بسم الله الرحمن الرحیم

عصر فضای مجازی

گزارش شماره ۸۱

مهر ۱۴۰۰

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

شبکه های ملی باند پهن
(مطالعه کشورهای چین - روسیه و ایران)

محتوای انتشار یافته در این اثر
الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست

تهیه شده درمعاونت فناوری مرکز ملی فضای مجازی

تهیه کنندگان: مجتبی نصیری یار
دکتر مریم حق شناس
نازیلا تقوایی

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶ غربی، پلاک ۲۰
تلفن: ۰۲۱-۸۶۱۵۱۰۶۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

فهرست اشکال

فهرست جداول

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

مقدمه

مقدمه

همان‌طور که در گزارش پیشین مطرح گردید[1]، موضوع «بخش روسی اینترنت (RUnet)»[2] بر اساس چارچوب نظری «همسوسازی فضای سایبر با مرزهای ملی[3]»، که توسط میلتون مولر[4](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 (اینترانت) 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 اهمیتِ دارابودن شبکه ارتباطی امن و فراخور نیازهای ملی، منحصر به کشورهای مذکور نبوده و در اغلب کشورها از جمله آمریکا، از زمان‌های گذشته با

۱. گزارش « RUnet بخش روسی اینترنت » آبان ۹۸

۲. محدود به «مرزهای جغرافیایی» نبوده و بیشتر بر «زبان روسی» تکیه دارد. این اصطلاح نه تنها مرتبط به وب سایت‌هایی با دامنه.ru بلکه تمام زبان‌های روسی است.

3. cyberspace alignment to national borders

4. Milton Mueller is Professor at the Georgia Institute of Technology School of Public Policy, USA. His research focuses on the political economy of the Internet.

عناوینی متفاوت دنبال شده است. مثلاً در آلمان، طرح D۲۱ پهن باند برای حمایت و گسترش جامعه اطلاعاتی برنامه‌ریزی شده، کانادا در سال ۱۹۹۳ طرحی را برای افزایش توسعه پهن باند و میزان اتصال شهروندان پایه‌ریزی 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.

بر اساس جستجوهای متعدد و منابع محدود منتشر شده درباره پدیده توسعه شبکه ملی در کشورها، ازآنجایی‌که مدل مفهومی یا معماری مشخصی برای RUnet وجود ندارد، ک از اقدامات قانون‌گذاری روسیه در این رابطه به زبان روسی یافت شد که اهم بندهای مطرح در آن نیز در بخشی از کتاب حاضر بیان شده 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 تفضیل شد. در هر بخش به طور مجزا، بیانات کشورهای روسیه و چین درباره این پدیده، با رویکرد و خطمشی ج.ا.ا در رابطه با شبکه ملی اطلاعات مورد مقایسه قرار گرفته است.

بخش اول

نوع بیان و تعریف

بخش اول

نوع بیـان و تعریف

۱-۱- بخش روسی اینترنت

روسـیه مدعـی اسـت کـه مدیریـت و حاکمیـت بخـش روسـی زبـانِ شـبکه جهانـی اینترنـت بـر عهـده ایـن کشـور اسـت. ایـن ادعـا، مبنـی بـر ایجـاد زیرسـاخت مسـتقل منابـع شـبکه، از جملـه DNS بـرای جلوگیـری از تحمیـل حاکمیـت بـر زیرسـاخت‌های شـبکه RUnet در عیـن حفـظ سـازگاری بـا بقیـه اینترنـت جهانـی اسـت. نـوع بیـان و ادعـای روسـیه در تعریـف بخـش روسـی اینترنـت، همان‌طـور کـه در شـکل ۱ مشـاهده می‌شـود، حفـظ سـازگاری و همـکاری بـا اینترنـت جهانـی بـوده و بـر ایـن اسـاس، نهـاد نظـارت فـدرال روسـیه بـا موتورهـای جسـتجو و شـرکت‌های Sputnik ، Yandex، Google وMail.Ru درخواسـت برقراری ارتباط داشـته اسـت. ایـن اپراتورهـا بـه اسـتثنای گـوگل، بـا سیسـتم ارتبـاط برقـرار کـرده و الزامـات قانونـی را رعایـت کردنـد.

RUnet فرصـت توسـعه قوانیـن مرتبـط بـا زیرسـاخت‌های مهـم اینترنـت را فراهـم کـرده و تـلاش می‌کنـد تـا امکانـی را فراهـم آورد تـا در شـرایط اضطـراری یـا خاموشـی (متوقـف شـدن سیسـتم‌ها توسـط کشـورهای متخاصـم)، مسـتقل از اینترنـت کار کنـد. بـرای کاربـران عـادی،

اصطلاح RUnet به معنی، دسترسی به خدمات و محتوای وب‌سایت‌ها 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، PayPal، eBay و غیره).

با وجود بسیاری از وب‌سایت‌های 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 فیس‌بوک 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

در حوزه دیجیتالی 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 ایالات‌متحده (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 عملی‌تری 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 درعین‌حال مؤثر را در برابر چنین تهدیدهایی فراهم کند.

درعین‌حال، 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 مد نظر 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.

شکل ۱: نوع بیان و تعریف بخش روسی اینترنت

۱-۲- پروژه سپر طلایی چین[1]

چین جزو کشورهایی است که در کنار استفاده از اینترنت، سال‌هاست شبکه ملی خود را راه‌اندازی کرده است. گفتنی است چین در برابر هجمه الکترونیکی 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[2] 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 ISP ها، شرکت‌ها و سازمان‌های دولتی اجرا می‌شود.

برخی منابع حاکی از آن است که نام «پروژه سپر طلایی» به طور اختصاصی و منحصراً به سیستم حفاظت اینترنت چین اشاره داشته و به عنوان فایروال بزرگ چین نیز شناخته می‌شود. بااین‌حال، برخی از کارشناسان حوزه فضای مجازی معتقدند که سپر طلایی و فایروال بزرگ، دو موجودیت جداگانه هستند. نیویورک تایمز اشاره می‌کند که فایروال بزرگ یکی از چندین مؤلفه سپر طلایی چین است.

1. GSP= Golden Sheild Project
2. GFW = Great Firewall

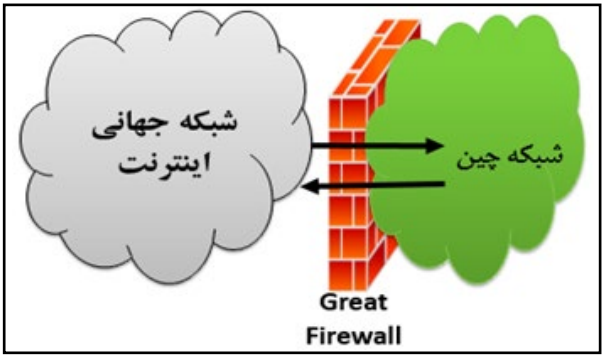
برخی نیز معتقدند که پروژه سپر طلایی»چیزی بیش از یک دیوار آتش نیست.»یک سیستم نظارت پیشرفته که به دولت این امکان را می‌دهد تا درخواست‌های جستجوی خاص را نظارت کند، فعالیت‌های کاربران اینترنتی را رصد و ردیابی کند». سیدنی مورنینگ هرالد[1] مدعی است که این سیستم توسط مقامات برای «حذف ارجاع به موضوعات حساس سیاسی[2]» به صورت آنلاین استفاده می‌شود. به همین ترتیب، اقتصاددان چینی در مجله Open می‌گویند که این فایروال توسط [شرکت فناوری آمریکایی] سیسکو ساخته شده است تا «اطلاعاتی را که توسط رژیم نظارت می‌شوند، بررسی کرده و در نهایت حذف کند». منابع مختلف خاطر نشان می‌کنند که این فایروال دسترسی به وب‌سایت‌های خاص، از جمله فیس‌بوک و توییتر را مسدود می‌کند. منابع دیگر تأیید می‌کنند که دولت از این فایروال برای فیلتر یا مسدود کردن محتوا و نظارت بر فعالیت‌های کاربران اینترنت استفاده می‌کنند. شکل ۲ نوع بیان و تعریف پروژه سپر طلایی چین را نشان می‌دهد.

بنابراین می‌توان این‌گونه جمع‌بندی کرد که به‌طورکلی سه دیدگاه متفاوت از نحوه ارتباط فایروال عظیم چین (GFW) و پروژه سپر طلایی (GSP) وجود دارد:

۱) GFW=GSP: در این تعبیر، GFW و GSP موجودیت یکسانی هستند؛

۲) GFW ∈ GSP: در این تعبیر، GFW عضوی از GSP است؛

۳) GFW ll GSP: در این تعبیر، GFW و GSP دو موجودیت مختلف بوده که به موازات یکدیگر، هدف محافظت و مراقبت از شبکه ملی چین را دنبال می‌کنند؛



شکل ۲: نوع بیان و تعریف پروژه سپر طلایی چین

۱-۳- 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 تهدیدت علیه امنیت و حریم خصوصی، در اسناد بالادستی کشور الزام شده است. شکل ۳ نوع بیان و تعریف شبکه ملی اطلاعات را نشان می‌دهد.

رویکرد ایران در تعریف شبکه ملی، به صورت زیرساخت ارتباطی فضای مجازی کشور، شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده‌ای به صورتی است که درخواست‌های داخلی برای اخذ اطلاعاتی که در مراکز داده

داخلی نگهداری می‌شوند به‌هیچ‌وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت 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 ≠ فضای مجازی کشور

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

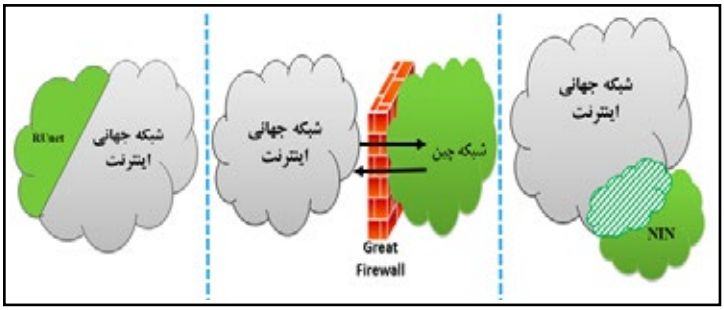
۳) طبیعتاً محتوی و خدمات میزبانی شده در مراکز داده داخلی، خارج از شبکه ملی نیز قابل دسترسی است.

رویکرد اصلی ج.ا.ا 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 IXP ها و اشتراک‌گذاری 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.

شکل ۳ : نوع بیان و تعریف شبکه ملی اطلاعات

۱-۴- مقایسه نوع بیان و تعریف

به نظر می‌رسد 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 شرکت‌هایSputnik ، Yandex، Google و Mail.Ru برای درخواست اتصال و همچنین تداوم دسترسی کاربران به شبکه ملی اینترنت در صورت حمله سایبری یا اقدامات خرابکارانه است. درصورتی‌که به نظر می‌رسد چین با استفاده از فایروال عظیم خود به عنوان بخشی از پروژه سپر طلایی، 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.



شکل ۴ : نوع بیان و تعاریف شبکه‌ها

بخش دوم

مدل مفهومی

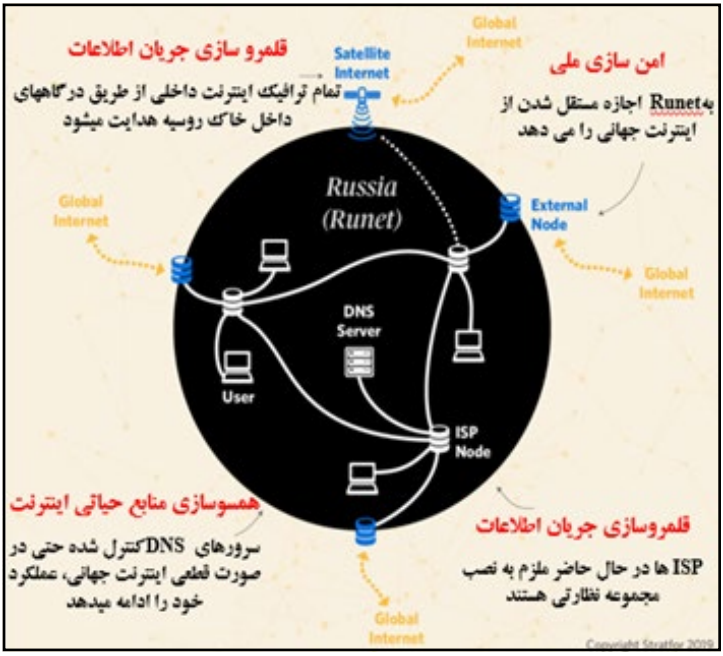
بخش دوم

مدل مفهومی

۲-۱- مدل مفهومی بخش روسی اینترنت

بخش روسی اینترنت، بر اساس چارچوب نظری «همسوسازی فضای سایبر با مرزهای ملی[1]»، که توسط میلتون 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[2]، (۲) قلمروسازی جریان اطلاعات[3] و (۳) تلاش برای ایجاد کنترل منابع مهم اینترنت در امتداد مرزهای ملی. شکل ۵ مؤلفه‌های کلیدی شبکه حاکمیتی روسیه را نشان می‌دهد.

1. cyberspace alignment to national borders
2. national securitization
3. territorialization of information flows



شکل ۵ : مؤلفه‌های کلیدی شبکه حاکمیتی روسی

۱. امن سازی ملی

وابستگی‌های اجتماعی به فناوری‌ها و شبکه‌های اطلاعاتی، آسیب‌پذیری‌هایی را ایجاد می‌کند که خود می‌تواند تهدیدی وجودی[1] برای دولت باشد. این بخش از چهار مؤلفه تشکیل شده است که با سطوح مختلفی از موفقیت و تکامل در لایه‌های مختلف، در روسیه دنبال می‌شوند. (۱) تبیین امنیت سایبری به عنوان یک مسئله امنیت ملی بر اساس اسناد دکترین روسیه. (۲) تمرکز بر هوشمندی مقابله با تهدیدات[2] مبتنی بر برنامه[3] GOSSOPKA و

1. existential threat
2. threat intelligence
۳. سیستم دولتی شناسایی، جلوگیری و مهار (از بین بردن) عواقب ناشی از حملات رایانه‌ای به منابع اطلاعاتی روسیه

ایجاد مرکز هماهنگی ملی در مواجهه با حوادث رایانه‌ای. (۳) اتکا به فن‌آوری‌های تولید ملی (جایگزین واردات نرم‌افزار و برنامه کاربردی) و تلاش برای ملی کردن استانداردهای فنی (۴) ایجاد مرجع قانونی برای قابلیت کلید قطع ارتباط[1] با شبکه خارجی اینترنت.

۲. قلمروسازی جریان اطلاعات

این بخش مربوط به قلمروسازی جریان اطلاعات مرتبط و شامل فیلترینگ محتوای خارجی، قوانین محلی‌سازی داده‌ها[2] و انسداد جغرافیایی[3] است. کشور روسیه ترکیب کاملی از این مؤلفه‌ها را در اختیار دارد. بااین‌حال، شباهتی به سپر طلایی چینی معروف (که در واقع یک فرایند تدریجی برای قلمروسازی داده‌ها و اطلاعات و تدوین قوانینی بود که موجب مسدود شدن وب‌سایت‌ها با محتوای غیرقانونی و فیلتر کردن نتایج موتورهای جستجو می‌شود) ندارد.

۳. همسوسازی منابع حیاتی اینترنت

این بخش به همسوسازی منابع حیاتی اینترنت با مرزهای ملی می‌پردازد. جالب‌توجه‌ترین دلیل این امر، پیامدهای آن در بخش‌بندی فضای اینترنت است. مولر معتقد است که این بخشی از فضای آدرس IP و نام دامنه جهانی است که حکومت و دولت‌ها، با ایجاد اهرم‌هایی می‌توانند برای حکمرانی اینترنت در فضای قلمرو خود (به عنوان بخشی از کل فضای مجازی) از آن بهره برند.

بنابراین بر اساس مؤلفه‌های مدل مفهومی ارائه شده، می‌توان گفت در مفهوم اینترنت حاکمِ مطلوب این کشور، این ایده مطرح

1. kill switch
2. data localization laws
3. geo-blocking

است که باید در ایجاد عملکردهای پایه‌ای وب، بین کشورها برابری وجود داشته باشد. یکی از عناصر اصلی بخش روسی اینترنت در توسعه زیرساختِ مستقل اینترنتی، عملکرد سرورهای DNS است که یک مؤلفه اصلی زیرساخت جهانی اینترنت است. با وجود صدها سرور DNS در روسیه و سراسر جهان، ICANN مدیریت این دایرکتوری را متمرکز کرده است. اما روسیه این نگرانی را دارد که اگر به عنوان مثال ایالات‌متحده به دنبال حذف دامنه ru از این دایرکتوری باشد، مسکو هیچ کنترل مستقیمی بر سرورهای DNS برای جلوگیری از این اقدام ندارد.

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 این‌حال، 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 Twitter، Facebook، Google و ... درخواست کرد تا سرورها یا مراکز داده خود در داخل روسیه را 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 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.

۲-۲- مدل مفهومی پروژه سپر طلایی چین

همان‌طور که در بخش نوع بیان و تعریف شبکه ملی چین،

مطرح شد، پروژه سپر طلایی که به صورت عامیانه از آن به عنوان فایروال عظیم چین نیز یاد می‌شود، پروژه‌ای 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 رسانه‌های اجتماعی، وب‌سایت‌ها و برنامه‌های پیام‌رسان خارجی مغایر با قوانین خود، به همراه مؤلفه‌های دیگری همچون:

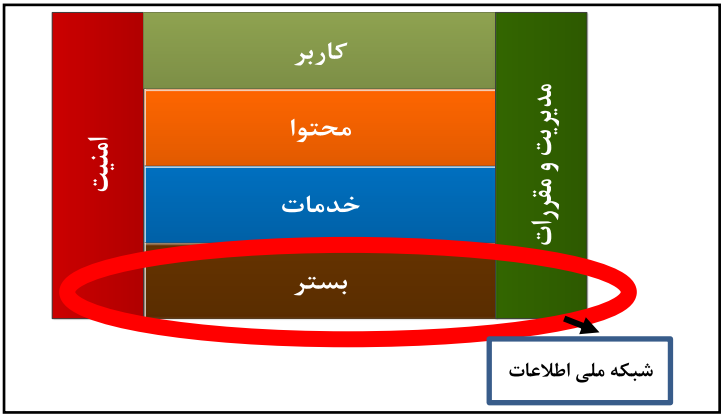
- حذف سیستمی پست‌های انتقادی از مقامات کشور (Content Removal)
- محروم شدن از اتصال به تلفن همراه و اینترنت به عنوان مجازات (Revoking Access)
- همسوسازی محتوا با ایدئولوژی حزب حاکم بر این کشور(Online Manipulation)
- تنظیم مقررات برای رسانه‌های آنلاین (Legislating Censorship)
- کنترل و مراقبت از اینترنت و نظارت بر رفتار مردم (High-Tech Surveillance)
- دستگیری افراد به دلیل پست‌های غیرقانونی(Critics Arrested)
- اعمال خشونت علیه فعالان دیجیتالی متخلف (Violence)
- لغو دسترسی هکرها و ممانعت از حملات سایبری (Technical Attacks)

در مدل مفهومی پروژه سپر طلایی چین مطرح شده است. شکل ۶ مدل و اجزای آن را نشان می‌دهد.

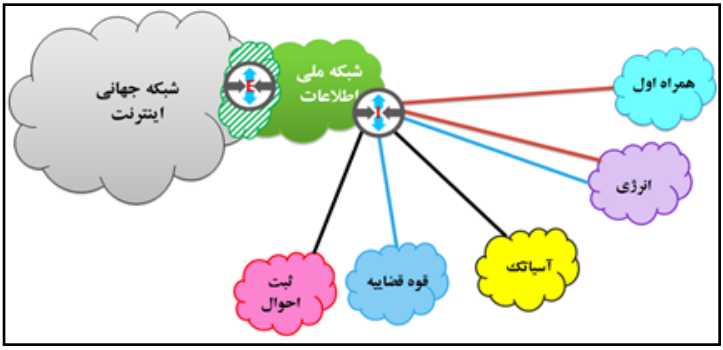
شکل ۶ : مدل مفهومی پروژه سپر طلایی چین

۲-۳- مدل مفهومی شبکه ملی اطلاعات ایران

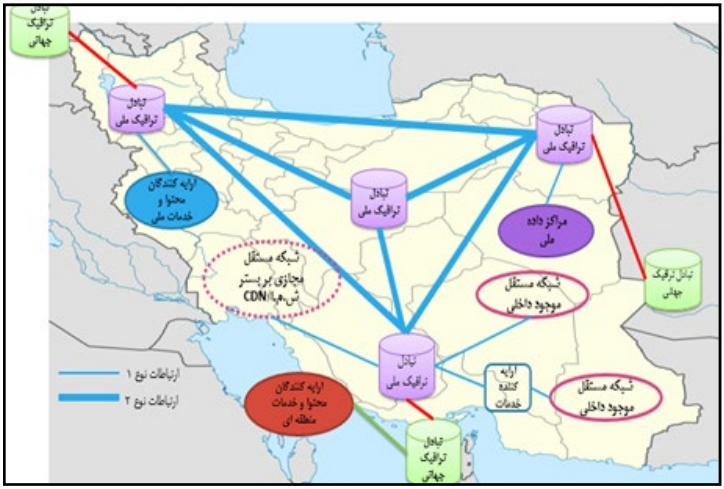
فضای مجازی دارای یک مدل چند لایه‌ای است که بستر آن، زیرساخت ارتباطی است که شبکه ملی اطلاعات نامیده می‌شود. در شکل ۷ مدل مفهومی لایه‌ای فضای مجازی و قلمروی شبکه ملی اطلاعات، در شکل ۸ ، مدل مفهومی و نحوه ارتباط و در شکل ۹ انواع موجودیت‌های متصل شبکه ملی اطلاعات نمایش داده شده است.



شکل ۷ : مدل مفهومی لایه‌ای فضای مجازی و قلمروی شبکه ملی اطلاعات



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



شکل ۹ : انواع موجودیت‌های متصل در شبکه ملی اطلاعات

خدماتی که توسط شبکه ملی اطلاعات می‌بایست به لاهای بالاتر آن (لایه خدمات و محتوا) ارائه شوند، در سند «تبیین الزامات شبکه ملی اطلاعات» تعیین و به تصویب شورای عالی فضای مجازی رسیده است. مهم‌ترین خدمات این شبکه، عبارت‌اند از:

- رمزنگاری
- شناسه و احراز هویت
- امضاء دیجیتال
- نام و نشانه‌گذاری
- میزبانی
- مسیریابی
- خدمات دسترسی
- رصد کمی و کیفی

- اشتراک فضا
- شبکه توزیع محتوا
- جستجوگر
- خدمات ابری
- رایانامه
- خدمات پایه نقشه
- دسترسی به اینترنت
- سالم‌سازی و امنیت
- خدمات NTP(Network Time Protocol)
- پیام‌رسان
- ابزار توسعه وب و app
- ارسال اعلان (push notification)
- آنالیز داده آنلاین
- آنتی‌ویروس
- سیستم‌عامل
- خدمات ترانزیت داخلی/ بین‌الملل و تبادل همتا به همتا (لایه ۲).

۲-۴- 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 شکل ۱۰ مقایسه مدل مفهومی شبکه‌ها نمایش داده شده است.

شکل ۱۰ : مقایسه مدل مفهومی شبکه‌ها

جدول (۱) 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

بخش سوم

مولفه های مطلوبیت

بخش سوم

مؤلفه‌های مطلوبیت

۳-۱- مؤلفه‌های مطلوبیت RUnet

شبکه ملی روسیه، دارای مؤلفه‌های مطلوبیت زیر است:

- تحقق حاکمیت اینترنت[1] در عینِ حفظ سازگاری و همکاری با اینترنت جهانی
- 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 (به دلیل عدم اعتماد به زیرساخت‌های جهانی DNS)
- دسترسی به خدمات و محتوای وب‌سایت‌ها برای کاربران روسی بدون نیاز به مهارت‌های زبان خارجی

1. Internet Sovereignty

- دسترسی کاربران به موتورهای جستجو، خدمات پست الکترونیک، آنتی‌ویروس‌ها، فرهنگ لغت روسی و خدمات آنلاین که دارای یک دفتر در روسیه هستند.
- عدم وابستگی‌های اجتماعی به فناوری‌ها و شبکه‌های اطلاعاتی
- تمرکز بر هوشمندی مقابله با تهدیدات و ایجاد مرکز هماهنگی ملی در مواجهه با حوادث رایانه‌ای
- اتکا به فن‌آوری‌های تولید ملی
- همسوسازی منابع حیاتی اینترنت با مرزهای ملی جهت فراهم‌سازی امکان کارکردن مستقل از اینترنت در شرایط اضطراری یا خاموشی (متوقف شدن سیستم‌ها توسط کشورهای متخاصم)

۳-۲- مؤلفه‌های مطلوبیت چین

شبکه ملی چین، دارای مؤلفه‌های مطلوبیت زیر است:

- محافظ کشور از پروپاگاندای اینترنت جهانی
- 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

۳-۳- مؤلفه‌های مطلوبیت شبکه ملی اطلاعات ایران

نیازمندی‌های شبکه ملی اطلاعات، در سند تبیین الزامات در ابعاد مختلف تدوین شده است که برخی از آن‌ها به شرح زیر است:

- کاهش اتکای زیرساخت فضای مجازی کشور به دیگر شبکه‌ها در تأمین نیازمندی کاربران خود در فضای مجازی
- جذاب سازی و غنی‌سازی 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 نقش‌آفرینان در فضای مجازی
- بهره‌مندی حداکثری کاربران داخلی از مزایای فضای مجازی کشور

۳-۴- مقایسه مؤلفه‌های مطلوبیت در روسیه، چین و ایران

همان‌طور که مطرح گردید، مؤلفه‌های مطلوبیت این شبکه‌ها متفاوت است. در جدول زیر مقایسه مؤلفه‌های مطلوبیت در روسیه، چین و ایران نمایش داده شده است.

جدول (۲) 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)
چین	• 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
ایران	• کاهش اتکای زیر ساخت فضای مجازی کشور به دیگر شبکه‌ها در تأمین نیازمندی کاربران خود در فضای مجازی • جذاب سازی و غنی‌سازی 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 نقش‌آفرینان در فضای مجازی • بهره‌مندی حداکثری کاربران داخلی از مزایای فضای مجازی کشور

بخش چهارم

بخش چهارم

الزام و ملاحظـــات طراحـی

۴-۱- ملاحظات طراحی RUnet

روسـیه بـه توسـعه و تقویـت آنچـه آن را «حاکمیـت اینترنـت» می‌نامـد، پرداختـه و سـرانجام می‌توانـد زیرسـاخت‌های مشـابه را اتخـاذ کنـد و بـا شـبکه‌های سـایر کشـورهای همفکـر ماننـد چیـن ادغـام شـود. درحالی‌کـه توسـعه سـاختارهای حاکـم بـر اینترنـت جهانـی، در انحصـار شـرکت‌هایی چـون ICANN اسـت بـا ایـن وجـود، الزامـات و ملاحظـات طراحـی شـبکه ملـی می‌توانـد باعـث رقابـت بیشـتر دولـت در دنیـای دیجیتـال و مانـع تلاش‌هـای جهانـی بـرای ایجـاد هنجارهـای جهانـی در فضـای مجـازی شـود. روسـیه بـرای ایجـاد زیرسـاخت‌ها و یـک چارچـوب قانونـی بـرای آنچـه آن را «اینترنـت حاکـم» می‌نامـد، تغییـرات اساسـی را ایجـاد می‌کنـد. در حقیقـت، روسـیه امیـدوار اسـت تـا یـک شـبکه داخلـی ایجـاد کـرده کـه بتوانـد بـه طـور مسـتقل از سـایر نقـاط جهـان کار کنـد تـا از این طریـق امـکان محافظـت از ترافیـک آنلایـن را فراهـم کـرده و در صـورت لـزوم اقـدام بـه دفـاع از ترافیـک اینترنـت خارجـی کنـد.

اختلافات روسیه و غرب در سال‌های اخیر در زمینه‌های گوناگونی از جمله حوزه سـایبر مشـهودتر شـده اسـت. دقیقـاً همان‌طور کـه در دنیـای فیزیکی،

مسکو برای مقاومت در برابر تهدیدها و تحریم‌ها اقدام به ایجاد یک بازدارندگی نظامی کرده و استقلال اقتصادی از غرب را دنبال می‌کند، زیرساخت‌های اینترنتی خود را نیز هم‌زمان شکل می‌دهد تا بتواند به طور مؤثرتری با چالش‌های داخلی برای حکومت متمرکز خود و همچنین تهدیدهای خارجی در قالب رقابت بین دولتی مقابله کند.
شبکه ملی روسیه دارای الزام و ملاحظات طراحی زیر است:

امن سازی ملی

- تبدیل موضوع امنیت سایبری به یک موضوع امنیت ملی
- ملی و متمرکز کردن هوشمندی مقابله با تهدیدات
- تلاش برای ملی کردن استانداردهای فنی و تکیه بیشتر بر فناوری‌های تولید شده ملی
- ایجاد قابلیت کلید قطع ارتباط

Kill switches

- انعطاف‌پذیری اینترنت روسیه در برابر آسیب‌پذیری و تهدیدهای خارجی
- نیاز به مقررات دولتی بیشتر برای سازمان‌های کلیدی که مسئول عملیات اینترنت در روسیه هستند
- نیاز به ایجاد سرورهای پشتیبان DNS و آدرس‌های IP

قلمرو سازی جریان اطلاعات

- فیلتر محتوا

• محلی سازی داده‌ها

همسوسازی منابع حیاتی اینترنت

• نقاط تبادل ترافیک، از جمله اپراتورهای مخابراتی و سازمان دهندگان توزیع اطلاعات
• آدرس‌های شبکه و اطلاعات مربوط به افرادی که این آدرس‌های شبکه را در اختیار دارند
• تعداد سیستم‌های خودمختار اینترنت و همچنین اطلاعات مربوط به شخص/ اشخاصی که چنین شناسه‌هایی را در اختیار آن‌ها قرار می‌دهند و تاریخ تهیه آن‌ها
• خط‌مشی‌های مسیریابی برای بسته‌های اینترنتی
• اپراتورهای مخابراتی

روسیه در راستای همسوسازی منابع حیاتی اینترنت خود باید از عملکرد ایمن و پایدار شبکه اینترنتی روسیه توسط اپراتورهای مخابراتی اطمینان حاصل کند. تمامی اپراتورهایی که برای دسترسی به شبکه اطلاعاتی و ارتباطی اینترنت، خدمات ارائه می‌دهند، موظفاند از نصب وسایل فنی جهت مقابله با تهدیدها در شبکه ارتباطی خود اطمینان حاصل کرده و اطلاعاتی را به صورت الکترونیکی به دستگاه اجرایی دولت روسیه ارائه دهند تا مورد کنترل و نظارت قرار گیرند.

برخی دیگر از اقدامات، جهت همسوسازی منابع حیاتی در بخش روسی اینترنت عبارت‌اند از:

• اطمینان از عملکرد بی‌وقفه تأسیسات و امکانات ارتباطی مطابق الزامات تعیین شده توسط بخش اجرایی دولت روسیه؛

• افزایش امنیت اطلاعات، یکپارچگی و ثبات عملکرد شبکه؛
• اختصاص سیستم خودمختار عددی[1]: شناسه منحصر به فرد در اینترنت (تنها مسیر دارای جنبه سیاسی)؛
• ایجاد منطقه دامنه ملی روسیه[2]: مجموعه‌ای از گروه‌های نام دامنه شبکه اینترنت که لیست آن‌ها توسط دستگاه اجرایی دولت روسیه تشکیل شده و وظایف نظارت و کنترل در زمینه رسانه جمعی، ارتباطات و فناوری اطلاعاتی و ارتباطی دارند؛
• فراهم کردن وضوح نام دامنه[3]: شناسایی یک آدرس شبکه متناسب با نام دامنه در اینترنت؛
• ایجاد یک سیستم ملی برای به دست آوردن اطلاعات در مورد نام دامنه و (یا آدرس شبکه) به عنوان مجموعه‌ای از نرم‌افزار و سخت‌افزار به‌هم‌پیوسته، به منظور اطمینان از عملکرد پایدار شبکه اینترنت. ابزاری که برای ذخیره و دریافت اطلاعات در مورد آدرس‌های شبکه در رابطه با نام دامنه، از جمله موارد موجود در منطقه دامنه ملی روسیه و همچنین مجوز هنگام حل‌وفصل نام دامنه طراحی شده است.
• ایجاد سیستم نام دامنه ملی و همچنین قوانین استفاده از آن توسط دستگاه اجرایی فدرال که وظایف کنترل و نظارت را در زمینه رسانه‌های جمعی، ارتباطات جمعی، فناوری‌های اطلاعاتی و ارتباطات انجام می‌دهد.
• سازمان‌دهی انتشار اطلاعات در اینترنت، با داشتن شماره سیستم خودمختار[4]، مطابق با الزامات تعیین شده توسط مرجع اجرایی فدرال در زمینه ارتباطات و همچنین نام دامنه سیستم ملی، از نرم‌افزار و سخت‌افزار لازم.

1. Numerical autonomous system
2. Russian national domain zone
3. Domain name resolution
4. AS number

• انتقال اطلاعات مربوط به بانک سیستم‌های اطلاعاتی که توسط افراد مجاز در منطقه ملی روسیه تشکیل می‌شوند با شیوه و مدت‌زمان تعیین شده، به کمک قوانین استفاده از سیستم نام دامنه ملی به این سیستم.

۴-۲- الزامات شبکه روسیه

۱) اهم الزامات در ارائه خدمات ارتباطی در شبکه روسیه به شرح ذیل است:

۲) اپراتورهای مخابراتی موظفاند در صورت تهدید، امکان مدیریت متمرکز ترافیک را فراهم کنند.

۳) نصب ابزارهای فنی در شبکه‌های ارتباطی که منبع ترافیک انتقال‌یافته را تعیین می‌کنند، امکان‌پذیر باشد.

۴) وسایل فنی باید بتوانند دسترسی به منابع دارای اطلاعات ممنوعه به آدرس‌های شبکه را محدود کنند.

۵) در صورت عدم امکان اتصال اپراتورهای مخابراتی روسی به سرورهای root اینترنتی خارجی، امکان ایجاد زیرساخت برای اطمینان از عملکرد منابع اینترنتی روسیه فراهم شده است.

۶) مالکان و صاحبان خطوط یا منابع ارتباطی که از مرزهای روسیه عبور می‌کنند، موظفاند در زمان، نحوه، ترکیب و فرمت تعیین شده مطابق وظایف تعیین شده کنترل و نظارت توسط دستگاه اجرایی دولت روسیه، عمل کنند. آن‌ها موظفاند:

۱) قواعد مربوط به مسیریابی ارتباطات مصوبه دولت را اجرا کنند.

۲) مسیریابی پیام‌های ارتباطی از راه دور باید به درخواست دولت روسیه صورت گیرد و در صورت تشخیص نقض قوانین

مسیریابی با آن‌ها برخورد می‌شود.

۷) در صورت استفاده از نقاط تبادل ترافیک برای تعامل با سایر اپراتورهای مخابراتی، اطلاعات آن‌ها در رجیستری ترافیک نقاط مبادله باید وجود داشته باشد. این اطلاعات شامل تعداد سیستم‌های خودمختارِ در اختیار، آدرس‌های شبکه متعلق به سیستمِ خودمختار، تعاملات با سایر افرادی که سیستم خودمختار را در اختیار دارند، مکان‌های اتصال امکانات ارتباطی در حال عبور از مرز، مکان‌های نصب تجهیزات ارتباطی متصل به خطوط ارتباطی در کشورهای خارجی است.

۴-۳- الزام و ملاحظات طراحی پروژه سپر طلایی چین

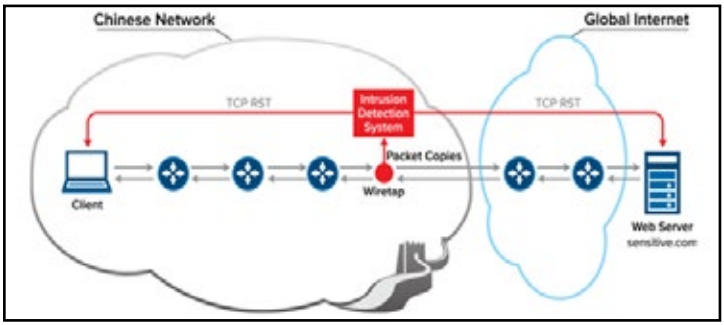
پروژه سپر طلایی چین از ۳ روش برای حفاظت از شبکه چین استفاده می‌کند که در ادامه شرح داده شده است:

۱. روش اول : (TCP Reset)

در این روش، ابتدا سرویس‌گیرنده، درخواستی را به سرویس‌دهنده وب ارسال می‌کند. دستگاه‌های مبتنی بر سیستم‌های تشخیص نفوذ (IDS [1])، محتوای بسته و URL درخواستی از سوی سرویس‌گیرنده را بررسی می‌کند و کلمات کلیدی مشکوک در آن‌ها را در لیست سیاه قرار می‌دهد. سپس روتر GFW ، بسته‌های جعلی TCP RST را به هر دو نقطه انتهایی سرویس‌دهنده و سرویس‌گیرنده تزریق می‌کند و این اتصال قطع می‌شود. فایروال عظیم چین، وضعیت جریان ارتباطی شامل آدرس‌های IP مبدأ و مقصد، شماره پورت و پروتکل

1. Intrusion Detection Systems

درخواست شده را برای جلوگیری از مسدود شدن سایر ارتباطات تا ساعت‌ها حفظ می‌کند. این روند همچنان ادامه خواهد داشت. شکل ۱۱، روش اول عملکرد فایروال عظیم چین (TCP Reset) را نشان می‌دهد.



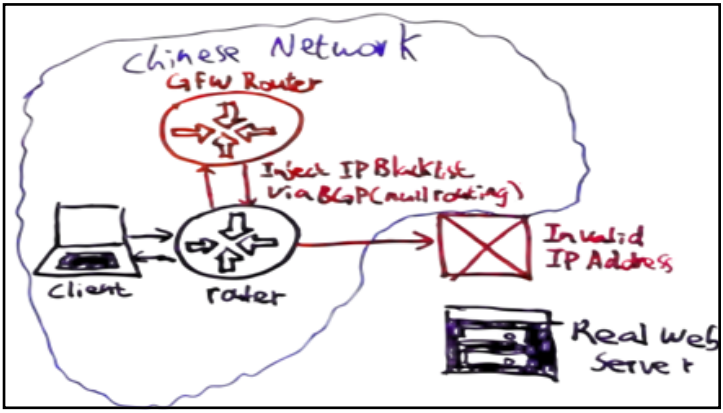
شکل ۱۱ : روش اول عملکرد فایروال عظیم چین (TCP Reset)

۲. روش دوم : Ip address blocking

در این روش، مسدود کردن آدرس‌های IP، به عنوان ابزاری مؤثر برای فیلتر محتوای شبکه در نظر گرفته شده است. پروتکل[1] BGP، برای تبادل اطلاعات مسیریابی در اینترنت و بین ارائه‌دهندگان سرویس اینترنت (ISPها) مورد استفاده قرار می‌گیرد. شبکه‌های مصرف‌کننده، مانند دانشگاه‌ها و شرکت‌های بزرگ و سازمان‌ها، برای تبادل اطلاعات مسیریابی در شبکه‌های داخلی، معمولاً از یک پروتکل مسیریابی داخلی[2] IGP استفاده می‌کنند. سرویس‌گیرندگان به ISP ها متصل می‌شوند و ISPها برای تبادل مسیر سرویس‌گیرندگان، از BGP استفاده می‌کنند. فایروال عظیم چین، به کمک روتر ISP ها، لیستی از آدرس‌های مقصد را از طریق پروتکل BGP به لیست سیاه اضافه می‌کند. وقتی‌که برای اولین بار اتصال TCP در شبکه برقرار

1. Borderway Gateway protocol
2. Interior Gateway Protocol

می‌شود، همسایه‌های BGP اطلاعات کامل مسیریابی را با هم تبادل می‌نمایند. زمانی که تغییرات در جدول مسیریابی شناسایی شوند، روترهای BGP تنها مسیرهایی را به همسایه‌هایشان می‌فرستند که تغییر کرده‌اند. روترهای BGP به‌روزرسانی‌های مسیریابی دوره‌ای را ارسال نمی‌کنند و BGP تنها مسیر بهینه به یک شبکه مقصد را مسیریابی می‌کند. این روش تنها می‌تواند ترافیک برون‌مرزی از چین را مسدود و ترافیک ورودی را مجاز نماید. شکل ۱۲، روش دوم عملکرد فایروال عظیم چین (Ip address blocking) را نشان می‌دهد.

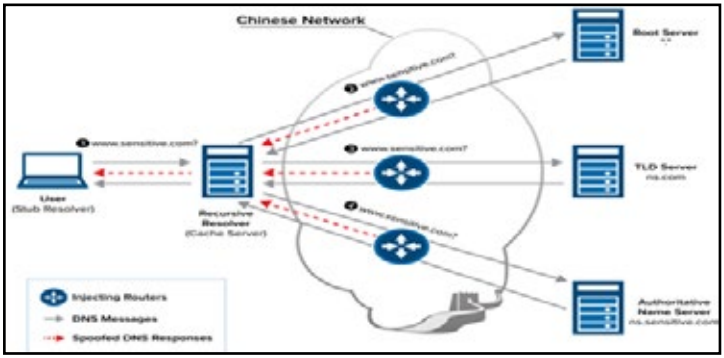


شکل ۱۲ : روش دوم عملکرد فایروال عظیم چین (Ip address blocking)

۳. روش سوم: DNS spoof

دستکاری DNS برای مسدود کردن آدرسIP به هدف تغییر نام دامنه بسیار سخت‌تر از تغییر آدرس‌های IP است. اولین قدم در مورد دستکاری DNS تزریق DNS است. هنگامی‌که کاربر تلاش می‌کند به یک نام دامنه متصل شود، از سرورهای DNS آدرس IP مرتبط

با نام دامنه را درخواست داده می‌شود. فایروال عظیم چین، هر درخواست DNS راکِ از مشتری‌های داخل چین در مرز اینترنت چین سرچشمه می‌گیرد، نظارت می‌کند. اگر درخواستی مرتبط با نام دامنه مسدود شده باشد، DNS پاسخ جعلی با یک IP نامعتبر به وب سایت دیگری تزریق می‌کند. این پاسخ جعلی به سرورهای بازگشتی داخلی DNS در چین می‌رود. بنابراین دست‌کاری DNS و مسدود کردن آدرس IP مورد استفاده در کنار هم می‌توانند سایت‌های سانسور شده در همه سطوح را به‌طور مؤثری متوقف کنند. شکل ۱۳، روش سوم عملکرد فایروال عظیم چین (DNS spoof) را نشان می‌دهد.



شکل ۱۳ : روش سوم عملکرد فایروال عظیم چین (Dns spoof)

۴-۴- الزام و ملاحظات طراحی شبکه ملی اطلاعات ایران

ملاحظات شبکه ملی اطلاعات در دو دسته کارکردی و غیرکارکردی تقسیم‌بندی می‌شوند. الزامات کارکردی، تعیین‌کننده توانمندی‌های

اصلی در شبکه ملی اطلاعات و الزامات غیرکارکردی، به نوعی ناظر بر کیفیت تحقق این توانمندی‌ها هستند. تفکیک الزامات با این دیدگاه در شکل ۱۴ نشان داده شده است:

شکل ۱۴ : الزامات طراحی شبکه ملی اطلاعات

الزامات شش‌گانه شبکه ملی اطلاعات، مصوب شورای عالی فضای مجازی عبارت‌اند از:

۱) متشکل از زیرساخت‌های ارتباطی با مدیریت مستقلِ کاملاً داخلی
۲) کاملاً مستقل و حفاظت شده نسبت به دیگر شبکه‌ها (از جمله اینترنت) با امکان تعامل مدیریت شده با آن‌ها
۳) با امکان عرضه انواع محتوا و خدمات ارتباطی سراسری برای آحاد مردم با تضمین کیفیت از جمله قابلیت تحرک
۴) با قابلیت عرضه انواع خدمات امن اعم از رمزنگاری و امضای دیجیتالی به کلیه کاربران
۵) با قابلیت برقراری ارتباطات امن و پایدار میان دستگاه‌ها و

مراکز حیاتی کشور

۶) پرظرفیت، پهن باند و با تعرفه رقابتی شامل مراکز داده و میزبانی داخلی

این الزامات در سند «تبیین الزامات شبکه ملی اطلاعات» مصوب شورای عالی فضای مجازی تصویب شده است.

منابع

[1] https://perspectives.mvdirona.com/2008/04/golden-shield-project

[2] http://www.wired.com/politics/security/magazine/15-11/ff_chinafirewall

[3] http://www.theatlantic.com/doc/200803/chinese-firewall?reddit

[4] https://afric.online/18106-internet-shutdown-rights-vs-consequences/

[5] http://www.cs.tufts.edu/comp/116/archive/fall2016/ctang-supporting.pdf

[6] http://council.gov.ru/activity/documents/

[7] https://irandoc.ac.ir/sites/fa/files/attach/article/model-strengthening-economic-effects-national-information-network.pdf

[8] http://www.irb-cisr.gc.ca/Eng/ResRec/RirRdi/Pages/index.aspx?doc=455174&pls=1

[9] http://www.cs.tufts.edu/comp/116/archive/fall2016/ctang-supporting.pdf

csri.majazi.ir