Internet y sus enemigos

Félix Arteaga | Investigador principal de Seguridad y Defensa, Real Instituto Elcano.

Tema[1]

La mayoría de los análisis de riesgos en el ciberespacio se centran en los objetivos de los ciberataques, mientras que pocos se centran en la infraestructura de Internet y en la información y datos que circulan por ella.

Resumen

Internet, una innovación tecnológica inicialmente ideada para la conexión de redes de comunicaciones de defensa y posteriormente ofrecida al bien público mundial, y la información (datos) que circula sobre ella se ven amenazadas por múltiples actores y prácticas que tratan de limitar el acceso o la inclusividad del bien público que es Internet y alterar o manipular el contenido de sus flujos. En este ARI se describen, por un lado, los riesgos tecnológicos, comerciales y políticos que afectan a la gobernanza de Internet y, por otro, los que amenazan a la sociedad de la información que se nutre de las ideas, noticias y datos que circulan por Internet.

Análisis

La infraestructura de Internet conecta a los usuarios a la Red mediante proveedores de servicios de acceso privados (ISP), que se conectan a su vez a la Red a través de operadores globales (*carriers*) o plataformas privadas especializadas en la entrega de contenidos (*content delivery networks*, CDN). En la gobernanza de la infraestructura, sus redes, conexiones, estándares y protocolos participan los expertos técnicos, los operadores y proveedores de servicios y los reguladores gubernamentales dentro de un modelo de gestión público-privado[2].

La gobernanza ha pasado de un enfoque estrecho, centrado en la asignación y gestión de direcciones IP públicas y nombres de los dominios de Internet, a otra más amplia que incluye el impacto de las nuevas tecnologías y la resolución de los problemas asociados a la infraestructura física y lógica de Internet. La gobernanza técnica de Internet se sostiene por la dedicación de un conjunto heterogéneo de instituciones que velan por la interconexión de distintos tipos de redes creando estándares y protocolos como el

[1] Este ARI desarrolla las ideas apuntadas por el autor durante el Foro de Gobernanza de Internet celebrado en Madrid el 7/XI/2019.

[2] Para un estado actualizado de la gobernanza, ver a Daniel Voelsen, "Cracks in the Internet's Foundation", SWP Research Paper 14, noviembre de 2019, https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2019RP14_job_Web.pdf; y a Emily Taylor y Stacie Hoffmann, "EU-US Relations on Internet Governance", Chatham House, noviembre de 2019, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-14-EU-US-Relations-Internet-Governance2.pdf.

Consorcio World Wide Web (W3C) o el Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers, IEEE).
Los dominios y las direcciones IP públicas asignados a dispositivos y redes conectados a Internet están controlados por una asociación privada (Internet Corporation for Assigned Names and Numbers, ICANN) organizada en torno a varios agentes (*multistakeholders*) académicos, privados o institucionales –gubernamentales o no– que adoptan acuerdos en pie de igualdad. No obstante, sus recomendaciones no tienen fuerza vinculante y las resoluciones gubernamentales que podrían tener esa fuerza en el marco de la Unión Internacional de Telecomunicaciones (UIT) no van más allá de la limitada voluntad de cooperar en la gobernanza de Internet, capitalizada por las grandes potencias (las resoluciones de la UIT se circunscriben a aspectos institucionales, técnicos –tipo ICANN– o relativos a las tasas de interconexión que favorecen a países emergentes).

Este mismo enfoque multiparticipativo (*multistakeholderism*) se replica en el Foro de Gobernanza de Internet, creado por Naciones Unidas para apoyar la gobernanza de Internet de forma abierta a la participación y los asuntos que la afectan; un foro que se reúne anualmente, la última vez en noviembre de 2018 en París, cuando se lanzó la "Paris Call for trust and security in the cyberspace" a iniciativa del presidente Emmanuel Macron y secundada por numerosos actores, públicos y privados, que preparan las agendas de trabajo[3]. En la defensa de una Internet abierta y accesible participan otras asociaciones, como Internet Society, dedicada a expandir la accesibilidad y fomentar la seguridad técnica mediante su Grupo de Trabajo de Ingeniería de Internet (Internet Engineering Task Force, IETF), su Consejo de Arquitectura de Internet (Internet Architecture Board, IAB) o su Grupo de Trabajo de Investigación en Internet (Internet Research Task Force, IRTF). Entre los valedores de Internet también se encuentran *think tanks* como el EastWest Institute y el Hague Centre for Strategic Studies, que dan soporte a la Global Commission on the Stability of the Cyberspace[4]. Estos ecosistemas abiertos, cosmopolitas y liberales, valedores de la sociedad de la información, coadyuvan a la gobernanza de Internet, pero carecen de instrumentos vinculantes para implantar sus propuestas y acuerdos y se enfrentan a la resolución de graves problemas de seguridad, conectividad y manipulación de sus contenidos.

Las amenazas y riesgos del soporte y los servicios de Internet

En líneas generales, la gobernanza de Internet se enfrenta a un riesgo de fragmentación debido a retos de naturaleza tecnológica, económica y política. Internet se configuró como una red de redes, una red de sistemas y aplicaciones que permitía la conectividad de esos sistemas autónomos. Por consiguiente, hay que diferenciar entre el riesgo

[3] El capítulo español (IGF Spain) organizó en Madrid sus jornadas de noviembre sobre "Conflicto en la red? Internet, el tablero estratégico mundial" para preparar la sesión anual del IGF de 2019 en Berlín en noviembre, https://www.internetsociety.org/events/igf/2019/?gclid=EAIaIQobChMIpIfx74D75QIVUIXTCh3yzwpgEAAYASAAEgJ_dvD_BwE.

[4] Esta Comisión Mundial sobre la Estabilidad en el Ciberespacio recomienda en su informe "Advancing Cyberstability" (noviembre de 2019, p. 17, https://cyberstability.org/wp-content/uploads/2019/11/Digital-GCSC-Final-Report-Nov-2019_LowRes.pdf) el enfoque multiparticipativo para la protección del ciberespacio y la promulgación de estándares.

tecnológico de la fragmentación de la conectividad formando islas y los riesgos que las malas prácticas comerciales y políticas representan para el bien común mundial que es Internet.

Entre los riesgos tecnológicos que amenazan a una Internet abierta, según el Foro Económico Mundial (WEF), están los que comprometen su arquitectura, sus estándares y protocolos en sus distintas capas[5], tales como la compatibilidad entre versiones de los protocolos de Internet, la separación entre la superficie accesible desde buscadores web y las partes más profundas de la web, el desvío de los flujos de información mediante el *secuestro* de puertas de enlace de red (BGP, *Border Gateway Protocol*, o Protocolo de Fronteras entre Puertas de Enlace), la alteración de las cachés de los servidores de nombres de dominio (DNS) o los certificados de autenticación falsos. Estos obstáculos técnicos dificultan la comunicación de extremo a extremo de la Red y disminuyen su capacidad de multiplicar la innovación.

Además de los riesgos tecnológicos que afectan a la infraestructura de Internet y la conectividad de los usuarios, existen otras prácticas que afectan a los servicios que se prestan a través de la Red y que limitan la libertad de acceso y uso de Internet y sus servicios debido a la creciente competencia comercial y política entre Estados y grandes plataformas. En efecto, las malas prácticas comerciales, especialmente debido al abuso de la posición de dominio de las grandes plataformas, también pueden afectar a la apertura de Internet. La fragmentación o los sesgos discriminatorios de las búsquedas, la geolocalización, el geobloqueo por razones arbitrarias, el pago adicional por el tráfico de acceso a determinados contenidos que se suma al pago por el acceso a Internet o la pérdida de la neutralidad de la Red son, entre otros, motivos de preocupación para los internautas, según el informe del WEF.

Fuera de motivos técnicos y comerciales, Internet corre el riesgo de que los Estados quieran controlar la gobernanza de los dominios que no son de titularidad gubernamental (*generic top-level domains*, gTLD), ya sea para proteger la privacidad de sus ciudadanos y empresas o para facilitar las investigaciones de las agencias de seguridad, con la consiguiente tensión entre los gestores gubernamentales de la UIT y los *multistakeholders* de la ICANN.

La acumulación de los riesgos anteriores ha llevado a cuestionar la integridad de Internet como una única red de redes y a prever su fragmentación en redes segregadas (*splinternet*), lo que se conoce como *balcanización*. El riesgo de fragmentación es constatable en regímenes autoritarios como China (el Gran Cortafuegos), Rusia (RuNet), Irán o Corea del Norte, entre otros, que tratan de aislar a sus ciudadanos de toda influencia exterior que pueda llegar por Internet y controlar el uso interno de las redes segregadas de la Internet mundial. Pero también existen precedentes de vigilancias y censuras sobre Internet en las democracias liberales por razones de seguridad nacional o para prevenir campañas de radicalización o de odio. Se espera en

[5] Los protocolos permiten un modelo de conexión entre los servicios (*Transmission Control Protocol/Internet Protocol*, TCP/IP) que se prestan a través de la capa física (cable, satélites, *routers*, IXP, ISP) y las distintas capas lógicas de Internet, como las de acceso (wifi, Ethernet), direccionamiento (IP), trasporte de datos (UDP, TCP) o aplicaciones (HTTP, SMTP).

ellas que las grandes plataformas ejerzan el papel de regulación y control que no pueden o no saben realizar sus Gobiernos. La tensión entre los servicios mundiales y las regulaciones nacionales puede agravar el riesgo de que las grandes plataformas privadas de uno u otro lado se acaben segregando en las redes privadas de la Internet pública y mundial[6].

En todos los casos, aunque con distinta motivación y alcance, la fragmentación aumenta la vulnerabilidad de los internautas frente a las prácticas de los Gobiernos y conglomerados tecnológicos. Se materialice o no, el riesgo de fragmentación se suma a los factores de seguridad e inestabilidad, que están haciendo crecer la desconfianza en la Red y disminuyendo su potencial dinamizador e innovador, lo que ralentiza el progreso hacia la economía digital. A pesar de todos estos riesgos y de los indicios de fragmentación de Internet, en relación con la gobernanza mundial o con los servicios que se prestan sobre ella, los valedores públicos, privados y público-privados de la gobernanza de Internet han conseguido preservar hasta ahora la conectividad de la infraestructura. Como señala Zoraida Frías: "Mientras la gobernanza técnica de Internet ha conseguido establecerse al margen de los Gobiernos, la gobernanza socioeconómica ha convertido la Red en el campo de batalla en el que se juega el nuevo orden mundial"[7]. No obstante, se enfrentan al reto de sostener esa conectividad de Internet frente a nuevos problemas como son la competencia geopolítica y tecnológica entre las grandes potencias y la alteración de la información que circula por ella.

Las amenazas y riesgos sobre el flujo de información y datos

La información y los datos no pueden escapar a su instrumentalización (*weaponization*) por las grandes potencias en su competición geotecnológica por el poder y la supremacía mundial[8]. Gobiernos como los de Estados Unidos, China o Rusia utilizan el ciberespacio para vigilar o espiar a sus rivales, influir en sus decisiones o desestabilizar sus sociedades. Desarrollan instrumentos, técnicas y prácticas que pueden emplearse tanto para defenderse como para atacar y entrenan a organizaciones gubernamentales o paragubernamentales en su empleo y perfeccionamiento. Entre otros, la desinformación, el espionaje, el robo de propiedad intelectual y el *malware* (p. ej. WannaCry, Stuxnet) son instrumentos gubernamentales que, más pronto que tarde, dejarán de serlo para pasar al ámbito no estatal, donde esos instrumentos y sus aplicaciones se ofrecerán para alentar conflictos sociales o económicos a través de Internet, una pérdida de la hegemonía estatal en el ciberespacio que ya han iniciado actores criminales, hacktivistas y terroristas cuyas acciones se dirigen contra Internet y contra la información que circula por ella.

[6] Steve Song, "Internet Drift: How the Internet is Likely to Splinter and Fracture", Digital Freedom Fund, https://digitalfreedomfund.org/wp-content/uploads/2018/12/04-Essay_Internet-Drift-How-the-Internet-is-Likely-to-Splinter-and-Fracture.pdf.

[7] Zoraida Frías, "Guerra por la gobernanza socioeconómica", *Telos* 110, pp. 37-43, https://telos.fundaciontelefonica.com/wp-content/uploads/2019/04/telos-110-cuaderno-geotecnologia-zoraida-frias.pdf.

[8] Eric Rosenbach y Katherine Mansted, "The Geopolitics of Information", Belfer Center, 28/V/2019, https://www.belfercenter.org/sites/default/files/2019-08/GeopoliticsInformation.pdf.

Las formas de dañar la infraestructura de Internet son distintas de las de atacar los datos que circulan por ella. Las sociedades avanzadas, al igual que la economía digital, funcionan en torno a datos (el nuevo petróleo), por lo que éstos son fuente de oportunidades y de vulnerabilidades. Mientras que las grandes plataformas luchan por acumular datos para competir en posiciones de ventaja frente a las compañías poco digitalizadas y sin capacidad para procesar los datos, los agentes estatales y no estatales luchan por desarrollar instrumentos de influencia construidos a partir de esos datos.

Los Estados han desarrollado instrumentos y doctrinas para influir sobre el comportamiento de los líderes y las opiniones públicas en tiempos de conflicto (guerra de la información, operaciones de influencia y cognitivas) que ahora aplican a la competición geopolítica distinta de la guerra. Son instrumentos que llevan la antigua guerra política (*political warfare*) de la Guerra Fría al ciberespacio y desarrollan nuevas formas de defensa y agresión para competir en los nuevos modos de conflicto geopolítico que no son ni de guerra ni de paz y para los que se emplean distintas denominaciones de guerra: "sin restricciones", "de nueva generación", "de zona gris", "híbrida" o "asimétrica". Y no solo actores estatales como Estados Unidos o Rusia, sino también actores como Daesh, según análisis como los de la Rand Corporation[9].

Las fuentes abiertas de información disponibles en Internet ofrecen estudios sobre la manipulación del contexto informativo y los valores, creencias y principios que condicionan la percepción social (cognición) de la información (infosfera) mediante operaciones de influencia o cognitivas[10]. Revelan la interferencia detectada en algunos procesos electorales, el recurso a la desinformación o las noticias falsas para facilitar la desestabilización social y política[11]. Las democracias liberales, especialmente las europeas, han sido ingenuas creyendo que el ciberespacio se mantendría al margen de la rivalidad geopolítica y que los agentes autoritarios no utilizarían como armas las infraestructuras y los datos de Internet. Sin embargo, lo preocupante no son tanto los ciberataques, la desinformación o las noticias falsas que utilizan Internet, sino el potencial de manipulación social que conllevan las nuevas tecnologías de análisis, procesamiento y computación de datos.

Basta una lectura rápida a la "Investigación sobre el uso del análisis de datos en campañas políticas" del comisario de Información al Parlamento del Reino Unido tras el escándalo de Cambridge Analytica para darse cuenta de la capacidad de influencia de

[9] Linda Robinson et ál., *Modern Political Warfare*, RAND Corporation, 2018, p. xiv, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1772/RAND_RR1772.pdf.

[10] Yossi Kupperwasser y David Simon-Tov, "The Cognitive Campaigns: Strategic and Intelligence Perspectives", *Intelligence in Theory and Proactive* 4, INSS, octubre de 2019, https://www.inss.org.il/wp-content/uploads/2019/10/Memo197_e_compressed.pdf.

[11] Entre otros en español, los del CCN-CERT sobre "Buenas Prácticas PP/13. Desinformación en el ciberespacio" (https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/7680-como-actuar-frente-a-las-campanas-de-desinformacion-en-el-ciberespacio-uno-de-los-mayores-retos-de-seguridad-del-pais.html) y el de Ángel Badillo sobre "La sociedad de la propaganda, 'fake news' y la nueva geopolítica de la información", DT 8/2019, Real Instituto Elcano, mayo de 2019, http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt8-2019-badillo-sociedad-de-desinformacion-propaganda-fake-news-y-nueva-geopolitica-de-informacion.

esas tecnologías. Y no sólo para alterar el resultado de las votaciones o manipular a la sociedad, sino para alterar la percepción de la realidad y cambiar el modelo de las relaciones o la estructura social provocando la disrupción social mediante las nuevas herramientas de ingeniería social disponibles –ahora *online*– para la sociedad de la información.

Por un lado, se fragmenta la percepción social de la realidad. Se reduce el número de fuentes de información solventes y contrastadas y se concentra su control en pocas manos. A la reducción de la diversidad se añade el aislamiento en *burbujas* de información y la presión de *influencers*, *trolls* y mecanismos de adicción sobre las redes sociales. La combinación de los factores anteriores aumentará la dificultad para discernir la realidad de la ficción, disminuirá la confianza en las instituciones y potenciará la polarización social, una disrupción potenciada desde el mal uso de Internet que amenaza la democracia, según la Fundación Koffi Annan de Stanford, salvo que se adopten medidas para prevenirlas[12]. La defensa de las sociedades abiertas frente a esta combinación de procesos e intenciones disruptivos resulta difícil, porque se lleva a cabo de forma larvada e imperceptible. Tras la sensación virtual de los internautas de que cada vez disponen de más información y mayor libertad de opciones que nunca se esconde la manipulación encubierta de sus emociones, preferencias y decisiones por la nueva ingeniería tecnológica, una disrupción que se acentuará con el perfeccionamiento de la inteligencia artificial y la llegada de la computación cuántica en un escenario distópico que la RAND etiqueta como de "conflicto social virtual"[13].

Para prevenir una evolución distópica de la sociedad de la información, los valedores de Internet abogan por una mayor coordinación de las iniciativas públicas y privadas[14]. Por su relevancia, hay que destacar la iniciativa "Contract for the Web" del creador de la *World Wide Web* y director de la Fundación del mismo nombre, Tim Berners-Lee, para restaurar la accesibilidad de Internet y proteger la privacidad de sus usuarios. Además, la Unión Europea se dispone a pelear, alineada con el Foro de Gobernanza de Internet, para avanzar hacia la próxima generación de Internet (*Next Generation Initiative*, NGI). La esperanza de que se descentralice Internet, de que su gobernanza pueda adoptar contramedidas activas y desarrollar servicios comunes contra el dominio de Internet, su información y los datos, para que los usuarios recuperen el control de sus datos y los innovadores, oportunidades de negocio[15].

Conclusión

Internet cuenta con tantos enemigos como defensores que velan por que mantenga su condición de bien común mundial y neutro que facilite la consolidación de la sociedad digital de la información.

[12] Nathaniel Persily, "The Internet's Challenge to Democracy. Framing the Problem and Assessing Reforms", Kofi Annan Commission on Elections and Democracy in the Digital Age, 2019.

[13] Michael J. Mazarr et ál., *The Emerging Risk of Virtual Societal Warfare*, RAND Corporation, 2019, https://www.rand.org/pubs/research_reports/RR2714.html.

[14] Dan J. B. Svantesson, "Global Status Report 2019", International & Jurisdiction Policy Network, p. 17, https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Global-Status-Report-2019-Key-Findings_web.pdf.

[15] DG Connect, "Next Generation Internet 2025", DG Connect, 2018, pp. 17-18.

La batalla se libra, por un lado, sobre las infraestructuras y los servicios de Internet y, aunque los defensores han conseguido hasta ahora preservar la conectividad mundial, los enemigos tienden a reforzar la fragmentación de los distintos sistemas de la Red, unos actores, los públicos, tratando de prevenir la influencia exterior y, otros, los privados, tratando de proteger sus mercados cautivos en sus grandes plataformas.

Por otro, la batalla se libra en el frente de la información, donde actores públicos y privados compiten por hacerse con los datos y desarrollar tecnologías que les garanticen el control social o de los mercados. En medio de una creciente rivalidad geopolítica entre las grandes potencias y de una revolución económica y tecnológica acelerada, los instrumentos y prácticas que han desarrollado esas potencias para competir o defenderse en el tablero mundial se irán transfiriendo a los actores no estatales para que compitan por los mercados de la economía, la influencia o la manipulación social.
El escenario favorece a los enemigos de Internet, porque el perímetro de ataque es demasiado grande, porque los atacantes pueden concentrar sus medios de ataque y porque cuentan con la ventaja de la despreocupación social y la actuación encubierta. Frente a lo anterior, los defensores de las sociedades y la Internet abiertas se ven ante las paradojas de tener que fragmentar sus sistemas para preservar la conectividad de Internet y de tener que controlar la información que reciben sus sociedades para evitar la disrupción. La defensa de Internet no sólo necesita valedores e iniciativas como las señaladas; también necesita más estrategia, coordinación, recursos y capacidad de movilización. La edad de la inocencia se ha acabado.