CARTILLA

Fragmentación de Internet y ciberseguridad

SAMUELE DOMINIONI

Resumen de puntos clave

- La promoción de un entorno de TIC abierto, seguro, estable, accesible y pacífico es un objetivo recurrente en los procesos multilaterales relacionados con la seguridad internacional y de las TIC en las Naciones Unidas. El propio GTCA representa un hito importante en la cooperación internacional hacia un entorno de TIC de este tipo.
- El Internet sigue siendo estable y, en general, abierto y seguro en sus cimientos. Sin embargo, su fragmentación es un fenómeno creciente y preocupante. La fragmentación puede entenderse de diferentes maneras según la naturaleza de las partes interesadas. Aun así, es posible identificar una dimensión técnica del mismo ya que puede afectar componentes críticos de Internet que garantizan la interoperabilidad de redes y dispositivos.

- Existen tres áreas principales de preocupación en la dimensión técnica de la fragmentación de Internet, a saber, las relacionadas con el direccionamiento, la denominación y el enrutamiento. Algunas de estas preocupaciones se relacionan con las innovaciones necesarias que la comunidad de múltiples partes interesadas tuvo que elaborar para abordar el uso cada vez mayor de tecnologías TIC pero que aún no están completamente implementadas (por ejemplo, IPv4 e IPv6); otros se refieren a tendencias emergentes en el desarrollo de componentes técnicos críticos que divergen de los estándares y protocolos internacionales actuales (por ejemplo, en el sistema de nombres de dominio); y finalmente, otros se refieren a fallas técnicas o limitaciones en el diseño y desarrollo de componentes críticos de Internet (por ejemplo, enrutamiento).
- Estas áreas de fragmentación no sólo perjudican la apertura, la estabilidad y la accesibilidad de Internet globalmente, sino que también tienen implicaciones para la ciberseguridad. Algunos de ellos se relacionan con la ciberseguridad de los propios estándares y protocolos (por ejemplo, protocolos de enrutamiento), que pueden verse afectados por una amplia variedad de actividades TIC maliciosas. Otros se refieren a la amenaza de accesibilidad, disponibilidad y seguridad de los datos (por ejemplo, sistemas de nombres alternativos). En general, debido a la complejidad y la interdependencia de la estructura de Internet, la fragmentación de la dimensión técnica puede plantear riesgos complejos y multifacéticos (los llamados "problemas perversos") para la ciberseguridad.
- Las investigaciones futuras analizarán cómo las áreas de riesgos y tendencias identificadas en este manual podrían tener un impacto en la implementación del marco para el comportamiento responsable de los Estados en el ciberespacio y, por lo tanto, en la paz y la seguridad internacionales.

Introducción

La promoción de un entorno de TIC abierto, seguro, estable, accesible y pacífico es un objetivo recurrente en los procesos multilaterales relacionados con la seguridad internacional y de las TIC en las Naciones Unidas. Por ejemplo, el informe final del Grupo de Expertos Gubernamentales (GEG) de 2021 sobre la promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional afirmó que “un entorno de TIC abierto, seguro, estable, accesible y pacífico es esencial para todos y requiere cooperación efectiva entre los Estados para reducir los riesgos para la paz y la seguridad internacionales”.[1] El informe final del Grupo de Trabajo de Composición Abierta (GTCA) sobre avances en el campo de la información y telecomunicaciones en el contexto de la seguridad internacional recordó que “[e]l GTCA representa un hito importante en la cooperación internacional hacia un entorno de TIC abierto, seguro, estable, accesible y pacífico”.[2] Además, ambos informes subrayaron la importancia de proteger la infraestructura técnica esencial para la disponibilidad general y la integridad del Internet.[3] La resolución de

---

1 Asamblea General, 2021, A/76/135, **https://undocs.org/Home/Mobile?FinalSymbol=A%2F76%2F135.**

2 Asamblea General, 2021, A/75/816, **https://undocs.org/Home/Mobile?FinalSymbol=A%2F75%2F816**.

3 El informe del GEG 2021 reclama “la disponibilidad general o integridad de Internet”. Véase Asamblea General, 2021, A/76/135, párr. 10.

la Asamblea General que estableció el actual GTCA (2021-2025) confirmó: "las conclusiones del Grupo de Expertos Gubernamentales, en sus informes de 2013 y 2015, de que el derecho internacional, y en particular la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz y la estabilidad y promover un entorno de tecnología de la información y las comunicaciones abierto, seguro, estable, accesible y pacífico".[4] Sin embargo, la fragmentación del entorno de las TIC, y más concretamente de Internet, se ha convertido en una posibilidad cada vez más preocupante, algo que ya se está produciendo en determinados entornos. De hecho, la fragmentación de Internet puede tener efectos en niveles diferentes y a veces entrelazados, incluidos el político, el comercial y el tecnológico.[5] Un número cada vez mayor de Estados y otras partes interesadas están expresando preocupación por un escenario de fragmentación de Internet. El documento del Secretario General, Nuestra Agenda Común, señala que evitar la fragmentación de Internet es una acción a considerar, y es uno de los principales temas que se incluirán en el próximo Pacto Digital Mundial.

Este manual es el primer resultado de un proyecto más amplio sobre fragmentación de Internet y seguridad internacional, y tiene como objetivo presentar el tema de la fragmentación de Internet y delinear los principales desafíos que se pueden plantear a la ciberseguridad entendida en sentido amplio. Sobre la base de este primer resultado, la segunda parte del proyecto de investigación analizará cómo la fragmentación de Internet afecta la seguridad internacional y, en particular, la implementación del marco de comportamiento estatal responsable en el ciberespacio (en adelante, el Marco). Este manual tiene como objetivo proporcionar a los responsables de políticas, diplomáticos y otras partes interesadas no técnicas una descripción general introductoria de los desarrollos de la fragmentación de Internet y sus implicaciones para la seguridad cibernética. El material presentado aquí se extrae de fuentes disponibles públicamente, entrevistas a expertos (realizadas entre septiembre y noviembre de 2023) y un diálogo de múltiples partes interesadas con oradores del sector privado, el mundo académico y la sociedad civil celebrado en línea el 17 de octubre de 2023.

¿Qué es la fragmentación de Internet?

La fragmentación de Internet es un concepto controvertido que puede tener diferentes interpretaciones según la naturaleza de la parte interesada. Sin embargo, según ciertos estudiosos, es posible identificar una tendencia en la comprensión tripartita de la fragmentación de Internet, que puede referirse a una fragmentación técnica, comercial,

---

[4] Asamblea General, 2020, A/RES/75/240, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf.

[5] William J. Drake, Vinton G. Cerf y Wolfgang Kleinwächter, 2016, "Fragmentación de Internet: Un Vistazo General", Artículo técnico de la Iniciativa sobre el futuro de Internet, Foro Económico Mundial, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_ An_Overview_2016.pdf.

y gubernamental.[6] Otros conciben la fragmentación tripartita con una comprensión ligeramente diferente.[7] Dado que este manual se centra en el impacto de la fragmentación de Internet en la ciberseguridad, enfoca el análisis en la dimensión técnica.[8] Según un documento técnico del Foro Económico Mundial (FEM) sobre la fragmentación de Internet, la fragmentación técnica ocurre cuando hay "condiciones en la infraestructura subyacente [es decir, las capas de Internet] que impiden la capacidad de los sistemas para interoperar e intercambiar completamente paquetes de datos y de Internet para funcionar consistentemente en todos los puntos finales".[9] El Recuadro 1 proporciona una breve descripción de las capas de Internet y sus funciones.

Recuadro 1: Las capas de Internet

Los modelos de Interconexión de Sistema Abierto (OSI, por sus siglas en inglés) y Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP) se encuentran entre los métodos más utilizados para clasificar la estructura en capas de Internet. Estos modelos suelen representarse como una pila vertical. Cada capa tiene la tarea de funciones diferentes pero interconectadas que transforman una pieza de información (por ejemplo, una consulta de texto en un navegador) en paquetes de datos para hacer posible la comunicación entre dos (o más) dispositivos.

El **modelo OSI** contiene siete capas: aplicación, presentación, sesión, transporte, red, enlace de datos y física.

1. La **capa de aplicación** proporciona servicios para aplicaciones de red que utilizan Internet, como navegadores, correo electrónico y aplicaciones de telecomunicaciones.
2. En la **capa de presentación**, la información de la capa de aplicación se formatea para mostrarse (en caso de que se esté recibiendo) o para procesarla más (en caso de que se esté enviando).
3. En la **capa de sesión**, se producen los procesos de autenticación y autorización. Por ejemplo, la autenticación (es decir, iniciar sesión en una aplicación) establece la conexión entre el usuario y el servidor de aplicaciones, iniciando así una sesión.

---

6 Ibídem.

7 Por ejemplo, el documento de debate sobre la fragmentación de Internet de la red de políticas del IGF sobre la fragmentación de Internet utiliza las siguientes dimensiones: fragmentación de la experiencia del usuario, fragmentación de la capa técnica de Internet y fragmentación de la gobernanza y coordinación de Internet; PNIF, 2023, Documento de debate del PNIF (aporte al IGF 2023), 15 de septiembre, https://www.int-govforum.org/en/filedepot_download/256/26218.

8 Los efectos de la fragmentación política y comercial sobre la ciberseguridad se considerarán en futuras publicaciones.

9 William J. Drake, Vinton G. Cerf y Wolfgang Kleinwächter, 2016, "Fragmentación de Internet: Un Vistazo General", Artículo técnico de la Iniciativa sobre el futuro de Internet, Foro Económico Mundial, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf. 14.

4. La **capa de transporte** garantiza la confiabilidad de la comunicación entre dispositivos y redes. Hay dos protocolos principales que permiten este "transporte", el Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP). El primer protocolo se utiliza para establecer conexiones que transfieren información de manera confiable entre dispositivos, pero puede ser lento. El segundo, UDP, se utiliza para conexiones que requieren mayor velocidad pero menor precisión en la transferencia de datos (por ejemplo, *streaming* de vídeos).

5. La **capa de red** facilita la transmisión de datos entre dispositivos en diferentes redes. Una de las funciones de esta capa es el direccionamiento lógico, que adjunta la dirección IP de cada usuario al paquete de datos para garantizar que pueda llegar al destino correcto. Luego, estos datos se transmiten a través de enrutadores de una red a otra. Esta capa utiliza la determinación de ruta que se utiliza para encontrar la mejor ruta posible para la entrega de datos.

6. La **Capa de enlace** de datos ayuda a preparar la información a enviar entre diferentes redes e intenta evitar errores que puedan ocurrir en el tránsito en la capa posterior.

7. En la última capa del modelo OSI, la **capa física**, los datos se convierten en código binario que a su vez se transforma en señales para transmitirse a través de medios locales (o al revés en caso de recibir los paquetes), que son la conexión física entre dispositivos (por ejemplo, cable de cobre, fibra óptica o aire para señales de radio).

TCP/IP es similar al modelo OSI pero sintetiza las capas de aplicación, presentación y sesión del modelo OSI en una sola capa que se llama capa de aplicación en el modelo TCP/IP. Las capas restantes reciben el mismo nombre que las del modelo OSI: transporte, red, enlace de datos y física.

Tabla 1: Los dos modelos

OSI	TCP/IP
Aplicación (la interacción persona-computador)	**Aplicación** (presentación de datos, codificación y control de sesión)
Presentación (representación de datos y cifrado)	
Sesión (comunicación entre hosts)	
Transporte (TCP y UDP)	**Transporte** (TCP y UDP)
Red (enrutamiento y direcciones IP)	**Red** (enrutamiento y direcciones IP)
Enlace de datos (recuperación de errores y retransmisión)	**Enlace de datos** (recuperación de errores y retransmisión)
Físico (envío de datos electrónica u ópticamente o como ondas de radio)	**Físico** (envío de datos electrónica u ópticamente o como ondas de radio)

De hecho, Internet puede funcionar como un bien público abierto y global debido a varias infraestructuras y propiedades que permiten la comunicación y el intercambio de información (en forma de paquetes de datos) independientemente de dónde se encuentra, quién es y a través de qué dispositivos se conecta a Internet. Entre estos, hay componentes críticos que garantizan la interoperabilidad de redes y dispositivos (ver Recuadro 2).

Recuadro 2. Componentes críticos de Internet

Las siguientes iniciativas han contribuido a resaltar cuáles constituyen los componentes críticos de Internet.

La Comisión Global sobre la Estabilidad del Ciberespacio elaboró el concepto de Núcleo Público de Internet, que incluye:

1. Enrutamiento y reenvío de paquetes
2. Sistemas de denominación y numeración.
3. Mecanismos criptográficos de seguridad e identidad.
4. Medios de transmisión
5. Software
6. Centros de datos[10]

La Sociedad de Internet ha propuesto cinco propiedades críticas que definen las funciones esenciales de las redes de Internet:

1. Una infraestructura accesible con un Protocolo Común abierto y con barreras de entrada bajas.
2. Arquitectura abierta de bloques de construcción interoperables y reutilizables basada en procesos de desarrollo de estándares abiertos adoptados voluntariamente por una comunidad de usuarios.
3. Gestión Descentralizada y un Sistema Único de Enrutamiento Distribuido, escalable y ágil.
4. Identificadores globales comunes que son inequívocos y universales.
5. Una red de uso general, tecnológicamente neutral, simple y adaptable.[11]

---

[10] Comisión Mundial sobre la Estabilidad del Ciberespacio, “Progreso hacia la ciberstabilidad”, noviembre de 2019, https:// hcss.nl/wp-con- tienda/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.

[11] Internet Society, “La forma de establecer contactos en Internet: Definición de las propiedades críticas de Internet”, septiembre de 2020, https:// www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/.

El documento de debate del Foro de Gobernanza de Internet, Red de Políticas de Fragmentación de Internet (PNIF) afirma que la fragmentación de la infraestructura técnica de Internet se relaciona con "una serie de desafíos a esta interoperabilidad en la capa de transporte técnico que hace que Internet funcione".[12] De hecho, el Internet global está "basado esencialmente en el diseño de la capa de transporte de Internet y el uso común de los mismos protocolos técnicos (TCP/IP, DNS, BGP, HTTP, IPv4&6, etc.), basado en un sistema de servidor raíz unificado pero descentralizado para todo tipo de comunicación por Internet".[13] Por lo tanto, debido a las características esenciales relacionadas con los componentes críticos de Internet, las acciones encaminadas a fragmentar esta dimensión técnica constituyen una amenaza muy grave a su apertura e interoperabilidad.

Áreas de riesgos de fragmentación de Internet a nivel técnico

La fragmentación técnica es una preocupación recurrente, especialmente para la comunidad de múltiples partes interesadas que se ocupa de los componentes críticos de Internet. El documento técnico del FEM sobre la fragmentación de Internet publicado en 2016 afirmaba que "Internet permanece estable y, en general, abierto y seguro en sus cimientos".[14] Casi ocho años después, lo que para la tecnología es un lapso de tiempo, estos cimientos siguen siendo sólidos, aunque existen fragilidades y riesgos crecientes.[15] Con el fin de basarse consistentemente en la literatura existente y, en particular, en el documento técnico del FEM, este informe utiliza las mismas áreas de riesgos, a saber, direccionamiento, denominación (el Sistema de Nombres de Dominio) y enrutamiento (interconexión) del Internet,[16] para determinar las tendencias actuales que están debilitando sus cimientos.

Direccionamiento

El direccionamiento se refiere a los identificadores únicos, también llamados direcciones

---

[12] PNIF, 2023, PNIF Discussion Paper (input to IGF 2023), 15 September, https://www.intgovforum.org/en/filedepot_download/256/26218, p. 12.

[13] Wolfgang Kleinwächter and Alexander Klimburg, 2023, "Fragment or Not Fragment – Is This the Question? Will the "One-World-One Internet" Survive Today's Geopolitical Stress Test?", CircleID, 6 June, https://circleid.com/posts/20230606-fragment-or-not-fragment-is-this-the-question-will-one-world-one-internet-survive-todays-geopolitical-stress-tests.

[14] William J. Drake, Vinton G. Cerf y Wolfgang Kleinwächter, 2016, "Fragmentación de Internet: Un Vistazo General", Artículo técnico de la Iniciativa sobre el futuro de Internet, Foro Económico Mundial, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_ An_Overview_2016.pdf. 8.

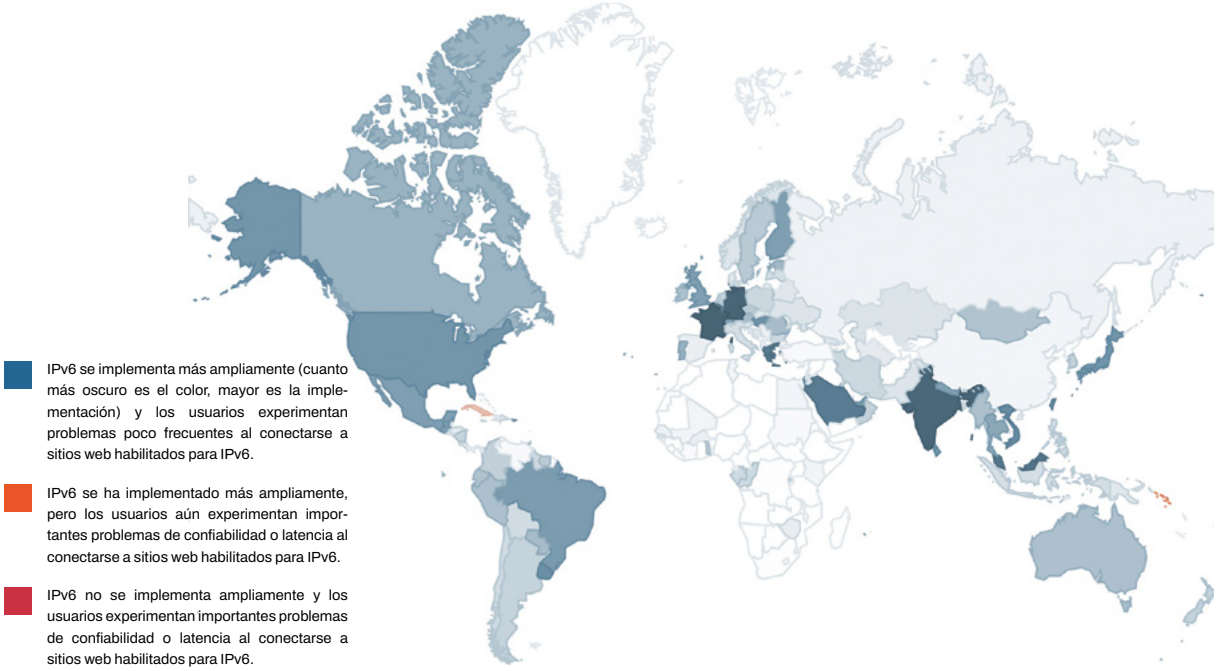
[15] Entrevista del autor con el Dr. Vinton G. Cerf, uno de los autores del Documento técnico del FEM sobre la fragmentación de Internet, 26 de octubre de 2023.

[16] Una forma sencilla de entender el direccionamiento, la denominación y el enrutamiento es considerar estos términos como "El nombre de un recurso indica lo que buscamos, una dirección indica dónde está y una ruta nos dice cómo llegar allí"; John F. Schoch, 1978, "A Note on Inter-Network Naming, Addressing, and Routing", Internet Experiment Note # 19, Notebook Sección 2.3.3.5, https://www.rfc-editor.org/ ien/ien19.txt.

IP, expresados en valores decimales, que designan puntos únicos en Internet. Existen dos temas importantes tienen que ver con la IP y la fragmentación. El primero se relaciona con la adopción y compatibilidad de dos versiones de IP (IPv4 e IPv6), y el segundo, con la gestión de números IP.

Actualmente existen dos versiones principales de direcciones IP: IPv4 e IPv6. El primero se compone de un espacio de direcciones de 32 bits y puede generar hasta alrededor de 4.300 millones de direcciones. Debido al enorme aumento de puntos finales (por ejemplo, dispositivos) en Internet en las últimas décadas, IPv4 ha agotado sus posibles combinaciones. Por lo tanto, para responder a esta necesidad de identificadores más únicos, se introdujo una nueva versión de IP (IPv6) con espacio de direcciones de 128 bits. IPv6 puede cubrir hasta 340 billones de billones de billones de puntos finales.[17] Sin embargo, IPv4 e IPv6 no son directamente interoperables. Esto significa que los dispositivos en redes IPv4 no pueden comunicarse con dispositivos en redes IPv6.[18] La compatibilidad sólo se puede lograr mediante tecnologías de transición, como las redes de doble pila. La fragmentación puede ocurrir en caso de discrepancias en versiones de IP no sostenidas por tecnologías de transición entre países y regiones del mundo. El nivel de adopción de IPv6 está aumentando constantemente[19] con variaciones entre países.

Figura 1: Adopción de IPv6 por país



Fuente: Estadísticas de Google (Google recopila estadísticas sobre la adopción de IPv6 en Internet de forma continua)

---

17 William J. Drake, Vinton G. Cerf y Wolfgang Kleinwächter, 2016, "Fragmentación de Internet: Un Vistazo General", Artículo técnico de la Iniciativa sobre el futuro de Internet, Foro Económico Mundial, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_ An_Overview_2016.pdf.

18 Erik Bais, "IPv4 frente a IPv6: Lo que los profesionales de la seguridad deben saber", Prefix Broker, https://www.prefixbroker.com/news/ipv4-vs-ipv6-what-security-professionals-should-know/.

19 En el momento de la publicación del documento técnico del FEM, la conectividad IPv6 representaba solo el 4 por ciento de Internet, mientras que en octubre de 2023, representa alrededor del 40 por ciento (fuente https://www.google.com/intl/en/ipv6/statistics.html).

Por lo tanto, la fragmentación en el sentido de esta faceta de la brecha digital es posible y plantea riesgos para la interoperabilidad general de las redes y dispositivos entre países y regiones.

El segundo aspecto de la fragmentación de IP se refiere a la gestión de los números IP utilizados para las direcciones IP. En el estado actual de Internet, esta tarea la gestiona la Autoridad de Números Asignados de Internet (IANA, una filial de la Corporación de Internet para la Asignación de Nombres y Números (ICANN), junto con los Registros Regionales de Internet (RIR), y se implementa en amplias regiones porque las estructuras de Internet no están contenidas dentro de las fronteras nacionales. Es clave que exista un sistema responsable de la singularidad global de los IP; de lo contrario, existe el riesgo de crear direcciones IP alternativas y no coordinadas que compliquen, o incluso imposibiliten, la compatibilidad con la infraestructura existente basada en IPv4 o IPv6.[20]

Denominación

La denominación se refiere al Sistema de nombres de dominio (DNS), que traduce los nombres en direcciones IP (por ejemplo, para el sitio web de UNIDIR el DNS es https://unidir.org y su IP correspondiente es 34.xyz).[21] Para garantizar esta característica, es esencial que la gestión de esta tarea única de mapeo y emparejamiento (realizada por ICANN) permanezca estable, consistente y legítima. Los intentos de establecer sistemas de nombres alternativos (incluida la gestión de la zona raíz)[22] sería una de las peores formas posibles de fragmentación[23] porque se perderían las traducciones DNS únicas. Esto daría lugar a inconsistencias y posibles errores de búsqueda de DNS; por ejemplo, diferentes usuarios que digiten https://unidir.org podrían abrir otras páginas distintas a la prevista.

Enrutamiento

El enrutamiento se refiere a los protocolos utilizados para garantizar que la información siga el camino correcto y óptimo cuando viaja a través de una red. En caso de que la información necesite viajar de una red a otra (Internet se compone de muchas redes diferentes a menudo administradas individualmente por un único proveedor de servicios), los protocolos de puerta de enlace fronteriza (BGP) sirven para conectarlas, permitiendo así el sistema de enrutamiento global de Internet. Como se señala en el documento técnico del FEM, “todavía es técnicamente posible que se produzca una corrupción deliberada o accidental de los datos de enrutamiento”.[24] La seguridad del sistema de enrutamiento aún necesita mejoras, por ejemplo, mediante la implementación de la llamada Infraestructura de clave pública de recursos (RPKI), un marco de infraestructura de clave pública diseñado para proteger el protocolo de puerta de enlace

---

[20] Véase, por ejemplo, el debate en torno a la propuesta de la 'Nueva IP': Alain Durand, 2020, “Nuevo IP”, Oficina del Director de Tecnología de ICANN, https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf.

[21] La dirección IP completa está oculta.

[22] La zona raíz es la parte de nivel superior (punta) de la jerarquía DNS (por ejemplo, en https://unidir.org la punta es “.org”).

[23] Diálogo entre múltiples partes interesadas sobre la fragmentación de Internet y la ciberseguridad, 17 de octubre de 2023; William J. Drake, Vinton G. Cerf y Wolfgang Kleinwächter, 2016, “Fragmentación de Internet: Un Vistazo General”, Artículo técnico de la Iniciativa sobre el futuro de Internet, Foro Económico Mundial, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

[24] Ibidem., pág. 23.

fronteriza.[25] En general, si el BGP no está protegido adecuadamente, puede ocurrir la fragmentación debido a la incapacidad de la red para garantizar la confidencialidad, integridad y disponibilidad de los datos.

Áreas de preocupación por la ciberseguridad

El objetivo de este manual no es sólo comprender la fragmentación de Internet y su estado actual, sino también identificar posibles implicaciones para la ciberseguridad. Este manual analiza la ciberseguridad desde un punto de vista muy integral, que se basa en la llamada tríada de ciberseguridad[26] y la autenticidad. En general, la fragmentación de Internet puede entrañar múltiples riesgos para la ciberseguridad que pueden englobar los llamados 'problemas perversos'.

Tabla 2: Tipos de problemas

TIPO	CARACTERÍSTICAS	RUTA DE SOLUCIÓN
Simple	Se conocen las soluciones o los enfoques de diseño para las soluciones	**Cooperación:** sensibilización, intercambio de información, normalmente grupos de operadores de red y a través de Grupos de Operador de Red
Complejo	No existe ninguna solución conocida. El problema abarca varias partes de Internet.	**Consenso:** desarrollo de estándares abiertos y basados en el consenso
Perverso	No existe ninguna solución en ningún ámbito. Falta general de acuerdo sobre la existencia o caracterización del problema.	**Colaboración:** ir más allá de los límites existentes del dominio y la organización y establecer procesos para determinar problemas y soluciones

Fuente: Leslie Daigle, Konstantinos Komaitis y Phil Roberts "Claves para una colaboración exitosa y para resolver problemas complicados", Internet Society, 2016.Internet Society, 2016.

---

[25] Entrevista del autor con el Dr. Vinton G. Cerf, uno de los autores del documento técnico, 26 de octubre de 2023.

[26] La tríada se centra en la seguridad de los datos y se refiere a su confidencialidad, disponibilidad e integridad. La disponibilidad se refiere al hecho de que los datos deben estar disponibles para los usuarios autorizados cuando sea necesario; cualquier evento que pueda retrasar su acceso está afectando la disponibilidad de los datos. La confidencialidad se refiere a la accesibilidad de los datos; sólo los usuarios autorizados deben tener acceso a datos específicos, que de otro modo deben mantenerse en secreto o privados. La integridad se refiere a la autenticidad, confiabilidad e integridad de los datos; esto significa que los datos no deben manipularse. Véase Samuele Dominioni y Giacomo Persi Paoli, 2022, "A Taxonomy of Malicious ICT Incidents", UNIDIR, https://unidir.org/publication/a-taxonomy-of-malicious-ict-incidents/.

Estos problemas surgen especialmente en campos o dominios compuestos, interconectados y de múltiples partes interesadas (por ejemplo, Internet) y pueden ser extremadamente complejos y multifacéticos.[27]

A menudo se necesita un enfoque de múltiples partes interesadas, que incluya la colaboración entre diferentes actores, sectores y países, para hacer frente a problemas complejos (véase la Tabla 1).[28] Por lo tanto, "un Internet fragmentado impide cualquier posible oportunidad de abordar la ciberseguridad porque descarta los muchos factores interdependientes y cierra los espacios para cualquier posible colaboración".[29] Además, fragmentar Internet en redes más pequeñas puede resultar en una reducción de la resiliencia general de las redes. Esto se debe a que la fortaleza de Internet es que está descentralizado y construido sobre componentes interoperables (por ejemplo, estándares y protocolos, dispositivos, etc.), que permiten a la comunidad técnica, en caso de necesidad, abordar problemas sin comprometer toda la red.[30]

Los siguientes títulos resaltan cuáles son las preocupaciones de seguridad de cada una de las áreas de fragmentación identificadas.

Direccionamiento

Hay dos implicaciones principales de ciberseguridad para la fragmentación del direccionamiento. En primer lugar, la adopción dispersa de IPv6 en todo el mundo no sólo puede fomentar la fragmentación debido a la incompatibilidad directa de los dos modelos de IP, sino también las inconsistencias en los diferentes niveles de exposición a amenazas de las TIC. IPv6 tiene características clave, incluida la integración de Seguridad del Protocolo de Internet (IPsec),[31] lo que ofrecería mayor seguridad.[32] Sin embargo, la implementación y configuración de IPv6 puede ser más desafiante que IPv4 y requiere conocimientos y habilidades técnicos específicos. Los errores en la configuración de dispositivos habilitados para IPv6 podrían introducir vulnerabilidades y, por lo tanto, hacer que los dispositivos sean más propensos a verse comprometidos.[33] Además, los dispositivos y redes que son de doble pila (es decir, que ejecutan IPv4 e IPv6 simultáneamente) pueden tener preocupaciones de seguridad adicionales debido a la mayor superficie de ataque.[34]

---

27 La mayoría de los incidentes críticos de TIC maliciosos tienen una naturaleza transfronteriza e involucran múltiples activos y actores de diferentes sectores y procedencia geográfica.

28 Leslie Daigle, Konstantinos Komaitis y Phil Roberts, 2016, "Claves para una colaboración exitosa y para resolver problemas perversos de Internet", Internet Society, **https://www.internetsociety.org/resources/doc/2017/keys-to-successful-collaboration-and-solving-wicked-internet-problems/**.

29 Konstantinos Komaitis, 2023, "Fragmentación de Internet: Por qué es importante para Europa", Investigación en enfoque, EU Cyber Direct – Iniciativa de Ciberdiplomacia de la UE, **https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/ioyLip9O/internet-fragmentation-why-it-matters-for-europe.pdf**, pag. 8.

30 Entrevista del autor con Konstantinos Komaitis, 9 de noviembre de 2023.

31 IPsec es un estándar que proporciona seguridad de canal en la capa de Internet. IPsec es obligatorio para IPv6, mientras que era opcional para IPv4. Consulte Internet Engineering Task Force (IETF), 2011, "Requisitos de nodo IPv6, Solicitud de comentario 6434", **https://www.rfc-editor.org/rfc/pdfrfc/rfc6434.txt.pdf**.

32 Emre Durda y Ali Buldu, 2010, "Comparaciones de amenazas y seguridad IPV4/IPV6", *Procedia—Ciencias sociales y del comportamiento* 2, **www.sciencedirect.com/science/article/pii/S187704281000902X**, págs. 5285–5291.

33 Agencia de Seguridad Nacional, 2023, "Guía de seguridad IPV6", U/OO/105622-23 | PP-22-1805, ver. 1.0, **https://media.defensa.gov/2023/Jan/18/2003145994/-1/-1/0/CSI_IPV6_SECURITY_GUIDANCE.PDF**.

34 Ibídem.

En segundo lugar, el desarrollo remoto, aunque posible, de IP nacionales sin coordinación o en contraste con el sistema existente perturbaría gravemente tanto la accesibilidad global como la seguridad de las redes nacionales. De hecho, en este caso, los Estados necesitarían trabajar para establecer acuerdos bilaterales con proveedores de servicios de Internet y garantizar estándares y protocolos de seguridad para sus propias redes. No todos los Estados tienen las mismas capacidades para alcanzar el mismo nivel de seguridad. Actualmente, cada Estado puede contar con una comunidad abierta de múltiples partes interesadas dedicada a desarrollar, discutir y actualizar estándares y protocolos para todos.

Denominación

La fragmentación a nivel de denominación, que se produce principalmente a través del desarrollo de sistemas de nombres alternativos, causaría enormes fallas de ciberseguridad. En este escenario, por ejemplo, al escribir el nombre de un sitio web, es posible que el usuario no pueda llegar al sitio deseado o termine en uno diferente. En general, en el caso de sistemas de nombres alternativos, los usuarios no podrán acceder a datos que, a su vez, no estarán disponibles. Además, los esfuerzos emprendidos por la comunidad de múltiples partes interesadas para conectar el DNS con sistemas de nombres alternativos pueden conducir a "resultados impredecibles, frustración de los usuarios, costos de soporte crecientes y, al final, un Internet menos seguro y estable".[35]

Enrutamiento

Los protocolos fronterizos son vulnerables a ataques que pueden alterar los flujos de datos. De hecho, BGP tiene mecanismos internos limitados que protegen contra actos maliciosos que modifican o incluso eliminan datos y, por lo tanto, interrumpen el comportamiento general de enrutamiento de la red.[36] De hecho, BGP es susceptible a amenazas TIC graves y diferentes, incluido el secuestro de rutas,[37] que puede resultar en la fragmentación de Internet y a efectos disruptivos o explotadores.[38] La mayoría de las veces, esos efectos tienen un impacto y un alcance limitados; sin embargo, otras veces, pueden producir fallos devastadores en las comunicaciones.[39] La implementación de RPKI puede ser una medida de ciberseguridad eficaz.

---

[35] Alain Durand, 2022, "Desafíos con los sistemas de nombres alternativos", OCTO-034, ICANN, **https://www.icann.org/en/system/files/files/octo-034-27apr22-en.pdf**.

[36] IETF, 2006, RFC#4272, "Análisis de vulnerabilidades de seguridad de BGP", **https://datatracker.ietf.org/doc/html/rfc4272**.

[37] Este escenario ocurre cuando los perpetradores redirigen maliciosamente el tráfico de Internet anunciando falsamente una dirección IP, que de hecho dirige el tráfico de Internet a otra IP. En otras palabras, "el secuestro de BGP es muy parecido a si alguien cambiara todas las señales en un tramo de autopista y desviara el tráfico de automóviles hacia salidas incorrectas"; Cloudflare, ¿Qué es el secuestro de BGP? **https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/**.

[38] Cada ciberincidente produce un efecto en un objetivo, y hay dos tipos principales de efectos primarios: disruptivos, que se refieren a interferir con la función de las TIC, y explotadores, que se relacionan con el robo de información. Véase Samuele Dominioni y Giacomo Persi Paoli, 2022, "A Taxonomy of Malicious ICT Incidents", UNIDIR, **https://unidir.org/files/2022-08/UNIDIR_Taxonomy_of_Malicious_ICT_Incidents.pdf**; Charles Harry y Nancy Gallagher, 2018, "Clasificación de eventos cibernéticos", *Revista de guerra de información*, vol. 17, núm. 3, **https://www.jstor.org/stable/26633163**, págs. 17-31.

[39] "Por ejemplo, aplicaciones críticas como la banca en línea, la negociación de acciones y la telemedicina funcionan a través de Internet"; Kevin Butler et al., 2010, "Una encuesta sobre problemas y soluciones de seguridad de BGP", *Actas del IEEE*, vol. 98, núm. 1, **https://ieeexplore.ieee.org/abstract/document/5357585**, págs. 100-122.

Conclusión y próximos pasos

Internet sigue siendo estable, generalmente abierto y seguro en sus cimientos. Sin embargo, existen crecientes fragilidades y riesgos en todos los niveles. La fragmentación de Internet a nivel técnico podría potencialmente destruir un entorno de TIC abierto, seguro, estable, accesible y pacífico, con implicaciones abrumadoras para la ciberseguridad.

Existen tendencias preocupantes que muestran un posible aumento de prácticas y políticas destinadas a contrastar estándares y protocolos internacionales, principalmente técnicos, lo que plantea varios desafíos para la ciberseguridad. Por lo tanto, cualquier intento arbitrario y unilateral de alterar los componentes críticos de Internet puede agravar aún más la fragmentación que ya está en curso y empobrecer la seguridad general de la red de redes y más allá. De hecho, la fragmentación de Internet podría tener implicaciones no sólo para la ciberseguridad sino también para la seguridad internacional. Investigaciones futuras analizarán cómo las áreas de riesgos y tendencias identificadas en este manual podrían tener un impacto en la implementación del marco y, por lo tanto, en la paz y la seguridad internacionales.

En conclusión, para garantizar un entorno de TIC abierto, seguro, estable, accesible y pacífico, la comunidad de múltiples partes interesadas (incluidos los Estados miembros) debería considerar la protección de la integridad, la disponibilidad y la interconexión de los componentes críticos de Internet. Para hacerlo, es clave evaluar las interdependencias de estos componentes y los efectos dominó que la manipulación de estos sistemas complejos e interconectados implicaría para estos bienes comunes globales creados por el hombre. Este manual es un esfuerzo con ese fin.

Reconocimientos

El apoyo de los principales financiadores del UNIDIR proporciona la base para todas las actividades del Instituto. Esta publicación fue financiada por la Unión Europea como parte del Programa de Tecnología y Seguridad de UNIDIR, que cuenta con el apoyo de los gobiernos de la República Checa, Alemania, Italia, los Países Bajos y Suiza, y por Microsoft. El autor extiende su agradecimiento al diverso grupo de expertos de toda la industria, el gobierno y el mundo académico que brindaron comentarios sustanciales sobre diferentes iteraciones y secciones de este documento y participaron en el taller de múltiples partes interesadas, incluidos Ang Benjamin, Jaya Baloo, Vinton Cerf, Alain Durand, Marie Humeau, Tommy Jensen, Konstantinos Komaitis, Allison Mankin, Kevin Reifsteck, Rob Spiger, Bill Woodcock, Michael Zappa. Elia Smith, profesional graduada del Programa de Seguridad y Tecnología, contribuyó al proyecto de investigación.

UNIDIR desea expresar su agradecimiento al Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) por traducir esta investigación y ponerla a disposición en español. Este informe se publicó originalmente en inglés en Diciembre 2023, que es la versión confiable; en el caso de divergencia, el texto en inglés prevalecerá.

Acerca de UNIDIR

El Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) es un instituto autónomo financiado voluntariamente dentro de las Naciones Unidas. UNIDIR, uno de los pocos institutos de políticas del mundo que se centra en el desarme, genera conocimientos y promueve el diálogo y la acción en materia de desarme y seguridad. Con sede en Ginebra, UNIDIR ayuda a la comunidad internacional a desarrollar las ideas prácticas e innovadoras necesarias para encontrar soluciones a problemas críticos de seguridad.

Autora

Dr. Samuele Dominioni es investigador del Programa de Seguridad y Tecnología de UNIDIR. Antes de unirse a UNIDIR, ocupó puestos de investigación tanto en entornos académicos como en centros de estudios. Tiene un doctorado en relaciones internacionales e historia política de Sciences Po, Francia, y de la Escuela de Estudios Avanzados del IMT, Italia.

Mención

S. Dominioni. *Fragmentación de internet y ciberseguridad: Una cartilla. Ginebra, Suiza: UNIDIR, 2023.*

Note

@unidir

/unidir

/un_disarmresearch

/unidirgeneva

/unidir

Palais des Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG