Contra el ciberfascismo:
autodefensa de derechos y soberanía tecnológica.

«Cuando desviaron las DNS a los catalanes,
guardé silencio,
porque yo no era catalán.
Cuando secuestraron los servidores de hackers,
guardé silencio,
porque yo no era hacker.
Cuando bloquearon varios rangos de IPs a sindicalistas,
no protesté,
porque yo no era sindicalista.
Cuando fueron a cortar la conexión a los inmigrantes,
no pronuncié palabra,
porque yo no era inmigrante.
Cuando finalmente vinieron a quitarme el móvil,
no había DNSs, ni IPs, ni servidores, ni conexiones con las que poderlo denunciar.»

Martin Hackmöller

Las imágenes de la represión contra la gente que reclamaba su derecho a decidir el día 1 de Octubre en Catalunya han dado la vuelta al mundo. Más de 800 ciudadanas heridas y los millones de personas que participaron en el referendum atestiguan la dureza represiva de aquel día: porrazos, patadas y golpes contra gente defendiendo urnas, más el miedo y la incertidumbre de no saber cuándo iban a llegar a por ti.

Lo que no ha captado suficiente atención social o mediática ha sido la represión cibernética que durante aquella jornada y durante las dos semanas previas sufrieron innumerables personas, infraestructuras, colegios, servidores, conexiones y dispositivos. Un ataque sin precedentes (ni en el estado español, ni en Europa) y que sienta un peligroso precedente de brutalidad y violencia tecnológica, máxime cuando éste se oculta o se presenta desde los medios como algo irrelevante, o que es perfectamente legítimo en una sociedad democrática. Una violencia amparada por el mismo sistema judicial que tardó 2 semanas en reclamar el ordenador de las cuentas del PP y aceptó impasible un ordenador antiguo con los discos duros cambiados, pero que no vaciló en dictar (sin jucio previo) condenas tan bestiales y absurdas como las de "borrar la identidad digital" de una persona cuyo "delito" fue enseñar a clonar una web. Una violencia ejercida en todas las capas de internet: proveedores, gestores de dominios, de contenidos, IPs, DNSs, conexiones y dispositivos.

He aquí un resumen de los hechos represivos que sucedieron aquellos días:

* Cambio de DNS en las operadoras de los dominios
* Redirección de tráfico HTTP
* Bloqueo de tráfico SSL a ip's
* Corte físico de conexiones a internet de la Red Educativa de la Generalitat
* Cierre del hosting de webs en empresas de hosting nacionales
* Ataque DDoS a las IP's para el registro a mesas de colegios electorales
* Detención y declaraciones de personas que han colgado réplicas de webs, requisación de mòvil, ordenador y cambio de contraseñas de cuentas como github
* Monitorización de las IP's de instituciones públicas educativas
* Se retira una aplicación de Play Store (Android) para saber dónde votar
* Se obliga a revelar contraseñas de aplicaciones de instituciones públicas

Algunas voces han descrito estos hechos como "la primera ciberguerra" contra la democracia. Una ciberguerra asimétrica, donde un gobierno, sus fuerzas armadas y turbas de ultras atacaron con todos los medios posibles mientras que otros defendieron de forma no violenta sus infraestructuras y derechos digitales. En gran medida, las instituciones y la sociedad civil catalana consiguió evitar que la represión alcanzara el fin que se había propuesto. Pero el precedente prevalece y las fuerzas represivas consiguieron un objetivo que tenemos el deber de resistir: activaron y normalizaron el fascismo cibernético.

Como en todas las guerras y formas de fascismo, las primeras víctimas fueron los derechos fundamentales: en este caso el derecho al acceso a la información, el derecho a la conexión y el derecho a la libre expresión. Desgraciadamente, si no hacemos nada, el "a por ellos" cibernético no parará aquí.

Desde el Ingoberhack, el Hackmeeting 2017 que se ha celebrado en Madrid queremos denunciar estos hechos y recordar que:

1. Por encima de toda medida de protección y resistencia tecnológica exigimos y reclamamos el respeto a los derechos de acceso a la información, a la conexión y a la libre expresión, el derecho a las infraestructuras que permiten que la gente se conecte, dialogue y exprese sus voluntades, opiniones y afectos.

2. Cuando la represión se ejerce sobre las infraestructuras de internet, nos afecta a todas las personas. Es responsabilidad de toda la sociedad denunciar y defendernos de esta represión.

3. Que la garantía del ejercicio efectivo de estos derechos, en última instancia, reside en una soberanía tecnológica que nos concierne por igual: en el desarrollo de infraestructuras de conectividad libres como Guifinet, en el desarrollo y difusión de sistemas distribuídos de tráfico como Tor, en la construcción y uso de información como IPFS, en la promoción y capacitación popular de herramientas de cifrado (como GPG), en el fomento y defensa del Software Libre.

4. Que esta soberanía tecnológica y la libertad de la información son la condición de posibilidad para una sociedad libre. Más allá de cualquier otra cuestión política, debemos defender el uso de las herramientas que nos pemiten expresarnos y organizarnos como seres humanos.

Por estos motivos, lanzamos un llamamiento a toda la sociedad civil para que, más allá de las diferentes posiciones políticas, se una en la defensa de las aldeas digitales que garantizan la libertad de expresión.

HACKMEETING 2017

INGOBERHACK