Dor: 20.1001.1.28212673.1401.6.18.3.9

فصلنامه محیط‌شناسی راهبردی ج.ا.ایران
سال ششم، شماره ۱، بهار ۱۴۰۱
مقاله پژوهشی، از صفحات ۱۰۲-۷۳

بررسی رویکردهای متعارض به حاکمیت سایبری
(مطالعهٔ موردی حاکمیت سایبری روسیه و آمریکا)

عسگر صفری[۱]

تاریخ دریافت: ۱۴۰۱/۰۱/۱۷ **تاریخ پذیرش: ۱۴۰۱/۰۳/۱۶**

چکیده

هدف این مقاله بررسی اصول رقابتی حاکم بر فضای سایبری جهانی است؛ یکی از راه‌های دست‌یابی بـه ایـن هدف مقایسهٔ نوع نگاه کشورها به‌ویژه قدرت‌های بزرگ به این موضوع است؛ با توجه به این مسئله سـؤال اصـلی پژوهش این است که روسیه و آمریکا چه دیدگاهی نسبت به حاکمیت سایبری دارند؟ در یـک زمینـهٔ گسـترده‌تـر دیدگاه آن‌ها نسبت به این حاکمیت متأثر از چه عواملی است؟ در پاسخ، پژوهش حاضـر بـا بهـره‌گیـری از روش توصیفی- تحلیلی نشان می‌دهد که همانند فضای واقعی، روسیه از حاکمیت وستفالی در فضای سـایبری حمایـت می‌کند؛ اما تحلیل این حاکمیت نشان می‌دهد که این نوع حاکمیت بیشـتر در مـورد روابـط روسـیه و کشـورهای غربی حاکم است و در ارتباط با کشورهای شوروی سابق روسیه از مدل حاکمیت پساشوری استفاده مـی‌کنـد؛ در مقابل آمریکا از مدل چند ذی‌نفعی در حاکمیت سایبری بهره می‌برد؛ اما بررسی دقیق‌تر این مدل نیز نشان می‌دهـد که آمریکا از این مدل صرفاً برای حفظ هژمونی خود در فضای سایبری بهره برده و در فضای داخلی قائل به نقش کنترل‌گر دولت است. پژوهش همچنین نشان می‌دهد بسیاری از اختلاف‌های روسیه و آمریکا در زمینـهٔ حاکمیـت سایبری ناشی از دو متغییر اساسی ایدئولوژی سیاسی حاکم بر نظام سیاسـی و نظـم مطلـوب در نظـام بـین‌المللـی است.

کلیدواژه‌ها:فضای سایبری، حاکمیت، روسیه، آمریکا، اختلاف.

۱. دکترای روابط بین‌الملل از دانشگاه گیلان (نویسنده مسئول). Asgar.safari2017@gmail.com

مقدمه

در یک دههٔ گذشته، مسائل مربوط به اینترنت و فضای سایبری جهانی به‌سرعت در دستور کار حکمرانی قرار گرفته و به‌تدریج از جایگاه حاشیه‌ای به جایگاه محوری در عرصهٔ بین‌المللی منتقل شده است. رشد شگفت‌انگیز فضای سایبری حتی باعث گردیده برخی استدلال کنند که امروز ما در آستانهٔ عصر درگیری سایبری هستیم که در آن جنگ‌ها به‌احتمال‌زیاد طولانی‌تر، پنهان‌تر، در مقیاس، اهداف و سرعت شگفت‌انگیزتر بوده و حتی تشخیص آغاز، پایان، دشمنان و انگیزه‌های آنان نیز دشوار خواهد بود. همهٔ درگیری‌های آینده نیز سایبری خواهند بود؛ زیرا رویدادهای مهم برای رخ دادن به مکانیسم‌های سایبری نیاز خواهند داشت؛ در این شکل نوظهور مبارزه، دشمنان سایبری از فضای سایبری برای تضعیف انعطاف‌پذیری سیستمی سایر بازیگران دولتی و غیردولتی حتی مدت‌ها قبل از اعلام عمومی خصومت‌ها یا بروز بحران آشکار؛ برای از کار انداختن عناصر کلیدی داخلی دولت‌ها استفاده خواهند کرد. نشانه‌هایی از این درگیری نیز در سال‌های گذشته ظهور وجود داشته است. به‌عنوان‌مثال افشای اسناد وزارت خارجه و دفاع ایالات‌متحده از سوی سایت ویکی‌لیکس، تأثیرگذاری رسانه‌ها بر شکل‌گیری و نتایج تحولات جهان عرب، مطرح شدن حملات سایبری روسیه و چین علیه آمریکا و مهم‌تر از همه حمله به زیرساخت‌های هسته‌ای ج.ا. ایران، ازجملهٔ همین نشانه‌ها است.

بنابراین شناخت و درک معنای سلسله رویدادهای ذکر شده، به‌ویژه از منظر روابط بین‌الملل، برای فهم بهتر تأثیری که تغییرات فوق بر امنیت ملی، روابط بین دولت‌ها و همچنین نظام حکمرانی فضای سایبری جهانی می‌گذارند به لحاظ نظری و عملی حائز اهمیت است؛ در کنار این موضوع پرداختن به حاکمیت سایبری نیز اهمیت دارد؛ درواقع درک اصل حاکمیت و معنای حاکمیت سایبری عنوان نقطهٔ شروعی برای تحلیل و درک این مسائل بسیار مهم است؛ زیرا از طریق فهم این موضوع است که می‌توان به درک درستی از نوع مواجههٔ کشورها با چالش‌های سایبری و پاسخ‌های متناسب با آن‌ها دست یافت. بررسی این مسئله (حاکمیت سایبری) به‌ویژه در روابط کشورهایی مانند روسیه و

آمریکا نیز بیشتر به فهم موضوع کمک می‌کند؛ زیرا استدلال بر این است که در وضعیت فعلی روابط روسیه و آمریکا اکنون در پایین‌ترین سطح خود از زمان جنگ سرد قرار دارد و رقابت و اختلافات آن‌ها جدای از فضای واقعی و در فضای سایبر نیز تشدید شده است؛ بر همین اساس سؤال اصلی پژوهش حاضر حاکی از این است که روسیه و آمریکا چه دیدگاهی نسبت به حاکمیت سایبری دارند؟ و در یک زمینهٔ گسترده‌تر دیدگاه آن‌ها نسبت به حاکمیت متأثر از چه عواملی است؟

مبانی نظری و پیشینه‌شناسی تحقیق

پیشینه‌شناسی تحقیق

در ارتباط با موضوع مقالهٔ حاضر، پژوهش‌های متعددی صورت گرفته است؛ بااین‌وجود ازجمله جدیدترین پژوهش‌ها در این زمینه می‌توان به موارد زیر اشاره کرد: هارنیش و زتل-شابات[1] (۲۰۲۲) در پژوهشی با عنوان «رازداری و ظهور هنجارها در فضای مجازی، تعامل آمریکا، چین و روسیه و حاکمیت جاسوسی سایبری»، این فرضیه را مطرح می‌سازند؛ در حالی کشورهایی مانند چین و روسیه به سمت حاکمیت سایبری در مقابل سایرین (داخلی و خارجی) رفته‌اند، آمریکا، به‌عنوان یک قدرت دموکراتیک، به‌دنبال امنیت سایبری برای هر دو کشور بوده است. بودنیتسکی[2] (۲۰۲۲) در پژوهشی با عنوان «رویکردی ارتباطی به حاکمیت دیجیتال: استونی الکترونیکی بین روسیه و غرب»؛ منطق‌های فرهنگی زیربنای حاکمیت ملی دیجیتال را بررسی کرده و با تکیه بر نظریه‌های سازنده‌گرایانهٔ هویت ملی و فناوری، رویکردی رابطه‌ای به حاکمیت دیجیتال پیشنهاد می‌کند که به‌طورکلی بر تحلیل پویایی‌های خود-دیگری ملی در توسعهٔ آن تمرکز دارد.

معصومی‌فر (۲۰۲۱) در مقاله‌ای با عنوان «حاکمیت فضای مجازی: آیا سرزمینی کردن فضای مجازی با داشتن اینترنت سازگار جهانی در تضاد است؟» بحث حاکمیت در فضای

1. Harnisch and Zettl-Schabath
2. Budnitsky

سایبری را به درگیری‌ها و کشمکش‌های ژئوپلیتیکی دنیای واقعی ارتباط داده و استدلال می‌کند که مفاهیم مختلف فضای سایبری تابعی از منافع ژئوپلیتیکی قدرت‌های مختلف است. چیسلوا[1] و سوکولووا (۲۰۲۱) در پژوهشی با عنوان «امنیت سایبری در روسیه» این مسئله را مطرح می‌سازند که امنیت سایبری در روسیه یک مفهوم مستقل نیست؛ بلکه بخشی جدایی‌ناپذیر از امنیت اطلاعات ملی است. مهم‌ترین مزیت پژوهش حاضر نسبت به آثار قبلی بررسی مقایسه‌ای حاکمیت سایبری در دو کشور آمریکا و روسیه و ارائهٔ مصداق‌های عینی از اقدامات آن‌ها در حوزهٔ حاکمیت سایبری است.

مبانی نظری

حاکمیت به این‌معنی که دولت‌ها آزادند هر کاری را که می‌خواهند در قلمرو خود انجام دهند برای چندین دهه است که اصل سازمان‌دهنده روابط بین‌الملل است (هاس،[2] ۲۰۰۹). رویکردهای مختلفی هم نسبت به این مفهوم وجود دارد. لیبرال‌ها حاکمیت را برحسب توانایی دولت برای کنترل بازیگران و فعالیت‌ها در داخل و خارج از مرزهایش تعریف می‌کنند. واقع‌گرایان، جوهر حاکمیت را توانایی دولت برای اتخاذ تصمیمات مقتدرانه (تصمیم به جنگ) می‌دانند (تامسون[3]، ۱۹۹۵: ۲) انواع مختلفی از حاکمیت نیز از سوی تئوری‌پردازان این حوزه مطرح شده است؛ به‌عنوان‌مثال استفان کراسنر[4] استدلال دارد چهار نوع از حاکمیت را می‌توان نام برد؛

- حقوقی بین‌المللی (به رسمیت شناختن متقابل بین نهادهای سرزمینی)؛
- وستفالیایی (سازماندهی سیاسی بر اساس حذف بازیگران سیاسی از ساختارهای اقتدار)؛
- داخلی (سازماندهی رسمی اقتدار سیاسی در داخل دولت)؛

1. Chislova and Sokolova
2. Haass
3. Thomson
4. Stephen D. Krasner

- وابستگی متقابل (توانایی دولت برای تنظیم اطلاعات، ایده‌ها، کالاها یا سرمایه در سراسر مرزها) (کراسنر[1]، ۱۹۹۹، ۳).

تا مدت‌ها نیز معنی اصلی و ضمنی حاکمیت بیشتر متوجه قلمرو فیزیکی دولت‌ها بود؛ اما در سال‌های اخیر حاکمیت به قلمرو فضای مجازی نیز گسترش پیدا کرده است؛ به عبارت بهتر استدلال اصلی در این زمینه این است که هرچند فعالیت‌های سایبری دولت‌ها جنبهٔ فیزیکی و ملموسی دارد (به‌عنوان‌مثال در قالب سخت‌افزار و زیرساخت رایانه)؛ اما تعاملات در فضای سایبری از طریق انتقال داده‌ها، سیگنال‌دهی و ارسال محتوا، جنبهٔ «مجازی» دارد؛ بنابراین در این حوزه نیز دولت‌ها نیازمند اقتدار هستند؛ به عبارت بهتر به‌عنوان یک موضوع حاکمیتی، دولت‌ها حق دارند قابلیت‌های سایبری خود را بر اساس خواسته‌ها و منابع خود توسعه دهند؛ در ارتباط با این حق، دولت‌های دیگر موظف‌اند این حق را به رسمیت شناخته و در تصمیمات سایبری داخلی کشور دیگر مداخله نکنند(جِنسن[2]، ۲۰۱۴: ۲۸۷).

این موضوع باعث گردیده مفهوم جدیدی با عنوان حاکمیت سایبری مطرح شود. حاکمیت سایبری در یک تعریف کلی عبارت از گسترش طبیعی حاکمیت دولت در فضای سایبری است؛ یعنی یک دولت دارای صلاحیت (حق مداخله در عملیات داده‌ها) در موارد ذیل است:

- فعالیت‌های فناوری اطلاعات و ارتباطات (در رابطه با نقش‌ها و عملیات سایبری) موجود در فضای سایبری؛
- سیستم‌های فناوری اطلاعات و ارتباطات فی‌نفسه (در رابطه با امکانات) و داده‌های جابه‌جا شده توسط سیستم‌های فناوری‌های اطلاعات و ارتباطات (دارایی‌های مجازی)(فانگ[3]، ۲۰۱۸: ۸۳).

در این تعریف فعالیت‌های فناوری اطلاعات و ارتباطات به نقش‌های سایبری که معادل «جمعیت شبکه» هستند، مربوط می‌شود. سیستم‌های فناوری اطلاعات و ارتباطات فی‌نفسه

1. Krasner
2. Jensen
3. Fang

به امکاناتی مربوط می‌شوند که پلتفرم‌های حامل فضای سایبری هستند و معادل «فضای سایبری سرزمینی» هستند و صلاحیت اشاره به حق دخالت در تأسیسات، داده‌ها و عملیات داده‌ها دارد که معادل «رژیم سایبری» است. همهٔ این مطالب نیز به این نکته اشاره می‌کنند که حاکمیت فضای سایبری هر چهار عنصر حاکمیت دولت را به ارث می‌برد، ویژگی «رژیم» حاکمیت فضای سایبری را روشن می‌کند؛ یعنی یک رژیم، «فضای سایبری سرزمینی»، «منابع سایبری» که در «فضای سایبری سرزمینی» وجود دارد، جمعیت و عملیات را در فضای سایبری کنترل می‌کند (فانگ، ۲۰۱۸: ۸۴).

به‌طور مشخص‌تر در حاکمیت سایبری بر سه مؤلفهٔ اصلی بسیار تأکید می‌شود که عبارت‌اند از:

- **استقلال**: (حق و توانایی یک دولت برای انتخاب مسیر توسعهٔ سایبری، مدل حاکمیت سایبری بدون مداخلهٔ خارجی)؛
- **برابری**: (حق یک کشور برای مشارکت در حکمرانی جهانی فضای مجازی و تدوین قانون)؛
- **صلاحیت قانونی**: (حق و توانایی یک کشور برای تنظیم قوانین برای زیرساخت‌ها، نهادها، رفتار و همچنین داده‌ها در قلمرو خود ب (هوآنگ[1] و همکاران، ۲۰۲۱).

کشورهایی مانند چین و روسیه از مهم‌ترین حامیان این مدل حاکمیتی هستند؛ در واقع این دو کشور بر مفهومی از حاکمیت سایبری تأکید دارند که به همهٔ کشورها اجازه می‌دهد تا در فضای سایبری بر اساس برابری عمل کنند (گائو[2]، ۲۰۲۲: ۳). حاکمیت سایبری مخالفانی نیز دارد. استدلال اصلی مخالفان این است که اعمال حاکمیت کلاسیک دولت بر حوزهٔ سایبری برخلاف روح اینترنت است که بر مفهوم اتصال نامحدود متکی است؛ به‌عنوان‌مثال میلتون مولر[3] استدلال می‌کند که در حالت ایده‌آل، به رسمیت شناختن متقابل حاکمیت در جهان فیزیکی، تعارض را محدود می‌کند و به هر دولت حوزه‌ای غیرقابل‌اعتراض

1. Huang
2. Gao
3. Milton L. Mueller

اختصاص می‌دهد که در آن دولت بتوانـد اقتـدار خـود را اعمـال کنـد؛ امـا وظیفـهٔ اصـلی پروتکل‌های اینترنتی تسهیل سازگاری و تبادل اطلاعـات در بـین فنـاوری‌هـا، رسـانه‌هـا و قلمروها است؛ این باعث می‌شود که ادعاهای حاکمیت ارضی به‌جای نظـم، منبـع درگیـری باشد (مولر[1]، ۲۰۲۰: ۷۹۸).

همچنین این ادعا وجود دارد که بـین حاکمیـت سـایبری کـه جریـان آزاد اطلاعـات را محدود می‌کند و اصل آزادی بیان تضاد وجود دارد (یلی[2]، ۲۰۱۷: ۱۱۰). استدلال اصلی در ایـن مورد این است که محـدودیت بـرای جریـان آزاد اطلاعـات بـه بهانـه محافظـت از حـریم خصوصی ارتباط اطلاعات را محدود کرده و بنابراین توانـایی کـاربران در فضـای سـایبری برای بیان خواسته‌های اصلی خود را محدود می‌کند (اسـپینلو[3]، ۲۰۲۰: ۶۴)؛ در این زمینـه بیشـتر مثال‌ها متوجه چین بوده و عنوان می‌شود که از اواخر دهـهٔ ۱۹۹۰ بـه بعـد، چـین اقـدامات زیادی را برای کنترل محتوای برخط انجام داده که شناخته شـده‌تـرین آن‌هـا دیـوار آتشـین بزرگ است (کریمرس[4]، ۲۰۲۰: ۱۱۸). آمریکا و بسیاری از کشورهای اروپـایی از حامیـان اصـلی جریان آزاد اطلاعات در فضای سایبری هستند.

به‌عنوان‌مثال یکی از اولویت‌های گفتگوی سـایبری اتحادیـهٔ اروپـا –آمریکـا، همـاهنگی نزدیک دو طرف در زمینهٔ ارتقای حقوق بشر برخط در مجـامع بـین‌المللـی ماننـد «ائـتلاف برخط آزادی« بوده است. به‌طور مشابه، گروه جی۷ در نشسـت وزرای دیجیتـال و فنـاوری جی۷ در آوریل ۲۰۲۱، نقشهٔ راه همکـاری در زمینـهٔ جریـان آزاد داده بـا اعتمـاد را ایجـاد کرد(گائو[5]، ۲۰۲۲: ۳)؛ این رویکرد دوگانه باعث شده اسـت کـه نـوعی تقابـل بـین کشـورهای طرفدار این دیدگاه در حوزهٔ سایبری شکل بگیرد که عموماً در قالب رقابت شـرق و غـرب در حکمرانی سایبری توصیف می‌شود؛ یکی از این رقابت‌ها، مدل حاکمیت سایبری روسیه و آمریکا است که در ادامه به آن اشاره می‌شود.

1. Mueller
2. Yeli
3. Spinello
4. Creemers
5. Gao

روش‌شناسی تحقیق

این تحقیق از نوع هدف کاربردی است و با روش توصیفی- تحلیلی انجام شده است؛ روش گردآوری اطلاعات نیز به‌صورت بررسی منابع اسنادی و کتابخانه‌ای ازجمله کتب، پایان‌نامه‌ها، مقالات چاپی و اینترنتی بوده است؛ برای گردآوری اطلاعات نیز از روش فیش‌برداری استفاده شده است. با توجه به اینکه از اسناد و منابع معتبر داخلی و خارجی برای تجزیه و تحلیل موضوع استفاده شده است، پژوهش از روایی و پایایی قابل قبولی برخوردار است.

یافته‌های تحقیق و تجزیه‌وتحلیل داده‌ها

حاکمیت سایبری روسیه

از زمان فروپاشی اتحاد جماهیر شوروی، روسیه؛ علی‌رغم فشارهای موجود در زمینهٔ در اولویت نبودن حاکمیت دولت و فرسایش این مفهوم به حاکمیت به‌عنوان یک اصل اساسی در سازماندهی روابط بین‌الملل نگاه کرده است. قانون اساسی ۱۹۹۳ روسیه به صراحت تأکید دارد که حاکمیت یک مفهوم اساسی بوده و باید در سراسر قلمرو کشور اعمال شود (قانون اساسی روسیه[1]). تأکید بر مفهوم حاکمیت در اظهارات مقامات روسیه نیز برجسته بوده است. ولادیمر پوتین بارها در اظهارات خود به اهمیت مفهوم حاکمیت برای روسیه اشاره داشته است؛ وی در سال ۲۰۰۷ در انجمن والدای کلاب عنوان داشت «برای روسیه، حاکمیت نه یک تجمل سیاسی، نه مایهٔ افتخار؛ بلکه شرط بقا در این جهان است(آرکادیویچ[2]، ۲۰۱۷)؛ البته باید به این مسئله نیز اشاره کرد روسیه دو برداشت متفاوت از مفهوم حاکمیت دارد.

یکی از آن‌ها مدل سنتی یا وستفالیایی است که برای خود روسیه و کشورهای خارج از فضای شوروی سابق اعمال می‌شود؛ اما در داخل (منظور کشورهای شوری سابق) نوعی از حاکمیت توسعه‌یافته است که تا حد زیادی می‌توان آن را در قالب رویکرد پسا-شوروی

1. constitution.ru
2. Аркадьевич

تعریف کرد؛ در این رویکرد حاکمیت دولت‌ها (جمهوری‌های استقلال یافته از روسیه) در رابطه با بازیگران «خارجی» غیرقابل تعرض اما در رابطه با روسیه قابل نفوذ تلقی می‌شود(دیاموند[1]، ۲۰۱۶: ۶)؛ این برداشت دوگانه به حوزهٔ سایبری نیز سرایت کرده است.

بر اساس دیدگاه اول (مدل وستقالیایی حاکمیت) روسیه جزء قدرت‌های پیشرو«سایبری وستفالیایی» به‌شمار می‌رود؛ به عبارت بهتر مفهوم حاکمیت سایبری برای روسیه، در قالب حق و توانایی دولت برای تعیین منافع ملی به‌صورت مستقل در محیط دیجیتالی تعریف می‌شود (آشمانوف[2]، ۲۰۱۳)؛ این برداشت نیز متأثر از رویدادهای تاریخی از جمله فروپاشی شوروی بوده است. مهم‌ترین درس فروپاشی شوروی برای روسیه به بی‌اعتمادی عمیق نسبت به غرب و ایدئولوژی لیبرال بود (لاهمن[3]، ۲۰۲۱: ۷۹). همین بی اعتمادی هست که باعث شده روسیه ایدهٔ جریان آزاد اطلاعات را که به عقیدهٔ آن منجر به گسترش ایده‌های لیبرال و کنترل شدید بر جریان اطلاعات در داخل و خارج از روسیه می‌شود را رد کرده و به دنبال اعمال حاکمیت در فضای سایبری باشد. مقامات روسیه فضای سایبری را تهدیدی بزرگ برای امنیت ملی روسیه می‌دانند؛ زیرا عقیده دارند که جریان اطلاعات در فضای سایبری می‌تواند اقتدار رژیم را تضعیف کند. به همین دلیل هم هست که مقامات روسیه از طریق قوانین و ابتکارات سایبری، تلاش می کنند تا فضای سایبری روسیه را کنترل کنند(تاباچنیک و توپور[4]، ۲۰۲۰) از جمله اقدامات در این زمینه عبارتند از:

رونت یا اینترنت روسی

رونت، اینترنت روسی یا بخشی از اینترنت با محتوای روسی زبان بوده که بخش ملی – روسی اینترنت کرملین است (داویدوف[5]، ۲۰۲۰: ۵) رونت یک فضای برخط نسبتاً بسته و مبتنی بر زبان روسی است. رونت همچنین یک محیط مستقل با موتورهای جستجوی توسعه‌یافته

1. Deyermond
2. Ashmanov
3. Lahmann
4. Tabachnik and Topor
5. Davydov

و بسیار محبوب، سایت‌های شبکه‌های اجتماعی و خدمات ایمیل رایگان است (نیککاریلا و ریستولاینن[1]، ۲۰۱۷: ۳۰)؛ البته برخی تحلیل‌گران استدلال دارند که رونت صرفاً یک فضای برخط نیست و ابعاد مختلفی دارد؛ به عنوان مثال از دید آسمولوف[2] و کولوزاریدی[3] رونت دارای ابعاد زیر است:

- فناورانه (کابل‌های فیبر، دامنه‌ها، پلت‌فرم‌های برخط مختلف و زیرساخت‌های نظارت)؛
- فرهنگی (ابزاری برای توسعهٔ فضای فرهنگی)؛
- رسانه‌ای (نوع جدیدی از پلتفرم‌های رسانه‌ای و ارتباطی)؛
- سیاسی (بسج سیاسی، توانمندسازی دولت برای کنترل و نظارت بر جمعیت)(اسمولوف و کولوزریدی[4]، ۲۰۲۱: ۲۸۱-۲).

نهادهای کنترل و نظارت

از مهم‌ترین نهادهای کنترل و نظارت روسیه در حوزهٔ سایبری می‌توان به سرویس فدرال نظارت بر ارتباطات، فناوری اطلاعات و رسانه‌های جمعی (روسکومنادزور[5]) اشاره کرد. روسکومنادزور یک نهاد اجرایی است که وظایف مانند کنترل و نظارت بر رسانه‌های جمعی (از جمله رسانه‌های جمعی الکترونیکی)، نظارت بر ارتباطات جمعی، فناوری اطلاعات و مخابرات؛ نظارت و کنترل انطباق قانونی بر پردازش داده‌های شخصی و مدیریت فعالیت‌های خدمات فرکانس رادیویی را انجام می‌دهد (سایت سرویس فدرال برای نظارت بر ارتباطات، فناوری روسیه). از مهم‌ترین اقدامات روسکومنادزور در سال‌های اخیر می‌توان به مقابلهٔ آن با توئیتر و فیسبوک اشاره کرد. در ۱۰ مارس ۲۰۲۱، روسکومنادزور شروع به سرکوب توییتر به دلیل عدم انطباق با درخواست های حذف

1. Nikkarila and Ristolainen
2. Gregory Asmolov
3. Polina Kolozaridi
4. Asmolov and Kolozaridi
5. Roskomnadzor

محتوای روسی کرده و محدود کردن توییتر بر روی ۱۰۰ درصد خدمات تلفن همراه و ۵۰ درصد از خدمات تلفن ثابت اجرا گردید. در ۵ آوریل ۲۰۲۱، نیز روسکومنادزور به توییتر اولتیماتوم داد تا الزامات را تا ۱۵ مه برآورده کند تا کاملاً مسدود نشود؛ بنابراین تحت فشار توییتر ۹۱ درصد از محتوای ممنوعهٔ درخواستی را حذف و در نتیجه، محدودیت ها در تلفن ثابت در ماه می لغو شد؛ درحالی‌که محدودیت در تلفن همراه همچنان ادامه داشت (خوِ[1] و همکاران، ۲۰۲۱: ۲).

بومی سازی داده

بومی‌سازی داده‌ها به صور کلی اشاره به عمل ذخیره‌سازی داده‌ها بر روی هر دستگاهی است که به صورت فیزیکی در داخل مرزهای کشور خاصی که داده‌ها در آنجا تولید شده می‌شود، دارد و بیشتر به عنوان مکانیزمی برای تحکیم و تقویت حاکمیت سایبری کشورها در نظر گرفته می‌شود (دوگال[2]، ۲۰۱۹: ۳). روسیه در سال ۲۰۱۴، بومی‌سازی داده‌ها را برای نگهداری و پردازش داده‌ها در حوزهٔ قضایی ملی معرفی کرد (قانون افف.زد ۲۴۲)؛ این الزام در ۱ سپتامبر ۲۰۱۵ (قانون اف.زد ۵۲۶) لازم‌الاجرا شد که بر تعهد پردازش داده‌های شخصی شهروندان روسیه با استفاده از پایگاه‌های داده، قرار داده شده در قلمرو روسیه تأکید دارد. روسیه همچنین در سال ۲۰۱۹ «قانون اینترنت مستقل روسیه»[3] را معرفی کرد؛ این قانون در تاریخ ۱ مه ۲۰۱۹ به‌عنوان قانون فدرال «اف.زد-۹۰»[4] معروف به قانون حاکمیت رونت به تصویب رسیده و از نوامبر ۲۰۱۹ به لازم‌الاجرا شد (استادنیک[5]، ۲۰۲۱). به قانون فدرالی «اف.زد ۳۷۴ و اف.زد ۳۷۵»[6] معروف به قانون یاروواوایا[7] نیز می‌توان اشاره کرد؛ این قانون شامل مجموعه‌ای از اصلاحات در قانون ضدتروریسم روسیه است که نقطهٔ عطف مهمی

1. Xue
2. Duggal
3. Russia's sovereign Internet law
4. FZ-90
5. Stadnik
6. FZ-374, FZ-375
7. Yarovaya law

در تشدید کنترل دولت بر فضای سایبری می‌باشد. (لیتوینکو[1]، ۲۰۲۱: ۱۲)؛ البته عملیاتی شدن این قانون تا سال ۲۰۲۳ به تأخیر افتاده است.

راهبرد جایگزینی واردات فناوری

راهبرد جایگزینی واردات فناوری پس از افشاگرهای اسنودن در سال ۲۰۱۳ تقویت شد. روسیه در سال ۲۰۱۵ قانونی دربارهٔ «ترجیح سیستم عامل‌های روسی در خریدهای عمومی» را از طریق دومای دولتی روسیه تصویب کرد (اپیفانووا و دیتریش[2]، ۲۰۲۲: ۱۲-۱۳)؛ بر همین اساس چندین شرکت پیشرو جهانی، از جمله اِنجین‌اِکس[3]، لوکسافت[4]، جت‌برینز[5]، توسط روس‌ها تأسیس شد؛ همچنین غول‌های دیجیتالی روسیه همانند یاندکس[6] و ف-کنتاک[7] در بسیاری از خدمات و شبکه های رسانهٔ اجتماعی موفقیت بدست آوردند؛ علاوه بر این روسیه به سمت امور مالی دیجیتالی حرکت کرد (اپیفانووا و دیتریش، ۲۰۲۲: ۶-۸)[8]، بر اساس دیدگاه دوم (مدل پسا-شوروی) نیز این استدلال از سوی روسیه مطرح می‌شود که هرچند فدارسیون روسیه به‌عنوان دولت مستقل پس از فروپاشی شوروی شکل گرفت؛ اما جانشین اتحادیهٔ جماهیر شوری است و بنابراین اقتدار عالی آن باید در مرزهای سابق شوروی گسترش یابد. با توجه به همین مسئله در چارچوب ذهنی مقامات روسیه یک «روسکی‌میر» یا «جهان روسی»[9] وجود دارد که محدودهٔ آن فراتر از مرزهای فیزیکی فدارسیون روسیه است (کوزدرا[10]، ۲۰۱۸: ۶۲). چنین برداشتی از گسترهٔ مرزهای فدارسیون روسیه صرفاً منوط به مرزهای فیزیکی نیست و روسیه در فضای سایبری و غیرواقعی نیز قائل به چنین قلمرویی

1. Litvinenko
2. Epifanova and Dietrich,
3. Nginx
4. Luxoft
5. JetBrains
6. Yandex
7. VKontakte
8. Epifanova and Dietrich,
9. Russkiy Mir Foundation (Russian World)
10. Kozdra

است؛ به عبارت بهتر جهان روسی هستهٔ اصلی فعالیت سایبری روسیه در فضایی سایبری برای ایجاد مرزهای حاکمیتی خود در اینترنت است؛ یکی از دلایل این امر هم این است که با انحلال شوروی، فدراسیون روسیه و سایر دولت‌ها، شبکهٔ گسترده‌ای از ارتباطات تلفنی و اطلاعاتی را به ارث برده‌اند؛ این شبکه اگرچه به‌معنای واقعی جهانی نیست؛ اما به‌عنوان ستون فقرات اولیه برای توسعهٔ اینترنت و توسعهٔ شبکه‌های آینده در کشورهای شوروی سابق و اروپای شرقی ایفای نقش می‌کند (کریتم[1] و همکاران، ۲۰۲۰: ۶-۷).

بر همین اساس هم روسیه پس از فروپاشی تلاش کرد تا از طریق چارچوب‌های قانونی مانند «مفهوم سیاست اطلاعات دولتی» مصوب دوما در سال ۱۹۹۸ بر اینترنت این مناطق کنترل داشته باشد. (کلاسن[2]، ۲۰۲۰: ۱۴۸)؛ درواقع با در نظر داشت جوامع مختلف روسی زبان، «جامعهٔ متصور»[3] روسیه بسیار فراتر از مرزهای فیزیکی این کشور برای حاکمیت سایبری خود قلمرو قائل است و می‌خواهد حاکمیت سایبری خود را در کشورهای پسا شوروی که دارای جنبه‌های میراث مشترک با روسیه هستند؛ گسترش دهد؛ بنابراین وقتی صحبت از حاکمیت سایبری روسیه می‌شود، می‌توان به این مسئله پی برد که روسیه یک قلمرو ذهنی (جهان روسی) در فضای سایبری برای خود ترسیم کرده و با استفاده از ابزارها و مکانیسم‌های مختلف در تلاش برای اعمال حاکمیت سایبری خود در این قلمرو است.

حاکمیت سایبری آمریکا

آمریکا به‌عنوان یکی از قدرت‌های سایبری غالب از بسیاری از مؤلفهٔ اصلی منابع سایبری از جمله زیرساخت‌ها، شبکه‌ها و سرورها برخوردار است و برخلاف روسیه که از حاکمیت دولتی حمایت می‌کند؛ بیشتر رژیم حاکمیت اینترنت چندذی‌نفعی را ترجیح می‌دهد. مفهوم حکمرانی چندذی‌نفعی در بحث حاکمیت اینترنت بعد از اجلاس جهانی جامعهٔ اطلاعاتی[4] اجلاس سران سازمان ملل ظاهر شد؛ همچنین اولین ارجاع به «رویکرد

1. Kreitem
2. Claessen
3. Imagined Community
4. he World Summit on Information Society (WSIS)

چندذی‌نفعی» در مرحلهٔ مقدماتی به‌عنوان یک حد وسط بین مواضع مختلف بود؛ از یک طرف کشورهای غربی و جوامع تجاری از وضعیت موجود حمایت کرده و مدیریت اینترنت را محدود به مدیریت فنی سیستم نام دامنه[1]می‌کردند که باید از طریق یک رژیم خودتنظیمی خصوصی با نظارت دولت آمریکا انجام می‌شد؛ از سوی دیگر بازیگران متعددی با این دیدگاه مخالفت کرده و مفهوم گسترده تری از حاکمیت اینترنت را که شامل موضوعات سیاست عمومی می‌شد، حمایت می‌کردند. اصطلاح «چندذی‌نفعان» نیز با تأسیس کارگروه حاکمیت اینترنت[2]رسماً وارد زبان حاکمیت اینترنت شد (پالادینو و سانتانیلو[3]، ۲۰۲۱: ۳). برخی از ویژگی‌هایی هم که برخی تحلیل‌گران به رویکرد چند ذی‌نفعی نسبت می‌دهند عبارتند از:

- ذی‌نفع محور (ذی‌نفعان فرایند و تصمیمات را تعیین می‌کنند)
- باز (هر ذی‌نفعی می‌تواند شرکت کند)
- شفاف (همهٔ ذی‌نفعان و مردم به بحث و گفتگو دسترسی دارند)
- مبتنی بر اجماع (نتایج مبتنی بر اجماع، مصالحه و برد-برد است) (استریکلینگ و فورس[4] هیل، ۲۰۱۷: ۳۰۰)

1. Domain Name System
2. the Working Group on Internet Governance (WGIG)
3. Palladino and Santaniello
4. Strickling and Force Hill

شکل ۱. ساده‌سازی شده مدل و یا رویکرد چند ذی‌نفعی

(داتون[1]، ۲۷، ۲۰۱۵)

موضوع دیگری که آمریکا حداقل در ظاهر در حاکمیت سایبری بر آن تأکید دارد، جریان آزاد اطلاعات است؛ به عبارت بهتر از دهۀ ۱۹۹۰، آمریکا از دیدگاه «آزاد و باز» به اینترنت حمایت کرده است؛ این دیدگاه باز به اینترنت شامل هنجارهای لیبرال دمکراسی آمریکایی از جمله آزادی بیان، دسترسی به اطلاعات و بازار آزاد و همچنین برخی از اخلاق آزادی‌خواهانه است (کریمرس[2]، ۲۰۲۰: ۱۰۷)؛ برخی از مهم‌ترین مثال‌های تأکید بر این دیدگاه عبارتند از:

1. Dutton
2. Creemers

- تأکید بیل کلینتون، رئیس‌جمهور سابق آمریکا بر گسترش اینترنت را به‌عنوان ابزاری برای گسترش آزادی از طریق کابل‌های مدرن (باربیسینو[1]، ۲۰۱۹: ۳۲)
- طرح ملی برای حفاظت از زیرساخت‌های اطلاعاتی و دفاع از فضای سایبری ارائه در سال ۲۰۰ با تأکید بر ایدهٔ آزادی اینترنت به‌عنوان یک اصل آزادی مدنی (کار[2]، ۲۰۱۳: ۶).
- تأسیس ، «گروه ویژهٔ آزادی اینترنت جهانی»[3] در سال ۲۰۰۶ توسط کاندولیزا رایس به‌عنوان یک گروه هماهنگی داخلی وزارت امور خارجه برای رسیدگی به چالش‌های آزادی بیان و جریان آزاد اطلاعات در اینترنت (وزارت خارجهٔ آمریکا، ۲۰۰۶)
- تأکید هیلاری کلینتون بر «آزادی اینترنت» به‌عنوان ستون مرکزی «دولت‌مداری قرن بیست و یکم»[4] (کوربالیجا[5]، ۲۰۱۶: ۹۵)

البته لازم به ذکر است که حمایت آمریکا از رویکرد یا مدل چند ذی‌نفعی یا جریان آزاد اطلاعات عمدتاً به دلیل جامع بودن و یا سایر ویژگی‌های مثبت آن‌ها نیست؛ بلکه در یک زمینهٔ گسترده‌تر، سیاست گذاران آمریکا اهمیت مدل چند ذی‌نفعی را ازچشم‌انداز آن در پیشبرد اهداف و منافع ملی کشورشان درک می‌کنند. دلیل این موضوع هم تا حد زیادی روشن است. بسیاری از ابعاد و زیرساخت‌های اینترنت همچنان توسط نهادهای ویژه تحت سلطه منافع اقتصادی آمریکا (یا حداقل منافع کشورهای توسعه‌یافته) اداره می‌شوند و بنابراین تقریباً کاملا خارج از کنترل نهادهای موجود مانند آژانس تخصصی فناوری اطلاعات و ارتباطات سازمان ملل متحد، اتحادیهٔ بین‌المللی مخابرات و خارج از کنترل هر دولت ملی به جز آمریکا هستند.

به همین دلیل هم هست که برخی تحلیل‌گران عنوان داشته‌اند که علی‌رغم لفاظی‌های فراوان در مورد باز بودن، مشارکت، مسئولیت‌پذیری و دموکراسی، مدل حاکمیت فعلی (موسوم به«مدل چند ذی‌نفعی») تا حد زیادی غیردموکراتیک است؛ زیرا تحت سلطهٔ

1. Barbesino
2. Carr
3. Global Internet Freedom Task Force (GIFT)
4. 21st Century Statecraft
5. Kurbalija

گروهی حرفه‌ای از نمایندگان منافع تجاری و سیاسی بوده و قادر بـه رسـیدگی بـه مسـائل کلیدی اینترنت مانند امنیت و مقرون به صرفه بودن دسترسی در کشورهای در حال توسـعه نیست (هیل[1]، ۲۰۱۵: ۲). شاون ام پاورز[2] و مایکل جابلونسکی[3] در کتاب جنگ سایبری واقعی؛ اقتصاد سیاسی آزادی اینترنت به این مسئله اشاره کرده و استدلال می‌کنند که تلاش‌ها بـرای ایجاد یک اینترنت منحصربه‌فـرد و جهـانی کـه بـر اسـاس ترجیحـات حقـوقی، سیاسـی و اجتماعی غربی در کنار «آزادی اتصال» بنا شده باشد، عمدتاً توسط انگیزه‌هـای اقتصـادی و ژئوپلیتیکی هدایت می‌شود تا آرمان‌های بشردوستانه و دموکراتیک کـه معمـولاً بـا گفتمـان سیاسی مرتبط همراه است. علاوه بر این عمیقاً بـا تـلاش‌هـای گسـترده‌تـر بـرای مـدیریت ساختار جامعهٔ جهانی به روش‌هایی که به نفع فرهنگ‌ها، اقتصادهای دولت‌هـا آمریکـایی و غربی باشد، پیوند خورده است. (پاورز و جابلونسکی[4]، ۲۰۱۵: ۲-۳).

از مثال‌های برجسته در این زمینه هم راهبردها و رویکردهای آمریکـا در مـورد شـرکت اینترنتی برای اسامی و اعداد اختصاصـی[5] (آیکـان) اسـت. از سـال ۲۰۱۶ وظـایف مرجـع شماره‌های اختصاصی اینترنت[6] به شناسه‌های فنی عمـومی[7]، یـک نهـاد قـانونی مسـتقل از آیکان انتقال یافت و این نهاد توانست استقلال عمل بیشتری بـه دسـت آورده و از نظـارت آمریکا خارج شود؛ اما آمریکا همچنان خود را ذی‌نفع اصلی در آیکان می‌داند؛ این موضـوع هم تا حد زیادی به دلیل پیوندهـای عمیـق آیکـان بـا آمریکـا اسـت. آیکـان در پاسـخ بـه درخواست وزارت بازرگانی آمریکا برای یک نهاد جدید راه اندازی شد تا مسئولیت اصـلی مدیریت نام‌ها و آدرس‌های اینترنتی را برعهده بگیرد (ویتزنبوک[8]، ۲۰۱۴: ۵۱).

1. Hill
2. Shawn M. Powers
3. Michael Jablonski
4. Powers and Jablonski,
5. internet Corporation for Assigned Names and Numbers
6. Internet Assigned Numbers Authority
7. The Public Technical Identifiers (PTI)
8. Weitzenboeck

در حال حاضر ادارهٔ ملی مخابرات و اطلاعات[1] (آژانسی در وزارت بازرگـانی) نماینـدهٔ دولت آمریکا در کمیتهٔ مشورتی دولتی آیکان است که مشاورهٔ سیاست عمومی را به هیئت مدیرهٔ آیکان ارائه می‌دهد. با این حال پـس از حملـهٔ نظـامی روسـیه بـه اوکـراین در سـال ۲۰۲۲، کنگرهٔ آمریکا اعلام کرد ممکن است رابطهٔ آمریکا با آیکان و چگونگی حفظ رهبری آمریکا در ایـن نهـاد را مجـدداً مـورد ارزیـابی قـرار دهـد (زو[2]، ۲۰۲۲: ۳)؛ البتـه از قبـل نیـز استدلال‌هایی مبنی بر ارزیابی رابطهٔ بین آمریکا و آیکان وجـود داشـت، از جملـه اینکـه؛ از زمانی‌که آیکان کنترل کامل اینترنت را در اختیار گرفت، تغییرات سیاستی بحث برانگیزی را اجرا کرده است؛ همچنین آیکان پس از مستقل شدن، از بحران بودجه رنج می‌برد؛ بنـابراین این نگرانی وجود دارد که مشکلات مالی مـی‌توانـد مـدیریت مقامـات آیکـان را در مـورد مسائل مهم فاسد کند، علاوه بر تمام مسائل داخلی خود، آیکان اکنون در تلاش برای حفـظ قدرت خود بر اینترنت است (گرابوفسکی[3]، ۲۰۱۸: ۷-۹).

موضوع قابل تأمل دیگر در ارتباط با رویکرد آمریکا به رویکـرد چنـدذی‌نفعـی و جریـان آزاد اطلاعات و همچنین مخالف آن با اعمال حاکمیت دولتی در حوزهٔ سایبر، ابتکارات خـود آمریکا در همین زمینه است؛ در این ارتباط می‌توان به مفهوم راهبرد سایبری دفاع رو به جلـو[4] اشاره کرد. بیان رسمی مفهوم عملیاتی «دفاع رو به جلو» در سال ۲۰۱۸ رخ داد. در ماه مـارس این سال، فرماندهی سایبری آمریکا یک دستورالعمل ده صفحه‌ای منتشر کرده و عنوان داشـت که «دفاع رو به جلو تا حد امکان نزدیک به مبدأ فعالیت دشـمن بـوده، دسترسـی مـا را بـرای افشای نقاط ضعف دشمنان، یادگیری مقاصد و قابلیت‌های آن‌ها و مقابله با حمـلات نزدیـک به مبدأ آن‌ها افزایش می‌دهد؛ این دستورالعمل بر نیـاز بـه «درگیـری مسـتمر» تأکیـد دارد کـه «اصطکاک تاکتیکی و هزینه‌های استراتژیک را بر دشمنان تحمیل کرده و آن‌ها را وادار می‌کنـد منابع را به سمت کاهش حملات تغییر دهند.» (اسمیتز[5]، ۲۰۲۰: ۳-۴).

1. The National Telecommunications and Information Administration (NTIA)
2. Zhu
3. Grabowski
4. Defend forward
5. Smeets

فرماندهی سایبری در این دستورالعمل همچنین سه «خط کلی تلاش» را شناسایی کـرده بود که شامل دفاع رو به جلو بود که شامل موارد ذیل بودند:

- موضع‌گیری[1](نیاز به «یک موقعیت سایبری رو به جلو برای کاهش مداوم اثربخشی قابلیت‌های دشمن و کاهش اقدامات و عملیات آن‌ها قبل از رسیدن به آمریکا)
- هشدار («هشدار تقویت‌شده دربارهٔ اقدامات، مقاصد و قابلیت‌های دشـمن» و دفـاع بهتر «از شبکه‌ها، داده‌ها و پلتفرم‌های دولتی و غیرنظامی»)
- نفوذ (تعهد مداوم آمریکا برای مقابله با فعالیت‌های خصمانه و تحمیـل هزینـه‌هـای انباشته برای اقدامات مخرب) (کوسف[2]، ۲۰۱۹: ۴).

آن چیزی هم که از استراتژی سایبری آمریکا قابل استنتاج است ایـن اسـت کـه راهبـرد دفاع روبه جلو مبتنی بر عناصر جدول زیر است.

جدول۱. عناصر راهبرد دفاع روبه جلو استراتژی سایبری آمریکا

آگاهی	جمع‌آوری اطلاعات در مورد تاکتیک‌ها، تکنیک‌ها و رویه‌های دشمن (TTP).
تاب‌آوری	تقویت امنیت سیستم‌ها و شبکه‌ها برای سخت‌تر و پرهزینه‌تر کردن تلاش دشمنان برای دستیابی به اهدافشان و در صورت امکان، بازدارندگی آن‌ها از تلاش.
همکاری	همکاری نزدیک با همتایان در اجرای قانون، در سراسر و بین بخش های صـنعتی، و بین بخش های دولتی و خصوصی برای تقویت دفاع آگاهانه که شامل هیچ‌گونـه تعامل غیرقانونی متقابل نمی‌شود.
توانایی‌ها	توسعهٔ قابلیت‌های مقیاس پذیر، سازگار، قانونی و متنوع برای مقابله با اقـدامات و فعالیت‌های دشمن.
تجزیه و تحلیل	استفاده از راه‌حل‌های امنیت سایبری سازمانی برای کار با سرعت ماشین، همراه بـا تجزیه و تحلیل داده‌های مقیاس بزرگ، بـرای شناسـایی فعالیـت‌هـای مخـرب در مراحل اولیه آن در شبکه‌های مختلف و دارایی‌های سیستم.

(بنتو[3]، ۲۰۲۲: ۸)

1. Positioning
2. Kossef
3. Bento

می‌توان به قوانین و مقرارات خود آمریکا در زمینهٔ کنترل و نظارت بیشتر بر فعالیت‌های صورت گرفته در حوزهٔ سایبری و شبکه‌های دیجیتال نیز اشاره کرد. در جدول زیر برخی از این قوانین و مقرارت به‌صورت خلاصه آورده شده است.

جدول ۲. قوانین و مقررات آمریکا در زمینهٔ کنترل و نظارت در حوزهٔ سایبری و شبکه‌های دیجیتال

قانون/مقررات	تاریخ ابلاغ	هدف ارتباط
فرمان اجرایی ۱۲۳۳۳	دسامبر ۱۹۸۱	ایجاد قانون پایه و اساس چگونگی نظارت آژانس امنیت ملی بر جمعیت ارائهٔ مجوز برای جمع‌آوری فراداده و محتوای ارتباطی آمریکایی‌ها استفاده از برنامهٔ پریزم[1] و برنامه «ام.وای.اس.تی.یی.سی»[2] برای مستندسازی تمام تماس-های خروجی و ورودی از/به کشورهای هدف
قانون میهن پرستی	اکتبر ۲۰۰۱	استفاده از دستگاه‌های استراق سمع برای شمارهٔ تلفن، منابع اینترنتی و ایمیل توسعهٔ تعریف تروریسم برای شامل شدن تروریسم داخلی
قانون حمایت از اینترنت کودکان	دسامبر ۲۰۰۱	الزام کتابخانه‌ها و برخی مدارس برای استفاده از نرم‌افزار فیلترکننده محتوا
قانون امنیت داخلی	نوامبر ۲۰۰۲	تأسیس وزارت امنیت داخلی و دادن اختیار برای تعریف و کنترل تروریسم
قانون اصلاحات اطلاعاتی و پیشگیری از تروریسم	دسامبر ۲۰۰۴	ایجاد دفتر مدیر اطلاعات ملی برای نظارت بر جامعهٔ اطلاعاتی
بخش ۷۰۲ قانون متمم قانون نظارت بر اطلاعات خارجی	جولای ۲۰۰۸	اجازه دادن به آژانس امنیت ملی برای جمع‌آوری داده‌های ارتباطی کاربران همراه با محتوای آن از شرکت‌های فناوری آمریکا و از طریق زیرساخت فیزیکی مجوز مستقیم برای نظارت جمعی بر اتباع خارجی و نظارت غیرمستقیم بر ارتباطات شهروندان آمریکا
قانون آزادی آمریکا	ژوئن ۲۰۱۵	تمدید مقررات منقضی شده قانون میهن پرستی بدون تغییرات قابل توجه در شیوه‌های نظارت جمعی
قانون به اشتراک‌گذاری اطلاعات امنیت سایبری	دسامبر ۲۰۱۵	محافظت از شرکت‌های آمریکایی در برابر شکایت به دلیل نقض حریم خصوصی کاربران هنگام افشای اطلاعات به آژانس‌های فدرال
شفاف‌سازی قانون استفاده از داده‌ها در خارج از کشور	مارس ۲۰۱۸	به‌روز کردن قانون ارتباطات ذخیره‌سازی۱۹۸۶ با مشخص کردن نحوهٔ اداره انتقال داده‌های فراملی

(باربیسینو،۲۰۱۹، ۲-۲۷)

1. PRISM

۲. یک برنامهٔ مخفی «MYSTIC» آژانس امنیت ملی آمریکا برای جمع‌آوری داده‌ها و همچنین محتوای تماس‌های تلفنی از چندین کشور استفاده می‌شود.

تقابل حاکمیت سایبری روسیه و آمریکا در یک زمینهٔ گسترده

همان‌گونه که ملاحظه گردید روسیه و آمریکا دو رویکرد نسبتاً متفاوت به حاکمیت سایبری دارند؛ این تفاوت به نوبهٔ خود ناشی از تفاوت دیدگاه دو کشور به دو موضوع کلان یعنی ایدئولوژی سیاسی حاکم بر نظام سیاسی و نظم مطلوب در نظام بین‌المللی نیز هست. در بعد ایدئولوژی سیاسی، بسیاری از تحلیل‌گران عقیده دارند ایدئولوژی حاکم در ساختار سیاسی و دیدگاه سیاست‌گذارن اصلی روسیه محافظه‌کاری است. محافظه‌کاری یک ایدئولوژی در مورد مدیریت تغییر است. در رویکرد محافظه‌کارانه تغییر و نوسازی باید بر اساس فرهنگ و سنت‌هایی باشد که طی قرن‌ها برای حفظ ملت و تمدن تمدن شکل گرفته است. طیف محافظه‌کاری نیز در قالب مقاومت در برابر تغییر که اغلب محافظه‌کاری سخت نامیده می‌شود و گرایش اصلاح‌طلب‌تر که معمولاً محافظه‌کاری لیبرال نامیده می‌شود وجود دارد (دیسن[1]، ۲۰۲۱: ۱).

از این دید، محافظه‌کاری روسیه به تدریج تکامل یافته و با ایده‌های فرهنگی رمانتیسیسم در اواخر قرن هجدهم ارتباط دارد که بر اهمیت استقلال فرهنگی و زبانی که برای حاکمیت لازم است، تأکید داشت؛ همچنین علی‌رغم اختلاف نظر در مورد عناصر محافظه‌کاری روسیه در دههٔ ۱۸۳۰، وزیر وقت روشنگری مردمی، کنت سرگئی اووارووف[2]، یک ایدئولوژی رسمی برای دولت روسیه تدوین و شعار «ارتدکس، حکومت مطلق، ملیت» را ابداع کرد که می‌توان اجزای این شعار را عناصر محافظه‌کاری روسیه دانست؛ یکی از دلایل اصلی برای این استدلال این است که در تمام مراحل رشد محافظه‌کاری عناصر فرمول «ارتدکس، حکومت مطلق، ملیت» وجود داشته است؛ علاوه براین، این سه عنصرکاملاً متمایز نیستند. به‌ویژه دیدگاه محافظه‌کاران دربارهٔ هویت ملی روسیه اغلب با ارتدکس پیوند خورده و تفکیک این دو دشوار است. حکومت مطلق نیز ارتباط نزدیکی با ایده‌های ارتدکس و ملیت دارد؛ همچنین محافظه‌کاری روسی به همان اندازه که یک پدیدهٔ

1. Diesen
2. Sergei Uvarov

سیاسی است، فرهنگی می‌باشد؛ بر همین اساس دو نوع محافظه‌کاری را می‌توان نام برد؛ محافظه‌کاری دولتی که بر ماهیت خاص دولت روسیه و نیاز به یک دولت قوی تأکید می‌کند و «محافظه‌کاری ارتدوکس–روس (اسلاووفیل)» که بر ماهیت متمایز فرهنگ روسیه تأکید می‌کند (رابینسون[1]، ۲۰۱۹: ۱۳).

در مقابل اندیشهٔ حاکم بر ساختار سیاسی آمریکا لیبرالیسم است. در یک تعریف کلی لیبرالیسم مجموعه‌ای از مصلحت‌های سیاسی است که به‌منظور جلوگیری از استبداد و ترویج همزیستی مسالمت‌آمیز در یک جامعهٔ کثرت‌گرا و در عین‌حال پرورش آزادی فردی است؛ البته این مصلحت‌ها متنوع هستند، یک کل منسجم را تشکیل نمی‌دهند، کاملاً بر اساس پیشبرد اهداف موردنظر توجیه می‌شوند و به‌صورت سلسله‌ای از مبادلات بین کالاهای موردنظر و با توجه به اهداف کلی محدود کردن استبداد، حفظ صلح مدنی و به حداکثر رساندن آزادی مورد استفاده قرار می‌گیرند (مک گوان[2]، ۲۰۰۷: ۱۴)؛ البته فرانسیس فوکویاما[3] در مورد انطباق این مفاهیم با لیبرالیم حاکم بر آمریکا استدلال دارد که لیبرالیسم در معنای سنتی آن یعنی دکترینی که برای محدود کردن اختیارات دولت‌ها از طریق قانون و ایجاد نهادهایی برای حمایت از حقوق افراد تحت صلاحیت آن‌ها به‌کار می‌رود با آن چیزی که در آمریکا با عنوان آزادی‌خواهی[4] نامیده می‌شود، تفاوت دارد. مضمون اصلی آزادی‌خواهی خصومت با یک دولت فراگیر و اعتقاد به تقدس آزادی فردی است(فوکویاما[5]، ۲۰۲۲: ۲۴).

علی‌رغم این تمایزگذاری از سوی فوکویاما، جریان لیبرالی حاکم بر آمریکا کشورهایی مانند روسیه را به‌عنوان یکی عوامل تهدیدکننده اندیشه‌های لیبرالی می‌داند و با توجه به همین تضاد نیز در سال‌های پس جنگ سرد، روسیه نقش اصلی را روند نوظهور سیاست‌های ضد لیبرالی ایفا کرده است که یکی از حوزه‌های آن نیز فضای سایبری بوده است؛ به عبارت بهتر در روسیه بیش از هرجای دیگری، ایدئولوژی لیبرال پس از جنگ

1. Robinson
2. McGowan
3. Francis Fukuyama
4. libertarianism
5. Fukuyama

سرد هم به‌عنوان تهدیدی وجودی برای نظم سیاسی در داخل کشور و هم برای جایگاه روسیه در نظام بین‌الملل درک شده است (لویس[1]، ۲۰۲۰: ۳)؛ به‌عنوان مثال انقلاب‌های رنگی در مناطق پس از شوری که روسیه آن‌ها را به‌عنوان نتایج ایدئولوژی لیبرالی می‌داند باعث ظهوری مفهومی بنام دموکراسی حاکمیتی[2] در ساختار فکری روسیه شده است؛ این مفهوم اصول لیبرال دموکراسی را رده کرده و عنوان می‌دارد روسیه یک کشور غربی با سنت‌های لیبرال که بر حقوق فردی تأکید می‌کند نیست؛ بلکه کشوری با سنت‌های جمع‌گرایی و دولتی قدرتمند است. جمع (یعنی ملت) ارادهٔ حاکمیت خود را از طریق دولت قدرتمندی که از جمع در برابر تحمیل ارادهٔ الیگارشی‌های داخلی یا قدرت‌های خارجی بر آن محافظت می‌کند، تحقق می‌بخشد (فینکل و برودنی[3]، ۲۰۱۲: ۲۸).

در ارتباط با نظم بین‌المللی نیز بین روسیه و آمریکا اختلاف نظر وجود دارد؛ به عبارت بهتر پس از پایان جنگ سرد، روسیه همواره یکی از منتقدین اصلی نظم تک‌قطبی به رهبری آمریکا بوده است. از دید رهبران روسیه از جمله شخص ولادیمیر پوتین آمریکا «با اعلام خود به‌عنوان برندهٔ جنگ سرد» در سال ۱۹۹۱، خود را «پیام‌آورخدا بر روی زمین» دانست که تعهدی ندارد، فقط منافعی دارد و آن منافع نیز مقدس هستند؛ با این حال واشنگتن این واقعیت را درک نمی‌کند که در دهه‌های اخیر «مراکز قدرت جدید» با «نظام‌های سیاسی و نهادهای عمومی» و همچنین «مدل‌های رشد اقتصادی» خود در حال شکل‌گیری و به دست آوردن جایگاهی هستند که حق حمایت از خود و تضمین حاکمیت ملی را دارند؛ بنابراین دوران به اصطلاح نظم جهانی تک‌قطبی به پایان رسیده است (پوتین[4]، ۲۰۲۲).

در مقابل نظم مطلوبی که روسیه از آن حمایت می‌کند نظم بین‌المللی چندقطبی است؛ نظم چندقطبی در حالت کلی به‌معنای توزیع قدرت به‌صورت مساوی در بین بیش از دو دولت–ملت است. رویکرد مسکو به نظم چندقطبی اولین‌بار توسط یوگنی پریماکوف[5]،

1. Lewis
2. sovereign democracy
3. Finkel and Brudny
4. Putin
5. Yevgeny Primakov

نخست‌وزیر سابق روسیه در اواخر دههٔ ۱۹۹۰ بیان شد. تعامل روسیه با مفهوم نظم چندقطبی با دیدگاه بلندمدت سیاست خارجی این کشور که به‌دنبال دور کردن نظام بین‌الملل از نظم تک‌قطبی تحت سلطه آمریکا بوده، هدایت می‌شود؛ بنابراین در اصطلاح سیاسی روسیه، چندقطبی بودن، مظهر جهان‌بینی خوش‌بینانه‌ای است که مبتنی بر توزیع «عادلانهٔ» قدرت در میان انواع قطب‌ها می‌باشد (ماکاریچف[1]، ۲۰۱۱: ۲). موضوع دیگری هم که در این مورد می‌توان اشاره کرد؛ این است که در مفهوم‌پردازی روسیه، اساس نظم جهانی چندقطبی؛ تخطی‌ناپذیری حاکمیت دولت است.

حاکمیت به نوبهٔ خود، خود را در توانایی دولت‌ها برای اجرای سیاست داخلی و خارجی مستقل و بدون دخالت خارجی در امور داخلی خود نشان می‌دهد؛ در همین‌حال تنوع جهانی این مفهوم را می‌رساند که جهان متشکل از ملت‌های مستقل با نظام‌های فرهنگی، اجتماعی و سیاسی به یک اندازه ارزشمند است؛ بنابراین روسیه دنیای چندقطبی را به این دلیل دموکراتیک‌تر، عادلانه‌تر و برابرتر می‌داند که نظم چندقطبی به حقوق مردم مستقل برای زندگی مطابق با ایدئولوژی‌های سیاسی و باورهای فرهنگی آن‌ها احترام می‌گذارد. بر اساس روایت چندقطبی روسیه، تهدید اصلی برای حاکمیت داخلی و تنوع جهانی نیز هژمونی یا انحصار تک‌قطبی (آمریکا) است (که اغلب با تعبیر «یک کشور» و «قدرت انحصاری» از آن یاد می‌شود). هژمونی که رفتارش مرتباً با عبارات انسان‌وارانه، غرور، بدبینی و خودپرستی توصیف می‌شود، ارادهٔ خود را بدون توجه به منافع و هویت‌های ملی بر دیگران تحمیل می‌کند (بودنیتسکی[2]، ۲۰۲۰: ۵).

نتیجه‌گیری

این پژوهش تلاش داشت رویکردهای متعارض روسیه و آمریکا نسبت به حاکمیت در فضای سایبری را نشان دهد؛ بر همین اساس پس از بررسی ابعاد مختلف اقدامات دو کشور در حوزهٔ فضای سایبری به این جمع‌بندی رسید؛

1. Makarychev
2. Budnitsky

- روسیه در فضای سایبری از رویکرد وستفالی حاکمیت حمایت می‌کند؛ به این معنی که نقش زیادی برای دولت در زمینهٔ تنظیم و کنترل فضای سایبری قائل است. از جمله اقداماتی هم که در این زمینه روسیه انجام داده می‌توان به ایجاد اینترنت روسی(رونت)، ایجاد نهادهای کنترل‌گر و نظارتی مانند (روسکومندوز)، بومی‌سازی داده و راهبرد جایگزینی واردات اشاره کرد؛ در عین‌حال بررسی بیشتر مدل حاکمیت روسیه در فضای سایبری نشان داد روسیه در فضای پساشوروی (جمهوری‌های سابق شوروی) از مدل حاکمیت پساشوروی حمایت می‌کند؛ بدین‌معنی که روسیه خود را میراث‌دار اتحاد جماهیر شوروی دانسته و برای خود حق اعمال حاکمیت بر فضای سایبری کشورهای پساشوروی است.
- بررسی رویکرد آمریکا نسبت به حاکمیت در فضای سایبری نیز نشان داد که این کشور در ظاهر تلاش دارد از مدل چند ذی‌نفعی در حاکمیت سایبری طرفداری کند؛ به این معنی که ضمن کم‌رنگ‌تر کردن نقش دولت در کنترل فضای سایبری سهم زیادی برای سایر بازیگران از جمله بازیگران غیردولتی، نهادهای کارشناسی، جامعهٔ مدنی و غیر قائل شود؛ با این حال اقدامات این کشور در حوزهٔ فضای سایبری مانند حفظ وابستگی نهادهای تخصصی اینترنتی مانند آیکان، به‌کارگیری راهبرد دفاع روبه‌جلو و همچنین تصویب و اجرای قوانین دولتی در حوزهٔ فضای سایبری نشان می‌دهد که این کشور نیز همچنان به نقش تنظیم‌گر دولت در فضای سایبری اعتقاد دارد و آن را در بسیاری از حوزه‌ها اجرایی کرده است.
- یافته‌های پژوهش همچنین نشان داد که دو متغیر ایدئولوژی حاکم بر ساختار سیاسی و نظم مطلوب در نظام بین‌المللی در نوع نگاه دو کشور به حاکمیت اثرگذار هستند. در ساختار سیاسی روسیه ایدئولوژی محافظه‌کاری حاکم است و این محافظه‌کاری مخالف هرگونه تغییر بوده و مهم‌تر از همه این‌که بر عنصر حاکمیت و نقش اساسی دولت در همهٔ امور تأکید دارد؛ از سوی دیگر ساختار سیاسی آمریکا مبتنی بر ارزش‌های لیبرالی است و بر همین اساس تلاش دارد نقش

دولت در همهٔ امور از جمله فضای سایبری محدود باشد. از سویی در مورد نظم مطلوب بین‌المللی نیز روسیه از منتقدین اصلی نظم تک‌قطبی به رهبردی ایالات متحده بوده و بنابراین تلاش می‌کند جهان به سمت نظم چندقطبی حرکت کند و در این نظم روسیه به‌عنوان یک بازیگر کلیدی در همه زمینه از جمله حکمرانی فضای سایبری نقش داشته باشد؛ با این حال آمریکا همچنان قائل به نقش رهبری آمریکا در نظم جهانی است و کشورهایی مانند روسیه را نوعی تهدید برای نظم خود می‌داند.

فهرست منابع و مآخذ

- Asmolov, G., & Kolozaridi, P. (2021). **Run Runet runaway: The transformation of the Russian Internet as a cultural-historical object**. The Palgrave Handbook of Digital Russia Studies, 277.
- Barbesino, K. (2019)."Treatment and Evolution of Digital Rights: A Comparative Analysis of China, Russia, the United States, and Germany", Rollins College Honors Program Theses. https://scholarship.rollins.edu/honors/97
- Benton, S. (2022), Defend Forward, A Proactive Model for Cyber Deterrence, Cyber defenders council, Available at: https://www.cybereason.com/hubfs/dam/collateral/ebooks/Defend_Forward_Proactive_Model_Cyber_Deterrence_ebook.pdf
- Budnitsky, S. (2020). Russia's great power imaginary and pursuit of digital multipolarity. Budnitsky, S. (2020). Russia's great power imaginary and pursuit of digital multipolarity. **Internet Policy Review**, 9(3).
- Budnitsky, S. (2022). A Relational Approach to Digital Sovereignty: e-Estonia Between Russia and the West. ***International Journal of Communication***, *16*, 22.
- Carr, M. (2013). Internet freedom, human rights and power. **Australian Journal of International Affairs**, 67(5), 6-18.
- Chislova, O., & Sokolova, M. (2021). Cybersecurity in Russia. International Cybersecurity Law Review, 2(2), 245-251.
- Claessen, E. (2020). "Reshaping the internet–the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU". **Journal of Cyber Policy**. 5(1), 140-157.
- Creemers, R. (2020). China's conception of cyber sovereignty. Governing cyberspace: **Behavior, power and diplomacy**, 107-145.
- Davydov, S. (Ed.). (2020). **Internet in Russia. A Study of the Runet and Its Impact on Social Life**. Springer. Cham
- Deyermond, R. (2016). The uses of sovereignty in twenty-first century Russian foreign policy. **Europe-Asia Studies**, 68(6), 957-984.
- Diesen, G. (2021). **Russian conservatism: Managing change under permanent revolution**. Rowman & Littlefield Publishers.
- Duggal, P. (2019). Data Localization. Data analysis. Available at: https://datacatalyst.org/wp-content/uploads/2020/06/Data-Localization-Pavan-Duggal.pdf
- Dutton, W. H. (2015). Multistakeholder internet governance? World Development Report 2016 Digital Dividends,
- Epifanova, A., & Dietrich, P. (2022). Russia's Quest for Digital Sovereignty: Ambitions, Realities, and Its Place in the World. (DGAP Analysis, 1). Berlin: Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V. https://nbn-resolving.org/urn: nbn: de: 0168-ssoar-77994-6.

- Fang, B. (2018). **Cyberspace Sovereignty Reflections on building a community of common future in cyberspace**. Science Press and Springer Nature Singapore Pte Ltd.
- Finkel, E., & Brudny, Y. M. (2012). Russia and the colour revolutions. **Democratization**, 19(1), 15–36.
- Fukuyama, F. (2022). **Liberalism and its discontents**. Profile Books.
- Gao, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the Western model. **The International Spectator**, 1-16.
- Grabowski, M. (2018). Should the US Reclaim Control of the Internet: Evaluating ICANN's Administrative Oversight Since the 2016 Handover? *Neb. L. Rev. Bulletin*, 1.
- Haass, R. (2004), Sovereignty, Foreign policy, Available at: https://foreignpolicy.com/2009/10/20/sovereignty
- Harnisch, S., & Zettl-Schabath, K. (2022). Secrecy and Norm Emergence in Cyber-Space. The US, China and Russia Interaction and the Governance of Cyber-Espionage. ***Democracy and Security***, 1-29.
- Hill, R. (2015). The true stakes of internet governance. State of Power. An annual anthology on global power and resistance. The Transnational Institute. Available at: http://www. tni. Org/sites/www. Tni. Org/files/download/03_tni_state-of-power-2015_the_true_ stakes of internet governance. pdf.
- Huang, ZH, Cai, C. Dai.L, Ping.L, Li. Y, (2021), Sovereignty in Cyberspace: Theory and Practice. Available at: https://www.wicwuzhen.cn/web21/information/Release/202109/t20210928_23158332.shtml
- Jensen, E. T. (2015). Cyber sovereignty: The way ahead. Tex. Int'l LJ, 50, 275.
- Kosseff, J. (2019, May). The Contours of 'Defend Forward'Under International Law. In 2019 11th International Conference on Cyber Conflict (CyCon) (Vol. 900, pp. 1-13). IEEE.
- Kozdra, M. (2018). "The Boundaries of Russian Identity Analysis of the Concept of Russkiy Mir in Contemporary Russian Online Media". **Lingua Cultura**, Vol.12, No.1, pp.61-66.
- Krasner, S. D. (1999). **Sovereignty. In Sovereignty**. Princeton University Press.
- Kreitem, H., Ragnedda, M. and Muschert, G. W. (2020). "**Digital inequalities in European post-Soviet states**". In Societies and political orders in transition, (pp. 3–15). S. Davydov (Ed.), Springer,
- Kurbalija, J. (2016 B). "Digital Connectivity. From Harmonising Cyberpolicies to Promoting Twiplomacy: How Diplomacy Can Strengthen Asia-Europe's Digital Connectivity". ASEF Outlook Report 2016/2017.
- Lahmann, H. (2021). On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace. **Duke J. Comp. & Int'l L**., 32, 61.

- Lewis, D. G. (2020). **Russia's New Authoritarianism: Putin and the Politics of Order**. Edinburgh University Press.
- Litvinenko, A. (2021). Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty. ***Media and Communication***, *9*(4), 5-15.
- Makarychev, A. (2011). Russia in a multipolar world: Role identities and "cognitive maps". **Revista CIDOB d'afers internationals**, 96(12), 1-19.
- Masoumifar, A. (2022). Cyberspace Sovereignty: Is Territorializing Cyberspace Opposed to Having a Globally Compatible Internet? ***Journal of Cyberspace Studies***, *6*(1), 1-20.
- McGowan, J. (2007). **American liberalism: An interpretation for our time**. Univ of North Carolina Press.
- Nikkarila, J. P., & Ristolainen, M. (2017, May). "'**RuNet 2020'-Deploying traditional elements of combat power in cyberspace?**" In Game Changer: Structural transformation of cyberspace. Kukkola, J., Ristolainen, M., & Nikkarila, J. P. (E.d). (pp. 27-50). Finnish Defence Research Agency.
- Palladino, N., & Santaniello, M. (2021). **Introduction: The IANA Transition and Internet Multistakeholder Governance**. In *Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance* (pp. 1-20). Palgrave Macmillan, Cham.
- Powers, S. M., & Jablonski, M. (2015). **The real cyber war: The political economy of internet freedom**. University of Illinois Press.
- Putin, V.(2022), Russian President Says the Unipolar World Has Come to an End, Available at: https://www.telesurenglish.net/news/Russian-President-Says-the-Unipolar-World-Has-Come-to-an-End-20220617-0018.html
- Robinson, P. (2019). Russian Conservatism. Northern Illinois University Press.
- Russia 1993 constitution, Available at: http://www.constitution.ru/en/10003000-02.htm.
- Smeets, M. (2020). US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection. ***Intelligence and national security,*** *35*(3), 444-453.
- Spinello, R. A. (2020). **Cyberethics: Morality and Law in Cyberspace: Morality and Law in Cyberspace**. Jones & Bartlett Learning.
- Stadnik, I. (2021). Russia: An independent and sovereign Internet? In Power and Authority in Internet Governance (pp. 147-167). Routledge.
- Statute of Roskomnadzor, (2022), Available at: https://eng.rkn.gov.ru/about/statute_of_roskomnadzor/
- Strickling, L. E., & Hill, J. F. (2017). Multi-stakeholder internet governance: successes and opportunities**.** ***Journal of Cyber Policy***, *2*(3), 296-317.
- Thomson, J. E. (1995). State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research. **International Studies Quarterly**, 39(2), 213. Doi: 10.2307/2600847.

- US Department of State. (2006, Dec 28). Global Internet Freedom Task Force (GIFT) Strategy: A Blueprint for Action, https://2001-2009.state.gov/g/drl/rls/78340.htm
- Weitzenboeck, E. M. (2014). Hybrid net: the regulatory framework of ICANN and the DNS. **International Journal of Law and Information Technology**, 22(1), 49–73.
- Xue, D., Ramesh, R., Evdokimov, L., Viktorov, A., Jain, A., Wustrow, E., & Ensafi, R. (2021, November). Throttling Twitter: an emerging censorship technique in Russia. In Proceedings of the 21st ACM Internet Measurement Conference (pp. 435-443).
- Yeli, H. (2017). A three-perspective theory of cyber sovereignty. **Prism**, 7(2), 108-115.
- Zh,L. (2022), A Revisit of the Domain Name System After Russia's Invasion of Ukraine, Congressional Research Service, Available at: https://crsreports.congress.gov/product/pdf/IN/IN11898
- Аркадьевич, К. (2017), Суверенная Россия, Available at: http://council.gov.ru/services/discussions/blogs/83371/