Guía para seguir comunicándonos ante bloqueos de internet

Digital
Defenders
Partnership

Créditos

Publicado por el Programa
de Defensoras Digitales

Autoría
Tatiana Avendaño y Jacobo Nájera,
Facilitdoras de Seguridad Digital,
Programa de Defensoras Digitales.

Revisión

Alexandra Haché, Oficial de Proyectos,
Redes de Respuesta Rápida e IGID,
Programa de Defensoras Digitales.

Ana Bermúdez Fong, Coordinadora
para América Latina, Programa de
Defensoras Digitales.

Inés Binder, Oficial de Comunicación,
Programa de Defensoras Digitales.

Contribuciones
Andrés Velásquez, Fundación Karisma.

Ilustraciones
Sofía Acosta Varea.

Diagramación y diseño
Juan Carlos León.

Corrección de estilo
Sebastián Goyeneche.

Credits

Published by Digital Defenders
Partnership

Authors
Tatiana Avendaño and Jacobo Nájera,
Digital Protection Facilitators, Digital
Defenders Partnership.

Reviewers

Alexandra Haché, Project Officer,
Rapid Response Network and GEDI,
Digital Defenders Partnership.

Ana Bermúdez Fong, Regional
Project Manager for Latin America,
Digital Defenders Partnership.

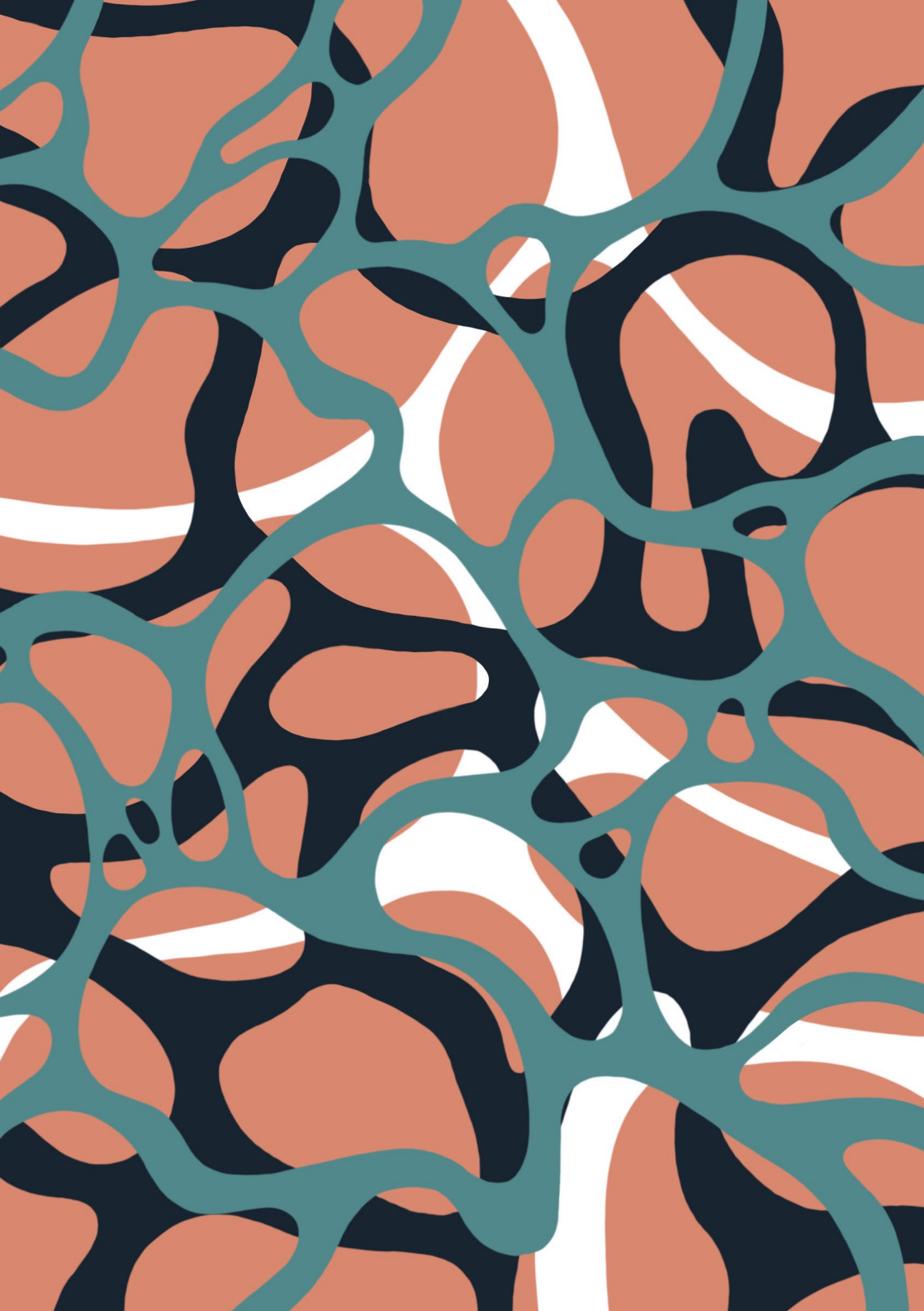
Inés Binder, Communications Officer,
Digital Defenders Partnership.

Contributions
Andrés Velásquez, Fundación Karisma.

Illustrations
Sofía Acosta Varea.

Layout and design
Juan Carlos León.

Proofreading
Sebastián Goyeneche.



Prólogo

Esta guía fue desarrollada entre junio y diciembre de 2021 como respuesta a distintos hechos de bloqueo y limitaciones en el acceso a internet en la región. La interrupción del servicio en Cali, en el marco de las protestas del Paro Nacional de Colombia, en mayo de ese mismo año, no solo expuso la necesidad de contar con herramientas para identificar, analizar y documentar los bloqueos, sino que nos enfrentó a la urgencia de expandir las maneras en las que nos comunicamos.

Comenzamos por estudiar el material existente sobre bloqueos de internet en la región y encontramos algunas ausencias. Decidimos, por lo tanto, que en vez de enfocarnos exclusivamente en los aspectos técnicos, abordaríamos los bloqueos desde una perspectiva integral. Fue así que trabajamos colectivamente e interconectadas, de sur a norte entre los dos extremos de Abya Yala,[1] con el objetivo de producir una guía que nos permitiera documentar los bloqueos pero que, a su vez, recopilara ideas para seguir comunicándonos en contextos de censura. Esa sería nuestra manera de aportar a la garantía del derecho a la comunicación y a la protesta.

Como parte de esta investigación decidimos organizar el laboratorio virtual "Más allá de internet: otras redes para comunicarnos",[2] con el apoyo del Programa de Defensoras Digitales y del Exploratorio, el taller público de experimentación del Parque Explora en Medellín. Participaron de las sesiones Pilar Sáenz y Andrés Velásquez, del K+Lab de Fundación Karisma, Nathaly Espitia, Natalia Santa, César Torres, Stephanie López y María Juliana Soto, del Colectivo Noís Radio, Víctor Mazón Gardoqui, artista sonoro e investigador electromagnético, y Rodrigo Bastidas, editor e investigador de ciencia ficción latinoamericana.

---

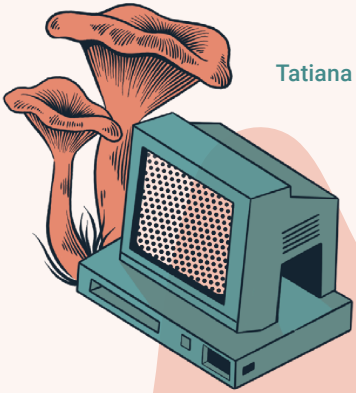
1 Abya Yala es el nombre más antiguo, hasta ahora conocido, para nombrar al territorio americano. En esta guía lo utilizaremos para hacer referencia al conglomerado de Mesoamérica y América del Sur. Para más información, consultar el glosario al final de la guía.

2 https://www.parqueexplora.org/comunicacion-mas-alla-de-internet

A lo largo de seis sesiones nos volcamos a reflexionar sobre las maneras en las que las tecnologías afectan las formas en las que nos comunicamos, y en los impactos que tienen tanto a nivel individual como colectivo. Pensamos en cómo el dominio del fuego nos reunió alrededor de la hoguera para compartir historias y construir nuestra memoria oral. En cómo el humo y las sensaciones acústicas abrieron la posibilidad de transmitir mensajes a la distancia y, así, ampliar el sentido de comunidad. Recordamos cómo las cartas y los diarios personales llevaban algo nuestro entre sus páginas, cómo el telégrafo nos introdujo a la noción de inmediatez y, más tarde, las maneras en las que la mediación de las máquinas nos transmitió la sensación de cercanía. Hoy, internet nos permite crear un simulacro de realidad. Sesión a sesión, las conversaciones fueron girando alrededor de conceptos con los que jugaremos y nos enredaremos en estas páginas: el más allá y el más acá de internet.

Entendemos que, como cada fragmento de este planeta y de esta galaxia, los contextos son orgánicos. A la vez que se actualizan formas de opresión lo hacen las estrategias de resistencia. Por eso hacemos nuestra la máxima de la documentación: “siempre completa, nunca terminada” y deseamos que este material pueda ser actualizado colectivamente con el paso del tiempo.

Esta guía no hubiese sido posible sin la dedicación de muchas colectivas y personas que han trabajado más allá y más acá de los bloqueos; pero, sobre todo, de quienes han compartido sus conocimientos y experiencias para desarrollar y mantener infraestructuras autónomas de comunicación que nos permiten seguir af rmando otras posibilidades de estar juntas. A todas ellas va dedicada esta guía.



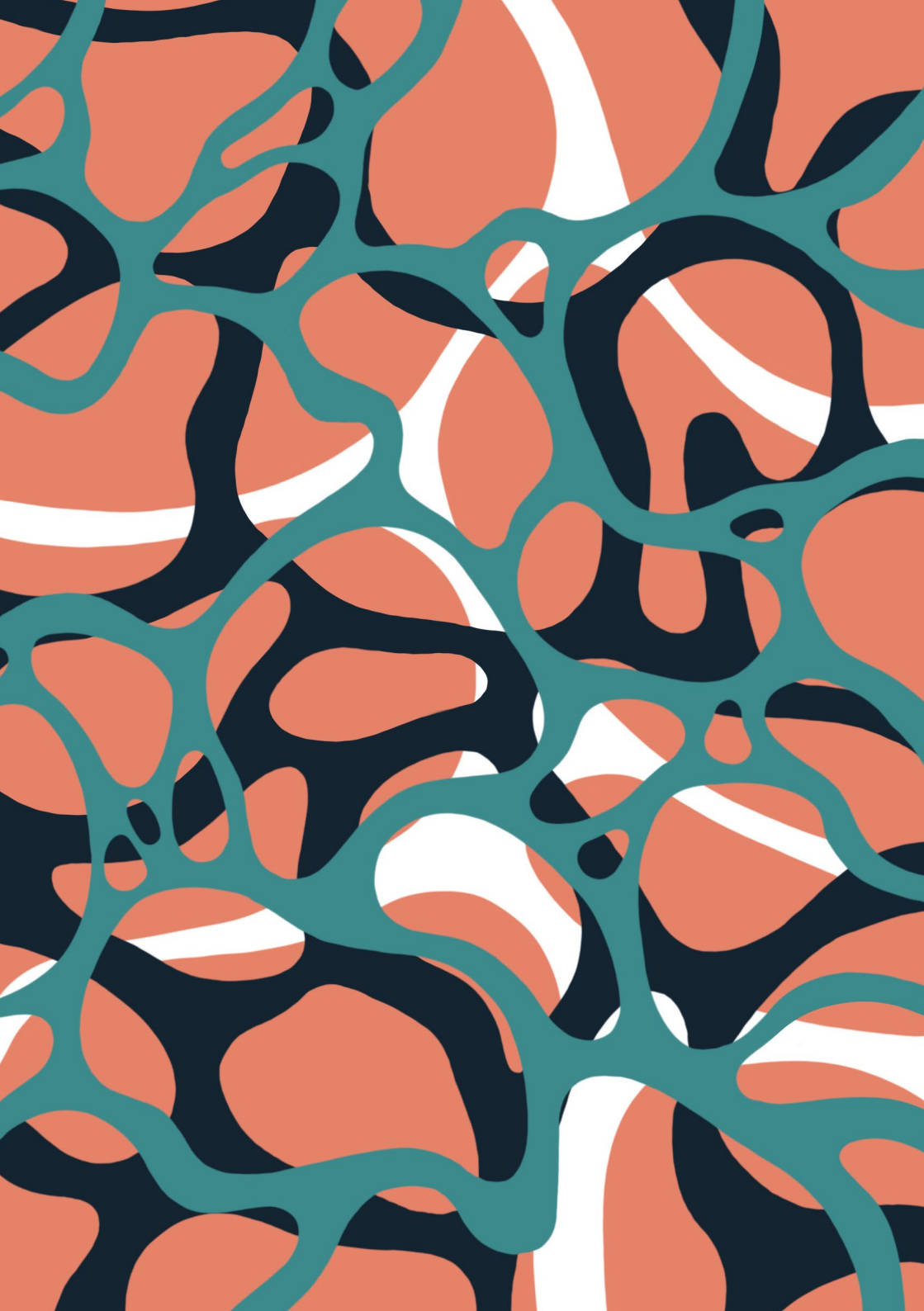
Tatiana Avendaño y Jacobo Nájera

Junio 2022.

Guía para seguir comunicándonos ante bloqueos de internet

Digital Defenders Partnership

Índice



Introducción

El 28 de abril de 2021, Colombia fue testigo de una jornada de movilizaciones masivas brutalmente reprimidas por las fuerzas públicas de seguridad, en abierta alianza con civiles armados. Las protestas se extendieron a lo largo de dos meses en lo que se denominó el “Paro Nacional”. Los días 4 y 5 de mayo, diversas plataformas internacionales que monitorean el estado de internet reportaron la caída del servicio en la ciudad de Cali. En una situación de movilización social, la falta de internet no sólo impedía la comunicación entre pares, también allanaba el terreno para la violación de derechos humanos.

Un bloqueo o apagón de internet puede definirse como "una interrupción intencionada de las comunicaciones electrónicas o de internet, haciéndolas inaccesibles o efectivamente inutilizables, para una población específica o dentro de un lugar concreto, a menudo motivada por un afán de ejercer control sobre el flujo de información".3 Los informes sobre bloqueos de internet nos muestran que la mayoría de las veces ocurren en contextos donde ya se padecen múltiples violaciones de derechos humanos. Allí donde la represión y la violencia se ejercen negando el acceso a derechos básicos, como el servicio de agua y de electricidad, la alimentación, la salud, la vivienda o la educación, es probable que, en algún momento, se experimenten bloqueos de internet. Los contextos de movilización social son propicios a este tipo de control.

Access Now y la coalición #KeepItOn, quienes han documentado entre 2018 y 2020 al menos 564 apagones en todo el mundo, nos recuerdan que incluso cuando los gobierno afirman que imponen bloqueos de internet por motivos de seguridad nacional y orden público,

---

3 Access Now, Keep It On, https://www.accessnow.org/keepiton/

los datos revelan que se trata de una “táctica para restringir los derechos de la ciudadanía a la libertad de expresión e información, y para interferir con el derecho a la libertad de reunión y asociación, particularmente durante eventos como las elecciones, conflictos o manifestaciones masivas”.4

Cada bloqueo de internet implica, por lo tanto, la violación de otros derechos más allá de la libertad de expresión y el acceso a la información. Como la vida digital se ha extendido a todos los ámbitos, junto con la conectividad se limitan también el derecho a la educación, a la salud, al trabajo y al ocio, a la protesta, a la asociación, entre muchos otros derechos y libertades. Poe eso debemos recordar que los derechos digitales también son derechos humanos.

Durante el Paro Nacional quedó en evidencia la centralidad del conocimiento sobre protección digital para garantizar el derecho a la protesta. Recursos como la sección “Asistir a una protesta” del Surveillance Self-Defense (EFF),5 la caja de herramientas de Sin Miedo,6 orientada al contexto colombiano, o la ampliación del plan gratuito de la VPN Tunnel Bear, fueron fundamentales a la hora de acompañar a personas defensoras de derechos humanos y a la ciudadanía que se había volcado a las calles.

Aunque la mayor parte de los apagones de internet se ha documentado en Asia, África y Oriente Medio, este fenómeno también se está extendiendo a Abya Yala. A pesar de ello, el problema de los bloqueos todavía no ha logrado instalarse en la esfera pública. Esto puede explicarse por la escasez de recursos en español para enfrentarse a ellos, o por la falta de análisis político y de datos certeros para caracterizar su

4 Access Now. (2020a). Manual sobre apagones de internet y elecciones. Una guía para observadores electorales, embajadas, activistas y periodistas. https://www.accessnow.org/manual-sobre-apagones-de-internet-y-elecciones/.

5 https://ssd.eff.org/es

6 https://www.sinmiedo.com.co/

naturaleza. Si bien existen iniciativas que facilitan la documentación y el registro de los bloqueos de internet, como la Microguía para el uso de OONI,[7] entendíamos que, en este contexto, no eran suficientes.

Decidimos, por lo tanto, desarrollar un instrumento que abordara los bloqueos de internet de forma integral. La "Guía para seguir comunicándonos ante bloqueos de internet" es una propuesta de vigilancia distribuida de la censura. A su vez, busca aportar herramientas y estrategias para sortear los bloqueos y garantizar que la información siga fluyendo en contextos hostiles. Además de pensarla como parte de una estrategia en la búsqueda de justicia, la motivación principal de esta guía es proponer un ejercicio de memoria, que evite la normalización de esta clase de abusos en nuestro territorio.

La presente guía está organizada en tres grandes partes. Cada una de ellas tiene sentido en relación a las otras dos, de modo que entre todas contemos con los elementos necesarios para comenzar a visibilizar y a enfrentar colectivamente los bloqueos.

La primera parte se centra en explicar cómo funciona internet y cuáles son los tipos de bloqueos o limitaciones en el acceso a los que podemos enfrentarnos. En esta sección nos dedicamos a mostrar la materialidad de internet como un tejido compuesto por una capa lógica y una capa física. De esta manera, podremos identificar los diferentes tipos de bloqueo y cómo operan. También presentaremos en esta parte una serie de elementos que contribuyen a al análisis y a la investigación sobre el tema. Por un lado, una cronología de los principales bloqueos y cortes de internet en la región, documentados en los últimos años. Y, por el otro, un mapeo de los actores involucrados en los bloqueos de internet, sus capacidades y motivaciones.

La segunda parte está dedicada a la documentación de los bloqueos y las limitaciones en el acceso a internet. Este ejercicio no sólo es el primer paso en la búsqueda de justicia en casos de abuso, sino un aporte fundamental para reconocer

7 https://web.karisma.org.co/micro-guia-para-el-uso-de-ooni/

las maneras en las que se ejerce el poder sobre la población y se profundiza el terror. En esta parte reflexionaremos sobre la importancia de documentar y nos detendremos en sus principales etapas: medición, registro, análisis y reporte. Presentaremos, a su vez, distintas herramientas de medición de los bloqueos y nos detendremos en el conjunto de herramientas desarrollada por el Observatorio Abierto de Interferencias de la Red *(Open Observatory of Network Interference – OONI)* y sus diferentes utilidades.

La tercera parte se enfoca en las estrategias, prácticas, medios y herramientas para seguir comunicándonos más allá de los bloqueos. Otras redes sociales y servicios que, con su comunicación distribuida, desafían a la concentración de las grandes tecnológicas. Redes de proyectos no comerciales, libres y/o abiertos comprometidos con el anonimato y la privacidad, en oposición al rastreo, el control y la comercialización de nuestros datos; herramientas que crean túneles y puentes para eludir la censura; e infraestructuras autónomas de comunicación que piden ser descubiertas y sostenidas.

Por último, hemos incluido un glosario de términos relacionados con los bloqueos de internet para facilitar la lectura de estas páginas. Creemos firmemente en que divulgar el conocimiento técnico es una apuesta por liberarlo, y que es urgente volver a enmarcar los debates sobre las telecomunicaciones en el campo de los derechos.

El pensamiento mítico que envuelve a las tecnologías digitales nos impide muchas veces reconocer que como especie hemos desarrollado y utilizado mil maneras de comunicarnos. Pensemos en los khipu, por ejemplo, un complejo sistema inca de registro y memoria que, al día de hoy, no ha sido descifrado a ciencia cierta.[8] Las tecnologías ancestrales vienen desde otras épocas para cuestionar la racionalidad occidental y para recordarnos que, más allá de la represión y la violencia, hay infinitas formas de permanecer juntas y construir entre todas mejores condiciones para vivir en esta Tierra. Esperamos que esta guía sea una pequeña contribución en ese sentido.

---

8 Para aprender más sobre los khipu visitar Proyecto Khipu: https://proyectokhipu.wordpress.com/

1. Cómo funciona internet y qué tipo de bloqueos podemos enfrentar

Internet es una compleja red de comunicación digital desplegada a nivel global (aunque concentrada en el norte). El primer paso para usar internet de manera estratégica a favor de las luchas por la vida y la dignidad, es entender cómo funciona. Esto no significa adentrarnos por años en el mundo de las telecomunicaciones, sino incorporar una mirada general sobre su materialidad: desde la infraestructura hasta los protocolos que hacen la comunicación posible. Aunque tendamos a pensar que internet es equivalente a la web, esta es apenas uno de sus tantos servicios. El correo electrónico, las redes P2P, el IRC, el protocolo VoIP, las VPN o el FTP, por ejemplo, son también parte de internet.[9] Cuando hablamos de internet a secas nos referimos, por lo tanto, a muchas cosas a la vez.

En primer lugar, aludimos a un conjunto de acuerdos o protocolos entre Estados, organismos internacionales, instituciones públicas, desarrolladoras de *software,* proveedoras de telecomunicaciones y fabricantes de *hardware*, que permiten utilizar una infraestructura de comunicación compuesta por servidores, cables de fibra óptica y de cobre, satélites y el propio espectro radioeléctrico, entre otros. Uno de los principales acuerdos es la posibilidad de realizar el intercambio de paquetes de datos desde y hacia cualquier destino y origen, sin discriminación alguna.

En segundo lugar, es importante comprender que internet no es algo inmaterial, ocurre en los límites del universo conocido. Es decir, se trata de una red de computadoras que, para comunicarse una con otra, requiere de dos infraestructuras: la capa lógica y la capa física. Gracias al entretejido de estas dos capas, podemos intercambiar datos que son presentados en nuestros dispositivos.

---

9 Si no conoces qué significan todas estas siglas consulta el glosario al final de la guía.

CAPA	DESCRIPCIÓN	COMPOSICIÓN
Física	Es el conjunto de hardware necesario para intercambiar datos a nivel global, entre los que se incluyen servidores, routers y los medios físicos para sus conexiones.	Fibra óptica Cables de cobre Espectro radioeléctrico Servidores Routers Modems Antenas
Lógica	Es el entramado inmaterial de código y protocolos que permite la transmisión de datos a través del hardware.	Software Protocolos Políticas y acuerdos Estándares Configuraciones

Veamos cómo funciona la infraestructura de internet con un ejemplo. Cuando queremos entrar a una página web, lo primero que hacemos es teclear en la computadora la dirección en el navegador. Esta dirección se convierte, gracias a los protocolos (capa lógica), en bits que viajan por cables de cobre, routers, antenas y más cables (capa física). Si bien la capa física posibilita materialmente la transmisión de bits, son los protocolos los que conocen la ruta, los que llevan el pedido y tienen (o piden) los permisos para entrar y salir de las computadoras y los *routers*. Cuando le "damos enter" a la dirección web, lo que estamos enviando es una serie de peticiones a un servidor DNS que traduce la URL en una dirección IP, que luego identifica a un servidor web y, dentro de él, a una página en particular. Esta petición nos devuelve, en este caso, una página web (texto, imágenes, video, etc.) que se nos presenta en la pantalla. En dicho proceso ocurren cientos de interacciones en milésimas de segundos. ¿Cómo estas peticiones y respuestas pueden ir y volver tan rápido? Porque viajan a la velocidad de la luz, a través de impulsos eléctricos.

Estos procesos son tan complejos que muchas veces se usan metáforas. Al conjunto de peticiones web se le llama "navegar", al conjunto de centros de datos que almacenan información se los denomina "nube", o llamamos "apagón" a una serie de medidas orientadas a

restringir el acceso a internet, por ejemplo. Son abstracciones que nos permiten comprender cómo opera un bloqueo, cómo podemos documentarlo y cómo podemos seguir comunicando a pesar de ello. En la siguiente ilustración observamos los flujos de destino- origen-destino que representan el intercambio de paquetes en internet.

Esta introducción nos permitirá caracterizar los tipos de bloqueos que han sido identificados en la región de Abya Yala y, así, entender mejor la influencia de los actores implicados en ellos.

Tipos de bloqueos y limitaciones de acceso

Como hemos visto, cuando hablamos de bloqueo nos referimos, en un sentido amplio, a la interrupción o disrupción intencional y dirigida de internet o de las comunicaciones electrónicas con el fin de ejercer control sobre el flujo de información. Los bloqueos o limitaciones en el acceso a internet pueden ser generalizados, con el objetivo de impedir el acceso en un territorio, como fue el caso de Cali, o dirigidos, buscando restringir el acceso a una web o servicio especifico.

Durante los apagones generalizados, el acceso a internet u otros servicios de telecomunicaciones se ven interrumpidos. Sin embargo, dada la complejidad de la red, este tipo de intervenciones tienen un alcance limitado en el tiempo (los opresores también necesitan internet para sus propias tareas) y el espacio (la infinidad de actores involucrados en el funcionamiento de internet solo permite ejercer control sobre un sector específico de la red).

Un apagón o bloqueo de internet también puede tomar la forma de “estrangulamiento”, cuando las velocidades de internet se reducen intencionalmente con el objetivo de dificultar o, incluso, imposibilitar el intercambio de información. Una de las tácticas comúnmente utilizadas por los gobiernos es ralentizar las velocidades de internet móvil de los niveles 4G y 3G a 2G.

Los obstáculos en el acceso a internet pueden interponerse en la capa lógica o en la física. En la primera, se concretan por medio de configuraciones que modifican el comportamiento habitual del tráfico de datos. En la segunda, se favorecen obstáculos físicos como corte del suministro eléctrico, saturación de los medios de transmisión, interferencias inducidas –por ejemplo, por *radio jamming*–[10] o daño físico de cables y/o antenas.

En esta sección nos ocuparemos específicamente de los bloqueos que ocurren por cambios o afectaciones en la capa lógica. Una de las prácticas en las que pueden incurrir los proveedores de servicio de internet es el bloqueo del acceso total o parcial a servicios. Esto puede ser resultado de las políticas internas de las empresas o por solicitudes gubernamentales, por ejemplo, para impedir el flujo de comunicaciones o el acceso a ciertos sitios web. A continuación describimos las técnicas más frecuentes de bloqueo en la capa lógica, los cuales pueden darse a nivel de DNS, a nivel de ruta o dirección IP o a nivel de paquetes.

A nivel de DNS

Ocurre cuando un proveedor de servicios de internet (ISP, por sus siglas en inglés) modifica, rechaza o bloquea las peticiones de DNS de sus usuarias y con esto impide el acceso a una página web. El DNS es el Sistema de Nombres de Dominio que vincula un nombre inteligible y fácil de recordar (lo que comúnmente llamamos dominio o, simplemente, "una dirección") con una dirección IP, un número compuesto que cumple la función de identificar una interfaz en la red y de direccionar su ubicación. Un ataque a nivel de DNS impide esta vinculación y, por lo tanto, la petición a un dominio no se puede resolver porque no se encuentra el servidor. Este tipo de bloqueos tienen el objetivo de limitar el acceso a una web determinada.

---

10 Ver glosario.


CAPA FÍSICA
CAPA LÓGICA

Puedes aprender más sobre cómo funcionan los DNS con el comic DNSimple.[11] Si quieres conocer ejemplos de bloqueo por DNS puedes seguir los casos de Women on Waves[12] y Women on Web,[13] dos proyectos sobre el derecho al aborto que fueron censurados. En sendas documentaciones puedes encontrar las estrategias usadas por las administradoras de la web para sortear los bloqueos. Otros ejemplos de este tipo en la región son los documentados por el Instituto de Prensa y Sociedad de Venezuela.[14]

A nivel ruta o dirección IP

Este tipo de ataques tienen lugar cuando un proveedor de servicios de internet bloquea el acceso a una o varias direcciones IP. De esta manera, los diferentes servicios que hay en los servidores de destino se vuelven inaccesibles. A diferencia del ataque de nivel DNS, aquí no se puede acceder al servidor aún conociendo la dirección IP a la que se busca acceder. Para conocer de cerca un ejemplo de bloqueo a nivel de ruta o IP, puedes seguir el caso del bloqueo a la red Tor en México.[15]

A nivel de paquetes

Internet funciona bajo el principio de neutralidad de la red, es decir, que ningún paquete de datos puede priorizarse por sobre otro. Cuando un proveedor de servicios de internet clasifica el tráfico de sus usuarias por medio de la técnica de inspección profunda de paquetes (*Deep Packet Inspection*, DPI) puede bloquear determinados sitios. Esta técnica también puede utilizarse para establecer políticas enfocadas a reducir y aumentar la velocidad de sitios específicos (por ejemplo, Movistar podría querer que en su internet su plataforma

---

11 https://howdns.works/es/

12 https://medium.com/codingrights/on-the-blocking-of-pro-choice-websites-women-on-waves-and-women-on-web-505ed6f17b63

13 https://blog.magma.lavafeld.org/es/post/women-on-web-blocking/

14 https://ipysvenezuela.org/navegarconlibertad/tag/bloqueos-dns/

15 https://es.globalvoices.org/2020/05/28/en-mexico-el-mas-grande-operador-de-telecomunicaciones-bloquea-la-internet-segura/

de contenidos se vea mejor que la de sus competidores), o ralentizar la conexión en general. Aunque no identificamos casos con estas características en la región, resulta importante incluirlo por ser un tipo de limitación de acceso que tiene origen en la capa lógica.

Si bien no se trata de técnicas de bloqueo de internet en sí, también podemos encontrar una serie de ataques informáticos que son utilizados para censurar y controlar a activistas de derechos humanos. Este tipo de ataques se hace explotando vulnerabilidades, como fallos del *software* o de las configuraciones de los servicios, por ejemplo, para saturar las capacidades instaladas o previstas de un servidor. Una de las técnicas más generalizadas son los ataques distribuidos de denegación de servicio (DDoS, por sus siglas en inglés) que consisten en saturar a un servidor con más solicitudes de las que tiene capacidad de responder. La saturación hace que el servicio se caiga y, por lo tanto, se vuelva inaccesible. En nuestra región encontramos casos con estas características principalmente orientados a medios de comunicación y a organizaciones de derechos humanos.

Estos diferentes niveles de bloqueos descritos pueden manifestarse simultáneamente y en combinación para lograr efectos más duraderos, algo que resulta importante tener presente al momento de documentarlos.


BOQUEO EN LA
CAPA **LÓGICA**
BLOQUEO EN LA
CAPA **FÍSICA**

Antecedentes de bloqueos de internet en Abya Yala

Los antecedentes regionales documentados que aquí compartimos dan cuenta de bloqueos tanto de redes sociales y de servicios de mensajería instantánea, así como de servicios enfocados a la privacidad y el anonimato. También identificamos registros de ataques informáticos contra sitios web de medios de comunicación, que vieron obstaculizado su acceso.

En general, podemos observar que la mayoría de los bloqueos han sido reportados en Mesoamérica y el Caribe, y han ocurrido a nivel de DNS, en contextos de protesta social. Estos bloqueos son el resultado de la colaboración entre agencias de inteligencia y seguridad, gobiernos, proveedoras de telecomunicaciones y, en uno de los casos documentados, una empresa de registro de dominios. En cuanto a su duración, los bloqueos a servicios enfocados en privacidad y anonimato fueron los de mayor duración, manifestándose durante meses, incluso años. Mientras que aquellos dirigidos a redes sociales y servicios de mensajería instantánea fueron más acotados en el tiempo.

Cronología de bloqueos documentados

Esta cronología constituye una aproximación a los bloqueos y cortes internet en el territorio de Abya Yala, documentados en el período comprendido entre los años 2009 y 2021. Entendemos que no es un recorrido exhaustivo ya que la mayoría de incidentes no llegan a registrarse. No obstante, es evidente que esta problemática se ha ido acrecentando y agudizando en toda la región, como un claro obstáculo al ejercicio de la libertad de expresión y de asociación en contextos de protesta social.

2009

2009. Wordpress se reportó bloqueado en Guatemala. Más información en: https://es.globalvoices.org/2009/07/02/wordpresscom-bloqueado-en-guatemala/.

2012. Con ayuda de Estados Unidos y el proveedor de nombres de dominio GoDaddy, el gobierno mexicano censuró el sitio 1DMX.org. Más información en: https://www.derechosdigitales.org/7028/la-censura-politica-en-internet-es-real-el-caso-de-1dmx-org/.

Agosto a septiembre de 2015. La cooperativa tecnológica de hospedaje seguro Primero de Mayo / May First (México - Estados Unidos) recibió ataques DDoS en su infraestructura a lo largo de tres semanas. Más información en: https://www.jacobo.org/sobrevivir-a-los-ataques-de-denegacion-de-servicio-distribuido/.

25 de noviembre de 2015 al 14 de enero de 2016. Se registraron 43 casos de sitios web que fueron objeto de bloqueo sistemático a nivel de DNS por parte de uno o más proveedores de servicios de internet en el marco de la campaña electoral parlamentaria de Venezuela. Más información en: https://ipysvenezuela.org/navegarconlibertad/tag/bloqueos-dns/.

2016. Los medios mexicanos Másde131, Rompeviento TV y Radio Zapote registraron ataques de denegación de servicio, dos de los cuales culminaron en la pérdida –total o parcial– de su archivo histórico. Más información en: https://www.jacobo.org/botnet-contra-sitios-web-de-medios-independientes-en-mexico y en https://articulo19.org/ataques-ciberneticos-inhabilitan-paginas-de-mas-de-131-y-radio-zapote.

Junio de 2016 a noviembre de 2017. Interferencias y limitaciones en el acceso al sitio web Pernambuco.com desde proveedoras de servicios de internet en Brasil. Más información en: https://lavits.org/wp-content/uploads/2018/04/32-Vasilis-Ververis-Olga-Khrustaleva-e-Eliana-Quiroz.pdf.

2017. El medio de comunicación El Pitazo reportó bloqueos intermitentes a su sitio web por parte de CANTV, Digitel y Movistar en Venezuela. Más información en: https://latamjournalismreview.org/es/articles/sitios-de-noticias-en-venezuela-reportan-ataques-a-sus-servidores-y-bloqueo-de-twitter-y-soundcloud/.

29 de mayo a 10 de junio 2017. El Observatorio Abierto de Interferencias en la Red (OONI) confirmó y reportó el bloqueo de 27 sitios web en Cuba. Más información en: https://ooni.org/posy/cuba-internet-censorship-2017/.

2021

11 de julio de 2021. Bloqueos a los servicios de Signal, Telegram y Whatsapp en el contexto de las protestas del #11J en Cuba. Más información en: https://www.yucabyte.org/2021/07/12/11j-internet-cuba y en https://www.accessnow.org/patria-y-vida-cuba-internet/.

4 y 5 de mayo de 2021. Interrupciones parciales en el servicio de internet en la ciudad de Cali en el contexto del #ParoNacional de Colombia. Más información en: https://web.karisma.org.co/una-mirada-a-la-interrupcion-del-servicio-de-internet-en-cali-durante-paronacional.

12 de octubre de 2019. Interrupciones de acceso móvil a internet por medio de la operadora de telecomunicaciones Claro en Ecuador. Más información en: https://www.cubaperiodistas.cu/index.php/2019/10/lenin-moreno-bloquea-internet-movil-en-ecuador-segun-netbloks.

7 de octubre de 2019. Interrupciones de acceso a redes sociales desde la operadora estatal de telecomunicaciones CNT, en medio de protestas sociales de Ecuador. Más información en: https://www.apc.org/es/news/disrupciones-de-internet-en-ecuador-como-ocurrieron-y-como-eludirlas y en https://www.apc.org/es/pubs/derechos-digitales-en-el-contexto-de-las-protestas-y-movilizacion-social-en-ecuador-en-octubre.

17 de mayo a agosto de 2017. El dominio de Riseup.net se registró con bloqueo a nivel DNS por la proveedora de telecomunicaciones VTR Banda Ancha de Chile. Más información en: https://lavits.org/wp-content/uploads/2018/04/32-Vasilis-Ververis-Olga-Khrustaleva-e-Eliana-Quiroz.pdf.

29 de mayo a 10 de junio de 2017. El Observatorio Abierto de Interferencias en la Red (OONI) con rmó y reportó el bloqueo a 47 sitios web en Cuba. Más información en: https://ooni.org/post/cuba-internet-censorship-2017/.

Julio de 2018. Interrupciones regionales de internet en medio de protestas de Nicaragua. Más información en: https://netblocks.org/reports/nicaragua-regional-internet-disruptions-amid-protests-gdAmMvA9.

12 al 18 de enero de 2019. Bloqueo de Wikipedia por parte de la operadora de telecomunicaciones CANTV de Venezuela. Más información en: https://ooni.org/post/venezuela-blocking-wikipedia-and-social-media-2019.

Actores involucrados en los bloqueos en Abya Yala

Como hemos visto, internet es una red compleja e interconectada en la que intervienen distintos actores. Ante un ataque, resulta imprescindible establecer el mapa de actores involucrados para entender sus capacidades y motivaciones.

ACTOR	CAPACIDAD	MOTIVACIONES
Administradores de redes locales (por ejemplo de universidades, espacios de trabajo, entre otros).	Gestionar el tráfico de las redes que operan y administran.	Mantener buenas relaciones con las autoridades nacionales y otros grupos de poder con intereses económicos en común.
Proveedoras de servicios de internet (ISP).	Gestionar y controlar el tráfico de las redes que operan y administran.	Mantener buenas relaciones con las autoridades nacionales y otros grupos de poder con intereses económicos en común.
Gobiernos y autoridades públicas.	Dar o retirar los permisos, licencias y/o concesiones a una empresa. Uso o abuso de poderes para limitar derechos en nombre de la estabilidad o la seguridad nacional.	Censurar información. Limitar o impedir el acceso a la información, la circulación y difusión de información y la libertad de expresión. Limitar el derecho a la organización y movilización.
Grandes plataformas tecnológicas.	Ofrecer y gestionar servicios de nube, redes sociales, correo electrónico, etc.	Mantener buenas relaciones con las autoridades nacionales y otros grupos de poder con intereses económicos en común. Moderación de los contenidos (control editorial, algoritmos, defensa copyright), etc.
Crimen organizado (grupos al margen de la ley y mafias, entre otros).	Control político y territorial.	Mantener su poder y control sobre un territorio y sus habitantes.
Trols, machitrols, grupos antiderechos autoorganizados.	Ataques dirigidos a páginas web, generalmente DDoS.	Rechazo a la ampliación de derechos feministas o LGTBIQ+, defensa de privilegios de clase, género, etc.

El mapa de actores es un elemento medular de cualquier análisis de riesgo. No solo ofrecerá elementos para una compresión más exhaustiva del contexto de violencia y las motivaciones de los actores involucrados, sino que permitirá desarrollar estrategias de respuesta con mayor precisión.

---

16 Al cierre de este documento no se encontraron casos documentados que cuenten con la participación de estos grupos. Sin embargo, no podemos omitir su influencia y su conexión con la delincuencia común o cualquiera de los otros actores detallados en esta tabla.

2. Cómo documentar los bloqueos y limitaciones en el acceso a internet

La documentación de los bloqueos y limitaciones en el acceso a internet es una actividad central para conocer la naturaleza y alcance de los ataques. Este registro no debe limitarse a sus aspectos técnicos sino que también deberá incorporar elementos contextuales que permitan un abordaje integral. De esta manera, lograremos construir evidencia sobre sus impactos y efectos a corto, mediano y largo plazo. Estos detalles suelen ser útiles para denunciar públicamente vulneraciones a los derechos humanos, evitar la normalización de los ataques digitales y aportar a la construcción de la memoria de las movilizaciones ciudadanas, que garantice la no repetición de la censura en los mundos por venir.

Por otra parte, la documentación abona al desarrollo de análisis pormenorizados sobre las técnicas y herramientas utilizadas, tanto en las capa lógica como en la capa física, y permite identificar patrones valiosos para la construcción y fortalecimiento de tecnologías anticensura e infraestructuras autónomas de comunicación.

El método más extendido para la documentación técnica de bloqueos y limitaciones en el acceso a internet son las mediciones de red, conocidas también como pruebas de conectividad. Estas pruebas permiten registrar e identificar la existencia de obstáculos entre origen y destino de una transmisión de datos en internet. No obstante, no son un método exhaustivo para abordar el fenómeno de la censura. En esta sección propondremos dimensiones adicionales para beneficiar una mirada situada.

Es importante recordar que si nos encontramos ante a un caso que se ha judicializado, la construcción de la prueba judicial tiene exigencias propias que trascienden la presente documentación. Si este es el caso, recomendamos acercarse a personas especializadas en litigio para que te asesoren en cómo realizar pruebas periciales.

Herramientas para la medición de bloqueos

En la última década han proliferando una serie de proyectos enfocados a desarrollar metodologías y herramientas para la documentación de bloqueos, interferencias, cortes y otras formas de limitaciones en el acceso a internet. Hemos seleccionado y estudiado seis de ellos: Censored Planet, IODA, Netblocks, OONI, Proyecto Magma y RIPE Atlas. Los proyectos son diversos y cuentan con distintos abordajes: mientras algunos están orientados a documentar apagones de internet otros ofrecen metodologías para documentar ataques a una web específica.

A continuación compartimos una sistematización de dichos proyectos. Cada uno cuenta con nombre y enlace a su página web, una descripción de su propuesta, si están orientados a registrar bloqueos o cortes e interrupciones y, por último, si cuentan con una metodología abierta que permita ser replicada en otros contextos. No incluimos Proyecto Magma[17] porque, a pesar de presentar una metodología para investigar iniciativas de control sobre la información y mediciones de las redes, no está del todo actualizada y presenta orientación muy técnica.

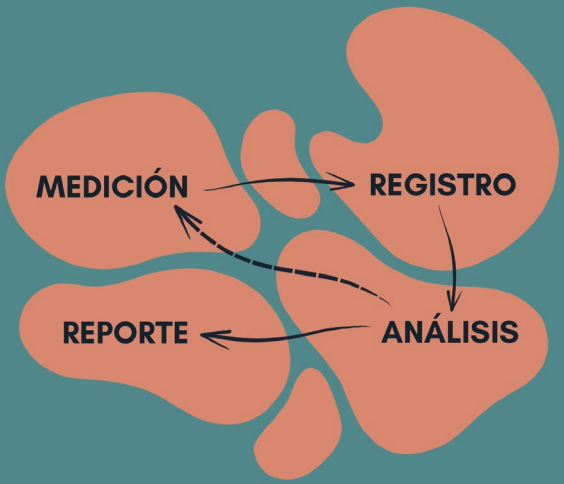
NOMBRE	DESCRIPCIÓN	BLOQUEOS	CORTES O INTERRUPCIONES	METODOLOGÍA ABIERTA Y REPRODUCIBLE
Censored Planet https://censoredplanet.org/	Censored Planet es una plataforma de medición de censura que recopila datos utilizando múltiples técnicas de medición remota en más de 200 países.	SI	NO	SI
IODA (Detección y Análisis de Cortes de Internet) https://ioda.caida.org/	IODA es una plataforma que monitorea la red para identificar cortes.	NO	SI	semiabierta
Netblocks https://netblocks.org	Netblocks cuenta con una plataforma de monitoreo global de la internet para identificar cortes y bloqueos.	SI	SI	NO
OONI (Observatorio Abierto de Interferencias en la Red) https://ooni.org/	OONI tiene como objetivo la observación de la censura en la red.	SI	NO	SI
RIPE Atlas https://atlas.ripe.net/	Plataforma de medición de internet global, abierta y distribuida, conformada por miles de dispositivos de medición alrededor del mundo.	SI	NO	SI

17 https://magma.lavafeld.org/

A los efectos de la presente guía, optamos por el conjunto de herramientas de OONI para recopilar evidencia e incorporarla al proceso de documentación. Esta elección se debe, en primer lugar, a que es una herramienta libre y de código abierto con documentación sólida y actualizada. Y, en segundo lugar, a la gran cantidad de personas que la utilizan, lo cual facilita el acceso a una comunidad internacional con quien compartir dudas y preguntas. Ofreceremos más detalles de las herramientas de OONI en el próximo apartado.

Etapas de la documentación

Para ordenar la documentación de un bloqueo, interferencia o limitaciones en el acceso a internet, proponemos cuatro etapas: medición, registro, análisis, y reporte. Cada una de ellas ofrece sus particularidades, las cuales, en conjunto, brindarán una mirada integral sobre el incidente. Esta propuesta puede ser adaptada para responder al contexto, experiencia, capacidades y necesidades de cada organización o colectiva.



Primera etapa: medición

La primera etapa consiste en recabar evidencia del bloqueo y registrarlo. Para ello se pueden utilizar una amplia variedad de herramientas, tanto técnicas como documentales. Es decir, podemos incorporar a este registro las mediciones sobre el bloqueo o las limitaciones en el acceso a internet, pero también los impactos percibidos por las personas y sus comunidades.

Entre las herramientas que ofrece el Observatorio Abierto de Interferencias en la Red, OONI Probe es la que permite medir bloqueos de sitios web, bloqueos de aplicaciones de mensajería instantánea (Facebook Messenger, Signal, Telegram, Whatsapp), bloqueos de herramientas de elusión de la censura (Psiphon, TOR), reconocimiento de sistemas de censura y/o vigilancia, y la velocidad y rendimiento de una conexión de internet específica.

Antes de comenzar con cualquier tipo de medición, has una evaluación de riesgos, teniendo en cuenta que:

- los actores con capacidad de monitoreo del tráfico de redes –proveedores de servicios de internet, gobiernos, administradores de red, etc.– pueden identificar el uso de herramientas como OONI Probe;
- entre los datos que pueden ser recolectados al momento de realizar mediciones, se encuentran datos sensibles como el país desde donde se realizan las pruebas, el nombre de la empresa proveedora de la conexión y, en algunos casos, la dirección IP desde donde se realiza la medición;
- una persona activista de alto perfil, que ya está bajo una fuerte vigilancia, por ejemplo, podría atraer más atención al realizar mediciones y/o registros con esta herramienta; y
- algunas herramientas de registro, como es el caso de OONI Probe, publican los resultados de las mediciones en su web para ponerlos a disposición pública.

OONI Probe puede usarse en el teléfono celular (disponible para Android en PlayStore y F-Droid, y para iOS en AppStore) o desde su versión de escritorio (disponible para Windows, GNU/Linux y MacOs). La interfaz es muy sencilla: verás un botón de "Ejecutar" para iniciar una prueba general de conectividad, y luego botones específicos para cada una de las pruebas disponibles. La prueba general revisa una selección predeterminada de sitios web incluidos en las listas de prueba de Citizen Lab.[18] En la prueba específica de bloqueos web puedes añadir sitios web concretos que deseas evaluar, por ejemplo, el de tu organización.

18 Los listados de sitios web de prueba pueden consultarse en https://github.com/citizenlab/test-lists/tree/master/lists.

Si vas a monitorear bloqueos o limitaciones en el acceso a internet con OONI, te recomendamos correr la aplicación desde distintas conexiones a internet y distintos proveedores. También es una buena práctica hacer las pruebas varias veces, en distintos días y horarios, para tener un registro sostenido en el tiempo y así evaluar las variaciones.

Luego de que hayas corrido la prueba se mostrará un informe con los resultados y, si presionas sobre cada uno de ellos, tendrás acceso a sus detalles. Por ejemplo, en los resultados del análisis de sitios web verás las URL de las páginas web bloqueadas. Y, si presionas en cada una de ellas, podrás acceder a información detallada sobre el bloqueo de esa web en particular. También verás un enlace "Ver registro", a través del cuál accederás al *log* de la prueba. Como veremos más adelante, esta información puede volcarse en una matriz.

Todos los resultados de las pruebas se suben automáticamente al repositorio de OONI,[19] el cual puedes consultar libremente para recopilar otra evidencia que refuerce tu documentación. Gracias a su búsqueda avanzada, se pueden obtener resultados filtrados por país, por período de tiempo, por tipo de prueba, por dominio o por resultado. Así, por ejemplo, podrías pedir todos los sitios web bloqueados en los últimos tres días. Esta información también puede utilizarse en la elaboración de reportes de bloqueos de internet a nivel nacional.

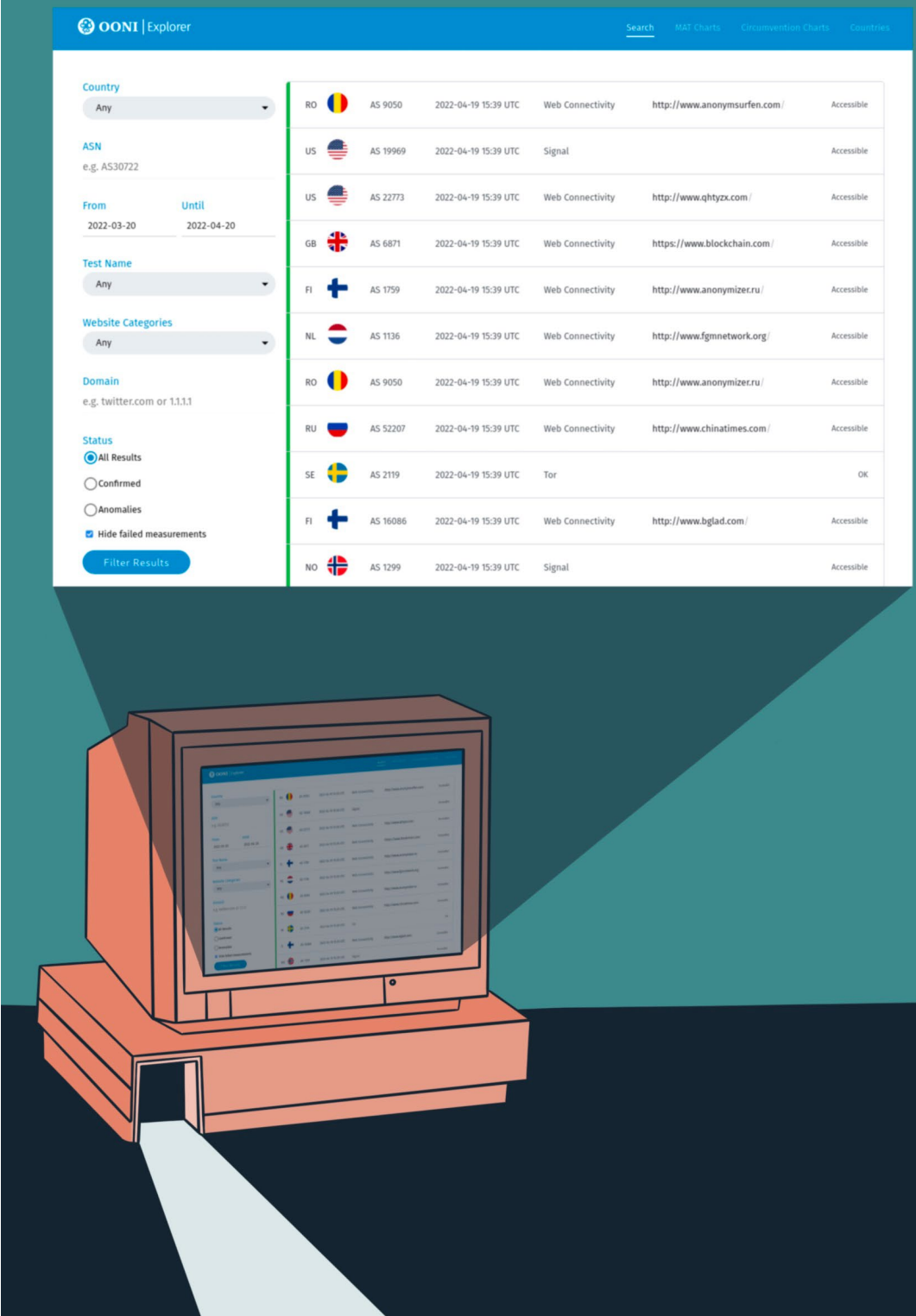
Segunda etapa: registro

Esta segunda etapa está orientada a llevar un registro detallado de los bloqueos o limitaciones en el acceso a internet que medimos en la etapa anterior. El objetivo del registro consiste no sólo en dejar asentadas las mediciones sino aportar elementos a la posterior etapa de análisis. Cuanto más detallado y sistemático sea el registro, estaremos en una mejor posición para respaldar una denuncia o una campaña pública.

Independientemente de las herramientas que utilicemos –en esta guía

---

19 Los datos pueden consultarse libremente en https://explorer.ooni.org/.


OONI | Explorer
Search
MAT Charts
Circumvention Charts
Countries
Country
Any
ASN
e.g. AS30722
From
2022-03-20
Until
2022-04-20
Test Name
Any
Website Categories
Any
Domain
e.g. twitter.com or 1.1.1.1
Status
All Results
Confirmed
Anomalies
Hide failed measurements
Filter Results
RO AS 9050 2022-04-19 15:39 UTC Web Connectivity http://www.anonymsurfen.com/ Accessible
US AS 19969 2022-04-19 15:39 UTC Signal Accessible
US AS 22773 2022-04-19 15:39 UTC Web Connectivity http://www.qhtyzx.com/ Accessible
GB AS 6871 2022-04-19 15:39 UTC Web Connectivity https://www.blockchain.com/ Accessible
FI AS 1759 2022-04-19 15:39 UTC Web Connectivity http://www.anonymizer.ru/ Accessible
NL AS 1136 2022-04-19 15:39 UTC Web Connectivity http://www.fgmnetwork.org/ Accessible
RO AS 9050 2022-04-19 15:39 UTC Web Connectivity http://www.anonymizer.ru/ Accessible
RU AS 52207 2022-04-19 15:39 UTC Web Connectivity http://www.chinatimes.com/ Accessible
SE AS 2119 2022-04-19 15:39 UTC Tor OK
FI AS 16086 2022-04-19 15:39 UTC Web Connectivity http://www.bglad.com/ Accessible
NO AS 1299 2022-04-19 15:39 UTC Signal Accessible

proponemos las de OONI, pero pueden ser otras–, sugerimos llevar a cabo una bitácora o diario que recopile las mediciones. Las bitácoras son documentos con categorías predeterminadas que facilitan el registro de eventos específicos. El registro cronológico de estas mediciones permitirá trazar la evolución el estado de la infraestructura de telecomunicaciones antes, durante y después de un hito, como puede ser un evento de protesta. A continuación proponemos un modelo de bitácora, con algunas de las categorías que pueden ser incorporadas.

Fecha y hora del registro	Marca temporal de la medición o toma de la muestra. No olvidar incluir la hora porque se pueden comparar distintas pruebas realizadas en un mismo día.
Autoría	Quién realizó el registro. Si se evalúa necesario, utilizar seudónimos individuales o colectivos. En caso de riesgo algo, no completar.
Lugar	Desde dónde se hizo la medición: barrio, ciudad, país.
Método y tipo de medición	OONI Probe (sitios web, mensajería, evasión, rendimiento), entrevista, observación, etc.
Proveedor de servicios de Internet	Desde el que se hizo la medición (si es técnica).
Tipo de bloqueo identificado	Detallar si el bloqueo ocurre a nivel de DNS, IP o de paquetes. O si se trata de otro tipo de ataque.
Consecuencias reportadas	Datos confirmados sobre los efectos del bloqueo en nuestra comunidad o región.
Impactos psicosociales	Ante la dificultad de medir los impactos psicosociales de los bloqueos de internet, es importante hacer referencia a los mismos según los deseos y las necesidades individuales y colectivas. Este registro puede nutrirse de testimonios escritos y orales, entrevistas, fotografías, noticias de periódico, etc.
Notas	Es una buena idea registrar las impresiones, sensaciones, las cosas que "nos salen de ojo" o nos llaman la atención. Por más que a primera vista parezcan irrelevantes, pueden ayudar en la etapa de análisis.

Este registro puede ser de carácter individual o colectivo, y llevarse a cabo simultánea o complementariamente. Es decir, varias personas hacen las mismas mediciones en simultáneo –corriendo pruebas sobre los mismos sitios web, en las mismas o distintas horas y a través de distintos proveedores de servicios de internet–. De esta manera, podrán contrastar y complementar los registros para contar con una bitácora sólida. En este sentido, se recomienda que confeccionen listas de los sitios web estratégicos que quieran monitorear: de medios censurados o atacados públicamente, de organizaciones y activistas con mucha visibilidad, espacios de debate público en red, etc.

Cada organización o colectiva podrá plantear la bitácora que quiera y necesite de acuerdo a su contexto y necesidades. Este es un documento vivo y, como tal, debe ajustarse a nuestras necesidades de documentación y no al revés. Cabe recordar que, como volcaremos información sensible, una tarea central será cuidar la seguridad de los archivos: trabajar de manera local o en una nube segura, guardar las copias en un disco cifrado, garantizar el anonimato de quienes registran –por ejemplo, borrando el nombre del dueño del dispositivo y otros metadatos–, hacer respaldos de manera cotidiana, etc.

Tercera etapa: análisis

Una vez que contamos con una bitácora completa – en cada caso se establecerá (y justificará) cuándo finaliza el período de registro– es momento de pasar al análisis. Este ejercicio nos permitirá poner en valor los datos registrados para explicar la situación de bloqueo o limitación en el acceso a internet en un contexto más amplio. Sabemos que los objetivos y necesidades a los que responde un análisis de este tipo serán mejor conocidos por las personas involucradas. No obstante, sugerimos a continuación algunas dimensiones que pueden ser incorporadas y que sirven como una invitación a la reflexión:

- Tipo de bloqueo y alcance: ¿qué herramientas se utilizaron para el bloqueo o limitación en el acceso a internet?, ¿fue generalizado o dirigido?, ¿a nivel nacional o local?, ¿en qué horarios tuvo lugar?.

- Duración: ¿se extendió en el tiempo o se trató de un bloque puntual?, ¿tuvo carácter constante o intermitente?.

- Posibles motivos o intenciones: ¿estuvo relacionado con algún evento específico, como una protesta, anuncio, publicación de una noticia?

- Actores involucrados: ¿quién asumió la responsabilidad del bloqueo?, ¿quién calló?, ¿quién tiene capacidad para bloquear o limitar internet en dicho sentido?, ¿a quiénes favoreció el bloqueo o la limitación?.

- Impactos reportados o conocidos: ¿a quiénes perjudicó el bloqueo y de qué maneras?, ¿qué tipos de impactos hemos identificado?, ¿fueron inmediatos o los veremos a mediano y largo plazo?.

- Antecedentes del contexto tecnopolítico: ¿es la primera vez que ocurría un bloqueo de estas características?, ¿en qué otras circunstancias ocurrieron eventos similares?, ¿ha aumentado su frecuencia?, ¿podemos relacionarlo con algún hecho o proceso político?.

Las metodologías para encarar este tipo de análisis son diversas. Pueden tratar de responderse las preguntas por separado y debatirlas en asamblea, armar grupos de discusión, hacer un mapa conceptual para simplificar la complejidad de actores involucrados o, por qué no, un *collage* colaborativo en el que se expongan las principales conclusiones en un formato visual. No existe la "mejor metodología", existen metodologías apropiadas a cada grupo y contexto.

Cada análisis representa una historia diferente y única, por lo que las preguntas que aquí proponemos no siempre podrán ser despejadas. Es muy probable que, en la mayoría de los casos, surjan incógnitas que requieran volver a iniciar el ciclo de la documentación. Estos agujeros en el análisis también deben visibilizarse, de la misma manera que deben hacerse explícitas las propias limitaciones o márgenes de error de las metodologías, en las que siempre existen diversidad de enfoques y perspectivas.

Cuarta etapa: reporte

Una vez realizado el análisis, es momento de comunicar los hallazgos por medio de un reporte o informe. Las maneras y estrategias para reportar pueden ser muy variadas en recursos visuales y narrativos, de acuerdo a las necesidades de comunicación de cada caso. Una estructura convencional de reporte incluye: un resumen ejecutivo de los hallazgos, el contexto de la investigación, las metodologías de medición y análisis, los principales hallazgos y aprendizajes. Es decir, se trata de exponer narrativamente las principales conclusiones del proceso.

El reporte será un instrumento valioso para identificar patrones comunes con otros eventos de bloqueo o ausencia de internet, denunciar ante instancias de control y regulación nacionales e internacionales, o diseñar estrategias para afrontar los bloqueos, que pueden ir optimizándose con la experiencia y los datos recopilados. También resulta instrumental para que otras organizaciones aliadas visibilicen el bloqueo más allá del espacio geográfico donde ha ocurrido.

En esta instancia, es importante diseñar una buena estrategia de difusión para que todo el esfuerzo que ha supuesto la documentación no haya sido en vano. Una buena estrategia es la creación de una comunidad interesada en el tema que se ofrezca a difundir y mantener actualizada la documentación. Se pueden abrir los datos con los que se trabajó y subirlos a un repositorio público –si es que esto no pone en riesgo a nadie– y trabajar colaborativamente en expandir y profundizar el análisis. El establecimiento de alianzas y participación en redes regionales y globales de monitoreo de la red también puede ayudar a optimizar recursos en ese sentido.

3. Caja de herramientas: tácticas y tecnologías para evadir los bloqueos y la censura

Los bloqueos y limitaciones en el acceso a internet buscan silenciarnos, separarnos y amedrentarnos. En estos escenarios, seguir comunicándonos es un acto de resistencia. Por suerte no existe una única estrategia para hacerlo. Hemos recopilado en esta tercera parte algunas herramientas y prácticas que permiten explorar maneras de seguir intercambiando información y, sobre todo, de poder seguir estando juntas, incluso en tiempos de estallido social. Ninguna de las herramientas y prácticas aquí enumeradas es infalible. Creemos, sin embargo, que apelan a la magia del trabajo colaborativo y, por lo tanto, son una oportunidad y una invitación a incorporarlas.

La caja de herramientas que aquí proponemos nos recuerda que internet es un territorio mucho más extenso que los jardines privados de las redes sociales comerciales.[20] Conoceremos, por lo tanto, herramientas digitales que nos permitirán eludir la censura. Pero también veremos que internet no el único medio para comunicarnos y que podemos mirar más allá para reconocer otras formas de transmitir mensajes. Por último, nos trasladaremos al "más allá del más allá de internet", un espacio de ficción especulativa para crear imaginarios radicales y subversivos en donde existen técnicas y tecnologías aún por crear. Al fin y al cabo, todas las tecnologías conocidas y por conocer deben primero ser imaginadas y deseadas.

Consideraciones de seguridad

Una situación de bloqueo o limitación en el acceso a internet puede generarse por error, y no tener mayores implicaciones, o puede ser parte de un contexto de represión, cuyas consecuencias e impactos deben ser evaluados y mitigados para no ponernos en riesgo. Es por ello que, antes de compartir las alternativas para seguir comunicándonos más allá y más acá de internet, creemos relevante prestar atención a las siguientes consideraciones de seguridad:

---

20 La analogía de los jardines privados es de Margarita Padilla. Para profundizar más en esta idea ver su obra.

- Evalúa las condiciones de seguridad del sector donde se encuentran los medios o recursos que piensas utilizar para difundir tu mensaje y pregúntate si no corres riesgos al dirigirte hacia allí y/u operar en esa zona. Este ejercicio puede ser parte de una evaluación de riesgos más amplia.[21]

- No te olvides antes de participar en una movilización de tener a mano los números de emergencia de tu territorio o localidad como, por ejemplo, bomberos, hospitales y centros de salud, entre otros. Incluye también los contactos de organizaciones que ofrezcan apoyo legal, técnico y/o financiero a personas defensoras de derechos humanos y participantes de movilizaciones.

- Cuida siempre tus dispositivos: mantén actualizado su sistema operativo y libres de virus, desinstala las aplicaciones en desuso y sin mantenimiento, usa contraseñas fuertes de inicio de sesión, no los prestes ni lo dejes sin supervisión. Las buenas prácticas de seguridad te harán menos vulnerable.

- Siempre y cuando las condiciones lo permitan, tómate el tiempo de pensar en cómo transmitir tus mensajes y sus consecuencias. Si pone en riesgo a una o varias personas, reformúlalo o no lo emitas.

- En caso de estar bajo vigilancia, crea un código compartido con tu destinatario o destinatarios transmitir mensajes importantes o asegúrate de usar comunicaciones cifradas.

- Para transportar datos sensibles utiliza discos duros o memorias flash cifradas para que, en caso de ser interceptadas, los archivos no puedan ser leídos. Iníciate en el mundo de la criptografía creando bóvedas cifradas en tus unidades de almacenamiento con Cryptomator.[22]

---

21 Aprende a hacer un análisis de riesgos con el fanzine Derechos humanos y seguridad digital de Codeando México: https://repository.anarchaserver.org/action.php?id=1534&part=e&download.

22 https://cryptomator.org/

Alternativas “más acá” de internet

Hemos sintetizado la información para compartir algunas formas de seguir comunicándonos “más acá” de internet, creando túneles y conectándonos a redes que nos permiten eludir la censura. Si bien identificar a qué tipo de bloqueo te enfrentas permite diseñar estrategias más precisas a la hora de mitigar el ataque, puedes probar estas alternativas aún sin tener certezas sobre el tipo de bloqueo.

Redes Privadas Virtuales (VPN)

Una red privada virtual (o *Virtual Private Network - VPN*, en inglés) es una conexión segura que permite sortear bloqueos y limitaciones en el acceso a internet. Este servicio anonimiza la ubicación geográfica de la conexión y cifra el tráfico en una suerte de túnel entre nuestro dispositivo y el servidor VPN, a través del cuál salimos posteriormente a internet. Es central, por lo tanto, confiar en quien provee el servicio de VPN porque tendrá acceso a nuestro tráfico de internet: desde el historial de navegación hasta las aplicaciones y servicios que estén corriendo en nuestra computadora o celular.

En ocasiones, las VPN se utilizan para simular que estamos en el lugar físico donde solemos trabajar, por ejemplo, y así acceder a la red local. Otras veces se usan para simular que estamos en otra ubicación y acceder a contenidos que están bloqueados en nuestro país. También es una buena opción para asegurar la conexión cuando usamos redes wi-fi públicas, ya que la capa de cifrado que proporciona la VPN nos protege frente a intrusiones en el tráfico.

No esperes a estar en una situación de bloqueo para usar una VPN. Recomendamos las VPN de Tunnel Bear[23] o Rise Up[24]. Y, si quieres aprender más, puedes escuchar el capítulo “La VPN: un túnel secreto” del *podcast* El Desarmador.[25]

---

23 https://www.tunnelbear.com/.

24 https://riseup.net/es/vpn/.

25 https://eldesarmador.org/15-la-vpn-un-tunel-secreto.html.

Navegador TOR

Tor Browser es un navegador de software libre que proporciona anonimato, privacidad y resistencia a la censura en internet. Esto lo hace conectándose a la red TOR (siglas de *The Onion Router* o "enrutador cebolla", en castellano), una red de computadoras que impide que las peticiones puedan ser rastreadas y vinculadas a quien las hace. Dependiendo del tipo de bloqueo, este navegador también permite eludir la censura.

La red TOR está mantenida por voluntarios y voluntarias de todo el mundo. Si quieres conocer en detalle cómo funciona visita Torifícate.[26] El navegador TOR se encuentra disponible para Windows, GNU/Linux, MacOS y Android.[27]

Servicios cebolla

Los sitios *.onion* o "servicios cebolla" permiten tener un sitio web accesible exclusivamente desde la red TOR. En situaciones de bloqueo o limitaciones en el acceso a internet, estos sitios se mantienen en línea. La privacidad y el anonimato, son otros de sus beneficios.

En el sitio de la comunidad de TOR encontrarás el paso a paso para utilizarlos y configurarlos, además de otros detalles sobre su funcionamiento.28 Plataformas de denuncia ciudadana y de alertadores (whistleblowers), como LatamLeaks y Mexicoleaks, o la Cooperativa Tierra Común, tienen sus sitios .onion.

Sitios web espejo y respaldos

Se entienden por "espejos" las copias exactas del contenido de un servidor en otro (u otros) servidores. Esta es una estrategia de seguridad digital utilizada para protegerse ante la pérdida de información. La diversificación a través de espejos también dificulta la censura y facilita el acceso al sitio web en cuestión en caso de bloqueos o ataques. También

---

26 https://tor.derechosdigitales.org/torificate/p1.2/

27 https://www.torproject.org/es/download/

28 https://community.torproject.org/es/onion-services/

puedes mantener actualizadas las copias de seguridad de tu sitio web para poder subirlas rápidamente a otro servidor en caso de ataque.

Si administras un sitio web, puedes hacer copias de los contenidos desde el FTP, o con scp o rsync, y de la base de datos con mysqldump. También puedes hacer copias locales de cualquier sitio web con el *software* HTTrack (disponible para Windows, GNU/Linux y Android).[29] Aunque técnicamente no es un espejo ni un respaldo, otro servicio útil para guardar una copia en línea de una página web es el proyecto Wayback Machine, de la organización Internet Archive,[30] que permite hacer copias de una web y consultar los respaldos de otras tantas.

Internet por satélite

El servicio de internet satelital es una conexión a internet provista mediante satélites de comunicación. Funciona cuando un ISP envía señales a un satélite en el espacio que las rebota a una antena parabólica en la Tierra, y viceversa. Si bien las conexiones de internet satelital pueden ser una opción ante bloqueos o limitaciones de las conexiones convencionales, e incluso en casos donde la infraestructura de telecomunicaciones no llega a nuestro territorio, ten en cuenta que son fáciles de monitorear y revelan fácilmente tu ubicación.

Alternativas “más allá” de internet

Si en el “más acá” de internet podemos seguir comunicándonos en situaciones de bloqueo o limitación en el acceso a través de herramientas como el navegador TOR y los sitios *.onion,* las VPN o las conexiones de internet satelital, también podemos hacerlo “más allá” de internet. Es decir, volcarnos al entorno *offline,* haciendo uso creativo de herramientas digitales y analógicas que no requieren de conexión a internet para intercambiar información.

---

29 https://www.httrack.com/

30 https://web.archive.org/

En este campo, todo vale: desde las estrategias más sencillas y cercanas, hasta las más complejas. Presentamos a continuación once herramientas para imaginar estrategias de comunicación "más allá" de internet: el boca en boca, Bluetooth, código Morse, dead-drops y burn stations, fanzines, ondas radioeléctricas, paredes que hablan, performances, redes comunitarias, servidores locales autónomos, sneakernet, y teléfonos públicos. Algunas de ellas pueden improvisarse, otras requieren trabajo previo de instalación de infraestructura y construcción de acuerdos de funcionamiento.

Recomendamos no esperar al momento de enfrentar un bloqueo o limitación en el acceso a internet para pensar en alternativas de comunicación. Un proceso colectivo de evaluación de riesgos debe tomar en consideración la dimensión comunicacional y acordar estrategias preventivas que mitiguen el impacto de este tipo de ataques. En situaciones de bloqueo, estas estrategias "más allá" de internet nos permitirán registrar, compartir y resguardar evidencia de represión y violaciones de derechos humanos, transmitir información valiosa en situaciones de censura, alertar sobre amenazas de seguridad, organizar movilizaciones ciudadanas, o difundir mensajes que buscan ser silenciados.

Boca en boca

Nos referimos al famoso chisme, boca-oído, comadreo, rumor, runrun o cotilleo como práctica comunicacional que establece redes fluidas de intercambio de información. Aunque lo demos por sentado, el boca en boca es un medio potente de transmisión de mensajes que no debe ser subestimado a la hora de pensar estrategias para enfrentar situaciones de bloqueo. Como las viejas cadenas de comunicación, donde cada uno sabía de quién recibía la información y a quién debía transmitírsela, sistemas similares pueden plantearse de antemano para estar preparadas ante cualquier eventualidad.

Bluetooth

El Bluetooth es una tecnología de red inalámbrica que utiliza las frecuencias de radiocomunicación para transmitir datos en distancias cortas. El uso más común del Bluetooth es el de conectar dispositivos cercanos. Sin embargo, se han desarrollado

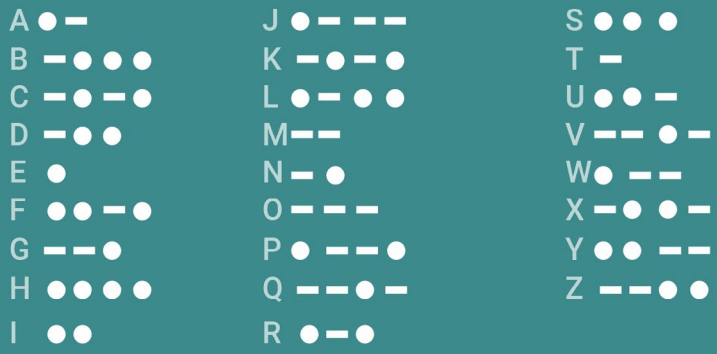
aplicaciones que han superado esta limitación conectando muchos dispositivos cercanos entre sí –por ejemplo, en una aglomeración de personas–, en una suerte de red distribuida que amplía su alcance. De esta manera, es posible transmitir mensajes en contextos de bloqueo del servicio de telecomunicaciones móviles.

Aunque FireChat ganó protagonismo en las protestas de Hong Kong de 2014, no la recomendamos porque no es una herramienta segura. Si quieres usar esta tecnología, mejor prueba las aplicaciones que proveen cifrado de extremo a extremo: Briar, disponible en PlayStore o F-Droid, o Bridgefy, disponible en PlayStore y AppStore.

Código Morse

Este código es un sistema de representación de letras y números mediante señales emitidas de forma intermitente, utilizado originalmente para la navegación, la aviación y distintos tipos de transmisiones por radio. Aprender código Morse nunca estará de más. Puede servirnos para comunicarnos tanto a grandes distancias, a través de la luz o el sonido, o de formas mucho más íntimas y discretas, como el pestañeo de los párpados. Si bien en una primera aproximación puede parecer complejo, con un poco de práctica puede dominarse. Lo importante es que expande la capacidad de enviar mensajes de formas inesperadas o que escapan a los sistemas complejos de monitoreo, control e interferencia.

ALFABETO MORSE



Dead-drops y burn stations

Estas estrategias son similares: se trata de ir a un lugar físico para descargar contenidos en un dispositivo. Los *dead-drops* –cuyo nombre es heredero de las prácticas espías de dejar mensajes en un lugar acordado previamente– son memorias USB ubicadas en lugares públicos para que transeúntes copien información.[31] Las *burn station***s**, o estaciones de quemado –en referencia a las épocas en las que se "quemaban" discos compactos para copiar información– son computadoras disponibles al público a través de las cuales se puede intercambiar información de manera local. Una persona puede dejar sus contenidos y, a la vez, llevarse otros. Tanto los *dead-drops* como las estaciones de quemado pueden ser portátiles e instalarse cerca de los lugares donde están convocadas las manifestaciones, por ejemplo.

Fanzines y otras formas de autopublicación

En caso de necesitar difundir información más extensa, los pasquines, fanzines y, en general, todas las prácticas de autopublicación, son herramientas muy eficaces. Los fanzines son pequeñas revistas de producción independiente que se distribuyen de mano en mano. Estas pequeñas publicaciones caseras son un medio práctico de difusión porque no requieren de más tecnología que una fotocopiadora. Se encuadernan y diagraman de manera muy rudimentaria, utilizando técnicas como el , el dibujo o la escritura a mano alzada. Su distribución también es autogestionada, por lo que los fanzines son efectivos a nivel local. Puedes aprender a hacer fanzines con la guía de la Aventura de aprender.[32]

---

31 https://deaddrops.com/es/

32 http://laaventuradeaprender.intef.es/documents/10184/71399/Guia-LADA_Como-hacer-un-fanzine

Ondas radioeléctricas

Dentro del espectro electromagnético, existe un rango de frecuencias de ondas radioeléctricas que se utiliza para distintas tecnologías de comunicación. Hay que tener en cuenta que la mayoría de usos de este rango de frecuencias necesita de autorización por parte del Estado. Sin embargo, tanto la radiocomunicación como la radiodifusión ofrecen amplias posibilidades.

La radiocomunicación incluye a los *walkie-talkies,* la banda ciudadana –que usa la policía, por ejemplo–, y la radioafición. Este tipo de comunicación requiere de equipos especializados que no son del todo accesibles. Aunque la radiocomunicación está pensadas para la transmisión de sonido también puede transmitir paquetes de datos, incluso cifrados, en las frecuencias de onda corta. Tal es el caso del sistema HERMES que conecta zonas aisladas de la Amazonía.[33]

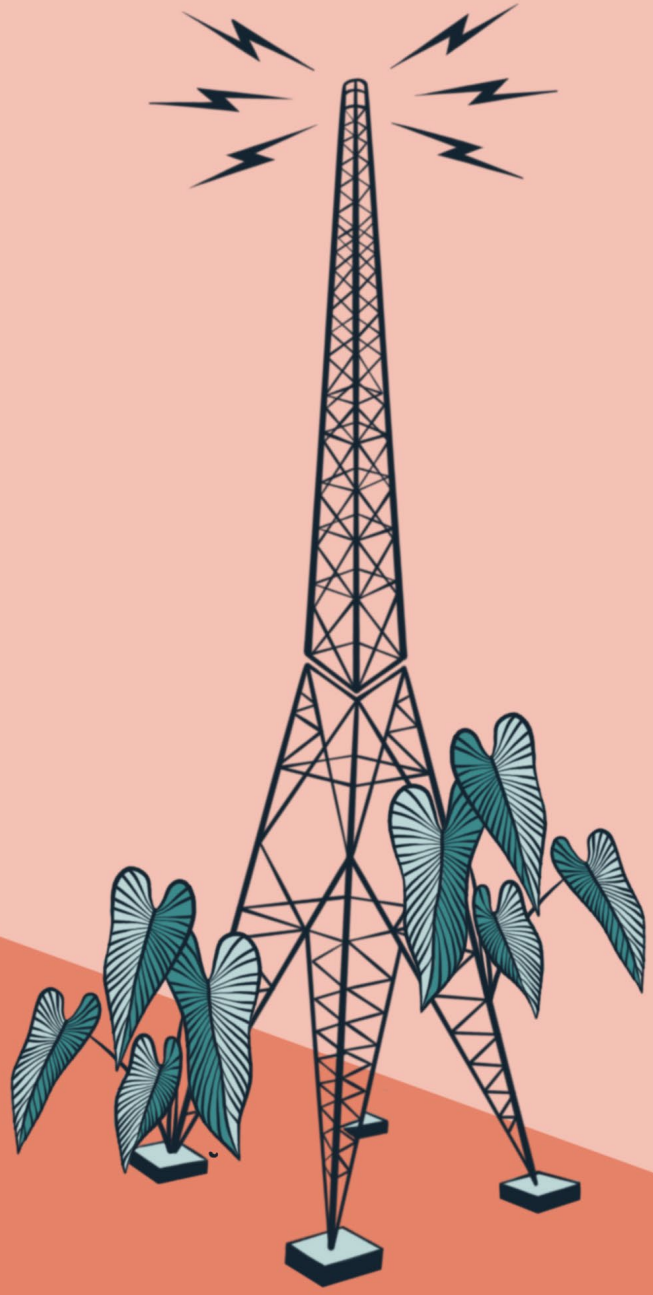
La radiodifusión, por otro lado, es la emisión de señales de radio y televisión. Desde mediados del siglo XX, las radios comunitarias, educativas, populares y alternativas –y las televisoras, aunque en menor medida– han sido actores centrales en la defensa de los derechos humanos y las luchas populares. También las radios abiertas o propaladoras, que salen a la calle para acompañar las protestas.[34] Durante el Paro Nacional de Colombia, por ejemplo, Noís Radio impulsó experiencias de radio en vivo que se amplificaban en los puntos de resistencia.[35]

---

33 Para conocer más sobre HERMES visita: https://es.globalvoices.org/2021/01/20/sistema-de-comunicaciones-digitales-adaptado-a-necesidades-y-contexto-local-de-comunidades-remotas-de-la-amazonia/

34 Puedes conocer las radios comunitarias iberoamericanas que usan software libre en https://mapa.liberaturadio.org/

35 Para conocer más sobre esta experiencia visitar https://noisradio.co/blog/la-radio-resiste-en-las-calles



Paredes que hablan

Los afiches, carteles, calcomanías, esténciles, grafitis, murales, pancartas y pintadas nos dan la oportunidad de compartir rápidamente un mensaje corto y preciso. Estas pueden colocarse en los lugares donde sabemos que se encuentran o transitan las personas con quienes queremos comunicarnos. Pueden tener la magia de la espontaneidad, permitiendo dejar un mensaje urgente en el espacio público. O también preparar de antemano los materiales para, además de ganar tiempo, apostar por la creatividad y la belleza al mensaje.

Otra opción para los entornos de cercanía es instalar carteleras o tablones para intercambiar mensajes con un grupo de confianza o con la ciudadanía en general que, llegado el caso, también pueden estar codificados. Para profundizar sobre el esténcil y otras maneras de hacer hablar a los muros, te recomendamos visitar la página del Instituto Bogotano de Corte.[36]

Performances

Las intervenciones públicas de carácter perfomático y artístico también pueden ser una estrategia para seguir comunicando en casos de bloqueos o limitaciones en el acceso a internet. Intervenir monumentos con mucha visibilidad, proponer bailes y conciertos colectivos, o *flashmobs* organizadas previamente, pueden tener impacto público a la hora de transmitir un mensaje. La *performance* Un violador en tu camino, de las chilenas Las Tesis, por ejemplo, recorrió el mundo y fue replicada en infinidad de ocasiones.[37]

Redes comunitarias libres

Las redes comunitarias son una solución para garantizar la conectividad en lugares a los que no llega la infraestructura de telecomunicaciones. Estas redes, gestionadas por las propias comunidades, funcionan gracias a la instalación de nodos interconectados a través de los cuales se construye una red en forma malla (*mesh*). Estas redes no pueden montarse de la noche a la mañana. Son procesos de

---

36 https://institutobogotanodecorte.home.blog/descargas/

37 https://es.wikipedia.org/wiki/Un_violador_en_tu_camino

largo recorrido en los que la comunidad es acompañada por organizaciones con experiencia en redes y ***software*** libres. Si te interesa este tema, te invitamos a conocer las experiencias de Altermundi,[38] y Red Fusa Libre.[39]

Servidores locales autónomos

De la misma manera que las *burn stations,* es posible montar un servidor local al que se acceda desde de la misma red wi-fi, sin necesidad de internet, y ofrecer todo tipo de servicios: páginas web, chats, herramientas de trabajo colaborativo, repositorios, etc. Este tipo de servidores puede configurarse rápidamente e instalarse en un lugar de mucha concurrencia: un centro cultural, un local que de a una calle transitada, una escuela. Sólo se necesita una computadora, un *router wi-fi* y un poco de práctica.

El fanzine "Cómo montar una servidora feminista con una conexión casera", del espacio hackfeminista la_bekka, te guiará paso a paso en la instalación de un servidor local.[40] También existen proyectos como Pirate Box que permiten armar bibliotecas digitales portátiles con una Raspberry Pi y una batería. Puedes aprender a crear y configurar tu biblioteca virtual portátil con Libre Virus.[41]

Sneakernet: el intercambio de archivos a pie

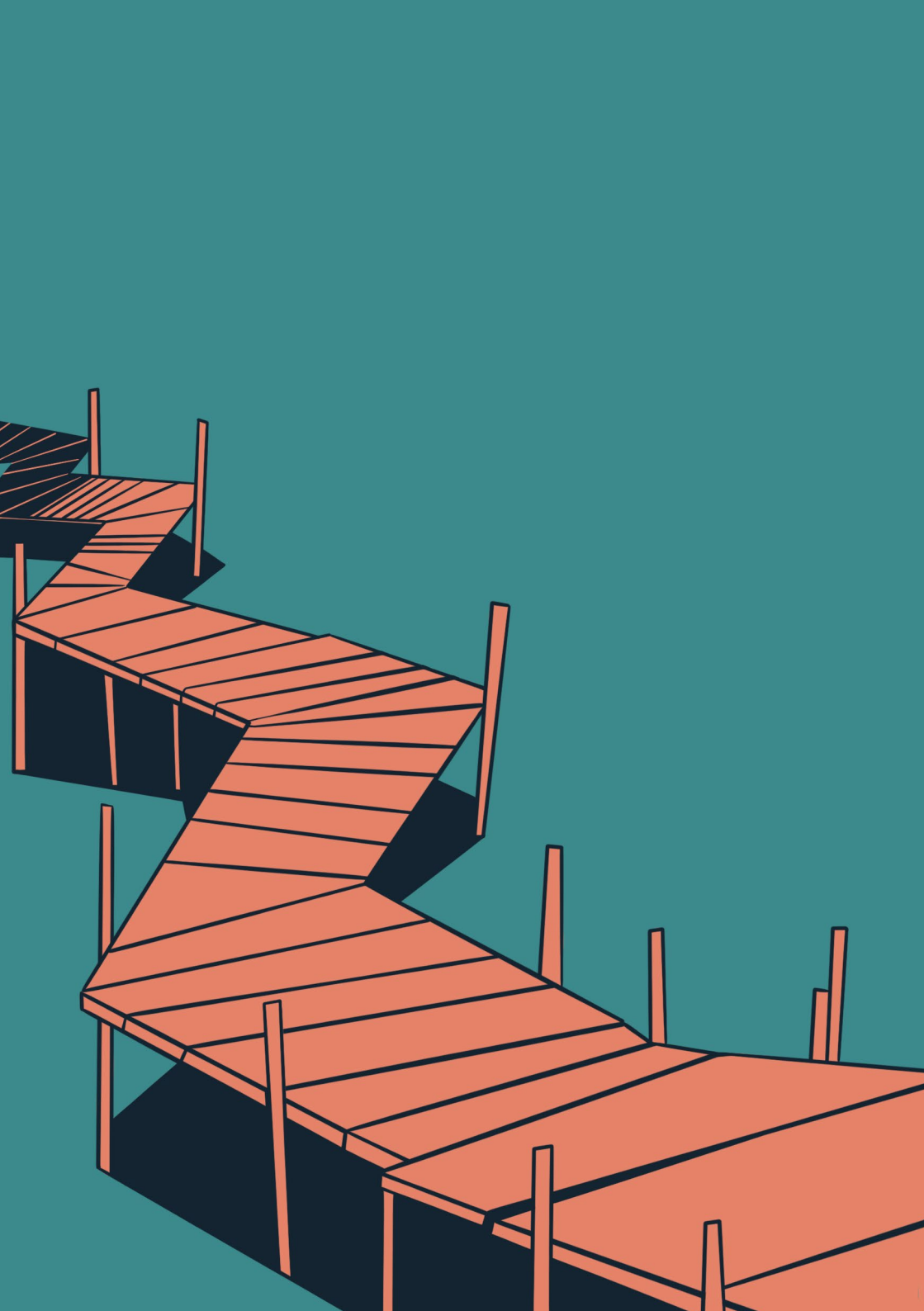
En inglés se utiliza el término *sneakernet* –conformado por las palabras *sneaker* (zapatilla, tenis o calzado deportivo) y *net* (red)– para hacer referencia a las estrategias de transferencia de datos a través del movimiento físico de medios (llevar una unidad de almacenamiento de un lugar a otro) en vez de una red informática. En Cuba, por ejemplo, existen los llamados "paquetes", memorias *flash* (USB o discos) con series, películas, *podcasts* y ***software*** que se distribuyen de mano en mano.

38 https://altermundi.net/

39 https://www.redfusalibre.org/

40 https://labekka.red/servidoras-feministas

41 https://librevirus.cc/docs.html



Teléfonos públicos

Antes de la próxima movilización, identifica en tu territorio los hogares o locales comerciales que tienen cabinas de teléfonos o teléfonos analógicos, es decir, que no dependan de internet, y a los que podrías tener acceso en situaciones de agitación social o cuando tu acceso a internet se vea limitado. Este mapeo puedes dejarlo asentado en un plano que esté disponible en situaciones de bloqueo. También puede incorporar una lista de números de teléfonos relevantes: personas u organizaciones clave que brinden apoyo en situaciones de agitación.

Más allá del más allá de internet: la comunicación post internetística

Imaginemos por un momento que todos los cuerpos son campos electromagnéticos con capacidad de emitir y recibir señales. Bastaría estar en la misma frecuencia para que todos estos cuerpos pudieran comunicarse entre sí.[42] En esta sección proponemos adentrarnos en el mundo de la ficción especulativa y la ciencia ficción como metodologías aliadas para imaginar otros mundos en los que deseamos vivir.

La ficción especulativa reúne a todos los géneros literarios que cambian las reglas, actores, escenarios y conjeturas del mundo tal y como lo conocemos, y exploran los resultados posibles de esa creación. Aunque el término comenzó a utilizarse en el siglo XX, la ficción especulativa incluye obras literarias desde la Grecia Antigua hasta las del siglo XXI. Entre sus géneros encontramos la ciencia ficción, la mitología, la fantasía, la literatura distópica y utópica, el terror, la ucronía, los superhéroes, el ciberpunk, o el steampunk, entre otros. De todos ellos, podemos aprender a despojarnos de la dimensión de "lo posible" para adentrarnos en la de "lo deseable".

La ciencia ficción puede acompañarnos a imaginar el devenir de la comunicación post internetística. Y, a partir de allí, fantasear con otros rumbos. Compartimos a continuación seis obras clásicas de la ciencia ficción que nos presentan diferentes tipos de tecnologías y sistemas de comunicación, y se detienen sobre los impactos que tienen en la comunidades o sociedades en las cuales existen.[43]

---

42 Avendaño, Tatiana (2020, agosto). Lectura performática Cuerpx Antenx. Quito: Arte Actual. https://www.facebook.com/arteactualflacso/videos/750259055546013/

43 Esta selección fue sistematizada a partir de la propuesta que Pilar Sáenz y Rodrigo Bastidas

OBRA	TECNOLOGÍA	SISTEMA DE COMUNICACIÓN	TIPO DE SOCIEDAD
Frankenstein Mary Shelley (1818)	Cartas y diarios: la palabra convertida en materia.	Máquinas de viaje: conocer el mundo y compartir los saberes.	Romanticismo: lo bello y lo sublime, el genio del autor.
Ciclo de Hainish Ursula K. Le Guin (1974 - 1995)	Ansible: simultaneidad en distancias largas.[44]	Interconexión: intercambio simultáneo de imágenes, sonidos y signos pero no de materia.	Ekumen: federación galáctica de mundos habitados por humanos.
Neuromante William Gibson (1984)	Ciberespacio: una alucinación consensuada.	Inteligencias artificiales (IA): la autoconciencia de las máquinas.	Ciborgs: seres cibernéticos y orgánicos.
Steampunk (subgénero sci-fi de los años 80)	Telégrafos postales: conversión del lenguaje.	Galvanismo: la aparición de la electricidad.	Sociedad victoriana: el descubrimiento de las maravillas.
Steampunk (subgénero sci-fi de los años 80)	Telégrafos postales: conversión del lenguaje.	Galvanismo: la aparición de la electricidad.	Sociedad victoriana: el descubrimiento de las maravillas.
Plop Rafael Pinedo (2002)	Narración: unir imágenes en una historia temporal.	Palabra: la palabra es la gran tecnología humana.	Neo-primitivista: la muerte de la cultura, el regreso al inicio.
Mad Max 4: Fury Road George Miller (director) (2015)	Naturaleza: conocer y modificar el entorno.	Símbolos e indicios: tecnología de la metáfora, desplazamiento simbólico.	Lo tribal: rasgos en común, comunidad y tribu.

Estas obras pueden servir como una primera pasarela para inspirar e idear, tanto en soledad como en colectivo, otras tecnologías y sistemas de comunicación que trasciendan a los conocidos. Incluso, a partir de ellas, podemos prototipar las tecnologías que necesitamos para la sociedad que queremos construir: tecnologías autónomas, descentralizadas, colectivas, sostenibles energéticamente o, por qué no, de muchos colores y que huelan a café recién hecho. Para profundizar en esta posibilidad proponemos el siguiente ejercicio.

---

presentaron en el laboratorio virtual “Más allá de internet: otras redes para comunicarnos”.

44 El ansible es un dispositivo de comunicación inventado por la escritoria Ursula K. Le Guin, y utilizado en muchas de sus novelas, cuya característica principal es que es más veloz que la luz, alcanzando la instantaneidad absoluta y por ende muy útil para enviar mensajes interestelares o intergalácticos. Otros autores posteriormente han incorporado el ansible en sus obras.

Ficción especulativa para seguir comunicándonos

Para imaginar una nueva forma de comunicación puedes partir de un escenario hipotético o de una situación real que quieras afrontar con nuevas herramientas o herramientas que ya tienes a disposición pero que utilizarías de otro modo. Empieza por identificar:

- ¿Quiénes desean comunicarse? ¿En qué sentidos? ¿De manera sincrónica o diacrónica? ¿En la misma dimensión o interdimensionalmente?
- ¿Qué mensajes quieren transmitir? ¿Que materialidad tiene el mensaje? ¿Por qué medio se conduce? ¿Qué tipo de receptores y emisores se necesitan? ¿Qué código utiliza?
- ¿Por cuánto tiempo se debe mantener esa comunicación? ¿Es permanente o intermitente?

No hace falta que respondas a todas las preguntas, ni que lo hagas con un gran relato, puedes escoger la extensión con la que te sientas más cómoda. Aprovecha la oportunidad para poner en palabras o imágenes cualquier idea que surja en tu mente. No descartes *a priori* ninguna imagen.

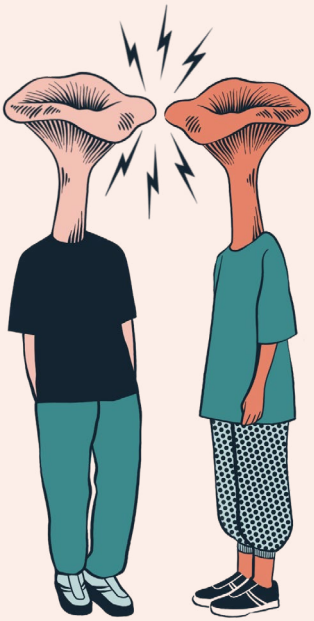
Ahora haz una lluvia de ideas de las tecnologías que esas formas de comunicación requieren hasta encontrar alguna que permita satisfacer las necesidades inicialmente planteadas. Continúa imaginando la relación de las personas y las tecnologías de la lluvia de ideas, y la manera en la que ellas condicionan la totalidad de sus relaciones:

- ¿Qué ha sucedido con quienes participan del acto comunicativo? ¿Ha cambiado algo en ellas? ¿Quienes emitieron sus mensajes quedaron satisfechas?
- Para finalizar, explora los impactos que este tipo de comunicación podría tener a nivel social, la forma en la que las personas, sus relaciones y la comunidad que habitan se verían modificadas:
- ¿Cómo se transforman por esta tecnología? ¿Qué impactos tienen estas

> tecnologías sobre los debates colectivos? ¿Cómo es la sociedad resultante? ¿Existen entes intermediarios en la conversación colectiva? ¿Algún otro tipo de mediación entra en juego? ¿Qué nuevos problemas surgen?

Contestando a estas preguntas no encontremos la solución de todos los males, pero es posible que nos permitan descubrir otras formas de usar las tecnologías que ya tenemos o recuperar otras que creíamos obsoletas.

Si quieres profundizar en otras metodologías para imaginar y crear tecnologías, puedes visitar el Taller de escritura especulativa sobre tecnologías feministas,[45] las Futurotopías feministas,[46] o los Borradores del futuro, historias y fabulaciones sobre mundos posibles.[47] En estas exploraciones imaginarias encontraremos, quizás, los caminos que nos lleven a esos otros mundos en los que queremos vivir.



45 http://cooptecniques.net/taller-de-escritura-especulativa-tecnologias-feministas/

46 https://zoiahorn.anarchaserver.org/specfic/recursos-que-inspiran-resources-inspiring/metodologias/

47 https://borradoresdelfuturo.net/

Glosario

Abya Yala: es el nombre más antiguo hasta ahora conocido para referirse al territorio americano. Literalmente significa “tierra en plena madurez” o “tierra de sangre vital”. Las naciones americanas tenían una idea vitalista de la tierra, inseparable de los humanos. Esta mirada se contrapone a la concepción europea basada en la división abstracta de la tierra como un objeto plausible de ser medido. De ahí que la idea occidental de continente, abstracto y aritméticamente separado por líneas, resulta incomprensible para dichas naciones.

Arquitectura de red: principios de diseño que orientan el desarrollo de ***software*** y ***hardware***.

Ausencia o escasez de internet: conjunto de limitaciones de acceso a las infraestructuras de telecomunicaciones como bloqueos, cortes, interrupción y congestión o saturación de la conexión.

Bloqueo: efecto que resulta de colocar deliberadamente obstáculos técnicos que impiden, limitan o interfieren la llegada de un paquete de datos o información a un destino de la red.

Capa física: conjunto de infraestructuras y medios materiales que permiten la transmisión, el procesamiento y el almacenamiento de datos.

Capa lógica: conjunto de programas informáticos, protocolos, configuraciones y políticas que definen el direccionamiento de la información.

Dirección IP: número que identifica a un dispositivo conectado a una red.

FTP (*File Transfer Protocol*): protocolo de transferencia de archivos basado en la arquitectura cliente-servidor.

Infraestructuras autónomas de comunicación: conjunto de tecnologías o herramientas digitales que conforman el ambiente virtual de trabajo de una organización, colectiva o comunidad organizada. Desde aparatos físicos (***hardware***) hasta aplicaciones, sistemas operativos, plataformas o servicios web (***software***). Además, incluye los acuerdos o protocolos que homologan los usos de éstas con el objetivo de hacer una gestión responsable de la información y la comunicación, basada en la noción de corresponsabilidad.[48]

IRC (*Internet Relay Chat*): es un protocolo de comunicación en tiempo real utilizado para conversar entre dos o más personas en un canal o "sala".

ISP: siglas en inglés para referirse al proveedor se servicios de internet, es decir, la empresa que brinda conexión a internet.

Medición de red: prueba de conectividad/conexión para verificar el envío y recepción de datos entre un destino y un origen.

Prueba: resultado registrado de los diferentes momentos de una medición de red.

Radio *jamming*: interferencia realizada por medio de dispositivos (***jammer***) con capacidad de emitir señales que interrumpen la comunicación. Este tipo de interferencias son muy difíciles de documentar y más allá de sospechas de uso no tenemos casos documentados en la región.

Redes P2P (red de pares o *peer-to-peer*): red en la que todos los nodos se comportan como iguales entre sí y no como clientes o servidores. Una de sus aplicaciones más conocidas es el intercambio de archivos a través del protocolo BitTorrent.

Tecnologías anticensura: todos aquellos desarrollos de ***software*** y ***hardware*** que por diseño contemplan características para dificultar o eludir restricciones de acceso.

VoIP (*Voice over IP*): conjunto de tecnologías que permiten transmitir la señal de voz en paquetes de datos.

---

48 Definición elaborada por Loreto Bravo en el marco de sus acompañamientos a organizaciones.

Referencias

Access Now. (2020a). Manual sobre apagones de internet y elecciones. Una guía para observadores electorales, embajadas, activistas y periodistas. https://www.accessnow.org/manual-sobre-apagones-de-internet-y-elecciones/.

Access Now. (2020b). #KeepItOn: Fighting internet shutdowns around the world. https://www.accessnow.org/keepiton/.

Access Now. (2021, agosto 17). Online safety resources for Afghanistan's human rights defenders. https://www.accessnow.org/online-safety-resources-afghanistan/.

Article19 (México y Centroamérica). (2016). Ataques cibernéticos inhabilitan páginas de Más de 131 y Radio Zapote. https://articulo19.org/ataques-ciberneticos-inhabilitan-paginas-de-mas-de-131-y-radio-zapote/.

Asociación para el Progreso de las Comunicaciones (APC), DDP, LaLibre.net y Taller de Comunicación Mujer. (2019). ***Derechos digitales en el contexto de las protestas y movilización social en Ecuador en octubre de 2019. Aporte para la visita de observación al Ecuador por parte del Relator Especial para la Libertad de Expresión, Edison Lanza, y del Comisionado Luis Ernesto Vargas de la Comisión Inter Americana de Derechos Humanos (CIDH)***. https://www.apc.org/es/pubs/derechos-digitales-en-el-contexto-de-las-protestas-y-movilizacion-social-en-ecuador-en-octubre.

Asociación para el Progreso de las Comunicaciones (APC), Karisma y Access Now. (2019). Disrupciones de internet en Ecuador: Cómo ocurrieron y cómo eludirlas. https://www.apc.org/es/news/disrupciones-de-internet-en-ecuador-como-ocurrieron-y-como-eludirlas.

Avendaño, Tatiana (2020, agosto). Lectura performática Cuerpx Antenx. Quito: Arte Actual. https://www.facebook.com/arteactualflacso/videos/750259055546013/.

Ávila, Renata. (2009). WordPress.com bloqueado en Guatemala. (Trad. De Burns, Alexandra). https://es.globalvoices.org/2009/07/02/wordpresscom-bloqueado-en-guatemala/.

Azpúrua, Andres, Chirinos, Mariengracia, Filastó, aRturo, Xynour, Maria, Basso, Simone, y Karan, Kanishk. (2019). From the blocking of Wikipedia to Social Media: Venezuela's Political Crisis. https://ooni.org/post/venezuela-blocking-wikipedia-and-social-media-2019/.

Bush, Lewis. (2018). ***Shadows of the State (2015-2018)***. Brave Books, 2018. http://www.lewisbush.com/shadows-of-the-state/.

Cahn, Albert Fox. (2021, agosto 24). The Taliban now controls a U.S.-made Super-Surveillance System. ***The Daily Beast.*** https://www.thedailybeast.com/the-taliban-now-controls-a-us-made-super-surveillance-system.

CAIDA.org. (s/f). Internet Outage Detection and Analysis (IODA). https://www.caida.org/projects/ioda/.

CIPESA. (2017). A Framework for calculating the economic impact of Internet disruptions in Sub-Saharan Africa.

Codeando México. (2020). ***Seguridad digital y derechos humanos***. https://repository.anarchaserver.org/action.php?id=1534&part=e&download.

Coding Rights. (2019, octubre 29). On the blocking of pro-choice websites: Women on Waves and Women on Web. ***Coding Rights.*** https://medium.com/codingrights/on-the-blocking-of-pro-choice-websites-women-on-waves-and-women-on-web-505ed6f17b63.

Committee to Protect Journalists (CPJ). (2021, abril 13). Digital Safety: Internet Shutdowns. https://cpj.org/2021/04/digital-safety-internet-shutdowns/.

Cubaperiodistas.cu. (2019, octubre 13). Lenin Moreno bloquea internet móvil en Ecuador, según Netbloks. https://www.cubaperiodistas.cu/index.php/2019/10/lenin-moreno-bloquea-internet-movil-en-ecuador-segun-netbloks/.

Díaz Hernández, Marianne. (2021, julio 16). ¡Patria y vida!: Cuba corta el acceso a internet para silenciar la protesta. ***Access Now.*** https://www.accessnow.org/patria-y-vida-cuba-internet/.

Fundación Karisma. (2021a, mayo 7). Una mirada a la interrupción del servicio de internet en Cali durante #ParoNacional. https://web.karisma.org.co/una-mirada-a-la-interrupcion-del-servicio-de-internet-en-cali-durante-paronacional/.

Fundación Karisma. (2021b, junio 3). Pedimos incorporar y analizar las violencias digitales en la protesta durante su visita. https://web.karisma.org.co/una-peticion-para-incorporar-y-analizar-las-violencias-digitales-en-la-protesta/.

Garay, Vladimir. (2014, marzo 6). La censura política en Internet es real: el caso de 1DMX.ORG. ***Derechos Digitales América Latina.*** https://www.derechosdigitales.org/7028/la-censura-politica-en-internet-es-real-el-caso-de-1dmx-org/.

Google.com. (2021). ***Google Transparency Report***. https://transparencyreport.google.com/traffic/overview.

Heacock, Rebekah. (2009, junio 29). WordPress blocked in Guatemala. ***OpenNet Initiative.*** https://opennet.net/blog/2009/06/wordpress-blocked-guatemala.

Hiperderecho. (2021). ***Vigilando a los vigilantes. Una guía para cuidarnos de estrategias basadas en la tecnología para monitorear, intimidar o silenciar nuestro activismo.*** https://hiperderecho.org/wp-content/uploads/2021/08/Guia-Vigilando-a-los-vigilantes.pdf.

International Human Rights Clinic (IHRC) y CyberLaw Clinic (2021). Lockdown and Shutdown. Exposing the Impacts of Recent Network Disruptions in Myanmar and Bangladesh. Disponible en https://clinic.cyber.harvard.edu/files/2021/01/Lockdowns-and-Shutdowns.pdf.

KillSwitch.pk. (2021). Kill Switch Timeline in Pakistan. https://killswitch.pk/.

Magma. (s/f). ***Magma Guide. Your first stop when conducting research on information controls, Internet censorship, and online surveillance***. https://magma.lavafeld.org/.

Nájera, Jacobo. (2016, agosto 10). Sobrevivir a los ataques de Denegación de Servicio Distribuido. ***Jacobo.org.*** https://www.jacobo.org/sobrevivir-a-los-ataques-de-denegacion-de-servicio-distribuido/.

Nájera, Jacobo. (2017, agosto 3). Botnet contra sitios web de medios independientes en México. ***Jacobo.org.*** https://www.jacobo.org/botnet-contra-sitios-web-de-medios-independientes-en-mexico/.

Nájera, Jacobo y Ververis, Vasilis. (2020, mayo 28). En México, el más grande operador de telecomunicaciones bloquea la internet segura. ***Global Voices.*** https://es.globalvoices.org/2020/05/28/en-mexico-el-mas-grande-operador-de-telecomunicaciones-bloquea-la-internet-segura/.

Netblocks. (2018). Regional internet disruptions in Nicaragua amid protests. https://netblocks.org/reports/nicaragua-regional-internet-disruptions-amid-protests-gdAmMvA9.

Netblocks. (2019a). Evidence of social media disruptions in Ecuador as crisis deepens. https://netblocks.org/reports/evidence-of-social-media-disruptions-in-ecuador-as-crisis-deepens-oy9RN483.

Netblocks. (2019b). Mobile internet disrupted in Quito as Ecuador political crisis escalates. https://netblocks.org/reports/mobile-internet-disrupted-in-quito-as-ecuador-political-crisis-escalates-eBOgkJBZ.

Netobservatory. (2020). Internet shutdown in Belarus. https://netobservatory.by/belarus-shutdown-2020-en/.

Qurium Media Foundation. (2021, enero 14). Uganda blocks Kenyan news ahead of the presidential elections. https://www.qurium.org/internet-blocking/the-elephant-blocked-in-uganda/.

Riley, M. Chris y Scott, Ben. (2009, marzo 19). Deep Packet Inspection: The end of The internet as we know it?. ***Free Press.*** https://www.freepress.net/policy-library/deep-packet-inspection-end-internet-we-know-it.

SafetyDetectives. (2021). 10 Best VPN Services (2021): Security, Features + Speed. https://www.safetydetectives.com/best-vpns/.

Sin Censura. (2020, junio 6). Solicitamos que se levante de inmediato el bloqueo de Women on Web en España. ***Sin Censura.*** https://sindominio.net/sincensura/.

Software Freedom Law Center India (SFLC.in). (2021). Internet Shutdowns Tracker. https://internetshutdowns.in/.

Steyerl, Hito. (2013, noviembre). Too Much World: Is the Internet Dead?. ***E-flux Journal,*** nº 49. https://www.e-flux.com/journal/49/60004/too-much-world-is-the-internet-dead/.

TunnelBear. (2020, diciembre 15). Iran and the four stages of censorship. ***The TunnelBear Blog.*** https://www.tunnelbear.com/blog/iran-and-the-four-stages-of-censorship/.

TunnelBear. (2021). TunnelBear Bandwidth Support: Free VPN Access in Restrictive Environments. https://www.tunnelbear.com/bandwidth-support.

Ververis, Vasilis; Khrustaleva, Olga y Quiroz, Eliana. (2017). Interferencia de red en América Latina: Evaluando mediciones de red para detectar controles de información y censura de Internet. ***5º Simposio Internacional LAVITS: Vigilancia, Democracia y Privacidad en América Latina***. https://lavits.org/wp-content/uploads/2018/04/32-Vasilis-Ververis-Olga-Khrustaleva-e-Eliana-Quiroz.pdf.

Ververis, Vasilis; Fadelkon, Ana y Bita, Samba. (2020, mayo 15). Women On Web, web censurada en España. ***Magma.*** https://blog.magma.lavafeld.org/es/post/women-on-web-blocking/.

Witness Org. (2020, febrero 2). Documenting during Internet Shutdowns. A blog series with practical tips. https://blog.witness.org/2020/02/documenting-during-internet-shutdowns/.

Witness Org. (2021). Atentxs a los apagones de internet: Documentar para los derechos humanos. https://es.witness.org/2021/09/atentxs-a-los-apagones-de-internet-documentar-para-los-derechos-humanos/.

Xynou, Maria, Filastò, Arturo y Basso, Simone. (2017, agosto 28). Measuring Internet Censorship in Cuba's ParkNets. ***OONI.*** https://ooni.org/post/cuba-internet-censorship-2017/.

YucaByte. (2021a, julio 12). #11J: Bloqueo de internet y redes para esconder las protestas en Cuba. https://www.yucabyte.org/2021/07/12/11j-internet-cuba/.

YucaByte. (2021b, julio 14). Mensajería ***offline*** y otros 'trucos' para burlar la censura en Cuba en tiempos de protestas. https://www.yucabyte.org/2021/07/14/protestas-comunicacion/.

Digital
Defenders
Partnership