



# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y  
SOCIALES

---

INTERNET, HERRAMIENTA DE PODER EN  
EL SIGLO XXI

TESIS

PRESENTA

JESÚS ARMANDO CAMPOS FLORES

Para obtener el título de Licenciado en  
Relaciones Internacionales

Asesor. Manuel Ortiz Escámez

Ciudad Universitaria, Cd. Mex., 2018



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



*Por muy alta que sea la montaña  
siempre hay un camino hacia la cima.*  
**Anónimo**

*Los hábitos son trenes  
y sólo de nosotros depende saber cuál tomar.*  
**Proverbio de Naftali**



## DEDICATORIAS

A Gabriela F. Mondragón, madre, por tu denodado e inexorable respaldo, por ser mi ejemplo para escalar incansable y con humildad en la cuesta de la vida hacia lo que anhelas y amas.

A José Armando Campos Martínez, padre, amigo de temple, creador de las puertas de madera, por tu apoyo, humildad, lealtad, y tenacidad.

A Esperanza Mondragón Benjume, abuela y amiga, por mostrarme el portal del absoluto más allá de lo terrenal.

A Marco Antonio Flores Mondragón, por ser el guía que desde mis primeros pasos me impulsó a descubrir otros mundos a través de las hojas y la tinta de la literatura.

A Ricardo F. Mondragón, por inspirarme a mirar hacia el cosmos y la tecnología desde el alba de mis días.

A María Esther y Elizabeth Flores Mondragón, por ser ejemplos de lid, pendencia y predisposición ante las adversidades

A Samantha Campos, aprendiz inteligente y prodigiosa, compañera en la creación de Nazumuz.

A Edel Flores, compañero de aventuras cuando niños, amigo desde siempre.

A Megan y Emiliano Flores, porque la verdadera grandeza se encuentra en aprender de los más pequeños.



## Índice

|  |            |
|--|------------|
| INTRODUCCIÓN.....  | 6          |
| <b>1. INTERNET, HERRAMIENTA DEL ESTABLISHMENT PARA LA RETENCIÓN<br/>INFORMÁTICA SISTEMATIZADA .....</b>                | <b>13</b>  |
| 1.1. El <i>establishment</i> .....   | 13         |
| 1.2. Educación y medios de comunicación .....  | 15         |
| 1.3. Contagio del pesimismo mediático.....   | 17         |
| 1.4. Censura y Limitación Sistemizada de la Información .....  | 19         |
| 1.4.1. <i>Surface Web</i> .....  | 26         |
| 1.4.2. <i>Deep Web</i> .....   | 29         |
| 1.4.3. Darknet .....   | 34         |
| 1.5. <i>Deep Web</i> y seguridad informática .....   | 36         |
| 1.5.1. Clasificación del <i>malware</i> .....  | 40         |
| 1.5.2. El negocio del <i>malware</i> .....   | 44         |
| 1.6. Técnicas de manipulación social en la <i>web</i> .....  | 48         |
| 1.6.1. Segmentación de usuarios por comportamiento .....   | 48         |
| 1.6.2. Ingeniería social.....  | 50         |
| 1.6.3. Spam dexing .....   | 54         |
| <b>2. LA PUGNA POR LA HEGEMONIA DEL TRÁFICO INFORMÁTICO .....</b>  | <b>56</b>  |
| 2.1. Neocolonialismo e Internet.....   | 56         |
| 2.1.1. Lenguaje .....  | 58         |
| 2.1.2. Tendencia política .....  | 62         |
| 2.2. Motores de búsqueda, navegadores <i>web</i> y redes sociales, herramientas de<br>influencia política mundial..... | 66         |
| 2.2.1. Navegadores y motores de búsqueda <i>web</i> .....  | 69         |
| 2.2.1.1. <i>Google</i> .....   | 73         |
| 2.2.1.2. <i>Baidu</i> .....  | 78         |
| 2.2.1.3. <i>Yandex</i> .....   | 83         |
| 2.2.2. Redes sociales .....  | 88         |
| 2.2.2.1. <i>Facebook</i> .....   | 91         |
| 2.2.2.2. <i>QZone</i> .....  | 95         |
| 2.2.2.3. <i>Vkontakte</i> .....  | 98         |
| <b>3. CASOS DE EMPLEO DE LA INTERNET COMO HERRAMIENTA DE PODER EN<br/>EL SIGLO XXI.....</b>                            | <b>102</b> |
| 3.1. Países del centro .....   | 106        |
| 3.1.1. Mediatización del terrorismo.....   | 107        |
| 3.1.2. Ciberensura de la NSA en Australia .....  | 110        |

|        |   |     |
|--------|---|-----|
| 3.1.3. | Ciberataques .....                              | 114 |
| 3.1.4. | Supresión de la neutralidad de la red .....     | 118 |
| 3.2.   | Países semi-periféricos y periféricos .....     | 120 |
| 3.2.1. | Global Online Freedom Act (GOFA) .....          | 120 |
| 3.2.2. | Mubarak apaga la Internet .....                 | 123 |
| 3.2.3. | Vehículos aéreos de combate no tripulados ..... | 125 |
| 4.     | <b>CONCLUSIÓN</b> .....                         | 132 |
| 5.     | <b>GLOSARIO</b> .....                           | 137 |
| 6.     | <b>FUENTES CONSULTADAS</b> .....                | 139 |

## Índice de gráficas

|                    |   |     |
|--------------------|---|-----|
| <b>Gráfica 1.</b>  | Gráfica que muestra el porcentaje de usuarios en la Internet por 100 personas desde 1990 hasta 2016. ....   | 24  |
| <b>Gráfica 2.</b>  | Escala aproximada de la distribución del contenido en la Internet por terabytes hasta 2016. ....  | 25  |
| <b>Gráfica 3.</b>  | Crecimiento del número de tipos de <i>malware</i> (en millones) de 2007 a 2017 en general y distribución en porcentajes del primer y segundo cuarto de 2016 específicamente en windows..... | 45  |
| <b>Gráfica 4.</b>  | Porcentaje y número de <i>Ddosen</i> Estados Unidos, en el último cuarto de 2016 por país de origen. ....   | 46  |
| <b>Gráfica 5.</b>  | Gráfica que muestra cómo se representan los idiomas en la vida real en comparación con los 10 millones de sitios web más populares de la Internet hasta 2015. ....                          | 60  |
| <b>Gráfica 6.</b>  | Los diez idiomas más usados en Internet según el número de sitios web en 2017.....  | 61  |
| <b>Gráfica 7.</b>  | Ingreso anual de Alphabet en dólares cuya principal subsidiaria es Google. ....   | 78  |
| <b>Gráfica 8.</b>  | Gráfica que muestra el porcentaje del precio de cambio de Baidu y Alphabet de 2016 a 2017 en millones de dólares. ....  | 83  |
| <b>Gráfica 9.</b>  | Ganancias de Yandex y Google de 2012 a 2016 en millones de dólares. ....  | 86  |
| <b>Gráfica 10.</b> | Cantidad en millones de búsquedas en los motores más utilizados en Rusia (tanto desde dispositivos móviles como desde ordenadores fijos) en los primeros dos meses de 2018. ....            | 88  |
| <b>Gráfica 11.</b> | Número de usuarios activos en Facebook en todo el mundo, dividida en cuartos de año desde 2008 a 2017.....  | 93  |
| <b>Gráfica 12.</b> | Número en promedio anual de usuarios de Vkontakte activos mensualmente de febrero 2010 a abril de 2017. ....  | 100 |
| <b>Gráfica 13.</b> | Porcentaje de ciberataques de acuerdo con el país de origen en todo mundo de 2012 a 2014. ....  | 117 |
| <b>Gráfica 14.</b> | Número aproximado de armas lanzadas por vants de combate (de acuerdo a su tipo) del reino unido de la Gran Bretaña contra Daesh en Iraq y Siria entre 2014 y 2016. ...                      | 130 |

## Índice de tablas

|   |    |
|---|----|
| <b>Tabla 1.</b> Tabla comparativa que muestra el incremento de usuarios de la Internet y propietarios de un <i>smartphone</i> en países en vías de desarrollo de 2013 a 2015. ....  | 23 |
| <b>Tabla 2.</b> Tabla que muestra los 20 sitios web más visitados del mundo en la <i>surface web</i> . Última actualización 28 de enero de 2018. ....   | 28 |
| <b>Tabla 3.</b> Aproximación obtenida de los sitios activos más populares en la <i>deep web</i> , accesibles solo mediante <i>Tor browser</i> . Última actualización 31/1/18. ....  | 31 |
| <b>Tabla 4.</b> Algunos sitios <i>web</i> disponibles en la <i>surface web</i> con contenido proveniente de la <i>darknet</i> . Última actualización 31/1/18. ....  | 35 |
| <b>Tabla 5.</b> Herramientas de análisis del tráfico de datos más populares hasta enero de 2018. ....   | 51 |
| <b>Tabla 6.</b> Tabla que muestra los 13 motores de búsqueda <i>web</i> más utilizados a nivel mundial hasta enero de 2018. ....  | 68 |
| <b>Tabla 7.</b> Los cinco motores de búsqueda <i>web</i> más utilizados en Rusia, así como el tiempo en promedio y el número de páginas de cada sitio visitadas a diario en ese país.. Última actualización 15/2/18. .... | 85 |

## Índice de mapas

|   |     |
|---|-----|
| <b>Mapa 1.</b> Mapa del uso en promedio de <i>Tor browser</i> en cada país del mundo hasta julio de 2013. ....  | 33  |
| <b>Mapa 2.</b> Porcentaje de usuarios de Internet en proporción con la población total por países en 2016. ....   | 65  |
| <b>Mapa 3.</b> Mapa que muestra las páginas más visitadas y la cantidad aproximada de .....   | 72  |
| <b>Mapa 4.</b> Redes sociales más usadas en el mundo hasta enero de 2018. ....  | 91  |
| <b>Mapa 5.</b> Países del mundo sujetos de los principales ataques de VANT de combate y las correspondientes operaciones militares, así como el número aproximado de abatidos (militares y civiles ) de 2002 a 2018. .... | 131 |

## Índice de esquemas

|   |    |
|---|----|
| <b>Esquema 1.</b> Árbol de la clasificación del malware por laboratorios Kaspersky. El orden de amenaza va de la parte inferior a la parte superior, donde se encuentran las amenazas más grandes. .... | 43 |
| <b>Esquema 2.</b> Alphabet (Google antes de la reforma interna) y sus subsidiarias principales. ....  | 77 |

## Índice de ilustraciones

|   |     |
|---|-----|
| <b>Ilustración 1.</b> El camión que atropelló a la multitud visiblemente baleado por la policía. .... | 109 |
| <b>Ilustración 2.</b> El camión del terrorista. ....  | 109 |



## INTRODUCCIÓN

El origen de la Internet se remonta a tiempos de guerra, tiempos convulsos, de profunda competencia y rivalidad, en este caso la Guerra Fría. En 1957 la URSS lanzó el *Sputnik* al espacio, convirtiéndose en el primer país que colocó en órbita un satélite artificial, en respuesta directa los Estados Unidos crean ARPANET<sup>1</sup> (Agencia de Proyectos de Investigación) cuyo propósito fue establecer una red que comunicara a científicos y profesores universitarios al interior de ese país y a lo largo del mundo, afín de desarrollar conocimiento para superar a los soviéticos y continuar en la escalada hacia la hegemonía<sup>2</sup> mundial.

Para 1962 los adelantos eran cuantiosos, ARPANET estaba destinada a expandirse, para conformar una hipotética red mundial de computadoras denominada *Galactic Network*. El amplio panorama a futuro desencadenado por esta nueva alternativa de comunicación pasó en el mismo año a orientarse directamente hacia el campo militar ya que fue Paul Baran un miembro de la RAND Corp. quien destacó la posibilidad de utilizar ARPANET para controlar bombas y misiles en caso de una guerra nuclear<sup>3</sup>, al mismo tiempo posicionando esta tecnología en manos de la fuerza aérea estadounidense.

En este mismo tenor, diez años más tarde, ya con aires plenamente orientados a la seguridad nacional ARPANET cambió su nombre a DARPA (Agencia de Proyectos de Investigación Avanzados de Defensa), simultáneamente fue introducido el protocolo de control de red (Network Control Protocol) que permite a varias computadoras ejecutarse en la misma red con otras. En 1976 una vez más como consecuencia de la ríspida tensión entre las inteligencias de ambos polos de poder (Estados Unidos y la Unión de Repúblicas Socialistas Soviéticas) el bloque

---

<sup>1</sup> Zimmermann Kim Ann & Emspak Jesse, Live Science contributors (2017), *Internet History Timeline: ARPANET to the World Wide Web*, Live Science, [en línea] Disponible en: <https://www.livescience.com/20727-internet-history.html> Consultado el 28/1/18

<sup>2</sup> La posición de ser el más poderoso y fuerte, por lo tanto, capaz de controlar a otros actores de la sociedad internacional. Definición extraída del Diccionario de Cambridge [en línea] Disponible en: <https://dictionary.cambridge.org/us/dictionary/english/hegemony> Consultado el 28/1/18

<sup>3</sup> Rand Corporation (2018) *Paul Baran and the Origins of the Internet*, Rand.org [en línea] Disponible en: <https://www.rand.org/about/history/baran.html> Consultado el 28/1/18



occidental comenzó la creación de un programa satelital que permitiera la vinculación de redes estadounidenses y europeas mediante una constelación de satélites lanzados tanto por la Administración Nacional de la Aeronáutica y del Espacio (NASA) como por la entonces recién creada Agencia Espacial Europea (ESA).

No obstante, es hasta 1981 que la Fundación Nacional de Ciencia mediante la liberación de CSNET 56<sup>4</sup> otorgó la libertad a las computadoras para conectarse a la red sin necesidad de estar vinculadas a las redes del gobierno, lo cual influyó en la expansión desmesurada de los usuarios de la Internet en los Estados Unidos. Tal cambio es en esencia el elemento que diversificó el fomento de usuarios en otros países, en consecuencia, ARPANET la red creada originalmente por y para el gobierno y el ejército estadounidense dejó de existir en 1989.

De este año en adelante los cambios en la Internet estarían orientados a softwares de comunicación, esto no quiere decir que la desvinculación del ejército y el gobierno fuera un hecho pues durante todos estos años, el desarrollo de la Internet fue vigilado de cerca por los creadores de su antecesor, ya que aún y con la eliminación de ARPANET la Internet continuaría trabajando hasta la actualidad con el mismo protocolo standard<sup>5</sup> creado por Vinton Cerf de la Universidad de Standford y Bob Kahn de DARPA en 1973. De tal suerte que la desaparición de la red anterior no significó otra cosa que la erradicación de un elemento que ya era obsoleto y la evolución del control del gobierno y el ejército detrás de las cortinas.

Pero la senda descentralizada de objetivos militares emprendida desde 1989 no fue sino el reflejo del contexto mundial, la URSS se acercaba a su implosión y la imposición de Estados Unidos como la superpotencia en solitario se aproximaba, tardando solamente dos años para volverse oficial su predominio mayoritario al menos durante los siguientes diez años. En la década de 1990 el mundo entraba a la era de la globalización y la drástica innovación de las telecomunicaciones, así como del mundo digital, con la preponderancia incondicional del neoliberalismo.

---

<sup>4</sup> Computer Science Network, fue una red desarrollada por la National Science Foundation como una vía alternativa, no vinculada directamente con el Departamento de Defensa.

<sup>5</sup> Zimmermann Kim Ann & Emspak Jesse, Live Science contributors *op. cit.* Nota 1..



A principios de 1990, el investigador inglés Tim Berners-Lee programador en la Organización Europea para la Investigación Nuclear, más conocida como CERN, con sede en Ginebra, Suiza, concluyó la creación del sistema de servidores de Internet<sup>6</sup> llamado WorldWideWeb (WWW)<sup>7</sup>, comúnmente conocido como la web; un espacio en donde documentos e información, identificados vía UR<sup>8</sup> e interconectados mediante el lenguaje HTML<sup>9</sup> conforman su propio título, la red informática mundial. Si bien, no toda la información en la Internet puede ser localizada a través de este sistema de servidores<sup>10</sup>, es el más común que existe.

El eco causado por el fin de una época contribuyó con la entrada de compañías privadas en el ciberespacio, el mercado de las telecomunicaciones en un nuevo campo como la Internet comenzaba su apertura. En 1991 el gobierno de los Estados Unidos dio “luz verde” a las empresas comerciales para tener un lugar en la red. La praxis y la funcionalidad fueron los componentes a mejorar durante esta década, es por eso, que ya en 1990 la Universidad McGill creó el primer buscador web denominado *Archie Search Engine*<sup>11</sup>.

Posteriormente la optimización y la aparición de nuevos buscadores *web* tal como *Netscape browser*, creado en 1993 por NCSA, el surgimiento de nuevas redes y la entrada del comercio electrónico, fue que la Internet se convirtió en el señero que conduciría a todas las grandes innovaciones ulteriores. Por ejemplo, en 1999 apareció la tecnología Wireless denominada 802.11b conocida corrientemente como Wi-Fi como una consecuencia de la exitosa funcionalidad de la Internet.

Ya en 2001 era claro que el ciberespacio había rebasado la centralización de los ordenadores y alcanzaba el terreno de la telefonía celular, en ese año *Blackberry* creó el primer celular conectado a la Internet. En un avance progresivo el campo del

---

<sup>6</sup> *Idem*.

<sup>7</sup> Gruchawka S. d(2006) How-To Guide to the Deep Web for IT Professionals. TechDeepWeb.com [en línea] Disponible en: <http://techdeepweb.com/3.html> Consultado el 7/8/16

<sup>8</sup> Del inglés Uniform Resource Locator, Localizador de recursos uniforme.

<sup>9</sup> Del inglés HyperText Markup Language, Lenguaje de marcas de hipertexto.

<sup>10</sup> De hecho, tomando en cuenta que la red informática mundial (WWW) o web, únicamente soporta documentos disponibles en la Surface Web, este sistema de servidores no tiene en su disponibilidad ni capacidad el ingreso a la Deep Web, donde se encuentra la mayor parte del contenido de la Internet.

<sup>11</sup> The History of SEO (2017) *Short History of Early Search Engines*, Thehistoryofseo.com [en línea] Disponible en: [http://www.thehistoryofseo.com/The-Industry/Short\\_History\\_of\\_Early\\_Search\\_Engines.aspx](http://www.thehistoryofseo.com/The-Industry/Short_History_of_Early_Search_Engines.aspx) Consultado el 28/1/18

ciberespacio se ensanchó, y comenzó su escalda hacia la conexión directa con cada uno de los usuarios de la red en todo el mundo, tanto así que para 2005 *Youtube* fue creado, y la cantidad de sitios web en línea rebasaba los noventa millones<sup>12</sup>.

La monopolización comercial se extendió con facilidad por Internet, en 2008 Google alcanzó un índice mayor a un billón de URLs, cuya cobertura está presente en casi todo el mundo y es utilizado como buscador web principal en tres cuartas partes del mapa político mundial. En la actualidad el impacto de la Internet está presente en aspectos públicos y privados de los usuarios, la cobertura de la red aún tiene muchos lugares a donde llegar, países y poblaciones marginadas, esparcidas por todo el hemisferio, pero principalmente en los territorios antaño colonias europeas, lugares asolados por el fuego del enfrentamiento indirecto de las dos superpotencias en el mundo bipolar.

Sin embargo, es un hecho que en nuestro tiempo la cantidad de actividad que anteriormente debía ser presencial se realiza a través del ciberespacio. De ahí que los marcos de regulación social, jurídico etcétera, estén siendo reproducidos en el mundo de la *web*. Consecuentemente el ciberespacio se torna un mundo más real y hasta cierto punto se el podría considerar más tangible, la realidad virtual es una realidad, y los mismos controles que existen en la sociedad habitual han sido no solo trasladados si no mejorados hacia este campo, de esta manera la Internet ofrece un panorama a escala del funcionamiento del mundo tangible, elementos sobran para comprobarlo: opinión pública, comercio, trámites administrativos, ciberterrorismo, transacciones bancarias, sin mencionar los marcos jurídicos, entre muchos otros pilares que conforman la atmósfera de la sociedad mundial.

Conjuntamente teniendo en cuenta la definición de Michel Foucault acerca de la verdad y su relación intrínseca con el poder, en esta investigación se concibe a la sociedad como una sociedad global, organizada en un orden multipolar, interconectada por la tecnología y donde las distintas formas de crear la verdad por cada sociedad son absorbidas y transgredidas por los regímenes construidos por las

---

<sup>12</sup> Éxito Exportador (2015) Estadísticas Mundiales del Internet 2005. Exitoexportador.com [en línea] Disponible en: <http://www.exitoexportador.com/stats.htm> Consultado el 5/5/16



economías más importantes del mundo, cuyo potencial de imposición directo e indirecto sobre los actores que conforman sus zonas de influencia se fortalece por medio de la progresiva capacidad de la Internet.

*“La verdad es una cosa de este mundo: se produce solo en virtud de múltiples formas de restricción. E induce efectos regulares de poder. Cada sociedad tiene su régimen de verdad, su "política general" de la verdad: es decir, los tipos de discurso que acepta y hace funcionar como verdadero; los mecanismos e instancias que le permiten a uno distinguir declaraciones verdaderas y falsas, los medios por los cuales cada uno es sancionado; las técnicas y procedimientos acordados de valor en la adquisición de la verdad; el estado de quienes están a cargo de decir lo que cuenta como verdadero”<sup>13</sup>*

Hoy, actividades cotidianas que antes de la creación de la Internet sólo se podían realizar de manera presencial como el enviar o recibir correos, efectuar pagos o buscar información se pueden hacer a través del ciberespacio. La tecnología y concretamente la Internet se interna progresivamente en la vida humana, transformando radicalmente la realidad social en general ¿o es que más bien como humanidad estamos transformando está última y adecuándola al ciberespacio? Lo cierto es que la tecnología interconectada se ha adaptado a la humanidad y la humanidad a esta, el mundo digital o bien las empresas que le concibieron han captado necesidades de la sociedad y han adecuado a la tecnología para volverlas más sencillas de realizar.

Por otro lado, la humanidad ha desarrollado ciertas patologías tales como pasar al menos más de ocho horas diarias (datos de 2015) adheridos a la pantalla de nuestro ordenador, celular, tableta<sup>14</sup>.

---

<sup>13</sup> Foucault, Michel Rabinow, Paul (editor) (1991) *The Foucault Reader: An introduction to Foucault's thought*, PDF , Penguin. pp. 72-73. Disponibles en: [https://monoskop.org/images/f/f6/Rabinow\\_Paul\\_ed\\_The\\_Foucault\\_Reader\\_1984.pdf](https://monoskop.org/images/f/f6/Rabinow_Paul_ed_The_Foucault_Reader_1984.pdf) Consultado el 28/1/18

<sup>14</sup> Davies, Madlen (2015) "Average person now spends more time on their phone and laptop than SLEEPING, study claims" *Daily Mail*, Dailymail.com Disponible en: <http://www.dailymail.co.uk/health/article-2989952/How-technology-taking-lives-spend-time-phones-laptops-SLEEPING.html> Consultado el 28/1/18



Un hecho innegable que necesidades que no existían hace quince años se han vuelto parte de la vida diaria de la audiencia de la Internet, incluso trastornos como la nomofobia<sup>15</sup> han revolucionado el entendimiento médico del funcionamiento del ser humano y su relación con aparatos electrónicos.

No se está sugiriendo que todos los cambios que trajo la última revolución tecnológica hayan ido en detrimento de la salud y el bienestar humano, puesto que gracias a la Internet las comunicaciones se han diversificado y las fuentes a las que se puede acudir para consultar eventos son innumerables, lo cual no significa que sean realmente alternativas, pero de eso se hablará más tarde.

Por otra parte, para la comprensión del objeto de estudio de esta investigación, el cual es la Internet entendido como una herramienta empleada en las relaciones políticas y económicas existentes entre grupos de poder a escala mundial se apela a la teoría de sistema-mundo elaborada por Immanuel Wallerstein<sup>16</sup>, interpretado como un sistema social asentado en la división de trabajo en todo el mundo y compuesto por sistemas culturales representados en civilizaciones y/o países. Asimismo, a pesar de tratarse de una construcción elaborada en el siglo pasado, el sistema-mundo constituye una unidad de análisis conveniente para comprender el contexto del sistema internacional en el siglo XXI, regido por un orden multipolar protagonizado por grupos de poder a su vez a la cabeza de Estados que representan bloques comerciales y políticos.

De este modo a lo largo de la presente investigación se exponen los más importantes mecanismos y estrategias a través de la Internet utilizados por los grupos de poder a la cabeza de los Estados con las economías más avanzadas, afín de perpetrar el control social y redoblar su capacidad de incidencia sobre las decisiones de otros actores internacionales, que van desde otros Estados, hasta empresas y sobre todo el individuo mismo. También, analizando a la red informática mundial más allá que como un medio incentivo de la dinámica económica crucial

---

Read more: <http://www.dailymail.co.uk/health/article-2989952/How-technology-taking-lives-spend-time-phones-laptops-SLEEPING.html#ixzz5BxD4LKVZ>

Follow us: @MailOnline on Twitter | DailyMail on Facebook

<sup>15</sup> Del inglés *no-mobile-phobia* es el miedo irracional a estar sin teléfono móvil, ligado a la obsesión de consultar los mensajes cada pocos segundos.

<sup>16</sup> Wallerstein Immanuel (2005) *Análisis de Sistemas-Mundo*, Siglo XXI, 153 pp.

para la globalización del mercado en prácticamente cada categoría del consumo humano, como una herramienta con influencia permanente e *increcendo* en la dinámica de poder del siglo XXI tanto de forma sistematizada en países centrales y periféricos como a escala global.

El análisis de esta investigación parte de un razonamiento deductivo, es decir de la premisa general del Internet como instrumento de control a nivel del sistema-mundo entendido como una totalidad hasta casos particulares que ejemplifican la aplicación de esta herramienta tecnológica a nivel local, en otros términos, desde el estudio del impacto de la Internet como medio de manipulación de la sociedad en general junto a la segregación de la información en pro de las élites<sup>17</sup> políticas y económicas, pasando por la pugna por el control del tráfico informático entre Estados que representan los intereses de bloques regionales, políticos y comerciales y finalmente culminando con casos específicos en donde estrategias y actos políticos como la censura y el terrorismo acentúan sus alcances a través de la Internet, siendo ejecutados de distinta forma en los países del centro <sup>18</sup>, semi-periféricos <sup>19</sup> y periféricos<sup>20</sup> del mundo.

---

<sup>17</sup> De acuerdo con Gaetano Mosca se trata de un grupo compuesto por la minoría de personas que detentan el poder en una sociedad. Reyes Román, Diccionario Crítico de Ciencias Sociales, Teoría de las élites, [en línea] Disponible en: [http://webs.ucm.es/info/eurotheo/diccionario/E/teoria\\_elites.htm](http://webs.ucm.es/info/eurotheo/diccionario/E/teoria_elites.htm) Consultado el 28/1/18

<sup>18</sup> Los países con mayor capacidad económica, como Estados Unidos y los Estados de Europa Occidental aquellos donde se asientan los centros políticos y económicas dentro de los cuales se lleva a cabo la toma de decisiones impuestas sobre las zonas periféricas.

<sup>19</sup> Países con características propias tanto de los países del centro como de la periferia, algunos de estos tienen la capacidad para rivalizar con los países del centro y por lo general funcionan como países de transición de los productos y tecnología provenientes tanto del centro como de la periferia.

<sup>20</sup> Se trata de los países productores y exportadores de materias primas, en este contexto especialmente quienes exportan los recursos con los que se crea y produce la tecnología en los países del centro y algunos semi-periféricos.



# 1. INTERNET, HERRAMIENTA DEL ESTABLISHMENT PARA LA RETENCIÓN INFORMÁTICA SISTEMATIZADA

## 1.1. El *establishment*

Ya se tiene claro el potencial de la Internet como una herramienta eficiente y funcional capaz de interconectar a miles de usuarios entre sí sin importar la latitud desde donde naveguen, ahora bien, es necesario puntualizar que un instrumento de este potencial es cardinal para imponer control en la sociedad mundial. Pero ¿a qué se alude cuando se señala la reticente presencia de grupos de poder que gestionan, planifican y de acuerdo con intereses particulares se disputan entre sí el control del comportamiento social por medio de la red informática mundial? La presente investigación concibe a estos grupos de poder como el *establishment* entendido como “el grupo de personas importantes y poderosas que controlan un país o una organización, especialmente aquellos que apoyan la situación existente, el *statu quo*<sup>21</sup> internacional”<sup>22</sup>, adicionalmente dichos grupos actúan mediante poderes de hecho o fácticos que según la Enciclopedia de la Política de Rodrigo Borja:

*Son las potestades públicas que no surgen de la ley, ni están en ella regladas, sino que nacen de la dinámica de las relaciones sociales. No son por tanto poderes formales, jurídicamente regulados, sino poderes informales que están al margen de la previsión de la ley y que son ostentados y ejercidos de facto por individuos o grupos para defender intereses económicos y sociales de carácter particular dentro de la comunidad política*<sup>23</sup>.

<sup>21</sup> Del latín. El estado actual de las cosas en cualquier fecha dada. Definición extraída de The Free Dictionary by Farlex, en línea, consultado el 28/1/18 Disponible en: <https://legaldictionary.thefreedictionary.com/status+quo>

<sup>22</sup> Definición extraída del Diccionario de Cambridge en línea, Disponible en: <https://dictionary.cambridge.org/dictionary/english/establishment> Consultado el 28/1/18

<sup>23</sup> Borja. R. Enciclopedia de la política. Poderes fácticos. [en línea] Disponible en: <http://www.encyclopediadelapolitica.org/Default.aspx?i=&por=p&idind=1192&termino=> Consultado el 25/7/16.

En otros términos, una red de *lobbys*<sup>24</sup> íntimamente vinculados que tienen la potestad de las decisiones sobre los Estados más poderosos y que, hasta la actualidad ostentan el protagonismo central en el escenario internacional. Aunque es verdad que las empresas privadas de alcance internacional comienzan a tomar mayor terreno en la toma de decisiones y son más influyentes que muchos Estados, un hecho fehaciente es que las más grandes economías y potencias militares continúan siendo mediáticamente quienes aglutinan el arbitraje del mundo.

Conjuntamente, realmente hoy se puede identificar los medios esenciales para dominar al mundo, la receta “mágica” utilizada por los poderosos desde que el planeta fuese gobernado. Los actores que poseen control sobre la información y el conocimiento, acompañado de otras dos fuentes de poder entendidas como la capacidad de ejercer coerción e imponer decisiones sobre las de otros actores, además del potencial económico y tecnológico ostentan un margen de maniobra solamente equivalente a otros grupos de poder.

Por supuesto el rol de la Internet está centrado en el campo del conocimiento, empero, se debe tener muy claro que la potencia de este medio consiste en la sinergia con las otras dos fuentes de poder. De esta forma no se puede crear una estrategia sin tener los medios ni la capacidad de acción para ejecutarla, o bien con la falta de cualquiera de estas facultades.

Históricamente la manera en la que los grupos de poder influyen en el pensamiento, la opinión y las acciones de la población mundial se puede dividir en dos vertientes esenciales actualmente relacionadas entrañablemente con la red informática mundial: la educación e intimidación, mediante los programas educativos de alcance global y los medios de comunicación exhibidos directa e indirectamente en la *Surface web*. Además de esas dos, se pueden emplazar también al monitoreo sistematizado de usuarios como otro de los mecanismos que

---

<sup>24</sup> Entendidos como los grupos de presión que ejercen el *lobbying*: la práctica y proceso de influenciar en políticas públicas y gubernamentales a todos los niveles: federal, estatal y local. Definición extraída de The Free Dictionary by Farlex *op.cit.* Nota 21. Disponible en: <https://legal-dictionary.thefreedictionary.com/Lobbying>



recientemente se han implementado y del que también se hablará a lo largo de este capítulo.

## 1.2. Educación y medios de comunicación

En realidad, la educación y los medios de comunicación son íntimamente concernientes, se trata de una sociedad de herramientas que funciona con el respaldo de la otra, cuya incidencia se ve potenciada en grande con ayuda de la Internet. La adaptación de ambas al ciberespacio significó la optimización de su fuerza de impacto, ya que en un instante la versión de los hechos acontecidos o las posturas de figuras políticas determinadas arriban a los millones de usuarios que han reemplazado el papel periódico y la televisión por su ordenador, teléfonos móviles y tabletas, o bien están en la etapa de transición.

La Internet ofrece un panorama auténticamente revolucionario y sectores tan cruciales como la educación familiar y escolar son objeto de constante instigación. Tal es el nivel de influencia que ha alcanzado el ciberespacio como un dominio de intercambio de información donde las fronteras no existen, que, la capacidad de reproducción de los sistemas educativos establecidos por las instituciones mundiales como la OCDE, UNESCO, es mucho más digerible, no solamente por su rápida transferencia sino por la falta de pensamiento crítico de los receptores. La humanidad ha sido educada para confiar en las instituciones inexorablemente, para creer que las medidas y los programas impuestos son para el bien colectivo. Sin embargo, como Jose Luis Camacho señala:

*Quizá la policía no esté solo para proteger a los ciudadanos, ni la medicina para curarnos, o nuestros respetables políticos para atender los intereses de las personas a las que representan. Quizá lo que pretendan sea algo diametralmente opuesto a lo que a usted le han hecho creer [...] Nacemos con la idea de que las instituciones internacionales o nacionales más importantes tienen una función específica, pero nunca sospechamos que detrás se esconde la ofuscación, la mentira, los intereses y, por supuesto,*

*su propia supervivencia a cualquier precio, por encima de la imagen mediática que tenemos de la institución*<sup>25</sup>.

La educación representa el componente inicial en la formación del individuo y en tanto las nuevas tecnologías se vayan incorporando a su construcción los usuarios crecen asimilando a la Internet como un incuestionable aliado. El problema no sólo es que se le considere así a la red, sino que ni siquiera se imagina quién o qué se encuentra detrás del telón y no muy a menudo se indaga a propósito de porqué cuando se navega, solo se encuentra determinada información sospechosamente selecta.

Teniendo como premisa que el periodo de la vida en el que el humano recibe y aprehende más información comienza desde la niñez y finaliza en la juventud se entiende que los jóvenes son el principal objetivo de las medidas grabadas, ya que se trata de la población más vulnerable, fácil de influenciar y manipular. Según datos de Statista.com casi el 40%<sup>26</sup> de la población mundial activa en Internet, se ubica entre los 16 y 34 años de edad, y solamente de los 16 a los 24 años conforman el 19.8% de usuarios en el planeta.

La gran mayoría del contenido en la Internet reproducido en la actualidad está dirigido precisamente hacia la población más activa en la *web*, alterando el comportamiento del ser humano, interviniendo en los pilares del desarrollo del individuo. Las “nuevas necesidades” son una creación cuyo impacto y funcionalidad ha repercutido indudablemente en el comportamiento de la sociedad actual, las cuales generalmente nadan en lo superfluo, atrapadas en la porción del baladí y la redundancia informática; entre ellas se encuentra la captura constante de *selfies*, realizar películas de su propia vida en *Facebook*, en otros términos, una oda a la distracción, la banalidad y el egocentrismo exacerbado, obsesiones con las que el ser humano no tuvo que lidiar hasta la contemporaneidad. Por otro lado, de manera descabellada el usuario es capaz de adoptar el manejo de aseveraciones que

---

<sup>25</sup> Camacho J. L. (2015) *La conspiración reptiliana y otras verdades que ignoras*. España. Ediciones Planeta. p.18 Consultado el 27/7/16

<sup>26</sup> Statista. *Distributioj of Internet users worldwide as of 1<sup>st</sup> quarter 2017, by age group*. Statista.com [en línea] Disponible en: <http://www.statista.com/statistics/272365/age-distribution-of-internet-usersworldwide/> Consultado el 2/2/18

sostienen fervientemente que este tipo de actividades son verdaderamente imprescindibles.

El núcleo de este tema radica en la facilidad con la que no sólo este porcentaje de usuarios sino la población activa en la Internet absorbe sin más las adaptaciones que significan los avances en la tecnología digital e informática. Por otra parte, todo este tipo de actividades promocionales se realizan a partir de estudios especializados y pedagógicos afín de que su captación se presente de manera empática.

Por añadidura, se emplaza al paralelo de las “nuevas necesidades” una cualidad axiomática <sup>27</sup> atribuida a todo lo transmitido por algún medio de comunicación prestigioso acerca de cualquier personaje, evento o noticia en el mundo. Asimismo, se traduce el desarrollo de esta rápida forma de captar información hacia el espionaje cibernético (a nombre de la seguridad), opiniones y orientaciones laborales, estereotipos, y pasatiempos.

Se trata de un marco canalizado a la promoción absoluta de la iniciativa privada en la red, trasladada a su aplicación en el mundo real en el que, el fomento de la competencia y la especialización conforman los pilares cruciales para la planificación a futuro de la sociedad. En un mundo volcado hacia el centro, donde naturalmente la colectividad no sea considerada como un elemento útil y esté en efecto solapada por la individualidad.

### 1.3. Contagio del pesimismo mediático

Para la supervivencia del *statu quo* mantenido desde el final de la Guerra Fría es sustancial una población que confíe en él, pero, si no toda la población lo hace ciegamente, el siguiente recurso es el miedo por medio de la intimidación o la sugestión. El rol de la Internet en esta labor es axiomático, máxime cuando se trata de imprimir trastornos puramente hipocondriacos<sup>28</sup>, además de la paranoia.

---

<sup>27</sup> La cual ha perdido el gobierno, por la acumulación de contenido crítico difundido en las redes sociales que han puesto en *boga*.

<sup>28</sup> Término empleado para designar a aquellas personas que demuestran permanente y constante sensación de estar enfermos, incluso cuando están físicamente saludables. Definición extraída de: Mayo Clinic (2018) *Illness anxiety disorder*, Mayoclinic.org [en línea] Disponible en:



Pero no se está aludiendo a una hipocondría ocasionada por enfermedades bilógicas, o de esa naturaleza, más bien a la búsqueda constante de la seguridad a cambio de la llave de la privacidad de los usuarios. Empero, en el caso hipotético en el que las medidas tomadas por las autoridades informáticas estuvieran realmente encaminadas a eliminar el riesgo de infiltraciones, lavado de dinero, robo de identidad, etcétera, ¿por qué mientras más medidas se establecen, el rango de percusión de los crímenes en la *web* se dispara portentosamente al igual que su cantidad?<sup>29</sup>

En septiembre de 2015 el periódico español La Vanguardia señaló el grandísimo escaño con un tamaño de 71% al que los crímenes informáticos habían ascendido en el último año “lo que supone un incremento de más de 10.000 actos ilícitos en la red en solo un ejercicio, y continúa una tendencia que se mantiene desde 2011, con un incremento de un 210 % (a nivel mundial) en cuatro años (hasta 2014)”<sup>30</sup>.

Por supuesto los números son escandalosos, pero eso no es todo, su impresión se refuerza con los datos publicados por la Memoria de la Fiscalía general del Estado (español) 2015 correspondientes a 2014, y cito “la mayor parte de procedimientos abiertos respondieron a estafas, 17.328 de los 20.534 del total, es decir, el 84%. En total, desde que se comenzaran a contabilizar los delitos informáticos en el año 2011, se ha producido un aumento del 210%, al pasar de 6.532 infracciones detectadas en 2011 a las 20.534 que se registraron durante el pasado ejercicio”<sup>31</sup>.

De esta manera se puede reparar en la Internet como una auténtica arma de doble filo, tanto una llave de la información como un riesgo para los datos y privacidad de los usuarios. Ahora bien, es necesario reiterar que para acceder a la

---

<https://www.mayoclinic.org/diseases-conditions/illness-anxiety-disorder/symptoms-causes/syc20373782>

<sup>29</sup> Ver nota 29.

<sup>30</sup> La vanguardia. (2015) *La ciberdelincuencia se dispara un 71% en 2014 y más del 210% en 4 años*. Lavanguardia.com [en línea] Disponible en:<http://www.lavanguardia.com/tecnologia/20150908/54436339519/la-ciberdelincuencia-se-dispara-un-71-en-2014-y-mas-del-210-en-4-anos.html> Consultado el 30/7/16

<sup>31</sup> *ídem*

parte más abundante de la red informática mundial se debe romper primero con algunos candados<sup>32</sup>, lo que se entiende como una contradicción.

#### 1.4. Censura y Limitación Sistematizada de la Información

La revolución tecnológica gestada a finales del siglo XX y potenciada con la entrada al siglo XXI ensanchó indudablemente la relación entre la humanidad y las tecnologías. Para ilustrar, la aparición de la Sociedad del conocimiento<sup>33</sup> y de la información<sup>34</sup> además de la digitalización progresiva de las comunicaciones transformaron la configuración<sup>35</sup> misma de la vida humana, implantado un panorama innovador en el que la interacción entre los humanos y las TIC<sup>36</sup> evocó la necesidad de derechos humanos fundamentales de cuarta generación; enunciados a continuación:

- El derecho de acceso a la informática.
- El derecho a acceder al espacio que supone la nueva sociedad de la información en condiciones de igualdad y de no discriminación.
- Al uso del espectro radioeléctrico y de la infraestructura para los servicios en línea sean satelitales o por vía de cable.
- El derecho a formarse en las nuevas tecnologías.
- El derecho a la autodeterminación informativa.

---

<sup>32</sup> Entrar por medio de buscadores *web* con mayor nivel de privacidad.

<sup>33</sup> La sociedad que integra más allá de los datos, el conocimiento adquirido por estos dentro de las estructuras sociales de poder. Definición extraída de. UNESCO, Foray Dominique (consejero editorial) (2002) *La sociedad del conocimiento*, Revista Internacional de Ciencias Sociales, Unesco.org. PDF, [en línea] Disponible en: <http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/SHS/pdf/171-fulltext171spa.pdf> Consultado el 2/2/18

<sup>34</sup> La sociedad de los meros datos en grandes cantidades. Definición extraída de: UNESCO Foray Dominique *op. cit.* Nota 32.

<sup>35</sup> Que si bien aparece como un fenómeno coaligado a la dinámica capitalista, dicho de otro modo exclusiva de los Estados y agentes que pueden pagar por ella, su propagación es acelerada y continúa abarcando más partes del mundo.

<sup>36</sup> Tecnologías de la Información y Comunicación



- El derecho al *Habeas Data*<sup>37</sup> y a la seguridad digital<sup>38</sup>.

Asimismo, es pertinente retomar que esta flamante generación de derechos retiene la idea fundamental de la libertad como la base de todas las garantías, sus posteriores modificaciones son netamente superficiales y solo responden a su adaptación al entorno actual. La Declaración Universal de Derechos Humanos en su artículo 19 se mencionaba que:

*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*<sup>39</sup>.

Por otra parte, desde el punto de vista teórico Federico César Lefranc Weegan sostiene que “ni estructural ni funcionalmente el derecho a internet está concebido como un derecho humano. Ni como un derecho humano individual, ni como uno social [...] el núcleo básico de los derechos humanos es un valor. Internet no es un valor como tal”<sup>40</sup>.

No obstante, se considera que los avances tecnológicos y el pulso de innovación en el que sintoniza la humanidad se dirige inevitablemente hacia una época en la que las TIC abarcaran sino es que ya ostentan un rol neurálgico en el desarrollo de la civilización. De modo que para el entendimiento más aclimatado a los nuevos tiempos es fundamental concebir el derecho a la Internet y la libertad de navegación como un elemento consustancial.

Existe una idea que en la actualidad parece muy común escucharla en todos los medios de comunicación, a tal grado que en verdad se reconozca a la Internet

---

<sup>37</sup> Derecho a la intimidad en el derecho informático.

<sup>38</sup> Graciano, Ambar (2013) *Los derechos humanos de tercera y cuarta generación*. Encuentro jurídico. [en línea] Disponible en: [http://www.encuentrojuridico.com/2013/01/los-derechos-humanos-de-terceray.html#/\\*\\*](http://www.encuentrojuridico.com/2013/01/los-derechos-humanos-de-terceray.html#/**) Consultado el 30/8/16

<sup>39</sup> Organización de las Naciones Unidas. (1948) *Declaración Universal de los Derechos Humanos*, United Nations. [en línea], Disponible en: <http://www.un.org/es/documents/udhr/> Consultado el 12/8/16

<sup>40</sup> Weegan Lefranc (2015) *Tera Incógnita Bases para una política criminal pro persona en la Sociedad Digital*, Infotec Centro de investigación e Innovación en Tecnologías de la Información y Comunicación, CONACYT, p.25. Consultado el 12/8/16



como un medio que, como señala Bruce Schneier “empodera a los desapoderados”<sup>41</sup>, en otras palabras, que les da voz a los agentes frente al resto de actores de la sociedad mundial, empero, realmente en caso de que tal cosa sea entendida como poder, ¿no está a disposición de todos? es decir, de quienes tienen la capacidad económica para poder conectarse al *Wi-fi*. Esto es, y ¿quién creo la Internet?, ¿quién la controla?, ¿quién aporta más a su crecimiento y optimización tecnológica?

¿Acaso el establishment es portador de tanta ingenuidad como para crear una tecnología sin que esta pueda ser utilizada por los mismos para perpetrar su poder?, es evidente que no.

El discurso es otro de los artefactos más poderosos que posee la humanidad desde tiempos ancestrales, y junto con la ignorancia es capaz de sacudirse la mitad de las sospechas acerca de la existencia real de un sub-mundo en el ciberespacio donde se podría recabar tanta información como fuese posible para aseverar la existencia de lo que siempre se ha negado: la economía basada en prácticas ilegales pero necesarias para la subsistencia del sistema actual, asentada en mercados donde los mismos actores internacionales que buscan hipócritamente su erradicación les han creado y los continúan reproduciendo. Naturalmente, los datos que desvelan este tipo de información se encuentran completamente cerrados al público, y ya sean personas físicas o morales quienes intenten destapar la cloaca, son censuradas, corrompidas, cooptadas o reprimidas inmediatamente, de tal suerte que encontrar contenido en la *web* que indague realmente más profundamente que fuentes supuestamente alternativas comprende una dificultad superior.

No se está sugiriendo que sea realmente necesario, después de tener en cuenta el exclusivismo y hermetismo en donde vivimos, mencionar la rotunda violación de la Declaración Universal de Derechos Humanos ya que, al final debería ser entendida más como un elemento político y parte efectivamente de la demagogia que como un documento destinado realmente a la consecución del bienestar común. Con todo, se estima que no puede ser obviada, y en su lugar se ha emplazado como

---

<sup>41</sup> Schneier B. (2013), *What should we be worried about?* Edge.com [en línea] Sitio web: <https://www.edge.org/response-detail/23818> Consultado el 25/7/16



una ejemplificación más de la paradoja y el contrasentido de los discursos y las acciones en el sistema internacional.

Muchas veces se confunden documentos como la Declaración y otros de la misma estirpe como un punto y aparte de la política, e incluso afirman que son víctimas de un sistema que no los comprende, no obstante, si en lugar de que se les entendiera así se les visualizase como herramientas muchas de las cosas aparentemente inexplicables, encontrarían su esclarecimiento.

Los filtros de información a los que se ha aludido en otro momento son componentes cruciales para la limitación de la información. Además, encontramos también a las redes de corrupción, y represión informática como otros de los medios para modelar la difusión de eventos y datos hacia una vía en particular.

Un hecho irrevocable es que la gigantesca expansión de la Internet en sí misma está ligada a factores económicos y políticos. Naturalmente el flujo de su crecimiento se concentra hasta la actualidad en las economías más grandes del mundo y en muy menor medida en sus áreas de influencia, el resto de las regiones del planeta aún se encuentra en un plano relegado.

Según los datos del Banco Mundial, la expansión de los usuarios de la Internet desde 1990 a 2016 se ha disparado estrepitosamente puesto que, en promedio, de cada país 45 personas sobre 100 navegan en la red<sup>42</sup>. Lo que significa que al menos el 40% de la población mundial se ve afectada directamente por el manejo de sus datos y la lluvia de información preseleccionada.

Pero antes de pasar a la categorización de la información es necesario señalar la importancia de la expansión progresiva de la audiencia internauta en países periféricos, si bien ya se ha mencionado que el foco de expansión se ubica sobre todo en los países más desarrollados, de 2013 a 2015 la media de población de países emergentes y en desarrollo que usaron Internet o tienen un *smartphone* pasó de 45% a 54% en 2015, es decir que aumentó 9%<sup>43</sup>. La mayor parte de ese crecimiento se debe a economías emergentes como Malasia, Chile o Brasil. En Brasil por ejemplo el 60% de la población ya sea usa Internet al menos de forma ocasional o posee un

---

<sup>42</sup> Ver gráfica no.1

<sup>43</sup> Ver tabla no.1

smartphone. Cabe destacar que el mayor índice de crecimiento se ubica en Turquía, al pasar de 41% a 72% en dos años. En Latinoamérica, la lista es encabezada por Chile con 78%, Argentina con 71%, Venezuela 67%, Brasil 60%, México 54% y Perú 52%. No obstante, el acceso a la Internet en los países con economías avanzadas continúa inclinando la balanza por mucho. Lo anterior de acuerdo a los datos más actuales recabados por el *Pew Research Center*.

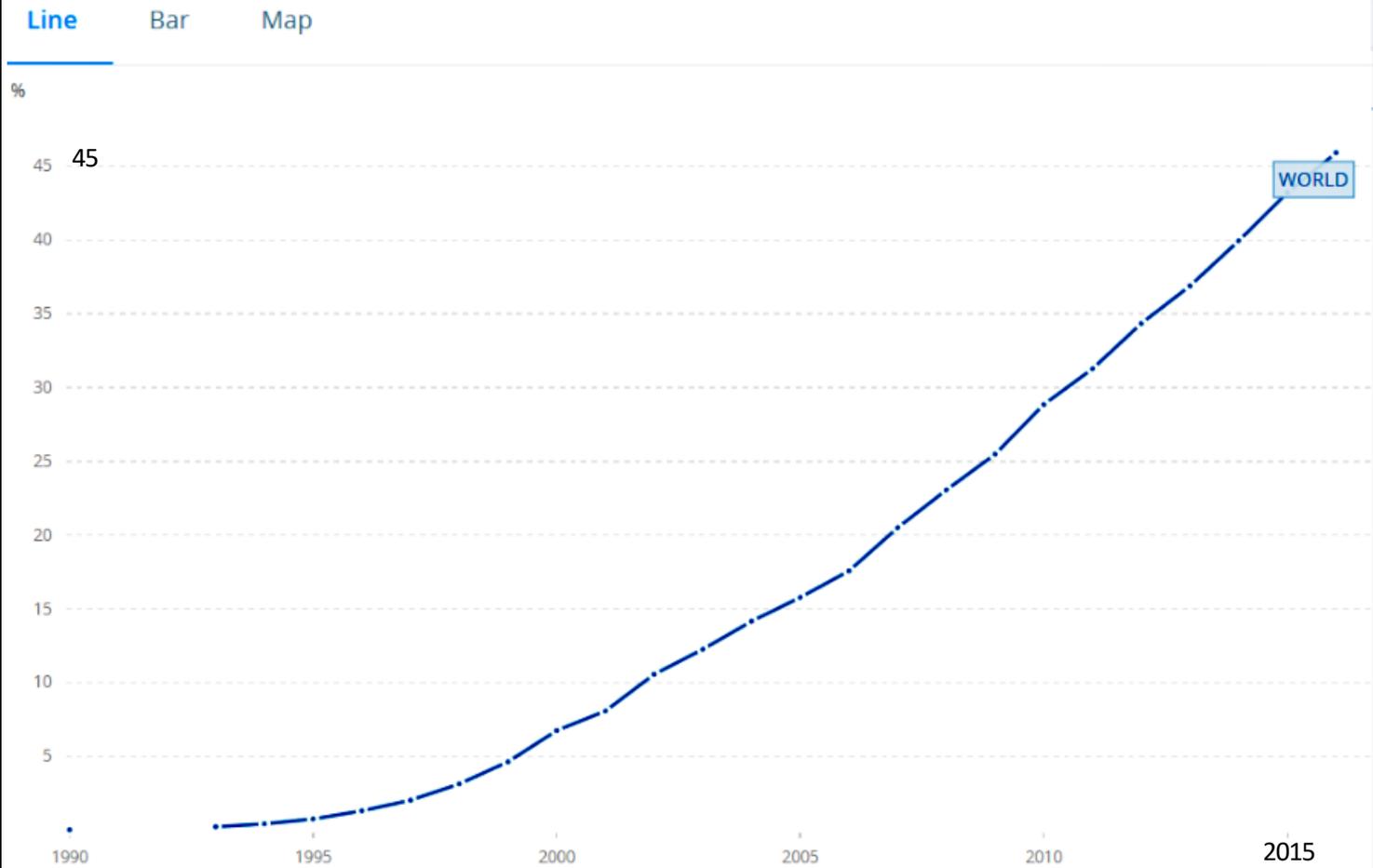
|           | 2013<br>% | 2014<br>% | 2015<br>% | 12-15<br>Cambio |
|-----------|-----------|-----------|-----------|-----------------|
| Turquía   | 41        | -         | 72        | +31             |
| Jordania  | 47        | 47        | 67        | +20             |
| Malaysia  | 49        | 55        | 68        | +19             |
| Chile     | 66        | 76        | 78        | +12             |
| Brasil    | 49        | 51        | 60        | +11             |
| Líbano    | 57        | 62        | 66        | +9              |
| México    | 45        | 50        | 54        | +9              |
| Venezuela | 59        | 67        | 67        | +8              |
| Indonesia | 23        | 24        | 30        | +7              |
| Pakistán  | 8         | 8         | 15        | +7              |
| Rusia     | 66        | 73        | 72        | +6              |
| Polonia   | 63        | 63        | 69        | +6              |
| Filipinas | 34        | 42        | 40        | +6              |
| Nigeria   | 33        | 49        | 39        | +6              |
| India     | 16        | 20        | 22        | +6              |

Tabla 1. Tabla comparativa que muestra el incremento de usuarios de la Internet y propietarios de un smartphone en países en vías de desarrollo de 2013 a 2015.<sup>44</sup>

Paradójicamente a la situación económica, política y social en los países periféricos y del centro, el fenómeno de la limitación de la información es similar en ambos. Debemos entenderle como un sistema que aplica en primera instancia este

<sup>44</sup> Pew Research Center (2016) *Internet access growing worldwide but remains higher in advanced economies*, Pewglobal.org, [en línea] Consultado el 28/1/18 Disponible en: <http://www.pewglobal.org/2016/02/22/internet-access-growing-worldwide-but-remains-higher-in-advanced-economies/>

tipo de estrategias<sup>45</sup> en el centro y las reproduce (si tienen éxito) en la periferia, todo, evidentemente con fines comerciales, pero también de control social.



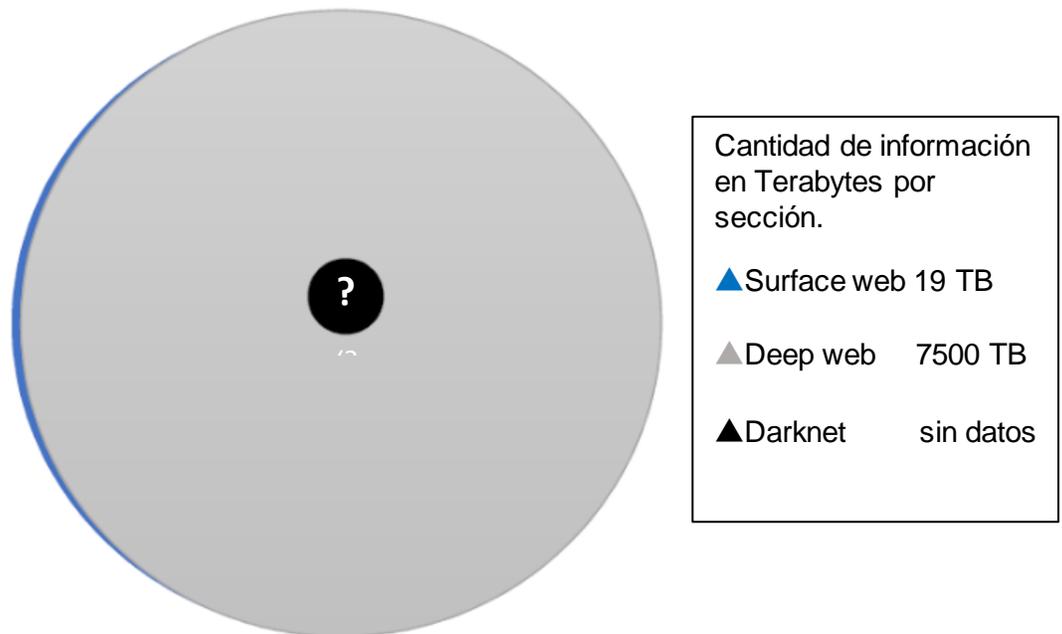
Gráfica 1. Gráfica que muestra el porcentaje de usuarios en la Internet por 100 personas desde 1990 hasta 2016.<sup>46</sup>

<sup>45</sup> Mencionamos “este tipo de estrategias” para referirnos a estrategias comerciales, y a las capacidades de un actor englobadas en el término poder blando, acuñado por *Joseph Nye*. Más adelante hablaremos sobre el poder duro (también obra de Nye) aplicado a través de la Internet, cuyo sistema de operación es completamente a la inversa, primero en países periféricos y después con un impacto proporcional en los países del centro.

<sup>46</sup> The World Bank (2016) *Internet Users per 100 people*, The World Bank, Worldbank.org, Última actualización 2016, [en línea] Disponible en: <https://data.worldbank.org/indicador/IT.NET.USER.ZS> Consultado el 28/1/18

Se puede clasificar a la limitación sistematización de la información disponible en la Internet en tres sub-dimensiones principales, la *Surface Web*, *Deep web* y *Darknet*. Siempre teniendo en cuenta la premisa de la Internet como una creación con fines militares, después hecha corriente con otro tipo de objetivos principalmente económicos.

Para entender de forma correcta la estructura de la Internet y la ubicación de las tres sub-dimensiones a las que se hará énfasis a lo largo de esta investigación, es necesario entender la siguiente gráfica:



Gráfica 2. Escala aproximada de la distribución del contenido en la Internet por terabytes<sup>47</sup> hasta 2016.<sup>48</sup>

<sup>47</sup> 1000 Gigabytes (GB).

<sup>48</sup> Elaboración propia. Datos extraídos de S/a. (2016) *The Deep Web*. Hewilson. [en línea] Disponible en: <https://hewilson.wordpress.com/what-is-the-deep-web/statistics/> Consultado el 28/1/18

### 1.4.1. *Surface Web*

Concretamente se alude a solo una parte de la Internet, aquella donde el promedio mundial de individuos navega desde el dispositivo que sea, la *web* superficial (*Surface web*). En ella los contenidos en línea se limitan a las páginas oficiales y autorizadas por el sistema, sin mencionar el rastreo de datos que es sencillamente una realidad incluso conocida por los usuarios. Un espacio exclusivo para el tipo de información sin profundidad, afín de que las búsquedas estén condenadas al enclaustrado paradigma diseñado para alinear el subconsciente de quien navega por esas aguas.

A menudo la *Surface web* se encuentra repleta de páginas de muchos colores, idiomas, ya sea noticieros, redes sociales, *blogs* etcétera, pero cuyo contenido es en el fondo sencillamente el mismo, y ciegamente creemos estar ingresando a fuentes de información realmente alternativas.

En esta parte de la red informática mundial se congrega al menos el 90% de la población mundial de usuarios. La presencia de los medios de manipulación pública, como preferimos llamarlos, es cardinal para la difusión de contenidos selectos que van a parar al criterio propio de quienes se mantienen al día mediante periódicos y revistas electrónicas, ya sea vía “directa” o de una forma todavía más distanciada, a través de *Twitter*, *Facebook* o alguna otra red social.

La aplicación de la impuesta visión estructurada no es estática, puesto que a diario debe ser corroborada por los mismos que crean esa realidad virtual, no se está refiriendo a los medios de comunicación en sí sino al complejo sistema al que rinden réditos. De esta manera cada evento relevante que acontezca en el mundo debe pasar por un filtro de intereses, es decir, antes de ser publicado en cualquier medio en su forma neta debe de ser evaluado y alisado hasta que los grandes intereses que hay detrás (políticos, económicos, etcétera.) no sean perjudicados, sin importar el grado de su implicación.

En realidad, el filtro de información al que se alude actúa tanto a escala global como regional y local, el esqueleto de la estructura jerárquica en esencia es el mismo. El contenido de la *Surface Web* dentro de su limitación obedece a la adaptación de la red informática mundial a los usuarios. Si bien se trata de una orientación al final

dirigida hacia el consumo, la moda y el *marketing*, no deja de ser a primera tendencia entre la población mundial de usuarios.

| Clasificación | Sitio web   | Categoría                                  | Evolución | Duración promedio de la visita | Páginas visitadas |
|---------------|---|--|-----------|--------------------------------|-------------------|
| 1             |  google.com      | Internet and Telecom > Search Engine       | =         | 00:07:07                       | 7.81              |
| 2             |  facebook.com    | Internet and Telecom > Social Network      | =         | 00:13:41                       | 12.63             |
| 3             |  youtube.com     | Arts and Entertainment > TV and Video      | =         | 00:19:56                       | 9.49              |
| 4             |  baidu.com       | Internet and Telecom > Search Engine       | =         | 00:08:49                       | 8.15              |
| 5             |  xvideos.com     | Adult                                      | =         | 00:13:01                       | 10.53             |
| 6             |  yidianzixun.com | Internet and Telecom > Search Engine       | +5        | 00:15:12                       | 7.51              |
| 7             |  google.co.in      | Internet and Telecom > Search Engine       | +1        | 00:07:47                       | 6.56              |
| 8             |  sogou.com         | Internet and Telecom > Search Engine       | -1        | 00:06:23                       | 5.11              |
| 9             |  xnxx.com          | Adult                                      | =         | 00:13:16                       | 10.45             |
| 10            |  yahoo.com         | News and Media                             | -4        | 00:06:14                       | 6.25              |
| 11            |  vk.com            | Internet and Telecom > Social Network      | -1        | 00:17:09                       | 22.13             |
| 12            |  twitter.com       | Internet and Telecom > Social Network      | +2        | 00:08:55                       | 7.45              |
| 13            |  google.com.br     | Internet and Telecom > Search Engine       | =         | 00:08:32                       | 6.96              |
| 14            |  wikipedia.org     | Reference > Dictionaries and Encyclopedias | -2        | 00:03:51                       | 2.91              |
| 15            |  pornhub.com       | Adult                                      | =         | 00:10:43                       | 8.36              |
| 16            |  amazon.com        | Shopping > General Merchandise             | =         | 00:06:51                       | 9.96              |
| 17            |  instagram.com     | Internet and Telecom > Social Network      | =         | 00:06:31                       | 12.03             |
| 18            |  yandex.ru         | Internet and Telecom > Search Engine       | +1        | 00:10:18                       | 8.72              |
| 19            |  live.com          | Internet and Telecom > Email               | -1        | 00:06:32                       | 7.97              |
| 20            |  google.co.uk      | Internet and Telecom > Search Engine       | =         | 00:08:56                       | 6.65              |

Tabla 2. Tabla que muestra los 20 sitios web más visitados del mundo en la Surface web. Última actualización 28 de enero de 2018.<sup>49</sup>

<sup>49</sup> Similar Web (2017) *Top Websites Ranking, Worldwide*, Similarweb.com, [en línea]. Disponible en: <https://www.similarweb.com/top-websites> Consultado el 28/1/18



### 1.4.2. *Deep Web*

Muchos investigadores y especialistas además de opiniones anónimas acerca del ciberespacio sitúan al origen de la *Deep Web* en el momento en el que la Internet fuese activada, específicamente a finales del año 1969, argumentando que como una parte de la red habría comenzado a existir en el momento del propio nacimiento general de la Internet. Lo cierto es que el término Deep Web se encuentra muy relacionado con el anonimato en la web, y hasta cierto punto se le podría considerar como un sinónimo.

Si bien fue hasta el año 2001 que el término Deep Web fue puesto en circulación por Bright Planet<sup>50</sup>, los trabajos conjuntos entre el ejército, el gobierno y las universidades estadounidenses para desarrollar una vía de comunicación que relacionara estaciones de seguridad en el país con agentes de inteligencia en el extranjero sin ser detectada, inició en la década de 1990. No obstante, la especialización en una vía completamente anónima y alternativa a la web tradicional fue impulsada por el Laboratorio de Investigación Naval en 1995 cuyos grandes matemáticos: David Goldschlag, Paul Syverson y Michael Reed comenzaron a trabajar en la creación del “onion routing”, “encaminamiento cebolla” en español<sup>51</sup>.

El fruto de su investigación derivó en el desarrollo de *The Onion Router Project*, mejor conocido como Tor, consolidado hasta 1997. Para este año los objetivos centrales con los que se había iniciado el proyecto, privacidad y anonimato, eran un hecho. En esta etapa dicho equipo de trabajo había conseguido diseñar para el gobierno y la milicia estadounidense un subsistema en la Internet resistente al análisis de tráfico, espionaje y otro tipo de ataques tanto por agentes ajenos al enrutador cebolla como por gente proveniente dentro del mismo enrutador<sup>52</sup>.

Sin embargo, el mundo conoció por primera vez la existencia de Tor en 2004, cuando fue revelado al público por la Marina de los Estados Unidos. Con todo, fue puesto a disposición de la población estándar dos años más tarde, en 2006 (continúa

---

<sup>50</sup> Empresa dedicada al desarrollo de tecnología y búsquedas en el contenido de la Deep Web. [en línea] Disponible en: <https://brightplanet.com/> Consultado el 6/8/16

<sup>51</sup> Syverson. P. (2005) *Onion Routing*. Onionrouter.net [en línea] Disponible en: <https://www.onionrouter.net/> Consultado el 6/8/16

<sup>52</sup> *Ibid.*



vigente) por un grupo de desarrolladores creadores de Tor Project<sup>53</sup> la plataforma en la que se puede descargar el buscador sin complicaciones.

Entre todo el abanico de utilidades que ofrece el anonimato, una vez efectuada su apertura al público en general, la Deep Web (principalmente vía Tor) emprendió de manera rauda la metamorfosis para adaptarse a las necesidades de la nueva población que se aventuraría por sus aguas, pero muy claramente bajo sus propios términos. De modo similar a la comercialización del uso de los satélites de comunicaciones y rastreo, producidos por los gobiernos de las grandes economías mundiales<sup>54</sup> y empresas trasnacionales alquilados por los mismos, el empleo de la Deep Web trasmuto en todas direcciones, generalmente lucrativas, desde la venta de muebles e inmuebles hasta redes de secuestro, tráfico de órganos, armas y droga.

Sin embargo, esta parte de la Internet también fue transformada en un espacio de libre opinión, funcionando como un nicho más para el activismo cibernético, ataques contra plataformas de gobiernos, empresas y figuras públicas. Su marca en la llamada “revolución” incluso traspasó las barreras de la web profunda y ha alcanzado a la Surface Web por medio de sitios en donde se pueden conseguir contenidos multimedia, productos y licencias gratuitas o a precios muy bajos, galerías en donde las limitaciones económicas no constituyen un borde para adquirir patentes y productos cuyo alto valor en el mercado convencional constituye un impedimento para muchas personas.

No obstante, debido al evidente estatus ilegal de algunas de las actividades realizadas en ese nivel de la red, yendo desde la rotunda violación de los derechos de autor hasta la exhibición en sus innumerables galerías de crímenes de lesa humanidad<sup>55</sup> la mayoría del contenido se encuentra indiscriminadamente bajo vigilancia, permanente bloqueados y bajo constante rastreo y monitoreo de las autoridades correspondientes en algunos países. Si bien es cierto que el consenso

<sup>53</sup> Tor Project [en línea] Disponible en: <https://www.torproject.org/> Consultado el 29/1/18

<sup>54</sup> Se alude al G-7, la Federación Rusa y la República Popular China.

<sup>55</sup> Cualquiera de los actos siguientes cuando se cometa como parte de un ataque generalizado o sistemático contra una población civil y con conocimiento de dicho ataque: a) Asesinato; b) Exterminio; c) Esclavitud [...] Definición extraída de: Organización de las Naciones Unidas (1998) *Estatuto de Roma de la Corte Penal Internacional*, United Nations, [en línea] Disponible en: [http://www.un.org/spanish/law/icc/statute/spanish/rome\\_statute%28s%29.pdf](http://www.un.org/spanish/law/icc/statute/spanish/rome_statute%28s%29.pdf) Consultado el 29/1/18

general para un cuerpo de normas sólidas específicamente acerca del ciberespacio aún no ha logrado ser implementado, en algunos países (principalmente economías más avanzadas y de alto desarrollo tecnológico) como Reino Unido<sup>56</sup>, Emiratos Árabes Unidos, Estados Unidos y Canadá, la creación y el uso de este tipo de sitios está penado por la ley, además de corresponder con coerción ejemplar.

| Nombre             | Dominio   | Categoría                |
|--------------------|---|--------------------------|
| Wall Street Market | <a href="http://wallstyizjhkrvmj.onion/signup?ref=276">http://wallstyizjhkrvmj.onion/signup?ref=276</a>   | Mercado negro            |
| Dream Market       | <a href="http://xsuee6v24g2q6phb.onion/?ai=1675">http://xsuee6v24g2q6phb.onion/?ai=1675</a>   | Mercado negro            |
| DeepDotWeb         | <a href="http://deepdot35wvmejd5.onion/">http://deepdot35wvmejd5.onion/</a>   | Noticias de la Deep Web  |
| The Hidden Wiki    | <a href="http://tdskbd7uolwsqqgn.onion/cgi-bin/wiki/TRHW.cgi/wiki?name=The+Hidden+Wiki">http://tdskbd7uolwsqqgn.onion/cgi-bin/wiki/TRHW.cgi/wiki?name=The+Hidden+Wiki</a> | Directorio Deep Web      |
| ChatTor            | <a href="http://chattorci7bcgygp.onion/">http://chattorci7bcgygp.onion/</a>   | Servicio de chat anónimo |

Tabla 3. Aproximación obtenida de los sitios activos más populares en la Deep Web, accesibles solo mediante Tor browser. Última actualización 31/1/18.<sup>57</sup>

Está claro que irónicamente se le ha catalogado al uso de las redes sociales y la libertad por navegar en la Surface web como la emancipación de los usuarios del sistema, como un espacio donde el libre albedrío está permitido y los cerrojos no existen y si lo hacen están allí para cuidar de los usuarios mismos. No obstante, la realidad es bastante adversa a este tipo de apologías ya que, esta parte de la web

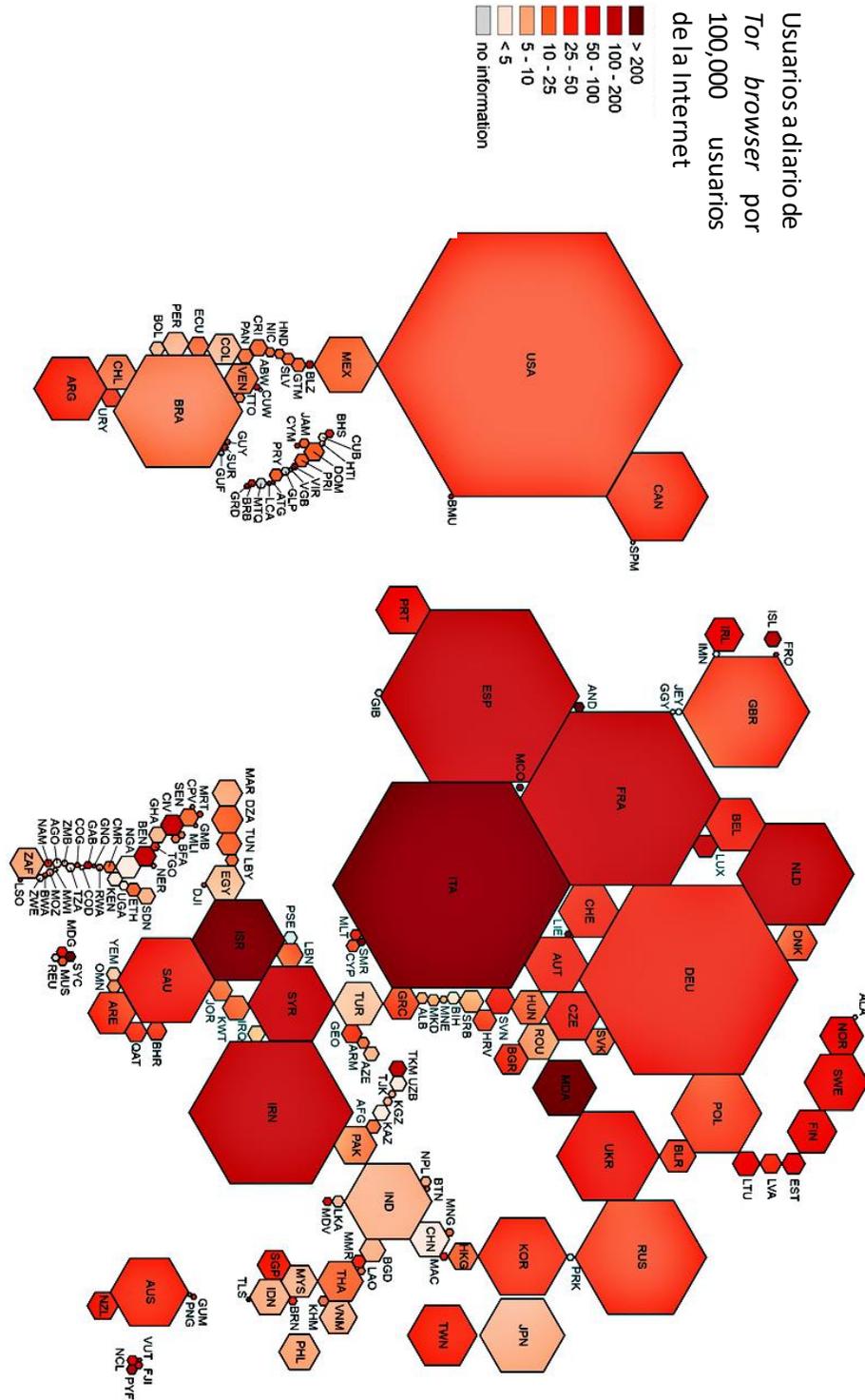
<sup>56</sup> Haworth J. (2016) *Putlocker blocked in the UK by internet service providers after High Court order bans streaming site*. Mirror. [en línea] Disponible en: <http://www.mirror.co.uk/news/uknews/putlocker-blocked-uk-internet-service-8060064> Consultado el 7/8/16

<sup>57</sup> Elaboración propia. Datos extraídos de: DeepDotWeb, *Top markets*, [en línea] Consultado el 31/1/18 Disponible con *Tor browser*: <http://deepdot35wvmejd5.onion/marketplace-directory/categories/top-markets/> y de: Deep Web, *Deep Web Destinations – A Massive List of Places to Visit on the Deep Web*, 31 de enero de 2018 [en línea] Disponible en: <https://www.deepweb-sites.com/deep-web-links-2015/> Consultado el 31/1/18

solo corresponde al 0.2% del contenido total en línea. Lo cierto es que a pesar de la relativa libertad para navegar y elegir información en el amplio contenido disponible en la Surface web, cerca del 99% de los datos e información en la red solo pueden ser alcanzados indirectamente. De acuerdo con The Deep Web, un artículo publicado en Hewillson Wordpress, la Surface web comprende solo 19 terabytes del contenido de la red informática mundial mientras que el resto de la web (Deep web) abarca hasta 7500 terabytes.<sup>58</sup>

---

<sup>58</sup> *Ibid. The Deep Web.* Hewilson.



Mapa 1. Mapa del uso en promedio de Tor browser en cada país del mundo hasta julio de 2013<sup>59</sup>.

<sup>59</sup> Graham Mark y De Sabbata Stefano (2014) *Average number of Tor users per day calculated between August 2012 and July 2013*, Internet geographies at the Oxford Internet Institute, Genbeta.com [en línea] Disponible en: <https://www.genbeta.com/seguridad/asi-es-el-mapa-del-uso-de-tor-en-cada-pais-del-mundo> Consultado el 2/2/18

### 1.4.3. Darknet

Si bien las opiniones están divididas respecto a una diferencia notoria entre la *Deep Web* y la *Darknet*, en realidad la segunda forma parte de la primera y si la podríamos ubicar en una escala se encuentra en la parte más profunda de la Internet, en el abismo, donde no existe algún tipo de regulación, cuyo contenido y navegantes son completamente anónimos y ya sea están libres de rastreo o poseen sistemas de seguridad muy avanzados. En otras palabras, hacemos alusión al corazón de la Internet, a la parte más recóndita y original con la que se comenzó el proyecto militar en la segunda mitad del siglo XX, la parte anónima antes de que existiera la necesidad por volverla oficialmente así, ya que se trataba de un proyecto exclusivo. Con el paso del tiempo y la evolución tecnológica, su tamaño se fue agrandando hasta alcanzar las dimensiones de toda la red informática mundial en la actualidad, sin embargo, particularmente la *Darknet*, permaneció intacta respecto a su alta confidencialidad.

El ingreso a este tipo de información es realmente complicado, y no se puede realizar sino con el empleo de *software* especializado, además de la encriptación del *hardware*. A diferencia de la *Deep Web*, ingresar es bastante complejo puesto que con un ordenador convencional y aún con *Tor*, sólo se puede alcanzar un ápice de la totalidad de sitios *web* y bases datos a tales cavidades.

Pero lo que hace tan trascendental e interesante los intentos por conseguir surcar estas aguas es la información que ahí se encuentra, en este nivel los mercados de droga y armas disponibles en la *Deep Web*, además de sitios de piratería, robo de identidad, no son lo más escabroso, ya que en la *Darknet* existe una gran cantidad de datos recopilados por organizaciones anónimas dedicadas al sabotaje de oficinas gubernamentales y empresariales, así como sitios auténticos para la contratación de asesinos a sueldo y otros servicios especiales propios del *underground*. Esto significa que documentos y cantidades exuberantes de archivos confidenciales que en algunos casos muestran los objetivos reales y las instrucciones de las operaciones del sistema pueden ser visualizados.

Al igual que la *Deep Web*, la *Darknet*, también posee anclas que consiguen asomar en la *Surface Web*. Aunque su presencia sea mucho menor a aquellas

mostradas en la tabla 3 su poder de incidencia es a veces más relevante, debido en gran medida a su impacto mediático en la población mundial de usuarios.

| Nombre                                 | Dominio   | Categoría  |
|--|---|--|
| Wikileaks                              | <a href="https://wikileaks.org/">https://wikileaks.org/</a>                       | Difusión de archivos confidenciales. (Documentos encriptados, seguridad nacional e inteligencia) |
| Cryptome                               | <a href="https://cryptome.org">https://cryptome.org</a>                           | Difusión de archivos confidenciales.   |
| FAS(Federation of American Scientists) | <a href="https://fas.org">https://fas.org</a>                                     | Difusión de archivos confidenciales.   |
| EFF(Electronic Frontier Foundation)    | <a href="https://www.eff.org/es">https://www.eff.org/es</a>                       | Defensa de los derechos fundamentales en el mundo digital.                                       |
| Intelligence Online                    | <a href="https://www.intelligenceonline.fr">https://www.intelligenceonline.fr</a> | Noticias y difusión de archivos confidenciales.  |

Tabla 4. Algunos sitios web disponibles en la Surface Web con contenido proveniente de la Darknet. Última actualización 31/1/18.<sup>60</sup>

Como se puede constatar en la tabla anterior donde se ha colocado los sitios más conocidos e importantes sustractores de información confidencial, las funciones que realiza cada uno no disciernen en mínimo de las demás, y es que a este tipo de páginas cuyo contenido está lleno de documentos, testimonios, opiniones que revelan las acciones de poderosos actores en las relaciones internacionales, desde empresas trasnacionales, bancos internacionales, pasando por Estados y Organismos no gubernamentales desenmascaran una realidad a la que se le da la espalda voluntariamente. En otros términos, podemos catalogar su función como auténticos destapadores de cloacas, espacios repletos de *Terabytes* de información cuyo

<sup>60</sup> Elaboración y búsqueda propia.

contenido es todo aquel que sencillamente comparte la característica de ser inadmisibles para su propagación en la superficie ya que discute el y los distintos regímenes de verdad pública impuestos por los grupos de poder que administran las decisiones de los países más poderosos.

De esta manera, podemos explicar la necesidad de estas élites por la existencia de dos mundos, el mundo visible y el mundo alternativo, de alguna manera subterráneo o bien con exigua legitimidad, y de este modo a la red informática mundial, como auténtico reflejo de la sociedad la cual proyecta la misma conformación (*Surface Web - Deep Web*). Una proporción dialéctica que a menudo, con un afán hermético atesora la información que indirectamente sostiene las bases de quienes detentan el poder en la parte “oculta”.

En este espacio dimensional la *Darknet* se ajusta como el rincón de los rincones. Límpidamente su contenido y navegantes son resguardados bajo altos niveles de seguridad por las agencias de inteligencia gubernamentales y empresas de ciberseguridad, a tal grado que se han desarrollado softwares con la facultad para perseguir a usuarios no autorizados.

### 1.5. *Deep Web* seguridad informática

La creación de una segmentación en la Internet no solamente supuso la utilización de un sistema alternativo a la *web* para distribuir información en la parte más grande de la Internet, sino también el reemplazo del lenguaje de hipertexto por el encaminamiento cebolla para acceder al vasto contenido en la *Deep Web*. Esta desmembración significó la exclusión de la población mundial de usuarios del contenido multiverso en la *web* profunda, quizá debido a la sobresaliente presencia de actividades ilegales, que amenazan la seguridad y la integridad moral del público y de las naciones. Presumiendo la veracidad de tal afirmación, debemos recordar que al final, se trata de un proyecto científico y militar orientado hacia la retención del poder, y creado por y para la inteligencia de las potencias mundiales, y que, a pesar de funcionar como un garante del anonimato y la privacidad, recientes sistemas creados por agencias del gobierno estadounidense, como MEMEX, son



capaces de detectar la verdadera IP<sup>61</sup> desde la que navegan los internautas en la penumbra de la Internet.

Antes ya se ha historiado acerca de los orígenes y las utilidades principales de la *Deep Web*, ya sabemos que se trata de una creación militar, que en sus entrañas acumula archivos clasificados, junto a montones de prácticas ilícitas de las que incluso los gobiernos a través de las agencias de inteligencia, grandes corporaciones, individuos que se autocalifican como parte de grupos ciberactivistas, terroristas y extremistas realizan sin auténticas limitaciones. Es momento de preguntarse si realmente se trata de adversarios del sistema o si en verdad solo conforman parte de la maquinaria, y que inclusive se les podría considerar como las baterías del mecanismo, como piezas necesarias.

Otra de las afirmaciones difundidas más comunes es entender no solamente a la *web* profunda sino a la Internet como espacios de libre opinión, pero es necesario reiterar que su nivel de alcance está medido hasta el nivel en el que pueden representar amenazas para el sistema. La tecnología avanza a una velocidad descomunal, y con ello los niveles de incidencia e interconexión de la cibercomunidad civil que se empeña por alcanzar nuevos niveles de intercambio de información más eficaces, aprovechando las ventajas que pueden ofrecer las nuevas modalidades digitales se vuelven más amplios.

De la misma manera, la industria de la ciberseguridad crece continuamente, abarcando paralelamente más aspectos de la vida en la red. Es cuestión de tiempo para que la censura sobre todos los contenidos contestatarios al sistema se convierta en una realidad total. Si bien, la Internet en su seno militar lleva implícitamente el *chip* la inspección y la potestad sobre la red informática mundial también es cierto que aún no se consigue perpetrar la regulación cabal de los usuarios y la información.

---

<sup>61</sup> Del inglés *Internet Protocol*, Protocolo de Internet. "Un protocolo es un método estándar que permite la comunicación entre procesos (que potencialmente se ejecutan en diferentes equipos), es decir, es un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red. En Internet, los protocolos utilizados pertenecen a una sucesión de protocolos o a un conjunto de protocolos relacionados entre sí. Este conjunto de protocolos se denomina TCP/IP." Definición extraída de la *web* CCM. [en línea] Disponible en: <http://es.ccm.net/contents/275-protocolos> Consultado el 12/8/16

La humanidad se encuentra en una etapa de transición hacia el control total de la sociedad a través de las nuevas tecnologías, a propósito, Brzezinski, ex consejero de Seguridad Nacional de Estados Unidos en el gobierno de Carter advirtió sobre las repercusiones que tendría sobre la humanidad la entrada a la *era tecnocrónica*.

*“la era tecnocrónica involucra la aparición gradual de una sociedad más controlada y dominada por una élite sin las restricciones de los valores tradicionales, por lo 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”<sup>62</sup>*

Lo cierto es, que las afirmaciones de Brzezinski, no se alejan en nada de la realidad actual, y es que precisamente mediante el uso de la Internet hoy hay empresas como *Global Web Index* o *Melissa* facultadas para la recopilación de datos privados y la creación de un perfil de cada usuario en el planeta. Los datos coleccionados son utilizados por la industria de la publicidad, que a partir del comportamiento de los sujetos crea estrategias de mercadotecnia más efectivas.

Solamente esta empresa tiene acceso al 89% de los usuarios de la Internet, que aglutina una cifra de más de 3 mil millones de personas<sup>63</sup><sup>41</sup>, es decir más de tres cuartas partes de la población mundial, por medio de sus más importantes clientes, cuyos sitios son visitados frecuentemente por la población mundial de internautas, entre ellos *Twitter*, *Google*, *Microsoft*, *Viacom*, *Procter & Gamble*, entre muchas otras. Es menester señalar que entre las grandes filas de sus clientes no solamente se encuentran grandes negocios dedicados a los servicios multimedia y relacionados de manera directa con Internet, muchas de estas empresas se dedican a la producción de la vida cotidiana del ser humano, en otros términos, conjuntan aspectos presentes en las vidas del modelo mundial a seguir por la mayoría de la

---

<sup>62</sup> Brzezinski Z. (1970) *Between two ages American role in the technetronic era*. Nueva York. Estados Unidos p. 97 Consultado el 12/8/16

<sup>63</sup> Éxito exportador (2015) Estadísticas Mundiales del Internet 2015. Exitoexportador.com. [en línea] Disponible en: <http://www.exitoexportador.com/stats.htm> Consultado el 5/5/16.



población, ya sea, la estética, comida, vehículos, desarrollo tecnológico, publicidad, etcétera.

Tales características, develan la mancomunidad entre los actores internacionales dedicados al ciberespacio, dan cuenta de que el objetivo nodal no es tanto quien consigue más audiencia, sino que se puede extraer de ella y como utilizar esa información para planificar las mejores estrategias para continuar con las riendas del poder mundial. Las violaciones a la privacidad de los usuarios son constantes, es evidente que una consigna de seguridad resulta un escaparate perfecto para ampararse ante cualquier forma de reclamación a futuro, lo cierto es que, es innegable la facilidad con la que corporaciones como *Facebook* emplean los datos de sus usuarios para compartirlos con empresas como la citada *Global Web Index*, (sin algún tipo de repercusión legal) vinculadas estrechamente con empresas dedicadas a la producción de un estándar a seguir por la población, orientado a comprender casi cada detalle de la vida de las personas.

Para ilustrar, recientemente se conoció que *WhatsApp* entregaría los números telefónicos de sus usuarios a *Facebook*, para que estos recibieran anuncios y mensajes de otras empresas, según Samuel Gibbs articulista en el periódico británico *The Guardian*, “los más de mil millones de usuarios de *WhatsApp* serán notificados de los cambios a su política de privacidad, el 25 de agosto. Tendrán 30 días para decidir si optar para que su información sea utilizada para la orientación de anuncios en Facebook, pero no serán capaces de optar por dejar de compartir sus datos con la red social”<sup>64</sup>. Y es que, hablamos de las redes sociales como verdaderas herramientas de control social, auténticos monopolios de la Internet, verbigracia, solo *Facebook* es la empresa matriz de aplicaciones como *Messenger*, *WhatsApp* e *Instagram* englobando a miles de millones de usuarios que cabe mencionar, de acuerdo con datos de Statista, de 2008 a 2017 se registró que más de 2 mil millones de usuarios visitó a diario activamente dicha matriz<sup>65</sup>.

<sup>64</sup> Gibbs S. (2016) *WhatsApp to give users' phone numbers to Facebook for targeted ads*. The guardian [en línea] Disponible en: <https://www.theguardian.com/technology/2016/aug/25/whatsapp-to-give-users-phone-number-facebook-for-targeted-ads> Consultado el 27/8/16

<sup>65</sup> Statista(2018) Number of monthly active Facebook users worldwide as of 4th quarter 2017 (in millions), Statista.com [en línea] Disponible en: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> Consultado el 11/2/18

El poder que significa la capacidad de incidencia en casi la totalidad de la población mundial activa en la Internet es vital para la planificación de los futuros acontecimientos dirigidos al público. Por medio de la Internet el usuario se da a conocer incluso más de lo que cree conocerse a sí mismo. Para ilustrar, recientemente se han agregado a la lista de aplicaciones y utilidades de los sistemas operativos asistentes como Siri y Cortana, capaces de interactuar con los usuarios como asistentes personales utilizando comandos de voz para consultar varios tipos de información.

No obstante, en ambos casos los datos ingresados por el usuario al dirigirse a esta clase de simuladores van directamente a la base de datos de *Microsoft* y *Macintosh*, respectivamente, lo que quiere decir que prácticamente el usuario autoriza a la empresa para ingresar a sus calendarios, su ubicación, fotos, contactos, programas y/o aplicaciones instaladas, historial de búsqueda etcétera. En otros términos ¿quién es?, ¿qué hace? y ¿qué le gusta? Y eso no es lo más grave, puesto que dichos ejemplos son pruebas del consentimiento al espionaje, y que a final de cuentas se encuentran disponibles en el mercado y a disposición de la mayoría de los usuarios en la Internet, sin que estos tengan mínimamente idea de que no solo están regalando, sino degradando su propia libertad a cambio de “seguridad”, ocio, simplemente por estar al día.

Todo esto teniendo como máximo colaborador al usuario mismo, hoy vuelto un sujeto con obsesiones denominadas por el sistema como “nuevas necesidades” que, dicho sea de paso, trata de cumplir compulsivamente. La ciberseguridad forma parte de ellas, y poco a poco ha escalado hasta alcanzar características paranoicas, rebasando lo necesario y alejándose en la infinita carrera de lo que considera “suficientemente seguro”.

### 1.5.1. Clasificación del *malware*

Existe una amplia cantidad y variedad de *malware*, categorizada de acuerdo a tres criterios fundamentales tomados en cuenta a menudo por la mayoría de las agencias y empresas dedicadas a la ciberseguridad.

- a) El nivel de daño y amenaza al sistema operativo.
- b) Su forma de afectarlo.



c) El grado de dificultad para ser combatido.

Para efecto del correcto entendimiento y evitar la confusión que puede existir entre uno y otro tipo de *malware* tomamos la clasificación del grupo internacional anglo-ruso Kaspersky Lab<sup>66</sup> el cual ofrece un panorama conciso para categorizar a las amenazas *malware* hoy día vigentes en la red. Entre los más comunes se encuentran

los siguientes:

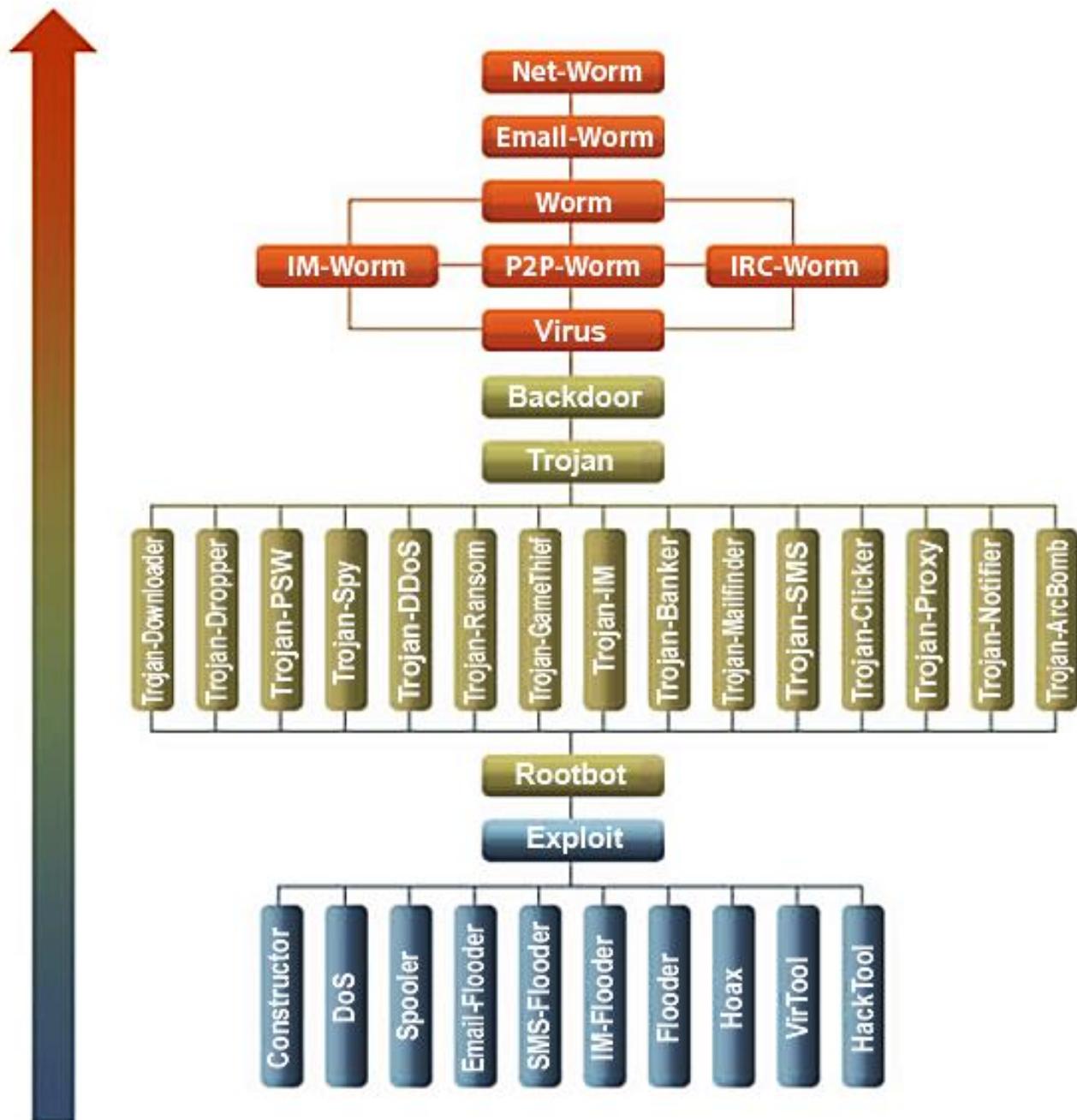
- **Virus.** Se propagan a través de archivos infectados disponibles en sitios *web* y correo electrónico; comienzan su operación al ejecutar dicho archivo causando un auténtico caos en el sistema operativo, eliminando archivos y/o información del directorio.
- **Gusano.** Tiene la misma función que el virus, sin embargo, se reproduce por sí mismo alcanzando un rango de propagación mucho más amplio; a diferencia del virus el gusano infecta el sistema operativo a través del ingreso a un sitio *web* o un correo electrónico no al abrir un archivo.
- **Troyano.** Es un *malware* oculto en archivos que lucen inofensivos, una vez descargados dentro de la computadora recopilan información personal del usuario además de permitir el acceso a distancia de quien perpetúa el ataque.
- **Ransomware.** *Malware* que bloquea el sistema operativo o confina información personal del usuario y pide dinero al usuario para devolver el equipo a su estado original.
- **Spyware.** Cuya función reside en tomar información del usuario ya sean archivos relevantes como números de tarjetas de crédito, contraseñas y el historial de búsqueda sin que este lo sepa. Rastrea el comportamiento del usuario mientras navega por la red y las acciones realizadas en su computadora.
- **Rootkit:** hoy en día, los Rootkit son una parte especial de los malware, ya que están diseñados específicamente para ni el usuario ni el software de

---

<sup>66</sup> Kaspersky Daily,(2013) *Clasificación de Malwares*, 29 de octubre de 2013, [en línea] Disponible en: <https://latam.kaspersky.com/blog/clasificacion-de-malwares/1608/> Consultado el 31/1/18

protección se enteren de la existencia del malware en el sistema. Algunos incluso se activan antes de que arranque el sistema operativo (éste rootkit se llama Bootkit). Algunos programas antivirus muy sofisticados consiguen detectar los Rootkit y eliminarlos.

- **Backdoor (RAT):** Estos malware, conocidos en inglés como “Remote Administration Tools”, son aplicaciones a través de las cuales los administradores de sistemas y los cibercriminales pueden acceder al sistema sin que el usuario se entere. Dependiendo de las funcionalidades de los *backdoor*, los hacker pueden instalar y lanzar otros programas, enviar keylogger, descargar o borrar archivos, encender los micrófonos o la cámara del dispositivo, registrar la actividad de la computadora y enviarla al cibercriminal.
- **Downloader:** son pequeñas piezas de códigos que toman archivos ejecutables o cualquier otro archivo del sistema para llevar a cabo algunas tareas específicas desde el servidor del cibercriminal. Una vez que el usuario haya descargado los downloader desde un adjunto de un correo o de una imagen, los delincuentes envían instrucciones para descargar otros malware en el equipo.

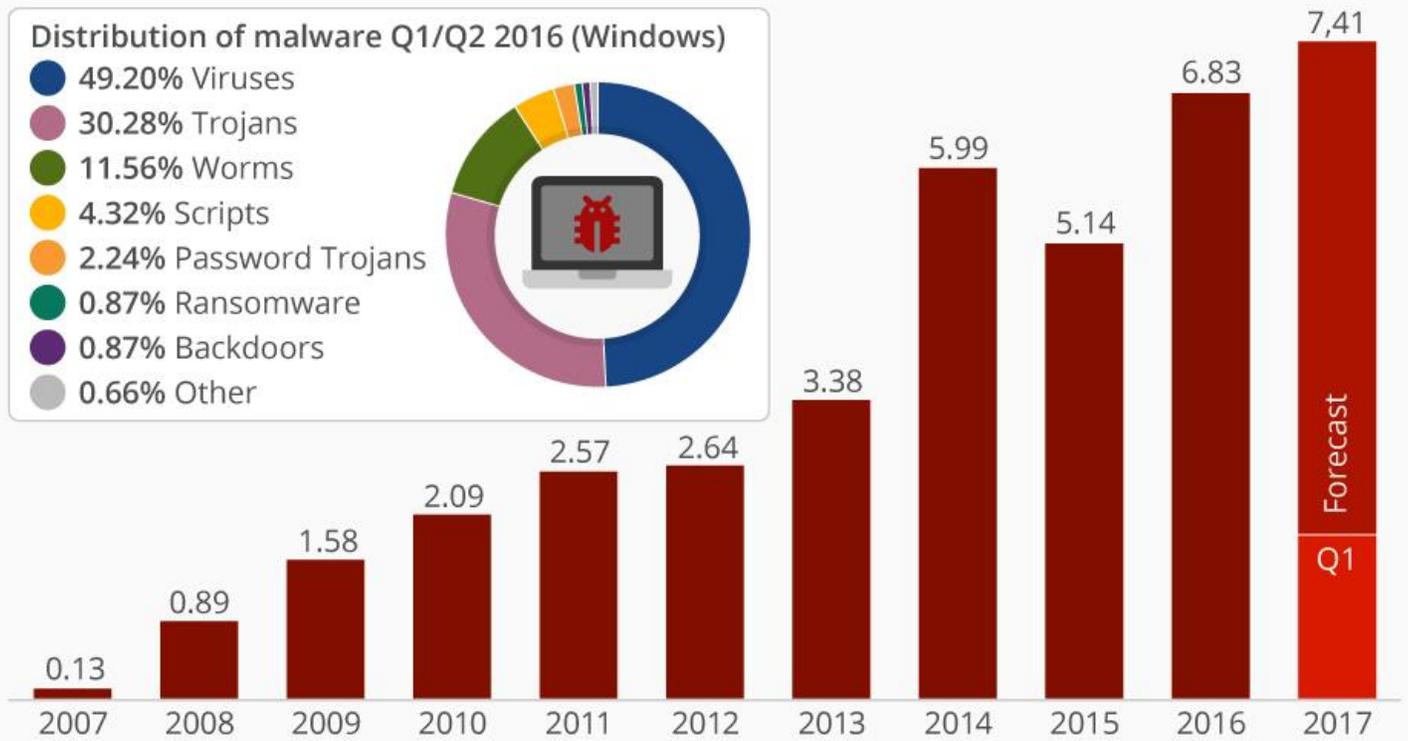


Esquema 1. Árbol de la clasificación del malware por laboratorios Kaspersky. El orden de amenaza va de la parte inferior a la parte superior, donde se encuentran las amenazas más grandes.<sup>67</sup>

<sup>67</sup> SecurityMosmetod (2017) *Классификация вредоносных программ* (clasificación del malware)[en línea] Disponible en: <http://security.mosmetod.ru/zashchita-ot-virusov/44-klassifikatsiya-vredonosnykh-programm> Consultado el 31/1/18

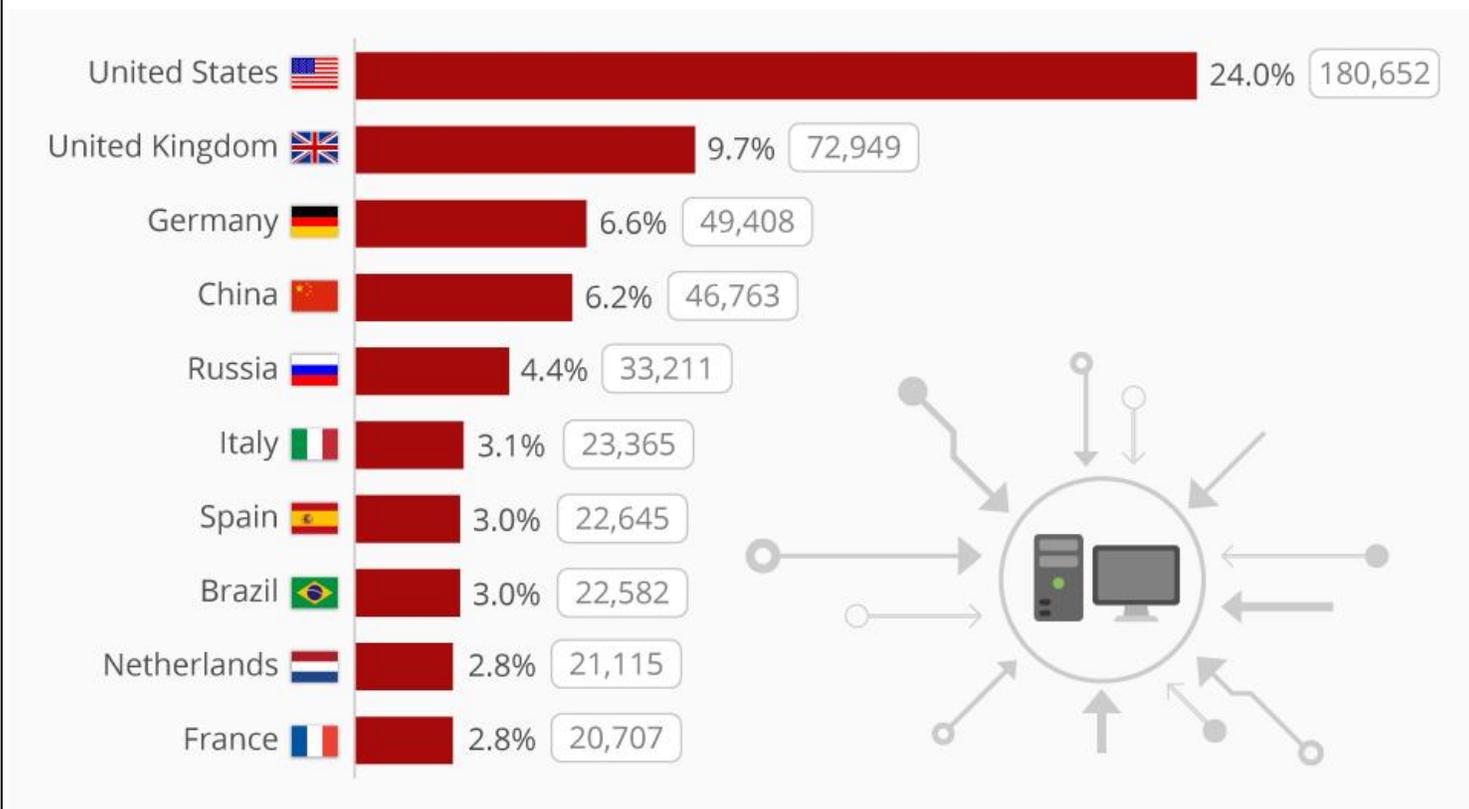
### 1.5.2. El negocio del *malware*

La existencia del *malware* es un fenómeno propio del “hábitat” que representa el ciberespacio, igualmente surge como resultado de la permisividad otorgada por los creadores y desarrolladores de la red informática mundial para conceder facilidades a ciber delincuentes, que van desde estafadores y chantajistas hasta secuestradores. En esta investigación se sostiene que el crecimiento acelerado de la presencia de *software* injurioso en la red tiene un trasfondo más importante que no puede ser tajantemente explicado con el incremento de individuos decididos a ganar dinero ilegal, sino que debemos agregar la relación paralela de su progresión con el aumento del uso de antivirus y los ingresos de estos. En suma, los antivirus más comerciales solo combaten al *malware* a pequeña escala ya que en realidad lo producen, desarrollan y propagan en la población activa en la Internet. Análogamente en los países con más presencia activa de antivirus han ocurrido más ataques de *malware*, específicamente bancos de los siguientes países: Estados Unidos, Reino Unido, Canadá y Alemania.



Gráfica 3. Crecimiento del número de tipos de malware (en millones) de 2007 a 2017 en general y distribución en porcentajes del primer y segundo cuarto de 2016 específicamente en Windows.<sup>68</sup>

<sup>68</sup>Loesche Dyfed (2017) *Ransomware Makes up Small Share of Growing Malware Threat*, Statista, 28 de junio de 2017, [en línea] Disponible en: <https://www.statista.com/chart/10045/new-malware-specimen-and-share-of-windows-based-malware/> Consultado el 31/1/18



Gráfica 4. Porcentaje y número de DDoS<sup>69</sup> en Estados Unidos, en el último cuarto de 2016 por país de origen.<sup>70</sup>

De manera equidistante a las innovaciones en ciberseguridad, la capacidad para infligir daño en la población activa en la red se vuelve más grande, así como la inversión de los usuarios en antivirus, anti *spyware* y/o dispositivos con características más sofisticadas y prometedoras. En este sentido, el negocio que genera la sugestión constante del usuario aporta ingresos cada vez más altos a las empresas dedicadas a la seguridad en el ciberespacio, sin mencionar el aumento de

<sup>69</sup> Ataque de denegación del servicio DDoS (por sus siglas en inglés *Distributed Denial of Service*): es un tipo de ataque informático que utiliza una gran cantidad de *hosts* para abrumar a un servidor, causando que un sitio *web* experimente un bloqueo completo del sistema. Este tipo de ataque es perpetrado por *hackers*, dirigido especialmente a sitios *web* populares y de gran escala para tratar de deshabilitarlos, de forma temporal o permanente. Definición extraída de Technopedia (2018) *Distributed Denial of Service* (DDoS), [en línea] Disponible en: <https://www.techopedia.com/definicion/10261/distributed-denial-of-service-ddos> Consultado el 1/2/18

<sup>70</sup> Armstrong Martin (2017), *U.S. Top Source of DDoS Attacks in Q4 2016*, Statista, 27 de febrero de 2017 [en línea] Disponible en: <https://www.statista.com/chart/8281/us-top-source-of-ddos-attacks-in-q4-2016/> Consultado el 1/2/18

su dependencia. Aunado a esto, podemos sumar la aparente debilidad de los navegadores *web* para garantizar la protección del usuario mientras explora en la red. Incidentalmente *Google Chrome*, (conocido más por ser uno de los *browsers* más populares que por su seguridad y eficacia, pero al que los *pluggins* de millones de páginas se han debido acoplar dada a su notable presencia mediática) según un reciente estudio efectuado por la *Brigham Young University* en cooperación con ingenieros de *Google Chrome*, reveló datos y estadísticas que exponen abiertamente su ineficaz sistema de seguridad.

Concretamente, el estudio se refiere a la infructuosidad de los mensajes de seguridad cuyo defecto se encuentra en su inoportuna aparición, ya que en lugar demostrarse antes de que las páginas descarguen *malware* u presenten algún otro tipo de amenaza informática, lo hacen después, “los investigadores especulan que los desarrolladores del *software* colocan adrede en mal momento las notificaciones de seguridad: si estos llegaran cuando los usuarios no están jlo entretenidos con programas y archivos, puede ser que tengan una mejor oportunidad de ser leído. Por ejemplo, al final de una película, mientras que se carga una página en línea o después de la interacción con un sitio *web*”.<sup>71</sup>

Para colmo, de acuerdo con los datos publicados por el periódico italiano la *Repubblica* se denota la actitud de connivencia entre los usuarios y el navegador, destacando que nueve personas de diez han ignorado los mensajes de seguridad. Además “el 74% ignora el mensaje de advertencia aparecido cuando estaba por cerrar una ventana del navegador. 79% ignora los mensajes si estaba viendo películas y el 87% cerró la alerta si se estaba transfiriendo información sensible, como un código de confirmación.”<sup>72</sup>

Si bien, el comportamiento del usuario puede considerarse hasta cierto punto la causa de su propia inseguridad también es cierto que paradójicamente la lógica de las empresas como *Google* ante la seguridad del usuario es bastante

---

<sup>71</sup> Repubblica (2016) *Oltre il 90% degli avvisi di sicurezza trascurati dagli utenti*, Repubblica.it [ en línea ] Disponible en: [http://www.repubblica.it/tecnologia/sicurezza/2016/08/19/news/oltre\\_il\\_90\\_degli\\_avvisi\\_di\\_sicurezza\\_trascurati\\_dagli\\_utenti-146258149/](http://www.repubblica.it/tecnologia/sicurezza/2016/08/19/news/oltre_il_90_degli_avvisi_di_sicurezza_trascurati_dagli_utenti-146258149/) Consultado el 27/8/16

<sup>72</sup> *Ibid.*

controvertida, puesto que ellas mismas son las que rastrean y monitorean cada búsqueda y contenido del usuario, sin mencionar su permisión ante la entrada y desarrollo de múltiples *malwares* y *spywares* que acechan en la Internet hoy día.

La condición endeble de Google *Chrome* genera automáticamente un vacío que pueden llenar las empresas de ciberseguridad, en ningún caso los hechos se encuentran aislados, y claro está que cuando se habla de seguridad aún se encuentran más entrelazados. Así como anteriormente mencionamos la presencia de una mancomunidad empresarial trabajando unida por y para el control de la información del usuario, el presente sector encaja dentro de un esquema similar. En occidente y sus áreas de influencia empresas de ciberseguridad como *Avast*, *AVG*, *Symantec*, *Eset*, *Intel Security*, etcétera. han ganado terreno los últimos años.

## **1.6. Técnicas de manipulación social en la web**

En este tenor los métodos de manipulación social constituyen un pilar protagónico en la pugna por el tráfico informático a nivel mundial entre los Estados sobre sus zonas de influencia. En seguida se emplazan las técnicas de clasificación y monitoreo de usuarios más empleadas.

### **1.6.1. Segmentación de usuarios por comportamiento**

Clasificar a la población en distintas categorías de acuerdo con su comportamiento es una realidad, numerosos estudios financiados por grandes corporaciones en colaboración con los gobiernos se realizan continuamente buscando la optimización de sus conocimientos acerca de los consumidores, de forma concisa, de la población activa en la Internet. Esto es, que las investigaciones van mucho más allá de solamente saber las preferencias de los usuarios en tal o cual producto o aplicación, verbigracia, existe un algoritmo que mediante Instagram es capaz de detectar la depresión en los usuarios, de acuerdo con información revelada por el periódico francés *L'express*, la detección fue realizada por dos investigadores estadounidenses a partir de un programa informático, con una tasa del 70% de éxito.

Además, el programa fue capaz de detectar “marcadores predictivos” presentes en los futuros o actuales depresivos: fotos con colores más fríos, de



luminosidad más sombría y con colores más apagados, utilizando especialmente el filtro *Inkwell*. Igualmente se realizó otro descubrimiento, y es que se determinó que las personas no deprimidas difunden menos fotos mostrando su propia cara y más fotos de sí mismos rodeados por terceros. Uno podría hablar de *selfies* “tristes” ya que los auto-retratos serían una tendencia más común en los depresivos, mientras que las demás personas se fotografiarían entre amigos, sostienen los investigadores.<sup>73</sup>

Los avances tecnológicos se adentran desmesuradamente en el estudio del comportamiento humano, las redes sociales, en particular, son como lo hace notar dicho estudio, un espacio con múltiples facetas y funcionalidades que equidistantemente a su rol como enlace de la población activa en la Internet, tienen la facultad para interpretar las conductas de los usuarios y consecuentemente advertir sus reacciones ante cualquier tipo de evento. Quizá no hayamos aún puntualizado la relevancia que el poder del conocimiento sobre las reacciones psicológicas de las personas puede significar para una empresa que desea mejorar su publicidad o un gobierno que pretende conocer a fondo el perfil de potenciales disidentes.

Dicho de otro modo, la gran mayoría de personas que frecuentan la Internet, concretamente las redes sociales<sup>74</sup> se encuentran en una condición sumamente vulnerable, pues en el afán ya mencionado como “nuevas necesidades”, clasificado en esta investigación como una obsesión compulsiva, entregan constantemente información, datos, fotos y vídeos sin ninguna precaución a la incertidumbre de la red, donde, como prácticamente un nuevo dicho moderno señala “todo lo que uno sube al Internet ya no pertenece a uno mismo”. Conceder información propia a una red social cuyos parámetros de seguridad son realmente cuestionables, tomando en consideración que a pesar de que todos los datos personales en la “nube” están ahí con prerrequisito del consentimiento propio de los usuarios es indisputablemente un riesgo que la modernización de la sociedad le exige al usuario.

---

<sup>73</sup> L'express (2016) *Un algorithme détecte les dépressifs à partir de leurs photos Instagram*. Lexpress.fr [en línea] Disponible en: [http://www.lexpress.fr/actualite/societe/sante/un-algorithme-detec-teles-depressifs-a-partir-de-leurs-photos-instagram\\_1822971.html](http://www.lexpress.fr/actualite/societe/sante/un-algorithme-detec-teles-depressifs-a-partir-de-leurs-photos-instagram_1822971.html) Consultado el 20/8/16

<sup>74</sup> Cabe recalcar la presencia abrumadora de personas jóvenes entre los 15 y 30 años de edad. Ver nota 21.

Para concluir, ya se ha indicado que, en el proceso de transformación tecnológica de la humanidad, y obviamente de la Internet con ella, es necesaria la adaptación de los sujetos al medio y del medio a los sujetos ya que, al final hablamos de un medio construido por el propio ser humano. Empero, dicha adaptación precisa otorgar información privada a medios manejados por desconocidos que utilizan con propósitos fluctuantes, a menudo traducidos en formas de control social.

### 1.6.2. Ingeniería social

La ingeniería social es otra de las técnicas más comunes y eficientes para la manipulación de usuarios, cabe recordar que como se señaló al principio de esta investigación<sup>75</sup> la construcción de un régimen de verdad es propia para ostentar el poder y control sobre la estructura de una sociedad. Hoy la conexión casi permanente entre la tecnología y el individuo hace posible acrecentar la capacidad de los grupos de poder a la cabeza de los Estados más poderosos para transmitir y reproducir a través de la Internet el conocimiento de una verdad y por consiguiente aprovechando dicha herramienta para seguir construyendo una realidad apegada a intereses particulares.

Conjuntamente, en el marco de la pugna por el tráfico informático es necesario señalar que incidentalmente *Google Analytics* es el principal proveedor de datos de los usuarios en Estados Unidos y sus zonas de influencia como América Latina o parte de Europa occidental para el propio gobierno de Estados Unidos, trabajando legítimamente y de manera unificada con las agencias federales de este gobierno en un programa denominado *Digital Analytics Program*<sup>76</sup>, a su vez habilitando el uso de esta herramienta con o sin el consentimiento del usuario a través de cada búsqueda en sitios *web* populares como *Google, Yahoo, Amazon* o *Facebook* (todas plataformas estadounidenses). En este tenor, se debe mencionar la existencia de otras herramientas de la misma naturaleza que cooperan con otros

---

<sup>75</sup> Ver Introducción p.9

<sup>76</sup> Analytics USA, (2018) *About this site*, Analytics.usa.gov [en línea] Disponible en: <https://analytics.usa.gov> Consultado el 6/2/18

gobiernos del mundo para mejorar el *performance* del monitoreo de usuarios, como lo es *Yandex.Metrica* que maniobra en colaboración y bajo la regulación de Moscú<sup>77</sup> en buscadores *web* como *Yandex*<sup>78</sup> y que al igual que su símil estadounidense trabajan en aumentar la efectividad del proceso y práctica de la ingeniería social sobre sus respectivas audiencias internautas.

| <b>Herramientas más populares de análisis de datos</b> |       |                                  |                           |                                  |
|--|-------|----------------------------------|---------------------------|----------------------------------|
| © W3Techs.com  | Uso   | Cambio desde 1º de enero de 2018 | Propagación en el mercado | Cambio desde 1º de enero de 2018 |
| 1. <a href="#">Google Analytics</a>                    | 51.7% | -0.7%                            | 82.4%                     | -0.3%                            |
| 2. <a href="#">Yandex.Metrica</a>                      | 5.4%  |                                  | 8.7%                      | +0.1%                            |
| 3. <a href="#">WordPress Jetpack</a>                   | 4.7%  | +0.1%                            | 7.4%                      | +0.1%                            |
| 4. <a href="#">LiveInternet</a>                        | 3.0%  |                                  | 4.8%                      |                                  |
| 5. <a href="#">New Relic</a>                           | 1.9%  |                                  | 3.0%                      |                                  |

Tabla 5. Herramientas de análisis del tráfico de datos más populares hasta enero de 2018.<sup>79</sup>

Ahora bien, la página *web Hack Story* define a esta actividad como “el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros”.<sup>80</sup> Si bien, esta técnica es utilizada para operar en general, es decir sin un marco referencial específico, naturalmente esta investigación se concentra en su aplicación al ciberespacio. Maniobrar con la ingeniería social es un trabajo que solo gente especialmente adiestrada, (los ingenieros sociales) puede realizar. De hecho, es necesario resaltar que las grandes corporaciones privadas que gestionan la

<sup>77</sup> Yandex (2018) *Privacy Policy*, Yandex.com [en línea] Disponible en: <https://yandex.com/legal/confidential/> Consultado el 6/2/18

<sup>78</sup> Ver Capítulo 2, Apartado 2.2.1 Navegadores y motores de búsqueda y 2.2.2 Redes sociales.

<sup>79</sup> W3Techs (2018) *Most Popular traffic analysis tools*, w3techs.com [en línea] Disponible en: <https://w3techs.com> Consultado el 6/2/18

<sup>80</sup> Hack Story (2013) *Ingeniería Social*. Hackstory.net [ en línea] Disponible en: [http://hackstory.net/Ingenier%C3%ADa\\_social](http://hackstory.net/Ingenier%C3%ADa_social) Consultado el 28/8/16

Internet y a la población que navega en ella poseen equipos exclusivos para trabajar en estrategias a partir del análisis y el comportamiento de los usuarios, sirviéndose de otras técnicas y medios también enunciados en esta investigación.

Se debe tener presente que, para comenzar el proceso se debe contar antes con *malware*, incidentalmente *spyware* ya infiltrado en el ordenador de la víctima, máxime cuando se trata de ataques aislados, centrados en un objetivo particular. Por ejemplo, los navegadores *web* como *Google* trabajan a menudo con sistemas operativos como *Microsoft*, manejando poderosos rastreadores como el ya mencionado *Google Analytics*, que monitorea constantemente las acciones del usuario dentro de la red, por otro lado, el sistema operativo en este caso *Microsoft* se encarga de recopilar la actividad fuera y dentro de la Internet.

De la misma forma, *Hack Story* establece una clasificación para las técnicas más usuales empleadas por los ingenieros sociales orientadas particularmente hacia la consecución de datos e información, las cuales están divididas en tres tipos, adcentados de acuerdo con el grado de interacción del operador con el sujeto. No obstante, en la presente investigación se ha pulido dicho orden además de perfilarlo hacia su neta y exclusiva aplicación en el ciberespacio, de tal suerte que el orden de las tres categorías no solamente irá en disposición del grado de interacción (mayor o menor) del ingeniero social, ya que en algunos casos supone una cronología en el proceso de recopilación de datos; presentada a continuación.

Técnicas de contacto:

- En ordenador:

1.1 Correo electrónico y redes sociales.

1.2 IRC<sup>81</sup> u otros chats.

- En móvil:

1.3 *Smartphone*:

1.3.1 Llamadas, y video llamadas (VoIP<sup>82</sup>54)

---

<sup>81</sup> Internet Relay Chat. Charla Interactiva Internet. Protocolo mundial para conversaciones simultáneas (party line) que permite comunicarse por escrito entre sí a través de ordenador a varias personas en tiempo real.

<sup>82</sup> Voz sobre protocolo de Internet



#### 1.4 Agendas y teléfonos móviles.

- Ambas:

#### 1.5 Desinformación.

#### 1.6 Monitoreo constante.

### 2 Técnicas de captura o aprisionamiento:

- Contacto empático.
- Presión psicológica.
- Recuperación de contraseña.
- Recopilación de información privada.

### 3 Técnicas para sustracción de datos:

- Suplantación de personalidad.
- Despersonalización.
- Chantaje o extorsión.

Recapitulando, el punto anterior conduce hacia el ferviente tema de la ingeniería

social, y es que, el mismo usuario le entrega todas las facilidades a estas empresas para construir herramientas, afin de desarrollar las mejores estrategias para influir en el público. La gravedad del conocimiento de información tan íntima como los estados emocionales de las personas por supuesto comprende una herramienta tan importante como para definir la forma de dar las noticias, como incidir en la perspectiva de la media de la población activa en la red. Por ejemplo, luego de los ataques de noviembre 2015 en Paris, en *Facebook* se disparó la tendencia del uso de un filtro con los colores del blasón francés, como un supuesto símbolo de la unión solidaria con los franceses; se adaptó un objetivo subyacente (generación y fomento de la xenofobia, tergiversación del Islam, aceptación del *état d'urgence* y la legitimación a las intervenciones armadas en Siria) a la moda o al estilo de los jóvenes, con el fin de sensibilizar a la población mundial.

Las consecuencias fueron diversas, puesto que además de que se ensombreció aún más al islam como religión (inclusive catalogada como de la guerra) se reencendió el cliché de que los devotos de esta fe son terroristas y generalidades absurdas por el estilo, reavivando de nuevo la llama del racismo, y disgregando aún



más a la población de Francia, de Europa y del mundo occidental en general. Claro está que independientemente de la endeble estructuración de estos prejuicios, tales afirmaciones consiguieron ser adoptadas por la población estándar en la Internet a nivel mundial, caracterizada por su ignorancia y falta de pensamiento crítico, por ende, no tardaron en ser absorbidas y reproducidas.

Si además agregamos el componente de la actividad del “Estado” Islámico, y su brutal mediatización *hollywoodense* a través de la *web*, cuyos vídeos sospechosamente arribaron con sorprendente solvencia a las redes sociales más importantes, noticieros y páginas de *streaming*, se pueden sacar varias conclusiones, puesto que a la par de generar desconcierto, sugestión, terror, y miedo, el pensamiento xenofóbico se expandió por todo occidente y sus zonas de influencia, verbigracia, México.

Pero la dimensión de impacto de la ingeniería social no implica ser solamente un medio utilizado directamente por los grupos de poder. También, mediante esta técnica organizaciones criminales que operan vía Internet, la utilizan para extorsionar usuarios, un delito que conlleva a mayores, inclusive la trata de personas, pornografía infantil, entre otras.

### 1.6.3. Spamdexing<sup>83</sup>

La *web Spam* le define como la práctica de SEO<sup>84</sup> *spamming*<sup>85</sup>, en el motor de búsqueda, dicho de otro modo, el *spamdexing* es la práctica en la que se crean sitios *web* indexados automática e ilegítimamente con posición más alta en los buscadores *web*, de tal suerte que la clasificación más alta (aquella que aparece en la primera página de resultados de búsqueda) de determinados tipos de información (noticias, imágenes, bases de datos) se encuentra totalmente preseleccionada. El *spamdexing* es una técnica de manipulación de información sumamente funcional y realmente difícil de evadir si solamente se tiene acceso a Internet mediante navegadores y buscadores *web* convencionales.

---

<sup>83</sup> Del inglés *spam-indexing*

<sup>84</sup> SEO es una abreviatura para “optimización del motor de búsqueda”, la cual es el arte de tener un sitio *web* optimizado, o atractivo, para los motores de búsqueda a través de la indexación óptima.

<sup>85</sup> *Spamming*, es el término en Internet para envío de información no solicitada.



Empresas como *Google* preseleccionan el orden de relevancia de los sitios *web* disponibles mediante programas muy especializados, verbigracia *PageRank* un algoritmo utilizado por *Google Search* canalizado hacia la compresión de los resultados en una categoría del motor de búsqueda. El uso de *PageRank* privilegia a los sitios *web* de negocios y publicidad en el *ranking* más elevado de búsqueda.

Igualmente se ha implementado en motores de búsqueda como *Google* y *Yahoo* otra forma de *spamdexing* caracterizada por mostrar artículos, productos y promociones del interés del usuario, previamente anunciadas por él mismo. Dicha información es extraída mediante rastreadores como *GooglAnalytics* y otros *softwares* con la facultad para recuperar los datos del historial de búsqueda, la compra-venta electrónica y el perfil del usuario. Tal recopilación de datos no únicamente tiene una funcionalidad para dirigir hacia páginas oficiales, sino que también puede ser utilizada para mostrar publicidad engañosa que a menudo direcciona a páginas que pueden descargar *malware* de cualquier tipo.

Naturalmente el *spamdexing* así como el resto de sus símiles están íntimamente ligadas, de modo que el funcionamiento de la maquinaria para la manipulación de la información depende del desempeño del conjunto de engranajes. Cabe mencionar que junto con la ingeniería social esta técnica ofrece un panorama de maniobra tan flexible que no únicamente las empresas que gestionan la indexación en la *Surface web* se sirven de su efectividad, dado que se halla a disposición de agencias de inteligencia, organizaciones, etcétera.

## 2. LA PUGNA POR LA HEGEMONIA DEL TRÁFICO INFORMÁTICO

El presente capítulo estudia las estrategias para mantener o modificar el *statu quo* en el tablero del poder mundial con el uso de la Internet. Ya comprendidas las principales técnicas de limitación de la información a escala global, es menester estudiar el papel de estas en el juego del poder mundial, entendiéndolo como la pugna sobre todo económica y tecnológica de los grupos de poder a través de los Estados y su andamiaje corporativo transnacional.

Es necesario entender a la Internet como un elemento que participe en el proceso cultural actual y no como un factor ajeno a su construcción, de tal suerte que la estructura social y *modus vivendi* de la población activa en la *web* se transforma y muta de acuerdo con los adelantos en todos los campos de la tecnología, pero taxativamente en el ciberespacio.

Entendiendo la dinámica multipolar que rige la organización política actual del mundo, en donde la Internet funge como la herramienta y campo de batalla principal en donde los Estados con las economías más avanzadas ejecutan estrategias para controlar más espacios (tanto en el ciberespacio como en el alcance de estos sobre otros territorios) y así poder extender y mantener su influencia política, desarrollar técnicas, *software* y plataformas fabricadas por sí mismos o bien por corporaciones emplazadas en sus territorios y vinculadas política y económicamente para monitorear el comportamiento de la audiencia en sus zonas de influencia, significa un acto político en sí mismo. En este sentido indirectamente el hecho de no permitir o menguar el acceso de la población internauta local o regional a plataformas de empresas ligadas a los intereses de los grupos de poder de otros Estados constituye la ejemplificación más evidente de la pugna por el tráfico informático.

### 2.1. Neocolonialismo e Internet

Recapitulando, desde su creación hasta la actualidad la Internet ha evolucionado constantemente, pasando de ser una herramienta exclusivamente militar para convertirse en una extensión más de la política. La relevancia del poder de impacto

de la red informática mundial en la Sociedad de la información ha optimizado la aplicación, alcance y efectividad del poder blando <sup>86</sup>, visto que las TIC han perfeccionado la manera de enviar mensajes de cualquier tipo y consecuentemente optimizado las habilidades para establecer estrategias con el fin de modificar o preservar el *statu quo*. Hoy día podemos aludir al ciberespacio no solamente como una plataforma para el progresivo avance científico y tecnológico en general, sino también como la auténtica expansión para hacer política, con todas las implicaciones y formas de manejar el poder posible. La internet como mecanismo político tiene como uno de sus fines fundamentales maniobrar con la población y adecuarla a un lado u otro del panorama internacional.

Naturalmente, la funcionalidad de poseer medios masivos de difusión de información mediante la red informática mundial impulsa copiosamente su capacidad de incidencia en la población tanto activa como no activa en la Internet. Como un fenómeno que integra a la sociedad, significa una vía más que efectiva para transmitir una forma de pensar, obviamente preseleccionada de acuerdo a intereses frecuentemente herméticos, provenientes de las élites de poder a nivel mundial, los gobiernos nacionales, locales, etcétera.

Además, si consideramos los avances de la era digital y a propósito la transformación de la sociedad como su propia consecuencia, debemos tomar en cuenta que a diferencia de hace cinco años cuando la televisión, los periódicos, revistas y libros componían las fuentes de información primordiales, hoy la captación de información requiere esfuerzo nulo dada su rotunda simplificación al estar al alcance de una suscripción o una notificación en el *Smartphone* o las redes sociales. De este modo, la audiencia en general actúa como una auténtica esponja de mensajes subliminales e información solapada en noticias, música de moda, publicidad, etcétera. Para mantener o alcanzar la hegemonía del tráfico informático y de esta manera influir en más y diversa población no solamente asentada en las

---

<sup>86</sup> Del inglés *soft power*, entendido en el contexto del sistema internacional, como la habilidad de un país para persuadir a otros de hacer lo que quiere sin el uso de la fuerza o la coerción, en otros términos a través de la atracción en lugar de la coerción.. Definición extraída de Nye Jr., Joseph (2004) *Soft power: The means to Success in World Politics*, Foreign Affairs, [en línea] Disponible en: <https://www.foreignaffairs.com/reviews/capsule-review/2004-05-01/soft-power-means-success-world-politics> Consultado el 6/2/18

zonas de influencia de una determinada potencia sino en las de sus adversarios, es necesario tener en valoración la ramificación fundamental en la que se asientan los componentes para mantener o modificar el *statu quo* mediante la Internet. Se trata de elementos sustanciales en el proceso del neocolonialismo que situamos a continuación:

### 2.1.1. Lenguaje

Su importancia deviene del origen mismo de la humanidad e históricamente en la cuna de los imperios occidentales (que dominarían casi cada parte del mundo y sembrarían vestigios ostensibles hasta la edad contemporánea), el empleo de una *lingua franca* fue muy importante para formar cohesión en los grandes territorios ocupados por poblaciones en ocasiones culturalmente muy diferentes. Es irrefutable que la lengua juega un papel central en el proceso neocolonizador y consecuentemente en la pugna por la influencia en la red.

Adaptando su utilidad y presencia histórica al año 2000, la progresiva expansión vía Internet del inglés como lengua de la potencia mundial imperante, Estados Unidos, hacia todas las partes del mundo respondió esencialmente a la capacidad económica de este país, cuyo desarrollo experimentó un realce significativo potenciado por el incremento de la compra-venta de armas producto de la dilatación de conflictos armados no convencionales en el mundo<sup>87</sup>, su estadio como superpotencia mundial en solitario después de la caída de la URSS en 1991 y el sólido posicionamiento en la punta de la economía mundial por parte de sus empresas transnacionales. De esta forma como país desarrollador de la Internet es evidente que la influencia de la lengua inglesa sería una causa más para que la población mundial comenzara su adaptación hacia la modernidad, adoptando anglicismos, cultura y visiones estadounidenses del mundo con mucha mayor solvencia.

Con todo, se considera que la pauta de la influencia lingüística en la Internet se traduce en el comportamiento económico y geopolítico de los actores

---

<sup>87</sup> Guerras civiles, guerrillas, terrorismo, combate del narcotráfico, etcétera.

internacionales, incidentalmente de la lucha entre potencias grandes y medias<sup>88</sup> por alcanzar un grado mayor de incidencia en la audiencia cibernética. Evocando lo anterior, de acuerdo con datos publicados por la *web* Techinasia<sup>89</sup>, la presencia del inglés como lengua predominante en la red informática mundial pasó de un aumento progresivo arribando hasta casi el 40% en 2000, para dirigirse hacia un lento pero activo decrecimiento que se mantiene hasta la actualidad debido al aumento de contenido en otros idiomas.

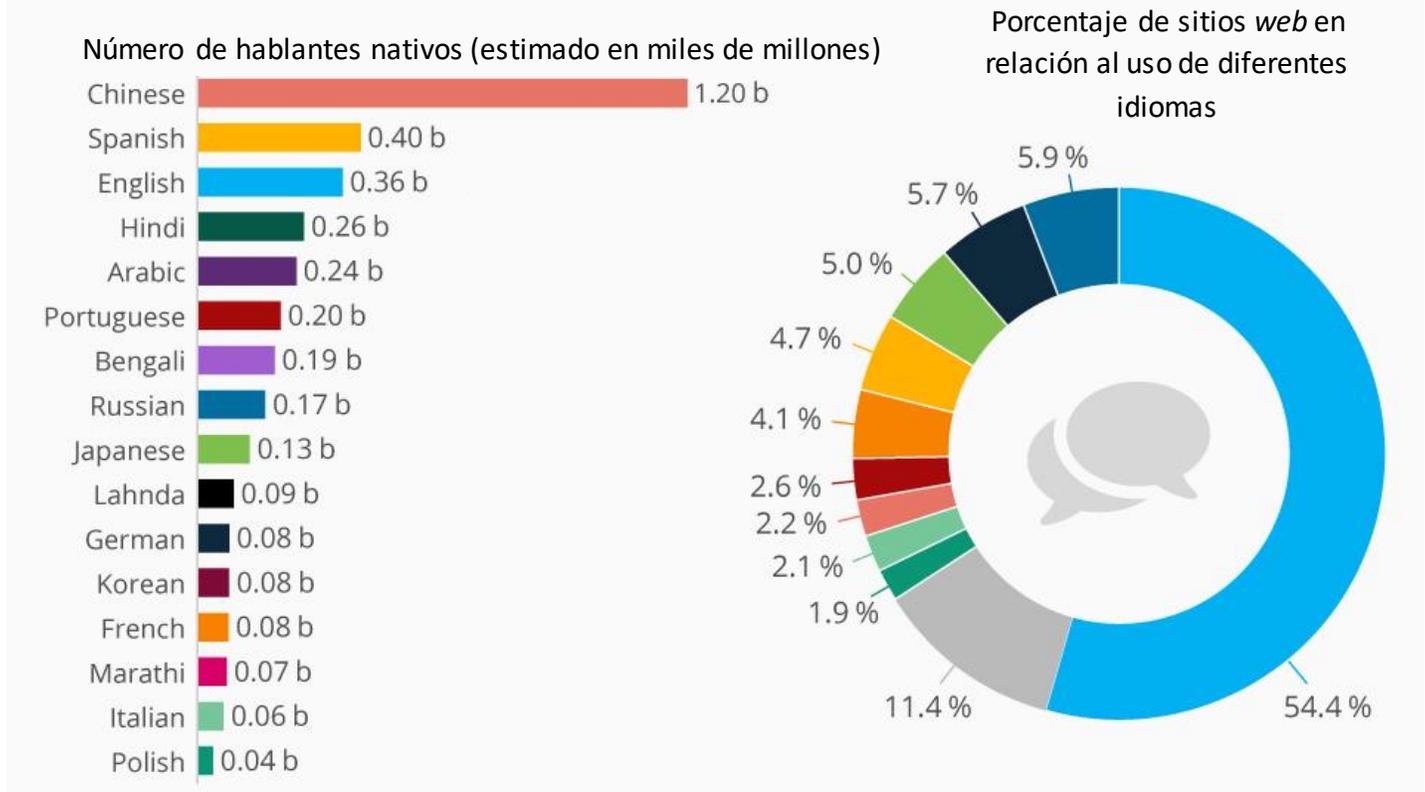
Es evidente que existe una relación intrínseca entre la cantidad de contenido *web* en un determinado idioma y la capacidad política y tecnológica de la potencia que literalmente patrocina su expansión, no obstante es menester resaltar la diferencia entre la cantidad y crecimiento de contenido en la *web* en un idioma y el número de hablantes en la vida real, y es que según datos recopilados por la *web* Statista.com a pesar de que por ejemplo la población del mundo cuya primera lengua es el español ocupa el segundo lugar en el mundo, el contenido en español conforma apenas una onceava parte del contenido en inglés. Sin mencionar que la mayoría de los sitios *web*y contenido a los que se accede al menos en los países hispanohablantes está inglés o traducido de este idioma como se puede observar en la gráfica 6.

---

<sup>88</sup> Términos acuñados por Paul Kennedy en su libro *Auge y caída de las grandes potencias*.

<sup>89</sup> Millwars S. (2012) *24% of Web Content is Now in Chinese, Will Soon Surpass English* [Infographic]. Techinasia. [en línea] Disponible en: <https://www.techinasia.com/dominantlanguages-on-internet-english-chinese> Consultado el 10/9/16

## Idiomas más usados en la *Web* y en la vida real



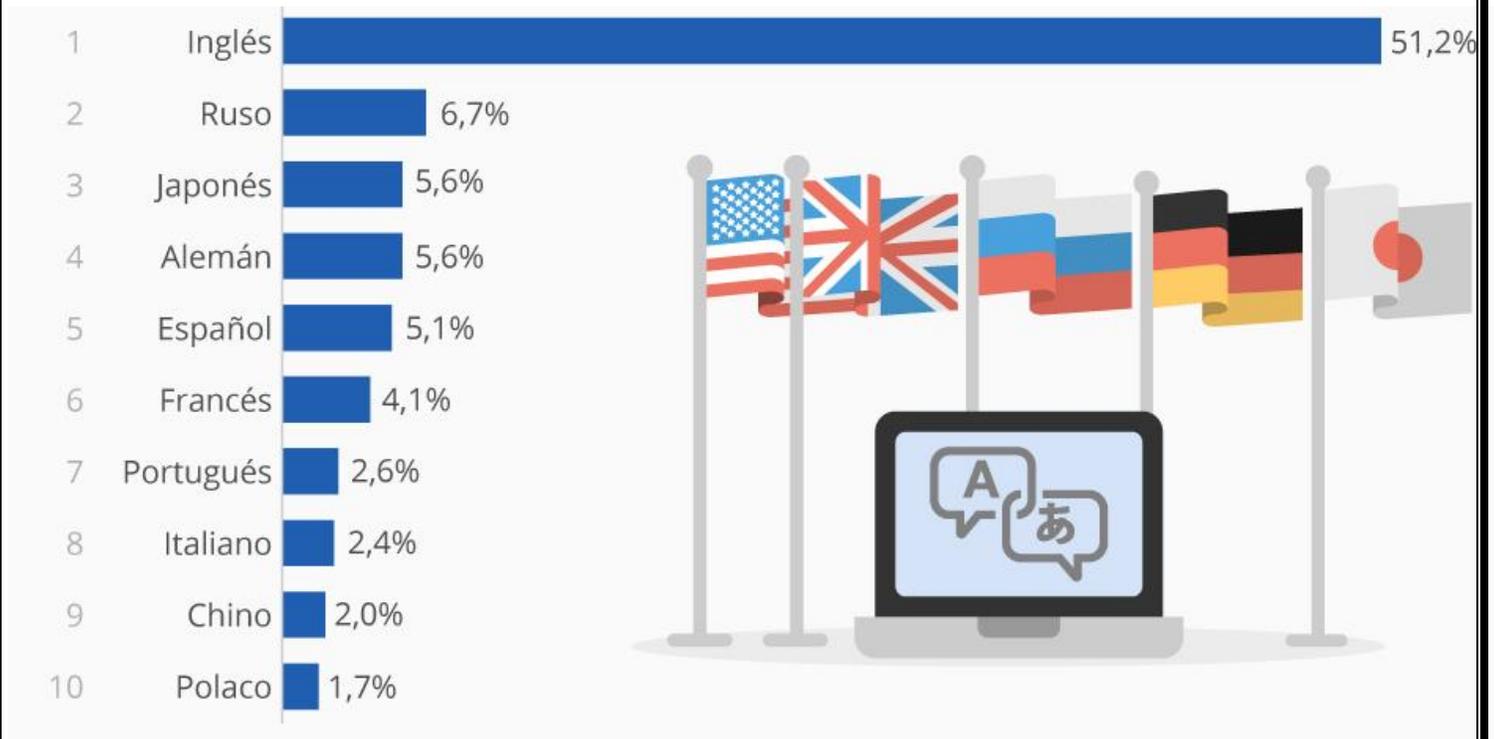
Gráfica 5. Gráfica que muestra cómo se representan los idiomas en la vida real en comparación con los 10 millones de sitios web más populares de la Internet hasta 2015.<sup>90</sup>

No obstante, a pesar del cuantioso crecimiento de la presencia del chino mandarín, así como de otros idiomas en la Internet un hecho innegable es que el inglés continúa ostentando el poder como una verdadera *lingua franca* en la denominada por Brzezinski como la “era tecnotrónica”<sup>91</sup>. A pesar de su rotunda predominancia, si se tiene en cuenta el panorama internacional actual en el que el protagonismo de los avances tecnológicos pasan de occidente hacia el oriente en donde además se debe mencionar que al menos en este ámbito los Estados ceden ante otros actores no convencionales, y es que incidentalmente solamente en Occidente las empresas trasnacionales se han apoderado de la generación, venta y

<sup>90</sup> Statista (2015) *Languages Most Used On the Web vs IRL*, Statista.com [en línea] Disponible en: <https://www.statista.com/chart/4140/low-diversity-of-languages-on-the-web-hinders-accessability/> Consultado el 6/2/18

<sup>91</sup> Brzezinski Z. (1970) *Between two ages American role in the technetronic era*. Nueva York. Estados Unidos. Consultado el 10/9/16

producción de técnicas y tecnologías innovadoras por medio de la robótica y la Internet, relegando al Estado que antaño (siglo XX) ostentaba en solitario la potestad y la capacidad económica para desarrollar este tipo de avances. Por otro lado, en países como la República Popular China la cohesión entre el gobierno y las prácticamente dos empresas proveedoras de servicios de Internet (*Alibaba* y *Tencent*)<sup>92</sup> han contribuido al crecimiento masivo del ciberespacio, así como el incremento de su uso en la vida cotidiana de las poblaciones asiáticas, lo cual podría cuestionar bastante en algunos años el rol del inglés como la lengua señera de la modernidad.



Gráfica 6. Los diez idiomas más usados en Internet según el número de sitios web en 2017.<sup>93</sup>

<sup>92</sup> Russell Ishita (2017) "China government pushes for stake in local tech giants Tencent, Alibaba, others" *Deal Street Asia*, [en línea] Disponible en: <https://www.dealstreetasia.com/stories/chinese-government-eyes-board-seats-in-local-tech-giants-including-tencent-84046/> Consultado el 6/2/18

<sup>93</sup> Moreno Guadalupe (2017), *Solo un 5% del contenido de Internet está en español*, Statista.com [en línea] Disponible en: <https://es.statista.com/grafico/11383/solo-un-5-del-contenido-de-internet-esta-en-espanol/> Consultado el 6/2/18

### 2.1.2. Tendencia política

*A priori* se ha mencionado la amplia variedad de medios dentro del ciberespacio para influir en la población, y es que, en un estricto sentido y como ya se ha mencionado se considera a la Internet como un medio para ejercer el poder blando a una intensidad completamente revolucionada, puesto que la capacidad de trasgredir de un actor internacional en la toma de decisiones de otros actores, legitimar sus resoluciones y acciones apoyadas en la opinión pública y la misma población se ve fortalecida con la velocidad y el poder de percusión de la Internet. La funcionalidad de la red para optimizar el impacto del poder blando se debe principalmente a su innovadora forma de propagación, pero también a todas las técnicas y características propias de los avances multimedia y de interfaz, los cuales acrecientan su nivel de utilidad al mostrar un rostro ciertamente efusivo a la audiencia.

Como mecanismo político a nivel al menos informativo las implicaciones de la red van desde lo más superficial como son los medios de comunicación en las que los actores más poderosos atestiguan su veracidad, hasta lo subliminal adentrándose en el terreno de las redes sociales, la moda, y la publicidad. Lo cierto es que las decisiones políticas de las potencias a las que pertenecen los sitios *web* más populares (desde redes sociales hasta motores de búsqueda) trasmutan a la desinformación.

Es muy común que ante cualquier evento relevante se muestren al usuario los acontecimientos desde solo una perspectiva moldeada por las aspiraciones políticas y/o los intereses del *establishment*, tratando de explicar los sucesos solamente desde esa visión, anulando las versiones alternativas, de hecho, podríamos decir que no solo se busca, sino que se fuerza el error analítico. Naturalmente, la trascendencia de la información manipulada políticamente a través del Internet se encuentra en que su propagación se realiza de forma sistemática con el apoyo de toda la plataforma mediática, repercutiendo no solo en el territorio de origen sino evidentemente expandiéndose hacia las zonas de influencia de la potencia mundial, o en su caso del gobierno u empresa local.

Como se ha explicado a lo largo de esta investigación es muy importante recalcar que el amplio conocimiento de la audiencia por parte de los orquestadores del poder

mundial se debe al monitoreo de su comportamiento en la red, elaborando incluso el perfil de cada usuario con base en la información recabada constantemente.

En el escenario político las contrapartes juegan al prestigio de sí mismas y al desprestigio de los adversarios empleando los medios más sofisticados para no solo legitimar sino inclusive para normalizar su visión de los hechos, dicho de otro modo, se sirven de la Internet para esparcir un mensaje favorable a las decisiones que convengan al grupo de poder dominante en sus Estados o del gobierno de la potencia con mayor poder político, económico y/o militar en la región<sup>94</sup>. Asimismo, la red se utiliza para vilipendiar a los elementos opuestos o encontrados con los intereses políticos del grupo dominante al interior de un Estado, ya sean organizaciones insurgentes, terroristas, etcétera. como gobiernos locales o de otros Estados, empresas transnacionales locales y/o extranjeras.

Citando una vez más a la concepción del ciberespacio como la reflexión de la sociedad internacional, actualmente la huella de la potencia mundial imperante, Estados Unidos se refleja, (como ya se ha visto y se ejemplificará más adelante) en su absoluta preponderancia ya no de contenido sino a nivel de páginas *web* visitadas a nivel mundial. Consecuentemente se debe denotar que la opinión y los actos públicos al menos en la parte del mundo donde la influencia política y económica de este país es más grande refleja la actual disputa interna entre su gobierno encabezado por Trump cuya política apoya al viejo modelo capitalista estadounidense <sup>95</sup> (caracterizado por la producción de energía propia como los combustibles fósiles, así como la industria de las armas, dominante hasta la entrada de la tecnología y la Internet en el mercado) y el nuevo modelo caracterizado por el desarrollo de dependencia tecnológica por parte los países en sus zonas de influencia como América Latina para con las empresas ubicadas en el *Silicon Valley*

---

<sup>94</sup> Bandurski, David (2015) "How China's Government Controls the News: A Primer", *Foreign Policy*, Foreignpolicy.com [en línea] Disponible en: <http://foreignpolicy.com/2015/07/21/china-media-xi-jinping-crackdown-newspaper/> Consultado el 6/2/18

<sup>95</sup> Parker, Ashley (2016) "Donald Trump's Energy Plan: More Fossil Fuels and Fewer Rules", *The New York Times*, Nytimes.com[en línea] Disponible en: <https://www.nytimes.com/2016/05/27/us/politics/donald-trump-global-warming-energy-policy.html> Consultado el 6/2/18



y otras partes de ese país, *incidentalmente Google, Facebook* y los proveedores de Internet como *Verizon* o *AT&T*.

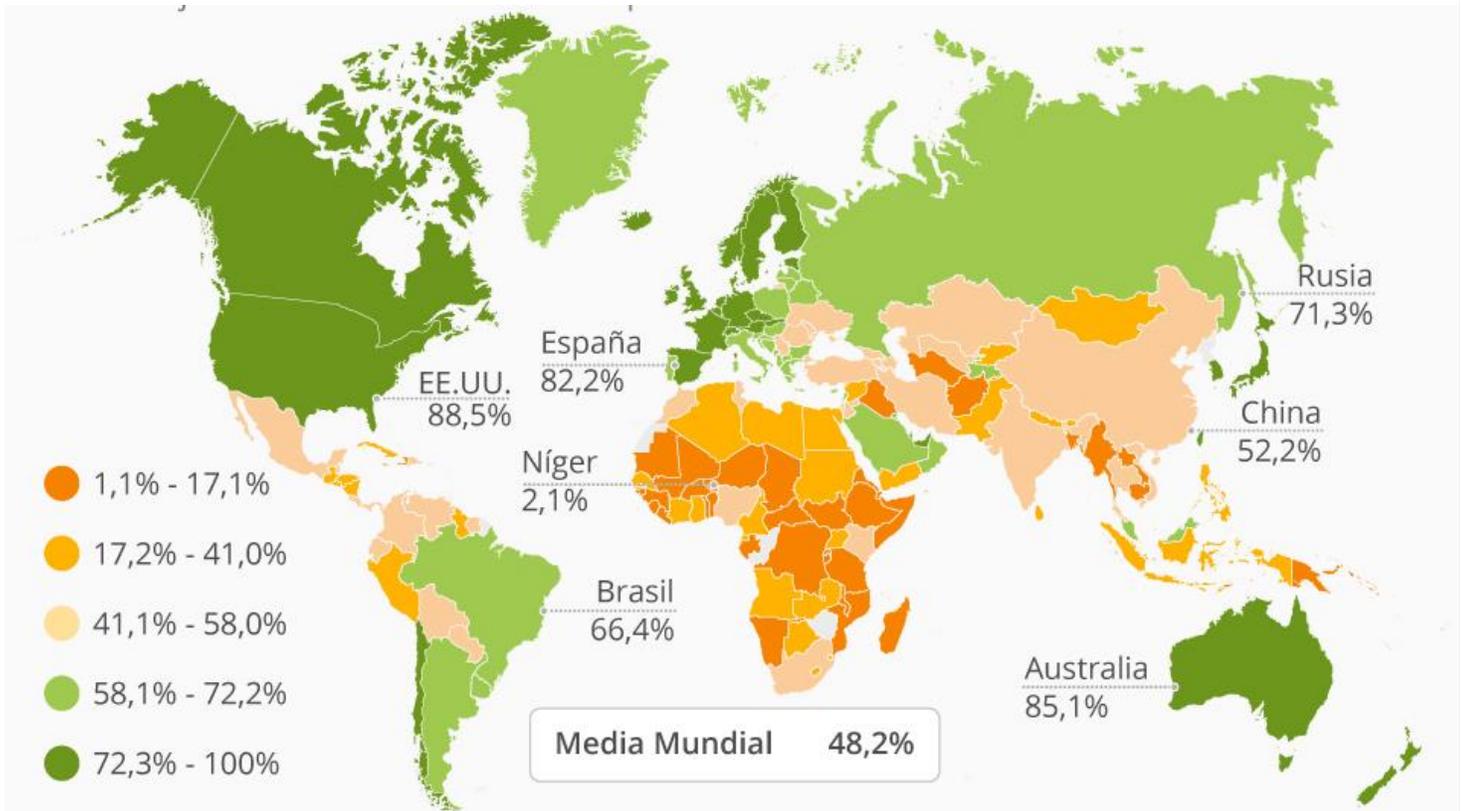
En resumen, se sostiene que, como construcción humana, hasta cierto punto el ciberespacio es el reflejo de la estructuración del sistema internacional e incluso se le puede considerar como el porvenir de esta, puesto que se encuentra mayoritariamente regido directamente por empresas privadas aún y cuando estas representan los intereses del Estado al que pertenecen o bien a aquel predominante en su región o bloque político y económico. Por otra parte, independientemente a la relativa relación (como es en el caso de la República popular China) de la distribución de los usuarios de Internet relacionada con el nivel demográfico en cada región, el nivel socioeconómico es el que marca la división entre la población con acceso a Internet concentrada en los países comprendidos en el G-7, las áreas metropolitanas de sus áreas de influencia y el resto del mundo.

Para ilustrar, de acuerdo con datos publicados por la Tech in Asia, hasta 2017 la República Popular China detenta más de 731 millones de usuarios, alrededor del 53% de la población en línea<sup>96</sup> Sin embargo, como antes ya se ha señalado a pesar de que la audiencia más grande se ubica en otras regiones del hemisferio, incidentalmente en la República Popular China, los servidores de Internet, las empresas dedicadas al registro de dominios, así como los proveedores de servicios de Internet, y la mayoría de desarrolladores de sitios *web* más populares y usados continúan perteneciendo o trabajando en las potencias occidentales<sup>97</sup>. La sombra del pasado colonial europeo y el presente neocolonial abanderado por Estados Unidos da cuenta del dominio informático concentrado en occidente que hasta hace 5 años vivía su auge más importante.

---

<sup>96</sup> Millward, Steven (2017) "China now has 731 million internet users, 95% access from their phones", *Tech in Asia*, Techinasia.com [en línea] Disponible en: <https://www.techinasia.com/china-731-million-internet-users-end-2016> Consultado el 6/2/18

<sup>97</sup> Ueland, Sig (2017) *20 Top Internet Service Providers*, Practivalcommerce.com [en línea] Disponible en: <https://www.practicalcommerce.com/20-Top-Internet-Service-Providers> Consultado el 6/2/18



Mapa 2. Porcentaje de usuarios de Internet en proporción con la población total por países en 2016.<sup>98</sup>

Extractando, el posicionamiento de Asia y particularmente de la República Popular China en el ciberespacio no deja de aumentar, ya se ha explicado antes el hecho potencial de que más de la mitad de la población activa en la Internet a nivel planetario está en ese país, sin mencionar el lento pero importante incremento del contenido disponible en la *web* en chino mandarín.

Asimismo, existe una relación directa entre el crecimiento de la población en la región de Asia y pacífico y la dilatación del contenido *web* en los últimos años; si a esto sumamos la presencia de grandes innovadores en tecnología como la República de China (Taiwán), Corea del Sur y Japón cuyos desarrollos se enfocan en las telecomunicaciones celulares, la robótica, y los sistemas computarizados. Cabe mencionar que, los adelantos llevados a cabo por estos países están dirigidos hacia

<sup>98</sup> Moreno Guadalupe (2017) *El mapa del alcance de Internet*, Statista.com [en línea] Disponible en: <https://es.statista.com/grafico/7742/el-mapa-del-alcance-de-internet/> Consultado el 6/2/18

el consumo de la sociedad civil, por otra parte, la República Popular China orienta la mayoría de sus esfuerzos hacia el campo militar y del poder blando<sup>99</sup>.

Esto es, que los chinos no solamente suman a la audiencia, sino que también producen contenido, cosechando avances para conquistar los ordenadores del mundo en medio de una guerra cibernética de desgaste contra las potencias mundiales occidentales. En realidad, la pugna por la hegemonía del control del tráfico informático se realiza fundamentalmente en la *Surface web*, dejando en un plano secundario el hermetismo del resto del contenido en la Internet, en este sentido límpidamente se compite aparentemente fuerte por el dominio de solo la parte más convencional y escrutable de la red debido claramente a que la presencia de la ciber audiencia mundial se localiza en tal pequeña porción.

## **2.2. Motores de búsqueda, navegadores *weby* redes sociales, herramientas de influencia política mundial.**

Hace al menos quince años, difícilmente se podía hablar de una competencia o rivalidad directa y potencial de cualquier otro actor internacional frente al poderío estadounidense evidenciado en su predominancia ciberespacial, así como en la innovación y desarrollo de las TIC. Empero, el tablero geopolítico actual refiere a la flamante presunción de que el mundo ya no es unipolar, y que consecuentemente la red informática mundial ha trascendido a una escala de complejidad amplísima que reúne a más de un actor en la lucha frontal por el dominio en la Internet.

Como riel del progreso técnico y científico en la contemporaneidad, la Internet es la refracción de la dinámica internacional, ya que los grandes avances están ciertamente focalizados entorno al enriquecimiento del poder blando. A propósito, el

---

<sup>99</sup> Wong E y Buckley C. (2015) *China's Military Budget Increasing 10% for 2015, Official Says*. The New York Times. [en línea] Disponible en: [http://www.nytimes.com/2015/03/05/world/asia/chinas-military-budget-increasing-10-for-2015-official-says.html?\\_r=0](http://www.nytimes.com/2015/03/05/world/asia/chinas-military-budget-increasing-10-for-2015-official-says.html?_r=0) Consultado el 21/9/16

epicentro de la evolución y actividades desarrolladoras del *soft* power están basadas fundamentalmente en la red.

En este tenor tanto los navegadores y buscadores *web* como las redes sociales tienen un papel central ya que como se explicará de forma concisa más adelante es a través de los buscadores *web* que se recopilan datos de cada búsqueda que realiza el usuario; de las redes sociales que se monitorea y analiza mediante algoritmos especializados el comportamiento de la audiencia que las utiliza, ambos funcionando por medio navegadores con rastreadores y herramientas integradas como las mencionadas *Google Analytics* o *Yandex.Metrica* que colaboran con las agencias gubernamentales de los Estados más poderosos.

Como se puede observar en la tabla 6 la idea expuesta a lo largo de la presente investigación en la que se asevera que la distribución, contenido y dinámica en la Internet evidencia la competencia inexorable entre los Estados con las economías más avanzadas que, además representan diferentes bloques políticos y comerciales alrededor del mundo, incidentalmente la rivalidad entre Estados Unidos, la República Popular China y Rusia y es que *Google(.com)* —estadounidense— es el motor de búsqueda más utilizado junto con sus servidores en otros países de su zona de influencia como Brasil(.br) Reino Unido(.uk.) y México(.mx), le sigue *Baidu* —chino— y poco después *Yandex* —ruso—.



| Clasificación | Sitio web       | Categoría                            | Evolución | Duración promedio de la visita | Páginas visitadas |
|---------------|-----------------|--------------------------------------|-----------|--------------------------------|-------------------|
| 1             | google.com      | Internet and Telecom > Search Engine | =         | 00:07:20                       | 8.10              |
| 2             | baidu.com       | Internet and Telecom > Search Engine | =         | 00:08:53                       | 8.29              |
| 3             | yidianzixun.com | Internet and Telecom > Search Engine | =         | 00:14:58                       | 7.34              |
| 4             | google.co.in    | Internet and Telecom > Search Engine | =         | 00:07:49                       | 6.46              |
| 5             | google.com.br   | Internet and Telecom > Search Engine | +1        | 00:08:45                       | 7.14              |
| 6             | yandex.ru       | Internet and Telecom > Search Engine | +1        | 00:10:23                       | 8.72              |
| 7             | google.co.id    | Internet and Telecom > Search Engine | +2        | 00:08:50                       | 7.39              |
| 8             | google.co.uk    | Internet and Telecom > Search Engine | =         | 00:09:25                       | 7.02              |
| 9             | sogou.com       | Internet and Telecom > Search Engine | -4        | 00:05:34                       | 4.69              |
| 10            | google.de       | Internet and Telecom > Search Engine | +1        | 00:08:59                       | 6.89              |
| 11            | google.com.mx   | Internet and Telecom > Search Engine | -1        | 00:07:36                       | 7.03              |
| 12            | google.co.jp    | Internet and Telecom > Search Engine | =         | 00:11:00                       | 7.75              |
| 13            | google.fr       | Internet and Telecom > Search Engine | =         | 00:09:46                       | 6.95              |

Tabla 6. Tabla que muestra los 13 motores de búsqueda web más utilizados a nivel mundial hasta enero de 2018.<sup>100</sup>

### 2.2.1. Navegadores y motores de búsqueda *web*

Si bien se ha señalado que en realidad la pugna por el dominio en la Internet la tenemos que reducir a la contienda por solo la parte más superficial de esta, es innegable que la rivalidad comercial y de influencia política afecta y trasforma la vida social de la población mundial activa en la Internet. De esta forma considerando la trascendencia de los navegadores y los motores de búsqueda *web* y las técnicas de manipulación de la información señaladas en el primer capítulo, se debe considerar al contenido informático al menos en la *Surface web* como el producto de la desinformación y la contra-propaganda no esencialmente dirigida a los rivales políticos y económicos de un lado u otro del tablero mundial sino contra la audiencia localizada en la órbita de una determinada potencia.

Dicho de otra manera, existe un control particular de la navegación adecuado a la legislación de cada Estado, y esta a su vez, no está de más señalar que se acopla a los intereses de la élite en el poder. Así pues, se debe tener en cuenta que a pesar de que se utilice el mismo navegador o motor de búsqueda, los criterios para la pesquisa de la información están preseleccionados en cada país.

En el mundo del ciberespacio los motores de búsqueda significan la puerta a la información, el mecanismo más convencional a través del cual la audiencia mundial de la Internet puede ingresar al contenido que, aunque limitado tiene una extensión gigantesca. Lo cierto es que al menos un 40% de la población mundial navega mediante motores de búsqueda caracterizados por el uso del *spamdexing*, rastreadores y *spyware*; como se muestra en el mapa 3 creado por Mark Graham y Stefano de Sabbata del *Oxford Internet Institute* a partir de los datos recopilados por la compañía de *Amazon*, *Alexa* encargada del análisis del comportamiento del tráfico informático mundial y que a pesar de haber sido creado en 2013 sigue constituyendo una referencia aproximada de la distribución de la audiencia en el ciberespacio a nivel mundial, como se puede constatar en la tabla 6 y el mapa 4.

Como bien menciona Michael Kelley “los resultados son fascinantes: *Google*

---

<sup>100</sup> Statista (2018) *Top Websites Ranking- Search Engine in the world*, Statista.com [en línea] Disponible en: <https://www.similarweb.com/fr/top-websites/category/internet-and-telecom/search-engine> Consultado el 6/2/18

domina la mayor parte de América del Norte, Europa, Asia del Sur y el sur del Pacífico, mientras que *Facebook* gana en las partes de habla hispana de América, Oriente Medio y el Norte de África [...]

Los investigadores Mark Graham y Stefano De Sabbata notan que entre los 50 países donde *Facebook* aparece como el sitio *web* más visitado, *Google* o *YouTube* (adquirido por *Google* en 2006) quedan en segundo lugar”<sup>101</sup>.

En suma, de acuerdo con los mismos datos resalta que la empresa estadounidense *Google* continúa ostentando el rol como la página con más visitas en casi todo el mundo, seguida de la también norteamericana *Facebook*<sup>102</sup>. Si bien el centro del desarrollo cibernético actual y futuro se encuentra en Estados Unidos, ciertamente la competencia asiática apuesta a un desarrollo cibernético a largo plazo con frutos que bien podrían desbancar incluso a los servicios prestados por las empresas de Norteamérica. Conjuntamente es necesario aludir a la cuestión del número de usuarios no solo como cantidad sino su grado de influencia en la transformación de la red informática mundial que más allá de conservar una identidad o rasgos específicos establecidos por sus creadores se adapta a la dinámica económica y política, en otros términos, se debe tener en cuenta que la población hoy no solamente cuenta, sino que produce y modifica, en efecto de acuerdo a parámetros antes instaurados. De cualquier modo, la audiencia digital otorga información que coadyuva para planificar el desarrollo de la estructura de la Internet en el porvenir, con cada palabra clave ingresada en los motores de búsqueda, o la simple utilización de un sistema operativo.

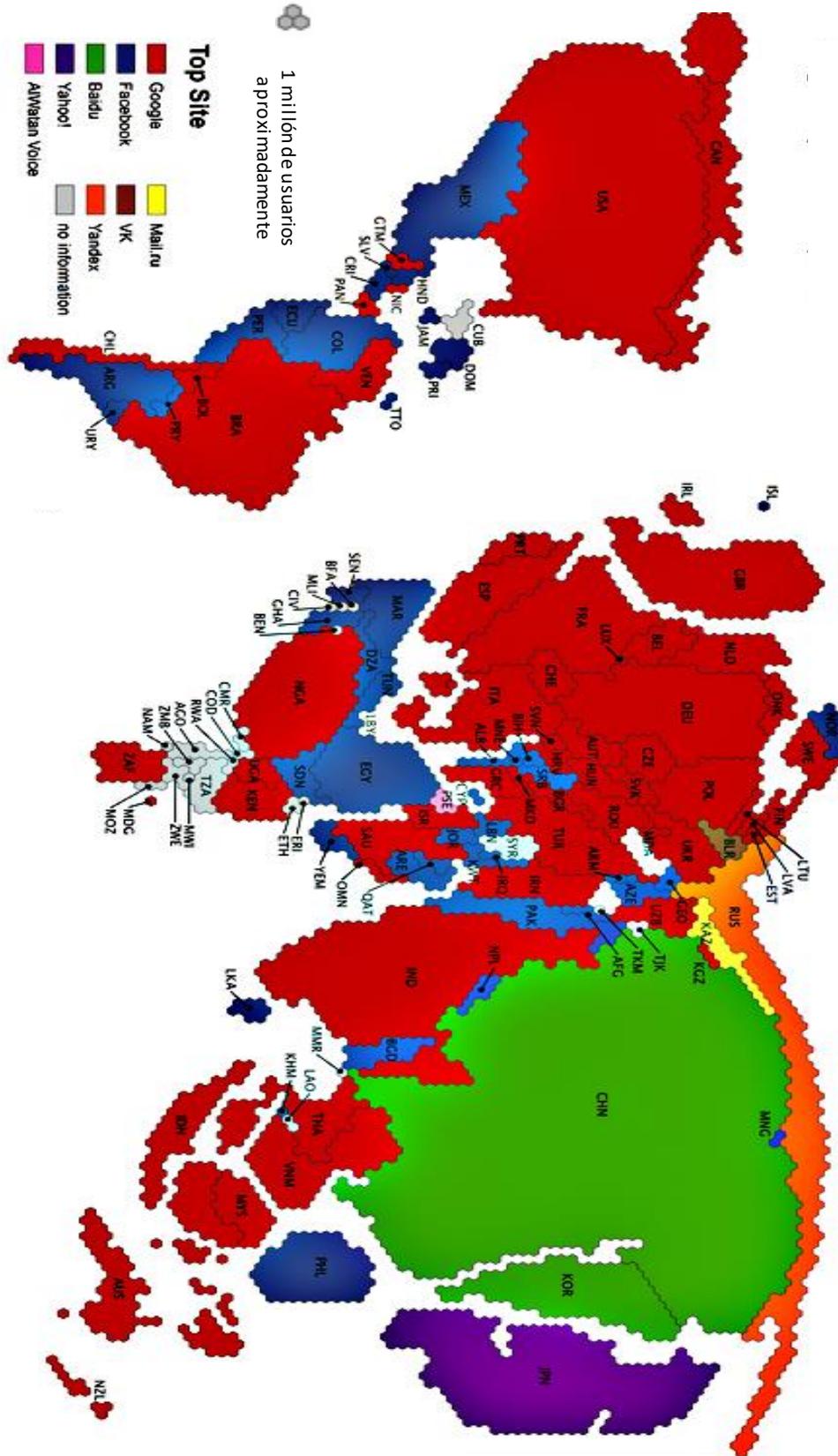
Como se verá más adelante concretamente centrándose en los navegadores y motores de búsqueda *web* más importantes del mundo, la balanza del número de usuarios activos mediante *Google* en la red parece estar equilibrada con respecto a su rival más cercana, *Baidu* no obstante, se debe hacer hincapié en que la influencia de la empresa estadounidense está posicionada como la página con mayor número de visitas en más de tres cuartas partes de los países del mundo, mientras que el

---

<sup>101</sup> Kelley M. (2013) *The World's Most Popular Web Sites By Country [MAP]*. Business Insider India [en línea] Disponible en: <http://www.businessinsider.in/The-Worlds-Most-Popular-Web-Sites-By-Country-MAP/articleshow/23530271.cms> Consultado el 28/19/16

<sup>102</sup> Similar Web (2017) *Top Websites Ranking, Worldwide*, op.Cit.

20% de la población mundial activa en la red se encuentra en un solo país: la República Popular China. Igualmente, en la Federación Rusa y su órbita de influencia, particularmente en Bielorrusia y Kazajstán, ni *Google* ni cualquiera de sus compañías hermanas figura como el navegador *web* más utilizado ya que su lugar lo ocupa *Yandex*.



Mapa 3. Mapa que muestra las páginas más visitadas y la cantidad aproximada de usuarios por país hasta 2013.<sup>103</sup>



### 2.2.1.1. Google

Si bien la Internet ya existía en la última década del siglo XX, estaba a un paso de popularizarse y devenir en un instrumento corriente y comercial, el medio para navegar a través de la cuantía de archivos indexados no había sido desarrollado de manera sofisticada, la red informática mundial aún estaba incompleta como para ingresar al mercado internacional. De 1994 a 2000 inició el proceso de desarrollo de los motores de búsqueda *web*, uno de los principales en esa época fue *World Wide Web Worm* (WWW) desarrollado en 1994 por Oliver McBryan de la Universidad de Colorado el cual contaba con un índice superior a las 110 mil páginas *web*<sup>104</sup> cifra considerada atroz en ese entonces; empero solamente tres años más tarde el buscador también estadounidense *WebCrawler* ya contaba con 2 millones de páginas *web* y con alrededor de 100 millones de documentos disponibles en línea.

No obstante, hasta 1997 es que Larry Page y Sergey Brin de la Universidad de Standford afianzan el proyecto de sus esfuerzos por la creación de un buscador *web* calificado para integrarse a la audiencia mundial y con grandes perspectivas a futuro, de modo que el dominio *Google.com* se registra el 15 de septiembre de ese año <sup>105</sup> cuyo nombre digno a las expectativas de sus creadores buscaba desde entonces organizar un número supuestamente inacabable de información en línea. La creación de *Google* significó el paso más allá de la acumulación de páginas *web* puesto que fue el primero que estableció una categorización de las búsquedas y palió la falta de orden y la dificultad para ingresar a la gama de información vertida en la red.

---

<sup>103</sup> Alexa (2013) *Most visited website per country*. Oxford Internet Institute en Kelley M. The World's Most Popular Web Sites By Country [MAP]. Business Insider India [en línea] Disponible en: <http://www.businessinsider.in/The-Worlds-Most-Popular-Web-Sites-By-Country-MAP/articleshow/23530271.cms> Consultado el 28/19/16

<sup>104</sup> Brin S. y Page L. The Anatomy of a Large-Scale Hypertextual Web Search Engine. Computer Science Department, Stanford University, Stanford. [en línea] Disponible en: <http://infolab.stanford.edu/~backrub/google.html> Consultado el 14/10/16

<sup>105</sup> Nuestra historia en profundidad. Google Empresa [en línea] Disponible en : <https://www.google.com/about/company/history/> Consultado el 14/10/16



Análogamente, Estados Unidos requería asestar un golpe de autoridad a las posibles competencias que ya se estaban desarrollando en otras partes del mundo, reafirmando su *status* como potencia mundial también en el ciberespacio. En los años subsecuentes *Google* creció gradualmente, potenciando su capacidad de incidencia e inserción en la vida de la población mundial activa en la Internet a través del uso mediante los ordenadores y posteriormente con los móviles.

A continuación, emplazamos la cronología que expresa el crecimiento de la compañía estadounidense a partir de 1999, recopilada por Danny Sullivan en *Google now handles at least 2 trillion searches per year*<sup>106</sup>.

- **1999:** Tan solo un año y medio después del registro *de* Google en la red ya se contaba con la cifra *de* 1 billón de búsquedas por año, con un índice de 3 millones de búsquedas por día.
- **2000:** 14 mil millones con más de 18 millones de búsquedas a diario para la primera mitad de ese año, mientras que para la segunda alcanzó 60 millones.
- **2001–2003:** Durante este periodo se llegó a 55 millones de búsquedas.
- **2004–2008:** *Google* llega a tener 73 miles de millones de búsquedas, bajando ligeramente su ritmo de crecimiento con respecto a los años precedentes.
- **2009:** Antes de la caída en picado del porcentaje de crecimiento la compañía alcanzó más de 365 mil millones de búsquedas en este año, con alrededor de mil millones de búsquedas diarias.
- **2012–2015:** Reafirmando su estancia en el pedestal de los motores de búsqueda, *Google* llega a 1.2 billones de búsquedas en estos años con 3 mil millones de búsquedas diarias.
- **2016:** Se registraron casi 2 billones de búsquedas.
- **2017-2018:** Según datos recopilados por el algoritmo de *Worldometers*, el cual procesa los datos elaborados mediante análisis estadísticos a partir de *Internet Live Stats*, *Google* procesa más de 40,000 consultas de búsqueda

---

<sup>106</sup> Sullivan D. (2016) *Google now handles at least 2 trillion searches per year*, Search Engine Land, [en línea] Disponible en: <http://searchengineland.com/google-now-handles-2-999-trillionsearches-per-year-250247> Consultado el 15/10/16

cada segundo en promedio, lo que se traduce en más de 3,500 millones de búsquedas por día y en promedio<sup>107</sup>.

Actualmente las cifras apuntalan a que la media de búsquedas de *Google* en el porvenir con todo y la competencia sigue siendo simplemente monstruosa ya que podría mantenerse en más de 1.2 mil de billones por año. Los números publicados por *Internet Live Stats* son inverisímiles y dan cuenta del potencial y la cantidad de incidencia que puede tener un motor de búsqueda en la vida de la audiencia, ya que podría decirse que al menos la población activa en la Internet mantiene en su media y en crecimiento la cantidad de búsquedas como se puede constatar en los números ya señalados.

Por otro lado, *Google* comenzó a decrecer en la medida en la que otras compañías de motores de búsqueda como, *Yahoo*, *Baidu* y *Yandex* apareciesen con mayor fuerza en el mercado internacional, en especial las últimas dos las cuales acapararon el contenido ciberespacial de sus zonas de influencia para controlar el tráfico informático interno en su territorio.

Sin embargo, es un hecho innegable que a pesar del progresivo declive en su utilización estos últimos años, *Google* ostenta por mucho el primer lugar como el motor de búsqueda más empleado a nivel mundial, y en realidad está lejos de ser desbancado por cualquier otra competencia. Paralelamente a su crecimiento, en cuestión de búsquedas millones de sitios *web* se integran a sus índices cada año, aseverando su trascendencia mediante todas las aplicaciones y espacios vinculados, que van desde redes sociales hasta *blogs*.

Si a esto sumamos la unión con otras importantes empresas de occidente, ya sean de servicios electrónicos de todo tipo, periódicos en línea, publicitarias etcétera. entendemos el potencial de la compañía estadounidense conjugado como un consorcio monopolístico gigantesco que busca abarcar ya no solamente las acciones en búsquedas por la Internet, sino también las actividades cotidianas de la población trasladadas a la red informática mundial. Conjuntamente cabe mencionar que en

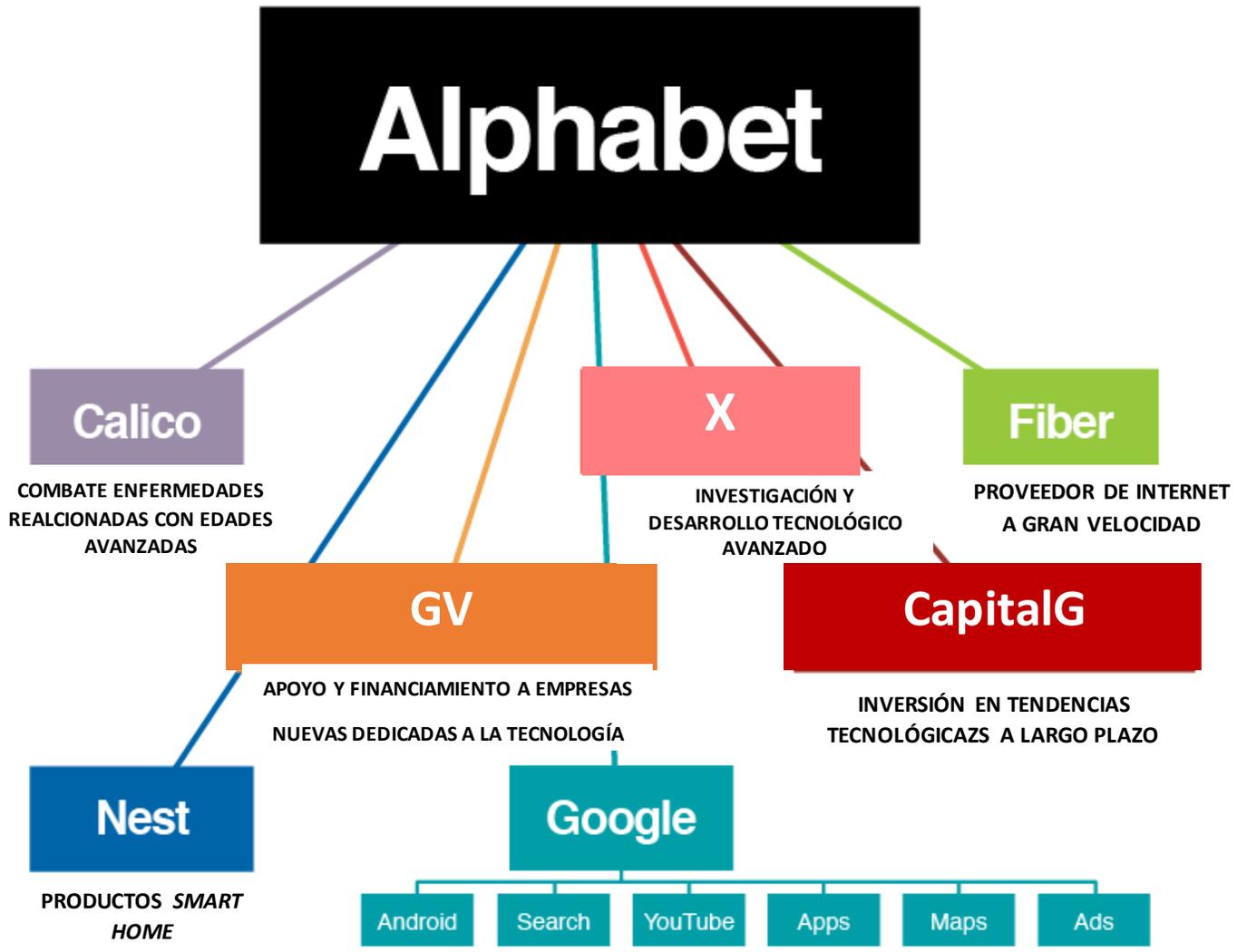
---

<sup>107</sup> Internet Live Stats (2018) *Google Search Statcs*, [Internetlivestats.com](http://www.internetlivestats.com) [en línea] Disponible en: <http://www.internetlivestats.com/google-search-statistics/> Consultado el 7/2/18

2015<sup>108</sup> *Google* reestructuró el consorcio en su totalidad, básicamente cambiando el nombre de su empresa a *Alphabet*, de esta manera *Alphabet* se convirtió en la cabeza de la empresa multinacional en otras palabras fue creada como una herramienta de gestión para todo el consorcio, cuyas subsidiarias principales son *Google* (desde entonces dedicada exclusivamente a servicios de Internet como correo electrónico y redes sociales ), *Nest* (dedicada a la creación de productos “Smart house”) entre otras.

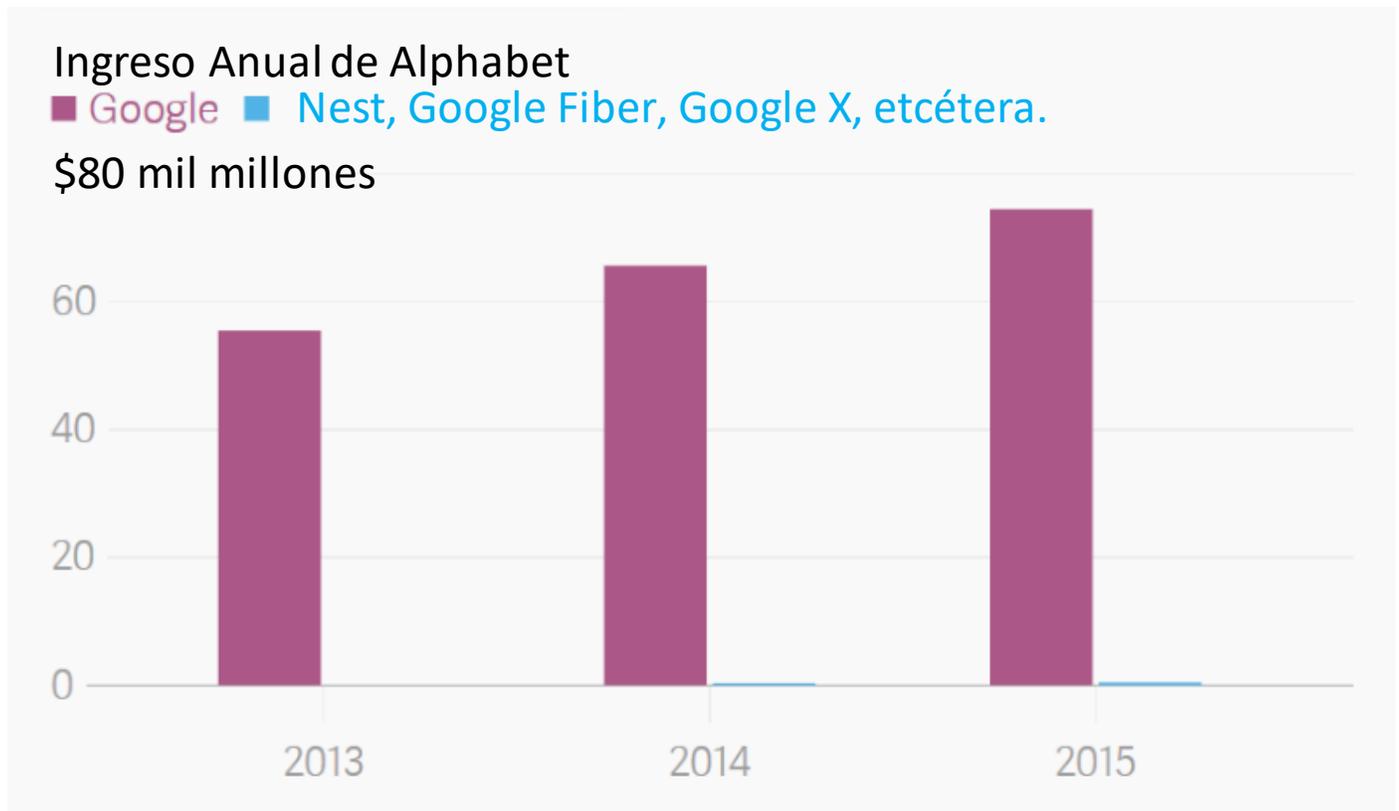
---

<sup>108</sup> Goldman, David (2015) *Google Will become Alphabet Today*, Cnn.com [en línea] Disponible en: <http://money.cnn.com/2015/10/02/technology/google-alphabet/index.html> Consultado el 11/2/18



Esquema 2. *Alphabet* (*Google* antes de la reestructuración interna) y sus subsidiarias principales. <sup>109</sup>

<sup>109</sup> *Íbid.*



Gráfica 7. Ingreso anual de *Alphabet* en dólares cuya principal subsidiaria es Google.<sup>110</sup>

### 2.2.1.2. *Baidu*

Es la compañía china más importante en materia de desarrollo de *software* y servicios en la Internet. Al igual que otras de sus grandes símiles, el proyecto que da origen a Baidu aparece en los años previos al nuevo milenio, y alcanza solidez para fundarse oficialmente en el año 2000 por Robin Li. Desde sus inicios, fue contemplado como una apuesta a largo plazo que contara con la posibilidad para contender con otras partes del mundo, y es que el mercado de Asia y pacífico es el segundo más grande del mundo<sup>111</sup>, de tal suerte que su desarrollo ha estado centrado no únicamente como un propósito de fomento económico sino con fines de control e

<sup>110</sup> Frommer Dan, (2016) *Google's first Alphabet earnings in charts*, Qz.com [en línea] Disponible en: <https://qz.com/607378/were-live-charting-googles-first-alphabet-earnings/> Consultado el 11/2/18

<sup>111</sup> Doland. A. (2016) *After New Regulations in China, What's Ahead for Baidu?* Advertising Age. [en línea] Disponible en: <http://adage.com/article/digital/regulations-china-ahead-china-sbaidu/304745/> Consultado el 08/10/16

influencia política sobre toda la región. Por consiguiente, la proposición de gobierno de la República Popular China está centrada en salvaguardar el baluarte ciberespacial estratégico de dicha zona ante el poderío creciente de las innumerables compañías de servicios *web* y *software* europeas, rusas y principalmente estadounidenses que abordaban a la audiencia asiática cuando la compañía china ni siquiera se había consolidado en el mercado local.

Empero, hay varios componentes que nos ayudan a analizar la magnitud de la importancia de *Baidu* en la contemporaneidad, y en suma se encuentran relacionados con la postura de la República Popular China, uno de ellos es la amenaza que las compañías extranjeras llegaron y representan hoy, puesto que dicho apereamiento fue potenciado por la utilización de los aliados de Estados Unidos como pivotes para la entrada del modelo de capitalismo estadounidense a través de la Internet, aliados por cierto permeados con una gran influencia occidental que por sí solos ya representaban una competencia incómoda, Japón, Corea del Sur y la misma República de China (Taipéi).

Es necesario resaltar la importancia que tiene la publicidad desde una lectura política, como medio crucial para la aplicación del poder blando y además como incentivo económico, puesto que la gran mayoría de los ingresos en el mercado de búsquedas provienen de los anuncios que aparecen en las búsquedas que efectúan los usuarios mientras navegan por la *web*. En este sentido, la necesidad por el control del tráfico de contenido de origen extranjero empujó al gobierno de este país a crear su propio modelo de navegación, en efecto a partir de las plantillas estadounidenses, pero con fines divergentes traducidos en la política de seguridad cibernética que restringió la entrada de empresas extranjeras las cuales estaban en la vía por la monopolización del ciberespacio chino.

Además, como bien asevera Keith Bradsher en *China Toughens Its Restrictions on Use of the Internet* “la nueva normativa, emitida por la Comisión permanente del Congreso Nacional del pueblo, permite a los usuarios de Internet continuar adoptando seudónimos para sus anuncios en línea, pero sólo si primero proporcionan sus nombres reales a los proveedores de servicios, una medida que podía relajar algunos de los vibrantes diálogos (en los *twits* y *microblogs* emitidos

dentro del país en relación con la política china). Las autoridades periódicamente detienen e incluso meten a la cárcel a los usuarios de Internet por comentarios políticamente sensibles, como las llamadas para una democracia multipartidista o acusaciones de deshonestidad de los funcionarios locales”<sup>112</sup>.

Y es que como se ha mencionado, la razón por la que los gigantes estadounidenses no tengan éxito en la República Popular China radica en que *Baidu* se encuentra adherido a la política de censura del gobierno. Por consiguiente, si el sitio web presenta características que se consideran inadecuadas para el público chino se incluye en la “lista negra” para no aparecer en los resultados del navegador y el motor de búsqueda.

En efecto el comportamiento del gobierno chino en el ciberespacio responde a sus aspiraciones comerciales y políticas, puesto que, poseer una población con visiones acotadas por un ámbito cibernético basado en el esquema desarrollado y monitoreado por el propio gobierno es sustancial para mantener bajo control a su población. Por añadidura Google ha sido relegado a Hong Kong para evadir el régimen de Beijing, además de que en cuanto a búsquedas referentes a la cultura occidental como ciertas páginas y medios de comunicación el buscador presente una ineficiencia occidental desde una I.P. china.

Si bien las políticas chinas afectaron el crecimiento a corto plazo de la compañía ya que se limitó el ingreso a sitios *web* y se endurecieron las medidas para las características y la cantidad de anuncios en sus búsquedas, se trata de un proyecto orientado a fines en grande y a largo plazo en busca de alcanzar la colosal magnitud de *Google* en la Internet, pero mediante un medio y plataforma chino. A propósito, según *eMarketer* actualmente *Baidu* que en cuestión de los ingresos por búsqueda global posee el 8.8% de las ganancias no consigue ser una competencia a nivel mundial para el titán estadounidense que en tanto aglomera la gigantesca proporción del 55% de los ingresos<sup>113</sup>.

---

<sup>112</sup> Bradsher K. (2012) *China Toughens Its Restrictions on Use of the Internet*. The New York Times. [en línea] Disponible en:[http://www.nytimes.com/2012/12/29/world/asia/china-toughensrestrictions-on-internet-use.html?\\_r=2](http://www.nytimes.com/2012/12/29/world/asia/china-toughensrestrictions-on-internet-use.html?_r=2) Consultado el 15/10/16

<sup>113</sup> Baidu Revenues en *op.Ccit*. Doland A.(2016)

No obstante, la trascendencia de la compañía China es gigantesca tanto que, según las últimas estadísticas, además de ser el buscador más popular en China, conforme a datos de Alexa ostenta el 5.5% del porcentaje global de usuarios de Internet, el cual es un número enorme si tenemos en cuenta que la población digital global se estima en 3,578 mil millones <sup>114</sup>.

Con todo y las políticas restrictivas, *Baidu* es el mejor buscador para encontrar información sobre la República Popular China, igualmente se ha convertido en los últimos cinco años en una máquina de gigantesco poder monopólico que, fusionando proyectos con socios y competidores locales como *Alibaba Group* y *Tencent Holdings* se ha abierto camino en el comercio electrónico principalmente local y regional e incluso en aspiraciones relacionadas con el *Big Data*<sup>115,116</sup> para generar un contrapeso firme en el ciberespacio. Del mismo modo la absorción de sitios *web* como *Youku Tudou* y *Renren* por parte Baidu por parte de *Tencent* fortalecen el desempeño del buscador chino como empresa innovadora y desarrolladora de los mejores servicios para seducir a la audiencia regional y también mundial.

Según las opiniones vertidas por usuarios de *Baidu* (incluyendo experiencia propia) en el sitio *web Quora* dedicado a la resolución de preguntas que intentan explicar los eventos del mundo actual a través de las opiniones de la población activa en la Internet, se resaltan los puntos en los cuales la compañía China funciona mejor que sus contendientes.

- Es 10 veces más rápido y confiable que *Google* (Google funciona a menos de 1/3 de tiempo recientemente).

---

<sup>114</sup> Cifras extraídas de: Statista (2018) Número de usuarios de internet en el mundo dentre 2005 hasta 2017. Statista.com [en línea] Disponible en: [h https://es.statista.com/estadisticas/541434/numero-mundial-de-usuarios-de-internet/](https://es.statista.com/estadisticas/541434/numero-mundial-de-usuarios-de-internet/) Consultado el 7/2/18

<sup>115</sup> Es el almacenamiento masivo de información, en cantidades tan estratosféricas que ningún ordenador convencional puede albergar. Definición extraída de visita propia al Centro Cultural Digital en la Ciudad de México, : *Expo Big Data*, 17 de febrero de 2017.

<sup>116</sup> Liu Jack, (2016) "Tencent to Baidu, Chinese internet giants big on Big Data" *South China Morning Post*, Scmp.com [en línea] Disponible en: <http://www.scmp.com/tech/article/1954550/tencent-baidu-chinese-internet-giants-big-big-data> Consultado el 11/2/18

- Posee la función de descarga directa en casi cualquier contenido multimedia sin necesidad de programas o aplicaciones adicionales.
- Permite la descarga de links para la activación de licencias de *software* con riesgos muy bajos para captar virus.
- El motor de búsqueda puede ser utilizado como un diccionario que ofrece traducción en chino directamente desde cualquier palabra inglesa.
- El sistema de escritura del chino mandarín es muy práctico y fácil de usar en su aplicación para *Android*.

La experta en buscadores *web*, Wendy Boswell en *A Brief Overview of Baidu* señala las características que distinguen a *Baidu* de otros buscadores, las cuales no son especialmente por su apariencia sino por la optimización de sus servicios, al respecto sostiene que “además de ofrecer más oportunidades de búsqueda, *Baidu* también brinda una variedad de productos relacionados con la búsqueda: ya sean de imagen, libros, mapas, búsqueda móvil y muchos más. *Baidu* ha sido desde alrededor el año 2000, el sitio *web* en idioma chino más popular en todo ese país<sup>117</sup>”; potencial engrandecido por la mezcla de los modelos de búsqueda de *Google y Yahoo* motores más empleados en el mundo y en Japón (rival tradicional y aliado estadounidense), respectivamente.

En síntesis, traducimos el comportamiento del gobierno de la República Popular China dentro de su territorio y dominio ciberespacial en que, el fin implícito a través del desarrollo de *Baidu* no es precisamente establecer como imperante el modelo chino en el mundo sino apoyar la evolución de lo cosmopolita, a través de plataformas y tecnologías diseñadas en ese país. Esto es que hoy la predisposición central recae en el control de su mercado interno antes de buscar alcanzar los servidores de la audiencia internacional.

---

<sup>117</sup> Boswell W. (2016) *A Brief Overview of Baidu*. AboutTech. [en línea] Disponible en: <http://websearch.about.com/od/enginesanddirectories/p/baidu.htm> Consultado el 11/10/16



Gráfica 8. Gráfica que muestra el porcentaje del precio de cambio<sup>118</sup> de *Baidu* y *Alphabet* de 2016 a 2017 en millones de dólares.<sup>119</sup>

### 2.2.1.3. *Yandex*

*Yandex* es un proyecto que data en los comienzos de la era digital, en la década de 1990 ya se tenía en Rusia una idea similar a la de los estadounidenses acerca de las posibilidades que se abrirían en el nuevo terreno llamado ciberespacio. Pero su origen toma forma hasta 1993, puesto que *Yandex* se origina<sup>120</sup> a partir de las bases adecentadas por la pequeña compañía de desarrolladores llamada *Arcadia*.

<sup>118</sup> Aumento o disminución en el precio de cierre de un valor en comparación con el precio de cierre del periodo anterior (en este caso cada dos meses). Definición extraída de The Free Dictionary by Farlex, *op. cit.* Nota 21.

<sup>119</sup> Vena, Danny (2017) *Better Buy: Baidu vs. Google*, Nasdaq.com [en línea] Disponible en: <http://www.nasdaq.com/article/better-buy-baidu-vs-google-cm812008> Consultado el 11/2/18

<sup>120</sup> Yandex History [en línea] Disponible en: <https://yandex.ru/company/history/1997> Consultado el 3/10/16

Originalmente como una compañía limitada a la búsqueda de productos y servicios orientados al mercado en línea, *Arcadia* se presentó como la opción más adecuada para completar las líneas del consorcio ruso en telecomunicaciones, *CompTek*, al que se une en el mismo año (1993). No obstante, es hasta 1997 que *Yandex.ru* es presentado como un prometedor motor de búsqueda con un amplio contenido indexado, producto del esfuerzo en adelantos dirigidos al ciberespacio en la carrera por no quedar detrás del imperante poder informático de Estados Unidos.

No obstante, la coyuntura que significó para *Yandex* el ascenso al protagonismo en Rusia y sus zonas de influencia se ubica en el marco de la guerra civil en Ucrania (2013-2015) y la crisis política internacional alrededor del conflicto puesto que fue en este contexto que el gobierno ruso encabezado por Vladimir Putin decidió disminuir la dependencia tecnológica de Estados Unidos y Europa. Y es que, fue en ese momento de fricción política que la Federación Rusa dio un fuerte paso hacia adelante en cuanto a su emancipación tecnológica ya que se creó *ReactOS* (que desde 2015 pasó a ser el segundo sistema operativo más utilizado en Rusia, concretamente reemplazando a *Windows* de *Microsoft* de los ordenadores del gobierno de ese país<sup>121</sup>) además de que *Yandex* incrementó su protagonismo en el mercado de búsqueda en línea. De acuerdo con la investigación de Samantha Nielson<sup>122</sup> en 2014 (en el medio de la crisis de Ucrania) *Google*, que continúa dominando a nivel mundial el mercado de búsqueda, tenía alrededor de un 26% de las acciones del mercado en Rusia. *Yandex* por su parte ya poseía el 61,7% de todo el tráfico de búsqueda en ese país, además de que por medio de sus sitios atrajo a 66 millones en ese mismo año. Además, apuntala el hecho que desde entonces *Yandex* también ya operaba en las zonas de influencia de la Federación Rusa como Ucrania (con 30% de las acciones del mercado), Kazajstán, Bielorrusia y Turquía (con 4% de

---

<sup>121</sup> ReactOS (2015) *ReactOS as a second OS in Russian government*, Reactos.org [en línea] Disponible en: <https://www.reactos.org/forum/viewtopic.php?f=2&t=14298&sid=10bbe8f5d2774077a4fffb1469340824>  
Consultado el 11/2/18

<sup>122</sup> Nielson, Samantha (2014) "Yandex sees a market share increase powered by its search service" Market Realist, Marketrealist.com [en línea] Disponible en: <https://marketrealist.com/2014/03/yandex-seeing-slowdown-growth>

las acciones del mercado) regiones (a excepción de Turquía) que utilizan el alfabeto cirílico<sup>123</sup>.

| Sitio web    | Tiempo diario estimado en el sitio | Número de páginas visitadas a diario |
|--------------|------------------------------------|--------------------------------------|
| 1-Yandex.ru  | 10:21                              | 8.72                                 |
| 2-Google.ru  | 7:46                               | 5.77                                 |
| 3-Mail.ru    | 7:21                               | 8.19                                 |
| 4-Google.com | 7:04                               | 6.13                                 |
| 5-Rambler.ru | 5:18                               | 4.50                                 |

Tabla 7. Los cinco motores de búsqueda *web* más utilizados en Rusia, así como el tiempo en promedio y el número de páginas de cada sitio visitadas a diario en ese país.. Última actualización 15/2/18. <sup>124</sup>

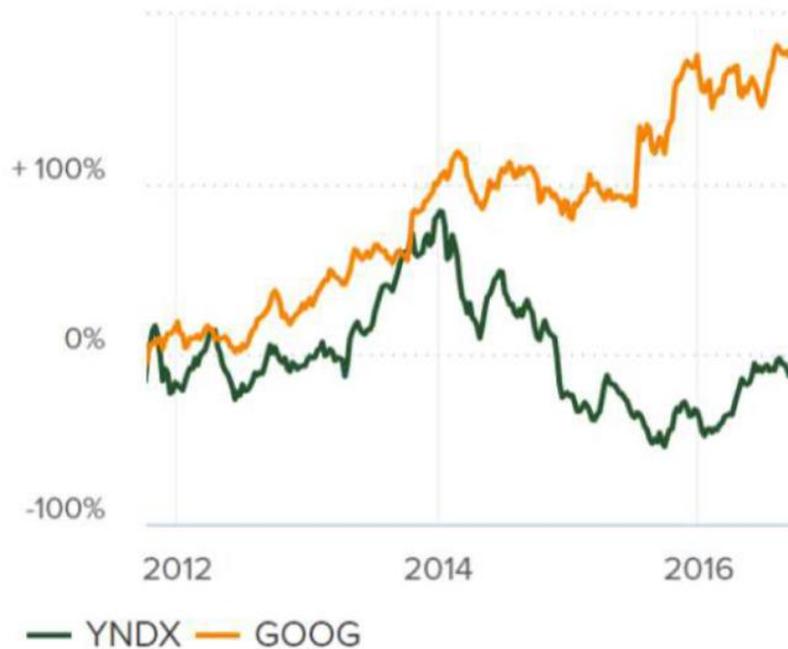
A pesar del comienzo de la relativa independencia tecnológica rusa, *Yandex* sufrió una recesión importante en ese mismo periodo, misma que se fue agudizando al tiempo en que la crisis separatista en Ucrania vivía su punto más estuoso. En otros términos, a partir de una lectura geopolítica se puede entender el comportamiento de la audiencia del mundo, pero específicamente la europea de acuerdo con el uso de los motores de búsqueda, respondiendo a su vez a un conflicto de impacto mundial.

Incidentalmente, al inicio de la crisis en el este de Ucrania *Yandex* fue afectado de manera positiva en cuanto al número de usuarios que utilizaba su motor de búsqueda o su navegador *web*, ya que mucha de la audiencia europea comenzó a emplear dichas herramientas a tal grado que a nivel mundial *Yandex* llegó a rivalizar en los punteros de las ganancias con los servicios otorgados por los gigantes estadounidenses. Sin embargo, entre 2014 y 2015 la popularidad del navegador bajó

<sup>123</sup> *Ibid.*

<sup>124</sup> Elaboración propia. Datos extraídos de: Similar Web (2018) *Top websites ranking, Search Engine Russia*, Similarweb.com [en línea] Disponible en: <https://www.similarweb.com/top-websites/russian-federation/category/internet-and-telecom/search-engine> Consultado el 15/2/18

drásticamente respecto a su previo auge. El impacto que esto tuvo con respecto a la economía de la compañía rusa se puede observar en la siguiente gráfica.



Gráfica 9. Ganancias de *Yandex* y *Google* de 2012 a 2016 en millones de dólares.<sup>125</sup>

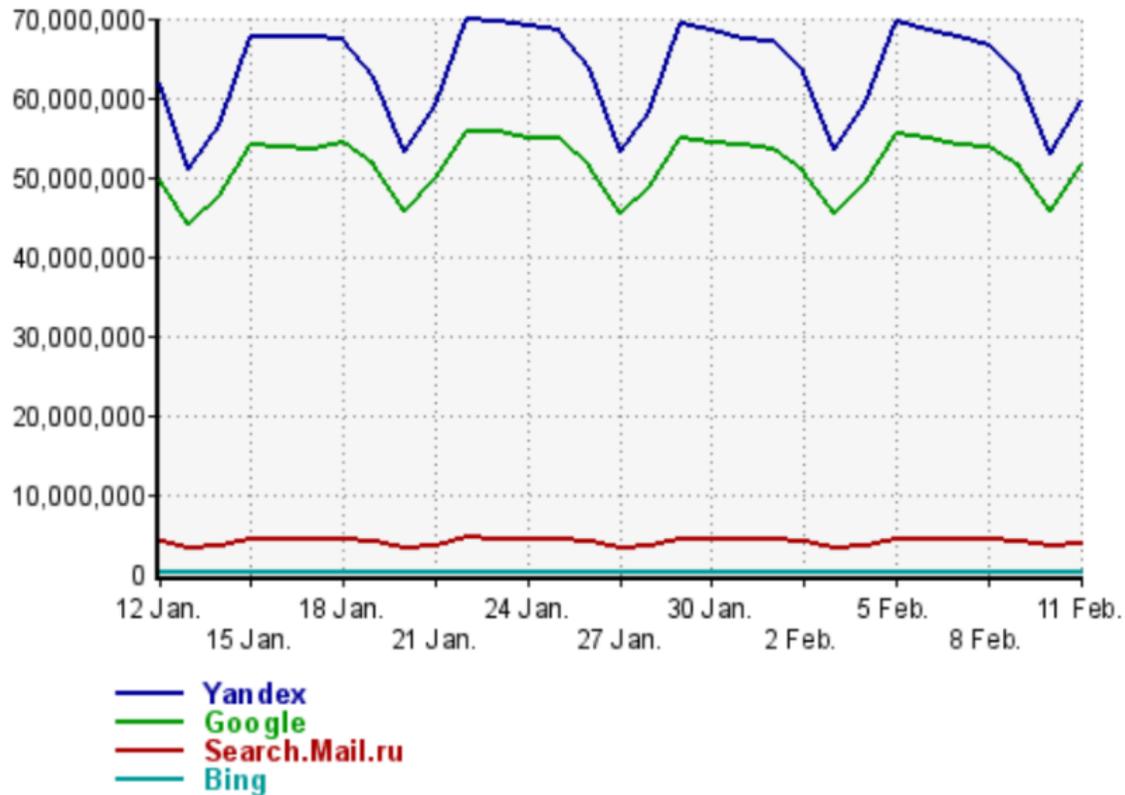
Lo cierto es que las percepciones económicas de la compañía rusa en 2016 no se ubican debajo de la media de 2012, a su vez es innegable que su crecimiento varía y se mueve con respecto a la situación e intereses económicos y políticos de la geopolítica rusa, trastocada por el contexto internacional. Por otro lado, se debe tomar en cuenta la trascendencia del conflicto (la crisis de Ucrania) que segmentó a la población de la órbita rusa, específicamente de Europa donde los niveles de la vista de sitios *web* rusos disminuyó drásticamente.

Con todo, hoy además de en la República Popular China, a lo largo de la gran región que ocupa la Federación Rusa y su órbita de influencia política extendida principalmente a través de su amplio borde fronterizo (Asia Central y Europa del Este), las grandes multinacionales estadounidenses proveedoras de servicios de

<sup>125</sup> *Ibid.*

Internet y tecnología no ocupan el primer lugar en solitario como motores de búsqueda ya que el peso de empresas locales como *Yandex* disputan permanentemente la supremacía del tráfico informático teniendo incluso más protagonismo en los ordenadores de la audiencia.

En los últimos años, *Yandex* ha crecido exponencialmente a través de la asimilación de la gama de servicios que ofrecen empresas como *Google* y el mismo *Baidu* a los consumidores; entre las innovaciones más importantes están el lanzamiento de un conjunto de aplicaciones disponibles para *Android* en celulares y *Linux* y *ReactOS* en ordenadores de escritorio destinadas a reemplazar a las aplicaciones de la familia *Google* en los dispositivos móviles. Dichas innovaciones añaden además del motor de búsqueda la introducción de mapas, una tienda virtual, correo electrónico y una nube, como los servicios incorporados más elementales. El esfuerzo de la empresa rusa se traduce en efecto no en la imitación de los servicios de la empresa estadounidense sino en la optimización de estos con toques y características propias y reformadoras que mejoran su funcionalidad.



Gráfica 10. Cantidad en millones de búsquedas en los motores más utilizados en Rusia (tanto desde dispositivos móviles como desde ordenadores fijos) en los primeros dos meses de 2018.<sup>126</sup>

### 2.2.2. Redes sociales

El exponencial crecimiento de la Internet en los últimos años, y por consiguiente de la audiencia activa en la red no se puede explicar sin las redes sociales, las cuales han funcionado como un motor para la expansión de la sociedad de la información en todas las latitudes geográficas del hemisferio. De hecho, las redes sociales los las que han levantado uno de los más altos revuelos en la población mundial, que antes de que estas existieran o bien consiguieran un impacto importante, irónicamente no le habrían visto alguna utilidad funcional a la Internet.

A todo esto, en 2017 el sitio *Global Web Index* inició un estudio a partir del rastreo de usuarios en todo el mundo para conocer la cantidad de tiempo promedio

<sup>126</sup> Live Internet Russia (2018), *Search Engines searches quantity on Russia*, Liveinternet.ru [en línea] Disponible en: [https://www.liveinternet.ru/stat/ru/searches.html?id=13&id=4&id=5&id=8&per\\_page=10&report=searchnmhes.html%3Fslice%3Dru&show=rebuild+graph&slice=ru](https://www.liveinternet.ru/stat/ru/searches.html?id=13&id=4&id=5&id=8&per_page=10&report=searchnmhes.html%3Fslice%3Dru&show=rebuild+graph&slice=ru) Consultado el 11/2/18

invertida en redes sociales por la audiencia desde 2012 hasta 2016. Los resultados fueron concluyentes, y apuntaron a un aumento gradual del uso de las redes sociales en la audiencia mundial, dado que, si la media del tiempo en la *web* en 2012 era de 1 hora gradualmente aumentó hasta llegar a más de 2 horas en 2016<sup>127</sup>.

Las redes sociales también son la razón por que muchas personas se hayan vuelto parte de la población activa en la Internet, dicho de otro modo, usuarios ávidos, y atentos a la red. Análogamente, debido a su rápido crecimiento y popularidad, además de la dinámica actividad de intercomunicación y retroalimentación que a su vez genera nuevos desafíos naturalmente se crean recomendaciones traducidas a futuro en perfeccionamientos. Se trata de la causa primaria para el ensanchamiento del contenido disponible en el ciberespacio.

Pero, las redes sociales no solamente son una vía de comunicación innovadora que permite a la audiencia mundial estar interconectada mediante la optimización que representa el ciberespacio para las telecomunicaciones. Evidentemente lo anterior no es sino una parte de sus grandes funcionalidades, sin embargo, su utilidad primaria está en ser la herramienta de manipulación social y política actual por excelencia.

La incidencia que la cultura exhibida mediante las redes sociales puede tener en una sociedad, es precisamente lo que corrobora su *statu* como un mecanismo de manipulación social, y es que a través de la reproducción en los medios sociales (*Social Media*) se contagia a la audiencia, con ideologías, costumbres, moda y música todas expresadas de una manera fundamentalmente sensacionalista, consiguiendo de esta forma que en especial los más vulnerables (y la mayoría de los usuarios en la Internet), la juventud, se acoplen a una determinada cultura impuesta.

Conjuntamente es relevante considerar que las redes sociales pertenecen junto con los blogs y otro tipo de plataformas a la categoría de los medios sociales, los cuales se caracterizan por poseer una accesibilidad gratuita y disponible para la audiencia global, de ahí también el factor que les vuelve tan seductores para las

---

<sup>127</sup> Mander J. (2017) *Daily time spent on social networks rises to over 2 hours*, Globalwebindex.net[en línea] Disponible en: <https://blog.globalwebindex.net/chart-of-the-day/daily-time-spent-on-social-networks/> Consultado el 11/2/18

personas, además de que límpidamente ése hecho les hace sentir con mayor libertad. Por otro lado, están los medios de masas, como son los periódicos y revistas en línea, programas de televisión disponibles en la Internet, entre otros, cuya diferencia estriba en que generalmente para acceder a este contenido es necesario pagar ya que son parte del gobierno o bien de empresas particulares con fines lucrativos.

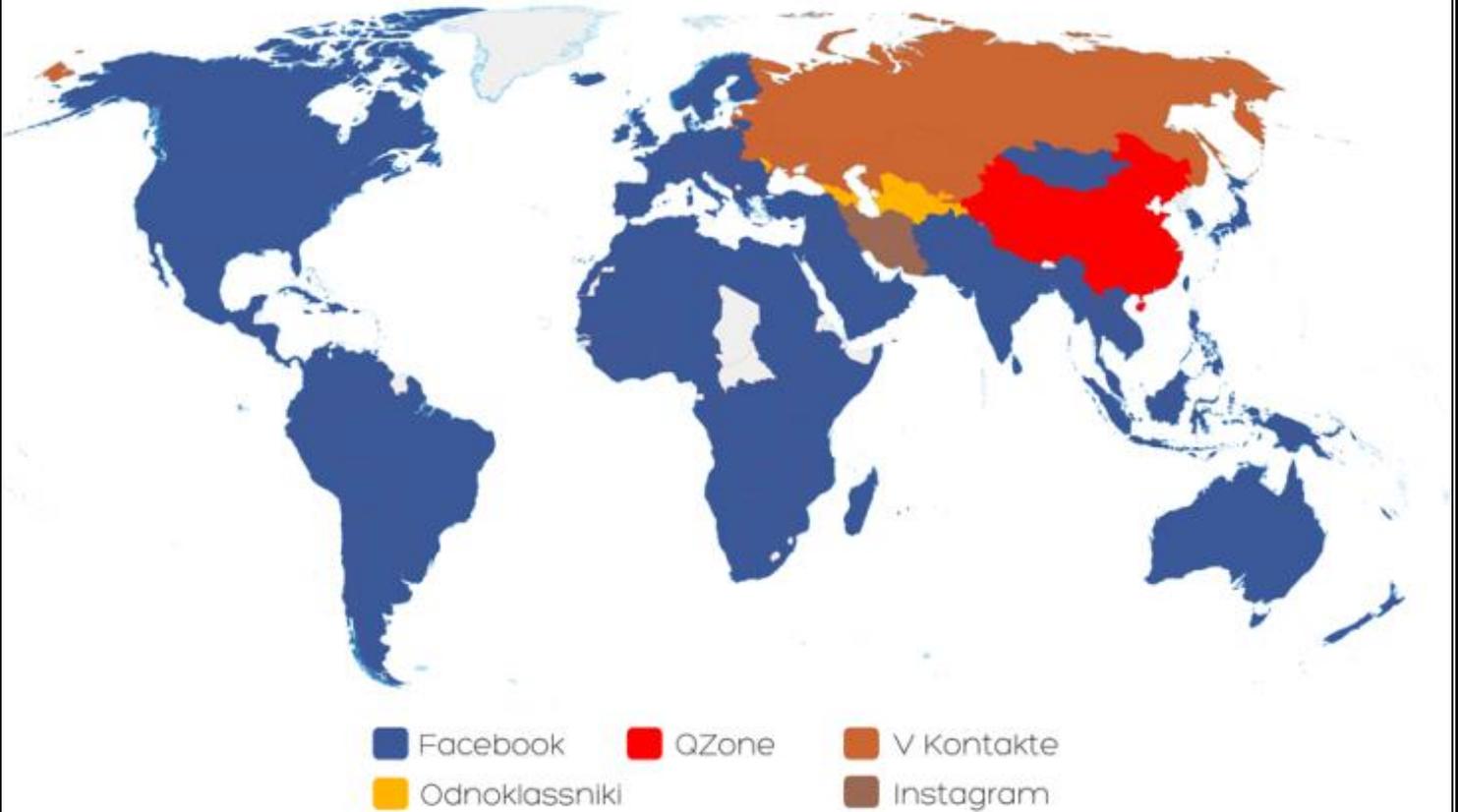
Con esto no se quiere decir que los medios sociales correspondan a empresas sin afán de lucro, ya que en este caso el usuario no paga por el producto simplemente porque él mismo es el producto y es por consiguiente el incentivo económico principal. Al igual que los buscadores *web* las ganancias de las redes sociales dependen de la publicidad, de tal suerte que el negocio radica en poseer los ojos de una audiencia entera para ver los anuncios de otras grandes empresas a través de sus plataformas, en un estricto sentido *Facebook*, *Twitter* o incluso *Linkedin* fueron fundadas por y para la industria de la publicidad.

Ahora bien, para entender la función de las redes sociales como mecanismo de control social con fines políticos es necesario mencionar que, mediante el rastreo de datos y direcciones geográficas, conocimiento y clasificación del tipo de contenido publicado, las páginas seguidas, sin dejar de lado el tiempo pasado ahí, se elabora un perfil de cada usuario, país y región. Las redes sociales también sirven para monitorear al comportamiento de la sociedad sin que ésta lo vea necesariamente como un acto impositivo o como algo que trasgrede su privacidad.

El monitoreo de la actividad informática de la población es fundamental para la retención del poder por parte de una potencia, y es que como se ha mencionado, la humanidad se encuentra en un marco de desinformación, producto de la pugna por el control del tráfico informático, lo que lleva a algunas potencias globales a fortalecer sus medidas en cuanto a censura, ciberataques, espionaje intensivo, etcétera.

Reiterando la idea central de esta investigación que refiere en efecto a una dinámica global multipolar, regida por un grupo de potencias mundiales a las cuales el resto de los actores se encuentra subordinado. Consecuentemente acreditando dicha afirmación en la que el ciberespacio refleja el esquema político en el hemisferio, situamos en seguida a las redes sociales con mayor presencia en la red

informática mundial, resaltando su manera de incidir social y políticamente afín al Estado al que pertenece.



Mapa 4. Redes sociales más usadas en el mundo hasta enero de 2018.<sup>128</sup>

### 2.2.2.1. *Facebook*

Recapitulando, durante y a finales de la década de 1990 el hacendoso modelo económico neoliberal incentivó las bases de la revolución digital y de las telecomunicaciones, alcanzando estas su punto más estuoso. Con la apertura de los mercados internacionales, y el crecimiento económico basado en el sector privado las empresas dedicadas al desarrollo de *software* protagonizaron una competencia para

<sup>128</sup> Cosenza Vincenzo (2018) *La mappa dei social network del mondo gennaio 2018*, Vincos.it (Datos recopilados de Alexa y Similar Web). [en línea] Disponible en: <http://vincos.it/2018/02/05/la-mappa-dei-social-network-nel-mondo-gennaio-2018/> Consultado el 11/2/18

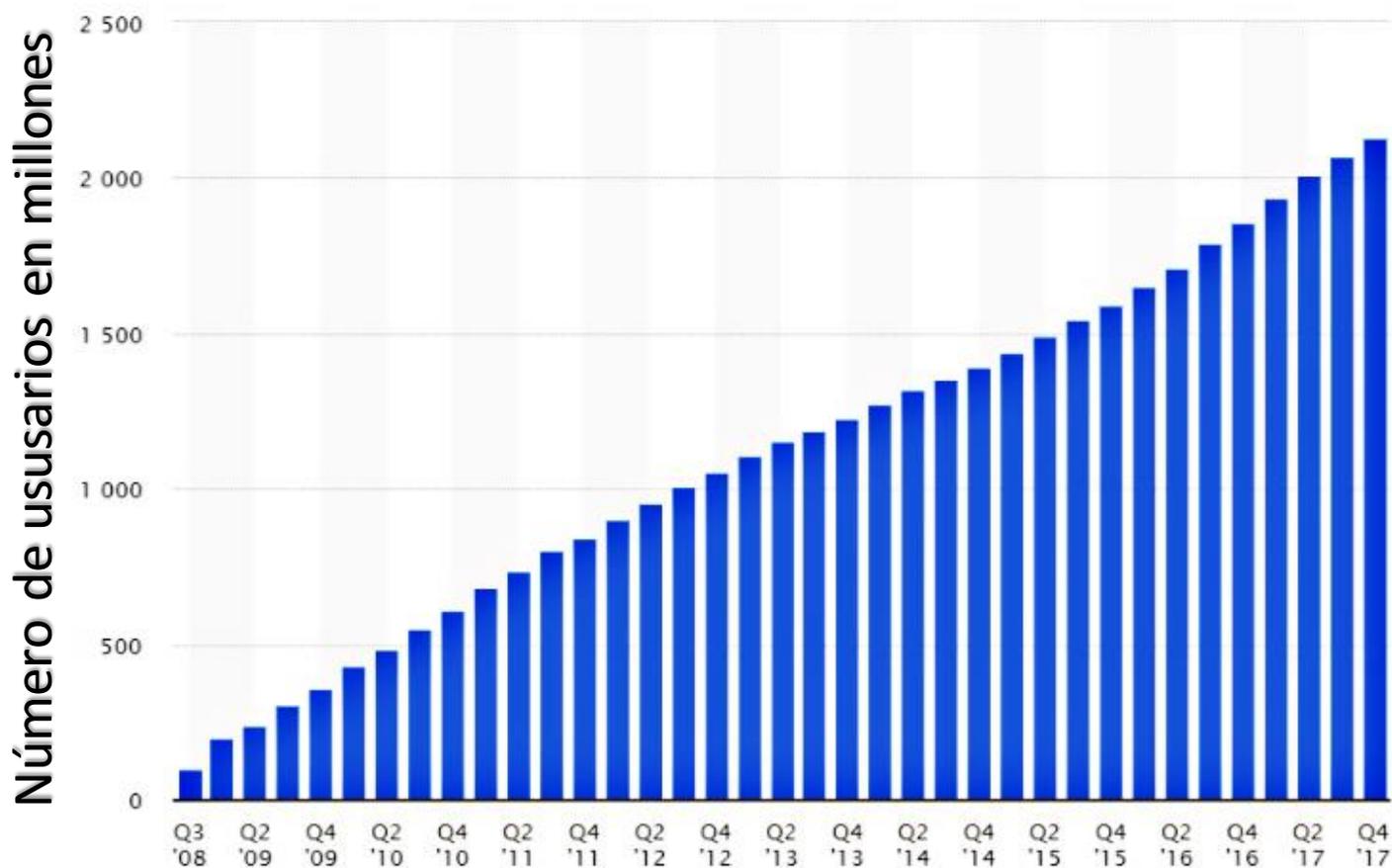
ganar más audiencia alrededor del mundo, creando plataformas y programas capaces de atraer al público. Es en este contexto que se dio el surgimiento de las redes sociales el cual responde concretamente a la propagación del ciberespacio en la creciente población global capaz de tener acceso a la red informática mundial, además de la necesidad de una nueva dinámica de comunicación más ágil que los correos electrónicos y otros de los medios disponibles de la misma índole.

En medio del florecimiento de las redes sociales, propiamente iniciado con la aparición de *Friendster* y *Linkedin* en 2002, seguida de *MySpace* y otras más en 2003, nace *Facebook* (2004) desarrollada por el programador estadounidense Mark Zuckerberg quien aprovecha las fallas, defectos y aciertos de sus antecesores para idear una plataforma que sumara los hitos de estas en una sola, por tanto, *Facebook* aglomeraría éxitos funcionales como el chat, la personalización de los perfiles, y una interfaz amigable capaz de hacer sentir al usuario en un pedestal.

Pero, el complemento que impulsó la fama de la red social de Zuckerberg y que integró a todos sus otros atractivos fue la facilidad para usarle, puesto que la accesibilidad de la plataforma, el sencillo registro, la búsqueda de amigos, entre otras. La hicieron volar sobre su competencia informática, tanto así que para 2009 Facebook ascendió sorprendentemente dejando a muchos de sus rivales atrás. Actualmente, de acuerdo con *Internet World Stats* la cantidad de usuarios registrados suma casi 2 mil millones<sup>129</sup>.

---

<sup>129</sup> Internet World Stats (2017) *Facebook Users In The World*. *Internetworldstats.com* [en línea] Disponible en: <http://www.internetworldstats.com/facebook.htm> Consultado el 11/2/18



Gráfica 11. Número de usuarios activos en *Facebook* en todo el mundo, dividida en cuartos de año desde 2008 a 2017.<sup>130</sup>

A lo largo de su existencia *Facebook* se ha vuelto más popular y más poderoso, ha optimizado su funcionalidad con nuevas y diversas actualizaciones que le tornan en un medio de comunicación casi imprescindible. Dada su condición como medio social está disponible a cualquier usuario en el mundo, además de poseer una política relativamente libre de publicaciones, a propósito, es justamente esa característica la que le da la facultad para integrarse con mayor solvencia a los hábitos de los individuos y de propia dinámica social. *Facebook* no solamente es una red social a secas, sus diversas herramientas le permiten ser una plataforma para movimientos sociales y políticos, un espacio en donde los usuarios pueden verter sus

<sup>130</sup> Statista(2018) *Number of monthly active Facebook users worldwide as of 4th quarter 2017 (in millions)*, Statista.com [en línea] Disponible en: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> Consultado el 11/2/18



ideas, gustos y preferencias, un sitio que traspasa las barreras de la distancia para crear lazos íntimos entre usuarios a través del ciberespacio. *Facebook* se ha dedicado a emular ciertas características de la estructura social mediante las emociones, entendiendo a la audiencia como un ente que reacciona sobre todo al sensacionalismo.

Lo cierto es que *Facebook* se adapta al contexto geopolítico mundial y a la agenda del *establishment* occidental, proyectando la imagen que este busca hacia su audiencia, incidiendo con una cultura prefabricada que sacraliza el papel de unos actores en el escenario internacional y literalmente sataniza a los rivales de estos en la pugna por la hegemonía mundial. Ahora bien, es menester resaltar que el margen de libertad en *Facebook* obedece a estándares fijados por un poder dominante primordialmente económico, no queremos decir que aquello que esté en contra del *establishment* vaya a ser necesariamente censurado de la plataforma, sino que en su lugar se mantiene bajo monitoreo constante, así como todos los usuarios registrados.

Debido a la gran cantidad de personas que le utilizan, aunado a la confianza y tiempo que estas depositan en la red social, *Facebook* se vuelve un medio en el que sin ninguna precaución miles de millones de personas vierten gran parte de los sucesos que acontecen en sus vidas, al grado que le podríamos considerar como un auténtico confesionario y esto desde luego incluye su tendencia política, donde estuvieron, a qué se dedican, sus lazos de amistad y contactos etcétera. En este sentido, al usuario no se le obliga solo se le invita a aportar su autobiografía y toda la información referente a sus relaciones interpersonales por supuestas cuestiones de seguridad, la realidad es que resulta una herramienta eficiente para moldear los perfiles de la población en todas sus aristas, es decir en todos y cada uno de los aspectos de la vida utilizando a los mismos usuarios como los trabajadores que se encargan de dar su información.

Idealmente el espionaje y la violación de la privacidad de los usuarios va directamente en contra de los estándares de seguridad de *Facebook*, empero la realidad obedece a otros hechos, y es que el medio más conocido con el que la empresa transgrede la privacidad de la audiencia no es únicamente mediante la irrupción en

perfiles a través de la matriz informática sino con un medio mucho más sutil, el empleo de juegos y aplicaciones como *CandyCrush* para recopilar sus datos y espiar a los usuarios. De conformidad con los datos develados en 2014 por Edward Snowden la *National Security Agency* coopera abiertamente con *Facebook* para acopiar los datos personales de los usuarios <sup>131</sup>, como los números telefónicos, correos electrónicos, contraseñas etcétera. mediante dichos programas, cabe señalar que funcionan con algoritmos creados para clasificar el comportamiento del individuo, deduciendo características propias del mismo, y posteriormente transferirlas a la base de datos de la agencia estadounidense.

Pero, la manipulación que se ejerce a través de Facebook va inclusive más allá y es que en vista del uso prioritario del chat ante el resto de la red social, su adquisición, *WhatsApp* comenzó a tener un crecimiento en usuarios muy por encima de su ahora matriz<sup>132</sup>, de manera que un buen número de usuarios comenzó a pasar más tiempo en conversaciones en esta aplicación que en el mismo *Facebook*, por esta razón no tardó en ser adquirida. No obstante, la búsqueda por más y más audiencia no es la causa solitaria para explicar dicha compra, puesto que meses después de haber agenciado el servicio de mensajería, este comenzó a entregarle a la plataforma social el número telefónico de cada usuario<sup>133</sup>.

#### 2.2.2.2. QZone

Fundada en 2005 por *Tencent*, la gigante china con múltiples filiales que prestan servicios de internet orientados al entretenimiento, la publicidad en línea, las redes sociales y la telefonía móvil. Se trata de un servicio de mensajería ligado a la matriz

<sup>131</sup> Roberston J. (2014) Leaked docs: NSA uses 'Candy Crush,' 'Angry Birds' to spy. SFGATE. [en línea] Disponible en: <http://www.sfgate.com/technology/article/Leaked-docs-NSA-uses-Candy-Crush-Angry-5186801.php#photo-5795281> Consultado el 4/11/16

<sup>132</sup> Neal R. W. (2014) "Is WhatsApp Worth \$19 Billion? 6 Reasons Why Facebook Purchased The Mobile Messaging App" *International Business Times*. [en línea] Disponible en: <http://www.ibtimes.com/whatsapp-worth-19-billion-6-reasons-why-facebook-purchased-mobile-messagingapp1557026> Consultado el 6/11/16

<sup>133</sup> Gaia Scorza Barcellona (2016) *Privacy, WhatsApp 'rivelera' il tuo numero a Facebook*. La repubblica [en línea] Disponible en: [http://www.repubblica.it/tecnologia/socialnetwork/2016/08/25/news/whatsapp\\_riveler\\_a\\_facebook-146611480](http://www.repubblica.it/tecnologia/socialnetwork/2016/08/25/news/whatsapp_riveler_a_facebook-146611480) Consultado el 6/11/16



del portal qq.com el cual provee a los usuarios registrados de todo tipo de formas de interacción social como juegos en línea, *blogs*, música, fotos y videos. Es el portal más grande y utilizado en la República Popular China después de *Baidu*, y de acuerdo con el top 500 de los sitios *web* con mayor visitas en la Internet, publicado por Alexa.com (compañía de *Amazon*), *QZone* se ubica en la posición 9 después de *Google* India, y sobre el mercado electrónico *Taobao* filial del competidor local *Alibaba*<sup>134</sup>.

Ante el panorama ciberespacial hacia el primer lustro del nuevo milenio en el que ya diversas redes sociales habían sido implantadas y donde el dominio informático era monopolio indiscutible de Estados Unidos, la aparición de *QZone* representa el refuerzo de la iniciativa comenzada por *Baidu* (fundada casi un año antes) para contrarrestar la influencia de los sitios *web* estadounidenses en el tráfico informático de la República Popular China. Dichas medidas obedecen a la necesidad por controlar a la población más grande y más activa en la red ya que, ciertamente en las redes sociales se plasman voluntariamente datos privados e información a los que ni siquiera las instituciones gubernamentales tendrían acceso.

Inconcusamente, el espionaje de la audiencia se encuentra implícito en los medios sociales, y *Tencent QZone* no es la excepción, a pesar de esto el crecimiento de usuarios registrados al interior del país fue capaz de darle un giro a la realidad ciberespacial china en solo cinco años. A propósito, paralelamente a las políticas restrictivas implantadas por el gobierno chino frente a los sitios *web* entonces predominantes en el ciberespacio regional como *Google*, *Yahoo* y la creciente propagación de *Facebook* fue que el uso de *Baidu* y *Qzone* se dispararon, sin dejar de lado a *Weibo Sina*, *WeChat* (también de *Tencent*) y al mercado electrónico *Taobao*.

Además de jugar con la legislación local a favor las empresas chinas cuentan con una divergencia muy ventajosa frente a su competencia extranjera, pues si bien la República Popular China ha accedido ante la mayoría de las convenciones internacionales referentes a la propiedad intelectual en el interior del país, la

---

<sup>134</sup> Alexa (2018) *The top 500 sites on the web*, Alexa.com [en línea] Disponible en: <https://www.alexa.com/topsites> Consultado el 11/2/18



violación de estos derechos no se considera estrictamente como un quebrantamiento de la ley y por lo tanto dichas prácticas no son sancionadas por los gobiernos locales, de hecho sitios tan populares como *Youku Tudou* ofrecen abiertamente los servicios de visualización de vídeos sin el permiso de sus autores para difundirlos. Por otra parte, las empresas occidentales se rigen por políticas que protegen seriamente a la propiedad intelectual y que diferencia de las normas de privacidad si concuerdan con sus acciones de censura, de esta forma la imposibilidad de reproducir el pirateo de contenidos directamente es una desventaja que ha marcado el descenso progresivo del uso de sus plataformas no solamente en ese país sino incluso en Estados Unidos, donde según datos de Alexa ha crecido el número de visitas a qq.com con una cifra ya significativa de 1.4%<sup>135</sup>.

Otras de las características y ventajas de las empresas proveedoras de servicios de Internet en la República Popular China en relación con aquellas de los países de occidente es que como señala la corresponsal de *Marketplace Tech* en Shanghai, China, Jennifer Pak, a diferencia de Estados Unidos, el rastreo y monitoreo de la población se efectúa de manera directa y legítima puesto que incluso la población acepta y asume que el gobierno vigila y posee todos los datos de cada persona al interior de ese país, por ende la privacidad no es una cuestión de que preocuparse<sup>136</sup>. En este tenor, las regulaciones laxas en cuanto a privacidad y transacciones en Internet para con las empresas locales han contribuido a desarrollar un ambiente de solvencia, muy fácil y cómodo tanto para los usuarios como para las empresas, ya que la vida de la población se desarrolla prácticamente a través de aplicaciones y servicios como *QZone* y *WeChat*, los cuales operan con libertad y eficacia, sin restricciones legales que entorpezcan su operatividad, al contrario de sus símiles en países como Estados Unidos muy bien regulados.

Con todo, el exitoso modelo de medios sociales que ha cautivado al mundo, desarrollado en Estados Unidos fue y continúa siendo el sujeto de inspiración chino

---

<sup>135</sup> *Ibid.*

<sup>136</sup> Marketplace Tech with Molly Wood (2017), "10/27/2017: Could Facebook Messenger be all things to all people?" *Marketplace tech*, [en línea] Disponible en: <https://www.marketplace.org/shows/marketplace-tech/102717-could-facebook-messenger-be-all-things-all-people> Consultado el 11/2/18

para crear el propio, conque se busca emular las funciones de las diferentes redes sociales occidentales aglomeradas en modelos y plataformas como *QZone* y *WeChat*, un todo en uno, es decir, un medio que contenga tanto mensajería, como videos y búsquedas propias de un buscador *web* en una red social. Efectivamente, por medio de esta plataforma se ha tratado de imitar el éxito de *Facebook*, pero no unilateralmente sino en complejo, ya que, haciendo una relación directa entre los medios sociales creados en ambas potencias, Youku *Tudou* equivaldría a *Youtube* y *Weibo Sina* a Twitter, entre muchos otros. Si además evocamos la referencia de las características similares que *Baidu* agregó a partir de la experiencia de *Google*, concluimos que no es precisamente una duplicación de los servicios occidentales y más bien el empleo del modelo de estos para crear un andamiaje propio ajustado a las tendencias de la sociedad china, antes de proyectar con fuerza su influencia fuera del territorio.

### 2.2.2.3. *VKontakte*

Habiendo ya comprendido la importancia de la red informática mundial en general y el papel de las redes sociales dentro de ella como la herramienta actualmente más empleada de manipulación y control social y político naturalmente deducimos los componentes que dan pie a la trascendencia que han alcanzado los medios sociales en la pugna de poder global. De manera similar al proyecto ciberespacial chino, *VKontakte* forma parte de un aparato que expresa el interés del *establishment* ruso para controlar el tráfico informático en su territorio y áreas de influencia, entendiéndole como el motor de los avances tecnológicos quizá más importante de hoy y del porvenir.

Fundada en 2006 *VKontakte* es la llave de la segunda ola de la florescencia de los medios sociales más importantes del mundo, pues su surgimiento viene acompañado de nuevas alternativas rusas como *Odnoklassniki* (2006), *Moi Mir*(2007) y la propia optimización de los servicios de *Yandex*. Y es que los esfuerzos de potencias tanto grandes como medias en el tablero geopolítico están inscritas en el ciberespacio, de esta forma, el ensanche de los medios sociales realmente

alternativos a la matriz - es decir no sub-plataformas dependientes y vinculadas a otra como *Instagram* a *Facebook*- surgen en potencias que buscan competir o al menos proyectar una imagen autónoma parcialmente alejada de la dependencia de quien cuenta con más del 60% de la audiencia mundial en la Internet.

A pesar de que *Vkontakte* tiene ciertas características que le hacen vulnerable frente a los intentos de conquista de *RuNet*<sup>137</sup> desde el exterior, como la susceptibilidad de las cuentas para ser *hackeadas*, la escasez inicial de un botón de “me gusta” o la reducida gama para hacer “amigos” en comparación con la gran red mundial de *Facebook*, posee otras particularidades para atraer a nuevos miembros diariamente que además gasten mucho, demasiado tiempo en línea. Verbigracia, los miembros de la red social tienen a su alcance bibliotecas enteras de películas sin licencia nacionales e internacionales dobladas al ruso, igualmente mediante la aplicación *VK Tracker* son capaces de subir o descargar vídeos y audios de y para toda la comunidad de la plataforma, sin dejar de lado que pueden acceder a cualquiera de estos contenidos mientras intercambian mensajes o visualizan otras páginas o publicaciones.

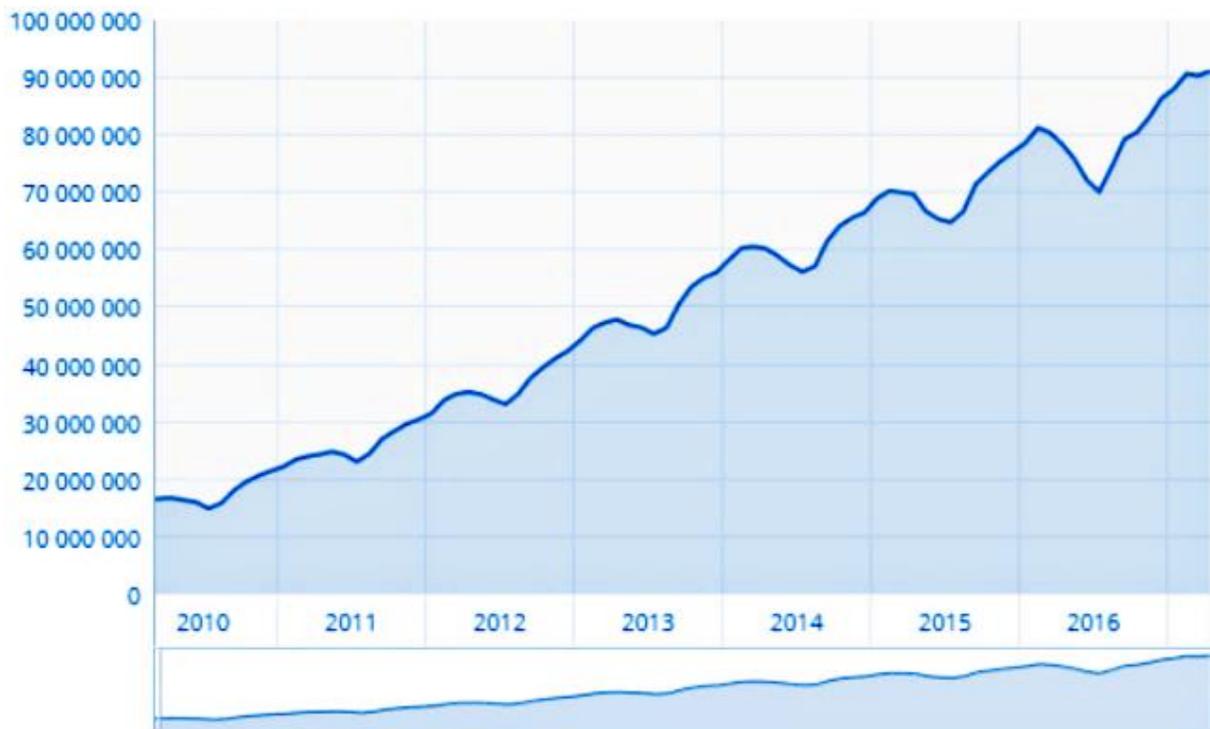
Tales son las ventajas de *VK* que le ponen en un peldaño sobre su rival estadounidense, y son verdaderamente la reproducción sin licencia de películas, canales, música entre otros elementos, los factores clave que le han restado poder en otros espacios del ciberespacio en el mundo, como el chino, el iraní o el propio ruso. Según los datos más recientes disponibles en la página oficial de la red social (2017) el número de miembros activos mensualmente de *Vkontakte* tanto en Rusia como en los países de su zona de influencia (la mayoría incluso en la Comunidad de Estados Independientes —Bielorrusia, Moldavia, Kazajstán, Uzbekistán, Kirguistán, Tayikistán, Armenia y Azerbaiyán—) ha crecido de manera estrepitosa y hasta ese año ascendió a más de 97 millones<sup>138</sup>, como se puede observar en la siguiente gráfica.

---

<sup>137</sup> Del ruso Рунет, término utilizado en la Federación Rusa para referirse al contenido en línea en idioma y dominio de Internet exclusivamente ruso. Definición extraída de: Schmidt H., Teubener K. Konradova N. (2006) *Control+Shift Public and private Usages of the Russian Internet*, Books on Demand GmbH, Norderstedt (Alemania) p. 12. Consultado el 14/2/18

<sup>138</sup> *VK* (2018), *O saïte Aудитория ВКонтакте* (Acerca del sitio, Audiencia de *Vkontakte*), *Vk.com* [en línea] Disponible en: [https://vk.com/page-47200925\\_44240810](https://vk.com/page-47200925_44240810) Consultado el 14/2/18

Número de usuarios en millones



Gráfica 12. Número en promedio anual de usuarios de *VKontakte* activos mensualmente de febrero 2010 a abril de 2017.<sup>139</sup>

VK ha sido objeto de acusaciones legales por piratería y violación de la propiedad intelectual, con todo aún no se ha probado la intencionalidad criminal de estas actividades. Sin duda alguna la debilidad de las instituciones internacionales o bien la falta de voluntad del parlamento ruso limitan directamente el margen de maniobra de redes sociales como *Facebook*, las cuales no pueden competir en los mismos rubros ilegales por los que otras plataformas si lo hacen. Igualmente, la capacidad de *Facebook* y de cualquier otro sitio o red social extranjero en Rusia y Asia Central está condicionado tremendamente ante la competencia imperante de otros sitios *web* sumamente poderosos.

*VKontakte* es la red social más importante de origen europeo y es la segunda con mayor número de usuarios en el continente, ha conseguido unificar el estilo de las redes sociales más importantes del mundo agregando el *plus* del acceso sin

<sup>139</sup> *Ibid.*

necesidad de licencia a contenidos multimedia en alta calidad como un estímulo fundamental para el crecimiento de su audiencia. Aunado a esto ha sido capaz de juntar todas estas características en una sola plataforma, a diferencia de otras competencias como la china en la que se consiguió formar un todo en uno, pero disperso en varias sub-categorías y páginas vinculadas a la matriz de la red social.

Para terminar, es fundamental recalcar que la dinámica ciberespacial y en especial de las redes sociales se sujeta al orden multipolar internacional, de esta manera es necesario concebir las actividades de estas empresas como parte de una mecánica política a través de la economía. Dicho de otro modo, grupos de poder a nivel mundial que cooperan y rivalizan entre sí por y para mantener el *statu quo*. Verbigracia, la mayor financiadora de *VKontakte* y *Odnoklassniki* es *Mail.Ru Group* internacionalmente conocida como *Digital Sky Technologies* la cual comenzó también a invertir seriamente en *Facebook*, lo que sugiere no ciertamente una rivalidad a muerte entre empresas supuestamente antagónicas, sino más bien una coexistencia en la que los usuarios de ambas redes (rusa o estadounidense) serán aprovechados y aprovecharán los resultados de la competencia.

### 3. CASOS DE EMPLEO DE LA INTERNET COMO HERRAMIENTA DE PODER EN EL SIGLO XXI

Atendiendo a la metodología deductiva explicada al inicio de esta investigación y a través del primer capítulo, en el cual se partió de la premisa general y el entendimiento del papel de los grupos de poder que rigen al mundo (entendido como una totalidad) y su incidencia directa en el tráfico informático, posteriormente en el capítulo segundo señalando la incidencia de la Internet ya no desde la totalidad del sistema sino específicamente centrada en la pugna de dichos grupos de poder al interior del mismo a su vez regido por un orden multipolar y dividido por brechas económicas que por su parte fraccionan dicho sistema en bloques comerciales y políticos, en este capítulo se emplazan algunos de los casos que dan cuenta del uso de la Internet como herramienta utilizada por los grupos de poder a escala mundial para controlar y monitorear a la población del mundo, tomando como referencia las zonas centrales, semi-periféricas y periféricas para categorizarlos:

- Países centrales

Como se ha explicado brevemente al inicio de la presente investigación, los países del centro son aquellos que conforman las economías más avanzadas del mundo, en donde se aglomeran los principales centros económicos y políticos del orbe, Estados con niveles más altos de calidad de vida, además de contar (en la mayoría de los casos) con mayor potencial militar o tecnológico. Concretamente se trata de los países occidentales (Estados Unidos, Europa Occidental) y sus aliados, Japón, Corea del Sur, entre otros. Igualmente, los países centrales concentran la cantidad más grande de empresas multinacionales proveedoras de servicios de Internet, como se ha explicado en esta investigación, ensanchando su potencial con la dependencia tecnológica del resto del mundo hacia estos.

- Países semi-periféricos y periféricos

Los países semi-periféricos son aquellos que tienen rasgos de atraso y a la vez de modernidad (genera desequilibrio interno traducido en

desigualdad).<sup>140</sup> caracterizan por poseer algunos de los centros económicos importantes, una alta demografía, niveles extremos de desigualdad (México<sup>140</sup>) con sectores de la población en pobreza extrema propios de países periféricos y en algunos casos poderío militar y tecnológico equiparable al de los países del centro. Además, como se ha explicado ya en este trabajo algunos de estos países cuentan con la capacidad para ser contendientes de los países del centro en cuanto al control del tráfico informático para ilustrar, los países industriales asiáticos, así también como China e India, los países del Cono Sur de Iberoamérica, los de Europa del Este y parte de las ex repúblicas soviéticas<sup>141</sup>. Finalmente, la última categoría está conformada por los países especializados en la producción y exportación de materias primas o productos industriales. Se basan principalmente en la explotación de una mano de obra barata, no obstante, necesitan importar capital y tecnología (lo cual acarrea a una gran deuda o a un descontrol de la gestión sobre sus propios recursos)<sup>142</sup>. Al igual que los países semi-periféricos la dependencia sobre todo tecnológica para con las empresas multinacionales de los países del centro es la más destacada característica de estos. África, Asia meridional y parte de Centroamérica y América del Sur son ejemplos.

Igualmente, es necesario resaltar que los casos serán divididos en las dos clasificaciones anteriormente mencionadas ya que las divergencias antes durante y después de la operación contienen particularidades propias que pueden parecer detalles minúsculos, pero que indiscutiblemente hacen muy diferente la reacción de la población activa en la Internet ya sea en Francia o en Mali, por poner un ejemplo. Para este análisis no solamente se deben tomar como variables el nivel socioeconómico de la población, además, la cantidad de usuarios activos en la

---

<sup>140</sup> Clemente Annabel (2018) "Pobreza y desigualdad en México, constantes desde 1996: Oxfam" *El Financiero*, Elfinanciero.com.mx [en línea] Disponible en: <http://www.elfinanciero.com.mx/nacional/mexico-parte-del-25-de-los-paises-mas-desiguales-del-mundo-oxfam.html> Consultado el 11/2/18

<sup>141</sup> Wallerstein Immanuel (2005) *op. cit.* Nota 16.

<sup>142</sup> *Ibid.* p.26

Internet y por supuesto los antecedentes y las consecuencias directas sobre potenciales intereses políticos y económicos.

Además de las dos categorías anteriormente mencionadas es menester resaltar que el terrorismo de Estado indirecto en el ámbito local y las operaciones de “falsa bandera” y las guerras “híbridas” en el ámbito internacional, (las cuales serán explicadas más adelante) conjuntan cabalmente el tipo de operaciones expuestas en este capítulo, dado que la red informática mundial figura en estas como el artilugio principal de sugestión antes, durante y/o después de la perpetuación.

- Falsa bandera:

De acuerdo con David Topí se trata de aquellos atentados o sucesos provocados por, normalmente, operaciones clandestinas y secretas de los propios gobiernos que los sufren, y achacados a terceros para poder crear así excusas y situaciones que permitan ofrecer la solución que aquellos auto-atacados deseaban imponer.<sup>143</sup>

Naturalmente las operaciones de falsa bandera expuestas en el presente capítulo contienen la variante de la Internet empleada ya sea como medio principal o secundario para ser perpetradas. No obstante, es menester señalar que no se ejecutan de la misma forma en los países centrales, semi-periféricos y periféricos, dado que mientras en los primeros el papel de la Internet estriba más en la mediatización y difusión a consecuencia de ataques previamente perpetrados tanto a través (por ejemplo ciberataques) como sin la intervención de la red informática mundial (por ejemplo atentados terroristas), en los ataques realizados en países semi-periféricos y periféricos recae más en el efecto directo de ataques frontales en donde la Internet funge como la herramienta principal para perpetrarlos, y donde la difusión no es necesariamente considerable o incluso permanecen casi nula, al borde del hermetismo.

---

<sup>143</sup> Topí David (2010) *Operaciones de Bandera Falsa*, Davidtopi.com [en línea] Disponible en: <http://davidtopi.com/operaciones-de-bandera-falsa/> Consultado el 15/2/18

En este tenor se puede entender el papel de la red en los ataques de falsa bandera en países centrales más como un anunciador y promotor de influencias e información que, efectivamente como un protagonista durante la maniobra (como en los países periféricos). Con todo la Internet no deja de ser un actor esencial en las operaciones y los efectos alcanzados en la población activa en la *web a priori y a posteriori*.

- Guerra híbrida:

Se entiende como aquella que acopia múltiples formas bélicas para maniobrar, empleando fuerzas convencionales y no convencionales, es decir, tanto al ejército como a grupos o empresas de mercenarios, además del uso intensivo de la propaganda, como medio para influir en las decisiones y la perspectiva de la población civil que se encuentra dentro y fuera del conflicto, corolario de esto último es el fenómeno de la desinformación, ya que en la pugna por poseer una versión más “real” de los hechos, evidentemente apegada a los intereses de cada parte, las afirmaciones de ambas tienden a la invención y la falsedad. Además de las intervenciones castrenses y la desinformación, a esta forma de hacer guerra se suman los ciberataques, que a través de *softwares* injuriosos provocan agravios a las bases de datos del contrario y/o de sus aliados, dichas ciber arremetidas no se limitan a los ficheros y archivos, van incluso contra cuentas bancarias y activar o desactivar maquinaria de industrias cuyo sistema se base en el ciberespacio. A diferencia de las operaciones de falsa bandera, la injerencia de la Internet es plenamente activa, puesto que se encuentra antes, durante y después de que la pugna entre en su punto más febril e incluso como se ha explicado anteriormente, está presente en daños frontales y en el campo de acción.

Es menester puntualizar que, si bien una categoría está al interior de la otra, debido a que las operaciones de falsa bandera pueden llegar a ser un medio dentro de la guerra híbrida, es decir, parte de las maniobras de un conflicto con tales características, se debe diferenciar entre una y otra pues

presentan particularidades muy propias. Verbigracia, un ejercicio de falsa bandera se puede realizar con o sin la presencia de conflicto armado, ya que puede ser utilizada como medio de provocación de efectos en la opinión pública para actuar ya sea al interior del Estado o intervenir en territorio ajeno, en otros términos, puede ser empleado como un predecesor de guerra, un alentador para revolucionar la intensidad del conflicto o bien para finalizar con el mismo eliminando a un miembro u organización peligrosa.

Por otra parte, una guerra híbrida, aunque no supone un sinónimo de guerra convencional y más bien un símil de las características de un conflicto armado no convencional donde tropas irregulares, como fuerzas especiales o mercenarios perpetran las operaciones, existe de manera estacionaria y se presenta en la pugna de poder de forma regularmente indirecta entre dos Estados y en algunos casos entre empresas trasnacionales. Conocer el origen y el final de un conflicto, con dichos componentes naturalmente se dificulta por los intereses de cada parte traslapada en la desinformación.

Es necesario tener en consideración la lectura geopolítica como el catalizador más importante en el análisis de los casos a continuación y es que ningún caso surge de forma casual, al contrario, son el resultado de un proceso.

### 3.1. Países del centro

Naturalmente las operaciones en los países del centro están caracterizadas por manifestar la aplicación del poder blando como sus mecanismos más eficientes y habituales, pero con una ligera utilización del poder duro<sup>144</sup>, potenciada a su vez por el gran impacto mediático y las consecuencias meramente legales que actos de este

---

<sup>144</sup> Joseph Nye Jr. le define en el contexto del sistema internacional como la capacidad de hacer que los demás actúen de forma contraria a sus preferencias y estrategias iniciales lo cual implica la coerción por medio de amenazas políticas, económicas e incluso militares. Definición extraída de Nye Jr. Joseph (2011) *The future of power*, Public Affairs, p.11

tipo podrían tener. A continuación, emplazamos casos que enuncian las operaciones para la retención del poder mundial en el mundo central.

### 3.1.1. Mediatización del terrorismo

El terrorismo es un fenómeno ejemplar, y un arquetipo muy plástico que refuerza nuestra hipótesis. Concretamente el ataque a la ciudad francesa de Niza el 14 de julio de 2016 fue difundido con la típica envoltura de incertidumbre que poco a poco se va separando.

Después de que en la víspera fuera efectuado el ataque, la cuestión de la constitucionalización de *l'état d'urgence* pasó a primera plana, ya que mucho se ha especulado acerca de esta modificación constitucional y si realmente tiene como objetivo atacar al terrorismo y no como Jean Claude-Paye sostiene “pasar de un poder emergido del Pueblo y puesto bajo su control a un poder discrecional reaccionando para la cuenta y el servicio de los Estados Unidos”<sup>145</sup>. Y es que la introducción del artículo 36-1 a la constitución francesa de 1958<sup>146</sup> permitiría que en caso de un estado de asedio por insurrecciones interiores, crisis graves o guerra se facultaría la transferencia de los poderes civiles de la policía al ejército, así como el establecimiento de jurisdicciones militares.

Pero ¿cuál es el nivel de impacto directo que esto puede tener sobre la población? que, hay que recordar, desde 2015 atravesaba por una situación convulsa, las manifestaciones contra la ley del trabajo que se tornaron en “revueltas” en 2016, así como el enervante ambiente bélico en Asia Occidental (protagonizado por *Daesh*) no hacen sino sugerir que ¿se estaría una vez más frente a un caso de “falsa bandera”, donde en consecuencia de terrorismo de Estado, se justificaría la aplicación del empoderamiento militar y el abuso de poder político en detrimento de los derechos de los ciudadanos de ese país? Ya que, realmente las facultades

---

<sup>145</sup> Claude-Paye J. (2016), « Constitusionaliser l'état d'urgence » Red Voltaire. [en línea] Disponible en : <http://www.voltairenet.org/article192869.html> *l'enjeu n'est pas de lutter contre le terrorisme, mais de passer d'un pouvoir issu du Peuple et placé sous son contrôle à un pouvoir discrétionnaire agissant pour le compte et au service des États-Unis*. Consultado el 29/7/16

<sup>146</sup> Assemblée Nationale (1958) *Constitution de la République Française*, Assemblée-nationale.fr [en línea] Disponible en: [http://www.assemblee-nationale.fr/connaissance/constitution.asp#titre\\_5](http://www.assemblee-nationale.fr/connaissance/constitution.asp#titre_5) Consultado el 14/2/18

concedidas por el 36-1 constitucional estarían otorgando un poder muy similar a la aplicación de la *ley marcial*<sup>147</sup>.

Por otro lado, los grandes medios de comunicación se empeñaron en alejar las opiniones alternativas a propósito de su “verdad”, una visión de los hechos evidentemente construida por ellos, moldeada con los intereses detrás y afín a los grupos de poder dominantes, así sea (en este caso) de Francia, pero también a las de el bloque económico de la civilización Occidental, liderado por Estados Unidos. Cabe mencionar que alguna falla en la coordinación entre los engranajes del control informativo entre uno y otro se traduciría realmente en una opinión adversa, que hasta ahora a ese nivel, no existe.

No obstante, las fisuras siempre están presentes a pesar de la intención por ser selladas: Las fotos y videos tomados la noche del siniestro dejan en duda si realmente la policía disparó contra el terrorista a bordo del camión o solo fingió hacerlo, ya que en varias fotografías presentadas por diferentes medios<sup>148</sup> se observa límpidamente como la ventana del piloto no presenta orificios de bala al contrario de la otra.

---

<sup>147</sup> Sistema de estatutos o normas que se lleva a cabo luego de una declaración de tipo formal, cuando una determinada situación solicita que una supremacía militar adquiera la gerencia o dominio normal de la justicia de forma general o de un estado total. Definición extraída de Concepto Definición (2016), *Definición de Ley marcial*, ConceptoDefinicion.de, [en línea] Disponible en: <http://conceptoDefinicion.de/ley-marcial/> Consultado el 29/7/16

<sup>148</sup> Ilustraciones 1 y 2.



Ilustración 1. El camión que atropelló a la multitud visiblemente baleado por la policía.<sup>149</sup>



Ilustración 2. El camión del terrorista.<sup>150</sup>

<sup>149</sup> BBC (2016) *Ataque en Niza: al menos 84 muertos al arrollar un camión a una multitud que celebraba la fiesta nacional de Francia*. BBC Mundo.. [en línea] Disponible en: <http://www.bbc.com/mundo/noticias-internacional-36800755> Consultado el 30/7/16

<sup>150</sup> Lavilla. E. (2016) *Al menos 84 muertos en un ataque terrorista con un camión en Niza*. El Español. [en línea] Disponible en: [http://www.elespanol.com/mundo/20160714/139986990\\_0.html](http://www.elespanol.com/mundo/20160714/139986990_0.html) Consultado el 30/7/16

Pero el trasfondo de este caso y de la cadena de hechos violentos que le anteceden responden al fomento del odio persiguiendo la xenofobia, ya que en realidad esto favorece la compraventa de armas, el estado de *shock* en el mundo occidental, y la legitimación del uso de la fuerza. Estamos ante un juego de poder en el que las potencias aprovechan los conflictos armados genuinos, para demostrar su autoridad y atraer aliados a su zona de influencia, a fin de cuentas, quien está con el mejor postor tiene mayores expectativas de ser beneficiado y no afectado.

El caso de Niza es un ejemplo más de la provocación de sugerencias y el estado de pánico en la sociedad, que empuja a las masas contra la pared, decididas entonces a optar por espionaje voluntario y la posesión y control de datos para mantenerse en “seguridad”. El público actual aglutinado en redes sociales, páginas de los diarios y periódicos principales está sumamente apegado a lo comercial, confundiendo la estética de las aplicaciones y el estilo de las páginas *web* con información verídica, oficial, considerada muchas veces irrefutable.

### **3.1.2. Ciber censura de la NSA en Australia**

A lo largo de esta investigación se mencionó a la censura de la información como una herramienta sustancial para perpetrar el poder. Concisamente su forma de actuar vía Internet, suprimiendo información indeseada o que simplemente vaya en contra de los intereses de un *establishment*, entiéndase desde nivel local a global.

Es menester recalcar que las operaciones para el mantenimiento del poder a través de la Internet siguen un patrón: en los países centrales, el impacto se caracteriza por la utilización del poder blando, afectando furtivamente la vida de los usuarios, repercutiendo en sus ideas y maniobrando con la estructura social a nivel abstracto, esto es, influyendo y controlando opiniones con el uso de la tecnología, si bien es cierto que el ciberterrorismo es eliminar individuos, no se realiza de la forma masiva y abierta con la que dichas operaciones son efectuadas en los países



periféricos, donde en efecto los daños son frontales y a menudo atentan directamente contra la vida de los individuos.<sup>151</sup>

Paradójicamente, en los países más desarrollados, donde por ende la presencia de la tecnología, particularmente la Internet, se encuentra en la vida cotidiana de casi toda la población, medidas como el control del ciberespacio son comunes, debido a que un ambiente propicio en donde la sociedad se ha adaptado a la tecnología dicha implementación conllevaría a resultados más concluyentes.

De esta manera el sistema aplica esta clase de operaciones primero en los países centrales y posteriormente las reproduce en el resto del mundo. Una vez que los próximos receptores se encuentren preparados para asimilar este tipo de control social.

Con todo, a pesar de que la censura y prohibición de sitios *web* es el ejercicio de control social más empleado dentro de la órbita de los países centrales no podemos acotarla al interior de un marco solamente definido por los niveles socioeconómico del país en donde este se realicen las maniobras, sino que es menester incluir entre las variables a la población activa en la red. Si bien es cierto que las pruebas sobran, el caso de Australia que tuvo lugar en 2009 es indudablemente uno de los ejemplos más referenciales para aludir a la época de transición hacia el ciber control. En esta ocasión, una vez más valiéndose de la reiterativa justificación de la protección de los usuarios en la Internet, la Agencia de Seguridad Nacional estadounidense (NSA) emitió un comunicado para la creación de un comando militar dedicado a la ciberseguridad, detallando la necesidad de posicionar al ciberespacio como un tema crucial en la seguridad nacional estadounidense y la de sus aliados.

*El ciberespacio y sus tecnologías asociadas ofrecen oportunidades sin precedentes para los Estados Unidos y son vitales para nuestra seguridad nacional y por consiguiente para todos los aspectos de las operaciones, militares. Aunado a nuestra dependencia progresiva del ciberespacio, junto al crecimiento de la matriz de ciber amenazas y*

---

<sup>151</sup> Se debe tener presente que únicamente aludimos a operaciones que como herramienta principal utilizan la Internet, no debe confundirse con los ataques terroristas en sí, (que en efecto dejan decenas de víctimas en el mundo central y en el periférico) sino a la planificación y la manera de difusión de su impacto por medio de la web.



*vulnerabilidades, adiciona un nuevo elemento de riesgo para nuestra seguridad nacional. Para abordar eficazmente este riesgo y para asegurar la libertad de acción en el ciberespacio el Departamento de Defensa requiere un comando que posea la capacidad técnica requerida y permanezca focalizado en la integración de las operaciones en el ciberespacio. Además, este comando debe ser capaz de sincronizar los efectos bélicos a través del ambiente de seguridad global, así como proveer apoyo a las autoridades civiles y sus socios internacionales.<sup>152</sup>*

Las operaciones comenzaron en octubre del mismo año, claro está que no fueron efectuadas en Estados Unidos sino en Australia, país donde el comando continúa activo. Los resultados fueron inmediatos, y en los albores de 2010 más de 1,370 sitios *web* ya habían sido prohibidos por la NSA, de secuencia fueron agregados a la "lista negra". A dichas acciones le siguieron las sanciones legales, puesto que los usuarios que ingresaran o compartieran contenido de cualquiera de estos sitios sería multado con 11 mil dólares australianos.

Sin embargo, las consecuencias de las actividades del ciber comando estadounidense en la población no se acaban ahí, lo más controversial de este caso es que ni el gobierno australiano ni la NSA revelaron al público cuales habían sido los sitios marcados como prohibidos, mientras que si fue exteriorizada para algunas empresas privadas de seguridad. Es decir que de acceder los usuarios de la población civil en alguno de los más de 1,370 sitios *web* estarían incurriendo en una conducta criminal, todo esto sin mencionar que ya se tiene en un supuesto que todas las conexiones en ese país ya estaban siendo rastreadas antes y después de la entrada del ciber comando.

No obstante, *Wikileaks* reveló meses después la lista completa de los sitios prohibidos, que cabe mencionar no tardó en ser incluida en la misma. De acuerdo a Ezra Levant, político, escritor y locutor canadiense, dentro de la lista figuraban

---

<sup>152</sup> Department of Defense, (2009) Establishment of Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations. The Secretary of Defense 1000 Defense Pentagon, Washington DC, [en línea] Disponible en: [http://www.voltairenet.org/IMG/pdf/Establishment\\_Command\\_for\\_Military\\_Cyberspace\\_Operations-2.pdf](http://www.voltairenet.org/IMG/pdf/Establishment_Command_for_Military_Cyberspace_Operations-2.pdf) Consultado el 14/8/16

algunos sitios pornográficos, y algunos que sugerían incluso a pornografía infantil considerados efectivamente como crimen. No obstante, afirma que si bien muchos sitios prohibidos poseen contenido ofensivo este no es ilegal y en algunos casos se trata de sitios desconocidos; al mismo tiempo hace énfasis en que sitios como Van Bokhorst están incluidos sin ser contenido injurioso. Levant acompaña su investigación sentenciando lo siguiente:

*Hemos visto este tipo de censura en otros países — y no sólo de los gustos de la China comunista. Tailandia creó una lista negra similar en nombre de la protección de sus ciudadanos contra la pornografía infantil. ¡Pero — sorpresa! — a los pocos meses, en la lista negra había otros sitios web, entre ellos 1.200 prohibidos por criticar a la familia real tailandesa. Una lista secreta, en manos de un gobierno, prácticamente garantiza un tipo de abuso político.*<sup>153</sup>

Pero tomando en cuenta la pesquisa realizada por Levant, al igual que otros casos similares más y menos documentados a lo largo del mundo, sabemos que en realidad no todo el contenido prohibido por los gobiernos y las agencias de inteligencia es representativo de actividades ilegales, ya que, en realidad se trata de censura que responde a los intereses de una élite. Particularmente en el caso de Australia las decisiones tomadas por la NSA y el gobierno del Estado insular fueron tomadas completamente a la espalda de la población, dictando arbitrariamente que es lo que podía ver o no.

Nos dirigimos hacia una etapa en la que la Internet constituirá el rubro central en el monitoreo de la población, los sitios *web* y la lluvia de información a la que podemos ingresar en la actualidad en un futuro estará cabalmente restringida y los intentos por emitir opiniones disidentes, compartir contenidos o visitar sitios web marcados en una lista negra tendrán como consecuencia sanciones tan severas como la prisión. De ninguna manera estamos avalando la presencia y la visita de sitios cuyo contenido se funde en el maltrato y la violación de seres humanos, como la pornografía infantil, violencia, trata de personas, etcétera. Empero, debemos

---

<sup>153</sup> Levant E. (2009) *Censorship in the internet age*. Red Voltaire [en línea] Disponible en:<http://www.voltairenet.org/article161124.html> Consultado el 14/8/16

tener en cuenta que la admonición, y supresión de sitios *web* en realidad no se basa solo en contenido que exhiba prácticas ilegales y que además atenten contra la integridad del individuo dado que muchas de las prohibiciones se realizan sobre páginas *web* que difunden información contestataria o que se encuentra con los intereses del *establishment*.

Paralelamente comenzamos a aproximarnos a un tema básico para comprender el accionar de las medidas represoras en la Internet, y que, como se ha señalado anteriormente refleja la forma de actuar de los gobiernos en el mundo tangible, la legalidad. ¿Qué es, y cuando y no es legal? es el cuestionamiento al que concurrimos para explicar el manejo de la información, puesto que cada vez cobra más legitimidad el hecho de que lo que se antepone a los intereses de un determinado grupo en el poder se considera ilegal.

Contradictoriamente, para la toma de todas estas medidas se recurre a la seguridad nacional y la de los ciudadanos como justificación, también se argumenta que la empresa de tales restricciones se realiza con el fin de garantizar el bienestar y la libertad del usuario para navegar en la red. Lo cierto es que con casos tan paradigmáticos de censura y prohibición como lo son el de Australia, Reino Unido entre otros países, tales afirmaciones son más que cuestionables.

### **3.1.3. Ciberataques**

La aparición de los primeros ciberataques se encuentra en concordancia con el uso inicial de la Internet, exclusivo para fines militares, ya que se comienzan a practicar casi 10 años antes de que se desatara la revolución informática (en la década de 1990). En 1982 cuando el ocaso de la Guerra Fría se acercaba, la CIA encontró la manera de interrumpir la operación de un gasoducto soviético en Siberia sin el uso de dispositivos explosivos tradicionales, tales como misiles o bombas. En su lugar, causaron la explosión del gasoducto usando una porción del código del sistema informático que controlaba su funcionamiento, lo cual fue categorizado por la

agencia de inteligencia como "bomba lógica". El caos que desató la explosión fue tan monumental que el incendio resultante fue incluso visto desde el espacio.<sup>154</sup>

Este episodio no significó otra cosa que el inicio de una nueva modalidad para causar daños al adversario, y su empleo fue creciendo cuantiosamente durante toda la década de 1990 donde su nivel de impacto fue perfeccionado, posteriormente en las puertas del nuevo milenio, con el cambio del orden mundial, el florecimiento del terrorismo religioso como un nuevo enemigo para Occidente, el bloque avante durante la Guerra Fría y la plena popularización de la Internet, el desarrollo de la tecnología utilizada en los ciberataques se disparó y debido al ya uso corriente del ciberespacio llegó a las manos a grupos de todo tipo desde gobiernos, y grupos insurgentes a terroristas.

Empero, el uso de esta nueva arma se concentraría entre las potencias mundiales del siglo XXI para infringir daños indirectamente (por medio de grupos terroristas, paramilitares, empresas transnacionales o incluso gobiernos títeres) o directamente, orientando sus esfuerzos a controlar el tráfico informático y paliar el efecto de los sitios *web* de la potencia rival. Verbigracia, tres años después de la entrada de Estonia a la Organización del Tratado del Atlántico Norte el 27 de abril de 2007, el gobierno báltico fue víctima de una operación de ciberterrorismo orquestada por el *Nashi*, un grupo pro-Kremlin de la pequeña República de Transnistria, ubicada entre Moldavia y Ucrania. La organización, por cierto, una de las más grandes después de *Titan Rain*, utilizó una serie de técnicas tales como el *ping floods*<sup>155</sup> para conseguir su objetivo, penetrar y tumbar los sitios *web* gubernamentales clave volviéndolos inútiles. Su método fue tan efectivo y difícil de neutralizar que el gobierno de Estonia creyó que *Nashi* habría contado con el apoyo del gobierno ruso, como represalia al aliarse con la Alianza del Atlántico. No obstante, el hecho subyacente que desencadenó estos ataques habría sido un icono importante para el pueblo ruso, el Soldado de Bronce de Tallin, un gran referente

---

<sup>154</sup> Balkhi, S. (2013) 25 Biggest Cyber Attacks In History. List 25. [en línea] Disponible en: <http://list25.com/25-biggest-cyber-attacks-in-history/5/> Consultado el: 23/10/16.

<sup>155</sup> Esta técnica consiste en saturar una línea de comunicación con un número excesivo de paquetes Internet Control *Message Protocol*. Dicha saturación causará una degradación de los servicios prestados por otros protocolos.



regional de la era soviética cuya sepultura fue reubicada por el gobierno de Estonia.<sup>156</sup>

Tomando en consideración el panorama global actual entendiéndole como la lucha entre capitalismo a nivel mundial, es necesario denotar que dicha rivalidad ya no solamente es expresada en guerras, ni en conflictos armados no convencionales sino en el resultado del crisol de todos los campos posibles, todos reunidos mediante el ciberespacio, dicho de otro modo, se da vida a la “guerra híbrida” que refiere a un entorno bélico complejo, no sólo con fuerzas del Estado o grupos paramilitares, sino también con la intervención destacada de la propaganda y los ciberataques. En dicho esquema resalta ser la Federación Rusa el actor más vulnerable ante ciberataques y al contar con un sistema de contra propaganda en germinación que aún no compite con el aparato occidental, pese a esto Estados Unidos es el actor más atacado en el mundo dado el incontable número de empresas ciberespaciales asentadas en su territorio, con una gran importancia en los diferentes pilares que rigen su esquema mediático y operativo.

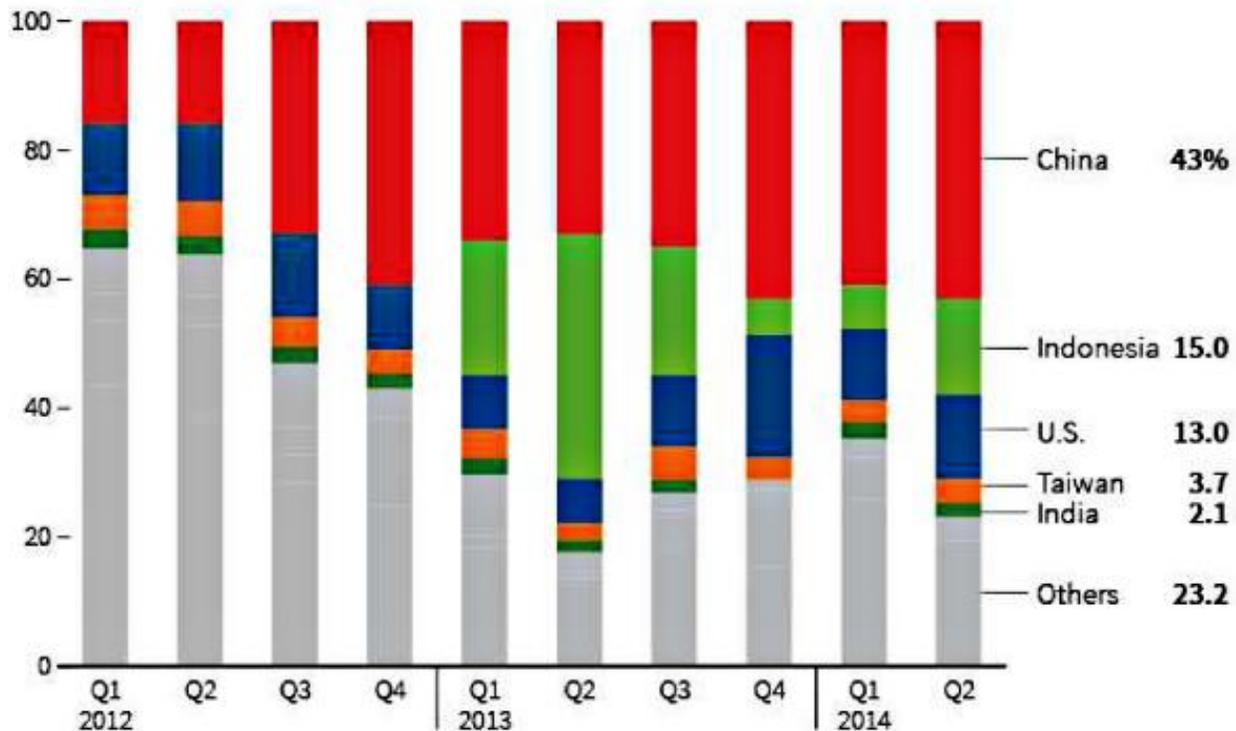
Otro caso controversial que avivó la fricción entre Estados Unidos y la Federación Rusa se desarrolló en octubre de 2016 en el marco de las elecciones presidenciales del país de Norteamérica, donde presuntamente el Kremlin estaría interviniendo en el proceso electoral en favor del candidato (ya electo presidente) Donald Trump, en respuesta a través de la Agencia Central de Inteligencia (CIA) Estados Unidos orquestó un ciberataque de magnitud sin precedentes contra el país eslavo<sup>157</sup>108, medida que ejemplifica la trascendencia del ciberespacio en el plano de la geopolítica, un medio que se aúna a las sanciones tradicionales meramente de poder blando empleadas para atacar a su contraparte. Pero ciertamente los ciberataques se encuentran la línea entre el poder blando y poder duro ya que mediante este tipo de operaciones se pueden infringir daños en páginas de privados y del gobierno como alterar programas de fábrica y desencadenar consecuencias que realmente pondrían en riesgo la vida de individuos.

---

<sup>156</sup> *Ibíd.*

<sup>157</sup> Redazione ANSA (2016) “Venti di cyber-guerra Usa-Russia. Mosca: ‘Giocano col fuoco’”. ,ANSA,ANSA.it [en línea] Disponible en: [http://www.ansa.it/sito/notizie/mondo/nordamerica/2016/10/15/usa-preparavano-cyberattacco-a-russia\\_f7bae3b0-0c20-4f5b-b0a2-a59554c3ba33.html](http://www.ansa.it/sito/notizie/mondo/nordamerica/2016/10/15/usa-preparavano-cyberattacco-a-russia_f7bae3b0-0c20-4f5b-b0a2-a59554c3ba33.html) Consultado el 25/10/16

Se evoca una vez más al ciberespacio chino para referirse a la campaña de ciberataques lanzados contra objetivos sobre todo estadounidenses, no efectuados directamente por el gobierno sino por medio de grupos especiales contratados por el mismo. Y es que entre 2012 y 2014 los ciberataques provenientes de la República Popular China sobrepasaron la media (con un crecimiento exponencial en cuanto a ciberataques originados en su país al respecto de Estados Unidos, como se puede observar en la Gráfica 11), paralelamente ese país continuó con aumento gradual en el presupuesto militar que continuó al alza hasta 2017<sup>158</sup>, así como el apoyo destinado al desarrollo de empresas locales dedicadas a la creación de *software* y plataformas reflejado en el crecimiento de empresas como *Baidu* y *Tencent*.<sup>159</sup>



Gráfica 13. Porcentaje de ciberataques de acuerdo con el país de origen en todo mundo de 2012 a 2014.<sup>160</sup>

<sup>158</sup> BBC (2017) *China to increase military spending by 7% in 2017*, Bbc.com [en línea] Disponible en: <http://www.bbc.com/news/world-asia-china-39165080>

<sup>159</sup> Ver Capítulo 2, Apartado 2.2.1.2 *Baidu*

<sup>160</sup> Chan F. (2014) *Akamai's State of the Internet reports*. Reuters en Seoul Reuters (2014) *North Korea says pro-Pyongyang supporters behind Sony cyber attack*. Daily FT [en línea] Disponible en: <http://www.ft.lk/2014/12/10/north-korea-says-pro-pyongyang-supporters-behindsonycyberattack/feed/> Consultado el 15/11/16

Los ataques forman parte de una estrategia conjunta con el enriquecimiento de las plataformas chinas dado que, navegadores y medios sociales se nutren de la reproducción de contenido sin el permiso de sus autores, lo que como se ha visto no representa un obstáculo real para que los actores dentro de la República Popular China detengan sus actividades. Debemos especificar que, a pesar de la laxa legislación china en contra de estos actos, los ciberataques no se efectúan desde trincheras exclusivamente gubernamentales o financiadas por la administración, pues las acciones individuales de los sujetos que forman parte del ciberespacio chino en conjunto infringen daños casi a la par que los grupos especializados.

De esta forma, la relevancia de los ciberataques hormiga realizados por agentes independientes, muchas veces apolíticos, actuando de forma completamente unilateral, pero desde el interior de un Estado ensombrece todavía más el panorama que se pueda tener de la relación entre dos actores internacionales especialmente poderosos, y por otra parte reafirma la trascendencia de un fenómeno muy activo en la actualidad que en estos momentos está marcando el desarrollo de la geopolítica y las grandes estrategias para la retención del poder mundial.

### 3.1.4. Supresión de la neutralidad de la red

La neutralidad de la red es el principio por el cual los Estados deben de velar por que las empresas proveedoras de los servicios de Internet no beneficien a unos sitios *web* sobre otros en cuanto a la velocidad de la conexión de la audiencia de la red para acceder a ellos o en su aparición privilegiada al principio de búsquedas en detrimento de las competidoras.

En 2015 el apoyo del ex-presidente Obama al principio de la “Neutralidad de la red” se hizo notar incluso con un informe oficial emitido desde la casa blanca<sup>161</sup>, lo que trajo como consecuencia que la Comisión Federal de Comunicaciones (FCC) de ese país aprobara nuevas regulaciones para proteger la neutralidad de la red, al

---

<sup>161</sup> Barack Obama White House, *Net neutrality President Obama's Plan for a Free and Open Internet*, [obamawhitehouse.archives.gov](https://obamawhitehouse.archives.gov) [en línea] Disponible en: <https://obamawhitehouse.archives.gov/node/323681> Consultado el 6/2/18

mismo tiempo prohibiendo los denominados "slow lanes" (carriles lentos) en la Internet así como nuevas medidas para proteger la privacidad de los suscriptores, lo que desde entonces fue visto como medidas agresivas por los republicanos.<sup>162</sup> Sin embargo, con la llegada de Trump al poder en 2017 se planteó incluso la supresión de dicho principio, lo que permitiría a gigantes proveedores de servicios de Internet como *Comcast* o *AT&T* privilegiar y agilizar el acceso a sitios *web* de unas empresas sobre otras competidoras del mismo tamaño o de menor escala, así como cobrar tarifas de suscripciones más altas a la audiencia para obtener dichos servicios.

Lo cierto es que prácticas como el *spamdexing*<sup>163</sup> que promueven en primeras posiciones a determinados sitios *web* sobre otros de forma sistematizada en uno y otro país, así como el rastreo y la violación permanente de la privacidad de los usuarios por medio de algoritmos integrados en navegadores *web*, motores de búsqueda, redes sociales<sup>164</sup> e incluso en los sistemas operativos mismos, siempre han y continúan operando indiscriminadamente desde la creación de la Internet, (necesario insistir en que su origen fue un proyecto de seguridad nacional<sup>165</sup>). En este tenor, no sólo contradicen derechos humanos como el de la privacidad<sup>166</sup> sino que directa e indirectamente van en contra de los pilares esenciales bajo los cuales supuestamente se rige la civilización occidental y los países en sus zonas de influencia, la democracia y la libertad del individuo.

Conjuntamente es necesario señalar que a pesar de que el debate de la supresión de la neutralidad de la red se lleva a cabo en Estados Unidos tendría impacto indirectamente a escala mundial puesto que las principales multinacionales estadounidenses proveedoras de servicios de Internet operan y son las más utilizadas en prácticamente tres cuartas partes de los países del mundo<sup>167</sup>. Además de significar una contradicción absoluta de los principios de la civilización occidental

---

<sup>162</sup> Finley Klint (2017) "This is the year Donald Trump kills net neutrality" *Wired*. *Wired.com* [en línea] Disponible en: <https://www.wired.com/2017/01/year-donald-trump-kills-net-neutrality/> Consultado el 6/2/18

<sup>163</sup> Apartado 1.6.3 *Spamdexing*.

<sup>164</sup> Ver Capítulo 2, Apartado Navegadores, motores de búsqueda *web* y redes sociales.

<sup>165</sup> Ver Introducción.

<sup>166</sup> Reconocido en instrumentos internacionales de derechos humanos. Ver el artículo 12 de la Declaración Universal de Derechos Humanos (1948), y el Pacto Internacional de Derechos Civiles y Políticos (1966).

<sup>167</sup> Ver mapa 3 y 4.

la supresión de la neutralidad de la red significaría también la aceptación abierta del monitoreo y control directo del tráfico informático y de los usuarios de la red informática mundial como se hace en la República Popular China<sup>168</sup> y ya no más de la manera indirecta y hermética en la que se venía realizando y que no salió a la luz hasta que agente independientes como Julian Assange y Edward Snowden hicieran publica la información.

### 3.2. Países semi-periféricos y periféricos

Dado sus bajos niveles de desarrollo económico, la desigualdad más marcada y brutal, gobiernos versátiles, población pobre, y la violencia generalizada, el mundo periférico es utilizado por las potencias mundiales para demostrar su poder duro y ganar legitimidad e influencia en el ámbito internacional. Por consiguiente, los conflictos armados en esta parte del mundo no son únicamente producto de la fricción del rose entre los intereses de potencias grandes y medias, además fungen como escenarios para la prueba y perfeccionamiento de los adelantos bélicos.

En efecto, el rol de las empresas trasnacionales es solamente la expresión del interés del gobierno al que pertenecen y su participación es medular ya que no son los ejércitos los que realizan estrictamente los ataques sino las mismas empresas privadas de seguridad. En suma, la Internet como medio para la perpetuación de los ataques no se puede considerar como uno aislado sino como parte de un andamiaje que engloba a las telecomunicaciones en general para la aplicación del poder duro.

Si bien las operaciones para retener o modificar el *statu quo* en el mundo periférico a través de la Internet se efectúan especialmente mediante el poder duro, las operaciones por medio del poder blando también están muy presentes, ambas aplicaciones expondremos a continuación.

#### 3.2.1. Global Online Freedom Act (GOFA)

Son una serie de proyectos de ley emitidos anualmente por el gobierno de los Estados Unidos a partir de 2005, en ellos se promueve el discurso occidental de la necesidad

---

<sup>168</sup> MarketplaceTech with Molly Wood (2017) *op. cit.* Nota 136.

por instaurar márgenes para propiciar la libertad y seguridad a nivel global en el ciberespacio. El *Global online freedom act* no es más que una extensión de la política exterior de ese país aplicada a la red informática mundial, teniendo como objetivos centrales controlar el tráfico informático a escala planetaria, regulando las actividades de los gobiernos extranjeros y de los negocios y empresas internacionales en la Internet, con estándares evidentemente creados en Estados Unidos y recogidos de manera arbitraria y unilateral.

Dicho proyecto se acopla periódicamente a las modificaciones en el escenario internacional, cabe destacar que, si bien Estados Unidos encabeza este tipo de actos impositivos, no se trata sino de un esquema complementado con otros gobiernos y compañías europeas y estadounidenses, por medio de las cuales el *establishment* occidental ha enviado apoyo a países autoritarios alrededor del mundo para censurar cierto contenido de la *web* además de vigilar con *software* sofisticado a los ciudadanos. Lo que GOFA significa afianza la posición de potencia preponderante de quien lo emite, puesto que incluso se declaran las medidas a tomar sobre los Estados cuyo comportamiento disienta de los estándares occidentales de seguridad o bien que no convenga a sus intereses. Concretamente dicho proyecto de ley asevera que se bloqueará la exportación de *software y hardware* a los países en la “lista negra” y que solamente mediante una licencia especial emitida por el gobierno estadounidense se podrán exportar.

Como bien se señala en la *web Electronic Frontier Foundation* (EFF) no es la primera vez que GOFA ha sido propuesto, ni la primera vez en ser aprobado por el *House sub-committee*, además de que el carácter plenamente autoritario y unilateral se reafirma, constantemente, asumiendo el rol de árbitro y juez de las relaciones entre todos los actores en el hemisferio capaces y no para navegar en la Internet. De hecho, en la versión de 2007 se nombran literalmente a los países restringidos para recibir tecnología informática (Bielorrusia, Cuba, Etiopía, Irán,

Laos, la República Democrática de Corea, la República Popular China, Túnez y Vietnam).<sup>169</sup>

Del mismo modo EFF señala los puntos medulares del GOFA del año 2012, emplazados a continuación:

1. El gobierno estadounidense requiere una evaluación de “la libertad de expresión respecto a información electrónica en cada país extranjero”.
2. El gobierno estadounidense requiere la divulgación las prácticas de derechos humanos por parte de las compañías para ser evaluadas por una tercera parte.
3. Limitación de la exportación de tecnologías al extranjero para facilitar la labor del gobierno estadounidense para vigilar y censurar a los gobiernos y países designados como “*internet-restricting*”.

En cuanto al último punto, el GOFA abiertamente señala las medidas para mantener su posición dominante evitando abastecer de su alta tecnología a los países principalmente periféricos que componen su lista restringida. Empero, una vez más Estados Unidos en su papel como potencia imperante, expresa su preminencia, implícitamente afirmándose como el más conveniente y único modelo a seguir en el planeta.

A pesar de que el GOFA atañe principalmente a la aplicación de poder blando en los países periféricos que representan una amenaza para occidente en el marco de la pugna por la retención del poder mundial a través de la Internet el *Global onlinefreedom act* representa un atentado directo contra los intereses de las potencias alternativas a occidente que buscan mantener el control del ciberespacio en su propio territorio y su órbita de influencia, como es el caso de la República Popular China o la misma Federación Rusa que a propósito de dicha imposición, declaró mediante el

---

<sup>169</sup> Cohn C., Timm T y York J. (2012) *Global Online Freedom Act 2012 Is An Important Step Forward*. *Electronic Frontier Foundation*. Eff.com [en línea] Disponible en: <https://www.eff.org/deeplinks/2012/04/global-online-freedom-act> Consultado el 28/10/16

primer ministro Aleksandr Lukashevich: “pareciese como si algunos de los miembros

del *establishment* estadounidense estuvieran retomando una mentalidad de confrontación, reviviendo los esquemas de la Guerra Fría en las tecnologías de la *web*. Estados Unidos está otra vez intentando tomar el rol de supremo regulador y de “gobernante de los destinos”<sup>170</sup> 111. Así también, Rusia llamó a una plática internacional acerca de la libertad de expresión y la seguridad informática sin que se tomen premeditadamente decisiones y acciones unilaterales, en su lugar cooperar para crear un documento avalado por las Naciones Unidas.

No obstante, debido en gran medida al caso omiso de la mayoría de la sociedad internacional, la Federación Rusa junto con sus socios del Pacto de Shanghái crearon un documento que propone un Código de conducta para la seguridad informática, sugerido como un documento oficial de las Naciones Unidas para ser evaluado en la última sesión de la Asamblea General.

### 3.2.2. Mubarak apaga la Internet

Si bien es cierto que en un estricto sentido el presente caso podría ser más entendido como una operación que no atañe directamente al uso del poder duro, también es cierto que constituye una agresión a los derechos humanos de cuarta generación y que a diferencia de su *modus operandi* en occidente (como el caso de la cibercensura en Australia) se realizó de manera plenamente frontal sin la necesidad de una agencia de inteligencia oculta detrás del gobierno, ya que fue el mismo gobierno egipcio quien anunció la aplicación de tales medidas. El hecho de que Hosni Mubarak, el entonces presidente de Egipto haya decidido apagar la Internet en su país, responde en efecto a la necesidad por tratar de mantener el control sobre su territorio y frustrar los intentos por tumbar su gobierno, y es que los movimientos contestatarios se comenzaron a gestar desde las redes sociales, y pronto ganaron legitimidad en la región y el mundo por conducto de los medios de comunicación occidentales y su amplia campaña mediática en contra de gobiernos que tiempo

---

<sup>170</sup> RT (2011) “Russia slams US Global Online Freedom Act as ‘Cold War scheme’ RT. Rt.com [en línea] Disponible en: <https://www.rt.com/news/usa-online-freedom-business-181/> Consultado el 27/10/16

atrás Estados Unidos había perpetuado en el poder, resultado claro de otra dinámica internacional, de ahí la propagación de la propaganda a lo largo y ancho del ciberespacio, la cual coadyuvó a escudriñar un movimiento libertador en busca de la emancipación de una dictadura con un líder déspota a la cabeza.

De hecho, se llegó a categorizar a este proceso como una revolución digital, lo cual fue avivado cuando tales medidas fueron establecidas, esto significó el pretexto perfecto para reforzar el impacto en la opinión pública mundial, las marchas a favor de los movimientos libertadores, el ciber activismo en las redes sociales, etcétera. Y es que para muchos como Alexia Tsotsis tratándose de un país con entonces 82 millones de personas, alrededor de 17 millones de usuarios de Internet, 60 millones de abonados de teléfonos celulares, 7 millones de teléfonos en casa, y 5 millones de usuarios de *Facebook* en línea con alrededor de 8 millones de manifestantes en las calles de todo el Egipto. "Apagar el Internet fue un movimiento poco hábil por parte de este régimen. Puesto que propició la gran atención de los medios a la revolución que no habría sido posible de otro modo."<sup>171</sup>

Lo cierto es que, a pesar de los supuestos cambios a la cabeza de la administración en el país africano, los mismos personajes miembros de la junta militar que encabezaba Mubarak, continúan en el poder. Pero el punto central es que la utilización de la potestad para privar de la Internet a la población generó un impacto generalizado tremendo para Egipto, puesto que la red informática mundial hoy día tiene un grado de incidencia tan alto que existen incluso economías que dependen de ello, por cierto según datos publicados por la entonces *Renesys*, hoy alojada en el sitio *web* de Dyn.com publicados por el periódico inglés *The Telegraph*, una vez que la Internet fuera apagada por el régimen de Mubarak, más de 3,500<sup>172</sup> sitios *web* extranjeros abandonaron Egipto, desvinculando sus acciones del país y sumiéndolo todavía más en la crisis.

<sup>171</sup> Tsotsis A. (2011) *Mubarak Shut Down The Internet, And The Internet Paid Him In Kind*. Tech Crunch. [en línea] Disponible en: <https://techcrunch.com/2011/02/11/feb11/> Consultado el 24/10/16

<sup>172</sup> Williams C. (2011) "How Egypt shut down the internet" *The telegraph*. [en línea] Disponible en: <http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shutdown-theinternet.html> Consultado el 24/10/16



Con todo y el aislamiento de comunicaciones orquestado por el gobierno egipcio no fue posible aislar completamente a la población de la Internet, ya que solamente se alcanzó a apagar hasta un 88% de los accesos en el país<sup>173</sup>122. Por otro lado, esta decisión le costó caro a Mubarak que, en su afán por tratar de controlar el tráfico informático en su territorio de manera indiscriminada, facultades que simplemente no tenía la capacidad para poder manejar.

### 3.2.3. Vehículos aéreos de combate no tripulados

Los VANT o mejor conocidos como “drones” significan hoy el adelanto tecnológico que reúne las utilidades de los avances más innovadores, la robótica, las telecomunicaciones e implícitamente el ciberespacio en un vehículo capaz de realizar recorridos programados o bien manejados desde distancias distantes por medio de los sistemas satelitales ubicados en la órbita de la Tierra.

Las funciones de los VANT se dividen básicamente en dos grupos, de uso civil y militar. El núcleo del funcionamiento de los drones se basa en la tecnología informática, de ahí el uso de los *SOC*<sup>174</sup> mejor conocidos en español como procesadores, pero con funciones y elementos adicionales en el mismo dispositivo tales como un procesador gráfico además de poseer una memoria integrada. De la misma manera los drones cuentan con una placa computadora u ordenador de placa reducida que sirve como plataforma para el circuito integrado o chip.

No obstante, en el marco de su empleo estricto como herramienta de poder duro la presente investigación se concentrará en su uso castrense y es que los VANT de combate constituyen el señero de los conflictos armados del futuro de tal suerte que el número de humanos requeridos para efectuar operaciones militares será reemplazado por la robótica, lo cual no significa que el número de pérdidas humanas en los escenarios belicosos pueda ser menor, dada la exactitud de las máquinas y el aumento de su eficacia para asestar en blancos y eliminar objetivos en relación al humano podrían redoblar fácilmente los daños causados hasta ahora en los conflictos armados de baja y mediana intensidad. En efecto, en la actualidad las

---

<sup>173</sup> *Ibid.*

<sup>174</sup> System-on-a-chip denominación anglosajona que define la tecnología capaz de integrar todos los componentes de un sistema computacional en un solo circuito integrado o chip.

armas que han causado más muertes no son precisamente las de destrucción masiva sino las armas denominadas convencionales.

En realidad, las operaciones protagonizadas por estas máquinas de guerra se llevan a cabo fundamentalmente en territorios de países periféricos, donde radica la población más marginada del mundo, con escaso o nulo acceso a la Internet, y donde consecuentemente al vacío dejado por las redes sociales y la difusión de la información por parte de la población civil a diferencia de los países del centro (donde existe difusión masiva de desastres o ataques incluso en la ausencia de muertos) su existencia no es demasiado relevante para los grandes medios de información, mientras no se les aniquile de forma masiva, en territorios donde las empresas trasnacionales dedicadas a la industria de la guerra pueden probar el potencial de sus armas apoyadas por las potencias mundiales justificadas a su vez en cualquier causa, pero siempre con un interés político y económico, sin mencionar el impacto en la sociedad internacional.

Para ilustrar Estados Unidos a través de la agencia de inteligencia más grande del mundo, la CIA, comenzó una serie de operaciones en Pakistán en 2011 con el fin de encontrar y asesinar al líder de los Muyahidines afganos, Osama bin Laden, así como exterminar a sus comandos armados.

Si bien como menciona el periódico pakistaní *The Nation* “los ataques con drones realizados por la CIA en las zonas tribales de Pakistán no sólo están contra las leyes internacionales y la carta de las Naciones Unidas, sino que también se encuentran en contra de la Constitución de Pakistán, que en su Artículo 9 de la dispone que, "nadie podrá ser privado de su vida o libertad personal de conformidad con la ley". Además de que el artículo 4 afirma que todo ciudadano debe disfrutar de la protección de la ley y ser tratado de acuerdo con esta, cuyos derechos son inalienables.”<sup>175</sup> 113 Por consiguiente, teóricamente no podría existir una justificación del Estado para permitir que una fuerza extranjera incursionara en su territorio para privar de la vida a individuos de manera arbitraria.

---

<sup>175</sup> The Nation (2014) Drone Attacks. Nation.com [en línea] Disponible en: <http://nation.com.pk/letters/03-Feb-2013/drone-attacks> Consultado el 19/1016



A pesar de que las quejas de parte de algunas secciones del gobierno son concluyentes respecto a la intervención armada con drones militares por parte de Estados Unidos en el país, conforme al informe de la Comisión *Abbottabad*<sup>176</sup>, divulgado por al-Jazeera el 8 de julio de 2013, se hace referencia a la existencia de un acuerdo secreto entre Washington e Islamabad sobre el uso de drones en territorio pastún. Concretamente la Comisión *Abbottabad* tuvo a su cargo el estudio de las condiciones de la operación militares de parte de Fuerzas Especiales estadounidenses contra la supuesta casa de Osama ben Laden en la localidad pakistaní que da su nombre a la comisión. El gobierno pakistaní había clasificado el contenido del informe como información confidencial.

Pero el riesgo de este nuevo mecanismo para hacer la guerra está en que sencillamente pueda ser empleado como el componente para desatar una nueva etapa de terrorismo, un factor más para alimentar la paranoia de la audiencia internacional y consecuentemente el incremento del gasto de los Estados y la población en la industria de la seguridad, así como un nuevo “enemigo”<sup>177</sup> a vencer para las potencias mundiales, y es que en la Declaración Conjunta sobre la exportación y el uso posterior de los vehículos aéreos no tripulados armados o *Strike-Enabled (UAVs)*<sup>178</sup>, emitida por el Departamento de Estado de los Estados Unidos el 5 de octubre de 2016 y firmada por 48 países entre los que destaca el Reino Unido y Francia, se admite el riesgo de que los VANT de combate puedan ser aprovechados por organizaciones que amenacen la seguridad internacional dado que facilitarían las actividades de estos grupos.

Pero Pakistán no es más que otro de los cuantiosos casos en los que drones de combate de la CIA han tenido acción, pasando por encima de las normas internacionales de los derechos humanos y la propia constitución estadounidense. Y

---

<sup>176</sup> Aljazeera (2013) “Pakistan’s Bin Laden Dossier” *Al-Jazeera*, Aljazeera.com [en línea] Disponible en: <http://www.aljazeera.com/indepth/spotlight/binladenfiles/> Consultado el 19/10/16

<sup>177</sup> Evidentemente un enemigo más creado por la manufactura del establishment orientado a activar la economía de guerra con nuevas intervenciones armadas, pero esta ocasión frente a una amenaza meramente híbrida, es decir mezclando distintos tipos de medios para causar daños.

<sup>178</sup> Department of State (2016) *Joint Declaration for the Export and Subsequent Use of Armed or Strike-Enabled Unmanned Aerial Vehicles (UAVs)*. U.S. Department of State, Washington D.C. [en línea] Disponible en: <http://www.state.gov/r/pa/prs/ps/2016/10/262811.htm> Consultado el 21/10/16

es que en realidad la gran mayoría de las operaciones de este tipo han sido ejecutadas desde dicha agencia de inteligencia.

Por ejemplo, en 2012 salió a la luz luego de una demanda impuesta contra la CIA por haber utilizado un dron, concretamente el *Armed MQ-9 Reaper* por asesinar a ciudadanos estadounidenses en Yemen, quienes supuestamente tenían vínculos con al-Qaeda. Conforme a la información publicada por la revista estadounidense *Wired*<sup>179</sup>117, el primero de los asesinados por el gobierno fue Anwar Al-Awlaki, un clérigo radical y nativo de Nuevo México. Era conocido originalmente para su blog y los vídeos que publicaba en YouTube. Pero de acuerdo con el gobierno de Obama, el papel de Awlaki pasó de comercializador a operador planificador y reclutador de al-Qaeda en la Península Arábiga. Las autoridades estadounidenses afirman que tenía contactos con los secuestradores del 9/11, y otros ataques suicidas. Otra de las víctimas fue Samir Khan, editor de la revista inglesa *Inspire*, la cual fue supuestamente publicada por Al-Qaeda en la Península Arábiga y contenía información que amenazaba la seguridad occidental, con mensajes de extremismo y propaganda para unirse a las filas de la organización terrorista. Dos semanas más tarde, el hijo de 16 años de edad del clérigo, Al-Awlaki, también fue asesinado con drones de combate en Yemen, aunque en esta ocasión no se encontraron las pruebas necesarias para determinar la responsabilidad del gobierno estadounidense.

En efecto, debido a su conexión permanente con el ciberespacio, y su necesidad de contener un *software* para funcionar, son un potencial objetivo para actividades ilícitas debido a que el quid de los drones es meramente un computador que a través de algún tipo de *malware* con características especialmente afrentosas puede ser saboteado y manipulado para cumplir con fines que pongan en riesgo la vida de los humanos o que simplemente ejecuten una actividad ilegal.

En síntesis, con toda la tecnología que poseen los gobiernos hipotéticamente comprometidos con la paz, cuyas acciones están dedicadas al bienestar colectivo, los altos estándares de seguridad cibernética, la capacidad satelital para vigilar al mundo desde el espacio ultraterrestre, suena muy difícil que existan las

---

<sup>179</sup> Wired (2012) *Pentagon, CIA Sued for Lethal Drone Attacks on U.S. Citizens* Wired. [en línea] Disponible en: <https://www.wired.com/2012/07/drone-attacks-lawsuit/> Consultado el 25/10/16

probabilidades para que grupos clandestinos paramilitares puedan vulnerar de manera autónoma e independiente la seguridad internacional a gran escala, claro, a menos que el mismo sistema los cree. Lo cierto es que los estropicios más grandes se practican sobre las poblaciones más vulnerables en todos los sentidos, esencialmente localizadas en los países periféricos.

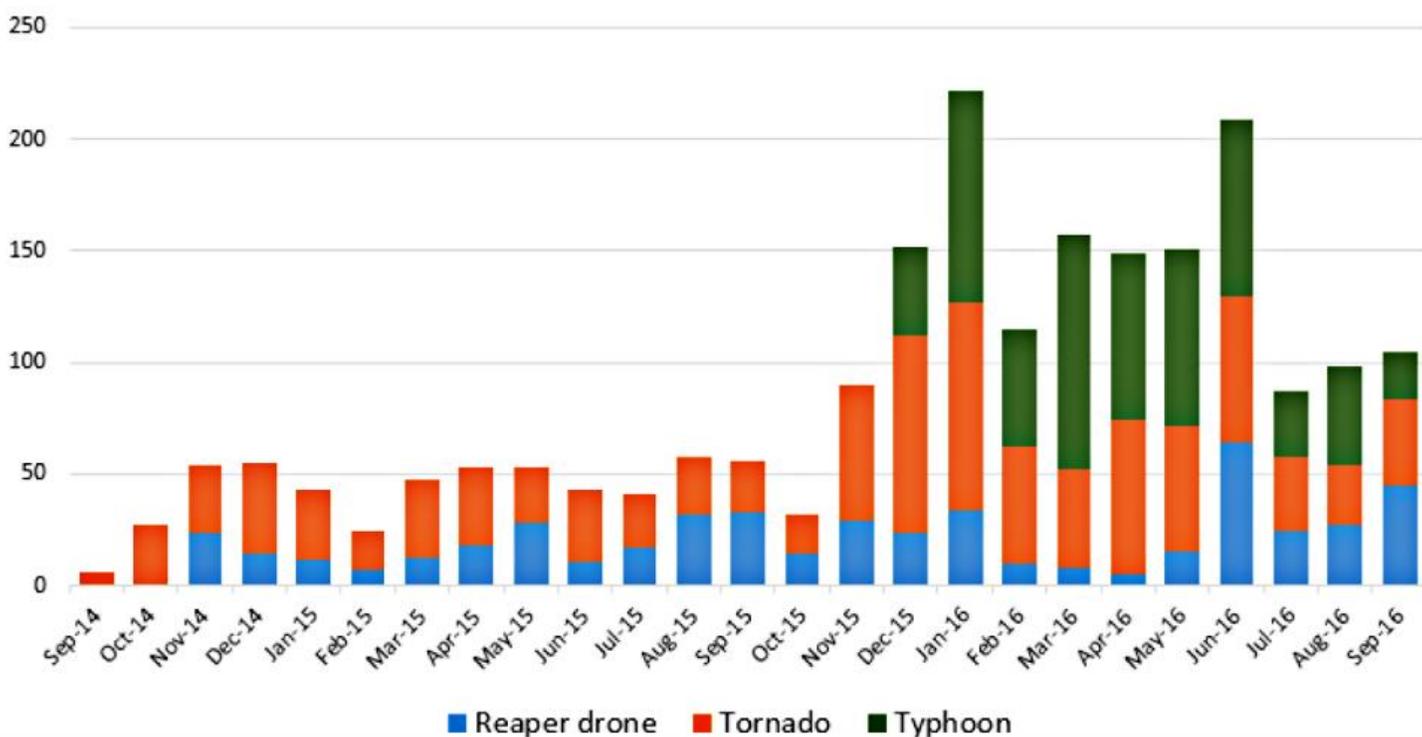
Conjuntamente, si bien hasta ahora no existe un grupo terrorista que amenace las seguridad local, regional o global por medio de VANT de combate la realidad es que los únicos que ya representan una amenaza real son agencias de inteligencia como la CIA, las únicas con la capacidad para utilizar estos métodos de guerra y por consiguiente quienes han vulnerado y aplastado las jurisdicciones en territorio ajeno. Entonces, ¿qué sentido tendría esperar a preocuparse a que los grupos extremistas cometan violaciones contra la humanidad, si las agencias de inteligencia hoy día tienen luz verde para practicar sus estrategias en cualquier parte del mundo periférico, sin límites, y causando laceraciones más agravantes?, encima de todo opacados por ser “daños colaterales” u operaciones necesarias para el mantenimiento de la paz.

Análogamente es menester resaltar que la fabricación de drones es la consecuencia de un mundo híper securitizado donde el complejo armado industrial no mediante el gobierno sino mediante importantes multinacionales dedicadas a la fabricación de armas como *General atomics*, *Boeing*, *Lockheed Martin* o *BAE Systems* llenan sus arcas ante la creciente tendencia por adquirir la tecnología destructiva más avanzada.

Para ilustrar, el conflicto armado en Siria e Iraq protagonizado por el choque de intereses de las potencias mundiales ha funcionado como un escenario más para la muestra del poderío militar de los países implicados en la destrucción del terrorismo, un campo de batalla producto de la pugna por la retención del poder donde las operaciones atestiguan el nivel de eficiencia de las armas y sobre todo consolidan la imagen de quien las posee. Inconcusamente, el actual conflicto en esa parte del mundo solo es una secuela del uso constante del poder duro por unos y otros países, lo cierto es que

desde la creación de *Daesh* países como el Reino Unido elevaron de forma literalmente estratosférica el número de ataques con VANT de ataque.

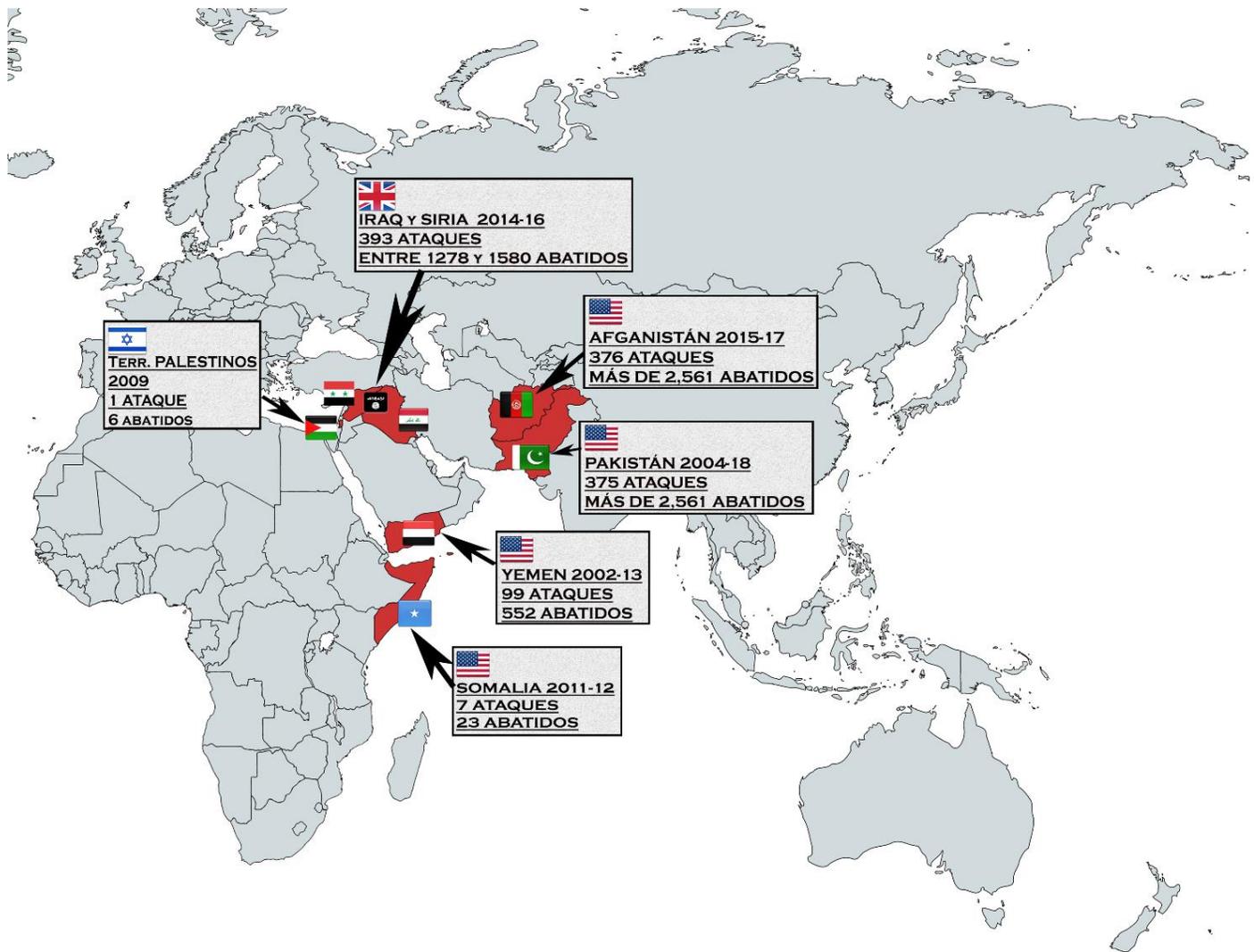
De acuerdo con los datos publicados por *Drone Wars* de septiembre de 2014 a noviembre de 2016 solamente en Iraq, el Reino Unido ha efectuado un total de 2,500 misiones y en Siria 706, lo que da un total de 3,206 operaciones militares con drones de combate aéreos<sup>180</sup>.



Gráfica 14. Número aproximado de armas lanzadas por VANTS de combate (de acuerdo a su tipo) del Reino Unido de la Gran Bretaña contra *Daesh* en Iraq y Siria entre 2014 y 2016. <sup>181</sup>

<sup>180</sup> Drone Wars (2016) UK Drone Strike Stats. Drone Wars UK. [en línea] Disponible en: <https://dronewars.net/uk-drone-strike-list-2/> Consultado el 15/11/16

<sup>181</sup> *Ibid.*



Mapa 5. Países del mundo sujetos de los principales ataques de VANT de combate y las correspondientes operaciones militares, así como el número aproximado de abatidos (militares y civiles) de 2002 a 2018.<sup>182</sup>

<sup>182</sup> Elaboración propia, datos extraídos de: Applegate Evan (2013) *The Drone War: A Comprehensive Map of lethal U.S. Attacks*, Bloomberg.com [en línea] Disponible en: <https://www.bloomberg.com/news/articles/2013-05-23/the-drone-war-a-comprehensive-map-of-lethal-u-dot-s-dot-attacks> Consultado el 15/2/18; Forensic Architecture (2018) *Drone Strikes*, Forensic-architecture.org [en línea] Disponible en: <http://www.forensic-architecture.org/case/drone-strikes/> Consultado el 15/2/18; Purkiss Jessica y Serie Jack (2017) "Obama's covert drone war in numbers: ten times more strikes than Bush", *The Bureau of Investigate Journalism*, Thebureauinvestigates.com [en línea] Disponible en: <https://www.thebureauinvestigates.com/stories/2017-01-17/obamas-covert-drone-war-in-numbers-ten-times-more-strikes-than-bush> Consultado el 15/2/18



## 4. CONCLUSIÓN

La Internet representa el eje central del desarrollo político, económico, social, cultural y por supuesto tecnológico de la civilización contemporánea, es la vía por medio de la que se conectan los adelantos tecnológicos de cada materia, su incidencia se extiende desde los complejos militares más importantes hasta la vida cotidiana de la audiencia global. Asimismo, su nivel de trascendencia se ejemplifica en la contemporaneidad como la proyección de la estructura social, política y económica del presente, y del porvenir.

La red informática mundial es una herramienta, a través de la cual grupos de poder que por medio de Estados y a su vez grandes multinacionales a escala mundial cooperan y rivalizan entre sí por y para el control del tráfico informático y consiguientemente el monitoreo de las audiencias de la Internet en el ámbito local, regional y global, empleando técnicas de manipulación, mecanismos de censura y de control del contenido.

En este tenor, a lo largo de esta investigación se ha explicado la actuación de los principales medios utilizados dentro del ciberespacio para hacer efectivas dichas estrategias. En cuanto a la educación y los medios de comunicación<sup>183</sup> fueron develadas algunas de las maniobras ejecutadas a través de las proveedoras de servicios de Internet ya fuesen tanto de la República Popular China como de Estados Unidos para generar un ambiente en donde la seguridad sea necesaria ante todo, aún y cuando esta implique transgredir la privacidad de los usuarios, indirectamente otorgando los datos a empresas multinacionales y al gobierno mismo acerca de toda actividad de la audiencia en el ciberespacio.

Conjuntamente se debe resaltar la trascendencia adjudicada a los medios sociales como una alternativa supuestamente independiente que permite a la audiencia global ser capaz de exponer sus ideas libres de la censura y difundirlas con mucha mayor facilidad y solvencia a través del ciberespacio, por otro lado, ante el vacío dejado por la falta de regulación y la permisividad en el ciberespacio,

---

<sup>183</sup> Ver apartado 1.2. Educación y medios de comunicación.

acentuada principalmente en países semi-periféricos y periféricos, los agentes<sup>184</sup> autónomos cobran protagonismo y suman a la complejidad de la Internet.

No obstante, se considera que entender a la red como un espacio libre capaz de empoderar a la sociedad frente a los detentores del poder resulta una idea ingenua cuyos hechos que le convalidan solo son parte del andamiaje del control en la red. Y es que, la Internet y los medios sociales en especial son un arma de doble filo, puesto que tanto son la fuente de información más frecuentada, grande y accesible para al menos la mitad de la población, como un medio de monitoreo social a la que esencialmente la sociedad civil en general se ha tenido que someter voluntariamente para estar al día con la modernidad, en el mismo sentido las redes sociales son el medio de comunicación que, paulatinamente continúa desplazando a los antiguos medios masivos de comunicación, aunado a su aproximación inexorable con la tecnología y el raudo paso de los avances tecnológicos en la contemporaneidad lo que ha dado pie a convertirse en el medio informativo y comunicativo más popular e importante.

Lo cierto es que la Internet es una herramienta necesaria en la estructura de la sociedad contemporánea e independientemente si aún la mitad de la población mundial no cuenta con acceso al ciberespacio mes con mes las cifras de quienes se conectan a la red crecen, encaminando a la audiencia de la Internet hacia un futuro que perpetre la integración de la tecnología y la Internet cabalmente al *modus vivendi* cada ciudadano del mundo. De ahí la significancia del ciberespacio y sus alcances en el ámbito geopolítico conque la función medular se afinca en la capacidad para incidir en la población en determinadas formas.

También, es necesario reiterar que la humanidad vive los efectos de un contexto global abanderado por los esfuerzos de grupos de poder que lideran a los Estados más poderosos para mantener o modificar el *statu quo* a escala mundial, esto es que se debe entender que la estructura del ciberespacio obedece a la dinámica de poder regida por un orden multipolar donde la colisión de modelos capitalistas se enuncia a través de la desinformación, la contra propaganda, los ciberataques y los conflictos armados no convencionales cuyas operaciones son orquestadas desde la

---

<sup>184</sup> Entendidos como actores a nivel individual.



red informática mundial. En otras palabras, el ciberespacio refleja la realidad internacional. Una pugna que comprende primeramente a Estados Unidos como la potencia hegemónica alimentada por los procesos políticos y los raudos avances tecnológicos producto de la competencia directa del siglo pasado que le permitieron exaltar su autoridad en la actualidad y ubicarse incuestionablemente como el depositario de los sitios *web* más grandes y populares del ciberespacio. Asimismo, otros Estados como la Federación Rusa y la República Popular China quienes han comprendido la trascendencia de la *web* y han encaminado esfuerzos para fortalecer su papel en el mundo a través de este medio; uno resurgiendo del encapotado término del siglo pasado, conservando aún un *status* importante como potencia propietaria de uno de los arsenales más vastos y devastadores, además del territorio más extenso del mundo; otro manifestándose como una opción fuerte sustentada en su capacidad económica, y su creciente expansión comercial y de dependencia tecnológica hacia cada región del planeta. Del mismo modo, las desgastadas potencias tradicionales arraigadas en Europa que se encargaron del llevar el capitalismo colonial e imperial a través del mundo, hoy ensambladas en la Unión Europea y precedidas por Alemania y Francia asociadas con su cófrade externo, el Reino Unido poseen junto con sus intendentos al otro lado del océano Atlántico la zona de libre comercio más grande del mundo, donde se concentra la dinámica de compraventa electrónica y de intercambio de información ciberespacial más grande además de casi la mitad del producto interno bruto mundial<sup>185</sup>.

De esta forma se sostiene que, la mecánica ciberespacial en Occidente está encaminada a la atracción de las audiencias de otros actores internacionales y sus áreas de influencia que aún no son usuarios de las multinacionales proveedoras de servicios de Internet principalmente estadounidenses. Por otra parte, la Federación Rusa y la República Popular China concentran sus esfuerzos en desarrollar estrategias orientadas hacia el blindaje del ciberespacio principalmente en su territorio (como el apoyo a *Rutnet* o la libertad para operar otorgada a *Tencent* y

---

<sup>185</sup> TAFTA *Transatlantic Free trade area*, datos extraídos de: Victor, Jean-Christophe (2016) "Comment le commerce international se transforme-t-il?", La dessous des cartes, *Arte.tv* [en línea] Disponible en: <https://www.youtube.com/watch?v=QcXOrl-025U> Consultado 11/2/18

*Alibaba*, respectivamente<sup>186</sup>) dado que la hegemonía del tráfico informático en los países de sus zonas de influencia aún se encuentra en disputa con las plataformas occidentales.

En este tenor, en el caso de la Federación Rusa el perfeccionamiento de redes sociales como *VKontakte* y navegadores y motores de búsqueda como *Yandex* y *Mail.ru* que más allá de emplear como primera lengua el ruso, promueven el uso del alfabeto cirílico también concentran al mismo tiempo a la audiencia de países más allá de sus fronteras que utilizan este alfabeto, fortaleciendo los lazos culturales y exaltando la identidad e incluso el nacionalismo, *tête à tête* con las empresas predominantemente de habla inglesa y cuyo contenido de una u otra manera gira en torno a Estados Unidos. Paralelamente en la República Popular China las proveedoras de servicios de Internet más importantes *Tencent*, y *Alibaba* igualmente detentoras de las redes sociales y motores de búsqueda más populares encauzan sus objetivos hacia el comercio y consumo masivo interno, y la propagación de sus plataformas en más ámbitos de la vida cotidiana como la venta de comida, inmuebles y otros bienes siempre a través de la red.<sup>187</sup>

Aunado a esto se debe resaltar que como se explicó a lo largo de esta investigación, las plataformas alternativas a las estadounidenses creadas en dichos adversario geopolíticos no son ni opuestas ni completamente alternativas, en su lugar tratan de conjuntar los servicios ya prestados en estas y expandirlos hacia otras funcionalidades como la visualización de videos o bien la integración de funciones de compra-venta en línea, las cuales en el modelo de Occidente se encuentra fraccionadas por empresas especializadas, verbigracia *Amazon* (comercio electrónico) *Facebook* (red social), etcétera, de este modo adaptando sus plataformas al modelo predominante, tomando rasgos y asimilando las bases de este en lugar de crear uno nuevo.

Para ilustrar, las versiones del navegador y buscador web chino *Baidu* descargables fuera de la República Popular China disponibles en países

---

<sup>186</sup> Ver apartado 2.2. Motores de búsqueda, navegadores *web* y redes sociales, herramientas de influencia política mundial.

<sup>187</sup> Ver apartado 2.2.2.2. *QZone*, p.94

Occidentales como Estados Unidos y sus zonas de influencia como México, contienen los botones de *Facebook* y *WhatsApp* como extensiones por *default*, también temas con mosaicos de ciudades, películas monumentos y gente de Occidente, estos últimos disponibles también al interior de ese país. De manera similar en *Youtube* aparecen los iconos de *VK* y *Odnoklassniki* para compartir contenido a los cuales incluso se puede iniciar sesión mediante una cuenta de *Facebook*. En suma, no se busca la creación de un modelo diferente, ni el contrapeso a la cultura Occidental, sino emularla, pero a través de sus propias empresas y publicidad, inscribiendo una nueva lógica política, social y cultural, pero principalmente económica centrada a futuro en el ciberespacio.

Para finalizar, se visualiza a la población a nivel mundial cabalmente ligada a la tecnología y monitoreada a través de la Internet, en un panorama donde desde los detalles más superfluos como las búsquedas en la red, hasta las emociones transmitidas por los usuarios son recopiladas por empresas multinacionales y gobiernos de los Estados más poderosos a escala mundial. Se considera que además de todos sus usos y aplicaciones la Internet posee una función medular en el orden social actual y del porvenir pues es gracias a la telecomunicación que la interrelación entre los actores, desde Estados hasta agentes ha sido avivada a una velocidad estrepitosa. Es por eso que se estiman las posibilidades de la germinación de una cultura más allá del ámbito social directo, orientada a la moda y el súper consumismo, centrada en el ciberespacio y controlada por los grupos de poder dominantes a la cabeza de los Estados más poderosos.

Así, se entiende la dinámica de poder en el mundo, como una regida por un orden multipolar a su vez dominado por monopolios de empresas dedicadas a la tecnología, pero con su dominio extendido igualmente sobre recintos anteriormente no propios de la tecnología, sino más bien adaptados y optimizado hacia ella, como la compra-venta instantánea de artículos de cualquier índole, la salud, o bien los productos *Smart house*.



## 5. GLOSARIO

***Big Data***: Es el almacenamiento masivo de información, en cantidades estratosféricas que ningún ordenador convencional puede albergar.

**Ciberespacio**: Es un término de cibernética con el cual se designa una “realidad artificial” creada por medios electrónicos.<sup>188</sup>

***Deep web***: Es la parte más grande de la Internet, consiste en el contenido que no puede ser encontrado con buscadores *web* convencionales.

***Darknet*** también llamada: Es la parte de la *Deep Web* cuyo contenido es completamente anónimo y al que no se puede ingresar con buscadores *web* ya sean convencionales o no, sino a través de *software* especializado.

**Internet**: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.<sup>189</sup>

***Malware (Malicious software)***: es un *software* diseñado para causar daño o realizar acciones indeseadas en el sistema operativo de la computadora.<sup>190</sup>

**Motores de búsqueda *web* convencionales**: Es el término que en esta investigación se ocupa para referirse a motores de búsqueda como *Google, Yahoo, Bing*, entre otros. que pueden encontrar páginas *web* disponibles en la *Surface web*.

***Smart House products***: Productos para uso en el hogar, caracterizados por ser mecánicos, funcionar con energía eléctrica, estar conectados con la Internet ya sea

---

<sup>188</sup> Definición extraída de la página oficial de la Real Academia Española. Consultado el 26/7/16

<sup>189</sup> Definición extraída de la Enciclopedia de la política de Rodrigo Borja. Consultado el 26/7/16

<sup>190</sup> 125 Christensson, P. (2006). *Malware Definition*. [en línea] Disponible en: <http://techterms.com> Consultado el 27/8/16

con o sin la necesidad de cables, además contar con microprocesadores almacenamiento de datos, sensores y *software* integrado.

***Software:*** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.<sup>191</sup>

***Surface web:*** Se refiere al contenido de la Internet que puede ser encontrado con buscadores *web* convencionales.

**Virus informático:** Los virus son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se de cuenta. Estos, por lo general, infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada archivos o datos almacenados en el computador.

---

<sup>191</sup> *Ibid.*



## 6. FUENTES CONSULTADAS

### Bibliografía:

1. **Bartlett, Jamie** (2015) *The Dark Net: Inside the Digital Underworld*, Melville House. Estados Unidos.
2. **Brzezinski, Zbigniew** (1970) *Between two ages American role in the technetronic era*. Nueva York. Estados Unidos.
3. **Camacho, José Luis**. (2015) *La conspiración reptiliana y otras verdades que ignoras*. Ediciones Planeta, España.
4. **Foucault, Michel, Rabinow, Paul** (editor) (1991) *The Foucault Reader: An introduction to Foucault's thought*, Penguin, Estados Unidos.
5. **Kennedy, Paul** (1994) *Auge y caída de las grandes potencias*. Debolsillo. Estados Unidos
6. **Madhavan J.** (2009) *Harnessing the Deep Web: Present and Future* Cornell University Library.
7. **MacMillan. I.C.** (1978). *Strategy Formulation: political concepts*. West Publishing. Estados Unidos.
8. **Mills W.** (1956) *The power elite*. New Edition Estados Unidos.
9. **Moore, Daniel & Rid, Thomas** (2016) *Cryptopolitik and the Darknet*, Survival.
10. **Nye Jr., Joseph S.** (2011) *The future of power*, Public Affairs. Estados Unidos
11. **Nye Jr., Joseph S.** (2003). *La paradoja del poder norteamericano*. Taurus. Estados Unidos.
12. **Nye Jr., Joseph S.** (2005) *Soft Power: The Means To Success In World Politics*, Public Affairs, Estados Unidos.
13. **Pallaver, Matteo** (2011) *Power and Its Forms: Hard, Soft, Smart*, The London School of Economics and Political Science. Londres, Reino Unido.
14. **Schmidt H., Teubener K. Konradova N.** (2006) *Control+Shift Public and private Usages of the Russian Internet*, Books on Demand GmbH, Norderstedt, Alemania.
15. **Téllez, Carvajal Evelyn** (2016). *Derecho y TIC Vertientes Actuales*, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, México.
16. **Turow, Joseph** (2017) *The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power*, Yale University press books, Estados Unidos.
17. **Wallerstein, Immanuel** (2005) *Análisis de Sistemas-Mundo*, Siglo XXI. México.
18. **Weegan, Federico César** (2015) *Terra Incógnita Bases para una política criminal pro persona en la Sociedad Digital*, INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación México.



### Cyberografía:

#### *Surface web.*

1. **Alexa** (2018) Alexa.com [en línea] Disponible en: <http://www.alexacom/>
2. **Aljazeera** (2013) “Pakistan’s Bin Laden Dossier” *Al-Jazeera*, Aljazeera.com [en línea] Disponible en: <http://www.aljazeera.com/indepth/spotlight/binladenfiles/>
3. **Analytics USA**, (2018) About this site, Analytics.usa.gov [en línea] Disponible en: <https://analytics.usa.gov>
4. **ANSA** (2016) “Venti di cyber-guerra Usa-Russia. Mosca: 'Giocano col fuoco’”. ,ANSA, ANSA.it [en línea] Disponible en [http://www.ansa.it/sito/notizie/mondo/nordamerica/2016/10/15/usa-preparavano-cyberattacco-a-russia\\_f7bae3b0-0c20-4f5b-b0a2-a59554c3ba33.html](http://www.ansa.it/sito/notizie/mondo/nordamerica/2016/10/15/usa-preparavano-cyberattacco-a-russia_f7bae3b0-0c20-4f5b-b0a2-a59554c3ba33.html)
5. **Applegate, Evan** (2013) *The Drone War: A Comprehensive Map of lethal U.S. Attacks*, Bloomberg.com [en línea] Disponible en: <https://www.bloomberg.com/news/articles/2013-05-23/the-drone-war-a-comprehensive-map-of-lethal-u-dot-s-dot-attacks>
6. Balkhi, S. (2013) *25 Biggest Cyber Attacks In History*. List25.com [en línea] Disponible en: <http://list25.com/25-biggest-cyberattacks-in-history/5/>
7. **Banco Mundial**, (2018) [en línea] Sitio web: <http://datos.bancomundial.org>
8. **Bandurski, David** (2015) “How China’s Government Controls the News: A Primer”, *Foreign Policy*, Foreignpolicy.com [en línea] Disponible en: <http://foreignpolicy.com/2015/07/21/china-media-xi-jinping-crackdown-newspaper/>
9. **Barack Obama White House** (2015) *Net neutrality President Obama’s Plan for a Free and Open Internet*, Obamawhitehouse.archives.gov [en línea] Disponible en: <https://obamawhitehouse.archives.gov/node/323681>
10. **Barber, John F.** (2016) *Digital storytelling: New opportunities for humanities scholarship and pedagogy*. Cogent arts&humanities. Tandfonline.com [en línea] Disponible en: <http://www.tandfonline.com/doi/full/10.1080/23311983.2016.1181037>
11. **BBC** (2016) “Ataque en Niza: al menos 84 muertos al arrollar un camión a una multitud que celebraba la fiesta nacional de Francia.” *BBC Mundo*. Bbc.com [en línea] Disponible en: <http://www.bbc.com/mundo/noticias-internacional-36800755>
12. **Borja, Rodrigo** (2012) **Enciclopedia de la Política**. México [en línea] Disponible en: <http://www.encyclopediadelapolitica.org/Default.aspx?i=e>



13. **Boswell W.** (2016) *A Brief Overview of Baidu*. AboutTech. Websearch.about.com [en línea] Disponible en: <http://websearch.about.com/od/enginesanddirectories/p/baidu.htm>
14. **Business Insider**, (2018) Businessinsider.com [en línea] Disponible en: <http://www.businessinsider.com/>
15. **Claude-Paye J.** (2016), “Constitutionaliser l'état d'urgence” *Red Voltaire*. Voltaire.net Disponible en : <http://www.voltairenet.org/article192869.html>
16. **Clemente Annabel** (2018) “Pobreza y desigualdad en México, constantes desde 1996: Oxfam” *El Financiero*, Elfinanciero.com.mx [en línea] Disponible en: <http://www.elfinanciero.com.mx/nacional/mexico-parte-del-25-de-los-paises-mas-desiguales-del-mundo-oxfam.html>
17. **Cohn C., Timm T y York J.** (2012) *Global Online Freedom Act 2012 Is An Important Step Forward*. Electronic Frontier Foundation. [en línea] [en línea] Disponible en: <https://www.eff.org/deeplinks/2012/04/global-online-freedom-act>
18. **Davies, Madlen** (2015) “Average person now spends more time on their phone and laptop than SLEEPING, study claims” Daily Mail, Dailymail.com Disponible en: <http://www.dailymail.co.uk/health/article-2989952/How-technology-taking-lives-spend-time-phones-laptops-SLEEPING.html> Consultado el 28/1/18
19. **Doland. A.** (2016) *After New Regulations in China, What's Ahead for Baidu?* Advertising Age. Adage.com [en línea] Disponible en: <http://adage.com/article/digital/regulations-china-ahead-chinasbaidu/304745>
20. **Drone Wars** (2016) *UK Drone Strike Stats*. Drone Wars UK. [en línea] Disponible en: <https://dronewars.net/uk-drone-strike-list-2/>
21. **Finley, Klint** (2017) “This is the year Donald Trump kills net neutrality” *Wired*. Wired.com [en línea] Disponible en: <https://www.wired.com/2017/01/year-donald-trump-kills-net-neutrality/>
22. **Fombelle P.** (2013) *Estudio demográfico de los mercados digitales hispanoparlantes*. Mailify.com [en línea] Disponible en: [blog.es.mailify.com/emailmarketing-2/estudio-demografico-de-los-mercados-digitaleshispanoparlantes/](http://blog.es.mailify.com/emailmarketing-2/estudio-demografico-de-los-mercados-digitaleshispanoparlantes/)
23. **Forensic Architecture** (2018) *Drone Strikes*, Forensic-architecture.org [en línea] Disponible en: <http://www.forensic-architecture.org/case/drone-strikes/>
24. **Gaia Scorza Barcellona** (2016) “Privacy, WhatsApp 'rivelera' il tuo numero a Facebook” *La repubblica*, Repubblica.it [ en línea ] Consultado el 6/11/16 Disponible en:



- [http://www.repubblica.it/tecnologia/socialnetwork/2016/08/25/news/w-hatsapp\\_rivelera\\_il\\_tuo\\_numero\\_a\\_facebook-146611480/](http://www.repubblica.it/tecnologia/socialnetwork/2016/08/25/news/w-hatsapp_rivelera_il_tuo_numero_a_facebook-146611480/)
25. **GData Russia.** (2016) *G Data Security Labs published the report and the development of malware in 2014 | 2014 H2 G DATA Malware Report.* G Data Security [en línea] Disponible en: <http://gdatarussia.blogspot.mx/2015/05/g-data-securitylabs-2014-2014-h2-g.html>
  26. **Gibbs S.** (2016) “WhatsApp to give users' phone numbers to Facebook for targeted ads” *The guardian* [ en línea] Disponible en: <https://www.theguardian.com/technology/2016/aug/25/whatsapp-to-giveusers-phone-number-facebook-for-targeted-ads>
  27. **GlobalWebIndex.** (2018) *Globalwebindex.net* [en línea] Disponible en: <http://www.globalwebindex.net/>
  28. **Graciano, Ambar** (2013) *Los derechos humanos de tercera y cuarta generación.* Encuentro jurídico. [en línea] Disponible en: [http://www.encuentrojuridico.com/2013/01/los-derechos-humanos-de-terceray.html#/\\*\\*](http://www.encuentrojuridico.com/2013/01/los-derechos-humanos-de-terceray.html#/**)
  29. **Graham Mark y De Sabbata Stefano** (2014) *Average number of Tor users per day calculated between August 2012 and July 2013,* Internet geographies at the Oxford Internet Institute, Genbeta.com [en línea] Disponible en: <https://www.genbeta.com/seguridad/asi-es-el-mapa-del-uso-de-tor-en-cada-pais-del-mundo>
  30. **Gruchawka S.** (2006) *How-To Guide to the Deep Web for IT Professionals.* Techdeepweb.com [en línea] Disponible en: <http://techdeepweb.com/3.html>
  31. **Hack Story** (2013) *Ingeniería Social.* Hack Story. [ en línea ] Disponible en: [http://hackstory.net/Ingenier%C3%ADa\\_social](http://hackstory.net/Ingenier%C3%ADa_social)
  32. **Haworth J.** (2016) “Putlocker blocked in the UK by internet service providers after High Court order bans streaming site” *Mirror.* Mirror.co.uk [en línea] Disponible en: <http://www.mirror.co.uk/news/uk-news/putlocker-blocked-uk-internet-service-8060064>
  33. **Internet live stats** (2016) *Internet users.* Internetlivestats. [en línea] Disponible en: <http://www.internetlivestats.com/internet-users>
  34. **Kaspersky Daily,**(2013) *Clasificación de Malwares,* Kaspersky.com [en línea] Disponible en: <https://latam.kaspersky.com/blog/clasificacion-de-malwares/1608/>
  35. **Kim, Gyong Ho; Paddon, Anna R.** (1999) *Digital Manipulation as New Form of Evidence of Actual Malice in Libel and False Light Cases.* Communications and the law. Highbeam.com [en línea] Disponible en: <https://www.highbeam.com/doc/1G1-57388949.html>
  36. **L'express** (2016) “Un algorithme détecte les dépressifs à partir de leurs photos Instagram” *L'express.* Lexpress.fr [ en línea ] Disponible en: <http://www.lexpress.fr/actualite/societe/sante/un-algorithme->



[detecte-lesdepressifs-a-partir-de-leurs-photosinstagram\\_1822971.html](#)

37. **La Vanguardia** (2015) “La ciberdelincuencia se dispara un 71% en 2014 y más del 210% en 4 años.” *La Vanguardia*. Lavanguardia.com [en línea] Disponible en: <http://www.lavanguardia.com/tecnologia/20150908/54436339519/1-aciberdelincuencia-se-dispara-un-71-en-2014-y-mas-del-210-en-4-anos.html>
38. **Lavilla. E.** (2016) “Al menos 84 muertos en un ataque terrorista con un camión en Niza” *El Español*. Elespanol.com [en línea] Disponible en: [http://www.elespanol.com/mundo/20160714/139986990\\_0.html](http://www.elespanol.com/mundo/20160714/139986990_0.html)
39. **Le Monde** (2016) ”Terrorisme : état d’urgence et Etat de droit”. *Le Monde*. Lemonde.fr [en línea] Disponible en: [http://www.lemonde.fr/idees/article/2016/07/21/france-etat-durgence-et-etat-de-droit\\_4972713\\_3232.html#KbVzOOSFTTP7zKAO.99](http://www.lemonde.fr/idees/article/2016/07/21/france-etat-durgence-et-etat-de-droit_4972713_3232.html#KbVzOOSFTTP7zKAO.99)
40. **Levant E.** (2009) “Censorship in the internet age” *Red Voltaire*. *Voltairenet.com* [en línea] Disponible en: <http://www.voltairenet.org/article161124.html>
41. **Liu, Jack**(2016) “Tencent to Baidu, Chinese internet giants big on Big Data” *South China Morning Post*, Scmp.com [en línea] Disponible en: <http://www.scmp.com/tech/article/1954550/tencent-baidu-chinese-internet-giants-big-big-data>
42. **LiveInternet.ru through February 2014 en Nielson S.** (2014) *Yandex sees a market share increase powered by its search service*. Market Realist. [en línea] Disponible en: <http://marketrealist.com/2014/03/yandex-market-share-increase-poweredsearch/>
43. **Live Internet Russia** (2018), *Search Engines searches quantity on Russia*, Liveinternet.ru [en línea] Disponible en: [https://www.liveinternet.ru/stat/ru/searches.html?id=13&id=4&id=5&id=8&per\\_page=10&report=searchnmhes.html%3Fslice%3Dru&show=rebuild+graph&slice=ru](https://www.liveinternet.ru/stat/ru/searches.html?id=13&id=4&id=5&id=8&per_page=10&report=searchnmhes.html%3Fslice%3Dru&show=rebuild+graph&slice=ru)
44. **Loesche, Dyfed** (2017) *Ransomware Makes up Small Share of Growing Malware Threat*, Statista, 28 de junio de 2017, [en línea] Disponible en: <https://www.statista.com/chart/10045/new-malware-specimen-and-share-of-windows-based-malware/>
45. **Mander J.** (2017) *Daily time spent on social networks rises to over 2 hours*, Globalwebindex.net[en línea] Disponible en: <https://blog.globalwebindex.net/chart-of-the-day/daily-time-spent-on-social-networks/>
46. **Marketplace Tech with Molly Wood** (2017), “10/27/2017: Could Facebook Messenger be all things to all people?” *Marketplace tech*, [en línea] Disponible en:



- <https://www.marketplace.org/shows/marketplace-tech/102717-could-facebook-messenger-be-all-things-all-people>
47. **Mayo Clinic** (2018) *Illness anxiety disorder*, Mayoclinic.org [en línea] Disponible en: <https://www.mayoclinic.org/diseasesconditions/illness-anxiety-disorder/symptoms-causes/syc20373782>
48. **Moreno, Guadalupe** (2017), *Solo un 5% del contenido de Internet está en español*, Statista.com [en línea] Disponible en: <https://es.statista.com/grafico/11383/solo-un-5-del-contenido-de-internet-esta-en-espanol/>
49. **Neal R. W.** (2014) “Is WhatsApp Worth \$19 Billion? 6 Reasons Why Facebook Purchased The Mobile Messaging App” *International Business Times*. Ibtimes.com [en línea] Disponible en: <http://www.ibtimes.com/whatsapp-worth-19-billion-6-reasons-why-facebook-purchased-mobile-messaging-app-1557026>
50. **Nielson, Samantha**(2014) “Yandex sees a market share increase powered by its search service” *Market Realist*, Marketrealist.com [en línea] Disponible en: <https://marketrealist.com/2014/03/yandex-seeing-slowdown-growth>
51. **Oreskovic A.** (2015) *Facebook CFO: Expect growth to keep slowing*. Business Insider. Bussinessinsider.com [en línea] Disponible en: <http://www.businessinsider.com/facebook-cfo-expect-growth-to-keep-slowing-2015-7>
52. **Oshkalo A.** (2014) *All Facebook's and Odnoklassniki's users in Russia also use VK*. Russian Search Tips. Russiansearchtips.com [en línea] Disponible en: <http://www.russiansearchtips.com/2015/03/all-facebooks-and-odnoklassnikisusers-in-russia-also-use-vk/#more-3297>
53. **Parker, Ashley** (2016) “Donald Trump’s Energy Plan: More Fossil Fuels and Fewer Rules”, *The New York Times*, Nytimes.com [en línea] Disponible en: <https://www.nytimes.com/2016/05/27/us/politics/donald-trump-global-warming-energy-policy.html>
54. **Purkiss, Jessica & Serie, Jack** (2017) “Obama’s covert drone war in numbers: ten times more strikes than Bush”, The Bureau of Investigate Journalism, Thebureauinvestigates.com [en línea] Disponible en: <https://www.thebureauinvestigates.com/stories/2017-01-17/obamas-covert-drone-war-in-numbers-ten-times-more-strikes-than-bush>
55. **Radiosefarad** (2016), “¿Qué son las Guerras Híbridas?, con Jesús Manuel Pérez Triana” *Radio Sefarad*. Radiosefarad.com [en línea] Disponible en: <http://www.radiosefarad.com/que-son-las-guerras-hibridas-con-jesus-manuel-perez-triana/>



56. **Rand Corporation** (2018) *Paul Baran and the Origins of the Internet*, Rand.org [en línea] Disponible en: <https://www.rand.org/about/history/baran.html>
57. **ReactOS** (2015) *ReactOS as a second OS in Russian government*, Reactos.org [en línea] Disponible en: <https://www.reactos.org/forum/viewtopic.php?f=2&t=14298&sid=10bbe8f5d2774077a4fffb1469340824>
58. **Real Academia Española**. Diccionario de la lengua española. Edición del tricentenario. [en línea] Disponible en: <http://dle.rae.es/?id=LvskgUG>
59. **La Repubblica** (2016) “Oltre il 90% degli avvisi di sicurezza trascurati dagli utenti” *La repubblica*, Repubblica.it [ en línea ] Disponible en: [http://www.repubblica.it/tecnologia/sicurezza/2016/08/19/news/oltre\\_il\\_90\\_degli\\_avvisi\\_di\\_sicurezza\\_trascurati\\_dagli\\_utenti-146258149/](http://www.repubblica.it/tecnologia/sicurezza/2016/08/19/news/oltre_il_90_degli_avvisi_di_sicurezza_trascurati_dagli_utenti-146258149/)
60. **Roberston J.** (2014) “Leaked docs: NSA uses 'Candy Crush,' 'Angry Birds' to spy” *SFGATE*. [en línea] Disponible en: <http://www.sfgate.com/technology/article/Leaked-docs-NSA-uses-Candy-Crush-Angry-5186801.php#photo-5795281>
61. **Russell, Ishita** (2017) “China government pushes for stake in local tech giants Tencent, Alibaba, others” *Deal Street Asia*, [en línea] Disponible en: <https://www.dealstreetasia.com/stories/chinese-government-eyes-board-seats-in-local-tech-giants-including-tencent-84046/>
62. **S/a.** (2016) The Deep Web. Hewilson. [en línea] Disponible en: <https://hewilson.wordpress.com/>
63. **SecurityMosmetod** (2017) *Классификация вредоносных программ* (clasificación del malware) Security.mosmetod.ru [en línea] Disponible en: <http://security.mosmetod.ru/zashchita-ot-virusov/44-klassifikatsiya-vredonosnykh-programm>
64. **Schneier B.** (2013), *What should we be worried about?* Edge.org Disponible en: <https://www.edge.org/response-detail/23818>
65. **Statista** (2018) Statista.com [en línea] Disponible en: <http://www.statista.com>
66. **Sullivan D.** (2016) *Google now handles at least 2 trillion searches per year*. Search Engine Land. Searchengineland.com [en línea] Disponible en: <http://searchengineland.com/google-now-handles-2-999-trillion-searches-peryear-250247>
67. **Syverson. P.** (2005) *Onion Rounting*. Onion Router. Onionrouter.net [en línea] Disponible en: <https://www.onion-router.net>
68. **T. Marx Gary**, *Technology and Social Control: The Search for the Illusive Silver Bullet Continues*, *Encyclopedia of the Social & Behavioral Sciences*, 2nd edition, forthcoming, Mit.edu [en línea] Disponible en: <http://web.mit.edu/gtmarx/www/techsoccon.html>



69. **Technopedia** (2018) *Distributed Denial of Service (DDoS)*, [en línea] Disponible en: <https://www.techopedia.com/definition/10261/distributed-denial-of-service-ddos>
70. **The Free Dictionary by Farlex**, Thefreedictionary.com [en línea], Disponible en: <https://legaldictionary.thefreedictionary.com>
71. **The History of SEO** (2017) *Short History of Early Search Engines*, fThehistoryofseo.com [en línea] Disponible en: [http://www.thehistoryofseo.com/TheIndustry/Short\\_History\\_of\\_Early\\_Search\\_Engines.aspx](http://www.thehistoryofseo.com/TheIndustry/Short_History_of_Early_Search_Engines.aspx)
72. **Topí, David** (2010) *Operaciones de Bandera Falsa*, Davidtopi.com [en línea] Disponible en: <http://davidtopi.com/operaciones-de-bandera-falsa/>
73. **Tsotsis A.** (2011) *Mubarak Shut Down The Internet, And The Internet Paid Him In Kind*. Tech Crunch. [en línea] Disponible en: <https://techcrunch.com/2011/02/11/feb11/>
74. **Ueland, Sig.** (2017) *20 Top Internet Service Providers*, Practivalcommerce.com [en línea] Disponible en: <https://www.practicalecommerce.com/20-Top-Internet-ServiceProviders>
75. **UNESCO, Foray Dominique** (consejero editorial) (2002) *La sociedad del conocimiento, Revista Internacional de Ciencias Sociales*, Unesco.org. PDF, [en línea ] Disponible en: <http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/SHS/pdf/171-fulltext171spa.pdf>
76. **Vena, Danny** (2017) *Better Buy: Baidu vs. Google*, Nasdaq.com [en línea] Disponible en: <http://www.nasdaq.com/article/better-buy-baidu-vs-google-cm812008>
77. **VK** (2018), *O сайте Аудитория ВКонтакте* (Acerca del sitio, Audiencia de VKontakte), Vk.com [en línea] Disponible en: [https://vk.com/page-47200925\\_44240810](https://vk.com/page-47200925_44240810)
78. **Vocativ Underworld.** (2018) Vocativ.com [en línea] Disponible en: <http://www.vocativ.com/underworld/>
79. **Yandex** (2018) *Privacy Policy*, Yandex.com [en línea] Disponible en: <https://yandex.com/legal/confidential/>
80. **Yippi**, (2018) Internet Users Search, Yippi.com [en línea] Disponible en: [http://new.yippy.com/search?query=Internet+users&tb=sitesearch\\_all&v%3Aproject=clusty-new](http://new.yippy.com/search?query=Internet+users&tb=sitesearch_all&v%3Aproject=clusty-new)
81. **W3Techs** (2018) *Most Popular traffic analysis tools*, w3techs.com [en línea] Disponible en: <https://w3techs.com>
82. **Wikileaks**, (2018) Wikileaks.org [en línea] Disponible en: <https://wikileaks.org/>
83. **Wired** (2018) Wired.com [en línea] Disponible en: <https://www.wired.com>



84. **Zimmermann Kim Ann & Emspak Jesse**, Live Science contributors (2017), *Internet History Timeline: ARPANET to the World Wide Web*, Livescience.com [en línea] Disponible en: <https://www.livescience.com/20727-internet-history.html>
- **Documentos Oficiales**
    1. **Asamblea Nacional** (1958) *Constitution de la République Française*, Assemblée-nationale.fr [en línea] Disponible en: [http://www.assemblee-nationale.fr/connaissance/constitution.asp#titre\\_5](http://www.assemblee-nationale.fr/connaissance/constitution.asp#titre_5)
    2. **Department of Defense** (2009) *Establishment of Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*. The Secretary of Defense 1000 Defense Pentagon, Washington DC, [en línea] Disponible en: [http://www.voltairenet.org/IMG/pdf/Establishment\\_Command\\_for\\_Military\\_Cyberspace\\_Operations-2.pdf](http://www.voltairenet.org/IMG/pdf/Establishment_Command_for_Military_Cyberspace_Operations-2.pdf)
    3. **Department of State** (2016) *Joint Declaration for the Export and Subsequent Use of Armed or Strike-Enabled Unmanned Aerial Vehicles (UAVs)*. U.S. Department of State, Washington D.C. [en línea] Disponible en: <http://www.state.gov/r/pa/prs/ps/2016/10/262811.htm>
    4. **G Data**. (2014) *G Data Security labs Malware Report*. G Data [en línea] Disponible en: [https://public.gdatasoftware.com/Presse/Publikationen/Malware\\_Reports/GData\\_PCMWR\\_H2\\_2014\\_EN\\_v1.pdf](https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/GData_PCMWR_H2_2014_EN_v1.pdf)
    5. **Moloney P.** (2012) *Promoting Global Internet Freedom: Policy and Technology*. Congressional Research Service. [en línea] Consultado el 29/10/16 Disponible en: <http://fpc.state.gov/documents/organization/201085.pdf>
    6. **Organización de las Naciones Unidas** (1948) *Declaración Universal de Derechos Humanos*, United Nations, [en línea] Disponible en: [http://www.un.org/es/documents/udhr/UDHR\\_booklet\\_SP\\_web.pdf](http://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf)
    7. **Organización de las Naciones Unidas** (1998) *Estatuto de Roma de la Corte Penal Internacional*, United Nations, [en línea] Disponible en: [http://www.un.org/spanish/law/icc/statute/spanish/rome\\_statute%28s%29.pdf](http://www.un.org/spanish/law/icc/statute/spanish/rome_statute%28s%29.pdf)
    8. **Organización de las Naciones Unidas** (1966) *Pacto Internacional de Derechos Civiles y Políticos*, Colegio de México, [en línea] Disponible en: [https://www.colmex.mx/assets/pdfs/2-PIDCP\\_49.pdf?1493133879](https://www.colmex.mx/assets/pdfs/2-PIDCP_49.pdf?1493133879)

*Deep web*



1. **Chat Tor** (2018) [en línea] Disponible a través de *Tor browser* en: <http://chattorci7bcgygp.onion/>
2. **DeepDotWeb** (2018) *Markets categories*, Deepdot35wvmeyd5.onion [en línea] Disponible a través de *Tor browser* en: <http://deepdot35wvmeyd5.onion/marketplacedirectory/categories/top-markets/>
3. **Dream market** (2018) [en línea] Disponible a través de *Tor browser* en: <http://xsuee6v24g2q6phb.onion/?ai=1675>
4. **Hansa Market** (2017) Hansamkt.onion [Fuera de línea desde octubre de 2017] Sitio *web*: [hansamkt2rr6nfg3.onion](http://hansamkt2rr6nfg3.onion)
5. **Soylent News** (2018) SoylentNews is people, [en línea] Disponible a través de *Tor browser* en: <http://7rmatpsvygnpjhrt.onion/breakingnews/>
6. **The Hidden Wiki** (2018) [en línea] Disponible a través de *Tor browser* en: <http://tdskbd7uolwsqqgn.onion/cgi-bin/wiki/TRHW.cgi/wiki?name=The+Hidden+Wiki>
7. **Wall Street Market** (2018) [en línea] Disponible a través de *Tor browser* en: <http://wallstyizjhkrvmj.onion/signup?ref=276>