La urdimbre de RuNet

Soberanía y multipolaridad como principios rectores en el intento por articular un ciberespacio autónomo en Rusia

XVI Congreso Español de Ciencia Política y de la Administración

---

Daniel Pérez Fernández (Universidad Autónoma de Madrid)


EL ESPAÑOL

omicrono

TECNOLOGÍA

Así es RuNet, el internet de Putin que permite a Rusia estar conectada aunque todo el mundo le bloquee

Putin no sólo ha preparado sus tropas, también sus telecomunicaciones: su búnker digital le permite minimizar los bloqueos de servicios online.

8 marzo, 2022 - 03:53


EL PAÍS

Tecnología

TU TECNOLOGÍA · CIBERSEGURIDAD · PRIVACIDAD · INTELIGENCIA ARTIFICIAL · INTERNET · GRANDES TECNOLÓGICAS · ÚLTIMAS NOTICIAS

OFENSIVA DE RUSIA EN UCRANIA >

El Kremlin da el primer paso para aislar el internet ruso del resto del mundo

Moscú está preparado para desconectar el país del ciberespacio global. Aunque oficialmente descarta aplicarlo de forma generalizada, el proyecto opera desde el viernes en las webs del Gobierno


LA VANGUARDIA

TEKNEO

AISLAMIENTO DIGITAL

¿Podría Rusia desconectarse del internet global y tener una red propia? Ya tiene un plan en marcha

• El Kremlin tiene preparada una especie de intranet rusa, conocida como RuNet, para desconectar el país del ciberespacio global y controlar así todo el tráfico de datos


ABC Economía

→ ABC → Economía

Runet, el arma secreta de Putin para mantener un control total de internet

Rusia trabaja desde 2014 en una red propia que puede ser tanto un elemento defensivo frente a sabotajes como un potente instrumento de censura

Sigue en directo la última hora de la guerra en Ucrania

En los últimos meses, la prensa española ha comenzado a prestar atención al proyecto de RuNet (no sin hipérboles, y con artículos plagados de imprecisiones y de errores de bulto) → En este contexto, se echa en falta la aparición de análisis académicos detallados en lengua castellana que traten el fenómeno con más sobriedad ⟹ **Laguna en la literatura**

1) Emergencia del pulso por controlar RuNet

- Las primeras medidas implementadas con el objeto de "blindar" el ciberespacio de la Federación Rusa –frente a un combinado de amenazas internas y externas– se remontan a **2012** → Puesta en marcha de la famosa "lista negra" de sitios y recursos web del ***Roskomnadzor***

- En la mayoría de la literatura especializada (vid. Nocetti, 2015; Gaufman, 2021; Litvinenko, 2021; Stadnik, 2021) se señala que este *primer envite regulatorio* se produce como respuesta a la **oleada de protestas** que sacudió Rusia entre 2011 y 2013

  ↳ Importancia de RRSS, servicios de mensajería instantánea, foros y blogs en la organización de las protestas

- Lógica de la "fortaleza asediada" (Kari, 2019) → La oficialidad rusa señala que las protestas han sido organizadas gracias al **apoyo de "agentes occidentales"** por medios digitales

  ↳ Motivo para comenzar con el "blindaje" del ciberespacio ruso alimentado, después, por fenómenos tales como: (1) Las revelaciones de Edward Snowden de 2013 → Programa PRISM de la NSA | (2) Las severas sanciones impuestas a la Federación Rusa tras la anexión de Crimea en 2014 | (3) La inclusión por parte de la OTAN del ciberespacio como dominio militar en 2016 | (4) El señalamiento explícito de Rusia como amenaza para la seguridad de EEUU y sus aliados en su estrategia de ciberseguridad de 2018

2) Las "cuatro patas" del proyecto de RuNet

- Garantizar el dominio del espacio informacional ruso por parte de agentes domésticos → Uso singular del concepto de "espacio informativo" (*informatsionnaia sfera*) en la Federación Rusa (Ristolainen, 2017) → Entorno complejo, de corte *total*, compuesto por tres expresiones informativas diferenciadas: (1) las comunicaciones que se originan dentro de la Federación, (2) las comunicaciones que se dirigen a agentes situados dentro de sus límites territoriales y (3) las comunicaciones que transitan, o que simplemente recalan en algún punto geográfico o sistema dependiendo de la FR, siguiendo luego su camino hacia otras latitudes.

- Reducir los márgenes de dependencia exterior de la Federación Rusa en materia de software, hardware e infraestructura técnica → La FR importa el grueso de las soluciones tecnológicas que se emplean en su territorio → Esto genera vulnerabilidades de índole cibersecuritaria, y coloca además al país en una posición económicamente subordinada respecto de aquellos países que producen y distribuyen internacionalmente sus propias soluciones tecnológicas.

- Controlar los flujos de datos que atraviesan el territorio de la Federación → Las revelaciones de Snowden de 2013 pusieron de manifiesto que empresas como Microsoft, Google, Facebook o Apple habían servido como fautores de la NSA a través del programa PRISM → A partir de ahí, la FR encuentra un pretexto sólido para ejercitar una regulación draconiana en materia de "localización de datos", por la que se fuerza a toda empresa que opere en su territorio a almacenar los datos de los usuarios dentro de las fronteras de la FR

- Promover la "rusificación" del espacio digital ruso y de su esfera de influencia inmediata → La dimensión frecuentemente más desatendida del proyecto de RuNet la integra el intento por motivar el uso de aplicaciones, recursos web y soluciones tecnológicas producidas en Rusia en los países que componen su "esfera de influencia" inmediata (concepto clave: *Ruskii Mir*) → Tentativa dirigida a, especialmente, los países que componen –o que han formado parte de– la Comunidad de Estados Independientes (CEI)

3) El concepto de "soberanía digital" en la Federación Rusa

- El concepto de "soberanía digital" hace acto de presencia discusión pública rusa a partir de 2012 → El primer agente en ofrecer una definición más o menos depurada del concepto es **Igor Ashmanov**, dueño de la firma de tecnoinversores *Ashmanov & Partners* y creador en 2013 de la desafortunadamente famosa *Agencia de Investigación de Internet*, también conocida como Glavset

  ↳ Soberanía digital → "El **derecho** y la **capacidad** de un gobierno para determinar autónomamente su política nacional y también sus intereses y cursos de actuación geopolíticos en el entorno digital" (Ashmanov, 2013)

- Desde que comenzara a emplearse el concepto, una amplia cohorte de académicos y de miembros del estamento militar se han afanado por operacionalizarlo (Streltsov, 2014; Zinovieva, 2014; Kucheryavyi, 2015; Bukharin, 2016…)

  ↳ Resultado → Señalamiento de las "cuatro patas" del proyecto de RuNet a las que se ha hecho alusión en la anterior diapositiva

- El análisis de estos textos deja entrever, además, que desde la oficialidad rusa se trabaja con una lectura del concepto de soberanía ciertamente simplista, de tintes absolutos → No se observan lecturas **relativas, condicionales o limitadas** del concepto

- Resumen → El Estado es "soberano" solo si dispone de **supremacía** en el ámbito doméstico y de plena **autonomía** en el ámbito internacional

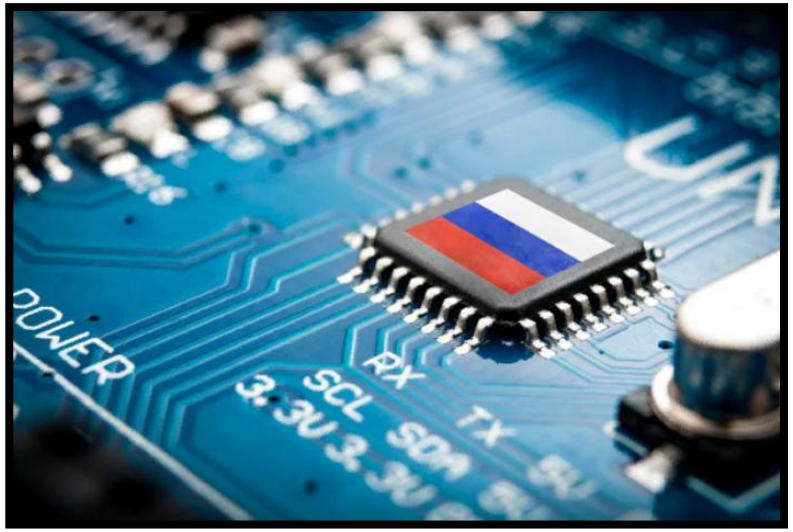
  ↳ Guía para el proyecto de regulación de RuNet

4) La apuesta por un mundo "digitalmente multipolar"

- El concepto de "multipolaridad" no ha recibido tanta atención en la literatura sobre RuNet → Al margen de las aproximaciones de Stanislav Budnitsky (2020) y Dmitri Trenin (2022), no se observa un análisis sistemático del encaje de este concepto en el proyecto general de desacoplamiento del ciberespacio ruso del ciberespacio "global"

- Concepto fuertemente arraigado en la política exterior rusa desde finales de la década de los '90 → La literatura suele coincidir en atribuir al Ex-Ministro de Asuntos Exteriores de Rusia **Yevgeny Primakov** el rol de figura clave en la emergencia y uso de este concepto (e.g. Makarychev & Morozov, 2011) → Sin embargo, autores como Stanislav Budnitsky (2020) postulan que el concepto ya gozaba de uso corriente durante la primera mitad de los '90.

  ↳ Multipolaridad → Rechazo a la hegemonía y estructura-mundo "unipolar" encabezada por los Estados Unidos, y rechazo paralelo a arreglos de tipo "bipolar" como los que caracterizaron a etapas como la Guerra Fría



- En fases recientes, el concepto de "multipolaridad" no ha gozado de una presencia tan destacada en documentos programáticos de la FR como en el pasado → Ahora, el legislador ruso prefiere hablar de "policentrismo" → Dos conceptos que, según **Andrey Kortunov**, director del RIAC, "resultan prácticamente intercambiables en el discurso oficial ruso" (Kortunov, 2019)

- Rusia apuesta por la multipolaridad digital → Huida de los espacios dominados por **EEUU** y **China**, tanto en términos de servicios web como de equipamiento y/o infraestructura → Pretensión paralela de convertir a Rusia en un **proveedor regional** de equipo y servicios.

5.1) Medidas implementadas

2012

- Creación de "lista negra" de sitios y recursos web → Ley Federal 139-FZ → Mantenimiento y actualización del listado a cargo del *Servicio Federal de Supervisión de las Telecomunicaciones, Tecnologías de la Información y Medios de Comunicación* (**Roskomnadzor**)

  ↳ Cuatro motivos para la inclusión de un sitio/recurso web en el listado: (1) Difusión de contenido "extremista" | (2) Difusión de pornografía infantil, de contenido sobre drogas o que "anime" al suicidio (sic.) | (3) Infracción de leyes de copyright | (4) Movilización de la población con vistas a la realización de manifestaciones o de reuniones no autorizadas

2013

- Puesta en marcha del GosSOPKA → *Sistema Estatal para la Detección, Prevención y Eliminación de las Consecuencias de Ataques Informáticos en Recursos Informativos* → Centralización de los mecanismos de coordinación entre proveedores de servicios de ciberseguridad en la Federación Rusa

  ↳ Desde su creación en 2013, el Servicio Federal de Seguridad (FSB) se encarga de operar el GosSOPKA → El sistema elimina la posibilidad de comunicación autónoma entre proveedores de servicios de ciberseguridad (i.e. todo pasa por las manos del FSB)

2014

- Implementación del SORM-3 → Actualización del *Sistema de Actividades Operativas de Investigación*, operado por el FSB y orientado al monitoreo activo de las redes de telecomunicación rusas → Incorporación de tecnologías de "Inspección Profunda de Paquetes" (DPI)

5.2) Medidas implementadas

2014

- Redacción de la Ley de "Localización de Datos" de la Federación Rusa ⟹ Ley Federal 242-FZ → Requisitos: (1) Obligación de almacenar datos de todos los usuarios del servicio que vivan en la Federación Rusa o que usen dicho servicio desde cualquier punto geográfico situado dentro de los límites territoriales de la Federación | (2) Obligación de almacenar dichos datos en instalaciones situadas dentro de la Federación Rusa | (3) Obligación de transferir o copiar las bases de datos de una entidad a una instalación situada en la Federación Rusa si se opera con datos vinculados a cualquier ciudadano, sistema o entidad rusa

2015

- Implementación del sistema "Revizor" ⟹ Automatización y mejora del sistema de bloqueo de páginas y recursos web → Conexión permanente de los *Proveedores de Servicios de Internet* (ISPs) de la Federación Rusa a la "lista negra" operada por el Roskomnadzor

- Puesta en marcha del "Programa de Sustitución de Importaciones" en materia de TICs ⟹ Medidas: (1) Creación de un registro de "soluciones de software creadas en Rusia" (desde 2015) | (2) Obligatoriedad en el uso de "software ruso" para agencias estatales y compañías participadas por el Estado (desde 2016) | (3) Inversión masiva en el desarrollo de soluciones de 5G y gran desembolso para sustituir el "backbone" (troncal de red) de la Federación, poniéndolo en manos de empresas rusas (desde 2020) | (4) Pre-instalación forzosa de una batería de aplicaciones rusas en ordenadores personales, smartphones y Smart TVs (desde 2022)

  ↳ Información detallada sobre el programa en: Semenov y Baranova, 2018; Lowry, 2021; Pérez Fernández, 2021

5.3) Medidas implementadas

2016

- Redacción de las "Leyes Yarovaya" → Leyes Federales 374-FZ y 375-FZ → Medidas: (1) Los proveedores de servicios de mensajería instánea y de correo electrónico, y los propietarios de redes sociales y de motores de búsqueda, deben almacenar los metadatos de las operaciones realizadas en sus respectivas plataformas durante un año (extendido a tres años tras las modificaciones a la ley introducidas en 2018) | (2) Los proveedores de estos servicios deberán almacenar el contenido de dichas operaciones –texto, imagen, sonido, etc.– durante treinta días (aumentando el periodo de almacenamiento en un 15% cada año desde 2018) | (3) Los proveedores de estos servicios que usen algún sistema de encriptación deben proporcionar al FSB las claves de desencriptado si así se les solicita

2018

- Creación del NCCCI → *Centro Nacional de Coordinación de Incidentes Informáticos*, dependiente del FSB → (1) El NCCCI pasa a controlar el funcionamiento del GosSOPKA | (2) El NCCCI puede vetar la transferencia de información sobre ciberataques sucedidos dentro del territorio de la Federación, e identificados por firmas localizadas en su territorio, a firmas o servicios de ciberseguridad que operen desde cualquier otro país

2019

- Redacción de la "Ley de Internet Soberano" → Ley Federal 90-FZ → Medidas: (1) Preparación de un "sistema de apagado de emergencia" (*Kill Switch*) con el que desconectar RuNet del Internet "global" en "casos de extrema necesidad" | (2) Obligación de instalación de tecnologías de "inspección profunda de paquetes" (DPI) por parte de los *Proveedores de Servicios Internet* (ISPs) que operen en la Federación Rusa | (3) Propuesta de creación de un "Sistema de Nombres de Dominio" (DNS) estrictamente nacional

6) Algunos éxitos del proyecto

- Bloqueo de las operaciones de LinkedIn en el territorio de la Federación Rusa desde 2016 → Motivo: Incumplimiento de la legislación en materia de "localización de datos"

- Imposición de varias multas a Google → Motivo: Negarse a filtrar los resultados de las búsquedas realizadas en su plataforma en atención a la "lista negra" operada e impuesta por el Roskomnadzor

- Replicación satisfactoria de los registros de DNS del operador RIPE NCC → En caso necesario, la Federación Rusa ya cuenta con una "copia de seguridad" con la que garantizar el acceso a recursos web localizados dentro de su territorio…

  Nota: el DNS funciona como una suerte de "listín telefónico" → El sistema garantiza que cuando, por ejemplo, escribimos en nuestro navegador una URL como www.aecpa.es, nuestro navegador sebe lanzar la solicitud de entrada al servidor con IP 185.50.196.212, que es donde se aloja la página

- El Roskomnadzor ha conseguido introducir en su "lista negra" una cantidad admirable de recursos y páginas web y, además, ha logrado bloquear el uso de un buen número de servicios de VPN

- El sistema SORM-3 goza de una altísima pervasividad → La incorporación de tecnologías de "inspección profunda de paquetes" ha dotado a los programas del FSB de una capacidad de monitoreo digital (activo) sin precedentes

7) Y muchos más fracasos…

- Aunque se han impuesto varias multas a Google por no acatar las directrices marcadas por el Roskomnadzor… ¡Los dueños del motor de búsqueda se las han ingeniado para no pagar varias de ellas! → vid. Ermoshina et al. (2021)
- Algunos ISPs han encontrado vías efectivas para sortear la "lista negra" del Roskomnadzor →
- El intento de bloquear los servicios de la aplicación Telegram en Rusia ha sido un sonoro *fiasco* → En marzo de 2018 la *Corte del Distrito de Tagansky* de Moscú mandó bloquear la famosa aplicación de mensajería instantánea en todo el territorio de la Federación → Motivo: Telegram se negó a proporcionar al FSB las claves de desencriptado de su aplicación → Después de varios intentos infructuosos por bloquear los servicios de Telegram –y de ver, en paralelo, cómo crecía su base de usuarios en la Federación–, las autoridades rusas finalmente claudicaron y pasaron a considerar *legal* el uso de la aplicación empezando en junio de 2020
- Evidencia extremadamente escasa sobre la implementación efectiva de un *kill switch* en la FR → Aunque las autoridades rusas han declarado que disponen de las capacidades técnicas necesarias para implementar un "sistema de apagado de emergencia", no hay evidencia de que dicho sistema se encuentre operativo
- Buena parte de los proveedores de servicios no son capaces de lidiar con los costes crecientes vinculados al almacenamiento de metadatos y contenido → Imposibilidad para cumplir con las exigencias impuestas por las "Leyes Yarovaya"
- El programa de "sustitución de importaciones" no ha cosechado prácticamente ningún éxito → Datos: (1) En 2019, el uso de soluciones de software "nacional" por parte de empresas rusas con participación del Estado solo llegaba al 10% | (2) Para los dos últimos ciclos, los datos indican que, en lugar de bajar, la importación de hardware por parte de la FR ha aumentado | (3) El Kremlin no ha conseguido, ni de lejos, poner en manos de empresas rusas el *backbone* (troncal de red) de la Federación….

Conclusiones

Referencias

- Ashmanov, I. (2013). “Information Sovereignty – A new reality” [Информационный суверенитет – новая реальность]. Disponible en: http://eurasian-defence.ru/sites/default/files/doc/ashmanov.pdf
- Budnitsky, S. (2020). “Russia’s great power imaginary and pursuit of digital multipolarity”. *Internet Policy Review*, 9(3)
- Bukharin, V. (2016). “Components of digital sovereignty of the Russian Federation as the technical basis of information security” [Компоненты цифрового суверенитета российской федерации как техническая основа информационной безопасности]. *Vestnik*, 6(51).
- Ermoshina, K.; Loveluck, B. & Musiani, F. (2022). “A market of black boxes: The political economy of Internet surveillance and censorship in Russia”. Journal of Informa-tion Technology and Politics, 19(1), pp. 18-33.
- Gaufman, A. (2021). “Personal Data Protection in Russia”, en V. Gritsenko; M. Wijermars & M. Kopotev (eds.): *The Palgrave Handbook of Digital Russia Studies*. Cham: Palgrave Macmillan
- Kortunov, A. (2019). “Between Polycentrism and Bipolarity. On Russia’s World Order Evolution Narratives”. *Russia in Global Affairs*, 1, pp. 10-51
- Kucheryavyi, M. (2015). “Realizing Information Sovereignty in the trends of the global information space” [К осознанию информационного суверенитета в тенденциях
- глобального информационного пространства]. *Science, New Technologies and Innovations in Kyrgyzstan*, 12
- Litvinenko, A. (2021). “Re-defining Borders Online: Russia’s Strategic Narrative on Internet Sovereignty”. *Media and Communication*, 9(4), pp. 5-15
- Lowry, A. (2021). “Russia’s Digital Economy Program: An Effective Strategy for Digital Transformation?”, en V. Gritsenko; M. Wijermars & M. Kopotev (eds.): The Palgrave Handbook of Digital Russia Studies. Cham: Palgrave Macmillan.
- Makarychev, A. & Morozov, V. (2011). “Multilateralism, Multipolarity and Beyond: A Menu of Russia’s Policy Strategies”. *Global Governance*, 17, pp. 353-373
- Nocetti, J. (2015). “Contest and conquest: Russia and global internet governance”. *International Affairs*, 91(1), pp. 111-130
- Pérez Fernández, D. (2021). “Made in Russia: Making sense of the Kremlin’s ICT import substitution program”. Internet Governance Project [Online]. Disponible en: https://www.internetgovernance.org/2021/10/19/made-in-russia-making-sense-of-the-kremlins-ict-import-substitution-program/
- Ristolainen, M. (2017). “Should ‘RuNet 2020’ be taken seriously? Contradictory views about cyber security between Russia and the West”. *Journal of Information Warfare*, 16(4), pp. 113-131
- Semenov, V. & Baranova, L. (2018). “About Import Substitution in the Field of Information Technologies”. *Proceedings of the 2018 IEEE International Conference “Quality Management, Transport and Information Security”*. Institute for Electrical and Electronics Engineering.
- Stadnik, I. (2021). “Russia. An independent and sovereign internet?”, en B. Haggart, N. Tusikov & J.A. Scholte (eds.): *Power and Authority in Internet Governance. Return of the State?*. London: Routledge.
- Streltsov, A. (2014). “The main development directions of armed conflicts’ international law as applied to cyberspace” [Основные направления развития международного права вооруженных конфлик]. *VIII International Forum on International Information Security*.
- Trenin, D. (2022). “Russia: Looking for Prominence in the Global System”, en S. Ülgen (ed.): *Rewiring Globalization*. Washington D.C.: Carnegie Endowment for International Peace
- Zinovieva, E. (2014). “Analysis of Russia’s Foreign Policy Initiatives in the Field of International Information Security” [Анализ внешнеполитических инициатив РФ в области международной информационной безопасности]. *Bulletin of the MGIMO University*, pp. 47-52