Foreign Relations Center for Strategic Research
https://frqjournal.csr.ir E-ISSN: 2588-6541
Vol. 15, No. 4, Issue. 60, Winter 2024 **Received:** 2023/10/07 **Accepted:** 2024/03/04
Research paper

Cyber Geopolitics at the Crossroads of Power: An Analysis of US Cyber Hegemony in Confrontation with China

Mostafa Esmaeili
Corresponding Author, Assistant Professor in International Relations, Supreme National Defense University, Tehran, Iran.
Email: Esmaili@sndu.ac.ir 0000-0002-3215-5256
Amir Abbas Rokni
Ph.D. student in National Security, Supreme National Defense University, Tehran, Iran.
Email: Amir.roknni@gmail.com 0000-0002-0700-4624
Seyed Reza Hosseini
Master of Regional Studies (North America), Faculty of Law and Political Sciences, Allameh Tabataba'i University, Tehran, Iran.
Email: sr_hoseini96@yahoo.com 0000-0000-0000-0000

Abstract
The United States of America has long been the primary actor in shaping international cyber law norms and global cyberspace governance frameworks, actively engaging in this domain for nearly two decades. However, China's emergence as a key player in the cyber and technology realm has significantly changed the international landscape in recent years. Consequently, America's influence in this sphere appears to be challenged, and its discourse on cyberspace governance is seemingly declining. This profound investigation seeks to elucidate the far-reaching repercussions of the United States waning assertive power within the intricate tapestry of international law, juxtaposed against the meteoric rise of China's global influence, on the complicated dynamics of global cyber-geopolitics and the evolving paradigm of internet governance. Therefore, This research delves into the factors contributing to the erosion of US cyber power, including the decline of trust and credibility, policy shifts, and challenges in norm creation and enforcement. To this end, a descriptive-analytical approach examines China's growing influence in international cyber law. This entails a comprehensive analysis of its expanding cyber capabilities (espionage, offensive operations, technological advancements), diplomatic assertiveness in shaping global cyber governance frameworks and promoting alternative, state-centric norms aligned with the Communist Party's vision. Our analysis reveals that China's burgeoning cyber capabilities position it as a formidable competitor to the United States. Additionally, its diplomatic assertiveness enables China to advocate for alternative norms and establish itself as a proponent of national independence in cyberspace governance.

Keywords: cyber diplomacy, cyber governance, international norms, United States of America, China.

E-ISSN: 2588-6541 / Center for Strategic Research / Quarterly of Foreign Relations

10.22034/FR.2024.453168.1517

سال پانزدهم، شماره چهارم (پیاپی ۶۰)، زمستان ۱۴۰۲، صص. ۲۶۷- ۲۹۶
تاریخ دریافت: ۱۴۰۲/۰۷/۲۷ ـ تاریخ پذیرش: ۱۴۰۲/۱۲/۱۴

مقاله پژوهشی

ژئوپلیتیک سایبری در گذرگاه قدرت: تحلیل هژمونی سایبری ایالات‌متحده آمریکا در تقابل با چین

مصطفی اسماعیلی
استادیار روابط بین‌الملل، دانشگاه عالی دفاع ملی، تهران، ایران.
Email: Esmaili@sndu.ac.ir 0000-0002-3215-5256

امیرعباس رکنی
دانشجوی دکتری امنیت ملی، دانشگاه عالی دفاع ملی، تهران، ایران.
Email: Amir.roknni@gmail.com 0000-0002-0700-4624

سید رضا حسینی
کارشناسی ارشد مطالعات منطقه‌ای (آمریکای شمالی)، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران.
Email: sr_hoseini96@yahoo.com 0000-0000-0000-0000

چکیده

ایالات‌متحده آمریکا برای مدت طولانی، نزدیک به دو دهه به‌عنوان اصلی‌ترین بازیگر در شکل‌دهی به هنجارهای حقوق بین‌الملل سایبری و چهارچوب‌های حکمرانی جهانی بر فضای سایبر اقدام به کنشگری نموده است؛ اما در سال‌های اخیر، چین در مقام یکی از بازیگران کلیدی حوزه سایبری و فناوری، تغییرات چشم‌گیری در چشم‌انداز بین‌المللی به وجود آورده و درنتیجه، به نظر می‌رسد قدرت اثرگذاری آمریکا در این زمینه به چالش کشیده شده و گفتمان آمریکایی در حوزه حکمرانی بر فضای سایبری رو به افول گذاشته است. سؤال اصلی پژوهش حاضر بررسی این موضوع است که کاهش قدرت کنشگری فعال ایالات‌متحده در نظام حقوق بین‌الملل، در تقابل با افزایش قدرت روزافزون چین، چه پیامدهایی برای ژئوپلیتیک سایبری جهانی و تغییر شیوه حکمرانی بر اینترنت خواهد داشت؟ از همین‌رو، تلاش داریم تا عواملی که در کاهش قدرت سایبری آمریکا، ازجمله افت اعتماد و اعتبار، تغییرات سیاست‌ها و چالش‌های شکل‌گیری همچنین اجرای هنجارها نقش دارند را بررسی کنیم. به همین منظور، از رویکرد توصیفی-تحلیلی برای بررسی افزایش قدرت چین در حقوق بین‌الملل سایبری با استفاده از تحلیل جامع توانمندی‌های سایبری رو به رشد این کشور، قاطعیت دیپلماتیک و رویکردهای جایگزین برای حکمرانی سایبری استفاده شده است. نتایج نشان می‌دهد که گسترش قابلیت‌های سایبری چین، ازجمله جاسوسی سایبری، عملیات تهاجمی و پیشرفت‌های تکنولوژیک، این کشور را به یک رقیب سرسخت برای آمریکا تبدیل کرده است. قاطعیت دیپلماتیک نیز چین را قادر به کنشگری فعالانه در شکل‌دهی چهارچوب‌های حکمرانی سایبری جهانی و دفاع از هنجارهای جایگزین مورد تأیید حزب کمونیست ساخته و با ایجاد هنجارهای جدید توانسته است تا اقدام به ارائه رویکرد استقلال ملی در چشم‌انداز حکمرانی سایبری بین‌المللی نماید.

کلیدواژه‌ها: دیپلماسی سایبری، حکمرانی سایبری، هنجارهای بین‌المللی، ایالات‌متحده آمریکا، چین.

شاپای الکترونیک: ۶۵۴۱-۲۵۸۸/ پژوهشکده تحقیقات راهبردی/ فصلنامه روابط خارجی

10.22034/FR.2024.453168.1517

مقدمه و بیان مسئله

سال‌ها پیش، زمانی که اینترنت در مراحل ابتدایی خود بود، ایالات‌متحده به‌عنوان پیشوای فناوری اطلاعات نقش محوری در تشکیل آینده این فضای نوپا داشت. دانشگاه‌ها و مراکز تحقیقاتی آمریکایی، مهد نوآوری‌های بزرگی بودند که ساختمان اینترنت امروزی بر روی آن بنا شده است(Telefonica, 2023) . از آن دوران، دولت آمریکا با حمایت از ایده‌هایی همچون جریان آزاد اطلاعات و اینترنت باز و بدون مرز، سعی در هدایت جوامع جهانی به‌سوی فضایی مشترک داشته که قوانین و استانداردهای خاصی بر آن حاکم باشد (Global Free Flow of Information on the Internet, 2010)؛ اما با گذر زمان، غلبه اولیه آمریکا با چالش‌های جدی مواجه شد (Sherman, 2022) . مواردی همچون افشاگری‌های «ادوارد اسنودن»[1] در سال ۲۰۱۳ نشان داد که آژانس امنیت ملی آمریکا در فعالیت‌های گسترده جاسوسی سایبری دخیل بوده و اعتماد جوامع جهانی به استقلال نظام‌های ملی در حکمرانی بر فضای سایبر و احترام به حریم خصوصی کاربران در فضای آنلاین را نقض کرده است (Greenwald, 2014). این اتفاق زخم عمیقی بر پیکره رهبری جهانی آمریکا در حوزه فناوری اطلاعات وارد کرد. رفته‌رفته بسیاری از کشورها و حتی شرکای دیرینه آمریکا از پذیرش بی‌پرده استانداردها و ابتکارات واشنگتن امتناع کردند. همچنین، تغییر در سیاست خارجی آمریکا در دوره ریاست جمهوری دونالد ترامپ و یک‌جانبه‌گرایی افسارگسیخته او در رویکرد «نخست آمریکا» باعث بی‌اعتمادی بیشتر جامعه جهانی به این کشور شد (McTague, 2020). هرچند آمریکایی‌ها در ادامه و به دنبال سیاست‌های خود فهمیدند که دیگر تنها با استفاده از زور در فضای مجازی نمی‌توانند تضمین امنیت دائمی داشته باشند، اما ماهیت غیرمتمرکز و متغیر فضای سایبری، کنترل جامع بر آن را برای هر بازیگری دشوار و چالش‌برانگیز می‌کرد(Segal, 2022) .

به‌موازات ایجاد این فضای جدید و دگرگونی ژئوپلیتیکی سایبری، چین با پشتوانه اقتصاد در حال رشد و صعود خود، وارد این صحنه رقابت شد تا سهم خود را از قدرت در فضای سایبری نیز مطالبه کند. رویکرد چینی‌ها تفاوت‌های بنیادینی با آمریکایی‌ها داشت. آن‌ها بر کنترل دولتی بر فضای مجازی تأکید داشتند و شرایطی را ترجیح می‌دادند که بتوان از طریق آن فضای سایبری را کاملاً تحت نظارت و اختیار دولت قرار داد و البته این رویکرد، ریشه در باورهای عمیق چینی‌ها مبنی بر

1. Edward Snowden

لزوم حفظ ثبات و وحدت داخلی داشت و دقیقاً برعکس دیدگاه طرفداران فضای باز و آزاد اینترنت در آمریکا بود. بر همین اساس، با ورود یک بازیگر تازه‌نفس و قدرتمند به صحنه، رقابت بر سر تعیین قواعد حاکم بر فضای مجازی شدت یافت (Creemers, 2021). هرکدام از طرفین معتقد بودند که راه‌حل مورد نظرشان برای فضای سایبر بهتر است و باید آن را بر دیگری تحمیل کرد.

درهرحال، این رقابت پیامدهای متعددی برای جامعه بین‌المللی به همراه داشت، ازجمله این‌که آمریکایی‌ها مکرراً به جامعه جهانی تذکر می‌دادند که رویکرد چینی‌ها ممکن است بنیان‌های همکاری و وحدت جهانی در دنیای مجازی را تضعیف کند و موجب تکه‌تکه شدن اینترنت و دورشدن از آرمان اینترنت آزاد و یکپارچه گردد (Hoffmann, Lazanski & Taylor, 2020). علاوه بر این، برتری هرکدام از طرفین می‌تواند قرائت‌های کنونی از مفاهیم بنیادینی همچون آزادی‌های فردی و حقوق بشر آنلاین را به‌طورکلی دگرگون کند و حتی انتظار می‌رود که این رقابت موجب بروز واگرایی در استانداردهای فناورانه و ایجاد موانع در مسیر ادامه همکاری‌ها و تعاملات بین‌المللی شود(Larkin, 2022) .

از سوی دیگر، باید توجه داشت که ظهور چین به‌عنوان یک قدرت سایبری تأثیرگذار، با پیامدهای مهم و قابل‌توجه دیگری نیز همراه است. نخست اینکه منجر با ایجاد رقابتی شدید میان واشنگتن و پکن برای تسلط بر فضای سایبر یک جنگ سرد فناورانه شکل گرفت (Tung, Zander, & Fang, 2023). دوم اینکه با ارائه الگو و رویکردی متفاوت در خصوص حکمرانی سایبری، چین توانست هواداران متعددی را در میان کشورهای درحال‌توسعه به دست آورد. سوم اینکه رشد فزاینده قدرت سایبری چین به همراه ضعف نسبی آمریکا در این حوزه، منجر به دگرگونی بنیادین در موازنه قوا و ساختار کنونی حقوق بین‌الملل سایبری شده است.

یکی از مهم‌ترین پیامدهای تغییر قدرت در عرصه حقوق بین‌الملل سایبری، تأثیر بر فرایند شکل‌گیری و اجرای هنجارها و قواعد حاکم بر رفتار دولت‌ها در فضای مجازی است. تا پیش‌ازاین، ایالات‌متحده توانسته بود با تکیه بر برتری‌های خود، هنجارها و ارزش‌های مورد نظرش را در خصوص مقوله‌هایی چون دسترسی آزاد، حریم خصوصی، امنیت و ثبات سایبری در قالب قطعنامه‌ها و معاهدات بین‌المللی تدوین و تصویب کند؛ اما با ظهور چین، این فرایند با چالش مواجه شده و شاهد واگرایی در دیدگاه‌ها و سیاست‌ها هستیم.

چین با معرفی مفهوم «استقلال نظام‌های ملی در حاکمیت سایبری» سعی

دارد کنترل بیشتری بر فعالیت‌های سایبری در قلمرو خود داشته باشد. این رویکرد با تأکید بر نقش پررنگ دولت در تنظیم فضای سایبری، امنیت ملی و مصونیت داده‌ها، در تقابل با دیدگاه غربی قرار دارد که بر اصولی همچون بازبودن، آزادبودن و بی‌طرفی شبکه تأکید می‌ورزد. این امر سبب شده تا روند تکوین و پذیرش هنجارهای جهان‌شمول سایبری با چالش مواجه شود و شاهد تقابل دو مجموعه متمایز از قواعد و هنجارها باشیم (Lee, 2022).

یکی دیگر از پیامدهای مهم ناشی از تحول در موازنه قدرت، تأثیر بر روند همگرایی یا واگرایی درزمینه‌های فناوری، اقتصاد دیجیتال و حقوق مالکیت معنوی است. تا پیش‌ازاین ایالات‌متحده توانسته بود با ترویج الگوها و استانداردهای خود، روند همگرایی بین‌المللی را در این عرصه‌ها حداقل میان خود و شرکای استراتژیک اروپایی و آسیایی‌اش شکل دهد؛ اما با ظهور چین، شاهد ترویج الگوها و استانداردهای بومی از سوی این کشور بوده و نشانه‌هایی از واگرایی و تقسیم‌شدن به محورها و بلوک‌های مجزا مشاهده می‌شود.

غرب به‌طور مستمر با به‌کارگیری استراتژی «چین‌هراسی» و ایجاد ادراک تهدیدآمیز نسبت به حزب کمونیست چین سعی بر خنثی‌سازی ابتکارات پیش‌رونده پکن در عرصه نظام بین‌الملل دارد (ارغوانی پیرسلامی و علی‌پور،۱۴۰۲، ص. ۲۳). درهمین‌راستا، ایالات‌متحده آمریکا در مقام رهبر اصلی این استراتژی، به‌طور پیوسته در مجامع جهانی هشدار می‌دهد که تداوم این روند می‌تواند به تضعیف همبستگی و همکاری بین‌المللی در حوزه فناوری اطلاعات و ارتباطات منجر شود، اما با نگاهی عمیق به این هشدارها و اغراض پنهان در پشت آن، می‌توان گفت که تحولات اخیر در حقوق بین‌الملل سایبری و تغییر موازنه قدرت، ترس از تغییر قرائت آمریکایی حاکم بر این ساختار و کارکرد فعلی این نظم کنونی را آشکار می‌سازد. درواقع می‌توان گفت ما در آستانه ورود به دوران جدیدی در حقوق بین‌الملل سایبری قرارداریم؛ دورانی که ویژگی آن استقلال نظام‌های ملی در اداره فضای سایبری خواهد بود؛ امری که با مرکزیت چین در حال شکل‌گیری است (Segal, 2020).

با طرح این توضیحات، سؤال اصلی پژوهش حاضر بررسی این موضوع است که کاهش قدرت کنشگری فعال ایالات‌متحده در نظام حقوق بین‌الملل، در تقابل با افزایش قدرت روزافزون چین، چه پیامدهایی برای ژئوپلیتیک سایبری جهانی و تغییر شیوه حکمرانی بر اینترنت خواهد داشت؟ و به دنبال آن، فرایند دگرگونی قدرت چه تأثیری بر جهت‌گیری آینده و کارکرد نظام حقوق بین‌الملل سایبری

خواهد گذاشت؟ و آیا شاهد ظهور دوران جدیدی در حقوق بین‌الملل سایبری با ویژگی‌های متفاوت خواهیم بود؟ پاسخ به این پرسش‌ها نیازمند بررسی دقیق تحولات صورت گرفته و تجزیه‌وتحلیل پیامدهای آتی است تا بتوان به درکی جامع از آینده نظام حقوق بین‌الملل سایبری دست‌یافت.

پژوهش حاضر با هدف کمک به درک بهتر ماهیت تحولات در حقوق بین‌الملل سایبری و ظهور یک نظم نوین بین‌المللی درصدد است که در یک اثر پژوهشی توصیفی-تحلیلی، به بررسی جامع چالش‌ها و تحولات در حقوق بین‌الملل سایبری و تأثیر آن بر موازنه قدرت و آینده این نظام حقوقی بپردازد. در ابتدا، وضعیت فعلی حقوق بین‌الملل سایبری و نقش حاکم ایالات‌متحده در آن تشریح می‌شود. سپس به بررسی عوامل قدرت‌یابی چین و چالش این کشور با سلطه آمریکا پرداخته شده و در ادامه، پیامدهای کلان حاصل از این تغییر قدرت برای ساختار و کارکرد حقوق بین‌الملل سایبری تجزیه‌وتحلیل می‌گردد و درنهایت چشم‌انداز آتی این حوزه حقوقی تشریح خواهد شد. یافته‌های این پژوهش نشان می‌دهد که نتیجه تحولات اخیر در عرصه حقوق بین‌الملل سایبری، افول نسبی جایگاه ایالات‌متحده به‌عنوان یک ابرقدرت سایبری و هم‌زمان با آن، صعود فزاینده قدرت چین در این عرصه بوده است. این تحول ژئوپلیتیکی و جابجایی قدرت، پیامدهای مهمی به همراه خواهد داشت که مهم‌ترین آن تأثیر بر فرایند شکل‌گیری و ساماندهی هنجارها و قواعد حاکم بر حقوق بین‌الملل سایبری است. با توجه به این‌که تاکنون ایالات‌متحده توانسته بود با تکیه بر برتری‌های خود، الگوها و ارزش‌های مورد نظرش را در قالب مجموعه‌ای از هنجارها در خصوص مفاهیمی همچون دسترسی آزاد، حریم خصوصی، بی‌طرفی شبکه و ... منتشر و تحمیل نماید، با ظهور چین به‌عنوان یک قطب قدرت در فضای سایبر، دیگر شاهد این وضعیت یک‌سویه نخواهیم بود. دلیل این امر نیز واضح است، چراکه چین درصدد است تا با معرفی و ترویج مفهوم «استقلال نظام‌های ملی در حاکمیت سایبری» الگو و رویکردی متمایز و مجزا از الگوی فعلی «حکمرانی بر اینترنت» را جایگزین سازد. الگوی چین برخلاف الگوی ایالات‌متحده، بر تأکید بر کنترل دولت‌ها بر فضای سایبری داخل مرزها و همچنین حفاظت از حریم خصوصی و صیانت از داده‌های ملی تأکید دارد (Segal, 2020). با توجه به تمایل روزافزون کشورها به حفاظت از حاکمیت سرزمینی خود و تسری هنجارهای حقوق بین‌الملل سنتی به حوزه سایبر، انتظار می‌رود الگوی حکمرانی سایبری چین، در آینده‌ای نه‌چندان دور، جایگزین الگوی حکمرانی اینترنت آزاد آمریکایی شود.

۱. زمینه تاریخی رهبری آمریکا در حقوق بین‌المللی سایبری

رهبری آمریکا در قوانین بین‌المللی سایبری را می‌توان در روزهای اولیه اینترنت جست‌وجو کرد. ایالات‌متحده به‌عنوان پیشگام در حوزه نوآوری‌های فناوری، نقش مهمی در توسعه و گسترش فضای سایبری ایفا کرده است. مؤسساتی مانند «آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی»[1] (*DARPA*) و مؤسسات دانشگاهی مانند دانشگاه ام‌آی‌تی و استنفورد، نقش مهمی در پایه‌گذاری اینترنت داشتند. در این‌دوره، ایالات‌متحده به دلیل تخصص تکنولوژیک، زیرساخت‌های قوی و حضور شرکت‌های فناوری پیشرو، برگ برنده فضای مجازی را داشت. دولت ایالات‌متحده فعالانه جریان آزاد اطلاعات، اینترنت باز، قابل همکاری و اصول حکمرانی چندجانبه را ترویج کرد. این ارزش‌ها اساس نفوذ ایالات‌متحده در شکل‌دادن به هنجارهای سایبری جهانی را تشکیل دادند. ایالات‌متحده از طریق ابتکارات و چهارچوب‌های مختلف، کمک‌های زیادی به توسعه قوانین بین‌المللی سایبری کرده است. یکی از نقاط عطف، ایجاد گروه کارشناسان دولتی سازمان ملل متحد درزمینهٔ تحولات در حوزه اطلاعات، مخابرات و امنیت بین‌المللی بود. ایالات‌متحده نقش مهمی در تشکیل و رهبری کارشناسان دولتی سازمان ملل متحد ایفا نمود و این گروه گزارش‌های اثرگذاری در مورد رفتار مسئولانه دولت در فضای سایبری ارائه کرد (West, 2019). همچنین، ایالات‌متحده فعالانه در شکل‌دادن به طرح‌های سایبری منطقه‌ای و جهانی مشارکت داشته است و نقشی کلیدی در ارتقای برنامه‌های ظرفیت‌سازی سایبری، تسهیل همکاری‌های بین‌المللی درزمینهٔ جرائم سایبری و حمایت از حفاظت زیرساخت‌های حیاتی ایفا کرده است. آمریکا از طریق تعاملات دوجانبه و چندجانبه، به دنبال ایجاد هنجارهای رفتار مسئولانه دولت، تشویق به اتخاذ بهترین شیوه‌های تأمین امنیت سایبری و تقویت همکاری بین‌المللی در مقابله با تهدیدات سایبری است.

۲. عوامل مؤثر در افول هژمونی سایبری ایالات‌متحده آمریکا

آمریکا برای مدتی طولانی در شکل‌دادن به قوانین و حکمرانی سایبری بین‌المللی نیروی غالب بوده است؛ اما در سال‌های اخیر، دچار کاهش نفوذ و جایگاه خود در چشم‌انداز سایبری جهانی شده است(Chen & Yang, 2022) . این کاهش را می‌توان به عوامل متعددی نسبت داد که شدیداً بر موقعیت و اثربخشی آمریکا در قوانین

1. *D*efense *A*dvanced *R*esearch *P*rojects *A*gency

بین‌المللی سایبری تأثیر گذاشته است. درک این عوامل برای درک تغییرات در حال وقوع حکمرانی سایبری جهانی و چالش‌های پیش‌روی آمریکا در حفظ نقش رهبری خود بسیار مهم است.

در این بخش، عوامل کلیدی مؤثر در افول آمریکا یعنی کاهش اعتماد و اعتبار، تغییر سیاست‌ها و درک جهانی و چالش در شکل‌گیری و اجرای هنجارها را بررسی خواهیم کرد. با بررسی این عوامل، می‌توانیم دیدگاه‌های ارزشمندی در مورد تغییرات پیچیده شکل‌دهنده چشم‌انداز کنونی حقوق بین‌المللی سایبری و پیامدهای نقش آمریکا در این حوزه به دست آوریم.

۲-۱. از بین رفتن اعتماد و اعتبار

یکی از عوامل مهم در افول هژمونی آمریکا به‌عنوان کنشگر مؤثر و فعال در حقوق بین‌الملل سایبری، از بین رفتن اعتماد و اعتبار این کشور به‌عنوان تنها قطب نظام بین‌المللی است (قلخانباز، یزدانی و ابراهیمی،۱۴۰۲، ص. ۴۵). اعتماد یکی از مؤلفه‌های اصلی همکاری بین‌المللی، به‌ویژه در حوزه امنیت سایبری است؛ اما افشای فعالیت‌های نظارتی گسترده آمریکا، مانند آنچه توسط «ادوارد اسنودن»[1] در سال ۲۰۱۳ افشا شد، به‌شدت اعتماد سایر کشورها به تعهد آمریکا نسبت به حریم خصوصی و حفاظت از داده‌ها را خدشه‌دار کرده است.

افشاگری‌های اسنودن، گستره برنامه‌های نظارتی «آژانس امنیت ملی آمریکا»[2] را که ارتباطات داخلی و بین‌المللی را هدف قرار می‌داد، نمایان کرد. این افشاگری نه‌تنها جامعه بین‌المللی را شوکه کرد، بلکه نگرانی‌هایی در مورد نقض حقوق حریم خصوصی و سوءاستفاده از قدرت را برانگیخت(Bowden, 2013) . درنتیجه، بسیاری از کشورها در خصوص مشارکت و همکاری در حوزه امنیت سایبری با آمریکا محتاط شدند، زیرا می‌ترسیدند حریم خصوصی و حاکمیت خودشان به خطر بیفتد.

علاوه بر این، تصور تقدم منافع امنیت ملی ایالات‌متحده بر همکاری‌های جهانی، موجب تشدید فرسایش اعتماد شد. رویکرد قاطع دولت آمریکا در حمایت از اقدامات سخت‌گیرانه‌تر در حوزه امنیت سایبری، ازجمله طرح‌هایی نظیر ایجاد درهای پشتی (راه‌های نفوذ) در رمزنگاری و افزایش نظارت، نگرانی‌ها را پیرامون تعهد این کشور به حفظ حقوق حریم خصوصی و حاکمیت قانون تشدید کرد.

1. Edward Snowden
2. U.S. National Security Agency's (NSA)

از بین رفتن اعتماد و اعتبار آمریکا عواقب زیادی بر توانایی این کشور برای تأثیرگذاری بر شکل‌گیری هنجارهای سایبری و اجرای آن‌ها در جهان داشته است. سایر کشورها، به‌ویژه آن‌هایی که منتقد اقدامات نظارتی آمریکا هستند، به دنبال متحدان و مشارکت‌های جایگزین برای متعادل‌کردن قدرت آمریکا در حکمرانی سایبری بوده‌اند. این شرایط، موقعیت آمریکا را تضعیف کرده و توانایی آن برای شکل‌دادن به هنجارهای سایبری جهانی مطابق با ترجیحات خود را محدود کرده است.

۲-۲. تغییر سیاست و ادراک جهانی

از دیگر عواملی که در کاهش قدرت حقوق بین‌الملل سایبری آمریکا نقش داشته، تغییر در اولویت‌های سیاستی این کشور و در پیِ آن درک جهانی از تعهد این کشور به حکمرانی سایبری است. در طول یک دهه گذشته، آمریکا شاهد تغییراتی در سیاست خود بوده است که همگی ناشی از مسائل امنیتی داخلی، تغییرات ژئوپلیتیکی و ماهیت در حال تحول تهدیدات سایبری بوده است.

تأکید روزافزون بر امنیت ملی و حفاظت از زیرساخت‌های حیاتی منجر به امنیتی‌شدن فضای سایبری در آمریکا شده است. در برخی کشورها این تغییر در اولویت‌های سیاستی آمریکا به‌عنوان رویکردی بیش‌ازحد نظامی برای امنیت سایبری تلقی شده که تأکید نامتناسبی بر قابلیت‌های تهاجمی و بازدارندگی سایبری دارد (Harnisch & Zettl-Schabath, 2022). چنین تصوراتی در میان سایر کشورها شک‌برانگیزشده و توانایی آمریکا برای جلب حمایت جهانی برای ابتکارات سایبری خود را کاهش می‌دهد.

علاوه بر این، برداشت جهانی از تعهد آمریکا به حکمرانی سایبری توسط اقدامات و سیاست‌های این کشور شکل گرفته است. استفاده از قابلیت‌های سایبری تهاجمی، مانند کرم «استاکس‌نت» که برنامه هسته‌ای ایران را هدف قرار داد، سؤالاتی در مورد پایبندی آمریکا به قوانین بین‌المللی و اصول حکمرانی در فضای سایبری برانگیخته است (Kalen & Howard, 2016). برخی کشورها این اقدامات را به‌عنوان سابقه خطرناکی برای سایر کشورها در نظر می‌گیرند که به‌طور بالقوه منجر به تشدید درگیری‌های سایبری و تضعیف ثبات اکوسیستم سایبری جهانی می‌شود.

علاوه بر این، خروج آمریکا از توافق‌نامه‌ها و نهادهای بین‌المللی نیز به کاهش نقش آمریکا در حکمرانی سایبری جهانی کمک کرده است. تصمیم برای خروج از

«توافقنامه پاریس در مورد تغییرات آب و هوایی»[1] و «توافق هسته‌ای ایران»[2] در کنار تیرگی روابط با سازمان‌های چندجانبه مانند سازمان ملل، در مورد تعهد آمریکا به چندجانبه‌گرایی و تمایل این کشور برای مشارکت در تلاش‌های مشترک برای رسیدگی به چالش‌های جهانی، ازجمله چالش‌های حوزه سایبری، تردیدهایی را برانگیخته است.

۲-۳. چالش در شکل‌گیری و اجرای هنجارها

چالش در شکل‌گیری و اجرای هنجارها بر موقعیت آمریکا در قوانین بین‌المللی سایبری تأثیر گذاشته است. هنجارها، رهنمودهایی برای رفتار مسئولانه دولت در فضای سایبری هستند و به ثبات و امنیت محیط دیجیتال کمک می‌کنند؛ اما آمریکا در ترویج و اجرای هنجارهای سایبری درصحنه جهانی با چالش‌هایی مواجه است.

یکی از این چالش‌ها ماهیت پیچیده و متنوع خود فضای مجازی است. فضای مجازی از مرزهای ملی فراتر رفته و توسعه هنجارهای جهانی که برای همه دولت‌ها قابل اجرا و قابل قبول است را دشوار می‌کند. آمریکا در پذیرش و پایبندی به هنجارهای سایبری تحت رهبری خود، با مقاومت سایر کشورها، به‌ویژه کشورهایی با نظام‌های سیاسی و ارزش‌های فرهنگی متفاوت، مواجه شده است (Studies, 2019). این تفاوت در دیدگاه‌ها و منافع، مانع شکل‌گیری هنجارهای منسجم جهانی شده و تلاش برای اجرا را پیچیده می‌کند.

ازطرفی سرعت بسیار پیشرفت‌های فناوری در حوزه سایبری، توسعه هنجارهای اثربخش را دچار معضل می‌کند. آمریکا، به‌عنوان کشوری پیشرو در فناوری، اغلب خود را در رقابتی برای همگام‌شدن با تهدیدات و آسیب‌پذیری‌های سایبری نوظهور می‌بیند. تکامل دائمی چشم‌انداز سایبری نیازمند چهارچوب‌های هنجاری چابک و سازگار است که بتواند چالش‌های جدید را رفع کند. بااین‌حال، روند شکل‌گیری هنجارها عموماً کُند است و همگام‌شدن با تهدیدات سایبریِ به‌سرعت در حال تغییر را دشوار می‌کند. چالش دیگر، نبود اجماع در چهارچوب قانونی و هنجاری حاکم بر فضای مجازی است. برخلاف حوزه‌های سنتی، مانند زمین، دریا و هوا، فضای سایبری فاقد چهارچوب قانونی تعریف‌شده و قوانین تثبیت‌شده جهت تعامل است. فقدان هنجارهای جهانی مورد توافق و تفسیرهای متفاوت از قوانین بین‌المللی

1. Paris Agreement on climate change
2. Iran nuclear deal

موجود، اجرای هنجارهای سایبری در کشورهای مختلف را چالش‌برانگیز می‌کند. آمریکا، علی‌رغم تلاش‌های خود برای ترویج رویکردی مبتنی بر قانون در حکمرانی سایبری، با مقاومت کشورهایی مواجه است که حامی رویکرد دولت‌محورتر یا مبتنی بر قدرت هستند (Segal, 2020). آمریکا در اجرای مؤثر هنجارهای سایبری در محیطی که ویژگی‌هایی چون ناشناس‌بودن، مشکل در انتساب و تکثیر عوامل سایبری تحت حمایت دولتی و غیردولتی دارد، با چالش مواجه است. به‌طور خاص، انتساب، مانع مهمی در پاسخگو نگه‌داشتن عوامل مسئول در فعالیت‌های سایبری است. دشواری ذاتی در نسبت‌دادن حملات سایبری به عوامل یا دولت‌های خاص، اجرای هنجارها و تحمیل پیامدهای نقض آن را مختل می‌کند. این امر توانایی آمریکا برای جلوگیری از رفتار مخرب سایبری و حفظ چهارچوب قوانین بین‌المللی سایبری را به چالش می‌کشد (Abu Alead & AMHMED AB ALTALIBE, 2023M Salem) . برای مقابله با این معضلات، آمریکا می‌تواند اقدامات متعددی انجام دهد. اول، باید برای ارتقای گفت‌وگو و همکاری با سایر کشورها، افزایش درک مشترک از اهمیت هنجارهای سایبری و مزایای آن، در مسائل مهم دیپلماتیک شرکت کند. دوم، آمریکا می‌تواند برای کمک به کشورهای درحال‌توسعه در تقویت دفاع سایبری و پیروی از هنجارهای بین‌المللی، از طرح‌های ظرفیت‌سازی حمایت کند. سوم، آمریکا باید در جهت افزایش همکاری بین‌المللی و مکانیسم‌های اشتراک اطلاعات برای بهبود قابلیت‌های اسناد و تسهیل اجرای مؤثرتر هنجارهای سایبری گام بردارد.

آمریکا با چالش‌هایی در شکل‌گیری و اجرای هنجارهای سایبری در قوانین بین‌المللی سایبری مواجه است. فرسایش اعتماد و اعتبار، تغییر سیاست‌ها و درک جهانی و چالش در شکل‌گیری و اجرای هنجارها، همگی به کاهش نفوذ آمریکا در این حوزه می‌انجامد. غلبه بر این چالش‌ها مستلزم تلاش‌های هماهنگ برای ایجاد اجماع، ترویج گفت‌وگو و تقویت همکاری‌های بین‌المللی است. با پرداختن به این مسائل، آمریکا می‌تواند نقشی حیاتی در شکل‌دهی آینده حکمرانی سایبری جهانی و تضمین فضای سایبری امن و پایدار برای همه ایفا کند.

۳. عوامل ظهور چین به‌عنوان یک کنشگر مؤثر در عرصه حقوق بین‌الملل سایبر

ظهور چین به‌عنوان یک قدرت جهانی پیامدهای گسترده‌ای در حوزه‌های مختلف ازجمله حوزه فضای مجازی داشته است. در سال‌های اخیر، چین به‌عنوان یک بازیگر

مهم درزمینهٔ حقوق بین‌الملل سایبری ظاهر شده است و سلطه سنتی آمریکا را به چالش می‌کشد (Segal, 2020). با قدرت و نفوذ رو به رشد چین که تأثیری دگرگون‌کننده بر قوانین، هنجارها و پویایی‌های استراتژیک در فضای سایبری دارد؛ این تغییر در پویایی اساساً چشم‌انداز حاکمیت سایبری جهانی را تغییر داده است. در این بخش، عوامل کلیدی افزایش قدرت چین در حوزه حقوق بین‌الملل سایبری، ازجمله قابلیت‌های رو به رشد سایبری، قاطعیت دیپلماتیک و رویکردهای جایگزین برای حکمرانی سایبری را بررسی خواهیم کرد. با بررسی این عوامل، می‌توانیم بینش‌های ارزشمندی در مورد پویایی‌های در حال تغییر حاکمیت سایبری جهانی و پیامدهای آن برای موقعیت و نقش آمریکا در این چشم‌انداز در حال تحول به دست آوریم.

۳-۱. قابلیت‌های سایبری رو به رشد چین

یکی از عوامل مهمی که روند تدوین قوانین بین‌المللی سایبری را تغییر می‌دهد، رشد سریع قابلیت‌های سایبری چین است. چین با سرمایه‌گذاری‌های کلان در زیرساخت‌های امنیت سایبری، تحقیق، توسعه و قابلیت‌های سایبری تهاجمی تبدیل به یک بازیگر بزرگ جهانی در حوزه سایبری شده است. قابلیت‌های سایبری رو به ازدیاد چین، این کشور را قادر ساخته تا نفوذ و قدرت خود در حوزه سایبری را نشان داده و سلطه دیرینه آمریکا را به چالش بکشد.

قابلیت‌های سایبری چین در طیف گسترده‌ای از حوزه‌ها، ازجمله جاسوسی سایبری، عملیات سایبری تهاجمی و توسعه فناوری‌های پیشرفته است (زاهدی‌خطیر و صالحی،۱۴۰۱، ص. ۱۵۵). این کشور به خاطر کمپین‌های جاسوسی سایبری گسترده خود که نهادهای دولتی، صنایع دفاعی، مالکیت معنوی و شرکت‌های تجاری را هدف قرار می‌دهد، شناخته شده است (Fedoniuk & Maghdysiuk, 2022). این فعالیت‌ها چین را قادر ساخته است که اطلاعات و فناوری‌های ارزشمندی به دست آورده و به پیشرفت‌های فناورانه و اهداف استراتژیک خود، کمک شایانی کرده است.

علاوه بر این، قابلیت‌های سایبری تهاجمی چین شدیداً پیچیده شده است و این کشور قادر است عملیات سایبری مخرب مانند حملات مخرب به زیرساخت‌های حیاتی و بهره‌برداری از نقاط آسیب‌پذیری در شبکه‌های خارجی برای اهداف استراتژیک و اطلاعاتی را انجام دهد(Jinghua, 2019) . قابلیت‌های رو به رشد سایبری چین موقعیت این کشور را به‌عنوان یک بازیگر قدرتمند در عرصه سایبری جهانی

تقویت نموده و سلطه دیرینه آمریکا را به چالش می‌کشد و نگرانی‌هایی در میان سایر کشورها در خصوص نیات و فعالیت‌های چین برمی‌انگیزد.

۳-۲. قاطعیت دیپلماتیک و تعامل استراتژیک

چین در پیشبرد منافع خود در حوزه سایبری رویکرد دیپلماتیک قاطعانه‌تری را اتخاذ کرده است(Sullivan & Wang, 2022) . این کشور در بحث‌ها و مذاکرات دوجانبه و چندجانبه شرکت داشته و به دنبال شکل‌دهی به چهارچوب‌های جهانی حکمرانی سایبری است تا با ترجیحات و منافع ملی خود هماهنگ باشد. تلاش‌های دیپلماتیک چین به دلیل تمایل این کشور برای افزایش نفوذ خود در قوانین و حکمرانی سایبری بین‌المللی و به چالش‌کشیدن هنجارها و قوانین موجود که تحت رهبری آمریکا هستند، انجام شده است.

هدف چین از تعامل استراتژیک با سایر کشورها، ایجاد اتحاد و مشارکت، به‌ویژه با اقتصادهای نوظهور، برای جلب حمایت از رویکردهای جایگزین خود برای حکمرانی سایبری است. چین مفهوم «قدرت سایبری»[1] را به تعالی رسانده و از یک مدل دولت‌محور همراه با کنترل ملی و تنظیم فضای سایبری، حمایت می‌کند (Hong & Goodnight, 2019) این رویکرد در تضاد با تأکید آمریکا بر فضای سایبری باز و آزاد است که توسط قوانین و هنجارهای مشترک اداره می‌شود.

قاطعیت دیپلماتیک و تعامل استراتژیک چین منجر به ایجاد طرح‌ها و انجمن‌های مدیریت سایبری جایگزین شده است که خارج از چهارچوب سنتی آمریکایی عمل می‌کنند. به‌عنوان‌مثال، چین نقش مهمی در ایجاد مکانیسم امنیت سایبری «سازمان همکاری شانگهای»[2] ایفا کرده است که هدف آن افزایش اشتراک و هماهنگی اطلاعات بین کشورهای عضو است. این ابتکارات جایگزین، نفوذ آمریکا را به چالش می‌کشد و به‌طور بالقوه موجب تکه‌تکه شدن حکمرانی سایبری جهانی می‌شود.

۳-۳. هنجارسازی و رویکردهای حکمرانی سایبری جایگزین

چین در حوزه حکمرانی سایبری کارآفرینی هنجاری نشان داده و فعالانه هنجارها و قوانین جایگزینی را ترویج کرده و به آن‌ها شکل می‌دهد تا با منافع خود همسو

1. cyber sovereignty
2. Shanghai Cooperation Organization (SCO)

باشند. رویکرد چین نسبت به حکمرانی سایبری حول مفهوم قدرت سایبری متمرکز است، مفهومی که بر کنترل دولتی و تنظیم فضای سایبری در محدوده قلمروی آن‌ها تأکید دارد (Gao, 2022). این مفهوم با رویکرد رهبری آمریکا که بر فضای سایبری باز و جهانی که بر اساس هنجارها و اصول مشترک اداره می‌شود، در تضاد است.

چین در حمایت از هنجارهایی که امنیت و حکمرانی دولت را بر حقوق و آزادی‌های فردی اولویت می‌دهند، تأثیرگذار بوده است. به‌عنوان‌مثال، چین مدافع هنجارهای مربوط به بومی‌سازی داده‌ها است و شرکت‌ها را ملزم می‌کند که داده‌ها را در داخل مرزهای خود ذخیره کنند تا به‌عنوان ابزاری برای ارتقای امنیت ملی و اعمال کنترل بر جریان اطلاعات از آن‌ها استفاده کند. چین مدافع هنجارهایی است که برخی از فعالیت‌های سایبری را محدود می‌کند. ازجمله این هنجارها می‌توان به مواردی چون استفاده از سلاح‌های سایبری و عملیات تهاجمی، به‌منظور ارتقای ثبات و جلوگیری از تشدید تنش‌ها در فضای سایبری اشاره کرد.

چین با ترویج رویکردها و هنجارهای حکمرانی سایبری جایگزین، به دنبال تغییر گفتمان بین‌المللی در مورد قوانین سایبری و تأثیرگذاری بر توسعه هنجارهای جهانی متناسب با منافع خود است. این امر به تکه‌تکه شدن چشم‌انداز حکمرانی سایبری جهانی خواهد انجامید، به‌طوری‌که کشورهای مختلف بر اساس متحدان و ترجیحات خود، رویکردهای متفاوتی را برای حکمرانی سایبری اتخاذ می‌کنند (Hoffmann, Lazanski, & Taylor, 2020). این تکه‌تکه شدن برای آمریکا معضلاتی ایجاد می‌کند، زیرا نفوذ چهارچوب مورد نظر آمریکا را کاهش داده و تلاش برای ایجاد هنجارهای منسجم و پذیرفته‌شده جهانی در حقوق بین‌المللی سایبری را پیچیده می‌کند.

همچنین رویکردهای حکمرانی سایبری جایگزین چین، در میان برخی از کشورها به‌ویژه کشورهایی که به دنبال اثبات قدرت خود و به چالش‌کشیدن سلطه قدرت‌های غربی هستند، مورد توجه قرار گرفته است. این کشورها تأکید چین بر قدرت سایبری را رویکردی جذاب‌تر و عادلانه‌تر و همسو با منافع ملی خودشان می‌دانند. درنتیجه، تمایل بیشتری به حمایت و اتخاذ هنجارها و مدل‌های حکمرانی چین دارند و می‌خواهند نفوذ آمریکا در شکل‌دهی به حکمرانی سایبری جهانی را از بین ببرند.

افزایش قدرت چین و رویکردهای جایگزین حاکمیت سایبری آن پیامدهایی برای آینده قوانین سایبری بین‌المللی دارد. در چنین شرایطی آمریکا تلاش دارد این پویایی‌های در حال تغییر را هدایت کند و استراتژی‌ها و سیاست‌های خود را

به‌گونه‌ای تطبیق دهد که در چشم‌انداز سایبری در حال تحول، تأثیرگذار باقی بماند. لذا ایالات‌متحده برای مقابله با این چالش سعی دارد در امور دیپلماتیک برای ایجاد ائتلاف‌ها و مشارکت‌های مختلف شرکت کند، دیدگاه خود در مورد فضای سایبری باز و مبتنی بر قوانین را ارتقا دهد و درعین‌حال به نگرانی‌ها و دیدگاه‌های یک‌جانبه‌گرایانه رسیدگی کند. علاوه بر این، آمریکا می‌تواند از تخصص و نوآوری فناورانه خود برای توسعه زیرساخت‌های سایبری قوی و ایمن استفاده کند و از این طریق اعتبار خود را در حوزه سایبری افزایش دهد. این کار شامل سرمایه‌گذاری در تحقیق و توسعه، افزایش مشارکت‌های عمومی و خصوصی و ترویج همکاری‌های بین‌المللی در حوزه‌هایی چون اشتراک‌گذاری اطلاعات، ظرفیت‌سازی و واکنش به حوادث سایبری است (Runde & Ramanujam, 2022).

آمریکا همچنین این امکان را دارد که به دفاع از هنجارها و قوانین بین‌المللی مروج رفتار مسئولانه دولت‌ها در فضای سایبری ادامه دهد(Schulte & Schaffer, 2012) . دولت این کشور برای پیشبرد برنامه امنیت سایبری خود و جمع‌بندی موضوعات کلیدی، سعی دارد در مجامع چندجانبه‌ای چون سازمان ملل متحد و سازمان‌های منطقه‌ای شرکت کند. آمریکا با مشارکت فعال در این بحث‌ها این امکان را دارد که گفتمان مؤثری را شکل داده و بر توسعه هنجارهای جهانی همسو با ارزش‌ها و منافع خود، تأثیر بگذارد (Joint Statement on the United States-European Union 9th Cyber Dialogue in Brussels - United States Department of State, 2023). درنتیجه، افزایش قدرت چین در حوزه سایبری، همراه با قابلیت‌های رو به رشد سایبری این کشور، قاطعیت دیپلماتیک چین و رویکردهای حکمرانی سایبری جایگزین، به تغییر حرکت در مسیر قوانین بین‌المللی سایبری کمک کرده است. آمریکا با معضل حفظ نفوذ و نقش رهبری خود در مواجهه با ظهور چین مواجه شده است. از همین روی، این کشور سعی بر آن دارد که استراتژی‌های خود را تطبیق داده و در دیپلماسی فعال، نوآوری‌های فناورانه و حمایت از هنجارها مشارکت کند تا آینده حکمرانی سایبری جهانی را به‌گونه‌ای شکل دهد که از منافع خود حمایت کند.

۴. پیامدهای ظهور چین برای ژئوپلیتیک سایبری جهانی

چشم‌انداز حقوق بین‌الملل سایبری با کاهش نفوذ ایالات‌متحده و ظهور قدرت چین، شاهد تغییرات ژئوپلیتیک قابل‌توجهی بوده است. این تغییرات پیامدهای عمیقی برای حکمرانی سایبری جهانی دارد و بررسی دقیق چالش‌ها و فرصت‌های موجود را

ضروری می‌کند. در این بخش، پیامدهای حکمرانی سایبری جهانی درزمینهٔ تغییر قدرت و همسویی ژئوپلیتیک، با تمرکز بر سه جنبه اصلی بررسی می‌شود:

۱. تغییر قدرت و بازتنظیم ژئوپلیتیک: این تغییر منجر به ظهور قدرت‌های جدیدی در فضای سایبری شده است که منافع و دیدگاه‌های متفاوتی نسبت به ایالات‌متحده دارند. این امر می‌تواند منجر به افزایش رقابت و تنش در فضای سایبری شود.

۲. چالش‌ها و فرصت‌ها برای همکاری بین‌المللی: کاهش نفوذ ایالات‌متحده، همکاری بین‌المللی مدنظر این کشور درزمینهٔ حکمرانی سایبری را با چالش‌هایی مواجه کرده است. بااین‌حال، این تغییرات همچنین فرصت‌هایی را برای ایجاد ترتیبات همکاری جدید و مبتنی بر مشارکت فراهم می‌کند.

۳. برقراری تعادل بین منافع ملی و امنیت سایبری جهانی: تغییر قدرت و شرایط ژئوپلیتیک، چالش‌های جدیدی را برای برقراری تعادل بین منافع ملی و امنیت سایبری جهانی ایجاد کرده است. در چنین وضعیتی، دولت‌ها باید به دنبال راه‌هایی برای حمایت از منافع ملی خود در فضای سایبر باشند، بدون اینکه امنیت سایبری جهانی را به خطر بیندازند.

۴-۱. تغییر قدرت و تنظیم مجدد ژئوپلیتیک سایبری

جابه‌جایی قدرت و تنظیم مجدد جغرافیای سیاسی در حوزه حقوق بین‌الملل سایبری، با کاهش نفوذ آمریکا و ظهور چین، پیامدهای مهمی بر حکمرانی سایبری جهانی دارد. تغییر در توزیع قدرت، نفوذ و فرایندهای تصمیم‌گیری در فضای مجازی را شکل می‌دهد. پیامدهای زیر را می‌توان شناسایی کرد:

الف) چشم‌انداز سایبری چندقطبی: تغییر قدرت نشان‌دهنده ظهور یک چشم‌انداز سایبری چندقطبی با بازیگران مختلف برای اعمال‌نفوذ و شکل‌دادن به هنجارها و سیاست‌های سایبری است. آمریکا و چین، همراه با دیگر قدرت‌های بزرگ سایبری، نقش‌های مهمی در تعیین دستور کار و تعیین مسیر آینده حکمرانی سایبری جهان دارند (Savaş & Karataş, 2022).

ب) رقابت برای تنظیم هنجارها: تغییر قدرت یک محیط رقابتی برای تنظیم هنجارها در فضای مجازی ایجاد می‌کند. آمریکا و چین، به همراه دیگر بازیگران تأثیرگذار، به دنبال افزایش منافع و ارزش‌های خود از طریق ایجاد هنجارها و قوانین هستند. این رقابت ممکن است منجر به رویکردهای متفاوت و پراکندگی هنجارهای

سایبری شود و دستیابی به یک چهارچوب یکپارچه و منسجم جهانی سایبری را با چالش مواجه کند (Zinovieva, 2022).

ج) اتحادها و مشارکت‌های جدید: تغییر قدرت ممکن است باعث ایجاد اتحادها و مشارکت‌های جدید بین دولت‌ها با منافع و اهداف مشترک شود. در چنین شرایطی ممکن است کشورها به دنبال همکاری بیشتر با کشورهای همفکر باشند و از این طریق به پیشبرد برنامه‌های سایبری خود و تقویت موقعیت خود در عرصه حکمرانی سایبری جهانی بپردازند. این اتحادها می‌توانند تغییر در همکاری‌های بین‌المللی را سبب شوند و بر توسعه هنجارها و شیوه‌های سایبری اثر بگذارند (Pijovic, 2021).

۴-۲. چالش‌ها و فرصت‌های همکاری بین‌المللی

تغییر قدرت در حقوق بین‌الملل سایبری چالش‌ها و فرصت‌هایی را برای همکاری بین‌المللی فراهم می‌کند. در این زمینه مفاهیم زیر به وجود می‌آیند:

الف) اطمینان و اعتمادسازی: کاهش قدرت آمریکا و ظهور چین چالش‌هایی را در ایجاد اعتماد و اطمینان در بین دولت‌ها ایجاد می‌کند. اعتماد برای همکاری مؤثر در فضای سایبری، به‌ویژه در حوزه‌هایی چون اشتراک‌گذاری اطلاعات، واکنش به حوادث و ظرفیت‌سازی بسیار مهم است. با عنایت به این مفروضات، تلاش برای ایجاد اعتماد و افزایش شفافیت بین دولت‌ها برای غلبه بر فقدان اعتماد و تقویت همکاری معنادار ضروری است.

ب) پُل‌زدن بر شکاف‌ها و غلبه بر تفاوت‌ها: تغییر قدرت می‌تواند به تفاوت در هنجارها، شیوه‌ها و سیاست‌های سایبری بین دولت‌ها منجر شود. در این هنگام پُل‌زدن بر این شکاف‌ها و یافتن زمینه‌های مشترک برای همکاری بین‌المللی حیاتی می‌شود. از همین‌رو گفت‌وگو، مذاکره و سازش برای تطبیق‌دادن منافع متفاوت و تقویت همگرایی در حکمرانی سایبری جهانی ضروری است.

ج) مکانیسم‌های همکاری افزایشی: تغییر قدرت فرصت‌هایی برای توسعه مکانیسم‌های همکاری افزایشی فراهم می‌کند. مجامع کنونی، مانند سازمان ملل متحد، سازمان‌های منطقه‌ای و مشارکت‌های سازمان‌های عمومی-خصوصی، می‌توانند منجر به تسهیل گفت‌وگو، اشتراک‌گذاری اطلاعات و ابتکارات ظرفیت‌سازی شود. همچنین باید در نظر داشت که برای ارتقای همکاری بین دولت‌ها و ذینفعان در رسیدگی به چالش‌های سایبری نوظهور می‌توان از پلتفرم‌ها و ابتکارات جدید استفاده کرد.

۴-۳. ایجاد تعادل بین منافع ملی و امنیت سایبری جهانی

تغییر قدرت در قوانین بین‌المللی سایبری پرسش‌هایی را در مورد برقراری تعادل بین منافع ملی و امنیت سایبری جهانی ایجاد می‌کند. با عنایت به این مسئله، می‌توان به مفاهیم زیر اشاره کرد:

- حاکمیت ملی و حکمرانی سایبری: دولت‌ها ممکن است در شکل‌دادن به سیاست‌ها و مقررات حکمرانی سایبری، منافع ملی خود را در اولویت قرار دهند. تغییر قدرت می‌تواند این روند را تقویت کند، زیرا کشورها به دنبال اعمال حاکمیت خود و محافظت از منافع امنیت سایبری داخلی خود هستند. برقراری تعادل بین حاکمیت ملی و همکاری جهانی یک چالش کلیدی می‌شود، زیرا مستلزم یافتن زمینه‌های مشترک و هماهنگ‌کردن رویکردهای متفاوت است(Liaropoulos, 2017) .
- حقوق بشر و امنیت سایبری: تغییر قدرت بر تعادل ظریفی که بین امنیت سایبری و حقوق بشر برقرار است نیز تأثیر می‌گذارد. کشورهای مختلف ممکن است از رابطه بین این دو مفهوم تفسیرهای متفاوتی داشته باشند که منجر به درگیری‌های بالقوه می‌گردد. اطمینان از این‌که اقدامات امنیت سایبری به اصول حقوق بشر احترام گذاشته و حافظ آن‌ها است، در حکمرانی سایبری جهانی بسیار حائز اهمیت است (Allahrakha, 2023).
- مسئولیت مشترک و تقسیم بار: تغییر قدرت مستلزم مسئولیت مشترک و تقسیم بار میان دولت‌ها در رسیدگی به چالش‌های سایبری جهانی است. تهدیدها و آسیب‌پذیری‌های امنیت سایبری ماهیت فراملی دارند و به اقدامات مشترکی جهت کاهش خطرات و افزایش انعطاف‌پذیری نیاز دارند. کشورها باید از پیوستگی فضای سایبری آگاه باشند و برای راه‌حل‌های جمعی که امنیت سایبری جهانی را بر منافع محدود ملی ترجیح می‌دهد تلاش کنند (Carr, 2016).
- رهبری هنجاری: تغییر قدرت فرصتی برای کشورها فراهم می‌کند تا رهبری هنجاری خود را در حکمرانی سایبری جهانی نشان دهند. کشورهایی که از رویکردهای فراگیر، شفاف و مبتنی بر قوانین در فضای سایبری حمایت می‌کنند، می‌توانند در شکل‌دادن به هنجارها و روش‌های بین‌المللی نقش مهمی ایفا کنند. این کشورها با ترویج رفتار مسئولانه دولت، حمایت از حقوق

بشر و تقویت همکاری‌ها می‌توانند به ایجاد فضای سایبری ایمن و باثبات‌تر کمک کنند.

- ظرفیت‌سازی و کمک: تغییر قدرت مستلزم افزایش تلاش‌ها و کمک به ظرفیت‌سازی در کشورهایی است که ممکن است منابع یا تخصص کمی در مقابله با تهدیدات سایبری داشته باشند. همکاری بین قدرت‌های سایبری پیشرفته و کشورهای درحال‌توسعه می‌تواند به رفع شکاف ظرفیتی و ارتقای یک اکوسیستم سایبری جهانی فراگیرتر و انعطاف‌پذیرتر بینجامد (Goldsmith, & Creese, 2018 ,Hameed ,Agrafiotis, Weisser,).

درنهایت، تغییر قدرت و همسویی دوباره جغرافیای سیاسی در حقوق بین‌الملل سایبری پیامدهای مهمی برای حکمرانی سایبری جهانی دارد. در این چشم‌انداز در حال تغییر، چالش‌ها و فرصت‌ها به تلاش‌های هماهنگ برای ایجاد اعتماد، تقویت همکاری‌های بین‌المللی و برقراری تعادل بین منافع ملی با هدف پیشبرد امنیت سایبری جهانی نیاز دارند. هنگام وقوع این تغییرات جامعه بین‌المللی با تعهد به مسئولیت مشترک و همکاری، می‌تواند به سمت یک فضای سایبری امن، باثبات و فراگیر که در خدمت منافع همه کشورها است، تلاش کند.

۵. چالش‌های تداوم هژمونی سایبری ایالات‌متحده

آمریکا علی‌رغم غلبه اولیه خود، با چالش‌های متعددی برای رهبری خود در حوزه قوانین بین‌المللی سایبری روبرو بوده است. یکی از چالش‌های اصلی، از بین رفتن اعتماد و اعتبار به دلیل افشای برنامه‌های نظارتی گسترده این کشور بوده است. افشاگری‌های اسنودن، فعالیت‌های اطلاعاتی ایالات‌متحده را فاش کرد (Bowden, 2013) و موجب نگرانی سایر کشورها در مورد حریم خصوصی، حفاظت از داده‌ها و احترام به حاکمیت در فضای سایبری و از بین رفتن اعتماد سایر کشورها به ایالات‌متحده به‌عنوان رهبر حوزه حکمرانی سایبری شد.

علاوه بر این، تغییر در سیاست‌های ایالات‌متحده نسبت به فضای سایبری در دولت ترامپ بر موقعیت رهبری این کشور تأثیر داشت. رویکرد «اول آمریکا» که بر امنیت ملی و اقدامات حفاظتی تأکید داشت، نشان‌دهنده موضع درون‌گراتر آمریکا در مورد امنیت سایبری بود. این تغییر، همراه با یک‌جانبه‌گرایی در استفاده از قابلیت‌های تهاجمی سایبری، منجر به بدبینی و مقاومت سایر کشورها شد. خروج ایالات‌متحده از توافقات بین‌المللی مانند توافق پاریس و توافق هسته‌ای ایران نیز

نگرانی‌هایی را در مورد تعهد این کشور به همکاری جهانی درزمینهٔ مسائل سایبری برانگیخت (Ettinger, 2018).

علاوه بر تغییر سیاست‌ها، ماهیت غیرمتمرکز و در حال تحول فضای سایبری معضلاتی را برای رهبری آمریکا ایجاد کرده است. فقدان یک مرجع حکمرانی متمرکز و مشکل در نسبت‌دادن حملات سایبری به عوامل خاص، مانع از تلاش برای ایجاد هنجارها و مقررات پذیرفته‌شده جهانی شده است. کار هنجارسازی در حقوق بین‌الملل سایبری به دلیل اختلاف نظر بین دولت‌ها در مورد تفسیر و اجرای هنجارهای موجود پیچیده‌تر شده است.

درحالی‌که آمریکا با معضلات متعددی در حوزه تداوم رهبری حکمرانی سایبری جهان روبرو است، چین به‌عنوان یک بازیگر مهم در فرایند تدوین قوانین بین‌المللی سایبری ظاهر شده است. رشد سریع اقتصادی، پیشرفت‌های فناورانه و گسترش توانمندی‌های سایبری چین، این کشور را به نقش‌آفرینی درصحنه جهانی سوق داده است. چین به دلیل برخورداری از جمعیت زیاد، اقتصاد دیجیتال رو به رشد و زیرساخت سایبری قوی، به نیروی مهمی در فضای سایبری تبدیل شده است.

رویکرد چین در خصوص حکمرانی سایبری با رویکرد ایالات‌متحده متفاوت است. رویکرد چین بر کنترل دولت، امنیت سایبری و حفاظت از قدرت ملی تأکید دارد. چین از یک مدل دولت‌محورتر از حکمرانی سایبری حمایت می‌کند، که در آن دولت در تنظیم و نظارت بر فعالیت‌های فضای سایبری نقش اصلی را ایفا می‌کند (Creemers, China's emerging data protection framework, 2022). این رویکرد با اصول سیاسی و ایدئولوژیکی گسترده چین بر ثبات، نظم اجتماعی و کنترل بر جریان اطلاعات همسویی دارد.

چین، فعالانه به دنبال افزایش قابلیت‌ها و نفوذ سایبری خود در قوانین بین‌المللی سایبری بوده است. این کشور در توسعه فناوری‌های پیشرفته مانند هوش مصنوعی، محاسبات کوانتومی و شبکه‌های 5G سرمایه‌گذاری کرده است که پیامدهای مهمی برای آینده فضای سایبری دارد. توانمندی‌های رو به رشد سایبری چین، همراه با دیپلماسی قاطعانه و نفوذ اقتصادی این کشور، چین را قادر ساخته تا هنجارهای حکمرانی سایبری جهانی را بر اساس منافع و اولویت‌های خود شکل دهد (Attatfa, Renaud, & Paoli, 2020).

چین، مدافع مفهوم «حکمرانی سایبری» است و ادعا می‌کند دولت‌ها حق دارند فضای سایبری خود را بر اساس قوانین و مقررات داخلی خود مدیریت و اداره کنند.

این رویکرد، مفهوم اینترنت باز و به‌هم‌پیوسته که مورد حمایت ایالات‌متحده و سایر کشورهای همفکر او است را به چالش می‌کشد. مشارکت فعال چین در بحث‌های سایبری بین‌المللی، تعامل با سازمان‌های منطقه‌ای و ایجاد موافقت‌نامه‌های دوجانبه، موقعیت این کشور را به‌عنوان یک بازیگر اصلی در شکل‌دهی آینده حقوق بین‌المللی سایبری تثبیت کرده است.

ظهور چین به‌عنوان یک قدرت سایبری، چالشی مستقیم برای رهبری آمریکا در قوانین بین‌المللی سایبری ایجاد کرده است. با این‌که آمریکا همچنان از قابلیت‌های سایبری پیشرفته‌ای برخوردار است، نفوذ چین و رویکرد جایگزین آن برای حکمرانی سایبری، توازن قدرت را در این زمینه تغییر داده است. این تغییر قدرت پیامدهای مهمی برای هنجارهای سایبری جهانی، آینده اینترنت و چشم‌انداز ژئوپلیتیکی دارد.

۶. پیامدهای تغییر قدرت

۶-۱. تغییر پارادایم ژئوپلیتیک سایبری

تغییر قدرت از آمریکا به چین در قوانین بین‌المللی سایبری پیامدهای ژئوپلیتیکی بسیاری دارد. فضای مجازی با رقابت ژئوپلیتیک درهم‌آمیخته شده است، زیرا دولت‌ها اهمیت استراتژیک کنترل و تأثیرگذاری بر حوزه دیجیتال را دریافته‌اند. کاهش قدرت آمریکا و ظهور چین، حوزه قدرت جدیدی را در حکمرانی سایبری جهانی معرفی می‌کند که سلطه دیرینه ایالات‌متحده را به چالش می‌کشد.

این تغییر قدرت، پتانسیل تغییر شکل و اتحادهای ژئوپلیتیکی را دارد. کشورها ممکن است روابط و همسویی‌های خود را بر اساس منافع و مزایای خود در چشم‌انداز سایبری در حال تغییر، مجدداً ارزیابی کنند. برخی کشورها ممکن است به همسویی با چین گرایش داشته باشند و به دلیل نفوذ اقتصادی و توانایی‌های تکنولوژیک آن جذب چین شده باشند، اما برخی دیگر ممکن است به دنبال حفظ روابط با ایالات‌متحده و تکیه بر اتحادهای تاریخی و ارزش‌های مشترک باشند. این تغییر قدرت پرسش‌هایی را در مورد تقسیم احتمالی فضای سایبری به حوزه‌های مختلف نفوذ ایجاد می‌کند. ازآنجایی‌که آمریکا و چین برای تسلط سایبری با یکدیگر رقابت می‌کنند، دولت‌ها ممکن است مجبور شوند طرف‌هایی را انتخاب کرده و سیاست‌های سایبری خود را بر این اساس هماهنگ کنند. این امر می‌تواند منجر به ظهور هنجارها، استانداردها و مقررات جداگانه شود و به‌طور بالقوه منجر به تقسیم فضای سایبری و اینترنت پراکنده جهانی گردد.

۶-۲. پیامدهای اقتصادی و فناوری

کاهش قدرت آمریکا در قوانین بین‌المللی سایبری پیامدهای اقتصادی و فناورانه دارد. آمریکا در خط مقدم نوآوری‌های فناورانه، توسعه فناوری‌های پیشرفته، تقویت اکوسیستم‌های نوآوری و جذب سرمایه‌گذاری‌های جهانی بوده است. تأثیر آمریکا در شکل‌دهی به هنجارهای سایبری، به ایجاد استانداردها و شیوه‌هایی کمک کرده است که قابلیت همکاری بین‌المللی را افزایش می‌دهد.

با ظهور چین به‌عنوان یک قدرت سایبری، شاهد واگرایی بالقوه در استانداردهای تکنولوژیک و چهارچوب‌های نظارتی هستیم. رویکرد چین در خصوص حکمرانی سایبری، که با کنترل دولتی و حمایت‌گرایی همراه است، ممکن است به توسعه اکوسیستم‌ها و استانداردهای فناوری جایگزین منجر شود. این واگرایی می‌تواند به شکل‌گیری یک اقتصاد دیجیتال پراکنده منجر شود، اقتصادی که در مناطق مختلف، قوانین و شیوه‌های مختلفی برای خود دارند و مانع از قابلیت همکاری و رشد اقتصادی جهانی می‌شوند (Can the Digital Economy Survive in a Splinternet, n.d.).

اقتصاد دیجیتال در حال گسترش چین که توسط بازار مصرف‌کننده گسترده و شرکت‌های نوآور این کشور هدایت می‌شود، فرصت‌ها و چالش‌های جدیدی را برای تجارت و سرمایه‌گذاری جهانی ارائه می‌دهد. ازآنجاکه چین در حال تقویت موقعیت خود در فضای سایبری است، ممکن است به دنبال اعمال‌نفوذ اقتصادی و ترویج پروژه‌های زیرساخت دیجیتال خود، مانند «ابتکار کمربند و جاده»[1]، برای گسترش اثر فناورانه خود و شکل دادن به قوانین اقتصاد دیجیتال باشد.

۶-۳. حقوق بشر و آزادی بیان

تغییر قدرت در قوانین بین‌المللی سایبری پیامدهایی برای حقوق بشر و آزادی بیان دارد. آمریکا همواره مدعی است که مدافع سرسخت برای اینترنت آزاد و باز بوده است و برای حفظ حقوق فردی، حریم خصوصی و حاکمیت قانون به‌صورت آنلاین اهمیت قائل است. کاهش قدرت ایالات‌متحده و ظهور چین، با تأکید این کشور بر کنترل و نظارت دولتی، ممکن است به تغییر تعادل بین امنیت و حقوق بشر در فضای سایبری منجر شود.

1. Belt and Road Initiative

کشورهایی که با رویکرد چین در مورد حکمرانی سایبری همسو هستند، ممکن است تدابیر سخت‌گیرانه‌تری را برای تنظیم و کنترل فضای سایبری اتخاذ کنند که به‌طور بالقوه منجر به محدودیت‌های بیشتر در آزادی بیان، حریم خصوصی و دسترسی به اطلاعات می‌شود. قابلیت‌های نظارتی پیشرفته چین و استفاده از فناوری برای کنترل اجتماعی، نگرانی‌هایی را در مورد کاهش بالقوه حقوق بشر و تأثیر مخرب آن بر جامعه مدنی در عصر دیجیتال ایجاد می‌کند(Piper, n.d.) . این تغییر قدرت پیامدهایی برای بحث در مورد حکمرانی اینترنت و نقش دولت‌ها در شکل‌دادن به فضای سایبری نیز دارد. آمریکا و چین در مورد مسائلی چون حکمرانی اینترنت، تنظیم محتوا و حریم خصوصی داده‌ها دیدگاه‌های متفاوتی دارند. برخورد این دیدگاه‌ها ممکن است منجر به دیدگاه‌های رقابتی فضای مجازی شود و پیامدهای بالقوه‌ای برای آینده حکمرانی اینترنت و حمایت از حقوق بشر در قلمرو دیجیتال داشته باشد.

۷. چشم‌اندازها و چالش‌های آینده

چشم‌انداز در حال تغییر حقوق بین‌الملل سایبری چالش‌ها و فرصت‌هایی را برای جامعه بین‌المللی ایجاد می‌کند. با تغییر قدرت، دولت‌ها، سازمان‌ها و ذینفعان دیگر باید در این چشم‌انداز به‌طور مؤثر حرکت کنند و با واقعیت‌های در حال تغییر فضای سایبری سازگار شوند. دیدگاه‌ها و استراتژی‌های زیر می‌توانند به شکل‌دهی آینده حکمرانی سایبری جهانی کمک کنن؛

۷-۱. تعامل و همکاری چندجانبه

هنگام تغییر قدرت، تعامل و همکاری چندجانبه اهمیت زیادی دارد. دولت‌ها و سازمان‌های بین‌المللی باید برای ایجاد زمینه‌ها و هنجارهای مشترک گفت‌وگو و همکاری را تقویت کنند. ابتکارات چندجانبه، مانند گروه کارشناسان دولتی سازمان ملل متحد و انجمن‌های منطقه‌ای، می‌توانند بسترهایی برای گفت‌وگو، اعتمادسازی و توسعه اجماع در مورد مسائل حیاتی سایبری باشند.

۷-۲. تقویت مشارکت‌ها میان بخش دولتی و خصوصی

مشارکت بخش دولتی و خصوصی نقش مهمی در مقابله با تهدیدات سایبری و پیشبرد هنجارهای سایبری دارد.

همکاری بین دولت‌ها، شرکت‌های فناوری، جامعه مدنی و دانشگاه‌ها می‌تواند به توسعه راه‌حل‌های نوآورانه، ابتکارات ظرفیت‌سازی و ارتقای رفتار مسئولانه دولت کمک کند. همکاری نزدیک بین ذینفعان می‌تواند به رفع شکاف‌ها، اشتراک‌گذاری بهترین روش‌ها و افزایش انعطاف‌پذیری سایبری در مقیاس جهانی کمک کند (Lostri, Lewis, & Wood, 2022).

۷-۳. ترویج رویکردهای فراگیر و مشارکتی

فراگیر و مشارکتی‌بودن، در شکل‌دادن به قوانین بین‌المللی سایبری ضروری است. دیدگاه‌های همه ذینفعان، ازجمله عوامل غیردولتی، جوامع اقلیتی و کشورهای درحال‌توسعه باید شنیده‌شده و مورد توجه قرارگیرد. این کار تضمین می‌کند که هنجارها و سیاست‌های سایبری عادلانه بوده و منعکس‌کننده منافع گوناگون هستند و به نگرانی‌ها و نیازهای بازیگران مختلف در جامعه جهانی می‌پردازند.

نتیجه‌گیری

مقاله حاضر به بررسی جامع تحولات اخیر در حوزه حقوق بین‌الملل سایبری پرداخت. تجزیه‌وتحلیل یافته‌های این پژوهش نشان می‌دهد که طی سال‌های اخیر شاهد تغییر بنیادینی در موازنه قدرت و ساختار حاکم بر نظام حقوق بین‌الملل سایبری بوده‌ایم. به‌طوری‌که شاهد افول نسبی جایگاه ایالات‌متحده به‌عنوان یک ابرقدرت سایبری و هم‌زمان با آن صعود فزاینده قدرت چین در این عرصه هستیم. یافته‌های پژوهش حاکی از آن است که عوامل متعددی همچون فرسایش اعتماد بین‌المللی، تغییر سیاست‌های آمریکا در قبال فضای سایبری، چالش‌های فزاینده در فرایند شکل‌گیری و اجرای هنجارها در شرایط کنونی و هم‌زمان با آن پیشرفت سریع توانمندی‌ها و زیرساخت‌های سایبری چین و همچنین فعالیت دیپلماتیک فزاینده این کشور در عرصه بین‌الملل، موجب تضعیف موقعیت ایالات‌متحده و تقویت جایگاه راهبردی چین در حوزه حقوق بین‌الملل سایبری شده است.

در این میان، شاید بتوان مهم‌ترین پیامد حاصل از این تحول قدرت را دگرگونی اساسی در فرایند تدوین و ساماندهی هنجارها و قواعد حاکم بر رفتار دولت‌ها در فضای سایبر دانست. بدین معنا که دوران غلبه یک‌جانبه ایالات‌متحده و الگوسازی مبتنی بر اصولی همچون آزادی بیان، دسترسی باز، خنثی بودن شبکه و حداقل

مداخله دولت، به پایان رسیده و وارد عصر جدیدی شده‌ایم که ویژگی آن وجود چندصدایی و تکثرگرایی در تعیین دستور کار و سیاست‌گذاری برای فضای مجازی است.

در این میان، چین با معرفی مفهوم نوظهور «حاکمیت سایبری» و تأکید بر کنترل بیشتر دولت‌ها بر فعالیت‌های سایبری در قلمرو خود، درصدد است تا الگو و رویکرد جایگزینی را جایگزین پارادایم فعلی مبتنی بر «حکمرانی اینترنت» نماید. با توجه به گرایش روزافزون کشورها به تأکید بر حاکمیت ملی و تمایل آن‌ها برای کنترل بیشتر بر فضای سایبری، می‌توان انتظار داشت که الگوی حاکمیت سایبری چین، در آینده نزدیک جایگزین الگوی کنونی غربی شود. درمجموع باید گفت یافته‌های این پژوهش مؤید آن است که تحولات حاصله در توازن قدرت در عرصه حقوق بین‌الملل سایبری، ضرورت بازاندیشی و تجدیدنظر بنیادین در ساختار و کارکرد فعلی این حوزه حقوقی را آشکار می‌سازد. دراین‌راستا نیاز است تا چهارچوب جدیدی طراحی شود که بتواند نیازها و منافع همه بازیگران عرصه بین‌المللی را مدنظر قرار داده و ضمن تأمین امنیت ملی، زمینه همکاری و تعامل بین‌المللی را نیز در جهت تحقق یک فضای مجازی جهانی، آزاد، امن و باثبات فراهم نماید.

به نظر می‌رسد تنها راه برون‌رفت از این بن‌بست، اتحاد و ائتلاف سایر بازیگران بین‌المللی برای کمک به هدایت اوضاع در مسیری سازنده است. کشورها و سازمان‌های منطقه‌ای باید با برگزاری نشست‌ها و اجلاس‌هایی، زمینه گفت‌وگو و تبادل‌نظر میان طرفین اختلاف را فراهم کنند تا از این رهگذر بتوانند حداقل‌هایی از تفاهم مشترک را در خصوص چهارچوب حاکم بر فضای سایبر شکل دهند. علاوه بر این، بخش خصوصی شامل غول‌های فناوری و شرکت‌های نوپای دانش‌بنیان نیز می‌توانند با ارائه راه‌حل‌ها و محصولات نوآورانه، به بهبود سطح امنیت و اعتماد در فضای مجازی کمک شایانی کنند. از سوی دیگر، آمریکا و چین نیز به‌عنوان دو بازیگر اصلی این عرصه، مسئولیت بسیاری در قبال آینده فضای سایبر دارند. آن‌ها می‌بایست با تعلیق دشمنی‌ها و بی‌اعتمادی‌های دیرپا، بر سر میز مذاکره نشسته و در یک گفت‌وگوی صادقانه و سازنده، به جست‌وجوی راه‌حل‌های مشترک بپردازند. باوجود تمام تفاوت‌های موجود، نکته مشترکی که همگان بر آن اتفاق‌نظر دارند این است که بدون همکاری و مساعدت یکدیگر هیچ‌کس قادر به حل تنهایی چالش‌های پیش‌رو در جهان دیجیتال نخواهد بود.

بر همین اساس، در پایان می‌توان این‌گونه نتیجه گرفت که تغییر قدرت در پارادایم حقوق بین‌الملل سایبری چالش‌های جدیدی را به همراه دارد که نیازمند تلاش‌های جمعی و استراتژی‌های فعال به شرح زیر است:

الف. شکل‌گیری و اجرای هنجارها

تغییر قدرت، رویکرد سنتی در خصوص شکل‌گیری و اجرای هنجارها را به چالش می‌کشد. با کاهش نفوذ ایالات‌متحده و اظهارنظر چین درباره دیدگاه خود از حاکمیت سایبری، رسیدن به اجماع، پیچیده‌تر می‌شود. دولت‌ها باید در جهت ایجاد هنجارهای جهانی مروج رفتار مسئولانه، احترام به حقوق بشر و حفاظت از ثبات و امنیت فضای سایبری تلاش کنند. همچنین، مکانیسم‌های مؤثر برای اجرای هنجارها، مسئولیت‌پذیری و انتساب برای جلوگیری از فعالیت‌های مخرب سایبری بسیار حیانی و مهم هستند.

ب. ایجاد تعادل بین امنیت و حریم خصوصی

تغییر قدرت ممکن است منجر به ارزیابی مجدد نقطه تعادل بین امنیت و حریم خصوصی در فضای سایبری شود. دولت‌ها باید با چالش حفاظت از امنیت ملی در عین احترام به حقوق و آزادی‌های فردی دست‌وپنجه نرم کنند. برقراری تعادل مناسب نیازمند چهارچوب‌های قانونی قوی، فرایندهای شفاف و مکانیسم‌های نظارتی مستقل است تا از عدم تجاوز اقدامات امنیت سایبری به حقوق حریم خصوصی یا تبدیل آن به ابزاری برای سانسور و نظارت اطمینان حاصل شود.

ج. رفع شکاف تکنولوژیک

تغییر قدرت پیامدهایی برای رقابت و همکاری در حوزه فناوری دارد. کشورها باید در تحقیق و توسعه سرمایه‌گذاری کنند تا قابلیت‌های سایبری خود را افزایش دهند، نوآوری را تقویت کنند و شکاف تکنولوژیک را برطرف سازند. تلاش‌های مشترک برای رفع شکاف تکنولوژیک، ترویج انتقال فناوری و ایجاد ظرفیت سایبری در کشورهای درحال‌توسعه می‌تواند به ایجاد یک اکوسیستم دیجیتال فراگیرتر و امن‌تر کمک کند.

د. ملاحظات اخلاقی و استانداردهای بین‌المللی

همان‌طور که فناوری‌های نوظهور مانند هوش مصنوعی و محاسبات کوانتومی، آینده فضای سایبری را شکل می‌دهند، ملاحظات اخلاقی و استانداردهای بین‌المللی نیز اهمیت می‌یابند. جامعه بین‌المللی باید در مورد چهارچوب‌های اخلاقی، توسعه هوش مصنوعی مسئولیت‌پذیر و تأثیر فناوری‌های نوظهور بر حقوق بشر وارد بحث شود. تلاش برای ایجاد اصول و هنجارهای اخلاقی مشترک می‌تواند منجر به استفاده مسئولانه از فناوری‌های پیشرفته شده و خطرات احتمالی را کاهش دهد.

فهرست منابع

- ارغوانی پیرسلامی، فریبرز؛ علی پور، حسین (۱۴۰۲). ***انتقال نهادی قدرت در نظم بین‌المللی: فرصت‌ها و چالش‌های بانک سرمایه‌گذاری زیرساخت آسیا برای چین***. فصلنامه روابط خارجی، ۱۵(۴)، صص.۱-۳۴ . doi: 10.22034/fr.2024.403607.1403
- زاهدی خطیر، الهام؛ صالحی، مختار (۱۴۰۱). ***روند پژوهی تداوم جنگ تجاری آمریکا علیه چین (۲۰۱۸-۲۰۲۲)***. فصلنامه روابط خارجی، ۱۴(۳)، صص. ۱۳۳-۱۶۲. doi: 10.22034/fr.2022.165684.
- قلخانباز، خلیل؛ یزدانی، عنایت‌الله؛ ابراهیمی، شهروز (۱۴۰۲). ***رقابت استراتژیک آمریکا و چین و تأثیر آن بر سیاست هندو- پاسیفیک ایالات‌متحده: درس آموخته‌های راهبردی جمهوری اسلامی ایران***. فصلنامه روابط خارجی، ۱۵(۳) ، صص ۲۸-۵۶. doi:10.22034/fr.2024.428449.1468

References

- Allahrakha, N. (2023). Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age. *Legal Issues in the Digital Age, 4*(2), 78–121. doi:DOI:10.17323/2713-2749.2023.2.78.12
- Attatfa, A., Renaud, K., & Paoli, S. D. (2020). Cyber Diplomacy: A Systematic Literature Review. *Procedia Computer Science, 176*, 60–69. Retrieved from https://doi.org/10.1016/j.procs.2020.08.007
- Bowden, C. (2013). *The US surveillance programmes and their impact on EU citizens' fundamental rights.* Brussel: DIRECTORATE GENERAL FOR INTERNAL POLICIES European Parliament. Retrieved from https://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf
- *Can the Digital Economy Survive in a Splinternet*. (n.d.). Retrieved from The Centre for International Governance Innovation: https://www.cigionline.org/newsletters/can-digital-economy-survive-splinternet/
- Carr, M. (2016). Crossed Wires: International Cooperation on Cyber Security. *Interstate - Journal of International Affairs*. Retrieved from https://discovery.ucl.ac.uk/id/eprint/10056277/3/Carr_InterState_Dec2015.pdf
- Chen, X., & Yang, Y. (2022). Contesting Western and Non-Western Approaches to Global Cyber Governance beyond Westlessness. *The International Spectator, 57*, 1 - 14. Retrieved from https://www.tandfonline.com/doi/full/10.1080/03932729.2022.2101231
- Creemers, R. (2021). China's Emerging Data Protection Framework. *Leiden Institute for Area Studies*, 4. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3964684
- Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity, 8*(1). Retrieved from https://doi.org/10.1093/cybsec/tyac011
- Ettinger, A. (2018). Trump's National Security Strategy: "America First" meets the establishment. *International Journal, 73*(3), 474-483. Retrieved from https://doi.org/10.1177/0020702018790274
- Fedoniuk, S., & Maghdysiuk, S. (2022). US-China Confrontation in Cyber Security. *Історико-Політичні Проблеми Сучасного Світу, 45*, 113–127. Retrieved from https://doi.org/10.31861/mhpi2022.45.113-127
- Gao, X. (2022). An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model. *The International Spectator, 57*(3), 15–30. Retrieved from https://doi.org/10.1080/03932729.2022.2074710
- *Global Free Flow of Information on the Internet*. (2010). Retrieved from Federal Register: https://www.federalregister.gov/documents/2010/09/29/2010-24385/global-free-flow-of-information-on-the-internet
- Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* New York: Henry Holt and Company.
- Hameed, F., Agrafiotis, I., Weisser, C., Goldsmith, M., & Creese, S. (2018). Analysing trends and success factors of international cybersecurity capacity−building initiatives. *Department of Computer Science University*

of Oxford. Retrieved from https://ora.ox.ac.uk/objects/uuid:50e9c5aa-4f3d-40f0-a0a0-ff538b735291/files/mf1ff1854d7b0d2cf2a244539752a2274

- Harnisch, S., & Zettl-Schabath, K. (2022). Secrecy and Norm Emergence in Cyber-Space. The US, China and Russia Interaction and the Governance of Cyber-Espionage. *Democracy and Security, 19*, 82-110. Retrieved from https://www.tandfonline.com/doi/full/10.1080/17419166.2022.2097074
- Hoffmann, S., Lazanski, D., & Taylor, E. (2020). Standardising the splinternet: how China's technical standards could fragment the internet. *Journal of Cyber Policy, 5*, 1-26. Retrieved from Retrieved from: https://www.researchgate.net/publication/343978312_Standardising_the_splinternet_how_China's_technical_standards_could_fragment_the_internet
- Hong, Y., & Goodnight, G. T. (2019). How to think about cyber sovereignty: the case of China. *Chinese Journal of Communication, 13*(1), 8–26. Retrieved from https://doi.org/10.1080/17544750.2019.1687536
- Jinghua, L. (2019). *What Are China's Cyber Capabilities and Intentions?* Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734
- (2023). *Joint Statement on the United States-European Union 9th Cyber Dialogue in Brussels - United States Department of State.* United States Department of State. Retrieved from https://www.state.gov/joint-statement-on-the-united-states-european-union-9th-cyber-dialogue-in-brussels/
- Kalen, S., & Howard, W. S. (2016). Reclaiming Accountability: Transparency, Executive Power, and the U.S. Constitution. By Heidi Kitrosser. Chicago: University of Chicago Press, 2015. Pp. 283. ISBN: 978-0-226-19163-8. *International Journal of Legal Information, 44*(1), 62–65. Retrieved from https://www.cambridge.org/core/journals/international-journal-of-legal-information/article/abs/reclaiming-accountability-transparency-executive-power-and-the-us-constitution-by-heidi-kitrosser-chicago-university-of-chicago-press-2015-pp-283-isbn-978022619
- Larkin, T. (2022). *How China Is Rewriting the Norms of Human Rights*. Retrieved from Lawfare: https://www.lawfaremedia.org/article/how-china-rewriting-norms-human-rights
- Lee, J. (2022). Cyberspace Governance in China, Evolution, Features and Future Trends, ASIE. *VISIONS, 129*. Retrieved from Retrieved from: https://www.ifri.org/sites/default/files/atoms/files/lee_cyberspace_governance_china_2022.pdf
- Liaropoulos, A. N. (2017). Cyberspace Governance and State Sovereignty. *Democracy and an Open-Economy World Order*, 25–35. Retrieved from https://doi.org/10.1007/978-3-319-52168-8_2
- Lostri, E., Lewis, J. A., & Wood, G. (2022). *A Shared Responsibility: Public-Private Cooperation for Cybersecurity*. Retrieved from Center for Strategic and International Studies: https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity
- M Salem Abu Alead, R., & AMHMED AB ALTALIBE, A. (2023). Attribution Challenges in the Era of Cyber Warfare: Unraveling the Identity of Cyber-Attackers. *3*(16), 5309-5287. Retrieved from https://doi.org/10.21608/hiss.2023.337323
- McTague, T. &. (2020, October 29). *HOW 'AMERICA FIRST' BECAME AMERICA ALONE*. Retrieved from The Atlantic:

https://www.theatlantic.com/international/archive/2020/10/donald-trump-foreign-policy-america-first/616872/

- Pijovic, N. (2021). The Cyberspace 'Great Game'. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms. *2021 13th International Conference on Cyber Conflict (CyCon)*, (pp. 215-231). Tallinn, Estonia. doi:doi: 10.23919/CyCon51939.2021.9468296.
- Piper, A. (n.d.). *Digital surveillance's threat to human rights*. Retrieved from International Bar Association: https://www.ibanet.org/article/CEE365AB-CC04-4E2C-91F6-D5F4D353A0A0
- Runde, D. F., & Ramanujam, S. R. (2022). *Digital Governance: It Is Time for the United States to Lead Again*. Retrieved from Center for Strategic and International Studies: https://www.csis.org/analysis/digital-governance-it-time-united-states-lead-again
- Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review, 3*(1), 7–34. Retrieved from https://doi.org/10.1365/s43439-021-00045-4
- Schulte, G. L., & Schaffer, A. M. (2012). Enhancing Security by Promoting Responsible Behavior in Space. *Strategic Studies Quarterly, 6*(1), 9–17. Retrieved from http://www.jstor.org/stable/26270787
- Segal, A. (2020). *China's Alternative Cyber Governance Regime: Hearing on A 'China Model?' Beijing's Promotion of Alternative Global Norms and Standards*. Retrieved from Council on Foreign Relations: https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf
- Segal, A. (2022, July 12). *A New U.S. Foreign Policy for Cyberspace*. Retrieved from Council on Foreign Relations: https://www.cfr.org/blog/new-us-foreign-policy-cyberspace
- Sherman, J. &. (2022). *The US must broaden its internet strategy beyond China*. Retrieved from Brookings: https://www.brookings.edu/articles/the-us-must-broaden-its-internet-strategy-beyond-china/
- Studies, C. A. (2019). International Cyberspace Governance. In: Chinese Academy of Cyberspace Studies. In P. Ping, *World Internet Development Report 2017* (pp. 235–266). Berlin: Springer.
- Sullivan, J., & Wang, W. (2022). China's "Wolf Warrior Diplomacy": The Interaction of Formal Diplomacy and Cyber-Nationalism. *Journal of Current Chinese Affairs, 52*(1), 68–88. Retrieved from https://doi.org/10.1177/18681026221079841
- Telefónica. (2023). *History of the Internet: how did it come into being and how has it evolved*. Retrieved from Telefónica: https://www.telefonica.com/en/communication-room/blog/history-internet-how-come-being-how-evolved/
- Tung, R. L., Zander, I., & Fang, T. (2023). The Tech Cold War, the multipolarization of the world economy, and IB research. *International Business Review, 32*(6). Retrieved from https://www.sciencedirect.com/science/article/pii/S0969593123000951
- Zinovieva, E. S. (2022). Cyber Diplomacy under Increased Competition Between the Great Powers. *MGIMO Review of International Relations*, 1–21. Retrieved from https://doi.org/10.24833/2071-8160-2022-olf5