



دفترآبی ۱۲

مجموعه گزارش‌های پژوهشی
اردیبهشت ماه ۱۴۰۵

دیپلماسی سایبری، رویکردی نوین در نقش آفرینی در فضای بین‌المللی

(مطالعه موردی چین)





دیپلماسی سایبری، رویکردی نوین در نقش آفرینی

در فضای بین‌المللی (مطالعه موردی چین)

دفتر آبی (Research Paper) شماره دوازدهم (اردیبهشت ماه ۱۴۰۵)

مؤلف: فرید کریمی

تهیه شده در اندیشکده حکمرانی آوا

تمام حقوق مادی و معنوی این اثر متعلق به پژوهشگاه فضای مجازی است و استفاده از آن تنها با ذکر منبع مجاز است. همچنین محتوای منتشر شده در این گزارش بیانگر دیدگاه رسمی مرکز ملی فضای مجازی نیست.

نشانی: تهران، سعادت آباد، خیابان علامه شمالی، کوچه هجدهم غربی، پلاک ۱۷

تلفن: ۰۲۱-۲۲۰۷۳۳۱

کد پستی: ۱۹۹۷۹۸۷۶۲۹

مقالات پژوهشی (Research Paper) از مهم‌ترین ابزارهای توسعه دانش هستند که با تکیه بر داده‌های تجربی به بررسی دقیق و جامع موضوعات تخصصی می‌پردازند. این مقالات معمولاً توسط پژوهشگران، استادان دانشگاه و محققان حرفه‌ای نوشته می‌شوند و به تفصیل از مشاهدات و داده‌های تحقیق بحث می‌کنند. مخاطب این مقالات نیز عمدتاً محققان و کارشناسان آن رشته است. امروزه در مسئله فضای مجازی و سایبری، به‌طور مرتب مقالات پرشماری توسط محققان و اندیشکده‌ها تولید می‌شود که به بررسی موشکافانه مسائل جاری در این حوزه می‌پردازند. آگاهی از این مطالعات و رصد شرایط و ابعاد مختلف این حوزه از این رهگذر، برای کارشناسان و به‌خصوص قانون‌گذاران، حکمرانان و متولیان این عرصه ضروری است.

دفترهای آبی دسته‌ای از گزارش‌های تفصیلی تولیدشده در پژوهشگاه فضای مجازی، و محصول رصد مطالعات اندیشکده‌ها و نخبگان جهان و منطقه در این موضوع است.

پیشگفتار

دیپلماسی سایبری تا همین یک دهه پیش، بیشتر در محافل فنی و امنیتی کاربرد پیدا می کرد، اما امروز به یکی از محوری ترین عرصه های رقابت قدرت ها تبدیل شده است. در این عرصه، چین دیگر تنها یک بازیگر منفعل یا مدافع حاکمیت داخلی خود نیست؛ بلکه با برنامه ای بلندمدت و همه جانبه، در تلاش است در نظم دیجیتال جهانی طرحی برای ارائه داشته باشد. پکن با طرح ایده «حاکمیت سایبری» در برابر «اینترنت آزاد» غرب، در صدد است مدل دولت محور خود را به عنوان هنجاری جهانی تثبیت کند. این رویکرد بازتابی از یک تحول راهبردی عمیق در سیاست خارجی چین است. امروز غول های فناوری چینی، فقط ابزارهای تجاری نیستند بلکه سفیران مدل حکمرانی سایبری چین در کشورهای در حال توسعه نیز هستند. ابتکار جاده ابریشم دیجیتال، حضور فعال در سازمان ملل و مجامع بین المللی، و گفت وگوهای دوجانبه با آمریکا، روسیه و اروپا، همگی نشانه هایی از یک دیپلماسی سایبری پویا و هدفمند است. گزارش حاضر به دنبال آن است که نشان دهد چین چگونه میان تهدیدات داخلی و نقش آفرینی جهانی خود تعادل برقرار می کند و در این مسیر، چه فرصت ها و چالش هایی دارد. مطالعه این گزارش به همه کسانی که آینده نظم بین المللی و نقش قدرت های نوظهور در فضای سایبری را دنبال می کنند مفید خواهد بود.

میثم غلامی

سرپرست پژوهشگاه فضای مجازی

اردیبهشت ماه سال ۱۴۰۵

چکیده

امروزه فضای مجازی به فضای سیاسی مورد مناقشه میان قدرت‌های بزرگ جهان در حوزه فناوری، بخصوص چین و ایالات متحده آمریکا که منافع، هنجارها و ارزش‌های متفاوت و بعضاً متضادی دارند، تبدیل شده است. چین از سال‌های ابتدایی اتصال به اینترنت همواره سعی نموده تا با کنترل اینترنت در مرزهای خود، مدل اینترنتی خود را گسترش دهد و با اینترنت آزاد ادعایی مورد نظر آمریکا که از دید پکن به عنوان عاملی برای نفوذ و کنترل جوامع دیگر پنداشته شده است، مقابله نماید. انگیزه اصلی چین در مسائل مربوط به فضای سایبری، پیشی گرفتن از غرب در سراسر قلمروهای هنجاری، اقتصادی، فنی، سیاسی و همچنین تضمین جایگاه برابر در میز تصمیم‌گیری به عنوان یک قانون‌گذار بوده است. در بحث‌های سایبری بین‌المللی، جمهوری خلق چین به شدت بر اصول الزام‌آور حقوق بین‌الملل که در منشور سازمان ملل متحد اعلام شده است، از جمله اصولی مانند حاکمیت و برابری، حل و فصل مسالمت‌آمیز اختلافات، عدم استفاده از زور، عدم مداخله، احترام متقابل و دیگر اهداف منشور مانند حق تعیین سرنوشت تأکید کرده است. چین برای تقویت موقعیت خود در نظم دیجیتال جهانی، به دنبال تغییر شکل زنجیره‌های تأمین، سیستم‌های اقتصادی و فناوری جهانی است و از عرصه‌ها و ابتکارات مختلف در سطح بین‌المللی برای دستیابی به این اهداف استفاده می‌کند.

به طور خاص، پکن به دنبال ارتقای قدرت نهادی و نفوذ هنجاری خود در جهت توسعه ایده حاکمیت فضای سایبری بوده است. این رکن مرکزی دیپلماسی سایبری چینی که بیشتر جهت گیری بین المللی دارد، مستلزم ترویج ایده حاکمیت سایبری و یک مدل چند جانبه از حاکمیت اینترنت با اعطای نقش اصلی به دولت ها (در مقابل مدل چند ذی نفعی مورد نظر دولت های غربی که در آن شرکت های فناوری نقش اصلی را ایفا می نمایند) می باشد. البته چین برای رسیدن به این اهداف محدودیت هایی نیز دارد: کمبود استعداد و نوآوری برای اجرای این اهداف استراتژیک و وابستگی گسترده به فناوری های خارجی، مهم ترین چالش های پیش روی چین برای دستیابی به این اهداف است.

یافته‌های کلیدی

- دورویکرد عمده در نگاه به دیپلماسی سایبری وجود دارد: یک جنبه از نقطه نظر دیپلماسی عمومی است؛ و دیگری دیدگاه ژئوپلیتیکی را در دیپلماسی سایبری دنبال می‌کند. چشم‌انداز ژئوپلیتیکی دیپلماسی سایبری مربوط به ایجاد دیپلماسی فضای سایبری و پیگیری منافع سایبری ملی یک کشور در سطح دوجانبه و چندجانبه است. موضوعات رایجی که دیپلماسی سایبری حول محور آنها می‌چرخد عبارتند از: آزادی اینترنت، حاکمیت اینترنت، جرایم سایبری و امنیت سایبری. جنبه دیپلماسی عمومی آن، تنها به یک جنبه از دیپلماسی سایبری نگاه می‌کند که معمولاً به عنوان دیپلماسی دیجیتالی شناخته می‌شود.
- چین از سال‌های ابتدایی اتصال به اینترنت همواره سعی نموده تا با کنترل اینترنت در مرزهای خود مدل اینترنتی خود را گسترش دهد و با اینترنت آزاد ادعایی مورد نظر آمریکا که از دید پکن به عنوان عاملی برای نفوذ و کنترل جوامع دیگر پنداشته شده است، مقابله نماید.
- محور تلاش‌های چین ایده حاکمیت سایبری^۱ است. همان‌طور که رئیس‌جمهور شی-جین‌پینگ در کنفرانس جهانی اینترنت ۲۰۱۵ در ووژن توضیح داد، حاکمیت سایبری به معنای احترام به حق هر کشور برای انتخاب مسیر توسعه اینترنت خود، مدل مدیریت

1. Cyber Sovereignty

اینترنت خود و سیاست‌های عمومی خود در اینترنت است. اولین اصل ذکر شده در استراتژی ملی سایبری ۲۰۱۶، احترام و حفاظت از حاکمیت در فضای سایبری است. اولین وظیفه راهبردی در این سند، دفاع قاطعانه از حاکمیت در فضای مجازی و مخالفت با تمامی اقدامات برای براندازی نظام ملی چین یا تخریب حاکمیت چین از طریق فضای سایبری است. در حالی که حاکمیت در فضای سایبری یک ایده ذاتا تجدیدنظرطلبانه نیست، اما این موضع برخلاف دیدگاه فضای سایبری به عنوان یک پلتفرم باز و جهانی که توسط ایالات متحده و هم‌پیمانان آن مطرح می‌شود، می‌باشد.

- رویکرد پکن به کاربرد مقررات بین‌المللی در فضای سایبری گزینشی و هدفمند بوده است. مشخصه اصلی دیدگاه حقوقی چین، ترجیح اصول حقوقی مندرج در منشور سازمان ملل متحد بر دیگر مقررات بین‌المللی و پذیرش کاربرد منشور سازمان ملل در فضای سایبری بوده است.

- عدم تمایل به اعمال روش‌هایی که از طریق آن مقررات عرفی و معاهده‌های بین‌المللی ممکن بر حوزه سایبری حاکم شود، از دیگر اصول حقوقی چین بوده است. چین بارها بر سر اجرای مقررات موجود که توسل به زور و اعمال حقوق مخاصمات مسلحانه را در سناریوهای سایبری تنظیم می‌کند، مخالفت ورزیده است. پکن اساساً با این ایده که چارچوب فعلی مقررات بین‌المللی می‌تواند عملیات مخرب سایبری را غیرقانونی اعلام کند و به دولت‌ها اجازه دهد تا برای محافظت از خود در برابر فعالیت‌های مخرب، پاسخ‌هایی از جمله اقدام متقابل سایبری را برگزینند، مخالفت نموده است. این امر ریشه در آگاهی پکن نسبت به آسیب‌هایی دارد که می‌تواند توسط ابزارهای سایبری، به‌ویژه توسط دولت‌هایی که از قابلیت‌های سایبری تهاجمی برای برانگیختن ناآرامی‌های اجتماعی، مداخله در امور داخلی، براندازی سیستم یا آسیب رساندن به امنیت ملی و امنیت اطلاعات کاربران بهره‌مند هستند، وارد شود.

- دولت چین یکی از مهم‌ترین اولویت‌های خود را در حوزه هنجارسازی، گسترش و ارتقای حاکمیت فضای سایبری تعریف نموده است. به طور خاص، پکن به دنبال ارتقای قدرت

نهادی و نفوذ هنجاری خود در جهت توسعه ایده حاکمیت فضای سایبری بوده است. این رکن مرکزی دیپلماسی سایبری چینی که بیشتر جهت‌گیری بین‌المللی دارد، مستلزم ترویج ایده حاکمیت سایبری و یک مدل چندجانبه از حاکمیت اینترنت با اعطای نقش اصلی به دولت‌ها (در مقابل مدل چندذی‌نفعی مورد نظر دولت‌های غربی که در آن شرکت‌های فناوری نقش اصلی را ایفا می‌نمایند) می‌باشد.

- دومین هدف کلیدی در رویکرد دولت چین به دیپلماسی سایبری، جاه‌طلبی استراتژیک برای تبدیل شدن به یک ابرقدرت سایبری در چند محور است. یکی از ویژگی‌های اصلی ابرقدرت سایبری بودن، ارتقای چشم‌انداز هنجاری و قدرت تعیین دستور کار چین در بحث‌های سایبری بین‌المللی است. دولت چین تحت رهبری شی در "استراتژی بین‌المللی همکاری در فضای مجازی"^۱ خود به روشنی بیان داشته است که معتقد است تبدیل شدن به یک قانون‌گذار و هنجارساز و ایجاد مکانیسم‌های قدرتمند برای شکل دادن به رفتار دیگران در فضای سایبری، اولویتی مهم برای منافع چین در آینده می‌باشد.
- دولت چین از سال ۲۰۱۴ درگیر فرایند ساده‌سازی و تحکیم محیط سیاسی - نهادی بازیگران حوزه امنیت سایبری بوده است. پکن با هدف ساده‌سازی توانایی حزب برای هدایت سیاست‌ها، به طور هدفمند اصلاحاتی مانند تغییر نهادی، تغییر و سازماندهی مجدد قدرت و ایجاد ارگان‌های سیاسی جدید برای مقابله با بوروکراسی گسترده، تضادها بر سر مسئولیت‌ها، پراکندگی نهادی، مسائل مربوط به تقسیم قدرت و درگیری‌های عملیاتی اجرا کرده است. برای بهبود هماهنگی، شورای دولتی چین^۲ اعلام کرد که کمیسیون مرکزی امور فضای سایبری به رهبری رئیس‌جمهور، اکنون مرجع تصمیم‌گیری متمرکز در فضای سایبری و خط‌مشی‌گذاری امور فناوری اطلاعات و ارتباطات می‌باشد. تمرکز دستگاه حاکمیت فضای سایبری چین، بیش از همه، برای تحکیم قدرت سیاسی در استان حزب کمونیست چین و

1. International Strategy of Cooperation on Cyberspace

2. The State Council of the People's Republic of China

تمرکز ظرفیت حزب - دولت برای هدایت تحولات از طریق تصمیم‌گیری از بالا به پایین طراحی شده است.

- پکن از تجارت و سرمایه‌گذاری در زیرساخت‌های فناوری اطلاعات به عنوان یک ابزار سیاسی اقتصادی استفاده کرده است. تلاش‌های چین در آفریقا، آسیای جنوب شرقی و آسیای مرکزی برای دسترسی به بازارها و همچنین ایجاد حمایت از سیاست خارجی پکن و هنجارهای فضای سایبری طراحی شده است. بدین ترتیب ایجاد زیرساخت‌های ارتباطی در کشورهای مورد نظر در ابتکار کمربند - جاده (BRI)، به جمهوری خلق چین اجازه می‌دهد تا به مجموعه داده‌های کشورهای دریافت‌کننده دسترسی داشته باشد و بتواند این اطلاعات را مورد تجزیه و تحلیل قرار دهد. همچنین از طریق این تجهیزات و شرکت‌های فناوری چینی، پکن می‌تواند مدل حاکمیتی، سیستم نظارتی و مؤسسات مالی خود را در خارج از کشور گسترش دهد.
- یکی از فرصت‌های کلیدی دیپلماسی سایبری چین، ظرفیت‌سازی در کشورهای در حال - توسعه بوده است. ظرفیت‌سازی در فناوری‌های دیجیتال از جمله زیرساخت‌های شبکه، سیستم‌های اطلاعاتی، 5G، فیبر نوری و کابل‌های زیردریایی و ابزارهای فیلتر محتوا، در خدمت هدف استراتژیک بزرگ‌تر متقاعد کردن کشورهای در حال توسعه برای پذیرش ایده‌ها و مفاهیم حوزه سایبری پکن است. ابتکار همکاری بین‌المللی اقتصاد دیجیتال در ابتکار کمربند جاده، که در سال ۲۰۱۷ راه‌اندازی شد و جاده ابریشم دیجیتال، به دنبال بین‌المللی کردن فناوری چینی ساخته شده توسط شرکت‌های دولتی یا وابسته، از جمله هواوی و زدتی‌ای می‌باشد و از این طریق، استانداردها و ایجاد شرایط بالقوه مطلوب برای اهداف سایبری سیاسی و فنی چین را مهیا می‌کنند.
- حرکت چین به سمت حاکمیت سایبری که به نحوی نتیجه افزایش تهدیدات تنش‌ها با ایالات متحده آمریکا بوده است، یک عامل مؤثر در بی‌اعتمادی دولت‌ها و شرکت‌های خارجی به دولت پکن و غول‌های فناوری چین شده است. از آنجایی که فضای کسب و کارهای خارجی به تدریج دشوارتر و چالش‌برانگیزتر شده است، حمایت از تعامل با چین در میان

شرکت‌های بین‌المللی، کاهش یافته است. علاوه بر این، نگرانی‌ها در مورد خطرات بالقوه ناشی از ردپای جهانی روبه‌رشد کسب‌وکارهای چینی، دولت‌های توسعه‌یافته سراسر جهان را به تجدیدنظر در میزان مشارکت چین در بازارهای داخلی خود سوق داده است.

- چین در راستای تلاش برای همسو کردن نظام بین‌المللی با چشم‌انداز خود و در عین حال دستیابی به استقلال بیشتر در نظم دیجیتال جهانی، استراتژی آینده خود را بر سه حوزه بسیار مهم از جمله استانداردسازی، خوداتکایی فناوری و ایجاد روایت‌های جایگزین امنیت سایبری بین‌المللی معطوف نموده است.
- شایان ذکر است عوامل متعددی می‌توانند اهداف کلی چین در رابطه با فضای سایبری را مختل کند؛ رویکردهای مبتنی بر حاکمیت چین برای حکمرانی اینترنت، مستلزم اعمال مستمر فیلتر و کنترل جریان آزاد اطلاعات است که نیاز به تدوین فزاینده قوانین و مقررات امنیت سایبری دارد. این موضوع ممکن است چالش آسیب دیدن وجهه داخلی و بین‌المللی، هم برای دولت و هم برای غول‌های فناوری چین را به همراه داشته باشد.

مقدمه

فضای سایبری امروزه به یکی از کانون‌های اصلی روابط بین‌الملل تبدیل شده است. اکثر قدرت‌های جهانی در حال حاضر مسائل سایبری را در اهداف و اسناد سیاست خارجی خود پیاده نموده، استراتژی‌های سایبری را اتخاذ کرده و دیپلمات‌هایی را برای تعقیب این اهداف استراتژیک منصوب کرده‌اند. جاسوسی سایبری، حملات سایبری، نفوذ، سانسور اینترنتی و حتی مسائل فنی مانند بی‌طرفی شبکه، اکنون به طور گسترده در تیتراژها قرار گرفته‌اند. امروزه فضای مجازی به فضای سیاسی مورد مناقشه میان قدرت‌های بزرگ جهان در حوزه فناوری، بخصوص چین و ایالات متحده آمریکا که منافع، هنجارها و ارزش‌های متفاوت و بعضاً متضادی دارند، تبدیل شده است. در نتیجه این سیاست‌زدگی فضای سایبری، دیپلمات‌ها نیز برای حفظ منافع دولت خود وارد این مناقشه شده‌اند. بدین ترتیب، می‌توان گفت دوره‌ای که در آن فضای مجازی حوزه‌ای برای بحث‌های فنی در میان متخصصان فناوری اطلاعات بود، به پایان رسیده است.

در فضای مجازی و همچنین در فضای واقعی، رهبری چین عنوان داشته است که حفظ حاکمیت و اقتدار ملی، سنگ بنای رویکرد حاکمیتی آن است. این امر عمدتاً ناشی از درک حزب کمونیست چین از ارزش‌های لیبرال، نه به عنوان مجموعه‌ای جهانی از ارزش‌ها، بلکه به عنوان ابزاری هژمونیک در دست قدرت‌های غربی است. به این ترتیب، چین ارزش‌های لیبرال را به عنوان پایان تاریخ قلمداد نمی‌کند،

بلکه به عنوان یک تهدید وجودی برای یکپارچگی و ثبات نظام سیاسی چین می‌داند. این کشور تلاش کرده است که این موضوع را در هنجارها و توافقات در سطح بین‌المللی لحاظ کند و گام‌های قابل توجهی برای تضمین توانایی حاکمیتی خود در فضای سایبری، حتی در صورت نبود اجماع جهانی، بردارد (Creemers R. , 2020).

از زمان به قدرت رسیدن شی جین‌پینگ در سال ۲۰۱۲، پکن به صورت فعال درگیر دیپلماسی سایبری بوده است. چین به عنوان یک بازیگر عقلانی، دریافته است که با تهدیدات گوناگونی در فضای سایبری از جمله توزیع نابرابر منابع اینترنتی که در آن بسیاری از منابع و اختیارات در فضای سایبری به ایالات متحده آمریکا اعطا شده، مواجه است. علاوه بر این، ارزش‌های لیبرال دموکراتیک از طریق پلتفرم‌های آنلاین در سرتاسر جهان در حال گسترش هستند. این موضوعات در پکن بسیار مورد توجه قرار گرفته است، زیرا شی جین‌پینگ نمی‌خواست شاهد انقلاب‌های توده‌ای در چین با هدف فروپاشی کل سیستم باشد.

بدین ترتیب پکن، ایالات متحده آمریکا را به عنوان یک تهدید مستقیم در حوزه فضای سایبری درک کرده است. برای مقابله با این قدرت سایبری، چین از فایروال بزرگ چین (Great Fire Wall) به عنوان مکانیسمی برای کنترل فضای سایبری در سطح داخلی استفاده نموده است. رئیس‌جمهور شی جین‌پینگ در طول دوران تصدی خود به عنوان یکی از اهداف سیاست خارجی خود به منظور تقویت امنیت ملی و بقای حزب توجه بسیاری به دیپلماسی سایبری داشته است، زیرا معتقد است چین از سوی دیگر بازیگران سایبری در خطر می‌باشد. به دنبال این رویکرد، چین دیپلماسی سایبری خود را از طریق دیپلماسی تجاری فناوری اطلاعات از طریق طرح جاده ابریشم دیجیتال، دیپلماسی دوجانبه با ایالات متحده آمریکا، بریتانیا و روسیه و برگزاری کنفرانس‌های بین‌المللی برای گسترش اصل حاکمیت سایبری انجام داده است.

این پژوهش به دنبال پاسخ به این پرسش است که چگونه چین توانسته است بین تهدیدات و مکانیسم‌هایی که چین برای تضمین نگرانی‌های ملی خود، یعنی بقای حزب و امنیت ملی و تبدیل شدن به یک بازیگر سایبری مسلط در جهان استفاده کرده است، تعادل برقرار کند. بنابراین، اهداف اولیه این تحقیق بررسی رویکرد سایبری چین، بازیگران و اقدامات چین در دیپلماسی سایبری می‌باشد. اهداف

ثانویه نیز تجزیه و تحلیل و بررسی موفقیت و شکست سیاست‌های دیپلماتیک سایبری چین و برنامه آینده چین در فضای سایبری بین‌المللی برای مهار تسلط ایالات متحده آمریکا و مقابله با تهدیدات فضای سایبری بوده است.

رویکرد اتخاذ شده یک روش کیفی است. در این تحقیق از ادبیات موجود برای تجزیه و تحلیل استفاده شده است. داده‌های اولیه این تحقیق از طریق کتاب‌ها، مقالات، مجلات و منابع خبری جمع‌آوری شد و منابع دیگر از طریق توافق‌نامه‌ها، صورت جلسه‌ها، سخنرانی‌ها، وب‌سایت‌های رسمی و سایر منابع گردآوری شده‌اند.

دیپلماسی سایبری، رویکرد و اهداف چین

دو رویکرد عمده در نگاه به دیپلماسی سایبری وجود دارد: یک جنبه از نقطه نظر دیپلماسی عمومی است؛ و دیگری دیدگاه ژئوپلیتیکی را در دیپلماسی سایبری دنبال می‌کند. چشم‌انداز ژئوپلیتیکی دیپلماسی سایبری مربوط به ایجاد دیپلماسی فضای سایبری و پیگیری منافع سایبری ملی یک کشور در سطح دو جانبه و چند جانبه است. جنبه دیپلماسی عمومی آن، تنها به یک جنبه از دیپلماسی سایبری نگاه می‌کند که معمولاً به عنوان دیپلماسی دیجیتال شناخته می‌شود. دیپلماسی دیجیتال به طور گسترده از اینترنت به عنوان ابزاری برای پیشبرد اهداف دیپلماسی عمومی استفاده می‌کند (Mihai Sebastian Chihai and Jan Rempala, 2021).

دیپلماسی سایبری: تعریف و درهم آمیختگی مفهومی

آندره بارینا و توماس رنارد (۲۰۱۷) در مقاله "دیپلماسی سایبری: ایجاد یک جامعه بین‌المللی در عصر دیجیتال"^۱ که دیپلماسی سایبری را از دیپلماسی الکترونیک یا دیجیتال متمایز می‌نمود، دیپلماسی سایبری را به عنوان پیگیری منافع ملی یک دولت در حوزه فضای سایبری در نظر گرفته‌اند. به بیانی دیگر،

1. Cyber-diplomacy: The making of an international society in the digital age

دیپلماسی سایبری عبارت است از استفاده از منابع دیپلماتیک و انجام وظایف دیپلماتیک برای تامین منافع ملی در رابطه با فضای سایبری. به عقیده بارینا و رنارد موضوعات رایجی که دیپلماسی سایبری حول محور آنها می چرخد عبارتند از: آزادی اینترنت، حاکمیت اینترنت، جرایم سایبری و امنیت سایبری (Barrinha, A., & Renard, T., 2017).

تلاش‌ها برای تعریف دیپلماسی سایبری معمولاً با توضیح معنای دیپلماسی مرتبط است. تعریف استفاده شده توسط آندره وبارینادر مفهوم مکتب انگلیسی از دیپلماسی گنجانده شده است که به عنوان تلاش برای تعدیل منافع متضاد در روابط بین الملل از طریق مذاکره و سازش بیان شده است. طبق دیدگاه مکتب انگلیسی، بارینا ورنارد تعریف خود از دیپلماسی سایبری را نتیجه یک فرایند همیشه در حال تحول در سیاست و جامعه بین المللی می دانند (Ibid).

تا سال ۲۰۱۶ یعنی پیش از انتشار مقاله شان ریوردان^۱ با عنوان "دیپلماسی سایبری در مقابل دیپلماسی دیجیتال: یک تمایز اصطلاحی"^۲، بحث پیرامون دیپلماسی در حوزه دیجیتال با اصطلاحاتی که به صورت مترادف به کار می رفتند تا حدی گمراه کننده بود. اصطلاحاتی مانند دیپلماسی الکترونیک، دیپلماسی دیجیتال، دیپلماسی توده ای^۳ و دیپلماسی^۴، در کنار دیپلماسی سایبری برای اشاره به موارد مشابه استفاده می شد. بسیاری از سردرگمی ها در این حوزه را شاید بتوان به متخصصانی نسبت داد که کاربرد اینترنت را به عنوان روشی انقلابی برای انجام دیپلماسی عمومی، می دیدند. بدین ترتیب برای بسیاری از کارشناسان و دست اندرکاران، دیپلماسی سایبری در آن زمان صرفاً استفاده از ابزارهای دیجیتال برای انجام دیپلماسی بود. نمونه هایی از این تلفیق را می توان در دوره های اولیه دانشگاهی مشاهده کرد. در سال ۲۰۰۲، "سایبر دیپلماسی: مدیریت سیاست خارجی در قرن بیست و یکم"^۴ یکی از اولین منابع دانشگاهی بود که از اصطلاح دیپلماسی سایبری استفاده کرده بود، اما فرض اصلی بر این بود که چگونه وزارت امور خارجه و تجارت بین الملل کانادامی تواند به بهترین شکل از فناوری اطلاعات برای

1. Shaun Riordan

2. Cyber diplomacy vs. Digital diplomacy: A terminological distinction

3. Mass diplomacy

4. Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century

برقراری ارتباط استفاده‌کند. مقاله سکون (اینرسی) دیپلماسی^۱ از یورگن کلایئر^۲ در سال ۲۰۰۸ نیز بخشی با عنوان دیپلماسی سایبری دارد، اما این ایده را مطرح می‌کند که دیپلماسی سایبری صرفاً دیپلماسی عمومی در اینترنت است.

در دهه اخیر، برجستگی موضوعات سایبری و نیاز به همکاری در این حوزه، باعث شد تا دولت‌ها دپارتمان‌های خاصی را در وزارت خارجه‌های خود ایجاد کنند و سفیران یا نمایندگانی را در حوزه‌های سایبری که به آنها دیپلمات سایبری^۳ نیز می‌گویند، تعیین کنند. هدف اصلی از ایجاد این بخش‌های تخصصی، متمرکز کردن تمام جنبه‌های مسائل سایبری در یک اداره بود که کار دولت را در این زمینه هماهنگ می‌کرد. در عین حال، انجام تعاملات چندجانبه را آسان‌تر می‌کرد و یک صدا از طرف دولت صحبت می‌نمود.

این امر بخشی از فرایند گسترش تعامل و گفتگو باهدف ایجاد مشارکت در سطح دوجانبه و همچنین در چارچوب فرمت‌های بین‌المللی بوده است. با این حال، به دلیل درهم‌تنیدگی بازیگران خصوصی و غول‌های فناوری، نقش یک دیپلمات سایبری ممکن است بسیار کم‌رنگ‌تر از همتای سنتی آنها باشد. یک دیپلمات سایبری باید طیف وسیعی از این دیدگاه‌ها و رویکردهای افراد و کارشناسان غیردولتی را نیز در هنگام مذاکره در نظر بگیرد. در واقع، دیپلمات‌های سایبری به‌طور منظم با بازیگران غیردولتی گفتگو می‌کنند تا از آخرین پیشرفت‌های فناوری مطلع شوند. این جنبه مهم تعامل، مستلزم همکاری با جامعه مدنی و صنعت برای دریافت نظرات آنها و ایجاد یک مدل چندذی-نفعی در رویکرد به همکاری‌ها و چالش‌های فضای سایبری است. این رویکرد به دیپلماسی سایبری، هر حوزه‌ای که با فضای سایبری مرتبط باشد را تحت تأثیر دیپلماسی سایبری قرار می‌دهد، مانند سیاست‌های تجاری، امنیت، آزادی حاکمیت سایبری و آزادی بیان (Mihai Chihaiia & Jan Rempala, 2021).

گرچه دیپلماسی سایبری همچنین فرایندی برای گسترش ارزش‌های هنجاری و ایجاد چارچوب مشترک اصلی برای رفتار در فضای سایبری است، با این حال، دولت‌های مختلف در مورد اینکه این

1. The Inertia of Diplomacy

2. Jurgen Kleiner

3. cyber diplomats

چارچوب چگونه باید باشد، تضاد منافع یا دیدگاه‌های متفاوت دارند. چنین درگیری خطر چندپاره شدن هنجارها و ایجاد اختلاف بین المللی را به دنبال دارد (Homburger, 2019). دیپلماسی سایبری، به عنوان بخشی از سیاست خارجی، علاوه بر هنجارسازی بین المللی در فضای سایبری، مشارکت، اتحاد و اقدامات اعتماد ساز را نیز در بر می گیرد (Bendiek, 2018).

رویکرد چین به دیپلماسی سایبری

رویکرد چین به فضای سایبری از لحاظ تاریخی مبتنی بر هدف ملی جوان سازی ملت چین^۱ پس از قرن تحقیر^۲ بوده است. انگیزه اصلی چین در مسائله مربوط به فضای سایبری، پیشی گرفتن از غرب در سراسر قلمروهای هنجاری، اقتصادی، فنی و سیاسی و همچنین تضمین جایگاه برابر در میز تصمیم گیری به عنوان یک قانون گذار بوده است. در بحث های سایبری بین المللی، چین به شدت بر اصول الزام آور حقوق بین الملل که در منشور سازمان ملل اعلام شده است، از جمله اصولی مانند حاکمیت و برابری، حل و فصل مسالمت آمیز اختلافات، عدم استفاده از زور، عدم مداخله، احترام متقابل و دیگر اهداف منشور مانند حق تعیین سرنوشت و حقوق بشر تأکید کرده است (Judge Xue, Hanqin, and Elizabeth Wilmschurst, 2013).

سیاست گذاران و تحلیلگران چینی از لحظه ای که چین برای اولین بار به اینترنت متصل شد، فضای مجازی را به عنوان یک شمشیر دولبه دیده اند، از این جهت که آن را برای رشد اقتصادی و حکمرانی خوب ضروری می دانستند، اما همچنین تهدیدی برای ثبات داخلی و مشروعیت حزب قلمداد می کردند. با توجه به این حساسیت نسبت به تهدیدات داخلی، سیاست گذاران چینی معمولاً به امنیت اطلاعات^۳

1. Rejuvenation of the Chinese Nation

جوان سازی ملت چین که به نام رویای چینی نیز شناخته می شود، نشان دهنده تلاش پکن برای به دست آوردن مجدد اعتبار خود - که در قرن تحقیر توسط قدرت های امپراتوری در اواخر قرن نوزدهم و اوایل قرن بیستم آسیب دید - و تبدیل چین به یک کشور پیشرفته و پیشرو در جهان تا سال ۲۰۴۹ است.

2. Century of Humiliation

در مقابل امنیت سایبری^۱ اشاره نموده‌اند. برای مقامات آمریکایی و اروپایی، امنیت سایبری به طور کلی به معنای محافظت از ارتباطات و سایر شبکه‌های مهم در برابر دسترسی غیرمجاز است. برای سیاست‌گذاران چینی، امنیت اطلاعات مقوله بسیار گسترده‌تری است که شامل کنترل جریان اطلاعات و محتوا و همچنین دفاع از شبکه‌ها و رایانه‌ها است (Segal, 2017).

چین این نگرانی‌ها را عمدتاً از طریق اعمال قوانین داخلی و به کارگیری فناوری‌های کنترل و نظارت که به طور گسترده به عنوان فایروال بزرگ (Great Firewall) شناخته می‌شود، مرتفع نمود. در سطح بین‌المللی، پکن عنوان داشته است که همکاری باید بر اساس احترام متقابل و به رسمیت شناختن شرایط ملی متمایز هر کشور باشد. برای مثال، گزارش رسمی چین در سال ۲۰۱۰ درباره اینترنت، همکاری بین‌المللی را از نظر تفاوت‌های ملی نشان می‌دهد: «موقعیت‌های ملی و سنت‌های فرهنگی در بین کشورها متفاوت است، بنابراین نگرانی در مورد امنیت اینترنت نیز متفاوت است. ما باید به دنبال زمینه‌های مشترک باشیم و اختلافات را حفظ کنیم، توسعه را از طریق مبادلات ارتقا دهیم و به طور مشترک از امنیت اینترنت بین‌المللی محافظت کنیم». این گزارش همچنین اعلام کرد: «در قلمرو چین، اینترنت تحت صلاحیت حاکمیت چین است و حق حاکمیت چین بر اینترنت باید مورد احترام قرار گیرد» (State Council Information Office, 2010).

محور تلاش‌های چین ایده حاکمیت سایبری^۲ است. همان‌طور که رئیس‌جمهور شی جین‌پینگ در کنفرانس جهانی اینترنت ۲۰۱۵ در ووژن^۳ توضیح داد، حاکمیت سایبری به معنای احترام به حق هر کشور برای انتخاب مسیر توسعه اینترنت خود، مدل مدیریت اینترنت خود و سیاست‌های عمومی خود در اینترنت است. اولین اصل ذکر شده در استراتژی ملی سایبری ۲۰۱۶، احترام و حفاظت از حاکمیت در فضای سایبری است. اولین وظیفه راهبردی در این سند، دفاع قاطعانه از حاکمیت در فضای مجازی و مخالفت با تمامی اقدامات برای براندازی نظام ملی چین یا تخریب حاکمیت چین از طریق اینترنت است (National Cyberspace Security Strategy, 2016).

1. Cybersecurity

2. Cyber Sovereignty

3. Wuzhen

حاکمیت سایبری ممکن است در مرکز فعالیت‌های دیپلماسی سایبری چین باشد، اما پکن همچنین از دیپلماسی تجاری و مشارکت در ایجاد استانداردهای فنی بین‌المللی برای شکل‌دادن به فضای سایبری برای تأمین منافع اقتصادی و سیاسی خود نیز استفاده کرده است. علاوه بر این، دیپلماسی سایبری بخشی از تلاش‌های پکن برای مهار خطر تروریسم، تحکیم نفوذ منطقه‌ای خود و مدیریت روابط دو جانبه خود با ایالات متحده آمریکا و سایر دولت‌ها بوده است.

شی جین‌پینگ در نشست افتتاحیه گروه کوچک پیشرو امنیت اینترنت و اطلاعات که اکنون به عنوان دفتر کمیسیون مرکزی امور فضای سایبری شناخته می‌شود، بیان کرد که چشم‌انداز چین از سال ۲۰۱۴ این بوده است که چین را به یک قدرت سایبری تبدیل کند. نقشه راه او ایجاد یک زیرساخت اینترنتی قوی با پشتوانه فناوری پیشرفته، تقویت جامعه‌ای با دانش اینترنت و استفاده از اقتصاد دیجیتال برای رفاه کشور بود. علاوه بر این، پکن در مورد ایدئولوژی حاکمیت اینترنتی خود همواره بر حاکمیت دولتی تأکید داشته و در سیاست خارجی خود به طور فعال به تقویت همکاری‌های بین‌المللی امنیت سایبری توجه داشته است (Rizki, 2023).

• رویکرد چین به کاربرد مقررات بین‌المللی در فضای سایبری

رویکرد پکن به کاربرد مقررات بین‌المللی در فضای سایبری گزینشی و هدفمند بوده است. مشخصه اصلی دیدگاه حقوقی چین، ترجیح اصول حقوقی مندرج در منشور سازمان ملل متحد بر دیگر مقررات بین‌المللی و پذیرش کاربرد منشور سازمان ملل در فضای سایبری بوده است (Segal, 2017). تلاش‌ها برای توضیح چگونگی اعمال مقررات مربوط به استفاده از زور، دفاع از خود، مسئولیت دولت و حقوق بشر دوستانه بین‌المللی در مورد اقدامات و قابلیت‌های سایبری در دور ۲۰۱۶ گروه کارشناسان دولتی (GGE) به یک نقطه چالش برانگیز تبدیل شد. انتقاد شدید چین، روسیه، کوبا و دیگران در نهایت منجر به فروپاشی کوتاه مدت سازوکار گروه کارشناسان دولتی شد. در این دوره، اختلاف نظرهای اساسی بین دوازدگانه در مورد این سؤال که آیا فضای سایبری باید منحصر به حوزه غیرنظامی باقی بماند که تحت چارچوب‌های قانونی زمان صلح است یا اینکه فضای سایبری باید تابع مقررات حقوق مخاصمات مسلحانه باشد، به حد اکثر رسید (Ibid).

مشخصه اصلی موضع چین، عدم تمایل به اعمال روش‌هایی بوده است که از طریق آن مقررات عرفی و معاهده‌های بین‌المللی ممکن بر حوزه سایبری حاکم شود. چین بارها بر سر اجرای مقررات موجود که توسل به زور و اعمال حقوق مخاصمات مسلحانه را در سناریوهای سایبری تنظیم کند، مخالفت ورزیده است. پکن اساساً با این ایده که چارچوب فعلی مقررات بین‌المللی می‌تواند عملیات مخرب سایبری را غیرقانونی اعلام کند و به دولت‌ها اجازه دهد تا برای محافظت از خود در برابر فعالیت‌های مخرب، پاسخ‌هایی از جمله اقدام متقابل سایبری را برگزینند، مخالفت نموده است (Bozhkov, 2020).

چین اعمال حقوق دفاع مشروع، قواعد عمومی مسئولیت دولت و اصول حقوق بین‌الملل بشردوستانه به‌ویژه اصول تناسب، ضرورت، تمایز، بی‌طرفی و خسارات جانبی را به منزله مشروعیت بخشیدن و تشدید درگیری در فضای سایبری و استفاده خشونت‌آمیز از قابلیت‌های سایبری به‌جای منع کامل آنها، قلمداد نموده است. چین به این دیدگاه پایبند است که استفاده از دکت‌ترین دفاع از خود که در منشور سازمان ملل متحد و قوانین عرفی ذکر شده است، همراه با حقوق مخاصمات مسلحانه می‌تواند به نحوی اعطای مجوز قانونی به کشورهای پیشرفته در زمینه فناوری برای راه‌اندازی جنگ سایبری و انجام اقدامات متقابل خودسرانه علیه دیگران تلقی شود (Ibid).

این امر ریشه در آگاهی پکن نسبت به آسیب‌هایی دارد که می‌تواند توسط ابزارهای سایبری، به‌ویژه توسط دولت‌هایی که از قابلیت‌های سایبری تهاجمی برای برانگیختن ناآرامی‌های اجتماعی، مداخله در امور داخلی، براندازی سیستم یا آسیب رساندن به امنیت ملی و امنیت اطلاعات کاربران بهره‌مند هستند، وارد شود (Grigsby, 2017).

در آخر پکن از کشورها می‌خواهد که اصول مندرج در ماده ۲ منشور سازمان ملل متحد، یعنی برابری حاکمیتی همه کشورها، تعهد به خودداری از تهدید یا استفاده از زور علیه تمامیت ارضی یا استقلال سیاسی هر کشور، اصول عدم مداخله در امور مربوط به صلاحیت داخلی هر کشور و حل و فصل مسالمت‌آمیز اختلافات را در فضای سایبری رعایت کنند (Bozhkov, 2020).

اهداف دیپلماسی سایبری چین

• حاکمیت سایبری و مدل چندجانبه حاکمیت اینترنت

دولت چین یکی از مهم‌ترین اولویت‌های خود را در حوزه هنجارسازی، گسترش و ارتقای حاکمیت فضای سایبری تعریف نموده است. به طور خاص، پکن به دنبال ارتقای قدرت نهادی و نفوذ هنجاری خود در جهت توسعه ایده حاکمیت فضای سایبری بوده است. این رکن مرکزی دیپلماسی سایبری چینی که بیشتر جهت‌گیری بین‌المللی دارد، مستلزم ترویج ایده حاکمیت سایبری و یک مدل چندجانبه از حاکمیت اینترنت با اعطای نقش اصلی به دولت‌ها (در مقابل مدل چندذی‌نفعی مورد نظر دولت‌های غربی که در آن شرکت‌های فناوری نقش اصلی را ایفا می‌نمایند) می‌باشد.

چین همواره از به رسمیت شناختن حقوق حاکمیتی و نقش بیشتر دولت‌های مستقل در حاکمیت اینترنت برای مشروعیت بخشیدن به نظارت دولت در فضای سایبری حمایت نموده است (Hampson, 2017). توجه ویژه پکن به اصل حاکمیت سایبری، فضای سایبری را تابع منافع و ارزش‌های دولت می‌کند. برتری این مفهوم بر اصول دیگر، به نوبه خود، تداوم نظارت و کنترل محتوا از طریق سیستم‌های فیلتر محتوا مانند فایروال بزرگ چین^۱ که ایده یک فضای سایبری قابل کنترل و مدیریت شده را عملیاتی کرده، توجیه نموده است. چین از جمله کشورهایی است که بر نقش مرکزی امنیت ملی و برتری بازیگران دولتی همراه با اولویت‌ها، منافع و منطق امنیتی آنها در اداره فضای سایبری و فناوری اطلاعات تأکید دارد. این مدل از مدیریت ریسک و تهدید در تضاد با رویکرد پایین به بالا حاکمیت اینترنت است که از لحاظ تاریخی مورد حمایت دولت‌های لیبرال غربی است.

گفتمان سایبری رسمی چین ادعا می‌کند که تغییر سیستم جهانی حاکمیت اینترنت که توسط دولت‌های غربی پیکربندی شده است، تنها با پذیرش گسترده حاکمیت سایبری می‌تواند رخ دهد. این مفهوم ایده احترام به حق تمامی دولت‌ها برای انتخاب مستقل مسیر توسعه سایبری، مدل مقررات-گذاری سایبری و سیاست‌های عمومی اینترنت و مدیریت فضای سایبری مطابق با قوانین ملی و زمینه‌های سیاسی-فرهنگی و چارچوب‌های قانونی متمایز آن‌ها را مطرح می‌کند (Bozhkov, 2020).

1. China's Great Firewall

ایده حاکمیت سایبری همچنین شامل حق اعمال صلاحیت بر زیرساخت‌ها، منابع و فعالیت‌های فناوری اطلاعات و ارتباطات در قلمرو خود و حفاظت از امنیت فناوری اطلاعات و ارتباطات برای حفاظت از حقوق و منافع مشروع شهروندان در فضای سایبری می‌باشد (china, 2017).

شی جین‌پینگ در سخنان خود در افتتاحیه دومین کنفرانس جهانی اینترنت عنوان داشت: «چین از همه دولت-ملت‌ها حمایت می‌کند تا در حکمرانی بین‌المللی فضای سایبری به صورت برابر مشارکت کنند و از دولت‌های دارای فناوری پیشرفته می‌خواهند تا از تعقیب اهداف خود در تبدیل شدن به هژمونی سایبری، مداخله در امور داخلی سایر کشورها، مشارکت یا حمایت از فعالیت‌های سایبری در راستای تضعیف امنیت ملی کشورها، یا اعمال نفوذ تکنولوژیک یا تسلط نهادی برای تضعیف امنیت زنجیره تأمین محصولات و خدمات فناوری اطلاعات و ارتباطات در کشورهای دیگر امتناع ورزند»^۱.
ترجیح پکن برای مدل مبتنی بر حاکمیت سایبری که اکنون در غرب نیز مورد توجه برخی قرار گرفته است، به طور هم‌زمان از کاهش هژمونی غرب در سیستم حکمرانی جهانی و در عین حال تقویت نقش چین در سطح بین‌المللی، حمایت می‌کند. به طور قابل توجهی، ترویج ایده‌های چینی در قلمرو ایده‌پردازان هم‌زمان با صادرات فناوری‌های نظارتی و تجهیزات شبکه ساخت چین در کشورهایمانند تانزانیا، اکوادور و زیمبابوه و بین‌المللی شدن سیستم حقوقی داخلی چین و گسترش آن به کشورهایمانند ویتنام صورت گرفته است (Bozhkov, 2020).

• ابرقدرت سایبری

دومین هدف کلیدی در رویکرد دولت چین به دیپلماسی سایبری، جاه‌طلبی استراتژیک برای تبدیل شدن به یک ابرقدرت سایبری در چند محور است. این چشم‌انداز استراتژیک برای اولین بار در سخنرانی شی جین‌پینگ در سال ۲۰۱۴ با بیان این نکته که چین از ایجاد زیرساخت‌های دیجیتالی پیشرفته گرفته تا تقویت نقش آن در هنجارها و مقررات بین‌المللی مرتبط با فضای سایبری باید پیشرو

۱. برای اطلاع بیشتر رجوع کنید به:

Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference:

https://www.mfa.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html

باشد، مورد استناد قرار گرفت (Central Leading Group for Internet Security and Informatization Established, 2014)

در درازمدت، پکن تصور می‌کند که تبدیل شدن به یک ابرقدرت در فضای سایبری می‌تواند به آن کمک کند تا یک اقتصاد مدرن، خودکفا و پیشرو در رقابت جهانی ایجاد نماید. علاوه بر این، تحقق این چشم‌انداز می‌تواند ارتش چین را با فناوری‌های پیشرفته بازسازی کند و همچنین گسترش صادرات فناوری ساخت چین می‌تواند جایگزین وابستگی دولت‌های دیگر به قدرت‌های خارجی شود و در نهایت حضور امنیتی منطقه‌ای چین را تقویت نماید (Bozhkov, 2020).

یکی از ویژگی‌های اصلی ابرقدرت سایبری بودن، ارتقای چشم‌انداز هنجاری و قدرت تعیین دستور کار چین در بحث‌های سایبری بین‌المللی است. دولت چین تحت رهبری شی در "استراتژی بین‌المللی همکاری در فضای مجازی"^۱ خود به روشنی بیان داشته است که معتقد است تبدیل شدن به یک قانون‌گذار و هنجارساز و ایجاد مکانیسم‌های قدرتمند برای شکل دادن به رفتار دیگران در فضای سایبری، اولویتی مهم برای منافع چین در آینده می‌باشد (International Strategy of Cooperation on Cyberspace, 2017).

• تضمین امنیت سایبری

امروزه، فضای سایبری توسط برخی کشورها به عنوان میدان نبرد جدید برای کسب مزیت‌های نظامی در نظر گرفته می‌شود. این دولت‌ها با ایجاد اتحاد نظامی با دول دیگر، خطر درگیری در فضای سایبری را افزایش می‌دهند و صلح و امنیت بین‌المللی را تضعیف می‌کنند. در پی این اقدام، زیرساخت‌های حیاتی فناوری اطلاعات و ارتباطات با آسیب‌پذیری و خطر بالقوه قابل توجهی مواجه هستند؛ حملات سایبری و جنایات افزایش یافته است و تروریسم سایبری به یک تهدید جهانی تبدیل شده است. چین در مواضع اعلامی خود در مورد مقررات بین‌المللی در فضای مجازی عنوان می‌دارد که جامعه بین‌المللی باید هنجارها، قواعد و اصول پذیرفته شده جهانی را در چارچوب سازمان ملل تدوین کند تا به طور مشترک به خطرات و چالش‌های رسیدگی کند و از صلح، امنیت و رفاه در فضای سایبری حمایت کند. در این راستا چین به همراه کشورهای عضو سازمان همکاری شانگهای در سال ۲۰۱۱ آیین‌نامه رفتار بین‌المللی

1. International Strategy of Cooperation on Cyberspace

برای امنیت اطلاعات^۱ و نسخه اصلاح شده آن را در سال ۲۰۱۵ به مجمع عمومی سازمان ملل متحد ارائه کردند. علاوه بر این، پکن در ادامه تلاش‌های بین‌المللی خود، "ابتکار جهانی در مورد امنیت داده‌ها"^۲ را در سال ۲۰۲۰ به مجمع عمومی تقدیم کرد.

چین در سند رسمی که توسط وزارت امور خارجه در سال ۲۰۲۱ با عنوان "مواضع چین در مورد مقررات بین‌المللی در فضای مجازی"^۳ منتشر شد، معتقد است که هنجارها، قوانین و اصول زیر باید رعایت شوند:

کشورها باید حفاظت از زیرساخت‌های حیاتی فناوری اطلاعات و ارتباطات را افزایش دهند. دولت‌ها باید با فعالیت‌های فناوری اطلاعات و ارتباطات که به زیرساخت‌های حیاتی دیگر کشورها آسیب می‌زند، داده‌های مهم زیرساخت‌های حیاتی دیگر کشورها را مختل می‌کند یا به سرقت می‌برد، مقابله نمایند. کشورها باید مبادلات مربوط به قوانین، شیوه‌ها و استانداردها را با توجه به حفاظت از زیرساخت‌های حیاتی فناوری اطلاعات و ارتباطات افزایش دهند و همکاری‌های بین‌المللی را در زمینه آموزش پرسنل، نوآوری‌های فناوری، هشدار و پیشگیری اولیه، واکنش اضطراری، استانداردها و مقررات و اشتراک‌گذاری اطلاعات ارتقا دهند؛

کشورها باید امنیت داده‌ها را به شیوه‌ای جامع، عینی و مبتنی بر شواهد مدیریت کنند. کشورها باید یک محیط تجاری باز، منصفانه و بدون تبعیض ایجاد کنند و زنجیره عرضه باز، ایمن و پایدار محصولات و خدمات فناوری اطلاعات و ارتباطات را حفظ کنند. دولت‌ها باید اقداماتی را برای جلوگیری و پایان دادن به فعالیت‌هایی که اطلاعات شخصی را از طریق استفاده از فناوری اطلاعات و ارتباطات به خطر می‌اندازد و بصورت غیرمجاز اطلاعات شخصی سایر کشورها را سرقت می‌کنند، انجام دهند؛

ارائه دهندگان خدمات و محصولات فناوری اطلاعات و ارتباطات باید از قوانین و مقررات دولتی که در آن فعالیت می‌کنند پیروی کنند، در محصولات و خدمات خود از روش‌هایی برای به دست آوردن غیرقانونی داده‌های کاربران، کنترل یا دستکاری سیستم‌ها و دستگاه‌های کاربران استفاده نکنند.

1. International Code of Conduct for Information Security

2. Global Initiative on Data Security

3. China's Positions on International Rules-making in Cyberspace

همچنین نباید با استفاده از وابستگی کاربران به محصولات خود به دنبال کسب منافع نامشروع باشند؛

برای حفظ صلح و ثبات طولانی مدت در فضای سایبری، اسناد حقوقی بین المللی جدید متناسب با ویژگی های فناوری اطلاعات و ارتباطات و واقعیت های در حال تحول باید بر اساس مشارکت گسترده همه دولت ها توسعه یابد. علاوه بر این، تروریسم سایبری تهدید قابل توجهی بر امنیت ملی و ثبات اجتماعی کشورها تحمیل می کند که نیاز است ابزارهای قانونی جدید برای مقابله با آن در نظر گرفته شود؛

کشورها می توانند مبادلات سیاستی و فنی، همکاری مجری قانون و به اشتراک گذاری اطلاعات را به صورت داوطلبانه انجام دهند تا اعتماد متقابل را افزایش دهند و درک نادرست و محاسبات نادرست را کاهش دهند (China's Positions on International Rules-making in Cyberspace, 2021)

بازیگران دیپلماسی سایبری چین

در چین بخش‌های گوناگونی اعم از سازمان‌های دولتی، سازمان‌های خصوصی، اندیشکده‌ها و مؤسسات تحقیقاتی در حوزه دیپلماسی سایبری فعال هستند. با توجه به تغییرات مستمر نهادی، تغییر در اختیارات نظارتی سازمان‌های دولتی و مؤسسات علمی و تحقیقاتی در حال گسترش در چین، فهرست زیر دامنه محدودی از این بازیگران را شامل شده است و تنها اطلاعات ارائه شده در گزارش‌های عمومی را منعکس نموده است.

بازیگران دولتی

دولت چین از سال ۲۰۱۴ درگیر فرایند ساده‌سازی و تحکیم محیط سیاسی-نهادی بازیگران حوزه امنیت سایبری بوده است. پکن با هدف ساده‌سازی توانایی حزب برای هدایت سیاست‌ها، به طور هدفمند اصلاحاتی مانند تغییر نهادی، تغییر و سازماندهی مجدد قدرت و ایجاد ارگان‌های سیاسی جدید برای مقابله با بوروکراسی گسترده، تضادها بر سر مسئولیت‌ها، پراکندگی نهادی، مسائل مربوط به تقسیم قدرت و درگیری‌های عملیاتی اجرا کرده است.

برای بهبود هماهنگی، شورای دولتی چین^۱ اعلام کرد که کمیسیون مرکزی امور فضای سایبری به رهبری رئیس جمهور، اکنون مرجع تصمیم‌گیری متمرکز در فضای سایبری و خط‌مشی‌گذاری امور فناوری اطلاعات و ارتباطات می‌باشد (Bozhkov, 2020). تمرکز دستگاه حاکمیت فضای سایبری چین، بیش از همه، برای تحکیم قدرت سیاسی در استان حزب کمونیست چین و تمرکز ظرفیت حزب - دولت برای هدایت تحولات از طریق تصمیم‌گیری از بالا به پایین طراحی شده است. در ادامه مهم‌ترین نهادها و صلاحیت‌های کلیدی آن‌ها توصیف شده است که نشان‌دهنده تثبیت اولویت دولت - حزب در فضای سایبری است.

• کمیسیون مرکزی امور فضای سایبری (CCAC)^۲

اقدام در راستای اولویت‌بندی نهادهای فعال در امنیت سایبری در جهت سیاست‌گذاری‌های آینده، یکی از مهم‌ترین اقدامات شی جین‌پینگ پس از روی کار آمدن بود. ارتقای گروه مرکزی پیش‌رودر امور فضای سایبری^۳ در سال ۲۰۱۸ به وضعیت کمیسیون مرکزی امور فضای سایبری که کمیسیون مرکزی امنیت سایبری و اطلاعات (CCCI)^۴ نیز نامیده می‌شود، در چارچوب تلاش‌های رئیس‌جمهور شی برای متمرکز کردن و ساده‌سازی ساختار بوروکراتیک موازی و ناکارآمد مرتبط با سیاست‌گذاری فضای سایبری صورت گرفت. این تغییر منعکس‌کننده یک اولویت مهم برای رهبری حزب در جهت حل و فصل جنگ رقابتی بین بازیگرانی مانند وزارت امنیت عمومی (MPS)، وزارت صنعت و فناوری اطلاعات (MIIT) و بخش تبلیغات کمیته مرکزی حزب کمونیست چین بود (Creemers, Rogier, et al., 2018).

این کمیسیون به ریاست اسمی شی جین‌پینگ بر کل فضای سایبری چین نظارت می‌کند. با وجود اینکه میزان درگیر شدن این نهاد در مسائل مربوط به سیاست‌گذاری‌های جزئی مبهم است، اما وجود آن انگیزه‌های درگیری بوروکراتیک را کاهش می‌دهد و یک تریبون برای حل و فصل چنین اختلافاتی به شیوه‌ای مقتدرانه فراهم نموده است (Lee, 2022).

1. The State Council of the People's Republic of China

2. The Central Cyberspace Affairs Commission (CCAC)

3. The leading Group for Cyberspace Affairs

4. The Central Commission for Cybersecurity and Informatization (CCCI)

• اداره فضای سایبری چین (CAC)^۱

اداره فضای سایبری چین در ماه می ۲۰۱۱ تأسیس شد و یک دفتر تحت اداره اطلاع‌رسانی شورای دولتی (SCIO)^۲ بود. از آوریل ۲۰۱۴، اداره فضای سایبری چین تحت نظارت مستقیم گروه مرکزی پیشرو برای امور فضای مجازی^۳ که در ۲۰۱۸ به کمیسیون مرکزی امور فضای سایبری تغییر نام داد، فعالیت می‌کند.^۴ ارتقاء گروه مرکزی پیشرو به وضعیت کمیسیون مرکزی در سال ۲۰۱۸ آن را مستقیماً تحت کمیته مرکزی حزب کمونیست چین (CCP) قرار داد (Lee, 2022).

برخی از وظایف مدیریتی مرتبط با اینترنت که توسط اداره اطلاع‌رسانی شورای دولتی صورت می‌گرفت، در آوریل ۲۰۱۴ به اداره فضای سایبری منتقل شد، از جمله صدور مجوز برای ارائه اخبار اینترنتی، فعالیت مؤسسات خارجی و زیرمجموعه‌های چینی آنها برای ارائه خدمات اطلاعاتی تجاری. اداره فضای سایبری همچنین به عنوان اداره دولتی اطلاع‌رسانی اینترنتی (SIIO)^۵ شناخته می‌شود (Cyberspace Administration of China، بدون تاریخ). در سال ۲۰۱۴، این اداره بر تمام محتوای آنلاین، قدرت اعمال کنترل و تنظیم‌گری پیدا کرد و عملاً عمده قدرت حوزه آنلاین را به کنترل خود درآورد. در این موقعیت، همه مدیران این اداره به طور هم‌زمان یک معاونت در اداره مرکزی تبلیغات حزب^۶ داشته‌اند. با انعکاس این گستردگی مسئولیت‌ها، نام آن در زبان انگلیسی در سال ۲۰۱۴ به اداره فضای سایبری چین تغییر کرد، اگرچه نام چینی آن همان اداره دولتی اطلاع‌رسانی اینترنتی باقی مانده است. (Notice concerning Empowering the Cyberspace Administration of China to be Responsible for Internet Information Content Management Work, 2014)

قانون امنیت داده ۲۰۲۱^۷ چین، اداره فضای سایبری را مسئول هماهنگی جامع امنیت داده‌های شبکه و کارهای نظارتی مرتبط و تدوین اقدامات امنیتی برای کنترل صادرات داده‌های مهم به خارج از

-
1. The Cyberspace Administration of China (CAC)
 2. the State Council Information Office of China (SCIO)
 3. the Central Leading Group for Cyberspace Affairs

۴. برای اطلاع بیشتر رجوع کنید به:

https://www.uschina.org/sites/default/files/2021_04.15_cac.pdf

5. the State Internet Information Office (SIIO)
6. the Central Propaganda Department
7. The Data Security Law (DSL)

چین با همکاری سایر آژانس‌ها می‌سازد.^۱ به نظر می‌رسد اداره فضای سایبری با دریافت مسئولیت اصلی اجرای برنامه پنج ساله جدید اطلاعات ملی، نقش خود را به عنوان آژانس هماهنگ کننده اصلی چین در سیاست فضای سایبری تثبیت نموده است. این امر احتمالاً به دلیل ماهیت آن است، که به طور هم‌زمان ارگانی از دولت اجرایی چین و بخشی از حزب کمونیست چین می‌باشد (Lee, 2022).

• وزارت امنیت کشور (MSS)^۲

وزارت امنیت کشور دارای مأموریت دوگانه اطلاعات خارجی (ضد جاسوسی) و اطلاعات داخلی (باانگیزه سیاسی) است. تمرکز اصلی این وزارتخانه بر تضمین ثبات داخلی است. این نهاد، اطلاعات مورد نیاز در باره اهداف و تهدیدات داخلی و خارجی، به عنوان بخشی از ابتکارات ضد تروریسم و ضد افراط‌گرایی را جمع‌آوری می‌کند. همچنین نقش مهمی در حوزه بررسی‌های امنیت سایبری دارد. علاوه بر این، این وزارتخانه با ایجاد نیروهای پشتیبانی استراتژیک^۳، تلاش برای سازماندهی مجدد استفاده از قابلیت‌های سایبری تهاجمی در داخل چین، بین سازمان‌های اطلاعاتی نظامی و غیرنظامی و گروه‌های عملیاتی وابسته به وزارت امنیت کشور را انجام می‌دهد (Bozhkov, 2020).

• وزارت امنیت عمومی (MPS)^۴

وزارت امنیت عمومی مأموریت امنیتی و اجرای قانون برای تضمین نظم اجتماعی عمومی به صورت آفلاین و آنلاین را دارد. این وزارتخانه با هماهنگی با وزارت صنعت و فناوری اطلاعات که دسترسی را تنظیم می‌کند و وزارت امنیت کشور که بر محتوا نظارت می‌کند، مسئول اجرای کنترل ترافیک اینترنت در چین است. وزارت امنیت عمومی بر مبارزه با جرایم سایبری و تروریسم سایبری، محدود کردن استفاده از وی‌پی‌ان (VPN) برای دور زدن فایروال چین تمرکز دارد و مسئولیت حفاظت از زیرساخت‌های حیاتی را همراه با اداره فضای سایبری چین بر عهده دارد (Ibid).

۱. برای اطلاع بیشتر رجوع کنید به؛

<https://www.cov.com/-/media/files/corporate/publications/2021/05/covington-alert--china-released-updated-draft-data-security-law-and-personal-information-protection-law-for-public-comments-may-3-2021.pdf>

2. The Ministry of State Security (MSS)

3. the Strategic Support Forces (SSF)

4. The Ministry of Public Security (MPS)

• وزارت صنعت و فناوری اطلاعات (MIIT)^۱

وزارت صنعت و فناوری اطلاعات موظف است سیاست صنعتی بخش فناوری اطلاعات و ارتباطات را تنظیم کند. این وظیفه در ابتکاراتی مانند ساخت چین ۲۰۲۵^۲، اینترنت پلاس^۳ و غیره ظاهر شده است. این نهاد ارتباطات راه دور، فناوری اطلاعات و ارتباطات و زیرساخت شبکه چین را مدیریت می کند. اگرچه یکی از مهم ترین وزارتخانه ها در رابطه با حوزه سایبری است، اما نقش آن در سیاست امنیت سایبری چین از سال ۲۰۱۸ به دلیل نقش آفرینی اداره فضای سایبری، تضعیف شده است (Creemers R. e., 2018).

در حالی که این وزارتخانه بسیاری از کارکردهای خود را به اداره فضای سایبری چین واگذار نموده است، اما اختیارات خود بر عناصر گسترده فضای سایبری چین، به عنوان مثال ساخت شبکه های مخابراتی و اقدامات امنیتی مرتبط با آن و اختیارات نظارتی بر DNS (سیستم آدرس دهی اینترنتی جهانی) را حفظ نموده است (Creemers R. , 2021).

• کمیته فنی استانداردسازی امنیت اطلاعات ملی^۴

کمیته فنی استانداردسازی امنیت اطلاعات ملی (کمیته فنی ۲۶۰)^۵ مرجع ارزیابی و تست استانداردهای حوزه فناوری اطلاعات و ارتباطات است. نقش اصلی آن اجرای قانون امنیت سایبری در سازمان ها، شرکت های خصوصی و ارگان های دولتی، با استفاده از دستورالعمل های اجرایی، اقدامات فنی، چارچوب های انطباق و استانداردها می باشد. چارچوب استانداردسازی امنیت سایبری چین از چندین کمیته استانداردسازی دیگر، مانند انجمن استانداردسازی ارتباطات (CCSA)^۶ و کمیته فنی استانداردسازی صنعت رمزنگاری (CISTC)^۷ تشکیل شده است (Bozhkov, 2020).

1. The Ministry of Industry and Information Technology (MIIT)

2. Made in China 2025

3. Internet+

4. The National Information Security Standardization Technical Committee

5. Technical Committee 260 (TC260)

6. the Communication Standardization Association (CCSA)

7. the Cryptography Industry Standardisation Technical Committee (CISTC)

• وزارت امور خارجه

وزارت امور خارجه (به‌ویژه اداره کنترل تسلیحات و خلع سلاح^۱ و اداره معاهده و قانون^۲) دیپلماسی سایبری و قانون‌گذاری بین‌المللی فضای سایبری را پوشش می‌دهد. وزارت امور خارجه، یکی از نویسندگان استراتژی ۲۰۱۷ چین در زمینه همکاری بین‌المللی در فضای سایبری و مجری خط سیاستی رسمی حزب در دیپلماسی سایبری چین است. نمایندگان وزارت امور خارجه در اداره کنترل تسلیحات و خلع سلاح، تلاش‌های چین را در کمیته اول سازمان ملل متحد رهبری و هماهنگ کرده‌اند و دیدگاه‌های پکن را در تمام دوره‌های گروه کارشناسان دولتی بین سال‌های ۲۰۰۴ تاکنون نمایندگی نموده‌اند (Ibid).

وزارت امور خارجه باهدف مدیریت دیپلماسی سایبری، همانند اداره هماهنگ‌کننده امور سایبری وزارت امور خارجه ایالات متحده^۳، یک بخش سایبری تأسیس کرده است. همچنین این وزارتخانه مشارکت کشور در فرایندهای گفتگوی سازمان ملل برای توسعه هنجارهای بین‌المللی فضای سایبری را رهبری کرده و نهادهای تخصصی مرتبط با این حوزه را توسعه داده است (Creemers, 2021). علاوه بر این، وزارت امور خارجه گفتگوهای سایبری Track 1 را با مقامات ارشد اتحادیه اروپا (مانند کارگروه سایبری اتحادیه اروپا و چین) هماهنگ نموده است. این سازمان دهی و نظارت بر گفتگوهای Track 1.5 (گفت‌وگوی سایبری چین و اروپا) نیز وجود داشته است و وزارت خارجه اغلب نقش تسهیل‌کننده را در گفتگوهای دوجانبه درباره فضای سایبری ایفا کرده است (Bozhkov, 2020).

• ارتش آزادی‌بخش خلق چین (PLA)^۴

ارتش چین در گذشته مسئول جمع‌آوری سایبری اطلاعات صنعتی بود (به‌ویژه، اداره سوم ستاد کل ارتش). امروزه، نیروی پشتیبانی استراتژیک جدید ارتش چین بر توسعه قابلیت‌های نفوذ تهاجمی چین، دفاع سایبری، شناسایی اطلاعات نظامی و بهره‌برداری سایبری نظارت می‌کند. در نتیجه اصلاحات نیروی پشتیبانی استراتژیک (SSF) در سال ۲۰۱۵ که قابلیت‌های فضایی، سایبری و جنگ اطلاعاتی را یکپارچه کرد، اکنون ارتش تمرکز اندکی بر سناریوهای شناسایی و درگیری‌های سایبری و دفاع از

1. The Department of Arms Control and Disarmament

2. the Department of Treaty and Law

3. Office of the Coordinator for Cyber Issues

4. The People's Liberation Army of China (PLA)

زیرساخت‌های حیاتی دارد. علاوه بر این، ارتش متعهد شده است که اطلاع‌رسانی نیروهای مسلح خود و دفاع سایبری و ظرفیت‌های شناسایی نفوذ شبکه‌ای خود را به منظور حفظ ارتقای امنیت دولتی، حاکمیت ملی، امنیت اطلاعات و ثبات اجتماعی بهبود بخشد (China's National Defense in the New Era, 2019).

بازیگران بخش خصوصی

• شرکت نرم‌افزاری چیهو۳۶۰ (Qihoo 360)

چیهو۳۶۰ پیشروترین شرکت خصوصی امنیت سایبری چین است. این مرکز اولین شرکت نوآوری امنیت سایبری غیرنظامی چین را تحت نظارت کمیسیون مرکزی توسعه یکپارچه نظامی و غیرنظامی^۱ و ارگان‌های نظامی مرتبط اداره می‌کند. همراه با دیگر شرکت‌های خصوصی امنیت سایبری چینی، چیهو نقش حیاتی در ایجاد سیستم‌های دفاع سایبری در سرویس‌های اینترنتی مرتبط با ارتش چین ایفا می‌کند و نقش اطلاعاتی یکپارچه‌ای را ایفا می‌کند که آگاهی موقعیتی ارتش چین را در مورد تهدیدات سایبری افزایش می‌دهد (China Unveils Its First Civil-Military Cybersecurity Innovation Center, 2017).

• BATJ (یا GAFA^۲ چین)

بایدو^۳، علی‌بابا^۴، تنسنت^۵ و جی‌دی. کام^۶ چهار شرکت قدرتمند ارائه‌دهنده برنامه‌های کاربردی وب در چین هستند. آنها از نظر ارزش و نفوذ با شرکت‌های آمریکایی رقابت می‌کنند و نقش حیاتی در مدیریت و کنترل فضاهای اطلاعات عمومی دارند. هر چهار شرکت فناوری که در جستجو (بایدو)، تجارت الکترونیک (علی‌بابا و جی‌دی. کام)، رسانه‌های اجتماعی و بازی‌های موبایلی (تنسنت) فعالیت

1. the Central Commission for Integrated Military and Civilian Development

۲. چهار شرکت بزرگ و غول فناوری آمریکا شامل گوگل، اپل، فیسبوک و آمازون موسوم به گافا (GAFA)

3. Baidu

4. Alibaba

5. Tencent

6. JD.com

می‌کنند، کسب‌وکار خود را در اواخر دهه ۱۹۹۰ یا اوایل دهه ۲۰۰۰ آغاز کردند. با این حال، چهار شرکت فناوری چینی چیزی فراتر از شرکت‌های جستجو، تجارت الکترونیک یا رسانه‌های اجتماعی هستند. در طول دود دهه گذشته، هریک از آنها امپراتوری دیجیتالی بسیار پیچیده‌ای را ایجاد کرده‌اند و توانایی‌های خود را تقریباً در هر جنبه‌ای از اقتصاد سیاسی چین گسترش داده‌اند.

با به دست آوردن موقعیت مسلط در بازار چین، این چهار شرکت به طور فزاینده‌ای به بازارهای بین‌المللی نیز توجه داشته‌اند و به طور فعال درگیر خرید سهام جهانی برخی شرکت‌ها بوده‌اند. به عنوان مثال، علی‌بابا، پس از ثبت عرضه اولیه بی‌سابقه سهام ۲۵ میلیارد دلاری خود در سال ۲۰۱۴، یک میلیارد دلار برای خرید سهام گروه لازادا (Lazada)، بزرگ‌ترین شرکت تجارت الکترونیک در جنوب شرقی آسیا، هزینه کرد. بایدو، به طور مشابه، سرمایه‌گذاری ۶۰۰ میلیون دلاری را در سال ۲۰۱۴ در اوپر (Uber)، شرکت تاکسی اینترنتی مستقر در ایالات متحده، انجام داد. در اواسط سال ۲۰۱۶، تنسنت رهبری یک گروه سرمایه‌گذاری را برای خرید ۸۴ درصد از شرکت فنلاندی بازی‌های موبایل سوپرسل (Supercell) به قیمت ۸٫۶ میلیارد دلار بر عهده گرفت (Shen, 2019).

• هوای وزدتی‌ایی

هوآوی (Huawei) شرکتی است که بیشترین ثبت اختراع و نوآوری را در فناوری 5G دارد و شرکتی است که غالباً کم‌هزینه‌ترین گزینه در ساخت سیستم 5G به حساب می‌آید. این شرکت یکی از قهرمانان ملی چین است، یک شرکت خصوصی که توسط عضو حزب کمونیست چین و افسر سابق ارتش آزادی بخش خلق، رن ژنگفی^۱، اداره می‌شود (Moore, 2023).

شرکت زدتی‌ای (ZTE) نیز یک سازنده بزرگ تجهیزات مخابراتی چینی است که در شنژن، استان گوانگدونگ مستقر است. سه تجارت اصلی این شرکت شامل تجهیزات مخابراتی، تلفن‌های هوشمند و سایر پایانه‌های تلفن همراه و همچنین خدمات سیستمی مشابه هوآوی است. این شرکت همچنین به بازارهای خارجی نیز نفوذ کرده است و تجارت خارجی آن حدود ۵۰ درصد از کل فروش شرکت را تشکیل می‌دهد. زدتی‌ای که در سال ۱۹۸۵ تأسیس شده است، در اصل یک شرکت دولتی و تحت کنترل شهرداری شنژن بود. این شرکت در سال ۱۹۹۷ در بورس اوراق بهادار شنژن و در سال ۲۰۰۴ در بورس و

1. Ren Zhengfei

اوراق بهادر هنگ کنگ فهرست شده است. از اواخر مارس ۲۰۱۵، ژونگ شینگ شین (Zhongxingxin)، یک نهاد دولتی، بزرگ‌ترین سهامدار این شرکت شده است و حدود ۳۰ درصد از سهام شرکت را در اختیار دارد. (ZTE Corp., n.d.)

برخی خارج از چین معتقدند که این کشور در صدور رویکرد خود در زمینه حاکمیت سایبری فراتر از مرزهای خود عمل می‌کند و از هواوی، زدتی‌ای و سایر شرکت‌های چینی برای انجام این امر استفاده نموده است. به نظر می‌رسد که حزب کمونیست چین اکنون تصمیم گرفته است که حاکمیت سایبری که به عنوان اینترنت با ویژگی‌های چینی شناخته می‌شود و معتقد است حاکمیت اینترنت باید هنجار پیش فرض در سراسر جهان باشد را مناسب برای صدور به دیگر کشورها ببیند. اقدام چین برای کمک به روسیه و سایر کشورها برای ساختن نسخه خود از نمونه فایروال چین نیز ممکن است یک مصداق برای این رویکرد باشد (Moore, 2023).

مؤسسات تحقیقاتی و دانشگاهی

مؤسسات تحقیقاتی زیر با درجات مختلفی با دستگاه سیاست خارجی چین در ارتباط هستند. سازمان‌ها و آژانس‌های سیاست خارجی برجسته چین، مانند وزارت امور خارجه، وزارت امنیت کشور، سازمان‌های نظامی، نهادهای محلی و خود حزب، همگی مؤسسات تحقیقاتی خود را مدیریت می‌کنند که در سطوح مختلف سیاست‌گذاری فضای سایبری حضور دارند.

• آکادمی فناوری اطلاعات و ارتباطات چین (CAICT)^۱

آکادمی فناوری اطلاعات و ارتباطات چین در سال ۱۹۵۷ تأسیس شده است و یک مؤسسه تحقیقاتی علمی است که مستقیماً زیر نظر وزارت صنعت و فناوری اطلاعات چین فعالیت می‌کند. آکادمی متعهد به توانمندسازی برای نوآوری و توسعه جامعه اطلاعاتی امروزی است. این مؤسسه از استراتژی‌ها، برنامه‌ها، سیاست‌ها، استانداردها، آزمون‌ها و گواهی‌نامه‌ها برای توسعه و کاربست

1. The China Academy of Information and Communications Technology (CAICT)

فناوری اطلاعات و ارتباطات پشتیبانی می‌کند. بدین ترتیب می‌توان گفت آکادمی تسهیل‌کننده مهمی در توسعه و نوآوری بخش اطلاعات و ارتباطات چین می‌باشد.

در سال‌های اخیر، با هدف انطباق با الزامات جدید اقتصادی اجتماعی، آکادمی تلاش‌های خود را در زمینه نوآوری برای دستیابی به چشم‌انداز تحقیقاتی گسترده‌تر تقویت کرده است. در این راستا این مؤسسه تحقیقات دقیق و برنامه‌ریزی آینده‌پژوهانه در زمینه‌های 5G، اینترنت صنعتی، اینترنت اشیا (IoT)، اینترنت وسایل نقلیه (IoV)، رایانش ابری، بلاک‌چین، هوش مصنوعی (AI)، واقعیت مجازی/واقعیت افزوده (VR/AR) و امنیت سایبری و امنیت اطلاعات انجام داده است. این امر آکادمی را قادر ساخته است تا نقش مهمی در مطالعه استراتژی، نوآوری فناوری و همکاری‌های بین‌المللی مرتبط با بخش فناوری اطلاعات ایفا نماید (Academy Profile, n.d.).

آکادمی همچنین نماینده چین در همکاری با صنایع آلمان است که در قالب طرح "صنایع چین و آلمان ۲۰۴۰" شکل گرفته است که منجر به توسعه تولید هوشمند و توسعه یک سیستم آدرس دهی دیجیتال برای اینترنت صنعتی در چین شده است (Lee, The Connection of Everything: China and the Internet of Things, 2021).

• مؤسسه روابط بین‌الملل معاصر چین (CICIR)^۱

مؤسسه روابط بین‌الملل معاصر چین یک اندیشکده است که مستقیماً به وزارت امنیت کشور وابسته است. این مؤسسه به حوزه سیاست خارجی و روابط بین‌الملل می‌پردازد و اغلب در گفتگوهای با اندیشکده‌های خارجی در گفتگوهای Track 1.5 حضور داشته است.

مؤسسه مطالعات بین‌المللی شانگهای (SIIS)^۳ (در ارتباط با وزارت امور خارجه چین و شهرداری شانگهای)، مؤسسه مطالعات بین‌المللی چین (CIIS)^۴ (وابسته به وزارت امور خارجه چین) آکادمی علوم اجتماعی چین (CASS)^۵ (زیر مجموعه شورای دولتی چین و بزرگ‌ترین اندیشکده دولتی در این

1. the Sino-German Industrie 4.0

2. The China Institutes of Contemporary International Relations (CICIR)

3. The Shanghai Institute for International Studies (SIIS)

4. The China Institute of International Studies (CIIS)

5. The Chinese Academy of Social Sciences (CASS)

کشور)، آکادمی علوم نظامی ارتش آزادی‌بخش خلق چین (CAMS)^۱، مؤسسه مطالعات استراتژیک بین‌المللی چین (CISS)^۲ و دانشگاه دفاع ملی (NDU)^۳ نیز اندیشکده‌هایی هستند که با موضوعات دیپلماسی سایبری سروکار دارند (Bozhkov, 2020).

1. The Chinese Academy of Military Sciences of the People's Liberation Army (CAMS)
2. the China Institute for International Strategic Studies (CISS)
3. the National Defence University (NDU)

اقدامات چین در دیپلماسی سایبری

گفتمان حزب کمونیست چین عموماً مقررات بین‌المللی و رژیم‌های حقوقی را بقایای زمانی تفسیر می‌کند که چین موقعیت نهادی و تکنولوژیکی را که از طریق آن قادر به تصمیم‌گیری در مورد قوانین جهانی باشد، نداشت؛ بنابراین اصلاحات کلیدی می‌تواند صدای بین‌المللی چین و کشورهای در حال توسعه را تقویت کند که متعاقباً به آنها اجازه می‌دهد تا از حاکمیت، فرهنگ‌ها، زمینه‌های سیاسی و منافع خود در تصمیم‌گیری در باره نحوه مدیریت فضای سایبری استفاده کنند. از این رو چین سعی نموده است تا از طریق مشارکت در بحث‌های سایبری بین‌المللی، مقابله با تروریسم سایبری، دیپلماسی اقتصادی حوزه فناوری اطلاعات و ارتباطات و گفتگوهای دوجانبه اهداف خود در دیپلماسی سایبری را دنبال نماید.

مشارکت و نقش‌آفرینی در نهادهای بین‌المللی

چشم‌انداز یک ابرقدرت سایبری فراتر از داشتن توانایی پیشرفته در فناوری، به نقش‌آفرینی در قلمرو هنجاری، گفتمانی و عقیدتی نیاز دارد. شی در سال ۲۰۱۶ تأکید کرد که عنصر اصلی جاه‌طلبی

بین‌المللی چین، شامل تقویت صدای گفتمانی جهانی، نفوذ آن و حق صحبت چین در بحث‌های تنظیم استانداردها و مقررات و هنجارهای بین‌المللی برای کمک به ایجاد نظمی در فضای سایبری بین‌المللی است که برای سیاست خارجی و ارتقای منافع ملی چین مفید باشد.^۱

پکن مشارکت خود در شکل‌دهی استانداردها و رفتار قابل قبول در حوزه سایبری را به عنوان یک مزیت استراتژیک ابزاری می‌پندارد. شی دریافت‌هسته است که حتی در فضای سایبری، رقابت استراتژیک بین دولت‌های قدرتمند، مستلزم یک نفوذ متشکل از عوامل مادی و گفتمانی است که در آن توزیع نسبی قدرت با توانایی دولت‌ها برای حفظ رهبری تکنولوژیک و القای استانداردهای داخلی، ایده‌ها و قدرت گفتمانی تعیین می‌شود (Building China's International Cyberspace Discourse Power, 2016). در زمینه رقابت فزاینده بر سر ایده‌ها در بحث‌های بین‌المللی، کمیته مرکزی حزب کمونیست چین از دولت خواسته است تا برای پیشبرد منافع چین در آینده، اقدامات بیشتری در حوزه تدوین و توسعه حقوق بین‌الملل انجام دهد. پیرو این منطق، دیپلمات‌ها، حقوق‌دانان و دانشمندان چینی تشویق می‌شوند تا در تدوین هنجارهای بین‌المللی با هدف تقویت قدرت گفتمانی و نفوذ پکن در امور حقوقی بین‌المللی مشارکت فعال داشته باشند.^۲

جوامع فنی، سازمان‌های دولتی و خصوصی تشویق می‌شوند تا مشارکت خود را در چشم‌انداز استانداردسازی فناوری‌های نوظهور جهانی افزایش دهند. ارتقای استانداردسازی در نهادهای بین‌المللی از جمله سازمان بین‌المللی استاندارد (ISO) هسته اصلی سیاست‌های صنعتی پکن مانند ساخت چین ۲۰۲۵، جاده ابریشم دیجیتال و استانداردهای چین ۲۰۳۵ است (Kristin Shi-Kupfer, Mareike Ohlberg, 2019).

۱. برای اطلاع بیشتر رجوع کنید به:

https://web.archive.org/web/20190115054041/http://www.cac.gov.cn/2016-10/09/c_1119682237.htm

۲. برای اطلاع بیشتر رجوع کنید به:

"CCP Central Committee Decision Concerning Some Major Questions in Comprehensively Moving Governing the Country According to the Law Forward." China Copyright and Media, 28 Oct. 2014, <https://chinacopyrightandmedia.wordpress.com/2014/10/28/ccp-central-committee-decision-concerning-some-majorquestions-in-comprehensively-moving-governing-the-country-according-to-the-law-forward/>

در پیوند با فرایند نهادینه‌سازی دیپلماسی سایبری چین، به معنای ایجاد آژانس‌ها و موقعیت‌های جدید و اجرای اصلاحات سازمانی داخلی، جمهوری خلق چین به تدریج مشارکت خود را در انجمن‌های مختلف موضوع محور و چندذی‌نفعی مانند یانا (IANA)^۱، آیکن (ICANN)^۲، کارگروه مهندسی اینترنت (IETF)^۳ و مجمع حکمرانی اینترنت (IGF)^۴ گسترش داده است. دیپلمات‌های چینی که به طور گسترده‌ای از نگرانی‌های حکمرانی اینترنت آگاه هستند، تلاش‌های خود را در راستای برهم‌زدن انحصار واشنگتن بر زیرساخت‌های حیاتی اینترنت متمرکز کرده‌اند. کنار گذاشتن کنترل نظارتی ایالات متحده آمریکا بر یانا (IANA) تحت فشار پکن نمونه‌ای از این موارد است (Why is America giving up control of ICANN?, 2016).

• نقش آفرینی در مجمع عمومی سازمان ملل متحد

شاید بتوان گفت جاه طلبانه‌ترین تلاش چین برای هنجارسازی شامل دو پیشنهاد به مجمع عمومی در غالب "پیش‌نویس آیین‌نامه رفتار بین‌المللی برای امنیت اطلاعات"^۵ بود که در

۱. مرجع واگذاری اعداد در اینترنت (Internet Assigned Numbers Authority)، نهادی است که مسئولیت آدرس‌های پروتکل اینترنت (IP Address) و سیستم خودگردان (Autonomous System) تخصیص داده شده، مدیریت منطقه ریشه سامانه نام دامنه (DNS root zone)، ساختار رسانه هادر اینترنت (Internet Media Type) یا همان MIME type، و وظایف مربوط به پروتکل‌های اینترنتی دیگر را به عهده دارد. این کارها به وسیله آیکن اداره می‌شود.

۲. آیکن (Internet Corporation for Assigned Names and Numbers) مخفف عبارت شرکت اینترنتی تخصیص نام‌ها و شماره‌ها است که یک شرکت غیرانتفاعی در ایالات متحده آمریکا است که مسئولیت مدیریت واگذاری نام‌های دامنه و آدرس‌های پروتکل اینترنت را به عهده دارد. آیکن یک شرکت بین‌المللی است که تحت نفوذ نظام دولتی کشور آمریکا بوده و مقرآن در ایالت کالیفرنیا است.

۳. کارگروه مهندسی اینترنت (Internet Engineering Task Force)، سازمانی است که استانداردهای اینترنت را ایجاد کرده و بهبود می‌بخشد.

۴. مجمع حکمرانی اینترنت (Internet Governance Forum) یکی از مهم‌ترین نتایج اجلاس جهانی سران درباره جامعه اطلاعاتی بود که از ۱۶ تا ۱۸ نوامبر ۲۰۰۵ در تونس برگزار شد. هدف اصلی این مجمع، بحث بر سر مسائل مرتبط با حاکمیت اینترنت و در صورت امکان ارائه توصیه‌هایی برای جامعه جهانی است.

5. the international Code of Conduct for Information Security

سال‌های ۲۰۱۱ و ۲۰۱۵ همراه با روسیه و اعضا سازمان همکاری‌های شانگهای (SCO) ارائه شد. این آئین‌نامه، تهدیدات سایبری بالقوه را در زمینه امنیت بین‌المللی به عنوان موضوعات امنیت اطلاعات، یعنی استفاده از فناوری‌های ارتباطی اطلاعات برای بی‌ثبات سازی، مداخله، حمله یا خرابکاری، برهم زدن امنیت اجتماعی، سیاسی و اقتصادی و ایجاد اختلال در نظم عمومی سایر دولت‌ها در نظر گرفت. این پیشنهاد بر اساس اصل حاکمیت دولت‌ها بر فضای سایبری الگوبرداری شده بود و دولت‌ها را ملزم می‌کرد از فضاهای اطلاعاتی و زیرساخت‌های اطلاعاتی حیاتی خود با اعمال قوانین و مقررات ملی سختگیرانه محافظت کنند.^۲ علاوه بر این، با تردید نسبت به نقش بازیگران غیردولتی و خصوصی در فرآیندهای چند ذی‌نفعی موجود، آئین‌نامه رفتار سال ۲۰۱۵ همچنین به دنبال ایجاد مکانیسم‌های حاکمیت بین‌المللی اینترنت چندجانبه، شفاف و دموکراتیک بود، که به دولت‌ها برای تعیین خط‌مشی عمومی مرتبط با اینترنت اختیارات گسترده‌ای می‌داد. به طور مشابه، در سال ۲۰۱۶، اعضای بریکس (BRICS)^۳ برای تقویت قدرت تصمیم‌گیری دولت‌ها به عنوان مجریان اصلی سیاست‌گذاری فضای سایبری بحث کردند و نقش سایر سهامداران غیردولتی را به نقش ارائه‌دهندگان پیشنهاد در تصمیم‌گیری‌ها تقلیل دادند (8th BRICS Summit, 2016).

۱. سازمان همکاری‌های شانگهای (Shanghai Cooperation Organisation)، سازمانی میان‌دولتی است که برای همکاری‌های چندجانبه امنیتی، اقتصادی و فرهنگی تشکیل شده است. این سازمان در سال ۲۰۰۱ توسط رهبران چین، روسیه، قزاقستان، قرقیزستان، تاجیکستان و ازبکستان با هدف برقرار کردن موازنه در برابر نفوذ آمریکا و ناتو در منطقه، پایه‌گذاری شد. سازمان همکاری‌های شانگهای در حقیقت ترکیب جدید سازمان «شانگهای ۵» است که در سال ۱۹۹۶ تأسیس شده بود، ولی نام آن پس از عضویت ازبکستان به سازمان همکاری‌های شانگهای تغییر داده شد.

۲. برای اطلاع بیشتر رجوع کنید به:

An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?

<https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/>

۳. بریکس (BRICS) نام گروهی از کشورها به رهبری قدرت‌های اقتصادی نوظهور است و عنوان آن کوتاه نوشتی است که از به هم پیوستن حروف اول نام انگلیسی آن کشورها یعنی برزیل، روسیه، هند، چین و آفریقای جنوبی ساخته شده است.

- نقش آفرینی در اتحادیه بین‌المللی مخابرات (ITU)^۱

پکن همواره در تلاش بوده است تا حاکمیت اینترنت را تحت چارچوب نهادهای وابسته به سازمان ملل متحد قرار دهد. در کنفرانس جهانی ارتباطات بین‌المللی^۲ در سال ۲۰۱۲ در دبئی، چین به همراه روسیه، عربستان سعودی و چندین دولت دیگر خواهان ارتقای نقش اتحادیه بین‌المللی مخابرات بر نهادهای چند ذی‌نفعی مانند کارگروه مهندسی اینترنت، از طریق گسترش اختیارات این اتحادیه و کشورهای عضو بر منابع اینترنت و سیاست‌گذاری آن بودند (Blue, 2012).

علاوه بر این پیشنهاد اصلاح معاهده مقررات بین‌المللی ارتباطات راه دور (ITR)^۳ در سال ۲۰۱۲ می‌توانست کنترل و نظارت دولتی را مشروعیت بخشد و نقش چندجانبه‌ایکن را در تخصیص و مدیریت DNS (سیستم آدرس دهی اینترنتی جهانی) تضعیف کند. ۸۹ دولت، طرح اصلاح را باهدف گسترش کنترل دولتی بر اینترنت امضا کردند. کشورهایی از جمله ایالات متحده، کانادا و فرانسه اساساً با اصلاحیه‌های پیشنهادی که به اتحادیه بین‌المللی مخابرات اجازه می‌داد وظایف حاکمیتی را که پیش از آن تحت اختیار نهادهای غیردولتی بود را بدست گیرد، مخالفت کردند (Kehl, Danielle, and Tim Maurer, 2012). در ادامه نقش آفرینی پکن در اتحادیه، در نوامبر ۲۰۱۸، در بیستمین نشست کنفرانس تام‌الاختیار اتحادیه بین‌المللی مخابرات^۴ در دبئی، کشورهای عضو اتحادیه، هولین ژائو^۵، یک شهروند چینی را برای دومین دوره چهار ساله خود به عنوان دبیرکل اتحادیه انتخاب کردند، که این دوره در اول ژانویه ۲۰۲۳ به پایان رسید.

- نقش آفرینی در شرکت اینترنتی تخصیص نام‌ها و شماره‌ها (ICANN)

۱. اتحادیه بین‌المللی مخابرات (International Telecommunication Union) یک سازمان بین‌المللی وابسته به سازمان ملل متحد است. این اتحادیه وظیفه قانون‌گذاری و نیز مدیریت فضای فرکانسی، تدوین استانداردهای تبادل داده و اطلاعات و همچنین کمک به رشد و توسعه ارتباطات در سراسر جهان را بر عهده دارد.

2. the World Conference on International Telecommunications

3. the International Telecommunications Regulations (ITR)

4. the ITU's Plenipotentiary Conference (PP-18)

5. Houlin Zhao

دیپلماسی سایبری پکن همچنین بر آنچه رهبران و تحلیلگران چینی تحت عنوان توزیع نابرابر منابع اینترنتی، کنترل آمریکا بر مرجع واگذاری اعداد در اینترنت (IANA) و قرارداد با شرکت اینترنتی تخصیص نام‌ها و شماره‌ها موسوم به آیکن (ICANN) می‌دانستند، متمرکز بوده است. همان‌طور که محقق چینی، لو چوانینگ توضیح می‌دهد، ایالات متحده عملاً کنترل کاملی بر تدوین و مدیریت استانداردهای اینترنت در همه سازمان‌های بین‌المللی و صنایع اصلی داشت و از بین‌المللی کردن وظایف و مدیریت مربوطه یا واگذاری اختیارات به یک آژانس تخصصی تحت کنترل سازمان ملل متحد خودداری کرده است (Chuanying, 2016).

در واکنش به نفوذ گسترده ایالات متحده آمریکا در فضای اینترنت، چین در نشست مقدماتی در اولین اجلاس جهانی سران در باره جامعه اطلاعاتی^۱ در سال ۲۰۰۳، خواستار جایگزینی الگوی حکمرانی چندجانبه از طریق انعقاد یک معاهده بین‌المللی اینترنت و تشکیل یک سازمان اینترنت بین‌الدولی شد (Mueller, 2010).

• نقش آفرینی در گروه کارشناسان دولتی سازمان ملل متحد (GGE)^۲

سازمان ملل برای اولین بار بررسی مسائل مربوط به امنیت سایبری را پس از ارائه پیش‌نویس قطعنامه روسیه در سال ۱۹۹۸ به کمیته اول مجمع عمومی سازمان ملل (کمیته خلع سلاح و امنیت بین‌المللی) ارجاع داد. کمیته اول، اولین گروه کارشناسان سایبری را در سال ۲۰۰۴ ایجاد نمود. چین در این ابتدا یک شرکت‌کننده منفعل بود و نمایندگان آن در جلسات ۲۰۰۴-۲۰۰۵ از وزارت ارتباطات آمدند، نه وزارت خارجه، که نشان دهنده کم اهمیت بودن این نشست برای حزب کمونیست چین بود. با این حال، در سال ۲۰۰۹، شروع فعالیت گسترده ایالات متحده آمریکا در زمینه ترویج مقررات بین‌المللی در فضای سایبری، موجب شد چین، در دوره‌های بعدی مذاکرات، دیپلمات‌های با سابقه‌تری را برای حضور در این گروه بفرستد (Segal, 2017).

جلسات اول و دوم گروه کارشناسان دولتی سازمان ملل متحد نتوانست به یک تفاهم و نقطه مشترک دست پیدا کند. در ژوئن ۲۰۱۳، برای اولین بار، گروه کارشناسان به اجماع رسید. اعضای این گروه

1. the World Summit on the Information Society (WSIS)

2. The UN Group of Governmental Experts (GGE)

که شامل نمایندگانی از چین، روسیه، ایالات متحده و دوازده کشور دیگر بود^۱، توافق کردند که مقررات بین‌المللی و به‌ویژه منشور سازمان ملل متحد، در فضای سایبری نیز اعمال می‌شود. در این گزارش همچنین آمده است که حاکمیت دولت و هنجارها و اصول بین‌المللی که از حاکمیت سرچشمه می‌گیرد، در رفتار دولتها اعمال می‌شود^۲. در پی این تصمیم، مقامات ایالات متحده آمریکا از این اجماع استفاده کردند تا استدلال کنند که با این موافقت علاوه بر منشور سازمان ملل، کنوانسیون ژنو و حقوق مخاصمات مسلحانه (LOAC)^۳ نیز در فضای سایبری قابل اعمال می‌باشد. به نظر می‌رسد امضای توافقنامه ۲۰۱۲-۲۰۱۳ توسط چین، یک تصمیم دیپلماتیک ناآگاهانه و برنامه‌ریزی نشده بوده است. بر اساس برخی اظهارات، نماینده چین به دلیل اینکه نگران بود تا روایتی از ناسازگاری چین در رسانه‌ها مطرح شود و اجلاس راتحت الشعاع قرار دهد، این توافقنامه را تایید کرد (Segal, 2017).

مقامات چینی پس از پایان نشست گروه در سال ۲۰۱۳، استقبال گروه کارشناسان دولتی از اقتدار دولت را برجسته کردند، نه پیامدهای حقوق بین‌الملل ناشی از پذیرش منشور سازمان ملل در فضای سایبری. به عنوان مثال، در اواخر سال ۲۰۱۳، لووی^۴، که در آن زمان رئیس اداره اطلاعات اینترنتی دولتی چین بود، شروع به ترویج حاکمیت سایبری به عنوان محوری‌ترین موضوع در رویکرد چین در مورد فضای سایبری و به عنوان مبنایی برای همکاری‌های بین‌المللی نمود. در تصور لو، حاکمیت مفهومی در حال تکامل بود؛ همان‌طور که قرن هفدهم شاهد گسترش حاکمیت ملی بر بخش‌هایی از دریا و قرن بیستم بر حریم هوایی بودیم، اکنون حاکمیت ملی به فضای سایبری نیز تعمیم یافته است.

۱. تعداد کشورهای عضو گروه کارشناسان دولتی، در قطعنامه معین و مشخص نشده است و اصولاً عدد معین و مقطوعی نیست. اما در چند گروه کارشناسان دولتی که تاکنون در مجمع عمومی با موضوع امنیت سایبری تشکیل شده است، تعداد کشورهای عضو گروه، بین ۱۵ تا ۲۵ کشور، متغیر بوده است. دبیرکل سازمان ملل متحد، کشورهای عضو گروه را مشخص می‌کند.

۲. برای اطلاع بیشتر رجوع کنید به:

“Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,” United Nations General Assembly, June 24, 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=E

3. Law of armed conflict (LOAC)

4. Lu Wei

سرویس‌های اطلاعاتی می‌توانند از مرزها عبور کنند، اما فضای سایبری نمی‌تواند بدون حاکمیت به بقای خود ادامه دهد (Segal A. , 2013).

نشست ۲۰۱۴-۲۰۱۵ گروه کارشناسان دولتی، وظیفه بررسی هنجارها، مقررات و اصول مربوط به رفتار مسئولان دولت‌ها و همچنین نحوه اعمال مقررات بین‌المللی در استفاده از فناوری‌های اطلاعات و ارتباطات توسط دولت‌ها را بر عهده داشت. چین به همراه روسیه در سال ۲۰۱۵ برای حفاظت و گسترش بیانیه هنجار حاکمیت تلاش کردند. گزارش ۲۰۱۵ ضمن تایید مجدد مقررات قبلی، شامل بخش دیگری با عنوان "نحوه اعمال مقررات بین‌المللی در زمینه استفاده از فناوری اطلاعات و ارتباطات" بود، که این ایده‌ها را توسعه می‌دهد و اشاره می‌کند که «دولت‌ها باید اصول حقوق بین‌الملل از جمله حاکمیت دولت، برابری حاکمیت، حل و فصل اختلافات از طریق مسالمت‌آمیز و عدم مداخله در امور داخلی سایر کشورها را رعایت کنند»^۱.

پکن و مسکو چهار هنجار پیشنهادی واشنگتن در گزارش سال ۲۰۱۵ را امضا کردند. این گزارش هنجاری، مسئولیت و وظیفه دولت برای ترویج این امر که دولت‌ها نباید عمداً به زیرساخت‌های حیاتی دیگران آسیب بزنند یا تیم‌های واکنش اضطراری رایانه‌ای را در زمان صلح هدف قرار دهند، را مورد تایید قرار داد. اما چین و روسیه، همراه با پاکستان، مالزی و بلاروس، با تلاش ایالات متحده برای گنجاندن ارجاع به ماده ۵۱ منشور سازمان ملل، که استفاده از زور را برای دفاع از خود در برابر حمله مسلحانه مجاز می‌داند، مخالفت کردند (Mark, 2015). تحلیلگران چینی این استدلال را مطرح می‌کنند که چنین اقدامی فضای سایبری را نظامی می‌کند. آنها همچنین نگران این موضوع هستند که ایالات متحده از مقررات بین‌المللی به عنوان توجیهی برای انجام حملات تلافی جویانه استفاده کند (Harold, S. W., Libicki, M. C., & Cevallos, A. S., 2016).

گزارش ۲۰۱۴-۲۰۱۵ همچنین اشاره می‌کند که اگرچه دولت‌ها باید به تعهدات خود در قبال اعمال غیرقانونی بین‌المللی منتسب به آن‌ها عمل نمایند، به این نکته اشاره می‌کند که اینکه یک فعالیت

۱. برای اطلاع بیشتر رجوع کنید به؛

سایبری از قلمرو یا زیرساخت فناوری اطلاعات و ارتباطات یک کشور نشأت گرفته باشد، به خودی خود برای نسبت دادن آن اقدام به آن دولت کافی نمی‌باشد. با توجه به این چالش، گزارش نتیجه می‌گیرد که اتهامات سازماندهی و یا انجام اقدامات خلاف مقررات بین‌المللی علیه کشورها باید بصورت دقیق اثبات شود.^۱

راهبرد بین‌المللی چین در سال ۲۰۱۷ در راستای بازتاب این نگرانی استدلال می‌کند که از آنجایی که «حملات سایبری معمولاً فراملی هستند و نسبت دادن آن دشوار است، کشورها باید با همکاری یکدیگر امنیت سایبری را از طریق مشاوره و همکاری سازنده تضمین نمایند» (International Strategy of Cooperation on Cyberspace, 2017).

• برگزاری کنفرانس جهانی اینترنت^۲

سازمان ملل متحد تنها مجمع برای توسعه هنجارهای بین‌المللی نبوده است؛ نشست‌های دیگری مانند کنفرانس لندن و برگزاری جلسات بعدی آن در سئول و لاهه نیز به فرایندی برای هنجارسازی در فضای سایبری تبدیل شده‌اند. این رویدادها که حد وسطی میان رویکرد چندجانبه سازمان ملل متحد و رویکرد چندذی‌نفعی مجمع حکمرانی اینترنت (IGF)^۳ هستند، بیشتر تحت سلطه ایالات متحده و کشورهای هم‌فکر آن قرار داشته‌اند و شامل بحث‌هایی درباره حقوق آنلاین و مزایای اقتصادی اینترنت باز بوده‌اند.

گسترش بحث‌های سایبری در این کنفرانس‌ها، پکن را تحریک نمود تا برای مقابله با تلاش‌های ایالات متحده و متحدان آن که با هدف گسترش تعاریف و انتظارات خود از رفتار غیرمسئولانه در فضای مجازی، تبلیغ طرح‌های حاکمیت اینترنت چندذی‌نفعی و اشباع کردن گفتمان از بحث‌هایی در مورد حقوق بشر دیجیتال انجام می‌شد، در نوامبر ۲۰۱۴، کنفرانس جهانی اینترنت خود را در ووژن، شهر تاریخی نزدیک هانگژو، محل مقر گروه علی بابا، برگزار کند. این رویداد که توسط اداره فضای سایبری

۱. برای اطلاع بیشتر رجوع کنید به؛

“Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”, United Nations General Assembly 22 July 2015

<https://documents.un.org/doc/undoc/gen/n15/228/35/pdf/n1522835.pdf?token=5yEY7BYB4xYgl2Fy7i&fe=true>

2. World Internet Conference

3. Internet Governance Forum (IGF)

چین سازماندهی شد، به عنوان ویتیرینی برای اقتصاد اینترنتی چین و به عنوان مجمعی برای ترویج دیدگاه پکن در مورد حاکمیت فضای سایبری نمود پیدا کرد (Segal A. , 2017). در بیانیه افتتاحیه این کنفرانس بیان شد که رئیس جمهور شی خواستار «سیستم حکمرانی چندوجهی، دموکراتیک و شفاف برای اینترنت بین المللی» می باشد (Bandurski, 2014).

در انتهای کنفرانس، سازمان دهندگان پیش نویس سندی را به شرکت کنندگان ارائه دادند. این سند شامل ۹ اصل بود که شامل تشویق تلاش های مشترک در زمینه امنیت سایبری و مبارزه با تروریسم سایبری، توسعه اقتصاد اینترنتی، افزایش ارتباطات و همچنین خواستار احترام به حق حاکمیت اینترنت همه کشورها بود. با این حال، بسیاری از شرکت کنندگان از امضای این سند خودداری کردند و کنفرانس بدون اعلامیه نهایی پایان یافت (Segal A. , 2017).

یک سال پس از این کنفرانس، چین اهمیت سیاسی و دیپلماتیک کنفرانس جهانی اینترنت را با ارائه نظرات خود در افتتاحیه دومین کنفرانس ووژن در سال ۲۰۱۵ نشان داد. شی در اظهارات خود استدلال کرد که همه باید به حق کشورها برای انتخاب مسیر مستقل توسعه سایبری خود، الگوی مقررات سایبری و سیاست های عمومی اینترنت و مشارکت در حکمرانی فضای سایبری بین المللی در شرایط برابر احترام بگذارند. وی ادامه داد: هیچ کشوری نباید به دنبال تبدیل شدن به هژمونی سایبری، مداخله در امور داخلی سایر کشورها یا شرکت و حمایت از فعالیت های سایبری که امنیت ملی دیگر کشورها را تضعیف می نماید، باشد. شی همچنین از مجمع حکمرانی اینترنت که به گفته وی نتوانسته بود منعکس کننده تمایلات و منافع اکثر کشورها باشد، انتقاد کرد (Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference, 2015).

چین همچنین سعی کرد با ایجاد یک کمیته مشورتی سطح بالا^۱، به ریاست مشترک فادی چهاده^۲، رئیس سابق آیکن (ICANN) و جک ما^۳، مدیر عامل علی بابا، بخشی از توان رویکرد چنددلی نفعی در

1. high-level advisory committee

2. Fadi Chehade

3. Jack Ma

حکمرانی اینترنت را نیز به کار گیرد. این کمیته به عنوان اولین اقدام خود، ابتکار ووژن^۱ را تصویب کرد که رویکردی چنددلی نفعی برای حاکمیت اینترنت بر اساس اصل حاکمیت دولت در فضای سایبری، ارائه کرد. این کمیته وظیفه داشت این پیام را در صحنه بین‌المللی تبلیغ کند و به اداره سایبری چین در مورد برنامه ریزی کنفرانس‌های آینده یاری رساند (McCarthy, 2015).

مقابله با تروریسم سایبری

دولت چین بر حمایت خود از همکاری بین‌المللی در مورد جرایم سایبری و تروریسم در سازمان ملل متحد در کمیسیون پیشگیری از جرم و عدالت کیفری (CCPCJ)^۲، دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد (ODC)^۳، مجمع منطقه‌ای آسیا آن (ARF)^۴، سازمان بریکس و سامان همکاری شانگهای تأکید نموده است (Bozhkov, 2020).

رویکردهای دیپلماتیک چین به تروریسم سایبری ناشی از تلاش‌های هنجارسازی در سازمان همکاری شانگهای بوده است. در حالی که سازمان شانگهای در ابتدا با هدف غیرنظامی کردن مرزها و ایجاد اعتماد در میان اعضاء شکل گرفته بود، دستور کار آن به ابتکارات اقتصادی و تهدیدات امنیتی غیرسنتی گسترش یافت. به ویژه، شانگهای بر سه تهدید عمده تمرکز کرده است: تروریسم، جدایی‌طلبی و افراط‌گرایی. ساختار منطقه‌ای ضدتروریستی سازمان شانگهای همکاری بین آژانس‌های سایبری مختلف در کشورهای عضو را هماهنگ می‌کند و پایگاه داده‌ای از اطلاعات مربوط به سازمان‌ها و فعالیت‌های تروریستی مشکوک را نگهداری می‌کند. در اکتبر ۲۰۱۵، چین اولین مانور مشترک ضدتروریسم اینترنتی خود را با نام Xiamen 2015 انجام داد. در این مانور، اعضای سازمان شانگهای بر روی بهبود اشتراک گذاری اطلاعات و هماهنگی فرامرزی باهدف پاسخ به بکارگیری یک گروه تروریستی شبیه سازی شده از رسانه‌های اجتماعی برای تحریک فعالیت‌های تروریستی، تمرین کردند (Wood, 2015).

1. the Wuzhen Initiative

2. the Commission on Crime Prevention and Criminal Justice (CCPCJ)

3. the United Nations Office on Drugs and Crime (ODC)

4. the ASEAN Regional Forum (ARF)

در سپتامبر ۲۰۱۴، در اجلاس شورای امنیت سازمان ملل متحد در مورد تروریسم، وانگ یی، وزیر امور خارجه چین خاطرنشان کرد که «رسانه‌های اجتماعی به میدان نبرد گروه‌های تروریستی و افراطی برای تحریک ایدئولوژی خود، طراحی حملات تروریستی و بستری برای عضوگیری تبدیل شده است». وانگ اشتراک‌گذاری اطلاعات و همچنین اقدامات قاطعانه برای توقف استفاده از رسانه‌های اجتماعی برای گسترش ایده‌های افراطی را پیشنهاد کرد و همچنین عنوان داشت که سازمان ملل باید بر نگارش یک آیین‌نامه رفتاری در حوزه صنعت فناوری جهانی تمرکز کند (Yi, 2014).

دو ماه بعد، پکن میزبان سمپوزیومی در مورد مبارزه با تروریسم سایبری بود که توسط مجمع جهانی ضد تروریسم^۱، یک پلت فرم غیررسمی متشکل از بیست و نه کشور، اتحادیه اروپا و آژانس‌های منطقه‌ای و سازمان‌های مختلف برای حمایت از اجرای "استراتژی جهانی مبارزه با تروریسم سازمان ملل متحد"^۲، برگزار شد.

پکن به تلاش‌های خود در زمینه مقابله با تروریسم در سازمان ملل متحد ادامه داده است. پکن همواره ابراز داشته است که از سازمان ملل برای ایفای نقش رهبری و همچنین ترویج هنجارهای بین‌المللی در فضای سایبری که به طور جهانی توسط همه طرف‌ها به رسمیت شناخته شود و ایجاد یک معاهده بین‌المللی ضد تروریسم در فضای سایبری حمایت خواهد کرد (Segal A., 2017).

طرح جاده ابریشم دیجیتال^۳

پکن از تجارت و سرمایه‌گذاری در زیرساخت‌های فناوری اطلاعات به عنوان یک ابزار سیاسی اقتصادی استفاده کرده است. تلاش‌های چین در آفریقا، آسیای جنوب شرقی و آسیای مرکزی برای دسترسی به بازارها و همچنین ایجاد حمایت از سیاست خارجی پکن و هنجارهای فضای سایبری طراحی شده است. چین در تلاش است تا نظم جهانی را از طریق ابتکار کمربند - جاده (BRI)^۴ به تدریج تغییر دهد. برای این منظور، پکن ممکن است از فناوری‌های جدید که به آن اجازه می‌دهد بر داده‌ها و ارتباطات در

1. the Global Counterterrorism Forum

2. the UN's Global Counter Terrorism Strategy

3. Digital Silk Road (DSR)

4. Belt and Road Initiative (BRI)

حوزه‌های سیاسی، اقتصادی و اجتماعی در سراسر گستره وسیع ابتکار کمر بند - جاده تسلط یابد، استفاده نماید. در این راستا، جاده ابریشم دیجیتال حداقل از سال ۲۰۱۵، زمانی که برای اولین بار در گزارش رسمی دولت مطرح شد، بخشی از رویکرد جمهوری خلق چین بوده است. جاده ابریشم دیجیتال فناوری‌های جدید را در بسته‌هایی مانند شهرهای هوشمند، بنادر هوشمند و ارتباطات شبکه‌های ماهواره‌ای به هم پیوند می‌دهد و از 5G به عنوان پایه‌ای برای فناوری‌های دیگر مانند هوش مصنوعی، تجزیه و تحلیل داده‌ها و اینترنت اشیا استفاده می‌کند. موفقیت در استفاده از این زیرساخت ارتباطی برای تسلط بر بازارها، استانداردها و نخبگان سیاسی به چین پایگاهی چندمنطقه‌ای می‌دهد که از طریق آن هنجارها، سیستم‌ها و شبکه‌های خود را به بازار جهانی گسترده‌تر صادر نماید (Hemmings, 2020).

بدین ترتیب ایجاد زیرساخت‌های ارتباطی در کشورهای مورد نظر در ابتکار کمر بند - جاده، به جمهوری خلق چین اجازه می‌دهد تا به مجموعه داده‌های کشورهای دریافت‌کننده دسترسی داشته باشد و بتواند این اطلاعات را مورد تجزیه و تحلیل قرار دهد. همچنین از طریق این تجهیزات و شرکت‌های فناوری چینی، پکن می‌تواند مدل حاکمیتی، سیستم نظارتی و مؤسسات مالی خود را در خارج از کشور گسترش دهد (Duesterberg, 2019).

نهادهای چینی، اعم از دولتی و خصوصی، نقش بزرگی در طراحی و ساخت این آینده‌ایفا کرده‌اند و تا سال ۲۰۲۰ بیش از ۱۷ میلیارد دلار برای پروژه‌های جاده ابریشم دیجیتال تدارک دیده‌اند که شامل ۷ میلیارد دلار وام برای پروژه‌های فیبر نوری و ارتباطات راه دور می‌شود. همانند ورود هواوی و زدتی‌ای به بازار اروپا، تامین مالی هواوی و زدتی‌ای در اوراسیا مرکزی به میزان قابل توجهی توسط بانک توسعه چین و بانک صادرات و واردات چین تامین شده است. در حالی که پروژه‌ها به نوبه خود نیاز به توجه دارند، هنجارها و استانداردهایی نیز در این طرح وجود دارند که مستلزم بررسی دقیق هستند؛ این هنجارها از اولویت‌بندی رزمینی به عنوان ارز انتخابی در تجارت دیجیتال و هنجارهای حاکمیت اینترنت، تا استانداردهای مرتبط با نظارت و حقوق سیاسی را شامل می‌شود (Hemmings, 2020).

دیپلماسی سایبری دوجانبه و منطقه‌ای چین

دیپلماسی سایبری چین با دولت‌های غربی

مسائل سایبری بخش مهمی از روابط دوجانبه و منطقه‌ای چین را تشکیل می‌دهند. هنگامی که ایالات متحده آمریکا برای اولین بار شروع به اقامه دعوی علیه چین برای سرقت سایبری و نقض مالکیت معنوی نمود، استراتژی اولیه پکن، تکذیب بود. هر اعلامیه مبنی بر اینکه هکرهای چینی در پشت حمله قرار داشتند با اعتراضات طرف چینی روبرو می‌شد و پکن همواره ابراز می‌داشت که هک در چین عملی غیرقانونی است و چین بزرگ‌ترین قربانی در فضای سایبری است. گفتگوهای دوجانبه در زمینه امنیت سایبری چیزی بود که واشنگتن بیش از پکن خواستار آن بود. اما درحالی که آمریکا خواستار گفتگو به صورت گسترده با ارتش خلق چین بود، مذاکرات عموماً به دیپلمات‌ها از طریق گفتگوهای استراتژیک و اقتصادی محدود می‌شد (Sanger, 2014).

در مارس ۲۰۱۳، مشاور امنیت ملی آمریکا، تام دونیلون، طی سخنرانی خود از نگرانی‌های جدی در مورد سرقت هدفمند و پیچیده اطلاعات تجاری محرمانه از طریق نفوذهای سایبری ناشی از چین در مقیاسی بی سابقه صحبت به میان آورد (Flora, 2013). در ژوئن ۲۰۱۳، او باما، رئیس‌جمهور اسبق در

طی دیدار خود در کالیفرنیا، طبق گزارش‌ها به رئیس‌جمهور شی هشدار داد که جاسوسی سایبری به روابط دوجانبه آسیب جدی می‌زند. اما بلافاصله پس از پایان اجلاس، افشای عملیات جاسوسی گسترده آژانس امنیت ملی آمریکا توسط ادوارد اسنودن^۱ به پکن اجازه داد تا انگشت اتهام را به سمت آمریکا بگیرد (Segal A. , 2017).

در می ۲۰۱۴، پس از کیفرخواست پنج هکر ارتش چین، پکن تمام گفتگوهای دوجانبه را به حالت تعلیق درآورد و عنوان داشت که گفتگوهای رسمی تنها پس از رفع کیفرخواست‌ها از سر گرفته می‌شود. روابط دوطرف پس از رفع اتهامات علیه هک‌های چینی تا حدودی بهبود یافت. پس از ورودی جین پینگ به کاخ سفید برای اولین سفر دولتی خود در سپتامبر ۲۰۱۵، پکن و واشنگتن تا حدی برای اجتناب از تحریم‌ها و تا حدی به دلیل ملاحظات داخلی توافق کردند که از سرقت سایبری دارای معنوی، از جمله اسرار تجاری یا سایر اطلاعات تجاری محرمانه، باهدف ارائه مزیت‌های رقابتی به شرکت‌ها یا بخش‌های تجاری، خودداری کنند. هر دو طرف همچنین برای شناسایی و تایید هنجارهای رفتاری در فضای سایبری و ایجاد دو کارگروه سطح بالا (یکی در مورد امنیت، یکی در مورد جرائم سایبری) و ایجاد یک خط ارتباطی برای واکنش به بحران‌ها، توافق کردند (Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference, 2015). قراردادی که به امضای سیدالگوی برای مدیریت روابط سایبری با بریتانیا، آلمان و سایر کشورهای غربی شد.

پس از روی کار آمدن رئیس‌جمهور ترامپ نیز طی دیداری با رئیس‌جمهور شی در فلوریدا در آوریل ۲۰۱۷، واشنگتن و پکن باگفت‌وگوی جامع ایالات متحده و چین موافقت کردند که دارای چهار رکن، از جمله در مورد مکانیسم اجرای قانون و گفتگوی امنیت سایبری ایالات متحده و چین (LECD)^۲ است (Statement from the Press Secretary on the United States-China Visit, 2017).

۱. ادوارد جوزف اسنودن (Edward Joseph Snowden) افشاگر کنونی و کارمند سابق سازمان اطلاعات مرکزی آمریکا و پیمانکار سابق آژانس امنیت ملی است. افشای‌های ادوارد اسنودن از عملیات بزرگ جاسوسی و مراقبت گسترده جهانی توسط آمریکا و متحدانش پرده برداشت.

2. the US-China Law Enforcement and Cybersecurity Dialogue (LECD)

علاوه بر آمریکا، چین با بریتانیا نیز گفت‌وگوی سالانه امنیتی در سطح مقامات ارشد برگزار کرده است که عمدتاً بر جرایم سایبری تمرکز داشته است. به عنوان مثال، در سال ۲۰۱۶، پکن و لندن توافق کردند که به هر درخواست برای دریافت اطلاعات یا کمک از طرف دولت دیگر در رابطه با فعالیت‌های مخرب، فوراً پاسخ دهند. آنها همچنین اعلام کردند که همکاری در زمینه جلوگیری از استفاده از اینترنت برای تحریک، استخدام، تامین مالی و برنامه‌ریزی فعالیت‌های تروریستی را تقویت خواهند نمود (China-UK High Level Security Dialogue: Communique, 2016).

در میان روابط دوجانبه باید به مشارکت ایجاد شده با اتحادیه اروپا نیز اشاره کرد. از سال ۲۰۱۲، یک کارگروه سایبری شامل اعضای از اتحادیه اروپا و چین در طول اجلاس سالانه اتحادیه اروپا و چین تشکیل جلسه داد و از آن سال تاکنون بطور مداوم تشکیل جلسه داده است. به نظر می‌رسد که این کارگروه یک انجمن برای ابراز نگرانی اتحادیه اروپا در مورد سیاست‌های امنیت سایبری داخلی چین و همچنین بحث در مورد حاکمیت اینترنت و نقش دولت در فضای سایبری باشد (Pawlak, 2015).

علاوه بر این، مؤسسه‌های تحقیقاتی آمریکا و چین از جمله مرکز مطالعات استراتژیک و بین‌المللی (CSIS) و مؤسسه روابط بین‌الملل معاصر چین (CICIR) در گفتگوهای Track 1.5 و Track II که در سال ۲۰۰۹، تأسیس شد، شرکت داشته‌اند. در این نشست‌ها طیف گسترده‌ای از مقامات و محققان آمریکایی و چینی که فعال در زمینه مسائل امنیت سایبری هستند، شرکت کرده‌اند. اهداف این گفتگوها کاهش برداشت‌های نادرست و افزایش شفافیت میان دو کشور و درک چگونگی رویکرد هر کشور به امنیت سایبری و شناسایی زمینه‌های همکاری بالقوه از جمله اقدامات اعتمادسازی و توافق بر روی هنجارها و قوانین امنیت سایبری بوده است (Track 1.5 U.S.-China Cyber Security Dialogue, n.d.). مرکز علوم و امور بین‌الملل بلفر مدرسه هاروارد کندی^۱ نیز میزبان "گروه کاری امنیت سایبری ایالات متحده و چین"^۲ با مؤسسه مطالعات استراتژیک بین‌المللی چین (CIISS)، مرتبط با ارتش خلق چین بوده است. در این گروه کاری طرفین با استفاده از مانورهای آینده‌پژوهانه به دنبال دستیابی به روش‌هایی برای پیشگیری از درگیری‌های غیرعمدی و افزایش قابلیت پیش‌بینی در فضای

1. Harvard Kennedy School's Belfer Center for Science and International Affairs

2. US-China Cyber Security Working Group

سایبری بوده‌اند. علاوه بر این، این گفتگو بستری را برای تبادل علمی در مورد سایر موضوعات مرتبط با حوزه سایبری، از جمله سرقت مالکیت معنوی، هوش مصنوعی، امنیت زنجیره تامین و چارچوب‌های کنترل تسلیحات و کنترل گسترش بدافزارها در دارک وب فراهم نموده است (Voo, 2019).

دیپلماسی سایبری چین با روسیه

علاوه بر دولت‌های غربی، مهم‌ترین روابط دوجانبه پکن با مسکو بوده است. دو دولت در سال ۲۰۱۵ توافقنامه همکاری در زمینه امنیت اطلاعات بین‌المللی را امضاء کردند. این توافقنامه، امنیت اطلاعات را به طور گسترده تعریف می‌کند که شامل انتقال اطلاعاتی است که سیستم‌های سیاسی و اجتماعی را تهدید می‌کند. همچنین شامل سیستم مدیریت چند جانبه، دموکراتیک و شفاف برای اینترنت است که به دولت‌ها نقش بیشتری در فرآیند حکمرانی فضای سایبری می‌دهد (Roth, 2015). این توافقنامه شامل فهرستی از اقدامات مشخص از جمله ایجاد نقاط تماس و کانال‌های ارتباطی و پروژه‌های علمی مشترک است. علاوه بر این، هر دو کشور توافق کردند که در ایجاد و انتشار هنجارهای حقوقی بین‌المللی در فضای سایبری همکاری کنند و مواضع خود را در مجامع بین‌المللی از جمله سازمان ملل متحد هماهنگ نمایند (Korzak, 2015).

یکی دیگر از مهم‌ترین مفاد توافقنامه، تعهد عدم تجاوز بود که به موجب آن روسیه و چین توافق کردند از حملات رایانه‌ای علیه یکدیگر خودداری کنند. این عبارت مبهم بود و به نظر نمی‌رسد جاسوسی را پوشش دهد یا حداقل از آن جلوگیری کند. به عنوان مثال، در فوریه ۲۰۱۷، چیهو (Qihoo ۳۶۰) 360 گزارش سالانه خود را در مورد تهدیدات پایدار پیشرفته (APTs)^۱ فعال در چین منتشر کرد که در میان سی و شش گروه جاسوسی از چین، نام APT 28، که با سازمان اطلاعات روسیه مرتبط است، آورده شده است (Segal A., 2017). همکاری در توسعه نسل بعدی فناوری‌های فیلتر اینترنت نیز یکی دیگر از بخش‌های این توافقنامه بود. در این راستا، فانگ بینگ شینگ^۲، که به عنوان پدر فایروال یا دیوار آتش بزرگ چین شناخته می‌شود، و لو وی، رئیس اداره فضای سایبری چین، در آوریل ۲۰۱۶ برای

1. advanced persistent threats (APTs)

2. Fang Bingxing

حضور در مجمع توسعه و امنیت فناوری اطلاعات روسیه و چین^۱ به مسکوفتند تا نسخه چینی کنترل اینترنت را در این کشور توسعه دهند (Wade, 2016).

به گفته شی جین‌پینگ، روسیه شریک استراتژیک کلیدی چین در هماهنگی و پیشبرد مفهوم چینی - روسی امنیت اطلاعات و حفظ ثبات استراتژیک جهانی در بحبوحه وضعیت پیچیده و بی‌ثبات بین‌المللی ناشی از مداخله فزاینده دولت‌های غربی در امور داخلی آن‌ها است. در بحث‌های سایبری بین‌المللی، دو کشور بر اهمیت حاکمیت سایبری و عدم مداخله تأکید دارند و در دیدگاه آن‌ها نسبت به نظم لیبرال مبتنی بر مقررات غربی فعلی و حمایت ایالات متحده از آزادی اینترنت و ابتکارات هنجار ساز تحت رهبری آمریکایی اعتمادی گسترده وجود دارد (Broeders, 2019).

دیپلماسی سایبری منطقه‌ای چین

پکن از مسائل سایبری برای تقویت موقعیت منطقه‌ای و نقش رهبری خود از طریق گروه بندی و اتحاد با کشورهای منطقه‌ای و کشورهای در حال توسعه نیز استفاده نموده است. مشارکت چین در مذاکره (هم‌فکری) سیاست‌گذاری سایبری چین، ژاپن و کره^۲، مجمع منطقه‌ای آسه‌آن (ARF)، مجمع آسیایی بوآئو (Boao)^۳ مجمع همکاری چین و آفریقا (FOCAC)^۴، مجمع همکاری چین و کشورهای عربی^۵، مجمع چین و جامعه کشورهای آمریکای لاتین و کارائیب^۶ و سازمان مشورتی حقوقی آسیایی آفریقایی^۷ از جمله

1. the Russia-China ICT Development & Security Forum

2. China-Japan-Korea cyber policy consultation

3. The Boao Forum for Asia

مجمع آسیایی بوآئو به عنوان مهمترین مجمع اقتصادی آسیا، یک سازمان بین‌المللی است که در سال ۱۹۹۸ توسط فیدل راموس، رئیس جمهور سابق فیلیپین، باب هاوک، نخست وزیر سابق استرالیا و موریرو هوسوکاوا، نخست وزیر سابق ژاپن پیشنهاد شد و در ۲۷ فوریه سال ۲۰۰۱ در شهر بوآئو استان هاینان چین به طور رسمی با حضور ۲۶ کشور عضو افتتاح شد.

4. the Forum on China-Africa Cooperation (FOCAC)

5. China-Arab States Cooperation Forum

6. Forum of China and the Community of Latin American and Caribbean States

7. the Asian-African Legal Consultative Organization

مصادیقی است که پکن سعی نموده تا اهداف خود در زمینه فضای سایبری را از طریق آن هادنبال نماید (Segal A. , 2017).

در سپتامبر ۲۰۱۱، چین و روسیه با حمایت تاجیکستان و ازبکستان، نامه‌ای را ارائه کردند که در آن پیش‌نویس قانون رفتار بین‌المللی برای امنیت اطلاعات را به مجمع عمومی سازمان ملل متحد پیشنهاد کردند. این تسلیم دوماه قبل از کنفرانس لندن، تلاشی تحت حمایت بریتانیا برای شناسایی هنجارهای رفتاری دولت، انجام شد و تاحدی برای کم‌رنگ کردن تلاش‌های دیپلماتیک ایالات متحده و متحدانش نقش داشت. این آیین نامه از فرآیند سازمان ملل در تدوین هنجارها و مقررات در حوزه سایبری پشتیبانی می‌کند و از دولت‌های خواهد موافقت کنند که از فناوری‌های اطلاعات و ارتباطات، از جمله شبکه‌ها، برای انجام فعالیت‌های خصمانه یا اقدامات تجاوزکارانه و یا تهدید علیه صلح و امنیت بین‌المللی استفاده نکنند. این آیین نامه همچنین تأکید می‌کند که صلاحیت سیاست‌گذاری برای مسائل عمومی مرتبط با اینترنت، حق حاکمیتی دولت‌هایی است که دارای حقوق و مسئولیت در موضوعات سیاستی عمومی بین‌المللی مرتبط با اینترنت هستند (International Code of Conduct for Information Security, 2011).

این آیین نامه مجدداً در سال ۲۰۱۵ توسط سازمان همکاری شانگهای (SCO)، سازمان منطقه‌ای اوراسیا که شامل چین، روسیه، قزاقستان، قرقیزستان، تاجیکستان و ازبکستان است، به سازمان ملل ارسال شد. حامیان این نسخه اصلاح شده امیدوار بودند که از پیامدهای سیاسی ناشی از افشای اطلاعات طبقه بندی شده توسط ادوارد اسنودن، پیمانکار آژانس امنیت ملی آمریکا، بهره ببرند و حمایت سایر دولت‌ها در زمینه هنجارهای حفظ امنیت اطلاعات که توسط نظارت جامعه اطلاعاتی پنج چشم (Five Eyes)^۱ تهدید می‌شد، را کسب نمایند (Segal A. , 2017).

۱. جامعه اطلاعاتی پنج چشم (Five Eyes) متشکل از ایالات متحده، کانادا، بریتانیا، استرالیا و نیوزلند، یک ائتلاف با سابقه آنگلو سافر اشتراک اطلاعات است. این جامعه از یک قرارداد همکاری طولانی مدت برای به اشتراک گذاری اطلاعات و همکاری در زمینه‌های هوش سیگنالی (SIGINT) است که در دوران جنگ سرد علیه اتحاد جماهیر شوروی ایجاد شده بود. این سازمان جنبه‌های مختلف فناوری اطلاعات و ارتباطات، مانند نظارت الکترونیکی، رهگیری ارتباطات، اطلاعات سایبری، تجزیه و تحلیل داده‌ها را میان کشورهای عضو به اشتراک می‌گذارد.

چین در اجلاس گروه راهبردی بریکس در سال ۲۰۱۶ و ۲۰۱۷ نیز بر مشارکت دموکراتیک و عادلانه دولت‌ها بر توزیع نامتقارن قدرت در سیستم حاکمیت اینترنتی موجود تأکید کرد. در دهمین بیانیه اجلاس سران بریکس در ژوئیه ۲۰۱۸، پکن بر اهمیت همکاری بین دولت‌ها در چارچوب سازمان ملل متحد برای توسعه یک ابزار الزام آور نظارتی جهانی باهدف مبارزه با استفاده مجرمانه از فناوری اطلاعات و ارتباطات تأکید کرد (10Th BRICS Summit Johannesburg Declaration, 2018).

در گروه ۲۰ (G20)^۱، چین بیانیه نشست وزرای دارایی و رؤسای بانک مرکزی گروه ۲۰، در سال ۲۰۱۷ را تأیید کرد و بر اهمیت امنیت سایبری برای محافظت از سیستم‌های مالی و اطلاعاتی تأکید داشت (Communiqué G20 Finance Ministers and Central Bank Governors Meeting, 2017). پکن همچنین در بیانیه رهبران گروه ۲۰ و زاکادر سال ۲۰۱۹، همراه با سایر کشورها متعهد شد که برای افزایش تاب‌آوری سایبری تلاش کند. اصطلاح «تاب‌آوری سایبری» به افزایش توانایی سازمان برای ادامه انجام مأموریت خود از طریق پیش‌بینی و انطباق با تهدیدات سایبری و سایر تغییرات مرتبط در محیط و به مقاومت، مهار و باز یابی سریع از حوادث سایبری اشاره دارد (Lopez, 2020).

علاوه بر این، چین توافقنامه مشارکت اقتصادی جامع منطقه‌ای^۲ که بر اساس آن ۱۵ کشور عضو از جمله چین مقررات منطقه‌ای مربوط به امضای الکترونیکی و احراز هویت الکترونیکی، حفاظت از مصرف‌کننده آنلاین، حفاظت از اطلاعات شخصی آنلاین، امنیت سایبری، انتقال اطلاعات بین‌المللی با استفاده از وسایل الکترونیکی و حفاظت از حق مالکیت معنوی را مورد تأیید قرار دادند، تصویب کرد. چین همچنین گام‌های جدی برای پیوستن به توافقنامه جامع و مترقی مشارکت ترانس پاسیفیک^۳ و توافقنامه مشارکت اقتصاد دیجیتال^۴ به منظور شرکت در تدوین استانداردهای حوزه اقتصاد دیجیتال برداشته است.

۱. گروه ۲۰ (G20) یک سازمان بین‌دولتی متشکل از ۱۹ کشور به همراه اتحادیه اروپا (EU) و اتحادیه آفریقا (AU) است. این گروه برای رسیدگی به مسائل عمده مرتبط با اقتصاد جهانی مانند ثبات مالی بین‌المللی، تغییرات اقلیمی و توسعه پایدار فعالیت می‌کند.

2. the Regional Comprehensive Economic Partnership agreement

3. the Comprehensive and Progressive Agreement for Trans-Pacific Partnership

4. the Digital Economy Partnership Agreement

برای مبارزه با تروریسم سایبری، چین همکاری با سایر کشورها را از طریق مانورهای مشترک ضد تروریستی، عملیات مشترک دفاع مرزی و همکاری قضایی برای مقابله با تهدیدات و چالش‌ها و حفاظت از صلح جهانی و ثبات منطقه‌ای را افزایش داده است. در مبارزه با کلاهبرداری‌های آنلاین، چین همکاری‌های قضایی را با سایر کشورها تقویت کرده است، پرونده‌های عمده مرزی را بررسی کرده و نتایج قابل توجهی به دست آورده است. بین مارس و ژوئن ۲۰۲۲، ۷۶ کشور از جمله چین در عملیاتی با نام رمز First Light 2022 که توسط سازمان بین‌المللی پلیس جنایی^۱ آغاز شده بود، شرکت کردند و حدود ۲۰۰۰ مظنون دستگیر شدند و حدود ۵۰ میلیون دلار وجوه غیرقانونی کشف شد که به طور موثر کلاهبرداری‌های فراملی را مهار کرد.

چین در راستای حفاظت مشترک از حقوق و منافع افراد زیر سن قانونی در فضای مجازی نیز با صندوق کودکان سازمان ملل متحد^۲ و سایر سازمان‌های بین‌المللی و بخش‌های مربوطه در انگلستان، آلمان، امارات متحده عربی و سایر کشورها برای مبارزه با پورنوگرافی آنلاین کودکان، همکاری داشته است. چین به عنوان عضو اتحاد جهانی WeProtect^۳، با سایر دولت‌های عضو، شرکت‌ها و سازمان‌های جامعه مدنی برای مقابله با بهره‌برداری جنسی از کودکان و سوءاستفاده آنلاین اقدام کرده است و در راستای ایجاد یک محیط سایبری امن برای کودکان تلاش نموده است (China's Law-Based Cyberspace Governance in the New Era, 2023).

1. the International Criminal Police Organization
 2. The United Nations Children's Fund (UNICEF)
 3. WeProtect Global Alliance

پیامدهای دیپلماسی سایبری برای چین

فرصت‌های دیپلماسی سایبری برای چین

- افزایش نقش بین‌المللی چین در حکمرانی فضای سایبری
چین به طور گسترده در مبادلات بین‌المللی و همکاری در زمینه مقررات فضای سایبری درگیر بوده است. پکن عنوان می‌دارد که با حفظ استقلال، برابری و احترام متقابل، به سایر کشورها می‌پیوندد تا سیستم حاکمیت جهانی فضای مجازی را اصلاح کند تا اطمینان حاصل شود که همه کشورها فرصت‌های حاصل از توسعه اینترنت را به اشتراک می‌گذارند و یک جامعه با آینده مشترک در فضای مجازی ایجاد می‌کنند. همان‌طور که ذکر شد، چین قاطعانه از سیستم بین‌المللی که در آن سازمان ملل متحد از نظم بین‌المللی از طریق مقررات بین‌المللی به عنوان پایه و اساس آن و هنجارهای اساسی روابط بین‌الملل بر اساس اهداف و اصول منشور سازمان ملل متحد محافظت نماید، حمایت می‌کند.
این کشور از تلاش سازمان ملل متحد برای تدوین کنوانسیون جرایم سایبری در سطح جهانی حمایت می‌کند و همچنین از مجمع عمومی خواسته است تا قطعنامه‌ای را برای ایجاد یک کمیته بین‌دولتی در حوزه فضای سایبری تصویب کند. علاوه بر این پکن نقش سازنده‌ای در مذاکرات برای ایجاد یک کنوانسیون بین‌المللی ایفا کرده است و خواهان آن است که جامعه بین‌المللی در اسرع وقت

در مورد یک کنوانسیون معتبر و جهانی به توافق برسد تا زمینه‌های قانونی برای مبارزه با جرایم سایبری ایجاد شود.

بدین ترتیب، چین برای نقش کلیدی سازمان ملل در پاسخ به تهدیدات بین‌المللی حوزه امنیت اطلاعات ارزش قائل است و همراه با دیگر کشورهای عضو سازمان همکاری شانگهای، آیین‌نامه بین‌المللی امنیت اطلاعات را به مجمع عمومی سازمان ملل متحد ارائه داد. ابتکار همکاری چین و اتحادیه عرب در مورد امنیت داده‌ها در مارس ۲۰۲۱ و ابتکار همکاری امنیت داده‌های چین به همراه پنج کشور آسیای مرکزی (قزاقستان، قرقیزستان، تاجیکستان، ترکمنستان و ازبکستان) در ژوئن ۲۰۲۲، طرحی برای توسعه مقررات امنیت داده‌های جهانی ارائه نمود. پکن همچنین نقش فعالی در تدوین توصیه یونسکو در مورد اخلاق هوش مصنوعی ایفا کرده است و همکاری گسترده‌ای با سازمان جهانی مالکیت معنوی در تدوین قوانین نام دامنه و حل اختلافات در این زمینه انجام داده است (China's Law-Based Cyberspace Governance in the New Era, 2023).

• اعتمادسازی

پکن از سال ۲۰۱۲ تاکنون با ایجاد موافقت‌نامه‌های منطقه‌ای و بین‌المللی، سعی بر ایجاد اعتماد متقابل با دیگر دولت‌ها داشته است. راهبرد بین‌المللی چین در زمینه همکاری فضای سایبری عنوان می‌کند که جمهوری خلق چین متعهد به حفظ صلح و ثبات در فضای سایبری از طریق همکاری بین‌المللی در زمینه شکل‌گیری هنجارها و ایجاد اقدامات اعتمادساز است. حوزه‌های قانونی تعامل اعتمادسازی چین شامل ایجاد اقدامات عملی باهدف جلوگیری از ایجاد درگیری‌های ناخواسته یا مسابقات تسلیحاتی و گسترش قابلیت‌های سایبری تهاجمی است. بر اساس این استراتژی بین‌المللی، اقدامات اعتمادساز چین همچنین شامل اقداماتی برای مهار سوءاستفاده از فناوری‌های اطلاعاتی و تضمین امنیت زنجیره تامین در تجهیزات شبکه و سیستم‌های کنترل صنعتی خواهد بود. علاوه بر این، ایجاد فضای اعتماد متقابل و قابل‌پیش‌بینی نیز مستلزم افزایش شفافیت در مورد بازراندگی و راهبردهای دکترین دولت‌ها و شفاف‌سازی ظرفیت اصول حقوقی برای حکمرانی بر اقدامات سایبری است (Ibid).

• ظرفیت‌سازی

یکی دیگر از فرصت‌های کلیدی دیپلماسی سایبری چین، ظرفیت‌سازی در کشورهای درحال-توسعه بوده است. ظرفیت‌سازی در فناوری‌های دیجیتال از جمله زیرساخت‌های شبکه، سیستم‌های اطلاعاتی، 5G، فیبر نوری و کابل‌های زیردریایی و ابزارهای فیلتر محتوا، در خدمت هدف استراتژیک بزرگ‌تر متقاعد کردن کشورهای درحال توسعه برای پذیرش ایده‌ها و مفاهیم حوزه سایبری پکن است. ابتکار همکاری بین‌المللی اقتصاد دیجیتال در ابتکار کمربند جاده، که در سال ۲۰۱۷ راه‌اندازی شد و جاده ابریشم دیجیتال، به دنبال بین‌المللی کردن فناوری چینی ساخته شده توسط شرکت‌های دولتی یا وابسته، از جمله هواوی و زدتی‌ای می‌باشد و از این طریق، استانداردها و ایجاد شرایط بالقوه مطلوب برای اهداف سایبری سیاسی وفی چین را مهیا می‌کنند (Joe Parkinson, et al., 2019). علاوه بر سرمایه‌گذاری زیرساختی، ظرفیت‌سازی بر افزایش ظرفیت اشتراک‌گذاری اطلاعات، آموزش پرسنل دفاع سایبری و مدیریت بحران نیز تمرکز دارد. در بلندمدت، پکن امیدوار است از سرمایه‌گذاری زیرساخت‌های فناوری اطلاعات و ارتباطات در کشورهای درحال توسعه برای اهداف سیاسی استفاده کند و اطمینان حاصل نماید که چین در موقعیت مناسبی برای بهره‌برداری از تغییر تدریجی قدرت در نظم بین‌المللی قرار گیرد (Bozhkov, 2020).

چالش‌های دیپلماسی سایبری برای چین

- ایجاد تنش با دیگر بازیگران

نبردهای تکنولوژیک میان چین و آمریکا اکنون به یک درگیری گسترده تبدیل شده است، زیرا دو قدرت دیجیتال برای برتری فناوری می‌جنگند. طی چند سال گذشته، ایالات متحده با برخی اتهامات درباره نگرانی‌های امنیت ملی، اقداماتی را برای محدود کردن دسترسی چین به فناوری‌های استراتژیک انجام داده است. چین نیز اقدام متقابل انجام داده است و محدودیت‌های صادراتی و سرمایه‌گذاری گسترده‌ای را علیه شرکت‌های آمریکایی اعمال نموده است. این رقابت ادامه دار همچنین به مسابقه پرداخت یارانه به بخش‌های تکنیک دامن زده است، زیرا ایالات متحده آمریکا و چین هر دو به دنبال تقویت توانایی‌های خود در فناوری‌های حیاتی مانند نیمه‌هادی‌ها هستند.

کشورهای دیگر، از جمله کشورهای اتحادیه اروپا، در بحبوحه تنش‌های فزاینده آمریکا و چین و از هم‌گسیختگی زنجیره‌های عرضه جهانی، به سیاست صنعتی روی آورده‌اند. در نتیجه، جنگ فناوری خطر تثبیت تکنوناسیونالیسم به عنوان یک هنجار جهانی را به دنبال دارد. این می‌تواند به عنوان یک پیروزی برای مدل دولت محور چین در نظر گرفته شود، زیرا دولت‌ها چشم‌انداز ایالات متحده در مورد اقتصاد دیجیتال باز، آزاد و جهانی را کنار می‌گذارند. اما این نکته بسیار برای اقتصاد چین حائز اهمیت است که برهم خوردن زنجیره‌های تأمین و فشارهای خارجی بر چین می‌تواند باعث تحریم و عدم سرمایه‌گذاری خارجی در صنایع چین گردد و بازار خارجی شرکت‌ها و غول‌های فناوری چین را از بین ببرد (Bradford, 2023).

• بی‌اعتمادی به رویکرد دولت محور چین

حرکت چین به سمت حاکمیت سایبری که به نحوی نتیجه افزایش تهدید یا تنش‌ها با ایالات متحده بوده است، یک عامل مؤثر در بی‌اعتمادی دولت‌ها و شرکت‌های خارجی به دولت پکن و غول‌های فناوری چین بوده است. از آنجایی که فضای کسب‌وکارهای خارجی به تدریج دشوارتر و چالش‌برانگیزتر شده است، حمایت از تعامل با چین در میان شرکت‌های بین‌المللی، کاهش یافته است. علاوه بر این، نگرانی‌ها در مورد خطرات بالقوه ناشی از ردپای جهانی روبه‌رشد کسب‌وکارهای چینی، دولت‌های توسعه‌یافته سراسر جهان را به تجدیدنظر در میزان مشارکت چین در بازارهای داخلی خود سوق داده است. استفاده چین از فناوری برای اهداف نظارتی و کنترلی داخلی، به‌ویژه در منطقه سین‌کیانگ، روند برداشت بدبینانه از چین در اروپا و آمریکا را تشدید کرده است. در نتیجه این امر، امروزه هواوی برای فروش در بازارهای غربی با مشکلات فزاینده‌ای مواجه است، به‌طوری‌که برخی کشورها از جمله بریتانیا مشارکت این شرکت در توسعه شبکه‌های 5G را ممنوع کرده است. دولت ایالات متحده اقداماتی را برای محدود کردن استفاده از برنامه‌های تلفن همراه متعلق به چین، به‌ویژه تیک‌تاک (TikTok) و وی‌چت (WeChat) انجام داده است. هند نیز پس از درگیری‌های مرزی با ارتش چین، تیک‌تاک را ممنوع کرد.

دهه‌ها توسعه نسبتاً بدون مرز که در آن نرم‌افزار، سخت‌افزار و سرویس‌های آنلاین، بخش‌ها و زیرساخت‌های تجاری حمایت‌کننده آنها، و جریان داده‌ها و اطلاعات به روش‌های پیچیده‌ای

درهم‌تنیده شده بودند، امروزه به حوزه‌های ملی تبدیل شده‌اند. در نتیجه، جداسازی در حوزه دیجیتال به سرعت از یک کلمه کلیدی سیاستی در پکن به یک واقعیت اولیه تبدیل شده است و به طور بالقوه ممکن است برای منافع چین بسیار زیان‌آور باشد. حوزه دیجیتال اکنون برای بسیاری از کشورها از یک قلمرو عمدتاً اقتصادی به یک موضوع کلیدی امنیت ملی تبدیل شده است که فراتر از ملاحظات سنتی مانند امور نظامی است. همان‌طور که اقدام ایالات متحده علیه تیک‌تاک نشان می‌دهد، اکنون مسائل اجتماعی و حتی هویتی نیز زیر چتر امنیتی قرار می‌گیرند. روند روبه‌افزایش ناشی از گسترش سریع مرزهای حاکمیتی در فضای سایبری پتانسیل تغییر این چشم‌انداز به فضای سایبری را دارد. این تغییرات احتمالاً هزینه مالی قابل توجهی را به همراه خواهد داشت و خطر تشدید بیشتر بی‌اعتمادی و درگیری میان چین و دولت‌های غربی را به همراه خواهد داشت (Creemers R. , 2020).

برنامه آینده چین در دیپلماسی سایبری

امنیت سایبری و نوآوری از اهمیت استراتژیک بالایی برای چین برخوردار است؛ زیرا هدف پکن این است که یک قدرت بزرگ متعارف و پیشرو در فضای دیجیتال باشد. برای این منظور، اولویت سیاسی داده شده به فناوری دیجیتال از سال ۲۰۱۲ به طور قابل توجهی افزایش یافته است. رئیس جمهور شی در سال ۲۰۲۳ عنوان داشت: آموزش، علم و فناوری و منابع انسانی ستون‌های اساسی و استراتژیک برای ساختن یک کشور مدرن سوسیالیستی از همه جهات هستند. جاه‌طلبی‌های چین در خدمت هدف عالی تقویت و حفاظت از حزب-دولت و تقویت مشروعیت آن هستند؛ بنابراین، فناوری‌های دیجیتال در درجه اول برای دستیابی به نیازها و منافع داخلی، ایجاد رفاه و حفظ رشد اقتصادی و ثبات اجتماعی استفاده می‌شود. تمرکز اصلی پکن بر پاک‌سازی اینترنت چین از ایده‌ها و اطلاعاتی است که ممکن است قدرت حزب کمونیست چین را به چالش بکشد، بدین ترتیب حزب به دنبال بهره‌برداری از پتانسیل اقتصادی اینترنت بدون به خطر انداختن قدرت خود است. از این رو، درک همه‌جانبه چین از امنیت ملی به امنیت سایبری نیز گسترش می‌یابد و جاه‌طلبی‌های حوزه فناوری دیجیتال آن نشان‌دهنده نگرانی‌ها و همچنین اهداف داخلی چین است. از این رو، چین در راستای تلاش برای همسو کردن نظام بین‌المللی با چشم‌انداز خود و درعین حال دستیابی به استقلال بیشتر در نظم

دیجیتال جهانی، قصد دارد بر نظم بین‌المللی و توسعه جهانی اینترنت تأثیر بگذارد. بدین ترتیب پکن استراتژی آینده خود را بر سه حوزه بسیار مهم از جمله استانداردسازی، خوداتکایی فناوری و ایجاد روایت‌های جایگزین امنیت سایبری بین‌المللی معطوف نموده است.

استانداردسازی

یکی از مهم‌ترین برنامه‌های پیش‌روی چین، تبدیل شدن به یک قدرت استانداردسازی فنی است. با تعیین استانداردهای فنی، می‌توان بر بازیگران تأثیر گذاشت و هنجارهای بین‌المللی را که به نفع منافع پکن باشد، ترویج نمود. مقامات پکن معتقدند هر طرف که استانداردهای فنی را تعیین نماید، عملکردها و انتظارات اخلاقی، سیاسی و امنیتی را نیز شکل خواهد داد. از این رو، استانداردها در رابطه با رقابت اقتصادی و امنیت ملی و سایبری حیاتی هستند. بدین ترتیب، استانداردسازی به طور فزاینده‌ای سیاسی شده است، برخی این را چالش راناشی از رقابت دابلوک بر سر ترویج ارزش‌های خود در فضای سایبری می‌دانند.

برای تأثیرگذاری بر استانداردسازی، چین روش‌های مختلفی از جمله به دست آوردن نفوذ در نهادهای تنظیم‌کننده استانداردهای بین‌المللی از طریق قرارداد اتباع چینی در پست‌های کلیدی، ریاست کمیته‌های فنی و گروه‌های کاری و واداشتن شرکت‌های چینی به رای دادن به نفع ایدئولوژی و افراد چینی در مجامع چند ذی‌نفعی را دنبال نموده است. علاوه بر این، پکن برای دستیابی به نقشی پیش‌رو در توسعه فناوری‌های جدید مانند 5G، هوش مصنوعی و اینترنت اشیا که هنوز استانداردهای آن به صورت گسترده تنظیم نشده است، بسیار تلاش نموده است. پروژه‌هایی مانند جاده ابریشم دیجیتال نیز به تعیین استانداردهای مورد نظر پکن کمک نموده است، زیرا طرف‌های موجود در این طرح متعهد به استفاده از فناوری چینی هستند و توافقاتی در راستای هماهنگ نمودن استانداردهای فنی میان طرفین حاصل شده است (Pleil, 2023).

خوداتکایی در حوزه فناوری

در حال حاضر چین به فناوری خارجی وابسته است. شی جین پینگ همواره تأکید کرده است که خطر پنهان برای چین این است که فناوری‌های اصلی آن تحت کنترل دیگران هستند. بدین ترتیب، خوداتکایی در فناوری، یکی از مهم‌ترین محورهای رقابت و انعطاف‌پذیری اقتصادی و سیستمی برای پکن می‌باشد. به همین دلیل، چین در برنامه‌های خود برای فضای سایبری قصد دارد از نظر فناوری به خود متکی شود و در نتیجه از وابستگی این کشور به دیگر رهبران فناوری و دخالت دولت‌های خارجی در شبکه‌های دیجیتال چین راکاهش دهد. علاوه بر این، چین بر تبدیل شدن به یک رهبر در فناوری‌های استراتژیک و نوظهور مانند هوش مصنوعی و 5G متمرکز شده است. این امر به چین اجازه می‌دهد تا وابستگی ساختاری در زنجیره‌های تولید جهانی ایجاد نماید (Ibid).

روایت‌های جایگزین امنیت سایبری بین‌المللی

پکن از عرصه دیپلماتیک در سطح جهانی برای ترویج نظم دیجیتال جهانی با محوریت چین نیز استفاده می‌نماید. یکی از جنبه‌های اصلی این امر ارتقای حاکمیت سایبری است. چنین برداشتی برخلاف ایده رایج غربی در مورد اینترنت آزاد است، زیرا این امر به دولت‌ها اجازه می‌دهد تا قدرت نهایی را در فضای دیجیتال داشته باشند. این امر باعث ایجاد مرزهای ملی در فضای سایبری می‌شود که جریان آزاد اطلاعات را مسدود می‌کند و کنترل اینترنت را آسان‌تر می‌کند و اقتدارگرایی دیجیتال را فعال می‌کند. علاوه بر این، این یک تهدید برای رویکرد چندذی‌نفعی است. همچنین این امر باعث ایجاد تضادهای ایدئولوژیک و شکاف در فضای مجازی می‌شود. یکی از نمونه‌های آن پیشنهاد جایگزینی پروتکل اینترنت (IP) قبلی با طرح "NewIP"^۱ بود. در این طرح، هوآوی یک طراحی مجدد اینترنت را پیشنهاد نمود

۱. پیشنهاد New IP در جلسه ۲۰۱۹ اتحادیه بین‌المللی مخابرات ارائه شد. پشتیبانان این طرح پیشنهادی، هوآوی، به همراه بازوی تحقیقاتی هوآوی ایالات متحده، Futurewei Technologies، وزارت صنعت و فناوری اطلاعات و دولت چین هستند و همچنین سه شرکت اصلی مخابراتی شامل China Telecom، China Unicom، China Mobile نیز از آن حمایت کردند. هوآوی در این راستا اعلام کرد که New IP نسبت به استاندارد رایج اینترنت، IP / TCP نرخ تبادل داده‌های بیشتر و تأخیر کمتری در ارتباطات دارد.

که برای ایجاد "امنیت ذاتی" در فضای وب طراحی شده است. امنیت ذاتی به این معنی است که افراد باید برای استفاده از اینترنت ثبت نام کنند و مقامات می توانند دسترسی به اینترنت یک کاربر را در هر زمان مسدود نمایند. به طور خلاصه، هواوی به دنبال ادغام سیستم اعتبار اجتماعی^۲، نظارت و مقررات حاکم بر محدودیت چین در معماری اینترنت است (Mark Montgomery and Theo Lebryk, 2021).

چین برای تقویت موقعیت خود در نظم دیجیتال جهانی، به دنبال تغییر شکل زنجیره های تأمین، سیستم های اقتصادی و فناوری جهانی است. چین از عرصه ها و ابتکارات مختلف در سطح بین المللی برای دستیابی به این اهداف استفاده می کند. البته این جاه طلبی ها نیز محدودیت هایی دارند: کمبود استعداد و نوآوری برای اجرای این اهداف استراتژیک و وابستگی گسترده به فناوری های خارجی، مهم ترین چالش های پیش روی چین برای دستیابی به این اهداف در آینده است. با این حال، ابتکارات و ایده های چینی برای برخی از بازیگران در حال توسعه بسیار جذاب می باشد (Pleil, 2023).

جمع بندی و نتیجه گیری

پکن، در یک بازه زمانی نسبتاً کوتاه، دیپلماسی سایبری گسترده ای را توسعه داده است. دیپلماسی سایبری چین با توجه به اهداف آن از جمله محدود کردن تهدید مشروعیت حزب، گسترش نفوذ پکن و مقابله با نفوذ ایالات متحده آمریکا در فضای سایبری، نسبتاً موفق بوده است. امروزه این ایده که فضای مجازی مانند هر فضایی دیگری مستقل و تحت حاکمیت دولت است، به طور گسترده پذیرفته شده است. با این حال، تلاش ها برای عملیاتی کردن این ایده از سوی کشورهای هم فکر چین، به ویژه کشورهای در حال توسعه که نگران ثبات داخلی هستند، بیشتر از اقتصادهای پیشرفته مورد توجه و حمایت قرار گرفته است. بدین ترتیب، پکن توانسته دیدگاه خود در مورد حق حاکمیت اینترنت را ترویج نماید و جهانی سازی انتخابی را به عنوان یک استراتژی حاکمیتی اتخاذ کند و توافق های منطقه ای را که در خدمت منافع خود است، پیش ببرد.

1. intrinsic security

2. social credits system

در حال حاضر احتمال اندکی وجود دارد که اقدامات پکن در فیلتر اینترنت توسط دولتمردان واشنگتن محکوم شود. با توجه به اینکه دولت ترامپ در گذشته و بایدن در حال حاضر، بر مبارزه با افراط‌گرایان متمرکز هستند و توجه اندکی بر انتقاد از سیاست‌های داخلی کشورهای گوناگون دارند، چین ممکن است راهی پیدا کند تا این عمل‌گرایی به تعاملات آمریکا و چین در فضای سایبری نیز هدایت شود. یکی از نمونه‌های آن، پایان برنامه آزادی اینترنت بود که نه تنها بخش عمده‌ای از نارضایتی‌های پکن را از بین برد، بلکه می‌تواند این باور را زنده کند که فضای مشترکی بین چین و ایالات متحده برای همکاری بخصوص در راستای مقابله با استفاده تروریستی از اینترنت ایجاد شود. در گذشته، همکاری دو دولت به دلیل نگرانی‌های ایالات متحده در مورد شناسایی برخی گروه‌های اویغور و تبتی به عنوان تروریست و محدودیت‌های آزادی بیان، محدود شده بود، اما شواهد نشان می‌دهد پکن به طرح این موضوع ادامه خواهد داد و ممکن است در آینده استقبال بیشتری در کاخ سفید برای همکاری در مورد مقابله با این گروه‌ها میان پکن و واشنگتن ایجاد شود.

در آخر شایان ذکر است عوامل متعددی می‌تواند اهداف کلی چین در رابطه با فضای سایبری را مختل کند؛ رویکردهای مبتنی بر حاکمیت چین برای حکمرانی اینترنت، مستلزم اعمال مستمر فیلتر و کنترل جریان آزاد اطلاعات است که نیاز به تدوین فزاینده قوانین و مقررات امنیت سایبری دارد. این امر در تضاد با ماهیت توزیع شده اینترنت و محیط ذاتاً فرامرزی و باز است که توسط این ارتباط رسانه‌ای ترویج می‌شود. همچنین این موضوع ممکن است چالش آسیب دیدن وجهه داخلی و بین‌المللی، هم برای دولت و هم برای غول‌های فناوری چین را به همراه داشته باشد.

یادداشت‌ها و منابع

1. 10Th BRICS Summit Johannesburg Declaration. (2018, July 26). Retrieved from Ministry of External Affairs, Government of India: https://www.mea.gov.in/bilateral-documents.htm?dtl/30190/10th_BRICS_Summit_Johannesburg_Declaration
2. 8th BRICS Summit. (2016, Oct 16). Retrieved from BRICS: https://www.brics2017.org/English/Documents/Summit/201701/t20170125_1410.html
3. Academy Profile. (n.d.). Retrieved from caict: http://www.caict.ac.cn/english/intro/201804/t20180428_161365.htm
4. Bandurski, D. (2014, November 20). Envisioning the Splinternet. Retrieved from China Media Project: <http://cmp.hku.hk/2014/11/20/chinas-splinternet-making-insularity-global/>
5. Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs*, 353-364.
6. Bendiek, A. (2018, April 26). The EU as a force for peace in international cyber diplomacy. Retrieved from <https://www.swp-berlin.org/en/publication/the-eu-as-a-force-for-peace-in-international-cyber-diplomacy/>
7. Blue, V. (2012, December 8). WCIT-12 leak shows Russia, China, others seek to define 'government-controlled Internet'. Retrieved from ZDNET:

- <https://www.zdnet.com/article/wcit-12-leak-shows-russia-china-others-seek-to-define-government-controlled-internet/>
8. Bozhkov, N. (2020). China's Cyber Diplomacy: A Primer. EU Cyber Direct.
 9. Bradford, A. (2023). The Battle for Technological Supremacy: The US-China Tech War. Digital Empires: The Global Battle to Regulate Technology.
 10. Broeders, D. e. (2019). A Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace. The Hague Cyber.
 11. Building China's International Cyberspace Discourse Power. (2016, November 14). Retrieved from Information Office of the State Council of the People's Republic of China: http://webcache.googleusercontent.com/search?q=cache%3Awww.scio.gov.cn%2Fzhzc%2F10%2FDocument%2F1519386%2F1519386.htm&rlz=1C1GCEB_enBE813BE813&oq=cache%3Awww.scio.gov.cn%2Fzhzc%2F10%2FDocument%2F1519386%2F1519386.htm&aqs=chrome..69i57j69i58.919j0j4&source
 12. Central Leading Group for Internet Security and Informatization Established. (2014, March 1). Retrieved from China Copyright and Media: <https://chinacopyrightandmedia.wordpress.com/2014/03/01/central-leading-group-for-internet-security-and-informatization-established/>
 13. China Unveils Its First Civil-Military Cybersecurity Innovation Center. (2017, December 28). Retrieved from People's Daily: <http://en.people.cn/n3/2017/1228/c90000-9309428.html>
 14. china, i. o. (2017, March 2). International Strategy of Cooperation on Cyberspace. Retrieved from <http://www.scio.gov.cn/32618/Document/1543874/1543874.htm>
 15. China's Positions on International Rules-making in Cyberspace. (2021, September 20). Retrieved from Ministry of Foreign Affairs, the People's Republic of China: https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html
 16. China's Law-Based Cyberspace Governance in the New Era. (2023, March 16). Retrieved from The State Council Information Office of the People's Republic of China: http://www.scio.gov.cn/zfbps/zfbps_2279/202303/t20230320_709283.html
 17. China's National Defense in the New Era. (2019, July 24). Retrieved from Ministry of National Defence of the People's Republic of China: <http://eng.mod.gov.cn/xb/Publications/WhitePapers/4846452.html>
 18. China-UK High Level Security Dialogue: Communique. (2016, June 13). Retrieved from GOV.UK: <https://www.gov.uk/government/publications/china->

- uk-high-level-security-dialogue-official-statement/china-uk-high-level-security-dialogue-communique
19. Chuanying, L. (2016, December 2). The International Cyberspace Rule-based System and the China-U.S. New Type of Great. Retrieved from People's Daily: <http://theory.people.com.cn/n1/2016/1202/c386965-28920732.html>
20. Communiqué G20 Finance Ministers and Central Bank Governors Meeting. (2017, March 18). Retrieved from G20 Information Centre: <http://www.g20.utoronto.ca/2017/170318-finance-en.pdf>
21. Creemers, R. (2020). China's Approach to Cyber Sovereignty. Konrad-Adenauer-Stiftung e. V., Berlin.
22. Creemers, R. (2021, January). China's Cyber Governance Institutions. Retrieved from Leiden Asia Centre: <https://leidenasiacentre.nl/report-chinas-cyber-governance-institutions/>
23. Creemers, R. e. (2018, March 26). China's Cyberspace Authorities Set to Gain Clout in Reorganization. Retrieved from Digi China, New America: <https://digichina.stanford.edu/work/chinas-cyberspace-authorities-set-to-gain-clout-in-reorganization/>
24. Creemers, Rogier, et al. (2018, March 26). China's Cyberspace Authorities Set to Gain Clout in Reorganization. Retrieved from New America: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/>
25. Cyberspace Administration of China. (n.d.). Retrieved from Thomson Reuters: [https://uk.practicallaw.thomsonreuters.com/8-618-2325?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/8-618-2325?transitionType=Default&contextData=(sc.Default)&firstPage=true)
26. Duesterberg, T. (2019, December 12). Can We Avoid Collateral Damage in the 5G Battle with China? The Role of International Standards. Retrieved from Forbes: <https://www.forbes.com/sites/thomasduesterberg/2019/12/12/can-we-avoid-collateral-damage-in-the-5g-battle-with-china-the-role-of-international-standards/?sh=4886a1dd6fb9>
27. Flora, L. (2013, March 11). Complete Transcript: Thomas Donilon at Asia Society New York. Retrieved from Asia Society: <https://asiasociety.org/new-york/complete-transcript-thomas-donilon-asia-society-new-york>
28. Grigsby, A. (2017). The End of Cyber Norms. *Survival*, 59:6, 109-122.
29. Hampson, F. O. (2017). Getting Beyond Norms: New Approaches to International Cyber Security Challenges. Special Report, Centre for International Governance Innovation.

30. Harold, S. W., Libicki, M. C., & Cevallos, A. S. (2016). Getting to yes with China in cyberspace. Rand Corporation.
31. Hemmings, J. (2020). Reconstructing Order: The Geopolitical Risks in China's Digital Silk Road. *Asia Policy* Vol. 15, No. 1, 5-22.
32. Homburger, Z. (2019). The necessity and pitfall of cybersecurity capacity building for norm development in cyberspace. *Global Security*, 33(2), 224–242.
33. International Code of Conduct for Information Security. (2011, September 14). Retrieved from United Nations General Assembly: <http://www.rusemb.org.uk/data/doc/internationalcodeeng.pdf>
34. International Strategy of Cooperation on Cyberspace. (2017, March 1). Retrieved from xinhuanet: http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm
35. International Strategy of Cooperation on Cyberspace. (2017, March 2). Retrieved from State Council Information Office: http://www.scio.gov.cn/xwfb/bwxwfb/gbwfbh/wjb/202207/t20220715_199452.html
36. Joe Parkinson, et al. (2019, August 15). Huawei Technicians Helped African Governments Spy on Political Opponents. Retrieved from Wall Street Journal: <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017>
37. Judge Xue, Hanqin, and Elizabeth Wilmschurst. (2013). China and International Law: 60 Years in Review. international law summary chatham house.
38. Kehl, Danielle, and Tim Maurer. (2012, December 14). Did the U.N. Internet Governance Summit Actually Accomplish Anything? Retrieved from Slate: <https://slate.com/technology/2012/12/wcit-2012-has-ended-did-the-u-n-internet-governance-summit-accomplish-anything.html>
39. Korzak, E. (2015, August 20). The Next Level for Russia-China Cyberspace Cooperation? Retrieved from Council on Foreign Relations.: <https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation>
40. Kristin Shi-Kupfer , Mareike Ohlberg. (2019). China's Digital Rise. Mercator Institute for China Studies, 1-55.
41. Lee, J. (2021, June 21). The Connection of Everything: China and the Internet of Things. Mercator Institute for China Studies (MERICS). Retrieved from Mercator Institute for China Studies (MERICS): <https://merics.org/en/report/connection-everything-china-and-internet-things>

42. Lee, J. (2022). Cyberspace Governance in China: Evolution, Features and Future Trends. *Asie.Visions*, No. 129, Ifri.
43. Lopez, S. (2020). 2019 G20 Osaka Summit Final Compliance Report. University of Toronto.
44. Mark Montgomery and Theo Lebyrk. (2021, April 13). China's Dystopian "New IP" Plan Shows Need for Renewed US Commitment to Internet Governance. Retrieved from Just Security: <https://www.justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance/>
45. Mark, J. (2015, July 9). U.N. body Agrees to U.S. Norms in Cyberspace. Retrieved from Politico: <http://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900>
46. McCarthy, K. (2015, December 18). The Firewall Awakens: ICANN's exiting CEO takes internet governance to the dark side. Retrieved from The Register: https://www.theregister.com/2015/12/18/ex_icann_ceo_will_work_with_china/
47. Mihai Chihaiia & Jan Rempala. (2021). Cyber Diplomacy.
48. Mihai Sebastian Chihaiia and Jan Rempala. (2021). Cyber Diplomacy. The Palgrave Encyclopedia of Global Security Studies.
49. Moore, G. (2023). Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies. *Journal of Chinese Political Science*, 28, 151–167 .
50. Mueller, M. (2010). *Network and States: The Global Politics of Internet Governance*. Cambridge: MIT Press.
51. National Cyberspace Security Strategy. (2016, December 27). Retrieved from China Copyright and Media: <https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/>
52. Notice concerning Empowering the Cyberspace Administration of China to be Responsible for Internet Information Content Management Work. (2014, August 26). Retrieved from China Copyright and Media: <https://chinacopyrightandmedia.wordpress.com/2014/08/26/notice-concerning-empowering-the-cyberspace-administration-of-china-to-be-responsible-for-internet-information-content-management-work/>
53. Pawlak, P. (2015, June 29). Cyber Diplomacy: EU Dialogue with Third Countries. Retrieved from European Parliament Think Tank:

- [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2015\)564374](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2015)564374)
54. Pleil, H. (2023, March 30). Being a Cyberpower – China’s Ambitions in Cyberspace. Retrieved from Tech Policy Press: <https://www.techpolicy.press/being-a-cyberpower-chinas-ambitions-in-cyberspace/>
 55. Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference. (2015, December 16). Retrieved from Ministry of Foreign Affairs, People’s Republic of China: https://www.mfa.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html
 56. Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference. (2015, September 25). Retrieved from White House: <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint>
 57. Rizki, S. (2023, December 18). China’s Cyber Foreign Policy under Xi Jinping. Retrieved from medium: <https://medium.com/@livethesearch84/chinas-cyber-foreign-policy-under-xi-jinping-7aaf7ed3ba68>
 58. Roth, A. (2015, May 8). Russia and China Sign Cooperation Pacts. Retrieved from New York Times: https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0
 59. Sanger, D. E. (2014, April 6). U.S. Tries Candor to Assure China on Cyberattacks. Retrieved from New York Times: https://www.nytimes.com/2014/04/07/world/us-tries-candor-to-assure-china-on-cyberattacks.html?_r=0
 60. Segal, A. (2013, December 10). Cyberspace Cannot Live without Sovereignty, Says Lu Wei. Retrieved from Asia Unbound (blog), Council on Foreign Relations: <http://blogs.cfr.org/asia/2013/12/10/cyberspace-cannot-live-without-sovereignty-says-lu-wei/>
 61. Segal, A. (2017). Chinese cyber diplomacy in a new era of uncertainty. Hoover Institution, Aegis Paper Series, 1703, 1-23.
 62. Shen, H. (2019). China’s Tech Giants: Baidu, Alibaba, Tencent. Konrad Adenauer-Stiftung, 33-41.
 63. State Council Information Office, P. R. (2010, June 8). The Internet in China. Retrieved from http://news.xinhuanet.com/english2010/china/2010-06/08/c_13339232.htm

64. Statement from the Press Secretary on the United States-China Visit. (2017, April 7). Retrieved from Office of the Press Secretary, White House: <https://www.whitehouse.gov/the-press-office/2017/04/07/statement-press-secretary-united-states-china-visit>
65. Stauffacher, D. (2019, May). UN GGE and UN OEWG: How to live with two concurrent UN Cybersecurity processes. Retrieved from ict for peace.org: <https://ict4peace.org/wp-content/uploads/2019/11/ICT4Peace-2019-OEWG-UN-GGE-How-to-live-with-two-UN-processes.pdf>
66. Track 1.5 U.S.-China Cyber Security Dialogue. (n.d.). Retrieved from Center for Strategic & International Studies: <https://www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/other-projects-8>
67. Voo, J. (2019, May 3). Belfer Center Convenes U.S.-China Cyber Security Working Group. Retrieved from Belfer Center for Science and International Affairs, Harvard Kennedy School: <https://www.belfercenter.org/publication/belfer-center-convenes-us-china-cyber-security-working-group>
68. Wade, S. (2016, April 27). Chinese Cyberchiefs Preach Net Sovereignty in Moscow. Retrieved from China Digital Times: <http://chinadigitaltimes.net/2016/04/chinese-cyberchiefs-preach-Internet-sovereignty-moscow/>
69. Why is America giving up control of ICANN? (2016, September 30). Retrieved from The Economist: <https://www.economist.com/the-economist-explains/2016/09/29/why-is-america-giving-up-control-of-icann>
70. Wood, P. (2015, October 19). China Conducts Anti-Terror Cyber Operations with SCO Partners. Retrieved from Jamestown Foundation: <https://jamestown.org/program/china-conducts-anti-terror-cyber-operations-with-sco-partners/>
71. Yi, W. (2014, September 24). Working Together to Address the New Threat of Terrorism. Retrieved from Ministry of Foreign Affairs, People's Republic of China: https://www.mfa.gov.cn/web/ziliao_674904/zyjh_674906/201409/t20140925_9869403.shtml
72. ZTE Corp. (n.d.). Retrieved from asia.nikkei: <https://asia.nikkei.com/Companies/ZTE-Corp>

دفترهای آبی

مقالات پژوهشی (Research Papers) از مهم ترین ابزارهای توسعه دانش هستند که با تکیه بر داده های تجربی به بررسی دقیق و جامع موضوعات تخصصی می پردازند.

دفترهای آبی دسته ای از گزارش های تفصیلی تولید شده در پژوهشگاه فضای مجازی، و محصول رصد مطالعات تحقیقی اندیشکده ها و نخبگان جهان در موضوعات مرتبط با فضای مجازی است.



اندیشکده حکمرانی آوا
Ava Governance Think Tank

پژوهشگاه
فضای مجازی

