

INTERNET'S *KILL SWITCH*

(Interruptor de emergencia o botón de pánico)

Resulta revelador que los distintos estudios realizados en materia de tecnologías de la información y comunicación partan de la presunción, tanto en los expertos como en el común de las personas, de la existencia del Internet como elemento connatural a la humanidad, aun cuando esta red de comunicación apenas cumplió su mayoría de edad. Por ello, el presente estudio abarca algunas aristas fundamentales de dicho tema, partiendo del análisis de los conceptos, antecedentes y aplicación reciente, así como el entorno dentro de las comunicaciones, derechos humanos y garantías individuales en México, y en otros países (entorno internacional) y, por último, ofrecer las conclusiones del trabajo.

La designación *Kill Switch (KS)* o interruptor de apagado/desactivado consiste en un procedimiento por el que en un muy breve período se interrumpen las comunicaciones especialmente aquellas vinculadas a la Internet¹ en una circunscripción geográfica o territorial, sea de forma legal, mediante la ejecución de una prerrogativa de Estado directamente con los prestadores del servicio concesionado de comunicación, o simplemente de facto por funcionarios públicos. En otras palabras, se crea un punto de control para que una autoridad pueda desactivar las comunicaciones a fin de proteger o protegerse de un agresor o atacante mediante la Internet², incluyendo la toma de las instalaciones y personal utilizados por los prestadores de dichos servicios.

Inicialmente, el concepto fue utilizado en el contexto de los estudios realizados en una eventual guerra cibernética (*cyberwarfare*),³ y era la acción de hackear⁴ sistemas o redes contra objetivos estratégicos tales como el suministro de energía, el transporte o los recursos tácticos militares con propósitos de espionaje o sabotaje; sin embargo, esta designación ha migrado hasta encontrarse inmersa en la legislación de diversos países como norma de protección del propio Estado, e incluso puede ir más allá como lo explicaremos en su oportunidad, ya que las comunicaciones pueden verse interrumpidas no únicamente en la

infraestructura⁵ como lo indicamos, sino también en los propios dispositivos de comunicación propiedad de particulares.

Uno de los creadores de Internet, Sir Tim Berners-Lee, respondió a pregunta expresa: “ the only way the Internet could ever be entirely shut down is if governments all over the world coordinated to make it a centralized system.[...] The way the Internet is designed is very much as a decentralized system. At the moment, because countries connect to each other in lots of different ways, there is no one off-switch; there is no central place where you can turn it off.” Al respecto de lo antes citado, por supuesto que hemos visto la ejecución de actos contundentes del *KS* por razones más cercanas a gobernantes que a instituciones democráticas (en tales situaciones se desconectó Internet); ejemplo de ello se dio durante el inicio y las etapas subsecuentes del período conocido como la “Primavera árabe⁶”, que sucedió en Túnez, Libia y Egipto⁷, cuando de manera franca, los gobiernos bloquearon el acceso a Internet y telefonía móvil a su población, en un esfuerzo para limitar la organización de los pobladores (quienes, aparentemente, estaban en su contra) y para hacer valer su “botón de pánico”. Un hecho similar ocurrió en China, con el llamado sistema nacional de filtrado conocido como “Proyecto Escudo Dorado”, que en 2009 bloqueó las comunicaciones celulares y de Internet en la región separatista denominada Xinjiang; asimismo, se pueden citar los casos en Nepal, durante la conmoción civil de 2005, y en Myanmar en 2007, entre otros.

Precisamente ésta, como otras prerrogativas que se han allegado los Estados, pueden, con facilidad en su ejercicio, llevar a un choque con ciertos derechos de los ciudadanos. Cabe preguntarnos, en este sentido, si existe o no un derecho a proteger, y si éste califica dentro de los derechos humanos fundamentales; pero también es necesario cuestionarnos si en términos generales los Estados tienen la prerrogativa de legislar o no sobre el tema. Respecto del primer cuestionamiento, existen dos disposiciones internacionales: el art. 19 de la Declaración Universal de los Derechos Humanos,⁸ que indica: “Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”; y por otra parte, está el art. 19 del Pacto Internacional de Derechos Civiles y Políticos,⁹ que establece:

“a) Nadie podrá ser molestado a causa de sus opiniones; b) Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir

informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección; c) El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para asegurar el respeto a los derechos o a la reputación de los demás; [y] d) La protección de la seguridad nacional, el orden público o la salud o la moral pública”.

De ambos textos, debemos considerar la validez jurídica para aquellos Estados miembro que además los han suscrito, a fin de integrarlos a su Derecho positivo; por lo que, además, les son legalmente vinculantes.¹⁰ En relación con los propios textos, los derechos humanos fundamentales a la libertad de opinión y expresión están vinculados no sólo con los medios de la persona humana para transmitirlos en el sentido del habla, sino que se encuentran intrínsecamente vinculados con todos los medios tecnológicos que nos permitan ejercerlos, pues se permite “investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”. Es justamente aquí donde aparece la Internet y las telecomunicaciones como parte de los medios antes indicados, ya que desde hace mucho tiempo, éstos son sinónimo de expresión, por lo que la humanidad se encuentra vinculada con la tecnología en la llamada globalización de las comunicaciones.

Frank La Rue, Relator Especial de la Asamblea de las Naciones Unidas, resalta la efectividad con la que la Internet provee y potencia el ejercicio de los derechos humanos indicados; por ende, podemos inferir que hoy no podemos disociarlos, pues es claro que el medio utilizado para comunicar y ejercer el derecho de expresión forma parte de los derechos humanos mencionados.

Por lo que hace al segundo aspecto, y de conformidad con el derecho internacional, el espacio que ocupa el territorio de un país está sujeto al régimen jurídico que los poderes del Estado han establecido (si bien éste no sea del todo absoluto con ciertas Naciones que son excepciones, por virtud de los tratados internacionales suscritos, como aquellos en la materia del Convenio de la Unión de Telecomunicaciones y el Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones¹¹ que define telecomunicación como “toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o

informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos”).¹²

Circunscrito a su ámbito territorial, todos los Estados tienen regulaciones relacionadas con las telecomunicaciones, algunas más estrictas, otras más modernas, pero indudablemente todas forman parte de la globalización, y, en este sentido, de acuerdo con el informe A/HRC/17/27, del 16 de mayo de 2011, expresa La Rue que: “los Estados en general han aumentado las restricciones impuestas al acceso a Internet mediante el uso de tecnologías cada vez más avanzadas para bloquear contenidos, vigilar y detectar a activistas y críticos, tipificar como delito la expresión legítima de opiniones y adoptar legislación restrictiva para justificar esas medidas.”¹³

A partir de lo expresado por el Relator, se observa que la tendencia es utilizar los argumentos de seguridad nacional y cumplimiento de la ley para restringir, con el fin de realizar una vigilancia, e impedir las comunicaciones en su momento, lo cual puede causar la violación de la secrecía en las mismas.¹⁴ Sin embargo, conforme a la Observación General núm. 34 sobre el artículo 19 del Pacto, el Comité de Derechos Humanos ha precisado que las restricciones al ejercicio del derecho a la libertad de expresión deben estar fijadas por la ley y sólo pueden imponerse para determinados propósitos debiendo cumplir pruebas estrictas de necesidad y proporcionalidad¹⁵. Consideramos que este derecho incluye la expresión y recepción de comunicaciones sobre toda clase de ideas u opiniones que puedan transmitirse a otros, y abarca el pensamiento político, los comentarios sobre los asuntos propios y los públicos, entre otros.

La Corte Interamericana de Derechos Humanos ha expresado que el derecho a la libertad de expresión no es un derecho absoluto y puede ser objeto de restricciones proporcionales al interés que las justifica bajo dos dimensiones: la individual, como el derecho a manifestar la propia opinión y a recibir informaciones, y la social, como derecho colectivo a recibir y buscar información.¹⁶ Adicionalmente, la Resolución A/HRC/20/L.13, de julio de 2012, del Consejo de Derechos Humanos de las Naciones Unidas, estableció un avance importante al fundar que la libertad de Internet asegura la aplicación en línea de los derechos humanos.

El lícito camino que utilicen los Estados mediante la emisión de disposiciones para contar con las facultades necesarias para llevar a cabo un bloqueo en las comunicaciones con la bandera de la seguridad nacional o equivalentes, requiere de claros marcos de referencia que garanticen el respeto a la libertad de opinión y de expresión. Organizaciones como la Electronic Frontier Foundation¹⁷, Article 19¹⁸ y El Alto Comisionado de Derechos Humanos, Human Rights First¹⁹ entre muchas otras, mantienen agendas y realizan trabajos de análisis sobre estos temas buscando la protección de los derechos humanos vinculados a los medios electrónicos.

Un último aspecto a considerar son los esfuerzos que cierto sector de la sociedad civil internacional ha publicado la agenda de los llamados “Derechos Humanos Emergentes”, entendidos como la parte no estática y evolutiva de esas garantías, dentro de la cual no se encuentra tema alguno relacionado con las telecomunicaciones. En mi opinión, la razón es que tales derechos ya se encontraban considerados en la Declaración de 1948.²⁰

México

Entrando al análisis del *KS*, el derecho que el Gobierno Federal Mexicano tiene respecto de las telecomunicaciones y de los concesionarios de dichos servicios se encuentra el contenido en el art. 66 de la Ley Federal de Telecomunicaciones, donde se establece: [en caso de] “desastre natural, de guerra, de grave alteración del orden público o cuando se prevea algún peligro inminente para la seguridad nacional, la paz interior del país o para la economía nacional, se podrá ejecutar una requisa de las vías generales de comunicación²¹ y de los bienes muebles e inmuebles necesarios para operar dichas vías y disponer de todo ello como lo juzgue conveniente. [...] La requisa se mantendrá mientras subsistan las condiciones que la motivaron”.

Si bien es cierto que las primeras dos causales provienen de orígenes evidentes que implican incluso la suspensión de ciertos derechos para los ciudadanos, la grave alteración, el peligro inminente, la paz interior o la economía nacional son conceptos cargados de un fuerte componente de interpretación de la autoridad, que puede alejarse del propio fundamento de ese derecho para convertirse en un instrumento de suspensión de los derechos humanos vinculados al derecho de expresión y las comunicaciones. La ejecución del *KS* no se ha realizado o al menos no se ha identificado que se hubiere realizado; me atrevo a indicar que se

puede cuestionar la ejecución con los fundamentos indicados por su separación de cumplimiento en los extremos del Pacto Internacional de Derechos Civiles y Políticos, del cual México es parte desde el 23 de marzo de 1981.

Egipto

Protestas en favor de la democracia en el país se presentaron en las calles de las principales ciudades, organizadas, al menos parcialmente, a través de las redes sociales (Twitter, Facebook y Twitpic) para compartir noticias, videos y fotos en tiempo real de los eventos ocurridos en las calles. El gobierno, en consecuencia, impidió las protestas mediante el bloqueo digital del acceso a dichas redes para, así, dejar a la población civil incomunicada. Una investigación realizada por la empresa Renesys demostró que alrededor de las 12:34 de la mañana, simultáneamente, todas las redes conectadas al sistema de ruteo internacional de IP's fueron desconectadas, al igual que el servicio de mensajería instantánea y de comunicación celular²²; esto se realizó físicamente al tomar las instalaciones de los proveedores de servicios de Internet y eliminando las tablas de ruteo necesarias para la comunicación, al amparo de las disposiciones legales por las que otorgaron los títulos de operación de los mismos a favor del Estado.²³ Por lo que debemos indicar que sí existía un derecho legítimo del Estado para proteger a la población y, sin embargo, el ejercicio de ese derecho tuvo fines distintos. Es de mencionar que Egipto, al igual que Túnez, en el tiempo en que ejerció su *KS*, no era Estado firmante de las Resoluciones emitidas por la Comisión de Derechos Humanos de las Naciones Unidas en materia de libertad de expresión.

Es de mencionar que Egipto al igual que Túnez en el tiempo en que ejercieron su *KS*, no eran Estados firmantes de las Resoluciones emitidas por la Comisión de Derechos Humanos de las Naciones Unidas en materia de libertad de expresión.

EUA

Desde hace cierto tiempo se realiza el espionaje o grabación telefónica sobre restringidas bases y fuertemente penalizado en tribunales,²⁴ al ser considerado una amenaza al derecho de privacidad y sólo autorizado en crímenes de importancia; pero, con el tiempo, el gobierno ha ido expandiendo sus facultades de vigilancia en virtud de la seguridad nacional como

justificación fundamental. Sin embargo, el tiempo ha pasado y, en el ámbito de las comunicaciones –Internet incluida– también se analiza cómo puede afectar el *KS* a la Comisión Federal de Comunicaciones (FCC, por las siglas en inglés correspondiente a U.S. Federal Communications Commission) y a las políticas norteamericanas de telecomunicaciones, en vista de la legislación impulsada por el senador Joe Lieberman (19 de junio de 2010), la cual se rige con el principio de que el ciberespacio debe protegerse como un activo nacional.

Dicha propuesta permite al Presidente establecer limitaciones a la libertad de expresión bajo el concepto de la “ciberseguridad”; con lo cual puede declararse una “ciberemergencia”²⁵. Al efecto, se establecería una lista de sistemas o activos que constituyan la infraestructura crítica, los cuales estarían a resguardo del Departamento de Seguridad Nacional²⁶. Esta historia no se ha terminado y los activistas a favor de los derechos y libertades han provocado que el diálogo se extienda buscando detener dicha iniciativa.

Las Naciones Unidas²⁷ han realizado varios estudios, de los que destacamos los realizados por La Rue respecto de los derechos humanos, en su confluencia con el uso de tecnologías de la comunicación, que tomaron especial relevancia después de las declaraciones de Edward Snowden, en las que la National Security Agency (NSA) había realizado la descarga de información directamente de los prestadores de servicios mediante una operación de espionaje denominada PRISM. Incluso, en los foros internacionales de la Comisión de Telecomunicaciones se comentó la posibilidad de que un país pudiera desconectar o interferir a otro en Internet, en pro del concepto de la “ciberseguridad”.

En el caso de los dispositivos *iPhones* y *iPads*, un funcionario de la empresa Apple indicó, en la Conferencia Anual de Desarrolladores de este año,²⁸ que, a fin de desincentivar el robo de dichos dispositivos, dentro del recién lanzado IOS 7, se tendría una aplicación ligada a la llamada *find my pone*, que bloquearía las comunicaciones y borraría de manera remota la información contenida en el dispositivo. Si bien la sustracción de dispositivos no es tema del presente estudio, es importante señalar la posibilidad de que las compañías que los diseñan puedan llevar a cabo, por mandato u otra causa, el borrado de la información contenida en ellos.

Debemos mencionar que el *KS* es un instrumento convertido en arma que se utiliza con la ley en la mano, ya que se ha construido, o está en proceso de construcción, una infraestructura legal que o permitirá los actos antes mencionados en nombre de la seguridad y utilizando mecanismos de bloqueo y filtrado con fines de censura cada vez más avanzados.

La falta de transparencia que rodea estas medidas hace difícil determinar si el bloqueo proviene realmente de un riesgo o ciberataque al Estado, o se trata de una violación o incumplimiento de su obligación de respetar el derecho a la libertad de opinión y expresión.

La ejecución del *KS* requiere de la implementación de las excepciones contenidas en el Pacto que se examinó anteriormente, a fin de no caer en una violación o menoscabo del derecho a la libertad de expresión, con el deber de superar la siguiente prueba acumulativa integrada por tres elementos de conformidad con establecido por la Comisión de Derechos Humanos: “*a*) Prevista por ley de manera clara y accesible para todos (principios de previsibilidad y transparencia); *b*) Obedecer a uno de los fines establecidos en el párrafo 3 del artículo 19 del Pacto, que son: *I*) asegurar el respeto a los derechos o a la reputación de los demás, o *II*) proteger la seguridad nacional, el orden público o la salud o la moral públicas (principio de legitimidad); y *c*) Debe revelarse necesaria y ser el medio menos restrictivo requerido para lograr el objetivo previsto (principios de necesidad y proporcionalidad).

Finalmente, la aplicación de cualquier legislación que restrinja el derecho a la libertad de expresión deberá corresponder a un órgano formado según la tradición jurídica de cada país pero considerando forzosamente que sea independiente de cualquier influencia indebida como las de tipo político, comercial u otro; de manera que no haya arbitrariedad ni discriminación y existan las debidas salvaguardias contra el abuso, incluida la posibilidad de impugnación y recurso contra su aplicación abusiva.

¹ Considerando VOIP, email, redes sociales, páginas, contenidos y servicios como los de cómputo en la red

² http://en.wikipedia.org/wiki/Internet_kill_switch.

The theory behind a kill switch is creation of a single point of control for one authority or another to control in order to "shut down the internet to protect it" from unspecified assailants.

³ The prospect of cyberwarfare over the 2000s has prompted the drafting of legislation by US officials, but worldwide the implication of actually of “killing” the Internet has prompted criticism of the idea in the United States.

⁴ <http://INTERNATIONAL TELECOMMUNICATION UNION. WSIS Thematic Meeting on Cybersecurity. Geneva, 28 June – 1 July 2005>. En términos generales Hacker es quien

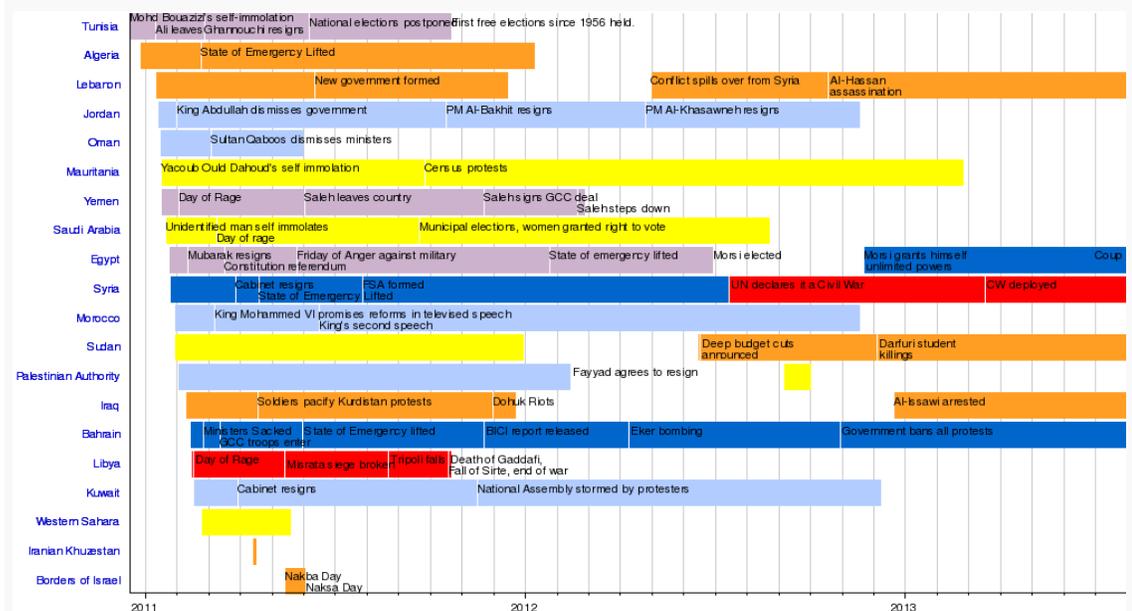
explota, distorsiona, interrumpe y destruye información, dentro de los que se encuentran los Script kiddies, Hacktivists, Cracker, “Black Hat Hacker” y los Sneakers, or “White Hat Hackers” entre otros.

⁵ <http://news.discovery.com/tech/does-the-internet-have-a-kill-switch-120907.htm>.

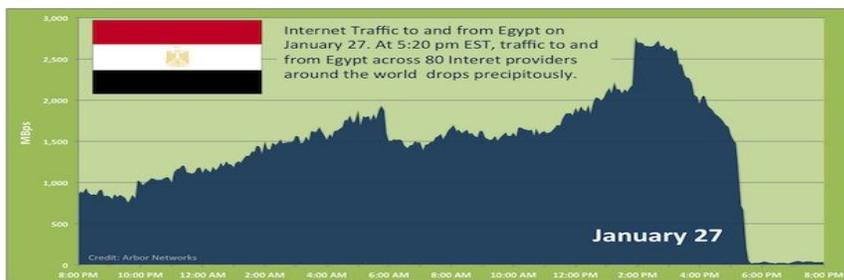
HTTP Error 404 o “no encontrado” es un código de estado HTTP que indica que el host ha sido capaz de comunicarse con el servidor.

⁶ http://en.wikipedia.org/wiki/Timeline_of_the_Arab_Spring#December

Diagrama de tiempo de la primavera árabe



⁷ <http://www.fastcompany.com/1721708/egypt-shuts-tech-tries-shut-protesters>



⁸ http://www.un.org/es/documents/udhr/index_print.shtml

⁹ <http://www.juridicas.unam.mx/publica/librev/rev/derhum/cont/34/pr/pr40.pdf>

10

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Asimismo, a nivel regional existen disposiciones espejo como en la Carta Africana de los Derechos de las Personas (art. 9), La Convención Americana de Derechos Humanos (art. 13)

y la Convención para la Protección de de los Derechos Humanos y Libertades Fundamentales (art. 10)

¹¹ <http://www.itu.int/es/about/Pages/default.aspx>

¹² <http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf>

¹³ A/HRC/17/27, del 16 de mayo de 2011

¹⁴ Declaración Universal de los Derechos Humanos, art 12. "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

¹⁵ www2.ohchr.org/english/bodies/hrc/docs/CCPR.C.GC.34_sp.doc

¹⁶ www2.ohchr.org/english/bodies/hrcouncil/.../A-HRC-17-27-Add3_sp.pdf, párr. 6.

¹⁷ <https://www.eff.org/deeplinks/2012/07/un-human-rights-council-resolution-internet-and-human-rights-step-right-direction>

¹⁸ <http://www.article19.org/pages/en/mandate.html>

¹⁹ <http://www.humanrightsfirst.org/our-work/human-rights-defenders/protecting-human-rights-defenders/>

²⁰ http://www.idhc.org/eng/1241_ddhe.asp

Al respecto de los Derechos Humanos, con motivo del proceso de discusión que tiene como origen un diálogo organizado por el Instituto de Derechos Humanos de Cataluña (IDHC), en el marco del Foro Universal de las Culturas Barcelona 2004, titulado "Derechos Humanos, Necesidades Emergentes y Nuevos Compromisos", se presenta la idea de derechos no estáticos que se vierten en una Declaración Universal de los Derechos Humanos Emergentes (DUDHE), que es un instrumento programático de la sociedad civil internacional dirigido a los actores estatales y a otros foros institucionalizados para la cristalización de los derechos humanos en el nuevo milenio.

²¹ Se entiende como el espectro radioeléctrico las redes de telecomunicaciones y los sistemas de comunicación vía satélite LFT art 4.

²² http://www.nytimes.com/2011/02/16/technology/16internet.html?_r=3&pagewanted=all&



²³ The New York Times

How Egypt Disappeared From the Internet

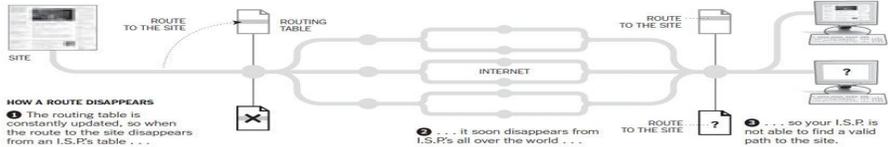
On Jan. 28, the routes to Egypt's networks disappeared from routing tables, the core mechanism used to direct traffic across the Internet.

HOW TRAFFIC IS ROUTED ACROSS THE INTERNET

1 An Internet service provider shares the route to a given Web site with other I.S.P.'s. It does this by adding the site's route to a document called the routing table, which is then passed to those providers.

2 Those I.S.P.'s repeat the process, and the routing information spreads across the Internet within seconds . . .

3 . . . so when you request the site, your I.S.P. uses the routing table to find its way to the site.

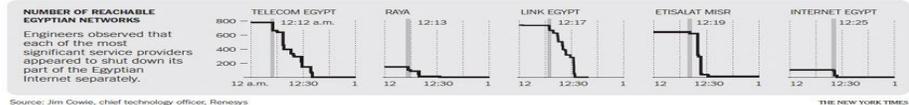


HOW A ROUTE DISAPPEARS

1 The routing table is constantly updated, so when the route to the site disappears from an I.S.P.'s table . . .

2 . . . it soon disappears from I.S.P.'s all over the world . . .

3 . . . so your I.S.P. is not able to find a valid path to the site.



Source: Jim Cowie, chief technology officer, Rensys

THE NEW YORK TIMES

24

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

In the first judicial validation of wiretapping, Justice Brandeis of the United States Supreme Court wrote a scathing dissent that noted that wiretapping was a “subtler and more far-reaching means of invading privacy” that could not be justified under the Constitution. In a chillingly accurate forecast, the eminent jurist predicted: “Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrence of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.” *Olmstead v. United States*, 277 U.S. 438 (1928).

25 <http://www.fastcompany.com/1721753/could-egypt-happen-here-obamas-internet-kill-switch>

26 “Emergency Wireless Protocols,” (Standard Operating Procedure 303 or “SOP 303), the federal agency also claims the power to shut down all communications, including the Internet, in the event of a national crisis.

27 <http://www.infowars.com/russian-cyberspace-head-calls-for-internet-kill-switch/>

28 <http://www.cnn.com/2013/06/11/tech/mobile/iphone-ios7-kill-switch>