

National Information Network and the realization of cyber governance in the Islamic Republic of Iran with the experience approach of countries

Hafez Mohammadi¹

¹ PhD Student, Strategic Management of Cyberspace, supreme National Defence University, Tehran. hafez.mohammadi@sndu.ac.it

Corresponding author: hafez.mohammadi@sndu.ac.it

Copyright © 2019 The First National Congress of Governance. All rights reserved.

Abstract : Cyberspace can be considered the undisputed birthplace of the maturity of information and communication technology. A complex space consisting of communication and computing hardware and software, control systems, information, humans and the interaction between them. Today, cyberspace is so intertwined with various aspects of human life that without it, the continuation of individual and social life becomes impossible. As the dominance and hegemony of cyberspace over societies, especially our country, is increasing rapidly, so the realization of the rule of this space is vital for the macro management of society. In this regard, many countries with cyber power to manage their cyberspace have designed and implemented a national network of indigenous information. The type of present research is applied and futuristic and its research method is qualitative and descriptive-analytical. First, the information required for this research was collected based on library resources and by analyzing documents in this field, and then it was studied and analyzed, describing the concepts of governance, cyber governance and the national information network. Considering the cyberspace ecosystem of the country based on domestic requirements and the principled policy of the Islamic Republic of Iran against the arrogant front and global Zionism to explain the components of the desirability of establishing a national information network in the country using the experiences of two leading countries in this field. Russia and China.

Keywords: National Information Network, Governance, Cyber Governance, Cyberspace, Information and Communication Technology

شبکه ملی اطلاعات و تحقق حکمرانی سایبری در جمهوری اسلامی ایران با رویکرد تجربه کشورها

حافظ محمدی¹

1 - دانشجوی دکتری، مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی، تهران

چکیده. فضای مجازی را می‌توان مولود بلا منازع بلوغ فناوری اطلاعات و ارتباطات دانست. فضایی پیچیده متشکل از سخت افزارها و نرم-افزارهای ارتباطی و محاسباتی، سیستم‌های کنترلی، اطلاعات، انسان و تعامل بین آنها. امروزه فضای مجازی آن چنان با ابعاد مختلف زندگی بشر درهم تنیده است که بدون آن امکان تداوم زندگی فردی و اجتماعی غیرممکن می‌نماید. از آنجا که تسلط و هژمونی فضای مجازی بر جوامع و به ویژه کشور ما با شتاب روزافزونی در حال افزایش است، بنابراین تحقق حکمرانی این فضا برای مدیریت کلان جامعه دارای اهمیت حیاتی است. در این راستا بسیاری از کشورهای صاحب قدرت سایبری برای مدیریت فضای سایبر خود مبادرت به طراحی و اجرایی نمودن شبکه ملی اطلاعات بومی نموده‌اند. نوع پژوهش حاضر کاربردی و آینده نگرانه است و روش تحقیق آن کیفی و از نوع توصیفی-تحلیلی است. در ابتدا اطلاعات مورد نیاز برای این پژوهش با استناد به منابع کتابخانه‌ای و با تحلیل و بررسی اسناد در این حوزه، گردآوری شده و سپس مورد مذاقه و تحلیل قرار گرفته است و با توصیف مفاهیم حکمرانی، حکمرانی سایبری و شبکه ملی اطلاعات، با در نظر داشتن زیست بوم فضای مجازی کشور بر مبنای اقتضائات داخلی و سیاست اصولی جمهوری اسلامی ایران در مقابله با جبهه استکبار و صهیونیسم جهانی به تبیین مولفه های مطلوبیت استقرار شبکه ملی اطلاعات در کشور با استفاده از تجربیات دو کشور پیشرو در این زمینه یعنی روسیه و چین پرداخته است.

کلیدواژگان: حکمرانی، حکمرانی هوشمند، فناوری اطلاعات و ارتباطات، فضای مجازی، دولت الکترونیک

مقدمه

امروز شرایط ویژه‌ای را در سطح جهان تجربه می‌کنیم که بسیاری از آن به عنوان دوره گذار در جهان صحبت می‌کنند. به فرمایش مقام معظم رهبری (۱۰ / ۱۱ / ۹۰) « امروز تاریخ جهان، تاریخ بشریت، بر سر یک پیچ بزرگ تاریخی است. دوران جدیدی در همه‌ی عالم دارد آغاز می‌شود. «یکی از مهم‌ترین پیش‌رانه‌ی این پیچ تاریخی، فناوری اطلاعات و ارتباطات به عنوان یک فناوری تحول آفرین و پیدایش زیست بوم فضای مجازی است که با تأثیر فزاینده خود در حال شکل دادن به تمام عرصه‌های زندگی حقیقی است به نحوی که امروزه فاصله بین مجاز و حقیقت در این فضا به صفر رسیده است. این فضا تمام ساحت‌های حیات بشری را آن گونه تحت تأثیر قرارداده است که دنیای ما را در کمیت و کیفیت دچار تحولاتی عمیق ساخته به نحوی که فضای مجازی به اندازه انقلاب اسلامی اهمیت پیدا کرده است.

گسترش فضای مجازی پس از گذار از عصر کشاورزی و صنعتی، تحولات گسترده‌ای را به همراه داشته و دریچه‌ای به سوی دوران پسامدرن گشوده است. این تحولات تمامی ابعاد زندگی فردی و اجتماعی مردم جهان را تغییر داده و در حال ایجاد یک تمدن جدید است، تمدنی که در آن نه قلمرویی وجود دارد و نه حکومت به معنای متعارف آن؛ از این رو حکمرانی فضای مجازی یکی از چالشی‌ترین حوزه‌های پیش روی حاکمیت‌هاست و موفقیت در آن نیازمند کسب شناختی صحیح از این پدیده و مواجهه‌ای فعالانه با آن است.

فضای مجازی را می‌توان مولود بلا منازع بلوغ فناوری اطلاعات و ارتباطات دانست. فضایی پیچیده متشکل از سخت افزارها و نرم افزارهای ارتباطی و محاسباتی، سیستم‌های کنترلی، اطلاعات، انسان و تعامل بین آنها. امروزه فضای مجازی آن چنان با ابعاد مختلف زندگی بشر درهم تنیده است که بدون آن امکان تداوم زندگی فردی و اجتماعی غیرممکن می‌نماید. در واقع در استفاده کردن یا نکردن از این فضا هیچ گونه حق انتخابی وجود ندارد. به همین دلیل بهترین گزینه در مورد استفاده از این فضا، بهره‌گیری از فرصت‌ها و پرهیز از تهدیدات آن است. در این راستا بسیاری از کشورهای صاحب قدرت سایبری برای مدیریت فضای سایبر خود مبادرت به طراحی و اجرایی نمودن شبکه ملی اطلاعات بومی نموده‌اند. شبکه ملی اطلاعات به عنوان زیر ساخت ارتباطی فضای مجازی کشور شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده است به صورتی که درخواست‌های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند به هیچ وجه از طریق خارج کشور مسیر یابی نشود و امکان ایجاد شبکه‌های اینترنت، خصوصی و امن داخلی در آن فراهم شود. (مرکز ملی فضای مجازی، ۱۳۹۲)

نگاه درون‌زا با تقویت حاکمیت ملی در عرصه فضای مجازی و افزودن بر دارایی‌های حیاتی آن در این عرصه، مانع خدشه دار شدن این حاکمیت به دلیل تبعیت از حاکمیت پلتفرم‌های خارجی می‌شود. طبق این راهبرد، شبکه ملی اطلاعات یک کلید واژه است که مفهوم این کلید واژه حاکمیت جمهوری اسلامی در فضای مجازی است. امروزه ایجاد شبکه ملی اطلاعات امن، به عنوان یک راهبرد اساسی در اعمال حاکمیت کشورها در فضای مجازی محسوب شده و بیشتر کشورها نسبت به ایجاد و ارائه خدمات بر روی این بستر اهتمام نموده‌اند.

از آنجا که تسلط و هژمونی فضای مجازی بر جوامع و به ویژه کشور ما با شتاب روزافزونی در حال افزایش است، بنابراین تحقق حکمرانی این فضا برای مدیریت کلان جامعه دارای اهمیت حیاتی است. در این راستا طراحی کلان شبکه ملی اطلاعات و بهره‌برداری از آن موجب مدیریت صحیح فضای مجازی و در نهایت ارتقاء حکمرانی آن در کشورمان خواهد گردید و عدم استقرار شبکه ملی اطلاعات، نظام مدیریت این فضا را ناکارآمد، تهدیدات سیاسی، اجتماعی، اقتصادی و ... آن را افزون و خارج از کنترل حاکمیت خواهد ساخت.

مهم‌ترین پژوهش‌های انجام شده در ارتباط با موضوع این تحقیق عبارتند از:

نصرت آبادی در پژوهشی با عنوان "ارائه الگوی راهبردی ارزیابی شبکه ملی اطلاعات" با بررسی موضوع امنیت شبکه ملی

اطلاعات، الگوی راهبردی ارزیابی شبکه ملی اطلاعات را در سه بعد امنیتی، مدیریتی و فناورانه ارائه نموده است. (نصرت آبادی، ۱۳۹۸)

میرزاپور در تحقیقی با عنوان "چالش‌های حکمرانی و تنظیم‌گری فضای مجازی در کشور" با بررسی چالش‌های حکمرانی فضای مجازی، نتیجه‌گیری کرده است که برای حکمرانی این فضا صرفاً به فرآیندهای تقنین و اعمال قانون نمی‌توان بسنده کرد؛ بلکه باید با حضور فعالانه در آن خصوصاً از طریق ایجاد زیرساخت‌های فناورانه به حکمرانی در این فضا پرداخت. کنشگری هوشمند در حوزه فضای مجازی با به خدمت گرفتن ظرفیت نهادهای فعال در حوزه حکمرانی فضای مجازی اعم از شورای عالی فضای مجازی، وزارت ارتباطات و فناوری اطلاعات، معاونت علمی و فناوری ریاست جمهوری، کمیته فضای مجازی مجلس شورای اسلامی و ... با ایجاد پلتفرم‌های مرجع محقق می‌شود. (میرزاپور، ۱۳۹۸)

کیان خواه در پژوهشی با عنوان "چالش‌های راهبردی حکمرانی با گسترش فضای سایبر" به بررسی چالش‌های راهبردی حکمرانی با گسترش فضای سایبر پرداخته و هژمونی آمریکایی در مدیریت و کنترل فضای سایبر، شناسایی و نظارت فراحاکمیتی بر توانمندی‌های اقتدارافزای جامعه، تهدیدات و تهاجمات سایبری، پذیرش الگوی رفتاری و سبک زندگی فراملی و فرافرهنگی و مهندسی و مدیریت فرهنگی فراملی را به عنوان چالش‌های راهبردی حکمرانی عرصه جهانی سازی سایبری احصاء نموده است. (کیان خواه، ۱۳۹۷)

غلامی در پژوهشی با عنوان "الگوی شش ضلعی حکمرانی جمهوری اسلامی ایران در فضای مجازی" الگوی حکمرانی فضای مجازی را برای جمهوری اسلامی با توجه به اصول راهبردی کشور در مواجهه با فضای مجازی، با شش محور اساسی شامل شبکه ملی اطلاعات، شبکه فراملی اطلاعات، نظام حقوق بین الملل، گفتمان مواجهه انقلابی، شرکت-های بزرگ غیردولتی با رویکرد فراملی و ایجاد بسیج سایبری با رویکرد محتوایی ارائه نموده است. (غلامی، ۱۳۹۸)

نوع پژوهش حاضر کاربردی و آینده نگرانه است و روش تحقیق آن کیفی و از نوع توصیفی-تحلیلی است. در ابتدا اطلاعات مورد نیاز برای این پژوهش با استناد به منابع کتابخانه‌ای و با تحلیل و بررسی معتبرترین اسناد در این حوزه، گردآوری شده و سپس مورد مذاقه و تحلیل قرار گرفته است و با توصیف مفاهیم حکمرانی، حکمرانی سایبری و شبکه ملی اطلاعات، با در نظر داشتن زیست بوم فضای مجازی کشور بر مبنای اقتضائات داخلی و سیاست اصولی جمهوری اسلامی ایران در مقابله با جبهه استکبار و صهیونیسم جهانی به تبیین مولفه‌های مطلوبیت استقرار شبکه ملی اطلاعات در کشور با استفاده از تجربیات دو کشور پیشرو در این زمینه یعنی روسیه و چین پرداخته است.

ماهیت فناورانه فضای مجازی و خاستگاه شکل‌گیری و گسترش آن، منجر به شکل‌گیری چالش‌هایی برای حکمرانی این فضا شده است لذا مسئله اصلی این پژوهش، حکمرانی این فضای نوظهور با استقرار شبکه ملی اطلاعات و با رویکرد تجربه‌های کشورهای پیشرو در این حوزه برای کشورمان است.

مبانی نظری پژوهش

حاکمیت موضوعی درباره شیوه تعامل دولتها و دیگر سازما نه‌ای اجتماعی با یکدیگر، شیوه ارتباط آنها با شهروندان و شیوه گرفتن تصمیمات در جهانی پیچیده است. حاکمیت فرآیندی است که از آن طریق جوامع یا سازمان‌ها تصمیمات مهم خود را می‌گیرند و مشخص می‌کنند چه کسانی در این فرآیند درگیر شوند و چگونه وظیفه خود را به انجام برسانند. (کاملی و الوانی، ۱۳۹۰). سیستم حاکمیت، چارچوبی است که فرآیند متکی بر آن، بدین معناست که مجموعه‌ای از توافقات، رویه‌ها، قراردادهای سیاستها را مشخص می‌کنند که قدرت در دست چه کسی باشد و تصمیمات چگونه اتخاذ و وظایف چگونه انجام شوند (Folke, Hahn, Olsson & Norberg, 2005)

حکمرانی در واقع، قدرت برتری است که در حیطه دولت کشور، اراده‌ای فراتر از آن وجود ندارد، به گونه‌ای که در مقابل

اعمال اراده و اجرای اقتدارش مانعی نمی‌پذیرد و از هیچ قدرت دیگری تبعیت نمی‌کند. این قدرت و اقتدار حاصل شده بر پایه ملت دارای هویت مشترک شکل گرفته که در پهنه جغرافیایی خاصی زیست می‌کنند. این اقتدار درونی و هویت ملی و مشترک با گسترش فضای مجازی در حال به چالش کشیده شدن است. (کیان خواه، ۱۳۹۷: ۶)

فضای مجازی فضایی فناوری پایه، مبتنی بر فناوری اطلاعات و ارتباطات است که در آن تولید محتوا، پالایش داده، ذخیره سازی داده، پردازش داده و توزیع داده صورت می‌گیرد و در تعامل با انسان فضایی شبکه‌ای را می‌سازد که این فضا دارای خصوصیات مختلف و حتی منحصربه‌فردی است که آن را از فضاهای پیشین مجزا و متفاوت می‌کند. (فیروز آبادی، ۱۳۹۸: ۱۳)

حاکمیت در قانون بین الملل یک مفهوم واضح است؛ در حالی که حاکمیت فضای مجازی به طور کلی مفهوم مبهمی است که اغلب در ارتباط با قدرت دولتی و استقلال در فضای مجازی استفاده می‌شود. بنابراین، مفهوم حاکمیت فضای مجازی باید دقیق‌تر تعریف شود.

در تعریف معنای حکمرانی فضای مجازی، می‌توان به تعریف حکمرانی اینترنت از سوی اجلاس جهانی سران درباره جامعه اطلاعاتی (WSIS)^۱ اشاره نمود: حکمرانی اینترنت، توسعه و کاربرد اصول، هنجارها، قوانین، رویه‌های تصمیم‌گیری و برنامه‌های شکل‌دهنده تکامل استفاده از اینترنت از سوی دولت‌ها، بخش خصوصی و جامعه مدنی، هر یک در نقش خاص خود می‌باشد.

شبکه ملی اطلاعات بستری است امن، پیشرفته و متکی به جدیدترین فناوری های نوین و بومی برای تحقق فضای مجازی براساس ارزش های والای اسلامی-ایرانی جهت رسیدن به اهداف چشم انداز ایران ۱۴۰۴. این شبکه بنابر تکالیف قانونی و مصوبات شورای عالی فضای مجازی باید تحت نظارت مرکز ملی فضای مجازی، توسط وزارت ارتباطات و فناوری ایجاد شود و پس از صدور مجوز توسط مرکز ملی فضای مجازی، آغاز به کار نماید و خدمات خود را به عنوان زیرساخت ارتباطی فضای مجازی، به آحاد ملت اعم از کاربران حقیقی و حقوقی در بخش‌های مختلف دولتی، عمومی و خصوصی ارایه نماید.

بر اساس مصوبه اول جلسه پانزدهم شورای عالی فضای مجازی، "شبکه ملی اطلاعات"، به عنوان زیرساخت ارتباطی فضای مجازی کشور، شبکه ای مبتنی بر قرارداد اینترنت به همراه سوئیچ ها و مسیریاب ها و مراکز داده ای است به صورتی که درخواست های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می شود به هیچ وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه های اینترنت و خصوصی و امن داخلی در آن فراهم شود. (مرکز ملی فضای مجازی، ۱۳۹۶)

برخی از مؤلفه های مطلوبیت برای فضای مجازی در راستای چشم انداز بیست ساله ایران اسلامی، در ابلاغیه حکم تشکیل شورای عالی فضای مجازی توسط مقام معظم رهبری به شرح زیر است:

- به حداقل رساندن اتکای کشور به کشورهای دیگر در استفاده از فضای مجازی و توابع آن در عرصه های فنی.
- جذاب سازی و غنی سازی محتوا و خدمات بومی جهت پاسخگویی حداکثری به نیازهای داخلی.
- ساماندهی تبادل اطلاعات با شبکه جهانی.
- فراهم آوردن شرایط لازم برای دستیابی فضای مجازی کشور به بالاترین سطح از امنیت و سلامت برای آحاد مردم، نظام و کلیه نقش آفرینان در فضای مجازی.
- استفاده حداکثری از فضای مجازی به منظور ارتباط و همکاری وسیع و هدفمند با ملت‌ها خصوصا ملل مسلمان در

¹ World Summit on the Information Society

جهت ترویج و تحقق گفتمان انقلاب اسلامی.

فضای مجازی دارای یک مدل چند لایه‌ای است که بستر آن، زیرساخت ارتباطی است که شبکه ملی اطلاعات آن را محقق خواهد ساخت. بر این اساس، دستیابی به فضای مجازی مطلوب بدون تحقق بستر آن یا شبکه ملی اطلاعات معنا ندارد. این توضیح، اهمیت تبیین مدل شبکه ملی اطلاعات را روشن می‌سازد. تحقق شبکه ملی اطلاعات، در واقع تحقق بستر مطلوب برای فضای مجازی مطلوب کشور است. بدون تردید، توسعه دانش‌بنیان این شبکه، انعطاف و انطباق همیشگی آن با الزامات جدید فضای مجازی را تضمین خواهد کرد. شکل زیر نمایی از افق و ضرورت تحقق شبکه ملی اطلاعات را نشان می‌دهد. (مرکز ملی فضای مجازی، ۱۳۹۶)

جایگاه شبکه ملی اطلاعات در مدل مفهومی لایه ای فضای مجازی

فضای مجازی را با مبنا قرار دادن وجه انسانی و نه بستر فناورانه و تعاملات اطلاعات، می‌توان امتداد فرهنگ و اجتماع انسانی در فضای شبکه های اطلاعاتی بر بستر فناوری اطلاعات و ارتباطات و به عبارتی دیگر، اجتماع و فرهنگ نوین انسانی که در بستر فناوری اطلاعات و ارتباطات شکل می‌گیرد، دانست. فضای مجازی دارای ویژگی‌های زیر است:

- افراد و جوامع، از طریق فضای مجازی، با همدیگر روابط اجتماعی دارند و خود را سازماندهی می‌کنند.
- بنگاه‌های تجاری بصورت ملی و بین‌المللی، در فضای مجازی، تجارت کالا و خدمات می‌کنند.
- سرعت ارتباط و تبادل (اطلاعات، دارایی و فناوری) در فضای مجازی بسیار بالاست.
- امنیت و عملکرد موثر زیرساخت‌های ملی (ازجمله انرژی، بانکداری و امور مالی، حمل و نقل، ارتباطات و صنایع) به فضای مجازی متکی هستند.
- زندگی روزمره مردم بطور فزاینده‌ای در سراسر جهان به تاروپود فضای مجازی درآمیخته شده است.

الزامات شبکه ملی اطلاعات

الزامات شبکه ملی اطلاعات بر اساس مصوبه دوم جلسه پانزدهم شورای عالی فضای مجازی عبارت است از:

- شبکه‌ای متشکل از زیرساخت‌های ارتباطی با مدیریت مستقل کاملاً داخلی؛
 - شبکه‌ای کاملاً مستقل و حفاظت شده نسبت به دیگر شبکه‌ها (از جمله اینترنت) با امکان تعامل مدیریت شده با آنها؛
 - شبکه‌ای با امکان عرضه انواع محتوا و خدمات ارتباطی سراسری برای آحاد مردم با تضمین کیفیت از جمله قابلیت تحرک؛
 - شبکه‌ای با قابلیت عرضه انواع خدمات امن اعم از رمزنگاری و امضای دیجیتالی به کلیه کاربران؛
 - شبکه‌ای با قابلیت برقراری ارتباطات امن و پایدار میان دستگاه‌ها و مراکز حیاتی کشور؛
 - شبکه‌ای پر ظرفیت، پهن باند و با تعرفه رقابتی شامل مراکز داده و میزبانی داخلی.
- نیازمندی‌های عملکردی قابل استخراج از الزامات شش‌گانه شورای عالی فضای مجازی عبارتند از:
- مدیریت مستقل کاملاً داخلی
 - تعاملات مدیریت شده با دیگر شبکه‌ها
 - مسیریابی داخلی درخواست داخلی برای اطلاعات داخلی
 - برقراری ارتباطات امن و پایدار دستگاه‌ها و مراکز حیاتی

- ارایه انواع محتوا و خدمات ارتباطی سراسری
 - ارایه انواع خدمات امنیتی (رمزنگاری و امضای دیجیتالی) به کلیه کاربران
 - ارایه خدمات مراکز داده و میزبانی داخلی
- الزامات غیرعملکردی قابل استخراج از الزامات شش گانه شورای عالی فضای مجازی عبارتند از:

- کاملاً مستقل
- پرمهریت و پهن باند
- حفاظت شده از دیگر شبکه ها
- ارایه خدمات با تعرفه رقابتی
- ارایه خدمات با تضمین کیفیت و تحرک (مرکز ملی فضای مجازی، ۱۳۹۶)

بررسی تجربیات کشورهای روسیه و چین در راه اندازی شبکه ملی اطلاعات

موضوع "بخش روسی اینترنت 1" (RUnet) بر اساس چارچوب نظری "همسوسازی فضای سایبر با مرزهای ملی ۲"، که توسط میلتن مولر^۳ (۲۰۱۷) تدوین شده است، قابل بررسی و تحلیل است. در این چارچوب به جای جداسازی فنی و فیزیکی شبکه یک کشور از اینترنت، تلاش‌هایی برای همسوسازی نظارت و کنترل بر فضای سایبری با مرزهای ملی صورت گرفته است. از سوی دیگر، کشور چین نیز در زمینه اجرای ملی شدن اینترنت، تلاش‌های بسیاری نموده است تا ساختار اینترنت کشور را برخلاف دیگر کشورها، به یک شبکه داخلی ملی (اینترنت) تبدیل نماید. در ایران، شبکه ملی اطلاعات، زیرساخت فضای مجازی کشور بوده و بستری است امن، پیشرفته و متکی به جدیدترین فناوری‌های نوین و بومی، برای تحقق اهداف و ارزش‌های والای نظام جمهوری اسلامی ایران. موضوع حائز اهمیت دارا بودن شبکه ارتباطی امن و فراخور نیازهای ملی، منحصر به کشورهای مذکور نبوده و در اغلب کشورها از جمله آمریکا، از زمان‌های گذشته با عناوینی متفاوت دنبال شده است. مثلاً در آلمان، طرح D21 پهن باند برای حمایت و گسترش جامعه اطلاعاتی برنامه ریزی شده، کانادا در سال ۱۹۹۳ طرحی را برای افزایش توسعه پهن باند و میزان اتصال شهروندان پایه ریزی کرده و استرالیا نیز شرایطی مشابه آمریکا داشته و در این زمینه سازمانی به نام NBN تأسیس کرد که متولی ارائه سرویس شبکه پهن باند ملی است. در ابتدا پس از بیان دیدگاه‌های متفاوت کشورهای روسیه، چین و ایران درباره نوع بیان و تعریف آن‌ها در خصوص شبکه ملی، مدل مفهومی هر یک از کشورها ارائه گردیده است. سپس مؤلفه‌های مطلوبیت و ملاحظات طراحی کشورها و رویکرد آن‌ها در خصوص شبکه ملی تفصیل خواهد شد. در هر بخش به طور مجزا، رویکرد کشورهای روسیه و چین درباره این پدیده، با رویکرد و خط‌مشی جمهوری اسلامی ایران در رابطه با شبکه ملی اطلاعات مورد مقایسه قرار گرفته است.

۱- بخش روسی اینترنت

روسیه مدعی است که مدیریت و حاکمیت بخش روسی زبان شبکه جهانی اینترنت بر عهده این کشور است. این ادعا، مبنی بر ایجاد زیرساخت مستقل منابع شبکه، از جمله DNS برای جلوگیری از تحمیل حاکمیت بر زیرساخت‌های شبکه RUnet در عین حفظ سازگاری با بقیه اینترنت جهانی است. نوع بیان و ادعای روسیه در تعریف بخش روسی اینترنت،

بلکه تمام .ru محدود به "مرزهای جغرافیایی" نبوده و بیشتر بر "زبان روسی" تکیه دارد. این اصطلاح نه تنها مرتبط به وب سایتهایی با دامنه^۱

زبان‌های روسی است.

^۲ cyberspace alignment to national borders

^۳ Milton Mueller

همان‌طور که در شکل ۱ مشاهده می‌شود، حفظ سازگاری و همکاری با اینترنت جهانی بوده و بر این اساس، نهاد نظارت فدرال روسیه با موتورهای جستجو و شرکت‌های Google، Yandex، Sputnik و Mail.Ru درخواست برقراری ارتباط داشته است. این اپراتورها به استثنای گوگل، با سیستم ارتباط برقرار کرده و الزامات قانونی را رعایت کردند. RUnet فرصت توسعه قوانین مرتبط با زیرساخت‌های مهم اینترنت را فراهم کرده و تلاش می‌کند تا امکانی را فراهم آورد تا در شرایط اضطراری یا خاموشی (متوقف شدن سیستم‌ها توسط کشورهای متخاصم)، مستقل از اینترنت کار کند. برای کاربران عادی، اصطلاح RUnet به معنی، دسترسی به خدمات و محتوای وب سایت‌ها برای کاربران روسی، بدون نیاز به مهارت‌های زبان خارجی است. به عنوان مثال موتورهای جستجوگر، خدمات پست الکترونیکی، آنتی‌ویروس‌ها، فرهنگ لغت روسی و ارائه‌دهندگان خدمات آنلاین که دارای یک دفتر در روسیه هستند. (از جمله شرکت‌های خارجی مثل آمازون، یوتیوب، eBay، PayPal و غیره).

با وجود بسیاری از وب سایت‌های بین‌المللی با کیفیت بسیار بالا و جستجوگر گوگل که حدود ۱۰ سال از ساختار روسی پشتیبانی کاملی داشته، امروزه برخی از کاربران روسی علاقه‌ای به استفاده از خدماتی مانند فیس بوک یا گوگل مپ ندارند، زیرا خدمات بومی دارای ویژگی‌های خاص کشور روسیه و دارای جامعه محلی هستند. علاوه بر این، بسیاری از مقامات دولت روسیه به طور فعال از این اصطلاح به عنوان مترادف اینترنت در قلمرو روسیه یعنی زیرساخت‌های اینترنتی که تابع قوانین روسیه است (از جمله قوانین سانسور روسیه، کپی‌رایت، شرکت‌های بزرگ، قوانین تبلیغ و غیره) استفاده می‌کنند.

ایده اصلی RUnet، یک اینترنت مستقل بوده که با شبکه سراسری کره شمالی که کاملاً از اینترنت جهانی جدا است، متفاوت است. این سیستم‌های اینترنتی مستقل، شباهت‌هایی به "شبکه چین" یا مکانیسم‌های کنترلی پیاده‌سازی شده توسط ایران نیز دارد. به ویژه از نظر کنترل جریان داده‌ها از داخل و خارج از کشور و هدف آن‌ها صرفاً کنترل دسترسی به اینترنت در یک منطقه جغرافیایی خاص نیست. بلکه هدف واقعی، تأمین ابزارهای لازم برای اعمال سطح حاکمیتی در حوزه دیجیتال است که در دنیای فیزیکی نیز صورت می‌گیرد. در چنین شرایطی، دولت، کنترل مستقیم زیرساخت‌های اینترنت را در خاک خود به عهده می‌گیرد و به آن اجازه دفاع از سیستم‌ها در برابر حملات خارجی با هدف تضمین تمامیت ارضی مشابه حوزه فیزیکی را می‌دهد.

در حال حاضر، انجمن غیردولتی مستقر در ایالات متحده (ICANN)، زیرساخت‌های پایه اینترنت جهانی را مدیریت می‌کند. برای کشورهایی مانند ایران، روسیه و چین، این وضعیت پر ریسک است، زیرا این سازمان هرچند مستقل از دولت آمریکا بوده، می‌تواند در برابر مداخلات واشنگتن آسیب‌پذیر باشد. در نهایت، مفهوم حاکمیت اینترنت مطلوب این کشور، بر این ایده وابسته است که باید در ایجاد پایه‌های عملکرد اصلی اینترنت از طریق کنترل مستقیم بر سرورهای DNS، که اساساً همه ترافیک را به‌صورت آنلاین هدایت می‌کنند، بین کشورها برابری ایجاد شود.

البته برای روسیه این صرفاً تلاشی برای ایجاد برابری در زیرساخت‌های اینترنت نیست. مسکو با در نظر گرفتن تغییراتی در عملکرد RUnet، اهداف عملی تری را در ذهن دارد. با وجود اختلافات فزاینده بین مسکو و غرب و به ویژه با افزایش تمرکز در حوزه سایبر، روسیه نگران آسیب‌پذیری زیرساخت‌های داخلی خود در برابر حملات سایبری بزرگ خارجی است. ضمناً یک زیرساخت مستقل‌تر و توانایی حفظ مقداری از کارکردهای داخلی در هنگام قطع ارتباط با دنیای خارج، می‌تواند دفاعی بیهوده و درعین حال مؤثر را در برابر چنین تهدیدهایی فراهم کند.

درعین حال، امنیت اطلاعات برای تلاش‌های مسکو درباره RUnet از اهمیت اساسی برخوردار است. با توجه به ماهیت ذاتی اینترنت، مکاتبات آنلاین بین شهروندان روسی و اشخاص، اغلب زیرساخت‌های داخلی روسیه را مدنظر قرار نداده و

این خطر را از نظر مسکو ایجاد می‌کند که قدرت‌های خارجی می‌توانند از این طریق، این ارتباطات را پالایش کرده یا در آن اختلال ایجاد کنند. بنابراین، با طراحی مجدد زیرساخت‌های اینترنتی خود برای مقابله با این‌گونه تهدیدات، مسکو همچنین درصدد است تا اطمینان حاصل کند که ارتباطات دیجیتال یا انتقال داده‌ها بین روس‌ها، زیرساخت‌های داخلی این کشور را ترک نمی‌کند. شکل ۱ بخش روسی اینترنت را نشان می‌دهد. (مرکز ملی فضای مجازی، ۱۳۹۸)



شکل ۱: نوع بیان و تعریف بخش روسی اینترنت

۲- پروژه سپر طلایی چین^۱

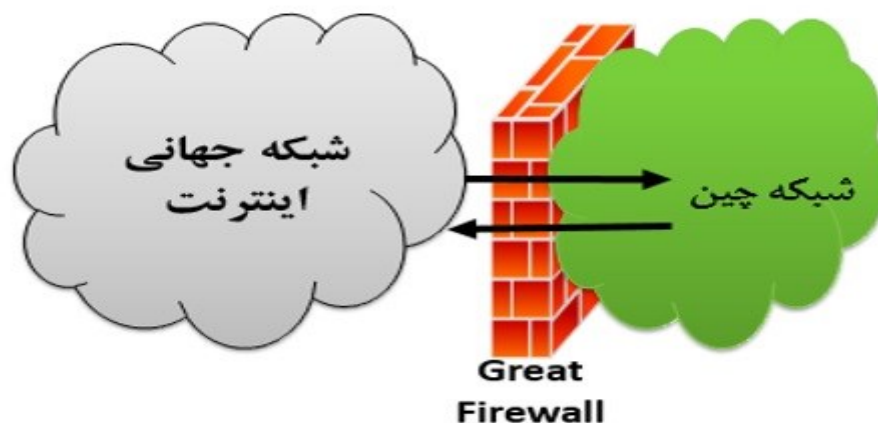
چین جزو کشورهایی است که در کنار استفاده از اینترنت، سال‌هاست شبکه ملی خود را راه‌اندازی کرده است. گفتنی است چین در برابر هجمه سایبری آمریکا بیشترین مقاومت بین‌المللی را تاکنون از خود نشان داده است. به‌طوری‌که تاکنون بیشترین تعداد بازی‌های ملی رایانه‌ای، موتور جستجوی ملی، میل سرورهای ملی و از همه مهم‌تر سیستم عاملی ملی را طراحی کرده است. اخیراً دفتر اطلاعات شبکه اینترنت ملی چین اعلام کرده که استفاده کاربران از وبلاگ‌ها و دیگر خدمات این شبکه با نام‌های مجازی ممنوع است و کاربران باید در فضای مجازی از نام و مشخصات حقیقی خود استفاده نمایند.

پروژه سپر طلایی، که به صورت عامیانه از آن به عنوان فایروال عظیم چین^۲ نیز یاد می‌شود، یک پروژه جهت کنترل و مراقبت از اینترنت است که توسط وزارت امنیت عمومی چین اجرا می‌شود. اجرای این پروژه از سال ۱۹۹۸ آغاز شد. کنترل اینترنت در چین به دلیل طیف وسیعی از قوانین و مقررات اداری بسیار شدید است. بیش از ۶۰ درصد مقررات اینترنتی مربوط به دولت چین، توسط ISPها، شرکت‌ها و سازمان‌های دولتی اجرا می‌شود.

نام "پروژه سپر طلایی" به طور اختصاصی و منحصرأ به سیستم حفاظت اینترنت چین اشاره داشته و به عنوان فایروال بزرگ چین نیز شناخته می‌شود. با این حال، برخی از کارشناسان حوزه فضای مجازی معتقدند که سپر طلایی و فایروال بزرگ، دو موجودیت جداگانه هستند. که فایروال بزرگ یکی از چندین مؤلفه سپر طلایی چین است. برخی نیز معتقدند که پروژه سپر طلایی "چیزی بیش از یک دیوار آتش نیست." یک سیستم نظارت پیشرفته که به دولت این امکان را می‌دهد تا درخواست‌های جستجوی خاص را نظارت کند، فعالیت‌های کاربران اینترنتی را رصد و ردیابی کند^۳. شکل ۲ نوع بیان و تعریف پروژه سپر طلایی چین را نشان می‌دهد.

^۱ GSP= Golden Sheild Project

^۲ GFW = Great Firewall



شکل ۲: نوع بیان و تعریف پروژه سپر طلایی چین

۳. شبکه ملی اطلاعات ایران

شبکه ملی اطلاعات، به عنوان زیرساخت ارتباطی فضای مجازی ایران، از جمله مهم‌ترین پروژه‌های ملی در عرصه فضای مجازی است که تحقق آن بنا بر رویکردهای جهانی و ضرورت‌های ملی مانند ارائه خدمات زیرساختی پیشرفته و مطابق نیازهای کشور، بهره‌مندی از مزایای اقتصادی صنعت و زیست‌بوم ملی فضای مجازی، صیانت و رشد فرهنگ اسلامی-ایرانی در فضای مجازی و حفاظت از اطلاعات و ارتباطات کاربران ایرانی در برابر تهدیدات علیه امنیت و حریم خصوصی، در اسناد بالادستی کشور الزام شده است. شکل ۳ نوع بیان و تعریف شبکه ملی اطلاعات را نشان می‌دهد.



شکل ۳: نوع بیان و تعریف شبکه ملی اطلاعات

رویکرد ایران در تعریف شبکه ملی، به صورت زیرساخت ارتباطی فضای مجازی کشور، شبکه ای مبتنی بر قرارداد اینترنت به همراه سوئیچ ها و مسیریاب ها و مراکز داده ای به صورتی است که درخواست‌های داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می شوند به هیچ وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه های اینترنت و خصوصی و امن داخلی در آن فراهم شود.

در این تعریف، توجه به سه نکته اساسی زیر بسیار حائز اهمیت است:

(۱) شبکه ملی اطلاعات معادل فضای مجازی کشور نیست.

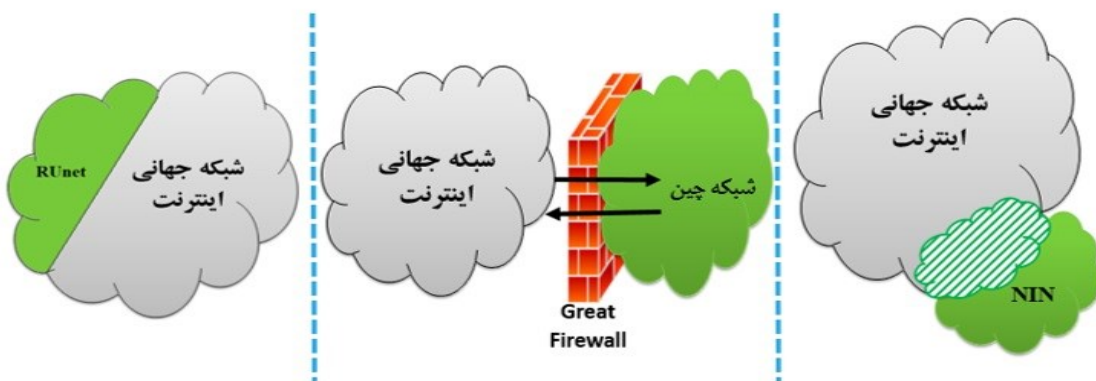
۲) مسیریابی در داخل شبکه ملی اطلاعات، نیازی به منابع خارج از خود ندارد.

۳) محتوی و خدمات میزبانی شده در مراکز داده داخلی، خارج از شبکه ملی نیز قابل دسترسی است.

رویکرد اصلی جمهوری اسلامی ایران در نوع بیان شبکه ملی اطلاعات، افزایش سرعت ارائه محتوا و پهنای باند توسط منابع داخلی، برقراری امنیت و دسترسی دائم و توزیع مناسب منابع و گردش اطلاعات بین شبکه‌های شرکت‌های مختلف ISP به وسیله IXPها و اشتراک گذاری داده‌ها در بخشی مجزا از اینترنت جهانی است. به علاوه، بخش مشترکی با اینترنت جهانی که سرویس‌های قابل دسترس تحت استانداردهای اینترنت جهانی و ترانزیت ترافیک را ارائه می‌نماید. (مرکز ملی فضای مجازی، ۱۳۹۸)

۴. مقایسه نوع بیان و تعریف

در هر سه رویکرد، موضوع و حرف یکسانی با اشکال و ادبیات مختلف بیان می‌شود. همان‌طور که عنوان گردید، نوع بیان و تعاریف این شبکه‌ها متفاوت است. هدف اصلی قانون‌گذاری در روسیه، ایجاد زیرساخت‌های مستقل DNS برای جلوگیری از تحمیل حاکمیت بر زیرساخت‌های شبکه داخلی در عین حفظ سازگاری با بقیه اینترنت جهانی و همکاری نهاد نظارت فدرال روسیه با موتورهای جستجو و شرکت‌های Google، Yandex، Sputnik و Mail.Ru برای درخواست اتصال و همچنین تداوم دسترسی کاربران به شبکه ملی اینترنت در صورت حمله سایبری یا اقدامات خرابکارانه است. در صورتی که به نظر می‌رسد چین با استفاده از فایروال عظیم خود به عنوان بخشی از پروژه سپر تلایی، هدف کنترل و نظارت و بومی‌سازی را دنبال می‌کند و در پایان، رویکرد و نوع بیان ایران در تعریف شبکه ملی اطلاعات، افزایش حاکمیت بر زیرساخت فضای مجازی کشور همچنین ارائه سرویس‌های قابل دسترس تحت استانداردهای اینترنت جهانی و ترانزیت ترافیک است. در شکل ۴، نوع بیان و تعاریف شبکه‌ها نمایش داده شده است. (مرکز ملی فضای مجازی، ۱۳۹۸)

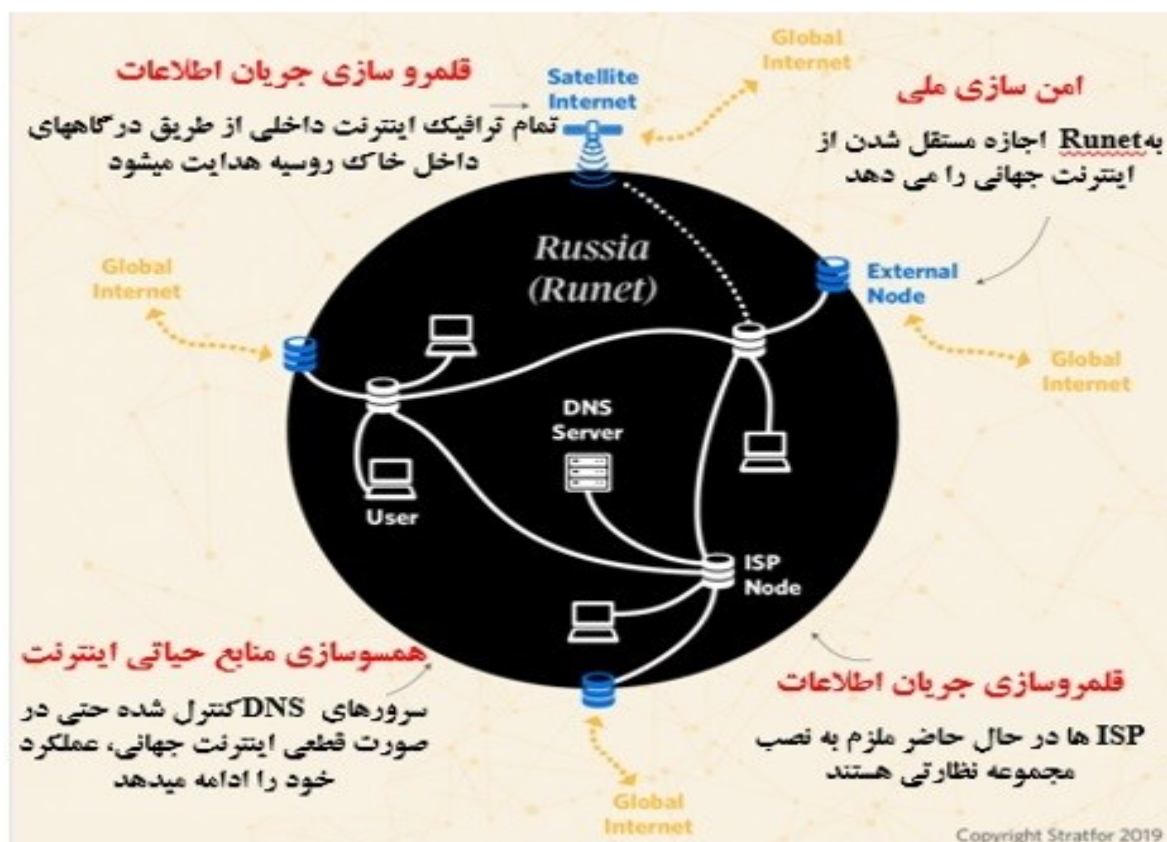


شکل ۴: نوع بیان و تعاریف شبکه‌ها

۵. مدل مفهومی بخش روسی اینترنت

بخش روسی اینترنت، بر اساس چارچوب نظری "همسوسازی فضای سایبر با مرزهای ملی"، که توسط میلتن مولر (۲۰۱۷) تدوین شده است، قابل بررسی و تحلیل است. در این چارچوب به جای جداسازی از اینترنت، تلاش‌هایی برای همسوسازی نظارت و کنترل بر فضای سایبری با مرزهای ملی صورت گرفته است. اگرچه در منابع عمومی، مدل مفهومی یا معماری مشخصی برای RUnet وجود ندارد، لیکن این سه روش اصلی همسوسازی به عنوان مؤلفه‌های اصلی مدل

مفهومی بخش روسی اینترنت مطرح شده است: (۱) امن سازی ملی، (۲) قلمروسازی جریان اطلاعات و (۳) تلاش برای ایجاد کنترل منابع مهم اینترنت در امتداد مرزهای ملی. شکل ۵ مؤلفه‌های کلیدی شبکه حاکمیتی روسیه را نشان می‌دهد.



شکل ۵: مؤلفه‌های کلیدی شبکه حاکمیتی روسی

در گذشته روسیه و چین سعی بر آن داشتند تا مدیریت سیستم DNS را تحت حمایت سازمان ملل قرار دهند و در آنجا نفوذ بیشتری داشته باشند. روسیه معتقد است که باید زیرساخت DNS خود که مستقیماً قابل کنترل است را توسعه دهد. زیرا در صورت جدا شدن از اینترنت جهانی و جلوگیری از وقوع اتفاقات سایبری، نمی‌تواند به زیرساخت‌های جهانی DNS اعتماد کند. دستکاری عملکرد DNS از طریق ساختار فعلی به ضرر آن است. زیرا در چنین شرایطی، دامنه ru ارتباط خود با سایر نقاط جهان را از دست خواهد داد. با این حال، این نگرانی نیز برای روسیه وجود دارد که چنین اقداماتی اینترنت را تضعیف کرده و زیرساخت‌های فعلی متمرکز و همگن DNS را با گروه‌های جداگانه‌ای از شبکه‌های رقابتی DNS جایگزین کند. از این گذشته، هدف اصلی ایجاد زیرساخت‌های مستقل DNS، تحمیل حاکمیت بر زیرساخت‌های شبکه داخلی در عین حفظ سازگاری با بقیه اینترنت جهانی است.

روسیه بر اساس قوانینی، از ارائه‌دهندگان بزرگ خدمات مانند Google، Facebook، Twitter و ... درخواست کرد تا سرورها یا مراکز داده خود را در داخل روسیه مستقر نمایند. این تلاش روسیه برای حفظ ترافیک اینترنت در داخل کشور بسیار مهم و قابل توجه است، ضمن اینکه این عملیات را نیز تحت قانون ملی انجام می‌دهد. ارائه‌دهندگان خدمات اینترنتی که در داخل روسیه فعالیت می‌کنند، طبق قانون موظف هستند تا با ارائه مجموعه نظارتی، اجازه ردیابی ارتباطات

¹ national securitization

² territorialization of information flows,

آنلاین را برای مقامات روسی فراهم نمایند. با نظارت بر ترافیک اینترنت در بین نهادهای روسی این کشور، دولت با تقویت قابلیت‌های امنیتی داخلی خود، امکان ردیابی ارتباطات را تضمین می‌کند. در پاسخ به ظهور اینترنت ماهواره‌ای که این امکان را تهدید می‌کند، مسکو قانونی را تصویب کرد که کلیه ارائه‌دهندگان این‌گونه خدمات را موظف به ایجاد ایستگاه‌های زمینی مستقر در روسیه می‌کند. بر این اساس، حتی اینترنت از طریق امواج هوایی نیز تحت کنترل سیستم نظارتی توسعه‌یافته دولت روسیه است.

تلاش روسیه برای واگذاری مسئولیت به اشخاص خاص در داخل کشور با جداسازی RUnet پیچیده می‌شود. در پایان، یک اینترنت مستقل، راهی برای ثبات سیاسی بیشتر به روسیه ارائه می‌دهد به ویژه اینکه این امر امکان کنترل بیشتر بر روی شبکه‌های غیرقانونی و مقاومت بیشتر در برابر فشارهای بیرونی را فراهم می‌کند. (مرکز ملی فضای مجازی، ۱۳۹۸)

۶. مدل مفهومی پروژه سپر طلایی چین

پروژه سپر طلایی که به صورت عامیانه از آن به عنوان فایروال عظیم چین نیز یاد می‌شود، پروژه ای جهت کنترل و مراقبت از اینترنت است که توسط وزارت امنیت عمومی چین اجرا می‌شود و سه تعبیر متفاوت درباره این شبکه ملی وجود دارد:

- ۱) پروژه سپر طلایی و فایروال عظیم چین دو موجودیت یکسان هستند.
 - ۲) فایروال عظیم چین یکی از چندین مؤلفه سپر طلایی است.
 - ۳) پروژه سپر طلایی و فایروال عظیم چین به موازات یکدیگر عمل می‌کنند.
- بر اساس تعبیر دوم، فایروال عظیم چین (GFW) به عنوان یکی از چندین مؤلفه سپر طلایی و با هدف بلوکه کردن رسانه های اجتماعی، وب سایت ها و برنامه های پیام رسان خارجی مغایر با قوانین خود، به همراه مؤلفه‌های دیگری همچون:
- حذف سیستمی پستهای انتقادی از مقامات کشور
 - محروم شدن از اتصال به تلفن همراه و اینترنت به عنوان مجازات
 - همسوسازی محتوا با ایدئولوژی حزب حاکم بر این کشور
 - تنظیم مقررات برای رسانه‌های آنلاین
 - کنترل و مراقبت از اینترنت و نظارت بر رفتار مردم
 - دستگیری افراد به دلیل پست های غیرقانونی
 - اعمال خشونت علیه فعالان دیجیتالی متخلف
 - لغو دسترسی هکرها و ممانعت از حملات سایبری
- در مدل مفهومی پروژه سپر طلایی چین مطرح شده است. شکل ۶ مدل و اجزای آن را نشان می‌دهد.



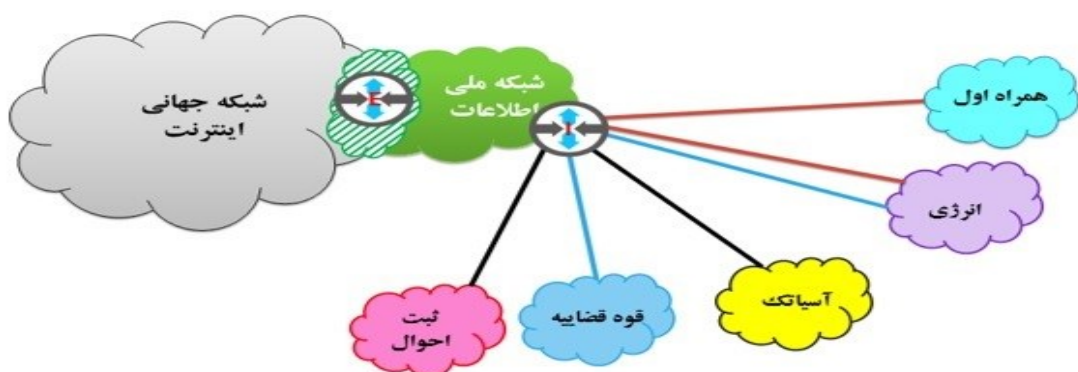
شکل شماره ۶: مدل مفهومی پروژه سپر طلایی چین

۷. مدل مفهومی شبکه ملی اطلاعات ایران

فضای مجازی دارای یک مدل چند لایه‌ای است که بستر آن، زیرساخت ارتباطی است که شبکه ملی اطلاعات نامیده می‌شود. در شکل ۷ مدل مفهومی لایه‌ای فضای مجازی و قلمروی شبکه ملی اطلاعات، در شکل ۸، مدل مفهومی و نحوه ارتباط نمایش داده شده است. (مرکز ملی فضای مجازی، ۱۳۹۸)



شکل شماره ۷: مدل مفهومی لایه ای فضای مجازی و قلمروی شبکه ملی اطلاعات



شکل شماره ۸: مدل مفهومی و نحوه ارتباط در شبکه ملی اطلاعات

۸. مقایسه مدل مفهومی در روسیه، چین و ایران

همان‌طور که در بخش‌های قبل مطرح گردید، مدل مفهومی شبکه‌های ملی در روسیه، چین و ایران متفاوت است. در مدل مفهومی ارائه شده برای بخش روسی اینترنت، توسعه قوانین مرتبط با زیرساخت‌های مهم اینترنت، مستقل شدن از اینترنت در شرایط اضطراری یا خاموشی، دسترسی به خدمات و محتوای وبسایت‌ها برای کاربران روسی بدون نیاز به مهارت‌های زبان خارجی، هدایت تمام ترافیک اینترنت داخلی از طریق درگاه‌های داخل خاک روسیه و ارائه سرویس اینترنت بدون قطعی تحت هر شرایط و فعالیت زیرساخت ملی روسیه بدون دسترسی به اینترنت به عنوان مؤلفه‌های اصلی مطرح می‌شوند.

از سوی دیگر، چین با استفاده از فایروال عظیم خود به عنوان بخشی از پروژه سپر طلایی چین، هدف اصلی کنترل و نظارت و بومی‌سازی را دنبال می‌کند و در این راستا از فعالیت‌هایی همچون حذف سیستمی پست‌های انتقادی از مقامات کشور، محروم شدن از اتصال تلفن همراه و اینترنت به عنوان مجازات، همسوسازی محتوا با ایدئولوژی حزب حاکم بر این کشور، تنظیم مقررات برای رسانه‌های آنلاین، کنترل و مراقبت از اینترنت و نظارت بر رفتار مردم، دستگیری افراد به دلیل پست‌های غیرقانونی، خشونت علیه فعالان دیجیتالی متخلف و لغو دسترسی هکرها و ممانعت از حملات سایبری استفاده می‌کند.

مدل مفهومی شبکه ایران، برقراری تعامل مدیریت شده با اینترنت با هدف ایجاد بستر ارتباطی امن و پیشرفته برای توسعه فناوری اطلاعات و ارتباطات در کشور، ایجاد بستر لازم برای نگهداری و انتقال اطلاعات و ارائه خدمات بومی در داخل کشور، ایجاد زمینه لازم برای تبدیل ایران به عنوان هاب و ترانزیت ترافیک منطقه، صرفه‌جویی و کاهش هزینه‌های ارتباط با اینترنت جهانی، در نظر گرفته می‌شود که توسط مؤلفه‌های زیرساخت ارتباطی، شبکه دسترسی مستقل و پهن باند، ارتباط با شبکه‌های مستقل داخلی و ارتباط با شبکه جهانی اینترنت قابل انجام است. در جدول ۱-۲ مدل مفهومی شبکه‌های ملی اطلاعات در سه کشور روسیه، چین و ایران مقایسه شده است. (مرکز ملی فضای مجازی، ۱۳۹۸)

جدول (۱-۲) خلاصه مقایسه مدل مفهومی در روسیه، چین و ایران

کشور	موارد حائز اهمیت در مدل مفهومی
روسیه	• توسعه قوانین مرتبط با زیرساخت‌های مهم اینترنت • مستقل شدن از اینترنت در شرایط اضطراری یا خاموشی • دسترسی به خدمات و محتوای وبسایت‌ها برای کاربران روسی بدون نیاز به مهارت‌های زبان خارجی • هدایت تمام ترافیک اینترنت داخلی از طریق درگاه‌های داخل خاک روسیه • ارائه سرویس اینترنت بدون قطعی تحت هر شرایطی • فعالیت زیرساخت ملی روسیه بدون دسترسی به اینترنت • ایجاد زیرساخت‌های مستقل DNS برای جلوگیری از تحمیل حاکمیت بر زیرساخت‌های شبکه داخلی در عین حفظ سازگاری با بقیه اینترنت جهانی • همکاری نهاد نظارت فدرال روسیه با موتورهای جستجو و شرکت‌های Google، Yandex، Sputnik و Mail.Ru برای درخواست اتصال

	• تداوم دسترسی کاربران به شبکه ملی اینترنت در صورت حمله سایبری یا اقدامات خرابکارانه
چین	• حذف سیستمی پست‌های انتقادی از مقامات کشور • محروم شدن از اتصال تلفن همراه و اینترنت به عنوان مجازات • همسوسازی محتوا با ایدئولوژی حزب حاکم بر این کشور • تنظیم مقررات برای رسانه‌های آنلاین • کنترل و مراقبت از اینترنت و نظارت بر رفتار مردم • دستگیری افراد به دلیل پست‌های غیرقانونی • خشونت علیه فعالان دیجیتالی • لغو دسترسی هکرها و ممانعت از حملات سایبری
ایران	• زیرساخت ارتباطی فضای مجازی کشور • شبکه امن، مستقل و پهن باند، دارای مدل اقتصادی و بر اساس ضوابط فرهنگی • امکان ایجاد شبکه‌های مستقل داخلی • ارتباط و تعامل مدیریت شده با شبکه جهانی اینترنت

۹. مقایسه مؤلفه‌های مطلوبیت در روسیه، چین و ایران

مؤلفه‌های مطلوبیت این شبکه‌ها متفاوت است. در جدول زیر مقایسه مؤلفه‌های مطلوبیت در روسیه، چین و ایران نمایش داده شده است. (مرکز ملی فضای مجازی، ۱۳۹۸)

جدول (۱-۳) مقایسه مؤلفه‌های مطلوبیت در روسیه، چین و ایران

کشور	مؤلفه‌های مطلوبیت
روسیه	• تحقق حاکمیت اینترنت • افزایش رقابت دولت روسیه در دنیای دیجیتال و ممانعت از انحصار و ایجاد هنجارهای جهانی یک‌طرفه در فضای مجازی • ایجاد اینترنت داخلی مستقل از سایر نقاط جهان و محافظت از ترافیک آنلاین و در صورت لزوم اقدام جهت حمله به ترافیک اینترنت خارجی • بازدارندگی نظامی و استقلال اقتصادی از غرب و مقابله با تهدیدهای خارجی در قالب رقابت بین دولتی • ایجاد هنجارهای مشترک در خصوص رفتار افراد در فضای سایبر

• ممانعت از حذف دامنه‌های .ru و کنترل مستقیم بر سرورهای DNS به جای انحصار مدیریت در (ICANN) (عدم اعتماد به زیرساخت‌های جهانی (DNS))	
• کنترل و مراقبت از اینترنت و نظارت بر رفتار مردم • همسوسازی محتوا با ایدئولوژی حزب حاکم این کشور • مبادله ترافیک میان شرکت‌های مخابراتی محلی • تنظیم مقررات برای رسانه‌های آنلاین • امکان لغو دسترسی هکرها و ممانعت از حملات سایبری • عدم فعالیت شرکت‌های مخابراتی بین‌المللی و خارج نشدن ترافیک اینترنت از مرزهای این کشور • گسترش امور مخابراتی چین به فراتر از مرزهای این کشور	چین
• کاهش اتکای زیرساخت فضای مجازی کشور به دیگر شبکه‌ها در تأمین نیازمندی کاربران خود در فضای مجازی • جذاب سازی و غنی سازی محتوا و خدمات بومی جهت پاسخگویی حداکثری به نیازهای داخلی • مدیریت و ساماندهی تعامل و تبادل اطلاعات با شبکه جهانی اینترنت • فراهم آوردن شرایط لازم برای دستیابی فضای مجازی کشور به بالاترین سطح از امنیت و سلامت برای آحاد مردم، نظام و کلیه نقش آفرینان در فضای مجازی • بهره‌مندی حداکثری کاربران داخلی از مزایای فضای مجازی کشور	ایران

نتیجه گیری

سناریوی کلی کشور به منظور مواجهه صحیح با فضای مجازی و در اختیار گرفتن حکمرانی فضای مجازی با توجه به منویات مقام معظم رهبری، «تغییر رویکرد جمهوری اسلامی ایران از مواجهه انفعالی به مواجهه فعال، خردمندانه و مبتکرانه» است در این راستا تکمیل و بهره برداری از شبکه ملی اطلاعات و خدمات پایه آن به عنوان بستر اصلی حکمرانی فضای مجازی یک اصل می‌باشد. وجود یک برنامه و راهبرد در زمینه طراحی جامع و استقرار شبکه ملی اطلاعات براساس راهبردی بلندمدت بر مبنای مطالعات بومی و با در نظر داشتن تجربیات موفق جهانی و توجه به بحث آموزش و مهارت به کارگیری فناوری‌های نوظهور فضای مجازی در تحقق حکمرانی فضای مجازی نقشی تعیین کننده خواهد داشت. با در نظر داشتن زیست بوم فضای مجازی کشور بر مبنای اقتضائات داخلی و سیاست اصولی جمهوری اسلامی ایران در مقابله با جبهه استکبار و صهیونیسم جهانی و استفاده از تجربیات کشورهای پیشرو در مقابله با استیلای سایبری آمریکا نظیر روسیه و چین، مولفه های مطلوبیت استقرار شبکه ملی اطلاعات در جمهوری اسلامی ایران عبارتند از:

۱. کاهش اتکای زیر ساخت فضای مجازی کشور به دیگر شبکه ها در تامین نیازمندی کاربران خود در فضای مجازی
۲. جذاب سازی و غنی سازی محتوا و خدمات بومی جهت پاسخگویی حداکثری به نیازهای داخلی
۳. مدیریت و ساماندهی تعامل و تبادل اطلاعات با شبکه جهانی اینترنت
۴. فراهم آوردن شرایط لازم برای دستیابی فضای مجازی کشور به بالاترین سطح از امنیت و سلامت برای آحاد مردم، نظام و کلیه نقش آفرینان در فضای مجازی
۵. بهره مندی حداکثری کاربران داخلی از مزایای فضای مجازی کشور

فهرست منابع

منابع فارسی

۱. کاملی، محمدجواد و الوانی، سیدمهدی (۱۳۹۰) شبکه ها و خط مشی گذاری عمومی. تهران، انتشارات دانشگاه علوم انتظامی.
۲. فیروزآبادی، سید ابوالحسن (۱۳۹۸)، فضای مجازی و تحولات آن، مشهد، به نشر، انتشارات آستان قدس رضوی
۳. طرح کلان شبکه ملی اطلاعات (۱۳۹۸)، وزارت ارتباطات و فناوری اطلاعات
۴. غلامی، رضا (۱۳۹۸)، الگوی شش ضلعی حکمرانی ج.ا.ا در فضای مجازی، مرکز ملی فضای مجازی
۵. کیان خواه، احسان (۱۳۹۷)، چالش های راهبردی حکمرانی با گسترش فضای سایبر، فصلنامه علمی امنیت ملی، سال نهم، شماره سی و چهارم، زمستان ۱۳۹۸
۶. میرزاپور، حسین (۱۳۹۸)، چالش های حکمرانی و تنظیم گری فضای مجازی در کشور، اندیشکده حکمرانی شریف
۷. نصرت آبادی، جمشید (۱۳۹۸)، ارائه الگوی راهبردی ارزیابی شبکه ملی اطلاعات، فصلنامه امنیت ملی، سال نهم،

۸. مرکز ملی فضای مجازی، (۱۳۹۲)، (۱۳۹۶)، (۱۳۹۸)، شبکه ملی اطلاعات، بازیابی از:

<http://majazi.ir/page/national-information-network>

۹. حافظ نیا، محمدرضا (۱۳۹۳)، جغرافیای سیاسی فضای مجازی، تهران: سازمان مطالعه و تدوین کتب علوم انسانی

دانشگاهها (سمت)

۱۰. کرامر، فرانکلین و همکاران (۱۳۹۴)، قدرت سایبری و امنیت ملی، تهران: دانشکده اطلاعات، معاونت پژوهش و تولید

علم

۱۱. انتظامی، حسین (۱۳۹۲)، افق فناوری اطلاعات و ارتباطات در نگاه امنیت ملی، تهران، دانشگاه عالی دفاع ملی

۱۲. حسن بیگی، ابراهیم (۱۳۸۸)، حقوق و امنیت در فضای سایبر، تهران: دانشگاه عالی دفاع ملی

۱۳. گزارش فن حکمرانی (فن توسعه انسانی) (۱۳۹۶)، مرکز پژوهش ها مجلس شورای اسلامی

۱۴. گزارش مفهوم تنظیم گری و ارتباط آن با نظام حکمرانی (۱۳۹۷)، مرکز پژوهش ها مجلس شورای اسلامی

منابع انگلیسی

15. Folke, C.; Hahn, T.; Olsson, P. & Norberg, J. (2005). Adaptive Governance of Social-Ecological Systems. *Annual Review of Environment and Resources*, 30, pp. 441-473
16. World Bank, 1999, "Findings on Governance, Institutions and Development", p. 3 •
17. Kaufmann, Daniel, 2003. "Rethinking Governance: Empirical Lessons Challenge •
18. Kettl, D. (2005). *The Next Government of the United States: Challenges for Performance in the 21st Century*. Washington: IBM Center for the Business of Government.
19. Rowland, Jill, Mason Rice, and Sujeet Shenoi. "The anatomy of a cyber-power." *International Journal of Critical Infrastructure Protection* 7, no. 1 (2014): 3-11.
- [20] Rowland, Jill, Mason Rice, and Sujeet Shenoi. "Whither cyberpower?" *International Journal of Critical Infrastructure Protection* 7, no. 2 (2014): 124-137.