Original Article Open Access

The Iranian Association of Medical Law

Medical Law Journal

2022; 16(Special Issue on Legal Developments): e33

Journal Homepage: http://ijmedicallaw.ir

The Bioethics and Health Law Institute

The Dimensions of States Obligation to Cooperation in Establishing Rules in Response to Cyber Terrorism

Leila Mirbod[1], Sadegh Salami[2*], Saber Niavarani[1], Seyed Ghasem Zamani[3]

1. Department of Public and International Law, Faculty of Divinity, Political Science and Law, Science and Research Branch, Islamic Aazad University, Tehran, Iran.
2. Department of International Law, Islamic Azad University of Central Tehran branch, Tehran, Iran
3. Department of Public and International Law, Faculty of Law and Political Sciences, Allameh Tabataba'i University, Tehran, Iran.

ABSTRACT

Background and Aim: Cyber terrorism as a potential danger threatens all governmtnts all over the world and its characteristics create serious violations of international peace, security and human rights. On the other hand, its different committement from classic terrorism has established fundamental challenges in the field of jurisdiction, crime detection, extradition and punishment of the perpetrators. Therefore, a phenomenon that has a cross-border nature cannot be fought and suppressed by national measures and requires organized cooperation with the serious efforts of subjects of international law. These cooperations have wide dimensions, the first and most important aspect of which is the effort to establish rules in the fight against cyber terrorism.

Method: The research method in this article is descriptive-analytical and the method of collecting information is library-based, referring to documents, books and articles. First, the parctices of some leading institutions in the field of policy-making in the fight against cyber terrorism will be studied in a descriptive manner and then with an analytical method, criteria for future effective measures will be presented from these actions and practices.

Ethical Considerations: In this research, the principles of trustworthiness, honesty, neutrality and originality of the work have been observed.

Results: Due to the problem of terrorism in all its types, the ease of committing cyber attacks, creating terror and its severe consequences compared to classical terrorism, organizations ranging from the United Nations to regional organizations, groups and the subgroups have take several measures in their agenda in order to realize effective and diligent cooperation among their members, from criminalization to detection, extradition and punishment of criminals. In international efficiency analysis conducted by international organizations, factors such as the status of rules with preventive features and criminalization and implementation of rules by international cooperations and coordination should be taken into consideration.

Conclusion: According to the study conducted on the procedure of international and regional organizations in fulfilling the commitment of governments to cooperate in establishing rules in response to cyber terrorism, it is noteworthy that regional organizations with a security approach such as NATO have had significant success compared to the United Nations.

Keywords: Cyber Terrorism; International Cooperation; United Nations Organazation; International Organizations; State Obligation

Corresponding Author: Sadegh Salimi; **Email:** sadegsalimi@yahoo.com

Received: June 25, 2023; **Accepted:** August 28, 2023; **Published Online:** December 03, 2023

Please cite this article as:

Mirbod L, Salami S, Niavarani S, Zamani SGH. The Dimensions of States Obligation to Cooperation in Establishing Rules in Response to Cyber Terrorism. Medical Law Journal. 2022; 16(Special Issue on Legal Developments): e33.

© Copyright (2022) Iranian Association of Medical law, Tehran, Iran.

دسترسی آزاد | مقاله پژوهشی

مجله حقوق پزشکی

دوره شانزدهم، ویژه‌نامه تحولات حقوقی، ۱۴۰۱

Journal Homepage: http://ijmedicallaw.ir

ابعاد تعهد دولت‌ها به همکاری در وضع قواعد در واکنش به تروریسم سایبری

لیلا میربد[۱]، صادق سلیمی[۲*]، صابر نیاورانی[۱]، سیدقاسم زمانی[۳]

۱. گروه حقوق عمومی و بین‌الملل، دانشکده حقوق، الهیات و علوم سیاسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.

۲. گروه حقوق بین‌الملل، دانشکده حقوق، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران.

۳. گروه حقوق عمومی و بین‌الملل، دانشکده حقوق و علوم و سیاسی، دانشگاه علامه طباطبایی، تهران، ایران.

چکیده

زمینه و هدف: تروریسم سایبری به عنوان یک خطر بالقوه تمامی کشورهای جهان را تهدید می‌کند و با ویژگی‌هایی که دارد ناقض جدی صلح، امنیت بین‌المللی و حقوق بشر است. از سوی دیگر شیوه ارتکاب آن با جرائم تروریستی کلاسیک، چالش‌های اساسی در حوزه صلاحیت، کشف جرم، استرداد و مجازات عاملان ایجاد نموده است، لذا پدیده‌ای که ماهیت فرامرزی دارد با اقدامات ملی قابل مبارزه و سرکوب نیست و نیاز به همکاری‌های سازمان یافته با عزم جدی تابعان حقوق بین‌الملل دارد. این همکاری‌ها ابعاد گسترده‌ای دارد که اولین و مهم‌ترین بعد آن تلاش در راستای وضع قواعد در راستای مبارزه با تروریسم سایبری است.

روش: روش پژوهش در این مقاله توصیفی ـ تحلیلی است و روش جمع‌آوری اطلاعات به صورت کتابخانه‌ای است و با مراجعه به اسناد، کتب و مقالات صورت گرفته است. ابتدا به شیوه توصیفی عملکرد برخی نهادهای شاخص در حوزه سیاستگذاری در مبارزه با تروریسم سایبری بررسی و سپس با شیوه تحلیلی، از این اقدامات و عملکردها ملاکی برای اقدامات مؤثر آتی ارائه خواهد شد.

ملاحظات اخلاقی: در تحقیق حاضر، اصل امانتداری، صداقت، بی‌طرفی و اصالت اثر رعایت شده است.

یافته‌ها: با توجه به مبتلابه‌بودن مسأله تروریسم در تمامی انواع آن، سهولت ارتکاب حملات سایبری، ایجاد رعب و وحشت و نیز عواقب بسیار شدید آن نسبت به تروریسم فیزیکی، سازمان‌ها اعم از سازمان ملل تا سازمان‌های منطقه‌ای، گروه‌ها و زیرگروه‌ها، اقدامات متعددی را در راستای تحقق همکاری‌های مؤثر و مجدانه میان اعضای خود از جرم‌انگاری گرفته تا کشف، استرداد تا مجازات مجرمین، در دستور کار خود قرار داده‌اند. در حوزه تحلیل میزان کارآمدی اقدامات صورت‌گرفته توسط سازمان‌های بین‌المللی، باید فاکتورهایی چون اقدامات در حوزه وضع قواعد با رویکرد پیشگیرانه و جرم‌انگاری و در نیز اجرای قواعد با همکاری و هماهنگی بین‌المللی را مد نظر قرار داد.

نتیجه‌گیری: با توجه به مطالعه صورت‌گرفته در رویه سازمان‌های بین‌المللی و منطقه‌ای در تحقق تعهد دولت‌ها به همکاری در وضع قواعد در واکنش به تروریسم سایبری، این نکته قابل ملاحظه است که سازمان‌های منطقه‌ای با رویکرد امنیتی مانند ناتو توفیق قابل ملاحظه‌تری نسبت به سازمان ملل متحد داشته‌اند.

واژگان کلیدی: تروریسم سایبری؛ همکاری بین‌المللی؛ سازمان ملل؛ سازمان‌های بین‌المللی؛ تعهد دولت

نویسنده مسئول: صادق سلیمی؛ **پست الکترونیک:** sadegsalimi@yahoo.com

تاریخ دریافت: ۱۴۰۲/۰۴/۰۴؛ **تاریخ پذیرش:** ۱۴۰۲/۰۶/۰۶؛ **تاریخ انتشار:** ۱۴۰۲/۰۹/۱۲

خواهشمند است این مقاله به روش زیر مورد استناد قرار گیرد:

Mirbod L, Salami S, Niavarani S, Zamani SGH. The Dimensions of States Obligation to Cooperation in Establishing Rules in Response to Cyber Terrorism. Medical Law Journal. 2022; 16(Special Issue on Legal Developments): e33.

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

مقدمه

اصول و سازوکارهای اساسی در زمینه مقابله جهانی با تروریسم سایبری، بر پایه اصول حقوقی مشترک و مرتبط با هدف تسهیل همکاری‌های بین‌المللی ایجاد می‌شود. این اصول، کمک‌های حقوقی متقابل، کشف جرم، تعقیب مجرمان، استرداد، انتقال زندانیان و همکاری‌های بین‌المللی را راهبری می‌کند. ترتیبات منطقه‌ای و بین‌المللی برای مبارزه با تروریسم به ویژه تروریسم سایبری به سرعت در حال تحول هستند، تا با فناوری‌های جدید همگام شوند. برای اینکه این اصول و مکانیسم‌ها در عمل مؤثر باشند، مهم است که آن‌ها به طور کامل در سیستم‌های حقوقی ملی گنجانیده و به مرحله اجرا درآیند. درک اهمیت همکاری‌های بین‌المللی و نیز تسهیل فعالیت نهادهای داخلی برای تقویت تعاملات بین‌المللی در راستای پیشگیری و مقابله با جرائم سایبری، نیاز به پایش کلیه تحولات در حوزه‌های امنیت و جرائم سایبری با همکاری و حضور در نشست‌های تخصصی در جهت یافتن راه حل‌های مشترک دارد. راهبرد سازمان ملل در سال ۲۰۰۲ راهبردی با سه هدف را پیشنهاد می‌دهد: بحث و بررسی (پیشگیری و بازداشتن گروه‌های ناراضی از پذیرش تروریسم)، رد (انکار گروه‌هایی که ابزار اعمال تروریستی می‌باشند) و همکاری (حمایت از همکاری‌های بین‌المللی گسترده در مبارزه با تروریسم). گذشته از همکاری‌های بین‌المللی آنچه در اجرای مندرجات اسناد بین‌المللی و منطقه‌ای مهم می‌نماید، هماهنگی اقدامات اجرای دولت‌ها در ظرفیت‌سازی دستگاه عدالت و نیز همسان‌سازی قوانین ملی، با توجه به ویژگی‌ها و ماهیت تروریسم سایبری به مثابه یک جرم سازمان‌یافته فراملی است. در نبود وفاقی عام در تعریف تروریسم و به تبع آن تروریسم سایبری، بنابراین باید از کنوانسیون‌های موجود در زمینه جرائم سایبری و تروریسم بهره گرفته شود تا همکاری بین‌المللی تسهیل شود، اما برای مقابله با این نوع تهدید جهانی، عامل کلیدی، توافق بر سر یک تعریف مشترک از تهدید تروریسم سایبری است. با وجود اینکه ممکن است رسیدن به یک توافق جهانی غیر محتمل به نظر برسد نمونه‌های بسیاری از همکاری‌های بین‌المللی هم‌اکنون در حال اجرا است. کنترل ترافیک هوایی نمونه‌ای از توافقات امنیتی جهانی است. علاوه بر این به عنوان یک تهدید قریب‌الوقوع در تبدیل تروریسم سایبری به جنگ سایبری، شورای امنیت سازمان ملل نیز باید بر تهدید تروریسم سایبری متمرکز شود. بسیاری از اعضای دائم این شورا آسیب‌پذیرترین کشورها در جهان نیز هستند. این کشورها همچنین مبدأ بسیاری از حملات سایبری بین‌المللی هستند. بنابراین تصمیمات قانونی برای مقابله با تروریسم سایبری در درجه اول، توسط سازمان ملل قابل اتخاذ است. در این راستا مبارزه با تروریسم، پس از حوادث ۱۱ سپتامبر به صورت جدی و عملی‌تری دنبال گردید، تشکیل کمیته ضد تروریسم (CTC) با هدف تهیه یک کنوانسیون جامع در رابطه با تروریسم بین‌الملل به عنوان یک چارچوب قانونی جامع بر اساس قطعنامه ۱۳۷۳ شورای امنیت و تعهد همکاری دول عضو در زمینه‌های اطلاعاتی، تعقیب و مجازات تروریست‌ها و تصویب کنوانسیون‌های بین‌المللی از دستاوردهای مثبت این قطعنامه است.

از آنجایی که طبیعت تهدید سایبری جهانی است، سازمانی که به این تهدید واکنش نشان می‌دهد باید جامع و جهانی باشد، اما به نظر می‌رسد سازمان‌های منطقه‌ای قدرتمند که از نظر فنی و قانونی توان همه‌جانبه‌ای برای مبارزه با انواع تروریسم دارند، در واکنش به این تهدید که موضوع مبتلابه امروز جامعه جهانی است، بسیار موفق‌تر عمل کرده‌اند. در مبارزه همه‌جانبه با تروریسم، تبادل اطلاعات، پیشگیری، محاکمه و استرداد، مساعدت حقوقی متقابل، اجرای قانون و ظرفیت‌سازی نیازمند همکاری‌ها و هماهنگی‌های مؤثر است. سازمان‌های منطقه‌ای و زیرمنطقه‌ای نیز همکاری مناسبی در جهت ساخت یا تقویت مراکز و سازوکارهای ضد تروریسم همگام با فناوری‌های نوین را در دستور کار خود قرار داده‌اند. سرمایه‌گذاری‌های بسیاری برای اقدامات پیشگیرانه از مصادیق تروریستی سنتی شده است، اما کشورهای توسعه‌یافته در برابر حملات تروریستی به شبکه‌های رایانه‌ای که برای امنیت اقتصادی و ملی حیاتی هستند، آسیب‌پذیرند. پیچیدگی روزافزون و به هم‌پیوستگی این سیستم‌های زیرساختی و وابستگی آن‌ها به رایانه‌ها، نه‌تنها

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

آن‌ها را در برابر حملات آسیب‌پذیرترند، بلکه همچنین دامنه بالقوه اثرات یک حمله را نیز افزایش می‌دهند. این ترس، دولت‌ها را بر آن داشته تا منابع قابل توجهی را برای محافظت از زیرساخت‌های ملی حیاتی تزریق کنند. برای محافظت از منافع حیاتی خود، بسیاری از کشورهای وابسته به فناوری بر سازمان‌دهی سیاست‌های امنیت سایبری خود متمرکز شده‌اند. برخی نیز از تصمیمات نظامی و قانونی را اتخاذ کرده‌اند، اما بدون همکاری بین‌المللی، این تصمیمات ملی برای مقابله با تروریسم سایبری ناکافی هستند. مشارکت منطقه‌ای نیز امنیت سایبری کافی را فراهم نمی‌کند، چراکه حملات سایبری می‌توانند از کشورهای خارج از منطقه یا خارج از کشورهای مشارکت‌کننده نشأت بگیرند. برای فراهم‌کردن یک همکاری بین‌المللی گسترده، اصطلاح «تروریسم سایبری» بایستی به صورت دقیق تعریف شود و اقداماتی که فعالیت تروریستی محسوب می‌شوند، باید در گام اول معین گردد. بعد از آن، توسعه همکاری‌های نظامی و قانونی باید مورد بحث قرار بگیرند. در این اثنا نباید فراموش کرده که مهم‌ترین هدف این همکاری‌ها حفظ صلح و امنیت بین‌المللی است.

مهم‌ترین پرسش در این حوزه این است که با در نظرگرفتن روند شکل‌گیری همکاری‌های بین‌المللی، این همکاری‌ها در چه محورهایی صورت گرفته و تا چه میزانی مؤثر بوده و چه چالش‌ها و موانعی بر سر راه نیل به هماهنگی‌های بین‌المللی در مبارزه با تروریسم سایبری وجود دارد؟ به نظر می‌رسد در سیاق مبارزه با تروریسم سایبری از آنجایی که دولت‌ها همچنان تمایل به رسیدگی به این جرم تحت صلاحیت دولت متبوع خود دارند، سازمان عام‌الشمولی چون سازمان ملل با تصمیمات الزام‌آور، قطعنامه‌ها، دفاتر تخصصی، کمیته‌ها و کارگروه‌ها بتواند مرکزی برای جلب همکاری‌های بین‌المللی در این حوزه باشد. در این مقاله با روش توصیفی ـ تحلیلی هدف آن است تا با تحلیل عملکرد سازمان‌های بین‌المللی، تصویری روشن از حوزه‌های همکاری بین‌المللی ارائه نمود تا میزان تأثیر آن‌ها را سنجیده و بتوان راهکارهای عملی و علمی بر پایه میزان توفیق اقدامات صورت‌گرفته، پیشنهاد داد. باید تأکید کرد که مهم‌ترین هدف از همکاری‌های بین‌المللی در مسأله دفاع سایبری و منع تروریسم سایبری، حفظ صلح و امنیت بین‌المللی است. محوریت مباحث امنیت، به زیرساخت‌های حیاتی ارتباط دارند، لذا سازمان‌های دولتی و بخش خصوصی باید توانمندی‌های امنیت سایبری را کسب کنند و این توانمندی در شکل دفاع سایبری جهانی تنها از طریق همکاری بین‌المللی میان دولت‌ها قابل حصول است. موضوعی که هرگز به طور مستقل موضوع مقاله علمی ـ پژوهشی نبوده است.

اما به عنوان پیشینه پژوهش می‌توان به موارد زیر اشاره نمود:

علیرضا دلخوش در کتاب مقابله با جرائم بین‌المللی: تعهد دولت‌ها به همکاری، چاپ ۱۳۹۰، ضمن بررسی ابعاد تعهدات دولت‌ها به همکاری در مبارزه با جرائم بین‌المللی، این مهم را در اسناد بین‌المللی و به ویژه در حوزه حقوق کیفری بررسی نموده و سازوکارهای اجرایی تعهدات دولت‌ها در حقوق بین‌المللی کیفری را تحلیل نموده است.

در گزارش مرکز عالی دفاع سایبری ناتو در سال ۲۰۱۸ عنوان شده: دستورالعمل‌های سیاست ضد تروریسم ناتو بر روی سه زمینه اصلی آگاهی، تعامل برای ایجاد تغییرات سریع و متناسب با تهدیدات سایبری و نیز حفظ دفاع قدرتمند سایبری، متمرکز است. افزایش همکاری‌های ناتو با دولت‌های عضو و نیز بخش‌های خصوصی و دانشگاهی، شامل به اشتراک گذاشتن اطلاعات و تبادل تجربیات برای جلوگیری و کاهش‌دادن حملات سایبری است.

در گزارش هیأت عالی‌رتبه در مورد برنامه جهانی امنیت سایبری که در سال ۲۰۰۸ توسط اتحادیه جهانی مخابرات تهیه شده است و سپس در سال ۲۰۱۷ نیز به روزرسانی شده، اقدامات اتخاذشده در این حوزه توسط ارکان سازمان ملل متحد و سایر سازمان‌های بین‌المللی بررسی شده و اقدامات حقوقی، فنی و اطلاعاتی و ظرفیت‌سازی و همکاری‌های بین‌المللی به بحث گذاشته شده است.

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

روش

روش پژوهش در این مقاله توصیفی ـ تحلیلی است و روش جمع‌آوری اطلاعات به صورت کتابخانه‌ای است و با مراجعه به اسناد، کتب و مقالات صورت گرفته است. ابتدا به شیوه توصیفی عملکرد برخی نهادهای شاخص در حوزه سیاستگذاری در مبارزه با تروریسم سایبری بررسی و سپس با شیوه تحلیلی، از این اقدامات و عملکردها ملاکی برای اقدامات مؤثر آتی ارائه خواهد شد.

یافته‌ها

با توجه به مبتلابه‌بودن مسأله تروریسم در تمامی انواع آن، سهولت ارتکاب حملات سایبری، ایجاد رعب و وحشت و نیز عواقب بسیار شدید آن نسبت به تروریسم فیزیکی، سازمان‌ها اعم از سازمان ملل تا سازمان‌های منطقه‌ای، گروه‌ها و زیرگروه‌ها، اقدامات متعددی را در راستای تحقق همکاری‌های مؤثر و مجدانه میان اعضای خود از جرم‌انگاری گرفته تا کشف، استرداد تا مجازات مجرمین، در دستور کار خود قرار داده‌اند. در حوزه تحلیل میزان کارآمدی اقدامات صورت‌گرفته توسط سازمان‌های بین‌المللی، باید فاکتورهایی چون اقدامات در حوزه وضع قواعد با رویکرد پیشگیرانه و جرم‌انگاری و در نیز اجرای قواعد با همکاری و هماهنگی بین‌المللی را مد نظر قرار داد. یافته های این پژوهش حاکی از آن است که، فعالیت‌های سازمان ملل متحد به عنوان مهم ترین و عام الشمول ترین سازمان بین المللی، در مورد امنیت سایبری بسیار پراکنده به نظر می‌رسد، همکاری‌های بین‌المللی در این راستا باید از همکاری در وضع قواعد ضد تروریسم سایبری آغاز و به همکاری در اجرای قانون و تلاش برای هماهنگی اقدامات ملی با تعهدات بین‌المللی ختم می‌شود. قانونگذار نیز در حوزه قانونگذاری ملی نیز باید عدم نقض حقوق بشر و آزادی‌های بنیادین را همزمان با مبارزه با تروریسم سایبری تضمین نماید.

بحث

۱. مبانی و مفاهیم: در ابتدای بحث جهت تنویر موضوع، لازم است مفهوم تروریسم سایبری که البته تعریف مورد اجماعی در مورد آن وجود ندارد و نیز مبنای تعهد دولت‌ها به لزوم همکاری در سرکوب آن را مورد مداقه قرار دهیم.

۱-۱. تروریسم سایبری: تعاریف متعددی با تکیه بر عناصر تشکیل‌دهنده تروریسم سایبری، هدف، وسیله انجام یا عاملان آن ارائه شده است. قاعده شماره ۳۶ از دستورالعمل تالین، مرکز حمایت از زیرساخت‌های ملی آمریکا، ماده ۱ طرح کنوانسیون بین‌المللی برای افزایش حمایت در برابر تروریسم و جرم سایبری، پلیس فدرال آمریکا، بری کلین (Barry Klein) محقق ارشد مؤسسه حفاظت اطلاعات و مبدع اصطلاح تروریسم سایبری، این جرم را به انواع مختلفی تعریف کرده‌اند، اما برآیند همه این تعارف می‌تواند این تعریف باشد: اعمال خشونت یا تهدید به آن توسط عوامل دولتی، غیر دولتی یا سازمان‌های مجرمانه در حمله به زیرساخت‌های حیاتی یک کشور با تخریب، ممانعت یا اختلال داده‌ها یا سیستم، شبکه یا مؤلفه اطلاعاتی رایانه‌ای با ایراد صدمه و خسارت فیزیکی یا اطلاعاتی به اموال و اشخاص و رعب و وحشت در میان غیر نظامیان، جهت تحت فشار قراردادن دولت یا سازمان دولتی در جهت انگیزه‌های سیاسی، ایدئولوژیک یا اجتماعی.

بنابراین به طور خلاصه می‌توان ویژگی‌های فضای سایبر را برای اعمال تروریسم سایبری این‌گونه بر شمرد:

ـ امکان انجام اقدامات تروریستی با کمترین هزینه، تلفات، خسارت و بدون نیاز به سلاح خاص.

ـ گمنام‌بودن و مخفی‌بودن عملیات تروریستی ناهنجارمند و کنترل‌ناپذیربودن فضای سایبر و کمتربودن احتمال کشف عملیات و دستگیری.

ـ جهانی بودن و امکان انجام عملیات در کسری از ثانیه با ایجاد خسارات شدید.

ـ ایراد خسارات بسیار شدیدتر از تروریسم سنتی با اهداف غیر قابل شمار.

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

ـ قدرت انتخاب و اختیارات بیشتر در انجام، محل و زمان حملات.

ـ امکام استفاده از ابزارهای مختلف برای انجام اقدامات تروریستی، از جمله استفاده از بدافزارها، تروژان‌ها، ویروس‌ها و کرم‌های اینترنتی (۱).

بنا بر آنچه گفته شد، این جنایت با توجه به ابعاد و پیچیدگی‌های ارتکاب آن از حوزه اختیارات یک دولت در مبارزه و جرم‌انگاری فراتر رفته و نیاز به همکاری دولت‌ها در ریشه‌کنی آن دارد.

۱-۲. مبنای تعهد به همکاری بین‌المللی: باید در ابتدا تبیین نمود که مهم‌ترین مبنای عمل در همکاری‌های بین‌المللی در مسأله دفاع سایبری و منع تروریسم سایبری، حفظ نظم، صلح و امنیت بین‌المللی است. این تعهد در حقوق بین‌الملل عام به شکل تعهدات معاهداتی و تعهدات عرفی، عینیت می‌یابند. کنوانسیون‌هایی که در خصوص مبارزه با تروریسم شکل گرفته‌اند، در نبود یک کنوانسیون جامع در حوزه تروریسم سایبری و لزوم تعهد دولت‌ها به همکاری در راستای تعهدات سازمانی، مهم‌ترین مبانی تعهد دولت‌ها در همکاری‌های بین‌المللی است. در مبارزه همه‌جانبه با تروریسم، تبادل اطلاعات، پیشگیری، محاکمه و استرداد، مساعدت حقوقی متقابل، اجرای قانون و ظرفیت‌سازی نیازمند همکاری‌ها و هماهنگی‌های مؤثر است. سازمان‌های منطقه‌ای و زیرمنطقه‌ای نیز همکاری مناسبی در جهت ساخت یا تقویت مراکز و سازوکارهای ضد تروریسم همگام با فناوری‌های نوین را در دستور کار خود قرار داده‌اند.

حمله‌ای که از مرزهای کشورها عبور کرده، مفهوم سرزمین، حاکمیت و صلاحیت را درمی‌نوردد، برای مبارزه نیز نیاز به تلاش‌های فرامرزی دارد. محوریت مباحث امنیت، به زیرساخت‌های حیاتی ارتباط دارند. سازمان‌های بخش خصوصی و دولتی باید توانمندی‌های امنیت سایبری را کسب کنند، این توانمندی در شکل دفاع سایبری جهانی تنها از طریق همکاری بین‌المللی میان دولت‌ها قابل حصول است.

روند شکل‌گیری همکاری‌های بین‌المللی که بدان پرداخته خواهد شد، از تدوین عرف در مبارزه با تروریسم گرفته تا تلاش برای همکاری‌ها در قالب ارکان سازمان ملل و قطعنامه‌های شورای امنیت، نهادهای بین‌المللی و نیز کنوانسیون‌های بین‌المللی، متنوع است. تشکیل مراکزی چون مرکز دفاع سایبری سازمان پیمان آتلانتیک شمالی و زیرمجموعه‌ای موسوم به گروه لیون در گروه جی ۷ در همین راستا بوده است. شاخص امنیت سایبری جهانی (GCI) بر اساس پنج محور اصلی ساخته شده است که نشان‌دهنده اقدامات کلیدی در امنیت سایبری است و عبارت است از: حقوقی، فنی، سازمانی، همکاری، ظرفیت‌سازی، در همکاری بین‌المللی نیاز است میزان تحقق این شاخص‌ها سنجیده و برآورد شود (۲) و این همکاری‌ها باید در راستای جرم‌انگاری و وضع قواعد و مقررات، اجرای قانون در پیشگیری و بازدارندگی، دفاع سایبری و معاضدت قضایی و تبادل اطلاعات صورت گیرد.

۲. روند شکل‌گیری همکاری‌های بین‌المللی: شکل‌گیری همکاری در راستای مبارزه با تروریسم سایبری از تدوین عرف در مبارزه با تروریسم گرفته تا تلاش برای همکاری‌ها در قالب ارکان سازمان ملل، نهادهای بین‌المللی و نیز کنوانسیون‌های بین‌المللی نمود می‌یابد. گذاشته از اقدامات سازمان ملل در تصویب قطعنامه ۱۳۶۸ و ۱۳۷۳ و تشکیل کارگروه ویژه اجرایی مبارزه با تروریسم، سازمان‌های دیگری نیز در تشکیل این روند مؤثر بوده‌اند. استراتژی جهانی مبارزه با تروریسم، می‌تواند عامل هماهنگی مؤثری در اقدامات دولت‌ها و سازمان‌های بین‌المللی باشد.

حوادث ۱۱ سپتامبر، منجر گردید تا اختلافات دولت‌ها در مورد تعیین دامنه شمول تروریسم و اقدامات پیشگیرانه و قضایی علیه آن کم‌رنگ شده و اساساً روند مبارزه با تروریسم به سمت عرفی‌شدن حرکت نماید. به همین دلیل نیز قطعنامه ۱۳۶۸ مورخ ۱۲ سپتامبر ۲۰۰۱ شورای امنیت، مبارزه با تروریسم را تعهد کلیه کشورها دانسته است. ممنوعیت تروریسم برگرفته از حقوق بین‌الملل عرفی می‌باشد. آنچه در

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

معاهدات مربوط به مبارزه با تروریسم اهمیت دارد، تلاش برای هماهنگی در تعقیب و مجازات تروریست‌ها توسط دول متعاهد است. این دولت‌ها ملزم به همکاری و مساعدت در مبارزه با تروریسم بوده که این همکاری شامل، پیشگیری، دستگیری، تعقیب، محاکمه، استرداد و مجازات متهمان به تروریسم می‌باشد (۳).

قطعنامه ۱۳۷۳ شورای امنیت سازمان ملل متحد از آنجایی که در قالب فصل ۷ به تصویب رسیده، برای کلیه دول عضو سازمان ملل متحد الزام‌آور بوده و به مجموعه قوانین مبارزه با تروریسم مشهور شده است. ابتکار این قطعنامه ایجاد یک سیستم منظم گزارش‌دهی بر اساس تشکیل کمیته ضد تروریسمی است که اجرای این قطعنامه را توسط دول عضو کنترل می‌نماید. دولت‌ها ملزم به ارائه گزارش در مورد اقدامات ضد تروریستی خود بر اساس جدول زمان‌بندی و حداکثر ۹۰ روز پس از تصویب قطعنامه می‌باشند. قطعنامه‌های دیگری از جمله ۱۵۴۰ مصوب ۲۰۰۵ و ۱۷۳۵ مصوب ۲۰۰۶ به انضمام کنوانسیون‌های بین‌المللی مربوط به تروریسم، چارچوبی حقوقی برای مبارزه با تروریسم به دست می‌دهد که باید به گونه‌ای اجرا شوند که با مندرجات اسناد حقوق بشری در تعارض نباشند. الزمات ناشی از این اسناد عبارتند از: جرم‌انگاری تأمین منابع مالی تروریسم، استرداد، پرهیز از حمایت از افراد و سازمان‌های تروریستی، ممانعت از فعالیت‌های تروریستی و جرم‌انگاری کلیه فعالیت‌های تروریستی. شورای امنیت سازمان ملل با تصویب این کنوانسیون تکالیف قراردادی ناشی از کنوانسیون‌ها و سایر اسناد سازمان ملل را به تکالیف سازمانی مبدل کرده است (۴).

رابطه بین قطعنامه و کنوانسیون‌های ضد تروریسم به عنوان یک مبنای شکل‌گیری حقوق بین‌الملل عرفی تمرکز دارد. تشکیل کمیته هم در راستای بند ۶ قطعنامه ناظر بر همین مسأله است. از آنجایی که این قطعنامه به موجب فصل ۷ است، تروریسم به طور آشکار تهدید علیه صلح و امنیت بین‌المللی در نظر گرفته شده است (۵).

ایجاد کارگروه ویژه اجرایی مبارزه با تروریسم (مبارزه با استفاده از اینترنت برای اهداف تروریستی) یکی از ۹ گروه کاری ملل متحد با هدف فراهم‌نمودن چارچوبی متمرکز، منسجم و مشترک علیه تروریسم، برای نهادهای سیستم ملل متحد می‌باشد. کارگروه در تلاش برای ایجاد اسناد (قوانین و کنوانسیون‌ها)، برنامه‌ها، منابع اختصاص داده‌شده برای مبارزه با استفاده از اینترنت برای اعمال تروریستی است. داده‌های ارائه‌شده توسط این کارگروه در سطح بین‌المللی، منطقه‌ای و ملی بوده و با همکاری صنایع مربوطه، جوامع مدنی و دانشگاهی انجام گرفته است. بر اساس این اطلاعات، کارگروه در پی تدوین نقشه راه شناسایی حوزه‌هایی است که در آینده ممکن است با مسائل مطروحه درگیر باشند، می‌باشد.

یکی از نمونه‌های اخیر مشارکت بین‌المللی چندجانبه علیه تهدیدات سایبری با هدف ارائه ابتکار عمل‌هایی در مورد مبارزه با تروریسم سایبری، از جمله ایجاد یک فروم جهانی برای دولت‌ها و صنعت، توانایی واکنش سریع بین‌المللی، آموزش امنیت سایبری و تست امنیت و صدور گواهینامه، بوده است. مباحث مربوط به امنیت سایبری در شرایط عادی به مباحث مرتبط با تهدیدهای تروریستی و به قطعنامه‌های شورای امنیت در این زمینه ارجاع داده می‌شود. موضوع با تلاش کمیته ضد تروریسم پوشش داده شده و در استراتژی بین‌المللی سازمان ملل علیه تروریسم قرار می‌گیرد. گذشته از سیستم عام‌الشمول سازمان ملل متحد، همگرایی اعضای جامعه جهانی به طور مثال در اقدامات سازمان‌های بین‌المللی چون ناتو امروزه نمود یافته است. اقدامات ناتو در این‌باره در موضوعاتی چون کشف جرم، دفاع و بهبود مقابله با حملات تروریستی، تسهیل همکاری‌ها و تسهیم اطلاعات و توانایی‌های ملی برای اتخاذ یک سیاست هماهنگ میان کشورهای عضو است که شامل مراحل اجرایی جهت اتخاذ تدابیر جهانی با این پدیده نیز می‌باشد. مرکز دفاع سایبری سازمان پیمان آتلانتیک شمالی (ناتو) در تالین استونی، یک مرکز پژوهشی است که هدف آن ارائه مشاوره تخصصی در امور امنیتی به اعضای سازمان است. سازمان‌های دیگری مانند انجمن ملل آسیای جنوب شرقی (ASEAN)، سازمان کشورهای آمریکایی (OAS) و سازمان همکاری شانگهای (SCO) همکاری بین اعضای خود ارتقا بخشیده‌اند (۶).

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

نمونه دیگر گروه جی ۷ است که زیرمجموعه‌ای موسوم به گروه لیون در سال ۱۹۹۶ برای مبارزه با جرائم سازمان‌یافته بین‌المللی ایجاد نموده است. هدف ارتقای توانایی کشورهای گروه هشت برای حفاظت، تحقیق و تعقیب جرائم ارتکابی، استفاده از کامپیوترها، شبکه ارتباطات و دیگر تکنولوژی‌های جدید بود. مدیریت زیرمجموعه، متعاقباً گسترش یافت تا استفاده از اینترنت توسط تروریست‌ها و حفاظت از زیرساخت اطلاعات ضروری را شامل گردید. این مجموعه در تلاش است تا اصولی را ایجاد کند که نه‌تنها برای کشورهای عضو جی ۷، که برای سایر کشورها نیز قابل اجرا باشد. در این راستا مستنداتی از فعالیت‌های گروه پیرامون رهنمودهایی برای ارزیابی تهدیدات سایبری و امنیت شبکه منتشر شده است (۷).

نهایتاً باید گفت در راستای همکاری‌های بین‌المللی و منطقه‌ای در واکنش به تروریسم سایبری کشورهای عضو باید، طبق استراتژی جهانی مبارزه با تروریسم، اقدامات فوری را برای جلوگیری و مبارزه با تروریسم در همه اشکال و مظاهر آن انجام دهند. مهم‌ترین این اقدامات عبارتند از: ۱ـ عضویت بدون تأخیر در کنوانسیون‌ها و پروتکل‌های بین‌المللی موجود علیه تروریسم و اجرای آن‌ها و تلاش برای دستیابی به توافق جهت کنوانسیون جامع تروریسم بین‌المللی؛ ۲ـ اجرای کلیه قطعنامه‌های مجمع عمومی جهت از بین‌بردن تروریسم بین‌المللی و قطعنامه‌های مربوط به مجمع عمومی در مورد حمایت از حقوق بشر و آزادی‌های اساسی ضمن مقابله با تروریسم؛ ۳ـ اجرای کلیه مصوبات شورای امنیت در رابطه با تروریسم بین‌المللی و همکاری کامل با ارگان‌های فرعی ضد تروریسم شورای امنیت در انجام وظایف آن‌ها (۸).

بنابراین باید ابتدا به ابعاد تعهدات دولت‌ها در راستای همکاری در راستای تحقق امنیت سایبری و مبارزه با تروریسم سایبری و سپس به تحلیل میزان کارآمدی این همکاری‌ها و چالش‌های آن پرداخت.

۳. ابعاد تعهد دولت‌ها به همکاری: از آنجایی که تروریسم سایبری یک جرم بین‌المللی است، مقررات ملی به تنهایی قادر به دفاع و واکنش به چنین حملاتی نیستند، برای دستیابی به یک درک مشترک در زمینه مقابله با تهدیدهای تروریسم سایبری، ابتدا باید راه حل‌های ارائه‌شده توسط معاهدات بین‌المللی حاضر در نظر گرفته شود تا به پاسخ‌های موجود در برابر تهدیدات سایبری بین‌المللی بپردازیم. تروریسم سایبری نیاز به واکنش فراملی دارد. بنابراین یک کشور مورد حمله، ممکن است از طریق اعمال صلاحیت جهانی، از حقوق بین‌الملل برای اعمال عدالت در مورد هرگونه خسارت وارده، استفاده کند. از سوی دیگر بدون کمک سازمان‌های بین‌المللی، جلوگیری از تروریسم سایبری دشوار است. حملات تروریسم سایبری به دلیل کمبود یک پیمان بین‌المللی جامع و عدم عزم بین‌المللی به یک مسأله مهم تبدیل شده است و افزایش حملات سایبری علیه کشورها و زیرساخت‌های مهم اطلاعاتی‌شان رو به فزونی بوده و نیاز به یک واکنش جهانی دارد. موافقت‌نامه‌های منطقه‌ای، دوجانبه و قوانین محلی برای جلوگیری از حملات سایبری کافی نیست. بنابراین حقوق بین‌الملل ابزاری ضروری است تا جامعه جهانی بتواند از تهدیدات سایبری در حوزه‌های صلاحیت خود جلوگیری کند؛ نکته دوم اینکه، اگرچه دولت‌ها باید برای مقابله با سوءاستفاده از فناوری‌های جدید، سازوکارهای قانونی و نیز نظارتی را خود را تقویت کنند، اما این سازوکارها باید با توافق‌های بین‌المللی مناسب حمایت شوند. در صورت تصویب تعداد زیادی از کشورها، سازمان‌های منطقه‌ای ممکن است به عنوان سازمان‌های چندجانبه عمل کنند. نمونه آن کنوانسیون شورای اروپا در مورد جرائم سایبری است که توسط بسیاری از کشورها (حتی بیشتر از اتحادیه اروپا) تصویب شده و در حال حاضر به تنها پیمان بین‌المللی علیه جرائم سایبری تبدیل شده است.

معاهدات قابل ملاحظه‌ای در مورد تروریسم مورد تصویب قرار گرفته اند و از آن جا که تروریسم سایبری بخشی از تروریسم کلاسیک می‌باشد، چنین معاهداتی ممکن است تروریسم سایبری را نیز تحت پوشش قرار دهد. علاوه بر این، سهولت اختفای منشأ حملات سایبری و این واقعیت که حملات

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

سایبری به یک کشور می‌تواند از هر کجای کره زمین اتفاق بیفتد، بدان معنی است که جرائم سایبری و تروریسم سایبر واقعاً تهدیدهای بین‌المللی هستند. طی سال‌های اخیر، آمارها نشان می‌دهد که همکاری چندجانبه، مؤثرترین روش برای پاسخ به تروریسم سایبری فراملی است. ضرورت چنین همکاری به خاطر این واقعیت به ذهن متبادر می‌شود که کشورها برای قواعد مربوط به استرداد و کمک‌های حقوقی برای کنترل جرائم سایبری قوانین مختلفی دارند. بنابراین مؤثرترین شکل همکاری بین‌المللی برای پاسخ به حملات سایبری، ماهیت چندجانبه دارد. لازم به توضیح است حقوق معاهدات و سازمان‌های بین‌المللی مبنایی قانونی برای اعمال صلاحیت جهانی بر تروریسم سایبری را ارائه می‌نماید. صلاحیت جهانی هم از طریق دولت‌ها و هم جامعه بین‌الملل اعمال می‌گردد و صلاحیتی که از طریق جامعه بین‌المللی اعمال می‌گردد، بر صلاحیت محاکم داخلی در زمینه مبارزه با جرائم اولویت دارد (۹).

یک معاهده بین‌المللی عواقب سیاسی مختلفی دارد که ممکن است اهداف اساسی چون امنیت، جلوگیری از ارتکاب جرائم خاص، امکان پیگرد قانونی و استرداد و به تبع آن، افزایش سطح بازدارندگی در برابر تروریسم سایبری در اولویت باشد. با انجام این کار، معاهدات، مشکلات مربوط به صلاحیت را در رسیدگی به جرائم از بین می‌برد و بدین ترتیب مجرمان سایبری از ارتکاب جرائم سایبری و تروریسم سایبری باز خواهند ماند. علاوه بر این، همکاری‌های حاصل از یک معاهده، همکاری بین کشورهای امضاکننده در سطح همکاری‌های فنی را فراتر از مرزهای این معاهده تقویت می‌کند. علیرغم اینکه در زمان ایجاد برخی از اسناد بین‌المللی، تروریسم سایبری مورد توجه قرار نگرفته است، اما کلیات متن آن‌ها اغلب کافی است، اگرچه بیشتر فعالیت‌های تروریسم سایبری نیز تحت پوشش چنین سازمان‌های بین‌المللی است، اما برخی از مشکلات عمده هنوز وجود دارد. به عنوان مثال، ابتدا تعداد کشورهایی که به این تعهدات پیوسته‌اند و در واقع آن‌ها را اجرا کرده‌اند محدود است و این وضعیت مشکلات زیادی را ایجاد می‌کند. بنابراین فقط یک اجماع گسترده بین‌المللی می‌تواند راه را هموار نموده و در مبارزه با تروریسم سایبری موفقیت کسب کند؛ دوم، فقدان قواعد رویه‌ای برای تحقیقات و پیگرد قانونی است که از محکومیت احتمالی جلوگیری می‌کند.

اگرچه سازمان‌های بین‌المللی متعددی بر پایه تعهدات چندجانبه، دوجانبه و منطقه‌ای وجود دارند، اما به نظر می‌رسد مؤثرترین روش‌ها در واکنش به جرائم سایبری فراملی و تروریسم سایبر از طریق سازمان‌هایی صورت بپذیرد که بر اساس توافقات چندجانبه ایجاد شده‌اند. بنابراین ابعاد تعهدات دولت‌ها به همکاری بین‌المللی یا از خلال معاهدات بین‌المللی محقق می‌گردد و یا اقدامات سازمان‌های بین‌المللی که در ادامه به تفصیل بیان خواهد شد.

شایان ذکر است، به دلیل تهدید تروریسم و نقایص معاهدات چندجانبه، کنوانسیون‌های منطقه‌ای سعی در ایجاد زمینه‌ای مناسب و قانونی برای مبارزه با تروریسم دارند. همکاری در سطح ملی، منطقه‌ای و بخش‌های خصوصی برای پاسخگویی به تهدیدات سایبری در مرکز این تلاش‌ها می‌باشد. بنابراین می‌توان ابعاد همکاری تابعان حقوق بین‌الملل در مبارزه با تروریسم سایبری را از رهگذر معاهدات بین‌المللی و تمرکز سازمان‌های بین‌المللی به ویژه سازمان ملل متحد و تقویت همکاری فراتر از سطح مورد انتظار معاهدات، در وضع و اجرای قانون شایسته و بایسته در حوزه تلاش برای ایجادچارچوب قانونی و جرم‌انگاری و نیز پیشگیری و دفاع سایبری دانست.

۳-۱. همکاری بین‌المللی در وضع قواعد و مقررات: عدم وجود یک چارچوب قانونی که تروریسم سایبری، تکالیف و اختیارات دولت‌ها را در سراسر جهان مخاطب قرار دهد، چالش‌های وسیعی را در زمینه کشف و تعقیب حملات تروریستی سایبری به وجود آورده است. در سال‌های اخیر با رشد فزاینده نگرانی‌ها در مورد حملات ترویستی سایبری که گاهی آسیب‌های شدیدتری از حملات مسلحانه ایجاد می‌کنند، نیاز به چارچوب قانونی و اقدامات مؤثر اجرایی در حوزه سایبری که منجر به کشف عاملان و سازمان‌دهندگان آن‌ها شود، بیش از پیش احساس می‌شود. عاملان حملات فارغ از دغدغه مکانی می‌توانند در هر جای گیتی که بخواهند

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

اقدام به عملیات خود نمایند، این عملیات یا به دستور نهاد یا سازمان جنایتکار بین‌المللی یا حتی توسط سازمان‌هایی که توسط دولت دیگر حمایت می‌شود، ارتکاب می‌یابد. دستورالعمل‌ها، راهنماها، قوانین مدون و معاهدات بین‌المللی یا به اندازه کافی مرتبط با تروریسم سایبری نبوده‌اند یا در این زمینه اقدام مؤثری به شمار نمی‌آیند. در فقدان چنین چارچوب جامعی دولت‌ها به سمت جرم‌انگاری ترویسم سایبری در قوانین داخلی خود رفته‌اند.

دولت‌ها و سازمان ملل متحد برای مقابله با تروریسم کنوانسیون‌های متعددی تصویب کرده‌اند، اما حق این است که به موازات پیشرفت تروریست‌ها و تبدیل‌شدن آنان به بازیگران بین‌المللی و فعالیت در قالب سازمان‌ها و مجموعه‌های هماهنگ، جامعه بین‌المللی باید اقدامات ضد تروریستی مؤثری را توسعه دهد که تجلّیات هرچه پیچیده‌تر و جهانی تهدیدهای تروریستی را مورد توجه قرار دهد. به نظر نمی‌رسد اقدامات یک‌جانبه یا حتی دوجانبه، برای مقابله با تهدیدی که جهانی است کافی باشد. برای محدودساختن تروریست‌های بین‌المللی، همکاری و هماهنگی بین‌المللی ضروری است. اگر همچون خانم رزالین هیگینز (Rosalyn Higgins) قاضی معروف دیوان دادگستری بین‌المللی «تروریسم را چالشی برای حقوق بین‌الملل معاصر» بدانیم، برای مواجهه با آن باید از ابزارهای مختلف حقوقی و سیاسی همچون اجرای قانون و دیپلماسی مذاکره، بهره‌مند گردیم (۱۰).

بنابراین راهکار وضع قواعد متحد شکل به سازمان‌های بین‌المللی می‌انجامد، از برجسته‌ترین و کلیدی‌ترین سازمان‌ها جهت وضع قواعد در فضای سایبری، می‌توان به سازمان ملل متحد و اتحادیه بین‌المللی مخابرات در سطح جهانی و اتحادیه اروپا، ناتو، اتحادیه آفریقا، سازمان دولت‌های آمریکایی، سازمان همکاری‌های شانگهای، آسه آن و سازمان همکاری اقتصادی آسیا اقیانوسیه در سطح منطقه‌ای اشاره نمود، در حالی که اغلب امور در حوزه سایبری به ویژه جنگ سایبری توسط دولت‌ها سازماندهی می‌شود، سازمان‌های بین‌المللی به بهبود وضع و ارتقای راهبردهای جهانی، ایجاد ساختارها، نهادها و سیاست‌های مناسب منطقه‌ای و بین‌المللی در راستای پیشگیری از سوءاستفاده از فناوری‌ها، ارتقای توانایی مقابله با حوادث سایبری و اجرای حقوق مخاصمات مسلحانه می‌پردازند (۱۱).

قبل از هر چیز باید به زمینه‌ها و پیشینه تلاش‌های جهانی در راستای شکل‌گیری همکاری بین‌المللی در وضع قانون اشاره کرد. در سال ۱۹۹۶، پیش‌نویس کنوانسیون جامع مقابله با تروریسم بین‌المللی را برای بررسی به دبیرکل سازمان ملل متحد تقدیم شد و پس از اعمال اصلاحات در سال ۲۰۰۲ منتشر گردید که تعریف محدودی از تروریسم را ارائه نمود. در این پیش‌نویس چارچوبی برای بررسی اعمال و شیوه‌های اقدامات تروریستی مشخص شده است. هر دولت می‌پذیرد که جرائم مندرج در ماده ۲ را، طبق قانون داخلی خود جرم کیفری قلمداد نماید. صلاحیت قضایی، همکاری بین دولت‌ها و محاکمه و اجرای معیارها نیز در این پیش‌نویس آمده است. ماده (ب) (۱)۲ تصریح می‌کند: هر فرد در حیطه معنایی این کنوانسیون در صورتی مرتکب جرم شده که به هر طریق و وسیله، به طور غیر قانونی و عمدی باعث صدمات شدید و جدی به اموال دولتی یا شخصی از جمله تأسیسات کشوری، سیستم حمل و نقل عمومی و تأسیسات زیرساختی یا محیط زیست شود تا از طریق مرعوب‌ساختن مردم، یک دولت یا سازمان بین‌المللی را به انجام یا خودداری از انجام یک عمل وادار کند. اشاره این ماده به «به هر طریق و وسیله» و نیز «تأسیسات زیرساختی» می‌تواند به موضوع تروریسم سایبری نیز ورود پیدا کند. زیرساخت‌های حیاتی یک کشور شامل مخابرات، ارتباطات و شبکه‌های اطلاع‌رسانی است که کاربرد جرائم مندرج در پیش‌نویس را برای جرائم تروریسم سایبری امکان‌پذیر می‌سازد (۴). در پیش‌نویس کنوانسیون جامع مبارزه با تروریسم، دو نظام حقوقی در نظر گرفته شده است: اول پذیرش کلیه تعهدات مقرر در کنوانسیون‌های قبلی مبارزه با تروریسم؛ دوم وظیفه دولت‌های عضو در جلوگیری از استفاده از سرزمینشان برای ارتکاب اعمال مجرمانه در قلمرو دولت دیگر، همکاری با سایر دولت‌ها در پیداکردن شواهد،

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

مدارک و استرداد مجرمین و نیز تعهدات خاص در رابطه با رعایت حقوق بشر افراد مظنون.

از سوی دیگر در پژوهشی که سال ۲۰۱۳ به همت اداره مبارزه با جرائم ومواد مخدر سازمان ملل متحد صورت گرفته است، ۵ دسته از اسناد در این خصوص توسط سازمان ملل متحد مورد شناسایی قرار گرفته‌اند که عبارتند از: اسناد ایجادشده به وسیله شورای اروپا یا اتحادیه اروپا؛ اسناد ایجادشده به وسیله دولت‌های مستقل و مشترک‌المنافع یا سازمان همکاری شانگهای؛ اسناد ایجادشده به وسیله دولت‌های آفریقایی و اتحادیه آفریقا؛ اسناد ایجادشده به وسیله اتحادیه عرب و دسته پنجم: اسناد ایجاد شده تحت توجهات یا با همکاری نهادهای سازمان ملل متحد (۱۲).

با توجه به ویژگی‌های تروریسم سایبری وجود همکاری‌های بین‌المللی و وجود یک چارچوب قانونی در کنار اقدامات داخلی دولت‌ها در کشف و مبارزه با عاملان تروریسم سایبری لازم است. آنچه می‌توان به عنوان وضع قواعد در اقدامات سازمان‌های بین‌المللی برشمرد ذیلاً مورد بررسی قرار می‌گیرد.

۳-۱-۱. ایجاد چارچوب بین‌المللی برای همکاری در وضع قواعد در رویه سازمان ملل متحد: روشن است که تلاش‌های سازمان ملل متحد و ارکان آن به عنوان یک سازمان عام‌الشمول در رأس توجهات است. اسناد بین‌المللی که به ابتکار سازمان ملل متحد به تصویب رسیده‌اند، مبارزه با تروریسم برای دولت‌های عضو تعهدات لازم را برای اتخاذ اقدامات اساسی کیفری و دادرسی برای مقابله با اقدامات مختلف تروریسم و همچنین اقدامات اداری در برخی موارد برای مقابله با تأمین مالی تروریسم ایجاد می‌کند تا اطمینان یابد سیستم‌های عدالت کیفری مجهز به مکانیسم‌های مؤثر و قانونی برای جلوگیری و مجازات اقدامات تروریستی باشند. این اقدامات به گونه‌ای طراحی شده است که هم بتواند تأثیر پیشگیرانه و هم ممانعت از وقوع تروریسم را داشته باشد. جنبه منع‌کننده این ابزارهای بین‌المللی تا حدودی در تلاش برای هماهنگی قوانین جزایی کشورها و تقویت اجرای قانون و همکاری عدالت کیفری است. هدف پیشگیرانه آن جرم‌انگاری رفتارهای جنایت کارانه تروریستی توسط همه کشورها به منظور از بین‌بردن پناهگاه‌های امن برای عاملان جنایات تروریستی و تسهیل همکاری‌های بین‌المللی بین سازمان‌های دولتی درگیر در مبارزه با تروریسم است.

در این راستا مجمع عمومی سازمان ملل متحد استراتژی جهانی مبارزه با تروریسم را در ۸ سپتامبر ۲۰۰۶ به تصویب رساند. این استراتژی ابزار بی‌نظیر جهانی برای تقویت تلاش‌های ملی، منطقه‌ای و بین‌المللی برای مقابله با تروریسم است. تصویب این موضوع که همه کشورهای عضو برای اولین‌بار با یک رویکرد مشترک استراتژیک و عملیاتی برای مبارزه با تروریسم موافقت کرده‌اند، نه‌تنها این پیام صریح را که تروریسم در همه اشکال و تجلیات آن قابل قبول نیست به جهانیان اعلام می‌کند، بلکه نشان‌دهنده این تصمیم است که اقدامات عملی یک‌جانبه و جمعی اتخاذ خواهد شد. جلوگیری و مبارزه با تروریسم شامل طیف گسترده‌ای از اقدامات اعم از تقویت ظرفیت دولت‌ها برای مقابله با تهدیدات تروریستی تا هماهنگی بهتر فعالیت‌های ضد تروریستی سازمان ملل متحد می‌گردد. تصویب این استراتژی در راستای تعهدات رهبران جهان در اجلاس سپتامبر ۲۰۰۵ است و بسیاری از عناصر پیشنهادی دبیرکل (در گزارش خود در تاریخ ۲ مه ۲۰۰۶ با عنوان اتحاد علیه تروریسم: توصیه‌هایی برای یک استراتژی جهانی مقابله با تروریسم) را شامل می‌شود. در برنامه عملِ ضمیمهِ قطعنامه مصوب ۲۰۰۶ مجمع عمومی سازمان ملل، ضمن محکوم‌کردن تروریسم در تمام اشکال و جلوه‌های خود، اتخاذ اقدامات فوری برای جلوگیری و مبارزه با تروریسم در همه اشکال و مظاهر آن، عضویت بدون تأخیر در کنوانسیون‌ها و پروتکل‌های بین‌المللی موجود علیه تروریسم و اجرای آن‌ها و تلاش برای دستیابی به توافقنامه و نتیجه‌گیری کنوانسیون جامع درباره تروریسم بین‌المللی، اجرای همه قطعنامه‌های مجمع عمومی در مورد اقدامات برای از بین‌بردن تروریسم بین‌المللی و قطعنامه‌های مجمع عمومی مربوطه در مورد حمایت از حقوق بشر و آزادی‌های اساسی در ضمن مقابله با تروریسم، برای اجرای کلیه قطعنامه‌های شورای امنیت مربوط به تروریسم بین‌المللی و همکاری کامل با نهادهای تابعه ضد

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

تروریسم شورای امنیت، به رسمیت‌شناختن این همکاری بین‌المللی و هرگونه اقداماتی که برای پیشگیری و مبارزه با تروریسم و انجام تعهدات دولت‌ها را طبق قوانین بین‌المللی، از جمله منشور سازمان ملل متحد و کنوانسیون‌ها و پروتکل‌های بین‌المللی مربوطه به ویژه حقوق بشر، حقوق پناهندگان و حقوق بشردوستانه بین‌المللی در دستور کار قرار گرفته است (۱۳).

مجمع عمومی هر دو سال یک بار استراتژی مورد نظر را بررسی و آن را تبدیل به سندی می‌کند که حاوی اولویت‌های ضد تروریسم کشورهای عضو می‌باشد. چهارمین بررسی استراتژی مبارزه با تروریسم (A/RES/68/276) در ژوئن ۲۰۱۴ انجام شد و قبل از آن گزارشی از دبیرکل سازمان ملل متحد که شامل یک نمای کلی از منظر در حال تحول و شامل توصیه‌هایی برای مقابله با چالش‌ها و تهدیدات و مجموعه‌ای از اقدامات انجام‌شده توسط کشورهای عضو و نهادهای سازمان ملل برای مبارزه با تروریسم بود، بررسی گردید. استراتژی جهانی مقابله با تروریسم در قالب قطعنامه و برنامه ضمیمه آن (A/RES/60/288) متشکل از ۴ محور است. اول، پرداختن به شرایطی که منجر به گسترش تروریسم می‌شود؛ دوم، اتخاذ اقدامات برای جلوگیری و مبارزه با تروریسم؛ سوم، اقداماتی برای ظرفیت‌سازی کشورها برای جلوگیری و مبارزه با تروریسم و تقویت نقش سیستم سازمان ملل در این زمینه؛ چهارم، اقداماتی برای اطمینان از احترام به حقوق بشر برای همه و حاکمیت قانون به عنوان پایه اساسی مبارزه با تروریسم. ششمین بررسی استراتژی جهانی مبارزه با تروریسم سازمان ملل متحد در تاریخ ۲۶ ژوئن ۲۰۱۸ انجام شد. دهه گذشته مجمع عمومی، گزارش دبیر کل در مورد اجرای استراتژی جهانی ضد تروریسم سازمان ملل را بررسی نمود و بر اساس آن قطعنامه (A/RES/72/284) را با کنسانوس تصویب کرد (۸).

ماحصل بحث اینکه پاسخ‌های سیستم عدالت کیفری به تهدیدهای ناشی از استفاده از اینترنت توسط تروریست‌ها، دولت‌ها را ملزم به تدوین سیاست‌ها و قوانین ملی مشخصی می‌کند که از جمله آن‌ها:

۱ـ جرم‌انگاری اقدامات غیر قانونی انجام‌شده توسط تروریست‌ها از طریق اینترنت یا خدمات مرتبط؛ ۲ـ ارائه اختیارات بازرسی برای دستگاه‌های مجری قانون که در تحقیقات مرتبط با تروریسم مشغول هستند؛ ۳ـ تنظیم خدمات مرتبط با اینترنت (به عنوان مثال ارائه‌دهندگان خدمات اینترنتی) و کنترل محتوا؛ ۴ـ تسهیل امور بین‌المللی مشارکت؛ ۵ـ توسعه روش‌های تخصصی قضایی یا اثبات؛ ۶ـ حفظ استانداردهای بین‌المللی حقوق بشر.

طبقه‌بندی وسیع رویکردهای استراتژیک ارائه‌شده توسط گروه کاری گروه مقابله با تروریسم در مقابله با استفاده از اینترنت برای اهداف تروریستی، شامل استفاده از قوانین عمومی جرائم سایبری، قوانین ضد تروریسم، چارچوب مفهومی مفیدی را برای سیاستگذاران و قانونگذاران فراهم می‌کند. در حال حاضر، تعداد کمی از کشورها قوانینی را تدوین کرده‌اند که به طور خاص اقدامات تروریست‌ها را از طریق اینترنت مورد هدف قرار می‌دهد. اکثر کشورها از قوانین جنایی عمومی، جرائم سایبری و یا از قوانین ضد تروریسم برای جرم‌انگاری و تعقیب این نوع جنایات استفاده می‌کنند.

بنابراین باید گفت، چهار عنصر کلیدی برای ایجاد چارچوب قانونی بین‌المللی مؤثر در مبارزه با تروریسم سایبری عبارتند از: توافق بر مسأله تعریف تروریسم سایبری، راهبری سازمان ملل متحد، بهره‌برداری و بسط کنوانسیون‌های موجود، قانونگذاری برای ایجاد یک سیستم به هم پیوسته و قدرتمند و ایجاد یک نظام الزام‌آور قانونی. گذشته از عدم اجماع بر سر تعریفی جامع از تروریسم تحت معاهده‌ای بین‌المللی، در مورد رهبری سازمان ملل متحد باید گفت: سازمان ملل متحد باید به عنوان یک عامل تسهیل‌کننده در جهت حصول توافق میان اعضا و فهم مشترک مفهوم تروریسم سایبری عمل کند، اعضای سازمان ملل متحد در راستای رسیدن به یک چارچوب قانونی برای کشف و تعقیب اقدامات مرتبط با امنیت سایبری در حال تلاشند. سازمان می‌تواند از کمیته ضد تروریسم در

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

جهت هماهنگ‌سازی قوانین کیفری متنوع داخلی کشورها در جهت مدیریت جرائم حوزه تروریسم سایبری به وسیله تسهیل ارتباط دولت‌ها از طریق بحث بر روی موارد اساسی این جرائم، به اشتراک‌گذاری اطلاعات و اقدامات مربوط به تعقیب قضایی، استفاده کند. از سال ۲۰۱۰ کمیته اقداماتی را انجام داده تا از ۱۹۲ عضو سازمان ملل درباره جرم‌انگاری تروریسم در حوزه صلاحیتشان، محاکمه و مبارزه با منابع مالی تروریسم و ممانعت از آزادی رفت و آمدشان اطلاع حاصل کند. این همکاری بین‌المللی می‌تواند در ایجاد یک سیستم پاسخگو و مدیریت همکاری مؤثر در جهت جلوگیری و پاسخگویی سریع از طریق همکاری فنی و حقوقی به حملات سایبری و نیل به توافق در زمینه دستیابی به اصول راهنما در این زمینه، مفید باشد (۱۴).

تلاش جهانی در راستای تصویب قطعنامه‌های شورای امنیت نیز قابل بررسی است. قطعنامه‌های (۲۰۰۰ م.) ۵۵/۶۳ و (۲۰۰۱ م.) ۵۶/۱۲۱ در مورد مبارزه با سوءاستفاده از فناوری اطلاعات، به هشت اصل توجه شده است. علاوه بر این، قطعنامه‌های دیگری نیز وجود دارند که کشورهای عضو را «برای ارتقای توجه چندجانبه به تهدیدهای موجود و بالقوه در زمینه امنیت اطلاعات و همچنین اقدامات احتمالی برای محدودکردن تهدیدها» دعوت می‌کنند.

همان‌گونه که قبلاً اشاره شد، به دنبال فاجعه ۱۱ سپتامبر، قطعنامه ۱۳۷۳ شورای امنیت سازمان ملل متحد به سمت پیشبرد مبارزه با تروریسم رفت و تعهدی را به تمام کشورهای عضو سازمان ملل متحد برای جلوگیری از حمایت و تأمین مالی تروریسم و همچنین جرم‌انگاری فعالیت‌های تروریستی، تأمین مالی تروریسم و حمایت از فعالیت‌های تروریستی تحمیل نمود که مطابق آن تمام کشورهای عضو ملزم به همکاری با سایر دولت‌ها و سازمان‌های بین‌المللی برای از بین‌بردن پناهگاه‌های امن برای تروریست‌ها هستند. کنوانسیون سازمان ملل برای سرکوب تأمین مالی تروریسم که در قطعنامه ۵۴/۱۰۹ در سال ۱۹۹۹ توسط مجمع عمومی سازمان ملل به تصویب رسید، همکاری‌های بین‌المللی را ارتقا می‌بخشد. طبق ماده ۱۴ این کنوانسیون درخواست‌های همکاری به دلایل سیاسی رد نمی‌شود. سازمان برای نظارت بر اجرای قطعنامه ۱۳۷۳ و کمک به دولت‌ها در توسعه توانمندی‌های مورد نیاز، کمیته مبارزه با تروریسم (CTC) که به عنوان «مرکز تلاش‌های جهانی برای مبارزه با تروریسم» شناخته می‌شود و تعهدات قانونی گسترده‌ای را برای کشورهای عضو سازمان ملل در مقابله با تهدیدات تروریستی جهانی ایجاد کرده است. همانطور که قبلاً گفته شد، پنج سال بعد، تمام کشورهای عضو مجمع عمومی برای اولین‌بار در مورد چارچوب استراتژیک مشترک برای مقابله با معضل تروریسم توافق کردند: استراتژی جهانی مبارزه با تروریسم سازمان ملل.

مورد دیگر قطعنامه ۱۵۶۶ شورای امنیت سازمان ملل است که دولت‌ها را ملزم به همکاری کامل در مبارزه با تروریسم می‌کند و قطعنامه ۱۶۲۴ (۲۰۰۵ م.) از کشورها می‌خواهد که «توسط قانون انجام یک عمل یا اقدامات تروریستی» را منع کنند. این قطعنامه که بر اساس فصل هفتم منشور سازمان ملل متحد تصویب شده است، تروریسم را در هر شکلی محکوم می‌کند و کشورها را به همکاری کامل با کمیته مبارزه با تروریسم که مطابق قطعنامه ۱۳۷۳ (۲۰۰۱ م.) تأسیس شده است، فرامی‌خواند و برای اولین بار تعریفی بین‌المللی از «ترور» را به رسمیت می‌شناسد که به نظر می‌رسد ممنوعیت همه‌جانبه‌ای در مورد انواع خشونت‌هایی که به طور بین‌المللی غیر نظامیان را هدف قرار می‌دهند، فراهم می‌کند و همچنین از کشورها می‌خواهد خواستار پیگرد قانونی تروریست‌ها شود.

قطعنامه ۱۵۳۵ شورای امنیت سازمان ملل متحد برای تسهیل مساعدت فنی به کشورها، یک دفتر اجرایی کمیته مبارزه با تروریسم (CTED) ایجاد کرد. این امر همکاری بین بخش‌های سازمان ملل متحد و همچنین همکاری میان نهادهای منطقه‌ای و بین دولتی را ارتقا می‌بخشد. علاوه بر این، مشاوره تخصصی را به در کلیه موارد تحت پوشش قطعنامه ۱۳۷۳ ارائه می‌دهد. قطعنامه ۱۶۱۷ (۲۰۰۵ م.) از کشورها می‌خواهد که مطابق منشور سازمان ملل متحد با تروریسم در هر شکل خود مبارزه کنند و همچنین تأکید می‌کند که کشورها باید اطمینان حاصل کنند که هرگونه اقدامات انجام‌شده برای مبارزه با تروریسم مطابق با تمام

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

تعهدات خود طبق قانون بین‌المللی است (به ویژه با حقوق بشر بین‌الملل، حقوق پناهندگان و حقوق بشردوستانه).

قطعنامه‌های لازم‌الاجرای شورای امنیت ابزار اجرایی قوی و مؤثر است که کاربردی جهانی برای همه اعضای سازمان ملل دارد. به عنوان مثال، قطعنامه ۱۳۷۳ تعهدات مختلفی را از کنوانسیون‌های ضد تروریسم موجود دریافت می‌کند و آن‌ها را برای همه کشورهای عضو سازمان ملل متحد اعمال می‌کند، بدون اینکه نیازی به امضای آن کنوانسیون‌ها باشد. علاوه بر این، قطعنامه شورای امنیت می‌تواند در یک دوره زمانی کوتاه، در مقایسه با مدت زمانی که برای تصویب یک معاهده طول می‌کشد، ایجاد شود. به نظر نگارنده با توجه به این مزایا، اگرچه یک قطعنامه شورای امنیت نمی‌تواند یک ابزار بین‌المللی ضد تروریسم کامل ایجاد کند، اما هنوز هم می‌تواند یک ابزار مؤثر باشد.

در سال ۱۹۹۸، دولت روسیه پیش‌نویس قطعنامه‌ای را در کمیته اول با عنوان «تحولات در حوزه اطلاعات و ارتباطات در زمینه امنیت» ارائه نمود. در قطعنامه سال ۲۰۰۱، این دولت خواستار ایجاد گروهی از کارشناسان دولتی (GGE) متشکل از کارشناسان ۱۵ دولت (انتخاب‌شده بر اساس توزیع عادلانه جغرافیایی) برای یک مطالعه در مورد تهدیدات موجود و بالقوه درحوزه اطلاعات بود. این گروه در سال ۲۰۰۴ به دلیل اختلافات مهم در جنبه‌های اصلی امنیت اطلاعات بین‌المللی، نتوانست گزارش جامعی را ارائه کند. در سال ۲۰۰۹ گزارش گروه دوم کارشناسان عمدتاً بر لزوم ادامه بحث درباره هنجارهای بیشتر برای مقابله با تهدیدات موجود و بالقوه در حوزه امنیت اطلاعات تأکید کرد؛ گروه سوم کارشناسان در سال ۲۰۱۱ فراخوانده شد. این گروه در سال ۲۰۱۲-۲۰۱۳ تشکیل شد و با موفقیت گزارشی تهیه کرد که در زمینه همکاری‌های بین‌المللی درمورد هنجارهای امنیت سایبری، پیشرفتی اساسی تلقی می‌شود. شاید مهم‌ترین نتیجه این بود که در این گزارش به اثبات رسیده است که قواعد حقوق بین‌المللی به ویژه منشور سازمان ملل در فضای مجازی قابلیت اعمال دارد. در این گزارش درک مشترک و لزوم همکاری با ارائه چندین توصیه برای ارتقای صلح و امنیت در استفاده دولت از فناوری اطلاعات و ارتباطات بیان شده است (به عنوان مثال، ظرفیت‌سازی و مشارکت در مبادله اطلاعات) که در جای مقتضی بیشتر بدان پرداخته خواهد شد.

اگرچه قطعنامه‌ها و گزارش‌های سالانه گروه کارشناسان دولتی را می‌توان نشانه‌های افزایش اجماع تلقی کرد، اما درک مشترکی در مورد چگونگی اعمال قوانین بین‌المللی در فضای مجازی وجود ندارد و توسعه هنجارهای جدید جهانی سایبری محدود شده است. به عنوان مثال، در سال ۲۰۱۱، گروهی از دولت‌ها قواعد رفتاری بین‌المللی بحث برانگیز برای امنیت اطلاعات را پیشنهاد کردند که در ژانویه سال ۲۰۱۵، به مجمع عمومی ارسال شد. کمیته اقتصادی و مالی همچنین سه قطعنامه مربوط به فضای سایبری را به مجمع عمومی ارائه کرده است که مربوط به ایجاد فرهنگ جهانی امنیت سایبری است و شامل موضوع حمایت از زیرساخت‌های مهم اطلاعاتی می‌باشد. کمیته اجتماعی، فرهنگی و بشردوستانه عمدتاً به مسائل مربوط به جرائم سایبری و حقوق حریم خصوصی پرداخته است. دو قطعنامه (تصویب‌شده در سال ۲۰۰۰ و ۲۰۰۱ م.) می‌تواند به عنوان تمرکز ویژه در مبارزه با سوءاستفاده مجرمانه از فناوری‌های اطلاعاتی برجسته شود. در سال ۲۰۱۳ و در نتیجه افشاگری‌های ادوارد اسنودن (Edward Snowden) مجمع عمومی قطعنامه حق حفظ حریم خصوصی در عصر دیجیتال را تصویب کرد که برای اولین‌بار توسط برزیل و آلمان تهیه شد. این قطعنامه بر مسئولیت دولت‌ها برای احترام و محافظت از حریم خصوصی تأکید کرده و برای اولین‌بار تأیید کرده است که همان حقوقی که مردم به صورت آفلاین دارند، باید به صورت آنلاین محافظت شوند. این قطعنامه از کمیساریای عالی حقوق بشر خواسته است تا گزارشی را درباره این موضوع تهیه کند. نگرانی‌های مربوط به حقوق اساسی بشر در عصر دیجیتال بارها توسط سازمان ملل تکرار شده است در مارس ۲۰۱۵، مجمع عمومی تصمیم گرفت یک گزارشگر ویژه جدید در مورد حق حفظ حریم

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

خصوصی را به منظور رسیدگی بهتر به این موضوعات و ایجاد محیط دیجیتال ایمن‌تر منصوب کند (۱۵).

مجمع عمومی سازمان ملل نیز در سال ۲۰۰۸، قطعنامه (A/RES/2321) را در مورد تروریسم سایبری با تمرکز بر تقویت آگاهی‌های عمومی و مجازات استاندارد برای این نوع حملات تصویب کرد. علاوه بر این، در سال ۲۰۱۰، مجمع عمومی قطعنامه‌ای را در مورد «ایجاد فرهنگ جهانی امنیت سایبری و حمایت از تلاش‌های ملی برای حفاظت از زیرساخت‌های مهم اطلاعاتی» به تصویب رساند و کشورهای عضو خود را برای به اشتراک‌گذاشتن بهترین روش‌ها و اقدامات در زمینه امنیت سایبر تشویق کرد.

از سوی دیگر، شورای اقتصادی و اجتماعی (ECOSOC) به طور فزاینده‌ای با جرائم سایبری سروکار دارد. جرائم سایبری همچنین در کنگره سازمان ملل در زمینه پیشگیری از جرم و عدالت کیفری (UNCPCJ) مورد بررسی قرار گرفته است که هر پنج سال یک بار انجام می‌شود و نقش مهمی در تنظیم استاندارد بین‌المللی و سیاستگذاری در پیشگیری از جرم و عدالت کیفری دارد، از جمله گزارش سال ۲۰۱۳ دفتر مواد مخدر و جرم سازمان ملل (UNODC) که در مورد جرائم سایبری و واکنش به آن تهیه شده است.

تنها نهاد سازمان ملل که در زمینه مقابله با حملات سایبری تخصص دارد، اتحادیه بین‌المللی ارتباطات از راه دور (ITU) می‌باشد که در سه بخش اصلی فعالیت می‌کند: اختصاص فرکانس‌های رادیویی و مدیریت مدار ماهواره‌ای و فناوری، توسعه استانداردهای فنی مخابرات و حمایت از تلاش‌های توسعه برای بهبود دسترسی جهانی به فناوری اطلاعات و ارتباطات. اتحادیه چارچوب لازم و جهانی را برای تنظیم ارتباطات بین‌المللی ایجاد می‌کند. اساسنامه اتحادیه، توافقات و مقررات قانونی الزام‌آور اداری و نیز اسناد غیر الزام‌آور مانند توصیه‌نامه و قطعنامه‌های صادره از نهادهای اتحادیه در راستای ایجاد چارچوب‌های قانونی مؤثر، نقش اساسی ایفا می‌کنند. نقش تسهیل‌کننده جهانی همکاری در زمینه امنیت سایبری در اجلاس جهانی جامعه اطلاعات (WSIS) که در سال ۲۰۰۳ و ۲۰۰۵ برگزار شد، به این اتحادیه واگذار گردید. در این راستا انجمن بین‌المللی امنیت سایبری سال ۲۰۰۷ راه‌اندازی شد تا چارچوبی برای همکاری‌های بین‌المللی با هدف ارتقای امنیت در جامعه اطلاعاتی به وسیله اقدامات قانونی، اقدامات فنی و رویه‌ای، ساختارهای سازمانی، ظرفیت‌سازی و همکاری‌های بین‌المللی، ایجاد نماید. یک گروه متخصصین عالی رتبه (HLEG)، متشکل از بیش از ۱۰۰ متخصص امنیت سایبری، سیاستگذاران و دست‌اندرکاران از سراسر جهان برای ارائه مشاوره به مجمع عمومی اتحادیه تدوین پیشنهادات برای آینده در حوزه امنیت سایبر مشغول به کار شدند. این اتحادیه همچنین با سازمان همکاری چندجانبه بین‌المللی علیه تهدیدات سایبری (IMPACT) مشارکت می‌نماید.

دبیرکل پیشنهاد یک قانون مشترک در برابر جرائم سایبری را داد که کشورها را موظف می‌کند تا: ۱ـ از شهروندان خود در برابر مجرمان سایبری محافظت کنند؛ ۲ـ داشتن پناهگاه امن برای تروریست‌ها یا مجرمان را در سرزمین‌های خود منع کند؛ ۳ـ کشوری به دیگری حمله نکند (۱۶).

علاوه بر این، تحقیقات و ابتکارات مربوط به فضای مجازی توسط بسیاری از بسترهای سازمانی دیگر در سازمان ملل مانند مؤسسه تحقیقات سازمان ملل برای خلع سلاح (UNIDIR) و پژوهشکده جرائم و عدالت بین سازمانی سازمان ملل (UNICRI) انجام می‌شود. همچنین امنیت سایبری در گروه مقابله با استفاده از اینترنت برای اهداف تروریستی در کارگروه اجرایی مقابله با تروریسم سازمان ملل نیز دنبال می‌گردد.

۳-۱-۲. همکاری در وضع قواعد در رویه سایر سازمان‌های بین‌الدولی: سازمان‌های بین‌المللی و منطقه‌ای دیگری نیز در این حوزه، فعالیت تخصصی داشته‌اند. باید دید در رویه سازمان‌های منطقه‌ای و تخصصی، مبارزه با تروریسم سایبری در وضع قواعد لازم چگونه نمود می‌یابد. بنابراین در این قسمت تلاش‌های صورت‌گرفته در سطح اروپا و سپس سایر سازمان‌های منطقه‌ای بررسی می‌گردد.

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

۳-۱-۲-۱. عملکرد سازمان‌های بین‌المللی در سطح اروپا:
شورای اروپا و اتحادیه اروپا اقدامات جدی را در این راستا در دستور کار خود داشته‌اند. طیف گسترده از قوانین ضد تروریسم مربوط به همکاری بین‌المللی میان دول عضو یا با کشورهای ثالث هستند. در اتحادیه اروپا این تعهد به همکاری در هر دو حوزه وجود دارد. شورای اتحادیه اروپا در سال ۱۹۹۸، راهنمایی را در مورد جرائم سایبری منتشر کرد. این راهنما، اصول و خط مشی مبارزه با جرم سایبری و تروریسم را مشخص کرده و مکانیزم‌های لازم برای مبارزه با آن بدون به تأخیرانداختن رشد سریع تجارت الکترونیک و یا نقض حقوق شهروندان چون حق حریم خصوصی را تبیین نموده است. این دستورالعمل شامل اقدامات قانونگذاری و نیز اقدامات سیاسی بود. پیشنهادات قانونگذاری مربوط به هماهنگ‌سازی قوانین دولت‌های عضو می‌گردید و از دیگر اقدامات آن، ایجاد یک مرکز اروپایی با مشارکت آژانس‌های اجرای قانون، فراهم‌آورندگان خدمات اینترنتی و کاربران حرفه‌ای شبکه جهت افزایش آگاهی‌های عمومی و اقدامات امن در حوزه فناوری اطلاعات بود (۱).

موضع مشترک شورا در ۲۰۰۱ در مورد اجرای اقدامات خاص برای مبارزه با تروریسم، تعهدی را بر دوش دول عضو می‌گذارد که طبق آن هرگونه کمک ممکن برای پیشگیری و مبارزه با اعمال تروریستی را به یکدیگر ارائه نمایند. این همکاری با هدف هماهنگی تلاش‌های قضایی و پلیسی در موضوعات کیفری محقق می‌گردد. همکاری قضایی با شبکه عدالت اروپایی (EJN) امکان‌پذیر می‌باشد که شبکه غیر متمرکزی بین وکلا و قضات اتحادیه اروپا در مورد پرونده‌های کیفری است و تلاش می‌کند تا به تبادل سریع و مؤثر اطلاعات مورد نیاز بپردازد. مورد دیگر این همکاری‌ها در مورد رویه استرداد بین دولت‌های عضو است، به جای رویه‌های سنتی استرداد مبتنی بر این اصل که یک دولت تصمیمات دولت دیگر را اجرا نمی‌کند، هم‌اکنون دولت‌های عضو به شکل اتوماتیک صلاحیت قضایی یکدیگر را در ارتباط با دستور بازداشت فرد با توجه به اعتماد به سیستم حقوقی یکدیگر به رسمیت می‌شناسند. در مورد همکاری با سایر دولت‌ها نیز همکاری با ایالات متحده آمریکا از یک اولویت در انعقاد معاهدات استرداد و معاضدت‌های حقوقی دوجانبه برخوردار است (۱۷). اقدامات شورای اروپا پس از حوادث ۱۱ سپتامبر در مبارزه با تروریسم حول سه محور عمده بوده است: ۱ـ تقویت اقدام قانونی علیه تروریسم با همکاری بین‌المللی همزمان مقامات قضایی؛ ۲ـ تشکیل یک گروه چندرشته‌ای در زمینه اقدام بین‌المللی علیه تروریسم (GMT) (از جمله اقدامات این گروه، مطالعه بر انگیزه تروریسم و تقویت همکاری مبتنی بر حقوق بین‌الملل بوده است)؛ ۳ـ تقویت فعالیت‌های موجود در زمینه جرائم سازمان‌یافته و جرائم اینترنتی، حمایت از ارزش‌های بنیادین با کار بر پیش‌نویس بیانیه کمیته وزیران در مورد رسانه و تروریسم و نیز تطبیق آزادی بیان و اطلاعات و مبارزه با تروریسم و توجه به ریشه‌های تروریسم با تکیه بر مفهوم دموکراسی به عنوان عامل تضعیف‌کننده تروریسم (۱۸).

ـ اتحادیه اروپا بیش از یک دهه است که در زمینه امنیت شبکه و اطلاعات و جرائم سایبری فعالیت می‌کند و در سال ۲۰۱۳ اولین سند جامع در رابطه با طیف گسترده‌ای از تهدیدات سایبری و استراتژی سایبری اتحادیه اروپا را منتشر کرده است. این استراتژی چشم‌اندازها، نقش‌ها، مسئولیت‌ها و اقدامات لازم برای اتحادیه اروپا در حوزه امنیت سایبر را تشریح می‌کند. نکته مورد تأکید سند این است که در زمینه امنیت سایبری، نظارت متمرکز اتحادیه اروپا پاسخ کافی به چالش‌های سایبری نیست و از این رو دولت‌های ملی باید به عنوان نهادهای اصلی که مانع از بروز حوادث سایبری می‌شوند، مورد تأکید اصلی باقی بمانند. فعالیت اصلی اتحادیه اروپا در حوزه امنیت سایبری بر سه اصل امنیت شبکه و اطلاعات، اجرای قانون و واکنش مبتنی است و نیز نهادهای ملی و ارگان‌های اتحادیه اروپا که مسئول تضمین امنیت سایبر هستند را تعیین می‌کند. اقدامات مربوط به امنیت سایبری نیز در برنامه دستورالعمل دیجیتال اتحادیه اروپا گنجانیده شده است که امنیت اینترنت را برای یک جامعه دیجیتالی فعال ضروری می‌داند و دستور کار اروپا برای

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

تهدیدهای نوظهور علیه امنیت، جرم و جنایت سایبری (تروریسم و جرم سازمان‌یافته) را در اولویت قرار می‌دهد. همچنین شورای اروپا چارچوب سیاست‌های دفاع سایبری اتحادیه اروپا را به عنوان یک سند مکمل برای حمایت از نهادهای اروپایی در رابطه با دفاع سایبری و نیز تهیه ابزار استراتژی امنیت سایبری اتحادیه اروپا به تصویب رسانده است. در زمینه امنیت شبکه و اطلاعات، بازیگران اصلی اتحادیه اروپا شامل کمیسیون اروپا، آژانس امنیت شبکه‌ها و اطلاعات اروپا (ENISA)، شبکه‌ای از مراجع ذی‌صلاح و مشارکت بخش‌های عمومی ـ خصوصی اروپا برای انعطاف‌پذیری (EP3R) می‌باشند. در سال ۲۰۱۳، کمیسیون پیشنهاد کرد که دستورالعملی درباره امنیت شبکه و امنیت اطلاعات اتخاذ شود که هدف آن تعیین استاندارد اقدامات قانونی و ایجاد انگیزه برای تبدیل محیط آن لاین اتحادیه اروپا به امن‌ترین فضای مجازی در جهان است. سیاست اتحادیه اروپا همچنین حاکی از اهمیت همکاری با بخش خصوصی است. علاوه بر این، سیاست حمایت از زیرساخت‌های اطلاعات با هدف تقویت امنیت و انعطاف‌پذیری زیرساخت‌های حیاتی فناوری اطلاعات و ارتباطات از طریق توسعه امنیت و قابلیت‌های تاب‌آوری، هم در سطح ملی و هم در اتحادیه اروپا از مهم‌ترین استراتژی‌های اتحادیه اروپا می‌باشد (۱۶).

ـ تنها پیمان بین‌المللی موجود برای مقابله با جرائم سایبری، کنوانسیون سایبری شورای اروپا است، اینکه بسیاری از کشورها تلاش‌های خود را برای اتخاذ اصول این کنوانسیون در چارچوب‌های قانونی خودشان آغاز کرده‌اند، دلگرم‌کننده است. کنوانسیون جرائم سایبری در سال ۲۰۰۱ در بوداپست با یک مقدمه و در چهار فصل و ۴۸ ماده به تصویب رسید. هدف از آن هماهنگ‌سازی حقوق و مقررات داخلی کشورها در حوزه جرائم سایبر و به تبع آن ایجاد مقررات یکپارچه بین‌المللی در خصوص عناصر تشکیل‌دهنده جرم سایبری است. این کنوانسیون، اگرچه در حوزه اتحادیه اروپا شکل گرفته، اما یک معاهده باز به حساب می‌آید و ۱۶۰ کشور جهان که عضو شورای اروپا نیستند، از قبیل برزیل و هند نیز از این کنوانسیون به مثابه یک اصل در قانونگذاری داخلی‌شان استفاده می‌کنند. این کنوانسیون اقدامات و فعالیت‌های غیر قانونی و تهدیدهای سایبری گوناگونی را هدف قرار داده است و استانداردها و فرآیندهای متداولی را برای امضاکنندگان ایجاد می‌کند و نهایتاً الزاماتی را برای بررسی داده‌ها و دسترسی به اطلاعاتی که موجبات نگرانی در حوزه حریم خصوصی ایجاد می‌کنند را معرفی می‌نماید (۷). این سند به عنوان یک سند بین‌المللی الزام‌آور، چارچوبی کلی را برای توسعه قانونگذاری ملی جامع علیه جرم سایبری از طریق همکاری‌های بین‌المللی بین دول عضو معاهده ارائه می‌کند. در راستای عملکرد مؤثرتر این سند، اجرای این کنوانسیون از مرزهای اروپا فراتر رود. نکته قابل تأمل اینکه کنواسیون فوق تنها ناظر بر جرائمی چون هرزه‌نگاری کودکان، کلاهبرداری اینترنتی، نقض کپی‌رایت، نقض امنیت شبکه و جرائمی است که از طریق شبکه و رایانه محقق می‌شود و به طور خاص شامل تروریسم سایبری نمی‌شود. بنابراین برای اینکه به عنوان مکانیزم مؤثری به کار رود این جرم نیز باید در کنواسیون مندرج گردد.

۳-۱-۲-۲. سازمان‌های منطقه‌ای و وضع قواعد ضد تروریسم سایبری: سازمان‌های بسیاری در این حوزه فعالیت داشته‌اند، اما در این مجال بررسی تمامی آنان نخواهد گنجید، لذا به اهم این فعالیت‌ها اشاره خواهد شد:

ـ سازمان پیمان آتلانتیک شمالی (NATO) یک سازمان منطقه‌ای با ۳۱ عضو با هدف ایجاد اتحاد نظامی و سیاسی، دفاع جمعی و مدیریت بحران، دفاع سایبری را به عنوان بخشی از برنامه‌های سیاسی ناتو در اجلاس پراگ در سال ۲۰۰۲ آغاز نموده است. پس از حملات سایبری علیه استونی در سال ۲۰۰۷، نخستین سیاست دفاع سایبری ناتو در سال ۲۰۰۸ تهیه شد. در اجلاس لیسبون در سال ۲۰۱۰، دفاع سایبری در مفهوم استراتژیک ناتو گنجانده شد و اعلامیه اجلاس، سیاست دفاع سایبری در سال ۲۰۱۱ و ایجاد یک برنامه اقدام در سال ۲۰۱۲ را تسریع کرد. در ۵ سپتامبر ۲۰۱۴، سیاست جدید دفاع سایبری پیشرفته در اجلاس ولز به تصویب رسید. این سیاست روشن می‌کند که یک حمله

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

دیجیتالی بزرگ به یک کشور عضو می‌تواند توسط ماده ۵ پیمان آتلانتیک شمالی پوشش داده شود. در اجلاس سران ورشو در سال ۲۰۱۶، ناتو فضای مجازی را به عنوان یک حوزه از فعالیت‌ها به رسمیت شناخت و متعهد شد توسعه همکاری‌های پدافند سایبری ناتو و اتحادیه اروپا را توسعه و منابع بیشتری را به توانایی‌های دفاع سایبری اختصاص دهد. در سال ۲۰۱۸، وزیران دفاع کشورهای عضو ناتو در مورد ایجاد یک مرکز عملیات سایبر جدید به توافق رسیدند تا به ادغام سایبر در برنامه‌ریزی‌ها و عملیات‌های ناتو در همه سطوح کمک کند. سیاست ناتو در زمینه دفاع سایبری توسط مقامات سیاسی، نظامی و فنی ناتو انجام می‌شود. شورای آتلانتیک شمالی نظارت سیاسی سطح بالایی بر همه جنبه‌های اجرایی آن دارد و نهادهای مختلفی برای انجام منسجم اهداف خود دارد: ۱ـ کمیته دفاع سایبری (CDC) که مشاور ارشد در امور دفاع سایبری است؛ ۲ـ هیأت مدیره دفاع سایبری (CDMB) که تحت نظارت بخش چالش‌های امنیت سایبری مقر فرماندهی ناتو فعالیت می‌کند و متشکل از نمایندگان کلیه ذی‌نفعان اصلی در زمینه امنیت سایبری مانند فرماندهی عملیات متفقین ACO و آژانس‌های ناتو است. هیأت مدیره، عهده‌دار برنامه‌ریزی استراتژیک و جهت اجرایی در رابطه با شبکه‌های ناتو است و همچنین برای تسهیل اطلاعات، تفاهم‌نامه همکاری با کشورهای عضو را امضا می‌کند؛ ۳ـ هیأت مشاوره، کنترل و فرماندهی ناتو (NC3)، کمیته اصلی مشاوره در مورد جنبه‌های فنی و اجرایی دفاع سایبری را تشکیل می‌دهد؛ ۴ـ آژانس اطلاعات و ارتباطات ناتو (NCIA)، در تعاقب اهداف اعلامیه لیسبون با ادغام ۷ آژانس ناتو ایجاد شد و در حوزه فعالیت‌های سایبری اقدام می‌کند؛ ۵ـ قابلیت واکنش به حوادث رایانه‌ای ناتو (NCIRC) که مسئول حفاظت فنی از دارایی‌های سایبری ناتو است؛ ۶ـ مرکز عالی همکاری دفاع سایبری ناتو (NATO CCD COE) یک مرکز تحقیقاتی و آموزشی معتبر است که با آموزش، مشاوره تحقیق و توسعه در زمینه امنیت سایبر فعالیت می‌کند (۲۰).

ـ جامعه اقتصادی کشورهای آفریقای غربی (ECOWAS) یکی از فعال‌ترین سازمان‌های منطقه‌ای در حوزه امنیت سایبری است. در سال ۲۰۱۰ قانون تکمیلی در مورد محافظت از داده‌های شخصی که به نظر می‌رسد تحت تأثیر دستورالعمل حفاظت از داده‌های اتحادیه اروپا باشد را تصویب کرد. قانونگذاری در حوزه قوانین مربوط به حریم خصوصی داده‌ها و موظف‌نمودن کشورهای عضو به ایجاد یک سازمان حفاظت از داده‌ها، از نتایج این قانون است. همچنین دستورالعملی در مورد مبارزه با جرائم سایبری و تأکید بر نیاز روزافزون به هماهنگی یا ایجاد مقررات منطقه‌ای با توجه به افزایش فزاینده جرائم سایبری در منطقه را اتخاذ کرده است. در سال ۲۰۱۷، در زمینه توسعه توانایی‌های کشورهای عضو خود برای مبارزه با جرائم سایبری و با ایالات متحده و در زمینه توسعه استراتژی‌های امنیت سایبری کشورهای عضو خود با شورای اروپا آغاز به همکاری کرده است (۲۱).

ـ سازمان ارتباطات کشورهای مشترک المنافع (Commonwealth Telecommunication Organisation) در حوزه امنیت سایبری، این سازمان بر ایجاد ظرفیت، به اشتراک‌گذاری اطلاعات و ارائه کمک به کشورهای عضو مشترک‌المنافع در اجرای یک چارچوب قانونی جامع برای پاسخ به جرائم سایبری و به دست‌آوردن شواهد سایبری متمرکز است. این فعالیت‌ها از طریق انجمن امنیت سایبری و ابتکار امنیت سایبری که زیر چتر سازمان ارتباطات مشترک المنافع فعالیت می‌کنند، انجام می‌شود. این سازمان مأموریت ارتقا، تسهیل و راهنمایی اعضا در استفاده از فناوری اطلاعات و ارتباطات در راستای توسعه را عهده‌دار است، در برنامه استراتژیک خود برای سال‌های ۲۰۱۲ تا ۲۰۱۶ حوزه‌هایی را برای فعالیت متمرکز مشخص کرده است که شامل تمرکز بر ظرفیت‌سازی، تسهیل مشارکت‌ها، امنیت سایبری و جرائم سایبری است. در جریان مجمع امنیت مشترک‌المنافع در لندن در سال ۲۰۱۴ لیستی از اصول برای هدایت کشورهای عضو مشترک‌المنافع جهت برنامه‌ریزی و اجرای اقدامات عملی در توسعه سیاست، مقررات، همکاری‌های مرزی، ایجاد

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

ظرفیت، اقدامات فنی و سایر فعالیت‌های عملیاتی مرتبط با فضای مجازی در نظر گرفته شد (۲۲).

ـ گروه هفت (G7) دارای یک گروه کار در زمینه جرائم سایبری است و از سال ۲۰۱۴ بیش از ۷۰ کشور را شامل می‌شود. هدف اصلی آن «حفظ شواهد دیجیتالی برای انتقال بعدی از طریق مجاری قانونی» است. در سال ۲۰۱۶، وزیران فناوری اطلاعات و ارتباطات گروه هفت برای نخستین‌بار در ژاپن با هم دیدار کردند و اسناد متعددی را با تمرکز بر موضوعات سایبری تصویب نمایند (۱۶).

ـ سازمان همکاری اقتصادی و توسعه (OECD) با توجه به فعالیت‌های فضای مجازی، با اقتصاد مبتنی بر اینترنت، دولت الکترونیک، امنیت سایبری و حفظ حریم خصوصی نیز سروکار دارد. در سال ۲۰۰۸، وزرا، اعلامیه سئول برای آینده اقتصاد مبتنی بر اینترنت را صادر کردند که در آن اعلام شد سازمان حمایت خود را از دسترسی، تقویت خلاقیت و تقویت امنیت اینترنت اعلام می‌کنند. این زمینه‌ها عبارتند از: حمایت از زیرساخت‌های اطلاعاتی مهم، استراتژی‌های امنیت سایبری، بدافزارها و باتنت‌ها، محافظت از کودکان به صورت آنلاین و مدیریت هویت دیجیتالی و احراز هویت الکترونیکی (۲۳).

ـ سازمان همکاری شانگهای (SCO) تمرکز ویژه‌ای بر مبارزه با تروریسم، جدایی‌طلبی و افراط‌گرایی دارد. در سال ۲۰۰۹، موافقتنامه دولت‌های کشورهای عضو در مورد همکاری در زمینه تضمین امنیت بین‌المللی اطلاعات منعقد شد و در ۱۲ سپتامبر ۲۰۱۱، چهار عضو این سازمان پیش‌نویس قواعد رفتاری بین‌المللی در مورد امنیت اطلاعات را به مجمع عمومی سازمان ملل متحد ارسال کردند. مفهوم «امنیت اطلاعات بین‌المللی» بحث‌برانگیز است و کشورهای عضو معتقدند که محتوای این سند مربوط به یک تهدید امنیتی بالقوه است که باید قاعده‌مند شود، اما «اجماع غربی» این سطح از تنظیم محتوا را تهدیدی برای حقوق اساسی بشر می‌داند. در سال ۲۰۱۵، رهبران کشورهای عضو مجدداً بر موضع خود در مورد امنیت اطلاعات تأیید کردند. در جلسه دبیران شورای امنیت ملی ۲۰۱۸ در پکن تأکید شد که فناوری اطلاعات و ارتباطات از جمله اینترنت برای تبلیغ همه مظاهر تروریسم، جدایی‌طلبی و افراط‌گرایی به طور جدی مورد استفاده قرار می‌گیرد، استخدام ستیزه‌جویان، گسترش فعالیت‌های تروریستی و مداخله در امور داخلی سایر کشورها و همچنین انجام اقدامات مجرمانه دیگراز مواردی است که اینترنت را تبدیل به بستر جرم نموده است. بنابراین شرکت‌کنندگان خواستار تقویت همکاری عملی در زمینه امنیت اطلاعات بین‌المللی و پیش‌نویس مقررات جهانی اصول و هنجارهای رفتار مسئولانه دولت‌ها در حوزه رسانه تحت نظارت سازمان ملل شدند (۱۶).

ـ سازمان همکاری اقتصادی آسیا و اقیانوسیه (APEC) در ساختار این سازمان چندین کمیته رهبری و کارگروه وجود دارد که در زمینه‌های مختلف فعالیت می‌کنند. یکی از این زمینه‌ها فناوری اطلاعات و ارتباطات است که به عنوان یک فاکتور مهم برای و رشد اقتصادی شناخته می‌شود. فناوری اطلاعات و ارتباطات در اختیار کار گروه ارتباطات و اطلاعات است. در سال ۲۰۰۲ این کارگروه استراتژی امنیت سایبری را صادر کرد که شامل توصیه‌هایی در زمینه مقررات مربوط به جرائم سایبری، دستورالعمل‌های امنیتی و فنی، آگاهی عمومی و آموزش است. در جلسه وزیران ارتباطات و اطلاعات در سال ۲۰۰۵، اعلامیه لیما با هدف بهبود زیرساخت‌های اطلاعاتی برای پیشرفت جامعه اطلاعات صادر شد. در این اعلامیه همچنین به امنیت شبکه و اهمیت ایجاد تیم‌های واکنش اضطراری رایانه پرداخته شده است. رهبران اپک استراتژی مهمی را برای اطمینان از یک محیط آنلاین مطمئن، ایمن و پایدار اتخاذ کردند. این استراتژی عملکرد اپک را در زمینه ارتقای اطلاعات و امنیت شبکه، هماهنگی چارچوب‌های مربوط به تضمین معاملات و ارتباطات و مبارزه با جرائم سایبری گسترش می‌دهد. این اقدامات به طور فزاینده، شامل همکاری نزدیک با بخش خصوصی و سایرنهادها و سازمان‌های بین‌المللی است. اهداف و فعالیت‌های اپک در زمینه امنیت سایبری در کارگروه ارتباطات و اطلاع‌رسانی بر اساس برنامه اقدام استراتژیک تصویب شده است. مقاومت زیرساخت‌های مهم داخلی، امنیت و مدیریت ریسک، ایجاد ظرفیت امنیت سایبری، افزایش آگاهی از امنیت سایبری، امنیت سایبری ابتکارات حوزه صنعت، فعالیت‌هایی برای ارتقای محیط‌های

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

امن و ایمن آنلاین برای گروه‌های آسیب‌پذیر و نهایتاً مبارزه با حملات سایبری از دیگر اولویت‌های این استراتژی می‌باشد. در راستای وضع قواعد باید به موارد دیگری نیز اشاره نمود، از جمله کارگروه اطلاعات و ارتباطات اپک (APEC Telecommunications and Information Working Group) که از سال ۲۰۱۶ تا ۲۰۲۰ بر اساس طرح اقدام استراتژیک انجام فعالیت کرده و هدف اصلی آن ارتقای امنیت و حفظ محرمانگی اطلاعات و ارتباطات، اتخاذ رویکرد افزایش آگاهی سایبری و ایجاد محیط‌های امن سایبری برای گروه‌های آسیب‌پذیر است (۱۶).

نهایتاً باید به بحث مهم نقش آموزش و نیز ضمانت اجرای این قواعد نیز در عملکرد سازمان‌های مربوطه اشاره کرد. به طور نمونه، از سال ۲۰۰۹، پلیس بین‌الملل با کالج دانشگاه دوبلین همکاری نزدیکی داشته تا آموزش‌های تخصصی و مبادلات دانشگاهی را برای ارتقا و تخصص تحقیق در مورد جرائم سایبری در اجرای قانون ارائه دهد. در آگوست ۲۰۱۱، محققان جرائم اینترنتی و متخصصان رایانه از ۲۱ کشور در اولین دوره آموزش مدرسه تابستانی جرائم اینترنتی پلیس بین‌الملل و دانشگاه دوبلین شرکت کردند. این برنامه دو هفته‌ای که توسط دانشگاه تدوین شد شامل تمرینات شبیه‌سازی پرونده‌ها بود و توسط متخصصان اجرای قانون، دانشگاه دوبلین و بخش خصوصی ارائه شد. این رویداد با هدف توسعه دانش و مهارت‌های نظری و عملی در طیف وسیعی از زمینه‌ها برای کمک به محققان در انجام تحقیقات مؤثرتر در مورد جرائم اینترنتی انجام شد. واحد جرائم پیشرفته پلیس بین‌الملل از طریق همکاری بین پلیس، بخش صنعت و دانشگاه، همکاری بین کشورهای عضو را تسهیل می‌کند. همچنین در صورت حمله سایبری و تحقیقات مربوط به جرائم اینترنتی، از طریق خدمات تحقیقاتی و پایگاه داده، به کشورهای عضو کمک می‌کند (۸).

از دیدگاه دیوان بین‌المللی کیفری نیز باید گفت: اگرچه پیش‌نویس معاهده رم مقرراتی در زمینه تعریف تروریسم، استناد به معاهدات ضد تروریسم و جرم‌انگاری آن وجود اشت و اسپانیا نیز طرحی را جهت درج تروریسم در معاهده رم ارائه داده بود که متعاقب آن نیز هند، الجزایر، ترکیه و سریلانکا طرحی را برای بازگرداندن تروریسم به وضع قبلی به عنوان یک جرم در حیطه صلاحیت موضوعی دیوان بین‌المللی کیفری ارائه نمودند، اقدامات دیگری نیز تحت عنوان جنایت علیه بشریت صورت گرفت، اما بدان علت که تنها مصادیقی از تروریسم در آستانه شدت جنایت علیه بشریت قرار می‌گیرند، حذف شد (۲۴)، اما در نهایت اساسنامه دیوان بین‌المللی کیفری، به دلیل فقدان تعریف جامع از تروریسم این جرم از صلاحیت ذاتی دیوان حذف گردید. در کامپالا هم سخنی از تروریسم به میان نیامد. گویا جرائم تروریستی به قدر کافی خطیر پنداشته نشدند که محاکمه از طریق یک دیوان بین‌المللی را الزامی کنند. نبود اجماع دولت‌ها در خصوص تبیین اقدامات تروریستی و نزدیکی آن با اقدامات سازمان‌های آزادی بخش نیز مزید بر علت گردیده است.

گذشته از سازمان‌ها، دولت‌ها نیز به عنوان تابعان حقوق بین‌الملل اقداماتی را در جهت همکاری با نهادها و سازمان‌ها و اجرای قواعد نظام‌مند در راستای مبارزه با تروریسم سایبری در دستور کار خود قرار داده‌اند. همکاری دولت‌ها با گروه تخصصی کارشناسان ملل متحد برای بررسی جرائم سایبری در دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد، تقویت ظرفیت‌های ملی قانون‌گذاری و سازمانی در مبارزه با شیوه‌های متعدد جرائم سازمان‌یافته فراملی در فضای سایبری مانند پولشویی، تأمین مالی تروریسم، قاچاق انسان، قاچاق مهاجران و ترغیب همکاری‌های مؤثر بین‌المللی از توفیقاتی است که این همکاری‌های نظام‌مند در پی داشته‌اند.

۳-۲. همکاری و اقدام در راستای جرم‌انگاری تروریسم سایبری:

اصطلاح تروریسم سایبری در راستای جرم‌انگاری آن اهمیت دارد و از تعاریف بسیار موسع تا متمرکز متفاوت است. اگر تعریف مضیق مد نظر باشد، بسیاری از عناصر حملات سایبری در مقیاس بزرگ را از بین خواهد برد، در مقابل، یک تعریف بسیار گسترده شامل بسیاری از عناصر جرائم سایبری واقعی در مقوله تروریسم سایبری می‌شود، اما در حقیقت، در میان تعاریف بی‌شماری که برای تروریسم سایبر وجود دارد،

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

برخی اشتراکات وجود دارد که می‌تواند در درک ما از موضوعات مربوط به تروریسم سایبر نقش داشته باشد. تروریسم سایبری به عنوان نسخه جدیدی از فعالیت‌های تروریستی و جرم قدیمی تروریسم توصیف شده است که با استفاده از فناوری‌های جدید انجام می‌شود. گروه‌های تروریستی از حملات متعارف قدیم به حملات سایبری تبدیل شده‌اند. آن‌ها می‌توانند حملات خود را از مسافت‌های دور انجام دهند و از مرزها و موانع فیزیکی چشم‌پوشی کنند. با این وجود، نتیجه چنین جرائمی می‌تواند بسیار بیشتر از روش‌های سنتی باشد و می‌تواند عواقب سنگین‌تری نسبت به تروریسم متعارف داشته باشد. این امر به این دلیل است که حمله تروریستی قدیمی به مجاورت خاصی محدود می‌شود، در حالی که تروریسم سایبری با استفاده از رایانه‌ها و از طریق اطلاعات یک شبکه، به طور بالقوه قادر به انجام حملات سایبری در بیش از یک منطقه وسیع در منطقه‌ای دورتر از محل حمله است. ماهیت اینترنت این امکان را به کاربر می‌دهد تا هویت خود را پنهان کند که منجر به مشکلات اصلی در تعیین کشورهای مبدأ و مقصد می‌شود و باعث شکست در جلوگیری از حملات می‌گردد. بنابراین دولت‌ها برای به اشتراک‌گذاشتن اطلاعات به منظور شناسایی مهاجمین باید با یکدیگر همکاری کنند.

سرانجام، از نکاتی که در بالا ذکر شد، نتیجه گرفته می‌شود که تروریسم سایبری یک جرم بین‌المللی است و واکنش به چنین جرمی نیز باید بین‌المللی باشد. ماهیت فراملی جرائم تروریسم سایبر منجر به پیچیدگی قضایی می‌شود و به دلیل دشواری ناشی از پیگرد قانونی و تحقیق، کشوری که مورد حمله قرار گرفته برای جستجوی عدالت در مورد خسارات وارده، از قوانین بین‌المللی استفاده می‌کند.

جرم‌انگاری تروریسم سایبری در اقدامات تابعان حقوق بین‌الملل مورد توجه بوده است. اسناد جهانی، اگرچه شامل تعریف تروریسم سایبری نیستند، اما وظایفی را برای دولت‌های عضو ایجاد می‌کنند که جرائم مورد نظر را در قانون داخلی خود (یعنی عناصر مادی و معنوی جرم) جرم‌انگاری و مکانیسم‌های همکاری بین‌المللی را نیز فراهم کنند که کشورهای دیگر نیز قادر باشند برای پیگرد قانونی یا استرداد متهم با آنان مشارکت کنند. برخلاف برخی دیگر از رژیم‌های حقوقی بین‌المللی، از جمله رژیم‌های حاکم بر حقوق بشر و درگیری‌های مسلحانه، در حال حاضر هیچ پیمان بنیادی یا رژیم حقوقی جامع برای تروریسم سایبری و مبارزه با آن وجود ندارد. گرچه رژیم حقوقی چندجانبه کنونی، دولت‌ها را قادر به پاسخگویی به اشکال موجود تروریسم کرده است، اما بسیاری معتقدند که این امر با تصویب پیمان چندجانبه، تقویت خواهد شد. مطمئناً دستیابی به توافق جهانی در مورد چگونگی تعریف تروریسم، می‌تواند به افزایش انسجام و اطمینان بین‌المللی با رویکرد حاکمیت قانون کمک کند.

تلاش اولیه برای توافق در مورد تعریف جهانی از تروریسم در چارچوب معاهده بین‌المللی و نیز ایجاد یک دادگاه بین‌المللی جنایی، کنوانسیون پیشگیری و مجازات تروریسم ۱۹۳۷ می‌باشد که به دنبال تعریف تروریسم به عنوان یک جرم بین‌المللی بود. در سال ۲۰۰۰، هند به طور غیر رسمی پیش‌نویس متن کنوانسیون جامع مبارزه با تروریسم را به کمیته ویژه تروریسم بین‌المللی منتشر کرد و از آن زمان، کشورهای عضو در حال مذاکره درمورد متن پیش‌نویس کنوانسیون جامع تروریسم بین‌المللی (کنوانسیون جامع) هستند. این متن شامل موارد زیر است: اهمیت جرم‌انگاری جرائم تروریستی، مجازات آن‌ها بر اساس قانون و درخواست تعقیب عاملان یا استرداد متهمان، لزوم از بین‌بردن قوانینی که استثنائات مجرمانه‌ای را در زمینه‌های سیاسی، عقیدتی، نژادی، قومی یا مذهبی ایجاد می‌کنند، فراخوان جدی برای کشورهای عضو برای انجام اقدامات پیشگیری از اقدامات تروریستی، تأکید بر لزوم همکاری کشورهای عضو، همکاری، تبادل اطلاعات و ارائه بیشترین کمک‌های پلیس و قضایی به منظور پیشگیری، تحقیق و پیگرد اقدامات تروریستی.

پیش‌نویس کنوانسیون جامع توسط استراتژی جهانی مبارزه با تروریسم سازمان ملل متحد به رسمیت شناخته شده است. طبق ماده ۲ پیش‌نویس در مورد اقدامات سایبری آمده است: اقدامات زیر تروریستی به حساب می‌آید:

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

۱ـ مرگ یا جراحت جدی بدنی برای هر شخص یا ۲ـ ایراد خسارت جدی به املاک عمومی یا خصوصی، از جمله اماکن دولتی یا تأسیسات دولتی، سیستم حمل و نقل عمومی، تأسیسات زیربنایی یا محیط زیست یا ۳ـ خسارت به املاک، اماکن، امکانات یا سیستم‌های مذکور در بند ۱(ب) این ماده که منجر به خسارت اقتصادی بزرگی خواهد شد. هنگامی که هدف از این رفتار، براساس ماهیت یا زمینه آن، ارعاب یک جمعیت یا وادارکردن دولت یا سازمان بین‌المللی برای انجام یا خودداری از انجام هرگونه عمل باشد.

استراتژی از دولت‌ها می‌خواهد بدون هیچ‌گونه تأخیر در اجرای کنوانسیون‌ها و پروتکل‌های بین‌المللی موجود علیه تروریسم، همه تلاش خود را برای دستیابی به توافق برای کنوانسیون جامع درباره تروریسم بین‌المللی انجام می‌دهند. پیش‌نویس کنوانسیون جامع از لحاظ ارتباط با ابزارهای جهانی موجود، مانند چتر سایر معاهدات را دربر خواهد گرفت و خلأهای موجود را پر می‌کند، قوانین ملی شفافیت بیشتری در جرم‌انگاری‌های تروریستی خواهند یافت و نگرانی‌های کمیته حقوق بشر سازمان ملل و گزارشگر ویژه در زمینه ترویج و حمایت از حقوق بشر و آزادی‌های اساسی در رعایت حقوق بشر ضمن مقابله با تروریسم بر طرف خواهد شد. با این وجود، دستیابی به توافق نهایی برای تعریف تروریسم به دلیل عدم توافق در مورد استثنائات تعقیب قضایی، مانند اعمال ارتکابی در اقدامات نهضت‌های آزادی بخش، با چالش مواجه است. مانع دیگر نحوه تعریف تروریسم و جرائم تروریستی، به ویژه در رابطه با حق تعیین سرنوشت و همچنین مبارزات و گروه‌ها در همین حوزه است. در اینجا تنش اصلی بین این دولت‌ها و سایر بازیگرانی است که می‌خواستند پیش‌نویس کنوانسیون در این زمینه بدون هیچ‌گونه استثنایی فراگیر شود.

در سال ۲۰۱۱، دستیابی به توافق برای تعریف جهانی از تروریسم به بن‌بست رسید، کمیته ششم مجمع عمومی به طور موقت مذاکرات را تا سال ۲۰۱۳ به طور موقت به تعویق انداخت. کمیته دوباره آغاز به کار نمود، اما یک بار دیگر بدون پیشرفت ملموس در رسیدن به توافق، به شکست برخورد. مجمع عمومی در قطعنامه سال ۲۰۱۶ خود بار دیگر تشکیل کارگروه با هدف نهایی‌کردن متن پیش‌نویس کنوانسیون در دستور کار قرار داد، اما نهایتاً سرانجام این توافقنامه مبهم است (۲۵).

با توجه به عدم توفیق در تعریف تروریسم سایبری باید گفت پیرامون جرم‌انگاری تروریسم سایبری، البته تلاش‌هایی در میان سازمان‌های بین‌المللی و منطقه‌ای صورت گرفته است که به نظر می‌رسد در میان آن‌ها شورای اروپا از همه موفق‌تر عمل کرده است.

شورای اروپا، از دهه ۱۹۷۰ خود را به مبارزه با تروریسم آغاز نموده است. به دنبال افزایش حملات تروریستی فعالیت شورای اروپا در نبرد علیه تروریسم در سه حوزه متمرکز گردید: ۱ـ تقویت اقدامات حقوقی علیه تروریسم؛ ۲ـ پاسداری از ارزش‌های اساسی؛ ۳ـ پرداختن به علل تروریسم. هدف اقدامات شورای اروپا افزایش اثربخشی اسناد بین‌المللی موجود در زمینه مبارزه با تروریسم و تقویت تلاش‌های کشورهای عضو برای جلوگیری از تروریسم است. دو راه برای دستیابی به این هدف تعیین شده است: اول، اعمال خاصی مانند تحریک عمومی و عضوگیری، جرم‌انگاری شود؛ راه حل دوم جلب همکاری‌ها در سطح ملی و بین‌المللی است. در این راستا کمیته تخصصی اروپاییِ شورای اروپا در مورد جرائم در فضای سایبری در سال ۱۹۹۷ برای رسیدگی به مشکل قانون آیین دادرسی کیفری مرتبط با جرائم سایبری با فناوری اطلاعات و همکاری بین‌المللی ایجاد شد. تدوین کنوانسیون جرائم سایبری ۴ سال به طول انجامید تا سرانجام به عنوان نخستین سند برای ایفای نقش واسط، جهت کنترل بین‌المللی جرائم مربوط به حوزه سایبر، هماهنگ‌سازی اقدامات و همکاری‌های بین الدولی و روندهای کشف جرم شناخته شد. این کنوانسیون به جهت لحاظ ملاحظات حقوق بشر در مبارزه با تروریسم منحصر به فرد است و می‌تواند در حوزه مبارزه با تروریسم سایبری نیز کارایی داشته باشد، مانند آنچه در ماده ۵ در مورد منع تحریک عمومی در ارتکاب جرائم تروریستی آمده است. جرائم طبق کنوانسیون جرائم سایبری به چهار

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

دسته تقسیم می‌شوند: ۱ـ جرائم علیه محرمانگی، تمامیت، در دسترس بودن؛ ۲ـ جرائم مربوط به رایانه؛ ۳ـ جرائم مرتبط با محتوا؛ ۴ـ جرائم مربوط به نشر و حقوق مربوط به آن (۲۶). این کنوانسیون در پی دنبال‌کردن یک سیاست جنایی مشترک برای محافظت از جامعه در برابر تهدید سایبری است. در زمان پیش‌نویس کنوانسیون دغدغه اصلی تهیه‌کنندگان این بود که یک تعریف انعطاف‌پذیر که توانایی انطباق با جرائم جدید را داشته و فناوری‌های جدید در زمینه جرائم سایبری مانند تروریسم سایبری را دربر گیرد، لحاظ شود، اگرچه این امر با مشکلی اساسی مواجه شد و آن اصرار دولت‌ها برای جرم‌انگاری طبق حقوق داخلی‌شان و تفاوت‌های دیدگاه‌های سیاسی در مسائلی مانند حقوق بشر، حفاظت از داده‌ها و آزادی بیان بود. بنابراین تهیه‌کنندگان پیش‌نویس جزئیات را برای حصول تصویب حداکثری کنوانسیون کنار نهادند (۹).

شورای اروپا در طی سال‌های فعالیت خود بیش از ۲۰۰ کنوانسیون و توافقنامه دوجانبه در موضوعات متنوع ایجاد کرده است که کنوانسیون بوداپست در مورد جرائم سایبری مهم‌ترین ابتکار آن تلقی می‌گردد، زیرا اولین تلاش برای هماهنگ‌کردن قوانین سایبری است. این کنوانسیون به عنوان یک راهنما برای کشورهایی که در حال توسعه قانونگذاری ملی جامع خود پیرامون جرائم سایبری هستند و نیز یک چارچوب برای همکاری‌های بین‌المللی به کشورهای عضو ارائه می‌دهد. کنوانسیون، پروتکلی پیرامون دشمن هراسی و نژادپرستی از طریق سیستم‌های کامپیوتری نیز دارد. شورای اروپا خود، رهنمودهای در زمینه تفسیر کنوانسیون بوداپست و برنامه‌های مختلف ظرفیت‌سازی ارائه می‌دهد. در کنوانسیون، جرم‌انگاری برخی رفتارهای مرتبط با سیستم‌های رایانه‌ای، وضع آیین دادرسی جهت تحقیق و تضمین دسترسی‌پذیری آن‌ها برای مجریان قانون داخلی برای تحقیق درباره جرم‌های سایبری از جمله آین دادرسی در تحصیل ادله الکترونیک و ایجاد یک نظام همکاری بین‌المللی گسترده برای اهدافی همچون کمک برای استرداد مرتکبان جرائم مندرج در کنوانسیون شورای اروپا درج شده است (۱۶). به علاوه کمیسیون اروپا مقرراتی را تدوین نموده است که به موجب آن کلیه اعضای اتحادیه اروپا موظف هستند تمامی فعالیت‌هایی که تحت عنوان حمله برای تداخل در سیستم‌های ارتباطی تعریف می‌شود، چنانچه هدف آن‌ها تغییر یا تخریب جدی ساختارهای سیاسی، اقتصادی یا اجتماعی باشد را به مثابه عمل تروریستی، قابل مجازات بدانند.

اما راه حل دیگر، تمهید رسیدگی به جرائم تروریسم سایبری با توسل به صلاحیت جهانی است. این صلاحیت برای جرائم جدی هستند اعمال می‌شود که از دو طریق تحت صلاحیت جهانی قرار دارند: اول، ماهیت و مقیاس جرم که شامل نقض شدید قوانین بشردوستانه است؛ دوم، به دلیل ناکافی‌بودن قوانین توسط ملل درگیر، این جنایات در مناطقی صورت می‌گیرد که مشمول اختیارات هیچ دولتی نیستند. صلاحیت جهانی ممکن است توسط نظام معهدات بین‌المللی یا عرف بین‌المللی ایجاد شود. نظام معاهدات بین‌المللی برای کشورهایی طرف معاهده، الزام‌آور است. با این حال، در برخی شرایط، آن‌ها به عنوان مدرکی برای وجود عرف حقوق بین‌الملل عمل می‌کنند. اصل کلی صلاحیت جهانی به جامعه بین‌المللی در حوزه‌های قضایی مقرر اجازه می‌دهد که قوانین ملی را با قوانین بین‌المللی جایگزین کنند. صلاحیت جهانی برای تروریسم سایبری به عنوان یک امر موضوعی حقوق بین‌الملل عرفی تعیین شده است. حقوق بین‌الملل عرفی شامل اعتقاد به الزام حقوقی و رویه دولت‌ها است. تروریسم در تعدادی از معاهدات مطرح شده است و معاهدات بی‌شماری انواع مختلف تروریسم را به رسمیت شناخته است. آن‌ها پذیرفتند که تروریسم سایبری عموماً نوعی تروریسم است، با وجود این واقعیت که آن‌ها از تروریسم سایبری منحصراً یاد نمی‌کنند. همچنین تروریسم سایبری جنایت علیه بشریت تلقی می‌شود. بنابراین این دو عنصر عرف حقوق بین‌الملل و رویه دولت‌ها برای اقدام علیه تروریسم و مبحث تروریسم در صلاحیت جهانی مناسب هستند. جنایات علیه بشریت، مانند نسل‌کشی و دزدی دریایی، با اعمال صلاحیت جهانی مورد رسیدگی قرار می‌گیرند. ماهیت فجیع تروریسم سایبری به عنوان نوعی جدید از تروریسم می‌تواند، تروریسم سایبری را در حوزه صلاحیت جهانی قرار می‌دهد. بنابراین بر اساس اصل

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

صلاحیت جهانی، این جرائم از آنجا که اگر توسط یک کشور یا نماینده‌ای از کشور اتفاق بیفتند، ممکن است بدون مجازات بمانند، در حوزه صلاحیت جهانی هستند. در این راستا، با توجه به ماهیت تروریسم سایبری که یک امر فراملی است و این واقعیت که صلاحیت جهانی بهترین روش برای اعمال (قانون) در مبارزه با تروریسم سایبری است، پاسخ مناسب به موضوعات تروریسم سایبری باید بین‌المللی باشد. با همین اشاره، تلاش‌های سازمان‌های بین‌المللی علیه تروریسم سایبر باید بر اساس صلاحیت جهانی اعمال شود (۲۵).

کشورها می‌توانند با استناد به صلاحیت جهانی به تعقیب مجرمان سایبری نیز بپردازند. امروزه اشتراک نظر زیادی در مورد برخی مصادیق جرائم سایبری شکل گرفته، مانند هرزه‌نگاری کودکان، پول‌شویی الکترونیکی و نشر تروریستی ویروس. به زعم برخی بهترین شکل صلاحیت در این فضا همین صلاحیت جهانی است که نیاز به انعقاد کنوانسیون بین‌المللی یا قانونگذاری داخلی در این خصوص دارد. ماده ۲۲ کنوانسیون جرائم سایبری به این نوع صلاحیت اشاره دارد (۲۷).

رویه دولت‌ها نیز در پرتو اسناد بین‌المللی موجود درخور توجه است، به عنوان مثال در عملکرد دولت‌ها نیز تلاش‌هایی در راستای استفاده از کنوانسیون بوداپست به عنوان یک دستورالعمل دیده می‌شود. در قوانین استرالیا جرمی تحت عنوان تروریسم سایبری وجود ندارد، اما طبق قوانین کشورهای مشترک‌المنافع جرائمی جرم‌انگاری شده که می‌توانند بر اقدامات تروریستی در محیط سایبری نیز اعمال شوند. علاوه بر این قوانین که در حوزه صلاحیت قانونگذاری مشترک‌المنافع می‌باشد، مقررات خاص دولتی در مورد کشف و رویه‌های جنایی در ارتباط با جرائم تروریستی وجود دارد. کنوانسیون بوداپست نیز به عنوان یک دستورالعمل مورد استفاده قرار می‌گیرد. در مورد هماهنگ‌سازی قوانین ماهوی، هماهنگ‌سازی رویه‌های مربوط به کشف جرم و نیز تسهیلاتی در مورد معاضدت‌های دوجانبه این کنوانسیون مقرراتی دارد که لازمه آن انتقال قوانین مربوطه از کنوانسیون جرائم سایبری به قوانین ملی است (۲۸).

بنابراین پس از همکاری‌ها و تلاش‌ها در راستای جرم‌انگاری تروریسم سایبری، در قالب اسناد بین‌المللی، منطقه‌ای یا قوانین داخلی، آنچه اهمیت می‌یابد شکل اجرای این مقررات و قوانین و نیز میزان کارآمدی آن‌ها است، که خود به صورت مفصل موضوع پژوهش دیگری می‌تواند باشد.

نتیجه‌گیری

تروریسم سایبری نقطه تلاقی تروریسم و جرائم سایبری است، بنابراین ویژگی‌های مخرب هر دو گروه را داراست، لذا مبارزه با آن در گام اول در وضع قواعد برای مبارزه همه‌جانبه نیاز به همکاری همه‌جانبه دولت‌ها و بازیگران غیر دولتی دارد. هر بار تصمیمات قانونی در بعد داخلی برای قاعده‌مندکردن تکنولوژی سایبری اتفاق می‌افتد، بلافاصله پس از آن مسأله پیشرفت تکنولوژی، جلوه‌ای نوظهور از خود را به نمایش گذاشته و مشکل از نو آغاز خواهد شد. بنابراین همکاری و اقدام در سطح بین‌المللی نظاماتی را به دست می‌دهد که می‌تواند در اجرای قوانین داخلی و قواعد بین‌المللی و نیز کشف جرم و تعقیب مجرمان مؤثر واقع شود. محققان دریافته‌اند که مسأله امنیت اطلاعات ماهیتاً به طور اجتناب‌ناپذیری جهانی است. قضات و مأموران اجرای قانون نیز بر این باورند که وسایل در دسترس برای کشف جرم و تعقیب اقدامات تروریست‌ها از طریق رایانه یا اینترنت، در حال حاضر تنها ملی و محلی است، بنابراین چالش پیش رو این است که تکنولوژی را که ارتباطات را در کسری از ثانیه میان قاره‌ها و کشورها تسهیل می‌کند، با استفاده از ابزار کشف جرم و قوانین ملی و صلاحیت قضایی درون مرزی قاعده‌مند نمود.

به هر حال باید گفت هم در بعد داخلی، جرم‌انگاری و کشف جرم و مجازات تروریست‌ها اهمیت می‌یابد و هم در بعد بین‌المللی مبارزه همه‌جانبه از طریق همکاری و معاضدت بین‌المللی صورت می‌پذیرد. کنوانسیون‌های بین‌المللی برای افزایش امنیت در برابر جرائم سایبری و تروریسم توصیه

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

کرده‌اند که بالاترین سطح همکاری چندجانبه در این حوزه لازم است. همان‌گونه که تصمیم‌سازی و قانونگذاری شایسته در سطح داخلی در کشورها اهمیت دارد، مبارزه همه‌جانبه از طریق همکاری چندجانبه مؤثر خواهد بود. بنابراین توافق کلی باید بر سر این مسأله باشد که چه نوع همکاری باید در مورد مبارزه با جرائم سایبری و تروریسم صورت گیرد.

در این راستا کشورها باید دائماً راهبردهای همکاری خود را اصلاح کنند تا به رویکردهای هماهنگ جهت اجرای قواعد و قوانین مبارزه با تروریسم سایبری و مجازات مجرمین دست پیدا کنند. مهم‌ترین شکل همکاری بین‌المللی، همکاری میان سازمان‌های تصمیم‌ساز و سپس مجری قانون است که مستلزم تلاش‌های ملی جهت پیروی از استانداردهای بین‌المللی جدید و تقویت همکاری در سطح بین‌المللی است. از آنجایی که محاکمه متهمین تروریسم در صلاحیت هیچ محکمه بین‌المللی نیست، احضار مرتکبان صرفاً بر دوش دادگاه‌های داخلی است، اما چون عملیات ضد تروریسم به ویژه در تروریسم سایبری، ماهیت و حوزه‌ای بین‌المللی دارد، جمع‌آوری مدارک و شواهد همکاری نزدیک دولت‌ها را طلب می‌کند. اسناد بین‌المللی ضرورت همکاری برای امحا بی‌کیفری که متهمان به تروریسم در مرزهای یک کشور برای خود پدید می‌آورند را بیش از پیش نمایان می‌کند. اقدامات تابعان حقوق بین‌الملل در این حوزه نیز شایان ذکر است.

برخلاف آنچه در ابتدا به نظر می‌رسید در اقدامات صورت‌گرفته توسط سازمان‌های بین‌المللی جهت جلب همکاری با توجه به پراکندگی اقدامات سازمان ملل به علت بررسی موضوع در بسیاری از نهادهای مختلف بین دولتی و بسترهای سازمانی آن و اینکه تاکنون هیچ قطعنامه‌ای در رابطه با مسائل مربوط به امنیت سایبری توسط شورای امنیت سازمان ملل به تصویب نرسیده است. عدم توفیق سازمان در تحقق اجماعی بر سر تعریف تروریسم و شکل‌گیری معاهده‌ای همه‌جانبه جهت مبارزه با تروریسم سایبری، مزید بر علت است تا سازمان‌های منطقه‌ای با رویکردهای نظامی و امنیتی با پشتوانه تحقیقاتی با ارائه راهکارهای عملی و یکپارچه‌نمودن رویکردها نسبت به سازمان ملل، موفقیت بیشتری در مبارزه با تروریسم سایبری داشته باشند.

باید افزود، فعالیت‌های سازمان ملل متحد در مورد امنیت سایبری بسیار پراکنده به نظر می‌رسد، همکاری‌های بین‌المللی در این راستا از همکاری در وضع قواعد ضد تروریسم سایبری آغاز و به همکاری در اجرای قانون و تلاش برای هماهنگی اقدامات ملی با تعهدات بین‌المللی ختم می‌شود. قانونگذار در حوزه قانونگذاری ملی نیز باید عدم نقض حقوق بشر و آزادی‌های بنیادین را همزمان با مبارزه با تروریسم سایبری تضمین نماید. اینترنت به عنوان بستر جدیدی برای ابراز حقوق اساسی بشر می‌باشد. شورای حقوق بشر سازمان ملل متحد تأیید کرد که همان حقوقی که مردم به صورت آفلاین دارند باید از طریق اینترنت نیز محافظت شوند، به این ترتیب اعلامیه‌های حقوق بشر، در اینترنت قابل اجرا است.

از بررسی مجموعه اقدامات سازمان ملل، سازمان‌های منطقه‌ای و گروه‌ها در حوزه وضع قواعد جهت پیشگیری و مبارزه با تروریسم سایبری می‌توان موارد زیر را به عنوان محورهای لازم جهت سرکوب این جرم با توجه به تفاوت دولت‌ها در میزان وابستگی آنان به فضای سایبر و آسیب‌پذیری آن‌ها و نیزکارآمدنمودن مکانیسم‌های موجود، پیشنهاد نمود:

ـ سازمان ملل متحد به عنوان مرکز هماهنگی همکاری‌های بین‌المللی، نقش خود را با اعمال اصلاحات به ویژه در زمینه ضمانت اجراهای سازمانی در مبارزه با تروریسم سایبری باز یابد.

ـ اسناد بین‌المللی همکاری‌های خود را بر مبنای اولویتِ خودداری از سازماندهی، مشارکت در تأمین مالی، تشویق یا تحمل فعالیت‌های تروریستی و اتخاذ اقدامات عملی مناسب برای اطمینان از عدم استفاده از قلمروهای مربوطه برای تأسیسات تروریستی یا اردوگاه‌های آموزشی یا آماده‌سازی یا سازماندهی اقدامات تروریستی علیه سایر کشورها یا شهروندانشان سامان دهند.

ـ تعهد دولت‌ها به عضویت بدون تأخیر در کنوانسیون سازمان ملل متحد علیه جرائم سازمان‌یافته فراملی و کنوانسیون‌های

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

ضد تروریسم و اجرای آن‌ها و تقویت هماهنگی و همکاری بین کشورها در زمینه مبارزه با جرائمی که ممکن است با تروریسم در ارتباط باشد.

ـ همکاری کامل در ایجاد اطمینان از دستگیری و تعقیب یا استرداد مجرمین اقدامات تروریستی، مطابق با مقررات مربوط به حقوق ملی و بین‌المللی، به ویژه حقوق بشر، حقوق پناهندگان و حقوق بشردوستانه بین‌المللی.

ـ تعهد به تقویت همکاری بین دستگاه‌های اجرای قانون و همکاری در تبادل اطلاعات به موقع و دقیق در مورد پیشگیری و مبارزه با تروریسم سایبری مانند آنچه در نقطه تماس بین‌المللی ۲۴ ساعته و ۷ روز هفته اتفاق می‌افتد.

ـ تشویق سازمان‌های ذی‌ربط منطقه‌ای و فرعی برای ایجاد یا تقویت مکانیسم‌های ضد تروریسم و همکاری و مساعدت برای این منظور و همکاری با کمیته مبارزه با تروریسم سازمان ملل متحد و دفتر مواد مخدر و جرم و نیز پلیس بین‌الملل.

مشارکت نویسندگان

لیلا میربد: نگارش مقاله، گردآوری منابع و جمع‌آوری داده‌ها.

صادق سلیمی: مشاوره و راهنمایی در نگارش متن و اعمال اصلاحات محتوایی.

صابر نیاورانی: مشاوره و نظارت بر پیشرف مقاله و اعمال اصلاحات شکلی.

سیدقاسم زمانی: مشاوره و نظارت بر حسن انجام کار و اعمال اصلاحات.

نویسندگان نسخه نهایی را مطالعه و تأیید نموده و مسئولیت پاسخگویی در قبال پژوهش را پذیرفته‌اند.

تشکر و قدردانی

ابراز نشده است.

تضاد منافع

نویسندگان هیچ‌گونه تضاد منافع احتمالی را در رابطه با تحقیق، تألیف و انتشار این مقاله اعلام نکرده‌اند.

تأمین مالی

نویسندگان اظهار می‌نمایند که هیچ‌گونه حمایت مالی برای تحقیق، تألیف و انتشار این مقاله دریافت نکرده‌اند.

ملاحظات اخلاقی

در پژوهش حاضر جنبه‌های اخلاقی مطالعه کتابخانه‌ای شامل اصالت متون، صداقت و امانتداری رعایت شده است.

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

References

1. Kim J, Hung T. Status and requirements of counter cyber terrorism. World Academy of Science, Engineering and Technology, International Journal of Social, Behavior, Educational, Economic and Management Engineering. 2007; 1(6): 2.

2. Troein C, Acayo G. ITU Global Cyber Security Index overview. 2020. p.9. WTO Cyber Security Webinar. Available at: https://www.wto.org/english/res_e/reser_e/caroline_troein_and_grace_acoyo.pdf.

3. Delkhosh A. Combating with international crimes states obligation to cooperation. Tehran: Allameh Tabatabaei; 2010. p.145-156. [Persian]

4. Namamian P. Facing Cyber Terrorism in Criminal Law. The Journal of Communication Research. 2013; 20(73): 9-42. [Persian]

5. Namamian P, Abbasi S. A Scrutiny of the Security Council's Resolution 1373: Modification of Legal Commitments and Necessities of Combating Terrorism. Police International Studies Journal. 2013; 3(9): 149-168 [Persian]

6. Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes. Counter-Terrorism Implementation Task Force (CTITF). 2009. p.12-13.

7. Bogdanoski M, Petreski D. Cyber Terrorism-Global Security Threat. Contemporary Macedonian Defense - International Scientific Defense, Security and Peace Journal. 2013; 13(24): 59-73.

8. UNODC. The use of the Internet for terrorist purposes. New York: United Nations; 2012. p.17, 137.

9. Moslemzadeh Tehrani P, Abdul Manap N. A rational jurisdiction for cyber terrorism. Computer Law & Security Review. 2013; 29(6): 689-701.

10. Ghorbannia N. Response to Terrorism: Military, Political or Legal Approach? Journal of Comparative Law. 2004; 43: 141-168. [Persian]

11. Lewis JA, Götz N. The Cyber Index International Security Trends and Realities. New York and Geneva: UNIDIR; 2013.

12. UNODC. Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. 2013. p.64.

13. Resolution adopted by the General Assembly on 8 September 2006. 60/288. The United Nations Global Counter-Terrorism Strategy. Available at: https://www.documents-dds-ny.un.org/doc/UNDOC/GEN/N05/504/88/PDF/N0550488.pdf.

14. Prasad K. Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework. Perth: Australian Counter Terrorism Conference; 2012. p.12.

15. Brown D. UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights. Online. 2019. Available at: https://www.apc.org/en/news/un-general-assembly-adopts-record-number-resolutions-internet-governance-and-policy-mixed.

16. Available at: https://www.ccdcoe.org/research/incyder/.

17. Gehr W. The Committee against Terrorism and Security Council Resolution 1373 (2001). News and International Law. 2003; 1-11. Available at: http://www.ridi.org/adi/articles/2003/200301geh.htm.

18. Benedek W, Yotopoulos-Marangopoulos A. Anti-Terrorist Measures and Human Rights: UNESCO Chair in Human Rights, Democracy, Peace, Tolerance and International Understanding. Translated by Tila P, Afshari M, Saed MJ, Asadi T, Saed N. Tehran: Dadgostar Publications; 2010. p.66-72. [Persian]

19. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en.

20. Available at: https://www.ccdcoe.org/.

21. Available at: https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Cybersecurity-Cybercrime-Strategy-EN.pdf.

22. Available at: https://www.cto.int/strategic-goals/cybersecurity/.

23. Available at: https://www.oecd.org/digital/digital-security/.

24. Moazzami SH, Namamian P. Law of combating nuclare terrorism under international instrumens. Theran: Dadgostar publication. 2014. p.210-212. [Persian]

25. Available at: https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/treaty-based-crimes-of-terrorism.html. Treaty-based crimes of terrorism - universal counter terrorism instruments.

26. Moslemzadeh Tehrani P, Abdul Manap N, Taji H. Cyber terrorism challenges: The need for global response to a multi-jurisdictional crime. Computer Law and Security Review. 2013; 29(3): 207-215.

27. Ziaee SY. Philosophical discourse on human rights in cyber space. Online. 2009. Available at:

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.

http://www.hoghough85.blogfa.com/post/2688. [Persian]

28. Tsipas P. A Legal Response to Cyber Terrorism. Online. 2005. Available at: https://www.docplayer.net/45164141.

تمامی حقوق انتشار این اثر، متعلق به انجمن علمی حقوق پزشکی ایران است.