambridge University Press.
- Enders, W., & Sandler, T. (2011). *Who adopts MIND/FIND in INTERPOL's fight against international crime and terrorism?* Public Choice, 149.



- Gardeazabal, J. (2015). INTERPOL's Surveillance Network in Curbing Transnational Terrorism, *J Policy Anal Manage*, 34 (4)
- Gassebner, M., & Luechinger, S. (2011). Lock, stock, and barrel: A comprehensive assessment of the determinants of terror. *Public Choice*, 149.
- Horgan, J. (2014). *The Psychology of Terrorism Second Edition*, eBook Published, London.
- Houck, M., W.P. McAndrew. (2020). *Interpol review of forensic science management literature 2016-2019*, Forensic Sci. Int.: Synergy, 2
- Lutz, James M. and Lutz, Brenda J. (2013). *Global Terrorism*, 3rd ed. London: Routledge.
- McAndrew, W. P. et al. (2023). *Interpol review of forensic management, 2019–2022*, Forensic Science International: Synergy, 6
- Mickolus, Edward F.; Sandler, Todd; Flemming, Peter A.; Simmons, Susan L. (2016). *The International Terrorism: Attributes of Terrorist Events (ITERATE) Datasets*.
<https://doi.org/10.5683/SP/YRFU12>
- Mueller, J., & Stewart, M. G. (2014). Evaluating counterterrorism spending. *Journal of Economic Perspectives*, 28.
- San, S. (2022). Transnational policing between national political regimes and human rights norms: *The case of the Interpol Red Notice system*, *Sag Journals*, 26(4).
- Sandler, T., Enders, W., & Gaibullov, K. (2011). Domestic versus transnational terrorism: Data, decomposition, and dynamics. *Journal of Peace Research*, 48.
- Schmid, A. (2004). Terrorism: The Definitional Problem, *Case Western Reserve Journal of International Law*.36
- Ganor, B. (2005). *Strategy of Modern Terrorism*, Innovation Exchange, 10.