---Criminal Law Research ---------
Autumn 2022, Vol 11 (40), PP. 105-125
jclr.atu.ac.ir
DOI: 10.22054/jclr.2023.59356.2297

Original Research
Received: 14/Apr/2021 Accepted: 19/Oct/2022
eISSN: 2476-6224 ISSN: 2345-3575

Online boycott: criminal action or reaction at the level of international law

Abolfath Khaleghi* Associate Professor, Faculty of Law, The University of Qom, Qom, Iran.

Parisa Saghafi PhD Candidate of Criminal Law and Criminology, The University of Qom, Qom, Iran.

Abstract

In today's age, the Internet as a wide and important communication tool can be sanctioned based on Article 41 of the United Nations Charter and international laws under the guaranty of implementation. Despite this prediction, no clear action has been reported by the Security Council in this regard. Although in practice, these are the governments that apply this restriction against each other without any permission and legal order and accept such restrictions within the limits of their international treaties and legal principles, but this is only as long as the countries are within the scope of power. have not taken action. In this case, instead of being a guarantee of enforcement, the internet ban becomes criminal in nature and is condemned by another enforcement guarantee. With the studies carried out in this research, in a descriptive-analytical way, the internet embargo is expressed in two distinct concepts and examples, one time as a guarantee of implementation and another time as an international crime, and finally, this is expected from the Security Council with Such behavior that violates international security and peace on a macro level, such as war and internet terrorism, and the International criminal Court should apply the necessary procedures for judicial proceedings.

Keywords: Sanctions (Boycott), Enforcement Guarantees, Internet, International Law.

* Corresponding Author: ab-khaleghi@qom.ac.ir
How to Cite: Khaleghi, A., & Saghafi, P. (2022). Online boycott: criminal action or reaction at the level of international law. *Journal of Criminal Law Research*, 11(40), 105-125. doi: 10.22054/jclr.2023.59356.2297.

مقاله پژوهشی

--فصلنامه علمی پژوهش حقوق کیفری---------

دوره ۱۱، شماره ۴۰، پاییز ۱۴۰۱، ۱۲۵-۱۰۵

jclr.atu.ac.ir

DOI: 10.22054/jclr.2023.59356.2297

تحریم اینترنتی: کنش یا واکنش کیفری در سطح حقوق بین‌الملل

ابوالفتح خالقی * دانشیار دانشکده حقوق دانشگاه قم، قم، ایران.

پریسا ثقفی دانشجوی دکتری حقوق جزا و جرم‌شناسی دانشگاه قم، قم، ایران.

تاریخ دریافت: ۱۴۰۰/۰۱/۲۵ تاریخ پذیرش: ۱۴۰۱/۰۷/۲۷ ISSN: ۲۳۴۵-۳۵۷۵ eISSN: ۲۴۷۶-۶۲۲۴

چکیده

در عصر حاضر اینترنت به عنوان یک ابزار ارتباطی گسترده و مهم می‌تواند بر مبنای مادۀ ۴۱ منشور سازمان ملل متحد و قوانین بین‌المللی تحت عنوان یک ضمانت اجراء مورد تحریم قرار گیرد. با وجود این پیش‌بینی، تاکنون اقدام بارزی از سوی شورای امنیت در این خصوص گزارش نشده است. اگرچه در عمل، این دولت‌ها هستند که بدون هیچ مجوز و دستور قانونی این محدودیت را علیه یکدیگر اعمال می‌کنند و چنین محدودیت‌هایی را در حدود معاهدات و اصول حقوقی بین‌الدولی خود می‌پذیرند، اما این هم تا زمانی است که کشورها از حیطۀ قدرت وارد عمل نشده باشند. در این صورت تحریم اینترنتی بجای ضمانت اجراء بودن، ماهیت مجرمانه می‌یابد و توسط ضمانت اجرایی دیگر پاسخ داده می‌شود. با مطالعات انجام‌شده در این تحقیق به روشی توصیفی-تحلیل به بیان تحریم اینترنتی در دو مفهوم و مصداق متمایز، شامل ضمانت اجراء و جرم بین‌المللی پرداخته می‌شود. النهایه از شورای امنیت ملل متحد انتظار می‌رود با ارتکاب رفتارهایی که ناقض امنیت و صلح بین‌المللی هستند نظیر آنچه در سطح کلان جنگ و تروریسم اینترنتی محسوب می‌شوند، مقابله نماید و دیوان کیفری بین‌المللی جهت رسیدگی قضائی مراحل لازم را اعمال کند.

واژگان کلیدی: تحریم، ضمانت اجرا، اینترنت، حقوق بین‌الملل.

* نویسنده مسئول: ab-khaleghi@qom.ac.ir

مقدّمه

برمبنای منشور سازمان ملل، مقابله با رفتارهای ناقض صلح و امنیت تابعان در سطح بین‌الملل، در سه قالب ضمانت اجرای اخلاقی، محدودکنندهٔ حقوق و ضمانت اجرای نظامی صورت می‌پذیرد. در حال حاضر ابتنای اکثر این ضمانت اجراها ناشی از تصمیمات مجمع عمومی و شورای امنیت سازمان ملل می‌باشد، اما در خصوص ضمانت اجرای محدودکنندهٔ حقوق بجز تحریم سیاسی یا اقتصادی، از دیگر تحریم‌ها نظیر تحریم فرهنگی، اجتماعی و بویژه تحریم اینترتی، سوابق روشن و دقیقی در دسترس نیست. پیشی گرفتن ارتباطات اینترنتی بر سایر روش‌های متداول و استفادهٔ ابزاری از اینترنت در اکثر ابعاد زندگی اجتماعی، در سطح بین‌الملل بر کنش‌های مجرمانه و واکنش‌های نسبت به آن تأثیر بسزایی داشته است، به نحوی که در عرصهٔ ضمانت اجراهای بین‌المللی بحث از ضمانت اجرای اینترنتی یا تحریم ارتباطات اینترنتی می‌شود. دسترسی به شبکهٔ اینترنت و محتوای مجازی پیوند مستقیمی با حق دسترسی آزاد به اطلاعات ذیل حقوق ارتباطات بدل شده است. بدین ترتیب هر فردی حق دارد تا به اینترنت دسترسی داشته باشد. البته ابعاد مفهومی و مصداقی این حق نوپدید مورد مناقشه است (انصاری، ۱۳۹۹: ۵۲). علیرغم شناسایی حق دسترسی آزاد به اطلاعات و بالطبع شبکه‌های رایانه‌ای و اینترنتی، به دلیل وجود امکان استفاده‌های ناروا از این حق، پیش‌بینی سلب حق دسترسی به اینترنت اجتناب‌ناپذیر می‌نماید. نمونهٔ واضح سوءاستفاده از این حق، انتشار بدافزار یا ویروس‌های مخرب رایانه‌ای است که در فضای سایبر تولید و تکثیر می‌شوند. نظیر آنچه در سال ۲۰۱۰ در خصوص ویروس بسیار خطرناک استاکس نت توسط رژیم صهیونیستی (دولت اسرائیل) رخ داد (Yong Wang, Dawn Gu, Dao gang Peng, Shuai Chen & Heng Yang, 2012: 640). هر چند به طور رسمی مسئولیت آن را نپذیرفتند، اما این ویروس نسبت به دستگاه‌های مشابه در مرکز اتمی دیمونا مورد آزمایش قرار گرفته بود.[1] این ویروس به گونه‌ای طراحی شده بود که با ورود به تجهیزات هسته‌ای نطنز، کنترل چرخش و دوران سانتریفیوژهای غنی‌سازی اورانیوم را در اختیار گرفت. کارکرد مخرب ویروس این

1. www.nytimes.com/2011/01/16/world/middleeast

گونه بود که به صورت ناگهانی در وضعیت چرخش‌های دورانی سانتریفیوژها، اختلال پدید می‌آورد، به نحوی که گاه سرعت حرکت سانتریفیوژها بیش از حد معمول و گاه بسیار کمتر از آن می‌شد. با این روش در غنی‌سازی اورانیوم اختلال ایجاد و ماشین‌های استخراج از مدار تولید خارج می‌شدند. بکارگیری این شیوه در واقع ترجیح بکارگیری جنگ‌افزارهای سایبری بر یورش و حملهٔ نظامی به تأسیسات هسته‌ای صلح آمیز ایران بود.[1]

حملهٔ سایبری ۱۲ خرداد ماه ۱۴۰۱ به زیرساخت‌های الکترونیکی شهرداری تهران و قطع خدمات‌رسانی طیف وسیعی از خدمات غیرحضوری این شهرداری نمونهٔ دیگری از تهاجم اینترنتی است. پس از این حمله سازمان پدافند غیرعامل اعلام داشت: امروز الگوی جدیدی به نام جنگ سایبری زیرساختی داریم که مدل توسعه‌یافته‌ای از جنگ است؛ امنیت سایبری، موضوعی کاملاً پیشرفته است. این سازمان تلویحاً رژیم صهیونیستی را مسئول حادثه اعلام کرد.[2] سوءاستفاده از ارتباطات اینترنتی شبکه‌های سایبری و هوش مصنوعی تا آنجا پیشرفته که آتش سلاح‌های جنگی اتوماتیک را کنترل و در مواردی برای ترورهای هدفمند بکار گرفته شده‌اند. مانند تجهیزات و ابزارهای نظامی که در ترور شهیدان هسته‌ای کشورمان همچون حادثهٔ منجر به ترور شهید فخری‌زاده مورد استفاده قرار گرفتند؛[3] بنابراین سلب حق دسترسی به شبکهٔ اینترنت یا تحریم اینترنتی از جمله واکنش‌هایی است که برای حفظ صلح و امنیت بین‌المللی ذیل مادهٔ ۴۱ منشور ملل متحد توسط شورای امنیت ظرفیت اعمال خواهد داشت.

تحریم در لغت به معنای ناروا کردن و حرام کردن (معین، ۱۳۶۰: ۱۰۳۷) و تحریم اینترنتی به معنای ایجاد محدودیت در استفاده از اینترنت، در دو سطح ملی و بین‌المللی قابل بررسی است؛ ۱- تحریم اینترنتی در سطح ملی زمانی است که دولت‌ها جهت مقابله با جرائم اینترنتی در محدودهٔ قلمرو سرزمینی خود اقدام به محرومیت مجرمان در استفاده از اینترنت می‌کنند (Castell, 2005: 98)، نظیر آنچه در حقوق داخلی تحت عنوان مجازات تکمیلی و تبعی از

1. www.researchgate.net/publication/
2. https://paydarymelli.ir
3. www.nytimes.com/2021/09/19/world/middleeast

آن یاد می‌شود، مانند منع حق دسترسی به فضای مجازی و همچنین در مواقعی که دولت‌ها جهت اعمال سیاست‌های راهبردی ملی با هدف جلوگیری از آشوب‌های داخلی و پیشگیری از اقدامات مجرمانه مبتنی بر سوءاستفاده از ارتباطات اینترنتی و انتشار محتوای مجعول یا تعاملات سایبری بزهکاران به ناچار دسترسی اتباع و شهروندان به اینترنت را موقتاً به صورت کلی یا جزئی قطع می‌نمایند (Government Printing Office, 2011: 321)؛ در راستای همین اقدام قطعنامه‌ای تحت عنوان دفاع از آزادی اینترنت در شورای حقوق بشر از سوی مجمع عمومی سازمان ملل با مفهوم «حق اینترنت از حقوق بشر است» به تصویب رسید (Andrade, 2016: 249). ۲- تحریم اینترنتی در سطح بین‌الملل محدودیت در روابط اجتماعی است که از سوی کشورها (زمانی، غریب‌آبادی، ۱۳۹۴: ۹۳) و یا سازمان‌های بین‌المللی علیه دولت دیگر صورت می گیرد. آنچه از این تحقیق مدنظر است تحریم اینترنتی در سطح بین‌الملل می‌باشد. در سطح بین‌الملل دو نوع تحریم اینترنتی وجود دارد. یک نوع تحریمی است که از سوی شورای امنیت در قالب ضمانت اجرای محدودکنندهٔ روابط اجتماعی موضوع مادهٔ ۴۱ منشور سازمان ملل می‌تواند شمرده شود و در قالب قطع وسایل ارتباطی از آن یاد شده است.

بنابراین از آنجایی که اینترنت نیز به عنوان رسانهٔ نوین (سلطانی‌فر، ۱۳۹۱: ۷۶) و به عنوان یک وسیلهٔ ارتباطی در نظر گرفته می‌شود، می‌تواند در قالب این نوع ضمانت اجراء موضوع تحریم شورای امینت قرار گیرد (Schmitt, 2013: 70-71). تحریم بین‌المللی در نوع دیگر، تحریم یک دولت توسط دولت دیگر است که در اصل مشروعیت یا فقدان آن جای تامل بسیار دارد. مقابله با جرائم اینترنتی در سطح بین‌الملل طبق کنوانسیون جرائم سایبری مصوب شورای اروپا در ۲۳ نوامبر ۲۰۰۱ با عنوان همکاری بین‌المللی بر عهدهٔ دولت‌ها نهاده شده است (Hlubik Schell, 2007: 120). در حالی که برخی معتقدند مقابله با چنین رفتارهایی برخلاف سایر ابزارهای رسانه‌ای صرفاً توسط یک نهاد نظارتی بین‌المللی و با استفاده از قوانین بین‌المللی و تحریم‌ها صورت می‌پذیرد (Kung, 2008: 11). مطابق این دیدگاه چنین اقدامی نمی‌تواند توسط کشورها به انفراد انجام شوند اما حتی اگر این نظر را بپذیریم چرا در قالب همکاری با شورای امنیت قابل تصور نباشد؟ بویژه آنکه در منشور نیز بدین نحو مقرر

شده است. با وجود این، در عمل چنین تحریم‌هایی توسط کشورها علیه یکدیگر[1] به کار گرفته می‌شود.

پیش از گسترش فضای سایبر و توسعهٔ اینترنت، تحریم وسایل ارتباطی بر سایر ابزارهای ارتباط جمعی نظیر ماهواره، تلویزیون و ... صورت می‌گرفت. برای مثال در سال ۲۰۱۱ یوتل‌ست از ارائهٔ خدمات به ایستگاه‌های تلویزیونی ایران به ادعای ارسال پارازیت بر شبکه بی‌بی‌سی از سوی ایران، به دستور پارلمان اروپا در قطعنامهٔ ۱۷ نوامبر برخلاف مقررات بین‌المللی ناظر بر ارتباطات ماهواره‌ای خودداری نمود (حکمتی، ۱۳۹۶: ۷۸). استفادهٔ ابزاری از تحریم ارتباط ماهواره‌ای در کشورها به عنوان یک ضمانت اجراء در نظر گرفته شده است (Frosio, 2020: 537) و با رسوخ ارتباطات اینترنتی در اکثر ابعاد زندگی به تدریج تحریم هر یک از موارد قیدشده در منشور بر روند اینترنتی آن بخش نیز ایجاد محرومیت نمود، نظیر تحریم اقتصادی که موجبی برای ایجاد منع و محدودیت در تجارت الکترونیک کشور مورد تحریم می‌شود. در سطح بین‌الملل نمونه‌هایی از تحریم اینترنتی در قالب تحریم اقتصادی کشورها علیه یکدیگر ملاحظه می‌شود که در ادامه در اقسام تحریم اینترنتی به آن پرداخته می‌شود، تحریم اقتصادی عراق توسط شورای امنیت از آن موارد است (Inc. Ibp, 2015: 175). در حال حاضر نمونه‌ای از تحریم اینترنتی صرفاً مجزا از سایر تحریم‌ها یافت نشده و هنوز اقدامی از سوی شورای امنیت جهت تحریم اینترنتی کشور متخلف دیده نشده ولیکن این امر از امکان تحقق این نوع از تحریم اینترنتی توسط شورای امنیت نمی‌کاهد و همچنان استفاده از چنین مکانیزمی در سطح بین‌الملل مورد شناسایی و پذیرش قرار گرفته است.

اینکه تحریم اینترنتی چیست و ماهیت آن چگونه است و حول چه محورها و انواعی قرار می‌گیرند، پرسش‌هایی هستند که کشف پاسخ آنها هدف اصلی این مقاله می‌باشد تا با استفاده از روش توصیفی- تحلیلی با رجوع به منابع و ضوابط موجود این تحقیق به انجام رسد.

1. https://www2.computable.nl/uploads/pdf/multistakeholder-imposition-of-internet-sanctions.pdf.

۱. امکان‌سنجی تحریم اینترنتی

مادۀ ۴۱ منشور ملل متحد مقرر می‌دارد که شورای امنیت می‌تواند تصمیم بگیرد که برای اجرای تصمیمات آن شورا به اقداماتی که متضمن به کارگیری نیروی مسلح نباشد مبادرت نماید و می‌تواند از اعضای ملل متحد بخواهد که به این قبیل اقدامات مبادرت ورزند. این اقدامات ممکن است شامل متوقف ساختن تمام یا قسمتی از روابط اقتصادی و ارتباطات راه‌آهن، دریایی، هوایی، پستی، تلگرافی، رادیویی و سایر وسائل ارتباطی و قطع روابط سیاسی باشد. در مواردی که خطر تهدید یا نقض صلح و امنیت بین‌المللی باشد، امکان تحریم اینترنتی از سوی شورای امنیت ذیل سایر وسایل ارتباطی وجود دارد، اما با توجه به بررسی انجام‌شده در حال حاضر نمونه‌ای از این نوع تحریم در عالم خارج محقق نشده است. برخی عقیده دارند که تحقق عملی و فنّی چنین تحریمی امکان‌پذیر نیست، زیرا اکنون اکثر کشورها دارای مرکز داده می‌باشند (Schmitt, 2016: 359). بالعکس در نوع دیگر، تحریم اینترنتی دولت‌ها علیه یکدیگر عملاً در حال وقوع است و همچنان ادامه می‌یابد. البته در زمانی که با وجود پیش‌بینی قانونی و طبق اصل مشروعیت و عدالت در اعمال ضمانت اجراها، به شورای امنیت مجوز داده می‌شود تا علیه اشیاء غیرنظامی حملات سایبری داشته باشد در اینکه آیا چنین اقدامی قانونی است یا خیر، شبهه ایجاد می‌شود (Schmitt, 2016: 359)، به طریق اولی در مشروعیت چنین اقداماتی که توجیه قانونی ندارد، تصور قانونی بودن آن دشوار است.

برای مثال در تحریم قدرت‌های بزرگ جهانی مانند ایالات متحده علیه کشورهای در حال توسعه یا توسعه‌نیافته همچون کوبا (Deibert, 2008: 272) هیچ یک از این تحریم‌ها که به طور خودسرانه اعمال می‌شود در قوانین بین‌المللی مورد تایید و پیش‌بینی قرار نگرفته است. اکنون این موضوع در مقام بحث است که آیا می‌شود این رفتار را هر چند در قوانین به آن تصریح نشده است طبق عرف و اصول بین‌المللی، قانونی بحساب آوریم یا چنین اقدامی یک رفتار علیه صلح و امنیت جهانی و ناقض قوانین بین‌المللی است؟ در قالب دو فرض می‌توان به این سؤال پاسخ داد:

فرض اول زمانی است که کشوری در راستای حفظ صلح و امنیت بین‌المللی طی درخواست شورای امنیت و یا به جهت معاضدت جهانی اقدام به مقابله با کشور متخلف در قالب تحریم در روابط بین‌المللی می‌نماید. فرض دوم در صورتی است که دولت‌ها برخلاف معاهدات و عرف بین‌المللی در منافع اینترنتی اقدام کرده و سبب تحریم اینترنتی توسط دولت صاحب منافع اینترنتی می‌شوند (ضیائی بیگدلی، ۱۳۸۵: ۱۸۲). در این دو حالت اگر کشور تحریم‌کننده در حد دستور شورای امنیت (Eeckhout, 2011: 504)، طبق معاهدات و بنابر اصول حقوقی نظیر اصل حاکمیت اراده، استقلال و حاکمیت سرزمینی و مادۀ ۴۳ منشور، روابط اینترنتی، اقتصادی و دیپلماتیک خود را با کشور متخلف قطع و محدود نماید، عملی موافق با صلح و امنیت بین‌الملل و قابل پذیرش انجام داده است، اما در فرض سومی اگر از حیطۀ اختیار فراتر رود و سازمان‌های خدمت‌رسان اینترنتی بین‌المللی مانند ICANN[1] و سایر کشورها را جهت ایجاد محدودیت اینترنتی که مورد انتفاع کلیه دولت‌ها به شکل آزادانه است با خود همراه سازد، این اقدام می‌تواند نقض قواعد بین‌المللی و سرآغاز روابط خصمانه قلمداد شود. در عمل نیز این نوع تحریم‌ها اکثراً به جهت کدورت و اختلافات در روابط سیاسی و اقتصادی بین دولت‌ها رخ می‌دهد که در نهایت به تحریم اینترنتی ختم می‌گردد. کمتر موردی یافت می‌شود که چنین اقدامی به عنوان یک ضمانت اجرای عادلانه از سوی دولت‌ها جهت مقابله با رفتارهای اینترنتی خلاف حقوق بین‌الملل نظیر تروریسم سایبری صورت گیرد.

۱-۱. نحوۀ عملکرد در سطح بین‌الملل

در طول ادوار گذشته ایالات متحده از جمله کشورهایی بوده که با تکیه بر قدرت اقتصادی خود سایر کشورها را مورد تحریم اقتصادی و اینترنتی قرار داده است. اگرچه از سال ۱۹۹۸

---

2. The Internet Corporation for Assigned Names and Numbers.

(ICANN) یک شرکت بین‌المللی و غیرانتفاعی است که مسئولیت تخصیص مکان آدرس پروتکل اینترنت (IP)، اختصاص شناسۀ پروتکل، ژنریک (gTLD) و کد کشور (ccTLD) را بر عهده دارد و مالکیت آن به دولت خاصی باز نمی‌گردد و سهامداران متعدد آن شامل کارشناسان فنی و همچنین نمایندگان دولت‌ها هستند (United States Congress, 2015: 15).

طبق طرحی که سال‌ها در دستورکار بوده است، وزارت بازرگانی ایالات متحده طی طرح خصوصی‌سازی، کنترل اینترنت را به یک سازمان بین‌المللی غیرانتفاعی موسوم به اینترنت برای نام‌ها و شماره‌ها (ICANN) اختصاص داده و در سال ۲۰۰۹ نیز در کنفرانسی جهت حفظ حقوق بشر در پی آزادسازی جهانی اینترنت اقدام نموده است (Figliola, 2010: 6)، اما همچنان سیاستگذاری‌های ایالات متحده در راستای تحریم‌های اینترنتی و فشار بر این سازمان‌ها جهت اجرایی کردن اینگونه از تحریم‌ها ادامه دارد. چنین رویه‌ای به این خاطر است که در این سازمان‌ها از روش خودانتظامی استفاده می‌شود. به این معنا که طبق اساسنامهٔ آنها برای آمریکا و کشورهای عضو این سازمان حق وتو در تصمیمات قرار داده شده و این شرکت‌های اینترنتی و یا مالکان تارنماها هستند که طبق تصمیمات ملزم به ایجاد محدودیت در فضای اینترنتی می‌باشند (Casey, 2008: 1-2). لذا علت اعمال تحریم‌های صورت‌گرفته از سوی آمریکا هر چند به صورت جزئی و محدود می‌تواند این مطلب باشد. بنابراین، با وجود احتمال اینکه ملی شدن دسترسی به دیتا سنترها امکان چنین تحریمی را از میان می‌برد، اما بالاخره این دیتا سنترها و سرورهای حمایت‌کنندهٔ اینترنت در معاهدات از طریقی تامین می‌گردند که این طرق بر اساس نوع روابط بین‌المللی کشورها می‌تواند محدود گردد.

۱-۲. مصادیق تحریم اینترنتی

تحریم اینترنتی در قالب سه مصداق تحریم از طریق دامنه‌ها، تحریم هاست‌ها و سرورهای میزبان، تحریم روترها و مسیریاب‌ها (در قالب تحریم اینترنتی مستقل و مستقیم) و تحریم اینترنتی غیرمستقیم قابل بررسی است که به شکل مختصر در ذیل به آنها پرداخته می‌شود.

دامین Domain در لغت به معنی «گستره» می‌باشد. در فرهنگ اصطلاحات اینترنتی به نام ویژه‌ای اطلاق می‌شود که هر یک از وب‌سایت‌ها برای تشخیص و قابلیت دسترسی در مقایسه با وب‌سایت‌های دیگر یا مشابه به خود اختصاص می‌دهند (www.onlindictionary.com). دامین در معنای دامنه و آدرس صفحات اینترنتی در پهنای جهانی با پسوندهایی نظیر COM ORG , و ... در پهنای هر کشور با پسوندی مخصوص مانند نام دامنهٔ IR در ایران، CA در کانادا و ... مشخص می‌گردد. به این معنا که آدرس و دامین خاص هر کشور به عنوان کد

شناسایی آن کشور است و طبق پروتکل‌های اینترنتی هر آدرسی که مشخصهٔ پایانی آن IR. باشد در سطح جهان مشخص می‌گردد که کاربر و مکان استفاده از دامنه ایران است. لذا بر این مبنا گاه اتفاق می‌افتد کشوری که مورد تحریم قرار می‌گیرد امکان ثبت دامنه‌های جهانی را ندارد و این تحت عنوان یک کد در پروتکل‌های اینترنتی قید می‌شود. هرگاه کشور محرومی مثل کانادا با آدرس CA درخواست ثبت دامنه خود را مطرح می‌کند به طور اتوماتیک برای این کشور ثبت دامنه جهانی با اشکال مواجه شده و بیان می‌دارد که امکان ثبت دامنهٔ جهانی را ندارد. در سطح جهان و در زمان تحریم زمانی که IP و یا آدرس دامنه و دامین کشور محروم مورد شناسایی قرار می‌گیرد، سایت‌ها و صفحات خاص اجازه ورود به کاربر آن کشور را نمی‌دهند (سجادی، حیدری، ۱۴۰۰: ۱۶۹).

هاست یا به تعبیر دقیق‌تر وب هاستینگ (Web Hosting) اصطلاحی تخصصی در علم مهندسی رایانه بوده که به معنی میزبانی وب می‌باشد. داده‌ها و محتوای هر سایت در فضایی اختصاصی با منابع سخت‌افزاری مشخص قرار دارد که به کمک آنها سایت در دسترس کاربران برای در اختیار داشتن محتوا قرار می‌گیرد. این فضا تمام یا بخشی از ظرفیت سرور می‌باشد که سایت اینترنتی را میزبانی می‌کند (روحانی رانکوهی و امیری، ۱۳۹۲: ص۱). هر سیستمی هنگام اتصال به اینترنت نیازمند ذخیره‌سازی اطلاعات خود در فضای اینترنت است که این ذخیره‌سازی‌ها در سرورها صورت می‌گیرد که باید مورد خریداری قرار گیرند. هر آنقدر سرور حجم کوچک‌تری داشته باشد و امکان ذخیره نباشد، فعالیت سیستم مورد نظر با اختلال مواجه می‌شود و نیاز به حجم سرور بیشتر دارد که اکثر این سرورها در کشورهای اروپایی قرار دارند (Nakahira, 2006, P1). در حالت تحریم یک کشور ممکن است سیستم‌هایی که فعالیت‌های اصلی را در آن کشور انجام می‌دهند با کمبود حجم سرور مواجه شوند و امکان خرید آنها سلب شده باشد.

اطلاعات اینترنتی از طریق کابل‌ها، کانال‌ها، مسیریاب‌ها و سیستم‌های تبدیلگر IP طبق پروتکل‌های تعریفی صورت می‌پذیرد. این امکان وجود دارد که تحریم در حدود مسیریاب‌ها باشد. یعنی اطلاعات در حدی به پیش بروند ولیکن در مسیر بین مبدا و مقصد هیچگاه به مقصد نهایی نرسیده و به جهت تحریم برخی مسیرها محدود گردند (تنن بام،

۲۰۰۳, ص ۴۲۲ و ۷۰۳). سه نوع یادشده از جمله مصادیق تحریم اینترنتی به شکل مستقیم می‌باشند. اما یک نوع تحریم اینترنتی دیگر وجود دارد که به شکل غیرمستقیم به دنبال سایر تحریم‌ها به وقوع می‌پیوندد.

۲. تحریم اینترنتی غیرمستقیم

اکثر ضمانت اجراهای اجتماعی و محدودکنندهٔ روابط بین‌المللی در قالب تحریم اقتصادی هستند که مستقیما توسط شورای امنیت اعمال می‌شود (نظیر تحریم اقتصادی عراق) یا بواسطه کشورها علیه یکدیگر صورت می‌گیرند (Müller, 2006: 369). البته لازم به ذکر است زمانی‌که تحریم اقتصادی صورت می‌گیرد این تحریم در کلیهٔ زیرساخت‌های اجتماعی-اقتصادی نفوذ می‌کند، لذا هنگامی که کشوری از طرق اینترنتی در حال فعالیت اقتصادی است، این تحریم بعد اینترنتی آن را نیز دربرمی‌گیرد (National Research Council, 2009: 259). از سوی دیگر از آنجایی که محیط اینترنتی در اکثر فعالیت‌های اجتماعی ریشه گسترانیده است، زمانی که بحث از تحریم اقتصادی، فرهنگی، حمل و نقل و سایر تحریم‌های موضوع مادهٔ ۴۱ منشور می‌شود، بعد اینترنتی آن حوزه نیز مورد تحریم قرار می‌گیرد. بنابراین، تحریم اینترنتی می‌تواند در قالب هر یک از روش‌های محدودکنندهٔ روابط تحقق یابد. اما این سؤال مطرح است که چه زمانی تحریم اینترنتی به صورت مستقل قابل اعمال خواهد بود؟

استفاده از ضمانت اجرای تحریم دولت‌ها طبق منشور سازمان ملل در زمان نقض قوانین بین‌المللی است، اما مشخص نگردیده که در مقابل هر نقض چه نوع تحریمی مورد استفاده قرار می‌گیرد. اما طبق آنچه در سطح بین‌الملل به عنوان ضمانت اجرای کارآمد و اصل هوشمندسازی ضمانت اجراها شناسایی شده است، تحریم‌های اینترنتی باید به جا و در همان زمینه که تخلف صورت پذیرفته اعمال شود و مانع دسترسی کل اتباع و افراد آن کشور نشود (حکمتی، ۱۳۹۶: ۸۱). لذا می‌توان بیان کرد که تحریم اینترنتی به طور مستقل زمانی قابل اعمال است که اینترنت به عنوان ابزاری برای ارتکاب تخلف در اختیار تابعان حقوق بین‌الملل قرار گیرد. جنگ رسانه‌ای و سایبری، مانند انتشار ویروس خطرناک استاکس‌نت، تروریسم

سایبری مانند ترور رهبران سیاسی- نظامی و نظیر این رفتارها از جمله موارد ابزاری اینترنت در نقض حقوق بین‌الملل است.

۳. حق دستیابی و انتشار اطلاعات

امروزه با گسترش فضای اینترنتی و وجود شبکه‌های اجتماعی، اتباع کشورها از این طریق اطلاعات مورد نظر خود را نشر و یا کسب می‌کنند که همین امر تا حد زیادی در شکل‌گیری دهکدهٔ جهانی نقش‌آفرین بوده است. در مادهٔ ۱۹ اعلامیهٔ حقوق بشر نیز چنین حقی به صراحت به رسمیت شناخته شده است.[1] با چنین تدبیری تحریم اینترنتی خواه به صورت قانونی یا غیرقانونی حقوق یادشدهٔ اتباع را تحت‌الشعاع قرار می‌دهد. در تحریم غیرقانونی که توسط دولت‌ها علیه یکدیگر اعمال می‌شود پر واضح است که چنین اقدامی حقوق افراد در نشر و دستیابی به اطلاعات را منع یا محدود می‌سازد و یکی از حقوق مقررشدهٔ بشری را دستخوش مخاصمات سیاسی قرار می‌دهد. در این صورت چنین رفتاری می‌تواند هم از جهت مخاصمانه بودن و هم مغایرت داشتن با قواعد حقوق بشری، ناقض حقوق بین‌الملل باشد. در تحریم قانونی توسط شورای امنیت نیز چنین نقضی مشهود به نظر می‌رسد. هیچ کس نمی‌تواند تضمین نماید که حقوق کلیهٔ شهروندان در تحریم اینترنتی کشور تحمل‌کنندهٔ ضمانت اجراء حفظ گردد، زیرا در مقام اعمال ضمانت اجراء و حفظ مصالح حقوق بین‌الملل است. بنابراین، چون قانونی و بنابر ملاحظات سیاسی است، قابل توبیخ نمی‌باشد. در این مواقع همانگونه که بیان گردید تنها طریق عام به حداقل رساندن تبعات تحریم بر اتباع کشور متخلف، می‌تواند استفاده از اصل هوشمندسازی اقدامات تحریم باشد.

---

۱. مادهٔ ۱۹ اعلامیهٔ حقوق بشر: هر انسانی محق به آزادی عقیده و بیان است؛ و این حق شامل آزادی داشتن باور و عقیده‌ای بدون [نگرانی] از مداخله [و مزاحمت]، و حق جستجو، دریافت و انتشار اطلاعات و افکار از طریق هر رسانه‌ای بدون ملاحظات مرزی است.

۳-۱. اعمال عادلانهٔ تحریم اینترنتی

رفتارهای مجرمانه در سطح بین‌الملل برخلاف قوانین ملی مشخصاً مورد جرم‌انگاری و واکاوی در قالب عناصر مادی، معنوی و قانونی قرار نگرفته است. آنچه به عنوان یک جرم بین‌المللی در سطح بین‌الملل شناخته می‌شود همواره رفتارهایی است که در معاهدات، کنوانسیون‌ها و عرف بین‌المللی مجرمانه قلمداد می‌گردد (فیوضی، ۱۳۸۶: ۳۱). لذا در سطح جامعه جهانی، قواعد بین‌المللی که رفتارهای مجرمانه را جرم انگاری می‌نمایند به دو دسته تقسیم می‌شوند: قواعد اولیه شامل عرف و معاهدات و قواعد ثانویه نظیر کنوانسیون‌ها هستند که بعد از نقض تعهدات اولیه ایجاد می‌شوند (دلخوش، ۱۳۹۰: ۲۲۹). از جمله این قوانین مادهٔ ۳۹ منشور سازمان ملل و مواد ۶، ۷ و ۸ اساسنامهٔ دیوان کیفری بین‌المللی است که رفتارهای مجرمانهٔ جنایات جنگی، جنایات علیه بشریت و نسل‌کشی را به شکل کلی پیش‌بینی نموده‌اند.

تخلفات و جرائم اینترنتی بین‌المللی نیز در دو حالت قابل تصور می‌باشند. یک حالت اینترنت به عنوان ابزار مورد استفاده قرار می‌گیرد و حالت دیگر زمانی است که ایجاد محدودیت در اینترنت یک کشور توسط کشور غالب و برتر صورت می‌پذیرد و ایجاد یک نوع تحریم در حقوق و آزادی‌های کشور مغلوب است که بدون وجود پشتوانهٔ قانونی و به شکل مخاصمانه انجام می‌شود. از نمونه‌های بارز هر دو حالت جنگ و تروریسم سایبری است. جنگ سایبری اعمال حملات اینترنتی شامل ایجاد اختلال، حذف و یا تخریب اطلاعات اریانه‌ای علیه شبکهٔ رایانه‌ای کشور متخاصم است که اغلب از طریق بات‌نت[1] به شکل حملات DDOS (حمله‌ای روی سیستم کامپیوتری یا شبکه است که منجر به از دست دادن سرویس‌دهی به کاربران می‌شود)، Spamming (ایجاد بیش از ۸۰ درصد اسپم در سیستم‌های کامپیوتری یک کشور که ایجاد اختلال می‌کند) و سایر حملاتی از این قبیل رخ

---

۱. بات (Bot) مخفف ربات (Robot) و بانت‌نت گسترده‌ترین و جدی‌ترین نرم‌افزار مخرب از راه دور است که در قالب حملات یادشده و سایر حملاتی نظیر سرقت هویت در مقیاس بزرگ (Mass identify theft)، هجوم به سرورها از طریق هک و انتقال پول (Anonymous Internet Access) و سایر موارد چنینی رخ می‌دهد.

می‌دهد. مثال بارز جنگ سایبری حادثهٔ معروف به فارول روسیه در سال ۱۹۸۲ است؛ این حمله با سرقت اطلاعات از قدرت‌های غربی نظیر ایالات متحده توسط دستگاه‌های جاسوسی شوروی و با کنترل و دستکاری در سیستم اتصالات لوله‌های گاز منجر به انفجاری بزرگ و آتش غیراتمی گردید (هریسن داینیس، ۱۳۹۵: ۱۹ و ۲۲). چنین اقداماتی تلویحاً تحت عنوان تروریسم سایبری در مادهٔ ۱۳ قانون جرائم رایانه‌ای ایران نیز جرم‌انگاری شده است. حملهٔ رایانه‌ای آمریکا به تأسیسات هسته‌ای ایران از دیگر نمونه‌های این حملات است (موسوی و همکاران، ۱۳۹۲: ۱۲۴). در هر دو حالت یادشده باید برخوردی هدفمند از سوی جامعهٔ بین‌الملل علیه کشور خاطی صورت پذیرد.

همانگونه که اشاره شد، در سطح بین‌الملل برای آنکه اعمال ضمانت اجراهایی نظیر تحریم علیه یک کشور از سوی شورای امنیت آلودهٔ غرض‌ورزی‌های سیاسی و تبعیض‌آمیز نشوند و در زمان تحمیل آن بر خلاف آنچه تحت عنوان اصل شخصی بودن در قوانین داخلی است، جز کشور متخلف، اتباع آن درگیر صدمات ناشی از تحریم برخلاف حقوق و آزادی‌های بشری نشوند (عاملی، محسنی آهویی، ۱۳۹۷: ۱۰)، استفاده از اصل هوشمندسازی ضمانت اجراها پیشنهاد می‌شود که البته در حد نظریه باقی مانده است. در جهان واقع بیشتر شاهد اعمال اینگونه ضمانت اجراها در قالب غرض‌ورزی سیاسی هستیم. در تحریم اینترنتی نیز باید این اصل پیاده‌سازی شود و مشخص گردد استفاده از اینترنت به چه صورت از سوی دولت و یا سایر اتباع حقوق بین‌الملل سبب نقض حقوق بین‌الملل شده است. برای مثال در بادی امر به این مطلب پرداخته می‌شود که استفاده از چه ابزار اینترنتی سبب قطع سراسری شبکه در کشور متضرر شده و یا موجبات انفجار گسترده در آن کشور فراهم کرده است؛ سپس کشور متخاصم را از استفاده از آن ابزار یا ابزار مشابه در هر زمینه‌ای، محروم می‌کنند.

۳-۲. صلاحیت اجرایی و رسیدگی

با عنایت به اینکه در سطح بین‌الملل دیوان کیفری بین‌المللی جهت رسیدگی به جرائم و جنایات بین‌المللی صلاحیت تکمیلی دارد و این مراجع قضایی ملی هستند که در صورت جرم‌انگاری این جرائم در قوانین خود، صلاحیت اولیهٔ رسیدگی را دارا می‌باشند (عابدینی،

۱۳۹۳: ۳۱۵)، لذا در صورت وقوع جرائم اینترنتی نظیر تروریسم و جنگ سایبری که ویژگی بین‌المللی دارند دولت‌ها مطابق قواعد و اصل صلاحیت جهانی در قلمرو حقوق کیفری بین‌المللی و معاضدت قضائی حق رسیدگی به این نوع از جرائم را خواهند داشت و در درجهٔ دوم در صورت عدم توانایی و یا عدم تمایل نظام‌های قضایی ملی، این دیوان کیفری بین‌المللی است که به این قسم از جنایات رسیدگی می‌کند (خالقی، ۱۳۹۹: ۲۵). اکنون جای این سؤال باقی است که اگر این کشورها هستند که در نهایت صلاحیت رسیدگی به جرائم بین‌المللی نظیر جنگ سایبری یا رایانه‌ای را دارند پس چرا باید تحریم اینترنتی کشوری علیه کشور دیگر را که در موضع قدرت می‌باشد یک رفتار خلاف حقوق بین‌الملل قلمداد نماییم؟

پاسخ به این سؤال در قالب دو دیدگاه متمایز در خصوص حاکمیت قانونی بر فضای سایبری قابل بررسی است. برخی نظر بر حاکمیت انحصاری دولت‌ها بر فضای اینترنت همچون حاکمیت بر آب‌های آزاد دارند، به این نحو که هر دولتی بنابر قدرت خود می‌تواند از این فضا استفاده کند و بر آن حاکمیت داشته باشد. در جایگاه نقد این نظریه بیان می‌شود اینترنت مانند آب‌های آزاد بین دولت‌ها قابل تقسیم نیست. این دیدگاه بر حاکمیت فیزیکی دولت‌ها بر سرورها شکل گرفته و چون در فضای اینترنت یک حاکمیت واحد یا مرکزی نیست و به همین خاطر بین دولت‌ها اختلاف به وجود آمده است. برخی دیگر نظر بر میراث مشترک بشریت بودن اینترنت دارند و اینکه هیچ کشوری حق اعمال حاکمیت بر اینترنت را ندارد؛ طبق این نظریه باید مرجعی فراتر از دولت‌ها بر آن حاکمیت داشته و به وضع قانون بپردازد (ضیایی، شکیب‌نژاد، ۱۳۹۵: ۲۲۸). همین تعارض در مرحلهٔ رسیدگی و اجرای ضمانت اجراهای آن قابل طرح است. لذا در هر مسئله‌ای در حوزهٔ اینترنت به جهت گذران و سیال بودن اینترنت این دو دیدگاه کاربرد دارد. بر مبنای قوانین و اصول حقوقی بین‌الملل در زمینهٔ صلاحیت اجرای تحریم اینترنتی به طور عام، اختیار چنین اقدامی به شورای امنیت سپرده شده و بنابراین نظر دوم یعنی قدرتی فراتر از دولت‌ها باید چنین ضمانت اجرایی را اعمال کند. در مقابل، بنابر اصل صلاحیت مراجع قضائی ملی در خصوص صلاحیت در رسیدگی به جرائم بین‌المللی چون تروریسم و جنگ سایبری، می‌توان نظر اول یعنی

انحصاری بودن قدرت‌ها را پذیرفت. اما در هر دو مورد بهتر آن است که حسب مورد نظر بینابینی را اعمال نمود، به این شرح که برای هر صلاحیت دو فرض در نظر گرفته شود:

در صلاحیت اجرای تحریم اینترنتی و اعمال محدودیت در استفاده از اینترنت، در فرض اول اگر اقدام دولت‌ها بنابر اصل حاکمیت سرزمینی و استقلال سرزمینی باشد و دولتی بنابر نقض تعهدات طرف متعاهد خود، بخواهد وی را از منافع اینترنتی در معاهدهٔ فی مابین محروم سازد، طبق نظر انحصاری بودن می‌تواند تحریم را اجرایی کرد. اما در فرض دوم، اگر در اجرای تحریم خارج از اصول عمل نماید و بخواهد بطور خودسرانه و از موضع قدرت این اقدام را انجام دهد باید زیر نظارت شورای امنیت سازمان ملل باشد و آنجایی که پای منافع مشترک در میان است، باید دیدگاه اعمال قدرت نهادی فراتر از دولت‌ها مطرح گردد.

در مورد صلاحیت رسیدگی نیز در فرض اول، وقتی یک جرم اینترنتی در قلمرو یک یا چند سرزمین در حال وقوع است، از آنجایی که خارج از بعد زمانی و مکانی می‌باشد، به حدی که به جرم بین‌المللی موضوع مفاد قوانین بین‌المللی نرسد، طبق نظر انحصاری بودن حاکمیت دولت‌ها، محاکم هر کشوری می‌توانند بنابر حاکمیت سرزمینی و یا معاضدت بین‌المللی اقدام به رسیدگی نمایند. اما در فرض دوم، زمانی که این جرم و رفتار در حد نقض صلح و امنیت بین‌المللی و در قالب جنگ و تروریسم سایبری بین کشورها ارتکاب یابد، بهتر آن است که قدرتی فراتر از دولت‌ها وارد عمل شود و صلاحیت اصلی آن به دیوان بین‌المللی کیفری داده شود.

نتیجه

در مقررات و اسناد بین‌المللی و قوانین داخلی صریحاً به ضمانت اجرایی تحت عنوان ضمانت اجرای تحریم اینترنتی اشاره نشده است، اما با توجه به اینکه اینترنت از جمله ابزارهای ارتباطی است، می‌توان آن را داخل در مفهوم موسع تحریم وسایل ارتباطی که از جمله ضمانت اجراهای محدودکنندهٔ حقوق اجتماعی موضوع مادهٔ ۴۱ منشور است به شمار آورد. در این صورت چنین اقدامی در حیطهٔ اختیارات شورای امنیت قرار می‌گیرد، در حالی که در عمل ما با تحریم اینترنتی کشورها علیه یکدیگر مواجه هستیم که هیچ گونه توجیه قانونی

ندارد. اگرچه دولت‌ها در حوزهٔ اعمال اصول حقوقی نظیر اصل حاکمیت و استقلال سرزمینی در قالب نقض معاهدات می‌توانند یکدیگر را از تأمین منابع اینترنتی محروم سازند، اما این اقدام وقتی یکجانبه و در راستای اعمال قدرت باشد قابل پذیرش نخواهد بود و با هیچ یک از اصول حقوقی و عرف بین‌المللی قابل توجیه نمی‌باشد. در جایی که با وجود حکم قانونی، نسبت به مشروعیت اقدامات شورای امنیت و خارج شدن آن از حیطهٔ وظایفش شبهه و تردید وجود دارد، به طریق اولی در مواجهه با چنین رفتارهایی نمی‌توان بنا را بر مشروعیت آنها قرار داد. چنین اقداماتی در سطح کلان خود می‌تواند رفتاری علیه صلح و امنیت بین‌المللی باشد. با وجود آنکه در سطح بین‌الملل جهت حفظ حقوق بشر اقدام به تأسیس یک سازمان بین‌المللی با مالکیت دولت‌های مختلف جهانی جهت سرویس‌دهی و تأمین منابع اینترنتی شده است، اما باز هم این سازمان مانند سابق تحت سیطره و حق وتوی ایالات متحده و سایر قدرت‌های بزرگ قرار دارد. بنابراین، طبق بررسی انجام‌شده تحریم اینترنتی با وجود تأسیس نهاد مشروع آن در قوانین بین‌المللی، به شکل مشروع و قانونی اعمال نمی‌شود. لذا لازم است با اینگونه از اقدامات زمانی که به شکل یک جرم خلاف صلح و امنیت بین‌المللی ظاهر می‌شود، از سوی شورای امنیت برخورد جدی صورت گیرد و در سطح گستردهٔ آن نظیر جنگ و تروریسم سایبری توسط دیوان کیفری بین‌المللی به عنوان نهادی فراملی مورد تعقیب و رسیدگی قرار گیرد و اگر مغایر با حاکمیت یک دولت و اصل سرزمینی آن باشد، طبق اصل انحصاری بودن از طریق محاکم و مقامات ملی پیگیری شوند.

Abolfath Khaleghi http://orcid.org/0000-0002-0518-8204

Saghafi Parisa http://orcid.org/0000-0002-9259-6985

منابع

الف) فارسی

انصاری، باقر، (۱۳۹۹). «*حق دسترسی به اینترنت؛ مبانی و محتوا*»، *مجلهٔ حقوقی دادگستری*، دورهٔ ۸۴، شمارهٔ ۱۱۲، زمستان.

تنن بام، اندرو اس. (۲۰۰۳). *شبکه‌های کامپیوتری*، ترجمه: احسان ملکان و علیرضا زارع پور، موسسهٔ علمی فرهنگی (نص)، چاپ بیست و دوم پاییز ۱۳۹۱.

حکمتی، فاطمه، ضیایی، سیدیاسر (۱۳۹۶). *تحریم رسانه‌ای ایران از منظر حقوق بین‌الملل*، خرسندی، تهران.

خالقی، ابوالفتح (۱۳۹۹). *رژیم دادرسی جنایات بین‌المللی*، انتشارات مجد، تهران

دلخوش، علیرضا (۱۳۹۰). «جنبه‌های گوناگون مسئولیت در حقوق بین‌الملل کیفری»، *حقوقی بین‌المللی*، مرکز امور حقوقی بین‌المللی ریاست جمهوری، سال بیست و هشتم، شمارهٔ ۴۴ .

روحانی رانکوهی، سیدمحمدتقی و امیری یوسف (۱۳۹۲). *واژه‌نامهٔ مهندسی داده‌ها*، نشر جلوه، تهران.

زمانی، سیدقاسم، غریب‌آبادی، کاظم (۱۳۹۴). «واکاوی قانونی بودن و مشروعیت تحریم‌های یکجانبهٔ اقتصادی به موجب حقوق بین‌الملل»، *دیدگاه‌های حقوق قضایی*، شمارهٔ ۷۲.

سجادی، سیدکمال؛ حیدری، مهتاب (۱۴۰۰). «شیوه‌های حل‌وفصل اختلافات نام دامنه»، مطالعات حقوق، شمارهٔ ۲۳.

سلطانی‌فر، محمد (۱۳۹۱). «حقوق بین‌الملل، رسانه‌ها، صلح و امنیت بین‌المللی»، *دانشنامهٔ حقوق و سیاست*، شمارهٔ ۱۸.

ضیائی بیگدلی، محمدرضا (۱۳۸۵). *حقوق بین‌الملل عمومی*، چاپ بیست و چهارم، گنج دانش.

ضیایی، سیدیاسر، شکیب‌نژاد، احسان (۱۳۹۵). «قانونگذاری در فضای سایبر رویکرد حقوق بین‌الملل و حقوق ایران»، *حقوقی بین‌المللی*، شمارهٔ ۵۷.

عابدینی، عبدالله (۱۳۹۳). *حقوق بین‌الملل کیفری، نظریه و رویه*، شهر دانش، تهران.

عاملی، سعیدرضا، محسنی آهویی، ابراهیم (۱۳۹۷). *فقدان مشروعیت قانونی-بین‌المللی تحریم و نقض حقوق بشر*، موسسهٔ اسلامی حقوق بشر ۲۰۱۸، لندن.

فیوضی، رضا (۱۳۸۶). *حقوق بین‌المللی کیفری*، انتشارات دانشگاه تهران.

موسوی، محمدرضا و همکاران (۱۳۹۲). «تأثیرات تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن»، *مطالعات بین‌المللی پلیس*، شمارهٔ پیاپی ۱۴.

معین، محمد (۱۳۶۰). *فرهنگ فارسی*، ج ۱، چاپ چهارم، امیر کبیر، تهران.

هریسن داینیس، هیتر (۱۳۹۵). *جنگ سایبری و حقوق جنگ*، ترجمه: سعید حکیمی‌ها هومان شاهرخ، میزان، تهران.

ب) انگلیسی

Abedini, Abdullah (2014). *International criminal law, theory and practice*, Shahr Danesh, Tehran. (In Persian**(:**

Ameli, Saeedreza, Mohseni Ahoyi, Ibrahim (2017). *Lack of legal-international legitimacy of sanctions and human rights violations*, Islamic Human Rights Institute 2018, London. [in Persian]

Andrade, Norberto Nuno Gomes de .(2016). *New Technologies and Human Rights*: challenges to Regulation. Routledge.

Ansari, Baqir, (2019). "*The right to access the Internet*; Basics and Content", Judiciary Legal Journal, Volume 84, Number 112, Winter. [in Persian]

Castell, Wolfgang zu. Et Al. (2005). *Inzell Lectures on Orthogonal Polynomials. Nova Publishers*.

Casey, Rebecca E. (2008) ICANN or ICANN' t *Represent Internet User*. Faculty of the Virginia polytechnic Institute and State University.

Deibert, Ronald & etc (2008) *Access Denied*: The Practice and Policy of Global Internet Filtering. MIT Press.

Delkhosh, Alireza (1390). "*Different Aspects of Responsibility in International Criminal Law*", International Law, Center for International Legal Affairs of the Presidency, Year 28, Number 44. [in Persian]

Eeckhout Piet. (2011)*EU External Relations Law*. Oxford University Press.

Fayouzi, Reza (1386). *International Criminal Law*, Tehran University Publications. [in Persian]

Frosio, Giancarlo F. (2020) *Oxford Handbook of Online Intermediary Liability*. Oxford University Press.

Government Printing Office. (2011) *Country Reports on Human Rights Practices* for 2011.

Harrison Dinis, Heater (2015). *Cyber war and the laws of war*, translated by: Saeed Hakimiha - Homan Shahrokh, Mizan, Tehran. [in Persian]

Hekmati, Fatemeh, Ziyaei, Sidyaser (2016). *Iranian media boycott from the perspective of international law*, Khorsandi, Tehran. [in Persian]

Hlubik Schell, Bernadette. (2007). *The Internet and Society*: AReference Handbook. ABC-CLIO.

Inc.Ibp. (2015). *CUBA Information Strategy. Internet and E-Commerce Development Handbook*. International Business Publications. USA.

Khaleghi, Abolfath (2019). *International Crimes Procedural Regime, Majed Publications*, Tehran. [in Persian]

Kung, Lucy. Et Al. (2008). *The Internet and The Mass Media*, Sange.

Moin, Mohammad (1360). *Farhang Farsi*, Vol. 1, 4th edition, Amir Kabir, Tehran. [in Persian]

Mousavi, Mohammad Reza et al. (2012). "*Effects of security threats of cyber terrorism on the national security of the Islamic Republic of Iran and strategies to deal with it*", International Police Studies, serial number 14. [in Persian]

Müller, Joachim. (2006). *Reforming the United Nations [electronic resource]: the struggle for legitimacy and effectiveness*. Martinus Nijhoff Publishers.

Nakahira, Katsuko T. et al. (2006). *Geographic Locations of web servers*. Proceedings of 15th international conference on worldwide.

National Research Council, *Division on Engineering and Physical Sciences*. Committee on offensive Information Warfare. (2009). Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. National Academies Press.

Patricia Moloney Figliola. (2010). *U.S. Initiatives to Promote Global Internet Freedom*: Issues, Policy, and Technology. DIANE Publishing.

Rouhani Rankohi, Seyyed Mohammad Taghi and Amiri Yusuf (2012). *Glossary of Data Engineering*, Jaloh Publishing House, Tehran. [in Persian]

Sajjadi, Seyyed Kamal; Heydari, Mehtab (1400). "*Methods of resolving domain name disputes*", Law Studies, No. 23. [in Persian]

Schmitt, Michael N. .(2016).*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Schmitt, Michael N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University press.

Soltanifar, Mohammad (1391). "*International law, media, international peace and securit*y", Encyclopedia of Law and Politics, No. 18. [in Persian]

Tenenbaum, Andrew S. (2003). *Computer networks, translated* by: Ehsan Malekan and Alireza Zarepour, Scientific and Cultural Institute (text), 22nd edition of Fall 2011. [in Persian]

United States. Congress. Senate. *Committee on Commerce, Science and Transportation*. (2015). Internet Corporation for Assigned Names and Numbers (ICANN). U.S. Government Printing Office.

Yong Wang, Dawn Gu. Et al. (2012). *Stuxnet Vulnerabilities Analysis of SCADA Systems. International Conference on Network Computing and Information Security*. NCIS: Network Computing and Information Security pp 640–646.

Zamani, Seyyed Ghasem, Gharibabadi, Kazem (2014). "*Examination of the legality and legitimacy of unilateral economic sanctions according to international law*", Jurisprudence Perspectives, No. 72. [in Persian]

Ziai Begdali, Mohammad Reza (2015). *General International Law*, twenty-fourth edition, Ganj Danesh. [in Persian]

Ziyai, Sidyaser, Shakibnejad, Ehsan (2015). "*Legislation in the cyberspace approach of international law and Iranian law*", International Law, No. 57. [in Persian]

www.*researchgate*.net/publication/

www.*nytimes.com*/2011/01/16/world/middleeast) Israeli Test on worm called crucial in Iran nuclear delay, William J. Broad, John Markoff and David E. Sanger Jan. 15, 2011.

استناد به این مقاله: خالقی، ابوالفتح و ثقفی، پریسا. (۱۴۰۱). تحریم اینترنتی: کنش یا واکنش کیفری در سطح حقوق بین‌المللی. *فصلنامه پژوهش حقوق کیفری*. ۱۱ (۴۰)، ۱۰۵-۱۲۵. doi: 10.22054/jclr.2023.59356.2297