Original Article

Cyber Terrorism: Violation of Human Rights and Fundamental Freedoms

Leila Mirbod[1], Sadegh Salimi[2*], Saber Niavarani[3], Seyed Ghasem Zamani[4]

1. Ph.D. Student in Public International Law, Department of Public and International Law, Faculty of Divinity, Political Science and Law, Science and Research Branch, Islamic Aazad University, Tehran, Iran.
2. Associate Professor of International Law, Department of International Law, Islamic Azad University of Central Tehran branch, Tehran, Iran. (Corresponding Author) Email: sadegsalimi@yahoo.com
3. Assistant Professor of International Law, Department of Public and International Law, Faculty of Divinity, Political Science and Law, Science and Research Branch, Islamic Azad University, Tehran, Iran.
4. Associate Professor of International Law, Department of Public and International Law, Faculty of Law and Political Sciences, Allameh Tabataba'i University, Tehran, Iran.

Received: 6 Jul 2018 Accepted: 12 Jun 2019

Abstract

Cyber terrorism occurs if the critical infrastructure of a state including air transportation, dams, nuclear power plants and power generation plants, banking and financial systems are attacked politically motivated or under the ideological actions aimed at forcing the government or organizations with a variety of malware weapons, and thereby causing fear and panic. There is no a comprehensive definition of terrorism on international community and even there is no compulsory comprehensive instrument on this issue, but this new form of terrorism along with other forms such as bioterrorism, nuclear terrorism and eco-terrorism may cause harmful damages compared to the classic types of terrorism. Cyber terrorism disturbs public order and therefore it is known as violating human rights law in each of its four generations in addition to breaches of the Peace and Security. The importance of addressing human rights violations by terrorists in the cyberspace, as well as in the context of the fight against cyber-terrorism, must be taken into account in a comprehensive response to this phenomenon. The current paper is a descriptive-analytical study. Data was collected using library sources.

Keywords: Terrorism; Cyber Terrorism; Human Rights; Fundamental Freedoms; Human Rights Generations

Please cite this article as: Mirbod L, Salimi S, Niavarani S, Zamani SQ. Cyber Terrorism: Violation of Human Rights and Fundamental Freedoms. *Iran J Med Law*, Special Issue on Human Rights and Citizenship Rights 2019; 223-240.

مقاله پژوهشی

تروریسم سایبری: نقض حقوق بشر و آزادی‌های بنیادین

لیلا میربد[۱]، صادق سلیمی[۲*]، صابر نیاورانی[۳]، سیدقاسم زمانی[۴]

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

۲. دانشیار رشته حقوق بین‌الملل، گروه حقوق بین‌الملل، دانشکده حقوق، واحد تهران مرکزی، تهران، ایران. (نویسنده مسؤول)

Email: sadegsalimi@yahoo.com

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

۴. دانشیار رشته حقوق بین‌الملل، گروه حقوق عمومی و بین‌الملل، دانشکده حقوق و علوم و سیاسی، دانشگاه علامه طباطبایی، تهران، ایران.

دریافت: ۱۳۹۷/۴/۱۵ پذیرش: ۱۳۹۸/۳/۲۲

چکیده

تروریسم سایبری به عنوان گونه‌ای جدید از تروریسم، نشانگر آسیب‌پذیربودن تابعان حقوق بین‌الملل در فضای سایبر است. اگر تروریست‌ها زیرساخت‌های حیاتی یک دولت مانند حمل نقل هوایی، سدها، نیروگاه‌های هسته‌ای و تولید برق، سیستم بانکی و مالی را با انواع بدافزارها مورد حمله قرار دهند و از این طریق باعث رعب و وحشت عمومی گردند و با داشتن انگیزه‌های سیاسی یا ایدئولوژیک این اقدامات را در راستای اجبار دولت یا سازمان‌ها انجام دهند، آنگاه تروریسم سایبری محقق می‌گردد. جامعه جهانی بر سر تعریف جامعی از تروریسم، به توفیقی دست نیافته و حتی سند جامع الزام‌آوری نیز در این موضوع وجود ندارد، اما این شکل از تروریسم به همراه دیگر گونه‌های نوینی چون بیوتروریسم، تروریسم هسته‌ای و اکوتروریسم، ممکن است خسارات زیان‌بارتری نسبت به انواع کلاسیک تروریسم ایجاد کند. تروریسم سایبری تهدیدی علیه صلح و امنیت بین‌المللی است و در عین حال ناقض قواعد حقوق بشر در هر چهار نسل شناخته‌شده آن نیز به شمار می‌آید. اهمیت پرداختن به نقض حقوق بشر توسط تروریست‌ها در فضای سایبر و نیز در سیاق مبارزه با تروریسم سیابری در مقابله همه‌جانبه با این پدیده باید مطمح نظر قرار گیرد. مقاله حاضر بر پایه روش تحقیق از حیث گردآوری اطلاعات توصیفی و کتابخانه‌ای و از نظر هدف توسعه‌ای است.

واژگان کلیدی: تروریسم؛ تروریسم سایبری؛ حقوق بشر؛ آزادی‌های بنیادین؛ نسل‌های حقوق بشر

مقدمه

اولین مورد از خطر جدی تروریسم سایبری در سال ۲۰۰۷ در استونی علیه وب‌سایت‌های مهم دولتی صورت گرفت. در آن زمان اشتراک نظر بر دست‌داشتن روسیه در این حمله بود که البته هرگز اثبات نگردید. صرف نظر از این‌که چه دولتی مسؤولیت دارد، آنچه اهمیت دارد، این است که اتفاق مورد بحث اولین مورد یک حمله وسیع سایبری علیه یک کشور بود و به همین جهت این مسأله را بیش از پیش مورد توجه قرار داد که روزی بقیه کشورهای ممکن است بسیار شدیدتر از آنچه استونی از تروریسم سایبری متحمل شده، آسیب ببینند. تروریسم سابقه طولانی دارد و با پیشرفت تکنولوژی به حوزه‌های جدیدی نیز وارد شده است. امروزه تروریسم هسته‌ای، بیولوژیک و سایبری ممکن است تلفات جانی و آسیب‌های مالی به مراتب بیشتری نسبت به انواع سنتی تروریسم در پی داشته باشند. برخی تروریسم سایبری را در زمره جرائم سایبری طبقه‌بندی نموده‌اند و بر این اعتقادند که این امر در مبارزه با بی‌کیفری، مؤثر عمل خواهد نمود، اما با توجه گسترش روزافزون این پدیده و مشخصه‌های آن، مبارزه همه‌جانبه در پرتو همکاری‌های بین‌المللی با این پدیده شوم و انواع مدرن آن در سیاق مبارزه با تروریسم ضرورت می‌یابد. ضرورت مبارزه با تروریسم در چند حوزه جدی حقوق بین‌الملل نمود پیدا می‌کند. تروریسم مخل نظم و امنیت بین‌المللی، صلح و حقوق بشر است و بسیاری از انواع آن با حوزه‌های کلاسیک حقوق مخاصمات مسلحانه و حقوق بشر دوستانه، به سختی قابل انطباق هستند. اقدامات تروریستی به طور جدی حق بهره‌مندی انسان از حقوق بشر را مختل نموده، توسعه اجتماعی و اقتصادی دولت‌ها را تهدید و ثبات جهانی را تضعیف می‌نماید.

امروزه با وابستگی زیرساخت‌های حیاتی دولت‌ها در بخش‌هایی چون سیستم‌های کنترل حمل و نقل هوایی، شبکه‌های مخابراتی، برق، آب، بهداشت و حتی پلیس و آتش نشانی، حملات سایبری ممکن است اقتصاد، نظام آموزش و سلامت یک کشور را نابود سازد و اکثر جمعیت آن کشور را از خدمات پایه‌ای محروم سازد. هک یک وب‌سایت حتی ممکن است باعث تخلیه یک شهر در اثر نشت مواد شیمیایی یا زیر آب سد رفتن یک روستا شود. این پیام‌ها اگر در شبکه‌های اجتماعی انتشار یابد موجب رعب و وحشت جمعیت غیر نظامی خواهد گردید و مسلماً تلفات و خسارات مالی و جانی زیادی در پی خواهد داشت. بنابراین حمله به زیرساخت‌های اطلاعاتی در جهت اهداف تروریستی دور از ذهن نیست.

این مقاله در پی پاسخگویی به این سؤال است که با توجه به برداشت‌های متفاوتی که از مفهوم تروریسم سایبری وجود دارد، آیا این جرم می‌تواند ناقض و یا تهدیدکننده حقوق بشر تلقی شود و اگر پاسخ مثبت است در چه حوزه‌هایی حقوق بشر را نقض نماید و آیا ممکن است مصداق جنایت علیه بشریت باشد؟

آنچه در بدو امر مهم به نظر می‌رسد، این است که حقوق بشر و تروریسم سایبری در دو حوزه با یکدیگر ارتباط می‌یابند، اول ضرورت مبارزه همه‌جانبه با تروریسم توسط قانونگذار، مجریان قانون و نهادهای بین‌المللی به مثابه ناقض و تهدید کننده حقوق و آزادی‌های بنیادین که با توجه به نوین‌بودن این پدیده، بحث در مورد چگونگی نقض این حقوق بیشتر ناظر به آینده است؛ دیگری لزوم رعایت حقوق بشر در سیاق مبارزه با تروریسم سایبری که البته از بحث ما خارج است. بنابراین این پژوهش ابتدا به تعریف تروریسم سایبری پرداخته و سپس به عنوان ناقض حقوق بشر و آزادی‌های بنیادین در چهار نسل شناخته‌شده حقوق بشر با ذکر مثال‌هایی بررسی شده است.

تروریسم سایبری: ماهیت و تعریف

اصطلاح تروریسم سایبری در ۱۹۹۷ توسط بری کالین (Barry C. Collin) محقق ارشد موسسه حفاظت اطلاعات در کالیفرنیا ابداع شد و این‌گونه تعریف گردید: «سوءاستفاده عمدی از یک سیستم، شبکه یا مؤلفه اطلاعاتی رایانه‌ای برای تحقق هدفی که مؤید یا تسهیل‌کننده اقدام تروریستی باشد.» پس از آن این مفهوم بارها و بارها توسط محققان در حوزه‌های حقوق، فناوری اطلاعات و علوم ارتباطات تعریف شد و گاهی با مفاهیم مشابه نیز امتزاج یافت (۱).

اما اختلاف نظر در مورد این‌که چه اقداماتی تروریسم سایبری است، گسترده است، حتی برخی استدلال کرده‌اند چیزی به نام تروریسم سایبری وجود ندارد و اگر هم باشد، ناظر به آینده است.

با توجه به مؤلفه‌های تشکیل‌دهنده فضای سایبر که عبارتند از سامانه‌های ارتباطی چون ماهواره، ناقل‌های داده، سیستم‌های تلفنی و تلفن‌های همراه، شبکه‌های رایانه‌ای و بالاخره ارائه‌دهندگان خدمات اینترنتی (شامل سه دسته واسطه‌های انتقال ارتباطات، شامل ایجادکنندگان نقطه تماس بین‌المللی، رساها (ISP) و کافی‌نت‌ها، دسته دیگر تأمین کنندگان فضای شبکه و بالاخره سرویس‌دهندگان نام دامنه می‌باشند) (۲) و ویژگی‌هایی مانند امکان انجام اقدامات تروریستی با کم‌ترین هزینه، ایراد تلفات و خسارت بدون نیاز به سلاح خاص، گمنامی و مخفی‌بودن عملیات تروریستی، کنترل‌ناپذیربودن فضای سایبر و کم‌تربودن احتمال کشف عملیات و دستگیری، جهانی‌بودن و امکان انجام عملیات در کسری از ثانیه با ایجاد خسارات شدیدتر از تروریسم سنتی، فضای سایبر از چنان اهمیتی برای تروریست‌ها برخوردار شده که از کلیه فرصت‌های موجود در آن مانند استفاده از بدافزارها، تروژان‌ها، ویروس‌ها و کرم‌های اینترنتی برای قطع سرویس یا اختلال در آن و سرقت داده‌ها برای مقاصد خود استفاده می‌کنند (۳).

برخی دیگر تروریسم سایبری را حاصل تلاقی فضای سایبر و مقوله تروریسم می‌دانند و ماهیتی متفاوت از جرائم سایبری برای آن در نظر گرفته و معتقدند از آنجایی که حوزه‌های مختلفی از حقوق بین‌الملل را به چالش می‌کشد، اعمال قواعد کلاسیک در مبارزه با آن را ناکافی است. در نظریه دیگر تروریسم سایبری نوعی حمله سایبری قلمداد شده و این باور وجود دارد که تاکنون اقدامی که مصداق تروریسم باشد، در حوزه سایبر رخ نداده است. این دسته معتقدند حملات سایبری یا به شکل جرم سایبری قابل پیگرد هستند یا اگر به سطح حمله مسلحانه برسند، در حوزه حقوق مخاصمات مسلحانه قابل بحث خواهند بود.

از آنجایی که تروریسم با چالش عدم وجود اجماع بر سر تعریف از آن مواجه است، بنابراین باید به ماهیت آن توجه کرد. ماهیت یا چیستی منحصراً از طریق قانون یا حقوق معلوم نمی‌شود، بلکه جامعه‌شناسی، فلسفه، روان‌شناسی و جرم‌شناسی نیز در آن دخیل هستند (۴).

باید گفت ماهیت تروریسم سایبری به فضای مجازی و اقدام تروریستی آمیخته است، لذا با تعاریفی از این دو مفهوم می‌توان به تعریفی ترکیبی از تروریسم سایبری دست یافت. تروریسم و انواع آن موضوع کنوانسیون‌های بین‌المللی متعدد، تلاش‌های منطقه‌ای و سازمانی بوده است، اما همچنان از تعریف جامع و قابل قبول جامعه جهانی بی‌بهره مانده است. (اما مسأله قابل توجه این است که از آنجایی که تعاریف به عمل‌آمده در این باره بسیار تنوع است، ممکن است عملیاتی که از نظر دولت استرالیا در افغانستان علیه اتباع وی صورت می‌گیرد، تروریستی بوده، اما از نظر دولت افغانستان موجه و در راستای مبارزه با اشغال یا استعمار و در راستای حق تعیین سرنوشت باشد)، حتی با ارائه تعریف از فضای سایبر و تروریسم نیز معنای تروریسم سایبری آشکار نمی‌شود، زیرا همه رفتارهایی که ذیل تروریسم بررسی می‌شوند، در فضای سایبر جای نمی‌گیرد و هر چیزی که ضد فضای سایبر باشد، تروریسم سایبری نیست.

اولین عنصر مهم برای ایجاد چارچوب مؤثر در مبارزه با تروریسم، توافق در مورد تعریف تروریسم سایبری است. سازمان ملل متحد ۱۹ کنوانسیون، پروتکل و اصلاحیه را در مورد ترویسم به تصویب رسانده است که مربوط به مصادیق خاص این جرم می‌باشد. این تلاش‌ها در سال ۲۰۱۰ از طریق هیأت‌رییسه انحصاری کمیته ضدتروریسم (CTED: Counter Terrorism Committee Executive Directorate) گسترش یافته است. وظیفه این نهاد بررسی قوانین موضوعه ملی در فقدان تعریف شفاف برای تروریسم سایبری است (۵).

تعاریف متعددی از تروریسم سایبری ارائه شده است، دروتی دنینگ، محقق برجسته حوزه سایبر، تروریسم سایبری را این‌گونه تعریف می‌کند: حمله یا تهدید به حمله غیر قانونی علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره‌شده در آن‌ها که به

منظور ارعاب یا اعمال زور بر دولت یا مردم جهت جهت پیشبرد اهداف سیاسی یا اجتماعی. حمله باید منجر به خشونت علیه اموال یا اشخاص شده و یا حداقل موجب صدمه به میزانی شود که ایجاد ترس و وحشت نماید. طبق ماده ۱، طرح کنوانسیون بین‌المللی برای افزایش حمایت در برابر تروریسم و جرم سایبری، تروریسم سایبری به معنی استفاده عمدی یا تهدید به خشونت، تخریب یا اختلال علیه سیستم‌های سایبری، بدون اختیار رسمی و قانونی، زمانی که محتمل است چنین استفاده‌ای منجر به مرگ یا آسیب جسمی به افراد، خسارت اساسی به اموال فیزیکی، بی‌نظمی مدنی یا صدمه اقتصادی مهم شود (۲).

تعریفی که توسط مرکز حمایت از زیرساخت‌های ملی (NIPC: National Infrastructure Protection Center) ارائه شده، قابل طرح است: تروریسم سایبری، عملی مجرمانه است که با استفاده از شبکه اینترنت و سیستم کامپیوتری و قابلیت‌های رسانه‌ای ارتکاب می‌یابد و منجر به اعمال خشونت یا تهدید به آن، تخریب یا قطع خدمات می‌گردد تا ایجاد رعب و وحشت در میان جمعیت غیر نظامی کند تا دولت یا سازمان را به خواسته‌های سیاسی، اجتماعی یا ایدئولوژیک خود مجبور نماید (۳).

به هر حال برای انجام تعریفی جامع و مانع می‌توان تروریسم سایبری را از سه بعد مورد بررسی قرار داد. یکی تعریف معنوی، با تأکید بر عنصر روانی یا قصد و انگیزه که در این نوع از تروریسم موضوع قصد، شهروندان یا اموال هستند و قصد نهایی که عبارت است از هدفی که مرتکب با اعمال خشونت‌بار در جستجوی آن است. در واقع تفاوت اصلی تروریسم سایبری با سایر جرائم سایبری، انگیزه سیاسی است. دوم، تعریف عینی، یعنی نمود خارجی تروریسم سایبری به عنوان یک اقدام ناهنجار و ضد ارزش در فضای سایبر است. این شکل از تعریف بر اساس رکن مادی جرم استوار است و در آن موضوع جرم ارزشی است که قانونگذار درصدد حمایت از آن است، وسیله ارتکاب جرم فضای سایبر و نتیجه که ایجاد رعب و وحشت یا به زانودرآوردن دولت یا سازمان در جهات اهداف تروریست‌ها است، (برخی متخصصین مانند اولریش زیبر سه نتیجه را برای تروریسم سایبری لازم می‌داند: اختلال در داده‌ها، اجزای اهداف سیاسی و ایراد خسارت دیجیتالی یا فیزیکی)، اما شکل سوم تعریف، تعریف مقایسه‌ای است که در آن با مقایسه تروریسم سایبری با مفاهیم مشابه می‌توان سیمای روشن‌تری از این جرم ارائه کرد. برخی از این مفاهیم مشابه عبارتند از جنگ شبکه‌ای، جنگ اطلاعاتی و جرم سایبری (۲).

از تمامی تعاریفی که در بالا گفته شد، می‌توان این‌گونه جمع‌بندی کرد: تروریسم سایبری اعمال خشونت یا تهدید به آن در حمله به زیرساخت‌های حیاتی یک کشور با اعمال تخریب، ممانعت یا اختلال در داده‌ها، سیستم‌ها، شبکه یا مؤلفه‌های اطلاعاتی رایانه‌ای است که با ایراد صدمه و خسارت فیزیکی یا اطلاعاتی به اموال و اشخاص، ایجاد رعب و وحشت نموده و هدف از آن به زانودرآوردن دولت یا سازمان دولتی در جهت انگیزه‌های سیاسی، ایئولوژیک یا اجتماعی است.

از آنجایی که تروریسم سایبری، سیستم‌های کامپیوتری و شبکه‌های ارتباطی را هدف قرار می‌دهد، سیستم‌های چون آب و برق و گاز، کنترل حمل و هوایی، سیستم‌های مالی و پولی، ارتباطات و حمل و نقل و حتی جان انسان‌ها ممکن است با چنین حملاتی آسیب ببینند، مثلاً ویروس استاکس نت که تأسیسات هسته‌ای ایران را مورد هدف قرار داد، خطر بالقوه‌ای برای جان ملت ایران و مردم کشورهای همسایه بود. این ویروس همچنین بر سیستم‌های خدمات رسانی کشورهای آمریکا، پاکستان، آذربایجان و اندونزی نیز تأثیر داشته است. بنابراین دولت‌ها باید زیرساخت‌های هسته‌ای و نظامی‌شان را به عنوان اهداف بالقوه برای تهدیدات تروریسم سایبری بنگرند. از این گذشته چنین اقداماتی می‌تواند نقض شدید حقوق بشر را نیز در پی داشته باشد. همانطور که کوفی عنان در سال ۲۰۰۴ گفته است، تروریسم قلب آنچه که سازمان ملل برای آن به وجود آمده است را نشانه گرفته و به عنوان تهدیدی جهانی برای دموکراسی، حاکمیت قانون، حقوق بشر، صلح و امنیت بین‌المللی در نظر گرفته شده که نیازمند یک پاسخ جهانی است (۶).

به عنوان نمونه می‌توان به حملات ۲۷ آوریل ۲۰۰۷ استونی اشاره نمود که در طی چند ساعت شبکه‌های اینترنتی بانکی آن کشور از کار افتاد، انتشار تمام روزنامه‌های اصلی متوقف شد و ارتباطات دولتی مختل گردید. این کشور با تأسیس دولت الکترونیک، ۹۰٪ از خدمات بانکی و حتی انتخابات پارلمانی را توسط اینترنت تحت پوشش قرار می‌داد، مالیات‌ها به طور آنلاین دریافت می‌شد و مردم از سیستم تلفن همراه برای خرید و پرداخت پول پارکینگ استفاده می‌کردند. در طی چند روز این حملات سایبری بیشتر وب‌سایت‌های مهم را از کار انداخت و نهایتاً موجب نافرمانی مدنی وسیع و آشوبی گردید که طی آن ۱۵۰ نفر زخمی و یک تبعه روسی کشته شد (۷).

تروریسم سایبری و جنایت علیه بشریت

مسأله اصلی که در این جا مورد بحث قرار می‌گیرد، این است که آیا تروریسم سایبری نقض قواعد حافظ حقوق بشر است و در چه صورت ممکن است جنایت علیه بشریت تلقی گردد. در پاسخ به این سؤال باید به هدف، علت وجودی و محورساخت تروریسم سایبری توجه کرد. هدف تروریست‌ها ایجاد رعب و وحشت است و نه کشتار یا تخریب اطلاعات. علت وجودی تروریسم سایبری نیز وادارکردن دولت یا سازمان دولتی در گردن‌نهادن به خواست‌های تروریست‌هاست و محور ساخت این پدیده را باید برهم‌زدن نظم عمومی دانست.

با دقت در مفهوم برهم‌زدن نظم عمومی می‌توان به سادگی دریافت که هر نظام حقوقی، با تدارک قواعدی امری، درصدد صیانت از نظم عمومی است و روشن است که نقض این قواعد با واکنشی شدیدتر از نقض قواعد عادی مواجه خواهد شد. این واکنش در نظام حقوق بین‌الملل نیز به شکل جرم‌انگاری و مجازات‌های کیفری وجود دارد. در جامعه بین‌المللی دو دسته قواعد مربوط به صلح و حقوق بشر از جمله قواعد امری هستند که وظیفه صیانت از نظم عمومی را بر عهده دارند (۸).

تروروریسم سایبری یک وسیله برهم‌زننده نظم عمومی است که ضمن نقض قواعد اساسی، نظم عمومی بین‌المللی را نیز تهدید می‌کند. تروریسم سایبری، به شرط آنکه اقدامات صورت‌گرفته دارای شرایط مندرج در تعریف جنایت علیه بشریت باشند (بر اساس ماده ۷ اساسنامه دیوان کیفری بین‌المللی جنایات بر ضد بشریت اعمالی چون قتل، قلع و قمع، آزار گروه‌های سیاسی و اعمال ضد انسانی است مشروط بر این‌که در یک حمله «گسترده» یا «سازمان‌یافته» بر ضد یک «جمعیت غیر نظامی» و با «علم به آن حمله» ارتکاب یابند. بنابراین چنانچه حملات تروریستی در حوزه سایبر واجد چنین تعریفی باشد، جنایت علیه بشریت خواهد بود)، قواعد بنیادین و آمره جامعه بین‌المللی را نقض می‌کند. شایان ذکر است هر گونه اقدام تروریستی نمی‌تواند مصداق جنایت علیه بشریت باشد. جنایت بین‌المللی که در کنوانسیون‌های بین‌المللی مورد توجه قرار گرفته‌اند، دو دسته پیامد به همراه دارند، تکلیف به محاکمه و استرداد و بحث صلاحیت جهانی، اما نظر دیگری نیز وجود دارد و آن جنایت دانستن برخی اقدامات از آن رو که به طور کلی در حقوق بین‌الملل جرم دانسته شده‌اند، بی‌آنکه دولت‌ها با قراردادن آن‌ها در چارچوب صلاحیت جهانی موافقت کرده باشند. از سوی دیگر با توجه به مقدمات و مذاکرات انجام‌شده در خلال کنوانسیون رم، نامی از تروریسم و انواع آن امروزه در صلاحیت‌های موضوعی دیوان دیده نمی‌شود، اما با احراز شرایط مندرج در تعاریف جرائم در صلاحیت آن، می‌توان تروریسم سایبری را نیز جنایت جنگی یا علیه بشریت دانست.

بنابراین در حقوق هنجاری، با توجه به هدف، محور ساخت و علت وجودی تروریسم سایبری، می‌توان تروریسم و انواع آن را جنایت دانست، اما در حقوق موضوعه، اگرچه به ویژه پس از حوادث ۱۱ سپتامبر، در اسناد بین‌المللی و توسط دبیرکل و کمیسر عالی کمیسیون حقوق بشر جنایت بر ضد بشریت خوانده شد، اما عدم موفقیت جامعه بین‌المللی در ارائه تعریف جامع از تروریسم و ضعف ساز و کارهای حقوق بین‌الملل برای مبارزه کیفری با آن، تروریسم را فاقد عناصر لازم برای جنایت تلقی‌کردن در بعد بین‌المللی نموده است. از این رو هیچ قاعده جهانی وجود ندارد که تعقیب متهمان را در قالب صلاحیت جهانی اجازه دهد (تعهدات امری ناشی از قطع‌نامه ۱۳۷۳ و

قطع‌نامه‌های بعدی شورای امنیت، تکلیف به جرم‌انگاری، تعقیب و مجازات عاملان جنایات تروریستی را دربر دارند)، اما همچنان یکی از مصادیق جنایت شدید دارای اهمیت بین‌المللی که تکلیف به مجازات یا استرداد متهان در مورد آن وجود دارد (۸).

در حوزه مناسبات حقوق بشر و تروریسم ما با دو مسأله مواجه هستیم، یکی این چگونه تروریستم سایبری باعث نقض حقوق بشر می‌شوند و دیگر این‌که در سیاق مبارزه با تروریسم سایبری چه موازین حقوق بشری باید رعایت گردد. رعایت قواعد حقوق بشر گذشته از تضمین نظم عمومی بین‌المللی که به تدریج به هدف محوری حقوق بین‌الملل تبدیل می‌شود، در جهت تضمین صلح نیز می‌باشد. تروریسم سایبری با هدف قراردادن بنیادی‌ترین حقوق بشر، یعنی حق حیات، درصدد حصول به هدف خود یعنی برهم‌زدن نظم عمومی، از طریق ایجاد ناامنی و رعب و وحشت عمومی است. بخش بعدی به بررسی حقوق و آزادی‌های اساسی که توسط تروریست‌های سایبری نقض می‌شود، اختصاص یافته است.

تروریسم سایبری نقض و تهدید نسل‌های حقوق بشر

از اواخر دهه ۱۹۸۰، اینترنت ابزاری بسیار پویا برای ارتباطات بوده است و توسعه فناوری‌های پیشرفته، شبکه‌ای را با دسترسی جهانی ایجاد کرده که موانع نسبتاً ناچیزی برای ورود به آن وجود دارد. فناوری اینترنت این قابلیت را به افراد می‌دهد تا با تعداد نامحدود مخاطبین در سراسر مرزها به صورت گمنام، سریع و راحت در ارتباط باشند. یکی از اساسی‌ترین ویژگی‌ها و مزایای فناوری اینترنت، قابلیت منحصر به فرد آن برای انتشار اطلاعات و افکار می‌باشد که به عنوان یکی از حقوق اساسی بشر شناخته شده است. این نکته نیز باید در نظر گرفته شود که همان فناوری که اینچنین ارتباطاتی را سهولت می‌بخشد، می‌تواند به منظور اهداف تروریستی نیز مورد سوءاستفاده قرار گیرد. استفاده از اینترنت برای اهداف تروریستی فرصت‌هایی را نیز برای مبارزه با تروریسم به وجود می‌آورد (۹).

حقوق بشر احترام، ضمانت و اجرای حقوق مدنی، فرهنگی، اقتصادی، سیاسی و اجتماعی است که به تمامی بشریت و بدون تبعیض تعلق دارد و دارای اوصافی چون جهان‌شمولی، مطلق‌بودن، سلب‌ناشدنی‌بودن و انتقال‌ناپذیری است، اگرچه تخلف از برخی حق‌های بشری در شرایط اضطراری طبق ماده ۴ میثاق حقوق مدنی و سیاسی مجاز است. (هرگاه یک خطر عمومی استثنایی (فوق‌العاده) موجودیت ملت را تهدید کند و این خطر، رسماً اعلام بشود، کشورهای طرف این میثاق می‌توانند تدابیری خارج از الزامات مقرر در این میثاق به میزانی که وضعیت حتماً ایجاب می‌کند، اتخاذ نمایند، مشروط بر این‌که تدابیر مزبور با سایر الزاماتی که طبق حقوق بین‌الملل به عهده دارند مغایرت نداشته باشد و منجر به تبعیضی منحصراً بر اساس نژاد، رنگ، جنس، زبان، اصل و منشأ مذهبی یا اجتماعی نشود.)

تروریسم پدیده شومی است که جان، مال و آزادی‌های اساسی بشریت را هدف قرار داده است. نقض حقوق بشر توسط تروریسم در معنای عام خود برکسی پوشیده نیست. اقدامات تروریستی به طور جدی حق بهره‌مندی انسان از حقوق بشر را مختل می‌کند و توسعه اجتماعی و اقتصادی همه دولت‌ها را تهدید و ثبات جهانی و رفاه را تضعیف می‌کند. همانطور که کمیسرعالی سابق حقوق بشر سازمان ملل، خانم مری رابینسون اظهار داشت: «اساس حقوق بشر این است که زندگی انسان و کرامت وی نباید به مصالحه گذاشته شود و اعمال خاص دولت‌ها یا غیر دولتی‌ها هم هرگز نمی‌تواند هدف را توجیه کند. حقوق بشر بین‌المللی و حقوق بشردوستانه، حد و مرزهایی را که در ارتباط با رفتار نظامی و سیاسی تعریف می‌کنند، دیدگاه بی‌ملاحظه نسبت به زندگی و آزادی انسانی اقدامات ضدتروریستی را زیر سؤال می‌برد» (۱۰).

حمله به زیرساخت‌های حیاتی یک دولت که از فاکتورهای مهم شناسایی تروریسم سایبری است، توسط حمله به سیستم‌های کنترل نظارتی و کسب داده (SCADA: Supervisory Control and Data Acquisition) انجام می‌شود که عملیات بسیاری از زیرساخت‌های مهم و حیاتی مثل ژنراتورهای تولید برق و آب‌رسانی را کنترل و تنظیم

می‌نمایند. این سیستم‌ها به صورت خودکار فرایندهای کنترل، تولید و تعویض را بر اساس بازخوردهای عددی دریافت شده از حسگرها رصد و تنظیم می‌کنند و یا اعمال فیزیکی مانند سطح فشار در لوله‌ها را انجام داده یا این‌که یک سد باز یا بسته است را کنترل می‌کنند (به عنوان مثال در سال ۱۹۹۷ یک هکر اینترنتی توانست به سیستم ارتباطی فرودگاهی در ماساچوست آمریکا دستیابی پیدا کند که باعث مختل‌شدن خط تلفنی شد که به برج مراقبت فرودگاه متصل بود و همچنین توانایی روشن‌کردن چراغ‌های باند فرود را توسط هواپیماهایی که در حال نزدیک‌شدن به باند بودند را غیر ممکن ساخت. در نمونه‌ای دیگر یک کارمند سابق صنایع مدیریت پسماند استرالیا به سیستم‌های رایانه‌ای آنجا دستیابی پیدا کرد و باعث شد که هزاران لیتر فاضلاب در کوئینزلند جاری شود و به گیاهان و جانوران صدمه وارد شده و مردم نیز آنجا را تخلیه کنند). رایانه‌ای که از القاعده در افغانستان مصادره شد، حاوی نمونه‌هایی از یک سد بود که با سبک معماری و نرم‌افزار مهندسی طراحی شده بود و طراحان آن را قادر می‌ساخت که سطح آسیب‌پذیری و تخریب سد را تخمین بزنند. دفتر تحقیقات فدرال ایالات متحده از موارد زیادی از نمونه‌های طراحی‌شده توسط القاعده که برای اهداف آنلاین و نظارت بر سیستم‌های تلفن اضطراری، ژنراتورها و دستگاه‌های مخابراتی، مخازن آب و و سیستم توزیع، نیروگاه‌های اتمی و شبکه‌های مخازن سوخت برنامه‌ریزی شده بودند، پرده برداشت (۱۱).

برای بررسی این‌که اقدامات تروریستی در فضای سایبر به مفهوم تروریسم سایبری که برخی آن را شامل افراطی‌گری سایبری نیز دانسته‌اند، چه حقوق و آزادی‌های بنیادینی را تحت تأثیر قرار می‌دهد و چگونه باعث نقض حقوق بشر می‌شود، این مطالعه را در خلال نسل‌های حقوق بشر انجام خواهیم داد.

۱ـ نسل اول: حقوق مدنی و سیاسی

نسل اول حقوق بشر که نسل «حقوق ـ آزادی‌ها» نامیده می‌شود، به انقلاب فرانسه بازمی‌گردد و مبنای فلسفی آن در اصالت فرد می‌باشد. دولت در مورد این حقوق که بدان حق‌های منفی نیز گفته می‌شود، هم باید به وظیفه «احترام» عمل نماید و هم با پاسبانی از این حقوق در برابر تعدی دیگر افراد، وظیفه «حمایت» را به انجام رساند. انعکاس این ایده در نظام حقوق بشر را می‌توان در مواد ۲ تا ۲۱ اعلامیه جهانی حقوق بشر و نیز میثاق بین‌المللی حقوق مدنی و سیاسی دید. از مهم‌ترین حقوق این نسل می‌توان به حق‌ها و آزادی‌هایی چون حق حیات، حق بر امنیت فردی، منع شکنجه، آزادی بیان و رفت و آمد، آزادی اندیشه و عقیده و نیز آزادی‌های مذهبی را برشمرد. بسیاری از این حقوق در جریان فعالیت‌های تروریسم سایبری ممکن است تهدید یا نقض شود که در ادامه به بررسی مواردی از آن‌ها در خلال چهار نسل شناخته‌شده حقوق بشر پرداخته شده است.

۱-۱- حق حیات و امنیت شخصی: حق حیات به عنوان بنیادی‌ترین ارزش انسانی این پیامد حقوق بشری را به دنبال دارد که هیچ حق یا ارزش انسانی دیگری بر حق حیات تقدم نخواهد داشت (۱۲). خشونت‌باربودن، ایجاد رعب و وحشت نمودن و انگیزه سیاسی خصایص مشترک کلیه اقدامات تروریستی است. همین مسأله تروریسم را معارض بنیادی‌ترین حق بشری، یعنی حق بر حیات قرار می‌دهد. توجیه‌ناپذیری اقدامات تروریستی با هر ملاحظه سیاسی و ایدئولوژیک، تمام قربانیان مستقیم و غیر مستقیم اقدامات ترویستی را بی‌گناه و سلب یا تحدید حقوق آنان را خودسرانه جلوه می‌دهد (۱۳).

حق حیات مندرج در بخش دوم ماده ۴ و بند ۱، ماده ۶ میثاق حقوق مدنی و سیاسی، حقی است ذاتی که باید به موجب قانون مورد حمایت قرار گرفته و هیچ کس را نمی‌توان به طور خودسرانه از آن محروم کرد و دولت‌های نیز به بهانه این‌که حیات ملت در شرایط اضطراری در معرض تهدید است نمی‌توانند آن را نقض کنند. اقدامات تروریستی در حوزه سایبر می‌تواند ناقض این حق باشد. حملات تروریسم سایبری ممکن است از طریق اختلال، تخریب یا دستکاری داده‌ها و مختل نمودن عملکرد سیستم ترافیک هوایی و راه آهن (مانند آنچه در ۱۹۸۵ علیه سیستم‌های رایانه‌ای فرودگاه و راه آهن ژاپن اتفاق افتاد)، شلیک موشک‌های هدایت شونده دوربرد، اختلال در سیستم‌های خدمات اورژانس، آتش‌نشانی و نیروگاه‌های

اتمی و یا آلوده ساختن منابع آبی آشامیدنی یک شهر، جان انسان‌های بی‌گناهی را قربانی اهداف شوم خود نماید. دستکاری سیستم‌های رایانه‌ای رادارهای هوایی، سیستم حمل و نقل ترن‌های سریع‌السیر یا کنترل‌کننده خروجی سدها ممکن است به از بین‌رفتن صدها تن منجر شود.

از سوی دیگر حق امنیت شخصی افراد مندرج در ماده ۳ اعلامیه جهانی حقوق بشر و بند ۱ ماده ۹ میثاق حقوق مدنی و سیاسی، به حق زندگی به دور از ترس و واهمه اشاره دارد (۱۳). وابستگی زندگی امروزی هم در حوزه خصوصی و هم عمومی، نگرانی‌هایی را در از دست‌رفتن اطلاعات، خرابکاری، افشای رمزهای عبور و اطلاعات فردی یا محرمانه در دنیای سایبر ایجاد نموده است. امنیت شخصی در محیط اینترنت ناظر بر امنیت داده‌های نیز هست. دسترسی عمدی بدون مجوز به تمام یا بخشی از یک سامانه رایانه‌ای، دسترسی غیر قانونی به فایل‌های اطلاعاتی، تغییر یا تخریب داده‌ها، دسترسی به گذر واژه‌ها طبق مندرجات کنوانسیون بوداپست، ناقض امینت شخصی و حریم خصوصی افراد است.

حق بر امنیت مستلزم دو تضمین اساسی است: یکی تضمین امنیت افراد در برابر هرگونه توقیف، زندانی‌شدن، مجازات و دیگر تعرضات خودکامه و غیر قانونی، دیگر تضمین امنیت افراد از طریق حمایت‌های جامعه برای حمایت از هر یک از اعضای خود به منظور حفظ حقوق، تعلقات و برخورداری از آزادی‌های انسانی. در این راستا ماده ۲ کنوانسیون بوداپست در مورد جرائم سایبری مقرر داشته است که «هر یک از اعضا باید به گونه‌ای اقدام به وضع قوانین و سایر تدابیر کند که در صورت لزوم، بر اساس حقوق داخلی خود، دسترسی عمدی بدون حق را به تمام یا بخشی از یک سامانه رایانه‌ای جرم‌انگاری کند. اعضا می‌توانند مقرر دارند این جرم با نقض تدابیر امنیتی و به قصد تحمیل داده‌های رایانه‌ای یا سایر مقاصد ناروا یا نسبت به سامانه رایانه‌ای که با سامانه رایانه‌ای دیگری ارتباط دارد، محقق می‌شود» (۱۰). بنابراین از آن جایی که حق حیات در حالت‌های مختلفی ممکن است به مخاطره افتد یا مورد تعرض قرارگیرد، عدم پیش‌بینی مقررات لازم در برخورد با کسانی که این حق را مورد تعرض قرار دهند نیز نوعی نقض حق حیات محسوب می‌شود (۱۲).

۲-۱- حق بر حریم خصوصی: مطابق ماده ۳ و ۱۲ اعلامیه جهانی حقوق بشر «هر فردی حق زندگی، آزادی و امنیت شخصی دارد» و «نباید در زندگی خصوصی امور خانوادگی، اقامتگاه یا مکاتبات هیچ کس مداخله‌های خودسرانه صورت گیرد یا به شرافت و آبرو و شهرت کسی حمله شود.» (برخی اسناد در این مورد عبارتند از: قطع‌نامه شورای اروپا که حریم خصوصی را به عنوان حقی نسبت به داشتن زندگی با سلیقه خود و حداقل مداخله دیگران تعریف کرده است. بند ۲ اعلامیه کنفرانس حقوقدانان درباره حق رعایت حریم خصوصی: «حق حریم خصوصی حقی است نسبت به تنهاماندن نسبت به زندگی‌کردن با سلیقه خود و یا حداقل درجه مداخله دیگران» و ماده ۸ کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی هر کس از حق احترام به زندگی خصوصی و خانوادگی، خانه و مراسلات خود برخوردار است). طبق ماده ۱۷ میثاق حقوق مدنی و سیاسی، مکاتبات هیچ کس نباید مورد مداخله خودسرانه قرار گیرد. حق بر عدم ورود بدون اجازه به حریم خصوصی، شامل شنود الکترونیک، جاسوسی سایبری و بازرسی مکاتبات الکترونیک و اطلاعاتی شخصی مانند سیستم پست الکترونیک، اطلاعات کارت‌های بانکی و... نیز می‌گردد (۱۴).

نقض این حق توسط تروریست‌های سایبری به ویژه در تروریسم دولتی به شدت قابل توجه است. حق دسترسی به اطلاعات مربوط به فرد که مقامات دولتی را ملزم به پاسخگویی در قبال آن نیز می‌کند، با تخریب و حذف اطلاعات در جریان یک حمله گسترده سایبری ممکن است نقض شود. حریم خصوصی تعریف‌شده در اعلامیه جهانی حقوق بشر و میثاق حقوق مدنی و سیاسی به حق بر حفظ اطلاعات تولیدشده در فضای سایبر تبدیل می‌شود.

حق دیگری که می‌توان زیرمجموعه حق برحریم خصوصی در فضای سایبری مورد توجه قرار داد که اغلب نیز با افشای اطلاعات مربوط به کاربری افراد نقض می‌شود، حق بر ناشناختگی است. در جامعه اطلاعاتی حق بر ناشناختگی دارای

دو بعد است: یکی مربوط به رعایت حقوق بشری مردم دیگری نحوه رعایت چنین تکلیفی از سوی دولت‌ها. سهل‌انگاری در ایفای این تکلیف، این فرصت را برای تروریست‌های سایبری فراهم می‌کند تا با خیال آسوده، اقدامات تروریستی خود را انجام دهند (۱۰). تجاوز به حریم خصوصی افراد توسط تروریست‌ها در فضای سایبر از طریق فریب فرد در استفاده از داده‌های کاذب، دستکاری و حذف داده‌های شخصی، جمع آوری غیر قانونی داده‌ها، افشای غیر قانونی و سوء استفاده از داده‌ها صورت می‌گیرد. تروریست‌ها دقیقاً به حوزه‌هایی وارد می‌شوند که ضعف‌های امنیتی دارند مانند، بانکداری و خدمات دولتی الکترونیکی (۱۵).

۳-۱- حق آزادی بیان: معنای واقعی آزادی اطلاعات، در فضای سایبر محقق شده است. از این رو هر نوع اطلاعاتی اعم از فرهنگی، سیاسی و اقتصادی، بدون محدودیت‌های حاکم بر دیگر رسانه‌ها، در فضای سایبر در دسترس است. آزادی ارتباطی نیز از ویژگی‌های دیگر فضای مجازی است که در دیگر وسایل ارتباطی تا این حد قابل دستیابی نیست.

شورای حقوق بشر سازمان ملل متحد بارها تأیید کرده است که همان حقوقی که مردم به صورت آفلاین دارند، باید به صورت آنلاین نیز محافظت شوند، به ویژه آزادی بیان که به عنوان حقی تلقی می‌شود که بهره‌مندشدن از سایر حقوق اساسی اقتصادی، اجتماعی، فرهنگی، مدنی و سیاسی از جمله حق آزادی اجتماعات و اجتماعات مسالمت‌آمیز، حق تحصیل و حق مشارکت در زندگی فرهنگی در سایه تحقق آن میسر است. مجمع عمومی سازمان ملل متحد همچنین تصدیق کرده است که حق استفاده از حریم خصوصی برای تحقق حق آزادی بیان و داشتن عقاید بدون دخالت نیز مهم است و یکی از پایه‌های جامعه دموکراتیک به شمار می‌آید.

آزادی بیان از جمله حق‌هایی است که در اسناد بین‌المللی متعددی از جمله میثاق حقوق مدنی و سیاسی و اعلامیه جهانی حقوق بشر مورد تأکید قرار گرفته است. ماده ۱۹ اعلامیه جهانی حقوق بشر با به کارگیری واژه بیان، مفهوم موسع آزادی «بیان» را مورد حمایت قرار داده است. این تفسیر شامل انتقال افکار و اطلاعات است. بند ۲ ماده ۱۹ میثاق حقوق مدنی سیاسی نیز اعلام می‌دارد که این حق شامل جستجو، دریافت و دادن همه انواع اطلاعات و ایده‌ها بدون توجه به مرزهای سرزمینی می‌گردد. خواه این ایده‌ها و اطلاعات به صورت مکتوب شفاهی و یا چاپی یا از طریق رسانه‌های گروهی یا هر وسیله دلخواه دیگر باشد (۱۲).

افراط‌گرایی، تبلیغات گروه‌های نفرت پراکن مانند نئونازی‌ها و موعظه برای جهاد توسط مسلمانان افراطی از دسته محتواهایی هستند که توسط تروریست‌ها در محیط سایبر در اتاق‌های گفتگو، کانال‌های ارتباطی و شبکه‌های اجتماعی منتشر می‌شوند. مجرمان در پناه توسل به آزادی بیان اقداماتشان را مشروع جلوه می‌دهند، در حالی که حق آزادی بیان، حق مطلقی نیست و با نفرت‌پراکنی و دعوت به ستیزه‌جویی تعارض دارد. حق آزادی تجمعات نیز که ممکن است به شکل مجازی رخ دهد، محمل دیگری برای اقدامات تروریستی است. تشکیل گروه‌های گفتگو، دعوت به انجام اقدامات تروریستی در قالب جهاد الکترونیک و تلاش در جهت توجیه اقدامات، افراد ناآگاه بسیاری را به سمت اجتماعات تروریستی کشانده است.

در مورد آزادی بیان، اگرچه طیف گسترده‌ای از نظریات شامل آزادی مطلق تا خود محدود سازی مطرح شده است، اما آنچه اولین اقدام سایبری تروریست‌ها تلقی می‌شود، نقض همین آزادی است. اقدامات ترویست‌ها با اختلال، تغییر محتوا و یا از دسترس خارج‌کردن اطلاعات وب‌سایت‌ها آغاز می‌شود. شبکه‌های اجتماعی که امروزه فعال‌ترین بخش ارتباطات رایانه‌ای را در اختیار دارند، مانند توییتر سهواً ممکن است باعث گسترش اطلاعات غلط به جای حقایق شوند، اگرچه امکان اصلاح محتوای توییت‌شده وجود دارد، اما وجود میلیون‌ها مخاطب به همان داده‌های غلط مشروعیت خواهد داد. اعمال تروریستی در چنین محیط‌هایی با خطر و صرف هزینه کم ارتکاب می‌یابد (۱۶).

۴-۱- حق مالکیت: طبق ماده ۱۷ اعلامیه جهانی حقوق بشر، هر کس منفرداً یا به طور دسته جمعی حق مالکیت دارد و احدی را نمی‌توان خودسرانه از حق مالکیت محروم نمود. در حوزه سایبری نیز حق مالکیت به دو نوع مالکیت داده‌ها و

مالکیت معنوی قابل تقسیم است. از سنتی‌ترین جرائم سایبری که به شدت مورد توجه تروریست‌های سایبری است، نقض حق مالکیت است که به شیوه‌هایی گوناگونی قابل اعمال می‌باشد. سرقت و یا دستکاری داده‌های شخصی، اطلاعات نظامی و طبقه‌بندی‌شده در خلال جاسوسی سایبری، نفوذ به سیستم‌های بانکداری اینترنتی و سرقت رمزهای عبور، سرقت اینترنتی، هک، ویروسی‌کردن رایانه‌های شخصی یا دولتی و سیستم‌های ارتباطی از مصادیق نقض حق مالکیت در فضای سایبر هستند. حمل و نقل بین‌المللی پول از این طریق امکان ردیابی و مسدودسازی را مشکل می‌کند و از سوی دیگر بسیاری از سازمان‌های تروریستی، فعالیت‌های خود را از طریق آنلاین انجام می‌دهند، جرم‌هایی از قبیل جعل کارت اعتباری و سرقت مالکیت فکری در همین راستا رخ می‌دهد.

نقض حق مالکیت به ویژه در زمان نیاز مادی تروریست‌ها برای انجام اقداماتشان فراوانی می‌یابد. تروریست‌ها و حامیانشان از اینترنت به چهار شیوه برای کسب درآمد و افزایش بودجه استفاده می‌کنند: درخواست مستقیم از طرفداران، استفاده از مزایای تجارت الکترونیک، بهره‌مندی از روش‌های پرداخت آنلاین و نهادهای خیریه. در این شیوه‌ها، ترویست‌ها به طور مستقیم از طرفدارانشان از طریق وب‌سایت‌ها، اتاق‌های گفتگو و شبکه‌های اجتماعی می‌خواهند تا به آن‌ها کمک مالی کنند. این کمک‌های مالی از طریق پرداخت آنلاین از طریق سرقت کارت‌های اعتباری و هویت‌های جعلی صورت می‌گیرد. گاهی نیز تروریست‌ها برای انجام مقاصد مالی‌شان از طریق تأسیس نهادهای به ظاهر قانونی مانند خیریه‌ها اقدام می‌کنند. این خیریه‌ها اغلب ادعای کمک‌های بشردوستانه دارند، اما در حقیقت برای کلاهبرداری از افراد در جهت کسب منافع مالی برای مقاصد شوم خود هستند (۹).

۲ـ نسل دوم حقوق بشر

این مفهوم از حق بشر پس از انقلاب صنعتی پدیدار شد و ریشه در مطالبات اقشار آسیب‌پذیر و نیازمند جامعه مانند کارگران داشت. نسل دوم حقوق بشر مندرج در مواد ۲۲ تا ۲۷ اعلامیه جهانی حقوق بشر و میثاق حقوق اقصادی، اجتماعی و فرهنگی که به «حقوق رفاهی» مشهور است، می‌باشد. در این نسل حقوق بشر تقاضای اقدام و مداخله از دولت در تأمین حداقل شرایط مناسب که برای حفظ کرامت ذاتی انسان ضروری است. از این رو این حق‌ها را حقوق مثبت نیز خوانده‌اند. حق‌هایی همچون حق بر آموزش، بهداشت، مسکن، اشتغال و تأمین اجتماعی حقوق بشر نسل دوم به شمار می‌روند.

۱-۲- حق بر آموزش: حق بر آموزش به عنوان سازنده زیربنایی فهم و درک انسانی و مجرای تعین و تحقق دیگر حقوق معنوی از جمله آزادی اندیشه، بیان و مذهب، از منزلتی بسیار رفیع در میان سایر حقوق انسان برخوردار است. با مطالعه دقیق اهداف ملل متحد و ارتباط درونی آن‌ها می‌توان گفت بنیانگذاران سازمان ملل بر این عقیده بوده‌اند که حفظ صلح و امنیت بین‌الملل، توسعه روابط دوستانه، پیشبرد و احترام به حقوق بشر و آزادی‌های اساسی به هم تنیده و غیر قابل تفکیک هستند و آموزش یکی از راه‌های نیل به این اهداف است. آموزش وسیله انتقال فرهنگ، جامعه‌پذیری و یادگیری و شاه‌کلید استفاده از سایر حقوق انسانی است (۱۷).

حق بهره‌مندی از آموزش به شکل مبسوطی در اسناد حقوق بشری مورد تأکید قرار گرفته است. بند ۱ ماده ۱۳ میثاق حقوق اقتصادی، اجتماعی و فرهنگی (کشورهای طرف این میثاق حق هر کس را به آموزش و پرورش به رسمیت می‌شناسند. کشورهای مزبور موافقت دارند که هدف آموزش و پرورش باید نمو کامل شخصیت انسانی و احساس حیثیت آن و تقویت احترام حقوق بشر و آزادی‌های اساسی باشد. علاوه بر این کشورهای طرف این میثاق موافقت دارند که آموزش و پرورش باید کلیه افراد را برای ایفای نقش سودمند در یک جامعه آزاد آماده سازد و موجبات تفاهم و تساهل و دوستی بین کلیه ملل و کلیه گروه‌های نژادی ـ قومی یا مذهبی را فراهم آورد و توسعه فعالیت‌های سازمان ملل متحد را به منظور حفظ صلح تشویق نماید) برای هر فرد حق بهره‌مندی از آموزش و پرورش را مورد شناسایی قرار داده است. نکته قابل ملاحظه این‌که از دیدگاه این سند، جهت‌گیری آموزش باید به سمت رشد و کمال و کرامت انسانی و به ویژه تقویت حقوق و آزادی‌های اساسی باشد (۱۲).

از سوی دیگر طبق بند ۲ ماده ۲۶ اعلامیه جهانی حقوق بشر، آموزش باید طوری اعمال شود که انسان را به کمال برساند و با روح نابردباری، افراطی‌گری و تعصبات نژادی و مذهبی مبارزه کند. ماده ۲۰ میثاق حقوق مدنی و سیاسی نیز اعلام می‌دارد که تبلیغ برای جنگ ممنوع بوده و هرگونه دعوت به کینه ملی، نژادی یا مذهبی که محرک تبعیض یا مخاصمه باشد نیز ممنوع است. تروریست‌های سایبری و افراط‌گرایان در محیط سایبر، از دو طریق این حق را با چالش مواجه می‌کنند، یکی با اختلال در سیستم‌های آموزش الکترونیک یا تغییر محتوا سایت‌های آموزش و دانشگاهی به ویژه در حوزه تکنولوژی و دیگری با آموزش اجباری به مردمان حوزه‌های تحت تسلط خود در راستای افراطی‌گری، تعصبات قومی و مذهبی و نژادی و دیگری از طریق آموزه‌های خشونت‌بار در راستای اهداف تروریستی‌شان، مانند ساخت بمب یا انجام حملات انتحاری.

اینترنت حوزه وسیعی را در اختیار سازمان‌های تروریستی قرار می‌دهد تا به راحتی و سرعت اطلاعات را به اشتراک گذارند و از قابلیت‌های جستجو استفاده کنند. نمونه‌های بسیاری از جزوات و دستورالعمل‌های تروریستی در اینترنت وجود دارد که در آن شیوه‌های تهیه بمب با مواد در دسترس، شیوه سازماندهی حملات، چگونگی پیوستن به گروه تروریستی، استفاده از ویروس‌ها، هک و نیز ساخت شبکه‌های ارتباطی میان اعضا برای تبادل اطلاعات آموزش داده می‌شود (۹).

این قابلیت برای سازمان‌های تروریستی که شبکه سلسله مراتبی افقی دارند، دارای جذابیت بیشتری است. آن‌ها از این طریق می‌توانند بدون تماس رسمی، عملیات خود را انجام دهند. فلسفه آن‌ها حمایت آنلاین از طرفداران است که بدون حضور فیزیکی بتوانند از آموزش‌های لازم بهره‌مند شوند (۱۶).

۲-۲- حق بر بهداشت: حق بر سلامت از موضوعات نوظهور در حقوق نیست، اما با پیشرفت علم و گشوده‌شدن عرصه‌های جدید این مسأله پیوسته وارد چالش‌های جدیدی می‌شود. حق بر بهداشت، طیف گسترده‌ای از اقدامات ضروری و عاجل در پیشگیری، درمان و مراقبت‌های پس از درمان و پژوهش‌های علمی تا عمل‌های پیوند اعضا را شامل می‌شود.

جامعه بین‌المللی در چندین سند، به این حق پرداخته است. اعلامیه جهانی حقوق بشر در بند ۱ ماده ۲۵ خود، «مراقبت‌های بهداشتی» را در کنار خوراک، پوشاک، مسکن و خدمات اجتماعی ضروری، جزء شرایط حداقلی اقتصادی و اجتماعی برای استاندارد مناسب زندگی و رفاه و سلامتی هر فرد دانسته است. همچنین ماده۱۲ میثاق بین‌المللی حقوق اقتصادی و اجتماعی و فرهنگی از حق برخورداری از بالاترین استانداردهای قابل دستیابی سلامت فیزیکی و روانی یاد کرده و تحقق آن را برعهده دولت‌ها گذاشته است (۱۸).

برای روشن‌شدن چهارچوب کلی این حق، ضروری است به محتوای «سلامت» پرداخته شود. سازمان جهانی بهداشت سلامت را چنین تعریف می‌کند: «حالتی است که افراد در آن از رفاه کامل جسمی، روانی، اجتماعی و معنوی برخوردار باشند، زندگی مولد از نظر اقتصادی و باروری و زندگی با نشاطی داشته باشند.» با دقت بیشتر در این تعریف می‌توان دریافت که سلامتی تنها به معنی نبود بیماری نیست، بلکه یک حق گسترده است و لازمه رسیدن به آن نیازمند تحقق همه حق‌های بشری است (۱۹)، اما تروریسم سایبری چگونه این حق در نقض می‌کند؟ مثال عینی در این مورد در کشور استرالیا است، یک کارمند سابق، به دلیل نارضایتی شغلی در سال ۲۰۰۰ با استفاده از اینترنت، یک میلیون لیتر فاضلاب خام به درون رودخانه و آب‌های ساحلی در کوئینزلند وارد نمود. نمونه‌های دیگر قطع برق بیمارستان، دستکاری پرونده‌های پزشکی، از دسترس خارج‌کردن مراقبت‌های آنلاین و جراحی‌های از راه دور می‌باشد.

کشورهای عضو سازمان بهداشت جهانی (WHO: World Health Organization) مقررات بین‌المللی بهداشتی را در سال ۲۰۰۵ به منظور تقویت توانایی‌های ملی و بین‌المللی برای شناسایی و مدیریت حوادث ویرایش کردند. این مقررات، کشورهای عضو را برای شرکت در یک سیستم نظارت به منظور افزایش ظرفیت‌های ملی برای حوادث جدی سلامت، اعم از پیدایش تهدید از پدیده‌های طبیعی، تصادفات و یا

حملات تروریستی متعهد می‌نماید. (در مورد آلودگی فرامرزی و حوادث صنعتی و یا هسته‌ای فرامرزی هم مقرراتی دارد که برای تقویت توانایی‌های کشورهای عضو برای کنترل اثرات چنین آلودگی و حوادثی که به هر علت اتفاق می‌افتند، تلاش می‌کند) (۲۰).

۳ـ نسل سوم حقوق بشر

ایده نسل سوم را باید پاسخی به کاستی‌ها و ناکارآمدی‌های دو نسل پیشین دانست که به ویژه پس از جنگ سرد مورد توجه قرار گرفت. بعدها دبیرکل وقت سازمان ملل متحد در گزارش خود به مجمع عمومی به تاریخ ۶ ژوئن ۱۹۹۴ تحت عنوان «دستور کار برای توسعه»، پیامدهای منفی ناشی از جهانی‌شدن، مثل نابودی محیط زیست، فقر فزاینده، رشد جمعیت، تروریسم و قاچاق مواد مخدر را مانعی بر سر راه توسعه دانسته و راه‌کارهایی ارائه می‌دهد. حق توسعه، حق صلح، حق محیط زیست سالم، میراث مشترک بشریت، حق ارتباطات و کمک‌های بشر دوستانه، حق تعیین سرنوشت و... از جمله حقوق نسل سوم هستند (۲۱).

از جمله حقوق همبستگی که ممکن است توسط حملات تروریستی در فضای سایبر به طور مستقیم یا غیر مستقیم نقض شود عبارتند از: حق بر توسعه که دربردارنده توسعه انسانی در تمام وجوه زندگی از جمله امنیت فیزیکی، انسانی است، حق بر صلح و حق بر محیط زیست سالم که در ادامه به آن خواهیم پرداخت.

۱-۳- حق بر توسعه: حق بر توسعه با تلاش‌های کشورهای کم‌تر توسعه‌یافته شکل گرفت که حقی بر مبنای نگرانی‌ها و دغدغه‌های حقوقدانان جهان سوم است. اعلامیه حق بر توسعه ۱۹۸۶، پس از آن اعلامیه وین و برنامه اقدام و تأکید بر حق بر توسعه در قطع‌نامه‌های مجمع عمومی سازمان ملل از جمله تلاش‌های صورت‌گرفته در راستای به رسمیت شناختن این حق به شمار می‌رود. طبق بند یک ماده ۱، اعلامیه حق بر توسعه، این حق یک حق مسلم بشری است که به موجب آن هر فرد استحقاق مشارکت و سهیم‌بودن و برخورداری از توسعه اجتماعی، سیاسی، اقتصادی و فرهنگی را دارد، به نحوی که در آن کلیه حقوق بشر و آزادی‌های اساسی کاملاً تحقق یابد (۲۲).

در سال ۱۹۷۷ نیز کمیسیون حقوق بشر سازمان ملل متحد به طور رسمی حق بر توسعه را به رسمیت شناخت. حق توسعه یک حق اساسی است که پیش‌شرط اولیه آزادی، پیشرفت، عدالت و خلاقیت است، ابزار و هدف حقوق بشر به شمار می‌رود و به طور خلاصه، هسته مرکزی حقوق است که سایر حقوق نیز از آن می جوشد (۲۳).

حق بر توسعه و فضای سایبر بر یکدیگر تأثیر متقابل دارد. از یکسو حق بر توسعه به عنوان یکی از حقوق بشری در ترویج و توسعه فضای سایبر مؤثر است. طبق این حق کشورها موظف‌اند که امکانات لازم برای رفاه و توسعه افراد جامعه را فراهم آورند. ارائه فناوری‌های اطلاعاتی به مردم یکی از جلوه‌های این حق است. حق بر توسعه به عنوان یکی از مصادیق نسل سوم حقوق بشر (۲۴) در کنار سایر حقوق مندرج در نسل سوم، به غنی‌ترشدن فضای سایبر کمک می‌کند (این حق در قطع‌نامه ۳۳۸۴ مجمع عمومی سازمان ملل متحد ذکر شده است. همچنین دو قطع‌نامه در سال ۱۹۷۱ تصویب شد که به نقش کامپیوتر در توسعه اشاره داشته است. این قطع‌نامه‌ها اعلام می‌دارند که بهره‌برداری در سطح جهانی از کامپیوتر و فناوری‌های کامپیوتری می‌تواند نقش مهمی در تسریع پیشرفت بخش‌های اقتصادی و اجتماعی داشته باشد.)

از سوی دیگر، از آن جایی که حق بر توسعه یک رهیافت حقوق بشری به توسعه انسانی است. تروریسم سایبری می‌تواند با اثرگذاری بر اقدامات دولت‌ها در حوزه‌های اقتصادی، منجر به کاهش توسعه اقتصادی و رشد فقر شود و در برخورداری عادلانه از فرصت‌ها و خدمات دولتی در بهداشت عمومی و آموزش، حق تعیین سرنوشت و حاکمیت بر منابع طبیعی مانع ایجاد کند. از این گذشته تحقق توسعه انسانی تنها در سایه صلح امکان‌پذیر است و در مقدمه اعلامیه حق بر توسعه نیز به نظم اجتماعی اشاره شده که حقوق بشر در سایه آن محقق می‌شود. این در حالی است که تروریسم و اشکال مختلف آن ناقض صلح و نظم اجتماعی به شمار می‌آیند. در این راستا

تکالیف دولت‌ها در تحقق کلیه حقوق بشری که توسط اقدامات تروریستی مورد آسیب یا نقض قرار می‌گیرند، وابسته به مبارزه همه‌جانبه و چندبعدی در سایه مقررات حقوق بین‌الملل است.

۲-۳- حق بر صلح: اهمیت صلح در تحقق حقوق بشر و آزادی‌های اساسی در مقدمه منشور ملل متحد ذکر شده است. حق بر صلح را می‌توان، توسعه ماده سوم اعلامیه جهانی حقوق بشر دانست که حق همه افراد را به حیات، آزادی و امنیت فردی به رسمیت می‌شناسد. بیانیه کنفرانس تهران در ۱۹۶۸ نخستین سندی است که برخورداری از صلح را از منظر حقوق بشر مورد اشاره قرار داده است. این بیانیه با برقراری ارتباط میان صلح و حقوق بشر به این نکته تأکید می‌کند که صلح جهانی آرمان بشر است و صلح و عدالت لازمه قطعی تحقق کامل حقوق و آزادی‌های بشر است. بیانیه زمینه را برای طرح و شناسایی «حق بر زندگی در صلح» به عنوان حقی بشری فراهم آورد.

در پی ظهور این مفهوم در ادبیات حقوقی بین‌الملل، مجمع عمومی سازمان ملل متحد نیز با تصویب قطع‌نامه «آماده‌کردن جوامع برای زندگی در صلح» گام در مسیر نهادینه‌سازی حق بر صلح گذاشت. در این قطع‌نامه آمده است که هر ملت و هر فردی قطع نظر از نژاد، زبان، باور و جنسیت از حق زندگی در صلح برخوردار است. به علاوه چندی بعد در سال ۱۹۸۴ مجمع عمومی سازمان ملل متحد اقدام به صدور قطع‌نامه‌ای تحت عنوان اعلامیه حق مردم بر صلح کرد و در آن ضمن شناسایی حق بر صلح، به عنوان حقی مقدس دولت‌ها را مکلف به حفظ و ترویج آن در سطوح ملی و بین‌المللی دانست. حق بر صلح زمینه را برای تحقق دو نسل دیگر حقوق بشر فراهم می‌سازد.

تروریسم در اسناد اعلامی و الزامی همواره به عنوان یک عمل جنایت کارانه و عملی غیر قابل توجیه در نظر گرفته شده است. همچنین دبیرکل سازمان ملل متحد پس از حوادث ۱۱ سپتامبر و نیز کمیسرعالی کمیسیون حقوق بشر از آن به عنوان جنایت بر ضد بشریت یاد کرده‌اند (۸).

تروریسم ویرانگر نظم حقوقی است، حمایت از حقوق انسانی خواه در زمان صلح یا جنگ به مثابه اصلی استوار به نظر می‌رسد و جامعه بین‌المللی چنین کارکردی را رسالت نظم حقوقی می‌داند. تحولات اخیر نشان داده است که صلح بیش از هر زمان دیگری در معرض تهدید و نقض می‌باشد و فقدان حاکمیت عدالت بر روابط بین‌المللی به آن دامن زده است. جامعه جهانی نیز به جای شناخت علت‌ها، بر سر معلول‌ها متمرکز شده است و همین عامل باعث شده پیشگیری لازم برای بحران‌های تروریستی صورت نگیرد (۲۵).

۳-۳- حق بر محیط زیست سالم: طرفداران حقوق بشر حق بر محیط زیست سالم را به عنوان یک حق مستقل حقوق بشری برای داشتن زیست با کیفیت به رسمیت می‌شناسند. حق به محیط زیست هم منعکس‌کننده ارزش‌های متعالی و پایه‌ای همانند حق به حیات، حق سلامتی، حق به زندگی با استاندارد است و هم با پیش‌نیازهای تداوم حیات نسل کنونی و نسل‌های آتی همانند توسعه پایدار ارتباط تنگاتنگ دارد.

حقوق بشر در سطح ملی و بین‌المللی متوجه حمایت از افراد انسانی است. حق برخورداری از محیط زیست سالم به عنوان یک حق مستمر با نگاه به نسل‌های آینده در حقوق بین‌الملل و حقوق داخلی شناسایی شده است. پروفسور رنه مدرس آکادمی لاهه در ۱۹۷۴ بیان نموده که: «مفهوم کنونی حمایت از حقوق بشر باید به حق محیط زیست پاک و عاری از آلودگی مانند حق برآب وهوای سالم گسترش یابد.» این حق نخستین‌بار در اعلامیه ۱۹۷۲ استکهلم، وصف حقوق بشری یافت. در اصل اول این اعلامیه، حق بهره‌مندی همگان از محیط زیست سالم را بیان می‌کند و این حق را مکمل دو نسل دیگر حقوق بشر، یعنی حقوق آزادی و برابری قلمداد نموده است. در پیش‌نویس میثاق حقوق همبستگی ۱۹۸۲ نیز، تأکید بر این حق به چشم می‌خورد (۲۶).

تروریست‌ها از طریق فضای سایبر، با پخش مواد سمی و خطرناک مانند مواد هسته‌ای ممکن است باعث آلودگی آب‌ها، هوا و محیط زیست شوند. دسترسی تروریست‌ها به زباله‌های اتمی، مواد و تجهیزات هسته‌ای و رادیواکتیو و نیز سرقت و

تجارت مواد هسته‌ای این خطر را دوچندان ساخته است. این اقدامات البته حق بر سلامت را نیز به مخاطره خواهد افکند. داعش پیش از این از سلاح شیمیایی از جمله گاز خردل در عراق و سوریه استفاده کرده است.

۴ـ نسل چهارم حقوق بشر

در تحولات نوین جوامع بشری حق ارتباطات به عنوان نسل چهارم حقوق بشر گفتمانی نوین و ایده‌ای جدید در عصر اطلاعات محسوب می‌شود. اهمیت این نسل ازحقوق بشر تا آنجاست که کارشناسان تأکید دارند که امروزه تحقق حقوق مهمی چون حق حیات یا حق تعیین سرنوشت بدون برخورداری از حق ارتباطات به طور کامل میسر نیست (البته برخی حقوقدانان محتوای نسل چهارم حقوق بشر را در حمایت از کرامت انسانی در برابر سوءاستفاده‌های احتمالی از علم دانسته‌اند).

حق ارتباطات به عنوان نسل چهارم حقوق بشر برای نخستین‌بار توسط ژان فیلیپ دارسی فرانسوی در سال ۱۹۵۴ مطرح شد. او در مقاله خویش در «مجله فرانسوی ارتباطات»، راجع به «حق ارتباط» چنین نوشته بود: «مفهوم تحول پیاپی آزادی‌ها و مسؤولیت‌ها، در واقع در کانون اصلی و مربوط به حق ارتباط، قرار دارد.»

فرانسیس بال استاد علوم ارتباطات انستیتوی مطبوعات دانشگاه پاریس، برای «حق اطلاع» تعریف زیر را ارائه کرده است: حق اطلاع (شامل حق آزادی فکر، وجدان و مذهب، حق دارابودن عقاید، حق بیان عقاید، بدون دخالت طرف‌های عمومی یا خصوصی، حق مردم برای برخورداری از اطلاعات لازم در مورد امور مربوط به علائق و منافع عمومی و حق دسترسی به اطلاعات درباره موضوع‌های طرف توجه عموم)، ضرورت برخورداری همه شهروندان، از امکان دسترسی به تمام اخبار و گزارش‌های جاری، چه درباره خود رویدادها و چه در مورد بیان و تشریح نظرات و عقاید مربوط به آن‌ها را دربر می‌گیرد. مشروط به آنکه رویدادها و بازتاب‌های آن‌ها، به شیوه قابل درک برای هر فرد ارائه شوند. در غیر این صورت، آزادی به امتیازی برای چند نفر، تبدیل خواهد شد...» (۲۷).

حق بر ارتباط و اطلاع، به عنوان مقدمه تضییع حقوق بشری دیگر در فضای سایبر مورد نقض و تهدید قرار می‌گیرد. تروریست‌ها در فضای سایبر با استفاده از انواع بدافزارها، این حق را که امروزه به عنوان یکی از ارکان ارتباطات اینترنتی است مورد هجمه قرار می‌دهند. آنان داده‌ها را تغییر می‌دهند یا غیر قابل دسترس می‌نمایند، سرویس‌های ارائه خدمات را قطع نموده یا با اختلال مواجه می‌کنند، دستیابی مجاز به تمام یا بخشی از یک سیستم پردازش داده را با اختلال مواجه می‌کنند و آموزش‌های غیر انسانی خود را جایگزین مطالب آموزشی مفید می‌نمایند. ارتباط در این راستا اعم از ارتباطات مالی و پولی، کمک‌ها و روابط بشردوستانه، مکاتبات دولتی و... است، لذا تروریسم سایبری در حوزه نسل چهارم مقدمه‌ای بر نقض سایر نسل‌های حقوق بشری است.

نتیجه‌گیری

از آنجایی که حقوق بشر به طور ذاتی به همه ابنای بشر تعلق دارد، دولت‌ها باید تکالیف و تعهدات خود را مطابق مندرجات اسناد بین‌المللی حقوق بشری در مبارزه با نقض حقوق بشر و آزادی‌های بنیادین به فضای سایبری هم تسری دهد. با ویژگی‌هایی که فضای مجازی برای اقدامات تروریستی فراهم می‌آورد و خسارات شدید مالی، جانی و ترس شدیدی که چنین اقداماتی در جوامع ایجاد می‌کنند، از تعداد کسانی که باور به وجود تروریسم سایبری ندارند، کاسته خواهد شد. محیط سایبر قابلیت اعمال بسیاری از قواعد کلاسیک حقوق بین‌الملل، از جمله حقوق بشر را ندارد و پارادایم حاکم، قانونگذار صالح، قابلیت انتساب، مرجع رسیدگی صلاحیت‌دار و قواعد حل تعارض در این فضا منحصر به فرد است.

اگرچه تروریسم سایبری مانند دیگر انواع اقدامات تروریستی مانع استیفای کامل از حقوق بشر و آزادی‌های اساسی می‌شود، اما شیوه نقض حقوق بشر و آزادی‌های بنیادین در این فضا کاملاً متفاوت است. بنابراین شیوه مبارزه با آن نیز روش‌های خاص خود را می‌طلبد، علاوه بر حقوق مدنی در جامعه‌ای که وحشت از اقدامات تروریستی بر آن سایه افکنده، امکان بهره‌مندی کامل از حقوق سیاسی،

اقتصادی، اجتماعی، فرهنگی و حقوق همبستگی نیز تا حد زیادی منتفی است.

طبق مندراجات مواد ۲۹ و ۳۰ اعلامیه جهانی حقوق بشر، هر شخص یا گروه در مقابل جامعه دارای تکالیفی است، از آن جمله آنکه نباید به فعالیتی مبادرت ورزد که هدف یا نتیجه آن مخدوش‌کردن حقوق بشر و آزادی‌های اساسی دیگران باشد. این نکته اساسی در ماده ۵ میثاق بین‌المللی حقوق مدنی و سیاسی نیز تکرار شده و مؤید این مطلب است که فعالیت‌های تروریستی ناقض اسناد بین‌المللی حقوق بشر به شمار می‌آید. دولت نیز متعهد است که نه‌تنها از تعرض به حقوق بشر و آزادی‌های اساسی بپرهیزد، بلکه تعهد به تضمین رعایت حقوق بشر (Duty to Ensure) در نتیجه اصل حاکمیت و صلاحیت انحصاری دولت بر قلمرو و افراد تحت صلاحیت خود، دارد.

در مورد مسأله جنایت علیه بشریت بودن تروریسم سایبری نیز اگرچه حقوق موضوعه آن را جنایت تلقی نمی‌کند، اما طبق حقوق هنجاری، امکان شناسایی آن در صورت مطابقت اقدامات با ماده ۷ اساس‌نامه رم، به عنوان جنایت علیه بشریت وجود دارد. مسأله دیگر تفکیک میان حقوق فردی و جمعی در اسناد حقوق بشری است، در حالی که در این اسناد تمایل به سمت فردگرایی است، فضای سایبر به سمت ایجاد شهروند جهانی پیش می‌رود که حمایت جمعی را می‌طلبد، لذا همکاری‌های بین‌المللی در حوزه حقوق کیفری، فنی و قانونگذاری می‌تواند راه مبارزه همه‌جانبه با این پدیده شوم را هموار نماید.

References

1. Krasavin S. What is Cyber-terrorism? Computer Crime Research Center. Computer Crime Research Center; 2002. Available at: http://www.crime-research.org/library/ Cyber-terrorism.htm. Accessed December, 2018.

2. Pakzad B. Cyber Terrorism a New Threat to National Security. Tehran: Islamic Azad University, Research Vice-Chancellor, Office of Science Production Expansion; 2010.

3. Kim JT, Hung T. Status and requirements of counter cyber terrorism. World Academy of Science, Engineering and Technology; 2011. p.1-4.

4. Alipour H. The notion of being relative crime. M.A, Faculty of Humanities. Tehran: Tarbiat Modares University; 2002.

5. Prasad K. Cyberterrorism: addressing the challenges for establishing an international legal framework. Western Australia: Edith Cowan University; 2012. p.1-9.

6. Available at: http://www.un.org/press/en/2004/ sgsm9372.doc.htm. Accessed December, 2018.

7. Shackelford SJ. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkeley J Int'l Law* 2009; 27(192): 192-251. Available at: https://www.scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil. Accessed December, 2018.

8. Abdollahi M. Terrorism: Human rights and Humanitarian law. Tehran: The SD Institute of Law Research and Study; 2009.

9. UNODC, in collaboration with the United Nations Counterterrorism Implementation Task Force. "The use of the Internet for terrorist purposes", Library Section. Vienna: United Nations Office; 2012. p.1-158.

10. Ghassemi GH, Bagherzadeh S. The Status of Human Rights in the Fight against Cyber-Terrorism. *International Law Review* 2015; 32(52): 227-254.

11. Working Group Compendium. Countering the Use of the Internet for Terrorist Purposes - Legal and Technical Aspects. United Nations Office at Vienna: United Nations Counter - Terrorism Implementation Task Force; 2011. p.1-66.

12. Ghari Seyed Fatemi SM. Hoghooghe Bashar dar Jahane Moaser. Daftare Dovom: Jostarhaye Tahlili az Hagh ha va Azadi ha. Tehran: The SD Institute of Law Research and Study; 2010.

13. Zamani GH. Bistoyek Goftar dar Hoghooghe Beinolmelal. Tehran: Khorsandy Publication; 2016.

14. Voorhoof D. Internet and the Right of Anonymity, Proceedings of the Conference Regulating the Internet, Belgrade. Edied by Surculija J. Belgrade, Serbia: Center for Internet Development; 2010. p.163-173. Available at: https://www.core.ac.uk/download/pdf/ 55901120.pdf. Accessed December, 2018.

15. Sieber U. Cybercrimes. Translated by Nouri MA. Tehran: Ganjedanesh; 2011.

16. Charvat JM. Cyber Terrorism: A New Dimension in Battle space. Estonia: NATO Cooperative Cyber Defense Centre of Excellence; 2009. p.1-11. Available at: https://www.ccdcoe.org/publication-library.html. Accessed December, 2018.

17. Niavarani S. Manzelate Haghe bar Amoozesh dar Nezame Beinolmelali Hoghooghe Bashar. *Legal Research Quarterly* 2010; 13(144): 176-201.

18. Committee on Economic, Social & Cultural Rights (CESCR), the Right to the Highest Attainable Standard of Health, General Comment No.14. Office of the High Commissioner of Human Rights; 2000.

19. Javid E, Niavarani S. The scope of the right to health in international human right law. *Public Law Research* 2014; 15(41): 47-70.

20.Study Group on Cybersecurity, Terrorism,and International Law. Overview of international legal issues and cyber terrorism, international law association. London: International Law Association; 2014. p.1-21. Available at: http://www.ila-hq.org/ download.cfm/docid. Accessed December, 2018.

21. Vakil AS, Askari P. Third generation of human rights. Tehran: Majd Publication Institute; 2005.

22. Rezaee Nejad E. Tamoli bar Mafhoome Haghe bar Tose-e. *Daneshnameh Hoghoogh Siasat* 1999; 4(3): 13-34.

23. Raee M. Jaygahe Haghe Tose-e dar Hoghooghe Bashare Moaser. *Marefat* 2001; 49: 16-27.

24. E.S.C. Res. 1571(L), U.N. ESCOR, 15th Sess., Supp. No.1, at 4,1971G.A. Res. 2804, U.N. GAOR, 26th Sess., Supp. No.29, at 55, U.N. Doc. A/8578; 1971.

25. Harrison dinniss H. Cyber Warfare and the Laws of 3War, Gorouhe Tadvin va Tarjomeh Sazman Padafand Gheire Amel. Tehran: Jahan Jame Jam; 2015.

26. Habibi MH. Haghe Barkhordri az Mohite Ziste Salem be onvane Haghe Bashariat. *Law and Political Science* 2003; 60(0): 131-170.

27. Motamed Nejad K, Motamed Nejad R. Hoghooghe Ertebatat. Tehran: Bureau of Media Studies and Planning; 2007.