Journal iranian political sociology
Vol.٤,No٣,fall٢٠٢١

Compilation of treaties in cyberspace law: challenges and opportunities

Review:

The evolution and transformation in information technology has made societies undergo a fundamental change and transformation that will continue in the future, on the other hand, new technology has challenged legal concepts. Information and communication have flowed in the easiest way in the world and borders are no longer an obstacle to this flow, in addition to the fact that the development and evolution of the cyberspace has caused cybercrimes and that criminals can commit crimes without being present at the scene. be criminalized, the validity of the law in the stability of order and public security depends on the support of the governments, and the governments have drawn an indicator called territory (land - nationals) to avoid interfering in each other's affairs.

In the cyber world, the sovereign territory of the states as a baseline no longer has any function, and in such a situation, it seems that the position of international treaties has been elevated and they have taken on a more prominent role, in the sense that the drawing of the cyber territories of the countries is only after harmonizing the laws for They do not advance their goals and they also play the role of international consensus laws, the issue raised in this article is to examine the point that what are the influencing factors on the drafting of treaties in cyberspace rights? Therefore, due to the function of domestic law, which is unique to a certain territory, and the law that guarantees public order and security, it faces a great limitation of national sovereignty, and outside this territory, the solution to problems should be provided in international law.

فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال چهارم،شماره سوم(پیاپی۱۵)پاییز ۱٤۰۰،صص۲۸٦۳-۲۸٤۸

تدوین معاهدات در حقوق فضای سایبر: چالش‌ها و فرصت ها

سید وحید لاجوردی[۱]
محمد رضا حکاک زاده[۲]

تاریخ دریافت :۱٤۰۰/۰٦/۲۱
تاریخ پذیرش: ۱٤۰۰/۰۸/۰۱

چکیده

تحول و دگرگونی در فناوری اطلاعات، جوامع را دستخوش تغییر و تحول بنیادینی کرده است که در آینده نیز این روند ادامه خواهد یافت، از طرفی فناوری جدید مفاهیم قانونی را دچار چالش کرده است. اطلاعات و ارتباطات به آسان‌ترین شکل در جهان جریان پیدا کرده و دیگر مرزها مانعی بر سر راه این جریان به حساب نمی آیند، مضافا این که توسعه و تکامل فضای سایبر سبب ایجاد جرایم سایبری شده و این که جنایت کاران می‌توانند بدون حضور در صحنه جرم مرتکب جرم شوند، اعتبار قانون در پایداری نظم و امنیت عمومی به پشتیبانی حاکمیت‌ها بستگی دارد و حکومت‌ها نیز برای پرهیز از مداخله در امور یکدیگر، شاخصی به نام قلمرو (سرزمین – اتباع) را ترسیم کرده‌اند.

در دنیای سایبری قلمرو حاکمیتی دولت‌ها به عنوان یک خط مبنا دیگر کارکردی از آن باقی نمانده که در چنین شرایطی به نظر می‌رسد جایگاه معاهده‌های بین‌المللی ارتقاع یافته و نقش پررنگ‌تری را عهده‌دار شده‌اند، به این تعبیر که ترسیم قلمروهای سایبری کشورها تنها در پی هماهنگ‌سازی قوانین برای پیشبرد اهدافشان نیستند و نقش قوانین مورد اتفاق نظر بین‌المللی را هم ایفا می‌کنند، مساله‌ای که در این نوشتار مطرح می‌باشد، بررسی این نکته است که عوامل تاثیر گذار بر تدوین معاهدات در حقوق فضای سایبر کدامند؟ لذا با توجه به کارکرد حقوق داخلی که منحصر به قلمرو خاصی است و قانون که تضمین کننده نظم و امنیت عمومی است با محدودیت بزرگ حاکمیت ملی روبرو است که در بیرون این قلمرو راه حل مشکلات می‌بایست در حقوق بین الملل ارایه گردد.

واژگان کلیدی: فضای سایبر- تدوین معاهدات – فناوری اطلاعات – حقوق بین الملل

[۱]گروه حقوق، واحد قم، دانشگاه آزاد اسلامی، قم، ایران.
v.lajevardi۹٤@gmail.com
[۲]گروه حقوق، واحد قم، دانشگاه آزاد اسلامی، قم، ایران. (نویسنده مسئول)
Hakakreza@qom-iau.ac.ir

مقدمه

استفاده از فناوری‌های فضای سایبر با توجه به رویکردهای جدید در دنیای کنونی امری اجتناب ناپذیر است. با توجه به قواعد و ابزارهای فضای سایبر، کشوری که می‌خواهد وارد این عرصه شود، باید به همه چالش‌ها و ظرفیت‌ها توجه نموده و با تهدیدهای موجود در این فضا مبارزه نماید تا بتواند حداکثر بهره برداری را از این فضا داشته باشد، که بدون توجه به موارد پیش گفته، مقابله با چالش‌ها و تهدیدها در این عرصه امکان پذیر نیست. استفاده از فضای سایبر که دستاورد فناوری‌های نوین اطلاعات است، گر چه برای کشورهای در حال توسعه به عنوان یک فرصت به منظور جبران عقب ماندگی‌های فناورانه نسبت به جوامع پیشرفته است، اما همین فناوری اگر به صورت درست و صحیح مورد بهره برداری قرار نگیرد و چالش‌های آن مورد توجه واقع نشود، خود می‌تواند تهدیدی مهم تلقی شود.

امروزه به دلیل ویژگی‌های خاص این فضا، اقدامات و حملات تروریستی فراوانی در فضای سایبر متوجه دولت هاست که از این ویژگی‌ها می‌توان به ناشناخته بودن و گمنامی و سرعت حملات، اشاره نمود که معمولا این گونه حملات پس از وقوع مورد شناسایی قرار می‌گیرند. ضمنا باید یادآور شد که جنگ سایبری دیگر داستانی علمی تخیلی نیست و بحث در میان سیاست مداران درباره این که چه هنجارهایی باید تعیین کننده نوع رفتار در فضای سایبر باشد، به شدت محل اختلاف است. می‌توان گفت که سازمان ملل یکی از عالی‌ترین مراجعی است که این چالش‌ها در آن جا پیگیری می‌شود. با تامل بر فعالیت سازمان ملل در طول دو دهه گذشته، پیشرفت قابل توجهی از ظهور هنجارهای سایبری را می‌توان مشاهده کرد.

همان گونه که علاقمندان به این عرصه مستحضرند، در حال حاضر کنوانسیون بین‌المللی در حوزه سایبر وجود ندارد تا محقق به بررسی چالش ها، فرصت‌ها و فراز و فرودهای حقوقی آن همت گمارد. اما هنجارها و روال حاکم بر این عرصه، نشان از عزم دولت‌ها در زمینه نظام مند کردن فعالیت در قلمرو سایبر است که در این راستا می‌توان به فعالیت‌های سازمان ملل اشاره کرد.

فرصت ها

ایجاد مفاهیم

ظهور فضای سایبر موجب شکل گیری دنیایی درون دنیای عینی شده، دنیایی که جایگاهی برای بهره وری بعضی از اشخاص (حقیقی – حقوقی) – دولت‌ها و بازیگران غیر دولتی شده که با استفاده از ویژگی‌های این فضای جدید در پی دستیابی به اهداف خود، اهدافی که می‌تواند به صورت غیر قانونی، آن‌ها را از طریق فضای سایبر به خواسته هایشان برساند، هستند گرچه دولت مردان سعی می‌کنند با توسعه دامنه قوانین موجود و تفسیر موسع این قوانین که مبتنی بر ویژگی‌های دنیای عینی تدوین شده اند، دنیای سایبر را همچون دنیای عینی، نظام مند و مبتنی بر قانون کنند، اما ویژگی‌های این فضا و تفاوت آن با دنیای عینی در برخی مفاهیم، تا کنون مانع تحقق این هدف شده است.

از جمله این بهره‌وری‌ها که از طریق فضای سایبر تحقق پیدا کرده و آثار جبران ناپذیری در بعد عینی و نیز در بعد سایبری به جای گذاشته است و می‌توان آن را با حملات مسلحانه مقایسه نمود، حملات سایبری می‌باشد.

اما بر خلاف فضای عینی که حقوق توسل به زور و حقوق بشر دوستانه برای آن تدوین یافته و مورد قبول نیز واقع شده است در حال حاضر، قواعدی در حقوق بین الملل مربوط به حملات سایبری که مورد استقبال دولت‌ها بوده و مورد اتفاق نظر

دولت‌ها قرار گرفته و نیز الزام آور باشد، وجود ندارد. البته می‌توان یاد آور شد که در خصوص تدوین حقوق بین الملل حاکم بر حملات سایبری، ناتو در سال‌های ۲۰۱۳ و ۲۰۱۷ در قالب دو نسخه (راهنمای تالین برای حقوق بین الملل قابل اعمال در نبردهای سایبری)[۱] راهنمایی تدوین نموده و با آن که این دو نسخه همان طور که از نامشان پیداست، بیش از راهنما نیستند ولی به هر روی گامی به جلو محسوب شده و می‌تواند مقدمه‌ای برای تدوین قوانین و مقررات لازم الاجرا در این حوزه باشد، که رسیدن به چنین مرحله‌ای، تحلیل و بررسی جنبه‌های حملات سایبری و شناسایی خلاهای موجود در این حوزه می‌باشد که راه حل این مشکلات می‌بایست در حقوق بین الملل ارایه شود.

بی شک مهمترین مانع در مقابل حقوق بین الملل، چالش‌های مرتبط با مفاهیم ناملموس در فضای سایبر در رابطه با زمان و مکان حملات سایبری است. بنابراین برای بررسی این موانع باید نقش معیارهای زمان و مکان در حملات سایبری مورد توجه قرار گیرد.

۱. معیارهای مکان

فضای سایبر بستری برای تحقق حملات سایبری است. به علت ماهیت ناملموس فضای سایبر، در رابطه با مفاهیم مطرح در این محیط، علیرغم اختلاف نظرهای فراوان، ادبیات موجود کم رنگ است که لازم است تعریف حملات سایبری و فضای سایبر و تفکیک تعاریف میان این فضا و فضای عینی و نیز بیان تفاوت‌ها و تشابهات میان این دو فضا به جهت راهکارهای حقوقی بر این فضا بیان گردد.

۱- ۱. مفهوم فضای سایبر

مرز رکن جدایی ناپذیر و تعیین کننده قلمرو کشور است که با طرح حملات سایبری باید حدود این مرز و همچنین قلمرو مجازی دولت‌ها در فضای سایبر مشخص شود، چالش مهم در رابطه با حملات سایبری تعریف فضای سایبر در حقوق بین الملل است. زیرا حمله در فضای عینی زمانی معنا می‌یابد که مرزهای یک دولت مورد حمله نظامی دولتی دیگر قرار گیرد[۲]. در واقع تعریف فضای سایبر و تشخیص چارچوب‌های این فضا مطابق با معیارهای حقوق بین الملل، می‌تواند اولین اقدام در مسیر تدوین حقوق بین الملل حاکم بر حملات سایبری باشد.

چهار شرط (جمعیت دایمی – قلمرو مشخص – حکومت – اهلیت برقراری ارتباط با دولت‌ها) کنوانسیون حقوق و تکالیف دولت‌ها (مونته ویدیو) به عنوان شرایط دولت برشمرده است. ۳ مرز در دنیای عینی خطی است که قلمرو سرزمینی یا فضای دریایی بین دو کشور را ترسیم می‌کند. ٤ از طرفی مرز از منظر حقوق بین الملل (باید به آساتی قابل شناسایی و به سختی قابل عبور) باشد. ٥ اما در فضای سایبر مرز مفهومی ندارد. فضای سایبر " فضای جهانی در محیط اطلاعاتی متشکل از

---

۱. Tallinn Manual on the International Law Applicable Cyber Warber Defence Ceter Excellence, Cambridge University Press ,۲۰۱۳; Tallinn Manual ۲. ۰ on the International Law Applicable to Cyber opperations, Prepred by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence Cambridge University Press, ۲۰۱۷

۲. How is the Term "Armed Conflict" Defined in International Humanitarian Law? International Committee of the Red Cross (ICRC) Opinion Paper, March ۲۰۰۸. pp. ۱-۳.

۳. Convention on Rihgts and Duties of States (Montevideo Convention)۱۹۳۳, art. ۱.

٤. Martin Pratt, Book Let of Applied Issues in International Land Boundary Delimitation / Demarcation Practices, (A Seminar Organized by the OSCE Borders Team in co-operation With the Lithuanian OSCD Chairmanship,۳۱ May to ۱ June ۲۰۱۱ Vilnius, Lithuania) ۲۰۱۱, p. ۸.

٥. Brittish Guiana Boundary Case (۱۸۹۹) ۱۸۸ C. t. s. ٦٧; AlaskaBoundary Arbitration (۱۹۰۳) ۱٥ R. I. A. A. ٤٨۱ cited in; John P. Grant and J. Gaig Barker. Parry &Grant Encyclopedic Dictionary of International Law, Third Edition, Oxford University Press,۲۰۰۹. P. ٦٩.

شبکه وابسته زیر ساخت‌های فناوری اطلاعات از جمله اینترنت، شبکه‌های ارتباطی راه دور –سامانه‌های رایانه‌ای پردازنده و کنترل تعبیه شده برای آن ها"۱ تعریف شده است که ویژگی مهم فضای سایبر، وابستگی زیر ساخت‌ها در فضای یکپارچه و جهانی (بدون مرز) است که از خصوصیات دهکده جهانی۲ و نقطه مقابل فضای عینی است. بنابراین مرز در فضای عینی ملموس و در فضای سایبر غیر ملموس است.

۱- ۲. مفهوم حملات سایبری

در خصوص ارایه تعریف "حملات سایبری"، مشکل اصلی پیش روی حقوق بین الملل، نبود اجماع در این مورد و عدم وجود چارچوب مشخصی برای آن است. یکی از مشکلات این است که هر دولتی با لحاظ توانایی‌ها و منافع و تهدیدهای پیش رو، حملات سایبری را تعریف می‌کند. معمولا دولت هایی که زیر ساخت هایشان در این حوزه به فضای سایبر وابسته‌تر بوده و ممکن است بیشتر در معرض این حملات قرار گیرند۳ ، تمایل بیشتری دارند که هر گونه حمله سایبری را توسل به زور تلقی کرده و در چارچوب بند ٤ ماده ۲ منشور ملل متحد به حساب آورند تا به دفاع مشروع متوسل شوند٤. در مقابل دولت‌های کمتر وابسته به فضای سایبر، تمایل دارند که حدود حملات سایبری را محدود کنند. واضح است که هر چه فناوری یک کشور پیشرفته‌تر باشد، نسبت به حملات سایبری آسیب پذیرتر است. ایالات متحده مثال بارزی از یک کشور آسیب پذیر در مقابل حملات سایبری به جهت وابستگی اقتصادی و نظامی به فناوری شبکه‌های اطلاعاتی می‌باشد.۵ همین حساسیت موجب شده است که اندیشمندان آمریکایی حملات سایبری را از نگاه حقوق بین الملل مورد بررسی قرار داده تا از این طریق اقدامات نظامی آمریکا به حملات فوق را قانونی جلوه دهند.٦ بنا بر مطالب پیش گفته می‌توان بیان نمود که تعاریف مطروحه بی طرفانه نبوده و اتفاق نظری که توازن میان منافع دولت‌ها و آثار حقوقی را تحصیل کند، حاصل نشده است.

از سوی سیاست مداران و نظامیان، عبارات مختلفی چون جنگ سایبری۷ و حملات سایبری۸ در فضای سایبر به کار می‌رود که معمولا خارج از مفهوم اخص قرار می‌گیرند.۹ به طوری که در راهنمای تالین ۲۰۱۳ اقداماتی از قبیل عملیات سایبری روانی و جاسوسی سایبری در مفهوم نظامی به عنوان حمله شناخته نشده است.۱۰

---

۱. Department of Defens Dictionary of military and Associated Terms (Joint Publication ۱-۰۲). ۸. November ۲۰۱۰(As Amended through ۱۵ December,۲۰۱۰. P. ۷٤.)

۲. Marcel Danesi Dictionary of Media and Communications, M, E Sharpe,۲۰۰۹. P. ۱۳۵.

۳. آهنی، آمینه، محمد و فاطمه زهرا، فتح الهی، "حقوق بین الملل مدرن در مواجهه با جنگی پست مدرن(نبرد سایبری)"، راهبرد، سال بیست و سوم، شماره ۷۲، پاییز ۱۳۹۳، ص ۱۳۰.

۴. کیهانلو، فاطمه، وحید، رضادوست، "حملات سایبر به مثابه توسل به زور در سیاق منشور سازمان ملل متحد"، فصل نامه تحقیقات حقوقی شماره ۶۹، ۱۳۹۴، ص ۲۰۴.

۵. Matthew C. Waxman. Cyber Attacks as Forse Under UN Charter Article ۲ (٤), International Law Studies, Vol۸۷،۲۰۱۱. p. ٤٥.

٦. Marco Roscini, op. cit. p. ۹۰.

۷. Cyber war-Cyber warfare.

۸. Cyber attak.

۹. Launie K. Blank,International Law Cyber from Non-State Actors,International Law Studies (U. S. Naval war College),Vol. ۸۹،۲۰۱۳. p. ٤۳٥.

۱۰. Tallinn, ۲۰۱۳, Ibid, Rule ۳۰, Second Commentary.

فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال چهارم، شماره سوم (پیاپی ۱۵)، پاییز ۱۴۰۰

از بهترین تعاریفی که با حقوق بین الملل بشردوستانه سازگاری دارد، تعریف ارایه شده از حملات سایبری در راهنمای تالین است که عبارت از: " عملیات در محیط سایبری، خواه تهاجمی یا دفاعی که معقولانه این انتظار از آن می‌رود که منتهی به جرح یا مرگ افراد یا ورود خسارت به اشیا یا تخریب آن‌ها شود "[۱].

از جمله ویژگی‌های حملات سایبری، می‌توان به کم هزینه بودن –خدشه وارد کردن به مرزهای سنتی – گسترش فریب و مدیریت افکار عمومی – چالش جدید راهبرد اطلاعات – دشواری مشکلات هشدار دهنده تاکتیکی و ارزیابی حمله – دشواری ایجاد و نگهداری اعتلاف – آسیب پذیری کشورهای توسعه یافته و آسیب رسانی غیر قطعی و نا معلوم اشاره نمود که درباره گسترش فناوری و ایجاد عملیات سایبری و حقوق بین الملل که در طول زمان از طریق منابع خود توسعه و تدوین یافته است، نکته‌ای که باید مورد توجه قرار گیرد کارآیی این قوانین در بستر جدید فضای سایبر می‌باشد.

حقوق بین الملل حاکم بر فضای سایبر و حملات سایبری کماکان با ضعف ادبیات حقوق بین الملل در قبال مفاهیم تکنیکی حملات سایبری مواجه است، بدیهی است که این ضعف‌ها باید رفع شود تا دیگر مسایل مرتبط با فضای سایبر نیز مرتفع گردد.

۲. معیارهای زمان

تطبیق فضای سایبر با فضای عینی به جهت وجود مسایل فنی، امری پیچیده است که می‌توان در این خصوص دو هنجار (تقابل حملات سایبری با حملات عینی) و (شناسایی منشا حمله در حملات سایبری و تقابل آن با فوریت) را در حقوق بین الملل مورد بررسی قرار داد.

۲- ۱. تقابل حملات سایبری با حملات عینی

پیدایش فضای سایبر و توسعه آن، چالش مهمی را در رابطه با حملات سایبری و حملات عینی در حقوق بین الملل ایجاد کرده است.

توسل به دفاع مشروع مندرج در ماده ۵۱ منشور ملل متحد، بارزترین نوع واکنش به حملات عینی است. از طرفی بهترین پاسخ به حملات سایبری، اقدام متقابل سایبری است که باید در چارچوب منشور ملل متحد و حقوق توسل به زور صورت گیرد. حال در فرض اخیر آیا می‌توان در مقابل حملات عینی به دفاع سایبری متوصل شد؟ برای پاسخ به این پرسش می‌بایست شرایط تحقق دفاع مشروع را در برخورد با حمله سایبری تحلیل کرد که این شرایط به شرایط عرفی و شرایط معاهده‌ای (مدون) تقسیم می‌شوند. در حقوق بین الملل عرفی، رعایت شروط ضرورت - تناسب - فوریت برای تحقق فعل ضروری است[۲]. از منظر منشور ملل متحد، شرایط توسل به دفاع مشروع شامل وقوع حمله مسلحانه - وجود تهدید فوری - رعایت تناسب و گزارش به شورای امنیت می‌باشد. که در صورت وجود شرایط مذکور، کشوری که مورد حمله مسلحانه واقع شده می‌تواند به دفاع مشروع توسل جوید. بنابراین اگر دفاع سایبری با شرایط دفاع مشروع منطبق باشد، می‌توان بیان نمود که منعی برای مفروض انگاشتن این اقدامات در قالب دفاع مشروع در مقابل حملات مسلحانه عینی وجود ندارد.

طبیعتا این رویکرد دیوان بین‌المللی دادگستری مورد استقبال کشورهایی از جمله ایالات متحده است که سلاح‌های هسته‌ای دارند. ن. ک.

---

۱. Tallinn Manual on the International Law Applicable to Cyber Warfare, prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Center of Excellence, Cambridge University Press, ۲۰۱۳, Rule ۳۰.

۲. Nicaragua v. United states. ۱۹۸٦, p,۹٤. para. ۱۷٦.

Robert F. Turner, "Nuclear Weapons and the World Court: The ICJ's Advisory Opinion and Its Significance for U. S. Strategic Doctrine", International *Law Studies*, in: *The Law of Military Operations*: *Liber Amicorum, Professor Jack Grunawalt*, Michael N., Schmitt (ed.), ۱۹۹۸.

۲- ۲. شناسایی

یکی از ویژگی‌های جنگ‌های سایبری، گمنامی است که شناسایی منبع حملات سایبری به دلیل مقابله اهمیت بالایی دارد. در این مورد باید توجه داشت که اقدام از رایانه در یک کشور، دلیل آن که حمله از همان کشور صورت گرفته، نیست[۱]. که ممکن است حمله از کشورهای دیگر عبور کرده و قابل رد یابی باشد[۲]. به طوری که ادعا شده مسیر حمله سایبری ۲۰۰۷ به کشور استونی از کشورهای (ایالات متحده – مصر – پرو – روسیه) عبور کرده است[۳]. بنابراین نباید چنین پنداشت که کشور محل سخت افزار رایانه‌ای، به طور حتم آغاز گر حمله بوده است که می‌بایست پیش از توسل به هر اقدامی، کشور قربانی از منشا حمله اطمینان یابد[٤]. امروزه با پیشرفت فناوری و همراه شدن حملات سایبری با حملات عینی امکان شناسایی منبع حمله در بیشتر موارد امکان پذیر است[٥].

حقوق نرم

هدف تنظیم کنندگان حقوق نرم (قوام نیافته) که شاکله اصلی اسناد بین‌المللی می‌باشد، ایجاد یک معاهده لازم الاجرا نیست بلکه هدف آن‌ها رشد هنجارهای توصیه آمیزی است که قابلیت توسعه حقوقی در سطح جهانی را دارا باشد[٦] علت ایجاد چنین اسنادی به عنوان حقوق نرم و غیر لازم الاجرا، این است که به دلیل عدم توسعه فاقد اجماع میان دولت‌ها هستند[۷]. دلیل دیگری که به ایجاد حقوق نرم می‌انجامد، مشکلات پیش رو در شکل گیری حقوق سخت (هزینه بر و زمان بر بودن) است. از طرفی حقوق نرم سهل الوصول‌تر از حقوق سخت است به ویژه در جایی که عاملان، دولت‌ها بوده و نسبت به تحدید اقتدار خود حساس باشند. که در این صورت حقوق نرم بهترین راهکار برای جلب رضایت کشورهای مختلف با منافع متضاد خواهد بود[۸].

اکثر اسناد بین‌المللی مرتبط با فضای سایبر، تشکیل دهنده حقوق نرم و غیر الزام آورند. قطعنامه‌های مجمع عمومی سازمان ملل، قطعنامه‌های اتحادیه بین‌المللی مخابرات، اعلامیه‌های سازمان‌های منطقه‌ای و اجلاس جهانی جامعه اطلاعاتی از این زمره اند. که در میان آن‌ها اسناد اجلاس جهانی جامعه اطلاعاتی به جهت آن که نتیجه مذاکرات طولانی و توافق کشورها در پذیرش آن می‌باشند، قابلیت توسعه هنجارهای خاصی از حقوق نرم را دارند.

به طور کلی دولت‌ها تمایلی به پذیرش تعهدات حقوقی بین‌المللی جز بر اساس اراده و توافق نداشته اند که آثار این رویکرد با باقی ماندن اهمیت و جایگاه معاهدات در حقوق بین الملل قابل رویت است. اما اتفاقاتی فارغ از خواست دولت‌ها مانند تغییرات اقلیمی در جهان رخ می‌دهد که با فعالیت سازمان‌های بین‌المللی در این حوزه ها، اراده دولت را تحت تاثیر قرار

---

۱. Marco Roscini, op. cip. p. ۹٦.
۲. Laurie K Blank, op. cit. pp. ٤۱٦-٤۱۷.
۳. Marco Roscini, op. cip. ۹٦-۹۷.
٤. Laurie K Blank, op,cip. pp. ٤۱٦-٤۱۷.
٥. Marco Roscini, op. cip. p. ۹۷.
٦. این اسناد غیر معاهداتی عموما به عنوان راهنما ها، اصول، اعلامیه ها، آیین نامه ها، توصیه نامه‌ها یا برنامه‌ها خوانده می‌شوند.
۷. Anthony Aust, op cit. p. ۷۷.
۸. Kennth W. Abbott, Duncan Snidal, Hard and Soft Law in International Governance,The IO Foundation and the Massachusetts Institute of Technology , Vol,٥٤,Issue۳،۲۰۰۰,p. ٤۲۳.

می‌دهند. بر همین اساس دولت‌ها علاوه بر الزام هایی که معاهدات برایشان ایجاد می‌کند، ناگذیرند تا ابزاری انعطاف پذیر برای واکنش حقوقی در مقابل اتفاقات نامعین و غیر قابل پیش بینی ایجاد کنند. حقوق نرم قالب حقوقی مناسبی برای توسعه مفاهیم در حال شکل گیری حقوق بین الملل[۱] است و دولت‌ها در آن، به آثار محتمل این تعهدات و برآورد کلی آن، نسبت به منافع خود می‌پردازند که در پی آن، فرآیند شکل گیری قواعد در تنظیم روابط حقوقی به تدریج از انحصار دولت‌ها خارج شده و تابعان جدید، در شکل سازمان‌ها و موسسات منطقه‌ای و بین‌المللی ظهور پیدا می‌کنند.

تا کنون تعریف مشترکی از حقوق نرم[۲] ارایه نشده و توافق قابل استنادی در مورد مفهوم آن، در این حوزه ارایه نگردیده است.

مراد از قاعده نرم آن است که در مرحله‌ای از شکل گیری قواعد حقوقی قرار دارد[۳] و نیز اسناد حقوقی نرم هنوز اعتبار قاعده حقوقی به معنای خاص را پیدا نکرده است، ولی می‌توان گفت که از ارزش حقوقی بیش از متون فاقد ارزش برخوردارند[٤]. و نیز حقوق نرم خلا مابین حقوق لازم الاجرا و عدم وجود نظم حقوقی را پوشش می‌دهد، که به همین جهت تفکیک آن برای مفسران دشوار است[٥].

بنا بر این مطالب حقوق نرم عبارت از، مقررات حقوقی که فاقد قدرت الزام آوری بوده و از طریق پذیرش اختیاری[٦] به عرصه حقوق وارد شده[۷] و غالبا ماهیتی ارشادی و توصیه‌ای دارند[۸] اما مفاد این اسناد می‌توانند زمینه ساز ایجاد قواعد لازم الاجرا قرار گرفته و در قانونگذاری ملی یا معاهدات بین‌المللی مورد استفاده قرار گیرند. همچنین این حقوق به لحاظ تراضی طرفین قرارداد می‌توانند بر روابط قراردادی حاکم و یا توسط مراجع قضایی و داوری مورد تمسک قرار گیرند. اعلامیه جهانی حقوق بشر مثال بارزی در این زمینه است که یکی از مهمترین اسناد غیر الزامی بوده و در زمره حقوق نرم قرار می‌گیرند. اما خود اعلامیه، الهام بخش ایجاد و تصویب ده‌ها سند الزام آور حقوق بین الملل و حقوق داخلی کشورها بویژه درباره پاسداری از کرامت انسانی بوده است. اسناد کنفرانس ۱۹۷۲، ۱۹۹۲ استکهلم[۹] و ریو[۱۰]، اصول دفاع از محیط زیست در برابر زیاده خواهی‌های بشر مصرف گرا را تبیین کرده و دکترین توسعه پایدار را بنا نهاده است که این اسناد با این که جزو حقوق نرم هستند، اما زمینه ساز کنوانسیون‌های مرتبط این حوزه و قرارداد جهانی درباره صیانت از طبیعت شده اند.

چنین به نظر می‌رسد که با توجه به روند جهانی شدن، همکاری و مشارکت بیشتر در عرصه روابط بین الملل بیش از توسعه ابزار سنتی قدرت اعتبار جهانی قدرت‌ها را به همراه می‌آورد و توسعه حقوق بین الملل نیز بر مبنای چارچوب سازی

---

۱. حقوق بین الملل سایبری، یکی از این مفاهیم نوظهور در عرصه روابط بین الملل است که مراحل اولیه شکل گیری خود را طی می‌کند.

۲. Soft Law

۳. ایدا، ریوشی، "شکل گیری قواعد بین‌المللی در دنیایی رو به تحول – نقد مفهوم حقوق قوام نیافته "، ترجمه اردشیر امیر ارجمند، مجله تحقیقات حقوقی، ۱۳۷٦، شماره ۱۹-۲۰، ص۵۵۲

٤. همان ص ٥٥٦

٥. Guzman, Andrew T. andmeyer Timothy L.., "International Soft Law", Journal of Legal Analysis, Spring ۲۰۱۰. Vol ۲, No. ۱, http;/papers. ssrn. com/so۱۳/papers,cfm?id =۱۳٥۳٤٤٤,accessed ۲٥ March ۲۰۱۲. pp,۱۷٤-۱۷٥.

٦. Voluntary Acceptance

۷. Binding by Agreement

۸. Persuasive Nature

۹. Stockholm Declaration,۱۹۷۲, UN

۱۰. Rio Declaration ,۱۹۹۲

برای توسعه همکاری صورت می‌گیرد و نه بر اساس تلاش برای مکلف سازی دولت به منظور پذیرش اسناد جدید الزام آور، از طرفی حقوق نرم برنامه مدار است و به جای الزام‌های سخت به ارایه دستورالعمل‌های راهگشا برای خروج از مشکلات جهانی گرایش دارد.

در تقابل دیدگاه سنتی مبتنی بر لزوم مداخله دولت در شکل دهی و ایجاد قواعد حقوقی، رویکردهای مبتنی بر جامعه شناسی حقوقی در دهه‌های اخیر مفاهیم و نظریاتی را مطرح نموده که مبنای آن عدم لزوم استفاده از ضمانت اجرای قانونی و دخالت دولت به شکل رسمی در عرصه حقوق است که حقوق نرم از مفاهیم شکل گرفته بر اساس دیدگاه اخیر است، بنابراین رابطه میان حقوق نرم و حقوق سخت بیشتر از جنس تعامل است، نه تقابل. حقوق نرم در مرور زمان و به واسطه شناسایی و مقبولیت روز افزون تکامل یافته و در عمل به شکل حقوق سخت در می‌آیند و دولت‌ها نیز که در بدو امر نمی توانند زیر بار حقوق سخت بروند به حقوق نرم روی می‌آورند زیرا حداقلی از الزام با وجود حقوق نرم، بهتر از بی قاعدگی در روابط بین الملل است.

باید یاد آور شد که در بخش حقوق بین الملل سایبر در سازمان ملل آنچه وجود دارد حقوق نرم است که به سمت حقوق سخت در حرکتند. بخش‌های مختلف حقوق سایبر در سه کمیته اول – دوم – سوم مجمع عمومی بررسی شده و برای تصویب به مجمع ارسال می‌گردند. لذا قطعنامه هایی که تاکنون از طرف مجمع عمومی در خصوص موضوعاتی مثل جرایم سایبری، امنیت سایبری، فرهنگ سایبری و حقوق بشر سایبری و.. . صادر شده اند، همه در زمره حقوق نرم قرار می‌گیرند. شورای امنیت تاکنون هیچ قطعنامه‌ای در ارتباط با فضای سایبر[۱] صادر نکرده است. بنابراین در محدوده ارکان و سازمان‌های تخصصی سازمان ملل، حقوق سخت در این فضا شکل نگرفته است. اسنادی هم که توسط اکوسوک[۲]، شواری حقوق بشر سازمان ملل و اتحادیه بین‌المللی مخابرات در حوزه سایبر صادر کرده اند، هم در حکم حقوق نرم می‌باشند.

مسلما حقوق نرم دارای ویژگی هایی در زمینه موضوعات مرتبط با فضای سایبر است:

۱. به جهت عدم رسمیت و غیر الزام آور بودن نیازمند تعهد رسمی دولت نیست، بنابراین مشارکت بیشتر دولت‌ها را به همراه دارد.

۲. پایش رویکردهای جدید را تسهیل و خود را با توسعه سریع در عرصه فضای سایبر تطبیق می‌دهد.

۳. فرصت بیشتری برای ایجاد یک رویکرد چند وجهی نسبت به یک رویکرد بین‌المللی که محدود به دولت‌ها و سازمان‌های بین‌المللی است فراهم می‌کند و در نتیجه علاوه بر دولت ها، مشارکت فعال و مستمر سازمان ها، نهادهای دیگر و بخش خصوصی را تضمین می‌کند[۳].

حقوق نرم با لحاظ تمامی موارد پیش گفته در عین ویژگی‌ها و مزایایی که دارا هستند، فاقد قواعد الزام آور بوده و مادامی که این حقوق و قواعد مربوط به آن غیر الزامی باشند، تسری قواعد مندرج در آن‌ها به دادگاه‌های ملی غیر ممکن می‌باشد[٤] که به این موضوع، اختلاف کشورهای توسعه‌یافته و در حال توسعه را که در قطع نامه‌های مجمع عمومی نمایان است باید افزود که این اختلافات راه را برای رسیدن به اجماع بین‌المللی در شکل گیری حقوق نرم دشوار می‌سازد.

---

۱. Syber Spase
۲. ECOSOC (United Nation Economic and Social Council)
۳. William J. Drake. op cit. p. ۱۱٤
٤. آیگناتس زایدل هومن فلدرن، حقوق بین الملل اقتصادی (ترجمه قاسم زمانی) تهران، شهر دانش، ۱۳۸۵، ص ۸۵

فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال چهارم، شماره سوم (پیاپی ۱۵)، پاییز ۱۴۰۰

سازمان ملل به عنوان مهمترین نهاد جهانی، می‌تواند نقش موثری را در تنظیم چارچوب حقوقی فضای سایبر ایجاد کند که در موضوع فوق این سوال مطرح است که سازمان ملل چگونه می‌تواند مبانی لازم را برای قاعده سازی فضای سایبر فراهم کند که طرح این سوالات نشانگر تلاش دولت‌ها و سازمان‌های بین‌المللی برای یافتن راه حلی در این حوزه است.

اسناد بین‌المللی

برخی اسناد حقوق بین الملل مربوط به موضوعات فضای سایبر می‌باشند. مقررات ارتباطی تنظیم شده از سازمان اتحادیه بین‌المللی مخابرات، قطعنامه‌های سازمان ملل، مقررات حقوق بشری و مقررات تجارت بین الملل و.. . از این دسته اند. با این حال نباید به اسناد بین‌المللی بسنده کرد. منابع دیگری از حقوق بین الملل هستند که در رابطه با فضای سایبر مورد اشاره قرار می‌گیرند. عرف و حقوق نرم در کنار دیگر منابع حقوق بین الملل هستند که در همه زمینه‌ها از جمله فضای سایبر، نظام دهنده و انتظام بخش مسایل چالش برانگیز در این حوزه هستند. البته باید یاد آور شد که با توجه به سرعت تغییر پذیری این فضا، حقوق بین الملل عرفی چندان قادر به همراهی با این فضای در حال گسترش نخواهد بود[۱].

از آنجا که معاهده جامعی در سطح بین الملل در حوزه فضای سایبر منعقد نشده است و علت این امر، اختلاف نظر میان کشورها در موضوعات مختلف فضای سایبر از مسایل زیر بنایی تا مسایل خرد می‌باشد، ولیکن در سطح منطقه‌ای مهمترین معاهده‌ای که در این باره به تصویب رسیده است و از آن به عنوان الگویی برای قانون گذاری در فضای سایبر یاد می‌شود، کنوانسیون جرایم سایبر اتحادیه اروپاست.

علاوه بر کنوانسیون جرایم سایبر، دیگر سازمان‌های منطقه‌ای نیز مقرراتی در این حوزه وضع نموده اند. همچنین مقررات اتحادیه بین‌المللی مخابرات و سلسله مباحث اجلاس جهانی جامعه اطلاعاتی تشکیل دهنده توافقاتی در عرصه منطقه‌ای بوده اند، با این حال ذکر این نکته لازم است که نقطه ضعف مشترک این مقررات، پراکندگی و عدم جامعیت آنهاست.

قطعنامه‌ها و اعلامیه‌های بین‌المللی نقش موثری در فراهم سازی همگرایی بین‌المللی کشورها به سوی انتظام بخشی فضای سایبر داشته اند که علاوه بر این خاصیت، می‌توان گفت که قطعنامه‌های بین‌المللی درایجاد هماهنگی و همسان سازی سیاست‌های مختلف کشورها در عرصه بین‌المللی بسیار موثر بوده اند. با این توصیف عموم قطعنامه‌ها و اعلامیه‌های بین‌المللی در رابطه با فضای سایبر فاقد قدرت الزامی بوده و جنبه توصیه‌ای دارند که نیاز جامعه جهانی به تدوین معاهده‌ای بین‌المللی در این عرصه مورد توجه این نوشتار می‌باشد.

چالش

حاکمیت بر فضای سایبر

در این مبحث برخی به جای حاکمیت از عبارت "راهبری" استفاده می‌کنند. برخی حاکمیت را به معنای "مدیریت"[۲] و عده‌ای آن را به معنای "هماهنگی"[۳] می‌دانند.

موضوع مشارکت در حاکمیت در فضای سایبر و به طور اخص اینترنت، اولین بار در اجلاس ژنو در سال ۲۰۰۳ به طور جدی مطرح شد و در اجلاس تونس در سال ۲۰۰۵ نیز تعریفی از حاکمیت بر اینترنت به عمل آمد. اما در حال حاضر نیز که

---

۱. Noel Cox, op cit. p. ۷
۲. Management
۳. Coordinate

بیش از ده سال از آن تاریخ می‌گذرد، یک تعریف جهان شمول که مورد وفاق همه باشد، در مورد حاکمیت بر اینترنت وجود ندارد.

با مرور زمان که اینترنت به بخش‌های دیگر سرایت کرد، ایالات متحده کماکان به عنوان سرمایه گذار اولیه و اصلی مطرح بوده و قراردادهایی را با طراحان شبکه منعقد نموده، بنابراین در تمام این سال ها، حاکمیت ایالات متحده بر فضای سایبر، تحت عنوان "نظارت و کنترل بر عملکرد اینترنت " وجود داشته است. در اواخر ۱۹۹۰ زمانی که اینترنت به دنیای تجارت راه یافته بود، آیکان تاسیس شد و رهبری اینترنت را بر عهده گرفت. همزمان با تاسیس آیکان در سال ۱۹۹۸، اتحادیه بین‌المللی مخابرات موضوع حاکمیت بر فضای سایبر را در دستور کار خود قرار داد که اجلاس‌های ژنو ۲۰۰۳ و تونس ۲۰۰۵، دستاورد این فعالیت‌ها بودند. می‌توان گفت که برگزاری این دو اجلاس آغازی بر پایان فعالیت ایالات متحده بر اینترنت بوده و تا امروز که بیش از ده سال از این اجلاس می‌گذرد، بحث حاکمیت بر فضای سایبر یکی از مباحث محوری در مجامع، اتحادیه‌ها و نشست‌های مرتبط با جامعه اطلاعاتی بوده است. به همین دلیل از سال ۲۰۰۵ به بعد شاهد کارشکنی‌های سایبری ایالات متحده در سازمان ملل هستیم که نمونه‌های آن، رای منفی آمریکا به پیش نویس روسیه در کمیته اول در سال ۲۰۰۵ و شکست گروه کارشناسان دولتی در همین سال است.

ایالات متحده تا سال ۲۰۰۹ مشارکت هیچ کشور یا بخش خصوصی دیگری غیر از آیکان را برای اداره و حاکمیت بر اینترنت نمی پذیرفت. اما تحت فشار جهانی و یک عقب نشینی در ۳۰ سپتامبر ۲۰۰۹ اعلام کرد که به سایر دولت‌ها و بخش خصوصی نقش نظارتی بیشتری در آیکان خواهد داد و موافقت کرد تا از هیات‌های مشورتی متشکل از نماینده دولت‌ها و بخش خصوصی سراسر جهان استفاده کند و این هیات‌ها به بازنگری تصمیم‌های آیکان بپردازند تا این تصمیم‌ها به طور علنی گرفته شوند به صورتی که نشانه منافع عمومی باشند. البته اعلام شد که توصیه‌های این هیات‌ها برای آیکان الزام آور نخواهد بود و وزارت بازرگانی آمریکا نظارت خود را بر دستکاری نام‌های دامنه‌ها بر اساس قرارداد جداگانه با آیکان حفظ خواهد کرد که قرارداد فوق هم در سال ۲۰۱۱ به پایان رسید.

در این خصوص اقداماتی به صورت پراکنده برای مقابله با انحصار طلبی آمریکا در جهان صورت گرفت که به نتایج مطلوبی نرسید، یکی از این اقدامات جدایی در جهان شمولی اینترنت بود. این اقدام که در سال ۲۰۱٤ شروع شد و در پی آن بود که با ایجاد زیر ساخت شبکه‌ای جایگزین، یک اینترنت منطقه‌ای در منطقه بالکان ایجاد کند. این حرکت به هیچ وجه مطلوب ایالات متحده نگردید و این اقدام را بالکانیزه کردن اینترنت[۱] نامیدند و بدترین اقدام در حوزه اینترنت تلقی کردند، مسلما این اقدام که موجب رفع حصر امور فنی اینترنت از دست آمریکایی‌ها می‌شد و می‌توانست به الگویی برای دیگر نقاط جهان تبدیل شود، طبیعتا با واکنش منفی آمریکایی‌ها روبرو می‌شد.

با نگاهی دقیق‌تر به موضوع باید گفت به موازات فعالیت‌های انجام شده در کمیته اول، دوم و سوم مجمع عمومی و سازمان‌های تخصصی که موضوعات اساسی مرتبط با فضای سایبر از جمله تامین امنیت فضای سایبر و پیش گیری از جرم در فضای سایبر را در دستور کار خود داشتند، در گوشه دیگری از سازمان ملل (اتحادیه بین‌المللی ارتباطات راه دور) مخابرات[۲]

۱. Balkanisation of the Internet.
۲. International Telecommunication Union (ITU).

فصلنامه علمی (مقاله علمی-پژوهشی) جامعه‌شناسی سیاسی ایران، سال چهارم، شماره سوم (پیاپی ۱۵)، پاییز ۱۴۰۰

موضوع حاکمیت سایبری در دستور کار قرار گرفت. این سازمان تخصصی[۱] در زمینه امنیت سایبری نیز فعالیت‌های مهمی داشته است. اما بحث حاکمیت بر فضای سایبر با نام این سازمان گره خورده است.

اجلاس تونس در سال ۲۰۰۵، ادامه تلاش‌های بین‌المللی برای مقابله با حاکمیت انحصاری آمریکا بر فضای سایبر می‌باشد.

در ماده ۳٤ "دستور کار تونس برای جامعه اطلاعاتی" همان گونه که قبلا اشاره شد، مفهوم حاکمیت بر اینترنت، این گونه تعریف شد:

"توسعه و کاربرد نقش‌های مربوطه، اصول مشترک، هنجارها، قواعد، رویه‌های تصمیم سازی و برنامه هایی است که توسط دولت ها، بخش خصوصی و جامعه مدنی به منظور شکل دهی به تکامل و استفاده از اینترنت صورت می‌گیرد "

در نتیجه مفهوم حاکمیت بر اینترنت بین کارشناسان و صاحب نظران، محل چالش است. فارق از مفهوم تعوریک، آنچه در عمل دیده می‌شود تسلط کامل ایالات متحده بر تار و پود فضای سایبر در تاریخ این فناوری است.

بنابراین آنچه در تاریخ حکمرانی اینترنت شاهد هستیم، تلاش‌های ملی، بین‌المللی و منطقه‌ای علیه حاکمیت انحصاری ایالات متحده بر فضای سایبر است که این تلاش‌ها به خاطر کارشکنی‌های ایالات متحده نتایج حداقلی در پی داشته است.

چالش

نگرش دولت‌ها و تعارض با حاکمیت

دولت به دلیل داشتن صلاحیت از مصونیت‌ها و مزایای خاصی برخوردار است و حاکمیت (Sovereignty) به معنای قدرت عالیه و تجزیه ناپذیر دولت جهت وضع قوانین خود و وقایع که داخل مرزهای خود رخ می‌دهد، تحت تاثیر دیگر دولت‌ها قرار نمی گیرد. طبق نظریه رضایت دولت، می‌توان بیان نمود که هر دولتی می‌تواند محدودیت هایی بر اختیارات خود از طریق پذیرش محدودیت‌های ناشی از حقوق بین الملل و یا تحت تاثیر سازمان‌های بین‌المللی که در آن عضویت دارد را اعمال کند.۲ برای مفهوم صلاحیت دولت در حقوق بین الملل اصولی ایجاد شده است که عبارتند از: " اصل تابعیت، اصل سرزمینی بودن، اصل حمایتی (واقعی) بودن، اصل جهانی بودن " که کشورها از طریق این اصول صلاحیت خود را اعمال می‌کنند.

اختلاف صلاحیت زمانی رخ می‌دهد که ادعای صلاحیت ناروای یک کشور می‌تواند در مغایرت با منافع تجاری و اقتصادی اتباع (حقیقی یا حقوقی) یک دولت بیگانه باشد.۳ فقدان رویکردی مشترک در فضای سایبر از مواردی است که کشورها به اعمال صلاحیت خویش در آن می‌پردازند.

ابتدا باید در نظر داشت که تفاوت میان تعارض صلاحیت قانونی و تعارض صلاحیت قضایی از یک سو و شناسایی و اجرای حکم از سوی دیگر مورد نظر قرار می‌گیرد. از طرفی تعارض، هم پیرامون صلاحیت قانون گذاری مطرح است و هم صلاحیت قضایی.

---

۱. Specialized Agency.

۲. رابرت بلدسو، بوسچک، فرهنگ حقوق بینالملل، ترجمه بهمن آقایی، تهران، کتابخانه گنج دانش، ۱۳۷۵، صص۸۲-۸۳.

۳. See Authony Aust, op cit. p. ۱۰۸.

در بحث تعارض قوانین، منظور از صلاحیت قانون گذاری تشخیص قانونی است که از بین قوانین متعارض می‌بایست بر موضوع معینی حکومت کند و منظور از صلاحیت قضایی نیز تشخیص دادگاهی است که صلاحیت رسیدگی به موضوع معینی را دارد[۱].

موضوع اصلی که موجب ایجاد تعارض صلاحیت در فضای سایبر است، رویه متفاوت کشورها در اتخاذ صلاحیت‌های مختلف قانونی و ارایه راهکارهای حقوقی متضاد است. بنابراین حل تعارض صلاحیت در این فضا متوقف به تعیین قانونگذار صالح در فضای سایبر است. بی شک بخش عمده قانونگذاری در این فضا از جانب دولت‌ها صورت گرفته است. سازمان‌های بین‌المللی و نهادهای فنی تخصصی سایبری در این زمینه اقدامات موثری داشته اند که در مواردی میان حوزه‌های صلاحیت آن‌ها تداخل ایجاد شده است. بنابراین تعیین حدود صلاحیتی هر کدام تا حدود زیادی به حل تعارض در خصوص صلاحیت قانونگذاری خواهد انجامید.

موارد فوق سبب می‌شود که تجارت و ارتباطات در فضای سایبر خطرناک شود. عدم توانایی محاکم در دستیابی به موازنه برای رفع نگرانی‌ها به دلیل نا کافی بودن اصول سنتی صلاحیت قابل اعمال در فضای سایبر است[۲]. در حالی که رسانه‌های دیگر از جمله روزنامه‌ها با علم به عواقب قانونی اقداماتشان، اغلب رفتار خویش را با عملکردشان سازگار کرده و مسلما به نتایج اعمالشان عالم هستند[۳].

مساله ابتدایی در تعارض صلاحیت در فضای سایبر، مربوط به قوانین حاکم بر این فضاست. این که چه قوانینی باید ملاک قرار گیرند که در صورت تعارض، می‌بایست در فکر حل آن بود. بعضی بر این باورند که قوانینی که مربوط به اختلافات اینترنت می‌باشند باید لحاظ گردند، که باوری نادرست است زیرا علاوه بر قوانین خاص این فضا مثل تجارت الکترونیک، قواعد حقوق بین الملل نیز باید مطمع نظر قرار گیرند[٤].

در فضای سایبر، چالش اصلی درانتخاب قانون خارجی و اجرای آرای دادگاه‌های خارجی، وجود احتمال تعارض با حاکمیت کشورهاست.

دولت‌ها موظفند مطابق حقوق بین الملل در هنگام مواجهه با موضوعاتی مرتبط با عناصر خارجی، علیرغم وجود ارتباط میان فعل مرتکب و صلاحیت کشور، صلاحیت خود را به نحو محدود اعمال نمایند به نحوی که منجر به تجاوز به صلاحیت دیگر کشورها نگردد[٥]. بنا بر مطالب فوق اعمال نامحدود صلاحیت دولت هم ناقض حقوق بین الملل است و هم می‌تواند نظم بین‌المللی را مختل نماید و منجر به اقدامات تلافی جویانه[٦] در سطوح سیاسی، حقوقی و اقتصادی گردد[۷]. بر اساس مطلب اخیر

۱. نجاد علی الماسی، تعارض قوانین، تهران مرکز نشر دانشگاهی، ۱۳۸۹، صص ۱۵-۱٦.

۲. Philip Adam Davis, 'The Defamation of Choice –of-Law in Cyberspace; Countering the View that the Restatement (second) of Conflict of Laws is Inadequate to Navigate the Borderless Reaches of the Intangible Frontier Communications Law Journal, Vol. ٥٤. Issue ۲. ۲۰۰۲. p. ۳٦۲.

۳. James R. Pielemeier,Constitution Limitation on Choice of Law; The Special Case of Multistate Defamation , University of Pennsylviana Law Review , Vol ۱۳۳. ۱۹۸٥, p. ۳۸۷.

٤. C. Lan Kyer, "Jurisdiction in cyberspace", Fasken Martineau Dumoulin LLP. pp. ۱-۲, available at: http: //www. fasken, com/files/Publication/ a۰۹۲۸۹da-le٤۳-٤٦ fa-b۸۹۱-a٤a۸۹٥٥f۷۳٦٦/Presentation /Publication Attachment /d۸a۳٤٤c۳-۷۸cc-٤٤f٤-bb٤۰-۰۳dlb٥۷۹۷٥b۰/JURISDICTION/۲۰IN۲۰/CYBERSPACE, PDF, (viaited۲۰۱۷).

٥. See ICJ,Judgment , Barcelona Traction, Light and Power Co. (belg. v. Spain),۱۹۷۰, Paras. ۱۷-٥۳.

٦. Reprisal.

۷. Gary B. Born, Reflections on Judicial Jurisdiction in International Cases, Georgia Journal of International and Comparative Law, Vol. ۱۷. No. ۱. ۱۹۸۷, p. ۳۳.

می‌توان اقدام آژانس رسمی ایالات متحده[۱] بر اعمال تحریم‌های ثانویه هلمز- باتون[۲] نسبت به ارتباطات اینترنتی شرکت‌های تجاری با کوبا را خلاف حقوق تلقی کرد.

کنوانسیون جرایم سایبری شورای اروپا (بوداپست) در بند ۵ ماده ۲۲، همکاری بین‌المللی را به عنوان راهکاری برای جلوگیری از تعارض صلاحیت دادگاه‌ها به کار بسته است که مقرر می‌دارد:

" در جایی که بیش از یک عضو ادعای صلاحیت رسیدگی به جرایم مقرر در این کنوانسیون را دارد، در صورت صلاحدید به شور نشسته و شایسته‌ترین عضو جهت تعقیب و پیگرد را تعیین می‌کند"

که البته ماده فوق بیشتر جنبه توصیه‌ای داشته و به صلاحیت قانونگذاری توجه نکرده است.

چالش

فرامرزی بودن فضای سایبر

فضای سایبر در سطح معنایی، فضای خیالی بین شبکه‌های رایانه‌ای است. می‌توان گفت که فضای سایبر برای توصیف هر مفهومی که در ارتباط با شبکه‌های رایانه‌ای، اینترنت و جامعه اطلاعاتی و فناوری اطلاعات به کار برده می‌شود و کاربران در این فضا به تجربه‌ای اجتماعی از تعامل و اشتراک گذاری اطلاعات، کسب و کار، بحث‌های گروهی و بازی و تفریح که به صورت غیر فیزیکی است، دست پیدا می‌نمایند. فضای سایبر فراتر از اینترنت است که اینترنت در حال گسترش این فضاست. با شکل گیری فضای سایبر و توسعه سریع آن، مفاهیم عرصه زندگی نیز به سمت تغییر ماهوی گام برمی دارد به طوری که در آن همه چیز از هویت، فرهنگ، روابط خصوصی و گروهی و نیز حکمرانی در حال تغییر و دگرگونی است.

به هر روی طراحی اینترنت به عنوان بزرگترین شبکه به صورت آزاد[۳] در فضای سایبر بوده[٤] و معماری آن به نحوی است که دسترسی به آن امکان پذیر و اختیاری است[٥].

با توجه به مطالب پیش گفته، فضای سایبر از نقطه نظر تکنولوژیکی، بدون مرز باقی مانده و از منظر تعوری‌های روابط بین الملل فرا ملی بودن و جهانی بودن، دو ویژگی بارز آن می‌باشد.

از ویژگی‌های بارز فضای سایبر فقدان مرزهای فیزیکی است به طوری که فعالیت در این فضا، فعالیت و حضور در شبکه گسترده جهانی محسوب می‌شود. رعایت حدود مرزها و نیز جغرافیای سیاسی در این فضا دشوار است با این توضیح که محتویات یک سایت از نظر حریم خصوصی - آزادی بیان – حقوق مالکیت فکری و ارتکاب جرایم در کشورها متفاوت است.

ماهیت سیالی فضای سایبر به گونه‌ای است که کار را برای انتظام بخشی هر چه بهتر این فضا دشوار نموده است. ضوابط و قواعد در فضای جغرافیایی و فیزیکی در برخی موارد قابلیت تطبیق و اجرا در این فضا را نخواهد داشت که در این رابطه می‌توان به فقدان مرزهای سیاسی به عنوان ماهیت چالشی موجود در فضای سایبر اشاره نمود.

می‌توان گفت که فضای سایبر حاصل پیشرفت در زمینه فناوری‌های ارتباطی و اطلاعاتی است، با توجه به ماهیت ناملموس و مجازی خود، به تدریج در کنار فضای عینی و واقعی قرار گرفته و هر روز نقش پررنگ تری در زندگی بشر ایفا می‌کند. فضای سایبر مانند فضای عینی دارای عناصر مختلفی است. اگر در فضای عینی و جغرافیایی مفاهیمی مانند حاکمیت و امنیت

---

۱. U. S. Agency Official.
۲. Cuban Liberty and Democratic Solidarity (Libertad) Act (helms-Burton Act), ۱۹۹٦.
۳. open
٤. Wu and Goldsmith, ۲۰۰۸: ۲۳.
٥. Wu and Goldsmith, ۲۰۰۸: ۹۰

وجود دارد، در فضای سایبر این مفاهیم کارکردهای متفاوتی پیدا کرده است. برای مثال در حاکمیت ملی کشورها مواردی مانند حاکمیت سیاسی، اقتصادی و نظامی دچار دگرگونی شده و تهدیدها تغییر کرده است و چهره جدیدی از تهدیدها مانند هکرها، ویروس ها، تروریسم سایبری و سایت‌های هرزه نگاری به وجود آمده است. بنابراین اگر در فضای عینی مرزها، محدود کننده فعالیت‌ها و عدم تداخل آن‌ها با یکدیگر هستند و برای جلوگیری از آن، از مرزها پاسداری می‌کنیم، می‌توان گفت که ماهیت مرز همان است ولی دگرگون شده و کارکرد آن تغییر کرده و در فضای سایبر مرزهای مجازی داریم که مانند مرزهای عینی قابل پاسداری نمی باشند.

با بررسی کارکرد مرزها در عصر فناوری ارتباطات و اطلاعات در دو فضای عینی و مجازی (سایبر) می‌توان به ماهیت متفاوت این فضا پی برد.

۲. کارکرد مرزها در فضای عینی (واقعی)

با گسترش و توسعه نظریه جهانی شدن، بحث‌های گسترده‌ای در خصوص تغییرهای ساختاری ماهیت مرزها مورد نظر قرار گرفته است. این تغییرها به عنوان فرآیند فرسایشی سرزمین و مرز ارایه شد[۱]. به عبارتی با پیشرفت فناوری ارتباطات و اطلاعات و انقلاب رسانه‌ای در جهان با بهره گیری از سامانه‌های ارتباطی، بسیاری از متفکران علوم اقتصادی و اجتماعی خبر از حذف مرزها و پیدایش دهکده جهانی دادند. همچنین با توسعه شبکه‌های اقتصادی و شرکت‌های چند ملیتی رشد سریع همگرایی اقتصادی در جهان سرمایه داری و تسری آن به نقاط مختلف جهان موجب شد تا افراط گرایان در باره جهانی شدن، بیشتر از آنچه اتفاق افتاده بود اغراق کنند.

۳. کارکرد مرزها در فضای سایبر

در فضای سایبر بر خلاف فضای عینی نیاز به جابجایی‌های فیزیکی نیست، ماهیت فضای سایبر، ماهیتی فرا فیزیکی و ناملموس و متفاوت با فضای عینی است. در واقع پیدایش این فضا با چنین ماهیتی است که هرگز مبتنی بر پارامترهای فضای عینی (سنتی) نباشد و در نتیجه درگیر مسایل و قیدهای موجود نگردد.

با توسعه و گسترش فضای سایبر، مفاهیم جدیدی در ادبیات این رشته در جهان رایج شد که مبنای این ادبیات نیز فعالیت‌ها و توسعه بشر در فضای عینی است که برخی از آن‌ها عبارت از: دولت الکترونیک – تجارت الکترونیک – بانک داری الکترونیک – شهر الکترونیک و...

پیدایش و توسعه فضای سایبر و شکل گیری دولت الکترونیک در کشورها، موجب پیدایش مرزهای مجازی شده است. دولت‌ها و مدیران شرکت‌ها برای حفظ ارزش‌ها و نیز تامین امنیت روانی، اجتماعی و اقتصادی مشترکان خود، ضمن ترویج و انتشار اندیشه‌ها و ارزش‌های مادی و معنوی خود، اقدام به ایجاد مرزهای سایبر نظیر فیلتر، رمز ورود، دامنه، حق عضویت، رمز نگاری اطلاعات و... می‌کنند. با این توصیف می‌توان بیان نمود که مرز در فضای سایبر به نسبت مرزها در فضای عینی، دارای ماهیتی پایدار و حتی نفوذ ناپذیر خواهد بود.

به طور کلی خرابکاری‌ها و درز اطلاعات در فضای سایبر از عوامل اصلی شکل گیری مرزها در این فضا می‌باشد زیرا صدمه‌ای که بدین وسیله به شبکه‌ها وارد می‌شود به دلیل گستردگی کاربران و میزان خسارت، می‌تواند بسیار مخاطره انگیز

۱. Appadurai, A,۱۹۹٦. Modernity at large. Cultural dimensions of globalization. Minneapolis: University of minnestoa.

باشد و آثار آن تا مدت‌ها باقی بماند. لاکور[۱] معتقد است که تروریسم رایانه‌ای ممکن است برای تعداد کثیری از مردم بسیار ویران کننده‌تر از جنگ‌های بیولوژیکی و رایانه‌ای باشد – از منظر امنیت ملی در شرایط حاضر دولت‌ها با تهدیدهای نامشخص در این فضا روبرو هستند که امنیت آنها را به خطر انداخته و ابزارهای سنتی تامین کننده امنیت دیگر قابلیت مقابله با آن‌ها را ندارند. – که با لحاظ ویژگی خاص این فضا ضرورت ایجاد مرزهای مجازی احساس می‌شود. این باور می‌تواند وجود داشته باشد که میان مرزهای عینی و مجازی، از نظر ویژگی‌های هویت ساز پیوند معنا داری وجود دارد و نیز میان مرزهای فیزیکی (عینی) و مجازی همپوشی کارکردی وجود دارد و محدودیت‌های مرزها در فضای عینی، در فضای سایبر نیز میان جوامع و گروه‌های مختلف قابل پیگیری است.

نتیجه گیری

نظر به این که بررسی چالش‌ها و ظرفیت‌ها و جریان شناسی هنجارهای منتج به کنوانسیون سایبری از اهداف این نوشتار می‌باشد، تحلیل روندهای بین‌المللی و تلاش‌های جامعه جهانی برای شناسایی این جریان‌ها و تامین امنیت فضای سایبر و چالش‌ها و مشکلات مربوط به آن نیز مد نظر است. بنابراین در ابتدا لازم بود تعریف و تصویری از فضای سایبر و مفهوم امنیت در فضای سایبر ارایه دهیم و نیز با عنایت به این که هنوز کنوانسیون یا معاهده جهان شمولی در زمینه فضای سایبر بین دولت‌ها وجود ندارد و تلاش‌های جامعه بین‌المللی برای رسیدن به این مهم، در مرحله هنجارسازی است که در خصوص مفاهیم مرتبط با چالش‌ها و فرصت‌ها و نیز هنجارسازی به عنوان یکی از مراحل شکل گیری قواعد بین‌المللی مطالبی بیان گردید. رسیدن به توافق برای انعقاد معاهده در سطح جهانی، نیازمند همکاری بین‌المللی بازیگران اصلی این عرصه، یعنی دولت‌ها است که لزوم این همکاری مورد امعان نظر می‌باشد. تاکید بر این است، با توجه به این که سازمان ملل به عنوان بزرگ‌ترین سازمان بین‌المللی، مظهر همکاری دولت‌ها برای تامین صلح و امنیت جهانی است و امنیت سایبر نیز در حال تبدیل شدن به بخش مهمی از گفتمان مربوط به امنیت ملی و بین‌المللی است، بخش هایی در سازمان ملل مرتبط با فضای سایبر ایجاد و معرفی شوند.

---

۱. Walter Laqueur

منابع

فارسی

۱. آهنی، آمینه، محمد و فاطمه زهرا، فتح الهی (۱۳۹۳)، "حقوق بین الملل مدرن در مواجهه با جنگی پست مدرن(نبرد سایبری)"، راهبرد، سال بیست و سوم، شماره ۷۲.

۲. آیگناتس زایدل هومن فلدرن (۱۳۸۵)، حقوق بین الملل اقتصادی (ترجمه قاسم زمانی) تهران، شهر دانش.

۳. الماسی، نجاد علی (۱۳۹۲)، تعارض قوانین، تهران مرکز نشر دانشگاهی.

٤. ایدا، ریوشی (۱۳۷٦)، "شکل گیری قواعد بین‌المللی در دنیایی رو به تحول – نقد مفهوم حقوق قوام نیافته "، ترجمه اردشیر امیر ارجمند، مجله تحقیقات حقوقی، شماره ۱۹-۲۰.

٥. رابرت بلدسو، بوسچک (۱۳۷٥)، فرهنگ حقوق بینالملل، ترجمه بهمن آقایی، تهران، کتابخانه گنج دانش.

٦. کیهانلو، فاطمه، وحید، رضادوست (۱۳۹٤)، "حملات سایبر به مثابه توسل به زور در سیاق منشور سازمان ملل متحد"، فصل نامه تحقیقات حقوقی شماره ٦۹.

لاتین

۱. Appadurai, A,۱۹۹٦. Modernity at large. Cultural dimensions of globalization. Minneapolis: University of minnestoa.

۲. Brittish Guiana Boundary Case (۱۸۹۹) ۱۸۸ C. t. s. ٦۷; AlaskaBoundary Arbitration (۱۹۰۳) ۱٥ R. I. A. A. ٤۸۱ cited in; John P. Grant and J. Gaig Barker (۲۰۰۰). Parry &Grant Encyclopedic Dictionary of International Law, Third Edition, Oxford University Press.

۳. C. Lan Kyer, "Jurisdiction in cyberspace", Fasken Martineau Dumoulin LLP. pp. ۱-۲, available at: http: //www. fasken, com/files/Publication/ a۰۹۲۸۹da-le٤۳-٤٦ fa-b۸۹۱-a٤a۸۹٥٥f۷۳٦٦/Presentation /Publication Attachment /d۸a۳٤٤c۳-۷۸cc-٤٤f٤-bb٤۰-۰۳dlb٥۷۹۷٥b۰/JURISDICTION/۲۰IN۲۰/CYBERSPACE, PDF, (viaited۲۰۱۷).

٤. Department of Defens Dictionary of military and Associated Terms (Joint Publication ۱-۰۲). ۸. □□□□□□□□□ ۲۰۱۰(□□ □□□□□□□ □□□□□□□ ۱٥ □□□□□□□□□,۲۰۱۰. □. ۷٤.)

٥. Gary B. Born (۱۹۸۷), Reflections on Judicial Jurisdiction in International Cases, Georgia Journal of International and Comparative Law, Vol. ۱۷. No. ۱.

٦. Guzman, Andrew T. (۲۰۱۰) andmeyer Timothy L..., (۲۰۱۲) "International Soft Law", Journal of Legal Analysis. Vol ۲, No. ۱, khttp;/papers. ssrn. com/so۱۳/papers,cfm?id =۱۳٥۳٤٤٤,accessed ۲٥ March.

۷. James R. Pielemeier (۱۹۸٥), Constitution Limitation on Choice of Law; The Special Case of Multistate Defamation, University of Pennsylviana Law Review, Vol ۱۳۳.

۸. Kennth W. Abbott, Duncan Snidal, Hard and Soft Law in International Governance,The IO Foundation and the Massachusetts Institute of Technology , Vol,٥٤,Issue۳،۲۰۰۰,p. ٤۲۳.

۹. Launie K. Blank,International Law Cyber from Non-State Actors,International Law Studies (U. S. Naval war College),Vol. ۸۹،۲۰۱۳. p. ٤۳٥.

۱۰. Martin Pratt (۲۰۱۱), Book Let of Applied Issues in International Land Boundary Delimitation / Demarcation Practices, (A Seminar Organized by the OSCE Borders Team in co-operation With the Lithhuanian OSCD Chairmanship,۳۱ May to ۱ June ۲۰۱۱ Vilnius, Lithuania).

۱۱. Matthew C. Waxman. (۲۰۱۱) Cyber Attacks as Forse Under UN Charter Article ۲ (٤), International Law Studies, Vol۸۷.

۱۲. Philip Adam Davis, (۲۰۰۲) 'The Defamation of Choice –of-Law in Cyberspace; Countering the View that the Restatement (second) of Conflict of Laws is Inadequate to Navigate the Borderless Reaches of the Intangible Frontier Communications Law Journal,