

¿Internet en manos de las élites?

Por: Germán Gorraiz López. Eco Republicano. 22/09/2018

Zbigniew Brzezinski, ex-consejero de Seguridad Nacional durante el mandato de Carter en su libro *“Entre dos edades: El papel de Estados Unidos en la era tecnocrática”* (1971) aboga por el control de la población por una élite mediante la “manipulación cibernética” al afirmar que “pronto será posible asegurar la vigilancia casi continua sobre cada ciudadano y mantener al día los expedientes completos que contienen incluso la información más personal sobre el ciudadano, archivos que estarán sujetos a la recuperación instantánea de las autoridades”, lo que anunciaría ya la posterior implementación del programa PRISM o del reciente “affaire Spyon” de la NSA.

En consecuencia, tras ser denunciado EE.UU. por intentar controlar la nube mediante programas secretos como el Programa PRISM, estaríamos ya asistiendo al final de la democratización de la información (siguiendo la senda emprendida por los llamados “países totalitarios”, mediante la imposición de leyes que prohíben el uso de determinados términos para continuar con la implementación de filtros en los servidores de los ISP. Así, según un estudio de la organización OpenNet (integrada por las universidades de Oxford, Cambridge, Harvard y Toronto), 61 países ejercerían la censura de webs con contenidos políticos o sociales “peligrosos” e impedirían asimismo el acceso a aplicaciones como YouTube o Google Maps aplicando sofisticados métodos de censura gracias a la colaboración de empresas occidentales, como ocurre en Egipto y Turquía.

La guerra híbrida como elemento diferencial de la Guerra Fría 2.0

La nueva doctrina geoestratégica conocida como “Guerra Híbrida” sería atribuible al Jefe de Estado Mayor de las FF.AA. Rusas, Valery Gerasimov quien afirmó que “cada vez es más frecuente que se dé prioridad a un uso conjunto de medidas de carácter no militar, políticas, económicas, informativas y de otro tipo que estarían sustentadas en la fuerza militar. Son los llamados métodos híbridos”, concepto que se habría puesto en práctica por primera vez con ocasión de las recientes Elecciones Presidenciales en EE.UU. Así, en la web de investigación “Mother Jones” apareció una versión reducida del informe de los servicios de inteligencia de EE.UU. en el que acusaban directamente al Gobierno de Putin de estar detrás de “supuestos ataques cibernéticos de hackers rusos para desequilibrar la campaña electoral de Hillary Clinton e inclinar la balanza a favor del supuesto submarino ruso, Donald Trump”.

Según el citado documento de los servicios de inteligencia de EE.UU., el Departamento Central de Inteligencia ruso (GRU) con sede en Moscú, considerado el “servicio de espionaje más poderoso y efectivo ruso en la actualidad tras asumir las funciones del primigenio Servicio de Inteligencia Exterior (SVR) “, se habría servido del pirata informático Guccifer 2.0 así como de la página web DC Leaks.com y de WikiLeaks para “difundir públicamente información de los correos secretos de Hillary Clinton obtenidos mediante hackeo cibernético”, (extremo negado por el fundador de WikiLeaks, Julian Assange), pero que no habría sido óbice para que la red social Twitter haya prohibido toda publicidad en las cuentas de los medios rusos RT y Sputnik tras acusarles de “divulgar informaciones que interfirieron en las elecciones estadounidenses del 2016”.

¿Final del “acceso abierto” a Internet?

Zbigniew Brzezinski, en un discurso pronunciado en una reunión del *Council on Foreign Relations* (CFR) advirtió que “la dominación de las élites ya no es posible debido a una aceleración del cambio social impulsado por la comunicación instantánea que han provocado el despertar universal de la conciencia política de las masas (Global Political Awakening) y que está resultando perjudicial para la dominación externa como la que prevaleció en la época del colonialismo y el imperialismo”.

La necesidad de escapar al control del Big Brother en redes como Youtube, Twitter o Facebook, habría impulsado la red TOR (Dark web), creada por defensores del software libre para proteger la identidad de los usuarios. Dicha red contó en sus inicios con las bendiciones de los Gobiernos occidentales para permitir el acceso a Internet en “países totalitarios” como China, Corea del Norte, Rusia e Irán, pero tras los atentados yihadistas de París, las actividades propagandística del ISIS estarían siendo monitorizadas y filtradas por las agencias de seguridad occidentales lo que habría forzado al grupo yihadista a utilizar masivamente la nueva aplicación

Telegram, al estar sus contenidos encriptados (sus usuarios pueden formar grupos de hasta 200 personas y utilizar chats secretos donde el material propagandístico se autodestruye), con la consiguiente dificultad de los servicios secretos occidentales para acceder a sus contenidos.

En un nuevo intento para preservar el anonimato de los usuarios en la Red, asistimos a la aparición de las VPN o Red Privada Virtual, herramientas que ocultan la identidad de los usuarios y permiten mantener la comunicación con cualquier país del mundo libre de vigilancia, lo que habría impulsado a países como Rusia o China a imponer normas para el acceso de los usuarios a dichas herramientas. Asimismo, Francia, Gran Bretaña, Indonesia, China y Rusia exigen eliminar los mensajes encriptados en Whatsapp y Telegram, medidas constrictoras que tendrán como efecto colateral la imposibilidad del acceso abierto (Opens Access) a los contenidos de la Red en la próxima década y el retorno a sus orígenes de la Red de Redes, al quedar Internet convertido en herramienta exclusiva de las élites políticas, económicas y militares.

[LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ.](#)

Fotografía: Eco Republicano

Fecha de creación

2018/09/22